THE p-ADIC NUMBERS AND A PROOF OF THE KRONECKER-WEBER THEOREM

JAE HYUNG SIM

Abstract. This paper is an introduction to the p-adic numbers and their field extensions with the goal of proving the Kronecker-Weber theorem by using the local Kronecker-Weber theorem.

Contents

1. Introduction

As extensions of number fields and their rings of integers are crucial in the study of algebraic number theory, understanding extensions of number fields is an important task. The Kronecker-Weber theorem is a powerful theorem that significantly facilitates this task for abelian extensions of $\mathbb{Q}$.

Theorem 1.1 (Kronecker-Weber)**.** *Any finite abelian extension of $\mathbb{Q}$ is a subextension of a cyclotomic extension of $\mathbb{Q}$.*

This greatly simplifies the study of abelian extensions of $\mathbb{Q}$ by filtering to the study of cyclotomic extensions. Cyclotomic extensions have Galois groups which are readily accessible, so by making use of Galois theory, we can easily construct abelian extensions of $\mathbb{Q}$ by finding quotients of the cyclotomic Galois groups.

To prove this theorem, we will make use of the p-adic numbers $\mathbb{Q}_p$, which is an example of a local field. We will first prove the Kronecker-Weber theorem for $\mathbb{Q}_p$ and "lift" our findings to $\mathbb{Q}$.

Theorem 1.2 (Local Kronecker-Weber)**.** *Any finite abelian extension of $\mathbb{Q}_p$ is a subextension of a cyclotomic extension of $\mathbb{Q}_p$.*

Note that the only difference between the two theorems is their base field: the first being over the rationals and the latter being over the p-adic numbers. However,

Date: August 26, 2018.

the local case is much easier to prove in that the classification of extensions is readily accessible. Our proof of the Kronecker-Weber theorem will rely on the local case.

A crucial part of our proof of the Kronecker-Weber theorem will be the use of Minkowski's theorem which states that for any nontrivial extension of $\mathbb{Q}$, there exists a ramified prime (for readers who are not familiar with the concept of ramification, more explanation will follow in Section 3). As a result, if one can find a way of "getting rid of ramification" for an extension using roots of unity, then the remaining extension must be trivial. In essence, the p-adic numbers will let us do just that.

We begin with a discussion of the p-adic numbers with elementary constructions and properties followed by a discussion of its field extensions. The rigorous proof of the Kronecker-Weber theorem will start at Section 4, so readers with familiarity in local fields and p-adic field extensions can start reading from Section 4. We will assume that the reader has familiarity with Galois theory, Kummer theory, and basic concepts in algebraic number theory such as the discriminant. We will also denote the group of units of a ring R as R^*.

2. p-adic Numbers

For a prime $p \in \mathbb{Z}$, there are three ways of constructing p-adic numbers $\mathbb{Q}_p$ which we will introduce below.

Remark 2.1. Many (though not all) of the results that we will show for p-adic fields can be generalized to local fields and discrete valuation rings. Readers should consult Chapter 1 of [4] for further abstractions.

2.1. **Inverse Limit of $\mathbb{Z}/p^n\mathbb{Z}$.** One way of constructing the p-adic numbers $\mathbb{Q}_p$ is first constructing the p-adic integers $\mathbb{Z}_p$ using the groups $\mathbb{Z}/p^n\mathbb{Z}$.

Definition 2.2.

$$\begin{aligned}\mathbb{Z}_p &:= \varprojlim \mathbb{Z}/p^n\mathbb{Z} \\ &:= \{(a_n)_{n\in\mathbb{N}} \mid a_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ and } a_n \equiv a_{n+1} \bmod p^n\}\end{aligned}$$

The ring operations on $\mathbb{Z}_p$ are "coordinate-wise," so $(a_n) + (b_n) = (a_n + b_n)$ and $(a_n) \cdot (b_n) = (a_n b_n)$. It is easy to verify that these operations satisfy the ring axioms.

One can also verify that thanks to p being prime, $\mathbb{Z}_p$ is an integral domain, so we can define p-adic numbers as follows:

Definition 2.3.

$$\mathbb{Q}_p := \operatorname{Frac}(\mathbb{Z}_p)$$

where Frac denotes the fraction field of the given ring.

However, this definition is not very illuminating in that many p-adic integers are already invertible in $\mathbb{Z}_p$. In fact, one can verify that a p-adic integer x is invertible in $\mathbb{Z}_p$ if (and only if) x is divisible by p. As a result, we get the following equivalent definition.

Definition 2.4.

$$\mathbb{Q}_p := \mathbb{Z}_p\left[\tfrac{1}{p}\right]$$

The inverse limit definition of the p-adic integers gives us a method of working with p-adic integers by looking at their projections onto $\mathbb{Z}/p^n\mathbb{Z}$. The next approach, which is technically equivalent, gives a more accessible interpretation from a metric and topological standpoint.

2.2. **Completion of the p-adic Norm.** The inverse limit naturally provides an injection of $\mathbb{Z}_p$ to $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$, which we will view as a product of discrete topological spaces endowed with the product topology. Our next construction of $\mathbb{Z}_p$ will be to define a metric on $\mathbb{Z}$ whose metric completion will produce $\mathbb{Z}_p$ with a topology that coincides with the subspace topology we would expect from the injection into the product $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$.

To do so, we first define the p-adic valuation.

Definition 2.5. The p-adic valuation is the function $\nu_p : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ where if n is a nonzero integer, then $\nu_p(n)$ is the largest integer such that $p^{\nu_p(n)} \mid n$. For consistency, we define $\nu_p(0) = \infty$.

With this function defined, one can define the p-adic metric on $\mathbb{Z}$ as follows:

Definition 2.6. Let n be a nonzero integer. The p-adic norm of n is defined as

$$|n|_p = \frac{1}{p^{\nu_p(n)}}.$$

For consistency, we define $|0|_p = 0$.

One can easily verify that the p-adic norm satisfies the criteria for a norm. As a result, we get an induced metric $d_p(x, y) := |x - y|_p$ which we call the p-adic metric.

Definition 2.7. The ring of p-adic integers $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the p-adic metric.

We can also extend the valuation to $\mathbb{Q}$ where if $a, b \in \mathbb{Z}$, we define:

$$\nu_p\left(\tfrac{a}{b}\right) := \nu_p(a) - \nu_p(b).$$

This is clearly well-defined since ν_p is a group homomorphism from $\mathbb{Z}^*$ to $\mathbb{Z}$. We can extend the p-adic absolute value and the p-adic metric to $\mathbb{Q}$ with this extended valuation to define the p-adic numbers.

Definition 2.8. The field of p-adic numbers $\mathbb{Q}_p$ is the metric completion of $\mathbb{Q}$ with respect to the p-adic metric.

An important aspect of this approach is that we can observe the compactness of $\mathbb{Z}_p$ in the metric topology: Endow $X := \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ with the product topology where each $\mathbb{Z}/p^n\mathbb{Z}$ is given the discrete topology. By Tychonoff's theorem, X is compact. For all $m, n \in \mathbb{N}$, we can define the open sets

$$U_{m,n} := \{(a_\ell) \in X \mid a_n \equiv m \bmod p^n \text{ and } a_{n+1} \not\equiv a_n \bmod p^n\}.$$

Let U be the union of $U_{m,n}$ for all $m, n \in \mathbb{N}$. As a result, U is an open set and the construction of $\mathbb{Z}_p$ given in Definition 2.2 is exactly $X \setminus U$. Thus, the subspace topology is compact.

Furthermore, this construction is equivalent to our prior definition as follows: Let (a_m) be a Cauchy sequence of integers which converges to $z \in \mathbb{Z}_p$ with respect to the p-adic metric. We can construct a map from $\mathbb{Z}_p$ in Definition 2.7 into $\mathbb{Z}_p$ in Definition 2.2 such that z is mapped to $(z_n) \in \prod \mathbb{Z}/p^n\mathbb{Z}$ where $z_n = \lim_{m\to\infty}(a_m \bmod p^n)$

(this limit always exists since (a_m) is Cauchy with respect to the p-adic metric). It is easy to check that this map is a homeomorphism.

In a similar manner, one can check that Definition 2.4 and Definition 2.8 are equivalent.

In addition, this norm satisfies a criterion that is stronger than the triangle inequality. Notice that for every $x, y \in \mathbb{Z}$, one can check that $\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$. This translates to the following:

Proposition 2.9. *For all $x, y, z \in \mathbb{Q}_p$, $d_p(x,z) \leq \max\{d_p(x,y), d_p(y,z)\}$.*

Metrics that satisfy this property are called **ultrametrics** or **nonarchimedean** metrics. This property will significantly simplify our next approach to p-adic numbers.

2.3. **Power Series.** We can now combine the two approaches to come up with a concrete method of expressing p-adic numbers.

Definition 2.10.

$$\mathbb{Z}_p = \left\{ \sum_{n=0}^{\infty} a_n p^n \mid a_n \in \{0, \cdots, p-1\} \right\}$$

$$\mathbb{Q}_p = \left\{ \sum_{n=-\ell}^{\infty} a_n p^n \mid a_n \in \{0, \cdots, p-1\} \text{ and } \ell < \infty \right\}$$

This approach may seem like a formalism in that power series are being assigned values without regard to convergence. However, if we compare these formal power series to our earlier metric framework, the sequence

$$\left(\sum_{i=0}^{n} a_i p^i \right)_{n \in \mathbb{N}}$$

is a Cauchy sequence in the p-adic metric. In fact, we can construct an explicit equivalence between our definitions of $\mathbb{Z}_p$ by mapping $\sum_{i=0}^{\infty} a_n p^n$ to $\left(\sum_{n=0}^{m-1} a_n p^n \right)_{m \in \mathbb{N}}$. Such a mapping allows us to observe that the valuation of a series $\sum_{i=0}^{\infty} a_n p^n$ coincides with the smallest $n \in \mathbb{Z}$ such that $a_n \neq 0$.

The following are some concrete representations in this form:

Examples 2.11. In $\mathbb{Z}_2$, these are the unique power series representations of the following integers:

$$\begin{aligned} 3 &= 1 \cdot 2^0 + 1 \cdot 2^1 \\ 5 &= 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 \\ -1 &= 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + \cdots \\ &= \sum_{n=0}^{\infty} 1 \cdot 2^n \end{aligned}$$

In fact, for any power series with coefficients in $\mathbb{Z}_p$ (as opposed to $\{0, 1, \cdots, p-1\}$), the power series $\sum_{n=0}^{\infty} a_n x^n$ converges with respect to the p-adic metric if and only if $\lim_{n \to \infty} |a_n x^n|_p = 0$. Recall that $|\cdot|_p$ is defined with respect to the valuation ν_p,

so when analyzing power series, we can focus our attention on the valuations of the terms to identify the necessary conditions on x for the series to converge. Note that since $|\cdot|_p$ is inversely proportional to ν_p, we want $\nu_p(a_n x^n) \to \infty$ for convergence. We demonstrate this framework in the following example.

Example 2.12. If p is an odd prime and $x \in \mathbb{Z}_p$, then

$$\exp(x) \in \mathbb{Z}_p \Leftrightarrow \nu_p(x) \geq 1.$$

We can show this by first noting that the formal power series that represents $\exp(x)$ is

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

If $\nu_p(x) \geq 1$, then $p \,|\, x$, so

$$\begin{aligned}
\lim_{n\to\infty} \nu_p\left(\frac{x^n}{n!}\right) &\geq \lim_{n\to\infty} \nu_p\left(\frac{p^n}{n!}\right) \\
&\geq \lim_{n\to\infty} \nu_p\left(\frac{p^n}{p^{n/(p-1)}}\right) \\
&= \lim_{n\to\infty} n - \frac{n}{p-1} \\
&= \lim_{n\to\infty} n \cdot \frac{p-2}{p-1} \\
&= \infty.
\end{aligned}$$

which implies that the power series converges within $\mathbb{Z}_p$.

If $\nu_p(x) = 0$, then we get a similar computation as follows:

$$\begin{aligned}
\lim_{n\to\infty} \nu_p\left(\frac{x^n}{n!}\right) &= \lim_{n\to\infty} \nu_p\left(\frac{1}{n!}\right) \\
&= -\infty
\end{aligned}$$

so the power series does not converge to a value in $\mathbb{Z}_p$.

As we will see in Section 3.2, there is an analogue to this power series framework in finite extensions of the p-adic numbers which we will use extensively in our proof of the local Kronecker-Weber theorem.

2.4. **Commutative Algebra of Local Fields.** Our next task is to translate properties of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ to extensions of the p-adic numbers. To do so, we start with the following definition.

Definition 2.13. Let L be a finite extension of $\mathbb{Q}$ (or $\mathbb{Q}_p$). The ring of integers $\mathcal{O}_L$ is the integral closure of $\mathbb{Z}$ (resp. $\mathbb{Z}_p$) in K, i.e.

$$\mathcal{O}_L = \{z \in L \mid z \text{ is the root of a monic polynomial } f(x) \in \mathbb{Z}[x] \,(\text{resp. } \mathbb{Z}_p)\}.$$

The following two paragraphs will be a quick discussion on the ring of integers and its importance without rigorous proofs of all claims. If the reader is interested in learning the proofs of these claims, they should consult Chapter 12 of [1].

The ring of integers of a number field allows us to translate the notion of prime numbers to general number fields. However, most rings of integers are not unique factorization domains, so we do not always have explicit prime numbers. Luckily, rings of integers are Dedekind domains, so every ideal has a unique factorization into

prime ideals. Thus, with this slight alteration, we can translate many properties of primes in the rationals/integers to other number fields.

The simplest example of a ring of integers is $\mathbb{Z}$ within $\mathbb{Q}$. Similarly, as our construction of $\mathbb{Q}_p$ may suggest, $\mathbb{Z}_p$ is the ring of integers within $\mathbb{Q}_p$. However, this fact may not be rigorous transparent from the definition of the ring of integers.

In general, finding the ring of integers given a number field is not always straightforward, but when one has a nonarchimedean absolute value $|\cdot|_L$ on a number field L, the ring of integers is much easier to find. In fact, if L is a finite extension of $\mathbb{Q}_p$, the ring of integers is precisely $\{z \in L \,||z|_L \leq 1\}$. Note that in the context of $\mathbb{Q}_p$ with the p-adic absolute value, the elements with absolute values less than or equal to 1 are precisely the p-adic integers.

We now take the opportunity to define a discrete valuation and a discrete valuation ring:

Definition 2.14. A discrete valuation ν is a function from a field L to $\mathbb{Z} \cup \{\infty\}$ such that for all $x, y \in L$:

(a) $\nu(x) = \infty$ if and only if $x = 0$
(b) $\nu(xy) = \nu(x) + \nu(y)$
(c) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$

Definition 2.15. A discrete valuation ring A is an integral domain such that there is a discrete valuation ν on $L = \mathrm{Frac}(A)$ such that $A = \{z \in L \mid \nu(z) \geq 0\}$.

Proposition 2.16. *If A is a discrete valuation ring, then A is integrally closed and A has a unique non-zero prime ideal.*

For a rigorous proof of the proposition, the reader can refer to Proposition 3 in Chapter 1.2 of [4]. For our purposes, it is sufficient to know that $\mathbb{Z}_p$ is a discrete valuation ring with respect to the valuation ν_p defined on $\mathbb{Q}_p$. We will also build a valuation on finite extensions $L/\mathbb{Q}_p$ which will also make $\mathcal{O}_K$ a discrete valuation ring. As a result, by Proposition 2.16, we can restrict ourselves to focusing on just one prime in $\mathbb{Z}_p$ and $\mathcal{O}_L$ as opposed to the many primes that exist in other rings of integers like $\mathbb{Z}$.

3. Field Extensions of the p-adic numbers

Now that we have established some basic facts about $\mathbb{Q}_p$, we want to look at its field extensions. Though we can quickly package finite field extensions of the p-adic numbers as quotients of the polynomial ring $\mathbb{Q}_p[x]$, the structure of the p-adic numbers (specifically its local nature) gives us stronger properties about its finite extensions than one would expect in extensions of $\mathbb{Q}$.

Let $L/\mathbb{Q}_p$ be a finite Galois extension of the p-adic numbers. We can uniquely extend our p-adic valuation to L as follows:

To define our our valuation ν_L on L, we first define an intermediate function ν_p' on L. If $\alpha \in \mathbb{Q}_p$, we let $\nu_p'(\alpha) = \nu_p(\alpha)$. If $\alpha \in L$ is not in $\mathbb{Q}_p$, we can observe that if $N : L \to \mathbb{Q}_p$ (called the norm function) is the product of the Galois conjugates of α, $N(\alpha)$ is in $\mathbb{Q}_p$. We would like ν_p' to be a Galois invariant group homomorphism on L^*, so the following must hold:

$$\nu_p'(N(\alpha)) = \nu_p'\left(\prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)} \sigma(\alpha)\right) = \left|\mathrm{Gal}(L/\mathbb{Q}_p)\right| \cdot \nu_p'(\alpha).$$

In fact, this criterion now uniquely determines ν_p'. Notice that ν_p' maps to $\frac{1}{e}\mathbb{Z}\cup\{\infty\}$ for some $e \in \mathbb{N}$ (this value will have significance in Section 3.1). To get a true discrete valuation, we define $\nu_L(x) = e \cdot \nu_p'(x)$.

This valuation makes the ring of integers $\mathcal{O}_L$ a discrete valuation ring, so $\mathcal{O}_L$ has a unique maximal prime ideal. This will greatly simply the discussion of ramification of primes in the following section.

3.1. **Ramification of Ideals.** In algebraic number theory, we say that a prime p is unramified in an extension $L/\mathbb{Q}$ if the (possibly trivial) factorization of (p) into prime ideals in $\mathcal{O}_L$ has no exponents greater than 1. Alternatively, p is ramified if there is a prime ideal $\mathfrak{p}$ in $\mathcal{O}_L$ such that $(p) \subset \mathfrak{p}^2$. Furthermore, if (p) is ramified and there is a unique prime ideal that divides (p), then we say that (p) is totally ramified. However, if L is a finite extension of $\mathbb{Q}_p$, then we demonstrated that $\mathcal{O}_L$ has a unique prime ideal. Since $\mathbb{Z}_p$ also has a unique prime ideal, we only need to consider the cases of unramified and totally ramified extensions when our base field is $\mathbb{Q}_p$. For the remainder of this section, L will be a finite extension of $\mathbb{Q}_p$ with $\mathcal{O}_L$ as its ring of integers.

At first, our approach will seem tangential, but the following definitions of unramified and totally ramified extensions will coincide with the above.

We first define ramification degree. Recall that when extending the p-adic valuation to L, we first defined ν_p' which mapped to $\frac{1}{e}\mathbb{Z} \cup \{\infty\}$ for some $e \in \mathbb{N}$. We define e to be the **ramification degree** of $L/\mathbb{Q}_p$. We say that L is an unramified extension if $e = 1$. This coincides with the definition of unramified above, since if $e = 1$, then p still generates the unique prime ideal. However, the value of e is insufficient in describing unramified extensions. To complete the picture, we define a different value called the inertial degree as follows:

Let $\mathfrak{m}(L)$ denote the maximal ideal of the ring of integers $\mathcal{O}_L$. We define $\ell := \mathcal{O}_L/\mathfrak{m}(L)$ to be the **residue field** of L. Since L is an extension of $\mathbb{Q}_p$, $\mathbb{Z}_p \subset \mathcal{O}_L$ and $p\mathbb{Z}_p \subset \mathfrak{m}(L)$. It follows that $\mathfrak{m}(L) \cap \mathbb{Z}_p = p\mathbb{Z}_p$, so $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p \subset \mathcal{O}_L/\mathfrak{m}(L)$. The degree $f := \left[\ell : \mathbb{F}_p\right]$ is called the **inertial degree** of $L/\mathbb{Q}_p$. It is not entirely transparent that f is a finite value. However, since L is a finite extension of $\mathbb{Q}_p$, $\mathcal{O}_L$ is a finitely generated free $\mathbb{Z}_p$-module (for rigorous proof, refer to Proposition 12.2.2 of [1]). Then, as an abelian group, $\mathcal{O}_L = \bigoplus_{i=1}^{n} \mathbb{Z}_p$ for some $n \in \mathbb{N}$. Since $p\mathcal{O}_L$ is a proper ideal, $p\mathcal{O}_L \subset \mathfrak{m}(L)$. As a result, $\#(\mathcal{O}_L/p\mathcal{O}_L) = n \cdot p$, and since $\mathcal{O}_L/p\mathcal{O}_L$ surjects onto $\mathcal{O}_L/\mathfrak{m}(L)$, ℓ must be finite. Thus, $f = \left[\ell : \mathbb{F}_p\right]$ is finite.

A powerful property of the ramification degree and inertial degree is the following theorem.

Theorem 3.1. *If $L/\mathbb{Q}_p$ is Galois, then $\left[L : \mathbb{Q}_p\right] = ef$ where e is the ramification degree and f is the inertial degree.*

The idea for the proof of this theorem will be to work with the ring of integers as a free abelian $\mathbb{Z}_p$-module and show that its rank is equal to ef which will correspond to the degree $\left[L : \mathbb{Q}_p\right]$. As the rigorous proof of the theorem is not very enlightening in our context, we omit it, but interested readers can refer to Proposition 10 in Chapter 1.5 of [4].

3.2. **Residue Fields and Ring of Integers.** A very convenient property of the residue field will be its role in extending the idea of power series representations of elements of $\mathbb{Z}_p$ to $\mathcal{O}_L$. Let $\pi \in \mathcal{O}_L$ be such that $\nu_L(\pi) = 1$. Then, we know that

$(\pi) = \mathfrak{m}(L)$, so for all $a \in \mathcal{O}_L$, there exists some $a_0 \in \ell$ such that $a \equiv a_0 \bmod \pi$. We can then look at a modulo π^2 to get that $a \equiv a_0 + a_1\pi \bmod \pi^2$. By continuing this process, we can get a representation of a as a power series $\sum_{i=0}^{\infty} a_i\pi^i$ where $a_i \in \ell$. Such an element π is called a **uniformizer**. Note that the uniformizer is not unique since $-\pi$ would be a perfectly legitimate choice of uniformizer. However, as we will see later on, some choices of uniformizer will naturally facilitate calculations.

Remark 3.2. Given a power series representation $\sum_{i=0}^{\infty} a_i\pi^i$ as constructed above, the coefficients a_i are representatives in ℓ. As a result, there seems to be a choice involved in lifting these representatives to $\mathcal{O}_L$. However, we know that $\ell = \mathbb{F}_{p^\ell}$ for some n and therefore its elements are characterized by the polynomial $x^{p^n} - x$. Thus, by use of Theorem 3.4, we will be able to lift the elements of ℓ to $\mathcal{O}_L$ to get a canonical choice of elements for coefficients.

Unfortunately, this choice of canonical coefficients does not necessarily coincide with the specific choice of coefficients used in Definition 2.10 (i.e. $1, \cdots, p-1$).

Proposition 3.3. *If $\alpha \in \mathcal{O}_L$ is such that $\nu(\alpha) = 0$, then $\alpha \in \mathcal{O}_L^*$.*

Proof. If α has valuation 0, without loss of generality, we can let $\alpha \equiv 1 \bmod \pi$ for a uniformizer π: since otherwise, we can see that $\alpha^{p^f-1} \cong 1 \bmod \pi$. Then, $\alpha = 1 + \pi \cdot \beta$ for some $\beta \in \mathcal{O}_L$. By taking $u_1 = 1 + \pi z_1$ such that $\nu(z_1 + \beta) \geq 1$, we get that $u_1 \cdot \alpha = 1 + \pi^2\beta_2$ for some $\beta_2 \in \mathcal{O}_L$. Similarly, we can construct $u = 1 + \sum_{i=1}^{\infty} z_i\pi^i$ such that for all $n \in \mathbb{N}$, $\alpha \cdot u \equiv 1 \bmod \pi^n$. The element u is, by construction, in $\mathcal{O}_L$, so $\alpha \in \mathcal{O}_L^*$. □

This process of inductively lifting an element in ℓ to $\mathcal{O}_L$ can be used to prove the following powerful theorem.

Theorem 3.4 (Hensel's Lemma for $\mathbb{Q}_p$)**.** *Given $L/\mathbb{Q}_p$, if $g(x) \in \mathcal{O}_L[x]$ is a monic, separable polynomial and $\overline{g}(x) \in \ell[x]$ is its reduction* modπ*, then any simple root $\overline{\alpha}$ of $\overline{g}$ has a unique lift $\alpha \in \mathcal{O}_L$ such that $g(\alpha) = 0$.*

Proof. Let $g(x) \in \mathcal{O}_L[x]$ satisfy the given criteria with $\overline{\alpha}$ being a root of $\overline{g}(x)$. It suffices to show that for any lift $\alpha' \in \mathcal{O}_L$ of $\overline{\alpha}$, there exists $z \in \mathcal{O}_L$ such that $f(\alpha' + \pi \cdot z) = 0$. Recall that in general,

$$g(z+h) = g(z) + \sum_{i=1}^{\infty} \frac{g^{(i)}(z)}{i!} \cdot h^i$$

where $g^{(i)}$ is the i-th formal derivative of g. We use the following calculation to find a candidate for z.

$$\begin{aligned}
g(\alpha' + \pi \cdot z) &= g(\alpha') + \sum_{i=1}^{\infty} \frac{g^{(i)}(\alpha')}{i!} \cdot \pi^i z^i \\
&= \pi \cdot k + \sum_{i=1}^{\infty} \frac{g^{(i)}(\alpha')}{i!} \cdot \pi^i z^i \qquad \text{for some } k \in \mathcal{O}_L \\
-\pi \cdot k &= \sum_{i=1}^{\infty} \frac{g^{(i)}(\alpha')}{i!} \cdot \pi^i z^i \\
z \cdot g^{(1)}(\alpha') &= -k - \sum_{i=1}^{\infty} \frac{g^{(i+1)}(\alpha')}{(i+1)!} z^{i+1}\pi^i.
\end{aligned}$$

Since g is separable, we know that $g^{(1)}(\alpha') \not\equiv 0 \bmod \pi$, so we know that $g^{(1)}(\alpha')$ is a unit in $\mathcal{O}_L$. Thus,

$$z = -(g^{(1)}(\alpha'))^{-1}\left(k + \sum_{i=1}^{\infty} \frac{g^{(i+1)}(\alpha')}{(i+1)!} z^{i+1}\pi^i\right).$$

This expression for z is now sufficient to show both existence and uniqueness of an element $z \in \mathcal{O}_L$. This is because in a discrete valuation ring, an element's equivalence class modulo powers of a uniformizer is sufficient to uniquely specify an element. The expression above for z uniquely determines the equivalence class of z modulo π^n for any $n \in \mathbb{N}$.

To see this concretely, for any fixed $n \in \mathbb{N}$, we take the expression above modulo π^n to get a finite sum. For each term of this sum, we can replace z with the series above and get another finite sum modulo π^n. Each substitution will increase the valuation of any term involving z, so a finite number of iterations will yield a fixed finite sum. We demonstrate this process for the case of taking modulo π^2 (for the sake of simplicity, we let $f^{(1)}(\alpha) = -1$):

$$\begin{aligned} z &\equiv k + \pi \cdot \frac{f^{(2)}(\alpha)}{2} \cdot z^2 && \bmod \pi^2 \\ &\equiv k + \pi \cdot \frac{f^{(2)}(\alpha)}{2} \cdot \left(k + \pi \cdot \frac{f^{(2)}(\alpha)}{2} \cdot z^2\right)^2 && \bmod \pi^2 \\ &\equiv k + \pi \cdot \frac{f^{(2)}(\alpha)}{2} \cdot k^2 && \bmod \pi^2. \end{aligned}$$

□

A quick application of Hensel's lemma reveals that $\mathbb{Z}_p$ contains a primitive $(p-1)$-root of unity. Recall that if $L = \mathbb{Q}_p$, $\mathcal{O}_L = \mathbb{Z}_p$ and $\ell = \mathbb{F}_p$. If $f(x)$ is the $(p-1)$-st cyclotomic polynomial, then $\bar{f}(x)$ is separable with a root in $\mathbb{F}_p$. It follows from Theorem 3.4 that there exists $\alpha \in \mathcal{O}_L$ which is a primitive $(p-1)$-st root of unity.

4. The Local Kronecker-Weber Theorem

The goal of this section will be to prove the local Kronecker-Weber theorem. For reference, we restate the theorem below.

Theorem 4.1. *Let $p \in \mathbb{N}$ be a prime number. Then, every abelian extension of $\mathbb{Q}_p$ arises as a subextension of a cyclotomic extension of $\mathbb{Q}_p$.*

We will first show that all unramified extensions of $\mathbb{Q}_p$ are cyclotomic extensions. We will then address the ramified extensions by categorizing them into "tamely ramified" extensions and "wildly ramified" extensions.

4.1. Unramified Extensions.

Our first step is to classify unramified extensions as cyclotomic extensions.

Recall that if $L/\mathbb{Q}_p$ is unramified, then $e = 1$, so by Theorem 3.1, $f = \big[L : \mathbb{Q}_p\big]$. Since ℓ is a finite extension of $\mathbb{F}_p$, it follows that $\ell = \mathbb{F}_p(\zeta_m)$ for some $m \in \mathbb{N}$ that is prime to p. By using Theorem 3.4, we can lift ζ_m to $\mathcal{O}_L$. Furthermore, Theorem 3.4

allows us to see that $\big[\mathbb{Q}_p(\zeta_m) : \mathbb{Q}_p\big] \geq \big[\mathbb{F}_p(\zeta_m) : \mathbb{F}_p\big]$, so we get the following:

$$\begin{aligned} f &= \big[L : \mathbb{Q}_p\big] \\ &\geq \big[\mathbb{Q}_p(\zeta_m) : \mathbb{Q}_p\big] \\ &\geq \big[\mathbb{F}_p(\zeta_m) : \mathbb{F}_p\big] \\ &= f. \end{aligned}$$

Thus, $L = \mathbb{Q}_p(\zeta_m)$.

4.2. **Tamely Ramified Extensions.** For extensions $L/\mathbb{Q}_p$ that are ramified, we can use the same process above to get an unramified subextension $K = \mathbb{Q}_p(\zeta_m) \subset L$. We call K the maximal unramified subextension of L. We can see that K has degree $\big[K : \mathbb{Q}_p\big] = f$, so since $\big[L : \mathbb{Q}_p\big] = [L : K] \cdot \big[K : \mathbb{Q}_p\big]$, we get that $[L : K] = e$. The corresponding tower diagram is shown below.

$$\begin{array}{c} L \\ \Big| e \\ \mathbb{Q}_p(\zeta_m) \\ \Big| f \\ \mathbb{Q}_p \end{array}$$

At this point, it is helpful to classify ramified extensions of $\mathbb{Q}_p$ into two categories: tamely ramified extensiosn and wildly ramified extensions.

Definition 4.2. Let $L/\mathbb{Q}_p$ be a ramified extension. The extension $L/\mathbb{Q}_p$ is a tamely ramified extension if $p \nmid e$. If $p \mid e$, $L/\mathbb{Q}_p$ is a wildly ramified extension.

Suppose $L/\mathbb{Q}_p$ is a tamely ramified extension. Let π be a uniformizer of the extension, so that $\pi^e = u \cdot p$ for some unit $u \in \mathcal{O}_L^*$. We know that the reduction $\overline{u}$ in ℓ is nonzero, so the polynomial $x^e - \overline{u}$ is separable. If ℓ does not contain an e-th root of $\overline{u}$, we can shift our focus to $L(\zeta_m)$ such that $p \nmid m$ and the residue field ℓ' of $L(\zeta_m)$ has an e-th root of $\overline{u}$. Note that adjoining ζ_m only extends our unramified subextension and the ramified part of our extension is unaffected. By applying Theorem 3.4 in $L(\zeta_m)$, we can find an e-th root of u which gives us a uniformizer that is exactly $p^{1/e}$.

Since our discussion above required adjoining some extra root of unity, it is not true that every tamely ramified extension is obtained by adjoining an e-th root of p to its maximal unramified subextension. However, by shifting our framework to working above the maximal unramified extension of $\mathbb{Q}_p$, we get every (prime-to-p)-root of unity.

Remark 4.3. Although we did not affect the ramified part of our extension by adjoining a root of unity in this case, it is worth noting that in general, adding any root of unity can affect ramification. Specifically, adding an m-th root of unity where $p \mid m$ can add ramification to our extension.

We refer to the maximal tamely ramified extension as $\mathbb{Q}_p^{\text{tame}}$ and the maximal unramified extension as $\mathbb{Q}_p^{\text{ur}}$. By the previous discussion, we know that

$$\mathbb{Q}_p^{\text{tame}} = \mathbb{Q}_p^{\text{ur}}(\{p^{1/e}\}_{p \nmid e}) \text{ and } \mathbb{Q}_p^{\text{ur}} = \mathbb{Q}_p(\{\zeta_\ell\}_{p \nmid \ell}).$$

These maximal extensions are profinite extensions, so we can compute the Galois groups:

The Chinese remainder theorem tells us that

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}_p^{\mathrm{ur}}) &= \varprojlim_{p\nmid e} \mathbb{Z}/e\mathbb{Z} \\ &= \prod_{\substack{\ell\neq p \\ \ell \text{ prime}}} \varprojlim \mathbb{Z}/\ell^n\mathbb{Z} \\ &= \prod_{\substack{\ell\neq p \\ \ell \text{ prime}}} \mathbb{Z}_\ell.\end{aligned}$$

In a similar fashion, we can see that

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z} \simeq \widehat{\mathbb{Z}}.$$

As a result, we get the following tower:

$$\begin{array}{c} \mathbb{Q}_p^{\mathrm{tame}} = \mathbb{Q}_p^{\mathrm{ur}}(\{p^{1/e}\}_{p\nmid e}) \\ \Big| \ \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}_p^{\mathrm{ur}}) = \textstyle\prod_{\ell\neq p}\mathbb{Z}_\ell \\ \mathbb{Q}_p^{\mathrm{ur}} = \mathbb{Q}_p(\{\zeta_m\}_{p\nmid m}) \\ \Big| \ \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \widehat{\mathbb{Z}} \\ \mathbb{Q}_p \end{array}$$

Recall that for all $n \in \mathbb{N}$, there is a caononical isomorphism that maps $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ to $\mathbb{Z}/n\mathbb{Z}$ where the Frobenius Frob_p is mapped to $1 \in \mathbb{Z}/n\mathbb{Z}$. It follows that we can choose a lift $g \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}_p)$ of Frob_p. We then know that $\langle g\rangle \subset \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}$, so its topological closure $\widehat{\langle g\rangle}$ surjects onto $\hat{\mathbb{Z}}$. However, since all completions of $\mathbb{Z}$ are subsets of $\hat{\mathbb{Z}}$ when the generator is mapped to the generator of $\hat{\mathbb{Z}}$, it follows that $\widehat{\langle g\rangle} \simeq \hat{\mathbb{Z}}$.

Thus, we get that

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}_p) = \left(\prod_{\ell\neq p}\mathbb{Z}_p\right) \rtimes \hat{\mathbb{Z}}.$$

To find the maximal abelian tamely ramified extension $\mathbb{Q}_p^{\mathrm{tame,ab}}$, we now find the abelianization of $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}_p)$ and classify the corresponding extension. To do so, we first need to explicitly compute the semi-direct product.

Since $\prod_{\ell\neq p}\mathbb{Z}_\ell = \varprojlim_{p\nmid e}\mathbb{Z}/e\mathbb{Z}$, let σ be the generator of $\mathbb{Z}/e\mathbb{Z}$ for some e such that $\sigma(p^{1/e}) = \zeta_e p^{1/e}$. Then, if g is a lift of Frob_p, we get the following:

$$\begin{aligned}(g\sigma g^{-1})(p^{1/e}) &= g(\zeta_e \cdot g^{-1}(p^{1/e})) \\ &= g(\zeta_e)\cdot p^{1/e} \\ &= \zeta_e^p \cdot p^{1/e}.\end{aligned}$$

This means that our semi-direct product can be represented as the topological closure of the following semi-direct product:

$$\langle \sigma, g \mid g\sigma g^{-1} = \sigma^p \rangle.$$

It follows that the abelianization takes the following form:

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}_p)^{\mathrm{ab}} &= \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tame,ab}}/\mathbb{Q}_p) \\ &= \langle \sigma, g \mid \sigma^{p-1} = 1; \sigma g = g\sigma \rangle^{\mathrm{closure}} \\ &= \mathbb{Z}/(p-1)\mathbb{Z} \times \widehat{\mathbb{Z}}. \end{aligned}$$

The corresponding subextension for the abelianization of the semidirect product must have the property that $\zeta_e^{p-1} = 1$, so $e \mid (p-1)$. Thus,

$$\mathbb{Q}_p^{\text{tame, ab}} = \mathbb{Q}_p^{\mathrm{ur}}(p^{1/(p-1)}).$$

We can quickly see that this extension is exactly $\mathbb{Q}_p^{\mathrm{ur}}(\zeta_p)$: recall that $\mathbb{Q}_p$ contains ζ_{p-1}, so by Kummer theory, there exists $\ell \in \mathbb{Q}_p$ such that $\mathbb{Q}_p^{\mathrm{ur}}(\zeta_p) = \mathbb{Q}_p^{\mathrm{ur}}(\ell^{p-1})$. Let $\omega = \zeta_{p-1}$ and consider the Gauss sum

$$\alpha = \zeta_p + \omega\zeta_p^k + \omega^2\zeta_p^{k^2} + \cdots + \omega^{p-2}\zeta_p^{k^{p-2}}$$

where k is a choice of a multiplicative generator of $\mathbb{F}_p^*$. If σ sends ζ_p to ζ_p^k, then σ generates the Galois group and $\sigma(\alpha) = \omega\alpha$. A quick calculation shows that $\alpha^{p-1} = -p$, so we get that α is both nonzero and is a primitive element of the extension.

4.3. **Wildly Ramified Extensions.** With our classification of ramification, we can build a tower for any finite extension $L/\mathbb{Q}_p$ as follows: Let K be the maximal unramified subextension of L and K' be the maximal tamely ramified subextension of L. By comparing our previous findings and Theorem 3.1, we can see that $w \cdot u = e$ where $w = \big[L : K'\big]$ and $u = \big[K' : K\big]$. Furthermore, since K' is the maximal subextension whose degree is coprime to p, it follows that w is a power of p.

$$\begin{array}{c} L \\ \big| \, w \\ K' \\ \big| \, u \\ K \\ \big| \, f \\ \mathbb{Q}_p \end{array}$$

If our extension is abelian, we can take $\mathrm{Gal}(L/\mathbb{Q}_p) = P \times Q$ where P is the p-Sylow subgroup and Q has order prime to p. As a result, $L = L^Q.L^P$ where L^Q and L^P are the fixed fields of Q and P, respectively. We already know that L^P is precisely K', so it is sufficient so show that L^Q is a subextension of a cyclotomic extension.

First, we will work with odd primes p and address the edge case of $p = 2$ afterward.

Since P is abelian, the subgroup P^p is normal. Furthermore, we can use the structure theorem for finite abelian groups to decompose P into r cyclic p-power factors for some $r \in \mathbb{N}$. To find a bound for r, we can consider the Galois extension that is fixed by P^p since its Galois group will take on the form $P/(P^p) = (\mathbb{Z}/p\mathbb{Z})^r$. We now show that $r \leq 2$.

If L is a Galois extension of $\mathbb{Q}_p$ such that $\mathrm{Gal}(L/\mathbb{Q}_p) = C_p^r$, then we can adjoin ζ_p to both L and $\mathbb{Q}_p$ without affecting the Galois group, i.e. $\mathrm{Gal}(L(\zeta_p)/\mathbb{Q}_p(\zeta_p)) = (\mathbb{Z}/p\mathbb{Z})^r$. By Kummer theory, we know that $L(\zeta_p)$ is obtained by adjoining r multiplicatively independent p-th roots of elements in $\mathbb{Q}_p(\zeta_p)^*$. Thus, we shift focus to see how many independent p-th roots of elements in $\mathbb{Q}_p(\zeta_p)^*$ there are which will yield abelian Galois extensions not only over $\mathbb{Q}_p(\zeta_p)$ but also $\mathbb{Q}_p$.

Suppose $\alpha \in \mathbb{Q}_p(\zeta_p)$ is such that $\mathbb{Q}_p(\zeta_p, \alpha^{1/p})$ is a Galois extension over $\mathbb{Q}_p$. This is true if and only if the Galois closure of $\mathbb{Q}_p(\zeta_p, \alpha^{1/p})$ over $\mathbb{Q}_p$ is itself, which in turn is true if and only if for all $g \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$,

$$\mathbb{Q}_p(\zeta_p, \alpha^{1/p}) = \mathbb{Q}_p(\zeta_p, g(\alpha)^{1/p}).$$

In other words, if we view $\mathbb{Q}_p(\zeta_p)^*/(\mathbb{Q}_p(\zeta_p)^*)^p$ as an $\mathbb{F}_p$ vector space, we need the subspace generated by α to contain $g(\alpha)$ to get a Galois extension.

We will now decompose $\mathbb{Q}_p(\zeta_p)^*/\mathbb{Q}_p(\zeta_p)^{*p}$ as a $\mathbb{F}_p$ vector space. Let ν be the extended valuation on $\mathbb{Q}_p(\zeta_p)$ and note that $\pi = \zeta_p - 1$ has valuation 1. If $\alpha \in \mathbb{Q}_p(\zeta_p)^*$, $\alpha = \pi^{\nu(\alpha)}\beta$ where $\nu(\beta) = 0$. Thus, we can express $\mathbb{Q}_p(\zeta_p)^*$ as follows:

$$\mathbb{Q}_p(\zeta_p)^* = \pi^{\mathbb{Z}} \times \mathcal{O}^*$$

where $\mathcal{O}$ is the ring of integers of $\mathbb{Q}_p(\zeta_p)$ (recall that the units of $\mathcal{O}$ are exactly the elements with valuation 0). The residue field is $\ell = \mathbb{F}_p$ since $\mathbb{Q}_p(\zeta_p)$ is totally ramified. By Remark 3.2, every element in $\mathcal{O}^*$ can be presented as $\zeta + \pi\beta$ where $\zeta \in \mathbb{F}_p^*$ and $\beta \in \mathcal{O}$, so for every $\alpha \in \mathcal{O}^*$, $\mathcal{O}^* = \mathbb{F}_p^* \times (1 + \pi\mathcal{O})$.

Proposition 4.4.

$$(1 + \pi\mathcal{O})^p = 1 + \pi^{p+1}\mathcal{O}$$

Proof. Observe the following calculation:

$$\begin{aligned}(1 + \pi x)^p &= 1 + p\pi x + \binom{p}{2}\pi^2 x^2 + \cdots + \binom{p}{p-1}\pi^{p-1}x^{p-1} + \pi^p x^p \\ &\equiv 1 + p\pi(x - x^p) \bmod \pi^{p+1} \\ &\equiv 1 \bmod \pi^{p+1}\end{aligned}$$

(recall that $\pi^{p-1} = -p$). Thus, $(1 + \pi\mathcal{O})^p \subset 1 + \pi^{p+1}\mathcal{O}$.

If we have $1 - \pi^{p+1}x$ for some $x \in \mathcal{O}$, then we get the following:

$$(1 - \pi^{p+1}x)^{1/p} = 1 + \sum_{n=1}^{\infty} \frac{\frac{1}{p}\left(\frac{1}{p} - 1\right)\cdots\left(\frac{1}{p} - n\right)}{n!}(\pi^{p+1}x)^n$$

$$\begin{aligned}\nu\left(\frac{\frac{1}{p}\left(\frac{1}{p} - 1\right)\cdots\left(\frac{1}{p} - n\right)}{n!}(\pi^{p+1}x)^n\right) &\geq \nu\left(\frac{\pi^{n(p+1)}}{p^n \cdot p^{n/(p-1)}}\right) \\ &= n(p+1) - pn = n.\end{aligned}$$

Thus, $(1 - \pi^{p+1}x)^{1/p} \in \mathcal{O}^*$, so $1 + \pi^{p+1}\mathcal{O} \subset (1 + \pi\mathcal{O})^p$. □

We now have the following:

$$\mathbb{Q}_p(\zeta_p)^* = \pi^{\mathbb{Z}} \times \mathbb{F}_p^* \times (1 + \pi\mathcal{O}),$$

so Proposition 4.4 lets us conclude that:

$$\mathbb{Q}_p(\zeta_p)^*/\mathbb{Q}_p(\zeta_p)^{*p} = \pi^{\mathbb{Z}/p\mathbb{Z}} \times (1 + \pi\mathcal{O})/(1 + \pi^{p+1}\mathcal{O}).$$

Ideally, we would like to find a generator of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$, but finding a canonical generator is not quite possible. We work around having to make a choice by defining the function $\chi : \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \to \mathbb{Z}/p\mathbb{Z}^*$ defined implicitly for each $\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ by the condition that $\sigma(\zeta_p) = \zeta_p^{\chi(\sigma)}$. Then,

$$\begin{aligned}
\sigma(\pi) &= \sigma(\zeta_p - 1) \\
&= \sigma(\zeta_p) - 1 \\
&= \zeta_p^{\chi(\sigma)} - 1 \\
&= (\zeta_p - 1)(\zeta_p^{\chi(\sigma)-1} + \zeta_p^{\chi(\sigma)-2} + \cdots + 1) \\
&= \pi((\pi + 1)^{\chi(\sigma)-1} + (\pi + 1)^{\chi(\sigma)-2} + \cdots + 1) \\
&\equiv \chi(\sigma) \cdot \pi \bmod \pi^2.
\end{aligned}$$

We then filter $(1 + \pi\mathcal{O})/(1 + \pi^{p+1}\mathcal{O})$ as:

$$\frac{1 + \pi\mathcal{O}}{1 + \pi^{p+1}\mathcal{O}} = \frac{1 + \pi\mathcal{O}}{1 + \pi^2\mathcal{O}} \times \frac{1 + \pi^2\mathcal{O}}{1 + \pi^3\mathcal{O}} \times \cdots \times \frac{1 + \pi^p\mathcal{O}}{1 + \pi^{p+1}\mathcal{O}}.$$

In each $(1 + \pi^n\mathcal{O})/(1 + \pi^{n+1}\mathcal{O})$, $1 + \pi^n$ is a generator and $1 + \ell\pi^n$ belongs to the coset $[(1 + \pi^n)^\ell]$. As a result, we get that $\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ acts on $(1 + \pi^n\mathcal{O})/(1 + \pi^{n+1}\mathcal{O})$ by the eigenvalue $\chi^n(\sigma) \in (\mathbb{Z}/p\mathbb{Z})^*$ where $\chi^n(\sigma)$ is defined as $\chi(\sigma)^n$. Thus, our decomposition of $\mathbb{Q}_p(\zeta_p)^*/\mathbb{Q}_p(\zeta_p)^{*p}$ is a decomposition into eigenspaces.

Our next step is to identify which of these eigenspaces produces abelian extensions over $\mathbb{Q}_p$. If we consider the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p, \alpha^{1/p}/\mathbb{Q}_p)$ where α is taken from one of the factors in the decomposition above, we know the group will be generated by g and σ where σ is lifted from $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ and g maps $\alpha^{1/p}$ to $\zeta_g\alpha^{1/p}$ where ζ_g is a p-th root of unity. To get an abelian extension, we need g and σ to commute. Suppose $\sigma(\alpha) = \alpha^s$. Then, we get the following:

$$(g\sigma)(\alpha^{1/p}) = g(\alpha^s)^{1/p} = (\zeta_g\alpha)^{s/p}$$

$$(\sigma g)(\alpha^{1/p}) = \sigma(\zeta_g\alpha)^{1/p} = \sigma(\zeta_g)^{1/p}\alpha^{s/p}.$$

Thus, we need σ to act on α and ζ_g by the same eigenvalue.

Note that $\zeta_p = 1 - \pi \in 1 + \pi\mathcal{O}$, so ζ_p has the eigenvalue $\chi(\zeta_p)$. Thus, to find the elements in $\mathbb{Q}_p(\zeta_p)^*$ whose p-th roots produce abelian extensions over $\mathbb{Q}_p$, we want to find the number of one dimensional subspaces of $\mathbb{Q}_p(\zeta_p)^*/\mathbb{Q}_p(\zeta_p)^{*p}$ with eigenvalue $\chi(\sigma)$. By our calculations above, $(1+\pi\mathcal{O})/(1+\pi^2\mathcal{O})$ and $(1+\pi^p\mathcal{O})/(1+\pi^{p+1}\mathcal{O})$ are the only lines in our decomposition with eigenvalue χ. Thus, if our Galois group is $(\mathbb{Z}/p\mathbb{Z})^r$, then $r \leq 2$.

We know that the maximal cyclotomic extension of $\mathbb{Q}_p$ takes the form

$$\mathbb{Q}_p^{\mathrm{cyclo}} = \mathbb{Q}_p^{\mathrm{ur}}.\mathbb{Q}_p(\zeta_{p^\infty})$$

where $\mathbb{Q}_p(\zeta_{p^\infty}) := \mathbb{Q}_p(\{\zeta_{p^n}\}_{n\in\mathbb{N}})$. The Galois group of $\mathbb{Q}_p^{\text{cyclo}}/\mathbb{Q}_p$ is $\hat{\mathbb{Z}} \times \mathbb{Z}_p^*$, so the pro-$p$ cyclotomic extension has Galois group $\mathbb{Z}_p \times \mathbb{Z}_p$. Let L be our finite p-power abelian extension and K the maximal pro-p cylotomic extension. If $\Gamma = \text{Gal}(K.L/\mathbb{Q}_p)$, then Γ/Γ^p has at most 2 cyclic factors. Since Γ surjects onto $H = \text{Gal}(L/\mathbb{Q}_p)$ which has 2 cyclic factors, it follows that Γ/Γ^p has exactly two cyclic factors.

We finally show that the quotient map $\psi : \Gamma \to \mathbb{Z}_p \times \mathbb{Z}_p = H$ is an isomorphism.

Proof. Let $g, h \in \Gamma$ such that $\psi(g)$ is a generator of $\mathbb{Z}_p \times \{1\} \subset H$ and $\psi(h)$ is a generator of $\{1\} \times \mathbb{Z}_p \subset H$. Then, g and h each topologically generates a quotient of $\mathbb{Z}_p$. However, since $\widehat{\langle g \rangle}$ surjects onto $\mathbb{Z}_p$, it follows that $\widehat{\langle g \rangle} \simeq \widehat{\langle h \rangle} \simeq \mathbb{Z}_p$.

Similarly, $\widehat{\langle g, h \rangle}$ surjects onto $\mathbb{Z}_p \times \mathbb{Z}_p$, so it maps isomorphically to $\mathbb{Z}_p \times \mathbb{Z}_p$. Thus, $\Gamma = \mathbb{Z}_p \times \mathbb{Z}_p \times I$ for some pro-p group I.

However, observe that:

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \Gamma/\Gamma^p = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times I/I^p$$

so I/I^p is trivial. Since I is a pro-p group, it follows that I is trivial. □

Thus, since $\text{Gal}(L.K/\mathbb{Q}_p) = \text{Gal}(L/\mathbb{Q}_p)$, $K.L = L$ which implies that $K \subset L$. This concludes the proof of the local Kronecker-Weber theorem for odd primes p.

Unfortunately, the same analysis cannot be done immediately for $p = 2$ since not all degree 2 extensions are contained in $\mathbb{Z}/4\mathbb{Z}$ extensions. However, we can perform a similar calculation by instead looking at both degree 2 and degree 4 extensions and bounding the number of cyclic factors of order 2 and order 4.

Let us first observe the quadratic extensions of $\mathbb{Q}_2$. By Kummer theory, we can see that the quadratic extensions are parametrized by

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = 2^{\mathbb{Z}/2\mathbb{Z}} \times \{\pm 1\} \times (1 + 4\mathbb{Z}_2)/(1 + 4\mathbb{Z}_2)^2.$$

Thus, $r \leq 3$.

However, we get a different bound when we investigate $\mathbb{Q}_2(i)^*/\mathbb{Q}_2(i)^{*4}$. If we take $\pi = i - 1$ as a uniformizer, we have the following decomposition:

$$\mathbb{Q}_2(i)^* = \pi^{\mathbb{Z}} \times \mathcal{O}^*.$$

By analyzing the power series for $(1 - x)^{1/4}$, we get the following calculation:

$$(1-x)^{1/4} = \sum_{i=0}^{\infty} \frac{\frac{1}{4}\left(\frac{1}{4}-1\right)\cdots\left(\frac{1}{4}-n\right)}{n!} \cdot x^n$$

$$\begin{aligned}
\nu\left(\frac{\frac{1}{4}\left(\frac{1}{4}-1\right)\cdots\left(\frac{1}{4}-n\right)}{n!} \cdot x^n\right) &\geq \nu\left(\frac{x^n}{4^n \cdot 2^n}\right) \\
&= \nu\left(\frac{x^n}{\pi^{4n} \cdot \pi^{2n}}\right) \\
&= \nu(x) \cdot n - 6n
\end{aligned}$$

which gives us that $\nu(x) \geq 7$ for the fourth power to be in $\mathcal{O}$.

Observe that $1 + \pi$ and $1 - i\pi^2$ are both elements of $\langle i \rangle$, so we are left with the following decomposition:

$$\mathbb{Q}_2(i)^*/\mathbb{Q}_2(i)^{*4} = \pi^{\mathbb{Z}} \times \langle i \rangle \times (1 + \pi^3\mathcal{O})/(1 + \pi^7\mathcal{O}).$$

We can see that $(1+\pi^3\mathcal{O})/(1+\pi^7\mathcal{O})$ is generated by $[1+\pi^3]$ and $[1+\pi^4]$, so we can get a more explicit representation as:

$$\mathbb{Q}_2(i)^*/\mathbb{Q}_2(i)^{*4} = \pi^{\mathbb{Z}} \times \langle i \rangle \times \langle 1+\pi^3, 1+\pi^4 \rangle / (1+\pi^7\mathcal{O}).$$

$\mathrm{Gal}(\mathbb{Q}_2(i)/\mathbb{Q}_2) = \langle c \rangle$ where c is complex conjugation, so $c(\pi) = c(i-1) = -i-1 = i(i-1) = i\pi$. Therefore, we get the following mapping for the generators:

$$\begin{aligned} c(\pi) &= \pi \times i \\ c(i) &= -i = i^{-1} \\ c(1+\pi^3) &= 1 - i\pi^3 \\ c(1+\pi^4) &= 1+\pi^4. \end{aligned}$$

The elements $\pi \times i, i^{-1}, 1+\pi^4$ all have transparent representations in our decomposition. As for $1-i\pi^3$, observe the following calculation:

$$\begin{aligned} (1-i\pi^3)(1+\pi^3) &= 1+\pi^3 - i\pi^3 - i\pi^6 \\ &= 1 + (1-i)\pi^3 - i\pi^6 \\ &= 1 + (-\pi)\pi^3 - i\pi^6 \\ &= 1 - \pi^4 - i\pi - i\pi^6 \\ &= 1 - (-4) - i(-4)(-2i) \\ &= 1 + 12 \\ &= 1 + \pi^4 + \pi^8 \\ &= (1+\pi^4)\cdot(1+\pi^8+\cdots). \end{aligned}$$

This tells us that $1-i\pi^3$ has a factor of $(1+\pi^3)^{-1}$ and a factor of $(1+\pi^4)$ up to a multiple of $1+\pi^7\mathcal{O}$. Thus, we can now display c as a matrix, taking our generators as a "basis":

$$c = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Since c acts by -1 on the cyclotomic factors, it follows that there are at most 2 independent choices of nontrivial 4-th roots of elements in $\mathbb{Q}_2(i)$ which produce abelian extensions over $\mathbb{Q}_2$.

Similar to the p odd case, we observe that

$$\mathbb{Q}_2^{\mathrm{cyclo}} = \mathbb{Q}_2^{\mathrm{ur}}.\mathbb{Q}_2(\zeta_{2^\infty}).$$

As a result, the maximal pro-2 cyclotomic extension has Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$. We take L to be a finite 2-power abelian extension and K to be the maximal pro-2 cyclotomic extension and show that $K.L = K$.

Let $\Gamma = \mathrm{Gal}(K.L/\mathbb{Q}_2)$. Then, Γ/Γ^4 has at most two cyclic factors of order 4 with at most one extra cyclic factor of order 2. We know that Γ surjects onto H, so Γ must have exactly 2 cyclic factors of order 4.

Let $g, h \in \Gamma$ such that the quotient map $\Gamma \to H = \mathrm{Gal}(K/\mathbb{Q}_2)$ maps g and h to generators of $\mathbb{Z}_2 \times \{1\} \times \{1\}$ and $\{1\} \times \mathbb{Z}_2 \times \{1\}$, respectively. By the same reasoning as the p odd case, we get that $\Gamma = \mathbb{Z}_2 \times \mathbb{Z}_2 \times I$ for some pro-2 group I. However, since Γ maps surjectively onto H, we know that $I = \mathbb{Z}/2\mathbb{Z}$, so $\Gamma = H$.

This completes the proof of the local Kronecker-Weber theorem.

5. The Kronecker-Weber Theorem

We would now like to extend the proof of the Local Kronecker-Weber theorem to abelian extensions of $\mathbb{Q}$. However, unlike the p-adic numbers, $\mathbb{Q}$ has many primes. This problem can be alleviated by looking at specific parts of our proof of the local case and connecting the p-adic case with the global case by using decomposition groups and inertia groups.

5.1. **Decomposition & Inertia Groups.** For the following discussion, L will be a finite extension of $\mathbb{Q}$ and $\mathcal{O}_L$, its ring of integers.

Remark 5.1. Many of our definitions and observations will hold if we take our base field to be an extension of $\mathbb{Q}$. However, for the sake of simplicity, we will restrict ourselves to taking $\mathbb{Q}$ as the base field.

Definition 5.2. We say that a prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ lies above a prime ideal $(p) \subset \mathbb{Z}$ if $p\mathcal{O}_L \subset \mathfrak{p}$.

Since $\mathcal{O}_L$ is a Dedekind domain, $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ for prime ideals $\mathfrak{p}_i$.

Since $\mathfrak{p}_i$ are all maximal prime ideals, we get that $\mathcal{O}_L/\mathfrak{p}_i$ is a field. Furthermore, it is a field that contains $\mathbb{Z}/p\mathbb{Z}$ which is also a field, so we can define the inertial degree f_i of $\mathfrak{p}_i$ as $\left[\mathcal{O}_L/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}\right]$.

We then define the decomposition group and inertia group as follows:

Definition 5.3. Let $L/\mathbb{Q}$ be Galois and $\mathfrak{p} \subset \mathcal{O}_L$ be a prime ideal lying above $(p) \subset \mathbb{Z}$. The decomposition group $D_\mathfrak{p}$ is the stabilizer of $\mathfrak{p}$ in the group action of $\mathrm{Gal}(L/K)$ on the prime ideals lying above p, i.e.

$$D_\mathfrak{p} = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Since $\mathfrak{p}$ is fixed by $D_\mathfrak{p}$, it follows that there is a map $\phi_\mathfrak{p} : D_\mathfrak{p} \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{p})/(\mathbb{Z}/p\mathbb{Z}))$ which is surjective.

Definition 5.4. The inertia group $I_\mathfrak{p}$ is the kernel of $\phi_\mathfrak{p}$ defined above.

The key reason we are concerned with the decomposition group is due to the following properties:

Proposition 5.5. *Given an extension $L/\mathbb{Q}$ and some prime $p \in \mathbb{Z}$, let $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_g\}$ be the set of prime ideals in $\mathcal{O}_L$ that lie above (p) with respective ramification and inertia degrees e_i, f_i. Then, we get that*

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

Furthermore, we get that $D_\mathfrak{p} \simeq Gal(L_\mathfrak{p}/\mathbb{Q}_p)$ where if $\alpha \in L$ is such that $L = \mathbb{Q}(\alpha)$, then $L_\mathfrak{p} = \mathbb{Q}_p(\alpha)$.

The reader can find a proof of this proposition as the proof of Proposition 1.2 of [2].

From our previous discussion on p-adic extensions, we can see that if K is the maximal unramified subextension of $L_\mathfrak{p}$:

$$\mathrm{Gal}(L_\mathfrak{p}/K) = I_\mathfrak{p} \subset D_\mathfrak{p} = \mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p).$$

Furthermore, $f_i = I_{\mathfrak{p}_i}$.

By Proposition 5.5, the group action on the prime ideals above (p) is transitive, so for any $\mathfrak{p}_i$ and $\mathfrak{p}_j$ above (p), we can find $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$. We know that σ must fix p, so we get

$$\sum_{i=1}^{g} \mathfrak{p}_i^{e_i} = \sum_{i=1}^{g} \sigma(\mathfrak{p}_i)^{e_i}.$$

Since the factorization of ideals is unique, we can conclude that $e_i = e_j$. It follows that $f_i = f_j$, so the ramification degree and inertia degree only depend on $p \subset \mathcal{O}_K$ and not on the choice of prime ideal $\mathfrak{p}_i$ lying above p.

5.2. **Discriminants and Minkowski's Theorem.** This subsection will be introducing the necessary concepts of the discriminant. We will not be proving any theorems, but we will be interpreting all necessary theorems in our context to create a base case for the sake of induction. For an abstract discussion of this section with rigorous proofs, the reader can refer to Chapter 2 of [3].

In order for us to define the discriminant, which will act as our index for induction, we first need to view $L/\mathbb{Q}$ as a vector space over $\mathbb{Q}$. Then, for all $\alpha \in L$, we can view multiplication by α as a linear transformation $\sigma_\alpha : L \to L$. By choosing a basis $\{\alpha_1, \cdots, \alpha_n\}$, we can find a matrix representation for σ_α which means we can define the trace and determinant of α. As a result, we get the following definitions.

Definition 5.6. Let $\alpha \in L$ where L is a finite field extension of $\mathbb{Q}$. Then, we define

$$\mathrm{Tr}\,(\alpha) := \mathrm{trace}\,(\sigma_\alpha)$$

$$\mathrm{Norm}\,(\alpha) := \det\,(\sigma_\alpha).$$

Though the explicit computation of the trace and norm rely on a choice of basis, the trace and determinant of a linear transformation are independent of the choice of basis, so the trace and norm of an element are well-defined. However, for the sake of calculation, it is often convenient to work with an integral basis, defined as follows:

Definition 5.7. Given $L/\mathbb{Q}$, a basis $\{\alpha_1, \cdots, \alpha_n\}$ of L over $\mathbb{Q}$ is called an integral basis if it is also a set of generators for $\mathcal{O}_L$ as a $\mathbb{Z}$-module.

Though it is not a transparent fact, there will always exist an integral basis. Thus, we can define the discriminant of a field extension as follows:

Definition 5.8. Let $\{\alpha_1, \cdots, \alpha_n\}$ be an integral basis for L/K. Then, the discriminant of L/K is

$$\Delta_L := \det \begin{pmatrix} \mathrm{Tr}\,(\alpha_1 \cdot \alpha_1) & \mathrm{Tr}\,(\alpha_1 \cdot \alpha_2) & \mathrm{Tr}\,(\alpha_1 \cdot \alpha_3) & \cdots & \mathrm{Tr}\,(\alpha_1 \cdot \alpha_n) \\ \mathrm{Tr}\,(\alpha_2 \cdot \alpha_1) & \mathrm{Tr}\,(\alpha_2 \cdot \alpha_2) & \mathrm{Tr}\,(\alpha_2 \cdot \alpha_3) & \cdots & \mathrm{Tr}\,(\alpha_2 \cdot \alpha_n) \\ \mathrm{Tr}\,(\alpha_3 \cdot \alpha_1) & \mathrm{Tr}\,(\alpha_3 \cdot \alpha_2) & \mathrm{Tr}\,(\alpha_3 \cdot \alpha_3) & \cdots & \mathrm{Tr}\,(\alpha_3 \cdot \alpha_n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}\,(\alpha_n \cdot \alpha_1) & \mathrm{Tr}\,(\alpha_n \cdot \alpha_2) & \mathrm{Tr}\,(\alpha_n \cdot \alpha_3) & \cdots & \mathrm{Tr}\,(\alpha_n \cdot \alpha_n) \end{pmatrix}.$$

It can be shown that every choice of integral basis will produce the same discriminant which makes the discriminant well-defined. In fact, Δ_L will always be an integer.

Remark 5.9. This definition of the discriminant coincides with the more common notion of a discriminant for a quadratic polynomial: Let $L/\mathbb{Q}$ be a quadratic extension and $\theta \in L$ such that $\mathcal{O}_L = \mathbb{Z}[\theta]$. If $x^2+bx+c \in \mathbb{Z}[x]$ is the minimal polynomial of θ, then $\Delta_L = b^2 - 4ac$.

Initially, the discriminant may look contrived and convoluted. However, the discriminant encodes many important properties of a field. For example, the discriminant has extensive value when finding the ramified primes of a given extension. The following theorem sheds light on this use.

Theorem 5.10. *Given a finite extension $L/\mathbb{Q}$, a prime $p \in \mathbb{Z}$ is ramified in L if and only if $p \mid \Delta_L$.*

An abstraction of this theorem is taken as Corollary 2.12 in [3].

As a result, we can look at the prime factorization of the discriminant and we get the precise set of primes that ramify in our extension.

In general, a number field can have nontrivial extensions that have no ramified primes. Equivalently, there can be nontrivial extensions whose discriminant is a unit. However, thanks to a stroke of luck, this cannot happen when the base field is $\mathbb{Q}$ as stated in the following theorem:

Theorem 5.11 (Minkowski's Theorem)**.** *If $L/\mathbb{Q}$ is a nontrivial extension, then $|\Delta_L| > 1$ where Δ_L is the discriminant.*

A proof of this theorem can be found in Chapter 2 of [3] as Theorem 2.17.

Explicitly, we can use Theorem 5.10 to see that if some extension $L/\mathbb{Q}$ has no ramified primes, then by Theorem 5.11, $L = \mathbb{Q}$. This will validate our following inductive argument for the proof of the Kronecker-Weber theorem.

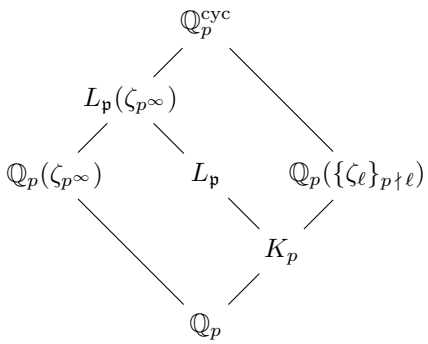
5.3. **Proof of the Kronecker-Weber Theorem.** Recall the statement of Theorem 1.1. We want to show that every abelian extension of $\mathbb{Q}$ is a subextension of a cyclotomic extension of $\mathbb{Q}$.

Our approach will be to observe a given abelian extension and its corresponding extensions over $\mathbb{Q}_p$ for a ramified prime p. The $\mathbb{Q}_p$ extensions will provide information about the decomposition groups which will allow us to decompose our $\mathbb{Q}$ extension as the compositum of two extensions, each of which arises as a subextension of a cyclotomic extension of $\mathbb{Q}$.

Proof. Let $L/\mathbb{Q}$ be an abelian extension with discriminant Δ_L. Let $p \in \mathbb{Z}$ be a prime such that $p \mid \Delta_L$. By Theorem 5.10, p is ramified in L. To analyze this ramification, we shift over to $\mathbb{Q}_p$.

Let $L_\mathfrak{p}/\mathbb{Q}_p$ be the corresponding extension of $\mathbb{Q}_p$. By Proposition 5.5, we get that $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p) = D_\mathfrak{p} \subset \mathrm{Gal}(L/\mathbb{Q})$ so $L_\mathfrak{p}/\mathbb{Q}_p$ is an abelian extension (since we are working with abelian groups, any choice of $\mathfrak{p}$ lying above p provides the same decomposition group). By the local Kronecker-Weber theorem, $L_\mathfrak{p}$ is a subextension of $\mathbb{Q}_p^{\mathrm{cyclo}}$. It follows that $L_\mathfrak{p}(\zeta_{p^\infty})$ is also a subextension of $\mathbb{Q}_p^{\mathrm{cyclo}}$.

We can then split $L_{\mathfrak{p}}(\zeta_{p^\infty})$ into $\mathbb{Q}_p(\zeta_{p^\infty}).K_p$ where $K_p \subset \mathbb{Q}_p(\{\zeta_\ell\}_{p\nmid\ell})$. Visually, we get the following diagram.



Let $H = \text{Gal}(L_{\mathfrak{p}}(\zeta_{p^\infty})/\mathbb{Q}_p)$. By the above analysis, we know that $I_p = \mathbb{Z}_p^*$ is a subgroup of H. Furthermore, H surjects onto $\text{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) = \mathbb{Z}_p^*$ as a quotient such that I_p maps isomorphically in the quotient map. Thus, $H = \mathbb{Z}_p^* \times A_p$ for some abelian group A_p.

Relating this to $L/\mathbb{Q}$, let $\Gamma = \text{Gal}(L(\zeta_{p^\infty})/\mathbb{Q})$. We know that $D_{\mathfrak{p}}$ and I_p manifest themselves as a subgroup in Γ. In parallel to our local case, Γ maps surjectively onto $\text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \mathbb{Z}_p^* = I_p$ as a quotient. Once again, I_p maps isomorphically in this quotient, so we can split $\Gamma = \mathbb{Z}_p^* \times A$ for some abelian group A.

By Galois theory, we know that $L(\zeta_{p^\infty})/\mathbb{Q}$ is the compositum of the disjoint fixed fields $K = L(\zeta_{p^\infty})^{\mathbb{Z}_p^*}$ and $L(\zeta_{p^\infty})^A$. We can further explicate this compositum and see that $L(\zeta_{p^\infty})^A = \mathbb{Q}(\zeta_{p^\infty})$. By definition, K is fixed by the inertia group, so K is unramified at p.

It is now sufficient to show that if p' is a prime that is unramified in L, then p' is unramified in K. Observe that $L.\mathbb{Q}(\zeta_{p^\infty}) = L(\zeta_{p^\infty})$ and $K \cap \mathbb{Q}(\zeta_{p^\infty}) = \mathbb{Q}$ by the Galois correspondence. Thus, $K \subset L$ which means that any prime that is ramified in K must also be ramified in L.

We can now continue this process to see that if $\Delta_L = p_1^{\ell_1} \cdots p_w^{e_w}$ as a prime factorization, we can continually add all (p_i-power)-roots of unity which we can express as a compositum of cyclotomic extensions as follows:

$$L(\zeta_{p_1^\infty}, \cdots, \zeta_{p_w^\infty}) = \mathbb{Q}(\zeta_{p_1^\infty}).\mathbb{Q}(\zeta_{p_2^\infty}).\cdots.\mathbb{Q}(\zeta_{p_w^\infty}).M$$

where M is an extension of $\mathbb{Q}$ that is unramified at all primes. By Minkowski's Theorem, we know that M is trivial, so $L(\zeta_{p_1^\infty}, \cdots, \zeta_{p_w^\infty})$ is the compositum of cyclotomic extensions. Thus, L is a subextension of a cyclotomic extension of $\mathbb{Q}$. This completes the proof of the Kronecker-Weber theorem. □

6. Acknowledgements

I would like to sincerely thank Professor Matthew Emerton for guiding me through all the material that went into this paper and sparking my interest in algebraic number theory. I definitely would not have been able to learn all of this material and more in one summer without your mentoring. I would also like to thank Karl Schaefer for being infintely patient with me and struggling together

through the numerous calculation and conceptual errors I made during our sessions. I would also like to extend my thanks to Professor Peter May for organizing the 2018 University of Chicago REU.

References

[1] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Algebraic Number Theory*. Springer-Verlag, New York, 1982.

[2] John Torrence Tate Jr. Global class field theory. In J. W. S. Cassels and A. Frohlich, editors, *Algebraic Number Theory*, chapter 7, pages 163–203. Thompson Book Company Inc., Washington, DC, 1967.

[3] Jurgen Neukirch. *Algebraic Number Theory*. Springer-Verlag, Germany, 1999.

[4] Jean-Pierre Serre. *Local Fields*. Springer-Verlag, New York, 1979.