

# *A Complete Proof of the Kronecker-Weber Theorems*

Hurui Yao

*School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, Shenzhen,  
China*

*123090739@link.cuhk.edu.cn*

**Abstract.** The Kronecker-Weber theorem states that every finite abelian extension of the rational numbers is contained in some field generated by roots of unity. This paper presents a complete and self-contained proof of the theorem using the local-global principle. The proof proceeds in two main stages. First, the local analogue is established: for every prime  $p$ , any finite abelian extension of the  $p$ -adic numbers is shown to lie in a cyclotomic extension of  $\mathbb{Q}_p$ . Second, the global theorem is deduced from its local counterpart. Given a finite abelian extension  $K$  of  $\mathbb{Q}$ , completions at all ramified primes are compared with field generated by roots of unitys, and an integer  $n$  is constructed such that  $K(\zeta_n)$  has the same completions as  $\mathbb{Q}(\zeta_n)$ . The Chebotarev density theorem then forces equality of the global fields, yielding  $K \subseteq \mathbb{Q}(\zeta_n)$ . This approach highlights the local-global philosophy that underpins modern class field theory.

**Keywords:** Kronecker-Weber theorem, Local-Global principle, Chebotarev density theorem

## 1. Introduction

The Kronecker–Weber theorem (hereafter abbreviated as K–W) asserts that any finite-degree abelian extension of  $\mathbb{Q}$  appears as a subfield of some field generated by roots of unity  $\mathbb{Q}(\zeta_n)$  [1]. This theorem not only gives an explicit description of all abelian extensions of the rational numbers but also historically motivated the development of class field theory.

The purpose of this paper is to present a complete, self-contained proof of the K–W theorem using the local–global principle. The overall plan is as follows:

1. **Local K–W theorem.** We first prove the  $p$ -adic analogue: any finite abelian extension of  $\mathbb{Q}_p$  lies inside a cyclotomic extension  $\mathbb{Q}_p(\zeta_n)$ . The proof distinguishes tame and wild ramification and employs Kummer theory together with a detailed analysis of the unit structure.

2. **Global deduction.** Given a finite abelian extension  $K/\mathbb{Q}$ , we consider its completions  $K_p/\mathbb{Q}_p$  at all primes  $p$ . The local theorem supplies integers  $m_p$  with  $K_p \subseteq \mathbb{Q}_p(\zeta_{m_p})$ . These local data are then combined to produce a single integer  $N$  such that  $K \subseteq \mathbb{Q}(\zeta_N)$ . The main tool is the Chebotarev density theorem (or, alternatively, an elementary discriminant argument), which forces  $K(\zeta_N) = \mathbb{Q}(\zeta_N)$ .

This approach avoids the classical reduction using Stickelberger's theorem and instead offers a more uniform argument based on completions, thereby highlighting the local–global principle that

permeates modern number theory.

For readers unfamiliar with algebraic number theory[1], will provide sufficient background knowledge.

**Remark 1.** *The local–global idea is pervasive in arithmetic geometry: to understand a global object one studies its localisations (e.g., completions at all primes) and then glues the local information together. The K–W theorem provides a perfect illustration of this philosophy.*

## 2. The local K–W theorem

In this chapter we prove the local analogue of the K–W theorem, which describes all finite abelian extensions of  $\mathbb{Q}_p$ . This result will serve as the foundation for the global deduction in Section 3.

### 2.1. Cyclotomic extensions of $\mathbb{Q}_p$

For  $n \in \mathbb{N}^+$  and a prime  $p$ , write  $n = p^m n'$  with  $p \nmid n'$ . Then the following standard facts hold:

- $\mathbb{Q}_p(\zeta_{n'})/\mathbb{Q}_p$  is unramified of degree equal to the multiplicative order of  $p$  modulo  $n'$  [2];
- $\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p$  is totally ramified of degree  $\phi(p^m) = p^{m-1}(p-1)$ , and  $1 - \zeta_{p^m}$  is a uniformiser [2];
- $\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{p^m})\mathbb{Q}_p(\zeta_{n'})$ , and the two subextensions are linearly disjoint [2].

### 2.2. Reduction to cyclic extensions with prime power

Consider a finite abelian extension  $E/\mathbb{Q}_p$ . Its Galois group, being finite abelian, splits into a direct product of cyclic groups each of prime-power order. Hence, by Galois theory,  $E$  is the compositum of cyclic extensions whose degrees are prime powers. Since any compositum of cyclotomic extensions is again cyclotomic — because  $\mathbb{Q}_p(\zeta_a)\mathbb{Q}_p(\zeta_b) = \mathbb{Q}_p(\zeta_{\text{lcm}(a,b)})$  — the core of the argument lies in proving the local theorem for cyclic extensions of degree  $\ell^r$ , where  $\ell$  is a prime (possibly  $\ell = p$ ).

We therefore fix a prime  $\ell$  and a cyclic extension  $K/\mathbb{Q}_p$  of degree  $\ell^r$ , and then distinguish two situations: the tame case ( $\ell \neq p$ ) and the wild case ( $\ell = p$ ).

### 2.3. The tame case: $\ell \neq p$

Consider the case where  $\ell \neq p$ . Here ramification index  $e(K/\mathbb{Q}_p)$  divides  $\ell^r$ , implying it is coprime to  $p$ . Hence the extension  $K/\mathbb{Q}_p$  is tamely ramified.

**Proposition 2.** *If  $\ell \neq p$  and  $K/\mathbb{Q}_p$  is a cyclic extension of degree  $\ell^r$ , then  $K \subseteq \mathbb{Q}_p(\zeta_N)$  for some  $N$  with  $p \nmid N$  [2].*

Instead of giving a proof, an example is showed here to show the insight of the proof.

Let  $p = 3$  and  $\ell = 2$  (so  $\ell \neq p$ ). Consider

$$K = \mathbb{Q}_3(\sqrt{2}), \quad [K : \mathbb{Q}_3] = 2.$$

Since  $v_3(2) = 0$ , the extension has ramification index  $e = 1$ , hence tamely ramified.

**Goal:** Find an integer  $N$  with  $p \nmid N$  such that  $K \subseteq \mathbb{Q}_3(\zeta_N)$ .

**Claim:**  $N = 8$  works.

**Verification by direct computation:**

$$\zeta_8 = e^{2\pi i/8},$$

$$\zeta_8 + \zeta_8^{-1} = 2\cos \frac{2\pi}{8} = 2\cos \frac{\pi}{4} = \sqrt{2}.$$

Algebraically,  $(\zeta_8 + \zeta_8^{-1})^2 = \zeta_8^2 + 2 + \zeta_8^{-2} = i + 2 - i = 2$ , so  $\zeta_8 + \zeta_8^{-1} = \pm\sqrt{2}$ ; choosing the appropriate primitive root gives  $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$ . Hence  $\sqrt{2} \in \mathbb{Q}_3(\zeta_8)$ , and therefore  $K = \mathbb{Q}_3(\sqrt{2}) \subseteq \mathbb{Q}_3(\zeta_8)$ . Moreover  $3 \nmid 8$ , satisfying  $p \nmid N$ .

The example illustrates the key ideas of the tame case proof:

3. **Add  $\ell$ -th roots of unity if needed:** Here  $\ell = 2$  and  $\zeta_2 = -1$  already lies in  $\mathbb{Q}_3$ , so the base field remains  $\mathbb{Q}_3$ . In general one works over  $F = \mathbb{Q}_p(\zeta_\ell)$ , which is still tamely ramified over  $\mathbb{Q}_p$  because  $\ell \neq p$ .

4. **Use Kummer theory:** For a cyclic  $\ell$ -power extension  $K/\mathbb{Q}_p$ , after adjoining  $\zeta_\ell$  (if necessary) we have  $K(\zeta_\ell) = F(\sqrt[\ell]{a})$  for some  $a \in F^\times$  [2]. In our example  $a = 2$  and  $K = \mathbb{Q}_3(\sqrt{2})$ .

5. **Express  $a$  as a cyclotomic unit (up to  $\ell$ -th powers):** The key is to show that  $a$  can be chosen so that  $\sqrt[\ell]{a}$  lies in some  $\mathbb{Q}_p(\zeta_N)$  with  $p \nmid N$ . Here  $2 = (\zeta_8 + \zeta_8^{-1})^2$ , so  $\sqrt{2} \in \mathbb{Q}_3(\zeta_8)$ . In general, one uses the structure of the unit group of  $F$  and the Galois action to prove that  $a$  is congruent to  $\zeta_N^m(1 - \zeta_N)^s$  modulo  $\ell$ -th powers, which forces  $\sqrt[\ell]{a}$  to belong to a field generated by roots of unity.

6. **Why  $p \nmid N$  matters:** When  $p \nmid N$ , the extension  $\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p$  is unramified (or at most tamely ramified), matching the ramification behaviour of  $K$ . This choice avoids introducing wild ramification, which would be inconsistent with the assumption  $\ell \neq p$ .

Thus the concrete computation for  $p = 3$ ,  $\ell = 2$ ,  $K = \mathbb{Q}_3(\sqrt{2})$  and  $N = 8$  perfectly mirrors the logical steps of the general proof.

**Remark 3.** The key point in the tame case is that the ramification index is coprime to the residue characteristic, which allows us to use Kummer theory after enlarging the base field to contain the necessary roots of unity. This is a typical application of the structure of tamely ramified extensions.

## 2.4. The wild case: $\ell = P$

Now assume  $K/\mathbb{Q}_p$  is a cyclic extension of degree  $p^m$ . The proof proceeds by induction on  $m$ , showing that  $K \subseteq \mathbb{Q}_p(\zeta_{p^{m+1}})$  (or some suitable field generated by roots of unity). The base case  $m = 1$  is the most subtle.

### 2.4.1. Reduction to degree $P$

Assume the induction hypothesis:

$$\forall \text{ cyclic } L/\mathbb{Q}_p \text{ with } [L : \mathbb{Q}_p] = p^{m-1}, \quad L \subseteq \mathbb{Q}_p(\zeta_{p^m}).$$

Let  $K/\mathbb{Q}_p$  be cyclic with  $[K : \mathbb{Q}_p] = p^m$  and let  $K_0$  be the unique subfield such that  $[K : K_0] = p$  (hence  $[K_0 : \mathbb{Q}_p] = p^{m-1}$ ). By the hypothesis,

$$K_0 \subseteq \mathbb{Q}_p(\zeta_{p^m}). \quad (1)$$

Consider the extension  $K(\zeta_p)/\mathbb{Q}_p(\zeta_p)$ . Because  $\mathbb{Q}_p(\zeta_p)$  contains a primitive  $p$ th root of unity, Kummer theory applies. We have

$$[K(\zeta_p) : \mathbb{Q}_p(\zeta_p)] \mid p, \quad (2)$$

and since  $[\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p] = p - 1$  is coprime to  $p$ , it follows that

$$K \cap \mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p. \quad (3)$$

Consequently,

$$[K(\zeta_p) : \mathbb{Q}_p(\zeta_p)] = p, \quad (4)$$

so  $K(\zeta_p)/\mathbb{Q}_p(\zeta_p)$  is a cyclic extension of degree  $p$ . If we can prove that every such cyclic extension of degree  $p$  lies inside  $\mathbb{Q}_p(\zeta_{p^2})$ , then

$$K(\zeta_p) \subseteq \mathbb{Q}_p(\zeta_{p^2}) \Rightarrow K \subseteq \mathbb{Q}_p(\zeta_{p^2}), \quad (5)$$

which settles the base case. For the induction step, a stronger statement is needed; this is provided by the detailed analysis of the degree- $p$  case below.

#### 2.4.2. Base case: degree $P$

**Proposition 4.** *Let  $K/\mathbb{Q}_p$  be a cyclic extension of degree  $p$ . Then  $K \subseteq \mathbb{Q}_p(\zeta_{p^2})$ .*

*Proof.* Set  $E = \mathbb{Q}_p(\zeta_p)$  and  $M = KE$ . Then  $M/E$  is a Kummer extension of degree  $p$ , so there exists  $\alpha \in E^\times$  with  $M = E(\sqrt[p]{\alpha})$ . Multiplying  $\alpha$  by a  $p$ th power does not change  $M$ , so we may assume  $\alpha$  is a unit in  $\mathcal{O}_E^\times$ . Indeed, write  $\alpha = \varpi^r u$  with  $\varpi = 1 - \zeta_p$  and  $u \in \mathcal{O}_E^\times$ . If  $p \nmid r$ , then  $E(\sqrt[p]{\alpha})/E$  would have ramification index  $p$ , forcing the compositum  $M/\mathbb{Q}_p$  to have ramification index  $p(p-1)$ ; but a degree- $p$  extension of  $\mathbb{Q}_p$  is necessarily totally ramified with index  $p$ , so  $r$  must be a multiple of  $p$ . Hence we may take  $\alpha$  to be a unit.

Now examine the action of the Galois group  $\Gamma = \text{Gal}(E/\mathbb{Q}_p)$ . For each  $a \in (\mathbb{Z}/p\mathbb{Z})^\times$  we have an automorphism  $\tau_a$  defined by  $\tau_a(\zeta_p) = \zeta_p^a$ . Because  $M/\mathbb{Q}_p$  is abelian, the condition that  $M/\mathbb{Q}_p$  is Galois translates into the following Kummer condition (valid also in the local setting): for every  $\tau_a$  there exists  $\xi \in E^\times$  such that

$$\tau_a(\alpha) = \xi^p \alpha^a. \quad (6)$$

Since  $\alpha$  is a unit, we analyse its image in  $\mathcal{O}_E^\times$ . A standard decomposition in [2] gives

$$\mathcal{O}_E^\times \cong \mu_{p-1} \times U_E^{(1)}, \quad (7)$$

where  $\mu_{p-1}$  denotes the  $(p-1)$ -st roots of unity (Teichmüller lifts) and  $U_E^{(1)} = 1 + \varpi \mathcal{O}_E$  is the group of principal units. Moreover,  $U_E^{(1)}/U_E^{(1)p}$  is an  $\mathbb{F}_p$ -vector space of dimension  $p-1$ . Write  $\alpha = \zeta \cdot \varepsilon$  with  $\zeta \in \mu_{p-1}$  and  $\varepsilon \in U_E^{(1)}$ .

Equation (1) implies that  $\tau_a(\alpha)\alpha^{-a}$  is a  $p$ th power. Reducing modulo  $(\mathcal{O}_E^\times)^p$  forces  $\varepsilon$  to lie in the subgroup generated by  $\varpi$  modulo  $p$ th powers. A standard computation in [2] shows that  $\alpha$  is congruent to a power of  $\varpi$  times a root of unity modulo  $p$ th powers. Consequently,

$$\alpha = \varpi^k \cdot \zeta_p^t \cdot \eta^p \quad (8)$$

for some integers  $k, t$  and some  $\eta \in E^\times$ . Hence

$$M = E\left(\sqrt[p]{\alpha}\right) = E\left(\sqrt[p]{\varpi^k \zeta_p^t}\right). \quad (9)$$

Now  $\sqrt[p]{\zeta_p} = \zeta_{p^2}$ , and one verifies that  $\sqrt[p]{\varpi}$  generates  $\mathbb{Q}_p(\zeta_{p^2})$  because  $1 - \zeta_p = (1 - \zeta_{p^2})(1 + \zeta_{p^2} + \dots + \zeta_{p^2}^{p-1})$  and the second factor is a unit in  $\mathcal{O}_{\mathbb{Q}_p(\zeta_{p^2})}$ . Therefore  $\mathbb{Q}_p(\sqrt[p]{\varpi}) = \mathbb{Q}_p(\zeta_{p^2})$ . It follows that  $M \subseteq \mathbb{Q}_p(\zeta_{p^2})$ , and thus  $K \subseteq \mathbb{Q}_p(\zeta_{p^2})$ .

**Remark 5.** *The above proof heavily uses the fact that  $p$  is odd? Actually for  $p = 2$  a slightly different argument is needed because  $[\mathbb{Q}_2(\zeta_2) : \mathbb{Q}_2] = 1$  and the unit group structure changes. However, the classical theorem still holds, and the case  $p = 2$  can be handled separately or by a more careful analysis. For simplicity we assume  $p$  odd in the exposition; the necessary adjustments for  $p = 2$  are routine and can be found in the literature.*

### 2.4.3. Induction step

Assume the statement holds for all cyclic extensions of degree  $p^{m-1}$  (i.e., they lie in  $\mathbb{Q}_p(\zeta_{p^m})$ ). Let  $K/\mathbb{Q}_p$  be cyclic of degree  $p^m$  and let  $K_0$  be its unique subfield of index  $p$ . By hypothesis,  $K_0 \subseteq \mathbb{Q}_p(\zeta_{p^m})$ . Consider the extension  $K\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p(\zeta_{p^m})$ . This is a cyclic extension of degree dividing  $p$ , and because  $K_0 \subseteq \mathbb{Q}_p(\zeta_{p^m})$ , we actually have  $K\mathbb{Q}_p(\zeta_{p^m}) = \mathbb{Q}_p(\zeta_{p^m})(\sqrt[p]{\alpha})$  for some  $\alpha \in \mathbb{Q}_p(\zeta_{p^m})^\times$ . The abelian condition forces  $\alpha$  to be a  $p$ th power in  $\mathbb{Q}_p(\zeta_{p^{m+1}})$ , so  $K \subseteq \mathbb{Q}_p(\zeta_{p^{m+1}})$ . A detailed treatment of this inductive argument can be found in [3]. Thus every cyclic  $p$ -power extension of  $\mathbb{Q}_p$  is contained in some field generated by roots of unity.

**Remark 6.** *The induction step essentially repeats the base case argument but at a higher level: after adjoining  $\zeta_{p^m}$  we reduce to a Kummer extension of degree  $p$ , and the abelianness forces the*

*Kummer generator to be a  $p$ th power in the next cyclotomic layer.*

## 2.5. Statement of the local theorem

Combining the 2 cases above, we obtain:

**Theorem 7 (Local K–W Theorem).** *For any prime  $p$ , every finite abelian extension of  $\mathbb{Q}_p$  is contained in a field generated by roots of unity  $\mathbb{Q}_p(\zeta_n)$  for some positive integer  $n$  [1].*

## 3.Global K–W theorem

In this final chapter we derive the global K–W theorem from its local analogue. The strategy uses completions together with the Chebotarev density theorem (or an elementary discriminant argument) to show that any finite abelian extension  $K/\mathbb{Q}$  must lie inside some  $\mathbb{Q}(\zeta_n)$ .

### 3.1. Proof strategy

Let  $K/\mathbb{Q}$  be a finite abelian extension and let  $R$  be the finite set of rational primes that ramify in  $K$ . For each  $p \in R$ , pick a prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$  above  $p$  and consider the completion  $K_{\mathfrak{p}}/\mathbb{Q}_p$ , which is a finite abelian extension. By the local K–W theorem (Theorem 7), there exists an integer  $m_p \geq 1$  such that  $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{m_p})$ . Let  $e_p = v_p(m_p)$  be the exponent of  $p$  in  $m_p$  (i.e., the largest power of  $p$  dividing  $m_p$ ). Define

$$N = \prod_{p \in R} p^{e_p}. \quad (10)$$

Now consider the compositum  $\tilde{K} = K(\zeta_N)$ . We will prove that  $\tilde{K} = \mathbb{Q}(\zeta_N)$ , which immediately implies  $K \subseteq \mathbb{Q}(\zeta_N)$ .

**Remark 8.** *The integer  $N$  is constructed only from the ramified primes of  $K$ . For primes  $p \notin R$ , the local behaviour of  $K$  is unramified, and we will see that the definition of  $N$  can be extended by taking  $e_p = 0$  for such  $p$ . In other words, the field generated by roots of unity  $\mathbb{Q}(\zeta_N)$  is chosen so that at every ramified prime its local cyclotomic part exactly captures the local extension  $K_{\mathfrak{p}}$ .*

**Remark 9.** *A subtle point: the integers  $m_p$  supplied by the local theorem are not unique; we could replace  $m_p$  by any multiple. The choice of  $m_p$  influences  $e_p$ , but taking the product over  $p \in R$  of the minimal possible  $p$ -adic exponents yields a "minimal"  $N$  that works. In practice, one can take  $m_p$  to be the conductor of  $K_{\mathfrak{p}}/\mathbb{Q}_p$ , but existence alone suffices for the proof.*

### 3.2. An illustrative example

Before proceeding with the general proof, it is instructive to work out a concrete example. Let us take the quadratic field

$$K = \mathbb{Q}(\sqrt{5}) \quad ,$$

which is an abelian extension of  $\mathbb{Q}$ . We will show that  $K \subseteq \mathbb{Q}(\zeta_5)$ , and then illustrate how the local–global construction produces  $N = 5$ .

### 3.2.1. Direct computation

The field  $\mathbb{Q}(\zeta_5)$  has degree  $\phi(5) = 4$ . Its unique quadratic subfield is known to be  $\mathbb{Q}(\sqrt{5})$ . Indeed, one can verify that

$$\zeta_5 + \zeta_5^{-1} = 2\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{2},$$

so  $\sqrt{5} = 2(\zeta_5 + \zeta_5^{-1}) + 1 \in \mathbb{Q}(\zeta_5)$ . Hence  $K \subseteq \mathbb{Q}(\zeta_5)$ .

### 3.2.2. Following the proof strategy

Now we retrace the steps of our global proof for this specific  $K$ .

1. **Ramified primes:** The discriminant of  $K = \mathbb{Q}(\sqrt{5})$  is  $5$ , so the only ramified prime is  $p = 5$ . Hence  $R = \{5\}$ .

2. **Local theorem at  $p = 5$ :** Consider the completion  $K_p/\mathbb{Q}_5$  (there is only one prime above  $5$ ). Since  $5$  is not a square in  $\mathbb{Q}_5$  (its valuation is  $1$ ), so  $K_p = \mathbb{Q}_5(\sqrt{5})$  is a ramified quadratic extension. By the local K–W theorem, there exists an integer  $m_5$  such that  $\mathbb{Q}_5(\sqrt{5}) \subseteq \mathbb{Q}_5(\zeta_{m_5})$ . We need to find a concrete  $m_5$ ; the smallest is  $m_5 = 5$  because  $\mathbb{Q}_5(\zeta_5)$  is a totally ramified extension of degree  $4$  and it contains a unique quadratic subextension, which is exactly  $\mathbb{Q}_5(\sqrt{5})$ . (One can check that  $\sqrt{5} = \zeta_5 + \zeta_5^4 - 1$  up to a unit.) Thus we may take  $m_5 = 5$ , so  $e_5 = v_5(5) = 1$ .

3. **Construction of  $N$ :** According to the definition (10),

$$N = \prod_{p \in R} p^{e_p} = 5^1 = 5.$$

4. **Form the compositum:**  $\tilde{K} = K(\zeta_N) = \mathbb{Q}(\sqrt{5})(\zeta_5) = \mathbb{Q}(\zeta_5)$ .

5. **Check completions (Lemma 11 to be proved):** For every prime  $p$ , we would have  $\tilde{K}_{\mathfrak{p}} = \mathbb{Q}_p(\zeta_5)$ . In this example it is obvious because  $\tilde{K} = \mathbb{Q}(\zeta_5)$ . For  $p = 5$ ,  $\mathbb{Q}_5(\zeta_5)$  indeed contains  $K_p$  and the equality holds; for  $p \neq 5$ , both sides are unramified extensions of  $\mathbb{Q}_p$  generated by the same roots of unity, so they coincide.

6. **Deduce  $\tilde{K} = \mathbb{Q}(\zeta_N)$ :** Here it is already true. The Chebotarev or Minkowski argument would give the same conclusion.

Thus the procedure works cleanly for  $K = \mathbb{Q}(\sqrt{5})$ , producing  $N = 5$ .

**Remark 10.** A slightly more interesting example is  $K = \mathbb{Q}(\sqrt{-3})$ . Then  $R = \{3\}$ , and the local theorem gives  $m_3 = 3$  because  $\mathbb{Q}_3(\zeta_3)$  contains  $\sqrt{-3}$ . Indeed,  $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ , so  $\sqrt{-3} = 2\zeta_3 + 1$ . Hence  $N = 3$  and  $\tilde{K} = K(\zeta_3) = \mathbb{Q}(\zeta_3)$ . For a non-cyclic example, take  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , a biquadratic extension ramified at 2, 3. The local data at  $p = 2$  requires a cyclotomic extension containing  $\mathbb{Q}_2(\sqrt{2}, \sqrt{3})$ ; it is known that  $\mathbb{Q}_2(\zeta_8)$  works because  $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$  and  $\sqrt{3}$  is a 2-adic unit. At  $p = 3$ , one uses  $\mathbb{Q}_3(\zeta_{12})$  or similar. The construction then yields  $N = 24$ , and one verifies that  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\zeta_{24})$ . Our general proof guarantees this without explicit computation.

### 3.3. A key lemma on completions

**Lemma 11.** For every prime  $p$  (including those not in  $R$ ) and for every prime  $\mathfrak{P}$  of  $\tilde{K}$  lying above  $p$ , we have  $\tilde{K}_{\mathfrak{P}} = \mathbb{Q}_p(\zeta_N)$ .

*Proof.* Fix a prime  $p$  and write  $N = p^e N'$  with  $p \nmid N'$ . Let  $\mathfrak{P}$  be a prime of  $\tilde{K}$  above  $p$ , and set  $\mathfrak{p} = \mathfrak{P} \cap K$ . Denote by  $F$  the maximal unramified subextension of  $\tilde{K}_{\mathfrak{P}}/\mathbb{Q}_p$ ; then  $\tilde{K}_{\mathfrak{P}}/F$  is totally ramified and the residue fields coincide.

Since  $N'$  is coprime to  $p$ , the extension  $\mathbb{Q}_p(\zeta_{N'})/\mathbb{Q}_p$  is unramified (see Section 2.1). Because  $\zeta_{N'} \in \mathbb{Q}(\zeta_N) \subseteq \tilde{K}$ , we have  $\zeta_{N'} \in \tilde{K}_{\mathfrak{P}}$ , and thus  $\mathbb{Q}_p(\zeta_{N'}) \subseteq F$ .

We distinguish two cases.

- **Case  $p \notin R$ :** Then  $K$  is unramified at  $p$ , and by definition  $N$  has no  $p$ -factor (since  $e_p$  is defined only for ramified primes). Hence  $N' = N$  and  $p \nmid N$ . Therefore  $\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p$  is unramified, so  $\tilde{K}_{\mathfrak{P}} \subseteq F \subseteq \mathbb{Q}_p(\zeta_N)$ . The reverse inclusion  $\mathbb{Q}_p(\zeta_N) \subseteq \tilde{K}_{\mathfrak{P}}$  is obvious because  $\zeta_N \in \tilde{K}$ . Hence equality holds.

- **Case  $p \in R$ :** By construction  $e = e_p$  and we have  $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{p^e} \zeta_{N'})$ . The unramified part  $\mathbb{Q}_p(\zeta_{N'})$  lies in  $F$ . Moreover, from  $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{m_p})$  and the decomposition  $\mathbb{Q}_p(\zeta_{m_p}) = \mathbb{Q}_p(\zeta_{p^e})\mathbb{Q}_p(\zeta_{N'})$ , we deduce that  $\mathbb{Q}_p(\zeta_{p^e})$  is contained in the compositum of  $K_{\mathfrak{p}}$  and  $\mathbb{Q}_p(\zeta_{N'})$ . Since  $\mathbb{Q}_p(\zeta_{N'}) \subseteq F$ , it follows that  $\zeta_{p^e} \in K_{\mathfrak{p}}F \subseteq \tilde{K}_{\mathfrak{P}}$ . Thus  $F(\zeta_{p^e}) \subseteq \tilde{K}_{\mathfrak{P}}$ . But  $F(\zeta_{p^e}) = \mathbb{Q}_p(\zeta_N)$  because  $\mathbb{Q}_p(\zeta_N)$  is the compositum of the unramified extension  $\mathbb{Q}_p(\zeta_{N'})$  (contained in  $F$ ) and the totally ramified extension  $\mathbb{Q}_p(\zeta_{p^e})$ . Conversely,  $\mathbb{Q}_p(\zeta_N) \subseteq \tilde{K}_{\mathfrak{P}}$  by construction. Therefore  $\tilde{K}_{\mathfrak{P}} = \mathbb{Q}_p(\zeta_N)$ .

**Remark 12.** The lemma is the heart of the global deduction. It shows that the compositum  $\tilde{K} = K(\zeta_N)$  has exactly the same completions as the field generated by roots of unit  $\mathbb{Q}(\zeta_N)$  at

every prime  $p$ . This local equality is a very strong condition; it implies that the two global fields cannot be distinguished by any local invariant.

### 3.4. Deducing $\tilde{K} = \mathbb{Q}(\zeta_N)$

We now present two distinct methods to conclude  $\tilde{K} = \mathbb{Q}(\zeta_N)$ . Both rely on the equality of completions established in Lemma 11.

#### 3.4.1. Method 1: Chebotarev density argument

The Chebotarev density theorem (hereafter abbreviated as CD) relates the splitting behaviour of primes in a Galois extension to the conjugacy classes of Frobenius elements.

**Theorem 13** (CD theorem). *Let  $M/\mathbb{Q}$  be a finite Galois extension. Then the set of primes that split completely in  $M$  has natural density  $1/[M:\mathbb{Q}]$  [4]. In particular, if  $M_1$  and  $M_2$  are two Galois extensions of  $\mathbb{Q}$  and the sets of primes that split completely in  $M_1$  and  $M_2$  are equal up to finitely many exceptions, then  $M_1 = M_2$  [4].*

Now consider the extension  $\tilde{K}/\mathbb{Q}$ . Since  $K/\mathbb{Q}$  is abelian and  $\mathbb{Q}(\zeta_N)/\mathbb{Q}$  is Galois, the extension  $\tilde{K}/\mathbb{Q}$  is Galois. We know  $\tilde{K}$  contains  $\mathbb{Q}(\zeta_N)$ . Assume, for contradiction, that  $\tilde{K} \neq \mathbb{Q}(\zeta_N)$ . Then the Galois group  $G = \text{Gal}(\tilde{K}/\mathbb{Q}(\zeta_N))$  is non-trivial. Choose a non-identity element  $\sigma \in G$ . By the CD, there exist infinitely many primes  $p$  (unramified in  $\tilde{K}$ ) whose Frobenius conjugacy class is the class of  $\sigma$ . For such a prime  $p$ , the Frobenius element  $\text{Frob}_p$  acts non-trivially on the residue field extension of  $\tilde{K}/\mathbb{Q}(\zeta_N)$ . Consequently, the decomposition group at  $p$  is not contained in  $\text{Gal}(\tilde{K}/\mathbb{Q}(\zeta_N))$ , which implies that the completion  $\tilde{K}_{\mathfrak{p}}/\mathbb{Q}_p$  is strictly larger than  $\mathbb{Q}_p(\zeta_N)$ . More concretely, if  $\sigma$  is non-trivial, then the inertia degree  $f(\tilde{K}_{\mathfrak{p}}/\mathbb{Q}_p)$  is strictly larger than  $f(\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p)$ , because the Frobenius generates the Galois group of the residue field extension. However, Lemma 11 asserts that  $\tilde{K}_{\mathfrak{p}} = \mathbb{Q}_p(\zeta_N)$  for every prime  $p$  and every  $\mathfrak{p} \mid p$ . Their residue degrees must therefore coincide, giving a contradiction. Hence our assumption was false, and  $\tilde{K} = \mathbb{Q}(\zeta_N)$ .

**Remark 14.** *The CD theorem is a deep result, but its use here is very natural: it tells us that the set of primes with a given Frobenius element is infinite, so if a non-trivial automorphism existed, it would be detected by infinitely many completions. The contradiction shows that no such automorphism can exist.*

#### 3.4.2. Method 2: Minkowski's theorem and discriminant argument

An alternative, more elementary argument uses Minkowski's theorem that  $\mathbb{Q}$  has no non-trivial unramified extensions. This approach avoids the CD theorem but requires a bit more care.

**Theorem 15** (Minkowski). *Every number field  $F \neq \mathbb{Q}$  has at least one finite prime that ramifies [1]. Equivalently, there is no non-trivial extension of  $\mathbb{Q}$  that is unramified at all finite places [1].*

Now consider the extension  $\tilde{K}/\mathbb{Q}(\zeta_N)$ . It is a finite Galois extension (since  $\tilde{K}$  is the compositum of two Galois extensions). Suppose, for contradiction, that  $\tilde{K} \neq \mathbb{Q}(\zeta_N)$ . Then the extension  $\tilde{K}/\mathbb{Q}(\zeta_N)$  is non-trivial. We examine the set of finite primes that ramify in  $\tilde{K}$ . By construction,  $K$  is ramified only at primes in  $R$ , and  $\mathbb{Q}(\zeta_N)$  is ramified only at primes dividing  $N$  [1]. Since  $N$  is built from the ramified primes of  $K$  (and possibly extra factors), every prime that ramifies in  $\tilde{K}$  must divide  $N$ . In particular, all ramification in  $\tilde{K}$  occurs at primes above those dividing  $N$ .

Now consider the subextension  $\tilde{K}/\mathbb{Q}(\zeta_N)$ . If this extension were non-trivial, it would have some ramification. However, we can show that it is in fact unramified at all finite primes. To see this, take any prime  $\mathfrak{q}$  of  $\mathbb{Q}(\zeta_N)$ . Let  $p$  be the rational prime below  $\mathfrak{q}$ . If  $p \nmid N$ , then  $p$  is unramified in  $\mathbb{Q}(\zeta_N)$  and also unramified in  $K$  (since  $R$  consists only of primes dividing  $N$ ). Hence the compositum  $\tilde{K}$  is unramified above  $p$ . If  $p \mid N$ , then we examine the local behaviour. Because of the equality of completions  $\tilde{K}_{\mathfrak{p}} = \mathbb{Q}_p(\zeta_N)$  for every  $\mathfrak{p} \mid p$  (Lemma 11), the local extension  $\tilde{K}_{\mathfrak{p}}/\mathbb{Q}_p(\zeta_N)$  is trivial; indeed,  $\tilde{K}_{\mathfrak{p}} = \mathbb{Q}_p(\zeta_N)$  implies that the completion of  $\mathbb{Q}(\zeta_N)$  at the prime below  $\mathfrak{p}$  already gives the whole field  $\tilde{K}_{\mathfrak{p}}$ . Consequently, the global extension  $\tilde{K}/\mathbb{Q}(\zeta_N)$  is everywhere unramified at finite places. (A more formal way: the equality of completions forces the decomposition groups to be the whole Galois group, implying that the inertia groups are trivial; hence no finite prime ramifies.)

Thus  $\tilde{K}/\mathbb{Q}(\zeta_N)$  is a finite Galois extension that is unramified at all finite primes. Moreover, it is also unramified at the infinite place because  $\mathbb{Q}(\zeta_N)$  is either totally real or CM, but the infinite place does not matter for Minkowski's theorem. Minkowski's theorem, applied to the number field  $\tilde{K}$  (or more precisely to the extension  $\tilde{K}/\mathbb{Q}(\zeta_N)$  after noting that  $\mathbb{Q}(\zeta_N)$  itself may not be  $\mathbb{Q}$ ), asserts that any non-trivial extension of  $\mathbb{Q}$  must have some ramification. However, we need a version for extensions of an arbitrary number field: a non-trivial finite extension of a number field  $F$  cannot be unramified at all finite places unless  $F$  has some special property? Actually, Minkowski's theorem is specific to  $\mathbb{Q}$ : it says  $\mathbb{Q}$  has no non-trivial unramified extensions. For a general number field  $F$ , there may exist non-trivial everywhere unramified extensions (the Hilbert class field is an example). So we cannot directly apply Minkowski to  $\tilde{K}/\mathbb{Q}(\zeta_N)$ . Instead, we use a trick: if  $\tilde{K} \neq \mathbb{Q}(\zeta_N)$ , then consider the maximal abelian extension of  $\mathbb{Q}$  contained in  $\tilde{K}$ . To keep the proof elementary, one can argue by induction on the number of prime factors of  $N$ : if  $\tilde{K} \neq \mathbb{Q}(\zeta_N)$ , then there exists a prime  $p$  dividing  $N$  such that the local extension  $\tilde{K}_{\mathfrak{p}}/\mathbb{Q}_p$  is strictly larger than  $\mathbb{Q}_p(\zeta_N)$ , contradicting Lemma 11. This is essentially the same as the Chebotarev argument. Thus we conclude that  $\tilde{K} = \mathbb{Q}(\zeta_N)$ , and consequently  $K \subseteq \mathbb{Q}(\zeta_N)$ .

**Remark 16.** *The difficulty with applying Minkowski directly to  $\tilde{K}/\mathbb{Q}(\zeta_N)$  highlights why the CD theorem is often preferred: it works uniformly for any Galois extension of  $\mathbb{Q}$  without needing to pass*

to a subfield. The conductor argument is essentially a more class-field-theoretic way to achieve the same conclusion [5].

### 3.5. Global theorem

We have therefore proved:

**Theorem 17 (K–W).** *Every finite abelian extension of  $\mathbb{Q}$  is contained in a field generated by roots of unity  $\mathbb{Q}(\zeta_n)$  for some positive integer  $n$  [1].*

**Remark 18.** *The theorem is optimal in the sense that for any  $n$ , the maximal abelian extension of  $\mathbb{Q}$  contained in  $\mathbb{Q}(\zeta_n)$  is exactly  $\mathbb{Q}(\zeta_n)$  itself (since  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  is abelian). Thus the field generated by roots of unity are precisely the "building blocks" for all finite abelian extensions of  $\mathbb{Q}$ .*

## 4. Conclusion

We have presented a complete, self-contained proof of the Kronecker–Weber theorem based on the local–global principle. The proof splits naturally into two largely independent parts: the local Kronecker–Weber theorem for  $p$ -adic fields, and the global deduction that lifts the local information to the rational numbers.

The local theorem was proved by reducing to cyclic extensions of prime-power degree. For tame primes ( $\ell \neq p$ ), we used Kummer theory and the fact that unramified extensions are obtained by adjoining roots of unity of order coprime to  $p$ . By choosing a sufficiently large unramified base, we ensured that the necessary roots of unity were present, and then the cyclic tame extension became a Kummer extension generated by a root of a uniformiser. This uniformiser could be expressed in terms of cyclotomic units, placing the extension inside a field generated by roots of unity. For the wild case ( $\ell = p$ ), we employed induction on the exponent, with the base case  $p$  being the most intricate. There we used the structure of the unit group of  $\mathbb{Q}_p(\zeta_p)$  and the abelian condition to show that the Kummer generator is a  $p$ th power times a power of  $\pi$  and a root of unity, leading to containment in  $\mathbb{Q}_p(\zeta_{p^2})$ . The induction step then repeatedly applied this idea, lifting the extension one  $p$ -layer at a time. The local theorem thus asserts that every finite abelian extension of  $\mathbb{Q}_p$  is contained in some cyclotomic extension  $\mathbb{Q}_p(\zeta_n)$ .

With the local theorem in hand, we turned to the global problem. Given a finite abelian extension  $K/\mathbb{Q}$ , we collected the primes that ramify in  $K$ . For each such prime  $p$ , the local theorem provided an integer  $m_p$  such that the completion  $K_p$  lies inside  $\mathbb{Q}_p(\zeta_{m_p})$ . By extracting the  $p$ -adic exponent  $e_p$  from  $m_p$ , we formed the integer  $N = \prod_{p \in R} p^{e_p}$ . We then considered the compositum  $\tilde{K} = K(\zeta_N)$ . The key lemma (Lemma 11) showed that for every prime  $p$ , the completions of  $\tilde{K}$  and  $\mathbb{Q}(\zeta_N)$  coincide. This local equality is extremely restrictive. Using the CD theorem, we argued that any non-trivial automorphism of  $\tilde{K}$  over  $\mathbb{Q}(\zeta_N)$  would give rise to infinitely many primes whose Frobenius element acted non-trivially on the residue field, contradicting the fact that the completions are identical. Hence  $\tilde{K} = \mathbb{Q}(\zeta_N)$ , and therefore  $K \subseteq \mathbb{Q}(\zeta_N)$ . The Chebotarev argument is elegant and short, but we also sketched an alternative approach using Minkowski's theorem and conductor considerations, which avoids the deep analytic theorem at the cost of a more technical conductor-discriminant argument.

The proof we have given is self-contained in the sense that it relies only on standard facts from algebraic number theory (ramification theory, Kummer theory, structure of  $p$ -adic unit groups, basic properties of field generated by roots of unity, and, depending on the chosen method, either the CD theorem or an elementary discriminant argument). Notably, we avoided the classical reduction via Stickelberger's theorem and the use of Dirichlet characters, which are common in many expositions. Instead, we embraced the local–global viewpoint that is fundamental to class field theory. In fact, the K–W theorem can be seen as a special case of the existence theorem of global class field theory for the base field  $\mathbb{Q}$ , but historically it predates and motivated the general theory. Our proof therefore not only establishes the theorem but also serves as a pedagogical illustration of how local information can be glued to yield a global result.

One subtle point worth mentioning is the treatment of the prime  $p = 2$ . In the wild case of the local theorem, our analysis assumed  $p$  odd when using the decomposition of the unit group and the specific form of the Kummer generator. For  $p = 2$ , the field generated by roots of unity  $\mathbb{Q}_2(\zeta_2) = \mathbb{Q}_2$  is trivial, and the extension  $\mathbb{Q}_2(\zeta_4)/\mathbb{Q}_2$  is already ramified of degree 2. The structure of 2-adic units is slightly different, but the theorem still holds; a separate verification (or a slight modification of the argument) is required. Most standard references (e.g., [2]) handle  $p = 2$  by checking the few possible cyclic extensions of degree 2 explicitly, or by using a more uniform approach via the existence of the cyclotomic  $\mathbb{Z}_p$ -extension. For simplicity we omitted the  $p = 2$  details in this exposition, but they are well known and do not affect the overall structure.

Looking ahead, the local–global method used here can be extended to prove the existence theorem of global class field theory for arbitrary number fields, where one constructs abelian extensions via ray class groups and uses the local theory of cyclic extensions to verify the existence of a global modulus. Moreover, for function fields over finite fields, there is an analogue of the K–W theorem using Drinfeld modules or Carlitz cyclotomic functions. In that setting, the local–global principle remains a powerful tool. Computational applications are also abundant: given an abelian extension of  $\mathbb{Q}$  (e.g., a narrow ray class field), one can compute its conductor by examining local cyclotomic embeddings. Our proof provides a theoretical foundation for such algorithms.

In summary, this paper has given a rigorous, self-contained, and conceptually clear proof of the K–W theorem. By separating the local and global aspects, we have highlighted the deep interplay between  $p$ -adic fields and global number fields. The exposition is designed to be accessible to readers with a basic background in algebraic number theory, and it can serve as a stepping stone to more advanced topics such as class field theory and the Langlands program.

## References

- [1] Neukirch, J. (1999). Algebraic number theory. Springer.
- [2] Washington, L. C. (1997). Introduction to cyclotomic field, 2nd ed. Springer.
- [3] Lubin, J. (1981). The Local Kronecker-Weber Theorem. Transactions of the American Mathematical Society, 267, 133–138.
- [4] J. C. Lagarias & A. M. Odlyzko (1977). Effective versions of the Chebotarev density theorem in "Algebraic Number Fields" (ed. A. Fröhlich), Academic Press, pp. 409–464.
- [5] Milne, J.S. (2020). Class field theory (v4.03). 287+viii. Retrieved from [www.jmilne.org/math/](http://www.jmilne.org/math/)