Kummer theory and a complete proof of the Kronecker-Weber Theorems

Hurui Yao

2026/01/25

Introduction

The Kronecker–Weber theorem is a classical landmark in algebraic number theory: it states that every finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$. This theorem not only provides an explicit classification of all abelian extensions of the rationals, but also served as the historical motivation for class field theory.

The goal of this report is to present a complete, self-contained proof of the Kronecker–Weber theorem. The overall strategy is as follows:

1. **Reduce to cyclic extensions of prime power degree** – any finite abelian group decomposes into cyclic prime-power factors, and the compositum of cyclotomic fields is again cyclotomic.

2. **Reduce to a single ramified prime** – by adjoining suitable roots of unity, we can eliminate ramification at all primes except possibly one (the prime p dividing the degree).

3. **Reduce to degree p** – an inductive argument on the exponent shows that it suffices to prove the theorem for cyclic extensions of prime degree p ramified only at p.

4. **Prove the core case** – for odd p we use Kummer theory over $\mathbb{Q}(\zeta_p)$ together with Stickelberger's theorem on the class group; the case $p = 2$ is treated separately using $\mathbb{Q}(i)$ and explicit quadratic fields.

5. **Local-global approach** – we also prove the local Kronecker–Weber theorem (every finite abelian extension of $\mathbb{Q}_p$ is cyclotomic) and show how it implies the global theorem via completions, illustrating the local-global principle.

The report is organised as follows. Section 1 recalls necessary background from algebraic number theory, cyclotomic fields and Kummer theory. Section 2 carries out the three reduction steps outlined above, culminating in Proposition 2.3 (the core case). Sections 3 and 4 prove Proposition 2.3 for odd primes and for $p = 2$, respectively. Section 5 proves the local Kronecker–Weber theorem. Section 6 uses the local theorem to give an alternative proof of the global theorem, completing the argument.

1 Preliminaries

This chapter collects the fundamental concepts from algebraic number theory, cyclotomic fields, and Kummer theory that will be essential for the proof of the Kronecker–Weber theorem. Readers familiar with these topics may proceed directly to the next chapter.

1.1 Algebraic Number Theory Essentials

Definition 1.1.

(i) A complex number α is called an *algebraic number* if there exists a non-zero polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$.

(ii) α is called an *algebraic integer* if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

(iii) A field K is called a *number field* if it is a finite extension of $\mathbb{Q}$.

Theorem 1.2.

(i) The set of all algebraic numbers forms a field; the set of all algebraic integers forms a ring.

(ii) A rational number is an algebraic integer if and only if it belongs to $\mathbb{Z}$.

For a number field K, we denote its *ring of integers* by $\mathcal{O}_K$, i.e. the set of all algebraic integers in K.

1.1.1 Discriminant and integral bases

Let $K/\mathbb{Q}$ be a number field of degree $n = [K : \mathbb{Q}]$. The ring $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. A set $\{\alpha_1, \dots, \alpha_n\} \subset \mathcal{O}_K$ is called an *integral basis* if it is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

Definition 1.3. Given an integral basis $\{\alpha_1, \dots, \alpha_n\}$, the *discriminant* of K is defined as

$$d_K = \det\big(\sigma_i(\alpha_j)\big)^2,$$

where $\sigma_1, \dots, \sigma_n$ are the n distinct embeddings of K into $\mathbb{C}$. The discriminant is independent of the choice of integral basis and is a fundamental invariant of K.

1.1.2 Prime decomposition and ramification

In a number field K, $\mathcal{O}_K$ is a Dedekind domain, so every non-zero proper ideal factors uniquely into a product of prime ideals.

Theorem 1.4 (Unique factorization of ideals)**.** *Every non-zero proper ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be written uniquely as*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \qquad e_i \geq 1.$$

For a rational prime $p \in \mathbb{Z}$, consider its factorisation in $\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where the $\mathfrak{p}_i$ are distinct prime ideals. The exponent e_i is the *ramification index* of $\mathfrak{p}_i$ over p, and $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$ is the *inertia degree*. They satisfy

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

Definition 1.5. Let p be a rational prime.

- p is said to be *ramified* in K if some $e_i > 1$; otherwise it is *unramified*.
- p is *totally split* if $g = n$ and all $e_i = f_i = 1$.

1.1.3 Minkowski's theorem

A classical result of Minkowski tells us that $\mathbb{Q}$ has no non-trivial unramified extensions.

Theorem 1.6 (Minkowski)**.** *Every number field $K \neq \mathbb{Q}$ has at least one finite prime that ramifies. Equivalently, there is no non-trivial extension of $\mathbb{Q}$ that is unramified at all finite places.*

Proof. See [3]. □

This theorem will be used in the reduction steps to eliminate ramification outside a single prime.

1.2 Cyclotomic Fields

Definition 1.7. Let n be a positive integer and let ζ_n denote a primitive n-th root of unity. The field $\mathbb{Q}(\zeta_n)$ is called the n-th *cyclotomic field*.

Theorem 1.8 (Basic properties of cyclotomic fields)**.**

1. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, *where ϕ is Euler's totient function.*
2. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$*; the isomorphism sends $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ to the automorphism σ_a defined by $\sigma_a(\zeta_n) = \zeta_n^a$.*
3. $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.
4. *A rational prime p ramifies in $\mathbb{Q}(\zeta_n)$ iff $p \mid n$.*

For prime-power cyclotomic fields the structure is even more explicit.

Theorem 1.9. *Let p be an odd prime and consider $\mathbb{Q}(\zeta_{p^m})$.*

$$[\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = p^{m-1}(p-1).$$

The prime p is totally ramified: $p\mathcal{O} = (1-\zeta_{p^m})^{\phi(p^m)}$, and $1-\zeta_{p^m}$ is a uniformiser for the unique prime above p.

For $p = 2$ and $m \geq 3$, $[\mathbb{Q}(\zeta_{2^m}) : \mathbb{Q}] = 2^{m-2}$ and 2 is totally ramified as well.

1.2.1 Subfields of cyclotomic fields

The Kronecker–Weber theorem states that every finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field. The following examples illustrate how quadratic fields arise in this way.

Example 1.10.

- $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$.
- $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$.
- For an odd prime p, $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$ if $p \equiv 1 \pmod 4$, and $\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p)$ if $p \equiv 3 \pmod 4$.

1.3 Kummer Theory

1.3.1 Classical Kummer theory

Kummer theory describes extensions obtained by adjoining n-th roots, under the assumption that the base field contains the n-th roots of unity.

Theorem 1.11 (Fundamental theorem of Kummer theory)**.** *Let F be a field of characteristic not dividing n, and assume $\mu_n \subset F$ (i.e. F contains all n-th roots of unity). Then:*

1. *For every finite abelian extension E/F of exponent dividing n (i.e. $\mathrm{Gal}(E/F)$ is killed by n), there exists a finite subgroup $\Delta \subseteq F^\times/(F^\times)^n$ such that $E = F(\Delta^{1/n})$, where $\Delta^{1/n}$ denotes the field obtained by adjoining an n-th root of each element of Δ.*
2. *Conversely, for any finite subgroup $\Delta \subseteq F^\times/(F^\times)^n$, the extension $F(\Delta^{1/n})/F$ is Galois with Galois group $\mathrm{Hom}(\Delta, \mu_n)$.*
3. *There is a bijection*

   $$\{\text{finite abelian extensions of } F \text{ of exponent dividing } n\} \longleftrightarrow \{\text{finite subgroups of } F^\times/(F^\times)^n\}.$$

Proof. See [1]. □

1.3.2 Criterion for being abelian over $\mathbb{Q}$

In the proof of the Kronecker–Weber theorem we will need to decide when a Kummer extension of $\mathbb{Q}(\zeta_p)$ is actually abelian over $\mathbb{Q}$.

Lemma 1.12 (Abelianness criterion)**.** *Let p be an odd prime, $F = \mathbb{Q}(\zeta_p)$, and $L = F(\sqrt[p]{\mu})$ a Kummer extension of degree p with $\mu \in F^\times$. Then $L/\mathbb{Q}$ is abelian if and only if for every $\sigma_a \in \mathrm{Gal}(F/\mathbb{Q})$ (where $\sigma_a(\zeta_p) = \zeta_p^a$) there exists $\xi \in F^\times$ such that*

$$\sigma_a(\mu) = \xi^{\,p}\,\mu^{\,a}.$$

Proof. See [2]. □

This condition translates the global abelian requirement into a local constraint on the Kummer generator μ, and it will be used repeatedly.

2 Reduction Steps for the Global Theorem

In this chapter we reduce the proof of the Kronecker–Weber theorem to a tractable core statement. The strategy is to first decompose an arbitrary finite abelian extension into prime-power cyclic components, then eliminate ramification at all but one prime by composing with suitable cyclotomic fields, and finally reduce the problem to cyclic extensions of prime degree. The heart of the matter will be a proposition describing all cyclic extensions of degree p that are ramified only at p; this proposition will be proved in Chapters 3 and 4.

2.1 Reduction to Prime-Power Degree

Let $K/\mathbb{Q}$ be a finite abelian extension with Galois group G. Since G is a finite abelian group, it decomposes as a direct product of cyclic groups of prime power order:

$$G \cong \prod_{i=1}^{r} C_{p_i^{e_i}}.$$

By Galois theory there correspond intermediate fields K_i such that K is the compositum of the K_i and $\mathrm{Gal}(K_i/\mathbb{Q}) \cong C_{p_i^{e_i}}$.

Lemma 2.1. *If each K_i is contained in a cyclotomic field $\mathbb{Q}(\zeta_{n_i})$, then their compositum K is contained in $\mathbb{Q}(\zeta_N)$ with $N = \mathrm{lcm}(n_1, \ldots, n_r)$.*

Proof. The compositum of cyclotomic fields satisfies $\mathbb{Q}(\zeta_a)\mathbb{Q}(\zeta_b) = \mathbb{Q}(\zeta_{\mathrm{lcm}(a,b)})$. Hence

$$K \subseteq \mathbb{Q}(\zeta_{n_1}) \cdots \mathbb{Q}(\zeta_{n_r}) \subseteq \mathbb{Q}(\zeta_N). \quad \square$$

□

Thus it suffices to prove the theorem for cyclic extensions whose degree is a prime power.

2.2 Reduction to a Single Ramified Prime

Let $K/\mathbb{Q}$ be cyclic of degree p^m (with p prime). Denote by S the finite set of rational primes that ramify in K. If S contains a prime $\ell \neq p$, we can "kill" the ramification at ℓ by adjoining a primitive ℓ-th root of unity.

Lemma 2.2. *Let ℓ be an odd prime different from p. If ℓ ramifies in K, then in the compositum $K\mathbb{Q}(\zeta_\ell)$ the prime ℓ becomes unramified.*

Proof. In $\mathbb{Q}(\zeta_\ell)$ the prime ℓ is totally ramified with ramification index $\ell - 1$. In the extension $K\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_\ell)$ the ramification index at primes above ℓ divides both p^m and $\ell - 1$; because $p \neq \ell$ these numbers are coprime, hence the ramification index must be 1. Thus ℓ is unramified in $K\mathbb{Q}(\zeta_\ell)$. □

By successively adjoining ζ_ℓ for every ramified prime $\ell \neq p$ (and possibly ζ_4 for the prime 2), we obtain a finite extension

$$K' = K \cdot \prod_{\ell \in S \setminus \{p\}} \mathbb{Q}(\zeta_\ell)$$

which is still abelian over $\mathbb{Q}$ and whose ramification set is contained in $\{p\}$ (and possibly the infinite prime). Moreover, $K \subseteq K'$ and if we can show that K' lies in some cyclotomic field, then so does K.

Therefore we may assume from now on that $K/\mathbb{Q}$ is a cyclic p^m-extension ramified only at the prime p (and possibly at infinity).

2.3 Reduction to Degree p

Now we have a cyclic extension $K/\mathbb{Q}$ of degree p^m ramified only at p. We proceed by induction on m. The case $m = 1$ is exactly the statement that every cyclic extension of degree p ramified only at p is contained in $\mathbb{Q}(\zeta_{p^2})$.

Proposition 2.3 (Core case)**.** *Let p be an odd prime. If $K/\mathbb{Q}$ is a cyclic extension of degree p ramified only at p, then $K \subseteq \mathbb{Q}(\zeta_{p^2})$. For $p = 2$ the same holds with $\mathbb{Q}(\zeta_8)$ (or more generally $\mathbb{Q}(\zeta_{2^m})$ after induction).*

Assuming this proposition, we prove the inductive step. Let $K/\mathbb{Q}$ be cyclic of degree p^m ($m \geq 2$) ramified only at p. Consider the unique subfield K_0 of K with $[K : K_0] = p$ (so $[K_0 : \mathbb{Q}] = p^{m-1}$). By the induction hypothesis, $K_0 \subseteq \mathbb{Q}(\zeta_{p^m})$ after possibly enlarging the cyclotomic field (one can show that a p^{m-1}-extension ramified only at p is contained in $\mathbb{Q}(\zeta_{p^m})$; this follows from the structure of the cyclotomic tower).

Now look at the extension $K(\zeta_p)/\mathbb{Q}(\zeta_p)$. Since $\mathbb{Q}(\zeta_p)$ contains the p-th roots of unity, Kummer theory applies: there exists an element $\mu \in \mathbb{Q}(\zeta_p)^\times$ such that $K(\zeta_p) = \mathbb{Q}(\zeta_p)(\sqrt[p]{\mu})$. Using the fact that $K/\mathbb{Q}$ is abelian and ramified only at p, one shows (by an analysis similar to that in Chapter 3) that μ can be chosen so that $K(\zeta_p) \subseteq \mathbb{Q}(\zeta_p)(\sqrt[p]{1-\zeta_p}) = \mathbb{Q}(\zeta_{p^2})$. Consequently $K \subseteq \mathbb{Q}(\zeta_{p^2})\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{p^2})$, completing the induction. (The case $p = 2$ requires a separate but completely analogous treatment; the key point is that every quadratic extension ramified only at 2 is contained in $\mathbb{Q}(\zeta_8)$, and higher powers are handled by a similar induction using $\mathbb{Q}(i)$.)

2.4 Assembling the Pieces

Once Proposition 2.3 is established (which we do in Chapter 3 for odd p and in Chapter 4 for $p = 2$), the previous reductions show that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. The remaining chapters will therefore concentrate on proving Proposition 2.3.

3 Proof of Proposition 2.3 for Odd Primes

In this chapter we prove Proposition 2.3 for odd primes p. Recall that we are given a cyclic extension $K/\mathbb{Q}$ of degree p ramified only at p. We must show that $K \subseteq \mathbb{Q}(\zeta_{p^2})$.

3.1 Setup and Kummer Theory

Let $F = \mathbb{Q}(\zeta_p)$ and consider the compositum $L = KF$. Since F contains the p-th roots of unity, Kummer theory applies: there exists an element $\mu \in F^\times$ such that $L = F(\sqrt[p]{\mu})$. Moreover, we may choose μ to be an algebraic integer and assume that L/F is unramified outside p.

Remark 1. Because multiplying μ by a p-th power does not change the extension, we can clear denominators and remove p-power factors from the ideal factorization of (μ). The condition that $K/\mathbb{Q}$ is ramified only at p forces the valuation of μ at primes above p to be a multiple of p; hence we may also assume that (μ) is coprime to p. In particular, μ can be taken to be a unit in the localization of $\mathcal{O}_F$ away from p.

Denote by $\sigma_a \in G = \mathrm{Gal}(F/\mathbb{Q})$ the automorphism defined by $\sigma_a(\zeta_p) = \zeta_p^a$ for $1 \leq a \leq p-1$.

Lemma 3.1 (Abelianness criterion)**.** *The extension $L/\mathbb{Q}$ is abelian if and only if for every $\sigma_a \in G$ there exists $\xi \in F^\times$ such that*

$$\sigma_a(\mu) = \xi^{\,p}\,\mu^{\,a}.$$

Proof. This is a restatement of Lemma 1.12. □

3.2 Ideal-Theoretic Constraints

Write the principal ideal generated by μ as

$$(\mu) = \mathfrak{a}^p,$$

where $\mathfrak{a}$ is an ideal of $\mathcal{O}_F$ coprime to p. This is possible because we have arranged that the exponent of any prime ideal in (μ) is a multiple of p (otherwise L/F would be ramified at that prime, contradicting that $K/\mathbb{Q}$ is ramified only at p and that $F/\mathbb{Q}$ is unramified outside p).

3.3 The Abelian Condition on Ideal Classes

From Lemma 3.1 we have $\sigma_a(\mu) = \xi^p \mu^a$. Taking ideals and using $(\mu) = \mathfrak{a}^p$ we obtain

$$\sigma_a(\mathfrak{a})^p = (\mathfrak{a}^a)^p.$$

Since $\mathfrak{a}$ is coprime to p, unique factorisation of ideals allows us to take p-th roots:

$$\sigma_a(\mathfrak{a}) = \mathfrak{a}^a \cdot \mathfrak{b},$$

where $\mathfrak{b}$ is an ideal whose p-th power is principal. In the class group $\mathrm{Cl}(F)$ this becomes

$$\sigma_a([\mathfrak{a}]) = [\mathfrak{a}]^a.$$

3.4 Application of Stickelberger's Theorem

Recall Stickelberger's theorem:

Theorem 3.2 (Stickelberger)**.** *Let $F = \mathbb{Q}(\zeta_p)$. The Stickelberger element*

$$\theta = \sum_{a=1}^{p-1} a\sigma_a^{-1} \in \mathbb{Z}[G]$$

annihilates the class group of F: for every ideal class $c \in \mathrm{Cl}(F)$, we have $c^\theta = 1$.

Proof. See [4]. □

Now consider $c = [\mathfrak{a}] \in \mathrm{Cl}(F)$. From the previous section we have $\sigma_a(c) = c^a$ for all a. Applying the Stickelberger element:

$$c^\theta = c^{\sum a\sigma_a^{-1}} = \prod_{a=1}^{p-1} \left(\sigma_a^{-1}(c)\right)^a = \prod_{a=1}^{p-1} \left(c^{a^{-1}}\right)^a = c^{\sum_{a=1}^{p-1} 1} = c^{p-1}.$$

But Stickelberger's theorem tells us $c^\theta = 1$. Hence $c^{p-1} = 1$ in $\mathrm{Cl}(F)$.

On the other hand, from $\sigma_a(c) = c^a$ and the fact that the map $a \mapsto \sigma_a$ is an isomorphism $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$, we see that the order of c divides $a-1$ for every a not congruent to 1 modulo p. The only integer satisfying this for all such a is 1. Therefore c is the trivial ideal class.

Thus $\mathfrak{a}$ is principal: $\mathfrak{a} = (\alpha)$ for some $\alpha \in F^\times$. Then

$$\mu = \alpha^p \cdot \epsilon,$$

where ϵ is a unit in $\mathcal{O}_F^\times$.

3.5 Unit Analysis

We now have $L = F(\sqrt[p]{\alpha^p\epsilon}) = F(\sqrt[p]{\epsilon})$. The extension L/F is therefore generated by a p-th root of a unit.

Lemma 3.3. *Let $\epsilon \in \mathcal{O}_F^\times$ be a unit. If $F(\sqrt[p]{\epsilon})/\mathbb{Q}$ is abelian, then ϵ is congruent to a p-th power modulo $(1-\zeta_p)^p$.*

Sketch. The condition from Lemma 3.1 imposes restrictions on the Galois conjugates of ϵ. Using the structure of the unit group $\mathcal{O}_F^\times \cong \mu_{p-1} \times U^{(1)}$, where $U^{(1)} = 1+(1-\zeta_p)\mathcal{O}_F$ is the group of principal units, and the fact that $U^{(1)}/U^{(1)p}$ is an $\mathbb{F}_p$-vector space of dimension $(p-1)/2$, one shows that the abelianness forces ϵ to lie in the subgroup generated by the cyclotomic units $(1-\zeta_p^a)/(1-\zeta_p)$ up to a p-th power. A standard computation then gives $\epsilon \equiv \zeta_p^k \pmod{(1-\zeta_p)^p}$ for some integer k. □

Using the lemma, we find that $\epsilon = \eta^p \cdot \zeta_p^k$ for some $\eta \in F^\times$ and some integer k. Absorbing η^p into the p-th root, we obtain

$$L = F(\sqrt[p]{\zeta_p^k}) = F(\sqrt[p]{\zeta_p^k}).$$

But $\sqrt[p]{\zeta_p^k}$ is a root of unity of order p^2; indeed ζ_{p^2} satisfies $(\zeta_{p^2})^p = \zeta_p$. Hence $F(\sqrt[p]{\zeta_p^k}) \subseteq \mathbb{Q}(\zeta_{p^2})$.

3.6 Conclusion

We have shown that $L \subseteq \mathbb{Q}(\zeta_{p^2})$. Since $K \subseteq L$, it follows that $K \subseteq \mathbb{Q}(\zeta_{p^2})$, completing the proof of Proposition 2.3 for odd primes p.

4 The Case $p = 2$

The prime 2 requires special treatment because $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ does not contain the required roots of unity for Kummer theory. Nevertheless, a completely analogous argument works with $\mathbb{Q}(i)$ playing the role of the base field.

4.1 Quadratic Extensions

Proposition 4.1. *The maximal real abelian extension of exponent* 2 *unramified outside* 2 *is cyclic: it is the subfield* $\mathbb{Q}(\sqrt{2})$ *of* $\mathbb{Q}(\zeta_8)$*. Moreover, every quadratic extension of* $\mathbb{Q}$ *ramified only at* 2 *is contained in* $\mathbb{Q}(\zeta_8)$*.*

Proof. The only quadratic extensions of $\mathbb{Q}$ unramified outside 2 are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, and $\mathbb{Q}(\sqrt{2})$ (see e.g. [3]). All three are contained in $\mathbb{Q}(\zeta_8)$:

$$\mathbb{Q}(i) = \mathbb{Q}(\zeta_4) \subset \mathbb{Q}(\zeta_8), \quad \mathbb{Q}(\sqrt{-2}) \subset \mathbb{Q}(\zeta_8), \quad \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8).$$

□

4.2 Higher Powers of 2

Now let $K/\mathbb{Q}$ be a cyclic extension of degree 2^m ($m \geq 2$) ramified only at 2. We proceed by induction on m.

Lemma 4.2. *If every cyclic extension of degree* 2^{m-1} *ramified only at* 2 *is contained in some* $\mathbb{Q}(\zeta_{2^N})$*, then the same holds for degree* 2^m*.*

Sketch. Let $K/\mathbb{Q}$ be cyclic of degree 2^m. Consider the extension $K(i)/\mathbb{Q}(i)$. Since $\mathbb{Q}(i)$ contains the 4-th roots of unity, we are in a Kummer situation for exponent 2. Write $K(i) = \mathbb{Q}(i)(\sqrt{\mu})$ with $\mu \in \mathbb{Q}(i)^\times$. An analysis similar to the odd prime case (but simpler because we are dealing with square roots) shows that μ must be, up to squares, a unit. The unit group of $\mathbb{Q}(i)$ consists of roots of unity and powers of $1 + i$. Examining the possibilities shows that $K(i) \subseteq \mathbb{Q}(i)(\sqrt{1+i}) = \mathbb{Q}(\zeta_8)$. If K is totally real, one can argue directly with the maximal real subfield of $\mathbb{Q}(\zeta_{2^{m+2}})$ as in [4]. The key point is that the composition of K with this real cyclotomic field cannot contain more than the allowed number of quadratic subfields, forcing K to coincide with the cyclotomic subfield. □

4.3 Completing the 2-adic Case

By induction starting from Proposition 4.1, we conclude that every cyclic 2-power extension of $\mathbb{Q}$ ramified only at 2 is contained in some $\mathbb{Q}(\zeta_{2^N})$. This completes the proof of Proposition 2.3 for $p = 2$.

5 Local Kronecker–Weber Theorem

In this chapter we prove the local analogue of the Kronecker–Weber theorem. The local theorem describes all finite abelian extensions of the field of p-adic numbers $\mathbb{Q}_p$. It states that every such extension is contained in a cyclotomic extension $\mathbb{Q}_p(\zeta_n)$. This result is not only interesting in its own right, but also provides an alternative approach to the global theorem via completions (as sketched in Chapter 6).

5.1 Local Fields and Ramification

Let p be a rational prime. Denote by $\mathbb{Q}_p$ the field of p-adic numbers, by $\mathbb{Z}_p$ its ring of integers, and by $\mathbb{F}_p$ its residue field. For a finite extension $L/\mathbb{Q}_p$ we write:

- $\mathcal{O}_L$: the ring of integers,
- π_L: a uniformizer,
- v_L: the normalized valuation with $v_L(\pi_L) = 1$,
- $e(L/\mathbb{Q}_p) = v_L(p)$: the ramification index,
- $f(L/\mathbb{Q}_p) = [\mathcal{O}_L/\pi_L\mathcal{O}_L : \mathbb{F}_p]$: the inertia degree.

We recall the structure of the unit groups:

$$\mathcal{O}_L^\times \cong \mu(L) \times U_L^{(1)},$$

where $\mu(L)$ is the group of roots of unity in L (of order coprime to p) and $U_L^{(1)} = 1+\pi_L\mathcal{O}_L$ is the group of principal units. The quotients $U_L^{(n)}/U_L^{(n+1)}$ are isomorphic to the additive group of the residue field.

5.2 Cyclotomic Extensions of $\mathbb{Q}_p$

Let n be a positive integer. The field $\mathbb{Q}_p(\zeta_n)$ is obtained by adjoining a primitive n-th root of unity to $\mathbb{Q}_p$. Its structure depends on the relation between n and p.

Lemma 5.1. *Let N be a positive integer.*

1. *If $p \nmid N$, then $\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p$ is unramified of degree equal to the order of p modulo N. The residue field extension is generated by the image of ζ_N.*
2. *If $N = p^m$, then $\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p$ is totally ramified of degree $\phi(p^m) = p^{m-1}(p-1)$. A uniformizer is $1 - \zeta_{p^m}$.*
3. *In general, $\mathbb{Q}_p(\zeta_N)$ is the composition of the unramified part (for the prime-to-p part) and the totally ramified part (for the p-power part).*

5.3 Reduction to Prime-Power Degree

As in the global case, any finite abelian extension of $\mathbb{Q}_p$ is a composition of cyclic extensions of prime power degree. Therefore it suffices to prove the theorem for cyclic extensions of degree ℓ^r where ℓ is a prime (possibly equal to p).

5.4 The Tame Case: $\ell \neq p$

If $\ell \neq p$, then a cyclic extension $K/\mathbb{Q}_p$ of degree ℓ^r is necessarily tamely ramified. By local class field theory (or by elementary arguments using Hensel's lemma), such an extension is obtained by adjoining an unramified extension followed by a tame ramified extension.

Proposition 5.2. *Let $\ell \neq p$. Every cyclic extension of $\mathbb{Q}_p$ of degree ℓ^r is contained in $\mathbb{Q}_p(\zeta_N)$ for some N with $p \nmid N$.*

Proof. Write K as a tower $K \supset K_0 \supset \mathbb{Q}_p$ where $K_0/\mathbb{Q}_p$ is the maximal unramified subextension. Then $[K_0 : \mathbb{Q}_p]$ divides ℓ^r and is coprime to p; hence K_0 is obtained by adjoining roots of unity of order coprime to p. Indeed, the residue field extension is cyclic, generated by a primitive $(p^f - 1)$-th root of unity. By Hensel's lemma, such a root of unity lifts to $\mathbb{Q}_p$. Thus $K_0 \subseteq \mathbb{Q}_p(\zeta_{p^f-1})$.

The remaining part K/K_0 is totally tamely ramified of degree ℓ^s. By the structure of tame ramification, $K = K_0(\sqrt[\ell^s]{\pi_{K_0}})$ for some uniformizer π_{K_0}. Since K_0 contains all ℓ^s-th roots of unity (because the residue characteristic is different from ℓ), this extension is actually contained in $K_0(\zeta_{\ell^s})$. A more precise argument using the classification of tamely ramified extensions shows that $K \subseteq \mathbb{Q}_p(\zeta_M)$ for some M divisible only by primes different from p. □

5.5 The Wild Case: $\ell = p$

Now let $K/\mathbb{Q}_p$ be a cyclic extension of degree p^m. The prime p is wildly ramified in such extensions, so we need a more delicate analysis using Kummer theory after adjoining ζ_p.

5.5.1 Reduction to degree p

As in the global case, we proceed by induction on m. The base case $m = 1$ is the crucial step.

Proposition 5.3. *Let $K/\mathbb{Q}_p$ be a cyclic extension of degree p. Then $K \subseteq \mathbb{Q}_p(\zeta_{p^2})$.*

Assuming this proposition, we can climb the p-power tower: if $K/\mathbb{Q}_p$ is cyclic of degree p^m ($m \geq 2$), let K_0 be the subfield of degree p^{m-1}. By the induction hypothesis, $K_0 \subseteq \mathbb{Q}_p(\zeta_{p^m})$. Then consider $K(\zeta_p)/\mathbb{Q}_p(\zeta_p)$. Since $\mathbb{Q}_p(\zeta_p)$ contains the p-th roots of unity, Kummer theory applies: there exists $\mu \in \mathbb{Q}_p(\zeta_p)^\times$ such that $K(\zeta_p) = \mathbb{Q}_p(\zeta_p)(\sqrt[p]{\mu})$. Using the same techniques as in the proof of Proposition 5.3 (valuation analysis, unit group structure, and the abelian condition), we show that μ can be taken to be a p-th power of an element in $\mathbb{Q}_p(\zeta_{p^2})$, hence $K \subseteq \mathbb{Q}_p(\zeta_{p^2})$. The details are essentially identical to those in Chapter 3, adapted to the local setting.

5.5.2 Proof of Proposition 5.3

Let $F = \mathbb{Q}_p(\zeta_p)$ and let $L = KF$. By Kummer theory, $L = F(\sqrt[p]{\mu})$ for some $\mu \in F^\times$. We may assume $\mu \in \mathcal{O}_F^\times$ after multiplying by a suitable p-th power (since valuations that are multiples of p can be absorbed into the p-th root).

Let $\pi = 1 - \zeta_p$; it is a uniformizer of F. Write $\mu = \pi^r u$ with $u \in \mathcal{O}_F^\times$. The extension L/F is unramified outside p (because $K/\mathbb{Q}_p$ is ramified only at p), so the valuation r must be divisible by p. Hence $\mu = (\pi^{r/p})^p u$. Replacing μ by u, we may assume $\mu \in \mathcal{O}_F^\times$.

Now we use the abelian condition: since $L/\mathbb{Q}_p$ is abelian, for every $\sigma \in \mathrm{Gal}(F/\mathbb{Q}_p)$ there exists $\xi \in F^\times$ such that $\sigma(\mu) = \xi^p \mu^a$, where a is determined by $\sigma(\zeta_p) = \zeta_p^a$. Taking valuations and using that μ is a unit, we obtain $\sigma(u) \equiv u^a \pmod{p\text{-th powers}}$ in a suitable sense. This translates into a condition on the image of u in the unit group modulo p-th powers.

The unit group $\mathcal{O}_F^\times$ has a well-known structure:

$$\mathcal{O}_F^\times \cong \mu(F) \times U_F^{(1)},$$

where $\mu(F)$ is the group of roots of unity (of order $p-1$) and $U_F^{(1)}$ is the group of principal units. Moreover, $U_F^{(1)}/U_F^{(1)p}$ is an $\mathbb{F}_p$-vector space of dimension $[F:\mathbb{Q}_p] = p-1$. A detailed analysis using the expansion of units as series in π shows that the condition $\sigma(u) \equiv u^a \pmod{U_F^{(1)p}}$ forces u to lie in the subgroup generated by $1-\zeta_p$ and roots of unity. Consequently, u is, up to a p-th power, a power of $1-\zeta_p$ times a root of unity.

Therefore μ can be chosen to be a root of unity times a power of $1-\zeta_p$. Adjoining a p-th root of such an element yields a subfield of $\mathbb{Q}_p(\zeta_{p^2})$, because $\sqrt[p]{1-\zeta_p}$ is a primitive p^2-th root of unity (up to a factor). More precisely, if ζ_{p^2} satisfies $\zeta_{p^2}^p = \zeta_p$, then

$$1-\zeta_p = (1-\zeta_{p^2})(1+\zeta_{p^2}+\cdots+\zeta_{p^2}^{p-1}),$$

and the second factor is a unit, so $\mathbb{Q}_p(\sqrt[p]{1-\zeta_p}) = \mathbb{Q}_p(\zeta_{p^2})$. This completes the proof of Proposition 5.3.

5.6 Conclusion of the Local Theorem

Combining the tame case ($\ell \neq p$) and the wild case ($\ell = p$), we have shown that every cyclic prime-power extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension. Since any finite abelian extension is a compositum of such, the local Kronecker–Weber theorem follows.

Theorem 5.4 (Local Kronecker–Weber)**.** *Every finite abelian extension of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\zeta_n)$ for some n.*

6 From Local to Global: Completing the Proof

With the local Kronecker–Weber theorem established in Chapter 5 and the core Proposition 2.3 proved in Chapters 3–4, we are now in a position to assemble the complete proof of the global theorem. This chapter demonstrates how the local theorem alone suffices to deduce the global result, providing an elegant example of the local-global principle in number theory.

6.1 Proof Strategy

Let $K/\mathbb{Q}$ be a finite abelian extension. The strategy proceeds as follows:

1. For each rational prime p that ramifies in K, choose a prime $\mathfrak{p} \mid p$ in K and consider the completion $K_\mathfrak{p}/\mathbb{Q}_p$.

2. By the local Kronecker–Weber theorem (Chapter 5), there exists an integer $m_p \geq 1$ such that $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{m_p})$.

3. Let $e_p = v_p(m_p)$ be the p-adic valuation of m_p, and define

$$n = \prod_{p \text{ ramifies in } K} p^{e_p}.$$

   (The product is finite because only finitely many primes ramify in K.)

4. Consider the compositum $L = K(\zeta_n)$. We shall prove that $L = \mathbb{Q}(\zeta_n)$, which immediately implies $K \subseteq \mathbb{Q}(\zeta_n)$.

6.2 The Key Inclusion

For each ramified prime p, fix a prime $\mathfrak{p} \mid p$ in K and a prime $\mathfrak{P} \mid \mathfrak{p}$ in L. Consider the completion $L_{\mathfrak{P}}/\mathbb{Q}_p$.

Lemma 6.1. *With the notation above, we have $L_{\mathfrak{P}} = \mathbb{Q}_p(\zeta_n)$.*

Proof. Let F be the maximal unramified subextension of $L_{\mathfrak{P}}/\mathbb{Q}_p$ (i.e., the union of all finite unramified extensions of $\mathbb{Q}_p$ contained in $L_{\mathfrak{P}}$). Then $L_{\mathfrak{P}}/F$ is totally ramified, and $\mathrm{Gal}(L_{\mathfrak{P}}/F)$ is isomorphic to the inertia group at $\mathfrak{P}$.

Observe that for any divisor $d \mid n$ with $p \nmid d$, the extension $\mathbb{Q}_p(\zeta_d)/\mathbb{Q}_p$ is unramified by Lemma 5.1. Since all such ζ_d lie in $\mathbb{Q}_p(\zeta_n) \subseteq L_{\mathfrak{P}}$, we have $\mathbb{Q}_p(\zeta_d) \subseteq F$. Consequently, F contains ζ_d for all $d \mid n$ coprime to p.

Now consider the element $\zeta_{p^{e_p}}$. We claim that $\zeta_{p^{e_p}} \in L_{\mathfrak{P}}$. Indeed, from the local theorem we have $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{m_p})$. Since $m_p = p^{e_p} \cdot m'$ with $p \nmid m'$, we have

$$\mathbb{Q}_p(\zeta_{m_p}) = \mathbb{Q}_p(\zeta_{p^{e_p}})\,\mathbb{Q}_p(\zeta_{m'}).$$

The factor $\mathbb{Q}_p(\zeta_{m'})$ is unramified over $\mathbb{Q}_p$, hence contained in F. Thus

$$K_{\mathfrak{p}} \subseteq F(\zeta_{p^{e_p}}).$$

But $L_{\mathfrak{P}} = K_{\mathfrak{p}}(\zeta_n) = K_{\mathfrak{p}}(\zeta_{p^{e_p}}, \zeta_{m'})$ where m' is the part of n coprime to p. Since $\zeta_{m'} \in F$, we obtain

$$L_{\mathfrak{P}} \subseteq F(\zeta_{p^{e_p}}).$$

Conversely, $F(\zeta_{p^{e_p}}) \subseteq L_{\mathfrak{P}}$ because both F (as a subfield of $L_{\mathfrak{P}}$) and $\zeta_{p^{e_p}}$ (as an element of $\mathbb{Q}_p(\zeta_n) \subseteq L_{\mathfrak{P}}$) are contained in $L_{\mathfrak{P}}$. Therefore

$$L_{\mathfrak{P}} = F(\zeta_{p^{e_p}}).$$

Finally, note that $F(\zeta_{p^{e_p}}) = \mathbb{Q}_p(\zeta_n)$. Indeed, $\mathbb{Q}_p(\zeta_n)$ is the compositum of the unramified extension $\mathbb{Q}_p(\zeta_{m'})$ (which lies in F) and the totally ramified extension $\mathbb{Q}_p(\zeta_{p^{e_p}})$. This completes the proof. □

6.3 Conclusion of the Global Theorem

We have shown that for every ramified prime p and every prime $\mathfrak{P} \mid p$ in L, the completion $L_{\mathfrak{P}}$ equals $\mathbb{Q}_p(\zeta_n)$. In particular, the local degrees $[L_{\mathfrak{P}} : \mathbb{Q}_p]$ are the same for all primes above p, and they equal $[\mathbb{Q}_p(\zeta_n) : \mathbb{Q}_p]$.

Now consider the global extension $L/\mathbb{Q}$. By construction, L is Galois (in fact abelian) because it is the compositum of two abelian extensions. We claim that $L = \mathbb{Q}(\zeta_n)$. If not, then L properly contains $\mathbb{Q}(\zeta_n)$. Let σ be a non-trivial element of $\mathrm{Gal}(L/\mathbb{Q}(\zeta_n))$. By the Chebotarev density theorem (or a simpler argument using the existence of primes with prescribed Frobenius elements), there exists a prime p (unramified in L) such that the Frobenius element Frob_p corresponds to σ. But then the completion at a prime above p would have degree strictly larger than $[\mathbb{Q}_p(\zeta_n) : \mathbb{Q}_p]$, contradicting Lemma 6.1 which holds for all primes (including those unramified in K, for which the argument remains valid after noting that the product defining n includes only ramified primes, but the equality $L_{\mathfrak{P}} = \mathbb{Q}_p(\zeta_n)$ still holds because ζ_n is contained in L).

A more elementary argument avoiding Chebotarev uses Minkowski's theorem: the discriminant of L would be divisible by a prime not dividing the discriminant of $\mathbb{Q}(\zeta_n)$ if

$L \neq \mathbb{Q}(\zeta_n)$, leading to a contradiction with the fact that ramification in L can only occur at primes dividing n (since both K and $\mathbb{Q}(\zeta_n)$ are ramified only at primes dividing n). We omit the technical details, which can be found in standard references [3, 4].

Thus $L = \mathbb{Q}(\zeta_n)$, and consequently $K \subseteq \mathbb{Q}(\zeta_n)$. This completes the proof of the global Kronecker–Weber theorem.

Theorem 6.2 (Kronecker–Weber)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$ for some positive integer n.*

Remark 2. The proof presented in this chapter shows how the local theorem (which is conceptually simpler and can be proved with elementary methods as in Chapter 5) implies the global theorem via completion arguments. This local-global approach is a recurring theme in modern number theory and finds its fullest expression in class field theory.

Remark 3. The conductor of an abelian extension $K/\mathbb{Q}$ is the smallest n such that $K \subseteq \mathbb{Q}(\zeta_n)$. It is an important invariant that encodes arithmetic information about K; for example, the conductor of a quadratic field $\mathbb{Q}(\sqrt{d})$ is $|d|$ if $d \equiv 1 \pmod 4$ and $4|d|$ otherwise.

References

[1] Lang, S. (1994). *Algebraic Number Theory*. Springer. Chapter IV, Section 3.

[2] Lemmermeyer, F. (2005). Kronecker–Weber via Stickelberger. *Journal de Théorie des Nombres de Bordeaux*, 7(2), 555–558.

[3] Neukirch, J. (1999). *Algebraic Number Theory*. Springer. Section III.2.

[4] Washington, L. C. (1997). *Introduction to Cyclotomic Fields*, 2nd ed. Springer. Chapter 6.