Math 345 – Algebraic number theory

Nicolas Mascot (nm116@aub.edu.lb)

(Lecture notes originally written
in collaboration with Aurel Page)

Version: October 7, 2022

Contents

Introduction: why algebraic number theory?

Consider the following statement, known today as Fermat's last theorem:

Theorem 0.0.1 (Wiles & al., 1994)**.** *Let $n \geqslant 3$ be an integer. Then the Diophantine equation*

$$x^n + y^n = z^n$$

has no nontrivial solution, i.e.

$$x^n + y^n = z^n, \ x, y, z \in \mathbb{Z} \Longrightarrow xyz = 0.$$

In 1847, while this theorem still had not been proved, the French mathematician Gabriel Lamé had an idea for the case where n is an odd prime. Suppose we have $x^n + y^n = z^n$ with x, y and z all nonzero integers, which we may assume are relatively prime. Let $\zeta = e^{2\pi i/n}$, so that $\zeta^n = 1$, and consider

$$\mathbb{Z}[\zeta] = \{P(\zeta), \ P \in \mathbb{Z}[x]\},$$

the smallest subring of $\mathbb{C}$ containing ζ. Then, in this ring, we have

$$x^n = z^n - y^n = \prod_{k=1}^{n} (z - \zeta^k y).$$

Lamé claimed that to conclude that each factor $z - \zeta^k y$ is an n^{th} power, it suffices to show that these factors are pairwise coprime. If this were true, then we would be able to find integers x', y' and z', smaller than x,y and z but all nonzero, such that $x'^n + y'^n = z'^n$; this would lead to an "infinite descent" and thus prove the theorem.

Unfortunately, Lamé's claim relied on the supposition that factorisation into irreducibles is unique, and while this is true in $\mathbb{Z}$, we now know that it need not be true in more general rings such as $\mathbb{Z}[\zeta]$. For instance, in the ring

$$\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5},\ a, b \in \mathbb{Z}\} \subset \mathbb{C},$$

we have the two different factorisations

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

where each factor is irreducible. Lamé was thus unable to justify his claim, and the theorem remained unproved for almost 150 years.

The numbers ζ and $i\sqrt{5}$ are examples of *algebraic numbers*. The goal of this course is to study the property of such numbers, and of rings such that $\mathbb{Z}[\zeta]$, so as to know what we are allowed to do with them, and what we are not. As an application, we will see how to solve certain Diophantine equations.

Preliminary reminders

I have gathered here some standard results that I expect you to know, and that I will use without proof in this course.

Notation

$\forall x$ means for all x. $\exists x$ means there exists (at least one) x. Finally, $\exists! x$ means there exists a unique x.

For instance, the statement

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : y > x$$

is true, whereas the statement

$$\exists y \in \mathbb{R} : \forall x \in \mathbb{R}, y > x$$

is **false**.

Let X and Y be sets. A map from X to Y will be written as

$$\begin{aligned} f : X &\longrightarrow Y \\ x &\longmapsto f(x). \end{aligned}$$

The product $X \times Y$ is the set of pairs (x, y) with $x \in X$ and $y \in Y$.

Groups, rings, ideals, fields, and quotients

A *group* is a set G with an operation $\cdot : G \times G \longrightarrow G$ and an element $e \in G$ such that $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ for all $g_1, g_2, g_3 \in G$, $g \cdot e = e \cdot g = g$ for all $g \in G$, and such that for all $g \in G$ there exists $g^{-1} \in g$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

An *isomorphism* between a group G and a group H is a map $\phi : G \longrightarrow H$ which is bijective and satisfies $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$ for all $g_1, g_2 \in G$.

The *order* of an element $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$, if it exists.

If G is finite then the cardinal of G is also called the *order*[1] of G.

Lagrange's theorem states that the order of any subgroup of G divides that of G. In particular, if $g \in G$ has order n, then n divides[2] the order of G, since the subgroup $\langle g \rangle$ of G generated by g is $\{g, g^2, \cdots, g^{n-1}, g^n = e\}$ and is thus of order n. In particular, $g^{\#G} = e$ for all $g \in G$.

The converse to Lagrange theorem's in not true: in general, there will exist divisors d or $\#G$ such that G has no element of order[3] d. However, a theorem of Cauchy's tells us that if $p \in \mathbb{N}$ is a *prime* dividing G, then $\exists g \in G$ of order exactly p.

The group G is said to be *Abelian* if $g_1 \cdot g_2 = g_2 \cdot g_1$ for all $g_1, g_2 \in G$. Most of the groups considered in this course will be Abelian.

A *ring* is a set R with two operations $+$ and $\times$ and elements $0, 1 \in R$ such that R is an Abelian group for $+$, and such that $x \times (y + z) = x \times y + x \times z$ and $(y + z) \times x = y \times x + z \times x$ and $1 \times x = x \times 1 = x$ for all $x, y, z \in R$.

The *characteristic* of R is the smallest $n \in \mathbb{N}$ such that $n = 0$ in R; if no such n exists, we say that R has characteristic 0. For instance, $\mathbb{Z}/n\mathbb{Z}$ has characteristic n, and $\mathbb{Z}$ has characteristic 0.

We say that R is *commutative* if $x \times y = y \times x$ for all $x, y \in R$. Unless stated otherwise, all rings considered in this course will be commutative.

An *isomorphism* between a ring R and a ring S is a map $\phi : R \longrightarrow S$ which is bijective and satisfies $\phi(x \times y) = \phi(x) \times \phi(y)$ and $\phi(x \times y) = \phi(x) \times \phi(y)$ for all $x, y \in R$, as well as $\phi(1) = 1$.

A ring R is a *domain* if for all $x, y \in R$, $x \times y = 0$ implies $x = 0$ or $y = 0$.

An element $x \in R$ is a *unit* (or is *invertible*) if there exists $y \in R$ such that $x \times y = y \times x = 1$; one then writes $y = x^{-1}$. The set of units of R is denoted by $R^\times$; it forms a group under the operation $\times$.

---

[1] Do not confuse the notion of order of a group with that of order of a group element!

[2] Thus the lcm of the order of the elements of G (a.k.a. the *exponent* of G) divides the order of G. Beware however that this divisibility can be strict; for instance, the group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has order 4, but every element of G has order 1 or 2.

[3] Counter-example: $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has $\#G = 4$ but the elements of G have order 1 or 2, never 4. In fact, a group G has an element of order $\#G$ iff. it is cyclic, thus isomorphic to $\mathbb{Z}/\#G\mathbb{Z}$.

Two elements x, y of a ring R are said to be *associate* if there exists a unit $u \in R^\times$ such that $y = ux$ (note that this implies $x = u^{-1}y$).

A *field* is a ring in which $0 \neq 1$ and every nonzero element is a unit. An *isomorphism* of fields is a map between two fields which is an isomorphism of rings.

Given a domain[4] R, the then set of fractions $\frac{x}{y}$ with $x, y \in R$ and $y \neq 0$ forms a field containing R, called the *field of fractions* of R and denoted by $\operatorname{Frac} R$. For instance, if $R = \mathbb{C}[x]$ is the ring of polynomials with complex coefficients, then $\operatorname{Frac} R = \mathbb{C}(x)$ is the field of rational fractions with complex coefficients.

Let G be an Abelian[5] group whose operation is denoted by $+$, and let $H \subset G$ be a subgroup. The *quotient group* is the set G/H formed of all the elements of G, where $g_1 \in G$ and $g_2 \in G$ are identified whenever $g_1 - g_2 \in H$. The operation $+$ is still well-defined on G/H, i.e. if $g_1 - g_2 \in H$ and $g_1' - g_2' \in H$, then $(g_1 + g_1') - (g_2 + g_2') \in H$. The quotient group G/H is thus an Abelian group.

The *index* $[G : H]$ of H in G is the order of the quotient G/H (which may be infinite if $\#G$ is inifinte). Note that by Lagrange's theorem, if $[G : H] = m$ is finite, then $\bar{g}^m = \bar{e}$ for all $\bar{g} \in G/H$, where $\bar{e}$ denotes the neutral element of G/H. This can be rephrased by saying that $g^m \in H$ for all $g \in G$.

For example, for all $n \in \mathbb{N}$, the group $\mathbb{Z}/n\mathbb{Z}$ (under addition) is the quotient of the group $\mathbb{Z}$ by the subgroup $n\mathbb{Z}$. This quotient group is a group of order n, so the index $[\mathbb{Z} : n\mathbb{Z}]$ of $n\mathbb{Z}$ in $\mathbb{Z}$ is n.

An *ideal* of a ring R is a non-empty subset $I \subset R$ satisfying

$$\forall i, j \in I, i + j \in I$$

and

$$\forall i \in I, \forall x \in R, xi \in I.$$

Given a ring R and an ideal I of R, the *quotient ring* R/I is the set of elements of R where two elements x, y are identified whenever $x - y \in I$ (we sometimes say that x and y are *congruent* modulo I). The addition $+$ and the multiplication $\times$ are still well-defined on R/I, which is thus a ring.

[4]This construction fails if R is not a domain, or worse, if R is not commutative.

[5]The construction of quotient groups is also possible with non-Abelian groups, but the subgroup needs to satisfy and extra condition (it must be *normal*). We will not need this in this course.

For example, for all $n \in \mathbb{N}$, the ring $\mathbb{Z}/n\mathbb{Z}$ is the quotient of the ring $\mathbb{Z}$ by the ideal $n\mathbb{Z}$. The difference with the previous example is that we now view $\mathbb{Z}$ as a ring and not merely as a group, so that we obtain a ring structure (as opposed to a mere group structure) on $\mathbb{Z}/n\mathbb{Z}$.

Let R be a domain. Given $x \in R$, the set

$$xR = \{xy, y \in R\}$$

of multiples of x is an ideal of R, which is also written (x). Ideals of the form xR for some $x \in R$ are called *principal* ideals. Given x and $y \in R$, the principal ideals xR and yR agree if and only if $\exists u \in R^\times$ such that $y = ux$.

We say that R is a *PID* (short for *Principal ideal domain*) if every ideal of R is principal.

Let R be a PID. Given $a, b \in R$, the set $aR + bR = \{au + bv,\ u, v \in R\}$ is an ideal of R, so there exists $g \in R$ such that $aR + bR = gR$. This g is called the gcd of a and b, and is only defined up to multiplication by a unit. We say that a and b are *coprime* if their gcd is a unit, that is to say if $aR + bR = R$. This is the same as saying that there exist $u, v \in R$ such that $au + bv = 1$ (Bézout).

Polynomials and Euclidean division

Given a ring R, we let $R[x]$ be the set of polynomials in the indeterminate x with coefficients in R. More generally, given several indeterminates $x_1, \cdots, x_n$, we can consider the set $R[x_1, \cdots, x_n]$ of polynomials in $x_1, \cdots, x_n$ with coefficients in R. Then $R[x]$ (and more generally $R[x_1, \cdots, x_n]$) is a ring.

For example, $R = \mathbb{C}[u, v]$ is the set of polynomial in the two variables u and v and with complex coefficients. Note that the set $\{P(u, v) \in R \mid P(0, 0) = 0\}$ is an ideal of R, but not a principal ideal (it can be generated by the two elements U and v, but not by a single element); thus R is not a PID.

Let R be a domain. We say that R is *Euclidean* if there exists a map $\nu : R - \{0\} \longrightarrow \mathbb{N}$ such tat for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\nu(r) < \nu(b)$. The domain $\mathbb{Z}$ is Euclidean, and so is $K[x]$ for any field K. In fact, in the case of $\mathbb{Z}$ and of $K[x]$, quotients and remainders are unique for each division (this is not required in the definition of a Euclidean domain in general).

Every Euclidean domain is a PID. In particular, $\mathbb{Z}$ and $K[x]$ (K any field) are PID's.

Finally, we mention that every field K can be embedded in a (possibly larger) field L such that every polynomial in $K[x]$ factors completely (i.e. into terms of degree 1) over L (in many cases, for instance when $K = \mathbb{Q}$ or $\mathbb{R}$, we can take $L = \mathbb{C}$).

Linear algebra

Let R be a ring, let $n \in \mathbb{N}$, and let A be a matrix of size $n \times n$ with coefficients in R. Then A has a *trace* $\operatorname{Tr} A \in R$ and a *determinant* $\det A \in R$, and A is invertible (with an inverse also with coefficients in R) iff. $\det A$ is a unit in R.

Let $R[x]$ be the ring of polynomials with coefficients in R in the indeterminate x, and let I_n be the identity matrix of size n. Then $xI_n - A$ is an $n \times n$ matrix with coefficients in $R[x]$. Its determinant is the *characteristic polynomial* $\chi_A(x)$ of A; it is a polynomial of degree n, of the form

$$\chi_A(x) = x^n - (\operatorname{Tr} A)x^{n-1} + \cdots + (-1)^n \det A.$$

Besides, we have the identity

$$\chi_A(A) = 0,$$

the $n \times n$ zero matrix (Cayley-Hamilton).

In the special case when

$$A = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_p \end{pmatrix}$$

is a block-diagonal matrix, then we have (of course)

$$\operatorname{Tr} A = \sum_{k=1}^{p} \operatorname{Tr} A_k,$$

but also

$$\det A = \prod_{k=1}^{p} \det A_k.$$

In particular,

$$\chi_A(x) = \prod_{k=1}^{p} \chi_{A_k}(x).$$

Let now K be a field, V a vector space over K of finite dimension d, and $(e_1, \cdots, e_d)$ a basis of V. If $(f_1, \cdots, f_d)$ is another basis of V, then the *change of basis matrix*, also known as *transition matrix*, from the e_i's to the f_i's is the $d \times d$ matrix P whose columns express the f_i's on the e_i's; in other words, such that

$$f_j = \sum_{i=1}^{d} P_{i,j} e_i$$

for all $j = 1, \cdots, d$. This matrix is invertible, and its inverse is the change of basis matrix from the f_i's to the e_i's.

Let now $T \colon V \longrightarrow V$ be an *endomorphism*, that is to say a linear map from V to itself, and let A is the $d \times d$ matrix with coefficients in K representing T on the basis $(e_1, \cdots, e_d)$, in equations

$$T(e_j) = \sum_{i=1}^{d} A_{i,j} e_i.$$

Then the matrix representing the same map T on the other basis $(f_1, \cdots, f_d)$ is[6]

$$P^{-1}AP.$$

We have $\operatorname{Tr}(P^{-1}AP) = \operatorname{Tr} A$, $\det(P^{-1}AP) = \det A$, and $\chi_{P^{-1}AP}(x) = \chi_A(x)$. We may thus talk about the trace, determinant, and characteristic polynomial of the endomorphism T, since they do not depend on the basis chosen to express it.

[6] In general this is **not** the same as PAP^{-1}, nor than A, so be careful!

Chapter 1

Number fields

1.1 Resultants

Before we actually get started with number theory, let us introduce a tool which will turn out to be very valuable.

Definition 1.1.1. Let K be a field, and let $A = \sum_{j=0}^{m} a_j x^j$ and $B = \sum_{k=0}^{n} b_k x^k$ be two polynomials with coefficients in K. The *resultant* of A and B is the $(m+n) \times (m+n)$ determinant

$$\operatorname{Res}(A,B) = \begin{vmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_0 \end{vmatrix},$$

where the first n rows contain the coefficients of A and the m last ones contain those of B.

The main properties of the resultant are the following:

Theorem 1.1.2.

- $\text{Res}(A, B) \in K$*, and in fact, if the coefficients of both* A *and* B *lie in a subring* $\mathcal{R}$ *of* K*, then* $\text{Res}(A, B) \in \mathcal{R}$.
- *If we can factor (over* K *or over a larger field)* A *and* B *as*

$$A = a \prod_{j=1}^{\deg A} (x - \alpha_j) \text{ and } B = b \prod_{k=1}^{\deg B} (x - \beta_k),$$

then

$$\text{Res}(A, B) = a^{\deg B} \prod_{j=1}^{\deg A} B(\alpha_j) = a^{\deg B} b^{\deg A} \prod_{j=1}^{\deg A} \prod_{k=1}^{\deg B} (\alpha_j - \beta_k)$$
$$= (-1)^{\deg A \deg B} b^{\deg A} \prod_{k=1}^{\deg B} A(\beta_k) = (-1)^{\deg A \deg B} \text{Res}(B, A).$$

- $\text{Res}(A, B) = 0$ *if and only if* A *and* B *have a common factor in* $K[x]$.

Example 1.1.3. Take $K = \mathbb{Q}$, $A = x^2 - 2 \in \mathbb{Q}[x]$ and $B = x^2 + 1 \in \mathbb{Q}[x]$. Since actually A and B lie in $\mathbb{Z}[x]$, we have $\text{Res}(A, B) \in \mathbb{Z}$; this is simply because by definition,

$$\text{Res}(A, B) = \begin{vmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{vmatrix}.$$

Besides, since we have

$$A = (x - \sqrt{2})(x + \sqrt{2}) \text{ and } B = (x - i)(x + i)$$

over $\mathbb{C}$, we find that

$$\text{Res}(A, B) = B(\sqrt{2})B(-\sqrt{2}) = A(i)A(-i) = (\sqrt{2}-i)(\sqrt{2}+i)(-\sqrt{2}-i)(-\sqrt{2}+i) = 9.$$

Example 1.1.4. Suppose we have $A = BQ + R$ in $K[x]$, and let b be the leading coefficient of B. Then $A(\beta) = R(\beta)$ for all roots β of B, so that

$$\text{Res}(A, B) = (-1)^{\deg A \deg B} b^{\deg A - \deg R} \text{Res}(B, R).$$

This gives a way to compute $\text{Res}(A, B)$ by performing successive Euclidean divisions, which is more efficient (at least for a computer) than computing a large determinant when the degrees of A and B are large.

1.2 Field extensions

1.2.1 Notation

Let K and L be fields such that $K \subseteq L$. One says that K is a *subfield* of L, and that L is an *extension* of K.

In what follows, whenever $\alpha \in L$ (resp. $\alpha_1, \alpha_2, \cdots \in L$), we will write $K(\alpha)$ (resp. $K(\alpha_1, \alpha_2, \cdots)$) to denote the smallest subfield of L containing K as well as α (resp. $\alpha_1, \alpha_2, \cdots$). For example, we have $\mathbb{C} = \mathbb{R}(i)$, and $K(\alpha) = K$ if anf only if $\alpha \in K$.

Also, when $\mathcal{R}$ is a subring of K, we will write

$$\mathcal{R}[\alpha] = \{P(\alpha),\ P \in \mathcal{R}[x]\}$$

to denote the smallest subring of L containing $\mathcal{R}$ as well as α, and similarly

$$\mathcal{R}[\alpha_1, \cdots, \alpha_n] = \{P(\alpha_1, \cdots, \alpha_n),\ P \in \mathcal{R}[x_1, \cdots, x_n]\}.$$

Example 1.2.1. The ring $K[\alpha]$ is a subring of the field $K(\alpha)$.

1.2.2 Algebraic elements, algebraic extensions

Definition 1.2.2. Let $\alpha \in L$. Then set of polynomials $P \in K[x]$ such that $P(\alpha) = 0$ is an ideal V_α of $K[x]$, and one says that α is *algebraic* over K if this ideal is nonzero, that is to say if there exists a nonzero $P \in K[x]$ which vanishes at α. Else one says that α is *transcendental* over K, or just transcendental (for short) when $K = \mathbb{Q}$.

In the case when α is algebraic over K, the ideal V_α can be generated by one polynomial since the ring $K[x]$ is a PID. This polynomial is unique up to scaling, so there is a unique *monic* polynomial $m_\alpha(x)$ that generates V_α. This polynomial $m_\alpha(x)$ is called the *minimal polynomial* of α over K. One then says that α is algebraic over K of *degree* n, where $n = \deg m_\alpha \in \mathbb{N}$, and one writes $\deg_K \alpha = n$. When $K = \mathbb{Q}$, one says for short that α is algebraic of degree n.

If every element of L is algebraic over K, one says that L is an *algebraic extension* of K.

Theorem 1.2.3. *Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K of degree n. Then $K[\alpha]$ is a field, so it agrees with $K(\alpha)$. It is also a vector space of dimension n over K, with basis*

$$1, \alpha, \alpha^2, \cdots, \alpha^{n-1},$$

which we write as

$$K(\alpha) = K[\alpha] = \bigoplus_{j=0}^{n-1} K\alpha^j.$$

Remark 1.2.4. On the other hand, if $\alpha \in L$ is transcendental over K, then it is not difficult to see that

$$K(\alpha) = \{r(\alpha),\ r \in K(x)\}$$

is isomorphic to the field $K(x)$ of rational fractions over K via

$$\begin{array}{ccc} K(x) & \xrightarrow{\sim} & K(\alpha) \\ \dfrac{P(x)}{Q(x)} & \longmapsto & \dfrac{P(\alpha)}{Q(\alpha)} \end{array}$$

(this is well-defined since, as α is transcendental, $Q(\alpha) \neq 0$ as soon as $Q(x)$ is not the 0 polynomial), whence the notation $K(\alpha)$. In particular, it is infinite-dimensional as a K-vector space, and $K[\alpha]$ is a strict subring of $K(\alpha)$.

Proof of theorem 1.2.3. Let us begin with the second equality. Let $m(x) = m_\alpha(x) \in K[x]$ be the minimal polynomial of α over K, an irreducible polynomial of degree n. For all $P(x) \in K[x]$, euclidean division in $K[x]$ tells us that we may write

$$P(x) = m(x)Q(x) + R(x)$$

where $Q(x), R(x) \in K[x]$ and $\deg R(x) < n$. Evaluating at $x = \alpha$, we find that $P(\alpha) = R(\alpha)$, so that

$$K[\alpha] = \left\{ \sum_{j=0}^{n-1} \lambda_j \alpha^j,\ \lambda_j \in K \right\}.$$

Besides, if we had a relation of the form

$$\sum_{j=0}^{n-1} \lambda_j \alpha^j = 0$$

with the λ_j in K and not all zero, this would mean that the nonzero polynomial

$$\sum_{j=0}^{n-1} \lambda_j x^j \in K[x]$$

vanishes at $x = \alpha$, and since its degree is $< n$, this would contradict the definition of the minimal polynomial.

Therefore, the $(\alpha^j)_{0 \leqslant j < n}$ span $K[\alpha]$ as a K-vector space and are linearly independent over K, so they form a K-basis of $K[\alpha]$.

For the first equality, we must prove that the ring $K[\alpha]$ is actually a field. Let us thus prove that any nonzero $\beta \in K[\alpha]$ is invertible in $K[\alpha]$. We know from the above that $\beta = P(\alpha)$ for some nonzero $P(x) \in K[x]$ of degree $< n$. Since $m(x)$ is irreducible over K and $\deg P(x) < \deg m(x) = n$, it follows that $P(x)$ and $m(x)$ are coprime, so that there exist $U(x)$ and $V(x)$ in $K[x]$ such that

$$U(x)P(x) + V(x)m(x) = 1.$$

Evaluating at $x = \alpha$, we find that $U(\alpha)P(\alpha) + 0 = 1$, which proves that $U(\alpha) \in K[\alpha]$ is the inverse of $\beta = P(\alpha)$. □

Example 1.2.5. Let $\alpha = \sqrt{2}$. Then α is a root of $x^2 - 2 \in \mathbb{Q}[x]$. Since this polynomial is of degree only 2, if it were reducible, it would split into factors of degree 1; since $\alpha \notin \mathbb{Q}$, we conclude that $x^2 - 2$ is irreducible, so it is the minimal polynomial of α, which is thus is algebraic of degree 2. In particular, we have

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2},$$

which means that every element of $\mathbb{Q}(\sqrt{2})$ can be written in a unique way as $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$.

Similarly, since $i^2 = -1$, i is algebraic of degree 2, and its minimal polynomial is x^2+1. It is also algebraic of degree 2 over $\mathbb{R}$, with the same minimal polynomial $x^2 + 1$, but which is this time seen as lying in $\mathbb{R}[x]$. We deduce that

$$\mathbb{Q}(i) = \mathbb{Q}[i] = \mathbb{Q} \oplus \mathbb{Q}i$$

and that

$$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i] = \mathbb{R} \oplus \mathbb{R}i.$$

We thus recover the well-known fact that every complex number can be written uniquely as $a + bi$ with $a, b \in \mathbb{R}$.

On the contrary, one can prove that π is transcendental over $\mathbb{Q}$ (but this is not easy). In particular, $\mathbb{R}$ is not an algebraic extension of $\mathbb{Q}$, and its subfield $\mathbb{Q}(\pi)$ is isomorphic to $\mathbb{Q}(x)$.

Finally, one can prove that $\sqrt{3}$ is algebraic of degree 2 over $\mathbb{Q}(\sqrt{2})$. This amounts to say that x^2-3, which is irreducible over $\mathbb{Q}$, remains irreducible over $\mathbb{Q}(\sqrt{2})$. Indeed, if it became reducible, then $\sqrt{3}$ would lie in $\mathbb{Q}(\sqrt{2})$. Theorem 1.2.3 tells us that $(1, \sqrt{2})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$, so there would exist $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$. Squaring yields $3 = (a^2+2b^2) + 2ab\sqrt{2}$, which (again by theorem 1.2.3) implies that $a^2+2b^2 = 3$ and that $2ab = 0$, which is clearly impossible.

It follows that

$$\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{2})\sqrt{3}$$

as a vector space over $\mathbb{Q}(\sqrt{2})$, so that every element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be written in a unique way as $a + b\sqrt{3}$ with $a, b \in \mathbb{Q}(\sqrt{2})$.

We now prove that the four basic operations preserve algebraicity.

Theorem 1.2.6. *Let L/K be a field extension. The sum, difference, product, and quotient*[1] *of two elements of L which are algebraic over K are algebraic over K.*

Proof. Let α (resp. β) be algebraic over K, so that there exists a nonzero polynomial $A(x) \in K[x]$ (resp. $B(x) \in K[x]$) such that $A(\alpha) = 0$ (resp. $B(\beta) = 0$). Factor $A(x)$ and $B(x)$ in some large enough extension of K,

$$A(x) = \prod_{j=1}^{m} (x - \alpha_j), \quad B(x) = \prod_{k=1}^{n} (x - \beta_k),$$

with $\alpha = \alpha_1$ and $\beta = \beta_1$, and consider the polynomials $A(y)$ and $B(x-y)$ as polynomials in y over the field $K(x)$. Their resultant

$$C(x) = \operatorname{Res}\big(A(y), B(x-y)\big)$$

lies in $K(x)$, and actually even in $K[x]$ according to theorem 1.1.2, since the coefficients of $A(y)$ and $B(x-y)$ (still seen as polynomials in y) lie in $K[x]$.

[1] Not by 0, of course.

Besides, still according to theorem 1.1.2, we have

$$C(x) = \prod_{j=1}^{m} B(x-y)|_{y=\alpha_j} = \prod_{j=1}^{m} B(x-\alpha_j) = \prod_{j=1}^{m}\prod_{k=1}^{n}(x-\alpha_j-\beta_k),$$

so that $\alpha+\beta$ is a root of $C(x)$ and is thus algebraic over K.

The cases of $\alpha-\beta$, $\alpha\beta$ and α/β can be dealt with similarly. □

A consequence of this theorem is that the set of complex numbers which are algebraic over $\mathbb{Q}$ is actually a subfield of $\mathbb{C}$.

Example 1.2.7. According to this theorem, $\alpha = \sqrt{2}+\sqrt{3}$ is algebraic. However, the computations needed to exhibit a nonzero polynomial vanishing at α require a bit of effort. We will actually determine the degree and the minimal polynomial of α by another method in example 1.2.32 below.

1.2.3 The degree of an extension

Let L be an extension of a field K. If we forget temporarily about the multiplication on L, so that only addition is left, then L can be seen as a vector space over K.

Definition 1.2.8. The *degree* of L over K is the dimension (finite or infinite) of L seen as a K-vector space. It is denoted by $[L:K]$.

If this degree is finite, one says that L is a *finite extension* of K.

Example 1.2.9. Let $\alpha \in L$. If α is algebraic over K with minimal polynomial $m_\alpha(x) \in K[x]$ of degree n, then theorem 1.2.3 tells us that

$$K(\alpha) = \left\{ \sum_{k=0}^{n-1} \lambda_k \alpha^k,\ \lambda_k \in K \right\} = K \oplus K\alpha \oplus \cdots \oplus K\alpha^{n-1},$$

so $[K(\alpha):K] = n = \deg_K \alpha$. On the other hand, if α is transcendental over K, then $K(\alpha)$ is isomorphic to the rational fraction field $K(x)$, so $[K(\alpha):K] = \infty$.

Remark 1.2.10. Clearly, the only extension L of a field K such that $[L:K]=1$ is $L=K$ itself.

An important feature of the degree is that it is multiplicative. In fact, even more is true.

Proposition 1.2.11 (Multiplicativity of the degree)**.** *Let $K \subseteq L \subseteq M$ be finite extensions, let $(l_i)_{1 \leqslant i \leqslant [L:K]}$ be a K-basis of L, and let $(m_j)_{1 \leqslant j \leqslant [M:L]}$ be an L-basis of M. Then $(l_i m_j)_{\substack{1 \leqslant i \leqslant [L:K] \\ 1 \leqslant j \leqslant [M:L]}}$ is a K-basis of M. In particular, $[M : K] = [M : L][L : K]$.*

Proof. Let $m \in M$. Since $(m_j)_{1 \leqslant j \leqslant [M:L]}$ is an L-basis of M, we have

$$m = \sum_{j=1}^{[M:L]} \lambda_j m_j$$

for some $\lambda_j \in L$, and since $(l_i)_{1 \leqslant i \leqslant [L:K]}$ is a K-basis of L, each λ_j can be written

$$\lambda_j = \sum_{i=1}^{[L:K]} \mu_{i,j} l_i.$$

Thus we have

$$m = \sum_{j=1}^{[M:L]} \sum_{i=1}^{[L:K]} \mu_{i,j} l_i m_j,$$

which proves that the $l_i m_j$ span M over K.

Besides, if we had a linear dependency relation

$$\sum_{j=1}^{[M:L]} \sum_{i=1}^{[L:K]} \mu_{i,j} l_i m_j = 0$$

with $\mu_{i,j} \in K$, then we would have

$$\sum_{j=1}^{[M:L]} \lambda_j m_j = 0$$

where

$$\lambda_j = \sum_{i=1}^{[L:K]} \mu_{i,j} l_i \in L.$$

Since $(m_j)_{1 \leqslant j \leqslant [M:L]}$ is an L-basis of M, this would imply that

$$0 = \lambda_j = \sum_{i=1}^{[L:K]} \mu_{i,j} l_i \in L$$

for all j; and since $(l_i)_{1\leqslant i\leqslant[L:K]}$ is a K-basis of L, this means that the $\mu_{i,j}$ are all zero. Thus the $l_i m_j$ are linearly independent over K. $\square$

Example 1.2.12. According to example 1.2.5 above,

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2,$$

and

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2.$$

It then follows from proposition 1.2.11 that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4.$$

More precisely, since we know that $(1, \sqrt{2})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$ by theorem 1.2.3, and that $(1, \sqrt{3})$ is a $\mathbb{Q}(\sqrt{2})$-basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ by theorem 1.2.3 and example 1.2.5, we deduce from proposition 1.2.11 that $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

1.2.4 The trace, norm, and characteristic polynomial

Definition 1.2.13. Let L be a finite extension of K, and let $\alpha \in L$. Then multiplication by α induces a K-endomorphism of L, denoted by

$$\begin{array}{rcl} \mu_\alpha \colon L & \longrightarrow & L \\ \xi & \longmapsto & \alpha\xi. \end{array}$$

The *trace*, *norm*, and *characteristic polynomial* of α (with respect to the extension L/K) are, respectively, the trace, determinant, and characteristic polynomial of this endomorphism. They are denoted respectively by $\mathrm{Tr}_K^L(\alpha) \in K$, $N_K^L(\alpha) \in K$, and $\chi_K^L(\alpha) \in K[x]$. When the extension L/K is clear from the context, we will just write $\mathrm{Tr}(\alpha)$, $N(\alpha)$ and $\chi(\alpha)$.

Remark 1.2.14. Note that, as K-endomorphisms of L, $\mu_{\alpha+\beta} = \mu_\alpha + \mu_\beta$ and $\mu_{\alpha\beta} = \mu_\alpha \circ \mu_\beta$ for all $\alpha, \beta \in L$; this translates respectively into the identities $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$ and $N(\alpha\beta) = N(\alpha)N(\beta)$. Thus the trace is an additive group homomorphism from L to K, whereas the norm is a multiplicative group homomorphism from $L^\times$ to $K^\times$.

Also note that $N(\alpha) = 0$ if and only if $\alpha = 0$.

Example 1.2.15. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, seen for now as an extension of $\mathbb{Q}$, and let $\alpha = \sqrt{2} + \sqrt{3} \in L$. With respect to the $\mathbb{Q}$-basis $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ of L (cf. example 1.2.12), the matrix of μ_α is

$$\begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix};$$

therefore $\mathrm{Tr}_{\mathbb{Q}}^L(\alpha) = 0 \in \mathbb{Q}$, $N_{\mathbb{Q}}^L(\alpha) = 1 \in \mathbb{Q}$, and $\chi_{\mathbb{Q}}^L(\alpha) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$.

On the other hand, if we have the extension L/K in mind, where $K = \mathbb{Q}(\sqrt{2})$, then we find that the matrix of μ_α with respect to the K-basis $(1, \sqrt{3})$ of L is

$$\begin{pmatrix} \sqrt{2} & 3 \\ 1 & \sqrt{2} \end{pmatrix},$$

so that $\mathrm{Tr}_K^L(\alpha) = 2\sqrt{2} \in K$, $N_K^L(\alpha) = -1 \in K$, and $\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x - 1 \in K[x]$.

Proposition 1.2.16. *Let L/K be a finite extension, let α be an element of L, and let $\chi = \chi_K^L(\alpha) \in K[x]$ be its characteristic polynomial. Then χ vanishes at α.*

Proof. Since χ is the characteristic polynomial of the endomorphism μ_α, we have $\chi(\mu_\alpha) = 0$ by Cayley-Hamilton. But $P(\mu_\alpha) = \mu_{P(\alpha)}$ for every polynomial $P \in K[x]$, so in particular $0 = \chi(\mu_\alpha) = \mu_{\chi(\alpha)}$, which means that $\chi(\alpha) = 0$. $\square$

Corollary 1.2.17. *If an extension is finite, then it is algebraic.*

Remark 1.2.18. The converse does not hold! For instance, let $\overline{\mathbb{Q}}$ be the set of all complex numbers that are algebraic over $\mathbb{Q}$. Then $\overline{\mathbb{Q}}$ is a field by theorem 1.2.6, and is an algebraic extension of $\mathbb{Q}$ by construction, but it is not a finite extension of $\mathbb{Q}$.

Definition 1.2.19. A *number field* is a finite extension of $\mathbb{Q}$.

Thus every element of a number field is algebraic, and conversely every algebraic number α spans a number field $\mathbb{Q}(\alpha)$. In a nutshell, it can be said that this course is about the arithmetic properties of number fields.

Example 1.2.20. The fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ are number fields, of respective degrees 1, 2, 2, and 4. On the contrary, neither $\mathbb{R}$ nor $\mathbb{C}$ are number fields, for instance because $\pi \in \mathbb{R}$ so that $\mathbb{Q}(\pi) \subset \mathbb{R} \subset \mathbb{C}$ so $[\mathbb{R} : \mathbb{Q}]$ and $[\mathbb{C} : \mathbb{Q}]$ are infinite because $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ since π is transcendental over $\mathbb{Q}$. Similarly, the finite fields such as $\mathbb{Z}/p\mathbb{Z}$ are not number fields, since they are not extensions of $\mathbb{Q}$.

Proposition 1.2.16 above tells us in particular that the characteristic polynomial is a multiple of the minimal polynomial. In fact, more is true:

Proposition 1.2.21 (Characteristic poly. vs. minimal poly.)**.** *Let L/K be a finite extension of degree n. Let $\alpha \in L$, let $m(x)$ be its minimal polynomial over K, and let $\chi(x)$ be its characteristic polynomial (with respect to the extension L/K). Let $d = \deg m(x)$. Then d divides n, and $\chi(x) = m(x)^{n/d}$.*

Proof. We have a double extension $K \subset K(\alpha) \subset L$. By hypothesis, $[L : K] = n$; besides, we have $[K(\alpha) : K] = \deg m(x) = d$. Therefore, $[L : K(\alpha)] = n/d$ is an integer.

Next, multiplication by α defines a K-endomorphism of $K(\alpha)$. The characteristic polynomial of this endomorphism is monic, has degree $d = \deg m(x)$, and vanishes at α by proposition 1.2.16; therefore, this polynomial agrees with $m(x)$.

Let now $M_\alpha \in \mathrm{Mat}_{d \times d}(K)$ be the matrix of this endomorphism on a K-basis $(e_j)_{1 \leqslant j \leqslant d}$ of $K(\alpha)$, and let $(f_k)_{1 \leqslant k \leqslant n/d}$ be a $K(\alpha)$-basis of L. Then, by proposition 1.2.11, $(e_j f_k)_{\substack{1 \leqslant j \leqslant d \\ 1 \leqslant k \leqslant n/d}}$ is a K-basis of L, and in this basis, the matrix of the multiplication-by-α endomorphism of L is

$$\begin{pmatrix} M_\alpha & & 0 \\ & \ddots & \\ 0 & & M_\alpha \end{pmatrix},$$

a diagonal of n/d copies of M_α. Since $m(x)$ is the characteristic polynomial of M_α and $\chi(x)$ is the characteristic polynomial of this big block-diagonal matrix, the result follows. □

Remark 1.2.22. If the chosen K-basis of $K(\alpha)$ is $(1, \alpha, \cdots, \alpha^{d-1})$, then one sees easily that M_α is the *companion matrix*

$$M_\alpha = \begin{pmatrix} 0 & \cdots & 0 & -m_0 \\ 1 & \ddots & \vdots & -m_1 \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & 0 & \\ 0 & \cdots\ 0 & 1 & -m_{d-1} \end{pmatrix}$$

of the minimal polynomial $m(x) = x^d + m_{d-1}x^{d-1} + \cdots + m_1 x + m_0$.

1.2.5 Abstract field extensions

So far, we have been giving examples of field extensions (such as $\mathbb{Q} \subset \mathbb{Q}(i)$) by cutting out a piece of a very large field (such as $\mathbb{C}$) containing all the fields we were interested in. However, it is also possible to construct extensions of any field "out of thin air", without taking elements from an already constructed larger field.

Theorem 1.2.23. *Let K be a field, and let $P \in K[x]$ be an irreducible polynomial with coefficients in K. The quotient ring $E = K[x]/P(x)K[x]$ is a field, which is a finite extension of K of degree $\deg P$, and the image of x in L is a root of P.*

Proof. Since $P(x)K[x]$ is an ideal of the ring $K[x]$, the quotient $E = K[x]/P(x)K[x]$ inherits a ring structure. We want to show that this ring is in fact a field, that it contains K as a subfield, and that its degree as an extension of K is $\deg P$.

The proof of the fact that that E is a field is the same as that of theorem 1.2.3. More precisely, let us consider a nonzero element $\alpha \in E$, and prove that it is invertible. This element α is represented by a polynomial $A(x) \in K[x]$, which is not divisible by $P(x)$ since $\alpha \neq 0$. As $P(x)$ is irreducible, the polynomials $A(x)$ and $P(x)$ are coprime, so by Bézout there exist $U(x), V(x) \in K[x]$ such that

$$A(x)U(x) + P(x)V(x) = 1.$$

Thus $A(x)U(x) \equiv 1 \bmod P(x)$, which means that $U(x)$ represents the inverse of $A(x)$ in the quotient $E = K[x]/P(x)K[x]$.

Similarly, the proof of theorem 1.2.3 (namely, taking the remainder of the Euclidean division by $P(x)$) shows that $\{1, x, x^2, \cdots, x^{\deg P-1}\}$ is a K-basis of E. Therefore E contains a copy of K as a subfield (namely the K-span of 1), and is a vector space of dimension $\deg P$ over K. $\square$

Remark 1.2.24. The notation $K[x]/P(x)K[x]$ is often abbreviated into $K[x]/\big(P(x)\big)$.

Remark 1.2.25. In the special case when P is the minimal polynomial over K of some (necessarily algebraic over K) element α of some extension of K, then the ring morphism

$$\begin{array}{rcl} \mathrm{eval}_\alpha : K[x] & \longrightarrow & K(\alpha) \\ F(x) & \longmapsto & F(\alpha) \end{array}$$

factors through E and induces a field isomorphism between E and $K(\alpha)$:

$$\begin{array}{ccc} K[x] & \xrightarrow{\mathrm{eval}_\alpha} & K(\alpha) \\ \downarrow & \nearrow_{\sim} & \\ K[x]/P(x)K[x] & & \end{array}$$

Example 1.2.26. Take $K = \mathbb{R}$ and $P = x^2 + 1$. Then $E = \mathbb{R}[x]/(x^2+1)$ is a degree 2 extension of $\mathbb{R}$. In fact, x^2+1 is the minimal polynomial of i over $\mathbb{R}$, the evaluation map $F(x) \mapsto F(i)$ induces a field isomorphism between E and $\mathbb{R}(i) = \mathbb{C}$:

$$\begin{array}{ccc} \mathbb{R}[x] & \xrightarrow{\mathrm{eval}_i} & \mathbb{R}(i) = \mathbb{C} \\ \downarrow & \nearrow_{\sim} & \\ \mathbb{R}[x]/(x^2+1) & & \end{array}$$

Example 1.2.27. Take $K = \mathbb{Q}$ and $P = x^3 - 2$. One can show (cf. theorem 3.7.6) that P is irreducible over $\mathbb{Q}$. Therefore, $E = \mathbb{Q}[x]/(x^3-2)\mathbb{Q}[x]$ is a degree 3 extension of $\mathbb{Q}$.

This extension is isomorphic to $\mathbb{Q}(\sqrt[3]{2})$ via

$$\begin{array}{ccc} \mathbb{Q}[x] & \xrightarrow{\mathrm{eval}\,\sqrt[3]{2}} & \mathbb{Q}(\sqrt[3]{2})\ , \\ \downarrow & \nearrow_{\sim} & \\ \mathbb{Q}[x]/(x^3-2) & & \end{array}$$

but also to $\mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$ and to $\mathbb{Q}(e^{4\pi i/3}\sqrt[3]{2})$.

This illustrates the fact that which one of the 3 roots of $x^3 - 2$ we choose does not matter. The abstract extension $\mathbb{Q}[x]/(x^3-2)$ is thus a model for this extension that has the advantage of being canonical, since it does not pick a particular root of $x^3 - 2$: $\mathbb{Q}[x]/(x^3 - 2)$ is just $\mathbb{Q}(\alpha)$, where α is something having the property that $\alpha^3 - 2 = 0$ but whose nature does not matter. This reflects the fact that a number field can be seen as a subfield of $\mathbb{C}$ in several inequivalent ways. We will study this in detail in section 1.3.

We are now going to prove that every number field is a quotient of $\mathbb{Q}[x]$, that is to say is of the form $\mathbb{Q}(\alpha)$ for some α.

1.2.6 Primitive elements

Definition 1.2.28. Let L/K be a field extension, and let $\alpha \in L$, so that $K(\alpha) \subseteq L$. One says that α is a *primitive element* for L over K (or just a primitive element, when $K = \mathbb{Q}$) if $K(\alpha) = L$.

Remark 1.2.29. A primitive element for L/K, when it exists, has no reason to be unique (and in fact it is never unique).

By looking at the degrees and in view of proposition 1.2.21, one immediately gets the following

Proposition 1.2.30. *Let L/K be a finite extension, and let $\alpha \in L$. Then the following are equivalent:*

- *α is a primitive element for L/K,*
- $\deg_K \alpha = [L : K]$,
- *the characteristic polynomial $\chi_K^L(\alpha)$ is irreducible over K,*
- *the characteristic polynomial $\chi_K^L(\alpha)$ is squarefree over K,*
- *the characteristic polynomial $\chi_K^L(\alpha)$ agrees with the minimal polynomial of α over K.*

Remark 1.2.31. If K has characteristic 0 (in particular, if K is a number field), then $\chi_K^L(\alpha)$ is squarefree if and only if it is coprime with its derivative. This gives an efficient criterion to determine whether α is a primitive element for L/K.

Example 1.2.32. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and let $\alpha = \sqrt{2} + \sqrt{3} \in L$. We know from example 1.2.15 above that α is a root of

$$P(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x].$$

Since $\gcd\big(P(x), P'(x)\big) = 1$, $P(x)$ is squarefree. It follows that it is irreducible over $\mathbb{Q}$, and that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, so that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Thus α is a primitive element for the number field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Besides, it follows that the degree of α is 4, and that its minimal polynomial is $P(x)$. Furthermore, since (for instance) $\sqrt{2} \in L$, this also means that there exists a polynomial $F(x) \in \mathbb{Q}[x]$ such that $F(\sqrt{2} + \sqrt{3}) = \sqrt{2}$, a fact which was not obvious.

On the other hand, neither $\sqrt{2}$ nor $\sqrt{3}$ nor $\sqrt{6}$ are primitive elements for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, since they generate strictly smaller fields over $\mathbb{Q}$. By proposition 1.2.21, their respective characteristic polynomials with respect to L/K are $(x^2 - 2)^2$, $(x^2 - 2)^2$, and $(x^2 - 2)^2$.

However, $\sqrt{3}$ is a primitive element for L over $\mathbb{Q}(\sqrt{2})$; by proposition 1.2.30, its characteristic polynomial relative to this extension must agree with its minimal polynomial over $\mathbb{Q}(\sqrt{2})$ and has degree $[L : \mathbb{Q}(\sqrt{2})] = 2$, so it has to be $x^2 - 3$, which is thus irreducible over $\mathbb{Q}(\sqrt{2})$.

Example 1.2.33. i is a primitive element for $\mathbb{C}$ over $\mathbb{R}$, but certainly not over $\mathbb{Q}$ since $\mathbb{Q}(i)$ is much smaller than $\mathbb{C}$.

The following theorem guarantees the existence of primitive elements in many cases.

Theorem 1.2.34. *[Primitive element theorem] Let K be a field of characteristic 0. If L is a finite extension of K, then there exists a primitive element for L/K.*

In fact, one can even prove that with these hypotheses, "most" elements of L are primitive elements.

Remark 1.2.35 (Technical, feel free to skip this)**.** Without the characteristic 0 hypothesis, this theorem is false. A classical counterexample is the extension L/K, where K is the 2-variable rational fraction field $K = \mathbb{F}_p(x, y)$ over the finite field $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ with p elements, where $p \in \mathbb{N}$ is prime, and $L = \mathbb{F}_p(\sqrt[p]{x}, \sqrt[p]{y})$.

In particular, every number field K has primitive elements, so it can be written in the form $K = \mathbb{Q}(\alpha)$, where $\alpha \in K$ is an algebraic number of the same degree as K. This means that K can be seen as the abstract extension $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/m(x)$ where $m(x) = m_\alpha(x)$ is the minimal polynomial of α over $\mathbb{Q}$. We can this of K as "$\mathbb{Q}$ adjoined some abstract element α, which is entirely characterised by the relation $m(\alpha) = 0$". In particular, we can (and should) think of K abstractly, as opposed to as a subfield of $\mathbb{C}$.

Conversely, a convenient way of specifying a number field up to isomorphism is to give it in the form $\mathbb{Q}(\alpha)$, where α is a root of some irreducible polynomial $m(x)$, which is thus the minimal polynomial of α up to scaling. It is important that $m(x)$ be irreducible over $\mathbb{Q}$, since otherwise the number field is not well-defined.

We are now going to now explore the inequivalent ways a given number field can be seen as a subfield of $\mathbb{C}$.

1.3 Complex embeddings

1.3.1 Extension of complex embeddings

Let K be a number field, and let L be a finite extension of K. Let $\alpha \in L$ be a primitive element of the extension L/K, and let $m(x) \in K[x]$ be its minimal polynomial over K. Then $m(x)$ is irreducible over K; in particular, it is coprime with $m'(x)$, so all its roots are simple. Suppose that we have field embeddings $\sigma : K \hookrightarrow \mathbb{C}$ and $\tau \colon L \hookrightarrow \mathbb{C}$. If $\tau|_K = \sigma$, we say that τ *extends* σ.

Since $m(x) \in K[x]$, we may apply σ to its coefficients, which yields a polynomial $m^\sigma(x) \in \mathbb{C}[x]$. If τ extends σ, then $\tau(\alpha) \in \mathbb{C}$ must be a root of $m^\sigma(x)$; conversely, for each complex root $z \in \mathbb{C}$ of $m^\sigma(x)$, we can define an embedding of L into $\mathbb{C}$ which extends σ, by the formula

$$\begin{array}{ccc} L & \hookrightarrow & \mathbb{C} \\ \sum_k \lambda_k \alpha^k & \longmapsto & \sum_k \sigma(\lambda_k) z^k, \end{array}$$

where the λ_k lie in K. The polynomial $m^\sigma(x)$ is of degree $[L : K]$; besides, it is coprime with $m'^\sigma(x)$ (apply σ to a relation $U(x)m(x) + V(x)m'(x) = 1$), so it has no multiple roots in $\mathbb{C}$. We thus get the following result.

Theorem 1.3.1 (Extension of complex embeddings)**.** *Let K be a number field, $\sigma\colon K \hookrightarrow \mathbb{C}$ an embedding of K into $\mathbb{C}$, and L a finite extension of K. Then there are exactly $[L : K]$ embeddings of L into $\mathbb{C}$ that extend σ.*

Lemma 1.3.2. *The only embedding of $\mathbb{Q}$ into $\mathbb{C}$ is the identity.*

Proof. Let $\sigma : \mathbb{Q} \hookrightarrow \mathbb{C}$ be an embedding. If $x \in \mathbb{Q}^+$ is a positive rational. we may write $x = \frac{p}{q}$ with $p \in \mathbb{Z}_{\geqslant 0}$ and $q \in \mathbb{Z}_{\geqslant 1}$, so that

$$\sigma(x) = \sigma\left(\frac{p}{q}\right) = \frac{\sigma(p)}{\sigma(q)} = \frac{\sigma(1 + \cdots + 1)}{\sigma(1 + \cdots + 1)} = \frac{\sigma(1) + \cdots + \sigma(1)}{\sigma(1) + \cdots + \sigma(1)} = \frac{1 + \cdots + 1}{1 + \cdots + 1} = \frac{p}{q} = x,$$

and if $x \in \mathbb{Q}^-$ is negative, we have

$$\sigma(x) = \sigma(-|x|) = -\sigma(|x|) = -|x| = x$$

by the above. □

Corollary 1.3.3. *Let K be a number field. Then K can be embedded into $\mathbb{C}$ in exactly $[K : \mathbb{Q}]$ different ways.*

Proof. Apply the previous theorem to the extension $K/\mathbb{Q}$. □

In particular, every number field K can be embedded into $\mathbb{C}$ in at least one way, so it may be seen as a subfield of $\mathbb{C}$. Some fields such as $\mathbb{Q}(\sqrt{2})$ are given explicitly as a subfield of $\mathbb{C}$ and are thus equipped with a particular embedding into $\mathbb{C}$; however, unless $K = \mathbb{Q}$, there are $[K : \mathbb{Q}] > 1$ embeddings into $\mathbb{C}$, so there are $[K : \mathbb{Q}] > 1$ inequivalent ways of seeing K as a subfield of $\mathbb{C}$, none of which is better than the other ones. As a consequence, it is better to think of number fields as abstract extensions of $\mathbb{Q}$ rather than as subfields of $\mathbb{C}$ whenever possible.

Example 1.3.4. Let $K = \mathbb{Q}(\alpha)$ where $\alpha^2 - 3 = 0$. This is a number field of degree 2, so there are 2 distinct ways of seeing K as a subfield of $\mathbb{C}$, namely by interpreting α as $\sqrt{3}$ or as $-\sqrt{3}$.

Let $L = K(\beta)$, where $\beta^2 - 4 - \alpha = 0$. One can prove that $[L : K] = 2$, so for each embedding of K into $\mathbb{C}$ there are 2 embeddings of L into $\mathbb{C}$ that extend it.

Namely, the $[K : \mathbb{Q}] = 2$ embeddings of K into $\mathbb{C}$ are

$$\sigma_1\colon a + b\alpha \mapsto a + b\sqrt{3} \quad \text{and} \quad \sigma_2\colon a + b\alpha \mapsto a - b\sqrt{3}$$

where $(a, b \in \mathbb{Q})$; each of them can be extended to L in $[L : K] = 2$ ways, respectively by

$$c + d\beta \mapsto \sigma_1(c) \pm \sigma_1(d)\sqrt{4+\sqrt{3}} \quad \text{and by} \quad c + d\beta \mapsto \sigma_2(c) \pm \sigma_2(d)\sqrt{4-\sqrt{3}}$$

where $c, d \in K$. We thus recover all $[L : \mathbb{Q}] = 4$ embeddings of L into $\mathbb{C}$.

1.3.2 The signature of a number field

Definition 1.3.5. An embedding of a number field into $\mathbb{C}$ is *real* if its image is contained in $\mathbb{R}$. Nonreal embeddings come in conjugate pairs, so we can define the *signature* of a number field K to be the pair (r_1, r_2), where r_1 is the number of real embeddings of K, and r_2 is the number of conjugate pairs of nonreal embeddings of K.

A number field is said to be *totally real* if $r_2 = 0$, and *totally complex* if $r_1 = 0$.

Obviously, one has the relation $[K : \mathbb{Q}] = r_1 + 2r_2$.

Example 1.3.6. The number field $\mathbb{Q}(\sqrt{2})$ has signature (2,0) and is thus totally real, whereas $\mathbb{Q}(i)$ has signature (0,1) and is thus totally complex.

On the other hand, $\mathbb{Q}(\sqrt[3]{2})$ has signature (1,1), and is thus neither totally real nor totally complex.

More generally, the signature of $\mathbb{Q}(\alpha)$ is (r_1, r_2), where r_1 (resp. r_2) is the number of real roots (resp. the number of conjugate pairs of complex nonreal roots) of the minimal polynomial of α.

1.3.3 Traces and norms vs. complex embeddings

The trace, norm, and characteristic polynomial are related to the complex embeddings by the following formulae:

Theorem 1.3.7. *Let $K \subset L$ be number fields. Fix an embedding $\sigma \colon K \hookrightarrow \mathbb{C}$ of K into $\mathbb{C}$, and let Σ be the set of the $[L : K]$ embeddings of L into $\mathbb{C}$ that extend σ. We have*

$$\sigma\big(\operatorname{Tr}_K^L(\alpha)\big) = \sum_{\tau \in \Sigma} \tau(\alpha),$$

$$\sigma\big(N_K^L(\alpha)\big) = \prod_{\tau \in \Sigma} \tau(\alpha),$$

and

$$\chi_K^L(\alpha)^\sigma(x) = \prod_{\tau \in \Sigma} \big(x - \tau(\alpha)\big).$$

What this theorem expresses is that once we have fixed σ, that is to say once we have decided on a way to see K as a subfield of $\mathbb{C}$, then one can compute traces, norms and characteristic polynomials from the embeddings of L into $\mathbb{C}$ that are compatible with σ; the results are then complex numbers that represent elements of K via the chosen σ.

Proof. Let $n = [L : K]$. Let $\beta \in L$ be a primitive element for L/K (there exist many according to theorem 1.2.34), let $m(x) \in K[x]$ be its minimal polynomial over K, and let $m^\sigma(x) \in \mathbb{C}[x]$ be the polynomial obtained by applying σ to the coefficients of $m(x)$, so that the n embeddings $\tau_1, \cdots, \tau_n \in \Sigma$ correspond to the complex roots $b_1, \cdots, b_n \in \mathbb{C}$ of m^σ, in that $\tau_j(\beta) = b_j$ for all $1 \leqslant j \leqslant n$.

Fix a K-basis on L, and consider the matrix M of $\mu_\beta : L \longrightarrow L$, the multiplication by β, with respect to this basis. The characteristic polynomial of this matrix is $\chi_K^L(\alpha)(x)$, which agrees with $m(x)$ by proposition 1.2.30 since β is a primitive element, so the characteristic polynomial of the matrix $M^\sigma \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ obtained by applying σ to the entries of M is $m^\sigma(x) \in \mathbb{C}[x]$. We know that this polynomial has no repeated roots in $\mathbb{C}$, so M^σ is diagonalisable; in other words, there exists a matrix $P \in \mathrm{GL}_n(\mathbb{C})$ such that $P^{-1}M^\sigma P$ is diagonal, and the coefficients on this diagonal are the eigenvalues of M^σ, that is to say the complex roots $b_1, \cdots, b_n$ of $m^\sigma(x)$.

Since $\alpha \in L = K[\beta]$, there exists a polynomial $A(x) \in K[x]$ such that $\alpha = A(\beta)$. Let $\mu_\alpha : L \longrightarrow L$ be the multiplication by α; then we have $\mu_\alpha = \mu_{A(\beta)} = A(\mu_\beta)$, so the matrix of μ_α with respect to the K-basis of L that we have fixed is $A(M)$. Therefore, the matrix

$$P^{-1}A(M)^\sigma P = P^{-1}A^\sigma(M^\sigma)P = A^\sigma(P^{-1}M^\sigma P)$$

is diagonal, with diagonal entries $A^\sigma(b_1) = \tau_1(\alpha), \cdots, A^\sigma(b_n) = \tau_n(\alpha)$. The result then follows from the fact that the image by σ of the trace (respectively norm, characteristic polynomial) of α relatively to L/K is the trace (respectively determinant, characteristic polynomial) of $A(M)\sigma$, which is the same as that to the similar matrix $P^{-1}A(M)^\sigma P$. $\square$

Corollary 1.3.8 (Transitivity of traces and norms)**.** *Suppose we have a double extension $K \subset L \subset M$, and let $\alpha \in M$. Then we have*

$$\operatorname{Tr}_K^M(\alpha) = \operatorname{Tr}_K^L\big(\operatorname{Tr}_L^M(\alpha)\big)$$

and

$$N_K^M(\alpha) = N_K^L\big(N_L^M(\alpha)\big).$$

Proof. Let $\sigma\colon K \hookrightarrow \mathbb{C}$ be an embedding. Then we have

$$\begin{aligned}
\sigma\big(\operatorname{Tr}_K^M(\alpha)\big) &= \sum_{\substack{\rho\colon M\hookrightarrow\mathbb{C} \\ \rho_{|K}=\sigma}} \rho(\alpha) \\
&= \sum_{\substack{\tau\colon L\hookrightarrow\mathbb{C} \\ \tau_{|K}=\sigma}} \sum_{\substack{\rho\colon M\hookrightarrow\mathbb{C} \\ \rho_{|L}=\tau}} \rho(\alpha) \\
&= \sum_{\substack{\tau\colon L\hookrightarrow\mathbb{C} \\ \tau_{|K}=\sigma}} \tau\big(\operatorname{Tr}_L^M(\alpha)\big) \\
&= \sigma\big(\operatorname{Tr}_K^L(\operatorname{Tr}_L^M(\alpha))\big),
\end{aligned}$$

whence the result for traces since σ, being an embedding, is one-to-one. The proof for the norms is the same, with products instead of the sums. □

Corollary 1.3.9. *Let K be a number field, and let Σ be the set of all its embeddings into $\mathbb{C}$. Then for all $\alpha \in K$, we have*

$$\operatorname{Tr}_{\mathbb{Q}}^K(\alpha) = \sum_{\sigma\in\Sigma} \sigma(\alpha),$$

$$N_{\mathbb{Q}}^K(\alpha) = \prod_{\sigma\in\Sigma} \sigma(\alpha),$$

and

$$\chi_{\mathbb{Q}}^K(\alpha)(x) = \prod_{\sigma\in\Sigma} \big(x - \sigma(\alpha)\big).$$

Proof. K is an extension of $\mathbb{Q}$, and lemma 1.3.2 tells us that the identity is the only embedding of $\mathbb{Q}$ into $\mathbb{C}$; in particular all embeddings of K into $\mathbb{C}$ must extend it. Now apply theorem 1.3.7 with $\sigma = \operatorname{Id}$. □

Example 1.3.10. Let $K = \mathbb{Q}(\sqrt{-7}) = \{a + b\sqrt{-7},\ a, b \in \mathbb{Q}\}$. Then $[K : \mathbb{Q}] = 2$, so K has 2 embeddings into $\mathbb{C}$, namely

$$a + b\sqrt{-7} \longmapsto a + bi\sqrt{7}$$

and

$$a + b\sqrt{-7} \longmapsto a - bi\sqrt{7}.$$

Thus we have

$$\mathrm{Tr}_{\mathbb{Q}}^{K}(a + b\sqrt{-7}) = (a + bi\sqrt{7}) + (a - bi\sqrt{7}) = 2a,$$

$$N_{\mathbb{Q}}^{K}(a + b\sqrt{-7}) = (a + bi\sqrt{7})(a - bi\sqrt{7}) = a^2 + 7b^2,$$

and

$$\chi_{\mathbb{Q}}^{K}(a + b\sqrt{-7}) = \big(x - (a + bi\sqrt{7})\big)\big(x - (a - bi\sqrt{7})\big) = x^2 - 2ax + a^2 + 7b^2.$$

Chapter 2

Algebraic integers

2.1 The ring of integers

In the previous chapter, we have defined number fields, which can be seen as generalisations of $\mathbb{Q}$. In order to perform arithmetic there, we would now like to study subrings of number fields which are the analogue of $\mathbb{Z} \subset \mathbb{Q}$. The question we are asking is thus: what is the generalisation of the notion of integer to number fields?

2.1.1 Monic polynomials

Definition 2.1.1. Let α be an algebraic number. One says that α is an *algebraic integer* if its *monic* minimal polynomial, which a priori lies in $\mathbb{Q}[x]$, actually lies in $\mathbb{Z}[x]$.

The following lemma expresses the fact that monic polynomials with integer coefficients have the same factorisation in $\mathbb{Z}[x]$ as in $\mathbb{Q}[x]$.

Lemma 2.1.2 (Gauss). *Let $P \in \mathbb{Z}[x]$ be a* monic *polynomial with integer factorisations, and suppose that the exist* monic *polynomials $Q, R \in \mathbb{Q}[x]$ such that $P = QR$. Then Q, R also lie in $\mathbb{Z}[x]$.*

Proof. Since $Q \in \mathbb{Q}[x]$, we may find an integer $q \in \mathbb{N}$ such that the polynomial $Q_1 = qQ$ has integer coefficients, and such that the gcd of these coefficients is 1 (we then say that Q_1 is a *primitive* polynomial). Similarly, we can find $r \in \mathbb{N}$ such that $R_1 = rR$ lies in $\mathbb{Z}[x]$ and is primitive. We then have the identity the identity

$$qrP = Q_1 R_1$$

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

Suppose now that Q, or R, or both, do not lie in $\mathbb{Z}[x]$, i.e. have denominators. Then $qr > 1$, so there exists a prime $p \in \mathbb{N}$ dividing qr. Reducing the above identity mod p, we get that

$$0 \equiv Q_1 R_1 \pmod{p}.$$

But this is absurd: since p is prime, $\mathbb{Z}/p\mathbb{Z}$ is a domain (and even a field), so the product of two nonzero polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$ is nonzero, whereas neither Q_1 nor R_1 are the 0 polynomial mod p since they are primitive. □

Since the factorisation in $\mathbb{Z}[x]$ of a *monic* polynomial can only involve *monic* factors (up to sign), this lemma and proposition 1.2.21 imply the following characterisation of algebraic integers:

Theorem 2.1.3. *Let K be a number field, and let $\alpha \in K$. The following are equivalent:*

- *α is an algebraic integer,*
- *There exists a nonzero* ***monic*** *polynomial $P \in \mathbb{Z}[x]$ such that $P(\alpha) = 0$,*
- *The characteristic polynomial of α lies in $\mathbb{Z}[x]$.*

Example 2.1.4. In $\mathbb{Q}(\sqrt{-7})$, $\alpha = \sqrt{-7}$ is an algebraic integer, because it is a root of the monic polynomial $x^2 + 7$ (actually, this polynomial happens to be the minimal polynomial of α, but we do not need that here!). On the contrary, $\frac{1}{2}\sqrt{-7}$ is not an algebraic integer, because its characteristic polynomial $x^2 + \frac{7}{4}$ does not lie in $\mathbb{Z}[x]$; we could prove this by noticing that its *monic* minimal polynomial (which in this case is also $x^2 + \frac{7}{4}$) does not lie in $\mathbb{Z}[x]$. Finally, $\frac{1+\sqrt{-7}}{2}$ is an algebraic integer, since its characteristic polynomial $x^2 - x + 2$ lies in $\mathbb{Z}[x]$.

Dealing with monic polynomials allow us to perform some operations in $\mathbb{Z}[x]$ even though $\mathbb{Z}$ is not a field. Namely:

Lemma 2.1.5 (Euclidean division in $\mathbb{Z}[x]$)**.** *Let $A(x), B(x) \in \mathbb{Z}[x]$, and suppose that $B(x)$ is monic. Then there exist $Q(x), R(x) \in \mathbb{Z}[x]$ such that $A = BQ + R$ and such that either $R = 0$ or $\deg R < \deg B$. Moreover, the pair (Q, R) is unique.*

Proof. We can view A and B as elements of $\mathbb{Q}[x]$ and perform the Euclidean division there. The only divisions that occur are divisions by the leading term of B; as B is monic, these divisions are all exact, so the quotient and remainder actually lie in $\mathbb{Z}[x]$. □

As a result, we get an "integer" version of a previous theorem:

Theorem 2.1.6. *Let α be algebraic of degree n over $\mathbb{Q}$. If α is an algebraic integer, then we have*

$$\mathbb{Z}[\alpha] = \left\{ \sum_{j=0}^{n-1} \lambda_j \alpha^j \mid \lambda_0, \cdots, \lambda_{n-1} \in \mathbb{Z} \right\}.$$

Proof. By definition, $\mathbb{Z}[\alpha] = \{P(\alpha),\ P \in \mathbb{Z}[x]\}$. Since α is an algebraic integer, its mimimal polynomial is a monic polynomial in $\mathbb{Z}[x]$. Now combine the previous lemma with the first part of the proof of theorem 1.2.3. □

Remark 2.1.7. We will soon see that this means that $\mathbb{Z}[\alpha]$ is a *lattice*.

2.1.2 The ring of integers

The main point of this definition is that algebraic integers form a ring, just like classical integers.

Theorem 2.1.8. *The sum, difference, and product of two algebraic integers is an algebraic integer. As a consequence, the set of elements of a number field K which are algebraic integers forms a subring of K.*

Proof. This can be proved just like theorem 1.2.6, by considering resultants of polynomials in $\mathbb{Z}[x][y]$. □

Remark 2.1.9 (Sanity check)**.** The reason why the same proof fails (as it should !) to show that the quotient two algebraic integers α and β is an algebraic integer is that although we can use resultants to produce a polynomial in $\mathbb{Z}[x]$ which vanishes at α/β, this polynomial is *not monic* in general.

Definition 2.1.10. The subring of a number field K formed by the elements which are algebraic integers is called the *ring of integers* of K. It is denoted by $\mathbb{Z}_K$ (some people use the notation $\mathcal{O}_K$).

Proposition 2.1.11. *We have $\mathbb{Z}_K \cap \mathbb{Q} = \mathbb{Z}$.*

Proof. Let $\alpha \in K$. If α happens to lie in $\mathbb{Q}$, then its characteristic polynomial is $(x-\alpha)^{[K:\mathbb{Q}]}$, which lies in $\mathbb{Z}[x]$ if and only if $\alpha \in \mathbb{Z}$. □

Let α be an element of a number field K, and let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding. Then α and $\sigma(\alpha)$ have the same minimal polynomial, so α is an algebraic integer if and only if $\sigma(\alpha)$ is. In view of theorem 1.3.7, we deduce the following:

Proposition 2.1.12 (Integrality vs. trace and norm, relative)**.** *Let L/K be a finite extension of number fields, and let $\alpha \in L$. If $\alpha \in \mathbb{Z}_L$, then $\operatorname{Tr}_K^L(\alpha) \in \mathbb{Z}_K$, $N_K^L(\alpha) \in \mathbb{Z}_K$, and $\chi_K^L(\alpha)(x) \in \mathbb{Z}_K[x]$.*

Corollary 2.1.13 (Integrality vs. trace and norm, absolute)**.** *Let K be a number field. For all $\alpha \in \mathbb{Z}_K$, we have $\operatorname{Tr}_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}$, $N_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}$, and $\chi_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}[x]$.*

Note that we already knew that for the characteristic polynomial.

2.2 Orders and discriminants

2.2.1 Linear algebra over $\mathbb{Z}$

Definition 2.2.1. Let $\mathbb{K} = \mathbb{Q}$ or $\mathbb{R}$, so that $\mathbb{Z} \subset \mathbb{K}$, and let V be a $\mathbb{K}$-vector space of finite dimension n. A *lattice* in V is a sub-additive-group of V of the form

$$I = \Big\{ \sum_{j=1}^{n} \lambda_j v_j, \ \lambda_j \in \mathbb{Z} \Big\},$$

where $(v_j)_{1 \leqslant j \leqslant n}$ is a $\mathbb{K}$-basis of V. We thus have

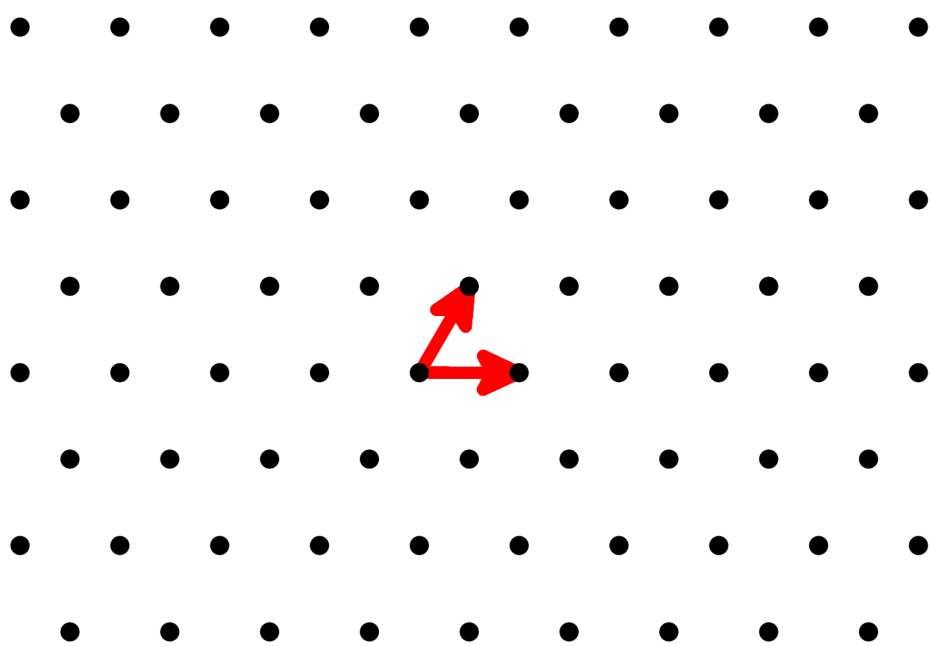
$$I = \Big\{ \sum_{j=1}^{n} \lambda_j v_j, \ \lambda_j \in \mathbb{Z} \Big\} \subsetneq V = \Big\{ \sum_{j=1}^{n} \lambda_j v_j, \ \lambda_j \in \mathbb{K} \Big\}.$$

We will write

$$I = \bigoplus_{j=1}^{n} \mathbb{Z} v_j = \mathbb{Z} v_1 \oplus \cdots \oplus \mathbb{Z} v_n,$$

and call $(v_j)_{1 \leqslant j \leqslant n}$ a $\mathbb{Z}$-basis of I.

Example 2.2.2. Here is an example of a lattice in dimension $n = 2$:



The red vectors form a $\mathbb{K}$-basis of $\mathbb{K}^2$, so they span a lattice, and form a $\mathbb{Z}$-basis of this lattice. You should keep this picture in mind, and try to imagine what a lattice looks like in dimension 3 and higher.

Just as a vector space, a lattice has many different bases. Any two $\mathbb{Z}$-bases of the lattice differ by an element of

$$\mathrm{GL}_n(\mathbb{Z}) = \{A \in \mathrm{GL}_n(\mathbb{Q}) \mid A, A^{-1} \in M_n(\mathbb{Z})\} = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}.$$

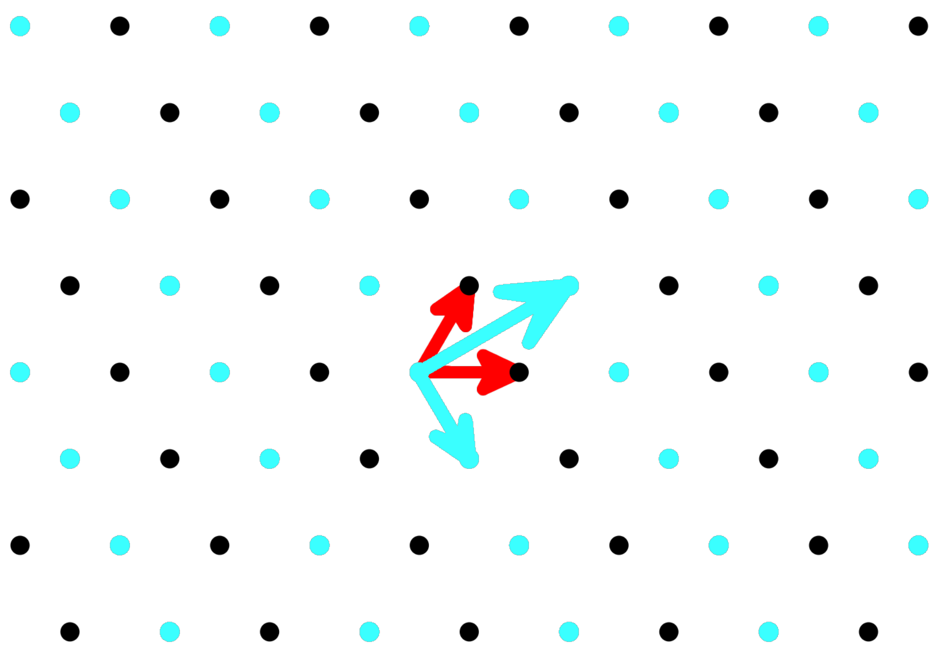
Suppose now that in $\mathbb{K}^n$, we have a lattice J which is contained in another lattice I; we then say that J is a *sublattice* of I. In particular, J is an additive subgroup of I, so it makes sense to consider the quotient group I/J; the cardinal of this quotient is then called the *index* of J in I, and we write it $[I : J]$.

Remark 2.2.3. This is the same notation as for the degree of a field extension, although these are rather different notions ! Unfortunately, these notations are well-established, so we cannot change them.

Theorem 2.2.4. *[Computation of the index] Suppose we have a lattice I in $\mathbb{K}^n$, and a sublattice $J \subseteq I$ be a sublattice. Fix a $\mathbb{Z}$-basis $v_1, \cdots, v_n$ of I, and a $\mathbb{Z}$-basis $w_1, \cdots w_n$ of J, and form the $n \times n$ matrix A expressing the w_j in terms of the v_i. Since $J \subset I$, the entries of A all lie in $\mathbb{Z}$; besides, $\det A \neq 0$ since the v_i and the w_j are two $\mathbb{K}$-bases of the vector space $\mathbb{K}^n$. The index of J in I is then given by $[I : J] = |\det A|$; in particular, it is always finite.*

We thus recover the fact that $I = J$ if and only if $\det A = \pm 1$.

Example 2.2.5. Let I be the lattice in the previous picture, and let us pick two linearly independent vectors (in blue) in I:



Since these vectors are linearly independent, they form another $\mathbb{K}$-basis of $\mathbb{K}^2$, so they span another lattice J. Besides, since these vectors lie in I, the lattice J is contained in I, so J is a sublattice of I.

In order to know whether J agrees I or is a strict sublattice, and more generally to compute the index of J in I, we form the matrix A expressing the $\mathbb{Z}$-basis of J in terms of the $\mathbb{Z}$-basis of I, in other words the blue vectors in terms of the red vectors:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

and we compute

$$|\det A| = |-2| = 2.$$

This result means that J vectors has index 2 in I; in particular, the containment $J \subsetneq I$ is proper: not every point of I can be expressed as a $\mathbb{Z}$-combination of the blue vectors. The fact that the index is 2 expresses that precisely half of the points I actually lie J, which becomes clear if we colourise the points of J in blue as on the picture above.

2.2.2 Orders

Definition 2.2.6. Let K be a number field of degree n. An *order* in K is a subring $\mathcal{O}$ of K which is also a lattice in the $\mathbb{Q}$-vector space K.

Example 2.2.7. For example, $\mathbb{Z}[\sqrt{5}]$ is an order in $\mathbb{Q}(\sqrt{5})$, whereas $\mathbb{Z}[\frac{1}{2}\sqrt{5}]$ is not (it is a subring but not a lattice), and neither is $\mathbb{Z} \oplus \mathbb{Z}\frac{1}{2}\sqrt{5}$ (it is a lattice but not a subring). Finally, $\mathbb{Z}[\sqrt{2}]$ is not an order in $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, because it does not span all of K over $\mathbb{Q}$.

Remark 2.2.8. Let $\mathcal{O} \subset K$ be an order. Then $\mathcal{O}$ is in particular a lattice in K, so it has a $\mathbb{Z}$-basis $\omega_1, \cdots, \omega_n$ (in fact it has many), where $n = [K : \mathbb{Q}]$. This basis is also a $\mathbb{Q}$-basis of K , so every $\alpha \in K$ can be written (uniquely) as $\alpha = \sum_{j=1}^{n} \lambda_j \omega_j$ with $\lambda_j \in \mathbb{Q}$. Clearing the denominators, we deduce that for all $\alpha \in K$ there exists $n \in \mathbb{N}$ such that $n\alpha \in \mathcal{O}$. In particular, the field of fractions of $\mathcal{O}$ is K.

More generally, theorem 2.1.6 tells us that $\mathbb{Z}[\alpha]$ is an order in $\mathbb{Q}(\alpha)$ whenever α is an algebraic integer. In fact, the relation between algebraic integers and latticies is even stronger:

Proposition 2.2.9. *Let α be an algebraic number. The following are equivalent:*

1. *α is an algebraic integer,*
2. *$\mathbb{Z}[\alpha]$ is an order in $\mathbb{Q}(\alpha)$,*
3. *There exist a number field K containing α and a lattice I in K which is stable under multiplication by α, i.e. such that $\alpha I \subseteq I$.*

Proof.

- $1 \Longrightarrow 2$: Let $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ be the degree of α over $\mathbb{Q}$. Then we know by theorem 1.2.3 that $1, \alpha, \cdots, \alpha^{n-1}$ is a $\mathbb{Q}$-basis of K, and theorem 2.1.6 tells us that $\mathbb{Z}[\alpha]$ is the lattice corresponding to this basis. Besides, $\mathbb{Z}[\alpha]$ is a subring of K by definition.
- $2 \Longrightarrow 3$: Simply take $K = \mathbb{Q}(\alpha)$ and $I = \mathbb{Z}[\alpha]$.
- $3 \Longrightarrow 1$: If $\alpha I \subset I$, then the matrix of the multiplication-by-α map μ_α of L with respect to a $\mathbb{Z}$-basis of I is a matrix with coefficients in $\mathbb{Z}$, so by definition $\chi_{\mathbb{Q}}^K(\alpha)$ lies in $\mathbb{Z}[x]$, which implies that α is an algebraic integer.

□

Corollary 2.2.10. *Let $\mathcal{O}$ be an order in a number field K. Every element of $\mathcal{O}$ is an algebraic integer, so $\mathcal{O} \subseteq \mathbb{Z}_K$.*

This explains why we did not manage to find an order in $\mathbb{Q}(\sqrt{5})$ containing $\sqrt{5}/2$: indeed, $\sqrt{5}/2$ is not an algebraic integer, since its minimal polynomial is $x^2 - 5/4 \notin \mathbb{Z}[x]$.

Corollary 2.2.11. *Let α be an element of a number field K. The subring $\mathbb{Z}[\alpha]$ of K is an order in K if and only if α is both a primitive element for $K/\mathbb{Q}$ and an algebraic integer.*

2.2.3 Discriminants, part I

Definition 2.2.12. Let K be a number field of degree n. The *trace pairing* is the bilinear form

$$\begin{array}{rcl} \mathrm{Tr}\colon K \times K & \longrightarrow & \mathbb{Q} \\ (\alpha, \beta) & \longmapsto & \mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha\beta) \end{array}.$$

Let $\alpha_1, \cdots, \alpha_n$ be n elements of K. Their *discriminant* is the determinant

$$\mathrm{disc}(\alpha_1, \cdots, \alpha_n) = \det \Big(\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha_i \alpha_j) \Big)_{1 \leqslant i,j \leqslant n} \in \mathbb{Q}.$$

Proposition 2.2.13. $\mathrm{disc}(\alpha_1, \cdots, \alpha_n) \neq 0$ *if and only if the* α_j *are* $\mathbb{Q}$*-linearly independent, that is to say if and only if they form a* $\mathbb{Q}$*-basis of* K*.*

Proof. Let $T \in \mathrm{Mat}_{n \times n}(\mathbb{Q})$ be the matrix such that $T_{i,j} = \mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha_i \alpha_j)$, so that $\mathrm{disc}(\alpha_1, \cdots, \alpha_n) = \det T$.

If the α_j are $\mathbb{Q}$-linearly dependent, then we get a relation of linear dependency on the columns (and also on the rows) of T, so $\det T = 0$.

Conversely, suppose that the α_j form a $\mathbb{Q}$-basis of K. If we had $\det T = 0$, we would deduce a linear dependency relation between the columns of T; in other words, we would have $\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha_i \alpha) = 0$ for all i for some $\alpha = \sum_{j=1}^{n} \lambda_j \alpha_j$ with $\lambda_j \in \mathbb{Q}$ not all zero. Since the α_j form a $\mathbb{Q}$-basis of K, this means that $\alpha \neq 0$, and that $\mathrm{Tr}_{\mathbb{Q}}^{K}(\beta\alpha) = 0$ for all $\beta \in K$. But this is absurd (take $\beta = \frac{1}{\alpha}$, and note that $\mathrm{Tr}_{\mathbb{Q}}^{K}(1) = n \neq 0$). □

Definition 2.2.14. Let $\mathcal{O}$ be an order in a number field K, and let $(\omega_j)_{1 \leqslant j \leqslant n}$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. The *discriminant* of $\mathcal{O}$ is

$$\mathrm{disc}\, \mathcal{O} = \mathrm{disc}(\omega_1, \cdots, \omega_n) \in \mathbb{Z},$$

a non-zero integer.

Remark 2.2.15. This does not depend on the chosen $\mathbb{Z}$-basis of $\mathcal{O}$. Indeed, using another $\mathbb{Z}$-basis amounts to replacing the matrix $T = \big(\mathrm{Tr}_{\mathbb{Q}}^{K}(\omega_i \omega_j) \big)_{i,j}$ with ${}^{\mathrm{t}}PTP$, where $P \in \mathrm{GL}_n(\mathbb{Z})$ is the transition matrix between the two bases and ${}^{\mathrm{t}}P$ is its transpose, but $\det {}^{\mathrm{t}}PTP = \det T$ since $\det P = \det {}^{\mathrm{t}}P = \pm 1$.

We now arrive to the central result of this chapter:

Theorem 2.2.16. *The ring of integers of a number field is an order in this number field.*

Example 2.2.17. Let us continue with example 1.3.10. An element $\alpha = a+b\sqrt{-7}$, $a, b \in \mathbb{Q}$ of $K = \mathbb{Q}(\sqrt{-7})$ lies in $\mathbb{Z}_K$ if and only if its characteristic polynomial $x^2-2ax+a^2+7b^2$ lies in $\mathbb{Z}[x]$, that is to say if and only if $2a \in \mathbb{Z}$ and $a^2+7b^2 \in \mathbb{Z}$. One checks easily that this condition is equivalent to $2a \in \mathbb{Z}$, $2b \in \mathbb{Z}$, and $a+b \in \mathbb{Z}$; thus

$$\mathbb{Z}_K = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{-7}}{2} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right].$$

The middle term makes it apparent that $\mathbb{Z}_K$ is a lattice, with $\mathbb{Z}$-basis $(1, \frac{1+\sqrt{-7}}{2})$; the right term makes it clear that $\mathbb{Z}_K$ is a ring.

In order to prove theorem 2.2.16, we need the following lemma, which is important in its own right:

Lemma 2.2.18. *Let K be a number field, and let α in K. There exists an integer $d \in \mathbb{N}$ such that $d\alpha$ is an algebraic integer.*

Proof. Let $\chi(x) \in \mathbb{Q}[x]$ be the characteristic polynomial of α, and let $d \in \mathbb{N}$ be a common denominator for the coefficients of $\chi(x)$, so that we may write

$$0 = \chi(\alpha) = \alpha^n + \sum_{j=0}^{n-1} \frac{\lambda_j}{d}\alpha^j$$

where $n = [K : \mathbb{Q}]$ and the λ_j are integers. Multiplying by d^n, we get

$$0 = d^n\chi(\alpha) = (d\alpha)^n + \sum_{j=0}^{n-1} d^{n-j}\lambda_j(d\alpha)^j,$$

which proves that $d\alpha$ is an algebraic integer. $\square$

Note that this implies in particular that the fraction field of $\mathbb{Z}_K$ is K itself (compare with remark 2.2.8).

Proof of theorem 2.2.16. We already know that $\mathbb{Z}_K$ is a subring, and we must show that it is also a lattice. According to the lemma, we can find a $\mathbb{Q}$-basis $(\omega_j)_{1\leqslant j\leqslant n}$ of K formed of algebraic integers; let

$$\Omega = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$$

be the lattice it spans. Let now $\alpha \in \mathbb{Z}_K$. We may write

$$\alpha = \sum_{j=1}^{n} \lambda_j \omega_j$$

where the λ_j are rational numbers. Multiplying by ω_k, $1 \leqslant k \leqslant n$, and taking the trace yields the $n \times n$ system of linear equations

$$\sum_{j=1}^{n} \lambda_j \operatorname{Tr}(\omega_j \omega_k) = \operatorname{Tr}(\alpha \omega_k) \quad (1 \leqslant k \leqslant n)$$

over $\mathbb{Z}$, of which the λ_j form a solution. The determinant of this system is $\Delta = \operatorname{disc}(\omega_1, \cdots, \omega_n)$, which is a nonzero integer since the ω_j are algebraic integers and form a $\mathbb{Q}$-basis of K. By inverting the matrix of the system, we thus see that the λ_j lie in $\frac{1}{\Delta}\mathbb{Z}$. We thus have

$$\Omega \subset \mathbb{Z}_K \subset \frac{1}{\Delta}\Omega,$$

which shows that $\mathbb{Z}_K$, being cornered between two lattices, is itself a lattice. □

Definition 2.2.19. In view of corollary 2.2.10, the ring of integers $\mathbb{Z}_K$ of K is thus an order which contains all the other orders of K as sublattices; it is therefore sometimes called the *maximal order* of K.

Definition 2.2.20. By theorem 2.2.4, every order is contained in $\mathbb{Z}_K$ with a finite index, and this index is called the *index* of the order.

Definition 2.2.21. The *discriminant* of K is defined as the discriminant of its ring of integers seen as an order, i.e.

$$\operatorname{disc} K = \operatorname{disc} \mathbb{Z}_K \in \mathbb{Z},$$

a nonzero integer.

Example 2.2.22. Let us continue with example 2.2.17. We now know that the ring of integers of $K = \mathbb{Q}(\sqrt{-7})$ is

$$\mathbb{Z}_K = \mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha,$$

where $\alpha = \frac{1+\sqrt{-7}}{2}$. As a consequence, we find that

$$\operatorname{disc} K = \operatorname{disc} \mathbb{Z}_K = \begin{vmatrix} \mathrm{Tr}_{\mathbb{Q}}^K(1) & \mathrm{Tr}_{\mathbb{Q}}^K(1 \cdot \alpha) \\ \mathrm{Tr}_{\mathbb{Q}}^K(\alpha \cdot 1) & \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^2) \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & -3 \end{vmatrix} = -7.$$

We will soon see a much more efficient way to get to the same result.

To conclude this section, let us mention a famous result of Hermite's:

Theorem 2.2.23 (Hermite-Minkowski)**.** *Up to isomorphism, there are finitely many number fields of given discriminant.*

2.3 Computing the maximal order

Given a number field K, it is (usually) not difficult to find orders in K. For instance, if it is given in the form $K = \mathbb{Q}(\alpha)$, we may assume without loss of generality that the primitive element α is integral thanks to lemma 2.2.18, and then $\mathcal{O} = \mathbb{Z}[\alpha]$ is clearly an order in K. It may not, however, be the full ring of integers of K.

2.3.1 Denominators vs. the index

Here is a consequence of the definition of the index of an order.

Proposition 2.3.1. *Let $\mathcal{O}$ be an order in a number field K of degree n, let $f \in \mathbb{N}$ be its index, and let $(\omega_j)_{1 \leqslant j \leqslant n}$ be any $\mathbb{Z}$-basis of $\mathcal{O}$. In particular, $(\omega_j)_{1 \leqslant j \leqslant n}$ is also a $\mathbb{Q}$-basis of K, so every element of K can be uniquely written in the form $\sum_{j=1}^n \lambda_j \omega_j$ with $\lambda_j \in \mathbb{Q}$. Let $\operatorname{denom}_{\mathcal{O}}\left(\sum_{j=1}^n \lambda_j \omega_j\right)$ denote the lcm of the denominators of the λ_j. Then $\operatorname{denom}_{\mathcal{O}}\left(\sum_{j=1}^n \lambda_j \omega_j\right)$ depends on $\mathcal{O}$, but not on the choice of the $\mathbb{Z}$-basis $(\omega_j)_{1 \leqslant j \leqslant n}$ of $\mathcal{O}$.*

Furthermore, we have $\operatorname{denom}_{\mathcal{O}}(\beta) \mid f$ for all $\beta \in \mathbb{Z}_K$; conversely, for all $p \in \mathbb{N}$ prime, there exists $\beta \in \mathbb{Z}_K$ such that $\operatorname{denom}_{\mathcal{O}}(\beta) = p$.

In other words, when the elements of $\mathbb{Z}_K$ are put in the form $\sum_j \lambda_j \omega_j$, the primes $p \in \mathbb{N}$ that divide the denominator of one (or more) of the λ_j are exactly the ones that divide f. For example, if $\mathcal{O}$ is of the form $\mathbb{Z}[\alpha]$, we may consider the $\mathbb{Z}$-basis $1, \alpha, \cdots \alpha^{n-1}$ of $\mathcal{O}$, and $\operatorname{denom}_{\mathcal{O}}(\beta)$ is then the common denominator of the coefficients of β expressed as a polynomial of degree $< n$ in α.

Proof. (Non examinable) Think of $\mathcal{O}$, $\mathbb{Z}_K$ and K as additive groups. Then for every $\beta \in K$, $\operatorname{denom}_{\mathcal{O}}(\alpha)$ is the order of this element in the quotient group $K/\mathcal{O}$, since

$$\forall n \in \mathbb{N}, \quad n\beta = 0 \text{ in } K/\mathcal{O} \iff n\beta \in \mathcal{O} \iff \operatorname{denom}_{\mathcal{O}}(\beta) \mid n.$$

Therefore, $\operatorname{denom}_{\mathcal{O}}(\beta)$ depends on $\mathcal{O}$ but not on the choice of a $\mathbb{Z}$-basis of $\mathcal{O}$.

Besides, $\mathbb{Z}_K/\mathcal{O}$ is an Abelian group whose order is by definition f, so the order of every element of $\mathbb{Z}_K$ divides f by Lagrange's theorem; conversely, for all $p \mid f$ prime, Cauchy's theorem tells us that there exists an element of $\mathbb{Z}_K/\mathcal{O}$ of order exactly p. □

Example 2.3.2. In $K = \mathbb{Q}(\sqrt{-7})$, the order $\mathcal{O} = \mathbb{Z}[\sqrt{-7}]$ is not the full ring of integers of K; in fact, we know from example 2.2.22 that $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, so $\mathcal{O}$ is a non-maximal order of index 2. By the theorem, if we express the elements of K in the form $a + b\sqrt{-7}$ with $a, b \in \mathbb{Q}$, then the denominator of every element of $\mathbb{Z}_K$ is a power of 2; for instance, $\mathbb{Z}_K \ni \frac{1+\sqrt{-7}}{2} = \frac{1}{2} + \frac{1}{2}\sqrt{-7}$.

2.3.2 Discriminants, part II

The general approach to compute $\mathbb{Z}_K$ consists in starting with an order of the form $\mathbb{Z}[\alpha]$, and enlarging it until it becomes maximal. We need to know when we can stop, that is to say when the order is maximal. For this, the following relation between the discriminant of and order and its index is primordial.

Theorem 2.3.3. *Let K be a number field, and let $\mathcal{O}$ be an order in K of index $f \in \mathbb{N}$. Then*

$$\operatorname{disc} \mathcal{O} = f^2 \operatorname{disc} K.$$

Proof. Let $(\omega_j)_{1 \leqslant j \leqslant n}$ be a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, and let T be the matrix of the $\operatorname{Tr}_{\mathbb{Q}}^K(\omega_i\omega_j)$, so that $\det T = \operatorname{disc} K$. If $P \in \operatorname{Mat}_{n\times n}(\mathbb{Z})$ is the change of basis matrix expressing a $\mathbb{Z}$-basis of $\mathcal{O}$ on the ω_i, then we have $\det P = \pm f$ by theorem 2.2.4, so $\operatorname{disc} \mathcal{O} = \det({}^{\mathrm{t}}PTP) = f^2 \operatorname{disc} K$. □

Definition 2.3.4. For prime $p \in \mathbb{N}$, let us say that $\mathcal{O}$ is *p-maximal* if p does not divide the index of $\mathcal{O}$.

Corollary 2.3.5. *Let $\mathcal{O}$ be an order in a number field K. If $\mathcal{O}$ is not p-maximal, then $p^2 \mid \operatorname{disc} \mathcal{O}$. In particular, if $\operatorname{disc} \mathcal{O}$ is squarefree, then $\mathcal{O} = \mathbb{Z}_K$ and $\operatorname{disc} K = \operatorname{disc} \mathcal{O}$.*

This allows us to compute the ring of integers when the discriminant of the field is squarefree; unfortunately, it is usually not the case. We will see other criteria for the p-maximality of orders in the next chapter.

To use theorem 2.3.3, we need to be able to compute discriminants of orders of the form $\mathbb{Z}[\alpha]$. In this view, we introduce the discriminant of a polynomial.

Definition 2.3.6. Let $\mathcal{R}$ be a domain, and let $A(x) \in \mathcal{R}[x]$ be a monic polynomial of degree $n \in \mathbb{N}$ and leading coefficient $a \in \mathcal{R}$. The *discriminant* of $A(x)$ is

$$\operatorname{disc} A = \frac{(-1)^{n(n-1)/2}}{a} \operatorname{Res}(A, A').$$

Remark 2.3.7. It can be easily seen on the definition of the resultant as a determinant that $\operatorname{Res}(A, A')$ must be divisible by a, so $\operatorname{disc} A$ lies in $\mathcal{R}$.

Example 2.3.8. Let $A(x) = ax^2 + bx + c$, $a \neq 0$. Then $A'(x) = 2ax + b$, so that

$$\operatorname{Res}(A, A') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = 4a^2c - ab^2,$$

so we recover the well-known formula

$$\operatorname{disc} A = \frac{-1}{a} \operatorname{Res}(A, A') = b^2 - 4ac.$$

Theorem 2.3.9. *Let K be a field, and $A(x) \in K[x]$ be a polynomial of degree $n \in \mathbb{N}$ and leading coefficient $a \in K$. Let Ω be a field large enough to contain all the roots of $A(x)$, and let $\alpha_1, \dots, \alpha_n \in \Omega$ be these roots, repeated with multiplicity. Then*

$$\begin{aligned} \operatorname{disc} A &= (-1)^{n(n-1)/2} a^{n-2} \prod_{j=1}^{n} P'(\alpha_j) \\ &= (-1)^{n(n-1)/2} a^{2n-2} \prod_{j \neq k} (\alpha_j - \alpha_k) \\ &= a^{2n-2} \prod_{j<k} (\alpha_j - \alpha_k)^2. \end{aligned}$$

Proof. The first equality is just an application of theorem 1.1.2. Then, since

$$A(x) = a\prod_{j=1}^{n}(x-\alpha_j),$$

we have

$$A'(x) = a\sum_{j=1}^{n}\prod_{k\neq j}(x-\alpha_k)$$

so

$$A'(\alpha_j) = a\prod_{k\neq j}(\alpha_j-\alpha_k),$$

whence the result. □

Corollary 2.3.10. *$A(x)$ has multiple roots if and only if* $\operatorname{disc} A = 0$.

As discriminants can be tedious to compute explicitly, we establish once and for all the following formula.

Proposition 2.3.11. *(Non examinable) For all $n \in \mathbb{N}$ and $b, c \in \mathbb{Q}$, we have*

$$\operatorname{disc}(x^n+bx+c) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big).$$

Proof. Let us introduce $\zeta = e^{2\pi i/(n-1)}$, and $\beta \in \mathbb{C}$ such that $\beta^{n-1} = -b/n$.

According to theorem 1.1.2, the resultant of P and P' can be computed in two ways: as the product of the values of P at the roots of P' (essentially), and vice versa. Here, the first way is easier, because the roots of P' are easy to express and manipulate. Explicitly, we have $P'(x) = nx^{n-1}+b$, whose complex roots are the $\zeta^k\beta$, $0 \leqslant k < n-1$, and

$$P(\zeta^k\beta) = \zeta^{kn}\beta^n + b\zeta^k\beta + c = \zeta^k\left(-\frac{\beta}{n}\right) + b\zeta^k\beta + c = \left(1-\frac{1}{n}\right)\beta\zeta^k b + c.$$

Therefore,

$$\begin{aligned}
\operatorname{Res}(P, P') &= n^n \prod_{k=0}^{n-2} P(\zeta^k \beta) \qquad \text{because the leading coefficient of } P' \text{ is } n \\
&= n^n \prod_{k=0}^{n-2} \left(\left(1 - \frac{1}{n} \right) \beta \zeta^k b + c \right) \\
&= n^n (-1)^{n-1} \prod_{k=0}^{n-2} \left(-c - \zeta^k \left(1 - \frac{1}{n} \right) \beta b \right) \\
&= n^n (-1)^{n-1} \left(\big(-c \big)^{n-1} - \big((1 - 1/n)\beta b \big)^{n-1} \right) \text{ as } \prod_{k=0}^{n-2} (x - \zeta^k y) = x^{n-1} - y^{n-1} \\
&= n^n c^{n-1} - n^n \beta^{n-1} b^{n-1} (1/n - 1)^{n-1} \\
&= n^n c^{n-1} - n \left(-\frac{b}{n} \right) (1 - n)^{n-1} b^{n-1} \\
&= n^n c^{n-1} + (1 - n)^{n-1} b^n.
\end{aligned}$$

The result then follows since $\operatorname{disc} P = (-1)^{n(n-1)/2} \operatorname{Res}(P, P')$. □

Corollary 2.3.12. *(Examinable) In particular, we obtain the important formula*

$$\operatorname{disc}(x^3 + bx + c) = -4b^3 - 27c^2,$$

which you should learn by heart.

So far, we have introduced two notions of discriminants, one for orders, and one for polynomials. We now show that these notions coincide.

Theorem 2.3.13. *Let $K = \mathbb{Q}(\alpha)$ be a number field, where α is integral, and let $m(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Then*

$$\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc} m.$$

Proof. Let $\alpha_1, \cdots, \alpha_n$ be the complex roots of $m(x)$ where $n = [K : \mathbb{Q}]$, and consider the matrix

$$A = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

Vandermonde tells us that $\det A = \prod_{j<k}(\alpha_k - \alpha_j)$. Besides, if $B = {}^{\mathrm{t}}AA$, then we have

$$B_{i,j} = \sum_{k=1}^{n} A_{k,i}A_{k,j} = \sum_{k=1}^{n} \alpha_k^{i-1}\alpha_k^{j-1} = \sum_{k=1}^{n} \alpha_k^{i+j-2} = \mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha^{i+j-2}) = \mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha^{i-1}\alpha^{j-1})$$

according to corollary 1.3.9. Since $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$, we conclude that

$$\operatorname{disc}\mathbb{Z}[\alpha] = \det B = (\det A)^2 = \prod_{j<k}(\alpha_j - \alpha_k)^2 = \operatorname{disc} m$$

since m is monic. □

We immediately deduce the following consequence:

Proposition 2.3.14. *Let K be a number field of signature (r_1, r_2). Then the sign of $\operatorname{disc} K$ is $(-1)^{r_2}$.*

Proof. Again, write $K = \mathbb{Q}(\alpha)$ where α is integral, let $m(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, and let $\alpha_1, \cdots, \alpha_n$ be its complex roots, ordered so that $\alpha_1, \cdots, \alpha_{r_1}$ are real and $\overline{\alpha_{r_1+j}} = \alpha_{r_1+r_2+j}$ for $1 \leqslant j \leqslant r_2$. We have

$$\operatorname{disc}\mathbb{Z}[\alpha] = \operatorname{disc} m = \prod_{j<k}(\alpha_j - \alpha_k)^2.$$

When j and k are both less than r_1, $(\alpha_j - \alpha_k)^2$ is the square of a real number and is thus positive. The other terms can be grouped in conjugate pairs and produce factors $\big(\pm|\alpha_j - \alpha_k|^2\big)^2$, which are also positive, except when $j, k > r_1$ and $k = j + r_2$, in which case we get $(\alpha_j - \alpha_k)^2 = (\alpha_j - \overline{\alpha_j})^2 < 0$. As a result, the sign of $\operatorname{disc} m$ is $(-1)^{r_2}$. Since $\operatorname{disc} K$ differs of $\operatorname{disc}\mathbb{Z}[\alpha]$ by a square (thus positive) factor, the result follows. □

Example 2.3.15. Let $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $f(x) = x^3 + x^2 - 2x + 8 = 0$. Since $f(x)$ is irreducible, this number field is well-defined and has degree 3, so its signature is either $(3, 0)$ or $(1, 1)$. One may compute that

$$\operatorname{disc}(x^3 + x^2 - 2x + 8) = -2012 = -2^2 \cdot 503.$$

Since this is negative, we can conclude that the signature of K is $(1, 1)$, which means that the polynomial $f(x)$ has one real root and one pair of complex conjugate nonreal roots.

Besides, as 503 is prime, theorem 2.3.3 implies that the order $\mathcal{O} = \mathbb{Z}[\alpha]$ is p-maximal for all p except maybe $p = 2$, and that the index of $\mathcal{O}$ divides 2. As a result, either $\mathcal{O} = \mathbb{Z}_K$ and $\operatorname{disc} K = -2012$, or $\mathcal{O}$ has index 2 and $\operatorname{disc} K = -503$.

In fact, since it can be checked that $\beta = \frac{\alpha^2+\alpha}{2}$ is an algebraic integer, $\mathcal{O}' = \mathbb{Z}[\alpha, \beta]$ is an order in which $\mathcal{O}$ has index 2 (if this is not obvious to you, write down the matrix expressing a $\mathbb{Z}$-basis of $\mathcal{O}$ on a $\mathbb{Z}$-basis of $\mathcal{O}'$, and check that its determinant is ± 2), so $\mathbb{Z}_K = \mathcal{O}'$ and $\operatorname{disc} K = -503$.

This example has the particularity that no order of the form $\mathbb{Z}[\gamma]$ is 2-maximal, whatever the algebraic integer $\gamma \in \mathbb{Z}_K$ is; we will see why in the next chapter (example 3.8.6). In particular, $\mathbb{Z}_K$ cannot be written in the form $\mathbb{Z}[\gamma]$ in the case of this number field.

2.4 The case of quadratic fields

Definition 2.4.1. A *quadratic field* is a number field of degree 2.

The classical formulae used to solve equations of degree 2 show that every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is squarefree and different from 0 and 1.

Quadratic fields are small enough that their ring of integers can be determined explicitly.

Theorem 2.4.2. *Let $d \in \mathbb{Z}$, $d \neq 1$ be a squarefree integer, and let $K = \mathbb{Q}(\sqrt{d})$. If $d \equiv 1 \bmod 4$, then $\mathbb{Z}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ and $\operatorname{disc} K = d$, whereas if $d \not\equiv 1 \bmod 4$, then $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$ and $\operatorname{disc} K = 4d$.*

Proof. First, note that $4 \nmid d$ since d is squarefree; thus $d \equiv 1, 2$, or $3 \bmod 4$.

The discriminant of the order $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$ is

$$\operatorname{disc} \mathcal{O} = \operatorname{disc}(x^2 - d) = 4d.$$

Since d is squarefree, we deduce by theorem 2.3.3 that the index of $\mathcal{O}$ is either 1 or 2, and that $\operatorname{disc} K = 4d$ or d, respectively.

Suppose that the index of $\mathcal{O}$ is 2. Since $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ by theorem 2.1.6, proposition 2.3.1 tells us that there exist $a, b \in \mathbb{Z}$ not both even such that

$\frac{a+b\sqrt{d}}{2} \in \mathbb{Z}_K$. If $b = 2b'$ were even, then $a = 2a' + 1$ would be odd; but $a' + b'\sqrt{d} \in \mathcal{O} \subset \mathbb{Z}_K$ by corollary 2.2.10, so we would have

$$\frac{1}{2} = \frac{a+b\sqrt{d}}{2} - (a' + b'\sqrt{d}) \in \mathbb{Z}_K,$$

which contradicts proposition 2.1.11. Similarly, the case a even, b odd implies that $\frac{1}{2}\sqrt{d} \in \mathbb{Z}_K$, which is also absurd since its characteristic polynomial relative to $K/\mathbb{Q}$ is $x^2 - \frac{d}{4} \notin \mathbb{Z}[x]$ as $4 \nmid d$. So a and b must both be odd, which by a similar line of reasoning implies that $\frac{1+\sqrt{d}}{2} \in \mathbb{Z}_K$. Its characteristic polynomial is

$$\left(x - \frac{1+\sqrt{d}}{2}\right)\left(x - \frac{1-\sqrt{d}}{2}\right) = x^2 - x + \frac{1-d}{4},$$

which lies in $\mathbb{Z}[x]$ iff. $d \equiv 1 \bmod 4$. Therefore, if $d \not\equiv 1 \bmod 4$, then the index of $\mathcal{O}$ cannot be 2, so it must be 1, so $\mathbb{Z}_K = \mathcal{O} = \mathbb{Z}[\sqrt{d}]$ in this case.

On the contrary, if $d \equiv 1 \bmod 4$, then $\frac{1+\sqrt{d}}{2} \in \mathbb{Z}_K \setminus \mathcal{O}$, so $\mathcal{O} \subsetneq \mathbb{Z}_K$. We then have have $\mathcal{O} \subsetneq \mathcal{O}' = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ since $\sqrt{d} = 2\frac{1+\sqrt{d}}{2} - 1$; the transition matrix between the $\mathbb{Z}$-basis $(1, \sqrt{d})$ of $\mathcal{O}$ and the $\mathbb{Z}$-basis $(1, \frac{1+\sqrt{d}}{2})$ of $\mathcal{O}'$ is $\begin{pmatrix} 1 & 1/2 \\ 0 & 1/2 \end{pmatrix}$ so $[\mathcal{O}' : \mathcal{O}] = 2$, so

$$\operatorname{disc} \mathcal{O}' = \frac{1}{2^2} \operatorname{disc} \mathcal{O} = d$$

by theorem 2.3.3. As d is squarefree, this forces $\mathbb{Z}_K = \mathcal{O}'$. □

Example 2.4.3. The ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$, and its discriminant is -4. Similarly, the ring of integers of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$, and its discriminant is 8, but the ring of integers of $\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, and its discriminant is 5.

2.5 The case of cyclotomic fields

Cyclotomic fields are another important class of number fields whose ring of integers is easily described.

Definition 2.5.1. An algebraic number ζ satisfying $\zeta^n = 1$ for some $n \in \mathbb{N}$ is called an n^{th} *root of unity.* If $\zeta^m \neq 1$ for $m < n$, then it is a *primitive* n^{th} root of unity. Thus in $\mathbb{C}$ the n^{th} roots of unity are the $e^{2k\pi i/n}$, $0 \leqslant k < n$, and the primitive ones are the ones for which k and n are coprime.

The n^{th} *cyclotomic polynomial* is

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive } n^{\text{th}} \\ \text{root of unity} \in \mathbb{C}}} (x - \zeta) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - e^{2k\pi i/n}).$$

It has degree $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ (Euler's phi function). Moreover, it lies in $\mathbb{Z}[x]$, and it is irreducible over $\mathbb{Z}$ (and hence over $\mathbb{Q}$).

The n^{th} *cyclotomic field* is $\mathbb{Q}(\zeta)$, where ζ is any primitive n^{th} root of unity. It is thus a number field of degree $\varphi(n)$.

Theorem 2.5.2. *Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive n^{th} root of unity, $n \in \mathbb{N}$. Then*

1. $\mathbb{Z}_K = \mathbb{Z}[\zeta]$, *and*

2. *(Non examinable) Let $n = \prod_j p_j^{v_j}$ be the factorisation of n, with $p_j \in \mathbb{N}$ distinct primes and $v_j \in \mathbb{N}$. Then*

$$\operatorname{disc} K = \frac{(-1)^{\varphi(n)/2} n^{\varphi(n)}}{\prod_j p_j^{\varphi(n)/(p_j - 1)}} = (-1)^{\varphi(n)/2} \prod_j p_j^{\varphi(n/p_j) p_j^{v_j - 1} \left((p_j - 1) v_j - 1\right)}.$$

In particular, when $n = p^v$ is a prime power, then $\operatorname{disc} K = \pm p^{p^{v-1}(pv - v - 1)}$; *more generally, for $p \in \mathbb{N}$ an odd prime we have*

$$p \mid \operatorname{disc} K \Longleftrightarrow p \mid n,$$

and for $p = 2$ we have

$$2 \mid \operatorname{disc} K \Longleftrightarrow 4 \mid n.$$

Chapter 3

Ideals and factorisation

In the previous chapter, we have defined the ring of integers $\mathbb{Z}_K$ of a number field K. We are now going to investigate the properties of this ring.

A very important (and a first glance disappointing) thing to notice is that in general, we do not have uniqueness of factorisation in $\mathbb{Z}_K$, as demonstrated by the following example.

Example 3.0.1. Take $K = \mathbb{Q}(\sqrt{-5})$, so that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$ by theorem 2.4.2. In $\mathbb{Z}_K$, a number $\alpha = a + b\sqrt{-5}$ $(a, b \in \mathbb{Z})$ is invertible if and only if its norm $N_{\mathbb{Q}}^K(\alpha) = a^2 + 5b^2$ is 1, as can be easily seen from the formulae $N_{\mathbb{Q}}^K(\alpha\beta) = N_{\mathbb{Q}}^K(\alpha)N_{\mathbb{Q}}^K(\beta)$ and $\alpha^{-1} = \frac{\bar{\alpha}}{N_{\mathbb{Q}}^K(\alpha)}$. In particular two associate elements must have the same norm.

Consider the two factorisations

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

No factor of the first one is associate to a factor of the second one, because the norms of these factors are respectively 4, 9, 6 and 6. Besides, these factors are irreducible: if they were not, by taking norms, we would get integer solutions to $a^2 + 5b^2 = 2$ or 3, which is clearly impossible. We thus have two complete and yet distinct factorisations of 6 in $\mathbb{Z}_K$.

A great insight came from Kummer, who imagined that there should exist what he called "ideal numbers" $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_4$ such that $2 = \mathfrak{p}_1\mathfrak{p}_2$, $3 = \mathfrak{p}_3\mathfrak{p}_4$, $1+\sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3$, and $1-\sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4$. Indeed, this would allow us to recover a unique factorisation

$$6 = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4).$$

We will see that the ring of integers is what is called a Dedekind domain, which means that it enjoys very nice properties which make up for the non-uniqueness of factorisation: in a nutshell, we do not have uniqueness of factorisation of *elements*, but we will see that we have uniqueness of factorisation of *ideals*. We we will study the non-uniqueness of factorisation of elements more closely in chapter 4.

3.1 Reminder on finite fields

Theorem 3.1.1.

1. *The cardinal of a finite field is always a prime power.*
2. *Conversely, if $q = p^n$ is a prime power, then there exists a finite field with q elements.*
3. *If two finite fields have the same number of elements, then they are isomorphic.*

This justifies the notation $\mathbb{F}_q$ for "the" finite field of size q when $q \in \mathbb{N}$ is a prime power. For instance, we have $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ for all prime $p \in \mathbb{N}$. Note however that $\mathbb{F}_{p^n} \not\simeq \mathbb{Z}/p^n\mathbb{Z}$ when $n \geqslant 2$, as the latter is not a field.

Theorem 3.1.2. *Let q and r be prime powers. Then $\mathbb{F}_q$ is isomorphic to a subfield of $\mathbb{F}_r$ if and only if r is a power of q.*

In particular, if $q = p^f$ with $p \in \mathbb{N}$ prime and $f \in \mathbb{N}$, then $\mathbb{F}_q$ contains a copy of $\mathbb{F}_p$, and is thus of characteristic p.

Example 3.1.3. $\mathbb{F}_4$ and $\mathbb{F}_8$ both contain a copy of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, but $\mathbb{F}_8$ does not have any subfield isomorphic to $\mathbb{F}_4$. The smallest finite field containing both a copy of $\mathbb{F}_4$ and $\mathbb{F}_8$ is $\mathbb{F}_{64}$.

Theorem 3.1.4. *The multiplicative group of every finite field is cyclic, i.e. $\mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.*

3.2 Reminders on ideals

Throughout this section, we let $\mathcal{R}$ be a commutative ring. When $\alpha_1, \cdots, \alpha_m$ are elements of a $\mathcal{R}$, we will denote by

$$(\alpha_1, \cdots, \alpha_m) = \left\{ \sum_{j=1}^{m} r_j \alpha_j \;\middle|\; r_1, \cdots, r_m \in \mathcal{R} \right\}$$

the ideal of $\mathcal{R}$ generated by these elements. We will say that an ideal of $\mathcal{R}$ is nonzero if it is not reduced to $\{0\}$, and that it is nontrivial if it is not the whole of $\mathcal{R}$.

Definition 3.2.1. Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_m$ be ideals of $\mathcal{R}$. Their sum and product are defined to be

$$\sum_{j=1}^{m} \mathfrak{a}_j = \mathfrak{a}_1 + \cdots + \mathfrak{a}_m = \{a_1 + \cdots + a_m \mid a_1 \in \mathfrak{a}_1,\ \cdots,\ a_m \in \mathfrak{a}_m\}$$

and

$$\prod_{j=1}^{m} \mathfrak{a}_j = a_1 \cdots \mathfrak{a}_m = \left\{ \sum_{j=1}^{n} a_{1,j} \cdots a_{m,j} \;\middle|\; n \in \mathbb{N},\ \text{and } \forall j,\ a_{1,j} \in \mathfrak{a}_1,\ \cdots,\ a_{m,j} \in \mathfrak{a}_m \right\}.$$

Both are ideals of $\mathcal{R}$.

Example 3.2.2. We have

$$(\alpha_1, \cdots, \alpha_m) = \alpha_1 \mathcal{R} + \cdots + \alpha_m \mathcal{R} = (\alpha_1) + \cdots + (\alpha_m),$$

and

$$(\alpha_1 \cdots \alpha_m) = (\alpha_1) \cdots (\alpha_m);$$

More generally,

$$(\alpha_1 \cdots \alpha_m)(\beta_1 \cdots \beta_n) = (\alpha_1 \beta_1, \cdots, \alpha_i \beta_j, \cdots, \alpha_m \beta_n).$$

Remark 3.2.3. An intersection of ideals $\bigcap_{j=1}^{m} \mathfrak{a}_j$ is also always an ideal; however the union $\bigcup_{j=1}^{m} \mathfrak{a}_j$ is usually not an ideal of $\mathcal{R}$. In fact, $\sum_{j=1}^{m} \mathfrak{a}_j$ is the ideal generated by $\bigcup_{j=1}^{m} \mathfrak{a}_j$, and we have

$$\prod_{j=1}^{m} \mathfrak{a}_j \subseteq \bigcap_{j=1}^{m} \mathfrak{a}_m \subseteq \mathfrak{a}_i \subseteq \sum_{j=1}^{m} \mathfrak{a}_j \qquad (\star)$$

for all $1 \leqslant i \leqslant m$, where each of these inclusions can be strict.

For instance, if we take $\mathcal{R} = \mathbb{Z}$, $\mathfrak{a}_1 = \mathfrak{a}_2 = 2\mathbb{Z}$, and $\mathfrak{a}_3 = 3\mathbb{Z}$, then ($\star$) becomes

$$12\mathbb{Z} \subsetneq 6\mathbb{Z} \subsetneq (2 \text{ or } 3)\mathbb{Z} \subsetneq \mathbb{Z}.$$

Definition 3.2.4. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of $\mathcal{R}$. We say that $\mathfrak{a}$ and $\mathfrak{b}$ are *coprime* if $\mathfrak{a} + \mathfrak{b} = \mathcal{R}$, that is to say if we can write $1 = \alpha + \beta$ for some $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$.

Theorem 3.2.5 (Chinese remainders)**.** *Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_m$ be ideals of $\mathcal{R}$ which are pairwise coprime, and let $\mathfrak{b} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Then the canonical projections induce a ring isomorphism*

$$\mathcal{R}/\mathfrak{b} \simeq \prod_{i=1}^{m} \mathcal{R}/\mathfrak{a}_i.$$

Definition 3.2.6. Let $\mathfrak{a} \subset \mathcal{R}$ be a nontrivial ideal of $\mathcal{R}$.

1. One says that $\mathfrak{a}$ is a *prime* ideal (or just a prime, for short) of $\mathcal{R}$ if for all $r, s \in \mathcal{R}$, $rs \in \mathcal{R}$ implies $r \in \mathcal{R}$ or $s \in \mathcal{R}$.

2. One says that $\mathfrak{a}$ is a *maximal* ideal of $\mathcal{R}$ if whenever $\mathfrak{b}$ is an ideal such that $\mathfrak{a} \subset \mathfrak{b} \subset \mathcal{R}$, then $\mathfrak{b} = \mathfrak{a}$ or $\mathfrak{b} = \mathcal{R}$.

Theorem 3.2.7. *Let $\mathfrak{a} \subset \mathcal{R}$ be a nontrivial ideal of $\mathcal{R}$.*

1. $\mathfrak{a}$ is prime if and only if the quotient ring $\mathcal{R}/\mathfrak{a}$ is a domain.

2. $\mathfrak{a}$ is maximal if and only if the quotient ring $\mathcal{R}/\mathfrak{a}$ is a field.

Proof. Whenever $x \in \mathcal{R}$, let $\overline{x}$ denote the class of x in $\mathcal{R}/\mathfrak{a}$.

1. $\mathfrak{a}$ is prime if and only if $rs \in \mathfrak{a} \Rightarrow r \in \mathfrak{a}$ or $s \in \mathfrak{a}$, if and only if $\overline{rs} = \overline{0} \Rightarrow \overline{r} = \overline{0}$ or $\overline{s} = \overline{0}$, if and only if $R/\mathfrak{a}$ is a domain.

2. Suppose $\mathfrak{a}$ is maximal, and let $\overline{r} \in \mathcal{R}/\mathfrak{a}$ be nonzero. Then $r \notin \mathfrak{a}$, so the ideal $(r) + \mathfrak{a}$ must be the whole of $\mathcal{R}$. In particular this ideal contains 1, so that there exist $s \in \mathcal{R}$ and $a \in \mathfrak{a}$ such that $1 = rs + a$. But then we have $\overline{rs} = \overline{1}$, which proves that $\mathcal{R}/\mathfrak{a}$ is a field.

   Conversely, suppose that $\mathcal{R}/\mathfrak{a}$ is a field, and let $\mathfrak{b}$ be an ideal such that $\mathfrak{a} \subsetneq \mathfrak{b}$, and let us prove that $\mathfrak{b} = \mathcal{R}$. There exists $r \in \mathfrak{b}$, $r \notin \mathfrak{a}$. We then have $\overline{r} \neq \overline{0}$, so there exists $s \in \mathcal{R}$ such that $\overline{rs} = 1$ since $\mathcal{R}/\mathfrak{a}$ is a field. This means that $rs = 1 + a$ for some $a \in \mathfrak{a}$, so $1 = rs - a \in \mathfrak{b}$, which proves that $\mathfrak{b} = \mathcal{R}$. □

Corollary 3.2.8. *Every maximal ideal is prime.*

Example 3.2.9. Let $\mathcal{R} = \mathbb{Z}[x]$, and let $p \in \mathbb{Z}$ be a prime number. Then the ideals (p) and (x) are prime but are not maximal, because the respective quotients, $\mathbb{F}_p[x]$ and $\mathbb{Z}$, are domains but are not fields. On the contrary, the ideal (p, x) is maximal, because the corresponding quotient is $\mathbb{F}_p$, which is a field.

3.3 Integral closure

Definition 3.3.1. Let $\mathcal{R} \subset \mathcal{S}$ be domains, and let $s \in \mathcal{S}$. One says that s is *integral* over $\mathcal{R}$ if there exists a nonzero *monic* polynomial $P \in \mathcal{R}[x]$ such that $P(s) = 0$.

If every $s \in \mathcal{S}$ is integral over $\mathcal{R}$, one says that $\mathcal{S}$ is an *integral extension* of $\mathcal{R}$.

On the contrary, if the only elements of $\mathcal{S}$ which are integral over $\mathcal{R}$ lie in fact in $\mathcal{R}$, one says that $\mathcal{R}$ is *integrally closed* in $\mathcal{S}$.

In particular, one says for short that $\mathcal{R}$ is *integrally closed* if it is integrally closed in its fraction field $\operatorname{Frac}\mathcal{R}$.

Thus, for example, the set of the elements of a number field K which are integral over $\mathbb{Z}$ is precisely $\mathbb{Z}_K$. Also, $\mathbb{Z}$ is integrally closed.

Example 3.3.2. The ring $\mathcal{R} = \mathbb{Z}[\sqrt{5}]$ is not integrally closed. Indeed, $\alpha = \frac{1+\sqrt{5}}{2}$ lies in $\operatorname{Frac}\mathcal{R}$, and satisfies $\alpha^2 - \alpha - 1 = 0$ so α is integral over $\mathcal{R}$ (and even over $\mathbb{Z}$), yet $\alpha \notin \mathcal{R}$.

Theorem 3.3.3. *Let K be a number field, and let $\mathbb{Z}_K$ be its ring of integers. Then $\mathbb{Z}_K$ is integrally closed.*

Proof. Let $\alpha \in K$ be such that there exists a nonzero monic polynomial $P(x) \in \mathbb{Z}_K[x]$ such that $P(\alpha) = 0$; we want to show that $\alpha \in \mathbb{Z}_K$.

Write $K = \mathbb{Q}(\beta)$ for some primitive element $\beta \in K$, and let $B(x) \in \mathbb{Q}[x]$ be the minimal polynomial fo β over $\mathbb{Q}$.

The coefficients of $P(x)$ lie in $\mathbb{Z}_K$ and in particular in K, so they can be expressed as polynomials in β with coefficients in $\mathbb{Q}$. Therefore there exists a polynomial $P_2(y, x) \in \mathbb{Q}[y, x]$ such that $P_2(\beta, x) = P(x)$. For each embedding σ of K into $\mathbb{C}$, let $P^\sigma(x) \in \mathbb{C}[x]$ be the polynomial obtained by applying σ to the coefficients of $P(x)$, so that $P^\sigma(x) = P_2(\sigma(\beta), x)$, and consider

$$Q(x) = \prod_{\sigma\colon K \hookrightarrow \mathbb{C}} P^\sigma(x).$$

On the one hand, since the $\sigma(\beta)$ are the roots of $B(y)$, we have

$$Q(x) = \prod_{\sigma\colon K \hookrightarrow \mathbb{C}} P_2(\sigma(\beta), x) = \operatorname{Res}_y\big(B(y), P_2(y, x)\big),$$

which shows that $Q(x) \in \mathbb{Q}[x]$. On the other hand, the coefficients of $P(x)$ are algebraic integers, so the coefficients of $P^\sigma(x)$ also are for all σ, therefore the coefficients of $Q(x)$, which are sums of products of these coefficients, are algebraic integers by theorem 2.1.8. As a result, $Q(x) \in \mathbb{Z}[x]$ by proposition 2.1.11; besides, $Q(x)$ is clearly monic. To conclude, notice that

$$Q(\alpha) = \operatorname{Res}_y\big(B(y), P_2(y, \alpha)\big) = 0$$

since $B(y)$ and $P_2(y, \alpha)$ have a common root, namely $y = \beta$. This shows that α is an algebraic integer. □

Corollary 3.3.4. *Let $\mathcal{O}$ be an order in a number field K. Then $\mathcal{O}$ is integrally closed if and only if $\mathcal{O} = \mathbb{Z}_K$.*

Remark 3.3.5. This proof is not the standard one. The usual way of proving this theorem consists in proving that when we have domains $\mathcal{R} \subset \mathcal{S} \subset \mathcal{T}$ such that $\mathcal{S}$ is integral over $\mathcal{R}$ and $\mathcal{T}$ is integral over $\mathcal{S}$, then $\mathcal{T}$ is integral over $\mathcal{R}$; unfortunately, the proof of this fact requires using the notion of module over a ring, which is beyond the scope of this course. For those of you who do know this theory, here is the (of course non examinable) proof:

First, if $\mathcal{R} \subset \mathcal{S}$ are two commutative rings, given finitely many elements $s_1, \cdots, s_n \in \mathcal{S}$ we have the equivalence

$s_1, \cdots, s_n$ integral over $\mathcal{R} \Longleftrightarrow \mathcal{R}[s_1, \cdots, s_n]$ is a finitely generated $\mathcal{R}$-module.

Indeed, $\Rightarrow$ is immediate from the definition of integrality, and $\Leftarrow$ follows from Cayley-Hamilton (cf. the proof of proposition 2.2.9). As a result, if we suppose that $\mathcal{R} \subset \mathcal{S} \subset \mathcal{T}$ are such that $\mathcal{S}$ is integral over $\mathcal{R}$ and $\mathcal{T}$ is integral over $\mathcal{S}$, then for all $t \in \mathcal{T}$, we have a relation $t^n + \sum_{i=0}^{n-1} s_i t^i = 0$ for some $s_i \in \mathcal{S}$; if we let $M = \mathcal{R}[s_0, \cdots, s_{n-1}]$, then M is a finitely generated $\mathcal{R}$-module, and $M[t]$ is a finitely generated M-module, so that $M[t] = \mathcal{R}[s_0, \cdots, s_{n-1}, t]$ is a finitely generated $\mathcal{R}$-module, which proves that t is integral over $\mathcal{R}$.

3.4 Dedekind domains

Proposition 3.4.1. *Let K be a number field, and let $\mathfrak{a}$ be a nonzero ideal of $\mathbb{Z}_K$. Then $\mathfrak{a}$ is a lattice in K; in particular, the index $[\mathbb{Z}_K : \mathfrak{a}]$ is finite.*

Proof. Let $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, so that $\alpha\mathbb{Z}_K \subset \mathfrak{a} \subset \mathbb{Z}_K$. We know that $\mathbb{Z}_K$ is a lattice in K; let $\omega_1, \cdots, \omega_n$ be a $\mathbb{Z}$-basis of it, where $n = [K : \mathbb{Q}]$. Then $\alpha\omega_1, \cdots, \alpha\omega_n$ is a $\mathbb{Z}$-basis of $\alpha\mathbb{Z}_K$, which is thus also a lattice in K. Since $\mathfrak{a}$ is an additive subgroup of K which is cornered between the two lattices $\alpha\mathbb{Z}_K$ and $\mathbb{Z}_K$, it is itself a lattice. □

This prompts the following definition.

Definition 3.4.2. Let $\mathfrak{a}$ be a nonzero ideal of $\mathbb{Z}_K$. The *norm* of $\mathfrak{a}$ is the index $[\mathbb{Z}_K : \mathfrak{a}]$. It is denoted by $N(\mathfrak{a}) \in \mathbb{N}$. By convention the norm of the zero ideal is 0.

Proposition 3.4.3. *Let $\mathfrak{a} \subset \mathbb{Z}_K$ be an ideal. Then $N(\mathfrak{a}) \in \mathfrak{a}$.*

Proof. By definition, $N(\mathfrak{a})$ is the order of the finite additive group $\mathcal{O}/\mathfrak{a}$, so the image of the integer $N(\mathfrak{a})$ in $\mathbb{Z}_K/\mathfrak{a}$ is 0 by Lagrange's theorem. □

Theorem 3.4.4. *Let $\alpha \in \mathbb{Z}_K$, and let $\mathfrak{a}$ be the ideal $\alpha\mathbb{Z}_K$ of $\mathbb{Z}_K$. Then*

$$N(\mathfrak{a}) = |N^K_{\mathbb{Q}}(\alpha)|.$$

Proof. Let $(\omega_j)_{1 \leqslant j \leqslant [K:\mathbb{Q}]}$ be a $\mathbb{Z}$-basis of $\mathbb{Z}_K$. Then $(\alpha\omega_j)_{1 \leqslant j \leqslant [K:\mathbb{Q}]}$ is a $\mathbb{Z}$-basis of $\mathfrak{a}$, and the change-of-basis matrix between these two bases is the matrix of the multiplication-by-α map with respect to the basis $(\omega_j)_{1 \leqslant j \leqslant [K:\mathbb{Q}]}$. The index $[\mathbb{Z}_K : \mathfrak{a}]$ is the absolute value of the determinant of this matrix, but by definition this determinant is $N^K_{\mathbb{Q}}(\alpha)$. □

Lemma 3.4.5. *Let $\mathfrak{a} \subset \mathfrak{b} \subset \mathbb{Z}_K$ be two ideals. Then $N(\mathfrak{b})$ divides $N(\mathfrak{a})$, with equality if and only if $\mathfrak{a} = \mathfrak{b}$.*

Proof. Since $\mathfrak{a} \subset \mathfrak{b} \subset \mathbb{Z}_K$ we have $[\mathbb{Z}_K : \mathfrak{a}] = [\mathbb{Z}_K : \mathfrak{b}][\mathfrak{b} : \mathfrak{a}]$, that is $N(\mathfrak{a}) = N(\mathfrak{b})[\mathfrak{b} : \mathfrak{a}]$. This proves the divisibility, and there is equality if and only if $[\mathfrak{b} : \mathfrak{a}] = 1$, if and only if $\mathfrak{a} = \mathfrak{b}$. □

Corollary 3.4.6. *Let $\mathfrak{a} \subset \mathbb{Z}_K$ an ideal, and let $\alpha \in \mathfrak{a}$, $\alpha \neq 0$. Then $N(\mathfrak{a})$ divides $|N^K_{\mathbb{Q}}(\alpha)|$, with equality if and only if $\mathfrak{a} = \alpha\mathcal{O}$.*

Proof. This follows immediately from Theorem 3.4.4 and Lemma 3.4.5. $\square$

Definition 3.4.7. Let $\mathcal{R}$ be a ring. We say that $\mathcal{R}$ is Noetherian if there exist no infinite strictly increasing sequence $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots$ of ideals of $\mathcal{R}$.

Remark 3.4.8. One can show that $\mathcal{R}$ is Noetherian iff. every ideal $\mathfrak{a}$ of $\mathcal{R}$ is *finitely generated*, that is to say that there exist finitely many elements $\alpha_1, \cdots, \alpha_m$ of $\mathcal{R}$ such that $\mathfrak{a} = (\alpha_1, \cdots, \alpha_m)$.

Proposition 3.4.9. *The ring of integers $\mathbb{Z}_K$ is a Noetherian ring.*

Proof. Consider a sequence of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$. The norms of these ideals form a nondecreasing sequence of positive integers, hence stabilises, so by Lemma 3.4.5 the sequence of ideals must stabilise. $\square$

Lemma 3.4.10. *Every finite domain is a field.*

Proof. Let $\mathcal{R}$ be a finite domain, let $r \in \mathcal{R}$ be nonzero, and consider the multiplication-by-r map

$$\begin{array}{rccc} \mu_r \colon & \mathcal{R} & \longrightarrow & \mathcal{R} \\ & x & \longmapsto & rx \end{array}.$$

Since $\mathcal{R}$ is a domain, μ_r is injective. In addition $\mathcal{R}$ is finite, so μ_r is a bijection. In particular, the element 1 has a preimage, which proves that r is invertible. $\square$

Proposition 3.4.11. *Every nonzero prime ideal of $\mathbb{Z}_K$ is maximal.*

Proof. Let $\mathfrak{p} \subset \mathcal{O}$ be a nonzero prime ideal. Then $\mathcal{R} = \mathcal{O}/\mathfrak{p}$ is a domain, and by Proposition 3.4.1 the ring $\mathcal{R}$ is finite. Lemma 3.4.10 proves that $\mathcal{R}$ is a field and therefore $\mathfrak{p}$ is a maximal ideal. $\square$

Definition 3.4.12. An domain $\mathcal{R}$ is called a *Dedekind domain* if it is Noetherian, integrally closed, and if every nonzero prime ideal of $\mathcal{R}$ is maximal.

Theorem 3.4.13. *The ring of integers of a number field is a Dedekind domain.*

Proof. This is the conjunction of Proposition 3.4.9, Theorem 3.3.3 and Proposition 3.4.11. $\square$

Remark 3.4.14. Apart from this theorem, all the statements in this section remain true if we replace $\mathbb{Z}_K$ with $\mathcal{O}$ and $\mathfrak{a}$ with an ideal of $\mathcal{O}$. In particular, every order is Noetherian, and has the property that all its nonzero prime ideals are maximal. What makes orders different from $\mathbb{Z}_K$ is that they are not integrally closed; in particular, they are *not* Dedekind domains.

3.5 Factorisation theory in Dedekind domains

The reason why we introduced the notion of Dedekind domain is the following major result.

Theorem 3.5.1. *Let $\mathcal{R}$ be a Dedekind domain. Every ideal $\mathfrak{a}$ of $\mathcal{R}$ is a product of prime ideals,*

$$\mathfrak{a} = \prod_{j=1}^{m} \mathfrak{p}_j.$$

Furthermore, this factorisation is unique[1].

Thanks to this theorem, we can perform arithmetic in a Dedekind domain, but on ideals, not on numbers. The usual notions of divisibility, gcd, lcm... can be translated in terms of operations on ideals:

Theorem 3.5.2. *Let $\mathcal{R}$ be a Dedekind domain.*

1. *Let $\mathfrak{a}$, $\mathfrak{b}$ be two ideals of $\mathcal{R}$. Then $\mathfrak{a}$ divides $\mathfrak{b}$ (meaning there exists an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$) if and only if $\mathfrak{a} \supset \mathfrak{b}$.*

2. *If $\mathfrak{a}_1, \cdots, \mathfrak{a}_m$ are ideals of $\mathcal{R}$, then*

$$\gcd(\mathfrak{a}_1, \cdots, \mathfrak{a}_m) = \mathfrak{a}_1 + \cdots + \mathfrak{a}_m$$

and

$$\operatorname{lcm}(\mathfrak{a}_1, \cdots, \mathfrak{a}_m) = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_m.$$

Example 3.5.3. For $\mathcal{R} = \mathbb{Z}$, this translates into the following more familiar statements:

$$a \mid b \Longleftrightarrow a\mathbb{Z} \supset b\mathbb{Z},$$

$$\gcd(a_1, \cdots, a_m)\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_m\mathbb{Z},$$

and

$$\operatorname{lcm}(a_1, \cdots, a_m)\mathbb{Z} = a_1\mathbb{Z} \cap \cdots \cap a_m\mathbb{Z}.$$

Example 3.5.4. Let $\mathfrak{p}$, $\mathfrak{p}'$ be two prime ideals. If $\mathfrak{p}$ and $\mathfrak{p}'$ are distinct, then they are coprime, which means that $\mathfrak{p} + \mathfrak{p}' = \mathbb{Z}_K$ and that $\mathfrak{p} \cap \mathfrak{p}' = \mathfrak{p}\mathfrak{p}'$. On the other hand, if $\mathfrak{p} = \mathfrak{p}'$, then we have $\mathfrak{p} + \mathfrak{p} = \mathfrak{p}$ and $\mathfrak{p} \cap \mathfrak{p} = \mathfrak{p}$. Note that $\mathfrak{p}^2$ is an ideal contained in $\mathfrak{p}$; in fact, this containment is strict by the uniqueness of the factorisation of ideals.

[1] Up to the order of the terms, of course.

Example 3.5.5. Let $x \in \mathcal{R}$, and let $\mathfrak{a}$ be an ideal of $\mathcal{R}$. Then

$$x \in \mathfrak{a} \Longleftrightarrow (x) \subseteq \mathfrak{a} \Longleftrightarrow \mathfrak{a} \mid (x).$$

This fact is frequently used in practice.

Remark 3.5.6. In fact, it can be shown that the factorisation property presented in theorem 3.5.1 characterises Dedekind domains. Briefly,

- because containment means divisibility, the fact that ideals factor into primes implies that the domain is Noetherian,
- if a domain is not integrally closed, then using elements of the field of fractions which are integral but not in the domain, one can exhibit ideals which do not factor properly,
- in view of the equivalence between containment and divisibility, the fact that nonzero prime ideals play the role of irreducibles means that they are maximal.

As a first application of this, we can prove that although Dedekind domains are not in general principal, every ideal can be generated by at most two elements. In fact, even more is true:

Proposition 3.5.7. *Let $\mathfrak{a}$ be an ideal in a Dedekind domain $\mathcal{R}$, and let $\alpha \in \mathfrak{a}$, $\alpha \neq 0$. Then there exists $\beta \in \mathfrak{a}$ such that $\mathfrak{a} = (\alpha, \beta)$.*

Proof. Since $\alpha \in \mathfrak{a}$, we have $\alpha\mathcal{R} \subset \mathfrak{a}$, so in the factorisations

$$\alpha\mathcal{R} = \prod_{j=1}^{m} \mathfrak{p}_j^{a_j}, \quad \mathfrak{a} = \prod_{j=1}^{m} \mathfrak{p}_j^{e_j},$$

we have $e_j \leqslant a_j$ for all j. By uniqueness of the factorisation, for each j there exists $\beta_j \in \mathfrak{p}_j^{e_j} \setminus \mathfrak{p}_j^{e_j+1}$, and by Chinese remainders we may find $\beta \in \mathcal{R}$ such that for all j, $\beta \equiv \beta_j \bmod \mathfrak{p}_j^{e_j+1}$. In particular, for all j we have $\beta \in \mathfrak{p}_j^{e_j} \setminus \mathfrak{p}_j^{e_j+1}$, so we have the factorisation

$$\beta\mathcal{R} = \mathfrak{b} \prod_{j=1}^{m} \mathfrak{p}_j^{e_j},$$

where $\mathfrak{b}$ is coprime to the $\mathfrak{p}_j$. As a result, we have

$$(\alpha, \beta) = \alpha\mathcal{R} + \beta\mathcal{R} = \gcd(\alpha\mathcal{R}, \beta\mathcal{R}) = \prod_{j=1}^{m} \mathfrak{p}_j^{e_j} = \mathfrak{a},$$

as wanted. □

We now take $\mathcal{R} = \mathbb{Z}_K$ to be the ring of integers of some number field K.

Theorem 3.5.8 (Multiplicativity of the norm)**.** *Let $\mathfrak{a}, \mathfrak{b} \subset \mathbb{Z}_K$ be ideals of the ring of integers of a number field K. Then $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.*

Proof. It is enough to prove that

$$N\left(\prod_{j=1}^{m} \mathfrak{p}_j^{e_j}\right) = \prod_{j=1}^{m} N(\mathfrak{p}_j)^{e_j}$$

whenever the $\mathfrak{p}_j$ are pairwise distinct nonzero primes and the e_j are positive integers.

By uniqueness of factorisation we have $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = \mathbb{Z}_K$, i.e. the $\mathfrak{p}_j$ are pairwise coprime. The Chinese remainder theorem 3.2.5 then tells us that

$$N\left(\prod_{j=1}^{m} \mathfrak{p}_j^{e_j}\right) = \prod_{j=1}^{m} N(\mathfrak{p}_j^{e_j}),$$

so to conclude we must show that $N(\mathfrak{p}_j^{e_j}) = N(\mathfrak{p}_j)^{e_j}$.

Let $\mathfrak{p} \subset \mathbb{Z}_K$ be a nonzero prime. By uniqueness of the factorisation of ideals, there exists $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. The factorisation of the ideal $\pi\mathbb{Z}_K$ must then be $\pi\mathbb{Z}_K = \mathfrak{p}\mathfrak{a}$, where the ideal $\mathfrak{a}$ is coprime to $\mathfrak{p}$ (else π would lie in $\mathfrak{p}^2$), i.e. $\mathfrak{a} + \mathfrak{p} = \mathbb{Z}_K$. Fix $n \in \mathbb{N}$, and consider the homomorphism of additive groups

$$\begin{array}{rcl} \mu : \mathbb{Z}_K/\mathfrak{p} & \xrightarrow{\sim} & \mathfrak{p}^n/\mathfrak{p}^{n+1} \\ x & \longmapsto & \pi^n x. \end{array}$$

It is well-defined, since if $x \in \mathfrak{p}$, then $\pi^n x$ is a product of $n+1$ elements of $\mathfrak{p}$ and hence lies in $\mathfrak{p}^{n+1}$. Suppose $x \in \mathbb{Z}_K$ represents and element of $\operatorname{Ker} \mu$, then $\pi^n x \in \mathfrak{p}^{n+1}$, so $\mathfrak{p}^{n+1} \mid (\pi^n x) = (\pi)^n x = \mathfrak{p}^n \mathfrak{a}^n (x)$; as $\mathfrak{a}$ and $\mathfrak{p}$ are coprime, this means that $\mathfrak{p}^{n+1} \mid \mathfrak{p}^n(x)$ by unicity of the factorisation, whence $\mathfrak{p} \mid (x)$ so $x \in \mathfrak{p}$; therefore $\operatorname{Ker} \mu = 0$ and μ is injective. Finally, the image of μ is

$$(\pi^n \mathbb{Z}_K + \mathfrak{p}^{n+1})/\mathfrak{p}^{n+1} = (\mathfrak{p}^n \mathfrak{a}^n + \mathfrak{p}^{n+1})/\mathfrak{p}^{n+1} = \big(\mathfrak{p}^n(\mathfrak{a}^n + \mathfrak{p})\big)/\mathfrak{p}^{n+1} = \mathfrak{p}^n/\mathfrak{p}^{n+1}$$

since $\mathfrak{a}^n + \mathfrak{p} = \mathbb{Z}_K$ as $\mathfrak{p}$ and $\mathfrak{a}$ are coprime, so μ is surjective. Thus μ is an isomorphism, so that

$$[\mathfrak{p}^n : \mathfrak{p}^{n+1}] = \#(\mathfrak{p}^n/\mathfrak{p}^{n+1}) = \#\mathbb{Z}_K/\mathfrak{p} = N(\mathfrak{p})$$

for all $n \in \mathbb{N}$. As a result, for all $e \in \mathbb{N}$, in view of the chain $\mathbb{Z}_K \supsetneq \mathfrak{p} \supsetneq \cdots \supsetneq \mathfrak{p}^e$ we have

$$N(\mathfrak{p}^e) = [\mathbb{Z}_K : \mathfrak{p}^e] = [\mathbb{Z}_K : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{e-1} : \mathfrak{p}^e] = N(\mathfrak{p})^e,$$

and the proof is complete. □

Remark 3.5.9 (Failure of multiplicativity for a non-maximal order)**.**
This proof relies heavily on unique factorisation, which comes from the fact that $\mathbb{Z}_K$ is a Dedekind domain. It is therefore not surprising that if we replace $\mathbb{Z}_K$ with an order, then the conclusion does not hold anymore!

For instance, take $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{-3}$, let $\mathcal{O} = \mathbb{Z}[\alpha] \subsetneq \mathbb{Z}_K = \mathbb{Z}[\frac{1+\alpha}{2}]$, and let $\mathfrak{a} = \mathbb{Z}2 \oplus \mathbb{Z}(\alpha+1) \subset \mathcal{O}$. We have $\alpha 2 = (-1)2 + 1(\alpha+1)$ and $\alpha(\alpha+1) = (-2)2 + 1(\alpha+1)$, so $\alpha\mathfrak{a} \subset \mathfrak{a}$ and $\mathfrak{a}$ is thus an ideal of $\mathcal{O}$, of "norm" $[\mathcal{O} : \mathfrak{a}] = \left|\det\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\right| = 2$. However, $\mathfrak{a}^2$ is generated by $\{2^2, 2(\alpha+1), (\alpha+1)^2\}$ over $\mathbb{Z}$, and since $(\alpha+1)^2 = -2(\alpha+1)$, the set $\{2^2, 2(\alpha+1)\}$ is a $\mathbb{Z}$-basis of $\mathfrak{a}^2$, whence $[\mathcal{O} : \mathfrak{a}^2] = \left|\det\begin{pmatrix} 4 & 2 \\ 0 & 2 \end{pmatrix}\right| = 8 \neq 2^2$.

This illustrates the fact that definition 2.1.1 is the "right" one.

3.6 Decomposition of primes

Since the primes (meaning the prime ideals) of $\mathbb{Z}_K$ are the building blocks of all the nonzero ideals, they deserve particular attention.

Lemma 3.6.1. *Let $\mathfrak{a} \subset \mathbb{Z}_K$ be a nonzero ideal. Then $\mathfrak{a} \cap \mathbb{Z}$ is of the form $a\mathbb{Z}$ for some nonzero $a \in \mathbb{N}$. Besides, if $\mathfrak{a}$ is a prime ideal, then a is a prime number.*

Proof. Let $f\colon \mathbb{Z} \to \mathbb{Z}_K/\mathfrak{a}$ be the canonical ring homomorphism. Then $\mathfrak{a} \cap \mathbb{Z} = \ker f$, so it is an ideal of $\mathbb{Z}$. Since $\mathbb{Z}$ is a PID, this ideal is of the form $a\mathbb{Z}$ with $a \in \mathbb{Z}$.

Now f induces an injective ring homomorphism $\bar{f}\colon \mathbb{Z}/a\mathbb{Z} \hookrightarrow \mathbb{Z}_K/\mathfrak{a}$. Since the ring $\mathbb{Z}_K/\mathfrak{a}$ is finite by Proposition 3.4.1, the ring $\mathbb{Z}/a\mathbb{Z}$ is also finite, so $a \neq 0$, and since we can replace a with $-a$, we may assume $a > 0$.

If $\mathfrak{a}$ is prime, then $\mathbb{Z}_K/\mathfrak{a}$ is a domain, so the subring $\mathbb{Z}/a\mathbb{Z}$ is also a domain and therefore a is a prime number. □

Remark 3.6.2. Another way to see this is that a is the characteristic of the finite ring $\mathbb{Z}_K/\mathfrak{a}$, and is therefore nonzero; moreover this characteristic must be a prime number if $\mathbb{Z}_K/\mathfrak{a}$ is a domain.

Definition 3.6.3. Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_K$, and let $p \in \mathbb{N}$ be the prime number such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. One says that p is the prime number *below* $\mathfrak{p}$, and that $\mathfrak{p}$ is a prime ideal *above* p.

By Lemma 3.4.10, for all nonzero prime $\mathfrak{p}$, the quotient $\mathbb{Z}_K/\mathfrak{p}$ is a finite field, called the *residue field* of $\mathfrak{p}$. The characteristic of this field is by definition the prime number p below $\mathfrak{p}$, so this field is isomorphic to $\mathbb{F}_q$, where $q = p^f$ for some $f \in \mathbb{N}$ called the *residue degree* of $\mathfrak{p}$ (some people say *inertial degree*).

Remark 3.6.4. The prime number below a prime ideal $\mathfrak{p}$ is the unique p such that $N(\mathfrak{p})$ is a power of p.

By definition, an integer is a prime if it does not factor in $\mathbb{Z}$. However, it may very well factor in the larger ring $\mathbb{Z}_K$. The following results tells us what kind of decompositions occur.

Theorem 3.6.5. *Let $p \in \mathbb{N}$ be prime, and let K be a number field. Then we have the factorisation*

$$p\mathbb{Z}_K = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j},$$

where the $\mathfrak{p}_j$ are exactly the primes of $\mathbb{Z}_K$ above p and $e_j \geqslant 1$ for all j. Besides, if we let f_j be the residue degree of $\mathfrak{p}_j$, we have the identity

$$\sum_{j=1}^{g} e_j f_j = [K : \mathbb{Q}].$$

Proof. Let $\mathfrak{p}$ be an ideal above p. Then by definition $\mathfrak{p} \supset p\mathbb{Z}_K$, so $\mathfrak{p}$ divides $p\mathbb{Z}_K$. This proves that the integers e_j are all nonzero.

Next, by definition, we have $N(\mathfrak{p}_j) = p^{f_j}$, so

$$N\left(\prod_{j=1}^{g} \mathfrak{p}_j^{e_j}\right) = \prod_{j=1}^{g} N(\mathfrak{p}_j)^{e_j} = \prod_{j=1}^{g} p^{e_j f_j}$$

by theorem 3.5.8. On the other hand, we also have

$$N(p\mathbb{Z}_K) = |N_{\mathbb{Q}}^{K}(p)| = |p^{[K:\mathbb{Q}]}|$$

by theorem 3.4.4, so the identity follows. □

Definition 3.6.6. The *ramification index* of a prime $\mathfrak{p}$ is the exponent $e \geqslant 1$ of $\mathfrak{p}$ in the decomposition of $p\mathbb{Z}_K$, where p is the prime below $\mathfrak{p}$. If $e \geqslant 2$, we say that $\mathfrak{p}$ is *ramified*; otherwise we say that $\mathfrak{p}$ is *unramified.* Let $n = [K : \mathbb{Q}]$.

- If there exists at least one ramified prime $\mathfrak{p}$ above p, we say that p *ramifies* in K.

- If $p\mathbb{Z}_K = \mathfrak{p}^n$ (so that the ramification index of $\mathfrak{p}$ is $e = n$ and its residue degree is $f = 1$), then we say that p is *totally ramified* in K.

- When $p\mathbb{Z}_K$ is a prime ideal, so that the above decomposition is simply $p\mathbb{Z}_K = \mathfrak{p}$, then we say that p is *inert* in K.

- If p is neither inert nor ramified, we say that p *splits* in K (or that K splits at p).

- If we have a decomposition $p\mathbb{Z}_K = \prod_{j=1}^{n} \mathfrak{p}_j$ with the $\mathfrak{p}_j$ all distinct (so that their residue degrees are all 1), we say that p *splits completely* in K.

3.7 Ramification

Ramification is an important type of behaviour that can occur when decomposing rational primes in a number field. The following theorem is extremely important, but we will not prove it.

Theorem 3.7.1. *The primes $p \in \mathbb{Z}$ which ramify in K are exactly the ones which divide the discriminant of K. In particular, there are only finitely many of them.*

Remark 3.7.2. One can be more specific. Indeed, one can show that if the decomposition of a prime $p \in \mathbb{N}$ in K is

$$p\mathbb{Z}_K = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j},$$

then the exponent of p in $\operatorname{disc} K$ is $\sum_{j=1}^{g}(e'_j - 1)f_j$, where f_j is the residue degree of $\mathfrak{p}_j$, and $e'_j = e_j$ if $p \nmid e_j$ (tame ramification case) but $e'_j > e_j$ if $p \mid e_j$ (wild ramification case). In other words, the more ramified p is, the more it divides $\operatorname{disc} K$.

We should mention the following result of Minkowski's.

Theorem 3.7.3. *If $K \not\simeq \mathbb{Q}$ is a number field, then $|\operatorname{disc} K| > 1$, so there is at least one ramified prime $p \in \mathbb{N}$.*

This can be rephrased by saying that there is no nontrival everywhere-unramified number field. We postpone the proof of this result to the next chapter.

The case when p is totally ramified is a very special one, which allows us in particular to take a nice shortcut when computing the ring of integers of K.

Definition 3.7.4. Let $P(x) = x^n + \sum_{j=0}^{n-1} \lambda_j x^j \in \mathbb{Z}[x]$ be a monic polynomial, and let $p \in \mathbb{N}$ be a prime. We say that $P(x)$ is *Eisenstein* at p if p divides all the λ_j, but $p^2 \nmid \lambda_0$.

Example 3.7.5. $P(x) = x^2 - 84x + 90$ is Eisenstein at 2, but not at 5 because $5 \nmid 84$, nor at 7 because $7 \nmid 90$, nor at 3 because $3^2 \mid 90$.

Theorem 3.7.6 (Eisenstein's criterion)**.** *Let p be a prime number, and let $P(x) \in \mathbb{Z}[x]$ be a monic polynomial. If $P(x)$ is Eisenstein at p, then it is irreducible over $\mathbb{Q}$ (and thus also over $\mathbb{Z}$). Moreover, let $K = \mathbb{Q}(\alpha)$ where α is an algebraic number such that $P(\alpha) = 0$; then K is totally ramified at p and the order $\mathbb{Z}[\alpha]$ is maximal at p.*

Remark 3.7.7 (non-examinable)**.** Conversely, if K is a number field which is totally ramified at p, then there exists a primitive element $\alpha \in \mathbb{Z}_K$ whose minimal polynomial over $\mathbb{Q}$ is Eisenstein at p.

The proof of this theorem being a bit more technical than the rest of this section, we only give it here for reference; it is not examinable.

Proof. Suppose that $P(x) \in \mathbb{Z}[x]$ is Eisenstein at p, and let n be its degree. If $P(x) = Q(x)R(x)$ were reducible over $\mathbb{Z}$, then we would have $Q(x)R(x) = P(x) \equiv x^n \bmod p$, so that $Q(x) \equiv x^q$ and $R(x) \equiv x^r \bmod p$ for some nonzero integers q, r. But this would mean that p divides the constant terms of $Q(x)$ and $R(x)$, so that p^2 would divide the constant term of $P(x)$, which contradicts the fact that P is Eisenstein at p. Therefore, $P(x)$ is irreducible over $\mathbb{Z}$ (and thus also over $\mathbb{Q}$).

In particular, $K = \mathbb{Q}(\alpha)$ is a well-defined number field of degree n. If the order $\mathbb{Z}[\alpha]$ were not maximal at p, then by Proposition 2.3.1 there would exist integers λ_j not all divisible by p such that $\sum_{j=0}^{n-1} \frac{\lambda_j}{p} \alpha^j \in \mathbb{Z}_K$ is an integer. Then, if j_0 is the smallest integer such that $p \nmid \lambda_j$, then after subtract an element of $\mathbb{Z}[\alpha] \subset \mathbb{Z}_K$ and multiplying by α^{n-1-j_0}, we would get

$$\frac{\lambda_{j_0}}{p} \alpha^{n-1} + \frac{\alpha^n}{p} \sum_{k=0}^{n-j_0-2} \lambda_{j_0+1+k} \alpha^k \in \mathbb{Z}_K.$$

However, the relation $P(\alpha) = 0$ and the fact that p divides the coefficients of $P(x)$ imply that $\frac{\alpha^n}{p} \in \mathbb{Z}[\alpha] \subset \mathbb{Z}_K$, so we would have $\frac{\lambda_{j_0}}{p} \alpha^{n-1} \in \mathbb{Z}_K$. Taking the norm, this would mean that $\frac{\lambda_{j_0}^n N_{\mathbb{Q}}^K(\alpha)^{n-1}}{p^n} \in \mathbb{Z}$. Now, $N_{\mathbb{Q}}^K(\alpha)$ is, up to sign, the constant coefficient of $P(x)$, so it is of the form pq for some integer $q \in \mathbb{Z}$ which is coprime to p. We would then have $\frac{\lambda_{j_0}^n q^{n-1}}{p} \in \mathbb{Z}$, a contradiction.

It follows that the order $\mathbb{Z}[\alpha]$ is maximal at p. Theorem 3.8.1, which we will prove in the next section, implies that since $P(x) \equiv x^n \bmod p$, the decomposition of p in K is $p\mathbb{Z}_K = \mathfrak{p}^n$, where $\mathfrak{p} = (p, \alpha)$. In particular, p is totally ramified in K.

Conversely, suppose now that K is a number field in which $p \in \mathbb{N}$ is totally ramified, say $p\mathbb{Z}_K = \mathfrak{p}^n$ where $n = [K : \mathbb{Q}]$. For nonzero $x \in \mathbb{Z}_K$, let $v_\mathfrak{p}(x)$ be the largest nonnegative integer such that $\mathfrak{p}^{v_\mathfrak{p}(x)} \mid x\mathbb{Z}_K$ (i.e $v_\mathfrak{p}(x)$ is the exponent of $\mathfrak{p}$ in the factorisation of the ideal $x\mathbb{Z}_K$), and set $v_\mathfrak{p}(0) = +\infty$. Clearly, for every finite family of algebraic integers $x_i \in \mathbb{Z}_K$, we have

$$v_\mathfrak{p}\left(\prod_i x_i\right) = \sum_i v_\mathfrak{p}(x_i) \text{ and } v_\mathfrak{p}\left(\sum_i x_i\right) \geqslant \min_i v_\mathfrak{p}(x_i).$$

Besides, if $\sum_i x_i = 0$, then the minimum $\min_i v_\mathfrak{p}(x_i)$ must be attained for at least two values of i, for if not, say $v_\mathfrak{p}(x_1) < v_\mathfrak{p}(x_i)$ for all $i \geqslant 2$ for instance, then we would have

$$v_\mathfrak{p}(x_1) = v_\mathfrak{p}\left(-\sum_{i\geqslant 2} x_i\right) \geqslant \min_{i\geqslant 2} v_\mathfrak{p}(x_i) > v_\mathfrak{p}(x_1),$$

a contradiction. Note that for all $m \in \mathbb{Z}$, we have $v_\mathfrak{p}(m) = n \cdot v_p(m)$, where $v_p(m)$ denotes the exponent of p in the factorisation of m in $\mathbb{Z}$; in particular, $v_\mathfrak{p}(p) = n$.

Since $p \in \mathfrak{p}$, according to proposition 3.5.7 there exists $\alpha \in \mathbb{Z}_K$ such that $\mathfrak{p} = (p, \alpha)$. This means that $\gcd(p\mathbb{Z}_K, \alpha\mathbb{Z}_K) = \mathfrak{p}$, so we must have $v_\mathfrak{p}(\alpha) = 1$. Let $P(x) = x^m + \sum_{i<m} \lambda_i x^i \in \mathbb{Z}[x]$ be the minimal polynomial of α, where $m \leqslant n$ is the degree of α. Then, in the relation

$$\alpha^m + \sum_{i<m} \lambda_i \alpha^i = 0,$$

the minimum of $v_\mathfrak{p}$ must be attained at least twice; but since $v_\mathfrak{p}(\alpha^i) = i \cdot v_\mathfrak{p}(\alpha) = i$ and $p \mid v_\mathfrak{p}(\lambda_i)$ for all i, this forces $m = n$ and $p \mid \lambda_i$ for all i. In particular, this shows that α is a primitive element for $K/\mathbb{Q}$. Finally, the constant coefficient λ_0 is, up to sign, the norm of α, which is, up to sign, the norm of the ideal $\alpha\mathbb{Z}_K$ by theorem 3.4.4. Since $v_\mathfrak{p}(\alpha) = 1$ and $\mathfrak{p}$ is the only prime above p, this proves that $p^2 \nmid \lambda_0$, so that $P(x)$ is Eisenstein at p. □

3.8 Practical factorisation

We are now going to see how to factor ideals explicitly. Let us start with the ideals $p\mathbb{Z}_K$, where $p \in \mathbb{N}$ is prime.

Theorem 3.8.1. *Let K be a number field, $p \in \mathbb{N}$ be prime, $\alpha \in \mathbb{Z}_K$ be an integral primitive element for K, $m(x) \in \mathbb{Z}[x]$ its minimal polynomial over $\mathbb{Q}$,*

$$\overline{m}(x) = \prod_{j=1}^{g} \overline{m_j}(x)^{e_j}$$

the full factorisation of $\overline{m}(x) = m(x) \bmod p$ (that is to say, in $\mathbb{F}_p[x]$), and $f_j = \deg \overline{m_j}(x)$. If the order $\mathbb{Z}[\alpha]$ is p-maximal, then the full factorisation of $p\mathbb{Z}_K$ is

$$p\mathbb{Z}_K = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j},$$

where $\mathfrak{p}_j = \big(p, m_j(\alpha)\big)$ and $m_j(x)$ denotes any lift of $\overline{m_j}(x)$ to $\mathbb{Z}[x]$. Besides, the residue degree of $\mathfrak{p}_j$ is $\deg \overline{m_j}(x)$.

Proof. (non-examinable) Let $n = [K : \mathbb{Q}] = \deg m(x)$. For each j, let $K_j \subset \mathbb{Z}[x]$ be the kernel of the ring homomorphism

$$\rho_j : \mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}[\alpha] \twoheadrightarrow \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \xrightarrow{\sim} \mathbb{Z}_K/p\mathbb{Z}_K \twoheadrightarrow \mathbb{Z}_K/\mathfrak{p}_j,$$

where the first map is evaluation at $x = \alpha$, the third is induced by the inclusion $\mathbb{Z}[\alpha] \subset \mathbb{Z}_K$, and the others are the reduction maps. All these maps are clearly surjective, except maybe for the third one; however, since $\mathbb{Z}[\alpha]$ is p-maximal, proposition 2.3.1 tells us that every element of $\mathbb{Z}_K$ is of the form $\sum_{k=1}^{n} \lambda_k \alpha^k$ with rationals $\lambda_k \in \mathbb{Q}$ whose denominators are coprime to p. As a result, it makes sense to reduce the λ_k mod p, so that this third map is in fact an isomorphism. Therefore, the composite map ρ_j is onto, so the quotient $\mathbb{Z}_K/\mathfrak{p}_j$ is isomorphic to $\mathbb{Z}[x]/K_j$. The fact that $\overline{m_j}(x)$ is irreducible over $\mathbb{F}_p$ implies that

$$\mathbb{Z}[x]/\big(p, m_j(x)\big) \simeq \mathbb{F}_p[x]/\overline{m_j}(x)$$

is a field, so the ideal $\big(p, m_j(x)\big)$ of $\mathbb{Z}[x]$ is maximal by theorem 3.2.7. But K_j clearly contains p and $m_j(x)$, so it contains this maximal ideal, so it is either equal to it, in which case

$$\mathbb{Z}_K/\mathfrak{p}_j \simeq \mathbb{Z}[x]/\big(p, m_j(x)\big) \simeq \mathbb{F}_p[x]/\overline{m_j}(x)$$

is a field with p^{f_j} elements, which means that $\mathfrak{p}_j$ is a prime of $\mathbb{Z}_K$ above p of residue degree f_j, or K_j is the whole of $\mathbb{Z}[x]$, in which case $\mathbb{Z}_K/\mathfrak{p}_j$ is the $\{0\}$ ring.

Let P be the ideal $\prod_{j=1}^{g} \mathfrak{p}_j^{e_j}$ of $\mathbb{Z}_K$. We have

$$\mathfrak{p}_j^{e_j} = (p^{e_j}, p^{e_j-1}\mu_j, \cdots, \mu_j^{e_j})$$

where $\mu_j = m_j(\alpha)$, so P is generated by the elements of $\mathbb{Z}_K$ of the form $\gamma = p^{a_0}\mu_1^{a_1}\cdots\mu_g^{a_g}$ with the a_j nonnegative integers such that $\sum_{j=0}^{g} a_j = \sum_{j=1}^{g} e_j$ and $a_j \leq e_j$ for $j \neq 0$. Clearly, $\gamma \in p\mathbb{Z}_K$ if $a_0 > 0$, whereas if $a_0 = 0$, then necessarily $a_j = e_j$ for all $j \neq 0$, in which case we have $\gamma \in p\mathbb{Z}_K$ anyway since the fact that

$$\prod_{j=1}^{g} m_j(x)^{e_j} = m(x) + pR(x)$$

for some $R(x) \in \mathbb{Z}[x]$ implies that

$$\gamma = \prod_{j=1}^{g} m_j(\alpha)^{e_j} = pR(\alpha).$$

Thus $P \subset p\mathbb{Z}_K$, so lemma 3.4.5 tells us that $p^n \mid N(P)$ with equality iff. $P = p\mathbb{Z}_K$, where $n = [K : \mathbb{Q}]$. But by multiplicativity of the norm, we have

$$N(P) = \prod_{j=1}^{g} N(\mathfrak{p}_j)^{e_j} = \prod_{j=1}^{g} (p^{e_j f_j} \text{ or } 1)$$

depending on whether $\mathbb{Z}_K/\mathfrak{p}_j$ is a field with p^{f_j} elements or the $\{0\}$ ring, whence

$$n \leq \sum_{j=1}^{g} (e_j f_j \text{ or } 0),$$

with equality iff. $P = p\mathbb{Z}_K$. However we have $n = \sum_{j=1}^{g} e_j f_j$ by looking at the degrees of $\overline{m}(x) = \prod_{j=1}^{g} \overline{m_j}(x)^{e_j}$, so the only possibility is that $P = p\mathbb{Z}_K$ and that $\mathbb{Z}_K/\mathfrak{p}_j$ is a field with p^{f_j} elements for all j.

To conclude, we note that since the $\overline{m_j}(x)$ are irreducible and pairwise distinct, they are pairwise coprime, so for each $i \neq j$ there exist $\bar{u}(x)$ and $\bar{v}(x) \in \mathbb{F}_p[x]$ such that

$$\bar{u}(x)\overline{m_i}(x) + \bar{v}(x)\overline{m_j}(x) = \bar{1}.$$

Lifting and evaluating at $x = \alpha$ shows that $1 \in (p, \mu_i, \mu_j) = \mathfrak{p}_i + \mathfrak{p}_j$, which means that the $\mathfrak{p}_j$ are pairwise coprime, and hence pairwise distinct. □

Remark 3.8.2. In the case when for some $p \in \mathbb{N}$, no order of the form $\mathbb{Z}[\beta]$ and maximal at p exists (or is known), it is still possible to determine explicitly the decomposition of $p\mathbb{Z}_K$, but the method is much more complicated.

Remark 3.8.3. Notice how this theorem is consistent with theorem 3.7.1. Namely, for all primes $p \in \mathbb{N}$ such that $\mathbb{Z}[\alpha]$ is p-maximal, we have

$$\begin{aligned} & p \mid \operatorname{disc} K \\ \overset{2.3.3}{\iff} & p \mid \operatorname{disc} \mathbb{Z}[\alpha] \\ \overset{2.3.13}{\iff} & p \mid \operatorname{disc} m(x) \\ \iff & \operatorname{disc} m \equiv 0 \bmod p \\ \overset{2.3.10}{\iff} & m(x) \bmod p \text{ has repeated factors} \\ \overset{3.8.1}{\iff} & p \text{ ramifies in } K. \end{aligned}$$

Remark 3.8.4. In the special case where $m(x)$ is Eisenstein at p, we know that $\mathbb{Z}[\alpha]$ is p-maximal by theorem 3.7.6, so theorem 3.8.1 applies. More precisely, since we have $m(x) \equiv x^n \bmod p$, we get that p splits as

$$p\mathbb{Z}_K = \mathfrak{p}^n \text{ where } \mathfrak{p} = (p, \alpha),$$

which is a refinement of theorem 3.7.6.

Example 3.8.5. Consider the number field $K = \mathbb{Q}(\alpha)$ where α is a root of $f(x) = x^3 - x + 1$. For K to be well-defined, we need to prove that $x^3 - x + 1$ is irreducible; in fact it is already irreducible modulo 2 as we will see below. The discriminant of $f(x)$ is $-4(-1)^3 - 27 \cdot 1^2 = -23$, and this is also the discriminant of $\mathbb{Z}[\alpha]$. Since the index $f = [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ satisfies

$$-23 = \operatorname{disc} \mathbb{Z}[\alpha] = f^2 \operatorname{disc} K,$$

we must have $f = 1$: we have $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. Let us look at some decompositions of primes that can occur.

- at 2: the polynomial $x^3 - x + 1$ has no root in $\mathbb{F}_2$. If it were reducible over $\mathbb{F}_2$, it would have a linear factor. So $f(x) \bmod 2$ is irreducible and $2\mathbb{Z}_K$ is prime: it has residue degree 3 and ramification index 1: the prime 2 is inert in K.

- at 5: the polynomial $x^3 - x + 1$ has 3 as a root modulo 5, yielding a factorisation $f(x) \equiv (x-3)(x^2+3x+3) \bmod 5$. Since x^2+3x+3 has no root modulo 5 and has degree 2, it is irreducible. We obtain $5\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p} = (5, \alpha - 3)$ has residue degree 1 and ramification index 1 and $\mathfrak{p}' = (5, \alpha^2 + 3\alpha + 3)$ has residue degree 2 and ramification index 1: the prime 5 is split but not totally split in K.

- at 23: we have $f(x) = (x+10)^2(x+3) \bmod 23$. We obtain $23\mathbb{Z}_K = \mathfrak{q}^2\mathfrak{q}'$ where $\mathfrak{q} = (23, \alpha + 10)$ has residue degree 1 and ramification index 2, and $\mathfrak{q}' = (23, \alpha + 3)$ has residue degree 1 and ramification index 1: the prime 23 is ramified but not totally ramified in K.

Example 3.8.6. Let $f(x) = x^3 + x^2 - 2x + 8$, and let $K = \mathbb{Q}(\alpha)$ where $f(\alpha) = 0$. We saw in example 2.3.15 that the order $\mathbb{Z}[\alpha]$ is p-maximal for all $p \neq 2$, so for instance we may compute that since $f(x)$ remains irreducible mod 3, the ideal $3\mathbb{Z}_K$ is prime, so that 3 is inert in K. Similarly, the full factorisation of $f(x)$ mod 5 is

$$f(x) \equiv (x + 1)(x^2 + 3) \bmod 5,$$

so

$$5\mathbb{Z}_K = (5, \alpha + 1)(5, \alpha^2 + 3)$$

splits as the product of a prime of degree 1 times another prime of degree 2.

With the help of a computer, we can increase the value of p until we find one which is totally split. We find that the smallest totally split $p \geqslant 3$ is $p = 59$, because

$$f(x) \equiv (x + 11)(x + 20)(x + 29) \bmod 59$$

splits completely mod 59 but does not for any smaller p. In particular, we have

$$59\mathbb{Z}_K = (59, \alpha + 11)(59, \alpha + 20)(59, \alpha + 29),$$

a product of three distinct primes of degree 1.

Finally, we know from example 2.3.15 that $\operatorname{disc} K = -503$, so 503 is the only prime $p \in \mathbb{N}$ which ramifies in K. More precisely, we can check that

$$f(x) = (x + 354)^2(x + 299) \bmod 503,$$

so that

$$503\mathbb{Z}_K = (503, \alpha + 354)^2(503, \alpha + 299).$$

However, we cannot see how $2\mathbb{Z}_K$ factors in $\mathbb{Z}_K$ by factoring $f(x)$ mod 2, because $\mathbb{Z}[\alpha]$ is not maximal at 2. In principle, we could look for another primitive element $\beta \in \mathbb{Z}_K$ such that the order $\mathbb{Z}[\beta]$ is maximal at 2, and then determine the decomposition of $2\mathbb{Z}_K$ by factoring the minimal polynomial of β mod 2. This approach usually works, but unfortunately it does not in this particular case; indeed it can be proved that 2 splits completely in K, so if $\mathbb{Z}[\beta]$ were maximal at 2, then the minimal polynomial of β would be completely split and squarefree mod 2, which is impossible since the only possible linear factors mod 2 are x and $x+1$. Therefore, an order in this field of the form $\mathbb{Z}[\beta]$ is never maximal at 2.

In general, to factor an integral ideal $\mathfrak{a}$, we can use the fact that the norm is multiplicative, and that every prime ideal having norm a power of a prime p appears in the factorisation of $p\mathbb{Z}_K$. The method consists in first factoring $N(\mathfrak{a})$ in $\mathbb{Z}$, then, for each prime p that appears in the factorisation, decomposing $p\mathbb{Z}_K$, and finally, collecting the prime ideals that divide $\mathfrak{a}$.

Example 3.8.7. Let us come back to the problem of factoring 6 in $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}_K$, where $K = \mathbb{Q}(\sqrt{-5})$. Since

$$x^2 + 5 \equiv (x+1)^2 \bmod 2$$

we have

$$2\mathbb{Z}_K = (2, 1+\sqrt{-5})^2,$$

and 2 is totally ramified in K.

Since

$$x^2 + 5 \equiv (x-1)(x+1) \bmod 3,$$

we have

$$3\mathbb{Z}_K = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}),$$

and 3 is totally split in K.

We obtain the factorisation

$$6\mathbb{Z}_K = (2\mathbb{Z}_K)(3\mathbb{Z}_K) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

Furthermore, since the ideals $(1 \pm \sqrt{-5})\mathbb{Z}_K$ are of norm 6, they must each factor into the product of a prime of norm 2 times a prime of norm 3, namely

$$(1 \pm \sqrt{-5})\mathbb{Z}_K = (2, 1+\sqrt{-5})(3, 1 \pm \sqrt{-5}).$$

Thus the factorisations

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

lead to the same decomposition into primes, as they should. Kummer's insight about "ideal numbers" was right!

Example 3.8.8. Let $K = \mathbb{Q}(\sqrt{-7})$ and let $\alpha = \frac{\sqrt{-7}+13}{2}$. Let us compute the factorisation of the ideal $\mathfrak{a} = (\alpha)$ in $\mathbb{Z}_K$. Since $-7 \equiv 1 \bmod 4$ we have $\mathbb{Z}_K = \mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-7}}{2}$. Since $\alpha = \omega + 6 \in \mathbb{Z}_K$, $\mathfrak{a}$ is an integral ideal of $\mathbb{Z}_K$. We compute the norm of this ideal using Theorem 3.4.4:

$$N(\mathfrak{a}) = \left|N_{\mathbb{Q}}^{K}(\alpha)\right| = \frac{1}{4}(7 + 13^2) = 44 = 2^2 \cdot 11.$$

From this we get that $\mathfrak{a}$ is a product of some primes above 2 (one prime of norm 4 or two primes of norm 2, possibly twice the same) and of one prime above 11 of norm 11. We therefore decompose the primes 2 and 11 in K. The minimal polynomial of ω is $m(x) = x^2 - x + 2$ and $\mathbb{Z}_K = \mathbb{Z}[\omega]$, so we can apply Theorem 3.8.1.

- $p = 2$: we have $m(x) \equiv x(x-1) \bmod 2$, so 2 splits completely in K and $2\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p} = (2, \omega)$ and $\mathfrak{p}' = (2, \omega - 1)$.

- $p = 11$: we have $m(x) \equiv (x+4)(x+6) \bmod 11$, so 11 splits completely in K and $11\mathbb{Z}_K = \mathfrak{q}\mathfrak{q}'$ where $\mathfrak{q} = (11, \omega + 4)$ and $\mathfrak{q}' = (11, \omega + 6)$.

Now we know that $\mathfrak{a}$ is a product of two primes above 2 (since they both have norm 2) and one prime above 11, and we must determine which ones.

We clearly have $\alpha = \omega + 2 \cdot 3 \in \mathfrak{p}$. On the other hand we have $\alpha = \omega + 6 \equiv 1 \bmod \mathfrak{p}'$ since $\omega \equiv 1 \bmod \mathfrak{p}'$, so $\alpha \notin \mathfrak{p}'$, in other words $\mathfrak{p}'$ does not divide $\mathfrak{a}$. So $\mathfrak{p}$ divides $\mathfrak{a}$ with exponent 2. In addition we have $\alpha = \omega + 6 \in \mathfrak{q}'$. We conclude that $\mathfrak{a} = \mathfrak{p}^2\mathfrak{q}'$.

3.9 The case of quadratic fields

In this section, we let $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is a squarefree integer different from 0 and 1, and we let $p \in \mathbb{N}$ be an odd prime.

Recall that the *Legendre symbol* is defined by

$$\left(\frac{d}{p}\right) = \begin{cases} 0 & \text{if } p \mid d, \\ +1 & \text{if } d \text{ is a nonzero square mod } p, \\ -1 & \text{if } d \text{ is a nonzero nonsquare mod } p. \end{cases}$$

The Legendre symbols tells us exactly how odd primes split in quadratic field.

Theorem 3.9.1. *Let $p \in \mathbb{N}$, $p \neq 2$ be a prime.*

- *If $\left(\frac{d}{p}\right) = 0$, then $p\mathbb{Z}_K = \mathfrak{p}^2$ is totally ramified in K.*
- *If $\left(\frac{d}{p}\right) = +1$, then $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$ splits completely in K.*
- *If $\left(\frac{d}{p}\right) = -1$, then $p\mathbb{Z}_K = \mathfrak{p}$ is inert in K.*

Proof. Since $p \neq 2$, the order $\mathbb{Z}[\sqrt{d}]$ is p-maximal, so theorem 3.8.1 applies, and tells us that the decomposition of $p\mathbb{Z}_K$ is governed by the splitting behaviour of $x^2 - d \bmod p$. When $\left(\frac{d}{p}\right) = 0, +1$, or -1, $x^2 - d \bmod p$ is respectively a square, a product of two distinct linear factors, or irreducible, hence the result. □

Remark 3.9.2. For the case $\left(\frac{d}{p}\right) = 0$, we could also have used Eisentein's criterion (theorem 3.7.6).

The case of $p = 2$ is special and must be stated separately.

Theorem 3.9.3.

- *If $d \equiv 2$ or $3 \bmod 4$, then $2\mathbb{Z}_K = \mathfrak{p}^2$ is totally ramified in K.*
- *If $d \equiv 1 \bmod 8$, then $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$ splits completely in K.*
- *If $d \equiv 5 \bmod 8$, then $2\mathbb{Z}_K = \mathfrak{p}$ is inert in K.*

Proof. If $d \equiv 2$ or $3 \bmod 4$, then theorem 2.4.2 tells us that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$, so we may apply theorem 3.8.1. Furthermore, we have $x^2 - d \equiv (x-d)^2 \bmod 2$, so 2 is totally ramified in K.

Let us now suppose that $d \equiv 1 \bmod 4$. Then $\mathbb{Z}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, so theorem 3.8.1 does not apply to $\mathbb{Z}[\sqrt{d}]$; on the other hand, it does apply to $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. The minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is $x^2 - x - \frac{d-1}{4}$; when $d \equiv 1 \bmod 8$ it reduces to $x(x-1) \bmod 2$, whereas when $d \equiv 5 \bmod 8$ it reduces to $x^2 + x + 1$, which is irreducible over $\mathbb{F}_2$. □

The point of this is that, thanks to quadratic reciprocity, the decomposition type of p can be read off the class of p modulo $4d$. If you have not seen quadratic reciprocity, do not worry: we will not ask you to use it in assignments or exams.

Example 3.9.4. In $K = \mathbb{Q}(\sqrt{-5})$, for all prime $p \in \mathbb{N}$ we have

- p is (totally) split in K if and only if $p \equiv 1, 3, 7$ or $9 \bmod 20$,
- p is inert in K if and only if $p \equiv 11, 13, 17$ or $19 \bmod 20$,
- p is (totally) ramified in K if and only if $p \equiv 2$ or $5 \bmod 20$.

3.10 The case of cyclotomic fields

In this section, we fix an integer $n \geqslant 3$, and we let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive n^{th} root of unity. The law governing the splitting of primes in K is the following.

Theorem 3.10.1. *Let $p \in \mathbb{N}$ be a prime number, let p^v be the largest power of p which divides n (so in particular $v = 0$ if $p \nmid n$), let $m = n/p^v$, and let $f \in \mathbb{N}$ be the smallest nonzero integer such that $p^f \equiv 1 \bmod m$, i.e. the order of p in the group $(\mathbb{Z}/m\mathbb{Z})^\times$. Then the decomposition of $p\mathbb{Z}_K$ is*

$$p\mathbb{Z}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{\varphi(p^v)},$$

where the $\mathfrak{p}_j$ are distinct primes which are all of inertial degree f. In particular, $g = \varphi(m)/f$.

Proof. (Non examinable) We know from theorem 2.5.2 that $\mathbb{Z}_K = \mathbb{Z}[\zeta]$, so by theorem 3.8.1 the decomposition of $p\mathbb{Z}_K$ corresponds to the factorisation of the cyclotomic polynomial $\Phi_n(x)$ mod p. When ξ_i (resp. η_j) ranges over the set of primitive m^{th} (resp. $(p^v)^{\text{th}}$) roots of unity, then the products $\xi_i \eta_j$ range over the set of primitive n^{th} roots of unity[2], so

$$\Phi_n(x) = \prod_{i,j} (x - \xi_i \eta_j).$$

Note that this factorisation takes place in $\mathbb{Z}_K[x]$, so it makes sense to reduce it modulo ideals of $\mathbb{Z}_K$. Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_K$ above p. Since $\Phi_{p^v}(x)$ divides $(x^{p^v} - 1)$ which is $(x-1)^{p^v}$ mod p and thus also mod $\mathfrak{p}$, we have

$$\Phi_{p^v}(x) = \prod_j (x - \eta_j) \equiv (x-1)^{\varphi(p^v)} \bmod \mathfrak{p},$$

and so $\eta_j \equiv 1 \bmod \mathfrak{p}$ for all j since $\mathbb{Z}_K/\mathfrak{p}$ is a field. As a result,

$$\Phi_n(x) \equiv \prod_{i,j} (x - \xi_i \cdot 1) = \Phi_m(x)^{\varphi(p^v)} \bmod \mathfrak{p},$$

so the coefficients of the difference $\Phi_n(x) - \Phi_m(x)^{\varphi(p^v)}$ lie in $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, i.e.

$$\Phi_n(x) \equiv \Phi_m(x)^{\varphi(p^v)} \bmod p.$$

We are thus led to studying how $\Phi_m(x)$ factors mod p. Now, $\Phi_m(x)$ divides $x^m - 1$, which is coprime mod p with its derivative mx^{m-1} since $p \nmid m$; therefore $x^m - 1$ is squarefree mod p, and so is $\Phi_m(x)$. In other words, reduction mod p is injective on m^{th} roots of unity, and in particular primitive m^{th} roots remain primitive mod p.

Since the multiplicative group of a finite field is cyclic, the field $\mathbb{F}_{p^a}$ contains a primitive m^{th} root of unity if and only if $m \mid p^a - 1$, if and only if $p^a \equiv 1 \bmod m$, if and only if $f \mid a$.

On the other hand, if $\Phi_m(x) \equiv f_1(x) \dots f_k(x) \bmod p$ is the factorisation of Φ_m into irreducibles over $\mathbb{F}_p[x]$, then Φ_m has a root in $\mathbb{F}_{p^a}$ if and only if one of the f_i has a root in $\mathbb{F}_{p^a}$, if and only if there is an i such that $\deg f_i \mid a$.

Putting these together, we obtain that for all i, $f \mid \deg f_i$. Moreover, the field $\mathbb{F}_{p^f}$ contains a primitive m-th root of unity, and therefore contains all

[2] This is just the isomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/p^v\mathbb{Z})^\times$ from Chinese remainders in disguise.

of them, so Φ_m splits completely over $\mathbb{F}_{p^f}$, and therefore we have $\deg f_i = f$ for all i. As a result, the primes above $\mathfrak{p}$ all have inertial degree f. The fact that $g = \varphi(m)/f$ follows from Theorem 3.6.5 since

$$[K : \mathbb{Q}] = \varphi(p^v m) = \varphi(p^v)\varphi(m)$$

as p^v and m are coprime. □

Corollary 3.10.2. *A prime $p \in \mathbb{N}$ splits completely in K if and only if $p \equiv 1 \bmod n$.*

Corollary 3.10.3. *A prime $p \in \mathbb{N}$ ramifies in K if and only if it divides n, except for $p = 2$, which ramifies in K if and only if $4 \mid n$.*

Remark 3.10.4. We already knew this last point from theorem 2.5.2.

Example 3.10.5. Let $n = 15$ and $K = \mathbb{Q}(\zeta_n)$. Let us compute the decomposition of some small primes.

- $p = 2$: we have $m = 15$, and by computing the powers of 2 mod 15 we see that it has order $f = 4$. We therefore have $g = \varphi(m)/f = 8/4 = 2$. The decomposition of 2 is

  $$2\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_2',$$

  and both these primes have residue degree 2 and ramification index 1. The prime 2 splits in K but is not totally split.

- $p = 3$: we have $m = 5$, and $3 \mod 5$ has order $f = 4$. We therefore have $g = \varphi(m)/f = 4/4 = 1$. The decomposition of 3 is

  $$3\mathbb{Z}_K = \mathfrak{p}_3^2 \text{ since } \varphi(3) = 2,$$

  and $\mathfrak{p}_3$ has residue degree 4 and ramification index 2. The prime 3 is ramified but not totally ramified in K.

- $p = 5$: we have $m = 3$, and $5 \equiv -1 \bmod 3$ has order $f = 2$. We therefore have $g = \varphi(m)/f = 2/2 = 1$. The decomposition of 5 is

  $$5\mathbb{Z}_K = \mathfrak{p}_5^4 \text{ since } \varphi(5) = 4,$$

  and $\mathfrak{p}_5$ has residue degree 2 and ramification index 4. The prime 5 is ramified but not totally ramified in K.

- The smallest prime that splits completely in K is $p = 31$, since it is the smallest prime which is 1 mod 15.

In the case when $n = p^v$ is itself a prime power, we can say a little more:

Theorem 3.10.6. *If $n = p^v$, then $p\mathbb{Z}_K = (\zeta - 1)^{\varphi(n)}$. In particular, p is totally ramified in K. Moreover, the minimal polynomial $\Phi_n(x+1)$ of $\zeta - 1$ is Eisenstein at p.*

Proof. We already know that p is totally ramified by Theorem 3.10.1, and that $p\mathbb{Z}_K = \mathfrak{p}^{\varphi(n)}$ where $\mathfrak{p} = (p, \zeta - 1)$, since $\Phi_n(x) \equiv (x-1)^{\varphi(n)} \bmod p$. We have

$$\Phi_n(x+1) \equiv x^{\varphi(n)} \bmod p.$$

Besides,

$$\Phi_n = \frac{x^{p^v} - 1}{x^{p^{v-1}} - 1} = \sum_{j=0}^{p-1} x^{p^{v-1}j},$$

so the constant term of $\Phi_n(x+1)$ is $\Phi_n(1) = p$, so that $N_{\mathbb{Q}}^{K}(\zeta - 1) = \pm p$. Therefore, $\Phi_n(x+1)$ is indeed Eisenstein at p. In addition, the inertial degree of the prime $\mathfrak{p}$ is 1 so its norm is p, and since $\zeta - 1 \in \mathfrak{p}$ has norm $\pm p$, we can conclude that $\mathfrak{p} = (\zeta - 1)$. $\square$

Chapter 4

The class group

4.1 UFDs. vs. PID. vs. Dedekind domains

Section 4.1 is not examinable.

Let $\mathcal{R}$ be a Noetherian domain.

Definition 4.1.1. Let $\alpha, \beta \in \mathcal{R}$. We say that $\alpha \mid \beta$ if there exists $\gamma \in \mathcal{R}$ such that $\beta = \alpha\gamma$. We say that α and β are *coprime* if the only $\delta \in \mathcal{R}$ such that $\delta \mid \alpha$ and $\delta \mid \beta$ are units. Finally, $\alpha \in \mathcal{R}$ is *irreducible* if it is not a unit and cannot be factored, that is to say whenever we have $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathcal{R}$, one of β or γ is a unit.

Example 4.1.2. The elements 2 and 3 are irreducible in $\mathbb{Z}$, and coprime in $\mathbb{Z}$.

Remark 4.1.3. We have $\alpha \mid \beta$ iff. $\beta\mathcal{R} \subset \alpha\mathcal{R}$. In particular, α is irreducible iff. the ideal $\alpha\mathcal{R}$ is maximal (with respect to inclusion) among the principal ideals of $\mathcal{R}$ distinct from $\mathcal{R}$. Note that the restriction to principal ideals means that $\alpha\mathcal{R}$ is not necessarily a maximal ideal in the sense of definition 3.2.6, as it need not be maximal among all ideals of $\mathcal{R}$.

Lemma 4.1.4. *Every nonzero element of $\mathcal{R}$ can be written as a finite product of irreducibles.*

Proof. Let $\alpha_1 \in \mathcal{R}$ be nonzero. If it is irreducible, we're good; else, α_1 factors non-trivially, so let α_2 be one of the factors, and start over.

This way we produce a sequence of elements of $\mathcal{R}$ such that

$$(\alpha_1) \subsetneq (\alpha_2) \subsetneq \cdots .$$

Since $\mathcal{R}$ is Noetherian, this sequence must stop; in other words, we get to an irreducible element after finitely many splittings. Now resume the process on the factors left aside. □

Definition 4.1.5. We say that $\mathcal{R}$ is a *UFD* (short for *Unique Factorisation Domain*) if for every nonzero$\alpha \in \mathcal{R}$, the decomposition of α as a product of irreducibles is unique up to the order of the factors and multiplication by units.

Example 4.1.6. $\mathbb{Z}$ is a UFD. The factorisations

$$6 = 2 \cdot 3 = 3 \cdot 2 = (-2)(-3)$$

do not contradict this fact since they only differ by units and by the order of the factors.

Definition 4.1.7. An element $\alpha \in \mathcal{R}$ is *prime* if the ideal (α) of $\mathcal{R}$ is a prime ideal.

The relation between irreducible elements and prime elements is expressed by the following two lemmas.

Lemma 4.1.8. *Let $\alpha \in \mathcal{R}$ be nonzero. If α is prime, then it is irreducible.*

Proof. Suppose that α is prime, and that we have a factorisation $\alpha = \beta\gamma$. Then $\beta\gamma \in (\alpha)$, so since (α) is a prime ideal, we have $\beta \in (\alpha)$ or $\gamma \in (\alpha)$. Suppose for instance that $\beta \in (\alpha)$. Then β is of the form $\alpha\delta$ for some $\delta \in \mathcal{R}$, whence $\alpha = \beta\gamma = \alpha\delta\gamma$ and

$$\alpha(1 - \delta\gamma) = 0.$$

Since $\alpha \neq 0$ and $\mathcal{R}$ is a domain, this implies $\delta\gamma = 1$, which means that γ (and δ) is a unit. Thus α cannot be factored non-trivially, which means that it is prime. □

The converse does not hold. In fact:

Theorem 4.1.9. *Let $\mathcal{R}$ be a Noetherian domain. The following properties of $\mathcal{R}$ are equivalent:*

(i) *$\mathcal{R}$ is a UFD,*

(ii) *(Converse of lemma 4.1.8) Every irreducible element of $\mathcal{R}$ is prime,*

(iii) *(Euclid's lemma) For all $\pi \in \mathcal{R}$ irreducible, for all $\alpha, \beta \in \mathcal{R}$, if $\pi \mid \alpha\beta$ then $\pi \mid \alpha$ or $\pi \mid \beta$,*

(iv) *(Gauss's lemma) For all $\alpha, \beta, \gamma \in \mathcal{R}$ such that α and β are coprime and $\alpha \mid \beta\gamma$, we have $\alpha \mid \gamma$.*

Proof. (i) $\implies$ (iii) and (iv): Suppose that $\mathcal{R}$ is a UFD. Then every nonzero element of $\mathcal{R}$ has a unique factorisation into irreducibles, the factorisation of $\alpha\beta$ is the joint of that of α and of that of β, and $\beta \mid \alpha$ iff. its factorisation is a part of the factorisation of α. These facts clearly imply Euclid's and Gauss's lemmas.

(ii) $\iff$ (iii): Let π be irreducible. Then (iii) can be rewritten as $\alpha\beta \in (\pi) \implies \alpha \in (\pi)$ or $\beta \in (\pi)$, and thus is equivalent to stating that π is prime.

(iv) $\implies$ (iii): Suppose (iv) holds and let π, α and β be as in (iii). As π is irreducible, either $\pi \mid \alpha$, or π and α are coprime. In the first case we're good, else (iv) implies that $\pi \mid \beta$.

(iii) $\implies$ (i): Finally, let us assume that (iii) holds, and prove that $\mathcal{R}$ is a UFD. Suppose that some $\alpha \in \mathcal{R}$ has two factorisations

$$\alpha = \prod_i \pi_i^{v_i} = \prod_j \Pi_j^{w_j},$$

then $\pi_1 \mid \alpha$ so by iterating (iii) we get that $\pi_1 \mid \Pi_j$ for some j. As π_1 and Π_j are irreducible, this means that they are associate to each other. As $\mathcal{R}$ is a domain, we can cancel π_1 and Π_j; continuing this way, we get that the two factorisations are the same of to units and permutation. □

In particular, Euclid's and Gauss's lemmas do not hold in domains that are not UFDs. Another consequence is the following:

Corollary 4.1.10. *Every PID is a UFD.*

Proof. Let $\mathcal{R}$ be a PID, and let $\pi \in \mathcal{R}$ be irreducible. By remark 4.1.3, (π) is maximal among principal ideals. But since $\mathcal{R}$ is a PID, all ideals are principal, so (π) is maximal among all ideals, hence prime by corollary 3.2.8, and so π is prime. We have thus shown that every irreducible of $\mathcal{R}$ is prime, which implies that $\mathcal{R}$ is a UFD by theorem 4.1.9. □

As demonstrated by example 3.0.1, Dedekind domains are not UFD's in general. In fact,

Proposition 4.1.11. *A Dedekind domain is a PID if and only if it is a UFD.*

Proof. By proposition 4.1.10, we only have to show that if a Dedekind domain is a UFD, then it is a PID.

Let thus $\mathcal{R}$ be a Dedekind domain which is a UFD, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{R}$; we want to show that $\mathfrak{a}$ is principal.

Let $\alpha \in \mathfrak{a}$ be a nonzero element. Since $\mathcal{R}$ is a UFD, we can factor α into irreducibles

$$\alpha = \prod_{j=1}^{m} \pi_j^{a_j}.$$

Since the π_j are irreducible, the ideals (π_j) are prime by theorem 4.1.9. Therefore,

$$\prod_{j=1}^{m} (\pi_j)^{a_j}$$

is the factorisation of the ideal (α) into prime ideals. Since $\mathfrak{a}$ divides (α), we have

$$\mathfrak{a} = \prod_{j=1}^{m} (\pi_j)^{e_j}$$

for some $e_j \leqslant a_j$. It follows that

$$\mathfrak{a} = \left(\prod_{j=1}^{m} \pi_j^{e_j} \right)$$

is principal. Therefore $\mathcal{R}$ is a PID as claimed. □

The ring of integers of a number field is thus not always a UFD. Given a number field K, we would like to be able to decide whether $\mathbb{Z}_K$ is a UFD; in fact, we would like to have a way of deciding whether, in certain situations where $\mathbb{Z}_K$ is not a UFD, we can still use factorisation techniques to prove results about algebraic integers. In this chapter we will introduce a tool to do this: the *class group*.

Remark 4.1.12. Every UFD is integrally closed. Indeed, let $\mathcal{R}$ be a UFD, and let $F = \operatorname{Frac} \mathcal{R}$ be its field of fractions. We must show that if $\alpha \in F$ satisfies $P(\alpha) = 0$ for some nonzero monic polynomial

$$P(x) = x^n + \sum_{j=0}^{n-1} r_j x^j \in \mathcal{R}[x],$$

then α lies in fact in $\mathcal{R}$.

Since $\mathcal{R}$ is a UFD, we may write $\alpha = a/d$, where $a, d \in \mathcal{R}$ are coprime. Clearing denominators, we get

$$a^n + d \sum_{j=0}^{n-1} r_j a^j d^{n-1-j} = 0,$$

which implies that d divides a^n. Therefore, d must be invertible in $\mathcal{R}$.

4.2 Ideal inversion

Definition 4.2.1. Let K be a number field. A *fractional ideal* of K (or of $\mathbb{Z}_K$) is a lattice in K of the form $\frac{1}{d}\mathfrak{a} = \left\{\frac{\alpha}{d}, \alpha \in \mathfrak{a}\right\}$ for some ideal $\mathfrak{a} \subset \mathbb{Z}_K$.

To avoid confusion, ideals of $\mathbb{Z}_K$ in the usual sense are also called *integral ideals*.

Example 4.2.2. The fractional ideals of $\mathbb{Q}$ are the $x\mathbb{Z}$, $x \in \mathbb{Q}^\times$.

The sum and product of a finite family of fractional ideals are defined the same way as for integral ideals, and are fractional ideals. More generally, the notations $(\alpha) = \alpha\mathbb{Z}_K$ and $(\alpha_1, \cdots, \alpha_m) = (\alpha_1) + \cdots + (\alpha_m)$ initially used for integral ideals (so for $\alpha, \alpha_1, \cdots, \alpha_m \in \mathbb{Z}_K$) can be extended to fractional ideals, i.e. to $\alpha, \alpha_1, \ldots, \alpha_m \in K^\times$. For instance, the fractional ideal generated by an element $\alpha \in K^\times$ is

$$(\alpha) = \alpha\mathbb{Z}_K \subset K.$$

Indeed, it is clear by lemma 2.2.18 that $(\alpha_1, \ldots, \alpha_m)$ is a fractional ideal for all $\alpha_1, \ldots, \alpha_m \in K^\times$. It is also clear that this ideal is an integral ideal if and only if $\alpha_1, \ldots, \alpha_m$ lie all in $\mathbb{Z}_K$.

Theorem 4.2.3. *Let K be a number field. Every fractional ideal $\mathfrak{a}$ of K is* invertible*, meaning there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathbb{Z}_K$. This ideal $\mathfrak{b}$ is unique, and is denoted by $\mathfrak{a}^{-1}$.*

Proof. It is enough to show that every nonzero *integral* ideal is invertible as a fractional ideal. Indeed, every fractional ideal $\mathfrak{b}$ is by definition of the form $\frac{1}{d}\mathfrak{a}$ for some nonzero integer $d \in \mathbb{N}$ and nonzero integral ideal $\mathfrak{a} \subseteq \mathbb{Z}_K$, but if $\mathfrak{a}^{-1}$ is an inverse of $\mathfrak{a}$, then clearly $d\mathfrak{a}^{-1}$ is an inverse of $\mathfrak{b}$. So let $\mathfrak{a}$ be a nonzero integral ideal. Then $N(\mathfrak{a}) \in \mathfrak{a}$ by proposition 3.4.3, so $\mathfrak{a} \mid N(\mathfrak{a})\mathbb{Z}_K$, which means that there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = N(\mathfrak{a})\mathbb{Z}_K$. As a result, $\frac{1}{N(\mathfrak{a})}\mathfrak{b}$ is an inverse of $\mathfrak{a}$. The fact that inverses are unique follows from the associativity of ideal multiplication. □

Remark 4.2.4. One can prove that

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset \mathbb{Z}_K\}.$$

Remark 4.2.5. Clearly, the inverse of an integral ideal contains $\mathbb{Z}_K$, and vice versa.

Definition 4.2.6. Let K be a number field. The *group of fractional ideals $\mathcal{I}_K$* is the set of fractional ideals of K, equipped with ideal multiplication.

Proposition 4.2.7. *Let K be a number field. Every fractional ideal $\mathfrak{a}$ of K admits a unique factorisation*

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i}$$

where $e_i \in \mathbb{Z}$ and $\mathfrak{p}_i$ are prime ideals of $\mathbb{Z}_K$.

Proof. Let $\mathfrak{a} = \frac{1}{d}\mathfrak{b}$ where $d \in \mathbb{Z}_{>0}$ and $\mathfrak{b}$ is an integral ideal. By factoring $\mathfrak{b}$ and (d) we obtain a factorisation of $\mathfrak{a}$. The uniqueness statement follows from uniqueness of factorisations of integral ideals. □

Remark 4.2.8.

To compute the factorisation of a fractional ideal, just put it in the form $\frac{1}{d}\mathfrak{a}$ with $d \in \mathbb{N}$ and $\mathfrak{a}$ integral, factor $\mathfrak{a}$ and d separately, and divide their factorisations.

Remark 4.2.9. We could define the norm of the fractional ideal $\frac{1}{d}\mathfrak{a}$ of K as $\frac{N(\mathfrak{a})}{|N^K_{\mathbb{Q}}(d)|} = \frac{N(\mathfrak{a})}{|d|^{[K:\mathbb{Q}]}}$. This extension of the norm is then multiplicative, so that the formulas $N\left(\prod_i \mathfrak{p}_i^{e_i}\right) = \prod_i N(\mathfrak{p}_i)^{e_i}$ (resp. $N(\alpha\mathbb{Z}_K) = |N^K_{\mathbb{Q}}(\alpha)|$) still hold with $e_i \in \mathbb{Z}$ (resp. $\alpha \in K$), but it is of little use. Also beware that the norm of a fractional ideal may be an integer even if this ideal is not an integral ideal (take for instance the fractional ideal $\mathfrak{p}\mathfrak{q}^{-1}$, where $\mathfrak{p}$ and $\mathfrak{q}$ are primes of the same norm).

4.3 Complement: the different

This section may be completely skipped. Its content is not examinable, and will not be covered by the lectures.

Definition 4.3.1. Let K be a number field. The set

$$\mathcal{C}_K = \{\alpha \in K \mid \forall \beta \in \mathbb{Z}_K,\ \mathrm{Tr}^K_{\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}\}$$

is a nonzero fractional ideal of K called the *codifferent* of K. It clearly contains $\mathbb{Z}_K$, so its inverse is an integral ideal of $\mathbb{Z}_K$, called the *different* of K, and denoted by $\mathcal{D}_K = \mathcal{C}_K^{-1}$.

In general, computing the different is tricky, but in some cases it is very easy:

Theorem 4.3.2. *Let K be a number field, assume that there exists $\alpha \in K$ such that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, and let $m(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Then the different of K is*

$$\mathcal{D}_K = m'(\alpha)\mathbb{Z}_K.$$

Proof. Write $m(x) = \sum_{j=0}^n m_j x^j$, where $n = [K : \mathbb{Q}]$. Since $m(\alpha) = 0$, there exist coefficients $\beta_j \in K$ such that

$$m(x) = (x - \alpha)\sum_{j=0}^{n-1} \beta_j x^j.$$

We have $\beta_{j-1} = \alpha\beta_j + m_j$, and since $\beta_{n-1} = 1$, we deduce that

$$\beta_{n-j} = \alpha^{j-1} + m_{n-1}\alpha^{j-2} + m_{n-2}\alpha^{j-3} + \cdots + m_{n-j+1}$$

for all $1 \leqslant j \leqslant n$. Therefore, $(\beta_j)_{0 \leqslant j < n}$ is another $\mathbb{Z}$-basis of $\mathbb{Z}_K$.

Next, let $\sigma_1, \dots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ be the embeddings of K into $\mathbb{C}$, so that the complex roots of $m(x)$ of the $\alpha_j = \sigma_j(\alpha)$. We have

$$\sum_{i=1}^{n} \frac{m(x)}{x - \alpha_i} \frac{\alpha_i^k}{m'(\alpha_i)} = x^k$$

for all $k < n$, since both sides are polynomials of degrees $< n$ which agree at the α_j. But

$$\frac{m(x)}{x - \alpha_i} = \sum_{j=0}^{n-1} \sigma_i(\beta_j) x^j,$$

so the coefficient of x^j in the left-hand side is

$$\sum_{i=1}^{n} \sigma_i(\beta_j) \frac{\alpha_i^k}{m'(\alpha_i)} = \sum_{i=1}^{n} \sigma_i \left(\beta_j \frac{\alpha^k}{m'(\alpha)} \right) = \operatorname{Tr}_{\mathbb{Q}}^{K} \left(\alpha^k \frac{\beta_j}{m'(\alpha)} \right).$$

As a consequence, we have

$$\operatorname{Tr}_{\mathbb{Q}}^{K} \left(\alpha^k \frac{\beta_j}{m'(\alpha)} \right) = \begin{cases} 1 & \text{if } j = k, \\ 0 & \text{else,} \end{cases}$$

for all $j, k < n$, which shows that the codifferent of K is

$$\mathcal{C}_K = \mathbb{Z} \frac{\beta_0}{m'(\alpha)} \oplus \cdots \oplus \mathbb{Z} \frac{\beta_{n-1}}{m'(\alpha)} = \frac{1}{m'(\alpha)} \mathbb{Z}_K,$$

whence the result by inverting both sides. □

The two fundamental properties of the different are the following.

Theorem 4.3.3. *The primes $\mathfrak{p}$ that divide the different $\mathcal{D}_K$ are precisely the ramified primes, and $N(\mathcal{D}_K) = |\operatorname{disc} K|$.*

We do not give the proof of the first point here, because it is unfortunately tedious to do so without introducing tools beyond the scope of these notes; we just mention that these tools make it possible to compute the factorisation the different prime-by-prime, by placing oneself in the case where theorem 4.3.2 applies. On the other hand, we obtain the second point as corollary 4.3.6 below.

One of the reasons to introduce the different is that it can be used to compute inverses of ideals.

Proposition 4.3.4. *Let K be a number field of degree n, and let $\mathfrak{a}$ be a fractional ideal of K. Pick a $\mathbb{Z}$-basis $(\omega_j)_{1 \leqslant j \leqslant n}$ of $\mathbb{Z}_K$ and a $\mathbb{Z}$-basis $(\alpha_j)_{1 \leqslant j \leqslant n}$ of $\mathfrak{a}$, let $A \in \operatorname{Mat}_{n \times n}(\mathbb{Q})$ be the matrix expressing the α_j in terms of the ω_j, and let $T \in \operatorname{Mat}_{n \times n}(\mathbb{Z})$ be the matrix such that $T_{i,j} = \operatorname{Tr}_{\mathbb{Q}}^K(\omega_i \omega_j)$. Then the matrix $({}^{\mathrm{t}}AT)^{-1}$ expresses a $\mathbb{Z}$-basis of $\mathfrak{a}^{-1}\mathcal{D}_K^{-1}$ on the basis $(\omega_j)_{1 \leqslant j \leqslant n}$. Thus, by multiplying the corresponding lattice by $\mathcal{D}_K$, one can recover $\mathfrak{a}^{-1}$.*

Proof. By definition of A we have $\alpha_j = \sum_{i=1}^n A_{i,j}\omega_i$ for all j, so that

$$({}^{\mathrm{t}}AT)_{i,j} = \sum_{k=1}^n A_{k,i} \operatorname{Tr}_{\mathbb{Q}}^K(\omega_k \omega_j) = \operatorname{Tr}_{\mathbb{Q}}^K \left(\sum_{k=1}^n A_{k,i} \omega_k \omega_j \right) = \operatorname{Tr}_{\mathbb{Q}}^K(\alpha_i \omega_j)$$

for all i and j since $A_{k,i} \in \mathbb{Q}$.

Let now C be a column vector with entries $c_1, \cdots, c_n$ in $\mathbb{Q}$, and let $\gamma = \sum_{i=1}^n c_i \omega_i$. Then C is in the $\mathbb{Z}$-span of the columns of $({}^{\mathrm{t}}AT)^{-1}$ iff. $({}^{\mathrm{t}}AT)C$ has integer entries, iff. $\operatorname{Tr}_{\mathbb{Q}}^K(\alpha_i \gamma) \in \mathbb{Z}$ for all i, iff. $\operatorname{Tr}_{\mathbb{Q}}^K(\alpha\gamma) \in \mathbb{Z}$ for all $\alpha \in \mathfrak{a}$, iff. $\operatorname{Tr}_{\mathbb{Q}}^K(\alpha\gamma\beta) \in \mathbb{Z}$ for all $\alpha \in \mathfrak{a}$ and $\beta \in \mathbb{Z}_K$ (because $\alpha\gamma\beta = (\alpha\beta)\gamma$ and $\mathfrak{a}$ is a fractional ideal), iff. $\alpha\gamma \in \mathcal{C}_K$ for all $\alpha \in \mathfrak{a}$, iff. $\gamma\mathfrak{a} \subset \mathcal{C}_K$, iff. $\gamma \in \mathfrak{a}^{-1}\mathcal{C}_K$. □

Remark 4.3.5. This method is convenient for a computer, but with pen and paper the method used in the proof of theorem 4.2.3 is usually much easier.

Corollary 4.3.6. *The norm of the different is $|\operatorname{disc} K|$.*

Proof. Taking $\mathfrak{a} = \mathbb{Z}_K$ in the above, we see that T^{-1} expresses a basis of the codifferent $\mathcal{D}_K^{-1}$ on the basis $(\omega_j)_{1 \leqslant j \leqslant n}$. Since by definition $\det T = \operatorname{disc} K$, the result follows. □

4.4 The class group

Recall that in a ring $\mathcal{R}$ we say that an ideal $\mathfrak{a} \subset \mathcal{R}$ is principal if it is generated by one element, i.e. if there is $x \in \mathcal{R}$ such that $\mathfrak{a} = x\mathbb{Z}_K$.

Definition 4.4.1. Let K be a number field, and let $\mathfrak{a} \subset K$ be a fractional ideal. We say that $\mathfrak{a}$ is *principal* if it is generated by one element, i.e. if there is $x \in K^\times$ such that $\mathfrak{a} = x\mathbb{Z}_K$.

Note that for an integral ideal, it is not clear that this is the same notion as before since we allow generators that are not integers. However, we have the following.

Lemma 4.4.2. *Let K be a number field, and let $\mathfrak{a} \subset \mathbb{Z}_K$ be an integral ideal. Then $\mathfrak{a}$ is principal as a fractional ideal if and only if it is principal in the usual sense.*

Proof. Assume that $\mathfrak{a}$ is principal, and let $x \in K^\times$ be a generator. Then $x\mathbb{Z}_K = \mathfrak{a} \subset \mathbb{Z}_K$, so that x is an algebraic integer. The converse is clear. □

Example 4.4.3. Let $K = \mathbb{Q}(\sqrt{-5})$, so that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$ and $\operatorname{disc} K = -20$. Let $\mathfrak{p}_2$ (resp. $\mathfrak{p}_5$) be the unique prime above 2 (resp. above 5) coming from the decomposition of those primes (Theorems 3.9.1 and 3.9.3). Since $N(\mathfrak{p}_2) = 2$, if $\mathfrak{p}_2$ admitted a generator $x + \sqrt{-5}y \in \mathbb{Z}_K$ then the integers x, y have to satisfy $N_{\mathbb{Q}}^K(x + \sqrt{-5}y) = x^2 + 5y^2 = 2$, which is clearly impossible. So $\mathfrak{p}_2$ is not principal. On the other hand, $\mathfrak{p}_5 = (\sqrt{-5})$ is principal. However, $\mathfrak{p}_2^2 = (2)$ is principal.

Example 4.4.4. Let $K = \mathbb{Q}(\sqrt{-23})$, so that $\mathbb{Z}_K = \mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-23}}{2}$, and $\operatorname{disc} K = -23$. Since $-23 \equiv 1 \bmod 8$, the prime $2 = \mathfrak{p}_2\mathfrak{p}_2'$ splits completely in K by Theorem 3.9.3. To see whether $\mathfrak{p}_2$ is principal, let us compute the norm of a generic element $z = x + \omega y \in \mathbb{Z}_K$. We have

$$N_{\mathbb{Q}}^K(z) = (x + \tfrac{1}{2}y)^2 + \frac{23}{4}y^2 = x^2 + xy + 6y^2.$$

If $N_{\mathbb{Q}}^K(z) = 2$, then $\frac{23}{4}y^2 \leq 2$ so $|y| \leq 2\sqrt{\frac{2}{23}} \approx 0.59$. So we must have $y = 0$, but then $z \in \mathbb{Z}$ cannot have norm 2. Therefore $\mathfrak{p}_2$ is not principal.

In the same way, if $\mathfrak{p}_2^2$ were principal, then its generator z would have norm 4, but again $|y| \leq \frac{2}{\sqrt{23}} \approx 0.83$ and z has to be an integer. Therefore the only element of norm 4 are ± 2, but $(2) = \mathfrak{p}_2\mathfrak{p}_2' \neq \mathfrak{p}_2^2$ by uniqueness of factorisation.

However, for $(x, y) = (1, 1)$ we get an element $z \notin \mathbb{Z}$ of norm 8. The ideals of norm 8 are $\mathfrak{p}_2^3$, $\mathfrak{p}_2^2\mathfrak{p}_2' = 2\mathfrak{p}_2$, $\mathfrak{p}_2\mathfrak{p}_2'^2 = 2\mathfrak{p}_2'$ and $\mathfrak{p}_2'^3$. Since z is not in $2\mathbb{Z}_K$ (because its coefficients on the $\mathbb{Z}$-basis of $\mathbb{Z}_K$ are not divisible by 2), the ideal (z) cannot be $2\mathfrak{p}_2$ or $2\mathfrak{p}_2'$. To determine whether (z) is $\mathfrak{p}_2^3$ or $\mathfrak{p}_2'^3$, we must distinguish them by giving explicit generators.

The minimal polynomial of ω is $x^2 - x + 6$, which factors modulo 2 as $x(x-1) \bmod 2$. We have $\mathfrak{p}_2 = (2, \omega)$ and $\mathfrak{p}_2' = (2, \omega - 1)$. Now $z = \omega + 1 = \omega - 1 + 2 \in \mathfrak{p}_2'$, so that $(z) = \mathfrak{p}_2'^3$.

Finally, $(8/z) = (\mathfrak{p}_2\mathfrak{p}_2')^3/\mathfrak{p}_2'^3 = \mathfrak{p}_2^3$ is principal.

In the last two examples, for each ideal we considered, a power of that ideal was principal. This is a general phenomenon, and suggests that we should look at the multiplicative structure of ideals and principal ideals. This motivates the following definition.

Definition 4.4.5. Let K be a number field. Let $\mathcal{I}_K$ be the group of fractional ideals of K and $\mathcal{P}_K$ be the subgroup of principal fractional ideals of K. The *class group* of K is

$$\mathrm{Cl}(K) = \mathcal{I}_K/\mathcal{P}_K.$$

An *ideal class* is a class in this quotient. We say that two ideals are *equivalent* if they are in the same class. We write $[\mathfrak{a}]$ for the ideal class of the fractional ideal $\mathfrak{a}$.

With this definition, $\mathbb{Z}_K$ is a PID if and only if $\mathrm{Cl}(K)$ is trivial: we say that the class group measures the obstruction for $\mathbb{Z}_K$ to be a PID. By definition, a fractional ideal $\mathfrak{a}$ is principal if and only if the class $[\mathfrak{a}]$ is trivial.

Note that every ideal class is represented by an integral ideal: a fractional ideal $\frac{1}{d}\mathfrak{a}$ with $\mathfrak{a} \subset \mathbb{Z}_K$ is in the same class as $\mathfrak{a}$.

4.5 Finiteness of the class group: the Minkowski bound

The most important result about the class group is that it is always finite.

Theorem 4.5.1 (Minkowski)**.** *Let K be a number field of signature (r_1, r_2) and degree $n = r_1 + 2r_2$. Let*

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\operatorname{disc} K|}.$$

Then every ideal class is represented by an integral ideal of norm at most M_K.

The number M_K is called the Minkowski bound (or the Minkowski constant). If time permits, we will prove this theorem after introducing "geometry of numbers" techniques.

Corollary 4.5.2. *The class group $\mathrm{Cl}(K)$ is finite.*

Proof. It suffices to prove that there are finitely many integral ideals of a given norm, but that follows from the factorisation theorem. □

Because of this finiteness result, the following definition makes sense.

Definition 4.5.3. The *class number* h_K of K is the order of $\mathrm{Cl}(K)$.

Corollary 4.5.4. *The class group of K is generated by the classes of the prime ideals of norm at most M_K.*

Proof. By the factorisation theorem, every integral ideal of norm at most M_K is a product of the primes of norm at most M_K. Passing to the quotient gives the result. □

As claimed, we obtain that every ideal has a power that is principal.

Corollary 4.5.5. *For every fractional ideal $\mathfrak{a}$ of K, the fractional ideal $\mathfrak{a}^{h_K}$ is principal.*

Proof. Since the group $\mathrm{Cl}(K)$ is finite, every element has finite order, and that order is a divisor of the order h_K of the group. □

Corollary 4.5.6. *For every fractional ideal $\mathfrak{a}$ of K and every integer m coprime to h_K, if $\mathfrak{a}^m$ is principal then $\mathfrak{a}$ is principal.*

Proof. Since m is coprime to h_K, there exists integers $u, v \in \mathbb{Z}$ such that $um + vh_K = 1$. We get

$$[\mathfrak{a}] = [\mathfrak{a}]^{um+vh_K} = ([\mathfrak{a}]^m)^u([\mathfrak{a}]^{h_K})^v = 1,$$

where $[\mathfrak{a}]^m = 1$ by hypothesis and $[\mathfrak{a}]^{h_K} = 1$ by Corollary 4.5.5. This says exactly that $\mathfrak{a}$ is principal. □

Theorem 3.7.3 is now a consequence of

Corollary 4.5.7. *If K is a number field of degree $n \geq 2$ and discriminant $\operatorname{disc} K$, then*

$$|\operatorname{disc} K| \geq \frac{4}{e^3}\left(\frac{\pi e^{3/2}}{4}\right)^n > 1.$$

Proof. Since every integral ideal has norm at least one, we have $M_K \geq 1$. We can rewrite this as

$$|\operatorname{disc} K| \geq \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2r_2} \geq \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{n}.$$

Let $u_n = \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^n$. For all $n \geq 2$ we have

$$\begin{aligned}\frac{u_{n+1}}{u_n} &= \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} = \frac{\pi}{4}\exp\left(2n\log\Big(1+\frac{1}{n}\Big)\right) \geq \frac{\pi}{4}\exp\left(2n\Big(\frac{1}{n}-\frac{1}{2n^2}\Big)\right)\\ &= \frac{\pi}{4}\exp\Big(2-\frac{1}{n}\Big) \geq \frac{\pi}{4}\exp\Big(\frac{3}{2}\Big).\end{aligned}$$

Since $u_2 = \pi^2/4$, we obtain the result. □

For examples of computations of class groups, see Section 6.3.

4.6 Applications: Diophantine equations

4.6.1 Sums of two squares

The problem in this section is to determine the integers that are sums of two squares. In other words, for each integer $n \in \mathbb{Z}$ we want to determine whether the equation

$$x^2 + y^2 = n, \quad x, y \in \mathbb{Z} \tag{4.1}$$

has a solution. An obvious necessary condition is that $n \geq 0$. Moreover, since Equation 4.1 clearly has a solution for $n = 0$, we can assume that $n > 0$. To study this equation, we remark that we can factor it as

$$n = x^2 + y^2 = (x + yi)(x - yi) = N_{\mathbb{Q}}^{\mathbb{Q}(i)}(x + yi), \quad x, y \in \mathbb{Z}.$$

Since the ring of integers of $K = \mathbb{Q}(i)$ is $\mathbb{Z}_K = \mathbb{Z}[i]$, we see that Equation 4.1 is actually a special case of a *norm equation*:

$$N_{\mathbb{Q}}^{K}(z) = n, \quad z \in \mathbb{Z}_K. \tag{4.2}$$

What we are going to see on this particular example is a general method to solve norm equations, although we may need to adapt it to the particular situation.

Note that a nice consequence of Equation 4.2 is that the set of solutions is multiplicative: a product of solutions is again a solution. This was not obvious from Equation 4.1.

The first step is to find which positive integers n are the norm of an integral ideal in $\mathbb{Z}_K$.

Lemma 4.6.1. *Let $n \in \mathbb{Z}_{>0}$, and let $n = \prod_i p_i^{a_i}$ be its factorisation into distinct primes. Then n is the norm of an integral ideal in $\mathbb{Z}[i]$ if and only if for every p_i that is inert in K, the exponent a_i is even.*

Proof. Let $\mathfrak{a} = \prod_j \mathfrak{q}_j^{b_j}$ be an integral ideal of $\mathbb{Z}_K$, and for all j let q_j be the prime below $\mathfrak{q}_j$ and f_j be the inertial degree of $\mathfrak{q}_j$, i.e. $f_j = 2$ if q_j is inert and $f_j = 1$ otherwise. Then we have

$$N(\mathfrak{a}) = \prod_j q_j^{f_j b_j},$$

so the condition of the lemma is necessary.

Let us prove that the condition is sufficient. By multiplicativity of the norm, it is enough to prove it for n a prime power, say $n = p^a$. If p is not inert then there is a prime $\mathfrak{p}$ above p of inertial degree 1, and hence of norm p, so that $N(\mathfrak{p}^a) = p^a$. If p is inert, the condition says that $a = 2b$ is even, and $N\big((p)^b\big) = p^a$. □

Theorem 4.6.2. *An integer $n > 0$ is a sum of two squares if and only if for every prime p dividing n and congruent to 3 modulo 4, the exponent of p in the factorisation of n is even.*

Proof. First, note that a prime number p is inert in K if and only if $\left(\frac{-1}{p}\right) = -1$, if and only if $p \equiv 3 \bmod 4$.

By Lemma 4.6.1, the condition is necessary. Conversely, if n satisfies the condition, then by Lemma 4.6.1 there exists an integral ideal $\mathfrak{a}$ such that $N(\mathfrak{a}) = n$. But we have seen that $h_K = 1$, so $\mathfrak{a}$ is principal: let z be a generator of $\mathfrak{a}$, so that $z \in \mathbb{Z}_K$. Then $n = N(\mathfrak{a}) = N(z\mathbb{Z}_K) = |N_{\mathbb{Q}}^K(z)| = N_{\mathbb{Q}}^K(z)$ is a sum of two squares. □

4.6.2 Another norm equation

Proposition 4.6.3. *The integers of the form $x^2 + xy + 5y^2$ are exactly the positive integers such that for every prime $p \mid n$ such that $p = 2$ or that -19 is not a square mod p, the exponent of p in the factorisation of n is even.*

Proof. The statement suggests to look at $K = \mathbb{Q}(\sqrt{-19})$. Since -19 is squarefree and $-19 \equiv 1 \bmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{-19}}{2}$, and $\operatorname{disc} K = -19$. The norm of a generic element $z = x + y\alpha$ is

$$N_{\mathbb{Q}}^K(z) = (x + \tfrac{y}{2})^2 + 19(\tfrac{y}{2})^2 = x^2 + xy + 5y^2.$$

So the problem again reduces to a norm equation.

As before, a positive integer n is the norm of an integral ideal of $\mathbb{Z}_K$ if and only if every prime that is inert appears with an even exponent.

In order to apply the same method as before, we need to compute the class group of K. Since the signature of K is $(0, 1)$, the Minkowski bound is $M_K = \frac{2}{\pi}\sqrt{19} \approx 2.77 < 3$, so the class group of K is generated by the classes of ideals above 2. Since $-19 \equiv 5 \bmod 19$, the prime 2 is inert, so the unique ideal above 2 is (2) which is principal, so $h_K = 1$.

As before, since $\mathbb{Z}_K$ is a PID, a positive integer is the norm of an integral ideal of K if and only if it is the norm of an element of $\mathbb{Z}_K$.

Since 2 is inert, the condition on p in the Proposition is indeed equivalent to p being inert. $\square$

Remark 4.6.4. The ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID, but one can prove that it is not Euclidean![1]

4.6.3 A norm equation with a nontrivial class group

Let us see what happens when the class group is not trivial. Let us take $K = \mathbb{Q}(\sqrt{-23})$. We know from example 6.3.4 that $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$, that the norm of $x + y\frac{1+\sqrt{-19}}{2}$ is $x^2 + xy + 6y^2$, that 2 splits in K, say $(2) = \mathfrak{p}_2\mathfrak{p}_2'$, and that $\mathrm{Cl}(K) \simeq \mathbb{Z}/3\mathbb{Z}$ is generated by the class of $\mathfrak{p}_2$.

Because $\mathrm{Cl}(K)$ is not trivial, discussing which $n \in \mathbb{N}$ are of the form $x^2 + xy + 6y^2$ is much more difficult in general, so we are going to restrict ourselves to prime powers. So lets us fix a prime $p \in \mathbb{N}$, and study the set of $n \in \mathbb{Z}_{\geqslant 0}$ such that p^n is of the form $x^2 + xy + 6y^2$.

This is the case if and only if there exists an element $\alpha \in \mathbb{Z}_K$ of norm p^n, and the ideal (α) is then an ideal of $\mathbb{Z}_K$ of norm p^n. Conversely, if there

[1] To see this, assume on the contrary that d is a Euclidean function, and let $\alpha \in \mathbb{Z}_K \setminus \mathbb{Z}_K^\times$ minimizing d. Then every element of $\mathbb{Z}_K/\alpha\mathbb{Z}_K$ can be represented by an element of $\mathbb{Z}_K^\times \cup \{0\}$, whence $|N_{\mathbb{Q}}^K(\alpha)| = \#(\mathbb{Z}_K/\alpha\mathbb{Z}_K) \leqslant 1 + \#\mathbb{Z}_K^\times = 3$. But that is not possible since 2 and 3 are both inert in K.

exits a *principal* ideal of $\mathbb{Z}_K$ of norm p^n, then there exists an $\alpha \in \mathbb{Z}_K$ of norm $\pm p^n$; but $N_{\mathbb{Q}}^K(\alpha) > 0$ for all $\alpha \in K^\times$, so the equation $x^2 + xy + 6y^2 = p^n$ has then a solution. To sum up,

$$x^2+xy+6y^2 = p^n \text{ has a solution } \iff \exists \text{ ideal } \mathfrak{a} \subset \mathbb{Z}_K \text{ principal and of norm } p^n.$$

Note that the condition $N(\mathfrak{a}) = p^n$ implies that the prime ideals dividing $\mathfrak{a}$ all lie above p. We now distinguish three cases.

- If p is inert in K (example : $p = 5$), then the only prime above p is $\mathfrak{p} = p\mathbb{Z}_K$, which has norm p^2. So there exists an ideal of norm p^n if and only if n is even; besides, this ideal, if it exists, is always principal since $\mathfrak{p} = (p)$ is principal. As a conclusion, p^n is of the form $x^2 + xy + 6y^2$ if and only if n is even.

- If p splits in K, say $p\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'$, then we have $N(\mathfrak{p}) = N(\mathfrak{p}') = p$, so the primes of norm p^n are exactly the $\mathfrak{p}^a\mathfrak{p}'^b$, where a and b are nonnegative integers such that $a + b = n$. We now distinguish two subcases:

  - If $\mathfrak{p}$ is principal (example: $p = 59$), then so is $\mathfrak{p}'$ since $[\mathfrak{p}'] = [\mathfrak{p}]^{-1}$, so $\mathfrak{p}^a\mathfrak{p}'^b$ is principal for all a and b. As a result, p^n is of the form $x^2 + xy + 6y^2$ for all n.
  - If $\mathfrak{p}$ is not principal (example: $p = 2$), then neither is $\mathfrak{p}'$ since $[\mathfrak{p}'] = [\mathfrak{p}]^{-1}$. Since $\mathrm{Cl}(K) \simeq \mathbb{Z}/3\mathbb{Z}$, $[\mathfrak{p}]$ and $[\mathfrak{p}']$ are inverse classes of order 3 in $\mathrm{Cl}(K)$. Therefore, $\mathfrak{p}^a\mathfrak{p}'^b$ is principal if and only if $a \equiv b \bmod 3$. As a result, p^n is of the form $x^2 + xy + 6y^2$ if and only if the equation
  $$\begin{cases} a + b = n \\ a \equiv b \bmod 3 \end{cases}$$
  has a solution with $a, b \in \mathbb{Z}_{\geqslant 0}$. Now, if $n = 1$, this equation clearly has no solution, whereas if n is even we can take $a = b = n/2$, and finally if n is odd and $\geqslant 3$, we can write $n = 2m + 3$ and take $a = m + 3$ and $b = m$. As a conclusion, p^n is of the form $x^2 + xy + 6y^2$ if and only if $n \neq 1$.

- If p is ramifies in K, say $p\mathbb{Z}_K = \mathfrak{p}^2$, then $p \mid \operatorname{disc} K$ so $p = 23$. There exits an element of norm 23 in $\mathbb{Z}_K$, namely $\sqrt{-23}$, and the ideal generated by this element, which has norm 23, can only be $\mathfrak{p}$. So $\mathfrak{p}$ is principal. Next, an ideal of norm p^n can only be $\mathfrak{p}^n$, which is principal for all n. As a conclusion, 23^n is of the form $x^2 + xy + 6y^2$ for all n.

4.6.4 Mordell equations

A *Mordell equation* is a Diophantine equation of the form

$$y^2 = x^3 + k, \quad x, y \in \mathbb{Z},$$

for some fixed $k \in \mathbb{Z}$. Our plan to study these equations is to factor them in the form

$$x^3 = (y - \sqrt{k})(y + \sqrt{k}),$$

and then hope that the factors on the right hand side must be cubes.

Lemma 4.6.5. *If a and b are coprime integers, and ab is an n-th power, then a and b are both of the form $\pm x^n$.*

Proof. Up to sign, the factorisation of ab is the product of the factorisations of a and b. Since ab is an n-th power, the exponent of every prime is a multiple of n. Since the sets of primes dividing a and b are disjoint, the exponents in their respective factorisation are multiples of n, so a and b are of the form $\pm x^n$. □

Example 4.6.6. Consider the Mordell equation

$$y^2 = x^3 + 16, \quad x, y \in \mathbb{Z}.$$

There are obvious solutions $(0, \pm 4)$. Are there any other ones?

We factor the equation as

$$x^2 = (y - 4)(y + 4).$$

If y is odd, then $a = y - 4$ and $b = y + 4$ are coprime: any common divisor would have to divide $b - a = 8$, but a and b are odd. By Lemma 4.6.5, a and b are cubes, but they differ by 8. Since cubes get further and further apart, there are no odd cubes that differ by 8. To see this, write the first few odd cubes:

$$\ldots, -27, -1, 1, 27, \ldots$$

and note that after these, the differences are larger than 8.

If y is even, then x is even, so $y^2 = x^3 + 16$ is divisible by 8 and y is divisible by 4: $y = 4y'$. Then $x^3 = 16y'^2 - 16$ is divisible by 16, so x is also a multiple of 4: $x = 4x'$. The equation now becomes

$$y'^2 = 4x'^3 + 1,$$

so y' is odd: $y' = 2y'' + 1$. Simplifying the equation we get

$$x'^3 = y''(y'' + 1).$$

Since y'' and $y'' + 1$ are coprime, they are cubes. Since they differ by 1, we must have $y'' = 0$ or $y'' = -1$. Again, to see this you can write down the small cubes

$$\ldots, -8, -1, 0, 1, 8, \ldots$$

and note that after these, the differences are larger than 1.

This gives $y' = \pm 1$ and hence $y = \pm 4$, so the obvious solutions are the only ones.

Proposition 4.6.7. *Let K be a number field and let $n \geq 1$ be coprime to the class number of K. Let $a, b \in \mathbb{Z}_K$ be such that the ideals (a) and (b) are coprime and such that ab is an n-th power. Then $a = ux^n$ and $b = vy^n$ where $u, v \in \mathbb{Z}_K^\times$ are units and $x, y \in \mathbb{Z}_K$.*

Proof. Since the ideal (ab) is the n-th power of an ideal and (a) is coprime to (b), by the factorisation theorem 3.5.1, (a) and (b) are n-th powers of ideals: $(a) = \mathfrak{a}^n$ and $(b) = \mathfrak{b}^n$. Now n is coprime to the class number, and the n-th power of $\mathfrak{a}$ and $\mathfrak{b}$ are principal, so $\mathfrak{a}$ and $\mathfrak{b}$ are principal: $\mathfrak{a} = (x)$ and $\mathfrak{b} = (y)$. This gives $(a) = (x^n)$ and $(b) = (y^n)$, so that a/x^n and b/y^n are units in $\mathbb{Z}_K$. □

Example 4.6.8. Consider the Mordell equation

$$y^2 = x^3 - 2, \quad x, y \in \mathbb{Z}.$$

Let $K = \mathbb{Q}(\sqrt{-2})$. Since $-2 \equiv 2 \bmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-2}]$ and the discriminant of K is $\operatorname{disc} K = -8$. The Minkowski bound is

$$M_K = \frac{4}{\pi}\frac{2!}{2^2}\sqrt{|-8|} \approx 1.8 < 2,$$

so the class group of K is trivial.

Suppose (x, y) is a solution. We have

$$x^3 = (y - \sqrt{-2})(y + \sqrt{-2}).$$

We want to prove that the ideals $(y - \sqrt{-2})\mathbb{Z}_K$ and $(y + \sqrt{-2})\mathbb{Z}_K$ are coprime. Let $\mathfrak{p}$ be a prime dividing both these ideals. Then both $y - \sqrt{-2}$

and $y+\sqrt{-2}$ belong to $\mathfrak{p}$, so their difference also does: $\mathfrak{p}$ divides $2\sqrt{-2}$. Since $N_{\mathbb{Q}}^{K}(2\sqrt{-2}) = 8$ is a power of 2 and 2 decomposes as $\mathfrak{p}_2^2$ in $\mathbb{Z}_K$, the prime $\mathfrak{p}$ must necessarily be $\mathfrak{p}_2$.

We compute that $\mathfrak{p}_2 = (2, \sqrt{-2})$. In particular, $\sqrt{-2} \in \mathfrak{p}_2$, so we have $y = (y+\sqrt{-2}) - \sqrt{-2} \in \mathfrak{p}_2$. But $y \in \mathbb{Z}$ and $\mathfrak{p}_2 \cap \mathbb{Z} = 2\mathbb{Z}$ (this is just saying that the prime $\mathfrak{p}_2$ lies above 2), so this implies that y is even. The equation then implies that x is also even, but then reducing modulo 4 gives a contradiction. So $\mathfrak{p}$ does not exist, and the ideals $(y-\sqrt{-2})\mathbb{Z}_K$ and $(y+\sqrt{-2})\mathbb{Z}_K$ are indeed coprime.

We have $\mathbb{Z}_K^\times = \{\pm 1\}$ (we will see why in the next chapter), so every element of $\mathbb{Z}_K^\times$ is a cube. By Proposition 4.6.7, $y+\sqrt{-2}$ is thus a cube, say $(a+\sqrt{-2}b)^3$ with $a, b \in \mathbb{Z}$. We have

$$(a+b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2},$$

giving the equations

$$a(a^2-6b^2) = y \text{ and } b(3a^2-2b^2) = 1.$$

By the second equation, we must have $b = \pm 1$.

- if $b = 1$, then $3a^2 - 2b^2 = 1$ so $3a^2 = 3$ and $a = \pm 1$, giving the solutions $(x, y) = (3, \pm 5)$.
- if $b = -1$, then $3a^2 - 2b^2 = -1$, so $3a^2 = 1$, which is impossible.

In conclusion, the solutions of the equation are $(x, y) = (3, \pm 5)$.

4.6.5 The regular case of Fermat's last theorem

Using Proposition 4.6.7, Kummer was able to fix Lamé's approach to Fermat's equation. Namely he proved that if $p \geq 3$ is *regular*, that is to say that it does not divide the class number of $\mathbb{Q}(\zeta_p)$ (which happens for all $p \leq 100$ except 37, 59 and 67), then $x^p + y^p = z^p$ has non nontrivial solutions.

Chapter 5

Units

As we saw in the last two chapters, using ideals we can recover a good factorisation theory in number fields. But by going from elements to ideals, we loose something: associate elements of $\mathbb{Z}_K$ generate the same ideal. This motivates the study of the unit group $\mathbb{Z}_K^\times$.

5.1 Units in a domain

In this section, we fix a commutative domain $\mathcal{R}$.

Definition 5.1.1. Let $u \in \mathcal{R}$. We say that u is a *unit* in $\mathcal{R}$ if it is invertible in $\mathcal{R}$, that is to say if there exists $v \in \mathcal{R}$ such that $uv = 1$.

Such a v is then necessarily unique[1], and is denoted by $v = u^{-1}$.

The set of units of $\mathcal{R}$ is denoted by $\mathcal{R}^\times$. It is an Abelian group under multiplication.

Example 5.1.2.

- For $\mathcal{R} = \mathbb{Z}$, we have $\mathcal{R}^\times = \{\pm 1\}$; this explains the term *unit*.
- If $\mathcal{R}$ is actually a field, then $\mathcal{R}^\times = \mathcal{R} \setminus \{0\}$.
- If $\mathcal{R} = k[X]$ is a polynomial ring over a field k, then $\mathcal{R}^\times = k^\times = k \setminus \{0\}$ consists of the nonzero constant polynomials.

[1] Indeed, if we have $uv = uv' = 1$, then multiplying the identity $uv = 1$ by v' yields $v = v'$.

Proposition 5.1.3. *Let $a, b \in \mathcal{R}$. Then the ideals $a\mathcal{R}$ and $b\mathcal{R}$ agree if and only if a and b are* associate *in ring, that is to say if and only if there exists a unit $u \in \mathcal{R}^\times$ such that $b = au$.*

In practicular, $a\mathcal{R} = \mathcal{R}$ if and only if a is a unit.

Proof. First, note that

$$b\mathcal{R} \subseteq a\mathcal{R} \iff b \in a\mathcal{R} \iff \exists u \in \mathcal{R} \colon b = au.$$

So if we have $a\mathcal{R} = b\mathcal{R}$, then there exist $u, v \in \mathcal{R}$ such that $b = au$ and $a = bv$, whence $a(1 - uv) = 0$. If $a \neq 0$, this implies that $uv = 1$ since $\mathcal{R}$ is a domain, so that u and v are units in $\mathcal{R}$; and if $a = 0$, then $b \in b\mathcal{R} = a\mathcal{R} = \{0\}$ so $b = 0$, and a and b are then trivially associate.

Conversely, if $b = au$ with $u \in \mathcal{R}^\times$, then $b\mathcal{R} \subseteq a\mathcal{R}$; but we also have $a = bu^{-1}$ with $u^{-1} \in \mathcal{R}$, so $a\mathcal{R} \subseteq b\mathcal{R}$. □

5.2 Units in $\mathbb{Z}_K$

Definition 5.2.1. Let K be a number field. A *unit* in K is an element of $\mathbb{Z}_K^\times$.

Note that we are slightly twisting the definition of unit here: in principle, we should talk about units in $\mathbb{Z}_K$, not in K, but such is the terminology!

Proposition 5.2.2. *Let K be a number field, and let $\alpha \in K$. The following are equivalent:*

(i) $\alpha \in \mathbb{Z}_K^\times$;

(ii) $\alpha\mathbb{Z}_K = \mathbb{Z}_K$;

(iii) $\alpha \in \mathbb{Z}_K$ *and* $N_{\mathbb{Q}}^K(\alpha) = \pm 1$;

(iv) $\alpha \in \mathbb{Z}_K$ *and the constant term of the minimal polynomial of* α *is* ± 1;

(v) $\alpha \in \mathbb{Z}_K$ *and* $\alpha^{-1} \in \mathbb{Z}[\alpha]$.

Proof.

- (i) $\Rightarrow$ (ii). This is a special case of proposition 5.1.3.

- (ii) $\Rightarrow$ (iii). Since $\alpha\mathbb{Z}_K = \mathbb{Z}_K$, we have $\alpha \in \mathbb{Z}_K$. By taking norms we have $|N_{\mathbb{Q}}^K(\alpha)| = N((\alpha)) = 1$.

- (iii) $\Rightarrow$ (iv). $N_{\mathbb{Q}}^K(\alpha) = \pm 1$ is a power of this constant term, and both are integers, so the constant term is also ± 1.

- (iv) $\Rightarrow$ (v). Let $\sum_{i=0}^n a_i x^i$ be the minimal polynomial of α, where $a_0 = \pm 1$ and $a_n = 1$. Write it as
$$\alpha \left(\sum_{i=1}^n a_i \alpha^{i-1} \right) = - \pm 1.$$
This proves that
$$\alpha^{-1} = - \pm \sum_{i=1}^n a_i \alpha^{i-1} \in \mathbb{Z}[\alpha],$$

- (v) $\Rightarrow$ (i). Since $\alpha \in \mathbb{Z}_K$ and $\alpha^{-1} \in \mathbb{Z}[\alpha] \subset \mathbb{Z}_K$, we have $\alpha \in \mathbb{Z}_K^\times$.

□

Example 5.2.3.

1. $\alpha = 1 + \sqrt{2} \in K = \mathbb{Q}(\sqrt{2})$ lies in $\mathbb{Z}_K = \mathbb{Z}[\sqrt{2}]$ and has norm -1, so it is a unit. Indeed, $1/\alpha = \sqrt{2} - 1 \in \mathbb{Z}[\alpha]$. Thus α^n is a unit for all $n \in \mathbb{Z}$, and $\mathbb{Z}_K^\times$ is infinite.

2. Similarly, $\phi = \frac{1+\sqrt{5}}{2} \in K = \mathbb{Q}(\sqrt{5})$ is a unit of norm -1, so $\mathbb{Z}_K^\times$ is again infinite.

3. However, $\alpha = \frac{3+4i}{5} \in \mathbb{Q}(i)$ has norm 1 but is not a unit, since it is not an algebraic integer.

Corollary 5.2.4. *For all number fields $K \subset L$, we have*
$$\mathbb{Z}_K^\times = K \cap \mathbb{Z}_L^\times.$$

Proof. Since $\mathbb{Z}_K = K \cap \mathbb{Z}_L$, this follows from (iv) of Proposition 5.2.2. □

Corollary 5.2.5. *Let $\mathcal{O} \subset \mathbb{Z}_K$ be an order. Then*
$$\mathcal{O}^\times = \mathcal{O} \cap \mathbb{Z}_K^\times.$$

Proof. The inclusion $\subset$ is clear. The opposite inclusion follows from (v) of Proposition 5.2.2. $\square$

In this setting, we can prove that the subgroup $\mathcal{O}^\times$ of $\mathbb{Z}_K^\times$ has finite index, and bound this index:

Proposition 5.2.6. *Let K be a number field, let $\mathcal{O}$ be an order in K and let f be the index of $\mathcal{O}$ in $\mathbb{Z}_K$. Then $\mathcal{O}^\times \subset \mathbb{Z}_K^\times$ is a subgroup of finite index, and*

$$[\mathbb{Z}_K^\times \colon \mathcal{O}^\times] \leq \#(\mathbb{Z}_K/f\mathbb{Z}_K)^\times.$$

Proof. Let $\phi\colon \mathbb{Z}_K^\times \to (\mathbb{Z}_K/f\mathbb{Z}_K)^\times$ be the reduction modulo f map. Let $u \in \ker\phi$. Then $u - 1 \in f\mathbb{Z}_K \subset \mathcal{O}$, so $u \in \mathcal{O}$. This proves that

$$\ker\phi \subset \mathcal{O}^\times \subset \mathbb{Z}_K^\times,$$

so that

$$[\mathbb{Z}_K^\times : \mathcal{O}^\times] \leq [\mathbb{Z}_K^\times \colon \ker\phi] \leq \#(\mathbb{Z}_K/f\mathbb{Z}_K)^\times,$$

where the last inequality holds because the induced map

$$\mathbb{Z}_K^\times/\ker\phi \to (\mathbb{Z}_K/f\mathbb{Z}_K)^\times$$

is injective. $\square$

5.3 Roots of unity

We will start by studying the simplest units: the ones that have finite order, that is, the roots of unity.

5.3.1 Roots of unity under complex embeddings

Definition 5.3.1. Let K be a number field of signature (r_1, r_2). We define the *Minkowski space* to be $K_\mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Let $\sigma_1, \dots, \sigma_{r_1}$ be the real embeddings of K, and let $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ be representatives of the nonreal embeddings of K up to complex conjugation. The *Minkowski embedding*

$$\Sigma\colon K \hookrightarrow K_\mathbb{R}$$

is defined by

$$\Sigma(x) = \big(\sigma_i(x)\big)_{i=1}^{r_1+r_2}.$$

Example 5.3.2.

1. Let $K = \mathbb{Q}(\alpha)$ where $\alpha^2 = 2$. The number field K has signature $(2, 0)$, and the two real embeddings are $\sigma_1 \colon \alpha \mapsto \sqrt{2}$ and $\sigma_2 \colon \alpha \mapsto -\sqrt{2}$. So the Minkowski embedding is
$$\Sigma \colon x + y\alpha \mapsto (x + y\sqrt{2}, x - y\sqrt{2}).$$

2. Let $K = \mathbb{Q}(\beta)$ where $\beta^3 = 2$. The number field K has signature $(1, 1)$, and we can choose the embeddings to be $\sigma_1 \colon \beta \mapsto 2^{1/3}$ and $\sigma_2 \colon \beta \mapsto 2^{1/3}j$ (where $j = \exp(2i\pi/3)$). The third complex embedding is $\sigma_3 = \overline{\sigma_2} \colon \beta \mapsto 2^{1/3}j^2$. We obtain the Minkowski embedding
$$\Sigma \colon x + y\beta + z\beta^2 \mapsto (x + y2^{1/3} + z2^{2/3}, x + y2^{1/3}j + z2^{2/3}j^2).$$

Proposition 5.3.3. *Let K be a number field, and let $B \subset K_{\mathbb{R}}$ be a bounded subset. Then $\Sigma(\mathbb{Z}_K) \cap B$ is finite.*

Proof. Let $x \in \mathbb{Z}_K$ be such that $\Sigma(x) \in B$, so that we have a bound on every complex embedding of x, say $|\sigma(x)| \leq R$ for all $\sigma \colon K \hookrightarrow \mathbb{C}$ (where R depends only on B, not on x). Let m_x be the minimal polynomial of x, whose roots are the $\sigma(x)$ by Corollary 1.3.9. By the expression of the coefficients in terms of the roots, we obtain a bound on the coefficients of m_x ($|a_i| \leq \binom{n}{i} R^{n-i}$ where $n = [K : \mathbb{Q}]$).

So there are finitely many possible characteristic polynomials for elements of $\Sigma(\mathbb{Z}_K) \cap B$, and each of them has at most $[K : \mathbb{Q}]$ roots. So the set $\Sigma(\mathbb{Z}_K) \cap B$ is finite. □

For K be a number field, we write W_K for the group of roots of unity in K (other notations exist, such as μ_K or $\mu_\infty(K)$).

Remark 5.3.4. We have $W_K \subset \mathbb{Z}_K^\times$. Indeed, let $\alpha \in W_K$. Then α has finite order, say n, so α is a root of $x^n - 1 \in \mathbb{Z}[x]$, so $\alpha \in \mathbb{Z}_K$. Moreover the inverse of α is also a root of unity, so $\alpha \in \mathbb{Z}_K^\times$.

Theorem 5.3.5. *Let K be a number field. Then W_K is a finite cyclic group. For all nonzero $x \in \mathbb{Z}_K$, the following are equivalent:*

(i) $x \in W_K$;

(ii) $|\sigma(x)| = 1$ *for every complex embedding σ of K;*

(iii) $|\sigma(x)| \leq 1$ *for every complex embedding* σ *of* K*.*

Proof. Let W_2 be the set of nonzero elements of $\mathbb{Z}_K$ satsifying (ii), and let W_3 be those satisfying (iii). We clearly have $W_K \subset W_2 \subset W_3$ since every complex embedding of a root of unity is of the form $\exp(ai\pi/b)$ for some $a, b \in \mathbb{Z}$. By Proposition 5.3.3, W_3 is finite, so W_K is also finite. Since every finite subgroup of the nonzero elements of a field is cyclic, W_K is cyclic.

To show that these sets are equal, let $x \in W_3$. For all integers $n \geq 0$, $x^n \in W_3$, but W_3 is finite, so some of these powers coincide, say $x^n = x^m$ with $n < m$. This gives $x^n(1 - x^{m-n})$, but $x \neq 0$ so $x^{m-n} = 1$, and x is a root of unity. □

Example 5.3.6.

- Let $K = \mathbb{Q}(i, \sqrt{2})$, and let $x = \frac{1+i}{\sqrt{2}}$. Then $x^2 = i$, so $x^4 + 1 = 0$, which proves that x is an algebraic integer. Besides, $|\sigma(x)| = 1$ for every complex embedding $\sigma\colon K \hookrightarrow \mathbb{C}$, so x is a root of unity by theorem 5.3.5. In fact, since $x^4 = -1$, we have $x^8 = 1$, so x is an 8-th root of unity. Since $x^4 \neq 1$, it is actually a *primitive* 8-th root of unity.

- Let $x = \frac{3+4i}{5} \in \mathbb{Q}(i)$. Then $|\sigma(x)| = 1$ for all embeddings of $\mathbb{Q}(i)$ into $\mathbb{C}$, but x is not a root of unity since it is not an algebraic integer.

5.3.2 Bounding the size of W_K

To begin with, we have the obvious following fact:

Proposition 5.3.7. *Let* K *be a number field. If* K *is not totally complex, then* $W_K = \{\pm 1\}$*.*

Proof. Since K is not totally complex, there exists at least one real embedding $\sigma\colon K \hookrightarrow \mathbb{R}$. If ζ be an n-th root of unity in K, then $\sigma(\zeta)$ is an n-th root of unity in $\mathbb{R}$, so $n \mid 2$. □

Example 5.3.8. If K is an odd degree number field, then $W_K = \{\pm 1\}$.

If K is totally complex, we can still bound the size of W_K by looking at degrees and ramification. Indeed, if $\zeta \in K$ is a primitive n-th root of unity, then K contains the n-th cyclotomic field $\mathbb{Q}(\zeta)$, so $\varphi(n)$ must divide $[K : \mathbb{Q}]$; besides, we can also apply the following lemma:

Lemma 5.3.9. *Let $K \subset L$ be two number fields, and let p be a prime number. If p ramifies in K then p ramifies in L.*

Proof. Let

$$p\mathbb{Z}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

be the decomposition of $p\mathbb{Z}_K$ in prime ideals of $\mathbb{Z}_K$, and let, for each i,

$$\mathfrak{p}_i \mathbb{Z}_L = \prod_{j=1}^{g_i} \mathfrak{P}_{i,j}^{e_{i,j}}$$

be the decomposition of the ideal $\mathfrak{p}_i\mathbb{Z}_L$ of $\mathbb{Z}_L$ in prime ideals of $\mathbb{Z}_L$. We have the decomposition

$$p\mathbb{Z}_L = \prod_{i=1}^{g} \left(\prod_{j=1}^{g_i} \mathfrak{P}_{i,j}^{e_{i,j}} \right)^{e_i} = \prod_{i=1}^{g} \prod_{j=1}^{g_i} \mathfrak{P}_{i,j}^{e_i e_{i,j}}.$$

In particular, if p ramifies in K, then one of the e_i is at least 2, and hence $\mathfrak{P}_{i,1}$ appears with an exponent at least 2, so p ramifies in L. $\square$

Example 5.3.10. Let $K = \mathbb{Q}(\alpha)$ where α is a root of the irreducible polynomial $P = x^4 - x + 1$. We compute that $\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(P) = 229$ is prime, so $\mathbb{Z}[\alpha]$ is maximal and the discriminant of K is $\operatorname{disc} K = 229$. Suppose that K contains a p-th root of unity for some odd prime p. Then K contains the p-th cyclotomic field, which has degree $p-1$ over $\mathbb{Q}$, so $p-1 \leq 4$ and $p \leq 5$. But K is unramified at 3 and 5, so it cannot contain the corresponding cyclotomic fields by lemma 5.3.9. Similarly, K cannot contain a 4-th root of unity since it is unramified at 2. So $W_K = \{\pm 1\}$.

Here is a last test we can perform to eliminate the possibility of some roots of unity:

Proposition 5.3.11. *Let K be a number field, let $\zeta \in K$ be a primitive n-th root of unity and let $\mathfrak{p}$ be a prime ideal such that n is coprime to $\mathfrak{p}$. Then $n \mid N(\mathfrak{p}) - 1$.*

Proof. Since ζ is a primitive n-th root of unity, it has exactly n distinct powers, which are the roots of $f(x) = x^n - 1$. We have $\operatorname{disc} f(x) = \pm n^n$ by proposition 2.3.11, so $\operatorname{disc} f(x)$ is nonzero in the quotient $\mathbb{Z}_K/\mathfrak{p}$ (since

$\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ and n is prime to p by assumption), so the roots of $f(x)$ remains distinct in $\mathbb{Z}_K/\mathfrak{p}$. Therefore, the image of $\zeta \in \mathbb{Z}_K/\mathfrak{p}$ still has multiplicative order exactly n, so that the multiplicative group $(\mathbb{Z}_K/\mathfrak{p})^\times$ contains an element of order n. By Lagrange, this implies that $n \mid \#(\mathbb{Z}_K/\mathfrak{p})^\times$. Finally, since $\mathfrak{p}$ is prime, $\mathbb{Z}_K/\mathfrak{p}$ is a field with $N(\mathfrak{p})$ elements, so $(\mathbb{Z}_K/\mathfrak{p})^\times = N(\mathfrak{p}) - 1$. □

Example 5.3.12. If 2 is unramified in K and there is a prime above 2 of residue degree 1, then $W_K = \{\pm 1\}$. Indeed, by Proposition 5.3.11 the only possible roots of unity would be ζ_{2^k}, but if $k \geq 2$ then 2 is ramified in $\mathbb{Q}(\zeta_{2^k})$, so this cyclotomic field cannot be contained in K by lemma 5.3.9.

5.4 Dirichlet's theorem

We will now describe the structure of the full unit group.

Definition 5.4.1. Let K be a number field of signature (r_1, r_2). Let $\sigma_1, \dots, \sigma_{r_1}$ be the real embeddings of K, and let $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ be representatives of the nonreal embeddings of K up to complex conjugation. For all $1 \leq i \leq r_1 + r_2$, let $n_i = 1$ if σ_i is real and $n_i = 2$ otherwise. The *logarithmic embedding*

$$\mathcal{L} \colon \mathbb{Z}_K^\times \longrightarrow \mathbb{R}^{r_1+r_2}$$

is defined by

$$\mathcal{L}(x) = \big(n_i \log|\sigma_i(x)|\big)_{i=1}^{r_1+r_2}.$$

Theorem 5.4.2 (Dirichlet)**.** *Let K be a number field of signature (r_1, r_2). Let $V \subset \mathbb{R}^{r_1+r_2}$ be the subspace of vectors whose coordinates sum to zero. Then $\mathcal{L}(\mathbb{Z}_K^\times)$ is a lattice in V. As an abstract abelian group, we have*

$$\mathbb{Z}_K^\times \cong W_K \times \mathbb{Z}^{r_1+r_2-1}.$$

Recall that every finitely generated abelian group is isomorphic to $T \times \mathbb{Z}^r$, where T is a finite group and $r \geq 0$ is an integer called the *rank*. The second part of the theorem says that the rank of the unit group of K is $r_1 + r_2 - 1$.

We will also prove this theorem after introducing "geometry of numbers" techniques.

Definition 5.4.3. Let K be a number field of signature (r_1, r_2), and let $r = r_1 + r_2 - 1$. A set of *fundamental units* of K is a $\mathbb{Z}$-basis for the unit group $\mathbb{Z}_K^\times/W_K$, that is, a set of units $\varepsilon_1, \dots, \varepsilon_r \in \mathbb{Z}_K^\times$ such that $(\mathcal{L}(\varepsilon_1), \dots, \mathcal{L}(\varepsilon_r))$

is a $\mathbb{Z}$-basis of the lattice $\mathcal{L}(\mathbb{Z}_K^\times)$. Let $M \in \mathrm{Mat}_{r+1,r}(\mathbb{R})$ be the matrix with columns $\mathcal{L}(\varepsilon_1), \dots, \mathcal{L}(\varepsilon_r)$. Let M' be a matrix obtained by deleting a row of M, which is an $r \times r$ matrix. The *regulator of* K is

$$\mathrm{Reg}_K = |\det M'|.$$

Proposition 5.4.4. *The regulator does not depend on the choice of a set of fundamental units, on the ordering of the complex embeddings, or on the choice of the deleted row.*

Proof. If we change the set of fundamental units, this amounts to multiplying M on the right by a matrix $P \in \mathrm{GL}_r(\mathbb{Z})$, and similarly M' becomes $M'P$. Since $\det P = \pm 1$, this does not change the regulator.

If we permute the rows of M' does not change its determinant up to sign, so this does not change the regulator.

Finally, since the sum of all the rows in M is zero, changing which row we delete amounts to replacing one row in M' by the negative of the sum of the rows of M'. Since the determinant is an alternating map, this does not change its value up to sign, so again this does not affect the regulator. $\square$

Example 5.4.5. Let K be a real quadratic field, which we see as a subfield of $\mathbb{R}$. By Dirichlet's theorem, the units of K have rank 1. Let ε be a fundamental unit of K. After changing ε into $\pm\varepsilon^{\pm 1}$ if necessary, we may assume that $\varepsilon > 1$. Then $\mathrm{Reg}_K = \log \varepsilon$: if σ denotes the other real embedding of K, then $\sigma(\varepsilon) = N_{\mathbb{Q}}^K(\varepsilon)/\varepsilon = \pm\varepsilon^{-1}$, so that

$$M = \begin{pmatrix} \log \varepsilon \\ \log|\pm \varepsilon^{-1}| \end{pmatrix} = \begin{pmatrix} \log \varepsilon \\ -\log \varepsilon \end{pmatrix}.$$

5.5 The case of quadratic fields

Proposition 5.5.1. *Let K be an imaginary quadratic field of discriminant* $\operatorname{disc} K$*. Then the unit group $\mathbb{Z}_K^\times$ is isomorphic to*

- $\{\pm 1\}$ *if* $\operatorname{disc} K \notin \{-3, -4\}$*;*
- $\mathbb{Z}/6\mathbb{Z}$ *if* $\operatorname{disc} K = -3$*;*
- $\mathbb{Z}/4\mathbb{Z}$ *if* $\operatorname{disc} K = -4$.

Proof. By Dirichlet's theorem we have $\mathbb{Z}_K^\times = W_K$. If $W_K = \langle \zeta_n \rangle$ with $n \geq 3$, then K contains the n-th cyclotomic field, and since K is quadratic we have $K = \mathbb{Q}(\zeta_n)$. So we need to determine the quadratic cyclotomic fields. The n-th cyclotomic field has degree $\varphi(n)$, and it is easy to see from the formula for $\varphi(n)$ that we have $\varphi(n) = 2$ if and only if $n \in \{3, 4, 6\}$. Finally $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$ has discriminant -3, and $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ has discriminant -4. □

Proposition 5.5.2. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field ($d > 0$ squarefree), seen as a subfield of $\mathbb{R}$. Then $\mathbb{Z}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$. Moreover, there exists a fundamental unit $u \in \mathbb{Z}_K^\times$ such that $u > 1$. Write $u = x + y\sqrt{d}$ with x, y integers or half-integers. Then u is characterized among the elements of $\mathbb{Z}_K^\times$ by any of the following properties:*

(i) $u > 1$ is the smallest as a real number;

(ii) $x > 0$ is the smallest possible;

(iii) $y > 0$ is the smallest possible (except for $d = 5$ where there are two units with $y = 1/2$ and the fundamental unit is the one having norm -1).

Proof. Since the signature of K is $(2, 0)$, we have $W_K = \{\pm 1\}$ by Proposition 5.3.7, and $\mathbb{Z}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$ by Dirichlet's theorem 5.4.2. If u is a fundamental unit, then $u, -u, u^{-1}, -u^{-1}$ are fundamental units and among those there is one in the interval $(1, \infty)$ since $u \neq 1$. Since every other unit in $(1, \infty)$ is of the form u^n for some $n > 0$, u is the smallest one as a real number. Let us prove that x and y are positive: we have $\pm u^{\pm 1} = \pm x \pm y\sqrt{d}$, and the choice giving the largest real value is $x, y > 0$. We now want to see that smallest u is equivalent to smallest x or y. Let $s \in \{\pm 1\}$, and consider units $x + y\sqrt{d} > 1$ of norm s, i.e. satisfying

$$x^2 - dy^2 = s, \quad x, y > 0.$$

We have $x = \sqrt{s + dy^2}$ and $y = \sqrt{\frac{x^2 - s}{d}}$, so x is an increasing function of y, y is an increasing function of x, and $x + \sqrt{d}y$ is an increasing function of x and of y. So if we sort the units of fixed norm by increasing x, y or $x + \sqrt{d}y$, the resulting ordering is the same.

- If a fundamental unit has norm 1, then every unit has norm 1 and we are done.

- If a fundamental unit u has norm -1, we need to compare it with units of norm 1 the smallest of which is u^2. But we have $(x+y\sqrt{d})^2 = (x^2+dy^2)+(2xy)\sqrt{d}$ and we have $x^2+dy^2 > x$ and $2xy > y$, unless $x = 1/2$. In order to prove the proposition, we only have to eliminate the possibility that $x = 1/2$. If that is the case, then $1 - dz^2 = \pm 4$ where $z = 2y \in \mathbb{Z}_{>0}$, so that $dz^2 = 5$ or -3. Since $dz^2 > 0$ we must have $dz^2 = 5$, so that $d = 5$. If the $d = 5$ case, there are two units with $y = 1/2$, and the unit of norm 1 is the square of the unit of norm -1.

□

Example 5.5.3.

1. $\phi = \frac{1+\sqrt{5}}{2}$ is a fundamental unit in $\mathbb{Q}(\sqrt{5})$. By Examples 5.4.5, the regulator is $\mathrm{Reg}_K = \log(\phi) \approx 0.481$.

2. Let $K = \mathbb{Q}(\sqrt{6})$, so that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{6}]$. In order to find the fundamental unit, we look for solutions of

$$x^2 - 6y^2 = \pm 1, \quad x, y \in \mathbb{Z}_{>0}.$$

   We try successive possible values for y:

   - if $y = 1$, then $x^2 = \pm 1 + 6y^2 = \pm 1 + 6 = 5$ or 7, which is impossible.
   - if $y = 2$, then $x^2 = \pm 1 + 6y^2 = \pm 1 + 24 = 23$ or 25, and $25 = 5^2$, so we found the smallest solution $(5, 2)$ and a fundamental unit $5 + 2\sqrt{6}$. The regulator of K is $\log(5 + 2\sqrt{6}) \approx 2.29$.

   We could have enumerated the values of x, but we would have had to try more values. This will be true in general, since $x \approx \sqrt{d}y$.

3. Let $K = \mathbb{Q}(\sqrt{13})$, so that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{13}}{2}$. So we need to look at solutions of $x^2 - 13y^2 = \pm 1$ with x, y positive half-integers, or equivalently for solutions of

$$X^2 - 13Y^2 = \pm 4, \quad X, Y \in \mathbb{Z}_{>0}$$

   by setting $X = 2x$, $Y = 2y$. We try values of Y:

- if $Y = 1$, then $X^2 = \pm 4 + 13Y^2 = \pm 4 + 13 = 9$ or 17, and $9 = 3^2$ so we find the smallest solution $(3, 1)$ and a fundamental unit $\varepsilon = \frac{3+\sqrt{13}}{2}$, which has norm -1. The regulator of K is $\log \varepsilon \approx 1.19$.

We need to be careful that the result $\frac{X+Y\sqrt{d}}{2}$ is an algebraic integer. But since $X^2 - dY^2 = \pm 4$ and d is odd, X and Y have the same parity so this will always work.

4. Fundamental units of real quadratic fields can be very large! For instance:

   - In $\mathbb{Q}(\sqrt{19})$, the fundamental unit is $170 + 39\sqrt{19}$;
   - In $\mathbb{Q}(\sqrt{94})$, the fundamental unit is $2143295 + 221064\sqrt{94}$;
   - In $\mathbb{Q}(\sqrt{9619})$, the fundamental unit is

$$8111902201124886039880853330204632752971143108402377064384465859022665754982415295880466304151382201 4290 +$$
$$8270994722308163637166352289743285357310230476298014517914389522478587045035412638334717098960969651 61\sqrt{9619}.$$

Remark 5.5.4. If you know what continued fractions are: it is also possible to find fundamental units of real quadratic fields by computing the continued fraction expansion of $\sqrt{d}$. This leads to an algorithm that is much faster than the one we saw here, but it is outside the scope of this course.

5.6 The Pell–Fermat equation

Let $d > 1$ be a squarefree integer. The *Pell–Fermat equation* is:

$$x^2 - dy^2 = 1, \quad x, y \in \mathbb{Z}. \tag{5.1}$$

We can immediately reinterpret it as follows: let $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$, which is an order in $K = \mathbb{Q}(\sqrt{d})$. Then the solutions of Equation (5.1) are the $(x, y) \in \mathbb{Z}^2$ such that $u = x + y\sqrt{d}$ is a solution of

$$N^K_{\mathbb{Q}}(u) = 1, \quad u \in \mathcal{O}^\times. \tag{5.2}$$

By Proposition 5.2.6, $\mathcal{O}^\times$ has finite index in $\mathbb{Z}_K^\times$, and the index of $\mathcal{O}^\times$ in $\mathbb{Z}_K^\times$ is at most $\#(\mathbb{Z}_K/f\mathbb{Z}_K)^\times$, where f is the index of $\mathcal{O}$ in $\mathbb{Z}_K$. If $f = 1$ then $\mathcal{O}^\times = \mathbb{Z}_K^\times$. If $f = 2$, then 2 is unramified in K, so $\mathbb{Z}_K/f\mathbb{Z}_K$ is isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$ or $\mathbb{F}_4$, so $\#(\mathbb{Z}_K/f\mathbb{Z}_K)^\times \leq 3$. Since $\pm 1 \in \mathcal{O}$, we have

$$\mathcal{O}^\times \cong \{\pm 1\} \times \mathbb{Z} \text{ and } [\mathcal{O}^\times : \mathbb{Z}_K^\times] \leq 3.$$

Let $\varepsilon_0 \in \mathbb{Z}_K^\times$ be a fundamental unit for $\mathbb{Z}_K^\times$. Let $n \geq 1$ be the smallest positive integer such that $\varepsilon_0^n \in \mathcal{O}$, and let $\varepsilon_1 = \varepsilon_0^n$. Then $n \leq 3$, and ε_1 is a fundamental unit for $\mathcal{O}^\times$. Let $\varepsilon_2 = \varepsilon_1^2$ if $N_{\mathbb{Q}}^K(\varepsilon_1) = -1$ and $\varepsilon_2 = \varepsilon_1$ otherwise. Then the solutions of Equation (5.2) are the $\pm\varepsilon_2^n$, $n \in \mathbb{Z}$, and the solutions of Equation (5.1) are the $\pm(x, y)$ where $x + y\sqrt{d} = \varepsilon_2^n$, $n \in \mathbb{Z}$.

Example 5.6.1. Consider the Pell–Fermat equation

$$x^2 - 13y^2 = 1, \quad x, y \in \mathbb{Z}.$$

Let $K = \mathbb{Q}(\sqrt{13})$, so that $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, and let $\mathcal{O} = \mathbb{Z}[\sqrt{13}]$. We saw in Example 5.5.3 that $\varepsilon_0 = \frac{3+\sqrt{13}}{2}$ is a fundamental unit of $\mathbb{Z}_K^\times$ and has norm -1. Since $\varepsilon_0 \notin \mathcal{O}$ and $\varepsilon_0^2 = \frac{11+3\sqrt{13}}{2} \notin \mathcal{O}$, the unit $\varepsilon_1 = \varepsilon_0^3 = 18 + 5\sqrt{13}$ is a fundamental unit of $\mathcal{O}^\times$. Since $N_{\mathbb{Q}}^K(\varepsilon_0) = -1$, we have $N_{\mathbb{Q}}^K(\varepsilon_1) = -1$, so $\varepsilon_2 = \varepsilon_1^2 = 649 + 180\sqrt{13}$ is a fundamental unit for the norm 1 subgroup of $\mathcal{O}^\times$. The solutions of that Pell–Fermat equation are the

$$(x, y) \text{ where } x + y\sqrt{13} = \pm(649 + 180\sqrt{13})^n, \; n \in \mathbb{Z}.$$

5.7 Class groups of real quadratic fields

In this example we will see how to use units to compute class groups.

Example 5.7.1. Let $K = \mathbb{Q}(\sqrt{79})$, so that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{79}]$ and the discriminant is $\operatorname{disc} K = 4 \cdot 79$. Let $\alpha = \sqrt{79}$. The signature of K is $(2, 0)$, so the Minkowski bound is $M_K = \frac{2}{4}\sqrt{\operatorname{disc} K} \approx 8.89$. The class group of K is generated by the classes of prime ideals of norm up to 8. We compute the decomposition of the small primes:

- 2 is ramified: $(2) = \mathfrak{p}_2^2$, and $[\mathfrak{p}_2]^2 = 1$.
- $79 \equiv 1 \equiv (\pm 1)^2 \bmod 3$, so 3 splits: $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ where $\mathfrak{p}_3 = (3, \alpha + 2)$ and $\mathfrak{p}_3' = (3, \alpha + 1)$, and $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$.
- $79 \equiv 4 \equiv (\pm 2)^2 \bmod 5$, so 5 splits: $(5) = \mathfrak{p}_5\mathfrak{p}_5'$ where $\mathfrak{p}_5 = (5, \alpha + 3)$ and $\mathfrak{p}_5' = (5, \alpha + 2)$, and $[\mathfrak{p}_5'] = [\mathfrak{p}_5]^{-1}$.
- $79 \equiv 2 \equiv (\pm 3)^2 \bmod 7$, so 7 splits: $(7) = \mathfrak{p}_7\mathfrak{p}_7'$ where $\mathfrak{p}_7 = (7, \alpha + 4)$ and $\mathfrak{p}_7' = (7, \alpha + 3)$, and $[\mathfrak{p}_7'] = [\mathfrak{p}_7]^{-1}$.

So $\mathrm{Cl}(K)$ is generated by the classes of $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5$ and $\mathfrak{p}_7$.

Let us compute some elements of small norm to try to get relations in the class group. The norm of a generic element $z = x + y\alpha \in \mathbb{Z}_K$ is $x^2 - 79y^2$. With $y = 1$ we try $x = 8, 9, 10$ and we get respective norms $-15, 2, 21$. Let us compute the factorisation of the corresponding elements.

- The ideal $(8+\alpha)$ has norm $15 = 3 \cdot 5$, so it is the product of a prime of norm 3 and a prime of norm 5. Since $8 + \alpha \equiv 2 + \alpha \bmod 3$ we have $\mathfrak{p}_3 \mid (8+\alpha)$. Since $8+\alpha \equiv 3+\alpha \bmod 5$ we have $\mathfrak{p}_5 \mid (8+\alpha)$. This gives $(8+\alpha) = \mathfrak{p}_3\mathfrak{p}_5$, so that $[\mathfrak{p}_5] = [\mathfrak{p}_3]^{-1}$.

- The ideal $(9+\alpha)$ has norm 2, so $(9+\alpha) = \mathfrak{p}_2$ and $[\mathfrak{p}_2] = 1$.

- The ideal $(10+\alpha)$ has norm $21 = 3 \cdot 7$, so it is the product of a prime of norm 3 and a prime of norm 7. Since $10 + \alpha \equiv 1 + \alpha \bmod 3$, we have $\mathfrak{p}'_3 \mid (10+\alpha)$. Since $10+\alpha \equiv 3+\alpha \bmod 7$, we have $\mathfrak{p}'_7 \mid (10+\alpha)$. This gives $(10+\alpha) = \mathfrak{p}'_3\mathfrak{p}'_7$, so that $[\mathfrak{p}'_3][\mathfrak{p}'_7] = 1$ and $[\mathfrak{p}_7] = [\mathfrak{p}_3]^{-1}$.

We still need to find an ideal class of finite order. After a few trials, we obtain the element $17 + 2\alpha$, which has norm $-27 = -3^3$. Since $17 + 2\alpha \equiv 2 + 2\alpha \equiv 2(1+\alpha) \bmod 3$, we have $\mathfrak{p}'_3 \mid (17+2\alpha)$ and $\mathfrak{p}_3 \nmid (17+2\alpha)$, so that $(17+2\alpha) = (\mathfrak{p}'_3)^3$. This gives $[\mathfrak{p}_3]^3 = 1$.

With this we know that $\mathrm{Cl}(K) \cong 1$ or $\mathbb{Z}/3\mathbb{Z}$, and distinguishing between these cases is equivalent to deciding whether $\mathfrak{p}_3$ is principal. If we were in an imaginary quadratic field, we could easily determine every element of norm 3. Here, because there are infinitely many units, there could be infinitely many elements of norm ± 3! However, up to multiplication by a unit, there are still finitely many. In order to determine these elements, we need to first compute a fundamental unit[2] of K. We need to find the smallest solution to

$$x^2 - 79y^2 = \pm 1, \quad x, y \in \mathbb{Z}.$$

After trying successive values of y, we find that $u = 80 + 9\sqrt{79}$ is a fundamental unit, and has norm 1.

Let us try to find an element $z = x + y\alpha$ of norm ± 3. By reducing modulo 4:

$$x^2 - 79y^2 \equiv x^2 + y^2 \bmod 4,$$

[2] Actually, any unit of infinite order would do, but using a fundamental one gives better bounds and hence saves us some work.

we see that 3 cannot be the norm of an element in $\mathbb{Z}_K$. However, we cannot rule out -3 using congruences. Suppose z has norm 3. After multiplying z by some power of u, we can assume that

$$u^{-1/2} < z < u^{1/2}.$$

Since $z = x + y\alpha$ has norm -3, we have $3/z = -x + y\alpha$. But we also have the inequality

$$3u^{-1/2} < 3/z < 3u^{1/2}.$$

Summing these inequalities we get

$$4u^{-1/2} < 2y\alpha < 4u^{1/2}, \text{ i.e. } \frac{2}{\alpha u^{1/2}} < y < \frac{2u^{1/2}}{\alpha}\cdot$$

We compute $\frac{2}{\alpha u^{1/2}} \approx 0.017$ and $\frac{2u^{1/2}}{\alpha} \approx 2.85$. So it is enough to try $y = 1$ and $y = 2$, and we easily see that none of these work. So $\mathbb{Z}_K$ does not contain any element of norm ± 3, the ideal $\mathfrak{p}_3$ is not principal, and finally

$$\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}.$$

5.8 The case of cyclotomic fields

Proposition 5.8.1. *Let $n \geq 3$ and $K = \mathbb{Q}(\zeta_n)$. Then we have*

- $W_K \cong \mathbb{Z}/(2n)\mathbb{Z}$ *if n is odd;*
- $W_K \cong \mathbb{Z}/n\mathbb{Z}$ *if n is even.*

Proof. Let $m = \#W_K$. Then the m-th cyclotomic field embeds in K, so that $\varphi(m) \leq \varphi(n)$. But $n \mid m$ since K contains the n-th roots of unity, so $\varphi(m) = \varphi(n)$. Moreover, if k is a multiple of n such that $\varphi(n) = \varphi(k)$, then K embeds in $\mathbb{Q}(\zeta_k)$ and by equality if degrees we have $K = \mathbb{Q}(\zeta_k)$ so K contains a primitive k-th root of unity. So m is the largest multiple of n such that $\varphi(m) = \varphi(n)$. But for all primes p, we have $\varphi(pk) = (p-1)\varphi(k)$ if $p \nmid k$ and $\varphi(pk) = p\varphi(k)$ if $p \mid k$. So $m = 2n$ if n is odd and $m = n$ if n is even. $\square$

Remark 5.8.2. Since the signature of $K = \mathbb{Q}(\zeta_n)$ is $(0, \varphi(n)/2)$, the rank of the unit group $\mathbb{Z}_K^\times$ is $\varphi(n)/2 - 1$.

Definition 5.8.3. Let $n \geq 3$ and $K = \mathbb{Q}(\zeta_n)$. For all divisors $d \mid n$ and for all a coprime to n we define the *cyclotomic unit*

$$u_{a,d} = \frac{\zeta_n^{ad} - 1}{\zeta_n^d - 1}.$$

Proposition 5.8.4. *Let $n \geq 3$ and let $K = \mathbb{Q}(\zeta_n)$. For all divisors $d \mid n$ and for all a coprime to n, we have $u_{a,d} \in \mathbb{Z}_K^\times$.*

Proof. Let $\zeta \in K$ be an arbitrary root of unity and $k > 0$ an integer. Then

$$\frac{\zeta^k - 1}{\zeta - 1} = \sum_{i=0}^{k-1} \zeta^k \in \mathbb{Z}_K.$$

Applying this to $\zeta = \zeta_n^d$ and $k = a$ we find that $u_{a,d} \in \mathbb{Z}_K$. Now since a is coprime to n, there exists an integer $b > 0$ such that $ab \equiv 1 \bmod n$, so that $\zeta_n^{ab} = \zeta_n$. We get

$$u_{a,d}^{-1} = \frac{\zeta_n^d - 1}{\zeta_n^{ad} - 1} = \frac{\zeta_n^{abd} - 1}{\zeta_n^{ad} - 1}.$$

Applying again the result above with $\zeta = \zeta_n^{ad}$ and $k = b$ shows that $u_{a,d}^{-1} \in \mathbb{Z}_K$, proving the proposition. □

Remark 5.8.5. Once we have proved that $u_{a,d} \in \mathbb{Z}_K$, we could also conclude by noticing that $\zeta_n^{ad} - 1$ and $\zeta_n^d - 1$ are both roots of the same irreducible polynomial $\Phi_{n/d}(x+1)$, so they have the same norm and $N_{\mathbb{Q}}^K(u_{a,d}) = 1$.

Remark 5.8.6. In the special case where n is a power of a prime $p \in N$, we know from theorem 3.10.6 that $\zeta_n - 1$ is a generator of the unique prime above p, and this is also true if we replace ζ_n by any primitive n-th root of unity. So for all a not divisible by p the element $\frac{\zeta_n^a - 1}{\zeta_n - 1}$ generates the trivial fractional ideal, which shows again that it is a unit.

Theorem 5.8.7. *Let $n \geq 3$ and let $K = \mathbb{Q}(\zeta_n)$. The group generated by the cyclotomic units $u_{a,d} \in \mathbb{Z}_K^\times$ has finite index in $\mathbb{Z}_K^\times$.*

We will not prove Theorem 5.8.7 here. A proof may be found in L. Washington's book on cyclotomic fields.

Example 5.8.8. Let $K = \mathbb{Q}(\zeta_5)$, which has degree 4, signature $(0, 2)$ and unit rank 1 by Dirichlet's theorem. Using Proposition 5.8.4, we find the cyclotomic unit $u = \frac{\zeta_5^2 - 1}{\zeta_5 - 1} = \zeta_5 + 1 \in \mathbb{Z}_K^\times$. It turns out that u is a fundamental unit for K.

Remark 5.8.9.

- It is not true that the cyclotomic units always generate the full group of units. For instance, in $K = \mathbb{Q}(\zeta_{136})$, they generate a subgroup of index 2.

- It is important not to forget the cyclotomic units $u_{a,d}$ with $d \neq 1$, even though there are exactly $\varphi(n)/2 - 1$ cyclotomic units of the form $u_{a,1}$. For instance, in $K = \mathbb{Q}(\zeta_{39})$, the cyclotomic units of the form $u_{a,1}$ generate a subgroup of rank 10, hence of infinite index in $\mathbb{Z}_K^\times$.

Chapter 6

Summary of methods and examples

6.1 Discriminant and ring of integers

In summary, to compute the ring of integers in a number field $K = \mathbb{Q}(\alpha)$ given by the minimal polynomial $P \in \mathbb{Z}[x]$ of α:

- Compute the discriminant of $\mathbb{Z}[\alpha]$, i.e. the **discriminant of** P, and find its **factorisation into prime numbers**.
- The discriminant $\operatorname{disc} K$ of K and the index f of $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K$ satisfy $\operatorname{disc}(\mathbb{Z}[\alpha]) = f^2 \operatorname{disc} K$. In particular every prime that ramifies in K must divide $\operatorname{disc}(\mathbb{Z}[\alpha])$.
- If a prime divides $\operatorname{disc}(\mathbb{Z}[\alpha])$ with **exponent** 1, then $\mathbb{Z}[\alpha]$ is p-maximal.
- If the minimal polynomial of α is **Eisenstein at** p, then $\mathbb{Z}[\alpha]$ is p-maximal.
- The order $\mathbb{Z}[\alpha]$ is often not maximal. In this case, you need to find an element $x \in \mathbb{Z}_K \setminus \mathbb{Z}[\alpha]$ and examine the larger order $\mathbb{Z}[\alpha, x]$. You are not supposed to know a general method to find x.

6.2 Factorisation

In summary, to compute factorisations in a number field $K = \mathbb{Q}(\alpha)$ given by the minimal polynomial $P \in \mathbb{Z}[x]$ of α:

- To find the decomposition of a prime number p (equivalently the factorisation of the ideal $p\mathbb{Z}_K$) when $\mathbb{Z}[\alpha]$ is maximal at p, **factor P modulo p into irreducible polynomials in $\mathbb{F}_p[x]$**, and apply Theorem 3.8.1.
- To find the factorisation of an integral ideal I, for instance of the form (β) with $\beta \in \mathbb{Z}_K$, first **compute the norm $N(I) \in \mathbb{Z}$ and factor this norm** into prime numbers.
- For each prime p dividing $N(I)$ with exponent e, find the decomposition of p into prime ideals, compute the possible products of these primes that have norm p^e, then find out which product really divides I.
- Testing whether a prime ideal $\mathfrak{p}$ divides (β) is equivalent to testing whether the image of β under the reduction modulo $\mathfrak{p}$ map $\mathbb{Z}_K \to \mathbb{Z}_K/\mathfrak{p}$ is zero.
- To compute the **reduction modulo $\mathfrak{p} = (p, \phi(\alpha))$** of an element β, when $\mathbb{Z}[\alpha]$ is p-maximal and ϕ is an irreducible factor of $P \bmod p$: write β as a polynomial in α[1]: $\beta = R(\alpha)$ for some $R \in \mathbb{Z}[x]$. Then you can obtain the reduction modulo $\mathfrak{p}$ of β by reducing every coefficient modulo p, and then dividing the resulting polynomial by ϕ in $\mathbb{F}_p[x]$.

6.3 Class group and units

We first study a number of examples of computations of class groups. The general method is to first compute the Minkowski bound for the field under consideration, then study the prime ideals up to that bound, and then study their products. We will focus mostly on quadratic fields.

Example 6.3.1. Let $K = \mathbb{Q}(i)$, so that $\mathbb{Z}_K = \mathbb{Z}[i]$ and $\operatorname{disc} K = -4$. We already know that $\mathbb{Z}_K$ is a Euclidean domain, hence a PID, but let's reprove

[1] If $\beta \notin \mathbb{Z}[\alpha]$, write $\beta = \beta'/d$ with $\beta' \in \mathbb{Z}[\alpha]$ and d coprime to p; this is always possible if $\mathbb{Z}[\alpha]$ is p-maximal. Then d has an inverse u modulo p ($du \equiv 1 \bmod p$), the reduction map sends $1/d$ to u.

it using our new methods. The Minkowski bound is $M_K \approx 1.27 < 2$, so by Corollary 4.5.4, the class group of K is trivial; in other words, $\mathbb{Z}_K$ is a PID (and hence a UFD) in this case.

Example 6.3.2. Let $K = \mathbb{Q}(\sqrt{437})$. Since 437 is squarefree and $437 \equiv 1 \bmod 4$, we have $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{437}}{2}]$ and $\operatorname{disc} K = 437$. The Minkowski bound is $M_K \approx 10.45 < 11$. By Corollary 4.5.4, $\mathrm{Cl}(K)$ is generated by the classes of the prime ideals of norm at most 10. Since $437 \equiv 5 \bmod 8$, by Theorem 3.9.3 the prime 2 is inert in K. So the only prime ideal above 2 is (2), which is principal, so it does not contribute to the class group. Since $437 \equiv 2 \bmod 3$ which is not a square, by Theorem 3.9.1 the prime 3 is inert in K. Again the prime (3) is principal. We similarly compute that 5 and 7 are inert in K. So again, the class group of K is trivial.

What you should remember from this example is that you can ignore inert primes when computing the class group.

Now let us complete the study of our examples $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{-23})$.

Example 6.3.3. Let $K = \mathbb{Q}(\sqrt{-5})$. We saw that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$ and that $\operatorname{disc} K = -20$. The Minkowski bound is $M_K \approx 2.85 < 3$. By Corollary 4.5.4, $\mathrm{Cl}(K)$ is generated by the classes of the prime ideals of norm at most 2. As we saw in Example 4.4.3, the unique ideal $\mathfrak{p}_2$ above 2 has norm 2 and is not principal, but its square is principal. We conclude that $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, our first nontrivial class group!

What you should remember from this example is that it is easy to get an upper bound on the order of totally ramified primes in the class group.

Example 6.3.4. Let $K = \mathbb{Q}(\sqrt{-23})$. We have $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ and $\operatorname{disc} K = -23$. The Minkowski bound is $M_K \approx 3.05 < 4$. The class group of K is generated by the classes of prime ideals of norm at most 3. We have seen that the prime 2 splits in K: $(2) = \mathfrak{p}_2\mathfrak{p}_2'$. This implies that $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1}$, so it suffices to consider one of them. We saw that $\mathfrak{p}_2$ and $\mathfrak{p}_2^2$ are not principal but that $\mathfrak{p}_2^3$ is. This proves that $[\mathfrak{p}_2]$ has order 3. Since $-23 \equiv 1 \bmod 3$ is a square, the prime 3 also splits in K: $(3) = \mathfrak{p}_3\mathfrak{p}_3'$, and $[\mathfrak{p}_3] = [\mathfrak{p}_3']^{-1}$. Now we can conclude by two different methods.

1. Recall that the norm of a generic element $z = x + \frac{1+\sqrt{-23}}{2}y \in \mathbb{Z}_K$ is $x^2 + xy + 6y^2$. Taking $(x, y) = (0, 1)$, we get an element $z \in \mathbb{Z}_K$ of

norm 6. We factor the ideal $(z) = \mathfrak{q}\mathfrak{q}'$ where $N(\mathfrak{q}) = 2$ and $N(\mathfrak{q}') = 3$. In the class group we have $[\mathfrak{q}'] = [\mathfrak{q}]^{-1}$, so that $[\mathfrak{p}_3]$ belongs to the group generated by $[\mathfrak{p}_2]$. This proves that $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$.

2. By Minkowski's Theorem 4.5.1, every ideal class is represented by an integral ideal of norm at most 3. The only such ideals are $\mathbb{Z}_K, \mathfrak{p}_2, \mathfrak{p}_2', \mathfrak{p}_3$, and $\mathfrak{p}_3'$, so we have $h_K \leq 5$. But we already exhibited an element $[\mathfrak{p}_2]$ of order 3 so h_K is a multiple of 3, so $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$.

What you should remember from this example is that the splitting of primes gives relations in the class group for free, and elements of small norm in $\mathbb{Z}_K$ provide the additional relations.

Example 6.3.5. Let $K = \mathbb{Q}(\sqrt{10})$. Since 10 is squarefree and $10 \equiv 2 \bmod 4$, by Theorem 2.4.2 we have $\mathbb{Z}_K = \mathbb{Z}[\sqrt{10}]$ and $\operatorname{disc} K = 40$. The Minkowski bound is $M_K \approx 3.16 < 4$. Since $2 \mid \operatorname{disc} K$, the prime 2 ramifies in K: $(2) = \mathfrak{p}_2^2$. Since $N(\mathfrak{p}_2) = 2$, if $\mathfrak{p}_2$ were principal then a generator $z = x + \sqrt{10}y \in \mathbb{Z}_K$ would have to satisfy

$$x^2 - 10y^2 = \pm 2.$$

By reducing modulo 5, we see that x would be a square root of $\pm 2 \bmod 5$. But only $0, 1$ and 4 are squares modulo 5, so z cannot exist. Hence $\mathfrak{p}_2$ is not principal, and $[\mathfrak{p}_2]$ has order 2 since $[\mathfrak{p}_2]^2 = [(2)] = 1$. Since $10 \equiv 1 \bmod 3$ is a square, the prime 3 splits in K: $(3) = \mathfrak{p}_3\mathfrak{p}_3'$. We have $[\mathfrak{p}_3] = [\mathfrak{p}_3']^{-1}$. We find another relation by looking for elements of small norm: taking $(x, y) = (2, 1)$ gives an element z of norm -6. We factor the ideal $(z) = \mathfrak{p}_2\mathfrak{p}_3''$, where $\mathfrak{p}_3''$ is a prime of norm 3, so it is either $\mathfrak{p}_3$ or $\mathfrak{p}_3'$. This gives $[\mathfrak{p}_3''] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$. Again, we can conclude by two methods.

1. By Minkowski's Theorem 4.5.1, every ideal class is represented by an integral ideal of norm at most 3. The only such ideals are $\mathbb{Z}_K, \mathfrak{p}_2, \mathfrak{p}_3$, and $\mathfrak{p}_3'$, but $[\mathfrak{p}_2]$ is the same as the class of one of the primes above 3, so $h_K \leq 3$. Since we already know an element $[\mathfrak{p}_2]$ of order 2, h_K is a multiple of 2, so $h_K = 2$ and $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

2. We have $\langle [\mathfrak{p}_3] \rangle = \langle [\mathfrak{p}_3'] \rangle = \langle [\mathfrak{p}_3''] \rangle = \langle [\mathfrak{p}_2] \rangle$. Since the class group is generated by the classes of prime ideals above 2 and 3, we obtain $\mathrm{Cl}(K) = \langle [\mathfrak{p}_2] \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

What you should remember from this example is that you can sometimes use congruences to prove that certain ideals are not principal.

In summary, to compute a class group:

- First, compute the **Minkowski bound**, and list the prime ideals up to that bound by decomposing prime integers.
- The **decomposition of primes** provides relations in $\mathrm{Cl}(K)$ for free.
- **Elements of $\mathbb{Z}_K$ of small norm** provide additional relations.
- In imaginary quadratic fields, you can test whether an ideal is principal by computing bounds on the coordinates of a possible generator.
- You can often prove that an ideal is not principal using congruences.
- In real quadratic fields, after computing a fundamental unit, you can determine all elements of $\mathbb{Z}_K$ of a given norm up to multiplication by a unit. This allows you to test whether an ideal is principal.
- Conclude using Minkowski's theorem and the group structure.

6.4 Complete examples

Here is an example of computations with a number field. It is meant to illustrate pretty much everything that has been seen in this course, and represents the upper limit of what can be done without the help of a computer so do not be alarmed by its length! Also, if you feel that you could have performed these computations by yourself (with a reasonable amount of intermediate questions) this means that you have understood algebraic number theory very well.

Example 6.4.1. Let $P(x) = x^3 + 6x + 6 \in \mathbb{Z}[x]$, and let $K = \mathbb{Q}(\alpha)$, where α is a root of $P(x)$. Since $P(x)$ is Eisenstein at 2 (and also at 3), it is irreducible over $\mathbb{Z}$ and over $\mathbb{Q}$, so K is a well-defined number field of degree $[K : \mathbb{Q}] = 3$.

In order to compute the ring of integers $\mathbb{Z}_K$ of K, let us have a look at the order $\mathcal{O} = \mathbb{Z}[\alpha]$. Its discriminant is

$$\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc} P(x) = -4.6^3 - 27.6^2$$

by theorem 2.3.13. We want it in factored form (it is more interesting this way, because we can then get information about ramification), so we factor and compute that

$$\operatorname{disc}\mathbb{Z}[\alpha] = -6^2(2^2 6 + 3^3) = -6^2 3(2^3 + 3^2) = -2^2 3^3 17.$$

Next, we know that $\operatorname{disc}\mathbb{Z}[\alpha] = f^2 \operatorname{disc} K$, where $f = [\mathbb{Z}_K : \mathbb{Z}[\alpha]] \in \mathbb{N}$ is the index of $\mathbb{Z}[\alpha]$. This tells us that $f \in \{1, 2, 3, 6\}$, so that the order $\mathbb{Z}[\alpha]$ is maximal at every prime except possibly at 2 and at 3. Besides, since the primes that ramify in K are the ones that divide $\operatorname{disc} K$, we see that the set of ramified primes is a subset of $\{2, 3, 17\}$. In fact, we can be more accurate: since $\operatorname{disc}\mathbb{Z}[\alpha]$ differs from $\operatorname{disc} K$ by a square and since the exponents of 3 and 17 in $\operatorname{disc}\mathbb{Z}[\alpha]$ are odd, both 3 and 17 do ramify in K. On the other hand, we do not know yet whether 2 ramifies (the factor 2^2 in $\operatorname{disc}\mathbb{Z}[\alpha]$ could come either from $\operatorname{disc} K$, in which case 2 would ramify, or from f^2, in which case 2 would not ramify).

To determine $\mathbb{Z}_K$, we must discover whether $\mathbb{Z}[\alpha]$ is maximal at 2 and 3 or not. In general, we have not seen how to do that, but in this particular case, our only weapon, theorem 3.7.6, applies, and tells us that since $P(x)$ is Eisenstein at 2, the order $\mathbb{Z}[\alpha]$ is maximal at 2 (i.e $2 \nmid f$), and similarly for 3. As a result, we have $f = 1$ and $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. In particular, $\operatorname{disc} K = -2^2 3^3 17$, so 2 does ramifies in K.

Let us now compute the class group of K. The signature of K is (r_1, r_2) with $r_1 + 2r_2 = [K : \mathbb{Q}] = 3$, so the only possibilities are $(3, 0)$ and $(1, 1)$. This corresponds to $P(x)$ having 3 real roots, vs. $P(x)$ having 1 real root and 1 conjugate pair of complex roots (note that in the former case, K would be totally real). To find out what the signature of K actually is, we have two possibilities: studying the function $P(x)$ to see if it has 1 or 3 real zeroes, or using the fact that the sign of $\operatorname{disc} K$ is $(-1)^{r_2}$ (proposition 2.3.14). The latter is much faster of course, and allows us to effortlessly see that the signature of K is in fact $(1, 1)$ (so in particular $P(x)$ has 1 real root and 1 conjugate pair of complex roots). As a result, the Minkowski bound for K is

$$M_K = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)^1 \sqrt{2^2 3^3 17} = 12.123\ldots,$$

which tells us that that $\operatorname{Cl}(K)$ is generated by the prime ideals above 2,3,5,7 and 11.

Let us determine these prime ideals. We are of course going to use theorem 3.8.1, which means that we will have to compute the factorisation of $P(x)$ modulo these primes. Now, a polynomial of degree 3 is irreducible over a field if and only if it has no root in this field, so a table of values of $P(x)$ at small integers will be useful[2]. Here it is:

n	-5	-4	-3	-2	-1	0	1	2	3	4	5
$P(n)$	-149	-82	-39	-14	-1	6	13	26	51	94	161

Actually, we do not really need that for $p = 2$ and 3, since we already know by theorem 3.7.6 that these primes are totally ramified in K. Indeed, for both of them we have $P(x) \equiv x^3 \bmod p$, so that

$$2\mathbb{Z}_K = (2, \alpha)^3 = \mathfrak{p}_2^3$$

and

$$3\mathbb{Z}_K = (3, \alpha)^3 = \mathfrak{p}_3^3.$$

Next, we observe that although the values of n in the table represent the whole of $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ (there is even plenty of overlap), none of the values of $P(n)$ is divisible by 5; this means that $P(x)$ has no root mod 5. It is thus is irreducible mod 5, so that 5 is inert in K, i.e.

$$5\mathbb{Z}_K = \mathfrak{p}_{5^3}$$

(here and in what follows, we denote prime ideals by $\mathfrak{p}_N, \mathfrak{p}'_N, \dots$, where N is their norm). Next, we observe that 7 divides $P(-2)$, but none of the other values of P in our table. Since the values of n in this table cover $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$, this means that -2 is the only root of $P(x)$ mod 7. In fact, we compute by Euclidean division that $P(x) \equiv (x+2)(x^2 - 2x + 3) \bmod 7$, and that the quadratic factor is irreducible over $\mathbb{F}_7$ (because it does not have any root, since it does not vanish at -2). In fact, we can save ourselves the trouble of this irreducibility check: we know that 7 does not ramify in K since it does not divide $\operatorname{disc} K$, so theorem 3.8.1 tells us that $P(x)$ is squarefree mod 7, which shows that the quadratic factor is irreducible (since its only possible root over $\mathbb{F}_7$ would be -2). Anyway, we deduce from theorem 3.8.1 that the decomposition of 7 in K is

$$7\mathbb{Z}_K = (7, \alpha + 2)(7, \alpha^2 - 2\alpha + 3) = \mathfrak{p}_7 \mathfrak{p}'_{7^2}.$$

[2] It will be even more useful when we will be looking for relations in the class group, cf. infra.

Finally, since the values of n in our table cover $\mathbb{F}_{11}$ and since none of the $P(n)$ is divisible by 11, we have that 11 is inert in K,

$$11\mathbb{Z}_K = \mathfrak{p}_{11^3}.$$

Now that we have decomposed 2, 3, 5, 7 and 11 in K, we can apply theorem 4.5.1, which tells us that $\mathrm{Cl}(K)$ is generated by the classes of $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_{5^3}, \mathfrak{p}_7, \mathfrak{p}'_{7^2}$ and $\mathfrak{p}_{11^3}$ (in fact we could throw away $\mathfrak{p}_{5^3}, \mathfrak{p}'_{7^2}$ and $\mathfrak{p}_{11^3}$ because their norms exceed the Minkowski bound, but let us pretend we failed to notice that). The above decompositions also give us for free some relations satisfied by these classes, namely

$$[\mathfrak{p}_2]^3 = [2\mathbb{Z}_K] = 1,$$

$$[\mathfrak{p}_3]^3 = [3\mathbb{Z}_K] = 1,$$
$$[\mathfrak{p}_{5^3}] = [5\mathbb{Z}_K] = 1,$$
$$[\mathfrak{p}_7].[\mathfrak{p}'_{7^2}] = [7\mathbb{Z}_K] = 1,$$
$$[\mathfrak{p}_{11^3}] = [11\mathbb{Z}_K] = 1.$$

In particular, we see that $\mathrm{Cl}(K)$ is in fact generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_7]$ only.

There must be extra relations between $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_7]$ (otherwise the class group would be infinite, which would contradict corollary 4.5.2). To find them, we look for elements of small norm. Indeed, if the only prime numbers dividing the norm of some $\beta \in \mathbb{Z}_K$ are 2,3 and 7, then theorem 3.4.4 tells us that the only prime ideals in the factorisation of the ideal (β) are $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_7$ and $\mathfrak{p}'_{7^2}$, so we have found a relation between the classes of these ideals. To find such elements β, we use our table of values of $P(x)$ again.

For instance, we see that $P(0) = 6$, which tells us that the norm of α is ± 6 (here we are using the fact that the constant term of the characteristic polynomial of a matrix is, up to sign, the determinant of this matrix), so the ideal (α) must factor as a prime of norm 2 times a prime of norm 3. As $\mathfrak{p}_2$ (resp. $\mathfrak{p}_3$) is the only prime of norm 2 (resp. 3), we therefore have

$$(\alpha) = \mathfrak{p}_2\mathfrak{p}_3.$$

Indeed, we can check (although is is not necessary of course) that

$$\mathfrak{p}_2\mathfrak{p}_3 = (2, \alpha)(3, \alpha) = (6, 3\alpha, 2\alpha, \alpha^2) = (6, \alpha, \alpha^2) = (6, \alpha),$$

and $N((\alpha)) = |N_{\mathbb{Q}}^K(\alpha)| = 6$ so $6 \in (\alpha)$ by proposition 3.4.3 (another way to see this is simply to write $6 = \alpha(-\alpha^2 - 6)$), whence $(6, \alpha) = (\alpha)$. Anyway, we have found the relation

$$[\mathfrak{p}_2][\mathfrak{p}_3] = [(\alpha)] = 1$$

in $\mathrm{Cl}(K)$.

Similarly, we see in the table that $\alpha + 2$ has norm ± 14, so $(\alpha + 2)$ factors as a prime of norm 2 times a prime of norm 7, whence

$$(\alpha + 2) = \mathfrak{p}_2\mathfrak{p}_7$$

since $\mathfrak{p}_7$ is the only prime of norm 7 (the norm of $\mathfrak{p}_7'$ being 7^2, not 7). Therefore, we have found the relation

$$[\mathfrak{p}_2][\mathfrak{p}_7] = [(\alpha + 2)] = 1.$$

(incidentally, this shows that there exists $\beta \in K^\times$ such that $\mathfrak{p}'_{7^2} = \beta\mathfrak{p}_2$, and also $\gamma \in K^\times$ such that $\mathfrak{p}_7 = \gamma\mathfrak{p}_3$. Of course, such β and γ cannot lie in $\mathbb{Z}_K$.)

As a result, $\mathrm{Cl}(K)$ is generated by the class of $\mathfrak{p}_2$ alone. As $[\mathfrak{p}_2]^3 = 1$, we have two possibilities; either $[\mathfrak{p}_2] = 1$ (i.e $\mathfrak{p}_2$ is principal), and then $\mathrm{Cl}(K)$ is trivial, or $[\mathfrak{p}_2] \neq 1$ (i.e $\mathfrak{p}_2$ is not principal), and then $\mathrm{Cl}(K) \simeq \mathbb{Z}/3\mathbb{Z}$.

We are going to prove that $\mathfrak{p}_2$ is actually not principal. A possibility for this would be to write down the norm of a generic element of $\mathbb{Z}_K$ in terms of $[K : \mathbb{Q}]$ indeterminates, and prove that this norm can never be ± 2. However, this would lead to a horrible homogeneous expression of degree 3 in 3 variables, so this approach would be very tedious, if not intractable. We thus need another method.

If $\mathfrak{p}_2$ were principal, say $\mathfrak{p}_2 = (\beta)$ for some $\beta \in \mathbb{Z}_K$, then we would have $(2) = \mathfrak{p}_2^3 = (\beta^3)$, so that $v = \beta^3/2$ would be a unit. If we could prove that, for all $v \in \mathbb{Z}_K^\times$, the equation $\beta^3 = 2v$ has no solution $\beta \in K$, then we could conclude that $\mathfrak{p}_2$ is not principal. Unfortunately, this means considering infinitely many cases : indeed, the rank of $\mathbb{Z}_K^\times$ is 1 according to Dirichlet's theorem 5.4.2, so $\mathbb{Z}_K^\times$ is infinite. To be precise, the only roots of unity in K are ± 1 since K is not totally complex, so $\mathbb{Z}_K^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

However, we see that $\mathbb{Z}_K^\times/(\mathbb{Z}_K^\times)^3 \simeq \frac{\mathbb{Z}/2\mathbb{Z}}{3(\mathbb{Z}/2\mathbb{Z})} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \simeq \mathbb{Z}/3\mathbb{Z}$, so if u is any unit which is not the cube of a unit, then its image in $\mathbb{Z}_K^\times/(\mathbb{Z}_K^\times)^3$ generates this quotient, so every unit is of the form $u^i w^3$ for some $w \in \mathbb{Z}_K^\times$ and some unique $i \in \{0, 1, 2\}$. Thus, if $\mathfrak{p}_2$ were principal, we could write $\beta^3 = 2v = 2u^i w^3$, whence $2u^i = (\beta w^{-1})^3$ so either 2, $2u$ or $2u^2$ would be a cube in $\mathbb{Z}_K$. We are going to prove that none of these three possibilities can occur. Note how we are led to studying the units of K in order to reduce the study of its class group from infinitely many cases to finitely many cases.

We need to find a unit u which is not the cube of a unit. In the table of values of $P(x)$, we spot that $P(-1) = -1$, which shows that $u = \alpha + 1$ is a unit. To prove that it is not the cube of a unit, we have two possibilities: reduce u modulo a prime ideal and prove that it is not a cube in the quotient, or write u in terms of a fundamental unit of K.

As an example of the first method, we can try to prove that the image of u mod $\mathfrak{p}_7$ is not a cube in $\mathbb{Z}_K/\mathfrak{p}_7 \simeq \mathbb{F}_7$ (we have skipped $\mathfrak{p}_2$ and $\mathfrak{p}_3$ because everybody is a cube in $\mathbb{F}_2$ and in $\mathbb{F}_3$, and we have skipped $\mathfrak{p}_{5^3}$ because we prefer to stay away from[3] $\mathbb{F}_{5^3}$). Unfortunately, $\alpha+2 \in \mathfrak{p}_7$, so α reduces to -2 mod $\mathfrak{p}_7$, so $u = \alpha + 1$ reduces mod $\mathfrak{p}_7$ to -1 which is a cube in $\mathbb{Z}_K/\mathfrak{p}_7 \simeq \mathbb{F}_7$, so we cannot conclude anything. Let us try another prime. We do not want to work in $\mathbb{F}_{7^2}$ nor in $\mathbb{F}_{11^3}$, so let us try to find a new prime of inertial degree 1. We see in the table that $P(-3)$, $P(1)$ and $P(2)$ are all divisible by 13, which means that $P(x) \equiv (x+3)(x-1)(x-2)$ mod 13. As a result, 13 splits completely,

$$13\mathbb{Z}_K = (13, \alpha + 3)(13, \alpha - 1)(13, \alpha - 2) = \mathfrak{p}_{13}\mathfrak{p}'_{13}\mathfrak{p}''_{13}.$$

The image of α modulo these primes is -3, 1 and 2 respectively, so the image of u is -2, 2 and 3 respectively. This time, we are in luck: -2 is not a cube in $\mathbb{F}_{13}$, so u is not a cube in $\mathbb{Z}_K$. (In fact, neither -2 nor 2 nor 3 are cubes in $\mathbb{F}_{13}$, so we have three distinct proofs of the fact that u is not a cube).

As a example of the second method, we can use the method from assignment 5 to prove that u is actually a fundamental unit of K; in particular, it is not a cube (nor a square, nor a fifth power, ...).

Anyway, we now have that if $\mathfrak{p}_2$ were principal, then either 2, $2u$ or $2u^2$ would be a cube in $\mathbb{Z}_K$. But we have already seen that $u \equiv -1$ mod $\mathfrak{p}_7$, so 2, $2u$ and $2u^2$ reduce to 2, -2 and 2 mod $\mathfrak{p}_7$. But neither 2 nor -2 is a cube in $\mathbb{F}_7$, so we finally conclude that $\mathfrak{p}_2$ is not principal, and that $\mathrm{Cl}(K) \simeq \mathbb{Z}/3\mathbb{Z}$ is a cyclic group of order 3 generated by $[\mathfrak{p}_2]$. Phew!

[3] Actually it is not so hard to work in $\mathbb{F}_{5^3}$, it is even pretty easy; but I don't want to scare you!

Example 6.4.2. Here is another example with almost the same polynomial, to show how delicate an invariant the class group is, and also to illustrate more how to play with units.

Let $P(x) = x^3 - 6x + 6 \in \mathbb{Z}[x]$, and let $K = \mathbb{Q}(\alpha)$, where α is a root of $P(x)$.

Just as in the previous example, we find that $P(x)$ is irreducible over $\mathbb{Q}$ because it is Eisenstein at 2 (and also at 3), so K is a well-defined number field. We compute that $\operatorname{disc} P(x) = -2^2 3^3$, and since $P(x)$ is Eisenstein at 2 and 3, we again conclude that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ and $\operatorname{disc} K = -2^2 3^3$.

Besides, the sign of $\operatorname{disc} K$ shows that the signature of K is again $(1,1)$, so the Minkowski bound has the same shape as before. But this time the discriminant is much smaller, so the Minkowski bound is

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)^1 \sqrt{2^2 3^3} = 2.94\ldots$$

only. This means that $\operatorname{Cl}(K)$ is generated by the primes above 2 only. But we know by Eisenstein's criterion 3.7.6 that 2 is totally ramified in K,

$$2\mathbb{Z}_K = \mathfrak{p}_2^3,$$

so $\operatorname{Cl}(K)$ is cyclic and generated by the class of $\mathfrak{p}_2$. If we make a table of values of $P(x)$ at small integers, we spot that $P(2) = 2$, which tells us that $N_{\mathbb{Q}}^K(\alpha - 2) = \pm 2$, so that the norm of the ideal $(\alpha - 2)$ is 2 by proposition 3.4.3. Since $\mathfrak{p}_2$ is the only prime of norm 2, this means that $\mathfrak{p}_2 = (\alpha - 2)$. In particular, $\mathfrak{p}_2$ is principal, so the class group of K is trivial, i.e. $\mathbb{Z}_K$ is a PID this time.

The relation $\mathfrak{p}_2 = (\alpha - 2)$ also tells us that $(2) = ((\alpha - 2)^3)$, so $u = \frac{(\alpha-2)^3}{2} = -3\alpha^2 + 9\alpha - 7$ is a unit. As in the previous example, we have $\mathbb{Z}_K^\times = \{\pm\varepsilon^n,\ n \in \mathbb{Z}\}$ for some fundamental unit ε, so could our unit u be a fundamental unit (i.e. one of $\pm\varepsilon^{\pm 1}$)? Let $\sigma \colon K \hookrightarrow \mathbb{R}$ be the unique real embedding of K in $\mathbb{R}$. The real root of $P(x)$ is $-2.85\cdots = \sigma(\alpha)$, so the image of $\sigma(u) = -56.95\ldots$, whereas the method from assignment sheet 5 merely tells us that there exists a fundamental unit ε of K such that $\sigma(\varepsilon) > 2.76\ldots$. Therefore, all that we can say is that $u = -\varepsilon^n$ for some $n \in \{1, 2, 3\}$. In fact, $56.95\ldots$ is so much larger than $2.76\ldots$ that we can legitimately suspect that our unit u is in fact **not** a fundamental unit.

Actually, if we have made a table of values of $P(x)$, we spot that $P(1) = 1$, which means that $N_{\mathbb{Q}}^K(\alpha - 1) = \pm 1$, so that $u' = \alpha - 1$ is also a unit. But

$\sigma(u') = -3.85\ldots$, so we must have $u' = -\varepsilon$, so u' is also a fundamental unit. This confirms our doubts: since $u \neq \pm\varepsilon^{\pm 1}$ (this is obvious under σ), u is not a fundamental unit. In fact, by computing the powers of u', we find that $u = u'^3 = -\varepsilon^3$.

But this means that $2 = \left(\frac{\alpha-2}{u'}\right)^3 = (\alpha^2+\alpha-4)^3$ is a cube in K, i.e. that K contains a subfield isomorphic to $\mathbb{Q}(\sqrt[3]{2})$. Actually, we have $[K:\mathbb{Q}] = 3 = [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$ (because x^3-2, being Eisenstein at 2, is irreducible over $\mathbb{Q}$), so that K is in fact isomorphic to $\mathbb{Q}(\sqrt[3]{2})$, an isomorphism being given explicitly by

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2}) & \xrightarrow{\sim} & K \\ \sum_{j=0}^{2} \lambda_j (\sqrt[3]{2})^j & \longmapsto & \sum_{j=0}^{2} \lambda_j \beta^j \end{array}$$

where $\beta = \alpha^2+\alpha-4$ and the λ_j lie in $\mathbb{Q}$.

If we want, we can compute the reverse isomorphism; this amounts to expressing α in terms of β (which must be possible because the above description of the isomorphism implies that β is a primitive element of K). In general, this kind of rewriting process can be done by computing the powers of β as polynomials in α, and by performing linear algebra over $\mathbb{Q}$. For example, in our case, we know that α must be a polynomial in β of degree at most 2 (since we are in a field of degree 3), so we compute that $\beta^2 = -\alpha^2 - 2\alpha + 4$, and we try to write α as a linear combination of 1, β and β^2. We find that $\alpha = -\beta^2 - \beta$, which means that the reverse isomorphism is

$$\begin{array}{ccc} K & \xrightarrow{\sim} & \mathbb{Q}(\sqrt[3]{2}) \\ \sum_{j=0}^{2} \lambda_j \alpha^j & \longmapsto & \sum_{j=0}^{2} \lambda_j (-\sqrt[3]{2}^2 - \sqrt[3]{2})^j. \end{array}$$

By looking at the image of $\varepsilon = 1-\alpha$ under this isomorphism, we can infer that $\sqrt[3]{2}^2 + \sqrt[3]{2} + 1$ is a fundamental unit in $\mathbb{Q}(\sqrt[3]{2})$, so that

$$\operatorname{Regulator}(K) = \operatorname{Regulator}\big(\mathbb{Q}(\sqrt[3]{2})\big) = \log(\sqrt[3]{2}^2 + \sqrt[3]{2} + 1) = 1.347\cdots.$$

Chapter 7

Geometry of numbers

This chapter is not examinable.

7.1 Lattices

Definition 7.1.1. Let G be an abelian group, and $g_1, \cdots, g_r$ in G. We say that $(g_1, \cdot, g_r)$ is a *basis* of G if every element of g can be written *uniquely* as $\sum_{i=1}^{r} n_i g_i$ with $n_i \in \mathbb{Z}$.

Remark 7.1.2. Most abelian groups do not have a basis. Indeed, a group having a basis with r elements is by definition isomorphic to $\mathbb{Z}^r$.

Proposition 7.1.3. *Let $n \geq 1$, V a real vector space of dimension n and let $L \subset V$ be a subgroup. The following are equivalent:*

(i) There exists a $\mathbb{Z}$-basis $b_1, \ldots, b_r$ of L with $(b_1, \ldots, b_r)$ linearly independent over $\mathbb{R}$;

(ii) L is discrete;

(iii) For all compact subsets $K \subset V$, the intersection $K \cap L$ is finite.

Proof.

- (i) $\Rightarrow$ (ii): Let $y_m = \sum_{i=1}^{r} x_i^{(m)} b_i$ be a sequence in L ($x_i^{(m)} \in \mathbb{Z}$), and assume that it has a limit: $y_m \to_{m\to\infty} y \in L$. Since (b_i) are linearly independent, each $(x_i^{(m)})_m$ converges, as $m \to \infty$, to some $x_i \in \mathbb{R}$. But since $x_i^{(m)} \in \mathbb{Z}$, the sequences $(x_i^{(m)})_m$ are eventually constant, so y_m is eventually constant. Hence L is discrete.

- (ii) $\Rightarrow$ (iii): $K \cap L$ is compact and discrete, hence finite.
- (iii) $\Rightarrow$ (i): Let $X = \{b_1, \ldots, b_r\}$ be a maximal $\mathbb{R}$-linearly independent subset of L (it is finite since V has finite dimension n). Let $L' = \{\sum_i x_i b_i \colon x_i \in \mathbb{Z}\}$ be the group generated by X. We will first prove that L' has finite index in L. Let $K = \{\sum_i x_i b_i \colon x_i \in [0,1]\}$, which is compact. Then $K \cap L$ is finite, say of cardinality M, so let $d = M!$.

  Now let $x \in L$ be arbitrary. We can write $x = \sum_i x_i b_i$ where $x_i \in \mathbb{R}$. For all $m \geq 1$, define $y_m = \sum_i (m x_i - \lfloor m x_i \rfloor) b_i$, which belongs to K. Since $mx \in L$ and $\sum_i \lfloor m x_i \rfloor b_i \in L' \subset L$, we have $y_m \in L$. Since $M = \# K \cap L$, as m ranges over $0, \ldots, M$, some of the y_m must coincide, say

  $$y_{m_1} = y_{m_2}.$$

  For all i we then have

  $$m_1 x_i - \lfloor m_1 x_i \rfloor = m_2 x_i - \lfloor m_2 x_i \rfloor,$$

  which we rewrite as

  $$x_i = \frac{\lfloor m_1 x_i \rfloor - \lfloor m_2 x_i \rfloor}{m_1 - m_2} \in \frac{1}{d}\mathbb{Z},$$

  since $|m_1 - m_2| \leq M$. We have proved that

  $$L' \subset L \subset \frac{1}{d} L',$$

  so that L' has finite index in L. Now by construction, L' has a $\mathbb{Z}$-basis that is $\mathbb{R}$-linearly independent, and since it has finite index in L we can obtain a $\mathbb{Z}$-basis of L by multiplying the $\mathbb{Z}$-basis of L' by a matrix with nonzero determinant, so that $\mathbb{Z}$-basis is also linearly independent over $\mathbb{R}$.

$\square$

Remark 7.1.4. We must have $r \leq n$: a linearly independent set in V can have at most n elements.

Example 7.1.5.

- $L = \mathbb{Z}(1,2) + \mathbb{Z}(\pi, 0) \subset \mathbb{R}^2$ satisfies the conditions of Proposition 7.1.3.
- $L = \mathbb{Z} + \mathbb{Z}\sqrt{2} \subset \mathbb{R}$ does not satisfy the conditions of Proposition 7.1.3.

Proposition 7.1.6. *Let $n \geq 1$, V a real vector space of dimension n, let $L \subset V$ be a subgroup satisfying the equivalent conditions of Proposition 7.1.3, and let $b_1, \ldots, b_r$ be a $\mathbb{Z}$-basis of L. The following are equivalent:*

(i) $r = n$*;*

(ii) There exists a compact subset $K \subset V$ such that for all $x \in V$, there exists $y \in L$ such that $x - y \in K$.

Proof.

- (i) $\Rightarrow$ (ii): Let $K = \{\sum_{i=1}^n x_i b_i, x_i \in [0,1]\}$. Let $x \in V$, and write $x = \sum_{i=1}^n x_i b_i$ with $x_i \in \mathbb{R}$. Let $y = \sum_{i=1}^n \lfloor x_i \rfloor b_i \in \mathbb{Z}$. Then $x - y = \sum_{i=1}^n (x_i - \lfloor x_i \rfloor) b_i \in K$.
- (ii) $\Rightarrow$ (i): Let $W \subset V$ be the real vector space generated by L. Since $b_1, \ldots, b_r$ is a basis of W, we want to prove that $W = V$. Let $x \in V$. For all $m \geq 1$, $mx \in V$, so there exists $y_m \in L$ and $k_m \in K$ such that $mx = y_m + k_m$. We write this as

  $$x = \frac{y_m}{m} + \frac{k_m}{m}.$$

  Since K is compact, $k_m/m \to 0$ when $m \to \infty$. Since $y_m/m = x - k_m/m$, $y_m/m \to x$ when $m \to \infty$. But $y_m/m \in W$ and W is closed, so x belongs to W. This proves that $V = W$, so that $r = n$.

□

Remark 7.1.7. A subgroup $L \subset V$ satisfying the properties of Propositions 7.1.3 and 7.1.6 is a *lattice*.

Example 7.1.8.

- $L = (1, \sqrt{2})\mathbb{Z} + (\sqrt{3}, 0)\mathbb{Z} \subset \mathbb{R}^2$ is a lattice.
- $L = (1,2)\mathbb{Z} + (\pi, 2\pi)\mathbb{Z} \subset \mathbb{R}^2$ is not a lattice.
- $L = (1,-1)\mathbb{Z} \subset \mathbb{R}^2$ is not a lattice in $\mathbb{R}^2$, but it is a lattice in $V = \{(x,y) \in \mathbb{R}^2 \mid x + y = 0\}$.

7.2 Volumes

We will admit[1] that there is a good notion of "volume" of subsets of $\mathbb{R}^n$, such that the volume of the unit cube $[0,1]^n \subset \mathbb{R}^n$ is 1, and such that any linear map $f\colon \mathbb{R}^n \to \mathbb{R}^n$ multiplies volumes by $|\det f|$.

Definition 7.2.1. Let $n \geq 1$, $V = \mathbb{R}^n$ and L be a lattice in V. If $b_1, \ldots, b_n$ is a $\mathbb{Z}$-basis of L, the set

$$K = \Big\{ \sum_{i=1}^n x_i b_i \mid x_i \in [0,1] \Big\}$$

is called a *fundamental parallelotope* of L. The *covolume* $\operatorname{covol}(L)$ *of* L is defined to be the volume of K.

Proposition 7.2.2. *Let $n \geq 1$, $V = \mathbb{R}^n$ and L be a lattice in V. Let $b_1, \ldots, b_n$ be a $\mathbb{Z}$-basis of L, let A be the matrix with columns (b_i), and let G be the matrix with (i,j)-th coefficient $\langle b_i, b_j \rangle$, where $\langle \cdot, \cdot \rangle$ denotes the standard inner product on $\mathbb{R}^n$. Then*

$$\operatorname{covol}(L) = |\det A| = (\det G)^{1/2}.$$

In particular, the covolume of L does not depend on the choice of a $\mathbb{Z}$-basis.

Proof. Let $C = [0,1]^n$ be the unit cube and let K be the fundamental parallelotope corresponding to the basis (b_i). Let $f : \mathbb{R}^n \to \mathbb{R}^n$ be the linear map sending the element e_i of the standard basis of $\mathbb{R}^n$ to b_i. Then A is the matrix of f, so $|\det A| = |\det f|$. Moreover, $K = f(C)$, so the volume of K is $|\det A|$ times the volume of C, which is 1.

The matrix G is exactly ${}^{\mathrm{t}}AA$, so $\det G = (\det A)^2$.

If we change the $\mathbb{Z}$-basis, we replace A with AP where $P \in \mathrm{GL}_n(\mathbb{Z})$, so $\det P = \pm 1$ and the covolume does not change. □

Corollary 7.2.3. *Let $L' \subset L$ be lattices in $\mathbb{R}^n$. Then L' has finite index in L, and*

$$\operatorname{covol}(L') = [L\colon L'] \operatorname{covol}(L).$$

Proof. We can obtain a basis of L' from a basis of L by multiplying it on the right by a matrix, whose determinant is $[L\colon L']$ by theorem 2.2.4. □

[1] This is done properly by using the Lebesgue measure on $\mathbb{R}^n$, but you do not need to know measure theory to understand what follows.

7.3 Minkowski's theorem on lattices

Lemma 7.3.1 (Blichfeldt)**.** *Let $L \subset \mathbb{R}^n$ be a lattice and let S be a subset*[2] *such that*

$$\mathrm{vol}(S) > \mathrm{covol}(L).$$

Then there exists distinct elements $x, y \in S$ such that $x - y \in L$.

Proof. Let (b_i) be a $\mathbb{Z}$-basis of L and $K = \{\sum_i x_i b_i, x_i \in [0,1]\}$ be the corresponding fundamental parallelotope. Let $f : \mathbb{R}^n \to K$ be the map defined by $f(\sum_i x_i b_i) = \sum_i (x_i - \lfloor x_i \rfloor) b_i$. By construction, for all $x \in \mathbb{R}^n$ we have $f(x) - x \in L$.

Now assume that the restriction of f to S is injective. The since f is a piecewise translation, $\mathrm{vol}(f(S)) = \mathrm{vol}(S)$, so $\mathrm{vol}(f(S)) > \mathrm{vol}(K)$. But $f(S) \subset K$, so that is impossible.

So f is not injective: there exists distinct elements $x, y \in S$ such that $f(x) = f(y)$. But then $x - y = x - f(x) + f(y) - y \in L$. □

Definition 7.3.2. A subset $S \subset \mathbb{R}^n$ is called

- *convex* if for all $x, y \in S$, the line segment $[x, y]$ is contained in S, i.e. for all $t \in [0,1]$, $tx + (1-t)y \in S$.
- *symmetric* if for all $x \in S$, we have $-x \in S$.

Remark 7.3.3. A nonempty convex symmetric subset always contains $0 = \frac{1}{2}x + \frac{1}{2}(-x)$.

Theorem 7.3.4 (Minkowski)**.** *Let $L \subset \mathbb{R}^n$ be a lattice, and let S be a convex symmetric subset such that*

$$\mathrm{vol}(S) > 2^n \,\mathrm{covol}(L).$$

Then there exists a nonzero vector $v \in S \cap L$.

Proof. Let $S' = \frac{1}{2}S$, which has volume $\mathrm{vol}(S)/2^n > \mathrm{covol}(L)$. By Blichfeldt's Lemma 7.3.1, there exists distinct elements $x, y \in S'$ such that $v = x - y \in L$. But $v = \frac{2x + (-2y)}{2}$, and $2x$ and $2y$ are in S, so $v \in S$. □

[2]The correct hypothesis on S is that it is Lebesgue-measurable.

Corollary 7.3.5. *Let $L \subset \mathbb{R}^n$ be a lattice, and let S be a compact convex symmetric subset such that*

$$\mathrm{vol}(S) \geq 2^n \,\mathrm{covol}(L).$$

Then there exists a nonzero vector $v \in S \cap L$.

Proof. For all $m \geq 1$, let $S_m = (1 + 1/m)S$, which has volume strictly greater than $\mathrm{covol}(L)$. By Minkowski's Theorem 7.3.4, there exists nonzero vectors $v_m \in S_m \cap L$. Write $v_m = (1 + 1/m)s_m$ with $s_m \in S$. Since S is compact, there exists a subsequence $s_{\phi(m)}$ which converges to an element $s \in S$. But then $v_{\phi(m)} = (1 + 1/\phi(m))s_{\phi(m)}$ also converges to $s \in S$. Every $v_{\phi(m)}$ is in $L \setminus \{0\}$, which is closed, so the limit s is also a nonzero element of L. $\square$

Remark 7.3.6. The corollary is false without the compactness hypothesis: take $L = \mathbb{Z}^2 \subset \mathbb{R}^2$ and S the open square centred at the origin and with sides of length 2.

7.4 Applications to number theory

7.4.1 Minkowski's theorem on the class group

Proposition 7.4.1. *Let K be a number field of signature (r_1, r_2) and let $\Sigma : K \hookrightarrow K_{\mathbb{R}} \cong \mathbb{R}^{r_1+2r_2}$ be the Minkowski embedding of K. Let $\mathcal{O}$ be an order in K and let $L = \Sigma(\mathcal{O})$. Then L is a lattice in $K_{\mathbb{R}}$ and*

$$\mathrm{covol}(L) = 2^{-r_2} |\,\mathrm{disc}(\mathcal{O})|^{1/2}.$$

Proof. Since $\mathcal{O}$ has rank $n = r_1 + 2r_2$, proposition proposition 5.3.3 implies that L is a lattice in $K_{\mathbb{R}}$. Let $b_1, \ldots, b_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}$, so that by definition we have $\mathrm{disc}(\mathcal{O}) = \det\big(\mathrm{Tr}^K_{\mathbb{Q}}(b_i b_j)\big)$. Let $\sigma_1, \ldots, \sigma_{r_1+r_2}$ be representatives of the complex embeddings of K up to conjugacy. For $1 \leq k \leq r_1 + r_2$, let $n_k = 1$ if σ_k is real and $n_k = 2$ otherwise. By Corollary 1.3.9 we have

$$\mathrm{Tr}^K_{\mathbb{Q}}(b_i b_j) = \sum_k n_k \,\mathrm{Re}(\sigma_k(b_i)\sigma_k(b_j)).$$

We want to relate this to

$$\langle \Sigma(b_i), \Sigma(b_j) \rangle = \sum_k \mathrm{Re}(\sigma_k(b_i)\overline{\sigma_k(b_j)}).$$

Let $C : K_{\mathbb{R}} \to K_{\mathbb{R}}$ be the linear map defined by $C(x)_k = n_k \overline{x_k}$ for all $1 \leq k \leq r_1 + r_2$. Then $|\det C| = 2^{r_2}$, and we have

$$\mathrm{Tr}^K_{\mathbb{Q}}(b_i b_j) = \langle \Sigma(b_i), C(\Sigma(b_j)) \rangle,$$

so that by Proposition 7.2.2, we have

$$|\operatorname{disc}(\mathcal{O})| = |\det C| \operatorname{covol}(L) = 2^{r_2} \operatorname{covol}(L).$$

□

Corollary 7.4.2. *Let K be a number field of signature (r_1, r_2) and discriminant $\operatorname{disc} K$ and let $\Sigma : K \hookrightarrow K_{\mathbb{R}} \cong \mathbb{R}^{r_1+2r_2}$ be the Minkowski embedding of K. Let $\mathfrak{a}$ be a fractional ideal in K and let $L = \Sigma(\mathfrak{a})$. Then L is a lattice in $K_{\mathbb{R}}$ and*

$$\operatorname{covol}(L) = 2^{-r_2} |\operatorname{disc} K|^{1/2} N(\mathfrak{a}).$$

Proof. Since for all $a \in \mathbb{Q}$ we have $N(a\mathfrak{a}) = a^n N(\mathfrak{a})$ and $\operatorname{covol}(aL) = a^n \operatorname{covol}(L)$, it is enough to prove it for integral ideals. If $\mathfrak{a}$ is an integral ideal then $N(\mathfrak{a}) = [\mathbb{Z}_K : \mathfrak{a}]$, so the result follows from Corollary 7.2.3 and Proposition 7.4.1. □

Lemma 7.4.3. *Let $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2}$, and let*

$$S_t = \left\{ ((x_i)_i, (z_j)_j) \in V \;\middle|\; \sum |x_i| + 2 \sum |z_j| \leq t \right\}.$$

Then

$$\operatorname{vol}(S_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

Proof. Omitted. □

We now prove Minkowski's theorem of the class group, which we restate here for convenience.

Theorem 7.4.4 (Minkowski)**.** *Let K be a number field of signature (r_1, r_2) and degree $n = r_1 + 2r_2$. Let*

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\operatorname{disc} K|}.$$

Then every ideal class is represented by an integral ideal of norm at most M_K.

Proof. Let Σ be the Minkowski embedding of K, let $\mathfrak{a}$ be a fractional ideal of K and let $L = \Sigma(\mathfrak{a}^{-1})$. Let $t > 0$ be such that

$$\operatorname{vol}(S_t) = 2^{n-r_2}|\operatorname{disc} K|^{1/2} N(\mathfrak{a}^{-1}) = 2^n \operatorname{covol}(L),$$

which we can rewrite as

$$t^n = n! \left(\frac{4}{\pi}\right)^{r_2} |\operatorname{disc} K|^{1/2} N(\mathfrak{a})^{-1}.$$

By Minkowski's theorem on lattices (Corollary 7.3.5) there exists a nonzero vector $l \in S_t \cap L$, which we write $l = \Sigma(\beta)$ with $\beta \in \mathfrak{a}^{-1}$ nonzero.

By definition of S_t we have

$$\sum_{\sigma} |\sigma(x)| \leq t,$$

so by the inequality of arithmetic and geometric means we have

$$|N_{\mathbb{Q}}^K(\beta)| = \prod_{\sigma} |\sigma(x)| \leq \left(\frac{t}{n}\right)^n = \frac{t^n}{n^n}.$$

Let $\mathfrak{b} = \beta\mathfrak{a}$, which is a fractional ideal in the same ideal class as $\mathfrak{a}$. Since $\beta \in \mathfrak{a}^{-1}$, we have $\mathfrak{b} = \beta a \subset \mathfrak{a}\mathfrak{a}^{-1} = \mathbb{Z}_K$, so J is an integral ideal. In addition we have

$$N(J) = |N_{\mathbb{Q}}^K(x)| N(\mathfrak{a}) \leq \frac{t^n}{n^n} N(\mathfrak{a}) = M_K,$$

which proves the theorem. □

7.4.2 Dirichlet's theorem on units

Definition 7.4.5. Let K be a number field of signature (r_1, r_2). Recall that $K_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. We endow $K_{\mathbb{R}}$ with the structure of a ring by coordinatewise operations. For all $x \in K_{\mathbb{R}}$, multiplication by x induces an $\mathbb{R}$-linear endomorphism of $K_{\mathbb{R}}$, denoted by

$$\begin{aligned} \mu_x \colon K_{\mathbb{R}} &\longrightarrow K_{\mathbb{R}} \\ y &\longmapsto xy. \end{aligned}$$

We define $N_{\mathbb{R}}^{K_{\mathbb{R}}}(x) = \det(\mu_x)$.

Lemma 7.4.6. *With notations as in Definition 7.4.5, let* $x = ((x_i), (z_j)) \in K_{\mathbb{R}}$. *Then*

$$N_{\mathbb{R}}^{K_{\mathbb{R}}}(x) = \prod_i x_i \times \prod_j |z_j|^2.$$

In particular, for all $\alpha \in K$, *we have* $N_{\mathbb{Q}}^K(\alpha) = N_{\mathbb{R}}^{K_{\mathbb{R}}}(\Sigma(\alpha))$.

Proof. It suffices to prove it on each $\mathbb{R}$ or $\mathbb{C}$ factor. For $x \in \mathbb{R}$, μ_x is the 1×1 matrix (x). For $z = x + iy \in \mathbb{C}$, on the basis $(1, i)$ the matrix of the endomorphism μ_z is $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$, which has determinant $x^2 + y^2 = |z|^2$ (compare with theorem 1.3.7). The second claim is a restatement of Corollary 1.3.9. □

We now prove Dirichlet's theorem, which we restate here for convenience.

Theorem 7.4.7 (Dirichlet)**.** *Let* K *be a number field of signature* (r_1, r_2). *Let* $V \subset \mathbb{R}^{r_1+r_2}$ *be the hyperplane of vectors whose coordinates sum to zero. Then* $\mathcal{L}(\mathbb{Z}_K^\times)$ *is a lattice in* V. *As an abstract abelian group, we have*

$$\mathbb{Z}_K^\times \cong W_K \times \mathbb{Z}^{r_1+r_2-1}.$$

Proof. We first prove that $L = \mathcal{L}(\mathbb{Z}_K^\times)$ is a subgroup of V: this follows from the fact that every unit has norm ± 1 (Proposition 5.2.2) and Corollary 1.3.9.

To prove that L is a lattice in V, we will prove that

a) $L \cap B$ is finite for all compact subsets $B \subset V$, and

b) there exists a compact subset $C \subset V$ such that for all $v \in V$, there exists $x \in L$ such that $v - x \in C$.

By Propositions 7.1.3 and 7.1.6, this is equivalent to L being a lattice.

a) In B, every coordinate is bounded, so by Proposition 5.3.3, the intersection with L is finite.

b) Let $K_{\mathbb{R}}^1 = \{x \in K_{\mathbb{R}} \mid N_{\mathbb{R}}^{K_{\mathbb{R}}}(x) = 1\}$, which contains $\Sigma(\mathbb{Z}_K^\times)$. By taking exponentials, it is enough to construct a set $C' \subset K_{\mathbb{R}}^1$ such that for all $x \in K_{\mathbb{R}}^1$, there exists $u \in \mathbb{Z}_K^\times$ such that $x\Sigma(u)^{-1} \in C'$.

   Let $L' = \Sigma(\mathbb{Z}_K)$, and let S be a compact convex symmetric subset of $K_{\mathbb{R}}$ such that

   $$\operatorname{vol}(S) \geq 2^n \operatorname{covol}(L').$$

   Let $R = N_{\mathbb{R}}^{K_{\mathbb{R}}}(S) \cap \mathbb{Z}$, which is finite. For all $r \in R$, define

- $S_r = \{x \in S \mid N_{\mathbb{R}}^{K_{\mathbb{R}}}(x) = r\}$;
- Y_r a set of representatives of the elements of norm r in $\mathbb{Z}_K$ up to multiplication by units.

Then S_r is compact, and Y_r is finite since two element differ by a unit if and only if they generate the same ideal and there are finitely many integral ideals of norm r. So $C_r = \Sigma(Y_r)^{-1}S_r = \{\Sigma(y)^{-1}x \colon y \in Y_r, x \in S_r\}$ is compact.

Let $C' = \bigcup_{r \in R} C_r$, which is compact. We claim that C' works.

Let $x \in K_{\mathbb{R}}^1$. Since $\operatorname{covol}(xL') = \operatorname{covol}(L')$, by Minkowski's theorem (Corollary 7.3.5) there exists $y \in S \cap xL'$. Let us write $y = x \cdot \Sigma(a)$ with $a \in \mathbb{Z}_K$. We have $r = N_{\mathbb{R}}^{K_{\mathbb{R}}}(y) = N_{\mathbb{R}}^{K}(a)$ since $N_{\mathbb{R}}^{K_{\mathbb{R}}}(x) = 1$, so $r \in R$ and $y \in S_r$. By definition of Y_r, there exists a unit $u \in \mathbb{Z}_K^\times$ such that $au \in Y_r$. But now $x\Sigma(u)^{-1} = \Sigma(au)^{-1}y \in Y_r^{-1}S_r \in C'$, as claimed.

This proves that $L \cong \mathbb{Z}^r$, where $r = \dim V = r_1 + r_2 - 1$. By Theorem 5.3.5, we have

$$\ker \mathcal{L} = W_K,$$

which is precisely the torsion subgroup of $\mathbb{Z}_K^\times$. By the structure theory of abelian groups, we get

$$\mathbb{Z}_K^\times \cong W_K \times \mathbb{Z}^r$$

as claimed. □