THE KRONECKER-WEBER THEOREM

AKASH GANGULY

Abstract. In this paper, we prove the Kronecker-Weber theorem, which says that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$. Our proof does not use any class field theory. Instead, we use higher ramification groups and the different, following the argument outlined in the exercises in Chapter 4 of Marcus [Mar18].

Contents

1. Introduction

If one wants to generate abelian extensions (finite normal extensions with abelian Galois group) of $\mathbb{Q}$, a surefire method is to look at subfields of cyclotomic fields. If ζ_m is a primitive m-th root of unity, we know that $\mathbb{Q}(\zeta_m)$ is a normal extension of $\mathbb{Q}$ with Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ (see Corollary 2 in Chapter 2 of Marcus [Mar18]). By the Galois correspondence, each subfield $K \subseteq \mathbb{Q}(\zeta_m)$ must be the fixed field of some subgroup $H \leq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is abelian, each subgroup is normal, which implies that K is again an abelian extension of $\mathbb{Q}$. The Kronecker-Weber theorem says that this construction is exhaustive; *every* abelian extension of $\mathbb{Q}$ can be obtained in this way.

Theorem 1.1 (Kronecker-Weber)**.** *Let K be an abelian extension of $\mathbb{Q}$. Then $K \subseteq \mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{N}$, where ζ_m is a primitive m-th root of unity.*

The goal of this paper is to prove this theorem. Throughout this paper, we assume some level of familiarity with number fields and algebraic number theory. Every extension is assumed to be finite. In any case, we attempt to give full references for results we use without proof. We collect some preliminary results in Section 2 and further results we use without proof are stated at the beginning of the subsections in which they are used.

Date: March 2024.

We prove the Kronecker-Weber Theorem in a few steps. First, we use group theory to reduce to the case of abelian p-extensions (abelian extensions with degree a power of p over $\mathbb{Q}$). Then, we use higher ramification groups to further reduce to the case of abelian p-extensions unramified outside of p. Finally, we use higher ramification groups and the different to prove the Kronecker-Weber Theorem for these extensions. The utility of the different and higher ramification groups is most clear in an amazing uniqueness result which says that for all odd primes $p \in \mathbb{Z}$, there is only one abelian extension of $\mathbb{Q}$ unramified outside of p with degree p.

2. Preliminaries

We collect some preliminary results on ramification in normal extensions here, along with more general results we will assume throughout the paper.

Lemma 2.1. *Let L, K be abelian extensions of $\mathbb{Q}$. Then KL is also a normal extension of $\mathbb{Q}$, and we have an embedding $\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$, so KL is again an abelian extension of $\mathbb{Q}$.*

Proof. The fact that KL is normal follows from the characterization of normal extensions as the splitting field of a separable polynomial (see Section 14.1 in Dummit and Foote [DF04]). In general, one can restrict automorphisms of a larger field to a subfield, and here the Galois correspondence says that every subfield is normal over $\mathbb{Q}$ since we are working with an abelian extension. The map is obtained by restricting automorphisms of KL to K and L respectively and is readily seen to have trivial kernel. So $\mathrm{Gal}(KL/\mathbb{Q})$ embeds into an abelian group and must thus be abelian. □

Corollary 2.2. *Let L, K be abelian p-extensions (extensions with degree a power of p) of $\mathbb{Q}$. Then KL is also an abelian p-extension of $\mathbb{Q}$.*

Proof. This follows directly from the embedding in Lemma 2.1. □

Theorem 2.3. *Let K be a number field. A prime $p \in \mathbb{Z}$ ramifies in K if and only if p divides the discriminant $\mathrm{disc}(\mathcal{O}_K)$.*

Proof. See Theorem 24 and Theorem 34 in Marcus [Mar18]. □

Lemma 2.4 (Minkowski)**.** *Every ideal class of $\mathcal{O}_K$ contains an ideal J with*

$$|\mathcal{O}_k/J| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathcal{O}_K)|}$$

Proof. See Theorem 37 and Corollary 2 in Marcus [Mar18]. □

Lemma 2.5. *Let K be an extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] > 1$. Then some prime $p \in \mathbb{Z}$ ramifies in K.*

Proof. This follows from Theorem 2.3 and Lemma 2.4 . □

Theorem 2.6. *Let L be a normal extension of K. Let Q be a prime of L lying over P, a prime of K. Let f be the residue degree of Q over P, let e be the ramification index of Q over P, and let r be the number of primes of L lying over P. For any subgroup H of $\mathrm{Gal}(L/K)$ let L_H denote the fixed field of H. Let $E(Q|P) = \{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(\mathcal{O}_L/Q) = \mathcal{O}_L/Q\}$ and $D(Q|P) = \{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma Q = Q\}$ be the inertia and decomposition subgroups respectively. Then we have the following.*

$$\begin{array}{c} L \\ | \\ e \\ | \\ L_{E(Q|P)} \\ | \\ f \\ | \\ L_{D(Q|P)} \\ | \\ r \\ | \\ K \end{array}$$

Moreover, Q is totally ramified (meaning $e(Q|Q \cap \mathcal{O}_{L_E}) = [L : L_E]$) over L_E and P is unramified (meaning $e(Q \cap \mathcal{O}_{L_E}|P) = 1$) in L_E.

Proof. See Theorem 28 in Marcus [Mar18]. □

3. The Kronecker-Weber Theorem

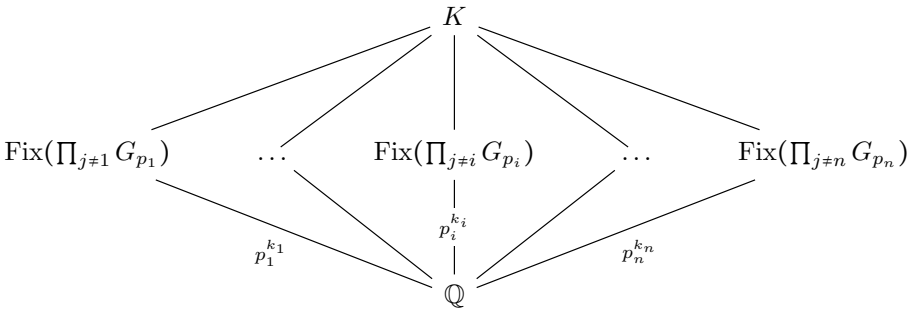
Now we are ready to give a proof of the Kronecker-Weber theorem. First, we reduce to the case of an abelian p-extension of $\mathbb{Q}$ via group theory. Then, by using higher ramification groups, we reduce further to the case of abelian p-extensions unramified outside of $p \in \mathbb{Z}$. We then finish by showing directly that such extensions are always contained in cyclotomic fields for any prime $p \in \mathbb{Z}$.

3.1. Reducing to abelian p-extensions.

Lemma 3.1. *Every abelian extension K of $\mathbb{Q}$ is the compositum of abelian p_i-extensions, for some collection of primes $\{p_i \,|\, p_i \in \mathbb{Z}\}$.*

Proof. By the fundamental theorem of finite abelian groups, $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_i G_{p_i}$ where G_{p_i} are p_i-groups for some collection of primes $p_i \in \mathbb{Z}$. Taking fixed fields $\mathrm{Fix}(\prod_{j \neq i} G_{p_j})$, we get abelian p_i-extensions of degree $|G_{p_i}|$ over $\mathbb{Q}$ whose compositum is contained in K with degree equal to $|\mathrm{Gal}(K/\mathbb{Q})|$ since the p_i are pairwise coprime. This shows the compositum of these fixed fields is indeed K. □

We can visualize this lemma with a field diagram.



If L, K are two abelian extensions of $\mathbb{Q}$, with $L \subseteq \mathbb{Q}(\zeta_n)$ and $K \subseteq \mathbb{Q}(\zeta_m)$, then $KL \subseteq \mathbb{Q}(\zeta_{nm})$, since $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{nm})$ and $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{nm})$. Put another way, if two abelian extensions are contained in cyclotomic fields, then so is their compositum. Thus, we have successfully reduced the Kronecker-Weber theorem to the case of abelian p-extensions.

3.2. **Reducing to abelian p-extensions unramified outside p.** Our next lemma makes the key reduction to extensions unramified outside p. It requires a few results about higher ramification groups, which we define and state below.

Definition 1. Let L/K be a normal extension of number fields. Let Q be a prime of L lying over P, a prime of K. The m-th higher ramification groups $V_m(Q|P)$ are defined as

$$V_m(Q|P) = \{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(\alpha) \equiv \alpha \mod Q^{m+1} \text{ for all } \alpha \in \mathcal{O}_L\}.$$

In other words, $V_m(Q|P)$ is the subgroup of $\mathrm{Gal}(L/K)$ fixing the finite ring $\mathcal{O}_L/Q^{m+1}$ pointwise.

Lemma 3.2. *The first higher ramification group $V_1(Q|P)$ is the unique Sylow-p subgroup of $E(Q|P)$, where p is the prime of $\mathbb{Z}$ lying under Q. Furthermore, $V_1(Q|P)$ is nontrivial if and only if $e(Q|P)$ is divisible by p.*

Proof. See Corollary 3 in Chapter 4 of Serre [Ser79]. □

Lemma 3.3. *If $D(Q|P)$ is abelian, then $E(Q|P)/V_1(Q|P)$ is cyclic and embeds into $(\mathcal{O}_K/P)^\times$. This implies that the order of $E(Q|P)/V_1(Q|P)$ divides $|\mathcal{O}_K/P|-1$.*

Proof. See Proposition 9 in Chapter 4 of Serre [Ser79]. □

With that, we are ready to state our lemma.

Lemma 3.4. *Let K be an abelian p-extension of $\mathbb{Q}$. Assume further that $q \neq p$ is a prime of $\mathbb{Z}$ ramifying in K. Then there exists another abelian p-extension K' of $\mathbb{Q}$ with the following properties.*

1. *q is unramified in K'*
2. *any prime of $\mathbb{Q}$ unramified in K is unramified in K'*
3. *K is contained a cyclotomic field whenever K' is*

Before proceeding to the proof of this lemma, we check that this gives us our desired reduction. By Theorem 2.3, only finitely many primes of $\mathbb{Z}$ ramify in a number field. By iteratively applying this lemma, we end up with an abelian p-extension K^* with the property that K is contained in a cyclotomic field when K^* is, and importantly, K^* is ramified only over $p \in \mathbb{Z}$.

Proof of Lemma 3.4. Fix a prime Q of K lying over $q \in \mathbb{Z}$. By Lemma 3.3 we have that the order of $E(Q|q)/V_1(Q|q)$ divides the order of $(\mathbb{Z}/q\mathbb{Z})^\times$. Since $e(Q|q)$ is a power of p (Theorem 2.6), $V_1(Q|q)$ is trivial by Lemma 3.2. This tells us that $E(Q|q)$ is cyclic of order dividing $q-1$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic, there is a unique subfield L of $\mathbb{Q}(\zeta_q)$ with $[L:\mathbb{Q}] = e(Q|q)$. Since $\mathrm{disc}(\mathbb{Q}(\zeta_q)) = q^{q-2}$ (see Chapter 2 of Marcus [Mar18]), it follows that $q \in \mathbb{Z}$ totally ramifies in $\mathbb{Q}(\zeta_q)$ and thus totally ramifies in every intermediate subfield.

Fix a prime U of KL lying over Q. We claim that $K' = KL_{E(U|q)}$, the fixed field of the inertia subgroup $E(U|q)$, is an abelian p-extension satisfying properties (1) through (3). First, by Corollary 2.2, we have that K' is an abelian p-extension. By Theorem 2.6, q is unramified in K' as K' is the fixed field of the inertia subgroup. Next, note that any prime of $\mathbb{Q}$ of KL that ramifies must ramify in either K or L (Theorem 31 in Marcus [Mar18]). Since the only prime of $\mathbb{Q}$ ramifying in L is q, this tells us that any prime unramified in K is also unramified in KL. Since

$K' \subseteq KL$, we see that the same holds for K'. We have verified properties (1) and (2).

Now we check property (3), that says K' is contained a cyclotomic field whenever K is. First, we check that $K' \cap L = \mathbb{Q}$. Towards a contradiction, assume that $K' \cap L$ is a nontrivial extension of $\mathbb{Q}$. Then $q \in \mathbb{Z}$ would totally ramify in $K' \cap L$, since $q \in \mathbb{Z}$ totally ramifies in L. However, if q ramified in $K' \cap L$, q would have to ramify in K', which we have shown is impossible.

Recall (Lemma 2.1) that we have an embedding obtained by restricting automorphisms

$$\phi : \mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}).$$

Since U is a prime of KL lying over Q, we have that $\mathcal{O}_L/Q \subseteq \mathcal{O}_{KL}/U$. Thus, any element of the inertia subgroup $E(U|q)$ restricts to an element of the respective inertia subgroup $E(Q|q)$ in K. This tells us that the embedding sends

$$\phi : E(U|q) \hookrightarrow E(Q|q) \times \mathrm{Gal}(L/\mathbb{Q}).$$

Since K' is an abelian p-extension, by the same reasoning as above, we see that $V_1(U|q)$ is trivial and $E(U|q)$ is cyclic. We will use this embedding and the fact that $E(U|q)$ is cyclic to calculate the ramification index $e(U|q)$ using Theorem 2.6. Let σ generate $E(U|q)$. Since ramification is multiplicative in towers, we know that the order of σ is at least $e(Q|q)$. On the other hand, $E(Q|q)$ and $\mathrm{Gal}(L/\mathbb{Q})$ are both groups of order $E(Q|q)$. This means that the order of $\phi(\sigma)$ must be $e(Q|q)$, so $e(U|q) = e(Q|q)$.

Finally, we show that $K'L = KL$ via a degree argument. Note that we have $K'L \subseteq KL$, $K' \cap L = \mathbb{Q}$, and $[L : \mathbb{Q}] = e(Q|q) = [KL : K']$. Putting this all together, we see that

$$\begin{aligned}[K'L : \mathbb{Q}] &= [K' : \mathbb{Q}][L : \mathbb{Q}] \\ &= [K' : \mathbb{Q}][KL : K'] \\ &= [KL : \mathbb{Q}],\end{aligned}$$

using the tower law in the last step. So, if K is contained a cyclotomic field, so is KL, since L is also contained in a cyclotomic field. Since $K'L = KL$, we have that K' is contained in a cyclotomic field whenever K is. □

This lemma eliminates a behavior called tame ramification. A prime Q of L lying over P a prime of K is said to be tamely ramified if its ramification index $e(Q|P)$ is coprime to the characteristic of the residue field $\mathrm{char}(\mathcal{O}_K/P)$. By Lemma 3.2, Q is tamely ramified if and only if $V_1(Q|P)$ is trivial. A prime with the property that its ramification index does divide the characteristic of the residue field is said to be wildly ramified. As mentioned above, Lemma 3.4 lets us reduce the proof of the Kronecker-Weber theorem to the case of an abelian p-extension unramified outside of $p \in \mathbb{Z}$; the case of wild ramification.

3.3. **The case $p = 2$.** To finish our proof, we plunge into the wild world of wild ramification. We start with the $p = 2$ case, which we can prove directly. The case where p is an odd prime takes more care and finally uses the different and Hilbert's formula, which we have not used thus far.

Theorem 3.5. *Let K be an abelian 2-extension unramified outside of 2. Then K is contained in a cyclotomic field.*

We prove this in a few steps. First, we characterize abelian extensions of degree 2 (over $\mathbb{Q}$) unramified outside of 2 using the discriminant.

Lemma 3.6. *Let K be an abelian extension with $[K:\mathbb{Q}] = 2$ unramified outside of 2. Then K is $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{-2})$.*

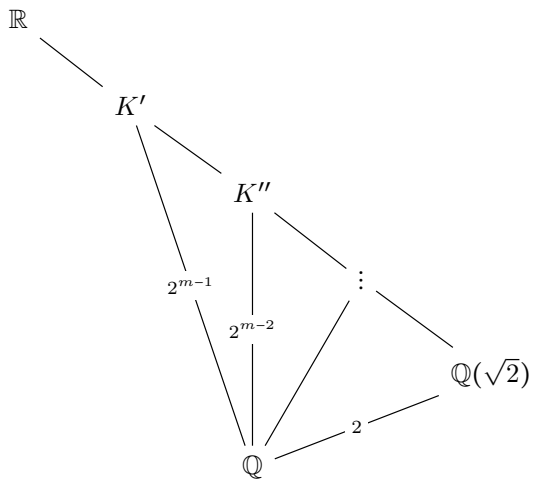
Proof. By Theorem 2.3 it suffices to calculate when the discriminant of K is a power of 2. The discriminant a of quadratic number field $\mathbb{Q}(\sqrt{m})$, m squarefree is

$$\operatorname{disc}(\mathcal{O}_{\mathbb{Q}(\sqrt{m})}) = \begin{cases} 4m, & \text{if } m \equiv 2 \text{ or } 3 \mod 4 \\ m, & \text{if } m \equiv 1 \mod 4. \end{cases}$$

This calculation can be found in Chapter 2 of Marcus [Mar18], for example. From this, it is clear that the only possible values of m are $-1, 2$ and -2. Any higher power of 2 will fail to be squarefree. □

We can check that these quadratic extensions are contained in cyclotomic fields directly. Let ζ be a primitive eighth root of unity. Then we have that $(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2$, so $\sqrt{2} \in \mathbb{Q}(\zeta_8)$. The fact that the number field $\mathbb{Q}(i)$ is contained in a cyclotomic field uses sophisticated results from class field theory so we omit it here. The eighth cyclotomic field contains i, so $\sqrt{-2}$ is also contained in a cyclotomic field. With this, we are ready to prove Theorem 3.5.

Proof of Theorem 3.5. Let K be an abelian extension of degree 2^m over $\mathbb{Q}$ unramified outside of $2 \in \mathbb{Z}$. The case where $m = 1$ is proven above. Now, if $m > 1$, we claim that K contains $\mathbb{Q}(\sqrt{2})$. Consider the fixed field of conjugation K'. Since $m > 1$, $K' \neq \mathbb{Q}$. Since $\operatorname{Gal}(K'/\mathbb{Q})$ has order 2^{m-1} it contains an element σ of order 2[1]. Let K'' be fixed field of $\langle\sigma\rangle$. Since $\operatorname{Gal}(K'/\mathbb{Q})$ is abelian, $\operatorname{Gal}(K'/\mathbb{Q})/\langle\sigma\rangle$ is an abelian group of order 2^{m-2}. We can continue inductively (see the field diagram below) to show that K' contains a quadratic subfield K^*. Since K' is unramified outside of 2 and contained in $\mathbb{R}$, it must be the case that $K^* = \mathbb{Q}(\sqrt{2})$.



[1]Every group G of even order contains an element of order 2. Here is a neat proof of the fact. The set $G - \{e\}$ then has odd cardinality, and the operation of taking inverses gives an involution on this set. An involution on a set of odd order must have a fixed point. In this case, a fixed point is a group element that is its own inverse; an element of order 2!

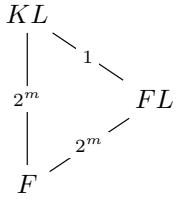
Let $L = \mathbb{R} \cap \mathbb{Q}(\zeta_{2^{m+2}})$. Since L is a subfield of the 2^{m+2} cyclotomic field, it is an abelian extension unramified outside of $2 \in \mathbb{Z}$ contained in $\mathbb{R}$. Thus, L contains the unique quadratic subfield $\mathbb{Q}(\sqrt{2})$. The Galois correspondence tells us that $\mathrm{Gal}(L/\mathbb{Q})$ is an abelian 2-group with a unique index 2 subgroup, which implies that $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic. Note that we already could have seen this from the fact that $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2^{m+2}\mathbb{Z})^\times/(\pm 1)$ is cyclic.

Let σ be a generator for $\mathrm{Gal}(L/\mathbb{Q})$ and lift it to an automorphism $\tilde{\sigma}$ of KL. Let F be the fixed field of $\langle\tilde{\sigma}\rangle$. Since $\tilde{\sigma}$ restricts to a generator of $\mathrm{Gal}(L/\mathbb{Q})$ on L, $F \cap L = \mathbb{Q}$ by the Galois correspondence. Since F is a subfield of the 2-extension KL, it must have degree 2^k over $\mathbb{Q}$. We have seen that if $k > 1$, then F would contain $\mathbb{Q}(\sqrt{2})$, contradicting that $K \cap L = \mathbb{Q}$. So, F has degree at most 2 over $\mathbb{Q}$, and since it must be contained in KL (and thus is unramified outside of 2), F must be $\mathbb{Q}, \mathbb{Q}(i)$, or $\mathbb{Q}\sqrt{-2}$.

Now we claim that $\tilde{\sigma}$ has order 2^m. Since $\tilde{\sigma}$ restricts to σ on L, it must have order at least 2^m. Recall that we have an embedding

$$\phi : \mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}),$$

and both $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(L/\mathbb{Q})$ are groups of order 2^m, so the order of $\tilde{\sigma}$ must be exactly 2^m. By the Galois correspondence, we have that $[KL : F] = 2^m$. Since $F \cap L = \mathbb{Q}$, we also have that $[FL : F] = 2^m$. This tells us that $FL = KL$.



Now, F is either $\mathbb{Q}$, $\mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{-2})$, all of which we have already seen to be contained in cyclotomic fields. Since L is also contained in a cyclotomic field, we have that $FL = KL$ is contained in a cyclotomic field, so K is too. □

Let us stop here to think about the method we utilized to prove the $p = 2$ case, as it turns out to be very similar to case where p is an odd prime. We started with an abelian p-extension K that was unramified outside of p. Then, we classified every abelian extension unramified outside of p with degree exactly p over $\mathbb{Q}$. This turned out to be the crucial step. From there, we took a subfield of a cyclotomic field L with cyclic Galois group with the property that $[L : \mathbb{Q}] = [K : \mathbb{Q}]$. We lifted a generator σ of $\mathrm{Gal}(L/\mathbb{Q})$ to an automorphism $\tilde{\sigma}$ of KL, which then told us that the fixed field of $\langle\tilde{\sigma}\rangle$, which we called F, had the property $F \cap L = \mathbb{Q}$. Finally, we used the embedding to calculate the order of $\tilde{\sigma}$, which told us that $FL = KL$. In the case that $p = 2$, since we had classified all abelian extensions of degree exactly 2 over $\mathbb{Q}$ that were unramified outside of 2, it was easy to narrow down the possible choices for F. Importantly, we proved that any abelian 2-extension with degree at least 4 over $\mathbb{Q}$ would have to contain $\mathbb{Q}(\sqrt{2})$ and used the fact that $F \cap L = \mathbb{Q}$.

3.4. **The case where p is an odd prime.** In the case of $p = 2$, we saw that there were three abelian extensions of degree 2 unramified outside of 2. It turns out that in the case where p is an odd prime, there is only one possibility. That is, there is a unique degree p abelian extension of $\mathbb{Q}$ unramified outside of $p \in \mathbb{Z}$. We

know that the unique degree p subfield of the p^2-th cyclotomic field is a number field satisfying these hypotheses, so this uniqueness result tells us that it is the only one. The proof of the Kronecker-Weber Theorem becomes very neat once we have this result, but the uniqueness result takes a significant amount of work to prove.

Theorem 3.7. *Let p be an odd prime. There is a unique abelian extension of degree p over $\mathbb{Q}$ that is unramified outside of $p \in \mathbb{Z}$. This extension is the unique degree p subfield of the p^2-th cyclotomic field.*

Specifically, we need a number of results regarding higher ramification groups and the different. We state these (without proof) below, then proceed to the proofs of our original claim.

Lemma 3.8. *The higher ramification groups $V_m(Q|P)$ are normal in $D(Q|P)$ and $\bigcap_m V_m(Q|P) = \{e\}$.*

Proof. See Proposition 1 in Chapter 4 of Serre [Ser79]. □

Lemma 3.9. *For $m \geq 2$, V_{m-1}/V_m can be embedded in the additive group of $\mathcal{O}_L/Q$.*

Proof. See Corollary 3 in Chapter 4 of Serre [Ser79]. □

Now, we define the different of a number field in an extension. The different is similar to the discriminant in that it measures ramification in an extension.

Definition 2. Let L/K be an extension of number fields. For an additive subgroup A of L, define $A^{-1} = \{\alpha \in L \,|\, \alpha A \subseteq \mathcal{O}_L\}$ and $A^* = \{\alpha \in L \,|\, T_K^L(\alpha A) \subseteq \mathcal{O}_K\}$. Here, T_K^L is the trace of the extension L/K. The different of L is defined as $\operatorname{diff}(\mathcal{O}_L|\mathcal{O}_K) = (\mathcal{O}_L^*)^{-1}$ and it is an ideal of $\mathcal{O}_L$.

Theorem 3.10. *Let L/K be number fields. The primes of L dividing $\operatorname{diff}(\mathcal{O}_L|\mathcal{O}_K)$ are exactly those ramified in the extension L/K.*

Proof. See Proposition 13 in Chapter 3 of Serre [Ser79]. □

Lemma 3.11 (Transitivity of the different)**.** *Let $M \subseteq K \subseteq L$ be a tower of number fields. Then*

$$\operatorname{diff}(\mathcal{O}_L|\mathcal{O}_M) = \operatorname{diff}(\mathcal{O}_L|\mathcal{O}_K)(\operatorname{diff}(\mathcal{O}_K|\operatorname{diff}\mathcal{O}_M)\mathcal{O}_L).$$

Proof. See Section 4 in Chapter 3 of Serre [Ser79]. □

Theorem 3.12 (Hilbert's formula)**.** *Let L be normal over K. Let Q be a prime of L lying over a prime P of K. Then*

$$\nu_P(\operatorname{diff}(\mathcal{O}_K|\mathbb{Z})) = \sum_{m \geq 0} (|V_m(Q|P)| - 1),$$

where the $V_i(Q|P)$ are the higher ramification groups and ν_P is the P-adic valuation.

Proof. See Proposition 4 in Chapter 4 of Serre [Ser79]. □

Lemma 3.13. *Let L/K be a normal extension of number fields. Let P be a prime of K and fix some prime Q of L lying over P. Suppose Q is totally ramified over P. Let $\pi \in Q - Q^2$. Let $f(x)$ be the minimal polynomial for π over K. Then*

$$\nu_Q(\operatorname{diff}(\mathcal{O}_L|\mathcal{O}_K)) = \nu_Q((f'(\pi)).$$

That is, the exact power of Q dividing $\operatorname{diff}(\mathcal{O}_L|\mathcal{O}_K)$ is the same as the exact power of Q dividing the principal ideal $(f'(\pi))$ in $\mathcal{O}_L$.

Proof. See Corollary 2 of Chapter 3 of Serre [Ser79]. □

Finally, we are ready to prove Theorem 3.7. We prove this results in two steps. First, we explicitly calculate the different of a degree p abelian extension of $\mathbb{Q}$ unramified outside of $p \in \mathbb{Z}$. Then, we use the transitivity of the different to show that any abelian extension unramified outside of p with degree p^2 over $\mathbb{Q}$ must have a cyclic Galois group.

Lemma 3.14. *Let p be an odd prime. Let K be an abelian extension with degree p over $\mathbb{Q}$ that is unramified outside of $p \in \mathbb{Z}$. Let P be a prime of K lying over p. Then* $\operatorname{diff}(\mathcal{O}_k|\mathbb{Z}) = P^{2p-2}$.

Proof. First, note that p totally ramifies in K. Otherwise, the inertia field K_E would be a subfield not equal to $\mathbb{Q}$ contained in K, a field of prime degree over $\mathbb{Q}$, which is impossible. By Theorem 3.10 and the fact that K is unramified outside of $p \in \mathbb{Z}$, we know that $\operatorname{diff}(\mathcal{O}_K) = P^\ell$. Our key tool in calculating ℓ will be Lemma 3.13, which says that ℓ is the same power of P dividing the principal ideal $(f'(\pi))$ for some uniformizer π.

Now, fix some π with $\nu_P(\pi) = 1$. We claim that $\pi \notin \mathbb{Q}$. Since $\pi \in \mathcal{O}_K$, it suffices to show that $\pi \notin \mathbb{Z}$. Assume $\pi \in \mathbb{Z}$. Since P is a prime lying over $p \in \mathbb{Z}$, this would imply that $\pi = pl$ for some integer $l \in \mathbb{Z}$. But then $\pi = pl \in p\mathcal{O}_k = P^p \subseteq P^2$, a contradiction. Thus, π is an element of degree p and Lemma 3.13 applies. Let

$$f(x) = x^p + a_1 x^{p-1} + \cdots + a_p$$

be the minimal polynomial for π over $\mathbb{Q}$. Since π is an algebraic integer, $a_i \in \mathbb{Z}$ for all i.

We claim that $p|a_i$ for all i. To do this, we will show that that $1, \pi, \ldots, \pi^{p-1}$ are all independent mod p. That is, they are linearly independent as elements of the $\mathbb{Z}/p\mathbb{Z}$ vector space $\mathcal{O}_K/p\mathcal{O}_K$. Once we have shown this, the minimal polynomial f will give us a $\mathbb{Z}$-linear dependence, which must imply $p|a_i$ for all i. Towards a contradiction, assume that $1, \pi, \ldots, \pi^{p-1}$ are not independent mod p. Then we would have

$$\sum_{i=0}^{p-1} b_i \pi^i \in p\mathcal{O}_K,$$

where the $b_i \in \mathbb{Z}/p\mathbb{Z}$ are not all zero. Now, $p\mathcal{O}_K = P^p \subseteq P^{p-1} \subseteq \cdots \subseteq P$ and $\pi \in P - P^2$. This means $\sum_{i=0}^{p-2} b_i \pi^i \in P^{p-1}$. By subtracting the $b_i\pi^i$ for $i > 0$, we obtain $b_0 \in P$, which implies $b_0 \in p\mathcal{O}_k = P^p$ because $b_0 \in \mathbb{Z}$. We already know that $b_0 + b_1\pi \in P^2$, so using the fact that $b_0 \in p\mathcal{O}_k$, we have that $b_1\pi \in P^2$. Since $\pi \in P - P^2$, $b_1 \in P$, which again implies $b_1 \in p\mathcal{O}_k$. Repeating this process, we see that the $b_i \in p\mathcal{O}_k$ for all $0 \le i \le p-1$. This gives us a contradiction, verifying that $1, \pi, \ldots, \pi^{p-1}$ are all independent mod p and importantly that the a_i are all divisible by $p \in \mathbb{Z}$.

We will bound the exact power ℓ of P dividing the different $\operatorname{diff}(\mathcal{O}_K|\mathbb{Z})$ from above and below. The key tool for the lower bound is Hilbert's formula (Theorem 3.12). By Lemma 3.2, $V_1(P|p) = V_0(P|p) = E(P|p)$. Since p totally ramifies in K, we have that $2p-2 \le \ell$. Note that Hilbert's formula also tells us that ℓ must be a multiple of $p-1$.

Bounding ℓ from above requires more work. By Lemma 3.13, the exact power of P dividing $\operatorname{diff}(\mathcal{O}_K|\mathbb{Z})$ is the same as the exact power of P dividing the principal

ideal $(f'(\pi))$. We write out the derivative

$$f'(\pi) = p\pi^{p-1} + (p-1)a_1\pi^{p-2} + \cdots + a_{p-1}.$$

Since we have shown the a_i are all divisible by p, we know that the power of P dividing each term in the sum (thought of as principal ideals in $\mathcal{O}_K$) are incongruent mod p. Namely, they are $p-1$, $p-2$, and so on. This means that the powers of P dividing each term are all distinct. We now prove a small lemma that will allow us to bound ℓ from above.

Lemma 3.15. *The highest power of P dividing $(f'(\pi))$ is the minimum power of P dividing $p\pi^{p-1}$, $(p-1)a_1\pi^{p-2}$, …, a_{p-1} thought of as principal ideals in $\mathcal{O}_K$ assuming that the powers of P dividing these terms are all distinct. That is,*

$$\nu_P((f'(\pi)) = \min\{\nu_P((p\pi^{p-1})), \nu_P(((p-1)a_1\pi^{p-2})), \ldots, \nu_P((a_0))\}.$$

Proof. Let k be the minimum power of P dividing each term in the sum. Then $p\pi^{p-1}, (p-1)a_1\pi^{p-2}, \ldots, a_{p-1}$ are all in P^k. Since P^k is an ideal, we have that $f'(\pi) \in P^k$ as a ring element, and thus P^k divides $(f'(\pi))$. Now, assume towards a contradiction that P^{k+1} divides $(f'(\pi))$. Then $f'(\pi) \in P^{k+1}$. Since the powers of P dividing each of the terms are distinct, there is exactly one term in the sum that is not in P^{k+1}. Call this term x. Since $f'(\pi) \in P^{k+1}$ and every other term not equal to x is in P^{k+1}, we have that $x \in P^{k+1}$ since ideals are closed under subtraction. However, this contradicts that $x \notin P^{k+1}$. □

Given this lemma, we can furnish an upper bound quickly. We know that $p\mathcal{O}_K = P^p$, so $\nu_P((p\pi^{p-1})) = 2p-1$ since π is a uniformizer. This gives us

$$2p-2 \leq \ell \leq 2p-1,$$

and since we know $p-1$ must divide ℓ, we get that $\ell = 2p-2$. □

This calculation will be vital in our next lemma. We show that for an odd prime $p \in \mathbb{Z}$, any abelian extension unramified outside of p with degree p^2 over $\mathbb{Q}$ has cyclic Galois group by showing there is a unique subgroup of order p.

Lemma 3.16. *Let p be an odd prime. Let K be an abelian extension unramified outside of $p \in \mathbb{Z}$ with degree p^2 over $\mathbb{Q}$. Then $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic.*

Proof. Let P be a prime of K lying over $p \in \mathbb{Z}$. Again, p must totally ramify in K, as otherwise, the inertia field K_E would be a nontrivial extension of $\mathbb{Q}$ with no primes of $\mathbb{Z}$ ramifying contradicting Lemma 2.4.

We will show that $\mathrm{Gal}(K/\mathbb{Q})$ has a unique subgroup of order p. Let H be a subgroup of order p and set K_H to be the fixed field of H. Then the transitivity of the different (Lemma 3.11) tells us that

$$\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}) = \mathrm{diff}(\mathcal{O}_K|\mathcal{O}_{K_H})(\mathrm{diff}(\mathcal{O}_{K_H}|\mathbb{Z})\mathcal{O}_K).$$

Since H is a subgroup of order p and $[K:\mathbb{Q}] = p^2$, $[K_H:\mathbb{Q}] = p$ and K_H is an abelian extension unramified outside of $p \in \mathbb{Z}$. By Lemma 3.14, we have that $\mathrm{diff}(\mathcal{O}_{K_H}|\mathbb{Z}) = P_H^{2p-2}$, where P_H is the prime of K_H lying over $p \in \mathbb{Z}$. Furthermore, since $p \in \mathbb{Z}$ totally ramifies in K, we have that $\mathrm{diff}(\mathcal{O}_{K_H}|\mathbb{Z})\mathcal{O}_K = P^{p(2p-2)} = P^{2p^2-2p}$. Going back to the transitivity, we get that

$$\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}) = \mathrm{diff}(\mathcal{O}_K|\mathcal{O}_{K_H})P^{2p^2-2p},$$

which tells us that the different $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$, and thus $\nu_P(\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}))$ is independent of the subgroup H we pick.

We will show that $\nu_P(\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_{K_H}))$ and by the above $\nu_P(\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}))$ is strictly maximized if we pick H to be a specific higher ramification group, which will tell us that there is a unique subgroup of order p. Let r be the minimal integer such that $V_r(P|p)$ has order less than p^2. Such an r must exist as the higher ramification groups are eventually trivial (Lemma 3.8). By Lemma 3.2, $E(P|p) = V_0(P|p) = V_1(P|p)$, so $r \geq 2$ necessarily. By Lemma 3.9 we have an embedding $V_{r-1}(P|p)/V_r(P|p) \hookrightarrow \mathbb{Z}/p\mathbb{Z}$. This means that $V_r(P|p)$ either has order p^2 or order p. Since we are assuming the order of $V_r(P|p) < p^2$, we have that the order of $V_r(P|p)$ must be p.

Let V denote the fixed field of $V_r(P|p)$. Let M be the fixed field of a subgroup H of order p distinct from $V_r(P|p)$. Now, we claim that $\nu_P(\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_V)) > \nu_P(\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_M)$, a strict inequality. As always, our key tool in calculating this will be Hilbert's formula. We will have to be careful in calculating them as there are two classes of higher ramification groups we will think about. Let P_V be the prime of V lying under P, and let P_M be the prime of M lying under P. By Galois theory, $V_i(P|P_M) = V_i(P|p) \cap H$. Similarly, $V_i(P|P_V) = V_i(P|p) \cap V_r(P|p)$. Since the higher ramification groups are nested, we see that $V_i(P|P_V) = V_r(P|p)$ for $i \leq r$. This tells us that $|V_i(P|P_V)| = p$ for $i \leq r$. On the other hand $|V_i(P|P_M)| \leq p$ for all $i < r$. Importantly, $V_r(P|P_M) = V_r(P|p) \cap H = \{e\}$ since H and $V_r(P|p)$ are taken to be distinct subgrops of order p. We illustrate this in a diagram and write bounds for the orders of the groups.

$$\begin{array}{ccccccccccccc}
V_0(P|P_V) & \supseteq & V_1(P|P_V) & \supseteq & \dots & \supseteq & V_{r-1}(P|P_V) & \supseteq & V_r(P|P_V) & \supseteq & V_{r+1}(P|P_V) & \supseteq & \dots \\
p & & p & & & & p & & p & & \leq p & & \\
V_0(P|P_M) & \supseteq & V_1(P|P_M) & \supseteq & \dots & \supseteq & V_{r-1}(P|P_M) & \supseteq & V_r(P|P_M) & \supseteq & V_{r+1}(P|P_M) & \supseteq & \dots \\
p & & p & & & & \leq p & & 1 & & 1 & &
\end{array}$$

This means that $\nu_P(\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_V)) > \nu_P(\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_M)$, as desired. Since H was taken to be an arbitrary subgroup of order p distinct from $V_r(P|p)$, we know that $V_r(P|p)$ must be the only subgroup of order p. Thus, $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic. □

Given this result, deducing the uniqueness result of Theorem 3.7 is quick.

Proof of Theorem 3.7. Assume towards a contradiction there exist two distinct abelian extensions K, K' both having the property that they are unramified outside of $p \in \mathbb{Z}$ with degree p over $\mathbb{Q}$. Then the compositum KK' is an abelian extension of degree p^2 over $\mathbb{Q}$ that is unramified outside of p. By Lemma 3.16, $\mathrm{Gal}(KK'/\mathbb{Q})$ is cyclic, which means there must be a unique subfield of degree p over $\mathbb{Q}$. However, K and K' are two distinct subfields both with degree p over $\mathbb{Q}$. □

Finally, we are ready to finish our proof of the Kronecker-Weber Theorem.

Theorem 3.17. *Let p be an odd prime. Let K be an abelian p-extension of $\mathbb{Q}$ unramified outside of $p \in \mathbb{Z}$. Then K is contained in a cyclotomic field.*

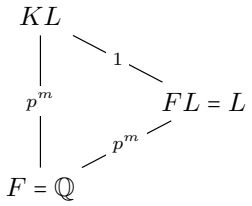
Proof. Set $[K : \mathbb{Q}] = p^m$. The case where $m = 1$ follows from Theorem 3.7. Let L be the unique subfield of the p^{m+1}-th cyclotomic field with $[L : \mathbb{Q}] = p^m$. Now, if one knows that $(\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$ is cyclic, then we already know that L has cyclic Galois group. It is also possible to see this using Theorem 3.7. Suppose L was not cyclic. Then L would have two distinct subgroups of index p which (by the Galois correspondence) would give us two distinct abelian extensions of degree p over $\mathbb{Q}$ that are unramified outside of p, which we know is impossible.

Now, let σ be a generator for $\mathrm{Gal}(L/\mathbb{Q})$. Lift σ to an automorphism $\tilde{\sigma}$ of KL and set F to be the fixed field of $\langle\tilde{\sigma}\rangle$. Since $\tilde{\sigma}$ restricts to a generator of the full Galois group $\mathrm{Gal}(L/\mathbb{Q})$ on L, we have that $F \cap L = \mathbb{Q}$. We also have that the order of $\tilde{\sigma}$ must be at least p^m. Recall that we have an embedding

$$\phi : \mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}),$$

and both $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(L/\mathbb{Q})$ are groups of order p^m, so the order of $\tilde{\sigma}$ must be exactly p^m. We claim that $F = \mathbb{Q}$. If not, F would be a subfield of KL an abelian p-extension unramified outside of p, and would have to contain the unique degree p extension of $\mathbb{Q}$ unramified outside of p, but this contradicts that $F \cap L = \mathbb{Q}$.

Finally, this tells us that $KL = FL$ using the same argument we used in the $p = 2$ case. We get the following field diagram.



Note that in this case we were able to actually show $K = L$. □

This proof shows us the utility of Theorem 3.7. We used it a number of times: to show that $\mathrm{Gal}(L/\mathbb{Q})$ was cyclic and crucially to prove that $F = \mathbb{Q}$. This completes our proof of the Kronecker-Weber theorem.

References

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 2004.

[Mar18] Daniel A. Marcus. *Number Fields*. Springer, 2018.

[Ser79] Jean-Pierre Serre. *Local Fields*. Springer, 1979.