Cornell University Mathematics Department Senior Thesis

# Inverse Galois Problem for Totally Real Number Fields

Sudesh Kalyanswamy

Class of 2012

April, 2012

Advisor: Prof. Ravi Ramakrishna, Department of Mathematics

**Abstract**

In this thesis we investigate a variant of the Inverse Galois Problem. Namely, given a finite group $G$, the goal is to find a totally real extension $K/\mathbb{Q}$, necessarily finite, such that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $G$. Questions regarding the factoring of primes in these extensions also arise, and we address these where possible.

The first portion of this thesis is dedicated to proving and developing the requisite algebraic number theory. We then prove the existence of totally real extensions in the cases where $G$ is abelian and where $G = S_n$ for some $n \geq 2$. In both cases, some explicit polynomials with Galois group $G$ are provided. We obtain the existence of totally real $G$-extensions of $\mathbb{Q}$ for all groups of odd order using a theorem of Shafarevich, and also outline a method to obtain totally real number fields with Galois group $D_{2p}$, where $p$ is an odd prime.

In the abelian setting, we consider the factorization of primes of $\mathbb{Z}$ in the constructed totally real extensions. We prove that the primes 2 and 5 each split in infinitely many totally real $\mathbb{Z}/3\mathbb{Z}$-extensions, and, more generally, that for primes $p$ and $q$, $p$ will split in infinitely many $\mathbb{Z}/q\mathbb{Z}$-extensions of $\mathbb{Q}$.

**Acknowledgements**

I would like to thank Professor Ravi Ramakrishna for all his guidance and support throughout the year, as well as for the time he put into reading and editing the thesis. I would also like to thank the Hunter R. Rawlings III Cornell Presidential Research Scholars Program for their financial support over the last four years.

# Contents

# Chapter 1

# Introduction

This thesis investigates a variant of the Inverse Galois Problem, which is an open problem in number theory. Given a polynomial or a field extension, one could calculate its Galois group, and though this can be difficult, especially for polynomials of large degree, it is "doable." Different methods for calculating Galois groups are used continuously throughout this thesis, so those not familiar with these methods (or terms) should consult Appendices A-C.

The Inverse Galois Problem is Galois theory "in reverse." Namely, given a finite group $G$, the question is whether $G$ occurs as a Galois group of some (finite) extension of $\mathbb{Q}$. If $\mathbb{Q}$ is not required to be the base field, then it is a theorem that every finite group occurs as the Galois group of *some* finite extension of fields. However, over $\mathbb{Q}$, the problem is not yet solved. And even for groups for which the problem is solved, another difficulty is actually producing a polynomial in $\mathbb{Q}[x]$ with the prescribed Galois group.

This is not to say that no progress has been made. For example, the following theorem of Shafarevich solves the problem for a whole class of groups, from [10].

**Theorem 1.0.1.** *If $G$ is a finite solvable group, then $G$ occurs as a Galois group over $\mathbb{Q}$.*

However, the proof Shafarevich provided did not include explicit polynomials.

In this thesis, the problem is amended slightly by adding another restriction to the possible fields. Not only do we want our fields to be finite extensions of $\mathbb{Q}$, we require that they be *totally real*, which we will define in the next chapter. As expected, this makes the problem slightly more challenging for some classes of groups.

Chapter 2 serves as an introduction to most of the algebraic number theory

needed for this thesis, including the ring of integers, factorizations of ideals in extensions, decomposition and inertia groups, and the Frobenius automorphism. Chapter 3 addresses the abelian case. We prove that all finite abelian groups occur as Galois groups of totally real fields, and also study how primes of $\mathbb{Z}$ factor in these extensions. For example, we calculate the Dirichlet density of the primes which split completely in these totally real extensions. These terms are defined in chapters 2 and 3. We begin chapter 4 by providing a brief introduction to $p$-adic numbers, which we then use to prove that $S_n$ can be realized as a Galois group of a totally real number field. Lastly, we outline a method to obtain $D_{2p}$ as a Galois group over $\mathbb{Q}$, again of a totally real field, in chapter 5. Appendices A-C cover most of the definitions and theorems from Field Theory and Galois Theory which are required to understand the material in the main portion of the thesis.

# Chapter 2

# Algebraic Number Theory

In this chapter, we introduce most of the algebraic number theory needed for this thesis. The primary motivation for writing this chapter is to provide as self-contained a thesis as possible, but almost all of these theorems can be found in other books, and we cite them along the way. Of course, there will be some results which we will not have the time to prove, but we state them and refer to them as needed.

## 2.1 Introduction to Number Fields

### 2.1.1 Definition and Embeddings

This thesis is concerned with *totally real number fields*. In this section, the goal is to explain what these are, as well as introduce the norm and the trace. We will be following the beginning of [6].

**Definition 2.1.1.** A *number field* $K$ is a finite extension of $\mathbb{Q}$. The dimension $\dim_{\mathbb{Q}} K$ of $K$ as a vector space over $\mathbb{Q}$ is called the *degree* of the number field, and is denoted $[K : \mathbb{Q}]$.

For example, $K = \mathbb{Q}(\sqrt{2})$ is a number field of degree two and $L = \mathbb{Q}(2^{1/3})$ is a number field of degree three. It is important to note that a number field is not necessarily a Galois extension of $\mathbb{Q}$, as the second example shows, but many of the results we will prove become considerably nicer (or easier) when dealing with Galois extensions.

All number fields are simple extensions of $\mathbb{Q}$. That is, a number field $L$ has the form $L = \mathbb{Q}(\alpha)$ for some element $\alpha \in L$. This follows from the following theorem, which is only stated. A proof can be found in [5], page 595.

**Theorem 2.1.2** (Primitive Element Theorem)**.** *If $K/F$ is a finite, separable field extension, then $K/F$ is a simple extension.*

Since $\mathbb{Q}$ has characteristic zero, all finite extensions are separable (Theorem A.3.5), and the theorem applies to all number fields. There do exist extensions which are not simple, but by the above reasoning they necessarily have characteristic $p$ for some prime $p$. This theorem gives us a useful way of working with number fields since they can be generated by one element.

Now suppose $L = \mathbb{Q}(\alpha)$ is a number field of degree $n$. Since $\mathbb{C}/\mathbb{Q}$ is algebraically closed, $L$ can be regarded as a subfield of $\mathbb{C}$. But there could be several ways of embedding $L$ into $\mathbb{C}$. For example, if $L = \mathbb{Q}(\sqrt{2})$, then an embedding (i.e. an injective homomorphism) $\sigma : L \hookrightarrow \mathbb{C}$ can map $\sqrt{2}$ to either $\sqrt{2}$ or $-\sqrt{2}$. For readers who like to view $\mathbb{Q}(\sqrt{2})$ as $\mathbb{Q}[x]/(x^2 - 2)$, this amounts to saying an embedding

$$\sigma : \mathbb{Q}[x]/(x^2 - 2) \hookrightarrow \mathbb{C}$$

sends $x$ to either $\sqrt{2}$ or $-\sqrt{2}$ since these are the roots of $x^2 - 2 \in \mathbb{Q}[x]$. This is the spirit of the following theorem.

**Theorem 2.1.3.** *Suppose $L = \mathbb{Q}(\alpha)$ is a number field of degree $n$. Then there are exactly $n$ distinct embeddings $\sigma_i : L \hookrightarrow \mathbb{C}$, $i = 1, 2, \ldots, n$.*

*Proof.* Write $L = \mathbb{Q}[x]/(m_\alpha(x))$, where $m_\alpha(x) \in \mathbb{Q}[x]$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$. Any embedding

$$\sigma : \mathbb{Q}[x]/(m_\alpha(x)) \hookrightarrow \mathbb{C}$$

must send $x$ to one of the roots of $m_\alpha(x)$ in $\mathbb{C}$. Since $m_\alpha(x)$ is irreducible over $\mathbb{Q}$ and $\mathbb{Q}$ is of characteristic zero, all roots of $m_\alpha(x)$ are distinct. More specifically, let $M$ denote the splitting field of $m_\alpha(x)$. Then as $M$ is finite and $\mathbb{Q}$ is of characteristic zero, by Theorem A.3.5, $M$ is separable over $\mathbb{Q}$, and since $m_\alpha(x)$ is irreducible it has distinct roots in $M$ by definition of a separable extension. Hence there are at most $n$ embeddings, one for each root of $m_\alpha(x)$ in $\mathbb{C}$.

Conversely, let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ denote the $n$ roots of $m_\alpha(x)$ in $\mathbb{C}$. Let

$$\sigma_i : \mathbb{Q}[x] \hookrightarrow \mathbb{C}$$

send $x$ to $\alpha_i$. Therefore $\sigma(f(x)) = f(\alpha_i)$. It is left to the reader show that this substitution map is a homomorphism, and that kernel of $\sigma_i$ is $(m_\alpha(x))$ (easily verified). By the first isomorphism theorem, $\sigma_i$ induces an injective homomorphism

$$\overline{\sigma}_i : \mathbb{Q}[x]/(m_\alpha(x)) \hookrightarrow \mathbb{C}.$$

This shows there are at least $n$ embeddings, meaning there are precisely $n$ embeddings. □

If $L$ is a number field of degree $n$, then an embedding $\sigma : L \hookrightarrow \mathbb{C}$ is called a *real embedding* if $\sigma(L) \subseteq \mathbb{R}$, i.e. if the image of $L$ under $\sigma$ sits inside the reals. Otherwise, $\sigma$ is referred to as a complex embedding. A *totally real number field* is a number field for which all the embeddings are real. For example, $\mathbb{Q}(\sqrt{2})$ is a totally real number field of degree two, because its two embeddings (seen above) are both real embeddings. However, $\mathbb{Q}(\sqrt[3]{2})$ (the subfield of $\mathbb{C}$) is not a totally real number field since there are two complex embeddings, one sending $\sqrt[3]{2}$ to $\omega\sqrt[3]{2}$ and another sending $\sqrt[3]{2}$ to $\omega^2\sqrt[3]{2}$, where $\omega$ is a cube root of unity (since $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$ are the three roots of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$).

However, what this second example does illustrate is that if $\sigma$ is a complex embedding, then its complex conjugate $\overline{\sigma}$ is also a complex embedding, since complex roots of polynomials over $\mathbb{R}$ (and hence over $\mathbb{Q}$) come in conjugate pairs. For this reason, we usually refer to the number of real embeddings and pairs of complex embeddings. More specifically, if $L$ is a number field of degree $n$, then we let $r_1$ be the number of real embeddings and $r_2$ be the number of pairs of complex embeddings. Since there are $n$ total embeddings, we have $r_1 + 2r_2 = n$.

### 2.1.2 Norm and Trace

#### Definition and Properties

In this section, we introduce two important functions on number fields: the norm and the trace. Although this thesis is concerned with number fields, we will work in a more general setting for much of this chapter. We will mainly be following [9].

Suppose $L/K$ is a finite extension of fields. For an element $\alpha \in L$, consider the map

$$r_\alpha : L \to L, \quad x \mapsto \alpha x.$$

By regarding $L$ as a vector space over $K$, it is clear that $r_\alpha$ is a $K$-linear transformation on $L$.

Next recall two terms from linear algebra: the *trace* and the *determinant* of a linear transformation. If $T : V \to V$ is a linear transformation, then the trace and determinant of $T$ are just the trace and determinant of the matrix of $T$ with respect to some basis of $V$. However, what makes the trace and determinant particularly interesting is that they do not depend on the choice of basis of $V$. This follows from the following facts.

**Proposition 2.1.4.** *If $A$ and $B$ are two square matrices of the same size, then:*

*(i)* $tr(AB) = tr(BA)$

*(ii)* $\det(AB) = \det(A)\det(B)$

If $A$ and $B$ are matrices of $T$ with respect to two different bases of $V$, then from linear algebra there exists an invertible matrix $P$ such that

$$A = PBP^{-1}.$$

Consequently, by the proposition,

$$\mathrm{tr}(A) = \mathrm{tr}(PBP^{-1}) = \mathrm{tr}(P^{-1}PB) = \mathrm{tr}(B),$$

and

$$\det(A) = \det(PBP^{-1}) = \det(P)\det(B)\det(P^{-1}) = \det(P)\det(B)\det(P)^{-1} = \det(B).$$

Hence the trace and determinant of a linear transformation do not depend on the choice of basis of the vector space $V$. Also, if the underlying field of the vector space $V$ is $F$, say, then because entries of the matrix of $T$ are elements of $F$, it easy to see that the trace and determinant will also be elements of $F$.

We can now define the norm and trace.

**Definition 2.1.5.** Suppose $L/K$ is a finite extension of fields.

1. The *trace* of $L/K$ is the function $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}(r_\alpha)$.
2. The *norm* of $L/K$ is the function $\mathrm{Norm}_{L/K}(\alpha) = \det(r_\alpha)$.

From the discussion above, the trace and norm do not depend on the choice of basis of $L$ as a vector space over $K$; they just depend on $L$ and $K$. With the way the trace and norm are defined, some easy properties follow.

**Proposition 2.1.6** (Norm and Trace Properties)**.** *Let $L/K$ be a finite extension of fields with $n = [L : K]$, and suppose $\alpha, \beta \in L$ and $c \in K$. Then the following hold:*

*(i)* $Tr_{L/K}(\alpha), Norm_{L/K}(\alpha) \in K$.

*(ii)* $Tr_{L/K}(\alpha + \beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta)$.

*(iii)* $Tr_{L/K}(c\alpha) = cTr_{L/K}(\alpha)$.

*(iv)* $Norm_{L/K}(\alpha\beta) = Norm_{L/K}(\alpha)Norm_{L/K}(\beta)$.

*(v)* $Norm_{L/K}(c\alpha) = c^n Norm_{L/K}(\alpha)$.

*Proof.* Property (i) follows from the observations preceding the definition. For the next two properties, we first notice that $r_{\alpha+\beta} = r_\alpha + r_\beta$ and $r_{c\alpha} = cr_\alpha$ for all $\alpha, \beta \in L$, $c \in K$ (this is easy). Applying the trace operator to both sides of both relations and using the linearity of the trace operator on matrices give properties (ii) and (iii). Taking the determinant of both sides in the second relation gives property (v). Finally, we have the easy relation: $r_{\alpha\beta} = r_\alpha r_\beta$ (a composition of maps). Taking determinants of both sides and using Proposition 2.1.4(2) yields property (iv). □

The proof shows that the trace is a linear operator on $L$ as a vector space over $K$, essentially because the trace operator on matrices is linear. Also, the proposition says the norm is multiplicative. Both of these are useful facts. Now before moving on, let us look at an example.

**Example 2.1.7.** Consider $\mathbb{Q}(i)/\mathbb{Q}$ (the subfield of $\mathbb{C}$). This is a degree two extension as $i$ is a root of the (irreducible) polynomial $x^2 + 1 \in \mathbb{Q}[x]$. We can consider an arbitrary element $a + bi \in \mathbb{Q}(i)$ $(a, b \in \mathbb{Q})$ and ask what

$$\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi) \quad \text{and} \quad \mathrm{Norm}_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi)$$

are. We just work with the definitions. We first need to find $r_{a+bi}$. To do this, take the basis $\{1, i\}$ for $\mathbb{Q}(i)$. Simple computations show

$$(a + bi) \cdot 1 = a + bi \quad \text{and} \quad (a + bi) \cdot i = -b + ai.$$

Therefore the $2 \times 2$ matrix $r_{a+bi}$ is

$$r_{a+bi} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

So

$$\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi) = \mathrm{tr}(r_{a+bi}) = 2a$$

and

$$\mathrm{Norm}_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi) = \det(r_{a+bi}) = a^2 + b^2.$$

Those who recall the definition of the *norm* of an element of $\mathbb{C}$ will notice that the norm $\mathrm{Norm}_{\mathbb{Q}(i)/\mathbb{Q}}$ agrees with the usual norm on $\mathbb{C}$.

### A Different Definition

It turns out that there is another way to define the trace and norm. Consider the number field case first. Let $L/\mathbb{Q}$ be a number field. If $n = [L : \mathbb{Q}]$, we can let $\{\sigma_i : i = 1, 2, \ldots, n\}$ be the $n$ embeddings of $L$ into $\mathbb{C}$. Then for $\alpha \in L$,

$$\mathrm{Tr}_{L/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha),$$

and

$$\mathrm{Norm}_{L/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) \cdots \sigma_n(\alpha).$$

We can redo Example 2.1.7 using the two embeddings

$$\sigma_1 : \mathbb{Q}(i) \hookrightarrow \mathbb{C}, i \mapsto i,$$

$$\sigma_2 : \mathbb{Q}(i) \hookrightarrow \mathbb{C}, i \mapsto -i.$$

Notice

$$\sigma_1(a + bi) = a + bi \quad \text{and} \quad \sigma_2(a + bi) = a - bi,$$

and therefore

$$\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = a+bi+(a-bi) = 2a$$

and

$$\mathrm{Norm}_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = (a+bi)(a-bi) = a^2+b^2,$$

which are the same answers as the ones above. So the two definitions are consistent, at least in this example. Ideally, we should be able to use our original definition to somehow prove that the trace and norm are given by the sum and product of the embeddings. This is what we aim to do now. The proof follows the one presented in [9], Section 1.5.

**Definition 2.1.8.** Let $L/K$ be a finite extension of fields and suppose $\alpha \in L$. Then the *characteristic polynomial* of $\alpha$ acting on $L$ is the polynomial in $t$ given by

$$c_{L/K}(t) = \det(tI - r_\alpha).$$

The reader will notice that in the notation $c_{L/K}(t)$, there is no $\alpha$, but it is inherent in the matrix $r_\alpha$.

Observe that $c_{L/K}(t)$ is in fact monic. Also, the Cayley-Hamilton theorem tells us that $c_{L/K}(r_\alpha) = 0$. However, by definition of $r_\alpha$, we can also view $c_{L/K}(r_\alpha)$ as a $K$-linear transformation on $L$ which multiplies each element of $L$ by $c_{L/K}(\alpha)$, since $r_\alpha$ was multiplication by $\alpha$. Therefore the statement $c_{L/K}(r_\alpha) = 0$ implies $c_{L/K}(\alpha) = 0$. This will be important later. Now, let us prove the following lemma.

**Lemma 2.1.9.** *Suppose $A = [a_{i,j}]$ is an $n \times n$ matrix with coefficients in some field, and let $I_n$ represent the $n \times n$ identity matrix. Then the coefficient of $t^{n-1}$ in $\det(tI_n - A)$ is $-tr(A)$.*

*Proof.* The proof will be by induction on $n$. The statement is clearly true for $n = 1, 2$ (after a small calculation for the $n = 2$ case). So let $n > 2$, and assume the statement is true for matrices of size smaller than $n$. We will expand the determinant along column $n$. If $B$ is the $(n-1) \times (n-1)$ matrix formed by removing the $n$-th row and column from $A$, then

$$\det(tI_n - A) = (t - a_{n,n}) \det(tI_{n-1} - B) + \ldots.$$

Crucially, the order of $t$ in the omitted terms will be (strictly) less than $n-1$. This is easily verified as the last entry in the $n$-th column will be the only entry with a $t$-factor, and each of the other subdeterminants will have an order of $t$ of only $n-2$. Therefore the only way to get a term with $t^{n-1}$ is from $(t - a_{n,n}) \det(tI_{n-1} - B)$. At this point we can use the induction hypothesis to see

$$\begin{aligned}
(t - a_{n,n}) \det(tI_{n-1} - B) &= (t - a_{n,n})(t^{n-1} - \mathrm{tr}(B)t^{n-2} + \ldots) \quad \text{(ind. hypothesis)} \\
&= t^n - \mathrm{tr}(B)t^{n-1} - a_{n,n}t^{n-1} + \ldots \\
&= t^n - (\mathrm{tr}(B) + a_{n,n})t^{n-1} + \text{lower order terms} \\
&= t^n - \mathrm{tr}(A)t^{n-1} + \text{lower order terms},
\end{aligned}$$

which proves the lemma. □

With this lemma, we can make some observations about the characteristic polynomial of $\alpha$ acting on $L/K$, where $[L : K] = n$ . Since

$$c_{L/K}(t) = \det(tI - r_\alpha),$$

the lemma tells us that the coefficient of $t^{n-1}$ is

$$-\mathrm{tr}(r_\alpha) = -\mathrm{Tr}_{L/K}(\alpha).$$

Plugging in $t = 0$ to $c_{L/K}(t)$ shows the constant term of $c_{L/K}(t)$ is

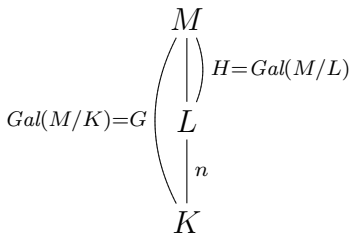
$$\det(-r_\alpha) = (-1)^n \det(r_\alpha) = (-1)^n \mathrm{Norm}_{L/K}(\alpha).$$

Since the norm and the trace are both encoded in the characteristic polynomial, one would imagine that working with the characteristic polynomial will yield information on the norm and trace. We can now state and prove the main theorem.

**Theorem 2.1.10.** *Suppose*

$$K \subseteq L \subseteq M$$

*is a chain of separable extensions, with $M$ also Galois over $K$ (normal and separable), and let $n = [L : K]$. Let $G = Gal(M/K)$ and $H = Gal(M/L)$. By the Galois correspondence (Theorem A.3.10), $H \leq G$ is a subgroup.*




*Since $[G : H] = n$, let*

$$\{\sigma_i H : i = 1, 2, \ldots, n\}$$

*be the $n$ distinct left cosets of $H$ in $G$. In this way, the $\sigma_i$ are (distinct) embeddings of $L$ into the normal extension $M$ of $K$. Then for $\alpha \in L$,*

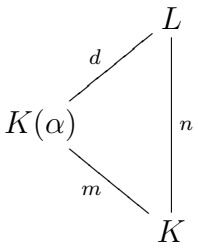
*(i)* $Tr_{L/K}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha)$, *and*

*(ii)* $Norm_{L/K}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) \cdots \sigma_n(\alpha)$.

*Proof.* Let $\alpha \in L$ and let $m_K(t) \in K[t]$ be the minimal polynomial of $\alpha$ over $K$. Then $m_K(t)$ is the characteristic polynomial of $\alpha$ acting on $K(\alpha)/K$. To see why, first recall that $c_{K(\alpha)/K}(\alpha) = 0$ (see remarks following Definition 2.1.8), and

therefore $m_K(t)|c_{K(\alpha)/K}(t)$. But since both are monic of degree $[K(\alpha) : K]$, in fact $m_K(t) = c_{K(\alpha)/K}(t)$. So now let

$$[L : K(\alpha)] = d \quad \text{and} \quad [K(\alpha) : K] = m.$$




Then $L$ is a vector space direct sum of $d$ copies of $K(\alpha)$ (it is a degree $d$ vector space over $K(\alpha)$), and the claim is that the characteristic polynomial of $\alpha$ acting on $L$ is $c_{L/K}(t) = m_K(t)^d$.

To prove this claim, let $A$ be the matrix of $\alpha$ acting on $K(\alpha)$. Since $L$ is the direct sum of $d$ copies of $K(\alpha)$, we can take $d$ linearly independent copies of the basis for $K(\alpha)/K$ and use that as a basis of $L$. Therefore, in this basis,

$$r_\alpha = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix}.$$

Consequently,

$$tI_{md} - r_\alpha = \begin{pmatrix} tI_m - A & 0 & \cdots & 0 \\ 0 & tI_m - A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & tI_m - A \end{pmatrix}.$$

Since the determinant of a block diagonal matrix is the product of the determinants of the individual blocks, we find

$$\det(tI_{md} - r_\alpha) = \det(tI_m - A)^d = c_{K(\alpha)/K}(t)^d = m_K(t)^d,$$

which proves the claim.

Next, since $m_K(t)$ is an irreducible polynomial of degree $m$ and $M$ is normal and separable over $K$, we can let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ be the $m$ distinct roots of $m_K(t)$ in $M$, meaning

$$m_K(t) = \prod_{i=1}^{m} (t - \alpha_i).$$

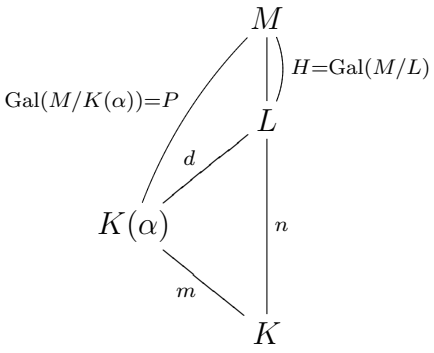
By Lemma 2.1.9 and the subsequent notes tell, $\mathrm{Tr}_{L/K}(\alpha)$ is the sum of the roots of the characteristic polynomial of $\alpha$ acting on $L$, and $\mathrm{Norm}_{L/K}(\alpha)$ is the product of the roots. Since the characteristic polynomial is $m_K(t)^d$ which has roots $\alpha_i : i = 1, 2, \ldots, m$, each with multiplicity $d$, we have

$$\mathrm{Tr}_{L/K}(\alpha) = d(\alpha_1 + \alpha_2 + \ldots + \alpha_m),$$

and

$$\mathrm{Norm}_{L/K}(\alpha) = (\alpha_1 \alpha_2 \cdots \alpha_m)^d.$$

Let $P = \mathrm{Gal}(M/K(\alpha))$.




The Galois Correspondence (A.3.10) says $H \leq P$. Moreover, $d = [P : H]$ and $m = [G : P]$. Choose coset representatives $\beta_i$ so that

$$\{\beta_i P : i = 1, 2, \ldots, m\}$$

are the distinct cosets of $P$ in $G$ and similarly choose representatives $\gamma_j$ so that

$$\{\gamma_j H : j = 1, 2, \ldots, d\}$$

are the distinct cosets of $H$ in $P$. Then the set

$$\{\beta_i \gamma_j : i = 1, 2, \ldots, m; j = 1, 2, \ldots, d\}$$

is a choice of coset representatives of $H$ in $G$. Notice that since the $\gamma_j \in P = \mathrm{Gal}(M/K(\alpha))$, we have $\gamma_j(\alpha) = \alpha$ for all $j$. Moreover, by reordering, we can ensure $\beta_i(\alpha) = \alpha_i$ for all $i$. From the setup preceding the theorem, the $\sigma_i$ were also coset representatives for $H$ in $G$, and therefore they differ from the elements $\beta_i \gamma_j$ by elements of $H$, all of which leave $\alpha$ fixed. Therefore

$$\begin{aligned}
\sum_{k=1}^{n} \sigma_k(\alpha) &= \sum_{i=1}^{m} \sum_{j=1}^{d} \beta_i \gamma_j(\alpha) \\
&= d \sum_{i=1}^{m} \beta_i(\alpha) \quad (\text{since } \gamma_j(\alpha) = \alpha) \\
&= d \sum_{i=1}^{m} \alpha_i \quad (\text{as } \beta_i(\alpha) = \alpha_i) \\
&= \mathrm{Tr}_{L/K}(\alpha).
\end{aligned}$$

Similarly,

$$\begin{aligned}
\prod_{k=1}^{n} \sigma_k(\alpha) &= \prod_{i=1}^{m}\prod_{j=1}^{d} \beta_i\gamma_j(\alpha) \\
&= \left(\prod_{i=1}^{m} \beta_i(\alpha)\right)^d \quad (\text{since } \gamma_j(\alpha) = \alpha) \\
&= \left(\prod_{i=1}^{m} \alpha_i\right)^d \quad (\text{as } \beta_i(\alpha) = \alpha_i) \\
&= \text{Norm}_{L/K}(\alpha).
\end{aligned}$$

□

Since number fields are finite extensions of $\mathbb{Q}$, which has characteristic zero, all number fields are separable, and so the theorem applies. Notice that if a number field is also Galois over $\mathbb{Q}$, then the theorem applies with $L = M$, meaning the $\sigma_i$ are just the elements of the Galois group.

## 2.2 Dedekind Domains and Ideal Factorization

The next step in the development of this material would be to examine the so called ring of integers. But before we do, we will use this section to prove the unique factorization of ideals in Dedekind rings. Once this is done, we can introduce the ring of integers and explain how the results of this section apply to that ring. Since it is an important result which we will be utilizing regularly throughout this chapter and the subsequent ones, it is worthwhile to go through this proof, despite the amount of space it will require. The lemmas, theorems, and proofs are all from [9], with the exception of the section on Noetherian rings.

### 2.2.1 Localization

The first concept to introduce is that of localization. In topology, one way to understand a certain space is to look at the local behavior around each point in the space, and then somehow combine all this information to yield a greater understanding of the space as a whole. This is the motivation behind "localization."

Recall the definitions of prime and maximal ideals:

**Definition 2.2.1.** If $R$ is a ring and $I$ is an ideal with $I \neq R$, then $I$ is said to be *prime* if whenever $ab \in I$, then either $a \in I$ or $b \in I$. The ideal $I$ is said to be *maximal* the only ideals containing $I$ are $R$ and $I$. That is, there is no ideal $J$ with $I \subset J \subset R$.

These should be fairly familiar concepts. In ring theory, the points of the associated "topological space" are the prime ideals of the ring, and the topology is the Zariski topology. For this reason, we want to understand localization at prime ideals.

Localization is actually defined more generally. Suppose $R$ is a ring which is an integral domain (no zero divisors), and let $S$ be a subset of $R$ which is multiplicative and does not contain zero. The set $S$ does not need to be a subring or even an ideal of $R$; the only requirement is that the product of two elements of $S$ is also in $S$. Consider the set $R \times S$ with the equivalence relation

$$(r, s) \sim (r', s') \Leftrightarrow rs' = r's.$$

This is in fact an equivalence relation, as the reader can easily verify. Typically, the equivalence class of $(r, s)$ is denoted $r/s$. The addition and multiplication on the set of equivalence classes of $R$ (under this relation) are defined as follows:

$$r/s + r'/s' = (rs' + r's)/(ss')$$

and

$$(r/s)(r'/s') = rr'/ss'.$$

It is another exercise for the reader to check that these operations are well-defined. The set of equivalence classes with these two operations form a ring, denoted $R_S$ (or sometimes $S^{-1}R$), called the localization of $R$ at $S$. It is easy to see that $0/s$ is the zero element and $s/s$ the identity element (here $s$ is any element of $S$). Moreover, choosing one $s \in S$ we find that the map

$$R \to R_S, \quad r \mapsto rs/s$$

is an embedding of $R$ into $R_S$. We choose any element $s$ instead of 1 since 1 is not assumed to be in $S$. The reader might recall that the field of fractions of a ring is constructed in a similar manner. In fact, if $S = R\backslash\{0\}$, then as $R$ has no zero divisors, $S$ is multiplicative and $R_S$ is the field of fractions of $R$. However, this definition of localization allows us to insert a wide variety of sets in for $S$.

**Example 2.2.2.** $R = \mathbb{Z}$ and $S = \{1, 4, 16, 64, \ldots\}$. Then $S$ is clearly a multiplicative subset of $R$ that does not contain zero. It is clear from the definition of $R_S$ that in this case

$$R_S = \{a/4^k : a, k \in \mathbb{Z}\}.$$

**Example 2.2.3.** Let $R = \mathbb{Z}$, but this time let $S$ be the set of integers not divisible by 5. This is also a multiplicative set because if two numbers are not divisible by 5 then their product cannot be divisible by 5 by the Fundamental Theorem of Arithmetic. Hence

$$R_S = \{a/b : a, b \in \mathbb{Z}, 5 \not| b\}.$$

We can look at this second example more generally. Indeed, the ideal $(5) \subset \mathbb{Z}$ is a prime ideal, so if $x$ and $y$ are two elements with $x, y \notin (5)$, then by definition of a prime ideal $xy \notin (5)$. This means the set $\mathbb{Z} - 5\mathbb{Z}$ forms a multiplicative set. Replacing $\mathbb{Z}$ and $(5)$ by a more general integral domain $R$ and prime ideal $\mathfrak{p}$ gives the localization at a prime ideal.

**Definition 2.2.4.** Let $R$ be an integral domain and $\mathfrak{p}$ a prime ideal. Then the localization of $R$ at $\mathfrak{p}$ is $R_{R-\mathfrak{p}}$.

To avoid writing $R-\mathfrak{p}$ continuously, the localization at $\mathfrak{p}$ is denoted $R_{\mathfrak{p}}$. However, try not to be confused and think that $\mathfrak{p}$ is the set $S$ in our definition of localization.

The last proposition we state in this section is the relationship between ideals of our original ring $R$ and ideals of the localization $R_S$. We will not prove the proposition, but a proof can be found in [9], Section 1.1.

**Proposition 2.2.5.** *Suppose $R$ is an integral domain and $S$ a multiplicative subset of $R$ (which does not contain zero). Then there is a 1-1 correspondence between the prime ideals of $R$ which have empty intersection with $S$ and prime ideals of $R_S$. More specifically, if $\mathfrak{p}$ is a prime ideal of $R$ with $\mathfrak{p} \cap S = \emptyset$, then the ideal $\mathfrak{p}$ corresponds to an ideal $\mathfrak{p}R_S$ of $R_S$.*

We also get the following corollary.

**Corollary 2.2.6.** *If $R$ is an integral domain and $\mathfrak{p}$ a prime ideal, then $R_{\mathfrak{p}}$ has only one maximal ideal, namely $\mathfrak{p}R_{\mathfrak{p}}$.*

*Proof.* Remembering that the localization at $\mathfrak{p}$ means $S = R - \mathfrak{p}$, the correspondence given by the proposition tells us that $\mathfrak{p}R_{\mathfrak{p}}$ is a prime ideal of $R_{\mathfrak{p}}$. Moreover, if it were properly contained in a maximal ideal $\mathfrak{q}R_{\mathfrak{q}}$, then since maximal ideals are always prime (general fact from ring theory; verify if need be), this would correspond to an ideal $\mathfrak{q}$ of $R$ which properly contains $\mathfrak{p}$ and has empty intersection with $R - \mathfrak{p}$, which is a clear contradiction. Hence $\mathfrak{p}R_{\mathfrak{p}}$ is a maximal ideal. The correspondence also tells us that there cannot be any others, since any other maximal ideal would have to correspond to an ideal of $R$ properly contained in $\mathfrak{p}$, and hence the ideal would be properly contained in $\mathfrak{p}R_{\mathfrak{p}}$, contradicting maximality. □

### 2.2.2 Noetherian Rings and Modules

#### Rings

There are two equivalent ways of defining Dedekind rings. One makes uses the word Noetherian and the other does not. However, since many of the theorems and lemmas make use of the word Noetherian, we will define the term and define Dedekind rings appropriately. The definition, along with the rest of the section, can be found in [5].

**Definition 2.2.7.** A commutative ring $R$ is *Noetherian* if whenever

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

is an increasing chain of ideals of $R$, there exists $n$ such that $I_m = I_n$ for all $m \geq n$.

So a ring is Noetherian if you cannot find an infinite (strictly) increasing chain of ideals. The ring in the definition is required to be commutative. For our purposes, this is fine, since we will be using subrings of our number fields, which are consequently commutative. There is a way to define a Noetherian condition for nonncommutative rings which is similar, but we will not go into that here since it is not needed. But in case we fail to characterize rings as commutative in this section, it is worth noting now that all rings in this section are assumed to be commutative.

We will see that Dedekind rings must be Noetherian (by definition), but in the proof of the unique factorization of ideals we will also need the fact that quotients of Noetherian rings are Noetherian as well. First, let us recall a fact from ring theory. If $R$ is a ring and $I$ an ideal, then there is a one-to-one correspondence

$$\{\text{ideals of } R \text{ containing } I\} \longleftrightarrow \{\text{ideals of } R/I\},$$

where the ideal $J$ of $R$ (containing $I$) corresponds to the ideal $J/I$ of $R/I$. With this in mind, we can prove the following proposition.

**Proposition 2.2.8.** *If $R$ is a Noetherian ring and $I$ is an ideal of $R$, then $R/I$ is Noetherian.*

*Proof.* Suppose we had an infinite ascending chain of ideals

$$\overline{J}_1 \subseteq \overline{J}_2 \subseteq \overline{J}_3 \subseteq \dots$$

of $R/I$. Then from the ideal correspondence preceding the proposition, this would correspond to an infinite ascending chains of ideals

$$J_1 \subseteq J_2 \subseteq J_3 \subseteq \dots$$

of $R$. But $R$ is Noetherian, so there exists $n$ such that $J_m = J_n$ for all $m \geq n$. Then again by the correspondence, this means $\overline{J}_m = \overline{J}_n$ for all $m \geq n$. Since this chain was arbitrary, $R/I$ is Noetherian. □

An example of a Noetherian ring is $\mathbb{Z}$, and this follows from the following theorem.

**Theorem 2.2.9.** *If a commutative ring $R$ is a PID, then $R$ is Noetherian.*

*Proof.* Since $R$ is a PID, an ascending chain of ideals is a chain

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots,$$

where $a_i \in R$. Consider the ideal

$$I = \bigcup_{n=1}^{\infty} (a_n) \lhd R.$$

Since $R$ is a PID, $I = (\alpha)$ for some $\alpha$. Since

$$\alpha \in \bigcup_{n=1}^{\infty} (a_n),$$

$\alpha \in (a_j)$ for some $j$, and hence $(\alpha) \subseteq (a_j)$. But then this means for all $k \geq j$,

$$(\alpha) \subseteq (a_k) \subseteq (\alpha),$$

and hence $(a_k) = (\alpha)$ for all $k \geq j$. Therefore $R$ is Noetherian by definition. □

For an example of a ring which is not Noetherian, consider $R = \mathbb{Q}[x_1, x_2, \ldots]$. The ring $R$ is certainly commutative, but the chain of ideals

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \ldots$$

is an ascending chain which does not stabilize after any term. Therefore $R$ cannot be Noetherian.

### Modules

While we will not be needing Noetherian modules in this section on Dedekind rings, it will be useful in later sections. The definition of Noetherian modules is nearly identical to that of Noetherian rings.

**Definition 2.2.10.** Suppose $R$ is a ring and $M$ a (left) $R$-module. Then $M$ is said to be *Noetherian* if whenever

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

is an increasing chain of submodules of $M$, there exists $n$ such that $M_k = M_n$ for all $k \geq n$.

It is worth remarking that if there is a ring $R$, then $R$ is naturally a left $R$-module over itself, sometimes denoted ${}_R R$. Moreover, submodules of ${}_R R$ correspond to left ideals of $R$, as the reader can easily check. If $R$ is commutative, left ideals are also two-sided ideals. So assuming $R$ is commutative, an ascending chain of submodules of ${}_R R$ corresponds to an ascending chain of ideals of $R$ (and vice-versa). Therefore an alternative definition of Noetherian (commutative) rings could be a ring $R$ is Noetherian if ${}_R R$ is a Noetherian module. This is summarized in the following proposition.

**Proposition 2.2.11.** *A commutative ring $R$ is Noetherian if and only if $R$ is Noetherian as a left module over itself.*

The following theorem is an important characterization of Noetherian modules:

**Theorem 2.2.12.** *Suppose $R$ is a ring and $M$ a left $R$-module. Then the following statements are equivalent:*

*(i) $M$ is a Noetherian $R$-module.*

*(ii) Every nonempty set of submodules of $M$ contains a maximal element (under inclusion).*

*(iii) Every submodule of $M$ is finitely generated.*

*Proof.* (i) $\implies$ (ii): Suppose $M$ is Noetherian, and let $\Sigma$ denote a nonempty collection of submodules of $M$. Choose some $M_1 \in \Sigma$ (possible as $\Sigma$ is nonempty). If $M_1$ is maximal, then (ii) holds. If not, then there exists some $M_2 \in \Sigma$ with $M_1 \subset M_2$. If $M_2$ is maximal, then (ii) holds. If not, then there exists $M_3 \in \Sigma$ with $M_2 \subset M_3$, and so on. If (ii) continually fails then we would have an infinite ascending chain of submodules of $M$

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

which does not stabilize, contradicting the fact that $M$ is Noetherian.

(ii) $\implies$ (iii): Suppose $N$ is a submodule of $M$, and let $\Sigma$ denote the set of all finitely generated submodules of $N$. Clearly $\{0\} \in \Sigma$, so $\Sigma$ is nonempty. By (ii), there exists a maximal element $N' \in \Sigma$. We want $N' = N$. Suppose $N' \subset N$. Then there exists $n \in N \backslash N'$. Since $N' \in \Sigma$, $N'$ is finitely generated, and so the submodule generated by $N'$ and $n$ is also finitely generated (hence in $\Sigma$) and properly contains $N'$, contradicting the maximiality of $N'$. Therefore $N' = N$ and $N$ is finitely generated.

(iii) $\implies$ (i): Suppose

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

is an increasing chain of submodules of $M$, and let

$$N = \bigcup_{i=1}^{\infty} M_i.$$

Then $N$ is a submodule of $M$, and by (iii) is finitely generated, say by $n_1, \ldots, n_k$. Since each $n_i \in N$, there exists some $M_{j_i}$ such that $n_i \in M_{j_i}$. Let $m = \max\{j_1, \ldots, j_k\}$. Then $n_i \in M_m$ for all $i$, meaning $N \subseteq M_m \subseteq N$, so $M_m = N$. Therefore $M_k = M_m$ for all $k \geq m$ and hence (i) holds. $\square$

**Corollary 2.2.13.** *A commutative ring $R$ is Noetherian if and only if every ideal of $R$ is finitely generated.*

*Proof.* By the proposition, $R$ is a Noetherian ring if and only if ${}_RR$ is a Noetherian module. But ${}_RR$ is a Noetherian module if and only if every submodule is finitely generated (by the theorem). Since ideals of $R$ are submodule of ${}_RR$ and vice-versa, the statement follows. □

It is a good exercise for the reader to use this corollary to give a one line proof of Theorem 2.2.9.

There are two other useful propositions. These proofs come from [12].

**Proposition 2.2.14.** *Let $R$ be a ring and $M$ be an $R$-module, with $N \subseteq M$ a submodule. If both $N$ and $M/N$ are Noetherian, then so is $M$.*

*Proof.* Suppose first that $M_1 \subseteq M_2$ are two submodules of $M$ such that $M_1 \cap N = M_2 \cap N$, and both $M_1$ and $M_2$ have the the same image in $M/N$. The claim is that $M_1 = M_2$. For suppose $m_2 \in M_2$. Since both $M_1$ and $M_2$ have the same image in $M/N$, we can certainly find an $m_1 \in M_1$ with $m_1 + N = m_2 + N$, so $m_2 - m_1 \in N$. But then $m_2 - m_1 \in M_2 \cap N$ (as $m_1 \in M_2$ as well), but as $M_1 \cap N = M_2 \cap N$, this implies $m_2 - m_1 \in M_1 \cap N \subset M_1$, so $m_2 \in M_1$. Therefore $M_1 = M_2$ (reverse inclusion was assumed).

So now suppose

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

is an increasing chain of submodules of $M$. Then the sequence

$$M_1 \cap N \subseteq M_2 \cap N \subseteq M_3 \cap N \subseteq \cdots$$

is an increasing chain of submodules of $N$. Since $N$ was assumed to be Noetherian, there exists $j$ such that $M_n \cap N = M_j \cap N$ for all $n \geq j$. Similarly,

$$M_1/N \subseteq M_2/N \subseteq M_3/N \subseteq \cdots$$

is an increasing chain of submodules of $M/N$, which was assumed to be Noetherian as well. Therefore there exists $k$ such that $M_i/N = M_k/N$ for all $i \geq k$. Taking $m = \max\{j, k\}$ shows that for all $n \geq m$, $M_n$ and $M_m$ have the same image in $M/N$ and $M_n \cap N = M_m \cap N$. Therefore by the claim above, $M_n = M_m$ for all $n \geq m$, meaning $M$ is Noetherian. □

*Remark* 2.2.15. The converse of this statement should be clear. Indeed if $M$ is a Noetherian module and $N$ a submodule, then as submodules of $N$ are also submodules of $M$, $N$ will clearly be Noetherian. Also, the proof that $M/N$ is Noetherian is very similar to the proof of Proposition 2.2.8.

By the above proposition, we get the following.

**Proposition 2.2.16.** *Let $R$ be a Noetherian ring. Then every finitely generated $R$-module is Noetherian.*

*Proof.* The proof is by induction on the number of generators. Suppose $M$ can be generated by a single element, say $m \in M$. Then we can construct a module homomorphism

$$\phi : R \to M, \quad r \mapsto rm.$$

It is easily checked that this is a surjective $R$-module homomorphism, and so by the first isomorphism theorem $M \cong R/\ker\phi$. Since $R$ is a Noetherian ring, it is Noetherian as a module over itself, and so quotients of $R$ by submodules are also Noetherian. Therefore $M$ is Noetherian. Now suppose it is true up to $n-1$ generators, and then suppose $M$ is generated by $n$ elements, say $m_1, \ldots, m_n$. Then $M$ contains a submodule $N$ generated by $n-1$ elements (say the submodule generated by $m_1, \ldots, m_{n-1}$), and the quotient $M/N$ is generated by one element. By induction, both $N$ and $M/N$ are Noetherian, and so by Proposition 2.2.14, $M$ is Noetherian. □

### 2.2.3 Dedekind Rings

In this section we finally define Dedekind rings. First, we make the following definition.

**Definition 2.2.17.** A *discrete valuation ring* is a principal ideal domain with exactly one maximal ideal.

Discrete valutation rings will be abbreviated DVR. As noted in [9], every field is a DVR. This is because there are only two ideals, namely the zero ideal and the whole field. Therefore fields are the "trivial case." However, in this thesis, we will only be concerned with the DVRs which are not fields. We will need the following proposition.

**Proposition 2.2.18.** *Suppose $R$ is a DVR and suppose $\mathfrak{p} = R\pi$ is the unique maximal ideal of $R$, where $\pi \in R$. Then*

*(i) If $R$ is not a field, then every nonzero element $\alpha \in R$ can be written as $\alpha = u\pi^k$ where $u \in R$ is a unit and $k \in \mathbb{Z}_{\geq 0}$.*

*(ii) Every nonzero ideal has the form $R\pi^k$ for $k \in \mathbb{Z}_{\geq 0}$.*

*Proof.* First, recall that in a PID, prime ideals are maximal and irreducible elements are prime (in general, maximal ideals are prime and prime elements are irreducible). The claim is that $\pi$ is the only prime element of $R$, up to multiplication by units. This is because if $\pi_1$ were another prime element which is not a unit multiple of $\pi$, then $R\pi_1$ would be another prime ideal of $R$, and hence

a maximal ideal distinct from $\mathfrak{p}$. But a DVR can only have one maximal ideal, so this cannot happen. Hence $\pi$ is the unique prime element of $R$ up to unit multiples. So now let $\alpha \in R$ be any element. Since $R$ is a PID, $R$ is necessarily a UFD and so $\alpha$ factors into a unit times a product of irreducible elements. Since irreducible elements are prime, the only irreducible element of $R$ is $\pi$ (or $\pi$ times a unit), and so (i) follows. Item (ii) immediately follows from (i) and the fact that $R$ is a PID. □

Property (ii) will be useful in the next section. But now we have all the definitions needed to introduce Dedekind rings.

**Definition 2.2.19.** An integral domain $R$ is a *Dedeking ring* if it is Noetherian and the localization $R_{\mathfrak{p}}$ is a DVR for every (nonzero) prime ideal $\mathfrak{p}$ of $R$.

**Example 2.2.20.** Consider $R = \mathbb{Z}$. We know $\mathbb{Z}$ is an integral domain and Theorem 2.2.9 implies $\mathbb{Z}$ is Noetherian. Corollary 2.2.6 says that $\mathbb{Z}_{(p)}$ has only one maximal ideal for every prime $p$ (these are all the prime ideals of $\mathbb{Z}$). Lastly, the correspondence given by Proposition 2.2.5 tells us that since $\mathbb{Z}$ is a PID, $\mathbb{Z}_{(p)}$ will be a PID for every prime $p$. Hence $\mathbb{Z}$ is a Dedekind ring.

There is also the following property of Dedekind rings.

**Proposition 2.2.21.** *If $R$ is a Dedekind ring, then every nonzero prime ideal of $R$ is maximal.*

*Proof.* Suppose the statement were false. Then there would exist a nonzero prime ideal $\mathfrak{p}_1$ of $R$ which was not maximal, and therefore would be properly contained in a maximal (and hence prime) ideal $\mathfrak{p}_2$ (i.e. $\mathfrak{p}_1 \subset \mathfrak{p}_2$). But the correspondence in Proposition 2.2.5 then implies that $\mathfrak{p}_1 R_{\mathfrak{p}_2} \subset \mathfrak{p}_2 R_{\mathfrak{p}_2}$ is a proper containment of prime ideals of $R_{\mathfrak{p}_2}$. But $R$ is a Dedekind domain, and hence $R_{\mathfrak{p}_2}$ is a DVR, and so can only have one nonzero prime ideal (remember in a PID, the maximal ideals are precisely the prime ideals). This is a contradiction, meaning $\mathfrak{p}_1$ was maximal. This proves the proposition. □

### 2.2.4 Unique Factorization into Prime Ideals

Recall some basic ideas from ring theory. If $R$ is a ring (commutative in our case) and $I$ and $J$ are ideals, then

$$I + J = \{i + j : i \in I, j \in J\}$$

and

$$IJ = \{\sum_{m=1}^{k} i_m j_m : i_m \in I, j_m \in J\}$$

are both ideals as well. The finite sums in the definition of $IJ$ are necessary to make $IJ$ into an ideal. It should be clear that $IJ \subseteq I$ (and similarly $IJ \subseteq J$).

The aim of this section is to show that in a Dedekind ring, we can decompose any ideal into a product of prime ideals, similar to the way integers have a prime factorization. So let us begin that process. This proof follows that of [9], Section 1.3.

There are a few lemmas and theorems which are needed. The first is a theorem the reader may or may not be familiar with: the Chinese Remainder Theorem. We will not supply a proof here, although we do mention the more classical version of this theorem in the next chapter.

**Theorem 2.2.22.** *Suppose $R$ is a ring with identity and $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ ideals of $R$ such that $\mathcal{Q}_i + \mathcal{Q}_j = R$ for $i \neq j$. Set $\mathcal{Q} = \cap_i \mathcal{Q}_i$. Then the mapping*

$$r \mapsto (r + \mathcal{Q}_1, \ldots, r + \mathcal{Q}_n)$$

*induces a ring isomorphism*

$$R/\mathcal{Q} \cong R/\mathcal{Q}_1 \oplus \cdots \oplus R/\mathcal{Q}_n.$$

The next goal is to give a better illustration of what $\mathcal{Q}$ in the CRT actually is. The following proposition does that.

**Proposition 2.2.23.** *Suppose $R$, $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$, $\mathcal{Q}$ are as in the previous theorem and assume further that $R$ is commutative. Then $\mathcal{Q} = \cap_i \mathcal{Q}_i$ is*

$$\mathcal{Q} = \mathcal{Q}_1 \mathcal{Q}_2 \cdots \mathcal{Q}_n.$$

*Proof.* The proof will be by induction on $n$. Suppose $n = 2$. We want to show $\mathcal{Q}_1 \cap \mathcal{Q}_2 = \mathcal{Q}_1 \mathcal{Q}_2$, so we will show both inclusions. First the inclusion $\mathcal{Q}_1 \cap \mathcal{Q}_2 \subseteq \mathcal{Q}_1 \mathcal{Q}_2$. Let $q \in \mathcal{Q}_1 \cap \mathcal{Q}_2$. Since $\mathcal{Q}_1 + \mathcal{Q}_2 = R$ by assumption, there exists $q_1 \in \mathcal{Q}_1$, $q_2 \in \mathcal{Q}_2$ such that $q_1 + q_2 = 1$. Then

$$q = \overbrace{q}^{\in \mathcal{Q}_2}\overbrace{q_1}^{\in \mathcal{Q}_1} + \overbrace{q}^{\in \mathcal{Q}_1}\overbrace{q_2}^{\in \mathcal{Q}_2},$$

and hence $q \in \mathcal{Q}_1 \mathcal{Q}_2$ (as $R$ is commutative). The reverse inclusion is immediate since $\mathcal{Q}_1 \mathcal{Q}_2 \subseteq \mathcal{Q}_1$ and $\mathcal{Q}_1 \mathcal{Q}_2 \subseteq \mathcal{Q}_2$. So the proposition is true for $n = 2$. Now let $n > 2$, and assume the theorem is true up to $n - 1$. Set

$$\mathcal{Q}'_{n-1} = \mathcal{Q}_{n-1} \cap \mathcal{Q}_n.$$

By the inductive hypothesis,

$$\mathcal{Q}'_{n-1} = \mathcal{Q}_n \mathcal{Q}_{n-1}.$$

We want to be able to apply the inductive hypothesis on the $n - 1$ ideals $\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_{n-2}, \mathcal{Q}'_{n-1}$. The only thing to check is that $\mathcal{Q}'_{n-1} + \mathcal{Q}_j = R$ for $j < n - 1$. First observe that

$$R = R \cdot R = (\mathcal{Q}_n + \mathcal{Q}_j)(\mathcal{Q}_{n-1} + \mathcal{Q}_j) \subseteq \mathcal{Q}_n \mathcal{Q}_{n-1} + \mathcal{Q}_j.$$

Since

$$\mathcal{Q}_n\mathcal{Q}_{n-1} \subseteq \mathcal{Q}_n \cap \mathcal{Q}_{n-1} = \mathcal{Q}'_{n-1},$$

we see

$$R \subseteq \mathcal{Q}_n\mathcal{Q}_{n-1} + \mathcal{Q}_j \subseteq \mathcal{Q}'_{n-1} + \mathcal{Q}_j \subseteq R,$$

and hence $R = \mathcal{Q}'_{n-1} + \mathcal{Q}_j$, as required. Therefore the inductive hypothesis can be applied to the $n-1$ ideals $\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_{n-2}, \mathcal{Q}'_{n-1}$. Clearly the intersection of all these ideals is still $\mathcal{Q}$, and so

$$\mathcal{Q} = \bigcap_{i=1}^{n} \mathcal{Q}_i = \mathcal{Q}_1 \cap \mathcal{Q}_2 \cap \cdots \mathcal{Q}_{n-2} \cap \mathcal{Q}'_{n-1} = \mathcal{Q}_1\mathcal{Q}_2 \cdots \mathcal{Q}_{n-2}\mathcal{Q}'_{n-1} = \mathcal{Q}_1\mathcal{Q}_2 \cdots \mathcal{Q}_n.$$

□

The next lemma and subsequent corollary are going to be important because they will tell us how to pick the prime ideal divisors in our ideal factorization.

**Lemma 2.2.24.** *Suppose $R$ is a commutative Noetherian ring in which every prime ideal is maximal. Then every ideal of $R$ contains a product of prime ideals.*

*Proof.* Suppose the statement were false. Then there would be an ideal $J$ such that $J$ does not contain a product of prime ideals. Pick $J$ maximal with this property. Then $J$ is not a prime ideal, so we can pick elements $x, y \notin J$ such that $xy \in J$. We let $\mathfrak{A} = Rx + J$ and $\mathfrak{B} = Ry + J$. Then as $\mathfrak{A}$ and $\mathfrak{B}$ both contain $J$, they both contain a product of prime ideals as $J$ was said to be the largest ideal without such a product. But then as $xy \in J$, we see $\mathfrak{A}\mathfrak{B} \subseteq J$. So this means $J$ must also contain a product of prime ideals, which is a contradiction. Therefore no such $J$ exists and the lemma is proved. □

**Corollary 2.2.25.** *With $R$ as in the previous lemma, there exists prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ of $R$ and positive integers $a_1, a_2, \ldots, a_n$ such that*

$$\mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_n^{a_n} = 0.$$

*Proof.* Take the zero ideal in the previous lemma, and use the fact that 0 is the only element of the zero ideal. □

There are two more lemmas we need. The next one will show that powers of prime ideals are coprime (meaning the sum of the ideals is equal to the whole ring), and so we will be able to apply the CRT to them later.

**Lemma 2.2.26.** *Suppose $R$ is a commutative ring and let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two distinct maximal ideals of $R$. Then $\mathfrak{p}_1^a + \mathfrak{p}_2^b = R$ for any $a, b \in \mathbb{Z}_{>0}$.*

*Proof.* First, recall that the sum of two distinct maximal ideals must be the whole ring, so $\mathfrak{p}_1 + \mathfrak{p}_2 = R$. This is because $\mathfrak{p}_1 + \mathfrak{p}_2$ contains the ideal $\mathfrak{p}_1$, and since $\mathfrak{p}_1$ is maximal, we must have $\mathfrak{p}_1 + \mathfrak{p}_2 = \mathfrak{p}_1$ or $R$. Applying the same logic to $\mathfrak{p}_2$ shows that $\mathfrak{p}_1 + \mathfrak{p}_2 = \mathfrak{p}_2$ or $R$. Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct, the only possibility is $\mathfrak{p}_1 + \mathfrak{p}_2 = R$. With this, we find

$$R = R^a = (\mathfrak{p}_1 + \mathfrak{p}_2)^a \subseteq \mathfrak{p}_1^a + \mathfrak{p}_2 \subseteq R,$$

meaning $\mathfrak{p}_1^a + \mathfrak{p}_2 = R$ for any integer $a > 0$. So now suppose $\mathfrak{p}_1^a + \mathfrak{p}_2^c = R$ for some integer $c \geq 1$. We want to get the same relation with $c+1$ instead of $c$. Well

$$\mathfrak{p}_2^c = \mathfrak{p}_2^c R = \mathfrak{p}_2^c(\mathfrak{p}_1^a + \mathfrak{p}_2) \subseteq \mathfrak{p}_1^a + \mathfrak{p}_2^{c+1}.$$

Therefore

$$R = \mathfrak{p}_1^a + \mathfrak{p}_2^c \subseteq \mathfrak{p}_1^a + (\mathfrak{p}_1^a + \mathfrak{p}_2^{c+1}) \subseteq \mathfrak{p}_1^a + \mathfrak{p}_2^{c+1} \subseteq R,$$

and so $\mathfrak{p}_1^a + \mathfrak{p}_2^{c+1} = R$, as required. Therefore the statement is true for any chosen positive integers $a, b$. □

One lemma which we will not prove is the following.

**Lemma 2.2.27.** *Let $R$ be as in lemma 2.2.24 and suppose $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ are the prime ideals in corollary 2.2.25. Then $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ are all the prime ideals of $R$.*

We are almost in position to prove the main theorem. The last lemma we need to prove will help describe ideals of $R/\mathfrak{p}^a$ where $R$ is a Dedekind ring and $\mathfrak{p}$ is a prime ideal.

**Lemma 2.2.28.** *Suppose $\mathfrak{p}$ is a maximal ideal of a commutative ring $R$ and let $a$ be a positive integer. Then the inclusion of $R$ into $R_\mathfrak{p}$ induces an isomorphism*

$$R/\mathfrak{p}^a \cong R_\mathfrak{p}/\mathfrak{p}^a R_\mathfrak{p}.$$

*Proof.* Consider the map

$$\phi : R/\mathfrak{p}^a \to R_\mathfrak{p}/\mathfrak{p}^a R_\mathfrak{p}, \quad r + \mathfrak{p}^a \mapsto r + \mathfrak{p}^a R_\mathfrak{p}.$$

It should be clear that $\phi$ is a ring homomorphism, and that $\phi$ is injective. Showing $\phi$ is surjective will prove the lemma. So take any $r/s \in R_\mathfrak{p}$ (so $r \in R$, $s \notin \mathfrak{p}$). We are assuming $\mathfrak{p}$ is a maximal ideal, so $Rs + \mathfrak{p} = R$. By the same logic as in the proof of the previous lemma, $Rs + \mathfrak{p}^a = R$. Therefore there exists $c \in R$, $p \in \mathfrak{p}^a$ with $cs + p = 1$. Therefore $c = 1/s - p/s$. So

$$\begin{aligned} \phi(rc + \mathfrak{p}^a) &= rc + \mathfrak{p}^a R_\mathfrak{p} \quad \text{(definition)} \\ &= r(1/s - p/s) + \mathfrak{p}^a R_\mathfrak{p} \\ &= r/s + \mathfrak{p}^a R_\mathfrak{p}, \end{aligned}$$

as $p \in \mathfrak{p}^a$ and $r/s \in R_\mathfrak{p}$ (meaning $pr/s \in \mathfrak{p}^a R_\mathfrak{p}$). Therefore $\phi$ is surjective and hence an isomorphism. □

**Corollary 2.2.29.** *If $R$ is a Dedeking ring and $\mathfrak{p}$ is a nonzero prime ideal of $R$, then for any positive $a \in \mathbb{Z}$, every ideal of $R/\mathfrak{p}^a$ is a power of $\mathfrak{p}/\mathfrak{p}^a$. Moreover, $\mathfrak{p}/\mathfrak{p}^a$ is principal.*

*Proof.* By the previous lemma, we can replace $R/\mathfrak{p}^a$ by $R_\mathfrak{p}/\mathfrak{p}^a R_\mathfrak{p}$. Since $R$ is a Dedekind ring and $\mathfrak{p}$ is a prime ideal, by definition $R_\mathfrak{p}$ is a DVR. So the statements follow from the properties of DVR we proved in Proposition 2.2.18. □

Finally, we can prove the unique factorization of ideals.

**Theorem 2.2.30.** *Let $R$ be a Dedekind ring and $\mathfrak{A}$ a nonzero ideal of $R$. Then $\mathfrak{A}$ is contained in only finitely many distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$, and moreover*

$$\mathfrak{A} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_n^{a_n}$$

*for some unique positive integers $a_i$.*

*Proof.* Let $B = R/\mathfrak{A}$. Then $R$ is a commutative ring which is Noetherian by Proposition 2.2.8, and every prime ideal of $B$ is maximal (as they are in $R$ by Proposition 2.2.21). Therefore the conditions of Lemma 2.2.24 are satisfied. Moreover, every prime ideal of $B$ corresponds to a prime ideal of $R$ which contains $\mathfrak{A}$. By Lemma 2.2.27, there are only finitely many prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ of $R$ containing $\mathfrak{A}$. Corollary 2.2.25 says some product

$$\mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_n^{b_n} = 0$$

in $B$ for some $b_i > 0$, which means $\mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_n^{b_n} \subseteq \mathfrak{A}$. Set $B' = R/\mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_n^{b_n}$. By Lemma 2.2.26, we can apply the CRT to get

$$B = R/\mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_n^{b_n} \cong R/\mathfrak{p}_1^{b_1} \oplus \cdots \oplus R/\mathfrak{p}_n^{b_n}.$$

It is a fact from ring theory that since each of the $R/\mathfrak{p}_i^{b_i}$ are rings with identity, the ideals of $B$ are precisely those which are the direct sum of ideals of the $R/\mathfrak{p}_i^{b_i}$. By Corollary 2.2.29, we find that ideals of $R/\mathfrak{p}_i^{b_i}$ are of the form $\mathfrak{p}_i^{c_i}/\mathfrak{p}_i^{b_i}$ for some $c_i \leq b_i$. Under the isomorphism given by the CRT, this means ideals of $B'$ are the image in $B'$ of ideals of $R$ of the form $\mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\cdots\mathfrak{p}_n^{c_n}$, where $c_i \leq b_i$ for all $i$. Since $\mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_n^{b_n} \subseteq \mathfrak{A}$, $\mathfrak{A}/\mathfrak{p}_1^{b_n}\cdots\mathfrak{p}_n^{b_n}$ is an ideal of $B'$, and this means $\mathfrak{A}$ has the same image in $B'$ as some product $\mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\cdots\mathfrak{p}_n^{c_n}$. Since both contain $\mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_n^{b_n}$, they must be equal. That is,

$$\mathfrak{A} = \mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\cdots\mathfrak{p}_n^{c_n}$$

for some positive integers $c_i$.

The prime ideals $\mathfrak{p}_i$ are uniquely determined by $\mathfrak{A}$ since those are the prime ideals containing $\mathfrak{A}$. The integers $c_i$ are uniquely determined because they are the least positive integer for which the power of the maximal ideal of $R_{\mathfrak{p}_i}/\mathfrak{A}R_{\mathfrak{p}_i}$ is the zero ideal in this ring. □

So we have proved the unique factorization of ideals in Dedekind rings. The proof was not overly complicated, but of course it required a series of lemmas and theorems.

We can talk about one ideal dividing another ideal in the same manner as we talk about one integer dividing another. In this case, we say for a ring $R$, ideal $B$ divides ideal $A$ if there exists ideal $C$ of $R$ with $BC = A$. What Theorem 2.2.30 says is that for two ideals $A$ and $B$, $B|A$ if and only if $B$ contains $A$. So ***to contain is to divide***, which a very helpful phrase when dealing with ideal factorization.

# 2.3 Ring of Integers

As noted in the beginning of the previous section, the next step in the development of Algebraic Number Theory is to examine the ring of integers. We can now define this ring and eventually show that it is a Dedekind ring.

## 2.3.1 Definition and Example

**Definition 2.3.1.** Suppose $R$ is a subring of a commutative ring $R'$. An element $a \in R'$ is said to be *integral* over $R$ if there exists a monic polynomial $f(x) \in R[x]$ with $f(a) = 0$. If it exists, $f(x)$ is an equation of *integral dependence* for $a$.

For example, we can let $R = \mathbb{Z}$ and $R' = \mathbb{Z}[\sqrt{2}]$, and then let $a = \sqrt{2}$. In this case, $a$ is integral over $\mathbb{Z}$ because $a$ satisfies the monic polynomial $x^2 - 2 \in \mathbb{Z}[x]$. For a nonexample, consider $R = \mathbb{Z}$ and $R' = \mathbb{Q}$. Then the element $1/2 \in \mathbb{Q}$ is not integral over $\mathbb{Z}$ because there is no *monic* polynomial in $\mathbb{Z}[x]$ with $1/2$ as a root. The reader will note, however, that $1/2$ does satisy $2x - 1 \in \mathbb{Z}[x]$, so the condition that the polynomial be monic is crucial.

Now suppose we have an integral domain $R$, and let $K$ denote its field of fractions. There is a natural embedding of $R$ into $K$.

**Definition 2.3.2.**

1. The set of all elements of $K$ which are integral over $R$ is called the *integral closure* of $R$ in $K$.
2. If every element of $K$ which is integral over $R$ already is an element of $R$, then $R$ is *integrally closed*.

Apply these definitions to the case $R = \mathbb{Z}$ to get the following.

**Definition 2.3.3.** If $K/\mathbb{Q}$ is a number field, then an element $\alpha \in K$ is called an *algebraic integer* if it is integral over $\mathbb{Z}$. That is, $\alpha$ is an algebraic integer if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ with $f(\alpha) = 0$.

By Gauss' lemma, it suffices to check if the minimal polynomial of the element $\alpha$ is in $\mathbb{Z}[x]$ because the minimal polynomial divides any other polynomial with $\alpha$ as a root. Namely, if $f(x) \in \mathbb{Z}[x]$ has $\alpha$ as a root, then if $m_\alpha(x) \in \mathbb{Q}[x]$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$ then we know $m_\alpha(x)|f(x)$. But Gauss' lemma implies that since $f(x)$ can be factored over $\mathbb{Q}$, it can be factored over $\mathbb{Z}$. Thus $m_\alpha(x) \in \mathbb{Z}[x]$.

It is also worth noting how this definition differs from that of an algebraic element, which is defined in Appendix A. An algebraic number has to satify some polynomial in $\mathbb{Q}[x]$, whereas the algebraic integer has to satisfy a monic polynomial in $\mathbb{Z}[x]$. So for example, the element $\alpha = 1/2 + \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is algebraic (as it lives in the finite extension $\mathbb{Q}(\sqrt{2})$; see appendix), but it is not an algebraic integer as its minimal polynomial does not lie in $\mathbb{Z}[x]$, as the reader will verify.

Now use Definition 2.3.2 in the case $R = \mathbb{Z}$.

**Definition 2.3.4.** If $K/\mathbb{Q}$ is a number field, then the integral closure of $\mathbb{Z}$ in $K$ is called the *ring of integers* of $K$, denoted $\mathcal{O}_K$.

The simplest example is when $K = \mathbb{Q}$. In this case, we know that elements of $\mathbb{Q}$ are integral over $\mathbb{Z}$ if and only if they are in $\mathbb{Z}$. This is because the minimal polynomial of $\alpha \in \mathbb{Q}$ is $x - \alpha \in \mathbb{Q}[x]$, which is clearly in $\mathbb{Z}[x]$ if and only if $\alpha \in \mathbb{Z}$. Hence for $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$. The easiest nontrivial case would be that of quadratic extensions. The following computations can also be found in [6].

**Example 2.3.5.** Let $K = \mathbb{Q}(\sqrt{d})$. First observe that we can assume $d$ is squarefree, since the square roots of any square factors are elements of $\mathbb{Z}$ (and hence of $\mathbb{Q}$). So assume $d$ is squarefree. Any element $\alpha \in K$ can be written as $\alpha = a + b\sqrt{d}$ for $a, b \in \mathbb{Q}$. If $b \neq 0$, then the minimal polynomial of $\alpha$ is going to have degree two over $\mathbb{Q}$, and one can check that it is

$$m_\alpha(x) = x^2 - 2ax + (a^2 - db^2).$$

Now we want to see what conditions on $a$ and $b$ give us $\alpha \in \mathcal{O}_K$. From the above, this happens precisely when $2a, a^2 - db^2 \in \mathbb{Z}$. Well if $a^2 - db^2 \in \mathbb{Z}$, then certainly $4(a^2 - db^2) \in \mathbb{Z}$, and expanding and absorbing into the squares we see this means $(2a)^2 - d(2b)^2 \in \mathbb{Z}$. But we already know $2a \in \mathbb{Z}$, so this implies $d(2b)^2 \in \mathbb{Z}$. We know that $b \in \mathbb{Q}$, so $2b \in \mathbb{Q}$ and we can write $2b = r/s$, for $r, s \in \mathbb{Z}$, $s \neq 0$. Then the condition

$$d(2b)^2 \in \mathbb{Z} \implies \frac{dr^2}{s^2} \in \mathbb{Z},$$

and this implies $s^2|dr^2$. But $d$ was assumed to be squarefree, so one quickly sees that this yields $s|r$, and since $2b = r/s$, this means $2b \in \mathbb{Z}$. Since $2a, 2b \in \mathbb{Z}$, write $2a = A$ and $2b = B$ for $A, B \in \mathbb{Z}$. Similarly to what we did earlier, we see that

$$a^2 - db^2 \in \mathbb{Z} \implies 4(a^2 - db^2) \in 4\mathbb{Z} \implies (2a)^2 - d(2b)^2 \in 4\mathbb{Z},$$

but we can now substitute in $A$ and $B$ to find $A^2 - dB^2 \in 4\mathbb{Z}$, or $4|A^2 - dB^2$. Hence $A^2 - dB^2 \equiv 0 \bmod 4$, or

$$A^2 \equiv dB^2 \bmod 4.$$

But squares can only be 0 or 1 modulo 4, and so we have two cases:

(a) $d \equiv 2, 3 \bmod 4$: In this case, we must have $A, B \equiv 0 \bmod 4$ as $A^2, B^2$ can only be 0 or 1 modulo 4. Hence $A$ and $B$ are even, and since $A = 2a$ and $B = 2b$ this means $a, b \in \mathbb{Z}$.

(b) $d \equiv 1 \bmod 4$: This means $A^2 \equiv B^2 \bmod 4$, and so both are either 0 or both are 1 modulo four. In either case, they must have the same parity, namely $A \equiv B \bmod 2$. If both are even, then $a, b \in \mathbb{Z}$ as in case (a). If both are odd, then $a$ and $b$ are half-integers.

Note that we do not need to check the case when $d \equiv 0 \bmod 4$ because this would mean $4|d$, contradicting the fact that $d$ is squarefree. We use the notation $\langle - \rangle_{\mathbb{Z}}$ to denote the $\mathbb{Z}$-span of the elements in the brackets. So for example $\left\langle 1, \sqrt{2} \right\rangle_{\mathbb{Z}} = a + b\sqrt{2}$ where $a, b \in \mathbb{Z}$. The above work shows

$$\mathcal{O}_K = \left\langle 1, \sqrt{d} \right\rangle_{\mathbb{Z}} \quad \text{if } d \equiv 2, 3 \bmod 4,$$

and

$$\mathcal{O}_K = \left\langle 1, \frac{1+\sqrt{d}}{2} \right\rangle_{\mathbb{Z}} \quad \text{if } d \equiv 1 \bmod 4.$$

While computing this answer took a page of tricks and algebra, it is good to see a concrete example to illustrate the more abstract definitions. Quadratic extensions are the easiest non-trivial examples to demonstrate many of the concepts we will be discussing throughout this thesis.

The next example we want to look at is the ring of integers of a cyclotomic field $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n$ is some primitive $n$-th root of unity. We will be dealing with cyclotomic extensions almost exclusively in Chapter 3, so this theorem will be of great importance. We will not prove it, but a proof can be found in [9].

**Theorem 2.3.6.** *If $\zeta_n$ is a primitive $n$-th root of unity, then the ring of integers of $K = \mathbb{Q}(\zeta_n)$ is $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.*

One remark before we move forward to the next section. While it is clear that not every element in $K$ is in $\mathcal{O}_K$, there is a nice result which we can prove. If $\alpha \in K$, then it satisfies some monic polynomial over $\mathbb{Q}$, say

$$\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_1\alpha + a_0 = 0, \quad a_i \in \mathbb{Q}.$$

For $n \in \mathbb{Z}$, mutliply both sides by $n^d$ and notice that this yields

$$(n\alpha)^d + na_{d-1}(n\alpha)^{d-1} + n^2a_{d-2}(n\alpha)^{d-2} + \ldots + n^{d-1}a_1(n\alpha) + a_0 = 0.$$

If $n$ is chosen so that it clears the denominators of the $a_i$, then $n\alpha \in \mathcal{O}_K$. We have just proved the following.

**Proposition 2.3.7.** *Suppose $\alpha \in K$, where $K$ is a number field. Then there exists $n \in \mathbb{Z}$ such that $n\alpha \in \mathcal{O}_K$.*

### 2.3.2 Proof $\mathcal{O}_K$ is a ring

We have yet to show that $\mathcal{O}_K$ is actually a ring. That is the purpose of this section, and the proof is from [6]. First, consider the following lemma.

**Lemma 2.3.8.** *If $K$ is a number field, then $\alpha \in K$ is an algebraic integer if and only if there exists a nonzero finitely generated $\mathbb{Z}$-module $M \subseteq K$ such that $\alpha M \subseteq M$.*

*Proof.* Suppose $\alpha \in \mathcal{O}_K$. Then $\alpha$ satisifes some polynomial over $\mathbb{Z}$, say

$$a_0 + a_1\alpha + \ldots + \alpha^n = 0, \quad a_i \in \mathbb{Z}.$$

If we let $M = \mathbb{Z}[\alpha]$, then $M$ is generated by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, and $\alpha M \subseteq M$ since

$$\alpha^n = -a_0 - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1}.$$

Conversely, suppose $M \subseteq K$ is a nonzero finitely generated $\mathbb{Z}$-module such that $\alpha M \subseteq M$. Let $w_1, \ldots, w_s$ be a generating set for $M$ over $\mathbb{Z}$. For each $w_i$, write

$$\alpha w_i = \sum_{j=1}^{s} c_{ij}w_j, \quad c_{ij} \in \mathbb{Z}$$

which is possible since $\alpha w_i \in M$. Let $C$ be the matrix $C = (c_{ij})$. Notice that

$$\alpha I(w_1, \ldots, w_s)^t = C(w_1, \ldots, w_s)^t,$$

meaning

$$(\alpha I - C)(w_1, \ldots, w_s)^t = 0.$$

Therefore $\det(\alpha I - C) = 0$, and so $\alpha$ is a solution to the polynomial $f(x) = \det(xI - C)$, which is a monic polynomial with coefficients in $\mathbb{Z}$ (as entries of C are integers). Therefore $\alpha \in \mathcal{O}_K$. □

Using this, we can show $\mathcal{O}_K$ is a ring.

**Theorem 2.3.9.** *Suppose $\alpha, \beta \in \mathcal{O}_K$, where $K$ is some number field. Then $\alpha + \beta$ and $\alpha\beta$ are both in $\mathcal{O}_K$, meaning $\mathcal{O}_K$ is a ring.*

*Proof.* Let $\alpha, \beta \in \mathcal{O}_K$. By the previous lemma, $M = \mathbb{Z}[\alpha]$ and $N = \mathbb{Z}[\beta]$ are nonzero finitely generated $\mathbb{Z}$-modules such that $\alpha M \subseteq M$ and $\beta N \subseteq N$ (see the proof of the lemma). Suppose $M$ is generated by $\{v_1, \ldots, v_m\}$ and $N$ is generated by $\{w_1, \ldots, w_n\}$. Then consider $MN$, where

$$MN = \left\{ \sum_{i=1}^{k} m_i n_i : m_i \in M, n_i \in N \right\}.$$

It is clear that $MN$ is generated by $\{v_i w_j\}$ where $1 \leq i \leq m$ and $1 \leq j \leq n$. Moreover

$$(\alpha + \beta)MN \subseteq (\alpha M)N + M(\beta)N \subseteq MN$$

and

$$\alpha\beta MN \subseteq (\alpha M)(\beta N) \subseteq MN.$$

Therefore $\alpha + \beta$ and $\alpha\beta$ are in $\mathcal{O}_K$ by the previous lemma. □

As a simple consequence, we have the following proposition.

**Proposition 2.3.10.** *If $K$ is a number field and $\alpha \in \mathcal{O}_K$, then $Tr_{K/\mathbb{Q}}(\alpha), Norm_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

*Proof.* Suppose $\alpha \in \mathcal{O}_K$, and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ denote the conjugates of $\alpha$ in a splitting field $L$ (of the minimal polynomial of $\alpha$ over $\mathbb{Q}$). Then $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ as each of the $\alpha_i$ satisfies the same minimal polynomial as $\alpha$. Since the trace and norm are the sum and product of these conjugates, respectively,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha), \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \in \mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}.$$

□

There is also the following proposition.

**Proposition 2.3.11.** *Suppose $\alpha \in \mathcal{O}_K$ for some number field $K$. Then $\alpha$ is a unit (i.e. $\alpha^{-1} \in \mathcal{O}_K$) if and only if $Norm_{K/\mathbb{Q}} = \pm 1$.*

*Proof.* First suppose $\alpha$ is a unit. Then $\alpha^{-1} \in \mathcal{O}_K$, so $\alpha\alpha^{-1} = 1$. Then as the norm is multiplicative,

$$\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)\mathrm{Norm}_{K/\mathbb{Q}}(\alpha^{-1}) = \mathrm{Norm}_{K/\mathbb{Q}}(1) = 1.$$

By the previous proposition, $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$, and so $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|1$ in $\mathbb{Z}$, which implies

$$\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1.$$

Conversely, suppose $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = 1$. Let $m(x) \in \mathbb{Z}[x]$ denote the minimal polynomial of $\alpha$ over $\mathbb{Z}$ (as $\alpha \in \mathcal{O}_K$ this makes sense) and let $L$ be a splitting

field of $m(x)$ which contains $K$. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ denote the $n$ conjugates of $\alpha$ in $L$ (where $n = \deg m(x)$). The norm is the product of these conjugates, so

$$\alpha(\alpha_2 \cdots \alpha_n) = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = 1,$$

meaning

$$\alpha^{-1} = \pm\alpha_2 \cdots \alpha_n.$$

However, $\alpha^{-1} \in K$ (as $K$ is a field), and $\alpha_2 \cdots \alpha_n \in \mathcal{O}_L$ as $\mathcal{O}_L$ is a ring. Therefore $\alpha^{-1} \in \mathcal{O}_L \cap K = \mathcal{O}_K$, meaning $\alpha$ is a unit. □

Note that the hypothesis that $\alpha \in \mathcal{O}_K$ is important. There could be elements of norm 1 in $K$, and although they are trivially units in $K$ (as all nonzero elements of $K$ are invertible), they need not be in $\mathcal{O}_K$. For example, take $K = \mathbb{Q}(i)$, so $\mathcal{O}_K = \mathbb{Z}[i]$. In Example 2.1.7, we proved

$$\mathrm{Norm}_{K/\mathbb{Q}}(a + bi) = a^2 + b^2.$$

We then see that the element $\frac{3}{5} + \frac{4}{5}i \in K$ has norm 1 but is not in $\mathcal{O}_K$, and thus is not a unit in $\mathcal{O}_K$.

### 2.3.3 Extension of Dedekind Rings

We now prove that the ring of integers of a number field is a Dedekind ring. Once we show this, then by Theorem 2.2.30, we will also have unique factorization of ideals for $\mathcal{O}_K$, which is a tool we use continuously through this chapter and the next.

#### A Bilinear Form

We will not prove everything, unfortunately. There are a few theorems which will only be stated because they are necessary for the proof of the main theorem. For this section, the proofs can be found in [9].

Let $L$ be a finite dimensional extension of $K$. Proposition 2.1.6 proves that the trace map of $L/K$ is a $K$-linear mapping. So define a $K$-bilinear form $L \times L \to K$ as

$$(x, y) = \mathrm{Tr}_{L/K}(xy).$$

It is left to the reader to verify (quite easily) that this is a symmetric bilinear form. Recall the following definition from linear algebra:

**Definition 2.3.12.** Let $V$ be a finite dimensional vector space over a field $K$, and let $B : V \times V \to K$ be a (symmetric) $K$-bilinear form. Then $B$ is said to be *nondegenerate* if for all $v \in V$ there exists $w \in V$ with $B(v, w) \neq 0$.

The trace bilinear form provides useful information about the extension $L/K$.

**Theorem 2.3.13.** *If $L/K$ is a finite field extension, then $L$ is separable over $K$ if and only if the bilinear form $(x, y) = Tr_{L/K}(xy)$ from $L \times L \to K$ is nondegenerate.*

There is a simple consequence of this which will be needed. Recall from linear algebra that with a symmetric, nondegenerate bilinear form and a basis of a vector space, we can find a dual basis. Formally:

**Theorem 2.3.14.** *Let $L$ be a finite dimensional separable extension of $K$, and let $u_1, \ldots, u_n$ be a basis of $L$ over $K$. Then there exists a basis $v_1, \ldots, v_n$ of $L$ over $K$ (called the* dual basis *with respect to the bilinear form $Tr_{L/K}$) such that $Tr_{L/K}(u_i v_j) = \delta_{ij}$, where $\delta_{ij}$ is the Kronecker delta symbol.*

Anyone who has taken a linear algebra course will probably have seen this already.

### The proof that $\mathcal{O}_K$ is a Dedekind ring

The last theorem we will need is a characterization of Dedekind rings. Again, we will not prove this, but the proof can be found in [9], Section 1.3.

**Theorem 2.3.15.** *Let $R$ be an integral domain which is not a field. Then $R$ is a Dedekind ring if and only if $R$ is a Noetherian, integrally closed domain such that each nonzero prime ideal of $R$ is maximal.*

It is this alternative definition which we use to prove the main theorem. Before stating the theorem, let us prove a couple of necessary lemmas.

**Lemma 2.3.16.** *Suppose $R \subset R'$ are integral domains with $R$ integrally closed and $R'$ integral over $R$. If $\mathfrak{P}$ is a nonzero prime ideal of $R'$, then $\mathfrak{P} \cap R$ is a nonzero prime ideal of $R$.*

*Proof.* Take $0 \neq x \in \mathfrak{P}$. As $R'$ is integral over $R$, $x$ satisfies some monic polynomial in $R[x]$. So let

$$f(t) = a_0 + a_1 t + \ldots + a_r t^r + t^{r+1} \in R[x]$$

be the polynomial of lowest degree satisfied by $x$. This ensures that $a_0 \neq 0$. Then

$$a_0 = -a_1 x - \ldots - x^{r+1} \in \mathfrak{P} \cap R.$$

Thus $\mathfrak{P} \cap R \neq \{0\}$. To show it is a prime ideal, suppose $xy \in \mathfrak{P} \cap R$, for some two elements $x, y \in R$. Then $xy \in \mathfrak{P}$, which means either $x \in \mathfrak{P}$ or $y \in \mathfrak{P}$ (as $\mathfrak{P}$ is a prime ideal). But as $x, y \in R$, this means either $x \in \mathfrak{P} \cap R$ or $y \in \mathfrak{P} \cap R$, meaning $\mathfrak{P} \cap R$ is a prime ideal, as required. □

**Lemma 2.3.17.** *If $K$ is a field and $R'$ is an integral domain containing $K$ and integral over $K$, then $R'$ is a field.*

*Proof.* If $R'$ is not a field, then it must have some proper nonzero maximal ideal, say $\mathfrak{P} \neq R'$. By the previous lemma, $\mathfrak{P} \cap K$ is a nonzero prime ideal of $K$. As $K$ is a field and all nonzero ideals contain $1 \in K$, $1 \in \mathfrak{P} \cap K$. But then $1 \in \mathfrak{P}$, and so $\mathfrak{P} = R'$, a contradiction. Therefore $R'$ is a field. □

Now to the main theorem.

**Theorem 2.3.18.** *Let $R$ be a Dedekind ring with quotient field $K$ and let $L$ be a finite dimensional separable extension of $K$. Then the integral closure of $R$ in $L$ is a Dedekind ring.*

*Proof.* Let $R'$ be the integral closure of $R$ in $L$, so that we have the following.

$$\begin{array}{ccc} L & \hookleftarrow & R' \\ | & & | \\ K & \hookleftarrow & R \end{array}$$

We will show that $R'$ satisfies the criteria given to us by the previous theorem. First, notice that $R'$ is integrally closed. If there is an element $a$ of $L$ which is integral over $R'$, then it would be integral over $R$ (verify if necessary). But as $R'$ is the integral closure of $R$ in $L$, we must have $a \in R'$. So $R'$ is integrally closed.

Next, we will show $R'$ is Noetherian. Select a basis $a_1, \ldots, a_n$ of $L$ over $K$. In much the same way as in Proposition 2.3.7, we can multiply each $a_i$ by an element of $R$ so that the new element lives in $R'$. Since we can do this with each individual element, we can find one $r \in R$ such that $ra_1, \ldots, ra_n$ is a basis of $L$ over $K$ (it is still linearly independent) and the basis elements lie in $R'$. So we can assume without loss of generality that the $a_i \in R'$ to begin with. Now let $b_1, \ldots, b_n$ be a dual basis of $L$ over $K$, which exists by Theorem 2.3.14. So

$$\mathrm{Tr}_{L/K}(a_i b_j) = \delta_{ij}.$$

The goal is to show

$$R' \subseteq \sum Rb_j.$$

Pick $y \in R'$ and write

$$y = \sum c_j b_j, \quad c_j \in K,$$

which is possible since the $\{b_j\}$ form a basis for $L$ over $K$. But notice that we have

$$\mathrm{Tr}_{L/K}(ya_j) = (y, a_j) = \sum c_k (b_k, a_j) = c_j.$$

But as $y, a_j \in R'$, so is $ya_j$ (the proof of this is very similar to the proof that $\mathcal{O}_K$ is a ring). But since $ya_j \in R'$, by an argument completely analagous to the one in

Proposition 2.3.10, $\mathrm{Tr}_{L/K}(ya_j) \in R' \cap K$. As $R$ is integrally closed, $R' \cap K = R$, as elements of $K$ which are integral over $R$ must be in $R$. Therefore

$$c_j = \mathrm{Tr}_{L/K}(ya_j) \in R' \cap K = R,$$

and thus

$$y \in \sum Rb_j.$$

Hence

$$R' \subseteq \sum Rb_j \subseteq L.$$

Thus $R'$ is a submodule of a finitely generated $R$-module. By Proposition 2.2.16, the finitely generated $R$-module

$$\sum Rb_j$$

is Noetherian, and so $R'$ is finitely generated as an $R$-module. But this clearly implies $R'$ is finitely generated as an $R'$-module, meaning $R'$ is Noetherian, as required.

Finally, we need nonzero prime ideals of $R'$ to be maximal, so let $\mathfrak{P}$ be a nonzero prime ideal of $R'$. By Lemma 2.3.16, $\mathfrak{p} = R \cap \mathfrak{P}$ is a nonzero prime ideal of $R$. Since $R$ is a Dedekind ring, $R/\mathfrak{p}$ is a field (as $\mathfrak{p}$ is a maximal ideal of $R$), and $R'/\mathfrak{P}$ is an integral domain (as $\mathfrak{P}$ is a prime ideal of $R'$) containing a copy of $R/\mathfrak{p}$. Take $\bar{x} = x + \mathfrak{P} \in R'/\mathfrak{P}$ with $x \in R'$. Then there exists a monic polynomial

$$f(t) = c_0 + c_1 t + \ldots + t^m \in R[x]$$

with $f(x) = 0$ because $x$ is integral over $R$. But reducing the coefficients mod $\mathfrak{p}$ gives a polynomial in $(R/\mathfrak{p})[x]$ with $\bar{x}$ as a root. Therefore $R'/\mathfrak{P}$ is integral over $R/\mathfrak{p}$. But then by Lemma 2.3.15, $R/\mathfrak{P}$ is a field, meaning $\mathfrak{P}$ is maximal, as required. □

**Corollary 2.3.19.** *If $K$ is a number field, $\mathcal{O}_K$ is a Dedekind ring.*

*Proof.* We have seen that $\mathbb{Z}$ is a Dedekind ring. Since $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in a separable extension of $\mathbb{Q}$, Theorem 2.3.18 implies $\mathcal{O}_K$ is a Dedekind ring. □

By using the proof of Theorem 2.3.18, we can actually conclude that $\mathcal{O}_K$ is a *free module* of rank $n = [K : \mathbb{Q}]$ over $\mathbb{Z}$. First, recall the definition of a free module (from [5]).

**Definition 2.3.20.** An $R$-module $M$ is called *free* on the subset $A \subset M$ if for every $m \in M$ there exist unique nonzero elements $r_1, \ldots, r_n \in R$ and unique $a_1, \ldots, a_n$ of $A$ such that

$$m = r_1 a_1 + r_2 a_2 + \ldots + r_n a_n.$$

If $R$ is assumed to be commutative, then $A$ is a set of free generators for $M$ (or a basis), and $|A|$ is called the *rank* of $M$.

It can be shown that every free $R$-module of finite rank has the form $R^m$ for some $m \in \mathbb{N}$. As a non-example, consider $R = \mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then the set $\{(1,0),(0,1)\}$ is a generating set for $M$. However, it is not free. For example, the element $(1,0)$ can be written as $(1,0)$, or $3 \cdot (1,0)$, or $5 \cdot (1,0)$, and so on. So the representation of elements as $R$-linear combinations of elements of $M$ is not unique. Therefore $M$ is not free (though it is finitely generated). This example provides a nice segue to the following theorem.

**Theorem 2.3.21.** *Let $R$ be a PID and let $M$ be a finitely generated $R$-module. Then $M$ has the following form:*

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m),$$

*where $r \geq 0$ and $a_1, a_2, \ldots, a_m \in R \backslash R^\times$ with $a_1 | a_2 | \ldots | a_m$.*

For obvious reasons, this is called the structure theorem for finitely generated modules over a PID. Thus if $R$ is a PID, every finitely generated $R$-module has a free part, as seen by the $R^r$, and a torsion part, namely the $m$ quotient summands. In particular, this theorem shows that for $R$ a PID, a submodule of a free $R$-module of finite rank is also free, and of no bigger rank.

Using these ideas, it becomes fairly straightforward to prove that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module.

**Theorem 2.3.22.** *If $L$ is a number field, then $\mathcal{O}_L$ is a free module of rank $n = [L : \mathbb{Q}]$.*

*Proof.* Recall that in Theorem 2.3.18, we had the following setup:

$$\begin{array}{ccc} L & \hookleftarrow & R' \\ | & & | \\ K & \hookleftarrow & R \end{array}$$

Notice that in the proof of that theorem, there came a point where we had

$$R' \subseteq \sum Rb_j,$$

where $b_j$ was a basis of $L/K$. This means that $R'$ is contained in a free $R$-module of rank $n (= [L : K])$. Similarly, using the original basis we had for $L/K$, namely $\{a_1, \ldots, a_n\} \subset R'$, it is clear that

$$\sum Ra_j \subseteq R'.$$

Thus $R'$ contains a free $R$-module of rank $n$ (free as the set $\{a_i\}$ was a basis). Now take $R = \mathbb{Z}$, so that $K = \mathbb{Q}$, $R' = \mathcal{O}_L$, and $L$ is our number field. Then as $\mathbb{Z}$ is a PID, the structure theorem says that $\mathcal{O}_L$ must be a free module of rank $\leq n$ by the first containment, and must also have rank $\geq n$ by the second containment. Therefore $\mathcal{O}_L$ is a free $\mathbb{Z}$-module of rank $n$. $\square$

This also shows that for number fields $K$, $\mathcal{O}_K$ will have an *integral basis*. That is, it will have a generating set of $n$ elements which are $\mathbb{Z}$-linearly independent.

To summarize, we have shown that $\mathcal{O}_K$ is a Dedekind ring, meaning there is unique factorization of ideals into prime ideals. We have also shown that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

### 2.3.4 Discriminant

For this section we will have the following setup. Let $R$ be a Dedekind ring, $K$ its quotient field. Also let $L/K$ be a finite, separable extension, and $R'$ the integral closure of $R$ in $L$. So the diagram is as follows:

$$\begin{array}{ccc} L & \hookleftarrow & R' \\ | & & | \\ K & \hookleftarrow & R \end{array}$$

In this section, we introduce the discriminant, which will be an extremely important tool for studying the factorization of ideals in extensions. The notes for this section come from a combination of [9] and [12].

**Definition 2.3.23.** Suppose $\{x_1, x_2, \ldots, x_n\}$ is a basis for $L/K$ (so $n = [L : K]$). Then the *discriminant* of this basis is defined as

$$\Delta(x_1, x_2, \ldots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j)).$$

Of course, this definition applies to number fields. If $K = \mathbb{Q}$ and $L$ is a a number field of degree $n$ over $\mathbb{Q}$, then we can calculate the discriminant of a number field. In fact, there is a nice way of calculating discriminants which uses the $n$ embeddings $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$. The proof of this fact is outlined in [6].

**Proposition 2.3.24.** *Suppose $L/\mathbb{Q}$ is a number field of degree $n$ and the $\sigma_i$ are the $n$ embeddings as described above. If $\{x_1, \ldots, x_n\}$ is a basis for $L/\mathbb{Q}$, then*

$$\Delta(x_1, \ldots, x_n) = [\det(\sigma_i(x_j))]^2.$$

*Proof.* Suppose $M = (\sigma_i(x_j))$. Simply observe that

$$\begin{aligned} \det(\mathrm{Tr}_{L/K}(x_i x_j)) &= \det\left(\sum_{k=1}^{n} \sigma_k(x_i x_j)\right) \quad \text{(Theorem 2.1.10)} \\ &= \det\left(\sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j)\right) \quad (\sigma_i \text{ are homomorphisms}) \\ &= \det(M^t M) \\ &= \det(M)^2, \end{aligned}$$

which is what we wanted. □

**Example 2.3.25.** Let $K = \mathbb{Q}(\alpha)$, where $\alpha$ is a root of the irreducible polynomial $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ (so it has no roots in $\mathbb{Z}$). Let us try to calculate $\Delta(1, \alpha)$, as $\{1, \alpha\}$ is clearly a basis for $K/\mathbb{Q}$. With any luck, the answer we get will agree with what we already know as the discriminant of a quadratic polynomial. Let us use both formulations. If we denote the other root of $f(x)$ as $\bar{\alpha}$, then the two embeddings are given by the maps

$$\sigma_1 : K \to \mathbb{C}, \quad \alpha \mapsto \alpha,$$

$$\sigma_2 : K \to \mathbb{C}, \quad \alpha \mapsto \bar{\alpha}.$$

(a) Using the trace definition: with Theorem 2.1.10, we can easily calculate

$$\mathrm{Tr}_{K/\mathbb{Q}}(1) = 2, \quad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = -a.$$

The last element we need the trace of is $\alpha^2 = -a\alpha - b$. Using the linearity of the trace we find

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2) = \mathrm{Tr}_{K/\mathbb{Q}}(-a\alpha - b) = -a\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) - \mathrm{Tr}_{K/\mathbb{Q}}(b) = -a^2 - 2b.$$

Therefore

$$\Delta(1, \alpha) = \det \begin{pmatrix} 2 & -a \\ -a & a^2 - 2b \end{pmatrix} = a^2 - 4b,$$

which is the discriminant of the quadratic as we know it.

(b) With the other formula, we find

$$\Delta(1, \alpha) = \left[\det \begin{pmatrix} 1 & \alpha \\ 1 & \bar{\alpha} \end{pmatrix}\right]^2 = (\alpha - \bar{\alpha})^2 = (\alpha + \bar{\alpha})^2 - 4\alpha\bar{\alpha} = a^2 - 4b,$$

which agrees with the answer in (a).

There is a special case we can consider.

**Proposition 2.3.26.** *Suppose $L/\mathbb{Q}$ is a number field of degree $n$, and suppose $L = \mathbb{Q}(\alpha)$ for some $\alpha \in L$. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of $\alpha$ over $\mathbb{Q}$. Then*

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} Norm_{L/\mathbb{Q}}(f'(\alpha)).$$

*Remark* 2.3.27. Since $L/\mathbb{Q}$ is a finite extension of characteristic zero fields, it is separable. Hence $f'(\alpha) \neq 0$, since if it were then $f(x) \in \mathbb{Q}[x]$ would not be separable.

*Proof.* This proof makes use of the Vandermonde determinant, which is a formula from linear algebra. Let $\sigma_i$, $1 \leq i \leq n$, be the $n$ embeddings of $L$ into $\mathbb{C}$, and

let $\alpha = \alpha_1, \ldots, \alpha_n$ denote the $n$ conjugates of $\alpha$ (that is, $\alpha_i = \sigma_i(\alpha)$). From the previous proposition,

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \det(\sigma_i(\alpha^j))^2 = \det(\alpha_i^j)^2.$$

The Vandermonde determinant formula says that this is precisely

$$\det(\alpha_i^j)^2 = \left(\prod_{i<j}(\alpha_i - \alpha_j)\right)^2.$$

Notice

$$(\alpha_i - \alpha_j)^2 = -(\alpha_j - \alpha_i)(\alpha_i - \alpha_j).$$

Applying this to each term in the product, we get

$$\left(\prod_{i<j}(\alpha_i - \alpha_j)\right)^2 = (-1)^{n(n-1)/2}\prod_i\left(\prod_{j\neq i}(\alpha_i - \alpha_j)\right).$$

Now, we know that $f(x)$ factors as

$$f(x) = (x - \alpha)(x - \alpha_2)\cdots(x - \alpha_n)$$

in the Galois closure of $L$. We will leave it to the reader to check that this implies

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

Therefore

$$(-1)^{n(n-1)/2}\prod_i\left(\prod_{j\neq i}(\alpha_i - \alpha_j)\right) = (-1)^{n(n-1)/2}\prod_j f'(\alpha_j) = (-1)^{n(n-1)/2}\prod_j f'(\sigma_j(\alpha)).$$

The coefficients of $f'(x)$ are in $\mathbb{Q}$, and the $\sigma_i$ necessarily fix $\mathbb{Q}$ (any homomorphism will fix $\mathbb{Q}$), the reader can verify that

$$(-1)^{n(n-1)/2}\prod_j f'(\sigma_j(\alpha)) = (-1)^{n(n-1)/2}\prod_j \sigma_j(f'(\alpha)) = (-1)^{n(n-1)/2}\mathrm{Norm}_{L/\mathbb{Q}}(f'(\alpha)).$$

□

This is just a helpful formula for when we want to calculate discriminants of sets of this form (which we will do later).

Now let us return to the situation we had to begin with. While we have technically defined the discriminant, we are most interested in the discriminants of bases of $L/K$ that lie in $\mathcal{O}_K$. If $\{x_1, \ldots, x_n\}$ is a basis for $L/K$ such that $x_i \in R'$

for all $j$, then $x_i x_j \in R'$ for all $i, j$, and consequently $\mathrm{Tr}_{L/K}(x_i x_j) \in K \cap R' = R$. Taking the determinant, we find

$$\Delta(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j)) \in R.$$

Since this is true for any basis of $L/K$ lying in $R'$, we can consider the ideal generated by the discriminants of all such bases. This ideal is what we refer to as the discriminant, sometimes referred to as the *relative discriminant* of $L/K$.

**Definition 2.3.28.** The discriminant ideal $\Delta = \Delta(R'/R)$ is defined as the ideal generated by $\Delta(x_1, \ldots, x_n)$, where the $\{x_1, \ldots, x_n\}$ range over all bases of $L/K$ such that $x_i \in R'$ for all $i$.

It may seem like calculating this ideal is a complicated procedure because we have to somehow consider all such bases. However, in number fields it is not so intimidating because of the following lemma.

**Lemma 2.3.29.** *If $R'$ is a free $R$ module with generators $x_1, \ldots, x_n$, then $\Delta(R'/R) = R\Delta(x_1, \ldots, x_n)$.*

*Proof.* Suppose $\{y_1, \ldots, y_n\}$ is a basis for $L/K$ with $y_i \in R'$ for all $i$. Since the $x_i$ are generators for $R'$ over $R$, we have

$$y_i = \sum_{j=1}^{n} c_{ij} x_j, \quad c_{ij} \in R.$$

We need to relate the matrix $[\mathrm{Tr}_{L/K}(y_i y_j)]$ to the matrix $[\mathrm{Tr}_{L/K}(x_i x_j)]$, and letting $C = [c_{ij}]$, a simple calculation shows

$$[\mathrm{Tr}_{L/K}(y_i y_j)] = C[\mathrm{Tr}_{L/K}(x_i x_j)]C^t.$$

Taking determinants, we find

$$\Delta(y_1, \ldots, y_n) = \det(C)^2 \Delta(x_1, \ldots, x_n).$$

Since $\det(C) \in R$, $\Delta(y_1, \ldots, y_n)$ is in the principal ideal generated by $\Delta(x_1, \ldots, x_n)$, which proves the inclusion

$$\Delta(R'/R) \subseteq R\Delta(x_1, \ldots, x_n).$$

The other conclusion is obvious from the definition. □

This applies to number fields because we have seen that for number fields $K$, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Taking a look at Lemma 2.3.29, we see that the $x_i$ were any set of $\mathbb{Z}$-generators. In fact, if we took the $\{y_i\}$ to be the set of generators, then the ideal generated by

$\Delta(y_1, \ldots, y_n)$ would have been the same as the one generated by $\Delta(x_1, \ldots, x_n)$. This is because the change of basis matrix $C$ above would have to be invertible since both sets are bases. Therefore $\det(C)$ is a unit in $R$, and hence so is $\det(C)^2$. So $\Delta(y_1, \ldots, y_n)$ and $\Delta(x_1, \ldots, x_n)$ differ by the square of a unit, and therefore generate the same principal ideal. In particular, if $R = \mathbb{Z}$ and $R' = \mathcal{O}_K$ for some number field $K$, then this shows $\Delta(\mathcal{O}_K/\mathbb{Z})$ is a well-defined integer, as the only element in $\mathbb{Z}^{\times 2}$ is 1. Hence the discriminants of any two integral bases must be equal. We refer to the *absolute discriminant* of a number field as being this well-defined integer.

An an exercise, the reader can prove that if $K = \mathbb{Q}(\sqrt{d})$, where $d$ is squarefree, then

$$\Delta(\mathcal{O}_K/\mathbb{Z}) = \begin{cases} 4d & \text{if } d \equiv 2, 3 \bmod 4 \\ d & \text{if } d \equiv 1 \bmod 4 \end{cases}.$$

(Hint: Use the integral basis we calculated.)

One last fact which we will not prove is the following.

**Proposition 2.3.30.** *Suppose $K$ is a number field over $\mathbb{Q}$ of degree $n$ with ring of integers $\mathcal{O}_K$. Take $n$ elements $w_1, \ldots, w_n$ in $\mathcal{O}_K$. Then the $\mathbb{Z}$-submodule of $\mathcal{O}_K$ they form (call it $N$) is of finite index in $\mathcal{O}_K$ if and only if $\Delta(w_1, \ldots, w_n) \neq 0$. Moreover, if this is the case, then*

$$\Delta(w_1, \ldots, w_n) = (\mathcal{O}_K : N)^2 \Delta(\mathcal{O}_K/\mathbb{Z}).$$

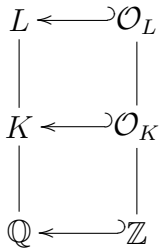
In particular, if the discriminant of the $n$ elements $w_1, \ldots, w_n$ is squarefree as an element of $\mathbb{Z}$, then they form an integral basis for $\mathcal{O}_K$.

### 2.3.5 Factoring Prime Ideals in Extensions

Before moving on, let us make a quick note. We have been providing theorems and proofs in a very general setting, only showing how it applies to number fields after the proofs. However, at this point, we will start using extensions of number fields and their ring of integers instead of arbitrary extensions of Dedekind rings. This will help narrow our attention to the true subject of this thesis.

#### Ramification Index

This section will follow a bit of both [9] and [12]. Suppose now that we have the following.




Here $\mathcal{O}_L$ and $\mathcal{O}_K$ are the ring of integers of the number fields $L$ and $K$, where $L/K$ is a finite extension. Of course, $\mathcal{O}_L$ is still the integral closure of $\mathcal{O}_K$ in $L$. Since $\mathcal{O}_L$ is a Dedekind ring, we know by Theorem 2.2.30 that there is unique factorization of ideals. One question we can ask is: if we take a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, how does it factor as an ideal in $\mathcal{O}_L$? We should be a little careful because the ideal we want to consider is $\mathfrak{p}\mathcal{O}_L$, as this makes it into an ideal in $\mathcal{O}_L$. However, by Theorem 2.2.30, we can say

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g},$$

where the $\mathfrak{P}_i$ are distinct prime ideals of $\mathcal{O}_L$, and the $e_i \in \mathbb{Z}$ with $e_i \geq 1$.

**Definition 2.3.31.** Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ with $\mathfrak{p}\mathcal{O}_L$ having the factorization as above. Then:

(a) If one of the $e_i > 1$, then $\mathfrak{p}$ is *ramified* in $\mathcal{O}_L$. Otherwise $\mathfrak{p}$ is *unramified* in $\mathcal{O}_L$. Sometimes we say $\mathfrak{p}$ is ramified (or unramified) in $L$ instead of $\mathcal{O}_L$.

(b) The number $e_i$ is called the *ramification index* of $\mathfrak{P}_i$, and is denoted $e(\mathfrak{P}_i/\mathfrak{p})$.

(c) We say $\mathfrak{P}$ divides $\mathfrak{p}$ if it occurs in the factorization of $\mathfrak{p}\mathcal{O}_L$.

(d) If the prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ occurs in the factorization of $\mathfrak{p}\mathcal{O}_L$, then $\mathfrak{P}$ is a prime *lying above* $\mathfrak{p}$.

The following theorem is a very powerful result, though we will not prove it immediately. We sketch a proof in Chapter 5 once we introduce the Minkowski bound.

**Theorem 2.3.32.** *If $K/\mathbb{Q}$ is a number field, then there exists a prime $p \in \mathbb{Z}$ such that $p\mathcal{O}_K$ is ramified. In particular, there is no unramified extension of $\mathbb{Q}$.*

This theorem is significant because unramified extensions of other fields do exist, but this theorem says that every extension over $\mathbb{Q}$ contains some ramification. This idea will be utilized in several proofs.

The following lemma (from [12]) describes the prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$.

**Lemma 2.3.33.** *A prime ideal $\mathfrak{P}$ divides $\mathfrak{p}$ (i.e. is a prime lying above $\mathfrak{p}$) if and only if $\mathfrak{p} = \mathfrak{P} \cap K$.*

*Proof.* In the forward direction, suppose $\mathfrak{P}$ is a prime lying above $\mathfrak{p}$. Then we know from Theorem 2.2.30 that $\mathfrak{P}$ contains $\mathfrak{p}\mathcal{O}_L$, and hence contains $\mathfrak{p}$. But of course $\mathfrak{p} \subset K$ as well. Therefore $\mathfrak{p} \subset \mathfrak{P} \cap K$. But as $\mathfrak{P} \cap K \neq \mathcal{O}_K$ and $\mathfrak{p}$ is a maximal ideal in $\mathcal{O}_K$ (recall in a Dedekind ring, prime ideals are maximal), we must have $\mathfrak{p} = \mathfrak{P} \cap K$.

Conversely, suppose $\mathfrak{p} = \mathfrak{P} \cap K$. Then $\mathfrak{p} \subset \mathfrak{P}$, and so $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}$ as $\mathfrak{P}$ is an ideal of $\mathcal{O}_L$. Again using Theorem 2.2.30, this means $\mathfrak{P}$ occurs in the factorization of $\mathfrak{p}\mathcal{O}_L$, proving the lemma.

□

*Remark* 2.3.34. We should note that in the lemma above and the subsequent proof, we could replace $K$ with $\mathcal{O}_K$ and everything will still be valid. So alternatively we will use the characterization that a prime ideal $\mathfrak{P}$ divides $\mathfrak{p}$ if and only if $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

This is more or less the formalization of the "to contain is to divide" principle mentioned at the end of section 2.2.4. Nonetheless, we will be utilizing it in proofs later in this section, so it is important to know.

**Example 2.3.35.** Take $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, so $\mathcal{O}_L = \mathbb{Z}[i]$. The ideal $(2) \subset \mathbb{Z}$ is prime, so we can consider how $(2)$ factors in $\mathcal{O}_L$. We claim

$$(2) = (1+i)^2.$$

Notice $(1+i)^2 = 2i$. It is left to the reader to verify that the product of two principal ideals is the principal ideal generated by the product of the generators. Therefore

$$(1+i)^2 = (2i)$$

as ideals. But as $-i$ is a unit in $\mathbb{Z}[i]$

$$(2i) = (-i \cdot 2i) = (2),$$

which proves the claim. We also claim $1+i \in \mathbb{Z}[i]$ is an irreducible element, and since $\mathbb{Z}[i]$ is a PID, this means $1+i$ is a prime element, so the ideal it generates is a prime ideal. To see it is irreducible, suppose $1+i = rs$, where $r, s \in \mathbb{Z}[i]$. Taking norms, we find

$$2 = \mathrm{Norm}_{L/\mathbb{Q}}(1+i) = \mathrm{Norm}_{L/\mathbb{Q}}(r)\mathrm{Norm}_{L/\mathbb{Q}}(s).$$

Since $r, s \in \mathbb{Z}[i]$, their norms are in $\mathbb{Z}$, so one of $\mathrm{Norm}_{L/\mathbb{Q}}(r)$ or $\mathrm{Norm}_{L/\mathbb{Q}}(s)$ is $\pm 1$, meaning one of the elements $r$ or $s$ is a unit. Therefore $1+i$ is irreducible, and by the above reasoning $(1+i)$ is a prime ideal. Therefore the ideal $(2) \subset \mathbb{Z}$ ramifies in $\mathcal{O}_L$.

Later we prove a theorem which helps determine the factorization of prime ideals in extensions, thereby reducing the amount of work needed.

### Residue Field

The next number to define is the residue field degree. However, we will explain why the definition makes sense before defining it. Assume we have the same setup as before, with $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. We have the natural inclusion

$$\mathcal{O}_K \hookrightarrow \mathcal{O}_L.$$

Compose this inclusion map with the natural projection

$$\mathcal{O}_L \twoheadrightarrow \mathcal{O}_L/\mathfrak{P}$$

to get a map

$$\phi : \mathcal{O}_K \to \mathcal{O}_L/\mathfrak{P}.$$

The kernel of this map is easily seen to be $\mathfrak{P} \cap \mathcal{O}_K$, which by Remark 2.3.34 is just $\mathfrak{p}$. Therefore the first isomorphism theorem yields an injective map, which we still call $\phi$,

$$\phi : \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{P}.$$

Since $\mathfrak{p}$ and $\mathfrak{P}$ are both maximal ideals in their respective rings, both $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{P}$ are fields, so we can view $\mathcal{O}_L/\mathfrak{P}$ as a finite extension of $\mathcal{O}_K/\mathfrak{p}$. Therefore the following definition makes sense.

**Definition 2.3.36.** With the above setup, the residue field degree, denoted $f(\mathfrak{P}/\mathfrak{p})$ is defined as

$$f(\mathfrak{P}/\mathfrak{p}) = \left[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}\right].$$

Indeed, if $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then these are fields of characteristic $p$, as they are extensions of $\mathbb{Z}/p\mathbb{Z}$ by the same reasoning as above. It is clear that $f(\mathfrak{P}/\mathfrak{p})$ is a finite number, but we have not shown $\mathcal{O}_K/\mathfrak{p}$ is a finite field, so let us quickly do that now. This proof comes from [6].

**Lemma 2.3.37.** *Suppose $\mathfrak{A} \subset \mathcal{O}_K$ is any ideal. Then $\mathcal{O}_K/\mathfrak{A}$ is a finite ring.*

*Proof.* Choose any $a \in \mathfrak{A} \cap \mathbb{Z}$. Then clearly

$$(a) \subseteq \mathfrak{A} \subseteq \mathcal{O}_K.$$

One easily checks that the map

$$\mathcal{O}_K/(a) \to \mathcal{O}_K/\mathfrak{A}, \quad \alpha + (a) \mapsto \alpha + \mathfrak{A}$$

is a well-defined, surjective homomorphism. Therefore, it suffices to show that $\mathcal{O}_K/(a)$ is finite. Since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, let $\{v_1, \ldots, v_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then $\mathcal{O}_K/(a)$ is isomorphic as an additive group to

$$\bigoplus (\mathbb{Z}/(a))v_i \cong (\mathbb{Z}/(a))^n.$$

Since $\mathbb{Z}/(a)$ is finite, so is $(\mathbb{Z}/(a))^n$ (with cardinality $a^n < \infty$), and thus $\mathcal{O}_K/(a)$ is finite. □

Therefore $\mathcal{O}_K/\mathfrak{p}$ really is a finite field of characteristic $p$, as is $\mathcal{O}_L/\mathfrak{P}$.

### Norms of Ideals

While we are on the subject, let us, very briefly, define the norm of an ideal. As it is not a major topic for this thesis, there is no point in lingering on the subject for too long. However, some examples become easier when utilizing the norm.

In general, if $L/K$ is a finite extension of number fields, then the *norm* of an ideal of $\mathcal{O}_L$ is an ideal in $\mathcal{O}_K$.

**Definition 2.3.38.** If $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_K$, then let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_L$. Then $\mathfrak{P}$ is a prime lying above $\mathfrak{p}$, and the (relative) norm of $\mathfrak{P}$ is defined as

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}.$$

We then extend the norm to all ideals of $\mathcal{O}_L$ multiplicatively. This is possible by unique factorization into prime ideals. If we take the case $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, then as the norm is an ideal in $\mathbb{Z}$, it is principal, generated by some $n \in \mathbb{Z}$. If we restrict to $n \geq 0$, then this norm is unique and so we can make another definition.

**Definition 2.3.39.** In the case of $K = \mathbb{Q}$, for an ideal $\mathfrak{A}$ of $\mathcal{O}_L$, its norm (also called the *absolute norm*) is the unique positive integer $N(\mathfrak{A})$ such that

$$N_{L/\mathbb{Q}}(\mathfrak{A}) = (N(\mathfrak{A})).$$

Recall in the last lemma, we proved that ideals in number fields have finite quotients. It turns out the norm is related to this cardinality.

**Proposition 2.3.40.** *If $\mathfrak{A}$ is a nonzero ideal in $\mathcal{O}_L$, where $L$ is a number field over $\mathbb{Q}$, then*

$$N(\mathfrak{A}) = |\mathcal{O}_L/\mathfrak{A}|.$$

Furthermore, if the ideal is principal, then we can relate the norm to the norm of elements.

**Proposition 2.3.41.** *If $\mathfrak{A} = (\alpha)$, for some $\alpha \in \mathcal{O}_L$, then $N(\mathfrak{A}) = |Norm_{L/\mathbb{Q}}(\alpha)|$.*

Let us take a look at a quick example.

**Example 2.3.42.** Consider $K = \mathbb{Q}(i)$, so $\mathcal{O}_K = \mathbb{Z}[i]$. Consider the ideal $\mathfrak{A} = (1+i) \in \mathbb{Z}[i]$. This is a principal ideal, so $N(\mathfrak{A}) = |\mathrm{Norm}_{K/\mathbb{Q}}(1+i)|$. We calculated the norm of an element $a + bi \in \mathbb{Q}(i)$ in Section 2.1, and found it to be $a^2 + b^2$. Therefore

$$N(\mathfrak{A}) = |\mathrm{Norm}_{K/\mathbb{Q}}(1 + i)| = 1 + 1 = 2.$$

Alternatively, recall Example 2.3.35. There, we found the factorization of the prime ideal $(2) \subseteq \mathbb{Z}$ as

$$(2) = (1 + i)^2 = \mathfrak{A}^2.$$

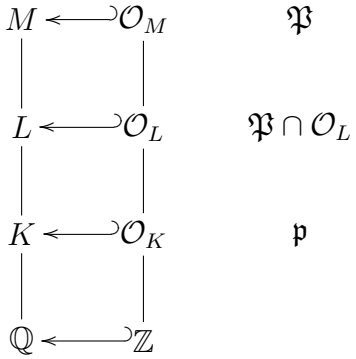
The norm of the ideal $(2)$ in $\mathbb{Z}[i]$ is the norm of the element 2 in $\mathbb{Q}(i)$, which is 4 by the above formula. The norm is multiplcative, so

$$4 = N(\mathfrak{A})^2.$$

Since $N(\mathfrak{A}) \geq 0$, this implies $N(\mathfrak{A}) = 2$, which is the same answer as above.

### Towers of Extensions

One extremely useful fact is that both the ramification index and the residue field degree multiply in towers. Namely, suppose we have the following tower of extensions.




Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_M$ lying above $\mathfrak{p}$. Then by Remark 2.3.34, $\mathfrak{P} \cap \mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$. We will prove the following proposition.

**Proposition 2.3.43.** *With the above setup,*

*(a)* $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P} \cap \mathcal{O}_L)e(\mathfrak{P} \cap \mathcal{O}_L/\mathfrak{p})$*, and*

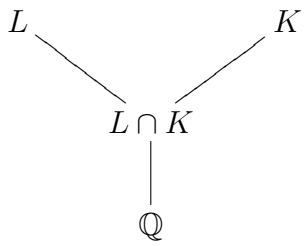
*(b)* $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{P} \cap \mathcal{O}_L)f(\mathfrak{P} \cap \mathcal{O}_L/\mathfrak{p})$.

*Proof.* Statement (b) follows because it is a statement about vector space dimensions, which we know are mutliplicative in towers. To prove (a), let $\mathfrak{P}_L = \mathfrak{P} \cap \mathcal{O}_L$. When we factor $\mathfrak{p}$ in $\mathcal{O}_L$, we know $\mathfrak{P}_L$ occurs in the factorization with exponent $e(\mathfrak{P}_L/\mathfrak{p})$. Moreover, in the factorization of $\mathfrak{P}_L$ in $\mathcal{O}_M$, the prime ideal $\mathfrak{P}$ occurs with exponent $e(\mathfrak{P}/\mathfrak{P}_L)$. Consequently, $\mathfrak{P}$ occurs in the factorization of $\mathfrak{p}$ with exponent $e(\mathfrak{P}/\mathfrak{P}_L)e(\mathfrak{P}_L/\mathfrak{p})$. But as the exponent is also $e(\mathfrak{P}/\mathfrak{p})$, we are done. □

As a simple example of how this can be useful, consider the following.

**Proposition 2.3.44.** *Suppose $L$ and $K$ are number fields over $\mathbb{Q}$, and suppose further that every prime which ramifies in $K$ remains unramified in $L$. Then $K \cap L = \mathbb{Q}$.*

*Proof.* Our diagram looks like this:



Suppose $L \cap K \neq \mathbb{Q}$. Then by Theorem 2.3.32, there must exist a prime $p \in \mathbb{Z}$ which is ramified in $L \cap K$. But by Proposition 2.3.43, $p$ must then be ramified in both $L$ and $K$. By assumption, every prime which ramified in $K$ is unramified in $L$, a contradiction. Therefore $L \cap K = \mathbb{Q}$. □

### Action of Galois group

Before we state and prove the main theorem of the section, let us discuss a special case of the setup we have been considering in previous subsections. If we assume that $L/K$ is a finite *Galois* extension of number fields, we can look at the action of $\mathrm{Gal}(L/K)$ on prime ideals. It should be clear that if $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. Indeed, $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$ because $\sigma$ must send elements of $\mathcal{O}_L$ to solutions of their respective minimal polynomials, which means integral elements are sent to integral elements. Applying the same logic to $\sigma^{-1}$ shows $\sigma^{-1}(\mathcal{O}_L) \subseteq \mathcal{O}_L$, so applying $\sigma$ to both sides shows $\mathcal{O}_L \subseteq \sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$, meaning $\sigma(\mathcal{O}_L) = \mathcal{O}_L$.

We can now take this a step further. Suppose $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ and $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$. We have the following proposition, whose proof comes from [1].

**Proposition 2.3.45.** *With the above notation, $\sigma(\mathfrak{P})$ is another prime ideal lying above $\mathfrak{p}$.*

*Proof.* First, we need to show that $\sigma(\mathfrak{P})$ is in fact a prime ideal. To see this, suppose $\alpha\beta \in \sigma(\mathfrak{P})$, where $\alpha, \beta \in \mathcal{O}_L$. Since $\sigma(\mathcal{O}_L) = \mathcal{O}_L$, there exists $\alpha', \beta' \in \mathcal{O}_L$ with $\alpha = \sigma(\alpha')$ and $\beta = \sigma(\alpha')$. Then

$$\alpha\beta = \sigma(\alpha')\sigma(\beta') = \sigma(\alpha'\beta') \in \sigma(\mathfrak{P}),$$

which means $\alpha'\beta' \in \mathfrak{P}$. As $\mathfrak{P}$ is a prime ideal, either $\alpha' \in \mathfrak{P}$ or $\beta' \in \mathfrak{P}$, meaning at least one of $\alpha, \beta \in \sigma(\mathfrak{P})$. Therefore $\sigma(\mathfrak{P})$ is a prime ideal.

Next, we need to show $\sigma(\mathfrak{P})$ lies above $\mathfrak{p}$. But this will follow almost immediately from Remark 2.3.34. We want to show $\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \mathfrak{p}$. Remember that $\sigma$ fixes element of $\mathcal{O}_K$ and $\mathfrak{p}$ pointwise as both are contained in $K$. Therefore

$$\mathfrak{p} = \sigma(\mathfrak{p}) = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma(\mathfrak{P}) \cap \mathcal{O}_K,$$

which means $\sigma(\mathfrak{P})$ is a prime above $\mathfrak{p}$, as required. □

In fact, what we will show now is that the action of the Galois group on the primes above $\mathfrak{p}$ is *transitive*. This proof comes from [12].

**Lemma 2.3.46.** *Let $L/K$ be a finite Galois extension of number fields. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are two primes of $\mathcal{O}_L$ above $\mathfrak{p}$, then there exists $\sigma \in Gal(L/K)$ with $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.*

*Proof.* Suppose there were no such $\sigma$. Then for all $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\mathfrak{P}_1) \neq \mathfrak{P}_2$. Lemma 2.2.26 implies we can use the Chinese Remainder Theorem (2.2.22), and so there exists $\beta \in \mathcal{O}_L$ such that $\beta \in \mathfrak{P}_2$ but $\beta \notin \sigma(\mathfrak{P}_1)$ for all $\sigma \in \mathrm{Gal}(L/K)$. Let

$$b = \mathrm{Norm}_{L/K}(\beta) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta).$$

Since each $\sigma(\beta) \in \mathcal{O}_L$, their product is as well. Since $b \in K$, we have $b \in K \cap \mathcal{O}_L = \mathcal{O}_K$. Moreover, taking the identity element in $\mathrm{Gal}(L/K)$ shows $\beta$ is in the product, meaning

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta) \in \mathfrak{P}_2$$

as $\mathfrak{P}_2$ is an ideal. That is,

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta) = \beta \cdot \left( \prod_{e \neq \sigma \in \mathrm{Gal}(L/K)} \sigma(\beta) \right) \in \mathfrak{P}_2.$$

Therefore $b \in \mathfrak{P}_2$, and hence $b \in \mathfrak{P}_2 \cap \mathcal{O}_K = \mathfrak{p}$. However, for all $\sigma \in \mathrm{Gal}(L/K)$, we know

$$\beta \notin \sigma^{-1}(\mathfrak{P}_1),$$

meaning $\sigma(\beta) \notin \mathfrak{P}_1$. However, the fact that

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta) = b \in \mathfrak{p} \subset \mathfrak{P}_1$$

contradicts the primality of $\mathfrak{P}_1$. Therefore there must exist $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$. □

We will use this lemma in the next subsection.

### Relating ramification index and residue field degree

We will now prove the following, which comes from [9] (with slight modifications from [12]).

**Theorem 2.3.47.** *Suppose $L/K$ is a finite extension of number fields with respective ring of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. Take $\mathfrak{p}$, a prime ideal of $\mathcal{O}_K$, and consider the factorization in $\mathcal{O}_L$,*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g},$$

*where the $\mathfrak{P}_i$ are distinct prime ideals of $\mathcal{O}_L$. Then*

$$\sum_{i=1}^{g} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) = [L : K].$$

*Proof.* Let $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ and $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. To show equality we will show that both sides are equal to $[\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L : \mathcal{O}_K/\mathfrak{p}]$, starting with the left side. From the Chinese Remainder Theorem (2.2.22), we have the decomposition

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \bigoplus_i \mathcal{O}_L/\mathfrak{P}_i^{e_i}.$$

Therefore, it suffices to show that $\mathcal{O}_L/\mathfrak{P}_i^{e_i}$ has dimension $e_i f_i$ over $\mathcal{O}_K/\mathfrak{p}$. Consider $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$, for $0 \leq a < e_i$. In the section on unique factorization of ideals, corollary 2.2.29 says that the ideal $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$ is principal in the ring $\mathcal{O}_L/\mathfrak{P}_i^{a+1}$, and so it has a single generator as an $\mathcal{O}_L/\mathfrak{P}_i^{a+1}$-module. But as there is a natural inclusion

$$\mathcal{O}_L/\mathfrak{P}_i \hookrightarrow \mathcal{O}_L/\mathfrak{P}_i^{a+1}, \quad \alpha + \mathfrak{P}_i \mapsto \alpha + \mathfrak{P}_i^{a+1},$$

it also has a single generator as an $\mathcal{O}_L/\mathfrak{P}_i$-module. It is therefore a one-dimensional vector space over $\mathcal{O}_L/\mathfrak{P}_i$. But as $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$, this means it is also an $f_i$-dimensional vector space over $\mathcal{O}_K/\mathfrak{p}$. As a vector space, $\mathcal{O}_L/\mathfrak{P}_i^{e_i}$ is the direct sum of the spaces $\mathfrak{P}_i^a/\mathfrak{P}_i^{a+1}$ for $0 \leq a < e_i$, and since each has dimension $f_i$ as an $\mathcal{O}_K/\mathfrak{p}$-vector space, the dimension of $\mathcal{O}_L/\mathfrak{P}_i^{e_i}$ over $\mathcal{O}_K/\mathfrak{p}$ is precisely $e_i f_i$, as required.

Now we need to show this dimension is also $[L : K]$. For simplicity of notation, let $R' = \mathcal{O}_L$ and $R = \mathcal{O}_K$. Consider the localization $R_\mathfrak{p}$ and the correponding localization $R'_\mathfrak{p}$ (that is, our multiplicative set in both cases is the complement of $\mathfrak{p}$ in $R$). In Theorem 2.3.18, we showed that $R'$ is a finitely generated $R$-module, so $R'_\mathfrak{p}$ is a finitely generated module over $R_\mathfrak{p}$. So let $x_1, \ldots, x_n$ be a minimal generating set. Since $R$ is a Dedekind ring, $R_\mathfrak{p}$ is a DVR by definition, and therefore it has a unique maximal ideal. Say it is $R_\mathfrak{p}\pi$ for some $\pi \in R$. We show the $x_i$ form a basis for $L/K$.

To show linear independence, suppose there were a nontrivial dependence relation

$$\sum_{i=1}^{n} a_i x_i = 0,$$

where the $a_i \in K$. Since not all the $a_i$ are zero (by assumption), multiply by a suitable constant so that the $a_i \in R_\mathfrak{p}$. Moreover, by dividing by the highest power of $\pi$ which divides all the $a_i$, we can find a relation where not all the $a_i$ are 0 and at least one $a_i \in R_\mathfrak{p} \backslash R_\mathfrak{p}\pi$. The claim is that $a_i^{-1} \in R_\mathfrak{p}$. To see this, since $a_i \notin R_\mathfrak{p}\pi$, the ideal it generates, namely $R_\mathfrak{p} a_i$, is not in $R_\mathfrak{p}\pi$. But as every proper ideal is contained in a maximal ideal and $R_\mathfrak{p}\pi$ is the unique maximal ideal of $R_\mathfrak{p}$, we must have $R_\mathfrak{p} a_i = R_\mathfrak{p}$. Therefore there exists $a_i^{-1} \in R_\mathfrak{p}$ with $a_i^{-1} a_i = 1$. But then this means

$$x_i = a_i^{-1} \sum_{j \neq i} a_j x_j.$$

Therefore $x_i$ is generated by the $x_j$ for $j \neq i$, contradicting the fact that the $x_i$ were a minimal generating set. Therefore no such dependence relation exists.

Now we show they span, so suppose they did not. Then $\sum_{i=1}^{n} Kx_i$ would be a proper subspace of $L$. That means we can find some $y \in L$ with

$$Ky \cap \sum_{i=1}^{n} Kx_i = \{0\}.$$

Since $y \in L$, there exists some $t \in R$ such that $ty \in R'$. This is exactly the same logic as in Proposition 2.3.7. That is, take the minimal polynomial of $y$ over $K$ and mutliply by a suitable constant so as to cancel the denominators. But if $ty \in R'$, then since $R'_{\mathfrak{p}}$ is generated by the $x_i$ as a module over $R_{\mathfrak{p}}$,

$$ty \in R'_{\mathfrak{p}} = \sum_{i=1}^{n} R_{\mathfrak{p}} x_i \subseteq \sum_{i=1}^{n} Kx_i,$$

which is a contradiction by choice of $y$. Therefore the $x_i$ form a basis of $[L : K]$, meaning $n = [L : K]$.

To finish off the proof, notice we have a vector space isomorphism

$$R'_{\mathfrak{p}}/\mathfrak{p}R'_{\mathfrak{p}} \cong \bigoplus_{i=1}^{n} (R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}})\bar{x_i},$$

where the $x_i$ are the reduction of $x_i$ modulo $\mathfrak{p}R_{\mathfrak{p}}$. Since $\mathfrak{p}$ is maximal in $R = \mathcal{O}_K$, Lemma 2.2.28 applies, and we have an isomorphism

$$R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong R/\mathfrak{p}.$$

Therefore

$$R'_{\mathfrak{p}}/\mathfrak{p}R'_{\mathfrak{p}} \cong \bigoplus_{i=1}^{n} (R/\mathfrak{p})\bar{x_i}.$$

Applying this same lemma to each term in the direct sum

$$R'/\mathfrak{p}R' \cong \bigoplus R'/\mathfrak{P}_i^{e_i}$$

we saw in the beginning of the proof, we find

$$R'_{\mathfrak{p}}/\mathfrak{p}R'_{\mathfrak{p}} \cong \bigoplus R'_{\mathfrak{p}}/\mathfrak{P}_i^{e_i} R'_{\mathfrak{p}} \cong \bigoplus R'/\mathfrak{P}_i^{e_i}.$$

Therefore the dimension of $R'_{\mathfrak{p}}/\mathfrak{p}R'_{\mathfrak{p}}$ as a vector space over $R/\mathfrak{p}$ is also

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

So now back to

$$R'_{\mathfrak{p}}/\mathfrak{p}R'_{\mathfrak{p}} \cong \bigoplus_{i=1}^{n}(R/\mathfrak{p})\bar{x}_i.$$

The left side as a vector space over $R/\mathfrak{p}$ is $\sum e_i f_i$, whereas the right side has dimension $n = [L : K]$. Therefore

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

□

A simple consequence of this theorem is the following.

**Corollary 2.3.48.** *With the same conditions as in the previous theorem, if $L/K$ is also Galois, then all the $e(\mathfrak{P}_i/\mathfrak{p}) = e$ and $f(\mathfrak{P}_i/\mathfrak{p}) = f$. Moreover*

$$efg = [L : K].$$

*Proof.* Let $G = \mathrm{Gal}(L/K)$. Lemma 2.3.46 states that $G$ acts transitively on the primes above $\mathfrak{p}$. It is clear that since the factorization into prime ideals is unique that

$$e(\sigma(\mathfrak{P}_i)/\mathfrak{p}) = e(\mathfrak{P}_i/\mathfrak{p}),$$

for $\sigma \in G$. By transitivity of the action, all the ramification indices must be equal. Moreover, $\sigma$ fixes $\mathcal{O}_K/\mathfrak{p}$ since it fixes elements of $K$ elementwise, and it takes $\mathcal{O}_L/\mathfrak{P}_i$ to $\mathcal{O}_L/\sigma(\mathfrak{P}_i)$ as $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. Therefore

$$f(\sigma(\mathfrak{P}_i)/\mathfrak{p}) = [\mathcal{O}_L/\sigma(\mathfrak{P}_i) : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}] = f(\mathfrak{P}_i/\mathfrak{p}).$$

Again by transitivity of the action of $G$ on the prime ideals above $\mathfrak{p}$, all the residue field degrees must be equal as well. Therefore by looking at the formula in the previous theorem and substituting $e$ for all the $e_i$ and $f$ for all the $f_i$ gives

$$efg = [L : K].$$

□

### Finding Factorizations

Before looking at some concrete examples, let us prove a theorem which will make factoring ideals considerably easier. The statement and proof are from [12].

**Theorem 2.3.49** (Dedekind-Kummer)**.** *Suppose $L/K$ is a finite extension of number fields and $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Let $f(x)$ denote the minimal polynomial of $\alpha$ over $K$, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Let $\bar{f}(x)$ denote the polynomial found by reducing the coefficients of $f(x)$ modulo $\mathfrak{p}$, and suppose $\bar{f}(x) \equiv \prod \bar{g}_i(x)^{e_i}$ mod $\mathfrak{p}$,*

*where the $\bar{g}_i(x)$ are distinct irreducible polynomials in $(\mathcal{O}_K/\mathfrak{p})[x]$. Choose $g_i(x) \in \mathcal{O}_K[x]$ to be any polynomial which reduces to $\bar{g}_i(x)$ modulo $\mathfrak{p}$. Then*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} (\mathfrak{p}, g_i(\alpha))^{e_i}$$

*is the factorization of $\mathfrak{p}\mathcal{O}_L$ into prime ideals. Moreover,*

$$\mathcal{O}_L/(\mathfrak{p}, g_i(\alpha))^{e_i} \cong (\mathcal{O}_K/\mathfrak{p})[x]/(\bar{g}_i(x)),$$

*and so the residue field degree corresponding to this prime ideal is the degree of $g_i(x)$.*

*Proof.* By assumption, $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, and so there is an isomorphism

$$\mathcal{O}_K[x]/(f(x)) \to \mathcal{O}_L, \quad x \mapsto \alpha.$$

Reducing both sides modulo $\mathfrak{p}$ gives an isomorphism

$$\mathbb{F}_\mathfrak{p}[x]/(\bar{f}(x)) \cong \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L, \quad x \mapsto \alpha,$$

where $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. Maximal ideals in $\mathbb{F}_\mathfrak{p}[x]/(\bar{f}(x))$ correspond to those generated by irreducible polynomials which divide $\bar{f}(x)$, which are precisely the $\bar{g}_i(x)$, and

$$\prod_{i=1}^{r} (\bar{g}_i(x))^{e_i} = 0 \in \mathbb{F}_\mathfrak{p}[x]/(\bar{f}(x)),$$

but no smaller powers $e_i$ give zero. Under the isomorphism, the ideal

$$(\bar{g}_i(x)) \mapsto (g_i(\alpha)) + \mathfrak{p}\mathcal{O}_L.$$

Lifting this to an ideal of $\mathcal{O}_L$ gives $\mathfrak{P}_i = (\mathfrak{p}, g_i(\alpha))$ (since it must contain $\mathfrak{p}\mathcal{O}_L$ by the ideal correspondence). Prime ideals are always mapped to prime ideals, and so the $\mathfrak{P}_i$ are a complete set of prime ideals of $\mathcal{O}_L$ which contain $\mathfrak{p}\mathcal{O}_L$, which means they are the ideals which occur in the factorization of $\mathfrak{p}\mathcal{O}_L$. The $e_i$ occuring in the factorization are uniquely determined since earlier we remarked that they were chosen so that no smaller power of $e_i$ accomplished

$$\prod_{i=1}^{r} (\bar{g}_i(x))^{e_i} = 0 \in \mathbb{F}_\mathfrak{p}[x]/(\bar{f}(x)).$$

Therefore the ramification indices are given by these $e_i$. Furthermore, the statement about the residue field degree follows because under the isomorphism,

$$\mathcal{O}_L/(\mathfrak{p}, g_i(\alpha))^{e_i} \cong (\mathcal{O}_K/\mathfrak{p})[x]/(\bar{g}_i(x)),$$

so as an $\mathcal{O}_K/\mathfrak{p}$-vector space, the dimension of $\mathcal{O}_L/(\mathfrak{p}, g_i(\alpha))^{e_i}$ is precisely $\deg g_i(x)$. □

Why this theorem is so useful is that it provides us with a quick way to determine the factorization into prime ideals.

**Examples**

As promised, let us work through a couple of examples.

**Example 2.3.50.** Consider $K = \mathbb{Q}(i)$ and $\mathcal{O}_K = \mathbb{Z}[i]$, just as in our previous examples. This is a Galois extension of $\mathbb{Q}$ (it is the splitting field of $x^2+1 \in \mathbb{Q}[x]$), and the degree of the extension is 2. So all the ramification indices and residue field degrees will be equal for all primes above any prime ideal of $\mathbb{Z}$. We have seen that the prime ideal (2) of $\mathbb{Z}$ factors as

$$(2) = (1+i)^2 = \mathfrak{P}^2.$$

Thus there is only one prime ideal above (2), and its ramification index is $e = 2$. By Corollary 2.3.48, $efg = 2$. Therefore $g = 1$ (which we could have gotten by inspection), and $f = 1$, which means $\mathcal{O}_K/\mathfrak{P} \cong \mathbb{Z}/2\mathbb{Z}$. Also, using this to calculate the norm of $\mathfrak{A}$ using the definition:

$$N(\mathfrak{A}) = (2)^{f(\mathfrak{A}/(2))} = (2)^2 = (4),$$

which is the same answer we got when we calculated the norm previously.

Let us try and factor the ideal (3) of $\mathbb{Z}$ by using the Dedekind-Kummer theorem. In this case, $\alpha = i$ and its minimal polynomial over $\mathbb{Q}$ is $x^2 + 1$. The theorem instructs us to factor $x^2 + 1$ modulo 3. As $-1$ is not a quadratic residue mod 3, $x^2+1$ has no roots mod 3, which means it is irreducible (as any non-trivial factor of a quadratic polynomial would be linear). Therefore (3) remains *inert*, which simply means it remains prime in $\mathcal{O}_K$. Technically, the theorem says

$$(3) = (3, 1 + i^2),$$

but as $1 + i^2 = 0$, we get $(3) = (3)$. Here $e = 1$, meaning 3 is unramified in $K$, and $g = 1$. This also means that $f = 2$, so

$$[\mathcal{O}_K/(3) : \mathbb{Z}/3\mathbb{Z}] = 2,$$

and hence the residue field $\mathcal{O}_K/(3)$ is the field of nine elements.

For the sake of completeness, let us consider the ideal (5) of $\mathbb{Z}$. Factoring $x^2 + 1$ mod 5 gives

$$x^2 + 1 = (x - 2)(x + 2) \bmod 5,$$

so the Dedekind-Kummer theorem says

$$(5) = (5, -2 + i)(5, 2 + i).$$

As $\mathbb{Z}[i]$ is a PID, it would be nice to find generators for these two ideals. Since the (absolute) norm of (5) in $\mathcal{O}_K$ is 25 and norm is multiplicative, the norm

of both these prime ideals must be 5 (no proper ideal has norm 1). Clearly $-2+i \in (5, -2+i)$, so $(-2+i) \subseteq (5, -2+i)$. But the norm of $(-2+i)$ is also 5, so by norm considerations $(-2+i) = (5, -2+i)$. Similarly, $(5, 2+i) = (2+i)$. Therefore

$$(5) = (2+i)(2-i) = \mathfrak{P}_1\mathfrak{P}_2.$$

Here $e = 1$, so 5 is unramified. Also $g = 2$, and so $f = 1$ for both prime ideals above (5). Consequently,

$$\mathcal{O}_K/\mathfrak{P}_1 \cong \mathcal{O}_K/\mathfrak{P}_2 \cong \mathbb{Z}/5\mathbb{Z}.$$

*Remark* 2.3.51. This example introduces two more terms. We defined *inert* in the example itself, and it means that a prime ideal remains prime in the extension field. In the last example, (5) split into as many prime ideal factors as possible, and in this case we say (5) *splits completely*.

**Example 2.3.52.** Let us consider a non-Galois extension, say $K = \mathbb{Q}(\sqrt[3]{2})$. It can be checked that the ring of integers is $\mathbb{Z}[\sqrt[3]{2}]$. This is a degree three number field, but it is not Galois as it is not normal. Consider the prime ideals $(2), (3)$, and $(5)$ in $\mathbb{Z}$. Again, we will use the Dedekind-Kummer theorem. We need to factor the minimal polynomial of $\sqrt[3]{2}$, which is $x^3 - 2$. Let $\alpha = \sqrt[3]{2}$. It is easily verified that

$$x^3 - 2 = x^3 \bmod 2,$$

$$x^3 - 2 = (x+1)^3 \bmod 3,$$

and

$$x^3 - 2 = (x+2)(x^2 + 3x - 1) \bmod 5.$$

Therefore

$$(2) = (2, \alpha)^3 = \mathfrak{p}^3,$$

$$(3) = (3, \alpha + 1)^3 = \mathfrak{q}^3,$$

and

$$(5) = (5, 2 + \sqrt[3]{2})(5, (\sqrt[3]{2})^2 + 3\sqrt[3]{2} - 1) = \mathfrak{P}_1\mathfrak{P}_2.$$

In the factorization of (2), we see $g = 1$, $e = e(\mathfrak{p}/(2)) = 3$, which means $f = 1$ (as $[K : \mathbb{Q}] = 3$). Therefore 2 is ramified (actually *totally ramified*, which means the ramification index is $[K : \mathbb{Q}]$). Moreover, as $f = 1$,

$$\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/2\mathbb{Z}.$$

For the ideal (3), again we have $g = 1$, $e = e(\mathfrak{q}/(3)) = 3$, and therefore $f = 1$. So 3 is also totally ramified in $K$, and

$$\mathcal{O}_K/\mathfrak{q} \cong \mathbb{Z}/3\mathbb{Z}.$$

Finally, for 5, let $e_i$ and $f_i$ denote the ramification indices and residue field degrees corresponding to $\mathfrak{P}_i$. Then we find $e_1 = e_2 = 1$, meaning 5 is unramified

in $K$. We also find $g = 2$. However, $f_1 = 1$ and $f_2 = 2$, so $f_1 \neq f_2$, which shows that they need not be equal if the extension is not Galois. So

$$\mathcal{O}_K/\mathfrak{P}_1 \cong \mathbb{Z}/5\mathbb{Z},$$

but

$$\mathcal{O}_K/\mathfrak{P}_2 \cong \mathbb{F}_{25},$$

the field of 25 elements. But it is still the case that

$$1 \cdot 1 + 1 \cdot 2 = 3,$$

meaning

$$\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}].$$

Observe that in the first example, as $-1 \equiv 3 \bmod 4$, the discriminant $\Delta(\mathcal{O}_K/\mathbb{Z}) = -4 = -2^2$, and 2 ramified in $K$. In the second example, the discriminant is calculated to be $-108 = -1 \cdot 2^2 \cdot 3^3$, and 2 and 3 both ramify. It seems that if a prime divides the discriminant, then it will ramify. As it turns out, this is a necessary and sufficient condition, which leads us into the next section.

### 2.3.6 Ramified Primes

Let us return to our general setting:

$$\begin{array}{ccc} L & \hookleftarrow & R' \\ | & & | \\ K & \hookleftarrow & R \end{array}$$

Recall this means $R$ is a Dedekind ring with quotient field $K$, $L$ is a finite separable extension of $K$, and $R'$ is the integral closure of $R$ in $L$. At this point, we want to prove that the prime ideals of $R$ which ramify in $R'$ are precisely those which contain the discriminant ideal $\Delta(R'/R)$. Of course, for number fields, this will translate to: the prime ideals of $\mathcal{O}_K$ which ramify in $\mathcal{O}_L$ are precisely those containing $\Delta(\mathcal{O}_L/\mathcal{O}_K)$. This proof will mostly be following [9]. First, we have the following lemma.

**Lemma 2.3.53.** *Let $S$ be a multiplicative set in $R$. Then*

$$\Delta(R'_S/R_S) = \Delta(R'/R)_S.$$

*Proof.* We prove both inclusions. For the "$\supseteq$" inclusion, suppose $x_1, \ldots, x_n$ is a basis for $L/K$ contained in $R'$. Then by the natural inclusion $R' \hookrightarrow R'_S$, we can regard the $x_i \in R'_S$. Therefore

$$\Delta(x_1, \ldots, x_n) \in \Delta(R'_S/R_S).$$

Since this is true for any basis of $L/K$ contained in $R'$, we get

$$\Delta(R'_S/R_S) \supseteq \Delta(R'/R),$$

from which is follows that

$$\Delta(R'_S/R_S) \supseteq \Delta(R'/R)R_S,$$

as $\Delta(R'_S/R_S)$ is an ideal in $R_S$. But as $\Delta(R'/R)$ is an ideal in $R$, $\Delta(R'/R)R = \Delta(R'/R)$, so

$$\Delta(R'/R)R_S = \Delta(R'/R)_S.$$

Therefore

$$\Delta(R'_S/R_S) \supseteq \Delta(R'/R)_S.$$

For the reverse inclusion, suppose $y_1, \ldots, y_n$ is a basis for $L/K$ with each $y_i \in R'_S$. Then certainly we can find some $s \in S$ with $sy_i \in R'$ for all $1 \leq i \leq n$. But then

$$\Delta(sy_1, \ldots, sy_n) \in \Delta(R'/R).$$

Also

$$\Delta(sy_1, \ldots, sy_n) = \det[\mathrm{Tr}_{L/K}(sy_i sy_j)] = \det[s^2 \mathrm{Tr}_{L/K}(y_i y_j) = s^{2n}\Delta(y_1, \ldots, y_n),$$

which implies

$$\Delta(y_1, \ldots, y_n) = \frac{\Delta(sy_1, \ldots, sy_n)}{s^{2n}} \in \Delta(R'/R)_S.$$

Since $y_1, \ldots, y_n$ was an arbitrary basis contained in $R'_S$, this yields

$$\Delta(R'_S/R_S) \subseteq \Delta(R'/R)_S.$$

Therefore equality holds. □

There is also a fact from linear algebra which we will need to call upon, so we state it without proof.

**Proposition 2.3.54.** *Suppose $V$ is a finite-dimensional vector space over a field $F$, and let*

$$B : V \times V \to F$$

*be a symmetric, non-degenerate bilinear form. If $v_1, \ldots, v_n$ is a basis for $V$, then the matrix of $B$ with respect to this basis, i.e.*

$$M = [B(v_i, v_j)],$$

*is invertible.*

We will be using the nondegeneracy of the trace bilinear form in separable extensions. We are now in position to prove the theorem.

**Theorem 2.3.55.** *Suppose $R$ and $R'$ are as above, and let $\mathfrak{p}$ be a prime ideal of $R$. Suppose that for every prime $\mathfrak{P}_i$ of $R'$ lying above $\mathfrak{p}$, the extension $R'/\mathfrak{P}$ is separable over $R/\mathfrak{p}$. Then $\mathfrak{p}$ ramifies in $R'$ if and only if $\Delta(R'/R) \subseteq \mathfrak{p}$.*

*Proof.* The proof will come in a series of steps.

(1) **Simplifying the situation**: Consider the localization at $\mathfrak{p}$. It is clear that $\Delta(R'/R) \subseteq \mathfrak{p}$ if and only if $\Delta(R'/R)_{\mathfrak{p}} \subseteq \mathfrak{p}R_{\mathfrak{p}}$. By Lemma 2.3.53, $\Delta(R'/R)_{\mathfrak{p}} = \Delta(R'_{\mathfrak{p}}/R_{\mathfrak{p}})$, so this happens if and only if $\Delta(R'_{\mathfrak{p}}/R_{\mathfrak{p}}) \subseteq \mathfrak{p}R_{\mathfrak{p}}$. Also $\mathfrak{p}$ is ramified in $R'$ if and only if $\mathfrak{p}R_{\mathfrak{p}}$ ramifies in $R'_{\mathfrak{p}}$. Therefore, it suffices to prove the theorem after replacing $R$ with $R_{\mathfrak{p}}$ and $R'$ with $R'_{\mathfrak{p}}$. Since $R$ is a Dedekind ring, $R_{\mathfrak{p}}$ is a DVR, and hence a PID. So we will assume that $R$ is a DVR to begin with and keep the current notation.

(2) **Proving equivalence with a simpler condition**: We know $R'$ is finitely generated over $R$, but now as $R$ is assumed to be a PID and $R'$ is torsion free, by the structure theorem (Theorem 2.3.21), $R'$ is a free $R$-module. Therefore there exist free generators $x_1, \ldots, x_n$ of $R'$ over $R$, which is also a basis for $L/K$. Taking residues modulo $\mathfrak{p}R'$ gives a basis $\bar{x}_1, \ldots, \bar{x}_n$ of $R'/\mathfrak{p}R'$ as a vector space over $R/\mathfrak{p}$. Recall that in the section on norms and traces we considered the regular representation of a field extension over its base field. In the same way, let $y \in R'$ and consider the map

$$r_y : R' \to R', \quad x \mapsto xy,$$

which is $R$-linear. We have a basis $x_1, \ldots, x_n$, so write

$$x_i y = \sum_{j=1}^{n} a_{ij} x_j.$$

Then the matrix of $r_y$ with respect to this basis is $[a_{ij}]$. By taking residues of both sides of the relation

$$x_i y = \sum_{j=1}^{n} a_{ij} x_j$$

modulo $\mathfrak{p}R'$, similar logic shows that the matrix of $r_{\bar{y}}$ with respect to the basis $\bar{x}_1, \ldots, \bar{x}_n$ is $[\bar{a}_{ij}]$. We will let

$$T_{\mathfrak{p}} : R'/\mathfrak{p}R' \to R/\mathfrak{p}$$

be the linear map given by

$$T_{\mathfrak{p}}(\bar{y}) = \mathrm{Tr}(r_{\bar{y}}) = \mathrm{Tr}[\bar{a}_{ij}].$$

What the above work shows is that

$$\overline{\mathrm{Tr}_{L/K}(y)} = T_{\mathfrak{p}}(\bar{y}).$$

Now that we know this, since $R'$ is free over $R$, by Theorem 2.3.29, we know

$$\Delta(R'/R) = R\Delta(x_1, \ldots, x_n).$$

Therefore

$$\Delta(R'/R) \subseteq \mathfrak{p} \iff \Delta(x_1, \ldots, x_n) \in \mathfrak{p}.$$

Again taking residues modulo $\mathfrak{p}R'$, this holds (by the above) if and only if

$$\Delta(\bar{x}_1, \ldots, \bar{x}_n) = \det[T_{\mathfrak{p}}(\bar{x}_i\bar{x}_j)] = \det[\overline{\mathrm{Tr}_{L/K}(x_ix_j)}] = \overline{\Delta(x_1, \ldots, x_n)} = 0.$$

So we have reduced the problem to seeing if

$$\Delta(\bar{x}_1, \ldots, \bar{x}_n) = 0 \in R/\mathfrak{p}.$$

(3) **Unramified means no containment**: Suppose we have the factorization

$$\mathfrak{p}R' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

which by the Chinese Remainder Theorem (2.2.22) implies

$$R'/\mathfrak{p}R' \cong R'/\mathfrak{P}_1^{e_1} \oplus \cdots \oplus R'/\mathfrak{P}_g^{e_g}.$$

*We will be assuming throughout this proof that $R'/\mathfrak{P}_i$ is separable over $R/\mathfrak{p}$!* If $\mathfrak{p}$ is unramified, then $e_i = 1$ for all $i$. Just as $T_{\mathfrak{p}}$ was used to denote the trace map from $R'/\mathfrak{p}R'$ to $R/\mathfrak{p}$, we will let $T_{\mathfrak{P}_i}$ denote the trace map from $R'/\mathfrak{P}_i$ to $R/\mathfrak{p}$. Form a new basis for $R'/\mathfrak{p}R'$ over $R/\mathfrak{p}$ by selecting a basis for each component in the direct sum above and combining them to form a basis for $R'/\mathfrak{p}R'$, and let this basis be denoted $\{u_i\}$. For $\bar{y} \in R'/\mathfrak{p}R'$, write

$$\bar{y} = \bar{y}_1 + \ldots + \bar{y}_g,$$

where $\bar{y}_i \in R'/\mathfrak{P}_i$. Consider now the matrix of $r_{\bar{y}}$ in this new basis. It is not hard to see that this matrix is formed by combining the matrices of $r_{\bar{y}_i}$, where $r_{\bar{y}_i}$ acts on $R'/\mathfrak{P}_i$. That is, in this new basis,

$$r_{\bar{y}} = \begin{pmatrix} r_{\bar{y}_1} & 0 & \cdots & 0 \\ 0 & r_{\bar{y}_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r_{\bar{y}_g} \end{pmatrix}.$$

Taking traces of both sides yields

$$T_{\mathfrak{p}}(\bar{y}) = T_{\mathfrak{P}_1}(\bar{y}_1) + T_{\mathfrak{P}_2}(\bar{y}_2) + \ldots + T_{\mathfrak{P}_g}(\bar{y}_g).$$

Equally as important, if $M$ denotes the matrix of the bilinear form $T_{\mathfrak{p}}$ in the basis $\{u_j\}$ and $M_i$ denotes the matrix of the bilinear form $T_{\mathfrak{P}_i}$ in the respective bases of $R'/\mathfrak{P}_i$, then

$$M = \begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_g \end{pmatrix}.$$

Taking determinants of both sides yields

$$\Delta(u_1, \ldots, u_n) = \det(M_1) \cdots \det(M_g).$$

Since $R'/\mathfrak{P}_i$ is a separable extension of $R/\mathfrak{p}$, by Proposition 2.3.54 each of the $\det(M_i) \neq 0$ as the $M_i$ are invertible. Letting $C$ denote the change of basis matrix between $\{\bar{x}_1, \ldots, \bar{x}_n\}$ and $\{u_1, \ldots, u_n\}$, we get

$$\Delta(\bar{x}_1, \ldots, \bar{x}_n) = \det(C)^2 \Delta(u_1, \ldots, u_n) \neq 0.$$

Therefore by step 2, $\Delta(R'/R) \not\subseteq \mathfrak{p}$.

(4) **Ramification means containment**: Let $\mathfrak{p}R'$ have the same factorization as above, and suppose $e_i > 1$ for some $i$. Without loss of generality, assume $e_1 > 1$. Let $f = f(\mathfrak{P}_1/\mathfrak{p})$. Let $u_1, \ldots, u_f$ be basis for $R'/\mathfrak{P}_1^{e_1}$ such that $u_1 \in \mathfrak{P}_1/\mathfrak{P}_1^{e_1}$. This is possible since $\mathfrak{P}_1/\mathfrak{P}_1^{e_1}$ is a 1-dimensional subspace of $R'/\mathfrak{P}_1^{e_1}$, so we can simply complete a basis after choosing $u_1 \in \mathfrak{P}_1/\mathfrak{P}_1^{e_1}$. Then $u_1^{e_1} = 0$, which means $u_1$ is nilpotent. This also implies that $u_1 u_j$ is nilpotent for $j = 1, \ldots, n$. Consider the operator $r_{u_1 u_j}$. This is a nilpotent matrix, and so all the roots of the characteristic polynomial are 0 (fact from linear algebra). Therefore

$$T_{\mathfrak{P}_1}(u_1 u_j) = \mathrm{Tr}(r_{u_1 u_j}) = 0.$$

But if this is the case, then letting $M_1$ be the matrix in step (3) shows $M_1$ has a row of zeroes. If a matrix has a row of zeroes, then its determinant is zero, so $\det(M_1) = 0$. But as we saw above

$$\Delta(\bar{x}_1, \ldots, \bar{x}_n) = \det(C)^2 \Delta(u_1, \ldots, u_n) = 0.$$

By step (2), this implies $\Delta(R'/R) \subseteq \mathfrak{p}$. This completes the proof.

□

**Corollary 2.3.56.** *Suppose $L/K$ is a finite extension of number fields with respective rings of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. Then a prime $\mathfrak{p}$ of $\mathcal{O}_K$ ramifies in $\mathcal{O}_L$ if and only if $\Delta(\mathcal{O}_L/\mathcal{O}_K) \subseteq \mathfrak{p}$.*

*Proof.* Since finite extensions of finite fields are separable (see appendix B), all the conditions of Theorem 2.3.55 are met. □

**Corollary 2.3.57.** *If $L/K$ is as in the previous corollary, only finitely many prime ideals of $\mathcal{O}_K$ ramify in $\mathcal{O}_L$.*

*Proof.* We know $\mathcal{O}_K$ is a Dedekind ring. We saw in the section on unique factorization of ideals into prime ideals that there are only finitely many prime ideals which can contain any given ideal. Therefore there are finitely many primes containing $\Delta(\mathcal{O}_L/\mathcal{O}_K)$. Now apply Theorem 2.3.55. □

Let us use the theorem to prove something about cyclotomic fields.

**Proposition 2.3.58.** *$K = \mathbb{Q}(\zeta_m)$, where $\zeta_m$ is a primitive $m$-th root of unity. If $p \nmid m$, then $p$ is unramified in $K$.*

*Proof.* Let $f(x) \in \mathbb{Q}[x]$ denote the minimal polynomial of $\zeta_m$ over $\mathbb{Q}$. We know $\zeta_m$ satisifes $x^m - 1 \in \mathbb{Z}[x]$, and so it is an algebraic integer, which means its minimal polynomial is also in $\mathbb{Z}[x]$ by Gauss' lemma. So $f(x) \in \mathbb{Z}[x]$. Write

$$x^m - 1 = f(x)h(x),$$

for some $h(x) \in \mathbb{Z}[x]$ (since the minimal polynomial must divide any other polynomial with $\zeta_m$ as a root). Consider $\mathcal{O}_K$, the ring of integers of $K$. By Theorem 2.3.6, $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$. By Theorem 2.3.55 above, the primes which ramify in $\mathcal{O}_K$ are those which contain the discriminant $\Delta(\mathcal{O}_K/\mathbb{Z})$. The discriminant of the set formed by powers of $\zeta_m$ sits inside $\Delta(\mathcal{O}_K/\mathbb{Z})$, i.e.

$$\Delta(1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\varphi(m)-1}) \in \Delta(\mathcal{O}_K/\mathbb{Z}).$$

But as we remarked in Section 2.3.4, the discriminant $\Delta(\mathcal{O}_K/\mathbb{Z})$ is a well-defined integer, and therefore $\Delta(1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\varphi(m)-1})$ is the discriminant $\Delta(\mathcal{O}_K/\mathbb{Z})$. Call this discriminant $\Delta$. Therefore the prime ideals which contain $\Delta(\mathcal{O}_K/\mathbb{Z})$ are precisely those containing $\Delta$. By Proposition 2.3.26, we have

$$\Delta = \pm \mathrm{Norm}_{K/\mathbb{Q}}(f'(\zeta_n)),$$

where the sign depends on $\varphi(m)$ (the degree $[K : \mathbb{Q}]$). Taking derivatives of both sides of $x^m - 1 = f(x)h(x)$ gives

$$mx^{m-1} = f'(x)h(x) + f(x)h'(x).$$

Plugging in $x = \zeta_m$ and remembering that $f(\zeta_m) = 0$ yields

$$m\zeta_m^{m-1} = f'(\zeta_m)h(\zeta_m).$$

Now we take norms of both sides. First recall the norm is multiplicative. Second, as $m \in \mathbb{Z}$,

$$\mathrm{Norm}_{K/\mathbb{Q}}(m) = m^{[K:\mathbb{Q}]} = m^{\varphi(m)},$$

where $\varphi(m)$ is Euler's totient function (see appendix C). Moreover, we know $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta_m) \in \mathbb{Z}$. But as $\zeta_m^m = 1$, this implies $\left(\mathrm{Norm}_{K/\mathbb{Q}}(\zeta_m)\right)^m = 1$, so $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta_m)$ is a root of unity in $\mathbb{Z}$. But there are only two, namely $\pm 1$. Therefore $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta_m) = \pm 1$, and so $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta_m^{m-1}) = \pm 1$. Taking norms of both sides above and putting all this together yields

$$m^{\varphi(m)} = \pm \mathrm{Norm}_{K/\mathbb{Q}}(f'(\zeta_m))\mathrm{Norm}_{K/\mathbb{Q}}(h(\zeta_m)).$$

Therefore $\mathrm{Norm}_{K/\mathbb{Q}}(f'(\zeta_m))$ divides a power of $m$, which means $\Delta$ divides a power of $m$. Therefore the only primes that ramify are those dividing $m$. This proves the proposition. □

*Remark* 2.3.59. Since we never proved theorem 2.3.6, it is worthwhile to remark that this proof would have worked without this theorem. Indeed, we could have simply observed that

$$\mathbb{Z}[\zeta_m] \subseteq \mathcal{O}_K,$$

so that

$$\Delta(1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\varphi(m)-1}) \in \Delta(\mathcal{O}_K/\mathbb{Z}).$$

With this, Janusz simply notes that if a prime ideal were to contain $\Delta(\mathcal{O}_K/\mathbb{Z})$, it would necessarily contain

$$\Delta = \Delta(1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\varphi(m)-1}),$$

and the rest of the proof follows exactly as above. So we can safely say that we have actually completed this proof without assuming any prior results.

So in the cyclotomic case, the only primes which ramify are those dividing $m$, and other primes are therefore unramified.

Going back to the two examples in the previous section, in both cases no other primes can ramify in those number fields since we considered every prime dividing the discriminant (and hence every prime ideal containing the discriminant as "to contain is to divide").

## 2.3.7 Decomposition and Inertia Groups

### Decomposition Group

In this section we will delve deeper into our study of the action of the Galois group on the prime ideals of the extension. Let us return to the setup,

$$\begin{array}{ccc} L & \hookleftarrow & \mathcal{O}_L \\ | & & | \\ K & \hookleftarrow & \mathcal{O}_K \\ | & & | \\ \mathbb{Q} & \hookleftarrow & \mathbb{Z} \end{array}$$

but now let us suppose that $L/K$ is a Galois extension. Lemma 2.3.46 states that if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathrm{Gal}(L/K)$ acts transitively on the primes lying above $\mathfrak{p}$. Let

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)^e$$

be the factorization of $\mathfrak{p}$ in $\mathcal{O}_L$. Notice that since the ramification indices of all the primes $\mathfrak{P}_i$ are equal in Galois extensions, it makes sense to write the factorization like this.

One may recall from group theory that if a group $G$ acts on a nonempty set $S$, then the *stabilizer* of the element $s \in S$ is the set of $G$ which fix $s$, i.e.

$$\{g \in G : g \cdot s = s\}.$$

In the above situation, we have $\mathrm{Gal}(L/K)$ acting on the $\mathfrak{P}_i$, so we can consider the stabilizer of one of these primes, which leads to the next definition. Most of this section can be found in [16], though some parts are from [12].

**Definition 2.3.60.** With the situation above, the *decomposition group* of the prime $\mathfrak{P}_i$ is defined as

$$D(\mathfrak{P}_i/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}.$$

Since the stabilizer of an element is a subgroup of the acting group $G$, we automatically get $D(\mathfrak{P}_i/\mathfrak{p}) \leq \mathrm{Gal}(L/K)$ is a subgroup. The next question to consider is: what is the order of $D(\mathfrak{P}_i/\mathfrak{p})$, and how are two groups for two different primes related? As it turns out, the order of the decomposition group does not depend on the prime $\mathfrak{P}_i$, and the decomposition groups for different primes are related. First, let us examine the order of the group. Recall the orbit-stabilizer theorem from group theory.

**Proposition 2.3.61** (Orbit-Stabilizer)**.** *Suppose $G$ acts on a nonempty set $S$, and take any $s \in S$. Let $G_s$ denote the stabilizer of $s$ and let $Gs$ denote the orbit of $s$. Then*

$$|Gs| = [G : G_s].$$

Let $e$ denote the ramification index (as above in the factorization of $\mathfrak{p}\mathcal{O}_L$) and let $f$ denote the common residue field degree (since all the $f(\mathfrak{P}_i/\mathfrak{p})$ are equal in Galois extensions by Corollary 2.3.48). Then we get the following proposition.

**Proposition 2.3.62.** *Let $\mathfrak{p}\mathcal{O}_L$ have the factorization as above, namely*

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)^e.$$

*Then for all $i$, $|D(\mathfrak{P}_i/\mathfrak{p})| = ef$.*

*Proof.* Let $G = \mathrm{Gal}(L/K)$. Since the action of $G$ on the primes above $\mathfrak{p}$ is transitive, the size of the orbit of $\mathfrak{P}_i$ is $g$. Therefore the orbit-stabilizer theorem says

$$[G : D(\mathfrak{P}_i/\mathfrak{p})] = g.$$

However,

$$|G| = |\mathrm{Gal}(L/K)| = [L : K]$$

since we are in a Galois extension, and by Corollary 2.3.48,

$$[L : K] = efg.$$

Therefore $|D(\mathfrak{P}_i/\mathfrak{p})| = efg/g = ef$, as required. □

This answers the question about the order of $D(\mathfrak{P}_i/\mathfrak{p})$. As for the second question, it would be nice to somehow relate $D(\mathfrak{P}_i/\mathfrak{p})$ with $D(\mathfrak{P}_j/\mathfrak{p})$, if possible.

**Proposition 2.3.63.** *For two different primes $\mathfrak{P}_i$ and $\mathfrak{P}_j$ dividing $\mathfrak{p}$, the decomposition groups $D(\mathfrak{P}_i/\mathfrak{p})$ and $D(\mathfrak{P}_j/\mathfrak{p})$ are conjugate in $Gal(L/K)$. Namely, there exists $\sigma \in Gal(L/K)$ with*

$$\sigma D(\mathfrak{P}_i/\mathfrak{p})\sigma^{-1} = D(\mathfrak{P}_j/\mathfrak{p}).$$

*Proof.* Since the action of $\mathrm{Gal}(L/K)$ on the primes above $\mathfrak{p}$ is transitive, we can choose $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Notice that

$$\sigma^{-1}\tau\sigma(\mathfrak{P}_i) = \mathfrak{P}_i \iff \tau\sigma(\mathfrak{P}_i) = \sigma(\mathfrak{P}_i).$$

Since $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$, this says

$$\sigma^{-1}\tau\sigma \in D(\mathfrak{P}_i/\mathfrak{p}) \iff \tau \in D(\mathfrak{P}_j/\mathfrak{p}),$$

which implies

$$\sigma^{-1}D(\mathfrak{P}_j/\mathfrak{p})\sigma = D(\mathfrak{P}_i/\mathfrak{p}),$$

or

$$D(\mathfrak{P}_j/\mathfrak{p}) = \sigma D(\mathfrak{P}_i/\mathfrak{p})\sigma^{-1}.$$

□

At this point, it would probably be helpful to look at a couple of examples. Both of these can be found in [20].

**Example 2.3.64.** Consider the cyclotomic extension $K = \mathbb{Q}(\zeta_{15})/\mathbb{Q}$. The degree of this extension is given by $\varphi(15)$, where $\varphi$ is Euler's totient function (see appendix C). It is easy to calculate that $\varphi(15) = 8$, so $[\mathbb{Q}(\zeta_{15}) : \mathbb{Q}] = 8$. Moreover, it can also be verified that the minimal polynomial of $\zeta_{15}$ over $\mathbb{Q}$ is

$$f(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

(Note: One only really needs to check that $\zeta_{15}$ satisfies $f(x)$ because $f(x)$ is a monic polynomial of degree 8.) The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/15\mathbb{Z})^\times$, which is a group of order 8. Elements of $\mathrm{Gal}(K/\mathbb{Q})$ can be labeled as $\sigma_i$ for $1 \leq i \leq 15$, $(i, 15) = 1$, where

$$\sigma_i : \zeta_{15} \mapsto \zeta_{15}^i.$$

Lastly, we will need that $\mathcal{O}_K = \mathbb{Z}[\zeta_{15}]$, which is Theorem 2.3.6.

(a) Let us factor the ideal (3) of $\mathbb{Z}$. By the Dedekind-Kummer theorem, we should factor $f(x)$ mod 3. One easily checks that

$$f(x) \equiv (1 + x + x^2 + x^3 + x^4)^2 \bmod 3,$$

which means that (3) factors as

$$(3)\mathcal{O}_K = (3, 1 + \zeta_{15} + \zeta_{15}^2 + \zeta_{15}^3 + \zeta_{15}^4)^2 = \mathfrak{p}_3^2.$$

So $e(\mathfrak{p}_3/3) = 2$ and $f(\mathfrak{p}_3/3) = 4$, again by the Dedekind-Kummer theorem. Therefore

$$|D(\mathfrak{p}_3/3)| = 2 \cdot 4 = 8,$$

but as

$$D(\mathfrak{p}_3/3) \leq \mathrm{Gal}(K/\mathbb{Q}),$$

and $\mathrm{Gal}(K/\mathbb{Q})$ has order 8, we must have $D(\mathfrak{p}_3/3) = \mathrm{Gal}(K/\mathbb{Q})$.

The other way we could have gotten this equality is by realizing that $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the primes above (3), but there is only one prime above (3), meaning every element of $\mathrm{Gal}(K/\mathbb{Q})$ must stabilize $\mathfrak{p}_3$.

(b) Now consider the ideal (2) of $\mathbb{Z}$. This time we need to factor $f(x)$ modulo 2, and we find

$$f(x) \equiv (1 + x + x^4)(1 + x^3 + x^4) \bmod 2.$$

Therefore, by the Dedekind-Kummer theorem,

$$(2) = (2, 1 + \zeta_{15} + \zeta_{15}^4)(1 + \zeta_{15}^3 + \zeta_{15}^4) = \mathfrak{p}_2\mathfrak{p}_2'.$$

Moreover,

$$e(\mathfrak{p}_2/2) = e(\mathfrak{p}_2'/2) = 1, \quad f(\mathfrak{p}_2/2) = f(\mathfrak{p}_2'/2) = 4.$$

Hence

$$|D(\mathfrak{p}_2/2)| = |D(\mathfrak{p}_2'/2)| = 1 \cdot 4 = 4.$$

So this time we will get proper subgroups of $\mathrm{Gal}(L/K)$. Let us try and find $D(\mathfrak{p}_2/2)$. As we see in the Dedekind-Kummer theorem, $\mathfrak{p}_2$ is the kernel of the map

$$\mathbb{Z}[\zeta_{15}] \to \mathbb{Z}[\zeta_{15}]/\mathfrak{p}_2 \cong \mathbb{F}_2/(x^4+x+1), \quad \zeta \mapsto x.$$

Take an element $\sigma_k \in \mathrm{Gal}(K/\mathbb{Q})$. We see

$$\sigma_k(\mathfrak{p}_2) = \sigma_k(2, 1+\zeta_{15}+\zeta_{15}^4) = (2, 1+\zeta_{15}^k+\zeta_{15}^{4k}).$$

So $\sigma_k(\mathfrak{p}_2) = \mathfrak{p}_2$ if and only if $(2, 1+\zeta_{15}^k+\zeta_{15}^{4k})$ lies in the kernel of the above map. By definition of the map, this will happen if and only if $1+x^k+x^{4k}$ is an $\mathbb{F}_2[x]$-multiple of $1+x+x^4$. Since we only need to check values of $k \leq 15$ and $(k, 15) = 1$, going through the list we find four values, namely $k = 1, 2, 4, 8$. Since $D(\mathfrak{p}_2/2)$ has order 4, this is the whole group, so

$$D(\mathfrak{p}_2/2) = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8\}.$$

Instead of finding $D(\mathfrak{p}_2'/2)$ in the same way, let us use the conjugate relation between the two groups. That is, we know $D(\mathfrak{p}_2/2)$ and $D(\mathfrak{p}_2'/2)$ are conjugate in $\mathrm{Gal}(K/\mathbb{Q})$, *which is an abelian group*. Therefore, conjugation in $\mathrm{Gal}(K/\mathbb{Q})$ leaves every element fixed, so we must have

$$D(\mathfrak{p}_2'/2) = D(\mathfrak{p}_2/2).$$

### A Surjective Homomorphism

In this section, we get to see a relationship between the decomposition group and the Galois group of the residue field for a given prime ideal of $\mathcal{O}_L$. Assume we are in the same situation as before, and consider $\sigma \in D(\mathfrak{P}_i/\mathfrak{p})$. We know that $\sigma \in \mathrm{Gal}(L/K)$ as $D(\mathfrak{P}_i/\mathfrak{p}) \leq \mathrm{Gal}(L/K)$. In the beginning of the subsection of Section 2.3.5 titled "Action of Galois Group," we showed $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. Moreover, $\sigma(\mathfrak{P}_i) = \mathfrak{P}_i$ by definition of the decomposition group of $\mathfrak{P}_i$. Therefore, $\sigma$ induces an automorphism $\bar{\sigma}$ of $\mathcal{O}_L/\mathfrak{P}_i$. As it clearly fixes $\mathcal{O}_K/\mathfrak{p}$ (as $\sigma \in \mathrm{Gal}(L/K)$ fixes every element of $K$ elementwise), we get a natural homomorphism of groups

$$D(\mathfrak{P}_i/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}_i}/\mathbb{F}_\mathfrak{p}),$$

where $\mathbb{F}_{\mathfrak{P}_i} = \mathcal{O}_L/\mathfrak{P}_i$ and $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. This is summarized in the following proposition.

**Proposition 2.3.65.** *Suppose $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Let $\mathbb{F}_\mathfrak{P} = \mathcal{O}_L/\mathfrak{P}$ and $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. Then there is a natural group homomorphism*

$$\phi : D(\mathfrak{P}/\mathfrak{p}) \to \mathit{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}).$$

The goal now is to show that the homomorphism $\phi$ is surjective. First, let us turn our attention to the group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}_i}/\mathbb{F}_{\mathfrak{p}})$. Both $\mathbb{F}_{\mathfrak{P}_i}$ and $\mathbb{F}_{\mathfrak{p}}$ are finite fields, so the Galois group is cyclic, and generated by the Frobenius automorphism (see appendix B). The Frobenius map is the map

$$x \mapsto x^q,$$

where $q$ is the number of elements in $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$. But recall from Proposition 2.3.40 that

$$N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|\,.$$

Therefore the Frobenius automorphism, which is the generator for $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}_i}/\mathbb{F}_{\mathfrak{p}})$, is the map

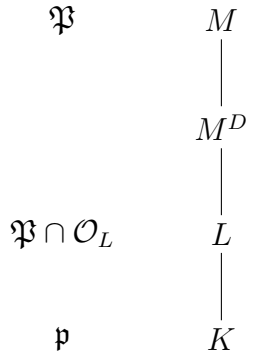
$$\mathrm{Frob}_{\mathfrak{p}} : x \mapsto x^{N(\mathfrak{p})}.$$

To show $\phi$ is surjective, it suffices to prove this Frobenius map is in the image of $\phi$.

Before we do this, we require two propositions, both of which can be found in [16].

**Proposition 2.3.66.** *Suppose $M/K$ is a finite Galois extension of number fields (as usual), and suppose $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_M$ lying above $\mathfrak{p}$. Then the fixed field $M^{D(\mathfrak{P}/\mathfrak{p})}$ is the smallest subfield of $L \subset M$ such that $\mathfrak{P}$ is the only prime ideal of $\mathcal{O}_M$ lying above $\mathfrak{P} \cap \mathcal{O}_L$.*

*Proof.* Let $D = D(\mathfrak{P}/\mathfrak{p})$. The picture we are considering is this




We will show that $M^D$ has the desired property (i.e. that $\mathfrak{P}$ is the only prime ideal of $\mathcal{O}_M$ lying above $\mathfrak{P} \cap \mathcal{O}_{M^D}$), and then show that any other field $L \subset M$ with this property must contain $M^D$. First consider the fixed field $M^D$. Then by the Fundamental Theorem of Galois Theory (FTGT, Theorem A.3.10), $\mathrm{Gal}(M/M^D) \cong D$. Certainly $\mathfrak{P}$ is a prime lying above the ideal $\mathfrak{P} \cap \mathcal{O}_{M^D}$. Moreover, the Galois group acts transitively on the primes above $\mathfrak{P} \cap \mathcal{O}_{M^D}$. But as $\mathrm{Gal}(M/M^D) \cong D = D(\mathfrak{P}/\mathfrak{p})$, every element in $\mathrm{Gal}(M/M^D)$ fixes $\mathfrak{P}$, meaning $\mathfrak{P}$ is the unique prime lying above $\mathfrak{P} \cap \mathcal{O}_L$.

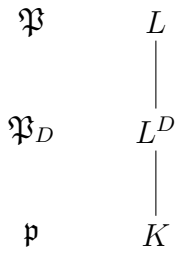
Now suppose $L$ is any subfield of $M$ which this property, i.e. that $\mathfrak{P}$ is the only prime lying above $\mathfrak{P} \cap \mathcal{O}_L$. Then every element of $\mathrm{Gal}(M/L)$ fixes $\mathfrak{P}$. As $\mathrm{Gal}(M/L) \leq \mathrm{Gal}(M/K)$, this means $\mathrm{Gal}(M/L) \leq D(\mathfrak{P}/\mathfrak{p})$. The FTGT then implies

$$M^{D(\mathfrak{P}/\mathfrak{p})} \subset L,$$

proving the proposition. □

Later, we complete the picture given by Proposition 2.3.66. Namely, we will see a more detailed illustration of what happens to $\mathfrak{p}$ as it climbs up the ladder of fields.

**Proposition 2.3.67.** *Let $L/K$ be a finite Galois extension of number fields, and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying above the ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Let $D = D(\mathfrak{P}/\mathfrak{p})$, and consider the field $L^D$. Denote $\mathfrak{P}_D = \mathfrak{P} \cap \mathcal{O}_{L^D}$. Then $e(\mathfrak{P}_D/\mathfrak{p}) = f(\mathfrak{P}_D/\mathfrak{p}) = 1$, and $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_D)$ and $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{P}_D)$.*




*Proof.* Let $G = \mathrm{Gal}(L/K)$, $g(\mathfrak{P}/\mathfrak{p})$ denote the number of prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$, and $g(\mathfrak{P}/\mathfrak{P}_D)$ denote the number of primes above $\mathfrak{P}_D$. As we saw in Proposition 2.3.62, $[G : D] = g(\mathfrak{P}/\mathfrak{p})$. The Fundamental Theorem of Galois Theory tells us that $[G : D] = [L^D : K]$, and therefore $g(\mathfrak{P}/\mathfrak{p}) = [L^D : K]$. By Corollary 2.3.48,

$$e(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}/\mathfrak{P}_D)g(\mathfrak{P}/\mathfrak{P}_D) = [L : L^D].$$

Proposition 2.3.66 asserts that $g(\mathfrak{P}/\mathfrak{P}_D) = 1$, which means

$$e(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}/\mathfrak{P}_D) = [L : L^D].$$

But

$$\begin{aligned}
[L : L^D] &= \frac{[L : K]}{[L^D : K]} \\
&= \frac{e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})g(\mathfrak{P}/\mathfrak{p})}{[L^D : K]} \\
&= \frac{e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})[L^D : K]}{[L^D : K]} \\
&= e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}).
\end{aligned}$$

Therefore,

$$e(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}/\mathfrak{P}_D) = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}).$$

But as ramification indices and residue field degrees are multiplicative (Proposition 2.3.43),

$$e(\mathfrak{P}/\mathfrak{P}_D) \leq e(\mathfrak{P}/\mathfrak{p}) \quad \text{and} \quad f(\mathfrak{P}/\mathfrak{P}_D) \leq f(\mathfrak{P}/\mathfrak{p}).$$

Hence, in both cases, equality must hold. And since

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_D)e(\mathfrak{P}_D/\mathfrak{p}) \quad \text{and } f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}_D/\mathfrak{p}),$$

we immediately find

$$e(\mathfrak{P}_D/\mathfrak{p}) = f(\mathfrak{P}_D/\mathfrak{p}) = 1,$$

proving the proposition. □

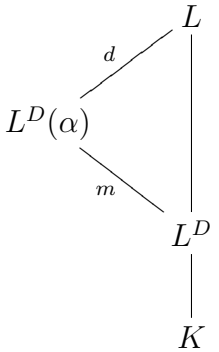
And now, with this, we can prove the surjectivity of our homomorphism $\phi$.

**Proposition 2.3.68.** *Let $L/K$ be a finite Galois extension of number fields. Suppose $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$ lying above the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Let $\mathbb{F}_\mathfrak{P} = \mathcal{O}_L/\mathfrak{P}$ and $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. Then the group homomorphism*

$$\phi : D(\mathfrak{P}/\mathfrak{p}) \to Gal(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$$

*is surjective.*

*Proof.* The extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is a finite separable extension (extensions of finite fields are separable; see appendix B), and so the conditions of the primitive element theorem 2.1.2 are satisfied, meaning there exists $\bar{\alpha} \in \mathbb{F}_\mathfrak{P}$ with $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}(\bar{\alpha})$. Let $\bar{m}(x) \in \mathbb{F}_\mathfrak{p}(x)$ denote the minimal polynomial of $\alpha$ over $\mathbb{F}_\mathfrak{p}$. Lift $\bar{\alpha}$ to an element $\alpha \in \mathcal{O}_L$, and consider its characteristic polynomial over $L^D$, $c_{L/L^D}(x)$ (we encountered this in Chapter 2, Section 1.2). In the proof of Theorem 2.1.10, we showed that $c_{L/L^D}(x)$ was a power of the minimal polynomial $m(x)$ of $\alpha$ over $L^D$. In fact, we showed $c_{L/L^D}(x) = m(x)^d$, where $d = [L : L^D(\alpha)]$.




But now consider

$$g(x) = \prod_{\sigma \in D} (x - \sigma(\alpha)).$$

The claim is that $c_{L/L^D}(x) = g(x)$. Clearly $g(x)$ is monic. Let $m = [L^D(\alpha) : L^D]$ and $H = \mathrm{Gal}(L/L^D(\alpha))$. Then we can let

$$\sigma_1 H, \sigma_2 H, \ldots, \sigma_m H$$

be the $m$ left cosets of $H$ in $D = \mathrm{Gal}(L/L^D)$. The minimal polynomial of $\alpha$ over $L^D$ has the form

$$m(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_m(\alpha)).$$

To see why, notice that since $m = [L^D(\alpha) : L^D]$, the degree of the minimal polynomial of $\alpha$ over $L^D$ must be $m$. Moreover, $D = \mathrm{Gal}(L/L^D)$ acts transitively on the roots of $m(x)$. Since elements of $H$ leave $\alpha$ fixed, the list of cosets above shows that the $\sigma_i(\alpha)$ are the $m$ distinct roots of $m(x)$. Therefore $m(x)$ will factor in $L$ in this way. But since

$$D = \sigma_1 H \cup \sigma_2 H \cup \cdots \cup \sigma_m H$$

and $H$ leaves $\alpha$ fixed, we find that

$$\begin{aligned} g(x) &= \prod_{\sigma \in D} (x - \sigma(\alpha)) \\ &= \prod_{h \in H} (x - \sigma_1 h(\alpha))(x - \sigma_2 h(\alpha)) \cdots (x - \sigma_m h(\alpha)) \\ &= \prod_{h \in H} (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_m(\alpha)) \\ &= m(x)^{|H|} \\ &= m(x)^d. \end{aligned}$$

Therefore $c_{L/L^D}(x) = g(x)$, so

$$c_{L/L^D}(x) = \prod_{\sigma \in D} (x - \sigma(\alpha)).$$

The coefficients of $c_{L/L^D}(x)$ are sums and products of elements of $\mathcal{O}_L$, and we know the coefficients of the characteristic polynomial must lie in the base field $L^D$. So we find the coefficients are in $\mathcal{O}_L \cap L^D = \mathcal{O}_{L^D}$. Therefore, it makes sense to reduce the polynomial $c_{L/L^D}(x) \in \mathcal{O}_{L^D}[x]$ modulo $\mathfrak{P}_D = \mathfrak{P} \cap \mathcal{O}_{L^D}$. So let

$$\bar{c}(x) = \overline{c_{L/L^D}}(x) = \prod_{\sigma \in D} (x - \bar{\sigma}(\bar{\alpha}))$$

denote the reduced polynomial. By the previous proposition, as $f(\mathfrak{P}_D/\mathfrak{p}) = 1$, we have an isomorphism $\mathcal{O}_{L^D}/\mathfrak{P}_D \cong \mathcal{O}_K/\mathfrak{p}$, so we can regard the coefficients of $\bar{c}(x)$ as living in $\mathbb{F}_\mathfrak{p}$, i.e. $\bar{c}(x) \in \mathbb{F}_\mathfrak{p}[x]$. Moreover, as $\alpha$ is a root of $c_{L/L^D}(x)$, $\bar{\alpha}$

is a root of $\bar{c}(x)$, so $\bar{m}(x)$ (i.e. the minimal polynomial of $\bar{\alpha}$ over $\mathbb{F}_{Ip}$) satisfies $\bar{m}(x)|\bar{c}(x)$. Therefore all the roots of $\bar{m}(x)$ are roots of $\bar{c}(x)$. But as $\bar{m}(x)$ is the minimal polynomial of $\bar{\alpha}$, we know

$$\bar{m}(x) = \prod_{\tau \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})} (x - \tau(\bar{\alpha})).$$

In particular, $\mathrm{Frob}_{\mathfrak{p}}(\bar{\alpha})$ is a root of $\bar{m}(x)$, so it is a root of $\bar{c}(x)$. Since the roots of $\bar{c}(x)$ have the form $\bar{\sigma}(\bar{\alpha})$ for some $\sigma \in D$ and $\bar{\alpha}$ generates $\mathbb{F}_{\mathfrak{P}}$, we get $\mathrm{Frob}_{\mathfrak{p}} = \phi(\sigma)$ for some $\sigma \in D$. As $\mathrm{Frob}_{\mathfrak{p}}$ generates $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$, $\phi$ must be surjective.

□

### Inertia Group

We have a surjective homomorphism

$$\phi : D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

We can now define the inertia group of $\mathfrak{P}$.

**Definition 2.3.69.** The *inertia group* of $\mathfrak{P}$ is defined as

$$I(\mathfrak{P}/\mathfrak{p}) = \ker \phi.$$

Explicitly,

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}/\mathfrak{p}) : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L\}.$$

*Remark* 2.3.70. In case it is unclear, the notation $\sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}$ means $\sigma(\alpha) - \alpha \in \mathfrak{P}$.

By defining the inertia group in this way, we get a corollary to Proposition 2.3.68.

**Corollary 2.3.71.** *The size of the inertia group is* $|I(\mathfrak{P}/\mathfrak{p})| = e(\mathfrak{P}/\mathfrak{p})$.

*Proof.* We know the size of $D(\mathfrak{P}/\mathfrak{p})$ is $e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$, and the size of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is $f(\mathfrak{P}/\mathfrak{p})$. The corollary follows because of the isomorphism

$$D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

□

*Remark* 2.3.72. A consequence of this corollary is that $\mathfrak{P}$ is unramified if and only if its inertia group $I(\mathfrak{P}/\mathfrak{p})$ is the trivial group. Moreover, if $\mathfrak{P}$ is unramified, then the surjective homomorphism becomes an isomorphism because it has trivial kernel.

This homomorphism (and isomorphism in the unramified case) gives us some idea of why we should care about the decomposition group. It relates the Galois group of what one might call a more "localized" view of the field extension $L/K$ to the "global" Galois group $\mathrm{Gal}(L/K)$. In fact, we will make this precise later in this thesis when we use this idea to help us calculate the Galois group of a polynomial over $\mathbb{Z}$.

Just as the decomposition groups of two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$ lying above $\mathfrak{p}$ were conjugate in $\mathrm{Gal}(L/K)$, the inertia groups of two different primes are conjugate as well.

**Proposition 2.3.73.** *If $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are two primes of $\mathcal{O}_L$ lying above $\mathfrak{p}$, then there exists $\sigma \in Gal(L/K)$ such that*

$$\sigma I(\mathfrak{P}_1/\mathfrak{p})\sigma^{-1} = I(\mathfrak{P}_2/\mathfrak{p}).$$

*Proof.* Let $\sigma \in \mathrm{Gal}(L/K)$ be such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$. Let $\tau \in I(\mathfrak{P}_1/\mathfrak{p})$. Then by definition, $\tau(\alpha) - \alpha \in \mathfrak{P}_1$ for all $\alpha \in \mathcal{O}_L$. So if $\alpha$ is any element of $\mathcal{O}_L$, notice

$$\begin{aligned} \sigma\tau\sigma^{-1}(\alpha) - \alpha &= \sigma\tau\sigma^{-1}(\alpha) - \sigma\sigma^{-1}(\alpha) \\ &= \sigma(\tau(\sigma^{-1}(\alpha)) - \sigma^{-1}(\alpha)) \\ &\in \sigma(\mathfrak{P}_1) = \mathfrak{P}_2. \end{aligned}$$

Since $\alpha$ was arbitrary, this shows $\sigma I(\mathfrak{P}_1/\mathfrak{p})\sigma^{-1} \subseteq I(\mathfrak{P}_2/\mathfrak{p})$. To get the reverse containment, repeat the same argument above with $\sigma^{-1}$ instead of $\sigma$ and $\tau \in I(\mathfrak{P}_2/\mathfrak{p})$. □

### A Tower of Extensions

We alluded to the fact that we would be providing a more "complete" tower of extensions so that we could see the behavior of $\mathfrak{p}$ as it climbed up to the top of the ladder. We are in a position to do that now. This proposition comes from [12]. The setup is as follows. We have our usual Galois extension of number fields $L/K$, $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$. We let $D = D(\mathfrak{P}/\mathfrak{p})$, $I = I(\mathfrak{P}/\mathfrak{p})$, $e = e(\mathfrak{P}/\mathfrak{p})$, $f = f(\mathfrak{P}/\mathfrak{p})$, and consider the fields $L^I$ and $L^D$. Denote $\mathfrak{P}_I = \mathfrak{P} \cap \mathcal{O}_{L^I}$ and $\mathfrak{P}_D = \mathfrak{P} \cap \mathcal{O}_{L^D}$.

$$\begin{array}{cc} \mathfrak{P} & L \\ & \Big| e \\ \mathfrak{P}_I & L^I \\ & \Big| f \\ \mathfrak{P}_D & L^D \\ & \Big| g \\ \mathfrak{p} & K \end{array}$$

**Proposition 2.3.74.** *(a) The only prime lying above $\mathfrak{P}_D$ in $\mathcal{O}_L$ is $\mathfrak{P}$.*

*(b) The prime ideal $\mathfrak{P}_D$ is unramified in $L^I$, with $f(\mathfrak{P}_I/\mathfrak{P}_D) = f$.*

*(c) The prime ideal $\mathfrak{P}_I$ is totally ramified in $L$, with $e(\mathfrak{P}/\mathfrak{P}_I) = e$.*

*(d) We have the factorization*

$$\mathfrak{p}\mathcal{O}_{L^D} = \mathfrak{P}_D\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}.$$

*(e) If $D$ is normal in $Gal(L/K)$, then*

$$\mathfrak{p}\mathcal{O}_{L^D} = \prod \sigma\mathfrak{P}_D,$$

*where $\sigma$ runs through the a set of representatives of $Gal(L/K)/D = Gal(L^D/K)$.*

*Proof.* We have already seen part (a) in Proposition 2.3.66. Item (d) follows from 2.3.66 and Proposition 2.3.67. Part (e) follows from (d) and the fact that $L^D/K$ is Galois if $D$ is normal, and the Galois group is $\mathrm{Gal}(L^D/K) \cong \mathrm{Gal}(L/K)/D$. First, let us prove (c). We know $L/L^I$ is Galois with Galois group $I$. Therefore it suffices to show that $e(\mathfrak{P}/\mathfrak{P}_I) = e$, since then by the relation in Corollary 2.3.48, we must have $f(\mathfrak{P}/\mathfrak{P}_I) = 1$ and $g(\mathfrak{P}/\mathfrak{P}_I) = 1$. And to show $e(\mathfrak{P}/\mathfrak{P}_I) = e$, all we need to show is that

$$|I(\mathfrak{P}/\mathfrak{P}_I)| = |I|.$$

First consider $D(\mathfrak{P}/\mathfrak{P}_I)$. By definition, this is

$$\{\sigma \in \mathrm{Gal}(L/L^I) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

But $\mathrm{Gal}(L/L^I) = I$, and

$$I \leq D = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Therefore every element of $I$ fixes $\mathfrak{P}$, meaning

$$D(\mathfrak{P}/\mathfrak{P}_I) = I.$$

However, we also know

$$I(\mathfrak{P}/\mathfrak{P}_I) = \{\sigma \in D(\mathfrak{P}/\mathfrak{P}_I) : \sigma(\alpha) - \alpha \in \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L\}.$$

So using the fact that $D(\mathfrak{P}/\mathfrak{P}_I) = I$, we get

$$I(\mathfrak{P}/\mathfrak{P}_I) = \{\sigma \in I : \sigma(\alpha) - \alpha \in \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L\} = I.$$

Since we have equality of sets, we certainly have equality of sizes, so

$$e(\mathfrak{P}/\mathfrak{P}_I) = e,$$

which proves part (c). Part (b) also follows, since

$$f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}_D/\mathfrak{p})f(\mathfrak{P}_I/\mathfrak{P}_D)f(\mathfrak{P}/\mathfrak{P}_I).$$

The first and third terms in the product on the right hand side are 1 by parts (a) and (c), which means

$$f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}_I/\mathfrak{P}_D).$$

Since the degree of the extension $L^I/L^D$ is $[D:I] = f(\mathfrak{P}/\mathfrak{p})$ by the Fundamental Theorem of Galois Theory, we find that $e(\mathfrak{P}_I/\mathfrak{P}_D) = g(\mathfrak{P}_I/\mathfrak{P}_D) = 1$ by Corollary 2.3.48, which proves (b). □

What this proposition shows is that all the ramification happens in the top extension, all the residue extension happens in the middle. If $D$ is also normal, then all the splitting happens in the bottom extension. So it really does give a picture as to what happens to $\mathfrak{p}$ as it climbs up to $L$.

### 2.3.8 Artin Automorphism

This section will be dealing exclusively with unramified primes, and most of the results come from [3]. However, we do have the same setup as usual.

Suppose $e(\mathfrak{P}/\mathfrak{p}) = 1$. Then we know that $I(\mathfrak{P}/\mathfrak{p})$ is the trivial group, meaning our surjective homomorphism

$$\phi : D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$$

becomes an isomorphism. We have seen that $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is a cyclic group, generated by the Frobenius map

$$\mathrm{Frob}_{\mathfrak{p}} : \alpha \mapsto \alpha^{N(\mathfrak{p})}.$$

Therefore, there is some element $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ which maps to it under $\phi$. Moreover, $D(\mathfrak{P}/\mathfrak{p})$ is also cyclic, and generated by $\sigma$.

**Definition 2.3.75.** The element $\sigma$ is called the *Frobenius element* at $\mathfrak{P}$, and it is denoted

$$\sigma = \left(\frac{\mathfrak{P}}{L/K}\right).$$

The following proposition provides a characterization of this Frobenius element.

**Proposition 2.3.76.** *The Frobenius element at $\mathfrak{P}$ is the unique element $\sigma \in Gal(L/K)$ such that*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ mod\ \mathfrak{P}$$

*for all $\alpha \in \mathcal{O}_L$.*

*Proof.* Suppose first that $\sigma$ satisfies the above relation. Then certainly $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$. But $\sigma(\mathfrak{P})$ takes $\mathfrak{P}$ to another prime lying above $\mathfrak{p}$, and since these primes are distinct, we must have $\sigma(\mathfrak{P}) = \mathfrak{P}$. Therefore $\sigma \in D(\mathfrak{P}/\mathfrak{p})$. But under our isomorphism $\phi$, the element $\sigma$ clearly maps to $\text{Frob}_{\mathfrak{p}}$, which means $\sigma = \left(\frac{\mathfrak{P}}{L/K}\right)$. If $\tau$ is another element of $\text{Gal}(L/K)$ satisfying

$$\tau(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$

for all $\alpha \in \mathcal{O}_L$, then the above work shows $\tau \in D(\mathfrak{P}/\mathfrak{p})$ and also gets mapped to $\text{Frob}_{\mathfrak{p}}$ under $\phi$. But since $\phi$ is an isomorphism, and hence injective, which means we must have $\sigma = \tau$. Therefore $\sigma$ is unique. □

Now to get to the Artin automorphism, we make the further assumption that $\text{Gal}(L/K)$ is abelian. To see why this is relevant, recall Proposition 2.3.63 which states that the decomposition groups for two different primes lying above $\mathfrak{p}$ are conjugate in $\text{Gal}(L/K)$. Conjugate subgroups in an abelian group are necessarily equal. Therefore the decomposition groups do not depend on the prime above $\mathfrak{p}$, and instead depend solely on $\mathfrak{p}$. It would be nice if the Frobenius element also did not depend on the prime above $\mathfrak{p}$, which is what the next proposition shows.

**Proposition 2.3.77.** *Assume Gal$(L/K)$ is abelian. Then the Frobenius element $\left(\frac{\mathfrak{P}}{L/K}\right)$ does not depend on the choice of prime $\mathfrak{P}$ lying above $\mathfrak{p}$.*

*Proof.* Suppose $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are two primes lying above $\mathfrak{p}$, and let $\sigma_1$ and $\sigma_2$ denote their respective Frobenius elements. Choose $\tau \in \text{Gal}(L/K)$ with $\tau(\mathfrak{P}_1) = \mathfrak{P}_2$ (the Galois group still acts transitively on the primes of $\mathfrak{p}$). Let $\alpha \in \mathcal{O}_L$. Then since $\sigma_1(\alpha) - \alpha^{N(\mathfrak{p})} \in \mathfrak{P}_1$, we get

$$\tau\sigma_1(\alpha) \equiv \tau(\alpha^{N(\mathfrak{p})}) \bmod \mathfrak{P}_2.$$

But $\tau$ is a homomorphism, so

$$\tau(\alpha^{N(\mathfrak{p})}) \equiv \tau(\alpha)^{N(\mathfrak{p})} \bmod \mathfrak{P}_2.$$

We know $\text{Gal}(L/K)$ is abelian, so $\sigma_1\tau = \tau\sigma_1$, meaning

$$\sigma_1\tau(\alpha) \equiv \tau(\alpha)^{N(\mathfrak{p})} \bmod \mathfrak{P}_2.$$

Since $\tau(\mathcal{O}_L) = \mathcal{O}_L$ (we have seen this before), as $\alpha$ ranges over all of $\mathcal{O}_L$, so does $\tau(\alpha)$, which means

$$\sigma_1(\beta) \equiv \beta^{N(\mathfrak{p})} \bmod \mathfrak{P}_2$$

for all $\beta \in \mathcal{O}_L$. But this means

$$\sigma_1 = \left(\frac{\mathfrak{P}_2}{L/K}\right) = \sigma_2,$$

which shows that the Frobenius elements for all primes lying above $\mathfrak{p}$ are the same. □

Since the Frobenius element does not depend on the prime above $\mathfrak{p}$, we can make the following definition.

**Definition 2.3.78.** The *Artin automorphism*, denoted $\left(\frac{\mathfrak{p}}{L/K}\right)$, is the Frobenius element at any prime lying above $\mathfrak{p}$.

Notice that if our extension is abelian and $\mathfrak{p}$ splits completely in $\mathcal{O}_L$, then the Artin automorphism $\left(\frac{\mathfrak{p}}{L/K}\right)$ is trivial, since the decomposition groups of the primes lying above $\mathfrak{p}$ are all the trivial group. Conversely, if the Artin automorphism is trivial, then since it generates the decomposition group of any prime above $\mathfrak{p}$, all the decomposition groups are trivial, which means $\mathfrak{p}$ splits completely. Therefore the Artin automorphism of $\mathfrak{p}$ is trivial if and only if $\mathfrak{p}$ splits completely.

There is one more proposition which we want to prove, and then we can apply this to cyclotomic extensions. This proposition talks about the restriction of the Artin automorphism to intermediate extensions.

**Proposition 2.3.79.** *Suppose $M/K$ is an abelian Galois exension and $L$ an intermediate field. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is unramified in $\mathcal{O}_M$. Then $\left(\frac{\mathfrak{p}}{L/K}\right)$ and $\left(\frac{\mathfrak{p}}{M/K}\right)$ are both defined and*

$$\left(\frac{\mathfrak{p}}{L/K}\right) = \left(\frac{\mathfrak{p}}{M/K}\right)\Big|_L.$$

*Remark* 2.3.80. Since $\mathrm{Gal}(M/K)$ is abelian, we immediately get $\mathrm{Gal}(M/L)$ is a normal subgroup, so $L/K$ is a Galois extension and it is abelian since quotients of abelian groups are abelian. Therefore both Artin maps in the proposition make sense.

*Proof.* The diagram illustrating the situation is:

$$\begin{array}{ccc} \mathfrak{P} & & M \\ & & | \\ \mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_L & & L \\ & & | \\ \mathfrak{p} & & K \end{array}$$

Let $\mathfrak{P}$ be a prime of $\mathcal{O}_M$ lying above $\mathfrak{p}$, $\sigma = \left(\frac{\mathfrak{p}}{M/K}\right)$ and $\sigma' = \left(\frac{\mathfrak{p}}{L/K}\right)$. By our characterization of Frobenius elements,

$$\sigma(\alpha) - \alpha^{N(\mathfrak{p})} \in \mathfrak{P}$$

for all $\alpha \in \mathcal{O}_M$. Let $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_L$. If $\alpha \in \mathcal{O}_L$, then $\sigma(\alpha) \in \mathcal{O}_L$ and $\alpha^{N(\mathfrak{p})} \in \mathcal{O}_L$, so

$$\sigma(\alpha) - \alpha^{N(\mathfrak{p})} \in \mathcal{O}_L.$$

But we know it is also in $\mathfrak{P}$, so

$$\sigma(\alpha) - \alpha^{N(\mathfrak{p})} \in \mathcal{O}_L \cap \mathfrak{P} = \mathfrak{P}'.$$

Since $\alpha \in \mathcal{O}_L$ was arbitrary, this implies

$$\sigma|_L = \sigma',$$

which is what we wanted to show. □

**Example 2.3.81.** Consider a cyclotomic extension. In the usual setup, $K = \mathbb{Q}$, and $L = \mathbb{Q}(\zeta_m)$ for some $m$, where $\zeta_m$ is a primitive $m$-th root of unity. We know that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

As usual, we will write elements of the Galois group as $\sigma_k$, where $\sigma_k$ is the map which maps $\zeta_m \mapsto \zeta_m^k$. Proposition 2.3.58 shows that the only primes which ramify are those dividing $m$. So pick $p$ prime with $p \not| m$. Theorem 2.3.6 asserts that the ring of integers of $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$. Let $\mathfrak{p}$ be a prime above $p$.

We want to determine $\left(\frac{p}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right)$. It is the unique element $\sigma$ such that

$$\sigma(\alpha) \equiv \alpha^p \bmod \mathfrak{p}$$

for all $\alpha \in \mathbb{Z}[\zeta_m]$.

The claim is that $\sigma = \sigma_p$. Take any element $\sum a_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$. Then

$$\sigma_p\left(\sum a_i \zeta_m^i\right) = \sum a_i \zeta_m^{ip}.$$

The field $\mathcal{O}_L/\mathfrak{p}$ is of characteristic $p$, and as $a_i \in \mathbb{Z}$, this means $a_i^p \equiv a_i \bmod \mathfrak{p}$. Therefore

$$\sum a_i \zeta_m^{ip} \equiv \sum a_i^p \zeta_m^{ip}.$$

But again as we are in characteristic $p$,

$$\sum a_i^p \zeta_m^{ip} \equiv \left(\sum a_i \zeta_m^i\right)^p \bmod \mathfrak{p}$$

(see appendix B if unclear). Therefore

$$\sigma_p\left(\sum a_i \zeta_m^i\right) \equiv \left(\sum a_i \zeta_m^i\right)^p \bmod \mathfrak{p}.$$

Since $\sum a_i \zeta_m^i$ represented any element in $\mathbb{Z}[\zeta_m]$, this shows $\sigma = \sigma_p$, as desired. Therefore the Artin automorphism is just the $p$-th power map.

# Chapter 3

# Finite abelian case

With most of the required algebraic number theory introduced, we can move on to the heart of the thesis. In this chapter, we will be proving that every finite abelian group occurs as the Galois group of a totally real number field, and we will be examining the primes in these extensions. That is, we will discuss which primes are ramified, which split completely, etc. In addition to all the material in the previous chapter, we will also be introducing and utilizing cubic reciprocity and Dirichlet density to help understand the factorizations of primes in these abelian extensions.

## 3.1 Existence

### 3.1.1 Four Essential Theorems

Before moving towards the existence proof, we will need a few theorems. The hope is that the reader has seen the first three in a course on group theory or abstract algebra, so we will not take the time to prove them here. Proofs can be found in [5], but we will make a few remarks along the way. The first theorem is Cauchy's theorem.

**Theorem 3.1.1** (Cauchy)**.** *Let $G$ be a finite group of order $n$ and $p$ a prime with $p|n$ Then $G$ contains an element of order $p$.*

*Remark* 3.1.2. Cauchy's theorem guarantees that for every prime divisior $p$ of $|G|$, there is a subgroup of order $p$, as one could take the subgroup generated by the element of order $p$.

The other theorem from group theory, perhaps unsurprisingly, is the structure theorem for finitely generated abelian groups.

**Theorem 3.1.3.** *Let $G$ be a finitely generated abelian group. Then there exist numbers $r \geq 0$, $n_i \geq 2$ for $i = 1, 2, \ldots, s$ (for some $s$) such that*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z},$$

*with the added condition that $n_i | n_{i+1}$ for all $1 \leq i \leq s-1$. This representation is also unique. Moreover, if $G$ is finite, then $r = 0$.*

This follows from the structure theorem for finitely generated modules over a PID which was introduced in the previous chapter, and the proof can be found in Chapter 12 of [5]. This theorem is nice because it provides a full classification of finitely generated abelian groups up to isomorphism, and in particular it produces every finite abelian group up to isomorphism. So in the existence proof we provide later, we just need to prove that every group of this form appears as the Galois group of a totally real number field, and this is precisely what we will do.

Using the structure theorem, we can get, rather easily in fact, the Chinese Remainder Theorem, although some books may refer to the Chinese Remainder Theorem when proving Theorem 3.1.3. For one particular case, consider

$$\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z},$$

where the $p_i$ are distinct primes. This is a finite group of order $n = p_1 \cdots p_k$. As it is written, it is not in the form given to us by the structure theorem. The claim is that the only group of order $n = p_1 \cdots p_k$, up to isomorphism, is $\mathbb{Z}/n\mathbb{Z}$. But this is almost immediate from the theorem. The condition $n_i | n_{i+1}$ and the fact $n_1 n_2 \cdots n_s = n$ imply that every prime factor of $n$ has to appear in the final term $n_s$, so $n_s = p_1 \cdots p_k$. But as there are no other factors of $n$ we must have $s = 1$. This says that the only abelian group of order $n$ (where $n$ is a product of distinct primes) is $\mathbb{Z}/n\mathbb{Z}$. Since

$$\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z}$$

has order $n$, it must be isomorphic to $\mathbb{Z}/n\mathbb{Z}$, as desired. This argument can be generalized to prime powers instead of primes.

We will state and prove the Chinese Remainder Theorem as it is generally known (i.e. in its classical form), although we already encountered a more general form of this theorem in Section 2.2.4.

**Theorem 3.1.4** (Chinese Remainder Theorem)**.** *Suppose $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers. Then for any numbers $r_1, \ldots, r_k$, the system of equations*

$$\begin{aligned} x &\equiv r_1 \mod m_1 \\ x &\equiv r_2 \mod m_2 \\ &\vdots \\ x &\equiv r_k \mod m_k \end{aligned}$$

*has a solution $x \in \mathbb{Z}$. Moreover, this solution is unique modulo $m = m_1 m_2 \cdots m_k$.*

*Proof.* We know that $\mathbb{Z}/m_i\mathbb{Z}$ has a natural ring structure, namely with addition and multiplication modulo $m_i$. Consequently, the direct product

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

has a ring structure given by componentwise addition and multiplication. Also, using the natural projections

$$\pi_i : \mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}$$

which are ring homomorphisms, we can build a ring homomorphism

$$\pi : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

given by

$$\pi(n) = (\pi_1(n), \pi_2(n), \ldots, \pi_k(n)).$$

This is easily verified to be a ring homomorphism since each of the $\pi_i$ are. Let $m = m_1 m_2 \cdots m_k$. It should be clear that the kernel of $\pi$ contains the ideal $(m)$ of $\mathbb{Z}$. But the reverse inclusion is also true, namely $(m) = \ker \pi$, because $\pi(n) = 0$ if and only if $n \in (m_i)$ for all $i$, which happens if and only if $n \in (m)$. Thus the first isomorphism theorem says that we have an injection

$$\mathbb{Z}/m\mathbb{Z} \hookrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

But since both the domain and the target space have the same size $m$, the map is also surjective, and therefore an isomorphism. Hence for

$$(r_1, r_2, \ldots, r_k) \in \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

we can find $r \in \mathbb{Z}/m\mathbb{Z}$ that maps to this element, and it is unique. Viewing $r$ as an element of $\mathbb{Z}$ gives the desired result. □

The last theorem we will need is Dirichlet's theorem for primes in arithmetic progressions, which will come in handy on more than one occassion. It is a wonderful theorem, but one whose proof takes us too far afield, so we will not be able to prove it here. A proof is presented in [14].

**Theorem 3.1.5.** *Let $a$ and $m$ be natural numbers such that $(a, m) = 1$ (i.e. relatively prime). There there are infinitely many primes $p$ such that $p \equiv a \bmod m$.*

When we discuss Dirichlet density later in this chapter, we will be able to say slightly more about this theorem.

### 3.1.2 The Proof

First, we will prove two lemmas and two propositions. Throughout this section, $\zeta_k$ denotes a primitive $k$-th root of unity.

**Proposition 3.1.6.** *If $(n, m) = 1$, then $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$.*

*Proof.* Recall from Theorem 2.3.58 that the primes of $\mathbb{Z}$ which ramify in $\mathbb{Q}(\zeta_n)$ are those dividing $n$. Since $(n, m) = 1$, every prime which ramifies in $\mathbb{Q}(\zeta_n)$ remains unramified when factored in $\mathbb{Q}(\zeta_m)$. Therefore the proposition follows from Proposition 2.3.44. □

With this, we can prove the following.

**Lemma 3.1.7.** *If $(n, m) = 1$, then $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{nm})$.*

*Proof.* Notice $\zeta_{nm}^n \in \mathbb{Q}(\zeta_m)$, because $\zeta_{nm}^n$ is an $m$-th root of unity, and $\zeta_{nm}^m \in \mathbb{Q}(\zeta_n)$. This shows $\mathbb{Q}(\zeta_{nm})$ contains both $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)$, and hence contains the composite extension,

$$\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{nm}).$$

Notice that the previous proposition (3.1.6) shows $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)$ are disjoint extensions of $\mathbb{Q}$. Therefore, their compositum, call it $K$, has degree

$$[K : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}][\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(n)\varphi(m)$$

(Corollary A.4.6). But

$$[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}] = \varphi(nm) = \varphi(n)\varphi(m)$$

by the multiplicative properties of Euler's totient function. Therefore

$$[\mathbb{Q}(\zeta_{nm}) : K] = 1.$$

But as $K \subseteq \mathbb{Q}(\zeta_{nm})$, we must have equality. □

As a consequence of this lemma, we get the following.

**Lemma 3.1.8.** *If $p_1, \ldots, p_k$ are distinct primes, then for all $i$,*

$$\mathbb{Q}(\zeta_{p_i}) \cap \prod_{j \neq i} \mathbb{Q}(\zeta_{p_j}) = \mathbb{Q}.$$

*Proof.* Pick any $1 \leq i \leq k$. Since the $p_j$ are distinct, continually using the previous lemma on the $\mathbb{Q}(\zeta_{p_j})$, $j \neq i$, shows

$$\prod_{j \neq i} \mathbb{Q}(\zeta_{p_j}) = \mathbb{Q}(\zeta_{m_i}), \quad m_i = \prod_{j \neq i} p_j.$$

But as $p_i$ is different from all the other $p_j$, $(p_i, m_i) = 1$, and so Proposition 3.1.6 yields

$$\mathbb{Q}(p_i) \cap \mathbb{Q}(\zeta_{m_i}) = \mathbb{Q},$$

or

$$\mathbb{Q}(p_i) \cap \prod_{j \neq i} \mathbb{Q}(\zeta_{p_j}) = \mathbb{Q}.$$

Since $i$ was arbitrary, the lemma is proved. □

Now, let us provide a setup for the last proposition, as well as recall some facts. Suppose we consider the field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, where $\zeta_n$ is a primitive $n$-th root of unity. As we saw in the previous chapter, this is a normal extension of $\mathbb{Q}$, because it is the splitting field of the polynomial $x^n - 1 \in \mathbb{Q}[x]$, and we know splitting fields are normal extensions (appendix A). Also recall that

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

An element $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is completely determined by its action on $\zeta_n$, as it is a generator for this extension, and also must send $\zeta_n \mapsto \zeta_n^a$, where $(a, n) = 1$, as these are the primitive $n$-th roots of unity. As $(n-1, n) = 1$ and the Galois group acts transitively on the primitive $n$-th roots of unity, there must be an element in the Galois group which sends $\zeta_n$ to $\zeta_n^{n-1} = \zeta_n^{-1}$. Denote that element by $\phi$. It is easy to see that $\phi$ has order two in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

**Proposition 3.1.9.** *If $H = \langle \phi \rangle$, where $\phi$ is as above, then $\mathbb{Q}(\zeta_n)^H = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.*

*Proof.* We clearly have the inclusion

$$\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subset \mathbb{Q}(\zeta_n)^H,$$

because $\phi(\zeta_n + \zeta_n^{-1}) = \zeta_n^{-1} + \zeta_n$. Thus if we can show that

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2,$$

we would be done by the Fundamental Theorem of Galois Theory (FTGT, Theorem A.3.10). But observe that $\zeta_n$ is a root of the polynomial

$$x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[x].$$

Since $\zeta_n$ satisfies a degree two polynomial over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, its minimal polynomial over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ cannot have a greater degree, meaning

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \leq 2.$$

But we know from the FTGT that

$$\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{Q}(\zeta_n)^H \subset \mathbb{Q}(\zeta_n)$$

because $H$ is a proper subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, meaning its fixed field is not the whole field (since that corresponds to the trivial subgroup). This implies

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \neq 1,$$

and hence the degree must be two. Therefore $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the fixed field of $H$, since the FTGT tells us that $\mathbb{Q}(\zeta_n)$ will be degree two over the fixed field. □

*Remark* 3.1.10. As easy consequence of this proposition is that the minimal polynomial of $\zeta_n + \zeta_n^{-1}$ is of degree $\varphi(n)/2$, and it is a good exercise for the reader to explain why.

With this proposition proved, we can now prove the main theorem.

**Theorem 3.1.11.** *Let $G$ be a finite abelian group. Then there exists a totally real number field $K/\mathbb{Q}$ with Galois group $G$.*

*Proof.* The structure theorem for finitely generated abelian groups tells us that

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$

where $n_1|n_2|\ldots|n_k$. For each $i$, choose $p_i$ prime such that

$$p_i \equiv 1 \bmod 2n_i,$$

and such that the $p_i$ are distinct (this will be possible by Dirichlet's theorem). Now consider $\mathbb{Q}(\zeta_{p_i})$. This is a Galois extension of $\mathbb{Q}$ with Galois group $G_i$ isomorphic to $(\mathbb{Z}/p_i\mathbb{Z})^\times$. Choose $H_i \leq G_i$ to be the unique subgroup of $G_i$ of order $\frac{p_i-1}{n_i}$ (unique as $G_i$ is cyclic of order $p_i - 1$). As $G_i$ is abelian, $H_i \triangleleft G_i$ is normal, so $\mathbb{Q}(\zeta_{p_i})^{H_i}$ is Galois over $\mathbb{Q}$ by the Fundamental Theorem of Galois Theory, and its Galois group over $\mathbb{Q}$ is isomorphic to $G_i/H_i$. As this is a quotient of a cyclic group, the quotient is still cyclic, and its order is

$$\frac{p_i - 1}{(p_i - 1)/n_i} = n_i.$$

Therefore $G_i/H_i \cong \mathbb{Z}/n_i\mathbb{Z}$. Moreover, by Lemma 3.1.8 above,

$$\mathbb{Q}(\zeta_{p_i}) \cap \prod_{j \neq i} \mathbb{Q}(\zeta_{p_j}) = \mathbb{Q}$$

for all $i$. As $\mathbb{Q}(\zeta_{p_i})^{H_i} \subseteq \mathbb{Q}(\zeta_{p_i})$, we immediately get

$$\mathbb{Q}(\zeta_{p_i})^{H_i} \cap \prod_{j \neq i} \mathbb{Q}(\zeta_{p_j})^{H_j} = \mathbb{Q}$$

for all $i$. Therefore, if we consider the composite

$$K = \mathbb{Q}(\zeta_{p_1})^{H_1} \cdots \mathbb{Q}(\zeta_{p_k})^{H_k},$$

then $K$ is Galois over $\mathbb{Q}$ with Galois group

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1})^{H_1}/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k})^{H_k}/\mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$

which is what we needed.

To finish the proof, we need to show $K$ is totally real. As $K$ is the composite of the $\mathbb{Q}(\zeta_{p_i})^{H_i}$, it suffices to show each of these is totally real. As $\frac{p_i-1}{n_i}$ is even (by choice of $p_i$), $|H_i|$ is even, so Cauchy's theorem says there is an element in $H_i$ of order two, say $\phi_i$. Moreover, $\phi$ is determined completely by its action on $\zeta_{p_i}$. Since $\phi_i : \zeta_{p_i} \mapsto \zeta_{p_i}^a$ (for some $a$) and $\phi_i^2 = e$, the number $a$ satisfies $a^2 = 1$, which means $a = \pm 1$. But $\phi_i \neq e$ implies $a = -1$, since $a = 1$ would correspond to the identity map. Therefore $\phi_i : \zeta_{p_i} \mapsto \zeta_{p_i}^{-1}$. The proposition above (3.1.9) shows that the fixed field of $\langle \phi_i \rangle$ is $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})$. By the Galois correspondence we have the inclusions

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_{p_i})^{H_i} \subset \mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1}) \subset \mathbb{Q}(\zeta_{p_i}).$$

But as $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})$ is a totally real number field, $\mathbb{Q}(\zeta_{p_i})^{H_i}$ must be totally real as well. Since this is true for all $i$ we get each $\mathbb{Q}(\zeta_{p_i})^{H_i}$ is totally real, and hence $K$ is totally real. □

This theorem proves the existence of such extensions. It would be nice to know there were infinitely many such extensions. Indeed, this is the case.

**Corollary 3.1.12.** *If $G$ is a finite abelian group, then there are infinitely many totally real number fields with Galois group $G$ over $\mathbb{Q}$.*

*Proof.* Again, let

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

In the proof of the above theorem, there was a choice in picking our primes $p_i$. But for each $n_i$, there are infinitely many primes $p_i$ satisfying $p_i \equiv 1 \bmod 2n_i$ by Dirichlet's theorem. This, in turn, allows us to construct infinitely many composite extensions (as in the proof of the theorem) with the required Galois group. □

So we have proved the existence of not just one, but infinitely many totally real extensions, for every finite abelian group.

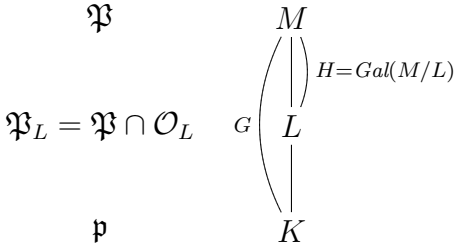
## 3.2 Primes in Extensions

Now that we have totally real extensions of $\mathbb{Q}$ for every finite abelian group, we can consider the behavior of primes in these extensions.

### 3.2.1 Ramified Primes

Let us consider the easiest case first, namely the ramified case. We will prove two lemmas, and these will help not only in this section, but also when we consider the primes which split completely. These come from [13].

**Lemma 3.2.1.** *Suppose $M/K$ is a Galois extension of number fields and $L$ is an intermediate extension. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ and $\mathfrak{P}$ the prime of $\mathcal{O}_M$ lying above $\mathfrak{p}$. Then $\mathfrak{P}_L = \mathfrak{P} \cap \mathcal{O}_L$ is the prime ideal of $L$ lying above $\mathfrak{p}$. Let $G = Gal(M/K)$ and $H = Gal(M/L)$.*




*Then*

*(a)* $D(\mathfrak{P}/\mathfrak{P}_L) = H \cap D(\mathfrak{P}/\mathfrak{p})$ *and*

*(b)* $I(\mathfrak{P}/\mathfrak{p}_L) = H \cap I(\mathfrak{P}/\mathfrak{p})$.

*If, in addition, $H$ is normal in $G$, then if $\pi$ denotes the canonical projection of $G$ onto $G/H \cong Gal(L/K)$, then*

*(c)* $\pi(D(\mathfrak{P}/\mathfrak{p})) = D(\mathfrak{P}_L/\mathfrak{p})$ *and*

*(d)* $\pi(I(\mathfrak{P}/\mathfrak{p})) = I(\mathfrak{P}_L/\mathfrak{p})$.

*Proof.* Items (a) and (b) follow directly from the definition of the decomposition group and inertia group. For (c), notice that $\pi$ certainly maps $D(\mathfrak{P}/\mathfrak{p})$ to $D(\mathfrak{P}_L/\mathfrak{p})$. The kernel of this map is $D(\mathfrak{P}/\mathfrak{p}) \cap H = D(\mathfrak{P}/\mathfrak{P}_L)$ (by (a)). To show the map is onto, we can compute the size of the image. By the first isomorphism theorem, the image has cardinality

$$\frac{|D(\mathfrak{P}/\mathfrak{p})|}{|D(\mathfrak{P}/\mathfrak{P}_L)|} = \frac{e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})}{e(\mathfrak{P}/\mathfrak{P}_L)f(\mathfrak{P}/\mathfrak{P}_L)}.$$

But by Proposition 2.3.43, $e$ and $f$ are multiplicative in towers, so

$$\frac{e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})}{e(\mathfrak{P}/\mathfrak{P}_L)f(\mathfrak{P}/\mathfrak{P}_L)} = e(\mathfrak{P}_L/\mathfrak{p})f(\mathfrak{P}_L/\mathfrak{p}) = |D(\mathfrak{P}_L/\mathfrak{p})|.$$

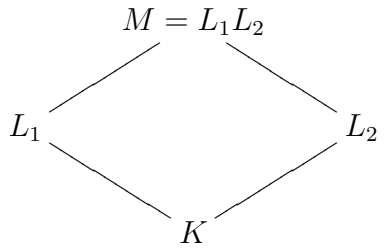
Therefore the map is onto and

$$\pi(D(\mathfrak{P}/\mathfrak{p})) = D(\mathfrak{P}_L/\mathfrak{p}),$$

which proves (c). For (d), the work is exactly the same except we do not have to worry about the residue field degree as the cardinality of the inertia group depends only on the ramification index. □

Using this lemma, we can prove the following.

**Lemma 3.2.2.** *Let $L_1/K$ and $L_2/K$ be two linearly disjoint (finite) Galois extensions of number fields (i.e. $L_1 \cap L_2 = K$) and $M = L_1L_2$ be the compositum. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}$ splits completely in $M$ if and only if it splits completely in $L_1$ and $L_2$. Similarly, $\mathfrak{p}$ is unramified in $M$ if and only if it is unramified in $L_1$ and $L_2$.*




*Proof.* Since $L_1$ and $L_2$ are disjoint,

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K).$$

Take $\mathfrak{P}$ to be a prime of $\mathcal{O}_M$ lying above $\mathfrak{p}$. We have seen that as $|D(\mathfrak{P}/\mathfrak{p})| = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$, $\mathfrak{p}$ splits completely in $M$ if and only if this decomposition group is trivial, i.e. $D(\mathfrak{P}/\mathfrak{p}) = \{e\}$. Let $\mathfrak{P}_1 = \mathfrak{P} \cap L_1$ and $\mathfrak{P}_2 = \mathfrak{P} \cap L_2$. Note that $L_1$ is the fixed field of $\{e\} \times \mathrm{Gal}(L_2/K)$, which is a normal subgroup of $\mathrm{Gal}(M/K)$. Similarly, $L_2$ is the fixed field of $\mathrm{Gal}(L_1/K) \times \{e\}$, which is another normal subgroup of $\mathrm{Gal}(M/K)$. Therefore, we can apply (c) of the previous lemma in both cases. But part (c) of the lemma above implies both $D(\mathfrak{P}_1/\mathfrak{p})$ and $D(\mathfrak{P}_2/\mathfrak{p})$ are trivial. Therefore $\mathfrak{p}$ splits completely in $L_1$ and $L_2$.

Conversely, suppose $\mathfrak{p}$ splits completely in $L_1$ and $L_2$. Then, as before, $D(\mathfrak{P}_1/\mathfrak{p})$ and $D(\mathfrak{P}_2/\mathfrak{p})$ are trivial. Take $\sigma \in D(\mathfrak{P}/\mathfrak{p})$. Again using (c) in the previous proposition (it applies for the same reason as above), we get the projections of $\sigma$ onto $\mathrm{Gal}(L_1/K)$ and $\mathrm{Gal}(L_2/K)$ are both trivial. But as

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K),$$

this implies $\sigma$ is the identity. Therefore the decomposition group $D(\mathfrak{P}/\mathfrak{p})$ is trivial, and so $\mathfrak{p}$ splits completely in $M$.

To prove the last part of the lemma, note that an unramified prime corresponds to a trivial inertia group. Follow the same steps as we just did for the decomposition group and replace $D$ with $I$. Since part (d) of the previous lemma gives a corresponding result for inertia groups, the same work can be used, and the statement follows. □

Of course, we can inductively extend this lemma to any finite number of extensions.

**Corollary 3.2.3.** *Suppose $L_1, \ldots, L_m$ are all finite Galois extensions of a number field $K$ such that*

$$L_i \cap \prod_{j \neq i} L_j = K$$

*for all $1 \leq i \leq m$. Let $M = L_1 \cdots L_k$. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}$ splits compeletely in $M$ if and only if it splits completely in all the $L_i$. Similarly, $\mathfrak{p}$ is unramified in $M$ if and only if it is unramified in all the $L_i$.*

So now let us consider the number field $K$ constructed in the proof of Theorem 3.1.11.

Let $G$ be a finite abelian group, and write

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

as before (with $n_i | n_{i+1}$). Recall that we first choose primes $p_i \equiv 1 \bmod 2n_i$. The totally real number field constructed in the proof of Theorem 3.1.11 is then

$$K = \prod \mathbb{Q}(\zeta_{p_i})^{H_i},$$

where $H_i \leq \mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q})$ is the unique subgroup of order $\frac{p_i - 1}{n_i}$.

The next proposition proves which primes ramify in $K$.

**Proposition 3.2.4.** *The only primes which ramify in $K$ are $p_1, \ldots, p_k$.*

*Proof.* Let $\mathbb{Q}(\zeta_{p_i})^{H_i}$ be as in the remarks preceding the proposition, and let $K_i = \mathbb{Q}(\zeta_{p_i})^{H_i}$. By Corollary 3.2.3, a prime is unramified in $K$ if and only if it is unramfied in all the $K_i$. This also means that a prime ramifies in $K$ if and only if it ramifies in some $K_i$. So let us consider which primes ramify in $K_i$. Well $K_i \subseteq \mathbb{Q}(\zeta_{p_i})$, and we know from Proposition 2.3.58 that the only prime which ramifies in $\mathbb{Q}(\zeta_{p_i})$ is $p_i$. Therefore the only prime which can possibly ramify in $K_i$ is $p_i$. However, as there are no unramified extensions of $\mathbb{Q}$ (Theorem 2.3.32), some prime must ramify in $K_i$, and therefore $p_i$ ramifies. Therefore $p_i$ is the only prime which ramifies in $K_i$, and hence $p_1, \ldots, p_k$ ramify in $K$. If $p$ is a prime different from the $p_i$, then we see that $p$ remains unramified in all the $K_i$, and hence in $K$ by Corollary 3.2.3. □

There are two simple corollaries of this proposition.

**Corollary 3.2.5.** *Suppose $G$ is a finite abelian group, and write*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

*where $n_i | n_{i+1}$, which is possible by the Structure Theorem for Finitely Generated Abelian Groups. Then there exist infinitely many totally real number fields $K$ which are ramified at precisely $k$ primes such that $Gal(K/\mathbb{Q}) \cong G$.*

*Proof.* We already constructed such a $K$ in Theorem 3.1.11, saw there were infinitely many in Corollary 3.1.12, and the previous proposition shows each $K$ is unramified outside a set of $k$ distinct primes. □

**Corollary 3.2.6.** *If $G$ is a finite cyclic group, then there exist infinitely many totally real number fields $K$ which are ramified at a single prime and such that $Gal(K/\mathbb{Q}) \cong G$.*

*Proof.* Cyclic groups correspond to the case $k = 1$ in the previous corollary. □

The totally real field $K$ of Proposition 3.2.4 is ramified at precisely $k$ primes, which is precisely the number of generators for the finite group $G$. Boston and Markin [2] prove that this we can do no better. That is, we cannot find a totally real extension $K$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$ ramified at fewer than $k$ primes. In fact, they conjecture that if $G$ is a finite group, then the fewest number of ramified primes in any extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ is the number of generators in the abelianization of $G$, namely $G/G'$, where $G'$ is the commutator subgroup of $G$.

### 3.2.2 Dirichlet Density

Before investigating the primes which split completely, we will introduce a tool that will allow us to, in a certain sense, understand how dense (or sparse) a set of primes is. This material will mainly come from [14].

Let $P$ be the set of all primes in $\mathbb{Z}$ and let $A \subseteq P$ be a subset. If one were to create a notion of "density" for the set $A$, a natural starting point would be the question "what fraction of $P$ is contained in $A$?" Of course, the set $P$ is an infinite set, so this would have to be modified. Instead, we could consider a given $n \in \mathbb{N}$ and consider the fraction

$$D_n(A) = \frac{\#\{x \in A : x \leq n\}}{\#\{x \in P : x \leq n\}}.$$

Both these sets are finite, and so this quotient makes sense and is a well-defined rational number in $[0, 1]$. Then the density of the set $A$ could be

$$D(A) = \lim_{n \to \infty} D_n(A).$$

This is, in fact, one notion of density, called "natural density." This density works fine, but there is another density which turns out to be the more useful one to consider.

**Definition 3.2.7.** If $A \subseteq P$ is a set of prime numbers, then the *Dirichlet density* of $A$ is defined to be

$$\delta(A) = \lim_{s \to 1^+} \frac{\sum_{p \in A} \frac{1}{p^s}}{\log\left(\frac{1}{s-1}\right)},$$

where the notation $s \to 1^+$ denotes a limit for $s \in \mathbb{R}$ as $s \searrow 1$.

The motivation behind this definition comes from the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

which is an analytic function on the half plane $\Re(s) > 1$ (i.e. real part of $s$ strictly greater than 1). The details go too far off topic, but the zeta function has a continutation to all of $\mathbb{C}$, with a simple pole at $s = 1$ (which is where the term $1/(s-1)$ comes from). So we can write

$$\zeta(s) = \frac{1}{s-1} + \text{some analytic function.}$$

Using the Euler product

$$\zeta(s) = \prod_{p \in P} \frac{1}{1 - p^{-s}},$$

one can show that

$$\sum_{p \in P} \frac{1}{p^s} \sim \log\left(\frac{1}{s-1}\right).$$

That is,

$$\lim_{s \to 1^+} \frac{\sum_{p \in P} \frac{1}{p^s}}{\log\left(\frac{1}{s-1}\right)} = 1.$$

Therefore the Dirichlet density of all the primes is $\delta(P) = 1$. Immediately, we get the following proposition.

**Proposition 3.2.8.** *A finite set of primes $A \subset P$ has Dirichlet density $\delta(A) = 0$.*

*Proof.* By definition,

$$\delta(A) = \lim_{s \to 1^+} \frac{\sum_{p \in A} \frac{1}{p^s}}{\log\left(\frac{1}{s-1}\right)}.$$

Since $A$ is finite, the numerator remains bounded as $s \to 1^+$, and the denominator is unbounded. Therefore the quotient tends to 0, meaning $\delta(A) = 0$. □

In the previous section, we made use of Dirichlet's theorem on primes in an arithemetic progression. We now restate that theorem in terms of Dirichlet density.

**Theorem 3.2.9** (Dirichlet)**.** *If $(a, m) = 1$, then the set of primes $p \equiv a \bmod m$ has Dirichlet density $1/\varphi(m)$.*

*Remark* 3.2.10. Of course, this implies the set of primes $\equiv a \bmod m$ is infinite, as $1/\varphi(m) > 0$. This also says that the set of primes is, in some sense, equally distributed amongst the equivalence classes (modulo $m$) which are coprime to $m$. So for example, if $m = 6$, then the two numbers $\leq 6$ and relatively prime to 6 are 1 and 5, so $\varphi(6) = 2$. Therefore, Dirichlet's theorem says that, with this notion of density, $1/2$ the primes are of the form $6n + 1$ and the other half are of the form $6n + 5$.

The Dirichlet density will come in handy in the next section as well as later in the chapter.

### 3.2.3 Primes which split completely

Now we can investigate the primes which split completely in our abelian extension. The following theorem, from [3], gives us part of the solution.

**Theorem 3.2.11.** *Suppose $K \subseteq \mathbb{Q}(\zeta_m)$ is a subfield, and make the usual identification $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. Let $H \leq (\mathbb{Z}/m\mathbb{Z})^\times$ be the subgroup identified with $Gal(\mathbb{Q}(\zeta_m)/K)$. Then the primes $p \nmid m$ which split completely in $K/\mathbb{Q}$ are those such that $p \bmod m \in H$.*

*Proof.* If $p \nmid m$, then $p$ is unramified in $K$. The reader will recall that a prime splits completely if and only if the Artin automorphism is trivial. Example 2.3.81 shows that the Artin automorphism for the prime $p \in \mathbb{Z}$ is $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/Q)$, where $\sigma_p$ is the map which sends $\zeta_m \mapsto \zeta_m^p$. Proposition 2.3.79 asserts

$$\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \left(\frac{p\mathbb{Z}}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right)\Big|_K = \sigma_p|_K.$$

So $p$ splits completely if and only if $\sigma_p|_K = 1$. Since

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta_m)/K),$$

we find

$$\sigma_p|_K = 1 \iff \sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K).$$

But under the identification $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$,

$$\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K) \iff p \bmod m \in H.$$

□

**Example 3.2.12.** Consider $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. The degree of the extension is $\varphi(7) = 6$, and the Galois group is cyclic. Consider the real subfield $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. We have seen (Proposition 3.1.9) that $K$ has index 2 in $\mathbb{Q}(\zeta_7)$. Therefore $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/K)$ has order 2. There is only one subgroup $H$ of order 2 in $(\mathbb{Z}/7\mathbb{Z})^\times$. It is easy to compute $H = \{1, 6\}$. Therefore, a prime splits completely in $K/\mathbb{Q}$ if and only if $p \equiv 1$ or 6 mod 7.

In the next section, we generalize this result to tell us about the behavior of other unramified primes, such as the ones which remain prime in $K$.

Let us quickly reintroduce notation. Let $G$ be a finite abelian group, and, as always, write

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_i | n_{i+1}$. The totally real number field we built was

$$K = \prod \mathbb{Q}(\zeta_{p_i})^{H_i},$$

where the $p_i$ are distinct primes such that $p_i \equiv 1 \bmod 2n_i$ and $H_i \leq \mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q})$ is the unique subgroup of order $\frac{p_i - 1}{n_i}$. We proved in Proposition 3.2.4 that the only primes of $\mathbb{Z}$ which ramify in $K$ are the $p_i$. Let $K_i = \mathbb{Q}(\zeta_{p_i})^{H_i}$.

We proved, in Corollary 3.2.3, that a prime $p$ will split completely in $K$ if and only if it splits completely in all the $K_i$. But Theorem 3.2.11 provides us with a useful way of describing the primes which split in $K_i$. So we can now state the main theorem of this section.

**Theorem 3.2.13.** *The set of primes which split completely in $K$ has Dirichlet density $\frac{1}{n_1 n_2 \cdots n_k}$. In particular, the set is infinite.*

*Proof.* Abusing notation slightly, we will let $H_i$ also denote the cyclic subgroup of $(\mathbb{Z}/p_i\mathbb{Z})^\times$ of order $\frac{p_i - 1}{n_i}$. By Theorem 3.2.11 above, the primes which split completely in $K_i$ are precisely those $p$ such that $p \bmod p_i \in H_i$. The Chinese Remainder Theorem (3.1.4), gives an isomorphism

$$\mathbb{Z}/p_1 \cdots p_k\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z}.$$

For each $i$, choose any element $h_i \in H_i$. This isomorphism says that there exists some unique $a \bmod p_1 \cdots p_k$ such that

$$a \equiv h_i \bmod p_i \quad \text{for all } i.$$

Moreover, if $p$ is a prime such that $p \equiv a \bmod p_1 \cdots p_k$, then $p$ will split completely in $K$. To see this, notice that $p \equiv a \bmod p_1 \cdots p_k$ implies $p \equiv h_i \bmod p_i$ for all $i$. Therefore $p \bmod p_i \in H_i$ for all $i$, and so by Theorem 3.2.11, $p$ splits in $K_i$ for all $i$, meaning $p$ splits completely in $K$.

Letting the various $h_i$ range over all the elements of $H_i$ provides a set $\{a_j\}$ of $|H_1||H_2|\cdots|H_k|$ unique values modulo $p_1\cdots p_k$. To see they are unique, it suffices to note that two different $a_i$ will be different modulo $p_j$ for some $j$, and hence must be distinct modulo $p_1\cdots p_k$. By the above argument $p$ will split completely in $K$ if $p$ is equivalent to one of these values of $a_j$ modulo $p_1\cdots p_k$. Conversely, if $p$ is not equivalent to one of these $a_j$, then $p \bmod p_i \notin H_i$ for some $i$, and hence will not split completely in $K$. Therefore $p$ splits completely if and only if it is equivalent to some $a_j$.

As noted above, there are $|H_1||H_2|\cdots|H_k|$ values in the set $\{a_j\}$. But

$$|H_1||H_2|\cdots|H_k| = \frac{(p_1-1)(p_2-1)\cdots(p_k-1)}{n_1\cdots n_k}.$$

Euler's totient function is multiplicative for relatively prime numbers, so

$$\varphi(p_1\cdots p_k) = \varphi(p_1)\cdots\varphi(p_k) = (p_1-1)\cdots(p_k-1).$$

By Dirichlet's theorem (Theorem 3.2.9), the set of primes equivalent to $a_j$ modulo $p_1\cdots p_k$ has Dirichlet density

$$\frac{1}{\varphi(p_1\cdots p_k)} = \frac{1}{(p_1-1)\cdots(p_k-1)}.$$

Since different values of $a_j$ give a different set of primes, and Dirichlet density is clearly additive for disjoint sets (provided the densities exist for each individual set), the Dirichlet density of the primes which split completely in $K$ is

$$\frac{1}{\varphi(p_1\cdots p_k)}\cdot|\{a_j\}| = \frac{1}{(p_1-1)\cdots(p_k-1)}\cdot\frac{(p_1-1)(p_2-1)\cdots(p_k-1)}{n_1\cdots n_k} = \frac{1}{n_1\cdots n_k}.$$

Since this number is strictly positive, the set of primes which split completely is necessarily infinite. □

*Remark* 3.2.14. This result is a special case of another theorem (which we will not prove), which says that if $K/\mathbb{Q}$ is a number field, then the Dirichlet density of the set of primes of $\mathbb{Z}$ which split completely in $K$ is $\frac{1}{[K:\mathbb{Q}]}$. Notice that in our case, the totally real extension has degree $n_1n_2\cdots n_k$ over $\mathbb{Q}$, showing that the theorem works in this specific case.

This theorem not only shows that set of primes which split completely is infinite, it provides a way of finding the primes. Let us take a look at two examples.

**Example 3.2.15.** Consider $G = \mathbb{Z}/4\mathbb{Z}$. In this example $k = 1$. First, we must select a prime congruent to 1 mod 8, so let us choose $p = 17$. Then $\frac{p-1}{n} = 4$. Our totally real number field $K$ is

$$K = \mathbb{Q}(\zeta_{17})^H,$$

where

$$H \leq \mathrm{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) \cong (\mathbb{Z}/17\mathbb{Z})^{\times}$$

is the unique subgroup of order four. Observe that $(\mathbb{Z}/17\mathbb{Z})^{\times}$ is cyclic. Therefore the elements of $H$ are those elements $a$, modulo 17, which have order dividing four. To find $H$ explicitly, we can simply consider the roots of the equation $x^4 = 1$ modulo 17. One readily checks that the solutions are $\{1, 4, 13, 16\}$. So $H$ is the subgroup consisting of $\{1, 4, 13, 16\}$ (or these equivalence classes modulo 17).

The only prime which ramifies is $p = 17$ since $K$ is a subfield of $\mathbb{Q}(\zeta_{17})$ and 17 is the only prime which ramifies in $\mathbb{Q}(\zeta_{17})$. Notice this agrees with Proposition 3.2.4 and Corollary 3.2.6. Moreover, by either Theorem 3.2.11 or the proof of the previous theorem (Theorem 3.2.13), the primes which split completely in $K$ are those $p$ such that $p \equiv 1, 4, 13,$ or 16 mod 17.

**Example 3.2.16.** Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Here, $k = 2$. This time, we need two distinct primes $p_1$ and $p_2$, each congruent to 1 mod $4(= 2 \cdot 2)$. Let $p_1 = 5$ and $p_2 = 13$. So

$$K = \mathbb{Q}(\zeta_5)^{H_1}\mathbb{Q}(\zeta_{13})^{H_2},$$

where $H_1$ is the unique subgroup of $(\mathbb{Z}/5\mathbb{Z})^{\times}$ is the unique subgroup of order $\frac{5-1}{2} = 2$ and $H_2$ is the unique subgroup of $(\mathbb{Z}/13\mathbb{Z})^{\times}$ of order $\frac{13-1}{2} = 6$. As in the previous example, to find $H_1$ we can search for solutions to $x^2 \equiv 1$ mod 5, which yields $H_1 = \{1, 4\}$. Similarly, $H_2$ consists of those numbers mod 13 which are solutions to $x^6 \equiv 1$ mod 13, and those are $H_2 = \{1, 3, 4, 9, 10, 12\}$.

Here, the primes of $\mathbb{Z}$ which ramify in $K$ are $p_1 = 5$ and $p_2 = 13$. To find the primes which split completely, we proceed as in the proof of Theorem 3.2.13. There are going to be $|H_1||H_2| = 12$ distinct values mod $5 \cdot 13 = 65$ to search for. They will come from the solutions $a$ of the equations

$$a \equiv h_1 \bmod 5,$$

$$a \equiv h_2 \bmod 13,$$

where $h_1$ and $h_2$ range over all values of $H_1$ and $H_2$, respectively. Again, it is readily checked that the set of 12 values is

$$H = \{1, 4, 9, 14, 16, 29, 36, 49, 51, 56, 61, 64\}.$$

Therefore the primes which split completely are those $p$ such that $p$ mod $65 \in H$. The reader will notice that

$$\varphi(65) = \varphi(5)\varphi(13) = 4 \cdot 12 = 48,$$

and so the Dirichlet density of primes which split completely in $K$ is

$$\frac{12}{48} = \frac{1}{4} = \frac{1}{2 \cdot 2}.$$

### 3.2.4 Other Primes

It would, of course, be nice to classify the behavior of the remaining primes of $\mathbb{Z}$ in our constructed abelian extensions (i.e. those which do not ramify and do not split completely). To do this, we make a generalization of Theorem 3.2.11, which characterized the primes which split completely.

**Theorem 3.2.17.** *Suppose $K \subseteq \mathbb{Q}(\zeta_m)$ is a subfield, let $n = [K : \mathbb{Q}]$, and make the usual identification $G = Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. Let $H \leq (\mathbb{Z}/m\mathbb{Z})^\times$ be the subgroup identified with $Gal(\mathbb{Q}(\zeta_m)/K)$. Suppose $p \nmid m$, so $p$ is unramified in $K$ and $\mathbb{Q}(\zeta_m)$. We have seen that the Artin automorphism $\left(\frac{p\mathbb{Z}}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right)$ for the prime $p$ is $\sigma_p$, where $\sigma_p : \zeta_m \mapsto \zeta_m^p$. Let $f$ be the smallest natural number for which $\sigma_p^f \in H$. Then $p\mathbb{Z}$ factors as the product of $\frac{n}{f}$ distinct prime ideals in $K$, each with residue field degree $f$. In particular, the primes which split into $\frac{n}{f}$ distinct prime ideals in $K$ are those primes such that $p^f \bmod m \in H$ but $p^d \bmod m \notin H$ for $d \leq f$.*

*Proof.* Recall $\mathrm{Gal}(K/\mathbb{Q}) \cong G/H$. The condition that $f$ is the smallest natural number for which $\sigma_p^f \in H$ is precisely the statement that the restriction of $\sigma_p$ to $K$ has order $f$ in $\mathrm{Gal}(K/\mathbb{Q})$. Proposition 2.3.79 shows

$$\bar{\sigma}_p = \left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \left(\frac{p\mathbb{Z}}{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\right)\Big|_K = \sigma_p|_K.$$

So $\bar{\sigma}_p$ has order $f$. Let $\mathfrak{P}$ be a prime of $\mathcal{O}_K$ lying above $p$. We know $p$ is unramified and so we have an isomorphism

$$D(\mathfrak{P}/p) \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_p),$$

where $\mathbb{F}_\mathfrak{P} = \mathcal{O}_K/\mathfrak{P}$ and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (Proposition 2.3.65 and Remark 2.3.72). Since $D(\mathfrak{P}/p)$ is cyclic (as $p$ is unramified) and generated by $\bar{\sigma}_p$, the order $|D(\mathfrak{P}/p)| = f$, and therefore $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_p)$ has order $f$ in $\mathrm{Gal}(K/\mathbb{Q})$. Since $|\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_p)| = [\mathbb{F}_\mathfrak{P} : \mathbb{F}_p]$, by definition residue field degree of $\mathfrak{P}$ is precisely $f$. As $K/\mathbb{Q}$ is a Galois extension, the residue field degree and ramification index is equal for every prime lying above $p$. If $p$ splits into $g$ distinct primes, we have the identity

$$efg = n$$

by Theorem 2.3.48. But $p$ is unramified, so $e = 1$, and therefore $g = \frac{n}{f}$. Hence $p$ splits into $\frac{n}{f}$ distinct prime ideals in $K$, each with residue field degree $f$.

For the last part of the theorem, notice that $\sigma_p^f : \zeta_m \mapsto \zeta_m^{p^f}$, and so $\sigma_p^f$ is the element $\sigma_{p^f}$ of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Of course, using the usual identification, we can regard this as the element $p^f$ of $(\mathbb{Z}/m\mathbb{Z})^\times$. But as

$$\sigma_{p^f}|_K = \sigma_p^f|_K = \bar{\sigma}_p^f = 1 \in \mathrm{Gal}(K/\mathbb{Q})$$

and $\mathrm{Gal}(K/\mathbb{Q}) \cong G/H$, this implies $p^f \bmod m \in H$. Moreover, if $d \leq f$, then $p^d \bmod m \notin H$ as this would imply $\sigma_p^d \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K) \cong H$, which contradicts the minimality of $f$. $\square$

Before applying this theorem, let us first illustrate a different way to view our constructed abelian extensions. As always, let $G$ be a finite abelian group with

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_i | n_{i+1}$. For each $i$ choose $p_i \equiv 1 \bmod 2n_i$ with all the $p_i$ distinct primes. Let $n = p_1 \cdots p_k$. We have been considering $K_i = \mathbb{Q}(\zeta_{p_i})^{H_i}$, where $H_i \leq \mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}) \cong (\mathbb{Z}/p_i\mathbb{Z})^\times$ is the unique subgroup of order $\frac{p_i-1}{n_i}$. Now, lemmas 3.1.7 and 3.1.8 tell us that

$$\mathbb{Q}(\zeta_n) = \prod_{i=1}^{k} \mathbb{Q}(\zeta_{p_i}),$$

and moreover

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k})/\mathbb{Q}).$$

Of course, we can write this this as

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times,$$

which could also have been found using the Chinese Remainder Theorem. Since

$$H_i \leq (\mathbb{Z}/p_i\mathbb{Z})^\times,$$

we can let

$$H = H_1 \times \cdots \times H_k,$$

and see that this is a subgroup of

$$(\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times.$$

Under the isomorphism above we can consider $H$ as a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. So instead of considering the composite

$$K = K_1 \cdots K_k = \mathbb{Q}(\zeta_{p_1})^{H_1} \cdots \mathbb{Q}(\zeta_{p_k})^{H_k},$$

we can look at

$$K = \mathbb{Q}(\zeta_n)^H.$$

It is clear from the way this is constructed that $K$ is the same totally real extension we had investigated in previous sections, only this time we see it in a different light. Namely, now we can view it is a subfield of a single cyclotomic field instead of considering it as a composite of extensions. It makes applying the theorems slightly easier.

Now let us look at a couple of examples to demonstrate the ideas in Theorem 3.2.17.

**Example 3.2.18.** Let us continue working with the group in Example 3.2.15, namely $G = \mathbb{Z}/4\mathbb{Z}$. Proceeding as in that example, we let $p = 17$ be our chosen prime, and $H$ is the subgroup of $(\mathbb{Z}/17\mathbb{Z})^\times$ consisting of $H = \{1, 4, 13, 16\}$. So $K = \mathbb{Q}(\zeta_{17})^H$ is our desired quartic extension. We have already seen the set of primes which split completely in $K$, and it consists of those $p$ such that $p \bmod m \in H$. This corresponds to the case $f = 1$ in Theorem 3.2.17.

Let $p$ be any unramified prime. Here, $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$, so $\sigma_p|_K$ (the Artin map corresponding to $p$ in $\mathbb{Q}(\zeta_{17})$ restricted to $K$) must have order 1, 2 or 4. If it has order one, then $p$ splits completely (as it splits into $\frac{4}{1} = 4$ distinct prime ideals each of residue field degree $f = 1$). If it has order 2, then $p^2 \bmod 17 \in H$ but $p \bmod 17 \notin H$. Therefore to find the primes for which $\sigma_p|_K$ has order two, we need to look for elements $a \bmod 17$ such that $a^2 \bmod 17 \in H$ but $a \notin H$. This corresponds to the set $H'$, where

$$H' = \{2, 8, 9, 15\}.$$

Thus if $p \equiv 2, 8, 9,$ or $15 \bmod 17$, then $p^2 \in H$ but $p \notin H$, and so $\sigma_p|_K$ has order 2. Therefore $p$ will split into a product of two distinct prime ideals, each with residue field degree $\frac{4}{2} = 2$.

Finally, $\sigma_p|_K$ could have order 4, in which case $p$ would remain prime in $K$ (i.e. remain inert) and would have residue field degree 4. This corresponds to primes $p$ such that $p^4 \bmod 17 \in H$, with $p^2 \bmod 17 \notin H$ and $p \bmod 17 \notin H$ (as in Theorem 3.2.17). To get equivalence classes mod 17 for this case, we need to find $a$ modulo 17 for which $a^4 \bmod 17 \in H$ but $a^2 \bmod 17, a \bmod 17 \notin H$. As the orders in $G/H \cong \mathbb{Z}/4\mathbb{Z}$ can only be $1, 2$ or 4, we need all the equivalence classes we have not used, and this is the set

$$H'' = \{3, 5, 6, 7, 10, 11, 12, 14\}.$$

Thus if $p \bmod 17 \in H''$, then $p$ remains inert in $K$.

*Remark* 3.2.19. Observe that this classifies the behavior of all primes in the extension $K$.

**Example 3.2.20.** For this, let us use $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as in Example 3.2.16. In that example, we chose $p_1 = 5$ and $p_2 = 13$ to be our two primes, so $n = p_1 p_2 = 65$. Moreover, $H_1 \leq (\mathbb{Z}/5\mathbb{Z})^\times$ is the cyclic subgroup of order 2 and $H_2 \leq (\mathbb{Z}/13\mathbb{Z})^\times$ is the subgroup of order 6. Therefore $H_1 \times H_2$ is a subgroup of $(\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/13\mathbb{Z})^\times$ of order 12, and under the isomorphism

$$(\mathbb{Z}/65\mathbb{Z})^\times \cong (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/13\mathbb{Z})^\times$$

corresponds to the subgroup $H \leq (\mathbb{Z}/65\mathbb{Z})^\times$ with elements

$$H = \{1, 4, 9, 14, 16, 29, 36, 49, 51, 56, 61, 64\}.$$

Therefore $K = \mathbb{Q}(\zeta_{65})^H$.

Now let $p \neq 5, 13$ be a prime (necessarily unramified as 5 and 13 are the only two primes which ramify in $K$), and consider its Artin automorphism $\sigma_p = \left(\frac{p\mathbb{Z}}{\mathbb{Q}(\zeta_{65})/\mathbb{Q}}\right)$. Now $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and so $\sigma_p|_K$ must have order 1 or 2 (as elements in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ all have order 1 or 2). If its order is 1, then $p$ splits completely, and so $p \bmod 65 \in H$ by Example 3.2.16. To find the primes for which $\sigma_p|_K$ has order 2, all we have to do is note that since $\sigma_p|_K$ must have order 1 or 2, the primes for which it has order 2 are the primes for which it does not have order 1 (or which ramify). Therefore, letting

$$H' = \{2, 3, 6, 7, 8, 11, 12, 17, 18, 19, 21, 22, 23, 24, 27, 28, 31, 32, 33, 34, 37, 38,$$

$$41, 42, 43, 44, 46, 47, 48, 53, 54, 57, 58, 59, 62, 63\},$$

we get $p$ splits into 2 distinct prime ideals, each with residue degree 2, if $p \bmod 65 \in H'$.

*Remark* 3.2.21. Note that this also implies no prime of $\mathbb{Z}$ remains inert in $K$. To see another reason why, notice that if $p$ is unramified and $\mathfrak{P}$ is a prime of $\mathcal{O}_K$ above $p$, then the isomorphism

$$D(\mathfrak{P}/p) \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p)$$

shows the decomposition group is cyclic. But as

$$D(\mathfrak{P}/p) \leq \mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

it cannot be cyclic of order greater than 2, meaning the Artin automorphism (which generates the decomposition group) cannot have order greater than 2. This reasoning will appear again in the last section of the chapter.

## 3.3 Polynomials with Abelian Galois group

Let us recap the results so far. For a finite abelian group $G$, we have constructed a totally real number field $K$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$. Moreover, we proved there were infinitely many such extensions. For these extensions, we have considered the factorization of primes of $\mathbb{Z}$, and have managed to classify which primes ramify, split completely, or factor in some alternative manner.

However, there are still things that we could do. For example, we have not actually exhibited polynomials with Galois group $G$ or splitting field $K$. And while we have seen that infinitely many primes of $\mathbb{Z}$ will split completely in $K$, we have not considered whether a given prime of $\mathbb{Z}$, say 2 or 5, splits in infinitely

many of these totally real extensions with Galois group $G$. These are the questions we will answer in the remaining sections of this chapter.

In this section, we will first show how to write down a polynomial with splitting field $K$. Let us, once again, recall the notation. Let $G$ be a finite abelian group, and write

$$G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$

with $n_i | n_{i+1}$. For each $i$, choose a prime $p_i$ with $p_i \equiv 1 \bmod 2n_i$, and let $n = p_1 \cdots p_k$. Also for each $i$, let $H_i$ be the unique subgroup of $(\mathbb{Z}/p_i\mathbb{Z})^\times$ of order $\frac{p_i - 1}{n_i}$, and then consider the subgroup

$$H_1 \times \cdots \times H_k \leq (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times .$$

Let $H$ denote the corresponding subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ under the isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times .$$

Then our totally real number field $K = \mathbb{Q}(\zeta_n)^H$ has Galois group $G$.

If we had a way to explicitly describe the fixed field $\mathbb{Q}(\zeta_n)^H/\mathbb{Q}$, i.e. find a generator $\alpha$ such that $\mathbb{Q}(\zeta_n)^H = \mathbb{Q}(\alpha)$, then we could find a polynomial with this field as its splitting field. We could, for example, let $m_\alpha(x) \in \mathbb{Q}[x]$ denote the minimal polynomial of $\alpha$ over $\mathbb{Q}$, in which case the splitting field of $m_\alpha(x)$ would be $K$. To see why, just observe that any splitting field (when regarded as a subfield of $\mathbb{C}$) would have to contain $\alpha$, and since $K = \mathbb{Q}(\alpha)$ is the smallest field containing $\mathbb{Q}$ and $\alpha$ and is also Galois over $\mathbb{Q}$, this would necessarily be the splitting field.

So the goal is to find a generator for the fixed field. The key to the proof will be the following lemma, which can be found in [4] and the associated link.

**Lemma 3.3.1.** *Suppose $n$ is squarefree. Then the primitive $n$-th roots of unity form a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.*

*Proof.* If $n$ is squarefree, then it is the product of distinct primes, $n = p_1 \cdots p_k$. We can use induction on the number of primes $k$. Suppose $k = 1$. Then $n = p$ is prime, and we know that

$$1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}$$

forms a basis for $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. This implies that the elements

$$\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}, -1 - \zeta_p - \ldots - \zeta_p^{p-2}$$

also forms a basis. Since

$$\zeta_p^{p-1} = -1 - \zeta_p - \ldots - \zeta_p^{p-2},$$

this implies that the $p-1$ primitive $p$-th roots of unity constitute a basis for $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, and the statement follows.

Now suppose it is true for $k-1$ primes. We want it true for $k$ primes. If $n = p_1 \cdots p_k$, then write $n = cp$, where $c = p_1 \cdots p_{k-1}$. By induction, the primitive $c$-th roots of unity form a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta_c)/\mathbb{Q}$ and and primitive $p_k$-th roots of unity form a basis for $\mathbb{Q}(\zeta_{p_k})/\mathbb{Q}$. Now, by Proposition 3.1.6, $\mathbb{Q}(\zeta_c) \cap \mathbb{Q}(\zeta_{p_k}) = \mathbb{Q}$, and by Lemma 3.1.7, $\mathbb{Q}(\zeta_c)\mathbb{Q}(\zeta_{p_k}) = \mathbb{Q}(\zeta_n)$. Since the two extensions are disjoint and the two bases are given by

$$\{\zeta_c^i : 1 \leq i \leq c, (i,c) = 1\} \quad \text{and} \quad \{\zeta_{p_k}^j : 1 \leq j \leq p_k, (j,p_k) = 1\},$$

a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_c)\mathbb{Q}(\zeta_{p_k})$ is given by

$$\{\zeta_c^i \zeta_{p_k}^j : 1 \leq i \leq c, 1 \leq j \leq p_k, (i,c) = 1, (j,p_k) = 1\}.$$

Now $\zeta_c = \zeta_n^{n/c}$ and $\zeta_{p_k} = \zeta_n^{n/p_k}$, and since

$$\frac{n}{c} i + \frac{n}{p_k} j = p_k i + cj,$$

we can write this basis as

$$\{\zeta_n^{p_k i + cj} : 1 \leq i \leq c, 1 \leq j \leq p_k, (i,c) = 1, (j,p_k) = 1\}.$$

Notice that for these $i$ and $j$, $(n, p_k i + cj) = 1$. To see why, notice first that $(p_k i, c) = 1$ and $(cj, p_k) = 1$ since $(p_k, c) = 1$ and $(i,c) = (j,p_k) = 1$. Therefore $(p_k i + cj, c) = (p_k i + cj, p_k) = 1$. But as $c$ and $p_k$ are relatively prime and $n = cp_k$, this immediately implies $(p_k i + cj, n) = 1$. Therefore $\zeta_n^{p_k i + cj}$ is a primitive $n$-th root of unity.

Morover, for distinct pairs $(i,j)$, we get distinct primitive $n$-th roots of unity. To see this, suppose the pair $(i_1, j_1)$ is different from $(i_2, j_2)$ (meaning either $i_1 \neq i_2$ or $j_1 \neq j_2$), and that $p_k i_1 + cj_1 \equiv p_k i_2 + cj_2 \bmod n$ (meaning $\zeta_n^{p_k i_1 + cj_1} = \zeta_n^{p_k i_2 + cj_2}$). Reducing modulo $p_k$ and using the fact that $(c, p_k) = 1$ gives $j_1 \equiv j_2 \bmod p_k$. But $1 \leq j_i \leq p_k$ for $i = 1, 2$, which means $j_1 = j_2$. Similarly, reducing the equivalence modulo $c$ and the fact that $1 \leq i_1, i_2 \leq c$ gives $i_1 = i_2$, contradicting the fact the the pairs $(i_1, j_1)$ and $(i_2, j_2)$ were distinct. Therefore we have a set of $\varphi(c)\varphi(p_k)$ primitive $n$-th roots of unity which form a basis for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. But as $\varphi(n) = \varphi(p_k)\varphi(c)$, this implies all primitive $n$-th roots of unity are elements of the basis. Therefore the inductive step is proved and so is the lemma. $\square$

Now we can prove the desired proposition.

**Proposition 3.3.2.** *Suppose $\zeta_n$ is a primitive $n$-th root of unity, where $n$ is squarefree, and consider the field $\mathbb{Q}(\zeta_n)$. Let $G = Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let $H \leq G$ denote any subgroup, and let*

$$\alpha = \sum_{\sigma \in H} \sigma(\zeta_n).$$

*Then the fixed field $\mathbb{Q}(\zeta_n)^H$ is the field $\mathbb{Q}(\alpha)$.*

*Proof.* Suppose $[G : H] = k$, and let $H = eH, g_2H, \ldots, g_kH$ denote the $k$ cosets of $H$ in $G$, and write $H_i = g_iH$, with $H = H_1$. Furthermore, let

$$\alpha_i = \sum_{\sigma_i \in H_i} \sigma_i(\zeta_n).$$

First observe that if $\tau \in H$, then $\tau(\alpha_i) = \alpha_i$, as $\tau$ merely permutes the terms in the sum for $\alpha_i$ (as elements of $H$ will permute the elements of $H_i$, for each $i$). Since $\tau \in H$ was arbitrary, this implies $\alpha_i \in \mathbb{Q}(\zeta_n)^H$ for all $i$.

Next, we claim the $\alpha_i$ are $\mathbb{Q}$-linearly independent. Recall that for all $\sigma \in G$, $\sigma(\zeta_n)$ is another primitive $n$-th root of unity. Moreover, distinct elements of $G$ map $\zeta_n$ to distinct primitive $n$-th roots of unity, and as $\sigma$ runs over all of $G$, we get all primitive $n$-th roots of unity. Since $n$ is assumed to be squarefree, by Lemma 3.3.1 above, the primitive $n$-th roots of unity form a basis for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, so in particular they are linearly independent. So suppose there was a nontrivial dependence relation

$$c_1\alpha_1 + \ldots + c_k\alpha_k = 0,$$

where the $c_i \in \mathbb{Q}$. Then observing that each primitive $n$-th root of unity appears in exactly one of the sums $\alpha_i$, this would yield a nontrivial dependence relation among the primitive $n$-th roots of unity, which is a contradiction. Therefore all the $c_i = 0$ and the $\alpha_i$ are linearly independent. Since $[\mathbb{Q}(\zeta_n)^H : \mathbb{Q}] = k$, this implies that the $\alpha_i$ form a basis for $\mathbb{Q}(\zeta_n)^H/\mathbb{Q}$.

Finally, the observation $\alpha_1 \in \mathbb{Q}(\zeta_n)^H$ clearly means $\mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\zeta_n)^H$. Since $G$ is abelian, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\alpha_1)) \triangleleft G$ is a normal subgroup, so the Fundamental Theorem of Galois Theory implies that $\mathbb{Q}(\alpha_1)$ is Galois over $\mathbb{Q}$, and in particular it is a normal extension. The fact that $\alpha_i = g_i(\alpha_1)$ for $i \geq 2$ says exactly that each of the $\alpha_i$ are roots of the minimal polynomial $m(x) \in \mathbb{Q}[x]$ of $\alpha_1$ over $\mathbb{Q}$. But as $\mathbb{Q}(\alpha_1)$ is normal, this implies $\alpha_i \in \mathbb{Q}(\alpha_1)$ for all $i$. So $\mathbb{Q}(\alpha_1)$ contains each basis element for $\mathbb{Q}(\zeta_n)^H$, and hence $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\zeta_n)^H$, which is what we wanted to prove. □

Let us apply this proposition to the two examples we have been examining throughout this chapter, namely $G = \mathbb{Z}/4\mathbb{Z}$ and $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**Example 3.3.3.** $G = \mathbb{Z}/4\mathbb{Z}$: Our totally real extension is $K = \mathbb{Q}(\zeta_{17})^H$, where $H \leq (\mathbb{Z}/17\mathbb{Z})^\times$ is the subgroup $H = \{1, 4, 13, 16\}$ (see Example 3.2.15). Of course, we could also identify $H$ with a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q})$ by writing

$$H = \{\sigma_k : k = 1, 4, 13, 16\},$$

where $\sigma_k : \zeta_n \mapsto \zeta_n^k$. Proposition 3.3.2 tells us that if

$$\alpha = \sum_{\sigma \in H} \sigma(\zeta_{17}),$$

then $K = \mathbb{Q}(\alpha)$. Using our description of $H$, we find

$$\alpha = \zeta_{17} + \zeta_{17}^4 + \zeta_{17}^{13} + \zeta_{17}^{16}.$$

The minimal polynomial of $\alpha$ over $\mathbb{Q}$ can be found via SAGE or Mathematica and is

$$m_\alpha(x) = x^4 + x^3 - 6x^2 - x + 1.$$

By the arguments preceding Lemma 3.3.1, we find $m_\alpha(x)$ has splitting field $K$ and Galois group $G = \mathbb{Z}/4\mathbb{Z}$.

**Example 3.3.4.** $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: Here our extension is $K = \mathbb{Q}(\zeta_{65})^H$, where $H \leq (\mathbb{Z}/65\mathbb{Z})^\times$ is the subgroup

$$H = \{1, 4, 9, 14, 16, 29, 36, 49, 51, 56, 61, 64\}.$$

Therefore the element $\alpha$ from Proposition 3.3.2 is

$$\alpha = \sum_{k \in H} \zeta_{65}^k.$$

Again using either SAGE or Mathematica, one can verify that the minimal polynomial over $\mathbb{Q}$ is

$$m_\alpha(x) = x^4 - x^3 - 10x^2 - 3x + 9.$$

Therefore $m_\alpha(x)$ has splitting field $K$ and Galois group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Those who really wanted to check this result could use SAGE to calculate the Galois group. For instance, the examples above could be checked as follows:

```
sage: K.<a> = NumberField(x^4 +x^3-6*x^2-x+1)
sage: G = K.galois_group(type = ''pari''); G
Galois group PARI group [4, -1, 1, ''C(4) = 4 ''] of degree
4 of the Number Field in a with defining polynomial
x^4 + x^3 - 6*x^2 - x + 1

sage: L.<b> = NumberField(x^4 - x^3 - 10*x^2 - 3*x + 9)
sage: H = L.galois_group(type = ''pari''); H
Galois group PARI group [4, 1, 2, ''E(4) = 2[x]2 ''] of
degree 4 of the Number Field in b with defining polynomial
x^4 - x^3 - 10*x^2 - 3*x + 9
```

Using this method and SAGE, we found polynomials with abelian Galois group $G$ for all abelian groups up to order 20, with the exception of one group. In addition, we calculated the ramified primes and the primes which split completely, again with the help of SAGE. Of course, one could use this method to find polynomials with bigger abelian Galois group. For complete tables, see Appendix D.

## 3.4 Splitting of primes 2 and 5 in $\mathbb{Z}/3\mathbb{Z}$-extensions

### 3.4.1 Motivation

The final two sections of this chapter will be devoted to the following question. Given two (finite) primes $p$ and $q$ of $\mathbb{Z}$, does $p$ split completely in infinitely many totally real $\mathbb{Z}/q\mathbb{Z}$ extensions? Of course, we will still use the totally real extensions we have been investigating the last few sections. This particular section will consider the cases $p = 2, 5$ and $q = 3$. The results require cubic reciprocity, so the cubic character will be the first topic of this section.

We are considering the case $G = \mathbb{Z}/3\mathbb{Z}$. As always, first choose a prime $p$ such that $p \equiv 1 \bmod 6$, and then the desired totally real number field is $K = \mathbb{Q}(\zeta_p)^H$, where $H$ is the unique subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ of order $\frac{p-1}{3}$. By Theorem 3.2.11 and the other notes in Section 3.2.3, the primes which split completely in $K$ are those primes $q$ such that $q \bmod p \in H$.

By making the usual identification $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, the subgroup $H$ is

$$H = \left\{a \in (\mathbb{Z}/p\mathbb{Z})^\times : a^{(p-1)/3} \equiv 1 \bmod p\right\}.$$

For 2 to split completely in $K$, Theorem 3.2.11 says $2^{(p-1)/3} \equiv 1 \bmod p$. What the next lemma shows is that this happens precisely when 2 is a cube modulo $p$. Note that the proof is adapted from [14], Section 1.3.

**Lemma 3.4.1.** *Let $p$ be a prime such that $p \equiv 1$ mod 3. Then an element $x \in \mathbb{F}_p^\times$ is a cube if and only if $x^{(p-1)/3} = 1$.*

*Proof.* Choose $\Omega$ to be an algebraic closure of $\mathbb{F}_p$. For $x \in \mathbb{F}_p^\times$, we can certainly choose $y \in \Omega$ with $y^3 = x$ (as $\Omega$ is an algebraic closure, the polynomial $t^3 - x \in \mathbb{F}_p[t]$ has a root in $\Omega$). Suppose first that $y \in \mathbb{F}_p$ (i.e. $x$ is a cube), then as $|\mathbb{F}_p^\times| = p - 1$, certainly

$$y^{p-1} = 1.$$

But

$$y^{p-1} = x^{(p-1)/3},$$

so $x^{(p-1)/3} = 1$. Conversely, if $x^{(p-1)/3} = 1$, then $y^{p-1} = 1$. But this implies $y \in \mathbb{F}_p$ as elements of $\mathbb{F}_p$ are the roots of the equation $t^p - t \in \mathbb{F}_p[t]$. Therefore $x$ is a cube modulo in $\mathbb{F}_p$. □

Therefore, to check whether 2 (or 5) splits completely in $K$, it is sufficient to check whether 2 (or 5) is a cube modulo $p$ ($\mathbb{Z}/p\mathbb{Z}$ is isomorphic to $\mathbb{F}_p$). This should, at least, provide some insight as to why we want to introduce the cubic character.

### 3.4.2 Cubic Character

The goal of this section is to state the cubic reciprocity law. The proof is not presented as it is not part of the scope of this thesis. The proof can be found in [15], and the definitions and theorems will mainly come from here. Most of the required machinery has already been developed at various points in this thesis, so the cubic character will come rather easily. The majority of the work is just a matter of putting the various results together and applying it to one specific number field.

The cubic character and cubic reciprocity law focus on the cyclotomic field $K = \mathbb{Q}(\zeta_3)$. In an effort to stick to standard notation, write $\omega = \zeta_3$, so $\omega$ is a primitive cube root of unity and $K = \mathbb{Q}(\omega)$. Of course, $\omega$ is a root of the polynomial $x^2 + x + 1 \in \mathbb{Q}[x]$ (Eisenstein for $x+1$ instead of $x$), and so alternatively we could write $K = \mathbb{Q}(\sqrt{-3})$. However, we mainly use $K = \mathbb{Q}(\omega)$. By Theorem 2.3.6, the ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$.

The ring $\mathcal{O}_K = \mathbb{Z}[\omega]$ is a Euclidean domain, with Euclidean function given by the norm inherited from $\mathbb{C}$ (this does not always lead to a Euclidean function, but it does in this case). Moreover, this norm agrees with the norm function on the number field $K$, which was introduced in Chapter 2. Here

$$\mathrm{Norm}_{K/\mathbb{Q}}(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2.$$

Since $\mathcal{O}_K$ is Euclidean, it is a UFD.

**Units**: We need the units of $\mathcal{O}_K$. In this instance, it is more helpful to write $K = \mathbb{Q}(\sqrt{-3})$. Instead of writing elements of $\mathcal{O}_K$ as $a + b\omega$, they are written as $a + b\sqrt{-3}$, where $a$ and $b$ are allowed to be half-integers because $\mathcal{O}_K = \mathbb{Z}[\omega] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. By Proposition 2.3.11, the units of $\mathcal{O}_K$ are precisely those $\alpha \in \mathcal{O}_K$ with $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1$. In this case, $\mathrm{Norm}_{K/\mathbb{Q}}(a + b\sqrt{-3}) = a^2 + 3b^2$. Since we have to allow half-integers, let $a' = 2a$, $b' = 2b$, so that both $a', b' \in \mathbb{Z}$. Then the equation $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1$ becomes

$$a'^2 + 3b'^2 = \pm 4,$$

where $a', b' \in \mathbb{Z}$. This clearly only has 6 solutions $(a', b')$:

$$(\pm 2, 0), \quad (\pm 1, \pm 1).$$

Since $a' = 2a$, $b' = 2b$, these correspond to the elements

$$\pm 1, \frac{-1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}.$$

Recalling that $\omega = \frac{-1+\sqrt{-3}}{2}$,

$$\mathcal{O}_K^\times = \{\pm 1, \pm\omega, \pm\omega^2\},$$

and these are all the units of $\mathcal{O}_K$.

**Factoring Primes**: Now consider a prime $p$ of $\mathbb{Z}$, and factor $p\mathcal{O}_K$ into a product of prime ideals. By Theorem 2.3.58, the only prime which ramifies in $K$ is 3. The Dedekind-Kummer Theorem 2.3.49 will aid in the factorization. We need to factor the minimal polynomial of $\omega$, namely $x^2+x+1 \in \mathbb{Q}[x]$, modulo 3. We find

$$x^2 + x + 1 \equiv x^2 - 2x + 1 \equiv (x-1)^2 \bmod 3.$$

Therefore

$$3\mathcal{O}_K = (3, -1+\omega)^2 = \mathfrak{p}^2.$$

Hence $e(\mathfrak{p}/3) = 2$, and as $K/\mathbb{Q}$ is a Galois extension, Theorem 2.3.48 implies $f(\mathfrak{p}/3) = 1$. Since $\mathcal{O}_K$ is a PID (as it is Euclidean), $\mathfrak{p}$ has a single generator. Clearly $1-\omega \in \mathfrak{p}$, and so $(1-\omega) \subseteq \mathfrak{p}$. By definition of the norm of an ideal, $N_{K/\mathbb{Q}}(\mathfrak{p}) = 3^1 = 3$. However, by Proposition 2.3.41,

$$N_{K/\mathbb{Q}}((1-\omega)) = |\mathrm{Norm}_{K/\mathbb{Q}}(1-\omega)| = 3.$$

This implies that $(1-\omega) = \mathfrak{p}$ as they both have the same norm, and hence the same index in $\mathcal{O}_K$ by Proposition 2.3.40. Therefore

$$(3) = (1-\omega)^2 = ((1-\omega)^2),$$

meaning 3 and $(1-\omega)^2$ differ by a unit, and it is readily checked that the unit is $-\omega^2$.

The results of the last few sections help describe the primes which split and stay inert. It is a good exercise for the reader to verify that the primes which split in $K$ are those such that $p \equiv 1 \bmod 3$ and the primes which are inert in $K$ are those $p$ such that $p \equiv 2 \bmod 3$.

**Primary Associates**: Recall that in a ring $R$, elements $r, s \in R$ are said to be left-associates if there exists a unit $u \in R$ such that $r = us$. As $\mathcal{O}_K = \mathbb{Z}[\omega]$ is

a commutative ring, left-associates can just be called associates. Ultimately, the desired irreducible elements of $\mathcal{O}_K$ will be those $\pi$ such that $\pi \equiv 2 \bmod 3$. That is, when writing $\pi = a + b\omega$, $a \equiv 2 \bmod 3$ and $b \equiv 0 \bmod 3$.

Now, if $\pi \in \mathcal{O}_K$ is irreducible, then $\mathfrak{P} = (\pi)$ is a prime ideal (as $\pi$ is a prime element in this PID), and so $\mathfrak{P}$ lies above some prime $p$ of $\mathbb{Z}$. Therefore $\pi | p$ for some (unique) rational prime $p$. We have the following lemma.

**Lemma 3.4.2.** *Let $p \neq 3$ be a prime of $\mathbb{Z}$. Then every divisor $\pi$ of $p$ has a unique associate $\pi'$ such that $\pi' \equiv 2 \bmod 3$.*

Such an associate is called the *primary associate* of $\pi$, and a prime $\pi \equiv 2 \bmod 3$ is called a *primary prime*. This lemma is not hard and the proof is just a matter of checking each of the six associates of $\pi$, so we will not prove it.

However, what this lemma does show is that for every rational prime $p \neq 3$, there must be a primary prime dividing $p$. Indeed, if $p \equiv 2 \bmod 3$, then $p$ remains prime in $\mathcal{O}_K$ and hence is a primary prime dividing $p$. If $p \equiv 1 \bmod 3$, then $p\mathcal{O}_K$ factors into two distinct prime ideals, and hence we can find two irreducible divisors of $p$, say $\pi_1$ and $\pi_2$. By Lemma 3.4.2, each of the $\pi_i$ has an associate which is a primary prime in $\mathcal{O}_K$, and hence will be a primary prime dividing $p$.

What is of greater use to us is the method to find a primary prime dividing a prime $p \neq 3$. If $p \equiv 2 \bmod 3$, then $p$ is prime as $p$ stays inert in $K$, and so it is a primary prime. So suppose $p \equiv 1 \bmod 3$, and let $\pi | p$ be a primary prime dividing $p$, which must exist by the above arguments. Then as $(\pi)$ is a prime ideal dividing $p\mathcal{O}_K$ and $p\mathcal{O}_K$ splits into two distinct prime ideals, $(\pi)$ must be one of the primes above $p$. Hence

$$N_{K/\mathbb{Q}}((\pi)) = |\mathrm{Norm}_{K/\mathbb{Q}}(\pi)| = p.$$

We want to be able to write $\pi = a + b\omega$ where $a \equiv 2, b \equiv 0 \bmod 3$. Using the formula for $\mathrm{Norm}_{K/\mathbb{Q}}(\pi)$, we find

$$a^2 - ab + b^2 = p.$$

Multiplying both sides by 4 and completing the square shows

$$4p = (2a - b)^2 + 3b^2.$$

Let $A = 2a - b$ and $B = b/3$, where the latter is possible since $3|b$. Then this becomes

$$4p = A^2 + 27B^2.$$

As a quick aside: from this it is easy to observe that $A$ and $B$ must have the same parity (take equivalences modulo 2). This will be useful later.

Since solutions $a, b \in \mathbb{Z}$ must exist, solutions $A$ and $B$ exist. Pick $A$ so that $A \equiv 1 \bmod 3$. To see that this is possible, first notice that $A$ cannot be 0 modulo 3 since the left side of

$$4p = A^2 + 27B^2$$

is not divisible by 3. Then if $(A, B)$ is a solution, then $(-A, B)$ is a solution, and one of $A, -A \equiv 1 \bmod 3$ since $A \not\equiv 0 \bmod 3$. After finding such $A$ and $B$, let

$$b = 3B, \quad a = \frac{A + b}{2}.$$

Then this is a primary prime dividing $p$. Note that this primary prime is not unique, as there are two possibilities for $B$ (as both $(A, B)$ and $(A, -B)$ could be solutions).

**Cubic Character**: Suppose $\pi \in \mathcal{O}_K$ is a primary prime, $\pi \neq 1 - \omega$. Then the ideal $\pi\mathcal{O}_K$ is a prime ideal, and there is a unique prime $p$ of $\mathbb{Z}$ lying below $\pi$. For an element $\alpha \in \mathcal{O}_K$, let $N(\alpha)$ (or $N\alpha$) be $N_{K/\mathbb{Q}}((\alpha))$. Then if $p \equiv 1 \bmod 3$, then

$$N\pi = p \equiv 1 \bmod 3,$$

and if $p \equiv 2 \bmod 3$, then $\pi = p$ and

$$N\pi = p^2 \equiv 1 \bmod 3.$$

In both cases, $N\pi \equiv 1 \bmod 3$. But $\mathcal{O}_K/\pi\mathcal{O}_K$ is a finite field of dimension $f((\pi)/p)$ over $\mathbb{F}_p$. So in particular, $\mathcal{O}_K/\pi\mathcal{O}_K$ is a field of $p^{f((\pi)/p)} = N\pi$ elements, and so $(\mathcal{O}_K/\pi\mathcal{O}_K)^\times$ is cyclic of order $N\pi - 1$. Since $3|N\pi - 1$, there are 3 elements of order dividing 3 in $(\mathcal{O}_K/\pi\mathcal{O}_K)^\times$. Three possible elements are $1 + \pi\mathcal{O}_K, \omega + \pi\mathcal{O}_K, \omega^2 + \pi\mathcal{O}_K$. To show that these are precisely the three we want, we need to make sure $1, \omega, \omega^2$ are inequivalent modulo $\pi$. But this is clear as $1 - \omega, \omega - \omega^2 = \omega(1 - \omega), 1 - \omega^2 = -\omega^2(1 - \omega)$ are all associates of $1 - \omega$, which is the irreducible element dividing 3 (see above), and hence these three differences cannot be divisible by $\pi$. Therefore these are the three roots of unity in $(\mathcal{O}_K/\pi\mathcal{O}_K)^\times$. If $\alpha \in (\mathcal{O}_K/\pi\mathcal{O}_K)^\times$, then

$$\alpha^{N\pi - 1} \equiv 1 \bmod \pi,$$

and therefore

$$\alpha^{(N\pi-1)/3} \equiv 1, \omega, \text{ or } \omega^2 \bmod \pi.$$

So we can define our cubic character as follows.

**Definition 3.4.3.** Suppose $\pi$ is a primary prime (and $\pi \neq 1 - \omega$). Then the cubic character modulo $\pi$,

$$\chi_\pi : (\mathcal{O}_K/\pi\mathcal{O}_K)^\times \to \{1 + \pi\mathcal{O}_K, \omega + \pi\mathcal{O}_K, \omega^2 + \pi\mathcal{O}_K\},$$

is defined by

$$\chi_\pi(\alpha) = \alpha^{(N\pi-1)/3} \bmod \pi.$$

From the way it is defined, it is easy to see that $\chi_\pi$ is a homomorphism. The other statement we want to prove is that $\chi_\pi(\alpha) = 1$ if and only if $\alpha$ is a cube modulo $\pi$. This is what the next proposition gives us.

**Proposition 3.4.4.** *$\chi_\pi(\alpha) = 1$ if and only if $\alpha$ is a cube in $(\mathcal{O}_K/\pi\mathcal{O}_K)^\times$.*

*Proof.* Since $(\mathcal{O}_K/\pi\mathcal{O}_K)^\times$ is cyclic, choose a generator $\gamma$. So $\gamma$ has order $N\pi - 1$ in $(\mathcal{O}_K/\pi\mathcal{O}_K)^\times$. Choose $\alpha \in (\mathcal{O}_K/\pi\mathcal{O}_K)^\times$ and write $\alpha = \gamma^c$. Then

$$\chi_\pi(\alpha) = 1 \iff \alpha^{(N\pi-1)/3} = 1 \iff g^{c(N\pi-1)/3} \iff c(N\pi-1)/3 | N\pi - 1 \iff 3|c.$$

Therefore the character gives a value of one precisely when $\alpha$ is a cube modulo $\pi$ (it is the cube of $\gamma^{c/3}$). □

And now we can state the law of cubic reciprocity.

**Theorem 3.4.5.** *Let $\pi$ and $\pi'$ be primary primes lying above different primes $p$ and $p'$, neither of which is 3. Then*

$$\chi_\pi(\pi') = \chi_{\pi'}(\pi).$$

### 3.4.3 Proof that 2 and 5 split in infinitely many $\mathbb{Z}/3\mathbb{Z}$ extensions

Having stated the law of cubic reciprocity, we can now prove that 2 and 5 split in infinitely many $\mathbb{Z}/3\mathbb{Z}$ extensions. Recall the idea in Section 3.4.1. First, we choose a prime $p \equiv 1 \bmod 6$, and then consider our totally real number field $K = \mathbb{Q}(\zeta_n)^H$, where $H$ is the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order $(p-1)/3$. Throughout this section, we make use of this selected prime $p$ and the associated field $K$. We noted, using the results from Section 3.2.3, that 2 (resp. 5) splits in $K$ if and only if $2 \in H$ (resp. $5 \in H$). This, in turn, happens if and only if 2 (resp 5) satisfied $2^{(p-1)/3} \equiv 1 \bmod p$ (and similarly for 5), which, by Lemma 3.4.1, occurs precisely when 2 (resp 5) is a cube mod $p$. But now we have the tools necessary to determine when this happens, namely the cubic character and the law of cubic reciprocity.

**Proposition 3.4.6.** *The prime 2 splits completely in $K$ if and only if our chosen prime $p$ has the form $p = a^2 + 27b^2$ for some $a, b \in \mathbb{Z}$.*

*Proof.* Let $L = \mathbb{Q}(\omega)$, so $\mathcal{O}_L = \mathbb{Z}[\omega]$. Since $p \equiv 1 \bmod 3$ (in fact, 1 mod 6), we can find a primary prime $\pi$ of $\mathcal{O}_L$ dividing $p$ using the method outlined in the previous section. Namely, write $4p = A^2 + 27B^2$ and choose a solution so that $A \equiv 1 \bmod 3$, and then

$$\pi = \frac{A + 3B}{2} + 3B\omega$$

is a primary prime dividing $p$. Let $k = \frac{A+3B}{2}$. First, observe that $A$ and $B$ must have the same parity, which is seen by reducing both sides of $4p = A^2 + 27B^2$ modulo 2. Second, note that we cannot have both $k$ and $B$ be even. To see this, notice that $N\pi = p$, and so

$$|\mathrm{Norm}_{K/\mathbb{Q}}(\pi)| = N\pi = p \implies \mathrm{Norm}_{K/\mathbb{Q}}(\pi) = \pm p.$$

But as

$$\mathrm{Norm}_{K/\mathbb{Q}}(\pi) = k^2 - k(3B) + (3B^2) = \pm p,$$

if both $k$ and $B$ are even, reducing modulo 2 gives a contradiction (as $p$ is necessarily odd being 1 mod 6). Therefore $k$ and $B$ cannot both be even.

Since $p$ splits completely and $\pi|p$, $f((\pi)/p) = 1$ and we have an isomorphism $\mathcal{O}_K/\pi\mathcal{O}_K \cong \mathbb{Z}/p\mathbb{Z}$. Hence checking whether 2 is a cube modulo $p$ (when regarded as elements of $\mathbb{Z}$) is the same as checking whether 2 is a cube modulo $\pi$, when regarded as elements of $\mathcal{O}_K$. So we want $\chi_\pi(2) = 1$. As both $\pi$ and 2 are primary primes and $\pi \neq 2$, cubic reciprocity says

$$\chi_\pi(2) = \chi_2(\pi) = \chi_2(k + 3B\omega).$$

If $B$ is even, then $k$ is odd, and $\chi_2(k + 3B\omega) = \chi_2(1) = 1$, which means 2 is a cube modulo $\pi$. So now suppose $B$ is odd. Then $k$ may be either even or odd. If $k$ is even, then

$$\begin{aligned}
\chi_2(\pi) &= \chi_2(k + 3B\omega) \\
&= \chi_2(\omega) \quad (\text{as } k \text{ is even and } B \text{ is odd}) \\
&= \omega^{(N(2)-1)/3} \quad (\text{by definition of the cubic character}) \\
&= \omega^{(4-1)/3} \\
&= \omega,
\end{aligned}$$

which means 2 will not be a cube modulo $\pi$. Similarly, if $k$ is odd, then

$$\begin{aligned}
\chi_2(\pi) &= \chi_2(k + 3B\omega) \\
&= \chi_2(1 + \omega) \quad (\text{as } k \text{ and } B \text{ are odd}) \\
&= \chi_2(-\omega^2) \\
&= \chi_2(\omega^2) \quad (\text{as } -1 \text{ is certainly a cube modulo 2}) \\
&= \chi_2(\omega)\chi_2(\omega) \\
&= \omega^2.
\end{aligned}$$

Therefore, in both cases, 2 will not be a cube modulo $\pi$, and hence not a cube modulo $p$. Therefore 2 is a cube modulo $p$ if and only if $B$ is even. Since $A$ and $B$ have the same parity, $A$ must be even. So write $A = 2a$, $B = 2b$ for integers $a, b$. The condition $4p = A^2 + 27B^2$ implies $p = a^2 + 27b^2$. Therefore 2 splits in $K$ if and only if $p$ has the form $p = a^2 + 27b^2$ for $a, b \in \mathbb{Z}$, which is what we wanted to show. □

This proposition is particularly nice because it gives a necessary and sufficient condition for 2 to split completely in $K$. Let us briefly illustrate this idea. Our chosen prime must be 1 mod 6, and so the first few choices are $7, 13, 19$, and 31. If we consider the corresponding totally real $\mathbb{Z}/3\mathbb{Z}$-extensions $K$, this proposition tells us that 2 will not split completely in the first three but will in the fourth, as $31 = 2^2 + 27 \cdot 1^2$, and the first three primes cannot be written in this way.

Before showing that there are infinitely many such primes, let us prove a similar proposition for the prime 5.

**Proposition 3.4.7.** *The prime* 5 *will split completely in* $K$ *if, when writing* $4p = A^2 + 27B^2$*, at least one of* $A, B \equiv 0$ *mod* 5*.*

*Remark* 3.4.8. The reader will notice that this proposition is, in some sense, weaker than Proposition 3.4.6 because it only provides a sufficient condition; it is not an "if and only if". It turns out that converse is true, but we will not prove that.

*Proof.* Let $L = \mathbb{Q}(\omega)$, so $\mathcal{O}_L = \mathbb{Z}[\omega]$. As in the proof of Proposition 3.4.6, we write $4p = A^2 + 27B^2$, where $A \equiv 1 \bmod 3$, and a primary prime dividing $p$ is

$$\pi = \frac{A + 3B}{2} + 3B\omega.$$

Write $k = \frac{A+3B}{2}$. Again, we have an isomorphism $\mathcal{O}_L/\pi\mathcal{O}_L \cong \mathbb{Z}/p\mathbb{Z}$, so that to check whether 5 is a cube modulo $p$ it is enough to see whether 5 is a cube modulo $\pi$. Cubic reciprocity says that $\chi_\pi(5) = \chi_5(\pi) = \chi_5(k + 3B\omega)$.

If $B \equiv 0 \bmod 5$, then

$$\chi_5(k + 3B\omega) = \chi_5(k).$$

Since $k \in \mathbb{Z}$, we find $\chi_5(k) = 1$ since every element modulo 5 is a cube (i.e. $x \mapsto x^3$ is an automorphism of $\mathbb{Z}/5\mathbb{Z}$).

In the case $A \equiv 0 \bmod 5$, slightly more work is needed. If $B$ is also 0 mod 5, then the previous case holds. So assume $B$ is not divisible by 5. First, observe that, modulo 5,

$$k \equiv 3A + 9B$$

since the inverse of 2 modulo 5 is 3. Therefore we can say

$$\chi_5(k+3B\omega) = \chi_5(3A+9B+3B\omega) = \chi_5(3)\chi_5(A+3B+B\omega) = \chi_5(A+3B+B\omega)$$

as $\chi_5(3) = 1$ by the earlier argument. But $A \equiv 0 \bmod 5$, so

$$\chi_5(A+3B+B\omega) = \chi_5(3B+B\omega) = \chi_5(B(3+\omega)) = \chi_5(B)\chi_5(3+\omega) = \chi_5(3+\omega),$$

as $\chi_5(B) = 1$ since, again, every element in $\mathbb{Z}/5\mathbb{Z}$ is a cube. Next, we want to find the unique primary associate of $3+\omega$, which exists by Lemma 3.4.2. We observe that $-\omega^2(3+\omega) = 2+3\omega$, which is a primary associate. Therefore

$$\begin{aligned}
\chi_5(3+\omega) &= \chi_5(-\omega^2)^{-1}\chi_5(2+3\omega) \\
&= (\omega^{2(N(5)-1)/3})^{-1}\chi_5(2+3\omega) \quad \text{(definition of cubic character)} \\
&= (\omega^{2(25-1)/3})^{-1}\chi_5(2+3\omega) \quad \text{(as the ideal (5) is prime in } \mathcal{O}_K) \\
&= \omega^2\chi_5(2+3\omega).
\end{aligned}$$

Again using cubic reciprocity,

$$\omega^2\chi_5(2+3\omega) = \omega^2\chi_{2+3\omega}(5).$$

A simple calculation will show that

$$5 - (2+3\omega)(1+2\omega^2) = 1+\omega = -\omega^2,$$

meaning $5 \equiv -\omega^2 \bmod (2+3\omega)$. Therefore

$$\begin{aligned}
\omega^2\chi_{2+3\omega}(5) &= \omega^2\chi_{2+3\omega}(-\omega^2) \\
&= \omega^2\chi_{2+3\omega}(\omega^2) \quad (\text{as } \chi_{2+3\omega}(-1) = 1) \\
&= \omega^2(\omega^{2(N(2+3\omega)-1)/3}) \quad \text{(by definition)} \\
&= \omega^2(\omega^{2(7-1)/3}) \\
&= \omega^2 \cdot \omega \\
&= 1,
\end{aligned}$$

which proves that 5 is a cube modulo $p$ in this case as well. Therefore 5 is a cube modulo $p$ when one of $A, B \equiv 0 \bmod 5$. □

To get that 2 and 5 split completely in *infinitely many* totally real $\mathbb{Z}/3\mathbb{Z}$-extensions, we just need the following theorem.

**Theorem 3.4.9.** *Suppose $ax^2+bxy+cy^2$ is a quadratic form, where $a, b, c \in \mathbb{Z}$ with $gcd(a,b,c) = 1$. Suppose the discriminant $D = b^2-4ac < 0$, and let $S$ denote the set*

$$S = \{p \text{ prime} : p = ax^2+bxy+cy^2 \text{ for some } x, y \in \mathbb{Z}\}.$$

*Then the Dirichlet density $\delta(S)$ exists and is positive.*

A proof of this theorem can be found in [8]. As an immediate consequence of this, we get the proposition we want.

**Proposition 3.4.10.** *Both 2 and 5 split in infinitely many $\mathbb{Z}/3\mathbb{Z}$ extensions.*

*Remark* 3.4.11. Just for clarification, we do not assert that they split simultaneously. The prime 2 will split in infinitely many and the prime 5 will split completely in infinitely many extensions.

*Proof.* Proposition 3.4.6 shows 2 splits completely in $K$ precisely when the chosen prime $p = a^2+27b^2$ for $a, b \in \mathbb{Z}$. By Theorem 3.4.9, there are infinitely many such primes, which means there are infinitely many such extensions $K$ in which 2 splits completely. Since $K$ is a totally real $\mathbb{Z}/3\mathbb{Z}$ extension, this proves the proposition for the prime 2.

For 5, Proposition 3.4.7 says that 5 will split completely in $K$ if $4p = 25a^2 + 27b^2$ or $4p = a^2 + 255b^2$ (i.e. when either $A$ or $B$ is divisible by 5 in the decomposition $4p = A^2 + 27B^2$). If we restrict to when both $a$ and $b$ are even, we get $p = 25a'^2 + 27b'^2$ or $p = a'^2 + 255b'^2$, where $a' = 2a$ and $b' = 2b$. By Theorem 3.4.9, there are infinitely many such primes for each decomposition, leading to infinitely many totally real $\mathbb{Z}/3\mathbb{Z}$ extensions in which 5 splits completely. □

## 3.5 Splitting of $p$ in $\mathbb{Z}/q\mathbb{Z}$-extensions

The phenomenon encountered in the previous section is not specific to $\mathbb{Z}/3\mathbb{Z}$ extensions or to the two specific primes 2 and 5. For any primes $p, q$, the prime $p$ will split in infinitely many totally real $\mathbb{Z}/q\mathbb{Z}$ extensions. We have all the results needed to prove this.

**Lemma 3.5.1.** *For any two totally real, linearly disjoint $\mathbb{Z}/q\mathbb{Z}$ extensions in which $p$ is unramified and does not split completely, there exists a subfield of the compositum in which it does split completely. Moreover, this extension is a totally real $\mathbb{Z}/q\mathbb{Z}$ extension of $\mathbb{Q}$.*

*Proof.* Suppose $K_1$ and $K_2$ the two extensions in the statement of the lemma (i.e. $p$ is unramified in $K_1$ and $K_2$ but does not split completely), and consider the compositum $K = K_1K_2$. As $K_1$ and $K_2$ are linearly disjoint, $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/q\mathbb{Z}\times \mathbb{Z}/q\mathbb{Z}$. Let $\mathfrak{P}$ be a prime of $\mathcal{O}_K$ lying above $p$, and consider the decomposition group $D = D(\mathfrak{P}/p)$. If $|D| = 1$, then $p$ splits completely in $K$, and hence splits completely in $K_1$ and $K_2$ by Lemma 3.2.2, a contradiction. Therefore $|D| = q$ or $|D| = q^2$ as $D \leq \mathrm{Gal}(K/\mathbb{Q})$. However, as $p$ is unramified in $K_1$ and $K_2$, it is unramified in $K$ by Lemma 3.2.2, and hence we have an isomorphism

$$D \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p),$$

where $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$ and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In particular, $D$ is cyclic, and so $|D| \neq q^2$ as there is clearly no cyclic subgroup of order $q^2$ in $\mathbb{Z}/q\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$. Therefore $|D| = q$. If we consider $L = K^D$, this will be a totally real extension (totally real since $K$ is totally real), and $p$ will split completely in $L$ by Proposition 2.3.73. Moroever, $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/q\mathbb{Z}$ as $\mathrm{Gal}(L/\mathbb{Q})$ is an abelian group of order $q$, and $q$ is prime. □

**Proposition 3.5.2.** *For any two primes $p$ and $q$, $p$ splits in infinitely many totally real $\mathbb{Z}/q\mathbb{Z}$-extensions.*

*Proof.* Let $\{r_i\}$ be the set of all primes $\equiv 1 \bmod 2q$. Theorem 3.1.11 and Corollary 3.2.6 say that for each $r_i$ there is a totally real $\mathbb{Z}/q\mathbb{Z}$ extension of $\mathbb{Q}$, say $K_i$, in which only $r_i$ ramifies. If $p$ split completely in only finitely many of these $K_i$, then there would clearly be infinitely many in which it did not split completely. Since each $K_i$ is a subfield of $\mathbb{Q}(\zeta_{r_i})$, $K_i \cap K_j = \mathbb{Q}$ by Lemma 3.1.6. Moreover, $p$ can ramify in at most one of these $K_i$ because each of the primes $r_i$ is distinct. Therefore, there are infinitely many $K_i$ in which $p$ is unramified and $p$ does not split completely. For any two of them, Lemma 3.5.1 says we can construct a totally real $\mathbb{Z}/q\mathbb{Z}$ extension in which $p$ does split completely, and it is realized as a subfield of the composite extension. We could therefore do this with all distinct pairs of extensions in which $p$ does not split completely to get infinitely many new extensions in which it does. □

# Chapter 4

# Symmetric Groups

We now shift gears and move on to the second class of groups: the symmetric groups $S_n$. We will need to develop more background material in order to present the proof of the existence of a totally real number field with Galois group $S_n$.

## 4.1 Additional Background Material

### 4.1.1 $p$-adic Numbers

#### $p$-adic Valuation

At the heart of both the desired results are the $p$-adic numbers. Presumably, at some point, the reader has seen the construction of $\mathbb{R}$ as a completion of $\mathbb{Q}$. Namely, we consider the usual *metric* on $\mathbb{Q}$, given by the normal absolute value on $\mathbb{R}$,

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}.$$

Then we form special sequences of rational numbers, called *Cauchy sequences*:

**Definition 4.1.1.** A sequence $\{x_n\}$ of rational numbers is called a *Cauchy sequence* if for all $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, there exists $N$ such that for all $m, n > N$,

$$|x_n - x_m| < \epsilon.$$

One then obtains $\mathbb{R}$ by taking equivalence classes of Cauchy sequences of rational numbers, where two Cauchy sequences $\{a_n\}$ and $\{b_n\}$ are equivalent if the sequence $\{a_n - b_n\}$ converges to zero. Then one shows that $\mathbb{R}$ is complete and the desired operations hold, which means the resulting complete field is actually $\mathbb{R}$.

The reader will observe that definition 4.1.1 is heavily dependent on the metric on $\mathbb{Q}$ given by the absolute value $|\cdot|$. It is this metric which defines when two numbers are "close together." Changing the metric could change the resulting

completion. But then two natural questions arise: are there any other metrics on $\mathbb{Q}$, and what do the resulting completions look like? The $p$-adics are formed by considering different metrics on $\mathbb{Q}$ and then completing $\mathbb{Q}$ in the same manner as we do to obtain $\mathbb{R}$.

It turns out that there are infinitely many *inequivalent* metrics, or absolute values, we can place on $\mathbb{Q}$. First, let us make the definition of absolute value precise. This definition comes from [3].

**Definition 4.1.2.** An *absolute value* on $\mathbb{Q}$ is a function $|\cdot| : \mathbb{Q} \to \mathbb{R}_{\geq 0}$, such that

(i) $|x| = 0$ if and only if $x = 0$,

(ii) $|xy| = |x||y|$ for all $x, y \in \mathbb{Q}$,

(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in \mathbb{Q}$.

An absolute value which, in addition, satisfies the inequality

(iii') $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in \mathbb{Q}$,

is known as a *non-Archimedean* absolute value.

*Remark* 4.1.3. At this point, it is worth noting that many of the definitions and results we use can be generalized to arbitrary number fields, and in fact this is the way they appear in many algebraic number theory texts. However, as we will only be needing the completion of $\mathbb{Q}$ and not other fields, we will only be presenting results for $\mathbb{Q}$.

The reader will note that (iii') clearly implies (iii), so (iii') is a stronger condition. Absolute values which do not satify (iii') (but do satisfy (iii)) are called *Archimedean*.

Any absolute value on $\mathbb{Q}$ gives rise to a metric function in the obvious way: we let the distance between $x, y \in \mathbb{Q}$ be $d(x, y) = |x - y|$. From this, we can say that two absolute values are *equivalent* if they induce the same metric topology on $\mathbb{Q}$. However, we will use the following definition, and the equivalence is proved in [9].

**Definition 4.1.4.** Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on $\mathbb{Q}$ are *equivalent* if $|x|_1 < 1$ holds if and only if $|x|_2 < 1$ (for any $x \in \mathbb{Q}$).

One can prove that the only Archimedean absolute value on $\mathbb{Q}$, up to equivalence, is the metric given by the usual absolute value on $\mathbb{Q}$. So now let us build some non-Archimedean absolute values.

Fix a prime number $p$. For $0 \neq x \in \mathbb{Q}$, write

$$x = p^k \frac{a}{b}, \quad p \nmid ab.$$

That is, "factor out" all possible powers of $p$ from $x$ when written in lowest terms. We then define a function $\text{ord}_p : \mathbb{Q}\backslash\{0\} \to \mathbb{Z}$ as $\text{ord}_p(x) = k$. Depending on the text, the reader may see $\text{ord}_p(0) = \infty$ as a special definition, and we will see why momentarily. So, for example,

$$\text{ord}_2(8) = 3, \quad \text{ord}_3\left(\frac{5}{3}\right) = -1, \quad \text{ord}_{11}\left(\frac{33}{8}\right) = 1.$$

Since the function $\text{ord}_p$ only takes values in $\mathbb{Z}$, it is referred to as a *discrete valuation* on $\mathbb{Q}$. The following proposition is easy, but crucial.

**Proposition 4.1.5.** *For $x, y \in \mathbb{Q}\backslash\{0\}$, $ord_p(x+y) \geq \min\{ord_p(x), ord_p(y)\}$.*

*Proof.* Let $n = \text{ord}_p(x)$ and $m = \text{ord}_p(y)$, and suppose first that they are unequal. Without loss of generality, assume $m < n$. Write

$$x = p^n \frac{a}{b}, \quad y = p^m \frac{c}{d},$$

where $p$ does not divide $a, b, c, d$. Since $m < n$, we find

$$x + y = p^m \left(\frac{p^{n-m}a}{b} + \frac{c}{d}\right) = p^m \frac{p^{n-m}ad + bc}{bd}.$$

As $n - m > 0$ and since $p$ does not divide either $b$ or $c$, $p$ cannot divide the numerator of this fraction. Similarly, the fact $p \nmid b, d$ implies $p$ does not divide the denominator of this fraction. Hence $\text{ord}_p(x+y) = m = \min\{\text{ord}_p(x), \text{ord}_p(y)\}$. So we get equality in this case. If $n = m$, then we see that, by the same logic,

$$x + y = p^m \frac{ad + bc}{bd}.$$

Again, as $p \nmid b, d$, we find $p$ does not divide the denominator. However $p$ could divide the numerator, which could only contribute more to $\text{ord}_p(x+y)$. Therefore

$$\text{ord}_p(x + y) \geq m = \min\{\text{ord}_p(x), \text{ord}_p(y)\}.$$

The statement is true in both cases, proving the proposition. □

An example of when equality does not hold is

$$\text{ord}_2(2 + 2) = \text{ord}_2(4) = 2 > 1 = \min\{1, 1\}.$$

Using this valuation, we can define the $p$-adic absolute value $|\cdot|_p$ as follows.

**Definition 4.1.6.** Choose any $0 < c < 1$, and let $x \in \mathbb{Q}$. Then the $p$-adic absolute value is defined as

$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ c^{\text{ord}_p(x)} & \text{if } x \neq 0 \end{cases}.$$

We noted above that sometimes texts define $\text{ord}_p(0) = \infty$. In Definition 4.1.6, with this notation, $|0|_p = c^\infty = 0$, meaning there is no need to make the special definition $|0|_p = 0$.

We will be using $c = \frac{1}{p}$, which is the common choice for $c$. However, any two choices of $c$ (with $0 < c < 1$) will provide equivalent absolute values on $\mathbb{Q}$. Two different primes, on the other hand, result in two inequivalent absolute values. That $|\cdot|_p$ is non-Archimedean follows immediately from the definition and Proposition 4.1.5.

The key observation to make is, in the corresponding metric, two numbers are close if their difference is divisible by a high power of $p$. For example,

$$|129 - 1|_2 = |128|_2 = \frac{1}{2^{\text{ord}_2(128)}} = \frac{1}{2^7} = .0078125,$$

which means 1 and 129 are "close" 2-adically. This probably contradicts any preconceived notion of distance the reader may have (such as the one learned in elementary school).

### $p$-adic Numbers and $p$-adic Integers

Armed with this $p$-adic metric, we can obtain the completion of $\mathbb{Q}$ with respect to this metric. One could follow the exact same method as the one outlined in the previous section to obtain $\mathbb{R}$, but we introduce a more "algebraic" approach. We will not prove many of the facts stated here, but proofs can be found in [9]. Fix a prime $p$. Let $\mathcal{C}$ denote the set of Cauchy sequences of elements of $\mathbb{Q}$ with respect to the $p$-adic metric. Then $\mathcal{C}$ can be made into a ring with the following operations:

$$\{a_n\} + \{b_n\} = \{a_n + b_n\},$$
$$\{a_n\} \cdot \{b_n\} = \{a_n b_n\}.$$

It can be shown that the two resulting sequences are indeed Cauchy sequences (and hence in $\mathcal{C}$). Both operations are clearly commutative, and if we define the multiplicative identity as $1 = \{1\}$, then $\mathcal{C}$ becomes a commutative ring with identity.

To obtain a field from $\mathcal{C}$, we can quotient out by a maximal ideal. Before, we considered two Cauchy sequences to be equivalent if their difference tended to zero. So we can consider $\mathcal{N}$, the sequences of $\mathcal{C}$ which have a limit of zero.

**Proposition 4.1.7.** *$\mathcal{C}/\mathcal{N}$ is a field.*

*Proof.* The proof is straightforward so we will present it here. First, let us show that $\mathcal{N}$ is an ideal. If $\{x_n\}, \{y_n\} \in \mathcal{N}$, it is clear that $\{x_n\} + \{y_n\} \in \mathcal{N}$. Suppose that $\{z_n\} \in \mathcal{C}$. We want

$$\{x_n\} \cdot \{z_n\} \in \mathcal{N}.$$

We will let the reader verify that $\{|z_n|_p\}$ is a Cauchy sequence in $\mathbb{Q}$, and this implies that the terms $|z_n|_p$ are bounded. But then we find

$$\lim_{n\to\infty} |x_n z_n|_p = \lim_{n\to\infty} |x_n|_p |z_n|_p = 0,$$

meaning $\{x_n\} \cdot \{z_n\} \in \mathcal{N}$. Hence $\mathcal{N}$ is an ideal of $\mathcal{C}$. To show the quotient is a field, it suffices to show every element of $\mathcal{C}$ not in $\mathcal{N}$ is invertible modulo $\mathcal{N}$. So suppose $\{x_n\}$ is in $\mathcal{C}$ but not in $\mathcal{N}$. Let

$$l = \lim_{n\to\infty} |x_n|_p \neq 0.$$

Then as $\{|x_n|_p\}$ is Cauchy, there exists $N$ such that $n > N$ implies $|x_n - l|_p \leq l/2$, so in particular for all $n > N$, $x_n \neq 0$. Therefore only a finite number of the $x_n$ are zero. Let $\{y_n\}$ be the sequence defined by

$$y_n = \begin{cases} 1 & \text{if } x_n = 0 \\ x_n^{-1} & \text{if } x_n \neq 0 \end{cases}.$$

Then it is easily verifed that $\{y_n\}$ is Cauchy and that $\{x_n\} \cdot \{y_n\} = 1 + \{z_n\}$, where $\{z_n\} \in \mathcal{N}$. Therefore $\mathcal{C}/\mathcal{N}$ is a field. □

The field $\mathcal{C}/\mathcal{N}$ is denoted $\mathbb{Q}_p$, and called the $p$-adic numbers. One can show that $\mathbb{Q}_p$ is complete, and this is done in [9].

Now, the proof above used the fact that if $\{x_n\}$ is a Cauchy sequence in $\mathbb{Q}$, then $\{|x_n|_p\}$ was a Cauchy sequence in $\mathbb{Q}$. We can say more. Since $|\cdot|_p$ is a discrete metric (i.e. its possible values form a discrete set in $\mathbb{R}$), a convergent Cauchy sequence means that after a point all the values in the sequence are the same. For this reason, we can make the following definition.

**Definition 4.1.8.** Suppose $x \in \mathbb{Q}_p$, and let $\{x_n\}$ be a Cauchy sequence (of rationals) which represents $x$. Then we can define

$$|x|_p = \lim_{n\to\infty} |x_n|_p.$$

Thus we can extend the $p$-adic absolute value on $\mathbb{Q}$ to all of $\mathbb{Q}_p$, and moreover it makes sense to discuss nice topological terms like "neighborhoods" and "dense sets." As a first example, via constant sequences, we can embed $\mathbb{Q}$ into $\mathbb{Q}_p$. And similarly to how $\mathbb{Q}$ is dense in $\mathbb{R}$, it is also true $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Let us prove that now, and a proof can be found in [7].

**Proposition 4.1.9.** *The image of $\mathbb{Q}$ in $\mathbb{Q}_p$ (under the natural inclusion) is dense in $\mathbb{Q}_p$.*

*Proof.* Suppose $x \in \mathbb{Q}_p$ and let $\{x_n\}$ denote a Cauchy sequence of rationals which represents $x$. Let $\epsilon > 0$. To show the image of $\mathbb{Q}$ is dense, we need to find a constant sequence within $\epsilon$ of $x$. Choose $\epsilon' < \epsilon$ (the reason will be clear by the end). Since $\{x_n\}$ is Cauchy, we can certainly find $N$ such that $n, m \geq N$ implies $|x_n - x_m|_p < \epsilon'$. We let $y = x_N$ and then consider the constant sequence $\{y\}$. The claim is that this is the constant sequence we want. Clearly $x - y$ is represented by the sequence $\{x_n - y\}$. Moroever, by definition,

$$|x - y|_p = \lim_{n\to\infty} |x_n - y|_p.$$

However, for $n \geq N$, $|x_n - y|_p < \epsilon'$ by choice of $y$. Therefore

$$|x - y|_p = \lim_{n\to\infty} |x_n - y|_p \leq \epsilon' < \epsilon,$$

as required. Since $x \in \mathbb{Q}_p$ was arbitrary, the image of $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. □

*Remark* 4.1.10. At times we say $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ or $\mathbb{Q}$ is dense in $\mathbb{R}$, but what we mean is that the image of $\mathbb{Q}$ in these fields, under the natural inclusion by constant sequences, is dense.

Next, we will examine a particular subring of $\mathbb{Q}_p$, given by

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leq 1\},$$

and called the *ring of p-adic integers*. This is, in fact, a ring because we have the non-Archimedean metric $|\cdot|_p$. It is clear that the embedding of $\mathbb{Z}$ into $\mathbb{Q}_p$, by constant sequences, will lie in $\mathbb{Z}_p$, as integers have no denominators. However, the fact we will need is that $\mathbb{Z}$ is actually *dense* in $\mathbb{Z}_p$. The following proof comes from [7].

**Proposition 4.1.11.** *The image of $\mathbb{Z}$ in $\mathbb{Z}_p$ (under the natural inclusion) is dense in $\mathbb{Z}_p$.*

*Proof.* Choose $x \in \mathbb{Z}_p$. Since the $p$-adic metric is discrete, it suffices to show that for any $n \geq 1$ (so that we stay in $\mathbb{Z}_p$), we can find an integer (i.e. a constant sequence consisting of intgers) within $\frac{1}{p^n}$ of $x$. By Proposition 4.1.9, we can find a rational number $a/b \in \mathbb{Q}$, $b \neq 0$, such that

$$\left|x - \frac{a}{b}\right|_p \leq \frac{1}{p^n} < 1.$$

As

$$\frac{a}{b} = \frac{a}{b} - x + x,$$

using the non-Archimedean property of the metric we find

$$\left|\frac{a}{b}\right|_p \leq \max\{|x|_p, |x - \frac{a}{b}|_p\} \leq 1.$$

But this implies that $\frac{a}{b}$ belongs to the localized ring $\mathbb{Z}_{(p)}$, which also gives $p \not| b$. But as $(p, b) = 1$, $b$ will have an inverse modulo $p^n$, so we find can $b' \in \mathbb{Z}$ such that $bb' \equiv 1 \bmod p^n$. With this, we find

$$p^n | bb' - 1 \implies p^n | abb' - a \implies p^n | \frac{a}{b} - ab'$$

as $(b, p^n) = (b, p) = 1$. By definition of the $p$-adic metric, this yields

$$\left| \frac{a}{b} - ab' \right|_p \leq \frac{1}{p^n}.$$

Clearly $ab' \in \mathbb{Z}$, and

$$|x - ab'|_p \leq \max \left\{ \left| x - \frac{a}{b} \right|_p, \left| \frac{a}{b} - ab' \right|_p \right\} \leq \frac{1}{p^n}.$$

Since $x \in \mathbb{Z}_p$ was arbitrary, this proves $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. □

Both $\mathbb{Z}_p$ and the proposition will be important when we prove that all symmetric groups exist as Galois groups of totally real fields.

### 4.1.2 Approximation Theorem

In this section we prove important result crucial to the proof of the main theorem of this chapter. As with many results in the previous two sections, the theorem can be proved in greater generality (for arbitrary number fields), but we state and prove the theorem only for $\mathbb{Q}$, as this is the only number field we will need to use it for.

**Theorem 4.1.12.** *Suppose $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ are non-trivial pairwise inequivalent absolute values on $\mathbb{Q}$, and let $\beta_1, \ldots, \beta_n$ be nonzero elements of $\mathbb{Q}$. Then for any $\epsilon > 0$, there exists $\alpha \in \mathbb{Q}$ such that $|\alpha - \beta_j|_j < \epsilon$ for each $j$.*

*Proof.* First, we claim there exist $x_i \in \mathbb{Q}$ such that for every $i$,

$$|x_i|_i > 1, \quad |x_i|_j < 1 \text{ for } i \neq j.$$

Then we will construct $\alpha$ using the $x_i$ and the $\beta_i$. To prove the claim, we use induction on $n$. Suppose $n = 2$. Then as $|\cdot|_1$ and $|\cdot|_2$ are non-equivalent by assumption, by definition we can find $y, z \in \mathbb{Q}$ such that $|y|_1 > 1$ with $|y|_2 \leq 1$, and $|z|_1 \leq 1$ with $|z|_2 > 1$. Then if $x_1 = \frac{y}{z}$, then $|x_1|_1 > 1$ and $|x_1|_2 < 1$. Construct $x_2$ similarly.

For the inductive step, assume there exists $x \in \mathbb{Q}$ such that

$$|x|_1 > 1 \quad \text{and} \quad |x|_j < 1 \text{ for } j = 2, 3, \ldots, n-1.$$

By the $n = 2$ case, there exists $t \in \mathbb{Q}$ such that $|t|_1 > 1$ and $|t|_n < 1$. Define

$$x_1 = \begin{cases} x & \text{if } |x|_n < 1 \\ x^r t & \text{if } |x|_n = 1 \\ \frac{x^r t}{1+x^r} & \text{if } |x|_n > 1 \end{cases}$$

where $r$ is a number which will be determined shortly. Let us go through each case.

(i) In the first case, $|x_1|_1 > 1$ and $|x_1|_j < 1$ for $j = 2, \ldots, n$, which is what we need.

(ii) In the second case, we certainly have $|x_1|_1 > 1$ (as $|x|_1 > 1$ and $|t|_1 > 1$) and $|x_1|_n < 1$. If $2 \leq j \leq n-1$, then as $|x|_j < 1$ and $t$ is some fixed element of $\mathbb{Q}$, we can choose $r$ large enough so that $|x_1|_j < 1$. (Take $r$ so that $0 < |x|_j^r < 1/|t|_j$.) With this $r$, $x_1$ becomes an element such that $|x_1|_1 > 1$ and $|x_1|_j < 1$ for $2 \leq j \leq n$.

(iii) Note that

$$|x_1|_j = \frac{|x|_j^r |t|_j}{|1 + x^r|_j} = \frac{|t|_j}{|x^{-r} + 1|_j}.$$

If $j = 1$, then

$$|x_1|_1 \geq \frac{|t|_1}{|x|_1^{-r} + 1} \to |t|_1 > 1$$

as $r \to \infty$. Therefore, for $r$ sufficiently large, $|x_1|_1 > 1$. Also observe that for all $y \in \mathbb{Q}$, $|1 + y|_j \geq \big||y|_j - 1\big|$ (break into cases $|y|_j \geq 1$ and $|y|_j < 1$ and use $|a - b|_j \geq |a|_j - |b|_j$), which implies

$$|x_1|_j \leq \frac{|t|_j}{\big||x|_j^{-r} - 1\big|}.$$

If $2 \leq j \leq n - 1$, then

$$|x_1|_j \leq \frac{|t|_j}{\big||x|_j^{-r} - 1\big|} \to 0$$

as $r \to \infty$ since $|x|_j < 1$. Lastly,

$$|x_1|_n \leq \frac{|t|_n}{\big||x|_n^{-r} - 1\big|} \to |t|_n < 1$$

as $r \to \infty$ since $|x|_n > 1$. Therefore for $r$ sufficiently large, we find $|x_1|_1 > 1$ and $|x_1|_j < 1$ for $2 \leq j \leq n$, as required.

In all three cases, provided $r$ is large enough, we can find $x_1$ such that $|x_1|_1 > 1$ and $|x_1|_j < 1$ for $2 \leq j \leq n$. By symmetry, we can find $x_i$ such that

$$|x_i|_i > 1 \quad \text{and} \quad |x_i|_j < 1 \text{ for } j \neq i.$$

To finish the proof, let

$$\alpha = \sum_j \frac{x_j^s}{1 + x_j^s} \beta_j,$$

where $s$ is to be determined. By the triangle inequality,

$$|\alpha - \beta_i|_i \leq \left| \frac{\beta_i}{1 + x_i^s} \right|_i + \sum_{j \neq i} \left| \frac{x_j^s}{1 + x_j^s} \beta_j \right|_i .$$

The $\beta_i$ and $x_i$ are all fixed. But by logic entirely similar to the steps in the three cases above, as $s \to \infty$, each of the terms goes to 0. Therefore for $s$ sufficiently large, we can make all the $|\alpha - \beta_i|_i < \epsilon$ (find $s$ for each case and take largest such $s$). This proves the theorem. □

One could think of this approximation theorem as an extension of the Chinese Remainder Theorem. If these absolute values are all $p$-adic (non-Archimedean) absolute values on $\mathbb{Q}$, then $\alpha$ and $\beta$ being "close" is the same as saying

$$\alpha \equiv \beta \bmod p^n$$

for some sufficiently large $n$. So suppose the metric $|\cdot|_i$ in the theorem corresponds to the $p_i$-adic metric for some prime $p_i$, and choose $n_i$ such that $\frac{1}{p_i^{n_i}} < \epsilon$. Then if the $\beta_i \in \mathbb{Z}$, then the approximation theorem says we can find $\alpha$ such that

$$\alpha \equiv \beta_i \bmod p_i^{n_i}$$

for all $i$, which is what the Chinese Remainder Theorem gives. The power of this theorem, however, lies in the fact that we can take $\beta_i \in \mathbb{Q}$, not just elements of $\mathbb{Z}$. Moreover, we can use the Archimedean absolute value on $\mathbb{Q}$, not just the $p$-adic ones. One also sees that the same proof works if we replace $\mathbb{Q}$ by an arbitrary number field $F$, and so this theorem extends even further.

### 4.1.3 Alternate Method for Computing Galois Groups

The approximation theorem is certainly the major tool in getting the symmetric group $S_n$ to be the Galois group of a totally real number field. The theorem we present in this section is the result used by the standard method for getting $S_n$ to be a Galois group of some extension of $\mathbb{Q}$, not necessarily totally real. We will also be using the theorem, and it is very helpful when trying to compute Galois groups.

Suppose we had a polynomial $f(x) \in \mathbb{Z}[x]$. Calculating the Galois group can be difficult, especially if the polynomial is of high degree. The main idea behind this theorem is that the factorizations modulo some prime $p$ give some information about the Galois group of the polynomial over $\mathbb{Z}$ (and hence over $\mathbb{Q}$). The theorem can be found in [11].

**Theorem 4.1.13.** *Suppose $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree $n$ and $p$ a prime for which the reduction $\bar{f}(x)$ of $f(x)$ modulo $p$ has no multiple roots. Suppose $\bar{f}(x)$ factors into irreducibles as*

$$\bar{f} = \bar{f}_1(x) \cdots \bar{f}_k(x),$$

*where $\bar{f}_i(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree $n_i$, say. Then regarded as a subgroup of $S_n$, the group $Gal(f)$ of $f(x)$ over $\mathbb{Q}$ contains an element $\sigma$ with cycle type $(n_1, n_2, \cdots, n_k)$.*

*Proof.* Let $K$ be a splitting field for $f(x)$ over $\mathbb{Q}$. The condition that the reduced polynomial $\bar{f}(x) \in \mathbb{F}_p[x]$ has no multiple roots means that $p$ is unramified in $K$ by the Dedekind-Kummer Theorem (Theorem 2.3.49). Let $\mathfrak{P}$ be a prime of $\mathcal{O}_K$ lying above $p$. Then letting $\mathbb{F}_\mathfrak{P} = \mathcal{O}_K/\mathfrak{P}$ as usual, it is clear that $\mathbb{F}_\mathfrak{P}$ will be the splitting field for $\bar{f}(x)$ over $\mathbb{F}_p$. Moreover, $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_p)$ transitively permutes the roots (in $\mathbb{F}_\mathfrak{P}$) of the irreducible factors of $\bar{f}(x)$. But over finite fields, all Galois groups are cyclic, and so $\mathrm{Gal}(\bar{f}_i)$ will be an element of order $n_i$ in $S_{n_i}$ (as $\mathrm{Gal}(\bar{f}_i)$ can be regarded as a subgroup of $S_{n_i}$), which is an $n_i$-cycle. Since each of the roots of the $\bar{f}_i$ are distinct, it is clear that $\mathrm{Gal}(\bar{f})$ will contain a permutation of cycle type $(n_1, \ldots, n_k)$ (a product of disjoint cycles of length $n_1, n_2, \ldots, n_k$). But as $p$ is unramified, by Remark 2.3.72 we have an isomorphism

$$D(\mathfrak{P}/p) \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_p).$$

Therefore $D(\mathfrak{P}/p)$, when regarded as a subgroup of $S_n$, contains a permutation $\sigma$ of the same cycle type. But as $D(\mathfrak{P}/p) \leq \mathrm{Gal}(f)$, we see $\mathrm{Gal}(f)$ also contains $\sigma$. □

Why this theorem is so nice is that we have explicit generating sets for, say, $S_n$. For example, from group theory, we have the following.

**Proposition 4.1.14.** *(i) For $n \geq 4$, $S_n$ is generated by a transposition and an $(n-1)$-cycle.*

*(ii) If $p \geq 3$ is prime, then $S_p$ is generated by a transposition and a $p$-cycle.*

In particular, it is possible that by reducing the polynomial modulo appropriate primes, we will get cycle types which generate $S_n$, such as a transposition and an $(n-1)$-cycle.

**Example 4.1.15.** Consider $f(x) = x^5 + 5x^4 - 20x^3 - 40x^2 + 5x + 1$. Since it is a quintic polynomial, the Galois group is isomorphic to a subgroup of $S_5$, so we consider $\mathrm{Gal}(f)$ to be this isomorphic subgroup. We show that $\mathrm{Gal}(f) \cong S_5$ by simply using Theorem 4.1.13. First, we can look at $f(x)$ modulo 11 and find that it is irreducible. (One could check this directly or use languages like Mathematica or SAGE to factor the polynomial.) This factorization yields two facts. For one thing, it shows that the polynomial is irreducible over $\mathbb{Z}$, and hence over $\mathbb{Q}$ (Theorem A.2.1). The other fact is that $\mathrm{Gal}(f)$ contains a 5-cycle by Theorem 4.1.13.

Next, reduce $f(x)$ modulo the prime 7 to get the factorization

$$f(x) = (x^3 + 5x + 5)(x^2 + 5x + 3) \bmod 7$$

which, by Theorem 4.1.13, implies that $\mathrm{Gal}(f)$ contains a permutation of cycle type $(3, 2)$. But cubing this element produces a transposition as disjoint cycles commute, and so $\mathrm{Gal}(f)$ contains a transposition. Therefore, by Proposition 4.1.14(ii), $\mathrm{Gal}(f) \cong S_5$, as $\mathrm{Gal}(f)$ contains a transposition and a 5-cycle.

On first glance, calculating the Galois group of the polynomial in the example might seem intimidating. But this example establishes just how powerful Theorem 4.1.13 can be.

## 4.2 Realizing $S_n$ as Galois group of totally real number field

Now that all the background material is set, we can begin our march towards the existence of a totally real number field with Galois group $S_n$. Just to give the reader an idea, without the totally real restriction, the approach would be to pick three primes, find three factorizations (modulo these three primes) which would give us the necessary cycle types to generate $S_n$ using Theorem 4.1.13, and use the Chinese Remainder Theorem to find $f(x) \in \mathbb{Z}[x]$ which reduce to these three factorizations modulo these primes. But the problem is there is absolutely no guarantee that all the roots of the constructed $f(x)$ will be real, which would be necessary for a totally real splitting field.

This idea will certainly be important to our proof, but the approximation theorem will be used to make sure all the roots of our polynomial are real. The proof will also require results which allow us to describe the behavior of polynomials after perturbing the coefficients slightly. This is what the following proposition and subsequent corollary do.

**Proposition 4.2.1.** *Let $I \subset \mathbb{R}$ be a bounded interval, and $f(x) \in \mathbb{R}[x]$ a polynomial of degree $n > 0$. Then for all $\epsilon > 0$, there exists $\delta > 0$ (which depends*

*on $I$ and $\epsilon$) such that if $g(x) \in \mathbb{R}[x]$ is a polynomial formed by perturbing the coefficients of $f(x)$ by at most $\delta$, then $|f(x) - g(x)| < \epsilon$ on $I$.*

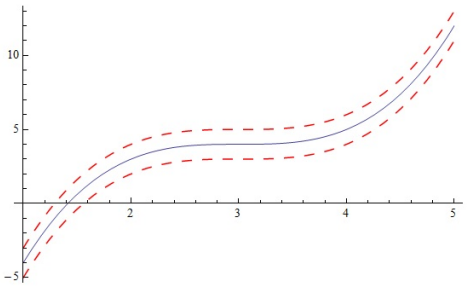



Figure 4.1: Perturbing coefficients of polynomial by at most $\delta$ ensures new polynomial stays within dashed red lines

*Proof.* Let $g(x) \in \mathbb{R}[x]$ be degree $n$ and write $g(x) = f(x) + c(x)$, where $c(x)$ is a polynomial of degree at most $n$, and let $\epsilon > 0$. Write

$$c(x) = \sum_{i=0}^{n} c_i x^i,$$

and let $C = \max_{0 \leq i \leq n} |c_i|$. Now, since $I$ is bounded, there exists $M$ such that $|x| \leq M$ on $I$ (just take $M = \sup_{x \in I} |x|$). Notice that on $I$,

$$\begin{aligned}
|f(x) - g(x)| &= |c(x)| \\
&= |c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0| \\
&\leq |c_n x^n| + |c_{n-1} x^{n-1}| + \ldots + |c_1 x| + |c_0| \quad \text{(triangle inequality)} \\
&\leq |c_n||x|^n + \ldots + |c_1||x| + |c_0| \\
&\leq |c_n| M^n + |c_{n-1}| M^{n-1} + \ldots + |c_1| M + |c_0| \quad \text{(by definition of } M\text{)} \\
&\leq C M^n + C M^{n-1} + \ldots C M + C \quad \text{(as each } |c_i| \leq C\text{)} \\
&\leq C(1 + M + \ldots + M^n).
\end{aligned}$$

If $C$ is such that

$$0 < C < \frac{\epsilon}{1 + M + \ldots + M^n},$$

then the above shows $|f(x) - g(x)| < \epsilon$ on $I$. Since $C = \max_{0 \leq i \leq n} |c_i|$, if we take $\delta = C$, then the work above shows that perturbing the coefficients of $f(x)$ by at most $\delta$ ensures that we stay within $\epsilon$ of $f(x)$ on $I$. Therefore the proposition is proved. □

**Corollary 4.2.2.** *If $f(x) \in \mathbb{R}[x]$ is a polynomial of degree $n > 0$ with $n$ distinct roots in $\mathbb{R}$, then there exists $\delta > 0$ such that if $g(x) \in \mathbb{R}[x]$ is a polynomial of degree $n$ formed by changing the coefficients of $f(x)$ by at most $\delta$, then $g(x)$ will also have $n$ real roots.*

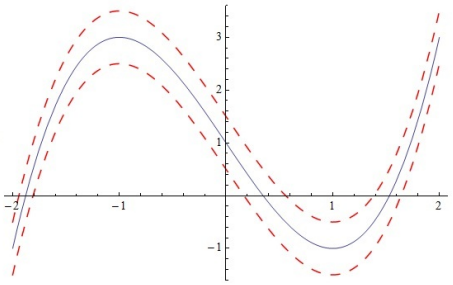



Figure 4.2: A cubic polynomial which stays within red dashed lines will still have three real roots

*Proof.* The diagram illustrates the basic idea of the proof.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{R}$ be the $n$ roots of $f(x)$, ordered so that $\alpha_i < \alpha_{i+1}$ for all $i$. Rolle's theorem from calculus says that between any two roots of $f(x)$ there must be a zero of the derivative. Consequently, the derivative of $f(x)$ must have $n-1$ (distinct) real roots, say $\beta_1, \beta_2, \ldots, \beta_{n-1}$. Choose any $\eta > 0$ and let $I = [\alpha_1 - \eta, \alpha_n + \eta]$. Finally, choose any $\epsilon$ such that

$$0 < \epsilon < \min\{|f(\alpha_1 - \eta)|, |f(\alpha_n + \eta)|, |f(\beta_1)|, \ldots, |f(\beta_n)|\}.$$

Note such an $\epsilon$ must exist because each of the $f(\beta_i) \neq 0$ since $f(x)$ has no multiple roots. Then using Proposition 4.2.1, there exists $\delta > 0$ such that if $g(x)$ is a polynomial formed by perturbing the coefficients of $f(x)$ by at most $\delta$, then $|f(x) - g(x)| < \epsilon$ on $I$. But by choice of $\epsilon$, this means that each of the pairs

$$f(\alpha_1 - \eta) \text{ and } g(\alpha_1 - \eta), f(\alpha_n + \eta) \text{ and } g(\alpha_n + \eta), f(\beta_i) \text{ and } g(\beta_i),$$

have the same sign. In particular, $g(x)$ will have as many sign changes on $I$ as $f(x)$ did, which was $n$, which means $g(x)$ will also have $n$ real roots (and in $I$). □

With these two results in hand, we can prove our main theorem of the chapter.

**Theorem 4.2.3.** *$S_n$ occurs as the Galois group of a totally real number field.*

*Proof.* Let $p_1, p_2, p_3$ be three (distinct) primes with $p_3 > n-2$. Let $\overline{f_{p_1}}(x) \in \mathbb{F}_{p_1}[x]$ be any irreducible polynomial of degree $n$, $\overline{f_{p_2}}(x) \in \mathbb{F}_{p_2}[x]$ be a product of an irreducible polynomial of degree $n-1$ times any linear factor, and let $\overline{f_{p_3}}(x) \in \mathbb{F}_{p_3}[x]$ be the product of an irreducible quadratic factor and $n-2$ distinct linear factors (possible since $p_3 > n-2$). Finally, let $f_\infty(x) \in \mathbb{Q}[x]$ be any polynomial of degree $n$ with $n$ (distinct) real roots.

Let $f_{p_i}(x) \in \mathbb{Z}_p[x]$ be any polynomials which reduce to $\overline{f_{p_i}}(x)$ modulo $p_i$. Now for $i = 1, 2, 3$, let $\epsilon_i > 0$. Notice that if the $\epsilon_i$ are chosen so that $\epsilon_i < 1$, then if we modify the coefficients of $f_{p_i}$ by at most $\epsilon_i$ (in the $p_i$-adic metric), then the new polynomial $g_{p_i}(x)$ still resides in $\mathbb{Z}_{p_i}[x]$. Moreover the coefficients are changing by

a multiple of $p_i$ so that the reduction mod $p_i$ remains $\overline{f_{p_i}}(x)$. So select the $\epsilon_i$ so that $0 < \epsilon_i < 1$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_{p_i}$, change the coefficients of $f_{p_i}(x)$ by at most $\epsilon_i$ so that the coefficients are now in $\mathbb{Z}$.

Finally, let $\delta$ be as in Corollary 4.2.2 applied to $f_\infty(x)$ and let $\epsilon_\infty = \delta$.

We will use the approximation theorem to construct a new polynomial. Define $\epsilon = \min\{\epsilon_\infty, \epsilon_1, \epsilon_2, \epsilon_3\}$. Suppose $c_{i,j}$ is the coefficient in $f_{p_i}$ of $x^j$ and suppose $c_{\infty,j}$ is the coefficient of $x^j$ in $f_\infty$. The approximation theorem (Theorem 4.1.12) says there exists $a_j \in \mathbb{Q}$ such that

$$|a_j - c_{i,j}|_{p_i} < \epsilon \quad \text{and} \quad |a_j - c_{\infty,j}| < \epsilon.$$

Do this for $j = 0, 1, \ldots, n-1$, and then define $h(x) \in \mathbb{Q}[x]$ as

$$h(x) = x^n + \sum_{j=0}^{n-1} a_j x^j.$$

By the arguments above, reduction of $h(x)$ modulo $p_i$ will still be $\overline{f_{p_i}}(x)$, and as $\epsilon \leq \epsilon_\infty$, $h(x)$ will also have $n$ real roots. But the reduction of $h(x)$ mod $p_1$ shows $h(x)$ is irreducible. The reduction modulo $p_2$ gives a permutation of cycle type $(n-1, 1)$ in $\mathrm{Gal}(h)$ (i.e. an $(n-1)$-cycle), and the reduction mod $p_3$ produces a permutation of type $(2, 1, \ldots, 1)$ in $\mathrm{Gal}(h)$ (i.e. a transposition). Therefore, by Proposition 4.1.14, $\mathrm{Gal}(h)$ has Galois group $S_n$. So if we let $K$ be a splitting field for $h(x)$ over $\mathbb{Q}$, we see $\mathrm{Gal}(K/\mathbb{Q}) \cong S_n$ and $K$ is totally real (as all the roots of $h(x)$ are real). □

## 4.3 Explicit Polynomials: Symmetric Group

In this section, we produce polynomials with Galois group $S_n$ and $n$ real roots for $2 \leq n \leq 8$ (meaning its splitting field is totally real and has Galois group $S_n$). In each example, it can be checked using SAGE or Mathematica that the polynomials do, in fact, have $n$ real roots, so we will not go through those details here.

$n = 2$: This is the simplest case to consider, and we take the polynomial $x^2 + x - 1$. As this polynomial has two real irrational roots, its Galois group is $S_2$.

$n = 3$: Take $f(x) = x^3 + 3x^2 - 6x - 4$. Then as the reduction of $f(x)$ mod 5 is irreducible, $f(x)$ is irreducible over $\mathbb{Q}$ and $\mathrm{Gal}(f)$ contains a 3-cycle (Theorem 4.1.13). Moreover, the factorization modulo 7 is

$$f(x) = (x^2 + 1)(x + 3) \bmod 7,$$

and so $\mathrm{Gal}(f)$ contains a transposition. Theorem 4.1.14 then implies $\mathrm{Gal}(f) = S_3$.

$n = 4$: $f(x) = x^4 + 4x^3 - 12x^2 - 16x + 1$. As its image modulo 3 is irreducible, $f(x)$ is irreducible. Modulo 11,

$$f(x) = (x^3 + 5x^2 + 4x + 10)(x + 10),$$

and so $\mathrm{Gal}(f)$ contains a 3-cycle. Finally,

$$f(x) = (x^2 + 19x + 14)(x + 21)(x + 22),$$

and hence Theorem 4.1.13 implies that $\mathrm{Gal}(f)$ contains a transposition. By Theorem 4.1.14, $\mathrm{Gal}(f) = S_4$.

$n = 5$: $f(x) = x^5 + 5x^4 - 20x^3 - 40x^2 + 5x + 1$. Example 4.1.15 shows $\mathrm{Gal}(f) = S_5$.

$n = 6$: $f(x) = x^6 + 6x^5 - 30x^4 - 80x^3 + 15x^2 + 6x - 1$. It is irreducible mod 11, meaning $f(x)$ is irreducible over $\mathbb{Q}$. We also find

$$f(x) = (x + 4)(x^5 + 2x^4 + 8x^3 + 3x^2 + 3x + 17) \bmod 23,$$

$$f(x) = (x^3 + 14x^2 + 19x + 23)(x^2 + 29x + 20)(x + 5) \bmod 31.$$

The first factorization shows that $\mathrm{Gal}(f)$ contains a 5-cycle. As the cube of a permutation of type $(3, 2, 1)$ is a transposition, and thus $\mathrm{Gal}(f)$ also possesses a transposition. Therefore $\mathrm{Gal}(f) = S_6$.

$n = 7$: $f(x) = x^7 + 7x^6 - 84x^5 - 140x^5 + 560x^3 + 336x^2 - 448x + 64$. We leave it to the reader to verify that $f(x)$ is irreducible modulo 19, which shows that $f(x)$ is irreducible over $\mathbb{Q}$ and $\mathrm{Gal}(f)$ contains a 7-cycle. We also let the reader check that the reduction of $f(x)$ modulo 3 and Theorem 4.1.13 imply that $\mathrm{Gal}(f)$ contains a transposition. Therefore $\mathrm{Gal}(f) = S_7$ by Theorem 4.1.14.

$n = 8$: This one will also be mostly left to the reader to check. Let

$$f(x) = x^8 + 8x^7 - 112x^6 - 224x^5 + 1120x^4 + 896x^3 - 1792x^2 + 512x + 1.$$

Then $f(x)$ is irreducible mod 71, and so it is irreducible over $\mathbb{Q}$. Reducing mod 3 produces a 7-cycle, and reducing mod 5 produces a $(5, 2, 1)$ cycle. By taking raising this element to the fifth power, we produce a transposition. Therefore $\mathrm{Gal}(f) = S_8$.

These examples truly exhibit the usefulness of Theorem 4.1.13. Without this theorem, calculating these Galois groups would prove more complicated. But clearly, with the theorem in hand, the calculation was simplified. This process, of course, requires that we find the right primes to use, and there is no guarantee that we will find the cycle types we need. But if you are lucky enough to find them, then the proof follows quite easily.

# Chapter 5

# Other Groups

In this chapter, we discuss the dihedral groups and groups of odd order. We will outline a method to get $D_{2p}$ as a Galois group of a totally real number field (where $p$ is a prime). As the methods involved would take a considerable amount of time and space to develop properly and thoroughly, we will omit most of the proofs.

## 5.1 Dihedral Groups

### 5.1.1 Class Group

We have seen (and used many times) that there is unique factorization of ideals of $\mathcal{O}_K$ into prime ideals. This was, in a certain sense, a consolation prize, since $\mathcal{O}_K$ is not always a UFD. As a simple example, take $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, which is a standard example of a ring which is not a UFD.

One could say that the class group measures how badly $\mathcal{O}_K$ fails to be a PID. But since all prime ideals are maximal in $\mathcal{O}_K$, it is a fact from ring theory that $\mathcal{O}_K$ is a PID precisely when it is a UFD. Therefore the class group measures how badly $\mathcal{O}_K$ fails to be a UFD as well. It is an important topic in algebraic number theory, and generalizations of this group are the subject of class field theory.

We first extend the notion of ideals of $\mathcal{O}_K$ to what are known as fractional ideals. If $K$ is a number field, then we can regard $K$ as an $\mathcal{O}_K$-module in the obvious way.

**Definition 5.1.1.** A *fractional ideal* of $\mathcal{O}_K$ is a (nonzero) finitely generated $\mathcal{O}_K$-submodule of $K$.

*Remark* 5.1.2. Notice that ideals of $\mathcal{O}_K$ can be thought of as $\mathcal{O}_K$-submodules of $\mathcal{O}_K$, and so this definition of fractional ideals should not seem completely mysterious.

So, for example, if $\alpha \in K$, then $\alpha\mathcal{O}_K$ is a fractional ideal of $\mathcal{O}_K$. Notice that $\alpha\mathcal{O}_K$ is *not* an ideal of $\mathcal{O}_K$ if $\alpha \notin \mathcal{O}_K$. Fractional ideals which are also ideals of $\mathcal{O}_K$ are called *integral ideals*.

The goal is to make the set of fractional ideals of $\mathcal{O}_K$, denoted $I_K$, a group under multiplication. The whole ring, $\mathcal{O}_K$, is clearly going to act as the identity element. But what we need are inverses, which is precisely why we use fractional ideals instead of integral ideals.

**Definition 5.1.3.** If $\mathfrak{M}$ is a fractional ideal of $\mathcal{O}_K$, then define

$$\mathfrak{M}^{-1} = \{x \in K : x\mathfrak{M} \subseteq \mathcal{O}_K\}.$$

Even with this definition, two things need to be proved. First, it is not immediately obvious that $\mathfrak{M}^{-1}$ is actually a fractional ideal. Second, we would need $\mathfrak{M}\mathfrak{M}^{-1} = \mathcal{O}_K$, so that $\mathfrak{M}^{-1}$ is the inverse of $\mathfrak{M}$.

As a simple example of an inverse, if $\alpha \in K$, then the reader can show that if $\mathfrak{M} = \alpha\mathcal{O}_K$, then $\mathfrak{M}^{-1} = \alpha^{-1}\mathcal{O}_K$, and in fact $\mathfrak{M}\mathfrak{M}^{-1} = \mathcal{O}_K$.

**Proposition 5.1.4.** *If $\mathfrak{M}$ is a fractional ideal, then $\mathfrak{M}^{-1}$ is a fractional ideal.*

*Proof.* Clearly $\mathfrak{M}^{-1}$ is an $\mathcal{O}_K$-submodule of $K$ (work through the definition). We just need to show that it is finitely generated. So choose any $0 \neq m \in \mathfrak{M}$. Then $m\mathfrak{M}^{-1} \subseteq \mathcal{O}_K$ (by definition of $\mathfrak{M}^{-1}$), which implies $\mathfrak{M}^{-1} \subseteq m^{-1}\mathcal{O}_K$, which is a finitely generated $\mathcal{O}_K$-module. Since $\mathcal{O}_K$ is Noetherian (as it is a Dedekind ring; Theorem 2.3.15), we find $\mathfrak{M}^{-1}$ is also finitely generated. Therefore $\mathfrak{M}^{-1}$ is a fractional ideal. □

That every fractional ideal $\mathfrak{M}$ has inverse $\mathfrak{M}^{-1}$ follows from the following lemma and theorem.

**Lemma 5.1.5.** *If $\mathfrak{A}$ is an integral ideal, then $\mathfrak{A}$ is invertible with inverse $\mathfrak{A}^{-1}$.*

**Theorem 5.1.6.** *If $\mathfrak{A}$ is a fractional ideal of $\mathcal{O}_K$, then $\mathfrak{A}$ can be uniquely expressed as a product*

$$\mathfrak{A} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n},$$

*where the $\mathfrak{p}_i$ are distinct prime ideals and the $a_i \in \mathbb{Z}\backslash\{0\}$.*

From these two results, it is clear that $\mathfrak{A}^{-1}$ is in fact the inverse of $\mathfrak{A}$. Notice, also, that the theorem serves as an extension of Theorem 2.2.30, which gave the unique factorization of integral ideals into prime ideals.

However, it is now clear that $I_K$ is a group, which is also clearly abelian. Moreover, we can consider $P_K$, the set of principal fractional ideals (i.e. generated by a single element). It is obvious that $P_K$ is a subgroup of $I_K$, and as $I_K$ is abelian, $P_K$ is a normal subgroup. Therefore, the following definition makes sense.

**Definition 5.1.7.** The class group $C_K$ is the quotient

$$C_K = I_K/P_K.$$

It is immediate from the definition that $C_K$ is the trivial group precisely when $I_K = P_K$, or when every fractional ideal is principal. If this is true, then clearly every integral ideal is principal, meaning $\mathcal{O}_K$ is a PID. However, if $\mathcal{O}_K$ is a PID, then Theorem 5.1.6 implies that every fractional ideal will be principal as well, which implies $C_K$ is the trivial group. Therefore $C_K$ is trivial if and only if $\mathcal{O}_K$ is a PID.

We denote the size of $C_K$ by $h_K$, called the *class number*. Perhaps surprisingly, we have the following theorem.

**Theorem 5.1.8.** *If $K$ is a number field, then $h_K < \infty$.*

The class number is, in its own right, a very interesting and mysterious number, and its value for different fields is a topic of interest for number theorists.

### 5.1.2 Hilbert Class Field

As a quick aside, the proof of the finiteness of the class number uses the following theorem.

**Theorem 5.1.9.** *Suppose $K$ is a number field of degree $n$. Let $s$ denote the number of pairs of complex embeddings of $K$. If $\mathfrak{A}$ is a fractional ideal of $\mathcal{O}_K$, then there is an (integral) ideal $\mathfrak{B}$ of $\mathcal{O}_K$ such that $\mathfrak{B} \in [\mathfrak{A}]$ and*

$$N(\mathfrak{B}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

The right hand side of the inequality is known as the Minkowski bound, and it helps when calculating the class group because it limits the number of ideals to check. As a consequence of this theorem, we can prove Theorem 2.3.32.

*Proof.* (of Theorem 2.3.32) Since ideals of $\mathcal{O}_K$ has norm at least 1, the inequality in Theorem 5.1.9 gives

$$|\Delta_K| \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}.$$

We want to show that the right hand side is at least 2 for $n \geq 2$. To do this, let

$$a_n = \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}.$$

Then

$$\frac{a_{n+1}}{a_n} = \sqrt{\frac{\pi}{4}}\left(1+\frac{1}{n}\right)^n > 1$$

for $n > 0$, which implies $a_{n+1} > a_n$. However, $a_2 > 1$, and therefore $|\Delta_K| > 1$ for $n \geq 2$. Hence at least one prime of $\mathbb{Z}$ divides the discriminant, and this implies that at least one prime of $\mathbb{Z}$ ramifies in $K$. □

This provides a nice segue into the next topic, which is the Hilbert class field. There are no unramified extensions of $\mathbb{Q}$, however there can be unramified extensions of other fields. The Hilbert class field is an example of an unramified extension. Properly defining the class field would take too long, so we will use the following theorem as if it were our definition.

**Theorem 5.1.10.** *Let $K$ be a number field. The Hilbert class field $K^{(1)}$ of $K$ is an abelian, unramified extension of $K$ which contains every other abelian, unramified extension of $K$. Moreover, $K^{(1)}$ is Galois over $K$, and $Gal(K^{(1)}/K) \cong C_K$, the class group of $K$.*

It takes real work to prove that such a class field should even exist, and the proof can be found in the appropriate sections of [9]. While the theorem says $K^{(1)}$ is Galois over $K$, it would be even nicer if it were Galois over $\mathbb{Q}$. This happens when $K$ is Galois over $\mathbb{Q}$.

**Proposition 5.1.11.** *Suppose $F$ is a number field and $K$ a Galois extension of $F$. Then $K^{(1)}$ is Galois over $F$.*

This is what will allow us to realize $D_{2p}$ as a Galois group of a totally real field.

### 5.1.3 $D_{2p}$, $p$ prime

Suppose $K = \mathbb{Q}(\sqrt{d})$, where $d > 0$ is squarefree. Suppose $K$ has class number $p$ for some odd prime $p$, so that $C_K$ is cyclic of order $p$ (as all groups of prime order are cyclic). Then $K^{(1)}$ is Galois over $K$ by Theorem 5.1.10, and $\mathrm{Gal}(K^{(1)}/K)$ is cyclic of order $p$. Moreover, $K^{(1)}$ is Galois over $\mathbb{Q}$ by Proposition 5.1.11, and as

$$[K^{(1)} : \mathbb{Q}] = [K^{(1)} : K][K : \mathbb{Q}] = 2p,$$

we find $\mathrm{Gal}(K^{(1)}/\mathbb{Q})$ is a group of order $2p$. We want to determine the structure of this group. Consider the following proposition.

**Proposition 5.1.12.** *If $G$ is a finite group of order $2p$, where $p$ is an odd prime, then $G$ is either cyclic or dihedral.*

*Proof.* By Theorem 3.1.1, $G$ has elements of order 2 and $p$, say $\tau$ and $\sigma$, respectively. Let $H = \langle\tau\rangle$ and $K = \langle\sigma\rangle$. Then $K$ has index 2 in $G$, and is therefore normal. Since elements of $H$ have order 1 or 2 and elements of $K$ have order 1 or $p$, we find $H \cap K = \{e\}$ (i.e. the only element of order 1 in both), and therefore $G = HK$, meaning $G$ is generated by $\sigma$ and $\tau$.

Since $K$ is normal, $\tau\sigma\tau^{-1} = \sigma^k$ for some $k \in \{0, 1, \ldots, p-1\}$. Since $\tau^2 = e$, we see

$$\begin{aligned} \sigma &= \tau^2\sigma\tau^{-2} \\ &= \tau\tau\sigma\tau^{-1}\tau^{-1} \\ &= \tau\sigma^k\tau^{-1} \\ &= (\tau\sigma\tau^{-1})^k \\ &= \sigma^{k^2}. \end{aligned}$$

Since $\sigma$ has order $p$, this implies $p|k^2 - 1$ or $k^2 \equiv 1 \bmod p$. Therefore $k \equiv 1$ or $k \equiv -1$ modulo $p$. In the first case, $\tau\sigma\tau^{-1} = \sigma$, which means $G$ is abelian. Moreover, the element $\sigma\tau$ has order $2p$, so $G$ is cyclic. In the latter case, $G$ is dihedral. □

What we want to show is that $\mathrm{Gal}(K^{(1)}/\mathbb{Q})$ is necessarily non-abelian, in which case the proposition implies $\mathrm{Gal}(K^{(1)}/\mathbb{Q})$ is isomorphic to $D_{2p}$.

**Proposition 5.1.13.** *In the situation above, Gal$(K^{(1)}/\mathbb{Q})$ is non-abelian.*

*Proof.* Recall $K = \mathbb{Q}(\sqrt{d})$, where $d > 0$, and $K^{(1)}$ is the Hilbert class field of $K$. Suppose $\mathrm{Gal}(K^{(1)}/\mathbb{Q})$ is abelian. By Proposition 5.1.12, this would imply $\mathrm{Gal}(K^{(1)}/\mathbb{Q})$ is cyclic of order $2p$, which means there is a unique subgroup $H \leq \mathrm{Gal}(K^{(1)}/\mathbb{Q})$ of order 2. By the Fundamental Theorem of Galois Theory (Theorem A.3.10), this implies there is a unique subfield $L \subset K^{(1)}$ of index 2, i.e. $[K^{(1)} : L] = 2$.

Now, as $K^{(1)}/K$ is unramified, the primes of $\mathbb{Z}$ which ramify in $K^{(1)}$ are precisely those which ramify in $K$. Let $q$ be such a prime. Then if $\mathfrak{q}$ is a prime of $\mathcal{O}_K$ lying above $q$, we must have $p\mathcal{O}_K = \mathfrak{q}^2$ (Theorem 2.3.48), meaning $e(\mathfrak{q}/q) = 2$. If $\mathfrak{Q}$ is a prime of $\mathcal{O}_{K^{(1)}}$ lying above $p$, then as ramification indices are multiplicative (Proposition 2.3.43), $e(\mathfrak{Q}/q) = 2$. Therefore the inertia group $I(\mathfrak{Q}/q)$ has order two, and so the fixed field of $I(\mathfrak{Q}/q)$ is $L$ (as $L$ is the unique subfield of index 2). By Proposition 2.3.74, $e((\mathfrak{Q} \cap \mathcal{O}_L)/q) = 1$. But this argument holds true for every prime $\mathfrak{Q}$ lying above $q$ in $K^{(1)}$. Therefore $q$ is unramified in $L$. Moreover, this argument holds true for every prime $q$ which ramifies in $K$. As primes of $\mathbb{Z}$ which do not ramify in $K$ will not ramify in $L$ (as they do not ramify in $K^{(1)}$), we find that $L$ becomes an everywhere unramified extension of $\mathbb{Q}$, which contradicts Theorem 2.3.32. Therefore $\mathrm{Gal}(K^{(1)}/\mathbb{Q})$ is non-abelian. □

**Corollary 5.1.14.** *In the same situation as above, Gal$(K^{(1)}/\mathbb{Q}) \cong D_{2p}$.*

*Proof.* This is immediate from Proposition 5.1.12. □

**Corollary 5.1.15.** *If $K = \mathbb{Q}(\sqrt{d})$, with $d > 0$, has class number $p$ for some odd prime $p$, then $K^{(1)}/\mathbb{Q}$ is a totally real field with Galois group $D_{2p}$.*

*Proof.* We have shown everything except that $K^{(1)}$ is totally real. Clearly $K$ is totally real. The extension $K^{(1)}/\mathbb{Q}$ is Galois, and so the embeddings of $K^{(1)}$ are given by the elements of the Galois group (at least when considering $K^{(1)}$ as a subfield of $\mathbb{C}$). If $K^{(1)}$ were not totally real, then complex conjugation would be one embedding of $K^{(1)}$ into $\mathbb{C}$, and hence an automorphism of order 2 in $\mathrm{Gal}(K^{(1)}/K)$ (complex conjugation would fix $K$). But we know $\mathrm{Gal}(K^{(1)}/K)$ has order $p$, which is odd, and so Lagrange's theorems implies there is no element of order 2 as $2 \not| p$. Therefore $K^{(1)}$ is totally real. □

Therefore we have found a totally real extension with Galois group $D_{2p}$. However, all this work is dependent on finding a real quadratic field with class number $p$, and the existence of such fields is not known for all primes $p$. However, using SAGE, it is possible to find examples of various $d$ such that the class number of $\mathbb{Q}(\sqrt{d})$ is prime. In appendix E we provide a few such $d$ for all primes up to 53, with the exception of 31 and 47.

## 5.2 Groups of Odd Order

In this section we prove that all groups of odd order occur as Galois groups of totally real number fields. The term "prove" is used lightly as we rely on two theorems with difficult proofs, which we will not present. One we encountered in the introduction, namely the theorem by Shafarevich which said that all solvable groups occur as Galois groups over $\mathbb{Q}$. The other theorem we need is known as the Feit-Thompson Theorem, found in [18].

**Theorem 5.2.1.** *If $G$ is a finite group of odd order, then $G$ is solvable.*

Utilizing the power of these two theorems, the result we want is immediate.

**Proposition 5.2.2.** *If $G$ is a group of odd order, then $G$ occurs as the Galois group of a totally real field.*

*Proof.* By Theorem 5.2.1 and Theorem 1.0.1, $G$ occurs as the Galois group of some number field $K$. That $K$ must be totally real follows by a similar argument as in the proof of Corollary 5.1.15. Namely, as $K$ is Galois, then when regarding $K$ as a subfield of $\mathbb{C}$, embeddings of $K$ are given by elements of the Galois group. If $K$ were not totally real, then complex conjugation would be an embedding of $K$ into $\mathbb{C}$, and hence an element of $\mathrm{Gal}(K/\mathbb{Q})$, which is of odd order. This contradicts Lagrange's theorem. Therefore $K$ must be totally real. □

# Appendices

# Appendix A

# Fields and Galois Theory

The purpose of this chapter is to serve as a quick reminder of (or very brief introduction to) Field Theory and Galois Theory, including the Fundamental Theorem and the Galois theory of composite extensions. Basic definitions and theorems will be recalled, mostly without proof. The source for most of the statements of these theorems is [17], but any standard text on fields and Galois Theory will have them as well. Basic understanding of groups and rings will be assumed.

## A.1 Fields and Field Extensions

A field can be described as a commutative ring $F$ in which every nonzero element is a unit (i.e. $F^\times = F - \{0\}$). Because of this, a field only has two ideals $\{0\}$ and $F$, because every nonzero ideal must contain the element $1 \in F$, and hence will be all of $F$. The *characteristic* of a field is the smallest integer $p$ such that $p \cdot 1_F = 0$ (and if no such $p$ exists the characteristic is defined to be 0). Also, if the characteristic is finite (i.e. nonzero), then by using the fact that a field has no zero divisors, it is very straightforward to prove that the characteristic must be a prime number.

A standard example of a field which will be central to this thesis is $\mathbb{Q}$, the rational numbers, which has characteristic 0. An example of a field of characteristic $p$ is $\mathbb{Z}/p\mathbb{Z}$, the integers modulo $p$ (written additively). We leave it as an exercise for the reader to verify that it is actually is a field. It has characteristic $p$ because clearly $p \cdot 1 = 0 \bmod p$ and no smaller integer accomplishes this.

This thesis continually utilizes *field extensions*, which we now define.

**Definition A.1.1.** If $K$ is a field which contains a subfield $F$, then $K/F$ is a *field extension.*

A simple example is the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, where

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

A good exercise is to show that this is actually a field. But it is certainly an extension of $\mathbb{Q}$ as it contains $\mathbb{Q}$ as a subfield. The definition is very straightforward and is also very intuitive, but there is another way to view field extensions. Recall the definition of field homomorphism:

**Definition A.1.2.** $\varphi : F \to F'$ is a ***field homomorphism*** if for all $x, y \in F$,

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$, and
2. $\varphi(x \cdot_F y) = \varphi(x) \cdot_{F'} \varphi(y)$.

Note that if $\varphi$ is not the zero map, then these two requirements also force $\varphi(1) = 1$ and $\varphi(0) = 0$. Field homomorphisms can also give rise to field extensiona. For example, consider the homomorphism $i : F \to K$, where $F$ and $K$ are fields. Indeed, all (nonzero) field homomorphisms must be injective. This is because field homomorphisms are also ring homomorphisms, so the kernel must be an ideal of $F$. But the only ideals of a field are the zero ideal and $F$. Since $i(1) = 1$, the kernel cannot be $F$, and so the kernel is $\{0\}$ and hence the homomorphism is injective. The first isomorphism theorem says the image of $F$ under $i$ will be isomorphic to $F$ and a subfield of $K$. So the "containment" which is inherent in the idea of field extensions can be a direct containment, or given in a slightly more indirect manner by a homomorphism.

Observe that the bigger field $K$ is a vector space over the smaller field $F$, which is simple enough to verify provided the scalar multiplication rule is defined. Since elements of $F$ are also elements of $K$ (viewed either directly or through a homomorphism), the element $\alpha \in F$ acts on $x \in K$ as $\alpha \cdot x$, where the multiplication is that of the field $K$. So we do indeed have a vector space. We say that the *degree* of the extension $K/F$, denoted $[K : F]$, is the vector space dimension of $K$ over $F$.

**Theorem A.1.3** (Tower Law)**.** *Suppose $K/L$ and $M/K$ are two field extensions. Then $M/K$ is also an extension of fields and*

$$[M : K] = [M : L][L : K].$$

The proof follows immediately from a consideration of bases of $K/L$ and $M/K$, and combining them in the natural way to get a basis for $M/K$.

**Definition A.1.4.** (i) Suppose $L/K$ is a field extension. An alement $\alpha \in L$ is *algebraic* over $K$ if there exists a polynomial $f \in K[x]$ (not the zero polyomial) such that $f(\alpha) = 0$.

(ii) If $\alpha \in L$ is algebraic over $K$, its *minimal polynomial* is the (unique) monic polynomial $m_\alpha(x) \in K[x]$ of lowest degree such that $m_\alpha(\alpha) = 0$.

For example, take $K = \mathbb{Q}$ and $L = \mathbb{R}$. It is a famous theorem proved by Lindemann that $\pi \in L$ is not algebraic (also called transcendental). However, $\sqrt{2} \in L$ is algebraic since it is a solution of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$.

All of the extensions in this thesis are finite. It is not hard to show that if $L/K$ is a finite extension, then every $\alpha \in L$ is algebraic. Namely, if $n = [L : K]$, then the elements $\{1, \alpha, \ldots, \alpha^n\}$ must have a $K$-dependence relation among them, being a set of $n + 1$ elements of $L$.

One way to build extension fields is by adjoining certain elements. In the example $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, the element $\sqrt{2}$, which is not in $\mathbb{Q}$, is somehow added to $\mathbb{Q}$ and a field is built from it. To make this concept precise, consider the following definition.

**Definition A.1.5.** Suppose $L/K$ is a field extension and $S \subset L$ is any subset. Then $K(S)$ is defined to be the smallest subfield of $L$ which contains both $K$ and $S$. Namely,

$$K(S) = \bigcap_{S \subseteq F \subseteq L} F,$$

the intersection of all subfields of $L$ containing $S$. If $S = \{x_1, \ldots, x_n\}$, then write $K(S) = K(x_1, x_2, \ldots, x_n)$.

Let $K$ be a field, $L/K$ a field extension, and $\alpha \in L$ an element which is algebraic over $K$. Consider the map

$$K[x] \xrightarrow{\phi} K(\alpha)$$

$$x \mapsto \alpha.$$

The reader can verify that this is a surjective ring homomorphism (a field is naturally a ring) and that the kernel is $(m_\alpha(x))$, where $m_\alpha(x) \in K[x]$ is the minimal polynomial of $\alpha$ over $K$. The first isomorphism theorem asserts

$$K[x]/(m_\alpha(x)) \cong K(\alpha).$$

Notice that $m_\alpha(x)$ is an irreducible element of a PID $K[x]$, so it generates a maximal ideal and therefore the quotient is indeed a field. Therefore this isomorphism makes sense. A consequence of this isomorphism is that

$$[K(\alpha) : K] = \deg m_\alpha(x).$$

## A.2 Testing Irreducibility of Polynomials

Before moving on, it will be useful to recall some simple tools for testing the irreducibility of polynomials in $\mathbb{Q}[x]$. First, Gauss' lemma says that a polynomial if $f \in \mathbb{Z}[x]$ is irreducible, then it is also irreducible in $\mathbb{Q}[x]$. We also have:

**Theorem A.2.1.** *Suppose $f \in \mathbb{Z}[x]$ is a monic polynomial and $p \in \mathbb{Z}$ a prime number. If the image of $f$ in $\mathbb{Z}/p\mathbb{Z}[x]$ (given by reduction of coefficients modulo $p$) is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$, then $f$ is irreducible in $\mathbb{Z}[x]$.*

Testing irreducibility modulo a prime $p$, in theory, seems like it should be an easier problem, since there are only finitely many possibilities for factors of $f$. In Chapters 2 and 4 of the main portion of the thesis, we show that factoring polynomials modulo primes provides more interesting information as well. The last useful theorem for irreducibility is the following.

**Theorem A.2.2** (Eisenstein)**.** *Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ and $p$ a prime such that $p|a_i$ for $0 \leq i < n$, $p \not| a_n$, and $p^2 \not| a_0$, then $f$ is irreducible in $\mathbb{Z}[x]$, and hence $\mathbb{Q}[x]$ by Gauss' lemma.*

In fact, most (if not all) of the polynomials discussed in this thesis are monic (i.e. lead coefficient of one), so $a_n = 1$ and we do not have to worry about the condition $p \not| a_n$. An example of an Eisenstein polynomial is $x^5 - 4x + 2$ with prime $p = 2$.

## A.3 Galois Theory

Let $K$ be a field, and $f(x) \in K[x]$ a polynomial. The idea now is to somehow associate a field, which will be an extension of $K$, to $f(x)$. In addition, to each field we would like to assign a group (the Galois group). The right field to "assign" to $f(x)$ turns out to be the smallest field containing all the roots of $f(x)$. This should at least somewhat motivate the following definition.

**Definition A.3.1.** Let $f(x) \in K[x]$ be a polynomial of degree $n$.

(i) The polynomial $f(x)$ *splits* over $K$ if there exist $c, \alpha_1, \ldots, \alpha_n \in K$ (with the $\alpha_i$ not necessarily distinct) such that

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

(ii) An extension $L/K$ is a *splitting field* of $f(x)$ if $f(x)$ splits in $L$ and if $f(x)$ splits in an intermediate field $M$ such that $K \subseteq M \subseteq L$, then $L = M$.

Note that this definition of a splitting field requires not only that $f(x)$ splits in its splitting field, but it must be the smallest field in which the polynomial splits, in that $f(x)$ does not split in any proper subfield. To see why this is important, consider $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Let $L/\mathbb{Q}$ be the extension

$$L = \mathbb{Q}(2^{1/4}) = \{a + b2^{1/4} + c2^{1/2} + d2^{3/4} : a, b, c, d \in \mathbb{Q}\}.$$

Again, it is an exercise to verify the field axioms for $L$. Then $f(x)$ will split in $L$ because $L$ contains the two roots of $f$, namely $\pm\sqrt{2}$. However, it is not the

splitting field because $f(x)$ also splits in $M = \mathbb{Q}(\sqrt{2})$, and $M \subset L$ is a proper containment. As it turns out $M$ is the splitting field, because $[M : \mathbb{Q}] = 2$, and if there were a smaller field in which $f$ split it would have to have degree one, i.e. be $\mathbb{Q}$, which is not the case.

It is a theorem that every polynomial has a splitting field, and this field is unique up to isomorphism. Moreover, the theorem says that the degree of the splitting field of $f(x) \in K[x]$ divides $n!$, where $n = \deg f(x) \in K[x]$. This tells us an equivalent definition would be that the splitting field is the field given by adjoining all the roots of $f(x)$ to $K$. This is the field to associate to a given polynomial.

**Definition A.3.2.** An extension $L/K$ is *normal* if every irreducible polynomial $f(x) \in K[x]$ which has a root in $L$ splits completely in $L$.

At first glance, this may appear to be a very strong condition, since this requires that if $L$ contains a root of any irreducible $f(x)$ then it contains all the roots of $f$. However, this following theorem provides a nice characterization of normal extensions.

**Theorem A.3.3.** *A finite extension $L/K$ is normal if and only if it is the splitting field of some polynomial $f(x) \in K[x]$.*

In particular, all splitting fields discussed in this thesis are normal extensions. As an example, this theorem implies that the extension $\mathbb{Q}(\sqrt{2})$ is normal because it is the splitting field of $x^2 - 2 \in \mathbb{Q}[x]$. An example of an extension which is not normal is

$$L = \mathbb{Q}(2^{1/3}) = \{a + b2^{1/3} + c2^{2/3} : a, b, c \in \mathbb{Q}\}$$

since the polynomial $x^3 - 2 \in \mathbb{Q}[x]$, irreducible by Eisenstein's criterion with $p = 2$, has a root in $L$ but does not split completely in $L$, as the other two roots are complex.

**Definition A.3.4.** Let $f(x) \in K[x]$ be a polynomial of degree $n$ and let $L/K$ a splitting field of $f(x)$.

(i) If $f(x)$ is irreducible over $K$, then $f(x)$ is *separable* if it has $n$ distinct roots in $L$.

(ii) If $f(x)$ is reducible, then $f(x)$ is *separable* if all its irreducible factors are separable.

(iii) If $M/K$ is any extension and $\alpha \in M$, then $\alpha$ is separable over $K$ if it is algebraic over $K$ and its minimal polynomial over $K$ is separable.

(iv) The extension $M/K$ is separable if every $\alpha \in M$ is separable.

The following theorem is also useful.

**Theorem A.3.5.** *If $L/K$ is a finite extension of fields and $K$ has characteristic zero, then $L$ is separable over $K$.*

Another useful fact is that $f(x) \in K[x]$ has a multiple root $\alpha$ if and only if $\alpha$ is a root of both $f(x)$ and $f'(x)$, where $f'(x)$ is the *formal derivative* of $f(x)$, obtained by using the power rule for polynomials learned in calculus. In fact, one can use this fact to prove Theorem A.3.5.

There are inseparable extensions. For example, let $K = \mathbb{F}_p[t]$, the polynomial ring over the field of $p$ elements, and consider $f(x) = x^p - t \in K[x]$. The claim is that $f(x)$ is not separable. The reader can show that $f(x)$ is in fact irreducible over $K[x]$. Assuming this, let $\alpha \in L$ be a root of $f(x)$ in some extension $L/K$. Then since $K$ has characteristic $p$, over $L$,

$$x^p - t = (x - \alpha)^p$$

as

$$(a + b)^p = a^p + b^p$$

in characteristic $p$ fields. So the root $\alpha$ has multiplicity $p$, meaning $f(x)$ is not separable.

The reader can also check that if $L/K$ is separable, then so is any intermediate extension. With all these definitions in hand, we can being discussing Galois theory.

**Definition A.3.6.** If $L/K$ is a field extension, then the *Galois group* of $L/K$, denoted $\mathrm{Gal}(L/K)$, is the group of automorphisms of $L$ which fix $K$ pointwise. That is,

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) : \sigma|_K = id_K\}.$$

It is easily verified that this is indeed a group under composition. There is also the following fact.

textbfFact: If $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma$ takes $\alpha \in L$ to another root of the minimal polynomial of $\alpha$.

*Proof.* Let $m_\alpha(x) \in K[x]$ be the minimal polynomial of $\alpha$, and say $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Then

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

Since $\sigma$ is a field homomorphism and fixes $K$ pointwise,

$$\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \ldots + a_1\sigma(\alpha) + a_0 = \sigma(0) = 0.$$

But this says exactly that $\sigma(\alpha)$ is another root of $m_\alpha(x)$, and hence also has minimal polynomial $m_\alpha(x)$. □

It can also be shown that $|\mathrm{Gal}(L/K)| \leq [L : K]$. However, the most interesting case for this thesis is where there is equality. First a couple of definitions.

**Definition A.3.7.** If $H$ is a subgroup of $\mathrm{Aut}(L)$, where $L/K$ is a field extension, then we define the ***fixed field*** of $H$ to be

$$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Again, one can verify that this is a subfield of $L$.

**Definition A.3.8.** $L/K$ is said to be a ***Galois extension*** if

$$L^{\mathrm{Gal}(L/K)} = K.$$

So for example, $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not a Galois extension. To see this, first notice that the only element in the Galois group is the trivial automorphism (the identity map), since any automorphism $\sigma$ must take $2^{1/3}$ to another root of the minimal polynomial, which is $x^3 - 2$. However, the other two roots are complex, and in particular not in the field $\mathbb{Q}(2^{1/3})$. So $\sigma(2^{1/3}) = 2^{1/3}$, and since this element generates the field, $\sigma$ is just the identity map. Therefore

$$\mathbb{Q}(2^{1/3})^{\mathrm{Gal}(\mathbb{Q}(2^{1/3})/\mathbb{Q})} = \mathbb{Q}(2^{1/3}) \neq \mathbb{Q}.$$

It turns out that in Galois extensions, $|\mathrm{Gal}(L/K)| = [L : K]$.

The next theorem provides arguably the quickest way to check whether a given extension is Galois.

**Theorem A.3.9.** *A finite extension $L/K$ is Galois if and only if it is normal and separable.*

This theorem allows us to say, for example, that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois and $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not, as it is not normal. Also, if the base field is $\mathbb{Q}$ as it is for most of this thesis, every finite extension is separable, so Galois extensions are precisely the splitting fields of polynomials.

Before moving on to the fundamental theorem, a few remarks about the Galois group. If $f(x) \in K[x]$, then the Galois group of a polynomial $\mathrm{Gal}(f)$ is defined to be the Galois group of the splitting field of $f(x)$. Moreover, if $f(x)$ has degree $n$, then since the Galois group merely permutes the roots of $f(x)$, we obtain an embedding of $\mathrm{Gal}(f)$ into $S_n$. Lastly, if $f(x)$ is irreducible, then the Galois group is a transitive subgroup of $S_n$. The proofs of these facts can be found in [17].

The following theorem is known as the Fundamental Theorem of Galois theory.

**Theorem A.3.10.** *Suppose $L/K$ is a finite Galois extension with $G = Gal(L/K)$. Then*

*(i) There is an inclusion-reversing bijection, the "Galois correspondence," between subgroups $H$ of $G$ and intermediate field extensions $K \subseteq M \subseteq L$ given by*

$$H \to L^H$$

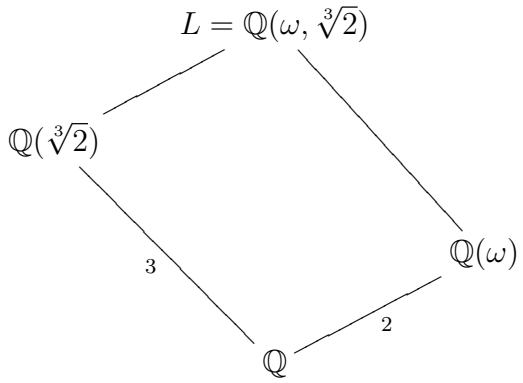
$$Gal(L/M) \leftarrow M$$

*with $[L : M] = |Gal(L/M)|$ and $[L : L^H] = |H|$.*

*(ii) If $M$ is an intermediate extension, then $M/K$ is a Galois extension if and only if $Gal(L/M) \triangleleft Gal(L/K)$, in which case $Gal(M/K) \cong G/Gal(L/M)$.*

It is important to note that the finiteness condition on the degree of the extension is critical. There is a similar statement about infinite Galois extensions, but it is not presented here.

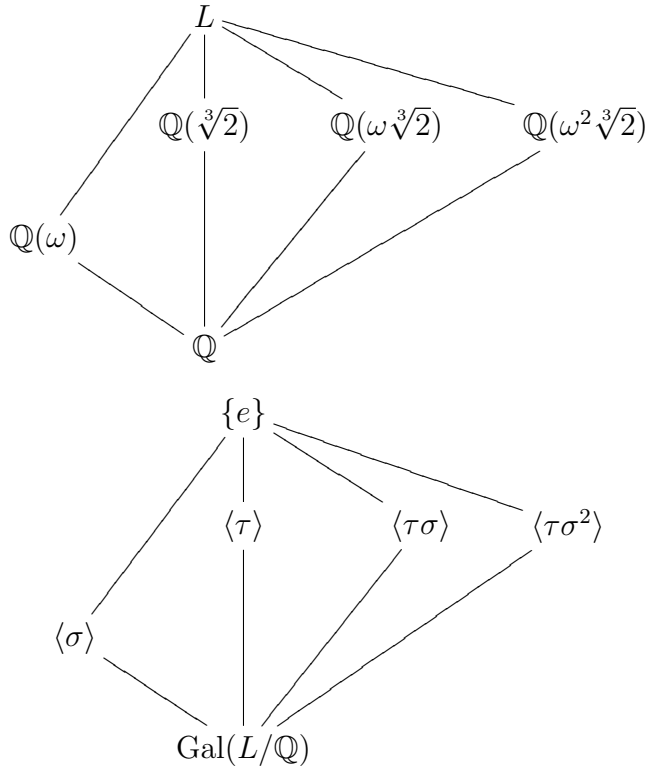
**Example A.3.11.** Consider the polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. It is easily verified that the splitting field of this polynomial is $L = \mathbb{Q}(\omega, \sqrt[3]{2})$, where $\omega$ is a cube root of unity, since any splitting field must contain both $\omega$ and $\sqrt[3]{2}$. The size of the Galois group $\mathrm{Gal}(L/K)$ is $[L : K]$, which we now calculate. First observe that the minimal polynomial of $\omega$ is $x^2 + x + 1 \in \mathbb{Q}[x]$, which is irreducible over $\mathbb{Q}$ as it has no roots in $\mathbb{Q}$. We have the following diagram:




In particular, $3|[L : \mathbb{Q}]$ and $2|[L : \mathbb{Q}]$, meaning $6|[L : \mathbb{Q}]$. However, as stated in the discussion on splitting fields, $[L : \mathbb{Q}]|3! = 6$, so $6|[L : K]|6$. Hence $[L : \mathbb{Q}] = 6$, and $|\mathrm{Gal}(L/\mathbb{Q})| = 6$. As $f(x)$ is a cubic polynomial, $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of $S_3$, which has order 6, meaning $\mathrm{Gal}(L/\mathbb{Q})$ must be all of $S_3$. Therefore $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. Elements of $\mathrm{Gal}(L/\mathbb{Q})$ are realized in the following way. Automorphisms in $\mathrm{Gal}(L/\mathbb{Q})$ are uniquely determined by their action on $\omega$ and $\sqrt[3]{2}$, and any automorphism must send these elements to other roots of their respective minimal polynomials. Let $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ be the element which takes $\omega \mapsto \omega^2$ and leaves $\sqrt[3]{2}$ fixed. Then let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ be the elemt which maps $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ and leaves $\omega$ fixed. Both $\sigma$ and $\tau$ can be regarded as elements of $S_3$ by enumerating the roots $r_1 = \sqrt[3]{2}$, $r_2 = \omega\sqrt[3]{2}$ and $r_3 = \omega^2\sqrt[3]{2}$ of $f(x)$ in $L$. The

element $\tau$ fixes $r_1$ and interchanges $r_2$ and $r_3$, so $\tau$ corresponds to the transposition $(2,3) \in S_3$. Similarly, the element $\sigma$ sends $r_1$ to $r_2$, maps $r_2$ to $r_3$, and lastly takes $r_3$ to $r_1$, so $\sigma$ is realized as the 3-cycle $(1,2,3)$. Since $S_3$ is generated by a transposition and a 3-cycle, $\sigma$ and $\tau$ generate $\mathrm{Gal}(L/\mathbb{Q})$.

Now to illustrate the fundamental theorem, notice there are four nontrivial proper subgroups of $S_3$: there is $A_3$, which is the subgroup generated by the 3-cycle $\sigma$, and the three subgroups of order 2 generated by the 3 distinct transpositions $\tau, \tau\sigma, \tau\sigma^2$. So consider the first subgroup $A_3$, or the subgroup generated by $\sigma$, and let $M_1$ be the corresponding subfield of $L$. Then $M_1 = L^{\langle\sigma\rangle}$. It is clear from the definition of $\sigma$ that elements of $\mathbb{Q}(\omega)$ will be fixed by $\sigma$. Therefore $\mathbb{Q}(\omega) \subseteq M_1$. However, the fundamental theorem also tells us that $[L : M_1] = |\langle\sigma\rangle| = 3$, and we know from the diagram above that $[L : \mathbb{Q}(\omega)] = 6/2 = 3$, so by comparing dimensions $M_1 = \mathbb{Q}(\omega)$. In a very similar manner, one can verify that the fixed field of $\langle\tau\rangle$ is $\mathbb{Q}(\sqrt[3]{2})$, the fixed field of $\langle\tau\sigma\rangle$ is $\mathbb{Q}(\omega\sqrt[3]{2})$ and the fixed field of $\langle\tau\sigma^2\rangle$ is $\mathbb{Q}(\omega^2\sqrt[3]{2})$. Displaying this in diagram form, we have the following lattices:




## A.4 Composite Extensions

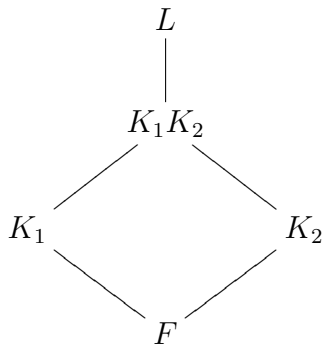
The source for this section will be [19]. Recall the definition of the compositum of fields.

**Definition A.4.1.** Suppose $K_1$ and $K_2$ are subfields of $L$, where $L$ is a field extension over a ground field $F$. Then the compositum of $K_1$ and $K_2$, denoted $K_1K_2$, is the smallest subfield of $L$ which contains both $K_1$ and $K_2$.

*Remark* A.4.2. The composite extension does exist, as one could take the intersection of all subfields of $L$ which contain both $K_1$ and $K_2$. Namely,

$$K_1K_2 = \bigcap_{K_1,K_2 \subseteq K \subseteq L} K.$$

The field diagram for the composite extension looks like this:




**Example A.4.3.** Consider $K_1 = \mathbb{Q}(\sqrt{2})$ and $K_2 = \mathbb{Q}(\sqrt{3})$, where both are regarded as subfields of $\mathbb{C}/\mathbb{Q}$ (or $\mathbb{R}/\mathbb{Q}$). Then $K_1K_2$ is the smallest field which contains $K_1$ and $K_2$. The claim is that $K_1K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Clearly $K_1K_2 \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, as $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ contains both $K_1$ and $K_2$. Conversely, the compositum must contain $\sqrt{2}$ and $\sqrt{3}$. By definition, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the smallest field over $\mathbb{Q}$ which contains both of these elements, and therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq K_1K_2$. Hence we have equality.

A natural question to ask is when is $K_1K_2$ Galois over, say $K_1$? The answer to that question is provided by the following theorem.

**Theorem A.4.4.** *Suppose $K_2$ is a finite Galois extension of $K_1 \cap K_2$. Then $K_1K_2$ is a (finite) Galois extension of $K_1$ and there is an isomorphism*

$$Gal(K_1K_2/K_1) \cong Gal(K_2/K_1 \cap K_2),$$

*where $\sigma \mapsto \sigma|_{K_2}$.*

Notice that the hypothesis of the theorem make no mention of $K_1$ as an extension of $K_1 \cap K_2$. As a simple consquence of this, we get the following corollary.

**Corollary A.4.5.** *If $K_2$ is a (finite) Galois extension of $K_1 \cap K_2$, then*

*(a)* $[K_1K_2 : K_1] = [K_2 : K_1 \cap K_2]$,

*(b)* $[K_1K_2 : K_2] = [K_1 : K_1 \cap K_2]$,

*(c)* $[K_1K_2 : K_1 \cap K_2] = [K_1 : K_1 \cap K_2][K_2 : K_1 \cap K_2]$.

*Proof.* Item (a) follows from the theorem since $|\mathrm{Gal}(K_1K_2/K_1)| = [K_1K_2 : K_1]$ and $|\mathrm{Gal}(K_2/K_1 \cap K_2)| = [K_2 : K_1 \cap K_2]$. Now notice that

$$[K_1K_2 : K_2][K_2 : K_1 \cap K_2] = [K_1K_2 : K_1 \cap K_2] = [K_1K_2 : K_1][K_1 : K_1 \cap K_2].$$

Using (a) with the right equality gives (c). Then using the left equality with (c) yields (b). □

Recall that $K_1$ and $K_2$ are called *disjoint* if $K_1 \cap K_2 = F$. In this case, we have:

**Corollary A.4.6.** *$K_1$ and $K_2$ are disjoint extensions if and only if $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.*

*Proof.* The "only if" direction follows immediately from the previous corollary. For the "if" direction, notice that

$$\begin{aligned}
[K_1 : F][K_2 : F] &= [K_1 : K_1 \cap K_2][K_1 \cap K_2 : F][K_2 : K_1 \cap K_2][K_1 \cap K_2 : F] \\
&= [K_1K_2 : K_1 \cap K_2][K_1 \cap K_2 : F]^2 \quad \text{(using (c) of previous corollary)} \\
&= [K_1K_2 : F][K_1 \cap K_2 : F].
\end{aligned}$$

Therefore, to get the equality

$$[K_1 : F][K_2 : F] = [K_1K_2 : F],$$

we must have $[K_1 \cap K_2 : F] = 1$, meaning $K_1 \cap K_2 = F$. Therefore $K_1$ and $K_2$ are disjoint. □

The last theorem needed is Theorem A.4.4 in the case of disjoint extensions.

**Theorem A.4.7.** *If $K_1$ and $K_2$ are disjoint extensions, then there is an isomorphism*

$$\mathit{Gal}(K_1K_2/F) \cong \mathit{Gal}(K_1/F) \times \mathit{Gal}(K_2/F),$$

*where the isomorphism is given by $\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$.*

Of course, we would like to also find an equivalent theorem for the composite of more than two fields. For example, suppose we wanted

$$\mathrm{Gal}(K_1K_2K_3/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \times \mathrm{Gal}(K_3/F).$$

Just having the $K_i$ pairwise disjoint will not suffice. Think back to linear algebra. If we had $V$ is a finite dimensional vector space and $V_1, \ldots, V_k$ subspaces of $V$, then in order to say that

$$V = V_1 \oplus \cdots \oplus V_k,$$

one condition which had to be satisfied was

$$V_i \cap \sum_{j \neq i} V_j = \{0\}$$

for all $i$. In this setting, just having $V_i \cap V_j = \{0\}$ for $j \neq i$ was not enough. Similarly, the condition we need is not pairwise disjointness, but rather

$$K_i \cap \prod_{j \neq i} K_j = F$$

for all $i$, where $F$ is still the ground field. So the generalization of the previous theorem is:

**Theorem A.4.8.** *Suppose $K_i/F$ are all subfields of $L/F$, $1 \leq i \leq n$, and each $K_i$ is Galois over $F$. If*

$$K_i \cap \prod_{j \neq i} K_j = F$$

*for all $1 \leq i \leq n$, then*

$$Gal(K_1 \cdots K_n/F) \cong Gal(K_1/F) \times Gal(K_2/F) \times \cdots \times Gal(K_n/F).$$

**Example A.4.9.** Consider the example presented earlier, namely $K_1 = \mathbb{Q}(\sqrt{2})$ and $K_2 = \mathbb{Q}(\sqrt{3})$. We found $K_1K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. A good exercise for the reader is to verify that $\mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathrm{Gal}(K_2/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. Notice that $K_1 \cap K_2 = \mathbb{Q}$. To see why, notice that $\mathbb{Q} \subseteq K_1 \cap K_2 \subseteq K_1$. But since $[K_1 : \mathbb{Q}] = 2$, either $K_1 \cap K_2 = \mathbb{Q}$ or $K_1 \cap K_2 = K_1$. The latter would imply that $K_1 \subseteq K_2$, which is a clear contradiction as the reader can easily show that $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$. Therefore $K_1$ and $K_2$ are disjoint extensions and the theorem says

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The theory of composite extensions is used extensively in Chapter 3.

# Appendix B

# Galois Theory of Finite Fields

Even though number fields are finite extensions of $\mathbb{Q}$, which has characteristic 0, many theorems and results make use of finite fields. Again, we do not wish to prove every result, so we will mainly be stating theorems (from [5] and [17]). However, we do prove a couple of results related to the Galois groups of finite fields.

## B.1 Existence and Uniqueness

Recall first that a finite field must have prime characteristic, as all characteristic zero fields are necessarily infinite. So let $\mathbb{F}$ be a finite field of characteristic $p$. Recall that the *prime subfield* of $\mathbb{F}$ is the intersection of all subfields of $\mathbb{F}$. Alternatively, it is the subfield generated by the element $1 \in F$. In characteristic $p$, the prime subfield of $\mathbb{F}$ is isomorphic to $\mathbb{F}_p$, the field of $p$ elements. Since $\mathbb{F}$ is finite, it is a finite extension over its prime subfield. If the degree of the extension $[\mathbb{F} : \mathbb{F}_p] = r$, then as $\mathbb{F}$ is a vector space of dimension $r$ over $\mathbb{F}_p$, it has $p^r$ elements. Moreover, as is proved in [5], $\mathbb{F}$ is the splitting field of the polynomial

$$f(x) = x^{p^r} - x \in \mathbb{F}_p[x],$$

which is the key step in the proof of following theorem.

**Theorem B.1.1.** *If $n$ is a positive integer and $p$ is a prime number, then there exists a finite field of cardinality $p^n$, and it is unique up to isomorphism.*

## B.2 Normal and Separable

Of course, as is the case throughout this thesis, we want to study field extensions. In this case, consider $\mathbb{F}/\mathbb{F}_q$, where $\mathbb{F}$ is a finite extension of the finite field $\mathbb{F}_q$, the field of $q$ elements. As seen above, $q = p^r$ for $p = \text{char}(\mathbb{F}_q)$ and some $r \geq 1$. As it turns out, if $[\mathbb{F} : \mathbb{F}_q] = d$, then $|\mathbb{F}| = q^d$, and moreover $\mathbb{F}$ is the splitting field of

$$f(x) = x^{q^d} - x \in \mathbb{F}_q[x],$$

which means $\mathbb{F}$ is a normal extension of $\mathbb{F}_q$. Therefore every finite extension of a finite field is normal, which is certainly a useful fact. If these extensions were also separable, then every finite extension of a finite field would be Galois, and thus the Galois theory discussed in appendix A could be applied to this situation.

The following proposition gives us the desired fact. See [5], Section 13.5, for a proof.

**Proposition B.2.1.** *Every irreducible polynomial over a finite field $\mathbb{F}$ is separable. Moreover, a polynomial in $\mathbb{F}[x]$ is separable if and only if it is the product of distinct irreducible polynomials in $\mathbb{F}[x]$.*

To see why this makes every extension separable, suppose $\mathbb{F}/\mathbb{F}_q$ is a finite extension of finite fields, where $q = p^r$ as before. Take $\alpha \in \mathbb{F}$. Then the minimal polynomial $m_\alpha(x) \in \mathbb{F}_q[x]$ over $\mathbb{F}_q$ is irreducible, and by the proposition it is therefore separable. By definition, this implies $\mathbb{F}/\mathbb{F}_q$ is separable. Thus we get the following.

**Proposition B.2.2.** *If $E/F$ is a finite extension of finite fields, then $E/F$ is Galois.*

## B.3 Galois group

Again, let $\mathbb{F}/\mathbb{F}_q$ be a finite extension of finite fields, where, as before, $q = p^r$ for some $r$ and $p = \text{char}(\mathbb{F}_q)$. If we let $[\mathbb{F} : \mathbb{F}_q] = d$, then $|\mathbb{F}| = q^d$. The previous proposition showed that $\mathbb{F}/\mathbb{F}_q$ is a Galois extension. Now we want to determine $\text{Gal}(\mathbb{F}/\mathbb{F}_q)$.

Consider the map

$$\varphi : \mathbb{F} \to \mathbb{F}, \quad \alpha \mapsto \alpha^q.$$

First, let us show that $\varphi$ is a field homomorphism. Clearly $\varphi(1) = 1$, $\varphi(0) = 0$, and $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ for $\alpha, \beta \in \mathbb{F}$. Thus we only need to show that addition is preserved.

Consider $(\alpha + \beta)^p$ for $\alpha, \beta \in F$. Remember that $\mathbb{F}$ has characteristic $p$. Consider the binomial coefficient $\binom{p}{i}$, for $1 \leq i \leq p-1$. This is precisely

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

Since $i, p - i < p$, no factor in the denominator can cancel the factor of $p$ in the numerator, and hence $p \Big| \binom{p}{i}$ for $1 \leq i \leq p-1$. As we are in a commutative setting, the binomial theorem holds, and since we are in characteristic $p$,

$$(\alpha + \beta)^p = \alpha^p + \beta^p.$$

An easy inductive argument shows that

$$(\alpha + \beta)^{p^r} = \alpha^{p^r} + \beta^{p^r},$$

which says precisely that

$$(\alpha + \beta)^q = \alpha^q + \beta^q.$$

Therefore $\varphi$ is in fact a field homomorphism. Since it is not the zero map, it is injective. But an injective map from a finite set to itself is surjective. Therefore $\varphi$ is an automorphism of $\mathbb{F}$.

But now consider $\mathbb{F}_q^\times$, the multiplicative group of $\mathbb{F}_q$. This has order $q-1$, and so by Lagrange's theorem, $a^{q-1} = 1$ for all $a \in \mathbb{F}_q^\times$. But this clearly implies $a^q = a$ for all $a \in \mathbb{F}_q$ (as 0 is the only element not in $\mathbb{F}_q^\times$). Therefore $\varphi$ fixes $\mathbb{F}_q$ elementwise, which implies $\varphi \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$.

Next we calculate the order of $\varphi$. By the same reasoning used above with $\mathbb{F}_q$, $\alpha^{q^d} = \alpha$ for all $\alpha \in \mathbb{F}$. Therefore $\varphi^d = e$, the identity element in $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. However, $\varphi$ cannot have order smaller than $d$, since then this would mean

$$\alpha^{q^i} = \alpha,$$

for some $i < d$ and all $\alpha \in \mathbb{F}$. This is a contradiction since this would imply there are $q^d$ roots of the polynomial

$$x^{q^i} - x \in \mathbb{F}_q[x],$$

which has degree strictly less than $q^d$. Therefore $\varphi$ has order $d$ and so generates $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. This proves the following theorem.

**Theorem B.3.1.** *If $\mathbb{F}/\mathbb{F}_q$ is a finite extension of finite fields, where $q = p^r$ and $p = char(\mathbb{F}_q)$, then $|Gal(\mathbb{F}/\mathbb{F}_q)| = [\mathbb{F} : \mathbb{F}_q]$, and the group is generated by the* Frobenius automorphism

$$\varphi : \mathbb{F} \to \mathbb{F}, \quad \alpha \mapsto \alpha^q.$$

# Appendix C

# Cyclotomic Fields

Like with the previous two appendices, we will not prove every detail here.

Consider the polynomial $f(x) = x^n - 1 \in \mathbb{Q}[x]$, and let $K$ denote a splitting field over $\mathbb{Q}$. Over $\mathbb{C}$, the roots of this polynomial are the $n$-th roots of unity, i.e. $\alpha \in \mathbb{C}$ such that $\alpha^n = 1$. Choose $\zeta_n$ to be a *primitive* $n$-th root of unity, meaning $\zeta_n^n = 1$ but $\zeta_n^m \neq 1$ for $0 < m < n$. For example, one could take $\zeta_n = e^{2\pi i/n}$. Then it is easy to see that $\zeta_n^k$ are roots of $f(x)$ for $0 \leq k < n$, which means $f(x)$ has all its roots in $K = \mathbb{Q}(\zeta_n)$. Since any splitting field, regarded as a subfield of $\mathbb{C}$, must contain $\zeta_n$, $K$ is the splitting field for $f(x)$ over $\mathbb{Q}$. We refer to $K$ as a *cyclotomic field*. This also means $K/\mathbb{Q}$ is Galois, as it is normal, being the splitting field of a polynomial, and separable, as all finite extensions of characteristic zero fields are separable by Theorem A.3.5.

Notice that not every power of $\zeta_n$ need be a primitive $n$-th root of unity. For example, the fourth roots of unity are $\{i, -1, -i, 1\}$. Though it is a fourth root of unity, $-1$ is a primitive second root of unity as $(-1)^2 = 1$. The primitive fourth roots of unity are $\pm i$. So an primitive $n$-th root of unity is one where it is not a $d$-th root of unity for any proper divisor $d|n$. We can ask how many powers of $\zeta_n$, say $\zeta_n^k$ with $0 < k < n$, are primitive $n$-th roots of unity? We leave it to the reader to verify that $\zeta_n^k$ will be a primitive $n$-th root of unity if and only if $(k, n) = 1$. Therefore the number of primitive $n$-th roots of unity is $\varphi(n)$, where $\varphi(n)$ is the number of natural numbers $\leq n$ which are relatively prime to $n$.

Next, we would like the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.

**Theorem C.0.2.** *If $\zeta_n$ is a primitive $n$-th root of unity, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*

Since we know the degree cyclotomic extensions and that they are Galois, we can try and determine the structure of the Galois group.

**Theorem C.0.3.** *Suppose $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n$ is a primitive $n$-th root of unity. Then $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

*Sketch of proof.* Any automorphism of $K$ is determined uniquely by where it sends $\zeta_n$. Moreover, it must send $\zeta_n$ to another primitive $n$-th root of unity. Since the other primitive roots are also roots of the minimal polynomial of $\zeta_n$ over $\mathbb{Q}$, there are $\varphi(n)$ choices to choose from. Moreover, they are given by

$$\zeta_n^k, \quad 1 \leq k \leq n, (k,n) = 1.$$

So we can define a homomorphism

$$\phi : \mathrm{Gal}(K/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times,$$

where $\sigma : \zeta_n \mapsto \zeta_n^{\phi(\sigma)}$. One checks that it is injective homomorphism. Since the sizes of both the domain and target space are equal, $\phi$ is a surjection, and hence an isomoprhism. □

For those who desire a more thorough development of cyclotomic fields, see [5], section 13.6.

# Appendix D

# Explicit Polynomials: Abelian Case

In this appendix, for abelian groups $G$ of order up to 20, we present polynomials whose splitting field is totally real and with Galois group isomorphic to $G$. Using the methods presented in chapter 3 of the thesis, we were able to implement a simple program in SAGE which output the desired polynomial. In addition, we also used SAGE to find the primes which ramified and split completely in these extensions (namely, the splitting fields for the polynomials given in the first table).

We could not use the method to compute the polynomial with Galois group

$$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

and this was due to the inability of SAGE to compute the polynomial in reasonable time. However, the methods presented in Chapter 3 still apply to this group. If one actually wanted a polynomial with Galois group $G$, it can be checked that

$$f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)(x^2 - 7)$$

has the required Galois group, and since all its roots are real its splitting field $K$ is a totally real number field with Galois group $G$.

The first table gives the polynomials for each group, and the second table describes the factoring of primes in the splitting fields for the polynomials in the first table.

| Explicit Polynomials for Abelian Groups of Small Order | | |
|---|---|---|
| $n$ | Group | Polynomial |
| 2 | $\mathbb{Z}/2\mathbb{Z}$ | $x^2+x-1$ |
| 3 | $\mathbb{Z}/3\mathbb{Z}$ | $x^3+x^2-2x-1$ |
| 4 | $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ | $x^4-x^3-10x^2-3x+9$ |
| | $\mathbb{Z}/4\mathbb{Z}$ | $x^4+x^3-6x^2-x+1$ |
| 5 | $\mathbb{Z}/5\mathbb{Z}$ | $x^5+x^4-4x^3-3x^2+3x+1$ |
| 6 | $\mathbb{Z}/6\mathbb{Z}$ | $x^6+x^5-5x^4-4x^3+6x^2+3x-1$ |
| 7 | $\mathbb{Z}/7\mathbb{Z}$ | $x^7+x^6-12x^5-7x^4+28x^3+14x^2-9x+1$ |
| 8 | $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ | $x^8+x^7-94x^6+79x^5+1933x^4-948x^3-13536x^2-1728x+20736$ |
| | $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ | $x^8-x^7-19x^6-2x^5+46x^4-2x^3-19x^2-x+1$ |
| | $\mathbb{Z}/8\mathbb{Z}$ | $x^8+x^7-7x^6-6x^5+15x^4+10x^3-10x^2-4x+1$ |
| 9 | $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ | $x^9-x^8-22x^7+x^6+91x^5-11x^4-71x^3-10x^2+8x+1$ |
| | $\mathbb{Z}/9\mathbb{Z}$ | $x^9+x^8-8x^7-7x^6+21x^5+15x^4-20x^3-10x^2+5x+1$ |
| 10 | $\mathbb{Z}/10\mathbb{Z}$ | $x^{10}+x^9-18x^8-13x^7+91x^6+47x^5-143x^4-7x^3+72x^2-23x+1$ |
| 11 | $\mathbb{Z}/11\mathbb{Z}$ | $x^{11}+x^{10}-10x^9-9x^8+36x^7+28x^6-56x^5-35x^4+35x^3+15x^2-6x-1$ |
| 12 | $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ | $x^{12}-x^{11}-16x^{10}+11x^9+79x^8-29x^7-145x^6+25x^5+107x^4$ $-2x^3-27x^2-3x+1$ |
| | $\mathbb{Z}/12\mathbb{Z}$ | $x^{12}+x^{11}-33x^{10}-70x^9+288x^8+929x^7-298x^6-3421x^5-2921x^4$ $+1195x^3+1718x^2-162x-211$ |
| 13 | $\mathbb{Z}/13\mathbb{Z}$ | $x^{13}+x^{12}-24x^{11}-19x^{10}+190x^9+116x^8-601x^7-246x^6+738x^5$ $+215x^4-291x^3-68x^2+10x+1$ |
| 14 | $\mathbb{Z}/14\mathbb{Z}$ | $x^{14}+x^{13}-13x^{12}-12x^{11}+66x^{10}+55x^9-165x^8-120x^7+210x^6+126x^5$ $-126x^4-56x^3+28x^2+7x-1$ |
| 15 | $\mathbb{Z}/15\mathbb{Z}$ | $x^{15}+x^{14}-14x^{13}-13x^{12}+78x^{11}+66x^{10}-220x^9-165x^8+330x^7+210x^6$ $-252x^5-126x^4+84x^3+28x^2-8x-1$ |
| 16 | $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ | $x^{16}+x^{15}-136x^{14}+77x^{13}+4633x^{12}-1600x^{11}-58282x^{10}-2090x^9$ $+271696x^8+6270x^7-524538x^6+43200x^5+375273x^4-18711x^3$ $-99144x^2-2187x+6561$ |
| | $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ | $x^{16}-x^{15}-201x^{14}-332x^{13}+7406x^{12}+9254x^{11}-77575x^{10}$ $-62969x^9+268627x^8+186178x^7-293220x^6-150432x^5+125056x^4$ $+35264x^3-18624x^2-1152x+256$ |
| | $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ | $x^{16}-x^{15}-22x^{14}+17x^{13}+172x^{12}-92x^{11}-601x^{10}+196x^9+1014x^8$ $-189x^7-844x^6+74x^5+325x^4-46x^2-4x+1$ |
| | $\mathbb{Z}/16\mathbb{Z}$ | $x^{16}+x^{15}-45x^{14}-98x^{13}+650x^{12}+2183x^{11}-2576x^{10}-17205x^9-9748x^8$ $+44003x^7+63779x^6-18576x^5-86644x^4-43324x^3$ $+15475x^2+17690x+3721$ |
| 17 | $\mathbb{Z}/17\mathbb{Z}$ | $x^{17}+x^{16}-48x^{15}-105x^{14}+763x^{13}+2579x^{12}-3653x^{11}-23311x^{10}$ $-11031x^9+74838x^8+107759x^7-50288x^6-198615x^5-102976x^4$ $+58507x^3+75722x^2+25763x+2837$ |
| 18 | $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ | $x^{18}-x^{17}-27x^{16}+22x^{15}+269x^{14}-180x^{13}-1259x^{12}+711x^{11}+2914x^{10}$ $-1420x^9-3300x^8+1287x^7+1831x^6-522x^5-466x^4+89x^3+45x^2-6x-1$ |
| | $\mathbb{Z}/18\mathbb{Z}$ | $x^{18}+x^{17}-17x^{16}-16x^{15}+120x^{14}+105x^{13}-455x^{12}-364x^{11}+1001x^{10}$ $+715x^9-1287x^8-792x^7+924x^6+462x^5-330x^4-120x^3+45x^2+9x-1$ |
| 19 | $\mathbb{Z}/19\mathbb{Z}$ | $x^{19}+x^{18}-90x^{17}-57x^{16}+3044x^{15}+1124x^{14}-51184x^{13}-4822x^{12}$ $+474003x^{11}-90110x^{10}-2465084x^9+1153239x^8+6854098x^7-5023125x^6$ $-8711114x^5+8950277x^4+2600136x^3-5125792x^2+1553447x-117649$ |
| 20 | $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ | $x^{20}-x^{19}-55x^{18}+34x^{17}+1000x^{16}-387x^{15}-7986x^{14}+831x^{13}+31642x^{12}$ $+5609x^{11}-64009x^{10}-26399x^9+61072x^8+35181x^7-21732x^6$ $-13143x^5+3700x^4+1628x^3-313x^2-23x+1$ |
| | $\mathbb{Z}/20\mathbb{Z}$ | $x^{20}+x^{19}-19x^{18}-18x^{17}+153x^{16}+136x^{15}-680x^{14}-560x^{13}$ $+1820x^{12}+1365x^{11}-3003x^{10}-2002x^9+3003x^8+1716x^7$ $-1716x^6-792x^5+495x^4+165x^3-55x^2-10x+1$ |

| Factoring Primes in Extensions | | | |
|---|---|---|---|
| | | Factoring Primes | |
| $n$ | Group | Ramified | Split Completely |
| 2 | $\mathbb{Z}/2\mathbb{Z}$ | 5 | $p \equiv 1, 4 \bmod 5$ |
| 3 | $\mathbb{Z}/3\mathbb{Z}$ | 7 | $p \equiv 1, 6 \bmod 7$ |
| 4 | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | 5, 13 | $p \equiv 1, 4, 9, 14, 16, 29, 36, 49, 51, 56, 61, 64 \bmod 65$ |
| | $\mathbb{Z}/4\mathbb{Z}$ | 17 | $p \equiv 1, 4, 13, 16 \bmod 17$ |
| 5 | $\mathbb{Z}/5\mathbb{Z}$ | 11 | $p \equiv 1, 10 \bmod 11$ |
| 6 | $\mathbb{Z}/6\mathbb{Z}$ | 13 | $p \equiv 1, 12 \bmod 13$ |
| 7 | $\mathbb{Z}/7\mathbb{Z}$ | 29 | $p \equiv 1, 12, 17, 28 \bmod 29$ |
| 8 | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | 5, 13, 17 | $p \equiv 1, 4, 9, 16, 36, 49, 64, 66, 69, 81, 94, 101, 121, 134, 144, 166, 179,$ $186, 191, 196, 246, 251, 256, 259, 264, 274, 276, 321, 324, 339, 341, 361,$ $376, 389, 399, 404, 406, 426, 441, 446, 451, 484, 491, 506, 511, 519, 529,$ $536, 569, 576, 586, 594, 599, 614, 621, 654, 659, 664, 679, 699, 701,$ $706, 716, 729, 744, 764, 766, 781, 784, 829, 831, 841, 846, 849, 854, 859,$ $909, 914, 919, 926, 939, 961, 971, 984, 1004, 1011, 1024, 1036, 1039,$ $1041, 1056, 1069, 1089, 1096, 1101, 1104 \bmod 1105$ |
| | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | 5, 17 | $p \equiv 1, 4, 16, 21, 64, 69, 81, 84 \bmod 85$ |
| | $\mathbb{Z}/8\mathbb{Z}$ | 17 | $p \equiv 1, 16 \bmod 17$ |
| 9 | $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ | 7, 13 | $p \equiv 1, 8, 27, 34, 57, 64, 83, 90 \bmod 91$ |
| | $\mathbb{Z}/9\mathbb{Z}$ | 19 | $p \equiv 1, 18 \bmod 19$ |
| 10 | $\mathbb{Z}/10\mathbb{Z}$ | 41 | $p \equiv 1, 9, 32, 40 \bmod 41$ |
| 11 | $\mathbb{Z}/11\mathbb{Z}$ | 23 | $p \equiv 1, 22 \bmod 23$ |
| 12 | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | 5, 13 | $p \equiv 1, 14, 51, 64 \bmod 65$ |
| | $\mathbb{Z}/12\mathbb{Z}$ | 73 | $p \equiv 1, 8, 9, 64, 65, 72 \bmod 73$ |
| 13 | $\mathbb{Z}/13\mathbb{Z}$ | 53 | $p \equiv 1, 23, 30, 52 \bmod 53$ |
| 14 | $\mathbb{Z}/14\mathbb{Z}$ | 29 | $p \equiv 1, 28 \bmod 29$ |
| 15 | $\mathbb{Z}/15\mathbb{Z}$ | 31 | $p \equiv 1, 30 \bmod 31$ |
| 16 | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | 5, 13, 17 | $p \equiv 1, 4, 16, 64, 69, 81, 101, 166, 186, 191, 251, 256, 259, 276, 324,$ $339, 341, 361, 404, 426, 441, 446, 506, 511, 594, 599, 659, 664,$ $679, 701, 744, 764, 766, 781, 829, 846, 849, 854, 914, 919, 939, 1004,$ $1024, 1036, 1041, 1089, 1101, 1104 \bmod 1105$ |
| | $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | 17, 41 | $p \equiv 1, 4, 16, 18, 64, 72, 81, 86, 98, 154, 174, 242, 256, 271,$ $288, 305, 310, 324, 327, 344, 353, 370, 373, 387, 392, 409, 426,$ $441, 455, 523, 543, 599, 611, 616, 625, 633, 679, 681, 693, 696 \bmod 697$ |
| | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | 5, 17 | $p \equiv 1, 16, 69, 84 \bmod 85$ |
| | $\mathbb{Z}/16\mathbb{Z}$ | 97 | $p \equiv 1, 35, 36, 61, 62, 96 \bmod 97$ |
| 17 | $\mathbb{Z}/17\mathbb{Z}$ | 103 | $p \equiv 1, 46, 47, 56, 57, 102 \bmod 103$ |
| 18 | $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | 7, 13 | $p \equiv 1, 27, 64, 90 \bmod 91$ |
| | $\mathbb{Z}/18\mathbb{Z}$ | 37 | $p \equiv 1, 36 \bmod 37$ |
| 19 | $\mathbb{Z}/19\mathbb{Z}$ | 191 | $p \equiv 1, 7, 39, 49, 82, 109, 142, 152, 184, 190 \bmod 191$ |
| 20 | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ | 5, 41 | $p \equiv 1, 9, 81, 91, 114, 124, 196, 204 \bmod 205$ |
| | $\mathbb{Z}/20\mathbb{Z}$ | 41 | $p \equiv 1, 40 \bmod 41$ |

# Appendix E

# Examples: Dihedral Groups

In Chapter 5 we proved (with some details omitted) that if $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field (i.e. $d > 0$) with class number $p$, an odd prime, then the Hilbert class field of $K$, namely $K^{(1)}$, is a totally real Galois extension of $\mathbb{Q}$ with Galois group $\mathrm{Gal}(K^{(1)}/\mathbb{Q}) \cong D_{2p}$.

Using SAGE, we were able to compute the class number of $K$ for $d$ up to 73000. In the table below, we list the primes $p$ which appeared, as well a few of the corresponding $d$ for which $\mathbb{Q}(\sqrt{d})$ has class number $p$. However, as examined cases up to $d = 73000$, in some cases listing all occurrences would be impractical. The "..." indicates there were more on the list.

| $p$ | $d$ |
|---|---|
| 3 | $79, 142, 223, 229, 254, 257, 321, 326, \ldots$ |
| 5 | $491, 439, 499, 727, 817, 982, \ldots$ |
| 7 | $577, 1009, 1087, 1294, 1601, 1761, \ldots$ |
| 11 | $1297, 4009, 5182, 6081, 8059, 10401, \ldots$ |
| 13 | $4759, 8101, 8441, 8647, 11491, \ldots$ |
| 17 | $7054, 11257, 14639, 18223, 29681, \ldots$ |
| 19 | $15409, 18229, 31333, 33487, 37507, \ldots$ |
| 23 | $23593, 30801, 30977, 44097, 61669, 65707, 66343, 67409$ |
| 29 | $49281, 49531, 56857, 61339, 72901$ |
| 31 | none found up to $d = 73000$ |
| 37 | $24337, 53359, 55561$ |
| 41 | 55966 |
| 43 | 14401 |
| 47 | none found up to $d = 73000$ |
| 53 | 69694 |

# Bibliography


[1] Jennifer Andreotti. Inverse galois theory. Master's thesis, École Polytechnique Fédérale de Lausanne, 2009.

[2] Nigel Boston and Nadya Markin. The fewest primes ramified in a G-extension of Q. *Ann. Sci. Math. Quebec*, 33(2), 2009.

[3] Nancy Childress. *Class Field Theory.* Springer Science+Business Media., 2009.

[4] Keith Conrad. Linear independence of characters. Online Notes.

[5] David S. Dummit and Richard M. Foote. *Abstract Algebra.* John Wiley and Sons, Inc., third edition, 2004.

[6] Victor Flynn. B9 algebraic number theory. Lecture Notes, January 2011.

[7] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction.* Springer-Verlag, second edition, 1997.

[8] Simon Hasenfratz. Representation of primes by quadratic forms. Bachelor Thesis, 2008.

[9] Gerald J. Janusz. *Algebraic Number Fields.* American Mathematical Society, second edition, 1996.

[10] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem.* Cambridge Unversity Press, 2002.

[11] Falko Lorenz. *Algebra Volume 1: Fields and Galois Theory.* Springer-Verlag, 1973.

[12] J.S. Milne. Algebraic number theory. Online Text, May 2011.

[13] Michael Ira Rosen. *Number theory in function fields.* Springer-Verlag, 2002.

[14] Jean-Pierre Serre. *A Course in Arithmetic.* Springer Science+Business Media, 2006.

[15] Jerry Shurmani. Number theory - twelfth lecture. Lecture Notes.

[16] William Stein. Algebraic number theory, a computational approach. Online Text, September 2011.

[17] Balázs Szendrői. Polynomial rings and galois theory. Lecture Notes.

[18] Bertram A. F. Wehrfritz. *Finite Groups: a second course on group theory.* World Scientific Publishing Co., 1999.

[19] Steven H. Weintraub. *Galois Theory.* Springer Science+Business Media, 2006.

[20] Tom Weston. A brief introduction to local fields. Online Text.