

ABELIAN EXTENSIONS OF \mathbb{Q}

by

Jason W. Elliot

Bachelor of Science, University of Colorado at Denver, 2002

A thesis submitted to the
University of Colorado at Denver
in partial fulfillment
of the requirements for the degree of
Master of Science
Applied Mathematics
2005

This thesis for the Master of Science

degree by

Jason W. Elliot

has been approved

by

Stan Payne

Bill Cherowitzo

Rich Lundgren

Date

Elliot, Jason W. (M.S., Applied Mathematics)

Abelian Extensions of \mathbb{Q}

Thesis directed by Professor Stan Payne

ABSTRACT

Our main aim in this paper is to prove the theorem of Kronecker and Weber, which states the following:

If K is a finite abelian extension of \mathbb{Q} then K is contained in a cyclotomic extension of \mathbb{Q} .

In our proof of this theorem we avoid the theory of localization, which is used in all proofs that this author has read.

Our proof requires theory of integral extensions of Dedekind domains, which we develop to some extent here. Some familiarity of this subject is assumed of the reader. Likewise, we develop some theory of algebraic numbers in Galois extensions.

In Chapter 3, we state many results from modern algebra that find an application in our investigations. This is meant as a reminder, or might serve as reference. The reader is assumed to have an acquaintance with basic modern algebra, including Galois theory. We state some relevant theorems from group theory and theory of Cyclotomic fields in Chapters 4 and 5, respectively.

This abstract accurately represents the content of the candidate's thesis. I recommend its publication.

Signed _____
Stan Payne

DEDICATION

I dedicate this thesis to Jennifer Hiromi Nakasone, my fiancé, soon to be my wife.

ACKNOWLEDGMENT

I would like to thank Bill Cherowitzo, Rich Lundgren, and Stan Payne, for teaching me most of the mathematics upon which this thesis is based and for encouraging me to write this thesis.

CONTENTS

Figures	x
Tables	xi
<u>Chapter</u>	
1. Introduction	1
2. Conventions	2
3. Rings and Fields	3
3.1 Quotient Fields	3
3.2 Ideals	4
3.3 Modules	6
3.4 Primes and Maximal Ideals	7
3.5 Integral Extensions	8
3.6 Residue Class Fields	10
3.6.1 Residue Class Vector Space	10
3.7 Fractional Ideals	10
3.8 Invertible Ideals	11
3.9 Field Extensions	13
3.10 Number Fields and Number Rings	15
4. Some Theorems on Abelian Groups	17
4.0.1 p -groups	17
4.1 Abelian Field Extensions	19

5. Cyclotomic Extensions	21
5.1 Roots of Unity	22
5.2 Cyclotomic Field Extensions	23
6. Trace, Norm, and Discriminant	25
6.1 The Discriminant	26
6.2 Quadratic Extensions of \mathbb{Q}	27
6.3 Cyclotomic Extensions of \mathbb{Q}	28
7. Dedekind Domains	29
7.1 Noether's Classification	30
7.2 Ideals	33
7.3 Ramification Index	35
7.4 Residue Class Fields and Inertial Degree	36
7.4.1 Norm for Ideals	38
7.5 Cyclotomic Extensions of \mathbb{Q}	39
8. The Different	40
8.1 Dual Basis	41
9. Galois Extensions	43
9.1 Subgroups of the Galois Group	44
9.1.1 The Decomposition Group	45
9.1.2 The Inertia Group	46
9.1.3 The Ramification Groups	48
9.2 The Frobenius Automorphism in the Classical Case	50
9.3 Embedding $\mathcal{E}/\mathcal{V}_1 \hookrightarrow (\mathfrak{d}/\mathfrak{p})^\times$	51
9.3.1 A Better Result for Abelian Extensions in the Classical Case	53

9.4	Embedding $\mathcal{V}_{m-1}/\mathcal{V}_m \hookrightarrow \mathfrak{D}/\mathfrak{P}$	56
9.5	Hilbert's Formula for Totally Ramified Primes in the Classical Case	58
10.	Abelian Extensions and the Kronecker-Weber Theorem	60
10.1	Reduction to Prime Power Degree	60
10.2	Reduction to One (Particular) Ramified Prime	61
10.3	The Case for 2	64
10.4	The Case When p is Odd and $m = 1$	67
10.4.1	The Case p is odd and $m = 2$	69
10.4.2	Back to $m = 1$	70
10.5	The Case p is odd and $m > 1$	71
	<u>Appendix</u>	
A.	Notation	72
B.	The Minkowski Bound	74
	<u>References</u>	76

FIGURES

Figure

4.1	The prime power decomposition of abelian extensions	20
10.1	The behavior of $q \neq p$	62

TABLES

Table

9.1 Decomposition and Inertia Fields: Ramification and Inertial Degrees 48

1. Introduction

In 1853, Kronecker stated the theorem now known as the “Kronecker-Weber Theorem,” but his proof was incomplete – there were difficulties with extensions of degree a power of 2. Weber gave a proof in 1886, but even his proof contained a gap. Both of these early proofs used theory of Lagrange resolvents. In 1896, Hilbert gave a correct proof using analysis of ramification groups. [20]

Most modern proofs of the Kronecker-Weber Theorem use local techniques, theory of p -adic numbers, and theory of valuations. We avoid all of these subjects entirely, and, following exercises in [10], we give a proof that, according to Milne [12], is likely similar to Hilbert’s.

According to the theorem, finite abelian extensions of \mathbb{Q} are, in a sense, generated by the function $e^{2\pi i X}$ at rational values of X . Kronecker’s hope was that finite abelian extensions of an arbitrary number field could be generated in the same sense by a set of analytic functions at algebraic values. It turns out that the abelian extensions of imaginary quadratic fields are generated by certain values of elliptic functions. [14] The area that studies abelian extensions of general number fields is known as “class field theory.” Kronecker’s hope has inspired much research in this area. Naturally, the first questions in class field theory concern how to describe the abelian extensions of \mathbb{Q} . Our investigation therefore lies at the beginning of class field theory.

2. Conventions

As usual, \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} respectively denote nonnegative integers, integers, rationals, reals, and complex numbers.

The following few paragraphs are an attempt to prepare the reader, but they are nothing necessary. In this thesis, we make systematic use of fonts to help remind the reader what symbols represent.

We reserve German letters for modules. Of course, rings and ideals are modules, and we use the German letters for them, too. Fields are denoted with letters such as k, F, K, L, M, N, T . A lower case letter in ordinary font indicates a rational integer: p, q, r, e, f, g , etc. Groups are denoted with letters such as $\mathcal{D}, \mathcal{E}, \mathcal{G}, \mathcal{H}, \mathcal{V}$. For polynomials we use script \mathcal{F}, \mathcal{G} , except in the case of the minimal polynomial $M_{\alpha, k}(X)$. Normal text font is generally reserved for certain special objects, such as the trace Tr , norm N , discriminant Disc , different Diff , and minimal polynomial M . These are all listed in Appendix A. Lower-case Greek letters are generally used for elements of some algebraic structure more general than \mathbb{Z} , for example a group, ring, or field. Special symbols are listed in the first appendix under the title “Notation.” We reserve the slash $/$ for quotients and use the vertical bar $|$ for extensions.

3. Rings and Fields

In general, a ring need not have commutative multiplication nor have multiplicative identity. In this thesis, however, we assume tacitly that all rings are commutative with nonzero identity. In addition, we assume that any ring homomorphism preserves the identity. In particular, if one ring contains another, then their identities coincide. We refer to a ring having no zero divisors as a *domain*, and a ring with the unique factorization property as *factorial*.

3.1 Quotient Fields

Proposition 3.1 *If \mathfrak{r} is a domain, then \mathfrak{r} can be embedded into a field.*

Proof: We consider ordered pairs $(\alpha, \beta) \in \mathfrak{r} \times \mathfrak{r}$ such that $\beta \neq 0$, under the relation

$$(\alpha, \beta) \sim (\gamma, \delta) \iff \alpha\delta = \beta\gamma.$$

This defines an equivalence relation. We use $(\alpha : \beta)$ to indicate the equivalence class containing (α, β) . We define

$$(\alpha : \beta) \cdot (\gamma : \delta) = (\alpha\gamma : \beta\delta)$$

and

$$(\alpha : \beta) + (\gamma : \delta) = (\alpha\delta + \beta\gamma : \beta\delta).$$

It is not hard to show that these definitions are natural, and that under these two operations our set is a field. By identifying $\alpha \in \mathfrak{r}$ with $(\alpha : 1) \in \mathfrak{k}$, we see

that \mathfrak{r} is contained in this field. For more details, we refer the reader to [18, p. 41]. ■

It is not hard to see that any field containing \mathfrak{r} must contain a field isomorphic to the field constructed in the proof of Proposition 3.1. In this sense, this field is the smallest field containing \mathfrak{r} , and we refer to it as the **quotient field** of \mathfrak{r} .

Proposition 3.2 *For each $\alpha \in \mathfrak{k}$ there is nonzero $\rho \in \mathfrak{r}$ such that $\rho\alpha \in \mathfrak{r}$.*

Proof: Assume $\alpha = (\alpha_1 : \alpha_2)$ with $\alpha_1, \alpha_2 \in \mathfrak{r}$, $\alpha_2 \neq 0$. Then $\alpha_2\alpha = (\alpha_2\alpha_1 : \alpha_2) = (\alpha_1 : 1) \in \mathfrak{r}$. ■

An application of this result is the following:

Corollary 3.3 *If \mathfrak{d} is a domain with quotient field \mathfrak{k} , then given a polynomial over \mathfrak{k} there is a polynomial over \mathfrak{d} of the same degree with precisely the same roots.*

3.2 Ideals

An **ideal** is a subring that is stable under the action of multiplication. If \mathfrak{a} and \mathfrak{b} are two ideals, then their product $\mathfrak{a}\mathfrak{b}$ is defined to be the smallest ideal containing all products $\alpha\beta$ with $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$. Equivalently, this is the set of all finite sums $\sum_i \alpha_i\beta_i$ such that $\alpha_i \in \mathfrak{a}$, $\beta_i \in \mathfrak{b}$, and $k \in \mathbb{N}$. Commutativity for ideals is inherited from commutativity in the ring.

Let \mathfrak{J} be an ideal in \mathfrak{r} . If there is a set S such that every element of \mathfrak{J} can be expressed as a finite sum $\sum \sigma_i\rho_i$ with $\sigma_i \in S$ and $\rho_i \in \mathfrak{r}$, then \mathfrak{J} is said to be **generated by** S . In this case we write $\mathfrak{J} = \langle S \rangle$. If S is any set of elements

from the ring \mathfrak{r} , then there is a smallest ideal containing S , which is necessarily generated by S . If the cardinality of S is finite, then $\langle S \rangle$ is said to be ***finitely generated***. If \mathfrak{r} is a subring of \mathfrak{R} and S is a set of elements of \mathfrak{r} , then the notation $\langle S \rangle$ can be ambiguous, and we use the notation $\langle S \rangle_{\mathfrak{r}}$ and $\langle S \rangle_{\mathfrak{R}}$ to denote the ideal generated by S in \mathfrak{r} , and the ideal generated by S in \mathfrak{R} , respectively.

A ***principal ideal*** is an ideal generated by a single element. In a commutative ring with identity, a principal ideal is the set of multiples of its generator. That is, $\langle \alpha \rangle = \mathfrak{r}\alpha$. A ring in which all ideals are principal is itself called ***principal***.

Following the categorical meaning, an ideal \mathfrak{a} is said to ***divide*** another ideal \mathfrak{b} provided that there is an ideal \mathfrak{d} such that $\mathfrak{d}\mathfrak{a} = \mathfrak{b}$. It should be clear that if \mathfrak{a} and \mathfrak{b} are two ideals with \mathfrak{a} dividing \mathfrak{b} , then $\mathfrak{a} \supseteq \mathfrak{b}$. We shall see later when the converse is true.

Assume that \mathfrak{a} and \mathfrak{b} are ideals of the domain \mathfrak{d} . As with rational integers, we say that \mathfrak{a}^x is an ***exact divisor*** of \mathfrak{b} if $\mathfrak{a}^x | \mathfrak{b}$, but $\mathfrak{a}^{x+1} \nmid \mathfrak{b}$. Of course, if $\mathfrak{a}^{x+1} \nmid \mathfrak{b}$, then neither does \mathfrak{a}^{x+2} , etc. As with rational integers, we express this as $\mathfrak{a}^x || \mathfrak{b}$.

If \mathfrak{a} and \mathfrak{b} are two ideals in the same ring \mathfrak{r} , then we define $\mathfrak{a} + \mathfrak{b}$ to be the set of sums $\alpha + \beta$ with $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$.

Proposition 3.4 *The ideal $\mathfrak{a} + \mathfrak{b}$ is the smallest ideal containing \mathfrak{a} and \mathfrak{b} . In symbols, $\mathfrak{a} + \mathfrak{b} = \langle \mathfrak{a}, \mathfrak{b} \rangle$.*

Proof: If \mathfrak{J} is an ideal containing \mathfrak{a} and \mathfrak{b} , then \mathfrak{J} must contain sums $\alpha + \beta$ with $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$. Moreover, $\mathfrak{a} + \mathfrak{b}$ clearly contains \mathfrak{a} and \mathfrak{b} . ■

3.3 Modules

If \mathfrak{r} is a ring, then an \mathfrak{r} -*module* is an abelian group \mathfrak{M} together with an action on it by \mathfrak{r} , that is, a ring homomorphism into the ring $\text{End}\mathfrak{M}$ of endomorphisms of \mathfrak{M} . We refer the reader to [5, p. 169] for more details. If \mathfrak{M} is an \mathfrak{r} -module, then we say \mathfrak{M} is a *module over* \mathfrak{r} .

If \mathfrak{r} is a subring of the ring \mathfrak{R} , then \mathfrak{R} is automatically an \mathfrak{r} -module; hence, the quotient field of \mathfrak{r} is an \mathfrak{r} -module. If \mathfrak{m} is a subring of \mathfrak{r} , we see that \mathfrak{m} is an \mathfrak{r} -module iff $\mathfrak{r}\mathfrak{m} = \mathfrak{m}$. Thus, we notice that ideals are precisely modules that are subrings.

The *rank* of a module is the maximum number of linearly independent elements and a *basis* is a maximal set of linearly independent elements. An \mathfrak{r} -module is said to be *free* if it is isomorphic to $\bigoplus_{\iota \in I} \mathfrak{r}$ for some set I . The free module $\bigoplus_{\iota \in I} \mathfrak{r}$ has rank $\#I$, and consists of a basis of generators with the same cardinality as I . See [3, pp. 439, 448], [9, p. 135], or [5, p. 181].

If \mathfrak{k} is a field, then a \mathfrak{k} -module is a \mathfrak{k} -*vector space* or a *vector space over* \mathfrak{k} , and its rank is referred to as its *dimension*. For a \mathfrak{k} -vector space \mathcal{V} , the collection of all \mathfrak{k} -linear maps from \mathcal{V} to \mathfrak{k} is itself a \mathfrak{k} -vector space, which is denoted by \mathcal{V}' and called the *dual space* of \mathcal{V} . If \mathcal{V} is finite dimensional, then $\dim \mathcal{V} = \dim \mathcal{V}'$. See [3, p. 412] or [9, p. 142].

Proposition 3.5 *Let \mathfrak{r} be a domain, \mathfrak{k} its quotient field. If \mathfrak{M} is a free \mathfrak{r} -module of rank n , then there is a \mathfrak{k} -vector space \mathcal{V} of dimension n containing \mathfrak{M} .*

Proof: Consider the \mathfrak{k} -span of \mathfrak{M} . See [15, pp. 107, 108] for the details. ■

Theorem 3.6 *Let \mathfrak{r} be a domain and suppose that \mathfrak{M} is a free \mathfrak{r} -module of rank*

n . Then any two bases of \mathfrak{M} have n elements.

Proof: See [15, pp. 107, 108]. ■

A module is said to be *torsion free* provided that there are no torsion elements, that is, if $\mu\rho = 0$ then either $\mu = 0$ or $\rho = 0$.

Proposition 3.7 *A finitely generated module over a principal domain is torsion free iff it is free.*

Proof: See [3, p. 442]. ■

3.4 Primes and Maximal Ideals

An ideal is maximal iff it is not properly contained in any proper ideal. Equivalently, the factor ring is a field; see [9, p. 93].

An ideal \mathfrak{P} is a *prime ideal* provided that whenever the product $\alpha\beta$ is in \mathfrak{P} either $\alpha \in \mathfrak{P}$ or $\beta \in \mathfrak{P}$; equivalently, $\mathfrak{R}/\mathfrak{P}$ is a domain. We shall refer to a prime ideal of \mathfrak{r} as a *prime* of \mathfrak{r} . When primes in \mathbb{Z} enter into our discussions, we refer to them as *rational primes* to distinguish them. Prime ideals in \mathbb{Z} are precisely those generated by rational primes, and it is often easier to refer to a rational prime than the prime ideal that it generates. Since fields are domains,

Proposition 3.8 *every maximal ideal is prime.*

Proof: For a direct proof, see [9, p. 92]. ■

Suppose \mathfrak{R} is a ring with subring \mathfrak{r} . Let \mathfrak{p} be a prime ideal of \mathfrak{r} . If \mathfrak{P} is a prime ideal of \mathfrak{R} such that $\mathfrak{P} \cap \mathfrak{r} = \mathfrak{p}$, then we say \mathfrak{P} *lies above* \mathfrak{p} or \mathfrak{p} *lies below* \mathfrak{P} . We write $\mathfrak{P}|\mathfrak{p}$ to refer to this relationship. When this is the case, the injection

$$\mathfrak{r} \hookrightarrow \mathfrak{R}$$

induces an injection

$$\mathfrak{r}/\mathfrak{p} \rightarrow \mathfrak{R}/\mathfrak{P}$$

of the factor rings, and gives the commutative diagram

$$\begin{array}{ccc} \mathfrak{r} & \longrightarrow & \mathfrak{r}/\mathfrak{p} \\ \downarrow & & \downarrow \\ \mathfrak{R} & \longrightarrow & \mathfrak{R}/\mathfrak{P} \end{array}$$

with all maps being the obvious ones. See also [8, p. 8].

3.5 Integral Extensions

Good treatments of this subject are given in [8, p. 4], [9, p. 333], and [11, p. 64].

If \mathfrak{A} is a ring contained in a ring \mathfrak{B} , then an element $\beta \in \mathfrak{B}$ is said to be *integral* over \mathfrak{A} if β is a root of a monic polynomial with coefficients in \mathfrak{A} . In other words, there is a relation of the form $\beta^n + \alpha_{n-1}\beta^{n-1} + \dots + \alpha_0 = 0$ with $\alpha_i \in \mathfrak{A}$. A relation such as this makes the \mathfrak{A} -module $\mathfrak{A}[\beta]$ finitely generated. Since the powers of β form a basis of $\mathfrak{A}[\beta]$ over \mathfrak{A} , the converse is also true:

The element $\beta \in \mathfrak{B}$ is integral over \mathfrak{A} iff $\mathfrak{A}[\beta]$ is finitely generated over \mathfrak{A} .

If every element of \mathfrak{B} is integral over \mathfrak{A} then we say that \mathfrak{B} is integral over \mathfrak{A} .

The property of integrality is transitive:

Proposition 3.9 *Assume $\mathfrak{A} \subseteq \mathfrak{B} \subseteq \mathfrak{C}$ is a tower of rings. If \mathfrak{C} is integral over \mathfrak{B} and \mathfrak{B} is integral over \mathfrak{A} , then \mathfrak{C} is integral over \mathfrak{A} .*

Proof: See [8, p. 5]. ■

Also, integrality is invariant under homomorphism:

Proposition 3.10 *If \mathfrak{R} is a ring that is integral over a subring \mathfrak{r} , and σ is a homomorphism of \mathfrak{R} , then $\sigma\mathfrak{R}$ is integral over $\sigma\mathfrak{r}$.*

Proof: Apply σ to any integral equation over \mathfrak{r} and it will be an integral equation over $\sigma\mathfrak{r}$. See [8, p. 5]. ■

Consequently, if \mathfrak{R} is integral over \mathfrak{r} , and \mathfrak{P} is a prime of \mathfrak{R} lying above the prime \mathfrak{p} of \mathfrak{r} , then $\mathfrak{R}/\mathfrak{P}$ is integral over $\mathfrak{r}/\mathfrak{p}$.

If \mathfrak{r} is a subring of \mathfrak{R} , then the set of all elements of \mathfrak{R} that are integral over \mathfrak{r} is a subring of \mathfrak{R} , and is called the *integral closure* of \mathfrak{r} in \mathfrak{R} . If every element in \mathfrak{R} that is integral over \mathfrak{r} is actually in \mathfrak{r} , then \mathfrak{r} is said to be *integrally closed* in \mathfrak{R} , or in some literature *normal* in \mathfrak{R} . If \mathfrak{r} is integrally closed in its field of fractions then we merely say that \mathfrak{r} is *integrally closed*.

Proposition 3.11 *Assume \mathfrak{r} is integrally closed in its quotient field k , and let $E|k$ be a separable extension of degree n . Let \mathfrak{R} be the integral closure of \mathfrak{r} in E . Then there exist free \mathfrak{r} -modules \mathfrak{M} and \mathfrak{M}' of rank n such that $\mathfrak{M}' \subseteq \mathfrak{R} \subseteq \mathfrak{M}$.*

Proof: See [15, p. 108]. ■

Consequently, in the setting of Proposition 3.11, \mathfrak{R} is an \mathfrak{r} -module of rank n , generated by n elements. Now, any field containing \mathfrak{R} must contain \mathfrak{M}' and k . Using the construction in Proposition 3.5, dimension considerations (over k) yield that the quotient field of \mathfrak{R} is E .

Proposition 3.12 *Assume \mathfrak{r} is a ring and \mathfrak{R} is a ring integral over \mathfrak{r} . Let \mathfrak{P} be a prime ideal of \mathfrak{R} lying above the prime \mathfrak{p} of \mathfrak{r} . Then \mathfrak{P} is maximal if and only if \mathfrak{p} is maximal.*

Proof: See [8, p. 10]. ■

3.6 Residue Class Fields

Assume that \mathfrak{d} is a domain and that \mathfrak{D} is a domain integral over \mathfrak{d} . If \mathfrak{P} is maximal, then of course \mathfrak{P} is prime. Assume further that \mathfrak{P} lies above the prime \mathfrak{p} of \mathfrak{d} . Then, by Proposition 3.12, \mathfrak{p} is maximal, and both $\mathfrak{D}/\mathfrak{P}$ and $\mathfrak{d}/\mathfrak{p}$ are fields. In this case, the restriction of the (canonical) epimorphism $\mathfrak{D} \rightarrow \mathfrak{D}/\mathfrak{P}$ to the subring \mathfrak{d} induces an homomorphism $\mathfrak{d} \rightarrow \mathfrak{D}/\mathfrak{P}$ whose kernel is $\mathfrak{d} \cap \mathfrak{P}$. By assumption, this intersection is \mathfrak{p} , so that we have an embedding $\mathfrak{d}/\mathfrak{p} \hookrightarrow \mathfrak{D}/\mathfrak{P}$. Thus, the field $\mathfrak{D}/\mathfrak{P}$ may be regarded as an extension of $\mathfrak{d}/\mathfrak{p}$.

3.6.1 Residue Class Vector Space

The natural map $\mathfrak{D} \rightarrow \mathfrak{D}/\langle \mathfrak{p} \rangle_{\mathfrak{D}}$ induces a map $\mathfrak{d} \rightarrow \mathfrak{D}/\langle \mathfrak{p} \rangle_{\mathfrak{D}}$ having kernel $\langle \mathfrak{p} \rangle_{\mathfrak{D}} \cap \mathfrak{d} = \mathfrak{p}$. Hence, there is an embedding $\mathfrak{d}/\mathfrak{p} \hookrightarrow \mathfrak{D}/\langle \mathfrak{p} \rangle_{\mathfrak{D}}$. Up to isomorphism, therefore, we may regard $\mathfrak{d}/\mathfrak{p}$ as a subring of $\mathfrak{D}/\langle \mathfrak{p} \rangle_{\mathfrak{D}}$. As such, $\mathfrak{D}/\langle \mathfrak{p} \rangle_{\mathfrak{D}}$ is a module over $\mathfrak{d}/\mathfrak{p}$, and since $\mathfrak{d}/\mathfrak{p}$ is a field, this module is a vector space. A set S of elements from \mathfrak{D} is said to be *independent modulo \mathfrak{p}* (or mod \mathfrak{p}) if the set of residue classes of the elements of S is linearly independent in this vector space.

3.7 Fractional Ideals

Much of this section and the next follows [21, V, §6].

If \mathfrak{d} is a domain, then we consider a submodule \mathfrak{f} of the quotient field of \mathfrak{d} a *fractional ideal* provided that there is $\gamma \in \mathfrak{d}$ such that $\gamma\mathfrak{f} \subset \mathfrak{d}$. In this case, it is easy to verify that $\gamma\mathfrak{f}$ is an ideal of \mathfrak{d} , and hence fractional ideals are precisely \mathfrak{d} -modules of the form $\gamma^{-1}\mathfrak{J}$ where \mathfrak{J} is an ideal of \mathfrak{d} and $\gamma \in \mathfrak{d}$. In this case,

notice that if \mathfrak{f} is a fractional ideal of \mathfrak{d} , then $\mathfrak{f}\mathfrak{d} = \gamma^{-1}\mathfrak{J}\mathfrak{d} = \gamma^{-1}\mathfrak{J} = \mathfrak{f}$. With $\gamma = 1$, we see that ideals are fractional ideals.

It will sometimes be simpler to refer to fractional ideals simply as ideals. To distinguish ideals from fractional ideals, we refer to them as *integral ideals*.

We extend the definition of “divide” to fractional ideals. An ideal \mathfrak{f} is said to *divide* another ideal \mathfrak{k} provided that there is an integral ideal \mathfrak{a} such that $\mathfrak{f}\mathfrak{a} = \mathfrak{k}$.

We also notice that finitely generated submodules of the quotient field are fractional ideals. If $\{\beta_i\}$ are generators of the module \mathfrak{M} , then find $\{\mu_i\} \subseteq \mathfrak{d}$ such that $\mu_i\beta_i \in \mathfrak{d}$. Then $(\prod \mu_i)\mathfrak{M} \subseteq \mathfrak{d}$.

For a pair of ideals $\mathfrak{b}, \mathfrak{b}'$ we adopt the following notation:

$$(\mathfrak{b} : \mathfrak{b}') = \{\alpha \in \mathfrak{k} : \alpha\mathfrak{b}' \subseteq \mathfrak{b}\}.$$

It is easily verified that $(\mathfrak{b} : \mathfrak{b}')$ is a \mathfrak{d} -module. In fact,

Proposition 3.13 $(\mathfrak{b} : \mathfrak{b}')$ is fractional ideal.

Proof: Assume $\gamma\mathfrak{b} \subseteq \mathfrak{d}$ and $\gamma'\mathfrak{b}' \subseteq \mathfrak{d}$. Then, if $\mu \in \gamma\gamma'\mathfrak{b}'$, then $\mu(\mathfrak{b} : \mathfrak{b}') \subseteq \gamma'\mathfrak{d} \subseteq \mathfrak{d}$. Moreover, $\gamma\gamma'\mathfrak{b}' \subseteq \gamma\mathfrak{d} \subseteq \mathfrak{d}$. ■

3.8 Invertible Ideals

A fractional ideal \mathfrak{f} is said to be *invertible* provided that there is a fractional ideal \mathfrak{f}^{-1} such that $\mathfrak{f}\mathfrak{f}^{-1} = \mathfrak{d}$.

Lemma 3.14 If \mathfrak{f} has an inverse, then it is unique. Particularly,

$$\mathfrak{f}^{-1} = (\mathfrak{d} : \mathfrak{f}).$$

Proof: If $\mathfrak{f}\mathfrak{f}^{-1} = \mathfrak{d}$, then $\mathfrak{f}^{-1} \subseteq (\mathfrak{d} : \mathfrak{f})$. On the other hand, $\mathfrak{f}(\mathfrak{d} : \mathfrak{f}) \subseteq \mathfrak{d}$, so if \mathfrak{f}^{-1} is an inverse of \mathfrak{f} , then $(\mathfrak{d} : \mathfrak{f}) = \mathfrak{f}^{-1}\mathfrak{f}(\mathfrak{d} : \mathfrak{f}) \subseteq \mathfrak{f}^{-1}\mathfrak{d} = \mathfrak{f}^{-1}$. ■

We note that there is a dependence of the inverse on the ring \mathfrak{d} , which is not represented in the notation. Usually such a representation will be unnecessary, as the intended ring will be clear. When we must distinguish, we shall use $\mathfrak{f}^{-1(\mathfrak{d})}$.

It is easy to see that the inverse operation is contravariant (i.e., inclusion reversing).

We now prove a series of lemmas that will be useful to us later.

Lemma 3.15 *If all nonzero integral ideals are invertible, then the collection of fractional ideals is a group under multiplication.*

Proof: Since multiplication of ideals is associative, and \mathfrak{d} acts as an identity, it suffices to show that fractional ideals are invertible provided that integral ideals are invertible. Indeed, if \mathfrak{f} is a fractional ideal then writing $\mathfrak{f} = \gamma^{-1}\mathfrak{J}$ shows us that \mathfrak{f} has inverse $\gamma\mathfrak{J}^{-1}$. ■

Lemma 3.16 *If a finite product of integral ideals is invertible, then the ideals themselves are invertible.*

Proof: If $\mathfrak{b}^{-1} \prod_i \mathfrak{a}_i = \mathfrak{d}$, then $\mathfrak{a}_j \left(\mathfrak{b}^{-1} \prod_{i \neq j} \mathfrak{a}_i \right) = \mathfrak{d}$. ■

Lemma 3.17 *Invertible ideals are finitely generated.*

Proof: If $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{R}$, then we may write $1 = \sum_{i=1}^n \alpha_i \alpha'_i$ with $\{\alpha_i\} \subseteq \mathfrak{a}$ and $\{\alpha'_i\} \subseteq \mathfrak{a}^{-1}$. For arbitrary $\rho \in \mathfrak{R}$, we have $\rho = \sum \rho \alpha'_i \alpha_i$, and moreover, the coefficients $\rho \alpha'_i \in \mathfrak{R}$. Thus, $\{\alpha_i\}$ generates \mathfrak{a} . [21, p. 272]. ■

Lemma 3.18 *If \mathfrak{a} is a product of invertible prime ideals, then the \mathfrak{a} factorization of \mathfrak{a} into prime ideals is unique.*

Proof: See [21, p. 272]. ■

3.9 Field Extensions

We assume that the reader has a basic knowledge of the theory of field extensions, including Galois theory. We review here only a few facts. Many of the details can be found in [3, Chapter 13]. If k is a subfield of E then we say that E is an extension field of k , and we refer to the extension $E|k$. In such a situation, E is a vector space over k , and we write $[E : k]$ for its dimension. If $[E : k] < \infty$ we say $E|k$ is finite. If $\alpha \in E$, then $k(\alpha)$ denotes the smallest subfield of E that contains k and α , and is called the field **generated by** α and k .

Assume that $E|k$ is an extension of fields. An element $\alpha \in E$ is **algebraic** over k iff α is a root of a polynomial in $k[X]$.

If α is algebraic then we may as well take the polynomial α satisfies to be monic, since we can divide by the leading coefficient. Indeed, every element of E that is algebraic over k satisfies a monic polynomial, and it is not difficult to see that there is a unique such polynomial of minimal degree, and that it must be an irreducible element of $k[X]$. We denote this polynomial by $M_{\alpha,k}(x)$ and refer to it as the **minimal polynomial** of α over k . When there can be no confusion, we write $M_\alpha(X)$ for $M_{\alpha,k}(X)$. An equivalent condition for α to be algebraic over k is that the extension $k(\alpha)|k$ be finite, since

$$k(\alpha) \cong k[X]/M_\alpha(X),$$

which is spanned over k by the powers of α .

Proposition 3.19 For $\mathcal{F}(X) \in k[X]$ we have $\mathcal{F}(\alpha) = 0$ iff $M_{\alpha,k} | \mathcal{F}$ (in $k[X]$).

Proof: Apply the division algorithm. For the details, see [3, p. 500]. ■

If α is algebraic over the field k , then the **degree** of α is the dimension of $k(\alpha)|k$, which is the degree of $M_{\alpha,k}$. We say that the extension $E|k$ is a **algebraic** provided that every element of E is algebraic over k .

Proposition 3.20 Finite extensions are algebraic.

Proof: If $[E : k] < \infty$, then for $\alpha \in E$, $[k(\alpha) : k] < \infty$ as $k(\alpha)$ is a subspace of E . Thus, α is algebraic over k . ■

A field extension $E|k$ is said to be **simple** provided that $E = k(\alpha)$ for some $\alpha \in E$. As we have seen, a basis for the simple extension $k(\alpha)|k$ consists of the powers of α .

If $\alpha \in E$ is algebraic over k , then α is said to be **separable** over k if its multiplicity as a root of $M_{\alpha,k}$ is 1. The extension $E|k$ is called separable if every $\alpha \in E$ is separable over k .

Proposition 3.21 (The Primitive Element Theorem) Finite separable extensions are simple.

Proof: See [5, p. 287]. ■

If all algebraic extensions of a field k are separable, then k is called **perfect**. See [5, p. 289].

Proposition 3.22 \mathbb{Q} is perfect.

Proof: See [3, p. 531] or [5, p. 287]. ■

Corollary 3.23 *Thus, all finite extensions of \mathbb{Q} are simple.*

A field L is **algebraically closed** if the only algebraic extension of L is trivial, or equivalently, any element of any extension that is algebraic over L is in L . The **algebraic closure** of L is the smallest extension of L that is algebraically closed. Every field has a unique algebraic closure; we denote the algebraic closure of L by L^{al} . The algebraic closure of a field is algebraically closed. For a more thorough development, see [9, p. 231].

A **splitting field** for a polynomial $\mathcal{F} \in k[X]$ is an extension of k in which \mathcal{F} splits into linear factors. The extension $E|k$ is called **normal** if every embedding of E into k^{al} induces an automorphism of E . Equivalently, E is the splitting field of a set of polynomials in $k[X]$. See [9, p. 237]. The smallest field that is normal over k and contains E is called the **normal closure** of E over k . An extension $E|k$ is called **Galois** if it is normal, separable, and algebraic. We assume that the reader is familiar with the Fundamental Theorem of Galois Theory, which is treated in [3, p. 554]. We denote the Galois group of the extension $E|k$ by $\mathcal{G}_{E|k}$ or $\mathcal{G}(E|k)$, whichever is more convenient.

3.10 Number Fields and Number Rings

An **algebraic number** is an element of \mathbb{Q}^{al} . Equivalently, an algebraic number is a complex number that satisfies a monic polynomial over \mathbb{Q} . If α is an algebraic number, then there is a unique irreducible polynomial in $\mathbb{Z}[x]$ having α as a root, which we obtain from $M_{\alpha, \mathbb{Q}}$ by multiplying by the lcd of its coefficients. If α is an algebraic number such that this irreducible polynomial over \mathbb{Z} is monic, then we say that α is an **algebraic integer**. Put differently, an **algebraic integer** is a complex number that is integral over \mathbb{Z} . As we noted

earlier in greater generality, this is equivalent to the \mathbb{Z} -module $\mathbb{Z}[\alpha]$ being finitely generated.

A **number field** is a finite extension of the rational numbers. Such an extension is necessarily algebraic, and since \mathbb{Q} is perfect, the extension is also simple. Thus, any number field has the form

$$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, \dots, a_{n-1} \in \mathbb{Q}\}$$

for some algebraic number α , which, in this case, has degree n over \mathbb{Q} . A **number ring** is the ring of algebraic integers in a number field, i.e., the integral closure of \mathbb{Z} in a number field.

Assume that k is a finite extension of \mathbb{Q} . We denote the integral closure of \mathbb{Z} in k by \mathfrak{o}_k . If E is a finite separable extension of k , then the integral closure of \mathfrak{o}_k in E is the same as the integral closure of \mathbb{Z} in E , by Proposition 3.9. In other words,

Proposition 3.24 *the integral closure of \mathfrak{o}_k in E is \mathfrak{o}_E .*

In particular,

Corollary 3.25 *if F is a finite extension of \mathbb{Q} , then \mathfrak{o}_F is integrally closed.*

Assume F is a finite extension of \mathbb{Q} . Then by Proposition 3.11, \mathfrak{o}_F is a finitely generated \mathbb{Z} -module of rank n . Since \mathfrak{o}_F is a domain it is torsion free over \mathbb{Z} . Since \mathbb{Z} is a principal domain, by Proposition 3.7, \mathfrak{o}_F is free over \mathbb{Z} . By an **integral basis** we mean a basis for \mathfrak{o}_F over \mathbb{Z} . Notice that any integral basis must be a basis for F over \mathbb{Q} .

4. Some Theorems on Abelian Groups

Here we state a few results concerning abelian groups that we will need later in this thesis.

Theorem 4.1 *For any group \mathcal{G} , if $\mathcal{H} \trianglelefteq \mathcal{G}$, then \mathcal{G}/\mathcal{H} is abelian iff \mathcal{H} is contained in the commutator subgroup of \mathcal{G} .*

Proof: See [16, p. 33]. ■

Lemma 4.2 *If \mathcal{G} is a finite abelian group whose order is divisible by a prime p , then \mathcal{G} contains an element of order p .*

In fact, this theorem is true more generally for any finite group, not necessarily abelian. We only need the result for abelian groups. For the proof of both results, see [16, pp. 73, 4].

Theorem 4.3 *Every finite subgroup of the multiplicative group of a field is cyclic.*

Theorem 4.4 *A cyclic group of order n has a unique subgroup of order d for every d dividing n .*

For the proofs of Theorems 4.3 and 4.4, See [16, p. 28].

4.0.1 p -groups

Assume that p is a rational prime, $m \geq 1$ is a rational integer, and \mathcal{G} is a group of order p^m .

Lemma 4.5 *Assume that \mathcal{G} is abelian and that $\mathcal{H} \leq \mathcal{G}$ has order p^h . Then for every h' satisfying $h < h' \leq m$ there is a subgroup \mathcal{H}' of \mathcal{G} having order $p^{h'}$ and containing \mathcal{H} .*

Proof: It suffices to argue for $h' = h + 1$. The quotient group $\overline{\mathcal{G}} = \mathcal{G}/\mathcal{H}$ is a p -group, so there is $\gamma \in \overline{\mathcal{G}}$ of order p . Let \mathcal{H}' be the group generated by \mathcal{H} and γ . Then $\mathcal{H} \subsetneq \mathcal{H}'$ (because $\gamma \notin \mathcal{H}$). Since $\gamma^p \in \mathcal{H}$,

$$\mathcal{H}' = \mathcal{H} \sqcup \mathcal{H}\gamma \sqcup \dots \sqcup \mathcal{H}\gamma^{p-1}.$$

Thus \mathcal{H}' has order p^{h+1} . [15, p. 276] ■

Proposition 4.6 *The group \mathcal{G} is cyclic if \mathcal{G} is abelian with a unique subgroup of order p^{m-1} .*

Proof: Let \mathcal{H} be the subgroup of order p^{m-1} and let $\gamma \in \mathcal{G} \setminus \mathcal{H}$. We show that γ has order p^m . Suppose not and let p^h be the order of γ . By Lemma 4.5, $\langle \gamma \rangle$ is contained in a subgroup of order p^{m-1} , which is necessarily \mathcal{H} by hypothesis. Thus $\gamma \in \mathcal{H}$, which is a contradiction. [15, p. 276] ■

Proposition 4.7 *A p -group \mathcal{G} is cyclic iff it is abelian and contains exactly one subgroup of order d for each d dividing $\#\mathcal{G}$.*

Proof: See [16, p. 29]. ■

Theorem 4.8 *Any finite abelian group is isomorphic to a direct product of groups of prime power order. Particularly, if $\{p_i\}$ are the distinct primes dividing the order of the abelian group \mathcal{G} , and*

$$\mathcal{G}_{p_i} = \{\gamma \in \mathcal{G} : \text{the order of } \gamma \text{ is a power of } p_i\},$$

then $\mathcal{G} \cong \prod \mathcal{G}_{p_i}$.

Proof: See [15, p. 47]. ■

Lemma 4.9 *If \mathcal{G} is a cyclic group of order p^m , and $\mathcal{G} \cong \mathcal{H} \times \mathcal{K}$, then either $\mathcal{H} = \mathbf{1}$ or $\mathcal{K} = \mathbf{1}$.*

Proof: This follows from the uniqueness assertion in the Fundamental Theorem of Finite Abelian Groups. See [16, p. 131]. ■

4.1 Abelian Field Extensions

We now prove a theorem concerning finite abelian field extensions. The case when the base field is \mathbb{Q} will play a crucial role in proving our main theorem.

Theorem 4.10 *Every finite abelian extension is the compositum of abelian extensions of prime power degree.*

Proof: Assume $E|k$ is a finite abelian extension. Using Theorem 4.8, write

$$\mathcal{G}_{E|k} \cong \prod_{i=1}^s \mathcal{H}_i$$

for some s with $|\mathcal{H}_i| = p_i^{a_i}$ and $[E : k] = \prod_{i=1}^s p_i^{a_i}$. Let $\mathcal{G}_j = \prod_{i \neq j} \mathcal{H}_i$ for each $j = 1, \dots, s$ and let K_j denote the fixed field of \mathcal{G}_j . Then $\mathcal{G}_{E|K_j} \cong \mathcal{G}_j$, by the Fundamental Theorem of Galois Theory. Now,

$$\mathcal{G}_{E|K_1 \cdots K_s} \leq \bigcap_{j=1}^s \mathcal{G}_{E|K_j} = \bigcap_{j=1}^s \mathcal{G}_j = \mathbf{1},$$

since the order of \mathcal{G}_j is not divisible by p_j , so the intersection is not divisible by any primes. Thus, $E = K_1 \cdots K_s$. ■

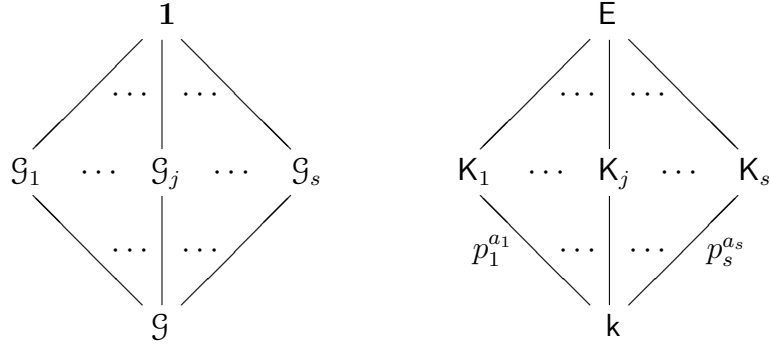


Figure 4.1: The prime power decomposition of abelian extensions

Theorem 4.11 *Assume E and F are extensions of a common field k . Then there is an embedding of $\mathcal{G}_{EF|k}$ into the subgroup of $\mathcal{G}_{E|k} \times \mathcal{G}_{F|k}$ consisting of (σ, τ) such that $\sigma|_{E \cap F} = \tau|_{E \cap F}$.*

Proof: Consider $\sigma \in \mathcal{G}_{EF|k}$. By the containment of the fields E and F in the compositum EF we may consider the restrictions $\sigma|_E$ and $\sigma|_F$ of σ to E and F , respectively. Consider the map

$$\sigma \mapsto (\sigma|_E, \sigma|_F).$$

The codomian of this map is the set of (σ, τ) such that $\sigma|_{E \cap F} = \tau|_{E \cap F}$. Moreover, if $\sigma|_E = \tau|_E$ and $\sigma|_F = \tau|_F$, then necessarily $\sigma = \tau$, so the map is injective. See also [15, p. 17]. ■

Corollary 4.12 *If $E|k$ and $F|k$ are abelian extensions, then so is $EF|k$.*

5. Cyclotomic Extensions

Given a complex number $\zeta = \xi + iv$, the **modulus** of ζ is given by $|\zeta| = \sqrt{\xi^2 + v^2}$, the **real part** of ζ by $\operatorname{Re}(\zeta) = \xi$, and the **imaginary part** of ζ by $\operatorname{Im}(\zeta) = v$. The plane spanned by 1 and i is the **complex plane**, which we coordinatize with $\operatorname{Re}(\zeta)$ and $\operatorname{Im}(\zeta)$. If θ represents the geometric angle of ζ as a point in the complex plane, then we can write $\zeta = |\zeta|e^{i\theta}$. We have the famous identity

$$e^{i\theta} = \cos \theta + i \sin \theta.$$

Since $\sin(X)$ and $\cos(X)$ both have period 2π , we can always take $\theta \in [0, 2\pi)$. When this is done we call θ the **argument** of ζ and write $\theta = \operatorname{Arg}(\zeta)$. Via this same identity we also have $1 = e^{i2k\pi}$ for any $k \in \mathbb{Z}$, but the argument of 1 is 0.

Multiplicativity of the modulus tells us that if $\zeta^n = 1$ then $|\zeta| = 1$. ($|z^n| = |z|^n$) Thus, $\zeta = e^{i\theta}$, and $n\theta = 2k\pi$ for some $k \in \mathbb{Z}$. For each k , the number

$$e^{2k\pi i/n} = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right)$$

is an n th root of unity. These numbers can be represented in the complex plane as points on the unit circle.

Over the algebraic closure \mathbb{Q}^{al} , any polynomial \mathcal{F} has as many roots, counting multiplicity, as its degree $\deg \mathcal{F}$. If the polynomial is irreducible over some subfield of \mathbb{Q}^{al} , then since algebraic extensions of \mathbb{Q} are separable (Proposition 3.22), \mathcal{F} has precisely as many *distinct* roots as its degree, that is, all of the multiplicities are 1.

The polynomial $P_n(X) = X^n - 1$ is not irreducible over \mathbb{Q} if $n > 1$ since $P_n(1) = 0$ implies that $(X - 1)$ divides $P_n(X)$ in $\mathbb{Q}[X]$. Degree considerations show that their quotient is nonconstant when $n > 1$. However, P_n does have n distinct roots, as we shall see.

5.1 Roots of Unity

In a field k , an n th **root of unity** is an element ζ such that $\zeta^n = 1$, that is, ζ is a root of the polynomial $X^n - 1$. Denote $X^n - 1$ by $P_n(X)$. If p is the characteristic of k , then, considering the Frobenius endomorphism, P_{p^m} has only one root, namely 1. If n is not divisible the characteristic of k , then P_n is separable because the derivative nX^{n-1} is not identically zero. The only root of nX^{n-1} is 0, which is not a root of P_n . Thus, P_n shares no common root with its derivative and in k^{al} ; hence, all of the roots of P_n are distinct.

Clearly if ξ and ζ are n th roots of unity then so is $\xi\zeta^{-1}$, so the n th roots of unity form a group, which we denote μ_n . By the Fundamental Theorem of Algebra, μ_n has order n . As a multiplicative subgroup of the field k^{al} , μ_n must be cyclic. A generator of μ_n is called a **primitive n th root of unity**.

Assume that ζ_n is a primitive n th root of unity in k^{al} . Since ζ_n^j has order $n/\gcd(j, n)$ in the group μ_n , we have a one-to-one correspondence between primitive n th roots of unity and positive integers $\leq n$ that are prime to n . Thus the Euler totient function $\phi(n)$ represents precisely the number of primitive n th roots of unity. Notice also that if $j \equiv i \pmod{n}$ then the orders of ζ_n^j and ζ_n^i are the same. Thus, the natural association of positive integers $\leq n$ with elements of the group $\mathbb{Z}/n\mathbb{Z}$ preserves group structure and induces a canonical isomorphism

$$\mu_n \cong \mathbb{Z}/n\mathbb{Z},$$

where the latter group is considered additive.

The elements of $\mathbb{Z}/n\mathbb{Z}$ prime to n form a multiplicative group, usually denoted $(\mathbb{Z}/n\mathbb{Z})^\times$. They correspond to the primitive n th roots of unity. Thus, the polynomial

$$\Phi_{n,k}(X) = \prod_{j \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^j)$$

has as roots precisely the primitive n th roots of unity, and clearly has degree $\phi(n)$. We refer to $\Phi_{n,k}$ as the *n th cyclotomic polynomial* over k .

A particularly interesting case is when $k = \mathbb{Q}$. When this is so we simply write Φ_n for $\Phi_{n,k}$.

Proposition 5.1 $\Phi_n(x) \in \mathbb{Z}[x]$ for every n .

Proof: See [6, p. 194]. ■

Theorem 5.2 Φ_n is irreducible over \mathbb{Q} (hence over \mathbb{Z}).

Proof: See [6, p. 195]. ■

Since Φ_n is monic, Φ_n is the minimal polynomial of ζ_n over \mathbb{Q} .

5.2 Cyclotomic Field Extensions

As a corollary to the above discussion, we obtain

Proposition 5.3 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

If ζ_n is a primitive n th root of unity over \mathbb{Q} , then ζ_n generates the group of n th roots of unity, the n th cyclotomic field $\mathbb{Q}(\zeta_n)$ contains all n th roots of unity. Hence, Φ_n splits in $\mathbb{Q}(\zeta_n)$. In fact, $\mathbb{Q}(\zeta_n)$ is the splitting field of Φ_n over \mathbb{Q} since $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n(x))$. The extension $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ is therefore Galois.

Notice that $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_{\text{lcm}[m,n]})$, and this clearly extends by induction.

Theorem 5.4 *We have*

$$\mathcal{G}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times;$$

the isomorphism is given by the map $\bar{a} \pmod{n} \mapsto \sigma_a$, where $\sigma_a(\zeta_n) = \zeta_n^a$.

¹ **Proof:** [3, p. 577]. ■

Thus, the extension $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ is abelian. In fact, in many cases, the Galois group of this extension is cyclic.

Proposition 5.5 *The group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic iff n is of the form 2 , 4 , p^a , or $2p^a$ for an odd prime p and positive integer a .*

Proof: See [6, p. 44] ■

By Proposition 4.4 and the Fundamental Theorem of Galois Theory, we obtain the following:

Corollary 5.6 *If n is of one of the forms mentioned in Proposition 5.5, then for every d dividing $\phi(n)$, there is a unique subfield of $\mathbb{Q}(\zeta_n)$ of degree d over \mathbb{Q} .*

The case when $n = p^a$ will be especially useful to us in proving our main theorem.

¹We notice an interesting relationship between the groups μ_n and $\text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$.

6. Trace, Norm, and Discriminant

If $E|k$ is a finite separable extension of fields and $\xi \in E$, then we define the *trace* of ξ relative to the extension $E|k$ to be

$$\mathrm{Tr}_{E|k}\xi = \sum_{\sigma \in \mathcal{H}_{E|k}} \xi^\sigma,$$

where $\mathcal{H}_{E|k}$ denotes the homomorphisms (necessarily monomorphisms) of E fixing k pointwise. In the case where $E|k$ is normal, $\mathcal{H}_{E|k}$ is the Galois group $\mathcal{G}_{E|k}$.

We note that the trace fixes k pointwise and is k -linear. We extend this definition to sets $S \subseteq E$ by defining

$$\mathrm{Tr}_{E|k}S = \{\mathrm{Tr}_{E|k}X : X \in S\}.$$

If S is an additive subgroup of E , then $\mathrm{Tr}_{E|k}S$ is an additive subgroup of k .

With the same situation as above, the *norm*¹ of ξ relative to the extension $E|k$ is defined to be

$$N_{E|k}\xi = \prod_{\sigma \in \mathcal{H}_{E|k}} \xi^\sigma.$$

When the base field is \mathbb{Q} , we write $\|\xi\|$ for $N_{E|\mathbb{Q}}\xi$ and refer to the norm as the *absolute norm*. We note that the norm fixes k pointwise and is multiplicative. See [15, p. 20].

¹The norm and trace can be defined more generally when the extensions are not necessarily separable, see [5, p. 289]. We only need the definitions given.

Proposition 6.1 *The norm and trace are transitive, meaning that if $\mathbf{k} \subseteq \mathbf{E} \subseteq \mathbf{F}$ is a tower of fields, then*

$$\mathrm{Tr}_{\mathbf{E}|\mathbf{k}}(\mathrm{Tr}_{\mathbf{F}|\mathbf{E}}(\xi)) = \mathrm{Tr}_{\mathbf{F}|\mathbf{k}}(\xi),$$

and

$$\mathrm{N}_{\mathbf{E}|\mathbf{k}}(\mathrm{N}_{\mathbf{F}|\mathbf{E}}(\xi)) = \mathrm{N}_{\mathbf{F}|\mathbf{k}}(\xi)$$

for all $\xi \in \mathbf{F}$.

Proof: See [15, p. 20]. ■

The trace is nondegenerate (in separable extensions), meaning that there is always an element $\xi \in \mathbf{E}$ such that $\mathrm{Tr}_{\mathbf{E}|\mathbf{k}}\xi \neq 0$. The general proof of this is non-trivial and uses Dedekind's theorem on the independence of \mathbf{k} -monomorphisms of \mathbf{E} . See [15, p. 20].

6.1 The Discriminant

The facts in this section are developed more fully in [15, pp. 20, 117]. Given a set of n elements $\{\xi_1, \dots, \xi_n\}$ in \mathbf{E} , we define the ***discriminant*** to be

$$\mathrm{Disc}(\xi_1, \dots, \xi_n) = \mathrm{Det}(\mathrm{Tr}_{\mathbf{E}|\mathbf{k}}(\xi_i \xi_j)).$$

If (σ_i) are the \mathbf{k} -monomorphisms of \mathbf{E} , then

$$\mathrm{Disc}_{\mathbf{E}|\mathbf{k}}(\xi_1, \dots, \xi_n) = \mathrm{Det}(\sigma_i(\xi_j))^2.$$

Another representation of the discriminant is given as follows. If $\xi'_j = \sum_{i=1}^n \alpha_{i,j} \xi_i$, then

$$\mathrm{Disc}_{\mathbf{E}|\mathbf{k}}(\xi'_1, \dots, \xi'_n) = \mathrm{Det}(\alpha_{i,j})^2 \mathrm{Disc}_{\mathbf{E}|\mathbf{k}}(\xi_1, \dots, \xi_n).$$

A corollary to this is the following:

Proposition 6.2 *If (ξ_i) and (ξ'_i) are two integral bases for $E|k$, then their discriminants are equal.*

Proof: For the details, see [15, p. 116]. ■

We refer to the common discriminant of an integral basis as the discriminant of E (over k), which we denote by $\text{Disc}_{E|k} \mathfrak{o}_E$.

Proposition 6.3 *The norm, trace, and discriminant lie in the base field.*

Proof: They are invariant under automorphisms of E fixing k . ■

For $\alpha \in E$, we write $\text{Disc}_{E|k} \alpha$ to mean

$$\text{Disc}_{E|k}(1, \alpha, \alpha^2, \dots, \alpha^{[E:k]-1}).$$

6.2 Quadratic Extensions of \mathbb{Q} .

We now wish to compute the discriminant of any quadratic extension of \mathbb{Q} . It is not hard to see that every quadratic extension of \mathbb{Q} is of the form $\mathbb{Q}(\sqrt{a})$ for some squarefree rational integer a . See [6, p. 188] for details.

Proposition 6.4 *The algebraic integers in $\mathbb{Q}(\sqrt{a})$ are*

$$\begin{cases} \mathbb{Z} \oplus \mathbb{Z}\sqrt{a}, & \text{if } a \equiv 2 \text{ or } 3 \pmod{4}; \\ \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{a}}{2}, & \text{if } a \equiv 1 \pmod{4}. \end{cases}$$

Proof: See [6, p. 189]. ■

From this, it is a straightforward calculation to verify that

$$\text{Disc } \mathbb{Q}(\sqrt{a}) = \begin{cases} 4a & \text{if } a \equiv 2 \text{ or } 3 \pmod{4}; \\ a & \text{if } a \equiv 1 \pmod{4}. \end{cases}$$

For the details, see [6, p. 189].

6.3 Cyclotomic Extensions of \mathbb{Q} .

If ζ is a primitive p th root of unity, then $\text{Disc}_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\mathfrak{o}_{\mathbb{Q}(\zeta)}) = \pm p^{p-2}$. For a proof of this result, see [15, p. 118].

7. Dedekind Domains

A *Dedekind domain* is a domain in which every proper nonzero ideal is a product of finitely many prime ideals. We shall see that in fact this product is necessarily unique up to permutations of the factors. We shall refer to this as the *prime decomposition* of an ideal. The ideals of a Dedekind domain provide a natural generalization of rational integers. In fact, there are many equivalent characterizations of Dedekind domains. See [21, V, §6], [5, p. 406], or [10, p. 59].

We first notice the following:

Proposition 7.1 *Principal ideal domains are Dedekind domains.*

Proof: In a principal ideal domain, prime ideals are generated by irreducible elements. Moreover, principal ideal domains are factorial. For these facts, we refer the reader to [21, p. 243]. The result follows. ■

Theorem 7.2 *In a Dedekind domain, fractional ideals are invertible.*

Proof: See [21, p. 274] or [4, p. 38]. ■

By the Lemmas in Section 3.8, fractional ideals of a Dedekind domain are finitely generated and factor uniquely as a product of prime ideals to integer powers. See [21, p. 274] for more details.

Corollary 7.3 *The fractional ideals under multiplication form a free group generated by the prime ideals.*

In fact, integral ideals can be written canonically (up to permutation of factors) as a product of distinct prime ideals to *positive* powers. See [21, p. 274] for more details.

Assume that \mathfrak{P} is a prime ideal in a Dedekind domain. Then $(\mathfrak{P}^m)_{m=0}^\infty$ is an infinite descending tower of ideals. The set $\bigcap_{m=0}^\infty \mathfrak{P}^m$ easily satisfies the properties of ideals. By unique factorization, the sequence never terminates, and hence this ideal is not expressible as a finite product of primes. Consequently, $\bigcap_{m=0}^\infty \mathfrak{P}^m$ must be the zero ideal (clearly it is not $\langle 1 \rangle$).

7.1 Noether's Classification

Let P be a set partially ordered by the relation \leq , i.e., \leq is reflexive and transitive, and $X \leq Y$ & $Y \leq X \Rightarrow X = Y$.

Proposition 7.4 *The following conditions are equivalent:*

1. *Every increasing sequence $X_1 \leq X_2 \leq \dots$ in S terminates, i.e., there is k such that $X_k = X_{k+1} = \dots$.*
2. *Every nonempty subset of S has a maximal element.*

Proof: [2, p. 74] ■

If \mathfrak{o} is a domain and \mathfrak{M} is an \mathfrak{o} -module, then the \mathfrak{o} -submodules of \mathfrak{M} can be partially ordered by \subseteq . In this case, \mathfrak{M} is said to be **Noetherian** (a Noetherian \mathfrak{o} -module) provided that the conditions in Proposition 7.4 hold.

Incidentally, if the submodules are ordered by \supseteq , then a module satisfying the conditions in Proposition 7.4 is said to be **Artinian**. As seen above, Dedekind domains are not Artinian.

Theorem 7.5 *An \mathfrak{o} -module \mathfrak{M} is Noetherian iff all of its \mathfrak{o} -submodules are finitely generated over \mathfrak{o} .*

Proof: [2, p. 75] ■

The ring \mathfrak{o} is said to be Noetherian if it is Noetherian as an \mathfrak{o} -module, i.e., if Proposition 7.4 holds for its ideals. Equivalently, by Theorem 7.5, all of its ideals are finitely generated.

Theorem 7.6 *Dedekind domains are Noetherian.*

Proof: It follows immediately from Theorem 7.2 and Proposition 3.17 that the fractional ideals of a Dedekind domain are finitely generated. Thus a Dedekind domain is Noetherian. ■

Theorem 7.7 *In a Dedekind domain, every nonzero prime ideal is maximal.*

Proof: See [15, p. 125]. ■

Incidentally, this means that a Dedekind domain has Krull dimension 1.

Theorem 7.8 *A Dedekind domain is integrally closed.*

Proof: See [21, p. 275]. ■

We have taken the historical approach in defining Dedekind domains as Dedekind did, and developing their properties. In fact, we have an alternative definition, which was discovered by Noether.

Theorem 7.9 (Noether's Classification of Dedekind Domains) *A ring \mathfrak{D} is a dedekind domain iff \mathfrak{D} is*

1. *Noetherian,*

2. integrally closed, and

3. every nonzero prime ideal is maximal.

Proof: In consideration of our development so far, it suffices to prove sufficiency. See [8, pp. 18-20]. ■

Proposition 7.10 *Let \mathfrak{R} be an integrally closed Noetherian ring, E a finite separable extension of its quotient field \mathfrak{k} . Then the integral closure of \mathfrak{R} in E is a finitely generated \mathfrak{R} -module.*

Proof: See [8, p. 6]. ■

Proposition 7.11 *Assume \mathfrak{R} is a principal domain and E is a finite separable extension of degree n of the quotient field of \mathfrak{R} . Then the integral closure of \mathfrak{R} in E is a free \mathfrak{R} -module of rank n .*

Proof: [9, p. 7] ■

Proposition 7.12 *Assume \mathfrak{d} is a Dedekind domain and E a finite separable extension of the quotient field of \mathfrak{d} . Let \mathfrak{D} be the integral closure of \mathfrak{d} in E . Then \mathfrak{D} is a Dedekind domain.*

Proof: It is simplest to use Noether's classification of Dedekind domains. By construction, \mathfrak{D} is integrally closed. Prime ideals are maximal by 3.12. For the details on why \mathfrak{D} is a Noetherian domain, see [21, p. 281]. ■

Applying Proposition 3.11 to the setting in Proposition 7.12, the quotient field of \mathfrak{D} is E . Notice that, in particular, since \mathbb{Z} is a Dedekind domain, if E is a finite separable extension of \mathbb{Q} , the number ring \mathfrak{o}_E is a Dedekind domain.

Indeed, this class of examples is our main motivation for developing the theory of Dedekind domains in this thesis. We shall refer to this case as the *classical case*.

7.2 Ideals

Proposition 7.13 *If \mathfrak{I} and \mathfrak{J} are two fractional ideals in a Dedekind domain \mathfrak{D} , then $\mathfrak{J}|\mathfrak{I}$ iff $\mathfrak{J} \supseteq \mathfrak{I}$.*

Proof: See [15, p. 129] ■

In other words, for ideals, “to contain is to divide.”

Lemma 7.14 *Assume \mathfrak{d} is a Dedekind domain and \mathfrak{I} is an ideal of \mathfrak{d} . Let $\{\alpha_i\}_{i=0}^s \subseteq \mathfrak{d}$ and assume for each i that $\mathfrak{I}^{x_i} \parallel \langle \alpha_i \rangle$. If the x_i are all distinct, then*

$$\mathfrak{I}^{\min\{x_i\}} \parallel \left\langle \sum \alpha_i \right\rangle.$$

Proof: Let x denote $\min\{x_i\}$. Since $\alpha_i \in \mathfrak{I}^x$ for each i , we see that $\sum \alpha_i \in \mathfrak{I}^x$; thus $\langle \sum \alpha_i \rangle \subseteq \mathfrak{I}^x$. Assume without loss of generality that $x = x_0$. Then for $i > 0$ we have $x_i > x$, so $\alpha_i \in \mathfrak{I}^{x+1}$ for $i > 0$; thus, $\sum_{i=1}^s \alpha_i \in \mathfrak{I}^{x+1}$. Assuming that $\sum_{i=0}^s \alpha_i \in \mathfrak{I}^{x+1}$ would imply that the difference $\alpha_0 \in \mathfrak{I}^{x+1}$. Then $\langle \alpha_0 \rangle \subseteq \mathfrak{I}^{x+1}$, contradicting that $\mathfrak{I}^x \parallel \langle \alpha_0 \rangle$. Thus, $\sum_{i=0}^s \alpha_i \notin \mathfrak{I}^{x+1}$, and $\langle \sum_{i=0}^s \alpha_i \rangle \not\subseteq \mathfrak{I}^{x+1}$. ■

If \mathfrak{a} and \mathfrak{b} are two ideals in a ring \mathfrak{R} , then the ideal generated by \mathfrak{a} and \mathfrak{b} , in view of Proposition 7.13, is the smallest ideal dividing them. We are motivated to therefore say that \mathfrak{a} and \mathfrak{b} are *coprime* or *relatively prime* provided that the ideal $\langle \mathfrak{I}, \mathfrak{J} \rangle$ is the ring \mathfrak{R} , which, incidentally, is the ideal $\langle 1 \rangle$. Distinct maximal ideals are clearly coprime, and thus, in a Dedekind domain, distinct primes are coprime.

Proposition 7.15 *If \mathfrak{a} and \mathfrak{b} are coprime, then \mathfrak{a}^n and \mathfrak{b} are coprime.*

Proof: If $1 = \alpha + \beta$, then

$$1 = 1^n = \sum_{i=1}^n \binom{n}{i} \alpha^i \beta^{n-i} = \alpha^n + \beta \sum_{i=1}^{n-1} \binom{n}{i} \alpha^i \beta^{n-1-i}.$$

■

Proposition 7.16 *If \mathfrak{a} and \mathfrak{b} are coprime, then $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.*

Proof: See [6, p. 181]

■

Theorem 7.17 (The Chinese Remainder Theorem) *If \mathcal{C} is a finite collection of pairwise coprime ideals in a ring \mathfrak{R} , then*

$$\mathfrak{R} / \left(\prod_{\mathfrak{a} \in \mathcal{C}} \mathfrak{a} \right) = \bigoplus_{\mathfrak{a} \in \mathcal{C}} \mathfrak{R} / \mathfrak{a}$$

Proof: See [6, p. 181].

■

Theorem 7.18 *Let \mathfrak{d} be a Dedekind domain, \mathfrak{k} its quotient field, E a finite separable extension of \mathfrak{k} and \mathfrak{D} the integral closure of \mathfrak{d} in E . Assume that \mathfrak{P} is a prime of \mathfrak{D} and \mathfrak{p} is a prime of \mathfrak{d} . Then the following are equivalent:*

1. $\mathfrak{P} | \langle \mathfrak{p} \rangle_{\mathfrak{D}}$
2. $\langle \mathfrak{p} \rangle_{\mathfrak{D}} \subseteq \mathfrak{P}$
3. $\mathfrak{p} \subseteq \mathfrak{P}$
4. $\mathfrak{P} \cap \mathfrak{d} = \mathfrak{p}$ (\mathfrak{P} lies above \mathfrak{p})
5. $\mathfrak{P} \cap \mathfrak{k} = \mathfrak{p}$.

Proof: Since \mathfrak{d} is integrally closed, $\mathfrak{D} \cap \mathfrak{k} = \mathfrak{d}$, and $4 \iff 5$ follows. The equivalence of 1 and 2 follows from Proposition 7.13. Since $\mathfrak{p} \subseteq \langle \mathfrak{p} \rangle_{\mathfrak{D}}$ we have $2 \Rightarrow 3$; the converse follows from $\mathfrak{P} = \langle \mathfrak{P} \rangle_{\mathfrak{D}}$, since $3 \Rightarrow \langle \mathfrak{p} \rangle_{\mathfrak{D}} \subseteq \langle \mathfrak{P} \rangle_{\mathfrak{D}}$. Obviously $4 \Rightarrow 3$. Conversely, if $\mathfrak{p} \subseteq \mathfrak{P}$, then $\mathfrak{p} \subseteq \mathfrak{P} \cap \mathfrak{d}$. Since \mathfrak{p} is maximal, $\mathfrak{P} \cap \mathfrak{d} = \mathfrak{p}$ or \mathfrak{d} . Since $\mathfrak{P} \neq \mathfrak{D}$, $1 \notin \mathfrak{P}$ and $\mathfrak{d} \not\subseteq \mathfrak{P}$, so $\mathfrak{P} \cap \mathfrak{d} \neq \mathfrak{d}$; hence $3 \Rightarrow 4$. ■

Proposition 7.19 *If \mathfrak{R} is integral over \mathfrak{r} , then there is exactly one nonzero prime of \mathfrak{r} lying under a given nonzero prime of \mathfrak{R} .*

Proof: Assume \mathfrak{P} is a prime of \mathfrak{R} . Since $\mathfrak{P} \neq \mathfrak{D}$, $1 \notin \mathfrak{P}$ and $\mathfrak{d} \not\subseteq \mathfrak{P}$. Thus, $\mathfrak{P} \cap \mathfrak{d} \neq \mathfrak{d}$. Now, the ideal $\mathfrak{P} \cap \mathfrak{r}$ is easily seen to be prime. By Proposition 3.12, $\mathfrak{P} \cap \mathfrak{r}$ is maximal, hence nonzero. ■

7.3 Ramification Index

Now, assume \mathfrak{d} is a Dedekind domain and \mathfrak{D} is the integral closure in a finite separable extension of the quotient field of \mathfrak{d} . If \mathfrak{p} is a prime of \mathfrak{d} , then we consider the prime decomposition of the integral ideal $\langle \mathfrak{p} \rangle_{\mathfrak{D}}$ in \mathfrak{D} , to which we shall refer as the *lifting* of \mathfrak{p} to \mathfrak{D} . Assume

$$\langle \mathfrak{p} \rangle_{\mathfrak{D}} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

with $e_i \geq 1$ for each i . Then prime \mathfrak{P} of \mathfrak{D} occurs in this decomposition iff \mathfrak{P} lies above \mathfrak{p} . Given this decomposition, we call e_i the *ramification index* of \mathfrak{P}_i over \mathfrak{p} and write $e_i = e(\mathfrak{P}_i | \mathfrak{p})$. When the ring \mathfrak{d} is understood, then considering Proposition 7.19 we write $e_{\mathfrak{P}}$ for $e(\mathfrak{P} | \mathfrak{p})$.

Proposition 7.20 *The ramification index is multiplicative in towers.*

Proof: See [15, p 191]. ■

The prime \mathfrak{p} of \mathfrak{d} is said to be *ramified* in \mathfrak{D} , or to *ramify* in \mathfrak{D} , provided that $\mathfrak{p}\mathfrak{D}$ is not squarefree, that is, for some prime \mathfrak{P} lying over \mathfrak{p} we have $e(\mathfrak{P}|\mathfrak{p}) > 1$. In this case we might also say that \mathfrak{P} is *ramified over* \mathfrak{p} , or over \mathfrak{d} . It is also common to say that \mathfrak{P} (or \mathfrak{p}) ramifies in the extension of the quotient fields.

Theorem 7.21 *Assume that \mathfrak{d} is a Dedekind domain with quotient field k , E a finite separable extension of k , and \mathfrak{D} the integral closure of \mathfrak{d} in E . A prime \mathfrak{p} of \mathfrak{d} ramifies in \mathfrak{D} if and only if $\mathfrak{p}|\text{Disc}_{E|k}(\mathfrak{D})$.*

Proof: [15, p. 238] ■

7.4 Residue Class Fields and Inertial Degree

If \mathfrak{p} is a nonzero prime ideal in the Dedekind domain \mathfrak{d} , then \mathfrak{p} is maximal and our previous discussion on residue class fields applies. If k is the quotient field of \mathfrak{d} , E a finite separable extension of k , \mathfrak{D} the integral closure of \mathfrak{d} in E , and \mathfrak{P} a prime ideal of \mathfrak{D} lying above \mathfrak{p} , then $\mathfrak{D}/\mathfrak{P}$ is an extension field of $\mathfrak{d}/\mathfrak{p}$. The degree of the extension $\mathfrak{D}/\mathfrak{P}|\mathfrak{d}/\mathfrak{p}$ is called the *residue class degree*, or *inertial degree* of \mathfrak{P} over \mathfrak{p} and is denoted by $f(\mathfrak{P}|\mathfrak{p})$, or $f_{\mathfrak{P}}$ when there is no ambiguity.

Proposition 7.22 *The inertial degree is multiplicative in towers.*

Proof: [15, p 191]. ■

Proposition 7.23 *The residue class vector space $\mathfrak{D}/\langle\mathfrak{p}\rangle_{\mathfrak{D}}$ has dimension $[E : k]$ over $\mathfrak{d}/\mathfrak{p}$.*

Proof: See [15, p. 212]. ■

If $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$ for each prime \mathfrak{P} lying above \mathfrak{p} , then \mathfrak{p} is said to *split completely* or *totally decompose* in \mathfrak{D} . The prime \mathfrak{p} is said to be *totally ramified* in \mathfrak{D} if $\langle \mathfrak{p} \rangle_{\mathfrak{D}} = \mathfrak{P}^n$ for some $n \geq 1$ with \mathfrak{P} prime, and $f(\mathfrak{P}|\mathfrak{p}) = 1$. In this case we might also say that \mathfrak{P} is *totally ramified over* \mathfrak{p} , over \mathfrak{d} , or over k .

We point out that if \mathfrak{P} is both totally ramified and unramified over \mathfrak{p} , then $E|k$ must be a trivial extension. This seems trivial, but we shall use this in the proof of our main theorem.

Notice that if a prime \mathfrak{p} is totally ramified in an extension $E|k$, then \mathfrak{p} is totally ramified in any intermediate extension. More precisely,

Proposition 7.24 *if $k \subseteq F \subseteq E$ is a tower of finite separable extensions of fields, and \mathfrak{p} is totally ramified in $E|k$, then \mathfrak{p} is totally ramified in $E|F$ and in $F|k$.*

Proof: This follows from Proposition 7.19 and Proposition 7.22. ■

Proposition 7.25 *For any prime \mathfrak{p} of \mathfrak{d} ,*

$$[E : k] = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}.$$

Proof: See [8, p. 25], [10, p. 68] and use Proposition 7.23. There is also a proof in [21, p. 287]. The most elementary proof, however, is in [15, p. 193], but Ribenboim only proves this for number rings. ■

Corollary 7.26 *The extension $\mathfrak{D}/\mathfrak{P}|\mathfrak{d}/\mathfrak{p}$ is finite.*

Corollary 7.27 *If \mathfrak{P} is totally ramified over \mathfrak{p} , then $\langle \mathfrak{p} \rangle_{\mathfrak{D}} = \mathfrak{P}^{[E:k]}$.*

7.4.1 Norm for Ideals

Theorem 7.28 *Assume that $\#\mathfrak{D}/\mathfrak{P} = p^f$. Then $\#\mathfrak{D}/\mathfrak{P}^e = p^{ef}$.*

Proof: See [6, p. 182]. ■

For a prime ideal \mathfrak{P} , we define the **norm** (for ideals) relative to the extension $E|k$ by

$$N_{E|k}\mathfrak{P} = \mathfrak{p}^{f_{\mathfrak{P}}},$$

and we extend our map $N_{E|k}$ to fractional ideals by multiplicativity, since the fractional ideals form a free abelian group generated by the prime ideals.

In the case when $\mathfrak{d} = \mathbb{Z}$, so $k = \mathbb{Q}$, $\mathfrak{D} = \mathfrak{o}_E$, and $\mathfrak{p} = p\mathbb{Z}$ for some rational prime p , we see that $\mathfrak{o}_E/\mathfrak{P}$ is a finite field of characteristic p . In this case, the norm is the (principal) ideal of \mathbb{Z} generated by the cardinality of $\mathfrak{o}_E/\mathfrak{P}$, and this fact extends to ideals that are not prime by Theorems 7.17 and 7.28. In other words,

$$N_{E|\mathbb{Q}}\mathfrak{I} = \langle \#\mathfrak{o}_E/\mathfrak{I} \rangle_{\mathbb{Z}},$$

for any ideal \mathfrak{I} of \mathfrak{o}_E . The cardinality $\#\mathfrak{o}_E/\mathfrak{P}$ is known as the **absolute norm** (for ideals). We write for the absolute norm

$$\|\mathfrak{I}\| = \#\mathfrak{o}_E/\mathfrak{I}.$$

The absolute norm for ideals generalizes the absolute norm for elements in the sense that $\|\xi\| = \|\langle \xi \rangle\|$ for $\xi \in E$. See [10, p. 66], [15, p. 141] and [8, p. 26].

7.5 Cyclotomic Extensions of \mathbb{Q} .

The following two results concerning cyclotomic extensions of \mathbb{Q} will prove useful. They are both proven in [6, p. 197].

Proposition 7.29 *Assume that ζ is a primitive n th root of unity, with p a rational prime. Then an odd rational prime p is ramified in $\mathbb{Q}(\zeta)$ iff $p|n$; 2 is ramified iff $4|n$.*

Proposition 7.30 *A rational prime q is totally ramified in $\mathbb{Q}(\xi_q)$.*

8. The Different

Assume \mathfrak{d} is a Dedekind domain, k its quotient field, E a finite separable extension of k , and \mathfrak{D} the integral closure of \mathfrak{d} in E .

If \mathcal{A} is an additive subgroup of E , then the set of all $\varepsilon \in E$ such that

$$\mathrm{Tr}_{E|k}(\varepsilon\mathcal{A}) \subseteq \mathfrak{d}$$

is a \mathfrak{d} -module, which we call the *complementary set* of \mathcal{A} (relative to the trace), and denote by \mathcal{A}^* .

Proposition 8.1 *If \mathfrak{K} is a fractional ideal of \mathfrak{D} , then \mathfrak{K}^* is also a fractional ideal of \mathfrak{D} .*

Proof: See [8, pp. 57, 8]. ■

Thus, in Dedekind domains, the complementary set of a fractional ideal is invertible. If \mathfrak{K} is a fractional ideal of \mathfrak{D} , then we define the *different* of \mathfrak{K} to be

$$\mathrm{Diff}_{E|k}\mathfrak{K} = (\mathfrak{K}^*)^{-1}.$$

When the fields are understood, we drop the subscript. The operation $\mathcal{A} \mapsto \mathcal{A}^*$ is easily seen to be contravariant, meaning that if $\mathcal{A} \subseteq \mathcal{B}$ then $\mathcal{A}^* \supseteq \mathcal{B}^*$. Since the operation of inverting fractional ideals is also contravariant, the different is monotone, i.e., if $\mathfrak{K} \subseteq \mathfrak{L}$, then $\mathrm{Diff}\mathfrak{K} \subseteq \mathrm{Diff}\mathfrak{L}$.

Proposition 8.2 *For each fractional ideal \mathfrak{K} of \mathfrak{D} , we have $\mathrm{Diff}\mathfrak{K} \subseteq \mathfrak{K}$.*

Proof: This follows from the containment $\mathfrak{K}^{-1} \subseteq \mathfrak{K}^*$. ■

Thus, in particular, $\text{Diff}_{\mathbb{E}|\mathbb{k}}(\mathfrak{D})$ is an integral ideal in \mathfrak{D} depending on \mathbb{k} .

8.1 Dual Basis

This section is similar to the development in [15, p. 240].

The trace $\text{Tr}_{\mathbb{E}|\mathbb{k}}$ induces a mapping $\mathbb{E} \times \mathbb{E} \rightarrow \mathbb{k}$ by $(\xi, \nu) \mapsto \text{Tr}_{\mathbb{E}|\mathbb{k}}(\xi\nu)$. This is a symmetric \mathbb{k} -bilinear form. For $\xi \in \mathbb{E}$, let $\varphi_\xi : \mathbb{E} \rightarrow \mathbb{k}$ be the linear form $\varphi_\xi(\nu) = \text{Tr}_{\mathbb{E}|\mathbb{k}}(\xi\nu)$. Thus, $\varphi_\xi \in \mathbb{E}'$, the dual \mathbb{k} -vector space of \mathbb{E} . For $\alpha \in \mathbb{k}$ and $\xi, \omega \in \mathbb{E}$, we have $\varphi_{\alpha\xi} = \alpha\varphi_\xi$ and $\varphi_{\xi+\omega} = \varphi_\xi + \varphi_\omega$. Thus φ is a \mathbb{k} -linear mapping from $\mathbb{E} \rightarrow \mathbb{E}'$. Since the trace is nondegenerate for separable extensions, $\varphi_x = 0$ iff $x = 0$, and this mapping is not the zero map. Thus, φ is an isomorphism between the \mathbb{k} -spaces \mathbb{E} and \mathbb{E}' .

If $\{\beta_1, \dots, \beta_m\}$ is a \mathbb{k} -basis of \mathbb{E} then let $\{\beta_1^*, \dots, \beta_n^*\} \subseteq \mathbb{E}$ be elements such that

$$\varphi_{\beta_i^*}(\beta_j) = \text{Tr}_{\mathbb{E}|\mathbb{k}}(\beta_i^* \beta_j) = \begin{cases} 1 & \text{if } i = j, \text{ and} \\ 0 & \text{otherwise,} \end{cases} \quad (8.1)$$

which certainly exists by surjectivity of φ .

Moreover, $\{\beta_1^*, \dots, \beta_n^*\}$ is another \mathbb{k} -basis for \mathbb{E} , which we call the **dual basis** (relative to the trace) of $\{\beta_1, \dots, \beta_n\}$.

Theorem 8.3 *Suppose $\alpha \in \mathbb{E}$ and consider $M_{\alpha, \mathbb{k}}(X)$ over $\mathbb{k}(\alpha)$, where we may write*

$$M_{\alpha, \mathbb{k}}(X) = (X - \alpha)(\gamma_0 + \gamma_1 X + \dots + \gamma_{n-1} X^{n-1}).$$

Then

$$\left\{ \frac{\gamma_0}{M'_{\alpha, \mathbb{k}}(\alpha)}, \dots, \frac{\gamma_{n-1}}{M'_{\alpha, \mathbb{k}}(\alpha)} \right\}$$

is the dual basis to $\{1, \alpha, \dots, \alpha^{n-1}\}$ in $k(\alpha)$.

Proof: See [8, p. 58] or [10, pp. 94,5]. ■

Proposition 8.4 *The different is multiplicative in towers, i.e., if $k \subseteq E \subseteq F$ is a tower of finite separable extensions, \mathfrak{d} is a Dedekind domain whose quotient field is k , \mathfrak{D} is the integral closure of \mathfrak{d} in E , and \mathfrak{R} the integral closure of \mathfrak{d} in F , then*

$$\text{Diff}_{F|k}(\mathfrak{R}) = \text{Diff}_{F|E}(\mathfrak{R}) \langle \text{Diff}_{E|k}(\mathfrak{d}) \rangle_{\mathfrak{R}}.$$

Proof: See [15, p. 244]. ■

We have an important application of the different for number fields:

Proposition 8.5 *An ideal \mathfrak{p} of \mathfrak{o}_E is ramified in $E|k$ iff \mathfrak{p} divides $\text{Diff}_{E|k}(\mathfrak{o}_E)$.*

Proof: See [15, p. 247] ■

Corollary 8.6 *Only finitely many primes are ramified in a number field.*

Lemma 8.7 *Suppose that \mathfrak{P} is totally ramified over \mathfrak{p} , and fix $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Then the exact power of \mathfrak{P} dividing $\text{Diff}_{E|k}\mathfrak{D}$ is the exact power of \mathfrak{P} dividing the ideal $\langle M'_{\pi,k}(\pi) \rangle_{\mathfrak{D}}$.*

Proof: See [15, p. 250]. ■

There are also many interesting exercises in [10] related to complementary sets and the different. See Exercises 3.33 through 3.40.

9. Galois Extensions

From now on assume that in our usual setting, the extension $E|k$ is Galois of degree n . Denote the Galois group of $E|k$ by \mathcal{G} and let \mathfrak{P} be one of the primes above \mathfrak{p} . If $\sigma \in \mathcal{G}$, then $\sigma\mathfrak{P}$ is maximal and hence a nonzero prime. Since \mathcal{G} fixes \mathfrak{d} , $\sigma\mathfrak{P}$ contains \mathfrak{p} , and $\sigma\mathfrak{P}$ is a prime of \mathfrak{D} lying above \mathfrak{p} . Hence, the Galois group acts on the primes above \mathfrak{p} .

Theorem 9.1 *The action of the Galois group on the primes above \mathfrak{p} is transitive.*

Proof: Assume that the lifting of \mathfrak{p} to \mathfrak{D} has the factorization

$$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Fix $i \in \{1 \dots g\}$ and denote \mathfrak{P}_i by \mathfrak{P} . Choose any $\alpha \in \mathfrak{P} \setminus \bigcup_{j \neq i} \mathfrak{P}_j$. We can do this by the Chinese Remainder Theorem, as we now argue. There exists a common solution to the set of congruences

$$\begin{aligned} X &\equiv 0 \pmod{\mathfrak{P}} \\ X &\equiv 1 \pmod{\mathfrak{P}_j} \text{ for } j \neq i. \end{aligned}$$

Now, if $X - 1 \in \mathfrak{P}_j$ and $X \in \mathfrak{P}$, then $1 \in \mathfrak{P}_j$, a contradiction. Thus, if α is such a solution, then $\alpha \in \mathfrak{P} \setminus \bigcup_{j \neq i} \mathfrak{P}_j$.

Now, $N_{E|k}\alpha$ is a multiple of α , and hence $N_{E|k}\alpha \in \mathfrak{P}$. Also $N_{E|k}\alpha \in k$, so $N_{E|k}\alpha \in k \cap \mathfrak{P} = \mathfrak{p}$. If $j \in \{1 \dots g\}$, then, since $\mathfrak{p} \subseteq \mathfrak{P}_j$, we have $N_{E|k}\alpha \in \mathfrak{P}_j$.

Assume j is fixed. Since \mathfrak{P}_j is prime, one of the factors, say $\gamma\alpha$, is in \mathfrak{P}_j . This implies that $\alpha \in \gamma^{-1}\mathfrak{P}_j$. Since $\gamma^{-1}\mathfrak{P}_j$ is a prime above \mathfrak{p} , it follows by our choice of α that $\gamma^{-1}\mathfrak{P}_j = \mathfrak{P}$, and $\gamma\mathfrak{P} = \mathfrak{P}_j$. Since i and j are arbitrary, we have our desired result.

Other proofs are given in [10, p. 70] and [6, p. 182]. ■

Now, notice that for $\sigma \in \mathcal{G}$, $\sigma\mathfrak{D} = \mathfrak{D}$. Thus, for any ideal, \mathfrak{I} of \mathfrak{D} , we have $\mathfrak{D}/\sigma\mathfrak{I} = \sigma\mathfrak{D}/\sigma\mathfrak{I} \cong \mathfrak{D}/\mathfrak{I}$, since σ is an isomorphism. This is particularly useful when \mathfrak{I} is prime. If \mathfrak{P} and \mathfrak{Q} are primes above \mathfrak{p} , then $\mathfrak{D}/\mathfrak{Q} \cong \mathfrak{D}/\mathfrak{P}$.

Proposition 9.2 *If \mathfrak{P} and \mathfrak{Q} are two primes lying above the same prime \mathfrak{p} , then $e_{\mathfrak{P}} = e_{\mathfrak{Q}}$ and $f_{\mathfrak{P}} = f_{\mathfrak{Q}}$.*

Proof: The fact that $e_{\mathfrak{P}} = e_{\mathfrak{Q}}$ follows from unique factorization and Theorem 9.1. The fact that $f_{\mathfrak{P}} = f_{\mathfrak{Q}}$ follows from the isomorphism $\mathfrak{D}/\mathfrak{Q} \cong \mathfrak{D}/\mathfrak{P}$. ■

In other words, all the primes in the factorization of the lifting of \mathfrak{p} to \mathfrak{D} occur with the same exponent, and have the same inertial degrees. We denote the common ramification index by e , and the common inertial degree by f .

Corollary 9.3 *If g denotes the number of distinct primes above \mathfrak{p} , then $efg = [E : k]$.*

Proof: This is a direct result of Proposition 9.2 and Proposition 7.25. ■

9.1 Subgroups of the Galois Group

We now investigate some of the structure of the Galois group $\mathcal{G}_{E|k}$. Some very good treatments can be found in [8, I, §5], [9, VII, §2], and [10, Chapter 4].

9.1.1 The Decomposition Group

For each prime ideal \mathfrak{P} of E we denote the stabilizer of \mathfrak{P} in \mathcal{G} by $\mathcal{D}_{\mathfrak{P}|\mathfrak{p}}$ or $\mathcal{D}(\mathfrak{P}|\mathfrak{p})$. That is,

$$\mathcal{D}_{\mathfrak{P}|\mathfrak{p}} = \{\gamma \in \mathcal{G}_{E|\mathfrak{k}} \mid \gamma\mathfrak{P} = \mathfrak{P}\},$$

and we call this subgroup of $\mathcal{G}_{E|\mathfrak{k}}$ the *decomposition group* of \mathfrak{P} over \mathfrak{d} , or over \mathfrak{p} , whichever is convenient. When there is no ambiguity, we write $\mathcal{D}_{\mathfrak{P}}$ or $\mathcal{D}(\mathfrak{P})$. If the prime \mathfrak{P} is understood, we simply write \mathcal{D} .

If \mathfrak{P} and \mathfrak{Q} are primes in \mathfrak{D} lying above \mathfrak{p} , then their decomposition groups are conjugate. Particularly, if $\sigma\mathfrak{P} = \mathfrak{Q}$, then $\mathcal{D}_{\mathfrak{Q}} = \sigma\mathcal{D}_{\mathfrak{P}}\sigma^{-1}$.

The *decomposition field* is the fixed field of the decomposition group, which we denote by $E_{\mathcal{D}(\mathfrak{P})}$. We denote sometimes the integral closure of \mathfrak{d} in $E_{\mathcal{D}(\mathfrak{P})}$ by $\mathfrak{D}_{\mathcal{D}(\mathfrak{P})}$, and if \mathfrak{Q} is a prime of \mathfrak{D} , then we denote the prime of $\mathfrak{D}_{\mathcal{D}(\mathfrak{P})}$ lying below \mathfrak{Q} by $\mathfrak{Q}_{\mathcal{D}(\mathfrak{P})}$.

Proposition 9.4

$$[\mathcal{G} : \mathcal{D}] = [E_{\mathcal{D}} : \mathfrak{k}] = g,$$

where g denotes the number of distinct primes above \mathfrak{p} .

Proof: In general, \mathcal{D} need not be normal in \mathcal{G} . Nonetheless, we may consider the cosets modulo \mathcal{D} , of which there are $[\mathcal{G} : \mathcal{D}]$. We notice that $\sigma\mathfrak{P} = \tau\mathfrak{P}$ iff σ and τ represent the same coset. Also, $\bar{\sigma} = \bar{\tau}$ iff $\sigma\mathfrak{P} = \tau\mathfrak{P}$. Using Theorem 9.1, this provides us with a one-to-one correspondence between the cosets modulo \mathcal{D} , and the primes lying above \mathfrak{p} , establishing $[\mathcal{G} : \mathcal{D}] = g$. The fact that $[\mathcal{G} : \mathcal{D}] = [E_{\mathcal{D}} : \mathfrak{k}]$ follows from Galois theory. ■

Proposition 9.5 *The field $E_{\mathcal{D}}$ is the smallest subfield T of E containing k such that \mathfrak{P} is totally ramified over $\mathfrak{P} \cap T$.*

Proof: This is proven in [9, p. 341]. ■

Proposition 9.6 $\mathfrak{d}/\mathfrak{p} \cong \mathcal{D}_{\mathcal{D}}/\mathfrak{P}_{\mathcal{D}}$.

Proof: This is proven in [9, p. 341]. ■

Corollary 9.7

$$e(\mathfrak{P}_{\mathcal{D}}|\mathfrak{p}) = f(\mathfrak{P}_{\mathcal{D}}|\mathfrak{p}) = 1;$$

$$f(\mathfrak{P}|\mathfrak{P}_{\mathcal{D}}) = f(\mathfrak{P}|\mathfrak{p});$$

$$e(\mathfrak{P}|\mathfrak{P}_{\mathcal{D}}) = e(\mathfrak{P}|\mathfrak{p}).$$

Since $\mathcal{D}_{\mathfrak{P}}$ fixes \mathfrak{P} , $\mathcal{D}_{\mathfrak{P}}$ acts naturally on the residue class field \mathcal{D}/\mathfrak{P} and fixes $\mathfrak{d}/\mathfrak{p}$. Associating each $\sigma \in \mathcal{D}_{\mathfrak{P}}$ with an automorphism $\bar{\sigma}$ of \mathcal{D}/\mathfrak{P} over $\mathfrak{d}/\mathfrak{p}$ induces a homomorphism of $\mathcal{D}_{\mathfrak{P}}$ into the Galois group of \mathcal{D}/\mathfrak{P} over $\mathfrak{d}/\mathfrak{p}$. For a proof that the extension is Galois, see [8, p. 15].

9.1.2 The Inertia Group

The action of the Galois group on \mathcal{D} induces an action on the cosets modulo \mathfrak{P} . The subgroup that induces the identity on the cosets, that is, stabilizes each coset, is denoted $\mathcal{E}_{\mathfrak{P}|\mathfrak{p}}$ or $\mathcal{E}(\mathfrak{P}|\mathfrak{p})$ and called the *inertia group* of \mathfrak{P} over \mathfrak{p} . Thus,

$$\mathcal{E}_{\mathfrak{P}|\mathfrak{p}} = \{\gamma \in \mathcal{G}_{E|k} \mid \forall \omega \in \mathcal{D}, \gamma(\omega) \equiv \omega \pmod{\mathfrak{P}}\}.$$

As with the decomposition group, we write $\mathcal{E}_{\mathfrak{P}}$, $\mathcal{E}(\mathfrak{P})$, or simply \mathcal{E} when there is no ambiguity. We notice that we have the tower

$$\mathcal{E} \leq \mathcal{D} \leq \mathcal{G}$$

of groups. In fact, $\mathcal{E} \trianglelefteq \mathcal{D}$, since \mathcal{E} is the kernel of the homomorphism of \mathcal{D} into the Galois group of the residue class field extension. The *inertia field* is the fixed field of the inertia group, and following the rest of our notation, we denote the inertia field by $E_{\mathcal{E}(\mathfrak{P})}$, and similarly we use $\mathcal{D}_{\mathcal{E}}$ and $\mathcal{Q}_{\mathcal{E}(\mathfrak{P})}$.

In the case when $\mathfrak{d}/\mathfrak{p}$ is a finite field, for example, in the classical case, the homomorphism \mathcal{D} into the Galois group of the residue class field extension is onto, as proven in [15, p. 261]. Thus, we have

Proposition 9.8 $\mathcal{D}/\mathcal{E} \cong \mathcal{G}(\mathcal{D}/\mathfrak{P}|\mathfrak{d}/\mathfrak{p})$, so $[\mathcal{D} : \mathcal{E}] = f$.

We summarize our development.

Theorem 9.9 *In the classical case,*

1. $E_{\mathcal{D}}$ is the largest subfield T of E containing k such that $e(\mathfrak{P} \cap T) = f(\mathfrak{P} \cap T) = 1$;
2. $E_{\mathcal{D}}$ is the smallest subfield T of E containing k such that \mathfrak{P} is the only prime lying over $\mathfrak{P} \cap T$;
3. $E_{\mathcal{E}}$ is the largest subfield T of E containing k such that $e(\mathfrak{P} \cap T) = 1$;
4. $E_{\mathcal{E}}$ is the smallest subfield T of E containing k such that \mathfrak{P} is totally ramified in $E|T$, i.e., $e(\mathfrak{P}|\mathfrak{P} \cap T) = [E : T]$.

Proof: For a complete proof, see [10, p. 104]. See also [15, p. 262]. ■

In other words, \mathfrak{p} does all of its splitting in $E_{\mathcal{D}}|k$, all of the inertia happens in the extension $E_{\mathcal{E}}|E_{\mathcal{D}}$, and all of the ramification of \mathfrak{P} over \mathfrak{p} happens in the extension $E|E_{\mathcal{E}}$. We point out that

$$\#\mathcal{E}(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}).$$

Groups	Fields	Ideals	Degrees	Ramification Indices	Inertial Degrees
1	E	\mathfrak{P}	e	e	1
\mathcal{E}	$E_{\mathcal{E}}$	$\mathfrak{P}_{\mathcal{E}}$	f	1	f
\mathcal{D}	$E_{\mathcal{D}}$	$\mathfrak{P}_{\mathcal{D}}$	g	1	1
\mathcal{G}	k	\mathfrak{p}			

Table 9.1: Decomposition and Inertia Fields: Ramification and Inertial Degrees

Notice that in the classical case, $f(\mathfrak{P}_{\mathcal{E}}|\mathfrak{p}) = f$ implies that $\mathcal{D}_{\mathcal{E}}/\mathfrak{P}_{\mathcal{E}} \cong \mathcal{D}/\mathfrak{P}$. It follows that $\mathcal{D}_{\mathcal{E}}$ contains a complete set of coset representatives of \mathcal{D} modulo \mathfrak{P} , i.e., that $\mathcal{D} = \mathcal{D}_{\mathcal{E}} + \mathfrak{P}$.

Lemma 9.10 *Assume E and F are Galois extensions of k such that $E \cap F = k$. Then if \mathfrak{p} is unramified in E and in F, then \mathfrak{p} is also unramified in EF.*

Proof: See [15, p. 278]. ■

9.1.3 The Ramification Groups

We define the *ramification groups* of \mathfrak{P} over \mathfrak{p} by

$$\mathcal{V}_m(\mathfrak{P}|\mathfrak{p}) = \{\gamma \in \mathcal{G}_{E|k} : \forall \omega \in \mathcal{D}, \gamma(\omega) \equiv \omega \pmod{\mathfrak{P}^{m+1}}\}$$

for each $m \geq 0$. That is, \mathcal{V}_m the stabilizer of $\mathcal{D} \pmod{\mathfrak{P}^{m+1}}$. Clearly, $\mathcal{V}_0 = \mathcal{E}$ and (\mathcal{V}_m) forms the descending tower

$$\cdots \leq \mathcal{V}_{k+1} \leq \mathcal{V}_k \leq \cdots \leq \mathcal{V}_1 \leq \mathcal{V}_0 = \mathcal{E}$$

of subgroups.

Proposition 9.11 *The chain stops, i.e., there is a k such that $\mathcal{V}_k = \mathbf{1}$.*

Proof: Since $\bigcap_{i \in \mathbb{Z}} \mathfrak{P}^i = \{0\}$, as discussed in Chapter 7, we have $\bigcap_{i \in \mathbb{Z}} \mathcal{V}_i = \mathbf{1}$.

The result follows. ■

As we shall see, the tower of ramification groups is normal in each stage, i.e.,

$$\mathbf{1} = \mathcal{V}_k \trianglelefteq \mathcal{V}_{k-1} \trianglelefteq \cdots \trianglelefteq \mathcal{V}_1 \trianglelefteq \mathcal{V}_0 = \mathcal{E}.$$

Proposition 9.12 *Assume that we are in the classical case. If $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$ and $\sigma \in \mathcal{V}_{m-1}$, then $\sigma \in \mathcal{V}_m$ iff $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{m+1}}$.*

¹ **Proof:** Necessity being trivial, assume that $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{m+1}}$. First, we prove that for $\alpha \in \langle \pi \rangle$, $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{m+1}}$. Write $\alpha = \lambda\pi$. Notice that $\sigma(\lambda) - \lambda \in \mathfrak{P}^m$ and $\pi \in \mathfrak{P}$, so

$$(\sigma(\lambda) - \lambda)\pi \in \mathfrak{P}^{m+1}.$$

Notice also that $\sigma(\lambda)(\pi - \sigma(\pi)) \in \mathfrak{P}^{m+1}$, so

$$\sigma(\lambda)\sigma(\pi) - \lambda\pi \equiv \sigma(\lambda)\pi - \lambda\pi \pmod{\mathfrak{P}^{m+1}}.$$

In other words, $\sigma(\alpha) - \alpha \equiv (\sigma(\lambda) - \lambda)\pi \pmod{\mathfrak{P}^{m+1}}$, and $\sigma(\alpha) - \alpha \in \mathfrak{P}^{m+1}$, establishing the claim.

Next, we prove that for $\alpha \in \mathfrak{P}$, $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{m+1}}$. Write $\langle \pi \rangle = \mathfrak{P}\mathfrak{J}$; thus $\mathfrak{P} + \mathfrak{J} = \mathfrak{D}$. Suppose that $\beta \in \mathfrak{D}_\varepsilon \cap (\mathfrak{J} \setminus \langle \pi \rangle)$. Then $\beta \in \mathfrak{J}$ implies $\beta\alpha \in \langle \pi \rangle$,

¹In fact, this result holds for $\sigma \in \mathcal{E}$, but we only need the weaker result. This stronger result can be obtained by induction. See [10, Exercise 4.20].

and $\beta \in \mathfrak{D}_\varepsilon$ implies $\sigma(\beta) = \beta$. Thus,

$$\beta\alpha \equiv \sigma(\beta\alpha) = \beta\sigma(\alpha) \pmod{\mathfrak{P}^{m+1}}.$$

Since $\beta(\sigma(\alpha) - \alpha) \in \mathfrak{P}^{m+1}$ and $\beta \notin \mathfrak{P}$ (because $\langle \pi \rangle = \mathfrak{P} \cap \mathfrak{I}$) it follows by unique factorization of ideals that $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{m+1}}$.

We need only argue that $\mathfrak{D}_\varepsilon \cap (\mathfrak{I} \setminus \langle \pi \rangle) \neq \emptyset$. Assume that $\mathfrak{I} = \mathfrak{Q}_1, \dots, \mathfrak{Q}_t$ are the primes dividing \mathfrak{I} , and for each i denote by $\mathfrak{Q}_{\varepsilon,i}$ the prime of \mathfrak{D}_ε lying below \mathfrak{Q}_i . We argue that none of these primes lies below \mathfrak{P} , whence we are done. If $\mathfrak{Q}_{\varepsilon,i} = \mathfrak{P}_\varepsilon$ for some i , then \mathfrak{P} and \mathfrak{Q}_i lie over the same prime \mathfrak{p} , but if that is so, then $\mathfrak{P}_\mathfrak{D} \neq \mathfrak{Q}_{\varepsilon,i}$, by Theorem 9.9 We have established the second claim.

Now, for $\alpha \in \mathfrak{D}$, recall that $\mathfrak{D} = \mathfrak{D}_\varepsilon + \mathfrak{P}$. Thus, we write $\alpha = \delta + \rho$ with $\delta \in \mathfrak{D}_\varepsilon$ and $\rho \in \mathfrak{P}$. Then, using the previous argument,

$$\begin{aligned} \sigma(\alpha) - \alpha &= \sigma(\delta + \rho) - \delta - \rho \\ &= \sigma(\delta) + \sigma(\rho) - \delta - \rho \\ &= \delta + \sigma(\rho) - \delta - \rho \\ &= \sigma(\rho) - \rho, \end{aligned}$$

which is in \mathfrak{P}^{m+1} by the preceding argument. ■

9.2 The Frobenius Automorphism in the Classical Case

Assume that k is a number field and E is a finite Galois extension with group \mathcal{G} . Let \mathfrak{p} be a prime of \mathfrak{o}_k and \mathfrak{P} a prime of \mathfrak{o}_E lying above \mathfrak{p} . Let p be the rational prime lying below \mathfrak{p} . The residue class field \mathfrak{o}_k is an extension of degree $f(\mathfrak{p}|p)$ over $\mathbb{Z}/p\mathbb{Z}$, and thus is isomorphic to the finite field $\mathbb{F}_{p^{f(\mathfrak{p}|p)}}$. The Galois group

of the extension $\mathfrak{o}_E/\mathfrak{P}$ over $\mathfrak{o}_k/\mathfrak{p}$ is cyclic and generated by the automorphism $X \mapsto X^{\|\mathfrak{p}\|}$.

In terms of congruences, $\phi(\xi) \equiv \xi^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}}$. Any member of the coset $\phi\mathcal{E}_{\mathfrak{P}}$ obviously has this effect. We shall call any member of this coset a ***Frobenius automorphism*** of \mathfrak{P} over \mathfrak{p} . See also [8, p. 17] and [10, p. 64].

9.3 Embedding $\mathcal{E}/\mathcal{V}_1 \hookrightarrow (\mathfrak{d}/\mathfrak{p})^\times$

This section follows Exercise 4.21 in [10]. We construct a homomorphism on \mathcal{E} with kernel \mathcal{V}_1 , showing that $\mathcal{V}_1 \trianglelefteq \mathcal{E}$. This homomorphism induces an embedding of the factor group $\mathcal{E}/\mathcal{V}_1$ into the multiplicative group $(\mathfrak{D}/\mathfrak{P})^\times$. We then show that with an additional assumption, this same embedding actually embeds $\mathcal{E}/\mathcal{V}_1 \hookrightarrow (\mathfrak{d}/\mathfrak{p})^\times$. Particularly, this works for abelian extensions. Throughout this section, fix $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$.

Lemma 9.13 *Suppose $\sigma \in \mathcal{V}_{m-1}$, $m \geq 1$, and $\sigma(\pi) \equiv \mu\pi \pmod{\mathfrak{P}^{m+1}}$. Then $\sigma(\xi) \equiv \mu\xi \pmod{\mathfrak{P}^{m+1}}$ for every $\xi \in \mathfrak{P}$.*

Proof: We follow a similar procedure as in the first two steps of the proof of Proposition 9.12. If $\xi \in \langle \pi \rangle$, say $\xi = \lambda\pi$, then notice that since $\sigma \in \mathcal{V}_{m-1}$ we have $\sigma(\lambda) - \lambda \in \mathfrak{P}^m$. Moreover,

$$\begin{aligned} \sigma(\xi) - \mu\xi &= \sigma(\lambda)\sigma(\pi) - \mu\lambda\pi \\ &\equiv \sigma(\lambda)\mu\pi - \mu\lambda\pi \\ &= \mu\pi(\sigma(\lambda) - \lambda) \pmod{\mathfrak{P}^{m+1}}. \end{aligned}$$

Since $\sigma(\lambda) - \lambda \in \mathfrak{P}^m$ and $\pi \in \mathfrak{P}$, we have $\mu\pi(\sigma(\lambda) - \lambda) \in \mathfrak{P}^{m+1}$, i.e.,

$$\sigma(\xi) - \mu\xi \in \mathfrak{P}^{m+1}.$$

Now, suppose $\xi \in \mathfrak{P}$. As before, write $\langle \pi \rangle = \mathfrak{P}\mathfrak{J}$, and find $\beta \in \mathfrak{D}_\varepsilon \cap (\mathfrak{J} \setminus \langle \pi \rangle)$. This implies that $\beta\alpha \in \langle \pi \rangle$, and $\sigma(\beta) = \beta$. Thus,

$$\mu\beta\alpha \equiv \sigma(\beta\alpha) = \beta\sigma(\alpha) \pmod{\mathfrak{P}^{m+1}}.$$

In other words, $\beta(\mu\alpha - \sigma(\alpha)) \in \mathfrak{P}^{m+1}$. Since $\beta \notin \mathfrak{P}$ (because $\langle \pi \rangle = \mathfrak{P} \cap \mathfrak{J}$) we must have $\sigma(\alpha) - \mu\alpha \in \mathfrak{P}^{m+1}$. \blacksquare

Lemma 9.14 *For all $\sigma \in \mathfrak{D}$ there exists $\mu_\sigma \in \mathfrak{D}$ such that*

$$\sigma(\pi) \equiv \mu_\sigma \pi \pmod{\mathfrak{P}^2}.$$

Proof: If $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, then we may write $\langle \pi \rangle_{\mathfrak{D}} = \mathfrak{P}\mathfrak{J}$ with \mathfrak{P} and \mathfrak{J} coprime. Then \mathfrak{P}^2 and \mathfrak{J} are also coprime, so we may apply the Chinese Remainder Theorem to find X such that

$$X \equiv \sigma(\pi) \pmod{\mathfrak{P}^2}, \text{ and} \tag{9.1}$$

$$X \equiv 0 \pmod{\mathfrak{J}}. \tag{9.2}$$

Now, because $\sigma \in \mathfrak{D}$ and $\pi \in \mathfrak{P}$ we have $\sigma(\pi) \in \mathfrak{P}$. Also $X - \sigma\pi \in \mathfrak{P}^2 \subseteq \mathfrak{P}$ so $X \in \mathfrak{P}$. In fact, $X \in \mathfrak{P} \cap \mathfrak{J}$, which, since $\mathfrak{P} + \mathfrak{J} = \mathfrak{D}$, is the ideal $\langle \pi \rangle_{\mathfrak{D}}$. Thus, $X = \mu_\sigma \pi$ for some $\mu_\sigma \in \mathfrak{D}$, establishing our result. \blacksquare

Now, if $\mu\pi \equiv \nu\pi \pmod{\mathfrak{P}^2}$, then $\pi(\mu - \nu) \in \mathfrak{P}^2$. This means that $\mathfrak{P}^2 | \langle \pi \rangle_{\mathfrak{D}} \langle \mu - \nu \rangle_{\mathfrak{D}}$, and by unique factorization, we get $\mu - \nu \in \mathfrak{P}$. Thus,

μ_σ is uniquely determined modulo \mathfrak{P} .

We therefore have a well-defined map $\mathfrak{D} \rightarrow \mathfrak{D}/\mathfrak{P}$ defined by $\sigma \mapsto \mu_\sigma$. We notice that $\pi \notin \mathfrak{P}^2$ implies that $\mu_\sigma \notin \mathfrak{P}$, so the codomain is actually contained in $(\mathfrak{D}/\mathfrak{P})^\times$.

Now, assume that $\sigma \in \mathcal{E}$. If $\beta \in \mathfrak{P}$, then, by Lemma 9.13, with $m = 1$, we have $\sigma(\beta) \equiv \mu_\sigma \beta \pmod{\mathfrak{P}^2}$. We apply this to $\tau(\pi)$ for $\tau \in \mathcal{E}$. Indeed, $\tau(\pi) \equiv \pi \pmod{\mathfrak{P}}$, so $\tau(\pi) \in \mathfrak{P}$. Applying the Lemma 9.13, and the fact that $\tau(\pi) = \mu_\tau \pi$, we have

$$\sigma\tau(\pi) = \sigma(\tau(\pi)) \equiv \mu_\sigma \tau(\pi) \equiv \mu_\sigma \mu_\tau \pi \pmod{\mathfrak{P}^2}.$$

On the other hand, $\sigma\tau \in \mathcal{E}$, so

$$\sigma\tau(\pi) \equiv \mu_{\sigma\tau} \pi \pmod{\mathfrak{P}^2}.$$

By the uniqueness modulo \mathfrak{P} proved earlier, we have

$$\sigma\tau(\pi) \equiv \mu_\sigma \mu_\tau \pi \pmod{\mathfrak{P}^2}, \text{ and } \mu_{\sigma\tau} \equiv \mu_\sigma \mu_\tau \pmod{\mathfrak{P}}.$$

In other words, our map is a homomorphism. It is obvious that the kernel is \mathcal{V}_1 . Thus, we have proven the following:

Theorem 9.15 *There is an embedding $\mathcal{E}/\mathcal{V}_1 \hookrightarrow (\mathfrak{D}/\mathfrak{P})^\times$. Consequently, in the classical case, $\mathcal{E}/\mathcal{V}_1$ is cyclic of order dividing $\|\mathfrak{P}\| - 1$.*

9.3.1 A Better Result for Abelian Extensions in the Classical Case

We have seen that in the classical case \mathfrak{D}/\mathcal{E} is abelian. If the commutator subgroup of \mathfrak{D} lies strictly between \mathcal{E} and \mathcal{V}_1 , then $\mathfrak{D}/\mathcal{V}_1$ is not abelian.

In this section, we prove the following:

Theorem 9.16 *In the classical case, if $\mathfrak{D}/\mathcal{V}_1$ is abelian, then the embedding $\mathcal{E}/\mathcal{V}_1 \hookrightarrow (\mathfrak{D}/\mathfrak{P})^\times$ actually sends $\mathcal{E}/\mathcal{V}_1$ into the subgroup $(\mathfrak{d}/\mathfrak{p})^\times$.*

This will be useful to us because of the following corollary:

Corollary 9.17 *In the classical case, $\mathcal{E}/\mathcal{V}_1$ is cyclic of order dividing $\|\mathfrak{p}\| - 1$.*

In particular, this is true when $\mathbb{E}|\mathfrak{k}$ is abelian. We first prove a lemma about the Frobenius automorphisms. Recall that $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$.

Lemma 9.18 *Let ϕ denote a Frobenius automorphism of \mathfrak{P} over \mathfrak{p} . Fix $\sigma \in \mathcal{E}$, and suppose that $\sigma(\pi) \equiv \mu\pi \pmod{\mathfrak{P}^2}$. Then*

$$\phi\sigma\phi^{-1}(\pi) \equiv \mu^{\|\mathfrak{p}\|}\pi \pmod{\mathfrak{P}^2}.$$

Proof: Notice that ϕ , ϕ^{-1} , and $\sigma \in \mathcal{D}$, so μ_ϕ , $\mu_{\phi^{-1}}$, and μ_σ are defined as in Lemma 9.14. Moreover, $\phi^{-1}(\pi) \in \mathfrak{P}$ since $\pi \in \mathfrak{P}$. Thus, by Lemma 9.13, since $\sigma \in \mathcal{E} = \mathcal{V}_0$, we have

$$\begin{aligned} \sigma\phi^{-1}(\pi) &\equiv \mu_\sigma\phi^{-1}(\pi) \\ &\equiv \mu_\sigma\mu_{\phi^{-1}}\pi \pmod{\mathfrak{P}^2}. \end{aligned}$$

Thus,

$$\phi\sigma\phi^{-1}(\pi) \equiv \phi(\mu_\sigma)\phi(\mu_{\phi^{-1}})\mu_\phi\pi \pmod{\mathfrak{P}^2}. \quad (9.3)$$

Now, $\phi(\mu_\sigma) \equiv \mu_\sigma^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}}$, by definition of ϕ . Hence, for some $\rho_\sigma \in \mathfrak{P}$, we have

$$\phi(\mu_\sigma) = \mu_\sigma^{\|\mathfrak{p}\|} + \rho_\sigma.$$

In addition, we have

$$\begin{aligned} \phi\phi^{-1}(\pi) &\equiv \phi(\mu_{\phi^{-1}}\pi) \\ &= \phi(\mu_{\phi^{-1}})\phi(\pi) \\ &\equiv \phi(\mu_{\phi^{-1}})\mu_\phi\pi \pmod{\mathfrak{P}^2}. \end{aligned}$$

Since we also have $\phi\phi^{-1}(\pi) \equiv \pi \pmod{\mathfrak{P}^2}$, the uniqueness assertion made following Lemma 9.14 implies

$$\phi(\mu_{\phi^{-1}})\mu_{\phi} \equiv 1 \pmod{\mathfrak{P}}.$$

We therefore assume that

$$\phi(\mu_{\phi^{-1}})\mu_{\phi} = 1 + \rho_{\phi}, \text{ with } \rho_{\phi} \in \mathfrak{P}.$$

Now, equation 9.3 becomes

$$\begin{aligned} \phi\sigma\phi^{-1}(\pi) &\equiv (\mu_{\sigma}^{\|\mathfrak{p}\|} + \rho_{\sigma})(1 + \rho_{\phi})\pi \\ &= \mu_{\sigma}^{\|\mathfrak{p}\|}\pi + \rho_{\sigma}\pi + \mu_{\sigma}^{\|\mathfrak{p}\|}\rho_{\phi}\pi + \rho_{\sigma}\rho_{\phi}\pi \\ &\equiv \mu_{\sigma}^{\|\mathfrak{p}\|}\pi \pmod{\mathfrak{P}^2}, \end{aligned}$$

since all other terms are in \mathfrak{P}^2 . ■

We now prove the theorem.

Proof: Let $\sigma \in \mathcal{E}$, and again let ϕ be a Frobenius automorphism of \mathfrak{P} over \mathfrak{p} . By Lemma 9.18, $\phi\sigma\phi^{-1}(\pi) \equiv \mu_{\sigma}^{\|\mathfrak{p}\|}\pi \pmod{\mathfrak{P}^2}$. Since $\phi\sigma\phi^{-1} \in \mathcal{E}$, we have $\phi\sigma\phi^{-1}(\pi) \in \mathfrak{P}$, so by Lemma 9.13,

$$\begin{aligned} \sigma^{-1}\phi\sigma\phi^{-1}(\pi) &\equiv \mu_{\sigma^{-1}}\phi\sigma\phi^{-1}(\pi) \\ &\equiv \mu_{\sigma^{-1}}\mu_{\sigma}^{\|\mathfrak{p}\|}\pi \pmod{\mathfrak{P}^2}. \end{aligned}$$

Now assume that $\mathcal{D}/\mathcal{V}_1$ is abelian. Thus, the commutator subgroup of \mathcal{D} is contained in \mathcal{V}_1 , so $\sigma^{-1}\phi\sigma\phi^{-1} \in \mathcal{V}_1$, and $\sigma^{-1}\phi\sigma\phi^{-1}(\pi) \equiv \pi \pmod{\mathfrak{P}^2}$. By the uniqueness assertion following Lemma 9.14, we must have $\mu_{\sigma^{-1}}\mu_{\sigma}^{\|\mathfrak{p}\|} \equiv 1 \pmod{\mathfrak{P}}$. Now, also $\mu_{\sigma^{-1}}\mu_{\sigma} \equiv 1 \pmod{\mathfrak{P}}$, so

$$\mu_{\sigma^{-1}}\mu_{\sigma} - \mu_{\sigma^{-1}}\mu_{\sigma}^{\|\mathfrak{p}\|} \in \mathfrak{P}.$$

Since $\mu_{\sigma^{-1}} \notin \mathfrak{P}$, we must have $\mu_\sigma \equiv \mu_\sigma^{\|\mathfrak{p}\|} \pmod{\mathfrak{P}}$. Considered in the field extension $\mathfrak{D}/\mathfrak{P}|\mathfrak{d}/\mathfrak{p}$, we see that μ_σ is fixed under the action of the Galois group. Thus, $\mu_\sigma \in \mathfrak{d}/\mathfrak{p}$. \blacksquare

9.4 Embedding $\mathcal{V}_{m-1}/\mathcal{V}_m \hookrightarrow \mathfrak{D}/\mathfrak{P}$

In this section we follow Exercise 4.22 in [10]. We prove that $\mathcal{V}_{m-1} \leq \mathcal{V}_m$, by constructing a homomorphism on \mathcal{V}_{m-1} having kernel \mathcal{V}_m . Moreover, this induces an embedding of $\mathcal{V}_{m-1}/\mathcal{V}_m \hookrightarrow (\mathfrak{D}/\mathfrak{P})^+$.

Again fix $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Notice that $\pi^m \in \mathfrak{P}^m \setminus \mathfrak{P}^{m+1}$ by unique factorization of ideals (particularly $\langle \pi \rangle^m$).

We first prove the following:

Lemma 9.19 *For each $\sigma \in \mathcal{V}_{m-1}$ there exists $\alpha_\sigma \in \mathfrak{D}$ such that $\sigma(\pi) \equiv \pi + \alpha_\sigma \pi^m \pmod{\mathfrak{P}^{m+1}}$.*

Proof: We have proven this result for $m = 1$ ($\alpha = \mu - 1$), so we assume tacitly that $m \geq 2$. The argument is similar to the proof of Lemma 9.14. Write $\langle \pi^m \rangle = \mathfrak{P}^m \mathfrak{J}$ (so \mathfrak{P}^m and \mathfrak{J} are coprime). Apply the Chinese Remainder Theorem to find $X \in \mathfrak{D}$ such that

$$X \equiv \sigma(\pi) - \pi \pmod{\mathfrak{P}^{m+1}}, \text{ and} \tag{9.4}$$

$$X \equiv 0 \pmod{\mathfrak{J}}. \tag{9.5}$$

First, $X \equiv \sigma(\pi) - \pi \pmod{\mathfrak{P}^{m+1}}$ implies $X \equiv \sigma(\pi) - \pi \pmod{\mathfrak{P}^m}$, so $X \in \mathfrak{P}^m$ and hence $X \in \mathfrak{P}^m \cap \mathfrak{J} = \langle \pi^m \rangle$. Writing $X = \alpha_\sigma \pi^m$, we have $\alpha_\sigma \pi^m \equiv \sigma(\pi) - \pi \pmod{\mathfrak{P}^{m+1}}$, or

$$\sigma\pi \equiv \pi + \alpha_\sigma \pi^m \pmod{\mathfrak{P}^{m+1}}.$$

■

Now, if $\pi + \alpha\pi^m \equiv \pi + \beta\pi^m \pmod{\mathfrak{P}^{m+1}}$, then $(\alpha - \beta)\pi^m \in \mathfrak{P}^{m+1}$. Since $\pi^m \in \mathfrak{P}^m \setminus \mathfrak{P}^{m+1}$, unique factorization forces $\alpha - \beta \in \mathfrak{P}$. Thus,

α_σ is unique modulo \mathfrak{P} .

We therefore have a well-defined map of $\mathcal{V}_{m-1} \rightarrow \mathfrak{D}/\mathfrak{P}$. We apply Lemma 9.13 to $\tau(\pi)$ for $\tau \in \mathcal{V}_{m-1}$. Since

$$\sigma(\pi) \equiv \pi + \alpha_\sigma \pi^m = (1 + \alpha_\sigma \pi^{m-1})\pi \pmod{\mathfrak{P}^{m+1}},$$

by Lemma 9.13, for $\beta \in \mathfrak{P}$, we have that $\sigma(\beta) \equiv (1 + \alpha_\sigma \pi^{m-1})\beta \pmod{\mathfrak{P}^{m+1}}$.

In particular, if $\tau \in \mathcal{V}_{m-1}$, then $\tau(\pi) \in \mathfrak{P}$, so

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

Now, $m \geq 2 \Rightarrow 2m - 1 \geq m + 1$, so $\alpha_\sigma \alpha_\tau \pi^{2m-1} \in \mathfrak{P}^{m+1}$, and we have

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

Thus,

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

Uniqueness modulo \mathfrak{P} implies

$$\alpha_\sigma + \alpha_\tau \equiv \alpha_{\sigma\tau} \pmod{\mathfrak{P}}.$$

In other words, our map is a homomorphism. Clearly the kernel is \mathcal{V}_m , and we have the following:

Theorem 9.20 *There is an embedding $\mathcal{V}_{m-1}/\mathcal{V}_m \hookrightarrow (\mathcal{D}/\mathfrak{P})^+$. Consequently, in the classical case, $\#\mathcal{V}_{m-1}/\mathcal{V}_m$ divides $\#\mathcal{D}/\mathfrak{P}$.*

Notice that we have now established that the tower

$$\mathbf{1} = \mathcal{V}_k \trianglelefteq \mathcal{V}_{k-1} \trianglelefteq \cdots \trianglelefteq \mathcal{V}_1 \trianglelefteq \mathcal{V}_0 = \mathcal{E}$$

is indeed normal in each stage.

Proposition 9.21 *In the classical case, \mathcal{V}_1 is a p -group. Hence, \mathcal{V}_i is a p -group for each $i \geq 1$.*

Proof: $\mathcal{E}/\mathcal{V}_1$ is cyclic and $\mathcal{V}_i/\mathcal{V}_{i+1}$ is an elementary abelian p -group, so \mathcal{E} is solvable and \mathcal{V}_1 is a p -group. [15, p. 269]. ■

Proposition 9.22 *In the classical case, \mathcal{D} is solvable.*

Proof: We have $\mathcal{D} \geq \mathcal{E} \geq \mathbf{1}$, with \mathcal{E} is solvable, and \mathcal{D}/\mathcal{E} cyclic.[15, p. 269] ■

9.5 Hilbert's Formula for Totally Ramified Primes in the Classical Case

Assume that \mathfrak{P} is totally ramified over \mathfrak{p} and that we are in the classical case. Then $\mathcal{G} = \mathcal{D} = \mathcal{E}$ by Theorem 9.9. Let t denote the exact power of \mathfrak{P} dividing $\text{Disc}_{\mathbb{E}|\mathbb{k}}(\mathfrak{o}_{\mathbb{E}})$. In this section we find an explicit formula for t .

Lemma 9.23 *If $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, then \mathfrak{P}^t is an exact divisor of $\langle M'_{\pi, \mathbb{k}}(\pi) \rangle_{\mathcal{D}}$.*

Proof: A direct corollary to Lemma 8.7. ■

Lemma 9.24 *If $\sigma \in \mathcal{V}_{m-1} \setminus \mathcal{V}_m$, then the ideal $\langle \pi - \sigma(\pi) \rangle_{\mathfrak{D}}$ is exactly divisible by \mathfrak{P}^m .*

Proof: If $\sigma \in \mathcal{V}_{m-1}$, then $\pi - \sigma(\pi) \in \mathfrak{P}^m$, by definition of the group \mathcal{V}_{m-1} . If $\sigma \notin \mathcal{V}_m$, then by Proposition 9.12, $\pi - \sigma(\pi) \notin \mathfrak{P}^{m+1}$. ■

Theorem 9.25

$$t = \sum_{m \geq 0} (\#\mathcal{V}_m - 1).$$

Proof: Write

$$M'_{\pi, k}(\pi) = \prod_{\gamma \in \mathcal{G}} (\pi - \gamma(\pi)).$$

Since \mathfrak{P} is totally ramified, $\mathcal{G} = \mathcal{V}_0$, and $\mathcal{G} = \bigsqcup \mathcal{V}_{m-1} \setminus \mathcal{V}_m$, it follows that

$$t = \sum_{m \geq 1} m \cdot \#(\mathcal{V}_{m-1} \setminus \mathcal{V}_m) = \sum_{m \geq 0} (\#\mathcal{V}_m - 1).$$

■

The formula in Theorem 9.25 is known as ***Hilbert's formula***.

10. Abelian Extensions and the Kronecker-Weber Theorem

We wish now to discuss abelian extensions. With our usual situation, assume that $E|k$ is an abelian extension, that is, Galois with abelian group, which we shall denote by \mathcal{G} . Let \mathfrak{p} be a prime of \mathfrak{d} and \mathfrak{P} a prime of D lying over \mathfrak{p} . Let \mathcal{D} and \mathcal{E} be the decomposition and inertia groups of $\mathfrak{P}|\mathfrak{p}$, respectively. Then any prime \mathfrak{Q} over \mathfrak{p} can be written as $\sigma\mathfrak{P}$ for some $\sigma \in \mathcal{G}$, and the decomposition and inertia groups of $\mathfrak{Q}|\mathfrak{p}$ are the conjugates $\sigma\mathcal{D}\sigma^{-1}$ and $\sigma\mathcal{E}\sigma^{-1}$, respectively; see [8, p. 18]. When $E|k$ is abelian, then these conjugations have no effect, and it makes sense to speak of the decomposition and inertia groups of \mathfrak{p} itself. See [7, p. 1].

We devote the remainder of this chapter to proving our main theorem:

Theorem 10.1 (Kronecker-Weber) *Every finite abelian extension of \mathbb{Q} is contained in a cyclotomic extension of \mathbb{Q} .*

10.1 Reduction to Prime Power Degree

Recall that in Chapter 4 we proved that any abelian extension is the compositum of abelian extensions of prime power degree; see Theorem 4.10. We wish to apply this to our present situation.

Theorem 4.10 reduces our problem to the case in which E is an abelian extension of prime power degree over \mathbb{Q} . If E is the compositum $K_1 \cdots K_s$, and for each i we have $K_i \subseteq \mathbb{Q}(\zeta_{m_i})$, then $E \subseteq \mathbb{Q}(\zeta_{m_1}) \cdots \mathbb{Q}(\zeta_{m_s}) \subseteq \mathbb{Q}(\zeta_{\text{lcm}[m_1, \dots, m_s]})$.

10.2 Reduction to One (Particular) Ramified Prime

At this point we are forced to forfeit some generality. The theorem that we wish to prove is not true in more general a context than when the base field is \mathbb{Q} . From here on, all of our extensions will be finite and abelian over \mathbb{Q} .

Assume that $K|\mathbb{Q}$ is a finite abelian extension. Considering Theorem 4.10 (and Section 10.1), we may assume that $[K : \mathbb{Q}] = p^m$ for some rational prime p , which we do. Assume that \mathfrak{P} is a prime of \mathfrak{o}_K lying over p . In this section, we shall reduce our situation further to one in which only p is ramified.

Suppose that q is a prime $\neq p$ that is ramified in K , and assume that \mathfrak{Q} is a prime of \mathfrak{o}_K lying over q . Now, $\mathcal{V}_1(\mathfrak{Q})$ is a q -group, by Proposition 9.21. As a subgroup of \mathcal{G} , which has order p^m , $\mathcal{V}_1(\mathfrak{Q})$ is also a p -group. Since p and q are distinct, we must have

$$\mathcal{V}_1(\mathfrak{Q}) = \mathbf{1}.$$

It follows from this and Theorem 9.16 that

$$e_{\mathfrak{Q}}|q - 1.$$

Now, $\mathbb{Q}(\zeta_q)$ has degree $q - 1$ over \mathbb{Q} , and the Galois group of $\mathbb{Q}(\zeta_q)|\mathbb{Q}$ is cyclic. By the Fundamental Theorem of Galois Theory and Theorem 4.4, $\mathbb{Q}(\zeta_q)$ has a unique subfield L of degree $e_{\mathfrak{Q}}$ over \mathbb{Q} . We now consider how q splits in L .

Assume $\overline{\mathfrak{Q}}$ is a prime of KL lying over \mathfrak{Q} , and let K' denote the inertia field $(KL)_{\mathcal{E}(\overline{\mathfrak{Q}})}$.

The prime q is unramified in $K'|\mathbb{Q}$ and every rational prime that is unramified in $K|\mathbb{Q}$ is also unramified in $K'|\mathbb{Q}$.

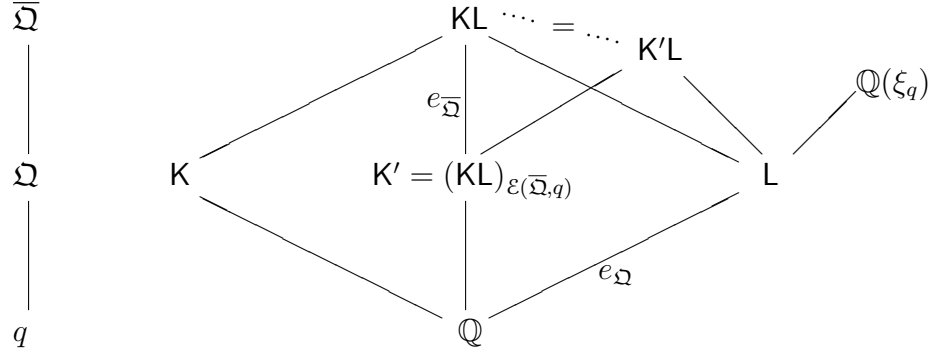


Figure 10.1: The behavior of $q \neq p$

Proof: First, q is unramified in K' , by Theorem 9.9. Let r be a rational prime $\neq q$. Then r is unramified in $\mathbb{Q}(\zeta_q)$ because $\text{Disc}\mathbb{Q}(\zeta_q) = \pm q^{q-2}$. Since $L \subseteq \mathbb{Q}(\zeta_q)$, r is unramified in L , by multiplicativity of the ramification indices, Proposition 7.20. Now, if r is unramified in K , then r is unramified in KL , by Lemma 9.10. Since $K' \subseteq KL$, r is unramified in K' . ■

Now, we wish to apply Theorem 4.11 to our present context. We have an embedding

$$\mathcal{G}_{KL|\mathbb{Q}} \hookrightarrow \mathcal{G}_{K|\mathbb{Q}} \times \mathcal{G}_{L|\mathbb{Q}}.$$

Since $\mathcal{E}_{\overline{\Omega}} \leq \mathcal{G}_{KL|\mathbb{Q}}$, we can consider the image of $\mathcal{E}_{\overline{\Omega}}$ under this embedding.

Proposition 10.2 *This embedding sends $\mathcal{E}_{\overline{\Omega}}$ into $\mathcal{E}_{\Omega} \times \mathcal{G}_{L|\mathbb{Q}}$.*

Proof: Let $\sigma \in \mathcal{E}_{\overline{\Omega}}$. What needs to be shown is that $\sigma|_K \in \mathcal{E}_{\Omega}$. First, for $\alpha \in \mathfrak{o}_{KL}$, we have $\sigma(\alpha) - \alpha \in \overline{\Omega}$, by definition of the group. Restricting σ to K leads us to consider $\alpha \in \mathfrak{o}_K$, since $\mathfrak{o}_{KL} \cap K = \mathfrak{o}_K$. Now, $\sigma(\alpha) - \alpha \in K$ because $K|\mathbb{Q}$ is assumed normal. Moreover, $\overline{\Omega} \cap K = \Omega$. Thus, $\sigma(\alpha) - \alpha \in \Omega$. ■

Recall that $[\mathbb{L} : \mathbb{Q}] = e_\Omega$, which divides p^m . By this and the preceding result, $\mathcal{E}(\overline{\Omega}|q)$ is a p -group. Thus, $\mathcal{V}_1(\overline{\Omega}|q)$ is also a p -group. Of course, by Proposition 9.21, $\mathcal{V}_1(\overline{\Omega}|q)$ is also a q -group. Again, $p \neq q$, so

$$\mathcal{V}_1(\overline{\Omega}|q) = \mathbf{1}.$$

The group $\mathcal{E}(\overline{\Omega}|q)$ is therefore cyclic, by Lemma 9.16. Also, $\mathcal{E}(\overline{\Omega}|q)$ may be regarded as a subgroup of $\mathcal{E}_\Omega \times \mathcal{G}_{\mathbb{L}|\mathbb{Q}}$, as argued above. In fact, $\mathcal{E}(\overline{\Omega}|q)$ may be regarded either as a subgroup of \mathcal{E}_Ω or of $\mathcal{G}_{\mathbb{L}|\mathbb{Q}}$, by Lemma 4.9. In either case, we conclude that $e_{\overline{\Omega}}|e_\Omega$. On the other hand, $e_\Omega|e_{\overline{\Omega}}$ by multiplicativity of the ramification index. Hence,

$$e_{\overline{\Omega}} = e_\Omega.$$

Now, q is totally ramified in $\mathbb{L}|\mathbb{Q}$, by Proposition 7.30, since $\mathbb{L} \subseteq \mathbb{Q}(\zeta_q)$. Since $[\mathbb{L} : \mathbb{Q}] = e_\Omega$, the equality $e_{\overline{\Omega}} = e_\Omega$, implies that q does not pick up any more ramification in $\mathbb{K}\mathbb{L}|\mathbb{L}$; more precisely,

$\overline{\Omega}$ is unramified over \mathbb{L} .

By multiplicativity of the ramification indices in the tower $\mathbb{L} \subseteq \mathbb{K}'\mathbb{L} \subseteq \mathbb{K}\mathbb{L}$, we conclude the more important fact that

$\overline{\Omega}$ is unramified over $\mathbb{K}'\mathbb{L}$.

Also, by Theorem 9.9, $\overline{\Omega}$ is totally ramified over \mathbb{K}' . By considering the tower $\mathbb{K}' \subseteq \mathbb{K}'\mathbb{L} \subseteq \mathbb{K}\mathbb{L}$ and using Proposition 7.24, we conclude that

$\overline{\Omega}$ is totally ramified over $\mathbb{K}'\mathbb{L}$.

Thus, $\overline{\mathfrak{Q}}$ is both unramified and totally ramified over $K'L$. The extension $KL|K'L$ must therefore be trivial, i.e.,

$$K'L = KL.$$

Since $L \subseteq \mathbb{Q}(\xi_q)$, if $K' \subseteq \mathbb{Q}(\xi_t)$ then $K \subseteq KL = K'L \subseteq \mathbb{Q}(\xi_q)\mathbb{Q}(\xi_t) \subseteq \mathbb{Q}(\xi_{\text{lcm}(q,t)})$. Thus, if K' is contained in a cyclotomic field, then so is K .

Notice that $[K' : \mathbb{Q}]$ is a power of p because $[L : \mathbb{Q}]$ and $[K : \mathbb{Q}]$ are both powers of p , and $K' \subseteq KL$. Also, recall that all primes unramified in $K|\mathbb{Q}$ are unramified in $K'|\mathbb{Q}$. Thus, we have reduced the number of ramified primes $\neq p$ by at least 1. Since there are only finitely many ramified rational primes in K , we can repeat this process until no primes other than p are ramified. We have therefore reduced the problem to the case when the extension is prime power degree, and that prime is the only ramified rational prime. Indeed, since we show in Appendix B that at least one prime is ramified unless the extension is trivial, we may assume that this prime is ramified. We henceforth assume this to be the case.

10.3 The Case for 2

¹ Assume that K is an abelian extension of degree 2^m over \mathbb{Q} .

Lemma 10.3 *If R is a real abelian extension of degree 2^m over \mathbb{Q} , and 2 is the only ramified prime in R , then R contains the unique quadratic subfield $\mathbb{Q}(\sqrt{2})$. Consequently, $\mathcal{G}_{R|\mathbb{Q}}$ is cyclic.*

Proof: If $m = 1$, then by the formula for the discriminant, $R = \mathbb{Q}(\sqrt{2})$. The Galois group is cyclic because its order is the prime 2.

¹Our treatment of this case is very similar to that in [15, pp. 278, 279].

Assume $m > 1$. By Lemma 4.5, the Galois group $\mathcal{G}_{\mathbb{R}|\mathbb{Q}}$ contains a subgroup of order 2^{m-1} , i.e., a subgroup of index 2. By the Fundamental Theorem of Galois Theory, \mathbb{R} contains a subfield \mathbb{F} such that $[\mathbb{F} : \mathbb{Q}] = 2$. Now, 2 is the only ramified rational prime in \mathbb{F} . Thus, $\text{Disc}_{\mathbb{F}|\mathbb{Q}}(\mathfrak{o}_{\mathbb{F}})$ is a power of 2, which, by the formula for discriminants of quadratic number fields, leaves $\mathbb{F} = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{-2})$. The only real field among these is $\mathbb{Q}(\sqrt{2})$. Thus, the subgroup of $\mathcal{G}_{\mathbb{R}|\mathbb{Q}}$ of order 2^{m-1} is unique, and we conclude that $\mathcal{G}_{\mathbb{R}|\mathbb{Q}}$ is cyclic. ■

Lemma 10.4 *For each m , there is exactly one real abelian extension of degree 2^m over \mathbb{Q} such that 2 is the only ramified prime.*

Proof: Assume that \mathbb{R} and \mathbb{R}' are two such extensions. Then the compositum $\mathbb{R}\mathbb{R}'$ has degree a power of 2, and only 2 is ramified by Lemma 10.3. Thus $\mathcal{G}_{\mathbb{R}\mathbb{R}'|\mathbb{Q}}$ is cyclic. The product

$$\mathcal{G}_{\mathbb{R}\mathbb{R}'|\mathbb{Q}} \cong \mathcal{G}_{\mathbb{R}|\mathbb{R}\mathbb{R}'} \times \mathcal{G}_{\mathbb{R}'|\mathbb{R}\mathbb{R}'}$$

must therefore have one of its factors trivial. In either case, $\mathbb{R} = \mathbb{R}'$. ■

Now, let ζ be a primitive root of unity of order 2^{m+2} . Set $\mathbb{L} = \mathbb{Q}(\zeta)$, so $[\mathbb{L} : \mathbb{Q}] = \phi(2^{m+2}) = 2^{m+1}$. Let $\mathbb{R} = \mathbb{L} \cap \mathbb{R}$. If $\zeta = \xi + iv$, with $\xi, v \in \mathbb{R}$, then $\xi - iv \in \mathbb{L}$ by normality, so the sum 2ξ and difference $2iv$ are in \mathbb{L} . Thus, $\xi \in \mathbb{L}$, and since $i \in \mathbb{L}$, also $v \in \mathbb{L}$. Since also $\xi, v \in \mathbb{R}$, we have $\xi, v \in \mathbb{R}$. Thus, $\zeta \in \mathbb{R}(i)$; hence $\mathbb{L} \subseteq \mathbb{R}$. On the other hand, $i \in \mathbb{L}$ and $\mathbb{R} \subseteq \mathbb{L}$ together imply that $\mathbb{R}(i) \subseteq \mathbb{L}$. Thus,

$$\mathbb{R}(i) = \mathbb{L}.$$

Since $i \notin \mathbb{R}$, we have that $[\mathbb{L} : \mathbb{R}] \neq 1$. Since i satisfies the quadratic equation $X^2 + 1 = 0$ over \mathbb{L} , we have $[\mathbb{L} : \mathbb{R}] = 2$, and

$$[\mathbb{R} : \mathbb{Q}] = 2^m.$$

Thus, \mathbb{R} is the unique real abelian extension of \mathbb{Q} of degree 2^m with only 2 ramified. We notice that \mathbb{R} is contained in a cyclotomic extension. The important fact, which we have proven, is this:

Lemma 10.5 *The unique real abelian extension of degree 2^m with only 2 ramified is contained in a cyclotomic field, namely $\mathbb{Q}(\zeta_{2^{m+2}})$.*

Now we return our attention to \mathbb{K} . Since $\mathbb{Q}(i)|\mathbb{Q}$ is abelian, the compositum $\mathbb{K}(i)$ is abelian over \mathbb{Q} . Also, since 2 is the only ramified prime in $\mathbb{Q}(i)$ as well as in \mathbb{K} , by Lemma 9.10, only 2 is ramified in $\mathbb{K}(i)$. Moreover, $[\mathbb{K}(i) : \mathbb{Q}]$ is a power of 2.

Let $\mathbb{T} = \mathbb{K}(i) \cap \mathbb{R}$. Thus, \mathbb{T} is a real abelian extension of \mathbb{Q} , and as a subfield of $\mathbb{K}(i)$, \mathbb{T} has degree a power of 2 over \mathbb{Q} and only 2 is ramified. Assume by Lemma 10.5 that $\mathbb{T} \subseteq \mathbb{Q}(\omega)$ with ω a primitive root of unity.

Now, by the Primitive Element Theorem, Proposition 3.21, we may assume that $\mathbb{K}(i) = \mathbb{T}(\alpha + i\beta)$ with $\alpha, \beta \in \mathbb{R}$. Then $\alpha - i\beta \in \mathbb{K}(i)$ by normality, so $\alpha, i\beta$, and thus β^2 are in $\mathbb{K}(i)$. We now have α and $\beta^2 \in \mathbb{K}(i) \cap \mathbb{R} = \mathbb{T}$. Consequently, $\alpha + i\beta$ satisfies the polynomial $X^2 - 2\alpha X + (\alpha^2 + \beta^2)$ with coefficients in \mathbb{T} , and hence $[\mathbb{K}(i) : \mathbb{T}] = 2$. Thus, $\mathbb{K}(i) = \mathbb{T}(i)$, and $\mathbb{K} \subseteq \mathbb{K}(i) = \mathbb{T}(i) \subseteq \mathbb{Q}(\omega, i)$, which is contained in a cyclotomic extension of \mathbb{Q} , since both ω and i are roots of unity.

10.4 The Case When p is Odd and $m = 1$

By assumption, \mathfrak{P} is ramified over p , that is, $e_{\mathfrak{P}} > 1$. If g denotes the number of primes above p , then $e_{\mathfrak{P}}f_{\mathfrak{P}}g = p$, so we must have $e_{\mathfrak{P}} = p$ and $f_{\mathfrak{P}} = g = 1$.

Let $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Notice that $\mathfrak{P} \cap \mathbb{Q} = p\mathbb{Z} \subseteq \mathfrak{P}^p \subseteq \mathfrak{P}^2$ because $p \geq 2$; hence, $\pi \notin \mathbb{Q}$. Since the degree of π divides $[\mathbb{K} : \mathbb{Q}] = p$, π must have degree p over \mathbb{Q} . Denote

$$M_{\pi, \mathbb{Q}}(X) = X^p + a_{p-1}X^{p-1} + \cdots + a_0.$$

Thus, $a_i \in \mathbb{Z}$ for each $i = 1, \dots, p$, and

$$\pi^p + a_{p-1}\pi^{p-1} + \cdots + a_1\pi + a_0 = 0.$$

Hence,

$$-a_0 = \pi^p + a_{p-1}\pi^{p-1} + \cdots + a_1\pi.$$

Since $\pi \in \mathfrak{P}$, it follows that $a_0 \in \mathfrak{P}$. Thus, we have $a_0 \in \mathbb{Z} \cap \mathfrak{P} = p\mathbb{Z}$, which is contained in \mathfrak{P}^p , so, in fact, $a_0 \in \mathfrak{P}^p$.

Now consider congruence modulo \mathfrak{P}^2 . Since

$$-a_1\pi - a_0 = \pi^p + a_{p-1}\pi^{p-1} + \cdots + a_2\pi^2,$$

it follows that $a_1\pi + a_0 \in \mathfrak{P}^2$. Since $p > 2$, we have $a_0 \in \mathfrak{P}^2$. Thus, $a_1\pi \in \mathfrak{P}^2$.

Now, $\pi \notin \mathfrak{P}^2$; by unique factorization of the ideal $\langle a_1\pi \rangle$, we must have $a_1 \in \mathfrak{P}$.

As with a_0 , we see that $a_1 \in \mathfrak{P}^p$. A simple induction argument shows that $a_i \in \mathfrak{P}$

for each $i = 1, \dots, p-1$.² Consequently,

²Notice that, in fact, we showed that $1, \pi, \dots, \pi^{p-1}$ are independent modulo p . This result can be obtained more generally. See [10, Ex. 3.20].

a_i is divisible by p for each $i = 0, \dots, p-1$.

Let \mathfrak{P}^k be the exact power of \mathfrak{P} dividing the principal ideal $\langle M'(\pi) \rangle$. Recall Hilbert's formula from Theorem 9.25:

$$k = \sum_{m \geq 0} (\#\mathcal{V}_m - 1).$$

Since $[\mathbb{K} : \mathbb{Q}] = p$, for each $m \geq 0$, \mathcal{V}_m has order 1 or p . Thus, each nonzero term is $p-1$, and

k is a multiple of $p-1$.

Consider the exact power of \mathfrak{P} dividing each ideal

$$\langle p\pi^{p-1} \rangle, \langle (p-1)a_{p-1}\pi^{p-2} \rangle, \dots, \langle 2a_2\pi \rangle, \langle a_1 \rangle$$

generated by a term of $M'(\pi)$. Now, if $p^{b_i} \parallel a_i$, then $\mathfrak{P}^{b_i p} \parallel \langle a_i \rangle$ because $\langle p \rangle = \mathfrak{P}^p$. Now $p \nmid 1, \dots, p-1$ implies $\mathfrak{P} \nmid \langle 1 \rangle, \dots, \langle p-1 \rangle$, and the only other power of \mathfrak{P} that can occur in the i th term (from the right) is that in $\langle \pi^{i-1} \rangle = \langle \pi \rangle^{i-1}$. Now, $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$ implies $\mathfrak{P}^{i-1} \parallel \langle \pi \rangle^{i-1}$, and the i th term has exact divisor $\mathfrak{P}^{b_i p + i - 1}$ for $i = 1, \dots, p-1$. The p th term clearly has exact divisor \mathfrak{P}^{2p-1} . Notice that these exponents are all distinct modulo p ; hence they are all distinct.

We now apply Lemma 7.14. Because the exponents considered above are all distinct, it follows by Lemma 7.14 that k is the minimum of these exponents, and since each exponent is at least p , we have $k \geq p$. On the other hand, the exponent in the term $p\pi^{p-1}$ was explicitly calculated to be $2p-1$. Hence,

$$p \leq k \leq 2p-1.$$

Now since $p > 2$,

$$1 < \frac{p}{p-1} \leq \frac{k}{p-1} \leq \frac{2p-1}{p-1} = 2 + \frac{1}{p-1} < 3.$$

Thus, $k = 2(p-1)$. Since only \mathfrak{P} is ramified, by Proposition 8.5,

$$\text{Diff}_{\mathbb{K}|\mathbb{Q}}(\mathfrak{o}_{\mathbb{K}}) = \mathfrak{P}^{2(p-1)}.$$

10.4.1 The Case p is odd and $m = 2$

Since p is unramified in $\mathbb{K}_{\mathcal{E}}$ and no other rational prime is ramified in \mathbb{K} , we conclude that no rational prime is ramified in $\mathbb{K}_{\mathcal{E}}$. By Theorem B.2, $\mathbb{K}_{\mathcal{E}} = \mathbb{Q}$, and by Theorem 9.9,

\mathfrak{P} is totally ramified over p .

In other words, $e(\mathfrak{P}|\mathfrak{p}) = p^2$. Thus, $\mathcal{E}(\mathfrak{P}|p)$ has order p^2 . Now, by Theorem 9.16, $\mathcal{E}(\mathfrak{P}|p)/\mathcal{V}_1(\mathfrak{P}|p)$ has order dividing $p-1$, but this group is also a p -group since both \mathcal{E} and \mathcal{V}_1 are p -groups. The only power of p that divides $p-1$ is 1; we conclude that $\mathcal{V}_1(\mathfrak{P}|p)$ has order p^2 .

Let $\mathcal{V}_r(\mathfrak{P}|p)$ be the first ramification group having order $< p^2$. By Theorem 9.20, $\mathcal{V}_{r-1}/\mathcal{V}_r$ has order dividing $\#\mathfrak{o}_{\mathbb{E}}/\mathfrak{P}$, which is p because $f_{\mathfrak{P}} = 1$. Thus

\mathcal{V}_r has order p .

Now, let \mathcal{H} be any subgroup of $\mathcal{G}_{\mathbb{K}|\mathbb{Q}}$ having order p , and let $\mathbb{K}_{\mathcal{H}}$ be the fixed field of \mathcal{H} . Then \mathfrak{P} is totally ramified in the extension $\mathbb{K}|\mathbb{K}_{\mathcal{H}}$. By our calculation in the case when $m = 1$, we have

$$\text{Diff}_{\mathbb{K}_{\mathcal{H}}|\mathbb{Q}}(\mathfrak{o}_{\mathbb{K}_{\mathcal{H}}}) = (\mathfrak{P} \cap \mathbb{K}_{\mathcal{H}})^{2(p-1)}.$$

Since \mathfrak{P} is totally ramified in $\mathbb{K}|\mathbb{K}_{\mathcal{H}}$, which is of degree p , we have

$$\langle \text{Diff}_{\mathbb{K}_{\mathcal{H}}|\mathbb{Q}}(\mathfrak{o}_{\mathbb{K}_{\mathcal{H}}}) \rangle_{\mathfrak{o}_{\mathbb{K}}} = \mathfrak{P}^{2(p-1)p}.$$

By multiplicativity of the different in the tower $\mathbb{Q} \subseteq \mathbb{K}_{\mathcal{H}} \subseteq \mathbb{K}$, we have

$$\text{Diff}_{\mathbb{K}|\mathbb{Q}}(\mathfrak{o}_{\mathbb{K}}) = \text{Diff}_{\mathbb{K}|\mathbb{K}_{\mathcal{H}}}(\mathfrak{o}_{\mathbb{K}}) \mathfrak{P}^{2(p-1)p}.$$

Thus, $\text{Diff}_{\mathbb{K}|\mathbb{K}_{\mathcal{H}}}(\mathfrak{o}_{\mathbb{K}})$ is independent of \mathcal{H} . On the other hand, the exponent of \mathfrak{P} in $\text{Diff}_{\mathbb{K}|\mathbb{K}_{\mathcal{H}}}(\mathfrak{o}_{\mathbb{K}})$ is strictly maximized when $\mathcal{H} = \mathcal{V}_r$, which we now prove.

Proof: By Hilbert's formula, Theorem 9.25, if t' is this exponent, then $t' = \sum (\#\mathcal{V}_m(\mathfrak{P}|\mathfrak{P}_{\mathcal{H}}) - 1)$. We consider each term. Notice that $\mathcal{V}_m(\mathfrak{P}|\mathfrak{P}_{\mathcal{H}}) = \mathcal{V}_m \cap \mathcal{H}$, by applying the definition. Moreover, $\#\mathcal{V}_m \cap \mathcal{H} \leq p$, and is maximized ($= p$) iff $\mathcal{H} \leq \mathcal{V}_m$. For m such that $\#\mathcal{V}_m = p^2$, this maximum is certainly achieved when $\mathcal{H} = \mathcal{V}_r$. On the other hand, for m such that $\#\mathcal{V}_m = p$, this maximum is achieved if and *only if* $\mathcal{V}_r = \mathcal{H}$. Thus we have the desired result. ■

We conclude that $\mathcal{G}_{\mathbb{K}|\mathbb{Q}}$ has only one subgroup of index p , namely \mathcal{V}_r ; hence

$\mathcal{G}_{\mathbb{K}|\mathbb{Q}}$ is cyclic.

10.4.2 Back to $m = 1$

Now, if \mathbb{K} and \mathbb{K}' are two extensions of \mathbb{Q} of degree p , and p is the only prime ramified in either \mathbb{K} or \mathbb{K}' , then the compositum $\mathbb{K}\mathbb{K}'$ is an extension of degree p^2 over \mathbb{Q} , and p is the only prime ramified in $\mathbb{K}\mathbb{K}'$, as argued earlier.

By Subsection 10.4.1, $\mathbb{K}\mathbb{K}'$ has only one subfield of degree p over \mathbb{Q} . This implies that $\mathbb{K}' = \mathbb{K}$, i.e., that \mathbb{K} is unique.

Now, the p^2 th cyclotomic field has cyclic Galois group of order $p(p-1)$, which has a subgroup of index p . The fixed field of this subgroup has degree p

over \mathbb{Q} . We conclude that \mathbf{K} is this unique subfield of the p^2 th cyclotomic field having degree p over \mathbb{Q} .

10.5 The Case p is odd and $m > 1$

Now, the extension $\mathbb{Q}(\zeta_{p^{m+1}})|\mathbb{Q}$ has Galois group $(\mathbb{Z}_{p^{m+1}})^\times$, which is cyclic of order $\phi(p^{m+1}) = p^m(p-1)$. As a cyclic group, there is a unique subgroup of order $p-1$. Let \mathbf{L} be the fixed field of this subgroup. Thus, \mathbf{L} is the unique subfield of $\mathbb{Q}(\zeta_{p^{m+1}})$ of degree p^m over \mathbb{Q} . Then $\mathcal{G}_{\mathbf{L}|\mathbb{Q}}$ has order p^m and is cyclic as a subgroup of a cyclic group (another way of seeing this is by using Subsection 10.4.2).

Now, $[\mathbf{KL} : \mathbb{Q}]$ is a power of p , and p is the only ramified rational prime. Since the extension is abelian, \mathbf{KL} contains a subfield of degree p over \mathbb{Q} , and as discussed in Section 10.4.2, this field is unique. We conclude that the Galois group of \mathbf{KL} is cyclic.

Thus, the product

$$\mathcal{G}_{\mathbf{KL}|\mathbf{K}\mathbf{L}} \cong \mathcal{G}_{\mathbf{K}|\mathbf{K}\mathbf{L}} \times \mathcal{G}_{\mathbf{L}|\mathbf{K}\mathbf{L}}$$

must have one of its factors trivial. In either case, we conclude that $\mathbf{K} = \mathbf{L}$.

This completes the proof of the theorem of Kronecker and Weber.

Appendix A. Notation

Notation	Meaning and Page Where Introduced
$M_{\alpha, k}$	The minimal polynomial of α over k , p. 13
$\mathcal{G}_{E k}$ or $\mathcal{G}(E k)$	The Galois group of the extension $E k$, p. 15
$E_{\mathcal{H}}$	The fixed field of \mathcal{H} , where $\mathcal{H} \leq \mathcal{G}_{E k}$
k^{al}	The algebraic closure of the field k , p. 15
\mathfrak{o}_k	The algebraic integers in k , p. 16
$e(\mathfrak{P} \mathfrak{p}), e_{\mathfrak{P}}$	The ramification index of \mathfrak{P} over \mathfrak{p} , p. 35
$f(\mathfrak{P} \mathfrak{p}), f_{\mathfrak{P}}$	The inertial degree of \mathfrak{P} over \mathfrak{p} , p. 36
$\mathcal{E}(\mathfrak{P} \mathfrak{p})$	The inertia group of \mathfrak{P} over \mathfrak{p} , p. 46
$\mathcal{D}(\mathfrak{P} \mathfrak{p})$	The decomposition group of \mathfrak{P} over \mathfrak{p} , p. 45
$\mathcal{V}_m(\mathfrak{P} \mathfrak{p})$	The ramification groups of \mathfrak{P} over \mathfrak{p} , p. 48
Φ_m	The m th cyclotomic polynomial, p. 23
ϕ	The Euler totient function, p. 22
$\langle \alpha_1, \dots, \alpha_n \rangle$	The ideal generated by $\alpha_1, \dots, \alpha_n$, p. 4
$\langle S \rangle_{\mathfrak{r}}$	The ideal generated by S in \mathfrak{r} , p. 4
$\text{Disc}_{E k}$	The discriminant relative to the extension $E k$, p. 26
$\text{Tr}_{E k}$	The trace relative to the extension $E k$, p. 25
$\text{Diff}_{E k}$	The different relative to the extension $E k$, p. 40
ζ_n	Any primitive n th root of unity, p. 22

$\operatorname{Re}(\zeta)$	The real part of ζ , p. 21
$\operatorname{Im}(\zeta)$	The imaginary part of ζ , p. 21
$\operatorname{Arg}(\zeta)$	The argument of ζ , p. 21
$ \zeta $	The modulus of ζ , p. 21
$p^a \parallel n$	p^a is an exact divisor of n
$(\alpha_{i,j})$	The matrix whose (i, j) entry is $\alpha_{i,j}$
Det	The determinant
$\mathcal{H} \leq \mathcal{G}$	\mathcal{H} is a subgroup of \mathcal{G}
$\mathcal{H} \subsetneq \mathcal{G}$	\mathcal{H} is a proper subgroup of \mathcal{G}
$\mathcal{N} \trianglelefteq \mathcal{G}$	\mathcal{N} is a normal subgroup of \mathcal{G}
$\mathbf{1}$	The group with one element
$S \subseteq T$	S is a subset of T
$\#S$	The cardinality of S
$S \sqcup T$	The disjoint union of S and T

Appendix B. The Minkowski Bound

In a Dedekind domain \mathfrak{D} it is common to define a relation \sim on the class of ideals by

$$\mathfrak{I} \sim \mathfrak{J} \iff (\exists \alpha, \beta \in \mathfrak{D}) \alpha \mathfrak{I} = \beta \mathfrak{J}.$$

It is not difficult to show that this is an equivalence relation, and hence partitions the class of ideals of \mathfrak{D} into equivalence classes. These equivalence classes are known as *ideal classes*. Under multiplication of ideals, the ideal classes can be shown to form a group known as the *ideal class group* or just *class group*. An interesting result is that for any abelian group there is a Dedekind domain with an isomorphic class group [3, p. 735]. Our concern here is only with one result concerning the class groups of number rings.

Assume that \mathbb{K} is an extension of degree $n > 1$ over \mathbb{Q} , and that $\sigma_1, \dots, \sigma_r$ are the monomorphisms $\mathbb{K} \rightarrow \mathbb{C}$ that in fact embed $\mathbb{K} \rightarrow \mathbb{R}$. Then the remaining $n - r$ embeddings $\mathbb{K} \rightarrow \mathbb{C}$ occur in conjugate pairs. The number of these pairs we denote by s (thus $n = r + 2s$).

Theorem B.1 *Every ideal class contains an ideal \mathfrak{J} having norm satisfying*

$$\|\mathfrak{J}\| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\text{Disc}_{\mathbb{K}}|}.$$

The number on the right of the inequality is known as the *Minkowski bound* since it is due to his lemma. For a proof of this result, we refer the reader to [10]. Our concern is only with one application of this result.

Theorem B.2 *Every number field other than \mathbb{Q} has a ramified rational prime.*

Proof: It follows that the Minkowski bound must be at least 1, so

$$\sqrt{|\text{Disc}\mathfrak{o}_K|} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}.$$

Denote this last quantity by b_n . First,

$$b_2 = \frac{2^2}{2!} \left(\frac{\pi}{4}\right)^{2/2} = \frac{\pi}{2} > 1.$$

Next,

$$\frac{b_{n+1}}{b_n} = \frac{\frac{(n+1)^{n+1}}{(n+1)!} \left(\frac{\pi}{4}\right)^{(n+1)/2}}{\frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}} = \left(\frac{n+1}{n}\right)^n \sqrt{\frac{\pi}{4}}.$$

Noting that for $n \geq 1$,

$$\left(\frac{n+1}{n}\right)^n \geq 2,$$

we see that

$$\frac{b_{n+1}}{b_n} \geq 2\sqrt{\frac{\pi}{4}} > 1,$$

so $b_{n+1} > b_n$ for each n . Hence, for $n \geq 2$ we have $b_n > 1$ and $\sqrt{|\text{Disc}\mathfrak{o}_K|} > 1$, that is, $|\text{Disc}\mathfrak{o}_K| > 1$, which means that there is a prime p dividing $\text{Disc}\mathfrak{o}_K$, and hence ramified in $K|\mathbb{Q}$. ■

REFERENCES

- [1] Lars V. Ahlfors. *Complex Analysis*. McGraw-Hill, New York, third edition, 1979.
- [2] M. F. Atiyah and I. G. MacDonal. *Introduction to Commutative Algebra*. Westview, 1969.
- [3] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, New York, second edition, 1999.
- [4] A. Fröhlich and M. J. Taylor. *Algebraic Number Theory*. Cambridge UP, 2000.
- [5] Thomas W. Hungerford. *Algebra*. Springer-Verlag, New York, 1974.
- [6] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, New York, second edition, 2000.
- [7] Kedlaya. The kronecker-weber theorem. course notes, Math 254B, UC Berkeley, Spring 2002.
- [8] Serge Lang. *Algebraic Number Theory*. Springer, New York, second edition, 1991.
- [9] Serge Lang. *Algebra*. Addison Wesley, Reading, MA, third edition, 1993.
- [10] Daniel A. Marcus. *Number Fields*. Springer, New York, 1991.
- [11] Hideyuki Matsumura. *Commutative Ring Theory*. Cambridge UP, 2002. trans. M. Reid from Japanese *Kakan kan ron*, Kyoritsu, Tokyo, 1980.
- [12] J. S. Milne. Algebraic number theory. course notes, Math 676, U Michigan, August 1998.
- [13] Stan Payne. Topics in algebra and number theory with applications to abelian difference sets. 107 pages, January 2005.
- [14] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier Analysis on Number Fields*. Springer, New York, 1998.

- [15] Paulo Ribenboim. *Classical Theory of Algebraic Numbers*. Springer-Verlag, New York, 2001.
- [16] Joseph Rotman. *An Introduction to the Theory of Groups*. Springer-Verlag, New York, fourth edition, 1995.
- [17] Pierre Samuel. *Algebraic Theory of Numbers*. Houghton Mifflin, Boston, 1970. trans. Allan J. Silberger from French *Théorie algébrique des nombres*, Hermann, Paris, 1967.
- [18] B. L. van der Waerden. *Algebra, Volume I*. Springer, New York, 2000. trans. Fred Blum and John R. Schulenberger from German *Algebra I*, Springer-Verlag, Berlin, seventh edition, 1966.
- [19] B. L. van der Waerden. *Algebra, Volume II*. Springer, New York, 2000. trans. John R. Schulenberger from German *Algebra II*, Springer-Verlag, Berlin, fifth edition, 1967.
- [20] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, New York, second edition, 1996.
- [21] Oscar Zariski and Pierre Samuel. *Commutative Algebra, Volume 1*. Van Nostrand, Princeton, 1958.