Imperial College London

Department of Mathematics

Class Field Theory and Reciprocity Laws

Name	CID
Yufan Zhao	01494528

Supervisor: Dr. David Helm

Date: June 14, 2022

Declaration

This is my own work except where otherwise stated. I declare that this report is entirely my own work and does not involve plagiarism or collusion. All sources have been fully acknowledged and appropriately referenced.

Yufan Zhao
Date: June 14, 2022

Abstract

This paper studies reciprocity laws. We study the question "Given two odd primes p and q, when is p an n^{th} power residue modulo q?" In this paper, we will make use of Class Field Theory and Hilbert Symbols to study this question. In section 2, We begin with the familiar quadratic reciprocity law and a simple definition of the Hilbert Symbol in the quadratic case. Then, we introduce global Class Field Theory in section 3, and in particular we will use it to give another proof for quadratic reciprocity. Next, in sections 4 and 5, we give a brief overview of local fields and galois theory for infinite extensions. Both of these are crucial to understanding Local Class Field Theory, which will be discussed in section 6. In section 7, we will define the Hilbert Symbol, which makes extensive use of the tools in Local Class Field Theory. Finally in section 8, we put all of these together to prove some higher reciprocity laws, including cubic and eisenstein reciprocity.

Contents

1 Introduction

1.1 Introduction

The law of quadratic reciprocity was first proven in 1801 by Gauss, and there have been many developments since then. In 1900, Hilbert published the famous 23 problems, of which the 9^{th} was to find the most general law of the quadratic reciprocity theorem in any algebraic number field, and the 12^{th} was to generalise the Kronecker-Weber Theorem. Progress has been made in the last two centuries by various great mathematicians such as Leopold Kronecker, David Hilbert, Teiji Takagi, Emil Artin, Helmut Hasse, Claude Chevalley and many more. In particular, Emil Artin established the Artin Reciprocity Law, an important theorem relating fractional ideals to Galois groups. This paper relies heavily on the contributions of the aforementioned great mathematicians. In this paper, we use Class Field Theory to give a more conceptual proof of some higher reciprocity laws, including the well known quadratic reciprocity and (not as well known) cubic reciprocity.

Class Field Theory is a fundamental branch of algebraic number theory that describes Abelian Galois extensions of local and global fields in terms of the arithmetic of the ground field itself. Three themes in number theory at the end of the 19^{th} century converged to become Class Field Theory: relations between abelian extensions and ideal class groups, density theorems for primes (and L-functions), and reciprocity laws. This paper explores the last of these three themes.

We now give a brief history of the development of Class Field Theory, with information drawn from [2]. We begin with the works of Leopold Kronecker. In 1853, Kronecker announced what is now known as the Kronecker-Weber Theorem. It says that any Abelian extension of $\mathbb{Q}$ is contained in some larger cyclotomic extension $\mathbb{Q}(\zeta_m)$. The first accepted proof (with an error that went unnoticed for about 90 years) was given by Weber in 1886, and the first correct proof was Hilbert's in 1896. Abelian extensions of $\mathbb{Q}(i)$ were constructed by Niels Henrik Abel (1829) with special values of the lemniscatic sine function $sl(z)$ (A function that relates the arc length to the chord length of a lemniscate $(x^2+y^2)^2 = x^2-y^2$). Extending Abel's work, Kronecker was able to generate Abelian extensions of imaginary quadratic fields using special values of elliptic and modular functions. In a letter to Dedekind in 1880, Kronecker described his "Jugendtraum" (dream of youth) as the hope that every finite Abelian extension of an imaginary quadratic field lies in one of the extensions he has found. In addition to the construction of Abelian extensions, Kronecker set off another path to Class Field Theory in an 1880 paper on densities of primes and factorization of polynomials. For a polynomial $f(X) \in \mathbb{Z}[X]$, Kronecker considered he number n_p of roots of $f(X)$ mod p in $\mathbb{F}_p$ as p varies. For example, if $f(X) = X^2 + 1$ then $n_2 = 1$ and $n_p = 0$ or 2 for odd p, depending on p modulo 4, so on average $n_p = 1$.

Kronecker's paper included two influential conjectures on sets of primes. The first of them asked for the density of the set of primes p such that $f(X)$ mod p has a fixed number of roots in $\mathbb{F}_p$, where $f(X) \in \mathbb{Z}[X]$. When the number of roots is deg f then $f(X)$ mod p splits completely, and Kronecker found that density. He was unable to prove the existence of these densities in general, but he conjectured that they exist and described some properties that they should have. The existence of these densities were first established by Ferdinand Georg Frobenius, In his work on this problem, Frobenius introduced (1896) the Frobenius Element of a prime ideal, and conjectured what later became the Chebotarev density theorem. Kronecker's second conjecture was that a Galois extension of $\mathbb{Q}$ is characterized by the set of primes in $\mathbb{Q}$ that split completely in the extension.

This conjecture was proven by M. Bauer in 1903 for Galois extensions of all number fields, not just $\mathbb{Q}$.

We now direct our attention to the contributions of David Hilbert. Hilbert's ideas about Abelian extensions of number fields developed from his careful study of three families of examples: quadratic and cyclotomic extensions of general number fields, and Kummer extensions of cyclotomic fields. One of his goals was to develop reciprocity laws in number fields, building on his conception (1897) of the quadratic reciprocity law over $\mathbb{Q}$ as a product of something now known as Hilbert Symbols $(a, b)_v$ (To be explored in greater detail in sections 2, 7, and 8 of this paper). This new conception is nicer than the original in two aspects: the prime 2 is on the same footing as the other primes, and there are no positivity or relative primality constraints on a and b. Both these constraints are present in the more traditional Legendre Symbol formulation of quadratic reciprocity. There are several new aspects being used in this new version of quadratic reciprocity: emphasis on norms rather than squares, p-adic equations rather than congruences modulo p, and the infinite places (embeddings) on an equal footing with the finite places. Ultimately, all three new ideas will appear in Class Field Theory. Hilbert also conjectured in 1898 about the existence of what is now known as Hilbert Class fields. It says that for each number field K, there is a maximal, unique, finite galois extension L/K such that L/K is unramified at all places, and any other unramified extension of E/K is a subfield of L. Hilbert proved part of this conjecture, and a full proof was given by Furtwängler in 1930 after continued work on it over more than two decades.

Next, we examine the work of Teiji Takagi. Takagi was a Japanese mathematician studied in Germany during 1898-1901, partly with Hilbert in Göttingen. In his 1903 thesis, Takagi proved Kronecker's Jugendtraum for the base field $\mathbb{Q}(i)$ using values of the lemniscatic function, as Kronecker had envisioned. Life was not easy for Takagi. When World War I broke out in 1914, scientific contact between Germany (the only place where algebraic number theory was under serious study at that time) and Japan ceased. There was no one in Japan studying algebraic number theory, so Takagi had no local colleagues who could check his work. Takagi worked in isolation to prove his results. Nevertheless, in his 1920 paper, Takagi proved several important theorems, including (what is now known as) the Takagi Existence Theorem, conductor theorem, and completeness theorem. These are explored in greater detail in section 3 of this paper. At the end of Takagi's paper, he also gave a proof of the Jugendtraum for all imaginary quadratic fields.

We now move on to Emil Artin. With Takagi's Class Field Theory in hand, the next natural step was to search for an analogue for non-abelian Galois extensions. Takagi raised this issue himself when he reported on his work at the 1920 International Congress of Mathematicians (ICM) in Strasbourg, France. Artin placed serious thought into this question. Artin first conjectured his reciprocity law in 1923, but at that time could only prove it in special cases, such as cyclotomic and Kummer extensions. Several years later, Artin read Chebotarev's proof of his density theorem, and from there he obtained ideas to prove his reciprocity law in general in 1927. The Artin Reciprocity Law and its implications are explored in section 3 in this paper. Non-abelian extensions however, continued to elude Artin (and also us, even today).

Finally, we discuss Helmut Hasse and Claude Chevalley. One flaw in Class Field Theory as described so far is the tendency to avoid dealing with ramified primes. Artin maps cannot be extended to ramified prime ideals. However, the version of quadratic reciprocity with Hilbert Symbols uses all places, ramified and unramified. Hasse generalised this symbol to a new one $(\alpha, L/K)_v$: instead of

using a symbol with values that are roots of unity, Hasse's symbol has values in a Galois group. In 1930, Hasse proved a similar product formula for his symbol. Hasse's study of $(\alpha, L/K)_v$ for finite v indicated that it should depend only on the local behaviour of K and L at v (i.e. the completion of K at v and of L at a place lying above v). This approach is much cleaner than the roundabout global definition in terms of the Artin map at an ideal in K that is relatively prime to v. This led Hasse to the discovery of Class Field Theory for local fields. The first version of Local Class Field Theory was worked out by Helmut Hasse and Friedrich Karl Schmidt in 1930 using Global Class Field Theory in an essential manner: an abelian extension of local fields is realized as the completion of an abelian extension of number fields, and the global Artin map for that extension of number fields is used to define a local Artin map. Local Class Field Theory is explored in section 6 of this paper. With Hasse's contributions, a new problem was created. Local Class Field Theory was set up on its own terms, and a remaining task was to derive the theorems of Global Class Field Theory from those of Local Class Field Theory. The new concept that allowed this is the idele group of a number field. This was first defined by Chevalley for the purpose of describing Global Class Field Theory for infinite extensions. Several years later, he also used ideles in a new way to obtain Global Class Field Theory from Local Class Field Theory.

In this paper, we focus on the reciprocity laws in the history of Class Field Theory described above, in roughly the same order. We begin with a proof of quadratic reciprocity using Hilbert Symbols in section 2. In section 3, we explore Global Class Field Theory and its implications. In sections 4 and 5, we give some background material on local fields and Galois theory for infinite extensions that are needed to understand Local Class Field Theory. In section 6, we dive into the topic of Local Class Field theory Finally in sections 7 and 8 we use Local Class Field Theory to define general Hilbert Symbols and use them to prove some higher reciprocity laws, including cubic reciprocity and Eisenstein reciprocity.

1.2 Prerequisites

As this is a paper on algebraic number theory, we will assume that the reader is familiar with the related core concepts covered in a typical undergraduate sequence of courses in algebra, number theory, and point-set topology. Topics include groups, rings, fields, galois theory (finite extension case), quadratic reciprocity, the p-adic numbers $\mathbb{Q}_p$ and $\mathbb{Z}_p$, open sets, closed sets, metrics, and norms. We will also assume familiarity with definitions and constructions in commutative algebra, in particular the concept of various types of rings (Noetherian, Artinian), types of domains (Euclidean, PID, UFD, Integral, Dedekind), types of ideals (prime, primary, maximal, radical, fractional), ideal factorization, and localization.

2 Quadratic Reciprocity

2.1 Quadratic Hilbert Symbol

This section is a gentle introduction to the topic of this paper. We give an elementary definition of the quadratic Hilbert Symbol, and show how it can be used to prove the law of quadratic reciprocity.

Theorem 2.1 (Quadratic Reciprocity)**.** *Let p and q be odd prime numbers. Define the Legendre Symbol as:*

$$\left(\frac{p}{q}\right) = \begin{cases} 1, \text{if } n^2 \equiv p \bmod q \text{ for some integer } n \\ -1 \text{ otherwise} \end{cases}$$

Then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

In this section, we will examine the quadratic reciprocity law, and provide a brief introduction to how some of the new tools we will introduce in future sections can be used to prove it:

Definition 2.2 (Quadratic Hilbert Symbol)**.** *Let k be either the real numbers $\mathbb{R}$ or the p-adic numbers $\mathbb{Q}_p$. Let $a, b \in k*$. We define:*

- $(a, b) = 1$ *if* $z^2 - ax^2 - by^2 = 0$ *has a solution* $(z, x, y) \in k^3, (z, x, y) \neq (0, 0, 0)$
- $(a, b) = -1$ *otherwise.*

It is clear that the value of (a, b) does not change when either a or b is multiplied by squares. Indeed, we can absorb the square into x and y, and a solution (x, y, z) still exist. Thus, the Hilbert Symbol defines a map:

$$k^*/(k^*)^2 \times k^*/(k^*)^2 \longrightarrow \{\pm 1\}$$

Proposition 2.3. *Let $a, b \in k*$, and let $k_b = k\sqrt{b}$. Then:*

$$(a, b) = 1 \iff a \in Nk_b^*$$

where Nk_b^* is the group of elements that are norms in k_b^*.

Proof. If b is the square of an element c, the equation $z^2 - ax^2 - by^2 = 0$ has $(c, 0, 1)$ as a solution, hence $(a, b) = 1$. The proposition is clear in this case, since $k_b = k(\sqrt{b}) = k$ and then $Nk_b^* = k^*$

Suppose now that b is not a square in k^*, so $k_b = k\sqrt{b}$ is quadratic over k. Let β denote a square root of b. Every element $\xi \in k_b$ can be written as $z + \beta y$ with $y, z \in k$, and the norm $N(\xi)$ of ξ is equal to $z^2 - by^2$. If $a \in Nk_b^*$, then there exists $y, z \in k$ such that $a = z^2 - by^2$.
Then, we can set $x = 1$ so that quadratic form $z^2 - ax^2 - by^2$ has a zero $(z, 1, y)$ and we have $(a, b) = 1$.
Conversely, if $(a, b) = 1$, this form has a zero $(z, x, y) \neq (0, 0, 0)$. We have $x \neq 0$, for otherwise b would be a square. From this, we see that a is the norm of $\frac{z}{x} + \beta\frac{y}{x}$. □

Proposition 2.4. *The Hilbert Symbol enjoys the following properties:*

1. $(a,b) = (b,a)$ *and* $(a,c^2) = 1$
2. $(a,-a) = 1$ *and* $(a,1-a) = 1$
3. $(a,b) = 1 \implies (aa',b) = (a',b)$
4. $(a,b) = (a,-ab) = (a,(1-a)b)$

Proof. 1. This is clear because the quadratic form $z^2 - ax^2 - by^2$ is symmetric in x and y. The second part is the preceding proposition.

2. If $b = -a$ the quadratic form $z^2 - ax^2 - by^2 = 0$ has a solution $(0,1,1)$.If $b = 1-a$ the quadratic form $z^2 - ax^2 - by^2 = 0$ has a solution $(1,1,1)$. Thus, $(a,b) = 1$ in both cases.

3. If $(a,b) = 1$ then by the preceding proposition $a \in Nk_b^*$. We then have:

$$a' \in Nk_b^* \iff aa' \in Nk_b^*$$

and apply the preceding proposition again.

4. Follows immediately from the previous 3 parts.

□

Lemma 2.5. *Let $v \in U$ be a p-adic unit. If the equation $z^2 - px^2 - vy^2 = 0$ has a non-trivial solution in $\mathbb{Q}_p$, it has a solution (z,x,y) such that $z,y \in U$ and $x \in \mathbb{Z}_p$.*

Proof. The equation has a primitive solution (z,x,y) because we can always multiply all 3 variables by a suitable power of p. We now show that this solution has the desired property that $z,y \in U$ and $x \in \mathbb{Z}_p$
Suppose that it does not. Then, we would have either $y \equiv 0$ mod p or $z \equiv 0$ (mod p). Since $z^2 - vy^2 \equiv 0$ (mod p) and $v \equiv 0$ (mod p), we would have both $y \equiv 0$ (mod p) and $z \equiv 0$ (mod p), hence $px^2 \equiv 0$ (mod p^2), contradicting (z,x,y) being a primitive solution. □

Theorem 2.6. *1. If $k = \mathbb{R}$, we have $(a,b) = 1$ if a or b is greater than 0, and $(a,b) = -1$ if a, b are both less than 0.*

2. *if $k = \mathbb{Q}_p$, and we write $a = p^\alpha u$,$b = p^\beta v$, where u and v belong to the group U of p-adic units (elements of p-adic norm 1), we have:*

   - $(a,b) = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$ *if* $p \neq 2$
   - $(a,b) = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)}$ *if* $p = 2$

   where

   - $\left(\frac{u}{p}\right)$ *denotes the Legendre Symbol* $\left(\frac{\bar{u}}{p}\right)$ *where* $\bar{u}$ *is the image of* u *by the homomorphism of reduction modulo the uniformizer* p *in* $\mathbb{Q}_p$.
   - $\epsilon(u)$ *denotes the class modulo 2 of* $\frac{u-1}{2}$ *and;*
   - $\omega(u)$ *denotes the class of* $\frac{u^2-1}{8}$ *modulo 2.*

Proof. The case for $k = \mathbb{R}$ is trivial. In this case, $z^2 = ax^2 + by^2$ clearly has no solutions besides $(0, 0, 0)$ a, b are both less than 0. If either a or b is greater than 0 then solutions exist.
For the $\mathbb{Q}_p$ case, we refer to pages 21 and 22 of J.P. Serre's book, A course in Arithmetic. [8]. □

Theorem 2.7. *The Hilbert Symbol is a nondegenerate bilinear form on the $\mathbb{F}_2$-vector space k^*/k^{*2}.*

Proof. Bilinearity is clear. It remains to show non-degeneracy. It suffices to show that, $\forall a \in k*/k^{*2}$, $a \neq e$, $\exists b \in k^*/k^{*2}$ such that $(a, b) = -1$. We can take $a = p$, u, or up with $u \in U$ such that $\left(\frac{u}{p}\right) = -1$, then we choose for b respectively. □

2.2 Proof of Quadratic Reciprocity using Hilbert Symbols

We now work towards proving theorem 2.1: Quadratic Reciprocity.

Theorem 2.8. *Let $a, b \in \mathbb{Q}^*$. We write $(a, b)_p$ (resp. $(a, b)_\infty$) to denote the Hilbert Symbol of their images in $\mathbb{Q}_p$ (resp. $\mathbb{R}$)*
We claim that $(a, b)_v = 1$ for almost all $v \in V$ and:

$$\prod_{v \in V} (a, b)_v = 1$$

("Almost all" means "all except a finite number".)

Proof. [8], a course in arithmetic by J.P. Serre, pages 23-24. □

We can now proof theorem 1: quadratic reciprocity, using the result above:

Proof. The preceding theorem says that the product of the Hilbert Symbol $(p, q)_v$ over all places $v \in V$ is 1. Assume that our primes p and q are positive. We then consider the different cases:

1. $v = \infty$. In this case $(p, q)_v$ because the equation $z^2 - px^2 - qy^2 = 0$ clearly has a solution in $\mathbb{R}$.
2. $v \neq p, q, 2$: Here, $(p, q)_v = 1$. By a result in quadratic forms, the equation $z^2 - px^2 - qy^2 = 0$ always has a solution mod v, for the values of v under consideration in this case.
3. $v = p$. $(p, q)_v = \left(\frac{p}{q}\right)$ by definition.
4. $v = q$. $(p, q)_v = \left(\frac{q}{p}\right)$ by definition.
5. $v = 2$. Theorem 2.6 is equivalent to saying that:

$$(p, q)_2 = (-1)^{(p-1)(q-1)/4}$$

Putting all 5 points above together, we obtain the law of quadratic reciprocity stated in Theorem 2.1.

□

3 Global Class Field Theory

In this section, we will study Global Class Field Theory and its applications. We first begin with some basic but essential definitions from Algebraic Number Theory to set the stage up. Next, we state, without proof, the three main theorems of Class Field Theory: Artin Reciprocity Theorem, Conductor Theorem, and Takagi Existence Theorem. Finally, we will apply these theorems to prove the Kronecker Weber Theorem, existence of Ray Class Fields, and the Hilbert Class Field. These results came before Class Field Theory, and served as a major motivation for its development in the last century. We finish by using the three theorems to provide a second, more conceptual proof to quadratic reciprocity.

3.1 Definitions and setup

Definition 3.1 (Ramification index, inertia degree)**.** *Let K be a number field, and let L be a finite extension of K.*

1. *if $\mathfrak{p}$ is a prime ideal of $\mathscr{O}_K$, then $\mathfrak{p}\mathscr{O}_L$ is an ideal of $\mathscr{O}_L$, and hence has a factorization into prime ideals:*
$$\mathfrak{p}\mathscr{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}...\mathfrak{P}_g^{e_g}$$
*where the $\mathfrak{P}_i$s are the distinct primes of L containing $\mathfrak{p}$. The integer e_i is called the **ramification index** of $\mathfrak{p}$ in $\mathfrak{P}_i$. $\mathfrak{p}$ is said to be **unramified** if all the e_is are 0 or 1. Otherwise it is said to be **ramified**.*

2. *Each prime $\mathfrak{P}_i$ containing $\mathfrak{p}$ also gives a residue field extension $\mathscr{O}_L/\mathfrak{P}_i$ over $\mathscr{O}_K/\mathfrak{p}$, and its degree, written as f_i or $f_{\mathfrak{P}_i|\mathfrak{p}}$, is the **inertial degree** of $\mathfrak{p}$ in $\mathfrak{P}_i$.*

Definition 3.2 (finite and infinite primes, ramification of field extensions)**.** *We need to distinguish between "finite" and "infinite" primes:*

1. *Prime ideals of $\mathscr{O}_K$ are called **finite primes**.*
2. *A **real infinite prime** is an embedding $\sigma : K \longrightarrow \mathbb{R}$.*
3. *A **complex infinite prime** is a pair of complex conjugate embeddings $\sigma, \bar{\sigma} : K \longrightarrow \mathbb{C}$, with $\sigma \neq \bar{\sigma}$*
4. *Given an extension $K \subset L$, an infinite prime σ of K ramifies in L provided that σ is real but it has an extension to L which is complex.*
5. *An extension $K \subset L$ is **unramified** if it is unramified at all primes, finite or infinite.*

Definition 3.3 (Decomposition, Inertia Groups)**.** *Let $K \subset L$ be a Galois extension, and let $\mathfrak{P}$ be a prime ideal of L. Then, the **decomposition group** and **inertia group** of $\mathfrak{P}$ are defined by:*

1. *$D_{\mathfrak{P}} := \{\sigma \in Gal(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$, this is the **decomposition group**.*
2. *$I_{\mathfrak{P}} := \{\sigma \in Gal(L/K) : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}\ \forall \alpha \in \mathscr{O}_L\}$, this is the **inertia group**.*

Lemma 3.4. *Let $K \subset L$ be a Galois extension, and let $\mathfrak{p}$ be a prime of $\mathscr{O}_K$ which is unramified in L. If $\mathfrak{P}$ is a prime of $\mathscr{O}_L$ containing $\mathfrak{p}$, then there is a unique element $\sigma \in Gal(L/K)$ such that for all $\alpha \in \mathscr{O}_L$,*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ mod \ \mathfrak{P}$$

where $N(\mathfrak{p}) = |\mathscr{O}_K/\mathfrak{p}|$ is the norm of $\mathfrak{p}$ in $\mathscr{O}_K$.

Proof. We only provide a brief sketch. For full details, refer to [1], proposition 5.10 on page 91 and lemma 5.19 on page 95.
The main idea is to consider the decomposition and inertia groups of $\mathfrak{P}$, and the extension of residual fields $\mathscr{O}_L/\mathfrak{P}$ over $\mathscr{O}_K/\mathfrak{p}$. This is an extension of finite fields, so the galois group is cyclic, with a canonical generator given by the Frobenius automorphism. Thus, this generator corresponds to a unique element in the decomposition group, and this is the element we seek. For this to work, it is crucial that $\mathfrak{p}$ is unramified so that the inertia group is trivial so that $D_{\mathfrak{P}}$ is also the Galois group of the extension of residual fields. □

Definition 3.5 (Artin Symbol for prime ideals)**.** *The unique element $\sigma \in Gal(L/K)$ in the preceding lemma is called the **Artin Symbol** and is denoted $\left(\frac{(L/K)}{\mathfrak{P}}\right)$, since it depends on the prime $\mathfrak{P}$ of L. Its crucial property is that for any $\alpha \in \mathscr{O}_L$, we have:*

$$\left(\frac{(L/K)}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ \ mod \ \mathfrak{P}$$

where $\mathfrak{p} = \mathfrak{P} \cap \mathscr{O}_K$.

Lemma 3.6. *The Artin Symbol $\left(\frac{(L/K)}{\mathfrak{P}}\right)$ enjoys some further useful properties:*

1. *If $\sigma \in Gal(L/K)$, then:*
$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$$
2. *The order of $\left(\frac{L/K}{\mathfrak{P}}\right)$ is the inertial degree $f_{\mathfrak{P}|\mathfrak{p}}$.*
3. *$\mathfrak{p}$ splits completely in L if and only if $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = 1$*

Proof. 1. This is exercise 5.12 in [1], Cox's book Primes of the form $x^2 + ny^2$. This is a simple transport of structure argument using the fact that σ is a field automorphism. We examine what each of the terms mean.

LHS: $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right)$ is the unique element $\tau \in Gal(L/K)$ such that $\tau(\alpha) \equiv \alpha^{N(\mathfrak{p})}$ mod $\sigma(\mathfrak{P})$, $\forall \alpha \in \mathscr{O}_L$.

RHS: σ is a field automorphism, or a symmetry of the field. We first apply σ^{-1} to the entire field, so now we are looking for the element $\gamma \in Gal(L/K)$ such that $\gamma(\alpha) \equiv \alpha^{N(\mathfrak{p})}$ mod $(\mathfrak{P})$, $\forall \alpha \in \mathscr{O}_L$, and this is defined to be the Artin symbol $\left(\frac{L/K}{(\mathfrak{P})}\right)$. We then apply σ to reverse the change caused by σ^{-1}, and the expression on the RHS must therefore be $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right)$, by thinking about how the prime ideal $\sigma(\mathfrak{P})$ "moves" with the actions of σ and σ^{-1}.

2. Since $\mathfrak{p}$ is unramified, the decomposition group $D_{\mathfrak{P}}$ is isomorphic to the Galois group of the extension of residual fields $\mathscr{O}_K/\mathfrak{p} \subseteq \mathscr{O}_L/\mathfrak{P}$, whose degree is the inertial degree f. By definition, the Artin Symbol maps to a generator of the Galois group, so that the Artin symbol has order f as desired.

3. A basic result is that $\mathfrak{p}$ splits completely in L if and only if $e = f = 1$. Since we are already assuming that $e = 1$, (3) follows immediately from (2).

□

When $K \subset L$ is an Abelian extension, the Artin symbol $\left(\frac{(L/K)}{\mathfrak{P}}\right)$ depends only on the underlying prime $\mathfrak{p} = \mathfrak{P} \cap \mathscr{O}_K$. Let $\mathfrak{P}'$ be another prime ideal containing $\mathfrak{p}$. We have that $\mathfrak{P}' = \sigma(\mathfrak{P})$ for some $\sigma \in Gal(L/K)$. Then, the preceding lemma implies that:

$$\left(\frac{(L/K)}{\mathfrak{P}'}\right) = \left(\frac{(L/K)}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{(L/K)}{\mathfrak{P}}\right)\sigma^{-1} = \left(\frac{(L/K)}{\mathfrak{P}}\right)$$

Since $Gal(L/K)$ is Abelian. Hence, whenever $K \subset L$ is an Abelian extension, we can simply write $\left(\frac{(L/K)}{\mathfrak{p}}\right)$ and there is no ambiguity. We don't have to specify a particular $\mathfrak{P}$ in the factorization of $\mathfrak{p}$.

Definition 3.7 (modulus)**.** *Given a number field K, a modulus in K is a formal product:*

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

over all primes $\mathfrak{p}$, finite or infinite, of K, where the exponents must satisfy:

- $n_{\mathfrak{p}} \geq 0$ *and at most finitely many are nonzero.*
- $n_{\mathfrak{p}} = 0$ *whenever $\mathfrak{p}$ is a complex infinite prime.*
- $n_{\mathfrak{p}} \leq 1$ *whenever $\mathfrak{p}$ is a real infinite prime.*

Definition 3.8 (Notation for some special fractional ideals)**.** *We write:*

1. *$I_K(\mathfrak{m})$ to mean the group of all fractional $\mathscr{O}_K$-ideals relatively prime to $\mathfrak{m}$ (which means relatively prime to $\mathfrak{m}_0$, meaning that we ignore the infinite primes)*

2. *$P_{K,1}(\mathfrak{m})$ to mean the subgroup of $I_K(\mathfrak{m})$ generated by the principal ideals $\alpha\mathscr{O}_K$, where $\alpha \in \mathscr{O}_K$ satisfies:*

$$\alpha \equiv 1 \mod \mathfrak{m}_0$$

$$\sigma(\alpha) > 0 \text{ for every real infinite prime dividing } \mathfrak{m}_\infty$$

We note that $P_{K,1}(\mathfrak{m})$ always has finite index in $I_K(\mathfrak{m})$.

We are working in a dedekind domain where ideals have unique factorization. It is clear that if we have two ideals $\mathfrak{p}$ and $\mathfrak{q}$ that are relatively prime to the modulus $\mathfrak{m}$, then their product $\mathfrak{pq}$ is also relatively prime to $\mathfrak{m}$. A result in algebraic number theory says that any fractional ideal $\mathfrak{a} \in I_K(\mathfrak{m})$ has a prime factorization:

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}, \quad r_i \in \mathbb{Z}$$

If $\mathfrak{a}$ is relatively prime to $\mathfrak{m}$, then so are all the prime factors on the right.

Definition 3.9 (Artin symbol for more general ideals, Artin map)**.** *From the prime factorization above, we can define the Artin symbol for any fractional ideal $\mathfrak{a} \in I_K(\mathfrak{m})$ for some fixed modulus $\mathfrak{m}$ by extending the definition multiplicatively from the prime factors of $\mathfrak{a}$:*

$$\left(\frac{(L/K)}{\mathfrak{a}}\right) = \prod_{i=1}^{r} \left(\frac{(L/K)}{\mathfrak{p}_i}\right)^{r_i}$$

*The Artin symbol thus defines a homomorphism, called the **Artin map**:*

$$\left(\frac{(L/K)}{\bullet}\right) : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

To simplify notation, we will write this as:

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

Or, if we want to refer explicitly to the extension involved, we will write $\Phi_{L/K,\mathfrak{m}}$ instead of $\Phi_{\mathfrak{m}}$.

3.2 The Theorems of Global Class Field Theory

In this subsection, we will state the three main theorems of Global Class Field Theory. We first begin with an important definition:

Definition 3.10 (Congruence Subgroup, generalised ideal class group)**.** *A subgroup $H \subset I_k(\mathfrak{m})$ is called a **congruence subgroup** for $\mathfrak{m}$ if it satisfies:*

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$$

and the quotient:

$$I_K(\mathfrak{m})/H$$

*is called a **generalised ideal class group** for $\mathfrak{m}$.*

Theorem 3.11 (Artin Reciprocity Theorem)**.** *Let $K \subset L$ be an Abelian extension, and let $\mathfrak{m}$ be a modulus divisible by all primes of K, finite or infinite, that ramify in L. Then:*

1. *The Artin map $\Phi_{\mathfrak{m}}$ is surjective.*

2. *If the exponents of the finite primes of* $\mathfrak{m}$ *are sufficiently large, then* $ker(\phi_{\mathfrak{m}})$ *is a congruence subgroup for* $\mathfrak{m}$*, i.e.:*

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$$

and consequently the isomorphism:

$$I_K(\mathfrak{m})/ker(\phi_{\mathfrak{m}}) \longrightarrow Gal(L/K)$$

shows that $Gal(L/K)$ *is a generalised ideal class group for the modulus* $\mathfrak{m}$*.*

Proof. See Janusz's book, Algebraic Number Fields, Chapter 5, Theorems 5.7 and 5.8. [5] □

One difficulty with the Artin Reciprocity Theorem is that the modulus $\mathfrak{m}$ for which $ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup is not unique. Depending on the sizes of $P_{K,1}(\mathfrak{m})$ and $I_K(\mathfrak{m})$ there can be many subgroups H lying between them. In fact, we have the following proposition:

Proposition 3.12. *Let* $K \subset L$ *be an Abelian extension, and let* $\mathfrak{m}$ *be a modulus for which the Artin map* $\Phi_{\mathfrak{m}}$ *is defined. If* $\mathfrak{n}$ *is another modulus and* $\mathfrak{m}|\mathfrak{n}$*, then:*

$$P_{K,1}(\mathfrak{m}) \subset ker(\Phi_{\mathfrak{m}}) \implies P_{K,1}(\mathfrak{n}) \subset ker(\Phi_{\mathfrak{n}})$$

Proof. This is exercise 8.4 in [1], Cox's book Primes of the form x^2+ny^2. We have two Artin maps:

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

$$\Phi_{\mathfrak{n}} : I_K(\mathfrak{n}) \longrightarrow Gal(L/K)$$

Since $\mathfrak{m}|\mathfrak{n}$, all the prime ideal factors of $\mathfrak{m}$ are also prime factors of $\mathfrak{n}$. $P_{K,1}(\mathfrak{m})$ (resp. $P_{K,1}(\mathfrak{n})$) is the subgroup of $I_k(\mathfrak{m})$ (resp.$I_k(\mathfrak{n})$) generated by the principal ideals $\alpha\mathscr{O}_K$ (resp. $\beta\mathscr{O}_K$), where α (resp.β) $\in \mathscr{O}_K$ satisfies α (resp.β) $\equiv 1 \ mod\ \mathfrak{m}_0$.

If $P_{K,1}(\mathfrak{m}) \subset ker(\Phi_{\mathfrak{m}})$ holds, then we are in the situation of part 2 of the Artin Recirocity Theorem. By considering the prime factorization of $\mathfrak{m}$ and $\mathfrak{n}$, we can make the following observations:

1. We must have that $P_{K,1}(\mathfrak{n})$ is a subgroup of $P_{K,1}(\mathfrak{m})$, since by definition $P_{K,1}(\mathfrak{n})$ is generated by principal ideals that satisfy the congruence conditions of $P_{K,1}(\mathfrak{m})$ and possibly more.

2. For the Artin map, an ideal $\mathfrak{a}$ that is relatively prime to $\mathfrak{n}$ is also relatively prime to $\mathfrak{m}$, so $I_K(\mathfrak{n})$ is a subgroup of $I_K(\mathfrak{m})$.

Since the Artin maps $\Phi_{\mathfrak{m}}$ and $\Phi_{\mathfrak{n}}$ are multiplicative extensions of the Artin Symbol on the individual prime factors of $\mathfrak{m}$ and $\mathfrak{n}$, the restriction of $\Phi_{\mathfrak{m}}$ to ideals that are coprime to $\mathfrak{n}$ must be the map $\Phi_{\mathfrak{n}}$. Then, since $P_{K,1}(\mathfrak{m})$ is in the kernel of $\Phi_{\mathfrak{m}}$, we must have $P_{K,1}(\mathfrak{n})$ is in the kernel of $\Phi_{\mathfrak{n}}$ because we have established that $P_{K,1}(\mathfrak{n})$ is a subgroup of $P_{K,1}(\mathfrak{m})$ and $\Phi_{\mathfrak{m}}$ is an extension of $\Phi_{\mathfrak{n}}$. □

The above proposition means that $Gal(L/K)$ is a generalised ideal class group for infinitely many moduli (plural of modulus). However, there is one modulus that is better than all the others:

Theorem 3.13 (Conductor Theorem)**.** *Let* $K \subset L$ *be an Abelian extension. Then, there is a modulus* $\mathfrak{f} = \mathfrak{f}(L/K)$ *such that:*

1. *A prime of* K*, finite or infinite, ramifies in* L *if and only if it divides* $\mathfrak{f}$*.*

2. *Let $\mathfrak{m}$ be a modulus divisible by all primes of K which ramify in L. Then, $ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f}|\mathfrak{m}$.*

The modulus $\mathfrak{f}(L/K)$ is uniquely determined by $K \subset L$ and is called the ***conductor*** *of the extension.*

Proof. See Janusz's book, Algebraic Number Fields, Chapter 5, section 6, and Theorem 12.7. [5] □

The final theorem of Global Class Field Theory is the **Takagi Existence Theorem**, which asserts that every generalised ideal class group is the Galois group of some Abelian extension $K \subset L$:

Theorem 3.14 (Takagi Existence Theorem)**.** *Let $\mathfrak{m}$ be a modulus of K, and let H be a congruence subgroup for $\mathfrak{m}_0$, i.e.:*

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$$

Then, there is a unique Abelian extension L of K, all of whose ramified primes, finite or infinite, divide $\mathfrak{m}$, such that if:

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(L/K)$$

is the Artin map of $K \subset L$, then:

$$H = ker(\Phi_{\mathfrak{m}})$$

Proof. See Janusz's book, Algebraic Number Fields, Chapter 5, Theorem 9.16. [5] □

3.3 Applications of Global Class Field Theory

Corollary 3.15. *Let L and M be Abelian extensions of K. Then, $L \subset M$ if and only if there is a modulus $\mathfrak{m}$, divisible by all primes of K ramified in either L or M, such that:*

$$P_{K,1}(\mathfrak{m}) \subset ker(\Phi_{M/K,\mathfrak{m}}) \subset ker(\Phi_{L/K,\mathfrak{m}})$$

Proof. First, assume that $L \subset M$, and let $r : Gal(M/K) \longrightarrow Gal(M/K)$ be the restriction map. (So the kernel is all the the elements that also fix L). By theorem 3.11 the Artin Reciprocity theorem and proposition 3.12, there is a modulus $\mathfrak{m}$ for which $ker(\Phi_{L/K,\mathfrak{m}})$ and $ker(\Phi_{M/K,\mathfrak{m}})$ are both congruence subgroups for $\mathfrak{m}$. Then, we have that $r \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$, and then $ker(\Phi_{M/K,\mathfrak{m}}) \subset ker(\Phi_{L/K,\mathfrak{m}})$ follows immediately by the same reasoning as proposition 3.12. □

Proposition 3.16. *This proposition is concerned with the Artin map of the cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_m)$, where $\zeta_m = e^{2\pi i/m}$. We will assume that $m > 2$.*

1. *All finite ramified primes of this extension divide m. Hence, the Artin map $\Phi_{m\infty}$ is defined.*
2. *The map*

$$\Phi_{m\infty} : I_{\mathbb{Q}}(m\infty) \longrightarrow Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (Z/mZ)^*$$

   is defined by:

$$\Phi_m\left(\frac{a}{b}\mathbb{Z}\right) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*$$

3. $ker(\Phi_{m\infty}) = P_{\mathbb{Q},1}(m\infty)$

Proof. This is exercise 8.2 in [1], Cox's book Primes of the form $x^2 + ny^2$.

1. The minimal polynomial of ζ_m is the m^{th} cyclotomic polynomial which is separable over $\mathbb{Q}$. Let $f(x)$ be the minimal polynomial of ζ_m. Clearly, $f(x)$ is a factor of $x^m - 1$. Proposition 5.11 in [1], the book Primes of the form $x^2 + ny^2$ by Cox, says that if $\mathfrak{p}$ is a prime ideal in $O_{\mathbb{Q}}$ and $f(x)$ is separable modulo $\mathfrak{p}$, then $\mathfrak{p}$ is unramified in $\mathscr{O}_{\mathbb{Q}(\zeta_m)}$. The prime ideals of $\mathscr{O}_{\mathbb{Q}} = \mathbb{Z}$ are those generated by prime numbers and are of the form (p). By a basic result in the study of fields and separability of polynomials, $f(x)$ is separable mod p iff. f and Df (Derivative of f) are coprime mod p. If $f(x)$ is inseparable mod p, then so is $x^m - 1$. Hence p divides m, and this proves part (1).

2. By a result in Algebraic Number Theory, for any fractional ideal $\mathfrak{a} \in I_{\mathbb{Q}}$ we have a prime factorization:
$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$$
for some prime ideals raised to some integer exponents. It is clear that the inverse of $b\mathbb{Z}$ is $(1/b)\mathbb{Z}$. Hence, the map is as defined above in (2).

3. $I_{\mathbb{Q}}(m\infty)$ is the group of all fractional ideals relatively prime to $\mathfrak{m}_0$ (The finite part of the modulus $\mathfrak{m}$). $P_{\mathbb{Q},1}(m\infty)$ is the subgroup of $I_{\mathbb{Q}}(\mathfrak{m})$ generated by the principal ideals $\alpha\mathscr{O}_k$, where $\alpha \in \mathscr{O}_k$ satisfies:
$$\alpha \equiv 1 \; mod \; \mathfrak{m}_0 \quad and \; \sigma(\alpha) > 0 \; for \; every \; real \; infinite \; prime \; dividing \; \mathfrak{m}_\infty$$
Since $\mathbb{Q}(\zeta_m)$ is not contained in $\mathbb{R}$, we need not worry about the second condition regarding infinite primes. Let $\mathfrak{m}_0 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3...\mathfrak{p}_m$ be the prime factorization of $\mathfrak{m}_0$. Then, $\alpha \equiv 1 \bmod \mathfrak{p}_i$ for each $1 \leq i \leq m$ iff. $\alpha \equiv 1 \bmod \mathfrak{m}_0$, due to the Chinese Remainder Theorem, since the prime factors are coprime. The fractional ideals $(a/b)\mathbb{Z}$ that gets mapped to $1 \in (\mathbb{Z}/m\mathbb{Z})^*$ are those where (a/b) factors and simplifies into $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3...\mathfrak{p}_m = \alpha$. Chinese Remainder Theorem then tells us that α must be congruent to 1 mod $\mathfrak{p}_i$. So $ker(\Phi_m) = P_{\mathbb{Q},1}(m)$.

□

Theorem 3.17 (Kronecker-Weber Theorem)**.** *Let L be an Abelian extension of $\mathbb{Q}$. Then, there is a positive integer m such that $L \subset \mathbb{Q}(\zeta_m)$, where $\zeta_m = e^{2\pi i/m}$ is a primitive m^{th} root of unity.*

Proof. By the Artin Reciprocity Theorem (Theorem 3.11), there is a modulus $\mathfrak{m}$ such that
$$P_{\mathbb{Q},1}(\mathfrak{m}) \subset ker(\Phi_{L/\mathbb{Q},\mathfrak{m}})$$
By Proposition 3.12, we may assume that $\mathfrak{m} = m\infty$. By Proposition 3.16,we know that:
$$P_{\mathbb{Q},1}(\mathfrak{m}) \subset ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) \subset ker(\Phi_{L/K,\mathfrak{m}})$$
Then, $L \subset \mathbb{Q}(\zeta_m)$ follows from corollary before the preceding proposition. □

Definition 3.18 (Ray Class Field)**.** *Given any modulus $\mathfrak{m}$, the existence theorem shows that there is a unique Abelian Extension $K_{\mathfrak{m}}$ such that:*
$$P_{K,1}(\mathfrak{m}) = ker(\Phi_{K_{\mathfrak{m}}/K,\mathfrak{m}})$$
*$K_{\mathfrak{m}}$ is called the **ray class field** for the modulus $\mathfrak{m}$.*

Definition 3.19 (Hilbert Class Field)**.** *The Ray Class Field for* $\mathfrak{m} = 1$ *is also called the* ***Hilbert Class Field of field*** K*.*

Proposition 3.16(3) shows that $\mathbb{Q}(\zeta_m)$ is the ray class field of $\mathbb{Q}$ for the modulus $m\infty$. We also get a nice interpretation of the conductor $\mathfrak{f}(L/K)$ of an arbitrary Abelian Extension L over K: It is the smallest modulus $\mathfrak{m}$ for which L is contained in the ray class field $K_{\mathfrak{m}}$.

3.4 Proof of Quadratic Reciprocity using Global Class Field Theory

Proposition 3.20. *Let* K *be a number field containing a primitive* n^{th} *root of unity* ζ*. Let* $a \in \mathscr{O}_K$*, and let* $\mathfrak{p}$ *be a prime ideal of* $\mathscr{O}_K$ *such that* $na \notin \mathfrak{p}$*. Let* $L = K(\sqrt[n]{a})$*. Clearly,* L *is an Abelian Extension of* K*. Then, we have that:*

1. $\mathfrak{p}$ *is unramified in* L*.*
2. $$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}$$

Proof. This is exercise 5.14 in [1].

1. $x^n - a$ is separable modulo $\mathfrak{p}$ because the characteristic of $\mathscr{O}_K/\mathfrak{p}$ does not divide n, so the derivative of $x^n - a$, which is nx^{n-1}, is non-zero, so $x^n - a$ is separable modulo $\mathfrak{p}$. By proposition 5.11 in [1], this implies that $\mathfrak{p}$ is unramified in L.

2. By definition, the Artin Symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$ is the unique element $\sigma \in Gal(L/K)$ such that $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \mod \mathfrak{p}$. $\left(\frac{a}{\mathfrak{p}}\right)_n$ is defined to be the unique root of unity congruent to $a^{(n(\mathfrak{p})-1)/n}$. Let $\mathfrak{P}$ be a prime ideal of $\mathscr{O}_L$ containing $\mathfrak{p}$. Then, we have:

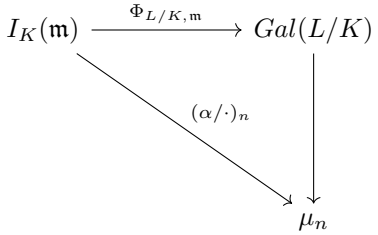
$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{a}) \equiv (\sqrt[n]{a})^{N(\mathfrak{p})} \equiv (\sqrt[n]{a})^{(N(\mathfrak{p})-1)/n} \cdot (\sqrt[n]{a})$$

By definition, $(\sqrt[n]{a})^{(N(\mathfrak{p})-1)/n} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n$, and $\mathfrak{p} \subseteq \mathfrak{P}$. Hence:

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}$$

□

Theorem 3.21 (Weak Reciprocity)**.** *Let* K *be a number field containing a primitive* n^{th} *root of unity* ζ*. Let* $\alpha \in \mathscr{O}_K$ *be non-zero. Let* $L = K(\sqrt[n]{\alpha})$*. Assume that* $\mathfrak{m}$ *is a modulus divisible by all primes of* K *containing* $n\alpha$*, and assume in addition that* $ker(\Phi_{L/K,\mathfrak{m}})$ *is a congruence subgroup for* $\mathfrak{m}$*. Then, there is a commutative diagram:*



where $Gal(L/K) \hookrightarrow \mu_n$ is the natural injection. Thus, if G is the image of $Gal(L/K)$ in μ_n, then the n^{th} power Legendre Symbol $\left(\frac{\alpha}{\mathfrak{a}}\right)_n$ induces a surjective homomorphism:

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n : I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \longrightarrow G \subset \mu_n$$

Proof. From the preceding proposition, we have that:

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}$$

so the diagram commutes. For the second statement, we know that $ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$. Thus, $P_{K,1}(\mathfrak{m}) \subset ker(\Phi_{L/K,\mathfrak{m}}) \subset I_K(\mathfrak{m})$, so that the Artin map $\Phi_{L/K,\mathfrak{m}}$ induces a surjective homomorphism:

$$I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \longrightarrow I_K(\mathfrak{m})/ker(\Phi_{L/K,\mathfrak{m}}) \cong Gal(L/K)$$

Then, from the commutative diagram, the result follows immediately. □

This result is called "Weak Reciprocity" because it does not give formulas to compute $\left(\frac{\alpha}{\mathfrak{a}}\right)_n$. It only asserts that the symbol is a homomorphism on an appropriate group. Nevertheless, it is still strong enough to give another proof quadratic reciprocity. We first need some preliminary results:

Proposition 3.22. *These are some preliminary results needed for the next proof of quadratic reciprocity:*

1. *If $K \subset L$ is an Abelian Extension such that $Gal(L/K)$ is a generalized ideal class group for the modulus $\mathfrak{m}$ of K, then the same is true for any intermediate field $K \subset M \subset L$. (I.e. $Gal(L/M)$ is also a generalized ideal class group.)*
2. *If K is a quadratic field which ramifies only at an odd prime p, then $K = \mathbb{Q}(\sqrt{p^*})$. (Where $p^* = (-1)^{(p-1)/2} \cdot p$)*
3. *The map that sends an integer a relatively prime to p to the ideal $a\mathbb{Z}$ induces an isomorphism $(\mathbb{Z}/p\mathbb{Z})^* \to I_{\mathbb{Q}}(p\infty)/P_{\mathbb{Q},1}(p\infty)$.*

Proof. This is exercise 8.7 in [1].

1. Recall that a congruence subgroup is a subgroup H of $I_K(\mathfrak{m})$ that contains $P_{K,1}(\mathfrak{m})$, i.e.:

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$$

We have a tower of fields $K \subset M \subset L$, and we want to show that there exists a congruence subgroup H' such that $Gal(L/M) \cong I_L(\mathfrak{m})/H'$ for any intermediate field M. By the fundamental theorem of Galois Theory, $Gal(L/M)$ is a subgroup of $Gal(L/K)$. We have the quotient map $I_L(\mathfrak{m}) \longrightarrow Gal(L/K)$ where H is the kernel. The 4th isomorphism theorem says that the subgroups of $Gal(L/K)$ corresponds to subgroups of $I_L(\mathfrak{m})$ that contain H. Applying this to $Gal(L/M)$ we get the subgroup H' must exist, and then our generalized ideal class group is $I_L(\mathfrak{m})/H'$.

2. A result in Algebraic Number Theory (Also corollary 5.17 in [1]) says that if K is a quadratic field of discriminant d, $p \in \mathbb{Z}$ is a prime, then p ramifies in K if and only if p divides d. Hence, we must have that either $K = \mathbb{Q}(\sqrt{p})$ or $K = \mathbb{Q}(\sqrt{-p})$.

   - if $p \equiv 3 \mod 4$, then $\mathbb{Q}(\sqrt{p})$ has discriminant $d = 4p$, so it ramifies at 2 in addition to p. In this case, $-p \equiv 1 \mod 4$, so we must have $K = \mathbb{Q}(\sqrt{-p})$.
   - if $p \equiv 1 \mod 4$, the opposite happens: $\mathbb{Q}(\sqrt{p})$ has discriminant $d = p$, while $\mathbb{Q}(\sqrt{-p})$ has discriminant $d = 4p$. so $K = \mathbb{Q}(\sqrt{-p})$.

   Putting both cases together, we get that $K = \mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2} \cdot p$.

3. a is relatively prime to p, so a has a natural image in $(\mathbb{Z}/p\mathbb{Z})^*$ by reducing mod p. We are working in the field $\mathbb{Q}$ whose ring of integers is $\mathbb{Z}$, so all fractional ideals are principal, and we only need to worry about the $\equiv 1$ condition. Principal ideals multiply by multiplying the generator together, and there are $p-1$ equivalence classes of them, so $I_{\mathbb{Q}}(p\infty)/P_{\mathbb{Q},1}(p\infty)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$. Next, the induced map is mapping a to the ideal generated by a. Since multiplication on both sides is the same as multiplication in the integers, the structure carries over and the induced map is well defined.

□

Theorem 3.23 (Quadratic Reciprocity)**.** *Let p and q be odd prime numbers. Then:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

We rewrite this slightly here. Letting $p^* = (-1)^{(p-1)/2} \cdot p$, we get that:

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

Proof. We first first examine $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p^*})$. By Proposition 3.16(Description of the Artin Map), $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a generalized ideal class group for the modulus $p\infty$, so part 1 of the preceding proposition implies that the Galois group of any subfield of $\mathbb{Q}(\zeta_p)$ is also a generalized ideal class group.

Since $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of order $p-1$, it has a unique subgroup of index 2, and hence, by the Galois correspondence, there is a unique subfield $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_p)$ that is quadratic over $\mathbb{Q}$. Then, $Gal(K/\mathbb{Q})$ is a generalized ideal class group for $p\infty$, which implies that p is the only finite prime of $\mathbb{Q}$ that ramifies in K. If we write $K = \mathbb{Q}(\sqrt{m})$, then part 2 of the preceding proposition says that $K = \mathbb{Q}(\sqrt{p^*})$.

It follows that $ker(\Phi_{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q},p\infty})$ is a congruence subgroup for $p\infty$, and thus by Weak Reciprocity, the Legendre Symbol $\left(\frac{p^*}{\cdot}\right)$ gives a surjective homomorphism:

$$I_{\mathbb{Q}}(p\infty)/P_{\mathbb{Q},1}(p\infty) \longrightarrow \pm 1$$

Part 3 of the preceding proposition says that the map that sends an integer a relatively prime to p to the ideal $a\mathbb{Z}$ induces an isomorphism $(\mathbb{Z}/p\mathbb{Z})^* \to I_{\mathbb{Q}}(p\infty)/P_{\mathbb{Q},1}(p\infty)$. Composing this map with the one above shows that $\left(\frac{p^*}{\cdot}\right)$ induces a surjective homomorphism from $(\mathbb{Z}/p\mathbb{Z})^*$ to ± 1.

But the Legendre Symbol $\left(\frac{\cdot}{p}\right)$ is also a surjective homomorphism between the same two groups, and since $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, there is only one such homomorphism. This proves that:

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

and we are done. □

4 Local Fields

Local Class Field Theory is about Class Field Theory in local fields, as the name suggests. So it is natural that we explore the topic of local fields first. Definitions in Section 4.1 on basic definitions of discrete valuation rings (DVRs) and local fields are mainly drawn from chapter 9 of [6], Introduction to Commutative Algebra by Atiyah and MacDonald. Section 4.2 on extensions of the valuation function and section 4.3 on extensions of fields are drawn from chapters 1 and 2 of [7], Local Fields by J.P. Serre.

4.1 Discrete Valuation Rings and Local Fields

Definition 4.1 (Total order, Ordered Group, Valuation of a field K, Discrete Valuation, Valuation Ring, Discrete Valuation Ring)**.** *We work towards defining a discret valuation ring:*

1. *A **total order** is a binary relation on a set, written as $x < y$, such that for any elements a and b in the set, exactly one of the following holds: $a < b$, $a = b$, $a > b$.*
2. *An **ordered group** is an abelian group with a total order compatible with the group structure. (i.e. $a < b$ implies $a + c < b + c$ for any c.*
3. *Let K be a field. A **valuation** of K is a surjective homomorphism $v : K^* \longrightarrow G$, where G is an ordered group, such that $v(xy) = v(x) + v(y)$ and $v(x \pm y) \geq min\{v(x), v(y)\}$*
4. *A **discrete valuation** of a field K is a valuation where the group G is the integers $\mathbb{Z}$.*
5. *The set $R = \{x \in K^* | v(x) \geq 0\}$ is a ring (by looking at (3) above and thinking about how valuations work). R is called the **valuation ring** of v.*
6. *A valuation ring with the value group $G = \mathbb{Z}$ is called a **discrete valuation ring**, or a DVR.*

Theorem 4.2 (Main Theorem on Discrete Valuation Rings)**.** *Let R be a Noetherian local domain of Krull dimension 1 (local means there is only one maximal ideal), $\mathfrak{m}$ its maximal ideal, $k = R/\mathfrak{m}$ its residue field. Then, the following are equivalent:*

1. *R is a Discrete Valuation Ring.*
2. *R is integrally closed.*
3. *$\mathfrak{m}$ is a principal ideal.*
4. *$dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.*
5. *Every non-zero ideal is a power of $\mathfrak{m}$.*
6. *There exists $\pi \in R$ such that every non-zero ideal is of the form (π^n), $n \geq 0$.*

Proof. [6], proposition 9.2 on page 94. □

Definition 4.3. *Part (6) of the theorem above says that R has one and only one irreducible element π, up to multiplying by units. Such an element π is called the **uniformizing element of** R, or a **uniformizer**. In particular, R is a Principal Ideal Domain.*

Definition 4.4 (Absolute value defined by a valuation)**.** *Let K be a field on which a discrete valuation v is defined, and let A be its valuation ring. If a is any real number between 0 and 1, we define:*

- $\|x\| = a^{v(x)}$ *for* $x \neq 0$
- $\|0\| = 0$

We then have the formulas:

- $\|x \cdot y\| = \|x\| \cdot \|y\|$
- $\|x + y\| \leq sup(\|x\|, \|y\|)$
- $\|x\| = 0$ *if and only if* $x = 0$.

*We say that $\|x\|$ is an **absolute value** on K. The second formula above is called the **ultrametric inequality**. Norms that satisfy the ultrametric inequality are called **non-archimedean**. (In the case of $\mathbb{Q}_p$ and $\mathbb{Z}_p$, we usually set a to be $\frac{1}{p}$.)*

Definition 4.5 (Local Field)**.** *A field K is called a **Local Field** if it is complete (every cauchy sequence converges to an element in K) with respect to a topology induced by a discrete valuation v and its residue field (valuation ring of K quotient by its maximal ideal) is finite.*

Convention: For local fields and their valuation rings, the valuation of a non-zero element x (written as $v(x)$) is usually defined to be the largest power of the maximal ideal (π) that x lies in, where π is the uniformizer. i.e. it is the largest integer $n \in \mathbb{Z}$ such that $x \in (\pi)^n$ (Other definitions are possible by picking subgroups of $\mathbb{Z}$ such as the even integers $2\mathbb{Z}$, but this is the convention we will adopt). $v(0)$ is defined to be 0 (despite always being in $(\pi)^n$ for arbitrarily large n).

4.2 Extensions of a discrete valuation

We now examine extensions of rings and fields, and how valuations can be extended. Recall in section 3 definition 3.1, we defined the concepts of ramification index and inertial degree. We will provide a more complete treatment here as they are essential to understanding how discrete valuations carry over to ring and field extensions. Loosely speaking, an extension of a valuation is a valuation on a bigger field that agrees with the original valuation on the smaller subfield.

Setup for this subsection: Throughout this subsection, we use the following notation and make the following assumption:

1. K is a field and L is a finite extension of K. The degree of the extension $[L : K]$ will be denoted by n.
2. A is a Noetherian integrally closed domain having K as its field of fractions. B is the *integral closure* of A in L (i.e. the set of elements in L that are integral over A). The field of fractions of B is L ([7] , due to the remark after proposition 4 on page 18).
3. We assume that B is a finitely generated A-module. This assumption implies that B is a Noetherian integrally closed domain. In particular, this assumption is always satisfied when L/K is a separable extension ([7] proposition 8, page 21)

Proposition 4.6. *If A is a Dedekind domain, then B is also a Dedekind domain.*

Proof. Due to (3) in our setup above, we know that B is Noetherian and integrally closed. By definition, a dedekind domain is an integrally closed Noetherian domain with Krull dimension one, so it remains to show the Krull dimension one part. Suppose otherwise. Let $\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \mathfrak{P}_2$ be a chain of distinct prime ideals in B. The next claim will show that the $\mathfrak{P}_0 \cap A$ are distinct, thus forming a chain of distinct ascending prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2$ in A, contradicting A being Dedekind:

Claim: Let $A \subset B$ be rings, with B integral over A. If $\mathfrak{P} \subset \mathfrak{Q}$ are prime ideals of B such that $\mathfrak{P} \cap A = \mathfrak{Q} \cap A$, then $\mathfrak{P} = \mathfrak{Q}$.

Proof of claim: Passing to the quotient by $\mathfrak{P}$, we may assume that $\mathfrak{P} = 0$. If $\mathfrak{Q} \neq \mathfrak{P}$, then there is a non-zero $x \in \mathfrak{Q}$. Let:

$$x^n + a_{n-1}x^{n-1} + ... + a_0 = 0 \ , \quad a_i \in A$$

be its minimal polynomial over A. We have that $a_0 \neq 0$, and a_0 belongs to the ideal of B generated by x, therefore it belongs to $\mathfrak{Q} \cap A = \mathfrak{P} \cap A$, which is absurd. This proves the claim.
This also proves the proposition. □

From this point on, we also assume that the statement of proposition 4.5 holds, i.e. A and B are Dedekind domains each time they are introduced.

Lemma 4.7 (Approximation lemma)**.** *Let k be a positive integer. For every i, $1 \leq i \leq k$, let $\mathfrak{p}_i$ be distinct prime ideals of A, x_i elements of a field K, and let n_i be integers. Then, there exists an $x \in K$ such that $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ for all i, and $v_{\mathfrak{q}}(x) \geq 0$ for $\mathfrak{q} \neq \mathfrak{p}_1, ..., \mathfrak{p}_k$.*

Proof. [7], Local fields by J.P. Serre, page 12 approximation lemma. □

Definition 4.8. *We now introduce some core definitions crucial to studying field extensions and the corresponding extensions of their ring of integers:*

1. *If $\mathfrak{P}$ is a non-zero prime ideal of B, and if $\mathfrak{p} = \mathfrak{P} \cap A$, we say that $\mathfrak{P}$ **divides** $\mathfrak{p}$, (or that $\mathfrak{P}$ is **'lying above'** $\mathfrak{p}$). This relation is also equivalent to saying that $\mathfrak{P}$ contains the ideal $\mathfrak{p}B$ generated by $\mathfrak{p}$. We will write $\mathfrak{P}|\mathfrak{p}$.*

2. *We have a factorization of $\mathfrak{p}B$ into prime ideals. Denote by $e_{\mathfrak{P}}$ the exponent of $\mathfrak{P}$ in the decomposition:*

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{P}} \mathfrak{P}^{e_{\mathfrak{P}}}$$

   *the integer $e_{\mathfrak{P}}$ is called the **ramification index** of $\mathfrak{P}$ in the extension L/K.*

3. *We also have that $e_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathfrak{p}B)$. This comes from observing how valuations work. the valuation of a non-zero element x under $\mathfrak{P}$ (written as $v_{\mathfrak{P}}(x)$) is taken to be the largest power of $\mathfrak{P}$ that x lies in. Since in the factorization of $\mathfrak{p}B$ there are $e_{\mathfrak{P}}$ copies of $\mathfrak{P}$, if an element x lies in $\mathfrak{p}^n$ for some n then it must lie in $\mathfrak{P}^{n \cdot e_{\mathfrak{P}}}$, and hence we get our formula.*

4. *If $\mathfrak{P}$ divides $\mathfrak{p}$, the field $B/\mathfrak{P}$ is an extension of the field $A/\mathfrak{p}$. As B is finitely generated over A, $B/\mathfrak{P}$ is an extension of $A/\mathfrak{p}$ of finite degree. The degree of this extension is called the **residue degree** of $B/\mathfrak{P}$ in the extension L/K, and is denoted $f_{\mathfrak{P}}$. Thus:*

$$f_{\mathfrak{P}} = [B/\mathfrak{P} : A/\mathfrak{p}]$$

5. *If there is only one prime ideal $\mathfrak{P}$ which divides $\mathfrak{p}$ and $f_{\mathfrak{P}} = 1$, we say that L/K is* ***totally ramified*** *at $f_{\mathfrak{p}}$.*

6. *If $e_{\mathfrak{P}} = 1$ and $B/\mathfrak{P}$ is separable over $A/\mathfrak{p}$, we say that L/K is* ***unramified at*** *$\mathfrak{P}$.*

7. *If L/K is unramified for all prime ideals $f_{\mathfrak{P}}$ dividing $\mathfrak{p}$, we say that L/K is* ***unramified at*** *$\mathfrak{p}$ (or above $\mathfrak{p}$).*

Proposition 4.9. *Let $\mathfrak{p}$ be a non-zero prime ideal of A. The ring $B/\mathfrak{p}B$ is an $A/\mathfrak{p}$-algebra of degree $n = [L : K]$, isomorphic to the product $\prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$. We have the formula:*

$$n = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$$

Proof. Let S be the multiplicative set $A\backslash\mathfrak{p}$, $A' = S^{-1}A$, and $B' = S^{-1}B$. The ring $A' = A_{\mathfrak{p}}$ is a discrete valuation ring, and B' is its integral closure in L. We have that $A'/\mathfrak{p}A' = A'/\mathfrak{p}$, and then we see that $B'/\mathfrak{p}B' = B/\mathfrak{p}B$. As A' is principal, B' is a free module of rank $n = [L : K]$, and $B'/\mathfrak{p}B'$ is free of rank n over $A'/\mathfrak{p}A'$. Thus, $B/\mathfrak{p}B$ is an algebra of degree n.

Since $\mathfrak{p}B = \bigcap \mathfrak{P}^{e_{\mathfrak{P}}}$, the canonical map:

$$B/\mathfrak{p}B \longrightarrow \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$$

is injective. By lemma 4.7 (approximation lemma), the map is also surjective, hence it is an isomorphism. By comparing degrees, we see that n is the sum of the degrees:

$$n_{\mathfrak{P}} = [B/\mathfrak{P}^{e_{\mathfrak{P}}} : A/\mathfrak{p}]$$

We have that:

$$n_{\mathfrak{P}} = \sum_{i=0}^{e_{\mathfrak{P}}-1} [\mathfrak{P}^i/\mathfrak{P}^{i+1} : A/\mathfrak{p}] = e_{\mathfrak{P}} \cdot [B/\mathfrak{P} : A/\mathfrak{p}] = e_{\mathfrak{P}} f_{\mathfrak{P}}$$

which completes the proof of the proposition. □

Corollary 4.10. *The number of prime ideals $\mathfrak{P}$ of B which divide a prime ideal $\mathfrak{p}$ is at least 1 and at most n. If A has only finitely many ideals then so does B (which is therefore principal).*

Definition 4.11. *Let $\mathfrak{P}$ be a non-zero prime ideal of B, and let $\mathfrak{p} = A \cap \mathfrak{P}$. Clearly, $v_{\mathfrak{P}}(x) = e_{\mathfrak{P}} v_{\mathfrak{p}}(x)$ if $x \in K$. We say that the valuation $v_{\mathfrak{P}}$* ***prolongs (or "extends")*** *the valuation $v_{\mathfrak{p}}$ with index $e_{\mathfrak{P}}$. This is well defined because of the preceding corollary: there is at least one prime ideal $\mathfrak{P}$.*

Proposition 4.12. *Conversely, every discrete valuation function corresponds to some prime ideal $\mathfrak{P}$. Let $v_{\mathfrak{p}}$ be a discrete valuation of K. Let w be a discrete valuation of L which prolongs (extends) $v_{\mathfrak{p}}$ with index e. Then, there is a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ with $w = v_{\mathfrak{P}}$ and $e = e_{\mathfrak{P}}$.*

Proof. Let W be the valuation ring induced by the valuation w, and let $\mathfrak{Q}$ be its maximal ideal. This ring is integrally closed with field of fractions L, and contains A; hence it contains B. Let $\mathfrak{P} = \mathfrak{Q} \cap B$. Clearly, $\mathfrak{P} \cap A = \mathfrak{p}$, so $\mathfrak{P}$ divides $\mathfrak{p}$. The ring W thus contains $B_{\mathfrak{P}}$. Every discrete valuation ring is a maximal subring in its field of fractions. Hence, $W = B_{\mathfrak{P}}$, so that $w = v_{\mathfrak{P}}$ and $e = e_{\mathfrak{P}}$. □

4.3 Extensions of a complete field

We now move on to extensions of local fields. In particular, we will examine how extension of fields interacts with the corresponding extension of the ring of integers and valuations.

Proposition 4.13. *Let K be a field on which a discrete valuation v is defined, having valuation ring A. Assume K to be complete in the topology defined by v. Let L/K be a finite extension of K, and let B be the integral closure of A in L. Then, B is a discrete valuation ring and is a free A-module of rank $n = [L : K]$. Also, L is complete in the topology defined by B.*

Proof. We split into two cases, the separable case and purely inseparable case. Once these two cases are proven, any field extension can then be broken down into a series of separable and purely inseparable extensions and then the argument for each case can be applied as appropriate.

1. **(Separable case)** We begin with the case where L/K is separable. Then, B is a finitely generated A-module. As A is a Principal Ideal Domain, it follows that B is a free A-module of rank n. Let $\mathfrak{P}_i$ be the prime ideals of B, with w_i the corresponding valuations. Each w_i defines a norm on L, which makes L a Hausdorff topological vector space over K, as K is complete. It follows that the topology $\mathscr{T}_i$ defined by w_i is actually the product topology on L (identified with K^n), and hence does not depend on the index i. But w_i is determined by $\mathscr{T}_i$. Thus there is only one w_i, which shows that B is a discrete valuation ring.

2. **(Purely inseparable case)** When L/K is purely inseparable, there is a power q of the exponent characteristic such that $x^q \in K$ for all $x \in L$. Let $v'(x) = v(x^q)$; the map $v' : L^* \longrightarrow \mathbb{Z}$ is a homomorphism. Let m denote the positive generator of the subgroup $v'(L^*)$, then the function $w = \frac{1}{m} \cdot v$ is a discrete valuation of L. It is clear that its valuation ring is B, and the same argument as above shows that the topology defined by w coincides with that of K^n, making L into a complete field.

   It remains to prove that B is a finitely generated A-module. Let π be a uniformizer of A, and let $\bar{B}$=$B/\pi B$. Let b_i be elements of B whose images $\bar{b_i}$ in $\bar{B}$ are linearly independent over $\bar{K} = A/\pi A$. We claim that that b_i are linearly independent over A. If there is a relation $\sum a_i b_i = 0$ that was non-trival, we can assume that at least one of the a_i is not divisible by π. Reducing mod πB, we would obtain a non-trivial relation among the $\bar{b_i}$. In particular, the number of b_i is less than or equal to n. Supose now that the $\bar{b_i}$ form a basis of $\bar{B}$ and let E be the sub A-module of B spanned by the b_i. Every $b \in B$ can then be written in the form $b = b_0 + \pi b_1$, with $b_0 \in E$ and $b_1 \in B$. Applying this to b_1 and iterating the procedure, we get b into the form:

$$b = b_0 + \pi b_1 + \pi^2 b_2 + \dots , \; b_i \in E$$

   and since A is complete, this shows that $b \in E$.

□

Corollary 4.14. *1. If e denotes the ramification index and f denotes the residue degree of the extension L/K, then $ef = n$.*

2. There is a unique valuation w of L that prolongs v.

3. Two elements of L that are conjugate over K have the same valuation.

4. *For every* $x \in L$, $W(X) = \left(\frac{1}{f}\right) v(N_{L/K}(x))$. *(*$(N_{L/K}(x)$ *is the product of all Galois conjugates of* x*)*

Proof. 1. This follows from proposition 4.9, which we can now apply because we have proven that B is a finitely generated A-module. (proposition 4.9 was made under the assumption that A is a finitely generated A-module written under the setup for the previous subsection.)

2. This follows from the part of the proof that says the topologies generated by two w_i's are the same, so the two w_i must be the same, so the valuation w of L that prolongs v is unique.

3. Enlarging L if necessary, we can assume that L/K is normal. If $\sigma \in Gal(L/K)$, then $w \circ \sigma$ prolongs v, and hence coincides with w by part (2) of this corollary. The statement for (3) then results from the fact that conjugates $x \in L$ are just $\sigma(x)$ for all $\sigma \in Gal(L/K)$.

4. For this, we can reduce to the case where L/K is normal, and then we apply part (3), from which the result follows immediately.

□

5 Infinite Galois Theory

We will now go on a field excursion to the topic of Galois Theory for infinite extensions. Galois theory is about studying field extensions and their automorphism groups. For finite degree extensions, the fundamental theorem of Galois theory gives a correspondence between intermediate fields and subgroups of the Galois group. However, for infinite degree extensions, the Galois correspondence runs into problems. There are mappings in both directions as in the finite case, from intermediate fields to subgroups and vice versa, but this is no longer a bijection. There are too many subgroups, so more than one subgroup can have the same fixed field. This was first discovered by Dedekind in 1901. In 1928, Krull proposed how to use Topology to rescue the Galois correspondence.

The definition of the Artin map for local fields involves an infinite field extension and Krull's topology on its Galois group. We will study them here. We will be slightly less generous with the proofs here because they are neither interesting nor crucial to the understanding of the main results in future sections. Instead, we will give a few examples to illustrate the concepts.

5.1 Infinite-Degree Galois Extensions

Theorem 5.1. *For an algebraic extension L/K, the following properties are equivalent:*

1. *$L = \bigcup_i L_i$ with each extension L_i/K a finite Galois Extension.*
2. *L is the splitting field over K of a set of separable polynomials in $K[X]$.*
3. *$L^{Aut(L/K)} = K$. (This notation means K is the fixed field of $Aut(L/K)$ in L.)*
4. *L/K is both separable and normal.*

Proof. This is a result from Keith Conrad's expository paper on Infinite Galois Theory [3]. □

Definition 5.2. 1. *We call an algebraic extension L/K **Galois** if it satisfies the conditions in the preceding theorem.*

2. *When L/K is a Galois extension, we set its Galois group $Gal(L/K)$ to be the group of all K-automorphisms of L.*

Example 5.3. *let p be a prime, and define $\mathbb{Q}(\zeta_{p^\infty}) := \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{p^n})$. We can describe an element $\sigma \in Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ by indicating what σ looks like on each field $\mathbb{Q}(\zeta_{p^n})$. By finite Galois theory, $Gal(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \equiv (\mathbb{Z}/p^n\mathbb{Z})^*$ by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_n}$ for some integer a_n mod p^n where $(a_n, p) = 1$. We have a tower of field extensions:*

$$\mathbb{Q}(\zeta_{p^\infty}) \subseteq ... \subseteq \mathbb{Q}(\zeta_{p^3}) \subseteq \mathbb{Q}(\zeta_{p^2}) \subseteq \mathbb{Q}(\zeta_{p^1})$$

Each σ gives us a list of numbers a_n mod p^n in $(\mathbb{Z}/p^n\mathbb{Z})^*$, which tells us what happens in each of the finite extension subfields. However, the numbers in this list are not independent of each other: there is a compatibility condition between them coming from the fact that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. Hence, we have:

$$\sigma(\zeta_{p^{n+1}}^p) = \sigma(\zeta_{p^n})$$

$$\implies \sigma(\zeta_{p^{n+1}})^p = \zeta_{p^n}^{a_n}$$
$$\implies (\zeta_{p^{n+1}}^{a_{n+1}})^p = \zeta_{p^n}^{a_n}$$
$$\implies \zeta_{p^n}^{a_{n+1}} = \zeta_{p^n}^{a_n}$$

so $a_{n+1} \cong a_n \ mod\ p^n$. *This condition means that* $Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ *is the p-adic integers* $\mathbb{Z}_p$.

Theorem 5.4. *If* L/K *is an infinite-degree Galois Extension then* $Gal(L/K)$ *is infinite.*

Proof. If $Gal(L/K)$ was finite with order m, then each $\alpha \in L$ has degree at most m over K. So there is a uniform upper bound on the degrees over K of all elements of L. So L/K is finite. □

Theorem 5.5. *Let* L/K *be a Galois extension. Then, for for each* $\alpha \in L$*, the roots of its minimal polynomial over* K *are* $\{\sigma(\alpha) : \sigma \in Gal(L/K)\}$.

Proof. Since L/K is Galois, there exists a finite Galois extension $F/K \subseteq L/K$ that contains α. By finite Galois theory, the K-conjugates of α are $\{\phi(\alpha) : \phi \in Gal(F/K)\}$. Then, for $\phi \in Gal(F/K)$, $\phi(\alpha) = \sigma(\alpha)$ for some $\sigma \in Gal(F/K)$, so:

$$\{\phi(\alpha) : \phi \in Gal(F/K)\} \subset \{\sigma(\alpha) : \sigma \in Gal(L/K)\}$$

Conversely, for $\sigma \in Gal(L/K)$ and $f(x)$ the minimal polynomial of α over K, $f(\alpha) = 0 \implies f(\sigma(\alpha)) = 0$. So $\sigma(\alpha)$ is a K-conjugate of α. □

The preceding theorem is almost exactly the same as the finite extension case. However, there are some slight subtleties to it:

1. $Gal(L/K)$ being infinite does not imply that $\{\sigma(\alpha) : \sigma \in Gal(L/K)\}$ is infinite. In fact, this set is always finite since it's the K-conjugates of α.

2. In a finite extension, there exists primitive elements for which $L = K(\alpha)$ and then the number of K-conjugates is $[L : K]$. This never happens in infinite Galois extensions.

At the beginning of this section, we mentioned that there are too many subgroups for a 1-1 galois correspondence. We now give two examples to illustrate this.

Example 5.6. *Let* $L = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, ...)$ *(adjoining* $\mathbb{Q}$ *with* $\sqrt{-1}$ *and* $\sqrt{all\ prime\ numbers}$*), so* $Gal(L/\mathbb{Q}) = \prod\{\pm 1\}$*, a countable direct product of the group* $\{\pm 1\}$*. This is an abelian group where each non-identity element has order 2, and whose cardinality is uncountable (By Cantor's diagonal argument: Suppose it is countable. Then we can make a list/enumeration of the elements. Consider the element* $s \in Gal(L/\mathbb{Q})$ *whose* i^{th} *term differs from the* i^{th} *element in our list at position* i*, for all* $i \geq 1$*. Then* s *will never appear on our list of enumeration of elements of* $Gal(L/\mathbb{Q})$*.)*

So $Gal(L/\mathbb{Q})$ *has uncountably many subgroups of order 2 (each element generates a unique subgroup). At the same time,* L *only has countably many subfields of each 2-power degree over* $\mathbb{Q}$*. Therefore, the subfields of* L *and the subgroups of* $Gal(L/\mathbb{Q})$ *do not have the same cardinality, and so there can't be a bijection between them.*

Example 5.7. *We use the same setup as example 5.3, this time specializing to the case $p = 2$. Set $\mathbb{Q}(\zeta_{2^\infty}) := \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{2^n})$. Then, $Gal(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}) \equiv (\mathbb{Z}/2^n\mathbb{Z})^*$. We have the following tower of fields:*

$$\mathbb{Q}(\zeta_{2^\infty}) \subseteq ... \subseteq \mathbb{Q}(\zeta_{2^3}) \subseteq \mathbb{Q}(\zeta_{2^2}) \subseteq \mathbb{Q}(\zeta_2) = \mathbb{Q}$$

For odd $a \in \mathbb{Z}$, let $\sigma_a \in Gal(L/\mathbb{Q})$ act by $\zeta_{2^n} \mapsto \zeta_{2^n}^a$. We examine $a = 5$ and $a = 13$:

$$\sigma_5(\zeta_{2^n}) = \zeta_{2^n}^5$$
$$\sigma_{13}(\zeta_{2^n}) = \zeta_{2^n}^{13}$$

Let $H =< \sigma_5 >$ and $H' =< \sigma_{13} >$, the cyclic subgroups generated by those elements. The cyclic subgroups H and H' in $Gal(L/\mathbb{Q})$ are not the same: If they were, the generator σ_{13} of H' would be one of the generators $\sigma_5^{\pm 1}$ of H, which, when applied to ζ_{2^n}, would mean:

$$\zeta_{2^n}^{13} = \zeta_{2^n}^{5\pm 1}$$

so $13 \equiv 5^{\pm 1}$ mod 2^n for all n, which is clearly a contradiction.
Even though $H \neq H'$, we claim that $L^H = L^{H'}$ (This notation means the fixed field of H and H'). Set $L_n = \mathbb{Q}(\zeta_{2^n})$. Then:

$$Gal(L_n/\mathbb{Q}) \cong (\mathbb{Z}/2^n\mathbb{Z})^* \text{ by } \sigma_a(\zeta_{2^n}) = \zeta_{2^n}^a$$

Then, we have a tower of fields:

$$L_r = \mathbb{Q}(\zeta_{2^n}) \subset ... \subset \quad \mathbb{Q}(\zeta_4) = \mathbb{Q}(i) \quad \subset \quad \mathbb{Q}(\zeta_2) = \mathbb{Q}$$

Since $5, 13 \equiv 1$ mod 4, σ_5 and σ_{13} both fix i, so $\mathbb{Q}(i)$ is in both L^H and $L^{H'}$. For $n \geq 2$, it turns out that < 5 mod $2^n > = < 13$ mod $2^n >$ in $(\mathbb{Z}/2^n\mathbb{Z})^*$, and both subgroups have index 2. Since those two subgroups are the same, the subfields of L_n that are fixed by 5 mod 2^n and 13 mod 2^n (as elements of $Gal(L_n/\mathbb{Q})$ acting as the 5^{th} and 13^{th} power of ζ_{2^n}) are the same. By the finite Galois correspondence, this common fixed field has degree 2 over $\mathbb{Q}$.
Since $\mathbb{Q}(i)$ is known to be fixed and it has degree 2, it is the whole fixed field. Notice that $\mathbb{Q}(i)$ is independent of n: $L_n^H = \mathbb{Q}(i)$ and $L_n^{H'} = \mathbb{Q}(i)$ $\forall n \geq 2$. Every element of L is inside some L_n, so $L^H = \mathbb{Q}(i) = L^{H'}$. These are two different subgroups of $Gal(L/\mathbb{Q})$ with the same fixed field, so the Galois correspondence breaks down.

This example was the same type as the one discovered by Dedekind in 1901, except that he used odd primes instead of $p = 2$.

5.2 The Krull Topology on Galois Groups

To fix the Galois correspondence for infinite-degree Galois extensions, Krull defined a topology on Galois groups so that there is a $1-1$ correspondence between intermediate fields and *closed* subgroups of the Galois group. For a finite Galois extension, this topology turns out to be discrete, so it was unnecessary to cover it when studying finite extensions in an undergraduate course. In this subsection, we define this topology and study some of the immediate results.

Intuitively, two automorphisms σ and τ in $Gal(L/K)$ are "close" in this topology if $\sigma = \tau$ on

a finite subextension F/K with large degree. The larger the degree, the "closer" σ and τ are, because a larger finite extension F/K in L covers "more" of L.

We start off with a simple lemma examining the cosets of subgroups of the Galois group of infinite extensions:

Lemma 5.8. *Let L/K be a Galois extension with $G = Gal(L/K)$.*

1. *For $\sigma \in G$ and an intermediate field E between L and K, the coset $\sigma Gal(L/E)$ is all automorphisms of G that agrees with σ on E:*

$$\sigma Gal(L/E) = \{\tau \in G : \tau|_E = \sigma|_E\}$$

2. *If F/K is a finite extension inside L, then $Gal(L/F)$ has index $[F : K]$ in $Gal(L/K)$.*

Proof. 1. For $\phi \in Gal(L/E)$ and $\alpha \in E$, $(\sigma\phi)(\alpha) = \sigma(\phi(\alpha)) = \sigma(\alpha)$. Thus, $\sigma\phi = \sigma$ on E. Conversely, suppose $\tau \in G$ satisfies $\tau|_E = \sigma|_E$. Let $\phi = \sigma^{-1}\tau \in G$, so $\tau = \sigma\phi$. For $\alpha \in E$, $\tau(\alpha) = \sigma(\alpha)$, so $\sigma^{-1}(\tau(\alpha)) = \alpha$, or $\phi(\alpha) = \alpha$. Therefore, ϕ fixes all elements of E, so $\phi \in Gal(L/E)$ and $\tau = \sigma\phi \in \sigma Gal(L/E)$.

2. The index of $Gal(L/F)$ in $Gal(L/K)$ is the number of (left) cosets. Saying that $\sigma Gal(L/F) = \tau Gal(L/F)$ means that $\sigma = \tau$ on F. Since F/K is a finite separable extension inside the Galois Extension L/K, the number of field homomorphisms $F \longrightarrow L$ that fixes K is $[F : K]$. Therefore, the number of left cosets of $Gal(L/F)$ in $Gal(L/K)$ is $[F : K]$.

□

Definition 5.9 (Krull Topology: Open sets definition)**.** *We split this into two parts: basic open sets and general open sets:*

1. *(basic open set) For $\sigma \in Gal(L/K)$, a **basic open set** around σ, or a basic open neighbourhood of σ, is a coset $\sigma Gal(L/F)$ where F/K is a finite extension.*

2. *(open set) A non-empty subset U of $Gal(L/K)$ is open when each element of U is contained in a basic open set of U. i.e. for each $\sigma \in U$, $\sigma Gal(L/F) \subset U$ for some finite extension F/K inside of L.*

*The open sets in $Gal(L/K)$ as described above, along with the empty set, defines a topology on $Gal(L/K)$ called the **Krull Topology**. We will not check the topological space axioms here, instead we will refer to theorem 4.3 on page 8 of [3].*

Every open set around the identity contains $Gal(L/F)$ for some finite extension F/K in L. Indeed, open sets are defined to be the unions of basic open sets, and the basic open sets around the identity are defined to be the subgroups $Gal(L/F)$.

By the preceding lemma, a basic open set of σ in $Gal(L/K)$ is the set of all elements of $Gal(L/K)$ that agree with σ on some finite extension F/K inside L. The intuition is that a "small" open set around σ is all the automorphisms in $Gal(L/K)$ that agrees with σ on a "big" finite extension of K inside L. Note that $F \subset F' \implies Gal(L/F') \subset Gal(L/F)$, so being equal to σ on a bigger subfield corresponds to a smaller open set around σ.

Example 5.10. *For $L = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, ...)/\mathbb{Q}$ whose Galois group $Gal(L/\mathbb{Q})$ is $\prod\{\pm 1\}$, the Krull topology on this product is the product topology where each factor $\{\pm 1\}$ has the discrete topology.*

Example 5.11. *Consider $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$, where $\mathbb{Q}(\zeta_{p^\infty}) := \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{p^n})$. Its Galois group is the "sequences" $\{a_n \ mod \ p^n\}$ in $\prod_{n\geq 1}(\mathbb{Z}/p^n\mathbb{Z})^*$ with compatibility condition $a_n \equiv a_{n-1} \ mod \ p^{n-1}$ for $n \geq 2$ (i.e. action on $p^n - th$ roots of unity must agree with p^{n-1}-th roots of unity). Two such compatible sequences $\{a_n \ mod \ p^n\}$ and $\{b_n \ mod \ p^n\}$ are "close" if the n^{th} terms are equal for a set of early values of n: this is what it means for the automorphisms associated to these two sequences to be the same function on $\mathbb{Q}(\zeta_{p^n})$. We notice that this is the same definition as the $p-$adic integers $\mathbb{Z}_p$, and two elements are "close" if their difference has small $p-$adic norm, i.e. they differ by a large power of p. Hence, we conclude that $Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ is $\mathbb{Z}_p$.*

Every finite extension F/K can be enlarged to a finite Galois extension $\tilde{F}/K$ in L, so every basic open set $\sigma Gal(L/F)$ contains $\sigma Gal(L/\tilde{F})$. Therefore, when dealing with a basic open neighbourhood of an automorphism σ, by shrinking it we can assume the F defining the basic open neighbourhood of σ is Galois over K. This is used in the next theorem:

Theorem 5.12. *The topology on $Gal(L/K)$ has the following properties:*

1. *The operations of:*
   - *multiplication $m : Gal(L/K) \times Gal(L/K) \longrightarrow Gal(L/K)$ and;*
   - *inversion $i : Gal(L/K) \longrightarrow Gal(L/K)$*

   are continuous. This turns $Gal(L/K)$ into a ***topological group.***
2. *When $Gal(L/K)$ is finite, the topology is discrete.*
3. *$Gal(L/K)$ is Hausdorff.*

Proof. Theorem 4.6 on page 9 of [3]. □

Theorem 5.13 (Krull)**.** *Let L/K be Galois and set $G = Gal(L/K)$, equipped with the Krull topology. Associate to each intermediate field E the subgroup $Gal(L/E)$ of G, and associate toeach subgroup H of G the intermediate field $L^H = \{\alpha \in L : h(\alpha) = \alpha, \ \forall h \in H\}$. Then:*

1. *For all E, $Gal(L/E)$ is a closed subgroup of G.*
2. *For all H, $Gal(L/L^H)$ is the closure of H in G.*
3. *(Galois Correspondence) The mappings $E \mapsto Gal(L/E)$ and $H \mapsto L^H$ are inclusion-reversing bijections between the intermediate fields in L/K and the closed subgroups of $Gal(L/K)$, and they are inverses of each other: $L^{Gal(L/E)} = E$ and $Gal(L/L^H) = H$ when H is closed.*
4. *For an arbitrary subgroup $H \subset G$, $L^H = L^{\bar{H}}$.*

Proof. See theorem 4.7 on page 10 in [3]. □

Theorem 5.14. *Let L/K be a Galois extension.*

1. *The closed subgroups of $Gal(L/K)$ are $Gal(L/E)$ for intermediate field extensions E/K in L.*

2. *The open subgroups of $Gal(L/K)$ are $Gal(L/F)$ for finite extensions F/K in L.*

3. *The closed normal subgroups of $Gal(L/K)$ are $Gal(L/E)$ where E is a Galois extension of K in L. Equivalently, a closed subgroup H of $Gal(L/K)$ is normal if and only if L^H/K is a Galois extension.*

4. *The open normal subgroups of $Gal(L/K)$ are $Gal(L/F)$ where F is a finite Galois extension of K in L. Equivently, an open subgroup H of $Gal(L/K)$ is normal if and only if L^H/K is a finite Galois extension.*

Proof. See theorem 4.10 on page 13 in [3]. □

Theorem 5.15. *For a Galois extension L/K, the Krull topology on $Gal(L/K)$ is compact.*

Proof. See theorem 5.4 on page 17 in [3]. □

Corollary 5.16. *A subgroup of $Gal(L/K)$ in the Krull topology is open if and only if it is closed with finite index.*

Proof. This follows by definition of $Gal(L/K)$ being a compact topological group. □

Theorem 5.17. *If L/K is Galois and E is an intermediate field, then the subspace topology on $Gal(L/E)$ as a subset of $Gal(L/K)$ equals the Krull topology on $Gal(L/E)$.*

Proof. See theorem 5.2 on page 15 in [3]. □

6 Local Class Field Theory

As the Hilbert Symbol is a local object, we must now explore Local Class Field Theory.

Historically, Class Field Theory for global fields were studied before local fields, since local fields require a more intricate construction. However, we are now armed with the intuition from Global Class Field Theory, studying the local case should be easier, despite the more involved construction of local fields and local rings. As with the global case, there are three main theorems for Local Class Field Theory: Local Artin Reciprocity, Local Existence, and the Main Theorem of Local Class Field Theory. Again, we will begin with some important definitions in the first subsection, before stating the theorems (without proof) in the next subsection.

6.1 Definitions and Setup

Definition 6.1 (Maximal Abelian Extension)**.** *Let K be a field with separable closure K^{sep} (Maximal Galois extension of K). The field:*

$$K^{ab} := \bigcup_{\substack{L \subseteq K^{sep} \\ L/K \, finite \, abelian}} L$$

is the maximal abelian extension of K in K^{sep}.

The field K^{ab} contains the field K^{unr}, the maximal unramified subextension of K^{sep}/K. (from [12] MIT course 18.785 lecture notes, lecture 24, discussion after definition 24.1) Hence, we have the tower of extensions:

$$K \subseteq K^{unr} \subseteq K^{ab} \subseteq K^{sep}$$

Definition 6.2 (Profinite Groups, profinite completion)**.** *Let G be a topological group (a group with a topology such that the inversion and group operation $m : G \times G \to G$ maps are continuous. $G \times G$ is given the product topology.) Let H be a subgroup of G that is open, normal, and has finite index. Certainly, there is a map $G \to G/H$ for each possible H. Now, we put all these information together:*

$$G \longrightarrow \varprojlim_{H} G/H$$

Where $\varprojlim_H G/H$ is a subgroup of

$$\prod_{\substack{H open \\ finite \, index}} G/H$$

Whenever we have a containment of subgroups $H \subseteq H'$, we have a map:

$$\prod_{H \; H'} : G/H \longrightarrow G/H'$$

Profinite groups are defined as the inverse limit:

$$\hat{G} = \varprojlim_{H} \{X_H : \forall H \subseteq H', \prod_{H \; H'} (X_H) = X'_H\}$$

This is also called the profinite completion of G.

Proposition 6.3 (Galois group of K^{ab}/K)**.** *([12], lecture 24) The Galois group of K^{ab}/K is the profinite group:*

$$Gal(K^{ab}/K) \cong \varprojlim_{L} Gal(L/K)$$

where the fields L range over finite abelian extensions of K in K^{sep} and are ordered by inclusion. This is a profinite group (meaning that it is the inverse limit of an inverse system of discrete finite groups. Each finite group has discrete topoology, and then we take the product topology on the inverse limit.). The group $Gal(K^{ab}/K)$ is a totally disconnected compact Hausdorff group (meaning there are no non-trivial connected subsets.)

Theorem 6.4. *(Galois correspondence)([12], lecture 24) We have the Galois correspondence:*

$$\{Sub-extensions\ L/K\ in\ K^{ab}/K\} \longleftrightarrow \{Closed\ subgroups\ H\ in\ Gal(K^{ab}/K)\}$$

$$L \mapsto Gal(K^{ab}/K)$$
$$(K^{ab})^H \hookleftarrow H$$

Under this correspondence, Abelian extensions L/K correspond to finite index open subgroups of $Gal(K^{ab}/K)$. However, $Gal(K^{ab}/K)$ is normal, is abelian, and so every subgroup of $Gal(K^{ab}/K)$ is normal. It follows that every subextension of K^{ab}/K is Galois and Abelian.

When K is an archimedean local field its Abelian extensions are easy to understand. Either $K = \mathbb{R}$, in which case $\mathbb{C}$ is its only nontrivial Abelian extension, or $K = \mathbb{C}$ and there are no nontrivial abelian extensions.

Now suppose K is a non-archimedean local field with ring of integers $\mathscr{O}_K$, maximal ideal $\mathfrak{p}$, and its residue field $\mathbb{F}_\mathfrak{p} := \mathscr{O}_K/\mathfrak{p}$. If L/K is a finite unramified extension, where L has residue field $\mathbb{F}_\mathfrak{q} := \mathscr{O}_L/\mathfrak{q}$, then we have a canonical isomorphism:

$$Gal(L/K) \cong Gal(\mathbb{F}_q/\mathbb{F}_p)$$

$$x \mapsto x^{|\mathbb{F}_\mathfrak{p}|}$$

between the Galois group of L/K and the Galois group of the residue field extension $\mathbb{F}_q/\mathbb{F}_p$, which is the cyclic group generated by the Frobenius automorphism $x \mapsto x^{|\mathbb{F}_\mathfrak{p}|}$. We henceforth use:

$$Frob_{L/K} \in Gal(L/K)$$

to denote the inverse image of the Frobenius automorphism under this isomorphism. This only makes sense when L/K is unramified.

Definition 6.5 (Field Norm (also sometimes called Galois Norm))**.** *We define this in two ways. The first one for Galois extensions, and the second one for general extensions.*

1. *Let L/K be a Galois extension. Then, the norm of an element $\alpha \in L$ is the product of all the Galois conjugates of α:*

$$N_{L/K}(\alpha) = \prod_{\sigma \in Gal(L/K)} \sigma(\alpha)$$

2. *Now, let L/K be a general field extension, and let $\alpha \in L$ be a non-zero element. Let $\sigma_1(\alpha), ..., \sigma_n(\alpha)$ be the roots of the minimal polynomial of α over K, listed with multiplicity and lying in some extension field of L. Then:*

$$N_{L/K}(\alpha) = \left(\prod_{i=1}^{n} \sigma_i(\alpha) \right)^{[L:K(\alpha)]}$$

Definition 6.6 (Norm group of a field K)**.** *Let K be a local field. A **norm group**(of K) is a subgroup of the form:*

$$N(L^*) := N_{L/K}(L^*) \subseteq K^*$$

for some finite abelian extension L/K. (So this is the subset of K^* that appear as norms of elements of L^*.

6.2 The Theorems of Local Class Field Theory

Theorem 6.7 (Local Artin Reciprocity)**.** *Let K be a local field. There is a unique continuous homomorphism:*

$$\theta_K : K^* \longrightarrow Gal(K^{ab}/K)$$

with the property that for each finite extension L/K in K^{ab}, the homomorphism:

$$\theta_{L/K} : K^* \longrightarrow Gal(L/K)$$

obtained by composing θ_K with the quotient map $Gal(K^{ab}/K) \to Gal(L/K)$ satisfies:

1. *If K is non-archimedean and L/K is unramified then $\theta_{L/K}(\pi) = Frob_{L/K}$ for every uniformizer π of $\mathcal{O}_K$.*
2. *$\theta_{L/K}$ is surjective with kernel $N_{L/K}(L^*)$, inducing $K^*/N_{L/K}(L^*) \cong Gal(L/K)$.*

Given an element $\alpha \in K^*$ and a field extension L/K, we shall write $(\alpha, L/K)$ to denote the image of α in $Gal(L/K)$ under the map $\theta_{L/K}$ as defined above.

Proof. See [13], MIT Lecture notes for 18.786 Number Theory II, lecture 31. □

Comparing this to Global Class Field Theory in Theorem 3.11, we have a few differences:

1. There is no modulus $\mathfrak{m}$ to worry about. Working in K^{ab} lets us treat all class fields at once.
2. There are no class groups involved. The class group of a local field is necessarily trivial since $\mathcal{O}_K$ is a Principal Ideal Domain, so instead we just take quotients of K^*.
3. We have the topology of $Gal(K^{ab}/K)$ and K^* to work with.
4. The local Artin homomorphism is not an isomorphism, but after taking profinite completions, it becomes one.

Local Artin Reciprocity tells us that in order to understand the finite Abelian extensions of a local field K, we just need to understand its norm groups. In particular, the isomorphism $K^*/N_{L/K}(L^*) \cong Gal(L/K)$ implies that $[K^* : N(L^*)] = [L : K]$ is finite. Moreover, there is an order-preserving isomorphism between the lattice of norm groups in k^* and the lattice of finite abelian extensions of K. This is essentially the Galois correspondence with Galois groups replaced by norm groups.

Corollary 6.8. *The map $L \longrightarrow N(L^*)$ defines an inclusing reversing bijection between the finite abelian extensions L/K in K^{ab} and the norm groups in K^* that satisfy:*

1. $N((L_1L_2)^*) = N(L_1^*) \cap N(L_2^*)$
2. $N((L_1 \cap L_2)^*) = N(L_1^*)N(L_2^*)$

Proof. [13] MIT 18.785 Lecture 24, corollary 24.5. □

Lemma 6.9. *Let L/K be an extension of local fields. If $N(L^*)$ has finite index in K^*, then it is open.*

Proof. This is clear if L and K are archimedean, so we assume otherwise. Suppose $[K^* : N(L^*)] < \infty$. The unit group $\mathscr{O}_L^*$ is compact, so $N(\mathscr{O}_L^*)$ is compact and therefore closed in the Hausdorff space K^*. For any $\alpha \in L$ we have:

$$\alpha \in \mathscr{O}_L^* \iff |\alpha| = 1 \iff |N_{L/K}(\alpha)| = 1 \iff \alpha \in \mathscr{O}_K^*$$

and therefore:

$$N(\mathscr{O}_L^*) = N(\mathscr{O}_L^*) \cap \mathscr{O}_K^*$$

It follows that $N(\mathscr{O}_L^*)$ is equal to the lernel of the map $N(\mathscr{O}_K^*) \hookrightarrow K^* \to K^*/N(L^*)$, and therefore $[\mathscr{O}_K^* : N(\mathscr{O}_K^*)] \leq [K^* : N(L^*)] < \infty$. Thus, $N(\mathscr{O}_L^*)$ is a closed subgroup of finite index in $\mathscr{O}_K^*$, hence open (its complement is a finite union of closed cosets, hence closed), and $\mathscr{O}_K^*$ is open in K^*, so $N(\mathscr{O}_L^*)$ is open in K^*. □

Theorem 6.10 (Local Existence Theorem)**.** *Let K be a local field. For every finite index open subgroup H of K^*, there is a unique finite Abelian extension L/K inside K^{ab} for which $H = N_{L/K}(L^*)$.*

The local Artin homomorphism $\theta_K : K^* \longrightarrow Gal(K^{ab}/K)$ is not an isomorphism. It cannot be one, because $Gal(K^{ab}/K)$ is compact but K^* is not. However, the local existence theorem implies that after taking profinite completions it becomes one.

Theorem 6.11 (Main Theorem of Local Class Field Theory)**.** *Let K be a local field. The local Artin homomorphism induces a canonical isomorphism of profinite groups:*

$$\hat{\theta_K} : \hat{K^*} \longrightarrow Gal(K^{ab}/K)$$

Proof. We first note that $Gal(K^{ab}/K)$ is a profinite group under the Krull topology, isomorphic to the inverse limit:

$$Gal(K^{ab}/K) \cong \varprojlim_L Gal(L/K)$$

where L ranges over the finite Abelian extensions of K (in K^{sep}). It follows from lemma 6.9, the local existence theorem, and the definition of profinite completion, that:

$$\hat{K^*} \cong \varprojlim_L K^*/N(L^*)$$

where L again ranges over the finite Abelian extensions of K (in K^{sep}). By local Artin Reciprocity (Theorem 6.7), for every finite abelian extension L/K we have an isomorphism:

$$\hat{\theta_K} : \hat{K^*}/N(L^*) \longrightarrow Gal(L/K)$$

and these isomorphisms commute with the inclusions among the finite abelian extensions of K. We thus have an isomorphism of the two inverse systems above, and the isomorphism is canonical because the Artin map is unique and the isomorphisms in both of them are canonical. □

7 Hilbert Symbol

In section 2, we introduced the Hilbert Symbol in the quadratic case via the existence of non-trivial solutions to a specific quadratic form (Namely, $(a,b) = 1$ if $z^2 - ax^2 - by^2 = 0$ has a solution $(z,x,y) \neq (0,0,0)$ in the field we are considering). This was then used to prove quadratic reciprocity. In this section, we will introduce the general Hilbert Symbol for n^{th} powers. Next, we will compute some Hilbert Symbols, in the cases where the ground field is $\mathbb{R}$ and $\mathbb{Q}_2$. We will then use this to examine higher reciprocity laws in the next section.

7.1 The Hilbert Symbol

We first begin with an important lemma:

Lemma 7.1. *Let F be a field of characteristic 0 containing the n^{th} roots of unity, and let $\beta \in F^*$. Then, $F(\sqrt[n]{\beta})$ is cyclic, and every element in F of the form $x^n - \beta$ is a norm from $F(\sqrt[n]{\beta})$.*

Proof. Fix a specific n^{th} root $\sqrt[n]{\beta}$, and let $G = Gal(F(\sqrt[n]{\beta})/F)$. The map $\sigma \mapsto \frac{\sigma(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}$ is a homomorphism from G to the group of n^{th} roots of unity. Since an element of G is completely determined by its effect on $\sqrt[n]{\beta}$, this map is an injection.

Hence, G and its image are cyclic, let d be the order of this image. Fix a generator σ of G. Then, the image of σ has order d, so there exists a primitive n^{th} root of unity ζ such that $\sigma(\sqrt[n]{\beta}) = \zeta^{\frac{n}{d}} \cdot \sqrt[n]{\beta}$. By induction and the fact that σ fixes the n^{th} roots of unity (for they lie in F), we have that $\sigma^k(\sqrt[n]{\beta}) = \zeta^{\frac{n}{d}} \cdot \sqrt[n]{\beta}$. Now, for $0 \leq j \leq \frac{n}{d} - 1$, the norm of $x - \zeta^j \sqrt[n]{\beta}$ is:

$$\prod_{k=0}^{d-1} \sigma^k(x - \zeta^j \sqrt[n]{\beta}) = \prod_{k=0}^{d-1} (x - \zeta^j \zeta^{\frac{n}{d} \cdot k}(\sqrt[n]{\beta}))$$

So the norm of $\prod_{j=0}^{\frac{n}{d}-1}(x - \zeta^j \sqrt[n]{\beta})$ is:

$$\prod_{j=0}^{\frac{n}{d}-1} \prod_{k=0}^{d-1} (x - \zeta^{j + \frac{n}{d} \cdot k}(\sqrt[n]{\beta})) = \prod_{i=0}^{n-1} (x - \zeta^i \sqrt[n]{\beta}) = x^n - \beta$$

□

Definition 7.2 (General Hilbert Symbol)**.** *Let K be a number field, v a place of K (by "place" we mean an equivalance class of absolute values on K. Two absolute values are equivalent if they induce the same topology), and E^v the maximal Abelian extension of K_v of exponent n. For $\alpha, \beta \in K_v$, define:*

$$\langle \alpha, \beta \rangle_v = \frac{\Phi_{E^v/K_v}(\alpha)(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}$$

to be the Hilbert Symbol at K_v. ($\Phi_{E^v/K_v}(\alpha)$ is the unique element of $Gal(E^v/K_v)$ determined by Theorem 6.7 (Local Artin Reciprocity).

Lemma 7.3 (Properties of the General Hilbert Symbol)**.** *The Hilbert Symbol enjoys the following properties (Some of them were already stated in the quadratic case in section 2, this is the more general case):*

1. $\langle \alpha, \beta \rangle_v = 1$ *if and only if* α *is a norm from* $K_v(\sqrt[n]{\beta})$.

2. *If* v *is finite, and* α, β, n *are units in* $\mathcal{O}_v$, *then* $\langle \alpha, \beta \rangle_v = 1$.

3. $\langle \alpha, -\alpha \rangle_v = 1$, *and* $\langle \alpha, 1-\alpha \rangle_v = 1$, *for* $\alpha \neq 1$.

4. $\langle \alpha, \beta \rangle_v = \langle \beta, \alpha \rangle_v^{-1}$. *(In the quadratic case in proposition 2.4 it was written as* $\langle \alpha, \beta \rangle_v = \langle \beta, \alpha \rangle_v$, *but that was because the roots of unity* ζ_2 *is just* ± 1 *so each element is its own inverse, so it doesn't matter if we have the inverse on RHS or not, so this is not a contradiction)*

Proof. 1. The restriction of the Artin map for E^v/K_v to $K_v(\sqrt[n]{\beta})$ is the same as the Artin map for $K_v(\sqrt[n]{\beta})/K_v$. Fixing β and varying α, we see that we can just work with this latter Artin map. So:
$\langle \alpha, \beta \rangle_v = 1$
$\iff (\alpha, K_v(\sqrt[n]{\beta})/K_v)$ fixes $\sqrt[n]{\beta}$
$\iff (\alpha, K_v(\sqrt[n]{\beta})/K_v)$ fixes all of $K_v(\sqrt[n]{\beta})$
$\iff \alpha$ is in the kernel of the Artin map for $K_v(\sqrt[n]{\beta})/K_v$
$\iff \alpha$ is a norm from $K_v(\sqrt[n]{\beta})$.
This proves (1).

2. $K_v(\sqrt[n]{\beta})/K_v)$ is unramified, in which case the norm map on the group of units is surjective. Hence, α is a norm, so $< \alpha, \beta >_v = 1$ by part (1).

3. By Lemma 7.1, $0^n - (-\alpha) = \alpha$ is a norm from $K_v(\sqrt[n]{\alpha}))$, so $< \alpha, -\alpha >_v = 1$ by part (1). Similarly, $1^n - \alpha = 1 - \alpha$ is a norm from $K_v(\sqrt[n]{\alpha}))$, so $< 1-\alpha, \alpha >_v = 1$.

4. This follows from (3). We have:
$$\begin{aligned} 1 &= \langle \alpha\beta, -\alpha\beta \rangle_v \\ &= \langle \alpha, -\alpha \rangle_v \cdot \langle \alpha, \beta \rangle_v \cdot \langle \beta, \alpha \rangle_v \cdot \langle \beta, -\beta \rangle_v \\ &= \langle \alpha, \beta \rangle_v \cdot \langle \beta, \alpha \rangle_v \end{aligned}$$

□

7.2 Computations of some Hilbert Symbols

We now compute some Hilbert Symbols in some specific cases. We first begin by giving the general setup in order to give a formula for the Hilbert Symbol:
Let F be a local field with group of units U (Let $U = F^*$ if F is archimedean). We will analyse the restricted Hilbert Symbol:

$$\langle -, - \rangle : U \times U \to \mathbb{C}^*$$

by finding a finite subgroup N of U such that $\langle x, y \rangle = 1$ whenever x or y is in U. This induces a well defined pairing:

$$U/N \times U/N \longrightarrow \mathbb{C}^*$$

Thus, for any $(x, y) \in U \times U$, the symbol $\langle x, y \rangle$ is completely determined by the representative classes of x and y in U/N.

Proposition 7.4. *Let $n = 2$. The Hilbert Symbol:*

$$\mathbb{R}^* \times \mathbb{R}^* \longrightarrow \{-1, 1\}$$

is given by the formula:

$$\langle x, y \rangle = (-1)^{\frac{sgn(x)-1}{2} \cdot \frac{sgn(y)-1}{2}}$$

where $sgn(\bullet)$ is the sign function.

Proof. Let $N = (0, \infty)$ (This is the interval, not the set). We claim that $\langle x, y \rangle$ is trivial whenever x or y is in N.

- If $y \in N$, then $\mathbb{R}(\sqrt{y}) = \mathbb{R}$, so the Artin map is trivial.
- If $x \in N$, then whether or not y is in N (i.e. whether or not $\mathbb{R}(\sqrt{y})$ is $\mathbb{R}$ or $\mathbb{C}$), x is a norm from $\mathbb{R}(\sqrt{y})$, so x is in the Artin map $\mathbb{R}(\sqrt{y})/\mathbb{R}$.

By the discussion in the setup above, we only have to compute the Hilbert Symbol at different coset representatives. The only that that still remains to be computed is $\langle -1, -1 \rangle$, but this is clear -1, since $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$, and -1 is not a norm from $\mathbb{C}$. □

Proposition 7.5. *Let $n = 2$. If $F = \mathbb{Q}_2$, and U its group of units, then the Hilbert Symbol*

$$U \times U \to \{-1, 1\}$$

is given by the formula:

$$\langle x, y \rangle = (-1)^{\frac{x-1}{2} \cdot \frac{y-1}{2}}$$

Proof. Define

$$U_1 := 1 + 2\mathbb{Z}_2$$

Then clearly $U = U_1$. We also define:

$$U_2 := 1 + 4\mathbb{Z}_2 = \{x \in \mathbb{Z}_2 : x \equiv 1 (mod\ 4)\}$$

Furthermore, $U_1/U_2 = \{x \in \mathbb{Z}_2 : x \equiv 3 (mod\ 4)\}$. Observe that $U^2 \subseteq U_2$, which implies that $U_2 = U^2$, since U has the same degree over both of these subgroups.
Now suppose x or y is in U_2. If y is in U_2, they y is a square, so $\mathbb{Q}_2(\sqrt{y}) = \mathbb{Q}_2$, which immediately implies that $\langle x, y \rangle = 1$. If $x \in U_2$, then x is a square, and hence a norm, from $\mathbb{Q}_2(\sqrt{y})$. So in this case we also have $\langle x, y \rangle = 1$.
Thus we have a well defined pairing $U/U^2 \times U/U^2 \to -1, 1$. It remains to compute $\langle x, y \rangle$ when neither x nor y is in U_2, i.e. when $x \equiv y \equiv 3 (mod\ 4)$. Reducing to coset representatives, we only have to compute $\langle -1, -1 \rangle$. In this case, $\mathbb{Q}_2(\sqrt{-1}) = \mathbb{Q}_2(i)$ is a proper extension of $\mathbb{Q}_2$ (-1 is not a square in $\mathbb{Q}_2$, and 2 ramifies in $\mathbb{Q}_2(i)$). The kernel of the Artin map $\mathbb{Q}_2(i)/\mathbb{Q}_2$ is $U^2 = U_2$. Since $-1 \notin U_2$, clearly $\langle -1, -1 \rangle = -1$.
We have just shown that $\langle x, y \rangle$ is 1 if x or y is $\equiv 1 (mod\ 4)$, and it is -1 otherwise. This is a reformulation of the claim given in the statement of the proposition. □

8 Higher Reciprocity Laws

In this section, we finally introduce the higher power reciprocity laws that we have been promising since the beginning of the paper.

8.1 Hilbert Reciprocity Law

We first introduce the law of Hilbert Reciprocity, which is the key ingredient in proving all the subsequent reciprocity laws in this section.

Theorem 8.1 (Law of Hilbert Reciprocity)**.** *[10] For any $\alpha, \beta \in K^*$, we have:*

$$\prod_v \langle \alpha, \beta \rangle = 1$$

Proof. We first note that the Artin map from Local Class Field Theory was the composition of two maps:

$$K^* \to Gal(L/K) \xrightarrow{\phi} \mu_n$$

where:

$$\phi : Gal(L/K) \longrightarrow \mu_n$$
$$\sigma \mapsto \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}$$

The Hilbert Reciprocity law follows immediately from the Artin Reciprocity Law. In fact, we have:

$$\prod_v \langle \alpha, \beta \rangle_v = \prod_v \phi(\alpha, K_v(\sqrt[n]{\beta}))$$
$$= \frac{\prod_v (\alpha, K_v(\sqrt[n]{\beta}))(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}$$
$$= \frac{id(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}$$
$$= 1$$

where the second last equality is by the Artin Reciprocity Law. □

8.2 Power Residue Law

In this subsection, we let $A = \mathcal{O}_K$, where K is a number field containing the n^{th} roots of unity. Let $\mathfrak{p}$ be a prime of K which does not divide n.

Lemma 8.2. *The n^{th} roots of unity are distinct modulo $\mathfrak{p}$.*

Proof. Suppose that they are not. Then, $\zeta^j \equiv 1 (mod\ \mathfrak{p})$ for some $1 \leq j \leq n-1$. Evaluate both sides of the expression:

$$1 + X + ... + X^{n-1} = \frac{X^n - 1}{X - 1} = \prod_{i=1}^{n-1} (X - \zeta^i)$$

at 1, and then reduce modulo p. This implies:

$$n \equiv \prod_{i=1}^{n-1} (X - \zeta^i) \equiv 0 \ (mod \ \mathfrak{p})$$

which is a contradiction. □

Observation. *n divides $N(\mathfrak{p})-1$. This is because $(\mathscr{O}_k/\mathfrak{p})^*$ has cardinality $N(\mathfrak{p})-1$, and ζ modulo p generates a subgroup of order n.*

Let $A_\mathfrak{p}$ be the localization of A at $\mathfrak{p}$. The inclusion $A \subseteq A_\mathfrak{p}$ induces an isomorphism of the residue fields $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ and $A/\mathfrak{p}$, so the n^{th} roots of unity are also distinct modulo $\mathfrak{p}A_\mathfrak{p}$. Now, if $\alpha \in K^*$ is a unit at $\mathfrak{p}$ (meaning that the image of α in $K_\mathfrak{p}$ lies in units of $K_\mathfrak{p}^*$), then it lies in $A_\mathfrak{p}$, and it remains nonzero when reduced modulo $\mathfrak{p}A_\mathfrak{p}$. We then make the following definition:

Definition 8.3 (Power Residue Symbol)**.** *We define:*

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n$$

*to be the unique n^{th} root of unity to which $\alpha^{\frac{N(\mathfrak{p})-1}{n}}$ is congruent modulo $\mathfrak{p}A_\mathfrak{p}$. Clearly $\alpha^{\frac{N(\mathfrak{p})-1}{n}}$ is indeed an n^{th} root of unity in this residue field because $\alpha^{N(\mathfrak{p})-1} = 1$ and $N(\mathfrak{p})-1$ is divisible by n, so we are taking an n^{th} root of 1. We call $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ the n^{th} **power residue symbol of** α **at** $\mathfrak{p}$.*

We have only defined this symbol for $\mathfrak{p}$ relatively prime to both n and α. If $\mathfrak{p}$ does divide n or α, then we set $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1$.
In this way, we can extend the denominator of the power residue symbol to arbitrary fractional ideals:

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n = \prod_\mathfrak{p} \left(\frac{\alpha}{\mathfrak{a}}\right)_n^{ord_\mathfrak{p}(\mathfrak{a})}$$

This is clearly a finite product. Given $\beta \in K^*$, by $\left(\frac{\alpha}{\beta}\right)_n$ we mean $\left(\frac{\alpha}{\beta\mathscr{O}_K}\right)_n$.

Proposition 8.4. *The following properties hold for $\alpha, \beta, \in K^*$:*

1. *The symbol $\left(\frac{\alpha}{-}\right)_n$ is a homomorphism in the argument of the denominator from the group of fractional ideals of K to the group of n^{th} roots of unity.*
2. *If α is a fractional ideal of K, and $\alpha_1, \alpha_2 \in K^*$ are both relatively prime to $\mathfrak{a}$, then:*

$$\left(\frac{\alpha_1\alpha_2}{\mathfrak{a}}\right)_n = \left(\frac{\alpha_1}{\mathfrak{a}}\right)_n \left(\frac{\alpha_2}{\mathfrak{a}}\right)_n$$

3. *If $\mathfrak{a}$ is relatively prime to α, then:*

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n = \frac{\left(\frac{\mathfrak{a}, K(\sqrt[n]{\alpha})}{K}\right)(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}}$$

4.

$$\left(\frac{\alpha}{\beta}\right)_n = \prod_v \langle \beta, \alpha \rangle_v$$

where v runs through all the finite places which do not divide α or n.

5. For a prime $\mathfrak{p}$ not dividing α or n, $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1$ if and only if $\mathfrak{p}$ splits completely in $K(\sqrt[n]{\alpha})$.

Proof. 1. Follows from the definition of the Power Residue Symbol and the way we extended the definition from prime ideals in the denominator to arbitrary ideals.

2. Also follows directly from the definition of the Power Residue Symbol. Multiplying two numerators together is the same thing as multiplying the two roots of unity that they correspond to, together.

3. It suffices by (1) to prove the case where $\mathfrak{a}$ is equal to a prime ideal $\mathfrak{p}$, relatively prime to α and n. In this case, $\mathfrak{p}$ is unramified in $K(\sqrt[n]{\alpha})$. So $\sigma := \left(\frac{\mathfrak{p}, k(\sqrt[n]{\alpha})}{K}\right)$ has the effect:

$$\sigma(\alpha) \equiv \alpha^p \ (mod\ \mathfrak{p}A_{\mathfrak{p}})$$

for any $\alpha \in A_{\mathfrak{p}}$. (Normally this is stated as happening in the larger ring of integers $\mathscr{O}_{K(\sqrt[n]{\alpha})}$, but we are only interested in $A = \mathscr{O}_K$ right now. This also holds in the localization $A\mathfrak{p}$.) Now, modulo $\mathfrak{p}A_{\mathfrak{p}}$, we have:

$$\frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}} \equiv \frac{(\sqrt[n]{\alpha})^p}{\sqrt[n]{\alpha}} = (\sqrt[n]{\alpha})^{p-1} = \alpha^{\frac{p-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n$$

so the left and right most expressions, both being roots of unity, must be equal.

4. This follows immediately from (3).

5.

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1$$

$$\iff \sigma := \left(\frac{\mathfrak{p}, k(\sqrt[n]{\alpha})}{K}\right) \ fixes \ \sqrt[n]{\alpha}$$

$$\iff \sigma \ fixes \ all \ of \ K(\sqrt[n]{\alpha})$$

$$\iff \sigma \ is \ the \ identity \ in \ Gal(K(\sqrt[n]{\alpha})/K)$$

but the order of σ is the inertial degree of $\mathfrak{p}$. Recall that $\mathfrak{p}$ splitting completely means that the inertial degree is 1 (and also the ramification index is 1).

□

Theorem 8.5 (Power Reciprocity Law)**.** *For $\alpha \in K^*$, let $S(\alpha)$ denote the set of places which either divide n or occur in the factorization of α. Then, for any $\alpha\beta \in K^*$:*

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{v \in S(\alpha) \cap S(\beta)} \langle \alpha, \beta \rangle_v$$

Proof. Part 4 of the preceding proposition says that:

$$\left(\frac{\alpha}{\beta}\right)_n = \prod_{v \notin S(\alpha)} \langle \beta, \alpha \rangle_v$$

which we can write as:

$$\prod_{v \in S(\beta) \setminus S(\alpha)} \langle \beta, \alpha \rangle_v \prod_{v \notin S(\beta) \cap S(\alpha)} \langle \beta, \alpha \rangle_v$$

For the v which are neither in $S(\beta)$ nor $S(\alpha)$, v is unramified in $K(\sqrt[n]{\alpha})$, and β is a unit at v. The local Artin map on a unramified extension is trivial on the units, so we conclude that $\langle \beta, \alpha \rangle_v = 1$. Therefore:

$$\left(\frac{\alpha}{\beta}\right)_n = \prod_{v \in S(\beta) \setminus S(\alpha)} \langle \beta, \alpha \rangle_v$$

On the other hand, part (4) of the preceding proposition also tells us that:

$$\left(\frac{\beta}{\alpha}\right)_n = \prod_{v \notin S(\beta)} \langle \alpha, \beta \rangle_v^{-1} = \prod_{v \in S(\beta)} \langle \alpha, \beta \rangle_v$$

where the second inequality follows from Theorem 8.1 Hilbert reciprocity. Lemma 7.3(4) (properties of the Hilbert Symbol) tells us that $\langle \beta, \alpha \rangle_v \langle \alpha, \beta \rangle_v = 1$ for each v. So:

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{v \in S(\beta) \setminus S(\alpha)} \langle \beta, \alpha \rangle_v \prod_{v \in S(\beta)} \langle \alpha, \beta \rangle_v = \prod_{v \in S(\alpha) \cap S(\beta)} \langle \alpha, \beta \rangle_v$$

□

8.3 Cubic Reciprocity

We now apply the Power Reciprocity Law to prove Cubic Reciprocity.

Definition 8.6. *Let $K = \mathbb{Q}(\omega)$, where $\omega = e^{\frac{2\pi i}{3}}$ is primitive 3rd root of unity. We call a prime π in $\mathcal{O}_K$ **primary** if $\pi \equiv \pm 1$ mod 3. Given any prime π not dividing 3, exactly two of the six associates $\pm\pi$, $\pm\omega\pi$, $\pm\omega^2\pi$ are primary.*

Theorem 8.7 (Cubic Reciprocity)**.** *If π and θ are primary primes in $\mathbb{Z}[\omega]$ of unequal norm (i.e. they are not associates), then:*

$$\left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3$$

Proof. This proof follows the approach given in exercise 8.9 of [1], primes of the form $x^2 + ny^2$. We use the Power Reciprocity Law with $n = 3$ and $K = \mathbb{Q}(\omega)$. The only prime of $\mathcal{O}_K$ dividing 3 is $\lambda = 1 - \omega$. Thus, given non-associate primes π and θ in $\mathcal{O}_K$, the Power Reciprocity Law tells us that:

$$\left(\frac{\theta}{\pi}\right)_3 \left(\frac{\pi}{\theta}\right)_3^{-1} = \langle \pi, \theta \rangle_\lambda$$

Hence, to prove cubic reciprocity, it suffices to show that:

$$\theta, \pi \; primary \implies \langle \pi, \theta \rangle_\lambda = 1$$

First, we note that $\left(\frac{-1}{\pi}\right)_3 = 1$ for any prime π, so replacing π with $-\pi$ does not affect the statement of cubic reciprocity. So we can assume that $\theta \equiv \pi \equiv 1 \; mod \; \lambda^2 \mathscr{O}_K$. Let K_λ be the completion of K at λ, and let $\mathscr{O}_\lambda$ be the valuation ring of K_λ. We will use the properties of the Hilbert Symbol to show that for any α and β,

$$\alpha, \beta \equiv 1 \; mod \; \lambda^2 \mathscr{O}_\lambda \implies \langle \alpha, \beta \rangle_\lambda = 1$$

We first note that by Hensel's Lemma, if $\alpha \equiv 1 \; mod \; \lambda^4 \mathscr{O}_\lambda$, then $\alpha = u^3$ for some $u \in \mathscr{O}_\lambda$. (This is because cubes roots in $\mathscr{O}_\lambda$ can be "lifted modulo every 2 powers of $\lambda^n \mathscr{O}_\lambda$, which then gives a lifting to all of $\mathscr{O}_\lambda$)

Next, we observe that the Hilbert Symbol is multiplicative in the first argument. This is because by definition $\langle \alpha, \beta \rangle_\lambda$ is $\frac{\Phi_{E^\lambda/K_\lambda}(\alpha)(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}$, where E^λ is the maximal abelian extension of K_λ, and $\Phi_{E^\lambda/K_\lambda}$ is the unique element of $Gal(E^\lambda/K_\lambda)$ determined by theorem 6.7, local Artin Reciprocity. The local Artin Reciprocity map is a group homomorphism $\theta_K : K^* \longrightarrow Gal(K^{ab}/K)$, so it respects multiplicative structure in K^* by definition. By the same reasoning, it also respects inverses.

Next, we make a claim:

Claim: If $\alpha \in \mathscr{O}_\lambda^*$ and $\alpha \equiv \alpha' \; mod \; \lambda^4 \mathscr{O}_\lambda$, then:

$$\langle \alpha, \beta \rangle_\lambda = \langle \alpha', \beta \rangle_\lambda$$

Proof of claim: We begin by examining the statement of the claim:
$\langle \alpha, \beta \rangle_\lambda = \langle \alpha', \beta \rangle_\lambda$
$\iff \langle \alpha, \beta \rangle_\lambda \langle \alpha', \beta \rangle_\lambda^{-1} = 1$
$\iff \langle \frac{\alpha}{\alpha'}, \beta \rangle_\lambda = 1$ (This operation is valid because α is in $\mathscr{O}_\lambda^*$, so it is invertible)
$\iff \langle u^3, \beta \rangle_\lambda = 1$, (This line follows from the fact that $\alpha \equiv \alpha'$ mod $\lambda^4 \mathscr{O}_\lambda$, hence $\frac{\alpha}{\alpha'} \equiv 1 \; mod \; \lambda^4 \mathscr{O}_\lambda$)
$\iff \langle u, \beta \rangle_\lambda^3 = 1$
The last line is obviously true because $\langle u, \beta \rangle_\lambda$ is a 3rd-root of unity by definition so its cube must be 1. Now, follow the reverse implications to arrive back at the statement of the claim, which must now be true.

Now, assume that $\alpha \equiv \beta \equiv 1$ mod $\lambda^2 \mathscr{O}_\lambda$. Write $\alpha = 1 + a\lambda^2$ for some $a \in \mathscr{O}_\lambda$, and $\beta = 1 + b\lambda^2$ for some $b \in \mathscr{O}_\lambda$. Property 3 of the Hilbert Symbol in Lemma 7.3 says that $\langle \alpha, 1 - \alpha \rangle_\lambda = 1$. We also observe that $1 - (1 + a\beta\lambda^2) = -a\beta\lambda^2$ (note that we are writing $a\beta$ and not $\alpha\beta$). Applying property 3 of Lemma 7.3, we have:

$$\langle \alpha, 1 - \alpha \rangle_\lambda = \langle 1 + a\beta\lambda^2, -a\beta\lambda^2 \rangle_\lambda = 1$$

Next, we have that:

$$1 + a\beta\lambda^2 = 1 + a(1 + b\lambda^2)\lambda^2 = 1 + a\lambda^2 + ab\lambda^4$$

$$1 + a\lambda^2 + ab\lambda^4 \equiv 1 + a\lambda^2 \; (mod \; \lambda^4 \mathscr{O}_\lambda)$$

So now we can apply the claim above to obtain:

$$1 = \langle 1 + a\beta\lambda^2, -a\beta\lambda^2\rangle_\lambda = \langle 1 + a\lambda^2, -a\beta\lambda^2\rangle_\lambda$$

Next, we observe that the Hilbert Symbol $\langle -, -\rangle_\lambda$ is also multiplicative in the second argument. We can use property (4) in Lemma 7.3 to swap the arguments and pass to the inverse, apply multiplicativity in the first argument as proven above, and then apply Lemma 7.3 (4) again to swap the arguments back. The "inverse" part does not affect the result because the Galois group is abelian. Then, we have:
$1 = \langle 1 + a\beta\lambda^2, -a\beta\lambda^2\rangle_\lambda$
$= \langle 1 + a\lambda^2, -a\beta\lambda^2\rangle_\lambda$
$= \langle 1 + a\lambda^2, -a\lambda^2\rangle_\lambda \langle 1 + a\lambda^2, \beta\lambda^2\rangle_\lambda$ *(Follows by multiplicativity in the second argument)*
$= \langle 1 + a\lambda^2, \beta\lambda^2\rangle_\lambda$ *(The first term above is of the form $\langle u, 1-u\rangle_\lambda$, so it is 1 by lemma 7.3) (3))*
$= \langle \alpha, \beta\lambda^2\rangle_\lambda$ *(We wrote α as $1 + a\lambda^2$ above)*
$= \langle \alpha, \beta\rangle_\lambda = 1$
And this completes the proof of cubic reciprocity.

□

8.4 Eisenstein Reciprocity

We now prove a very general reciprocity law for $K = \mathbb{Q}(\zeta_p)$, where ζ is a primitive p^{th} root of unity, and p is an odd prime number. The proof will follow the one given in [9]. Recall from definition 3.18 (ray class fields) that $K = \mathbb{Q}(\zeta_p)$ is the ray class field for the modulus $p\infty$, so any prime number q distinct from p is unramified in K, and its inertial degree is its multiplicative order modulo p. p itself is totally ramified, with $\lambda := 1-\zeta$ the unique prime element in $\mathscr{O}_K$ lying over it, up to associates.

We now give a more general definition of what it means for an element α in $\mathscr{O}_K$ to be primary. (Note that this agrees with the one given above in definition 8.6 in the case of $K = \mathbb{Q}(\omega)$):

Definition 8.8. *We call $\alpha \in \mathscr{O}_K$ **primary** if it is not a unit, is relatively prime to p, and is congruent modulo ζ^2 to a rational integer (a good, honest whole number in $\mathbb{Z}$).*

Although K is a complex field, the notion of being primary allows us to introduce an analogous notion of sign:

Proposition 8.9. *For any $\alpha \in \mathscr{O}_K$, there is a unique p^{th} root of unity ζ^c for which $\alpha\zeta^c$ is primary.*

Proof. The inertial degree of p is 1, so the inclusion $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathscr{O}_K/\lambda\mathscr{O}_K$ is an isomorphism. Hence, there exists $a \in \mathbb{Z}$ for which $\alpha \equiv a \ (mod\ \lambda)$.
Then, $\frac{\alpha-a}{\lambda} \in \mathscr{O}_K$, so again there exists $b \in \mathbb{Z}$ such that $\frac{\alpha-a}{\lambda} \equiv b \ (mod\ \lambda)$, hence $\alpha \equiv a + b\lambda \ (mod\ \lambda)$
Since α is relatively prime to λ, a is not divisible by p, so there is a unique solution $c \in \{0, 1, ..., p-1\}$ to the congruence $a \equiv bX \ (mod\ p)$. Modulo λ^2 we have:

$$\zeta^c = (1-\lambda)^c \equiv 1 - c\lambda$$

and so:

$$\alpha\zeta^c \equiv (a + b\lambda)(1 - c\lambda) \equiv a + (b - ac)\lambda \equiv a$$

The uniqueness of c is clear, as it is the only integer which makes $(b - ac)\lambda$ vanish modulo λ^2, and $a + k\lambda$ is never an integer for $k \in \mathbb{Z}\backslash\{0\}$.

□

.

Lemma 8.10. *Let q, r be rational numbers not divisible by p. Then, $\left(\frac{q}{r}\right)_p = 1$.*

Proof. Remember that we are in the field $K = \mathbb{Q}(\zeta)$. By multiplicativity, we may assume that r is a prime number. Let J be any prime ideal of $\mathscr{O}_K$ lying over r. First, suppose that r splits completely in K. Then:

$$r\mathscr{O}_K = \prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma J$$

so:

$$\left(\frac{q}{r}\right)_p = \prod_{\sigma \in Gal(K/\mathbb{Q})} \left(\frac{q}{\sigma J}\right)_p = \prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma \left(\frac{q}{J}\right)_p = N_{K/\mathbb{Q}} \left(\frac{q}{J}\right)_p$$

and the norm of a p^{th} root of unity for an odd prime p is 1. In the second equality, We can take σ out of the power residue symbol because the product is over all elements of $Gal(K/\mathbb{Q})$. So taking out σ amounts to permuting the terms in the product, and hence it doesn't change the final result.

Now, suppose that r does not split completely in K. Then, $r-1$ is not divisible by p. Now, the congruence $q \equiv X^p \ (mod\ r)$ is solvable if and only if $q^{\frac{r-1}{d}} \equiv 1 \ (mod\ r)$, where d is the greatest common divisor of $r-1$ and p. In this case $d = 1$, so the given congruence is solvable. So there exists a $y \in \mathbb{Z}$ for which $q \equiv y^p \ (mod\ r)$, hence modulo J. So:

$$\left(\frac{q}{J}\right)_p \equiv q^{\frac{N(J)-1}{p}} \equiv y^{N(J)-1} \equiv 1 \ (mod\ J)$$

Since $\left(\frac{q}{r}\right)_p$ is a product of various $\left(\frac{q}{J}\right)_p$ for prime ideals J lying over r, we can conclude that $\left(\frac{q}{r}\right)_p = 1$. □

Theorem 8.11 (Law of Eisenstein Reciprocity)**.** *If $\alpha \in \mathscr{O}_K$ is primary, and $a \in \mathbb{Z}$ is relatively prime to p and α, then:*

$$\left(\frac{\alpha}{a}\right)_p = \left(\frac{a}{\alpha}\right)_p$$

Proof. Let v be the place of K corresponding to λ, and let U be the units of $\mathscr{O}_v$. The Power Reciprocity Law tells us that:

$$\left(\frac{\alpha}{a}\right)_p \left(\frac{a}{\alpha}\right)_p^{-1} = \langle \alpha, a \rangle_v$$

So we just have to show that $\langle \alpha, a \rangle_v = 1$. We write U_n to mean the set of elements that are congruent to 1 $mod\ \lambda^n \mathscr{O}_v$. Since α is primary, there is an integer k such that $\alpha \equiv k \ (mod\ \lambda^2)$. Clearly k is a unit in $\mathscr{O}_v$, so $\frac{\alpha}{k} \in U_2$. Also, $a^{p-1} \equiv 1 \ (mod\ p)$, so $a^{p-1} \equiv 1 \ (mod\ \lambda^{p-1}\mathscr{O}_v)$, so $a^{p-1} \in U_{p-1}$. So by an application of Hensel's lemma, it follows that $\langle \frac{\alpha}{k}, a^{p-1} \rangle_v = 1$. Now:

$$1 = \langle \frac{\alpha}{k}, a^{p-1} \rangle_v = \langle \frac{\alpha}{k}, a \rangle_v^{p-1}$$

which implies that $\langle \frac{\alpha}{k}, a \rangle_v = 1$ as well, since $p-1$ is relatively prime to p. However:

$$\langle \frac{\alpha}{k}, a \rangle_v = \langle \alpha, a \rangle_v \langle k, a \rangle_v^{-1}$$

and the power reciprocity law gives:

$$\langle k, a \rangle_v = \left(\frac{\alpha}{a}\right)_p \left(\frac{a}{\alpha}\right)_p^{-1} = 1 \cdot 1 = 1$$

□

9 Further Directions

Here, we describe some possible continuations from the work done in this paper, or what we might have explored if we had more time. Some of these are more easily described and accessible, while others are massive, deep, and dark areas of mathematics where little is known. As such, this section is simply a laundry list along with a rough description of what we *wish* we could learn, know, or find out if we had an infinite amount of time remaining. It is not meant to be a list of topics to be mastered within the next year or decade. We have arranged them roughly in increasing order of "distance" from this paper.

9.1 Computational Class Field Theory

In our proofs of quadratic reciprocity (Theorem 3.23) and cubic reciprocity (Theorem 8.7), we relied on some special tricks to establish the results. For quadratic reciprocity, it was the fact that there was only one possible homomorphism from $(\mathbb{Z}/p\mathbb{Z})^*$ to ± 1. For cubic and eisenstein reciprocity, we relied on Hensel's lemma to establish congruence relations modulo $\lambda = 1 - \zeta$. However, the proofs of the power reciprocity and hilbert reciprocity laws does not use any of these tricks and tools; they only used properties of the Hilbert Symbol. The Hilbert Symbol is defined as:

$$\langle \alpha, \beta \rangle_v = \frac{\Phi_{E^v/K_v}(\alpha)(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}$$

where $\Phi_{E^v/K_v}(\alpha)$ is determined by Local Artin Reciprocity. It would certainly make things much clearer if we had a direct way of computing $\Phi_{E^v/K_v}(\alpha)$ explicitly. Then, we can directly use this to compute the Hilbert Symbol, and then apply it to prove the reciprocity laws. Making such computations explicit would be the natural next step.

9.2 Hilbert's Twelveth Problem

The Kronecker-Weber Theorem (Theorem 3.17) says that any finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. Hilbert's twelveth problem asks to generalise this to a more general algebraic number field K. The answer to this question has been worked out only when K is a *CM-field*, fields that are closely related to the theory of complex multiplication of elliptic curves. This leads us to the next possible area of exploration.

9.3 Elliptic Curves and Complex Multiplication

Mathematical definitions and results from this subsection are taken from [11].

Elliptic curves have two kinds of structures: they can both be viewed both as groups and as an algebraic varieties. Structure preserving maps between groups are group homomorphisms, while for algebraic varieties they are rational maps. Putting both of them together, we get the definition of a structure preserving maps for elliptic curve, called an **isogeny**. An **isogeny** of elliptic curves E_1 to E_2 is a non-constant rational map that is also a group homomorphism. (In particular the constant map $E \longrightarrow \mathcal{O}$ is not an isogeny. Here, $\mathcal{O}$ is the identity element in the group of the elliptic curve) Given an elliptic curve E, we can consider the set of all isogenies from E to itself, together with the constant map (that was defined above to not be an isogeny). We can turn this set into

a ring, by defining multiplication as composition of isogenies and addition as addition of points on the elliptic curve in the target. This ring is called the **endomorphism ring of** E.

The classification theorem says that for an elliptic curve E defined over a field K, its endomorphism ring is either $\mathbb{Z}$ or an order in an imaginary quadratic field if K has characteristic 0. An order in a quadratic field F is a subring of F that is a finitely generated $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis of F.

Another result in complex multiplication then says that the j-invariant of an elliptic curve, together with complex multiplication and its torsion points, can be used to generate the Hilbert Class Field and Ray Class Fields of an imaginary quadratic field. In section 3, the Takagi Existence Theorem (Theorem 3.14) proved their existence, and they were formally defined in definitions 3.18 and 3.19. Complex multiplication gives a way to compute them explicitly, and thus it is another natural next step.

9.4 Non-abelian Class Field Theory

This is perhaps the most interesting of all. This subsection is a brief introduction to the Langlands Program, with information mainly drawn from [4], a paper titled "An elementary introduction to the langlands program" by Stephen Gelbart, published in the AMS Bulletin in 1984.

Abelian Class Field Theory generalises quadratic reciprocity into higher power reciprocity laws by working in cyclotomic fields $\mathbb{Q}(\zeta_n)$. It also gives a criterions for splitting of primes in abelian extensions. Let E be a Galois extension of $\mathbb{Q}$, and let $G = Gal(E/\mathbb{Q})$. Let $\mathfrak{p}$ be a prime ideal in $\mathscr{O}_\mathbb{Q}$ (which is really just the integers in disguise), and let $\mathfrak{P}_i$ be the prime ideals of $\mathscr{O}_E$ that appear in the factorization:

$$\mathfrak{p}\mathscr{O}_E = \prod \mathfrak{P}_i$$

A well-known theorem then says that G acts transitively on the $\mathfrak{P}_i$'s. Thus, the "splitting type" of $\mathfrak{p}$ in $\mathscr{O}_E$ is completely determined by the subgroup of G which fixes any of the $\mathfrak{P}_i$, i.e. by the "isotropy" groups G_i which are conjugate in G. For simplicity, assume that the $\mathfrak{P}_i$s are distinct, i.e. $\mathfrak{p}$ is unramified in E. To obtain information on the factorization of $\mathfrak{p}$, we direct our attention on the frobenius element $Fr_{\mathfrak{P}_i}$ of G, the canonical generator of the subgroup of G which maps any $\mathfrak{P}_i$ to itself. $Fr_{\mathfrak{P}_i}$ is determined only *up to conjugacy* in G, but this conjugacy class (now written as $Fr_\mathfrak{p}$) completely determines the factorization type of $\mathfrak{p}$. For example, when $Fr_\mathfrak{p}$ is the class of the identity alone, then, and only then, $\mathfrak{p}$ splits completely in E.

In general, we seek to describe $\mathfrak{p}$ intrinsically in terms of $\mathfrak{p}$ and the arithmetic of $\mathbb{Q}$. For abelian extensions, we have Emil Artin's Reciprocity Law. It implies that the splitting properties of $\mathfrak{p}$ in E depends only on its residue modulo some fixed modulus N (depending on E). Artin's reciprocity law also implies the higher reciprocity laws of abelian Class Field Theory, which is what sections 1 to 8 of this paper have been about.

The natural question to ask now is: What happens when we move to non-abelian Galois extensions? How can $Fr_\mathfrak{p}$ and the splitting behaviour of $\mathfrak{p}$ be described in terms of the ground field $\mathbb{Q}$?

Artin focused his attention on n-dimensional representations of $Gal(E/\mathbb{Q})$ over $\mathbb{C}$. i.e. homomorphisms $\sigma : Gal(E/\mathbb{Q}) \longrightarrow GL_n(\mathbb{C})$. Thus, for analysing conjugacy classes, he also had the tools of linear algebra. Artin also introduced analytic objects known as Artin L-functions, which made available tools from complex analysis to study the problem as well. The original problem therefore reduces to describing these L-functions in terms of the arithmetic of $\mathbb{Q}$. It was in this context that Artin proved his reciprocity law.

When $Gal(E/\mathbb{Q})$ is abelian, the irreducible representations are 1-dimensional. The Langlands Program aims to answer this question for higher dimensional representations, which means for the case that $Gal(E/\mathbb{Q})$ is non-abelian. To begin on this subject, a good starting point would be the study of modular forms and elliptic curves.

References

[1] David A.Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, Inc., 2013.

[2] Keith Conrad. History of class field theory. https://kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf. Accessed: 14 June 2022.

[3] Keith Conrad. Infinite galois theory. https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf, 2020. Accessed: 31 March 2022.

[4] Stephen Gelbart. an elementary introduction to the langlands program. *Bulletin of the American Mathematical Society*, 10:177–220, 1984. Direct link: https://projecteuclid.org/journals/bulletin-of-the-american-mathematical-society-new-series/volume-10/issue-2/An-elementary-introduction-to-the-Langlands-program/bams/1183551573.full.

[5] Gerald J. Janusz. *Algebraic Number Fields, Second Edition.* American Mathematical Society, 1996.

[6] I.G.MacDonald M.F.Atiyah. *Introuduction to Commutative Algebra.* Addison-Wesley Publishing Company, 1969.

[7] Jean-Pierre Serre. *Local Fields.* Springer-Verlag, 1980.

[8] Jean-Pierre Serre. *A Course in Arithmetic.* Springer-Verlag, 1996.

[9] Freydoon Shahidi. Lecture notes on class field theory. https://www.math.purdue.edu/people/bio/fshahidi/Notes2014. Accessed: 31 March 2022.

[10] Parvati Shastri. Reciprocity laws: Artin-hilbert. https://www.bprim.org/sites/default/files/rlmain.pdf. Accessed: 21 May 2022.

[11] Andrew Sutherland. Massachusetts institue of technology course 18.783 - elliptic curves lecture notes. https://ocw.mit.edu/courses/18-783-elliptic-curves-spring-2021/pages/lecture-notes-and-worksheets/. Accessed: 11 June 2022.

[12] Andrew Sutherland. Massachusetts institue of technology course 18.785 - number theory lecture notes, lectures 20, 21, and 24. https://math.mit.edu/classes/18.785/2019fa/lectures.html. Accessed: 31 March 2022.

[13] Andrew Sutherland. Massachusetts institue of technology course 18.786 - number theory 2 lecture notes, lecture 31. https://math.mit.edu/classes/18.786/LectureNotes31.pdf. Accessed: 19 May 2022.