Algebraic Number Theory

Wintersemester 2013/14
Universität Ulm

Stefan Wewers
Institut für Reine Mathematik

vorläufige und unvollständige Version

Stand: 9.2.2014

Contents

Introduction

Two curious facts

Consider the following spiral configuration of the natural numbers $n \geq 41$:

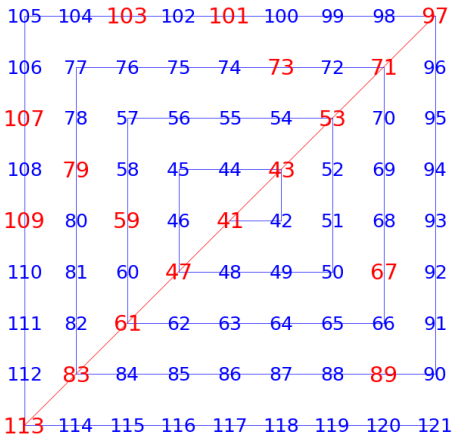


Figure 1: The Ulam spiral, starting at $n = 41$

The numbers printed in red are the prime numbers occuring in this list. Rather surprisingly, *all* numbers on the minor diagonal are prime numbers (at least in the range which is visible in Figure 1). Is this simply an accident? Is there an easy explanation for this phenomenon?

Visual patterns like the one above were discovered by Stanislav Ulam in 1963 (and are therefore called *Ulam spirals*), but the phenomenon itself was already known to Euler. More specifically, Euler noticed that the polynomial

$$f(n) = n^2 - n + 41$$

takes surprisingly often prime values. In particular, $f(n)$ is prime for all $n = 1, \ldots, 40$. An easy computation shows that the numbers $f(n)$ are precisely the numbers on the minor diagonal of the spiral in Figure 1. This connects Euler's to Ulam's observation.

Here is another curios fact. Compute a decimal approximation of $e^{\pi\sqrt{n}}$ for $n = 1, 2, \ldots$ and look at the digits after the decimal point. One notices that for a few n's, the real number $e^{\pi\sqrt{n}}$ is very close to an integer. For instance, for $n = 163$ we have

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999726263\ldots$$

Again one can speculate whether this is a coincidence or not.

Amazingly, both phenomena are explained by the same fact: the subring $\mathbb{Z}[\alpha] \subset \mathbb{C}$, with $\alpha := (1 + \sqrt{-163})/2$, is a unique factorization domain!

To see that the first phenomenon has something to to with the ring $\mathbb{Z}[\alpha]$, it suffices to look at the factorization of the polynomial $f(n)$ over $\mathbb{C}$:

$$f(n) = n^2 - n + 41 = \big(n - \frac{1+\sqrt{-163}}{2}\big)\big(n - \frac{1-\sqrt{-163}}{2}\big).$$

Using this identity we will be able to explain, later during this course, why $f(n)$ is prime for $n = 1, \ldots, 40$ (see Example 2.6.27). But before we can do this we have to learn a lot about the arithmetic of rings like $\mathbb{Z}[\alpha]$.

The explanation for the second phenomenon is much deeper and requires the full force of *class field theory* and *complex multiplication*. We will not be able to cover these subjects in this course. However, at the end we will have learned enough theory to be able to read and understand books that do (e.g. [3]). For a small glimpse, see §1.3 and in particular Example 1.3.12.

Algebraic numbers and algebraic integers

The two examples we just discussed are meant to illustrate the following point. Although number theory is traditionally understood as the study of the ring of integers $\mathbb{Z}$ (or the field of rational numbers $\mathbb{Q}$), there are many mysteries which become more transparent if we pass to a bigger ring (such as $\mathbb{Z}[\alpha]$, with $\alpha = (1+\sqrt{-163})/2$, for instance). However, we should not make the ring extension too big, otherwise we will loose too many of the nice properties of the ring $\mathbb{Z}$. The following definition is fundamental.

Definition 0.0.1 A complex number $\alpha \in \mathbb{C}$ is called an *algebraic number* if it is the root of a nonconstant polynomial $f = a_0 + a_1 x + \ldots + a_n x^n$ with rational $a_0, \ldots, a_n \in \mathbb{Q}$ (and $a_n \neq 0$).

An algebraic number α is called an *algebraic integer* if it is the root of a monic polynomal $f = a_0 + a_1 x + \ldots + x^n$, with integral coefficients $a_0, \ldots, a_{n-1} \in \mathbb{Z}$.

We let $\bar{\mathbb{Q}} \subset \mathbb{C}$ denote the set of all algebraic numbers, and $\bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}$ the subset of algebraic integers. One easily proves that $\bar{\mathbb{Q}}$ is a field and that $\bar{\mathbb{Z}}$ is a ring. Moreover, $\bar{\mathbb{Q}}$ is the fraction field of $\bar{\mathbb{Z}}$. See §???.

In some sense, algebraic number theory is the study of the field $\bar{\mathbb{Q}}$ and its subring $\bar{\mathbb{Z}}$. However, $\bar{\mathbb{Q}}$ and $\bar{\mathbb{Z}}$ are not very nice objects from an algebraic point of view because they are 'too big'.

Definition 0.0.2 A *number field* is a a subfield $K \subset \bar{\mathbb{Q}}$ which is a finite field extension of $\mathbb{Q}$. In other words, we have

$$[K : \mathbb{Q}] := \dim_{\mathbb{Q}} K < \infty.$$

We call $[K : \mathbb{Q}]$ the *degree* of the number field K. The subring

$$\mathcal{O}_K := K \cap \bar{\mathbb{Z}}$$

of all algebraic integers contained in K is called the *ring of integers* of K.

To be continued..

1 Roots of algebraic number theory

Before we introduce and study the main concepts of algebraic number theory in general, we discuss a few classical problems from elementary number theory. These problems were historically important for the development of the modern theory, and are still very valuable to illustrate a point we have already emphasized in the introduction: by studying the arithmetic of number fields, one discovers patterns and laws between 'ordinary' numbers which would otherwise remain mysterious. In writing this chapter, I was mainly inspired by the highly recommended books [5] and [3].

1.1 Unique factorization

Here is the most fundamental result of elementary number theory (sometimes called the *Fundamental Theorem of Arithmetic*):

Theorem 1.1.1 (Unique factorization in $\mathbb{Z}$) *Every nonzero integer $m \in \mathbb{Z}$, $m \neq 0$, can be written as*

$$m = \pm p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}, \tag{1}$$

where $p_1, \ldots, p_r$ are pairwise distinct prime numbers and $e_i \geq 1$. Moreover, the primes p_i and their exponents e_i are uniquely determined by m.

For a proof, see e.g. [5], §1.1. We call (1) the *prime factorization* of m and we call

$$\mathrm{ord}_p(m) := \begin{cases} e_i, & p = p_i, \\ 0, & p \neq p_i \ \forall i \end{cases}$$

the *order* of p in m (for any prime number p). This is well defined because of the uniqueness statement in Theorem 1.1.1. The following three results follow easily from Theorem 1.1.1. However, a typical proof of Theorem 1.1.1 proceeds by proving at least one of these results first, and then deducing Theorem 1.1.1. For instance, the first known proof of Theorem 1.1.1 in Euclid's *Elements* (Book VII, Proposition 30 and 32) proves the following statement first:

Corollary 1.1.2 (Euclid's Lemma) *Let p be a prime number and $a, b \in \mathbb{Z}$. Then*

$$p \mid ab \qquad \Rightarrow \qquad p \mid a \quad \text{or} \quad p \mid b. \tag{2}$$

Corollary 1.1.3 *For $a, b \in \mathbb{Z}$, $a, b \neq 0$, we denote by $\gcd(a, b)$ the greatest common divisor of a, b, i.e. the largest $d \in \mathbb{N}$ with $d \mid a$ and $d \mid b$.*

(i) *If d is a common divisor of a, b then $d \mid \gcd(a, b)$.*

(ii) *For $a, b, c \in \mathbb{Z} \backslash \{0\}$ we have*

$$\gcd(ab, ac) = a \cdot \gcd(b, c).$$

Corollary 1.1.4 *For $p \in \mathfrak{P}$ and $a, b \in \mathbb{Z}\backslash\{0\}$ we have*

$$\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$$

and

$$\mathrm{ord}_p(a+b) \geq \min\big(\mathrm{ord}_p(a), \mathrm{ord}_p(b)\big)$$

(To include the case $a + b = 0$ we set $\mathrm{ord}_p(0) := \infty$).

In the proof of *every*[1] nontrivial theorem in elementary number theory, Theorem 1.1.1 (or one of its corollaries) is used at least once. Here is a typical example.

Theorem 1.1.5 *Let $(x, y, z) \in \mathbb{N}^3$ be a Pythagorean tripel, i.e. a tripel of natural numbers which are coprime and satisfy the equation*

$$x^2 + y^2 = z^2. \tag{3}$$

Then the following holds.

(i) *One of the two numbers x, y is odd and the other even. The number z is odd.*

(ii) *Assume that x is odd. Then there exists coprime natural numbers $a, b \in \mathbb{N}^2$ such that $a > b$, $a \not\equiv b \pmod 2$ and*

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2.$$

Proof: We first remark that our assumption shows that x, y, z are *pairwise* coprime. To see this, suppose that p is a common prime factor of x and y. Then p divides z^2 by (3), and Corollary 1.1.2 shows that p divides z. But this contradicts our assumption that the tripel x, y, z is coprime and shows that x, y are coprime. The argument for x, z and y, z is the same.

Since x, y are coprime, they cannot be both even. Suppose x, y are both odd. Then a short calculation shows that

$$x^2, y^2 \equiv 1 \pmod 4.$$

Likewise, we either have $z^2 \equiv 1 \pmod 4$ (if z is odd) or $z^2 \equiv 0 \pmod 4$ (if z is even). We get a contradiction with (3). This proves (i).

For the proof of (ii) we rewrite (3) as

$$y^2 = z^2 - x^2 = (z - x)(z + x). \tag{4}$$

Using

$$2x = (z + x) - (z - x), \quad 2z = (z + x) + (z - x),$$

[1] with Theorem 1.1.1 as the only exception

Corollary 1.1.3 and the fact that x, z are coprime we see that

$$\gcd(z+x, z-x) = \gcd(2x, 2z) = 2 \cdot \gcd(x, z) = 2.$$

We write $z + x = 2u$, $z - x = 2v$, $y = 2w$, with $u, v, w \in \mathbb{N}$. Then u, v are coprime and (4) can be written as

$$w^2 = uv. \tag{5}$$

If p is a prime factor of u, then it does not not divide v. Hence Corollary 1.1.4 shows that

$$\mathrm{ord}_p(u) = \mathrm{ord}_p(uv) = 2\mathrm{ord}_p(w).$$

We see that $\mathrm{ord}_p(u)$ is even for all prime numbers p. Since, moreover, $u > 0$, it follows that u is a square, i.e. $u = a^2$ (here we use again Theorem 1.1.1!). Similarly, $v = b^2$ and hence $w = ab$. We conclude that

$$x = \frac{z+x}{2} - \frac{z-x}{2} = a^2 - b^2, \quad y = 2ab, \quad z = \frac{z+x}{2} + \frac{z-x}{2} = a^2 + b^2,$$

finishing the proof. □

Remark 1.1.6 There is an easy converse to Theorem 1.1.5: given two coprime numbers $a, b \in \mathbb{N}$, such that $a > b$ and $a \not\equiv b \pmod 2$, then

$$x := a^2 - b^2, \quad y := 2ab, \quad z := x^2 + y^2$$

is a Pythagorean triple. By Theorem 1.1.5, we get *all* Pythagorean tripel (for which y is even) in this way. Here is a table for the first 4 cases:

a	b	x	y	z
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25

Euclidean domains

Theorem 1.1.1 is a fundamental but not a trivial result. It requires a careful proof because it does not hold for arbitrary rings.

Example 1.1.7 Let $R := \mathbb{Z}[\sqrt{5}] \subset \mathbb{R}$ denote the smallest subring of $\mathbb{R}$ containing $\sqrt{5}$. It is easy to see that every element $\alpha \in \mathbb{Z}[\sqrt{5}]$ can be written uniquely as

$$\alpha = a + b\sqrt{5},$$

with $a, b \in \mathbb{Z}$. Consider the identities

$$2^2 = 4 = (1+\sqrt{5})(-1+\sqrt{5}). \tag{6}$$

We have written the ring element 4 as a product of two factors, in two essentially different ways. By this we mean the following. It is easy to see that the element $2 \in R$ cannot be written as the product of two nonunits. We say that $2 \in R$ is *irreducible*. If a naive generalization of Theorem 1.1.1 to the ring R would hold, then 2 would behave like a *prime element* of R, i.e. satisfy the implication (2) of Corollary 1.1.2. But it doesn't: (6) shows that 2 divides the product of the right hand side but none of its factors.

The example above shows that, in order to prove Theorem 1.1.1 we need to use certain special properties of the ring $\mathbb{Z}$. Looking carefully at any proof of Theorem 1.1.1 one sees that the heart of the matter is *division with remainder* or, what amounts to the same, the *euclidean algorithm*. So let us define a class of rings in which the euclidean algorithm works.

Definition 1.1.8 Let R be an integral domain (i.e. a commutative ring without zero divisors). We say that R is a *euclidian domain* if there exists a function $N : R\backslash\{0\} \to \mathbb{N}_0$ with the following property. Given two ring elements $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r, \quad \text{and either} \quad r = 0 \quad \text{or} \quad N(r) < N(b).$$

A function $N : R\backslash\{0\} \to \mathbb{N}_0$ with this property is called a *euclidean norm* on R.

Example 1.1.9 For $R = \mathbb{Z}$ the absolute value $N(a) := |a|$ is a euclidean norm. For the polynomial ring $k[x]$ over a field k the degree function $\deg : k[x]\backslash\{0\} \to \mathbb{N}_0$ is a euclidean norm function as well.

Definition 1.1.10 Let R be an integral domain. Recall that an *ideal* of R is a subgroup $I \subset (R, +)$ of the additive group underlying R such that $a \cdot I \subset I$ for all $a \in R$. The ring R is called a *principle ideal domain* if every ideal I is *principal*, i.e. $I = (a)$ for some $a \in R$.

Proposition 1.1.11 *Any euclidean domain is a principal ideal domain.*

Proof: Let $N : R\backslash\{0\} \to \mathbb{N}_0$ be a euclidean norm on R and let $I \lhd R$ be an ideal. We have to show that I is principal. If $I = (0)$ then there is nothing to show so we may assume that $I \neq (0)$. Clearly, the restriction of N to $I\backslash\{0\}$ takes a minimum. Let $d \in I$, $d \neq 0$, be an element such that $N(d)$ is minimal. We claim that $I = (d)$.

Since $d \in I$ we have $(d) \subset I$. To prove the other inclusion, we let $a \in I$ be an arbitrary element. By Definition 1.1.8 there exist $q, r \in R$ such that $a = qd + r$ and either $r = 0$ or $N(r) < N(d)$. However, $r = a - qd \in I$, so $r \neq 0$ and $N(r) < N(d)$ is impossible by the choice of d. We conclude that $r = 0$ and hence $a = qd \in (d)$. The proposition is proved. □

Corollary 1.1.12 (Existence of the gcd) *Let R be a euclidean domain and $a, b \in R$. Then there exists an element $d \in R$ with the following properties.*

(i) *The element d is a common divisor of a, b, i.e. $d \mid a$ and $d \mid b$.*

(ii) *If $d' \in R$ is a common divisor of a, b then $d' \mid d$.*

An element d satisfying (i) and (ii) is called a *greatest common divisor* of a, b.

Proof: Since R is a principal ideal domain we have $(a, b) = (d)$ for some element $d \in R$. The inclusion $(a, b) \subset (d)$ implies (i). Since $d \in (a, d)$ there exists $x, y \in R$ such that $d = xa + yb$. It follows that for any common divisor d' of a, b we have $d' \mid d$, proving (ii). □

Remark 1.1.13 The proofs of Proposition 1.1.11 and Corollary 1.1.20 can be easily made constructive, leading to the *extended euclidean algorithm*. More precisely, given two elements a, b of a euclidean domain R, with $b \neq 0$, we can compute a greatest common divisor of a, b by successive division with remainder:

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ \vdots \quad &\quad \vdots \quad \quad \vdots \end{aligned}$$

As long as $r_k \neq 0$ we have $N(r_1) > N(r_2) > \ldots > N(r_k)$. But this process must terminate at some point, i.e. there exists k such that $r_k \neq 0$ and $r_{k+1} = 0$ (if $r_1 = 0$ then we set $r_0 := b$). One easily shows that r_k is a greatest common divisor of a, b and can be written in the form

$$r_k = xa + yb, \qquad x, y \in R.$$

Definition 1.1.14 Let R be an integral domain. We write $R^\times$ for the group of units of R.

(i) Two elements $a, b \in R$ are called *associated* (written $a \sim b$) if $a = bc$ for a unit $c \in R^\times$. (Equivalently, we have $a \mid b$ and $b \mid a$.)

(ii) An element $a \in R$ is called *irreducible* if

  (a) $a \neq 0$,

  (b) a is not a unit, and

  (c) for any factorization $a = bc$, we have either $b \in R^\times$, $a \sim c$, or $c \in R^\times$, $a \sim b$.

(iii) Let $a \in R$ satisfy (a) and (b) from (ii). We call a a *prime element* if the following implication holds for all $b, c \in R$:

$$a \mid bc \quad \Rightarrow \quad a \mid b \text{ or } a \mid c.$$

It is easy to see that prime elements are irreducible. Example 1.1.7 shows that the converse does not hold. Indeed, 2 and $\pm 1 + \sqrt{5}$ are irreducible elements of $R = \mathbb{Z}[\sqrt{5}]$, but none of them is a prime element (see Exercise 1.3.1).

Definition 1.1.15 Let R be an integral domain. The ring R is called *factorial* (or a *unique factorization domain*) if every element $a \neq 0$ has a factorization of the form

$$a = u \cdot p_1 \cdot \ldots \cdot p_r, \tag{7}$$

where $u \in R^\times$ is a unit and $p_1, \ldots, p_r$ are irreducible, and moreover, the factorization (7) is essentially unique, in the following sense. If

$$a = v \cdot q_1 \cdot \ldots q_s$$

is another factorization with a unit v and irreducible elements q_i, then $r = s$, and there exists a permutation $\sigma \in S_r$ such that $q_i \sim p_{\sigma(i)}$ for all i.

By the following proposition, every principal ideal domain is factorial.

Proposition 1.1.16 *Let R be a principal ideal domain. Then the following holds.*

(i) *Every irreducible element of R is prime.*

(ii) *Let $I_1 \subset I_2 \subset I_3 \subset \ldots$ be an ascending chain of ideals of R. Then there exists $n \in \mathbb{N}$ such that $I_n = I_m$ for all $m \geq n$.*

(iii) *R is factorial.*

Proof: Let $a \in R$ be irreducible, and let $b, c \in R$ be elements such that $a \mid bc$. We have to show that $a \mid b$ or $a \mid c$. Let

$$I = (a, b) := \{xa + yb \mid x, y \in R\}$$

be the ideal generated by a, b. By assumption $I = (d)$ for some element $d \in R$. In particular, we have $d \mid a$ and $d \mid b$. Since a is irreducible, we can distinguish two cases. In the first case, $a \sim d$ which implies $a \mid d \mid b$, so we are done. In the second case, d is a unit and hence $I = R$. This means that there exist $x, y \in R$ such that

$$1 = xa + yb.$$

Multiplying with c we obtain the identity

$$c = xca + ybc.$$

Using the assumption $a \mid bc$ we conclude that $a \mid c$. This completes the proof of (i).

Let $I_1 \subset I_2 \subset I_3 \subset \ldots$ be an ascending chain of ideals of R. Then $I := \cup_n I_n$ is also an ideal, and hence $I = (a)$ for some a. Choose $n \in \mathbb{N}$ such that $a \in I_n$.

Then $I = (a) \subset I_n$ which immediately implies $I_n = I_{n+1} = \ldots = I$ and proves (ii).

For the proof of (iii) we first show, by contradiction, the existence of a factorization (7). So we assume that there exists an element $a \in R$, $a \neq 0$, which has no factorization into irreducibles elements. Then a is not irreducible and not a unit. This means that a admits a factorization $a = b_1 c_1$, where b_1, c_1 are nonunits. Moreover, one of the elements b_1, c_1 cannot be factored into irreducible elements (otherwise we could factor a as well). Say that b_1 cannot be factored. Repeating the same argument as before we obtain a factorization $b_1 = b_2 c_2$, where b_2, c_2 are nonunits and b_2 cannot be factored into irreducibles. Continuing this way we obtain a sequence of elements $b_1, b_2, \ldots$ such that $b_{n+1} \mid b_n$ and $b_n \nmid b_{n+1}$. In other words, the chain of ideals

$$(b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq \ldots$$

is strictly increasing. But this contradicts (ii). We conclude that every element $a \neq 0$ has a factorization into irreducible elements, as in (7).

It remains to prove uniqueness. Suppose we have two factorizations of a,

$$u \cdot p_1 \cdot \ldots \cdot p_r = a = v \cdot q_1 \cdot \ldots \cdot q_s, \tag{8}$$

with units u, v and irreducible elements p_i, q_j. We may assume that $1 \leq r \leq s$. In particular,

$$p_r \mid q_1 \cdot \ldots \cdot q_s.$$

By (i) p_r is a prime element, and hence $p_r \mid q_j$ for some j. After reordering we may assume that $p_r \mid q_s$. Since p_r and q_s are irreducible, we even have $p_r \sim q_s$. Dividing both sides of (8) by p_r we obtain

$$u \cdot p_1 \cdot \ldots \cdot p_{r-1} = v' \cdot q_1 \cdot \ldots \cdot q_{s-1},$$

with a new unit v'. The proof is now finished by an obvious induction argument. □

We remark that the converse to (iii) does not hold, i.e. there are factorial domains which are not principal ideal domains. A typical example is the polynomial ring $k[x_1, \ldots, x_n]$ over a field with $n \geq 2$ generators.

Combining Proposition 1.1.11 and Proposition 1.1.16 we obtain:

Corollary 1.1.17 *Every euclidean domain is factorial.*

In particular, this proves Theorem 1.1.1. We can summarize our general discussion of unique factorization by saying that we have established the following hierarchy of rings:

euclidian domains
$\cap$
principal ideal domains
$\cap$

unique factorization domains
$\cap$
integral domains

The ring of integers $\mathcal{O}_K$ of a number field K, which is the main object of study in algebraic number theory, is an integral domain but typically not a unique factorization domain. The two examples $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ considered below are rather special. However, $\mathcal{O}_K$ does belong to a very important class of rings in between *integral* and *factorial*, called *Dedekind domains*.

The rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$

We discuss two examples of euclidean domains which are very useful in number theory.

Definition 1.1.18 (i) Let $\mathbb{Z}[i] \subset \mathbb{C}$ denote the smallest subring of $\mathbb{C}$ containing the imaginary unit i. This ring is called the *ring of Gaussian integers*.

(ii) Set $\omega := e^{2\pi i}/3 = (-1+i\cdot\sqrt{3})/2 \in \mathbb{C}$. We denote by $\mathbb{Z}[\omega] \subset \mathbb{C}$ the smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and ω. It is called the *ring of Eisenstein*[2] *integers*.

It is clear that every element $\alpha \in \mathbb{Z}[i]$ can be uniquely written as

$$\alpha = x + y \cdot i, \qquad \text{with } x, y \in \mathbb{Z}.$$

Similarly, every element of $\mathbb{Z}[\omega]$ is of the form $z = x + y\omega$, with $x, y \in \mathbb{Z}$. Here we have used that ω satisfies the quadratic equation $\omega^2 + \omega + 1 = 0$. Hence addition and multiplication in $\mathbb{Z}[\omega]$ is given by the rules

$$\begin{aligned}(x_1 + y_1\omega) + (x_2 + y_2\omega) &= (x_1 + x_2) + (y_1 + y_2)\omega,\\ (x_1 + y_1\omega) \cdot (x_2 + y_2\omega) &= (x_1y_1 - y_1y_2) + (x_1y_2 + x_2y_1 - x_2y_2)\omega.\end{aligned}$$

The nice properties of the rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ can all be derived from the geometry of the embeddings $\mathbb{Z}[i], \mathbb{Z}[\omega] \subset \mathbb{C}$. In the second case this embedding is visualized by Figure 2.

An important feature of this embedding is that the square of the euclidean norm takes integral values: for $\alpha = x + iy \in \mathbb{Z}[i]$ we have

$$|\alpha|^2 = x^2 + y^2 \in \mathbb{N}_0.$$

Similarly, for $\alpha = x + y\omega \in \mathbb{Z}[\omega]$ we have

$$|\alpha|^2 = x^2 - xy + y^2 \in \mathbb{N}_0.$$

[2]Ferdinand Gotthold Max Eisenstein, 1823-1852, german mathematician

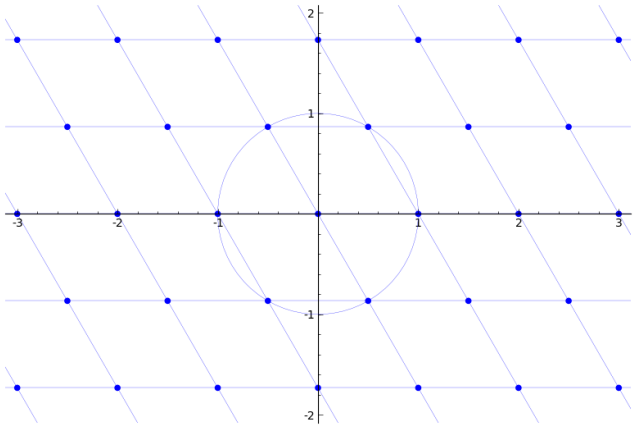


Figure 2: The ring of Eisenstein integers as a lattice in the complex plane

Proposition 1.1.19 *For both rings $R = \mathbb{Z}[i]$ and $R = \mathbb{Z}[\omega]$ the function*

$$N : R\backslash\{0\} \to \mathbb{N}, \qquad N(\alpha) := |\alpha|^2,$$

is a euclidean norm function.

Applying Corollary 1.1.17 we obtain:

Corollary 1.1.20 *The rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are factorial.*

Proof: (of Proposition 1.1.19) We prove this only for $\mathbb{Z}[\omega]$. The proof for $\mathbb{Z}[i]$ is similar. Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be given, with $\beta \neq 0$. Within the complex numbers, we can form the quotient α/β. It is of the form

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{|\beta|^2} = x + y\omega,$$

with $x, y \in \mathbb{Q}$. Choose $a, b \in \mathbb{Z}$ such that

$$|a - x|, |b - y| \leq 1/2$$

and set

$$\gamma := a + b\omega, \quad \rho := \alpha - \gamma\beta.$$

By definition we have

$$\alpha = \gamma\beta + \rho.$$

It remains to show that $N(\rho) < N(\beta)$. By the choice of γ we have

$$\begin{aligned} |\frac{\alpha}{\beta} - \gamma|^2 &= |(x - a) + (y - b)\omega|^2 \\ &= (x - a)^2 + (x - a)(y - b) + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4} < 1. \end{aligned}$$

We conclude that

$$N(\rho) = |\beta|^2 \cdot |\frac{\alpha}{\beta} - \gamma|^2 < |\beta|^2 = N(\beta).$$

This proves the proposition. □

Remark 1.1.21 The main argument of the proof of Proposition 1.1.19 may be phrased more geometrically as follows: if $D \subset \mathbb{C}$ is a disk with radius $r > 1/2$ inside the complex plane, then D contains at least one element of $\mathbb{Z}[\omega]$. This is related to the fact that the lattice of points $\mathbb{Z}[\omega] \subset \mathbb{C}$ corresponds to a so-called *dense sphere packing* of the plane.

As we will see in later chapters, the method of viewing algebraic integers as lattice points in a euclidean vector space is fundamental for algebraic number theory.

To understand the algebraic structure of $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ it is also important to know the unit groups.

Lemma 1.1.22 (i) *An element $\alpha \in \mathbb{Z}[i]$ (resp. an element $\alpha \in \mathbb{Z}[\omega]$) is a unit if and only if $N(\alpha) = 1$.*

(ii) *The group of units $\mathbb{Z}[i]^\times$ is a cyclic group of order 4 and consists precisely of the 4th roots of unity,*

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}.$$

(iii) *The group of units $\mathbb{Z}[\omega]^\times$ is a cyclic group of order 6 and consists precisely of the 6th roots of unity,*

$$\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}.$$

Proof: Let $R = \mathbb{Z}[i]$ or $R = \mathbb{Z}[\omega]$. Suppose $\alpha \in R$ is a unit. Then $N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = 1$. Since $N(\alpha), N(\alpha^{-1})$ are positive integers, it follows that $N(\alpha) = 1$. Conversely, if $N(\alpha) = \alpha\bar{\alpha} = 1$ then obviously $\alpha^{-1} = \bar{\alpha} \in \mathbb{Z}[\omega]$, and hence α is a unit. This proves (i). For the proof of (ii) one has to check that the Diophantine equation

$$N(\alpha) = x^2 + y^2 = 1$$

has exactly 4 solutions, namely $(x, y) = (\pm 1, 0), (0, \pm 1)$. This is clear. Similarly, one proves (iii) by showing that

$$N(\alpha) = x^2 + y^2 - xy = 1$$

has precisely six solutions, namely $(x, y) = (\pm 1, 0), (0, \pm 1), (1, 1), (-1, -1)$. □

Lemma 1.1.23 *Let $R = \mathbb{Z}[i]$ or $R = \mathbb{Z}[\omega]$.*

(i) *If the norm of an element $\alpha \in R$ is a prime number, i.e. $N(\alpha) = p \in \mathfrak{P}$, then α is a prime element of R. Moreover,*

$$p = \alpha \cdot \bar{\alpha}$$

is the prime factorization of p as an element of R.

(ii) *Let $p \in \mathfrak{P}$ be a prime number. Then either p is a prime element of R, or there is a prime element $\alpha \in R$ such that $p = N(\alpha) = \alpha\bar{\alpha}$.*

Proof: If $N(\alpha) = p \in \mathfrak{P}$ then it is clear that $\alpha \neq 0$ and that α is not a unit (Lemma 1.1.22 (i)). Suppose that $\alpha = \beta\gamma$ with $\beta, \gamma \in R$. Then

$$p = N(\alpha) = N(\beta) \cdot N(\gamma)$$

is a factorization of p in $\mathbb{N}$. It follows that $N(\beta) = 1$ or $N(\gamma) = 1$. Using Lemma 1.1.22 (i) we conclude that either β or γ is a unit. We have shown that α is an irreducible element of R. Now Proposition 1.1.16 (i) shows that α is a prime element. Since

$$p = N(\alpha) = N(\bar{\alpha}) = \alpha \cdot \bar{\alpha},$$

$\bar{\alpha}$ is a prime element, too, proving the second statement of (i).

For the proof of (ii) we assume that p is not a prime element of R, and we let $\alpha \in R$ be a prime divisor of p. Then $N(\alpha) = \alpha\bar{\alpha}|p^2$. But $N(\alpha) > 1$ (otherwise α would be a unit) and $N(\alpha) \neq p^2$ (otherwise $p \sim \alpha$ would be a prime element, contrary to our assumption). It follows that $N(\alpha) = p$. □

Example 1.1.24 Set

$$\lambda := 1 - \omega = \frac{3 - \sqrt{3}i}{2} \in \mathbb{Z}[\omega].$$

We have $N(\lambda) = 3$. Hence Lemma 1.1.23 (i) implies that λ is a prime element of $\mathbb{Z}[\omega]$. Moreover, the identity $3 = \lambda\bar{\lambda}$ is the decomposition of 3 in $\mathbb{Z}[\omega]$ into prime facors. But note that

$$\bar{\lambda} = 1 - \omega^2 = -\omega^2\lambda \sim \lambda.$$

Another way to write the prime factorization of 3 is therefore

$$3 = -\omega^2\lambda^2, \tag{9}$$

with λ as the only prime factor.

For later use we note the following lemma.

Lemma 1.1.25 (i) *The set $\{0, 1, -1\}$ is a set of representatives for the residue classes modulo λ:*

$$\mathbb{Z}[\omega]/(\lambda) = \{(\lambda), 1 + (\lambda), -1 + (\lambda)\}.$$

(ii) *The groups of units* $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ *is a set of representatives for the group of invertible residue classes modulo* λ^2.

(iii) *Suppose* $\alpha \equiv \beta \pmod{\lambda^k}$ *for* $\alpha, \beta \in \mathbb{Z}[\omega]$, $k \geq 1$. *Then*

$$\alpha^3 \equiv \beta^3 \pmod{\lambda^{k+2}}.$$

1.2 Fermat's Last Theorem

One of the highlights of modern number theory is without any doubt the proof by Andrew Wiles of the following theorem.

Theorem 1.2.1 (Wiles, 1995, [9]) *Let* $n \geq 3$. *Then there does not exist a tripel of positive integers* $x, y, z \in \mathbb{N}$ *with*

$$x^n + y^n = z^n. \tag{10}$$

Before Wiles' proof, the truth of this statement had been a famous open question for more than 300 years. Around 1640, Fermat had claimed (in a note written on the margin of a book) that *he had found a remarkable proof of this theorem, but unfortunately the margin he was writing on was too small to write it down.* For this reason Theorem 1.2.1 is often called *Fermat's Last Theorem.* For an account of the fascinating and amusing story of this problem and its final solution, see e.g. [7]

In this section we will use the special cases $n = 3, 4$ of Theorem 1.2.1 as a first motivating example. We will also briefly describe how the attempts to prove Fermat's Last Theorem have influenced the development of algebraic number theory.

Infinite descent

The case $n = 4$ of Fermat's Last Theorem is a corollary of the following proposition.

Proposition 1.2.2 *There is no tripel of positive integers* $x, y, z > 0$ *such that*

$$x^4 + y^4 = z^2. \tag{11}$$

Proof: We argue by contradiction. Suppose that $(x, y, z) \in \mathbb{N}^3$ is a solution for (11). It is then easy to see that we may assume the following:

(i) x, y, z are relatively prime,

(ii) x, z are odd and y is even,

(iii) z is minimal. More precisely, z is the smallest positive integer such that a solution $(x, y, z) \in \mathbb{N}^3$ for (11) exists.

The idea of the proof is to construct another solution $(x_1, y_1, z_1) \in \mathbb{N}^3$ of (11) with $z_1 < z$. This would be a contradiction to (iii), proving the proposition.

By assumption we have

$$(x^2)^2 + (y^2)^2 = z^2, \tag{12}$$

i.e. (x^2, y^2, z) is a pythagorean tripel. So by Theorem 1.1.5 (ii) there exist $a, b \in \mathbb{N}$, relatively prime, such that

$$x^2 = a^2 - b^2, \quad y^2 = 2ab, \quad z = a^2 + b^2. \tag{13}$$

Moreover, $a \not\equiv b \pmod 2$. If a was even and b odd, then we would have $1 \equiv x^2 \equiv -b^2 \equiv -1 \pmod 4$, contradiction. Hence a is odd and b even. Applying Theorem 1.1.5 once more to the pythagorean tripel (x, b, a) we find $c, d \in \mathbb{N}$, relatively prime, such that

$$x = c^2 - d^2, \quad b = 2cd, \quad a = c^2 + d^2. \tag{14}$$

Let us focus a while on the equation

$$y^2 = 2ab, \tag{15}$$

which is part of (13). We claim that a is a square and b is of the form $b = 2w^2$. To see this, let p be a prime factor of a and let e be the exponent of p in the prime factorization of a (i.e. $a = p^e a'$, $p \nmid a'$). To show that a is a square it suffices to show that e is even. Since a is odd we have $p > 2$, and since a, b are relatively prime, p does not divide b. It follows that p^e is the p-part of the prime factorization of $2ab$. But $2ab$ is a square by (15), and hence e is even. It follows that $a = z_1^2$ is a square. The same argument shows that b is of the form $b = 2w^2$.

From (14) we obtain

$$w^2 = cd. \tag{16}$$

Since c, d are relatively prime, we can use the same argument as in the previous paragraph again to show that c, d are squares, i.e.

$$c = x_1^2, \quad d = y_1^2.$$

Plugging this into (14) we get

$$x_1^4 + y_1^4 = c^2 + d^2 = a = z_1^2,$$

i.e. (x_1, y_1, z_1) is another solution for (11). However,

$$z_1 \leq z_1^4 = a^2 = z - b^2 < z,$$

contradicting (iii). This completes the proof of the proposition. □

The proof of Proposition 1.2.2 we have just given goes back to Fermat. The method of proof – which consists in constructing a smaller solution to a

Diophantine problem from a given solution and thus arriving at a contradiction – is called *infinite descent*. Although the logical structure of the argument seems clear to us today, it was not easily accepted by Fermat contemporaries.

Before going on we wish to point out that unique factorization in $\mathbb{Z}$ (Theorem 1.1.1) played a crucial role in the proof of Proposition 1.2.2. Our main tool to prove the case $n = 3$ of Fermat's Last Theorem will be Corollary 1.1.19 which says that the ring of Eisenstein integers $\mathbb{Z}[\omega]$ is factorial, too.

The case $n = 3$ of Fermat's Last Theorem

We shall prove Theorem 1.2.1 in the case $n = 3$ (compare with [5], §17.8). Suppose that $(x, y, z) \in \mathbb{N}^3$ is a solution to the equation $x^3 + y^3 = z^3$. We may, without loss of generality, assume that x, y, z are relatively prime. Note that this implies, via the equation $x^3 + y^3 = z^3$, that x, y, z are *pairwise* relatively prime.

Claim 1: $3 \mid xyz$.

To prove this claim, we assume the contrary. Then

$$x, y, z \equiv \pm 1 \pmod 3.$$

By an easy calculation we deduce that

$$x^3, y^3, z^3 \equiv \pm 1 \pmod 9.$$

But then

$$z^3 = x^3 + y^3 \equiv 0, \pm 2 \pmod 9,$$

which gives a contradiction. This proves the claim.

The claim implies that exactly one of the three numbers x, y, z is divisible by 3 and the other two are not. Rewriting the equation as $x^3 + y^3 + (-z)^3 = 0$ we see that all three numbers play symmetric roles. We may therefore assume that $3 \mid z$ and $3 \nmid xy$. Write $z = 3^k w$ with $3 \nmid w$.

Recall from Example 1.1.24 that the element $\lambda := 1 - \omega$ is a prime element of $\mathbb{Z}[\omega]$ such that $3 = -\omega^2\lambda^2$. We can therefore rewrite the Fermat equation as an equation in $\mathbb{Z}[\omega]$:

$$x^3 + y^3 = 3^{3k}w^3 = -\omega^{6k}\lambda^{6k}w^3. \tag{17}$$

By construction, x, y, w are pairwise relatively prime, and $\lambda \nmid xyw$. The following lemma shows that such a tripel (x, y, w) cannot exists, thus proving Theorem 1.2.1 for $n = 3$.

Lemma 1.2.3 *There do not exist nonzero, relatively prime elements $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ such that*

$$\alpha^3 + \beta^3 = \epsilon\lambda^{3m}\gamma^3, \qquad \lambda \nmid \alpha\beta\gamma, \tag{18}$$

for some unit $\epsilon \in \mathbb{Z}[\omega]^\times$ and with $m \geq 1$.

Proof: The proof is by infinite descent. We assume that a relatively prime solution (α, β, γ) to (18) exists, and we choose one in which the exponent m is minimal. Under this assumption, we are going to construct another solution $(\alpha_1, \beta_1, \gamma_1)$ to (18) for which the exponent m_1 is strictly smaller then m. This gives a contradiction and proves the lemma. Throughout the proof, we repeatedly use that $\mathbb{Z}[\omega]$ is a euclidean domain and hence factorial (Corollary 1.1.20).

Claim 2: We have $m \geq 2$.

By Lemma 1.1.25 (ii) we have

$$\alpha, \beta \equiv \pm 1, \pm\omega, \pm\omega^2 \pmod{\lambda^2}.$$

Using Lemma 1.1.25 (iii) we deduce that

$$\alpha^3, \beta^3 \equiv \pm 1 \pmod{\lambda^4}$$

and hence

$$\alpha^3 + \beta^3 \equiv 0, \pm 1, \pm 2 \pmod{\lambda^4}.$$

But $\lambda \mid \alpha^3 + \beta^3$ by (17), and we conclude that $\lambda^4 \mid \alpha^3 + \beta^3$. This means that $3m \geq 4$ in (17), proving the claim.

Equation (17) can be rewritten as

$$\epsilon\lambda^{3m}\gamma^3 = (\alpha + \beta)(\alpha + \omega\beta)(\alpha + \omega\beta). \tag{19}$$

Claim 3: Given two out of the three factors on the right hand side of (19), their gcd is λ.

Replacing β by $\omega^i\beta$ we see that the three factors are cyclicly permuted. It therefore suffices to look at the two factors $\alpha + \beta$ and $\alpha + \omega\beta$. Using

$$\begin{aligned} (\alpha + \beta) - (\alpha + \omega\beta) &= (1 - \omega)\beta = \lambda\beta \\ \omega(\alpha + \beta) - (\alpha + \omega\beta) &= (\omega - 1)\alpha = -\lambda\alpha \end{aligned} \tag{20}$$

we see that any common prime factor of $\alpha + \beta$ and $\alpha + \omega\beta$ not associated to λ is also a common prime factor of α and β. But α, β are relatively prime by assumption. It follows that λ is the only common prime factor of $\alpha + \beta$ and $\alpha + \omega\beta$. We also see from (20) that λ^2 is not a common factor. This proves the claim.

We can deduce from Claim 3 that all three factors on the right hand side of (19) are divisible by λ, and exactly one of them is divisible by λ^{3m-2}. By symmetry, we may assume that this distinguished factor is $\alpha + \beta$. Then (19) shows that there exists a tripel $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Z}[\omega]$, relatively prime, such that $\lambda \nmid \gamma_1\gamma_2\gamma_3$ and

$$\begin{aligned} \alpha + \beta &= \epsilon_1\lambda^{3m-2}\gamma_1^3, \\ \alpha + \omega\beta &= \epsilon_2\lambda\gamma_2^3, \\ \alpha + \omega^2\beta &= \epsilon_3\lambda\gamma_3^3, \end{aligned} \tag{21}$$

for certain units $\epsilon_1, \epsilon_2, \epsilon_3 \in \mathbb{Z}[\omega]^\times$. Note that we have used again unique factorization in an essential way here.

A suitable liear combination of the three equations in (21) yields

$$\begin{aligned} 0 &= (\alpha+\beta) + \omega(\alpha+\omega\beta) + \omega^2(\alpha+\omega^2\beta) \\ &= \epsilon_1\lambda^{3m-2}\gamma_1^3 + \omega\epsilon_2\lambda\gamma_2^3 + \omega^2\epsilon_3\lambda\gamma_3^3. \end{aligned} \tag{22}$$

After dividing by $\omega\epsilon_2\lambda$, we can rewrite (22) as

$$\gamma_2^3 + \epsilon_4\gamma_3^3 = \epsilon_5\lambda^{3(m-1)}\gamma_1^3, \tag{23}$$

for certain units $\epsilon_4, \epsilon_5 \in \mathbb{Z}[\omega]^\times$. By the proof of Claim 2, we have

$$\gamma_1^3, \gamma_2^3 \equiv \pm 1 \pmod{\lambda^3}.$$

Combining Claim 2 with (23) we obtain

$$\pm 1 \pm \epsilon_4 \equiv 0 \pmod{\lambda^3}.$$

By Lemma 1.1.25 (ii) this implies $\epsilon_4 = \pm 1$. Hence we may rewrite (23) further as

$$\gamma_2^3 + (\pm\gamma_3)^3 = \epsilon_5\lambda^{3(m-1)}\gamma_1^3.$$

We see that the tripel $(\gamma_2, \pm\gamma_3, \gamma_1)$ is a new solution to (19) with smaller exponent of λ. This gives the desired contradiction und proves the lemma. □

Historical remarks

The idea of the proof of Fermat's Last Theorem for $n = 3$ we have given is due to Euler. However, it is disputed whether Euler's original proof was complete (see [2]): To prove a crucial Lemma (see Exercise 1.3.4), Euler worked with the subring $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}[\omega]$ and seems to have made implicite use of the claim that this ring is factorial. But this is false (see Exercise 1.3.3). Later Gauss gave a proof in which unique factorization in the ring $\mathbb{Z}[\omega]$ plays the central role and is rigorously proved.

During the first half of the 19th century, many leading mathematicians of that time worked hard to prove more cases of Fermat's Last Theorem: Dirichlet, Legendre, Lamé, Cauchy ... . They succeded in settling the cases $n = 5, 7$ and established the following strategy for the general case. It is clear that it suffices to consider prime exponents $n = p$. So let $p > 3$ be a prime number and $x, y, z \in \mathbb{N}$ be a hypothetical solution to the Fermat equation

$$x^p + y^p = z^p. \tag{24}$$

It is useful to consider two distinct cases, depending on whether $p \nmid xyz$ (the *first case*) or $p \mid xyz$ (the *second case*).

Here we only consider the first case. Let $\zeta_p := e^{2\pi i/p} \in \mathbb{C}$ be a pth root of unity. Then we can write (24) as

$$z^p = (x+y)(x+\zeta_p y)\cdot\ldots\cdot(x+\zeta_p^{p-1}y). \tag{25}$$

This is an identity in the ring $\mathbb{Z}[\zeta_p] \subset \mathbb{C}$. Assume for the moment that the ring $\mathbb{Z}[\zeta_p]$ is factorial. Using the assumption $p \nmid xyz$ it is easy to see that the factors $x + \zeta_p^i y$ on the right hand side of (25) are all relatively prime. Unique factorization in $\mathbb{Z}[\zeta_p]$ then shows that all these factors are pth powers up to a unit. For instance,

$$x + \zeta_p y = \epsilon \cdot \alpha^p,$$

for a unit $\epsilon \in \mathbb{Z}[\zeta_p]^\times$ and an element $\alpha \in \mathbb{Z}[\zeta_p]$. A careful analysis of units and congruences in the ring $\mathbb{Z}[\zeta_p]$ then leads to a contradiction. See e.g. [8], Chapter 1. This proves the first case of Fermat's Last Theorem for all primes $p > 3$, under the assumption that the ring $\mathbb{Z}[\zeta_p]$ is factorial. Actually, a similar but more complicated argument (which also uses infinite descent) achieves the same in the second case.

For some time people tried to show that $\mathbb{Z}[\zeta_p]$ is factorial in order to prove Fermat's Last Theorem. Later Kummer discovered that this is false in general (the first case is $p = 23$). He also discovered a way to fix the argument, under some condition. His main tool was a variant of unique factorization for the rings $\mathbb{Z}[\zeta_p]$, formulated in terms of so-called *ideal numbers*. A bit later, Dedekind reformulated and generalized this result. He replaced the somewhat elusive *ideal numbers* of Kummer by *ideals* and proved the first main theorem of algebraic number theory: in the ring of integers of a number field, every nonzero ideal has a unique decomposition into *prime ideals*. Algebraic number theory was born!

Kummer's result on Fermats Last Theorem can be stated in modern terminology as follows.

Theorem 1.2.4 (Kummer) *Let p be an odd prime. Assume that p is regular, i.e. p does not divide the class number h_p of the number field $\mathbb{Q}(\zeta_p)$. Then the Fermat equation*

$$x^p + y^p = z^p$$

has no solution $x, y, z \in \mathbb{N}$.

We will define the term *class number* later on. At the moment it suffices to know that $h_p \geq 1$ is a positive integer that measures the deviation of the ring $\mathbb{Z}[\zeta_p]$ from being factorial. In particular, $\mathbb{Z}[\zeta_p]$ is factorial if and only if $h_p = 1$. Kummer also gave a criterion when a prime p is regular. Unfortunately, this criterion shows that there are infinitely many irregular primes (the first are $p = 37, 59, 67, 101, \ldots$). It is conjectured that about 60% of all primes are regular, but as of today it has not been proved that there are infinitely many. So Kummer's Theorem is still a rather weak result compared to Fermats Last Theorem. Nevertheless, all serious results on Fermats Last Theorem before Wiles' proof in 1995 were essentially extensions of Kummer's work.

1.3 Quadratic reciprocity

Another important discovery of Fermat was the following theorem. Here we write $p = x^2 + y^2$ as a shorthand for 'There exist integers x, y such that $p = x^2 + y^2$.'.

Theorem 1.3.1 *Let p be a prime number.*

(i) $p = x^2 + y^2$ *if and only if* $p = 2$ *or* $p \equiv 1 \pmod 4$.

(ii) $p = x^2 + 2y^2$ *if and only if* $p = 2$ *or* $p \equiv 1, 3 \pmod 8$.

(iii) $p = x^2 + 3y^2$ *if and only if* $p = 3$ *or* $p \equiv 1 \pmod 3$.

Somewhat similar to Theorem 1.2.1 it is unclear whether Fermat had actually proved these results (see [3], Chapter 1, §1). It was Euler who first gave complete proofs, and that took him about 40 years!

Proof: We will only discuss Claim (i) in detail and defer (ii) and (iii) to the exercises. The 'only if' direction of (i) is very easy. Suppose that $p \neq 2$ and $p = x^2 + y^2$ for integers $x, y \in \mathbb{Z}$. Then $x \neq y \pmod 2$, hence we may assume that x is odd and y is even. We conclude that

$$p = x^2 + y^2 \equiv 1 + 0 \equiv 1 \pmod 4.$$

The 'if' direction is much less obvious. The proof we shall give goes back to Gauss and is rather concise. The main tools are

- unique factorization in the ring $\mathbb{Z}[i]$, and
- the existence of *primitive roots*, i.e. the fact that the group $(\mathbb{Z}/\mathbb{Z}p)^\times$ is cyclic if p is a prime number.

To see what is going on we look more closely at primes $p \neq 2$ of the form $p = x^2 + y^2$. It is clear that x, y are prime to p and hence invertible modulo p. Therefore, the congruence

$$x^2 + y^2 \equiv 0 \pmod p$$

can be rewritten as

$$\left(\frac{x}{y}\right)^2 \equiv -1 \pmod p.$$

We have shown that if p is an odd prime of the form $p = x^2 + y^2$ then -1 is a *quadratic residue* modulo p!

Recall the following definition.

Definition 1.3.2 (The Legendre symbol) Let p be an odd prime number and $a \in \mathbb{Z}$.

(i) Suppose that $p \nmid a$. We say that a is a *quadratic residue* modulo p if there exists $x \in \mathbb{Z}$ with $a \equiv x^2 \pmod p$. Otherwise we say that a is a *quadratic nonresidue* modulo p.

(ii) We set

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue,} \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic nonresidue,} \\ 0 & \text{if } p \mid a. \end{cases}$$

Lemma 1.3.3 *Let p be an odd prime number and $a \in \mathbb{Z}$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Proof: We may assume that $p \nmid a$. We shall use the well known fact that the group $(\mathbb{Z}/\mathbb{Z}p)^\times$ is a cyclic group of order $p-1$, see e.g. [5], Chapter 4, §1. In particular, we have $a^{p-1} \equiv 1 \pmod{p}$. Set $b := a^{(p-1)/2}$. Then

$$b^2 \equiv a^{p-1} \equiv 1 \pmod{p}.$$

Since $\mathbb{Z}/\mathbb{Z}p$ is a field, this means that $b \equiv \pm 1 \pmod{p}$. It remains to be seen that $b \equiv 1 \pmod{p}$ if and only if a is a quadratic residue.

Let $c \in \mathbb{Z}$ be a primitive root modulo p. Then every element of $(\mathbb{Z}/\mathbb{Z}p)^\times$ can be written as the residue class of c^k, for some $k \in \mathbb{Z}$ (unique modulo $p-1$). It follows that $c^k \equiv 1$ iff $(p-1) \mid k$, and that c^k is a quadratic residue iff k is even. In particular, if we write $a \equiv c^k \pmod{p}$, then a is a quadratic residue iff k is even iff $(p-1) \mid k(p-1)/2$ iff

$$b \equiv a^{k(p-1)/2} \equiv 1 \pmod{p}.$$

The lemma is proved. □

In the special case $a = -1$ we obtain:

Corollary 1.3.4 *Let p be an odd prime. Then*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

We can now give a prove of Theorem 1.3.1 (i). Using Corollary 1.3.4 we see that we have to prove the implication

$$\left(\frac{-1}{p}\right) = 1 \quad \Rightarrow \quad p = x^2 + y^2. \tag{26}$$

Assume that -1 is a quadratic residue modulo p, and let $a \in \mathbb{Z}$ be such that $a^2 \equiv -1 \pmod{p}$. Then (inside the ring $\mathbb{Z}[i]$) we have

$$p \mid a^2 + 1 = (a+i)(a-i), \qquad \text{but} \quad p \nmid a \pm i. \tag{27}$$

Since $\mathbb{Z}[i]$ is factorial (Corollary 1.1.20), (27) shows that p is not a prime element. By Lemma 1.1.23 (ii) it follows that

$$p = N(\alpha) = x^2 + y^2$$

for a prime element $\alpha = x + yi \in \mathbb{Z}[i]$. This proves (26) and finishes the proof of Theorem 1.3.1 (i). $\square$

Remark 1.3.5 The proof of Theorem 1.3.1 (i) consists of two rather distinct steps and suggests a reformulation of Theorem 1.3.1 as follows. Assume $p \neq 2, 3$. Then:

$$p = x^2 + y^2 \quad \Leftrightarrow \quad \left(\frac{-1}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1 \pmod 4$$

$$p = x^2 + 2y^2 \quad \Leftrightarrow \quad \left(\frac{-2}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1, 3 \pmod 8$$

$$p = x^2 + 3y^2 \quad \Leftrightarrow \quad \left(\frac{-3}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1 \pmod 3$$

To prove the three equivalences on the left one can use unique factorization in the rings $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\omega]$ (see the argument above and Exercise 1.3.7). The three equivalences on the right follow from *quadratic reciprocity*, arguably one of the deepest and most beautiful theorems of elementary number theory.

Theorem 1.3.6 (Quadratic reciprocity) *Let $p, q \in \mathfrak{P}$ be two distinct, odd prime numbers. Then*

(i)
$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(ii)
$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

(iii)
$$\left(\frac{p}{p}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod 4, \\ -1 & \text{if } p, q \equiv 3 \pmod 4. \end{cases}$$

Claim (i) (resp. Claim (ii)) of the theorem is often called the first (resp. the second) *supplementary law* . Note that (i) is identical to Corollary 1.3.4 which is, as we have seen, a rather straightforward consequence of the existence of primitive roots. Claims (ii) and (iii) are much more difficult (see e.g. [5], Chapter 5, §3). We will give a very conceptual proof of Theorem 1.3.6 later, using the decomposition of prime ideals in cyclotomic fields.

Primes of the form $x^2 + ny^2$ and class field theory

Theorem 1.3.1 gives a nice answer to three special cases of the following question.

Question 1.3.7 Given a positive integer $n \in \mathbb{N}$, which prime numbers p are of the form $p = x^2 + ny^2$?

The main ingredients for the proof of Theorem 1.3.1 were quadratic reciprocity and unique factorization in the rings $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\omega]$. For general $n \in \mathbb{N}$, quadratic reciprocity still yields the following partial answer to Question 1.3.7: there exist integers $a_1, \ldots, a_r$ such that for all primes p, except a finite number of exceptions, we have

$$p = x^2 + ny^2 \quad \Rightarrow \quad \left(\frac{-n}{p}\right) \quad \Leftrightarrow \quad p \equiv a_1, \ldots, a_r \pmod{N}, \tag{28}$$

where

$$N := \begin{cases} n, & n \equiv 0, 3 \pmod 4, \\ 4n, & n \equiv 1, 2 \pmod 4. \end{cases}$$

However, the converse of the first implication in (28) fails for general n. We give two examples.

Example 1.3.8 Consider the case $n = 5$. Quadratic reciprocity shows that for all primes $p \neq 2, 5$ we have

$$\left(\frac{-5}{p}\right) = 1 \quad \Leftrightarrow \quad \left(\frac{p}{5}\right) = (-1)^{(p-1)/2} \quad \Leftrightarrow \quad p \equiv 1, 3, 7, 9 \pmod{20}. \tag{29}$$

However, $p = 3$ cannot be written as $p = x^2 + 5y^2$. The complete answer to Question 1.3.7 for $n = 5$ is given by

$$\begin{aligned} p = x^2 + 5y^2 \quad &\Leftrightarrow \quad p \equiv 1, 9 \pmod{20}, \\ 2p = x^2 + 5y^2 \quad &\Leftrightarrow \quad p \equiv 3, 7 \pmod{20}. \end{aligned} \tag{30}$$

This was conjectured by Euler and proved by Lagrange and Gauss, using the so-called *genus theory* of binary quadratic forms. From a modern point of view, the case distinction comes from the fact that $\mathbb{Z}[\sqrt{-5}]$ is *not* a unique factorization domain. For instance, we have

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

compare with Example 1.1.7. The number of cases to consider is equal to the *class number* of $\mathbb{Z}[\sqrt{-5}]$.

Example 1.3.9 Consider the case $n = 27$. Quadratic reciprocity gives

$$\left(\frac{-27}{p}\right) = \left(\frac{-3}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1 \pmod 3,$$

for all primes $p \geq 5$. The prime $p = 7$ satifies these conditions, but it is clearly not of the form $x^2 + 27y^2$. The complete answer to Question 1.3.7 for $n = 27$ is:

$$p = x^2 + 27y^2 \quad \Leftrightarrow \quad \begin{cases} p \equiv 1 \pmod 3 \text{ and } 2 \text{ is} \\ \text{a cubic residue modulo } p \end{cases} \tag{31}$$

This had been conjectured by Euler and proved by Gauss. See [3], Chapter 1, Theorem 4.15. For instance, the cubic residues of $p = 7$ are $1, 6$ and 2 is not among them. But for $p = 31$, we have $4^3 = 64 \equiv 2 \pmod{31}$, so 2 is a cubic residue. And indeed we can write $31 = 2^2 + 27 \cdot 1^2$.

We have seen that for $n = 27$ the answer to Question 1.3.7 is not simply given by a finite list of congruence classes modulo some fixed integer N. In general, the answer looks as follows (see [3], Theorem 9.2).

Theorem 1.3.10 *For every $n \in \mathbb{N}$ there exists a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ such that for every prime p not dividing neither n nor the discriminant of $f_n(x)$ we have*

$$p = x^2 + ny^2 \quad \Leftrightarrow \quad \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ and } f_n(x) \equiv 0 \pmod{p} \\ \text{has in integer solution.} \end{cases}$$

For instance, we have $f_{27}(x) = x^3 - 2$ by (31). Theorem 1.3.10 is a very deep result, and is in fact a consequence of *class field theory*. Class field theory is one of the highlights of algebraic number theory. In some sense, it is an extremely far reaching generalization of quadratic reciprocity. We refer to [3] for a first introduction to this subject which starts from the classical observations of Fermat explained above. A systematic account of class field theory is given e.g. in [6], Chapters IV-VI. The present course should enable you to read and understand these sources.

Complex multiplication

The statement of Theorem 1.3.10 above is still somewhat unsatisfactory because the polynomial $f_n(x)$ is not given explicitly. In order to compute $f_n(x)$ for a given integer n we need some interesting complex analysis. The theory behind this is called *complex multiplication*. A readable account is given in [3], Chapter 3. Here we only give a glimpse.

For a complex number $\tau \in \mathbb{C}$ with $\Im(\tau) > 0$ we define

$$g_2(\tau) := 60 \sum_{m,n}{}' \frac{1}{(m + n\tau)^4}, \quad g_3(\tau) := 140 \sum_{m,n}{}' \frac{1}{(m + n\tau)^6}.$$

Here $\sum'_{n,m}$ means that we sum over all pairs of integers $(m, n) \in \mathbb{Z}^2$ with $(m, n) \neq (0, 0)$. The series $g_2(\tau)$ and $g_3(\tau)$ are called the *Eisenstein series* of weight 4 and 6. We also define

$$j(\tau) := 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}.$$

It is easy to see that g_2, g_3, j are complex analytic functions on the upper half plane $\mathbb{H}$.

The function $j : \mathbb{H} \to \mathbb{C}$ has some remarkable properties. In particular, it is a *modular function*, which means that

$$j(\frac{a\tau + b}{c\tau + d}) = j(\tau), \qquad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

In particular, we have

$$j(\tau + 1) = j(\tau), \quad j(-1/\tau) = j(\tau). \tag{32}$$

The first equation in (32) implies that j has a Fourier expansion, i.e. it can be written as a Laurent series in $q := e^{2\pi i \tau}$. And indeed, one can show that

$$j(\tau) = \sum_{n=-1}^{\infty} a_n q^n = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots, \tag{33}$$

for certain positive integers $a_n \in \mathbb{N}$. Note that this series converges very quickly if $\Im(\tau) > 0$ is large, because

$$|q| = e^{-2\pi \Im(\tau)}.$$

As a complex analytic function, the j-function is already pretty remarkable. But even more astounding are its arithmetic properties.

Theorem 1.3.11 (i) *Let $\tau \in \mathbb{H}$ be a quadratic integer, i.e. $\tau \in \mathcal{O}_K$ for an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-m})$. Then $\alpha := j(\tau) \in \bar{\mathbb{Q}}$ is an algebraic integer. Moreover, the field extension $L := K(\alpha)/K$ is an abelian Galois extension, and the Galois group $\mathrm{Gal}(L/K)$ is isomorphic to the class group of the ring $\mathbb{Z}[\tau] \subset K$. In particular, if $\mathbb{Z}[\tau]$ is a unique factorization domain, then $j(\tau) \in \mathbb{Z}$ is an integer.*

(ii) *More specifically, let $\tau := \sqrt{-n}$ for a positive integer $n \in \mathbb{N}$. Then the minimal polynomial $f_n = a_0 + a_1 + \ldots + x^k$ of $\alpha = j(\tau)$ has the property stated in Theorem 1.3.10.*

Example 1.3.12 Let $\tau := (1 + \sqrt{-163})/2$. We will show show later that $\mathbb{Z}[\tau]$ is a unique factorization domain (see Example 2.6.27). Therefore, $j(\tau) \in \mathbb{Z}$ is an integer by Theorem 1.3.11 (i). By (33) we have

$$j(\tau) = -e^{\pi\sqrt{163}} + 744 + R, \qquad \text{with} \quad R := 196884q + 21493760q^2 + \ldots$$

Since $|q| = e^{-2\pi\sqrt{163}} \approx 1.45 \cdot 10^{-35}$ is very small, $R \approx 2.27 \cdot 10^{-12}$ is rather small as well. It follows that

$$e^{\pi\sqrt{163}} = -j(\tau) + 744 + R$$

is very close to an integer. This explains the second 'miracle' mentioned in the introduction. Note that we can use this to compute the *exact* value of $j(\tau)$ from a numerical approximation of $e^{\pi\sqrt{163}}$. The result is

$$j(\tau) = j\big(\frac{1+\sqrt{-163}}{2}\big) = -640320^3 = -(2^6 \cdot 3 \cdot 5 \cdot 23 \cdot 29)^3.$$

It is not an accident that this integer is *smooth* i.e. composed of many relatively small primes with high exponent. However, the beautiful explanation for this fact goes even beyond complex multiplication.

Exercises

Exercise 1.3.1 Prove that $2, \pm 1 + \sqrt{5}$ are irreducible elements of $\mathbb{Z}[\sqrt{5}]$, but not prime elements.

Exercise 1.3.2 Let $a, n \in \mathbb{N}$ be given and assume that a is not an nth power, i.e. $a \neq b^n$ for all $b \in \mathbb{N}$. Show that $\sqrt[n]{a} \in \mathbb{R}$ is irrational. (Use Theorem 1.1.1.)

Exercise 1.3.3 (Euler was wrong) Show that the subring $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}[\omega]$ is not factorial. Explain what goes wrong with the proof of Proposition 1.1.19.

Exercise 1.3.4 (Euler was right) Suppose that $a, b, s \in \mathbb{Z}$ are integers such that s is odd, $\gcd(a, b) = 1$ and

$$s^3 = a^2 + 3b^2.$$

Show that s is of the form $s = u^2 + 3v^2$, with $u, v \in \mathbb{Z}$.

Exercise 1.3.5 Let $S := \{\alpha = x + y\omega \mid 0 \leq y < x\} \subset \mathbb{Z}[\omega]\backslash\{0\}$. Show that for every element $\alpha \in \mathbb{Z}[\omega]$, $\alpha \neq 0$, there exists a unique associate element $\alpha' \in S$, $\alpha \sim \alpha'$. Deduce that α has a factorization

$$\alpha = \epsilon \cdot \pi_1 \cdot \ldots \cdot \pi_r,$$

with prime elements $\pi_i \in S$ and a unit ϵ, and that this factorization is unique up to a permutation of the π_i.

Exercise 1.3.6 (a) Compute the prime factorization of 14, $3+4\omega$ und $122+61\omega$ in $\mathbb{Z}[\omega]$.

(b) Compute the prime factorization of 14, $3+4i$ und $122+61i$ in $\mathbb{Z}[i]$.

Exercise 1.3.7 (a) Show that $\mathbb{Z}[\sqrt{-2}]$ is a unique factorization domain.

(b) Let $p \geq 5$ be a prime number. Prove the equivalences

$$p = x^2 + 2y^2 \quad \Leftrightarrow \quad \left(\frac{-2}{p}\right) = 1$$

and

$$p = x^2 + 3y^2 \quad \Leftrightarrow \quad \left(\frac{-3}{p}\right) = 1$$

from Remark 1.3.5.

Exercise 1.3.8 (a) Use quadratic reciprocity to show that

$$\left(\frac{-2}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1, 3 \pmod 8$$

and

$$\left(\frac{-3}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1 \pmod 3.$$

(Note that, together with Exercise 1.3.7, this proves (ii) and (iii) of Theorem 1.3.1.)

(b) For which prime numbers p is 35 a quadratic residue modulo p?

(c) For how many of all primes $p \leq 100$ is 35 a quadratic residue? Speculate about the asymptotic rule for all $p \leq N$, $N \to \infty$.

2 Arithmetic in an algebraic number field

2.1 Finitely generated abelian groups

We start by recalling some easy but fundamental algebraic facts. We consider abelian groups $(M, +)$. Note that M has the structure of a $\mathbb{Z}$-module via

$$\mathbb{Z} \times M \to M, \qquad a \cdot m := \pm(m + \ldots + m).$$

In fact, any $\mathbb{Z}$-module is completely determined by its underlying abelian group. Thus, the two notions *abelian group* and *$\mathbb{Z}$-module* are equivalent. We have a slight preference for the second.

The $\mathbb{Z}$-module M is called *finitely generated* if there are elements $m_1, \ldots, m_n$ such that

$$M = \langle m_1, \ldots, m_n \rangle_{\mathbb{Z}} := \{\sum_{i=1}^{n} a_i m_i \mid a_i \in \mathbb{Z}\}.$$

If this is the case then $m_1, \ldots, m_n$ is called a system of *generators* of M. A system of generators $(m_1, \ldots, m_n)$ of M is called a *$\mathbb{Z}$-basis* of M if every element $m \in M$ has a *unique* representation of the form $m = a_1 m_1 + \ldots + a_n m_r$. Another way to state this is to say that $(m_1, \ldots, m_r)$ induces an isomorphism

$$\mathbb{Z}^r \xrightarrow{\sim} M, \quad (a_1, \ldots, a_r) \mapsto \sum_{i=1}^{r} a_i m_i.$$

A $\mathbb{Z}$-module M is called *free of rank r* if it has a basis of length r. It is not hard to see that the rank of a free $\mathbb{Z}$-module M is well defined.

Here is the first fundamental result about finitely generated $\mathbb{Z}$-modules.

Theorem 2.1.1 *Let M be a free group of rank r and $M' \subset M$ a subgroup. Then there exists a basis $(m_1, \ldots, m_r)$ of M and a sequence of positive integers $d_1, \ldots, d_s \in \mathbb{N}$, $s \leq r$, such that*

$$d_1 \mid d_2 \mid \ldots \mid d_s$$

and such that $(d_1 m_1, \ldots, d_s m_s)$ is a basis of M'. In particular, M' is free of rank $s \leq r$.

Proof: See e.g. [1], Chapter 12, Theorem 4.11. □

Let $M' \subset M$ be as in the theorem, and assume that $r = s$. Let $m = (m_1, \ldots, m_r)$ be a basis of M and $m' = (m'_1, \ldots, m'_r)$ a basis of M'. Then for $j = 1, \ldots, r$ we can write

$$m'_j = a_{j,1} m_1 + \ldots + a_{j,r} m_r, \tag{34}$$

with uniquely determined integers $a_{i,j} \in \mathbb{Z}$. The system of equations (34) can be written more compactly as

$$m' = m \cdot A, \qquad A := (a_{i,j}) \in M_{r,r}(\mathbb{Z}), \tag{35}$$

where m and m' are considered as row vectors.

Proposition 2.1.2 *We have*

$$[M : M'] := |M/M'| = |\det(A)|.$$

Proof: We use the main ideas from the proof of Theorem 2.1.1, see [1], §14.4. Replacing A by $S \cdot A$, for $S \in \mathrm{GL}_n(\mathbb{Z})$, has the effect of replacing the basis m of M by the new basis $n := m \cdot S^{-1}$. Similarly, replacing A by $A \cdot T$, for $T \in \mathrm{GL}_n(\mathbb{Z})$, has the effect of replacing the basis m' of M' by the new basis $n' := m' \cdot T$. Now assume that $n = (n_1, \ldots, n_r)$ and $n' = (n'_1, \ldots, n'_r)$ are bases of M and M' which satisfy the conclusion of Theorem 2.1.1, i.e.

$$n'_1 = d_1 n_1, \ldots, n'_r = d_r n_r, \tag{36}$$

with positive integers $d_1, \ldots, d_r$. Then

$$S \cdot A \cdot T = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}. \tag{37}$$

Using (36) we can construct an isomorphism

$$\mathbb{Z}/\mathbb{Z}d_1 \times \ldots \times \mathbb{Z}/\mathbb{Z}d_r \xrightarrow{\sim} M/M', \quad (c_i + \mathbb{Z}d_i) \mapsto c_1 n_1 + \ldots + c_r n_r.$$

Counting the elements, we obtain

$$|M/M'| = d_1 \cdot \ldots \cdot d_r. \tag{38}$$

On the other hand, (37) shows that

$$\det(A) = \pm d_1 \cdot \ldots \cdot d_r. \tag{39}$$

The proposition follows by combining (38) and (39). □

2.2 The splitting field and the discriminant

Let $n \in \mathbb{N}$, K be a field and

$$f = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$$

be a polynomial of degree n (i.e. $a_n \neq 0$). Then there exists a field extension L/K such that f splits over L into linear factors,

$$f = a_n \prod_{i=1}^{n} (x - \alpha_i), \qquad \alpha_i \in L.$$

We may assume that L/K is generated by the roots α_i, i.e. $L = K(\alpha_1, \ldots, \alpha_n)$. With this assumption, the field extension L/K is unique up to isomorphism and called the *splitting field* of f (relative to K). The polynomial f is called *separable* if $\alpha_i \neq \alpha_j$ for all $i \neq j$.

Definition 2.2.1 The *discriminant* of f is defined as

$$\Delta(f) := a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Note that the definition of $\Delta(f)$ is independent of the chosen order of the roots α_i. By definition we have $\Delta(f) \neq 0$ if and only if f is separable.

Example 2.2.2 For $n = 2$ we can write $f = ax^2 + bx + c$, with $a, b, c \in K$ and $a \neq 0$. By the famous *Mitternachtsformel* we have

$$f = a(x - \alpha_1)(x - \alpha_2), \qquad \alpha_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

It follows that

$$\Delta(f) = a^2(\alpha_1 - \alpha_2)^2 = b^2 - 4ac.$$

We see that $\Delta(f)$ is a polynomial in the coefficients of f and therefore $\Delta(f) \in K$. This is a completely general phenomenon:

Theorem 2.2.3 *For every $n \in \mathbb{N}$ there exists a polynomial $\Delta_n \in \mathbb{Z}[x_0, \ldots, x_n]$ in $n + 1$ variables and integral coefficients, such that for all fields K and all polynomials $f = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$ of degree n we have*

$$\Delta(f) = \Delta_n(a_0, \ldots, a_n).$$

In particular, $\Delta(f) \in K$.

Proof: See e.g. [1], Chapter 14, §3. □

Corollary 2.2.4 *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n, with integral coefficients. Let $p \in \mathfrak{P}$ be a prime number and let $\bar{f} \in \mathbb{F}_p[x]$ denote the reduction of f modulo p. Then*

$$\Delta(\bar{f}) = \overline{\Delta(f)} \in \mathbb{F}_p.$$

Therefore, $\bar{f}$ is separable if and only if $\Delta(f)$ is prime to p.

2.3 Number fields

Definition 2.3.1 A *number field*[3] is a finite field extension K of the field of rational numbers $\mathbb{Q}$. The *degree* of K is the dimension

$$[K : \mathbb{Q}] := \dim_{\mathbb{Q}} K.$$

[3] The terminology is unfortunately not standardized. E.g. Artin ([1], Chapter 13, §1) defines a number field as any subfield of $\mathbb{C}$.

Let us fix a number field K of degree n. Then for any $\alpha \in K$ there must be a $\mathbb{Q}$-linear relation between the first $n+1$ powers of α, i.e. there exists rational numbers $a_0, a_1, \ldots, a_n \in \mathbb{Q}$, not all of them zero, such that

$$a_0 + a_1\alpha + \ldots, a_n\alpha^n = 0.$$

In other words, α is a root in K of the nonzero polynomial $a_0+a_1x+\ldots+a_nx^n \in \mathbb{Q}[x]$. We say that α is *algebraic* over $\mathbb{Q}$.

Consider the ring homomorphism

$$\phi_\alpha : \mathbb{Q}[x] \to K, \quad g \mapsto g(\alpha),$$

given by substituting $x := \alpha$. The kernel of ϕ_α,

$$I := \{f \in \mathbb{Q}[x] \mid f(\alpha) = 0\} \lhd \mathbb{Q}[x]$$

is an ideal. Since $\mathbb{Q}[x]$ is a euclidian domain, it is also a principal ideal domain, see Proposition 1.1.11. It follows that $I = (m_\alpha)$ for a nonzero polynomial m_α. We may assume that m_α is monic,

$$m_\alpha = c_0 + c_1x + \ldots + x^d,$$

and this condition determines m_α uniquely.

Definition 2.3.2 The monic polynomial $m_\alpha \in \mathbb{Q}[x]$ defined above is called the *minimal polynomial* of α. Its degree $d = \deg(m_\alpha)$ is called the *degree* of α over $\mathbb{Q}$.

By definition of m_α we have

$$f(\alpha) = 0 \quad \Leftrightarrow \quad m_\alpha \mid f, \tag{40}$$

for all $f \in \mathbb{Q}[x]$. In particular, m_α is the monic polynomial with the smallest possible degree which has α as a root.

Proposition 2.3.3 *Let K be a number field of degree $n = [K : \mathbb{Q}]$, and $\alpha \in K$ an element. Let $\mathbb{Q}[\alpha]$ denote the smallest subring of K containing α. Then $\mathbb{Q}[\alpha]$ is a subfield of K with $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg_{\mathbb{Q}}(\alpha)$. Moreover, $\deg_{\mathbb{Q}}(\alpha) \mid n$.*

Theorem 2.3.4 (Primitive Element) *Let K be a number field. Then there exists an element $\alpha \in K$ such that $K = \mathbb{Q}[\alpha]$.*

An element $\alpha \in K$ as in the theorem is called a *primitive element* or a *generator* of the number field K. By Proposition 2.3.3, α is a primitive element if and only if $[K : \mathbb{Q}] = \deg_{\mathbb{Q}}(\alpha)$. For a proof of Theorem 2.3.4 see e.g. [1], Chapter 14, §4.

Definition 2.3.5 Let $f = a_0 + a_1 x + \ldots + x^n \in \mathbb{Q}[x]$ be a monic and irreducible polynomial over $\mathbb{Q}$. Then the quotient ring

$$K_f := \mathbb{Q}[x]/(f)$$

is a number field, called the *Stammkörper*[4] of f.

It follows from Theorem 2.3.4 that every number field is isomorphic to a suitable *Stammkörper*. Indeed, if α is a generator of a number field K and $f := m_\alpha$ is its minimal polynomial, then

$$K_f = \mathbb{Q}[x]/(f) \xrightarrow{\sim} K, \quad g + (f) \mapsto g(\alpha),$$

is an isomorphism. This isomorphism tells us how to do explicit computations in the number field $K = \mathbb{Q}[\alpha]$. The point is that every element $\beta \in K$ can be written as $\beta = g(\alpha)$, for a *unique* polynomial $g \in \mathbb{Q}[x]$ with $\deg(g) < n := [K : \mathbb{Q}]$. If we want to express, say, β^2, in the same way, we compute the remainder of the polynomial g^2 after division by f,

$$g^2 = qf + r, \quad \text{with } q, r \in \mathbb{Q}[x] \text{ and } \deg(r) < n = \deg(f).$$

Then $\beta^2 = r(\alpha)$ is the standard way to write $\beta^2 \in K = \mathbb{Q}[\alpha]$.

Embeddings into the complex numbers

Another way to think about number fields is to consider them as subfields of the complex numbers.

Corollary 2.3.6 *Let K be a number field of degree n. Then there are exactly n distinct field homomorphisms*

$$\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$$

embedding K into the field of complex numbers.

Proof: Let $\alpha \in K$ be a primitive element for K (Theorem 2.3.4). By the Fundamental Theorem of Algebra, the minimal polynomial m_α decomposes over $\mathbb{C}$ into a product of n linear factors,

$$m_\alpha = \prod_{i=1}^{n} (x - \alpha_i),$$

with $\alpha_i \in \mathbb{C}$. Since m_α is irreducible over $\mathbb{Q}$, the roots α_i are pairwise distinct. For $i = 1, \ldots, n$ we define pairwise distinct homomorphisms as follows:

$$\sigma_i : K \to \mathbb{C}, \quad f(\alpha) \mapsto f(\alpha_i).$$

[4] If you know of a good english translation, please tell me!

This is well defined by (40) and the fact that $m_\alpha(\alpha_i) = 0$. Conversely, let $\sigma : K \to \mathbb{C}$ be a field homomorphism. Then

$$m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0.$$

It follows that $\sigma(\alpha_i) = \alpha_i$ for some i and hence $\sigma = \sigma_i$. □

Remark 2.3.7 Let K be a number field of degree n, and let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding into $\mathbb{C}$. Composing σ with complex conjugation, $z \mapsto \bar{z}$, we obtain another embedding $\bar{\sigma} : K \hookrightarrow \mathbb{C}$. It is clear that $\bar{\sigma} = \sigma$ if and only if $\sigma(K) \subset \mathbb{R}$. If this is the case we call σ a *real embedding*. Otherwise, we call $\{\sigma, \bar{\sigma}\}$ a *pair of complex conjugate embeddings*.

After reordering the n embeddings σ_i from Corollary 2.3.6, we may assume that

$$\sigma_1, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$$

are precisely the real embeddings and that

$$\{\sigma_{r+2i-1}, \sigma_{r+2i}\}, \quad i = 1, \dots, s,$$

are exactly all pairs of complex conjugate embeddings. Clearly, we have $r, s \geq 0$ and $n = r + 2s$.

Definition 2.3.8 The pair (r, s) is called the *type* of the number field. If $r = n$ and $s = 0$ then K is called *totally real*.

Remark 2.3.9 By Corollary 2.3.6, every number field K may be embedded into the complex numbers. Choosing one embedding, we may always consider K as a subfield of the complex numbers. This is often very useful, but one has to keep in mind that this choice may cause some loss of information.

The norm and the trace

Let K be a number field of degree n and $\alpha \in K$. The multiplication map

$$\phi_\alpha : K \to K, \qquad \beta \mapsto \alpha\beta,$$

is a $\mathbb{Q}$-linear endomorphisms.

Definition 2.3.10 We call

$$N_{K/\mathbb{Q}}(\alpha) := \det(\phi_\alpha) \in \mathbb{Q}$$

the *norm* and

$$T_{K/\mathbb{Q}}(\alpha) := \mathrm{tr}(\phi_\alpha) \in \mathbb{Q}$$

the *trace* of $\alpha \in K$.

It follows from the definition that the map

$$N_{K/\mathbb{Q}} : K^\times \to \mathbb{Q}^\times, \qquad \alpha \mapsto N_{K/\mathbb{Q}}(\alpha),$$

is a group homomorphism (w.r.t. multiplication) and that

$$T_{K/\mathbb{Q}} : K \to \mathbb{Q}, \qquad \alpha \mapsto T_{K/\mathbb{Q}}(\alpha),$$

is a linear form on the $\mathbb{Q}$-vector space K. There are two useful ways to compute the norm and the trace of an element.

Proposition 2.3.11 (i) *Let $f = a_0 + a_1 x + \ldots + x^m$ be the minimal polynomial of $\alpha \in K$. Then*

$$N_{K/\mathbb{Q}}(\alpha) = (-1)^n a_0^{n/m}, \qquad T_{K/\mathbb{Q}}(\alpha) = -\frac{n}{m} \cdot a_{m-1}.$$

(ii) *Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ denote the n distinct embeddings of K into $\mathbb{C}$. Then*

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \qquad T_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Proof: We first assume that α is a primitive element of K. Then $1, \alpha, \ldots, \alpha^{n-1}$ is a $\mathbb{Q}$-basis of K. Since $f(\alpha) = 0$ we have

$$\alpha \cdot \alpha^i = \begin{cases} \alpha^{i+1}, & i < n-1, \\ \alpha^n = -a_0 + -a_1\alpha - \ldots - a_{n-1}\alpha^{n-1}, & i = n-1, \end{cases}.$$

In other words, the matrix representing the endomorphism ϕ_α with respect to the basis $1, \alpha, \ldots, \alpha^{n-1}$ is

$$A := \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & & \ddots & 0 & -a_{n-2} \\ 0 & 0 & & 1 & -a_{n-1} \end{pmatrix}.$$

Let

$$f = a_0 + a_1 x + \ldots + x^n = \prod_{i=1} (x - \alpha_i)$$

be the factorization of f into linear factors over $\mathbb{C}$. Note that $\alpha_i \neq \alpha_j$ for $i \neq j$ and that $\alpha_i = \sigma_i(\alpha)$ are the images of α under the embeddings $\sigma_1, \ldots, \sigma_n$ (see

the proof of Corollary 2.3.6). The identity $f(\alpha_i) = 0$ shows that

$$A^t \cdot v = \alpha_i \cdot v, \qquad v := \begin{pmatrix} 1 \\ \alpha_i \\ \vdots \\ \alpha_i^{n-1} \end{pmatrix} \in \mathbb{C}^n.$$

We see that $\alpha_1, \ldots, \alpha_n$ are the pairwise distinct eingenvalues of A^t. It follows that A is diagonalizable over $\mathbb{C}$,

$$A \sim \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}, \tag{41}$$

and that f is, up to sign, the characteristic polynomial of A,

$$\det(A - x \cdot E_n) = \prod_{i=1}^{n} (\alpha_i - x) = (-1)^n f. \tag{42}$$

In particular,

$$N_{K/\mathbb{Q}}(\alpha) = \det(A) = \prod_{i=1}^{n} \alpha_i = (-1)^n a_0,$$
$$T_{K/\mathbb{Q}}(\alpha) = \mathrm{tr}(A) = \sum_{i=1}^{n} \alpha_i = -a_{n-1}.$$

Both (i) and (ii) follow immediately.

If α is not a primitive element, we consider the intermediate field $M := \mathbb{Q}[\alpha]$. We set $m := [M : \mathbb{Q}] = \deg(\alpha)$. Then

$$n = [K : \mathbb{Q}] = [K : M] \cdot [M : \mathbb{Q}],$$

see e.g. [1], Chapter 13, Theorem 3.4. It follows that $k := [K : M] = n/m$. Let $\beta_1, \ldots, \beta_k$ be an M-basis of K. The proof of Theorem 3.4 in [1], Chapter 13, shows that we have the following direct sum decomposition of $\mathbb{Q}$-vektor spaces:

$$K = \beta_1 \cdot M \oplus \ldots \oplus \beta_k \cdot M.$$

It is clear that this direct sum is invariant under the endomorphism ϕ_α. It follows that

$$\det(\phi_\alpha) = \prod_{i=1}^{k} \det(\phi_\alpha|_{\beta_i \cdot M}). \tag{43}$$

For a fixed i, $\beta_i, \alpha\beta_i, \ldots, \alpha^{m-1}\beta_i$ is a $\mathbb{Q}$-basis of $\beta_i \cdot M$, and the representing matrix for $\phi_\alpha|_{\beta_i \cdot M}$ with respect to this basis is again the matrix A from above. We conclude that

$$\det(\phi_\alpha|_{\beta_i \cdot M}) = \det(\phi_\alpha|_M) = N_{M/\mathbb{Q}}(\alpha).$$

and so by (43) we get

$$N_{K/\mathbb{Q}} = \det(\phi_\alpha) = N_{M/\mathbb{Q}}(\alpha)^k.$$

Similarly, one proves

$$T_{K/\mathbb{Q}}(\alpha) = \mathrm{tr}(\phi_\alpha) = k \cdot T_{M/\mathbb{Q}}(\alpha).$$

Now (i) and (ii) follow from the case we have already proved. □

Quadratic number fields

A number field of degree 2 is called a *quadratic number field*. Let α be a generator for K. Then α satifies a quadratic equation,

$$\alpha^2 + a\alpha + b = 0, \tag{44}$$

such that the polynomial $x^2 + ax + b \in \mathbb{Q}[x]$ is irreducible. If we set $\beta := \alpha + a/2$ then

$$\beta^2 = \alpha^2 + a\alpha + \frac{a^2}{4} = \frac{a^2}{4} - b =: \Delta.$$

We see that β is a generator for K which satisfies a relation $\beta^2 = \Delta$, where $\Delta \in \mathbb{Q}$ is *not* a square. An arbitrary element $\gamma \in K$ is of the form

$$\gamma = c + d\beta, \quad \text{with } c, d \in \mathbb{Q}.$$

Sometimes we write symbolically $\beta = \sqrt{\Delta}$ and $K = \mathbb{Q}[\sqrt{\Delta}]$, but this notation can be misleading. It should be understood as the statement that the minimal polynomial of β is $m_\beta = x^2 - \Delta$.

Now suppose that $\Delta > 0$. Then $\sqrt{\Delta} \in \mathbb{R}_{>0}$ is a well defined positive real number, and the minimal polynomial of β factors over $\mathbb{R}$ as

$$m_\beta = x^2 - \Delta = (x - \sqrt{\Delta})(x + \sqrt{\Delta}).$$

It follows that K has two real embeddings $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{R}$, given by

$$\sigma_1(c + d\beta) := c + d\sqrt{\Delta}, \qquad \sigma_2(c + d\beta) := c - d\sqrt{\Delta}.$$

We say that K is a *real quadratic number field*.

Note that $\sigma_1(K) = \sigma_2(K)$ as subfields of $\mathbb{R}$. The notation $K = \mathbb{Q}[\sqrt{\Delta}] \subset \mathbb{R}$ is therefore totally unambiguous. Still, from an algebraic point of view there is no good reason to prefer one of the two embeddings σ_1, σ_2 over the other.

Now suppose that $\Delta < 0$. Then m_β factors over $\mathbb{C}$ as

$$m_\beta = x^2 - \Delta = (x - i\sqrt{|\Delta|})(x + i\sqrt{|\Delta|}).$$

Hence we have two complex conjugate embeddings,

$$\sigma_1(c + d\beta) := c + di\sqrt{|\Delta|}, \qquad \sigma_2(c + d\beta) := c - di\sqrt{|\Delta|}.$$

We say that K is an *imaginary quadratic number field*. As in the real case, the two subfield $\sigma_1(K) = \sigma_2(K) \subset \mathbb{C}$ are identical.

Lemma 2.3.12 *Let K be a quadratic number field. Then there exists a unique nontrivial field automorphism*

$$\tau : K \xrightarrow{\sim} K.$$

Moreover, for every element $\alpha \in K \backslash \mathbb{Q}$, the minimal polynomial of α factors over K as follows:

$$m_\alpha = (x - \alpha)(x - \tau(\alpha)).$$

Proof: This lemma is a very special case of a more general statement from Galois theory (see e.g. [1], Chapter 14, §1). For readers who are still unfamiliar with Galois theory, it is a useful exercise to give a direct proof. □

If K is an imaginary quadratic field, then the automorphism τ from Lemma 2.3.12 is simply the restriction of complex conjugation to K, i.e. $\tau(\alpha) = \bar{\alpha}$ for $\alpha \in K \subset \mathbb{C}$ (it does not matter which embedding of K into $\mathbb{C}$ we choose). If K is a real quadratic number field, then it is customary to write

$$\tau(\alpha) = \alpha',$$

and to call α' the *conjugate* of α.

Exercises

Exercise 2.3.1 Let α be a primitive element for the number field K and let $f \in \mathbb{Q}[x]$ be the minimal polynomial of α. Then

$$N_{K/\mathbb{Q}}(f'(\alpha)) = \Delta(f).$$

2.4 The ring of integers

Let us fix a number field K of degree $n = [K : \mathbb{Q}]$.

Definition 2.4.1 An element $\alpha \in K$ is called *integral* (or an *algebraic integer*) if the minimal polynomial of α has integral coefficients,

$$m_\alpha \in \mathbb{Z}[x].$$

We let $\mathcal{O}_K \subset K$ denote the subset of all integral elements of K. (Theorem 2.4.4 below shows that $\mathcal{O}_K$ is a subring, but this is not obvious.)

A $\mathbb{Z}$-*submodule* $M \subset K$ is a subgroup of the additive group $(K, +)$. It is called *finitely generated* if there exists field elements $\beta_1, \ldots, \beta_k \in K$ such that

$$M = \langle \beta_1, \ldots, \beta_k \rangle_{\mathbb{Z}} := \{ \sum_{i=1}^{k} a_i \beta_i \mid a_i \in \mathbb{Z} \}.$$

Lemma 2.4.2 *For $\alpha \in K$ the following three statements are equivalent.*

(a) $\alpha \in \mathcal{O}_K$.

(b) There exists a monic, integral polynomial $f = a_0 + a_1 x + \ldots + x^k \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

(c) There exists a finitely generated $\mathbb{Z}$-submodule $M \subset K$ such that $\alpha \cdot M \subset M$.

Proof: The implication (a)⇒(b) is trivial. Conversely, let $f = a_0 + a_1 x + \ldots + x^k \in \mathbb{Z}[x]$ be monic and integral such that $f(\alpha) = 0$. Then m_α is a divisor of f inside the ring $\mathbb{Q}[x]$ by (40). The Lemma of Gauss (see [1], Chapter 11, §3) shows that $m_\alpha \in \mathbb{Z}[x]$ has integral coefficients as well. This proves the implication (b)⇒(a).

Assume that (b) holds and set

$$M := \langle 1, \alpha, \ldots, \alpha^{k-1} \rangle_{\mathbb{Z}} \subset K.$$

Then

$$\alpha \cdot \alpha^i = \begin{cases} \alpha^{i+1} \in M, & i < k-1, \\ \alpha^k = -a_0 + -a_1 \alpha - \ldots - a_{k-1} \alpha^{k-1} \in M, & i = k-1, \end{cases}$$

for $i = 0, \ldots, k-1$. Therefore, $\alpha \cdot M \subset M$. Conversely, let $M = \langle \beta_1, \ldots, \beta_k \rangle_{\mathbb{Z}} \subset K$ be a finitely generated submodule with $\alpha \cdot M \subset M$. For $i = 1, \ldots, k$ we can write

$$\alpha \cdot \beta_i = \sum_{j=1}^{k} a_{i,j} \beta_j,$$

with integers $a_{i,j} \in \mathbb{Z}$. Then the vector $\beta := (\beta_1, \ldots, \beta_k)^t \in K^n$ is an eigenvector of the matrix $A := (a_{i,j})$. It follows that $f(\alpha) = 0$, where $f = \det(A - x \cdot E_n) \in \mathbb{Z}[x]$ is the characteristic polynomial. Since f is monic and integral, (b) holds and the proof of the lemma is complete. □

Remark 2.4.3 Let $\alpha \in K$ we let $\mathbb{Z}[\alpha]$ denote the smallest subring of K containing α. Then as a $\mathbb{Z}$-submodule of K, $\mathbb{Z}[\alpha]$ is generated by the powers of α,

$$\mathbb{Z}[\alpha] = \langle 1, \alpha, \alpha^2, \ldots \rangle_{\mathbb{Z}}.$$

It follows immediately from the proof of Lemma 2.4.2 that $\alpha \in \mathcal{O}_K$ if and only if $\mathbb{Z}[\alpha] \subset K$ is a finitely generated submodule.

Theorem 2.4.4 *The subset $\mathcal{O}_K \subset K$ is a subring.*

Proof: Let $\alpha, \beta \in \mathcal{O}_K$. We have to show that $\alpha \pm \beta \in \mathcal{O}_K$ and $\alpha\beta \in \mathcal{O}_K$. Let $\mathbb{Z}[\alpha, \beta] \subset K$ be the smallest subring of K containing α and β. As a $\mathbb{Z}$-submodule of K, $\mathbb{Z}[\alpha, \beta]$ is generated by the monomials $\alpha^i\beta^j$, $i, j \geq 0$. As in the proof of Lemma 2.4.2 one shows that

$$\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\alpha] + \beta \cdot \mathbb{Z}[\alpha] + \ldots + \beta^{k-1}\mathbb{Z}[\alpha], \tag{45}$$

with $k := \deg_{\mathbb{Q}}(\beta)$. But $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module, and so (45) shows that $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-module as well. Clearly,

$$(\alpha \pm \beta) \cdot \mathbb{Z}[\alpha, \beta] \subset \mathbb{Z}[\alpha, \beta], \qquad \alpha\beta \cdot \mathbb{Z}[\alpha, \beta] \subset \mathbb{Z}[\alpha, \beta].$$

Therefore, Lemma 2.4.2 shows that $\alpha \pm \beta \in \mathcal{O}_K$ and $\alpha\beta \in \mathcal{O}_K$. □

Remark 2.4.5 For any $\alpha \in K$ there exists a nonzero integer $m \in \mathbb{Z}$ such that $m\alpha \in \mathcal{O}_K$ (see Exercise 2.4.1). Since $\mathbb{Z} \subset \mathcal{O}_K$, it follows that K is the field of fraction of $\mathcal{O}_K$.

Example 2.4.6 Let $K := \mathbb{Q}[\sqrt{2}, \sqrt{3}] \subset \mathbb{R}$ denote the smallest subfield of $\mathbb{R}$ containing $\sqrt{2}$ and $\sqrt{3}$. The elements $\sqrt{2}$ and $\sqrt{3}$ are clearly integral. So according to Theorem 2.4.4, the element

$$\alpha := \sqrt{2} + \sqrt{3} \in K$$

should be integral, too. This means that the minimal poylnomial m_α of α has integral coefficients. To find an explicit monic integral polynomial with root α we use ideas from the proofs of Lemma 2.4.2 and Theorem 2.4.4.

It is clear that the ring $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ is a finitely generated $\mathbb{Z}$-submodule of K, generated by the 4 elements $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$,

$$\mathbb{Z}[\sqrt{2}, \sqrt{3}] = \langle 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \rangle_{\mathbb{Z}}.$$

It is also easy to see that $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$, but we don't need this. The crucial fact is that $\alpha \cdot \mathbb{Z}[\sqrt{2}, \sqrt{3}] \subset \mathbb{Z}[\sqrt{2}, \sqrt{3}]$. Explicitly, we have

$$\begin{aligned} \alpha \cdot 1 &= \sqrt{2} + \sqrt{3}, \\ \alpha \cdot \sqrt{2} &= 2 + \sqrt{6}, \\ \alpha \cdot \sqrt{3} &= 3 + \sqrt{6}, \\ \alpha \cdot \sqrt{6} &= 3\sqrt{3} + 2\sqrt{3}. \end{aligned} \tag{46}$$

We can rewrite (46) as

$$\alpha \cdot \begin{pmatrix} 1 \\ \sqrt{2} \\ \sqrt{3} \\ \sqrt{6} \end{pmatrix} = A \cdot \begin{pmatrix} 1 \\ \sqrt{2} \\ \sqrt{3} \\ \sqrt{6} \end{pmatrix}, \qquad A := \begin{pmatrix} 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 \\ 0 & 3 & 2 & 0 \end{pmatrix}. \tag{47}$$

A short computation shows that the characteristic polynomial of A is

$$f := \det(A - x \cdot E_4) = x^4 - 10x^2 + 1 \in \mathbb{Z}[x].$$

Since $f(\alpha) = 0$, $\alpha \in \mathcal{O}_K$ is integral. In fact, $f = m_\alpha$ is the minimal polynomial of α (Exercise 2.4.3).

We have shown that $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$. However, this is not an equality. Consider, for instance, the element

$$\beta := \frac{\sqrt{2} + \sqrt{6}}{2} \in K.$$

A similar computation as for α shows that β is a root of the monic integral polynomial

$$g = x^4 - 4x^2 + 1 \in \mathbb{Z}[x].$$

We see that $\beta \in \mathcal{O}_K \backslash \mathbb{Z}[\alpha]$. We will show later that

$$\mathcal{O}_K = \langle 1, \sqrt{2}, \sqrt{3}, \beta \rangle_{\mathbb{Z}}.$$

In particular, $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-submodule of K.

Theorem 2.4.7 *Let K be a number field of degree n. Then the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. In other words, there exist elements $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ such that every element $\alpha \in \mathcal{O}_K$ can be uniquely written as*

$$\alpha = \sum_{i=1}^{n} a_i \alpha_i, \quad \textit{with } a_i \in \mathbb{Z}.$$

Definition 2.4.8 A tupel $(\alpha_1, \ldots, \alpha_n)$ as in Theorem 2.4.7 is called an *integral basis* of K.

We postpone the proof a bit, and give another example.

Example 2.4.9 Let $D \in \mathbb{Z}$ be a nonzero, squarefree integer. Then $K := \mathbb{Q}[\sqrt{D}]$ is a quadratic number field. We shall determine its ring of integers $\mathcal{O}_K$. An arbitrary element $\alpha \in K$ is of the form $\alpha = a + b\sqrt{D}$. We have $\alpha \in \mathbb{Q}$ if and only if $b = 0$. Since $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, we may assume that $b \neq 0$.

Let $\tau : K \xrightarrow{\sim} K$ denote the unique nontrivial automorphisms of K. The minimal polynomial of α is

$$m_\alpha = (x - \alpha)(x - \tau(\alpha)) = x^2 - T_{K/\mathbb{Q}}(\alpha) + N_{K/\mathbb{Q}}(\alpha) = x^2 - 2ax + (a^2 - Db^2).$$

Therefore,

$$\alpha \in \mathcal{O}_K \quad \Leftrightarrow \quad 2a \in \mathbb{Z},\ a^2 - Db^2 \in \mathbb{Z}. \tag{48}$$

Elementary arguments (see Exercise 2.4.2) now show the following.

(i) Assume that $D \equiv 2, 3 \pmod 4$. Then $\alpha = a + b\sqrt{D} \in \mathcal{O}_K$ if and only if $a, b \in \mathbb{Z}$. It follows that $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$, with integral basis $(1, \sqrt{D})$.

(ii) Assume that $D \equiv 1 \pmod 4$. Then $\alpha = a + b\sqrt{D} \in \mathcal{O}_K$ if and only if $a, b \in \frac{1}{2}\mathbb{Z}$ and $a + b \in \mathbb{Z}$. It follows that $\mathcal{O}_K = \mathbb{Z}[\theta]$, with $\theta := (1+\sqrt{D})/2$. Again $(1, \theta)$ is an integral basis.

The discriminant

As before we fix a number field K of degree n. Our main goal is to define the *discriminant* of K. This is a nonzero integer $d_K \in \mathbb{Z}$ which measures, in some sense, the complexity of the number field K. If the ring of integers of K is of the form $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for a primitive element α, then $d_K = \Delta(m_\alpha)$ is equal to the discriminant of the minimal polynomial of α (Remark 2.4.14). As a byproduct of the definition of d_K, we prove the existence of an integral basis for K (Theorem 2.4.7).

Definition 2.4.10 An (additive) subgroup $M \subset K$ is called a *lattice* if there exists a $\mathbb{Q}$-basis $(\beta_1, \ldots, \beta_n)$ of K such that

$$M = \langle \beta_1, \ldots, \beta_n \rangle_{\mathbb{Z}}.$$

The tupel $\beta = (\beta_1, \ldots, \beta_n)$ is then called an *integral basis* of M.

Remark 2.4.11 A subgroup $M \subset K$ is a lattice if and only it is a free $\mathbb{Z}$-module of rank n. Therefore, Theorem 2.4.7 is equivalent to the assertion that the ring of integers $\mathcal{O}_K \subset K$ is a lattice.

Definition 2.4.12 Let $M \subset K$ be a lattice with integral basis $\beta = (\beta_1, \ldots, \beta_n)$. We define a rational number

$$d(\beta) := \det \left(T_{K/\mathbb{Q}}(\beta_i \beta_j) \right)_{i,j} \in \mathbb{Q}.$$

By Proposition 2.4.13 (ii) below, this number depends only on the lattice M but not on the chosen basis. We therefore write $d(M) := d(\beta)$ and call it the *discriminant* of M.

Proposition 2.4.13 (i) *Let $M' \subset K$ be another lattice with integral basis $\beta' = (\beta'_1, \ldots, \beta'_n)$, and let $T \in \mathrm{GL}_n(\mathbb{Q})$ be the base change matrix from β to β' (this means that $\beta \cdot T = \beta'$). Then*

$$d(\beta') = \det(T)^2 \cdot d(\beta).$$

(ii) *If $M = M'$ in (ii) then $d(\beta) = d(\beta')$.*

(iii) *We have $d(\beta) \neq 0$. If $M \subset \mathcal{O}_K$ then $d(\beta) \in \mathbb{Z}$ is an integer.*

Proof: Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ denote the distinct embeddings of K into $\mathbb{C}$, and set

$$S := \begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{pmatrix} \in M_{n,n}(\mathbb{C}).$$

Then by Proposition 2.3.11 (ii) we have

$$S^t \cdot S = \Big(\sum_{k=1}^{n} \sigma_k(\beta_i)\sigma_k(\beta_j) \Big)_{i,j} = \Big(T_{K/\mathbb{Q}}(\beta_i \beta_j) \Big)_{i,j}. \tag{49}$$

It follows that

$$d(\beta) = \det(S)^2. \tag{50}$$

Now if $\beta' = (\beta'_1, \ldots, \beta'_n)$ is another $\mathbb{Q}$-basis of K and $T = (a_{i,j})$ is the base change matrix, then

$$S' := \big(\sigma_i(\beta'_j) \big)_{i,j} = S \cdot T. \tag{51}$$

Combining (50) and (51) we obtain a proof of (i). Now assume that $M = \langle \beta_i \rangle_{\mathbb{Z}} = \langle \beta' \rangle_{\mathbb{Z}}$. Then the coefficients $a_{i,j}$ of T are integers. Moreover, the coefficients of T^{-1} are integers as well. Therefore, $\det(T) = 1$, so (ii) follows from (i).

It remains to show that $d(\beta) \neq 0$. But by (i) it suffices to show this for one particular $\mathbb{Q}$-basis of K. Let α be a primitive element of K. Then $\beta := (1, \alpha, \ldots, \alpha^{n-1})$ is a $\mathbb{Q}$-basis of K. Moreover, $\alpha_i := \sigma_i(\alpha)$, for $i = 1, \ldots, n$, are precisely the n complex roots of the minimal polynomial of α (see the proof of Corollary 2.3.6). In particular, $\alpha_i \neq \alpha_j$ for $i \neq j$. Using (50) we get

$$d(\beta) = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdot & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix}^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 \neq 0. \tag{52}$$

This completes the proof of Proposition 2.4.13. □

Remark 2.4.14 If $\alpha \in \mathcal{O}_K$ is a primitive element for K, then the subring $\mathbb{Z}[\alpha]$ is a lattice, with $\mathbb{Z}$-basis $(1, \alpha, \ldots, \alpha^{n-1})$. Let $f \in \mathbb{Q}[x]$ denote the minimal polynomial of α and $\alpha_i \in \mathbb{C}$ the complex roots of f. Then (52) and Definition 2.2.1 show that

$$d(\mathbb{Z}[\alpha]) = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \Delta(f)$$

is equal to the discriminant of f. In practise, this is the easiest and most useful way to compute the discriminant of a number field.

Proof of Theorem 2.4.7: Let $\beta = (\beta_1, \ldots, \beta_n)$ be a $\mathbb{Q}$-basis of K. After replacing β_i by $m\beta_i$, for a suitable integer m, we may assume that $\beta_i \in \mathcal{O}_K$ (see Exercise 2.4.1). Therefore,

$$M := \langle \beta_1, \ldots, \beta_n \rangle_{\mathbb{Z}} \subset \mathcal{O}_K.$$

Lemma 2.4.15 *We have*

$$\mathcal{O}_K \subset d(M)^{-1} \cdot M.$$

Proof: Let $\alpha \in \mathcal{O}_K$ be given and write it as a linear combination of β:

$$\alpha = a_1\beta_1 + \ldots + a_n\beta_n, \qquad a_i \in \mathbb{Q}.$$

We have to show that $d(M)a_i \in \mathbb{Z}$, for $i = 1, \ldots, n$. Set

$$c_i := T_{K/\mathbb{Q}}(\alpha\beta_i) = \sum_{j=1}^{n} a_j T_{K/\mathbb{Q}}(\beta_i\beta_j), \tag{53}$$

for $i = 1, \ldots, n$. In matrix form, this definition becomes

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = S \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \qquad \text{with} \quad S := \left(T_{K/\mathbb{Q}}(\beta_i\beta_j)\right)_{i,j}. \tag{54}$$

By definition we have $d(M) = \det(S)$, so Cramer's rule yields

$$S^{-1} = d(M)^{-1} \cdot S^*,$$

where S^* is the adjunct of S. Applied to (54) we obtain

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = d(M)^{-1} \cdot S^* \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}. \tag{55}$$

Since the trace of an integral element is integral, the coefficents c_i as well as all entries of the matrix S^* are integers. We conclude from (55) that $a_i \in d(M)^{-1}\mathbb{Z}$, and this proves the lemma. □

The lemma shows that $\mathcal{O}_K$ is contained in the lattice $d(M)^{-1}M$. In particular, $\mathcal{O}_K$ is a $\mathbb{Z}$-submodule of a free $\mathbb{Z}$-module of rank n. By Theorem 2.1.1 this implies that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $m \leq n$. But we also have $M \subset \mathcal{O}_K$, so applying Theorem 2.1.1 again shows that $m = n$. Now Theorem 2.4.7 is proved. □

Since $\mathcal{O}_K \subset K$ is a lattice, it is natural to define:

Definition 2.4.16 Let K be a number field. The *discriminant* of K is the nonzero integer

$$d_K := d(\mathcal{O}_K).$$

Example 2.4.17 Let $D \in \mathbb{Z}$ be a squarefree integer and $K := \mathbb{Q}[\sqrt{D}]$. Then the subring $\mathbb{Z}[\sqrt{D}] = \langle 1, \sqrt{D} \rangle_{\mathbb{Z}} \subset \mathcal{O}_K$ is a lattice contained in $\mathcal{O}_K$. Its discriminant is

$$d(\mathbb{Z}[\sqrt{D}]) = \begin{vmatrix} T_{K/\mathbb{Q}}(1) & T_{K/\mathbb{Q}}(\sqrt{D}) \\ T_{K/\mathbb{Q}}(\sqrt{D}) & T_{K/\mathbb{Q}}(D) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2D \end{vmatrix} = 4D.$$

If $D \equiv 2, 3 \pmod 4$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$, and hence $d_K = 4D$, see Example 2.4.9. However, if $D \equiv 1 \pmod 4$ then $\mathcal{O}_K = \mathbb{Z}[\theta] = \langle 1, \theta \rangle_{\mathbb{Z}}$, where $\theta := (1 + \sqrt{D})/2$. One computes

$$d(\mathbb{Z}[\theta]) = \begin{vmatrix} T_{K/\mathbb{Q}}(1) & T_{K/\mathbb{Q}}(\theta) \\ T_{K/\mathbb{Q}}(\theta) & T_{K/\mathbb{Q}}(\theta^2) \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \frac{1+D}{2} \end{vmatrix} = D.$$

To summarize: the discriminant of the quadratic number field $K = \mathbb{Q}[\sqrt{D}]$ is equal to

$$d_K = \begin{cases} 4D, & D \equiv 2, 3 \pmod 4, \\ D, & D \equiv 1 \pmod 4. \end{cases} \tag{56}$$

Proposition 2.4.18 *Let K be a number field and $M' \subset M \subset K$ lattices. Then*

$$|M/M'| = \sqrt{\frac{d(M')}{d(M)}}.$$

Proof: Let $\beta = (\beta_1, \ldots, \beta_n)$ be a $\mathbb{Z}$-basis of M and $\beta' = (\beta'_1, \ldots, \beta'_n)$ be a $\mathbb{Z}$-basis of M'. Since $M' \subset M$, the base change matrix $T \in \mathrm{GL}_n(\mathbb{Q})$ with $\beta' = \beta \cdot T$ has integral coefficients. By Proposition 2.1.2 we have

$$|M/M'| = \det(T).$$

We can conclude that proof by applying Proposition 2.4.13 (i). □

Corollary 2.4.19 *Let $\alpha \in \mathcal{O}_K$ be a primitive elements for K, with minimal polynomial $f \in \mathbb{Z}[x]$. Then*

$$\Delta(f) = m^2 d_K,$$

with $m := (\mathcal{O}_K : \mathbb{Z}[\alpha]) \in \mathbb{N}$. In particular, if $\Delta(f)$ is square free, then $d_K = \Delta(f)$ and $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Proof: By assumption the subring $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ is a lattice in K. Therefore, the claim follows from Remark 2.4.14 and Proposition 2.4.18. □

Corollary 2.4.19 gives a useful criterion to determine the ring of integers $\mathcal{O}_K$ and the discriminant d_K of a number field K.

Example 2.4.20 Let $K = \mathbb{Q}[\theta]$ be the number field with generator θ and defining polynomial

$$f = x^3 + x^2 - 2x + 8.$$

A computer calculation shows that the discriminant of f is

$$\Delta(f) = -2012 = -2^2 \cdot 503.$$

Corollary 2.4.19 leaves us two possibilities. Either $\mathcal{O}_K = \mathbb{Z}[\theta]$ and $d_K = -2012$ or $(\mathcal{O}_K : \mathbb{Z}[\theta]) = 2$ and $d_K = -503$.

It is easier to prove the second possibility by disproving the first, than it is to prove the first. Consider the element

$$\alpha := \frac{\theta + \theta^2}{2} \in K \backslash \mathbb{Z}[\theta].$$

A computer calculation shows that the minimal polynomial of α is

$$g := m_\alpha = x^3 - 2x^2 + 3x - 10.$$

It follows that $\alpha \in \mathcal{O}_K$ is integral and hence $\mathbb{Z}[\theta] \neq \mathcal{O}_K$. We conclude that $\mathcal{O}_K = \mathbb{Z}[\theta, \alpha]$ and that $d_K = -503$.

Minkowski space

The *Minkowski space* of a number field K is a euclidean vector space $K_\mathbb{R}$ which contains K as a $\mathbb{Q}$-vector space, and is spanned by K. Moreover, the absolute value of the discriminant of a lattice $M \subset K \subset K_\mathbb{R}$ is related to the covolume of M as a lattice in $K_\mathbb{R}$. This gives a nice geometric interpretation of the discriminant and clarifies the proof of Proposition 2.4.13 above.

The method of viewing algebraic integers as lattice points in Minkowski space is called *Minkowski theory* or the *geometry of numbers*. In later chapters, it will be a fundamental tool to study the arithmetic of K.

Definition 2.4.21 Let V be a real vector space of dimension n. A *lattice* in V is a subgroup $\Gamma \subset V$ of the form

$$\Gamma = \langle v_1, \ldots, v_m \rangle_\mathbb{Z},$$

with m linearly independent vectors $v_1, \ldots, v_m$. The tupel $(v_1, \ldots, v_m)$ is called a *basis* of the lattice Γ, and the set

$$P := \{x_1 v_1 + \ldots + x_m v_m \mid x_i \in \mathbb{R},\ \ 0 \leq x_i < 1\} \subset V$$

is called the *fundamental domain* of the lattice (with respect to the basis (v_i)). If $n = m$ then the lattice Γ is called *complete*.[5]

Proposition 2.4.22 *Let $\Gamma \subset V$ be a subgroup of a real vector space of dimension n.*

(i) *Γ is a lattice if and only if it is a discrete subset of V.*

(ii) *Assume Γ is a lattice, with basis $(v_1, \ldots, v_m)$. Let P denote the fundamental domain of Γ with respect to the basis (v_i). Then Γ is a complete lattice if and only if V is the disjoint union of the translates $P + \gamma$, i.e.*

$$V = \coprod_{\gamma \in \Gamma} P + \gamma.$$

Proof: See e.g. [6], Satz I.4.2 und Lemma I.4.3. □

Now let $(V, \langle \cdot, \cdot \rangle)$ be a euclidean vector space of dimension n. Let $v_1, \ldots, v_n \in V$ be n vectors and $\Gamma := \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}} \subset V$. Let

$$A := \big(\langle v_i, v_j \rangle\big)_{i,j} \in M_{n,n}(\mathbb{R})$$

denote the *Gram matrix* of $v_1, \ldots, v_n$. Now Γ is a full lattice if and only if $v_1, \ldots, v_n$ are linearly independent. By [4], §5.4.10, this is the case if and only if $\det(A) > 0$. Moreover, if $\det(A) > 0$ then

$$\mathrm{vol}(P) = \sqrt{\det(A)}$$

is the volume of the fundamental domain given by the v_i. Note that $\mathrm{vol}(P)$ depends only on the lattice Γ but not on the basis $v_1, \ldots, v_n$. Indeed, if (v_i') is another basis of Γ, then the base change matrix T lies in $\mathrm{GL}_n(\mathbb{Z})$. It follows that

$$A' := \big(\langle v_i', v_j' \rangle\big)_{i,j} = T^t \cdot A \cdot T$$

and hence

$$\sqrt{\det(A')} = \det(T) \cdot \sqrt{\det A} = \sqrt{\det A}.$$

Definition 2.4.23 Let $(V, \langle \cdot, \cdot \rangle)$ be a euclidean vector space and $\Gamma \subset V$ a full lattice. Choose a $\mathbb{Z}$-basis $v_1, \ldots, v_n$ for Γ and let P be the corresponding fundamental domain. Then

$$\mathrm{vol}(\Gamma) := \mathrm{vol}(P) > 0$$

is called the *covolume* of the lattice $\Gamma \subset V$.

The name *covolume* can be explained as follows. By Proposition 2.4.22 (ii), the fundamental domain P is a set of representatives for the quotient group V/Γ. Therefore, $\mathrm{vol}(P)$ may be regarded as the volume of the space V/Γ.

[5] It is also common to include this assumption into the definition of a lattice.

Let K be a number field of degree n. Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ denote the n distinct embeddings of K into $\mathbb{C}$. Let (r, s) be the type of K (Definition 2.3.8). As in Remark 2.3.7 we may assume that the first r embeddings $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ are real and the remaining $2s$ embeddings are pairs if complex conjugate embeddings, i.e. $\bar{\sigma}_{r+2i-1} = \sigma_{r+2i}$, for $i = 1, \ldots, s$.

Definition 2.4.24 The real vector space

$$K_{\mathbb{R}} := \{(z_k) \in \mathbb{C}^n \mid z_1, \ldots, z_r \in \mathbb{R},\ ; \bar{z}_{r+2i-1} = z_{r+2i},\ i = 1, \ldots, s\}$$

is called the *Minkowski space* of K.

Note that $K_{\mathbb{R}}$ is a real vector space of dimension $r + 2s = n$; it is not a complex vector space. We have a natural $\mathbb{Q}$-linear embedding

$$j : K \hookrightarrow K_{\mathbb{R}}, \quad \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha)).$$

The skalar product $\langle \cdot, \cdot \rangle$ on $K_{\mathbb{R}}$ is defined as the restriction of the usual hermitian product on $\mathbb{C}^n$, i.e.

$$\langle z, w \rangle := \sum_{i=1}^{n} \bar{z}_i w_i = \sum_{i=1}^{r} z_i w_i + \sum_{i=1}^{s} 2\Re(z_{r+2i} \bar{w}_{r+2i}).$$

The second sum shows that $\langle \cdot, \cdot \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$ is indeed a symmetric and positive definit $\mathbb{R}$-bilinear form. Thus $(K_{\mathbb{R}}, \langle \cdot, \cdot \rangle)$ is a euclidean vector space.

Proposition 2.4.25 *Let $\beta = (\beta_1, \ldots, \beta_n)$ be a $\mathbb{Q}$-basis of K and*

$$M := \langle \beta_1, \ldots, \beta_n \rangle$$

the lattice spanned by β. Then $(j(\beta_1), \ldots, j(\beta_n))$ is an $\mathbb{R}$-basis of $K_{\mathbb{R}}$. Therefore, $j(M) \subset K_{\mathbb{R}}$ is a complete lattice in the sense of Definition 2.4.21. Moreover, we have

$$\mathrm{vol}(j(M)) = \sqrt{|d(M)|}.$$

Proof: Let

$$A := \big(\langle j(\beta_i), j(\beta_j) \rangle\big)_{i,j}$$

denote the Gram matrix of the vectors $j(\beta_1), \ldots, j(\beta_n) \in K_{\mathbb{R}}$, with respect to the scalar product $\langle \cdot, \cdot \rangle$. By the discussion preceeding Definition 2.4.24 we have to show that $\det(A) > 0$ and that

$$\det(A) = |d(M)|. \tag{57}$$

In fact, we have $d(M) \neq 0$ by Proposition 2.4.13 (iii), so it suffices to prove (57).

By definition we have

$$\langle j(\beta_i), j(\beta_j) \rangle = \sum_{k=1}^{n} \overline{\sigma_k(\beta_i)} \sigma_k(\beta_j),$$

for all i, j. In matrix form this means that

$$A = \bar{S}^t \cdot S, \qquad \text{with} \quad S := \big(\sigma_i(\beta_j)\big)_{i,j}.$$

Using (50) we conclude that

$$\det(A) = |\det(S)|^2 = |d(M)|.$$

This completes the proof. □

Corollary 2.4.26 *The subgroup $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ is a complete lattice with covolume*

$$\mathrm{vol}(j(\mathcal{O}_K)) = \sqrt{|d_K|}.$$

Example 2.4.27 Let $D > 0$ be a squarefree positive integer, and let $K := \mathbb{Q}[\sqrt{-D}]$ denote the corresponding imaginary quadratic number field. We have two complex conjugate embeddings $\sigma_1, \sigma_2 : K \hookrightarrow K$ given by

$$\sigma_1(\sqrt{-D}) = i\sqrt{D}, \qquad \sigma_2(\sqrt{-D}) = -i\sqrt{D}.$$

So the Minkowski space of K is the real vector space

$$K_{\mathbb{R}} = \{(z_1, z_2) \in \mathbb{C}^2 \mid \bar{z}_1 = z_2\},$$

equipped with the skalar product

$$\langle z, w\rangle = \bar{z}_1 w_1 + \bar{z}_2 w_2 = \bar{z}_1 w_2 + z_1 \bar{w}_1 = 2\Re(\bar{z}_1 w_1).$$

In particular, the *Minkowski norm* is given by

$$||(z_1, z_2)|| = \sqrt{2} \cdot |z_1|.$$

We may identify $K_{\mathbb{R}}$ with $\mathbb{C}$ (considered as a real vector space!) via the projection to the first coordinate:

$$K_{\mathbb{R}} \cong \mathbb{C}, \quad (z_1, z_2) \mapsto z_1.$$

With this identification, the Minkowski norm is equal to the usual euclidean norm on $\mathbb{C} = \mathbb{R}^2$, multiplied with $\sqrt{2}$. Also, the embedding $j : K \hookrightarrow K_{\mathbb{R}}$ is identified with the embedding $\sigma_1 : K \hookrightarrow \mathbb{C}$.

Consider, for instance, the case $D = 3$. The ring of integers is $\mathcal{O}_K = \mathbb{Z}[\omega]$, with $\omega = (1 + \sqrt{-3})/2$. If we consider $\mathcal{O}_K$ as a lattice in Minkowski space $K_{\mathbb{R}} = \mathbb{C}$, we obtain the lattice depicted in Figure 2. Note that the volume (meaning area) of the fundamental domain, with respect to the Minkowski norm, is equal to $\sqrt{|d_K|} = \sqrt{3}$, which is twice the area computed with the usual euclidean norm.

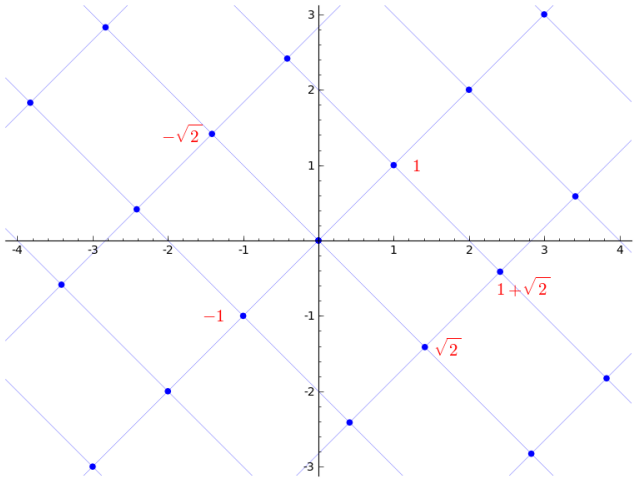


Figure 3: The ring of integers of $\mathbb{Q}[\sqrt{2}]$ as a lattice in Minkowski space

Example 2.4.28 Let $D > 0$ be a positive square free integer and $K := \mathbb{Q}[\sqrt{D}]$ the corresponding real quadratic number field. We may consider K as a subfield of $\mathbb{R}$ and $\sqrt{D} \in \mathbb{R}$ in the usual way as the unique positive square root of D. Let $K \xrightarrow{\sim} K, \alpha \mapsto \alpha'$ denote the unique nontrivial automorphism of K, given by $\sqrt{D}' = -\sqrt{D}$. The Minkowski space of K is simply $K_{\mathbb{R}} = \mathbb{R}^2$, and the embedding of K into $K_{\mathbb{R}}$ is the map

$$j : K \hookrightarrow K_{\mathbb{R}} = \mathbb{R}^2, \quad \alpha \mapsto (\alpha, \alpha').$$

The Minkowski norm on $K_{\mathbb{R}} = \mathbb{R}^2$ is simply the euclidean norm.

Consider the example $D = 2$, $K = \mathbb{Q}[\sqrt{2}]$. The ring of integers is $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \langle 1, \sqrt{2} \rangle_{\mathbb{Z}}$. The lattice $j(\mathcal{O}_K) \subset \mathbb{R}^2$ is spanned by the two vectors

$$j(1) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad j(\sqrt{2}) = \begin{pmatrix} \sqrt{2} \\ -\sqrt{2} \end{pmatrix}.$$

See Figure 3.

Note that the projection of $j(\mathcal{O}_K)$ to the first (resp. the second) coordinate gives rise to the canonical embedding $\mathcal{O}_K \subset K \subset \mathbb{R}$ (resp. the embedding $\mathcal{O}_K \subset K \hookrightarrow \mathbb{R}$, $\alpha \mapsto \alpha'$). In contrast to Example 2.4.27, the image of this embedding, i.e. the subgroup $\mathcal{O}_K \subset \mathbb{R}$, is not a lattice. In fact, it is a dense subset of $\mathbb{R}$. Here we see that, to see the 'full picture', it is essential to consider both embeddings of K into $\mathbb{R}$ at the same time.

Exercises

Exercise 2.4.1 Let K be a number field and $\alpha \in K$ an arbitrary element. Show that there exists a positive integer $m \in \mathbb{N}$ such that $m\alpha \in \mathcal{O}_K$.

Exercise 2.4.2 Prove the Claims (i) and (ii) from Example 2.4.9.

Exercise 2.4.3 Show that the polynomial $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ is irreducible. Deduce that $\alpha := \sqrt{2} + \sqrt{3}$ is a primitive element for $K := \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

2.5 Ideals

We start with discussing the general concept of an ideal. Let R be a commutative ring with unit. Recall that an *ideal* of R is a subgroup $I \subset R$ of the additive group of R such that $a \cdot I \subset I$ holds for all $a \in R$. An ideal $I \lhd R$ is called *finitely generated* if there are elements $a_1, \ldots, a_n \in I$ such that

$$I = (a_1, \ldots, a_n) := \{\sum_{i=1}^{n} b_i a_i \mid b_i \in R\}.$$

We call I a *principal ideal* if it is generated by one element, i.e. $I = (a)$ for some $a \in I$.

Ideals are an abstraction of the set of all multiples of a ring element. Indeed, for principal ideals we have

$$(a) = \{\, b \in R \mid \ a \mid b \,\}.$$

For a general ideal $I \lhd R$ and a ring element $a \in I$ this suggests the following notation:

$$I \mid b \quad :\Leftrightarrow \quad b \in I.$$

The axioms imposed on ideals are then equivalent to the rule

$$I \mid a, \ \ I \mid b \quad \Rightarrow \quad I \mid a \pm b, \ \ I \mid ac,$$

for all $a, b, c \in R$. In this sense, ideals behave just like ordinary ring elements. More generally, we may define a divisibility relation between ideals of a given ring R by

$$I \mid J \quad :\Leftrightarrow \quad J \subset I.$$

This is compatibel with the previous notation because

$$I \mid a \quad \Leftrightarrow \quad I \mid (a).$$

Let $I, J \lhd R$ be ideals. Then it is easy to check that $I \cap J \subset R$,

$$I + J := \{a + b \mid a \in I, \ b \in J\} \subset R$$

and

$$I \cdot J := \{\, \sum_{i=1}^{r} a_i b_i \mid a_i \in I, \ b_i \in J \,\} \subset R$$

are again ideals of R. We also have many rather obvious rules for addition and multiplication of ideals:

- Addition and multiplication of ideals is associative and commutative.
- We have a distributive law

$$I \cdot (J + K) = I \cdot J + I \cdot K.$$

- The zero ideal $(0) \lhd R$ is neutral with respect to addition; moreover $I \cdot (0) = (0)$ for all $I \lhd R$. The ideal $(1) = R$ is neutral with respect to multiplication.

However, neither addition nor multiplication have an inverse. Thus, the set of all ideals of R, together with the operations $+$ and $\cdot$, has a similar structure as the set of nonnegative integers $(\mathbb{N}_0, +, \cdot)$. But this analogy is at least partially misleading, as the following example shows.

Example 2.5.1 Let $R = \mathbb{Z}$. Since $\mathbb{Z}$ is a euclidean ring, every ideal $I \lhd \mathbb{Z}$ is principal and has a unique nonnegative generator,

$$I = (a), \qquad a \in \mathbb{N}_0.$$

In other words, we have a canonical bijection between $\mathbb{N}_0$ and the set of all ideals of $\mathbb{Z}$. This bijection is multiplicative,

$$(a) \cdot (b) = (ab),$$

but not additive. Actually, by Corollary 1.1.20 we have

$$(a) + (b) = (a, b) = (\gcd(a, b)).$$

It is also easy to check that

$$(a) \cap (b) = (\operatorname{lcm}(a, b)),$$

where $\operatorname{lcm}(a, b)$ stand for the *least common multiple* of $a, b \in \mathbb{Z}$.

As this example indicates, we should consider addition of ideals as a generalization of the greatest common divisor and intersection as a generalization of the least common multiple. This analogy goes quite far. For instance, we have the following generalization of the classical *Chinese Remainder Theorem* to general rings.

Proposition 2.5.2 (Chinese Remainder Theorem) *Let $I_1, \ldots, I_n \lhd R$ be ideals in a ring R which are pairwise relatively prime, i.e.*

$$I_i + I_j = R \quad \text{for } i \neq j.$$

Set $I := \cap_i I_i$. Then the natural ring homomorphism

$$R/I \to \oplus_i R/I_i, \quad a \mod I \mapsto \big(a \mod I_i\big)_i$$

is an isomorphism.

Ideals in $\mathcal{O}_K$

Let us fix a number field K of degree n. From now on and for the rest of this chapter all ideals will be ideals of the ring of integers $\mathcal{O}_K$. We will denote them by $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$.

Proposition 2.5.3 *Let $\mathfrak{a} \lhd \mathcal{O}_K$ be a nonzero ideal. Then $\mathfrak{a}$ is a lattice, i.e. a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank n.*

Proof: Let us first assume that $\mathfrak{a} = (\alpha)$ is principal. Since $\alpha \neq 0$, the map

$$\mathcal{O}_K \xrightarrow{\sim} \mathfrak{a} = (\alpha), \quad \beta \mapsto \alpha\beta$$

is an isomorphism of $\mathbb{Z}$-modules. Let $\beta_1, \ldots, \beta_n$ be an integral basis of $\mathcal{O}_K$. It follows that $\alpha\beta_1, \ldots, \alpha\beta_n$ is a $\mathbb{Z}$-basis of $\mathfrak{a}$. So the proposition is true for principal ideals.

For the general case we choose an element $\alpha \in \mathfrak{a}\backslash\{0\}$. Then

$$(\alpha) \subset \mathfrak{a} \subset \mathcal{O}_K.$$

These are inclusions of $\mathbb{Z}$-modules, and both (α) and $\mathcal{O}_K$ are free of rank n. In this situation, Theorem 2.1.1 implies that $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank n as well. □

As a trivial consequence of the proposition we obtain:

Corollary 2.5.4 *Every ideal $\mathfrak{a} \lhd \mathcal{O}_K$ is finitely generated, i.e. there exists $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}$ such that*

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_n).$$

Remark 2.5.5 In the language of commutative algebra Corollary 2.5.4 says that $\mathcal{O}_K$ is a *noetherian ring*.

Corollary 2.5.6 *For any ideal $\mathfrak{a} \lhd \mathcal{O}_K$, the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite.*

Proof: Since $\mathfrak{a}$ is a lattice by Proposition 2.5.3, Proposition 2.4.18 shows that

$$|\mathcal{O}_K/\mathfrak{a}| = \sqrt{d(\mathfrak{a})/d_K} < \infty. \tag{58}$$

□

Definition 2.5.7 The *norm* of an ideal $\mathfrak{a} \lhd \mathcal{O}_K$ is defined as the cardinality of its quotient ring,

$$N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}| \in \mathbb{N}_0.$$

Proposition 2.5.8 *Let $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$. Then*

$$N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|.$$

Proof: Let $\beta_1, \ldots, \beta_n$ be an integral basis of $\mathcal{O}_K$. Then $\alpha\beta_1, \ldots, \alpha\beta_n$ is an integral basis of (α) (see the proof of Proposition 2.5.3). Since $\alpha\beta_i \in \mathcal{O}_K$, we can write

$$\alpha\beta_i = \sum_{j=1}^{n} a_{i,j}\beta_j,$$

with $a_{i,j} \in \mathbb{Z}$. This means that $A := (a_{i,j})$ is the matrix of the base change from (β_i) to $(\alpha\beta_i)$. By Proposition 2.4.13 (i) and Corollary 2.5.12 we have

$$N((\alpha)) = \sqrt{d((\alpha))/d_K} = |\det(A)|.$$

But we may also consider A as the matrix representing the endomorphism $\phi_\alpha : K \to K$, $\phi_\alpha(\beta) := \alpha\beta$, see Definition 2.3.10. Therefore,

$$N((\alpha)) = |\det(A)| = |N_{K/\mathbb{Q}}(\alpha)|.$$

□

Definition 2.5.9 A nonzero ideal $\mathfrak{p} \lhd \mathcal{O}_K$ is called a *prime ideal*[6] if $\mathfrak{p} \neq \mathcal{O}_K$ and if for all $\alpha, \beta \in \mathcal{O}_K$ the following implication holds:

$$\alpha\beta \in \mathfrak{p} \quad \Rightarrow \quad \alpha \in \mathfrak{p} \text{ or } \beta \in \mathfrak{p}. \tag{59}$$

If we use the suggestive notation $\mathfrak{p} \mid \alpha$ for the relation $\alpha \in \mathfrak{p}$, then (59) becomes

$$\mathfrak{p} \mid \alpha\beta \quad \Rightarrow \quad \mathfrak{p} \mid \alpha \text{ or } \mathfrak{p} \mid \beta. \tag{60}$$

This looks very similar to the definition of a prime element of a ring (Definition 1.1.14 (iii)). We immediately obtain:

Remark 2.5.10 (i) A principal ideal $(\alpha) \lhd \mathcal{O}_K$ is a prime ideal if and only if α is a prime element of $\mathcal{O}_K$.

(ii) Let $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$ be ideals and $\mathfrak{p} \lhd \mathcal{O}_K$ a prime ideal. Then

$$\mathfrak{p} \mid \mathfrak{a} \cdot \mathfrak{b} \quad \Rightarrow \quad \mathfrak{p} \mid \mathfrak{a} \text{ or } \mathfrak{p} \mid \mathfrak{b}$$

(recall that $\mathfrak{p} \mid \mathfrak{a} :\Leftrightarrow \mathfrak{a} \subset \mathfrak{p}$).

See Exercise 2.5.2.

Theorem 2.5.11 (i) *Let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal. Then $\mathfrak{p} \cap \mathbb{Z} = \mathbb{Z} \cdot p$, for a unique prime number p.*

(ii) *An ideal $\mathfrak{a} \lhd \mathcal{O}_K$ is a prime ideal if and only if the residue ring $\mathcal{O}_K/\mathfrak{a}$ is a field.*

[6] In abstract algebra, the zero ideal of an integral domain is also considered as a prime ideal, since it satisfies (59). In number theory this is a bit unnatural, since $0 \in \mathbb{Z}$ is not a prime number. We will therefore use the term *prime ideal* only for nonzero ideals.

Proof: Let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal. To prove (i) we have to show that $\bar{\mathfrak{p}} := \mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. It is clear that $\bar{\mathfrak{p}}$ is an ideal and that it satisfies the Condition 59 of Definition 2.5.9. It remains to show that $\bar{\mathfrak{p}} \neq \{0\}$. Choose $\alpha \in \mathfrak{p} \backslash \{0\}$ and let

$$m_\alpha(\alpha) = \alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_0 = 0$$

be its minimal equation. We have $a_i \in \mathbb{Z} \subset \mathcal{O}_K$ and $a_0 \neq 0$. Therefore, the equation shows that $a_0 \in \bar{\mathfrak{p}} = \mathfrak{p} \cap \mathbb{Z}$, proving (i).

Let $\mathfrak{a} \lhd \mathcal{O}_K$ be an ideal such that the ring $\bar{\mathcal{O}} := \mathcal{O}_K/\mathfrak{a}$ is a field. It is immediately clear that $\mathfrak{a} \neq (0), \mathcal{O}_K$. Now let $\alpha, \beta \in \mathcal{O}_K$ with $\alpha\beta \in \mathfrak{a}$. Write $\bar{0}$ for the zero element of $\bar{\mathcal{O}}$ and $\bar{\alpha}, \bar{\beta}$ for the residue classes of α, β. Then

$$\bar{0} = \overline{\alpha\beta} = \bar{\alpha} \cdot \bar{\beta}$$

in $\bar{\mathcal{O}}$. Since $\bar{\mathcal{O}}$ is a field it follows that $\bar{\alpha} = \bar{0}$ or $\bar{\beta} = \bar{0}$, which is equivalent to $\alpha \in \mathfrak{a}$ or $\beta \in \mathfrak{a}$. We have shown that $\mathfrak{a}$ satisfies Condition (59) of Definition 2.5.9 and hence is a prime ideal.

To prove the converse we let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal and denote the residue ring by $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. Reversing the previous argument one shows that $\mathbb{F}_\mathfrak{p}$ is an integral domain. Let p be the prime number with $\mathfrak{p} \cap \mathbb{Z} = \mathbb{Z} \cdot p$. The inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ induces an embedding

$$\mathbb{F}_p := \mathbb{Z}/\mathbb{Z} \cdot p \hookrightarrow \mathbb{F}_\mathfrak{p}$$

of the field $\mathbb{F}_p$ with p elements into $\mathbb{F}_\mathfrak{p}$. Moreover, $\mathbb{F}_\mathfrak{p}$ is an algebraic ring extension of the field $\mathbb{F}_p$. But $\mathbb{F}_\mathfrak{p}$ is also an integral domain. By Exercise 2.5.3 this implies that $\mathbb{F}_\mathfrak{p}$ is a field. □

Corollary 2.5.12 *If $\mathfrak{p} \lhd \mathcal{O}_K$ is a prime ideal, then $N(\mathfrak{p})$ is a prime power, i.e.*

$$N(\mathfrak{p}) = p^f, \qquad f \in \mathbb{N}.$$

Here p is the prime number such that $\mathfrak{p} \cap \mathbb{Z} = \mathbb{Z} \cdot p$.

Recall that an ideal $I \lhd R$ of a ring R is called *maximal* if $I \neq R$, and if the strict inclusion $I \subsetneq J$ implies $J = R$, for every ideal $J \lhd R$. It is an easy but fundamental fact that an ideal $I \lhd R$ is maximal if and only if R/I is a field (see [1], Chapter 10, Corollary 7.3 (a)). Moreover, a maximal ideal is a prime ideal ([1], Chapter 11, Proposition 6.8). The converse is false, in general. However, Theorem 2.5.11 shows:

Corollary 2.5.13 *In the ring $\mathcal{O}_K$ an ideal is prime if and only if it is maximal.*

Prime factorization

The ring of integers $\mathcal{O}_K$ of a number field is typically not a unique factorization domain. As a compensation, we have the following fundamental result.

Theorem 2.5.14 *Every nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ has a factorization into prime ideals,*

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r,$$

and this factorization is unique up to permutation of the factors.

We need three lemmas before we can give a proof.

Lemma 2.5.15 *Let $\mathfrak{M}$ be a nonempty set of ideals of $\mathcal{O}_K$. Then $\mathfrak{M}$ has a maximal element.*

Proof: Assume the contrary. Then there exists an infinite ascending chain $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \ldots$ of ideals $\mathfrak{a}_i \in \mathfrak{M}$. It follows that the norms of $\mathfrak{a}_i$ form an infinite descending sequence of nonnegative integers,

$$N(\mathfrak{a}_1) > N(\mathfrak{a}_2 > \ldots, \quad N(\mathfrak{a}_i) \geq 0.$$

But this is impossible, and the lemma follows. □

Lemma 2.5.16 *Let $\mathfrak{a}$ be a nonzero ideal.*

(i) *There exist a prime ideal $\mathfrak{p}$ with $\mathfrak{a} \subset \mathfrak{p}$.*

(ii) *There exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that*

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset \mathfrak{a}.$$

Proof: Let $\mathfrak{M}_1$ be the set of all ideals $\mathfrak{b}$ such that $\mathfrak{a} \subset \mathfrak{b} \subsetneq \mathcal{O}_K$. Let $\mathfrak{p}$ be a maximal element of $\mathfrak{M}_1$ (Lemma 2.5.15). Clearly, $\mathfrak{p}$ is a maximal ideal and hence a prime ideal by Corollary 2.5.13. We have $\mathfrak{a} \subset \mathfrak{p}$ by construction, so (i) is proved.

Let $\mathfrak{M}_2$ be the set of all ideals $\mathfrak{a} \in \mathcal{O}_K$ which violate the conclusion of Claim (ii) of the lemma. We have to show that $\mathfrak{M}_2$ is empty. We argue by contradiction and assume that $\mathfrak{M}_2$ is nonempty. By Lemma 2.5.16 we may choose a maximal element $\mathfrak{a} \in \mathfrak{M}_2$. Since prime ideals trivially satisfy the conclusion of Claim (ii), $\mathfrak{a}$ is not a prime ideal. Hence there exist ring elements α_1, α_2 such that $\alpha_1\alpha_2 \in \mathfrak{a}$ and $\alpha_1, \alpha_2 \notin \mathfrak{a}$. Let $\mathfrak{a}_1 := \mathfrak{a} + (\alpha_1)$ and $\mathfrak{a}_2 := \mathfrak{a} + (\alpha_2)$. Then

$$\mathfrak{a} \subsetneq \mathfrak{a}_1, \ \mathfrak{a} \subsetneq \mathfrak{a}_2, \ \mathfrak{a}_1 \cdot \mathfrak{a}_2 \subset \mathfrak{a}.$$

It follows that $\mathfrak{a}_1, \mathfrak{a}_2 \notin \mathfrak{M}_2$, and hence $\mathfrak{a}_1, \mathfrak{a}_2$ contain a product of prime ideals. But since $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \subset \mathfrak{a}$, the same is true for $\mathfrak{a}$, contradicting the choice of the $\mathfrak{a}$. Now the lemma is proved. □

Lemma 2.5.17 *Let $\mathfrak{p}$ be a prime ideal and*

$$\mathfrak{p}^{-1} := \{\, \beta \in K \mid \beta \cdot \mathfrak{p} \subset \mathcal{O}_K \}.$$

Then for every nonzero ideal $\mathfrak{a}$ we have

$$\mathfrak{a} \cdot \mathfrak{p}^{-1} := \{ \sum_{i=1}^{r} \alpha_i \beta_i \mid \alpha_i \in \mathfrak{a},\ \beta_i \in \mathfrak{p}^{-1} \} \neq \mathfrak{a}.$$

Moreover,

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathcal{O}_K.$$

Proof: It is clear that $\mathcal{O}_K \subset \mathfrak{p}^{-1}$. We first prove $\mathfrak{p}^{-1} \neq \mathcal{O}_K$. Choose $\alpha \in \mathfrak{p} \backslash \{0\}$. By Lemma 2.5.16 (ii) there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset (\alpha) \subset \mathfrak{p}. \tag{61}$$

We may assume that r is minimal with this property. It follows from (61) and Remark 2.5.10 (ii) that $\mathfrak{p}_i \subset \mathfrak{p}$ for at least one index i. But $\mathfrak{p}_i$ is a maximal ideal (Corollary 2.5.13) and hence $\mathfrak{p}_i = \mathfrak{p}$. After reordering, we may assume that $\mathfrak{p} = \mathfrak{p}_1$. By the minimality of r we have $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \subsetneq (\alpha)$. Choose an element $\beta \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \backslash (\alpha)$. Then on the one hand we have

$$\alpha^{-1}\beta \notin \mathcal{O}_K, \tag{62}$$

but on the other hand (61) shows that

$$\beta \cdot \mathfrak{p} \subset (\alpha). \tag{63}$$

Combining (62) and (63) we get

$$\alpha^{-1}\beta \in \mathfrak{p}^{-1} \backslash \mathcal{O}_K.$$

Hence $\mathfrak{p}^{-1} \neq \mathcal{O}_K$.

Now let $\mathfrak{a}$ be a nonzero ideal and assume that $\mathfrak{a} \cdot \mathfrak{p}^{-1} = \mathfrak{a}$. Let $\beta \in \mathfrak{p}^{-1}$ be an arbitrary element. Then

$$\beta \cdot \mathfrak{a} \subset \mathfrak{a}.$$

But $\mathfrak{a} \subset K$ is a lattice by Proposition 2.5.3 and hence $\beta \in \mathcal{O}_K$ by Lemma 2.4.2. It follows that $\mathfrak{p}^{-1} = \mathcal{O}_K$, but this contradicts what we have shown above. We conclude that $\mathfrak{a} \cdot \mathfrak{p}^{-1} \neq \mathfrak{a}$.

Finally, the strict inclusion $\mathfrak{p} \subsetneq \mathfrak{p} \cdot \mathfrak{p}^{-1}$ and the fact that $\mathfrak{p}$ is a maximal ideal (Corollary 2.5.13) shows that $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathcal{O}_K$. Now the lemma is proved. □

Proof of Theorem 2.5.14: We first show that every nonzero ideal has a factorization into prime ideals. Let $\mathfrak{M}$ be the set of all ideals which are different from (0) and $\mathcal{O}_K$ and which do *not* have such a factorization. Assume that $\mathfrak{M}$ is nonempty. Then $\mathfrak{M}$ has a maximal element $\mathfrak{a}$ by Lemma 2.5.15. Let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{a}$ (Lemma 2.5.16 (i)). Then

$$\mathfrak{a} \subset \mathfrak{a} \cdot \mathfrak{p}^{-1} \subset \mathfrak{p} \cdot \mathfrak{p}^{-1} \subset \mathcal{O}_K. \tag{64}$$

It follows from Lemma 2.5.17 that the first inclusion in (64) is strict, whereas the third inclusion is an equality. Thus, (64) becomes

$$\mathfrak{a} \subsetneq \mathfrak{a} \cdot \mathfrak{p}^{-1} \subset \mathcal{O}_K. \tag{65}$$

By the maximality of $\mathfrak{a} \in \mathfrak{M}$ there exists a prime factorization

$$\mathfrak{a} \cdot \mathfrak{p}^{-1} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r.$$

It follows that

$$\mathfrak{a} = \mathfrak{a} \cdot \mathfrak{p}^{-1} \cdot \mathfrak{p} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \cdot \mathfrak{p},$$

which contradicts the choice of $\mathfrak{a}$. The existence statement of Theorem 2.5.14 is proved.

To prove uniqueness, we assume that an ideal $\mathfrak{a}$ has two factorizations,

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s. \tag{66}$$

If a prime ideal $\mathfrak{p}$ divides the product of two ideals, then it must divide one of them (Remark 2.5.10 (ii)). It follows that $\mathfrak{p}_1$ divides one of the factors $\mathfrak{q}_i$, say $\mathfrak{q}_1$, and then $\mathfrak{p}_1 = \mathfrak{q}_1$ because $\mathfrak{q}_1$ is maximal. We multiply (66) with $\mathfrak{p}_1^{-1} = \mathfrak{q}_1^{-1}$ and, using the equality $\mathfrak{p}_1 \cdot \mathfrak{p}_1^{-1} = \mathcal{O}_K$ (Lemma 2.5.16), get

$$\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_s.$$

Iterating this argument we obtain $r = s$ and, after some reordering, $\mathfrak{p}_i = \mathfrak{q}_i$ for all i. □

It is instructive to compare the proof of Theorem 2.5.14 with the proof of unique factorization in $\mathbb{Z}$ (see Theorem 1.1.1 and Proposition 1.1.11). The structure of both proofs is essentially identical, but the substance is rather different. To prove Theorem 1.1.11 the main step was to show that irreducible elements of $\mathbb{Z}$ (i.e. prime numbers) are prime elements: this is Euclid's Lemma, see Corollary 1.1.2. But in the context of prime ideals the corresponding statement is true almost by definition (Remark 2.5.10). In contrast, two statements that were obvious when dealing with prime numbers and the ring $\mathbb{Z}$ are in fact the crucial ingredients for the proof of Theorem 2.5.14. On the one hand, this is the fact that prime ideals of $\mathcal{O}_K$ are maximal (Corollary 2.5.13), on the other hand it is the method of 'dividing by $\mathfrak{p}$', which is possible by Lemma 2.5.17.

Analyzing the proof of Theorem 2.5.14 in more detail one can see that only the following three properties of the ring $\mathcal{O}_K$ are needed:

(a) The ring $\mathcal{O}_K$ is *noetherian*, i.e. every ideal is finitely generated (see Corollary 2.5.4).

(b) The ring $\mathcal{O}_K$ is *integrally closed*, i.e. every element of K satisfying a monic polynomial equation with coefficients in $\mathcal{O}_K$ lies in $\mathcal{O}_K$. This property was used implicitly in the proof of Lemma 2.5.17, when we applied Lemma 2.4.2.

(c) Every prime ideal of $\mathcal{O}_K$ is maximal.

An integral domain R satisfying properties (a)-(c) is called a *Dedekind domain*. Theorem 2.5.14 holds more generally for Dedekind rings, and the proof we gave essentially carries over. This is important in other branches of algebra, in particular algebraic geometry.

We can now draw several useful conclusions from Theorem 2.5.14. The first corollary shows that addition (resp. intersection) of ideals corresponds to taking the greatest common divisor (resp. the least common multiple).

Corollary 2.5.18 *Let $\mathfrak{a}, \mathfrak{b}$ be nonzero ideals of $\mathcal{O}_K$ with prime factorization*

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}, \qquad \mathfrak{b} = \prod_{i=1}^{r} \mathfrak{p}_i^{b_i}.$$

Here $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct prime ideals and $a_i, b_i \geq 0$. Then

$$\mathfrak{a} + \mathfrak{b} = \prod_{i=1}^{r} \mathfrak{p}_i^{\min(a_i, b_i)} \tag{67}$$

and

$$\mathfrak{a} \cap \mathfrak{b} = \prod_{i=1}^{r} \mathfrak{p}_i^{\max(a_i, b_i)}. \tag{68}$$

Proof: Fix an indix i and set

$$\mathfrak{a}' := \mathfrak{p}_i^{a_i - \min(a_i, b_i)} \cdot \prod_{j \neq i} \mathfrak{p}_j^{a_j}, \qquad \mathfrak{b}' := \mathfrak{p}_i^{b_i - \min(a_i, b_i)} \cdot \prod_{j \neq i} \mathfrak{p}_j^{b_j}.$$

Then either $\mathfrak{p}_i \nmid \mathfrak{a}'$ or $\mathfrak{p}_i \nmid \mathfrak{b}'$. It follows that $\mathfrak{p}_i \nmid \mathfrak{a}' + \mathfrak{b}'$, and hence the prime factorization of $\mathfrak{a}' + \mathfrak{b}'$ is of the form

$$\mathfrak{a}' + \mathfrak{b}' = \prod_{j \neq i} \mathfrak{p}_j^{c_j},$$

with $c_j \geq 0$. We conclude that

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{p}_i^{\min(a_i, b_i)} \cdot (\mathfrak{a}' + \mathfrak{b}') = \mathfrak{p}_i^{\min(a_i, b_i)} \cdot \prod_{j \neq i} \mathfrak{p}_j^{c_j}.$$

The uniqueness part of Theorem 2.5.14 shows that $\min(a_i, b_i)$ is the exponent of i in the unique prime factorization of $\mathfrak{a} + \mathfrak{b}$. This proves (67). The proof of (68) is similar and left as an exercise. □

Corollary 2.5.19 (i) *Let $\mathfrak{a} = \mathfrak{p}_1^{a_i} \cdot \ldots \cdot \mathfrak{p}_r^{a_r}$ be the prime factorization of a nonzero ideal $\mathfrak{a}$. Then*

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)^{a_i} \cdot \ldots \cdot N(\mathfrak{p}_r)^{a_r}.$$

(ii) *The ideal norm is multiplicative, i.e. we have*

$$N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b}),$$

for two ideals $\mathfrak{a}, \mathfrak{b}$.

Proof: For $i \neq j$ the ideals $\mathfrak{p}_i^{a_i}$ and $\mathfrak{p}_j^{a_j}$ are relatively prime, i.e. we have

$$\mathfrak{p}_i^{a_i} + \mathfrak{p}_j^{b_j} = \mathcal{O}_K.$$

Therefore, the Chinese Remainder Theorem (Proposition 2.5.2) gives us a ring isomorphism

$$\mathcal{O}_K/\mathfrak{a} \cong \mathcal{O}_K/\mathfrak{p}_1^{a_1} \oplus \ldots \oplus \mathcal{O}_K/\mathfrak{p}_r^{a_r}.$$

We conclude that

$$N(\mathfrak{a}) = N(\mathfrak{p}_1^{a_i}) \cdot \ldots \cdot N(\mathfrak{p}_r^{a_r}).$$

Thus, for the proof of (i) we may assume that $\mathfrak{a} = \mathfrak{p}^a$ for a prime ideal $\mathfrak{p}$. We consider the chain of ideals

$$\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \ldots \supset \mathfrak{p}^a = \mathfrak{a}. \tag{69}$$

We claim that for $i = 0, \ldots, a-1$, the quotient group $\mathfrak{p}^i/\mathfrak{p}^{+1}$ may be considered as a one dimensional vector space over the field $\mathbb{F}_\mathfrak{p} := \mathcal{O}/\mathfrak{P}$. Once we have proved this claim, it follows immediately from the multiplicativity of the index of a subgroup that

$$N(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}) = (\mathcal{O}_K : \mathfrak{p}) \cdot (\mathfrak{p} : \mathfrak{p}^2) \cdot \ldots \cdot (\mathfrak{p}^{a-1} : \mathfrak{p}^a) = N(\mathfrak{p})^a,$$

finishing the proof of (i).

To prove the claim we first have to endow the abelian group $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ with a scalar multiplication by the field $\mathbb{F}_\mathfrak{p}$. But this is the obvious map

$$\mathbb{F}_\mathfrak{p} \times \mathfrak{p}^i/\mathfrak{p}^{i+1} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}, \qquad (\alpha + \mathfrak{p}, \beta + \mathfrak{p}^{i+1}) \mapsto \alpha\beta + \mathfrak{p}^{i+1}.$$

It is a routine exercise to check that this map is well defined and makes $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ an $\mathbb{F}_\mathfrak{p}$-vector space. By the uniqueness of prime factorization we have $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$. Choose any element $\alpha \in \mathfrak{p}^i \backslash \mathfrak{p}^{i+1}$ and set $\mathfrak{b} := \mathfrak{p}^{i+1} + (\alpha)$. Then $\mathfrak{p}^i \supset \mathfrak{b} \supsetneq \mathfrak{p}^{i+1}$. Using again the uniqueness of prime factorization, we see that $\mathfrak{b} = \mathfrak{p}^i$. It follows immediately that the residue class $\alpha + \mathfrak{p}^{i+1}$ spans $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ as an $\mathbb{F}_\mathfrak{p}$-vector space. Thus we have $\dim_{\mathbb{F}_\mathfrak{p}} \mathfrak{p}^i/\mathfrak{p}^{i+1} = 1$, and (i) is proved.

Finally, the multiplicativity of the norm follows directly from (i). □

Decomposition of prime numbers

Let us now fix a prime number p. We are interested in the prime decomposition of the ideal $(p) \lhd \mathcal{O}_K$,

$$(p) = \mathfrak{p}_1^{e_i} \cdot \ldots \cdot \mathfrak{p}_r^{e_i}. \tag{70}$$

Here $\mathfrak{p}_i$ are pairwise distinct prime ideals, and $e_i \geq 1$. We call (70) the *decomposition* or *prime factorization* of p in K.

We will first fix some terminology related to (70).

Definition 2.5.20 Let $\mathfrak{p}$ be a prime ideal of K and p the unique prime number such that $\mathfrak{p} \mid p$. Then $\mathfrak{p} = \mathfrak{p}_i$ for a unique index i in (70).

(i) The exponent

$$e(\mathfrak{p}) := e_i$$

in (70) is called the *ramification index* of $\mathfrak{p}$. The prime ideal $\mathfrak{p}$ is called *ramified* if $e(\mathfrak{p}) > 1$. If $e(\mathfrak{p}) = 1$ then $\mathfrak{p}$ is called *unramified*.

(ii) By Corollary 2.5.12 we have $N(\mathfrak{p}) = p^f$, for some $f \geq 1$. In fact,

$$f = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p].$$

The number $f = f(\mathfrak{p})$ is called the *inertia degree* of the prime ideal $\mathfrak{p}$.

Sometimes we also write $f_i = f(\mathfrak{p}_i)$ and $e_i = e(\mathfrak{p}_i)$ for $i = 1, \ldots, r$.

By Proposition 2.5.8 and Corollary 2.5.12 we have

$$p^n = N((p)) = \prod_{i=1}^{r} N(\mathfrak{p})^{e_i} = \prod_{i=1}^{r} p^{e_i f_i}.$$

The resulting identity

$$n = \sum_{i=1} e_i f_i \tag{71}$$

is called the *fundamental equality*. If we do not want to order the factors of p we can write it in the form

$$n = \sum_{\mathfrak{p} \mid p} e(\mathfrak{p}) f(\mathfrak{p}). \tag{72}$$

Definition 2.5.21 (i) The prime number p is called *ramified* in K if there exists a prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$ with $\mathfrak{p} \mid p$ and $e(\mathfrak{p}) > 1$. Otherwise p it is called *unramified* in K.

(ii) The prime number p is called *totally split* in K if $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$ for all $\mathfrak{p} \mid p$. It is called *totally ramified* if $e(\mathfrak{p}) = n$ and $f(\mathfrak{p}) = 1$ for the (unique) prime divisor $\mathfrak{p}$ of p. It is called *totally inert* if $e(\mathfrak{p}) = 1$ and $f(\mathfrak{p}) = n$, for the (unique) prime divisor $\mathfrak{p}$ of p.

The next theorem gives a concrete way to compute the decomposition of a prime number p in K; unfortunately it only works under an extra assumption which is not always satisfied (but see Remark 2.5.25).

Theorem 2.5.22 *Assume that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for a primitive element α. Let $f \in \mathbb{Z}[x]$ denote the minimal polynomial of α. Let p be a prime number and let $\bar{f} \in \mathbb{F}_p[x]$ denote the reduction of f modulo p. Let*

$$\bar{f} = \bar{f}_1^{e_1} \cdot \ldots \cdot \bar{f}_r^{e_r}$$

be the decomposition of $\bar{f}$ into pairwise distinct, monic and irreducible factors in $\mathbb{F}_p[x]$. Finally, let $f_i \in \mathbb{Z}[x]$ be a monic integral polynomial which reduces to $\bar{f}_i$. Then

$$(p) = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i},$$

where

$$\mathfrak{p}_i := (p, f_i(\alpha)) \lhd \mathcal{O}_K$$

are pairwise distinct prime ideals, with inertia degree $f(\mathfrak{p}_i) = \deg(\bar{f}_i)$.

Proof: Let $\bar{g} \in \mathbb{F}_p[x]$ be one of the irreducible factors of $\bar{f}$ and $g \in \mathbb{Z}[x]$ a monic integral polynomial lifting $\bar{g}$. Let $e \in \mathbb{N}$ be the exponent of $\bar{g}$ in the decomposition of $\bar{f}$ in irreducible factors (recall that $\mathbb{F}_p[x]$ is a euclidean domain and hence factorial). In view of Theorem 2.5.14 and the fundamental equality (71), the following claim is all we need to show.

Claim: The ideal

$$\mathfrak{p} := (p, g(\alpha))$$

is prime with $N(\mathfrak{p}) = p^{\deg(\bar{g})}$. Furthermore, e is the exponent of $\mathfrak{p}$ in the prime factorization of (p), i.e.

$$e = \max\{\, k \in \mathbb{N} \mid \ \mathfrak{p}^k \mid p \,\}.$$

We are now going to prove the claim. It is immediately clear that $\mathfrak{p}$ does not depend on the choice of the lift g but only on $\bar{g}$. Using the isomorphism

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(f)$$

and the *third isomorphism theorem* (see Exercise 2.5.4) we obtain isomorphisms

$$\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}[x]/(p, f, g) \cong \mathbb{F}_p[x]/(\bar{f}, \bar{g}) = \mathbb{F}_p[x]/(\bar{g}).$$

Since $\bar{g}$ is irreducible, the quotient ring $\mathbb{F}_p[x]/(\bar{g})$ is a finite field with $q = p^{\deg(\bar{g})}$ elements (see [1], Chapter 13, Lemma 5.2). It follows that $\mathfrak{p}$ is a prime ideal with norm $N(\mathfrak{p}) = p^{\deg(\bar{g})}$, proving the first half of the claim.

Now we use the quotient ring $\bar{\mathcal{O}} := \mathcal{O}_K/(p)$. Reasoning as above we get isomorphisms

$$\bar{\mathcal{O}} \cong \mathbb{Z}[x]/(p, f) \cong \mathbb{F}_p[x]/(\bar{f}).$$

For convenience, we will consider this isomorphism as an equality. Then the canonical homomorphism

$$\pi : \mathcal{O}_K = \mathbb{Z}[\alpha] \to \bar{\mathcal{O}} = \mathbb{F}_p[x]/(\bar{f})$$

sends an element $\beta = h(\alpha)$, with $h \in \mathbb{Z}[x]$, to the residue class of the polynomial $\bar{h} \in \mathbb{F}_p[x]$. Let $\bar{\mathfrak{p}} := (\bar{g})/(\bar{f}) \lhd \bar{\mathcal{O}}$ be the ideal generated by the residue class of $\bar{g}$. For any $k \in \mathbb{N}$ we have

$$\bar{\mathfrak{p}}^k = (\bar{g}^k, \bar{f})/(\bar{f}). \tag{73}$$

It follows that

$$\mathfrak{p}^k + (p) = (p, g(\alpha)^k) = \pi^{-1}(\bar{\mathfrak{p}}^k). \tag{74}$$

By the definition of $\bar{g}$ and e we can write $\bar{f} = \bar{g}^e \bar{h}$, for a polynomial $\bar{h}$ which is relatively prime to $\bar{g}$. It follows that

$$(\bar{g}^k, \bar{f}) = (\bar{g}^k, \bar{g}^e \bar{h}) = \begin{cases} (\bar{g}^k), & k \leq e, \\ (\bar{g}^e), & k \geq e. \end{cases} \tag{75}$$

Together with (73) this shows that

$$\bar{\mathfrak{p}} \supsetneq \bar{\mathfrak{p}}^2 \supsetneq \ldots \supsetneq \bar{\mathfrak{p}}^e = \bar{\mathfrak{p}}^{e+1} = \ldots$$

and, using (74) we obtain

$$\mathfrak{p} + (p) \supsetneq \mathfrak{p}^2 + (p) \supsetneq \ldots \supsetneq \mathfrak{p}^e + (p) = \mathfrak{p}^{e+1} + (p) = \ldots \tag{76}$$

Let

$$(p) = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

be the factorization of (p) into distinct prime factors. Since $\mathfrak{p} \mid p$ we have $\mathfrak{p} = \mathfrak{p}_i$ for a unique index i. By Corollary 2.5.18 we have

$$\mathfrak{p}^k + (p) = \mathfrak{p}_i^{\min(e_i,k)} \cdot \prod_{j \neq i} \mathfrak{p}_j^{e_j}.$$

Together with (76) this shows that $e = e_i$. This finishes the proof of the claim and hence of Theorem 2.5.22. □

Corollary 2.5.23 *Assume $\mathcal{O}_K = \mathbb{Z}[\theta]$. Then a prime number p is ramified in K if and only if $p \mid d_K$. In particular, all except finitely many prime numbers p are unramified in K.*

Proof: Let f denote the minimal polynomial of θ and $\bar{f} \in \mathbb{F}_p[x]$ the reduction of f modulo p. By Theorem 2.5.22, p is ramified in K if and only if $\bar{f}$ is inseparable (i.e. one of its prime factors occurs with mutiplicity > 1). By Corollary 2.2.4, this happens if and only if $d \mid \Delta(f)$. But $\Delta(f) = d_K$ by Remark 2.4.14. □

Example 2.5.24 Let $K := \mathbb{Q}[i]$ be the field of Gaussian numbers. The ring of integers of K is the ring of Gaussian integers $\mathbb{Z}[i]$. According to Theorem 2.5.22, the decomposition of a prime number p in K depends on the factorization of the polynomial $x^2 + 1 \in \mathbb{F}_p[x]$. There are three distinct cases.

- For $p = 2$ we have $x^2 + 1 = (x + 1)^2$ in $\mathbb{F}_2[x]$. This shows that

$$(2) = \mathfrak{p}^2, \quad \text{with } \mathfrak{p} := (2, i + 1) = (i + 1).$$

- Assume $p \equiv 1 \pmod 4$. Then -1 is a quadratic residue modulo p. This means that
$$x^2 + 1 = (x + \bar{a})(x - \bar{a}) \in \mathbb{F}_p[x],$$
for some integer a prime to p. It follows that
$$(p) = \mathfrak{p}_1\mathfrak{p}_2, \quad \text{where } \mathfrak{p}_1 := (p, a + i),\ \mathfrak{p}_2 := (p, a - i).$$

- Assume $p \equiv 3 \pmod 4$. Then -1 is a quadratic nonresidue modulo p and the polynomial $x^2 + 1 \in \mathbb{F}_p[x]$ is irreducible. It follows that (p) is a prime ideal of $\mathcal{O}_K = \mathbb{Z}[i]$.

Remark 2.5.25 In order to apply Theorem 2.5.22 the ring of integers of K has to be of the form $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for a primitive element α. Unfortunately, this is not always the case, see Example 2.5.26 and Remark 2.5.27.

There always exists an element $\alpha \in \mathcal{O}_K$ which is a primitive element for the number field K. Then $\mathbb{Z}[\alpha]$ is a subring of $\mathcal{O}_K$ with fraction field K. Such a subring is called an *order* of K. The *conductor* of $\mathbb{Z}[\alpha]$ is the ideal
$$\mathfrak{F} := \{\, \beta \in \mathcal{O}_K \mid \beta\mathcal{O}_K \subset \mathbb{Z}[\alpha] \,\}.$$
One can prove that the statement of Theorem 2.5.22 remains true for all prime number p such that (p) is relatively prime to $\mathfrak{F}$. Note that this condition holds for almost all p. See [6], Satz I.8.3 and Exercise 2.5.5.

Furthermore, one can show that the statement of Corollary 2.5.23 is true without any assumption. See [6], Korollar III.2.12.

Example 2.5.26 Let $K = \mathbb{Q}[\theta]$ be the number field considered in Example 2.4.20, with generator θ and defining polynomial
$$f = x^3 + x^2 - 2x + 8.$$
We have seen that $d_K = -503$ and that $\mathcal{O}_K = \mathbb{Z}[\theta, \alpha]$, where
$$\alpha := \frac{\theta^2 + \theta}{2}.$$
It follows that $\mathbb{Z}[\theta] \subsetneq \mathcal{O}_K$ and that the conductor $\mathfrak{F}$ of the order $\mathbb{Z}[\theta]$ is a divisor of 2,
$$\mathfrak{F} \mid 2.$$
Therefore, by Remark 2.5.25 the conclusion of Theorem 2.5.22 holds for all prime numbers $p \neq 2$. Consider, for instance, the prime $p = 503$. A computation in the finite field $\mathbb{F}_{503}$ shows that
$$f = x^3 + x^3 - 2x + 8 \equiv (x + 299)(x + 354)^2 \pmod{503}.$$
We conclude that
$$(503) = \mathfrak{q}_1\mathfrak{q}_2^2,$$

where

$$\mathfrak{q}_1 := (503, \theta + 299), \qquad (503, \theta + 354)$$

are the two distinct prime divisors of 503 in K. In particular, $p = 503$ is ramified in the number field K.

What about $p = 2$? Since $2 \nmid d_K = -503$, $p = 2$ should be unramified by Remark 2.5.25. In order to verify this directly, we are going to show that

$$(2) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3,$$

where

$$\mathfrak{p}_1 := (2, \theta, \alpha), \quad \mathfrak{p}_2 := (2, \theta, \alpha - 1), \quad \mathfrak{p}_3 := (2, \theta - 1, \alpha - 1)$$

are pairwise distinct prime ideals. Note that we cannot use Theorem 2.5.22 directly, and that

$$f \equiv x^2(x + 1) \pmod 2.$$

Let $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \lhd \mathcal{O}_K$ be the ideals defined above. Clearly, $\mathfrak{p}_i \mid 2$. It is also easy to see that the ideals $\mathfrak{p}_i$ are relatively prime and hence pairwise distinct. For instance,

$$\mathfrak{p}_1 + \mathfrak{p}_2 = (2, \theta, \alpha, \alpha - 1) = (1) = \mathcal{O}_K.$$

Next we show that $\mathfrak{p}_i \neq \mathcal{O}_K$. Clearly, it suffices to find elements $\beta_i \in K \backslash \mathcal{O}_K$ such that $\beta_i \cdot \mathfrak{p}_i \subset \mathcal{O}_K$, for $i = 1, 2, 3$. We leave it for the reader to check that

$$\beta_1 := \frac{\alpha + 1}{2}, \quad \beta_2 := \frac{\alpha}{2}, \quad \beta_3 := \frac{\theta}{2}$$

do the job.

Since the ideals $\mathfrak{p}_i$ are relatively prime and $\mathfrak{p}_i \mid 2$, Theorem 2.5.14 implies that

$$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \mid 2.$$

Using the multiplicativity of the norm we obtain

$$N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{p}_3) \mid N((2)) = 8.$$

But $N(\mathfrak{p}_i) > 1$ because $\mathfrak{p}_i \neq \mathcal{O}_K$. We conclude that $N(\mathfrak{p}_i) = 2$ for $i = 1, 2, 3$. It follows that $\mathfrak{p}_i$ is a prime ideal with $N(\mathfrak{p}_i) = 2$ and that $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Remark 2.5.27 The previous calculation shows that the ring of integers $\mathcal{O}_K$ of the number field $K = \mathbb{Q}[\theta]$ is *not* of the form $\mathbb{Z}[\gamma]$, for any $\gamma \in \mathcal{O}_K$. To see this, assume that $\mathcal{O}_K = \mathbb{Z}[\gamma]$ and let $g \in \mathbb{Z}[x]$ be the minimal polynomial of γ and $\bar{g} \in \mathbb{F}_2[x]$ its reduction modulo 2. As the prime number 2 splits into three distinct prime ideals, Theorem 2.5.22 shows that $\bar{g}$ would split into three distinct linear factors, i.e.

$$\bar{g} = (x - a_1)(x - a_2)(x - a_3),$$

with $a_i \in \mathbb{F}_2$ and $a_i \neq a_j$. But $\mathbb{F}_2$ has only two elements, so this is impossible.

Exercises

Exercise 2.5.1 Let R be a commutative ring and $I, J \lhd R$ relatively prime ideals. Show that

$$I \cap J = I \cdot J.$$

Exercise 2.5.2 Prove the claims made in Remark 2.5.10.

Exercise 2.5.3 Let K be a field and L an integral domain which contains K as a subfield. Assume that L/K is algebraic, i.e. that every element $\alpha \in L$ is algebraic over K. Prove that L is a field.

Exercise 2.5.4 Prove the *third isomorphism theorem*: let A be an abelian group, with subgroups $B, C \subset A$ such that $C \subset B$. Then there is a canonical isomorphism

$$(A/C)/(B/C) \xrightarrow{\sim} A/C.$$

Exercise 2.5.5 Let K be a number field of degree n, $\alpha \in \mathcal{O}_K$ an integral primitive element, $f \in \mathbb{Z}[x]$ the minimal polynomial of α, p a prime number and $\bar{f} \in \mathbb{F}_p[x]$ the reduction of f modulo p.

(i) Show that $\mathfrak{F} := \{\beta \mid \beta\mathcal{O}_K \subset \mathbb{Z}[\alpha]\}$ is a nonzero ideal of $\mathcal{O}_K$.

(ii) Assume that $(p) + \mathfrak{F} = \mathcal{O}_K$. Construct a ring isomorph

$$\bar{\mathcal{O}} := \mathcal{O}_K/(p) \xrightarrow{\sim} \mathbb{F}_p[x]/(\bar{f})$$

and extend the proof of Theorem 2.5.22 to the situation considered in this exercise.

Exercise 2.5.6 Let $K = \mathbb{Q}[\sqrt{-7}]$ and $\theta := (1 + \sqrt{-7})/2$.

(i) Show that $\mathfrak{p} := (11, \theta - 5) \lhd \mathcal{O}_K$ is a prime ideal.

(ii) Determine a $\mathbb{Z}$-basis of $\mathfrak{p}^{-1}$.

(iii) Is $\mathfrak{p}$ a principal ideal?

(iv) Determine the decomposition of $(22) \lhd \mathcal{O}_K$ into prime ideals.

Exercise 2.5.7 Let K be a number field and $C > 0$ a constant. Show that there are only finitely many ideals $\mathfrak{a} \lhd \mathcal{O}_K$ with $N(\mathfrak{a}) \leq C$.

2.6 The class group

As before, we fix a number field $K/\mathbb{Q}$. Our next goal is to define the *class group* Cl_K of K. Together with the type (r, s) and the discrimant d_K, this is another fundamental invariant of a number field.

The fastes way to define Cl_K goes as follows. Two nonzero ideals $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$ are called *equivalent* if there is an element $\alpha \in K^\times$ such that $\mathfrak{b} = \alpha \cdot \mathfrak{a}$. Then Cl_K is defined as the set of equivalence classes of nonzero ideals $\mathfrak{a} \lhd \mathcal{O}_K$. In particular, an ideal $\mathfrak{a}$ is equivalent to the ideal $(1) = \mathcal{O}_K$ if and only if $\mathfrak{a}$ is a principal ideal. This means that the class group Cl_K is trivial (i.e. consists of just one element) if and only if $\mathcal{O}_K$ is a principal ideal domain.

It is easy to see that multiplication of ideals is compatible with the equivalence relation and hence gives rise to a multiplication operation $\cdot$ on Cl_K. The main problem is then to show that $(Cl_K, \cdot)$ forms a group. The proof of this crucial fact becomes easier and more transparent if we generalize the notion of an ideal and include this notion in the definition of Cl_K.

Definition 2.6.1 A *fractional ideal* of K is a finitely generated $\mathcal{O}_K$-submodule $\mathfrak{a} \subset K$, with $\mathfrak{a} \neq \{0\}$. In other words,

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_r) := \{ \sum_{i=1}^{r} \alpha_i \beta_i \mid \beta_i \in \mathcal{O}_K \},$$

with elements $\alpha_1, \ldots, \alpha_r \in K^\times$. We write $\mathfrak{a} \lhd K$ to indicate that $\mathfrak{a}$ is a fractional ideal of K. A fractional ideal is said to be *principal* if it is generated by one element, i.e. $\mathfrak{a} = (\alpha)$.

Example 2.6.2 Assume $K = \mathbb{Q}$. Then every fractional ideal is principal. Indeed, let

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_r) \lhd \mathbb{Q}, \quad \alpha_i \in \mathbb{Q}^\times,$$

be a fractional ideal. We can write $\alpha_i = a_i/b$, with $a_i, b \in \mathbb{Z}\backslash\{0\}$, where b is the common denominator. Since $\mathbb{Z}$ is a principal ideal domain, we have $(a_1, \ldots, a_r) = (a) \lhd \mathbb{Z}$, where a is the gcd of the a_i. It follows that

$$\mathfrak{a} = \frac{1}{b} \cdot (a_1, \ldots, a_r) = (\frac{a}{b})$$

is principal.

Remark 2.6.3 The following facts are either immediate consequences of Definition 2.6.1, or are easy to show. Note, however, that the condition of being finitely generated is crucial for the proof of (ii) and (iii).

(i) A nonzero ideal of $\mathcal{O}_K$ is the same thing as a fractional ideal of K contained in $\mathcal{O}_K$. To stress this, we will sometimes call a fractional ideal contained in $\mathcal{O}_K$ an *integral ideal*.

(ii) Given a fractional ideal $\mathfrak{a} \lhd K$ there exists an integer $m \neq 0$ such that $m \cdot \mathfrak{a} \lhd \mathcal{O}_K$ is an integral ideal. This follows from (i) and Remark 2.4.5.

(iii) Every fractional ideal $\mathfrak{a} \lhd K$ is a lattice, i.e. a free $\mathbb{Z}$-submodule of K of rank $n = [K : \mathbb{Q}]$. This follows from (ii) and Proposition 2.5.3.

(iv) If $\mathfrak{a}, \mathfrak{b} \lhd K$ are fractional ideals then so are $\mathfrak{a} + \mathfrak{b}, \mathfrak{a} \cap \mathfrak{b}$ and

$$\mathfrak{a} \cdot \mathfrak{b} := \{ \sum_i \alpha_i \beta_i \mid \alpha_i \in \mathfrak{a},\ \beta_i \in \mathfrak{b} \}.$$

The next lemma shows that fractional ideals are 'invertible'.

Lemma 2.6.4 *Let $\mathfrak{a} \lhd K$ be a fractional ideal. Then*

$$\mathfrak{a}^{-1} := \{ \beta \in K \mid \beta \cdot \mathfrak{a} \subset \mathcal{O}_K \}$$

is a fractional ideal as well, and we have $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathcal{O}_K$.

Proof: It follows from its definition that $\mathfrak{a}^{-1}$ is an $\mathcal{O}_K$-submodule of K. To see that it is finitely generated, choose an element $\alpha \in \mathfrak{a} \backslash \{0\}$. Then $\alpha \cdot \mathfrak{a}^{-1}$ is again an $\mathcal{O}_K$-submodule of K and moreover, $\alpha \cdot \mathfrak{a}^{-1} \subset \mathcal{O}_K$. This means that $\alpha \cdot \mathfrak{a}^{-1}$ is an integral ideal and hence finitely generated (Corollary 2.5.4). We conclude that $\mathfrak{a}^{-1}$ is finitely generated and hence a fractional ideal.

To show that $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathcal{O}_K$ we first assume that $\mathfrak{a} \lhd \mathcal{O}_K$ is integral. Let

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$$

be the prime decomposition of $\mathfrak{a}$ (Theorem 2.5.14). We set

$$\mathfrak{b} := \mathfrak{p}_1^{-1} \cdot \ldots \cdot \mathfrak{p}_r^{-1}.$$

That's a fractional ideal by what we have already shown. Using Lemma 2.5.17 we see that

$$\mathfrak{a} \cdot \mathfrak{b} = (\mathfrak{p}_1 \cdot \mathfrak{p}_1^{-1}) \cdot \ldots \cdot (\mathfrak{p}_r \cdot \mathfrak{p}_r^{-1}) = \mathcal{O}_K. \tag{77}$$

This shows that $\mathfrak{b} \subset \mathfrak{a}^{-1}$. On the other hand, for every $\beta \in \mathfrak{a}^{-1}$ we have $\beta \cdot \mathfrak{a} \subset \mathcal{O}_K$. Using (78) we get

$$\beta \in (\beta) = \beta \cdot \mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{b}.$$

We conclude that $\mathfrak{b} = \mathfrak{a}^{-1}$ and now (78) shows that $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathcal{O}_K$.

If $\mathfrak{a} \lhd K$ is a general fractional ideal, we choose $m \in \mathbb{Z} \backslash \{0\}$ such that $\mathfrak{b} := m \cdot \mathfrak{a} \lhd \mathcal{O}_K$ (Remark 2.6.3 (ii)). Using what we have already shown we see that

$$\mathfrak{a} \cdot \mathfrak{a}^{-1} = (m \cdot \mathfrak{a}) \cdot (m^{-1} \cdot \mathfrak{a}^{-1}) = \mathfrak{b} \cdot \mathfrak{b}^{-1} = \mathcal{O}_K.$$

This completes the proof of the lemma. □

Definition 2.6.5 We let J_K denote the set of all fractional ideals of K. Lemma 2.6.4 shows that J_K is an abelian group with respect to multiplication. We call $(J_K, \cdot)$ the *ideal group* of K.

The subset $P_K \subset J_K$ consisting of all principal fractional ideals is obviously a subgroup. The *ideal class group* of K is the quotient group

$$Cl_K := J_K/P_K.$$

Elements of Cl_K are called *ideal classes* and written as $[\mathfrak{a}]$, where $\mathfrak{a} \in J_K$ is a representing element.

Remark 2.6.6 It follows from Remark 2.6.3 (ii) that every ideal class in Cl_K is represented by an integral ideal. Moreover, two integral ideals $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$ represent the same class if and only if there exists an element $\alpha \in K^\times$ such that $\mathfrak{b} = \alpha \cdot \mathfrak{a}$. We see a posteriori that Definition 2.6.5 gives the same result as the informal and preliminary definition of the class group given at the beginning of this section.

Remark 2.6.7 For a number field K, the following three conditions are equivalent:

(a) The class group Cl_K is trivial.

(b) The ring $\mathcal{O}_K$ is a principal ideal domain.

(c) The ring $\mathcal{O}_K$ is factorial.

Indeed, the equivalence (a)$\Leftrightarrow$(b) follows from the previous remark. The implication (b)$\Rightarrow$(c) is Proposition 1.1.16. For the implication (c)$\Rightarrow$(b), see Exercise 2.6.1.

Example 2.6.8 We consider the number field $K = \mathbb{Q}[\sqrt{-5}]$. Let $\mathfrak{a} \lhd \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ be an integral ideal.

Proposition 2.6.9 *The ideal $\mathfrak{a}$ is either principal, i.e. $\mathfrak{a} = (\alpha)$, or of the form*

$$\mathfrak{a} = (\alpha, \alpha \cdot \frac{1+\sqrt{-5}}{2}),$$

for some $\alpha \in \mathfrak{a}$, $\alpha \neq 0$. In the second case, $\mathfrak{a}$ is not a principal ideal.

Proof: We consider $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ as a subring of $\mathbb{C}$ (by setting $\sqrt{-5} := i\sqrt{5}$). Then $\mathfrak{a} \subset \mathbb{C}$ is a lattice, in the sense of Definition 2.4.21. Let $\alpha \in \mathfrak{a}\backslash\{0\}$ be an element with $r := |\alpha|$ minimal. If $(\alpha) = \mathfrak{a}$ then we are done. So we assume that $(\alpha) \neq \mathfrak{a}$.

Lemma 2.6.10 *Let $n \in \mathbb{N}$, $\gamma \in \mathfrak{a}$ and*

$$D := \{z \in \mathbb{C} \mid |z - \gamma/n| < r/n\}.$$

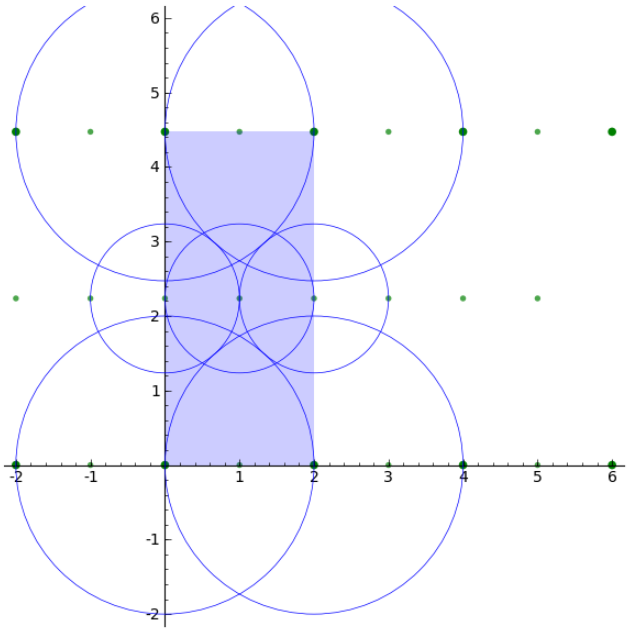
Then $D \cap \mathfrak{a} = \{\gamma/n\}$.

Proof: Let $\beta \in D \cap \mathfrak{a}$. Then $n\beta - \gamma \in \mathfrak{a}$ and $|n\beta - \gamma| < r$. Now the definition of r implies $n\beta = \gamma$, proving the lemma. □

The principal ideal $(\alpha) \subset \mathbb{C}$ is a lattice with $\mathbb{Z}$-basis $(\alpha, \alpha\sqrt{-5})$. Let

$$P := \{t\alpha + s\alpha\sqrt{-5} \mid 0 \leq t, s < 1\} \subset \mathbb{C}$$

be the corresponding fundamental domain for the lattice (α) (Definition 2.4.21). The assumption $(\alpha) \neq \mathfrak{a}$ means that there exist $\beta \in \mathfrak{a} \cap P$, $\beta \neq 0$. Let $D_1, \ldots, D_4 \subset \mathbb{C}$ be the circles with radius r and centers $0, \alpha, \alpha\sqrt{-5}, \alpha + \alpha\sqrt{-5}$ (the vertices of P!). Also, let D_5, D_6, D_7 be the circles with radius $r/2$ and centers $\alpha/2, \alpha(1+\sqrt{-5})/2, \alpha + \sqrt{-5}/2$. The following picture shows that the disks $D_1, \ldots, D_7$ cover the fundamental domain P (where $\alpha = 2$):



Therefore, by Lemma 2.6.10, the element $\beta \in \mathfrak{a} \cap P$ must be a center of one of the disks. Since $\beta \neq 0$ and since $\alpha, \alpha\sqrt{-5}, \alpha(1+\sqrt{-5})$ and $\alpha + \sqrt{-5}/2$ do not lie on P, this leaves us with only two possibilities, namely

$$\beta = \alpha\sqrt{-5}/2, \alpha(1+\sqrt{-5})/2.$$

Suppose $\beta = \alpha\sqrt{-5}/2$. Then $\beta\sqrt{-5} + 2\alpha = -\alpha/4 \in \mathfrak{a}$. But this contradicts the choice of α. We conclude that $\beta = \alpha(1+\sqrt{-5})/2$ is the only element in $\mathfrak{a}\backslash(\alpha)$ which lies in P. It is now easy to see that $\mathfrak{a} = (\alpha, \beta)$.

It remains to be seen that $\mathfrak{a} = (\alpha, \beta)$ is not a principal ideal. So assume that $\mathfrak{a} = (\gamma)$. Then $\gamma \mid \alpha$ which implies $|\gamma| \leq |\alpha| = r$ and then also $|\gamma| = |\alpha|$, by the choice of α. It follows that $\gamma = \pm\alpha$ and hence $\mathfrak{a} = (\gamma) = (\alpha)$. However, $\beta \in \mathfrak{a}\backslash(\alpha)$, contradiction! This completes the proof of Proposition 2.6.9. □

Corollary 2.6.11 *The class group of $K = \mathbb{Q}[\sqrt{-5}]$ is a cyclic group of order 2. Its unique nontrivial element is represented by the fractional ideal*

$$\mathfrak{a}_0 := (1, \frac{1+\sqrt{-5}}{2}).$$

Finiteness of the class group

Theorem 2.6.12 *Let K be a number field of type (r, s). Set*

$$C_K := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

Then every ideal class in Cl_K is represented by an integral ideal $\mathfrak{a} \lhd \mathcal{O}_K$ with $N(\mathfrak{a}) \leq C_K$.

Together with Exercise 2.5.7, this implies the finiteness of Cl_K.

Corollary 2.6.13 *The class group Cl_K is finite.*

Definition 2.6.14 The order $h_K := |Cl_K|$ is called the *class number* of K.

Remark 2.6.15 With a bit more work one can show that the constant C_K in Theorem 2.6.12 can be replaced by

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$

This stronger version of Theorem 2.6.12 is called *Minkowski's bound*. See e.g. [6], I, §5, Aufgabe 3.

The proof of Theorem 2.6.12 uses the following general result on lattices in euclidean vector spaces.

Theorem 2.6.16 (Minkowski) *Let $(V, \langle\cdot,\cdot\rangle)$ be a euclidean vector space of dimension n, $\Gamma \subset V$ a complete lattice and $X \subset V$ a nonempty subset. Assume the following:*

(a) X is symmetric around the origin, i.e. $-X = X$.

(b) X is convex.

(c) $\mathrm{vol}(X) > 2^n \cdot \mathrm{covol}(\Gamma)$.

Then $X \cap \Gamma$ contains a nonzero vector.

Proof: Let $(\gamma_1, \ldots, \gamma_n)$ be a $\mathbb{Z}$-basis of Γ and

$$P := \{\, x = x_1\gamma_1 + \ldots + x_n\gamma_n \mid 0 \le x_i < 1 \,\}$$

the corresponding fundamental domain. Recall that V is the disjoint union of the sets $P + \gamma$, $\gamma \in \Gamma$ (Proposition 2.4.22 (ii)).

Claim: There exist $\gamma_1, \gamma_2 \in \Gamma$ with $\gamma_1 \neq \gamma_2$ such that

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset.$$

To prove the claim we assume the contrary, i.e. that the sets $\frac{1}{2}X + \gamma$ are pairwise disjoint. Then the sets $P \cap (\frac{1}{2}X + \gamma)$ are also pairwise disjoint. It follows that

$$\begin{aligned} \mathrm{vol}(P) &\ge \sum_{\gamma\in\Gamma} \mathrm{vol}\big(P \cap (\frac{1}{2}X + \gamma)\big) \\ &= \sum_{\gamma\in\Gamma} \mathrm{vol}\big((P - \gamma) \cap \frac{1}{2}X\big) \\ &= \mathrm{vol}\big(\frac{1}{2}X\big) = 2^{-n}\mathrm{vol}(X). \end{aligned} \tag{78}$$

But this contradicts Assumption (c) and proves the claim.

We have shown that there exist $\gamma_1, \gamma_2 \in \Gamma$ and $x_1, x_2 \in X$ such that $\gamma_1 \neq \gamma_2$ and

$$\frac{x_1}{2} + \gamma_1 = \frac{x_2}{2} + \gamma_2. \tag{79}$$

Then $-x_2 \in X$ by Assumption (a) and hence $(x_1 - x_2)/2 \in X$ by Assumption (b). Using (79) we conclude that

$$\gamma := \gamma_2 - \gamma_1 = \frac{x_1 - x_2}{2} \in (X \cap \Gamma)\backslash\{0\}.$$

This proves Minkowski's theorem. □

We return to the situation of Theorem 2.6.12.

Lemma 2.6.17 *Let $\mathfrak{a} \lhd \mathcal{O}_K$ be a nonzero ideal. Then there exists an element $\alpha \in \mathfrak{a}\backslash\{0\}$ with*

$$|N(\alpha)| \le N(\mathfrak{a}) \cdot C_K.$$

Proof: Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the n distinct embedding of K into $\mathbb{C}$. We may assume that σ_i is real for $i = 1, \ldots, r$ and that $\bar{\sigma}_{r+2i} = \sigma_{r+2i-1}$ for $i = 1, \ldots, s$. Recall that the Minkoski space for K is the real vector space

$$K_{\mathbb{R}} := \{(z_i) \in \mathbb{C}^n \mid z_1, \ldots, z_r \in \mathbb{R},\ z_{r+2i} = \bar{z}_{r+2i-1}\,\}.$$

The map

$$j : K \hookrightarrow K_{\mathbb{R}}, \qquad \alpha \mapsto (\sigma_1(\alpha, \ldots, \sigma_n(\alpha)),$$

is a $\mathbb{Q}$-linear embedding which maps any $\mathbb{Q}$-basis of K to an $\mathbb{R}$-basis of $K_{\mathbb{R}}$. This implies that the subgroup $j(\mathfrak{a}) \subset V$ is a complete lattice. Furthermore, we have

$$\mathrm{covol}(j(\mathfrak{a})) = \sqrt{|d(\mathfrak{a})|} = N(\mathfrak{a}) \cdot \sqrt{|d_K|}. \tag{80}$$

Let us choose positive constants $c_1, \ldots, c_n > 0$ such that $c_{r+2i} = c_{r+2i-1}$ for $i = 1, \ldots, s$ and

$$\prod_i c_i = N(\mathfrak{a}) C_K + \epsilon. \tag{81}$$

We set

$$X := \{(z_i) \in K_{\mathbb{R}} \mid |z_i| < c_i,\ i = 1, \ldots, n\} \subset K_{\mathbb{R}}.$$

Clearly, X is symmetrical around the origin and convex (Conditions (a) and (b)) from Theorem 2.6.16). An easy calculation also shows that

$$\mathrm{vol}(X) = 2^{r+s} \pi^s \prod_i c_i. \tag{82}$$

Together with (80) and (81) and the definition of C_K we obtain

$$\mathrm{vol}(X) > 2^n N(\mathfrak{a}) \sqrt{|d_K|} = 2^n \mathrm{vol}(j(\mathfrak{a})).$$

We see that Condition (c) of Theorem 2.6.16 is also verified. Applying the theorem we conclude that there exists $\alpha \in \mathfrak{a} \backslash \{0\}$ such that $j(\alpha) \in X$. The latter condition, combined with (81), means that

$$|N(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| < \prod_i c_i = N(\mathfrak{a}) C_K + \epsilon.$$

Since $N(\alpha) \in \mathbb{Z}$, this shows that $|N(\alpha)| \leq N(\mathfrak{a}) C_K$, provided that ϵ was choosen sufficiently small. The lemma is proved. □

Proof: (of Theorem 2.6.12) Let $\mathfrak{a} \lhd \mathcal{O}_K$ be a nonzero ideal. By Lemma 2.6.4 we can choose $m \in \mathbb{N}$ such that $\mathfrak{b} := m \cdot \mathfrak{a}^{-1}$ is an integral ideal. Applying Lemma 2.6.17 to $\mathfrak{b}$ we obtain an element $\beta \in \mathfrak{b} \backslash \{0\}$ with

$$|N(\beta)| \leq N(\mathfrak{b}) C_K.$$

Set $\mathfrak{a}' := \beta \mathfrak{b}^{-1} = m^{-1} \beta \mathfrak{a}$. This is an integral ideal in the same ideal class as $\mathfrak{a}$ such that

$$N(\mathfrak{a}) = |N(\beta)| \cdot N(\mathfrak{b})^{-1} \leq C_K.$$

(Here we have used Exercise 2.6.2.) Now Theorem 2.6.12 is proved. □

The class group of imaginary quadratic fields

We fix a squarefree integer $d < 0$ and set $K := \mathbb{Q}[\sqrt{d}]$. Then $\mathcal{O}_K = \mathbb{Z}[\theta]$, where

$$\theta := \begin{cases} \sqrt{d}, & d \equiv 2,3 \pmod 4, \\ \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod 4. \end{cases}$$

The discriminant of K is $d_K = 4d$ in the first and $d_K = d$ in the second case. We let $f := m_\theta \in \mathbb{Z}[x]$ denote the minimal polynomial of θ, so $f = x^2 - d$ in the first and $f = x^2 - x + c$, with $c := (-d+1)/4$, in the second case. Given $\alpha = x + y\theta \in \mathcal{O}_K$, with $x, y \in \mathbb{Z}$, we have

$$N_{K/\mathbb{Q}}(\alpha) = Q(x,y) := \begin{cases} x^2 - dy^2, & d \equiv 2,3 \pmod 4, \\ x^2 + xy + cy^2, & d \equiv 1 \pmod 4. \end{cases} \tag{83}$$

Note that $Q(x,y)$ is a positive definite quadratic form in x, y. This is in fact the only way in which we use the assumption $d < 0$.

Our goal is to determine the class group C_K explicitly. This is possible by a finite amount of calculation for two reasons. Firstly, every ideal class is represented by an ideal $\mathfrak{a}$ with $N(\mathfrak{a}) \le C_K = 2\sqrt{|d_K|}/\pi$ (Theorem 2.6.12), and it is relatively easy to list the finitely many ideals with this property. Secondly, in order to identify or distinguish the ideals in this list up to equivalence, it is necessary to solve, for certain $m \in \mathbb{N}$, the norm equation

$$N_{K/\mathbb{Q}}(\alpha) = m, \qquad \alpha \in \mathcal{O}_K. \tag{84}$$

Writing $\alpha = x + y\theta$, (84) becomes

$$Q(x,y) = m, \qquad x, y \in \mathbb{Z}. \tag{85}$$

Since the left hand side is a positive definite quadratic form, we can decide in finite time whether or not (84) has a solution.

For a systematic approach the following notion is very useful.

Definition 2.6.18 A nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ is called *primitive* if there exists an integer $a \in \mathbb{Z}$ such that

$$\theta \equiv a \pmod{\mathfrak{a}}.$$

Proposition 2.6.19 (i) *A nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ is primitive if and only if there is a ring isomorphism $\mathcal{O}_K/\mathfrak{a} \cong \mathbb{Z}/m\mathbb{Z}$, where $m := N(\mathfrak{a})$.*

(ii) *Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ be given, with*

$$f(a) \equiv 0 \pmod m.$$

Then

$$\mathfrak{a} := (m, \theta - a) \lhd \mathcal{O}_K$$

is primitive, and $N(\mathfrak{a}) = m$.

(iii) *Every primitive ideal* $\mathfrak{a}$ *is of the form* $\mathfrak{a} = (m, \theta - a)$*, with* m, a *as in (ii). Moreover,* m *and the image of* a *in* $\mathbb{Z}/m\mathbb{Z}$ *are uniquely determined by* $\mathfrak{a}$*.*

Proof: For any nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ we can write $\mathfrak{a} \cap \mathbb{Z} = m\mathbb{Z}$ for a unique positive integer $m \in \mathbb{N}$. We obtain an injective ring homomorphism

$$\mathbb{Z}/m\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{a}, \qquad a + m\mathbb{Z} \mapsto a + \mathfrak{a}. \tag{86}$$

If $\mathfrak{a}$ is primitive, and $a \in \mathbb{Z}$ is such that $\theta \equiv a \pmod{\mathfrak{a}}$, then (86) is surjective. Indeed, for any element $\alpha = x + y\theta \in \mathcal{O}_K$ we have $\alpha \equiv x + ya \pmod{\mathfrak{a}}$. Conversely, if (86) is surjective, then there exists $a \in \mathbb{Z}$ with $\theta \equiv a \pmod{\mathfrak{a}}$ and hence $\mathfrak{a}$ is primitive. This proves (i).

In (ii) the only nontrivial thing to prove is the equality $N(\mathfrak{a}) = m$. The Taylor expansion of $f \in \mathbb{Z}[x]$ at $x = a$ and the assumption $f(a) \equiv a \pmod{m}$ show that

$$f(x) = f(a) + (x - a)g(x) \equiv f(a) \equiv 0 \pmod{(x - a, m)}.$$

Therefore, we have natural ring isomorphisms

$$\mathcal{O}_K/\mathfrak{a} \cong \mathbb{Z}[x]/(f, m, x - a) = \mathbb{Z}[x]/(m, x - a) \cong \mathbb{Z}/m\mathbb{Z}.$$

Now (ii) follows. The proof of (iii) is similar and left to the reader. □

The representation $\mathfrak{a} = (m, \theta - a)$ from Proposition 2.6.19 (ii) is called the *standard form* of $\mathfrak{a}$. Note that, if we assume $0 \leq a < m$ then the pair (m, a) is uniquely determined by $\mathfrak{a}$.

Corollary 2.6.20 *Let* $\mathfrak{a} = (m, \theta - a)$ *be a primitive ideal in standard form. Then* $\mathfrak{a}$ *is principal if and only if there exists* $x, y \in \mathbb{Z}$*, such that*

$$Q(x, y) = m \quad \textit{and} \quad x + ay \equiv 0 \pmod{m}. \tag{87}$$

Here $Q(x, y)$ *is defined as in* (83)*.*

Proof: Assume first that $\mathfrak{a} = (\alpha)$ is principal, with $\alpha = x + y\theta$. Then $N(\mathfrak{a}) = N_{K/\mathbb{Q}}(\alpha) = Q(x, y)$ by Proposition 2.5.8. So Proposition 2.6.19 shows that $Q(x, y) = N(\mathfrak{a}) = m$. Morever, the congruences $\theta \equiv a \pmod{\mathfrak{a}}$ and $\alpha \equiv 0 \pmod{\mathfrak{a}}$ imply

$$x + ya \equiv \alpha \equiv 0 \pmod{\mathfrak{a}}.$$

This means that $x + ya \in \mathfrak{a} \cap \mathbb{Z} = m\mathbb{Z}$, i.e. $x + ay \equiv 0 \pmod{m}$.

Conversely, assume that (87) holds. Then $\alpha := x + y\theta \equiv x + ya \equiv 0 \pmod{\mathfrak{a}}$, which means that $(\alpha) \subset \mathfrak{a}$. Therefore, the equality of norms $N((\alpha)) = N_{K/\mathbb{Q}}(\alpha) = N(\mathfrak{a})$ implies the equality of ideals $(\alpha) = \mathfrak{a}$. □

Remark 2.6.21 Let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal. Then $\mathfrak{p}$ is either primitive or principal. Indeed, let p be the unique prime number such that $\mathfrak{p} \mid p$, and let $\bar{f} \in \mathbb{F}_p$ denote the reduction of f modulo p. If $\bar{f}$ is irreducible, then (p) is a

prime ideal by Theorem 2.5.22, and hence $\mathfrak{p} = (p)$. We say that the prime p is *inert*.

Otherwise, $f = (x-a)(x-b) \pmod p$, with $a, b \in \mathbb{Z}$, and then

$$(p) = (p, \theta - a) \cdot (p, \theta - b)$$

is the prime decomposition of the ideal (p) (Theorem 2.5.22). We say that p *splits*. It follows that $\mathfrak{p}$ is one of the two factors, say $\mathfrak{p} = (p, \theta - a)$. But then $f(a) \equiv 0 \pmod p$, and hence $\mathfrak{p}$ is primitive, by Proposition 2.6.19 (ii). Note that $\mathfrak{p}$ (resp. p) is ramified if and only if the two factors are equal. By Theorem 2.5.22, this is the case if and only if $a \equiv b \pmod p$.

Lemma 2.6.22 *Let $\mathfrak{a} = (m, \theta - a) \lhd \mathcal{O}_K$ be a primitive ideal in standard form. Let $m = \prod_i p_i^{e_i}$ be the prime factorization of m. Then the prime factorization of $\mathfrak{a}$ is*

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

where $\mathfrak{p}_i := (p_i, \theta - a)$.

Proof: Since $p_i \mid m$ we have $f(a) \equiv 0 \pmod{p_i}$, for all i. Hence it follows from Proposition 2.6.19 (ii) that $\mathfrak{p}_i := (p, \theta - a) \lhd \mathcal{O}_K$ is a primitive prime ideal with $N(\mathfrak{p}_i) = p_i$.

Let $\mathfrak{p} \mid \mathfrak{a}$ be an arbitrary prime divisor of $\mathfrak{a}$. Then $\theta \equiv a \pmod{\mathfrak{p}}$, so $\mathfrak{p}$ is primitive. By Remark 2.6.21, $\mathfrak{p} = (p, \theta - b)$ for some prime number p, and $N(\mathfrak{p}) = p$. Since $p = N(\mathfrak{p}) \mid N(\mathfrak{a}) = m$ it follows that $p = p_i$ for some i. Moreover, $b \equiv \theta \equiv a \pmod{\mathfrak{p}}$. We may therefore assume that $b = a$ and hence $\mathfrak{p} = \mathfrak{p}_i$.

We have shown that the prime decomposition of $\mathfrak{a}$ has the form $\mathfrak{a} = \prod_i \mathfrak{p}_i^{c_i}$, with $c_i \geq 0$. But then the multiplicativity of the norm implies

$$\prod_i p_i^{e_i} = m = N(\mathfrak{a}) = \prod_i p_i^{c_i}.$$

We conclude that $c_i = e_i$ for all i, and the lemma is proved. □

Lemma 2.6.23 (i) *Let $\mathfrak{p} \lhd \mathcal{O}_K$ be a primitive and unramified prime ideal. Then $\mathfrak{p}^e$ is primitive, for all $e \geq 1$.*

(ii) *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \lhd \mathcal{O}_K$ be primitive ideals, and assume that the norms $m_i := N(\mathfrak{a}_i)$ are pairwise relatively prime. Then $\mathfrak{a} := \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_r$ is primitive.*

Proof: By Remark 2.6.21 we can write $\mathfrak{p} = (p, \theta - a)$, where p is a prime number and $a \in \mathbb{Z}$ is such that $f(a) \equiv 0 \pmod p$. Furthermore, $f \equiv (x-a)(x-b) \pmod p$, with $a \not\equiv b \pmod p$. We claim that there exists $a_i \in \mathbb{Z}$ such that $a_i \equiv a \pmod p$ and $f(a_i) \equiv 0 \pmod{p^{i+1}}$, for all $i \geq 0$.

We prove the claim by induction on i. For $i = 0$ we set $a_0 := a$. For $i > 0$ we set $a_i := a_{i-1} + p^i d$, for some $d \in \mathbb{Z}$. Then $a_i \equiv a_{i-1} \equiv a \pmod p$, no matter

how we choose d. We will show that $f(a_i) \equiv 0 \pmod{p^{i+1}}$ for some d. Our induction hypothesis says that $f(a_{i-1}) \equiv 0 \pmod{p^i}$. This shows that

$$f = (x - a_{i-1})(x - b') + p^i g, \tag{88}$$

for certain $b' \in \mathbb{Z}$ and $g \in \mathbb{Z}[x]$. Using $f(b) \equiv 0 \pmod{p}$ and $a \not\equiv b \pmod{p}$ one easily shows that $b' \equiv b \pmod{p}$. Furthermore,

$$\begin{aligned} f(a_i) &= p^i d(a_{i-1} - b' + p^i d) + p^i g(a_i) \\ &\equiv p^i \big(d(a_{i-1} - b') + g(a_i)\big) \pmod{p^{i+1}} \\ &\equiv p^i \big(d(a - b) + g(a_i)\big) \pmod{p^{i+1}}. \end{aligned} \tag{89}$$

Using $a \not\equiv b \pmod{p}$ and the fact that $\mathbb{F}_p$ is a field one shows that there exist $d \in \mathbb{Z}$ such that

$$d(a - b) + g(a_i) \equiv 0 \pmod{p}. \tag{90}$$

Combining (89) and (90) yields the desired congruence $f(a_i) \equiv 0 \pmod{p^{i+1}}$ and proves the claim.

Set $\mathfrak{q}_i := (p^{+1}, \theta - a_i)$. Then $\mathfrak{q}_i$ is a primitive ideal with $N(\mathfrak{q}_i) = p^{i+1}$, by Proposition 2.6.19 (ii) and the claim. In particular, every prime deal dividing $\mathfrak{q}_i$ also divides p and is therefore equal to $\mathfrak{p} = (p, \theta - a)$ or $\overline{\mathfrak{p}} = (p, \theta - b)$. However,

With $a_i \in \mathbb{Z}$ as in the claim we have

$$\mathfrak{p}^{i+1} = (p^{i+1}, \theta - a_i).$$

Indeed, the right hand side is a primitive ideal

Theorem 2.6.24 *Every nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ has a unique presentation of the form*

$$\mathfrak{a} = k \cdot \mathfrak{a}_0,$$

with $\mathfrak{a}_0 \lhd \mathcal{O}_K$ primitive.

Proof: Let $\mathfrak{a} \lhd \mathcal{O}_K$ be an arbitrary ideal, with prime factorization $\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i}$. We will show the existence of a presentation $\mathfrak{a} = k \cdot \mathfrak{a}_0$, with $k \in \mathbb{N}$ and $\mathfrak{a}_0$ primitive, and leave the proof of its uniqueness as an exercise.

Assume that there exists an index i such that the prime ideal $\mathfrak{p}_i$ is not primitive. Then $\mathfrak{p}_i = (p_i)$ for a prime number p_i, by Remark 2.6.21. This means that

$$\mathfrak{a} = p_i^{e_i} \cdot \mathfrak{a}', \qquad \text{with} \quad \mathfrak{a}' := \prod_{j \neq i} \mathfrak{p}_j^{e_j}.$$

Now it suffices to prove the theorem for the ideal $\mathfrak{a}'$. Therefore, we may assume that all prime factors $\mathfrak{p}_i$ of $\mathfrak{a}$ are primitive. Similarly, if $\mathfrak{p}_i$ is ramified and $e_i > 1$, then $\mathfrak{p}_i^2 = (p_i)$ for a prime number p_i, and we can write

$$\mathfrak{a} = p_i \cdot \mathfrak{a}', \qquad \text{with} \quad \mathfrak{a}' := \mathfrak{p}_i^{e_i - 2} \cdot \prod_{j \neq i} \mathfrak{p}_j^{e_j}.$$

Hence we may also assume that $e_i = 1$ if $\mathfrak{p}_i$ is ramified. But now Lemma 2.6.23 shows that $\mathfrak{a}$ is primitive. □

Combining Theorem 2.6.12 with Theorem 2.6.24 we obtain:

Corollary 2.6.25 *Every class in Cl_K is represented by a primitive ideal $\mathfrak{a} \lhd \mathcal{O}_K$ with $N(\mathfrak{a}) \leq C_K$.*

This means that, in order to compute the class group we may restrict our attention to primitive ideals. Using Lemma 2.6.22 and Lemma 2.6.23 it is actually rather easy to list all primitive ideals $\mathfrak{a}$ with $N(\mathfrak{a}) \leq C_K$, by writing them as products of primitive prime ideals $\mathfrak{p} \lhd \mathcal{O}_K$ with $N(\mathfrak{p}) \leq C_K$. The structure of the class group can then be determined by solving a finite list of norm equations $Q(x, y) = m$, using Corollary 2.6.20.

Example 2.6.26 We set $d := -47$. Then $\mathcal{O}_K = \mathbb{Z}[\theta]$, with $\theta := (1 + \sqrt{-47})/2$. The minimal polynomial of θ is $f = x^2 - x + 12$, and the norm of an element $\alpha = x + y\theta$ is

$$N_{K/\mathbb{Q}}(\alpha) = Q(x, y) := x^2 - xy + 12y^2.$$

The constant C_K is equal to

$$C_K = \frac{2\sqrt{47}}{\pi} \cong 4,364 < 5.$$

The first step is to find all primitive ideals with norm less than 5. For $p = 2$ we have

$$f \equiv x(x-1) \pmod 2.$$

It follows that

$$(2) = \mathfrak{p}_2 \cdot \bar{\mathfrak{p}}_2, \qquad \text{with} \quad \mathfrak{p}_2 := (2, \theta), \;\; \bar{\mathfrak{p}}_2 := (2, \theta - 1).$$

Similarly, $f \equiv x(x-1) \pmod 3$ and hence

$$(3) = \mathfrak{p}_3 \cdot \bar{\mathfrak{p}}_3, \qquad \text{with} \quad \mathfrak{p}_3 := (3, \theta), \;\; \bar{\mathfrak{p}}_3 := (3, \theta - 1).$$

By Lemma 2.6.22, every primitive ideal $\mathfrak{a}$ with $N(\mathfrak{a}) < 5$ is a product of the four primitive prime ideals $\mathfrak{p}_2, \bar{\mathfrak{p}}_2, \mathfrak{p}_3, \bar{\mathfrak{p}}_3$. For norm reasons, there are exactly eight possibilities. Only one of them, $(2) = \mathfrak{p}_2 \cdot \bar{\mathfrak{p}}_2$, is not primitive, by Lemma 2.6.23. We see that there are exactly 7 distinct primitive ideals $\mathfrak{a}$ with $N(\mathfrak{a}) < 5$, namely

$$(1), \mathfrak{p}_2, \bar{\mathfrak{p}}_2, \mathfrak{p}_3, \bar{\mathfrak{p}}_3, \mathfrak{p}_2^2, \bar{\mathfrak{p}}_2^2. \tag{91}$$

The second step consists in finding all relations between the ideal classes of the 7 ideals listed in (91). Using Corollary 2.6.20 this can be done very systematically, but the procedure would be rather tedious. It is easier to first simplify the situation a bit. Note that the equality $N(\theta) = 12$ together with Lemma 2.6.22 shows that

$$(\theta) = \mathfrak{p}_2^2 \mathfrak{p}_3.$$

This implies the relation $\mathfrak{p}_2^2 \sim \mathfrak{p}_3^{-1} \sim \bar{\mathfrak{p}}_3$. Applying this relation to the ideals in (91) we see that every ideal is equivalent to one of the following 5 ideals

$$(1), \mathfrak{p}_2, \bar{\mathfrak{p}}_2, \mathfrak{p}_3, \bar{\mathfrak{p}}_3. \tag{92}$$

We claim that these 5 ideals are pairwise not equivalent. To prove this claim we assume that $\mathfrak{a}_1 \sim \mathfrak{a}_2$, where $\mathfrak{a}_1, \mathfrak{a}_2$ are distinct ideals listed in (92). Using the relations $\mathfrak{p}_2^{-1} \sim \bar{\mathfrak{p}}_2$ and $\mathfrak{p}_3^{-1} \sim \bar{\mathfrak{p}}_3$ one easily shows that there exists an integral ideal $\mathfrak{b} \sim \mathfrak{a}_1 \cdot \mathfrak{a}_2^{-1} \sim (1)$ such that

$$\mathfrak{b} \in \{\mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_2^2, \mathfrak{p}_3^2\}. \tag{93}$$

The ideals in this list have norm $4, 6, 9$. However, for $\alpha = x + y\theta$ we have

$$N(\alpha) = \big(\frac{2x+y}{2}\big)^2 + \frac{47}{4}y^2,$$

which is either > 9 or equal to x^2. It follows easily that none of the three ideals listed in (93) is principal, contradiction. This proves the claim.

We have shown that the class group Cl_K has exactly 5 elements. Since 5 is a prime number, this implies that Cl_K is cyclic of order 5, and generated by any of its 4 nontrivial elements. For instance,

$$Cl_K = \langle [\mathfrak{p}_2] \rangle \cong \mathbb{Z}/5\mathbb{Z}.$$

One consequence of this result is that the ideals $\mathfrak{p}_2^5$ and $\mathfrak{p}_3^5$ should be principal. Indeed, using Lemma 2.6.22 and Corollary 2.6.20 one shows that

$$\mathfrak{p}_2^5 = (32, \theta - 5) = (\theta - 5), \qquad \mathfrak{p}_3^5 = (243, \theta - 115) = (2\theta + 13).$$

Example 2.6.27 We set $d := -163$. Then $\mathcal{O}_K = \mathbb{Z}[\theta]$, with $\theta := (1 + \sqrt{-163})/2$. The minimal polynomial of θ is $f = x^2 - x + 41$, and the norm of an element $\alpha = x + y\theta$ is

$$N_{K/\mathbb{Q}}(\alpha) = Q(x, y) := x^2 - xy + 41y^2.$$

The constant C_K is equal to

$$C_K = \frac{2\sqrt{163}}{\pi} \cong 8,128 < 9.$$

One checks that for all primes $p < 9$ (i.e. for $p = 2, 3, 5, 7$) the reduction of f modulo p is an irreducible element of $\mathbb{F}_p[x]$. It follows that there are no primitive prime ideals with norm < 9. We conclude that the class group of K is trivial, and hence $\mathcal{O}_K = \mathbb{Z}[\theta]$ is a principal ideal domain.

With this result available, we can now solve the mystery observed at the beginning of the introduction and give a conceptual explanation of the following observation made by Euler in 1772.

Claim 2.6.28 For $a = 0, \ldots, 40$, the integer $f(a) = a^2 - a + 41$ is a prime number.

Proof: Set $m := f(a) = a^2 - a + 41$, for $0 \leq a < 41$. Then $0 < m < 41^2$. Assume that m was not a prime number, and let $p \mid m$ be the smallest prime factor. Then $p < 40$. Moreover, the congruence $f(a) \equiv 0 \pmod{p}$ shows that

$$\mathfrak{p} := (p, \theta - a)$$

is a primitive prime ideal of $\mathcal{O}_K$ with $N(\mathfrak{p}) = p$. On the other hand, $\mathcal{O}_K$ is a principal ideal domain, so there exists $\alpha = x + y\theta \in \mathcal{O}_K$ such that

$$\mathfrak{p} = (\alpha).$$

It follows that

$$p = N(\mathfrak{p}) = N(\alpha) = x^2 + xy + 12y^2 = \big(\frac{2x+y}{2}\big)^2 + \frac{163}{4}y^2.$$

If $y = 0$ then $p = x^2$ which is impossible because p is prime. On the other hand, if $y \neq 0$ then we see that $p > 163/4 > 40$, which is also impossible. We conclude that m is prime. □

The number field K from Example 2.6.27 is the imaginary quadratic number field with the largest discriminant and class number one. More general, we have the following famous theorem, which was already conjectured by Gauss (although his formulation was quite different).

Theorem 2.6.29 (Heegner, Stark) *Let $d < 0$ be a negative, square free integer and $K = \mathbb{Q}[\sqrt{d}]$ the corresponding imaginary quadratic number field.*

(i) *We have $h_K \to \infty$ as $d \to \infty$. In other words, for every constant $C > 0$, there are only finitely many imaginary quadratic number field with class number $h_K \leq C$.*

(ii) *There are precisely 9 imaginary quadratic number fields with class number one. They occur for*

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

The *class number problem* is the problem to determine, for a given number $m \in \mathbb{N}$, all number fields of a certain type (e.g. imaginary quadratic) with class number $h_K = m$.

Exercises

Exercise 2.6.1 Let K be a number field, and assume that $\mathcal{O}_K$ is factorial. Show that the class group Cl_K is trivial. (Hint: use factorization into prime ideals and the fact that all nonzero prime ideals in $\mathcal{O}_K$ are maximal.)

Exercise 2.6.2 Let K be a number field of degree n.

(i) We define the *norm* of a fractional ideal $\mathfrak{a} \lhd K$ by the formula

$$N(\mathfrak{a}) := m^{-n} \cdot N(m \cdot \mathfrak{a}),$$

where $m \in \mathbb{N}$ is chosen such that $m \cdot \mathfrak{a} \lhd \mathcal{O}_K$. Show that the norm defines a group homomorphism

$$N : J_K \to \mathbb{Q}^\times.$$

(ii) Show that for any nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ there exists a unique nonzero ideal $\mathfrak{a}^* \lhd \mathcal{O}_K$ such that

$$\mathfrak{a} \cdot \mathfrak{a}^* = (N(\mathfrak{a})).$$

In particular, $[\mathfrak{a}] \cdot [\mathfrak{a}^*] = [(1)]$ in Cl_K.

Exercise 2.6.3 Let $K = \mathbb{Q}[\sqrt{-30}]$. Determine the class number h_K and the structure of the class group Cl_K.

2.7 The unit group

We end this chapter with a study of the unit group of a number field K. Recall that the unit group $\mathcal{O}_K^\times$ is the multiplicative group of elements $\alpha \in \mathcal{O}_K$ such that $\alpha \neq 0$ and $\alpha^{-1} \in \mathcal{O}_K$.

Proposition 2.7.1 *We have*

$$\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(\alpha) = \pm 1\}.$$

Proof: Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the distinct embeddings of K into $\mathbb{C}$. Without loss of generality we may assume that $K \subset \mathbb{C}$ and that σ_1 is the identity on K. By Proposition 2.3.11 (ii) we have

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in \mathbb{Z}, \tag{94}$$

for all $\alpha \in \mathcal{O}_K$. Now suppose that $\alpha \in \mathcal{O}_K^\times$ is a unit. Then the multiplicativity of the norm shows that

$$1 = N_{K/\mathbb{Q}}(1) = N_{K/\mathbb{Q}}(\alpha) \cdot N_{K/\mathbb{Q}}(\alpha^{-1}),$$

and both factors on the right hand side are integers. It follows that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Conversely, assume that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Then (94) shows that

$$\alpha^{-1} = \sigma_1(\alpha^{-1}) = \pm\sigma_2(\alpha) \cdot \ldots \cdot \sigma_n(\alpha)$$

is a product of algebraic integers. More precisely, the $\sigma_i(\alpha) \in \mathcal{O}_L$ are integers of the number field $L := \mathbb{Q}[\sigma_1(\alpha), \ldots, \sigma_n(\alpha)]$ and therefore $\alpha^{-1} \in \mathcal{O}_L$ as well. We conclude that

$$\alpha^{-1} \in \mathcal{O}_L \cap K = \mathcal{O}_K,$$

and hence that $\alpha \in \mathcal{O}_K^\times$ is a unit. $\square$

We let

$$\mu(K) := \{\zeta \in K \mid \exists k \in \mathbb{N} : \zeta^k = 1\}$$

be the set of roots of unity contained in K. It is clear that $\mu(K)$ is a subgroup of $K^\times$. Moreover, $\mu(K) \subset \mathcal{O}_K$ because every root of unity $\zeta \in \mu(K)$ satisfies an integral relation of the form $\zeta^k - 1 = 0$. It follows immediately that $\mu(K) \subset \mathcal{O}_K^\times$ is a subgroup of the unit group. In fact,

$$\mu(K) = (\mathcal{O}_K^\times)_{\mathrm{tor}}$$

is the *torsion subgroup* of $\mathcal{O}_K^\times$, i.e. the subgroup consisting of all elements of $\mathcal{O}_K^\times$ which have finite order. Therefore, the quotient group

$$E_K := \mathcal{O}_K^\times / \mu(K)$$

is *torsion free*, i.e. it has no element of finite order except the unit.

Example 2.7.2 Let K be an imaginary quadratic number field. We have seen in ?? that the norm equation $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ for $\alpha \in \mathcal{O}_K$ is equivalent to a quadratic Diophantine equation of the form

$$Q(x, y) = 1, \qquad x, y \in \mathbb{Z},$$

where $Q(x, y)$ is a positive definite quadratic form. Such an equation has at most finitely many solutions. It follows that the unit group $\mathcal{O}_K^\times$ is finite. This means that $\mu(K) = \mathcal{O}_K$ and hence $E_K = \{1\}$ is trivial.

We have also seen that $\mu(K) = \{\pm 1\}$ is as small as possible except in two cases, namely for $K = \mathbb{Q}[i]$ (where $\mu(K)$ is a cyclic group of order 4) and for $K = \mathbb{Q}[\sqrt{-3}]$ (where $\mu(K)$ is a cyclic group of order 6).

Theorem 2.7.3 (Dirichlet's Unit Theorem) *Let K be a number field of type (r, s).*

(i) *The group $\mu(K)$ is finite and cyclic.*

(ii) *$E_K = \mathcal{O}_K^\times / \mu(K)$ is a free abelian group of rank $r + s - 1$.*

The statement of the theorem may be rephrased as follows. Let $t := r+s-1$. Then there exist units $\epsilon_1, \ldots, \epsilon_t \in \mathcal{O}_K^\times$ such that every unit $\alpha \in \mathcal{O}_K^\times$ has a unique representation of the form

$$\alpha = \zeta \cdot \epsilon_1^{k_1} \cdot \ldots \cdot \epsilon_t^{k_t},$$

with $\zeta \in \mu(K)$ and $k_i \in \mathbb{Z}$. The tupel (ϵ_i) is called a *fundamental system of units*.

Remark 2.7.4 Note that the fundamental system of units (ϵ_i) is not unique. On the one hand, we may replace ϵ_i with $\zeta_i\epsilon_i$, where $\zeta_i \in \mu(K)$ is an arbitrary root of unity. On the other hand, if $A = (a_{i,j}) \in \mathrm{GL}_t(\mathbb{Z})$ is a unimodular matrix of dimension t then the system (ϵ_i'), where

$$\epsilon_i' := \prod_{j=1}^{t} \epsilon_j^{a_{i,j}},$$

is again a fundamental system of units.

Before we give the proof of Theorem 2.7.3 we have a closer look at the special case of real quadratic fields.

The unit group of real quadratic fields and the Pell equation

Let $d > 0$ be a positive and square free integer and let $K := \mathbb{Q}[\sqrt{d}]$. For simplicity we assume that $d \equiv 2, 3 \pmod 4$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, and for $\alpha = x + y\sqrt{d} \in \mathcal{O}_K$ we have

$$N_{K/\mathbb{Q}}(\alpha) = x^2 - dy^2.$$

Therefore, the units of the ring $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ correspond bijectively to the solitions of the Diophantine equation

$$x^2 - dy^2 \pm 1, \qquad x, y \in \mathbb{Z}. \tag{95}$$

This equation is traditionally called *Pell's equation*[7]

Equation (95) has two trivial solutions, $(\pm 1, 0)$, corresponding to the roots of unity $\pm 1 \in \mathcal{O}_K$. In fact, $\mu(K) = \{\pm 1\}$ is a cyclic group of order 2 simply because the field K can be embedded into the real numbers.

By Theorem 2.7.3 there exists a *fundamental unit* $\epsilon_1 \in \mathcal{O}_K^\times$ such that every other unit $\epsilon \in \mathcal{O}_K^\times$ can be written uniquely in the form

$$\epsilon = \pm\epsilon_1^k,$$

for a uniquely determined integer $k \in \mathbb{Z}$. It follows in particular that Pell's equation has infintely many solutions.

By Remark 2.7.4 the fundamental unit ϵ_1 is not unique: there are exactly four distinct choices, namely $\pm\epsilon_1, \pm\epsilon_1^{-1}$. Replacing ϵ_1 by one of these, we may assume that $\epsilon_1 > 1$, and then ϵ_1 is uniquely determined. In fact, we will see in a moment that

$$\epsilon_1 = \min\{\epsilon \in \mathcal{O}_K^\times \mid \epsilon > 1\}. \tag{96}$$

The unit determined by (96) is called *the fundamental unit* of $K = \mathbb{Q}[\sqrt{d}]$. If we write $\epsilon_1 = x_1 + y_1\sqrt{d}$, then (x_1, y_1) is a solution to Pell's equation called the *fundamental solution*.

[7]Named after the english mathematician John Pell (1611-1685). However, the attribution of Pell's name with Equation (95) is due to a confusion of Pell with Lord Brouncker (1620-1684). Historically more accurate would be the name *Brahmagupta's equation* (after the indian mathematician and astronomer Brahmagupta (597-668). See the Wikipedia entry for *Pell's equation*

Example 2.7.5 Let $d = 2$. It is easy to find several small nontrivial solutions to the Pell equation $x^2 - 2y^2 = \pm 1$. For instance $(x, y) = (1, 1)$ is the nontrivial solution with smallest positive entries. Let $\epsilon_1 := 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ be the corresponding unit. It is easy to see that (96) holds, so ϵ_1 is the fundamental solution. It follows that we can enumerate *all* solutions by computing powers of ϵ_1. In particular, if we take positive powers of ϵ_1 then we obtain exactly all solutions (x, y) with $x, y > 0$. For instance,

$$\epsilon_1 = 1 + \sqrt{2},\ \epsilon_1^2 = 3 + 2\sqrt{2},\ \epsilon_1^3 = 7 + 5\sqrt{2},\ \epsilon_1^4 = 17 + 12\sqrt{2}$$

gives the first 4 solutions

$$(x, y) = (1, 1), (3, 2), (7, 5), (17, 12).$$

Example 2.7.6 Even for relatively small values of d the fundamental solution $\epsilon_1 = x_1 + y_1\sqrt{d}$ can be surprisingly large. Here is a small (and rather randomly chosen) list of such cases:

d	x_1	y_1
19	170	39
31	1520	273
46	24335	3588
103	227528	22419

It can be shown that there is an increasing sequence of values for d such that the absolute values of x_1 and y_1 grow exponentially with d.

Remark 2.7.7 Before trying to work through the proof of Theorem 2.7.3 in the general case given below, it is instructive to study a proof in the special case of real quadratic number fields. This can be done for instance by reading [5], Chapter 17, §5 and solving Exercise 2.7.2.

The proof of Dirichlet's Unit Theorem

Advice: The following proof is rather long and heavy with notation. At first reading it may be helpful to mentally translate everything into the special case of a real quadratic number field which we already looked at in the previous section (i.e. to set $n := 2$, $r := 2$ and $s := 0$). Examples 97 and 98 and the pictures therein are meant to support this point of view. See also [1], Chapter 11, §11.

Let $K/\mathbb{Q}$ be a number field of degree n and type (r, s). Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the distinct embeddings of K into $\mathbb{C}$. As usual, we assume that $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ are real and that $\bar{\sigma}_{r+2i-1} = \sigma_{r+2i}$ for $i = 1, \ldots, s$. Let

$$K_{\mathbb{R}} := \{(z_i) \in \mathbb{C}^n \mid z_1, \ldots, z_r \in \mathbb{R},\ \bar{z}_{r+2i-1} = z_{r+2i} \text{ for } i = 1, \ldots, s\}$$

be the Minkowski space of K and $j : K \hookrightarrow K_{\mathbb{R}}$, $j(\alpha) = (\sigma_i(\alpha))$, the canonical embedding (Definition 2.4.24). Recall that $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ is a complete lattice with covolume

$$\mathrm{vol}(j(\mathcal{O}_K)) = \sqrt{|d_K|}$$

(Corollary 2.4.26). In particular, $j(\mathcal{O}_K)$ is a discrete subset of $K_{\mathbb{R}}$. This fact will be used several times in the proof of Theorem 2.7.3.

We define

$$K_{\mathbb{R}}^{\times} := \{(z_i) \in K_{\mathbb{R}} \mid z_i \neq 0 \ \forall i\}, \qquad S := \{(z_i) \in K_{\mathbb{R}}^{\times} \mid \prod_i |z_i| = 1\}.$$

Clearly, $K_{\mathbb{R}}^{\times}$ is an abelian group with respect to componentwise multiplication and $S \subset K_{\mathbb{R}}^{\times}$ is a subgroup. Furthermore, the restriction of j to $K^{\times}$ is an injective group homomorphism $j : K^{\times} \hookrightarrow K_{\mathbb{R}}^{\times}$. It follows from Proposition 2.7.1 (i) that

$$j(\mathcal{O}_K^{\times}) = j(\mathcal{O}_K) \cap S \tag{97}$$

In fact, for $\alpha \in K$ we have $j(\alpha) \in S$ if and only if $|N_{K/\mathbb{Q}}(\alpha)| = 1$, by (94).

Example 2.7.8 Let us try to visualize the subgroup $S \subset K_{\mathbb{R}}^{\times}$ and the lattice $j(\mathcal{O}_K)$ in the special case $r = 2$, $s = 0$, i.e. in the case of a real quadratic number field (compare with Example 2.4.28). We can write $K = \mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$, where $d > 0$ is a positive, square free integer. Then $K_{\mathbb{R}} = \mathbb{R}^2$ and for $\alpha = x + y\sqrt{d}$ we have

$$j(\alpha) = (\alpha, \alpha') = (x + y\sqrt{d}, x - y\sqrt{d}).$$

The group $K_{\mathbb{R}}^{\times}$ is the complement of the two coordinate axis, and the subgroup $S \subset K_{\mathbb{R}}^{\times}$ is the union of two hyperbolas,

$$S = \{(z_1, z_2) \in \mathbb{R}^2 \mid z_1 z_2 = \pm 1\}.$$

By (97), the unit group, considered as subgroup of $K_{\mathbb{R}}^{\times}$, is the intersection of the lattice $\mathcal{O}_K$ with S. See Figure 4 for the case $K = \mathbb{Q}[\sqrt{2}]$. In this picture we can see 6 units of $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, namely

$$\epsilon = \pm 1, \pm(1 + \sqrt{2}), \pm(1 - \sqrt{2}).$$

These are the points of intersection of the lattice $\langle j(1), j(\sqrt{2})\rangle_{\mathbb{Z}} \subset \mathbb{R}^2$ with the double hyperbola S, which occur in the range of the coordinates visible in the picture. Theorem 2.7.3 says that there are in fact infinitely many such intersection points, corresponding to the units

$$\epsilon = \pm(1 + \sqrt{2})^k, \qquad k \in \mathbb{Z}.$$

See Example 2.7.5.

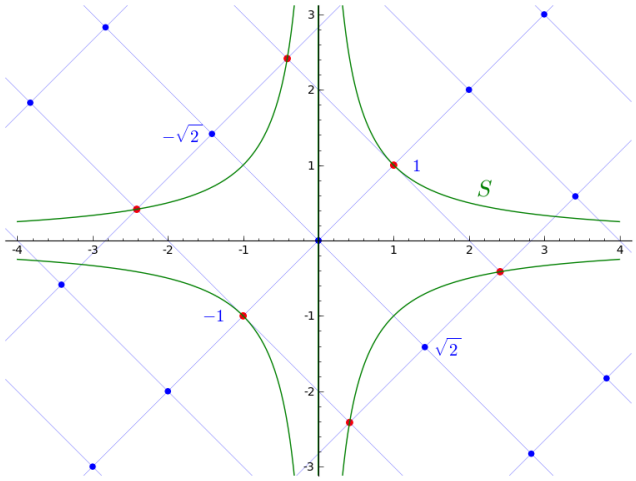


Figure 4: Looking for units in $\mathbb{Z}[\sqrt{2}]$

The main new ingredient needed for the proof of Theorem 2.7.3 is the *logarithmic space*

$$L := \{(x_i) \in \mathbb{R}^n \mid x_{r+2i-1} = x_{r+2i} \text{ for } i = 1, \ldots, s\}$$

and the *logarithmic map*

$$l : K_{\mathbb{R}}^{\times} \to L, \qquad (z_i) \mapsto (\log(|z_i|)).$$

Note that L is a real vector space of dimension $r + s$, and that l is a group homomorphism (turning multiplication into addition). Note also that the image of $S \subset K_{\mathbb{R}}^{\times}$ under the logarithmic map l lies in the linear subspace

$$H := \{(x_i) \in L \mid \sum_i x_i = 0\}.$$

We can summarize the notation introduced so far by the following commutative diagram of abelian groups:

$$\begin{array}{ccccc} \mathcal{O}_K^{\times} & \longrightarrow & S & \longrightarrow & H \\ \downarrow & & \downarrow & & \downarrow \\ K^{\times} & \xrightarrow{j} & K_{\mathbb{R}}^{\times} & \xrightarrow{l} & L \end{array} \tag{98}$$

(the vertical maps are simply the natural inclusions). The most important map here is the composition of the two top horizontal maps,

$$\lambda := l \circ j|_{\mathcal{O}_K^{\times}} : \mathcal{O}_K^{\times} \to H.$$

This is a homomorphism of abelian groups. Note also that the second horizontal map $l|_S : S \to H$ is surjective because the logarithm $\log : \mathbb{R}_{>0} \to \mathbb{R}$ is surjective.

The following lemma proves Part (i) of Theorem 2.7.3.

Lemma 2.7.9 *We have* $\ker(\lambda) = \mu(K)$*, and this group is finite and cyclic.*

Proof: Let $\zeta \in \mu(K)$ be a root of unity. Then $\zeta_i := \sigma_i(\zeta) \in \mathbb{C}$ is also a root of unity, and therefore $|\zeta_i| = 1$, for $i = 1, \ldots, n$. It follows that $\lambda(\zeta) = (\log(|\zeta_i|)) = 0$, i.e. $\zeta \in \ker(\lambda)$. Conversely, let $\alpha \in \ker(\lambda)$. This means that $|\sigma_i(\alpha)| = 1$ for all i. We see that $j(\ker(\lambda))$ is a subset of the compact subgroup

$$(S^1)^n := \{(z_i) \in K_{\mathbb{R}}^{\times} \mid |z_i| = 1 \ \forall i\}.$$

But $j(\ker(\lambda))$ is also a subset of the discrete subset $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$. It follows that $\ker(\lambda)$ is a finite group. But every element of a finite group has finite order, and therefore $\ker(\lambda) \subset \mu(K)$. We have shown that $\ker(\lambda) = \mu(K)$ and that this group is finite. By [1], Chapter 13, Proposition 6.18, every finite subgroup of $K^{\times}$ is cyclic. This completes the proof of the lemma. □

Set

$$\Lambda := \lambda(\mathcal{O}_K^{\times}) \subset H.$$

this is a subgroup of H which, by Lemma 2.7.9 and the first isomorphism theorem, is isomorphic to the group $E_K = \mathcal{O}_K^{\times}/\mu(K)$. So in order to prove Part (ii) of Theorem 2.7.3 we have to show that Λ is a free abelian group of rank $r + s - 1$. In fact we will show more, namely that Λ is a full lattice inside the real vector space H (Definition 2.4.21). Since $\dim_{\mathbb{R}} H = r + s - 1$, this implies that Λ (and hence E_K as well) is a free abelian group of rank $r + s - 1$.

Example 2.7.10 We return to the special case of a real quadratic number field considered in Example 2.7.8. Then $L = \mathbb{R}^2$ and the logarithmic map is

$$l : \mathbb{R}^2 \to \mathbb{R}^2, \qquad (z_1, z_2) \mapsto (\log(|z_1|), \log(|z_2|)).$$

The linear subspace $H \subset L$ is the plane given by the equation $z_1 + z_2 = 0$. In Figure 5 we see the position of $H \subset L$ and, for $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, the lattice $\Lambda = \lambda(\mathcal{O}_K^{\times}) = \langle \gamma_1 \rangle_{\mathbb{Z}}$, with generator

$$\gamma_1 := \lambda(1 + \sqrt{2}) \sim (0.881, -0.881).$$

By Proposition 2.4.22 (i) the following lemma proves that $\Lambda \subset H$ is a lattice (but not yet that it is complete).

Lemma 2.7.11 *The subgroup* $\Lambda \subset H$ *is a discrete subgroup.*

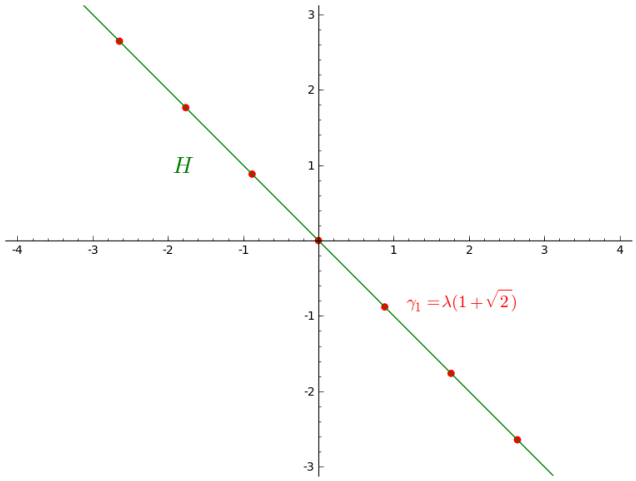


Figure 5: Looking for the units of $\mathbb{Z}[\sqrt{2}]$ in logarithmic space

Proof: For the proof we may also consider Λ as a subgroup of the vector space L containing H. The subset

$$U := \{(x_i) \in L \mid |x_i| \leq 1 \ \forall i \} \subset L$$

is a neighborhood of $0 \in L$. Its inverse image via the logarithmic map is

$$W := l^{-1}(U) = \{(z_i) \in K_{\mathbb{R}} \mid e^{-1} \leq |z_i| \leq e\}.$$

This is a compact subset of $K_{\mathbb{R}}$. Since $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ is a lattice and hence a discrete subset, it follows that $W \cap j(\mathcal{O}_K)$ is a finite set. We conclude that $U \cap \Lambda$ is a finite set as well. This shows that $\Lambda \subset L$ is a discrete subgroup. $\square$

To finish the proof of Theorem 2.7.3 we have to show that the lattice $\Lambda \subset H$ is complete. This is the hardest part of the proof; it consists in showing that there exists as many units as possible. Indeed, the fact that $\Lambda \subset H$ is a lattice shows that $E_K = \mathcal{O}_K/\mu(K)$ is a free abelian group of rank $\leq r + s - 1$. Completeness of the lattice Λ means that the previous inequality is in fact an equality.

The general idea of the proof is the following. Our goal is produce a large supply of units $\epsilon \in \mathcal{O}_K$. Let $C > 0$ be some positive constant. Suppose we have a method to produce an infinite set of elements $\alpha \in \mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(\alpha)| < C$. Then the corresponding principal ideals $(\alpha) \lhd \mathcal{O}_K$ satisfy $N((\alpha)) < C$. By Exercise 2.5.7 there are only finite many ideals with this property. It follows that there exist infinitely many pairs of distinct nonzero elements $\alpha_1, \alpha_2 \in \mathcal{O}_K$ which generate the same principal ideal, i.e. $(\alpha_1) = (\alpha_2)$. This means that $\epsilon := \alpha_1/\alpha_2 \in \mathcal{O}_K^{\times}$ is a unit.

To make this idea work we use Minkowski's theorem (Theorem 2.6.16) in a similar way as we did in the proof of the finiteness of the class number (see §2.6,

in particular Lemma 2.6.17). We choose positive constants $c_1, \dots, c_n > 0$ such that

$$C := \prod_i c_i > C_K = \Big(\frac{2}{\pi}\Big)^s \sqrt{|d_K|}. \tag{99}$$

Recall that the subgroup $S \subset K_{\mathbb{R}}^{\times}$ contains the elements $y = (y_i)$ such that $\prod_i |y_i| = 1$.

Lemma 2.7.12 *For all $y = (y_i) \in S$ there exists an element $\alpha \in \mathcal{O}_K$ such that $\alpha \neq 0$ and*

$$|\sigma_i(\alpha)| < |y_i| c_i,$$

for $i = 1, \dots, n$. In particular, we have

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_i |\sigma_i(\alpha)| < C.$$

Proof: Let

$$X := \{(z_i) \in K_{\mathbb{R}} \mid |z_i| < c_i \ \forall i\}. \tag{100}$$

This is a convex and centrally symmetric subset of $K_{\mathbb{R}}$ with

$$\mathrm{vol}(X) = 2^{r+s}\pi^s C > 2^n \sqrt{|d_K|} = 2^n \mathrm{vol}(j(\mathcal{O}_K)),$$

see (82). So Minkowski's theorem applies to X. More generally, for any $y = (y_i) \in S$ we consider the set

$$y \cdot X = \{(z_i) \in K_{\mathbb{R}} \mid |z_i| < |y_i| c_i \ \forall i\}.$$

It is of the same shape as X, and since $\prod_i |y_i| c_i = C$ we have $\mathrm{vol}(y \cdot X) = \mathrm{vol}(X)$. As in the proof of Lemma 2.6.17 one shows that there exists $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, such that $j(\alpha) \in y \cdot X$. This means that $|\sigma_i(\alpha)| < |y_i| c_i$ for all i. □

By Exercise 2.5.7 there are at most finitely many ideals $\mathfrak{a} \lhd \mathcal{O}_K$ with $N(\mathfrak{a}) < C$. Let $(\alpha_1), \dots, (\alpha_N) \lhd \mathcal{O}_K$ be a complete list of all nonzero principal ideals with this property. Then $\alpha_j \neq 0$ and

$$|N_{K/\mathbb{Q}}(\alpha_j)| < C, \tag{101}$$

for $j = 1, \dots, N$, by Proposition 2.5.8. Moreover, for any $\alpha \in \mathcal{O}_K \backslash \{0\}$ with $|N_{K/\mathbb{Q}}(\alpha)| < C$ there exists an index j such that $(\alpha) = (\alpha_j)$.

Lemma 2.7.13 *Set*

$$T := S \cap \Big(\bigcup_{j=1}^{N} j(\alpha_j^{-1}) \cdot X \Big).$$

Then T is a bounded subset of S such that

$$S = \bigcup_{\epsilon \in \mathcal{O}_K^{\times}} j(\epsilon) \cdot T. \tag{102}$$

Proof: By definition, T is a finite union of bounded subsets of S and therefore itself bounded. Also, for every unit $\epsilon \in \mathcal{O}_K^\times$ we have $j(\epsilon) \in S$ and hence $j(\epsilon) \cdot T \subset S$. To prove the inclusion $\subset$ in (102) we fix an element $y = (y_i) \in S$. By Lemma 2.7.12 there exists $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, such that $|\sigma_i(\alpha)| < y_i c_i$ for all i. This is equivalent to

$$j(\alpha) \in y \cdot X, \tag{103}$$

and it implies

$$|N_{K/\mathbb{Q}}(\alpha)| < C. \tag{104}$$

Therefore, $(\alpha) = (\alpha_j)$ for some index $j \in \{1, \ldots, N\}$. It follows that

$$\alpha_j = \epsilon\alpha, \qquad \epsilon \in \mathcal{O}_K^\times. \tag{105}$$

By (103) we can write $j(\alpha) = y \cdot x$, with $x \in X$. Using (105) we conclude that

$$y = j(\alpha^{-1}) \cdot x = j(\epsilon\alpha_j^{-1}) \cdot x = j(\epsilon) \cdot j(\alpha_j^{-1}) \cdot x \in j(\epsilon) \cdot T.$$

This proves (102) and completes the proof of the lemma. □

We can now finish the proof of Theorem 2.7.3. We have already shown that $\Lambda \subset H$ is a lattice. We assume that Λ is not a complete lattice. This means that Λ is contained in a proper linear subspace $H' \subsetneq H$.

Consider the bounded subset $T \subset S$ from Lemma 2.7.13. Its image $l(T)$ under the logarithmic map is a bounded subset of H. Since $l|_S : S \to H$ is surjective, (102) shows that

$$H = l(S) = \bigcup_{\gamma \in \Lambda} \big(\gamma + l(T)\big). \tag{106}$$

Let $v \in (H')^\perp$ be a vector in H which is orthogonal to H' and such that $||v|| > ||w||$ for all $w \in l(T)$. Then we also have

$$||v + \gamma|| \geq ||v|| > ||w|| \tag{107}$$

for all $\gamma \in \Lambda$ and $w \in l(T)$ (we have used $v \perp \gamma$). This shows that $v + \gamma \notin l(T)$, for all $\gamma \in \Lambda$, contradicting (107). We conclude that $\Lambda \subset H$ is a complete lattice, and Theorem 2.7.3 is proved. □

Exercises

Exercise 2.7.1 Compute the fundamental unit $\epsilon_1 = x_1 + y_1\sqrt{d}$ of $K = \mathbb{Q}[\sqrt{d}]$, for $d = 3, 6, 7, 10, 11$.

Exercise 2.7.2 Let $d > 0$ be a squarefree integer, $d \equiv 2, 3 \pmod 4$, and let $K := \mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$. Assume that the Pell equation

$$x^2 - dy^2 = \pm 1$$

has at least one nontrivial solution. Under this assumption, reprove Theorem 2.7.3 for K, via the following steps.

(i) Show that the Pell equation has infinitely many solutions.

(ii) Show that the minimum

$$\epsilon_1 := \min\{\epsilon \in \mathcal{O}_K^\times \mid \epsilon > 1\}$$

exists.

(iii) Show that every unit $\epsilon \in \mathcal{O}_K^\times$ with $\epsilon > 1$ is of the form $\epsilon = \epsilon_1^k$, for a unique positive integer $k \in \mathbb{N}$.

3 Cyclotomic fields

3.1 Roots of unity

For $n \in \mathbb{N}$ we let $\mathbb{\mu}_n \subset \mathbb{C}$ denote the group of nth roots of unity,

$$\mathbb{\mu}_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}.$$

Clearly, $\mathbb{\mu}_n$ is a cyclic group of order n, generated by $\zeta_n := e^{2\pi i/n} = \cos(2\pi/n) + i \cdot \sin(2\pi/n)$. Note that every element $\zeta \in \mathbb{\mu}_n$ is an algebraic integer, because it satifies the integral equation $\zeta^n - 1 = 0$.

Definition 3.1.1 The number field $K_n := \mathbb{Q}[\zeta_n]$ is called the nth *cyclotomic field*.

Our first goal is to find the minimal polynomial of ζ_n and thereby compute the degree $[K_n : \mathbb{Q}]$. An element $\zeta \in \mathbb{\mu}_n$ is called a *primitive nth root of unity* if the order of ζ in the group $\mathbb{\mu}_n$ is equal to n. This means that $\zeta^d \neq 1$ for all proper divisors $d \mid n$. The corresponding subset of $\mathbb{\mu}_n$ is written as $\mathbb{\mu}_n^\times$. An elementary argument shows that for $a \in \mathbb{Z}$ the element $\zeta_n^a \in \mathbb{\mu}_n$ is a primitive root of unity if and only if $\mathrm{ggT}(a, n) = 1$. Hence we obtain a bijection

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathbb{\mu}_n^\times, \qquad a \mapsto \zeta_n^a. \tag{108}$$

In particular, we have

$$|\mathbb{\mu}_n^\times| = \phi(n),$$

where $\phi(n)$ denotes the nth value of Euler's ϕ-function.

The *nth cycloctomic polynomial* is defined as

$$\Phi_n := \prod_{\zeta \in \mathbb{\mu}_n^\times} (x - \zeta) \in \mathbb{C}[x].$$

Note that Φ_n is a monic polynomial of degree $\phi(n)$.

Lemma 3.1.2 (i) *We have*

$$x^n - 1 = \prod_{d \mid n} \Phi_d.$$

(ii) *The polynomial Φ_n has integral coefficients, i.e. $\Phi_n \in \mathbb{Z}[x]$.*

(iii) *The polynomial Φ_n is irreducible over $\mathbb{Q}$.*

Proof: The first statement follows from the decomposition

$$x^n - 1 = \prod_{\zeta \in \mathbb{\mu}_n} (x - \zeta)$$

and the fact that every element $\zeta \in \mu_n$ lies in $\mu_d^\times$, for a unique divisor $d \mid n$. The second statement follows from the first by induction, as follows. Clearly, $\Phi_1 = x - 1$, so the claim is true for $n = 1$. For $n > 1$, we may assume that $\Phi_d \in \mathbb{Z}[x]$ for all proper divisors $d \mid n$. Then (i) shows that

$$\Phi_n = \frac{x^n - 1}{\prod_{d|n, d<n} \Phi_d}. \tag{109}$$

The denominator on the right hand side of (109) is a monic integral polynomial by the induction hypothesis. Since the left hand side (109) is a poylnomial (a priori with complex coefficients), the polynomial division algorithm shows that $\Phi_n \in \mathbb{Z}[x]$. This proves (ii).

We now prove (iii). Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of ζ_n. Then $f \mid \Phi_n$ in $\mathbb{Z}[x]$, i.e. $\Phi_n = f \cdot g$ for some monic polynomial $g \in \mathbb{Z}[x]$. To prove $f = \Phi_n$ it suffices to show that $f(\zeta_n^a) = 0$ for all $a \in \mathbb{Z}$ which is prime to n. More generally, for a prime to p we let P_a denote the statement

$$\forall \zeta \in \mu_n^\times : \ \Big(f(\zeta) = 0 \ \Rightarrow \ f(\zeta^a) = 0 \Big).$$

Then P_a and P_b together imply $P_{a \cdot b}$. Therefore, it suffices to prove P_p for all prime numbers p which are prime to n.

Let us fix p as above, and let $\bar{\Phi}_n, \bar{f}, \bar{g} \in \mathbb{F}_p[x]$ denote the reduction of Φ_n, f, g. We assume that there exists $\zeta \in \mu_n^\times$ such that $f(\zeta) = 0$ and $f(\zeta^p) \neq 0$. Then $g(\zeta^p) = 0$. Since f is the minimal polynomial of ζ we conclude that $f \mid g(x^p)$. This implies

$$\bar{f} \mid \bar{g}(x^p) = \bar{g}^p. \tag{110}$$

Let $\bar{h}$ be an irreducible factor of $\bar{f}$. Then (110) shows that $\bar{h}^2 \mid \bar{f} \cdot \bar{g} = \bar{\Phi}_n$, i.e. $\bar{\Phi}_n$ is not separable. On the other hand, using $p \nmid n$ we see that

$$\mathrm{ggT}(\bar{\Phi}_n, \bar{\Phi}_n') = \mathrm{ggT}(x^n - 1, \bar{n} x^{n-1}) = 1,$$

i.e. $\bar{\Phi}_n$ is separable. The contradiction finishes the proof of the lemma. □

Remark 3.1.3 The proof of Part (iii) of the lemma is a bit mysterious. We will give a more conceptual proof later. For both proofs (and for significant parts of algebraic number theory), the heart of the matter is the existence of the *Frobenius endomorphism*: if R is a commutative ring of characteristic $p > 0$ (e.g. $R = \mathbb{F}_p[x]$) then the map

$$\varphi_p : R \to R, \qquad a \mapsto a^p,$$

is a ring homomorphism. In particular, $(a + b)^p = a^p + b^p$.[8]

Corollary 3.1.4 *The cyclotomic polynomial Φ_n is the minimal polynomial of ζ_n (in fact, of every element of $\mu_n^\times$). We have*

$$[K_n : \mathbb{Q}] = \phi(n).$$

[8] This formula is also called *freshman's dream* .

Example 3.1.5 (i) Using (109) we can compute Φ_n for small values of n:

$$\Phi_1 = x - 1, \qquad \Phi_2 = x + 1,$$
$$\Phi_3 = x^2 + x + 1, \qquad \Phi_4 = x^2 + 1,$$
$$\Phi_5 = x^4 + x^3 + x^2 + x^2 + x + 1, \qquad \Phi_6 = x^2 - x + 1.$$

(ii) If p is a prime number, then

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1.$$

(iii) More generally, if p is prime and $k \geq 1$ then

$$\Phi_{p^k} = \frac{x^{p^k} - 1}{x^{k-1} - 1} = x^{(p-1)p^{k-1}} + \ldots + x^{p^{k-1}} + 1 = \Phi_p(x^{p^{k-1}}).$$

See Exercise 3.1.1.

The Galois group of $\mathbb{Q}[\zeta_n]/\mathbb{Q}$

We briefly recall the definition of a Galois extension and its most useful characterization. See [1] for more details.

Definition 3.1.6 Let L/K be a finite field extension. An *automorphism* of L/K is a field automorphism $\sigma : L \xrightarrow{\sim} L$ which fixes every element of K. The group of all automorphisms of L/K is written as $\mathrm{Aut}(L/K)$. The extension L/K is called a *Galois extension* if

$$|\mathrm{Aut}(L/K)| = [L : K].$$

If this is the case, then $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$ is called the *Galois group* of L/K.

Theorem 3.1.7 *A finite field extension L/K is a Galois extension if and only if L/K is the splitting field of a separable polynomial $f \in K[x]$.*

Theorem 3.1.8 (i) *The extension $K_n/\mathbb{Q}$ is a Galois extension.*

(ii) *For $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ we have*

$$\sigma(\zeta_n) = \zeta_n^a,$$

where $a \in \mathbb{Z}$ is prime to n. The resulting map

$$\mathrm{Gal}(K_n/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times, \qquad \sigma \mapsto a + n \cdot \mathbb{Z},$$

is an isomorphism of groups.

Proof: We have already observed that $K_n/\mathbb{Q}$ is the splitting field of the separable polynomial $x^n - 1$. By Theorem 3.1.7, $K_n/\mathbb{Q}$ is a Galois extension, proving (i).

Let $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$. Since σ is a field automorphism, it acts on the subgroup $\mu_n \subset K_n^\times$ as a group automorphism. But $\mu_n = \langle \zeta_n \rangle$ is a cyclic group of order n, and hence any automorphism is of the form $\zeta \mapsto \zeta^a$, for a unique $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. It follows that the map $\sigma \mapsto a$ is an injective group homomorphism from $\mathrm{Gal}(L/K)$ to $(\mathbb{Z}/n\mathbb{Z})^\times$. It is also surjective, because by Corollary 3.1.4 and the fact that L/K is Galois we have

$$|\mathrm{Gal}(L/K)| = [L_K] = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

This completes the proof of the theorem. □

Example 3.1.9 Let $n = 5$. The minimal polynomial of ζ_5 is $\Phi_5 = x^4 + x^3 + x^2 + x + 1$ (Example 3.1.5). In particular, we have the identity

$$1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0,$$

whose truth can also be seen geometrically in Figure ??. It follows from Theorem 3.1.8 that $\mathbb{Q}[\zeta_5]/\mathbb{Q}$ is a Galois extension whose Galois group is cyclic of order 4:

$$\mathrm{Gal}(\mathbb{Q}[\zeta_5]/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}.$$

Let $H \subset \mathrm{Gal}(\mathbb{Q}[\zeta_5]/\mathbb{Q})$ be the unique subgroup of order 2. Clearly, H is generated by the element σ_{-1}. Since $\sigma_{-1}(\zeta) = \zeta^{-1} = \bar{\zeta}$ for all $\zeta \in \mu_5$, σ_{-1} is equal to complex conjugation, restricted to the subfield $\mathbb{Q}[\zeta_5] \subset \mathbb{C}$.

By the Main Theorem of Galois Theory, the fixed field $K := \mathbb{Q}[\zeta_5]^H$ is a quadratic number field. To describe K explicitly, we set

$$\alpha := \zeta_5 + \zeta_5^4, \quad \alpha' := \zeta_5^2 + \zeta_5^3.$$

Almost by definition,

$$\sigma_{-1}(\alpha) = \alpha, \quad \sigma_{-1}(\alpha') = \alpha'.$$

It follows that $\alpha, \alpha' \in K$. Note that

$$\alpha = 2\cos(2\pi/5), \qquad \alpha' = 2\cos(4\pi/5).$$

Note also that

$$\Phi_5 = (x - \zeta_5)(x - \zeta_5^4)(x - \zeta_5^2)(x - \zeta_5^3) = (x^2 - \alpha x + 1)(x^2 - \alpha' x + 1). \quad (111)$$

If we expand the product on the right end of (111) and compare coefficients, we find the identities

$$\alpha + \alpha' = -1, \qquad \alpha\alpha' = -1. \quad (112)$$

This means that α, α' are the two roots of the polynomial

$$x^2 + x - 1 = (x - \alpha)(x - \alpha').$$

Since $\alpha > 0$ and $\alpha' < 0$ (see Figure ??) we conclude that

$$\alpha = \frac{-1 + \sqrt{5}}{2}, \quad \alpha' = \frac{-1 - \sqrt{5}}{2}.$$

It follows that $K = \mathbb{Q}[\sqrt{5}]$.

Exercises

Exercise 3.1.1 (i) Let p be a prime number and $k \geq 1$. Compute Φ_{p^k}.

(ii) Compute Φ_{12} and Φ_{24}.

Exercise 3.1.2 (i) Let $\alpha := \zeta_7 + \zeta_7^6$. Show that $K_1 := \mathbb{Q}[\alpha]$ is a cubic number field and that $K_1 = \mathbb{Q}[\zeta_7] \cap \mathbb{R}$.

(ii) Find an imaginary quadratic number field $K_2 \subset \mathbb{Q}[\zeta_7]$. (Hint: by Galois theory, there should be an element $\beta = \sum_{k=1}^{6} a_k \zeta_7^k$ such that

$$\sigma_a(\beta) = \begin{cases} \beta, & a \equiv 1, 2, 4 \pmod 7, \\ -\beta, & a \equiv 3, 5, 6 \pmod 7. \end{cases}$$

Find coefficents a_k such that this holds, and then compute β^2.)

3.2 The decomposition law for primes in $\mathbb{Q}[\zeta_n]$

Let $n \in \mathbb{N}$ and p be a prime number. In this section we study the decomposition of p into prime ideals of $K_n = \mathbb{Q}[\zeta_n]$. Our main result is that the decomposition behaviour of p in the extension $K_n/\mathbb{Q}$ only depends on the residue class of p in $\mathbb{Z}/n\mathbb{Z}$. This is our first *reciprocity law*. In the next section we will see that it implies, for instance, the quadratic reciprocity law of Gauss.

We start with a brief remainder on the structure of finite fields.

Theorem 3.2.1 *Let p be a prime number and $n \in \mathbb{N}$. Set $q := p^n$. Then there exists, up to isomorphism, a unique field $\mathbb{F}_q$ with q elements. It has the following properties.*

(a) $\mathbb{F}_q/\mathbb{F}_p$ is the splitting field of the polynomial $x^q - x$, and we have

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

(b) *$\mathbb{F}_q/\mathbb{F}_p$ is a Galois extension. The Galois group is cyclic of order n, generated by the Frobenius automorphism*

$$\varphi_p : \mathbb{F}_q \xrightarrow{\sim} \mathbb{F}_q, \qquad \alpha \mapsto \alpha^p.$$

(c) *The multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$.*

Proof: See [1], Chapter 13, Theorem 6.4. □

Corollary 3.2.2 *Let p be a prime number and $n, m \in \mathbb{N}$. Then $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ if and only if $m \mid n$. If this is the case then*

$$\mathbb{F}_{p^m} = \{\alpha \in \mathbb{F}_{p^n} \mid \alpha^{p^m} = \alpha\}.$$

To illustrate the power of finite fields, we prove the following special case of quadratic reciprocity. The argument can be easily extended to prove the general case.

Proposition 3.2.3 *Let $p \neq 5$ be a prime number. Then*

$$\left(\frac{5}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv \pm 1 \pmod 5.$$

Let $\bar{\Phi}_5 = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_p[x]$ denote the reduction of Φ_5 modulo 5. Let $n \in \mathbb{N}$ denote the order of $p + \mathbb{Z} \cdot 5$ in $(\mathbb{Z}/5\mathbb{Z})^\times$. In other words, n is minimal with the property

$$q := p^n \equiv 1 \pmod 5.$$

Let $\mathbb{F}_q$ be the field with q elements, given by Theorem 3.2.1. Since $5 \mid q-1$ and $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$, there exists an element $\zeta \in \mathbb{F}_q^\times$ of order 5, i.e. a primitive 5th root of unity. It follows that $\bar{\Phi}_5$ splits over $\mathbb{F}_q$, as follows:

$$\bar{\Phi}_5 = (x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4).$$

In fact, $\mathbb{F}_q$ is the splitting field of $\bar{\Phi}_5$ because it is the smallest extension of $\mathbb{F}_p$ which contains ζ.

The trick is now to write $\bar{\Phi}_5$ as a product of two quadratic polynomials, as in Example 3.1.9:

$$\bar{\Phi}_5 = f \cdot g, \qquad f := (x-\zeta)(x-\zeta^4), \quad g := (x-\zeta^2)(x-\zeta^3). \tag{113}$$

Then

$$\begin{aligned} f &= x^2 - \alpha x + 1, \qquad \text{with} \quad \alpha := \zeta + \zeta^4, \\ g &= x^2 - \alpha' x + 1, \qquad \text{with} \quad \alpha' := \zeta^2 + \zeta^3. \end{aligned} \tag{114}$$

Combining (113) with (114) we find the relations

$$\alpha + \alpha' = -1, \qquad \alpha\alpha' = -1. \tag{115}$$

These relations are equivalent to an explicit quadratic equation satisfied by α and α':

$$x^2 + x - 1 = (x - \alpha)(x - \alpha'). \tag{116}$$

Note that these calculations are the same as in Example 3.1.9, with the only difference that we have replaced the complex numbers by the finite field $\mathbb{F}_q$.

Proposition 3.2.3 follows from Claim 1 and Claim 2 below.

Claim 1: $\alpha \in \mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod 5$.

We use Corollary 3.2.2 for $m = 1$ and the calculation

$$\alpha^p = \zeta^p + \zeta^{-p} = \begin{cases} \zeta + \zeta^{-1} = \alpha, & p \equiv \pm 1 \pmod 5, \\ \zeta^2 + \zeta^3 = \alpha', & p \equiv 2, 3 \pmod 5. \end{cases}.$$

Since $\alpha \neq \alpha'$ by (115), we see that

$$\alpha \in \mathbb{F}_p \quad \Leftrightarrow \quad \alpha^p = \alpha \quad \Leftrightarrow \quad p \equiv \pm 1 \pmod 5,$$

proving Claim 1.

Claim 2: $\alpha \in \mathbb{F}_p$ if and only if $\left(\frac{5}{p}\right) = 1$.

To prove Claim 2, we set $\beta := 2\alpha + 1$. Clearly, $\alpha \in \mathbb{F}_p$ if and only if $\beta \in \mathbb{F}_p$. Moreover, the quadratic equation (116) satisfied by α shows that

$$\beta^2 = 4\alpha^2 + 4\alpha + 1 = 5.$$

This shows that $\left(\frac{5}{p}\right) = 1$ if $\beta \in \mathbb{F}_p$. Conversely, if $\left(\frac{5}{p}\right) = 1$ then there exists $\gamma \in \mathbb{F}_p$ with $\gamma^2 = 5$ and then $\beta = \pm\gamma \in \mathbb{F}_p$. This completes the proof of Claim 2 and of Proposition 3.2.3. □

The ring of integers of $\mathbb{Q}[\zeta_n]$

Theorem 3.2.4 *Let $n \in \mathbb{N}$ and $K_n := \mathbb{Q}[\zeta_n]$. Then $\mathcal{O}_{K_n} = \mathbb{Z}[\zeta_n]$.*

Lemma 3.2.5 *Assume that $n = p^k$ is a prime power. We write $\zeta := \zeta_n$ and set $\lambda := 1 - \zeta \in \mathcal{O}_{K_n}$.*

(i) *The principal ideal $(\lambda) \lhd \mathcal{O}_{K_n}$ is a prime ideal with $N((\lambda)) = p$, and we have*

$$(p) = (\lambda)^{(p-1)p^{k-1}}.$$

(ii) *The discriminant of the lattice $\mathbb{Z}[\zeta] \subset \mathcal{O}_{K_n}$ is*

$$d(\mathbb{Z}[\zeta]) = \pm p^s, \qquad s := p^{k-1}(kp - k - 1).$$

Proof: By Example 3.1.5 (iii) we have

$$\Phi_n = x^{(p-1)p^{k-1}} + \ldots + x^{p^{k-1}} + 1 = \prod_a (x - \zeta^a),$$

where a runs over $(\mathbb{Z}/n\mathbb{Z})^\times$. Substituting $x := 1$ we obtain the identity

$$p = \prod_a (1 - \zeta^a). \tag{117}$$

The quotient

$$\epsilon_a := \frac{1-\zeta^a}{1-\zeta} = 1 + \zeta + \ldots + \zeta^{a-1} \in \mathcal{O}_{K_n}$$

is clearly integral. But so is its inverse,

$$\epsilon_a^{-1} = \frac{1-\zeta}{1-\zeta^a} = \frac{1-(\zeta^a)^b}{1-\zeta^a} = 1 + \zeta^a + \ldots + \zeta^{a(b-1)} \in \mathcal{O}_{K_n}$$

(here $b \in \mathbb{N}$ is chosen with $ab \equiv 1 \pmod{n}$). It follows that $\epsilon_a \in \mathcal{O}_{K_n}^\times$ is a unit and hence (117) shows that

$$(p) = (\lambda)^{(p-1)p^{k-1}}.$$

But $(p-1)p^{k-1} = [K_n : \mathbb{Q}]$ by Corollary 3.1.4. Now the fundamental equality (71) implies that (λ) is a prime ideal with $N((\lambda)) = p$. This proves (i).

The cyclotomic polynomial Φ_n is the minimal polynomial of ζ. Therefore, by Remark 2.4.14 and Exercise 2.3.1 we have

$$d(\mathbb{Z}[\zeta]) = \Delta(\Phi_n) = N_{K_n/\mathbb{Q}}(\Phi_n'(\zeta)). \tag{118}$$

To compute the right hand side of (118) we start with the identity

$$X^{p^k} - 1 = \Phi_n \cdot (X^{p^{k-1}} - 1), \tag{119}$$

see Example 3.1.5 (iii). Computing the derivative of both sides of (119) and substituting $x := 1$ we obtain

$$p^k \zeta^{-1} = \Phi_n'(\zeta) \cdot (\xi - 1), \tag{120}$$

where $\xi := \zeta^{p^{k-1}}$. Note that $\xi \in \mu_p^\times$ is a primitive pth root of unity. This means that

$$\Phi_p = x^{p-1} + \ldots + x + 1 = \prod_{a=1}^{p-1} (x - \xi^a).$$

Again substituting $x := 1$ we see that

$$p = \prod_{a=1}^{p-1} (1 - \xi^a) = N_{\mathbb{Q}[\xi]/\mathbb{Q}}(1 - \xi). \tag{121}$$

Using (120), (121) and the multiplicativity of the norm we get

$$N_{K_n/\mathbb{Q}}(\Phi_n'(\zeta)) = \frac{N_{K_n/\mathbb{Q}}(p^k\zeta^{-1})}{N_{K_n/\mathbb{Q}}(\xi-1)} = \frac{\pm p^{k(p-1)p^{k-1}}}{\pm p^{p^{k-1}}} = \pm p^s, \tag{122}$$

with $s := k(p-1)p^{k-1} - p^{k-1}$. Combining (118) and (122) yields the desired formula. This completes the proof of the lemma. □

We start with the proof of Theorem 3.2.4. First we assume that $n = p^k$ is a prime power. Then by Lemma 3.2.5 we have

$$d(1, \zeta_n, \ldots, \zeta_n^{\phi(n)-1}) = \pm p^s,$$

for some $s \geq 1$. Using Lemma 2.4.15 we conclude that

$$p^s \mathcal{O}_{K_n} \subset \mathbb{Z}[\zeta_n] \subset \mathcal{O}_{K_n}. \tag{123}$$

Lemma 3.2.5 also shows that the element $\lambda := 1 - \zeta_n \in \mathbb{Z}[\zeta_n]$ generates a prime ideal of $\mathcal{O}_{K_n}$ of norm p, i.e. $\mathcal{O}_{K_n}/(\lambda) \cong \mathbb{Z}/p\mathbb{Z}$. It follows that

$$\mathcal{O}_{K_n} = \mathbb{Z}[\lambda] + (\lambda). \tag{124}$$

Multiplying both sides of (124) with λ and substituting the result into the right hand side of (124) we obtain

$$\mathcal{O}_{K_n} = \mathbb{Z}[\lambda] + \lambda \cdot \mathbb{Z}[\zeta_n] + (\lambda^2) = \mathbb{Z}[\lambda] + (\lambda^2). \tag{125}$$

Iterating this argument we see that

$$\mathcal{O}_{K_n} = \mathbb{Z}[\lambda] + (\lambda^t), \tag{126}$$

for all $t \geq 1$. In particular, for $t = s(p-1)p^{k-1}$ we obtain, by combining Lemma 3.2.5 with (123) and (126),

$$\mathcal{O}_{K_n} = \mathbb{Z}[\zeta_n] + p^s \mathcal{O}_{K_n} = \mathbb{Z}[\zeta_n].$$

This proves Theorem 3.2.4 in case where $n = p^k$ is a prime power. The general case follows from this special cases, applying iteratively Lemma 3.2.6 and Lemma 3.2.7 below. □

Lemma 3.2.6 *Let $n, m \in \mathbb{N}$ be relatively prime. Then*

$$\mathbb{Q}[\zeta_{nm}] = \mathbb{Q}[\zeta_n] \cdot \mathbb{Q}[\zeta_m]$$

and

$$\mathbb{Q}[\zeta_n] \cap \mathbb{Q}[\zeta_m] = \mathbb{Q},$$

as subfields of $\mathbb{C}$.

Lemma 3.2.7 *Let $K, K' \subset \mathbb{C}$ be number fields with integral basis (α_i) and (α'_j), respectively. We assume that $K \cap K' = \mathbb{Q}$ and that the discriminants d_K and $d_{K'}$ are relatively prime. Then $(\alpha_i \alpha'_j)$ is an integral basis for $L := K \cdot K'$, and $d_L = d_K \cdot d_{K'}$.*

Proof: See [6], Kapitel I, Satz 2.11. □

Here is the main result of this section. It describes the decomposition of a prime number p in the cyclotomic extension $K_n = \mathbb{Q}[\zeta_n]/\mathbb{Q}$.

Theorem 3.2.8 *Let $n \in \mathbb{N}$ and p be a prime number. Write $n = p^k m$ with $p \nmid m$, and let $f \in \mathbb{N}$ be the smallest positive integer such that $p^f \equiv 1 \pmod{m}$. Set $r := \phi(m)/f$. Then*

$$(p) = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r)^{\phi(p^k)},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \lhd \mathcal{O}_{K_n}$ are pairwise distinct prime ideals with $N(\mathfrak{p}_i) = p^f$, for all i.

Corollary 3.2.9 (i) *A prime p is ramified in $K_n/\mathbb{Q}$ if and only if $p \mid n$ (with the exception of $p = 2$, which is ramified if and only if $4 \mid n$).*

(ii) *Assume $p \neq 2$. Then p is totally split in the extension $K_n/\mathbb{Q}$ if and only if $p \equiv 1 \pmod{n}$.*

Example 3.2.10 Let $n = 3$. Then $K_3 = \mathbb{Q}[\zeta_3] = \mathbb{Z}[\sqrt{-3}]$. Corollary 3.2.9 (ii) says that a prime p splits in K_3, i.e.

$$(p) = \mathfrak{p} \cdot \bar{\mathfrak{p}}, \quad \text{with } \bar{\mathfrak{p}} \neq \mathfrak{p},$$

if and only if $p \equiv 1 \pmod{3}$. But we have see before that this happens if and only if $\left(\frac{-3}{p}\right) = 1$, and then

$$\mathfrak{p} := (p, \sqrt{-3} - a), \qquad \text{with } a^2 \equiv -3 \pmod{p}.$$

We conclude that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{3}, \\ -1, & \text{if } p \equiv -1 \pmod{3}. \end{cases}$$

This is a special case of the Quadratic Reciprocity Law (Theorem 1.3.6).

Proof: By Theorem 3.2.4 we have $\mathcal{O}_{K_n} = \mathbb{Z}[\zeta_n]$, and by Corollary 3.1.4 we know that Φ_n is the minimal polynomial of ζ_n. Therefore, the prime factorization of p in $\mathcal{O}_{K_n}$ corresponds to the decomposition of $\bar{\Phi}_n \in \mathbb{F}_p[x]$ into irreducible factors, see Theorem 2.5.22. More precisely, we have to show that

$$\bar{\Phi}_n = (\bar{g}_1 \cdot \ldots \cdot \bar{g}_r)^{\phi(p^k)}, \tag{127}$$

where $\bar{g}_i \in \mathbb{F}_p[x]$ are irreducible polynomials of degree f. To prove (127) we first assume that $n = m$ is prime to p. Let $q := p^f$. The field $\mathbb{F}_q$ is the smallest extension of $\mathbb{F}_p$ which contains a primitive nth root of unity ζ, by the choice of f. It follows that $\mathbb{F}_q$ is the splitting field of $\bar{\Phi}_n$ and that

$$\bar{\Phi}_n = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta^a).$$

Let $\varphi_p : \mathbb{F}_q \xrightarrow{\sim} \mathbb{F}_q$ denote the Frobenius automorphism, $\varphi_p(\alpha) = \alpha^p$. By Theorem 3.2.1, ϕ_p generates the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. It follows that ϕ_p permutes the roots of $\bar{\Phi}_n$ and that the irreducible factors of $\bar{\Phi}_n$ over $\mathbb{F}_p$ correspond to the orbits of this permutation. More explicitly, let $a_1, \ldots, a_r \in (\mathbb{Z}/n\mathbb{Z})^\times$ be a set of representatives for the cosets of the subgroup $\langle \bar{p} \rangle \subset (\mathbb{Z}/n\mathbb{Z})^\times$. Then

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a_i p^l + n\mathbb{Z} \mid i = 1, \ldots, r,\ l = 0, \ldots, f-1\}$$

and

$$\bar{g}_i := \prod_{l=0}^{f-1} (x - \zeta^{a_i p^l}) \in \mathbb{F}_p[x]$$

is an irreducible factor of $\bar{\Phi}_n$. This proves (127) if $n = m$ is prime to p.

Now assume that $n = p^k m$ with $k \geq 1$. We have to show that

$$\bar{\Phi}_n = \bar{\Phi}_m^{\varphi(p^k)}. \tag{128}$$

We use induction over m and k. For $k = 0$ the claim is already proved. For $m = 1$ we have

$$\bar{\Phi}_{p^k} = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \frac{(x-1)^{p^k}}{(x-1)^{p^{k-1}}} = (x-1)^{(p-1)p^{k-1}} = \bar{\Phi}_1^{\varphi(p^k)},$$

so (128) holds as well. We may therefore assume $m > 1$ and $k \geq 1$. By (109) we have

$$\bar{\Phi}_n = \frac{x^{p^k m} - 1}{\prod_{d | p^k, d < p^k m} \bar{\Phi}_d} = \frac{(x^m - 1)^{p^k}}{\prod_{d | p^k, d < p^k m} \bar{\Phi}_d}. \tag{129}$$

We write the divisor $d \mid p^k m$ as $d = p^l d'$, with $0 \leq l \leq k$ and $d' \mid m$. Then $d < p^k m$ if and only if $l < k$ or $d' < d$. Therefore, the denominator in (129) can be rewritten, using the induction hypothesis, as

$$\begin{aligned}
\prod_{d | p^k, d < p^k m} \bar{\Phi}_d &= \Big(\prod_{l=0}^{k-1} \cdot \prod_{d' | m} \bar{\Phi}_{p^l d'} \Big) \cdot \Big(\prod_{d' | m, d' < m} \bar{\Phi}_{p^k d'} \Big) \\
&= \prod_{l=0}^{k-1} (x^m - 1)^{\varphi(p^l)} \cdot \Big(\prod_{d' | m, d' < m} \bar{\Phi}_{d'} \Big)^{\varphi(p^k)} \\
&= (x^m - 1)^{p^{k-1}} \cdot \Big(\prod_{d' | m, d' < m} \bar{\Phi}_{d'} \Big)^{\varphi(p^k)}.
\end{aligned} \tag{130}$$

In the last step we have used the equality

$$\sum_{l=0}^{k-1} \varphi(p^l) = p^{k-1},$$

which we leave as an exercise. Combining (129) and (130) we obtain

$$\bar{\Phi}_n = \Big(\frac{x^m - 1}{\prod_{d'|m, d'<m} \bar{\Phi}_{d'}}\Big)^{\varphi(p^k)} = \bar{\Phi}_m^{\varphi(p^k)}.$$

proving (128). This completes the proof of Theorem 3.2.8. □

3.3 Dirichlet characters, Gauss sums and Jacobi sums

We start with the abstract theory of characters of finite abelian groups. This theory should be seen as a finite version of Fourier theory.

Definition 3.3.1 Let $(A, \cdot)$ be a finite abelian group. A *character* on A is a group homomorphism

$$\chi : A \to \mathbb{C}^\times.$$

The set of all characters on A is called the *dual group* and is denoted by $\hat{A}$. The *principal character* is the element $\epsilon \in \hat{A}$ with $\epsilon(a) = 1$ for all $a \in A$.

Remark 3.3.2 (i) The set $\hat{A}$ is again an abelian group with respect to multiplication of characters, defined as follows:

$$(\chi_1 \cdot \chi_2)(a) := \chi_1(a) \cdot \chi_2(a),$$

for $\chi_1, \chi_2 \in \hat{A}$. The principal character is the neutral element of $\hat{A}$.

(ii) Let $n := |A|$ be the order of A. Then $a^n = 1$ for all $a \in A$. Therefore, $\chi^n(a) = \chi(a^n) = 1$ for all $a \in A$ and $\chi \in \hat{A}$. It follows that a character $\chi \in \hat{A}$ can actually be seen as a group homomorphism

$$\chi : A \to \mathbb{\mu}_n.$$

Moreover, every character has exponent n, i.e. $\chi^n = \epsilon$.

(iii) For $\chi \in \hat{A}$ and $a \in A$ we have

$$\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}.$$

Proposition 3.3.3 *Let A be a finite abelian group. Then $|A| = |\hat{A}|$. Moreover, for every $a \in A$, $a \neq 1$, there exists a character $\chi \in \hat{A}$, $\chi \neq \epsilon$, with $\chi(a) \neq 1$.*

Proof: We assume first that A is cyclic of order n, and we fix a generator $a_0 \in A$. Then

$$\chi_0 : A \to \mathbb{\mu}_n, \qquad a_0^k \mapsto \zeta_n^k,$$

is a character on A of order n. It has the property that $\chi_0(a) = 1$ if and only if $a = 1$. Moreover, for any character $\chi \in \hat{A}$ we have $\chi(a_0) = \zeta_n^k$, for some $k \in \mathbb{Z}/n\mathbb{Z}$, and then $\chi = \chi_0^k$. It follows that $\hat{A}$ is cyclic of order n, generated by χ_0. In particular, $|A| = |\hat{A}|$. This proves the proposition in case that A is cyclic.

The proof in the general case uses essentially the same argument as before. We leave the details to the reader, noting only that one has to use the structure theorem of finite abelian groups (see [1], Chapter 12, Theorem 6.12). It says that there exists elements $a_1, \ldots, a_r \in A$, of order $n_1, \ldots, n_r$, such that

$$\mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z} \xrightarrow{\sim} A, \qquad (k_1, \ldots, k_r) \mapsto a_1^{k_1} \cdot \ldots \cdot a_r^{k_r},$$

is an isomorphism. □

Remark 3.3.4 The proof of Proposition 3.3.3 shows that $A \cong \hat{A}$ are isomorphic as abelian groups. However, the isomorphism that comes up depends on the choice of the generators $a_1, \ldots, a_r$ of A (resp. a_0 in the cyclic case). Since there is no canonical choice of such generators, there is also no canonical choice of the isomorphism $A \cong \hat{A}$.

Theorem 3.3.5 *Let A be a finite abelian group.*

(i) *For every $\chi \in \hat{A}$ we have*

$$\sum_{a \in A} \chi(a) = \begin{cases} |A|, & \chi = \epsilon, \\ 0, & \chi \neq \epsilon. \end{cases}$$

(ii) *For every $a \in A$ we have*

$$\sum_{\chi \in \hat{A}} \chi(a) = \begin{cases} |A|, & a = 1, \\ 0, & a \neq 1. \end{cases}$$

Proof: If $\chi = \epsilon$ then the statement (i) is obvious. Suppose that $\chi \neq \epsilon$ and choose $b \in A$ such that $\chi(b) \neq 1$. Since the map $A \to A$, $a \mapsto ab$, is bijective, we have

$$\chi(b) \cdot \sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(ab) = \sum_{a \in A} \chi(a).$$

It follows that $\sum_{a \in A} \chi(a) = 0$, proving (i). The proof of (ii) is very similar and left to the reader (hint: use Proposition 3.3.3). □

Corollary 3.3.6 (Orthogonality relations)

(i) *For $\chi_1, \chi_2 \in \hat{A}$ we have*

$$\frac{1}{|A|}\sum_{a\in A}\chi_1(a)\cdot\overline{\chi_2(a)} = \begin{cases}1, & \chi_1 = \chi_2,\\ 0, & \chi_1 \neq \chi_2.\end{cases}$$

(ii) *For $a_1, a_2 \in A$ we have*

$$\frac{1}{|A|}\sum_{\chi\in\hat{A}}\chi(a_1)\cdot\overline{\chi(a_2)} = \begin{cases}1, & a_1 = a_2,\\ 0, & a_1 \neq a_2.\end{cases}$$

Remark 3.3.7 The name *orthogonality relation* is easily explained. If we order the elements of A as $a_1, \ldots, a_n$ and the elements of $\hat{A}$ as $\chi_1, \ldots, \chi_n$, then the matrix $M := (\chi_i(a_j))_{i,j}$ is orthogonal in the sense that

$$M^t \cdot \overline{M} = n \cdot E_n.$$

Another way to formulate (ii) is that the set of characters $\hat{A}$ is an orthogonal basis of the vector space of all functions $f : A \to \mathbb{C}$, endowed with the hermitian scalar product

$$\langle f, g\rangle_A := \frac{1}{|A|}\sum_{a\in A} f(a)\overline{g(a)}.$$

Example 3.3.8 Let's consider the group $A := (\mathbb{Z}/5\mathbb{Z})^\times$. It is a cyclic group of order 4, generated for instance by the residue class of 2. Using the proof of Proposition 3.3.3 we see that $\hat{A}$ is cyclic of order 4, generated by the character χ which is determined by $\chi(\bar{2}) := i$. So the *character table* of the group $(\mathbb{Z}/5\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ looks as follows.

	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
ϵ	1	1	1	1
χ	1	i	$-i$	-1
χ^2	1	-1	-1	1
χ^3	1	$-i$	i	1

The reader should check by hand that the orthogonality relations of Corollary 3.3.6 hold.

Dirichlet characters

Definition 3.3.9 A function $\chi : \mathbb{Z} \to \mathbb{C}$ is called a *Dirichlet character* if there exists a positive integer $n \in \mathbb{N}$ such that the following holds.

(a) $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$.

(b) $\chi(a)$ depends only on the residue class of a in $\mathbb{Z}/n\mathbb{Z}$.

(c) $\chi(a) = 0$ if and only if $\mathrm{ggT}(a, n) \neq 1$.

For a given Dirichlet character χ any positive integer n which satisfies (b) and (c) is called a *modulus* of χ. Clearly, there exists a smallest modulus for χ.

It is clear from the definition that $\chi(1) = 1$, for all Dirichlet characters χ. There is a unique Dirichlet character ϵ of modulus 1 which is called the *trivial character*. Note that $\epsilon(a) = 1$ for all $a \in \mathbb{Z}$. Note also that for all Dirichlet characters $\chi \neq \epsilon$ we have $\chi(0) = 0$.

A Dirichlet character modulo n is called *principal* if it assumes only the values 0 and 1. We usually write ϵ for the unique principal character modulo n. Note that ϵ is not the trivial character unless $n = 1$.

Let $n \in \mathbb{N}$ and $d \mid n$. If χ is a Dirichlet character modulo d then

$$\chi^* : \mathbb{Z} \to \mathbb{C}, \qquad a \mapsto \begin{cases} \chi(a), & \mathrm{ggT}(a, n) = 1, \\ 0, & \mathrm{ggT}(a, n) = 0, \end{cases}$$

is a Dirichlet character modulo n, called the *induced character*. A Dirichlet character modulo n is called *primitive* if it is not induced from a Dirichlet character modulo d for a proper divisor $d \mid n$.

A Dirichlet character χ modululo n gives rise to a character

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times.$$

Conversely, every character on the group $(\mathbb{Z}/n\mathbb{Z})^\times$ comes from a unique Dirichlet character modulo n. Another possible convention is to associate to a character χ on $(\mathbb{Z}/n\mathbb{Z})^\times$ the unique primitive Dirichlet character which agrees with χ on all invertible residue classes modulo n. We will decide from case to case which convention will be more convenient. Apart from this sublety we will use the notions *Dirichlet character modulo n* and *character on* $(\mathbb{Z}/n\mathbb{Z})^\times$ interchangeably.

Example 3.3.10 Let p be an odd prime. Then the Legendre symbol (see Definition 1.3.2)

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & p \nmid a \text{ and } a \text{ is a quadratic residue mod } p, \\ -1, & p \nmid a \text{ and } a \text{ is a quadratic nonresidue mod } p, \\ 0, & p \mid a. \end{cases}$$

is a primitive Dirichlet character modulo p. It corresponds to the unique element of order 2 in the character group of $\mathbb{F}_p^\times$.

More generally, for every odd squarefree integer $n = p_1 \cdot \ldots \cdot p_r$ we have the *Jacobi symbol*

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{r} \left(\frac{a}{p}\right).$$

It is a primitive quadratic Dirichlet character modulo n, see [5], §5.2.

Gauss sums

Let us fix an odd prime number p. A Dirichlet character modulo p is now regarded as a function $\chi : \mathbb{F}_p \to \mathbb{C}$. We use the convention that all Dirichlet characters are supposed to be primitive. In the current setting this just means that the Dirichlet character ϵ corresponding to the unit element in the character group of $\mathbb{F}_p^\times$ is the trivial Dirichlet character, i.e. the function $\epsilon : \mathbb{F}_p \to \mathbb{C}$ with $\epsilon(a) = 1$ for all $a \in \mathbb{F}_p$. For all Dirichlet characters $\chi \neq \epsilon$ we have $\chi(0) = 0$.

Definition 3.3.11 Let p be an odd prime and χ be a Dirichlet character modulo p. For all $a \in \mathbb{F}_p$ we define the *Gauss sum* for χ with respect to a as the complex number

$$g_a(\chi) := \sum_{x \in \mathbb{F}_p} \chi(a)\zeta_p^{ax}.$$

Example 3.3.12 Let $p = 5$ and $\chi = \left(\frac{\cdot}{5}\right)$ be the Legendre symbol modulo 5. Then

$$g_1(\chi) = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4.$$

Using Example 3.1.9 one sees that

$$g_1(\chi) = \sqrt{5}.$$

Proposition 3.3.13 *Let χ be a Dirichlet character modulo p and $a \in \mathbb{F}_p$. We have*

$$g_a(\chi) = \begin{cases} p, & a = 0, \chi = \epsilon, \\ 0, & a = 0, \chi \neq \epsilon, \\ 0, & a \neq 0, \chi = \epsilon, \\ \overline{\chi(a)} g_1(\chi), & a \neq 0, \chi \neq \epsilon. \end{cases} \tag{131}$$

Proof: Suppose that $a \neq 0$ and $\chi \neq \epsilon$. Then

$$\chi(a) g_a(\chi) = \sum_x \chi(ax)\zeta_p^{ax} = \sum_x \chi(x)\zeta_p^x = g_a(\chi),$$

as claimed. We leave the other three cases as easy exercises. □

Proposition 3.3.14 *Let p be an odd prime number and $\chi := \left(\frac{\cdot}{p}\right)$ the Legendre symbol, i.e. the unique Dirichlet character modulo p of order 2. Then*

$$g_1(\chi)^2 = p^* := \begin{cases} p, & p \equiv 1 \pmod 4, \\ -p, & p \equiv -1 \pmod 4. \end{cases}$$

Proof: Using the definition of $g_1(\chi)$ we obtain

$$g_1(\chi)^2 = \sum_{x,y} \chi(xy)\zeta_p^{x+y}, \tag{132}$$

where x, y run over $\mathbb{F}_p^\times$. The trick is to substitute $y := xz$ (which only permutes the summands) and use the fact that $\chi(x^2) = 1$. We get

$$g_1(\chi)^2 = \sum_{x,z} \chi(x^2 z)\zeta_p^{x(z+1)} = \sum_{z\neq 0} \chi(z)\Big(\sum_{x\neq 0} \zeta_p^{x(z+1)}\Big). \tag{133}$$

The inner sum is equal to $p-1$ if $z = -1$ and equal to $\zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1} = -1$ for $z \neq 0, -1$. Using Theorem 3.3.5 (i) we get

$$\begin{aligned} g_1(\chi)^2 &= (p-1)\chi(-1) - \sum_{z\neq 0,-1} \chi(z) \\ &= (p-1)\chi(-1) + \chi(-1) = \chi(-1)p. \end{aligned} \tag{134}$$

Finally, by Lemma 1.3.3 we have

$$\chi(-1) = \left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv -1 \pmod 4. \end{cases} \tag{135}$$

Combining (134) and (135) proves the proposition. □

The proposition says that $g_1(\chi) = \pm\sqrt{p^*}$. Since $g_1(\chi)$ is, by definition, an element of $\mathbb{Q}[\zeta_p]$ we obtain the following result.

Corollary 3.3.15 *The quadratic number field $\mathbb{Q}[\sqrt{p}]$ is contained in the cyclotomic field $\mathbb{Q}[\zeta_p]$.*

Remark 3.3.16 Proposition 3.3.14 determines the quadratic Gauss sum $g_1(\chi)$ only up to sign. The computation of the sign is more difficult, but the result is very simple:

$$g_1(\chi) = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

See [5], §6.4, Theorem 1.

3.4 Abelian number fields

We start with a quite general setup. Let L/K be a Galois extension of number fields, with Galois group $G = \mathrm{Gal}(L/K)$. We also fix a prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$ and look at the set of prime ideals $\mathfrak{P} \lhd \mathcal{O}_L$ with $\mathfrak{P} \mid \mathfrak{p}$,

$$S_\mathfrak{p} := \{\mathfrak{P} \lhd \mathcal{O}_L \mid \mathfrak{P} \mid \mathfrak{p}\}.$$

Note that a prime ideal $\mathfrak{P} \lhd \mathcal{O}_L$ lies in $S_\mathfrak{p}$ if and only if $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. It follows that for an element $\sigma \in G$ of the Galois group we have $\sigma(\mathfrak{P}) \in S_\mathfrak{p}$. This means that the group G acts on the set $S_\mathfrak{p}$ (from the left).

Lemma 3.4.1 *The action of G on $S_\mathfrak{p}$ is transitive.*

The stabilizer

$$G_\mathfrak{P} := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

is called the *decomposition group* of $\mathfrak{p}$. Lemma **??** and the orbit-stabilizer-formula imply that

$$|S_\mathfrak{p}| = \frac{|G|}{|G_\mathfrak{P}|}. \tag{136}$$

It is clear that

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

Therefore, the lemma implies that all decomposition groups $G_\mathfrak{P}$ for $\mathfrak{P} \in S_\mathfrak{p}$ are conjugate subgroups of G. In particular, if G is an abelian group, then $G_\mathfrak{P}$ is actually independent of $\mathfrak{P} \in S_\mathfrak{p}$. We may then write $G_\mathfrak{p} := G_\mathfrak{P}$ and call it the decomposition group of $\mathfrak{p}$ in the extension L/K.

Let us fix $\mathfrak{P} \in S_\mathfrak{p}$. Let $\mathbb{F}_\mathfrak{P} := \mathcal{O}_L/\mathfrak{P}$ and $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ denote the residue fields of $\mathfrak{P}$ and $\mathfrak{p}$. These are finite fields with $N(\mathfrak{P})$ resp. $N(\mathfrak{p})$ elements. Since $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$, we have a natural embedding $\mathbb{F}_\mathfrak{p} \hookrightarrow \mathbb{F}_\mathfrak{P}$. It follows that $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is a finite field extension and that

$$N(\mathfrak{P}) = N(\mathfrak{p})^{[\mathbb{F}_\mathfrak{P}:\mathbb{F}_\mathfrak{p}]}. \tag{137}$$

The degree $f_\mathfrak{p} := [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}]$ is called the *inertia degree* of $\mathfrak{p}$ in L/K. It follows from Lemma 3.4.1 that $f_\mathfrak{p}$ is independent of the choice of $\mathfrak{P} \in S_\mathfrak{p}$.

As a finite extension of finite fields, $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is automatically a Galois extension (see Theorem **??**). Moreover, every element $\sigma \in G_\mathfrak{P}$ induces an element $\bar{\sigma} \in \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ defined by

$$\bar{\sigma}(\bar{\alpha}) := \overline{\sigma(\alpha)}$$

(where $\alpha \in \mathcal{O}_L$ and $\bar{\alpha}$ denotes the image of α in $\mathbb{F}_\mathfrak{P}$). A routine verification shows that we obtain a group homomorphism

$$G_\mathfrak{P} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}), \qquad \sigma \mapsto \bar{\sigma}. \tag{138}$$

Proposition 3.4.2 *The homomorphism* (138) *is surjective. It is an isomorphism if and only if $\mathfrak{p}$ is unramified in the extension L/K.*

Recall from Theorem **??** that the Galois group $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ is cyclic, generated by the element φ determined by

$$\varphi(\bar{\alpha}) = \bar{\alpha}^{N(\mathbb{F}_\mathfrak{p})}.$$

Therefore, Proposition 3.4.2 implies the following statement.

Corollary 3.4.3 *Assume that $\mathfrak{p}$ is unramified in the extension L/K. Then for every $\mathfrak{P} \in S_\mathfrak{p}$ there exists a unique element $\mathrm{Frob}_\mathfrak{P} \in G_\mathfrak{P}$ such that*

$$\mathrm{Frob}_\mathfrak{P}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}} \tag{139}$$

Definition 3.4.4 The element $\mathrm{Frob}_{\mathfrak{P}} \in G_{\mathfrak{P}}$ is called the *Frobenius element* of G for the prime ideal $\mathfrak{P}$. Alternatively, it is also called a Frobenius element *above* $\mathfrak{p}$.

Remark 3.4.5 It is easy to check that

$$\mathrm{Frob}_{\sigma(\mathfrak{P})} = \sigma \,\mathrm{Frob}_{\mathfrak{P}}\, \sigma^{-1},$$

for all $\sigma \in G$ and $\mathfrak{P} \in S_{\mathfrak{p}}$. Therefore, all Frobenius elements above $\mathfrak{p}$ are conjugate, by Lemma 3.4.1.

If, moreover, G is abelian then this shows that $\mathrm{Frob}_{\mathfrak{P}}$ only depends on $\mathfrak{p}$ but not on the choice of $\mathfrak{P} \in S_{\mathfrak{p}}$. If this is the case we write $\mathrm{Frob}_{\mathfrak{p}} := \mathrm{Frob}_{\mathfrak{P}}$ and call it *the Frobenius element for* $\mathfrak{p}$. The statement of Corollary 3.4.3 is now considerably stronger: we have

$$\mathrm{Frob}_{\mathfrak{P}}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

for *all* $\mathfrak{P} \in S_{\mathfrak{p}}$.

Definition 3.4.6 A number field $K/\mathbb{Q}$ is called *abelian* if $K \subset K_n = \mathbb{Q}[\zeta_n]$ for some $n \in \mathbb{N}$.

Recall from §**??** that $K_n/\mathbb{Q}$ is a Galois extension, with abelian Galois group $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. In the following we will identify the two groups $\mathrm{Gal}(K_n/\mathbb{Q})$ and $(\mathbb{Z}/n\mathbb{Z})^\times$ via the isomorphism $a \pmod n \mapsto \sigma_a$ from ??. If K is an abelian number field, contained in K_n, then the Main Theorem of Galois Theory says that $K = K_n^H$ for a unique subgroup $H \subset (\mathbb{Z}/n\mathbb{Z})^\times$. Moreover, we have a canonical isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times/H \xrightarrow{\sim} \mathrm{Gal}(L/\mathbb{Q}), \qquad pH \mapsto \sigma_a|_K. \tag{140}$$

In particular, we see that an abelian number field K is a Galois extension of $\mathbb{Q}$ with abelian Galois group.

Remark 3.4.7 The famous *Kronecker-Weber-Theorem* asserts that every Galois extension of $\mathbb{Q}$ with abelian Galois group is in fact an abelian extension.

Theorem 3.4.8 *Let $K = K_n^H$ be an abelian number field, and let p be a prime number such that $p \nmid n$. Then p is unramified in $K/\mathbb{Q}$. Furthermore, the Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$ corresponds, via the isomorphism (140), to the image of pH, i.e. we have*

$$\mathrm{Frob}_p = \sigma_p|_K.$$

Corollary 3.4.9 *With $K = K_n^H$ and p be as in the theorem. Then the prime factorization of $(p) \lhd \mathcal{O}_K$ is of the form*

$$(p) = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r,$$

where $\mathfrak{p}_1, \dots, \mathfrak{p}_r \lhd \mathcal{O}_K$ are pairwise distinct prime ideals of norm $N(\mathfrak{p}_i) = p^f$, and where f is the minimal positive integer such that

$$p^f + n\mathbb{Z} \in H.$$

In particular, a prime p splits completely in $K/\mathbb{Q}$ if and only if $p + n\mathbb{Z} \in H$.

We can also apply Theorem 3.4.8 to a relative extension of abelian number fields. Let $K = K_n^{H_K}$ and $L = K_n^{H_L}$ be abelian number fields corresponding to nested subgroups

$$H_L \subset H_K \subset (\mathbb{Z}/n\mathbb{Z})^\times.$$

Then $K \subset L$ and L/K is a Galois extension with abelian Galois group

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} H_K/H_L.$$

For $a \in H_K$ we let $\sigma_a \in \mathrm{Gal}(L/K)$ denote the element corresponding to the class aH_L.

Let p be a prime number, $p \nmid n$, and let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal above p. Then we have a well defined Frobenius element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K)$.

Corollary 3.4.10 *We have*

$$\mathrm{Frob}_\mathfrak{p} = \sigma_{p^f},$$

where $p^f = N(\mathfrak{p})$.

Quadratic reciprocity

We are now going to show that the law of quadratic reciprocity is an easy and direct consequence of Theorem 3.4.8. In the next section we will use similar but more involved arguments to prove the law of cubic reciprocity.

Let p be an odd prime, and set

$$p^* := \left(\frac{-1}{p}\right)p = \begin{cases} p, & \text{if } p \equiv 1 \pmod 4, \\ -p, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Then $\mathbb{Q}[\sqrt{p^*}] \subset \mathbb{Q}[\zeta_p]$ by Corollary 3.3.15. This means that the quadratic number field $K := \mathbb{Q}[\sqrt{p^*}]$ is an abelian number field. More precisely, $K = \mathbb{Q}[\zeta_p]^H$, where $H \subset (\mathbb{Z}/p\mathbb{Z})^\times$ is a subgroup of index 2. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$, which is even, there exists in fact a unique subgroup H of index 2, namely the kernel of the unique quadratic Dirichlet character $\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{\mu}_2$. Hence

$$H = \{a \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \left(\frac{a}{p}\right) = 1\}.$$

Now let ℓ be another prime, different from 2 and p. By Corollary 3.4.9, ℓ splits completely in $K = \mathbb{Q}[\zeta_p]^H$ if and only if $\ell + p\mathbb{Z} \in H$, i.e. if and only if

$$\left(\frac{\ell}{p}\right) = 1.$$

On the other hand, we know from ??? that ℓ splits completely in $K = \mathbb{Q}[\sqrt{p^*}]$ if and only if

$$\left(\frac{p^*}{\ell}\right).$$

We conclude that

$$\left(\frac{\ell}{p}\right) = \left(\frac{p^*}{\ell}\right). \tag{141}$$

This identity is just a reformulation of the law of quadratic reciprocity.

Exercises

Exercise 3.4.1 Show (without using Quadratic Reciprocity!) that for primes $p \neq 3$ we have

$$\left(\frac{3}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv \pm 1 \pmod{12}.$$

Hint: do something similar as in the proof of Proposition 3.2.3.

3.5 The law of cubic reciprocity

Let $d \in \mathbb{Z}$ be a squarefree integer. The law of quadratic reciprocity shows that the set of primes $p \nmid 2d$ for which the congruence

$$x^2 \equiv d \pmod{p}$$

has a solution in $\mathbb{F}_p$ is itself given by a congruence condition of the form

$$p \equiv a_1, \ldots, a_r \pmod{N}.$$

Here $N = d$ or $N = 4d$, and $a_1, \ldots, a_r$ are certain integers which only depend on d. In fact, by Exercise ?? the integers $a_1, \ldots, a_r$ are representatives of the subgroup

$$H = \{a \in (\mathbb{Z}/N\mathbb{Z})^\times \mid \left(\frac{a}{d}\right) = 1\}.$$

It is a very obvious question whether there is a similar rule for higher powers x^n with $n > 2$. For instance, for which primes p does the congruence

$$x^3 \equiv 2 \pmod{p}$$

have a solution in $\mathbb{F}_p$? As we will see, the law of cubic reciprocity does answer this question, but the answer is more complicated than for squares. See Corollary 3.5.13 and Remark 3.5.14. In fact, the set of primes for which 2 is a cubic residue mod p is *not* given by a congruence condition on p.

We start by defining the *nth power residue symbol*, which generalize the Legendre symbol. We fix an integer $n \geq 2$ and a number field K such that all n-th roots of unity are contained in K. More precisely, $K \subset \mathbb{C}$ and $\mu_n \subset K$.

Let p be a prime number prime to n and let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime ideal of $\mathcal{O}_K$ dividing p. Then $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ is a finite field with $q := N(\mathfrak{p})$ elements.

Proposition 3.5.1 *For every $\alpha \in \mathcal{O}_K$ with $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$ there exists a unique nth root of unity $\zeta \in \mu_n$ such that*

$$\alpha^{(q-1)/n} \equiv \zeta \pmod{\mathfrak{p}}.$$

Moreover, $\zeta = 1$ if and only if there exists $\beta \in \mathcal{O}_K$ such that

$$\beta^n \equiv \alpha \pmod{\mathfrak{p}}.$$

Proof: We have seen in the proof of .. that the polynomial $x^n - 1 \in \mathbb{F}_p[x]$ is separable. This shows that the natural map

$$\mu_n \to \mathbb{F}_\mathfrak{p}^\times \tag{142}$$

is injective. Since $\mathbb{F}_\mathfrak{p}^\times$ is a cyclic group of order $q-1$, the image of (142) is the unique subgroup of $\mathbb{F}_\mathfrak{p}^\times$ of order n. We conclude that $n \mid q-1$. Moreover, for $\bar{\alpha} \in \mathbb{F}_\mathfrak{p}^\times$ we have

$$\left(\bar{\alpha}^{(q-1)/n}\right)^3 = \bar{\alpha}^{q-1} = 1.$$

This means that $\bar{\alpha}^{(q-1)/n}$ lies in the image of (142), i.e. there exists a unique element $\zeta \in \mu_n$ such that $\zeta \equiv \alpha^{(q-1)/n} \pmod{\mathfrak{p}}$. We have $\zeta = 1$ if and only if $\bar{\alpha}$ lies in the unique subgroup $H \subset \mathbb{F}_\mathfrak{p}^\times$ of index n. But H consists precisely of the nth powers (this sort of argument was already used in the proof of Lemma 1.3.3). It follows that $\zeta = 1$ if and only if there exists $\beta \in \mathcal{O}_K$ with $\beta^n \equiv \alpha \pmod{\mathfrak{p}}$. □

Definition 3.5.2 For $\alpha \in \mathcal{O}_K$, $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$ we write $\left(\frac{\alpha}{\mathfrak{p}}\right)_n := \zeta$ for the nth root of unity $\zeta \in \mu_n$ from Proposition **??**. For $\alpha \equiv 0 \pmod{\mathfrak{p}}$ we set $\left(\frac{\alpha}{\mathfrak{p}}\right)_n := 0 \in \mathbb{C}$. The resulting map

$$\left(\frac{\cdot}{\mathfrak{p}}\right)_n : \mathcal{O}_K \to \mathbb{C}$$

is called the *nth power residue symbol* with respect to the prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$.

Remark 3.5.3 By its definition, the nth power residue symbol has the following properties.

(i) If $\alpha \equiv \alpha' \pmod{\mathfrak{p}}$ then

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n = \left(\frac{\alpha'}{\mathfrak{p}}\right)_n.$$

(ii) For $\alpha, \beta \in \mathcal{O}_K$ we have

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right)_n = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \left(\frac{\beta}{\mathfrak{p}}\right)_n.$$

(iii) Suppose $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$. Then $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1$ if and only if the congruence

$$x^n \equiv \alpha \pmod{\mathfrak{p}}$$

has a solution $x = \beta \in \mathcal{O}_K$.

(iv) We have

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{(q-1)/2} \pmod{\mathfrak{p}}.$$

By (i) and (ii) we may regard the nth power residue symbol as a group homomorphism

$$\left(\frac{\cdot}{\mathfrak{p}}\right)_n : \mathbb{F}_{\mathfrak{p}}^{\times} \to \mathbb{\mu}_n \subset \mathbb{C}^{\times},$$

i.e. as a character on $\mathbb{F}_{\mathfrak{p}}^{\times}$. This character has order n.

Example 3.5.4 For $K = \mathbb{Q}$ and p an odd prime number the 2nd power residue symbol is equal to the Legendre symbol $\left(\frac{\cdot}{p}\right)$ (Definition 1.3.2).

For the rest of this section we set $n = 3$ and $K := K_3 = \mathbb{Q}[\omega]$, where $\omega := \zeta_3 = (-1 + \sqrt{-3})/2$. Let $p \neq 3$ be a prime number. First we assume that $p \equiv 1 \pmod 3$. Then p is totally split in the extension $K/\mathbb{Q}$, i.e. $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, with $\mathfrak{p} \neq \bar{\mathfrak{p}}$. Since $\mathcal{O}_K = \mathbb{Z}[\omega]$ is a principal ideal domain, $\mathfrak{p} = (\pi)$ and $\bar{\mathfrak{p}} = (\bar{\pi})$ for a prime element $\pi \in \mathbb{Z}[\omega]$ with $N_{K/\mathbb{Q}}(\pi) = \pi\bar{\pi} = p$. If we write $\pi = a + b\omega$, then $p = \pi\bar{\pi} = a^2 - ab + b^2$. Since $\mathbb{Z}[\omega]/\mathfrak{p} = \mathbb{F}_p$, the power residue symbols

$$\chi_\pi := \left(\frac{\cdot}{\pi}\right)_3, \quad \chi_{\bar{\pi}} := \left(\frac{\cdot}{\bar{\pi}}\right)_3 : \mathbb{F}_p^{\times} \to \mathbb{\mu}_3$$

are cubic Dirichlet characters modulo p.

Lemma 3.5.5 *We have $\chi_{\bar{\pi}} = \chi_\pi^{-1}$. Hence $\chi_\pi, \chi_{\bar{\pi}}$ are precisely the two distinct cubic Dirichlet characters modulo p.*

Proof: The characters χ_π and $\chi_{\bar{\pi}}$ are determined by their values on the intergers. For $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod p$ we have

$$\chi_\pi(a) \equiv a^{(p-1)/3} \pmod{\pi},$$

by definition. Applying complex conjugation we obtain

$$\overline{\chi_\pi(a)} \equiv a^{(p-1)/3} \pmod{\bar{\pi}}.$$

We conclude that $\chi_{\bar{\pi}} = \overline{\chi_\pi} = \chi_\pi^{-1}$, proving the lemma. □

Let us now assume that $p \equiv 2 \pmod 3$. Then $(p) \lhd \mathbb{Z}[\omega]$ is a prime ideal with $N((p)) = p^2$. The residue field $\mathbb{F}_{p^2} := \mathbb{Z}[\omega]/(p)$ is a field with p^2 elements. Therefore, the power residue symbol gives us a canonical choice of a cubic character

$$\chi_p := \left(\frac{\cdot}{p}\right) : \mathbb{F}_{p^2}^\times \to \mu_3.$$

Remark 3.5.6 If $p \equiv 2 \pmod 3$, then the restriction of χ_p to the field $\mathbb{F}_p$ is the principal character, i.e. $\chi_p(a) = 1$ for all $a \in \mathbb{F}_p$. To see this, note that

$$a^{(p^2-1)/3} = (a^{p-1})^{(p+1)/3} \cong 1 \pmod p,$$

by Fermat's little theorem.

Definition 3.5.7 An element $\alpha \in \mathbb{Z}[\omega]$ is called *primary* if $\alpha \equiv 2 \pmod 3$.

Lemma 3.5.8 *Let $\alpha \in \mathbb{Z}[\omega]$ be a nonunit, relatively prime to 3. Then exactly one of the six associates of α is primary. In other words: the principal ideal $(\alpha) \lhd \mathbb{Z}[\omega]$ has a unique primary generator.*

Proof: The six associates of α are

$$\pm\alpha, \pm\omega\alpha, \pm\omega^2\alpha.$$

Let us write $\alpha = a + b\omega$. Then α is relatively prime to 3 if and only if

$$N_{K/\mathbb{Q}}(\alpha) = a^2 - ab + b^2 \not\equiv 0 \pmod 3.$$

Since $(a+b)^2 \equiv a^2 - ab + b^2 \pmod 3$, it follows that $a \not\equiv -b \pmod 3$. Consider the three associates

$$\alpha = a + b\omega, \quad \omega\alpha = -b + (a-b)\omega, \quad \omega^2\alpha = (b-a) - a\omega.$$

Since $a \not\equiv -b \pmod 3$, exactly one of the three numbers $b, a-b, -a$ is $\equiv 0 \pmod 3$. Therefore, exactly one of the three associates $\alpha, \omega\alpha, \omega^2\alpha$ is $\equiv c \pmod 3$ for an integer $c \in \mathbb{Z}$. Then $c \equiv \pm 1 \pmod 3$, and hence exactly one of the six associates of α is primary. □

As an elementary consequence we have the following variant of Theorem 1.3.1 (iii).

Corollary 3.5.9 *Let p be a prime number. Then $p \equiv 1 \pmod 3$ if and only if there exist integers A, B such that*

$$4p = A^2 + 27B^2.$$

Proof: Let $\pi = a + b\omega$ be a prime element of $\mathbb{Z}[\omega]$ with norm p. By the lemma we may assume that $\pi \equiv 2 \pmod 3$, which means that $a \equiv -1 \pmod 3$ and $b \equiv 0 \pmod 3$. Therefore,

$$2\pi = (2a - b) + b\sqrt{-3} = A + 3B\sqrt{-3},$$

with $A := 2a - b$, $B := b/3$. Taking the norm on both sides we obtain the identity $4p = A^2 + 27B^2$. This proves one direction of the corollary. The other direction is obvious. □

Theorem 3.5.10 (Law of cubic reciprocity) *Let $\pi, \lambda \in \mathbb{Z}[\omega]$ be two primary prime elements. Assume that $N(\pi) \neq N(\lambda)$ and that $N(\pi), N(\lambda) \neq 3$. Then*

$$\left(\frac{\lambda}{\pi}\right)_3 = \left(\frac{\pi}{\lambda}\right)_3.$$

Proof: The prime elements π, λ can be rational or complex primes. By symmetry, there are three cases to consider.

In the first case $\pi = p$ and $\lambda = \ell$ are both rational primes. Then $p, \ell \equiv 2 \pmod 3$. By Remark 3.5.6,

$$\left(\frac{p}{\ell}\right)_3 = \left(\frac{\ell}{p}\right)_3 = 1.$$

So the theorem is true in this case.

We may therefore assume that one of the two prime elements, say π, is not rational. Then $p := \pi\bar{\pi}$ is a prime number, $\equiv 1 \pmod 3$. Write $\chi_\pi := \left(\frac{\cdot}{\pi}\right)_3 : \mathbb{F}_p^\times \to \mu_3$; this is a cubic Dirchlet character modulo p.

Lemma 3.5.11 *Let $g(\chi_\pi) = \sum_x \chi_\pi(x)\zeta_p^x$ be the cubic Gauss sum associated to χ_π.*

(i) *We have*

$$g(\chi_\pi)^3 = p\pi.$$

(ii) *Let $L := K[g(\chi_\pi)]$ be a extension of K generated by $g(\chi_\pi)$. Then L is an abelian number field. More precisely,*

$$L = \mathbb{Q}[\zeta_{3p}]^H,$$

where

$$H \subset \{a \in (\mathbb{Z}/3p\mathbb{Z})^\times \mid a \equiv 1 \pmod 3,\ \chi_\pi(a) = 1\}.$$

(iii) *Let $a \in (\mathbb{Z}/3p\mathbb{Z})^\times$ be given, with $a \equiv 1 \pmod 3$. Let $\sigma_a \in \mathrm{Gal}(L/\mathbb{Q})$ denote the corresponding element. Then*

$$\sigma_a(g(\chi_\pi)) = \chi_\pi(a)^{-1} \cdot g(\chi_\pi).$$

Remark 3.5.12 We note that the relative extension L/K is also a Galois extension with abelian Galois group. In fact,

$$\mathrm{Gal}(L/K) \cong \mathbb{F}_p^\times / H',$$

where

$$H' = \{a \in \mathbb{F}_p^\times \mid \chi_\pi(a) = 1\}.$$

We may therefore apply Corollary 3.4.10 to the extension L/K. As usual, we will write $\sigma_a \in \mathrm{Gal}(L/K)$ for the element corresponding to $aH' \in \mathbb{F}_p^\times / H$.

Let us now assume that $\ell \equiv 2 \pmod 3$. Then $\mathfrak{l} := (\ell) \lhd \mathcal{O}_K$ is a prime ideal with $N(\mathfrak{l}) = l^2$. Therefore, by Corollary 3.4.10, we have

$$\mathrm{Frob}_\mathfrak{l} = \sigma_{\ell^2}.$$

Combined with Lemma 3.5.11 (iii), this shows that

$$\chi_\pi(\ell^2)^{-1} g(\chi_\pi) = \mathrm{Frob}_\mathfrak{l}(g(\chi_\pi)) \equiv g(\chi_\pi)^{\ell^2} \pmod \ell. \tag{143}$$

Dividing by $g(\chi_\pi)$ and using Lemma 3.5.11 (i) yields

$$\chi_\pi(\ell^2)^{-1} \equiv g(\chi_\pi)^{\ell^2 - 1} \equiv (p\pi)^{(l^2-1)/3} \equiv \left(\frac{p\pi}{\ell}\right)_3 \pmod \ell. \tag{144}$$

Since $\chi_\pi = \left(\frac{\cdot}{\pi}\right)_3$ is a cubic character, we deduce the identity

$$\left(\frac{\ell}{\pi}\right)_3 = \chi_\pi(\ell^2)^{-1} = \left(\frac{p\pi}{\ell}\right)_3 = \left(\frac{p}{\ell}\right)_3 \left(\frac{\pi}{\ell}\right)_3. \tag{145}$$

It follows from Remark **??** that $\left(\frac{p}{\ell}\right)_3 = 1$. Therefore, (145) shows that

$$\left(\frac{\ell}{\pi}\right)_3 = \left(\frac{\pi}{\ell}\right)_3,$$

proving the law of cubic reciprocity in this where π is a complex and $\lambda = \ell$ is a rational prime.

It remains to consider the case where both π and λ are complex primes. Then $\ell := \lambda\bar{\lambda}$ is a rational prime, $\ell \equiv 1 \pmod 3$. Since $(\lambda) \lhd \mathcal{O}_K$ is a prime ideal with $N((\lambda)) = \ell$, Corollary 3.4.10 shows that

$$\mathrm{Frob}_\lambda = \sigma_\ell.$$

By the same argument as in the previous case (see (143)–(145)) we obtain the identity

$$\left(\frac{\ell}{\pi}\right)_3^{-1} = \left(\frac{p}{\lambda}\right)_3 \left(\frac{\pi}{\lambda}\right)_3. \tag{146}$$

Reversing the roles of λ and π we obtain

$$\left(\frac{p}{\lambda}\right)_3^{-1} = \left(\frac{\ell}{\pi}\right)_3 \left(\frac{\lambda}{\pi}\right)_3. \tag{147}$$

Combining (146) and (147) we get

$$\left(\frac{\ell}{\pi}\right)_3 = \left(\frac{p}{\lambda}\right)_3^{-1} \left(\frac{\pi}{\lambda}\right)_3^{-1} = \left(\frac{\ell}{\pi}\right)_3 \left(\frac{\lambda}{\pi}\right)_3 \left(\frac{\pi}{\lambda}\right)_3^{-1}. \tag{148}$$

Rearranging and dividing by $\left(\frac{\ell}{\pi}\right)_3$ we conclude that

$$\left(\frac{\lambda}{\pi}\right)_3 = \left(\frac{\pi}{\lambda}\right)_3.$$

The proof of the theorem is now complete. □

Corollary 3.5.13 *A prime number p is of the form*

$$p = x^2 + 27y^2, \qquad x, y \in \mathbb{Z},$$

if and only if $p \equiv 1 \pmod 3$ and 2 is a cubic residue modulo p (i.e. the congruence $x^3 \equiv 2 \pmod p$ is solvable in $\mathbb{Z}$).

Proof: We may assume that $p \neq 3$. By Theorem 1.3.1 (iii) we know that p is of the form $p = x^2 + 3y^2$ if and only $p \equiv 1 \pmod 3$. Hence we may assume that $p \equiv 1 \pmod 3$, and then all we have to show is that $y \equiv 0 \pmod 3$ if and only if 2 is a cubic residue modulo p.

Let $\pi = a + b\omega$ be a primary prime divisor of p. As in the proof of Corollary 3.5.9, we have

$$4p = A^2 + 27B^2,$$

where $A := 2a - b$ and $B := b/3$. We see that p can be written as $p = x^2 + 27y^2$ if and only if A and B are even.

By Remark 3.5.14 (iii), 2 is a cubic residue modulo p if and only if $\left(\frac{2}{\pi}\right)_3 = 1$. Applying Theorem 3.5.10 we see that 2 is a cubic residue modulo p if and only if

$$\left(\frac{\pi}{2}\right)_3 = \left(\frac{2}{\pi}\right)_3 = 1. \tag{149}$$

By Remark 3.5.14 (iv) this holds if and only if

$$\pi \equiv 1 \pmod 2,$$

i.e. $a \equiv 1$, $b \equiv 0 \pmod 2$. This equivalent to $A = 2a - b$ and $B = b/3$ being even. The proof is now complete. □

Remark 3.5.14 For a prime p with $p \equiv 2 \pmod 3$, *every* integer a prime to p is a cubic residue modulo p. Therefore, Corollary 3.5.13 may be reformulated as follows. For $p \neq 3$, 2 is a cubic residue modulo p if and only if one of the following conditions hold:

(a) $p \equiv 2 \pmod 3$, or

(b) $p \equiv 1 \pmod 3$, and p is of the form $p = x^2 + 27y^2$.

It can be shown that (b) is not a 'congruence condition'. More precisely, there does not exist an integer N such that (b) only depends on the residue class of p modulo N.

4 Zeta- and L-functions

4.1 Riemann's ζ-function

For $s \in \mathbb{C}$ with $\Re(s) > 1$ we set

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s}. \tag{150}$$

If $\sigma = \Re(s) \geq 1 + \delta$, with $\delta > 0$, then

$$\sum_{n \geq 1} |n^{-s}| \leq \sum_{n \geq 1} n^{-1-\delta} < \infty.$$

Therefore, the series defining $\zeta(s)$ converges absolutely and locally uniformly on the domain $\{s \in \mathbb{C} \mid \Re(s) > 1\}$. Hence $\zeta(s)$ is an analytic function, called the *Riemann ζ-function*.

This function has first been studied by Euler because of its connection with the distribution of prime numbers. The connection to prime numbers is made via the following *Euler product formula*. This formula encodes the Fundamental Theorem of Arithmetic by an analytic identity, enabling us to use analytic tools to study prime numbers.

Lemma 4.1.1 *We have the following product formula for $\zeta(s)$:*

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}.$$

Here p runs over all prime numbers.

Proof: We first show that the infinite product

$$E(s) := \prod_{p} \frac{1}{1 - p^{-s}}$$

converges absolutely for $\Re(s) > 1$. To see this, we compute its logarithm:

$$\log E(s) = \sum_{p} -\log(1 - p^{-s}) = \sum_{p} \sum_{k \geq 1} \frac{p^{-ks}}{k}. \tag{151}$$

For $\Re(s) \geq 1 + \delta$, the series on the right hand side has

$$\sum_{p} \sum_{k \geq 1} p^{-1-\delta} = \sum_{p} \frac{1}{p^{1+\delta} - 1} \leq 2 \sum_{p} \frac{1}{p^{1+\delta}}$$

as a convergent majorant, proving our claim.

Fix a positive integer N and let $p_1, p_2, \ldots, p_r$ be the prime numbers $p \leq N$. Then the Fundamental Theorem of Arithmetic shows that

$$\begin{aligned} \prod_{p \leq N} \frac{1}{1-p^{-s}} &= \prod_{p \leq N} (1 + p^{-s} + p^{-2s} + \ldots) \\ &= \sum_{k_1, \ldots, k_r \geq 0} (p_1^{k_1} \cdot \ldots \cdot p_r^{k_r})^{-s} = \sum_n{}' n^{-s}, \end{aligned} \tag{152}$$

where $\sum_n'$ is the sum over all positive integers n all of whose prime factors are $\leq N$. It follows that

$$|\zeta(s) - \prod_{p \leq N} \frac{1}{1-p^{-s}}| \leq \sum_{n > N} n^{-\sigma}. \tag{153}$$

Since the series defining $\zeta(s)$ converges absolutely, the right hand side of (153) tends to 0 for $N \to \infty$. We conclude that

$$\zeta(s) = \lim_{N \to \infty} \prod_{p \leq N} \frac{1}{1-p^{-s}} = \prod_p \frac{1}{1-p^{-s}}.$$

□

It is well known that the series $\zeta(1) = \sum_n n^{-1}$ diverges. The following lemma gives us some control over the divergence.

Lemma 4.1.2 *Assume that $s > 1$. Then*

$$\lim_{s \to 1} (s-1)\zeta(s) = 1.$$

Proof: Since t^{-s} is strictly decreasing for $t > 0$, we have

$$(n+1)^{-s} < \int_n^{n+1} t^{-s} dt < n^{-s},$$

for all $n \geq 1$. Summing over all n shows that

$$\zeta(s) - 1 < \int_1^{\infty} t^{-s} dt = (s-1)^{-1} < \zeta(s).$$

Multipliplying with $(s-1)$ gives

$$(s-1)\zeta(s) - s + 1 < 1 < (s-1)\zeta(s),$$

and the lemma follows immediately. □

Theorem 4.1.3 (Euler) *The series*

$$\sum_p \frac{1}{p}$$

diverges.

Proof: If f and g are two continous functions on $\mathbb{R}_{>1}$ then we shall write $f \sim g$ if $|f(s) - g(s)|$ remains bounded for $s \to 1$. We first look at the logarithm of the Euler product and obtain (as in the proof of Lemma 4.1.1)

$$\log \zeta(s) = \sum_p \sum_{k \geq 1} \frac{p^{-ks}}{k} = \sum_p p^{-s} + R(s),$$

where

$$R(s) = \sum_p p^{-2s} \sum_{k \geq 0} \frac{p^{-ks}}{k+2} \leq \sum_p p^{-2s} \sum_{k \geq 0} p^{-ks} \leq 2 \sum_p p^{-2s}.$$

Since the series $\sum_p p^{-2}$ converges, $R(s)$ remains bounded for $s \to 1$. Therefore, $\log \zeta(s) \sim \sum_p p^{-s}$. On the other hand, Lemma 4.1.2 implies that $\zeta(s) \sim (s-1)^{-1}$. Therefore,

$$\sum_p p^{-s} \sim \log \zeta(s) \sim -\log(s-1)$$

tends to infinity for $s \to 1$. We conclude that the series $\sum_p p^{-1}$ diverges. □

For the rest of this section we give a few hints at why the Riemann ζ-functions plays such an important role in analytic number theory. We will not give any proofs, which may be found in any book on analytic number theory.

As a very special corollary of Theorem 4.1.3 we get a new proof of the well known fact that there exist infinitely many primes. But actually, we get a much stronger, qualitative result about the density of the primes inside the natural numbers. For instance, since the series $\sum_n n^2$ converges, Theorem 4.1.3 says that 'there are more primes numbers than squares'.

A much more precise result is the *Prime Number Theorem*.

Theorem 4.1.4 *Let $\pi(x)$ denote the number of primes $p \leq x$. Then*

$$\pi(x) \sim \frac{x}{\log x},$$

meaning that the function $\pi(x) \log(x)/x$ tends to 1 for $x \to \infty$.

A useful heuristic interpretation of the Prime Number Theorem is to say that 'the probability that a randomly chosen large integer n is prime is equal to $1/\log(n)$'. Indeed, using this heuristic one may predict that the number of primes $p \leq x$ is roughly equal to

$$\mathrm{Li}(x) := \int_2^x \frac{dt}{\log t},$$

and it is easy to see that

$$\mathrm{Li}(x) \sim \frac{x}{\log x}.$$

In fact, the function $\mathrm{Li}(x)$ gives an even better asymptotics for $\pi(x)$ than $x/\log(x)$.

The Prime Number Theorem was conjectured by Gauss on the basis of numerical evidence. It took over ?? years until the first proof was given by Hadamard in ??, but the main strategy of the proof was devised by Riemann. In his famous paper [**?**] he studies the distribution of the prime numbers using $\zeta(s)$. Among other things, he proved the following result.

Theorem 4.1.5 *The function $\zeta(s)$ has an analytic continuation to $\mathbb{C} - \{1\}$, with a simple pole at $s = 1$. Moreover, $\zeta(s)$ satisfies the functional equation*

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos(\pi s/2)\zeta(s). \tag{154}$$

Here

$$\Gamma(s) := \int_0^\infty e^{-y}y^s\frac{dy}{y}$$

is Euler's Γ-function, defined for $\Re(s) > 0$.

Because of the Euler product (Lemma 4.1.1), $\zeta(s) \neq 0$ for $\Re(s) > 1$. Since $\Gamma(s) \neq 0$ for $\Re(s) > 1$ as well, the functional equation (154) shows that

$$\zeta(-2k) = 0, \qquad k = 1, 2, \ldots.$$

These are the so-called *trivial zeroes* of $\zeta(s)$. The same argument shows that all nontrivial zeroes lie in the *critical strip*

$$\{s \in \mathbb{C} \mid 0 \leq \Re(s) \leq 1\}.$$

Moreover, if ρ is a nontrivial zero, then $1 - \rho$ is a zero as well.

Using methods from complex analysis, Riemann proved his *explicit formula* relating the distribution of the prime numbers to the nontrivial zeroes of $\zeta(s)$. From this formula one sees that the prime number theorem holds if and only if $\zeta(s) \neq 0$ if $\Re(s) = 1$, i.e. if no zero lies on the boundary of the critical strip. It is in this way that the Prime Number Theorem was finally proved.

In the same paper, Riemann formulated the following conjecture, which remains open and is generally considered as the most famous problem in mathematics.

Conjecture 4.1.6 (The Riemann Hypothesis) *All nontrivial zeroes of $\zeta(s)$ have real part $\Re(s) = 1/2$.*

4.2 Dirichlet series

The Riemann ζ-function is just the prototype of a class of functions which we will now discuss.

Definition 4.2.1 Let $(a_n)_{n\geq 1}$ be a sequence of complex numbers. Then the series

$$F(s) := \sum_{n\geq 1} \frac{a_n}{n^s}, \qquad s \in \mathbb{C},$$

is called the *Dirichlet series* attached to (a_n).

Lemma 4.2.2 *Assume that $F(s_0)$ converges for some $s_0 \in \mathbb{C}$. Then $F(s)$ converges uniformly on every region of the form $\Re(s-s_0) \geq 0$, $\arg(s-s_0) \leq \alpha$, with $\alpha < \pi/2$.*

Proof: We note that

$$F(s-s_0) = \sum_{n\geq 1} \frac{n^{s_0} a_n}{n^s} = \sum_{n\geq 1} \frac{\tilde{a}_n}{n^s}$$

is again a Dirichlet series. Therefore, we may assume that $s_0 = 0$. Now our assumption means that the sum $\sum_n a_n$ converges. We set

$$A_N := \sum_{n=1}^{N}, \quad A_{M,N} := \sum_{n=M}^{N} a_n$$

for $1 \geq M \leq N$. Partial summation shows that

$$\sum_{n=M}^{N} a_n n^{-s} = \sum_{n=M}^{N-1} A_{M,n}(n^{-s} - (n+1)^{-s}) + A_{M,N} N^{-s}. \tag{155}$$

Let $\epsilon > 0$ be given. Since the sum $\sum_n a_n$ converges, there exists N_0 such that

$$|A_{M,N}| < \epsilon, \qquad \text{for all } N \geq M \geq N_0.$$

So (155) shows that for $\Re(s) \geq 0$ we have

$$|\sum_{n=M}^{N} a_n n^{-s}| \leq \epsilon \sum_{n=M}^{N-1} |n^{-s} - (n+1)^{-s}| + \epsilon. \tag{156}$$

Write $\sigma = \Re(s)$. Then

$$|n^{-s} - (n+1)^{-s}| = |s| \int_n^{n+1} \frac{dx}{x^{\sigma+1}}$$

and therefore

$$\sum_{n=M}^{N-1} |n^{-s} - (n+1)^{-s}| = |s| \int_M^N \frac{dx}{x^{\sigma+1}} \leq \frac{|s|}{\sigma}(M^{-\sigma} - N^{-\sigma}) \leq 2\frac{|s|}{\sigma}.$$

Plugging this estimate into (156) we obtain

$$|\sum_{n=M}^{N} a_n n^{-s}| \leq \epsilon(2\frac{|s|}{\sigma} + 1).$$

Since $|s|/\sigma$ is bounded on every region of the form $\sigma = \Re(s) \geq 0$, $\arg(s) \leq \alpha$, with $\alpha < \pi/2$, the lemma follows. □

Corollary 4.2.3 *The domain of convergence of $F(s)$ contains a maximal open half plan $\{s \in \mathbb{C} \mid \Re(s) > \sigma_c\}$, for some $\sigma_c \in [-\infty, \infty]$. Moreover, $F(s)$ defines a holomorphic function on this region.*

Definition 4.2.4 We call σ_c the *abscissa of convergence* and $\{s \in \mathbb{C} \mid \Re(s) > \sigma_c\}$ the *half plane of convergence* of the Dirichlet series $F(s)$. (If $\sigma = -\infty$ (resp. $\sigma_c = \infty$) we mean that $F(s)$ converges everywhere (resp. nowhere).)

The abscissa of convergence of the Dirichlet series $\sum_n |a_n| n^{-s}$ is called the *abscissa of absolute convergence*. We denote it by σ_a.

Example 4.2.5 The Riemann ζ-function $\zeta(s) = \sum_n n^{-1}$ is a Dirichlet series with $\sigma_c = \sigma_a = 1$.

Lemma 4.2.6 *Suppose that the partial sums*

$$A_{M,N} = \sum_{n=M}^{N} a_n$$

are bounded, independently of M, N. Then $\sigma_c \leq 0$, i.e. $F(s)$ converges for $\Re(s) > 0$.

Proof: Let $C > 0$ be a constant such that $|A_{M,N}| \leq C$, and let $s > 0$. Using partial summation as in the proof of Lemma 4.2.2 we see that

$$|\sum_{n=M}^{N} a_n n^{-s}| \leq C \sum_{n=M}^{N-1} (n^{-s} - (n+1)^{-s}) + CN^{-s} = CM^{-s}.$$

For a fixed $s > 0$, this converges to zero if M goes to infinity. Therefore, $F(s)$ converges for all $s > 0$. By Lemma 4.2.2 it follows that $F(s)$ converges in the half plane $\Re(s) > 0$. □

Example 4.2.7 The Dirichlet η-function is defined by the series

$$\eta(s) := \sum_{n \geq 1} \frac{(-1)^{n-1}}{n^s} = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \dots.$$

Using Lemma 4.2.6 it is easy to see that $\eta(s)$ converges on the half plane $\Re(s) > 0$. On the other hand, the series

$$\eta(0) = 1 - 1 + 1 - 1 + \dots$$

is divergent. It follows that the abscissa of convergence is $\sigma_c = 0$. Note that the convergence of $\eta(s)$ is not absolute unless $\Re(s) > 1$.

The function $\eta(s)$ is closely related to Riemann's $\zeta(s)$. In fact, for $\Re(s) > 1$ we have

$$\begin{aligned}\eta(s) &= \Big(1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots\Big) - 2\Big(\frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{4^s} + \dots\Big) \\ &= (1 - 2^{1-s})\zeta(s).\end{aligned} \tag{157}$$

Since $\eta(s)$ is convergent for $\Re(s) > 0$,

$$\zeta(s) := (1 - 2^{1-s})^{-1}\eta(s)$$

defines an analytic continuation of $\zeta(s)$ to the half plane $\Re(s) > 0$, with a simple pole at $s = 1$. In particular, this gives a new proof of Lemma 4.1.2.

Definition 4.2.8 A series $(a_n)_{n\in\mathbb{N}}$ is called *multiplicative* if

$$a_{mn} = a_m a_n$$

holds for all pairs of relatively prime integers $n, m \in \mathbb{N}$. If it holds for all pairs of integers, then we call (a_n) *strongly multiplicative*.

Proposition 4.2.9 *Let $(a_n)_{n\in\mathbb{N}}$ be a bounded series of complex numbers and $F(s) = \sum_n a_n n^{-s}$ the associated Dirichlet series.*

(i) *If (a_n) is multiplicative, then we have an Euler product formula*

$$F(s) = \prod_p F_p(s),$$

valid for $\Re(s) > 1$, where

$$F_p(s) := \sum_{k\geq 0} \frac{a_{p^k}}{p^{ks}}.$$

(ii) *If, moreover, (a_n) is strongly multiplicative, then*

$$F_p(s) = \frac{1}{1 - a_p p^{-s}}.$$

Proof: (cf. the proof of Lemma 4.1.1) Since (a_n) is bounded, the series $F(s)$ converges absolutely for $\Re(s) > 1$. Then the series $F_p(s)$, being a subseries of $F(s)$, is absolutely convergent as well. Let S be a finite set of prime numbers, and let $\mathbb{N}(S)$ denote the set of integers n all of whose prime divisors lie in S. Using the assumption that (a_n) is multiplicative, we see that

$$\prod_{p\in S} F_p(s) = \prod_{p\in S} \sum_{k\geq 0} \frac{a_{p^k}}{p^{ks}} = \sum_{n\in\mathbb{N}(S)} \frac{a_n}{n^s}.$$

As S increases, the right hand side tends to $F(s)$. This proves (i). If (a_n) is strongly multiplicative, then $a_{p^k} = a_p^k$. So the boundedness of a_n implies that $|a_p| \leq 1$ and then

$$F_p(s) = \sum_{k \geq 0} (a_p n^{-s})^k = \frac{1}{1 - a_p p^{-s}}.$$

□

Dirichlet L-series

Recall from Definition 3.3.9 that a function

$$\chi : \mathbb{Z} \to \mathbb{C}$$

is called a *Dirichlet character* with modulus $m \in \mathbb{N}$ if the following conditions hold.

(a) χ is strongly multiplicative, i.e. $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$.

(b) $\chi(a)$ depends only on the residue class of a in $\mathbb{Z}/m\mathbb{Z}$,

(c) $\chi(a) = 0$ if and only if $\gcd(a, nm) \neq 1$.

Recall also that a Dirichlet character modulo m is uniquely determined by a character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.

Definition 4.2.10 The Dirichlet series

$$L(\chi, s) := \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

is called the L-series of the Dirichlet character χ.

Since the $(\chi(n))_{n \in \mathbb{N}}$ is bounded and strongly multiplicative, we have the Euler product formula

$$L(\chi, s) = \prod_p \frac{1}{1 - \chi(p)p^{-s}}, \tag{158}$$

valid for $\Re(s) > 1$, by Proposition 4.2.9. If $\chi = \epsilon$ is the principal character modulo m, then

$$L(\epsilon, 1) = \sum_{\gcd(n,m)=1} \frac{1}{n}$$

diverges. On the other hand, if $\chi \neq \epsilon$, then $\chi(1) + \ldots + \chi(m) = 0$ by Theorem 3.3.5 (i). It follows that

$$A_N = \sum_{n=1}^{N} \chi(n) = \lfloor \frac{N}{m} \rfloor \cdot \sum_{a=1}^{m} \chi(a) + \sum_{a=1}^{r} \chi(a) = \sum_{a=1}^{r} \chi(a),$$

with $0 \leq r < m$. In particular, A_N is bounded. By Lemma 4.2.6 this shows that $L(\chi, s)$ converges for $\Re(s) > 0$. In particular, the value

$$L(\chi, 1) = \sum_{n \geq 1} \frac{\chi(n)}{n}$$

is well defined.

Example 4.2.11 Let χ be the unique quadratic character modulo 4, i.e.

$$\chi(n) = \begin{cases} 1, & n \equiv 1 \pmod 4, \\ -1, & n \equiv 3 \pmod 4, \\ 0, & n \equiv 0 \pmod 2. \end{cases}$$

Then

$$L(\chi, s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots$$

converges for $\Re(s) > 0$, and for $\Re(s) > 1$ we have the Euler product

$$L(\chi, 1) = \frac{1}{(1 + 3^{-s})(1 - 5^{-s})(1 + 7^{-s})(1 + 11^{-s}) \cdots}.$$

A well known result due to Leibniz says that

$$L(\chi, 1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots = \frac{\pi}{4}.$$

We will prove this formula in the next section.

The ζ-function of a number field

Definition 4.2.12 Let K be an algebraic number field. The Dedekind ζ-function of K is defined as the series

$$\zeta_K(s) := \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$

where $\mathfrak{a} \lhd \mathcal{O}_K$ runs over all nonzero ideals of $\mathcal{O}_K$.

Clearly, if $K = \mathbb{Q}$ then $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ is simply the Riemann ζ-function. In general, we can rewrite $\zeta_K(s)$ as a Dirichlet series

$$\zeta_K(s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

where

$$a_n := |\{\mathfrak{a} \lhd \mathcal{O}_K \mid N(\mathfrak{a}) = n\}|$$

is the number of ideals with norm n. This works because a_n is a finite number, see Exercise 2.5.7.

Theorem 4.2.13 *The series $\zeta_K(s)$ converges on the half plane $\Re(s) > 1$, and in this region we have an Euler product formula like so:*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

Here $\mathfrak{p} \lhd \mathcal{O}_K$ runs over all nonzero prime ideals of $\mathcal{O}_K$.

Proof: The proof has two crucial ingredients. The first is Theorem 2.5.14 which says that every nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ has a unique factorization as a product of prime ideals,

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_r^{k_r}. \tag{159}$$

So at least formally, we can prove the Euler product formula exactly as for $\zeta(s)$:

$$\prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \prod_{\mathfrak{p}} \sum_{k \geq 0} N(\mathfrak{p})^{-ks} = \sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_r \\ k_1, \ldots, k_r \geq 1}} \prod_{i=1}^{r} N(\mathfrak{p}_i)^{-k_i s}$$
$$= \sum_{\substack{\mathfrak{p}_1, \ldots, \mathfrak{p}_r \\ k_1, \ldots, k_r \geq 1}} N(\mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_r^{k_r})^{-s} \overset{(159)}{=} \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} = \zeta_K(s).$$

To see that this formal manipulation makes sense for $\Re(s) > 1$, it suffices to show that the infinite product over all prime ideals converges absolutely. To do this, it suffices to show that the following sum converges absolutely (cf. the proof of Lemma 4.1.1):

$$\log\left(\prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}\right) = -\sum_{\mathfrak{p}} \sum_{k \geq 1} \frac{N(\mathfrak{p})^{-ks}}{k}. \tag{160}$$

Now we have to use the second main ingredient. The fundamental equality (72) implies that for a fixed prime number p, there at most $N := [K : \mathbb{Q}]$ prime ideals $\mathfrak{p} \mid p$, and for such a $\mathfrak{p}$ we have $N(\mathfrak{p}) \geq p$. This shows that the sum

$$N \log \zeta(s) = N \sum_{p} \sum_{k \geq 1} \frac{p^{-ks}}{k}$$

is an absolutely convergent majorant for the sum (160). The theorem is now proved. □

Remark 4.2.14 It is intersting to compare Theorem 4.2.13 with Proposition 4.2.9. The unique prime factorization in $\mathcal{O}_K$ shows that the sequence (a_n), where a_n is the number of ideals of $\mathcal{O}_K$ with norm n, is multiplicative. By Proposition 4.2.9 we have an Euler product formula

$$\zeta_K(s) = \prod_{p} F_p(s),$$

valid in the half plane of absolute convergence. Theorem 4.2.13 is much more precise. It shows that $\zeta_K(s)$ is absolutely convergent for $\Re(s) > 1$, but it also says that

$$F_p(s) = \prod_{\mathfrak{p}|p} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

We see that in general, the local Euler factor at p is not of the form $1/(1-a_p p^{-s})$, as in Proposition 4.2.9.

Example 4.2.15 Let $K = \mathbb{Q}[i]$ be the field of Gaussian numbers. There are three kinds of prime ideals in $\mathcal{O}_K = \mathbb{Z}[i]$:

(i) $\mathfrak{p}_2 = (1+i)$ is the unique prime ideal dividing 2. In fact, $(2) = \mathfrak{p}_2^2$, so $N(\mathfrak{p}_2) = 2$.

(ii) For a prime number p such that $p \equiv 1 \pmod 4$ we have $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, and $\mathfrak{p}, \bar{\mathfrak{p}}$ are two prime ideals with norm p.

(iii) For a prime number p such that $p \equiv 3 \pmod 4$, (p) is a prime ideal with norm p^2.

Now we see that

$$\begin{aligned} \zeta_K(s) &= \frac{1}{1-2^{-s}} \prod_{p \equiv 1\,(4)} \frac{1}{(1-p^{-s})^2} \prod_{p \equiv 3\,(4)} \frac{1}{1-p^{-2s}} \\ &= \zeta(s) \prod_{p \equiv 1\,(4)} \frac{1}{1-p^{-s}} \prod_{p \equiv 3\,(4)} \frac{1}{1+p} \\ &= \zeta(s) \cdot L(\chi, s), \end{aligned} \tag{161}$$

where χ is the quadratic Dirichlet character modulo 4, see Example 4.2.11. This remarkable formula is a special case of Theorem 4.2.16 below.

By the way, if we write $\zeta_K(s)$ as a Dirichlet series, we get

$$\zeta_K(s) = \sum_{n \geq 1} \frac{a_n}{n^s} = 1 + 2^{-2} + 4^{-s} + 5^{-s} + 8^{-s} + 9^{-s} + ..,$$

where a_n is the number of ideals $\mathfrak{a} \lhd \mathbb{Z}[i]$ of norm n. Since $\mathbb{Z}[i]$ is a principal ideal domain, every ideal of norm n is of the form $\mathfrak{a} = (x+yi)$, where $(x, y) \in \mathbb{Z}$ is a solution of the quadratic equation $x^2 + y^2 = n$. The generator $x + yi$ of $\mathfrak{a}$ is unique up to multiplication with a unit, and he unit group has order 4, $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. It follows that

$$a_n = \frac{1}{4} |\{(x, y) \mid x^2 + y^2 = n\}|$$

is the number of representations of n as a sum of two squares, divided by 4.

The ζ-function of an abelian number field

Our main theorem in this section expresses the Dedekind ζ-function of an *abelian* number field as the product of Dirichlet L-functions. This translates our previous results about the splitting of primes in abelian number field (our main *reciprocity law*) into the analytic language of Dirichlet series. It will be our main tool to prove Dirichlet's prime number theorem.

Let K be an abelian number field. Recall that this means that $K \subset \mathbb{Q}[\zeta_n]$, for some $n \in \mathbb{N}$. By the main theorem of Galois theory, $K = \mathbb{Q}[\zeta_n]^H$, where

$$H \subset \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

is a subgroup of the Galois group of $\mathbb{Q}[\zeta_n]/\mathbb{Q}$. In the following, we will identify the two groups $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ via the isomorphism that sends a to the Galois automorphism σ_a determined by $\sigma_a(\zeta_n) = \zeta_n^a$ (see §**??**). Since $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ is abelian, H is a normal subgroup and hence $K/\mathbb{Q}$ is a Galois extension, with Galois group

$$G := \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})/H.$$

Let $\hat{G}$ denote the group of characters $\chi : G \to \mathbb{C}^\times$. Composing χ with the natural projection morphism

$$\pi : (\mathbb{Z}/n\mathbb{Z})^\times \to G \tag{162}$$

gives a character $\chi \circ \pi$ on the group $(\mathbb{Z}/n\mathbb{Z})^\times$. The map $\chi \mapsto \chi \circ \pi$ is an injective group homomorphism

$$\hat{G} \hookrightarrow \widehat{(\mathbb{Z}/n\mathbb{Z})^\times}.$$

We shall consider $\hat{G}$ from now on as a subgroup of $\widehat{(\mathbb{Z}/n\mathbb{Z})^\times}$ via this map. Since H is the kernel of π, a Dirichlet character modulo n is of the form $\chi \circ \pi$ if and only if its restriction to H is trivial. In this way we obtain an identification

$$\hat{G} = \{\ \chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^\times} \mid \chi(a) = 1\ \forall a \in H\}.$$

Recall that a character $\chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^\times}$ may be extended to a Dirichlet character $\chi : \mathbb{Z} \to \mathbb{C}^\times$. In the following theorem we use the convention that this extension is chosen to be *primitive*, see ??.

Theorem 4.2.16 *With the notation introduced above we have*

$$\zeta_K(s) = \prod_{\chi \in \hat{G}} L(\chi, s).$$

Proof: The functions $\zeta_K(s)$ and $L(\chi, s)$ have an Euler product (Theorem 4.2.13 and ??). Therefore it suffices to prove, for every prime number p, the following identity:

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \prod_{\chi \in \hat{G}} \frac{1}{1 - \chi(p)p^{-s}}. \tag{163}$$

We shall first assume that p does not divide n. In this case the proof is simpler and more transparent, for the following reason. The image

$$\varphi_p := \pi(p + n\mathbb{Z}) \in G$$

of the residue class of p in G via the projection (162) is the Frobenius element for the prime p with respect to the abelian extension $K/\mathbb{Q}$. Furthermore, by Corollary 3.4.9 the prime factorization of $(p) \lhd \mathcal{O}_K$ is of the form

$$(p) = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r,$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \lhd \mathcal{O}_K$ are pairwise distinct prime ideals of norm $N(\mathfrak{p}_i) = p^f$, and where f is the order of φ_p in G. The fundamental equality then shows that $r = |G|/f$. Therefore, the left hand side of (163) can be written as

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \frac{1}{(1 - p^{-fs})^r}. \tag{164}$$

Note that the denominator of the right hand side of (164) is a polynomial in p^{-s}. Now (163) follows from (164) and the following lemma.

Lemma 4.2.17 *Let G be a finite abelian group, $\sigma \in G$ an arbitrary element and $f := \mathrm{ord}_G(\sigma)$ the order of σ. Then*

$$\prod_{\chi \in \hat{G}} (1 - \chi(\sigma)x) = (1 - x^f)^r,$$

as an identity in the poylnomial ring $\mathbb{C}[x]$ and with $r := |G|/f$.

Proof: The map

$$\phi : \hat{G} \to \mathbb{\mu}_f, \qquad \chi \mapsto \chi(\sigma), \tag{165}$$

is clearly a group homomorphism. The proof of Proposition 3.3.3 shows that there exists $\chi \in \hat{G}$ such that $\chi(\sigma)$ is a primitive fth root of unity. In other words, ϕ is surjective and hence induces an isomorphism

$$\hat{G}/\ker(\phi) \cong \mathbb{\mu}_f.$$

It follows that

$$\prod_{\chi \in \hat{G}} (1 - \chi(\sigma)x) = \prod_{\zeta \in \mathbb{\mu}_f} (1 - \zeta x)^r, \tag{166}$$

where $r := |\ker(\phi)| = |G|/f$. On the other hand, it is clear that

$$\prod_{\zeta \in \mathbb{\mu}_f} (1 - \zeta x) = 1 - x^f.$$

Together with (166) this proves the lemma. □

So far we have proved the identity (163) only for $p \nmid n$. For the general case we write $n = p^k m$ such that $p \nmid m$. We may assume that $k \geq 1$, because we have already dealt with the case $k = 0$. Now the problem is that the Frobenius element φ_p is not an element of G but of a certain quotient group, defined as follows. By the Chinese Remainder Theorem we have a natural isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p^k\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times.$$

We consider the first factor $(\mathbb{Z}/p^k\mathbb{Z})^\times$ as a subgroup and the second factor $(\mathbb{Z}/m\mathbb{Z})^\times$ as a quotient of the group $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $I_p \subset G$ denote the image under the projection map (162) of the subgroup $(\mathbb{Z}/p^k\mathbb{Z})^\times$. We obtain a natural and surjective homomorphism

$$(\mathbb{Z}/m\mathbb{Z})^\times \to G/I_p, \qquad a + m\mathbb{Z} \mapsto \sigma_a I_p.$$

We define the *Frobenius element* with respect to p and the extension $K/\mathbb{Q}$ as the element $\varphi_p := \sigma_p I_p \in G/I_p$. The statement of Corollary 3.4.9 can be extended as follows. Let f denote the order of φ_p in G/I_p. Then the prime factorization of $(p) \lhd \mathcal{O}_K$ is of the form

$$(p) = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r)^e \tag{167}$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are pairwise distinct prime ideals of norm $N(\mathfrak{p}_i) = p^f$, and where $e = |I_p|$ and $r = |G|/ef$. It follows that (164) holds as before – we just had to be more careful with the definition of f and r.

To finish the proof we have to analyse the right hand side of (163). The subtle point is somewhat hidden by our notation. Given a character $\chi \in \hat{G}$ we temporarily denote its extension to a *primitive* Dirichlet character by $\tilde{\chi} : \mathbb{Z} \to \mathbb{C}$. Note also that we have an injective group homomorphism

$$\widehat{G/I_p} \hookrightarrow \hat{G}$$

which maps a character $\chi : G/I_p \to \mathbb{C}^\times$ to its composition with the projection $G \to G/I_p$. We shall consider $\widehat{G/I_p}$ as a subgroup of $\hat{G}$ via this homomorphism.

Claim: We have $\tilde{\chi}(p) \neq 0$ if and only if $\chi \in \widehat{G/I_p}$.

The claim may aslo be formulated as follows. Given $\chi \in \hat{G}$, there are two cases. In the first case $\tilde{\chi}(p) = 0$, and then the corresponding term in (163) is equal to one and can be ignored. In the second case we have $\tilde{\chi}(p) = \chi(\varphi_p)$ where $\varphi \in G/I_p$ is the Frobenius element. Therefore we can rewrite the right hand side of (163) as

$$\prod_{\chi \in \widehat{G/I_p}} \frac{1}{1 - \chi(\varphi_p)p^{-s}}.$$

Applying Lemma 4.2.17 to the group G/I_p and the element $\varphi \in G/I_p$ we see that

$$\prod_{\chi \in \widehat{G/I_p}} \frac{1}{1 - \chi(\varphi_p)p^{-s}} = \frac{1}{(1 - p^{-fs})^r},$$

where f, r are defined by (167). This proves the identity (163) for all prime numbers p and concludes the proof of Theorem 4.2.16. □

Exercises

Exercise 4.2.1 Let $\eta(s)$ be the Dirichlet η-function from Example 4.2.7. For $\Re(s) > 1$ we can use the absolute convergence of $\eta(s)$ to see that

$$\eta(s) = \frac{1}{2} + \frac{1}{2} \sum_{n \geq 1} (-1)^n (n^{-s} - (n+1)^{-s}). \tag{168}$$

(i) Use (157) and (168) to define an analytic continuation of $\eta(s)$ and $\zeta(s)$ to the half plane $\Re(s) > -1$.

(ii) Compute $\eta(0)$ and

$$\eta(-1) := \lim_{s > -1} \eta(s), \qquad \zeta(-1) := \lim_{s > -1} \zeta(s).$$

With the last part of the exercise we have, in some sense, computed a value for the divergent series

$$1 + 2 + 3 + 4 + \ldots!$$

4.3 Dirichlet's prime number theorem

4.4 The class number formula

5 Outlook: Class field theory

5.1 Frobenius elements

5.2 The Artin reciprocity law

References

[1] M. Artin. *Algebra*. Birkhäuser, 1991.

[2] G. Bergmann. Über Eulers Beweis des großen Fermatschen Satzes für den Exponenten 3. *Math. Annalen*, 164:159.175, 1966.

[3] D.A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*. Wiley, 1989.

[4] G. Fischer. *Lineare Algebra*. Vieweg & Teubner, 17th edition, 2010.

[5] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. Springer-Verlag, 1990.

[6] J. Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, 1992.

[7] S. Singh. *Fermats letzter Satz. Die abenteuerliche Geschichte eines mathematischen Rätsels*. Carl Hanser Verlag, 1998.

[8] L.C. Washington. *Introduction to Cyclotomic Fields*. Number 83 in GTM. Springer-Verlag, 2. edition, 1982.

[9] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Math.*, 142:443–551, 1995.