

Class field theory and local global principle

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

Prasanna N Bhat



Indian Institute of Science Education and Research Pune

Dr. Homi Bhabha Road,

Pashan, Pune 411008, INDIA.

May, 2025

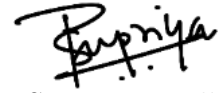
Supervisor: Dr. Supriya Pisolkar

© Prasanna N Bhat 2025

All rights reserved

Certificate

This is to certify that this dissertation entitled Class field theory and local global principle 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 Prasanna N Bhat at Indian Institute of Science Education and Research under the supervision of Dr. Supriya Pisolkar, Associate Professor, Department of Mathematics, during the academic year 2024-25.



Dr. Supriya Pisolkar

Committee:

Dr. Supriya Pisolkar

Dr. Debargha Banerjee

This thesis is dedicated to my parents for their constant support.

Declaration

I hereby declare that the matter embodied in the report entitled Class field theory and local global principle are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Dr. Supriya Pisolkar and the same has not been submitted elsewhere for any other degree.



Prasanna N Bhat

Acknowledgments

I would like to express my heartfelt gratitude to my supervisor, Dr. Supriya Pisolkar for her invaluable guidance during my Master's thesis. The insightful conversations that I have had with her, and the questions asked by her during presentations, have greatly enhanced my appreciation for class field theory. Most importantly, her emphasis on examples has helped me greatly appreciate their role in the development of a theory.

I am also grateful to Dr. Debargha Banerjee for the course in algebraic number theory offered by him, which has helped me significantly during my thesis. I would also like to thank him for agreeing to be the expert for my Master's thesis.

I would like to thank my friends for their affection and warmth which has made me feel at home here. The fun banter, the long walks around campus and our visits to various places across Pune have made my stay at IISER truly memorable.

I would like to express my sincere gratitude to Aravind, Ujwal, Josh and Ameya with whom I have had countless enriching discussions on mathematics, which have truly made my journey in mathematics an exciting journey of discovery. I would also like to thank Ameya and Manjima for discussing question papers of PhD entrances such as CSIR NET and NBHM with me, which has allowed me to devote ample time for my Master's thesis, without worrying about my preparation for these exams.

Lastly, I would like to express my sincere gratitude to my parents. They have not only been a bedrock of support to me, but have also gone out of their way on numerous occasions to help me in my endeavours.

Abstract

In this thesis, we explore the main statements of class field theory from the perspective of *local global principle*:

1. The existence of a canonical isomorphism from the Galois group $G(L|K)$ of a local (resp. number field) extension $L|K$ to $K^\times/N_{L|K}L^\times$ (resp. $C_K/N_{L|K}C_L$ where C_K is the idèle class group of the number field K).
2. A bijective correspondence between finite abelian extensions of a local field (resp. number field) and the finite index subgroups of its multiplicative group (resp. idèle class group).

In the process, we explore various instances of the *local global principle*, which asks whether a property that holds in all completions of the number field, holds in the number field itself. Important among them are the Kronecker-Weber theorem, Hasse norm theorem and the Grunwald-Wang theorem.

Contents

Abstract	xi
1 Preliminaries	3
1.1 Infinite Galois theory	3
1.2 Direct and inverse limits	5
1.3 Local fields	8
2 Kummer theory and Statements of local class field theory	19
2.1 Statements of local class field theory	20
2.2 Tate cohomology groups	21
2.3 Kummer theory	24
3 Abstract class field theory	27
3.1 G modules	27
3.2 Kummer theory	29
3.3 Abstract valuation theory	30
3.4 Construction of reciprocity map	34
3.5 Abstract reciprocity isomorphism	40
3.6 Abstract existence theorem	42

3.7 Herbrand quotients	43
4 Local class field theory: Proofs	47
4.1 Local class field axiom	47
4.2 Kronecker Weber theorem	51
5 Global class field theory	55
5.1 Preliminaries	56
5.2 Herbrand quotient of the Idèle class group	60
5.3 Global class field axiom	66
5.4 Global Reciprocity law	69
6 Grunwald Wang theorem	75
6.1 Local Global principle for n th powers	75
7 Primary units	79
7.1 p -primary units and behaviour of norm map	79
7.2 Local analogue of Martinet's theorem	82
7.3 Kummer's lemma	84
8 Conclusion	87

Introduction

We know that $\mathbb{Q}$ can be endowed with the Euclidean absolute value. $\mathbb{Q}$ can also be given the p -adic absolute values for every prime p . A remarkable theorem due to Ostrowski (1916) showed that the only non-trivial absolute values on $\mathbb{Q}$ are the p -adic absolute values and Euclidean absolute value. This can be easily generalised to a number field where the prime p is replaced by the prime ideals of its ring of integers, and the Euclidean absolute value is replaced by embeddings of the number field into $\mathbb{R}$ or $\mathbb{C}$. This led to the birth of the idea of *local global principle*, which says that a theorem or property holds for a number field if and only if it holds in all (or all but finitely many) of its completions. In other words, it asks whether given a property holding in all (or almost all) completions, we can ‘stitch together’ this information to obtain the property for the number field. As can be seen, this is not a rigorous mathematical statement, but only a guiding principle. The idea has led to significant advancements in various facets of mathematics, particularly in number theory.

In this thesis, we will explore class field theory, the development of which itself stands as a testament to the importance of local global principle. We will begin by exploring the main statements of local class field theory, and then go on to illustrate the striking parallel between local and global class field theory. In the process, we shall explore various instances of the local global principle. Particularly, we show that there is a local analogue of the famous Kronecker-Weber theorem, and use this to obtain the global Kronecker-Weber theorem. While exploring global class field theory, we will see another instance of the phenomenon, the so called Hasse norm theorem, which says that given a cyclic extension $L|K$, an element in a number field is a norm only if it is a norm at all its completions. Further, we will present the Grunwald-Wang theorem, which addresses the question of whether an element in a number field K that is a n^{th} power in almost all completions of K , is a n^{th} power in K .

Prerequisites: This thesis assumes a strong background in algebraic number theory.

It is also desirable that the reader be acquainted with local fields. However, most of the important results about local fields that will be used are presented in Chapter 1.

Original contributions: This thesis is purely expository and aimed to be a review of class field theory. No claims to originality are made. We have only attempted to write the proofs in a more accessible manner, and present a few clarificatory remarks and examples. The primary references for this thesis are [7] and [6].

Chapter 1

Preliminaries

We will begin the chapter by learning about the extension of Fundamental theorem of Galois theory to arbitrary algebraic extensions. We will also explore inverse and direct limits, and observe that the valuation ring of a local field and the Galois group of an algebraic extension are important examples of inverse limits. Finally, we will provide a quick review of local fields.

The contents of this chapter are primarily based on Sections 1 and 2 of chapter 4 and Chapter 2 of [7].

1.1 Infinite Galois theory

The fundamental theorem of Galois theory for finite extensions fails for infinite extensions. The below example will illustrate this.

Example 1. *The absolute Galois group of $\mathbb{F}_p$, i.e., $G_{\mathbb{F}_p} = G(\overline{\mathbb{F}_p}|\mathbb{F}_p)$, contains the Frobenius automorphism $\phi(x) = x^p$ for all $x \in \overline{\mathbb{F}_p}$. The subgroup generated by ϕ has the same fixed field as $G_{\mathbb{F}_p}$, but contrary to finite Galois theory, we do not have $\langle \phi \rangle = G_{\mathbb{F}_p}$.*

However, by defining a canonical topology called the Krull topology on the Galois group, we will be able to extend the fundamental theorem to infinite extensions.

Definition 1.1.1 (Krull topology). *Let $L|K$ be a Galois extension with Galois group $G(L|K)$.*

The Krull topology is defined by setting the basis of neighbourhoods about 1 as $\{G(L|M) \mid [M : K] < \infty\}$.

Theorem 1.1.1. *This topology endows $(G(L|K), \circ)$ with the structure of a compact Hausdorff (hence normal) topological group.*

Remark 1.1.1. *If the base field K is countable ($\mathbb{Q}, \mathbb{F}_p$), then the Galois group of any Galois extension $L|K$ is first countable, since the basis of neighbourhoods about 1 are in bijection with the finite Galois extensions of K contained in L . There are only countable many such distinct fields M , since $M = K(\alpha)$. A Hausdorff topological group that is first countable is metrisable by the Birkhoff Kakutani theorem.*

Definition 1.1.2 (Profinite groups). *A topological group that is compact, Hausdorff and has a basis of neighbourhoods about 1 comprising only of normal subgroups is called a profinite group.*

Example 2. 1. *Any finite group with discrete topology*

2. *The topological group $G = G(L|K)$ with Krull topology. Note that the groups $G(L|M)$ with $M|K$ Galois are normal subgroups, which are precisely the neighbourhoods about 1 in $G(L|K)$.*

In the next section, we will provide an important characterisation of profinite groups and give some examples.

We will now state the Fundamental theorem of Galois theory for arbitrary algebraic extensions.

Theorem 1.1.2 (Fundamental theorem of Galois theory). *Let $L|K$ be a Galois extension with Galois group $G = G(L|K)$. Then the map $f : M \mapsto G(L|M)$ is a 1-1 correspondence between*

$\{\text{Closed subgroups of } G\} \leftrightarrow \{\text{Subextensions } M|K \text{ of } L|K\}$ and

$\{\text{Open subgroups of } G\} \leftrightarrow \{\text{Finite extensions } M|K \text{ of } L|K\}$.

Furthermore closed normal subgroups $G(L|M)$ correspond to Galois extensions $M|K$ and open normal subgroups correspond to finite Galois extensions.

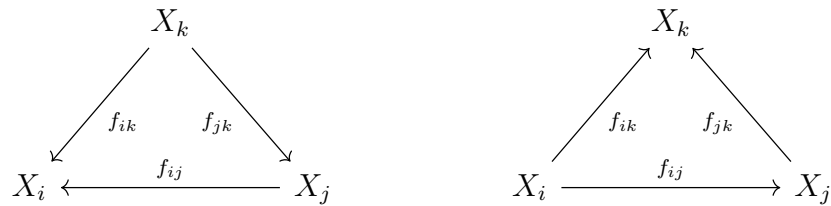
Remark 1.1.2. *It can now be shown that the closure of the subgroup generated by the Frobenius automorphism is equal to $G_{\mathbb{F}_p}$ in example 1.*

1.2 Direct and inverse limits

The notion of inverse (projective) and direct (inductive) limits generalise the operations of intersection and union. If $\{X_i\}$ is a family of subsets of a topological space X which for any two sets X_i, X_j also contain $X_i \cap X_j$ (resp. $X_i \cup X_j$), then the limit of this family is defined as $\varprojlim_{i \in I} X_i = \bigcap_{i \in I} X_i$ (resp. $\varinjlim_{i \in I} X_i = \bigcup_{i \in I} X_i$).

If $X_j \subseteq X_i$ (resp. $X_i \subseteq X_j$), then write $i \leq j$ such that the indexing set I is made into a directed system, i.e., a partially ordered set in which for every pair i, j , there is a k such that $i \leq k$ and $j \leq k$. Here, $X_k = X_i \cap X_j$ (resp. $X_k = X_i \cup X_j$). For $i \leq j$, let i_{ij} denote the inclusion $X_j \hookrightarrow X_i$ (resp. $X_i \hookrightarrow X_j$). We thus obtain a system $\{X_i, f_{ij}\}$ of maps and sets. We now replace inclusions by arbitrary maps f_{ij} .

Definition 1.2.1 (Projective and inductive system). *Let I be a directed system. A projective (resp. inductive) system over I is a family $\{X_i, f_{ij} \mid i, j \in I, i \leq j\}$ of topological spaces X_i and continuous maps $f_{ij} : X_j \rightarrow X_i$ (resp. $f_{ij} : X_i \rightarrow X_j$) such that $f_{ii} = \text{id}_{X_i}$ and the following diagrams commute (left diagram for projective system)*



Definition 1.2.2 (Projective/inverse limit). *The projective limit $X = \varprojlim_i X_i$ of the projective system $\{X_i, f_{ij}\}$ is defined to be $X = \{(x_i)_{i \in I} \in \prod_{i \in I} X_i \mid f_{ij}(x_j) = x_i \text{ for } i \leq j\}$. It inherits the subspace topology from the product topology on $\prod_{i \in I} X_i$.*

Remark 1.2.1. *It satisfies the following universal property: The inverse limit X of the*

system $\{X_i, f_{ij}\}$ is such that all the triangles commute in the following commutative diagram:

$$\begin{array}{ccccc}
 & & \varprojlim_{i \in I} X_i & & \\
 & \swarrow & \downarrow p_k & \searrow & \\
 & & X_k & & \\
 \swarrow f_{jk} & & & & \searrow f_{ik} \\
 X_j & \xrightarrow{f_{ij}} & & & X_i
 \end{array}$$

where p_i is the projection onto the i^{th} component. Here $i, j \leq k$.

Proposition 1.2.1. *The projective limit $X = \varprojlim_{i \in I} X_i$ of non-empty compact spaces is non-empty and compact. If all the X_i are Hausdorff, then X being the subspace of $\prod_{i \in I} X_i$ is Hausdorff.*

Definition 1.2.3 (Inductive/direct limit). *The inductive limit $X = \varinjlim_{i \in I} X_i$ of an inductive system $\{X_i, f_{ij}\}$ is the quotient $X := \sqcup_{i \in I} X_i / \sim$ of the disjoint union $\sqcup_{i \in I} X_i$, where two elements are considered equivalent if there is a $k \geq i, j$ such that $f_{ik}(x_i) = f_{jk}(x_j)$.*

Remark 1.2.2. *The direct limit satisfies the universal property as in Remark 1.2.1 with the direction of all the arrows reversed.*

Remark 1.2.3. *If $\{G_i, f_{ij}\}$ is a projective (resp. inductive) system of topological groups/rings, then the inverse limit (resp. direct limit) is also a topological group/ ring.*

Definition 1.2.4 (Morphism of a projective/ inductive system). *A morphism between two projective (resp. inductive systems) $\{G_i, g_{ij}\}$ and $\{G'_i, g'_{ij}\}$ of topological groups is a family of continuous homomorphisms $f_i : G_i \rightarrow G'_i$ such that the following diagrams commute:*

$$\begin{array}{ccc}
 G_j & \xrightarrow{f_j} & G'_j \\
 \downarrow g_{ij} & & \downarrow g'_{ij} \\
 G_i & \xrightarrow{f_i} & G'_i
 \end{array}
 \quad \text{resp.} \quad
 \begin{array}{ccc}
 G_i & \xrightarrow{f_i} & G'_i \\
 \downarrow g_{ij} & & \downarrow g'_{ij} \\
 G_j & \xrightarrow{f_j} & G'_j
 \end{array}$$

The following proposition shows that $\varinjlim$ preserves exact sequences.

Proposition 1.2.2. *Let $\alpha : \{G'_i, g'_{ij}\} \rightarrow \{G_i, g_{ij}\}$ and $\beta : \{G_i, g_{ij}\} \rightarrow \{G''_i, g''_{ij}\}$ be morphisms between inductive systems of topological groups such that the sequence $G'_i \xrightarrow{\alpha_i} G_i \xrightarrow{\beta_i} G''_i$ is exact for every $i \in I$. Then we obtain the exact sequence $\varinjlim_{i \in I} G'_i \xrightarrow{\alpha} \varinjlim_{i \in I} G_i \xrightarrow{\beta} \varinjlim_{i \in I} G''_i$.*

The next proposition shows that $\varprojlim$ preserves exact sequences for compact topological groups.

Proposition 1.2.3. *Let $\alpha : \{G'_i, g'_{ij}\} \rightarrow \{G_i, g_{ij}\}$ and $\beta : \{G_i, g_{ij}\} \rightarrow \{G''_i, g''_{ij}\}$ be morphisms between projective systems of compact topological groups such that the sequence $G'_i \xrightarrow{\alpha_i} G_i \xrightarrow{\beta_i} G''_i$ for every $i \in I$. Then $\varprojlim_{i \in I} G'_i \xrightarrow{\alpha} \varprojlim_{i \in I} G_i \xrightarrow{\beta} \varprojlim_{i \in I} G''_i$ is an exact sequence of compact topological groups.*

Remark 1.2.4. *Consider the family of exact sequences $\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z} \rightarrow 0$ with $\mathbb{Z}$ having discrete topology. Supposing that $\varprojlim$ preserves exact sequences in this case, we take the inverse limit to obtain that $\mathbb{Z} \rightarrow \mathbb{Z}_p \rightarrow 0$ is exact, which is absurd.*

The next proposition characterises profinite groups defined in Remark 1.1.2 as the inverse limit of finite groups.

Proposition 1.2.4. *If G is a profinite group and if N varies over all open normal subgroups of G , then $G \cong \varprojlim_N G/N$.*

Conversely, if $\{G_i, f_{ij}\}$ is a projective system of finite (even profinite) groups, then $G = \varprojlim_{i \in I} G_i$ is a profinite group.

Let us now look at some examples of inverse and direct limits.

Example 3 (Inverse limits). 1.

2. Let $\mathbb{Z}/p^i\mathbb{Z}$ be endowed with discrete topology. The system $\{\mathbb{Z}/p^i\mathbb{Z}, p_{ij}\}_{i,j \in \mathbb{N}}$ where $p_{ij} : \mathbb{Z}/p^j\mathbb{Z} \rightarrow \mathbb{Z}/p^i\mathbb{Z}$ for $i \leq j$ are the canonical surjections forms an inverse system. The inverse limit is called the ring of p -adic integers and is denoted $\mathbb{Z}_p$. It is in fact a compact, Hausdorff topological ring.

It can be shown that $\mathbb{Z}_p$ is a PID with unique maximal ideal. The fraction field of $\mathbb{Z}_p$ is called the field of p -adic numbers $\mathbb{Q}_p$. We will see in the next section that $\mathbb{Q}_p$ and their finite extensions are the so called p -adic local fields.

3. Notice that $\mathbb{Q}_p$ is a field of characteristic 0 since $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. There is a characteristic p analogue of this. Let $\mathbb{F}_q$ be the finite field with q elements where q is a power of a prime. Then the system $\{\mathbb{F}_q[t]/\langle t^n \rangle, p_{mn}\}$ where p_{mn} are the canonical projections forms an inverse system with inverse limit $\mathbb{F}_q[[t]]$, the ring of formal power series in $\mathbb{F}_q$. Its fraction field $\mathbb{F}_q((t))$ is the field of all formal Laurent series expansions in $\mathbb{F}_q$. $\mathbb{F}_q((t))$ together with their finite extensions are in fact the characteristic p local fields.
4. The Galois group of a Galois extension $L|K$ is a profinite group with respect to the Krull topology.
5. The rings $\{\mathbb{Z}/n\mathbb{Z}, p_{mn}\}$ where p_{mn} are the canonical surjections forms an inverse system. The inverse limit is denoted $\hat{\mathbb{Z}}$. It contains $\mathbb{Z}$ as a dense subring. The groups $n\hat{\mathbb{Z}}$ are precisely the open subgroups of $\hat{\mathbb{Z}}$, and we can easily see that $\hat{\mathbb{Z}}/n\hat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$. By applying Chinese remainder theorem and passing to the projective limit, we have $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$.
6. The absolute Galois group of $\mathbb{F}_q$ is the projective limit of $G(\mathbb{F}_{q^n}|\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$ which is $\hat{\mathbb{Z}}$.

Example 4 (Direct limits). 1. Let $\{X_i, f_{ij}\}$ be a system with X_i being topological spaces (groups/rings) such that for $i \leq j$, we have $X_i \subseteq X_j$, and let f_{ij} be the inclusions. This is a directed system as was shown at the start of the section. This is the most important example of direct limits that we will encounter throughout the thesis.

2. The system $\{\mathbb{Z}/p^i\mathbb{Z}, f_{ij}\}$ where $f_{ij} : \mathbb{Z}/p^i\mathbb{Z} \rightarrow \mathbb{Z}/p^j\mathbb{Z}$ where $i \leq j$ is given by $x \mapsto p^{j-i}x \bmod p^j$ forms an inductive system with direct limit $\mathbb{Z}(p^\infty)$, which is called the Prufer group.

1.3 Local fields

In the previous section, we described the ring $\mathbb{Z}_p$ as the inverse limit of $\mathbb{Z}/p^n\mathbb{Z}$ and called its fraction field $\mathbb{Q}_p$. In this section, let us study about $\mathbb{Q}_p$ and its finite extensions, which are called local fields.

We will only state the important results that will be used throughout the thesis. The proofs of these results may be found in Chapter 2 of [7]. We will first give an alternate and very important description of $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

Definition 1.3.1 (Absolute value). Let $a, b \in K$. An absolute value on a field K is a function $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$ such that:

1. $|a| = 0 \iff a = 0$.
2. Multiplicativity: $|ab| = |a||b|$ for all $a, b \in K$.
3. Triangle inequality: $|a + b| \leq |a| + |b|$ for all $a, b \in K$.

Definition 1.3.2 (Archimedean and non-Archimedean absolute value). If $|\cdot|$ satisfies the stronger triangle inequality $|a+b| = \max\{|a|, |b|\}$, then $|\cdot|$ is called non-Archimedean absolute value. If not, then $|\cdot|$ is called Archimedean absolute value.

Remark 1.3.1. Note that any absolute value induces a metric d by setting $d(x, y) = |x - y|$.

Example 5. The trivial absolute value $|a| = 1$ for all $a \in K$ is a non-Archimedean absolute value, while the Euclidean absolute value on $\mathbb{Q}$ is Archimedean.

Definition 1.3.3 (Equivalent absolute values). Two absolute values on K are said to be equivalent if they define the same topology on K .

We now state the approximation theorem, which may be regarded as a version of Chinese remainder theorem.

Theorem 1.3.1 (Approximation theorem). Let $|\cdot|_1, |\cdot|_2, \dots, |\cdot|_n$ be pairwise inequivalent absolute values on K , and let $a_1, \dots, a_n$ be given elements. Then for every $\epsilon > 0$, there is a $x \in K$ such that $|x - a_i|_i < \epsilon$ for all $i = 1, \dots, n$.

We now define the notion of a valuation.

Definition 1.3.4 (Discrete valuation). A discrete valuation is a surjective homomorphism $v : K^\times \rightarrow \mathbb{Z}$ such that $v_p(a+b) = \min\{v_p(a), v_p(b)\}$ for all $a, b \in K^\times$. v may also be regarded as a map $K \rightarrow \mathbb{Z} \cup \{\infty\}$ by declaring that $v(x) = \infty \iff x = 0$.

Definition 1.3.5 (p -adic absolute value). Fix a prime p . Let $a \in \mathbb{Q}^\times$ be such that $a = p^r u$ where $r \in \mathbb{Z}$ and $(u, p) = 1$. Then the p -adic absolute value of a , denoted $|a|_p$ is defined to be p^{-r} . This is a non-Archimedean absolute value. The p -adic valuation valuation v_p is given by $v_p(a) = r$.

Definition 1.3.6. The completion of $\mathbb{Q}$ with respect to the p -adic absolute value is called the field of p -adic numbers $\mathbb{Q}_p$, and the completion of $\mathbb{Z}$ with respect to the p -adic absolute value is called $\mathbb{Z}_p$.

Remark 1.3.2. *It can be shown that the ring of p -adic integers (also called the valuation ring) introduced here is in fact the inverse limit of $\mathbb{Z}/p^n\mathbb{Z}$ as introduced in the previous section, and the topology on $\mathbb{Z}_p$ induced as the inverse limit of $\mathbb{Z}/p^n\mathbb{Z}$ coincides with the topology induced from the p -adic absolute value.*

Remark 1.3.3. *The valuation ring $\mathbb{Z}_p$ can also be defined as the set of all elements in $\mathbb{Q}_p$ with p -adic absolute value less than or equal to 1. Equivalently, it is the set of all elements in $\mathbb{Q}_p$ with non-negative p -adic valuation.*

Remark 1.3.4. *The valuation ring $\mathbb{Z}_p$ is a PID and a local ring with unique maximal ideal $p\mathbb{Z}_p$.*

The following proposition says that any p -adic integer is a formal power series in p and any p -adic number is a formal Laurent series in p , thereby giving us a concrete way to understand elements of $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

Proposition 1.3.2. *Every p -adic integer $a \in \mathbb{Z}_p$ can be represented uniquely as a formal power series $a_0 + a_1p + \cdots + a_np^{n-1} + \cdots$. This power series converges in the p -adic absolute value. Furthermore, every $a \in \mathbb{Q}_p$ can be written uniquely as $a = p^n b$ where $n \in \mathbb{Z}$ and $b \in \mathbb{Z}_p$.*

The following result due to Ostrowski classifies all the absolute values on $\mathbb{Q}$.

Theorem 1.3.3 (Ostrowski). *The only non-trivial absolute values on $\mathbb{Q}$ are the p -adic absolute values for all primes p and the Euclidean absolute value.*

As a consequence, we obtain the important product formula.

Theorem 1.3.4 (Product formula). *For any $a \in \mathbb{Q}^\times$, we have $|a|_p = 1$ for almost all primes p and $\prod_{p \leq \infty} |a|_p = 1$ where $p = \infty$ denotes the Euclidean absolute value.*

The following theorem due to Ostrowski says that $\mathbb{R}$ and $\mathbb{C}$ are the only possible completions with respect to the Archimedean absolute value on any field K .

Theorem 1.3.5 (Ostrowski). *Let K be a field which is complete with respect to an Archimedean absolute value $|\cdot|$. Then, there is an isomorphism σ from K onto $\mathbb{R}$ or $\mathbb{C}$ satisfying $|a| = |\sigma(a)|^s$ for all $a \in K$ for some fixed $s \in (0, 1]$.*

Thus, we will henceforth restrict our attention to absolute values arising from a discrete valuation, which will in fact be non-Archimedean. Suppose that K is complete with respect to the non-Archimedean absolute value $|\cdot|$. The valuation ring is defined to be $O_K = \{x \in K \mid |x| \leq 1\}$. It will have unique maximal ideal which we will denote by $\mathcal{P}_K$. The quotient $O_K/\mathcal{P}_K$ is called the residue field of K and is denoted k_K . The groups of units of O_K will be denoted U_K . It is in fact the set $U_K = \{x \in K \mid |x| = 1\}$. It has a canonical filtration of subgroups $U_K^{(n)} := 1 + \mathcal{P}_K^n$. Note $U_K \supseteq U_K^{(1)} \supseteq U_K^{(2)} \cdots$. We also have

Proposition 1.3.6. *Let K be a field with a non-Archimedean valuation $|\cdot|$, and let $\mathcal{P}$, U_K and $U_K^{(n)}$ be as defined above. Then $U_K/U_K^{(1)} \cong k_K$ and $U_K^{(i)}/U_K^{(i+1)} \cong k_K^\times$. Furthermore, the maps $O \rightarrow \varprojlim_n O/\mathcal{P}^n$ and $U_K \rightarrow \varprojlim_n U_K/U_K^{(n)}$ are isomorphisms of topological groups.*

We will be interested in studying a finite extension $L|K$ of a complete valued field K . Thus, we must turn to the question of factoring polynomial equations. For this reason, Hensel's lemma is of fundamental importance.

We know that if a polynomial $p(x) \in K[x]$ is reducible in $K[x]$, then it factors in the residue field k_K . Hensel's lemma tells us that the converse is also true.

Proposition 1.3.7 (Hensel's lemma). *If a primitive polynomial $f(x) \in O_K[x]$ (i.e., if $|f| := \max\{|a_0|, \dots, |a_n|\} = 1$) admits modulo $\mathcal{P}$ a factorisation $f(x) \equiv \overline{g(x)h(x)} \pmod{\mathcal{P}}$ into relatively prime polynomials $\overline{g}, \overline{h}$, then $f(x)$ admits a factorisation $f(x) = g(x)h(x)$ into polynomials $g, h \in O_K[x]$ such that $\deg(g) = \deg(\overline{g})$ and $g(x) \equiv \overline{g(x)} \pmod{\mathcal{P}}$ and $h(x) \equiv \overline{h(x)} \pmod{\mathcal{P}}$.*

Remark 1.3.5. *The polynomial $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ factors into distinct linear factors in the residue field $\mathbb{F}_p$. Thus, from Hensel's lemma, we obtain the surprising fact that $(p-1)^{th}$ roots of unity are contained in $\mathbb{Q}_p$.*

Let us now address the question of extending a valuation.

Theorem 1.3.8 (Extension of absolute value). *Let K be complete with respect to an absolute value $|\cdot|$. Then $|\cdot|$ may be extended uniquely to an absolute value $|\cdot|'$ of any finite extension $L|K$. The extension is given by $|\alpha|' = \sqrt[n]{|N_{L|K}(\alpha)|}$, where $L|K$ has finite degree n . In this case, L is again complete.*

Remark 1.3.6. *An infinite algebraic extension of a complete field is never complete.*

We now turn to understanding arbitrary local fields.

Definition 1.3.7 (Local field). *A local field is a field complete with respect to a discrete valuation having finite residue field.*

Theorem 1.3.9. *A local field K is locally compact. Its valuation ring O_K is compact.*

We have the following important characterisation for local fields.

Theorem 1.3.10. *The local fields are precisely the finite extensions of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.*

Definition 1.3.8 (Ramification index and inertial degree). *Let $L|K$ be a finite extension of local fields. Then the inertia degree denoted $f_{L|K}$ is defined to be the degree of the residue field extension $k_L|k_K$, i.e., $f_{L|K} = [k_L : k_K]$.*

If $\mathcal{P}$ is the maximal ideal of O_K and $\mathcal{Q}$ that of O_L , then $\mathcal{Q} = \mathcal{P}^e$ for some natural number e , which is called the ramification index of $L|K$. It is denoted $e_{L|K}$. In fact, $e_{L|K}$ can also be defined as $[v(L^\times) : v(K^\times)]$.

We now state the important fundamental identity which relates the ramification index, inertial degree and degree of the local field extension.

Theorem 1.3.11 (Fundamental identity). *For a finite extension of local fields, we have $[L : K] = e_{L|K} f_{L|K}$.*

Also as a consequence of Theorem 1.3.8, we obtain

Theorem 1.3.12. *Let K be complete with respect to a valuation v_K and let $L|K$ be a finite extension. Then, $\frac{v_L}{e_{L|K}} = \frac{v_K(N_{L|K})}{n}$, where $e_{L|K}$ is the ramification index and $n = [L : K]$.*

We have the following structure theorem for the multiplicative group of a local field K :

Proposition 1.3.13. *$K^\times \cong \langle \pi_K \rangle \times U_K$ and $U_K \cong \mu_{q-1} \times U_K^{(1)}$. Here π_K is the prime element, $\langle \pi_K \rangle$ is the cyclic subgroup generated by π_K and $q = \#k_K$.*

Henceforth, we shall restrict our attention to finite extensions of $\mathbb{Q}_p$, which we will sometimes refer to as p -adic fields or p -adic number fields.

We now define two important maps, the logarithm and the exponential map which are inverses of each other.

Proposition 1.3.14. *For a p -adic number field K , there is a uniquely determined continuous homomorphism $\log : K^\times \rightarrow K$ such that $\log \mathcal{P} = 0$ which on $U^{(1)}$ is given by the series $\log(1+x) = x - x^2/2 + x^3/3 - \dots = \sum_{n=1}^{\infty} (-1)^{n-1} x^n/n$*

Theorem 1.3.15. *Let K be a p -adic number field with valuation ring O_K and maximal ideal $\mathcal{P}$, and let $pO_K = \mathcal{P}^{e_K}$. Then the power series*

$$\exp(x) = \sum_{i=0}^{\infty} x^i/i! \text{ and } \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} x^n/n$$

yield for $n > \overline{e_K} := e_K/(p-1)$ two mutually inverse topological isomorphisms

$$\mathcal{P}_K^{(n)} \xrightleftharpoons[\log]{\exp} U_K^{(n)}$$

Here e_K is the ramification index of $K|\mathbb{Q}_p$.

The following proposition gives the structure of the group of principal units.

Proposition 1.3.16. *Let K be a p -adic field and $q = p^f = \#k_K$. Then we have the topological group isomorphism $U_K^{(1)} \cong \mu_{p^a} \oplus \mathbb{Z}_p^d$ where μ_{p^a} is the group of roots of unity of p power order contained in $K^\times$ and $d = [K : \mathbb{Q}_p]$.*

As a corollary, we obtain the following result which determines the size of $K^\times/K^{\times n}$.

Corollary 1.3.17. $[K^\times : K^{\times n}] = n[U_K : U_K^{(n)}]$.

We now look at types of local field extensions: unramified, tamely ramified, totally and wildly ramified.

Definition 1.3.9. *A finite extension $L|K$ is called unramified if $[L : K] = [k_L : k_K] = f_{L|K}$, equivalently if the ramification index $e_{L|K} = 1$. An arbitrary algebraic extension is called unramified if it is the union of finite unramified subextensions.*

Example 6. *For any odd prime p , $\mathbb{Q}_p(\sqrt{u})|\mathbb{Q}_p$ such that $(u|p) = -1$ where $(\cdot|p)$ is the Legendre symbol is the unique degree 2 unramified extension of $\mathbb{Q}_p$. This is because the polynomial $x^2 - u$ is irreducible mod p , hence $\mathbb{F}_p(\sqrt{u})|\mathbb{F}_p$ is of degree 2.*

Theorem 1.3.18. *Unramified extensions form a distinguished class.*

Remark 1.3.7. By the previous theorem, composite of any two unramified extensions is again unramified, hence given any local field K , there is a maximal unramified extension denoted $\tilde{K}$ of K . If $L|K$ is an algebraic extension, then $L \cap \tilde{K}$ is the maximal unramified extension of $L|K$.

Proposition 1.3.19. The residue class field of $\tilde{K}$ is $\overline{\mathbb{F}_q}$ where $\mathbb{F}_q$ is the residue class field of K . The group of valuations of $\tilde{K}$ equals that of K .

The following theorem tells us that there is a unique unramified extension of any arbitrary degree over K .

Theorem 1.3.20. Let K be a local field and $n \in \mathbb{N}$. Then there is a unique unramified extension $L|K$ of degree n .

Definition 1.3.10. Tamely ramified extensions: An algebraic extension $L|K$ is called tamely ramified if $([L : L \cap \tilde{K}], p) = 1$ where $p = \text{ch}(k_K)$. For finite extensions $L|K$, this amounts to saying $e_{L|K} = 1$.

Remark 1.3.8. Note that by definition, an unramified extension is tamely ramified.

Example 7. For any odd prime p , the extension $\mathbb{Q}_p(\sqrt{p})|\mathbb{Q}_p$ has ramification index 2 since $\sqrt{p}$ is a prime lying above p in $\mathbb{Q}_p$ because $\sqrt{p}^2 = p$.

Theorem 1.3.21. Tamely ramified extensions form a distinguished class.

Definition 1.3.11 (Totally ramified extensions). A finite extension $L|K$ is said to be totally ramified if $[L : K] = e_{L|K}$.

Example 8. $\mathbb{Q}_p(\sqrt{p})|\mathbb{Q}_p$ is also an example of a totally ramified extension.

Definition 1.3.12 (Wildly ramified extensions). $L|K$ is wildly ramified if $(p, e_{L|K}) \neq 1$.

Example 9. $\mathbb{Q}_2(\sqrt{2})|\mathbb{Q}_2$ is a wildly ramified extension since $e_{L|K} = 2 = \text{ch}(\mathbb{F}_2)$.

The following two propositions tell us about the valuation ring, Galois group and ramification of p -adic cyclotomic extensions.

Proposition 1.3.22. Let $L = K(\zeta_n)$ and suppose that $(n, \text{ch}(k_K)) = 1$. Let $q = \#k_K$. Then we have:

(i) The extension $L|K$ is unramified of degree f , where f is the smallest integer such that

$q^f \equiv 1 \pmod{n}$.

(ii) The Galois group $G(L|K)$ is isomorphic to $G(k_L|k_K)$ and is generated by the automorphism $\phi : \zeta_n \rightarrow \zeta_n^q$.

(iii) $O_L = O_K[\zeta_n]$.

Proposition 1.3.23. *Let ζ be a primitive p^r th root of unity. Then we have:*

(i) $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$ is totally ramified of degree $p^{r-1}(p-1)$.

(ii) $G(\mathbb{Q}_p(\zeta)|\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$.

(iii) $\mathbb{Z}_p[\zeta]$ is the valuation ring of $\mathbb{Q}_p(\zeta)$.

(iv) $1 - \zeta$ is a prime element of $\mathbb{Z}_p[\zeta]$ with norm p .

Henceforth, let K be a number field and K_v its completion with respect to the valuation v . We turn to the problem of extending valuations to arbitrary algebraic extensions.

Theorem 1.3.24 (Extension theorem). *Let $L|K$ be an algebraic field extension and v a valuation of K . Then we have:*

(i) Every extension w of the valuation v arises as the composite $w = \bar{v} \circ \tau$ for some K embedding $\tau : L \rightarrow \overline{K_v}$.

(ii) Two extensions $\bar{v} \circ \tau$ and $\bar{v} \circ \tau'$ are equal if and only if τ and τ' are conjugate in w .

As a consequence, we obtain the following:

Proposition 1.3.25. *Suppose that $L|K$ is a finite extension of number fields, let $L = K(\alpha)$ and suppose that $f(X) = \min(\alpha, X)$. Then there is a 1-1 correspondence*

$$\{\text{Valuations } w_1, \dots, w_r \text{ extending } v \text{ to } L\} \leftrightarrow \{\text{Irreducible factors } f_1, \dots, f_r \text{ of } f(X) = \prod_{i=1}^r f_i(X)^{m_i} \text{ in } K_v\}$$

As a consequence of this, we obtain:

Proposition 1.3.26. *For a number field extension $L|K$, we have $L \otimes_K K_v \cong \prod_{w|v} L_w$.*

Corollary 1.3.27. *If $L|K$ is a number field extension, then $[L : K] = \sum_{w|v} [L_w : K_v]$, $N_{L|K}(\alpha) = \prod_{w|v} N_{L_w|K_v}(\alpha)$, $\text{Tr}_{L|K}(\alpha) = \sum_{w|v} \text{Tr}_{L_w|K_v}(\alpha)$ and $\sum_{w|v} e_w f_w = [L : K]$.*

We now define the decomposition, inertia and ramification groups.

Definition 1.3.13 (Decomposition group). *The decomposition group of an extension w of v to L is defined by $G_w(L|K) = \{\sigma \in G(L|K) \mid w \circ \sigma = w\}$.*

Definition 1.3.14 (Inertia group). *The inertia group of $w|v$ is defined by $I_w = I_w(L|K) = \{\sigma \in G_w \mid \sigma x \equiv x \pmod{\mathcal{P}} \text{ for all } x \in O_K\}$ where $\mathcal{P}$ is the prime ideal of L corresponding to the valuation w .*

Definition 1.3.15 (Ramification group). *The ramification group $R_w = R_w(L|K) = \{\sigma \in G_w \mid \frac{\sigma x}{x} \equiv 1 \pmod{\mathcal{P}} \text{ for all } x \in L^\times\}$.*

Proposition 1.3.28. *For a number field extension $L|K$, we have:*

$G_w(L|K) \cong G(L_w|K_v)$, $I_w(L|K) \cong I(L_w|K_v)$ and $R_w(L|K) \cong R(L_w|K_v)$. Here L_w and K_v are the completions of L and K with respect to w and v respectively.

The decomposition, inertia and ramification groups are only the first few terms in a whole series of subgroups which will be termed higher ramification groups. We assume now that $L|K$ is a finite Galois extension of number fields with Galois group G .

Definition 1.3.16 (Higher ramification groups). *For every real number $s \geq -1$, we define the s^{th} ramification group of $L|K$ by $G_s = G_s(L|K) = \{\sigma \in G \mid v_L(\sigma a - a) \geq s + 1\}$.*

Remark 1.3.9. *Clearly $G_{-1} = G$, G_0 is the inertia group and G_1 the ramification group. The higher ramification groups form a chain $G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \dots$ of normal subgroups of G . Also since G is finite and because there is no element with infinite valuation apart from zero, eventually $G_s = 1$.*

Definition 1.3.17 (Ramification break). *A real number $s \geq -1$ which satisfies $G_s \neq G_{s+r}$ for any real number r is called a ramification break of $L|K$.*

We will now determine the absolute values on a number field K . This will be crucial to our understanding of ‘local global principle’.

Definition 1.3.18 (Place). *A prime (or place) $\mathcal{P}$ of an algebraic number field K is a class of equivalent valuations of K . The nonarchimedean equivalence classes are called finite primes and the archimedean places are called infinite primes.*

Remark 1.3.10. *The infinite primes $\mathcal{P}$ are obtained from the embeddings $\tau : K \rightarrow \mathbb{C}$. There are two types of these: the real primes which are given by embeddings $\tau : K \rightarrow \mathbb{R}$, and the*

complex primes which are induced by pairs of complex conjugate embeddings $\tau : K \rightarrow \mathbb{C}$. If r denotes the number of real embeddings, s the number of complex conjugate embeddings, and if $[K : \mathbb{Q}] = n$, then $r + 2s = n$ and there are $r + s$ many infinite places.

We will refer to the finite primes as $\mathcal{P} \mid \infty$ and the infinite ones by $\mathcal{P} \nmid \infty$.

For a finite prime, $k(\mathcal{P})$ denotes the residue field of $K_{\mathcal{P}}$. For an infinite prime, we adopt the convention $k(\mathcal{P}) = K_{\mathcal{P}} = \mathbb{R}$ or $\mathbb{C}$.

If $\mathcal{P}$ is a finite prime, then $v_{\mathcal{P}}$ is the $\mathcal{P}$ adic valuation. For $a \in K^{\times}$, this is given by considering the prime ideal decomposition of the fractional ideal generated by a . If $\mathcal{P}$ is infinite, then $v_{\mathcal{P}}(a) := -\log|\tau a|$ where $\tau : K \rightarrow \mathbb{C}$ is an embedding defining $\mathcal{P}$.

For an arbitrary prime $\mathcal{P}$ lying above p (we denote this by $\mathcal{P} \mid p$), $f_{\mathcal{P}} := [k_K(\mathcal{P}) : k_K(p)]$.

Hence for infinite primes $f_{\mathcal{P}} = 1$ or 2 . We define $\mathcal{N}(\mathcal{P}) := \begin{cases} p^{f_{\mathcal{P}}} & \text{if } \mathcal{P} \mid \infty \\ e^{f_{\mathcal{P}}} & \text{if } \mathcal{P} \nmid \infty \end{cases}$.

Here the Euler number e may be regarded as an infinite prime.

We define the absolute value $|\cdot|_{\mathcal{P}} : K \rightarrow \mathbb{R}$ by $|a|_{\mathcal{P}} = \mathcal{N}(\mathcal{P})^{-v_{\mathcal{P}}(a)}$ for $a \neq 0$ and $|0|_{\mathcal{P}} = 0$. If $\mathcal{P}$ is infinite, then in fact, we have $|a|_{\mathcal{P}} = |\tau(a)|$ for a real prime $\mathcal{P}$ and $|a|_{\mathcal{P}} = |\tau(a)|^2$ for a complex prime $\mathcal{P}$.

For finite primes $\beta \mid \mathcal{P}$, the definition of ramification index $e_{\beta \mid \mathcal{P}}$ and inertial degree $f_{\beta \mid \mathcal{P}}$ are as defined for the local field extension $L_{\beta} \mid K_{\mathcal{P}}$. For $\mathcal{P}$ an infinite prime, we define $f_{\beta \mid \mathcal{P}} = [L_{\beta} : K_{\mathcal{P}}]$ and $e_{\beta \mid \mathcal{P}} = 1$.

We conclude this section with the product formula for a number field.

Proposition 1.3.29. *Given $a \in K^{\times}$, we have $|a|_{\mathcal{P}} = 1$ for almost all $\mathcal{P}$, and $\prod_{\mathcal{P}} |a|_{\mathcal{P}} = 1$.*

Chapter 2

Kummer theory and Statements of local class field theory

Class field theory characterises finite abelian extensions of a local/ global field in terms of some specific information, termed the ‘arithmetic’ of the base field. This information in the case of local fields are the finite index subgroups of the multiplicative group. This important result is called the existence theorem, as it talks about the existence of abelian extensions corresponding to these subgroups. Class field theory also tells us about the existence of a canonical homomorphism, called the reciprocity homomorphism on the Galois group of a finite Galois extension, which when restricted to abelian extensions is an isomorphism. This map has many important applications, such as in the proof of the existence theorem.

In this chapter, we will first look at the main statements of local class field theory, the proofs of which will be given in chapter 4. We will then define Tate cohomology groups, and restate the famous Hilbert Theorem 90 in terms of Tate cohomology groups. Finally, we will delve into Kummer theory, which will not only give us a partial result in the direction of the existence theorem, but is also important in its own right and will be used repeatedly throughout this exposition.

Throughout this chapter, L, K will denote local fields, (unless mentioned otherwise) and n a natural number, and G , $G(L|K)$ and $\text{Gal}(L|K)$ are used interchangeably to denote the Galois group of the Galois extension $L|K$, and the condition $(n, \text{ch}(K)) = 1$ is also taken to include the case $\text{ch}(K) = 0$, i.e., p -adic local fields.

The primary reference for this chapter is Chapters 4 and 5 of [7].

2.1 Statements of local class field theory

Theorem 2.1.1 (Reciprocity homomorphism). *Let $L|K$ be a finite Galois extension of local fields. Then there is a canonical homomorphism*

$$r_{L|K} : \text{Gal}(L|K) \rightarrow K^\times / N_{L|K} L^\times$$

which has the following properties:

1) *The induced map $r'_{L|K} : \text{Gal}(L|K)^{ab} \rightarrow K^\times / N_{L|K} L^\times$*

$$\begin{array}{ccc} G(L|K) & \xrightarrow{r_{L|K}} & K^\times / N_{L|K} L^\times \\ \downarrow & \nearrow r'_{L|K} & \\ G(L|K)^{ab} & & \end{array}$$

is an isomorphism.

In particular, when $L|K$ is abelian, $r_{L|K}$ is an isomorphism.

We will henceforth abuse notation by referring to $r'_{L|K}$ also as $r_{L|K}$.

2) *If $L|K$ is an unramified extension, then $r_{L|K}(\phi_{L|K}) = \pi_K \bmod N_{L|K} L^\times$, where π_K is a prime of $K^\times$.*

3) *Functoriality: If $L|K$ and $L'|K'$ are finite Galois extensions s.t. $L \subseteq L'$, $K \subseteq K'$, and if $\sigma \in G(L|K)$, then we have the commutative diagram*

$$\begin{array}{ccc} G(L'|K') & \xrightarrow{r_{L'|K'}} & K'^\times / N_{L'|K'} L'^\times \\ \sigma \mapsto \sigma|_L \downarrow & & \downarrow N_{K'|K} \\ G(L|K) & \xrightarrow{r_{L|K}} & K^\times / N_{L|K} L^\times \end{array} \quad \begin{array}{ccc} G(L|K) & \xrightarrow{r_{L|K}} & K^\times / N_{L|K} L^\times \\ \sigma * \downarrow & & \downarrow x \mapsto \sigma x \\ G(L^\sigma|K^\sigma) & \xrightarrow{r_{L^\sigma|K^\sigma}} & K^{\sigma^\times} / N_{L^\sigma|K^\sigma} L^{\sigma^\times} \end{array}$$

where $\sigma *$ is the conjugation map $\tau \mapsto \sigma^{-1} \tau \sigma$.

Corollary 2.1.2 (Norm residue symbol). *Let $L|K$ be an abelian extension of local fields. Then the inverse of the isomorphism $r_{L|K}$ gives a homomorphism*

$$(\cdot, L|K) : K^\times \rightarrow \text{Gal}(L|K)$$

whose kernel is precisely $N_{L|K}L^\times$.

The following theorem gives a 1-1 correspondence between finite abelian extensions of a local field K and the finite index subgroups of $K^\times$, which is the arithmetic/information required about the base field.

Theorem 2.1.3 (Existence theorem). *Let K be a local field, and let $\mathcal{N}_L := N_{L|K}L^\times$. Then there is a bijective correspondence*

$$\{\text{Finite abelian extensions } L \text{ of } K\} \leftrightarrow \{\text{Open subgroups of finite index in } K^\times\}$$

$$L \mapsto \mathcal{N}_L$$

Furthermore, $L_1 \subseteq L_2 \iff \mathcal{N}_{L_2} \subseteq \mathcal{N}_{L_1}$, $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \mathcal{N}_{L_2}$ and $\mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$.

Remark 2.1.1. Theorem [2.1.3](#) is referred to as existence theorem, because it guarantees the existence of an abelian extension of K which corresponds to an open subgroup of finite index $\mathcal{N}$ in $K^\times$. Such a field is called the ‘class field’ of $\mathcal{N}$.

2.2 Tate cohomology groups

In this section, we will define the 0^{th} , 1^{st} and -1^{th} Tate cohomology groups. There is an infinite family of Tate cohomology groups, and class field theory can be developed in the language of cohomology, (See for instance, [\[6\]](#).) but it is sufficient for our purposes to focus our attention on the above groups. We will also state Hilbert’s theorem 90 in the language of Tate cohomology groups, and a generalisation to arbitrary Galois extensions which is due to Emmy Noether.

Definition 2.2.1 (0^{th} Tate cohomology group). *It is denoted as $H^0(G, L^\times)$ and is defined to be $H^0(G, L^\times) := K^\times / N_{L|K}L^\times$.*

Remark 2.2.1. *Note that the reciprocity homomorphism $r_{L|K}$ is a map from $\text{Gal}(L|K) \rightarrow H^0(G, L^\times)$.*

Definition 2.2.2 (-1^{th} Tate cohomology group). *Let ${}_N L|K := \text{Kernel of } N_{L|K}$ and let $I_{G(L|K)}$ be the subgroup generated by $a^{\sigma-1} := \sigma a / a$, $\sigma \in G(L|K)$ and $a \in L^\times$. Then, the -1^{th}*

Tate cohomology group, denoted by $H^{-1}(G, L^\times)$ is defined to be

$$H^{-1}(G, L^\times) := {}_N L|K / I_{G(L|K)}$$

Note that if $L|K$ is a cyclic extension with a generator σ , then $I_{G(L|K)}$ is

$$L^{\sigma-1} := \{a^{\sigma-1} \mid a \in L^\times\}.$$

Remark 2.2.2. $I_{G(L|K)}$ is contained in the kernel of $N(L|K)$ because

$$N_{L|K}(a^{\sigma-1}) = \prod_{\tau \in G} \tau(\sigma(a)) / \prod_{\tau \in G} \tau(a) = 1.$$

Definition 2.2.3 (1 cocycle). A 1 cocycle or crossed homomorphism of $G = G(L|K)$ is a function $f : G \rightarrow L^\times$ satisfying

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

Remark 2.2.3. The set of all 1 cocycles forms an abelian group under multiplication, the identity of the group being the function $i : G \rightarrow L^\times$, $i(\sigma) = 1$ for all $\sigma \in G$, and the inverse of f being the function g such that $g(\sigma) := 1/f(\sigma)$ for all $\sigma \in G$. This group will be denoted $Z^1(G, L^\times)$.

Remark 2.2.4. If a 1 cocycle f is defined such that it takes values only in the base field $K^\times$, i.e., $f : G \rightarrow K^\times$, then f is in fact a group homomorphism from G to $K^\times$ since the action of G on K is trivial, i.e., $\tau(f(\sigma)) = f(\sigma)$ for all $\sigma \in G$.

Definition 2.2.4 (1 coboundaries). A 1 coboundary is defined to be a map $f_a : G \rightarrow L^\times$ satisfying $f_a(\sigma) = a^{\sigma-1}$ for all $\sigma \in G$, where $a \in L^\times$.

Remark 2.2.5. The set of all coboundaries forms a subgroup of $Z^1(G, L^\times)$ and is denoted $B^1(G, L^\times)$.

Definition 2.2.5 (1st Tate cohomology group). The first Tate cohomology group denoted $H^1(G, L^\times)$ is defined to be $H^1(G, L^\times) := Z^1(G, L^\times) / B^1(G, L^\times)$.

In the following two theorems, L, K may be any fields (not necessarily local fields). We now state and prove Hilbert theorem 90/ Satz 90.

Theorem 2.2.1 (Hilbert theorem 90). *For a finite cyclic extension $L|K$, $H^{-1}(G, L^\times) \cong H^1(G, L^\times) = 1$.*

Proof. Let σ be a generator of G , and $\#G = [L : K] := n$.

1. $H^{-1}(G, L^\times) = 1$: By linear independence of automorphisms $\{1, \sigma, \dots, \sigma^{n-1}\}$, $\exists \gamma \in L^\times$ such that

$$\beta = \gamma + \alpha\sigma(\gamma) + \dots (1 + \sigma + \dots \sigma^{n-2})\alpha \sigma^{n-1}(\gamma) \neq 0.$$

where α is an element of norm 1. By above, we get $\alpha\sigma(\beta) = \alpha$, so $\alpha = \beta/\sigma(\beta)$.

2. $H^1(G, L^\times) \cong H^{-1}(G, L^\times)$: $f \mapsto f(\sigma)$ is a well defined map since

$$N_{L|K}(f(\sigma)) = \prod_{\tau \in G} \tau(f(\sigma)) = \prod_{\tau \in G} f(\sigma\tau)/f(\tau) = 1, \text{ so } f(\sigma) \in N_{L|K}L^\times$$

and is clearly a homomorphism. For surjectivity, suppose $a \in N_{L|K}L^\times$. Set $f(\sigma) = a$, and

$$f(\sigma^k) = \prod_{i=0}^{k-1} \sigma^i(a). \text{ It is easy to show that } f \in Z^1(G, L^\times).$$

For injectivity, note that $f(\sigma^k) = \sigma(f(\sigma^{k-1}))f(\sigma) = \dots \prod_{i=0}^{k-1} \sigma^i(f(\sigma))$, so if $f(\sigma) = 1$, then $f = \text{Id}$.

To show the required isomorphism, we have to establish that the preimage of $L^{\times(\sigma-1)}$ is precisely $B^1(G, L^\times)$ under the map $f \mapsto f(\sigma)$. This can be seen easily because $f \in B^1(G, L^\times) \iff f(\sigma^k) = a^{\sigma^k-1}$ for some fixed $a \iff f(\sigma) = a^{\sigma-1} \iff f \in L^{\times(\sigma-1)}$. $\square$

We now prove Noether's generalisation of Hilbert theorem 90.

Theorem 2.2.2. *For a finite Galois extension $L|K$, $H^1(G, L^\times) = 1$.*

Proof. Let $f : G \rightarrow L^\times$ be a 1 cocycle. We need to show that f is in fact a coboundary.

For $c \in L^\times$, set $\alpha := \sum_{\sigma \in G} f(\sigma)\sigma(c)$. Since the automorphisms are linearly independent, we can choose $c \in L^\times$ such that $\alpha \neq 0$. For $\tau \in G$,

$$\tau(\alpha) = \sum_{\sigma \in G} \tau(f(\sigma))\sigma\tau(c) = \left(\sum_{\sigma\tau \in G} f(\sigma\tau)\sigma\tau(c) \right) / f(\tau) = \alpha / f(\tau), \text{ so } f(\tau) = \alpha / \tau(\alpha)$$

Now set $\alpha = 1/\beta$. Then, $f(\tau) = \tau(\beta)/\beta$. $\square$

Remark 2.2.6. The fact that $H^{-1}(G, L^\times) \cong H^1(G, L^\times)$ for cyclic G shows that the above theorem is indeed a generalisation of Hilbert theorem 90.

Remark 2.2.7. Even for infinite Galois extensions, we have Noether's generalisation of Hilbert theorem 90. i.e., $H^1(G(L|K), L^\times) = 1$. This is because $H^1(G(L|K), L^\times) = \varinjlim_M H^1(G(M|K), M^\times)$ where $M|K$ ranges over finite extensions.

2.3 Kummer theory

Definition 2.3.1 (Kummer extension). Let μ_n (group of n^{th} roots of unity) be contained in K , $(n, \text{ch}(K)) = 1$ and $K^{\times n} \subseteq \Delta \subseteq K^\times$. Then, $K(\sqrt[n]{\Delta})|K$ is called a Kummer extension.

Example 10. 1. Any quadratic extension of a p -adic field is Kummerian, since $\mu_2 \subseteq K$.
 2. The quadratic extension $F_2((\sqrt{t})|F_2((t))$ is not Kummerian, since $(2, \text{ch}(F_2((t)))) \neq 1$. (Note that this extension is not separable, hence not Galois, but we desire the property that Kummerian extensions be Galois, as the next proposition shows.)

Proposition 2.3.1. Let $K(\sqrt[n]{\Delta})|K$ be a Kummer extension. Then, it is an abelian extension of exponent n , i.e., $\text{Gal}(K(\sqrt[n]{\Delta})|K)$ is abelian of exponent n .

Proof. Let $a \in \Delta$. Then, $f(X) = X^n - a$ is separable because $f'(X) = nX^{n-1}$, which is coprime to $f(X)$ since $f(X)$ is not the zero polynomial (because $(n, \text{ch}(K)) = 1$), and the only root of $f'(X)$ is 0, which is not a root of $f(X)$. Also $\mu_n \subseteq K$, so $K(\sqrt[n]{\Delta})|K$ is normal, hence Galois. Furthermore, the roots of $X^n - a$ are $\zeta_n \alpha$, so

$$\sigma_1 \sigma_2(\alpha) = \zeta^{n_2} \sigma_1(\alpha) = \zeta^{n_2} \zeta^{n_1} \alpha = \zeta^{n_1} \zeta^{n_2} \alpha = \sigma_2 \sigma_1(\alpha)$$

Hence, the extension is abelian, and $\sigma^n(\alpha) = \zeta^{rn} \alpha = \alpha$ where $\sigma(\alpha) = \zeta_n \alpha$, so the Galois group is of exponent n . $\square$

Theorem 2.3.2. Let $(n, \text{ch}(K)) = 1$, $\mu_n \subseteq K$ and $L|K$ be an abelian extension of exponent n . Then $L = K(\sqrt[n]{\Delta})$ where $\Delta = L^{\times n} \cap K^\times$, that is $L|K$ is a Kummer extension.

In particular, if $L|K$ is cyclic, then $L = K(\alpha)$ with $\alpha^n = a \in K^\times$.

Proof. (1) $K(\sqrt[n]{\Delta}) \subseteq L^\times$: If $\Delta = L^{\times n} \cap K^\times$, and if $x \in \overline{K}$ is s.t. $x^n = a \in \Delta$, then $x = \zeta_n^r \sqrt[n]{a}$ for some $r \in \mathbb{N}$, but since $\mu_n \in K$, $x \in L$.

(2) $L \subseteq K(\sqrt[n]{\Delta})$: Since $L|K$ is an abelian extension, it is the composite of finite cyclic subextensions of K (It is the composite of finite abelian extensions of K , which are in turn the composite of finite cyclic extensions by fundamental theorem of finite abelian groups and fundamental theorem of Galois theory). So it suffices to prove that if $M|K$ is a cyclic subextension of $L|K$, then $M = K(\alpha)$ for some $\alpha \in \sqrt[n]{\Delta}$ and $M \subseteq K(\sqrt[n]{\Delta})$.

Now, let $G(M|K) = \langle \sigma \rangle$ and $d = [M : K]$, $d' = n/d$ and $\xi = \zeta_n^{d'}$. Since $\zeta_n \in K$, $M_{M|K}(\xi) = \xi^d = \zeta_n^n = 1$, which by Hilbert theorem 90, shows that $\xi = \alpha^{\sigma^{-1}}$ for some $\alpha \in M^\times$. So $K \subseteq K(\alpha) \subseteq M$. But $\sigma^i(\alpha) = \xi^i \alpha$. Thus, $\sigma^i(\alpha) = \alpha \iff d \mid i$, so the cardinality of the image $\sigma \mapsto \sigma|_{K(\alpha)}$ from $G(M|K) \rightarrow G(K(\alpha)|K)$ is d , so $K(\alpha) = M$. $\square$

Example 11. $\mathbb{Q}_2(\sqrt{2}+i)$ is an abelian extension of exponent 2, since $\mathbb{Q}_2(\sqrt{2}+i) = \mathbb{Q}_2(\sqrt{2}, i)$ and hence has Galois group as the Klein four group.

We now state and prove the main theorem of Kummer theory.

Theorem 2.3.3. Let $(n, \text{ch}(K)) = 1$ and $\mu_n \subseteq K$. Then, the map $\Delta \mapsto L = K(\sqrt[n]{\Delta})$ is a 1-1 correspondence between

$$\{\text{Subgroups of } K^\times \text{ containing } K^{\times n}\} \leftrightarrow \{\text{Abelian extensions of } K \text{ of exponent } n\}$$

If Δ and K correspond to each other, then $L^{\times n} \cap K^\times = \Delta$, and we have a canonical isomorphism

$$\Delta/K^{\times n} \cong \text{Hom}(\text{Gal}(L|K), \mu_n) \quad a \pmod{K^{\times n}} \mapsto \chi_a$$

where the homomorphism $\chi_a : G(L|K) \rightarrow \mu_n$, $\chi_a(\sigma) = \alpha^{\sigma^{-1}}$ where $\alpha^n = a$ for some $\alpha \in L$.

Proof. (1) The map $\Delta \mapsto K(\sqrt[n]{\Delta})$ is well defined and surjective: By Proposition 2.3.1, the map is well defined, that is the map takes Δ to an abelian extension of K of exponent n . By Theorem 2.3.2, this map is surjective.

(2) $\Delta/K^{\times n} \cong \text{Hom}(\text{Gal}(L|K), \mu_n)$: Consider the map $a \mapsto \chi_a$ from $K^\times$ to the dual of $G(L|K)$. χ_a is well defined since $(\sigma(\alpha)/\alpha)^n = a^{\sigma^{-1}} = 1$, so $\alpha^{\sigma^{-1}} \in \mu_n$, and because any two n^{th} roots of a differ by some element of μ_n , and since $\mu_n \subseteq K$, we have $(\zeta_n^r)^{\sigma^{-1}} = 1$, where $\zeta_n^r \in \mu_n$.

It is a homomorphism since $\chi_{ab}(\sigma) = (\alpha\beta)^{\sigma^{-1}} = (\alpha)^{\sigma^{-1}}(\beta)^{\sigma^{-1}} = \chi_a(\sigma)\chi_b(\sigma)$, where $\alpha^n = a$ and $\beta^n = b$.

$K^{\times n}$ is contained in the Kernel because $\alpha \in K^\times$. The kernel is contained in $K^{\times n}$ because if

$\chi_a = \text{Id}$, then $\alpha^{\sigma-1} = 1$ for all σ , hence $\alpha \in K^\times$, so $a \in K^{\times n}$.

To show surjectivity, let $\chi \in \text{Hom}(G(L|K), \mu_n)$. Since any subgroup of μ_n is cyclic, χ defines an isomorphism $\bar{\chi} : G(M|K) \rightarrow \text{Im}(\chi)$ where $M|K$ is a finite cyclic extension. Let $G(M|K) = \langle \sigma \rangle$. Since $N_{M|K}(\bar{\chi}(\sigma)) = (\bar{\chi}(\sigma))^{[M:K]} = 1$, by Hilbert theorem 90, $\bar{\chi}(\sigma) = \alpha^{\sigma-1}$ for some $\alpha \in M^\times$. Now, $(\alpha^n)^{\sigma-1} = (\alpha^{\sigma-1})^n = (\bar{\chi}(\sigma))^n = 1$, so $a = \alpha^n \in L^{\times n} \cap K^\times$. For $\tau \in G(L|K)$, $\chi(\tau) = \bar{\chi}(\tau \upharpoonright_M) = \alpha^{\tau-1} = \chi_a(\tau)$, so $\chi = \chi_a$.

(3) The map $\Delta \mapsto K(\sqrt[n]{\Delta})$ is injective: We need to show that if $K^{\times n} \subseteq \Delta \subseteq K^\times$ and $L = K(\sqrt[n]{\Delta})$, then $\Delta = L^{\times n} \cap K^\times$. Set $\Delta' = L^{\times n} \cap K^\times$. Then, by step (2), $\Delta'/K^{\times n} \cong \text{Hom}(G(L|K), \mu_n)$. The subgroup $\Delta/K^{\times n}$ ($\Delta \subseteq \Delta'$ since if $a \in \sqrt[n]{\Delta}$, then since $L = K(\sqrt[n]{\Delta})$, $a^n \in L^{\times n} \cap K^\times = \Delta'$) corresponds under Pontryagin duality (which can be applied since $G(L|K)$ with Krull topology is compact, so locally compact), to the subgroup $\text{Hom}(G(L|K), \mu_n)$, where $H = \{\sigma \in G(L|K) \mid \chi_a(\sigma) = 1 \forall a \in \Delta\}$.

As $\alpha^{\sigma-1} = \chi_a(\sigma)$ for α a n^{th} root of a , H fixes the elements of $\sqrt[n]{\Delta}$ and as $K(\sqrt[n]{\Delta}) = L$, we find $H = 1$, so $\text{Hom}(G(L|K)/H, \mu_n) = \text{Hom}(G(L|K), \mu_n)$, so $\Delta/K^{\times n} = \Delta'/K^{\times n}$, so $\Delta = \Delta'$. $\square$

Remark 2.3.1. Notice that the above theorem is a generalisation of the existence theorem for local fields (Theorem 2.1.3) containing a primitive n^{th} roots of unity. Hence, it was stated in the introduction that the above theorem is a step towards the existence theorem.

Let us conclude the chapter by showing that the maximal Kummer extension of a local field K is a finite extension of K , so every Kummer extension is a finite extension.

Corollary 2.3.4. Let $(n, \text{ch}(K)) = 1$ and $\mu_n \subseteq K$. Then $L = K(\sqrt[n]{K^\times})$ is a finite abelian extension of exponent n , $K^{\times n} = N_{L|K}L^\times$ and $K^\times/K^{\times n} \cong G(L|K)$.

Proof. By Theorem 2.3.3, we have $K^\times/K^{\times n} \cong \text{Hom}(G(L|K), \mu_n)$. On the other hand, since $K^\times/K^{\times n}$ is finite by Corollary 1.3.17, $L|K$ is a finite abelian extension of exponent n . By local reciprocity isomorphism (Theorem 2.1.1), $K^\times/N_{L|K}L^\times \cong G(L|K)$. By the previous theorem, $K^\times/K^{\times n} \cong \text{Hom}(G(L|K), \mu_n)$. Since, $G(L|K)$ is a finite group, it is non-canonically isomorphic to its dual $\text{Hom}(G(L|K), \mu_n)$. So $\#K^\times/K^{\times n} = \#G(L|K) = \#K^\times/N_{L|K}L^\times$. Furthermore, $K^{\times n} \subseteq N_{L|K}L^\times$, since $K^\times/N_{L|K}L^\times \cong G(L|K)$ and $G(L|K)$ is abelian of exponent n . So the canonical surjection $K^\times/K^{\times n} \rightarrow K^\times/N_{L|K}L^\times$ is an isomorphism, hence $K^{\times n} = N_{L|K}L^\times$. $\square$

Remark 2.3.2. The above corollary is not true if K is a number field. Notice for instance that the field $\mathbb{Q}(\{\sqrt{p} \mid p \text{ is prime}\})$ is an infinite extension of $\mathbb{Q}$.

Chapter 3

Abstract class field theory

We now prove the main theorems of class field theory, i.e., the existence of the reciprocity homomorphism and the existence theorem, abstractly for a G module A , under certain assumptions. This approach due to Neukirch, helps us tackle local and global class field theory within a unified framework. The proofs of the main statements of local and global class field theory can then be obtained with relative ease, replacing G by the Galois group of a local/ number field, A by the multiplicative group of a local field in the context of local class field theory, and by the idèle class group in the context of global class field theory, and showing that these G modules satisfy the required assumptions.

While this chapter deals with class field theory abstractly for G modules, it helps to have a concrete situation in mind. Thus, we will illustrate how some of the theory developed below is in consonance with our prior knowledge of local fields.

The primary reference for this chapter is Chapter 4 of [7].

3.1 G modules

In this section, we will first define a G module A . We will then set up some convention that will be used throughout the chapter.

Definition 3.1.1 (G module). *A G module is an abelian group A together with an action*

$$\cdot : G \times A \rightarrow A$$

such that $g \cdot (a_1 + a_2) = g \cdot a_1 + g \cdot a_2$.

Example 12. 1. If $L|K$ is a Galois extension of fields, then the Galois group acts on $K^\times$ as $\sigma \cdot a = \sigma(a)$ where $\sigma \in G(L|K)$ and $a \in K^\times$.

2. We will consider $\mathbb{Z}$ as trivial G module, i.e., the G action is trivial, i.e., $g \cdot a = a$ for all $g \in G$ and $a \in \mathbb{Z}$. This convention makes sense for our purpose since we may consider $\mathbb{Z}$ as a subgroup of $\mathbb{Q}$ which is fixed by the action of the Galois group for any Galois extension of $\mathbb{Q}$ or $\mathbb{Q}_p$.

Definition 3.1.2 (G module homomorphism). Let A and B be two G modules. Then a G module homomorphism $f : A \rightarrow B$ is a group homomorphism such that $f(g \cdot a) = g \cdot f(a)$. If f is furthermore a bijection, then it is a G module isomorphism.

Definition 3.1.3 (Continuous G module). Let A be a G module, and A and G be topological groups. If the action of G on A is continuous, then A is said to be a continuous G module.

Example 13. Let $A = L^\times$ with L a number field or local field, and G be the Galois group $\text{Gal}(L|K)$ with Krull topology. Then, A is a continuous G module.

For our purposes, we restrict our attention to a profinite group G . A is equipped with discrete topology. The following language will be used throughout the chapter:

1. The closed subgroups of G will be denoted G_K where the indices are termed ‘fields’.
2. The index k associated to G is called the ‘base field’ and the index associated to $\{1\}$ is denoted $\bar{k}$.
3. The field corresponding to the closure of the cyclic subgroup $\langle \sigma \rangle$, i.e., $\overline{\langle \sigma \rangle}$ is called the ‘fixed field’ of σ .
4. We write $K \subseteq L$ or $L|K$ if $G_L \subseteq G_K$, and we denote the pair (L, K) as $L|K$ and call it a ‘field extension’.
5. If G_L is open in G_K , equivalently of finite index in G_K by the fundamental theorem of Galois theory, then $L|K$ is termed a ‘finite extension’, and the index $[G_K : G_L]$ is denoted $[L : K]$ and is called the ‘degree of the field extension $L|K$ ’.
6. $L|K$ is said to be ‘normal’ or ‘Galois’ if G_L is a normal subgroup of G_K . In this case, we define the ‘Galois group’ of $L|K$ by $G(L|K) := G_K/G_L$.
7. The extension $L|K$ is ‘cyclic’, ‘abelian’, ‘solvable’ if $G(L|K)$ is.
8. We put $K := \bigcap_i K_i$ (‘intersection’) if G_K is topologically generated by the subgroups G_{K_i} , and $K = \prod_i K_i$ (‘composite’) if $G_K = \bigcap_i G_{K_i}$.

9. Lastly, A_K denotes the submodule of A fixed by G_K , i.e., $A_K = \{a \in A \mid \sigma a = a \text{ for all } \sigma \in G_K\}$.

It must be noted that in abstract class field theory, we will not consider any fields, but since the application of this theory is to address questions about local and number fields, we use the terms ‘fields’, ‘field extensions’ etc.

Remark 3.1.1. *The norm map and the Tate cohomology groups are defined as in previous chapter by replacing $K^\times$ by A_K . Furthermore, the norm map satisfies the tower property, i.e., for ‘fields’ $K \subseteq L \subseteq M$, we have $N_{M|K}N_{L|M}(A_L) = N_{L|K}(A_L)$. The proof of this fact for a G module A is exactly the same as for actual field extensions.*

Remark 3.1.2. *If G is a profinite group and A a G module, then A is a continuous G module if and only if $A = \bigcup_{[K:k] < \infty} A_K$ where A is endowed with discrete topology.*

The following proposition says that if we have an exact sequence of G modules, it induces an exact sequence of the corresponding submodules fixed by G and the 1st Tate Cohomology groups.

Proposition 3.1.1. *Let $1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$ be an exact sequence of G modules. Then, we have an exact sequence $1 \rightarrow A^G \rightarrow B^G \rightarrow C^G \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C)$.*

Remark 3.1.3. *The isomorphism $\Delta/K^{\times n} \cong \text{Hom}(G(L|K), \mu_n)$ in Theorem 2.3.3 can also be obtained by the above result. Consider the exact sequence $1 \rightarrow \mu_n \rightarrow L^\times \xrightarrow{\uparrow n} L^{\times n} \rightarrow 1$ and apply the above proposition and Hilbert theorem 90 to obtain $1 \rightarrow \mu_n \rightarrow K^\times \rightarrow L^{\times n} \cap K^\times = K^{\times n} \rightarrow H^1(G(L|K), \mu_n) = \text{Hom}(G(L|K), \mu_n) \rightarrow H^1(G(L|K), L^\times) = 1$.*

3.2 Kummer theory

In this section, we state the main theorems of Kummer theory. We obtain the statements by simply replacing $K^\times$ in the previous chapter by A_K . However, we state them here for future reference. The proofs are similar to the proofs in the case of local fields (See for instance [7]). However, we will require the important assumption

Let $L|K$ be a cyclic extension. (i.e. $G(L|K) = G_K/G_L$ is cyclic),
and suppose the kernel of $x \mapsto x^n$ is cyclic. Then $H^{-1}(G, A_L) = 1$.

Note that this assumption has been shown to hold for the G module $A = \bar{k}^{\times^{\text{sep}}}$ (k^{sep} is the separable closure of k) by Hilbert theorem 90, where k is a local field.

Theorem 3.2.1. *Let $L|K$ be an abelian extension of exponent n . Then, $L = K(\sqrt[n]{\Delta})$, such that $\Delta = A_L^n \cap A_K$, that is $L|K$ is a Kummer extension.*

In particular, if $L|K$ is cyclic, then $L = K(\sqrt[n]{\alpha})$ with $\alpha^n = a \in A_K$.

This was guaranteed in the context of local fields by the Hilbert theorem 90.

Theorem 3.2.2. *The map $\Delta \mapsto L = K(\sqrt[n]{\Delta})$ is a 1-1 correspondence between*

$$\{\text{Subgroups of } A_K \text{ containing } A_K^n\} \leftrightarrow \{\text{Abelian extensions of } K \text{ of exponent } n\}$$

If Δ and K correspond to each other, then $A_L^n \cap A_K = \Delta$, and we have a canonical isomorphism

$$\Delta/A_K^n \cong \text{Hom}(\text{Gal}(L|K), \mu_n) \quad a \pmod{A_K^n} \mapsto \chi_a$$

where the character $\chi_a : G(L|K) \rightarrow \mu_n$, $\chi_a(\sigma) = \alpha^{\sigma-1}$ where $\alpha^n = a$.

3.3 Abstract valuation theory

We will now define a continuous surjective homomorphism $d : G \rightarrow \hat{\mathbb{Z}}$ where G is a profinite group. This homomorphism helps us mimic the ramification theory of local fields. Suppose for now that k is a p -adic number field, $G_k = G(\bar{k}|k)$ and $\mathbb{F}_q$ is the residue field. Then such a surjective homomorphism arises via the maximal unramified extension. Recall $G(\tilde{k}|k) \cong G(\bar{\mathbb{F}}_q|\mathbb{F}_q) \cong \hat{\mathbb{Z}}$ which associates to $1 \in \hat{\mathbb{Z}}$ the Frobenius automorphism ϕ defined by $\phi(a) \equiv a^q \pmod{\bar{P}}$ for $a \in \bar{O}$ where $\bar{O}$ and $\bar{P}$ denote the valuation ring and the maximal ideal of $\tilde{k}$ respectively.

Switching back to the abstract situation, suppose there is a surjective homomorphism $d : G \rightarrow \hat{\mathbb{Z}}$. The kernel of d is denoted I and its fixed field is denoted $\tilde{k}$. d thus induces an isomorphism $d' : G(\tilde{k}|k) \rightarrow \hat{\mathbb{Z}}$.

For any field K , we denote by I_K the kernel of the restriction $d : G_K \rightarrow \hat{\mathbb{Z}}$ and call it the *inertia group* over K . Since $I_K = G_K \cap I = G_K \cap G_{\tilde{k}} := G_{K\tilde{k}}$, the fixed field $\tilde{k}$ of I_K is $K\tilde{k}$. We call $\tilde{K}|K$ the *maximal unramified extension* of K . Put $f_K := [\hat{\mathbb{Z}} : d(G_K)]$ and $e_K := [I : I_K]$. When f_K is finite, we obtain a homomorphism $d_K = \frac{1}{f_K}d : G_K \rightarrow \hat{\mathbb{Z}}$ which

is surjective since $d(G_K) = f_K \hat{\mathbb{Z}}$, and the homomorphism has kernel I_K , so we obtain an isomorphism $d : G(\tilde{K}|K) \rightarrow \hat{\mathbb{Z}}$.

Remark 3.3.1. *The condition that f_K be finite is satisfied for K a local field. This can be seen by observing that $d(G_K) \cong G(\overline{k_k}|k_K)$ has finite index in $G(\overline{k_k}|k_k)$.*

Definition 3.3.1 (Frobenius). *The element $\phi_K \in G(\tilde{K}|K)$ such that $d_K(\phi_K) = 1$ is called the Frobenius over K .*

For a field extension $L|K$, the inertia degree $f_{L|K}$ and the ramification index $e_{L|K}$ are given by $f_{L|K} = [d(G_K) : d(G_L)]$ and $e_{L|K} = [I_K : I_L]$. For a tower of fields $K \subseteq L \subseteq M$, the definition implies that $f_{M|K} = f_{L|K} f_{M|L}$ and $e_{M|K} = e_{M|L} e_{L|K}$.

Remark 3.3.2. *For an extension of local fields, we have defined the inertia degree $f_{L|K}$ of $L|K$. We show that this agrees with the above definition. $f_{L|K} = [k_L : k_K]$ as defined in Chapter 1. Now $[d(G_K) : d(G_L)] = \#(G(\overline{k_k}|k_K)/G(\overline{k_k}|k_{L \cap \tilde{K}})) = \#G(k_{L \cap \tilde{K}}|k_K) = [k_{L \cap \tilde{K}} : k_K] = [k_L : k_K]$. The last equality follows because $L \cap \tilde{K}$ is the maximal unramified extension of $L|K$.*

Proposition 3.3.1. *For every finite extension $L|K$, we have $[L : K] = f_{L|K} e_{L|K}$.*

Proof. We have the exact commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I_L & \longrightarrow & G_L & \xrightarrow{d} & d(G_L) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & I_K & \longrightarrow & G_K & \xrightarrow{d} & d(G_K) & \longrightarrow & 1 \end{array}$$

Now, if G_L is normal in G_K , then $d(G_L)$ is clearly normal in $d(G_K)$ and I_L . If $\tau \in I_L$ and $\sigma \in I_K$, then $d(\sigma\tau\sigma^{-1}) = d(\sigma) + d(\tau) - d(\sigma) = d(\tau) = 0$, so $\sigma\tau\sigma^{-1} \in I_L$, and the rest follows by commutativity and exactness of the above commutative diagram.

If $L|K$ is not Galois, then we pass to a Galois extension $M|K$ containing L (i.e., normal closure of G_K in G_L), and get the result from the transitivity rules for e and f , and the fact that $M|L$ is Galois. $\square$

Remark 3.3.3. *This identity together with the previous remark tells us that inertia degree $e_{L|K}$ for local fields L and K coincides with the already known definition.*

$L|K$ is called *unramified* if $e_{L|K} = 1$, i.e., if $L \subseteq \tilde{K}$. $L|K$ is called *totally ramified* if $e_{L|K} = 1$, i.e., if $L \subseteq \tilde{K}$. Observe that a finite unramified extension $L|K$ is cyclic, since it is a finite quotient of $G(\tilde{K}|K) \cong \hat{\mathbb{Z}}$ (hence is $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$).

$L|K$ is called *totally ramified* if $f_{L|K} = 1$, i.e., if $L \cap \tilde{K} = K$. In the unramified case, we have the surjective homomorphism $G(\tilde{K}|K) \rightarrow G(L|K)$, and if $f_K < \infty$, the image of the Frobenius automorphism ϕ_K is denoted $\phi_{L|K}$.

For an arbitrary extension $L|K$, we have $\tilde{L} = L\tilde{K}$ since $L\tilde{K} = LK\tilde{k} = L\tilde{k} = \tilde{L}$. We also have the obvious fact

Proposition 3.3.2. *If f_K and f_L are finite, then $f_{L|K} = f_L/f_K$ and we have the commutative diagram*

$$\begin{array}{ccc} G_L & \xrightarrow{d} & \hat{\mathbb{Z}} \\ \downarrow & & \downarrow x \mapsto f_{L|K}x \\ G_K & \xrightarrow{d} & \hat{\mathbb{Z}} \end{array}$$

In particular, we have $\phi_L \upharpoonright_{\tilde{K}} = \phi_K^{f_{L|K}}$.

Henceforth we assume $f_K < \infty$.

We pass from the Galois extension $L|K$ to the Galois extension $\tilde{L}|K$ and consider the semi-group $\text{Frob}(\tilde{L}|K) = \{\sigma \in G(\tilde{L}|K) \mid d_K(\sigma) \in \mathbb{N}\}$.

We have the following proposition about $\text{Frob}(\tilde{L}|K)$:

Proposition 3.3.3. *For a finite Galois extension $L|K$, the map*

$$\text{Frob}(\tilde{L}|K) \rightarrow \text{Gal}(L|K), \quad \sigma \mapsto \sigma \upharpoonright_L$$

is surjective.

Proof. Let $\sigma \in G(L|K)$ and $\phi \in G(\tilde{L}|K)$ be a lift of the Frobenius ϕ_K in $G(\tilde{K}|K)$, so that $d_K(\phi) = 1$. So, $\phi \upharpoonright_{\tilde{K}} = \phi_K$ and $\phi \upharpoonright_{L \cap \tilde{K}} = \phi_{L \cap \tilde{K}|K}$. Since $L \cap \tilde{K}|K$ is unramified and hence cyclic, $\sigma \upharpoonright_{L \cap \tilde{K}} = \phi_{L \cap \tilde{K}|K}^n$ for some $n \in \mathbb{N}$. As $\tilde{L} = L\tilde{K}$, $G(L\tilde{K}|\tilde{K}) \cong G(L|L \cap \tilde{K})$.

Now if $\tau \in G(\tilde{L}|\tilde{K})$ maps to $\sigma \phi^{-n} \upharpoonright_L$ under this isomorphism, then setting $\tilde{\sigma} = \tau \phi^n$, we have $\tilde{\sigma} \upharpoonright_L = \tau \phi^n \upharpoonright_L = \sigma \phi^{-n} \phi^n \upharpoonright_L = \sigma$ and $\tilde{\sigma} \upharpoonright_{\tilde{K}} = \phi_K^n$ since $\tau \upharpoonright_{\tilde{K}} = \text{Id}$. Hence $d_K(\tilde{\sigma}) \in \mathbb{N}$. $\square$

Proposition 3.3.4. *Let $\tilde{\sigma} \in \text{Frob}(\tilde{L}|K)$, and let Σ be the fixed field of $\tilde{\sigma}$ (i.e., the fixed field of $\langle \tilde{\sigma} \rangle$). Then: 1. $f_{\Sigma|K} = d_K(\tilde{\sigma})$ 2. $[\Sigma : K] < \infty$ 3. $\tilde{\Sigma} = \tilde{L}$ 4. $\tilde{\sigma} = \phi_{\Sigma}$*

- Proof.* (1) $\Sigma \cap \tilde{K}$ is the fixed field of $\tilde{\sigma} \upharpoonright_{\tilde{K}} = \phi_K^{d_K(\tilde{\sigma})}$, so $f_{\Sigma|K} = [\Sigma \cap \tilde{K} : K] = d_K(\tilde{\sigma})$.
- (2) We have $\tilde{K} \subseteq \Sigma\tilde{K} = \tilde{\Sigma} \subseteq \tilde{L}$, so $e_{\Sigma|K} = [I_K : I_{\Sigma}] = \#G(\tilde{\Sigma}|\tilde{K}) \leq \#G(\tilde{L}|\tilde{K})$ which is finite since $[L : K] < \infty$. So, $f_{\Sigma|K}e_{\Sigma|K} = [\Sigma : K] < \infty$.
- (3) We claim that the canonical surjection $\Gamma = G(\tilde{L}|\Sigma) \rightarrow G(\tilde{\Sigma}|\Sigma) \cong \hat{\mathbb{Z}}$ is bijective. To see this, note that since $\Gamma = \overline{\langle \tilde{\sigma} \rangle}$ is procyclic, we get $[\Gamma : \Gamma^n] \leq n \cong \hat{\mathbb{Z}}$ for some $n \in \mathbb{N}$. But Γ/Γ^n surjects onto $\hat{\mathbb{Z}}/n\hat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$, so $[\Gamma : \Gamma^n] \geq n$, so equality holds and thus $\Gamma/\Gamma^n \cong \hat{\mathbb{Z}}/n\hat{\mathbb{Z}}$ and by taking the inverse limit, $\Gamma \cong \hat{\mathbb{Z}}$.
- (4) $f_{\Sigma|K}d_{\Sigma}(\tilde{\sigma}) = d_K(\tilde{\sigma}) = f_{\Sigma|K}$, thus $d_{\Sigma}(\tilde{\sigma}) = 1$, so $\tilde{\sigma} = \phi_{\Sigma}$. $\square$

Definition 3.3.2 (Henselian valuation). *A Henselian valuation of A_k with respect to $d : G \rightarrow \hat{\mathbb{Z}}$ is a homomorphism $v : A_k \rightarrow \hat{\mathbb{Z}}$ satisfying the following:*

- (1) $v(A_k) = Z \supseteq \mathbb{Z}$ and $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$ for all $n \in \mathbb{N}$.
- (2) $v(N_{K|k}A_K) = f_K Z$ for all finite extensions $K|k$.

Example 14. *With k, K being local fields, the unique extension of the valuation of k to K satisfies (2) in the above definition, since $\frac{v(N_{K|k}A_K)}{n} = \frac{v(N_{K|k}A_K)}{e_K f_K} = \frac{v_K(A_K)}{e_K}$. (1) is satisfied since $v(A_k) = \mathbb{Z}$.*

Proposition 3.3.5. *For every finite extension $K|k$ of fields, $v_K = \frac{1}{f_K}v \circ N_{K|k} : A_K \rightarrow Z$ defines a surjective homomorphism satisfying the following properties:*

- (1) $v_K = v_{K^\sigma} \circ \sigma$, i.e., the following diagram commutes

$$\begin{array}{ccc} A_K & \xrightarrow{\sigma} & A_{K^\sigma} \\ \text{Id} \downarrow & & \downarrow v_{K^\sigma} \\ A_K & \xrightarrow{v_K} & \hat{\mathbb{Z}} \end{array}$$

- (2) *For every finite extension $L|K$, the following diagram commutes*

$$\begin{array}{ccc} A_L & \xrightarrow{v_L} & \hat{\mathbb{Z}} \\ N_{L|K} \downarrow & & \downarrow f_{L|K} \\ A_K & \xrightarrow{v_K} & \hat{\mathbb{Z}} \end{array}$$

Proof. (1) If τ runs through a system of representatives of G_k/G_K , then $\sigma^{-1}\tau\sigma$ runs through

a system of representatives of $G_k/\sigma^{-1}G_K\sigma = G_k/G_{K^\sigma}$. Hence, for $a \in A_K$, we have

$$v_{K^\sigma}(\sigma(a)) = \frac{1}{f_{K^\sigma}}v\left(\prod_{\tau}\sigma\sigma^{-1}\tau\sigma\right)(a) = \frac{1}{f_K}v\left(\sigma\left(\prod_{\tau}\tau(a)\right)\right) = \frac{1}{f_K}v(N_{K|k}(a)) = v_K(a).$$

The second equality follows because $f_{K^\sigma} = f_K$ and $\tau \mapsto \sigma^{-1}\tau\sigma$ is an automorphism.

(2) for $a \in A_L$, we have $f_{L|K}v_L(a) = f_{L|K}\frac{v_K(N_{L|K}(a))}{f_L} = \frac{1}{f_K}v(N_{K|k}(N_{L|K}(a))) = v_K(N_{L|K}(a)).$

□

Definition 3.3.3 (Prime element and unit). *A prime element of A_K is an element $\pi_K \in A_K$ such that $v_K(\pi_K) = 1$. We define U_K to be the set of all elements with valuation 0.*

Remark 3.3.4. *For an unramified extension $L|K$, $v_L \upharpoonright_{A_K} = v_K$, since $v_K(N_{L|K}(A_K)) = [L : K]v_K(A_K) = f_{L|K}v_L(A_L)$, the first equality following from the fact that every element $\sigma \in G_K/G_L$ fixes A_K , and the second equality from proposition 3.3.5. Thus a prime element of A_K is also a prime element in A_L .*

Remark 3.3.5. *If $L|K$ is totally ramified, i.e., $f_{L|K} = 1$, and π_L is a prime of A_L , then $\pi_K = N_{L|K}(\pi_L)$ is a prime of A_K .*

3.4 Construction of reciprocity map

We now consider a continuous G module A with the homomorphisms $d : G \rightarrow \hat{\mathbb{Z}}$ and $v : A_K \rightarrow \hat{\mathbb{Z}}$ where d and v are as defined in the previous section. In this abstract setting, we will construct the reciprocity map, demonstrate its functorial property and show that for a finite unramified extension, the Frobenius automorphism corresponds to a prime element of A_K under the reciprocity map.

Throughout this section, we make the following assumption:

Axiom: For every finite unramified extension $L|K$, $H^i(G, U_L) = 1$ ($i = 0, -1$).

For an infinite extension $L|K$, set $N_{L|K}(A_L) := \bigcap_{\{M|L \subseteq L, [M:K] < \infty\}} N_{M|K}.$

The commutative diagram below provides a road map for the construction of the reciprocity

homomorphism.

$$\begin{array}{ccc}
\text{Frob}(\tilde{L}|K) & \xrightarrow{r_{\tilde{L}|K}} & A_K/N_{\tilde{L}|K}A_{\tilde{L}} \\
\downarrow & & \downarrow \\
G(L|K) & \xrightarrow{\quad r_{L|K} \quad} & A_K/N_{L|K}A_L
\end{array}$$

We have proved in the preceding section that the left most map is surjective. Now, we will prove that there is a well defined homomorphism $r_{\tilde{L}|K}$ from $\text{Frob}(\tilde{L}|K)$ to $A_K/N_{\tilde{L}|K}A_{\tilde{L}}$. Composing with the canonical surjection to $A_K/N_{L|K}A_L$, we obtain a homomorphism from $\text{Frob}(\tilde{L}|K)$ to $A_K/N_{L|K}A_L$. Finally, we construct an assignment from $\text{Gal}(L|K)$ to $A_K/N_{L|K}A_L$ using surjectivity of the left most map, and show that this assignment is a well defined function, by proving that the assignment is independent of the lift.

Definition 3.4.1 (Reciprocity map $r_{\tilde{L}|K}$). *The map $r_{\tilde{L}|K} : \text{Frob}(\tilde{L}|K) \rightarrow A_K/N_{\tilde{L}|K}A_{\tilde{L}}$ is defined as*

$$r_{\tilde{L}|K}(\sigma) = N_{\Sigma|K}(\pi_\Sigma) \pmod{N_{\tilde{L}|K}A_{\tilde{L}}}$$

where Σ is the fixed field of $\overline{\langle \sigma \rangle}$ and $\pi_\Sigma \in A_\Sigma$ is a prime element.

Proposition 3.4.1. *The reciprocity map is well defined.*

Proof. By (2) of Proposition 3.3.4, $\Sigma|K$ is finite, so $N_{\Sigma|K}$ can act on π_Σ . Now if π_1 and π_2 are two prime elements of Σ , then $\pi_1 = u\pi_2$ for some $u \in U_\Sigma$. We must show that $N_{\Sigma|K}(u) \in N_{M|K}A_M$ for every finite Galois subextension $M|K$ of $\tilde{L}|K$. Now assume WLOG that $\Sigma \subseteq M$ (this assumption can be made because $N_{M|K} \subseteq N_{\Sigma|K} \ \forall \Sigma \subseteq M$, and hence $N_{\tilde{L}|K} = \bigcap_{M \supseteq \Sigma} N_{M|K}$). Since $M|\Sigma$ is finite and unramified ($M \subseteq \tilde{L}$), so $u = N_{M|\Sigma}(a)$ where $a \in U_\Sigma$, by applying the axiom $H^0(G, U_L) = 1$. So,

$$N_{\Sigma|K}(u) = N_{\Sigma|K}N_{M|\Sigma}(a) = N_{M|K}(a) \in N_{M|K}A_M$$

□

To show that $\text{Frob}(\tilde{L}|K)$ is multiplicative, we need a few lemmas. We will use the following notations:

$$(i) \ \sigma - 1 : A_{\tilde{L}} \mapsto A_{\tilde{L}} \quad a \mapsto \sigma(a)/a \quad (ii) \ \sigma_n : A_{\tilde{L}} \rightarrow A_{\tilde{L}} \quad a \mapsto \sigma_n(a) = \prod_{i=0}^{n-1} \sigma^i(a).$$

In this formal notation, this gives $\sigma_n = \frac{\sigma^n - 1}{\sigma - 1}$, and we find that $(\sigma - 1) \circ \sigma_n = \sigma_n \circ (\sigma - 1) = \sigma^n - 1$.

We now introduce the homomorphism $N = N_{\tilde{L}|\tilde{K}} : A_{\tilde{L}} \rightarrow A_{\tilde{K}}$ and prove two lemmas for it.

Lemma 3.4.2. *Let $\phi', \sigma \in \text{Frob}(\tilde{L}|K)$ with $d_K(\phi') = 1$ and $d_K(\sigma) = n$. If Σ is the fixed field of σ and $a \in A_\Sigma$, then $N_{\Sigma|K}(a) = (N \circ \phi_n)(a) = \phi_n \circ N(a)$.*

Proof. Since $d_K(\sigma) = f_K(\sigma)$ by Proposition 3.3.4, $[\Sigma \cap \tilde{K} : K] = f_K(\sigma) = d_K(\sigma) = n$, and its Galois group $G(\Sigma^0|K)$ is cyclic and generated by the Frobenius automorphism $\phi_{\Sigma^0|K} = \phi_K \upharpoonright_{\Sigma^0} = \phi \upharpoonright_{\tilde{K} \upharpoonright_{\Sigma^0}} = \phi' \upharpoonright_{\Sigma^0}$, the last equality being because $d_K(\phi') = 1$. Hence, $N_{\Sigma^0|K} = \prod_{i=0}^{n-1} \phi^i \upharpoonright_{\Sigma^0} = \phi_n \upharpoonright_{A_\Sigma}$. Again by Proposition 3.3.4, we have $\tilde{\Sigma} = \tilde{L}$, and we have $\Sigma^0 = \Sigma \cap \tilde{K}$, and so by the isomorphism $G(\tilde{\Sigma}|\tilde{K}) \cong G(\Sigma|\Sigma \cap \tilde{K}) = G(\Sigma|\Sigma^0)$, so we have $N_{\Sigma|\Sigma^0} = N \upharpoonright_{A_\Sigma}$. Therefore for $a \in A_\Sigma$, we get

$$N_{\Sigma|K}(a) = N_{\Sigma^0|K} N_{\Sigma|\Sigma^0}(a) = \phi_n(N(a)) = N(\phi_n(a))$$

The last equation follows from normality of $G(\tilde{L}|\tilde{K})$ in $G(\tilde{L}|K)$. $\square$

We now define $H_0(G(\tilde{L}|\tilde{K}), U_{\tilde{L}}) := U_{\tilde{L}} / I_{G(\tilde{L}|\tilde{K})} U_{\tilde{L}}$. Notice that the homomorphism $N = N_{\tilde{L}|\tilde{K}} : U_{\tilde{L}} \rightarrow U_{\tilde{K}}$ maps $I_{G(\tilde{L}|\tilde{K})} U_{\tilde{L}}$ which is generated by all elements of the form $u^{\tau-1}$, $u \in U_{\tilde{L}}$, $\tau \in G(\tilde{L}|\tilde{K})$ to 1, so we have an induced homomorphism $N : H_0(G(\tilde{L}|\tilde{K}), U_{\tilde{L}}) \rightarrow U_{\tilde{K}}$. The following lemma describes the behaviour of the norm map N in relation with this group.

Lemma 3.4.3. *If $x \in H_0(G(\tilde{L}|\tilde{K}), U_{\tilde{L}})$ is fixed by an element $\phi \in G(\tilde{L}|K)$ s.t. $d_K(\phi) = 1$, then $N(x) \in N_{\tilde{L}|K} U_{\tilde{L}}$.*

Proof. Let $x = u \pmod{I_{G(\tilde{L}|\tilde{K})} U_{\tilde{L}}}$ with $x^{\phi-1} = 1$, so

$$u^{\phi-1} = \prod_{i=1}^r u_i^{\tau_i-1}, u_i \in U_{\tilde{L}}, \tau_i \in G(\tilde{L}|\tilde{K}). \quad (3.1)$$

Let $M|K$ be a finite Galois subextension of $\tilde{L}|K$. To prove that $N(u) \in N_{M|K} U_M$, we may assume $u, u_i \in U_M$ and $L \subseteq M$ (u, u_i are in some finite Galois subextensions of $\tilde{L}$, take M to be their compositum). Let $n = [M : K]$, $\sigma = \phi^n$ and let $M \subseteq \Sigma$ be the fixed field of

σ . Also, let $\Sigma_n|\Sigma$ be the maximal unramified extension of degree n , i.e., the fixed field of $\sigma^n = \phi_\Sigma^n$. By $H^0(G(\Sigma_n|\Sigma), U_{\Sigma_n|\Sigma}) = 1$, we find $\tilde{u}, \tilde{u}_i \in U_{\Sigma_n}$ such that

$$u = N_{\Sigma_n|\Sigma}(\tilde{u}) = \sigma_n(\tilde{u}) \quad \text{and} \quad u_i = N_{\Sigma_n|\Sigma}(\tilde{u}_i) = \sigma_n(\tilde{u}_i) \quad (3.2)$$

By (3.1) above, the elements $\tilde{u}^{\phi^{-1}}$ and $\prod_i u_i^{\tau_i-1}$ only differ by some norm 1 element $\tilde{x} \in U_{\Sigma_n}$. So, by $H^{-1}(G(\Sigma_n|\Sigma), U_{\Sigma_n}) = 1$, they differ by an element $\tilde{y}^{\sigma^{-1}}$, with $\tilde{y} \in U_{\Sigma_n}$. Thus,

$$\tilde{u}^{\phi^{-1}} = \tilde{y}^{\phi^n-1} \prod_i \tilde{u}_i^{\tau_i-1} = (\tilde{y}^{\phi^n})^{\phi^{-1}} \prod_i \tilde{u}_i^{\tau_i-1}$$

Applying N , we have $N(\tilde{u})^{\phi^{-1}} = (N(\tilde{y}^{\phi^n}))^{\phi^{-1}}$, so $N(\tilde{u}) = N(\tilde{y}^{\phi^n})z$, for some $z \in U_{\tilde{K}}$ s.t. $z^{\phi^{-1}} = 1$, so $z^\phi = z$ and hence $z \in U_K$. Finally, setting $y := \tilde{y}^{\sigma^n}$ and noting that $\tilde{y}^{\sigma^n} = N_{\Sigma_n|\Sigma}(\tilde{y}) \in U_\Sigma$, and using (3.2), we get

$$N(u) = N(\tilde{u}^{\sigma^n}) = N(\tilde{y}^{\phi^n})^{\sigma^n} z^{\sigma^n} = N(y)^{\phi^n} z^n = N_{\Sigma|K}(y) M_{M|K}(z) \in N_{M|K} U_M$$

where the last equality follows from the previous lemma. $\square$

We now show that $r_{\tilde{L}|K}$ is multiplicative.

Theorem 3.4.4. *The reciprocity map $r_{\tilde{L}|K} : \text{Frob}(\tilde{L}|K) \rightarrow A_K/N_{L|K}A_L$ is multiplicative.*

Proof. Let $\sigma_1\sigma_2 = \sigma_3$, $\sigma_1, \sigma_2, \sigma_3 \in \text{Frob}(\tilde{L}|K)$, $n_i = d_K(\sigma_i)$, $i = 1, 2, 3$. We must show that $N_{\Sigma_1|K}(\pi_1)N_{\Sigma_2|K}(\pi_2) = N_{\Sigma_3|K}(\pi_3) \pmod{N_{\tilde{L}|K}A_{\tilde{L}}}$.

Choose a fixed $\phi \in G(\tilde{L}|K)$ such that $d_K(\phi) = 1$ and set $\tau_i = \sigma_i^{-1}\phi^{n_i} \in G(\tilde{L}|\tilde{K})$ ($\tau_i \upharpoonright_{\tilde{K}} = \text{Id}$, because $\sigma_i \upharpoonright_{\tilde{K}} = \phi_K^{n_i}$). Noting that $n_1 + n_2 = n_3$, we can infer $\tau_3 = \sigma_2^{-1}\sigma_1^{-1}\phi^{n_2+n_1} = \sigma_2^{-1}\phi^{n_2}(\phi^{-n_2}\sigma_1\phi^{n_2})^{-1}\phi^{n_1}$. Putting $\sigma_4 = \phi^{-n_2}\sigma_1\phi^{n_2}$, we get $n_4 = d_K(\sigma_4) = n_1$, $\Sigma_4 = \phi^{n_2}(\Sigma_1)$, $\pi_4 = \phi^{n_2}(\pi_1) \in A_{\Sigma_4}$ and $\tau_4 = \sigma_4^{-1}\phi^{n_4}$, we find $\tau_3 = \tau_2\tau_4$ and $N_{\Sigma|K}(\pi_4) = N_{\Sigma_1|K}(\pi_1)$.

We now show $N_{\Sigma_3|K}(\pi_3) \equiv N_{\Sigma_2|K}(\pi_2)N_{\Sigma_4|K}(\pi_4) \pmod{N_{\tilde{L}|K}A_{\tilde{L}}}$.

From Lemma 3.4.2, we have $N_{\Sigma_i|K}(\pi_i) = N(\pi_i^{\phi^{n_i}})$. Now if we put $u = \pi_3^{\phi^{n_3}}\pi_4^{-\phi^{n_4}}\pi_2^{-\phi^{n_2}}$, the required congruence boils down to $N(u) \in N_{\tilde{L}|K}A_{\tilde{L}}$. Since $\phi_{n_i} \circ (\phi - 1) = \phi^{n_i} - 1$, and $\pi_i^{\phi^{n_i}-1} = \pi_i^{\sigma_i^{-1}\phi^{n_i}-1} = \pi_i^{\tau_i-1}$ (the second last equality follows because π_i is in the fixed field of σ .) Now, we have $u^{\phi^{-1}} = \pi_3^{\tau_3-1}\pi_4^{1-\tau_4}\pi_2^{1-\tau_2}$. From the identity $\tau_3 = \tau_2\tau_4$, it follows that $(\tau_3 - 1) + (1 - \tau_2) + (1 - \tau_4) = (1 - \tau_2)(1 - \tau_4)$. Now setting $\pi_3 = u_3\pi_4$, $\pi_2 = u_2^{-1}\pi_4$ and

$\pi_4^{\tau_2} = u_4 \pi_4$, $u_i \in U_{\tilde{L}}$, we obtain $u^{\phi-1} = \prod_{i=2}^4 u_i^{\tau_i-1}$.

For $x = u \bmod I_{G(\tilde{L}|\tilde{K})} U_{\tilde{L}} \in H_0(G(\tilde{L}|\tilde{K}), U_{\tilde{L}})$, this means $x^{\phi-1} = 1$, so $x^\phi = x$. Then by the previous lemma, we get $N(u) = N(x) \in N_{\tilde{L}|K} A_{\tilde{L}}$. $\square$

We finally use the surjectivity of the map $\text{Frob}(\tilde{L}|K) \rightarrow G(L|K)$ to construct an assignment from $G(L|K) \rightarrow A_K/N_{L|K} A_L$, and show that the assignment is independent of the choice of preimage, thereby giving us the reciprocity map.

Theorem 3.4.5. *For every finite Galois extension $L|K$, there is a canonical homomorphism $r_{L|K} : G(L|K) \rightarrow A_K/N_{L|K} A_L$ where Σ is the fixed field of a preimage $\tilde{\sigma} \in \text{Frob}(\tilde{L}|K)$ of $\sigma \in G(L|K)$ and $\pi_\Sigma \in A_\Sigma$ is a prime element.*

Proof. Let $\tilde{\sigma}, \tilde{\sigma}' \in \text{Frob}(\tilde{L}|K)$ be two preimages of σ , Σ, Σ' the respective fixed fields and $\pi_\Sigma, \pi_{\Sigma'}$ be prime elements in A_Σ and $A_{\Sigma'}$ respectively. If $d_K(\tilde{\sigma}) = d_K(\tilde{\sigma}')$, then $\tilde{\sigma} \upharpoonright_{\tilde{K}} = \tilde{\sigma}' \upharpoonright_{\tilde{K}}$ and $\tilde{\sigma} \upharpoonright_L = \tilde{\sigma}' \upharpoonright_L = \sigma$, so $\tilde{\sigma} = \tilde{\sigma}'$. However, if we have (WLOG) $d_K(\sigma) < d_K(\sigma')$, then $\tilde{\sigma}' = \tilde{\sigma} \tilde{\tau}$ for $\tilde{\tau} \in \text{Frob}(\tilde{L}|K)$, and $\tilde{\tau} \upharpoonright_L = 1$. The fixed field Σ'' of $\tilde{\tau}$ contains L , so $r_{\tilde{L}|K}(\tilde{\tau}) \equiv N_{\Sigma''|K}(\pi_{\Sigma''}) = N_{L|K} N_{\Sigma''|L}(\pi_{\Sigma''}) \equiv 1 \bmod N_{L|K} A_L$. So, $r_{\tilde{L}|K}(\tilde{\sigma}') = r_{\tilde{L}|K}(\tilde{\sigma}) r_{\tilde{L}|K}(\tilde{\tau})$ by Theorem 3.4.4, and combining this with $r_{\tilde{L}|K}(\tilde{\tau}) \equiv 1 \bmod N_{L|K} A_L$, $r_{\tilde{L}|K}(\sigma) = r_{\tilde{L}|K}(\tilde{\sigma}')$. To see that the map is a homomorphism, consider σ_1 and σ_2 in $G(L|K)$ and suppose that $\tilde{\sigma}_1$ and $\tilde{\sigma}_2$ are preimages of σ_1 and σ_2 . Then apply Theorem 3.4.4. $\square$

Remark 3.4.1. *It is interesting to note that although the reciprocity isomorphism is a statement about finite Galois extensions $L|K$, we required the use of infinite extensions (in particular $\tilde{L}, \tilde{K}$) to construct the reciprocity map.*

We now prove that for unramified extensions $L|K$, the Frobenius automorphism corresponds to a prime element of A_K under the reciprocity isomorphism.

Theorem 3.4.6. *For every finite unramified extension $L|K$, we have*

$$r_{L|K} : G(L|K) \rightarrow A_K/N_{L|K} A_L \quad r_{L|K}(\phi_{L|K}) = \pi_K \bmod N_{L|K} A_L$$

and this map is an isomorphism.

Proof. Since $L|K$ is unramified, $L \subseteq \tilde{K}$, so $\tilde{L} = \tilde{K}$ and $\phi_K \in G(\tilde{K}|K)$ is a preimage of $\phi_{L|K}$ with fixed field K , i.e., $r_{L|K}(\phi_{L|K}) = \pi_K \bmod N_{L|K} A_L$. Let $n = [L : K]$ and consider the

composite

$$G(L|K) \xrightarrow{r_{L|K}} A_K/N_{L|K}A_L \xrightarrow{\tilde{v}} Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$$

where the map $\tilde{v}$ is induced by $v_K : A_K \rightarrow Z$ because $v_K(N_{L|K}A_L) \subseteq f_K Z = nZ$. It is injective because if $v_K(a) \equiv 0 \pmod{nZ}$, then $a = u\pi_K^{dn}$, and since $u = N_{L|K}(\epsilon)$ for some $\epsilon \in U_L$ by the axiom $H^0(G(L|K), U_L) = 1$ assumed for this section, we find $a = N_{L|K}(\epsilon\pi_K^d) \equiv 1 \pmod{N_{L|K}A_L}$. It is an isomorphism because we know $\#A_K/N_{L|K}A_L \geq n$ since $\#G(L|K) = n$ and the image of $r_{L|K}$ is contained in $A_K/N_{L|K}A_L$. Since we already know that $G(L|K) \cong \mathbb{Z}/n\mathbb{Z}$ since $G(L|K)$ is cyclic of order n , $r_{L|K}$ is an isomorphism. $\square$

We will now show that $r_{L|K}$ exhibits functoriality.

Theorem 3.4.7. *Let $L|K$ and $L'|K'$ be finite Galois extensions and $L \subseteq L'$, $K \subseteq K'$ and let $\sigma \in G$, then we have the commutative diagram*

$$\begin{array}{ccc} G(L'|K') & \xrightarrow{r_{L'|K'}} & A_{K'}/N_{L'|K'}A_{L'} \\ \sigma \mapsto \sigma|_L \downarrow & & \downarrow N_{K'|K} \\ G(L|K) & \xrightarrow{r_{L|K}} & A_K/N_{L|K}A_L \end{array} \quad \begin{array}{ccc} G(L|K) & \xrightarrow{r_{L|K}} & A_K/N_{L|K}A_L \\ \sigma* \downarrow & & \downarrow \sigma \\ G(L^\sigma|K^\sigma) & \xrightarrow{r_{L^\sigma|K^\sigma}} & A_K^\sigma/N_{L^\sigma|K^\sigma}A_L^\sigma \end{array}$$

where $\sigma*$ is the conjugation map $\tau \mapsto \sigma^{-1}\tau\sigma$.

Proof. 1. Left diagram: Let $\sigma' \in G(L'|K')$ and $\sigma = \sigma'|_L \in G(L|K)$. If $\tilde{\sigma}' \in \text{Frob}(\tilde{L}'|K')$ is a preimage of σ' , then $\tilde{\sigma} = \tilde{\sigma}'|_{\tilde{L}} \in \text{Frob}(\tilde{L}|K)$ is a preimage of σ such that $d_K(\tilde{\sigma}) = f_{K'|K}d_{K'}(\tilde{\sigma}') \in \mathbb{N}$ (The last equality is by Proposition 4.3). Let Σ' be the fixed field of σ' . Then $\Sigma = \Sigma' \cap \tilde{L} = \Sigma' \cap \tilde{\Sigma}$ (last equality by proposition 3.3.4) is the fixed field of $\tilde{\sigma}$ and $f_{\Sigma'|\Sigma} = 1$. Now if $\pi_{\Sigma'} \in A_{\Sigma'}$ is a prime of Σ' , then $\pi_\Sigma = N_{\Sigma'|\Sigma}(\pi_{\Sigma'}) \in A_\Sigma$ is a prime of Σ . Now, the commutativity is obtained by observing

$$N_{\Sigma|K}(\pi_\Sigma) = N_{\Sigma|K}(N_{\Sigma'|\Sigma}(\pi_{\Sigma'})) = N_{\Sigma'|K}(\pi_{\Sigma'}) = N_{K'|K}(N_{\sigma'|K'}(\pi_{\sigma'})).$$

2. Right diagram: Let $\tau \in G(L|K)$ and let $\tilde{\tau}$ be a preimage in $\text{Frob}(\tilde{L}|K)$ with fixed field Σ , and $\hat{\tau}$ a lift of $\tilde{\tau}$ to $\bar{k}$. Then Σ^σ is the fixed field of $\sigma^{-1}\hat{\tau}\sigma|_{\tilde{L}^\sigma}$, and if $\pi \in A_\Sigma$ is a prime element of Σ , then $\sigma(\pi) \in A_{\Sigma^\sigma}$ is a prime element of Σ^σ . The commutativity of the diagram now follows by $N_{\Sigma^\sigma|K^\sigma}(\sigma(\pi)) = \sigma(N_{\Sigma|K}(\pi))$. $\square$

3.5 Abstract reciprocity isomorphism

Class field axiom: For every finite cyclic extension $L|K$,

$$\#H^i(G(L|K), A_L) = \begin{cases} [L : K] & i = 0 \\ 1 & i = -1 \end{cases}$$

We now prove that given the class field axiom, we can obtain the axiom of the previous section.

Proposition 3.5.1. *For every finite unramified extension $L|K$, $H^i(G(L|K), U_L) = 1$. ($i = 0, 1, -1$).*

Proof. 1. $H^{-1}(G(L|K), U_L) = 1$: Let $u \in U_L$ be in the kernel of $N_{L|K}$. Since any unramified extension is cyclic, apply the class field axiom (in particular $H^{-1}(G(L|K), A_L) = 1$ to obtain $u = a^{\sigma^{-1}}$, $a \in A_L$. Since $L|K$ is unramified, a prime π_K of A_K is also a prime element of A_L , so $a = \epsilon \pi_K^m$, $\epsilon \in U_K$, so $u = \epsilon^{\sigma^{-1}}$.

2. $H^0(G(L|K), U_L) = 1$: Let $n = [L : K]$. Now $v_K : A_K \rightarrow \hat{\mathbb{Z}}$ maps $N_{L|K}A_L$ to $n\hat{\mathbb{Z}}$ by definition. So, we have an induced homomorphism $\tilde{v} : A_K/N_{L|K}A_L \rightarrow \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$, but this is an isomorphism because by class field axiom, $\#A_K/N_{L|K}A_L = n$. Now, $v_K(u) = 0$, so $u \bmod N_{L|K}A_L$ is in kernel of $\tilde{v}$, hence $u \in N_{L|K}A_L$. Now, if $u = N_{L|K}(a)$, then a must be a unit ($v_K(u) = v_K(N_{L|K}(a)) = nv_L(a) = 0$), so $a \in U_L$. $\square$

Definition 3.5.1 (Class field theory). *Class field theory is a pair of homomorphisms ($d : G \rightarrow \hat{\mathbb{Z}}, v : A \rightarrow \hat{\mathbb{Z}}$) (d and v as in previous section) where A is a G module satisfying the class field axiom.*

We now prove that a G module A admitting a class field theory has a canonical homomorphism - the reciprocity homomorphism, which induces an isomorphism.

Theorem 3.5.2. *Abstract reciprocity isomorphism: For every finite Galois extension $L|K$, the induced homomorphism*

$$r_{L|K} : G(L|K)^{ab} \rightarrow A_K/N_{L|K}A_L$$

is an isomorphism.

Proof. If $M|K$ is a Galois subextension of $L|K$, we get from functoriality of the reciprocity map the commutative exact diagram

$$\begin{array}{ccccccc}
1 & \longrightarrow & G(L|M) & \longrightarrow & G(L|K) & \longrightarrow & G(M|K) \longrightarrow 1 \\
& & \downarrow r_{L|M} & & \downarrow r_{L|K} & & \downarrow r_{M|K} \\
& & A_L/N_{L|M}A_M & \xrightarrow{N_{M|K}} & A_K/N_{L|K}A_L & \longrightarrow & A_K/N_{M|K}A_M \longrightarrow 1
\end{array}$$

First reduction: We show that it is enough to assume $L|K$ is abelian: Put $M = L^{\text{ab}}$ the maximal abelian subextension of $L|K$, we find $G(L|K)^{\text{ab}} = G(M|K)$ and the commutator $G(M|K)$ of $G(L|K)$ is in fact the kernel of $r_{L|K}$, i.e, $G(L|K)^{\text{ab}} \rightarrow A_K/N_{L|K}A_L$ is injective. We show surjectivity by induction on degree. In the case when $L|K$ is solvable, we have $M = L$ or $[L : M] < [L : K]$, and if $r_{L|M}$ and $r_{M|K}$ are surjective, (by strong induction and the fact that subgroup and quotient of a solvable group is solvable) then so is $r_{L|K}$ from the diagram. In general, let M be the fixed field of a p -Sylow subgroup. $M|K$ need not be Galois, but $r_{L|K}$ is still surjective (by induction and the fact that $L|M$ is always Galois). It then suffices to show that the image of $N_{M|K}$ is the p -Sylow subgroup H_p of $A_K/N_{L|K}A_L$. Clearly this holds true for all p if and only if $r_{L|K}$ is surjective. The inclusion $A_K \subseteq A_M$ induces a homomorphism $i : A_K/N_{L|K}A_L \rightarrow A_M/N_{L|M}A_L$ such that $N_{M|K} \circ i = [M : K]$ where $[M : K]$ is just $a \mapsto a^{[M:K]}$. Since $([M : K], p) = 1$, $H_p \xrightarrow{[M:K]} H_p$ is an isomorphism, hence surjective, so H_p lies in image of $N_{M|K}$, hence is $r_{L|K}$.

Second reduction: We claim that it is enough to show the theorem for $L|K$ cyclic. Suppose $L|K$ is abelian. Then the diagram shows that the kernel of $r_{L|K}$ is contained in kernel of $G(L|K) \rightarrow \prod_M G(M|K)$ where $M|K$ vary over the cyclic subextensions. Since $G(L|K)$ is abelian, this map is injective (fundamental theorem of finite abelian groups), so the same is true of $r_{L|K}$. Surjectivity follows by induction on degree.

Third reduction: It is enough to show the theorem when $L|K$ is cyclic and $f_{L|K} = 1$. Let $M = L \cap \tilde{K}$. Then $f_{L|M} = 1$ and $r_{M|K}$ is an isomorphism by Theorem 3.4.6. The below sequence in the theorem is left exact, since the groups in the sequence have orders $[L : M]$, $[L : K]$ and $[M : K]$. Hence $r_{L|K}$ is an isomorphism if $r_{L|M}$ is.

Proof of third reduction: Assume $L|K$ is cyclic and totally ramified. Let $G(L|K) = \langle \sigma \rangle$. σ may be identified as an element of $G(\tilde{L}|\tilde{K})$ by the isomorphism $G(\tilde{L}|\tilde{K}) \cong G(L|K)$, and obtain $\tilde{\sigma} = \sigma\phi_L \in \text{Frob}(\tilde{L}|\tilde{K})$, which is a preimage of σ under the surjection $\text{Frob}(\tilde{L}|\tilde{K}) \rightarrow G(L|K)$ such that $d_K(\tilde{\sigma}) = d_K(\phi_L) = f_{L|K} = 1$. So we find that $f_{\Sigma|K} = 1$ where Σ is the

fixed field of $\tilde{\sigma}$, so $\Sigma \cap \tilde{K} = K$. Let $M|K$ be a finite Galois subextension of $\tilde{L}|K$ containing σ and L , let $M^0 = M \cap \tilde{K}$ and $N = N_{M|M^0}$. As $f_{\Sigma|K} = f_{L|K} = 1$, we find that $N \upharpoonright_{A_\Sigma} = N_{\Sigma|K}$ and $N \upharpoonright_{A_L} = N_{L|K}$.

For the injectivity of $r_{L|K}$, we must show that if $r_{L|K}(\sigma^k) = 1$ where $0 \leq k < n = [L : K]$, then $k = 0$. Let $\pi_\Sigma \in A_\Sigma$, $\pi_L \in A_L$ be prime elements. Since $\Sigma, L \subseteq M$, π_Σ and π_L are both prime in L . Putting $\pi_\Sigma^k = u\pi_L^k$, $u \in U_M$, we obtain

$$r_{L|K}(\sigma^k) \equiv N(\pi_\Sigma^k) \equiv N(u)N(\pi_L^k) \equiv N(u) \pmod{N_{L|K}A_L}$$

From $r_{L|K}(\sigma^k) = 1$, it follows that $N(u) = N(v)$ for some $v \in U_L$, so $N(u^{-1}v) = 1$. By the class field axiom, we may write $u^{-1}v = a^{\sigma^{-1}}$, and find

$$(\pi_L^k v)^{\sigma^{-1}} = (\pi_L^k v)^{\tilde{\sigma}^{-1}} = (\pi_\Sigma^k u^{-1}v)^{\tilde{\sigma}^{-1}} = (a^{\sigma^{-1}})^{\tilde{\sigma}^{-1}} = (a^{\tilde{\sigma}^{-1}})^{\sigma^{-1}}$$

so $x = \pi_L^k v a^{1-\tilde{\sigma}} \in A_{M^0}$. Now $v_{M^0}(x) \in \hat{\mathbb{Z}}$ and $nv_{M^0}(x) = v_M(x) = k$, which implies $k \equiv 0 \pmod{n}$, hence $k = 0$.

The surjectivity then follows by the class field axiom. $\square$

Remark 3.5.1. *The below sequence can now be shown to be left exact for abelian groups. Suppose now that $G(L|M) = A_3$ and $G(L|K) = S_3$. Then $G(M|K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, so upto isomorphism, we get the sequence $A_3 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ which cannot be left exact by Lagrange.*

For number fields, the extension $G(\mathbb{Q}(\sqrt[3]{2}, \omega)|\mathbb{Q}) = S_3$ and $G(\mathbb{Q}(\sqrt[3]{2}, \omega)|\mathbb{Q}(\omega)) = A_3$. For local fields, $G(\mathbb{Q}_3(\sqrt[3]{3}, \omega)|\mathbb{Q}_3) = S_3$ and $G(\mathbb{Q}_3(\sqrt[3]{3}, \omega)|\mathbb{Q}_3(\omega)) = A_3$.

3.6 Abstract existence theorem

Definition 3.6.1 (Norm topology). *The norm topology on A_K is the topology generated by declaring the basic open sets about $a \in A_K$ to be the cosets $aN_{L|K}A_L$, where $L|K$ varies over all finite Galois extensions of K .*

Remark 3.6.1. *This forms a basis because $aN_{L|K} \cap aN_{M|K} \supseteq aN_{LM|K}$ LM is in fact a finite Galois extension of K .*

Remark 3.6.2. *A_K forms a topological group with this topology. Let f and g be the multiplication and inverse maps respectively. First note that it is enough to show that preimage*

of any basic neighbourhood about 1 is open. Then, observe that $f^{-1}(N_{L|K}A_L)$ contains the open subgroup $N_{L|K}A_L \times N_{L|K}A_L$, hence is open, and $g^{-1}(N_{L|K}A_L) = N_{L|K}A_L$, where $L|K$ is a finite extension.

Theorem 3.6.1 (Abstract existence theorem). *The map $L \mapsto N_{L|K}A_L$ sets up a 1-1 correspondence between*

$$\{\text{Finite abelian extensions of } K\} \leftrightarrow \{\text{Open subgroups of } A_K \text{ (in norm topology)}\}$$

Furthermore, $L_1 \subseteq L_2 \iff \mathcal{N}_{L_2} \subseteq \mathcal{N}_{L_1}$, $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$ and $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$, where $\mathcal{N}_L := N_{L|K}$.

Proof. 1. $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$: Since $L_1, L_2 \subseteq L_1L_2$, $\mathcal{N}_{L_1}, \mathcal{N}_{L_2} \supseteq \mathcal{N}_{L_1L_2}$ by transitivity of norm, so $\mathcal{N}_{L_1L_2} \subseteq \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$. Now if $a \in \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$, then $(a, L_1|K) = (a, L_2|K) = 1$, so $(a, L_1L_2|K) = 1$ (since an automorphism of $L_1L_2|K$ is determined by its action on L_1 and L_2), so $a \in \mathcal{N}_{L_1L_2}$.

2. $L_1 \subseteq L_2 \iff \mathcal{N}_{L_2} \subseteq \mathcal{N}_{L_1}$: $L_1 \subseteq L_2 \iff L_1L_2 = L_2 \iff \mathcal{N}_{L_1L_2} = \mathcal{N}_{L_2}$ but by (1), $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$, so $L_1 \subseteq L_2 \iff \mathcal{N}_{L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2} \iff \mathcal{N}_{L_2} \subseteq \mathcal{N}_{L_1}$. This also shows injectivity of $L \mapsto \mathcal{N}_L$.

3. Surjectivity of $\mathcal{N}_L$: If $\mathcal{N}$ is any open subgroup, then $1 \in \mathcal{N}$, hence $\mathcal{N}$ contains a basic open set about 1, which is of the form $N_{L|K}A_L$ for some finite Galois extension $L|K$. By the abstract reciprocity isomorphism, $\mathcal{N}_L = \mathcal{N}_{L^{\text{ab}}}$, so we may assume $L|K$ to be abelian. But $(\mathcal{N}, L|K) = G(L|L')$ for some intermediate field L' of $L|K$. Since $\mathcal{N}_L \subseteq \mathcal{N}$, $\mathcal{N}$ is the full preimage of $G(L|L')$ under the map $(\cdot, L|K) : A_K \rightarrow G(L|K)$, so it is the full kernel of $(\cdot, L'|K) : A_K \rightarrow G(L'|K)$. So $\mathcal{N} = \mathcal{N}_{L'}$.

4. $\mathcal{N}_{L_1}\mathcal{N}_{L_2} = \mathcal{N}_{L_1 \cap L_2}$: By transitivity of norms, $\mathcal{N}_{L_1 \cap L_2} \supseteq \mathcal{N}_{L_1}$ and $\mathcal{N}_{L_2}$, hence their product. Now since $\mathcal{N}_{L_1}\mathcal{N}_{L_2}$ is open ($\mathcal{N}_{L_1}\mathcal{N}_{L_2} = \bigcup_{a \in \mathcal{N}_{L_1}} a\mathcal{N}_{L_2}$), we have shown in (3) that $\mathcal{N}_{L_1}\mathcal{N}_{L_2} = \mathcal{N}_L$ for some finite abelian extension $L|K$. So $\mathcal{N}_{L_1}, \mathcal{N}_{L_2} \subseteq \mathcal{N}_L$ and hence by (2), this implies $L \subseteq L_1 \cap L_2$, so that $\mathcal{N}_{L_1}\mathcal{N}_{L_2} = \mathcal{N}_L \supseteq \mathcal{N}_{L_1 \cap L_2}$. $\square$

3.7 Herbrand quotients

We now develop an important tool called the Herbrand quotients. This will be essential to prove the class field axiom in the context of local and global class field theory, so that we

may apply the theory developed above in these concrete situations.

Throughout this section, we assume G is a cyclic group.

Theorem 3.7.1. *Let G be a cyclic group and $1 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 1$ be an exact sequence of G modules. Then we have an exact hexagon*

$$\begin{array}{ccccc}
 & H^{-1}(G, A) & \xrightarrow{f_1} & H^{-1}(G, B) & \\
 & \nearrow f_6 & & \searrow f_2 & \\
 H^0(G, C) & & & & H^{-1}(G, C) \\
 & \nwarrow f_5 & & \nearrow f_3 & \\
 & H^0(G, B) & \xleftarrow{f_4} & H^0(G, A) &
 \end{array}$$

Proof. See [7] for details. □

Remark 3.7.1. *Note that the cyclicity of G is only required for exactness at $H^{-1}(G, A)$. So, if G is any arbitrary finite group, we have the exact sequence $H^{-1}(G, A) \rightarrow H^{-1}(G, B) \rightarrow H^{-1}(G, C) \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C)$.*

Definition 3.7.1 (Herbrand quotient). *The Herbrand quotient $h(G, A)$ of a G module A is defined as*

$$h(G, A) := \#H^0(G, A) / \#H^{-1}(G, A)$$

whenever the above quantity exists.

Theorem 3.7.2. *If G is a cyclic group and $1 \xrightarrow{f} A \xrightarrow{g} B \xrightarrow{h} C \rightarrow 1$ is an exact sequence of G modules. Then*

$$h(G, B) = h(G, A)h(G, C)$$

that is, whenever any two of the quotients exist, the third exists and the above identity holds. For a finite G module A , $h(G, A) = 1$.

Proof. 1. $h(G, B) = h(G, A)h(G, C)$: By the exact hexagon in Theorem [3.7.1], calling n_i the order of the image f_i , we have

$$\begin{aligned}
 \#H^{-1}(G, A) &= n_6 n_1 & \#H^{-1}(G, B) &= n_1 n_2 & \#H^{-1}(G, C) &= n_2 n_3 \\
 \#H^0(G, A) &= n_3 n_4 & \#H^0(G, B) &= n_4 n_5 & \#H^0(G, C) &= n_5 n_6
 \end{aligned}$$

so $\#H^{-1}(G, A)\#H^{-1}(G, C)\#H^0(G, B) = \#H^0(G, A)\#H^0(G, C)\#H^{-1}(G, B)$, and if any two of the quotients are well defined, the third is and the identity in the theorem holds.

2. If A is finite, $h(G, A) = 1$. Consider the exact sequences

$$\begin{aligned} 1 \rightarrow A^G \rightarrow A \xrightarrow{\sigma-1} A^{\sigma-1} \rightarrow 1 \\ 1 \rightarrow {}_{N_G}A \rightarrow A \xrightarrow{N} N_G A \rightarrow 1 \end{aligned}$$

which gives $\#A = \#A^G\#A^{\sigma-1} = \#N_G A\# {}_{N_G}A$, so we obtain the required result. $\square$

Remark 3.7.2. Consider the action of $G = G(\mathbb{F}_{q_1}|\mathbb{F}_{q_2})$ on a finite field $\mathbb{F}_{q_1}^\times$. Since any finite field extension is cyclic, by Theorem 3.7.2, $h(G, \mathbb{F}_{q_1}^\times) = 1$, and by Hilbert theorem 90, $H^{-1}(G, \mathbb{F}_{q_1}^\times) = 1$, so $H^0(G, \mathbb{F}_{q_1}^\times) = 1$, which gives a proof of the fact that norm map is surjective for finite fields.

Definition 3.7.2 (Induced G modules). Let H be a subgroup of G , A a G module and B a H module. Then the induced G module denoted $A = \text{Ind}_G^H(B)$, is the set $\{f : G \rightarrow B \mid f(\sigma\tau) = \tau(f(\sigma)) \text{ for all } \tau \text{ in } H\}$. The G module operation is given by $(\sigma \cdot f)(\tau) = f(\sigma\tau)$. This is a G module operation because $(1 \cdot f)(\tau) = f(1 \cdot \tau) = f(\tau)$ and $(\sigma\gamma \cdot f)(\tau) = f(\sigma\gamma\tau) = \sigma \cdot f(\gamma\tau) = \sigma \cdot \gamma \cdot f(\tau)$ for all $\tau \in G$.

If $H = \{1\}$, then $\text{Ind}_G^H(B)$ is simply denoted $\text{Ind}_G(B)$.

We have a canonical H homomorphism $\pi : \text{Ind}_G^H(B) \rightarrow B$, $f \mapsto f(1)$, which maps the H submodule $B' = \{f \in \text{Ind}_G^H(B) \mid f(\sigma) = 1 \text{ for } \sigma \notin G\}$. Identifying B' with B , if $[G : H] < \infty$, then $\text{Ind}_G^H(B) = \prod_{\sigma \in G/H} \sigma(B)$ where σ varies over a set of left coset representatives of G/H .

Conversely if A is a G module with a H submodule B such that A is the direct product $A = \prod_{\sigma \in G/H} \sigma(B)$. Then $A \cong \text{Ind}_G^H(B)$ via $B \cong B'$.

Example 15. If $L|K$ is a finite Galois extension of fields, then L is an induced G module. This follows from the normal basis theorem, since $L = \bigoplus_{\sigma \in G} K\sigma a$, hence L is a $G(L|K)$ induced module.

The following proposition describes the cohomology groups of induced G modules.

Proposition 3.7.3. Let G be a finite cyclic group, H a subgroup of G and B a H module. Then we have $H^i(G, \text{Ind}_G^H(B)) \cong H^i(H, B)$ for all $i = 0, -1$. In particular, $H^i(G, \text{Ind}_G(B))$ is trivial.

Proof. See [7](#) for details. □

The following corollary is an analogue of Hilbert theorem 90 for the additive group of a field.

Corollary 3.7.4. *Let $L|K$ be a finite cyclic extension of fields. Then, $H^i(G(L|K), L) = 1$ for $i = 0, -1$. Thus, the trace map $Tr_{L|K}$ is always surjective.*

Proof. Follows from the explanation in Example [15](#). □

Chapter 4

Local class field theory: Proofs

In this chapter, we apply abstract class field theory to local fields to obtain the local reciprocity map and the local existence theorem. We will also see an important instance of ‘local global principle’: we will first prove the local Kronecker Weber theorem and use this to prove the global Kronecker Weber theorem.

Throughout this chapter, L and K will denote local fields unless mentioned otherwise.

The primary reference for this chapter is Chapter 5 of [7].

4.1 Local class field axiom

In this section, we prove the local class field axiom, thereby proving the existence of the local reciprocity map. Furthermore, we will prove the local existence theorem by showing that the open subgroups of finite index in $K^\times$ in the valuation topology are precisely the open subgroups of $K^\times$ in the norm topology.

Theorem 4.1.1 (Local class field axiom). *Let $L|K$ be a cyclic extension of local fields. Then*

$$\#H^i(G(L|K), L^\times) = \begin{cases} [L : K] & i = 0 \\ 1 & i = -1 \end{cases}$$

Proof. 1. $H^{-1}(G(L|K), L^\times) = 1$: This is by Hilbert theorem 90.

2. We prove now that it is enough to show $h(G, U_L) = 1$:

To prove the theorem, note that it suffices to show $h(G(L|K), L^\times) = [L : K]$. Consider the exact sequence

$$1 \rightarrow U_L \rightarrow L^\times \xrightarrow{v_L} \mathbb{Z} \rightarrow 1$$

Since G is cyclic, $h(G, L^\times) = h(G, U_L)h(G, \mathbb{Z})$ by Theorem 3.7.2. Since, the action of G on $\mathbb{Z}$ is trivial, $H^{-1}(G, \mathbb{Z}) = 1$ and $\#H^0(G, \mathbb{Z}) = [L : K]$.

3. $h(G, U_L) = 1$: Choose a normal basis $\{\sigma(\alpha) \mid \sigma \in G\}$, where α is a fixed element in O_L . Set $M = \sum_{\sigma \in G} O_K \sigma(\alpha)$ and $V^n = 1 + \pi_K^n M$. Now, O_K is compact, and the map $f : O_K \rightarrow O_L$ given by $f(\beta) = \beta \sigma(\alpha)$ is continuous, and the image is M , hence M is compact in the Hausdorff space O_L , so closed. M is open because it is the preimage of $\prod_{i=1}^n A_i$ ($A_i := O_K$

for all i) under the projection map from $L^\times \rightarrow \prod_{i=1}^n K_i^\times$ where $K_i^\times = K^\times$ for all i . Now, V^n forms a basis of neighbourhoods of 1 in U_L . Since M is open, we have N large enough such that $\pi_K^n O_L \subseteq M$ for all $n \geq N$. Now:

(a) V^n is an even subgroup (i.e., $V^n V^n \subseteq V^n$ for all $n \geq N$):

(i) V^n is closed under multiplication:

$(\pi_K^n M)(\pi_K^n M) = \pi_K^{2n} MM \subseteq \pi_K^{2n} O_L \subseteq \pi_K^{2n-N} M \subseteq \pi_K^n M$. Hence $V^n V^n \subseteq V^n$.

(ii) Inverse: For $1 - \pi_K^n \mu$, $\mu \in M$, we have $(1 - \pi_K^n \mu)^{-1} = 1 + \pi_K^n (\sum_{i=1}^{\infty} \mu_i \pi_K^{n(i-1)})$

We now have

$$V^n/V^{n+1} \cong M/\pi_K M = \bigoplus_{\sigma \in G} (O_K/\pi O_K) \alpha^\sigma = \text{Ind}_G(O_K/\pi O_K)$$

Thus $H^i(G, V^n/V^{n+1}) = 1$ for all $n \geq N$. Now, by the exact sequence of G modules

$$1 \rightarrow V^n \rightarrow U_L \rightarrow U_L/V^n \rightarrow 1$$

and since U_L/V^n is finite, we obtain $h(G, U_L/V^n) = 1$ by Theorem 3.7.2. Thus we only have to show $h(G, V^n) = 1$ for large enough n .

(b) To show that $H^i(G, V^n) = 1$ ($i = 0, -1$): We show that $H^0(G, V^n) = 1$. The proof for $H^{-1}(G, V^n) = 1$ follows similarly.

From $H^0(G, V^n/V^{n+1}) = 1$ if $a \in (V^n)^G$, we get $a = N_G(b_0)a_1$ with $a_1 \in (V^{n+1})^G$. Now, using $H^0(G, V^{n+1}/V^{n+2}) = 1$, we get $a_1 = N_G(b_1)a_2$, $a_2 \in (V^{n+2})^G$. In general, $a_i = N_G(b_i)a_{i+1}$ where $b_i \in V^{n+i}$, $a_{i+1} \in (V^{n+i})^G$. $\square$

This gives $a = N_G(b)$ with $b = \prod_{i=0}^{\infty} b_i$, where the product converges (since $v_K(b_i - 1) = n + i$), so that $H^0(G, V^n) = 1$. We have illustrated through various remarks in the previous chapter that the pair of homomorphisms d and v as described in the previous chapter exist for local fields, and now we have shown that $K^\times$ satisfies class field axiom. Thus, we have obtained a class field theory, and consequently we have

Corollary 4.1.2. *For every finite Galois extension $L|K$ of local fields, we have a canonical isomorphism $r_{L|K} : G(L|K)^{ab} \rightarrow K^\times / N_{L|K} L^\times$.*

Remark 4.1.1. *In global class field theory, we will have to account for the infinite places as well. We have a reciprocity law at the complex places as follows:*

$$\begin{aligned} (\cdot, \mathbb{C}|\mathbb{R}) : \mathbb{R}^\times &\rightarrow G(\mathbb{C}|\mathbb{R}) \\ (a, \mathbb{C}|\mathbb{R})\sqrt{-1} &= \sqrt{-1}^{\text{sgn}(a)} \end{aligned}$$

where $\text{sgn}(a) = 1$ for $a > 0$ and $\text{sgn}(a) = -1$ for $a < 0$, i.e., $(a, \mathbb{C}|\mathbb{R})$ is the identity map only if $a > 0$.

Theorem 4.1.3. *For every finite unramified extension $L|K$, $H^i(G(L|K), U_L^{(n)}) = 1$ ($i = 0, 1, -1$) for all $n \geq 0$. ($U_L^{(0)} = U_L$) In particular, $N_{L|K} U_L = U_K$ and $N_{L|K}(U_L^{(n)}) = U_K^{(n)}$.*

Proof. Since we have proved the local class field axiom, by Theorem 3.5.1, we have $H^i(G(L|K), U_L) = 1$, ($i = 0, 1, -1$). To prove $H^i(G(L|K), U_L^{(n)}) = 1$, we consider the exact sequences

$$1 \rightarrow U_L^{(1)} \rightarrow U_L \rightarrow k_L \rightarrow 1 \quad 1 \rightarrow U_L^{(n)} \rightarrow U_L^{(n-1)} \rightarrow k_L \rightarrow 1 \quad \text{for } n \geq 2$$

We know from Theorem 3.7.2 that $h(G, k_L) = h(G, k_L^\times) = 1$. (Note here that $G(L|K) \cong G(k_L|k_K)$ and G acts via this isomorphism on k_L .) So we obtain $h(G, U_L) = h(G, U_L^{(n)})$ for all $n \geq 1$, but $h(G, U_L) = 1$ from the first statement in the proof. Now $H^{-1}(G, k_L) = 1$ by Corollary 3.7.4, since any finite field extension is cyclic. Hence, applying the exact hexagon in Theorem 3.7.1, $1 = H^{-1}(G, U_L) = H^{-1}(G, U_L^{(n)})$, and combining this with $h(G, U_L^{(n)}) = 1$, we get $H^0(G, U_L^{(n)}) = 1$ for all $n \geq 0$. $\square$

Remark 4.1.2. *The above statement is not true for ramified extensions. Consider $L = \mathbb{Q}_2(\sqrt{-2})$ and $K = \mathbb{Q}_2$. This is a cyclic extension, hence from the proof of Theorem 4.1.1,*

we have $h(G(L|K), U_L) = 1$. Thus to show that $H^i(G, U_L)$ is non-trivial, it is enough to show that $H^0(G(L|K), U_L)$ is non-trivial. It can be shown that -1 is not a norm in $\mathbb{Q}_2(\sqrt{-2})$. By the fact that $H^i(G, U_L) = H^i(G, U_L^{(n)})$ for $n \geq 1$, we have $H^i(G, U_L^{(n)})$ is non-trivial.

We will now prove an important lemma that characterises unramified radical extensions $K(\sqrt[n]{\alpha})$ of local fields where $(n, \text{ch}(k_K)) = 1$. The case when $n = \text{ch}(k_K)$ is dealt with in the last chapter.

Theorem 4.1.4. *The extension $K(\sqrt[n]{\alpha})|K$ is unramified if and only if $\alpha \in U_K K^{\times n}$.*

Proof. If $K(\sqrt[n]{\alpha})|K$ is unramified, then $\sqrt[n]{\alpha} = u\pi_K^r$ where $u \in U_K$ and hence $v_{K(\sqrt[n]{\alpha})}(\sqrt[n]{\alpha}) = \frac{v_K(N_{K(\sqrt[n]{\alpha})|K}(\sqrt[n]{\alpha}))}{n} = \frac{v_K(\pi_K^r)}{n} = \frac{r}{n}$, so $r = kn$, where $k \in \mathbb{Z}$.

If $\alpha \in U_K K^{\times n}$, i.e., $\alpha = ux^n$ where $u \in U_K$ and $x \in K^\times$, then $K(\sqrt[n]{\alpha}) = K(\sqrt[n]{u})$. Let k' be the splitting field of $X^n - u \pmod{\mathcal{P}}$ over the residue class field k_K , and let $K'|K$ be the unramified extension with residue class field k' . By Hensel's lemma, $X^n - u$ splits into linear factors in K' , so $K(\sqrt[n]{u}) \subseteq K'$ is unramified. $\square$

Example 16. *By this, we can clearly see $\mathbb{Q}_p(\sqrt{u})|\mathbb{Q}_p$ is unramified degree 2 extension for all odd primes p given $(u/p) = -1$, where $(\)$ is the Legendre symbol.*

Finally let us prove the local existence theorem.

Proof of local existence theorem (Theorem 2.1.3). By the abstract existence theorem, we only have to show that the subgroups $\mathcal{N}$ that are open in the norm topology are precisely the open subgroups of finite index in the valuation topology.

(1) $\mathcal{N}$ is open in norm topology: If a subgroup $\mathcal{N}$ is open in norm topology, it contains by definition $N_{L|K}L^\times$. The reciprocity isomorphism provides the information that $N_{L|K}L^\times$ is of finite index in $K^\times$, so $\mathcal{N}$ has finite index in $K^\times$. It is open because it contains $N_{L|K}U_L$ (which is open, because it is compact, being the continuous image of U_L , hence closed, and has finite index in U_K).

(2) Converse: We will only consider the case $\text{char}(K) \nmid n$. Let $\mathcal{N}$ be a subgroup of finite index $n = [K^\times : \mathcal{N}]$. Then $K^{\times n} \subseteq \mathcal{N}$, and it is enough to show that $K^{\times n}$ contains $N_{L|K}$ for some finite abelian extension L of K .

We may assume that $K^\times$ contains μ_n : If not, then set $K_1 = K(\mu_n)$. If $K_1^{\times n}$ contains

$N_{L_1|K_1}L_1^\times$, and $L|K$ is a Galois extension containing L_1 , then

$$N_{L|K}L^\times = N_{K_1|K}N_{L|K_1}L^\times \subseteq N_{K_1|K}(N_{L_1|K_1}(L_1^\times)) \subseteq N_{K_1|K}(K_1^{\times n}) \subseteq K^{\times n}.$$

Suppose now $\mu_n \subseteq K$. Then by Corollary 2.3.4, we have $K^{\times n} = N_{L|K}L^\times$. $\square$

4.2 Kronecker Weber theorem

We will first introduce the notion of a conductor of an extension, which detects the ramification of the extension.

Definition 4.2.1 (Conductor). *Let $L|K$ be a finite abelian extension, and n the smallest non-negative integer such that $U_K^{(n)} \subseteq N_{L|K}L^\times$. Then the ideal $f = \mathcal{P}_K^n$ is called the conductor of $L|K$.*

Remark 4.2.1. *Every open subgroup of $K^\times$ contains $U_K^{(n)}$ for some large enough n , since $U_K^{(n)}$ forms a basis of neighbourhoods of 1. Hence, conductor of an extension is well defined.*

Theorem 4.2.1. *A finite abelian extension $L|K$ is unramified if and only if its conductor $f = 1$, (i.e., $n = 0$).*

Proof. If $L|K$ is unramified, then by Theorem 4.1.3 $U_K = N_{L|K}U_L$, so $n = 0$. Conversely, if $f = 1$, then $U_K \subseteq N_{L|K}U_L$ and $\pi_K^n \in N_{L|K}L^\times$ for $n = [K^\times : N_{L|K}L^\times]$. If $M|K$ is the unique unramified extension of degree n over K , then $N_{M|K}M^\times = \langle \pi_K^n \rangle \times U_K \subseteq N_{L|K}L^\times$, so $L \subseteq M$ by local existence theorem, so $L|K$ is unramified. $\square$

Every open subgroup $\mathcal{N}$ of finite index in $K^\times$ contains a group of the form $\langle \pi^f \rangle \times U_K^{(n)}$. Since $U_K^{(n)}$ is open, this group is open, and since $K^\times \cong \langle \pi \rangle \times U_K$ and $U_K^{(n)}$ has finite index in U_K , $\langle \pi^f \rangle \times U_K^{(n)}$ is open of finite index. Therefore the class fields of $\langle \pi^f \rangle \times U_K^{(n)}$ are important. Now setting $K = \mathbb{Q}_p$, we determine the class field of $\langle p \rangle \times U_K^{(n)}$.

Theorem 4.2.2. *The group of norms of the extension $\mathbb{Q}_p(\mu_{p^n})|\mathbb{Q}_p$ is $\langle p \rangle \times U_{\mathbb{Q}_p}^{(n)}$.*

Proof. Let $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\mu_{p^n})$. The extension $L|K$ is totally wildly ramified of degree $p^{n-1}(p-1)$. Now, we note that the exponential map $\exp : P_K^\nu \rightarrow U_K^{(\nu)}$ is an isomorphism

for $\nu \geq 1$ if $p \neq 2$ (since $\nu > e_{K|\mathbb{Q}_p}/(p-1) = 1/(p-1) < 1$), and for $\nu \geq 2$ when $p = 2$ (since $e_{K|\mathbb{Q}_2}/(2-1) = 1$). This map transforms the isomorphism $P_K^\nu \rightarrow P_K^{\nu+s-1}$ by $a \mapsto p^{s-1}(p-1)a$ into the isomorphism $U_K^{(\nu)} \rightarrow U_K^{(\nu+s-1)}$ by $x \rightarrow x^{p^{s-1}(p-1)}$. This is illustrated in the commutative diagram below.

$$\begin{array}{ccc}
P_K^\nu & \xrightarrow[\cong]{\exp} & U_K^{(\nu)} \\
\downarrow a \mapsto p^{s-1}(p-1)a \cong & & \downarrow \\
P_K^{\nu+s-1} & \xrightarrow[\exp]{\cong} & U_K^{\nu+s-1}
\end{array}$$

So $(U_K^{(1)})^{p^{n-1}(p-1)} = U_K^{(n)}$ if $p \neq 2$, and $(U_K^{(2)})^{2^{n-2}} = U_K^{(n)}$ if $p = 2$ and $n > 1$ (the case $p = 2$ and $n = 1$ is trivial). Therefore we obtain $U_K^{(n)} = N_{L|K}(U_K^{(1)}) \subseteq N_{L|K}L^\times$ if $p \neq 2$. For $p = 2$, we note that $U_K^{(2)} = U_K^{(3)} \cup 5U_K^{(3)} = (U_K^{(2)})^2 \cup 5(U_K^{(2)})^2$, because if $u \equiv 1 \pmod{4}$, (i.e., $u \in U_K^{(2)}$), then $u \equiv 1$ or $5 \pmod{8}$. Since $\mathbb{Q}_2(i) \subseteq \mathbb{Q}_2(\zeta_{2^n})$, $5^{2^{n-2}} = N_{L|K}(2+i)$, so $U_K^{(n)} \subseteq N_{L|K}L^\times$. Since $p = N_{L|K}(1-\zeta)$, we get $\langle p \rangle \times U_K^{(n)} \subseteq N_{L|K}L^\times$, and since both groups have index $p^{n-1}(p-1)$ ($N_{L|K}L^\times$ has index $p^{n-1}(p-1)$ since $G(\mathbb{Q}_p(\mu_{p^n})|\mathbb{Q}_p) \cong K^\times/N_{L|K}L^\times$), we have equality of the groups. $\square$

As an immediate consequence, we obtain the local analogue of the famous Kronecker Weber theorem.

Theorem 4.2.3 (Local Kronecker Weber theorem). *Every finite abelian extension $L|\mathbb{Q}_p$ is contained in a field $\mathbb{Q}_p(\zeta)$, where ζ is a primitive n^{th} root of unity for some $n \in \mathbb{N}$.*

Thus, the maximal abelian extension $\mathbb{Q}_p^{\text{ab}}|\mathbb{Q}_p$ is generated by adjoining all the roots of unity.

Proof. For some large enough f and n , $\langle p^f \rangle \times U_{\mathbb{Q}_p}^{(n)} \subseteq N_{L|K}L^\times$. Therefore L is contained in the class field M of the group $\langle p^f \rangle \times U_{\mathbb{Q}_p}^{(n)} = (\langle p \rangle \times U_{\mathbb{Q}_p}^{(n)}) \cap (\langle p^f \rangle \times U_{\mathbb{Q}_p})$. By the existence theorem, M is the composite of the class field for $\langle p^f \rangle \times U_{\mathbb{Q}_p}$, this being the unramified extension of degree f , and the class field for $\langle p \rangle \times U_{\mathbb{Q}_p}^{(n)}$, which by the previous theorem is $\mathbb{Q}_p(\zeta_{p^n})|\mathbb{Q}_p$. M is therefore generated by the $(p^f - 1)p^n$ th roots of unity. $\square$

Example 17 (Local Kronecker Weber for quadratic extensions). *The quadratic extension $\mathbb{Q}_p(\sqrt{p})|\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\zeta_p)$ for odd primes $p \equiv 1 \pmod{4}$, and $\mathbb{Q}_p(\sqrt{-p})|\mathbb{Q}_p$ is con-*

tained in $\mathbb{Q}_p(\zeta_p)$ for $p \equiv 3 \pmod{4}$. This can be seen as follows:

$$p = \prod_{i=1}^{p-1} (1 - \zeta_p^i) = \prod_{i=1}^{(p-1)/2} (1 - \zeta_p^i) \prod_{i=1}^{(p-1)/2} (1 - \zeta_p^{p-i}) = (-1)^{(p-1)/2} \frac{\prod_{i=1}^{(p-1)/2} (1 - \zeta_p^i)^2}{\zeta_p^{\frac{p^2-1}{4}}}$$

Note first that $\zeta_p^{\frac{p^2-1}{4}}$ is a square in $\mathbb{Z}_p[\zeta_p]$ since $2r \equiv \frac{p^2-1}{4} \pmod{p}$ has a solution. Hence $\sqrt{p} \in \mathbb{Q}_p(\zeta_p)$ if $p \equiv 1 \pmod{4}$ and $\sqrt{-p} \in \mathbb{Q}_p(\zeta_p)$ if $p \equiv 3 \pmod{4}$. The first equality above can be obtained by noting that the minimal polynomial for $1 - \zeta_p$ is obtained by replacing x by $x + 1$ in $1 + x + \cdots + x^{p-1}$, and thus the norm of $1 - \zeta_p$ is p by observing the constant term of the minimal polynomial of $1 - \zeta_p$, which is the required product. If $p \equiv 3 \pmod{4}$, then $\mathbb{Q}_p(\sqrt{p}) \subseteq \mathbb{Q}_p(\zeta_{4p}) = \mathbb{Q}_p(\zeta_p, i)$. Furthermore $(-1/p) = -1$, so the unique degree 2 unramified extension of $\mathbb{Q}_p$ is $\mathbb{Q}_p(i)|\mathbb{Q}_p$ which is itself cyclotomic.

The extension $\mathbb{Q}_2(\sqrt{2})|\mathbb{Q}_2$ and $\mathbb{Q}_2(\sqrt{-2})|\mathbb{Q}_2$ are contained in the biquadratic extension $\mathbb{Q}_2(\sqrt{2}, i) = \mathbb{Q}_2(\zeta_8)$. $\mathbb{Q}_2(i)|\mathbb{Q}_2$ is itself cyclotomic, since $i = \zeta_4$.

Remark 4.2.2. We cannot replace $\mathbb{Q}_p$ in the local Kronecker Weber theorem by an arbitrary local field. Let p be an odd prime and consider the extension $\mathbb{Q}_p(\sqrt[p]{p})|\mathbb{Q}_p(\sqrt{p})$. Suppose that $\mathbb{Q}_p(\sqrt[p]{p}) \subseteq \mathbb{Q}_p(\sqrt{p})(\zeta_n)$. Then since $\mathbb{Q}_p(\sqrt{p}) \subseteq \mathbb{Q}_p(\zeta_p)$ by the above example, we have $\mathbb{Q}_p(\sqrt[p]{p}) \subseteq \mathbb{Q}_p(\zeta_p, \zeta_n)$ which is an abelian extension of $\mathbb{Q}_p$. Since every subgroup of an abelian group is normal, we have $G(\mathbb{Q}_p(\zeta_p, \zeta_n)|\mathbb{Q}_p(\sqrt[p]{p}))$ is normal in $G(\mathbb{Q}_p(\zeta_p, \zeta_n)|\mathbb{Q}_p)$, which implies that $\mathbb{Q}_p(\sqrt[p]{p})|\mathbb{Q}_p$ is a normal extension which is absurd.

We will now obtain the Kronecker Weber theorem from its local analogue, which will serve as a testament to the beautiful idea of local global principle.

Theorem 4.2.4 (Global Kronecker Weber theorem). *Every finite abelian extension $L|\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta)$ of $\mathbb{Q}$.*

Proof. Let S be the set of all primes that ramify in L , and let $L_{\mathcal{P}}$ be the completion of p with respect to a prime $\mathcal{P}$ lying above p . Then, $L_{\mathcal{P}}|\mathbb{Q}_p$ is abelian (since the Galois group of $L_{\mathcal{P}}|\mathbb{Q}_p$ is the decomposition group $D(\mathcal{P}|p)$, which being the subgroup of the abelian group $L|\mathbb{Q}$ is abelian). Therefore, by the local Kronecker Weber theorem $L_{\mathcal{P}} \subseteq \mathbb{Q}_p(\mu_{n_p})$ for a suitable n_p . Let p^{e_p} be the maximum power of p dividing n_p , and let $n = \prod_{p \in S} p^{e_p}$.

We now claim that L is contained in $\mathbb{Q}(\zeta_n)$. To see this, put $M := L(\mu_n)$. Then, $M|\mathbb{Q}$ is abelian (compositum of L and $\mathbb{Q}(\mu_n)$, both of which are abelian), and if p is ramified in

$M|\mathbb{Q}$, then $p \in S$. If the restriction of M_β to L is $L_\mathcal{P}$ where β is a prime above $\mathcal{P}$, then $M_\beta = L_\mathcal{P}(\mu_n) = \mathbb{Q}_p(\mu_{p^{e_p}n'}) = \mathbb{Q}_p(\mu_{p^{e_p}})\mathbb{Q}_p(\mu_{n'})$ with $(n', p) = 1$. $\mathbb{Q}_p(\mu_{n'})|\mathbb{Q}_p$ is the maximal unramified subextension of $\mathbb{Q}_p(\mu_n)|\mathbb{Q}_p$, so the inertia group $I_\mathcal{P}$ of $M_\mathcal{P}|\mathbb{Q}_p$ is isomorphic to $G(\mathbb{Q}_p(\mu_{p^{e_p}})|\mathbb{Q}_p)$, and has order $\phi(p^{e_p})$ where ϕ is the Euler totient function. Let I be the subgroup of $G(M|\mathbb{Q})$ generated by all I_p , $p \in S$. Then the fixed field of I is unramified at all finite primes over $\mathbb{Q}$, hence must be $\mathbb{Q}$ (By Minkowski theorem, $d_K > 1$ for all number fields $K \neq \mathbb{Q}$), i.e., $I = G(M|\mathbb{Q})$. Meanwhile we have

$$\#I \leq \prod_{p \in S} I_p = \prod_{p \in S} \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$$

Hence $[M : \mathbb{Q}] = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$, so that $M = \mathbb{Q}(\mu_n)$, and hence $M = L\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_n)$, so $L \subseteq \mathbb{Q}(\mu_n)$. $\square$

Example 18 (Global Kronecker Weber theorem for quadratic extensions). *The quadratic extension $\mathbb{Q}(\sqrt{p})|\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_p)$ for all odd primes $p \equiv 1 \pmod{4}$ and $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_{4p})$ by following a similar argument as in Example 17. Thus, if $n = p_1 p_2 \cdots p_r$, then $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{4^r n})$. The extension $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is contained in the biquadratic extension $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8)$.*

Remark 4.2.3. *We cannot replace $\mathbb{Q}$ in the global Kronecker Weber theorem by an arbitrary global field. Let p be an odd prime and consider the extension $\mathbb{Q}(\sqrt[4]{p})|\mathbb{Q}(\sqrt{p})$. Proceed similarly as in Example 4.2.2 to obtain a contradiction.*

Chapter 5

Global class field theory

The role of the multiplicative group of the base field is taken up in global class field theory by the idèle class group. The notion of idèle was introduced by the French mathematician Claude Chevalley to provide a suitable framework for local global principle, since it holds information about all places of the number field.

In this chapter, we first define the idèle group and the idèle class group of a number field. Next, we show that the idèle group and the idèle class group are canonically G modules of the Galois group G . We then show that the idèle class group satisfies the class field axiom. As a consequence, we obtain the Hasse norm theorem, which states that an element is a norm globally if and only if it is a norm locally everywhere, thereby showing that the norm map satisfies local global principle.

We then construct a surjective homomorphism d from the absolute Galois group to $\hat{\mathbb{Z}}$ and a Henselian valuation v , to finally obtain the global reciprocity law. We use the local norm residue symbol at all places of a number field to construct the Henselian valuation, and ultimately obtain the global norm residue symbol as a product of the local norm residue symbols, thereby demonstrating the importance of local global principle in the development of class field theory.

Finally, we define the global conductor which detects ramification in number field extensions and the Hilbert class field, which is the maximal everywhere unramified abelian extension.

Throughout this chapter, L and K will denote number fields, $\mathcal{P}$ a prime ideal in K , $\beta|\mathcal{P}$

a prime β of L lying above a prime $\mathcal{P} \in K$, $K_{\mathcal{P}}$ the completion of K w.r.t $\mathcal{P}$ and $O_{\mathcal{P}}$ its valuation ring. $\mathcal{P} \mid \infty$ will denote the infinite places, while $\mathcal{P} \nmid \infty$ will denote the finite places, and S will denote a finite set of primes.

The primary reference for this chapter is Chapter 6 of [7].

5.1 Preliminaries

Definition 5.1.1 (Adèles). *An adèle is a tuple $(\alpha_{\mathcal{P}})$ where $\alpha_{\mathcal{P}} \in K_{\mathcal{P}}$ and $\alpha_{\mathcal{P}} \in O_{\mathcal{P}}$ for all but finitely many places $\mathcal{P}$.*

The set of adèles forms a ring under component-wise addition and multiplication.

We endow adèles with a topology where the basic neighbourhoods about 0 are given by $\prod_{\mathcal{P} \in S} W_{\mathcal{P}} \times \prod_{\mathcal{P} \notin S} O_{\mathcal{P}}$ such that $W_{\mathcal{P}} \subseteq K_{\mathcal{P}}$ is an open neighbourhood of 0. This topology makes the ring of adèles a topological ring.

Definition 5.1.2 (Idèles). *An idèle is a tuple $(\alpha_{\mathcal{P}}) \in K_{\mathcal{P}}^{\times}$ and in fact $\alpha_{\mathcal{P}} \in U_{\mathcal{P}}$ for all but finitely many places $\mathcal{P}$.*

The idèles form a group under component-wise multiplication. In fact the group of idèles is the multiplicative group of the ring of adèles.

We endow idèles with a topology where the basic neighbourhoods about 1 are given by $\prod_{\mathcal{P} \in S} W_{\mathcal{P}}^{\times} \times \prod_{\mathcal{P} \notin S} U_{\mathcal{P}}$ such that $W_{\mathcal{P}} \subseteq K_{\mathcal{P}}^{\times}$ is an open neighbourhood of 1. This topology makes the idèles a topological group.

Example 19. *Idèle group of $\mathbb{Q}$: The map $(a, b, (u_p)) \mapsto (ab, au_2, au_3, \dots) : \mathbb{Q}^{\times} \times \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^{\times} \rightarrow I_{\mathbb{Q}}$ is an isomorphism of topological groups. See [6] for details.*

Remark 5.1.1. *It can be easily observed that the adèle ring and idèle group are Hausdorff. Furthermore, noting that $O_{\mathcal{P}}$ and $U_{\mathcal{P}}$ are compact, we obtain the fact that the adèles and idèles are locally compact w.r.t. to their respective topologies.*

Remark 5.1.2. *The topology on idèles inherited as a subspace of adèles is strictly coarser than the topology endowed on the idèle class group. In fact, the topology on the idèle class group is the coarsest topology which makes the inverse map continuous.*

Definition 5.1.3 (*S*-idèles). For a finite set of places S , an S idèle is an idèle such that $\alpha_{\mathcal{P}} \in O_{\mathcal{P}}^{\times}$ for all $\mathcal{P} \notin S$. The set of S -idèles forms a subgroup of I_K .

We clearly have $I_K = \bigcup_S I_K^S$ where S ranges over all finite set of places, thus I_K is the direct limit of I_K^S .

Definition 5.1.4 (Principal idèles). The inclusions $K \hookrightarrow K_{\mathcal{P}}$ induces an injective homomorphism from $K^{\times} \rightarrow I_K$ given by $\alpha \mapsto (\alpha_{\mathcal{P}})$. We thus view $K^{\times}$ as a subgroup of I_K .

Now, K^S is defined to be the subgroup $I_K^S \cap K^{\times}$ which consists of all $a \in K^{\times}$ which are units at all finite places.

Definition 5.1.5 (Idèle class group). The idèle class group C_K is defined to be the quotient $C_K := I_K / K^{\times}$.

The idèle class group is endowed with the quotient topology from the topology on the group of idèles.

Example 20. The idèle class group of $\mathbb{Q}$ is $\mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^{\times}$ which can be seen from Example 19.

Definition 5.1.6 (Ideal class group). Let J_K denote the group of all fractional ideals of K and P_K the group of all principal fractional ideals. Then, the ideal class group is defined to be the quotient $Cl_K := J_K / P_K$.

Remark 5.1.3. It can be shown that the ideal class group is finite. The cardinality of the ideal class group is called the ‘class number’ of K .

Example 21. The ideal class group of $\mathbb{Q}$, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-2})$ are trivial since the ring of integers for these number fields are PIDs. The ideal class group of $\mathbb{Q}(\sqrt{-5})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Proposition 5.1.1. $K^{\times}$ is a discrete, hence closed subgroup of I_K .

Proof. 1. We first show that $K^{\times}$ is discrete by showing that there is a neighbourhood of $1 \in I_K$ which has no other principal idèles. We claim that $U = \{\alpha \in I_K \mid |\alpha_{\mathcal{P}}| = 1 \text{ for } \mathcal{P} \nmid \infty \text{ and } |\alpha_{\mathcal{P}} - 1|_{\mathcal{P}} < 1 \text{ for } \mathcal{P} \mid \infty\}$ is such a neighbourhood. Suppose $x \in K^{\times} \cap U$, then we get the contradiction

$$1 = \prod_{\mathcal{P}} |x - 1|_{\mathcal{P}} = \prod_{\mathcal{P} \nmid \infty} |x - 1|_{\mathcal{P}} \prod_{\mathcal{P} \mid \infty} |x - 1|_{\mathcal{P}} < \prod_{\mathcal{P} \mid \infty} \max(|x|_{\mathcal{P}}, 1) = 1$$

2. Since the map $(x, y) \mapsto xy^{-1}$ is continuous, there is a neighbourhood V of 1 such that $VV^{-1} \subseteq U$. For every $y \in I_K$, the neighbourhood V contains at most one element of $K^\times$, because if $x_1 = yv_1$ and $x_2 = yv_2$ such that $x_1 \neq x_2$, then clearly $v_1 \neq v_2$ but $x_1x_2^{-1} = v_1v_2^{-1} \in U$, which is a contradiction. Hence choosing a neighbourhood yW of y contained in yV which does not contain any element of $K^\times$, we have $yW \subseteq K^{\times \mathbb{C}}$. $\square$

Remark 5.1.4. From the above proposition, we can deduce that the idèle class group is a locally compact Hausdorff topological group.

The following theorem is a generalisation of Dirichlet's unit theorem, which gives the structure of the unit group of the ring of integers of an algebraic number field.

Theorem 5.1.2. If S contains all the infinite places, then the homomorphism

$$\lambda : K^S \rightarrow \prod_{\mathcal{P} \in S} \mathbb{R} \quad \lambda(a) = (\log|a|_{\mathcal{P}})_{\mathcal{P} \in S}$$

has as its kernel the roots of unity contained in K denoted $\mu(K)$, and its image is a complete lattice in the $s - 1$ dimensional space $H = \{(x_{\mathcal{P}}) \in \prod_{\mathcal{P} \in S} \mathbb{R} \mid \sum_{\mathcal{P} \in S} x_{\mathcal{P}} = 0\}$, where $s = \#S$.

Proof. For the set $S = S_\infty = \{\mathcal{P} \mid \infty\}$, this is the Dirichlet unit theorem. Now, let $S_f = S \setminus S_\infty$, and let $J(S_f)$ be the subgroup of J_K generated by the prime ideals $\mathcal{P} \in S_f$. We assign to every $a \in K^S$ the principal ideal $\langle a \rangle$ and obtain the below commutative diagram where the rows are exact.

$$\begin{array}{ccccccc} 1 & \longrightarrow & O_K^\times & \xrightarrow{j_1} & K^S & \xrightarrow{i_1} & J(S_f) \\ & & \downarrow \lambda' & & \downarrow \lambda & & \downarrow \lambda'' \\ 0 & \longrightarrow & \prod_{\mathcal{P} \in S_\infty} \mathbb{R} & \xrightarrow{j_2} & \prod_{\mathcal{P} \in S} \mathbb{R} & \xrightarrow{i_2} & \prod_{\mathcal{P} \in S_f} \mathbb{R} \end{array}$$

The map on the right is given by $\lambda''(\prod_{\mathcal{P} \in S_f} \mathcal{P}^{v_{\mathcal{P}}}) = - \prod_{\mathcal{P} \in S_f} v_{\mathcal{P}} \log(\mathcal{N}(\mathcal{P}))$ and $\lambda'(a) = (\log|a|_{\mathcal{P}})_{\mathcal{P} \in S_\infty}$.

The right square commutes because $|a|_{\mathcal{P}} = \mathcal{N}(\mathcal{P})^{-v_{\mathcal{P}}(a)}$. It maps $J(S_f)$ onto the complete lattice spanned by the vectors $e_{\mathcal{P}} = (0, \dots, 0, \log \mathcal{N}(\mathcal{P}), 0, \dots, 0)$ for $\mathcal{P} \in S_f$.

1. $\text{Ker}(\lambda') = \mu(K)$ and $\text{Im}(\lambda)$ is a lattice: By commutativity of both the squares and exactness of the first row, we have $\text{Ker}(\lambda) = \text{Ker}(\lambda') = \mu(K)$, and we obtain the exact sequence

$0 \rightarrow \text{Im}(\lambda') \xrightarrow{j_2} \text{Im}(\lambda) \xrightarrow{i_2} \text{Im}(\lambda'')$, where the groups on the left and right are lattices. This implies that the group in the middle is also a lattice, because if $x \in \text{Im}(\lambda)$ and U is a neighbourhood of $i(x)$ which contains no other point of $\text{Im}(\lambda'')$, then $i^{-1}(U)$ only contains the coset $x + \text{Im}(\lambda')$. It is discrete since $\text{Im}(\lambda')$ is discrete.

2. $\text{Rank}(\text{Im}(\lambda)) = s - 1$: For every $\mathcal{P} \in S_f$, if h is the class number of K , then $P^h \in i_1(K^S)$, so $J(S_f)^h \subseteq i(K^S) \subseteq J(S_f)$. The groups on the left and right have rank $\#S_f$, so $i(K^S)$ has the same rank (note that all of them are $\mathbb{Z}$ modules and $\mathbb{Z}$ is a PID). In the exact sequence $0 \rightarrow \text{Im}(\lambda') \xrightarrow{j_2} \text{Im}(\lambda) \xrightarrow{i_2} \text{Im}(\lambda'')$, the image of i has rank $\#S_f$, and the kernel has rank $\#S_\infty - 1$. Hence $\text{Im}(\lambda) = \#S_\infty - 1 + \#S_f = \#S - 1$. It lies in the $\#S - 1$ dimensional trace zero space H , since $\prod_{\mathcal{P} \in S} |a|_{\mathcal{P}} = \prod_{\mathcal{P}} |a|_{\mathcal{P}} = 1$ for $a \in K^S$ by product formula. $\square$

The following proposition will be used throughout the chapter. It says that the group of idèles is a group of S -idèles upto an element of $K^\times$ for a sufficiently large set of primes.

Proposition 5.1.3. $I_K = I_K^S K^\times$, i.e., $C_K = I_K^S K^\times / K^\times \cong I_K^S / K^S$ where S is a sufficiently large finite set of places of K , which will be described in the proof.

Proof. Let $I_1, \dots, I_h$ be ideals representing the h classes of the ideal class group. Choose a prime ideal $\mathcal{P}_i$ from each class. We claim that if S is a set of places containing the infinite places and the prime ideals above, then $I_K = I_K^S K^\times$.

If $\alpha \in I_K$, then the corresponding ideal $\langle \alpha \rangle = \prod_{\mathcal{P} \nmid \infty} \mathcal{P}^{v_{\mathcal{P}}(\alpha_{\mathcal{P}})}$ belongs to some class $I_i P_K$, i.e., $\langle \alpha \rangle = I_i \langle a \rangle$ for some $a \in K^\times$. The idèle $\alpha' = \alpha a^{-1}$ is mapped to the ideal $I_i = \prod_{\mathcal{P} \nmid \infty} \mathcal{P}^{v_{\mathcal{P}}(\alpha'_{\mathcal{P}})}$ under the canonical map from I_K to J_K . Since the prime ideals occurring in I_i are in S , $v_{\mathcal{P}}(\alpha'_{\mathcal{P}}) = 0$ for all $\mathcal{P}$ not in S , so $\alpha' = \alpha a^{-1} \in I_K^S$, so $\alpha \in I_K^S K^\times$. $\square$

Definition 5.1.7. The absolute norm of an idèle α is defined to be

$$\mathcal{N}(\alpha) = \prod_{\mathcal{P}} \mathcal{N}(\mathcal{P})^{v_{\mathcal{P}}(\alpha_{\mathcal{P}})} = \prod_{\mathcal{P}} |\alpha_{\mathcal{P}}|^{-1}.$$

If $x \in K^\times$ is a principal idèle, then $\mathcal{N}(x) = \prod_{\mathcal{P}} |x|_{\mathcal{P}}^{-1} = 1$. So we have a continuous homomorphism $\mathcal{N} : C_K \rightarrow \mathbb{R}_+^\times$. The kernel of this map is denoted C_K^0 . We have the following important result about C_K^0 , the proof of which may be found in Chapter 6 of [7].

Theorem 5.1.4. The group $C_K^0 = \{[\alpha] \in C_K \mid \mathcal{N}(\alpha) = 1\}$ is compact, and the exact sequence $1 \rightarrow C_K^0 \rightarrow C_K \xrightarrow{\mathcal{N}} \mathbb{R}_+^\times$ splits, i.e., $C_K \cong C_K^0 \times \mathbb{R}_+^\times$.

5.2 Herbrand quotient of the Idèle class group

In this section, we show that the idèle group I_L and the idèle class group C_L are $G = G(L|K)$ modules satisfying Galois descent (i.e., if $L|K$ is a Galois extension with Galois group G , then $I_L^G = I_K$ and $C_L^G = C_K$). We then compute the Herbrand quotient of the S -idèles I_L^S and the principal S -idèles L^S , which gives us the Herbrand quotient of the idèle class group C_L for a finite cyclic extension $L|K$ and for a sufficiently large set of places as described in proof of Proposition [5.1.3](#). We conclude with two important consequences of the value of the Herbrand quotient of the idèle class group.

We first show that the idèle group I_L is a $G(L|K)$ module.

Proposition 5.2.1. *For a finite Galois extension $L|K$, there is a canonical injection $I_K \hookrightarrow I_L$ and I_L is a $G(L|K)$ module.*

Proof. 1. $I_K \hookrightarrow I_L$: We map $\alpha = (\alpha_{\mathcal{P}}) \in I_K$ to $\alpha' = (\alpha'_{\beta}) \in I_L$ where $\alpha'_{\beta} = \alpha_{\mathcal{P}} \in K_{\mathcal{P}}^{\times} \subseteq L_{\beta}^{\times}$ for $\beta|\mathcal{P}$.

2. I_L is a $G(L|K)$ module: For each place β of L , σ induces an isomorphism $\sigma : L_{\beta} \rightarrow (\sigma L)_{\sigma\beta}$. This can be seen as follows: If $\alpha_i \in L$ converge in $|\cdot|_{\beta}$ to α , then $\sigma\alpha_i$ converges w.r.t $|\cdot|_{\sigma\beta}$ in $(\sigma L)_{\sigma\beta}$, and the isomorphism is given by $\alpha = \beta - \lim \alpha_i \mapsto \sigma\beta - \lim \sigma\alpha_i$. Thus we define $(\sigma\alpha) \in I_L$ by the components $(\sigma\alpha)_{\sigma\beta} := \sigma\alpha_{\beta}$. $\square$

We now show that the idèle class group satisfies Galois descent.

Proposition 5.2.2. *If $L|K$ is a Galois extension with Galois group G , then $I_L^G = I_K$*

Proof. 1. $I_K \subseteq I_L^G$: Let $\alpha \in I_K \subseteq I_L$. For $\sigma \in G$, the map $\sigma : L_{\beta} \rightarrow L_{\sigma\beta}$ is a $K_{\mathcal{P}}$ isomorphism, where $\beta|\mathcal{P}$. Hence $(\sigma\alpha)_{\sigma\beta} = \sigma\alpha_{\beta} = \alpha_{\beta} = \alpha_{\sigma\beta}$, the second equality following from the fact that σ fixes K .

2. $I_L^G \subseteq I_K$: If $\alpha \in I_L^G$, then $(\sigma\alpha)_{\sigma\beta} = \sigma\alpha_{\beta} = \alpha_{\sigma\beta}$ for all $\sigma \in G$. In particular, if σ belongs to the decomposition group $G_{\beta} = G(L_{\beta}|K_{\mathcal{P}})$, then $\sigma\beta = \beta$ and $\sigma\alpha_{\beta} = \alpha_{\beta}$, so $\alpha_{\beta} \in K_{\mathcal{P}}^{\times}$. If $\sigma \in G$ is arbitrary, then $\sigma : L_{\beta} \rightarrow L_{\sigma\beta}$ induces the identity map on $K_{\mathcal{P}}$, and we get $\alpha_{\beta} = \sigma\alpha_{\beta} = \alpha_{\sigma\beta}$ for any two places β and $\sigma\beta$ above $\mathcal{P}$. This shows $\alpha \in I_K$. $\square$

Define $L_{\mathcal{P}}^{\times} := \prod_{\beta|\mathcal{P}} L_{\beta}^{\times}$ and $U_{L,\mathcal{P}} := \prod_{\beta|\mathcal{P}} U_{L,\beta}$.

Proposition 5.2.3. *If $L|K$ is a finite extension and $\alpha = (\alpha_\beta) \in I_L$, the components of the idèle $N_{L|K}(\alpha) = \prod_{\beta|\mathcal{P}} N_{L_\beta|K_\mathcal{P}}(\alpha_\beta)$.*

Proof. Setting $\alpha_\mathcal{P} = (\alpha_\beta)_{\beta|\mathcal{P}} \in L_\mathcal{P}$, the $K_\mathcal{P}$ automorphism $\alpha_\mathcal{P} : L_\mathcal{P} \rightarrow L_\mathcal{P}$ given by $x \mapsto \alpha_\mathcal{P}x$ is the direct product of the $K_\mathcal{P}$ automorphisms $\alpha_\beta : L_\beta \rightarrow L_\beta$. Hence

$$N_{L_\beta|K_\mathcal{P}}(\alpha_\mathcal{P}) = \det(\alpha_\mathcal{P}) = \prod_{\beta|\mathcal{P}} \det(\alpha_\beta) = \prod_{\beta|\mathcal{P}} N_{L_\beta|K_\mathcal{P}}(\alpha_\beta)$$

□

The following proposition lists some properties of the norm map.

Proposition 5.2.4. (1) *For a tower of number fields $K \subseteq L \subseteq M$, we have $N_{M|K} = N_{L|K} \circ N_{M|L}$.*

(2) *If $L|K$ is embedded into the Galois extension $M|K$ and if $G = G(M|K)$ and $H = G(M|L)$, then for $\alpha \in I_L$, we have $N_{L|K}(\alpha) = \prod_{\sigma \in G/H} \sigma\alpha$.*

(3) *$N_{L|K}(\alpha) = \alpha^{[L:K]}$ for $\alpha \in I_K$.*

(4) *The norm of the principal idèle $x \in L^\times$ is the principal idèle of K defined by the usual norm $N_{L|K}(x)$.*

Proof. The proofs of (1)-(3) are same as for the norm in a field extension. (4) follows from the isomorphism $L_\mathcal{P} \cong L \otimes_K K_\mathcal{P}$. The $K_\mathcal{P}$ automorphism $x' : L_\mathcal{P} \rightarrow L_\mathcal{P}$, $y \mapsto xy$ is induced from the K automorphism $x : L \rightarrow L$ by tensoring with $K_\mathcal{P}$. Hence $\det(x') = \det(x)$. □

Proposition 5.2.5. *If $L|K$ is a finite extension, then the canonical embedding $I_K \rightarrow I_L$ induces an injection $C_K \rightarrow C_L$, $\alpha K^\times \mapsto \alpha L^\times$.*

Proof. The injection I_K to I_L clearly maps $K^\times$ to $L^\times$, so it is enough to show that the pre-image of $L^\times$ under the injection is precisely $K^\times$, i.e., $I_K \cap L^\times = K^\times$. Let $M|K$ be the Galois closure of $L|K$ with Galois group G . Then $I_K \subseteq I_L \subseteq I_M$, and $I_K \cap L^\times \subseteq I_K \cap M^\times \subseteq (I_K \cap M^\times)^G = I_K \cap M^{\times G} = I_K \cap K^\times$, where the second containment follows from the fact that $G(L|K)$ fixes I_K and hence $I_K \cap M^\times$. □

Proposition 5.2.6. *If $L|K$ is a Galois extension with Galois group $G = G(L|K)$, then C_L is a G module and $C_L^G = C_K$.*

Proof. The G module I_L contains $L^\times$ as a G submodule. Hence every $\sigma \in G$ induces an automorphism $C_L \xrightarrow{\sigma} C_L$, $\alpha L^\times \mapsto (\sigma\alpha)L^\times$, so C_L is a G module.

Thus we obtain an exact sequence of G modules $1 \rightarrow L^\times \rightarrow I_L \rightarrow C_L \rightarrow 1$ and consequently we obtain the exact sequence $1 \rightarrow L^{\times G} = K^\times \rightarrow I_L^G = I_K \rightarrow C_L^G \rightarrow H^1(G, L^\times) \rightarrow H^1(G, I_L) \rightarrow H^1(G, C_L)$. Noting that $H^1(G, L^\times) = 1$ by Noether's generalisation of Hilbert's theorem 90, we have $C_L^G = C_K$. $\square$

Having proved that the idèle class group C_L is a $G(L|K)$ module, we turn our attention to computing its Herbrand quotient.

Recall $L_{\mathcal{P}}^\times := \prod_{\beta|\mathcal{P}} L_\beta^\times$ and $U_{L,\mathcal{P}} := \prod_{\beta|\mathcal{P}} U_{L,\beta}$.

Proposition 5.2.7. $L_{\mathcal{P}}^\times$ and $U_{L,\mathcal{P}}$ are the induced G modules $L_{\mathcal{P}}^\times = \text{Ind}_G^{G_\beta}(L_{\beta^\times})$ and $U_{L,\mathcal{P}} = \text{Ind}_G^{G_\beta}(U_{L_\beta})$

Proof. $L_{\mathcal{P}}^\times = \prod_{\sigma \in G/G_\beta} L_{\sigma\beta}^\times = \prod_{\sigma \in G/G_\beta} \sigma(L_\beta^\times)$ and a similar deduction is made for $U_{L,\mathcal{P}}$. $\square$

Let S be a finite set of places of K containing the infinite places. We define $I_L^S = I_L^{\bar{S}}$ where $\bar{S}$ is the set of places of L lying above S . In the next proposition, we will determine the cohomology groups of the S idèles I_L^S and consequently that of the idèles.

Proposition 5.2.8. *If $L|K$ is a cyclic extension, and if S contains all the places ramified in L , then for $i = 0, -1$, $H^i(G, I_L^S) \cong \bigoplus_{\mathcal{P} \in S} H^i(G_\beta, L_\beta^\times)$ and $H^i(G, I_L) \cong \bigoplus_{\mathcal{P}} H^i(G_\beta, L_\beta^\times)$, where β is a chosen place above $\mathcal{P}$ in K .*

Proof. By definition, $I_L^S = \bigoplus_{\mathcal{P} \in S} L_{\mathcal{P}}^\times \oplus V$ where $V = \prod_{\mathcal{P}} U_{L,\mathcal{P}}$ which gives us the isomorphisms $H^i(G, I_L^S) \cong \bigoplus_{\mathcal{P} \in S} H^i(G, L_{\mathcal{P}}^\times)$ and $H^i(G, V) \cong \prod_{\mathcal{P} \notin S} H^i(G, U_{L,\mathcal{P}})$. Since $L_{\mathcal{P}}^\times$ and $U_{L,\mathcal{P}}$ are induced G modules, we have $H^i(G, L_{\mathcal{P}}^\times) \cong H^i(G_\beta, L_\beta^\times)$ and $H^i(G, U_{L,\mathcal{P}}) \cong H^i(G_\beta, U_{L_\beta})$. For $\mathcal{P} \notin S$, $L_\beta|K_\mathcal{P}$ is unramified, hence $H^i(G_\beta, U_{L_\beta})$ by Theorem 4.1.3. This shows the first claim. For the second, notice that I_L is a direct limit of I_L^S and hence

$$H^i(G, I_L) = \varinjlim_S H^i(G, I_L^S) \cong \varinjlim_S \bigoplus_{\mathcal{P} \in S} H^i(G_\beta, L_\beta^\times) = \bigoplus_{\mathcal{P}} H^i(G_\beta, L_\beta^\times)$$

$\square$

Remark 5.2.1. The proposition says that $H^{-1}(G, I_L) = 1$ since $H^{-1}(G_\beta, L_\beta^\times) = 1$ for all β by Hilbert's theorem 90, since if G is cyclic, then G_β being a subgroup of G is cyclic for all finite places. $\#G_\beta = 1$ or 2 if β is an infinite place, hence G_β is cyclic in this case too. Further the proposition says that $I_K/N_{L|K}I_L = \bigoplus_{\mathcal{P} \in S} K_{\mathcal{P}}^\times/N_{L_\beta|K_{\mathcal{P}}}L_\beta^\times$, hence an idèle is a norm if and only if each of its components is a norm. This is clearly another instance of local global principle.

Proposition 5.2.9. Let $L|K$ be a cyclic extension and S a finite set of places of K containing the infinite places and all the primes that ramify in L . Then $h(G, I_L^S) = \prod_{\mathcal{P} \in S} n_{\mathcal{P}}$ where $n_{\mathcal{P}} = [L_\beta : K_{\mathcal{P}}]$ and β is a chosen place above $\mathcal{P}$.

Proof. We know $H^{-1}(G, I_L^S) = \bigoplus_{\mathcal{P} \in S} H^{-1}(G_\beta, L_\beta^\times) = 1$ and $H^0(G, I_L^S) = \bigoplus_{\mathcal{P} \in S} H^0(G_\beta, L_\beta^\times)$. By the local reciprocity map, we have $\#H^0(G_\beta, L_\beta^\times) = n_{\mathcal{P}}$ for each finite place $\mathcal{P}$ in S . Hence, $h(G, I_L^S) = \frac{\#H^0(G, I_L^S)}{\#H^{-1}(G, I_L^S)} = \prod_{\mathcal{P} \in S} n_{\mathcal{P}}$. $\square$

We now determine the Herbrand quotient of I_L for the cyclic extension $L|K$. But first we need the following lemma.

Lemma 5.2.10. Let V be an s dimensional $\mathbb{R}$ vector space, and let G be a finite group of automorphism of V acting on a basis $v_1, \dots, v_s$ as a permutation group on the basis elements, i.e., $\sigma(v_i) = v_{\sigma(i)}$. If Γ is a G invariant complete sublattice, i.e., $\sigma\Gamma \subseteq \Gamma$ for all $\sigma \in G$, then there is a complete sublattice $\Gamma' \subseteq \Gamma$ such that $\Gamma' = \mathbb{Z}w_1 + \dots + \mathbb{Z}w_s$ such that $\sigma w_i = w_{\sigma(i)}$ for all $\sigma \in G$.

Proof. Let $\|\cdot\|$ be the sup norm on V with respect to the coordinates of the basis $v_1, \dots, v_s$, i.e., $\|x_1 - x_2\| = \max_{1 \leq i \leq s} c_i$ where c_i are the coordinates of $x_1 - x_2$ with respect to the basis $v_1, \dots, v_s$. Since Γ is a lattice, $\exists b \in \mathbb{R}$ such that for every $x \in V$, there is a $\gamma \in \Gamma$ satisfying $\|x - \gamma\| < b$. Choose a large enough positive t and $\gamma \in \Gamma$ such that $\|tv_1 - \gamma\| < b$ and define $w_i = \sum_{\sigma(1)=i} \sigma\gamma$, $i = 1, \dots, s$. For every $\tau \in G$, we have

$$\tau w_i = \sum_{\sigma(1)=i} \tau\sigma\gamma = \sum_{\rho(1)=\tau(i)} \rho\gamma = w_{\tau(i)}$$

Hence it is enough to check that the w_i are $\mathbb{R}$ linearly independent. Suppose $\sum_{i=1}^s c_i w_i = 0$, $c_i \in \mathbb{R}$. If not all of the c_i are zero, then by dividing throughout by the largest c_i , we may

assume $c_j = 1$ for some j and $|c_i| \leq 1$ for all other i . Let $y = tv_1 - \gamma$ for some y such that $|y| < b$. Then

$$w_i = \sum_{\sigma(1)=i} \sigma\gamma = t \sum_{\sigma(1)=i} \sigma(v_1) - y_i = t \sum_{\sigma(1)=i} v_{\sigma(1)} - y_i = tn_i v_i - y_i$$

where $y_i = \sum_{\sigma(1)=i} \sigma y$, hence $|y_i| \leq nb$ for $n = \#G$ and $n_i = \{\sigma \in G \mid \sigma(1) = i\}$. Therefore $0 = \sum_{i=1}^s c_i w_i = t \sum_{i=1}^s c_i n_i v_i - z$ with $|z| \leq sgb$, but this is contradicted by choosing t large enough in the expression $z = tn_j v_j + \sum_{i \neq j} tn_i v_i$. $\square$

Proposition 5.2.11. *The Herbrand quotient of the G module L^S satisfies $h(G, L^S) = \frac{1}{n} \prod_{\mathcal{P} \in S} n_{\mathcal{P}}$ where S contains all the infinite places of L and all the places of L lying above places of K that ramify in L .*

Proof. Let $\{e_{\beta} \mid \beta \in S\}$ be the standard basis of the $\mathbb{R}$ vector space $V = \prod_{\beta \in S} \mathbb{R}$. By the generalisation of Dirichlet unit theorem, the homomorphism $\lambda : L^S \rightarrow V$, $\lambda(a) = \sum_{\beta \in S} \log|a|_{\beta} e_{\beta}$ has kernel $\mu(L)$ and its image is the $s - 1$ dimensional lattice, $s = \#S$. The action of G on V is given via $\sigma e_{\beta} = e_{\sigma\beta}$. Then λ is a G module homomorphism because for $\sigma \in G$,

$$\lambda(\sigma a) = \sum_{\beta} \log|\sigma a|_{\beta} e_{\beta} = \sum_{\beta} \log|a|_{\sigma^{-1}\beta} e_{\beta} = \sum_{\beta} \log|a|_{\sigma^{-1}\beta} \sigma e_{\sigma^{-1}\beta} = \sigma \left(\sum_{\beta} \log|a|_{\sigma^{-1}\beta} e_{\sigma^{-1}\beta} \right) = \sigma \lambda(a)$$

Note that $e_0 = \sum_{\beta \in S} e_{\beta}$ and $\lambda(L^S)$ are $\mathbb{R}$ linearly independent since if $\lambda(a) = ce_0$, then $\log|a|_{\beta} = c$ for all β , and since $\sum_{\beta \in S} \log|a|_{\beta} = 0$, we have $sc = 0$, hence $c = 0$. Therefore e_0 and $\lambda(L^S)$ generate a G -invariant complete lattice Γ in V . Since $\mathbb{Z}e_0$ is isomorphic to $\mathbb{Z}$ as G modules, the exact sequence $0 \rightarrow \mathbb{Z}e_0 \rightarrow \Gamma \rightarrow \Gamma/\mathbb{Z}e_0 \rightarrow 0$ together with $\Gamma/\mathbb{Z}e_0 = \lambda(L^S)$ gives

$$h(G, L^S) = h(G, \lambda(L^S)) = h(G, \Gamma)/h(G, \mathbb{Z}) = \frac{1}{n} h(G, \Gamma)$$

Now we choose in Γ a sublattice Γ' as in the previous lemma. Then,

$$\Gamma' = \bigoplus_{\beta} \mathbb{Z}w_{\beta} = \bigoplus_{\mathcal{P} \in S} \bigoplus_{\beta \mid \mathcal{P}} \mathbb{Z}w_{\beta} = \bigoplus_{\mathcal{P} \in S} \Gamma'_{\mathcal{P}}$$

and $\sigma w_{\beta} = w_{\sigma\beta}$. Thus, $\Gamma'_{\mathcal{P}}$ is the induced G module

$$\Gamma'_{\mathcal{P}} = \bigoplus_{\beta \mid \mathcal{P}} \mathbb{Z}w_{\beta} = \bigoplus_{\sigma \in G/G_{\beta}} \sigma(\mathbb{Z}w_{\beta_0}) = \text{Ind}_G^{G_{\beta}}(\mathbb{Z}w_{\beta_0})$$

where β_0 is a chosen place above $\mathcal{P}$, and G_β its decomposition group. The lattice Γ' has the same rank as Γ , hence is of finite index in Γ . (by Fundamental theorem of finitely generated abelian groups). Hence we obtain

$$h(G, L^S) = \frac{1}{n} h(G, \Gamma') = \frac{1}{n} \prod_{\mathcal{P} \in S} h(G_\beta, \mathbb{Z}w_{\beta_0}) = \frac{1}{n} h(G_\beta, \mathbb{Z})$$

where $n_{\mathcal{P}} = [L_\beta : K_{\mathcal{P}}]$ □

Now choosing a finite set of places S such that $I_L = I_L^S L^\times$ and such that S contains all the ramified primes and all the infinite primes, we obtain the exact sequence

$$1 \rightarrow L^S \rightarrow I_L^S \rightarrow I_L^S / L^S = I_L^S L^\times / L^\times = I_L / L^\times = C_L \rightarrow 1,$$

we obtain the identity $h(G, I_L^S) = h(G, C_L) h(G, L^S)$, so $h(G, C_L) = \frac{\prod_{\mathcal{P} \in S} n_{\mathcal{P}}}{\prod_{\mathcal{P} \in S} n_{\mathcal{P}}/n} = n$. Therefore,

Theorem 5.2.12. *If $L|K$ is a cyclic extension of degree n and $G = G(L|K)$, then $h(G, C_L) = \frac{\#H^0(G, C_L)}{\#H^{-1}(G, C_L)} = n$. In particular, $\#H^0(G, C_L) = [C_K : N_{L|K} C_L] \geq n$*

Corollary 5.2.13. *Let $L|K$ be a cyclic extension of degree p^r . Then there are infinitely many primes that do not split in L .*

Proof. Suppose there are only finitely many primes that do not split. Let $M|K$ be the unique degree p subextension of $L|K$. For every $\mathcal{P} \notin S$, the decomposition group $G_{\mathcal{P}}$ of $L|K$ is strictly contained in $G(L|M)$. Hence, $\#G_{\mathcal{P}} \leq p^{r-1}$, so by cyclicity of $G(L|K)$, we have $G_{\mathcal{P}} \subseteq G(L|M)$, so every $\mathcal{P} \notin S$ splits completely in M . We will show now that $N_{M|K} C_M = C_K$, contradicting the fact that $\#H^0(G(L|K), C_L) \geq n$.

Let $\alpha \in I_K$. By approximation theorem, $\exists a \in K^\times$ such that $\alpha_{\mathcal{P}} a^{-1}$ is contained in the open subgroup $N_{M_\beta|K_{\mathcal{P}}} M_\beta^\times$ for all $\mathcal{P} \in S$. If $\mathcal{P} \notin S$, then $\alpha_{\mathcal{P}} a^{-1} \in N_{M_\beta|K_{\mathcal{P}}} M_\beta^\times$ because $M_\beta = K_{\mathcal{P}}$. Since $I_K / N_{M|K} I_M = \bigoplus_{\mathcal{P} \in S} K_{\mathcal{P}}^\times / N_{M_\beta|K_{\mathcal{P}}} M_\beta^\times$, the idèle αa^{-1} is a norm of some idèle γ of I_M , i.e., $\alpha = N_{M|K}(\gamma) a \in N_{M|K} I_M K^\times$, which shows that the class of α is in $N_{M|K} C_M$. □

Remark 5.2.2. *If $L|K$ is a non-cyclic Galois extension then there are only finitely many primes that do not split in L . This can be seen as follows: Suppose to the contrary that there are infinitely many primes that do not split. Since there are only finitely many ramified primes, the remaining primes are unramified. Choose such an unramified non-split prime $\mathcal{P}$. Since $e f r = \#G(L|K)$ where $r = \#G/G_{\mathcal{P}}$, hence $r = 1$ and e being the ramification index is 1. Thus, $f = \#G$, so $G \cong G_{\mathcal{P}}$ which is cyclic, which contradicts our assumption about G .*

Proposition 5.2.14. *Let $L|K$ be a finite extension of number fields such that almost all the places of K split completely in L . Then $L = K$.*

Proof. 1. We may assume WLOG that $L|K$ is Galois:

Let M be the Galois closure of $L|K$, and let $G = G(M|K)$, $H = G(M|L)$, β a place of M above a place $\mathcal{P}$ of K , and G_β its decomposition group. Then, the number of places of L above $\mathcal{P}$ equals the number of double cosets $\#H \backslash G / G_\beta$. This can be seen by considering the map $H\sigma G_\beta \mapsto \sigma\beta \cap L$. This map is well defined since if $H\sigma_1 G_\beta = H\sigma_2 G_\beta$, then $\sigma_1 = h\sigma_2 g$ where $h \in H$ and $g \in G_\beta$, so $\sigma_1\beta \cap L = h\sigma_2 g\beta \cap L = h\sigma_2\beta \cap L = h(\sigma_2\beta \cap L) = \sigma_2\beta \cap L$ since h fixes L . Since there is a unique prime ideal in L lying below any prime ideal in K , we obtain the bijectivity of the map. Now we have that $\mathcal{P}$ splitting completely in L is equivalent to $\#H \backslash G / G_\beta = [L : K] = \#H \backslash G$. This is equivalent to $G_\beta = 1$, hence $\mathcal{P}$ splits completely in M .

2. Suppose $L|K$ is Galois: Let K' be the fixed field of an element σ of prime order in $G(L|K)$. If almost all primes v of K split completely in L , then so is the case for primes $\mathcal{P}$ of K' lying above v in L . This contradicts the previous corollary. $\square$

5.3 Global class field axiom

Let K be a number field such that $\mu_n \subseteq K$ and $n = p^r$. Let $L|K$ be a Galois extension with Galois group $G(L|K) \cong (\mathbb{Z}/n\mathbb{Z})^r$. Let S be a finite set of primes containing the infinite primes, ramified primes, those that divide n and such that $I_K = I_K^S K^\times$, and let $K^S := I_K^S \cap K^\times$ and $s = \#S$.

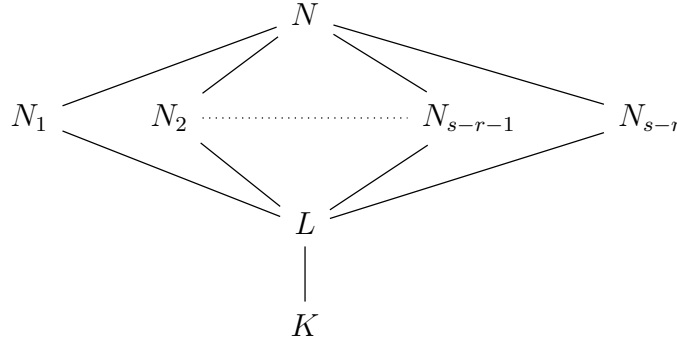
The following proposition gives a set of primes T disjoint from S . $S \cup T$ gives a large enough set of primes such that

Proposition 5.3.1. *Let $r \in \mathbb{N}$ be such that $G(L|K) \cong (\mathbb{Z}/n\mathbb{Z})^r$. Then, $s \geq r$ and there is a set of $s - r$ primes T of K that do not belong to S such that $L = K(\sqrt[n]{\Delta})$, where Δ is the kernel of the map $K^S \rightarrow \prod_{\mathcal{P} \in T} K_{\mathcal{P}}^\times / K_{\mathcal{P}}^{\times n}$.*

Proof. 1. $L = K(\sqrt[n]{\Delta})$ with $\Delta = L^{\times n} \cap K^\times$. $\mu_n \subseteq L$ and L is an abelian extension of exponent n , hence $L = K(\sqrt[n]{D})$ with $D = L^{\times n} \cap K^\times$, hence $\Delta \subseteq D$ and $K^{\times n} \subseteq L^{\times n} \cap K^\times \subseteq D$. Now if $x \in D$, then $K_{\mathcal{P}}(\sqrt[n]{x})|K_{\mathcal{P}}$ is unramified for all $\mathcal{P} \notin S$, because S contains all the

ramified places. Since S also contains primes dividing n , $\langle n \rangle + \mathcal{P} = O_K$ for all $\mathcal{P} \notin S$, so $(n, \text{ch}(k_{K_{\mathcal{P}}})) = 1$ for all $\mathcal{P} \notin S$. Thus, we may write $x = u_{\mathcal{P}} y_{\mathcal{P}}^n$, with $u_{\mathcal{P}} \in U_{\mathcal{P}}$, $y_{\mathcal{P}} \in K_{\mathcal{P}}^{\times}$. Setting $y_{\mathcal{P}} = 1$ for $\mathcal{P} \in S$, we obtain the idèle $y = (y_{\mathcal{P}})$. Now $y = \alpha z$ with $\alpha \in I_K^S$ and $z \in K^{\times}$. So $xz^{-n} = u_{\mathcal{P}} y_{\mathcal{P}}^n \in U_{\mathcal{P}}$ for all $\mathcal{P} \notin S$, i.e., $xz^{-n} \in I_K^S \cap K^{\times} = K^S$, so $xz^{-n} \in \Delta$, and hence $D = \Delta K^{\times n}$.

2. Choice of set of primes T : The field $N = K(\sqrt[n]{K^S})$ contains L because $\Delta = L^{\times n} \cap K^S \subseteq K^S$. By Kummer theory, we have $G(N|K) \cong \text{Hom}(K^S/(K^S)^n, \mathbb{Z}/n\mathbb{Z})$. By Theorem 5.1.2, K^S is the product of a free group of rank $s-1$ and the cyclic group $\mu(K)$ of n^{th} roots of unity contained in K , whose order is divisible by n . $K^S/(K^S)^n$ is non-canonically isomorphic to $\text{Hom}(K^S/(K^S)^n, \mathbb{Z}/n\mathbb{Z})$ and thus $K^S/(K^S)^n$ is isomorphic to $G(N|K)$. Hence $K^S/(K^S)^n$ is a free module of rank s , and so is $G(N|K)$. Also, $G(N|K)/G(N|L) \cong G(L|K) \cong (\mathbb{Z}/n\mathbb{Z})^r$ is a free $\mathbb{Z}/n\mathbb{Z}$ module of rank r , so $r \leq s$, and $G(N|L)$ is a $\mathbb{Z}/n\mathbb{Z}$ module of rank $s-r$. Let $\sigma_1, \dots, \sigma_s$ be a $\mathbb{Z}/n\mathbb{Z}$ basis of $G(L|N)$, and let N_i be a fixed field of σ_i , $i = 1, \dots, s-r$. Then $L = \cap_{i=1}^{s-r} N_i$.



For $i = 1, \dots, s-r$, choose a prime β_i of N_i which does not split in N such that the primes $\mathcal{P}_1, \dots, \mathcal{P}_{s-r}$ lying below $\beta_1, \dots, \beta_{s-r}$ are all distinct, and do not belong to S , and this can be done because of Corollary 5.2.13.

3. Δ is the kernel of $K^S \rightarrow \prod_{\mathcal{P} \in T} K_{\mathcal{P}}^{\times} / K_{\mathcal{P}}^{\times n}$: We claim that N_i is the decomposition field of $N|K$ at the unique prime β'_i lying above β_i , for $i = 1, \dots, s-r$.

The decomposition field Z_i is contained in N_i because β_i does not split in N . Now observe that $\mathcal{P}_i$ is unramified in N because it is unramified in the extension $K(\sqrt[n]{u})$, $u \in K^S$, and N is the composite of these extensions by (1). The decomposition group $G(N|Z_i) \subseteq G(N|N_i)$ is thus cyclic. It is of order n since each element of $G(N|K)$ has order dividing n , and at least one element with order n . (since $G(N|K) \cong (\mathbb{Z}/n\mathbb{Z})^s$) This shows that $N_i = Z$.

Since $L = \cap_{i=1}^{s-r} N_i$, it follows that $L|K$ is the maximal subextension of $N|K$ in which primes

split completely. For $x \in K^S$, we thus have

$$x \in \Delta \iff K(\sqrt[n]{x}) \subseteq L \iff K_{\mathcal{P}_i}(\sqrt[n]{x}) = K_{\mathcal{P}_i} \iff x \in K_{\mathcal{P}_i}^{\times n}$$

which concludes the result. The fact that $K(\sqrt[n]{x}) \subseteq L \iff K_{\mathcal{P}_i}(\sqrt[n]{x}) = K_{\mathcal{P}_i}$ follows from the fact that $\mathcal{P}_1, \dots, \mathcal{P}_{s-r}$ splits completely in L . $\square$

Now define $I_K(S, T) := \prod_{\mathcal{P} \in S} K_{\mathcal{P}}^{\times n} \times \prod_{\mathcal{P} \in S} K_{\mathcal{P}}^{\times} \times \prod_{\mathcal{P} \notin S \cup T} U_{\mathcal{P}}$ and $C_K(S, T) := I_K(S, T)K^{\times}/K^{\times}$ where S and T are a finite set of places as in the above theorem.

Lemma 5.3.2. $I_K(S, T) \cap K^{\times} = (K^{S \cup T})^n$

Proof. See [7] for the detailed proof. $\square$

Theorem 5.3.3. *With $I_K(S, T)$ and $C_K(S, T)$ defined as above, one has $N_{L|K}C_L \supseteq C_K(S, T)$ and $[C_K : C_K(S, T)] = [L : K]$. In particular, if $L|K$ is cyclic, then $N_{L|K}C_L = C_K(S, T)$.*

Proof. See [7] for the detailed proof. $\square$

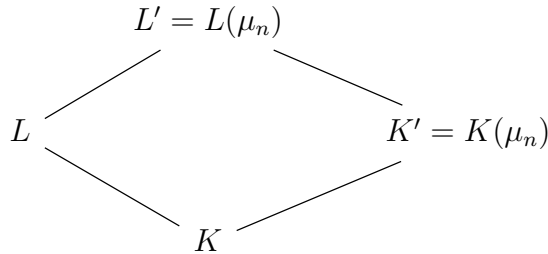
Theorem 5.3.4 (Global class field axiom). *Let $L|K$ be a cyclic extension of number fields.*

$$\text{Then, } \#H^i(G(L|K), C_L) = \begin{cases} [L : K] & i = 0 \\ 1 & i = -1 \end{cases}$$

Proof. Since $[C_K : N_{L|K}C_L] \geq [L : K]$, it is enough to show $[C_K : N_{L|K}C_L] \mid [L : K]$ (so that $[C_K : N_{L|K}C_L] \leq [L : K]$). Let $[L : K] = n$. We will prove that $[C_K : N_{L|K}C_L] \mid n$ by induction on n . Let $M|K$ be a subextension of prime degree p . We consider the exact sequence $C_M/N_{L|M}C_L \xrightarrow{N_{M|K}} C_K/N_{L|K}C_L \rightarrow C_K/N_{M|K}C_M \rightarrow 1$.

If $p < n$, then $\#C_L/N_{L|M}C_L \mid [L : M]$ and $\#C_K/N_{M|K}C_M \mid [M : K]$ by the induction hypothesis, hence $\#C_K/N_{L|K}C_L \mid [L : M][M : K] = [L : M]$.

Let $p = n$. Put $K' = K(\mu_n)$ and $L' = L(\mu_n)$.



$G(L'|K') \rightarrow G(L|K)$, $\sigma \mapsto \sigma|_L$ is injective because if $\sigma \mapsto 1$, then $\sigma|_L = 1$ but since $\mu_n \subseteq K'$ which is fixed by σ , $\sigma = 1$ and isomorphism follows from the fact that $[L : K]$ is prime. Therefore $L'|K'$ is a cyclic Kummer extension, so by Theorem 5.3.3, $\#C_{K'}/N_{L'|K'}C_{L'} = [L' : K'] = p$. Hence it suffices to show that $\#C_K/N_{L|K}C_L \rightarrow C_{K'}/N_{L'|K'}C_{L'}$ induced by the injection $C_L \rightarrow C_{L'}$ is injective.

$C_K/N_{L|K}C_L$ has exponent p , because for $x \in C_K$, $x^p = N_{L|K}C_L$. Note that $d = [K' : K] \mid (p-1)$ since $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$. Note also that $(d, p-1) = 1$. Now since $C_K/N_{L|K}C_L$ has exponent p , $C_L \mapsto C_{L'}$, $x \mapsto x^d$ is an isomorphism. Let $\bar{x} \equiv x \pmod{N_{L|K}C_L}$ belong to the kernel of $C_K/N_{L|K}C_L \rightarrow C_{K'}/N_{L'|K'}C_{L'}$. Writing $\bar{x} = \bar{y}^d$ for some $\bar{y} \in C_K/N_{L|K}C_L$, $\bar{y}$ is also in the kernel of the aforementioned map, i.e., $y = N_{L'|K'}(z')$, $z' \in C_{L'}$. Thus, we get

$$y^d = N_{K'|K}(y) = N_{K'|K}N_{L'|K'}(z') = N_{L'|K}(z') = N_{L|K}N_{L'|L}(z') \in N_{L|K}C_L$$

Hence $\bar{x} = \bar{y}^d = 1$. □

We now see the Hasse norm theorem, which is an instance of local global principle for norms of cyclic extensions:

Theorem 5.3.5 (Hasse norm theorem). *Let $L|K$ be a cyclic extension of number fields. Then, $\alpha \in K^\times$ is a norm if and only if it is a norm everywhere locally, i.e., a norm in $L_\beta|K_\beta$ for all places $\beta|P$.*

Proof. Consider the exact sequence $1 \rightarrow L^\times \rightarrow I_L \rightarrow C_L \rightarrow 1$ and apply Theorem 3.7.1 to obtain the sequence $H^{-1}(G, C_L) \rightarrow H^0(G, L^\times) \rightarrow H^0(G, I_L) \rightarrow H^0(G, C_L)$ and by the global class field axiom (Theorem 5.3.4), $H^{-1}(G, C_L) = 1$, hence $H^0(G, L^\times)$ injects into $H^0(G, I_L)$. Now, $H^0(G, I_L) = \bigoplus_{\mathcal{P}} H^0(G_\beta, L_\beta^\times)$ by Theorem 5.2.9. Thus, we have the required result. □

Remark 5.3.1. *The above theorem does not apply to non-cyclic extensions. An example is the degree four biquadratic extension $\mathbb{Q}(\sqrt{-3}, \sqrt{13})|\mathbb{Q}$. Cf. [5] for the details.*

5.4 Global Reciprocity law

In the previous section, we have shown that the idèle class group satisfies the class field axiom. We now have to determine the appropriate surjective homomorphism d and a Henselian

valuation v satisfying the rules of class field theory. This is the endeavour we turn to in this section.

Proposition 5.4.1. *Let $\Omega|\mathbb{Q}$ be the field obtained by adjoining all roots of unity, and let T be the torsion subgroup of $G(\Omega|K)$. Then the fixed field $\tilde{\mathbb{Q}}|\mathbb{Q}$ of T is a $\hat{\mathbb{Z}}$ extension.*

Proof. Since $\Omega = \bigcup_{n \geq 1} \mathbb{Q}(\mu_n)$, we have

$$G(\Omega|\mathbb{Q}) = \varprojlim_n G(\mathbb{Q}(\mu_n)|\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times$$

But $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ and $\mathbb{Z}_p^\times \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ for $p \neq 2$ and $\mathbb{Z}_2^\times \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ which is by the structure theorem for the unit group (Proposition 1.3.16). Thus, $G(\Omega|\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times \cong \hat{\mathbb{Z}} \times \hat{T}$ where $\hat{T} \cong \prod_{p \neq 2} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $\hat{\mathbb{Z}}$ is torsion free, the torsion subgroup T of $G(\Omega|\mathbb{Q})$ is isomorphic to the torsion subgroup of $\hat{T}$. If $\tilde{\mathbb{Q}}$ is the fixed field of T , this implies $G(\tilde{\mathbb{Q}}|\mathbb{Q}) = G(\Omega|\mathbb{Q})/\bar{T} \cong \hat{\mathbb{Z}}$. $\square$

We fix an isomorphism $G(\tilde{\mathbb{Q}}|\mathbb{Q}) \cong \hat{\mathbb{Z}}$. There is no canonical choice as in the case of local fields, but the reciprocity law does not depend on the choice of isomorphism. By $G(\Omega|\mathbb{Q}) \cong \hat{\mathbb{Z}}$, we obtain a continuous surjective homomorphism $G_{\mathbb{Q}} = G(\overline{\mathbb{Q}}|\mathbb{Q})$. We set $k = \mathbb{Q}$ as our base field, and proceed as in chapter 3. If $K|\mathbb{Q}$ is a finite extension, then set $f_K = [K \cap \tilde{\mathbb{Q}} : \mathbb{Q}]$ which is finite, and thus we obtain the homomorphism $d_K = \frac{1}{f_K} d : G_K \rightarrow \hat{\mathbb{Z}}$, where $\tilde{\mathbb{Q}} = \bigcup_{n \geq 1} \mathbb{Q}(\mu_n)$. This defines the $\hat{\mathbb{Z}}$ extension $\tilde{K} = K\tilde{\mathbb{Q}}$ of K . $\tilde{K}|K$ is called the **cyclotomic $\hat{\mathbb{Z}}$ extension** of K . We now choose as the $G_{\mathbb{Q}} = G(\overline{\mathbb{Q}}|\mathbb{Q})$ module A the union of the idèle class groups C_K of all finite extensions $K|\mathbb{Q}$. The Henselian valuation $v : C_{\mathbb{Q}} \rightarrow \hat{\mathbb{Z}}$ will be defined as the composite

$$C_{\mathbb{Q}} \xrightarrow{[\cdot, \tilde{\mathbb{Q}}|\mathbb{Q}]} G(\tilde{\mathbb{Q}}|\mathbb{Q}) \xrightarrow{d} \hat{\mathbb{Z}}$$

The symbol $[\cdot, \tilde{\mathbb{Q}}|\mathbb{Q}]$ will turn out to be the global norm residue symbol. For now however, we define it as follows: For a finite abelian extension $L|K$, we define the homomorphism $[\cdot, L|K] : I_K \rightarrow G(L|K)$ by $[\alpha, L|K] = \prod_{\mathcal{P}} (\alpha_{\mathcal{P}}, L_{\beta}|K_{\mathcal{P}})$ where β is a chosen place above $\mathcal{P}$, where the product means composition and $(\cdot, L_{\beta}|K_{\mathcal{P}})$ is the local norm residue symbol of $L_{\beta}|K_{\mathcal{P}}$.

Recall that if $L|K$ is abelian, then $L_{\beta}|K_{\mathcal{P}}$ is Galois with Galois group being isomorphic to

the decomposition group $D_{\beta|\mathcal{P}} \subseteq G(L|K)$, hence abelian. The product above makes sense because almost all factors are 1. This follows from Theorem 4.1.3 $L_\beta|K_{\mathcal{P}}$ are unramified for almost all primes $\mathcal{P}$ and almost all $\alpha_{\mathcal{P}}$ are units. Lastly, we may choose a place $\beta|\mathcal{P}$ because if β and γ are two places lying above $\mathcal{P}$, then $L_\beta = L_{\sigma\gamma} = \sigma(L_\gamma)$ but note that σ fixes $\alpha_{\mathcal{P}}$, so $(\alpha_{\mathcal{P}}, L_\beta|K_{\mathcal{P}}) = (\alpha_{\mathcal{P}}, L_\gamma|K_{\mathcal{P}})$.

We now show that v is indeed Henselian.

Proposition 5.4.2. *The map $v_K : G_K \rightarrow \hat{\mathbb{Z}}$ is surjective and a Henselian valuation with respect to d_K .*

Proof. See [7] for details. □

Now applying abstract class field theory, we obtain the **global reciprocity law**.

Theorem 5.4.3 (Global reciprocity law). *Let $L|K$ be a finite Galois extension of number fields. Then we have an isomorphism $r_{L|K} : G(L|K)^{ab} \rightarrow C_K/N_{L|K}C_L$.*

Corollary 5.4.4. *The inverse map of $r_{L|K}$ yields a surjective homomorphism $(\cdot, L|K) : C_K \rightarrow G(L|K)^{ab}$ with kernel $N_{L|K}C_L$.*

Finally we show the global existence theorem.

Theorem 5.4.5 (Global existence theorem). *Let K be a number field and let $\mathcal{N}_L := N_{L|K}C_L$. Then there is a 1-1 correspondence*

$$\{\text{Finite abelian extensions } L \text{ of } K\} \leftrightarrow \{\text{Open subgroups of finite index in } C_K\}$$

$$L \mapsto \mathcal{N}_L$$

Furthermore, $L_1 \subseteq L_2 \iff \mathcal{N}_{L_2} \subseteq \mathcal{N}_{L_1}$, $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \mathcal{N}_{L_2}$ and $\mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$

The field $L|K$ corresponding to the subgroup $\mathcal{N}$ of C_K is called the class field of $\mathcal{N}$. It satisfies $G(L|K) \cong C_K/\mathcal{N}$.

Proof. 1. $\mathcal{N}$ is open in the norm topology: It contains $N_{L|K}C_L$ for some finite Galois extension $L|K$, hence is of finite index in C_K . If we show that $N_{L|K}C_L$ is closed, then it is open since it is of finite index in C_K , so $\mathcal{N}$ is open, hence closed. To show that $N_{L|K}C_L$ is closed, we choose an infinite place $\mathcal{P}$ of K and denote by Γ_K the image of the

subgroup of positive real numbers in $K_{\mathcal{P}}$ under the canonical injection $<>: K_{\mathcal{P}}^{\times} \rightarrow C_K$, $\alpha_{\mathcal{P}} \mapsto (1, 1, \dots, \alpha_{\mathcal{P}}, \dots)$. Then $C_K = C_K^0 \times \mathbb{R}_+^{\times} = C_K^0 \times \Gamma_K$, by Theorem 5.1.4. Therefore

$$N_{L|K}C_L = N_{L|K}C_L^0 \times N_{L|K}\Gamma_K = N_{L|K}C_L^0 \times \Gamma_K^n = N_{L|K}C_L^0 \times \Gamma_K$$

Here $\Gamma_K^n = \Gamma_K$ since $\Gamma_K \cong \mathbb{R}_+^{\times}$ and $x \mapsto x^n$ is an isomorphism of $\mathbb{R}_+^{\times}$. The norm map is continuous and C_L^0 is compact, so $N_{L|K}C_L^0$ is compact in C_K which is Hausdorff, hence is closed. Since Γ_K is also closed in C_K , we get $N_{L|K}C_L^0$ is closed.

2. $\mathcal{N}$ is a closed subgroup of finite index: We have to show that $\mathcal{N}$ contains $N_{L|K}C_L$ for some finite Galois extension L . We may assume that n is a prime power, for if $n = p_1^{r_1} \cdots p_k^{r_k}$ and $\mathcal{N}_i \subseteq C_K$ is the group containing $\mathcal{N}$ of index $p_i^{r_i}$, then $\mathcal{N} = \cap_{i=1}^r \mathcal{N}_i$, and if $\mathcal{N}_i$ are open in the norm topology, then so is $\mathcal{N}$.

So now let $J = p^{-1}(\mathcal{N})$ where p is the canonical surjection $I_K \rightarrow C_K$. Then J is open in I_K because $\mathcal{N}$ is open in C_K . Therefore J contains a group (also a neighbourhood of 1), $U_K^S = \prod_{\mathcal{P} \in S} \{1\} \times \prod_{\mathcal{P} \notin S} U_{\mathcal{P}}$ where S is a sufficiently large set of places of K containing the infinite primes, primes dividing n and such that $I_K = I_K^S K^{\times}$. Since $[I_K : J] = n$, J also contains the group $\prod_{\mathcal{P} \in S} K_{\mathcal{P}}^{\times n} \times \prod_{\mathcal{P} \notin S} \{1\}$, hence the group $I_K^S = \prod_{\mathcal{P} \in S} K_{\mathcal{P}}^{\times n} \times \prod_{\mathcal{P} \notin S} U_{\mathcal{P}}$.

So it is enough to show that $C_K(S) = I_K(S)K^{\times}/K^{\times} \subseteq \mathcal{N}$ contains a norm group. If $\mu_n \subseteq K$, then $C_K(S) = N_{L|K}C_L$ with $L = K(\sqrt[n]{K^S})$. If they do not belong to K , then adjoin them and obtain an extension $K'|K$. Let S' be the set of primes of K' lying above primes in S . If S is chosen sufficiently large, then $I_{K'} = I_{K'}^{S'} K'^{\times}$ and $C_{K'}(S') = N_{L'|K'}C_{L'}$ with $L' = K'(\sqrt[n]{K^{S'}})$. On the other hand, we get $N_{K'|K}(I_{K'}(S')) \subseteq I_K(S)$, so that $N_{L'|K}C_{L'} = N_{K'|K}(N_{L'|K'}C_{L'}) = N_{K'|K}(C_{K'}(S')) \subseteq C_K(S)$. $\square$

Let us now attempt to understand the finite index subgroups of the idèle class group in more detail. Let $\mathcal{M} = \prod_{\mathcal{P} \nmid \infty} \mathcal{P}^{n_{\mathcal{P}}}$. We may write it as $\mathcal{M} = \prod_{\mathcal{P}} \mathcal{P}^{n_{\mathcal{P}}}$ with $n_{\mathcal{P}} = 0$ for the archimedean places $\mathcal{P}$. We will henceforth call $\mathcal{M}$ a module of K . Further, we set $U_{\mathcal{P}}^{(0)} = U_{\mathcal{P}}$ and

$$U_{\mathcal{P}}^{(n_{\mathcal{P}})} := \begin{cases} 1 + \mathcal{P}^{n_{\mathcal{P}}} & \text{if } \mathcal{P} \nmid \infty \\ \mathbb{R}_+^{\times} & \text{if } \mathcal{P} \text{ is real} \\ \mathbb{C}^{\times} & \text{if } \mathcal{P} \text{ is complex} \end{cases}$$

Definition 5.4.1 (Ray class groups). *The group $C_K^m := I_K^{(m)} K^{\times}/K^{\times}$ formed from the idèle group $I_K^m = \prod_{\mathcal{P}} U_{\mathcal{P}}^{(n_{\mathcal{P}})}$ is called the congruence subgroup mod m and the quotient group C_K/C_K^m*

is called the ray class group mod m .

The following proposition gives us examples of ray class groups.

Proposition 5.4.6. *For any module $m = \langle m \rangle$ of the field $\mathbb{Q}$, one has $C_{\mathbb{Q}}/C_{\mathbb{Q}}^m \cong (\mathbb{Z}/m\mathbb{Z})^\times$*

The congruence subgroups in fact provide us with all the finite index closed subgroups of the idèle class group. More precisely, we have

Theorem 5.4.7. *The closed subgroups of finite index of C_K are precisely those subgroups that contain C_K^m .*

Definition 5.4.2 (Ray class field). *The class field corresponding to the congruence subgroup C_K^m is called the ray class group mod m and is denoted K^m .*

Corollary 5.4.8. *The reciprocity map yields the isomorphism $G(K^m|K) \cong C_K/C_K^m$.*

Combining the global existence theorem with Theorem 5.4.7, we obtain the following result:

Corollary 5.4.9. *Every finite abelian extension $L|K$ is contained in a ray class field $K^m|K$.*

The above result is a generalisation of the Kronecker Weber theorem for the following reason.

Theorem 5.4.10. *Let $m \in \mathbb{N}$ and $m = \langle m \rangle$. Then the ray class field mod $\mathbb{Q}$ is the field $\mathbb{Q}^m = \mathbb{Q}(\mu_m)$ of m^{th} roots of unity.*

Definition 5.4.3. *Let $L|K$ be a finite abelian extension, and let $\mathcal{N}_L = N_{L|K}C_L$. The conductor f of $L|K$ is the gcd of all modules m such that $L \subseteq K^m$ (i.e., $C_K^m \subseteq \mathcal{N}_L$).*

The following proposition illustrates the relation between global and local conductors.

Proposition 5.4.11. *If f is the conductor of the abelian extension $L|K$, and $f_{\mathcal{P}}$ is the conductor of the local extension $L_{\mathcal{P}}|K_{\mathcal{P}}$, then $f = \prod_{\mathcal{P}} f_{\mathcal{P}}$.*

Corollary 5.4.12. *Let $L|K$ be a finite abelian extension and f its conductor. Then, $\mathcal{P}$ is ramified in $L \iff \mathcal{P} \mid f$.*

Definition 5.4.4 (Big Hilbert class field). *The big Hilbert class field H is the maximal everywhere unramified abelian extension of a number field K , i.e., $f_{H|K} = 1$.*

Example 22. *The big Hilbert class field of $\mathbb{Q}$ is itself by Minkowski's theorem.*

Definition 5.4.5 (Hilbert class field (Small Hilbert class field)). *The Hilbert class field H is the maximal everywhere unramified abelian extension of a number field K , including at the infinite places (i.e., the real places of K stay real in H).*

Proposition 5.4.13 (Galois group of Hilbert class field). *: The Galois group of the small Hilbert class field $H|K$ is isomorphic to the ideal class group Cl_K , i.e., $G(H|K) \cong Cl_K$. Hence the degree $[H : K]$ is the class number h_K of K .*

Example 23. *The Hilbert class field of any number field with class number 1 (such as $\mathbb{Q}$ and $\mathbb{Q}(i)$) is itself. Notice now that the big Hilbert class field of $\mathbb{Q}(i)$ is also itself, since its Hilbert class field is $\mathbb{Q}(i)$ and both the infinite places are complex. The Hilbert class field of $\mathbb{Q}(\sqrt{-15})$ is $\mathbb{Q}(\sqrt{-3}, \sqrt{5})$.*

Remark 5.4.1. *The Hilbert class field H of K has some special properties:*

1. *The prime ideals of K that split completely in H are precisely the principal prime ideals of K .*
2. *Every ideal I of K becomes a principal ideal in H .*

Chapter 6

Grunwald Wang theorem

The Grunwald Wang theorem is another important instance of local global principle. It states that, except for some exceptional cases which will be described below, an element of a number field K is a global n^{th} power if and only if it is a local n^{th} power in almost all completions K_v .

This theorem has an interesting tale associated with it. It was first proven by Wilhelm Grunwald, a student of Helmut Hasse, in 1933. However, he erroneously stated that a is an n^{th} power in K if and only if a is an n^{th} power in K_v for almost all v . George Whaples gave a second proof of the incorrect statement in 1942. (See remark 6.1.4 to understand Whaples' mistake.) However, Shianghaw Wang discovered a counterexample (see remark 6.1.3, see also [10]), and in his doctoral thesis written under Emil Artin, he stated and proved the correct statement (Theorem 6.1.4). He also expanded upon this in his paper [11].

In this chapter, n will denote a natural number, L, K will denote number fields, K_v a completion of K at a place v and the phrase ‘almost all places’ will refer to ‘all but finitely many places’.

The primary reference for this chapter is Chapter 8 of [6].

6.1 Local Global principle for n th powers

Proposition 6.1.1. *Let $a \in \mathbb{Q}^\times$ be an n^{th} power in $\mathbb{Q}_p$ for all primes p and $\mathbb{R}$. Then $a \in \mathbb{Q}^{\times^n}$.*

Proof. If a is an n^{th} power in $\mathbb{Q}^\times$, then a is an n^{th} power in $\mathbb{Q}_p$ for all primes p and $\mathbb{R}$, since $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ and $\mathbb{Q} \hookrightarrow \mathbb{R}$.

Now, let $a \in \mathbb{Q}^\times$. Then, $a = \pm \prod_p p^{v_p(a)}$, where $v_p(a) \in \mathbb{Z}$ and $v_p(a) = 0$ for almost all p . Since a is an n^{th} power in $\mathbb{Q}_p$ for all primes p , $v_p(a)$ is divisible by n . Now, if $a = \prod_p p^{v_p(a)}$, or if n is odd and $a = -\prod_p p^{v_p(a)}$, then a is an n^{th} power in $\mathbb{Q}$, since in the latter case, $-1 = (-1)^n$. If n is even, then $a > 0$ since a is an n^{th} power in $\mathbb{R}$, hence $a = \prod_p p^{v_p(a)}$ with n dividing $v_p(a)$, hence $a \in \mathbb{Q}^{\times^n}$. $\square$

Remark 6.1.1. In the above theorem, the phrase ‘all primes’ cannot be replaced by ‘almost all primes’. For instance, 16 is an 8^{th} power in $\mathbb{R}$ ($(\sqrt{2})^8 = 16$), and is an eighth power in $\mathbb{Q}_p$ for all odd primes p , because $X^8 - 16 = (X^2 - 2)(X^2 + 2)(X^2 + 2X + 2)(X^2 - 2X + 2)$ and 2, -2 or -1 is a square in $\mathbb{F}_p$ (since $(2/p)(-1/p) = (-2/p)$, where (a/b) is the Legendre symbol), hence in $\mathbb{Q}_p$ by Hensel’s lemma. However, none of $\sqrt{2}$, $\sqrt{-2}$ and $1 + i$ (which are roots of $X^2 - 2$, $X^2 + 2$ and $X^2 + 2X + 2$ resp.) are in $\mathbb{Q}_2$.

However, ‘all primes’ can be replaced by ‘almost all primes’ except when $8 \mid n$, as will be illustrated in Theorem [6.1.4](#).

Remark 6.1.2. The above theorem can be easily extended to the case of imaginary quadratic field with class number 1 and $U_K = \{\pm 1\}$ (there are 7 such fields) with the same proof, when n is odd.

Remark 6.1.3. The above theorem cannot be generalised to an arbitrary number field. Let $K = \mathbb{Q}(\sqrt{7})$. 16 is an 8^{th} power in $\mathbb{Q}_v(\sqrt{7})$ for all places lying above odd primes p , since it is an 8^{th} power in $\mathbb{Q}_p$ for all odd primes p . Furthermore, it is an 8^{th} power in the infinite places, which is $\mathbb{R}$. 16 is also an 8^{th} power in $K_{<1+\sqrt{-7}>} = \mathbb{Q}_2(\sqrt{7}) = \mathbb{Q}_2(i)$ since $(1+i)^8 = 16$. ($\mathbb{Q}_2(\sqrt{7}) = \mathbb{Q}_2(i)$ since -7 is a square in $\mathbb{Q}_2$ (because $-7 \equiv 1 \pmod{8}$), and $\sqrt{-7}i = -\sqrt{7}$). However, 16 is not an 8^{th} power in $\mathbb{Q}(\sqrt{7})$, since none of $\sqrt{2}$, $\sqrt{-2}$ or $1 + i$ are in $\mathbb{Q}(\sqrt{7})$.

Proposition 6.1.2. Let a primitive n^{th} root of unity $\zeta_n \in K$. Then, a is an n^{th} power in K if and only if a is an n^{th} power in K_v for almost all places v .

Proof. Let β be an n^{th} root of a in $\overline{\mathbb{Q}}$. Notice the proposition is tantamount to showing $K(\beta) = K$. If a is an n^{th} power in K_v , then the polynomial $X^n - a$ splits into linear factors in $K_v[X]$ since $\zeta_n \in K_v$. By hypothesis, a is an n^{th} power in K_v for almost all v , so $X^n - a$ splits completely in $K_v[X]$. By Proposition [1.3.25](#), almost all v split completely in L . By Proposition [5.2.14](#), $K[\beta] = K$. $\square$

Combining this with the fact that $\mu_2 \subseteq \mathbb{Q}$, we obtain

Corollary 6.1.3. *a is a p -adic square for almost all primes p if and only if a is a square in $\mathbb{Q}$.*

The following theorem relaxes the hypothesis of the existence of a primitive n^{th} root of unity in K in the above theorem. However, as illustrated in Remark [6.1.3](#), the case when $2 \mid n$ must be tackled carefully.

Theorem 6.1.4. *Let K be a number field, $n \in \mathbb{N}$ and $t := v_2(n)$ (maximum power of 2 dividing n). Furthermore, suppose that $K(\zeta_{2^t})|K$ is cyclic. Then, a is an n^{th} power in K if and only if a is an n^{th} power in K_v for almost all v .*

Proof. Step 1: It is enough to show the theorem is true when $n = p^r$.

Proof: We proceed by induction on number of prime divisors of n . Suppose $n = p_1^{r_1} p_2^{r_2}$. Since $(p_1^{r_1}, p_2^{r_2}) = 1$, by Bezout's lemma, $\exists c, d \in \mathbb{Z}$ such that $cp_1^{r_1} + dp_2^{r_2} = 1$. Now, if $a \in K^\times$ is a n^{th} power in K_v , so a is a $p_1^{r_1 \text{th}}$ power in K_v for almost all v , hence a is a $p_1^{r_1 \text{th}}$ power in $K^\times$ by hypothesis, and similarly is a $p_2^{r_2 \text{th}}$ power in $K^\times$. So for some $e, f \in K^\times$, we have

$$a = e^{p_1^{r_1}} = f^{p_2^{r_2}} \implies a = a^{cp_1^{r_1} + dp_2^{r_2}} = f^{nc} e^{nd} = (f^c e^d)^n.$$

Step 2: Claim: Suppose $n = p^r$ (p any prime) and $K(\zeta_n)|K$ is cyclic of prime power degree. Then, a is an n^{th} power in $K^\times$ if and only if a is an n^{th} power in K_v for almost all v .

Proof: Let $K' = K(\zeta_{p^r})$, and let a be an n^{th} power in K_v for almost all v , then $a = \beta^n$ ($\beta \in K'$) by Proposition [6.1.2](#). So $f(X) = \prod_i (X - \beta \zeta^i)$ in $K'[X]$. Let $X^n - a = \prod_i f_i(X)$ where $f_i(X)$ are irreducible over $K[X]$. For each i , choose a root $\beta \zeta_n^{j(i)}$ of $f_i(X)$. Then, $K(\beta_i) \subseteq K'$, so $K(\beta_i)|K$ is cyclic, so in particular $K(\beta_i)|K$ is Galois, so is the splitting field of $f_i(X)$. If a is an n^{th} power in K_v , then at least one of the $f_i(X)$ splits completely in K_v , so v splits completely in $K(\beta_i)$ for that i . So almost all v split completely in some subfield of K' , but we need to show that almost all v split completely in a single $K(\beta_i)$, and then applying proposition [5.2.14](#), $K(\beta_i) = K$, which will conclude the proof.

Since $K'|K$ is cyclic of prime power degree, the sub-fields of K' are totally ordered:

$$K \subseteq K_1 \subseteq K_2 \subseteq \dots K'$$

Let i_0 be the integer such that $K(\beta_{i_0})$ is the smallest field among $K(\beta_i)$. If v splits completely

in $K(\beta_i)$ for some i , then v splits completely in $K(\beta_{i_0})$. So, almost all v split completely in $K(\beta_{i_0})$, concluding the proof.

Step 3: Suppose now that $n = p^r$ (p an odd prime). Then $K(\zeta_{p^r})|K(\zeta_p)$ is cyclic of degree a divisor of p^r , so by step 2, if a is a n^{th} power in $K_{\mathcal{P}}(\zeta_p)$ for almost all $\mathcal{P}$ ($\mathcal{P}|v$), a is an n^{th} power in $K(\zeta_p)$. Let $d = [K(\zeta_p) : K]$. $N(a) = a^d = N(b^{p^r}) = N(b)^{p^r}$, and since $d \mid p-1$ and $(p-1, p) = 1$, a is a $p^{r^{\text{th}}}$ power in $K^{\times}$.

Finally, since $K(\zeta_{2^t})$ is cyclic of order a divisor of 2^{r-1} , the theorem is proved by combining the above 3 steps. $\square$

Remark 6.1.4 (Whaples' mistake). *The key step in the proof is Step 2. G. Whaples, who gave a second 'proof' of Grunwald's 'theorem' committed an error here, by denoting a root of $X^n - a$ by $a^{1/n}$. However, different roots may have different properties, such as the degree of the minimal polynomial.*

Remark 6.1.5. *Notice that the example in Remark [6.1.3](#) does not contradict Theorem [6.1.4](#) since $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ is not cyclic (its Galois group is Klein four group). It also does not contradict Proposition [6.1.2](#) since $\zeta_8 \notin \mathbb{Q}$.*

Remark 6.1.6. *Notice that in the above theorem, it is not necessary to check whether a is an n^{th} power in K_v for the infinite places v , since there are only finitely many infinite places.*

Corollary 6.1.5. *If $8 \nmid n$ (i.e., $v_2(n) = 0, 1$ or 2), then a is an n^{th} power in a number field K if and only if a is an n^{th} power in K_v for almost all places v of K . In particular, the above statement holds when n is odd.*

Proof. If $v_2(n) = t = 0$ or 1 , then $K(\zeta_{2^t}) = K$. If $t = 2$, then $K(\zeta_{2^2}) = K(i)$ is of degree 1 or 2 over K , hence cyclic. $\square$

Chapter 7

Primary units

In this chapter, we will see some instances where information at a particular completion of a global field is sufficient to provide information about the global field, in contrast to the local global principle, where information at all or all but finitely many places is required.

The reference for the first section, especially the behaviour of norm map and n^{th} power maps is [4]. The second section is primarily based on [8]. The main reference for the third section is [3].

7.1 p -primary units and behaviour of norm map

In this section, we will first define the notion of a p -primary unit and provide an important characterisation of the same. We then describe the behaviour of the norm map and the n^{th} power maps, which will be used in the rest of the chapter.

Definition 7.1.1 (p -primary units). *Let K be a p -adic field and $\zeta_p \in K$. A unit $\alpha \in U_K$ is said to be p -primary if $K(\sqrt[p]{\alpha})|K$ is unramified.*

Example 24. *Note that $\mu_2 \subseteq \mathbb{Q}_2$, and $\mathbb{Q}_2(\sqrt{5})|\mathbb{Q}_2$ is unramified, hence 5 is a p -primary unit. On the other hand, $-1 \in \mathbb{Q}_2$ is not a p -primary unit since $\mathbb{Q}_2(i)|\mathbb{Q}_2$ is totally ramified. Since $\zeta_p \notin \mathbb{Q}_p$ for any odd prime p , $\mathbb{Q}_p$ has no non-trivial p -primary units (i.e., not a p^{th} power).*

Remark 7.1.1. The condition $\zeta_p \in K$ is required for the extension $K(\sqrt[p]{\alpha})|K$ to be Galois. The polynomial $X^p - \alpha$ has one root in $K(\sqrt[p]{\alpha})$, hence must have all its roots.

Remark 7.1.2. If K is a p -adic field, then $K(\sqrt[p]{\alpha})|K$ is unramified by Lemma 4.1.4 if q is any other prime. Thus, the notion of a ‘ q -primary unit’ would be redundant. This is an important observation which will be used in Section 3.

We will state without proof an important characterisation of p -primary units.

Theorem 7.1.1. Let K be a p -adic field containing a primitive p^{th} root of unity. A unit $\alpha \in U_K$ is p -primary if and only if the image of $\alpha \in K^\times / K^{\times p}$ belongs to $\overline{U}_{p\overline{e}_K} := U_{p\overline{e}_K} / U_{p\overline{e}_K} \cap U^p$ where $\overline{e}_K = e_K / (p - 1)$.

Proof. For the proof of this, see [2]. □

We will now state some results about the behaviour of norm map.

For unramified extensions, we already know from Theorem 4.1.3 that the norm map is surjective at each step of the unit group filtration. The following proposition describes the behaviour of norm map for totally tamely ramified extensions.

Proposition 7.1.2. Let $L|K$ be a totally tamely ramified cyclic extension of degree n with residue fields k_L and k_K . Let $\lambda_{0,L} : U_L \rightarrow k_L^\times$ be the map $u \mapsto u \bmod \mathcal{P}_L$ and $\lambda_{i,L} : U_L^{(i)} \rightarrow k_L$ be the map $1 + \pi_L^i a \mapsto a \bmod \mathcal{P}_L$ where $a \in O_L$ and $\mathcal{P}_L$ is the maximal ideal of O_L . Then the following diagrams commute:

$$\begin{array}{ccc} U_L & \xrightarrow{\lambda_{0,L}} & k_L^\times \\ \downarrow N_{L|K} & & \downarrow \uparrow n \\ U_K & \xrightarrow{\lambda_{0,K}} & k_K^\times \end{array} \quad \begin{array}{ccc} U_L^{(ni)} & \xrightarrow{\lambda_{ni,L}} & k_L \\ \downarrow N_{L|K} & & \downarrow \times \overline{n} \\ U_K^{(i)} & \xrightarrow{\lambda_{i,K}} & k_K \end{array}$$

where $\uparrow p$ is the p^{th} power map and $\times \overline{n}$ is the multiplication map. Moreover $N_{L|K} U_L^{(i)} = N_{L|K} U_L^{(i+1)}$ if $n \nmid i$.

We now look at the behaviour of norm map for wildly ramified extensions.

Proposition 7.1.3. *Let s be the unique ramification break of the totally ramified cyclic extension $L|K$ of degree p where $\text{ch}(k_L) = p$ and let $\lambda_{i,L}$ and $\lambda_{i,K}$ be as described in previous proposition. Then the following diagrams commute:*

$$\begin{array}{ccc}
 U_L^{(i)} & \xrightarrow{\lambda_{i,L}} & k_L \\
 \downarrow N_{L|K} & & \downarrow \uparrow p \\
 U_K^{(i)} & \xrightarrow{\lambda_{i,K}} & k_K
 \end{array} \quad \text{if } 1 \leq i \leq s$$

$$\begin{array}{ccc}
 U_L^{(s)} & \xrightarrow{\lambda_{s,L}} & k_L \\
 \downarrow N_{L|K} & & \downarrow \bar{\theta} \mapsto \bar{\theta}^p - \bar{\eta}^{p-1} \bar{\theta} \\
 U_K^{(i)} & \xrightarrow{\lambda_{s,K}} & k_K
 \end{array}$$

$$\begin{array}{ccc}
 U_L^{(s+pi)} & \xrightarrow{\lambda_{s+pi,L}} & k_L \\
 \downarrow N_{L|K} & & \downarrow \times \bar{\eta}^{p-1} \\
 U_K^{(s+i)} & \xrightarrow{\lambda_{s+i,K}} & k_K
 \end{array} \quad \text{if } i > 0$$

Moreover $N_{L|K}(U_L^{(s+i)}) = N_{L|K}(U_L^{(s+i+1)})$ for $i > 0, p \nmid i$. Here $\theta \in U_K$ is such that $\sigma(\pi_L)/\pi_L = \theta\epsilon$ with $\epsilon \in U_L^{(1)}$, and $\eta \in U_L$ is such that $\sigma(\pi_L)/\pi_L = 1 + \eta\pi_L^s$.

We can capture the behaviour of norm map for any finite Galois extension of local fields by an integer valued function called the Hasse Herbrand function.

Proposition 7.1.4 (Hasse Herbrand function). *Let $L|K$ be a finite Galois extension of local fields and set $N := N_{L|K}$. Then there exists a unique function $h_{L|K} : \mathbb{N} \rightarrow \mathbb{N}$ such that $h(0) = 0$ and*

$$NU_L^{(h(i))} \subseteq U_K^{(i)}, NU_L^{h(i)} \not\subseteq U_K^{(i+1)}, NU_L^{(h(i)+1)} \subseteq U_K^{(i+1)}$$

1. For $L|K$ an unramified extension, $h(i) = i$.
2. For $L|K$ a totally tamely ramified extension, $h(i) = [L : K]i$.
3. If $L|K$ is a totally ramified extension of degree $p = \text{ch}(k_K)$, then
$$h(i) = \begin{cases} i & \text{if } i < s \\ s(1-p) + pi & \text{if } i \geq s \end{cases}$$
3. Tower property: If we have a tower of field extensions $K \subseteq M \subseteq L$, then
$$h_{L|K} = h_{L|M} \circ h_{M|K}.$$

Finally, let us look at some important results regarding the n^{th} power map.

Proposition 7.1.5. *Let K be a local field, k_K its residue field and $(n, \text{ch}(k_K)) = 1$. Then $\uparrow n : U_K^{(i)} \rightarrow U_K^{(i)}$, $x \mapsto x^n$ is an isomorphism.*

We now look at the p^{th} power map where $p = \text{ch}(k_K)$.

Proposition 7.1.6. *The homomorphism $\uparrow p$ maps U_i to U_{pi} for $i \leq \overline{e_K} := e_K/(p-1)$, and U_i to U_{i+e_K} for $i > \overline{e_K}$. For $i > \overline{e_K}$, the p^{th} power map is in fact an isomorphism.*

7.2 Local analogue of Martinet's theorem

We now state a theorem due to J. Martinet which is a generalisation of the well known Stickelberger's criterion concerning the discriminant of a number field.

Theorem 7.2.1 (Martinet). *Let $L|K$ be a quadratic extension of number fields such that the absolute norm of the relative discriminant ideal $\delta_{L|K}$ is odd. If $\mu_{2^m} \subseteq K$ for some $m \geq 2$, then $N_{K|\mathbb{Q}}(\delta_{L|K}) \equiv (1 \pmod{2^{m+1}})$.*

We will state and prove a local analogue of Martinet's theorem, and then show that in the case when $L|K$ has an integral basis, i.e., O_L is a free O_K module, Martinet's theorem can be obtained as a consequence of the local analogue at the prime 2.

Theorem 7.2.2 (Local analogue of Martinet's theorem). *Let K be a finite extension of $\mathbb{Q}_p$ containing a primitive p^m th root of unity where $m \geq 1$. Let α be a p -primary unit of U_K . Then $N_{K|\mathbb{Q}_p}(\alpha) \equiv 1 \pmod{p^{m+1}}$.*

We will first obtain Martinet's theorem as a consequence of the local analogue. The following result shows that the discriminant of an integral basis of an unramified extension $L|K$ is a 2-primary unit. We use this to prove Martinet's result.

Corollary 7.2.3. *Let $K|\mathbb{Q}_2$ be a finite extension such that $\mu_{2^m} \subseteq K$ for some $m \geq 1$. Let $L|K$ be a finite unramified extension and $\{\alpha_1, \dots, \alpha_n\}$ be an integral basis of $L|K$. Then, $\sqrt{d_{L|K}(\alpha_1, \dots, \alpha_n)}$ is 2-primary and $N_{K|\mathbb{Q}_2}(\sqrt{d_{L|K}(\alpha_1, \dots, \alpha_n)}) \equiv 1 \pmod{2^{m+1}}$.*

Proof. $K(\sqrt{d_{L|K}(\alpha_1, \dots, \alpha_n)})$ is a subextension of $L|K$ since $d_{L|K} = \prod_{i < j} (\alpha_i - \alpha_j)$, and thus an unramified extension of K . Hence $d_{L|K}(\alpha_1, \dots, \alpha_n)$ is a 2 primary unit of K , and the congruence follows by Theorem [7.2.2](#). $\square$

Corollary 7.2.4. *Let K be a number field such that $\mu_{2^m} \subseteq K$ where $m \geq 1$. Let $L|K$ be a finite extension, and let $\delta_{L|K}$ be the relative discriminant of $L|K$, and suppose $N_{K|\mathbb{Q}}(\delta_{L|K})$ is odd. Assume $A = \{\alpha_1, \dots, \alpha_n\}$ is an integral basis of $L|K$ such that A forms a $S^{-1}O_K$ basis of $S^{-1}O_L$ where $S = \mathbb{Z} \setminus \langle 2 \rangle$. If $d_{L|K}(A)$ denotes the discriminant, then $N_{K|\mathbb{Q}} \equiv 1 \pmod{2^{m+1}}$.*

Proof. Since the norm of the discriminant ideal is odd, all primes of O_K lying above $\langle 2 \rangle$ are unramified in L . Let $\mathcal{P}$ be a prime lying above 2. Let $\{\mathcal{Q}_j\}_{j=1}^r$ be the prime ideals of O_L lying above $\mathcal{P}$. Choose an integral basis $B_j = \{\beta_{j1}, \beta_{j2}, \dots\}$ of $L_{\mathcal{Q}_j}|K_{\mathcal{P}}$ and let $L_j := L_{\mathcal{Q}_j}$, and $M := L \otimes_K K_{\mathcal{P}}$. Since $A = \bigoplus L_j$, $C := \cup_{j=1}^r B_j$ forms an integral basis for the $K_{\mathcal{P}}$ algebra A . Here an integral basis of M means an O_K basis of $\bigoplus_j O_{L_j}$. Let $d_{M|K_{\mathcal{P}}}(C)$ denote the discriminant of M with respect to the basis C . A is also an integral basis of M , since it is given that A is an integral basis of $L|K$. Hence, $d_{L|K}(\alpha_{\mathcal{P}}) = d_{M|K_{\mathcal{P}}}(C)u^2$ for some $u \in U_{K_{\mathcal{P}}}$. Since $d_{M|K_{\mathcal{P}}}(C) = \prod_{j=1}^r d_{L_{\mathcal{Q}_j}|K_{\mathcal{P}}}$, by the above corollary and by the fact that A forms an $S^{-1}O_K$ basis of $S^{-1}O_L$ where $S = \mathbb{Z} \setminus \langle 2 \rangle$, we have $N_{K_{\mathcal{P}}|\mathbb{Q}_2} d_{M|K_{\mathcal{P}}}(B) = \prod_{j=1}^r N_{K_{\mathcal{P}}|\mathbb{Q}_2}(d_{L_{\mathcal{Q}_j}|K_{\mathcal{P}}}(B_j)) \equiv 1 \pmod{2^{m+1}}$. As $\mathbb{Q}_2(\zeta_{2^m}) \subseteq K_{\mathcal{P}}$, we have $N_{K_{\mathcal{P}}|\mathbb{Q}_2}(u) \in U_{\mathbb{Q}_2}^{(m)}$ by Theorem [4.2.2](#). Thus $N_{K|\mathbb{Q}_2}(u)^2 \in U_{\mathbb{Q}_2}^{(m+1)}$. Hence, $N_{K_{\mathcal{P}}|\mathbb{Q}_2}(d_{L|K}(A))_{\mathcal{P}} \equiv 1 \pmod{2^{m+1}}$. Thus, we obtain $N_{K|\mathbb{Q}}(d_{L|K}(A)) = \prod_{\mathcal{P}|2} N_{K_{\mathcal{P}}|\mathbb{Q}_2}(d_{L|K}(A)) \equiv 1 \pmod{2^{m+1}}$. $\square$

Now, we will turn our attention towards proving Theorem [7.2.2](#). But first we need the following lemma which says that the norm of a p-primary unit is again a p-primary unit.

Lemma 7.2.5. *Let $L|K$ be an extension of p -adic fields containing ζ_p . Then, $N_{L|K} : L^\times \rightarrow K^\times$ takes a p -primary unit of L to a p -primary unit of K .*

Proof. By theorem 7.1.1, $\alpha = ux^p$ where $u \in U_L^{(p\overline{e}_L)}$, so $N_{L|K}(\alpha) = N_{L|K}(u)(N_{L|K}(x))^p$. Now $N_{L|K}(u) = N_{L|K}(1 + \pi_L^{p\overline{e}_K}) = \prod_{\sigma}(1 + \sigma(\pi_L)^{p\overline{e}_L}) = 1 + \text{Tr}(\pi_L^{p\overline{e}_L}) + \text{terms with valuation } v_L \text{ greater than } p\overline{e}_L + 1$. Noting that $e_L = e_{L|K}e_K$, we obtain $N(u) \in U_{p\overline{e}_K}$.

For an alternative proof, cf. [8]. □

Proof of theorem 7.2.2. By hypothesis, $\mu_{p^m} \subseteq K$, so $\mathbb{Q}_p(\zeta_{p^m}) \subseteq K$. By the previous lemma, $N_{K|\mathbb{Q}_p(\zeta_{p^m})}$ of a p -primary unit in K is a p -primary unit in $\mathbb{Q}_p(\zeta_{p^m})$. Thus, it is enough to prove the result in the case $K = \mathbb{Q}_p(\zeta_{p^m})$.

Suppose $K = \mathbb{Q}_p(\zeta_{p^m})$. If $\alpha \in K$ is p -primary, then $\alpha = uw^p$, $u \in U_K^{(p\overline{e}_K)} = U_K^{(p^m)}$. By theorem 4.2.2, we have $N_{K|\mathbb{Q}_p}(U_K^{(p^m)}) = U_{\mathbb{Q}_p}^{(m)}$, hence $N_{K|\mathbb{Q}_p}(u)$ and $N_{K|\mathbb{Q}_p}(w) \in U_{\mathbb{Q}_p}^{(m)}$, hence $N_{K|\mathbb{Q}_p}(w)^p \in U_{\mathbb{Q}_p}^{(m+1)}$. So it remains to show that $h_{K|\mathbb{Q}_p}(m) = p^{m-1}$. Then, by using the property of Hasse Herbrand function, we obtain $N_{K|\mathbb{Q}_p}(U_K^{(h(m)+1)}) = N_{K|\mathbb{Q}_p}(U_K^{(p^m)}) \subseteq U_{\mathbb{Q}_p}^{(m+1)}$. Consider the tower of extensions $K = K_m \supseteq K_{m-1} \supseteq \cdots K_1$ where $K_i = \mathbb{Q}_p(\zeta_{p^i})$. For each $2 \leq i \leq m$, $K_i|K_{i-1}$ is a wildly ramified cyclic extension of degree p , and $K_1|\mathbb{Q}_p$ is tamely ramified of degree $p-1$. Observe the ramification breaks $s_{K_i|K_{i-1}} = p^{i-1}$ since $v_{K_i}(\sigma(\zeta_{p^i}) - \zeta_{p^i}) = v_{K_i}(\zeta_p - 1) = p^{i-1}$.

We now proceed by induction on m . For $m = 1$, we want to show $h_{K_1|\mathbb{Q}_p}(1) = p-1$, which follows by the property of Herbrand function for tamely ramified extensions. For $m \geq 2$, we need to show that $h_{K_m|\mathbb{Q}_p}(m) = p^{m-1}$, which can be shown using the transitivity of Hasse Herbrand function through the tower of field extensions K_i .

For the detailed calculation, see [8]. □

7.3 Kummer's lemma

In this section, we will see that Kummer's lemma which is a statement about the units of the ring of integers of $\mathbb{Q}(\zeta_p)$, p a prime, is essentially a statement about p -primary units.

Theorem 7.3.1 (Kummer's lemma). *Let p be a regular prime, i.e., $(p, \text{Cl}_K) = 1$. Let $a \in \mathbb{Z}$, $u \in U_K$ and $u \equiv a \pmod{p}$. Then, u is a p^{th} power, i.e., $u = x^p$, $x \in U_K$. Here, Cl_K denotes the class number of K .*

Remark 7.3.1. 2 and 3 are regular primes since $Cl_{\mathbb{Q}} = Cl_{\mathbb{Q}(\omega)} = 1$. It can be shown in fact that the first irregular prime is 37. It is known that there are infinitely many irregular primes, but it is not known whether there are infinitely many regular primes, though they seem far more numerous compared to irregular primes.

To see that Kummer's lemma is indeed a local statement, we first define the notion of a primaire unit.

Definition 7.3.1 (Primaire unit). Let $L = \mathbb{Q}_p(\zeta_p)$. Then, $u \in U_L$ is said to be a primaire unit if $u \equiv a \pmod{p}$.

Example 25. All p -primary units are primaire units by Theorem [7.1.1](#). It is easy to see that $1 + p$ is primaire but not p -primary.

Remark 7.3.2. Observe that Kummer's lemma is a statement about a global primaire unit.

First we provide a characterisation of primaire units.

Proposition 7.3.2. Let $L = \mathbb{Q}_p(\zeta_p)$ and $u \in U_L$. Then $u \equiv a \pmod{p} \iff u^{p-1} \in U_L^{(p-1)}$.

Proof. ($\implies$) Follows by Fermat's little theorem.

($\impliedby$) Since $L|\mathbb{Q}_p$ is totally ramified, $U_L = \mathbb{F}_p^\times \times U_L^{(1)}$, i.e., $u = au_1$, $a \in \mathbb{F}_p^\times$ and $u_1 \in U_L^{(p-1)}$. So $u^{p-1} = a^{p-1}u_1^{p-1} = u_1^{p-1} \in U_L^{(p-1)}$, and since $\uparrow(p-1)$ is an automorphism of $U_L^{(i)}$ for all $i \geq 1$, we have $u_1 \in U_L^{(p-1)}$. $\square$

Proposition 7.3.3. Let $L = \mathbb{Q}_p(\zeta_p)$. If norm of a primaire unit is $\equiv 1 \pmod{p\pi_L}$ where π_L is a prime of L , then α is p -primary.

Proof. First note that α is p -primary if and only if α^{p-1} is, since $K(\sqrt[p]{\alpha}) = K(\sqrt[p]{\alpha^{p-1}})$, so we may replace α by α^{p-1} . We may thus assume that $\alpha \in U_K^{(p-1)}$. $N_{K|\mathbb{Q}_p}(\alpha) \equiv 1 \pmod{p\pi}$ but since $N_{K|\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p$, we must have $N_{K|\mathbb{Q}_p}(\alpha) \in U_{\mathbb{Q}_p}^{(2)}$. By Proposition [7.1.2](#), $\lambda_{1,\mathbb{Q}_p}(N_{L|\mathbb{Q}_p}(\alpha)) = 0 = \lambda_{p-1,L}(\alpha)$ which implies that $\alpha \in U_L^{(p)}$. $\square$

In the following proposition, we show that any primaire global unit is primary and in fact a local p^{th} power.

Proposition 7.3.4. *Let $K = \mathbb{Q}(\zeta_p)$ and $L = \mathbb{Q}_p(\zeta_p)$. If a global unit $u \in \mathbb{Z}[\zeta]^\times$ is such that the p -adic image u_p of u in $\mathbb{Q}_p(\zeta_p)$ is primaire, then it is a p^{th} power in U_L .*

Proof. 1. Primaire global unit is p -primary: First we recall a few facts about global units. Every unit $u \in \mathbb{Z}[\zeta]^\times$ can be written uniquely as $u = \zeta_p w$ for some primitive p^{th} root of unity ζ_p and $w \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. If furthermore $u_p \equiv a \pmod{\pi_L^2}$ for some $a \in \mathbb{Z}$, then $u = w$ since $\zeta_p \in U_L^{(1)}$ but not in $U_L^{(2)}$ (because $v_L(\zeta_p - 1) = v_{\mathbb{Q}_p}(N_{L|\mathbb{Q}_p}(\zeta_p - 1)) = v_{\mathbb{Q}_p}(p) = 1$). Therefore $N_{K|\mathbb{Q}}(u) = N_{\mathbb{Q}(\zeta_p + \zeta_p^{-1})|\mathbb{Q}}(u)^2 = 1$, because the norm of a unit is a unit and $\mathbb{Z}^{\times 2} = \{1\}$. Also, $N_{L|\mathbb{Q}_p}(u_p) = N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(u) = 1$. Since u is primaire, $u_p \equiv a \pmod{\pi_L^2}$, so applying the previous proposition and noting that $N_{L|\mathbb{Q}_p}(u_p) = 1 \in U_L^{(p)}$, we obtain the fact that u is p -primary.

2. p -primary global unit is a p^{th} power: We now wish to show that u_p is in fact a p^{th} power. Upto replacing u by u^{p-1} , we may assume $u \in U_L^{(1)}$. If $u \in U_L^{(1)}$ is p -primary, then $u \in U_L^{(p)}$ by Theorem 7.1.1. By the above discussion, $u \in \mathbb{Q}_p(\zeta_p + \zeta_p^{-1})$. If a unit of $\mathbb{Q}_p(\zeta_p + \zeta_p^{-1})$ is in $U_L^{(n)}$ for some odd n , then it is in $U_L^{(n+1)}$, because the ramification index of $\mathbb{Q}_p(\zeta_p + \zeta_p^{-1})$ is two. But $U^{(p+1)} = (U^{(2)})^p$, so $u \in L^{\times p}$. $\square$

Remark 7.3.3. *The above proof shows that the local analogue of Martinet's theorem (Theorem 7.2.2) can be strengthened for a global unit u , since $N_{K|\mathbb{Q}_p}(u_p) = 1$ for any local field K containing a primitive p^{th} root of unity.*

Finally, we prove Kummer's lemma.

Proof of Kummer's lemma. Since a global primaire unit is p -primary, $\mathbb{Q}_p(\zeta_p, \sqrt[p]{u_p})|\mathbb{Q}_p(\zeta_p)$ is unramified. By combining this observation with Remark 7.1.2 and noting that all infinite places of $\mathbb{Q}(\zeta)$ are complex, we obtain the fact that the extension $\mathbb{Q}(\zeta_p, u)|\mathbb{Q}(\zeta)$ is unramified everywhere and cyclic of degree 1 or p . Since $(p, \text{Cl}_{\mathbb{Q}(\zeta)}) = 1$, $\mathbb{Q}(\zeta_p)$ has no everywhere unramified degree p extensions, $\mathbb{Q}(\zeta_p, \sqrt[p]{u}) = \mathbb{Q}(\zeta_p)$, so u is a global p^{th} power. $\square$

Chapter 8

Conclusion

The primary aim of this thesis was to present the main theorems of class field theory, and in the process illustrate the phenomenon of local global principle at play. We began by looking at the existence of a canonical homomorphism from the Galois group $G(L|K)$ of a local field extension $L|K$ to $K^\times/N_{L|K}L^\times$, which is in fact an isomorphism for abelian extensions. We then showed that for every finite index subgroup of the multiplicative group $K^\times$, there is a finite abelian extension of K corresponding to it. We then studied the groups of norms of cyclotomic extensions, and as a result obtained the Local Kronecker Weber theorem, and consequently the Global Kronecker Weber theorem, which demonstrated to us the power of local global principle.

In a beautiful parallel to the local theory, the main statements of global class field theory stay the same when the multiplicative group of the local field is replaced by the idèle class group C_K of a number field K . We again saw here various occurrences of the local global principle. We in fact used the local norm residue symbols at all the completions of the number field to construct the global norm residue symbol and the reciprocity map. In the process, we obtained the important Hasse norm theorem, which is essentially a local global principle for norms of a cyclic extension. We also explored the local global principle for n^{th} powers, the so called Grunwald Wang theorem.

We concluded the thesis with two instances which were seemingly global statements, but in fact turned out to be statements at a particular completion, hence not instances of local global principle.

Bibliography

- [1] Conrad, Keith. *The local-global principle*. URL: <https://kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf>.
- [2] Dalawat, Chandan Singh. *Local discriminants, Kummerian extensions, and elliptic curves*. In: *J. Ramanujan Math. Soc.* 25.1 (2010), pp. 25–80.
- [3] Dalawat, Chandan Singh. *Primary units in cyclotomic fields*. In: *Ann. Sci. Math. Québec* 36.1 (2012), pp. 93–98.
- [4] Fesenko, Ivan B and Vostokov, Sergei V. *Local fields and their extensions*. Vol. 121. American Mathematical Soc., 2002.
- [5] Keune, Merlijn. *The Hasse Norm Principle and Biquadratic Fields*. 2021. URL: <https://www.math.ru.nl/~bosma/Students/MerlijnKeuneMSc.pdf>.
- [6] Milne, James S. *Class field theory*. 2011. URL: <https://www.jmilne.org/math/CourseNotes/CFT.pdf>.
- [7] Neukirch, Jürgen. *Algebraic number theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571.
- [8] Pisolkar, Supriya. *Absolute norms of p -primary units*. In: *J. Théor. Nombres Bordeaux* 21.3 (2009), pp. 733–740.
- [9] Serre, Jean-Pierre. *Local fields*. Vol. 67. Springer Science & Business Media, 2013.
- [10] Wang, Shianghaw. *A counter-example to Grunwald’s theorem*. In: *Ann. of Math. (2)* 49 (1948), pp. 1008–1009.
- [11] Wang, Shianghaw. *On Grunwald’s theorem*. In: *Ann. of Math. (2)* 51 (1950), pp. 471–484.