Algebraic Number Theory and the Kronecker-Weber Theorem

Zachary Baugher

April 21, 2021

Submitted to the
Department of Mathematics
of the University of Virginia
in partial fulfillment of the requirements
for the degree of
Bachelor of Arts with Distinction

Faculty Advisor: Professor Andrei Rapinchuk

Abstract

The goal of this work is to prove the Kronecker-Weber theorem, an important first step to classifying abelian extensions of number fields. In chapter 1, we review the crucial concepts of Dedekind rings and ramification. Chapter 2 proceeds to study cyclotomic fields, ultimately developing the tools of ramification groups and the different. In chapter 3 we prove the main theorem, including two different proofs for the key statement to which we reduce the theorem for odd primes. We conclude with a brief look at the next steps, namely class field theory and Kronecker's *Jugendtraum*.

Acknowledgements

I would like to thank my advisor, professor Andrei Rapinchuk, for his invaluable mentorship during a difficult year. I would also like to thank my parents and friends for their constant love and support.

The template for this thesis is not mine, but instead comes from Amherst College. Information and files can be found here.

Contents

0 Introduction **1**
- 0.1 A Brief Roadmap . . . 1
- 0.2 Assumed Knowledge . . . 2
- 0.3 Notations and Conventions . . . 2

1 Necessary Algebraic Number Theory **4**
- 1.1 Dedekind Rings . . . 4
  - 1.1.1 Some Lemmas on Ideals in Commutative Rings . . . 4
  - 1.1.2 The Group of Fractional Ideals of a Dedekind Ring . . . 5
- 1.2 Ramification . . . 9
  - 1.2.1 Lifting Prime Ideals in Extensions . . . 9
  - 1.2.2 Ramification and the Discriminant . . . 11

2 Facts on Cyclotomic Fields **15**
- 2.1 Galois Theory of Cyclotomic Fields . . . 15
- 2.2 Extended Example: The Ring of Integers of Cyclotomic Fields . . . 17
- 2.3 Higher Ramification Groups and Cyclotomic Fields . . . 20
- 2.4 The Different Ideal and Cyclotomic Fields . . . 25

3 Two Proofs of the Kronecker-Weber Theorem **35**
- 3.1 Introduction . . . 35
- 3.2 Extensions of Degree p^r Ramified Only at p . . . 36
- 3.3 The Special Case for $p = 2$ . . . 37
- 3.4 The Special Case for p Odd, by Kummer Theory . . . 39
- 3.5 The Special Case for p Odd, Using the Different . . . 42

4 Kronecker-Weber in Context **46**

Bibliography **47**

Chapter 0

Introduction

The Kronecker-Weber theorem is the first major result of *class field theory*, which studies the structure of extensions of global fields which have abelian Galois group. Its statement is as follows:

Theorem 0.0.1 (Kronecker-Weber-Hilbert)**.** *Let $K/\mathbb{Q}$ be an extension such that $[K:\mathbb{Q}]$ is finite and $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. Then there is some positive integer m such that $K \subset \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive mth root of unity.*

The strength of this theorem lies in the concreteness of the result compared to the generality of the hypotheses. It is not at all clear on the surface how such abstract data as the degree of an extension, or the simple fact that its Galois group is abelian, should be able to tell us anything about the actual content of the field extension. The earlier development of Kummer theory marked progress in a similar direction, but even those results require extra assumptions on the exponent of the Galois group and on the content of the base field. Nevertheless, from so little information we can deduce that cyclotomic fields, those of the form $\mathbb{Q}(\zeta)$ for ζ a root of unity, capture all the information necessary to study abelian extensions of $\mathbb{Q}$.

The existence of such a strong structure theorem on extensions of $\mathbb{Q}$ relies in a crucial way on facts which do not generalize to arbitrary number fields (finite extensions of $\mathbb{Q}$). In particular, the Hermite-Minkowski theorem shows that every finite extension of $\mathbb{Q}$ has at least one ramified prime (we will see what this means, and why we care, later). In the larger context of abelian extensions of arbitrary number fields, we only know explicit generators for abelian extensions (analogous to roots of unity) for imaginary quadratic fields (and their generalizations), demonstrating the difficulty of constructively describing abelian extensions in general.

0.1 A Brief Roadmap

The proof of Kronecker-Weber we give here makes heavy use of classical algebraic number theory; as such, we devote the first chapter to developing topics within the subject. We begin by studying integral extensions and Dedekind rings, which provide a structure theory applicable to the rings of integers of number fields we will use. Ultimately, we are building

up to the theory of ramification, the phenomenon that describes how prime ideals in such rings lift in extensions, and which will allow us to prove the main theorem.

The second chapter focuses on cyclotomic fields. We will show that they are themselves abelian extensions of $\mathbb{Q}$, and we will analyze the structure of their Galois groups. From this work, we will follow Gauss in showing any quadratic field sits inside a cyclotomic field, and we will also give an application to the inverse Galois problem, which asks which groups are realizable as Galois groups over $\mathbb{Q}$. Then we get into the meat of the material. In calculating the ring of integers for cyclotomic fields we will also be able to glean its ramification behavior, after which we develop the theories of ramification groups and the different ideal to analyze this behavior and apply it to prove Kronecker-Weber.

In the third chapter, we tie everything together to prove the Kronecker-Weber theorem. The structure of the proof is essentially a series of reductions combined with applications of the theory developed at the end of chapter 2. Namely, we can reduce the problem to the case where the Galois group in question is cyclic of order p^r, where p is a prime and r a positive integer. We can reduce further to allow ourselves the assumption that the only ramified prime is p itself. Following this step, we must separate the cases of $p = 2$ and p odd; the former will be elementary while the latter will involve some theory. In any case, the key question to answer is the following: for a given prime p, what are the extensions $K/\mathbb{Q}$ such that $[K : \mathbb{Q}] = p$ and p is the only prime ramified in K?

When p is odd, it turns out that the only such extension is given by the degree-p subfield of $\mathbb{Q}(\zeta_{p^2})$, where ζ_{p^2} is a primitive p^2-root of unity. We will prove this fact in two ways, first using a direct argument via Kummer theory, and second by applying facts about the different ideal. We will then have proved the main theorem. After we have done this, we will turn to briefly consider the next steps, focusing on the analogous statement to Kronecker-Weber for the imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$.

0.2 Assumed Knowledge

We take for granted topics covered in a first-year graduate algebra course, such as the notions of ring and (prime, maximal) ideal and related constructions and theorems, and Galois theory. In the interest of space we assume also some more specialized knowledge, in particular that of the norm, trace, and discriminant constructed both via the regular representation and using Galois conjugates, integral extensions of rings, and the behavior of the norm, trace, and discriminant in integral extensions of rings. The interested reader who would like to refresh or to learn these concepts may do so in chapter 2 of Samuel's book [7].

0.3 Notations and Conventions

If K is a number field, we will denote by $\mathcal{O}_K$ its ring of integers. We will write ζ_n for a primitive nth root of unity for some positive integer n, and if $n = p^r$, we understand p to be a prime and r a positive integer. We generally denote rings by capital letters early in the alphabet, e.g. A, B, general ideals of rings using fraktur font, e.g. $\mathfrak{a}, \mathfrak{b}$, and prime ideals using $\mathfrak{p}$ or $\mathfrak{q}$. When we speak of primes lying over others in extension rings $A \subset B$, often we will denote the relationship using a change in case: e.g. we will have $\mathfrak{p} \subset A$ and $\mathfrak{P} \subset B$.

The one notable counterexample to this is in the case of rings of integers, where $\mathbb{Q}$ is the base field. We will usually denote the rational prime simply by p, the first prime above p by $\mathfrak{p}$, and subsequently a prime above $\mathfrak{p}$ by $\mathfrak{P}$.

A setup we will use several times is the following. Let A be a Dedekind domain, let K be its field of fractions, let L/K be a finite separable extension, and let B be the integral closure of A in L. We will denote prime ideals of in this setup using fraktur font (e.g. $\mathfrak{p}, \mathfrak{q}$), using capitals to signify primes of B which lie above a given prime in A. That is, if $\mathfrak{p} \subset A$ is a prime ideal, then $\mathfrak{P} \subset B$ will be a prime ideal such that $\mathfrak{P} \cap A = \mathfrak{p}$.

Due to length concerns, and so that we do not stray too far from our main goal, it will not be possible to prove every statement needed in our argument. Where a proof has been omitted, in its place will be a reference to one or more texts in which one may find a proof; for only two lemmas, we instead mention a result from which the lemmas follow.

Chapter 1

Necessary Algebraic Number Theory

The goal of this chapter is to develop quickly two key concepts for the proof of Kronecker-Weber: Dedekind rings and the ideal factorization, and ramification. In the interest of space, we will state most facts in this chapter with a reference rather than with proof, though we will prove some of the more important theorems. The material we cover here is presented in more depth in chapters 3 and 5 in Samuel's book [7]; some proofs are referenced also from Lang's *Algebra* [4].

1.1 Dedekind Rings

The first algebraic tool we construct is the Dedekind ring, which allows us to perform arithmetic using unique factorization of ideals in some cases where unique factorization of elements fails. The theory of Dedekind rings is crucial to answering questions about algebraic number fields, since since their rings of integers are always Dedekind domains. Our goal in this section will be to define fractional ideals and Dedekind rings and to prove the unique factorization theorem for ideals. To start, we recall some facts on ideal containment in Noetherian rings.

1.1.1 Some Lemmas on Ideals in Commutative Rings

In what follows, we suppose A to be a commutative ring with 1. If $\mathfrak{a}, \mathfrak{b}$ are ideals of A, recall that the **product ideal** $\mathfrak{ab}$ is the ideal generated as a group by products of the form xy, where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. Since A is commutative, it is clear that $\mathfrak{ab} = \mathfrak{ba}$, so ideal multiplication is commutative as well. Furthermore, it is quick to see from the definition of an ideal that $A\mathfrak{a} = \mathfrak{a}A = \mathfrak{a}$, so A serves as the identity with respect to this multiplication.

The connection to factorization into prime ideals starts off with an analogue to Euclid's lemma in number theory.

Proposition 1.1.1. *Suppose $\mathfrak{p}$ is a prime ideal of A and $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ any ideals of A. If $\mathfrak{p} \supseteq \mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_k$ then there is some $1 \leq j \leq k$ such that $\mathfrak{p} \supseteq \mathfrak{a}_j$.*

Proof. See section 3.3, lemma 2 in [7]. □

At this point we must begin to impose additional conditions on our ring A. The first of these is that A is Noetherian. Given this extra constraint we can make an improvement on the result above:

Proposition 1.1.2. *If A is a Noetherian ring then any ideal $\mathfrak{a}$ of A contains a product $\mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_k$ of prime ideals of A. If A is additionally an integral domain, then any nonzero ideal of A contains a product of nonzero prime ideals.*

Proof. See section 3.3, lemma 3 in [7]. □

To continue building to unique factorization of ideals, we introduce the notion of fractional ideal. Using fractional ideals creates a natural bridge between working with ideals and integrality properties, which will motivate the definition of Dedekind ring we will give below.

1.1.2 The Group of Fractional Ideals of a Dedekind Ring

Fractional ideals generalize ideals in the following sense: suppose A is an integral domain with field of fractions K. Then simply lifting an ideal of A to all of K does not produce an interesting effect: the result must be zero or all of K. But if we instead think of the ideals of A as A-submodules or A and of K, we can get more varied effects, leading to the following definition:

Definition 1.1.3. With the setup above, an A-submodule $\mathfrak{a}$ of K is called a **fractional ideal** of A if there is some nonzero element $d \in A$ such that $d\mathfrak{a} \subseteq A$.

One can think of d here as a "common denominator" for elements of $\mathfrak{a}$.

Example 1.1.4. Any ideal of A itself is also a fractional ideal: any value of d works as a common denominator (but it is simplest to take $d = 1$). When viewed in the context of fractional ideals, we call the ideals of A **integral ideals**.

Example 1.1.5. If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals of A, then the A-module sum $\mathfrak{a} + \mathfrak{b}$ is a fractional ideal of A as well. Indeed, if $d_1\mathfrak{a} \subseteq A$ and $d_2\mathfrak{b} \subseteq A$, then a quick calculation shows that $d_1d_2(\mathfrak{a} + \mathfrak{b}) \subseteq A$.

Example 1.1.6. Given $\mathfrak{a}$ and $\mathfrak{b}$ as above, we can define the **product** $\mathfrak{ab}$ of fractional ideals to be the A-submodule of $\mathbb{Q}$ generated by products xy, where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. If d_1, d_2 are as above, we have $d_1d_2(\mathfrak{ab}) \subseteq A$, so $\mathfrak{ab}$ is again a fractional ideal. Commutativity of A means that this ideal multiplication is commutative, and it is clear that $A\mathfrak{a} = \mathfrak{a}$ for any fractional ideal $\mathfrak{a}$ of A. This multiplicative structure makes the set of fractional ideals of A into a monoid; our goal is to see when this monoid becomes a group.

We are now ready to define Dedekind rings and begin exploring their arithmetic.

Definition 1.1.7. A **Dedekind ring** is an integrally closed Noetherian domain in which every nonzero prime ideal is a maximal ideal.

Example 1.1.8. The integers $\mathbb{Z}$, or more generally any PID, form a Dedekind ring. Indeed, a PID is Noetherian, and we have shown that UFDs, hence PIDs, are integrally closed. Prime ideals are generated by irreducible elements in a PID, and these must be maximal since any non-associated divisor of a prime must be a unit.

It is important to note here that, although PIDs are Dedekind rings, not all Dedekind rings will be PIDs or even UFDs. The point is that we will be able to recover unique factorization of ideals into prime ideals, even when unique factorization fails at the level of elements. This property will be important when we consider the arithmetic of rings of integers in number fields, which will always be Dedeking rings.

Proposition 1.1.9. *Let A be a Dedekind ring with $K = frac(A)$, and suppose char $K = 0$. Suppose L/K is a finite field extension, and let B be the closure of A in L. Then B is itself a Dedekind domain, and is a finitely-generated A-module.*

Corollary 1.1.10. *The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain.*

Proof. See section 3.4, theorem 1 in [7]. □

Before proving the main theorem, we give the following intermediate fact.

Proposition 1.1.11. *Let A be a Dedekind ring which is not a field, and let K be the field of fractions of A. Let $\mathfrak{m}$ be a maximal ideal of A. Then there is a fractional ideal $\mathfrak{m}' \subset A$ such that the ideal product $\mathfrak{m}\mathfrak{m}' = A$.*

Proof. We proceed in three steps. First, we construct a candidate for $\mathfrak{m}'$, and reduce the problem to showing $\mathfrak{m}\mathfrak{m}' \neq \mathfrak{m}$. Next, we again reduce the problem to showing $\mathfrak{m}' \neq A$. Finally, we actually show that $\mathfrak{m}' \neq A$. We start at the beginning.

The candidate $\mathfrak{m}'$ we will choose is

$$\mathfrak{m}' = \{x \in K : x\mathfrak{m} \in A\}.$$

To see that $\mathfrak{m}'$ is really a fractional ideal of A, note that any element of $\mathfrak{m}$ serves as a "common denominator" which sends $\mathfrak{m}'$ back into A. This observation shows that $\mathfrak{m}\mathfrak{m}' \subset A$, and by definition we see that $A \subset \mathfrak{m}'$, so $\mathfrak{m} \subset \mathfrak{m}\mathfrak{m}' \subset A$. But $\mathfrak{m}\mathfrak{m}'$ is an ideal of A, so maximality of $\mathfrak{m}$ implies $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$ or $\mathfrak{m}\mathfrak{m}' = A$.

Our goal now is to show $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$ is impossible. Suppose otherwise. Then for all $x \in \mathfrak{m}'$ we have $x\mathfrak{m} \subset \mathfrak{m}$ and, inductively, we have $x^n\mathfrak{m} \subset \mathfrak{m}$ for all n. In particular, any nonzero $d \in \mathfrak{m}$ serves as a common denominator to bring $A[x]$ back into A, so $A[x]$ is a fractional ideal of A. But $A[x]$ then lives in the fractional ideal $d^{-1}A$ of A, which is isomorphic to A as an A-module via multiplication by d. Since A is Noetherian as a module, we have that $d^{-1}A$ is a Noetherian module as well, hence $A[x] \subset d^{-1}A$ is finitely generated as an A-module. This means precisely that x is integral over A. But A is a Dedekind ring, hence integrally closed, so in fact $x \in A$. However, x was an arbitrary element of $\mathfrak{m}'$. So $\mathfrak{m}' \subset A$, and we showed earlier that $A \subset \mathfrak{m}'$, so in fact $\mathfrak{m}' = A$.

We conclude by showing $\mathfrak{m}' = A$ is impossible. Take a nonzero element $a \in \mathfrak{m}$ and consider the ideal $(a) \subset A$. By proposition 1.1.2 above and the fact that A is Noetherian, we have that (a) contains a product of nonzero prime ideals $\mathfrak{p}_1 \dots \mathfrak{p}_n$ where n is minimal. By proposition 1.1.1, there is some $\mathfrak{p}_i$, say $\mathfrak{p}_1$, such that $\mathfrak{m} \supset (a) \supset \mathfrak{p}_1$. Since A is Dedekind, the nonzero prime $\mathfrak{p}_1$ is maximal, so we must have $\mathfrak{m} = \mathfrak{p}_1$. Now write $\mathfrak{q} = \mathfrak{p}_2 \dots \mathfrak{p}_n$. We know that $(a) \supset \mathfrak{m} \dots \mathfrak{q}$, but $(a) \supset \mathfrak{q}$ by minimality of the number of factors n. Therefore,

we can find an element $b \in \mathfrak{q} \setminus (a)$. But then we have

$$\begin{aligned} & \mathfrak{m}b \subset (a) \\ \implies & \mathfrak{m}(b/a) \subset A \quad (\text{in } K) \\ \implies & b/a \in \mathfrak{m}', \end{aligned}$$

by the definition of $\mathfrak{m}'$. But we cannot have $b/a \in A$, as otherwise we get $b \in (a)$ which contradicts our definition of b. Since $b/a \in \mathfrak{m}'$ and $b/a \notin A$, we must have $\mathfrak{m}' \not\subset A$, which is what we set out to show. Backtracking, we find that $\mathfrak{m}\mathfrak{m}' = A$, so $\mathfrak{m}$ has an inverse fractional ideal, hence the result. □

We are now ready to prove the main theorem.

Theorem 1.1.12. *Let A be a Dedekind ring, and let P be the set of nonzero prime ideals in A. Then the following are true.*

1. *Any nonzero fractional ideal $\mathfrak{a} \subset A$ has a uniquely determined factorization*

$$\mathfrak{a} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

   where all $v_p(\mathfrak{a})$ are integers and all but finitely many of the $v_p(\mathfrak{a})$ are zero.

2. *The nonzero fractional ideals of A form a group under ideal multiplication.*

Proof. We begin with part (1) of the theorem, starting by reducing to the case where $\mathfrak{a}$ is an integral ideal. Indeed, if $\mathfrak{a}$ is a general fractional ideal then there is some nonzero $d \in A$ such that $d\mathfrak{a} \subset A$. Then $d\mathfrak{a}$ will be an integral ideal of A, with $\mathfrak{a} = (d\mathfrak{a})(dA)^{-1}$. If we construct a prime ideal factorization for dA then it will be easy to compute the factorization $(dA)^{-1}$ in the usual reverse-and-invert manner. So we may assume $\mathfrak{a}$ is already integral.

We use a common trick for working with Noetherian rings. Let $\mathcal{C}$ be the collection of (integral) ideals of A which do *not* factor as a product of prime ideals, and assume for the sake of contradiction that $\mathcal{C}$ is nonempty. The fact that A is Noetherian means any collection of ideals of A, including $\mathcal{C}$, has a maximal element under conclusion; let $\mathfrak{a} \in \mathcal{C}$ be such an element. Then $\mathfrak{a} \neq A$, since A can be written as a product of prime ideals with all exponents equal to zero. Since $\mathfrak{a}$ is now a proper ideal of A, it lives inside some maximal ideal $\mathfrak{m} \subset A$. By proposition 1.1.11, the ideal $\mathfrak{m}$ has an inverse fractional ideal $\mathfrak{m}'$. Let us consider the product $\mathfrak{a}\mathfrak{m}'$. One the one hand, we have that $\mathfrak{a}\mathfrak{m}' \subset A$, from the definition of $\mathfrak{m}'$ and the fact that $\mathfrak{a} \subset \mathfrak{m}$. On the other hand, from the proof of proposition 1.1.11, we know $A \subset \mathfrak{m}'$, so that $\mathfrak{a} \subset \mathfrak{a}\mathfrak{m}'$. Mirroring the integrality argument from the proof of proposition 1.1.11, we find that this inclusion is in fact proper. Since $\mathfrak{a}$ is maximal in $\mathcal{C}$, this means $\mathfrak{a}\mathfrak{m}' \notin \mathcal{C}$, so that $\mathfrak{a}\mathfrak{m}'$ has a prime ideal factorization

$$\mathfrak{a}\mathfrak{m}' = \mathfrak{p}_1 \dots \mathfrak{p}_n.$$

Multiplying on both sides by $\mathfrak{m}$ gives $\mathfrak{a} = \mathfrak{m}\mathfrak{p}_1 \dots \mathfrak{p}_n$, which is a prime ideal factorization for $\mathfrak{a}$. This contradicts the fact that $\mathfrak{a} \in \mathcal{C}$, so in fact $\mathcal{C}$ must be empty, and we have proved the existence portion of claim (1).

To show uniqueness, suppose an ideal $\mathfrak{a}$ has two prime factorizations $\prod_{i=1}^{r} \mathfrak{p}_i^{n_{\mathfrak{p}_i}(\mathfrak{a})}$ and $\prod_{j=1}^{s} \mathfrak{q}_j^{n_{\mathfrak{q}_j}(\mathfrak{a})}$. Equate these factorizations. If they differ at all, then we can multiply on either side and relabel to get an equation of the form

$$\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} = \mathfrak{q}_1^{f_1} \dots \mathfrak{q}_s^{f_s},$$

with no $\mathfrak{p}_i$'s equal to a $\mathfrak{q}_j$ and all exponents positive. Now $\mathfrak{p}_1$ contains both sides of the equation, hence contains some $\mathfrak{q}_j$ using proposition 4.1. Without loss of generality, say $\mathfrak{p}_1 \supset \mathfrak{q}_1$. Since A is a Dedekind ring, we have that $\mathfrak{q}_1$ is maximal, so in fact $\mathfrak{p}_1 = \mathfrak{q}_1$, which contradicts our assumption that the ideals on each side were distinct. We have now shown uniqueness of the prime ideal factorization, finishing the proof of claim (1).

Claim (2) now follows very quickly; to complete the group structure on fractional ideals we need only construct inverses, and once one has the prime factorization for a given ideal they need only negate all exponents to get said inverse. □

Example 1.1.13. It is known that a Dedekind domain is a PID if and only if it is a UFD. If A is as such, then an ideal (r) factors according to the prime factorization of the element r. To see a more explicit example of this, take $A = \mathbb{Z}[i]$, the Gaussian integers. We will see that A is the ring of integers of $\mathbb{Q}[i]$, hence a Dedekind ring, and it is known that A is a Euclidean domain, hence a PID and a UFD. The ideal (2) splits in A as $(2) = (1+i)^2$. On the other hand, the ideal generated by a rational prime $p \equiv 1 \pmod 4$ splits as $(p) = (a+bi)(a-bi)$, where a, b are integers satisfying $a^2 + b^2 = p$. In this case we do not get a repeated ideal factor since $a + bi$ and $a - bi$ are not associated in $\mathbb{Z}[i]$. The splitting of (2) as the square of a prime ideal is an example of ramification, which we will develop soon and which will be crucial to our proof of Kronecker-Weber.

We conclude by recording some properties of the function $v_{\mathfrak{p}}(\mathfrak{a})$ defined above, which counts the exponent of $\mathfrak{p}$ appearing in the prime ideal factorization of $\mathfrak{a}$.

Proposition 1.1.14. *Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of a Dedekind ring A, and for a given prime ideal $\mathfrak{p} \subset A$ denote by $v_{\mathfrak{p}}(\mathfrak{a})$ the exponent of $\mathfrak{p}$ appearing in the ideal factorization of $\mathfrak{a}$. Then following are true.*

1. $v_{\mathfrak{p}}(\mathfrak{ab}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$;
2. *$\mathfrak{b}$ is an integral ideal (that is, $\mathfrak{b} \subset A$) if and only if $v_{\mathfrak{p}}(\mathfrak{b}) \geq 0$ for every prime ideal $\mathfrak{p} \subset A$;*
3. *$\mathfrak{a} \subset \mathfrak{b}$ if and only if $v_{\mathfrak{p}}(\mathfrak{a}) \geq v_{\mathfrak{p}}(\mathfrak{b})$ for all prime ideals $\mathfrak{p} \subset A$;*
4. $v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))$;
5. $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \max(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))$.

Proof. See the end of section 3.4 in [7] for brief explanations. □

We will use these properties mostly in sections 2.4 and 3.5, when we discuss the different ideal and its connection to ramification.

1.2 Ramification

We just saw that the unique ideal factorization feature of Dedekind rings allows us to consider the exponent of a prime ideal occurring in the factorization of a fractional ideal. In this section, we develop basic tools for the study of ramification, which is defined using these factorization exponents upon lifting an ideal from one Dedekind ring to another. We will use ramification constantly as we work to prove Kronecker-Weber, including when we develop the more advanced tools of ramification groups and the different ideal later on.

1.2.1 Lifting Prime Ideals in Extensions

We now begin to use the theory we just developed to discuss ramification, the phenomenon of repeated prime factors upon lifting an ideal from one Dedekind ring to another. We will be able to describe in more detail the data of ideal factorization, and later we will develop tools such as ramification groups and the different to analyze this data in enough depth to prove Kronecker-Weber. Our goal for this section is to define ramification and prove a useful formula for the degree of a field extension.

We begin the discussion of lifting primes by defining lying-over (or lying above), which will allow us to determine the ideal factors of a prime lifted to an extension ring.

Definition 1.2.1. Let $A \subset B$ be an extension of rings, and suppose $\mathfrak{p}$ and $\mathfrak{P}$ are prime ideals of A and B, respectively. We say $\mathfrak{P}$ **lies above** $\mathfrak{p}$ if $\mathfrak{P} \cap A = \mathfrak{p}$.

Proposition 1.2.2 (Going-up lemma)**.** *Let $A \subset B$ be an integral extension of rings, let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}B \neq B$ and there is a prime ideal $\mathfrak{P}$ of B lying above $\mathfrak{p}$.*

Proof. See section VII.1, proposition 1.10 in [4]. □

The next order of business is to further analyze the splitting of a prime ideal upon lifting it in a field extension. We state these results in generality, though in the case of Kronecker-Weber we will only really care about what happens when the extension in question is Galois. The setup is as follows: here A is a Dedekind ring of characteristic 0, with field of fractions K. We take L/K to be a finite extension of fields, and denote by B the integral closure of A in B.

Let $\mathfrak{p} \subset A$ be a prime ideal, and recall from section 1.1.2 that the integral closure of a Dedekind ring in a finite field extension is again a Dedekind ring. So we have a factorization

$$\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i},$$

where the $\mathfrak{P}_i$ are prime ideals of B. Our first fact is that we know exactly the prime ideals of B that occur in this factorization.

Proposition 1.2.3. *The primes $\mathfrak{P}_i$ appearing with nonzero exponent in the ideal factorization of the lift $\mathfrak{p}B$ of a prime ideal $\mathfrak{p} \subset A$ are precisely those prime ideals of B which lie above $\mathfrak{p}$.*

Proof. See section 5.2, proposition 1 in [7]. □

Consider now the composition

$$A \hookrightarrow B \xrightarrow{\pi} B/\mathfrak{P},$$

where π is the projection and $\mathfrak{P}_i \subset B$ is an ideal lying over the prime ideal $\mathfrak{p} \subset A$. The kernel of this composition is precisely $\mathfrak{P}_i \cap A = \mathfrak{p}$, so applying the first isomorphism theorem gives us an embedding $A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}_i$. Since we are working with Dedekind rings, the prime ideals $\mathfrak{p}$ and $\mathfrak{P}_i$ are maximal, so that $B/\mathfrak{P}_i$ / $A/\mathfrak{p}$ is a field extension. Furthermore, we know that B is a finitely-generated A-module since A is integrally closed. Combining these facts, we see that the extension $B/\mathfrak{P}_i$ / $A/\mathfrak{p}$ has finite degree. We call the component fields of this extension **residue fields** and the degree $[B/\mathfrak{P}_i : A/\mathfrak{p}]$ the **residual degree**, and denote the latter by f_i. Note that it is important to consider each prime $\mathfrak{P}_i$ lying above $\mathfrak{p}$ separately, as in general different primes lying above $\mathfrak{p}$ need not have isomorphic residue fields. We will see later when we return to the topic of ramification that in the Galois case the choice of prime lying above does not matter, but for now we continue considering the more general case.

The formal definition of ramification is as follows:

Definition 1.2.4. In the setup we have been discussing, consider the factorization

$$\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

arising from a prime ideal $\mathfrak{p} \subset A$. We say $\mathfrak{p}$ **ramifies** in B (or in L) if any of the exponents e_i are at least 2. The e_i are referred to as **ramification indices**.

Finally, we consider how $\mathfrak{p}B$ interacts with the field $A/\mathfrak{p}$. Since each prime factor of $\mathfrak{p}B$ lies over $\mathfrak{p}$, we have $\mathfrak{p}B \cap A = \mathfrak{p}$. So we get an inclusion $A/\mathfrak{p} \hookrightarrow B/\mathfrak{p}B$ which makes $B/\mathfrak{p}B$ a finite-dimensional vector space over $A/\mathfrak{p}$. The degree of this vector space allows us to connect the residual degrees and ramification indices of primes lying over $\mathfrak{p}$ to the degree of the ambient field extension L/K, per the following theorem.

Theorem 1.2.5. *In the setup we have been discussing,*

$$\sum_{i=1}^{r} e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K].$$

Proof. We first prove the equality on the left. Consider, for each $\mathfrak{P}_i$, the sequence of quotient modules

$$B/\mathfrak{P}_i^{e_i} \supset \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supset \cdots \supset \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supset \{0\}.$$

By the isomorphism theorems for modules, the quotient of two successive members of this chain is of the form $\mathfrak{P}_i^e/\mathfrak{P}_i^{e+1}$ for some $0 \leq e < e_i$. Each such quotient must be nontrivial, as otherwise the power of $\mathfrak{P}_i$ in the factorization of $\mathfrak{p}B$ would not be unique, a contradiction. Hence, for a fixed value of e we can take $x \in \mathfrak{P}_i^e \setminus \mathfrak{P}_i^{e+1}$.

Now, consider the $A/\mathfrak{p}$-linear map $\varphi : B/\mathfrak{P}_i \to \mathfrak{P}_i^e/\mathfrak{P}_i^{e+1}$ given by $\alpha \mapsto x\alpha$. We will prove that φ is an $A/\mathfrak{p}$-vector space isomorphism. Since both spaces are finite-dimensional, we need only show φ is injective. It follows from the choice of x that φ is not the zero

map, since $1 \in B/\mathfrak{P}_i$ gets sent to $x \neq 0 \in \mathfrak{P}_i^e/\mathfrak{P}_i^{e+1}$. But since $\mathfrak{P}_\mathfrak{i}$ is a maximal ideal of B, the quotient $B/\mathfrak{P}_i$ contains only zero and full ideals. Therefore φ is injective, hence an isomorphism, as desired. Decomposing $B/\mathfrak{P}_i^{e_i}$ as a direct sum of quotient spaces and counting dimensions then gives

$$[B/\mathfrak{P}_i^{e_i} : A/\mathfrak{p}] = e_i f_i.$$

But the ideals $\mathfrak{P}_i^{e_i}$ are comaximal, so we can apply the Chinese Remainder Theorem and sum over all indices i to get

$$\sum_i e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}],$$

proving the first equality. It remains to show $[B/\mathfrak{p}B : A\mathfrak{p}] = [L : K]$.

We show this second equality first in the case where A is a PID, then reduce the general case to this case via localization. When A is a PID, we have via the theory of integral ring extensions that B is a free A-module of rank $[L : K]$. We can reduce a free A-module basis for B to a $A/\mathfrak{p}$-module basis for $B/\mathfrak{p}B$, proving the desired equality.

Now remove the assumption that A is a PID. Set $S = A \setminus \mathfrak{p}$ and consider the rings of fractions $S^{-1}A$ and $S^{-1}B$. We know $S^{-1}A$ is a local ring, and in particular is a PID with unique maximal ideal $\mathfrak{p}S^{-1}A$. We also know the integral closure of $S^{-1}A$ in L is $S^{-1}B$. Applying the PID case of the result we would like to prove, we see that

$$[S^{-1}B/\mathfrak{p}S^{-1}B : S^{-1}A/\mathfrak{p}S^{-1}A] = [L : K].$$

Next we factor $\mathfrak{p}S^{-1}B$ as a product of primes. We have

$$\mathfrak{p}S^{-1}B = \prod_{i=1}^{r} (S^{-1}B\mathfrak{P}_i)^{e_i}.$$

Since for each $\mathfrak{P}_i$ we have $\mathfrak{P}_i \cap A = \mathfrak{p}$, by definition we have $\mathfrak{P}_i \cap S = \emptyset$, so that $S^{-1}B\mathfrak{P}_i$ is a prime ideal of $S^{-1}B$ (using the characterization of primes in the localization at $\mathfrak{p}$). Applying the formula for $[B/\mathfrak{p}B : A/\mathfrak{p}]$ we have already proved, we find that

$$[S^{-1}B/\mathfrak{p}S^{-1}B : S^{-1}A/\mathfrak{p}S^{-1}A] = \sum_{i=1}^{r} e_i [S^{-1}B/\mathfrak{P}_i S^{-1}B : S^{-1}A/\mathfrak{p}S^{-1}A].$$

But it is known that $S^{-1}A/\mathfrak{p}S^{-1}A \simeq A/\mathfrak{p}$ and $S^{-1}B/\mathfrak{P}_i S^{-1}B \simeq B/\mathfrak{P}_i$, so the degrees on the right-hand side of the preceding equation are equal to f_i, proving the desired result in the general case. □

1.2.2 Ramification and the Discriminant

The goal of this section is to prove a useful criterion for ramification; namely, a prime ramifies in an extension if and only if it divides the discriminant. This makes sense both on the level of elements and of ideals, and we will discuss both senses of the relevant theorem.

In this section we will keep the setup of the previous section. We will phrase our results in terms of the **discriminant ideal**, which when B is a free A-module is defined to be the principal ideal $\mathscr{D}_{B/A}$ of A generated by the discriminant of any A-module base for B. Since

$\mathbb{Z}$ is a PID, this situation includes the case where $A = \mathbb{Z}$ and $B = \mathcal{O}_L$, the ring of integers for a number field L, which is the setting for the Kronecker-Weber theorem.

We begin to understand the connection between the discriminant and ramification via the following product rule:

Lemma 1.2.6. *Let A be a ring, and let $B_1, \ldots, B_q$ be rings containing A which are finitely-generated free A-modules, and let $B = B_1 \times \cdots \times B_q$. Then*

$$\mathscr{D}_{B/A} = \prod_i \mathscr{D}_{B_i/A}.$$

Proof. See section 5.3, lemma 1 in [7]. □

This result tells us that the discriminant commutes with products. Next, we show that it commutes with quotients. These results will combine to allow us to use the Chinese Remainder Theorem to study discriminants, providing the key piece in the link between the discriminant and ramification.

Lemma 1.2.7. *Let $A \subset B$ be an extension of rings, with B a finitely-generated free A-module. If $\{e_1 \ldots, e_n\}$ is a basis for B/A, then the reduction $\{\bar{e}_1, \ldots, \bar{e}_n\}$ modulo an ideal $B\mathfrak{a}$ (where $\mathfrak{a}$ is an ideal of A) is a basis for $B/B\mathfrak{a}$ over $A/\mathfrak{a}$. Furthermore, the discriminant of the reduced basis is equal to the reduction of the discriminant of $\{e_1, \ldots, e_n\}$ modulo $\mathfrak{a}$.*

Proof. See section 5.3, lemma 2 in [7]. □

Now we can use the Chinese Remainder Theorem into play. A contradiction argument shows that all prime powers $\mathfrak{P}_i^{e_i}, \mathfrak{P}_j^{e_j}$ in the factorization of $\mathfrak{p}B$ are comaximal, so we have an isomorphism

$$B/\mathfrak{p}B \simeq B/\mathfrak{P}_i^{e_i} \times \cdots \times B/\mathfrak{P}_r^{e_r}.$$

Using this isomorphism, we can quickly show that $\mathfrak{p}$ ramifies if and only if $B/\mathfrak{p}B$ is reduced; that is, it contains no nonzero nilpotents. Indeed, if $\mathfrak{p}$ is unramified then $B/\mathfrak{p}B$ is a direct product of fields, which cannot have a nonzero nilpotent. If $\mathfrak{p}$ is ramified, then we can take $x \in \mathfrak{P}_i \setminus \mathfrak{P}_i^2$ and construct a nonzero nilpotent element of $B/\mathfrak{p}B$ by taking the image of x under the projection $B \mapsto \mathfrak{p}B$.

The discriminant connects to nilpotents as well, via the following lemma.

Lemma 1.2.8. *Let K be a field which is finite or of characteristic 0, and let L be a finite-dimensional commutative K-algebra. Then $\mathscr{D}_{L/K} \neq (0)$ if and only if L contains no nonzero nilpotent elements.*

Proof. See section 5.3, lemma 3 in [7]. □

Before proving the main theorem on the discriminant and ramification, we extend our definition of the discriminant ideal. Let L/K be an extension of number fields with respective rings of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. We know from the characterization of integral ring extensions that $\mathcal{O}_L$ is contained in a free $\mathcal{O}_K$-module, but since $\mathcal{O}_K$ is not necessarily a PID we cannot guarantee that $\mathcal{O}_L$ is itself a free $\mathcal{O}_K$-module. In this case we define the discriminant ideal $\mathscr{D}_{\mathcal{O}_L/\mathcal{O}_K}$ to be the ideal of $\mathcal{O}_K$ generated by all discriminants of K-bases for L which lie in $\mathcal{O}_L$. Note that this really is an ideal in $\mathcal{O}_K$, since $\mathcal{O}_K$ is integrally closed.

In the case where $\mathcal{O}_K$ is a PID, changing basis allows us to show that any basis for L/K living in B can be converted to a basis for B/A, so the notion of discriminant ideal we have just defined is equivalent in this case to the one we have already been using.

We are now ready to prove the discriminant criterion for ramification in full generality.

Theorem 1.2.9. *Let L/K be an extension of number fields with respective rings of integers B, A. Then a prime ideal $\mathfrak{p} \subset A$ ramifies in L if and only if $\mathfrak{p}$ contains the discriminant ideal $\mathscr{D}_{B/A}$.*

Proof. Lift $\mathfrak{p}$ to $\mathfrak{p}B$, and factor into primes, giving

$$\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}.$$

From our work above, we have an isomorphism of rings

$$B/\mathfrak{p}B \simeq \prod_{i=1}^{r} B/\mathfrak{P}_i^{e_i}.$$

Combining lemma 1.2.8 with the remarks directly proceeding that lemma and this isomorphism, we have

$$\begin{aligned} \mathfrak{p} \text{ ramifies} &\iff B/\mathfrak{p}B \text{ contains nonzero nilpotents} \\ &\iff \mathscr{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0). \end{aligned}$$

We will use these equivalent conditions to recast the problem. Write $S = A \setminus \mathfrak{p}$ and $B' = S^{-1}B$, $A' = S^{-1}A$, and let $\mathfrak{p}' = \mathfrak{p}A'$ be the unique maximal ideal of A'.

Since localization preserves integral closures, and since A' is a PID, we have that B' is a free A'-module. Furthermore we have that $A/\mathfrak{p} \simeq A'/\mathfrak{p}'$, and since $B'/\mathfrak{p}'B'$ is finite and integral over $A'/\mathfrak{p}'$ we have that $\mathfrak{p}'B'$ is maximal in B', so that $B/\mathfrak{p}B \simeq B'/\mathfrak{p}'B'$ also.

Now let $\{e_1, \ldots, e_n\}$ be an A'-basis for B'. By lemma 1.2.7, we get that the reduction $\{\bar{e_1}, \ldots, \bar{e_n}\}$ modulo $\mathfrak{p}'B'$ is an $A'/\mathfrak{p}'$-basis for $B'/\mathfrak{p}'B'$. Applying lemma 1.2.6 gives us that

$$D_{(B'/\mathfrak{p}'B')/(A/\mathfrak{p}')}(\bar{e}_1, \ldots, \bar{e}_n) = \overline{D_{B'/A'}(e_1, \ldots, e_n)}.$$

In particular, we have that $\mathscr{D}_{(B'/\mathfrak{p}'B')/(A/\mathfrak{p}')} = (0)$ if and only if $D_{B'/A'}(e_1, \ldots, e_n) \in \mathfrak{p}'$. Applying the isomorphims $B'/\mathfrak{p}'B' \simeq B/\mathfrak{p}B$ and $A'/\mathfrak{p}' \simeq A/\mathfrak{p}$, we get that $D_{B'/A'}(e_1, \ldots, e_n) \in \mathfrak{p}'$ if and only $\mathscr{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0)$ Finally, tying in the chain of biconditionals above shows that $\mathfrak{p}$ ramifying in L is equivalent to $D_{B'/A'}(e_1, \ldots, e_n)$ being an element of $\mathfrak{p}'$. We show this last condition is equivalent to $\mathfrak{p}$ containing $\mathscr{D}_{B/A}$.

Suppose first that $D_{B'/A'}(e_1, \ldots, e_n) \in \mathfrak{p}'$, and let $\{x_1, \ldots, x_n\}$ be a K-basis for L which lies in B. If we consider B as a subring of B', we can write each of the x_i as a sum of the form $\sum a_{ij}e_j$, where all $a_{ij} \in A'$. Taking discriminants and using the change of base formula shows that $D(x_1, \ldots, x_n) \in \mathfrak{p}'$; but this discriminant is also in A, hence in $\mathfrak{p}$. We conclude that $\mathscr{D}_{B/A} \subset \mathfrak{p}$ in this case.

Going the other way, suppose that $\mathscr{D}_{B/A} \subset \mathfrak{p}$. Since $\{e_1, \ldots, e_n\} \subset B'$, we can write $e_i = y_i s^{-1}$ for appropriate $y_i \in B$ and $s \in S$. Then

$$\begin{aligned} D(e_1, \ldots, e_n) &= s^{-2n} D(y_1, \ldots, y_n) \\ &\in A' \mathscr{D}_{B/A} \\ &\subset A' \mathfrak{p} = \mathfrak{p}', \end{aligned}$$

so $\mathfrak{p}$ ramifies in L, and we are done. □

Corollary 1.2.10. *Only finitely many primes ramify in an extension of number fields.*

Proof. The ideal factorization for $\mathscr{D}_{B/A}$ lists exactly those primes containing $\mathscr{D}_{B/A}$, which by the theorem are precisely the primes which ramify. □

Remark. When $K = \mathbb{Q}$ (so that $A = \mathbb{Z}$), the above theorem shows that the primes which ramify are those which divide the discriminant of L/K in the usual numerical sense. Since we only care about the $K = \mathbb{Q}$ case in what follows, we will usually discuss ramification using this divisibility criterion rather than looking at the discriminant ideal.

We conclude the chapter with two examples.

Example 1.2.11 (Quadratic fields)**.** Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$ with d a square-free integer. If $d \equiv 2, 3 \pmod 4$, then the ring of integers of L is $\mathbb{Z}[\sqrt{d}]$. So $\{1, \sqrt{d}\}$ is an integral basis, with discriminant $4d$ (as one shows by a quick matrix calculation). So the primes that ramify here are 2 and those which divide d.

If $d \equiv 1 \pmod 4$, then the ring of integers is instead $\mathbb{Z}[(1 + \sqrt{d})/2]$, and we instead consider the integral basis $\{1, (1 + \sqrt{d})/2\}$. The discriminant of this basis is d, so in this case the ramified primes are those which divide d.

Example 1.2.12 (Cyclotomic fields)**.** We have that $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ is an integral basis for $\mathbb{Q}(\zeta_p)$, with discriminant a power of p. It follows that p is the only prime ramified in $\mathbb{Q}(\zeta_p)$, and it turns out this fact will be crucial in proving Kronecker-Weber, as we shall soon see.

Chapter 2

Facts on Cyclotomic Fields

In this chapter, we specialize our study to cyclotomic fields, which are obtained by adjoining roots of unity to $\mathbb{Q}$, and to number fields. We handle these topics in a more in-depth way, providing proofs for nearly all statements. We will prove several important structural facts about the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, namely, that it is Galois of degree $\phi(n)$ with abelian Galois group and has ring of integers $\mathbb{Z}[\zeta_n]$. We will also give a more thorough analysis of the structure of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ when n is a prime power and develop machinery to analyze ramification in these fields, namely, the ramification groups and the different ideal. As we go, we will note where certain tools and concepts will appear in the next chapter to aid us in the proof of the Kronecker-Weber theorem.

2.1 Galois Theory of Cyclotomic Fields

The goal of this section is to show the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois and to describe its Galois group. The interested reader can learn more about this this theory in section VI.3 of Lang's book [4], or in section 9.1 of Cox's book [2]. We begin with a discussion of the automorphisms of this extension.

The nth roots of unity form a group μ_n under multiplication. Since any finite multiplicative group contained in a field is cyclic, we have that $\mu_n \cong \mathbb{Z}/m\mathbb{Z}$ for some integer $m \leq n$. In fact m is equal to n; to see this, note that any nth root of unity satisfies the polynomial $x^n - 1$. Since $\mathbb{Q}$ has characteristic zero, this polynomial is separable and has n distinct roots, so $|\mu_n| = n$ and we get $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$.

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ containing $\mathbb{Q}(\zeta_n)$, and let σ be a $\mathbb{Q}$-embedding of $\mathbb{Q}(\zeta_n)$ into $\overline{\mathbb{Q}}$. The embedding is determined entirely by its action on ζ_n; furthermore, order considerations tell us that $\sigma(\zeta_n)$ is another primitive nth root of unity. Hence $\sigma\left(\mathbb{Q}(\zeta_n)\right) = \mathbb{Q}(\zeta_n)$, and $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is normal, hence Galois. Then $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Since $\sigma(\zeta_n)$ is a primitive nth root of unity, we have $\sigma(\zeta_n) = \zeta_n^i$ for some i relatively prime to n. Reducing mod n gives a well-defined value of i such that $1 \leq i < n$. If $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ maps ζ_n to ζ_n^j, where j is prime to n, we get

$$\sigma\tau(\zeta_n) = \zeta_n^{ij},$$

so this correspondence gives an embedding of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ into $(\mathbb{Z}/n\mathbb{Z})^\times$. Over $\mathbb{Q}$, this embedding becomes an isomorphism via the following theorem.

Theorem 2.1.1. *Any primitive nth root of unity is a root of the minimal polynomial over $\mathbb{Q}$ of a fixed primitive root ζ_n.*

We use the following lemmas, which we give here without proof. Both are consequences of Gauss' lemma on irreducibility of polynomials.

Lemma 2.1.2. *If a complex number z satisfies $f(z) = 0$ for some monic polynomial $f(x) \in \mathbb{Z}[x]$, then $\mu_{z,\mathbb{Q}}(x) \in \mathbb{Z}[x]$.*

Lemma 2.1.3. *Suppose $f \in \mathbb{Z}[x]$ is monic and satisfies $f = gh$ for polynomials g, h. If $g \in \mathbb{Z}[x]$ then $h \in \mathbb{Z}[x]$ as well.*

Proof of Theorem 2.1.1. By definition, ζ_n is a root of $x^n - 1$. By lemmas 2.1.2 and 2.1.3, we can then write

$$x^n - 1 = f(x)g(x),$$

where $f, g \in \mathbb{Z}[x]$ and f is the minimal polynomial for ζ_n over $\mathbb{Q}$. Suppose p is a prime not dividing n; we will show that ζ_n^p is a root of f. Assume for the sake of contradiction that $g(\zeta_n^p) = 0$. Then ζ_n is a root of $g(x^p)$. Since $f(x)$ is the minimal polynomial for ζ_n, we must have $f(x)|g(x)$, so there exists $h(x) \in \mathbb{Z}[x]$ with $g(x^p) = f(x)h(x)$. Reducing mod p, and using the fact that the pth power map is a homomorphism in characteristic p, we get

$$\bar{g}(x)^p = \overline{f}(x)\bar{h}(x),$$

where $\overline{f}, \bar{g}, \bar{h}$ are f, g, h with coefficients reduced mod p. In particular, $\bar{g}$ and $\overline{f}$ have a common factor in $\mathbb{F}_p[x]$. But we also have

$$x^n - \bar{1} = \overline{f}(x)\bar{g}(x);$$

since $\overline{f}$ and $\bar{g}$ share a factor, we know $x^n - \bar{1}$ has a repeated root. This is impossible: the formal derivative of $x^n - \bar{1}$ is $\bar{n}x^{n-1}$; since $p \nmid n$, this polynomial is not identically zero, hence it is separable and does not have a repeated root. We conclude by contradiction that ζ_n^p is a root of f.

To finish, note that any primitive nth root of unity is equal to ζ_n^i with i relatively prime to n. We can then write i as a product of primes not dividing n and apply the result we have just proved inductively to show that ζ_n^i is also a root of f. □

Corollary 2.1.4. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a finite Galois extension, the order of the Galois group is equal to the degree of the minimal polynomial of ζ_n. Our embedding shows that the order of the Galois group divides $\phi(n)$, and theorem 2.1 shows that the degree of the minimal polynomial is at least $\phi(n)$. Equality follows, and we conclude the embedding is an isomorphism. □

Corollary 2.1.5. *If m, n are relatively prime integers then $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$.*

Proof. One shows using order arguments that the compositum $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{mn})$. Multiplicativity of the ϕ function shows that $[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}][\mathbb{Q}(\zeta_m) : \mathbb{Q}]$, and the desired result follows. □

Remark. We could also have approached our discussion of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ from the direction of cyclotomic polynomials by constructing the minimal polynomials for ζ_n explicitly. Doing so here would bring us too far afield, but the book [2] of Cox does take this direction, for those interested in reading more.

Now that we know what $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ looks like in general, we analyze the structure of these groups more deeply in the case where n is a prime power. This analysis will be important for our proof of the Kronecker-Weber theorem, because we will reduce the proof to the case of abelian extensions of prime-power order. Knowing the Galois group for the cyclotomic extensions of prime-power order will allow us to choose useful subfields and utilize behavior of certain automorphisms more effectively. In the interest of space, we omit the proof, which largely consists of computation.

Proposition 2.1.6. *Let p be a prime. If $p > 2$, then for any $r \geq 1$ the group $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic of order $\phi(p^r) = p^{r-1}(p-1)$. If $p = 2$, then for any $r \geq 2$, the element $5 \pmod{2^r}$ generates a subgroup U of $(\mathbb{Z}/2^r\mathbb{Z})^\times$ of order 2^{r-2}, and $(\mathbb{Z}/2^r\mathbb{Z})^\times \simeq \{\pm 1\} \times U$.*

Proof. See section 3, lemma 5 in [6]. □

We can quickly derive a corollary which explains the extra $\{\pm 1\}$ in the $p = 2$ case of proposition 2.1.6: it is a factor corresponding to the fixed field of complex conjugation.

Corollary 2.1.7. *If p is an odd prime, then the cyclotomic extension $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$ is cyclic. If $p = 2$ and $r \geq 2$, with L the fixed subfield under complex conjugation inside $\mathbb{Q}(\zeta_{2^r})$, then $L/\mathbb{Q}$ is cyclic of degree 2^{r-2}.*

Proof. The statement for p odd is an immediate consequence of proposition 2.1.6. When $p = 2$, recall that the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}) \to (\mathbb{Z}/2^r\mathbb{Z})^\times$ takes the complex conjugation automorphism σ to -1. Then $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})/\langle\sigma\rangle$, and applying the isomorphism from proposition 2.1.6 shows that this is the same as $(\{\pm 1\} \times U)/\{\pm 1\} = U$, which is cyclic of order 2^{r-2}. □

We conclude with a description of ramification in cyclotomic fields.

Proposition 2.1.8. *If p is a prime and $r \geq 1$ an integer, then p is the only prime ramified in $\mathbb{Q}(\zeta_{p^r})$, and the ramification index of p equals the total degree of the field extension (we say in this case that p is **totally ramified**).*

Proof. We will prove this in the next section, when we show that the ring of integers for $\mathbb{Q}(\zeta_{p^r})$ is $\mathbb{Z}[\zeta_{p^r}]$ (see pp. 18-19). □

2.2 Extended Example: The Ring of Integers of Cyclotomic Fields

In this section we prove that the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$. Along the way, we will prove the very important property that when p is prime, the extension $\mathbb{Q}(\zeta_{p^r})$ is ramified only at p, and is totally ramified (proposition 2.1.9 of the previous section). We cite a few results we need with a reference, but note that we do not use them anywhere else. We also

make some use of the cyclotomic polynomials, which we have not yet seen; in the present case, one only needs to know what we will end up writing down: the expanded integer-coefficient polynomial, and the product form of the polynonomial over primitive roots of unity.

Set $K = \mathbb{Q}(\zeta_n)$ and work with the understanding that any trace, norm, or discriminant is taken for the extension $K/\mathbb{Q}$. We first reduce to the case of n a prime power. Suppose $n = p^r m$ with $p \nmid m$, and suppose also that $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. We use the following two results.

Proposition 2.2.1. *The discriminant of a cyclotomic field $\mathbb{Q}(\zeta_m)$ divides a power of m. In particular, if $p \nmid m$ then the discriminants of $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_m)$ are coprime.*

Proof. See section I.10, proposition 10.2 in [3]. Note that although this fact is proven after calculating the ring of integers for $\mathbb{Q}(\zeta_{p^r})$, the proof fact does not rely on knowing the precise ring of integers, so our work here is not circular. □

Theorem 2.2.2. *If K, L are number fields such that $K \cap L = \mathbb{Q}$ and the discriminants of K and L are relatively prime, then $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L$.* □

Proof. See section I.9, theorem 9.3 and corollary 9.4 in [3]. □

From these two results and from our earlier work on cyclotomic fields, we see that if we can show that $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathbb{Z}[\zeta_{p^r}]$ we will have

$$\mathcal{O}_K = \mathbb{Z}[\zeta_m, \zeta_{p^r}] = \mathbb{Z}[\zeta_n],$$

as desired. Hence it suffices to show $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathbb{Z}[\zeta_{p^r}]$, and we do so now.

Suppose $n = p^r$ is a prime power. We start with some calculations. Let k be a natural number prime to p, so that ζ_n^k is a primitive nth root of unity. Then $\zeta_n = (\zeta_n^k)^j$ for some j, so the ratios

$$\frac{1-\zeta_n^k}{1-\zeta_n} = 1 + \zeta_n + \cdots + \zeta_n^{k-1},$$
$$\frac{1-\zeta_n}{1-\zeta_n^k} = \frac{1-(\zeta_n^k)^j}{1-\zeta_n^k} = 1 + \zeta_n^k + \cdots + (\zeta_n^k)^{j-1}$$

are both units in $\mathcal{O}_K$. Using the cyclotomic polynomial

$$\Phi_n(x) = x^{p^{r-1}(p-1)} + \cdots + x^{p^{r-1}} + 1 = \prod_{1 \le i \le n;\ \gcd(i,n)=1} (x - \zeta_n^i)$$

we can also calculate

$$\begin{aligned}\Phi_n(1) &= p \\ &= \prod_{1 \le i \le n;\ \gcd(i,n)=1} (1 - \zeta_n^i) \\ &= (1-\zeta_n)^{\phi(n)} u,\end{aligned}$$

where $u \in \mathcal{O}_K^\times$ is a product of quotients of the form studied directly above. Writing $\pi = 1 - \zeta_n$, we then have $\Phi_n(1) = \pi^{\phi(n)}u = p$. This equality gives us an equality of ideals

$$p\mathcal{O}_K = \pi^{\phi(n)}\mathcal{O}_K = (\pi\mathcal{O}_K)^{\phi(n)}.$$

As an aside, note that with this equality we have proven proposition 2.1.8 above: that p is totally ramified in $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p^r})$.

The ideal $\pi\mathcal{O}_K$ factors into a product of prime ideals like so:

$$\pi\mathcal{O}_K = \prod_{j=1}^{r} \mathfrak{P}_j^{e_j}.$$

Substituting above gives

$$p\mathcal{O}_K = \prod_{j=1}^{r} \mathfrak{P}_j^{\phi(n)e_j},$$

and we can apply theorem 1.2.5 to get

$$\phi(n)\sum_{i=1}^{r} e_i f_i = \phi(n),$$

from which we conclude immediately that $r = e_1 = f_1 = 1$. In particular, we find $\pi\mathcal{O}_K$ is a prime ideal, and from $f_1 = 1$ we conclude that the dimension $[\mathcal{O}_K/\pi\mathcal{O}_K : \mathbb{F}_p] = 1$ and $\mathcal{O}_K/\pi\mathcal{O}_K \cong \mathbb{F}_p$. Additionally, we see from this that p is totally ramified in $\mathbb{Q}(\zeta_n)$.

We are now ready to make the main thrust of the proof. We start by citing one more result we will need.

Theorem 2.2.3. *Let A be a Dedekind ring with fraction field K, and let L be a finite separable extension of K with $[L : K] = n$. Let B be the integral closure of A in L. Suppose $\theta \in B$ is a primitive element for L over K. Then $D(1, \theta, \ldots, \theta^{n-1})B \subset A[\theta] \subseteq B$.*

Proof. See section I.7, theorem 7.5 in [3]. □

In the present case, this shows that there is some power k of p (recall $n = p^r$) such that

$$p^k\mathcal{O}_K \subset \mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_K.$$

Consider now the quotient $\mathbb{Z}[\zeta_n]/(\mathbb{Z}[\zeta_n] \cap \pi\mathcal{O}_K)$. This will be a nontrivial subring of the quotient $\mathcal{O}_K/\pi\mathcal{O}_K$, and from $\mathcal{O}_K/\pi\mathcal{O}_K \cong \mathbb{F}_p$ we see by order considerations that in fact the quotient is equal to $\mathcal{O}_K/\pi\mathcal{O}_K$. In particular, any coset of $\pi\mathcal{O}_K$ in $\mathcal{O}_K$ has a representative in $\mathbb{Z}[\zeta_n]$, so we can write

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

Substituting then gives

$$\begin{aligned}\mathcal{O}_K &= \mathbb{Z}[\zeta_n] + \pi(\mathbb{Z}[\zeta_n] + \pi\mathcal{O}_K) \\ &= \mathbb{Z}[\zeta_n] + \pi^2\mathcal{O}_K,\end{aligned}$$

and repeating the process we see that $\mathcal{O}_K = \mathbb{Z}[\zeta_n] + \pi^t\mathcal{O}_K$ for all positive integers t. But we saw above that

$$p^k\mathcal{O}_K = \pi^{k\phi(n)}\mathcal{O}_K \subset \mathbb{Z}[\zeta_n],$$

so for $t = k\phi(n)$ the expression collapses to give $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, and we are done.

2.3 Higher Ramification Groups and Cyclotomic Fields

In the last chapter, we saw an introduction to the idea of ramification. In this section we elaborate further on ramification in finite Galois extensions. The ultimate goal is to describe a filtration of the Galois group given by higher ramification groups, which allow us to single out automorphisms which act trivially modulo high powers of a prime. Parsing ramification data at this level will be crucial to implement the step in our proof of Kronecker-Weber in which we kill all ramification away from a single prime factor, determined by the relevant field extension.

Let L/K denote a finite Galois extension of number fields, and let $\mathcal{O}_L, \mathcal{O}_K$ denote the rings of integers of L and K, respectively. We know that any prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ lifts to a unique product of prime ideals in $\mathfrak{O}_L$. In symbols, we have

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^e.$$

In this case we have that the Galois group $G = \mathrm{Gal}(L/K)$ acts transitively on the $\mathfrak{P}_i$; the transitivity of this action forces all e_i to be equal. Then the formula

$$\sum_{i=1}^{r} e_i f_i = [L : K]$$

becomes simply $efr = [L : K] = |G|$.

We also have that this transitive action of G on primes above $\mathfrak{p}$ gives rise to a surjective map of groups

$$G(\mathfrak{P}) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})),$$

where $G(\mathfrak{P})$ denotes the stabilizer of the action of G on primes above $\mathfrak{p}$, known as the **decomposition group** of $\mathfrak{P}$. We call the kernel of this map the **inertia group** of $\mathfrak{P}$, and denote it $G_0(\mathfrak{P})$.

Let us interpret the formula $efr = |G|$ in terms of the decomposition and inertia groups. Applying the orbit-stabilizer lemma to the action of G on the primes lying above $\mathfrak{p}$ shows that $r = [G : G(\mathfrak{P})]$. Using the first isomorphism theorem on the map from $G(\mathfrak{P})$ to the Galois group of the extension of residue fields gives that $f = |G(\mathfrak{P})|/|G_0(\mathfrak{P})|$. Rearranging and substituting the information we have already found shows that $e = |G_0(\mathfrak{P})|$. By definition, we have that $e = 1$ if and only if $\mathfrak{p}$ is unramified in L, so we have proved the following fact.

Proposition 2.3.1. *Let L/K be a finite Galois extension of number fields, with Galois group G and respective rings of integers $\mathcal{O}_L, \mathcal{O}_K$. A prime $\mathfrak{p} \subset \mathcal{O}_K$ is unramified in L if and only if, for some prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ lying above $\mathfrak{p}$, the inertia group $G_0(\mathfrak{P})$ is trivial.*

Remark. We may rephrase the proposition to say that $\mathfrak{p}$ is unramified if and only if the surjection of $G(\mathfrak{P})$ onto the Galois group of the extension of residue fields is really an isomorphism.

The following consequences of this characterization of ramification will be useful to us as we go along. First, we get a mechanism to construct intermediate extensions in which $\mathfrak{p}$ does not ramify, so long as G is abelian.

Proposition 2.3.2. *In the setup of proposition 2.3.1, if G is abelian, then $\mathfrak{p}$ is unramified in $L_0 = L^{G_0(\mathfrak{P})}$.*

Proof. By proposition 2.3.1, it is enough to show that the inertia group of the Galois group $H = \mathrm{Gal}(L_0/K)$ is trivial. Note that L_0/K is guaranteed to be Galois since we assumed G was abelian.

Since $G_0(\mathfrak{P})$ is the kernel of the map of G to the Galois group of residue fields, any element of $G_0(\mathfrak{P})$ acts trivially on $\ell = \mathcal{O}_L/\mathfrak{P}$. But $G_0(\mathfrak{P}) = \mathrm{Gal}(L/L_0)$, and the decomposition group is $G_0(\mathfrak{P})$ itself since it is a subgroup of the decomposition group which stabilizes $\mathfrak{P}$. Writing $\mathfrak{P}_0 = \mathfrak{P} \cap \mathcal{O}_{L_0}$ and $\ell_0 = \mathcal{O}_{L_0}/\mathfrak{P}_0$, we get a surjective homomorphism

$$G_0(\mathfrak{P}) \to \mathrm{Gal}(\ell/\ell_0).$$

Combining the information we have gathered so far, we find that $\mathrm{Gal}(\ell/\ell_0)$ is trivial, so $\ell = \ell_0$. Now consider $H := \mathrm{Gal}(L_0/K) \simeq G/\mathrm{Gal}(L/L_0) = G/G_0(\mathfrak{P})$. The inertia group in this case is trivial, so $\mathfrak{p}$ does not ramify in L_0, as desired. □

Next we show that lack of ramification plays nicely with composita.

Proposition 2.3.3. *Let L'/K and L''/K be finite Galois extensions of number fields, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime. Then if $\mathfrak{p}$ is unramified in L' and in L'', it is unramified in $L'L''$.*

Proof. Write $L = L'L''$, and let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime lying above $\mathfrak{p}$. Write $\mathfrak{P}'$ and $\mathfrak{P}''$ for the intersections of $\mathfrak{P}$ with $\mathcal{O}_{L'}$ and $\mathcal{O}_{L''}$, respectively, and analogously define the residue fields ℓ, ℓ', ℓ'' and Galois groups G, G', G''. Since $\mathfrak{p}$ is unramified in L' and L'', we have that the inertia groups $G'_0(\mathfrak{P}')$ and $G''_0(\mathfrak{P}'')$ are trivial. Since ℓ' and ℓ'' are subfields of ℓ, restricting an element $\tau \in G_0(\mathfrak{P})$ to G' or to G'' gives an element of the respective inertia groups. These groups are trivial, so τ is the identity on L' and L''. But the theorem of the primitive element shows that there exist $\alpha \in L'$ and $\beta \in L''$ such that $L' = K(\alpha)$ and $L'' = K(\beta)$, so that $L = K(\alpha, \beta)$. That τ fixes L' and L'' pointwise says precisely that τ fixes α and β, so τ fixes L. We conclude that $G_0(\mathfrak{P})$ is also trivial, so $\mathfrak{p}$ is unramified in L, as desired. □

Higher ramification groups directly generalize the decomposition and inertia groups we have seen already: they are those subgroups of the decomposition group $G(\mathfrak{P})$ which act trivially modulo powers of $\mathfrak{P}$; more specifically, the ith ramification group $G_i(\mathfrak{P})$ acts trivially modulo $\mathfrak{P}^{i+1}$. From this definition we see that the inertia group $G_0(\mathfrak{P})$ really is the 0th ramification group, as it acts trivially modulo $\mathfrak{P}$. When the Galois group G is finite, we then have a descending chain of subgroups of G, namely,

$$G(\mathfrak{P}) \supset G_0(\mathfrak{P}) \supset G_1(\mathfrak{P}) \supset \dots.$$

It is quick to see that when G is finite (as it will be in the cases we care about), there is some integer d such that $G_d(\mathfrak{P})$ (and hence all ramification groups beyond d) are trivial. Indeed, any nonidentity element of $G(\mathfrak{P})$ acts nontrivially on some $a \in \mathcal{O}_L$, and hence acts nontrivially on a modulo $\mathfrak{P}^d$ for some integer d.

We now prove a few facts about ramification groups which we will need for Kronecker-Weber.

Proposition 2.3.4. *Let L/K be a finite Galois extension of number fields with Galois group G, and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying above the prime $\mathfrak{p} \subset \mathcal{O}_K$. Write ℓ and k for the residue fields $\mathcal{O}_L/\mathfrak{P}$ and $\mathcal{O}_K/\mathfrak{p}$, respectively. The following hold:*

1. *$G_m(\mathfrak{P}) \triangleleft G(\mathfrak{P})$ for all $m \geq 0$.*
2. *There is an embedding $G_0(\mathfrak{P})/G_1(\mathfrak{P}) \hookrightarrow \ell^\times$. Furthermore, if $G(\mathfrak{P})/G_1(\mathfrak{P})$ is abelian, then the image of this embedding lies in $k^\times$.*
3. *For any $m \geq 1$, there is an embedding $G_m(\mathfrak{P})/G_{m+1}(\mathfrak{P}) \hookrightarrow \ell$, where ℓ is considered as an additive group.*

Proof. 1. This will follow from a direct calculation. We check that any conjugate of an element $\tau \in G_m(\mathfrak{P})$ by some $\lambda \in G(\mathfrak{P})$ remains in $G_m(\mathfrak{P})$. For any $a \in \mathcal{O}_L$, we have $(\lambda^{-1}\tau\lambda)(a) - a = \lambda^{-1}(\tau(\lambda(a)) - \lambda(a))$. Then by the definition of ramification groups we have $\tau(\lambda(a)) \equiv \lambda(a) \pmod{\mathfrak{P}^{m+1}}$. This means $\tau(\lambda(a)) - \lambda(a) \in \mathfrak{P}^{m+1}$, so since $\lambda \in G(\mathfrak{P})$ which stabilizes $\mathfrak{P}$ we have $\lambda^{-1}(\tau(\lambda(a)) - \lambda(a)) \in \mathfrak{P}^{m+1}$, so the conjugate map $\lambda^{-1}\tau\lambda \in G_m(\mathfrak{P})$ and we are done.

2. Take an element $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Since $\mathcal{O}_L$ is a Dedekind ring having unique factorization of ideals into a product of primes, we see that there are no ideals strictly between $\mathfrak{P}$ and $\mathfrak{P}^2$. But $\pi\mathcal{O}_L + \mathfrak{P}^2$ strictly contains $\mathfrak{P}^2$ and is contained in $\mathfrak{P}$, so in fact $\pi\mathcal{O}_L + \mathfrak{P}^2 = \mathfrak{P}$. This tells us that, modulo $\mathfrak{P}^2$, any element of $\mathfrak{P}$ can be expressed as a product of π with an element of $\mathcal{O}_L$. From this we may conclude that the map of $\mathcal{O}_L$-modules (and in fact of ℓ-vector spaces) $\mathcal{O}_L/\mathfrak{P} \to \mathfrak{P}/\mathfrak{P}^2$ given by multiplication by π is surjective. It is injective as well: if $\pi\alpha = \pi\beta$ in $\mathfrak{P}/\mathfrak{P}^2$, then $\pi(\alpha - \beta) \in \mathfrak{P}^2$, so since π was defined not to be in $\mathfrak{P}^2$ we must have $\alpha - \beta \in \mathfrak{P}$, hence $\alpha = \beta$ in $\mathcal{O}_L/\mathfrak{P}$. So the multiplication-by-π map is an isomorphism of $\mathcal{O}_L/\mathfrak{P} = \ell$-vector spaces, and since the domain is ℓ itself, these spaces have dimension one. Sending the basis $\{1\}$ for ℓ to $\mathfrak{P}/\mathfrak{P}^2$, we see that $\pi + \mathfrak{P}^2$ is an ℓ basis for this space.

   Now take some $\tau \in G(\mathfrak{P})$. We have that $\tau(\pi) + \mathfrak{P}^2$ will also be an ℓ-basis for $\mathfrak{P}/\mathfrak{P}^2$; indeed, any nonzero $\gamma \in \mathfrak{P}/\mathfrak{P}^2$ satisfies

$$\tau^{-1}(\gamma) = (\pi + \mathfrak{P}^2)a,$$

   for some unique $a \in \ell^\times$. Applying τ gives

$$\gamma = (\tau(\pi) + \mathfrak{P}^2)\tau(a),$$

   where again we note that a is uniquely determined. This uniqueness lets us define a function $\rho : G_0(\mathfrak{P}) \to \ell^\times$ by sending τ to $u(\tau)$, the scalar in $\ell^\times$ such that $\tau(\pi) \equiv u(\tau)\pi \pmod{\mathfrak{P}^2}$. Note that we could also define this function on the decomposition group, but here we restrict to inertia since, as we will see, the map as defined on $G(\mathfrak{P})$ may not be a group homomorphism. We claim ρ is a group homomorphism with kernel $G_1(\mathfrak{P})$; upon showing this, we will have established the first claim.

First we show ρ is a group homomorphism. Take $\sigma, \tau \in G_0(\mathfrak{P})$. Then

$$\begin{aligned}(\sigma\tau)(\pi) &\equiv \sigma(\tau(\pi)) \\ &\equiv \sigma(u(\tau)\pi) \\ &\equiv \sigma(u(\tau))\sigma(\pi) \\ &\equiv \sigma(u(\tau))u(\sigma) \pmod{\mathfrak{P}^2}.\end{aligned}$$

But $u(\tau) \in \ell$, and σ acts trivially on ℓ. So we get

$$(\sigma\tau)\pi \equiv u(\tau)u(\sigma)\pi \pmod{\mathfrak{P}^2},$$

showing that $\rho(\sigma\tau) = \rho(\sigma)\rho(\tau)$, so ρ is a group homomorphism.

It remains to show that $\ker\rho = G_1(\mathfrak{P})$. To show $\ker\rho \supseteq G_1(\mathfrak{P})$, take $\tau \in G_1(\mathfrak{P})$ and note that since $G_1(\mathfrak{P})$ acts trivially modulo $\mathfrak{P}^2$, we have

$$\tau(\pi) \equiv \pi \pmod{\mathfrak{P}^2},$$

so $\rho(\tau) = 1$. We now show $\ker\rho \subseteq G_1(\mathfrak{P})$. Write $L_0 = L^{G_0(\mathfrak{P})}$, the fixed field of inertia; by the proof of proposition 2.3.2 (coloring) above, we then have

$$\ell = \ell_0 := \mathcal{O}_{L_0}/(\mathfrak{P} \cap \mathcal{O}_{L_0}).$$

Then for any $a \in \mathcal{O}_L$, the class $\bar{a} \in \ell$ corresponds to a class $\bar{a}_0 \in \ell_0$; namely, the elements a and $a_0 \in \mathcal{O}_{L_0} \subset \mathcal{O}_L$ satisfy $a_0 \equiv a \pmod{\mathfrak{P} \cap \mathcal{O}_L}$. So $a - a_0 \in \mathfrak{P} \cap \mathcal{O}_{L_0}$, and since $\ell_0 = \ell \simeq \mathfrak{P}/\mathfrak{P}^2$ (the latter isomorphism being as ℓ-vector spaces) we have that the map $x \mapsto \pi x$ gives an ℓ-vector space isomorphism of ℓ_0 and $\mathfrak{P}/\mathfrak{P}^2$. Then there is some $a_1 \in \mathcal{O}_{L_0}$ satisfying $a \equiv a_0 + a_1\pi \pmod{\mathfrak{P}^2}$. Taking $\tau \in \ker\rho$, we have by definition that $\tau(\pi) \equiv \pi \pmod{\mathfrak{P}^2}$, and since $\tau \in G_0(\mathfrak{P})$ we know τ fixes $a_0 + \pi a_1$ modulo $\mathfrak{P}^2$, so $\tau(a) \equiv a \pmod{\mathfrak{P}^2}$. Since $a \in \mathcal{O}_L$ was arbitrary, we see that τ acts trivially modulo $\mathfrak{P}^2$, so $\tau \in G_1(\mathfrak{P})$ as claimed. We have thus constructed the desired embedding $G_0(\mathfrak{P})/G_1(\mathfrak{P}) \hookrightarrow \ell^\times$.

To finish this part of the proposition, we need to show that $G_0(\mathfrak{P})/G_1(\mathfrak{P})$ embeds into $k^\times$ when the quotient $G(\mathfrak{P})/G_1(\mathfrak{P})$ (note the lack of subscript!) is abelian. In this case we find that for any $\sigma \in G(\mathfrak{P})$ and $\tau \in G_0(\mathfrak{P})$, the commutator $\tau^{-1}\sigma^{-1}\tau\sigma$ lies in $G_1(\mathfrak{P})$. So, for any $a \in \mathcal{O}_L$, we get

$$\begin{aligned}&\tau^{-1}\sigma^{-1}\tau\sigma(a) \equiv a \pmod{\mathfrak{P}^2} \\ &\quad\implies \tau\sigma(a) \equiv \sigma\tau(a) \pmod{\mathfrak{P}^2}.\end{aligned}$$

Taking a to be π from earlier, we have

$$\begin{aligned}(\sigma\tau)\pi &\equiv \sigma(u(\tau))\sigma(\pi) \pmod{\mathfrak{P}^2}; \\ (\tau\sigma)\pi &\equiv \tau(u(\sigma))u(\tau)\pi \\ &\equiv u(\sigma)\pi u(\tau) \\ &\equiv u(\tau)\sigma(\pi) \pmod{\mathfrak{P}^2},\end{aligned}$$

where we have used the fact that $\tau \in G_0(\mathfrak{P})$ to move from the second line to the third. But π, hence $\sigma(\pi)$, is an ℓ-basis for $\mathfrak{P}/\mathfrak{P}^2$, so comparing the two congruences immediately above shows that $u(\tau) = \sigma(u(\tau))$. Since $\sigma \in G(\mathfrak{P})$ was arbitrary and the induced map on Galois groups $G(\mathfrak{P}) \to \mathrm{Gal}(\ell/k)$ is surjective, varying σ shows that $u(\tau)$ lies in the fixed field of $\mathrm{Gal}(\ell/k)$, hence in k (really in $k^\times$). This is what we wanted to show.

3. We want to show that for $m \geq 1$, the quotient $G_m(\mathfrak{P})/G_{m+1}(\mathfrak{P})$ embeds into the additive group of ℓ. Again let $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. We can apply the same argument as that used in the proof of part (2) of the proposition to show that $\pi^s \mathcal{O}_L + \mathfrak{P}^{s+1} = \mathfrak{P}^s$ for any $s \geq 1$, and that $\pi^s + \mathfrak{P}^{s+1}$ is an ℓ-basis for the vector space $\mathfrak{P}^s/\mathfrak{P}^{s+1}$.

   By definition, any $\tau \in G_m(\mathfrak{P})$ fixes π modulo $\mathfrak{P}^{m+1}$. From the previous paragraph, we know $\pi^{m+1} + \mathfrak{P}^{m+2}$ is an ℓ-basis for $\mathfrak{P}^{m+1}/\mathfrak{P}^{m+2}$, so there is a unique $a(\tau) \in \ell$ such that

$$\tau(\pi) \equiv \pi + a(\tau)\pi^{m+1} \pmod{\mathfrak{P}^{m+2}}.$$

   We then get a map $\xi : G_m(\mathfrak{P}) \to \ell$ given by mapping τ to $a(\tau)$. We wish to show that ξ is a group homomorphism with kernel $G_{m+1}(\mathfrak{P})$.

   First we show ξ is a homomorphism. Take $\sigma, \tau \in G_m(\mathfrak{P})$. Direct calculation gives

$$\begin{aligned}\sigma(\tau(\pi)) &\equiv \sigma(\pi + a(\tau)\pi^{m+1}) \\ &\equiv \sigma(\pi) + \sigma(a(\tau))\sigma(\pi)^{m+1} \\ &\equiv \pi + a(\sigma)\pi^{m+1} + a(\tau)(\pi + a(\sigma)\pi^{m+1})^{m+1} \pmod{\mathfrak{P}^{m+2}}.\end{aligned}$$

   Notice that all terms in the product $(\pi + a(\sigma)\pi^{m+1})^{m+1}$ vanish modulo $\mathfrak{P}^{m+2}$ except π^{m+1}, so we have

$$\sigma(\tau(\pi)) \equiv \pi + (a(\sigma) + a(\tau))\pi^{m+1} \pmod{\mathfrak{P}^{m+2}},$$

   confirming that ξ is a group homomorphism.

   It remains to describe $\ker \xi$. If $\tau \in G_{m+1}(\mathfrak{P})$, then $\tau(\pi) \equiv \pi \pmod{\mathfrak{P}^{m+2}}$, so $a(\tau) = 0$ and $\tau \in \ker \xi$. Now suppose $\tau \in \ker \xi$. Since $\ell = \ell_0$ as in the proof of part (2), we have, for any $a \in \mathcal{O}_L$, elements $a_0, \ldots, a_{m+1} \in \mathcal{O}_{L_0}$ such that

$$a \equiv a + 0 + a_1\pi + \cdots + a_{m+1}\pi^{m+1} \pmod{\mathfrak{P}^{m+2}}.$$

   But $\tau \in \ker \xi$, so $\tau(\pi) \equiv \pi \pmod{\mathfrak{P}^{m+2}}$. In light of the above congruence, we then have $\tau(a) \equiv a \pmod{\mathfrak{P}^{m+2}}$, so $\tau \in G_{m+1}(\mathfrak{P})$. The desired result follows.

□

Remark. We proved the following fact in the course of our work above, which will be useful in proving Hilbert's formula later: an automorphism $\tau \in G_0(\mathfrak{P})$ is an element of $G_m(\mathfrak{P})$ if and only if $\tau(\pi) \equiv \pi \pmod{\mathfrak{P}^{m+1}}$.

We conclude the section by using the results we just proved to show divisibility properties involving the ramification index.

Corollary 2.3.5. *Let $p \neq q$ be rational primes. Let $K/\mathbb{Q}$ be an abelian Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) = G$ having $|G| = p^m$. For any prime ideal $\mathfrak{Q} \subset \mathcal{O}_K$ lying over (q) we have $G_1(\mathfrak{Q}) = \{e\}$. Then the ramification index $e(\mathfrak{Q}|q) = [G_0(\mathfrak{Q}) : G_1(\mathfrak{Q})]$ and this index divides $\gcd(p^m, q-1)$.*

Proof. We know that $k = \mathcal{O}_K/\mathfrak{Q}$ is a finite field of q-power order. By part (3) of proposition 2.3.4, the quotient $G_1(\mathfrak{Q})/G_2(\mathfrak{Q})$ embeds into k, hence is a q-group. But $G_1(\mathfrak{Q})$ and $G_2(\mathfrak{Q})$ are also p-groups by virtue of being subgroups of the p-group G, so in fact $G_1(\mathfrak{Q})/G_2(\mathfrak{Q}) = \{e\}$ and similarly $G_m(\mathfrak{Q})/G_{m+1}(\mathfrak{Q}) = \{e\}$ for all $m \geq 1$. Therefore, if $G_1(\mathfrak{Q})$ is nontrivial we must have that all ramification groups higher than $G_1(\mathfrak{Q})$ are nontrivial, which is not possible for a finite extension. So $G_1(\mathfrak{Q}) = 1$, which is part of our claim.

Now consider the order $|G_0(\mathfrak{Q})|$ of the inertia group. Since $G_1(\mathfrak{Q})$ is trivial, we have

$$e(\mathfrak{Q}|q) = |G_0(\mathfrak{Q})| = |G_0(\mathfrak{Q})|/|G_1(\mathfrak{Q})| = [G_0(\mathfrak{Q}) : G_1(\mathfrak{Q})] = |G_0(\mathfrak{Q})/G_1(\mathfrak{Q})|.$$

Part (2) of proposition 2.3.4 then gives an embedding of $G_0(\mathfrak{Q})/G_1(\mathfrak{Q})$ into $k^\times$ whose image lies in $\mathbb{F}_q^\times$, since G is abelian. Applying the equality involving the ramification index above, we find that $e(\mathfrak{Q}|q) \mid |\mathbb{F}_q^\times| = q-1$ and also $e(\mathfrak{Q}|q) \mid p^m$, hence divides their gcd, as desired. □

Remark. Here we use the fact that the residue fields in $\mathbb{Q}$ are equal to $\mathbb{F}_p$ for p a prime–this is one of the crucial properties of $\mathbb{Q}$ that allow the phenomenon described by Kronecker-Weber to occur.

We conclude with a tower law for ramification in finite extensions, which will be useful later.

Proposition 2.3.6. *Let $K \subset L \subset M$ be a tower of finite extensions of number fields. Take prime ideals $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}''$ in $\mathcal{O}_K, \mathcal{O}_L, \mathcal{O}_M$, respectively, with $\mathfrak{P}'$ lying over $\mathfrak{P}$ and $\mathfrak{P}''$ lying over $\mathfrak{P}'$. Then*

$$e(\mathfrak{P}''|\mathfrak{P}) = e(\mathfrak{P}'|\mathfrak{P})e(\mathfrak{P}''|\mathfrak{P}').$$

Proof. Write $\alpha = e(\mathfrak{P}'|\mathfrak{P})$ and $\beta = e(\mathfrak{P}''|\mathfrak{P}')$. We lift $\mathfrak{P}$ to $\mathcal{O}_M$ in steps:

$$\begin{aligned} \mathfrak{P}\mathcal{O}_L &= (\mathfrak{P}')^\alpha \times (\text{others}); \\ \mathfrak{P}'\mathcal{O}_M &= (\mathfrak{P}'')^\beta \times (\text{others}) \\ \implies \mathfrak{P}\mathcal{O}_M &= (\mathfrak{P}'')^{\alpha\beta} \times (\text{others}). \end{aligned}$$

The result now follows immediately. □

2.4 The Different Ideal and Cyclotomic Fields

Here we give some exposition on the **different ideal**, which allows us to measure ramification in a similar, and in fact even more precise, way to the discriminant. The idea behind the different generalizes that of a dual lattice in $\mathbb{R}^n$, which answers the question: when does one obtain an integral dot product with every vector in a set? In the setting of number fields, we replace the dot product with the trace form and place the resulting object in the

context of the arithmetic of fractional ideals in Dedekind domains. Ultimately, the different will be useful for us when we classify the degree p extensions of $\mathbb{Q}$ ramified only at p on our way to proving the Kronecker-Weber theorem.

The facts and proofs in this section are taken from section 2 of the paper [6] by Igor Rapinchuk; for a more thorough introduction to the different with emphasis on the lattice perspective, the paper [1] by Keith Conrad is an excellent source.

We begin with some definitions.

Definition 2.4.1. Let L/K be a finite extension of number fields with respective rings of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. Let M be an $\mathcal{O}_K$-submodule of L which contains a basis for L/K. The **dual** M^* is the set of all $a \in L$ such that $\mathrm{Tr}_{L/K}(aM) \subset \mathcal{O}_K$. The **different** of the extension L/K, denoted $\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K)$, is $(\mathcal{O}_L^*)^{-1}$, where here $\mathcal{O}_L$ is considered as an $\mathcal{O}_K$-module and the inverse is taken in the group of fractional ideals of $\mathcal{O}_L$.

Remark. The dual M^* is in fact an $\mathcal{O}_K$ module, by the K-linearity of the trace and commutativity of multiplication. Additionally, note that $\mathcal{O}_L^*$ really is a fractional ideal of $\mathcal{O}_L$: it is an $\mathcal{O}_K$-submodule of L, and it is finitely generated since $\mathcal{O}_L$ is finitely generated over $\mathcal{O}_K$. It is clear that $\mathcal{O}_L \subset \mathcal{O}_L^*$, so that $\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K)$ is then an integral ideal of $\mathcal{O}_L$.

When $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module, the description is nicer: if $\{e_i\}$ is an $\mathcal{O}_K$-basis for $\mathcal{O}_L$, then the dual basis $\{e_i^*\}$ with respect to the trace form is an $\mathcal{O}_K$-basis for $\mathcal{O}_L^*$. It is also the case that taking duals is inclusion-reversing (see theorem 3.4 and corollary 3.5 in [1]).

Example 2.4.2. Let $K = \mathbb{Q}(i)$, and consider the extension $K/\mathbb{Q}$. We will calculate the dual of the ring of integers $\mathcal{O}_K = \mathbb{Z}[i]$ and its ideal inverse, which will be $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$. To calculate $\mathcal{O}_K^*$ it is enough to check traces of elements $a+bi \in K$ multiplied by basis elements $\{1, i\}$ for $\mathcal{O}_K$. Thus, $a + bi \in \mathcal{O}_K^*$ if and only if

$$\mathrm{Tr}_{K/\mathbb{Q}}(a + bi) = 2a \in \mathbb{Z};$$
$$\mathrm{Tr}_{K/\mathbb{Q}}((a + bi)i) = -2b \in \mathbb{Z}.$$

From this fact we see that $\mathcal{O}_K^* = \frac{1}{2}\mathcal{O}_K$, so $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}) = 2\mathcal{O}_K$.

We begin building up the theory of the different with the following tower law.

Proposition 2.4.3. *If $K \subset L \subset F$ is a tower of extensions of number fields, then*

$$\mathrm{diff}(\mathcal{O}_F|\mathcal{O}_K) = \mathrm{diff}(\mathcal{O}_F|\mathcal{O}_L)\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K),$$

where we have written $\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K)$ *as shorthand for the lift* $\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K)\mathcal{O}_F$ *of the ideal* $\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K) \subset \mathcal{O}_L$ *to* $\mathcal{O}_F$.

Proof. Write D_K, D_L for the duals of $\mathcal{O}_F$ over K and L, respectively, and write $\mathcal{O}_L^*$ for the dual of $\mathcal{O}_L$ over K. Also write C for the $\mathcal{O}_F$-module generated by $\mathcal{O}_L^*$, and note that it is a fractional ideal of $\mathcal{O}_F$ (its common denominator inherited from $\mathcal{O}_L^*$). Taking inverses in the equality we wish to prove, we find that it is enough to show

$$D_K = D_L C.$$

We begin with the reverse inclusion, and start by considering generators of C as an $\mathcal{O}_F$-module. Taking $a \in D_L$ and $b \in \mathcal{O}_L^*$, we calculate using transitivity and linearity of the trace:

$$\begin{aligned}\mathrm{Tr}_{F/K}(ab\mathcal{O}_F) &= \mathrm{Tr}_{L/K}\left(\mathrm{Tr}_{F/L}(ab\mathcal{O}_F\right) \\ &= \mathrm{Tr}_{L/K}\left(b \cdot \mathrm{Tr}_{F/L}(a\mathcal{O}_F)\right).\end{aligned}$$

Since $a \in D_L$, by definition of the dual we get $\mathrm{Tr}_{F/L}(a\mathcal{O}_F) \subset \mathcal{O}_L$, so

$$\mathrm{Tr}_{L/K}(b \cdot \mathrm{Tr}_{F/L}(a\mathcal{O}_F)) \subset \mathrm{Tr}_{L/K}(b\mathcal{O}_L) \subset \mathcal{O}_K,$$

since $b \in \mathcal{O}_L^*$.

Now we consider an arbitrary $c \in C$, which can be written as a finite sum $\sum_i b_i d_i$, where $b_i \in \mathcal{O}_L^*$ and $d_i \in \mathcal{O}_F$. Again applying the linearity of the trace and using the fact that the d_i are in $\mathcal{O}_F$, we find that for any $a \in D_L$,

$$\begin{aligned}\mathrm{Tr}_{F/K}(ac\mathcal{O}_F) &= \mathrm{Tr}_{F/K}\left(a\left(\sum_i b_i d_i\right)\mathcal{O}_F\right) \\ &= \sum_i \mathrm{Tr}_{F/K}(ab_i d_i \mathcal{O}_F) \\ &\subset \sum_i \mathrm{Tr}_{F/K}(ab_i\mathcal{O}_F) \\ &\subset \mathcal{O}_K.\end{aligned}$$

If we take instead of ac a finite sum $\sum_i a_i c_i$ where $a_i \in D_L$ and $c_i \in C$ we see that the same inclusion holds, and we conclude that $D_L C \subset D_K$.

We now prove the other inclusion. Let $a \in D_k$. Familiar facts about the trace tell us that

$$\begin{aligned}\mathrm{Tr}_{F/K}(a\mathcal{O}_F) &= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{F/L}(a\mathcal{O}_F)) \\ &= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{F/L}(a\mathcal{O}_L\mathcal{O}_F)) \\ &= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{F/L}(a\mathcal{O}_F)\mathcal{O}_L) \\ &\subset \mathcal{O}_K.\end{aligned}$$

By definition of the dual, we see that $\mathrm{Tr}_{F/L}(a\mathcal{O}_F) \subset \mathcal{O}_L^*$. Multiplying by $\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K)$, we get

$$\mathrm{Tr}_{F/L}(a \cdot \mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K)\mathcal{O}_F) \subset \mathcal{O}_L.$$

But then

$$a \cdot \mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K) \subset D_L,$$

which, upon multiplying by $\mathcal{O}_L^*$, gives

$$\begin{aligned}& a\mathcal{O}_L \subset D_L\mathcal{O}_L^* \\ \implies\ & a\mathcal{O}_F \subset D_L C \\ \implies\ & a \in C,\end{aligned}$$

completing the proof. □

Our next fact establishes one way in which the different measures ramification.

Proposition 2.4.4. *Let $K/\mathbb{Q}$ be a finite extension. A prime p is ramified in K if and only if there exists a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ that lies over p and divides* $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$.

Proof. We show first that for any nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$, we have

$$[\mathfrak{a}^{-1} : \mathcal{O}_K] = [\mathcal{O}_K : \mathfrak{a}],$$

where the quantities in question are indices of additive groups. To accomplish this, we prove that the $\mathcal{O}_K$-modules $\mathfrak{a}^{-1}/\mathcal{O}_K$ and $\mathcal{O}_K/\mathfrak{a}$ are isomorphic.

Suppose $\mathfrak{a}$ has the ideal factorization $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$, and note that by proposition 1.1.14 we have $\mathfrak{p}_i^{e_i+1} + \prod_{i \neq j} \mathfrak{p}_j = \mathcal{O}_K$. So we can pick elements $s_i \in \mathfrak{p}_i^{e_i} \setminus \mathfrak{p}_i^{e_i+1}$ such that $s_i \equiv 1 \pmod{\prod_{i \neq j} \mathfrak{p}_j}$. Setting $s = s_1 \dots s_r$, we find that, by construction,

$$s\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \mathfrak{q}_1^{f_1} \dots \mathfrak{q}_t^{f_t},$$

where no $\mathfrak{q}_j$ is equal to one of the $\mathfrak{p}_i$. We claim the map $x \mapsto sx$ sets up an $\mathcal{O}_K$-module isomorphism $\phi : \mathfrak{a}^{-1}/\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$.

First note that ϕ is well-defined since $s\mathcal{O}_K \subset \mathfrak{a}$ (consider their ideal factorizations). Then ϕ is clearly an $\mathcal{O}_K$-module homomorphism since it is given by multiplication by an element of $\mathcal{O}_K$; it remains to show that ϕ is a bijection.

To show ϕ is surjective, we show that $s\mathfrak{a}^{-1} + \mathfrak{a} = \mathcal{O}_K$. We know $\mathfrak{a} \subset s\mathfrak{a}^{-1} + \mathfrak{a}$, so $s\mathfrak{a}^{-1} + \mathfrak{a}$ has an ideal factorization of the form

$$s\mathfrak{a}^{-1} + \mathfrak{a} = \mathfrak{p}_1^{g_1} \dots \mathfrak{p}_r^{g_r}$$

where $0 \leq g_i \leq e_i$ for each $1 \leq i \leq r$. Multiplying through by $\mathfrak{a}$, we see that

$$\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \mathfrak{q}_1^{f_1} \dots \mathfrak{q}_t^{f_t} = s\mathcal{O}_K \subset \mathfrak{a}(s\mathfrak{a}^{-1} + \mathfrak{a}) = \mathfrak{p}_1^{e_1+g_1} \dots \mathfrak{p}_r^{e_r+g_r},$$

so applying proposition 1.1.14 again shows that all the g_i are zero, hence $s\mathfrak{a}^{-1} + \mathfrak{a} = \mathcal{O}_K$ and ϕ is surjective.

We show ϕ is injective by proving $s^{-1}I \cap \mathfrak{a}^{-1} = \mathcal{O}_K$. Like surjectivity, this fact follows quickly upon considering ideal factorizations: we have

$$s^{-1}\mathfrak{a} = \mathfrak{q}_1^{-g_1} \dots \mathfrak{q}_t^{-g_t};$$
$$\mathfrak{a}^{-1} = \mathfrak{p}_1^{-e_1} \dots \mathfrak{p}_r^{-e_r},$$

so proposition 1.1.14 tells us that $s^{-1}\mathfrak{a} \cap \mathfrak{a}^{-1} = \mathcal{O}_K$, showing ϕ is an isomorphism and proving the desired equality of indices.

We are now ready to prove the main statement. We will show instead the equivalent statement: if $D = \mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$, the quantity $[\mathcal{O}_K : D]$ is divisible by p. The equivalence of these statements can be seen using the ideal norm, namely its multiplicativity, and the fact that residue fields for primes lying above p are field extensions of $\mathbb{F}_p$, hence have p-power order. Since the ideal norm is outside the scope of this work, we refer the reader to section 3.5 of [7] for the basics, and continue with the proof.

By our work above, we have that $[\mathcal{O}_K : D] = [\mathcal{O}_K^* : \mathcal{O}_K]$. Since the ramified primes are precisely those dividing the discriminant, it is enough to show $[\mathcal{O}_K^* : \mathcal{O}_K] = |d|$, the

discriminant of $K/\mathbb{Q}$. Toward this end, we note that in fact $[\mathcal{O}_K^* : \mathcal{O}_K] = |\det A|$, where A is the change-of-basis matrix from a $\mathbb{Z}$-basis $\{v_i\}$ of $\mathcal{O}_\mathcal{K}$ to the dual basis $\{v_i^*\}$ of $\mathcal{O}_K^*$ (a consequence of the compatible basis theorem for finitely-generated modules over a PID). But multiplying the equations defining the entries of A by v_i and taking traces shows that A is precisely the matrix of the trace form, so that $|\det A| = |d|$ by definition, completing the proof. □

To get as much information as we can from the different, we will need to extend what we know about the $v_\mathfrak{p}$ function which we first saw in proposition 1.1.14. Recall that we defined $v_\mathfrak{p}$ on fractional ideals of a Dedekind ring A to return the power of $\mathfrak{p}$ occurring in the factorization of a given fractional ideal. If $K = \mathrm{frac}(A)$, we can extend $v_\mathfrak{p}$ to $K^\times$ by defining, for $a \in K^\times$, $v_\mathfrak{p}(a) = v_\mathfrak{p}(aA)$. The fact we will need about this function follows, after which we prove two lemmas needed for proof of the main theorem connecting the different to ramification groups.

Lemma 2.4.5. *Let K be a number field and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal. Let $a_1, \ldots, a_n$ be such that the values $v_\mathfrak{p}(a_i)$ are pairwise distinct. Then $a_1 + \cdots + a_n \neq 0$, and*

$$v_\mathfrak{p}(a_1 + \cdots + a_n) = \min(v_\mathfrak{p}(a_i)).$$

Proof. We induct, beginning with the case $n = 2$. Note that $v_\mathfrak{p}(-1) = v_\mathfrak{p}(\mathcal{O}_K) = 0$, so that in particular $v_p(a) = v_p(-a)$ for any $a \in K^\times$. This means that if $v_\mathfrak{p}(a_1) \neq v_\mathfrak{p}(a_2)$, we must have $a_1 \neq a_2$, as we wanted. Now suppose without loss of generality that $v_\mathfrak{p}(a_1) < v_\mathfrak{p}(a_2)$. Then

$$\begin{aligned}\min(v_\mathfrak{p}(a_1 + a_2), v_\mathfrak{p}(a_2)) &\leq v_\mathfrak{p}(a_1 + a_2 - a_2)\\ &= v_\mathfrak{p}(a_1)\\ &= \min(v_\mathfrak{p}(a_1), v_\mathfrak{p}(a_2))\\ &\leq v_\mathfrak{p}(a_1 + a_2).\end{aligned}$$

Note now that we cannot have $\min(v_\mathfrak{p}(a_1 + a_2), v_\mathfrak{p}(a_2)) = v_\mathfrak{p}(a_2)$, as the work above then gives $v_\mathfrak{p}(a_2) \leq v_\mathfrak{p}(a_1)$ which directly contradicts our initial assumption. So $\min(v_\mathfrak{p}(a_1 + a_2), v_\mathfrak{p}(a_2)) = v_\mathfrak{p}(a_1 + a_2)$, and we get

$$v_\mathfrak{p}(a_1) = v_\mathfrak{p}(a_1 + a_2) = \min(v_\mathfrak{p}(a_1), v_\mathfrak{p}(a_2)),$$

which is what we wanted to show.

Now assume the result holds for $a_1, \ldots, a_k$ with $v_\mathfrak{p}(a_i)$ pairwise distinct, and let $a_{k+1} \in K^\times$ satisfy $v_\mathfrak{p}(a_{k+1}) \neq v_\mathfrak{p}(a_i)$ for all $i \neq k+1$. Then $v_\mathfrak{p}(a_1 + \cdots + a_k) = \min_{1 \leq i \leq k}(v_\mathfrak{p}(a_i)) \neq v_\mathfrak{p}(a_{k+1})$, so we can apply the $n = 2$ case to conclude immediately that $a_1 + \cdots + a_k + a^{k+1} \neq 0$ and $v_\mathfrak{p}(a_1 + \cdots + a_k + a_{k+1}) = \min_{1 \leq i \leq k+1}(v_\mathfrak{p}(a_i))$, as desired. □

Lemma 2.4.6. *Let L/K be a finite, degree-n extension of number fields, and suppose $\alpha \in \mathcal{O}_L$ satisfies $L = K(\alpha)$. If $f(x)$ is the minimal polynomial for α over K, then*

$$(\mathcal{O}_K[\alpha])^* = (f'(\alpha))^{-1}\mathcal{O}_K[\alpha].$$

Proof. Since α generates L/K, the $\mathcal{O}_K$-module $\mathcal{O}_K[\alpha]$ is free with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. To determine the structure of $(\mathcal{O}_K[\alpha])^*$, then, it is enough to calculate the dual of this basis. Write

$$g(x) := \frac{f(x)}{x - \alpha} = \beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1} \in L[x];$$

we claim that the dual basis is given by

$$\left\{ \frac{\beta_0}{f'(\alpha)}, \ldots, \frac{\beta_{n-1}}{f'(\alpha)} \right\}.$$

To show this, we write $\alpha_1, \ldots, \alpha_n$ for the roots of $f(x)$, and show that for all $0 \leq r \leq n-1$, we have

$$\sum_{i=1}^{n} \frac{f(x)}{x - \alpha_i} \cdot \frac{\alpha_i^r}{f'(\alpha_i)} = x^r.$$

Indeed, if we define $g_i(x) = f(x)/(x - \alpha_i)$ for all i, we find that

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) = g_i(\alpha_i).$$

Consider now the polynomial

$$\left(\sum_{i=1}^{n} \frac{\alpha_i^r}{f'(\alpha_i)} g_i(x) \right) - x^r.$$

At each α_i, every term in the sum on the left vanishes except for the ith term, which evaluates to α_i^r. It follows that this polynomial vanishes on all α_i, hence is a degree $n-1$ polynomial with n roots, and is therefore identically zero. This proves the identity we set out to show.

We can rewrite this identity using the trace, where we say the "trace" of a polynomial is the polynomial obtained by applying the trace to coefficients. In particular, since the left-hand side of the equation is a sum of Galois conjugates, we can write

$$\mathrm{Tr}_{L/K} \left(\frac{f(x)}{x - \alpha} \cdot \frac{\alpha^r}{f'(\alpha)} \right) = x^r.$$

Substituting $f(x)/(x - \alpha) = \beta_0 + \cdots + \beta_{n-1} x^{n-1}$ and using the fact that the identity immediately above holds for all $0 \leq r \leq n-1$, we find that for all $0 \leq i, j \leq n-1$,

$$\mathrm{Tr}_{L/K} \left(\alpha^i \frac{\beta_j}{f'(\alpha)} \right) = \delta_{ij},$$

proving the claim that $\{\beta_j / f'(\alpha)\}$ is the dual basis for $\{\alpha^i\}$.

Using this new fact, we have

$$(\mathcal{O}_K[\alpha])^* = (f'(\alpha))^{-1} (\beta_0 \mathcal{O}_K + \cdots + \beta_{n-1} \mathcal{O}_K).$$

From here, we need to show $\beta_0 \mathcal{O}_K + \cdots + \beta_{n-1} \mathcal{O}_K = \mathcal{O}_K[\alpha]$. For the reverse inclusion, note that since f and $x - \alpha$ are monic, we must have $\beta_{n-1} = 1$, so

$$\mathcal{O}_K \subset \beta_0 \mathcal{O}_K + \cdots + \beta_{n-1} \mathcal{O}_K =: R.$$

It remains to show $\alpha R \subset R$. From $g(x)(x-\alpha) = f(x)$ and the fact that $\alpha \in \mathcal{O}_L$ we see that $\beta_{i-1} - \alpha\beta_i \in \mathcal{O}_K$ for all i, forcing $\alpha\beta_i \in R$ for all i. Therefore $\alpha R \subset R$.

To show the forward inclusion, note that since $g(x)$, which determines the β_i, is obtained from long division by monic polynomials in $\mathcal{O}_K[\alpha][x]$, so the β_i are in $\mathcal{O}_K[\alpha]$ as well. $\square$

Lemma 2.4.7. *Let L/K be a finite, degree n extension of number fields. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is totally ramified in L. Let $\mathfrak{P} \subset \mathcal{O}_L$ be the unique prime ideal lying over $\mathfrak{p}$, and pick $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Then:*

1. *$\{1, \pi, \dots, \pi^{n-1}\}$ is a basis for L/K.*
2. *If $a_0, \dots, a_{n-1} \in \mathcal{O}_K$ satisfy $a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \in \mathfrak{P}^n$, then $a_i \in \mathfrak{p}$ for all i.*
3. *There exists $s \in \mathcal{O}_K \setminus \mathfrak{p}$ such that $s\mathcal{O}_L \subset \mathcal{O}_K[\pi]$.*

Proof. 1. Take $a_0, \dots, a_{n-1} \in K$ such that $a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} = 0$, and suppose for the sake of contradiction that not all (hence at least 2) of the a_i are nonzero. Since $\mathfrak{p}$ is totally ramified, its lift to L has ideal factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n.$$

By the tower law for ramification indices, for all $\alpha \in K$ we then have $v_{\mathfrak{P}}(\alpha) = n \cdot v_{\mathfrak{p}}(\alpha)$. The contrapositive of lemma 2.4.5 then shows there are indices i, j for which $a_i, a_j \neq 0$ and

$$\begin{aligned} v_{\mathfrak{P}}(a_i\pi^i) &= v_{\mathfrak{P}}(a_j\pi^j) \\ \implies v_{\mathfrak{P}}(a_i a_j^{-1}) &= v_{\mathfrak{P}}(\pi^{j-i}) \\ &= j - i. \end{aligned}$$

But $0 < |j - i| < n$, and by the above remark on ramification indices we have $v_{\mathfrak{P}}(a_i a_j^{-1}) \in n\mathbb{Z}$, a contradiction. So all $a_i = 0$ and $\{1, \pi, \dots, \pi^{n-1}\}$ is a basis for L/K.

2. Suppose $a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \in \mathfrak{P}^n$ with $a_i \in \mathcal{O}_K$. By the proof of part (1), we have that the $v_{\mathfrak{P}}(a_i\pi^i)$ are distinct. We may then apply lemma 2.4.5 to get

$$\begin{aligned} n &\leq v_{\mathfrak{P}}(a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}) \\ &= \min_{0 \leq i \leq n-1} (v_{\mathfrak{P}}(a_i\pi^i)) \\ &\leq v_{\mathfrak{P}}(a_i\pi^i) \quad \forall i. \end{aligned}$$

Then for all i we have $v_{\mathfrak{P}}(a_i) \geq n - i > 0$, and since $a_i \in \mathcal{O}_K$ we have $a_i \in \mathfrak{p}$ for all i, as desired.

3. By (1), the $\mathbb{Z}$-module $\mathcal{O}_K[\pi]$ is free of the same rank as $\mathcal{O}_L$. It follows that the set

$$\mathfrak{a} = \{s \in \mathcal{O}_K : s\mathcal{O}_L \subset \mathcal{O}_K[\pi]\}$$

is a nonzero ideal in $\mathcal{O}_K$. To prove the claim, we show that $\mathfrak{a} \not\subset \mathfrak{p}$. Assume the opposite is true. Using the ideal factorization of $\mathfrak{p}\mathcal{O}_L$ and part (2) above, we see that we have

$$\mathfrak{a}\mathcal{O}_L \subset \mathcal{O}_K[\pi] \cap \mathfrak{P}^n \subset \mathfrak{p}\mathcal{O}_K[\pi].$$

Working further, we get

$$\begin{aligned} & (\mathfrak{p}^{-1}\mathfrak{a})\mathcal{O}_L \subset \mathcal{O}_K[\pi] \\ \implies & \mathfrak{p}^{-1}\mathfrak{a} \subset \mathfrak{a}, \end{aligned}$$

which creates a contradiction upon taking $v_\mathfrak{p}$ for both sides.

□

We are now ready to prove the result known as Hilbert's formula, which will allow us to compare the fixed fields of ramification groups to the fixed fields of certain subgroups of the relevant Galois group. This information will be crucial to classifying the degree p abelian extensions ramified only at p when p is odd.

Theorem 2.4.8. *Let L/K be a finite Galois extension of number fields with Galois group G. Fix a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ and a prime $\mathfrak{P} \subset \mathcal{O}_L$ lying above $\mathfrak{p}$. For $n \geq 0$, write G_n for the nth ramification group $G_n(\mathfrak{P})$ (where as usual G_0 is the inertia group). Suppose the ramification index $e(\mathfrak{P}|\mathfrak{p}) = [L : K]$, write $d = v_\mathfrak{P}(\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K))$, and pick $\pi \in \mathfrak{P}/\mathfrak{P}^2$ with minimal polynomial f over K. Then:*

1. *$d = v_\mathfrak{P}(f'(\pi))$;*
2. *$d = \sum_{n\geq 0}(|G_n| - 1)$ (Hilbert's formula).*

Proof. 1. By part (3) of lemma 2.4.7, there exists $s \in \mathcal{O}_K \setminus \mathfrak{p}$ such that

$$s\mathcal{O}_L \subset \mathcal{O}_K[\pi] \subset \mathcal{O}_L.$$

Taking duals gives

$$\mathcal{O}_L^* \subset \mathcal{O}_K[\pi]^* \subset s^{-1}\mathcal{O}_L^*.$$

We have, by lemma 2.4.6, that $\mathcal{O}_K[\pi]^* = (f'(\pi))^{-1}\mathcal{O}_K[\pi]$, so we also know that

$$\mathcal{O}_L^* \subset (f'(\pi))^{-1}\mathcal{O}_K[\pi] \subset (f'(\pi))^{-1}\mathcal{O}_L.$$

By combining these chains of set inclusions and multiplying by s, we get

$$s^2(f'(\pi))^{-1}\mathcal{O}_L \subset s(f'(\pi))^{-1}\mathcal{O}_K[\pi] \subset \mathcal{O}_L^*.$$

Upon taking ideal inverses, we find from the chain of inclusions immediately above that $\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K) \subset s^{-2}(f'(\pi))\mathcal{O}_L$, and using the chain above the one just mentioned we find (again after taking inverses) that $f'(\pi)\mathcal{O}_L \subset \mathrm{diff}(\mathcal{O}_L|\mathcal{O}_K)$.

Recall now that $s \notin \mathfrak{p}$, so that $v_\mathfrak{p}(s) = v_\mathfrak{P}(s) = 0$. The preceeding paragraph then tells us that $v_\mathfrak{P}(f'(\pi)) \geq d$ and $d \geq v_\mathfrak{P}(s^{-2}f'(\pi)) = v_\mathfrak{P}(f'(\pi))$, so $d = v_\mathfrak{P}(f'(\pi))$ as we wanted to show.

2. Part (1) of lemma 2.4.7 shows that $L = K(\pi)$, so

$$f(x) = \prod_{\sigma \in G} (x - \sigma(\pi)).$$

The formula for the derivative at a root gives

$$f'(\pi) = \prod_{\sigma \in G \setminus \{1\}} (\pi - \sigma(\pi)).$$

Since the ramification index $e(\mathfrak{P}|\mathfrak{p}) = [L : K]$, the inertia group G_0 is the full Galois group G. Using the result quoted in the remark after the proof of proposition 2.3.4, we then know that if $\sigma \in G_{m-1} \setminus G_m$ for some m, we have $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^m}$ but $\sigma(\pi) \not\equiv \pi \pmod{\mathfrak{P}^{m+1}}$. Therefore $v_{\mathfrak{P}}(\pi - \sigma(\pi)) = m$ for this σ, and applying this argument to every element of G and combining with the result of part (1) of this theorem gives

$$d = v_{\mathfrak{P}}(f'(\pi)) = \sum_{m \geq 0} m(|G_{m-1}| - |G_m|).$$

Since the filtration of G via the higher ramification groups stabilizes at the trivial group after finitely many steps, we can pick N such that G_m is trivial for all $m \geq N$. We need then only take the sum on the right up to N. Writing out the terms of the sum, one sees that the sum telescopes to one of the form $\sum_{m=0}^{N-1} |G_m| - 1$, after which we are free to sum to infinity since the extra terms are zero. Doing so gives $d = \sum_{m \geq 0} |G_m| - 1$, which is what we wanted.

□

Corollary 2.4.9. *If $[L : K] = p$ a prime in the setup of the above theorem, then $(p-1) \mid d$.*

Proof. Since p is prime each ramification group has order p or order 1. Hilbert's formula then produces the desired result immediately. □

We conclude our development of the basic theory of the different by showing, as we noted earlier, how the different can be used to show certain intermediate fields of an extension are fixed by one of the ramification groups.

Proposition 2.4.10. *Keep the setup for theorem 2.4.8. Write $L_n = L^{G_n}$ for the fixed field of the nth ramification group. If $H \leqslant G$ with $|H| = |G_n|$ and $M = L^H$, we have*

$$v_{\mathfrak{P}}(\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_M)) \leq v_{\mathfrak{P}}(\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_{L_n})).$$

Equality holds if and only if $M = L^n$.

Proof. The ramification groups of L/M are precisely those elements of H which act trivially modulo powers of $\mathfrak{P}$. Therefore $H_m = H \cap G_m$ for all $m \geq 0$.

By the tower law for ramification indices, we have that $\mathfrak{P}' := \mathfrak{P} \cap \mathcal{O}_M$ is totally ramified in L. We can then apply Hilbert's formula, giving

$$v_{\mathfrak{P}}(\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_M)) = \sum_{m \geq 0} (H_m - 1).$$

We can repeat this process with H replaced by L_n, where the ramification groups of L/L_n are now given by $G_m \cap G_n$ for $m \geq 0$. Applying Hilbert's formula to this situation and using the fact that the G_m are related by a chain of inclusions, we find

$$\begin{aligned} v_{\mathfrak{P}}(\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_{L_n})) &= \sum_{m \geq 0} (|G_m \cap G_n| - 1) \\ &= (n+1)(|G_n| - 1) + \sum_{m > n} (|G_m| - 1). \end{aligned}$$

Now return to the sum $\sum_{m \geq 0}(H_m - 1)$. When $m > n$, we have $|H_m| = |H \cap G_m| \leq |G_m|$, so

$$\sum_{m > n} (H_m - 1) \leq \sum_{m > n} (|G_m| - 1).$$

For all $m \leq n$ we have $|H_m| \leq |H| = |G_n|$, so

$$\sum_{m=0}^{n} (|H_m| - 1) \leq (n+1)(|G_n| - 1).$$

Adding these two inequalities gives

$$v_{\mathfrak{P}}(\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_M)) \leq v_{\mathfrak{P}}(\mathrm{diff}(\mathcal{O}_L|\mathcal{O}_{L_n})),$$

proving the first part of the proposition.

To determine when equality holds, note that if $M \neq L_n$, we have $H \neq G_n$ by the Galois correspondence. Then $|H_n| < |H| = |G_n|$, forcing the above inequality to be strict. $\square$

Chapter 3

Two Proofs of the Kronecker-Weber Theorem

3.1 Introduction

We are finally in a position to prove the main theorem. Our exposition here essentially follows that in the expository paper [6] of Igor Rapinchuk, with the proof for p odd by Kummer theory coming from the note [5] by Andrei Rapinchuk.

Before getting started, let us give the idea of the structure of the proof. The important property of $\mathbb{Q}$ that allows us to take the approach we will use is the following result due to Hermite-Minkowski:

Theorem 3.1.1 (Hermite-Minkowski)**.** *No nontrivial finite extension $K/\mathbb{Q}$ has discriminant equal to* 1 *in absolute value; in particular, every such extension has at least one ramified prime.*

Proof. See section 4.3, theorem 1 in [7]. □

The field extension $K/\mathbb{Q}$ is assumed to be finite abelian, so the group $\operatorname{Gal} K/\mathbb{Q}$ is finite abelian. The structure theory of finite abelian groups guarantees the existence of prime powers $q_1, \ldots, q_r$ such that

$$\operatorname{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_r\mathbb{Z}.$$

For each factor $\mathbb{Z}/q_i\mathbb{Z}$ we define the subfield L_i to be the field fixed by $\prod_{j \neq i} \mathbb{Z}/q_j\mathbb{Z}$. Then $\operatorname{Gal}(K/L_i) = \mathbb{Z}/q_i\mathbb{Z}$, and K is the compositum of all L_i, so if L_i is contained in a cyclotomic extension for each i we will have that the same holds for K. Thus we may assume $K/\mathbb{Q}$ is a cyclic extension of prime-power degree. Afterward, we reduce to the case where K is ramified only at the prime appearing in this prime power. For the prime 2, we will be able to handle the rest using elementary techniques; for p odd, we will use the same general strategy but will need more theory to complete the proof. The point at which these two cases differ most is in classifying the degree p extensions of $\mathbb{Q}$ ramified only at p. This task will be much more difficult when p is odd, but on the other hand the extension in question will be unique when p is odd, in contrast with the case $p = 2$. We will give two proofs of this classification when p is odd: one using Kummer theory, and one using facts about

the different ideal we proved in section 2.4. Both rely on the Hermite-Minkowski theorem to produce contradictions in situations that would produce unramified extensions of $\mathbb{Q}$, so already we see how important this fact is to the proof of Kronecker-Weber. We will also be making use of the theory of ramification groups, which we developed also in the previous chapter.

3.2 Extensions of Degree p^r Ramified Only at p

We just discussed how the structure of finite abelian groups allows us to reduce Kronecker-Weber to the case of cyclic extensions of prime-power degree. Here we take the reduction one step further and put conditions on the ramification allowed in the extensions we consider. Namely, we will show it is enough to consider abelian extensions of p-power degree which are ramified only at p by constructing explicit subfields which remove ramification at one prime at a time. We prove the fact that allows us to make this reduction now.

Proposition 3.2.1. *Let p be a prime and $K/\mathbb{Q}$ an abelian extension with $[K:\mathbb{Q}] = p^r$. Assume there is a different prime q ramified in K. Then there is a subfield $L \subset \mathbb{Q}(\zeta_q)$ and an abelian extension $K'/\mathbb{Q}$ with degree p^s such that:*

1. *$KL = K'L$;*
2. *All primes other than p which are unramified in K are also unramified in K';*
3. *q is unramified in K'.*

Proof. We will construct the desired fields L and K', after which (2) and (3) will follow quickly. We save (1) for last.

Write $G = \mathrm{Gal}(K/\mathbb{Q})$, and let $\mathfrak{Q} \subset \mathcal{O}_K$ be a prime lying above $\mathfrak{q} := (q) \subset \mathbb{Z}$. Then by corollary 2.3.5 we have $e(\mathfrak{Q}|\mathfrak{q}) \mid \gcd(p^r, q-1)$. In particular this means

$$e(\mathfrak{Q}|\mathfrak{q}) \mid q - 1 = [\mathbb{Q}(\zeta_q) : \mathbb{Q}],$$

so the Galois correspondence gives us a unique subfield $L \subset \mathbb{Q}(\zeta_q)$ with degree equal to $e(\mathfrak{Q}|q)$.

Now let $\tilde{\mathfrak{Q}} \subset \mathcal{O}_{KL}$ be a prime lying above $\mathfrak{Q}$ (and hence above $\mathfrak{q}$). Then by proposition 2.3.2, if we write $\tilde{G} := \mathrm{Gal}(KL/\mathbb{Q})$, we know $\mathfrak{q}$ is unramified in $K' := (KL)^{\tilde{G}_0(\tilde{\mathfrak{Q}})}$. Since $K'/\mathbb{Q}$ is also an abelian extension with p-power degree, we have proved (3). To prove (2), let $\ell \neq q$ be a prime unramified in K. Since only q ramifies in L, we have that ℓ does not ramify in L, hence does not ramify in KL by proposition 2.3.3. The tower law for ramification indices (proposition 2.3.6) then shows that ℓ does not ramify in $K' \subset KL$, proving (2).

It remains to show that $KL = K'L$. Since $K'L \subset KL$ by construction, we only need to show the degrees are equal; we do this by determining the degree $[L:\mathbb{Q}]$. To start in this direction, note that by corollary 2.3.5 we have $\tilde{G}_1(\tilde{\mathfrak{Q}})$. Then applying part (2) of proposition 2.3.4 tells us that $\tilde{G}_0(\tilde{\mathfrak{Q}})/\tilde{G}_1(\tilde{\mathfrak{Q}}) \simeq \tilde{G}_0(\tilde{\mathfrak{Q}})$ embeds into $(\mathbb{F}_q)^\times$, hence is cyclic.

Now recall that $G = \mathrm{Gal}(K/\mathbb{Q})$ and $\tilde{G} = \mathrm{Gal}(KL/\mathbb{Q})$, so restricting automorphisms of $KL/\mathbb{Q}$ to K and to L gives an embedding of $\tilde{G}$ into $G \times \mathrm{Gal}(L/\mathbb{Q})$. Then the subgroup $\tilde{G}_0(\tilde{\mathfrak{Q}})$ embeds into $G_0(\mathfrak{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$. But by construction, we have $|G_0(\mathfrak{Q})| = |\mathrm{Gal}(L/\mathbb{Q})| = e(\mathfrak{Q}|q)$. In particular, since $\tilde{G}_0(\tilde{\mathfrak{Q}})$ is cyclic, the order of any element (hence the order of

the group itself) must divide $e(\mathfrak{Q}|q)$. But the order of $\tilde{G}_0(\tilde{\mathfrak{Q}})$ is $e(\tilde{\mathfrak{Q}}|q)$, and the tower law for ramification indices (proposition 2.3.6) tells us that $e(\mathfrak{Q}|q) \mid e(\tilde{\mathfrak{Q}}|q)$, so we get

$$|\operatorname{Gal}(L/\mathbb{Q})| = e(\mathfrak{Q}|q) = e(\tilde{\mathfrak{Q}}|q).$$

Now K' is unramified at q while L is totally ramified at q, so $K' \cap L = \mathbb{Q}$. We see, therefore, that $\tilde{G} \simeq G \times \operatorname{Gal}(L/\mathbb{Q})$, and we can calculate:

$$[K'L : \mathbb{Q}] = [K' : \mathbb{Q}][L : \mathbb{Q}] = [\tilde{G} : \tilde{G}_0(\tilde{\mathfrak{Q}})]|\tilde{G}_0(\tilde{\mathfrak{Q}})| = |\tilde{G}| = [KL : \mathbb{Q}],$$

showing $K'L = KL$. □

We conclude by showing how this proposition allows us to reduce the proof of Kronecker-Weber to a certain special case.

Proposition 3.2.2. *If any abelian extension $K/\mathbb{Q}$ of prime-power order p^r ramified only at p is contained in a cyclotomic extension, then any abelian extension $M/\mathbb{Q}$ is contained in a cyclotomic extension.*

Proof. We have previously remarked that the structure theorem for finite abelian groups implies that we can assume, without loss of generality, that $[M : \mathbb{Q}]$ is a prime power p^r. Since the number of ramified primes in M is a positive integer, we can induct on the number of primes other than p which ramify in M. If there are no such primes, then only p ramifies in M and we are done by hypothesis. Now let the set of primes other than p ramified in M be $\{q_1, \ldots, q_k\}$. By proposition 3.2.1, there is a subfield $L \subset \mathbb{Q}(\zeta_{q_k})$ and an abelian extension $M'/\mathbb{Q}$ such that M' has p-power degree, is not ramified at q, and is not ramified at any primes at which M is unramified. Then by induction M' lives in a cyclotomic extension $\mathbb{Q}(\zeta_m)$, and we have

$$M \subset ML = M'L \subset \mathbb{Q}(\zeta_{nq_k}),$$

as desired. □

We will now prove Kronecker-Weber in these special situations, distinguishing the cases $p = 2$ and p odd.

3.3 The Special Case for $p = 2$

The goal of this section is to prove the following proposition.

Proposition 3.3.1. *Let $K/\mathbb{Q}$ be an abelian extension of degree 2^m. If 2 is the only prime ramified in K, then $K \subset \mathbb{Q}(\zeta_{2^{m+2}})$.*

We will start with the case $m = 1$, and then handle the general case.

Lemma 3.3.2. *Let $E/\mathbb{Q}$ be a quadratic extension ramified only at 2. Then E is one of $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, or $\mathbb{Q}(\sqrt{2})$. Consequently, if E is real then $E = \mathbb{Q}(\sqrt{2})$.*

Proof. We can write $E = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a square-free integer. Then the discriminant of E is either d or $4d$, depending on whether d is $1 \pmod 4$. Since E ramifies only at 2, the discriminant is also equal to $\pm 2^k$ for some positive integer k. Since the discriminant cannot be odd, hence cannot be $1 \pmod 4$, we find that in fact the discriminant is always equal to $4d$ in our situation. The possible values of the discriminant are then $-4,\ \pm 8$, corresponding to $d = -1,\ \pm 2$, respectively. The desired result follows. □

To finish the $m = 1$ case, we need to show that each of $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(-\sqrt{2})$ lie in $\mathbb{Q}(\zeta_8)$. We show this by direct calculation. Indeed, we have $\zeta_8^2 = i$, so $\mathbb{Q}(i) \subset \mathbb{Q}(\zeta_8)$, and for the other two fields we see that

$$\begin{aligned}(\zeta_8 \pm \zeta_8^{-1})^2 &= \zeta_8^2 \pm 2 + \zeta_8^{-2} \\ &= i \pm 2 - i \\ &= \pm 2,\end{aligned}$$

so $\mathbb{Q}(\sqrt{\pm 2}) \subset \mathbb{Q}(\zeta_8)$, and we conclude proposition 3.3.1 is true for $m = 1$.

Before settling the proposition for larger m, we note the following corollary to lemma 3.3.2.

Corollary 3.3.3. *Let $K/\mathbb{Q}$ be an abelian real Galois extension of degree 2^ℓ ramified only at 2. Then $K = \mathbb{Q}$ or $\sqrt{2} \in K$.*

Proof. If $\ell = 0$ we have immediately that $K = \mathbb{Q}$. If ℓ is larger, then $\mathrm{Gal}(K/\mathbb{Q})$ has a subgroup of index 2. The fixed field of this subgroup is a real quadratic field ramified only at 2, hence is equal to $\mathbb{Q}(\sqrt{2})$ by lemma 3.3.2. Therefore $\sqrt{2} \in K$, as desired. □

We now prove proposition 3.3.1 for $m > 1$. Set $M = \mathbb{Q}(\zeta_{2^{m+2}})$ and $L = M^\sigma$, the fixed field of complex conjugation in M. By corollary 2.1.7, we know L is a cyclic extension of degree 2^m. Additionally, since L is fixed by complex conjugation, it is real, so corollary 3.3.3 lets us conclude $\sqrt{2} \in L$.

Let τ be a generator for the cyclic group $\mathrm{Gal}(L/\mathbb{Q})$, and lift to $\tilde{\tau} \in \mathrm{Gal}(KL/Q)$ (recall that $K/\mathbb{Q}$ is an arbitrary abelian extension of degree 2^m ramified only at 2). Let us consider the embedding

$$\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$$

given by restriction. By hypothesis we know $[K : \mathbb{Q}] = 2^m$, and by construction we know $[L : \mathbb{Q}] = 2^m$. So, since $\tilde{\tau}$ restricts to τ, which has order 2^m, on L, we can conclude that the order of $\tilde{\tau}$ is 2^m also.

Now, set $F = (KL)^{\tilde{\tau}}$. By our discussion of order above, we have $[KL : F] = 2^m$. Since τ generates $\mathrm{Gal}(L/\mathbb{Q})$, we have $L^\tau = \mathbb{Q}$, and so $F \cap L = \mathbb{Q}$ because any element of L lying in F is fixed by $\tilde{\tau}$, hence by τ. Furthermore, the embedding of $\mathrm{Gal}(KL/\mathbb{Q})$ above shows $[KL : \mathbb{Q}] = 2^\ell$ for some ℓ, and since only 2 ramifies in K and in L, proposition 2.3.3 lets us conclude that only 2 ramifies in KL, and therefore also in F.

Now set $F_0 = F^\sigma$, the fixed field of F under complex conjugation. We claim $F_0 = \mathbb{Q}$. Indeed, otherwise F_0 would be, by the discussion in the previous paragraph, a real abelian extension of 2-power order ramified only at 2 and not equal to $\mathbb{Q}$. Corollary 3.3.3 would then give $\sqrt{2} \in F_0 \subset F$. The same is true for L, meaning $\sqrt{2} \in F \cap L$. This is a contradiction,

since we showed above that $F \cap L = \mathbb{Q}$. We conclude that $F_0 = \mathbb{Q}$. Our construction of F_0 then tells us

$$[F : F_0] = [F : \mathbb{Q}] \leq 2.$$

If $[F : \mathbb{Q}] = 2$, then F is an imaginary quadratic field ramified only at 2, so $F = \mathbb{Q}(i)$ or $F = \mathbb{Q}(\sqrt{-2})$. In either case, we have seen $F \subset \mathbb{Q}(\zeta_8)$, which is in turn a subfield of $M = \mathbb{Q}(\zeta_{2^{m+2}})$.

Now write

$$2^m = [KL : F] = [KL : \mathbb{Q}]/[F : \mathbb{Q}].$$

If $[F : \mathbb{Q}] = 1$, we find $[KL : \mathbb{Q}] = 2^m = [L : \mathbb{Q}]$, which forces $K \subset L \subset M$, which is what we wanted.

If $[F : \mathbb{Q}] = 2$, then $[KL : \mathbb{Q}] = 2^{m+1}$. Since F is imaginary, we have $F \not\subset L$. But $F \subset KL$, so by degree considerations we get $FL = KL$. But $L = M^\sigma$, so since $F \subset M$ we must also have $FL = M$. This gives us $K \subset KL = M$, finishing the proof.

Recall that at the start of the chapter we mentioned that aside from the classification of degree p extensions ramified only at p, the proofs for the $p = 2$ and p odd cases are similar. Indeed, after classifying these extensions, the remaining argument for p odd is nearly the same; we give it in full after the two classification proofs.

3.4 The Special Case for p Odd, by Kummer Theory

Here we offer a computational proof of what will be referred to as the "key statement" in the proof of Kronecker-Weber:

Proposition 3.4.1. *If p is an odd prime, then there is a unique extension $K/\mathbb{Q}$ of degree p which is ramified only at p, and this K is the unique degree-p subfield of $\mathbb{Q}(\zeta_{p^2})$.*

The proof is taken from the note [5] by Andrei Rapinchuk. It is much more involved than the analogous proof for $p = 2$: where we could handle that case using the discriminant and a small amount of additional legwork, in this case we employ Kummer theory to study a certain radical extension of $\mathbb{Q}(\zeta_p)$ and ultimately calculate discriminants to show the extension is unramified, hence trivial. The proof also relies on the structure of the ring of integers for cyclotomic fields, which we determined in the previous chapter. In particular, we will use the fact that the residue field for a certain ideal of the ring of integers is isomorphic to $\mathbb{F}_p$ to study congruences. We begin with a lemma.

Lemma 3.4.2. *Let p be a prime, and F be a field of characteristic not equal to p. Set $L = F(\zeta_p)$ and $P = L(\sqrt[p]{a})$ for some $a \in L^\times$. Define $\omega : \mathrm{Gal}(L/F) \to (\mathbb{Z}/p\mathbb{Z})^\times$ by mapping $\sigma \in \mathrm{Gal}(L/F)$ to the well-defined class in $(\mathbb{Z}/p\mathbb{Z})^\times$ determined by the equation*

$$\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}.$$

If the extension P/F is abelian, then $\sigma(a)/a^{\omega(\sigma)} \in L^{\times p}$ for all $\sigma \in \mathrm{Gal}(L/F)$.

Proof. If $a \in L^{\times p}$ already, then pulling exponents to the outside shows that $\sigma(a)/a^{\omega(\sigma)} \in^{\times p}$ immediately. Now take $a \notin L^{\times p}$, so that $\mathrm{Gal}(P/L)$ has order p and a generator τ given by

$\tau(\sqrt[p]{a}) = \zeta_p \sqrt[p]{a}$. Take any $\sigma \in \mathrm{Gal}(L/F)$ and any lift $\tilde{\sigma} \in \mathrm{Gal}(P/F)$. Since $\mathrm{Gal}(P/F)$ is abelian, we have

$$\tilde{\sigma}(\tau(\sqrt[p]{a})) = \tilde{\sigma}(\zeta_p \sqrt[p]{a}) = \zeta_p^{\omega(\sigma)} \tilde{\sigma}(\sqrt[p]{a}) = \tau(\tilde{\sigma}(\sqrt[p]{a})).$$

We can apply this chain of equalities to calculate:

$$\begin{aligned} \tau\left(\frac{\tilde{\sigma}(\sqrt[p]{a})}{(\sqrt[p]{a})^{\omega(\sigma)}}\right) &= \frac{\tau(\tilde{\sigma}(\sqrt[p]{a}))}{\tau\left((\sqrt[p]{a})^{\omega(\sigma)}\right)} \\ &= \frac{\zeta_p^{\omega(\sigma)} \tilde{\sigma}(\sqrt[p]{a})}{\zeta_p^{\omega(\sigma)} (\sqrt[p]{a})^{\omega(\sigma)}} \\ &= \frac{\tilde{\sigma}(\sqrt[p]{a})}{(\sqrt[p]{a})^{\omega(\sigma)}}. \end{aligned}$$

Thus τ fixes this element, so it must be an element of $L^\times$. Taking pth powers then shows $\sigma(a)/a^{\omega(\sigma)} \in L^{\times p}$, which is what we wanted. □

We are now prepared to make headway on proving the key statement. Set $L = \mathbb{Q}(\zeta_p)$ and take K as defined at the beginning of the section. Degree considerations then show that $KL = \mathbb{Q}(\zeta_{p^2}) = L(\sqrt[p]{\zeta_p})$. Now let K' be an arbitrary degree-p extension of $\mathbb{Q}$ which is ramified only at p. Then $K'L$ is an abelian extension of L (also of $\mathbb{Q}$) which contains p distinct pth roots of unity, so Kummer theory tells us that $K'L = L(\sqrt[p]{a})$ for some $a \in L^\times$. We will show that $K'L = KL$, proving immediately that $K' = K$ because the degree-p subfield of $KL = \mathbb{Q}(\zeta_{p^2})$ is unique. We start in this direction by using the lemma we just proved to restrict our choices for a.

Recall from section 2.2 that the ring of integers $\mathcal{O}_L$ has only one prime ideal $\mathfrak{p}$ lying above p, and that this prime ideal is generated by $\lambda = 1 - \zeta_p$. Write A for the localization $\mathcal{O}_{L_\mathfrak{p}}$, and recall that A has unique maximal ideal $\mathfrak{m} = \lambda A$ and residue field $\mathbb{Z}/p\mathbb{Z}$. If $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is a generator, then the fact that $K'L/\mathbb{Q}$ is abelian combined with lemma 3.4.2 shows that

$$\frac{\sigma(a)}{a^{\omega(\sigma)}} \in L^{\times p} \quad \Longrightarrow \quad \frac{\sigma(a)}{a} \in a^{\omega(\sigma)-1} L^{\times p}.$$

Since σ generates $\mathrm{Gal}(L/\mathbb{Q})$, we have $\omega(\sigma) \not\equiv 1 \pmod{p}$. This fact combined with the equation above shows that $L(\sqrt[p]{\sigma(a)/a}) = L(\sqrt[p]{a})$. Furthermore, we know σ sends $\mathfrak{p}$ to itself, since

$$\sigma(1 - \zeta_p) = 1 - \zeta_p^{\omega(\sigma)} = (1 - \zeta_p)(1 + \zeta_p + \cdots + \zeta_p^{\omega(\sigma)-1}).$$

From this fact we can conclude that σ fixes A and $\mathfrak{m}$, and thus $\sigma(a)/a \in A^\times$. But ultimately we care about $L(\sqrt[p]{a})$, so this fact combined with the fact that $\sqrt[p]{\sigma(a)/a}$ generates the same extension of L means we can assume without loss of generality that $a \in A^\times$ from the start. Additionally, $\omega(\sigma)$ is prime to p, so we replace a by a^{p-1}; we now have that $a \equiv 1 \pmod{\lambda}$ in A since $A/\mathfrak{m} \cong \mathbb{F}_p$. Recall that $\lambda = 1 - \zeta_p$, so that for any $j \in \mathbb{Z}$ the binomial theorem tells us

$$\zeta_p^j = (1 - \lambda)^j \equiv 1 - j\lambda \pmod{\lambda^2}.$$

It follows that $a \equiv \zeta_p^j \pmod{\lambda^2}$ for some j. Now set $b = \zeta_p^{-j} a$, and note that $b \equiv 1 \pmod{\lambda^2}$. We will be done if we can show $b \in L^{\times p}$, for then we will have $a \in \langle \zeta_p \rangle L^{\times p}$ which

implies $KL = K'L$. Before showing this, we deduce one more fact about b. By definition we have $KL(\sqrt[p]{a}) = KL(\sqrt[p]{b})$; then, since $KL(\sqrt[p]{a})$ is an abelian extension of $\mathbb{Q}$ ramified only at p, the tower law for ramification shows that the same is true of $L(\sqrt[p]{b})/\mathbb{Q}$.

We now finish the proof by showing if $b \in A^\times$ satisfies $b \equiv 1 \pmod{\lambda^2}$ and $L(\sqrt[p]{b})/\mathbb{Q}$ is abelian and ramified only at p, then $b \in L^{\times p}$. If $b = 1$ there is no work to be done, so suppose $b \neq 1$. We claim that

$$b \equiv 1 \pmod{\lambda^p}.$$

To show this, let $\ell \geq 2$ be the largest integer not exceeding p such that $b \equiv 1 \pmod{\lambda^\ell}$. Assume $\ell < p$. We have that

$$b \equiv 1 + s\lambda^\ell \pmod{\lambda^{\ell+1}},$$

for some $s \in \mathbb{Z}$ not divisible by λ. Since $L(\sqrt[p]{b})/\mathbb{Q}$ is an abelian extension, we may apply lemma 3.4.2 to get $\sigma(b) = c^p b^{\omega(\sigma)}$ for some $c \in A^\times$ (rather than $L^\times$, since $\sigma(b)$ and b are elements of $A^\times$). Then $\sigma(c^p) \equiv 1 \equiv c \pmod{\lambda}$, so $c = 1 + d\lambda$ for some $d \in A$. But $pA = \lambda^{p-1}A$, so the binomial theorem ensures $c^p \equiv 1 \pmod{\lambda^p}$.

Since $\ell < p$ and $\sigma(b) = c^p b^{\omega(\sigma)}$, we have $\sigma(b) \equiv b^{\omega(\sigma)} \pmod{\lambda^{\ell+1}}$. Then we can use our congruence for b above to get

$$\begin{aligned}\sigma(b) &\equiv 1 + s\sigma(\lambda)^\ell \pmod{\lambda^{\ell+1}};\\ b^{\omega(\sigma)} &\equiv 1 + \omega(\sigma)s\lambda^\ell \pmod{\lambda^{\ell+1}}.\end{aligned}$$

We may equate these, and since $s \not\equiv 0 \pmod{\lambda}$, we can cancel s on both sides to get $\sigma(\lambda)^\ell \equiv \omega(\sigma)\lambda^\ell \pmod{\lambda^{\ell+1}}$, or

$$\left(\frac{\sigma(\lambda)}{\lambda}\right)^\ell \equiv \omega(\sigma) \pmod{\lambda}.$$

Applying the definitions of σ and λ, and using the geometric series summation formula, we get

$$\frac{\sigma(\sigma)}{\lambda} = \frac{1-\zeta_p^{\omega(\sigma)}}{1-\zeta_p} = 1 + \zeta_p + \cdots + \zeta_p^{\omega(\sigma)-1} \equiv \underbrace{1+1+\cdots+1}_{\omega(\sigma)} \equiv \omega(\sigma) \pmod{\lambda},$$

which gives us $\omega(\sigma)^\ell \equiv \omega(\sigma) \pmod{\lambda}$ when combined with the congruence above. But we assumed $\omega(\sigma)$ had order $p-1$ and that $\ell \geq 2$, so in fact $\ell \geq p$, contradicting our initial assumption that $\ell < p$. It follows that $\ell = p$, so that $b \equiv 1 \pmod{\lambda^p}$.

We are now ready to finish the proof that $b \in L^{\times p}$. Assume for the sake of contradiction that this is not the case. Define

$$\xi = \frac{1-\sqrt[p]{b}}{\lambda} \in L(\sqrt[p]{b}).$$

Then it is quick to see that $L(\xi) = L(\sqrt[p]{b})$, so that this extension has degree p over L. But ξ is also a root of the polynomial

$$f(x) = \left(x - \frac{1}{\lambda}\right)^p + \frac{b}{\lambda^p},$$

which must be the minimal polynomial for ξ since it is monic with degree p. Expanding using the binomial theorem gives

$$f(x) = \frac{b-1}{\lambda^p} + \sum_{i=1}^{p} \left(\frac{-1}{\lambda}\right)^{p-i} \binom{p}{i} x^i.$$

We showed above that $b \equiv 1 \pmod{\lambda^p}$, so the constant term of f is an element of A. Furthermore, in the sum on the right, each term is divisible by p. But we know from our calculation of the ring of integers of $\mathbb{Q}(\zeta_p)$ that $pA = \lambda^{p-1}A$, so in fact the binomial coefficients clear the denominators and we conclude that $f \in A[x]$. This means ξ is integral over A, so $\{1, \xi, \ldots, \xi^{p-1}\}$ is a basis of $L(\sqrt[p]{b})/L$ consisting of elements integral over A. Its discriminant is

$$\pm N_{L(\sqrt[p]{b})/L}(f'(\xi)) = \pm N_{L(\sqrt[p]{b})/L}\left(p\left(\xi - \frac{1}{\lambda}\right)^{p-1}\right) = \pm(p\lambda^{-(p-1)})^p b^{p-1}.$$

We have that $b \in A^\times$ by construction, and again using the fact that $pA = \lambda^{p-1}A$ we see that $p\lambda^{-(p-1)} \in A^\times$ as well. It follows that the discriminant is a unit in A, so that $\mathfrak{m}$ is unramified in $L(\sqrt[p]{b})$. In particular, we have that $L(\sqrt[p]{b})/\mathbb{Q}$ is an abelian extension ramified only at p and in which p is not totally ramified. By proposition 2.3.2, the fixed field M of the corresponding inertia group is a nontrivial extension of $\mathbb{Q}$ which is unramified everywhere, contradicting the Minkowski theorem. We conclude that $b \in L^{\times p}$, completing the proof that the only degree-p extension of $\mathbb{Q}$ ramified only at p is the degree-p subfield of $\mathbb{Q}(\zeta_{p^2})$.

3.5 The Special Case for p Odd, Using the Different

Now that we have seen a computational proof of the key statement, we give a more conceptual proof using the different. We will first show that degree p^2 abelian extensions of $\mathbb{Q}$ which are ramified only at p are cyclic. After doing so, we will be able to prove the key statement again. We will then be able to conclude our proof of the Kronecker-Weber theorem by constructing a cyclotomic field which must contain a given abelian extension of $\mathbb{Q}$ of degree p^m in which only p is ramified.

Note that although the proof to follow may look cleaner somehow than the one above, we still depend in a crucial way on Hermite-Minkowski, so the structure of $\mathbb{Q}$ is doing a lot of work for us.

Before getting to the key statement, we prove the following proposition, which allows us to calculate the different easily and explicitly in the situation of the key statement.

Proposition 3.5.1. *Let $K/\mathbb{Q}$ be a Galois extension of degree p in which no prime $q \neq p$ ramifies. Then p is totally ramified, and*

$$\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}) = \mathfrak{p}^{2(p-1)},$$

where $\mathfrak{p} \subset \mathcal{O}_K$ is the unique prime lying above p.

Proof. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime lying over p. We show first that p is totally ramified, so that this $\mathfrak{p}$ is really unique.

From the theory of lifts of primes in Galois extensions, we know

$$efr = [K : \mathbb{Q}] = p,$$

where e is the ramification index of primes dividing $p\mathcal{O}_K$, the quantity f is the residue field degree over $\mathbb{F}_p$, and r is the number of primes lying over p. This equation implies, in particular, that $e = e(\mathfrak{p}|p)$ is either 1 or p. But e cannot be 1, as otherwise $K/\mathbb{Q}$ is a nontrivial extension with no ramified primes, contradicting Hermite-Minkowski. So $e = p$ and $r = 1$, showing that p is totally ramified and $\mathfrak{p}$ is the unique prime lying over p.

Now pick $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Since p is totally ramified, we can apply part (1) of lemma 2.4.7, which says in this case that $K = \mathbb{Q}(\pi)$. We also know, since $\pi \in \mathcal{O}_K$, that the minimal polynomial $x^p + a_1 x^{p-1} + \cdots + a_p$ has integer coefficients. Then

$$a_i \pi^{p-1} + \cdots + a_p = -\pi^p \in \mathfrak{p}^p,$$

so by part (2) of the same lemma we find that all a_i are even multiples of p.

Now we consider the factorization of $\mathrm{diff}(\mathcal{O}_K|\mathbb{Z})$. By proposition 2.4.4, since p is the only ramified prime and is totally ramified, we see that

$$\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}) = \mathfrak{p}^d$$

for some integer d. The corollary to Hilbert's formula shows that in fact d is a multiple of $p - 1$, and part (1) of theorem 2.4.8 shows that $d = v_{\mathfrak{p}}(f'(\pi))$. Write

$$f'(\pi) = b_0 + b_1 + \cdots + b_{p-1},$$

where $b_0 = p\pi^{p-1}$ and $b_i = a_i(p-i)\pi^{p-i-1}$ for all $i > 0$. Additionally, since $p\mathcal{O}_K = \mathfrak{p}^p$, we see that $p \mid v_{\mathfrak{p}}(k)$ whenever $k \in \mathbb{Q}^\times$.

Now, if $v_{\mathfrak{p}}(b_i) = v_{\mathfrak{p}}(b_j)$ for some $i \neq j$, we have

$$v_{\mathfrak{p}}(a_i a_j^{-1}(p-i)(p-j)^{-1}) = v_{\mathfrak{p}}(\pi^{j-i}) = j - i.$$

But the left-hand side is a multiple of p, while the right-hand side is not. We conclude that the $v_{\mathfrak{p}}(b_i)$ are pairwise distinct, so we can apply lemma 2.4.5 to get

$$v_{\mathfrak{p}}(b_0 + \cdots + b_{p-1}) = v_{\mathfrak{p}}(f'(\pi)) = \min_i(v_{\mathfrak{p}}(b_i)).$$

To bound this minimum, note that $v_{\mathfrak{p}}(b_0) = 2p - 1$ and $v_{\mathfrak{p}}(b_i) \geq p$ for all $i > 0$ since the a_i are all divisible by p. Combining the information we have collected, we see that $v_{\mathfrak{p}}(f'(\pi))$ is a multiple of $p - 1$ satisfying

$$p \leq v_{\mathfrak{p}}(f'(\pi)) \leq 2p - 1,$$

hence equals $2(p-1)$ as desired. □

Next we analyze the structure of degree p^2 abelian extensions ramified only at p.

Proposition 3.5.2. *Suppose $K/\mathbb{Q}$ is a degree p^2 abelian extension which is ramified only at p. Then the extension is cyclic.*

Proof. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic either to $\mathbb{Z}/p^2\mathbb{Z}$ or to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, so to show it is cyclic it is enough to prove there is only one degree p intermediate field for $K/\mathbb{Q}$.

Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime lying above p. By proposition 2.3.2, we have that p is unramified in the fixed field K^{G_0}. Then no primes ramify in this fixed field, so it is in fact equal to $\mathbb{Q}$ and we conclude $\mathrm{Gal}(K/\mathbb{Q}) = G_0$. Part (2) of proposition 2.3.4 lets us conclude that $\mathrm{Gal}(K/\mathbb{Q}) = G_1$ as well, since the embedding of G_0/G_1 into $\mathbb{F}_p^\times$ must be trivial by order considerations.

The ramification index $e(\mathfrak{p}|p) = |G_0| = p^2$, so p is totally ramified and the residue field for $\mathfrak{p}$ is $\mathbb{F}_p$. Pick an integer r such that $|G_{r-1}| = p^2$ but $|G_r| < p^2$. By part (3) of proposition 2.3.4, we find that G_{r-1}/G_r embeds into the additive group of $\mathbb{F}_p$. So G_r cannot be trivial, as otherwise we would have an embedding of a group of order p^2 into one of order p. It follows that $|G_r| = p$.

Now fix some order p subgroup of $\mathrm{Gal}\, K/\mathbb{Q}$ and let $M = K^H$ be the corresponding fixed field. The tower law for the different tells us that

$$\mathrm{diff}(\mathcal{O}_K|\mathbb{Z}) = \mathrm{diff}(\mathcal{O}_K|\mathcal{O}_M)\mathrm{diff}(\mathcal{O}_M|\mathbb{Z}).$$

Applying proposition 3.5.1 shows that for any choice of M we have $\mathrm{diff}(\mathcal{O}_M|\mathbb{Z}) = \mathfrak{p}^{2(p-1)}$. In particular, the value $v_\mathfrak{p}(\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_M))$ does not depend on M, so if $K_r = K^{G_r}$ we have

$$v_\mathfrak{p}(\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_M)) = v_\mathfrak{p}(\mathrm{diff}(\mathcal{O}_K|\mathcal{O}_{L_r})),$$

which implies $L_r = M$ by proposition 2.4.10. We conclude that L_r is the only degree p subfield of $K/\mathbb{Q}$, so the extension is cyclic, as desired. □

Finally, we can prove the key statement (again):

Corollary 3.5.3. *There is a unique extension $K/\mathbb{Q}$ of degree p in which only p is ramified, and this extension is the degree p subfield of $\mathbb{Q}(\zeta_{p^2})$.*

Proof. We prove uniqueness first. Suppose $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ are two extensions satisfying the hypotheses of the corollary. If $K_1 \neq K_2$, then the embedding of the Galois group of a compositum along with the tower law for ramification shows that K_1K_2 has degree p^2 over $\mathbb{Q}$, is ramified only at p, but is not cyclic. This contradicts proposition 3.5.2, so $K_1 = K_2$. To see that such an extension exists, note that since $[\mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}] = p(p-1)$, the field $\mathbb{Q}(\zeta_{p^2})$ has a unique degree p subfield. Since p is the only prime ramified in $\mathbb{Q}(\zeta_{p^2})$, it is the only prime ramified in this subfield, showing that this subfield satisfies the conditions we want. □

We end by using the key statement to prove Kronecker-Weber for p odd, completing the proof of the theorem.

Proposition 3.5.4. *Let $K/\mathbb{Q}$ be a degree p^m abelian extension in which only p is ramified. Then $K \subset \mathbb{Q}(\zeta_{p^{m+1}})$.*

Proof. By proposition 2.1.6, the extension $\mathbb{Q}(\zeta_{p^{m+1}})/\mathbb{Q}$ is a cyclic Galois extension of degree $p^m(p-1)$, hence has a unique subfield L of degree p^m. Since $\mathbb{Q}(\zeta_{p^{m+1}})$ is ramified only at p, the same is true of L. Arguing as we did for $p = 2$ (see the proof of proposition 3.3.1), we find that if $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ is a generator, then any lift $\tilde{\tau} \in \mathrm{Gal}(KL/\mathbb{Q})$ has order p^m.

Writing $F = (KL)^{\tilde{\tau}}$, we then have $[KL : F] = p^m$. Since τ is a generator for $\mathrm{Gal}(L/\mathbb{Q})$, any element of L fixed by $\tilde{\tau}$ is rational, so $F \cap L = \mathbb{Q}$. In fact, we have even that $F = \mathbb{Q}$. Indeed, otherwise $F/\mathbb{Q}$ would be a nontrivial abelian extension of p-power order ramified only at p, hence would contain a degree p subfield F_0 ramified only at p. But L contains such a subfield L_0 as well, and by corollary 3.5.3 we see that $F_0 = L_0$ so that $F \cap L \supset L_0 \supsetneq \mathbb{Q}$, a contradiction. We conclude that

$$[KL : \mathbb{Q}] = p^m = [L : \mathbb{Q}],$$

proving $K \subset L \subset \mathbb{Q}(\zeta_{p^{m+1}})$, as desired. □

Chapter 4

Kronecker-Weber in Context

Now that we have shown every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field, one might ask, as Hilbert did in the twelfth of this twenty-three problems in 1900: is there an analogous construction for abelian extensions of a general number field K? Can we find explicit generators which play the role of roots of unity? This question is much more difficult, and in proving Kronecker-Weber we have already seen some of the reason for this. Namely, our strategy revolved around controlling ramification, which always occurs for nontrivial extensions of $\mathbb{Q}$ by the Minkowski theorem. Moving up even to quadratic fields, we no longer have guaranteed ramification. For example:

Example 4.0.1. Let $K = \mathbb{Q}(\sqrt{-5})$. Then the extension $K(\sqrt{5})/K$ is unramified at all primes.

Kronecker made it the dream of his youth (*liebster Jugendtraum*) to extend his result over $\mathbb{Q}$, giving explicit generators for abelian extensions, to imaginary quadratic fields. His dream was realized in the theory of elliptic curves with complex multiplication. The idea is as follows. If K is an imaginary quadratic field, we can consider its ring of integers $\mathcal{O}_K$ and its ideals as lattices in $\mathbb{C}$. Lattices in $\mathbb{C}$ are associated to the cubic curves known as elliptic curves through the Weierstrass $\wp$ function which can be defined on the lattice. In particular, the $\wp$ function $\wp(z;\Lambda)$ for the lattice Λ is related to its derivative by the equation

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 - g_2\wp(z;\Lambda) - g_3,$$

where g_2, g_3 are constants which depend on the lattice. When the endomorphism ring of the curve given by this equation is isomorphic to $\mathcal{O}_K$, we can use the curve to construct the maximal abelian extension of K by adjoining special values of functions. Namely, we adjoin the "j-invariant" of the curve, as well as values of the $\wp$ function at torsion points with respect to the addition law which can be defined on the curve (adjusted to be invariant under isomorphism). Thus, we see here that in the imaginary quadratic case we are also able to find explicit generators for abelian extensions. Beyond this, there are conjectures such as those of Stark, but there is still much to discover.

Bibliography

[1] Keith Conrad. *The Different Ideal*. URL: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf`.

[2] David Cox. *Galois Theory*. Pure and Applied Mathematics. Wiley, 2004.

[3] Gerald Janusz. *Algebraic Number Fields*. 2nd ed. Graduate Studies in Mathematics, vol. 7. American Mathematical Society, 1996.

[4] Serge Lang. *Algebra*. 3rd ed. Graduate Texts in Mathematics 211. Springer-Verlag, 2002.

[5] Andrei Rapinchuk. *Proof of Key Statement for p Odd*.

[6] Igor Rapinchuk. *A Proof of the Kronecker-Weber Theorem*.

[7] Pierre Samuel. *Algebraic Theory of Numbers*. Hermann, 1970.