The Kronecker-Weber Theorem and Current Progress in its Formalization

Reviewing The Proof of The Kronecker-Weber Theorem and Discussing Current Works on Formalizing it

Huanyu Zheng

Supervisor: Luciena Xiao

Xi'an Jiaotong University
School of Mathematics and Statistics
Department of Mathematics and Applied Mathematics

Xi'an, September 2024

Abstract

In this paper, we will begin by recalling the background and historical position of the Kronecker-Weber theorem. Then we present a suitable proof structure for formalization after listing relevant definitions and basic results. Finally, a discussion on current works in its formalization using Lean 4 is given.

Keywords: The Kronecker-Weber Theorem, Formalization, Lean.

Contents

Contents 1

1 Introduction 2

2 Higher Ramification Group 3

2.1 Basic Ramification Theory 3

2.2 Higher Ramification Group 6

3 The Kronecker-Weber Theorem 8

3.1 General Idea 8

3.1.1 General Idea: Reducing to Wild Ramification 8

3.1.2 General Idea: Reducing to Prime Power Cyclic Extension 10

3.1.3 General Idea: Finishing Proof 11

3.2 Reducing to Wildly Ramified Case 12

3.3 Reducing to Prime Power Cyclic Extension 13

4 Discussions 14

1

Introduction

Theorem 1.1 (Kronecker-Weber)**.**

Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

The Kronecker-Weber theorem stands as a landmark result in the field of algebraic number theory, representing a foundational moment in the development of class field theory. This theorem not only provides a deep understanding of the structure of number fields but also connects the seemingly abstract concept of abelian extensions to the concrete and well-understood world of roots of unity.

David Hilbert provided the first rigorous proof of the theorem, which was built upon the earlier insights of Kronecker and Weber. Hilbert's approach involved the usage of higher ramification groups, a tool that allows deeper analysis of how primes behave in field extensions, particularly in understanding the distinction between tame and wild ramification. This framework not only completed the proof of the Kronecker-Weber theorem but also laid the groundwork for the future development of class field theory, which would later be expanded by mathematicians such as Emil Artin and Helmut Hasse.

In recent years, there has been increasing interest in the formalization of mathematical theorems using computer assisted theorem prover like Lean. The Kronecker-Weber theorem, with its rich structure and historical importance, has become a subject of focus in this area. The formalization process involves encoding the proof of the theorem into a computer-verifiable format, ensuring not only the correctness of the proof but also making it accessible for future computational applications.

One of the main difficulty in formalization is to find relevant existing works, as they always lack of natural language annotation and appear very different from our expectation. Thus, throughout this paper, I will presents basic proof steps along side with existing relevant lemmas in mathlib, the theorem library for Lean, if any. And I shall also explain their connections. Finally I will build a basic algorithm or framework to prove Kronecker-Weber in a formalization fashion.

2

Higher Ramification Group

2.1 Basic Ramification Theory

In this section we define some basic concepts useful in analyzing how prime behaves while moving along algebra extensions. Main result here are Theorem 2.2 and 2.4.

Definition 2.1 (Residue field)**.**

- ***Residue field*** $k(\mathfrak{p})$ *at prime ideal* $\mathfrak{p}$ *in a general Dedekind domain* A*:* $A/\mathfrak{p}$

```
def LocalRing.ResidueField (R : Type u_1) [CommRing R] [LocalRing R] : Type u_1 :=
    R / LocalRing.maximalIdeal R
```

Remark 2.1. *In the first glimpse, the definition in Lean is very different from our definition. But in fact Lean's definition is more general.*
It can be proved that for general ring A *and its prime ideal* $\mathfrak{p}$*,*

$$Frac(A/\mathfrak{p}) \simeq A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$$

where $A_{\mathfrak{p}}$ *is a localization. In our case, take* A *a Dedekind domain, so* $\mathfrak{p}$ *is a maximal ideal, hence* $Frac(A/\mathfrak{p})$ *is just* $A/\mathfrak{p}$*. Therefore,*

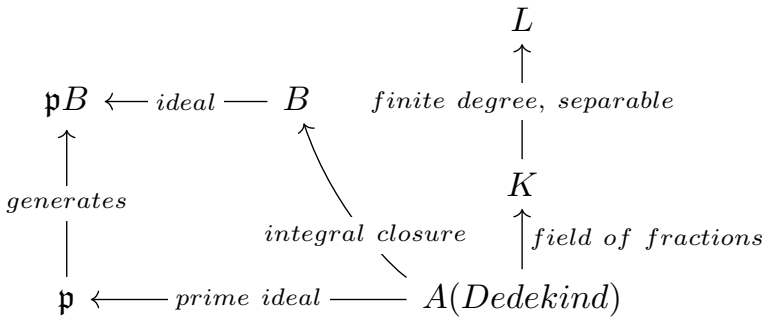
$$k(\mathfrak{p}) \simeq \texttt{LocalRing.ResidueField } A_{\mathfrak{p}}$$

Remark 2.2. *More on residue field*

> *The residue field at a prime* $\mathfrak{p}$ *is essentially the field you get by "modding out" by* $\mathfrak{p}$*. This operation simplifies the arithmetic and focuses on the essential behavior of that prime. Normally, we don't care much about what happends within the ideal* $\mathfrak{p}$*, rather, we study how* $\mathfrak{p}$ *behaves as a whole.*

Now consider A a Dedekind domain with field of fractions K, and B the integral closure of A in a finite separable extension L of K. $\mathfrak{p}$ is a prime ideal of A, it generates an

ideal $\mathfrak{p}B$ in B. In particular, if only number field is concerned, A, B, K are $\mathbb{Z}$, $\mathcal{O}_L$, $\mathbb{Q}$ respectively. We visualize our setup as below.



B is a Dedekind domain (see ANT.Theorem 3.29), then by the factorization of ideals in Dedekind domain (see `Ideal.uniqueFactorizationMonoid`), $\mathfrak{p}B$ factors into:

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

where $\mathfrak{P}_i$ are prime ideals in B.

Definition 2.2 (Lies over)**.**

- $\mathfrak{P}$ ***lies over*** $\mathfrak{p}$*:* $\mathfrak{P}$ *appears in the factorization of* $\mathfrak{p}$*.*

Remark 2.3. *One may also say that* $\mathfrak{P}$ *divides* $\mathfrak{p}$ *here. In Lean, there is no explicit definition of it, but one can still use* `map f p ≤ P` *(where* `f : R →+* S`*) to indicate the same thing.*

Definition 2.3 (Ramified)**.**

- $\mathfrak{p}$ *is* ***ramified*** *in* B *(or* L*): if any of the* e_i *is* ≥ 2*.*
- (***Unramified****: all* e_i *are 1. Also, we say the field* L *is ramified when there exists a ramified prime ideal of* A*, otherwise it is unramified*)

Definition 2.4 (Ramification index)**.**

- ***Ramification index*** $e(\mathfrak{P}/\mathfrak{p})$*: the power of* $\mathfrak{P}$ *in the factorization of* $\mathfrak{p}$*. e.g.,* $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$*.*

```
noncomputable def Ideal.ramificationIdx {R : Type u} [CommRing R] {S : Type v}
  [CommRing S] (f : R →+* S) (p : Ideal R) (P : Ideal S) : ℕ :=
    sSup {n | map f p ≤ P ∧ n}
```

Remark 2.4. *In Lean, ramification index is defined with respect to all ideals and all commutative rings, it is the largest exponent* e *such that* $\mathfrak{p}$ *is contained in* $\mathfrak{P}^e$*. In particular, if* $\mathfrak{p}$ *is not contained in any* $\mathfrak{P}^e$*, then the ramification index is 0. If there is no largest such* e *(like when* $\mathfrak{p}$ *is trivial), then it is also defined to be 0.*

Remark 2.5. *Understanding ramification more deeply:*

> *When we "move" a prime ideal of a domain into a larger domain, ramification helps us to determine whether it behaves well. Four things can happend here:*
>
> 1. *it stays as a single prime ideal.* (*unramified*)
> 2. *it splits into distinct primes.* (*unramified*)
> 3. *it stays as a single prime but with a higher exponent.* (*totally ramified*)
> 4. *it splits into several primes, some of which have higher exponents.* (*ramified*)
>
> *Obviously the prime behaves more complicated and "badly" in the last two situations - we name this "ramified". A ramified prime acts "badly", but how bad? Then it comes to tamely/wildly ramification.*

Theorem 2.1. *If L is Galois over K, then all the ramification indexes (of primes lying over $\mathfrak{p}$) are equal and all the residue class degrees are equal. Further, $efg = [L : K]$. (See ANT. Theorem 3.34 for proof.)*

Definition 2.5 (Tamely and wildly ramified)**.**

- $\mathfrak{P}/\mathfrak{p}$ *is* ***tamely ramified****: ramification index $e(\mathfrak{P}/\mathfrak{p})$ is relatively prime to the characteristic of residue field $k(\mathfrak{P})$.*
- (***wildly ramified****: otherwise.)*

Theorem 2.2. *If B is a free A-module, then prime $\mathfrak{p}$ ramifies in L iff $\mathfrak{p} \mid disc(B/A)$. In particular, only finitely many prime ideals ramify.* (See ANT. Theorem 3.35 for proof.)

Theorem 2.3 (Hermite)**.** *Every nontrivial number field has discriminant greater than 2.* (This is a direct collary of ANT. Theorem 4.3.)

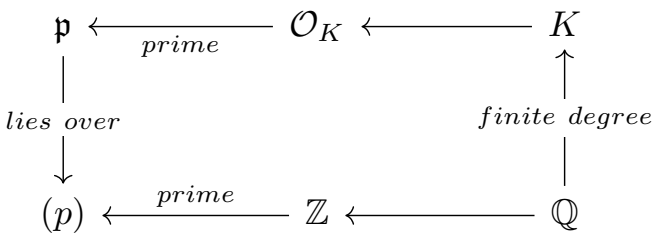
```
1  theorem NumberField.abs_discr_gt_two {K : Type u_1} [Field K] [NumberField K] (h : 1 <
   ↪  FiniteDimensional.finrank ℚ K) : 2 < |NumberField.discr K|
```

Theorem 2.4 (Minkowski)**.** *Every nontrivial number field is ramified.*(there must be a prime $p \in \mathbb{Z}$ ramifies in the extension.)

Proof. This is a direct result of Theorem 2.2 and Theorem 2.3. □

2.2 Higher Ramification Group

Previous section provides us with initial concepts to study prime's behaviour. But ramified/unramified is a rough classification, we often need more delicate analysis. That's when higher ramification group comes into play.
We now focus on number fields. Suppose the following setup:



Definition 2.6 (Decomposition group and decomposition field)**.**

- ***Decomposition group*** $D(\mathfrak{p}/p)$*: the stabilizer of* $\mathfrak{p}$ *under action of* $Gal(K/\mathbb{Q})$*. i.e.,* $\{\sigma \in Gal(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$.
- ***Decomposition field****: fixed field of* $D(\mathfrak{p}/p)$*, denoted* $\mathcal{F}_K(D(\mathfrak{p}/p))$.

```
@[reducible, inline]
 abbrev ValuationSubring.decompositionSubgroup (K : Type u_1) {L : Type u_2} [Field K]
↪  [Field L] [Algebra K L] (A : ValuationSubring L) : Subgroup (L ≃ₐ[K] L) :=
    MulAction.stabilizer (L ≃ₐ[K] L) A
```

Remark 2.6. *Similar to residue field, we investigate* $\mathfrak{p}$ *as a whole here. Thus* $\sigma \in D(\mathfrak{p}/p)$ *might permutes elements in* $\mathfrak{p}$*, but it must fix* $\mathfrak{p}$ *as a whole.*
Lean defines decomposition group to be the stabilizer of the action on the type of all valuation subrings of the field, where valuation subring of a field L *is a subring* A *such that for every* $x \in L$*, either* $x \in A$ *or* $x^{-1} \in A$*.*
These two definitions are not exactly the same. But the stabilizer of A *is the same as the stabilizer of the maximal ideal* $\mathfrak{m}$ *of* A*, i.e.,* $\{\sigma \in Gal(L/K) \mid \sigma(A) = A\} = \{\sigma \in Gal(L/K) \mid \sigma(\mathfrak{m}) = \mathfrak{m}\}$*. Hence we shall obtain the same thing by substituting* A *with* $(\mathcal{O}_K)_{\mathfrak{p}}$*.*
Technically, one can create a prime spectrum by `IsDedekindDomain.HeightOneSpectrum` *with desired prime and use* `IsDedekindDomain.HeightOneSpectrum.valuation` *to get a valuation attached to the ideal. Finally* `Valuation.valuationSubring` *can transform it into a valuation subring, then we can plug it into* `ValuationSubring.decompositionSubgroup`*.*

Since $\sigma \in D(\mathfrak{p}/p)$ sends $\mathfrak{p}$ to itself, a natural automorphism emerges here:

$$\sigma' : \ k(\mathfrak{p}) \longrightarrow k(\mathfrak{p}), \ x \ mod \ \mathfrak{p} \longmapsto \sigma(x) \ mod \ \mathfrak{p}$$

$D(\mathfrak{p}/p) \leq Gal(K/\mathbb{Q})$, so σ fixes $\mathbb{Q}$, hence $k(p)$. Consider group homomorphism:

$$D(\mathfrak{p}/p) \longrightarrow Gal(k(\mathfrak{p})/k(p)), \ \sigma \longmapsto \sigma'$$

Definition 2.7 (Inertia group)**.**

- ***inertia group*** $I(\mathfrak{p}/p)$ *of* $\mathfrak{p}$*: the kernel of this homomorphism. i.e.,* $\{\sigma \in D(\mathfrak{p}/p) \mid \forall x \in \mathcal{O}_K,\ \sigma(x) \equiv x \ mod\ \mathfrak{p}\}$

```
def ValuationSubring.inertiaSubgroup (K : Type u_1) {L : Type u_2} [Field K] [Field L]
↪ [Algebra K L] (A : ValuationSubring L) : Subgroup
↪ ↑(ValuationSubring.decompositionSubgroup K A) :=
    (MulSemiringAction.toRingAut ( ↑(ValuationSubring.decompositionSubgroup K A))
    ↪ (LocalRing.ResidueField ↑A)).ker
```

Remark 2.7. *More on inertia group*

The inertia group at a prime measures how much the elements of the Galois group "move" the prime ideal within its own orbit. It consists of those elements of the Galois group that act trivially on the residue field $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$*. In fact we can view inertia group as decomposition group with restriction that residue field must be fixed.*

Definition 2.8 (n^{th} ramification group)**.**

- *the* n^{th} ***ramification group*** $I_n(\mathfrak{p}/p)$ *of* $\mathfrak{p}$*:* $\{\sigma \in D(\mathfrak{p}/p) \mid \forall x \in \mathcal{O}_K, \sigma(x) \equiv x \ mod\ \mathfrak{p}^{n+1}\}$

Remark 2.8. *More on higher ramification group*

The first observation is that $I_0(\mathfrak{p}/p)$ *is exactly the inertia group. In fact, the inertia group* $I(\mathfrak{p}/p)$ *gives you the "first layer" of information about ramification of* p*.* $I_i(\mathfrak{p}/p)$ *are subgroups of the inertia group, and each higher* i *focuses on finer details of the ramification.*

- $I_1(\mathfrak{p}/p)$ *consists of elements of the inertia group that act more "mildly" on* $\mathfrak{p}$*. Specifically,* I_1 *measures those elements that do nothing up to the first power of* $\mathfrak{p}$*, leaving the ideal unchanged modulo* $\mathfrak{p}^2$*.*
- *For higher* n*,* I_n *measures those elements of the Galois group that leave elements of the ideal unchanged up to the* $n+1$ *power, meaning they only "kick in" at deeper, more refined levels of the ideal's structure.*

Of course we can also define n^{th} ramification group as kernels of group homomorphisms as we did in intertia group. Hence:

$$D(\mathfrak{p}/p) \rhd I(\mathfrak{p}/p) = I_0(\mathfrak{p}/p) \rhd \cdots \rhd I_n(\mathfrak{p}/p) \rhd \dots$$

The significance of higher ramification group comes as:

Theorem 2.5. $\mathfrak{p}/p$ *is tamely ramified iff all higher ramification groups* $(n > 1)$ *are trivial.* (see proof)

Theorem 2.6. *If* D/I_1 *(we omitte* $\mathfrak{p}/p$ *here) is abelian, then* I_0/I_1 *is contained in* $(k(p))^\times$*.* (see proof)

3

The Kronecker-Weber Theorem

3.1 General Idea

Recall that,

Theorem 1.1 (Kronecker-Weber)**.**

Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

We will first presents the general idea towards the goal and leave technical details to remaining sections. The main structure of our proof here is built in favor of formalization and automated theorem proving, which emphasis computability and clarity.

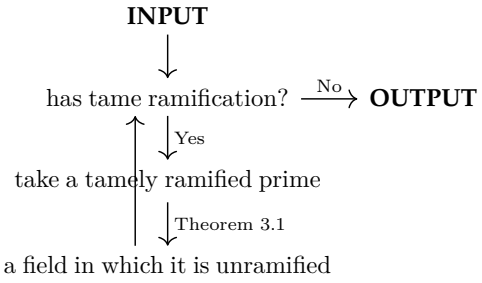
3.1.1 General Idea: Reducing to Wild Ramification

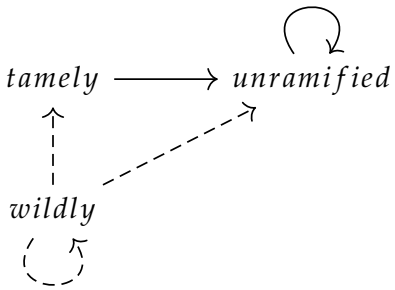
We first reduce the case into abelian extension $K/\mathbb{Q}$ **that only has wild ramification**. This is done by "turning every tame ramification one by one into unramified element".

Theorem 3.1. *Suppose that $K/\mathbb{Q}$ is an abelian extension, p is tamely ramified over K. Then we can construct another **abelian** extension $K'/\mathbb{Q}$, together with a subfield L of some cyclotomic field, such that*

1. *p is unramified in K'*
2. *unramified prime in K stays unramified in K'*
3. *$LK = LK'$*

This theorem induces an algorithm as shown on the right. We claim that **after finite steps of iteration, the algorithm will halt and we will get a field with only wildly ramified primes**. As drawn below, the fate of tamely ramified prime and unramified prime under the algorithm is destined - tamely ramified prime must be turned to unramified, whereas unramified must stay still. The only variant here is wildly ramified primes.

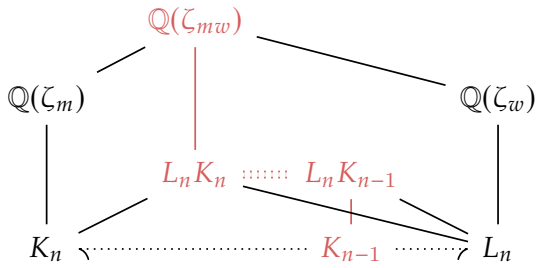




According to Theorem 2.4, there are only finitely many ramified primes. Viewing tame and wild ramification in the graph as a whole (imagine drawing a box around them). We shall notice that there are no arrows pointing to the box, only arrows pointing out (nothing get converted into ramified prime).
This means that whatever happends, the number of primes in the box is strictly decreasing - this decrease must halt within finite step since the number is finite. Thus the algorithm is halting. And since the process can go on as long as there exists a tamely ramified prime, it must leaves a field with only wild ramification when it halts.
Suppose the process ends with field $\mathscr{K}$, we claim that **if $\mathscr{K}$ is contained in a cyclotomic field, then so is** K. In fact, if we denote the field obtained at step n as K_n and L_n, we can assert that,

$$K_n \text{ is contained in a cyclotomic field} \Rightarrow \text{so is } K_{n-1}$$

This is because if K_n is contained in $\mathbb{Q}(\zeta_m)$, L_n is contained in $\mathbb{Q}(\zeta_w)$, then L_nK_n is contained in $\mathbb{Q}(\zeta_{mw})$. Since $L_nK_n = L_nK_{n-1}$, we have $K_{n-1} \leq L_nK_{n-1} \leq \mathbb{Q}(\zeta_{mw})$.



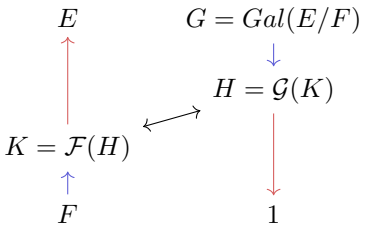
Then we can use reverse induction to prove the lemma. Then we shall presents the following algorithm for proving "contained in a cyclotomic field",

INPUT An abelian extension $K/\mathbb{Q}$.
STEP 1 Run K through the algorithm induced by Theorem 3.1.
STEP 2 STEP 1 halts with an abelian extension $\mathscr{K}/\mathbb{Q}$ which has only wild ramification.
STEP 3 Prove that $\mathscr{K}$ is contained in a cyclotomic field.
OUT Thus K is contained in a cyclotomic field.

Which finishes our first reduction.

3.1.2 General Idea: Reducing to Prime Power Cyclic Extension

Next we reduce the case into abelian extension $K/\mathbb{Q}$ **such that** $[K : \mathbb{Q}] = p^n$ **for some** p **and** n.



Recall that by abelian, we mean $[K : \mathbb{Q}]$ is finite and $Gal(K/\mathbb{Q})$ is abelian. Also recall the famous Galois fundamental theorem that establishes connection between Galois group and corresponding subfields.
E/F is a finite Galois extension, $F \leq K \leq E$ and $H \leq G$. K is the fixed field of H, denoted $K = \mathcal{F}(H)$. H is the fixing group of K, denoted $H = \mathcal{G}(K)$. $\mathcal{F}$ and $\mathcal{G}$ are inclusion-reversing bijections, meaning H descends as K moves up. And the segment with same color shares same index. E/K is always Galois, whereas K/F is Galois iff $H \lhd G$.

```
def IsGalois.intermediateFieldEquivSubgroup {F : Type u_1} [Field F] {E : Type u_2}
↪ [Field E] [Algebra F E] [FiniteDimensional F E] [IsGalois F E] :
IntermediateField F E ≃o (Subgroup (E ≃a[F] E))ᵒᵈ
```

Thus $|\ Gal(K/\mathbb{Q})\ | = [K : \mathbb{Q}]$ is finite. Therefore we can use the structure theorem of finite abelian group to break $Gal(K/\mathbb{Q})$ into product of prime power groups.

```
theorem AddCommGroup.equiv_directSum_zmod_of_finite (G : Type u) [AddCommGroup G]
↪ [Finite G] :
    ∃ (ι : Type) (x : Fintype ι) (p : ι → ℕ) (_ : ∀ (i : ι), Nat.Prime (p i))
    (e : ι → ℕ),
Nonempty (G ≃+ DirectSum ι fun (i : ι) => ZMod (p i ^ e i))
```

Then we may reconstruct K as the composition of corresponding fixed field of those prime power group. To do that, we need another property stated in fundamental Galois theorem,

Theorem 3.2. *Given finite Galois extension K/F, if $H_1,\ H_2 \leq Gal(K/F)$, then*

$$\mathcal{F}(H_1 \sqcap H_2) = \mathcal{F}(H_1) \sqcup \mathcal{F}(H_2),\ \mathcal{F}(H_1 \sqcup H_2) = \mathcal{F}(H_1) \sqcap \mathcal{F}(H_2)$$

In particular, the following algorithm to disassemble K into composition of prime power degree abelian extension of $\mathbb{Q}$ can be established,

INPUT An abelian extension K.
STEP 1 Decompose $Gal(K/\mathbb{Q})$ into $\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}}$.
STEP 2 For every $\mathbb{Z}_{p_i^{r_i}}$ (denoted as Z_i), denote $\prod_{j \neq i} Z_j$ as A_i,

1. Since $Gal(K/\mathbb{Q})$ is abelian, $A_i \lhd Gal(K/\mathbb{Q})$. (Strictly speaking, A_i is a subgroup of $Gal(K/\mathbb{Q})$ up to isomorphic)
2. According to Galois theory, $\mathcal{F}(A_i)/\mathbb{Q}$ is Galois.

STEP 3 By Theorem 3.2, $\mathcal{F}(\sqcap A_i) = \sqcup \mathcal{F}(A_i)$. $\sqcap A_i = 1$, hence $\mathcal{F}(\sqcap A_i) = K = \sqcup \mathcal{F}(A_i)$.
STEP 4 Each of $\mathcal{F}(A_i)$ is of prime power degree since $[\mathcal{F}(A_i) : \mathbb{Q}] = |Gal(K/\mathbb{Q})/A_i| = p_i^{r_i}$.
STEP 5 Each of $\mathcal{F}(A_i)$ is abelian since its Galois group is exactly $A_i = \prod_{j \neq i} \mathbb{Z}_{p_i^{r_i}}$.
OUT The decomposition $\sqcup \mathcal{F}(A_i)$.

3.1.3 General Idea: Finishing Proof

Now suppose we've got,

Theorem 3.3. *Given an abelian extension $K/\mathbb{Q}$ with $[K : \mathbb{Q}] = p^n$ for some p and n, if every prime other than p is unramified, then*

- *if $p \neq 2$, then K is contained in $\mathbb{Q}(\zeta_{p^{n+1}})$*
- *if $p = 2$, then K is contained in $\mathbb{Q}(\zeta_{2^{m+2}})$ for some m*

Then we can combine two algorithms given above and build the final algorithm towards the Kronecker-Weber theorem,

INPUT An abelian extension K.
STEP 1 Run K through the algorithm induced by Theorem 3.1, this halts with an abelian extension $\mathscr{K}$ which has only wildly ramified primes.
STEP 2 Run $\mathscr{K}$ through the decomposition algorithm, this gives $\mathscr{K} = \sqcup K_i$, where K_i are prime power degree abelian extensions.
STEP 3 For every K_i,

(a) Since $\mathscr{K}$ has no tamely ramified prime, K_i must also have no tame ramification.
(b) Suppose $[K_i : \mathbb{Q}] = p^n$, then for any prime $q \neq p$, q must be either tamely ramified or unramified.
(c) Thus by (a), the only wildly ramified prime in K_i is p.
(d) Thus by Theorem 3.3, K_i is contained in cyclotomic field.

STEP 4 Since the composite of cyclotomic fields is cyclotomic, $\mathscr{K}$ is contained in a cyclotomic field.
OUT K is contained in a cyclotomic field.

3.2 Reducing to Wildly Ramified Case

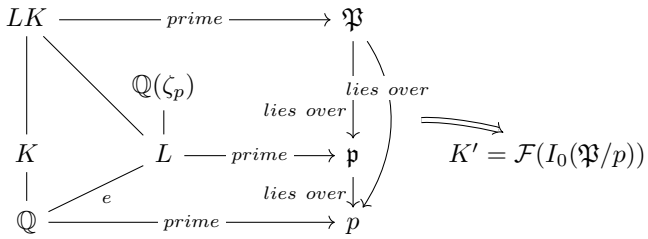
In this section we prove Theorem 3.1,

Theorem 3.1. *Suppose that $K/\mathbb{Q}$ is an abelian extension, p is tamely ramified over K. Then we can construct another **abelian** extension $K'/\mathbb{Q}$, together with a subfield L of some cyclotomic field, such that*

1. *p is unramified in K'*
2. *unramified prime in K stays unramified in K'*
3. *$LK = LK'$*

Proof. (**SKETCH**)

1. Constructing K'
   I_1 is trivial by Theorem 2.5. Then by Theorem 2.6, $I_0/I_1 = I_0 \leq (k(p))^\times = (\mathbb{Z}_p)^\times$. Thus $e \mid p-1$. Notice that $(\mathbb{Z}_p)^\times \simeq Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, then by Galois theory, $L = \mathcal{F}(I_0) \leq \mathbb{Q}(\zeta_p)$ has degree e over $\mathbb{Q}$.
   It can be proved that p is totally ramified in $\mathbb{Q}(\zeta_p)$. $e \mid p-1$ then e is relatively prime to p, and so p is tamely ramified in $\mathbb{Q}(\zeta_p)$. Hence p is totally and tamely ramified in L. Thus there is a unique prime $\mathfrak{p}$ in L that lies over p. Then take $\mathfrak{P}$ a prime of LK/L lying over $\mathfrak{p}$. So $\mathfrak{P}$ lies over p. Let $I_0' = I_0(\mathfrak{P}/p)$ and $K' = \mathcal{F}(I_0')$ the fixed field.



2. p is unramified in K' whereas unramified prime stays unramified
   L is ramified only at p, then q remains unramified in L as long as q is unramified in K and $q \neq p$. Consequently, q is unramified in the extension LK. Therefore, if q is unramified in K, it will also be unramified in $K' \leq LK'$. Additionally, p remains unramified in K' since K' is the inertial field of $\mathfrak{P}/p$.
3. $LK = LK'$
   - $[LK' : K'] \geq e$:
     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 index e, by Theorem 2.1, $e \mid [LK' : K']$, thus $[LK' : K'] \geq e$.
   - $e \geq [LK : K'] \geq [LK' : K']$:
     $[LK : K'] = |I_0'|$ according to the setup. $\mathfrak{P}$ is tamely ramified since p is tamely ramified in both L and K. By Theorem 2.6, $I_0' \leq (k(p))^\times = (\mathbb{Z}_p)^\times$, so I_0' is a cyclic group. Similarly, $Gal(LK/\mathbb{Q})$ injects into $Gal(K/\mathbb{Q}) \times Gal(L/\mathbb{Q})$ and so

I'_0 does as well.
Let $\mathfrak{p}' = \mathfrak{P} \cap K$. Then by definition, I'_0 restricted to K gives an element in the inertia group $I_0(\mathfrak{p}'/p)$ but $\mathfrak{p}'$ is conjugate to $\mathfrak{p}$ so the order of $I_0(\mathfrak{p}'|p)$ is $|I_0| = e$.
Thus I'_0 lives in the subgroup $I_0(\mathfrak{p}'|p) \times \mathrm{Gal}(L/\mathbb{Q})$, both of which are groups of order e so I'_0 has exponent e. Since it is cyclic and of exponent e, $|I'_0| \leq e$.

Thus $e \geq |I'_0| = [LK : K'] \geq [LK' : K'] \geq e$. Hence $[LK : K'] = [LK' : K']$, $LK = LK'$.

□

3.3 Reducing to Prime Power Cyclic Extension

In this section we prove Theorem 3.3,

Theorem 3.3. *Given an abelian extension $K/\mathbb{Q}$ with $[K : \mathbb{Q}] = p^n$ for some p and n, if every prime other than p is unramified, then*

- *if $p \neq 2$, then K is contained in $\mathbb{Q}(\zeta_{p^{n+1}})$*
- *if $p = 2$, then K is contained in $\mathbb{Q}(\zeta_{2^{m+2}})$ for some m*

Proof. (**SKETCH**)

1. $p \neq 2$ (p is odd):
The Galois group $Gal(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ is cyclic of order $p^n(p-1)$. Let L be the unique subextension of degree p^n. Then, $Gal(L/\mathbb{Q})$ is cyclic of order p^n.
Consider the compositum LK. Let σ be a generator of $Gal(L/\mathbb{Q})$, and let τ be a lift of σ to $Gal(LK/\mathbb{Q})$. Let F be the fixed field of $\langle\tau\rangle$. Since σ generates $Gal(L/\mathbb{Q})$, the fixed field of σ is $\mathbb{Q}$, implying $L \cap F = \mathbb{Q}$. Hence, $Gal(LK/\mathbb{Q})$ embeds into $Gal(L/\mathbb{Q}) \times Gal(K/\mathbb{Q})$, and τ has order exactly p^n.
Thus, $[LK : F] = p^n$, and since $L \cap F = \mathbb{Q}$, it follows that $LK = L$. Therefore, $K \subset L \subset \mathbb{Q}(\zeta_{p^{n+1}})$, proving the first part.
2. $p = 2$:
For $p = 2$, we reduce to the case where $K/\mathbb{Q}$ is a cyclic 2^n-extension with discriminant a power of 2. Consider $K(i)$, where $i = \sqrt{-1}$. Then $K(i)$ is unramified away from 2. Let K' be the fixed field of complex conjugation in $K(i)$. Then K' is totally real of degree 2^m with discriminant a power of 2 and is cyclic. Take $L = \mathbb{Q}(\zeta_{2^{m+2}}) \cap \mathbb{R}$, the real subfield of $\mathbb{Q}(\zeta_{2^{m+2}})$. Since K' and L are both totally real and cyclic of the same degree, $K' = L$. Finally, since $K \subset K(i) = K'(i) \subset \mathbb{Q}(\zeta_{2^{m+2}}, i)$ and the latter is cyclotomic, the proof is complete.

□

4

Discussions

In modern literature, the Kronecker-Weber theorem is usually deduced as a simple consequence of class field theory. In fact, one can first investigate the theorem in local scenario where $K_{\mathfrak{p}}$ and $\mathbb{Q}_p$ is concerned. Then global-local principle can be utilized to extend it into global situation as we presented here. Obviously class field theory offers a more elegant path towards our goal.

However, by the time this paper is written, mathlib still lacks of support of local fields and relevant concepts, making it much more difficult to start from this angle.

Through out the paper, I've listed all relevant lemmas that is already available in mathlib, and explained the difference between them and their natural language version as commonly known. One can observe easily that many things are still missing, and everything in mathlib is written in the most general form possible - more often than not, it takes complicated process to downgrade them to the version we normally encounter. This incompleteness and complexity repels many from getting into formalization with Lean. Fortunately the community is working hard to smoothen the learning curve and make formalization more accessible, an example would be the recent work in Beijing International Center for Mathematical Research, where a project trying to connect mathlib with the Stacks project is on going.

Experienced readers might find section 3.1 tautology, and some might consider viewing proofs as algorithm weird, but this level of clarity is essential during formalization, and the algorithm viewpoint greatly enhanced computablity of the theorem.

There are indeed still much to do to completely formalize Kronecker-Weber theorem. For instance, higher ramification group is still on TO-DO list in mathlib. Also, proving the halting condition of our algorithm would be challenging, let alone all the details in last two proofs. But hopefully this paper can serve as a start heading to the target.