KRONECKER-WEBER THEOREM

1. Introduction

These are some notes on the Kronecker-Weber theorem in algebraic number theory for Math 2530 at Brown university. The proof given here follows the notes found here: http://www.math.uchicago.edu/ may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Culler.pdf .

Let $K/\mathbb{Q}$ be a finite Galois extension. We call $K/\mathbb{Q}$ *abelian* if $\mathrm{Gal}(K/\mathbb{Q})$ is an abelian group. The Kronecker-Weber theorem characterizes abelian extensions of $\mathbb{Q}$. It is a vast generalization of the fact we proved in a previous lecture: if $K/\mathbb{Q}$ is degree 2 then K is contained in a cyclotomic extension $\mathbb{Q}(\zeta_n)$ where ζ_n is an n^{th} root of unity for some n.

Theorem 1.1. *(Kronecker-Weber) Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_n)$ for some n.*

The proof involves an analysis of the ramification of $K/\mathbb{Q}$ through the use of *higher ramification groups* which will be introduced in the first section. These are generalizations of the inertia group. It also makes use of the following theorem proved earlier in the class using the geometry of numbers:

Theorem 1.2. *(Minkowski) Every nontrivial extension of $\mathbb{Q}$ is ramified.*

1.1. **Notation.** We will fix standard notation so that if L/K is an extension of number fields or local fields, $B = \mathcal{O}_L$ and $A = \mathcal{O}_K$ will denote the corresponding ring of integers. We will denote by $\mathfrak{P}/\mathfrak{p}/p$ primes of L, K, and $\mathbb{Q}$ respectively. $L_{\mathfrak{P}}/K_{\mathfrak{p}}/\mathbb{Q}_p$ will denote the respective completions.

2. Ramification Groups

Let L/K be any Galois extension of number fields or local fields. The higher ramification groups are natural generalizations of the inertia group.

Definition 2.1. *The n^{th} ramification group $G_n(\mathfrak{P}|\mathfrak{p})$ is defined as*

$$G_n(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(x) = x \mod \mathfrak{P}^{n+1} \text{ for all } x \in B\}.$$

We will drop $\mathfrak{P}/\mathfrak{p}$ when it is clear. When $n = -1$ we get the whole Galois group G and for $n = 0$, G_0 is the inertia group. Recall that the ramification index $e(\mathfrak{P}|\mathfrak{p}) = |G_0|$. In particular, $\mathfrak{P}$ is unramified if and only if $G_0 = 0$.

By definition, $G_n \supset G_{n+1}$ and G_0 is a subgroup of $D = D(\mathfrak{P}|\mathfrak{p})$ where D is the decomposition group. The latter follows from the fact that $\sigma(x) = 0 \mod \mathfrak{P}$ for $\sigma \in G_0$ and $x \in \mathfrak{P}$ so $\sigma(\mathfrak{P}) \subset \mathfrak{P}$. Finally, G_n is normal in D. Indeed if $\sigma \in G_n$ and $\tau \in D$,

$$\sigma\tau x - \tau x \in \mathfrak{P}^{n+1}$$

since $\sigma \in G_0$ but then applying τ^{-1}, we still land in $\mathfrak{p}^{n+1}$ since $\tau^{-1} \in D$ so

$$\tau^{-1}\sigma\tau x - x \in \mathfrak{P}^{n+1} \implies \tau^{-1}\sigma\tau x = x \mod \mathfrak{P}^{n+1}.$$

Proposition 2.2. *The ramification groups G_n for $n \geq 0$ depend only on the local field extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$.*

Proof. The ramification groups are contained in D for all n. There is a natural map $D \to \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ because an automorphism in D lifts to the completion since it fixes $\mathfrak{P}$. This is clearly injective. On the other hand, there is an inverse map by restriction so in fact $D \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. Then this isomorphism sends G_n to the corresponding ramification group of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$.

□

Reducing to the local field simplifies proofs as in the following.

Recall for a local field extension L/K we had defined the unit groups U_n where $U_0 = B^\times$ and $U_n = 1 + \mathfrak{P}^n$ for $n \geq 1$. Let ϖ be a generator of $\mathfrak{P}$ in the completion. Then any $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ sends ϖ to another generator of $\mathfrak{P}$, i.e.,

$$\sigma(\varpi) = u\varpi$$

for $u \in U_0$. If $\sigma \in G_n$ for $n \geq 0$.

$$u\varpi = \varpi \mod \mathfrak{P}^{n+1} \implies u\varpi = \varpi + \eta\varpi^{n+1} \implies u = 1 + \eta\varpi^n \in U_n.$$

Thus if $\sigma \in G_n$ for $n \geq 0$, $\sigma(\varpi)/\varpi \in U_n$.

Proposition 2.3. *The correspondance above sending $\sigma \in E_n$ to $\sigma(\varpi)/\varpi \in U_n$ defines an injective homomorphism*

$$\varphi_n : G_n/G_{n+1} \to U_n/U_{n+1}.$$

that is independent of the choice of ϖ.

Proof. Suppose $v\varpi$ is another generator for $\mathfrak{P}$. Then v is a unit and $\sigma(v) = v \mod \mathfrak{P}^{n+1}$ so $\sigma(v)/v = 1 \mod \mathfrak{P}^{n+1}$ so $\sigma(v)/v \in U_{n+1}$ and

$$\frac{\sigma(v\varpi)}{v\varpi} = \frac{\sigma(v)\sigma(\varpi)}{v\varpi} = \frac{\sigma(\varpi)}{\varpi}$$

in U_n/U_{n+1}. Thus the map $\varphi_n : G_n \to U_n/U_{n+1}$, $\sigma \mapsto \sigma(\varpi)/\varpi$ is independent of choice of ϖ. To see it is a homomorphism, let $\sigma, \tau \in G_n$.

$$\varphi_n(\sigma\tau) = \frac{\sigma\tau(\varpi)}{\varpi} = \frac{\sigma(\alpha\varpi)}{\varpi} = \frac{\sigma(\alpha)\sigma(\varpi)}{\varpi} = \frac{\alpha\sigma(\varpi)}{\varpi} = \frac{\tau(\varpi)}{\varpi}\frac{\sigma(\varpi)}{\varpi}$$

in U_n/U_{n+1} since $\alpha = \tau(\varpi)/\varpi$ by definition.

Next suppose $\sigma \in G_{n+1}$. Then $\sigma(\varpi)/\varpi \in U_{n+1}$ so $\varphi_n(\sigma) = 1$ in U_n/U_{n+1} and the map factors as $G_n/G_{n+1} \to U_n/U_{n+1}$.

Finally, suppose $\varphi_n(\sigma) = \alpha = 1 \mod \mathfrak{P}^{n+1}$. Then since any $x = u\varpi^k$ for some unit u and $k \in \mathbb{Z}$, we have

$$\sigma(x) = \sigma(u)\sigma(\varpi^k) = \sigma(u)\alpha^k\varpi^k = u\varpi^k \mod \mathfrak{P}^{n+1}$$

so $\sigma \in G_{n+1}$ and $\varphi_n : G_n/G_{n+1} \to U_n/U_{n+1}$ is injective.

□

Corollary 2.4. *$\mathfrak{P}$ is tamely ramified over $\mathfrak{p}$ if and only if $G_n = 1$ for all $n \geq 1$.*

Proof. Suppose $\mathfrak{P}$ is tamely ramified. Then p is coprime to $|G_0|$ so since $G_n \subset G_0$ for all n, then p is coprime to G_n/G_{n+1}. $\varphi_n : G_n/G_{n+1} \to U_n/U_{n+1}$ is an injection and we proved in a previous lecture that for $n \geq 1$

$$U_n/U_{n+1} \cong B/\mathfrak{P}$$

which has order a power of p. Thus $G_n/G_{n+1} = 1$ for all $n \geq 1$ and so $G_n = 1$ for all $n \geq 1$.

Conversely, suppose $G_n = 1$ for all $n \geq 1$. Then $G_0/G_1 = G_0$ is a subgroup of $U_0/U_1 = (B/\mathfrak{P})^\times$ whose order is prime to p so $|G_0| = e(\mathfrak{P}|\mathfrak{p})$ is prime to p.

□

Remark 2.5. *This also lets us prove that the decomposition group D is solvable. Indeed we already know that D/G_0 is the Galois group of the residue field extension which is abelian. Then G_n/G_{n+1} is abelian for $n \geq 0$ since it injects into the abelian group U_n/U_{n+1}. In particular, when L/K is an extension of local fields, $D = \mathrm{Gal}(L/K)$ so the Galois group of local fields is solvable.*

Recall that we have the residue field extension $A/\mathfrak{p} \subset B/\mathfrak{P}$. Then $(A/\mathfrak{p})^\times \subset (B/\mathfrak{P})^\times = U_0/U_1$.

Proposition 2.6. *If D/G_1 is abelian, then the image G_0/G_1 in $(B/\mathfrak{P})^\times$ is contained in $(A/\mathfrak{p})^\times$.*

Proof. $G_0/G_1 \subset D/G_1$ so for any $\tau \in D$ and $\sigma \in G_0$, $\tau\sigma\tau^{-1} = \sigma$ in G_0/G_1 by the abelian assumption.

On the other hand, if $\varphi_0(\sigma) = \alpha$, then $\sigma\tau^{-1}(\varpi) = \alpha\tau^{-1}(\varpi) \mod \mathfrak{P}^2$ since $\tau^{-1}(\varpi)$ is also a generator and we showed that $\sigma(\varpi)/\varpi$ is independent of generator modulo U_1. So

$$\alpha\varpi = \sigma(\varpi) = \tau\sigma\tau^{-1}\varpi = \tau(\alpha)\varpi \mod \mathfrak{P}^2$$

so $\alpha = \tau(\alpha) \mod \mathfrak{P}$ for any $\tau \in D$. Since D surjects onto the resiude field, then α is fixed by any element of the Galois group of the residue field and so $\alpha \in A/\mathfrak{p}$, the base residue field.

□

3. The Proof

3.1. **Tamely ramified extensions.** Now we will prove that it suffices to show Kronecker-Weber in the case where $K/\mathbb{Q}$ only has wild ramification.

Theorem 3.1. *Suppose $K/\mathbb{Q}$ is an abelian extension so that $\mathfrak{p}/p$ is tamely ramified. Then there exists a root of unity ζ and field extensions $K'/\mathbb{Q}$ and $L \subset \mathbb{Q}(\zeta)$ such that the following hold:*

(a) if q is unramified in K then it is unramified in K',

(b) p is unramified in K',

(c) and $LK = LK'$.

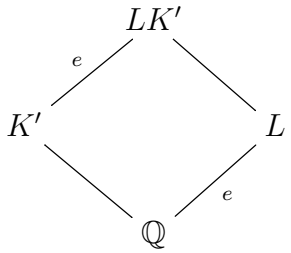
First let us see why this reduces to the case of only wildly ramified abelian extensions. Since there are only finitely many ramified primes, we can apply this theorem several times to get a field extension K' so that K' has no tamely ramified primes and has exactly the same wildly ramified primes as K and that $LK = LK'$. Furthermore, $LK = LK'$ is abelian since L and K each are so K' is also abelian. If we can show that K' is contained in a cyclotomic field, then LK' is as well so $K \subset LK'$ is and we are done.

Proof. $G_1 = 0$ by the tame ramification assumption so since the Galois group is abelian, we can apply the previous proposition to see that the inertia $G_0/G_1 = G_0$ is a subgroup of $(\mathbb{F}_p)^\times$. Thus $e|p-1$ and so there exists a unique extension $L \subset \mathbb{Q}(\zeta_p)$ with degree e over $\mathbb{Q}$.

We proved earlier that p is totally ramified in $\mathbb{Q}(\zeta_p)$ and so p is totally and tamely ramified in L since e is prime to p. In particular there is a unique prime $\mathfrak{q}/p$ in L. Then take $\mathfrak{Q}$ a prime of KL/L lying over $\mathfrak{q}$. So $\mathfrak{Q}$ lies over $p \in \mathbb{Z}$. Let $G_0' = G_0(\mathfrak{Q}|p)$ and $K' = (LK)^{G_0'}$ the fixed field.

L is ramified only at p so if q is unramified in K, then $q \neq p$ so it is also unramified in L and thus unramified in KL. Therefore if q is unramified in K, it is unramified in $K' \subset LK$. Furthermore, p is unramified in K' since K' is the inertial field of $\mathfrak{Q}/p$.

Now we show that $LK' = LK$ by comparing degrees. First, p is unramified in K' and p is totally ramified in L with ramification $e = [L : \mathbb{Q}]$ so p ramified in LK' with ramification e. In particular, $[LK' : K'] \geq e$ by comparing ramification indices in the diagram



On the other hand, $[LK : K'] = |G_0'|$ by assumption. $\mathfrak{Q}$ is tamely ramified since p is tamely ramified in both L and K. G_0' injects into the multiplicative group of the residue field $(\mathbb{Z}/p)^\times$ by the two previous propositions and so G_0' is a cyclic group. Similarly $\mathrm{Gal}(LK/\mathbb{Q})$ injects into $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ and so G_0' does as well. Let $\mathfrak{p}' = \mathfrak{Q} \cap K$. Then by definition, G_0' restricted to K gives an element in the inertia group $G_0(\mathfrak{p}'|p)$ but $\mathfrak{p}'$ is conjugate to $\mathfrak{p}$ so the order of $G_0(\mathfrak{p}'|p)$ is $|G_0| = e$.

Thus G_0' lives in the subgroup $G_0(\mathfrak{p}'|p) \times \mathrm{Gal}(L/\mathbb{Q})$, both of which are groups of order e so G_0' has exponent e. Since it is cyclic and of exponent e, $|G_0'| \leq e$.

Putting it together, we have

$$e \geq |G_0'| = [LK : K'] \geq [LK' : K'] \geq e$$

so in fact we have equalities everywhere and $LK = LK'$.

□

Since any abelian group is a product of cyclic groups of prime power, then we can decompose any abelian extension into the composite of cyclic subextensions of prime power degree. If we can show any such subextension is contained in a cyclotomic field, then we are done since compositums of cyclotomic fields are cyclotomic.

In the case when $[K : \mathbb{Q}] = p^n$, then every prime $q \neq p$ must be unramified or tamely ramified. Therefore by the proposition above, we can suppose without loss of generality that every prime other than p is unramified, and in this case p must be wildly ramified by Minkowski's theorem (otherwise $K = \mathbb{Q}$ and we're done).

3.2. **Cyclic p-power extensions.** By the discussion above, we have reduced to the case where $[K : \mathbb{Q}] = p^n$ is a prime power cyclic extension with p the only ramified prime. Because of the second condition, the discriminant $d(K/\mathbb{Q})$ is a power of p. So to finish the proof, we need only prove the following:

Theorem 3.2. *If $K/\mathbb{Q}$ is as above with p odd, then K is a subfield of $\mathbb{Q}(\zeta)$ where ζ is a p^{n+1} root of unity. If $p = 2$, then K is a subfield of $\mathbb{Q}(\zeta)$ with ζ and 2^{m+2} root of unity for some m.*

Proof. If p is odd, $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ is $p^n(p-1)$ with cyclic Galois group. Let L be the unique (cyclic) subextension of order p^n and let σ be a generator for the Galois group.

The compositum KL is also an abelian extension of p-power order and with p-power discriminant. Let τ be a lift of σ to KL and suppose F is the fixed field of $\langle\tau\rangle$. Since σ generates $\mathrm{Gal}(L/\mathbb{Q})$, its fixed field is $\mathbb{Q}$. Thus $L \cap F = \mathbb{Q}$ since $\tau|_L = \sigma$.

Consider the embedding

$$\mathrm{Gal}(LK/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q}).$$

The latter groups both have order p^n so any element of $\mathrm{Gal}(LK/\mathbb{Q})$ has order at most p^n. In particular τ has order at most p^n. However, σ has order p^n by construction so τ has order exactly p^n and $[KL : F] = p^n$.

Lemma 3.3. *If p is an odd prime, then there is a unique extension of $K/\mathbb{Q}$ of order p with discriminant a power of p.*

With the lemma in hand, suppose that $F \neq \mathbb{Q}$. Then L and F are both cyclic extensions of order p-power and p-power discriminant. Therefore they both contain the unique extension above, contradicting that $L \cap F = \mathbb{Q}$. Therefore $F = \mathbb{Q}$ so $[L : \mathbb{Q}] = p^n = [KL : F] = [KL : \mathbb{Q}]$ and $K \subset KL = L \subset \mathbb{Q}(\zeta)$.

For the case $p = 2$ we need the following lemma.

Lemma 3.4. *Suppose $E/\mathbb{Q}$ is a quadratic extension with 2-power discriminant. Then $E = \mathbb{Q}(\sqrt{l})$ with $l = -1, \pm 2$.*

Now suppose that $E/\mathbb{Q}$ is a 2-power extension with 2-power discriminant and that E is contained in the real numbers. Then the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is a 2-group. Note that a two group is cyclic if and only if there is a unique quotient of order 2. By Galois theory this is equivalent to saying that $E/\mathbb{Q}$ is cyclic if and only if there is a unique subextension of order 2. By the lemma above,

since $E/\mathbb{Q}$ is unramified away from 2 and 2-power, the only options for subextensions of order 2 are $\mathbb{Q}(\sqrt{l})$ for $l = -1, \pm 2$. Since E is real then $l = 2$ so is the unique subextension of order 2 and thus $E/\mathbb{Q}$ is cyclic.

Now recall what we wanted to show is that if K is a 2-power extension with 2-power discriminant, then K embeds into a cyclotomic field.

Consider $K(i)$ where i is a root of $x^2 + 1$. This is the compositum of K and $\mathbb{Q}(i)$, both of which are unramified away from 2, and so $K(i)$ is unramified away from 2. Let K' be the subextension of $K(i)$ that is the fixed field of complex conjugation. Then K' is totally real 2-power degree with 2-power discriminant and so is cyclic by the above argument. Say the degree of $K'/\mathbb{Q}$ is 2^m.

Take $L = \mathbb{Q}(\zeta) \cap \mathbb{R}$ where ζ is a 2^{m+2} root of unity as in the statement of the theorem. Then L is the fixed field of $\mathbb{Q}(\zeta)$ by complex conjugation and so is a totally real field of degree 2^m with 2-power discriminant (since its a subfield of a 2-power cyclotomic) and thus is also cyclic. Then the compositum LK' is also totally real 2-power degree with 2-power discriminant and is cyclic as well.

But $\mathrm{Gal}(LK'/L \cap K') = \mathrm{Gal}(L/L \cap K') \times \mathrm{Gal}(K'/L \cap K')$ where each of these groups are cyclic 2-groups. The only way this could happen is if one of the groups on the right is trivial since a product of nontrivial 2-groups is not cyclic. Therefore either $L = L \cap K'$ or $K' = L \cap K'$ but the degrees of L and K' over $\mathbb{Q}$ are equal so either way we get that $L = K'$. Therefore $K' = L \subset \mathbb{Q}(\zeta)$ but $K'(i) = K(i)$ since $K' = K(i) \cap \mathbb{R}$ and so

$$K \subset K(i) = K'(i) \subset \mathbb{Q}(\zeta, i)$$

and the latter is the compositum of cyclotomic extensions so it is cyclotomic and we are done.

□

3.3. **Proofs of Lemmas.**

Proof. (Lemma 3.3) This one is kind of involved so I'm not going to do the computations here. However I'll very roughly sketch the idea. See the link above for the full details.

Start with K the unique subfield of the p^2 cyclotomic field of order p. This satisfies the conditions of the lemma. Take K' another p order extension with p-power discriminant. Then look at $K'L$ where $L = \mathbb{Q}(\zeta)$ is a p-cyclotomic field. It can be shown that $K'L = L(\sqrt[p]{(\alpha)})$ for some α. It can also be shown after some heavy computations with the Galois group using the abelian property that

$$\alpha \equiv 1 \mod \lambda^p$$

where $\lambda := 1 - \zeta$.

Then the idea from here is to use this to construct an algebraic integer, namely

$$\xi = \frac{1 - \sqrt[p]{\alpha}}{\lambda}$$

in $KK'L$ and compute its discriminant by finding the minimal polynomial. If $K \neq K'$, this leads to a nontrivial extension $KL[\xi]/KL$. The discriminant ends up being coprime to p and by taking inertial fields, we get a nontrivial extension that is unramified at p but is also unramified at $q \neq p$

since KL is unramified away from p. This contradicts Minkowski's theorem that there are no nontrivial unramified extensions of $\mathbb{Q}$.

□

Proof. (Lemma 3.4) We have computed the number ring of a quadratic extension $\mathbb{Q}(\sqrt{l})$ with l squarefree as $\mathbb{Z}[\beta]$ where $\beta = \sqrt{l}$ if $l \equiv 2, 3 \mod 4$ and $\beta = (1+\sqrt{l})/2$ if $l \equiv 1 \mod 4$.

In the first case the minimal polynomial of β is $f(x) = x^2 - l$ so the discriminant $d = N(f'(l)) = N(2\sqrt{l}) = 4l$. The only way this is a power of 2 for $l \equiv 2, 3 \mod 4$ is if $l = -1, \pm 2$.

In the second case the minimal polynomial of β is

$$f(x) = x^2 + x + \frac{1-l}{2}$$

so we compute $d = N(f'(\beta)) = N(2\beta + 1) = N(\sqrt{l}) = l$. Since $l \equiv 1 \mod 4$, there are no l with d a power of 2 and so the above are the only options for l.

□