SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Class Field Theory as motivated by Kronecker-Weber

av

Niklas Livchitz

2018 - No K1

Class Field Theory as motivated by Kronecker-Weber

Niklas Livchitz

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Wushi Goldring

2018

Class Field Theory as motivated by Kronecker-Weber

Niklas Livchitz

Abstract

This is a brief introduction to algebraic number theory directed towards class field theory. The first part covers basic definitions and invariants, such as integral closures, norms, traces and discriminants. The second part deals with the Hilbert ramification theory with a proof of quadratic reciprocity given as an application. The final part covers the basic theorems of class field theory, and applies them to prove the *Kronecker-Weber* theorem.

Acknowledgements

I would like to thank my supervisor Wushi Goldring for his invaluable support and many inspirational talks over coffee. May they continue even after this project is finished.

Contents

Introduction **2**

1 Rings of Integers **4**

1.1 Rings of Integers 4

1.2 Some Ring Theory 7

1.3 Traces, Norms and Discriminants 9

1.4 A Few Examples 11

2 Ramification Theory **12**

2.1 Prime ideals in field extensions 12

2.2 Interaction with Galois Theory 16

2.3 Applications 19

2.3.1 Ramification in cyclotomic fields 19

2.3.2 Quadratic Reciprocity 20

3 Class Field Theory **22**

3.1 Generalized Class Groups 22

3.2 Three theorems of Class Field Theory 24

3.3 Applications: Quadratic Reciprocity revisited and Kronecker-Weber 26

Introduction

The conception of this text stems from trying to understand a single theorem, one which might be encountered in a course on Galois theory. That theorem can be stated as:

Theorem 0.0.1 (Kronecker-Weber)**.** *A finite algebraic extension of the rationals is Galois and has an abelian Galois group if and only if it is contained in a cyclotomic extension.*

There are a few accessible proofs which would have made a good topic. However, there is one in particular, included at the end of Chapter 3, that consists of just a few lines. Considering how the theorem itself is rather far-reaching, the brevity of that proof can be surprising at a first glance.

Given the elegance of that version, one might next turn to the machinery that provides such a simple solution. The proof relies on what is known as class field theory. This theory goes beyond facilitating such a proof to give a powerful description of abelian extensions of the rationals.

With that in mind, the end goal of this text is to state the main theorems of class field theory, and use them to derive the Kronecker-Weber theorem. While proofs of these theorems are beyond the scope of this project, merely being able to state them requires the development of interesting topics.

Thus, this text will consider finite algebraic extensions of the rationals, known as number fields. One point of view of the number fields is Galois theory. The other is number theory, and the first chapter will try to give a short brief on the main concepts of that topic. In Chapter 2 this becomes apparent with the theory of ramifications of prime ideals, where the main tool of use are the residue rings formed from quotients by prime ideals. It is at once a stepping stone to the definitions needed for the following chapter, and a useful theory in itself. As an example, and application, a proof of Quadratic Reciprocity is given.

Using constructions from the ramification theory and extending them, Chapter 3 will cover the very basics of class field theory. The focus is on three theorems with demonstrations of their application. There are a few different formulations of this topic, and the one given here is chosen for its relative simplicity over generality.

The text will assume a familiarity with Galois theory and the theory of finite algebraic extensions of fields, as well as some familiarity with the theory of commutative rings and modules. Fixing notation throughout, L and K will denote number fields if nothing else is stated, L/K a finite extension L over K, and $[L : K]$ the degree of the extension. Using the primitive element theorem, an extension of K will also be denoted $K(\alpha)$ for a primitive element α of the extension.

Chapter 1

Rings of Integers

1.1 Rings of Integers

The main object to be treated in this text is that of rings of integers of number fields. Intuitively, one might see this as the analogue of the role that the integers play in the field of the rationals. On the other hand, since number fields are algebraic extensions of the rationals, one might want a similar property for the rings of integers. The concept that turns out to be needed is that of the integral closure.

Definition 1.1.1. *Let R be a ring and $\mathcal{O}$ a subring of R. If an element $\alpha \in R$ is the root of a monic polynomial $p(x)$ in $\mathcal{O}[x]$, it is called* ***integral*** *over $\mathcal{O}$. The relation $p(x) = 0$ is called an* ***equation of integral dependence*** *for α over $\mathcal{O}$.*

Lemma 1.1.2. *Let R be a ring with a subring $\mathcal{O}$. Then the following are equivalent:*

a) *For any element $x \in \mathcal{O}$ there is an equation of integral dependence of x over O.*

b) *The ring $\mathcal{O}[x]$ is a finitely generated $\mathcal{O}$-module.*

c) *There exist a subring S of R containing $\mathcal{O}$ and x that is a finitely generated $\mathcal{O}$-module.*

Proof. See [6, Ch 2.1 Thm 1]. □

Corollary 1.1.2.1. *The elements S which are integral over $\mathcal{O}$ in R form a subring of R.*

Proof. Let x and y be integral over O. By lemma **[1.1.2]** $\mathcal{O}[x]$ and $\mathcal{O}[y]$ are finitely generated $\mathcal{O}$-modules. Therefore $\mathcal{O}[x, y]$ is as well. It holds that $x + y$, $x - y$ and xy are in $\mathcal{O}[x, y]$ and so are integral over $\mathcal{O}$. Thus S is a ring. □

The ring S will be denoted the **integral closure** of $\mathcal{O}$ in R. A ring will be called **integrally closed** if it is an integral domain and is its own integral closure in its field of fractions. Note that $\mathbb{Z}$ is integrally closed. Integral closures admit a transitive relation in that if A, B and C are rings such that $A \subseteq B \subseteq C$ where B is integral over A, and C is integral over B, then C is integral over A [4, Ch 1.2, Prop 3].

When the ring R is a number field, the following convention will be used:

Definition 1.1.3. *Let K be a number field. The integral closure of $\mathbb{Z}$ in K is called the **ring of integers** or **number ring** of K, denoted $\mathcal{O}_K$.*

The number rings are free $\mathbb{Z}$-modules. As an example of a class of rings of integers, consider those of the quadratic fields. Recall that a quadratic field K is one which is an extension of degree two over the rationals. Using the primitive element theorem[3, Ch V, Thm 4.6], let v be a primitive element. The minimal polynomial for v is of then of the form $x^2 + bx + c = 0$ so that $K = \mathbb{Q}(\sqrt{b^2 - 4c})$. Now $b^2 - 4c$ is a rational, say $\frac{m}{m} = \frac{mn}{n^2}$. However $\mathbb{Q}(\sqrt{mn/n^2}) = \mathbb{Q}(\sqrt{mn})$. Thus any quadratic field can be written as $\mathbb{Q}(\sqrt{d})$, and one may assume d to be square-free.

Theorem 1.1.4. *Let $\mathbb{Q}(\sqrt{d})$ be a quadratic extension, with $d \in \mathbb{Z}$ square-free.*

i) *If $d \equiv 2$ or 3 mod 4, then $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ consists of all elements of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. As a $\mathbb{Z}$-module, there is a basis $(1, \sqrt{d})$.*

ii) *if $d \equiv 1$ mod 4, then $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ consists of all elements $\frac{a+b\sqrt{d}}{2}$ with $a, b \in \mathbb{Z}$ of the same parity. In this case the $\mathbb{Z}$-module basis is of the form $(1, \frac{1+\sqrt{d}}{2})$.*

Proof. Recall that $\mathbb{Q}(\sqrt{d})$ consists of all the elements of the form $a + b\sqrt{d}$ with a, b in $\mathbb{Q}$. Fix an $x = a+b\sqrt{d}$. Then $y = a-b\sqrt{d}$ is in $\mathbb{Q}(\sqrt{d})$. Moreover $x + y = 2a$ and $xy = a^2 - b^2d$ are in $\mathbb{Q}$. Now assume x is integral over $\mathbb{Z}$. Since y is the Galois conjugate of x, it must satisfy the same equation of integral dependence. This implies that y, $2a$ and $a^2 - b^2d$ are all integral over $\mathbb{Z}$ by **1.1.2.1**. Now since $2a$ and $a^2 - b^2d$ are in $\mathbb{Q}$ and Z is integrally closed, they must both be integers.

Now, if $a^2 - b^2 d$ is an integer then so is $(2a)^2 - (2b)^2 d$. Moreover since $2a$ is an integer, $(2a)^2$ and $(2a)^2 - (2b)^2 d - (2a)^2 = (2b)^2 d$ are as well.

If $2b$ is not an integer it is of the form $\frac{p}{q}$. Since d is square-free, $\frac{d}{q^2}$ would not be an integer. However $(2b)^2 d$ was shown to be an integer, so $2b$ must be as well.

Following this calculation, substitute $u/2 = a, v/2 = b$ and get:

$$u^2 - v^2 d \in 4\mathbb{Z}$$

If v is odd, then $v^2 \equiv 1 \bmod 4$. Since d is square-free, 4 does not divide d. The only squares mod 4 are 0 and 1, and combining with the previous statements, this implies that $u^2 \equiv 1 \bmod 4$, and $d \equiv 1 \bmod 4$. This is case ii) and note that holds if and only if $d \equiv 1 \bmod 4$. For the cases of $d \equiv 2$ of $3 \bmod 4$, then v is even, u is even and a, b in $\mathbb{Z}$. This will be the i).

For the part about bases, the case when $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ is obvious. For other case let $d \equiv 1 \bmod 4$. First, following the above reasoning, 1 and $\frac{1+\sqrt{d}}{2}$ belong to the ring of integers. Second, let $\frac{u+v\sqrt{d}}{2}$ be an element of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Assuming u, v to be odd, subtract $\frac{1+\sqrt{d}}{2}$ to make them even. Then;

$$\frac{u + v\sqrt{d}}{2} = (\frac{u}{2} - \frac{v}{2}) + v\frac{1 + \sqrt{d}}{2}$$

which is a linear combination of 1 and $\frac{1+\sqrt{d}}{2}$. □

One of the more salient points of this example is even though the ring of integers are finitely generated $\mathbb{Z}$-modules and as such have a basis, it is not a priori obvious of what form they take. Taking a note from field extensions, it would be an easy mistake to assume that $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$ in general. In the case of the quadratics, the field is $\mathbb{Q}(\sqrt{d})$ whereas the number ring is either $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

1.2 Some Ring Theory

Having defined the rings of integers of number fields, the first question one might ask is what properties they share. They are in general not principal ideal domains nor unique factorisation domains. For these rings it turns out that unique factorisation implies principal ideal domains. Turning to positives they are Noetherian, and in particular Dedekind domains, a trait that will be put to heavy use.

Definition 1.2.1. *Let R be an integral domain. Then R is called a* ***Dedekind domain*** *if it is Noetherian and integrally closed, and if every non-zero prime ideal is maximal.*

Every principal ideal domain is Dedekind, and so in particular $\mathbb{Z}$. Together with the following theorem, this implies that the rings of integers of number fields are all Dedekind domains:

Theorem 1.2.2. *Let R be a Dedekind domain, K its field of fractions, L a finite extension of K and S the integral closure of R in L. Then S is a Dedekind domain. If K is of characteristic 0 then S is a finitely generated R-module.*

Proof. See [6, Ch 3.4 Thm 1] □

The fact that prime ideals are maximal yields one of the main tools to use in the study of these rings. That is, if $\mathfrak{p}$ is a prime ideal of the Dedekind ring $\mathcal{O}$, then $\mathcal{O}/\mathfrak{p}$ is a field. The other major result on Dedekind domains concerns factorisation of ideals. In order to state it in a way that will be useful also for the extension of the theory in Chapter 3, a few more definitions are required. The first new object is that of fractional ideals.

Definition 1.2.3. *Let R be an integral domain, and K its field of fractions. A* ***fractional ideal*** *of R is an R-submodule I of K such that there exist an element $d \in R \setminus (0)$ such that $dI \subset R$. Let a* ***principal fractional ideal*** *be one of the form xR with $x \in K^\times$.*

An intuitive way to think of a fractional ideal is as an ideal with denominators. Multiplying with d can be thought of as clearing out the denominator so that I turns into an ideal. Note particularly that ordinary ideals of R also are fractional ideals, with $d = 1$. Define the product IJ of two fractional ideals I and J as the set of finite sums $\sum x_i y_i$ with $x \in I$, $y \in J$. As with ideals, $I \cap J, I + J$, and IJ are again fractional ideals. In the general

case of integral domains, the set of fractional ideals form a monoid under multiplication [6, Ch 3.3, after Lemma 3]. In the case of Dedekind domains, the structure is even stronger.

Theorem 1.2.4. *Let R be a Dedekind domain and P the set of non-zero prime ideals of R. Then*

i) *Every non-zero fractional ideal $\mathfrak{b}$ of R may be uniquely expressed in the form*

$$\mathfrak{b} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})}$$

where, for any $\mathfrak{p} \in P, n_{\mathfrak{p}}(\mathfrak{b}) \in \mathbb{Z}$, and, for almost all $\mathfrak{p} \in P$, $n_{\mathfrak{p}}(\mathfrak{b}) = 0$.

ii) *The monoid of non-zero fractional ideals of R is a group.*

Proof. see [6, Ch 3.4 Thm 3] □

Note that in particular this applies to ordinary ideals, so that for any ideal in a Dedekind domain, there is a unique representation as a product of prime ideals. As motivated by part ii), with a slight abuse of language it is justified to say that a fractional ideal divides another ideal of it appears in the factorization of the latter. In fact, in this case, containment implies division [5, Ch 3 Thm 15 Corr 3].

Now consider the set of principal fractional ideals.

Definition 1.2.5. *Let R be a Dedekind ring, with field of fractions K. Denote by I_K the set of fractional ideals and P_K the set of principal fractional ideals. Then P_K is a subgroup of I_K. The quotient $I_K/P_K = C(K)$ is called the **Class Group** of K.*

For R to be a principal ideal domain is equivalent to R having a trivial class group. Computing the class group is in general a hard problem, however of note is a general result establishing it as finite [6, Ch 4.3 Thm 2]. The introduction of the class group here is motivated by its role as a prototype of objects developed in Chapter 3.

1.3 Traces, Norms and Discriminants

There are a few tools that should be constructed in order to use for proofs in the following chapter. They are a set of useful invariants of elements and ideals in the rings. Recall the definition of **trace** and **determinant** from linear algebra. Also recall that trace and determinant are independent of a particular choice of basis.

Let L is an algebraic extension of a number field K, then $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module. Then for $x \in \mathcal{O}_L$, denote by m_x multiplication by x. Then m_x is an endomorphism and fixing a basis m_x can be represented by a matrix.

Definition 1.3.1. *With notation as above, define the* ***trace*** *of x, $Tr_K^L(x)$, as the trace of m_x and the* ***norm*** *of x, $N_K^L(x)$ as the determinant of m_x.*

When the extension in question is clear from the context, one may drop the indices and simply write $Tr(x)$ and $N(x)$. While this definition might seem cumbersome at a first glance, there is the following theorem to help:

Theorem 1.3.2. *Keeping the notation from the definition, let $[L : K] = n$ and $x_1, x_2, ..., x_n$ be the roots of the minimal polynomial $\mu(x)$ for x over $\mathcal{O}_K$ in the splitting field for μ, each one repeated $[L : K(x)]$ times. Then $Tr_K^L(x) = \sum_{i=1}^n x_i$ and $N_K^L(x) = \prod_{i=1}^n x_i$*

Proof. See [6, Ch 2.6 Prop 1] □

Equivalently, these identites can be reformulated in Galois conjugates of x. Let the splitting field for the minimal polynomial of x over K be F . If $\sigma_i(x)$ are the conjugates of x, and $[F : K] = d$ then $Tr_K^L(x) = \frac{n}{d} \sum_{i=1}^d \sigma_i(x)$ and $N_K^L(x) = (\prod_{i=1}^d \sigma_i(x))^{\frac{n}{d}}$ [5, Ch 1 Thm 4']. As a short remark at this point, note that in the proof of theorem **1.1.4**, the terms $\sigma(x) + x$ and $\sigma(x)x$ were the trace and determinant for x respectively.

Some familiarity with linear algebra gives the relations $Tr(ax + by) = aTr(x) + bTr(y)$, $N(xy) = N(x)N(y)$ and $N(ax) = a^d N(x)$ [6, Ch 2.6, after Def 1].

Theorem 1.3.3. *If $x \in \mathcal{O}_L$, then $Tr_K^L(x) \in \mathcal{O}_K$ and $N_K^L(x) \in \mathcal{O}_K$.*

Proof. Since $\mathcal{O}_K$ is integrally closed in K, it suffices to show that the norm and trace are in K and that they are integral over $\mathcal{O}_K$. Since the conjugates

of x satisfy the minimal polynomial, they also satisfy any equation of integral dependence of x. Thus the trace and norm are sums and products of integral elements, and are therefore integral. □

There is also an extension of the concept of norms to ideals.

Definition 1.3.4. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_\mathcal{K}$. Then the **norm** of $\mathfrak{a}$ is $N_\mathbb{Q}^K(\mathfrak{a}) = Card(\mathcal{O}/\mathfrak{a})$.*

Theorem 1.3.5. *When $\mathfrak{a} = (a)$ is a principal ideal, $N_\mathbb{Q}^K((a)) = N_\mathbb{Q}^K(a)$*

Proof. [6, Ch 3.5 Prop 1] □

The final piece to be defined is the discriminant.

Definition 1.3.6. *Let L and K be as above. Given an n-tuple $(x_1, ..., x_n)$ in L^n, define the discriminant of $(x_1, ..., x_n)$ as*

$$D(x_1, ..., x_n) = det(Tr_K^L(x_i x_j))$$

Furthermore, the discriminant of an extension L/K is defined to be the principal ideal generated by the discriminant of any basis of L/K. It is denoted by $\mathcal{D}_{L/K}$.

That the second part of this definition is well defined follows from the fact that the discriminant of two bases differ by a unit, since the bases are conjugated by an invertible matrix [6, Ch 2.7 after Prop 1]. In the number field case, the discriminant of two such bases as extensions of $\mathbb{Q}$ are equal, and the discriminant is uniquely determined. It is the denoted the **absolute discriminant** of the number field.

Again, as with both the trace and norm, it is possible to simplify this definition to an easier form.

Theorem 1.3.7. *Let L/K be an extension of number fields, and $[L : K] = n$. Let σ_i the the n distinct K-isomorphisms of L into $\mathbb{C}$. Then, if $(x_1, ..., x_n)$ is a base of L/K;*

$$D(x_1, ..., x_n) = det(\sigma_i(x_j))^2 \neq 0$$

Proof. see [6, Ch 2.7 Prop 3] □

1.4 A Few Examples

The main point of these tools is to leverage them for proofs in Chapter 2, but they do have a few direct applications to showcase some of the structure of the number rings.

As a first, consider the following consequence of theorem **1.3.2**, a characterization of units of $\mathcal{O}_K$. Since the norm is multiplicative, and using the norm over $\mathbb{Q}$, it is easy to see that the norm of a unit has to be ± 1. Conversely, suppose that an element x has norm ± 1. Then x^{-1} has to be an algebraic integer, since the other factors of the norm is a product of algebraic integers as argued in the proof of theorem **1.3.3**. Generalizing this result for a quadratic field $K = \mathbb{Q}(\sqrt{d})$, x being a unit of $\mathcal{O}_K$ is equivalent to solving $x^2 - dy^2 = \pm 1$ in $\mathbb{Z}$. The case with $= +1$ is a classic equation known as the Pell-Fermat equation.

Taking the field $K = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$, theorem **1.1.4** gives $\mathcal{O}_K$ as $\mathbb{Z} + i\mathbb{Z}$, the Gaussian integers. Take the norm of an arbitrary element $N(a + ib) = (a + ib)(a - ib) = a^2 + b^2$. Thus, the only units are those that satisfies $a^2 + b^2 = \pm 1$. Thus, the units are $\{1, -1, i, -i\}$. As a note on units, there exist an explicit description of the group of units of a ring of integers due to Dirichlet, known as the Unit theorem.

As another example, recall that it was mentioned earlier how in general the number rings are not unique factorization domains. Using norms, it is now possible to explicitly demonstrate this behaviour. Consider the field $K = \mathbb{Q}(\sqrt{-5})$. Again using theorem **1.1.4**, the ring of integers is $\mathcal{O}_\mathcal{K} = \mathbb{Z} + \sqrt{-5}\mathbb{Z}$ and $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \times 3$. Now say that $1 + \sqrt{(-5)}$ had a non-unit divisor $y = a + b\sqrt{-5}$. Then the norm over the rationals of y, $N^K_\mathbb{Q}(y) = a^2 + 5b^2$, would have to divide $N^K_\mathbb{Q}(1 + \sqrt{(-5)}) = 6$. It is easy to see that neither $a^2 + 5b^2 = 2$ nor $a^2 + 5b^2 = 3$ has any solutions in $\mathbb{Z}$, and so 6 has two distinct factorizations in irreducible elements. Thus $\mathbb{Q}(\sqrt{-5})$ fails to be a UFD.

The final example of this part will be on discriminants. Consider the absolute discriminant of the quadratic field $\mathbb{Q}(\sqrt{19})$. Let σ be the non-trivial automorphism. Since $19 \equiv 3 \bmod 4$, a $\mathbb{Z}$-basis is $(1, \sqrt{19})$ and one obtains $D = det(\sigma_i(x_j)) = (\sigma(\sqrt{19}) - \sqrt{19})^2 = (-2\sqrt{19})^2 = 76$. The exact same argument works for any $d \equiv 2$ or $3 \bmod 4$, so that the absolute discriminant of any such quadratic field is $4d$. When $d \equiv 1 \bmod 4$, the $\mathbb{Z}$-basis is instead $(1, \frac{1+\sqrt{d}}{2})$ and the absolute discriminant becomes $D = (\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2})^2 = d$.

Chapter 2

Ramification Theory

2.1 Prime ideals in field extensions

This chapter will be concerned with the behaviour of prime ideals in algebraic extensions of number fields. Therefore it is convenient to let 'prime' denote a prime ideal in the ring of integers. The theme for this chapter is derived from one of the defining traits of Dedekind rings, that of prime factorization of ideals. Consider the following situation: Let L/K be an extension of number fields, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}$ can extended to be an ideal of $\mathcal{O}_L$ by taking $\mathfrak{p}\mathcal{O}_L$. How does the ideal $\mathfrak{p}\mathcal{O}_L$ factor in $\mathcal{O}_L$? Is it still a prime, or does it factor as a product of primes?

As an example, consider $\mathbb{Q}(i)/\mathbb{Q}$ with rings of integers $\mathbb{Z}(i)$ and $\mathbb{Z}$. There is a particularly good example in the ideal (2). Since prime ideals are maximal in a Dedekind domain, for (2) to remain prime in $\mathbb{Z}(i)$ requires $\mathbb{Z}(i)/(2)$ to be a field. However, there are obvious zero divisors in the quotient ring as 2 factors as $(1-i)(1+i)$. For another example, take the field $K = \mathbb{Q}(\sqrt{35})$ and the ideal (11). By **1.1.4** the ring of integers $\mathcal{O}_K = \mathbb{Z}(\sqrt{35})$, and the question now is whether $\mathbb{Z}(\sqrt{35})/(11)$ is a field. One may note that $x^2 - 35$ is the minimal polynomial for $\sqrt{35}$ over $\mathbb{Q}$. Thus $\mathbb{Z}(\sqrt{35})/(11) \cong (\mathbb{Z}[x]/(x^2 - 35))/(11) \cong \mathbb{Z}[x]/(x^2 - 35, 11) \cong \mathbb{Z}[x]/(11))/(x^2 - 35) \cong \mathbb{F}_{11}[x]/(x^2 - 35)$. This is a field since $x^2 - 35 \equiv x^2 - 2$ is irreducible over $\mathbb{F}_{11}$ implying that (11) is a prime ideal in $\mathbb{Q}(\sqrt{35})$.

One could continue in this manner, but it quickly grows impractical, especially so since most number fields are not principal ideal domains, and factorisation might get tricky. The rest of this section will give a few tools to manage the situation.

Theorem 2.1.1. *Let $\mathfrak{p}$ a prime of $\mathcal{O}_K$. Then the ideals $\mathfrak{P}_i$ of $\mathcal{O}_L$ such that $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$ are precisely those that appear in the factorization $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{p}_i^{e_i}$.*

Proof. $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \Leftrightarrow \mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}$ by maximality of $\mathfrak{p}$. Also, $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i} \Rightarrow \mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}_i$ for all i. □

There is some nomenclature associated to this definition. With definitions as above $\mathfrak{P}_i$ is said to **lie above** $\mathfrak{p}$. If there is only one prime lying above $\mathfrak{p}$ and $e_i = 1$, then it is said to be **inert**. If there are more, $\mathfrak{p}$ **splits**. If any of the exponents e_i are greater than 1, $\mathfrak{p}$ is said to **ramify** in the extension. In all of these cases, with some abuse of language, the behaviour may be said to take place in either $\mathcal{O}_L$, L or L/K equivalently, as is convenient for the situation.

Consider again the previous example of the prime (2) and the extension $\mathbb{Q}(i)/\mathbb{Q}$. As argued (2) will split as a product of prime ideals in $\mathbb{Z}(i)$. Furthermore $2 = (1-i)(1+i)$ which gives $(1-i)(1+i) = -i(1+i)^2$. Thus as ideals there is the factorisation $(2) = (1+i)^2$ and (2) ramifies in this extension.

One of the standard tools to study ramification is the residue fields associated to the primes. As a consequence of theorem **2.1.1**, one can see that $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}$. Furthermore, since $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module, we can take $\mathcal{O}_L/\mathfrak{P}$ to be a finite-dimensional vector space over $\mathcal{O}_K/\mathfrak{p}$, i.e. a finite extension. The dimension of this vector space is the **residual degree** of $\mathfrak{P}$, denoted f.

Theorem 2.1.2. *Let $[L:K] = n$ and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ with*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$$

Then

$$\sum_{i=1}^{q} e_i f_i = [\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L : \mathcal{O}_K/\mathfrak{p}] = n$$

Proof. See [6, Ch 5.2 Thm 1] □

The fact that the extension is finite gives a useful description of the residue fields. Since $\mathbb{Z}/(p) \cong \mathbb{F}_p$, all of the residue fields $\mathcal{O}/\mathfrak{p}$ for number fields are isomorphic to finite fields $\mathbb{F}_q$, and the Galois groups of their extensions are cyclic.

The residue rings will be of great use later in this chapter. To get a sense of the structure, there is the following theorem:

Theorem 2.1.3. *With L/K finite and $\mathfrak{p}$ a prime ideal of K, there is the following isomorphism of residue rings.*

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_{i=1}^{q} \mathcal{O}_L/\mathfrak{P}_i^{e_i}$$

Proof. The only maximal ideal containing $\mathfrak{P}_i^{e_i}$ is $\mathfrak{P}_i$. This implies that $\forall i \neq j, \mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = \mathcal{O}_L$. The result then follows from the Chinese Remainder Theorem. See [3, Ch 2.2 Corr 2.2]. □

Another very important tool is the discriminant from Chapter 2. Consider the following, which is a slight extension of the previous definition to one of extensions:

Definition 2.1.4. *Let L/K be a finite extension. The* ***discriminant ideal*** *$\mathfrak{D}_{L/K}$ of $\mathcal{O}_L$ over $\mathcal{O}_K$ is the ideal generated by the discriminants of those bases of L/K that are contained in $\mathcal{O}_L$.*

Note that $\mathfrak{D}_{L/K}$ is an integral ideal of $\mathcal{O}_K$. Motivation: If $(x_1, ..., x_n)$ is a basis contained in $\mathcal{O}_L$, then $Tr_{L/K}(x_i x_j) \in \mathcal{O}_K \Rightarrow D(x_1, ...x_n) \in \mathcal{O}_K$.

The usefulness of the discriminant comes from the following theorem:

Theorem 2.1.5. *Let L/K be a finite extension of number fields. A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ ramifies in $\mathcal{O}_L$ if and only if it contains $\mathfrak{D}_{L/K}$. Furthermore, only finitely many prime ideals of $\mathcal{O}_K$ ramify in $\mathcal{O}_L$.*

Proof. [6, Ch 5.3 Thm 1] □

Recall the example of absolute discriminants of quadratic fields at the end of Chapter 1. If $d \equiv 2$ or $3 \bmod 4$ then $\mathfrak{D}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} = (4d)$ and else $\mathfrak{D}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} = (d)$. From **2.1.4** it is clear that any ramified prime p of $\mathbb{Z}$ must divide $4d$ in the first case and d in the second.

As a nice example, all the tools are in place to study primes in quadratic extensions of the rationals.

Theorem 2.1.6. *Let $d \in \mathbb{Z}$ be square-free, and let $L = \mathbb{Q}(\sqrt{d})$. Then*

a) *If p is an odd prime such that d is a quadratic residue mod p or $p = 2$ and $d \equiv 1$ mod 8, then p splits.*

b) *If p is an odd prime and d is not a quadratic residue or $p = 2$ and $d \equiv 5$ mod 8, then p remains prime.*

c) *If p is an odd prime dividing d or $p = 2$ and $d \equiv 2$ or 3 mod 4, then p ramifies.*

Proof. Let p be odd. Then $\mathcal{O}_K = \mathbb{Z} + \sqrt{d}\mathbb{Z}$ or $\mathcal{O}_K = \mathbb{Z} + (1 + \sqrt{d}\mathbb{Z})/2$ depending on d. However, the situation simplifies when passing to the residue ring. Consider the latter case, and take an element $a + b(1 + \sqrt{d})/2$, with b odd. We see that modulo p this is congruent to $a + (p + d)(1 + \sqrt{d})/2 \in \mathbb{Z} + \sqrt{d}\mathbb{Z}$. Thus, in either case, $\mathcal{O}_L/p\mathcal{O}_L \cong (\mathbb{Z} + \sqrt{d}\mathbb{Z})/(p)$. Recall that $\mathbb{Z} + \sqrt{d}\mathbb{Z} \cong \mathbb{Z}[x]/(x^2 - d)$. This implies that

$$\mathcal{O}_L/p\mathcal{O}_L \cong (\mathbb{Z} + \sqrt{d}\mathbb{Z})/(p) \cong (\mathbb{Z}[x]/(x^2 - d))/(p) \cong \mathbb{Z}[x]/(p, x^2 - d)$$

continuing yields:

$$\mathbb{Z}[x]/(p, x^2 - d) \cong (\mathbb{Z}[x]/(p))/(x^2 - d) \cong \mathbb{F}_p[x]/(x^2 - d)$$

The problem is then one of characterizing $\mathbb{F}_p/(x^2 - d)$. By theorem **2.1.3** we can say that p splits if this is the product of two fields, that is if $(x^2 - d)$ splits in $\mathbb{F}_p$. This is equivalent to stating that d is a non-zero square in $\mathbb{F}_p$, i.e. a quadratic residue. If $(x^2 - d)$ on the other hand is irreducible, then $f_1 = 2$ and (p) would remain prime. The last case is when d is zero in $\mathbb{F}_p$, then the polynomial is a square (i.e. not separable) and $e_1 = 2$, so p ramifies.

Now let $p = 2$. If $d \equiv 2$ or 3 mod 4, then $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. As above, $\mathcal{O}_L/2\mathcal{O}_L \cong \mathbb{F}_2/(x^2 - d)$. Now the reduction of $(x^2 - d)$ in $\mathbb{F}_2$ is x^2 or $x^2 + 1 = (x + 1)^2$, in either case we will have nilpotent elements in the residue ring. Thus, as above, in this case p ramifies. Not let $d \equiv 1$ mod 4. Then $\mathcal{O}_L = \mathbb{Z} + (1 + \sqrt{d}\mathbb{Z})/2$. The minimal polynomial for $(1 + \sqrt{d})/2$ is $x^2 - x - (d - 1/)4$, thus $\mathcal{O}_L/2\mathcal{O}_L \cong \mathbb{F}_2/(x^2 - x - (d - 1)/4)$. If $d \equiv 1$ mod 8 then $(d - 1)/4 \equiv 0$ mod 2. This means $x^2 - x - (d - 1)/4 \equiv x(x - 1)$ and as above, splitting of the polynomial implies splitting of the prime. If $d \equiv 5$ mod 8 on the other hand, $(d - 1)/4 \equiv 1$ mod 2 and $x^2 - x - (d - 1)/4$ is irreducible, so p remains prime.

□

2.2 Interaction with Galois Theory

In the theory of field extensions, there is the particularly nice case of those that are Galois. This carries over to the theory of ramification in a beautiful way. A natural first question to ask would be how the elements of the Galois group of such an extension act on the ring of integers. Let L/K be Galois, and let $x \in \mathcal{O}_L$. Let $p(x)$ be the equation of integral dependence for x over $\mathcal{O}_K$. For any $\sigma \in Gal(L/K)$, the coefficients of $p(x)$ are fixed under the action of σ, so $\sigma p(x)$ is again an equation of integral dependence of some conjugate of x. Thus the ring of integers is stable under the action of the Galois group. Furthermore, if $\mathfrak{P}_i$ is a prime ideal of $\mathcal{O}_L$ lying above a prime $\mathfrak{p}$ of $\mathcal{O}_K$, then $\sigma(\mathfrak{P}_i) \cap \mathcal{O}_K = \mathfrak{p}$ since $\mathcal{O}_K$ is fixed. There is an even stronger version of this relation:

Theorem 2.2.1. *Let L/K be Galois, $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ and let $\mathfrak{p}\mathcal{O}_L = \prod_{k=1}^{g} \mathfrak{P}_k^{e_k}$. Then, for all i, j there exist $\sigma \in Gal(L/K)$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Furthermore, all the $\mathfrak{P}_i$ have the same ramification indices e and residual degrees f. Thus*

$$\mathfrak{p}\mathcal{O}_L = (\prod_{i=1}^{g} \mathfrak{P}_i)^e \text{ and } n = efg$$

Proof. Recall theorem **2.1.2** stating that $\sum_{i=1}^{g} e_i f_i = n$. Since σ is a field automorphism, it will preserve f and g. Thus, the only outstanding part to prove is the fact that the Galois group permutes the primes transitively.

Choose a $\mathfrak{P}_i$ and assume for a contradiction that there is some $\mathfrak{P}_j$ for which there is no $\sigma \in Gal(L/K)$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. The Chinese Remainder theorem then gives a solution in to the system

$$\begin{cases} x \equiv 0 \bmod \mathfrak{P}_j \\ x \equiv 1 \bmod \sigma(\mathfrak{P}_i) \text{ for all } \sigma \in Gal(L/K) \end{cases}$$

Let α be such a solution. Take the norm of alpha, $N(\alpha) = \prod_{\sigma \in Gal(L/K)} \sigma(\alpha)$. Since α appears as a factor, $N(\alpha) \in \mathfrak{P}_j \cap \mathcal{O}_K = \mathfrak{p}$. On the other hand, since $\alpha \notin \sigma(\mathfrak{P}_i) \Rightarrow \sigma^{-1}\alpha \notin \mathfrak{P}_i$. This implies that $N(\alpha) \notin \mathfrak{P}_i$, but $N(\alpha) \in \mathfrak{p} \subset \mathfrak{P}_i$. Contradiction. □

Primes $\mathfrak{P}_i, \mathfrak{P}_j$ are called **conjugate** if $\mathfrak{P}_i = \sigma(\mathfrak{P}_j)$ for some σ in $Gal(L/K)$. Now, as previously seen, one of the more powerful tools in characterizing ramification are the residue fields. There is a nice way of restricting the Galois group of the field extension to that of the residue fields. First, a few definitions:

Definition 2.2.2. *Let L/K be Galois with Galois group G. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ an ideal lying above it. Then the* ***decomposition group*** *(of $\mathfrak{P}$) is the subgroup $D_{\mathfrak{P}} = \{\sigma \in G | \sigma(\mathfrak{P}) = \mathfrak{P}\}$. The* ***inertia group*** *is the subgroup $I_{\mathfrak{P}} = \{\sigma \in G | \sigma(x) - x \in \mathfrak{P}$ for all $x \in \mathcal{O}_L\}$.*

The subscripted primes might be suppressed if the prime in question is clear. The main point of these groups comes from the following: Let $\sigma \in D_{\mathfrak{P}}$. Then σ restricts to an automorphism of $\mathcal{O}_L$ and since σ leaves $\mathfrak{P}$ stable, it induces an automorphism $\overline{\sigma}$ of $\mathcal{O}_L/\mathfrak{P}$. Since $\sigma \in Gal(L/K)$, it also fixes $\mathcal{O}_K/\mathfrak{p}$. This implies that $\overline{\sigma} \in Gal((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$. The mapping $\sigma \to \overline{\sigma}$ is clearly a group homomorphism with kernel $I_{\mathfrak{P}}$. In fact, this is an isomorphism from D/I onto the Galois group of the residue field extension as given by this theorem:

Theorem 2.2.3. *Let $L, K, \mathfrak{P}$ and $\mathfrak{p}$ be as above. Then $\mathcal{O}_L/\mathfrak{P}$ is a Galois extension of degree f over $\mathcal{O}_K/\mathfrak{p}$, and the homomorphism*

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

sending $\sigma \mapsto \overline{\sigma}$ is surjective.

Proof. Consider first L_D, the fixed field of D. Let $\mathcal{O}_D = \mathcal{O}_L \cap L_D$ and let $\mathfrak{p}_D$ be a prime ideal of $\mathcal{O}_D$ such that $\mathfrak{p}_D = \mathfrak{P} \cap \mathcal{O}_K$. Now note that by theorem **2.2.1**, there is one prime lying above $\mathfrak{p}_D$ since $\mathfrak{P}$ is stable under the action of D. Factor $\mathfrak{p}_D\mathcal{O}_K$ as $\mathfrak{P}^{e'}$ and let f' be the residual degree of $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_D/\mathfrak{p}_D)$. Then, by theorem **2.1.2** $e'f' = [L : L_D]$ and via Galois theory $[L : L_D] = Card(D)$. Furthermore, $Card(D) = ef$ since if $[L : K] = n$, then the cardinality is n divided by the number of conjugates of $\mathfrak{P}$. Thus $ef = e'f'$. Conclude that $e = e', f = f'$ and thus that $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_D/\mathfrak{p}_D$ (1).

Now let $\overline{\alpha}$ be a primitive element of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$ and let α be a representative of it in $\mathcal{O}_L$. Let $\mu_\alpha(x)$ be the minimal polynomial for α over L_D. Then $\mu_\alpha(x) \in \mathcal{O}_K[x]$ since α is integral and the roots are all of the form $\sigma(\alpha)$ for some $\sigma \in D$. Now let $\overline{\mu_\alpha}(x)$ be the reduction modulo $\mathfrak{p}$. By (1), it is in $\mathcal{O}_K/\mathfrak{p}[x]$, and the roots are all of those of the form $\overline{\sigma}(\overline{\alpha})$. Consequently, $\mathcal{O}_L/\mathfrak{P}$ is the splitting field of $\overline{\mu_\alpha}(x)$ and is Galois over $\mathcal{O}_K/\mathfrak{p}$. Furthermore, since we can write any conjugate of $\overline{\alpha}$ as $\overline{\sigma}(\overline{\alpha})$ fot some $\sigma \in D$, the homomorphism is surjective. By the first isomorphism theorem for groups, $D/I \cong Gal((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ and $f = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = |D/I|$ and since $Card(D) = ef$, $Card(I) = e$. □

Note that since the residue rings are finite, D/I is cyclic of order f. Also note that for $\mathfrak{p}$ to be unramified in an extension the inertia group for any

prime lying above it must be trivial. By theorem **2.2.1** and the argument in the proof above, for $\mathfrak{p}$ to split into $[L:K]$ distict factors, the decomposition group must be trivial. In terms of intermediate fields F_i with $K \subset F_i \subset L$, L_D can be characterized as the smallest such field for which $\mathfrak{P}$ is the only prime lying above $\mathfrak{P} \cap \mathcal{O}_{F_i}$. Similarily L_I is the largest F_i for which $\mathfrak{P}$ is totally ramified over $\mathfrak{P} \cap \mathcal{O}_{F_i}$, i.e. $e = [L : F_i]$ [5, Ch 4 Thm 29].

There is one more case that simplifies the structure of these extensions, and that is the case when the Galois group is abelian.

Theorem 2.2.4. *Let L/K be Galois. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ and $\sigma(\mathfrak{P})$ a conjugate for some $\sigma \in Gal(L/K)$. Then the decomposition and inertia groups are conjugate;*

$$D_{\sigma(\mathfrak{P})} = \sigma D_{\mathfrak{P}} \sigma^{-1}$$

$$I_{\sigma(\mathfrak{P})} = \sigma I_{\mathfrak{P}} \sigma^{-1}$$

Proof. See [6, Ch 6.2, remark following Prop 2] □

The final component to be defined before moving on to a few applications is the Artin symbol. Suppose there is a Galois extension L/K of number fields, with a prime $\mathfrak{P}$ lying above the prime $\mathfrak{p}$. Then as noted $\mathcal{O}_L/\mathfrak{P}$ is Galois of degree f over $\mathcal{O}_K/\mathfrak{p}$. Suppose further that $\mathfrak{p}$ is unramified so that $D_{\mathfrak{P}} \cong Gal(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$. The latter is the Galois group of an extension of a finite field. Recall from Galois theory that this implies the existence of a canonical generator $Frob : x \mapsto x^q$ with $q = Card(\mathcal{O}_K/\mathfrak{p})$ [3, Ch 5.5 Thm 5.4]. Thus, we have a generator σ of $D_{\mathfrak{P}}$ such that $\sigma(x) \equiv x^q \bmod \mathfrak{P}$, called the Frobenius automorphism of $\mathfrak{P}$. Furthermore, for conjugates $\mathfrak{P}_i$ and $\mathfrak{P}_j$, their Frobenius automorphisms are conjugate elements by theorem **2.2.4**. Thus, in an abelian extension the Frobenius element only depends on the underlying prime $\mathfrak{p}$ of $\mathcal{O}_K$.

Definition 2.2.5. *Let L/K be Galois. Then the **Artin symbol** $(\frac{\mathfrak{P}}{L/K})$ for a prime $\mathfrak{P}$ lying above an unramified prime $\mathfrak{p}$ denotes the Frobenius automorphism associated to $\mathfrak{P}$.*

*If L/K is abelian then the **Artin map** sends any unramified prime $\mathfrak{p}$ of $\mathcal{O}_K$ to the associated Frobenius element $(\frac{\mathfrak{p}}{L/K})$ in $Gal(L/K)$.*

Theorem 2.2.6. *Let L/K be Galois with an intermediate field F. Let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ and f the residual degree of $\mathfrak{P} \cap M$ over K. Then:*

i) $(\frac{\mathfrak{P}}{L/M}) = (\frac{\mathfrak{P}}{L/K})^f$

ii) *if F is Galois over K then* $(\frac{\mathfrak{P}}{L/K})|_M = (\frac{\mathfrak{P}\cap M}{M/K})$.

Proof. See [6, Ch 6.3 Prop 1] □

2.3 Applications

2.3.1 Ramification in cyclotomic fields

As a nice example of ramification in extensions, there is the case of the cyclotomic ones. First, a description of the corresponding number ring.

Lemma 2.3.1. *Let p be prime, $\zeta = \zeta_p$ and $K = \mathbb{Q}(\zeta)$. Then $\mathcal{O}_K = \mathbb{Z}(\zeta_p)$ for which a base as a $\mathbb{Z}$-module is $(1, \zeta, ..., \zeta^{p-2})$.*

Proof. See [5, Ch2 Thm 10] □

Theorem 2.3.2. *Let ζ_n be a primitive n:th root of unity. Then any prime p of $\mathbb{Z}$ ramifying in $\mathbb{Q}(\zeta_n)$ divides n.*

Proof. Starting first with the case where $n = p$ is a prime number. Recall that the minimal polynomial is $p(x) = x^{p-1} + x^{p-2} + ... + x + 1$ so that $(x-1)p(x) = x^p - 1$ [2, Ch 13.6]. There is an easier form of the discriminant in this case, using the Vandermonde matrix. See [Ch 2.7, the example] to obtain $D(1, \zeta, ..., \zeta^{p-2}) = (-1)^{\frac{1}{2}(p-1)(p-2)} N(p'(\zeta))$.

Taking derivatives of $(x-1)p(x) = x^p - 1$ and evaluating at ζ gives $(\zeta - 1)(p'(\zeta)) = p\zeta^{p-1}$. Now note that $\zeta^{-1} = \zeta^{n-1} \in \mathcal{O}_\mathcal{K}$ and so $N(\zeta) = \pm 1$. Furthermore, clearly $N(p) = p^{n-1}$ and by substituting $x-1$ into the minimal polynomial and taking coefficients one obtains $N(\zeta - 1) = \pm p$. Putting all of this together yields:

$$D(1, \zeta, ..., \zeta^{p-2}) = \pm p^{p-2}$$

Using theorem **2.1.5**, p is the only prime of $\mathbb{Z}$ that ramifies in $\mathbb{Q}(\zeta_p)$.

Now consider the case where n is not prime. In this case, the minimal polynomial $p(x)$ divides $x^n - 1$, so say that $x^n - 1 = p(x)g(x)$ for some $g(x) \in \mathbb{Q}[x]$ and that $deg(p(x)) = d$. Taking derivatives and evaluating at ζ now gives $n\zeta^{n-1} = p'(\zeta)g(\zeta)$. Taking norms gives

$$N(g(\zeta))N(p'(\zeta)) = \pm n^d$$

and so $N(p'(\zeta))$ divides n^d. As argued in the first subcase, $D(1, \zeta, ..., \zeta^{d-1}) = \pm N(p'(\zeta))$. Note now that in the first case $D(1, \zeta, ..., \zeta^{d-1})$ was the discriminant of the basis for the number ring, which was what solved the problem. In this case, it is a basis of the field extension, but not nessecarily of the the number ring as a $\mathbb{Z}$-module. However, as in the discussion after definition **1.3.6** since ζ is a unit, the absolute discriminant must divide this discriminant, and so must divide n^d. The theorem follows from **2.1.5**. □

2.3.2 Quadratic Reciprocity

A further example of an application is a nice proof of Quadratic Reciprocity. It is notable in that the case of $p = 2$ falls out without barely any extra work. Also note how the Artin symbol is used to express the quadratic Legendre symbol, which while in this text is defined first here, is usually introduced at a much earlier stage.

Definition 2.3.3. *Define the Legendre symbol* $(\frac{p}{q})$ *as:*

$$\begin{cases} +1 \text{ if } p \text{ is a quadratic residue mod } q \\ -1 \text{ else} \end{cases}$$

Lemma 2.3.4 (Euler's Criterion)**.** *Let p be an odd prime and $a \in \mathbb{Z} - p\mathbb{Z}$. Then:*

$$(\frac{a}{p}) \equiv a^{(p-1)/2} \text{ mod } p$$

Proof. See [6, Ch 5.5 Prop 1] □

Theorem 2.3.5 (Quadratic Reciprocity)**.** *Let p, q be distict odd primes. Then it holds that:*

$$(\frac{p}{q}) = (-1)^{(p-1)(q-1)/4}(\frac{q}{p})$$

If $p = 2$ then

$$(\frac{2}{q}) = (-1)^{(q^2-1)/8}$$

Proof. The strategy is to show that the Artin symbol subsumes the Legendre, and then show that both sides express the Artin for a suitable extension of the rationals.

Begin by letting q be an odd prime, and $K = \mathbb{Q}(\zeta_q)$. Recall from the Galois theory that $G := Gal(K/\mathbb{Q}) \cong \mathbb{F}_q^\times$ and that this group has a unique subgroup H of index 2 corresponding the the subgroup of squares. Since $\mathbb{F}_q^\times$

cyclic this subgroup is normal and so via the Galois correspondence there is a unique quadratic subfield F of K. No prime $p \neq q$ ramifies in F since they do not ramify in K by theorem **2.3.2**. Thus q is the only ramified prime, and must be the discriminant of F. If $q \equiv 1 \bmod 4$, then $D_{\mathbb{Q}(\sqrt{q})} = q$ so $F = \mathbb{Q}(\sqrt{q})$. If $q \equiv 3 \bmod 4$ then $D_{\mathbb{Q}(\sqrt{d})} = 4d$, but 2 will not ramify so the field must be $F = \mathbb{Q}(\sqrt{-q})$. To avoid splitting the proof into cases, set $q^* = (-1)^{(q-1)/2}q$ so that $F = \mathbb{Q}(\sqrt{q^*})$ covers them both.

Now let $p \neq q$ be a prime. Consider $(\frac{p}{K/\mathbb{Q}})$. By theorem **2.2.6** its restriction to F is $(\frac{p}{F/\mathbb{Q}})$. Since F is a quadratic field, $Gal(F/\mathbb{Q}) = G/H \cong \mathbb{Z}/2\mathbb{Z}$. The latter can be taken to be $\{+1, -1\}$ as a set. The squares in $\mathbb{F}_q^\times$ map to the identity $+1$, and the non squares to -1 under the projection onto G/H so that $(\frac{p}{F/\mathbb{Q}}) = (\frac{p}{q})$.

For the other identification, consider the decomposition of p in F. Recall theorem **2.1.6** on the ramification of primes in quadratic extensions, i.e. if q^* is a quadratic residue mod p then p splits, and if q^* is not, p remains prime. Now $(\frac{p}{F/\mathbb{Q}})$ is the identity if p splits since the decomposition group is trivial, and the non-identity element otherwise, so $(\frac{p}{F/\mathbb{Q}}) = (\frac{q^*}{p})$.

Put together

$$(\frac{p}{q}) = (\frac{q^*}{p}) = (\frac{-1}{p})^{(q-1)/2}(\frac{q}{p})$$

and Euler's Criterion finishes the proof for odd p.

For the case $p = 2$, again use the result on the splitting of primes in quadratic extensions. Following that, 2 splits if $q^* \equiv 1 \bmod 8$ and remains prime if $q^* \equiv 5 \bmod 8$. Now note that $(-1)^{((q^*)^2-1)/2} = 1$ if $q^* \equiv 1 \bmod 8$ and -1 if $q^* \equiv 5 \bmod 8$. Furthermore $(-1)^{((q^*)^2-1)/2} = (-1)^{(q^2-1)/2}$. Using the characterisation of $(\frac{2}{F/\mathbb{Q}})$ in splitting or not gives:

$$(\frac{2}{q}) = (\frac{2}{F/\mathbb{Q}}) = (-1)^{(q^2-1)/2}$$

□

As a remark note how the quadratic subfield was identified using discriminants. The observation being that the same primes ramified in the two extensions. This is closely related to the machinery in Chapter 3. One may compare the method used here to one stating that the conductor of the two extensions are equal.

Chapter 3

Class Field Theory

With the definitions from Chapter 2 in place, it will now be possible to state the main theorems of Class Field Theory.

3.1 Generalized Class Groups

In order to define the main theorems in this chapter, a generalization of the notion of the class group of a number field is needed. The first concept that is required is that of a **modulus**. This in turn demands an extension of the concept of primes of a number field. In addition to the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, there is the following:

Definition 3.1.1. *An **infinite prime** of a number field K is an embedding σ into an archimedean completion of K. If $\sigma : K \to \mathbb{R}$, it is called a real prime. If $\sigma : K \to \mathbb{C}$ is one of a pair of distinct conjugate embeddings, it is called a complex prime.*

The notion of ramification of a prime in an extension L/K can be extended to the infinite primes. An infinite prime of K **ramifies** in L if it is real but has an extension to L which is complex. As an example, $\mathbb{Q}$ has one real prime. It is unramified in a real quadratic extension, but ramifies in an imaginary.

Definition 3.1.2. *Let K be a number field. A **modulus** in K is a formal product*

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

over all primes of K such that:

1) $n_{\mathfrak{p}} \geq 0$ *and at most finitely many are nonzero.*

2) $n_{\mathfrak{p}} = 0$ *for all complex infinite primes.*

3) $n_{\mathfrak{p}} \leq 1$ *for all real infinite primes.*

It is thus possible and often convenient to factor a modulus $\mathfrak{m}$ into its finite and infinite parts. Write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_\infty$ are the real infinite primes. $\mathfrak{m}_0$ is clearly an ideal in $\mathcal{O}_K$.

Recall that the definition of a class group used the fractional ideals of $\mathcal{O}_K$. Given a modulus $\mathfrak{m}$ in a number field K define $I_K(\mathfrak{m})$ to be the group of all fractional ideals of $\mathcal{O}_K$ relatively prime to $\mathfrak{m}$.

The next construction is to extend the Artin map given in Chapter 2 to fractional ideals. Given an abelian extension of number fields L/K, a modulus $\mathfrak{m}$ in K and the map $\mathfrak{p} \to (\frac{\mathfrak{p}}{L/K})$, extend the map to a homomorphism: $\omega : I_K(\mathfrak{m}) \to Gal(L/K)$ by multiplicativity. That is; given $\mathfrak{a} \in I_K(\mathfrak{m}), \mathfrak{a} = \prod \mathfrak{p}_i^{n_i}$, define $(\frac{\mathfrak{a}}{L/K}) = \prod(\frac{\mathfrak{p}_i}{L/K})^{n_i}$.

Definition 3.1.3. *The homomorphism $\omega : I_K(\mathfrak{m}) \to Gal(L/K)$ is called the* ***Artin map*** *or* ***reciprocity law map****.*

The notation for the Artin map will be augmented with subscripts when either the extension or the modulus is not obvious from the context. To further the generalization of the class group, consider the subgroup of $I_K(\mathfrak{m})$ generated by principal ideals $(\alpha) \subset \mathcal{O}_K$ such that $\alpha \equiv 1$ modulo $\mathfrak{m}_0$ and $\sigma(\alpha) > 0$ for all $\sigma|\mathfrak{m}_\infty$. This subgroup will be denoted $P_{K,1}(\mathfrak{m})$.

Definition 3.1.4. *Let $P_{K,1}(\mathfrak{m})$ be as above. A subgroup H of $I_K(\mathfrak{m})$ is called a* ***congruence subgroup*** *if it satisfies $P_{K,1}(\mathfrak{m}) \subseteq H \subset I_K(\mathfrak{m})$. Furthermore, the quotient $I_K(\mathfrak{m})/H$ is called a* ***generalized ideal class group*** *for the modulus.*

Comparing this with the definition of the class group in chapter 1, the class group is a generalized ideal class group with the modulus 1.

3.2 Three theorems of Class Field Theory

The definitions in the previous section will now lend themselves to a very nice theorem due to Artin, one which the rest of this chapter will focus around.

Theorem 3.2.1 (The Artin Reciprocity Theorem)**.** *Let L be an abelian extension of a number field K, and let $\mathfrak{m}$ be a modulus divisible by all the primes that ramify the extension. Then:*

i) The Artin map is surjective

ii) If the exponents of the finite primes of the modulus are sufficiently large, then the kernel of the Artin map is a congruence subgroup. This gives the isomorphism

$$I_K(\mathfrak{m})/ker(\omega) \simeq Gal(L/K)$$

Part *ii*) of the theorem realizes the Galois group of the extension as a generalized ideal class group for the modulus. It relies on a a rather vague statement of 'sufficiently large'. There is however another theorem that gives an admissive modulus, as well as constraints on any other:

Theorem 3.2.2 (The Conductor Theorem)**.** *Let L be an Abelian extension of a number field K. Then there exist a modulus $\mathfrak{f}$ such that:*

i) *$\mathfrak{f}$ is divisible by all the primes of K that ramify in L.*

ii) *Given a modulus $\mathfrak{m}$ divisible by all the primes of K that ramify in L, it holds that $ker(\omega)$ is a congruence subgroup if and only if $\mathfrak{f}$ divides $\mathfrak{m}$*

*The modulus $\mathfrak{f}$ is called the **conductor** of L/K.*

The final component is a rather nice theorem that will allow constructions of extensions with given Galois groups and ramification. This theorem relates congruence subgroups with extensions:

Theorem 3.2.3 (The Existence Theorem)**.** *Given a number field K with a modulus $\mathfrak{m}$ and a congruence subgroup H for $\mathfrak{m}$, there exist a unique Abelian extension L such that all primes that ramify in L divides $\mathfrak{m}$ and such that $ker(\omega) = H$.*

These three theorems together gives a very strong description of Abelian extensions of a number field in terms of congruence subgroups of the fractional ideals. The reciprocity theorem states that for sufficiently nice moduli, the Artin map is surjective and the kernel is a congruence subgroup. In effect, the Galois group of the extension is found as a quotient in the group of fractional ideals relatively prime to the modulus. The conductor theorem gives an explicit modulus for a given Abelian extension, and gives a criterion to any other modulus. Finally, the existence theorem gives us a way of finding abelian extensions with particular congruence subgroups and ramification.

The final result to be given in this section is a corollary to the Existence Theorem:

Corollary 3.2.3.1. *Let K be a number field with two abelian extensions L and M. Then L is a subextension of M if and only if there exist some modulus $\mathfrak{m}$ such that*

$$P_{K,1}(\mathfrak{m}) \subset ker(\omega_{M/K}) \subset ker(\omega_{L/K})$$

3.3 Applications: Quadratic Reciprocity revisited and Kronecker-Weber

With these results in place, it is time to turn to some applications. The examples in this section rely on those of the previous, and are chosen such that proofs can be given to demonstrate some of the workings of the theory. The proofs are taken from [1, Chapter 8].

The name "reciprocity" for theorem **3.2.1** is connected to the power of the theorem to derive reciprocity theorems in the vein of quadratic reciprocity and its higher order variants. One way see the connection is via the Weak Reciprocity theorem, which will be stated here and used to reformulate the provious proof of quadratic reciprocity. The first point of order is to introduce the n:th power Legendre Symbol.

Definition 3.3.1. *Let K be a number field containing ζ_n. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and let $\alpha, n \in \mathcal{O}_K$ be relatively prime to $\mathfrak{p}$. Then define the* ***n:th power Legendre Symbol*** *$(\frac{\alpha}{\mathfrak{p}})_n$ to be the unique n:th root of unity satisfying*

$$\alpha^{(N(\mathfrak{p})-1)/n} \equiv (\frac{\alpha}{\mathfrak{p}})_n \ mod\ \mathfrak{p}$$

The uniqueness and existence of which follows from Fermat's little theorem [1, Ch 8, after Thm 8.10]. The next step is to extend this multiplicatively, similarly to what was done with the Artin map. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$, $\mathfrak{a} = \prod \mathfrak{p}_\mathfrak{i}$. Then

$$(\frac{\alpha}{\mathfrak{a}})_n = \prod (\frac{\alpha}{\mathfrak{p}_\mathfrak{i}})_n$$

The upshot of this is that if we have a modulus $\mathfrak{m}$ such that every prime containing $n\alpha$ divides $\mathfrak{m}$, then this defines a homomorphism $I_K(\mathfrak{m}) \to \mu_n$ for μ_n as the group of n:th roots of unity.

Recall from Galois theory that there is a natural injection

$$\varphi : Gal(K(\sqrt[n]{\alpha})/K) \hookrightarrow \mu_n$$

by associating $\sigma \in Gal(K(\sqrt[n]{\alpha})/K)$ with the ζ for which $\sigma(\sqrt[n]{\alpha}) = \zeta \sqrt[n]{\alpha}$ [1, Ch 8, before Thm 8.11].

Theorem 3.3.2 (Weak Reciprocity)**.** *Let K be a number field containing ζ_n and let $L = K(\sqrt[n]{\alpha})$ for $\alpha \in \mathcal{O}_K$. Assume that $ker(\omega_{L/K,\mathfrak{m}})$ is a congruence subgroup for a modulus $\mathfrak{m}$ divisible by all primes containing $n\alpha$. Then the following commutes:*

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\omega} & Gal(L/K) \\ & \searrow^{(\frac{\alpha}{\cdot})_n} & \downarrow \varphi \\ & & \mu_n \end{array}$$

Thus if the image of φ is G, there is a surjective homomorphism $(\frac{\alpha}{\cdot})_n : I_K(\mathfrak{m})/P_{K,1} \to G$.

Proof. To prove that the diagram commutes, it suffices to show that

$$(\frac{\mathfrak{p}}{L/K})(\sqrt[n]{\alpha}) = (\frac{\alpha}{\mathfrak{p}})_n \sqrt[n]{\alpha}.$$

Recall how this was already done in the case of the quadratic Legendre in the earlier proof of quadratic reciprocity. The result follows from the definition of the Legendre, noting that the Artin symbol can be rewritten in terms of norms as $(\frac{\mathfrak{p}}{L/K})(\alpha) \equiv \alpha^{N(\mathfrak{p})}$ so $(\frac{\mathfrak{p}}{L/K})(\sqrt[n]{\alpha}) \equiv \alpha^{\frac{N(\mathfrak{p})}{n}}$.

The second part follows from commutativity of the diagram together with the Artin Reciprocity theorem. □

This theorem, while interesting in its own right, can be leveraged into rephrasing the proof of quadratic reciprocity. First there is need of a lemma, which is an example of the Artin Reciprocity:

Lemma 3.3.3. *Let $Q(\zeta_m)$ be a cyclotomic extension of $\mathbb{Q}$. Then*

$ker(\omega_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}, \mathfrak{m}) = P_{\mathbb{Q},1}$ for the modulus $\mathfrak{m} = m\mathfrak{m}_\infty$.

Proof. As noted in **2.3.2**, for a prime in $\mathbb{Q}(\zeta_m)$ to ramify, they must divide m. Thus, consider the modulus $\mathfrak{m} = m\mathfrak{m}_\infty$. Take $\frac{a}{b}\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m})$ such that a and b are relatively prime to m. Identifying $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$ note that $\omega(\frac{a}{b}\mathbb{Z}) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$ by the definition of the Artin map. The kernel consists those fractional ideals $\frac{a}{b}\mathbb{Z}$ for which $[a][b]^{-1} \equiv 1$. That is, the kernel is precisely $P_{\mathbb{Q},1}(\mathfrak{m})$. □

This lemma will be useful for both following theorems. First a restated proof of theorem **2.3.5** which uses the Artin Reciprocity to derive the Quadratic Reciprocity:

Proof. The strategy is as in the proof of chapter 2 to show that $(\frac{p^*}{q}) = (\frac{q}{p})$. The idea is to show that both symbols define surjective homomorphisms from the same group to a certain cyclic, and therefore must be equal.

By lemma **3.3.3**, $Gal(\mathbb{Q}(\zeta_p), \mathbb{Q})$ is a congruence subgroup for the modulus $\mathfrak{k} = p\mathfrak{m}_\infty$. This implies that for any subfield K with $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_p)$ there is $Gal(K/\mathbb{Q})$ as a congruence subgroup. As noted in the previous proof, $\mathbb{Q}(\zeta_p)$ contains a unique quadratic subfield $K = \mathbb{Q}(\sqrt{p*})$.

Thus $ker(\omega_{K/\mathbb{Q},\mathfrak{k}})$ is a congruence subgroup for $\mathfrak{k}$. By the theorem **3.3.2** we get a a sujective homomorphism onto the group of second roots of unity:

$$(\frac{p^*}{\cdot}) : I_{\mathbb{Q}}(\mathfrak{k})/P_{\mathbb{Q},1}(\mathfrak{k}) \to \{\pm 1\}$$

According to lemma **3.3.2** and theorem **3.2.1** there is the isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong I_{\mathbb{Q}}(\mathfrak{k})/P_{\mathbb{Q},1}(\mathfrak{k})$. Composing these two gives a surjective homomorphism from $\mathbb{Z}/p\mathbb{Z}^\times$ onto $\{\pm 1\}$. However, the Legendre $(\frac{\cdot}{p})$ is also a surjective homomorphism between the same two groups, and by cyclicity of $(\mathbb{Z}/p\mathbb{Z})^\times$, they must be equal. □

The final theorem to be presented is Kronecker-Weber. Using all the machinery presented in this chapter, the proof given here is remarkably brief:

Theorem 3.3.4 (Kronecker-Weber)**.** *Let K be an abelian extension of $\mathbb{Q}$. Then there exist a cyclotomic extension $\mathbb{Q}(\zeta_m)$ such that $K \subset \mathbb{Q}(\zeta_m)$.*

Proof. By theorem **3.2.1** and **3.2.2** there is some modulus $\mathfrak{m}$ such that $P_{K,1} \subset ker(\omega_{K/\mathbb{Q},\mathfrak{m}})$. Take $\mathfrak{m}$ to be $m\mathfrak{m}_\infty$. Lemma **3.3.3** yields $ker(\omega_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) = P_{\mathbb{Q},1}$. Thus

$$P_{\mathbb{Q},1} = ker(\omega_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) \subset ker(\omega_{K/\mathbb{Q}})$$

Now according to corollary **3.2.3.1**: $L \subset \mathbb{Q}(\zeta_m)$. □

Bibliography

[1] D. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley, 2013

[2] D. Dummit, R. Foote, *Abstract Algebra*, Wiley, 2004

[3] S. Lang, *Algebra*, Springer-Verlag, 2005

[4] S. Lang, *Algebraic Number Theory*, Springer-Verlag, 1986

[5] D.A. Marcus, *Number Fields*, Springer-Verlag, 1977

[6] P. Samuel, *Algebraic Theory of Numbers*, Dover, 2008