Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

THE KRONECKER-WEBER THEOREM

a Bachelor Thesis

written by
Romain Branchereau

supervised by
Prof. Dr. Richard Pink
and Alexandre Puttick

Abstract

We present an elementary proof of the Kronecker-Weber Theorem and introduce the necessary mathematical background.

May 2016

Contents

Introduction

The aim of this Bachelor Thesis is to present an elementary proof due to Greenberg [Gre74] of the following theorem.

Theorem (Kronecker-Weber)**.** *Every finite abelian extension $K|\mathbb{Q}$ is cyclotomic.*

In other words, this means that if a Galois extension $K|\mathbb{Q}$ has a finite abelian Galois group, then K is contained in some cyclotomic field.

The Theorem was first stated by Leopold Kronecker in 1853, but his proof was incomplete. In 1886, Heinrich Weber presented a new proof that was still incomplete. David Hilbert finally proved it in 1896 using different techniques, and considered the generalization of this theorem concerning abelian Galois extension of general number fields instead of $\mathbb{Q}$. This generalization is known as Hilbert's 12th problem.

In modern literature, the proofs of the Kronecker-Weber Theorem are usually based on class field theory. The proof that we present in section 5 uses more elementary concepts from algebraic number theory, which will be introduced in sections 1 to 4. Standard results from Algebra, and in particular from Galois Theory will be assumed. However, the Fundamental Theorem of Galois Theory is stated in the appendix A.1, since we use it several times. The classical results that can be found in most books about algebraic number theory will usually be stated without proof, whereas the results that are more specific to the proof of the Kronecker-Weber Theorem will be proven.

I would like to thank my supervisors, Professor Richard Pink and Alexandre Puttick, for their helpful comments on drafts of this paper.

Notation and terminology

The rings we consider are always commutative with unity, and the fields are always number fields. When we say "abelian/cyclic extensions" we mean "Galois extension with abelian/cyclic Galois group". Several proofs are divided into claims. In this case the end of the proof of a claim is indicated by ■ whereas the end of the whole proof is indicated by □.

$R^\times$	Multiplicative group of units of a ring R
$U(n)$	The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$
$[L:K]$	Degree of a field extension $L\|K$
$(G:H)$	Index of a subgroup H in G
$H \leq G$	H is a subgroup of G
$H \trianglelefteq G$	H is a normal subgroup of G
$\mathrm{Quot}(R)$	The field of fraction of R
G_K	Galois group $\mathrm{Gal}(K\|\mathbb{Q})$

1 Ramification Theory

1.1 The ring of integers and factorization of primes

Let $R \subseteq S$ be a ring extension. An element $s \in S$ is *integral over* R if it is a root of a monic polynomial with coefficients in R, i.e. there exist $n \geq 1$ and elements $r_1, \ldots, r_n \in R$ such that

$$s^n + r_1 s^{n-1} + \cdots + r_{n-1} s + r_0 = 0.$$

We will assume the following Proposition:

Proposition 1.1. *Let $R \subset S$ be a ring extension and $s_1, \ldots, s_m \in S$. The following are equivalent:*

1. *$s_1, \ldots, s_m$ are integral over R,*
2. *$R[s_1, \ldots, s_m]$ is a finitely generated R-module.*

Proof. See [AM69, Proposition 5.1]. □

Corollary 1.2. *Let $\overline{R} \coloneqq \{s \in S \mid s \text{ is integral over } R\}$. Then $\overline{R}$ is a subring of S containing R.*

Proof. Every element $r \in R$ is integral over R, since it is a root of the monic polynomial $x - r$. It follows that $R \subseteq \overline{R}$. Let $x, y \in \overline{R}$. Then $R[x, y]$ is finitely generated as an R-module by Proposition 1.1. On the other hand, we know that $R[x, y, xy] = R[x, y]$. Thus $xy \in \overline{R}$ according to the same Proposition. Similarly for $x + y$. □

The ring $\overline{R}$ is called the *integral closure of R in S*. If $\overline{R} = R$ we say that R is *integrally closed* in S. If $\overline{R} = S$ we say that S is *integral over R*.

Definition 1.3. Let K be a number field, i.e. a finite degree extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is called the *ring of integers of K* and is denoted by $\mathcal{O}_K$. Equivalently, an element x is in $\mathcal{O}_K$ if there exist $n \geq 1$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that

$$x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

If $K = \mathbb{Q}$, the ring of integers is $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. A very useful property of $\mathbb{Z}$ is that it is a unique factorization domain, that allows us to decompose any nonzero integer into a product of primes in a unique way. Unfortunately, this property does not hold for an arbitrary ring of integers. For example, one can show that the ring of integers of $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}[\sqrt{-5}]$ which is not a unique factorization domain, since we have

$$2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Remark 1.4. Note that in general it is not true that the ring of integers of $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$.

Definition 1.5. A *Dedekind domain D* is an integral domain satisfying the following properties:

1. D is noetherian,
2. D is integrally closed,

3. every nonzero prime ideal in D is maximal.

The fundamental property of Dedekind Domains is that they allow a unique factorization of non zero ideals into prime ideals.

Theorem 1.6. *Let D be a Dedekind domain and $\mathfrak{a}$ be a nonzero proper ideal of D. Then we have a unique decomposition*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$$

where $\mathfrak{p}_1, \cdots, \mathfrak{p}_k$ are distinct nonzero prime ideals and $e_1, \cdots, e_k$ are positive integers.

Proof. See [Neu99, Theorem 3.3 in Chapter 1]. □

Theorem 1.7. *For any number field K, the ring of integers $\mathcal{O}_K$ is a Dedekind domain.*

Proof. See [Neu99, Theorem 3.1 in Chapter 1]. □

By Theorem 1.6, every nonzero ideal of $\mathcal{O}_K$ can be factored into prime ideals. This is a the generalization of the factorization into prime numbers that we have in $\mathbb{Z}$. The field of rationals $\mathbb{Q}$ is constructed by taking all the fractions of the integers $\mathbb{Z}$, hence $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. The following Proposition shows that this is also true for an arbitrary number field.

Proposition 1.8. *Let K be a number field. Then K is the field of fractions of $\mathcal{O}_K$.*

Proof. Let $y \in K$, then y is algebraic, i.e. it satisfies a relation $a_n y^n + a_{n-1} y^{n-1} + \cdots a_1 y + a_0 = 0$, where $a_i \in \mathbb{Z}$ and $a_n \neq 0$. Let $x \coloneqq y a_n$. Multiplying both sides by a_n^{n-1}, we get

$$x^n + a_{n-1} x^{n-1} + \cdots a_1 a_n^{n-2} x + a_0 a_n^{n-1} = 0.$$

Thus $x \in \mathcal{O}_K$ and $y = \frac{x}{a_n} \in \mathrm{Quot}(\mathcal{O}_K)$. On the other hand, we have $\mathcal{O}_K \subseteq K$. Thus $\mathrm{Quot}(\mathcal{O}_K) \subseteq \mathrm{Quot}(K) = K$, since K is a field. □

1.2 Ramification of primes

Let K be a number field and $n = [K : \mathbb{Q}]$. Let $\mathfrak{p}$ be a nonzero prime ideal in $\mathcal{O}_K$. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, generated by some prime p. So $(p) = \mathfrak{p} \cap \mathbb{Z}$ and we say that $\mathfrak{p}$ *lies over* p or that p *lies under* $\mathfrak{p}$. Let $p\,\mathcal{O}_K$ be the ideal generated by p in $\mathcal{O}_K$. Although the ideal (p) is prime in $\mathbb{Z}$, the ideal $p\,\mathcal{O}_K$ is not necessarily prime in $\mathcal{O}_K$.

Example 1.9. Consider $K = \mathbb{Q}(\sqrt{-5})$, with ring of integers $\mathbb{Z}[\sqrt{-5}]$. In $\mathbb{Z}$ the ideal generated by $p = 29$ is prime, but in $\mathbb{Z}[\sqrt{-5}]$ we have the decomposition

$$29 = (3 + 2\sqrt{-5}) \cdot (3 - 2\sqrt{-5}),$$

hence the ideal generated by 29 is not prime in $\mathbb{Z}[\sqrt{-5}]$.

Since $\mathcal{O}_K$ is a Dedekind domain, we know from Theorem 1.6 that we have a unique factorization into prime ideals $p\,\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, where the prime ideals $\mathfrak{p}_i$ are exactly the ideals lying over p. We will also say that $\mathfrak{p}_i$ *divides* p and use the notation $\mathfrak{p}_i \mid p$.

Definition 1.10. The exponent e_i is called the *ramification index of $\mathfrak{p}_i$ over p*.

We also write $e_i(\mathfrak{p}_i\,|p)$ for the ramification index if it is not clear which ideals are concerned. Since $\mathcal{O}_K$ is a Dedekind Domain, every prime ideal is maximal. Thus the quotients $\kappa(\mathfrak{p}_i) \coloneqq \mathcal{O}_K/\mathfrak{p}_i$ and $\kappa(p) \coloneqq \mathbb{Z}/p\,\mathbb{Z} \cong \mathbb{F}_p$ are fields, called the *residue fields*. Hence $\kappa(\mathfrak{p}_i)|\kappa(p)$ is a field extension of finite degree.

Definition 1.11. The degree $f_i \coloneqq f_i(\mathfrak{p}_i\,|p)$ of the extension $\kappa(\mathfrak{p}_i)|\kappa(p)$ is called the *inertial degree of* $\mathfrak{p}_i$ *over* p.

The residue field $\kappa(\mathfrak{p})$ contains the residue field $\mathbb{F}_p$, thus $\kappa(\mathfrak{p})$ is isomorphic to a finite field $\mathbb{F}_{p^f}$ where f is the inertial degree of $\mathfrak{p}$ over p.

Proposition 1.12. *The ramification and inertial degrees satisfy the following equality*

$$n = \sum_{i=1}^{g} e_i f_i.$$

Proof. See [Neu99, Proposition 8.2 in Chapter 1]. □

Let L be a number field containing K, such that $[L : K]$ is finite. In a similar way as before, the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ has a decomposition $\mathfrak{p}\,\mathcal{O}_L = \mathfrak{P}_1^{e_1'} \cdots \mathfrak{P}_g^{e_g'}$ in $\mathcal{O}_L$, where the $\mathfrak{P}_i$'s are prime ideals of $\mathcal{O}_L$. In the same way we can also define the ramification index $e(\mathfrak{P}_i\,|\,\mathfrak{p})$ and the inertial degree $f(\mathfrak{P}_i\,|\,\mathfrak{p})$.

Proposition 1.13. *Let $L|K|\,\mathbb{Q}$ be a tower of number fields. Let p be a prime in $\mathbb{Z}$, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Then we have $e(\mathfrak{P}\,|p) = e(\mathfrak{P}\,|\,\mathfrak{p}) \cdot e(\mathfrak{p}\,|p)$ and $f(\mathfrak{P}\,|p) = f(\mathfrak{P}\,|\,\mathfrak{p}) \cdot f(\mathfrak{p}\,|p)$.*

Proof. See [Mol11, Theorem 5.1]. □

Finally, it is natural to ask about the number of primes that ramify in a finite extension of number fields.

Theorem 1.14 (Minkowski)**.** *Let $K|\,\mathbb{Q}$ be a non trivial extension. Then there is at least one ramified prime and the number of ramified primes is finite.*

Proof. See [Neu99, Proposition 8.4 in Chapter 1] and [Neu99, Theorem 2.18 in Chapter 3]. □

Remark 1.15. For general number fields $K|L$ it is still true that the number of prime ideals of $\mathcal{O}_K$ that ramify in $\mathcal{O}_L$ is finite. However it is not necessarily true that there is a least one such prime.

1.3 Ramification of primes in Galois extensions

If $K|\,\mathbb{Q}$ is normal, the extension is Galois, since every number field is separable over $\mathbb{Q}$. Let G_K denote its Galois group, and $\mathfrak{p}_i$ a prime ideal lying over p.

First we note that for any $\sigma \in G_K$ we have $\sigma(\mathcal{O}_K) = \mathcal{O}_K$. Indeed, if $\alpha \in \mathcal{O}_K$, it is the root of some polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where the $a_i \in \mathbb{Z}$. Since $\mathbb{Z}$ is contained in $\mathbb{Q}$, the coefficients a_i are fixed by σ and $\sigma(\alpha)$ is also a root of the polynomial. Thus $\sigma(\alpha) \in \mathcal{O}_K$.

Since $\sigma \in G_K$ fixes $\mathbb{Q}$ and $\sigma(\mathfrak{p}_i) \cap \mathbb{Z} \subseteq \mathbb{Q}$, we have $\sigma(\mathfrak{p}_i) \cap \mathbb{Z} = \sigma(\mathfrak{p}_i \cap \mathbb{Z}) = \mathfrak{p}_i \cap \mathbb{Z} = (p)$. Thus $\sigma(\mathfrak{p}_i)$ is also a prime ideal lying over p. So G_K acts on the set of prime ideals $\mathfrak{p}_i$ lying over p.

Proposition 1.16. *The group G_K acts transitively on the set of prime ideals lying over p.*

Proof. See [Neu99, Proposition 9.1 in Chapter 1]. □

Proposition 1.17. *Let $K|\mathbb{Q}$ be a finite Galois extension and $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ be the prime ideals lying over p. Then the ramification indices $e_i = e(\mathfrak{p}_i|p)$ and inertial degrees $f_i = f_i(\mathfrak{p}_i|p)$ are both independant of i. Thus*

$$e_1 = \cdots = e_g \quad \text{and} \quad f_1 = \cdots = f_g.$$

Proof. Let $\mathfrak{p}_i$ be a prime lying over p. By Proposition 1.16 we have $\mathfrak{p}_i = \sigma_i(\mathfrak{p}_1)$ for some $\sigma_i \in G_K$. Since σ_i fixes $p \subseteq \mathbb{Q}$ and $\mathcal{O}_K$, we have

$$\begin{aligned} p\,\mathcal{O}_K = \sigma_i(p\,\mathcal{O}_K) &= \sigma_i(\mathfrak{p}_1^{e_1}\,\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}) \\ &= \sigma_i(\mathfrak{p}_1)^{e_1}\sigma_i(\mathfrak{p}_2)^{e_2}\cdots\sigma_i(\mathfrak{p}_g)^{e_g} \\ &= \mathfrak{p}_i^{e_1}\,\sigma_i(\mathfrak{p}_2)^{e_2}\cdots\sigma_i(\mathfrak{p}_g)^{e_g}. \end{aligned}$$

Thus for any i we have $e_i = e_1$. Moreover, the automorphism σ_i induces an isomorphism

$$\kappa(\mathfrak{p}_1) \longrightarrow \kappa(\mathfrak{p}_i), \quad x \mod \mathfrak{p}_1 \longmapsto \sigma_i(x) \mod \sigma_i(\mathfrak{p}_1).$$

This implies that $f_i = f_1$ for any i. □

From now on, let $e \coloneqq e_1 = \cdots = e_g$ and $f \coloneqq f_1 = \cdots = f_g$. Thus the factorization of p becomes $p\,\mathcal{O}_K = \left(\mathfrak{p}_1 \cdots \mathfrak{p}_g\right)^e$. Using Proposition 1.12 we deduce the following result.

Corollary 1.18. *If $K|\mathbb{Q}$ is a Galois extension of degree n, then we have*

$$n = efg.$$

Definition 1.19. If $p\,\mathcal{O}_K = \left(\mathfrak{p}_1 \cdots \mathfrak{p}_g\right)^e$ is the factorization of p in $\mathcal{O}_K$ we say that

1. p is *ramified* if $e > 1$,
2. p is *totally ramified* if $e = n$,
3. p is *unramified* if $e = 1$,
4. p *splits completely* if $g = n$.

1.4 Decomposition and Inertia groups

Let $K|\mathbb{Q}$ be a Galois extension of degree n with Galois group G_K and $p\,\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$ be the factorization of p in $\mathcal{O}_K$. We saw in Proposition 1.16 that G_K acts transitively on the set of prime ideals $\{\mathfrak{p}_1, \dots, \mathfrak{p}_g\}$ lying over p. Let $\mathfrak{p} \coloneqq \mathfrak{p}_i$ be one of these ideals. The stabilizer of $\mathfrak{p}$ under the action of G_K is called the *decomposition group of* $\mathfrak{p}$ and is denoted by

$$D_{\mathfrak{p}} \coloneqq \{\sigma \in G_K \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Its fixed field $K^{D_{\mathfrak{p}}}$ is called the *decomposition field of* $\mathfrak{p}$.

Remark 1.20. The decomposition group fixes $\mathfrak{p}$ as an ideal but not elementwise. This means that for $\sigma \in D_{\mathfrak{p}}$ and $x \in \mathfrak{p}$ we have $\sigma(x) \in \mathfrak{p}$ but not necessarily $\sigma(x) = x$.

Since every element $\sigma \in D_\mathfrak{p}$ sends $\mathfrak{p}$ to itself by definition, it induces an automorphism of the residue fields

$$\begin{aligned} \bar{\sigma} \colon \kappa(\mathfrak{p}) &\longrightarrow \kappa(\mathfrak{p}) \\ x \mod \mathfrak{p} &\longmapsto \sigma(x) \mod \mathfrak{p}\,. \end{aligned}$$

Furthermore, the automorphism $\bar{\sigma}$ fixes $\kappa(p)$ since σ fixes $\mathbb{Q}$, and hence $\bar{\sigma}$ is an automorphism of $\kappa(\mathfrak{p})$ fixing $\kappa(p)$.

Proposition 1.21. *The extension $\kappa(\mathfrak{p})|\kappa(p)$ is normal and the map*

$$\begin{aligned} D_\mathfrak{p} &\longrightarrow \mathrm{Gal}(\kappa(\mathfrak{p})|\kappa(p)) \\ \sigma &\longmapsto \bar{\sigma} \end{aligned}$$

is a surjective homorphism.

Proof. See [Neu99, Proposition 9.4 in Chapter 1]. □

The kernel of this homomorphism is called the *inertia group of* $\mathfrak{p}$ and denoted by $I_\mathfrak{p}$. Since the homomorphism is surjective, we have the following isomorphism:

$$D_\mathfrak{p}/I_\mathfrak{p} \cong \mathrm{Gal}(\kappa(\mathfrak{p})|\kappa(p)).$$

The fixed field $K^{I_\mathfrak{p}}$ of the inertia group is called the *inertia field of* $\mathfrak{p}$. An element $\sigma \in D_\mathfrak{p}$ lies in $I_\mathfrak{p}$ if its image is the identity in $\mathrm{Gal}(\kappa(\mathfrak{p})|\kappa(p))$, hence the inertia group is exactly

$$I_\mathfrak{p} = \{\sigma \in D_\mathfrak{p} \mid \forall x \in \mathcal{O}_K \ \ \sigma(x) \equiv x \mod \mathfrak{p}\}\,.$$

We saw in Subsection 1.2 that the residue fields are finite fields of characteristic p. Moreover, the degree of the extension $\kappa(\mathfrak{p})|\kappa(p)$ is the inertial degree $f = f(\mathfrak{p}\,|p)$. Thus we have an isomorphism

$$\mathrm{Gal}(\kappa(\mathfrak{p})|\kappa(p)) \cong \mathrm{Gal}(\mathbb{F}_{p^f}\,|\,\mathbb{F}_p).$$

The Galois group of $\mathbb{F}_{p^f}\,|\,\mathbb{F}_p$ is cyclic, generated by the automorphism $\sigma : x \mapsto x^p$, which is called the *Frobenius automorphism*. A proof of this fact can for example be found in [DSD03, Section 14.3].

Corollary 1.22. *The quotient $D_\mathfrak{p}/I_\mathfrak{p}$ is cyclic, generated by the coset of $\sigma \in D_\mathfrak{p}$, such that*

$$\sigma(x) \equiv x^p \mod \mathfrak{p}\,.$$

In other words, the image $\overline{\sigma}$ in $D_\mathfrak{p}/I_\mathfrak{p}$ is the Frobenius automorphism.

Proposition 1.23. *We have*

1. $|D_\mathfrak{p}| = ef$ *and* $(G_K : D_\mathfrak{p}) = g$,
2. $|I_\mathfrak{p}| = e$ *and* $(D_\mathfrak{p} : I_\mathfrak{p}) = f$.

Hence p is totally ramified in K if and only if $I_\mathfrak{p} = G_K$, and unramified if and only if $I_\mathfrak{p} = \{e\}$.

Proof. 1. Since the action of G_K is transitive, the orbit is exactly the set of prime ideals lying over p. Using the orbit stabilizer theorem and the fundamental equality from Corollary 1.18, we obtain $g \cdot |D_\mathfrak{p}| = |G_K| = n = efg$. This implies that $|D_\mathfrak{p}| = ef$ and $(G_K : D_\mathfrak{p}) = \frac{|G_K|}{|D_\mathfrak{p}|} = g$.

2. From the definition of the inertial degree, we know that $f = [\kappa(\mathfrak{p}) : \kappa(p)] = |\mathrm{Gal}(\kappa(\mathfrak{p})|\kappa(p))|$. Moreover, the quotient $D_\mathfrak{p}/I_\mathfrak{p}$ is isomorphic to $\mathrm{Gal}(\kappa(\mathfrak{p})|\kappa(p))$. Thus $|\mathrm{Gal}(\kappa(\mathfrak{p})|\kappa(p))| = \frac{|D_\mathfrak{p}|}{|I_\mathfrak{p}|}$. This implies that $(D_\mathfrak{p} : I_\mathfrak{p}) = f$. Since $|D_\mathfrak{p}| = ef$, we conclude that $|I_\mathfrak{p}| = e$. □

From the previous Proposition and the Fundamental Theorem of Galois theory, we deduce the following Corollary.

Corollary 1.24. *We have*

1. $[K : K^{I_\mathfrak{p}}] = e$,
2. $[K^{I_\mathfrak{p}} : K^{D_\mathfrak{p}}] = f$,
3. $[K^{D_\mathfrak{p}} : \mathbb{Q}] = g$.

Let F be a subfield of K containing $\mathbb{Q}$ and $\mathfrak{p}_F \coloneqq \mathfrak{p} \cap F$ be a prime of $\mathcal{O}_F$ lying under $\mathfrak{p}$ and over p. Everything we did before for the extension $K|\mathbb{Q}$ can also be done for $K|F$. In this case, the Galois group $\mathrm{Gal}(K|F)$ acts transitively on the set of primes of $\mathcal{O}_K$ lying over $\mathfrak{p}_F$, and we denote the decomposition group by $D_{\mathfrak{p}\,|\,\mathfrak{p}_F}$. Then, we get a surjective homormphism

$$D_{\mathfrak{p}\,|\,\mathfrak{p}_F} \to \mathrm{Gal}(\kappa(\mathfrak{p})|\kappa(\mathfrak{p}_F)),$$

with kernel $I_{\mathfrak{p}\,|\,\mathfrak{p}_F} = I_\mathfrak{p} \cap \mathrm{Gal}(K|F)$. Moreover, we have $|I_{\mathfrak{p}\,|\,\mathfrak{p}_F}| = e(\mathfrak{p}\,|\,\mathfrak{p}_F)$.

Proposition 1.25. *Let $K|\mathbb{Q}$ be a finite Galois extension and $\mathfrak{p}$ a prime of $\mathcal{O}_K$. Let F be a subfield of K and $\mathfrak{p}_F \coloneqq \mathfrak{p} \cap F$. Then $I_{\mathfrak{p}_F}$ is isomorphic to $I_\mathfrak{p}/I_{\mathfrak{p}\,|\,\mathfrak{p}_F}$.*

Proof. Let $\sigma \in I_\mathfrak{p}$, i.e. $\sigma(x) - x \in \mathfrak{p}$ for every $x \in \mathcal{O}_K$. Restricting to F, we have $\sigma\restriction_F (x) - x \in \mathfrak{p}_F$ for every $x \in \mathcal{O}_F$, since $\mathfrak{p}_F = \mathfrak{p} \cap F$ and $\mathcal{O}_F = \mathcal{O}_K \cap F$. Thus $\sigma\restriction_F \in I_{\mathfrak{p}_F}$. Consider the group homomorphism

$$\begin{array}{rccc} \phi & : & I_\mathfrak{p} & \longrightarrow & I_{\mathfrak{p}_F} \\ & & \sigma & \longmapsto & \sigma\restriction_F \end{array}.$$

The kernel of ϕ is $I_\mathfrak{p} \cap \mathrm{Gal}(K|F) = I_{\mathfrak{p}\,|\,\mathfrak{p}_F}$, thus $I_\mathfrak{p}/I_{\mathfrak{p}\,|\,\mathfrak{p}_F} \cong \mathrm{Im}\,\phi \leq I_{\mathfrak{p}_F}$. Since the ramification indices are multiplicative by Proposition 1.13, it follows that $|I_\mathfrak{p}/I_{\mathfrak{p}\,|\,\mathfrak{p}_F}| = \frac{e(\mathfrak{p}\,|p)}{e(\mathfrak{p}\,|\,\mathfrak{p}_F)} = e(\mathfrak{p}_F\,|p) = |I_{\mathfrak{p}_F}|$. Hence we have $I_{\mathfrak{p}_F} \cong I_\mathfrak{p}/I_{\mathfrak{p}\,|\,\mathfrak{p}_F}$ □

From this Proposition we can deduce two important corollaries.

Corollary 1.26. *The prime p is unramified in the inertia field $K^{I_\mathfrak{p}}$.*

Proof. Let $\mathfrak{p} \subset \mathcal{O}_K$ lying over p and $\mathfrak{p}_I \coloneqq \mathfrak{p} \cap K^{I_\mathfrak{p}}$. We know that $\mathrm{Gal}(K|K^{I_\mathfrak{p}}) = I_\mathfrak{p}$ from Galois theory. Moreover, we have $I_{\mathfrak{p}\,|\,\mathfrak{p}_I} = I_\mathfrak{p} \cap \mathrm{Gal}(K|K^{I_\mathfrak{p}}) = I_\mathfrak{p}$. By Proposition 1.25, it follows that $I_{\mathfrak{p}_I} = \{e\}$ and thus p is unramified in $K^{I_\mathfrak{p}}$. □

Corollary 1.27. *Let $K|\mathbb{Q}$ be a finite Galois extension and F a subfield of K cointaining $\mathbb{Q}$. If p is totally ramified in K, then p is totally ramified in F.*

Proof. Since p is totally ramified in K, we have $I_{\mathfrak{p}} = G_K$. This implies that

$$I_{\mathfrak{p} \mid \mathfrak{p}_F} = I_{\mathfrak{p}} \cap \mathrm{Gal}(K|F) = G_K \cap \mathrm{Gal}(K|F) = \mathrm{Gal}(K|F).$$

From Galois theory we know that $G_F \cong G_K / \mathrm{Gal}(K|F)$. According to Proposition 1.25 we have $I_{\mathfrak{p}_F} = G_F$ and thus p is totally ramified in F. □

1.5 Compositum of fields

Definition 1.28 (Compositum)**.** Let K_1 and K_2 be two subfields of a field L. The compositum K_1K_2 is the smallest subfield of L that contains both K_1 and K_2.

Remark 1.29. From now on we will assume that the number fields are contained in $\mathbb{C}$. Thus, the compositum of such number fields can be defined inside $\mathbb{C}$.

Proposition 1.30. *Let $K_1, K_2 | \mathbb{Q}$ be two finite Galois extensions. Then*

$$[K_1K_2 : \mathbb{Q}] = \frac{[K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]}{[K_1 \cap K_2 : \mathbb{Q}]}.$$

Proof. See [DSD03, Corollary 20 in Section 14.4]. □

Proposition 1.31. *Let $K_1 | \mathbb{Q}$ and $K_2 | \mathbb{Q}$ be two finite Galois extensions. Then $K_1 \cap K_2$ and K_1K_2 are Galois over $\mathbb{Q}$. Moreover, the Galois group $G_{K_1K_2}$ is isomorphic to the subgroup H of $G_{K_1} \times G_{K_2}$ given by*

$$H := \{(\sigma, \tau) \mid \sigma \restriction_{K_1 \cap K_2} = \tau \restriction_{K_1 \cap K_2}\}.$$

Proof. Let $f(x)$ be an irreducible polynomial in $\mathbb{Q}[x]$ with a root in $K_1 \cap K_2$. This root lies in K_1 and in K_2. Since K_1 is a normal extension, all the roots of f are in K_1. The same holds for K_2, thus all the roots of f are in $K_1 \cap K_2$ and $K_1 \cap K_2 | \mathbb{Q}$ is a normal extension. Since every extension of $\mathbb{Q}$ is separable, it follows that $K_1 \cap K_2 | \mathbb{Q}$ is Galois.

Let $f_1(x)$ and $f_2(x)$ be separable polynomials such that K_1 and K_2 are their respective splitting fields. Let $\alpha_1, \ldots, \alpha_r$ be the common roots of f_1 and f_2. Then $g(x) := \frac{f_1(x)f_2(x)}{(x-\alpha_1)\cdots(x-\alpha_r)}$ is separable and K_1K_2 is its splitting field. Thus $K_1K_2 | \mathbb{Q}$ is Galois.

Consider the group homomorphism

$$\begin{array}{rccc} \phi & : & G_{K_1K_2} & \longrightarrow & G_{K_1} \times G_{K_2} \\ & & \sigma & \longmapsto & (\sigma \restriction_{K_1}, \sigma \restriction_{K_2}) \end{array}.$$

Let $\sigma \in \ker \phi$. Then $\sigma \restriction_{K_1} = \sigma \restriction_{K_2} = e$. The field fixed by σ must contain K_1 and K_2, hence it must contain the compositum K_1K_2. So $\sigma = e$ in $G_{K_1K_2}$ and ϕ is injective. Clearly we have $\mathrm{Im}(\phi) \leq H$.

Let $\sigma \in G_{K_1}$. The restriction $\sigma \restriction_{K_1 \cap K_2}$ lies in $G_{K_1 \cap K_2} \cong G_{K_2} / \mathrm{Gal}(K_2|K_1 \cap K_2)$. Hence there are exactly $|\mathrm{Gal}(K_2|K_1 \cap K_2)|$ elements of G_{K_2} such that their restriction on $K_1 \cap K_2$ is equal to $\sigma \restriction_{K_1 \cap K_2}$. Thus we have

$$|H| = |G_{K_1}| \cdot |\mathrm{Gal}(K_2|K_1 \cap K_2)| = |G_{K_1}| \cdot \frac{|G_{K_2}|}{|G_{K_1 \cap K_2}|} = \frac{[K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]}{[K_1 \cap K_2 : \mathbb{Q}]} = [K_1K_2 : \mathbb{Q}],$$

where the last equality follows from Proposition 1.31. On the other hand, we also have

$$|\mathrm{Im}(\phi)| = |G_{K_1K_2}| = [K_1K_2 : \mathbb{Q}].$$

This implies that $|\mathrm{Im}(\phi)| = |H|$, thus $\mathrm{Im}(\phi) = H$. □

Proposition 1.32 ([Rib01, Lemma 3 Chapter 15])**.** *Let $K_1, K_2|\,\mathbb{Q}$ be two finite Galois extensions, and p a prime in $\mathbb{Z}$. Let $\mathfrak{P}$ be a prime of K_1K_2 lying over p, and let $\mathfrak{p}_i$ be the prime of K_i with $\mathfrak{P} \mid \mathfrak{p}_i \mid p$. Then $I_{\mathfrak{P}}$ is isomorphic to a subgroup of $I_{\mathfrak{p}_1} \times I_{\mathfrak{p}_2}$.*

Proof. Let ϕ be the homormorphism defined in 1.31, and consider the restriction $\phi \restriction_{I_{\mathfrak{P}}}$. If $\sigma \in I_{\mathfrak{P}}$ then $\sigma \restriction_{K_1} \in I_{\mathfrak{p}_1}$ and $\sigma \restriction_{K_2} \in I_{\mathfrak{p}_2}$. Thus we have a group homomorphism

$$\begin{array}{rccc} \phi \restriction_{I_{\mathfrak{P}}} \;:\; & I_{\mathfrak{P}} & \longrightarrow & I_{\mathfrak{p}_1} \times I_{\mathfrak{p}_2} \\ & \sigma & \longmapsto & (\sigma \restriction_{K_1}, \sigma \restriction_{K_2}) \end{array} .$$

The restriction $\phi \restriction_{I_{\mathfrak{P}}}$ is still injective and this implies that $I_{\mathfrak{P}} \cong \operatorname{Im}\phi \leq I_{\mathfrak{p}_1} \times I_{\mathfrak{p}_2}$. □

From this Proposition we can immediately deduce the following Corollary.

Corollary 1.33. *Let $K_1, K_2|\,\mathbb{Q}$ be two finite Galois extensions, and p a prime in $\mathbb{Z}$. If p is unramified both in K_1 and K_2, then p is unramified in K_1K_2.*

2 Valuations

2.1 Localization

The process of localization generalizes the construction of the fraction field of an integral domain R. Recall that we can define the following equivalence relation on $R \times R \setminus \{0\}$:

$$(r, s) \sim (r', s') \quad \text{if and only if} \quad (rs' - sr') = 0.$$

The set of equivalence classes is called the *field of fractions of* R or *fraction field of* R and is denoted by $\mathrm{Quot}(R)$. The equivalence class of a pair (r, s) is denoted by $\frac{r}{s}$.

Let R be any ring. A *multiplicatively closed subset* $S \subseteq R \setminus \{0\}$ is a subset containing 1 and closed under multiplication. Similarly to the fraction field, we define the following relation on $R \times S$:

$$(r, s) \sim (r', s') \quad \text{if and only if} \quad (rs' - sr')u = 0 \text{ for some } u \in S,$$

which is clearly an equivalence relation. The set of equivalence classes is called the *ring of fractions with respect to* S and is denoted by $S^{-1}R$. The equivalence class of an element (r, s) of the ring of fractions is written as a fraction $\frac{r}{s}$. The ring structure is defined by the rules

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'},$$

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}.$$

Let $\mathfrak{a}$ be an ideal of R and $S^{-1}\mathfrak{a} = \{\frac{a}{s} \mid a \in \mathfrak{a},\ s \in S\}$, which is clearly an ideal of $S^{-1}R$.

Proposition 2.1. *The maps* $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ *and* $\mathfrak{q} \mapsto \mathfrak{q} \cap R$ *are inverse to each other and give a* $1-1$ *inclusion preserving correspondance between prime ideals* $\mathfrak{p} \subseteq R \setminus S$ *and prime ideals* $\mathfrak{q}$ *of* $S^{-1}R$.

Proof. See [Neu99, Proposition 11.1 in Chapter 1]. □

Proposition 2.2. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are two ideals of* R, *then* $S^{-1}(\mathfrak{ab}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$.

Proof. See [AM69, Proposition 3.11]. □

If $\mathfrak{p}$ is a prime ideal of R, then $S = R \setminus \mathfrak{p}$ is a multiplicatively closed subset of R. The ring of fractions $S^{-1}R$ is called the *localization at* $\mathfrak{p}$ and is denoted by $R_{\mathfrak{p}}$.

Definition 2.3. A ring R is called a *local ring* if it has a unique maximal ideal.

Proposition 2.4. *The ring* $R_{\mathfrak{p}}$ *is a local ring with unique maximal ideal* $\mathfrak{m}_{\mathfrak{p}} \coloneqq S^{-1}\mathfrak{p}$.

Proof. This follows directly from Proposition 2.1 with $S = R \setminus \mathfrak{p}$, since $R \setminus S = \mathfrak{p}$. □

Proposition 2.5. *If* $\mathfrak{p}$ *is a maximal ideal of* R, *then* $R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} \cong R/\mathfrak{p}$.

Proof. See [Neu99, Corollary 11.2 in Chapter 1]. □

Proposition 2.6. *If* R *is an integral domain, then* $\mathrm{Quot}(S^{-1}R) = \mathrm{Quot}(R)$.

Proof. Let $\frac{r}{s} \in S^{-1}R$. Then $r, s \in R$ and $\frac{r}{s} \in \mathrm{Quot}(R)$. Thus $S^{-1}R \subseteq \mathrm{Quot}(R)$ and this implies that $\mathrm{Quot}(S^{-1}R) \subseteq \mathrm{Quot}(R)$. On the other hand, if $\frac{r_1}{r_2} \in \mathrm{Quot}(R)$, then for any $s \in S$ we have $\frac{r_1}{r_2} = \frac{r_1}{s}\left(\frac{r_2}{s_2}\right)^{-1} \in \mathrm{Quot}(S^{-1}R)$. Thus $\mathrm{Quot}(R) \subseteq \mathrm{Quot}(S^{-1}R)$. □

2.2 Localization of ring of integers

Proposition 2.7. *Let D be a Dedekind domain and S a multiplicatively closed subset of D. Then $S^{-1}D$ is a Dedekind domain.*

Proof. See [Neu99, Proposition 11.4 in Chapter 1] □

Let K be a number field. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$ and $\mathcal{O}_{K,\mathfrak{p}}$ the localization of $\mathcal{O}_K$ at $\mathfrak{p}$. According to Proposition 2.4 the localization $\mathcal{O}_{K,\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{m}_\mathfrak{p}$. Moreover, in a Dedekind domain every nonzero prime ideal is maximal, thus $\mathfrak{m}_\mathfrak{p}$ is also the unique nonzero prime ideal. By Proposition 2.7 the ring $\mathcal{O}_{K,\mathfrak{p}}$ is also a Dedekind domain, hence every nonzero ideal is the product of nonzero prime ideals. We immediately get the following result.

Corollary 2.8. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_{K,\mathfrak{p}}$. Then $\mathfrak{a} = \mathfrak{m}_\mathfrak{p}^k$ for some integer $k \geq 0$.*

Proposition 2.9. *For every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the localization $\mathcal{O}_{K,\mathfrak{p}}$ is a principal ideal domain.*

Proof. Let π be any element in $\mathfrak{m}_\mathfrak{p} \setminus \mathfrak{m}_\mathfrak{p}^2$. By Corollary 2.8 we have $(\pi) = \mathfrak{m}_\mathfrak{p}^k$ for some integer $k \geq 1$. Since $\pi \notin \mathfrak{m}_\mathfrak{p}^2$, we have $k = 1$. Hence for every integer $k \geq 1$, we have $\mathfrak{m}_\mathfrak{p}^k = (\pi^k)$. Using Corollary 2.8 again this proves that $\mathcal{O}_{K,\mathfrak{p}}$ is a principal ideal domain. □

Remark 2.10. A ring that is a principal ideal domain and a local ring is called a *discrete valuation ring*.

Definition 2.11. A generator of the unique prime ideal $\mathfrak{m}_\mathfrak{p}$ is called a *uniformizer*.

Remark 2.12. The unifomizer π is unique up to associates, i.e. if ρ is another uniformizer then $\rho = u\pi$ for some unit $u \in \mathcal{O}_{K,\mathfrak{p}}^\times$.

Let a be a nonzero element of $\mathcal{O}_{K,\mathfrak{p}}$. The nonzero ideal (a) is a power of $\mathfrak{m}_\mathfrak{p} = (\pi)$ for some uniformizer π, say $(a) = (\pi^i)$. Then we can be write

$$a = u\pi^i, \qquad u \in \mathcal{O}_{K,\mathfrak{p}}^\times, \quad i \in \mathbb{N}.$$

This can be extended to K, which is the ring of fraction of $\mathcal{O}_{K,\mathfrak{p}}$ by Propositions 1.8 and 2.6. If $x \in K^\times$, then x can be written as a fraction $\frac{a}{b}$ with $a, b \in \mathcal{O}_{K,\mathfrak{p}} \setminus \{0\}$. Hence it can be written:

$$x = u\pi^i, \qquad u \in \mathcal{O}_{K,\mathfrak{p}}^\times, \quad i \in \mathbb{Z},$$

and we have $v_\mathfrak{p}(x) = v_\mathfrak{p}(a) - v_\mathfrak{p}(b)$. The integer i is called the *valuation* of x and will be denoted by $v_\mathfrak{p}(x)$. We use the convention $v_\mathfrak{p}(0) = \infty$. Furthermore, the valuation does not depend on π. If ρ is an another uniformizer, then it generates the same ideal, thus it does not change the power i. It is straightforward computation to show the following Proposition.

Proposition 2.13. *The valuation $v_\mathfrak{p}(x)$ is a surjective map from $K^\times$ onto $\mathbb{Z}$ and satisfies for every $x, y \in K^\times$:*

1. $v_\mathfrak{p}(xy) = v_\mathfrak{p}(x) + v_\mathfrak{p}(y)$,
2. $v_\mathfrak{p}(x + y) \geq \min\{v_\mathfrak{p}(x), v_\mathfrak{p}(y)\}$, *with equality if $v_\mathfrak{p}(x) \neq v_\mathfrak{p}(y)$.*

Remark 2.14. Let x be a nonzero element of $\mathcal{O}_K$ and $(x) = x\,\mathcal{O}_K = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$ be the factorization of the ideal (x), where $\mathfrak{p}_i$ is a prime ideal in $\mathcal{O}_K$ and n_i a positive integer. By Proposition 2.2, for any two ideals $\mathfrak{a}$ and $\mathfrak{b}$ we have $(\mathfrak{ab})_{\mathfrak{p}_i} = \mathfrak{a}_{\mathfrak{p}_i}\mathfrak{b}_{\mathfrak{p}_i}$. Moreover, since $\mathcal{O}_{K,\mathfrak{p}_i}$ is a local ring, the only prime ideal that does not vanish in the localization is the ideal $\mathfrak{p}_i$, which becomes $\mathfrak{m}_{\mathfrak{p}_i}$. If we localize at $\mathfrak{p}_i$, we have $x\,\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}_i}^{n_i}$. Thus the exponent n_i is exactly the valuation $v_{\mathfrak{p}_i}(x)$, and we have $(x) = \mathfrak{p}_1^{v_{\mathfrak{p}_1}} \cdots \mathfrak{p}_k^{v_{\mathfrak{p}_k}}$, where $v_{\mathfrak{p}_i} \coloneqq v_{\mathfrak{p}_i}(x)$. This gives us a relation between the valuation and the factorization.

Let n be a nonzero integer in $\mathbb{Z}$ and $n = p^{v_p} m$ its factorization, where $p \nmid m$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ lying over p and $p\,\mathcal{O}_K = (\mathfrak{p}\,\mathfrak{p}_2 \cdots \mathfrak{p}_g)^e$ its factorization, where $e = e(\mathfrak{p}\,|p)$ is the ramification index. Then, in $\mathcal{O}_K$ the factorization becomes

$$n\,\mathcal{O}_K = \mathfrak{p}^{ev_p}\,\mathfrak{a},$$

where $\mathfrak{a}$ is an ideal not divisible by $\mathfrak{p}$. Thus for every integer n we get $v_{\mathfrak{p}}(n) = e(\mathfrak{p}\,|p) \cdot v_p(n)$. Since $v_{\mathfrak{p}}(\frac{n}{m}) = v_{\mathfrak{p}}(n) - v_{\mathfrak{p}}(m)$ we can deduce the following.

Proposition 2.15. *For any $x \in \mathbb{Q}$, we have $v_{\mathfrak{p}}(x) = e(\mathfrak{p}\,|p) \cdot v_p(x)$.*

2.3 Higher ramification groups

Let $K|\,\mathbb{Q}$ be a finite Galois extension with Galois group G_K. Let p be a prime of $\mathbb{Z}$ and $\mathfrak{p}$ a prime of $\mathcal{O}_K$ lying over p, with residue fields $\kappa(\mathfrak{p})$ and $\kappa(p)$.

Let σ be in the decomposition group $D_{\mathfrak{p}}$ and $i \geq 0$ be an integer. Since σ sends $\mathfrak{p}$ to itself, it also sends $\mathfrak{p}^{i+1} \subset \mathfrak{p}$ to itself, for every integer $i \geq 0$. Thus it induces an automorphism

$$\begin{array}{rccc} \overline{\sigma_i} & : & \mathcal{O}_K \,/\, \mathfrak{p}^{i+1} & \longrightarrow & \mathcal{O}_K \,/\, \mathfrak{p}^{i+1} \\ & & x \mod \mathfrak{p}^{i+1} & \longmapsto & \sigma(x) \mod \mathfrak{p}^{i+1} \end{array}.$$

Note that for $i > 0$, this is a ring automorphism and not a field automorphism. The group of ring automorphisms of $\mathcal{O}_K \,/\, \mathfrak{p}^{i+1}$ is denoted by $\mathrm{Aut}(\mathcal{O}_K \,/\, \mathfrak{p}^{i+1})$.

Proposition 2.16. *The map*

$$\begin{aligned} h_i : D_{\mathfrak{p}} &\longrightarrow \mathrm{Aut}(\mathcal{O}_K \,/\, \mathfrak{p}^{i+1}) \\ \sigma &\longmapsto \overline{\sigma_i} \end{aligned}$$

is a group homomorphism.

Proof. Let $\sigma, \tau \in D_{\mathfrak{p}}$ and $x \in \mathcal{O}_K$. Moreover, let $\overline{x}$ denote the residue $x \mod \mathfrak{p}^{i+1}$ for simplicity. Then, we have

$$\overline{\sigma_i\tau_i}(\overline{x}) = \overline{\sigma_i\tau_i(x)} = \overline{\sigma_i}\ \overline{\tau_i(x)} = \overline{\sigma_i}\ \overline{\tau_i}(\overline{x}),$$

and thus $\overline{\sigma_i\tau_i} = \overline{\sigma_i}\ \overline{\tau_i}$, since x was arbitrary.. □

The kernel of the map h_i is $V_i \coloneqq \left\{\sigma \in D_{\mathfrak{p}} \mid \forall x \in \mathcal{O}_K \quad \sigma(x) \equiv x \mod \mathfrak{p}^{i+1}\right\}$, which is called the *$i$-th ramification group of* $\mathfrak{p}$. Note that V_0 is precisely the inertia group $I_{\mathfrak{p}}$.

Proposition 2.17. *The groups V_i are normal subgroups of $D_{\mathfrak{p}}$ and they form a descending chain of subgroups*

$$I_{\mathfrak{p}} = V_0 \trianglerighteq V_1 \trianglerighteq V_2 \trianglerighteq \dots.$$

Proof. The ramification group V_i is a normal subgroup of $D_\mathfrak{p}$, because it is the kernel of a group homomorphism. If $\sigma \in V_{i+1}$, then $\sigma(x) - x \in \mathfrak{p}^{i+1}$ for every $x \in \mathcal{O}_K$. Since $\mathfrak{p}^{i+1} \subset \mathfrak{p}^i$, this implies that $\sigma(x) - x \in \mathfrak{p}^i$ for every $x \in \mathcal{O}_K$. Thus $\sigma \in V_i$. □

Lemma 2.18. *If $\mathfrak{a}$ is a proper ideal of $\mathcal{O}_K$, then*

$$\bigcap_{i=1}^{\infty} \mathfrak{a}^i = (0).$$

Proof. See [Sch07, Proposition 6.4.10]. □

Proposition 2.19. *There exists an integer $i_0 \geq 0$ such that*

$$V_{i_0} = V_{i_0+1} = V_{i_0+2} = \cdots = \{e\},$$

where e is the identity automorphism.

Proof. First we claim that $\bigcap_{i\geq 0} V_i = \{e\}$. Let $\sigma \in \bigcap_{i\geq 0} V_i$, i.e. $\sigma \in V_i$ for every $i \geq 0$. This means that

$$\sigma(x) - x \in \bigcap_{i=0}^{\infty} \mathfrak{p}^{i+1}$$

for every $x \in \mathcal{O}_K$. Since this intersection is trivial by Lemma 2.18, this proves that σ is the identity. Since $I_\mathfrak{p}$ is finite (it is a subgroup of the Galois group which is finite), it only has a finite number of distinct subgroups. This implies that there exists an integer $i_0 \geq 0$, such that $V_{i_0} = V_{i_0+1} = V_{i_0+2} = \ldots$. But since the intersection $\cap_{i\geq 0} V_i$ is trivial, the subgroups V_i for $i \geq i_0$ must be trivial. □

When we work with ramification groups, we restrict our attention to a particular prime ideal in the ring of integers. Consider the localization of $\mathcal{O}_{K,\mathfrak{p}}$ with unique maximal ideal $\mathfrak{m}_\mathfrak{p}$ and let π be a uniformizer. The two following Propositions extend the ramification groups and the decomposition groups to the localization of the ring of integers.

Proposition 2.20. *Let $\sigma \in G_K$. Then $\sigma(\mathfrak{p}) = \mathfrak{p}$ if and only if $\sigma(\mathfrak{m}_\mathfrak{p}) = \mathfrak{m}_\mathfrak{p}$.*

Proof. Let $x \in \mathcal{O}_K$. If σ satisfy $\sigma(\mathfrak{m}_\mathfrak{p}) = \mathfrak{m}_\mathfrak{p}$, then $\sigma(\mathcal{O}_K \cap \mathfrak{m}_\mathfrak{p}) = \mathcal{O}_K \cap \mathfrak{m}_\mathfrak{p}$. According to Proposition 2.1, we have $\mathcal{O}_K \cap \mathfrak{m}_\mathfrak{p} = \mathfrak{p}$ and thus $\sigma(\mathfrak{p}) = \mathfrak{p}$.

Conversely, let $y \in \mathfrak{m}_\mathfrak{p}$ and consider σ satisfying the condition $\sigma(\mathfrak{p}) = \mathfrak{p}$ i.e. $\sigma \in D_\mathfrak{p}$. We can write $y = \frac{r}{s}$ for some $r \in \mathfrak{p}$ and $s \in \mathcal{O}_K \setminus \mathfrak{p}$. Since $\sigma \in D_\mathfrak{p}$, it sends $\mathcal{O}_K \setminus \mathfrak{p}$ to itself, so $\sigma(s) \in \mathcal{O}_K \setminus \mathfrak{p}$ and $\sigma(r) \in \mathfrak{p}$. Hence we have $\sigma\left(\frac{r}{s}\right) = \frac{\sigma(r)}{\sigma(s)} \in \mathfrak{m}_\mathfrak{p}$, so $\sigma(\mathfrak{m}_\mathfrak{p}) = \mathfrak{m}_\mathfrak{p}$. □

Proposition 2.21. *Let $\sigma \in G_K$ and π be a uniformizer. The following are equivalent:*

1. $\sigma(x) - x \equiv 0 \mod \mathfrak{p}^{i+1}$ *for every $x \in \mathcal{O}_K$,*
2. $\sigma(y) - y \equiv 0 \mod \mathfrak{m}_\mathfrak{p}^{i+1}$ *for every $y \in \mathcal{O}_{K,\mathfrak{p}}$,*
3. $\sigma(\pi) - \pi \equiv 0 \mod \mathfrak{m}_\mathfrak{p}^{i+1}$.

Proof. The equivalence of (1.) and (2.) can be proved in a very similar way as done in the proof of Proposition 2.20. A proof of the equivalence of (1.) and (3.) can be found in [Rib01, Proposition G in Section 14.2]. □

Proposition 2.22. *Let $\sigma \in G_K$. Then $\sigma \in V_i$ if and only if $v_\mathfrak{p}(\sigma(\pi) - \pi) \geq i + 1$.*

Proof. By the previous Proposition, we know that $\sigma \in V_i$ if and only if $\sigma(\pi) - \pi \equiv 0 \mod \mathfrak{m}_\mathfrak{p}^{i+1}$. This is equivalent to $\sigma(\pi) - \pi = a\pi^{i+1}$ for some $a \in \mathcal{O}_{K,\mathfrak{p}}$. Since $v_\mathfrak{p}(a) \geq 0$, we have

$$v_\mathfrak{p}(\sigma(\pi) - \pi) = v_\mathfrak{p}(a) + v_\mathfrak{p}(\pi^{i+1}) \geq v_\mathfrak{p}(\pi^{i+1}) = i + 1.$$

Conversely, if $v_\mathfrak{p}(\sigma(\pi) - \pi) \geq i + 1$, then $\sigma(\pi) - \pi \in \mathfrak{m}_\mathfrak{p}^{i+1}$. □

Let σ be an element of the decomposition group. Since σ sends $\mathfrak{m}_\mathfrak{p} = (\pi)$ to itself, we can write $\sigma(\pi) = c_\sigma \pi$ for some $c_\sigma \in \mathcal{O}_{K,\mathfrak{p}}$.

Remark 2.23. If ρ and π are two uniformizers, then $\rho = u\pi$ for some unit $u \in \mathcal{O}_{K,\mathfrak{p}}^\times$. For $\sigma \in I_\mathfrak{p}$, we write $\sigma(\pi) = c_\sigma \pi$ and $\sigma(\pi) = c'_\sigma \pi$, for some $c_\sigma, c'_\sigma \in \mathcal{O}_{K,\mathfrak{p}}$. We have

$$c'_\sigma u\pi = c'_\sigma \rho = \sigma(\rho) = \sigma(u\pi) = \sigma(u)c_\sigma \pi.$$

Since $\sigma \in I_\mathfrak{p}$, it follows that $\sigma(u) \equiv u \mod \mathfrak{m}_\mathfrak{p}$. Because u is invertible, the residue class $u \mod \mathfrak{m}_\mathfrak{p}$ is also invertible. Hence after dividing both sides by π, we get $c_\sigma \equiv c'_\sigma \mod \mathfrak{m}_\mathfrak{p}$.

Lemma 2.24. *Let $\sigma \in D_\mathfrak{p}$, and π be a uniformizer. Then $c_\sigma \not\equiv 0 \mod \mathfrak{m}_\mathfrak{p}$.*

Proof. We have $\pi = \sigma(\sigma^{-1}(\pi)) = \sigma(c_{\sigma^{-1}}\pi) = \pi c_\sigma \sigma(c_{\sigma^{-1}})$, and after dividing both sides by π, we get $1 = c_\sigma \sigma(c_{\sigma^{-1}})$. Thus the element c_σ is a unit in $\mathcal{O}_{K,\mathfrak{p}}$ and $c_\sigma \notin \mathfrak{m}_\mathfrak{p}$, otherwise $\mathfrak{m}_\mathfrak{p}$ would be the whole ring. □

Recall that the residue field $\kappa(\mathfrak{p})$ is a finite field of characteristic p. Moreover, the multiplicative group of nonzero elements of a finite field is cyclic. A proof of this fact can be found in [DSD03, Proposition 18 in Section 9.5].

Proposition 2.25. *The group $I_\mathfrak{p}/V_1$ is isomorphic to a subgroup of the multiplicative group $\kappa(\mathfrak{p})^\times$. Thus it is a cyclic group.*

Proof. According to Remark 2.23, the residue $\overline{c_\sigma}$ is independant of the choice of the uniformizer. Furthermore, the residue $\overline{c_\sigma}$ is nonzero by Lemma 2.24. Thus the map

$$\begin{array}{rccc} f_0 & : & I_\mathfrak{p} & \longrightarrow & (\mathcal{O}_{K,\mathfrak{p}} \,/\, \mathfrak{m}_\mathfrak{p})^\times \\ & & \sigma & \longmapsto & \overline{c_\sigma}. \end{array}$$

is well-defined. Recall that the fields $\mathcal{O}_{K,\mathfrak{p}} \,/\, \mathfrak{m}_\mathfrak{p}$ and $\kappa(\mathfrak{p})$ are isomorphic by Proposition 2.5. Consequently, it suffices to show that f_0 is a group homorphism and that the kernel is V_1.

Let $\sigma, \tau \in I_\mathfrak{p}$. Then we have $c_{\sigma\tau}\pi = \sigma\tau(\pi) = \sigma(c_\tau \pi) = \sigma(c_\tau)\sigma(\pi) = \sigma(c_\tau)c_\sigma \pi$. Dividing by π we obtain the equality $c_{\sigma\tau} = \sigma(c_\tau)c_\sigma$. Reducing both sides modulo $\mathfrak{m}_\mathfrak{p}$ we get $\overline{c_{\sigma\tau}} = \overline{c_\sigma c_\tau}$, since $\sigma(c_\tau) \equiv c_\tau \mod \mathfrak{m}_\mathfrak{p}$. It follows that f_0 is a group homomorphism.

Let $\sigma \in \ker(f_0)$ i.e. $c_\sigma \equiv 1 \mod \mathfrak{m}_\mathfrak{p}$. Then $c_\sigma = 1 + t\pi$ for some $t \in \mathcal{O}_{K,\mathfrak{p}}$ and we get

$$\sigma(\pi) - \pi = (1 + t\pi)\pi - \pi = t\pi^2 \equiv 0 \mod \mathfrak{m}_\mathfrak{p}^2.$$

Conversely, if $\sigma \in V_1$, then $\sigma(\pi) = \pi + d\pi^2 = (1 + d\pi)\pi$ for some $d \in \mathcal{O}_{K,\mathfrak{p}}$. Thus $c_\sigma = d\pi \in \mathfrak{m}_\mathfrak{p}$ and $\sigma \in \ker(f_0)$. So $\ker(f_0) = V_1$ and the result follows. □

Corollary 2.26. *If $D_\mathfrak{p}$ is abelian, then $I_\mathfrak{p}/V_1$ is cyclic of order dividing $p - 1$.*

Proof. According to Proposition 2.25, the quotient $I_\mathfrak{p}/V_1$ is cyclic. Let $\tau \in I_\mathfrak{p}$, such that its image $\overline{\tau}$ in $I_\mathfrak{p}/V_1$ is a generator. Let $\sigma \in D_\mathfrak{p}$ be such that its image $\bar{\sigma} : \bar{x} \mapsto \bar{x}^p$ is the Frobenius automorphism, which generates $D_\mathfrak{p}/I_\mathfrak{p}$ by Corollary 1.22. As for the proof of Proposition 2.25, we can write

$$\sigma(\pi) = c_\sigma \pi, \quad \tau(\pi) = c_\tau \pi, \quad \sigma\tau\sigma^{-1}(\pi) = c_{\sigma\tau\sigma^{-1}}\pi.$$

Since $\tau \in I_\mathfrak{p}$, we have $\tau(c_{\sigma^{-1}}) = c_{\sigma^{-1}} + b\pi$ for some $b \in \mathcal{O}_{K,\mathfrak{p}}$. Furthermore, we know from the proof of Lemma 2.24 that $\sigma(c_{\sigma^{-1}}) \cdot c_\sigma = 1$. Using this, it is a straightforward computation to show

$$\sigma\tau\sigma^{-1}(\pi) = \sigma(c_\tau)\pi + bc_\sigma^2\sigma(c_\sigma)\pi^2.$$

Dividing by π and reducing modulo $\mathfrak{m}_\mathfrak{p}$, we get $\overline{c_{\sigma\tau\sigma^{-1}}} = \overline{\sigma(c_\tau)} = \overline{\sigma}(\overline{c_\tau}) = \overline{c_\tau}^p$. The last equality comes from the fact that $\overline{\sigma}$ is the Frobenius automorphism. On the other hand, if $D_\mathfrak{p}$ is abelian we have $c_{\sigma\tau\sigma^{-1}} = c_\tau$. This shows that $\overline{c_\tau} = \overline{c_\tau}^p$ and concludes the proof. □

Proposition 2.27. *For $i \geq 1$, the quotient V_i/V_{i+1} is isomorphic to a subgroup of the additive group $\kappa(\mathfrak{p})$.*

Proof. The proof is very similar to the proof of Proposition 2.25. Let σ be an element of V_i and π a uniformizer. By Proposition 2.21, we can write $\sigma(\pi) = \pi + a_\sigma\pi^{i+1}$ for some $a_\sigma \in \mathcal{O}_{K,\mathfrak{p}}$. Then we can define the map

$$\begin{array}{rccc} f_i & : & V_i & \longrightarrow & \mathcal{O}_{K,\mathfrak{P}} \,/\, \mathfrak{m}_\mathfrak{p} \\ & & \sigma & \longmapsto & \overline{a_\sigma} \end{array}.$$

It can be verified that this map is also independent of the uniformizer, but we omit the proof. We show that f_i is an additive group homorphism with kernel V_{i+1}.

Let σ, τ be in V_i and $\sigma\tau(\pi) = \pi + a_{\sigma\tau}\pi^{i+1}$. We have

$$\begin{aligned} \sigma\tau(\pi) &= \sigma\left(\pi + a_\tau\pi^{i+1}\right) \\ &= \sigma(\pi) + \sigma(a_\tau)\sigma(\pi)^{i+1} \\ &= \pi + a_\sigma\pi^{i+1} + \sigma(a_\tau)(1 + a_\sigma\pi^i)^{i+1}\pi^{i+1}. \end{aligned}$$

Since $a_\tau \in \mathcal{O}_{K,\mathfrak{p}}$ and $\sigma \in V_i$, we can write $\sigma(a_\tau) = a_\tau + x\pi^{i+1}$ for some $x \in \mathcal{O}_{K,\mathfrak{p}}$. Moreover, using the biomial formula we can write $(1 + a_\sigma\pi^i)^{i+1} = 1 + x'\pi$ for some $x' \in \mathcal{O}_{K,\mathfrak{p}}$. Putting this together we get

$$\begin{aligned} \sigma\tau(\pi) &= \pi + a_\sigma\pi^{i+1} + (a_\tau + x\pi^{i+1})(1 + x'\pi)\pi^{i+1} \\ &= \pi + (a_\sigma + a_\tau + x'\pi + x\pi^{i+1} + xx'\pi^{i+2})\pi^{i+1}. \end{aligned}$$

Since $x'\pi + x\pi^{i+1} + xx'\pi^{i+2} \equiv 0 \mod \mathfrak{m}_\mathfrak{p}$, we have $\overline{a_{\sigma\tau}} = \overline{a_\sigma} + \overline{a_\tau}$ and thus f_i is an additive group homomorphism.

Let σ lie in the kernel of f_i, i.e. $a_\sigma \equiv 0 \mod \mathfrak{m}_\mathfrak{p}$. Then $a_\sigma = t\pi$ for some $t \in \mathcal{O}_{K,\mathfrak{p}}$ and we have $\sigma(\pi) - \pi = t\pi^{i+2} \equiv 0 \mod \mathfrak{m}_\mathfrak{p}^{i+2}$. Conversely, if $\sigma \in V_{i+1}$, then $\sigma(\pi) = \pi + d\pi^{i+2}$ for some $d \in \mathcal{O}_{K,\mathfrak{p}}$. Thus $a_\sigma = d\pi \equiv 0\,\mathfrak{m}_\mathfrak{p}$, and it follows that $\ker(f_i) = V_{i+1}$. □

3 Cyclotomic fields

3.1 Recollections

We start by recalling some facts about cyclotomic fields. Let $n > 1$ be an integer and let $U(n)$ denote the group of units of $\mathbb{Z}/n\mathbb{Z}$.

Definition 3.1 (Root of unity)**.** A complex number ζ_n is called *n-th root of unity* if it is a root of the polynomial $x^n - 1$.

Let ζ_n and ζ_n' be n-th roots of unity, i.e. $a^n = 1$ and $b^n = 1$. Then ab is also a n-th root of unity since $(ab)^n = a^n b^n = 1$. Moreover, we have $(a^{-1})^n = (a^n)^{-1} = 1$. Hence a^{-1} is also an n-th root of unity. Obviously 1 is also an n-th root unity. Thus the n-th roots of unity form a group under multplication that will be denoted by μ_n.

Proposition 3.2. *The group μ_n is cyclic.*

Proof. The group μ_n is a finite subgroup of the multplicative group $\mathbb{C}^\times$, thus it is cyclic (see for example [DSD03, Proposition 18 in Section 9.5]). □

Definition 3.3 (Primitive root of unity)**.** A generator of the cyclic group μ_n is called a *primitive n-th root of unity.*

Proposition 3.4. *Let ζ_n be a primitive n-th root of unity. The map*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mu_n \\ a &\longmapsto \zeta_n^a \end{aligned}$$

is an isomorphism.

Let ζ_n be an n-th primitive root of unity. Then ζ_n^k is a primitive n-th root of unity if and only if $k \in U(n)$. Hence there are exactly $\varphi(n)$ distinct primitive roots of unity, where $\varphi(n)$ is the Euler φ-function.

Remark 3.5. The Euler φ-function gives the number of integers that are coprime to n. Equivalently, it is the order of the group of units, i.e. $\varphi(n) = |U(n)|$. For a prime power p^m, we have $\varphi(p^m) = p^{m-1}(p-1)$. If $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ is the prime factorization of n, then we have $\varphi(n) = \varphi(p_1^{m_1}) \cdots \varphi(p_r^{m_r})$.

The splitting field of the polynomial $x^n - 1$ is $\mathbb{Q}(\zeta_n)$ and is called the *n-th cyclotomic field.*

Definition 3.6. The *n-th cyclotomic polynomial* $\Phi_n(x)$ is defined as the polynomial

$$\Phi_n(x) \coloneqq \prod_{k \in U(n)} (x - \zeta_n^k),$$

whose roots are the n-th primitive roots of unity.

Theorem 3.7. *The polynomial $\Phi_n(x)$ is a monic irreducible polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.*

Proof. See [DSD03, Theorem 41 in Section 13.6]. □

Theorem 3.7 implies that $\Phi_n(x)$ is the minimal polynomial for ζ_n. Hence we have the following.

Corollary 3.8. *The cyclotomic field $\mathbb{Q}(\zeta_n)$ has degree $\varphi(n)$ over $\mathbb{Q}$.*

In particular, if p is a prime and $m > 0$ an integer, we get $[\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = p^{m-1}(p-1)$.

Proposition 3.9. *Let $n, m > 1$ be integers. Then*

$$\mathbb{Q}(\zeta_n)\,\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\mathrm{lcm}(m,n)}).$$

Proof. Let $f \coloneqq \mathrm{lcm}(m,n)$ and $d \coloneqq \gcd(m,n)$. Since $n|f$ and $m|f$, we have $\zeta_n^f = \zeta_m^f = 1$. Thus $\zeta_n, \zeta_m \in \mathbb{Q}(\zeta_f)$ and $\mathbb{Q}(\zeta_n)\,\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_f)$.

Let $\zeta_k \coloneqq e^{\frac{2\pi i}{k}}$ for $k > 1$, then ζ_k is a primitive k-th root of unity. By the Chinese Remainder Theorem, there exist integers $a, b \in \mathbb{Z}$, such that $am + bn = d = \frac{mn}{f}$. Dividing both sides by mn, we get $\frac{a}{n} + \frac{b}{m} = \frac{1}{f}$. Thus we have:

$$\zeta_n^a \zeta_m^b = e^{\frac{2\pi i a}{n}} e^{\frac{2\pi i b}{m}} = e^{2\pi i(\frac{a}{n} + \frac{b}{m})} = e^{\frac{2\pi i}{f}} = \zeta_f.$$

Hence $\zeta_f \in \mathbb{Q}(\zeta_n)\,\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_f) \subseteq \mathbb{Q}(\zeta_n)\,\mathbb{Q}(\zeta_m)$. □

3.2 The Galois group of cyclotomic field extensions

Let ζ_n be a primitive root of unity. We have seen that the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$ is the splitting field of the polynomial $x^n - 1$. The roots are exactly the roots of unity. Since they are all distinct (in $\mathbb{C}$), the polynomial $x^n - 1$ is separable and hence the extension $\mathbb{Q}(\zeta_n)|\,\mathbb{Q}$ is Galois.

Let σ be an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\,\mathbb{Q})$. The automorphism σ permutes the roots of the cyclotomic polynomial $\Phi_n(x)$, i.e. $\sigma(\zeta_n) = \zeta_n^a$ for some $a \in U(n)$. The image of ζ_n uniquely determines an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\,\mathbb{Q})$. We denote by σ_a the automorphism that sends ζ_n to ζ_n^a.

Theorem 3.10. *The map*

$$\begin{aligned} U(n) &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\,\mathbb{Q}) \\ a &\longmapsto \sigma_a \end{aligned}$$

is an isomorphism.

In the proof of the Kronecker-Weber Theorem we restrict ourselves to the case where $n = p^m$ is a prime power. Hence we state the following:

Corollary 3.11. *Let p be a prime and $m > 0$ an integer. Then $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^m})|\,\mathbb{Q})$ is a cyclic group of degree $p^{m-1}(p-1)$.*

3.3 Ramification in cyclotomic fields

In order to understand the ramification of primes in a cyclotomic field, we need to know the structure of its ring of integers. This is given by the following:

Theorem 3.12. *Let $n > 1$ be an integer. Let $K \coloneqq \mathbb{Q}(\zeta_n)$ and let $\mathcal{O}_K$ be the ring of integers. Then we have*

$$\mathcal{O}_K = \mathbb{Z}[\zeta_n].$$

Proof. See [Neu99, Theorem 10.2 in Chapter 1]. □

In the following Propositions, we will only consider ramification in the case where $n = p^m$ is a prime power.

Proposition 3.13. *The prime p is totally ramified in $\mathbb{Q}(\zeta_{p^m})$.*

Proof. Let $\zeta \coloneqq \zeta_{p^m}$ and $\Phi(x) \coloneqq \Phi_{p^m}(x)$ the p^m-th cyclotomic polynomial, the minimal polynomial of ζ. Recall that we have

$$\Phi(x) = \prod_{i \in U(p^m)} \left(x - \zeta^i\right) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = 1 + x^{p^{m-1}} + x^{2p^{m-1}} + \cdots + x^{(p-1)p^{m-1}}.$$

For $x = 1$, we get:

$$p = \prod_{i \in U(p^m)} \left(1 - \zeta^i\right). \tag{1}$$

Let $\xi_i \coloneqq \frac{1-\zeta^i}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{i-1} \in \mathbb{Z}[\zeta]$, for $i \in U(p^m)$. Since $i \in U(p^m)$, there exists an integer k, such that $ik \equiv 1 \mod p^m$. Thus we have

$$\xi_i^{-1} = \frac{1-\zeta}{1-\zeta^i} = \frac{1-\zeta^{ik}}{1-\zeta^i} = 1 + \zeta^i + \cdots + (\zeta^i)^{k-1} \in \mathbb{Z}[\zeta].$$

Hence ξ_i is a unit in $\mathbb{Z}[\zeta]$, Equation (1) becomes $p = \xi \cdot (1-\zeta)^{\varphi(p^m)}$, where $\xi \coloneqq \prod_{i \in U(p^m)} \xi_i$ is also a unit. Hence in $\mathbb{Z}[\zeta]$ we have $(p) = \mathfrak{p}^{\varphi(p^m)}$ where $\mathfrak{p} = (1-\zeta)$. Since $[\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = \varphi(p^m)$, the ideal $\mathfrak{p} = (1-\zeta_p)$ must be prime, and consequently p is totally ramified. □

Proposition 3.14. *The prime p is the only ramified prime in $\mathbb{Q}(\zeta_{p^m})$, except in the case where $p = 2$ and $m = 1$.*

Proof. See [Neu99, Corollary 10.4 in Chapter 1]. □

4 The quadratic Gauss sum

In order to prove the Kronecker-Weber Theorem, we need the notion of Gauss sums. A Gauss sum is a particular type of finite sum of roots of unity.

Definition 4.1 (Quadratic residue)**.** Let $n > 1$ and a be integers such that $\gcd(a, n) = 1$. We say that a is a *quadratic residue modulo* n, if there exists an integer x, such that $x^2 \equiv a \pmod{n}$. Otherwise, we say that it is a quadratic nonresidue.

Definition 4.2 (Legendre symbol)**.** Let a be an integer and q be an odd prime. The Legendre symbol is defined as:

$$\left(\frac{a}{q}\right) := \begin{cases} 1 & \text{if} \quad a \text{ is a quadratic residue modulo } q \\ -1 & \text{if} \quad a \text{ is a quadratic nonresidue modulo } q \\ 0 & \text{if} \quad a \equiv 0 \pmod{q} \end{cases}$$

Proposition 4.3 (Euler's Criterion)**.** *If* $a \not\equiv 0 \pmod{q}$*, then* $\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \pmod{q}$*.*

Proof. See [Rib01, Proposition G in Section 4.1]. □

Proposition 4.4 (Properties of the Legendre symbol)**.** *The Legendre symbol satisfies the following properties:*

1. *If* $a \equiv b \pmod{q}$*, then* $\left(\frac{a}{q}\right) = \left(\frac{b}{q}\right)$,
2. $\left(\frac{a^2}{q}\right) = \begin{cases} 1 & \textit{if} \quad a \not\equiv 0 \pmod{q} \\ 0 & \textit{if} \quad a \equiv 0 \pmod{q} \end{cases}$,
3. $\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right)$.

Proof. If $a \equiv 0 \pmod{q}$, then all the statements are trivial. So assume $a \not\equiv 0 \pmod{q}$. The statements (1.) and (2.) follow directly from the definition of the Legendre symbol.

From Euler's Criterion, we know that $(ab)^{\frac{q-1}{2}} \equiv \left(\frac{ab}{q}\right) \pmod{q}$. On the other hand, we also have $(ab)^{\frac{q-1}{2}} \equiv (a)^{\frac{q-1}{2}}(b)^{\frac{q-1}{2}} \equiv \left(\frac{a}{q}\right)\left(\frac{b}{q}\right) \pmod{q}$, thus $\left(\frac{a}{q}\right)\left(\frac{b}{q}\right) \equiv \left(\frac{ab}{q}\right) \pmod{q}$. Since q is odd, this implies $\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right)$. □

Proposition 4.5. *There are as many quadratic residues as quadratic nonresidues, i.e.*

$$\sum_{v=1}^{q-1} \left(\frac{v}{q}\right) = 0.$$

Proof. Consider the group homomorphism

$$\begin{array}{ccccc} \phi & : & U(q) & \longrightarrow & U(q) \\ & & x & \longmapsto & x^2 \end{array}.$$

Clearly a is a quadratic residue if and only if $a \in \mathrm{Im}(\phi)$. Moreover, we have $\ker(\phi) = \{\pm 1\}$ and $|\mathrm{Im}(\phi)| = \frac{|U(q)|}{|\ker(\phi)|} = \frac{q-1}{2}$. Thus there are exactly $\frac{q-1}{2}$ quadratic residues and $q - 1 - \frac{q-1}{2} = \frac{q-1}{2}$ quadratic nonresidues. □

Definition 4.6 (Quadratic Gauss sum)**.** Let q be a an odd prime and $\zeta \coloneqq \zeta_q$ a q-th root of unity. For $a \in \mathbb{Z}$, the *quadratic Gauss sum* is defined as:

$$\tau(a) \coloneqq \sum_{u=1}^{q-1} \left(\frac{u}{q}\right) \zeta^{au}.$$

Remark 4.7. Obviously $\tau(a) \in \mathbb{Z}[\zeta_q]$.

Proposition 4.8. *We have* $\tau(1)^2 = (-1)^{\frac{q-1}{2}} \cdot q$.

Proof. The sum $\tau(1)^2$ can be written as:

$$\begin{aligned}
\tau(1)^2 &= \left(\sum_{u=1}^{q-1} \left(\frac{u}{q}\right) \zeta^u\right) \cdot \left(\sum_{t=1}^{q-1} \left(\frac{t}{q}\right) \zeta^t\right) \\
&= \sum_{u=1}^{q-1} \sum_{t=1}^{q-1} \left(\frac{u}{q}\right) \left(\frac{t}{q}\right) \zeta^{(u+t)} \\
&= \sum_{u=1}^{q-1} \sum_{t=1}^{q-1} \left(\frac{ut}{q}\right) \zeta^{(u+t)},
\end{aligned}$$

where the last equation follows from Proposition 4.4. Since u and t are elements of the multplicative group $U(q)$, there exists a unique element v in this group, such that $t = uv$ for every u and t. Moreover, by Proposition 4.4, we have $\left(\frac{u^2 v}{q}\right) = \left(\frac{u^2}{q}\right)\left(\frac{v}{q}\right) = \left(\frac{v}{q}\right)$. Hence, it follows that

$$\begin{aligned}
\sum_{u=1}^{q-1} \sum_{t=1}^{q-1} \left(\frac{ut}{q}\right) \zeta^{(u+t)} &= \sum_{u=1}^{q-1} \sum_{v=1}^{q-1} \left(\frac{u^2 v}{q}\right) \zeta^{u(1+v)} \\
&= \sum_{u=1}^{q-1} \sum_{v=1}^{q-1} \left(\frac{v}{q}\right) \zeta^{u(1+v)} \\
&= \sum_{v=1}^{q-1} \left(\frac{v}{q}\right) \left(\sum_{u=1}^{q-1} \zeta^{u(1+v)}\right). \qquad (2)
\end{aligned}$$

If $v = q-1$, then for the inner sum we get

$$\sum_{u=1}^{q-1} \zeta^{u(1+v)} = \sum_{u=1}^{q-1} \zeta^{uq} = \sum_{u=1}^{q-1} 1 = q - 1.$$

If $v \neq q-1$, then $v+1 \neq 0$ in $U(q)$. Hence, for every $u \in U(q)$ there is a unique $x \in U(q)$ such that $u(v+1) = x$. This means that the inner sum is equal to

$$\sum_{u=1}^{q-1} \zeta^{u(1+v)} = \sum_{x=1}^{q-1} \zeta^x = \zeta + \zeta^2 + \cdots + \zeta^{q-1} = -1.$$

Substituing this into equation (2) and using Propositions 4.4 and 4.5, it follows that

$$\begin{aligned}
\sum_{v=1}^{q-1}\left(\frac{v}{q}\right)\left(\sum_{u=1}^{q-1}\zeta^{u(1+v)}\right) &= \left(\frac{q-1}{q}\right)\cdot(q-1)-\sum_{v=1}^{q-2}\left(\frac{v}{q}\right)\\
&= \left(\frac{q-1}{q}\right)\cdot q-\left(\frac{q-1}{q}\right)-\sum_{v=1}^{q-2}\left(\frac{v}{q}\right)\\
&= \left(\frac{-1}{q}\right)\cdot q-\sum_{v=1}^{q-1}\left(\frac{v}{q}\right)\\
&= \left(\frac{-1}{q}\right)\cdot q\\
&= (-1)^{\frac{q-1}{2}}\cdot q.
\end{aligned}$$

□

5 Proof of the Kronecker-Weber Theorem

In this last section, we present a proof of the Kronecker-Weber Theorem. We say that an extension $K|\mathbb{Q}$ is a *p-power extension* if the degree $[K:\mathbb{Q}]$ is a power of a prime p. We say that an extension is *unramified outside* p if p is the only prime that is ramified in K.

5.1 A few Lemmas

We begin by stating a sequence of Lemmas that will be needed in the proof. They are separated from the main Propositions to make the structure of the proof of the Kronecker-Weber Theorem more apparent.

Lemma 5.1. *Let $K|\mathbb{Q}$ be a finite Galois extension and let p be a rational prime. If p is the only ramified prime, then p is totally ramified in K.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p and $K^{I_\mathfrak{p}}$ the inertia field. By Corollary 1.26 the extension $K^{I_\mathfrak{p}}|\mathbb{Q}$ is unramified at p. Furthermore, this extension is also unramified outside p, since any prime that ramifies in $K^{I_\mathfrak{p}}$ must ramify in K. According to Minkowski's Theorem (1.14), we have $K^{I_\mathfrak{p}} = \mathbb{Q}$. Since $e(\mathfrak{p}|p) = [K : K^{I_\mathfrak{p}}]$ by Corollary 1.24, we get $e(\mathfrak{p}|p) = [K:\mathbb{Q}]$ and p is totally ramified. □

Lemma 5.2. *Let $K|\mathbb{Q}$ be a p-power Galois extension unramified outside p and $\mathfrak{p}$ a prime of $\mathcal{O}_K$ lying over p. Then, for the ramification groups we get:*

1. *V_i/V_{i+1} is trivial or cyclic of order p,*
2. *$I_\mathfrak{p} = V_1 = G_K$.*

Proof. Let $\mathfrak{p}$ be a prime lying above p. By Lemma 5.1 the prime p is totally ramified, hence the inertial degree $f(\mathfrak{p}|p)$ is equal to 1 and $I_\mathfrak{p} = G_K$. This means that the residue field $\kappa(\mathfrak{p})$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. By Proposition 2.27, we conclude that V_i/V_{i+1} is either trivial or isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Furthermore, we know from Proposition 2.25 that $I_\mathfrak{p}/V_1$ is a subgroup of $\kappa(\mathfrak{p})^\times$. Thus the order of $I_\mathfrak{p}/V_1$ divides $|\kappa(\mathfrak{p})^\times| = p-1$. On the other hand, the order of $I_\mathfrak{p}/V_1$ must be a power of p since it is a quotient of subgroups of the p-group G_K. This is only possible if $I_\mathfrak{p}/V_1$ is trivial, i.e. $V_1 = I_\mathfrak{p} = G_K$. □

Lemma 5.3. *Let p be an odd prime and $K|\mathbb{Q}$ be an extension of degree p unramified outside p. Then the second ramification group V_2 is trivial.*

Proof. Let $\mathfrak{p}$ be the prime of $\mathcal{O}_K$ lying above p. Consider the localization $\mathcal{O}_{K,\mathfrak{p}}$ and let π be a uniformizer. Finally, let $m(x) \coloneqq x^p + a_{p-1}x^{p-1} + \cdots + a_0$ be the minimal polynomial of π over $\mathbb{Q}$, and $m'(x) = px^{p-1} + (p-1)a_{p-1}x^{p-2} + \cdots + a_1$ its formal derivative.

We know from Proposition 2.19 that the ramification groups eventually become trivial. Let V_{i+1} be the first trivial ramification group. By Lemma 5.2, the quotient V_i/V_{i+1} must be cyclic of order p since $V_i \neq V_{i+1} = \{e\}$. Hence, the group V_i has to be cyclic of order p i.e. it is the whole Galois group G_K.

<u>*Claim 1:*</u> We have $v_\mathfrak{p}(m'(\pi)) = (p-1)(i+1)$.

Proof of Claim 1: The factorization of $m(x)$ is given by $\prod_{\sigma\in G_K}(x-\sigma(\pi))$. Using the product rule, it is a straightforward computation to show that

$$m'(\pi) = \prod_{\sigma\in G_K\setminus\{e\}} (\pi - \sigma(\pi)),$$

where e is the identity of G_K. Since $V_i = G_K$ and V_{i+1} is trivial, we can write $G_K\setminus\{e\} = V_i\setminus V_{i+1}$. By Proposition 2.22, for every $\sigma \in V_i \setminus V_{i+1}$ we have

$$v_{\mathfrak{p}}(\sigma(\pi) - \pi) = i + 1.$$

Since there are $p-1$ elements in $G_K \setminus \{e\}$ and $v_{\mathfrak{p}}(ab) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b)$, it follows that

$$v_{\mathfrak{p}}(m'(\pi)) = (p-1)(i+1).$$

■

Claim 2: We have $2p - 1 \geq v_{\mathfrak{p}}(m'(\pi))$.

Proof of Claim 2: According to Proposition 2.15, for any $x \in \mathbb{Q}$ we have $v_{\mathfrak{p}}(x) = e(\mathfrak{p}\,|p)v_p(x)$. Since p is totally ramified, we know that $e(\mathfrak{p}\,|p) = p$. Thus $v_{\mathfrak{p}}(p) = p$ and $v_{\mathfrak{p}}(a_k) \equiv 0 \mod p$, for $1 \leq k \leq p$. By the properties of the valuation, if $a_k \neq 0$ it follows that

$$v_{\mathfrak{p}}(ka_k\pi^{k-1}) = v_{\mathfrak{p}}(k) + v_{\mathfrak{p}}(a_k) + k - 1 \equiv k - 1 \mod p.$$

In particular, all these valuations are different and by Proposition 2.13 we get

$$v_{\mathfrak{p}}(m'(\pi)) = v_{\mathfrak{p}}(p\pi^{p-1} + \cdots + a_1) = \min_{\substack{1\leq k\leq p\\ a_k\neq 0}} \left\{v_{\mathfrak{p}}(ka_k\pi^{k-1})\right\} \leq v_{\mathfrak{p}}(pa_p\pi^{p-1}).$$

Since $m(x)$ is a minimal polynomial, it is monic. Thus $a_p = 1$ and we can conclude that

$$v_{\mathfrak{p}}(m'(\pi)) \leq v_{\mathfrak{p}}(p\pi^{p-1}) = v_{\mathfrak{p}}(p) + v_{\mathfrak{p}}(\pi^{p-1}) = 2p - 1.$$

■

From Claims 1 and 2 follows the inequality $2p - 1 \geq (p-1)(i+1)$, which is equivalent to $1 + \frac{1}{p-1} \geq i$. Since $p > 2$, we have $2 > 1 + \frac{1}{p-1}$. The only possible solutions are $i = 0$ and $i = 1$. If $i = 0$, then V_1 would be the first trivial ramification group and this would contradict Lemma 5.2. Hence $i = 1$ and V_2 is the first trivial ramification group. □

Lemma 5.4. *Let G be an abelian p-group with a unique subgroup H of index p. Then G is cyclic.*

Proof. See for example [Rib01, Lemma 1 in Chapter 15]. □

Lemma 5.5. *Let p be an odd prime and $K|\,\mathbb{Q}$ be an abelian p-power extension unramified outside p. Then $K|\,\mathbb{Q}$ is cyclic.*

Proof. Since $K|\,\mathbb{Q}$ is a p-power extension, we have $[K:\mathbb{Q}] = p^m$ for some integer $m \geq 1$. If $m = 1$, then $[K:\mathbb{Q}] = p$. Hence G_K must be isomorphic to $\mathbb{Z}/p\,\mathbb{Z}$, which is cyclic. So we can assume $m > 1$. Let $\mathfrak{p}$ be the prime ideal of $\mathcal{O}_K$ lying over p and V_i be the i-th ramification group of K. Recall that $\sigma \in V_i$ if and only if $\sigma(x) \equiv x \mod \mathfrak{p}^{i+1}$ for every $x \in \mathcal{O}_K$.

Claim 1: Let $H \leq G_K$ be a subgroup of index p. Then $V_2 \leq H$.

Proof of Claim 1: Let H be a subgroup of index p and $K' \coloneqq K^H$ its fixed field with Galois group $G_{K'} \cong G_K/H$. Let $\mathfrak{p}' \coloneqq \mathfrak{p} \cap K'$ be the prime ideal of $\mathcal{O}_{K'}$ lying over p and V_i' the i-th ramification group of K'. This means that $\sigma \in V_i'$ if and only if $\sigma(x) \equiv x \mod \mathfrak{p}'^{i+1}$ for every $x \in \mathcal{O}_{K'}$.

$$\mathbb{Q} \overset{p}{\text{———}} K' \overset{p^{m-1}}{\text{———————}} K$$

Let $\sigma \in V_2$. If we consider the restriction to K', then $\sigma \restriction_{K'}$ is in V_2' since $\mathfrak{p}' = \mathfrak{p} \cap K'$ and $\mathcal{O}_K' = \mathcal{O}_K \cap K'$. As $K'|\,\mathbb{Q}$ has degree p and is unramified outside p (since K is), we can apply Lemma 5.3. Thus V_2' is trivial. This means that every element $\sigma \in V_2$ fixes K', i.e $\sigma \in \mathrm{Gal}(K|K') = H$. Hence $V_2 \leq H$. ■

Claim 2: Let $H \leq G_K$ be a subgroup of index p. Then $H = V_2$.

Proof of Claim 2: Let V_i be the first ramification group that is not the entire Galois group. By Lemma 5.2, we have $I_\mathfrak{p} = V_1 = G_K$, thus $i \geq 2$. Since $V_i \neq V_{i-1} = G_K$, Lemma 5.2 implies that $V_{i-1}/V_i = G_K/V_i$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Thus V_i is a subgroup of index p. By Claim 1, it follows that $V_2 \leq V_i$. On the other hand, V_i is a subgroup of V_2 for $i \geq 2$, hence $V_i = V_2$ and V_2 has index p. We have $p = (G_K : V_2) = (G_K : H) \cdot (H : V_2) = p(H : V_2)$, and thus $(H : V_2) = 1$ i.e. $H = V_2$. ■

These two claims prove that V_2 is the unique subgroup of index p and by Lemma 5.4, this conludes the proof. □

Lemma 5.6. *Let $K|\,\mathbb{Q}$ be an abelian p-power extension. Let $q \neq p$ be a prime number and $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_K$ lying over q. Then the inertia group $I_\mathfrak{q}$ is cyclic and its order divides $q-1$.*

Proof. Let p^m be the degree of the extension, where $m > 0$ is some integer. By Proposition 2.27, for $i \geq 1$ the quotient V_i/V_{i+1} is isomorphic to a subgroup of the additive group of $\kappa(\mathfrak{q}) = \mathcal{O}_K/\mathfrak{q}$. Recall that $|\kappa(\mathfrak{q})| = q^f$ where $f = f(\mathfrak{q}\,|q)$ is the inertial degree. So on the one hand, the order of V_i/V_{i+1} has to divide q^f.

On the other hand, we have $V_i \leq G_K$ for every $i \geq 0$. Since G_K has order p^m, the order of V_i/V_{i+1} must divide p^m. Since $q \neq p$, the quotients V_i/V_{i+1} must be trivial for $i \geq 1$. By Proposition 2.19, there exists an integer i_0 such that $V_{i_0} = \{e\}$. Thus all the higher ramification groups are trivial for $i \geq 1$. In particular V_1 is trivial.

Moreover, the decomposition group $D_\mathfrak{q}$ is abelian, since it is a subgroup of G_K. By Corollary 2.26, we know that if $D_\mathfrak{q}$ is trivial, then $I_\mathfrak{q}/V_1$ is cyclic of order dividing $q-1$. Since V_1 is trivial, this concludes the proof. □

5.2 Proof for cyclic p-power extensions unramified outside p

5.2.1 The case $p = 2$

Proposition 5.7. *If $K|\,\mathbb{Q}$ is a quadratic extension, then K is cyclotomic.*

Proof. Let $K \coloneqq \mathbb{Q}(\sqrt{d})$, where d is a squarefree integer. If $d = \pm 2^r q_1 \cdots q_k$ with $r = 0, 1$ is the prime factorization of d, then

$$\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{q_1}, \ldots, \sqrt{q_k}).$$

Thus we can reduce the proof to the case $\mathbb{Q}(\sqrt{\pm q})$ where q is a prime.

Let $\zeta_8 \coloneqq e^{\frac{2\pi i}{8}}$ and $\zeta_4 \coloneqq e^{\frac{2\pi i}{4}}$. Since $\zeta_4^2 = -1$ and $\zeta_8^2 = \zeta_4$, we have

$$\left(\zeta_8 + \zeta_8^{-1}\right)^2 = \zeta_4 + \zeta_4^{-1} + 2 = \zeta_4^{-1}(\zeta_4^2 + 1) + 2 = 2 \quad \text{and} \quad \zeta_4^2\left(\zeta_8 + \zeta_8^{-1}\right)^2 = -2.$$

Thus $\sqrt{\pm 2} \in \mathbb{Q}(\zeta_8)$.

If q is an odd prime, then from Proposition 4.8 it follows that either $\tau(1)^2 = q$ or $\tau(1)^2 = -q$. Since $\zeta_4^2 = -1$, we have either $\tau(1)^2 = q$ or $\zeta_4^2\tau(1)^2 = q$. Since $\tau(1) \in \mathbb{Q}(\zeta_q)$, we get that $\sqrt{\pm q} \in \mathbb{Q}(\zeta_4, \zeta_q)$.

All this together shows that $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_4, \zeta_8, \zeta_{q_1}, \ldots, \zeta_{q_k}) = \mathbb{Q}(\zeta_8, \zeta_{q_1}, \ldots, \zeta_{q_k}) \subseteq \mathbb{Q}(\zeta_{8q_1\cdots q_k})$, hence $\mathbb{Q}(\sqrt{d})$ is cyclotomic.

□

Proposition 5.8. *Let $m > 0$ be an integer. If $K|\,\mathbb{Q}$ is a cyclic extension of degree 2^m and 2 is the only ramified prime, then K is cyclotomic.*

Proof. We will prove this by induction on m.

Induction basis: If $m = 1$, then $K|\,\mathbb{Q}$ is a quadratic extension and is cyclotomic by Proposition 5.7.

Induction step: Let $m > 1$ and let $K|\,\mathbb{Q}$ be a cyclic extension of degree 2^m where 2 is the only ramified prime. Let $\zeta \coloneqq \zeta_{2^{m+2}}$.

Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta)|\,\mathbb{Q}) \cong \left(\mathbb{Z}/2^{m+2}\,\mathbb{Z}\right)^\times \cong (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/2^m\,\mathbb{Z})$, where the $(\mathbb{Z}/2\,\mathbb{Z})$ part is the complex conjugation $\sigma\colon \zeta \mapsto \zeta^{-1}$. Hence the fixed field of $\langle\sigma\rangle$ is given by $L = \mathbb{Q}(\zeta + \zeta^{-1})$ and is cyclic of degree 2^m over $\mathbb{Q}$. Fix an embedding of K into $\mathbb{C}$. The complex conjugation restricted to K has order dividing 2. This means that the real subfield of K fixed by complex conjugation has degree 2^{m-1} or 2^m depending on whether K is real or not, and hence

$$[K \cap \mathbb{R} : \mathbb{Q}] \geq 2^{m-1}.$$

Because $m > 1$, the unique quadratic subfield of K is real and of the form $\mathbb{Q}(\sqrt{d})$ where d is a positive squarefree integer. Since it is unramified outside 2, we must have $d = 2$ [Rib01, Proposition K in Section 11.2]. Analogously, since L is unramified outside 2, the field $\mathbb{Q}(\sqrt{2})$ is also a quadratic subfield of L and hence

$$[K \cap L : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

From Proposition 1.31 we know that $G_{KL} \cong \{(\sigma, \tau) \mid \sigma\restriction_{K\cap L} = \tau\restriction_{K\cap L}\} \leq G_K \times G_L$.

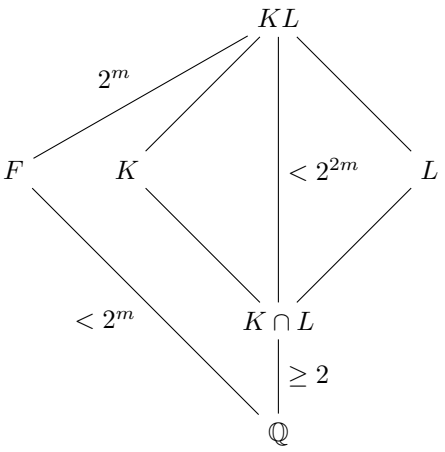
Claim 1: There exist generators σ and τ of the cyclic groups G_K and G_L agreeing on $K \cap L$.

Proof of Claim 1: Let $\langle x\rangle$ be a cyclic non-trivial 2-group, i.e. its order is a power of 2. Then from group theory we know that x^k is a generator of G if and only if k is odd.

Let σ be a generator of G_K. Then since $G_{K\cap L} \cong G_K/\,\mathrm{Gal}(K|K \cap L)$, the restriction $\sigma\restriction_{K\cap L}$ is a generator of $G_{K\cap L}$. Moreover, since we also have $G_{K\cap L} \cong G_L/\,\mathrm{Gal}(L|K \cap L)$, there exists $\tau \in G_L$ such that $\tau\restriction_{K\cap L} = \sigma\restriction_{K\cap L}$. Let ψ be a generator of G_L, then $\tau = \psi^k$ for some $k \in \mathbb{Z}$. Now $\psi\restriction_{K\cap L}$ is also a generator of $G_{K\cap L}$ and we have $(\psi\restriction_{K\cap L})^k = \psi^k\restriction_{K\cap L} = \sigma\restriction_{K\cap L}$. This implies that k is odd because $G_{K\cap L}$ is a nontrivial cyclic 2-group. Thus $\tau = \psi^k$ generates G_L, since k is odd. ■

Let $H \coloneqq \langle(\sigma, \tau)\rangle$ and $F \coloneqq (KL)^H$ be its fixed field. The group H has order 2^m and $2^{2m} > [KL : \mathbb{Q}]$ because $K \cap L \neq \mathbb{Q}$. Hence we have $[F : \mathbb{Q}] < 2^m$, since

$$2^{2m} > [KL : \mathbb{Q}] = [KL : F] \cdot [F : \mathbb{Q}] = |H| \cdot [F : \mathbb{Q}] = 2^m [F : \mathbb{Q}].$$



Claim 2: We have $FL = KL$.

Proof of Claim 2: We know that $FL \subset KL$, since both F and L are in KL. Let ϕ be an automorphism of KL fixing FL. The subfields F and L of FL are also fixed by ϕ. Since ϕ fixes F, we have $\phi \in H = \langle(\sigma, \tau)\rangle$ so $\phi = (\sigma^i, \tau^i)$ for some integer i. As the only automorphism fixing L is the identity, we get $\tau^i = e$. But σ and τ have the same order, thus $\sigma^i = e$. This implies that ϕ is the identity and hence $FL = KL$. ■

By our induction hypothesis, F is cyclotomic, and thus FL is also cyclotomic.

□

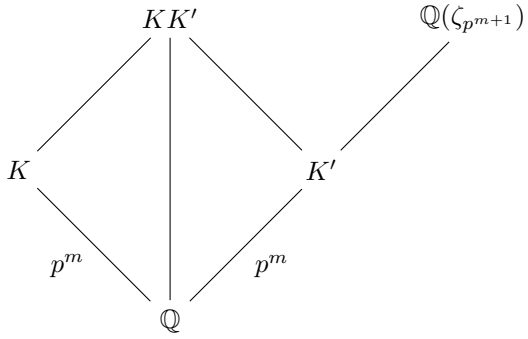
5.2.2 The case $p > 2$

Proposition 5.9. *Let p be an odd prime and $m > 1$ an integer. If $K|\,\mathbb{Q}$ is a cyclic extension of degree p^m and p is the only ramified prime, then K is cyclotomic.*

Proof. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{m+1}})|\,\mathbb{Q})$ is isomorphic to $\left(\mathbb{Z}/p^{m+1}\mathbb{Z}\right)^\times$. Since this is a cyclic group of order $p^m(p-1)$, it has a unique cyclic subgroup of index p^m. Let K' be the subfield of $\mathbb{Q}(\zeta_{p^{m+1}})$ corresponding to this subgroup. Thus we have

$$G_{K'} \cong \mathbb{Z}/p^m\mathbb{Z} \cong G_K.$$

Let KK' be the compositum of K and K'. We have the following diagram:



The compositum KK' is a p-power extension of $\mathbb{Q}$, since

$$[KK' : \mathbb{Q}] = \frac{[K : \mathbb{Q}][K' : \mathbb{Q}]}{[K \cap K' : \mathbb{Q}]} = \frac{p^{2m}}{[K \cap K' : \mathbb{Q}]}.$$

By Corollary 1.33, the compositum of two extensions unramified outside p is also unramified outside p. So KK' is unramified outside p. Hence $KK'|\,\mathbb{Q}$ is cyclic by Lemma 5.5. This implies that $[KK' : \mathbb{Q}] = |G_{KK'}| \leq p^m$, since $G_{KK'}$ is a cyclic subgroup of $(\mathbb{Z}/p^m\,\mathbb{Z}) \times (\mathbb{Z}/p^m\,\mathbb{Z})$.

On the other hand, we also have $p^m = [K : \mathbb{Q}] = [K' : \mathbb{Q}] \leq [KK' : \mathbb{Q}]$. Thus $K = K' = KK'$, since $[KK' : \mathbb{Q}] = [K : \mathbb{Q}] = [K' : \mathbb{Q}] = p^m$.

□

5.3 Proof for cyclic p-power extensions

Proposition 5.10. *Let $K|\,\mathbb{Q}$ be a cyclic p-power extension. Then K is cyclotomic.*

Proof. Let N be the number of rational primes $q \neq p$ that ramify in K; this number is finite by Minkowski's Theorem. We will prove this Proposition by induction on N.

Induction basis: If $N = 0$ and p is ramified, then $K|\,\mathbb{Q}$ is a cyclic p-power extension where p is the only ramified prime. This is exactly the content of Propositions 5.9 and 5.8. If p is unramified, then every prime is unramified in K. By Minkowski's Theorem, we have $K = \mathbb{Q}$ which is (trivially) cyclotomic.

Induction hypothesis If $K|\,\mathbb{Q}$ is a cyclic p-power extension where N primes different from p ramify, then K is cyclotomic.

Induction step: Let $K|\,\mathbb{Q}$ be a cyclic p-power extension where $N + 1$ primes different from p ramify. Let p^m be the degree of this extension, for some integer $m > 0$. Let $q \neq p$ be one of the primes that ramify and $\mathfrak{q}$ an ideal of $\mathcal{O}_K$ lying over q.

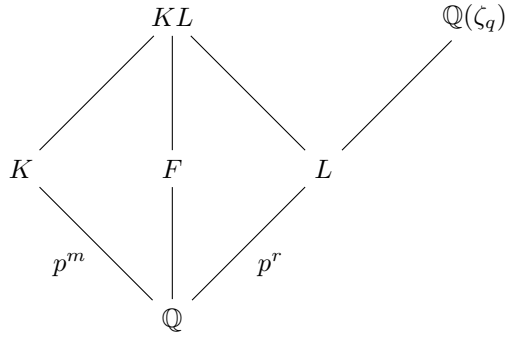
By Lemma 5.6, we know that the inertia group $I_\mathfrak{q}$ is cyclic of order dividing $q - 1$. We also know that the order of $I_\mathfrak{q}$ divides p^m, since the inertia group is a subgroup of G_K, which has order p^m. Hence we have $|I_\mathfrak{q}| = p^r$ for some $r \leq m$, such that p^r divides $q - 1$.

Consider the cyclotomic field extension $\mathbb{Q}(\zeta_q)|\,\mathbb{Q}$, which is cyclic of degree $q - 1$. Since p^r divides $q - 1$, there exists a unique subfield L of $\mathbb{Q}(\zeta_q)$ such that

$$[L : \mathbb{Q}] = p^r.$$

Because q is totally ramified in $\mathbb{Q}(\zeta_q)$, it is totally ramified in L by Corollary 1.27. Let $\mathfrak{L}$ be the prime ideal of $\mathcal{O}_L$ lying over q.

Finally, let KL be the compositum of K and L and let $\mathfrak{Q}$ be an ideal of $\mathcal{O}_{KL}$ lying over q. Let $I_{\mathfrak{Q}}$ be its inertia group and $F \coloneqq (KL)^{I_{\mathfrak{Q}}}$. The setup is summarized in the following diagram.



<u>*Claim 1:*</u> The extension $KL|F$ is cyclic of order p^r.

Proof of Claim 1: Applying Lemma 5.6 to the p-power extension $KL|\mathbb{Q}$, we can conclude that $I_{\mathfrak{Q}}$ is a cyclic group. Hence $KL|F$ is a cyclic extension, since $\mathrm{Gal}(KL|F) \cong I_{\mathfrak{Q}}$.

By Proposition 1.32, the inertia group $I_{\mathfrak{Q}}$ is a subgroup of $I_{\mathfrak{q}} \times I_{\mathfrak{L}}$, which is isomorphic to $(\mathbb{Z}/p^r\mathbb{Z}) \times (\mathbb{Z}/p^r\mathbb{Z})$ and has no element of order greater than p^r. Hence we have $|I_{\mathfrak{Q}}| \leq p^r$, otherwise there would be an element of order greater than p^r.

Furthermore, we know that $e(\mathfrak{L}|q) = [L : \mathbb{Q}] = p^r$ because q is totally ramified in L. Since the ramification degree is multiplicative for tower of fields by Proposition 1.13, we get

$$|I_{\mathfrak{Q}}| = e(\mathfrak{Q}\,|q) = e(\mathfrak{Q}\,|\mathfrak{L}) \cdot e(\mathfrak{L}|q) = e(\mathfrak{Q}\,|\mathfrak{L}) \cdot p^r \geq p^r,$$

thus $I_{\mathfrak{Q}} = p^r$. ■

<u>*Claim 2:*</u> We have $F \cap L = \mathbb{Q}$.

Proof of Claim 2: Let $\mathfrak{Q}' \coloneqq \mathfrak{q} \cap F \cap L$ be a prime ideal of $\mathcal{O}_{F\cap L}$ lying over q. On the one hand, the prime q is totally ramified in $F \cap L$; it is a subfield of L and q is totally ramified in L. This means that $e(\mathfrak{Q}'\,|q) = [F \cap L : \mathbb{Q}]$. On the other hand, the prime q is unramified in $F \cap L$ because it is a subfield of the inertia field F. This means that $e(\mathfrak{Q}'\,|q) = 1$. Thus we have $[F \cap L : \mathbb{Q}] = 1$ and hence $F \cap L = \mathbb{Q}$. ■

<u>*Claim 3:*</u> We have $KL = FL$.

Proof of Claim 3: We have $FL \subseteq KL$, because $F, L \subseteq KL$. From Claim 1, we can conclude that $[KL : F] = p^r = [L : \mathbb{Q}]$. Using this in addition to Claim 2 and Proposition 1.31, we get

$$[FL : \mathbb{Q}] = \frac{[L : \mathbb{Q}] \cdot [F : \mathbb{Q}]}{[F \cap L : \mathbb{Q}]} = [L : \mathbb{Q}] \cdot [F : \mathbb{Q}] = [KL : F] \cdot [F : \mathbb{Q}] = [KL : \mathbb{Q}].$$

Thus, it follows that $FL = KL$. ■

<u>*Claim 4:*</u> The prime q is unramified in F and there are no primes that are ramified in F and unramified in K.

Proof of Claim 4: Since F is the inertia field in KL, it follows directly from Corollary 1.26 that q is unramified in F. Now suppose that $\lambda \neq q$ is a prime that is ramified in F and unramified in

K. On the one hand, the prime λ is unramified in L, because q is the only ramified prime in L by Proposition 3.14. Since λ is unramified in K and L, it must be unramified in the compositum KL by Corollary 1.33. On the other hand, the prime λ is ramified in FL since it is ramified in F. This leads to a contradiction, since $KL = FL$ by Claim 3. ■

From Claim 1, we know that F is a cyclic p-power extension; from Claim 4 we know that there are (at most) N primes different from p that ramify in F. Thus by our induction hypothesis F is cyclotomic i.e. $F \subseteq \mathbb{Q}(\zeta_l)$ for some l. Using Claim 3, we get

$$K \subseteq KL = FL \subseteq \mathbb{Q}(\zeta_l)\,\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{\mathrm{lcm}(l,p)}),$$

where the last equality follows from Proposition 3.9. Hence K is cyclotomic and this proves that the proposition holds for $N + 1$.

□

5.4 Proof for any abelian extension

Theorem 5.11. *If $K|\,\mathbb{Q}$ is a finite abelian extension, then K is cyclotomic.*

Proof. Let $K|\,\mathbb{Q}$ be a finite abelian extension, which means that G_K is a finite abelian group. By the fundamental theorem of finite abelian groups, we can write G as a direct product of cyclic groups of prime power order:

$$G_K = G_1 \times \cdots \times G_l,$$

where each subgroup G_i is isomorphic to $\mathbb{Z}/p_i^{m_i}\mathbb{Z}$, for some prime p_i. Let K_i be the field fixed by the subgroup $H_i := \prod_{j \neq i} G_j$. We see that K is exactly the compositum of the K_i's. Since G_K is abelian, each subgroup H_i is normal in G_K, so each extension $K_i|\,\mathbb{Q}$ is a Galois extension of degree $p_i^{m_i}$. According to Proposition 5.10, these extensions are cyclotomic, i.e. $K_i \subset \mathbb{Q}(\zeta_{n_i})$ for some integer n_i. Hence, we have

$$K = K_1 \cdots K_l \subset \mathbb{Q}(\zeta_{n_1}) \cdots \mathbb{Q}(\zeta_{n_l}) = \mathbb{Q}(\zeta_{\mathrm{lcm}(n_1,\ldots,n_l)}),$$

where the last equality follows from Proposition 3.9. This concludes the proof of the Kronecker-Weber Theorem. □

A Fundamental Theorem of Galois Theory

Theorem A.1 (Fundamental Theorem of Galois Theory)**.** *Let $L|K$ be a Galois extension and $G \coloneqq \mathrm{Gal}(L|K)$. There is a bijective correspondence between subgroups H of G and subfields F of L containing K. This correspondence associates to a subgroup H the fixed field $F \coloneqq L^H$, and to a subfield F of K the subgroup $\mathrm{Gal}(L|F)$. Furthermore, we have*

1. *the bijection is inclusion reversing, i.e. if F_1 and F_2 correspond to subgroups H_1 and H_2 then $F_1 \subset F_2$ if and only if $H_2 \leq H_1$,*
2. *if F corresponds to H, then $[L : F] = |H|$ and $[F : K] = (G : H)$,*
3. *if F corresponds to H, then F is Galois over K if and only if H is a normal subgroup of G. In this case, we have $\mathrm{Gal}(F|K) = G/H$.*

Proof. See for example [Art11, Section. 16.7]. □

References

[AM69] M.F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[Art11] Michael Artin. *Algebra*. 2nd ed. Pearson Education, 2011.

[DSD03] Richard M.Foote David S. Dummit. *Abstract Algebra*. 3rd ed. Wiley, 2003.

[Gre74] M. J. Greenberg. "An elementary Proof of the Kronecker-Weber Theorem". In: *The American Mathematical Monthly* 81.6 (1974), pp. 601–607.

[Mol11] Richard A. Mollin. *Algebraic number theory*. 2nd ed. CRC Press, 2011.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. 1st ed. Springer, 1999.

[Rib01] Paulo Ribenboim. *Classical theory of algebraic numbers*. 2nd ed. Springer, 2001.

[Sch07] Alexander Schmidt. *Einführung in die algebraische Zahlentheorie*. 1st ed. Springer, 2007.