CLASS FIELD THEORY AND THE KRONECKER-WEBER THEOREM

TANVIR AHMED

Abstract. In this paper, we outline enough class field theory to establish the statement of Takagi's Existence Theorem and how the Kronecker-Weber Theorem is the special of the Existence Theorem where the base field is $\mathbb{Q}$. We also outline a proof of the theorem without the use of these class field theory statements, many of which are quite difficult to prove. This approach reduces Kronecker-Weber to proving the theorem over local fields, which are finite extensions of $\mathbb{Q}_p$ for primes p.

Contents

1. Introduction

A proof of the Kronecker-Weber Theorem was first announced by Leopold Kronecker in 1853, but the proof was not correct. The statement of the theorem is Theorem 2.1. The main issue he had in his proof is that he didn't address extensions of degree a power of 2 properly. Weber then published a proof in 1886, which was largely accepted, but it also had similar errors to Kronecker. The first correct proof was by Hilbert in 1896, who also made other conjectures in Algebraic Number Theory, such as about the Hilbert Class Field.

These ideas that Hilbert was working with were the start of Class Field Theory, which deals with abelian extensions of a field. For example, the Kronecker-Weber Theorem says that abelian extensions of $\mathbb{Q}$ have this special property that they're subfields of cyclotomic fields, and it is very easy to prove that subfields of cyclotomic fields are abelian. Thus, being an abelian extension of $\mathbb{Q}$ is equivalent to being a subfield of a cyclotomic field.

One well-known consequence is Gauss Sums. For example, consider the two identities:

$$\pm\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$$
$$\pm\sqrt{-7} = \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6$$

where ζ_5 and ζ_7 are primitive 5th and 7th roots of unity respectively. What this means in terms of Kronecker-Weber is that $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$ and $\mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$, so the extensions $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-7})$ have this property of being abelian. In general, if α is an algebraic number such that $\mathbb{Q}(\alpha)$ has this abelian property, α can be expressed as a sum of roots of unity.

The ideas in class field theory related to this theorem run very deep; although Kronecker-Weber was proved by the 1900s, it wasn't until 1920 when Teiji Takagi proved the existence of ray class fields, which essentially play the role cyclotomic extensions do over $\mathbb{Q}$ but for any base field K. Then, in 1927, Artin made Takagi's results more explicit by proving Artin Reciprocity, which not only provides a generalization of reciprocity laws like quadratic reciprocity (exclusive to abelian extensions), but also advanced the study of class field theory in general. Around this time, Class Field Theory was also developed through analysis, such as with Hecke's work on L-functions and Chebatorev's Density Theorem.

2. Algebraic Number Theory

In the study of Class Field Theory, knowledge of Algebraic Number Theory and of Galois Theory is essential, so let us go over some of the basic ideas relevant to these subjects. In Algebraic Number Theory, we are mostly studying **number fields**, which are finite extensions of $\mathbb{Q}$, such as $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{2}, i)$. Given a number field K, we might extend it and obtain a new number field L. In this case, we write L/K to indicate that L is an extension of K. Any extension of a field can be thought of as a vector space over the base field, and given an extension L/K, the degree of the extension is the dimension of this vector space.

For any extension L/K, we can consider the group of automorphisms $\mathrm{Aut}(L/K)$, which consists of all field automorphisms from L to itself which fix all elements of K. In the special case where L/K is a finite Galois extension, we have $|\operatorname{Aut}(L/K)| = [L : K]$, and we write $\mathrm{Gal}(L/K)$ instead of $\mathrm{Aut}(L/K)$. Recall that an extension of fields L/K is Galois if both:

(1) Every irreducible polynomial in $K[x]$ which has a root in L has all its roots in L.
(2) The minimal polynomial over K of every $\alpha \in L$ is separable.

A field extension with the first property is normal, and a field extension with the second property is separable. It is also well-known that an extension L/K is Galois if and only if L is the splitting field over K of some set of separable polynomials. This characterization is usually easier to think about.

If an extension L/K is Galois and has an abelian Galois group, we say the extension is abelian. The main theorem we will prove in this paper is the Kronecker-Weber Theorem, which can be stated as follows:

Theorem 2.1. *Every abelian extension K of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{Z}$.*

As a brief review of Galois theory, we will prove a lemma about the compositum of multiple field extensions. We will restrict our attention to finite extensions only. In particular, given a base field F, suppose A and B are finite extensions of F. Then, the smallest field generated by A and B is called the **compositum** of A and B, which is denoted by AB. We now prove the following theorem.

Theorem 2.2. *Suppose A/F and B/F are finite Galois extensions of some field F. Then, $A \cap B/F$ and AB/F are also finite Galois extensions, and we have 2 canonical injective maps:*

$$\mathrm{Gal}(AB/A) \to \mathrm{Gal}(B/F)$$
$$\mathrm{Gal}(AB/F) \to \mathrm{Gal}(A/F) \times \mathrm{Gal}(B/F).$$

Furthermore, these are both isomorphisms if and only if $F = A \cap B$.

Proof. Suppose A and B are the splitting fields of $f, g \in F[x]$ respectively. Then, $A \cap B$ is the splitting field of $\gcd(f, g)$ and AB is the splitting field of fg, so they are both Galois.

Let $G_A = \mathrm{Gal}(AB/A)$, $G_B = \mathrm{Gal}(AB/B)$, and $G_F = \mathrm{Gal}(AB/F)$. For the first statement, we consider the map $\sigma \to \sigma \mid_B \colon G_A \to \mathrm{Gal}(B/F)$, which restricts automorphisms in G_A to the field B. This is clearly a homorphism, and it has a trivial kernel since if $\sigma \in G_A$ is such that $\sigma \mid B$ fixes all elements of B, σ fixes both A and B. Thus, it must fix AB, and is thus trivial. Thus, $\sigma \to \sigma \mid_B$ is injective.

Now we will suppose that $F = A \cap B$ and prove that the map is surjective. Consider the image of G_A under this homomorphism, which we will denote by $G_A \mid_B$. By the Galois correspondence, this subgroup is equal to all of $\mathrm{Gal}(B/F) = \mathrm{Gal}(B/A \cap B)$ if and only if the fixed field of $G_A \mid_B$ is $A \cap B$. Suppose $\beta \in B$ is fixed by all elements of $G_A \mid_B$. Then, β is fixed by all elements of G_A, which has fixed field A. Thus, $\beta \in A \cap B$. Thus, the fixed field of the image of $G_A \mid_B$ is $A \cap B$, so we have an isomorphism between G_A and $\mathrm{Gal}(B/A \cap B)$.

For the second part, we consider the map $\sigma \to (\sigma \mid_A, \sigma \mid_B) : G_F \to \mathrm{Gal}(A/F) \times \mathrm{Gal}(B/F)$. This is clearly a homomorphism, and the kernel is injective because if $\sigma \in G_F$ maps to $(\mathrm{id}_A, \mathrm{id}_B)$, σ fixes A and B, so it must fix AB. Furthermore, in the case where $F = A \cap B$, using the first isomorphism we established, we have

$$\begin{aligned} |G_F| &= [AB : A \cap B] \\ &= [AB : A][A : A \cap B] \\ &= [B : A \cap B][A : A \cap B] \\ &= |G_A||G_B| \\ &= |G_A \times G_B|. \end{aligned}$$

Thus, we have an isormophism between G_F and $\mathrm{Gal}(A/F) \times \mathrm{Gal}(B/F)$. One thing we haven't shown yet is that if $F \neq A \cap B$, the maps are not isomorphisms. However, in this case, F is a proper subfield of $A \cap B$, so one can check that the orders of the groups on either side of each isomorphism are not the same, once again given that $A \cap B$ makes these isomorphisms. ■

Corollary 2.3. *Let A and B be abelian extensions of F. Then, AB is also an abelian extension.*

Proof. By Theorem 2.2, $\mathrm{Gal}(AB/F)$ is isomorphic to a subgroup of $\mathrm{Gal}(A/F) \times \mathrm{Gal}(B/F)$, which is an abelian group by assumption. Thus, AB/F is abelian. ■

Given a number field K, we let $\mathcal{O}_K$ denote its ring of integers; the set of elements of K which satisfy a monic polynomial with integer coefficients (over $\mathbb{Q}$). Though we will not prove it, it is well known that $\mathcal{O}_K$ is actually a ring. Here are examples of the ring of integers for two different number fields.

Example. The ring of integers of $\mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$ is a $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \bmod 4$ and $\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ if $d \equiv 1 \bmod 4$. Note we can assume $d \not\equiv 0 \bmod 4$ because then, d wouldn't be squarefree.

Example. The ring of integers of the mth cyclotomic extension $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$. This fact makes working with cyclotomic extensions easier than arbitrary extensions of $\mathbb{Q}$.

For a number field K, the ideals of $\mathcal{O}_K$ play a very important role in the multiplicative structure of the $\mathcal{O}_K$. In particular, given two ideals $\mathfrak{a}, \mathfrak{b} \in \mathcal{O}_K$, the product $\mathfrak{ab}$ is generated by the set $\{\alpha\beta \mid \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}$. It turns out that under this notion of multiplication, the ideals of $\mathcal{O}_K$ have unique factorization; that is, there are certain prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots \subset \mathcal{O}_K$ such that any nonzero ideal $\mathfrak{a}$ can be written uniquely as a product of these prime ideals.

In the case of $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, which is a PID, so every ideal is generated by a single element. Thus, multiplication of ideals is essentially the same as multiplication of integers, and up to sign, integers have unique factorization. The statement of unique ideal factorization takes care of the sign issue easily however since the ideal (a), the principal ideal generated by an integer a, is the same as $(-a)$.

$\mathcal{O}_K$ is not always a PID, and it is often much more complicated than being a PID. Recall the definition of the class group, which describes the different types of ideals that exist in $\mathcal{O}_K$. Before we can introduce the notion of a class group, we need to quickly define that of a fractional ideal.

Definition 2.4. Given a number field K, a fractional ideal of $\mathcal{O}_K$ is of the form $\alpha\mathfrak{a}$ where $\alpha \in K^\times$ and $\alpha \subset \mathcal{O}_K$ is an (integral) ideal of $\mathcal{O}_K$.

It turns out that under this definition, every nonzero fractional ideal has an inverse; that is, if A is a nonzero fractional ideal, there is some nonzero fractional ideal A^{-1} such that $AA^{-1} = \mathcal{O}_K$. Thus, fractional ideals form an abelian multiplicative group, and we call this group I_K. Furthermore, we define P_K to be the group of principal nonzero fractional ideals, which are of the form $\alpha\mathcal{O}_K$ for $\alpha \in K^\times$. Then, we define the class group $\mathrm{Cl}(K)$ as

$$\mathrm{Cl}(K) := I_K/P_K.$$

The fact that we are modding out by P_K indicates that two ideals are in the same ideal class if their quotient (in this larger group of fractional ideals) is principal. Thus, the class group contains all the different types of ideals. If the class group is trivial, then all ideals

are principal, and $\mathcal{O}_K$ is a PID, which implies that there is unique factorization up to units. However, the class group is usually more complicated than this.

3. Ramification Theory

From Algebraic Number Theory, we know that given a number field K, while $\mathcal{O}_K$ is not necessarily a PID, the set of ideals of $\mathcal{O}_K$ has unique factorization. In other words, there is some set of prime ideals such that every nonzero ideal of $\mathcal{O}_K$ factors uniquely as a product of powers of those prime ideals. For example, $\mathbb{Q}$ is a PID, so the prime ideals of $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$ are (p) for primes $p \in \mathbb{Z}$.

Similarly, we can consider $\mathbb{Q}(i)$, whose ring of integers $\mathbb{Z}[i]$, is also a PID, so the prime ideals of $\mathbb{Z}[i]$ are $(a+bi)$ for Gaussian primes $a+bi$. Now we will consider how rational primes p factor in $\mathbb{Z}[i]$. If $p \in \mathbb{Z}$ is a rational prime, we have $N_{\mathbb{Q}(i)/\mathbb{Q}}(p) = p^2$, so if p were to split into primes in $\mathbb{Z}[i]$, it could only split into at most two primes, each of which with norm p (we should really be considering the ideal (p) here, but considering individual elements suffices since we're in a PID). If a prime $a + bi \in \mathbb{Z}[i]$ has norm p, that means that $a^2 + b^2 = p$. By Fermat's Christmas Theorem, this is only the case when $p \equiv 1 \bmod 4$ or $p = 2$. In the case $p \equiv 1 \bmod 4$, we just have $p = (a + bi)(a - bi)$. One can check in this case that $a + bi$ and $a - bi$ are indeed distinct primes, meaning that the ideals $(a + bi)$ and $(a - bi)$ are distinct. Thus, in the case $p \equiv 1 \bmod 4$, p **splits** into a product of 2 distinct primes. In the case $p \equiv 3 \bmod 4$, p remains prime in $\mathbb{Z}[i]$, and we say that p is **inert**. However, something funny happens with $p = 2$. Recall that $2 = (1 + i)(1 - i)$, but the ideals $(1 + i)$ and $(1 - i)$ are the same since $1 - i = -i(1 + i)$. Thus, we really have

$$(2) = (1 + i)^2.$$

Thus, we say that 2 ramifies in $\mathbb{Z}[i]$. Our next goal is to be able to generalize all these notions to general extensions of number fields.

3.1. **Primes over general extensions of number fields.** Let L/K be an extension of number fields. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. We can naturally embed $\mathcal{O}_K$ as a subring of $\mathcal{O}_L$, so we can also regard $\mathfrak{p}$ as an ideal of $\mathcal{O}_L$; in particular, by $\mathfrak{p}$, we mean both the prime ideal in $\mathcal{O}_K$ as well as the ideal generated by $\mathfrak{p}$ after being embed into $\mathcal{O}_L$, which can also be thought of as $\mathfrak{p}\mathcal{O}_L$.

For example, the ideal (2) in $\mathbb{Z}$ is $2\mathbb{Z}$. However, when we lift this ideal up to $\mathbb{Z}[i]$, it becomes the ideal generated by $2\mathbb{Z}$, which is $2\mathbb{Z}[i]$. Either way, we denote these both by (2), and it will usually be clear based on context what we mean.

The ideal $\mathfrak{p} \in \mathcal{O}_L$ will factor into some product of primes. Suppose we have

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

where the $\mathfrak{P}_i$'s are distinct primes of L and $e_i \geq 1$ for $1 \leq i \leq g$. We say that each of the $\mathfrak{P}_i$'s are primes lying **above** $\mathfrak{p}$. We say that $\mathfrak{p}$ stays inert if $g = e_1 = 1$, which is equivalent to $\mathfrak{p}$ staying prime in $\mathcal{O}_L$. We say that $\mathfrak{p}$ splits completely if $g = [L : K]$, and as we will see later, this will imply that $e_i = 1$ for $1 \leq i \leq g$. Furthermore, we say that $\mathfrak{p}$ ramifies if $e_i > 1$ for some $1 \leq i \leq g$.

Recall that $\mathcal{O}_K$ is a Dedekind domain, and Dedekind domains have the nice property that prime ideals are maximal, so $\mathfrak{p}$, which is a prime ideal of $\mathcal{O}_K$, is also a maximal ideal. Thus, $\mathcal{O}_K/\mathfrak{p}$ is a field. It turns out that $\mathcal{O}_K/\mathfrak{p}$ is also a finite field (see [Mar18] Theorem 14, which is a different statement, but the proof establishes this fact along the way).

Proposition 3.1. *$\mathcal{O}_K/\mathfrak{p}$ is a subfield of $\mathcal{O}_L/\mathfrak{P}_i$.*

Proof. Consider the map from $\mathcal{O}_K \to \mathcal{O}_L/\mathfrak{P}_i$ given by $\alpha \to \alpha \bmod \mathfrak{P}_i$. The kernel of this map is the set of elements in $\mathcal{O}_K$ which are $0 \bmod \mathfrak{P}_i$. Recall that this is exactly $\mathcal{O}_K \cap \mathfrak{P}_i = \mathfrak{p}$. Thus, there is an injective homomorphism from $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{P}_i$, which is what we wanted to show. ∎

If we now write $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$, then it is well known that any finite field containing $\mathbb{F}_q$ must be of the form $\mathbb{F}_{q^f}$ for some f. Now let f_i be such that $\mathcal{O}_L/\mathfrak{P}_i = \mathbb{F}_{p^{f_i}}$. We call the f_i's the inertial degrees. There is the following useful relationship between the e_i's and f_i's.

Theorem 3.2. *Let L/K be an extension of number fields, and $\mathfrak{p} \in \mathcal{O}_K$ a prime. Suppose $\mathfrak{p}$ splits as*

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

for distinct primes $\mathfrak{P}_i \in \mathcal{O}_L$. Then, we have

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

Proof. See [Mar18] Theorem 21. ∎

3.2. **Galois Extensions.** In the case where L/K is a Galois extension, prime decomposition becomes much simpler. In particular, let L/K be a Galois extension of number fields with Galois Group G. Furthermore, let $\mathfrak{p}$ be a prime in K. We can factor $\mathfrak{p}$ over L as

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

for distinct primes $\mathfrak{P}_i$ in L. Now let $\sigma \in G$. Then, $\sigma(\mathfrak{p}) = \mathfrak{p}$ because $\mathfrak{p}$ is generated by elements in $\mathcal{O}_K$, which are fixed by σ. Thus, we can apply σ to both sides of this equality, so

$$\sigma(\mathfrak{p}) = \mathfrak{p} = \sigma(\mathfrak{P}_1)^{e_1} \dots \sigma(\mathfrak{P}_g)^{e_g}. \tag{3.1}$$

It is a very easy algebra exercise to show that if $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(\mathfrak{P}_i)$ is a prime ideal in $\mathcal{O}_L$. Thus, G acts on the prime ideals above $\mathfrak{p}$. In fact, the Galois group acts on the $\mathfrak{P}_i$'s transitively, which we will not prove.

Proposition 3.3. *Let L/K be a Galois extension with Galois group G. If $\mathfrak{p}$ is a prime in K and $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ are the distinct primes above $\mathfrak{p}$ in L, then for any $1 \le i < j \le g$, there is some $\sigma \in G$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.*

Proof. See [Mar18] Theorem 23. ∎

This allows us to easily prove the following fact:

Theorem 3.4. *Let L/K be a Galois extension of number fields and $\mathfrak{p} \subset \mathcal{O}_K$ a prime. If $\mathfrak{p}$ factors in $\mathcal{O}_L$ as $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ for distinct primes $\mathfrak{P}_i \subset \mathcal{O}_L$, then $e_1 = \cdots = e_g$ and $f_1 = \cdots = f_g$, where f_i is the inertial degree of $\mathfrak{P}_i$.*

Proof. Returning back to 3.1, we have factored $\mathfrak{p}$ into g prime powers, namely the $\sigma(\mathfrak{P}_i)^{e_i}$'s, and there is only one way to do that. Thus, σ permutes the $\mathfrak{P}_i$'s. This means that if $\sigma(\mathfrak{P}_1) = \mathfrak{P}_i$, then the exponent of $\mathfrak{P}_i$ in the factorization of $\mathfrak{p}$ is e_1, but it is also e_i, so $e_1 = e_i$. Because G acts transitively on the primes above $\mathfrak{p}$, we can choose i to be anything between 1 and g, so we have $e_1 = \cdots = e_g$.

We can also show that inertial degrees are all equal. To do this, we just need to show that $\mathcal{O}_L/\mathfrak{P}_i$ and $\mathcal{O}_L/\mathfrak{P}_j$ are isomorphic for any $1 \leq i, j \leq g$. To do this, let $\sigma \in G$ be such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ and consider the map from $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}_j$ given by $\alpha \to \sigma(\alpha) \bmod \mathfrak{P}_j$. The kernel of this map is all α such that $\sigma(\alpha) \in \mathfrak{P}_j$, which is equivalent to $\alpha \in \sigma^{-1}(\mathfrak{P}_j) = \mathfrak{P}_i$. Thus, we have $\mathcal{O}_L/\mathfrak{P}_i \cong \mathcal{O}_L/\mathfrak{P}_j$. This implies $f_1 = \cdots = f_g$. ■

Now let $e = e_1 = \cdots = e_g$ be the common ramification index and $f = f_1 = \cdots = f_g$ the common inertial degree. Then, by Theorem 3.2, we conclude that $efg = [L : K]$. Finally, we have the following definition:

Definition 3.5. An extension L/K is **unramified** if no primes in $\mathcal{O}_K$ ramify in $\mathcal{O}_L$.

3.3. **Examples.** We can create many examples of prime factorization by using the Dedekind-Kummer Theorem, which is an algorithm for factoring a prime over a monogenic extension.

Theorem 3.6 (Dedekind-Kummer)**.** *Let L/K be a monogenic extension, meaning $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$. Let $f \in \mathcal{O}_K[x]$ be the minimal polynomial of α. Then, if $\mathfrak{p} \subset \mathcal{O}_K$ is a prime, $\mathfrak{p}$ factors in $\mathcal{O}_L$ as*

$$\mathfrak{p} = \prod_{i=1}^{g} (\mathfrak{p}, f_i(\alpha))^{e_i}$$

where $f(x) \equiv \prod_{i=1}^{g} f_i(x)^{e_i} \bmod \mathfrak{p}$. Furthermore, the $(\mathfrak{p}, f_i(\alpha))$'s are prime ideals of $\mathcal{O}_L$.

For example, consider $K = \mathbb{Q}(\zeta_5)$. To factor the prime 11 over this extension, we need to factor the 5th cyclotomic polynomial $x^4 + x^3 + x^2 + x + 1 \bmod 11$, which factors as $(x-3)(x-4)(x-5)(x-9)$. Thus, (11) factors in $\mathbb{Z}[\zeta_5]$ as

$$(11) = (11, \zeta_5 - 3)(11, \zeta_5 - 4)(11, \zeta_5 - 5)(11, \zeta_5 - 9).$$

Thus, 11 completely splits since $g = 4 = [\mathbb{Q}(\zeta_5) : \mathbb{Q}]$. Now let's look at 5 splits. Notice that the 5th cyclotomic polynomial mod 5 is

$$\frac{x^5 - 1}{x - 1} \equiv \frac{(x-1)^5}{x-1} \equiv (x-1)^4 \bmod 5.$$

Thus, (5) factors as $(5) = (5, \zeta_5 - 1)^4$. Thus, 5 is ramified.

3.4. **The Discriminant of a Number Field.** Given an extension of number fields L/K with $[L : K] = n$, there are n embeddings (injective homomorphisms) of L into $\mathbb{C}$ fixing K. Furthermore, recall that $\mathcal{O}_L$ forms a lattice in K; in technical terms, it is a free $\mathcal{O}_K$-module of rank n. Suppose $\mathcal{O}_L$ has basis $\alpha_1, \ldots, \alpha_n$ over $\mathcal{O}_K$ and that $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. The relative discriminant of L/K, denoted $\Delta_{L/K}$, essentially measures how spread out the lattice $\mathcal{O}_L$ is in L. It is an ideal of $\mathcal{O}_K$, defined as follows:

$$\Delta_{L/K} := \left(\det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}^2 \right) \cdot \mathcal{O}_K$$

It can be shown that the determinant squared used in this definition is an element of K and that it is independent of the basis chosen for $\mathcal{O}_L$. In the special case where $\mathcal{O}_L$ is monogenic with $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, we can choose the basis $1, \alpha, \ldots, \alpha^{n-1}$ in the definition above,

and the determinant simplifies into a Vandermonde determinant. If we let $f \in \mathcal{O}_K[x]$ be the minimal polynomial of α, having roots $\alpha = \alpha_1, \ldots, \alpha_n$, then $\Delta_{L/K}$ has the following value:

$$\Delta_{L/K} = \left(\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \right) \cdot \mathcal{O}_K.$$

The expression on the right-hand side of this equation is also the definition of the discriminant of f, which we will denote Δ_f. In particular, the discriminant is invariant under any permutation of the roots, so it can be expressed as a polynomial in the symmetric polynomials of the α_i's. Thus, $\Delta_f \in \mathcal{O}_K$, since the values of the symmetric polynomials are the coefficients of f, which are in $\mathcal{O}_K$.

Let's continue with the same setup as before, in which $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ where $\alpha \in \mathcal{O}_K$ has minimal polynomial f. Furthermore, let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime. By the Dedekind-Kummer Theorem, we can find the factorization of $\mathfrak{p}$ in $\mathcal{O}_L$ by factoring $f \bmod \mathfrak{p}$. In particular, suppose

$$f \equiv f_1^{e_1} \ldots f_g^{e_g} \bmod \mathfrak{p}$$

for distinct irreducible polynomials $f_i(x) \in \mathcal{O}_K[x]$. Then, we have

$$\mathfrak{p} = (\mathfrak{p}, f_1(\alpha))^{e_1} \ldots (\mathfrak{p}, f_g(\alpha))^{e_g}$$

in $\mathcal{O}_L$. Notice that $\mathfrak{p}$ ramifies if and only one of the e_i's is greater than 1, which is equivalent to f having a double root mod $\mathfrak{p}$. This is only the case when $\Delta_f \equiv 0 \bmod \mathfrak{p}$. In other words, a prime $\mathfrak{p}$ ramifies in L/K if and only if $\mathfrak{p} \mid \Delta_{L/K}$. Although we have only considered the case where $\mathcal{O}_L$ is monogenic, it turns out that this fact is true in general, although the proof is not easy:

Theorem 3.7. *Let L/K be an extension of number fields. Then, a prime $\mathfrak{p} \subset \mathcal{O}_K$ ramifies in $\mathcal{O}_L$ if and only if $\mathfrak{p} \mid \Delta_{L/K}$.*

Proof. See [Neu07] Chapter 3 Section 2. ■

This also gives the following easy corollary:

Corollary 3.8. *For any extension of number fields L/K, there are only finitely many primes of $\mathcal{O}_K$ that ramify in $\mathcal{O}_L$.*

3.5. **Minkowski's Bound.** We will end this section with Minkowski's Bound, which will allow us to deduce that $\mathbb{Q}$ has no unramified extensions. Let K be a number field with $[K : \mathbb{Q}] = n$ which has $2s$ complex embeddings. Thus, $s \leq \frac{n}{2}$. We define

$$M_K = \sqrt{|\Delta_{K/\mathbb{Q}}|} \left(\frac{4}{\pi} \right)^s \frac{n!}{n^n}.$$

We then have the following statement of Minskowski's Bound:

Theorem 3.9. *Let K be a number field. Then, in every ideal class of K, there is an integral ideal with norm at most M_K.*

One application of this is the following theorem:

Theorem 3.10. *Given any number field K, Cl_K is finite.*

There is something else we can get out of this. Note that every integral idea has norm at least 1, so we have $M_K \geq 1$. In other words,

$$\begin{aligned}\sqrt{|\Delta_{K/\mathbb{Q}}|}\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} &\geq 1 \\ \iff \sqrt{|\Delta_{K/\mathbb{Q}}|} &\geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!} \\ &\geq \left(\frac{\pi}{4}\right)^{\frac{n}{2}} \frac{n^n}{n!}.\end{aligned}$$

Thus, we have the following theorem:

Theorem 3.11. *There are no nontrivial unramified extensions of* $\mathbb{Q}$.

Proof. Suppose $K/\mathbb{Q}$ is an unramified abelian extension of $\mathbb{Q}$. Then, $|\Delta_{K/\mathbb{Q}}| = 1$, so

$$1 \geq \left(\frac{\pi}{4}\right)^{\frac{n}{2}} \frac{n^n}{n!}.$$

This inequality only holds for $n = 1$, in which case we just have $K = \mathbb{Q}$. ∎

4. The Frobenius Element

Let L/K be a Galois extension with Galois group G. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ that splits as follows:

$$\mathfrak{p} = \mathfrak{P}_1^e \dots \mathfrak{P}_g^e.$$

Since G acts on the primes above $\mathfrak{p}$, we can consider the stabilizer subgroups of this action, which are known as the **decomposition groups**.

Definition 4.1. In the setup above, the decomposition group at the prime $\mathfrak{P}_i$ is

$$D_{\mathfrak{P}_i} = \{\sigma \in G \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}.$$

For now, let's restrict our attention to the case $e = 1$. We already established that G acts transitively on the $\mathfrak{P}_i$'s. It is a standard fact that for any group acting transitively on a set, there are an equal number of group elements taking any fixed element of the set to any other element of the set. Thus, since $|G| = fg$, the size of $D_{\mathfrak{P}_i}$ is exactly $\frac{fg}{g} = f$.

Given an element $\sigma \in D_{\mathfrak{P}_i}$, σ induces an automorphism on the residue field $\mathcal{O}_L/\mathfrak{P}_i$. In particular, we can consider the automorphism $\alpha \bmod \mathfrak{P}_i \to \sigma(\alpha) \bmod \mathfrak{P}_i$. Furthermore, σ must fix everything inside $\mathcal{O}_K/\mathfrak{p}$ (which can be naturally embedded in $\mathcal{O}_L/\mathfrak{P}_i$), so the automorphism induced by σ is in the Galois Group $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p}))$. It turns out that this map is also surjective (even in the case that $\mathfrak{p}$ doesn't ramify, see [Mar18] Theorem 28) Thus, since $|D_{\mathfrak{P}_i}| = |\mathcal{O}_L/\mathfrak{P}_i| = f$, we have an isomorphism $D_{\mathfrak{P}_i} \cong \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p}))$. However, recall that $\mathcal{O}_L/\mathfrak{P}_i$ and $\mathcal{O}_K/\mathfrak{p}$ are finite fields. In particular, if $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$, then $\mathcal{O}_L/\mathfrak{p}_i = \mathbb{F}_{q^f}$. It is well known that $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ is cyclic, where the generator is the map $a \to a^q$. This is is called the Frobenius map.

Now we know that $D_{\mathfrak{P}_i}$ is cyclic, so let $\sigma \in D_{\mathfrak{P}_i}$ be a generator. Then, σ must act as the Frobenius element on $\mathcal{O}_L/\mathfrak{P}_i$, so $\sigma(\alpha) \equiv \alpha^q \bmod \mathfrak{P}_i$. We call this σ the Frobenius element at $\mathfrak{P}_i$, which we will denote by $\sigma = \mathrm{Frob}_{\mathfrak{P}_i}$. The fact that Frobenius elements are unique is very useful because if we find that a certain element of the Galois Group has the defining property of the Frobenius element, then we know it must be the Frobenius element. There is also a useful relationship between the different Frobenius elements at the primes above $\mathfrak{p}$. In particular, they are conjugates of each other, as we will now prove:

Proposition 4.2. *Suppose L/K is a finite Galois extension of number fields, with $\mathfrak{p} \subset \mathcal{O}_K$ an unramified prime and $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ for primes $\mathfrak{P}_i \subset \mathcal{O}_L$. Then, if $\mu \in \mathrm{Gal}(L/K)$ such that $\mu(\mathfrak{P}_i) = \mathfrak{P}_j$ for $1 \leq i, j \leq g$, then*

$$\mu^{-1} \operatorname{Frob}_{\mathfrak{P}_j} \mu = \operatorname{Frob}_{\mathfrak{P}_i}$$

.

Proof. Let $\sigma = \operatorname{Frob}_{\mathfrak{P}_i}$ and $\tau = \operatorname{Frob}_{\mathfrak{P}_j}$. Let $\alpha \in \mathcal{O}_L$ and $q = |\mathcal{O}_K/\mathfrak{p}|$. Since $\alpha^q \equiv \tau(\alpha) \bmod \mathfrak{P}_j$ and $\mu^{-1}(\mathfrak{P}_j) = \mathfrak{P}_i$, $\mu^{-1}(\alpha^q) \equiv \mu^{-1}\tau(\alpha) \bmod \mathfrak{P}_i$. Thus, we have

$$\begin{aligned} \mu^{-1}\tau\mu(\alpha) &\equiv \mu^{-1}\left(\mu(\alpha)^q\right) \\ &\equiv \mu^{-1}\mu(\alpha^q) \\ &\equiv \alpha^q \bmod \mathfrak{P}_i. \end{aligned}$$

Thus, $\mu^{-1}\tau\mu$ is exactly the Frobenius map of $\mathcal{O}_L/\mathfrak{P}_i$, which is just σ. ∎

In the case where L/K is abelian, $\mu^{-1}\tau\mu = \tau = \sigma$, so all the Frobenius elements above any unramified prime $\mathfrak{p}$ must be the same. In this case, we write $\operatorname{Frob}_{\mathfrak{p}}$ as a stand-in for the common value of the $\operatorname{Frob}_{\mathfrak{P}_i}$'s.

4.1. **Frobenius and Splitting.** Suppose $\mathfrak{p}$ is unramified over the Galois extension L/K. If σ is the Frobenius element of one of the primes above $\mathfrak{p}$, then the order of σ is the inertial degree of $\mathfrak{p}$. Clearly, if we know the inertial degree of a prime, then we also know how many primes are above it. This is quite useful computationally, as we will demonstrate in the next few examples:

Example. We can prove Fermat's Christmas Theorem using Frobenius elements. We can restate this result as saying that all rational primes p with $p \equiv 1 \bmod 4$ split in $\mathbb{Q}(i)$ while those with $p \equiv 3 \bmod 4$ remain prime. The Galois Group of $\mathbb{Q}(i)/\mathbb{Q}$ is $\{1, \sigma\}$ where σ is complex conjugation. Now suppose an odd prime p remains inert in $\mathbb{Z}[i]$. Then, its Frobenius element is σ, and $\mathbb{Z}[i]/(p)$ is a field with p^2 elements. Therefore, we should have

$$(a + bi)^p \equiv a - bi \bmod p$$

for $a, b \in \mathbb{Z}$. But, since we are working in characteristic p, this implies $a^p + (bi)^p \equiv a - bi \bmod p$. Since $a, b \in \mathbb{Z}$, $a^p \equiv a \bmod p$ and $b^p \equiv b \bmod p$, so we should have $a + bi^p \equiv a - bi \bmod p$. This implies that we must have $p \equiv 3 \bmod 4$. The implication of $p \equiv 3 \bmod 4$ to p staying inert is easy since no sum of squares can be 3 mod 4 along with the fact that $\mathbb{Z}[i]$ is a PID.

Example. Suppose we wanted to find how 3 splits in $\mathbb{Q}[\zeta_{13}]$. The naive way to do this would be to factor the minimal polynomial ζ_{13}, which is degree 12 in $\mathbb{Z}/3\mathbb{Z}$. However, all we have to do is find the Frobenius element. The Frobenius element must act by raising everything to the 3rd power mod any of the primes above 3. No matter which prime above 3 we choose, the corresponding residue field is characteristic 3, so if we just choose the automorphism $\zeta_{13} \to \zeta_{13}^3$, this works. Composing this automorphism with itself is essentially equivalent to repeatedly multiplying by 3 and reducing by 13. Thus, the order of the Frobenius element is the multiplicative order of 3 mod 13, which can be checked to be 3. Thus, 3 splits into 4 primes, each of inertial degree 3 in $\mathbb{Z}[\zeta_{13}]$. In fact, any prime which is 3 mod 13 also splits this way. In general, the splitting of a prime in $\mathbb{Q}(\zeta_{13})$ only depends on its value mod 13, which is not unrelated to the fact that $\mathbb{Q}(\zeta_{13})/\mathbb{Q}$ is abelian.

4.2. **Inertia Subgroups.** let L/K be a Galois extension of number fields and $\mathfrak{p}$ a prime in K which splits as follows:

$$\mathfrak{p} = \mathfrak{P}_1^e \cdots \mathfrak{P}_g^e.$$

Let's fix $\mathfrak{P} = \mathfrak{P}_1$. As mentioned previously, $D_{\mathfrak{P}}$ is defined as the group of elements of $\mathrm{Gal}(L/K)$ which fix $\mathfrak{P}$. There is an important subgroup of the decomposition group, known as the inertia subgroup.

Definition 4.3. Let L, K, and $\mathfrak{P}$ be defined as above. Then, we define the inertia group at $\mathfrak{P}$ as

$$I_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(L/K) \mid \forall \alpha \in \mathcal{O}_L,\ \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}\}.$$

At the moment, we haven't actually proved $I_{\mathfrak{P}} \subset D_{\mathfrak{P}}$, although this is quite easy.

Proposition 4.4. *Given the same setup as above, $I_{\mathfrak{P}} \subset D_{\mathfrak{P}}$.*

Proof. Note that $\alpha \in \mathcal{O}_L$ is in $\mathfrak{P}$ if $\alpha \equiv 0 \bmod \mathfrak{P}$. Thus, if $\sigma \in I_{\mathfrak{P}}$, for $\alpha \in \mathfrak{P}$, $\sigma(\alpha) \equiv \alpha \equiv 0 \bmod \mathfrak{P}$, so $\sigma(\alpha) \in \mathfrak{P}$. Therefore, $\sigma(\mathfrak{P}) \subset \mathfrak{P}$. A similar argument shows that $\sigma^{-1}(\mathfrak{P}) \subset \mathfrak{P}$, which implies $\mathfrak{P} \subset \sigma(\mathfrak{P})$. Therefore, $\sigma(\mathfrak{P}) = \mathfrak{P}$, which is exactly what we need for $\sigma \in D_{\mathfrak{P}}$. Therefore, $I_{\mathfrak{P}} \subset D_{\mathfrak{P}}$. ■

In fact, we know what the size of $I_{\mathfrak{P}}$ is.

Proposition 4.5. *Given the same setup as above, we have $|I_{\mathfrak{P}}| = e$.*

Proof. As mentioned previously in this section, there is a natural map from $D_{\mathfrak{P}}$ to $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$. In the case where $e = 1$, we saw that this was in fact an isomorphism. However, although we will not prove it, this map is always surjective, and by the definition of the inertia subgroup, the kernel of this map is exactly the inertia subgroup. Thus, we have

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$$
$$\implies |I_{\mathfrak{P}}| = \frac{|D_{\mathfrak{P}}|}{|\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))|} = \frac{ef}{f} = e.$$

■

At the moment, we have decomposition and inertia subgroups for each individual prime above $\mathfrak{p}$. Quite naturally, these subgroups are conjugate to each other. In particular, we have the following statement:

Proposition 4.6. *Given the same setup as before, the $D_{\mathfrak{P}_i}$'s are conjugate, and the $I_{\mathfrak{P}_i}$'s are conjugate.*

Proof. Let $1 \le i, j \le g$, and let $\mu \in \mathrm{Gal}(L/K)$ be such that $\mu(\mathfrak{P}_i) = \mathfrak{P}_j$. Then, it is easy to check that $\mu^{-1} D_{\mathfrak{P}_i} \mu = D_{\mathfrak{P}_j}$. This is essentially a generalized statement of Proposition 4.2. ■

Thus, if L/K is abelian, all the $D_{\mathfrak{P}_i}$'s are the same, and so are the $I_{\mathfrak{P}_i}$'s. Thus, we may just write $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ instead. We will prove 2 final properties of inertia subgroups:

Proposition 4.7. *Given the same setup as above with the additional assumption that L/K is abelian, the subfield of L fixed by $I_{\mathfrak{p}}$ is the largest subfield in which $\mathfrak{p}$ is unramified.*

Proof. ■

Lemma 4.8. *Let $K/\mathbb{Q}$ be an abelian extension, and let $p_1, \ldots, p_k$ be the primes ramifying in K. Then, the inertia subgroups I_{p_i} generate* $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. ■

5. Statements of Class Field Theory

Let L/K be a Galois extension of number fields. We will let $\mathrm{Spl}(L/K)$ be the set of primes of K which split completely in L. Among other things, one of the consequences of Chebatorev's density theorem is that the density of $\mathrm{Spl}(L/K)$ among the set of primes of L is exactly $\frac{1}{[K:L]}$. In particular, if we let S be the set of prime ideals of $\mathcal{O}_L$, we have

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in \mathrm{Spl}(L/K) \mid N_{L/K}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in S \mid N_{L/K}(\mathfrak{p}) \leq x\}} = \frac{1}{[L:K]}.$$

Note that $\mathfrak{p} \in \mathrm{Spl}(L/K)$ is equivalent to the Frobenius element at every prime above $\mathfrak{p}$ being trivial. We will now give a sketch of the following theorem

Theorem 5.1. *Let K be a number field and let L_1/K and L_2/K be finite Galois extensions such that Spl(L_1/K) and Spl(L_2/K) differ by a finite set of primes (in particular, finitely many primes are in exactly one of these sets). Then, $L_1 = L_2$.*

Proof. Consider the compositum L_1L_2. The main claim, which we will not rigorously prove, is that a prime splits in L_1L_2 if and only if it splits in L_1 and L_2. The proof of this relies on how the Frobenius element controls splitting. A more detailed description of this can be found at [Mil20] Theorem 8.38. The density of $\mathrm{Spl}(L_1L_2)$, $\mathrm{Spl}(L_1)$, and $\mathrm{Spl}(L_2)$. By the corollary to Chebotarev, this means $[L_1L_2 : K] = [L_1 : K] = [L_2 : K]$, which can only occur if $L_1 = L_2$. ■

In other words, extensions of K are determined by the primes which split within them. In Class Field Theory, we are interested in abelian extensions of number fields in particular. Class Field Theory essentially gives a complete correspondence between abelian extensions L/K of number fields and the associated sets of primes $\mathrm{Spl}(L/K)$. Furthermore, this correspondence can be described entirely with respect to K only. Thus, if one were to know everything about the so-called ray class fields and ray class groups of K, then they would know everything about the abelian extensions of K. In fact, these things are very easy to describe for $\mathbb{Q}$, and this correspondence leads easily to the Kronecker-Weber Theorem.

5.1. Moduli and Ray Class Groups.

To understand the statements of class field theory, we first have to understand what a modulus is. A modulus $\mathfrak{m}$ of a number field K consists of a finite part $\mathfrak{m}_0$ and an infinite part $\mathfrak{m}_\infty$. The finite part is just an ideal of $\mathcal{O}_K$ while the infinite part is a subset of the real embeddings of K. In this case, we write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$.

Now we can define the ray class group for a given modulus $\mathfrak{m}$, which is a generalization of the usual class group. In particular, let $I_K^{\mathfrak{m}}$ be the multiplicative group of fractional ideals relatively prime to $\mathfrak{m}$. A generic element of this group will look like

$$\prod_{\mathfrak{p}\nmid\mathfrak{m}}{}' \mathfrak{p}^{a_\mathfrak{p}}$$

where the product is a restricted product over prime ideals $\mathfrak{p} \nmid \mathfrak{m}$ and the $a_\mathfrak{p}$'s are integers (the restricted product means that only finitely many of the $a_\mathfrak{p}$'s are 0). Thus, $I_K^{\mathfrak{m}}$ can also be thought of as the free group generated by the primes not dividing $\mathfrak{m}$.

We then define $P_K^{\mathfrak{m}}$ to be a certain subgroup of P_K, the multiplicative group of principal fractional ideals of $\mathcal{O}_K$. In particular, $P_K^{\mathfrak{m}}$ includes fractional ideals of the form $\alpha\mathcal{O}_K$ for $\alpha \in K^\times$ such that

- $\alpha \equiv 1 \bmod \mathfrak{m}_0$
- For $\tau \in \mathfrak{m}_\infty$, $\tau(\alpha) > 0$.

We then define the **ray class group of modulus $\mathfrak{m}$** to be $\mathrm{Cl}_K^{\mathfrak{m}} := I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. Notice that when $\mathfrak{m} = (1)$, $\mathrm{Cl}_K^{\mathfrak{m}}$ is just $\mathrm{Cl}(K)$, the usual class group. Given that $\mathrm{Cl}(K)$ is finite, it is actually not too hard to prove that $\mathrm{Cl}_K^{\mathfrak{m}}$ is always finite.

Proposition 5.2. *For any number field K and any modulus $\mathfrak{m}$, $\mathrm{Cl}_K^{\mathfrak{m}}$ is finite.*

Proof. There is a natural surjection $\mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}(K)$, so we just have to show that the kernel of this map has a finite index in $\mathrm{Cl}_K^{\mathfrak{m}}$. The kernel ∎

Example. Let's calculate the moduli and ray class groups for $\mathbb{Q}$. Ideals of $\mathbb{Z}$ look like (m) for $m > 0$. Furthermore, there is one infinite embedding of $\mathbb{Q}$, which is just the identity map. We will denote this as ∞. Thus, we can write all moduli of $\mathbb{Q}$ in the form $\mathfrak{m} = m$ or $\mathfrak{m} = m\infty$. Either way, we have

$$I_K^{\mathfrak{m}} = \left\{ \frac{a}{b}\mathbb{Q} \mid \gcd(a, m) = \gcd(b, m) = 1 \right\}.$$

Now suppose $\mathfrak{m} = m$. Then,

$$P_K^{\mathfrak{m}} = P_K^m = \left\{ \alpha\mathbb{Q} \mid \alpha \in \mathbb{Q}^\times,\ \alpha \equiv 1 \bmod m \right\}$$

.

It looks like the class group $\mathrm{Cl}_{\mathbb{Q}}^m$ might be isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$. However, note that for $\alpha \equiv -1 \bmod m$, $\alpha\mathbb{Q}^\times = -\alpha\mathbb{Q}^\times \in P_K^m$ since $-\alpha \equiv 1 \bmod m$. Thus, the class group ends up being isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$ since $\alpha\mathbb{Q}^\times$ for both $\alpha \equiv \pm 1$ become trivial in the quotient. What we really need to do is make sure that α is positive. This is exactly the case when $\mathfrak{m} = m\infty$, and as you might expect, we have $\mathrm{Cl}_{\mathbb{Q}}^{m\infty} \cong (\mathbb{Z}/m\mathbb{Z})^\times$. Thus, considering real embeddings is actually very fruitful.

5.2. **Takagi's Existence Theorem.** Fix a number field K and a modulus $\mathfrak{m}$. The first part of Takagi's Existence Theorem establishes the existence of the ray class field. In particular, there is an extension $K^{\mathfrak{m}}/K$ such that the primes that split completely are exactly those in $P_K^{\mathfrak{m}}$. By Theorem 5.1, this field is unique.

Example. Let $K = \mathbb{Q}$ and $\mathfrak{m} = m\infty$ for $m \in \mathbb{Z}^+$. We claim that $\mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}^{m\infty} = \mathbb{Q}(\zeta_m)$. Notice that the primes that are in $P_{\mathbb{Q}}^{m\infty}$ are exactly the rational primes that are 1 mod p, so we just need to show that the only primes that completely split in $\mathbb{Q}(\zeta_m)$ are those that are 1 mod m. A prime p completely splitting in $\mathbb{Q}(\zeta_m)$ is equivalent to the mth cyclotomic polynomial completely splitting mod p, by the Dedekind-Kummer Theorem. This is equivalent to ζ_m existing mod p, and since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, this is equivalent to $q \mid |(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$. In other words, p splitting is equivalent to $p \equiv 1 \bmod q$ as desired.

Let $K = \mathbb{Q}$ but $\mathfrak{m} = m$ for $m \in \mathbb{Z}^+$. We claim that $\mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. Based on our discussion of calculating $\mathrm{Cl}_{\mathbb{Q}}^{\mathfrak{m}}$ for this type of modulus, we saw that $P_K^{\mathfrak{m}}$ contained primes in $\mathbb{Q}$ that were both ± 1 mod m. Thus, we need to show that the primes splitting in $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ are those that are ± 1 mod m. Once again, by the Dedekind-Kummer Theorem, p splitting completely in this extension is equivalent to the minimal polynomial of $\zeta_m + \zeta_m^{-1}$ completely

splitting mod p, and this is equivalent to $\zeta_m + \zeta_m^{-1}$ being an element of $\mathbb{F}_p$, since $\zeta_m + \zeta_m^{-1}$ generates its Galois conjugates. If $\zeta_m + \zeta_m^{-1} \in \mathbb{F}_p$, we can solve a quadratic to find ζ_m; however the value of ζ_m may be in $\mathbb{F}_{p^2}$, so $m \mid |\mathbb{F}_{p^2}^\times| = p^2 - 1$, so $p \equiv \pm 1$. This shows that if p splits, then $p \equiv \pm 1 \bmod m$. The other direction is also not that hard to show.

The surprising part of Takagi's Theorem is that all finite abelian extensions of a number field K are subfields of one of the ray class fields. Furthermore, there is a very natural correspondence between subfields of $K^{\mathfrak{m}}$ and the ray class group, $\mathrm{Cl}_K^{\mathfrak{m}}$. In particular, here is the full statement:

Theorem 5.3 (Takagi's Existence Theorem)**.** *Let K be a number field and $\mathfrak{m}$ a modulus. Then, there is a unique extension $K^{\mathfrak{m}}/K$ such that Spl$(K^{\mathfrak{m}})$ is the set of or primes in $P_K^{\mathfrak{m}}$, with possibly finitely many exceptions. Furthermore, for every congruence subgroup H with $P_K^{\mathfrak{m}} \subset H \subset I_K^{\mathfrak{m}}$, there is a unique subfield L of $K^{\mathfrak{m}}$ such that Spl(L) is the set of primes in H, with finitely many exceptions. Furthermore, for this subfield L, we have*

$$\mathrm{Gal}(L/K) \cong I_K^{\mathfrak{m}}/H.$$

The proof of the Existence Theorem is not easy, and modern approaches to this theorem use Artin Reciprocity,, although this is in some sense, a more precise version of the existence theorem. Furthermore, the proof of Artin Reciprocity typically requires a lot of cohomology, which we won't be able to cover in this paper. However, assuming the existence theorem, we can easily prove Kronecker-Weber!

Proof of Theorem 2.1. The ray class fields of $\mathbb{Q}$ are $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ for $m \in \mathbb{Z}^+$, both of which are subfields of $\mathbb{Q}(\zeta_m)$. Thus, all finite abelian extensions of $\mathbb{Q}$ are contained in $\mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{Z}^+$. ■

6. Local Fields

In this section, we will introduce local fields, the simplest of which are the p-adic rationals $\mathbb{Q}_p$ for rational primes p. When constructing a local field, the goal is that we want to metrically complete $\mathbb{Q}$, since it is not already metrically complete. Such metric completions are local fields.

For example, in the usual metric space on $\mathbb{Q}$, the distance between two rational numbers is $|x - y|$. We can complete $\mathbb{Q}$ with respect to this metric, which means we form the space of Cauchy sequences in $\mathbb{Q}$ with respect to the metric. For this choice of metric, this forms $\mathbb{R}$, which is one of the local completions of $\mathbb{Q}$.

However, there are other useful metrics on $\mathbb{Q}$, such as the p-adic metric. Before we look at this, we should define what a metric is.

Definition 6.1. A norm function for a field F is a function $|\cdot| : F \to \mathbb{R}_{\geq 0}$ such that $|x| \geq 0$ for $x \in F$ and equality only when $x = 0$. Furthermore, $|xy| = |x||y|$ and $|x + y| \leq |x| + |y|$, the last condition being the triangle inequality.

We can then define the distance between two elements $x, y \in F$ as $|x - y|$. It is easily checked that this forms a metric space. The other useful norm over $\mathbb{Q}$ is the p-adic norm. In particular, for a prime p, we can write any nonzero rational number q as $p^n \frac{a}{b}$ for some $n \in \mathbb{Z}$ such that $p \nmid a, b$. In this case, we write $|q|_p = p^{-n}$ where $|\cdot|_p$ is the p-adic norm. In other words, if the numerator of q has many factors of p, q has a small norm, and if the denominator has many factors of p, q has a large norm. The only nontrivial thing that needs

to be shown to prove $|\cdot|_p$ is a norm is that it satisfies the triangle inequality. In fact, it satisfies a stronger inequality, which we will not prove.

Proposition 6.2. *Let $|\cdot|_p$ be the p-adic norm on $\mathbb{Q}$. Then, for $x, y \in \mathbb{Q}$, $|x+y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p$.*

The field of p-adic rationals $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ under this metric. The above inequality makes $\mathbb{Q}_p$ a **non-archimedean field**.

Instead of just thinking about the norm of this field, it is often better to think about the underlying valuation. For example, in $\mathbb{Q}_p$, the valuation should detect how many powers of p a certain element is divisible by. In particular, for $q \in \mathbb{Q}$, if $q = p^n \frac{a}{b}$ where $p \nmid a, b$, we write $\nu_p(q) = n$. Alternatively, we have $\nu_p(q) = -\log_p(|q|_p)$.

6.1. **Extensions of $\mathbb{Q}_p$.** We can now consider extensions of $\mathbb{Q}_p$, just as we consider extensions of $\mathbb{Q}$. For example, $\mathbb{Q}_3$ does not have $\sqrt{2}$, because there is no square root of 2 mod 3. Thus, we can consider $\mathbb{Q}_3(\sqrt{2})/\mathbb{Q}_3$, which is a quadratic extension. $\mathbb{Q}_3(\sqrt{2})$ also has an absolute value that extends that of $\mathbb{Q}_3$. For example, consider $|\sqrt{2}|_3$. It should satisfy $|\sqrt{2}|_3^2 = |2|_3 = 1$. Thus, $|\sqrt{2}|_3 = 1$. In fact, although it is a bit harder, it can be shown that $|a + b\sqrt{2}|_3 = 1$ if $3 \nmid a, b$, so $\nu_3(a + b\sqrt{2}) = \nu_3(\gcd(a, b))$, and the absolute value can be defined as usual based on the valuation. This is a demonstration of how there is a unique absolute value that extends the absolute value of the base field. These fields, which are finite extensions of $\mathbb{Q}_p$, are known as local fields.

Theorem 6.3. *Let L/K be an extension of local fields and $|\cdot|_K$ an absolute value on K. Then, there is a unique absolute value $|\cdot|_L$ which agrees with $|\cdot|_K$ on K, which is given by*

$$|\alpha|_L = \sqrt[n]{|N_{L/K}(\alpha)|_K}.$$

Proof. See [Neu07] Chapter 2 Section 8. ∎

Every local fields K as a ring of integers $\mathcal{O}_K$, defined as

$$\mathcal{O}_K = \{\alpha \in K \mid |\alpha|_K \leq 1\}.$$

For example, the ring of integers of $\mathbb{Q}_p$ is denoted $\mathbb{Z}_p$, the p-adic integers. While we will not prove it, it turns out that this ring has exactly one maximal ideal (and hence prime), which is given by

$$\{\alpha \in K \mid |\alpha|_K < 1\}.$$

Furthermore, this maximal ideal is generated by a single element, known as a **uniformizer**. For example, the ideal $\mathbb{Z}_p$ in $\mathbb{Q}_p$ is generated by p. If K is a local field and $\mathcal{O}_K$ is the ring of integers, we denote $k = K/\mathcal{O}_K$ to be the residue field, which is analogous to the notion of residue field with number fields.

6.2. **Hensel's Lemma.** Perhaps the most useful property about local fields is Hensel's Lemma, which allows us to find a root of a polynomial in the local field by only finding a root in the residue field, with a few extra conditions. Here is one version of the statement of Hensel's Lemma:

Theorem 6.4. *Let K be a local field with uniformizer π and ring of integers $\mathcal{O}_K$. If $f(x) \in \mathcal{O}_K[x]$ has a root r mod π and $f'(r) \not\equiv 0 \bmod \pi$, then f has a root $r' \in \mathcal{O}_K[x]$ with $r' \equiv r \bmod \pi$.*

Proof. See [Lan94] Chapter 3 Proposition 2. ■

In the initial hypothesis of Hensel's Lemma, we're looking for a root of f in $\mathcal{O}_K[x]$ mod π. However, recall that $\mathcal{O}_K/(\pi)$ is defined to be the residue field of K, which we established was finite. Thus, in Hensel's Lemma, we're initially looking for a root of the polynomial in the residue field, and we are usually able to "lift up" such a root if we find it in the residue field.

Example (Roots of unity). Consider $\mathbb{Q}_p$ which has residue field $\mathbb{F}_p$. Every nonzero element of $\mathbb{F}_p$ is a $p-1$th root of unity. In other words, the $p-1$ roots of $x^{p-1}-1$ are $1, 2, \ldots, p-1$. The derivative of this polynomial is $(p-1)x^{p-2}$ which is nonzero at none of these roots, so all of these roots can be lifted up to a $p-1$th root of unity in $\mathbb{Q}_p$. Furthermore, there are no other roots of unity in $\mathbb{Q}_p$ since there are no other possible roots of unity mod p.

6.3. **Ramification.** Just as we have ramification for number fields, we have ramification for local fields. A local field K only has one prime, which is of the form (π_K) for a uniformizer $\pi_K \in \mathcal{O}_K$. Thus, for L/K to be a ramified extension, we would need to have $(\pi_K) = (\pi_L)^e$ for $e > 1$ where π_L is a uniformizer of L. We have the following definition:

Definition 6.5. Let L/K be a finite extension of local fields, π_K a uniformizer of K, and π_L a uniformizer of L. Then, as ideals in L, we have $(\pi_K) = (\pi_L)^e$ for some $e > 0$. This value of e is the ramification index of L/K. We say L/K is ramified if $e > 1$.

This ramification index is completely analogous to that of number fields. There is also an analogue of inertial degree.

Definition 6.6. Let L/K be a finite extension of local fields. If ℓ is the residue field of L and k the residue field of K, the inertial degree f of L/K is $[\ell : k]$.

There isn't a useful analogue of g however, since primes can't factor as a product of multiple distinct primes, although one could say $g = 1$. Either way, there is an analogue of the efg formula for number fields:

Proposition 6.7. *Let L/K be a finite extension of local fields, and let e be the ramification index and f the inertial degree. Then, $ef = [L : K]$.*

Note that if L/K is ramified, then we have $(\pi_K) = (\pi_L)^e$ for uniformizers π_K and π_L, so $\pi_K = \pi_L^e u$ for a unit $u \in \mathcal{O}_L$. Assuming we have a valuation ν such that $\nu(\pi_K) = 1$, we can uniquely extend this valuation to L, and we will get $1 = \nu(\pi_K) = e\nu(\pi_L)$, so $\nu(\pi_L) = \frac{1}{e}$. Thus, ramified extension create new "levels" of possible valuations while unramified extensions only expand the residue field (although a single extension can do both of these).

Example. It can be checked that the quadratic extension $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$ is unramified. This corresponds to the fact that 5 is still a uniformizer in $\mathbb{Q}_5(\sqrt{2})$, and that the residue field of $\mathbb{Q}_5(\sqrt{2})$ is $\mathbb{F}_5(\sqrt{2}) = \mathbb{F}_{25}$. Furthermore, we can find a square root of 3 in $\mathbb{F}_{25}$, so by Hensel's Lemma, we can lift it up to find $\sqrt{3}$ in $\mathbb{Q}_5(\sqrt{2})$. This implies that $\mathbb{Q}_5(\sqrt{2}) = \mathbb{Q}_5(\sqrt{3})$. In fact, any two quadratic unramified extensions of $\mathbb{Q}_5$ are equal, as we will see by the next proposition.

On the other hand, $\mathbb{Q}_5(\sqrt{5})$ is ramified, because the prime (5) factors as $(\sqrt{5})^2$. Thus, $\sqrt{5}$ becomes a uniformizer of $\mathbb{Q}_5(\sqrt{5})$ rather than 5. Furthermore, the residue field of this extension is still $\mathbb{F}_5$.

Theorem 6.8. *Given a local field K, there is only one unramified extension of K with degree $q > 0$.*

Corollary 6.9. *Let L/K be an unramified extension of local fields. Then, $L = K(\zeta_{q-1})$ where q is the order of the residue field of L.*

7. Kummer Theory

Throughout the section, for a field K, $K^\times$ denotes the multiplicative group of K, which include all the nonzero elements of K. Furthermore, for any group G and positive integer n, we will let G^n denote the set $\{g^n \mid g \in G\}$, which is a group if G is abelian.

The goal of Kummer Theory is to classify extensions of a very particular type, which we call Kummer extensions. First, recall that the exponent of a group G is the smallest positive integer n such that $G^n = 1$, if it exists. Clearly, all finite groups have an exponent.

Definition 7.1. A Galois extension L/K is Kummer if there is some n for which $\zeta_n \in K$ and $\mathrm{Gal}(L/K)$ is abelian with exponent dividing n.

For example, any quadratic extension of $\mathbb{Q}$ and $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}(\zeta_3)$ are Kummer. It is very important in the second example that ζ_3 is in the base field because $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois. Conversely, if we have a field K containing ζ_n, adjoining any element of the form $\alpha^{\frac{1}{n}}$ for $\alpha \in K^\times$ gives a Galois extension, and in fact the Galois group of this extension will be a subgroup of $\mathbb{Z}/n\mathbb{Z}$. We will actually be able to explicitly describe all Kummer extensions of a given base field. We will need the following lemma however:

Lemma 7.2. *Let L/K be a field extension with autormorphism group G. Then, the elements of G are linearly independent over L. In particular, if $G = \{\sigma_1, \ldots, \sigma_n\}$, there are no elements $\alpha_1, \ldots, \alpha_n$, such that for all $x \in L$,*

$$\alpha_1\sigma_1(x) + \cdots + \alpha_n\sigma_n(x) = 0.$$

Theorem 7.3. *Let K be a field containing ζ_n for some positive integer n. Then, every extension L/K with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$ is of the form $K(\alpha^{\frac{1}{n}})/K$ for some $\alpha \in K^\times$ such that $\alpha^{\frac{1}{d}} \notin K$ for any $d > 1$ dividing n.*

Proof. Suppose we have some $\alpha \in K^\times$ such that $\alpha^{\frac{1}{d}} \notin K^\times$ for any $d > 1$ dividing n. Then, any element of $\mathrm{Gal}(K(\alpha^{\frac{1}{n}})/K)$ must take $\alpha^{\frac{1}{n}}$ to another nth root of α, so $\alpha^{\frac{1}{n}}$ must be taken to $\alpha^{1/n}\zeta_n^r$ for some r. No two elements of the Galois Group can send $\alpha^{1/n}$ to $\alpha^{1/n}\zeta_n^r$ for the same value of r since this r determines the automorphism. Thus, $\mathrm{Gal}(K(\alpha^{1/n})/K)$ is isomorphic to the group containing the possible values of r mod n, which is a subgroup of $\mathbb{Z}/n\mathbb{Z}$. Suppose $\mathrm{Gal}(K(\alpha^{1/n})/K)$ has exponent $e \mid n$. Then, it can easily be seen that $\alpha^{e/n}$ must be fixed by all automorphisms of the Galois Group, so $\alpha^{e/n} \in K^\times$. By our hypotheses, this means that $e = n$.

On the other hand, suppose L/K is a Kummer extension with Galois Group $\mathbb{Z}/n\mathbb{Z}$. Let σ be a generator of the Galois Group. By Lemma 7.2, $\sigma, \ldots, \sigma^n$ are linearly indepdendent, so the linear combination $\zeta_n\sigma(x) + \ldots \zeta_n^n\sigma^n(x)$ is not identically 0, so we can find some $t, \alpha \in L^\times$ such that

$$0 \neq t = \zeta_n\sigma(\alpha) + \cdots + \zeta_n^n\sigma^n(\alpha) = \sum_{i=1}^{n} \zeta_n^i\sigma^i(\alpha).$$

We claim that $L = K(t^{1/n})$. Note that

$$\begin{aligned}\sigma(t) &= \sigma\left(\sum_{i=1}^{n} \zeta_n^i \sigma^i(\alpha)\right) \\ &= \sum_{i=1}^{n} \zeta_n^i \sigma^{i+1}(\alpha) \\ &= \sum_{i=1}^{n} \zeta_n i - 1 \sigma^i(\alpha) \\ &= \zeta_n^{-1} t.\end{aligned}$$

Thus, $\sigma(t^n) = \sigma(t)^n = t^n$, so $t^n \in K^\times$. Clearly, no smaller powers of t are fixed by σ, so by the first part of the proof, $K(t^{1/n}) \subset L$ must have degree n, but L has degree n over K, so $L = K(t^{1/n})$. ■

Now we can state the full statement of Kummer Theory:

Theorem 7.4. *Let K be a field containing ζ_n for some positive integer n. Then, the finite subgroups of $K^\times/(K^\times)^n$ are in one-to-one correspondence with the finite Kummer extensions of K with exponent dividing n. In particular, given a subgroup $\Delta \subset K^\times/(K^\times)^n$, the corresponding Kummer extension is $K(\Delta^{\frac{1}{n}})$. Furthermore, $\Delta \cong \mathrm{Gal}(L/K)$.*

Proof. Note that $K^\times/(K^\times)^n$ is a group of exponent n, since any element of $K^\times$ raised to the nth power is in $(K^\times)^n$, and for ζ_n, this is the minimum possible power that achieves this. Thus, any subgroup $\Delta \subset K^\times/(K^\times)^n$ has exponent dividing n. Thus, we can write

$$\Delta \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$$

where $d_i \mid n$. Let α_i be a generator for the isomorphic copy of $\mathbb{Z}/d_i\mathbb{Z}$ in Δ. Then, $\alpha_i^{d_i} \in (K^\times)^n$, but no lower power of α_i is in $(K^\times)^n$. Now we construct the Kummer extensions $K_i = K(\alpha_i^{1/n})$. Note that $\alpha_i^{1/n} = (\alpha_i^{d_i/n})^{1/d_i}$, and it can be checked that $\alpha^{d_i/n} \in K^\times$ while no root of it is in $K^\times$, based on all our assumptions. Thus, by Theorem 7.3, K_i/K has Galois Group $\mathbb{Z}/d_i\mathbb{Z}$. It is also easy to see that the K_i's are mutually disjoint, so

$$K(\Delta^{1/n}) = K(\alpha_1^{1/n}, \ldots, \alpha_i^{1/n})$$

whose Galois Group is the direct product of the Galois Group of all the K_i/K's by Theorem 2.2, and that direct product is isomorphic to Δ.

The other direction follows similarly from Theorem 7.3, so we omit it. ■

Example. As an example, we can characterize all finite Kummer extensions of $\mathbb{Q}$ of exponent dividing 2. Such extensions are in correspondence with the finite subgroups of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, which can be identified with the group

$$\prod_p{}' \mathbb{Z}/2\mathbb{Z}$$

where the product is a restricted product (all but finitely many terms in the product have to be the trivial element of $\mathbb{Z}/2\mathbb{Z}$) where p goes over all places of $\mathbb{Q}$. If Δ is a finite subgroup of this group containing an element which has the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ in the places $p_1, \ldots, p_k$, then, this would correspond to adjoining $\sqrt{p_1 \cdots p_k}$ to $\mathbb{Q}$. Note that "multiplication" by the infinite place in this case is just multiplication by -1.

8. Reduction of the Statement of Kronecker-Weber

In this section, we will reduce Kronecker-Weber to a simpler equivalent statement. First of all, we will prove that it suffices to show Theorem 2.1 where $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of prime power order, and we will also show that the "Global" Kronecker-Weber Theorem is equivalent to the "Local" Kronecker-Weber Theorem, in which we use a base field of $\mathbb{Q}_p$ for primes p rather than $\mathbb{Q}$. This step heavily relies on the fact that the Kronecker-Weber Theorem is concerned with extensions of $\mathbb{Q}$ in particular.

8.1. **Reducing to Cyclic Galois Groups of Prime Power Order.** Suppose $K/\mathbb{Q}$ is abelian. Then, by the Fundamental Theorem of Finite Abelian Groups, we have a decomposition:

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{r_n}\mathbb{Z}$$

where the p_i's are not primes which are not necessarily distinct. Thus, K has subextensions K_i such that $\mathrm{Gal}(K_i/\mathbb{Q}) \cong \mathbb{Z}/p_i^{r_i}$. K_i is just the field fixed by the subgroup $\mathrm{Gal}(K/\mathbb{Q})/(\mathbb{Z}/p_i^{r_i}\mathbb{Z}) = \prod_{j\neq i} \mathbb{Z}/p_j^{r_j}\mathbb{Z}$. For $i \neq j$, $\mathrm{Gal}(K_i/\mathbb{Q})$ and $\mathrm{Gal}(K_j/\mathbb{Q})$ have trivial intersection, so $K_i \cap K_j$. By Theorem 2.2, we thus have that K is the compositum of the K_i's, also denoted as $\prod_i K_i$. Thus, if can show that each of the K_i's is contained in a cyclotomic extension, then so must their compositum, because the compositum of cyclotomic extensions is cyclotomic. In fact, for positive integers a and b, $\mathbb{Q}(\zeta_a, \zeta_b) = \mathbb{Q}(\zeta_{\mathrm{lcm}(a,b)})$. In other words, when proving Kronecker-Weber, we only have to consider extensions whose Galois group is cyclic of prime power order.

8.2. **Global to Local.** Our main strategy for proving Kronecker-Weber will be to prove the Local Kronecker-Weber Theorem, and then extend that to the global case. This is advantageous because local class field theory is much easier than global class field theory in general. The local version states the following:

Theorem 8.1 (Local Kronecker-Weber Theorem)**.** *For every prime p, every abelian extension K of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\zeta_m)$ for $m \geq 0$.*

We will now that Theorem 8.1 implies Theorem 2.1, and then we will prove Theorem 8.1.

Theorem 8.2. *The Local Kronecker-Weber Theorem implies the Global Kronecker-Weber Theorem.*

Proof. Suppose the Local Kronecker-Weber Theorem is true, and let $K/\mathbb{Q}$ be an abelian extension. Let $p_1, \ldots, p_k$ be the finitely many primes ramifying in K and $\mathfrak{p}_i$ a prime above p_i. Consider the localizations $K_{\mathfrak{p}_i}/\mathbb{Q}_{p_i}$. By the Local Kronecker-Weber Theorem, there exist m_i's such that $K_{\mathfrak{p}_i} \subset \mathbb{Q}_{p_i}(\zeta_{m_i})$. We can actually construct an m such that $K \subset \mathbb{Q}(\zeta_m)$ in terms of the m_i's. It turns out that

$$m = \prod_{i=1}^{k} p_i^{e_i}$$

works, where $p_i^{e_i}$ is the largest power of p_i dividing m_i. Intuitively, this makes sense because we are trying to find an m such that the p_i's have the right ramification indices. Then, the power of p_i that divides the ramification index of p_i in $\mathbb{Q}(\zeta_m)$ is only dependent on the number of power of p_i that divides m. Furthermore, the ramification index of p_i in

$\mathbb{Q}_{p_i}(\zeta_{m_i})$ should be the same as the ramification index in $\mathbb{Q}(\zeta_m)$, so we attempt to match up the exponents of all the p_i's between these two extensions.

To show this works, let $L = K(\zeta_m)$. We want to show that $L = K$. For each i, consider the localization of L at $\mathfrak{p}_i$. In particular,

$$\mathbb{Q}_p(\zeta_m) \subset L_{\mathfrak{p}_i} = K_{\mathfrak{p}_i}(\zeta_m) \subset \mathbb{Q}_p(\zeta_{m_i}, \zeta_m) = \mathbb{Q}_p(\zeta_{n_i})$$

where $n_i = \operatorname{lcm}(m_i, m)$. Because the largest power of p_i dividing both m_i and m is $p_i^{e_i}$, the inertia subgroups for $\mathbb{Q}_p(\zeta_m)$ and $\mathbb{Q}_p(\zeta_{n_i})$ are $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$. Thus, this is also the inertia subgroup for $L_{\mathfrak{p}_i}$. Therefore, the inertia subgroup I_{p_i} of $L/\mathbb{Q}$ with respect to the prime p is $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$, which has size $\varphi(p_i^{e_i})$. By Lemma 4.8, we thus have the following inequality:

$$[L : \mathbb{Q}] = |\operatorname{Gal}(L/\mathbb{Q})| \leq \prod_{i=1}^{k} |I_{p_i}| = \prod_{i=1}^{k} \varphi(p_i^{e_i}) = \varphi(m).$$

Meanwhile, $\mathbb{Q}(\zeta_m) \subset L$, so $[L : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$, so we must have an equality, which can only hold if $L = \mathbb{Q}(\zeta_m)$. Thus, we have $K \subset L = K(\zeta_m) \subset \mathbb{Q}(\zeta_m)$. ■

8.3. **Some Lemmas.** Before proving Local Kronecker-Weber, we will sketch the proofs of some lemmas will which be necessary as we go along.

Lemma 8.3. *Let L/K be a totally and tamely ramified extension of degree e of finite extensions $\mathbb{Q}_p$. Then, there exists a uniformizer π_K of K such that $L = K(\pi_K^{1/e})$.*

Proof. For the extension to be ramified of degree e, this means that $(\pi_K) = (\pi_L)^e$ (as ideals in $\mathcal{O}_L$), where π_L is a uniformizer of L. We can assume that $\pi_L^e \equiv \pi_K \bmod \pi_K^2$ since every element of $(\pi_K)\backslash(\pi_K)^2$ is a uniformizer of $\mathcal{O}_K$. Thus, $\pi_L^e = \pi_K u$. By our assumption, we can conclude that $u \equiv 1 \bmod \pi_K$. Thus, $X^e - u$, which is a separable polynomial, has a root mod π_K, so it has a root in $\mathcal{O}_K$ by Hensel's lemma. In other words, $u^{1/e} \in K$. Thus, $L = K(\pi_L) = K(\pi_K^{1/e} u^{1/e}) = K(\pi_K^{1/e})$. ■

Lemma 8.4. *We have the equality*

$$\mathbb{Q}_p\left((-p)^{\frac{1}{p-1}}\right) = \mathbb{Q}_p(\zeta_p)$$

.

Proof. See [Was97] Lemma 14.6. ■

Lemma 8.5. *For $p \neq 2$, there is no extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$.*

Proof. See [Was97] Lemma 14.8. ■

Proof of Theorem 8.1. Let $K/\mathbb{Q}_p$ be an abelian extension. We have two main cases in the proof, the second of which will be much harder than the first.

Case 1 ($K/\mathbb{Q}_p$ is either not ramified or tamely ramified.)**.** Let $L/\mathbb{Q}_p$ be the largest subextension of $K/\mathbb{Q}_p$ which is totally ramified. Furthermore, let $[L : \mathbb{Q}_p] = e$ where e is the ramification index of p in L. By our hypotheses for this case, we have $p \nmid e$. We claim that $e \mid p - 1$. By Lemma 8.3, we have $L = \mathbb{Q}_p(\pi^{1/e})$ for a uniformizer in $\mathbb{Q}_p$. Thus, the smallest Galois extension that contains L must contain ζ_e. However, $L(\zeta_e, \pi^{1/e})$, which is Galois, is not abelian unless $\zeta_e \in \mathbb{Q}_p$. On the other hand, $L(\zeta_e, \pi^{1/e}) \subset K$, and $K/\mathbb{Q}_p$ is abelian, so we must have $\zeta_e \subset \mathbb{Q}_p$. This only exists for $e \mid p - 1$ since $p - 1$th roots exist due to Hensel's lemma, and no other roots of unity exist mod p.

Now note that all uniformizers of $\mathbb{Q}_p$ are of the form pu for a unit $u \in \mathbb{Z}_p$. We will write $\pi = pu$ in this way. Thus, using $e \mid p-1$, Lemma 8.4, and Corollary 6.9, we have

$$\begin{aligned} L &= \mathbb{Q}_p(\pi^{1/e}) \\ &= \mathbb{Q}_p((pu)^{1/e}) \\ &\subset \mathbb{Q}_p((pu)^{\frac{1}{p-1}}) \\ &\subset \mathbb{Q}_p((-p)^{\frac{1}{p-1}}, (-u)^{\frac{1}{p-1}}) \\ &\subset \mathbb{Q}_p(\zeta_p, \zeta_{q-1}) \end{aligned}$$

where the q is such that $\mathbb{Q}_p((-u)^{\frac{1}{p-1}}) = \mathbb{Q}_p(\zeta_{q-1})$, as guaranteed by Corollary 6.9. Thus, L is contained within a cyclotomic extension of $\mathbb{Q}_p$. Using Corollary 6.9 again, we know that $K = L(\zeta_{r-1})$ for some integer r since K/L is unramified. Thus,

$$K = L(\zeta_{r-1}) \subset \mathbb{Q}_p(\zeta_p, \zeta_{q-1}, \zeta_{r-1})$$

which finishes this case.

Case 2 ($K/\mathbb{Q}_p$ is wildly ramified and $p \neq 2$)**.** We can assume that K is totally ramified. Otherwise, like in the previous case, we can let $\mathbb{Q}_p \subset L \subset K$ such that K/L is tamely ramified and $L/\mathbb{Q}_p$ is totally ramified. But, K is a cyclotomic extension of L since it is unramified, so in this case, it is sufficient to prove that L is contained in a cyclotomic extension of $\mathbb{Q}_p$. Furthermore, we can also assume that the degree of $K/\mathbb{Q}_p$ is p^r for some $r > 0$. Let $\mathbb{Q}_p^r$ be a totally ramified extension of $\mathbb{Q}_p$ with degree p^r and let $\mathbb{Q}_p^u$ be an unramified extension of $\mathbb{Q}_p$ of degree p^r. Both of these exist; the first one can be found by taking the degree p^r subfield of $\mathbb{Q}_p(\zeta_{p^r})$ while the second can be found by constructing a local field with residue field $\mathbb{F}_{p^r}$ and no ramification, which is cyclotomic by Theorem 6.8. Clearly, $\mathbb{Q}_p^r \cap \mathbb{Q}_p^u = \mathbb{Q}_p$. We claim that $K \subset \mathbb{Q}_p^r\mathbb{Q}_p^u$. Otherwise, we could consider $\mathbb{Q}_p^r\mathbb{Q}_p^uK$, and the Galois group of this over $\mathbb{Q}$ would have to have $(\mathbb{Z}/p\mathbb{Z})^3$. This is impossible by Lemma 8.5.

Case 3 ($K/\mathbb{Q}_p$ is wildly ramified and $p = 2$)**.** We will not go over all the details of this case, as it is somewhat similar in nature to the previous case. The main difference is that one has to prove that $\mathbb{Q}_2$ has no extensions with Galois Group $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$. More details can be found at [Was97] in the end of Chapter 14.

■

Acknowledgments

I would first like to thank Simon Rubinstein-Salzado for running the IRPW class and teaching the fundamental aspects of writing a paper. I would also like to thank all the Euler Circle students for giving great talks as well as attending my talk. Last but not least, I would like to thank all the TA's for their dedication to the class, especially Jacob Swenberg for his help and guidance while writing the paper.

References

[Lan94] Serge Lang. *Algebraic number theory.*, volume 110 of *Grad. Texts Math.* New York: Springer-Verlag, 2nd ed. edition, 1994.

[Mar18] Daniel A. Marcus. *Number fields.* Universitext. Cham: Springer, 2nd edition edition, 2018.

[Mil20] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[Neu07] Jürgen Neukirch. *Algebraische Zahlentheorie*. Berlin: Springer, reprint of the 1992 original edition, 2007.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields.*, volume 83 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed. edition, 1997.