

# The Kronecker–Weber Theorem

Anthony Várilly

*Harvard University, Cambridge, MA 02138  
Math 250a, Fall 2001*

## Abstract

We prove the celebrated Kronecker–Weber theorem. We develop much of the theory of ramification of prime ideals in Galois extensions of algebraic number fields for this purpose.

## 1 Introduction

The Kronecker–Weber theorem gives a characterization of all finite abelian extensions of the rational numbers  $\mathbb{Q}$ , i.e., extensions of finite degree over  $\mathbb{Q}$  with abelian Galois group. In fact,

**Theorem (Kronecker–Weber).** Every abelian extension of  $\mathbb{Q}$  is cyclotomic.

The key idea behind the proof we present here is the theory of ramification of prime ideals in Galois extensions of algebraic number fields. We will develop this theory following a simplified program of that presented by Zariski and Samuel [Z-S] and also inspired by Ribenboim [R]. Our exposition of the proof of the Kronecker–Weber theorem is inspired by Greenberg [G] and Ribenboim [R].

We will assume all field extensions to be of finite degree throughout this paper. We will also assume standard results about Dedekind domains. Chapter V of [Z-S] is a good reference for these results.

### 1.1 Cyclotomic Extensions

Throughout this paper  $\zeta_m$  will denote a primitive  $m^{\text{th}}$  root of unity. A *cyclotomic extension* of  $\mathbb{Q}$  is a subfield of  $\mathbb{Q}(\zeta_m)$ . Recall that  $\mathbb{Q}(\zeta_m)$  is an abelian extension of  $\mathbb{Q}$ , and that its Galois group is isomorphic to the group of units of  $\mathbb{Z}/m\mathbb{Z}$  [Lang, Thm VI.3.1]. We will be interested in cyclotomic extensions inside  $\mathbb{Q}(\zeta_{p^r})$ , where  $p$  is a prime number and  $r$  is a positive integer. We know from elementary number theory that the group of units of  $\mathbb{Z}/p^r\mathbb{Z}$

is

$$(\mathbb{Z}/p^r\mathbb{Z})^\times = \begin{cases} C(p^r - p^{r-1}) & \text{if } p \text{ is an odd prime,} \\ C(2^{r-2}) \times C(2) & \text{if } p = 2 \text{ and } r \geq 3, \\ C(2) & \text{if } p = 2, r = 2, \\ \{1\} & \text{if } p = 2, r = 1, \end{cases} \quad (1)$$

where  $C(m)$  denotes a cyclic group of order  $m$  [Long, 6, Proposition 2.2].

Our first stab at Kronecker–Weber theorem will be to reduce it to the case where the degree of the extension is a prime power. This follows from the fact that the composite of two cyclotomic extensions is also cyclotomic. Indeed, recall that if  $k$  is a field and  $K$  and  $L$  are two Galois extensions of  $k$  both contained in some larger field, with Galois groups  $G$  and  $H$  respectively, then the composite  $KL$  has Galois group canonically isomorphic to a subgroup of  $G \times H$  consisting of the pairs  $(\sigma, \tau)$ , where  $\sigma$  and  $\tau$  agree on elements of  $K \cap L$ . An automorphism  $\sigma \in \text{Gal}(KL|k)$  maps to  $G \times H$  by  $\sigma \mapsto (\sigma|_K, \sigma|_L)$  [Lang, p. 267]. Thus, if  $K$  is a subfield of  $\mathbb{Q}(\zeta_m)$  and  $L$  a subfield of  $\mathbb{Q}(\zeta_n)$ ,  $KL$  is a subfield of  $\mathbb{Q}(\zeta_{mn})$ .

**Theorem 1.1.** *Let  $K$  be an abelian extension of  $\mathbb{Q}$ . Suppose all abelian extensions of  $\mathbb{Q}$  of degree  $p^r$  ( $p$  a prime number) are cyclotomic. Then  $K$  is cyclotomic.*

*Proof.* By the structure theorem for finite abelian groups, the Galois group  $G$  of  $K|\mathbb{Q}$  is isomorphic to a direct product  $C(p_1^{\alpha_1}) \times \cdots \times C(p_n^{\alpha_n})$ , where the  $p_i$ 's are prime numbers. Let  $K_i$  be the fixed field of the subgroup  $\prod_{j \neq i} C(p_j^{\alpha_j})$ . This is a normal subgroup of  $G$  (since  $G$  is abelian). By the fundamental correspondence  $K_i$  is a Galois extension of  $\mathbb{Q}$  with Galois group isomorphic to  $C(p_i^{\alpha_i})$ . By assumption,  $K_i$  is cyclotomic. Since  $K$  is equal to the composite  $K_1 \cdots K_n$ , it is cyclotomic.  $\square$

## 2 Ramification of prime ideals in Galois Extensions

The next stage in the proof of the Kronecker–Weber theorem consists in further reducing the problem to the case when the abelian extension  $K$  over  $\mathbb{Q}$  is of prime power degree  $p^r$ , and where  $p$  is the only prime that ramifies in  $K$ . First, however, we must explain what ramification is. We will develop much of the theory of ramification groups, which is quite beautiful in its own right.

Let  $K$  be an abelian extension of  $\mathbb{Q}$ . We are interested in the behaviour of prime ideals  $p\mathbb{Z}$  of  $\mathbb{Z}$  when considered as ideals in  $\mathfrak{D}_K$ , the ring of integers of  $K$ . We will look at a slightly more general set-up; little is gained in our proofs by specializing to the case just described.

**Initial Set-up.** Unless otherwise indicated, we will use the following notation throughout the rest of this paper. Let  $k$  and  $K$  be two algebraic number fields with  $K$  a finite *Galois extension* of degree  $n$  over  $k$  with Galois group  $G$ . Let  $R$  be the ring of integers of  $k$  and  $R'$  the ring of integers of  $K$ . Then both  $R$  and  $R'$  are Dedekind domains (see, for example, [R, p. 113]). The case we want to keep in mind is  $k = \mathbb{Q}$ .

Let  $\mathfrak{p}$  be a proper prime ideal of  $R$ . Consider the ideal  $\mathfrak{p}R'$  of  $R'$ . Since  $R'$  is a Dedekind domain and  $\mathfrak{p}R' \neq R'$  [Z-S, p. 258], the ideal  $\mathfrak{p}R'$  has a unique factorization into proper prime ideals of  $R'$ ,

$$\mathfrak{p}R' = \prod_{i=1}^g \mathfrak{P}_i^{e_i}. \quad (2)$$

We call  $g$  the *decomposition number* of  $\mathfrak{p}$  in  $K|k$ ;  $e_i$  is the *ramification index* of  $\mathfrak{P}_i$  over  $\mathfrak{p}$  (which we will denote  $e_i(\mathfrak{P}_i|\mathfrak{p})$  if necessary). If  $e_1 = \cdots = e_g = 1$ , we say  $\mathfrak{p}$  is *unramified* in  $K|k$ . Otherwise, we say  $\mathfrak{p}$  *ramifies* in  $K|k$ . Alternatively, if  $e_i > 1$  for some  $i$ , we say  $\mathfrak{P}_i$  ramifies over  $\mathfrak{p}$ .

Note that  $\mathfrak{p} \subset (\mathfrak{p}R' \cap R) \subset (\mathfrak{P}_i \cap R)$ . However, since  $R$  is a Dedekind domain,  $\mathfrak{p}$  is a maximal ideal, and since  $\mathfrak{P}_i \cap R$  is a proper ideal of  $R$  (otherwise  $\mathfrak{P}_i$  contains 1), we conclude  $\mathfrak{p} = \mathfrak{P}_i \cap R$ . A prime ideal  $\mathfrak{P}$  of  $R'$  such that  $\mathfrak{P} \cap R = \mathfrak{p}$  is said to *lie over*  $\mathfrak{p}$ .

Since  $\mathfrak{p} = \mathfrak{P}_i \cap R$ ,  $R/\mathfrak{p}$  can be identified with a subfield of  $R'/\mathfrak{P}_i$ . Furthermore,  $R'/\mathfrak{P}_i$  is a *finite algebraic* extension of  $R/\mathfrak{p}$  [Z-S, p 284]. The degree  $f_i = [R'/\mathfrak{P}_i : R/\mathfrak{p}]$  is called the *inertial degree* of  $\mathfrak{P}_i$  over  $\mathfrak{p}$ .

**Remark 2.1.** One can show that the ramification index and the inertial degree satisfy transitivity relations. Let  $k \subset K \subset L$  be algebraic number fields with rings of integers  $R \subset R' \subset R''$  and let  $\mathfrak{P}'$  be a non-zero prime ideal of  $R''$ ,  $\mathfrak{P} = \mathfrak{P}' \cap R'$ ,  $\mathfrak{p} = \mathfrak{P} \cap R$ . If  $e$  is the ramification index of  $\mathfrak{P}$  in  $K|k$ ,  $e'$  is that of  $\mathfrak{P}'$  in  $L|K$  and  $e''$  that of  $\mathfrak{P}'$  in  $L|k$ , then  $e'' = ee'$ . With the obvious similar notation,  $f'' = ff'$ . See [R, p 162].

Until now, we have not made use of the hypothesis that  $K$  is a *Galois* extension of  $k$  of degree  $n$ . Our next goal is to show that in such a case,  $e_1 = \cdots = e_g := e$  and  $f_1 = \cdots = f_g := f$  in (2). Furthermore, we will show that  $efg = n$ .

**Lemma 2.2.** *Let  $\mathfrak{P}$  and  $\mathfrak{P}'$  be two prime ideals of  $R'$  such that  $\mathfrak{P} \cap R = \mathfrak{P}' \cap R$ . Then there exists an element  $\sigma \in G = \text{Gal}(K|k)$  such that  $\sigma(\mathfrak{P}) = \mathfrak{P}'$ .*

*Proof.* Suppose  $\mathfrak{P}' \neq \sigma_i(\mathfrak{P})$  for all  $\sigma_i \in G$ . Let  $\mathfrak{P}_1, \dots, \mathfrak{P}_m$  be the distinct conjugates of  $\mathfrak{P}$  under the action of  $G$  (these are prime ideals in  $R'$ ). Since  $\mathfrak{P}' \neq \mathfrak{P}_i$  for  $i = 1, \dots, m$ , there are elements  $a_i \in \mathfrak{P}' - \mathfrak{P}_i$ . Furthermore, since the  $\mathfrak{P}_i$  are distinct, there exist elements  $x_{ij} \in \mathfrak{P}_j - \mathfrak{P}_i$  for all  $i, j$  with  $i \neq j$ . Let  $b_i = a_i \prod_{j \neq i} x_{ij}$  and let  $b = b_1 + \cdots + b_m$ . Then, on the one hand,  $b$  is in  $\mathfrak{P}'$  since  $a_i \in \mathfrak{P}'$  for all  $i$ . On the other hand,  $b$  is not in  $\sigma_i(\mathfrak{P})$  for any  $\sigma_i \in G$  because there is one (and only one)  $j$  for which  $b_j \notin \sigma_i(\mathfrak{P})$ . Consider the norm of  $b$ ,  $N_{K|k}(b) = \prod_i \sigma_i(b)$ . Then  $N_{K|k}(b) \in \mathfrak{P}' \cap R = \mathfrak{P} \cap R$ . But  $N_{K|k}(b) \notin \mathfrak{P}$  since  $\mathfrak{P}$  is a prime ideal and  $\sigma_i(b) \notin \mathfrak{P}$  for any  $i$  (otherwise we would have  $b \in \sigma_i^{-1}(\mathfrak{P})$ ). Hence, there must be some  $i$  for which  $\mathfrak{P}' = \sigma_i(\mathfrak{P})$ .  $\square$

**Theorem 2.3.** *If  $K$  is a Galois extension of  $k$  and  $\mathfrak{p}$  a prime ideal of  $k$  such that  $\mathfrak{p}R' = \prod_i \mathfrak{P}_i^{e_i}$ , then  $e_1 = \cdots = e_g := e$  and  $f_1 = \cdots = f_g := f$ .*

*Proof.* The ideals of  $R'$  in the factorization of  $\mathfrak{p}R'$  all lie over  $\mathfrak{p}$ . Therefore, by Lemma 2.2, for each  $j$  there is a  $\sigma \in G$  such that  $\sigma(\mathfrak{P}_j) = \mathfrak{P}_1$ . We have  $\mathfrak{p}R' = \sigma(\mathfrak{p}R') = \prod_i \sigma(\mathfrak{P}_i)^{e_i}$ . Uniqueness of prime-ideal factorization in Dedekind domains gives  $e_j = e_1$  for each  $j$ . Also,  $R'/\mathfrak{P}_j \cong R'/\sigma(\mathfrak{P}_1)$ , and one may verify that  $R'/\sigma(\mathfrak{P}_1) \cong R'/\mathfrak{P}_1$ , so  $f_j = f_1$  for each  $j$ .  $\square$

Now, in order to show that  $efg = n$ , we will prove a more general relation and then show how the equality  $efg = n$  follows in our initial set-up. We need the following lemma.

**Lemma 2.4.** *Let  $R$  be a Dedekind domain,  $k$  its field of fractions,  $K$  a finite separable algebraic extension of  $k$  of degree  $n$  and  $R'$  the integral closure of  $R$  in  $K$ . (Note that our initial set-up is a special case of this, when  $K, k$  are algebraic number fields and  $\mathfrak{D}_k = R, \mathfrak{D}_K = R'$ .) Then  $R'$  is an  $R$ -submodule of a free  $R$ -module of rank  $n$ .*

*Sketch of proof.* Let  $\{x_1, \dots, x_n\}$  be a basis of  $K$  over  $k$ . Each  $x_i$  satisfies an algebraic relation over  $k$ . If  $s_i$  is the common denominator of the coefficients of this relation, then  $u_i = s_i x_i$  is integral over  $R$ . In this way we construct a basis  $\{u_1, \dots, u_n\}$  of  $K$  over  $k$  with elements in  $R'$ .

Consider  $K$  as a vector space over  $k$ . If  $K^*$  denotes the dual of  $K$ , and  $\langle \cdot, \cdot \rangle$  is a non-degenerate, bilinear symmetric form on  $K$ , then the map  $\phi : K \rightarrow K^*$  given by

$$\phi(x) : y \longmapsto \langle x, y \rangle,$$

is an isomorphism. Take  $\langle x, y \rangle = \text{Tr}(xy)$  (Tr is the trace map). Note  $\text{Tr}(xy)$  is non-degenerate since  $K$  is separable over  $k$  [Lang, Thm IV.5.2]. Let  $\{v_1, \dots, v_n\}$  be elements of  $K$  that are linearly independent over  $k$  such that  $\phi(v_i)$  from the dual basis of  $K^*$  to  $\{u_1, \dots, u_n\}$ , i.e.,  $\text{Tr}(v_i u_j) = \delta_{ij}$ . For  $x \in R'$ , we have  $x = \sum b_i v_i$ ,  $b_i \in k$  for every  $i$ . Since  $x \in R'$ , we have  $xu_i \in R'$  for every  $i$ , so  $\text{Tr}(xu_i) \in R$  since it is one of the coefficients of the minimal polynomial of  $xu_i$  in  $R$ . But  $\text{Tr}(xu_i) = \sum b_j \text{Tr}(u_i v_j) = b_i$ . Thus  $b_i \in R$  for every  $i$  and so  $R' \subset \sum Rv_j$ .  $\square$

**Corollary 2.5.** *With the set-up of Lemma 2.4, if  $R$  is also a principal ideal domain (PID), then there is a basis  $\{x_1, \dots, x_n\}$  of  $K$  over  $k$  such that  $R' = \sum Rx_i$ .*

*Proof.* If  $R$  is a principal ideal domain, a submodule of a free  $R$ -module is free. This means  $R'$  has rank  $\leq n$  as an  $R$ -module. But we've exhibited an  $n$ -element basis of  $K$  over  $k$  contained in  $R'$ , so  $R'$  must have rank  $\geq n$  as an  $R$ -module.  $\square$

We are now ready to show that  $efg = n$ . We will only do this for  $R$  a PID, since the case that interests us is  $R = \mathbb{Z}$ . The relation still holds true when  $R$  is a Dedekind domain; in fact, this case can be reduced to that of  $R$  being a PID by localization. We will not show how to do this for lack of space, but the proof can be found in Samuel's excellent book [S, §5.2, Theorem 1]. His proof we have slightly adapted for our purposes.

**Theorem 2.6.** *Using the set-up of Lemma 2.4, let  $R$  be a PID,  $\mathfrak{p}$  a prime ideal of  $R$ ,  $\prod_{i=1}^g \mathfrak{P}_i^{e_i}$  the factorization of  $\mathfrak{p}R'$  and  $f_i = [R'/\mathfrak{P}_i : R/\mathfrak{p}]$ . Then*

$$\sum_{i=1}^g e_i f_i = [R'/\mathfrak{p}R' : R/\mathfrak{p}] = n. \quad (3)$$

*Consequently, if  $K|k$  is Galois, then  $efg = n$ .*

*Proof.* Consider the chain of ideals given by

$$R' \supset \mathfrak{P}_1 \supset \mathfrak{P}_1^2 \supset \cdots \supset \mathfrak{P}_1^{e_1} \supset \mathfrak{P}_1^{e_1} \mathfrak{P}_2 \supset \cdots \supset \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \supset \cdots \supset \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} = \mathfrak{p}R'.$$

Two adjacent elements in this chain have the form  $\mathfrak{P} \supset \mathfrak{P}\mathfrak{P}_i$ . Now  $[\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i : R'/\mathfrak{P}_i] = 1$  since there are no intermediate ideals between  $\mathfrak{P}$  and  $\mathfrak{P}\mathfrak{P}_i$ . Therefore

$$[\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i : R/\mathfrak{p}] = [\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i : R'/\mathfrak{P}_i][R'/\mathfrak{P}_i : R/\mathfrak{p}] = f_i.$$

For a given  $i$ , there are  $e_i$  consecutive elements in our chain with associated quotient space of the form  $\mathfrak{P}/\mathfrak{P}\mathfrak{P}_i$  of dimension  $f_i$  over  $R/\mathfrak{p}$ . The total dimension of  $R'/\mathfrak{p}R'$  over  $R/\mathfrak{p}$  is the sum of the dimensions of these quotients. This establishes the first equality of (3).

Since  $R$  is a PID,  $R'$  is a free  $R$ -module of rank  $n$  by Corollary 2.5. If  $\{x_1, \dots, x_n\}$  is a basis of  $R'$  as an  $R$ -module, reduction mod  $\mathfrak{p}R'$  gives a basis for  $R'/\mathfrak{p}R'$  over  $R/\mathfrak{p}$ , so  $[R'/\mathfrak{p}R' : R/\mathfrak{p}] = n$ .

If  $K|k$  is Galois, we know from Theorem 2.3 (which also holds in the slightly more general set-up of Lemma 2.4) that  $e_1 = \cdots = e_g = e$  and  $f_1 = \cdots = f_g = f$ . Hence  $efg = n$ .  $\square$

The relation  $efg = n$  gives us a lot of information about the higher ramification groups of an ideal  $\mathfrak{P}$ . These groups are essential to our proof of the Kronecker-Weber theorem.

### 3 Decomposition, Inertia and Higher Ramification Groups

Let us go back to our initial set-up where  $K$  and  $k$  are algebraic number fields and  $K$  is a finite Galois extension of  $k$  of degree  $n$  and where  $R'$  and  $R$  denote the rings of integers of  $K$  and  $k$  respectively. We now turn our attention to certain groups associated with the phenomenon of ramification. We will start with the decomposition and inertia groups of a prime ideal  $\mathfrak{P}$  in  $R'$  lying over the prime ideal  $\mathfrak{p}$  of  $R$ . These are subgroups of the Galois group  $G$  of  $K$  over  $k$ . To make notation a little less cumbersome, we will write  $\overline{K} = R'/\mathfrak{P}$  and  $\overline{k} = R/\mathfrak{p}$ .

#### 3.1 Decomposition and Inertia groups

Given a proper prime ideal  $\mathfrak{p}$  of  $R$  and a prime ideal  $\mathfrak{P}$  of  $R'$  lying over  $\mathfrak{p}$ , the *decomposition group*  $Z$  of  $\mathfrak{P}$  is defined as

$$Z = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

By Lemma 2.2, the prime ideals that lie over  $\mathfrak{p}$  are conjugate by elements of  $G$  and appear in the factorization of  $\mathfrak{p}R'$ ; in particular, there are  $g$  of them. Hence the orbit of  $\mathfrak{P}$  under conjugation by  $G$  has size  $g$ . By Theorem 2.6, the stabilizer of  $\mathfrak{P}$  has size  $ef$ , i.e.,  $|Z| = ef$ .

Let  $K_Z$  denote the fixed field of  $Z$ . By the fundamental Galois correspondence,  $K$  is a Galois extension of  $K_Z$  and  $\text{Gal}(K|K_Z) = Z$ . Furthermore, if  $K$  is an *abelian* extension of  $k$  (recall we are interested in abelian extensions), then  $Z \triangleleft G$  and  $K_Z$  is a Galois extension of  $k$  with Galois group  $G/Z$ :

$$K \xleftarrow{Z} K_Z \xleftarrow{G/Z} k. \tag{4}$$

The *inertia group*  $T$  of  $\mathfrak{P}$  is defined as

$$T = \{\sigma \in G \mid \sigma(x) \equiv x \pmod{\mathfrak{P}} \quad \forall x \in R'\}$$

Clearly,  $T \leq Z$ . One may verify that  $T$  is a normal subgroup of  $Z$  (this is trivial if  $G$  is abelian).

Let  $K_T$  denote the fixed field of  $T$ . Again, by the fundamental Galois correspondence  $K$  is a Galois extension of  $K_T$  with  $\text{Gal}(K|K_T) = T$  and  $K_T$  is a Galois extension of  $K_Z$  with  $\text{Gal}(K_T|K_Z) = Z/T$  since  $T \triangleleft Z$ :

$$K \xleftarrow{T} K_T \xleftarrow{Z/T} K_Z \xleftarrow{G/Z} k. \quad (5)$$

We know already that  $Z$  has order  $ef$ , i.e.,  $[K_Z : K] = g$ . What is the order of  $T$ ? This is equivalent to knowing the order of  $Z/T$  since  $|T| \cdot |Z/T| = ef$ . We will show in fact that

$$Z/T \cong \text{Gal}(\overline{K}|\overline{k}). \quad (6)$$

By Theorem 2.3 it will follow that

$$|Z/T| = |\text{Gal}(\overline{K}|\overline{k})| = [\overline{K} : \overline{k}] = f. \quad (7)$$

Hence  $T$  has order  $e$ . In fact, the beautiful tower of extensions  $k \subset K_Z \subset K_T \subset K$  of (5)

$$n = [K : k] = [K : K_T] \cdot [K_T : K_Z] \cdot [K_Z : k] = e \cdot f \cdot g. \quad (8)$$

**Remark 3.1.** In the second equality of (7) we have tacitly assumed that  $\overline{K}$  is a Galois extension of  $\overline{k}$ . One can show in general that  $\overline{K}$  is a normal extension of  $\overline{k}$  [Z-S, p 292]. As for separability, since  $K$  and  $k$  are algebraic number fields and  $R', R$  their respective rings of integers,  $\overline{K}$  is a finite field of characteristic  $p$ , so by uniqueness of finite fields  $\overline{K} \cong \mathbb{F}_{p^m}$  for some  $m$ .  $\mathbb{F}_{p^m}$  consists of the roots of  $X^{p^m} - X$ , and this is a separable polynomial. So  $\overline{K}|\overline{k}$  is separable in our initial set-up.

To verify (6) we need another lemma.

**Lemma 3.2.** *Let  $K_Z$  be the decomposition field of a prime ideal  $\mathfrak{P}$  in  $R'$ . Define  $R_Z = R' \cap K_Z$  and  $\mathfrak{P}_Z = \mathfrak{P} \cap K_Z$ . Then  $\mathfrak{P}$  is the only prime ideal of  $R'$  lying over  $\mathfrak{P}_Z$ . Furthermore,  $R_Z/\mathfrak{P}_Z \cong R/\mathfrak{p}$  ( $= \overline{k}$ ).*

*Proof.* By definition of  $Z$ ,  $\mathfrak{P}$  is the only conjugate ideal of  $\mathfrak{P}$  in  $K_Z$ , so  $\mathfrak{P}$  is the only prime ideal of  $R'$  lying over  $\mathfrak{P}_Z$ . By Theorem 2.6 (using the ring  $R_Z$  as the starting Dedekind domain instead of  $R$ ), we have  $[K : K_Z] = e_Z f_Z$ , where  $e_Z$  is the ramification index of  $\mathfrak{P}$  over  $\mathfrak{P}_Z$  and  $f_Z$  the inertial degree of  $\mathfrak{P}$  over  $\mathfrak{P}_Z$ . We already know, however, that  $[K : K_Z] = ef$ , so  $ef = e_Z f_Z$ . By transitivity of the ramification index and the inertial degree, we have  $e_Z|e$  and  $f_Z|f$ , so  $e_Z = e$  and  $f_Z = f$ . Thus

$$[R'/\mathfrak{P} : R_Z/\mathfrak{P}_Z] = f_Z = f = [R'/\mathfrak{P} : R/\mathfrak{p}],$$

and it follows that  $R_Z/\mathfrak{P}_Z \cong R/\mathfrak{p}$ . □

**Theorem 3.3.** *With the above notation,  $Z/T \cong \text{Gal}(\overline{K}|\overline{k})$ .*

*Proof.* We will follow ideas set out in [R, p 222-3] for our proof. We will show there is a surjective homomorphism  $\Phi : Z \rightarrow \text{Gal}(\overline{K}|\overline{k})$  whose kernel is  $T$ . Every  $\sigma \in Z$  induces a map  $\bar{\sigma} : \overline{K} \rightarrow \overline{K}$  defined by  $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)}$  for  $x \in R'$ . One can check this is well-defined and is a  $R_Z/\mathfrak{P}_Z$ -automorphism. By Lemma 3.2,  $\bar{\sigma}$  determines a  $\overline{k}$ -automorphism, which we will also call  $\bar{\sigma}$  for simplicity.

Set  $\Phi(\sigma) = \bar{\sigma}$ . We must check  $\Phi$  is surjective. By the primitive element theorem there is an  $r \in R'$  such that  $\overline{K} = \overline{k}(\bar{r})$ . Let  $\tau$  be an element of  $\text{Gal}(\overline{K}|\overline{k})$ . Then  $\tau(\bar{r})$  is a conjugate of  $\bar{r}$  over  $\overline{k}$ .

Let  $f$  be the minimal polynomial of  $r$  over  $K_Z$ . Since  $K|K_Z$  is Galois with Galois group  $Z$ , we have  $f = \prod_{\sigma \in Z} (X - \sigma(r))$  [A, p. 553]. Note that  $r \in R'$  means  $\sigma(r) \in R'$  for  $\sigma \in Z$ , so  $f$  has coefficients in  $R' \cap K_Z = R_Z$ . We claim that  $\bar{f} = \prod (X - \overline{\sigma(r)})$  ‘lies in’  $\overline{k}[X]$ . Indeed, the quotient map  $R_Z \rightarrow R_Z/\mathfrak{P}_Z$  extends to the canonical map  $R' \rightarrow R'/\mathfrak{P} = \overline{K}$ . Since  $f$  has coefficients in  $R_Z$ ,  $\bar{f}$  has coefficients in  $R_Z/\mathfrak{P}_Z$ . So the image of  $\bar{f}$  under the identification of  $R_Z/\mathfrak{P}_Z$  with  $\overline{k}$  (Lemma 3.2) has coefficients in  $\overline{k}$ . We will write  $\bar{f}$  for this image for simplicity. (It is this image  $\bar{f}$  that lies in  $\overline{k}[X]$ .)

Since  $\bar{f}(\bar{r}) = 0$ , the conjugates of  $\bar{r}$  are roots of  $\bar{f}$ , so the minimal polynomial of  $\bar{r}$  over  $\overline{k}$  divides  $\bar{f}$ . Therefore, there is a  $\sigma \in Z$  such that  $\tau(\bar{r}) = \overline{\sigma(r)} = \bar{\sigma}(\bar{r})$ . Since  $\tau$  and  $\bar{\sigma}$  fix  $\overline{k}$  and they agree on the primitive element  $\bar{r}$ , they must be equal. Thus  $\sigma$  is the pre-image of  $\tau$  under  $\Phi$ , and  $\Phi$  is surjective.

Finally, every element  $\sigma \in T$  fixes  $\mathfrak{P}$ , so

$$\ker \Phi = \{\sigma \in Z \mid \bar{\sigma}(\bar{x}) = \bar{x} \quad \forall \bar{x} \in \overline{K}\} = T,$$

so  $Z/T \cong \text{Gal}(\overline{K}|\overline{k})$ , as claimed. □

With our initial set-up,  $\overline{K}$  is a finite-field extension of  $\overline{k}$  (see Remark 3.1). Let  $q$  be the number of elements in  $\overline{k}$ . The group  $\text{Gal}(\overline{K}|\overline{k})$  is cyclic and is generated by the Frobenius automorphism  $x \mapsto x^q$ . This observation yields a useful corollary to Theorem 3.3 that we will exploit in the proof of the Kronecker–Weber theorem.

**Corollary 3.4.**  *$Z/T$  is a cyclic group generated by the coset of  $\sigma \in G$  such that  $\sigma(x) \equiv x^q \pmod{\mathfrak{P}}$  for all  $x \in R'$ .* □

Before moving on to the theory of higher ramification groups, we present a theorem which ties together much of the material in this section and is crucial to our proof of the Kronecker–Weber theorem. It is an analogue of Lemma 3.2 for inertial fields.

We have shown so far, that under our initial set-up, if  $\mathfrak{p}$  is a prime ideal of  $R$ , then  $\mathfrak{p}R' = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ , where the  $\mathfrak{P}_i$  are the prime ideals of  $R'$  lying over  $\mathfrak{p}$  (conjugate by elements of  $G$ ) and  $efg = n$ . If  $e = n$ , we say  $\mathfrak{p}$  is *totally ramified* in  $K|k$ , or equivalently, any of the  $\mathfrak{P}_i$  is totally unramified over  $\mathfrak{p}$ .

**Theorem 3.5.** *Let  $\mathfrak{P}$  be a prime ideal of  $R'$  lying over a prime ideal  $\mathfrak{p}$  of  $R$ , and let  $K_T$  be its inertia field. Define  $R_T = R' \cap K_T$  and  $\mathfrak{P}_T = \mathfrak{P} \cap K_T$ . If  $\overline{K}$  is a separable extension of  $\overline{k}$ , then  $\mathfrak{P}_T$  is unramified over  $\mathfrak{p}$  (i.e.,  $\mathfrak{p}$  is unramified in  $K_T|k$ ), and  $\mathfrak{P}$  is totally ramified over  $\mathfrak{P}_T$  (i.e.,  $\mathfrak{P}$  is totally ramified in  $K|K_T$ ). Furthermore,  $R_T/\mathfrak{P}_T \cong R'/\mathfrak{P} (= \overline{K})$ .*

*Proof.* If  $\bar{K}$  is a separable extension of  $\bar{k}$ , then, on the one hand,  $[K : K_T] = e$  by (8) and Remark 3.1. On the other hand, by Theorem 2.6 (applied to  $R_T$  as our starting Dedekind domain instead of  $R$ ),  $[K : K_T] = e_T f_T$ , where  $e_T$  is the ramification index of  $\mathfrak{P}$  over  $\mathfrak{P}_T$  and  $f_T$  the inertial degree of  $\mathfrak{P}$  over  $\mathfrak{P}_T$ .

We claim  $f_T = 1$ , i.e.,  $[R'/\mathfrak{P} : R_T/\mathfrak{P}_T] = 1$ . Consider the Galois extension  $K|K_T$ . The inertia group  $Z(K|K_T)$  of  $\mathfrak{P}$  in this extension consists of elements  $\sigma$  of  $\text{Gal}(K|K_T) = T$  such that  $\sigma(\mathfrak{P}) = \mathfrak{P}$ . But this is all of  $T$ , i.e.,  $Z(K|K_T) = T$ . By Theorem 3.3 applied to  $Z(K|K_T)$  and  $T(K|K_T)$  it follows that  $\text{Gal}((R'/\mathfrak{P})|(R_T/\mathfrak{P}_T)) = Z(K|K_T)/T(K|K_T) = Z(K|K_T)/T = \{1\}$ . Hence  $[R'/\mathfrak{P} : R_T/\mathfrak{P}_T] = 1$ , and since  $R_T/\mathfrak{P}_T \subset R'/\mathfrak{P}$ ,  $R_T/\mathfrak{P}_T = R'/\mathfrak{P}$ .

Since  $f_T = 1$ ,  $e_T = e$ , so  $\mathfrak{P}$  is totally ramified over  $\mathfrak{P}_T$ . By transitivity of the ramification index,  $\mathfrak{P}_T$  must be unramified over  $\mathfrak{p}$ .  $\square$

### 3.2 Higher Ramification Groups

Given a non negative integer  $m$  we define the  $m^{\text{th}}$  *ramification group* of a prime ideal  $\mathfrak{P}$  of  $R'$  as

$$V_m = \{\sigma \in G \mid \sigma(x) \equiv x \pmod{\mathfrak{P}^m} \quad \forall x \in R'\}.$$

The first ramification group is the inertia group of  $\mathfrak{P}$ . These groups form a descending chain of subgroups of  $G$ ,  $T = V_1 \geq V_2 \geq \dots \geq V_m$  that terminates at the identity at a finite  $m$ . Indeed, since  $\bigcap_{i=0}^{\infty} \mathfrak{P}^i = 0$ , the intersection of all ramification groups must be the trivial group. Since  $G$  is a finite group,  $V_m$  must reduce to the identity for large enough  $m$ . One should verify that the ramification groups are normal subgroups of  $Z$ , the decomposition group of  $\mathfrak{P}$  [Z-S, p 294].

We are interested in the successive quotient groups  $V_i/V_{i+1}$ , as these are important to the proof of the Kronecker–Weber theorem. We know much about their structure, which we will explore in the following theorem.

Recall that under our initial set-up  $\bar{K}$  is a separable extension of  $\bar{k}$  (see Remark 3.1).

**Theorem 3.6.** *Let  $\mathfrak{P}$  be a prime ideal of  $R'$  (lying over a prime ideal  $\mathfrak{p}$  of  $R$ ), and let  $T = V_1 \geq V_2 \geq \dots \geq V_m$  be the ramification groups associated to  $\mathfrak{P}$ . If  $\bar{K}$  is a separable extension of  $\bar{k}$ , the group  $T/V_2$  is isomorphic to a subgroup of the multiplicative group  $K^\times = k \setminus 0$ , and  $V_i/V_{i+1}$  is isomorphic to an additive subgroup of the structure of  $\bar{K}$ , for  $i \geq 2$ .*

*Proof.* Suppose first that  $\mathfrak{P}$  is a principal ideal generated by some element  $b$ . Then  $\sigma(b) \in \mathfrak{P} \setminus \mathfrak{P}^2$  for  $\sigma \in T$ . Indeed, if  $\sigma(b) \in \mathfrak{P}^2$ , then  $\sigma^{-1}(\sigma(b)) \in \mathfrak{P}^2$ , so  $b \in \mathfrak{P}^2$ , which is absurd since  $\mathfrak{P} = (b)$ . Hence  $\sigma(b) = x_\sigma b$  for some  $x_\sigma \in R' \setminus \mathfrak{P}$ . One can check that for  $\tau \in T$ ,  $x_{\sigma\tau} \equiv x_\sigma x_\tau \pmod{\mathfrak{P}}$  so that  $\bar{x}_{\sigma\tau} = \bar{x}_\sigma \bar{x}_\tau$  in  $\bar{K}$ . This means the map  $\sigma \mapsto \bar{x}_\sigma$  is a homomorphism from  $T$  into a multiplicative subgroup of  $\bar{K}^\times$ . The kernel of this homomorphism consists of the automorphisms  $\sigma \in T$  such that  $\bar{x}_\sigma = 1$ , i.e.,  $\sigma(b) - b \in \mathfrak{P}^2$ . We will deal with this kernel shortly.

For the higher ramification groups ( $i \geq 2$ ),  $\sigma(b) - b \in \mathfrak{P}^i$  for  $\sigma \in V_i$ , so that  $\sigma(b) - b = y_\sigma b^i$  for some  $y_\sigma \in R'$ . One may verify that for  $\tau \in V_i$ ,  $y_{\sigma\tau} \equiv y_\sigma + y_\tau \pmod{\mathfrak{P}}$ , so that  $\bar{y}_{\sigma\tau} = \bar{y}_\sigma + \bar{y}_\tau$

in  $\overline{K}$ . This time the map  $\sigma \mapsto \bar{y}_\sigma$  is a homomorphism of  $V_i$  into an additive subgroup of  $\overline{K}$ . The kernel of this homomorphism consists of automorphisms  $\sigma \in V_i$  such that  $\bar{y}_\sigma = 0$ , i.e.,  $\sigma(b) - b \in \mathfrak{P}^{i+1}$ .

Now we deal with the kernels of both situations at once. We know so far they consist of elements  $\sigma \in V_i$  such that  $\sigma(b) - b \in \mathfrak{P}^{i+1}$  for  $i \geq 1$ . We want to show this set is the group  $V_{i+1}$ , i.e., that  $\sigma(x) - x \in \mathfrak{P}^{i+1}$  for all  $x \in R'$ , and not just for  $b$ . Since  $\overline{K}$  is separable over  $\bar{k}$ , Theorem 3.5 tells us  $R_T/\mathfrak{P}_T \cong R'/\mathfrak{P} (= \overline{K})$ . So for  $x \in R'$ ,  $x = y + z$  where  $y \in R_T$  and  $z \in \mathfrak{P}$ . Furthermore, for  $\sigma \in V_i$

$$\sigma(x) - x = \sigma(y) - y + \sigma(z) - z,$$

but  $\sigma(z) - z \in \mathfrak{P}^{i+1}$  since  $z \in (b) = \mathfrak{P}$ , and  $\sigma(y) - y = 0$  since  $\sigma \in V_i \leq T$ . Therefore  $\sigma(x) - x \in \mathfrak{P}^{i+1}$  for all  $x \in R'$ , as desired. This establishes the theorem for the case when  $\mathfrak{P}$  is a principal ideal.

Now we will argue that we can always reduce to the principal ideal case. We start by localizing  $R'$  at  $\mathfrak{P}$ . The local ring  $R'_\mathfrak{P}$  is still a Dedekind domain and its only proper maximal (hence prime) ideal is  $\mathfrak{P}R'_\mathfrak{P}$ . A Dedekind domain with a finite number of proper prime ideals is a PID (see for example [Z-S, V Theorem 16]). Thus  $\mathfrak{P}R'_\mathfrak{P}$  is a principal ideal.

Let  $V_i^{(\mathfrak{P})}$  denote the  $i^{\text{th}}$  ramification group of  $\mathfrak{P}R'_\mathfrak{P}$ . From what we have shown so far,  $T^{(\mathfrak{P})}/V_2^{(\mathfrak{P})}$  is isomorphic to a multiplicative subgroup of  $(R'_\mathfrak{P}/\mathfrak{P}R'_\mathfrak{P})^\times$  and  $V_i^{(\mathfrak{P})}/V_{i+1}^{(\mathfrak{P})}$  is isomorphic to an additive subgroup of  $R'_\mathfrak{P}/\mathfrak{P}R'_\mathfrak{P}$ .

One can verify that  $R'_\mathfrak{P}/\mathfrak{P}R'_\mathfrak{P} \cong R'/\mathfrak{P}$ . We claim that  $V_i^{(\mathfrak{P})} = V_i$ . This is enough to establish the theorem. The inclusion  $V_i \subset V_i^{(\mathfrak{P})}$  is easy. Let  $t$  be a generator of the principal ideal  $\mathfrak{P}R'_\mathfrak{P}$ . Then  $\sigma(t) - t \in \mathfrak{P}^i R'_\mathfrak{P}$  for  $\sigma \in V_i^{(\mathfrak{P})}$ . To see that  $V_i^{(\mathfrak{P})} \subset V_i$  we want to show  $\sigma(x) - x \in \mathfrak{P}^i$  for all  $x \in R'$ . One may write  $x$  as  $\sum_{j=0}^{e-1} a_j t^j$  where  $a_j \in K_T$  [R, p 225-6]. Then

$$\sigma(x) - x = \sum_{j=0}^{e-1} a_j (\sigma(t)^j - t^j).$$

Now,  $\sigma(t) - t \mid \sigma(t)^j - t^j$  for  $j = 1, \dots, e-1$ . Since  $\sigma(t) - t \in \mathfrak{P}^i R'_\mathfrak{P}$ , then also  $\sigma(t)^j - t^j \in \mathfrak{P}^i R'_\mathfrak{P}$ . Hence  $\sigma(x) - x \in R' \cap \mathfrak{P}^i R'_\mathfrak{P} = \mathfrak{P}^i$ .  $\square$

The following easy corollary of Theorem 3.6 is perhaps more important than the theorem itself.

**Corollary 3.7.** *With the notation of Theorem 3.6,  $T/V_2$  is cyclic and  $V_i/V_{i+1}$  is trivial or is a direct product of cyclic groups of order  $p$ , where  $p$  is the characteristic of  $R/\mathfrak{p}$ .  $\square$*

What is known about the size of  $T/V_2$ ? Since it is a subgroup of the multiplicative group  $(R'/\mathfrak{P})^\times$ , if  $q$  is the number of elements of  $R/\mathfrak{p}$ , then the order of  $T/V_2$  divides  $q^f - 1$ . If, however,  $Z/V_2$  is an abelian group (as is the case when the Galois extension  $K|k$  is abelian) then we can obtain a much better bound on the size of  $T/V_2$ .

**Theorem 3.8.** *Let  $\mathfrak{P}$  be a prime ideal of  $R'$  (lying over  $\mathfrak{p}$  in  $R$ ), and let  $Z$ ,  $T$ , and  $V_2$  denote the decomposition group and first two ramification groups of  $\mathfrak{P}$ , respectively. If  $Z/V_2$  is abelian, then  $T/V_2$  has order dividing  $q - 1$ , where  $q = \#(R/\mathfrak{p})$ .*

*Proof.* In the proof to Theorem 3.6 we showed that ramification groups remain unchanged if we localize  $R'$  at  $\mathfrak{P}$ . One can show that  $Z$  also remains unchanged. Thus, we may assume  $\mathfrak{P}$  is a principal ideal generated by some element  $t$ .

Given  $\sigma \in Z$ ,  $\sigma(t) = x_\sigma t$  for some  $x_\sigma \in R' \setminus \mathfrak{P}$  (see the proof to Theorem 3.6). Theorem 3.3 tells us  $Z/T \cong \text{Gal}(\overline{K}|\overline{k})$ ; let  $\sigma \in Z$  induce the coset of the Frobenius automorphism  $x \mapsto x^q$  that generates  $\text{Gal}(\overline{K}|\overline{k})$ . Let  $\tau \in T$  be such that its coset in  $V_2$  generates  $T/V_2$ . Thus

$$\sigma(t) = x_\sigma t, \quad \tau(t) = x_\tau t, \quad \text{and} \quad \sigma\tau\sigma^{-1}(t) = x_{\sigma\tau\sigma^{-1}}t.$$

A straightforward calculation shows that  $x_{\sigma\tau\sigma^{-1}} = \sigma\tau\sigma^{-1}(x_\sigma)^{-1}\sigma(x_\tau)x_\sigma$ . Now reduce this equation mod  $\mathfrak{P}$ . Notice that  $\tau$  reduces to the identity and that  $\bar{\sigma}(\bar{x}_\tau) = \sigma(x_\tau) = \bar{x}_\tau^q$ . Hence  $\bar{x}_{\sigma\tau\sigma^{-1}} = \bar{x}_\tau^q$ . Since  $Z/V_2$  is abelian,  $\bar{x}_{\sigma\tau\sigma^{-1}} = \bar{x}_\tau$ . This means  $\bar{x}_\tau^{q-1} = 1$ , i.e., the order of  $T/V_2$  divides  $q - 1$ .  $\square$

## 4 Back to the Kronecker–Weber theorem

### 4.1 Ramification in extensions of $\mathbb{Q}$

We are almost ready to take another stab at the Kronecker–Weber theorem. We reduced the theorem to the case when the degree of the abelian extension  $K$  over  $\mathbb{Q}$  is a prime power  $p^r$ . We will now further reduce to the case where all primes other than  $p$  do not ramify in  $K$ . Before we do this, however, we state, without proof, a theorem of Minkowski that guarantees the existence of at least one ramified prime in  $K$  [R, p. 202].

**Theorem (Minkowski).** In a finite, non-trivial extension  $K$  of  $\mathbb{Q}$ , there is at least one prime that ramifies. Furthermore, only finitely many primes ramify.

In fact, the only primes that ramify are the ones that divide the different of  $K|\mathbb{Q}$  [Z-S, p 303](see Section 4.3 for a discussion of the different). For a cyclotomic extension  $\mathbb{Q}(\zeta_m)$ , these are the primes that divide  $m$ .

### 4.2 One Ramified Prime is Enough

**Theorem 4.1.** *Let  $K$  be an abelian extension of  $\mathbb{Q}$  of prime power degree  $p^r$  with Galois group  $G$ . To prove the Kronecker–Weber theorem, it suffices to show  $K$  is cyclotomic under the additional hypothesis that  $p$  is the only ramified prime in  $K$ .*

*Proof.* Suppose  $\lambda \neq p$  is ramified in  $K$ . We will show there is a subfield  $L$  of  $\mathbb{Q}(\zeta_\lambda)$  and a field  $K'$  such that  $KL = K'L$ , and where  $\lambda$  is unramified in  $K'$ . If  $K'$  is cyclotomic, then  $K$  will be cyclotomic too. By Minkowski’s Theorem only finitely many primes ramify in  $K$ , so we can ‘remove’ all of them (except  $p$ ) by this process.

Since  $\lambda \neq p$ , all higher ramification groups of an ideal  $\mathfrak{P}$  in  $\mathfrak{O}_K$  lying over  $\lambda$  are trivial. Indeed,  $\lambda$  does not divide the order of any subgroup of  $G$ , and by Corollary 3.7  $V_i/V_{i+1}$  is a direct product of cyclic groups of order  $p$  for  $i \geq 2$ , so  $V_i$  is trivial for  $i \geq 2$ . The inertia group  $T$  has order  $p^m$  for some  $m \leq r$ . By Theorem 3.8 (with  $R = \mathbb{Z}$ ),

$$\lambda - 1 \equiv 0 \pmod{p^m}. \quad (9)$$

The Galois group of  $\mathbb{Q}(\zeta_\lambda)$  is cyclic of degree  $\lambda - 1$ . By (9), there exists a subfield  $L$  of  $\mathbb{Q}(\zeta_\lambda)$  which is a cyclic extension of  $\mathbb{Q}$  of degree  $p^m$ .

Let  $H = \text{Gal}(L|\mathbb{Q})$ . The composite  $KL$  is a Galois extension of  $\mathbb{Q}$  of degree  $p^{r+s}$ ,  $s \leq m$ , and its Galois group is isomorphic to a subgroup of  $G \times H$ .

Let  $\mathfrak{P}'$  be a prime ideal in  $KL$  lying over  $\mathfrak{P}$ ,  $T'$  the inertia group of  $\mathfrak{P}'$  over  $\lambda$  (i.e.,  $T' = T(KL|\mathbb{Q})$ ). For  $\sigma \in T'$ ,  $\sigma|_K \in T$ , and so  $T' \leq T \times H$ . The order of  $T'$  is at least  $p^m$  since

$$p^m = |T| = e(\mathfrak{P}|\mathfrak{p}) \leq e(\mathfrak{P}'|\mathfrak{p}) = |T'|.$$

As before, all higher ramification groups of  $\mathfrak{P}'$  are trivial, so  $T'$  must be cyclic by Corollary 3.7. No element of  $T \times H$ , however, has order greater than  $p^m$  since  $|T| = |H| = p^m$ . Hence  $|T'| = p^m$ .

Let  $K'$  be the fixed field of  $T'$  and let  $\mathfrak{P}'' = \mathfrak{P}' \cap K'$ . Then  $\lambda$  no longer ramifies in  $K'$ , since, by Theorem 3.5  $\mathfrak{P}''$  is unramified over  $\lambda$ . Furthermore, since  $\mathfrak{P}'' \cap L$  is unramified over  $\lambda$ , i.e.,  $\lambda$  does not ramify in  $K' \cap L$  because it does not ramify in  $K'$ . We may also check that  $\mathfrak{P}'' \cap L$  is also totally ramified over  $\lambda$ . It follows that  $[K' \cap L : \mathbb{Q}] = e(\mathfrak{P}'' \cap L|\mathbb{Q}) = 1$ , so that  $K' \cap L = \mathbb{Q}$  so  $[K'L : \mathbb{Q}] = [L : \mathbb{Q}] \cdot [K' : \mathbb{Q}]$ .

Now, because  $[KL : K'] = p^m = [L : \mathbb{Q}]$  it follows that

$$[K'L : \mathbb{Q}] = [L : \mathbb{Q}] \cdot [K' : \mathbb{Q}] = [KL : K'] \cdot [K' : \mathbb{Q}] = [KL : \mathbb{Q}],$$

and since  $K'L \subset KL$ , we conclude  $K'L = KL$ . Finally, no new primes ramify in  $K'$ . Otherwise, this prime would ramify in  $KL$ , and an isomorphic copy of the inertia group of an ideal lying over this prime would be contained in the direct product of the inertia groups of this prime in  $K$  and  $L$ . Since this prime did not ramify in  $K$  or  $L$  (recall  $\lambda$  is the only prime that ramifies in  $\mathbb{Q}(\zeta_\lambda)$ , *a fortiori*, in  $L$ ) both these inertia groups are trivial.  $\square$

It remains to prove that the Kronecker–Weber theorem holds for abelian extensions  $K$  of  $\mathbb{Q}$  of prime power degree  $p^r$  where  $p$  is the only ramified prime. We will consider two separate cases, according to the parity of  $p$ . For odd primes, we need to use a couple of facts from the theory of differentials of extensions. We will present those facts without proof, though references will be provided.

### 4.3 And now for something completely different<sup>1</sup>

We use the set-up of Lemma 2.4, which we will restate for convenience. Let  $R$  be a Dedekind domain,  $k$  its field of fractions,  $K$  a finite separable algebraic extension of  $k$  of degree  $n$  and

---

<sup>1</sup>Monty Python

$R'$  the integral closure of  $R$  in  $K$ . Now, let  $M$  be a subset of  $K$ . Define the complementary set  $M^*$  of  $M$  with respect to  $R$  as

$$M^* = \{x \in K \mid \text{Tr}(xy) \in R \ \forall y \in M\}.$$

One may verify that  $R'^*$  is a fractional ideal of  $R'$ . The *different* of  $R'$  over  $R$  is defined as the inverse of this fractional ideal, and is denoted  $\Delta(R'|R)$ . This particular different is also called *the different of  $K|k$*  and is denoted  $\Delta(K|k)$ .

If  $\mathfrak{p}$  is a prime ideal of  $R$ , we may form the rings of quotients  $M^{-1}R := R_M$  and  $M^{-1}R' := R'_M$ , where  $M = R \setminus \mathfrak{p}$ . Both rings are still Dedekind domains [Z-S, p. 270]. The different  $\Delta(R'_M|R_M)$  is called *the different of  $L|K$  above  $\mathfrak{p}$*  and is denoted  $\Delta_{\mathfrak{p}}(L|K)$ .

If  $K$  is a Galois extension of  $k$ , and  $\mathfrak{p}$  has only one prime ideal  $\mathfrak{P}$  lying above it, then  $\Delta_{\mathfrak{p}}(K|k) = R'_{\mathfrak{P}}\mathfrak{P}^s$ , where  $R'_{\mathfrak{P}}$  is the ring  $R'$  localized at  $\mathfrak{P}$  and  $s$  is a non-negative integer, called the exponent of  $\mathfrak{P}$  of the different  $\Delta_{\mathfrak{p}}(K|k)$ . It is sometimes denoted  $s_{\mathfrak{p}}(K|k)$  [R, p 230].

We will require the following three facts about differentials.

**Theorem 4.2 (Transitivity of the different).** *With the set-up of Lemma 2.4, let  $L$  be a separable extension of finite degree of  $K$ , and let  $R''$  be a Dedekind domain whose field of fractions is  $L$  and is also the integral closure of  $R'$  in  $L$ . Then*

$$\Delta(R''|R) = R''\Delta(R'|R) \cdot \Delta(R''|R').$$

See [R, p 209].

**Theorem 4.3 (Hilbert's formula).** *Let  $K$  be a Galois extension of  $k$ , and suppose the prime ideal  $\mathfrak{p}$  of  $R$  has only one prime ideal  $\mathfrak{P}$  lying above it. If  $\mathfrak{P}$  is totally ramified over  $\mathfrak{p}$  then*

$$s_{\mathfrak{p}}(K|k) = \sum_{i=0}^{r-1} (|V_i| - 1),$$

where  $V_i$  is the  $i^{\text{th}}$  ramification group of  $\mathfrak{P}$ . See [R, p 230].

**Theorem 4.4.** *Let  $K$  be an abelian extension of  $\mathbb{Q}$  with ring of integers  $R'$ , and  $H$  an intermediate field between  $\mathbb{Q}$  and  $K$  such that  $[H : \mathbb{Q}] = p$ , a prime number. If  $C$  is the ring of integers of  $H$ ,  $\mathfrak{P}$  a prime ideal of  $R'$  lying above  $p$  (which can be shown to be unique in this case), and  $\mathfrak{P}' = \mathfrak{P} \cap C$ , then*

$$s_{\mathfrak{P}'}(H|\mathbb{Q}) = 2(p - 1)$$

which is independent of the field  $H$ . See [R, p 234].

#### 4.4 Odd prime numbers

Let  $K$  be an abelian extension of  $\mathbb{Q}$  of degree  $p^r$ , where  $p$  is an odd prime and is the only prime which ramifies in  $K$ . Let  $G$  be its Galois group,  $\mathfrak{P}$  a prime ideal lying over  $p$  and  $V_i$  its  $i^{\text{th}}$  ramification group. We will show  $K$  is cyclotomic in two steps.

**Lemma 4.5.** *With the above notation,  $K$  is a cyclic extension of  $\mathbb{Q}$ .*

*Proof.* By Theorem 3.5,  $p$  is unramified in  $K_T$ . This means no primes ramify in  $K_T$ , so by Minkowski's theorem,  $K_T = \mathbb{Q}$ , and so  $G = T$ . It follows that

$$e = |T| = |G| = [K : \mathbb{Q}] = efg.$$

Hence  $\mathfrak{P}$  is totally ramified in  $K|\mathbb{Q}$  and  $[\overline{K} : \overline{k}] = f = 1$ , i.e.,  $\overline{K}$  is a finite field with  $p$  elements since  $\overline{k} = \mathbb{Z}/p\mathbb{Z}$  in this case. By Theorem 3.8  $T = V_2$  because  $p \nmid p-1$ .

Let  $l$  be the smallest index for which  $V_l \neq G$ . Let  $K_{V_l}$  denote the fixed field of  $V_l$ . We claim that  $[K_{V_l} : \mathbb{Q}] = p$  and that  $K_{V_l}$  is the only extension field of  $\mathbb{Q}$  of degree  $p$  contained in  $K$ .

We have  $[K_{V_l} : \mathbb{Q}] = |V_{l-1}/V_l|$ . By Corollary 3.7  $V_{l-1}/V_l$  is either trivial or a direct product of cyclic groups of order  $p$ . But  $V_{l-1}/V_l$  is an additive subgroup of  $\overline{K}$ ,  $|\overline{K}| = p$  and  $V_{l-1} \neq V_l$ , so that  $V_{l-1}/V_l$  is cyclic of order  $p$ . Hence  $[K_{V_l} : \mathbb{Q}] = p$ .

To see why  $K_{V_l}$  is unique, suppose there exists another intermediate extension  $H$  such that  $[H : \mathbb{Q}] = p$ . We will arrive at a contradiction through a computation of the different  $\Delta_\lambda(K|K_{V_l})$  and  $\Delta_\lambda(H|\mathbb{Q})$ .

Let  $H' = \text{Gal}(K|H)$  and let  $V'_i$  be the  $i^{\text{th}}$  ramification group of  $\mathfrak{P}$  in the extension  $K|H$ , i.e.,  $V'_i = V_i \cap H'$ . Then  $V'_1 = \cdots = V'_{l-1} = H'$  since  $V_1 = \cdots = V_{l-1} = G$ ,  $V'_i \subset V_i$  for  $i \geq l+1$ , and  $V'_i \subsetneq V_i$ , because if  $V'_i = V_i$  then  $V_i = H'$  and  $K_{V_l} = H$ . Similarly, let  $V''_i$  be the  $i^{\text{th}}$  ramification group of  $\mathfrak{P}$  in the extension  $K|K_{V_l}$ , i.e.,  $V''_i = V_i \cap V_l$ . Then  $V''_1 = \cdots = V''_l = V_l$  and  $V''_i = V_i$  for  $i \geq l+1$ .

Since  $|H'| = |V_l| = |G|/p$ , Hilbert's formula for the different tells us that

$$s_{\mathfrak{P}}(K|K_{V_l}) = \sum_{i=0}^{r-1} (|V''_i| - 1) > \sum_{i=0}^{r-1} (|V'_i| - 1) = s_{\mathfrak{P}}(K|H).$$

By the transitivity of the different we have

$$\begin{aligned} \Delta_{\mathfrak{P}}(K|\mathbb{Q}) &= R'_{\mathfrak{P}} \Delta_{\mathfrak{P}_1}(K_{V_l}|\mathbb{Q}) \cdot \Delta_{\mathfrak{P}}(K|K_{V_l}) \\ &= R'_{\mathfrak{P}} \Delta_{\mathfrak{P}_2}(H|\mathbb{Q}) \cdot \Delta_{\mathfrak{P}}(K|H) \end{aligned}$$

where  $\mathfrak{P}_1 = \mathfrak{P} \cap K_{V_l}$  and  $\mathfrak{P}_2 = \mathfrak{P} \cap H$ . Since  $\mathfrak{P}$  is totally ramified in  $K|\mathbb{Q}$  and  $[H : \mathbb{Q}] = [K_{V_l} : \mathbb{Q}] = p$ , by Theorem 4.4, the exponents of  $R'_{\mathfrak{P}} \Delta_{\mathfrak{P}_1}(K_{V_l}|\mathbb{Q})$  and  $R'_{\mathfrak{P}} \Delta_{\mathfrak{P}_2}(H|\mathbb{Q})$  are equal. Therefore

$$s_{\mathfrak{P}}(K|K_{V_l}) = s_{\mathfrak{P}}(K|H),$$

which is a contradiction. The result of this whole computation is simply that  $K_{V_l}$  is the unique extension field of  $\mathbb{Q}$  of degree  $p$  contained in  $K$ .

By the fundamental Galois correspondence,  $G$  has only one subgroup of order  $p^{r-1}$ . It is not a hard exercise in group theory to show this means  $G$  is cyclic.  $\square$

**Theorem 4.6.** *Let  $K$  be an abelian extension of  $\mathbb{Q}$  of degree  $p^r$ , where  $p$  is an odd prime, with  $G$  its Galois group. Then  $K$  is cyclotomic.*

*Proof.* By Theorem 4.1 and Minkowski's Theorem, we may assume  $p$  is the only ramified prime in  $K$ .

Let  $\zeta$  be a primitive  $p^{r+1}$  root of unity. Recall that  $\mathbb{Q}(\zeta)$  has a cyclic Galois group over  $\mathbb{Q}$  of order  $p^r(p-1)$ , and that  $p$  is the only ramified prime in  $\mathbb{Q}(\zeta)$ . Let  $K'$  be the unique subfield of  $\mathbb{Q}(\zeta)$  of degree  $p^r$  over  $\mathbb{Q}$  and let  $G'$  be its Galois group. *A fortiori*,  $p$  is the only ramified prime in  $K'$ .

Suppose  $K$  and  $K'$  are not equal. Consider the composite  $KK'$ . The only ramified prime in  $KK'$  is  $p$  and  $[KK' : \mathbb{Q}] > p^r$ . Lemma 4.5 tells us  $KK'$  is a cyclic extension of  $\mathbb{Q}$ . However, its Galois group is isomorphic to a subgroup of  $G \times G'$ , and no element of this group has order greater than  $p^r$ . This is a contradiction. Therefore,  $K$  coincides with the *cyclotomic* extension  $K'$  of  $\mathbb{Q}$ .  $\square$

#### 4.5 Even prime numbers

It remains to show the Kronecker–Weber theorem holds for abelian extensions  $K|\mathbb{Q}$  of degree  $2^r$ , where 2 is the only ramified prime. We will use induction on  $r$ . To establish the base case, we will use a Gauss sum, following [Lang, VI §3].

**Lemma 4.7.** *Let  $p$  be a prime number and  $\left(\frac{\cdot}{p}\right)$  denote the usual Legendre symbol and let*

*$S = \sum_{\nu} \left(\frac{\nu}{p}\right) \zeta_p^{\nu}$ , where  $\nu$  runs across residue classes mod  $p$ . Then*

$$S^2 = \left(\frac{-1}{p}\right)p.$$

*Proof.* Using the well-known properties of the Legendre symbol, we compute

$$S^2 = \sum_{\nu, \mu} \left(\frac{\nu}{p}\right) \left(\frac{\mu}{p}\right) \zeta^{\nu+\mu} = \sum_{\nu, \mu} \left(\frac{\nu\mu}{p}\right) \zeta^{\nu+\mu}.$$

As  $\nu$  runs through residue classes, so does  $\nu\mu$ , so

$$\begin{aligned} S^2 &= \sum_{\nu, \mu} \left(\frac{\nu\mu^2}{p}\right) \zeta^{\mu(\nu+1)} = \sum_{\nu, \mu} \left(\frac{\nu}{p}\right) \zeta^{\mu(\nu+1)}. \\ &= \sum_{\mu} \left(\frac{-1}{p}\right) \zeta^0 + \sum_{\nu \neq 1} \left(\frac{\nu}{p}\right) \cdot \underbrace{\sum_{\mu} \zeta^{\mu(\nu+1)}}_{-1}. \\ &= \left(\frac{-1}{p}\right)(p-1) + (-1) \sum_{\nu \neq 1} \left(\frac{\nu}{p}\right) = p \left(\frac{-1}{p}\right). \end{aligned}$$

$\square$

**Lemma 4.8.** *Every quadratic extension of  $\mathbb{Q}$  is abelian.*

*Proof.* Let  $\mathbb{Q}(\sqrt{a/b})$  be the quadratic extension we are interested in, with the fraction  $a/b$  in lowest terms. This extension is contained in the field obtained by adjoining the square roots of the prime factors of  $a$ ,  $b$  and  $-1$ . By Lemma 4.7, either  $p$  or  $-p$  is a square in  $\mathbb{Q}(\zeta_p)$  (for the case  $p = 2$ , note  $(1+i)^2 = 2i$ , so  $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ ). Our quadratic extension is therefore contained in the composite  $\mathbb{Q}(i) \prod \mathbb{Q}(\zeta_p)$ , where  $p$  runs across the prime factors of  $a$  and  $b$ , and this is a cyclotomic extension. So  $\mathbb{Q}(\sqrt{a/b})$  is itself cyclotomic.  $\square$

**Theorem 4.9.** *Let  $K$  be an abelian extension of  $\mathbb{Q}$  of degree  $2^r$ , with Galois group  $G$ . Then  $K$  is cyclotomic.*

*Proof.* As advertised, we will use induction on  $r$ . Lemma 4.8 establishes the base case. By Theorem 4.1 and Minkowski's Theorem, we may assume 2 is the only ramified prime in  $K$ .

Since  $G$  is a cyclic group,  $K$  has a unique quadratic subfield  $K'$ . In fact, if  $K'$  is real,  $K' = \mathbb{Q}(\sqrt{2})$  since 2 is the only ramified prime in  $K$  [Weiss, p. 235]. Otherwise, we may embed  $K$  in the field  $\mathbb{C}$  of complex numbers. The group generated by complex conjugation has a fixed field of degree at least  $2^{r-1}$  over  $\mathbb{Q}$ , and all its subfields must be real. So  $K' = \mathbb{Q}(\sqrt{2})$  in this case as well.

Now let  $\zeta$  be a  $2^{r+2}$  primitive root of unity. The unique quadratic subfield of  $\mathbb{Q}(\zeta)$  is  $\mathbb{Q}(\sqrt{2})$  because it satisfies the same hypotheses as  $K$ . Let  $L = \mathbb{Q}(\zeta + \zeta^{-1})$ . By (1),  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^{r+1}$ . It follows that  $[KL : \mathbb{Q}] < 2^{2r}$ , so  $\text{Gal}(KL|\mathbb{Q}) \leq G \times H$ , where  $H = \text{Gal}(L|\mathbb{Q})$ . Both  $G$  and  $H$  are cyclic; let  $\sigma$  and  $\tau$  be their respective generators chosen so that they agree on  $L \cap K$ . Then  $(\sigma, \tau) \in \text{Gal}(KL|\mathbb{Q})$  generates a subgroup  $G'$  of order  $2^r$ . The fixed field  $F$  of this group in  $KL$  has degree  $2^m$  over  $\mathbb{Q}$ ,  $m < r$ , and 2 is still the only ramified prime in  $F$ .  $F$  is cyclotomic by inductive hypothesis.

Furthermore,  $FL = KL$ . To see why this is true, notice first that  $FL \subset KL$ . Now suppose there exists  $\alpha \in \text{Gal}(KL|\mathbb{Q})$  that fixes the field  $FL$ . Then  $\alpha$  fixes both  $F$  and  $L$ . Since it fixes  $F$ , it is in  $G'$ . But  $G' = \langle (\sigma, \tau) \rangle$ , so  $\alpha = (\sigma^i, \tau^i)$  for some  $i$ . Since  $\alpha$  fixes  $L$ ,  $\tau^i$  must be the identity. However,

$$|\langle \sigma \rangle| = |G| = |H| = |\langle \tau \rangle|,$$

so  $\sigma^i$  must also be the identity. Therefore the only automorphism of  $KL$  fixing  $FL$  is the identity. It follows that  $FL = KL$ . Since both  $F$  and  $L$  are cyclotomic,  $K$  is also cyclotomic.  $\square$

This completes the proof of the Kronecker–Weber theorem.

## References

- [A] M. Artin, *Algebra* Prentice Hall, New Jersey, 1991.
- [G] M. J. Greenberg, “An Elementary Proof of the Kronecker–Weber Theorem” *Amer. Math. Monthly* **81** (1974) 601-607.

- [Ge] M. J. Greenberg, “Correction to ‘An Elementary Proof of the Kronecker–Weber Theorem’” *Amer. Math. Monthly* **82** (1975) 803.
- [Lang] S. Lang, *Algebra* Third Edition. Addison-Wesley, Reading, MA, 1993.
- [Long] R. Long, *Algebraic Number Theory* Marcel Dekker, New York, 1977.
- [R] P. Ribenboim, *Algebraic Numbers* John Wiley & Sons, New York, 1972.
- [S] P. Samuel, *Algebraic Theory of Numbers* Houghton Mifflin, Boston, 1970.
- [Weiss] E. Weiss, *Algebraic Number Theory* McGraw-Hill, New York, 1963.
- [Z-S] O. Zariski, P. Samuel, *Commutative Algebra Vol. 1* Van Nostrand, New York, 1958.