2. Ideals in Quadratic Number Fields

In this chapter we introduce some of the main actors: the ring of integers in quadratic number fields, as well as modules and ideals.

2.1 Algebraic Integers

In the last chapter we have studied some rings of the form $\mathbb{Z}[\sqrt{m}\,]$. It turned out, however, that these are not always the right domains to work with. The reason becomes apparent in the following example.

Consider the ring $R = \mathbb{Z}[\sqrt{-3}\,]$. There we have the factorization $2 \cdot 2 = (1+\sqrt{-3}\,)(1-\sqrt{-3}\,)$ into irreducibles, showing that R does not have unique factorization. The problem is that these factorizations cannot be explained by ideal factorization. In fact, consider the ideal $\mathfrak{a} = (1+\sqrt{-3}\,)$; then $\mathfrak{a}^2 = (-2+2\sqrt{-3}\,) = (2)\mathfrak{a}'$ with $\mathfrak{a}' = (1-\sqrt{-3}\,)$. Multiplying through by $\mathfrak{a}$ shows that $\mathfrak{a}^3 = (8)$. If we had unique factorization into prime ideals, this would imply $\mathfrak{a} = (2)$. But two principal ideals are equal if and only if their generators differ by a unit, hence we would have to conclude that $\frac{1+\sqrt{-3}}{2}$ is a unit; in fact, it is not even an element in R.

Help comes from studying Fermat's Last Theorem for exponent 3: for solving $x^3 + y^3 = z^3$ we could factor the left hand side as

$$x^3 + y^3 = (x+y)(x^2 - xy + y^2).$$

The quadratic factor is irreducible in $\mathbb{Z}$, but can be factored in $\mathbb{C}$ as

$$x^2 - xy + y^2 = (x + y\rho)(x + y\rho^2),$$

where $\rho = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity, i.e. a complex number $\rho \neq 1$ with the property $\rho^3 = 1$. Thus for studying this diophantine equation it seems we should work with the ring (!) $\mathbb{Z}[\rho] = \{a + b\rho : a, b \in \mathbb{Z}\}$; this ring contains $\mathbb{Z}[\sqrt{-3}\,]$ properly because $2\rho + 1 = \sqrt{-3}$.

Norm and Trace

Before we give the final definition of the "correct" rings of integers, let us introduce some notation. Consider the quadratic number field

$$K = \mathbb{Q}(\sqrt{m}\,) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}.$$

This is a Galois extension of $\mathbb{Q}$, i.e., there are two automorphisms, the identity and the conjugation map σ sending $\alpha = a + b\sqrt{m} \in K$ to $\sigma(\alpha) = \alpha' = a - b\sqrt{m}$. Clearly $\sigma^2 = 1$, and $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$. It is obvious that $\alpha \in K$ is fixed by σ if and only if $b = 0$, that is, if and only if $\alpha \in \mathbb{Q}$. We say that K is real or complex quadratic according as $m > 0$ or $m < 0$.

The element $\alpha = a + b\sqrt{m} \in K$ is a root of the quadratic polynomial $P_\alpha(X) = X^2 - 2aX + a^2 - mb^2 \in \mathbb{Q}[X]$; its second root $\alpha' = a - b\sqrt{m}$ is called the *conjugate* of α. We also define

$$\begin{array}{llll} \mathrm{N}\alpha & = \quad \alpha\alpha' & = a^2 - mb^2 & \text{the } \textit{norm} \text{ of } \alpha, \\ \mathrm{Tr}\,\alpha & = \ \alpha + \alpha' & = 2a & \text{the } \textit{trace} \text{ of } \alpha, \text{ and} \\ \mathrm{disc}(\alpha) & = (\alpha - \alpha')^2 & = 4mb^2 & \text{the } \textit{discriminant} \text{ of } \alpha. \end{array}$$

The basic properties of norm and trace are

Proposition 2.1. *For all $\alpha, \beta \in K$ we have $N(\alpha\beta) = N\alpha\, N\beta$ and $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}\,\alpha + \mathrm{Tr}\,\beta$. Moreover $N\alpha = 0$ if and only if $\alpha = 0$, $\mathrm{Tr}\,\alpha = 0$ if and only if $\alpha = b\sqrt{m}$, and $\mathrm{disc}(\alpha) = 0$ if and only if $\alpha \in \mathbb{Q}$.*

Proof. Left as an exercise. □

In particular, the norm is a group homomorphism $K^\times \longrightarrow \mathbb{Q}^\times$, and the trace is a group homomorphism from the additive group $(K, +)$ to the additive group $(\mathbb{Q}, +)$.

The Power of Linear Algebra

Let $K \subseteq L$ be fields; then L may be viewed as a K-vector space: the vectors are the elements from L (they form an additive group), the scalars are the elements of K, and the scalar multiplication is the restriction of the usual multiplication in L. The dimension $\dim_K L$ of L as a K-vector space is called the *degree* of L/K and is denoted by $(L : K)$.

Clearly $K = \mathbb{Q}(\sqrt{m}\,)$ has degree 2 over $\mathbb{Q}$: a basis is given by$\{1, \sqrt{m}\}$ since every element of K can be written uniquely as a $\mathbb{Q}$-linear combination of 1 and $\sqrt{m}$.

In algebraic number theory, fields of higher degree are also studied; for example,

$$\mathbb{Q}(\sqrt[3]{2}\,) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$$

is a number field of degree 3 with basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

Norm and trace can be defined in arbitrary number fields by generalizing the following approach: Let $\{1, \omega\}$ denote a basis of $K = \mathbb{Q}(\sqrt{m}\,)$ as a $\mathbb{Q}$-vector space (for example, take $\omega = \sqrt{m}$). Multiplication by α is a linear map because $\alpha(\lambda\beta + \mu\gamma) = \lambda(\alpha\beta) + \mu(\alpha\gamma)$ for $\lambda, \mu \in \mathbb{Q}$ and $\beta, \gamma \in K$. Now once a basis is chosen, linear maps can be represented by a matrix; in fact, all we have to do is compute the action of $\alpha = a + b\omega$ on the basis $\{1, \omega\}$.

To this end let us identify $a + b\sqrt{m}$ with the vector $\binom{a}{b}$; then 1 and $\sqrt{m}$ correspond to $\binom{1}{0}$ and $\binom{0}{1}$. The images of these vectors under multiplication by α are, in light of $\alpha \cdot 1 = a + b\omega$ and $\alpha \cdot \omega = bm + a\omega$ for $\omega = \sqrt{m}$, the vectors $\binom{a}{b}$ and $\binom{mb}{a}$. Thus multiplication by α is represented by the matrix $M_\alpha = ((\begin{smallmatrix} a & mb \\ b & a \end{smallmatrix}))$. Now we see that $\mathrm{N}(\alpha) = \det M_\alpha$ and $\mathrm{Tr}(\alpha) = \mathrm{Tr}\, M_\alpha$. It is an easy exercise to show that the norm and the trace in this definition do not depend on the choice of the basis.

From linear algebra we know that the characteristic polynomial of the matrix M_α is given by

$$\det(M_\alpha - XI) = \left| \begin{pmatrix} a - X & mb \\ b & a - X \end{pmatrix} \right| = X^2 - \mathrm{Tr}(\alpha)X + \mathrm{N}(\alpha) = P_\alpha(X).$$

We now say that α is **integral** if the characteristic polynomial $P_\alpha(X)$ has integral coefficients. Clearly α is integral if its norm and trace are ordinary rational integers. Thus all elements in $\mathbb{Z}[\sqrt{m}\,]$ are algebraic integers, but so are e.g. $\rho = \frac{-1+\sqrt{-3}}{2}$ and $\frac{1+\sqrt{5}}{2}$, as is easily checked. Moreover, a rational number $a \in \mathbb{Q}$ is integral if and only if $P_a(X) = X^2 - 2aX + a^2 = (X - a)^2$ has integral coefficients, which happens if and only if $a \in \mathbb{Z}$. This is a good sign: the integral numbers among the rationals according to our definition coincide with the integers!

Rings of Integers

Now let $\mathcal{O}_K$ denote the set of all algebraic integers in $K = \mathbb{Q}(\sqrt{m}\,)$, where m is a squarefree integer. In the following, we will determine $\mathcal{O}_K$ and show that it forms a ring.

Lemma 2.2. *We have $a + b\sqrt{m} \in \mathcal{O}_K$ if and only if $u = 2a$ and $v = 2b$ are integers with $u^2 - mv^2 \equiv 0 \bmod 4$.*

Proof. Assume that $\alpha = a + b\sqrt{m} \in \mathcal{O}_K$; then $u := 2a = \mathrm{Tr}(\alpha) \in \mathbb{Z}$ and $a^2 - mb^2 = \mathrm{N}(\alpha) \in \mathbb{Z}$. Multiplying the last equation through by 4 we find that $4mb^2$ must be an integer. Since m is squarefree, it cannot cancel any denominators in $4b^2$, hence $4b^2$ and therefore also $v := 2b$ are integers. Moreover, $u^2 - mv^2 = 4a^2 - 4mb^2 = 4\mathrm{N}(\alpha)$ is a multiple of 4, hence $u^2 - mv^2 \equiv 0 \bmod 4$.

Now assume that $u = 2a$ and $v = 2b$ are integers with $u^2 - mv^2 \equiv 0 \bmod 4$. Then for $\alpha = a + b\sqrt{m}$ we find that $P_\alpha(X) = X^2 - uX + \frac{1}{4}(u^2 - mv^2)$ has integral coefficients, hence $\alpha \in \mathcal{O}_K$. □

This lemma is now used to classify the algebraic integers in K:

Proposition 2.3. *We have*

$$\mathcal{O}_K = \begin{cases} \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} & \textit{if } m \equiv 2, 3 \bmod 4, \\ \{\frac{a+b\sqrt{m}}{2} : a \equiv b \bmod 2\} & \textit{if } m \equiv 1 \bmod 4. \end{cases}$$

In particular, $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}\,]$ is the ring of integers in K whenever $m \equiv 2, 3 \bmod 4$.

Proof. Assume that $a + b\sqrt{m}$ with $a, b \in \mathbb{Q}$ is an algebraic integer. Then $2a$, $2b$ and $a^2 - mb^2$ are integers by Lemma 2.2.

1. If $m \equiv 2 \bmod 4$, then $u^2 - mv^2 \equiv 0 \bmod 4$ for integers $u = 2a$ and $v = 2b$ implies that u and v are even, hence a and b are integers.

2. If $m \equiv 2 \bmod 4$, then $u^2 - mv^2 \equiv 0 \bmod 4$ for integers $u = 2a$ and $v = 2b$ can only happen if u and v have the same parity; if they are both odd, then $u^2 \equiv v^2 \equiv 1 \bmod 4$ and $u^2 - mv^2 \equiv 2 \bmod 4$: contradiction. Thus u and v are even, and a and b are integers.

3. Finally assume that $m \equiv 1 \bmod 4$. Again, $u^2 - mv^2 \equiv 0 \bmod 4$ if and only if u and v have the same parity. If u and v are both even, then a and b are integers; if not, then $u \equiv v \equiv 1 \bmod 2$ are both odd, and $a + b\sqrt{m} = \frac{u+v\sqrt{m}}{2}$ is an algebraic integer with trace u and norm $\frac{1}{2}(u^2 - mv^2)$. □

In the cases $m \equiv 2, 3 \bmod 4$, every integer in $\mathcal{O}_K$ can be written uniquely as a $\mathbb{Z}$-linear combination of 1 and $\sqrt{m}$: we say that $\{1, \sqrt{m}\}$ is an integral basis in this case. These are not unique: other examples are $\{1, a + \sqrt{m}\}$ for any $a \in \mathbb{Z}$ or $\{1 + \sqrt{m}, \sqrt{m}\}$.

In the case $m \equiv 1 \bmod 4$ we claim that $\mathcal{O}_K$ also has an integral basis, namely $\{1, \omega\}$ with $\omega = \frac{1}{2}(1 + \sqrt{m}\,)$. In fact, for any pair of integers $a, b \in \mathbb{Z}$, the number $a + b\omega = \frac{2a+b+b\sqrt{m}}{2}$ is integral since $2a + b \equiv b \bmod 2$; conversely, any integer $\frac{a+b\sqrt{m}}{2}$ with $a \equiv b \bmod 2$ can be written in the form $\frac{a-b}{2} + b\omega$ with $\frac{a-b}{2}, b \in \mathbb{Z}$. We have proved:

Corollary 2.4. *The ring $\mathcal{O}_K$ of integers in a quadratic number field K is a free abelian group, i.e., for*

$$\omega = \begin{cases} \sqrt{m} & \textit{if } m \equiv 2, 3 \bmod 4, \\ \frac{1+\sqrt{m}}{2} & \textit{if } m \equiv 1 \bmod 4 \end{cases}$$

we have $\mathcal{O}_K = \mathbb{Z} \oplus \omega\mathbb{Z}$.

Now that we have constructed the rings of integers in a quadratic number field, we want to prove that they are Dedekind rings, i.e., domains in which every ideal is the product of prime ideals in a unique way. As a first step we review the basics of ideals and modules in commutative rings – the actual proof of unique factorization into prime ideals will then actually be quite fast and easy.

2.2 Ideals

What is an ideal? Recall that a subset I of a ring R is called a subring if I it is closed under the ring operations, that is, adding and multiplying elements of I again produces elements of I. This is similar to the concepts of subgroups or subspaces of vector spaces; what is different in the category of rings is that the quotient $R/I = \{r + I : r \in R\}$ in general is not a ring with respect to addition $(r + I) + (s + I) = r + s + I$ and multiplication $(r+I) \cdot (s+I) = rs+I$. In fact, this multiplication is in general not defined: if $r + I = r' + I$ and $s + I = s' + I$, i.e., if $a = r - r' \in I$ and $b = s - s' \in I$, then $r's' + I = (r - a)(s - b) + I = rs + (ab - rb - sa) + I$, and this is equal to the coset $rs + I$ only if $ab - rb - sa \in I$; since $a, b \in I$ implies that $ab \in I$, this is equivalent to $rb + sa \in I$. But for general subrings I of R this is not necessarily the case (see Exercise 7).

In order to guarantee that $rb + sa \in I$ for $a, b \in I$ and $r, s \in R$ we have to demand that I be an ideal: this is a subring of R with the additional property that $ri \in I$ whenever $i \in I$ and $r \in R$ (we abbreviate this by writing $RI \subseteq I$).

Note that if I and J are ideals in R, then so are

$$\begin{aligned} I + J &= \{i + j : i \in I, j \in J\}, \\ IJ &= \{i_1 j_1 + \ldots + i_n j_n : i_1, \ldots, i_n \in I, j_1, \ldots, j_n \in J\}, \end{aligned}$$

as well as $I \cap J$. The index n in the product IJ is meant to indicate that we only form finite sums. If A and B are ideals in some ring R, we say that $B \mid A$ if $A = BC$ for some ideal C.

The difference between additive subgroups, subrings, and ideals is not visible in the ring $R = \mathbb{Z}$ of integers: see Exercise 2.

We say that an nonzero ideal $I \neq R$ is

- irreducible if $I = AB$ for ideals A, B implies $A = R$ or $B = R$;
- a prime ideal if $AB \subseteq I$ for ideals A, B always implies $A \subseteq I$ or $B \subseteq I$;
- a maximal ideal if $I \subseteq J \subseteq R$ for an ideal J implies $J = I$ or $J = R$.

For principal ideals, this coincides with the usual usage of prime and irreducible elements: an ideal (a) is irreducible (prime) if and only if a is irreducible (prime). In fact, $(r) \mid (s)$ is equivalent to $r \mid s$.

Prime ideals and maximal ideals can be characterized as follows:

Proposition 2.5. *An ideal I is*

- *prime in R if and only if R/I is an integral domain;*
- *maximal in R if and only if R/I is a field.*

Proof. R/I is an integral domain if and only if it has no zero divisors. But $0 = (r + I)(s + I) = rs + I$ is equivalent to $rs \in I$; if I is prime, then this implies $r \in I$ or $s \in I$, i.e., $r + I = 0$ or $s + I = 0$, and R/I is a domain. The converse is also clear.

Now let I be maximal and take some $a \in R \setminus I$; we have to show that $a+I$ has a multiplicative inverse. Since I is maximal, the ideal generated by I and a must be the unit ideal, hence there exist elements $m \in I$ and $r, s \in R$ such that $1 = rm + sa$. But then $(a+I)(s+I) = as + I = (1 - rm) + I = 1 + I$.

Conversely, assume that every coset $r + I \neq 0 + I$ has a multiplicative inverse. Then we claim that I is maximal. In fact, assume that M is an ideal strictly bigger than I. Then there is some $m \in M \setminus I$. Pick $r \in R$ sith $(m+I)(r+I) = 1 + I$; then $mr - 1 \in I \subset M$, and $m \in M$ now shows that $1 \in M$. □

Note that an integral domain is a ring with 1 in which $0 \neq 1$; thus (1) is not prime since the null ring R/R only has one element.

It follows from this proposition that every maximal ideal is prime; the converse is not true in general. In fact, consider the ring $\mathbb{Z}[X]$ of polynomials with integral coefficients. Then $I = (X)$ is an ideal, and $R/I \simeq \mathbb{Z}$ is an integral domain but not a field, hence I is prime but not maximal.

Example. Now consider the domain $R = \mathbb{Z}[\sqrt{-5}\,]$ and the ideal $\mathfrak{p} = (2, 1 + \sqrt{-5}\,)$. We claim that $R/\mathfrak{p} \simeq \mathbb{Z}/2\mathbb{Z}$; this will imply that $\mathfrak{p}$ is prime, and even a maximal ideal.

We first prove that every element of R is congruent to 0 or 1 modulo $\mathfrak{p}$. This is easy: reducing $a + b\sqrt{-5}$ modulo 2 shows that every element is congruent to $a + b\sqrt{-5} \bmod (2)$ with $a, b \in \{0, 1\}$, i.e., to one of 0, 1, $\sqrt{-5}$, $1 + \sqrt{-5}$.[1] Reducing these classes modulo $\mathfrak{p}$ we find that $\sqrt{-5} \equiv\equiv 1 \bmod \mathfrak{p}$ (the difference is in $\mathfrak{p}$ and $1 + \sqrt{-5} \equiv 0 \bmod \mathfrak{p}$. Thus every element is $\equiv 0, 1 \bmod \mathfrak{p}$. Moreover, these residue classes are different since $0 \equiv 1 \bmod \mathfrak{p}$ would imply $1 \in \mathfrak{p}$, which is not true: $1 = \alpha \cdot 2 + \beta \cdot (1 + \sqrt{-5}\,)$ is impossible for $\alpha, \beta \in R$, as a little calculation will show.

An important result is

Theorem 2.6 (Chinese Remainder Theorem)**.** *If A and B are ideals in R with $A + B = R$, then $R/AB \simeq R/A \oplus R/B$ as rings.*

Proof. Since $A + B = R$, there exist $a \in A$ and $b \in B$ such that $a + b = 1$. Consider the map $\phi : R/A \oplus R/B \longrightarrow R/AB$ defined by $\phi(r + A, s + B) = rb + sa + AB$. We claim that ϕ is a ring homomorphism. Checking that $\phi(r + A, s + B) + \phi(r' + A, s' + B) = \phi(r + r' + A, s + s' + B)$ is easy. Multiplication is more tricky: we have

$$\begin{aligned} \phi(r + A, s + B)\phi(r' + A, s' + B) &= (rb + sa)(r'b + s'a) + AB \\ &= rr'b^2 + ss'a^2 + AB \\ &= rr'b(1 - a) + ss'a(1 - b) + AB \\ &= rr'b + ss'a + AB = \phi(rr' + A, ss' + B). \end{aligned}$$

[1] Actually this is a complete set of residue classes modulo $\mathfrak{a} = (2)$ in R. The ring $R/(2)$ has zero divisors because $(1 + \sqrt{-5}\,)^2 = -4 + 2\sqrt{-5} \equiv 0 \bmod (2)$; in particular, (2) is not a prime ideal in R.

In order to show that ϕ is bijective, it is sufficient to define the inverse map $\psi : R/AB \longrightarrow R/A \oplus R/B$ by $\psi(r + AB) = (r + A, r + B)$ and verifying that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps; this is again easily done. □

2.3 Modules

Let R be a commutative ring; an (additively written) abelian group M is said to be an R-module if there is a map $R \times M \longrightarrow M : (r, m) \longmapsto rm$ with the following properties:

- $1m = m$ for all $m \in M$;
- $r(sm) = (rs)m$ for all $r, s \in R$ and $m \in M$;
- $r(m + n) = rm + rn$ for all $r \in R$ and $m, n \in M$;
- $(r + s)m = rm + sm$ for all $r, s \in R$ and $m \in M$.

The most important examples are abelian groups G: they are all $\mathbb{Z}$-modules via $ng = g + \ldots + g$ (n terms) for $n > 0$ and $ng = -(-n)g$ for $n < 0$. In particular, a subring M of a commutative ring R is a $\mathbb{Z}$-module; it is alsoan R-module if and only if M is an ideal.

If M and N are R-modules, then so is $M \oplus N = \{(m, n) : m \in M, n \in N\}$ via the action $r(m, n) = (rm, rn)$.

In the following, $K = \mathbb{Q}(\sqrt{d}\,)$ is a quadratic number field, and $\{1, \omega\}$ is a basis of its ring of integers $\mathcal{O}_K$. Our first job is the classification of all $\mathbb{Z}$-modules in $\mathcal{O}_K$.

Proposition 2.7. *Let $M \subset \mathcal{O}_K$ be a $\mathbb{Z}$-module in $\mathcal{O}_K$. Then there exist natural numbers m, n and and integer $a \in \mathbb{Z}$ such that $M = [n, a + m\omega] := n\mathbb{Z} \oplus (a + m\omega)\mathbb{Z}$.*

Note that this says that every element in M is a unique $\mathbb{Z}$-linear combination of n and $a + m\omega$; the elements n and $a + m\omega$ are therefore called a basis of the $\mathbb{Z}$-module M in analogy to linear algebra. Actually, studying R-modules is a generalization of linear algebra in the sense that R-modules are essentially vector spaces with the field of scalars replaced by a ring.

Note that, in general, not every R-module has a basis; R-modules possessing a basis are called **free**, and the number of elements in a basis is called the **rank** of the R-module. Proposition 2.7 claims that all $\mathbb{Z}$-modules in $\mathcal{O}_K$ are free of rank ≤ 2. In fact, the $\mathbb{Z}$-modules $M = \{0\} = [0, 0]$, $M = \mathbb{Z} = [1, 0]$ and $M = \mathcal{O}_K = [1, \omega]$ have ranks 0, 1 and 2, respectively.

Proof of Prop. 2.7. Consider the subgroup $H = \{s : r + s\omega \in M\}$ of $\mathbb{Z}$. Every subgroup of $\mathbb{Z}$ is automatically an ideal, hence H has the form $H = m\mathbb{Z}$ for some $m \ge 0$. By construction, there is an $a \in \mathbb{Z}$ such that $a + m\omega \in M$. Finally, $M \cap \mathbb{Z}$ is a subgroup of $\mathbb{Z}$, hence $M \cap \mathbb{Z} = n\mathbb{Z}$ for some $n \ge 0$.

We now claim that $M = n\mathbb{Z} \oplus (a + m\omega)\mathbb{Z}$. The inclusion $\supseteq$ is clear; assume therefore that $r + s\omega \in M$. Since $s \in H$ we have $s = um$ for some $u \in \mathbb{Z}$, and then $r - ua = r + s\omega - u(a + m\omega) \in M \cap \mathbb{Z}$, hence $r - ua = vn$. But then $r + s\omega = r - ua + u(a + m\omega) = vn + u(a + m\omega) \in n\mathbb{Z} \oplus (a + m\omega)\mathbb{Z}$. □

Clearly every ideal in $\mathcal{O}_K$ is a $\mathbb{Z}$-module (and therefore is generated by at most two elements); the converse is not true since e.g. $M = [1, 0] = \mathbb{Z}$ is a $\mathbb{Z}$-module in $\mathcal{O}_K$ but clearly not an ideal: the only ideal containing 1 is the unit ideal $(1) = \mathcal{O}_K$. A different way of looking at this is the following: ideals in $\mathcal{O}_K$ are $\mathcal{O}_K$-modules, and the fact that $\mathbb{Z} \subset \mathcal{O}_K$ implies that every ideal is a $\mathbb{Z}$-module.

Given a $\mathbb{Z}$-module $M = [n, a + m\omega]$, under what conditions on a, m, n is M an ideal? This question is answered by the next

Proposition 2.8. *A nonzero $\mathbb{Z}$-module $M = [n, a + m\omega]$ is an ideal if and only if $m \mid n$, $m \mid a$ (hence $a = mb$ for some $b \in \mathbb{Z}$) and $n \mid m \cdot N(b + \omega)$.*

Proof. Since M is an ideal, $c \in M \cap \mathbb{Z}$ implies $c\omega \in M$, hence $c \in H$ (see the proof of Prop. 2.7) by definition of H. This shows that $n\mathbb{Z} = M \cap \mathbb{Z} \subseteq H = m\mathbb{Z}$, hence $m \mid n$ (if the multiples of n are contained in the multiples of m, then m must divide n; this instance of "to divide means to contain" will reoccur frequently in the following).

In order to show that $m \mid a$ we observe that $\omega^2 = x + y\omega$ for suitable $x, y \in \mathbb{Z}$. Since M is an ideal, $a + m\omega \in M$ implies $(a + m\omega)\omega = mx + (a + my)\omega \in M$, hence $a + my \in H$ by definition of H, and therefore $a + my$ is a multiple of m. This implies immediately that $m \mid a$, hence $a = mb$ for some $b \in \mathbb{Z}$.

In order to prove the last divisibility relation we put $\alpha = a + m\omega = m(b + \omega)$. Then $\alpha \in M$ implies $\alpha(b + \omega') \in M$. Since $\frac{1}{m}N\alpha = m(b + \omega)(b + \omega') \in M \cap \mathbb{Z}$, we conclude that $\frac{1}{m}N(b + \omega)$ is a multiple of n. □

Norms of Modules

For an ideal I in some ring R, we define its norm as the cardinality of the quotient ring R/I, that is, as the index $(R : I)$ of the additive subgroup I of R in R. The same definition works for $\mathbb{Z}$-submodules M of R: the quotient R/M is an additive group, and can be given a ring structure of M happens to be an ideal.

In general, the norm $\mathrm{N}(M) = (R : M)$ will not be finite: just consider the module $M = \mathbb{Z} = [1, 0]$ in some ring $R = \mathcal{O}_K$. Reducing $a + b\sqrt{m}$ modulo M gives $a + b\sqrt{m} \equiv b\sqrt{m} \bmod M$, and in fact we have $R/M = \{b\sqrt{m} : b \in \mathbb{Z}\}$ since $b\sqrt{m} \equiv b'\sqrt{m} \bmod M$ implies $b = b'$. In particular, $(R : M) = \infty$.

This cannot happen if the $\mathbb{Z}$-module M has rank 2 (and in particular, if M is an ideal). Note that a $\mathbb{Z}$-module $M = [n, a + m\omega)]$ in $\mathcal{O}_K$ has rank 2 if and only if $mn \neq 0$. Modules of maximal rank in $\mathcal{O}_K$ (in the case of quadratic extensions $K/\mathbb{Q}$ this means rank 2) are also called **full** modules. Now we claim

Proposition 2.9. *Let $M = [n, a+m\omega)]$ be a full $\mathbb{Z}$-module in $\mathcal{O}_K$. Then*

$$S = \{r + s\omega : 0 \le r < n,\ 0 \le s < m\}$$

is a complete residue system modulo M in $\mathcal{O}_K$, and in particular $\mathrm{N}(M) = mn$.

Proof. We first show that every $x + y\omega \in \mathcal{O}_K$ is congruent mod M to an element of S. Write $y = mq + s$ for some $q \in \mathbb{Z}$ and $0 \le s < m$; then $x+y\omega-q(a+m\omega) = x'+s\omega$ for some integer x', hence $x+y\omega \equiv x'+s\omega \bmod M$. Now write $x' = nq'+r$ for $q' \in \mathbb{Z}$ and $0 \le r < n$; then $x'+s\omega \equiv r+s\omega \bmod M$.

Now we claim that the elements of S are pairwise incongruent modulo M. Assume that $r + s\omega \equiv r' + s'\omega \bmod M$ for $0 \le r, r' < n$ and $0 \le s, s' < m$; then $r - r' + (s-s')\omega \in M$ implies that $s - s' \in m\mathbb{Z}$ and $r - r' \in n\mathbb{Z}$, hence $r = r'$ and $s = s'$. □

We will also need a second way of characterizing the norm of ideals in $\mathcal{O}_K$. In contrast to the results above, which are valid in more general orders (they hold, for example, in rings $\mathbb{Z}[\sqrt{-m}\,]$), this characterization of the norm only holds in the ring of integers $\mathcal{O}_K$ (also called the maximal order). In fact, the following lemma due to Hurwitz exploits that we are working in $\mathcal{O}_K$:

Lemma 2.10. *Let $\alpha, \beta \in \mathcal{O}_K$ and $m \in \mathbb{N}$. If $N\alpha$, $N\beta$ and $\mathrm{Tr}\,\alpha\beta'$ are divisible by m, then $m \mid \alpha\beta'$ and $m \mid \alpha'\beta$.*

Proof. Put $\gamma = \alpha\beta'/m$; then $\gamma' = \alpha'\beta/m$, and we know that $\gamma + \gamma' = (\mathrm{Tr}\,\alpha\beta')/m$ and $\gamma\gamma' = \frac{N\alpha}{m}\frac{N\beta}{m}$ are integers. But if the norm and the trace of some γ in a quadratic number field are integral, then we have $\gamma \in \mathcal{O}_K$. □

Remark: the last sentence of the proof demands that any element in $\mathbb{Q}(\sqrt{m}\,)$ with integral norm and trace is in the ring. This means that the lemma holds in any subring of K containing $\mathcal{O}_K$, but not in smaller rings.

Proposition 2.11. *Let K be a quadratic number field with ring of integers $\mathcal{O}_K$ and integral basis $\{1, \omega\}$. If M is a full $\mathbb{Z}$-module in $\mathcal{O}_K$, then there is an $f \in \mathbb{N}$ such that $MM' = f\mathcal{O}_K$.*

Proof. Using Proposition 2.7 we can write $M = [\alpha, \beta]$ for $\alpha, \beta \in \mathcal{O}_K$ (actually Prop. 2.7 is more precise, but this is all we need for now). Then $M' = [\alpha', \beta']$ and therefore $MM' = [N\alpha, \alpha\beta', \alpha'\beta, N\beta]$. Now there is some integer $f > 0$ with $f = \gcd(N\alpha, N\beta, \mathrm{Tr}\,\alpha\beta')$ (in $\mathbb{Z}$); Hurwitz's Lemma shows that $\frac{\alpha\beta'}{f}$ and $\frac{\alpha'\beta}{f}$ are integral; thus we get $MM' = [f][\frac{N\alpha}{f}, \frac{N\beta}{f}, \frac{\alpha\beta'}{f}, \frac{\alpha'\beta}{f}]$ (the generators of this $\mathbb{Z}$-module are all integral by Hurwitz's Lemma). In order to prove $MM' = f\mathcal{O}_K$ it is therefore sufficient to show that $1 \in [\frac{N\alpha}{f}, \frac{N\beta}{f}, \frac{\alpha\beta'}{f}, \frac{\alpha'\beta}{f}]$. But 1 is a $\mathbb{Z}$-linear combination of $\frac{N\alpha}{f}$, $\frac{N\beta}{f}$ and $\frac{\mathrm{Tr}\,\alpha\beta'}{f}$ (by the definition of f), hence in particular a $\mathbb{Z}$-linear combination of $\frac{N\alpha}{f}$, $\frac{N\beta}{f}$, $\frac{\alpha\beta'}{f}$ and $\frac{\alpha'\beta}{f}$. This proves the claim. □

Once we know that such a natural number a exists it is easy to show that, for ideals $\mathfrak{a}$, we have $\mathrm{N}\mathfrak{a} = f$.

Proposition 2.12. *Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$, and write $\mathfrak{a}\mathfrak{a}' = f\mathcal{O}_K$ for some natural number f. Then $f = \mathrm{N}(\mathfrak{a})$.*

Proof. By Prop. 2.7 we can write $\mathfrak{a} = [n, m(b+\omega)]$, and we have $\mathrm{N}(\mathfrak{a}) = mn$. It remains to show that $\mathfrak{a}\mathfrak{a}' = (mn)$. To this end, we compute

$$\begin{aligned}\mathfrak{a}\mathfrak{a}' &= (n, a + m\omega)(n, a + m\omega') \\ &= (n^2, mn(b+\omega), mn(b+\omega'), m^2N(b+\omega)) \\ &= (mn)(c, b+\omega, b+\omega', \frac{1}{c}N(b+\omega)).\end{aligned}$$

The second ideal is integral because of Proposition 2.8. We want to show that it is the unit ideal. Note that the ideal must be generated by an integer since $\mathfrak{a}\mathfrak{a}' = (a)$. But the only integers dividing $b+\omega$ are ± 1 since $\{1, \omega\}$ is an integral basis. □

This implies in particular that $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$ because both sides generate the same ideal $\mathfrak{a}\mathfrak{b}\mathfrak{a}'\mathfrak{b}'$. Here are a few more useful properties:

- $N\mathfrak{a} = 1 \iff \mathfrak{a} = (1)$: if $N\mathfrak{a} = 1$, then $(1) = \mathfrak{a}\mathfrak{a}' \subseteq \mathfrak{a} \subseteq \mathcal{O}_K = (1)$, and the converse is clear.
- $N\mathfrak{a} = 0 \iff \mathfrak{a} = (0)$: if $\mathfrak{a}\mathfrak{a}' = (0)$, then $N\alpha = \alpha\alpha' = 0$ for all $\alpha \in \mathfrak{a}$.

2.4 Unique Factorization into Prime Ideals

We want to show that every ideal in the ring $\mathcal{O}_K$ of integers in a quadratic number field $K = \mathbb{Q}(\sqrt{d}\,)$ can be factored uniquely into prime ideals.

The Cancellation Law

Now we turn to the proof of unique factorization for ideals. The idea behind the proof is the same as in the proof of unique factorization for numbers: from equality of two products, conclude that there must be two equal factors, and then cancel. Now cancelling a factor is the same as multiplying with its inverse; the problem is that we do not have an inverse for ideals.

In the ring $R = \mathbb{Z}/6\mathbb{Z}$ we have $(2)(3) = (2)(0)$, but cancelling (2) yields nonsense. Similar examples exist in all rings with zero divisors. Are there examples in integral domains? Yes, there are. Simple calculations show that $(a,b)^3 = (a^2,b^2)(a,b)$ in arbitrary commutative rings; whenever $(a^2,b^2) \neq (a,b)^2$, we have a counter example to the cancellation law. For an example, take $R = \mathbb{Z}[X,Y]$ and observe that $XY \in (X,Y)^2$, but $XY \notin (X^2,Y^2)$.

The cancellation law even fails in subrings of $\mathcal{O}_K$: consider e.g. the ring $R = \mathbb{Z}[\sqrt{-3}\,]$; then a simple calculation shows that $(2)(2, 1+\sqrt{-3}\,) = (1+\sqrt{-3}\,)(2, 1+\sqrt{-3}\,)$, and cancelling would produce the incorrect statement $(2) = (1+\sqrt{-3}\,)$. It was Dedekind who realized that his ideal theory only works in rings $\mathcal{O}_K$:

Proposition 2.13. *If* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *are nonzero ideals in* $\mathcal{O}_K$ *with* $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$*, then* $\mathfrak{b} = \mathfrak{c}$.

Proof. The idea is to reduce the cancellation law for ideals to the one for numbers, or rather for principal ideals.

Thus assume first that $\mathfrak{a} = (\alpha)$ is principal. Then $\alpha\mathfrak{b} = \mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c} = \alpha\mathfrak{c}$. For every $\beta \in \mathfrak{b}$ we have $\alpha\beta \in \alpha\mathfrak{c}$, hence there is a $\gamma \in \mathfrak{c}$ such that $\alpha\beta = \alpha\gamma$. This shows $\beta = \gamma \in \mathfrak{c}$, hence $\mathfrak{b} \subseteq \mathfrak{c}$. By symmetry we conclude that $\mathfrak{b} = \mathfrak{c}$.

Now assume that $\mathfrak{a}$ is an arbitrary ideal. Then $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ implies that $(\mathfrak{a}\mathfrak{a}')\mathfrak{b} = (\mathfrak{a}\mathfrak{a}')\mathfrak{c}$. Since $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$ is principal, the claim follows from the first part of the proof. □

This shows that the ideals in $\mathcal{O}_K$ form a monoid with cancellation law, analogous to the natural numbers.

Divisibility of Ideals

We say that an ideal $\mathfrak{b}$ is divisible by an ideal $\mathfrak{a}$ if there is an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Since $\mathfrak{c} \subseteq \mathcal{O}_K$ we see $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}(1) = \mathfrak{a}$; this fact is often expressed by saying "to divide is to contain". As a matter of fact, the converse is also true:

Proposition 2.14. *If* $\mathfrak{a}, \mathfrak{b}$ *are nonzero ideals in* $\mathcal{O}_K$*, then* $\mathfrak{a} \supseteq \mathfrak{b}$ *if and only if* $\mathfrak{a} \mid \mathfrak{b}$.

Proof. From $\mathfrak{a} \supseteq \mathfrak{b}$ we deduce $\mathfrak{b}\mathfrak{a}' \subseteq \mathfrak{a}\mathfrak{a}' = (a)$, where $a = N\mathfrak{a}$. Then $\mathfrak{c} = \frac{1}{a}\mathfrak{b}\mathfrak{a}'$ is an ideal because of $\frac{1}{a}\mathfrak{a}'\mathfrak{b} \subseteq \mathcal{O}_K$ (the ideal axioms are easily checked) Now the claim follows from $\mathfrak{a}\mathfrak{c} = \frac{1}{a}\mathfrak{b}\mathfrak{a}\mathfrak{a}' = \mathfrak{b}$. □

We know that maximal ideals are always prime, as it is known that $\mathfrak{a}$ is maximal in a ring R if and only if $R/\mathfrak{a}$ is a field, and it is prime if and only if $R/\mathfrak{a}$ is an integral domain.

In the rings of integers in algebraic number fields all three notions coincide; irreducible and maximal ideals are the same:

- irreducible ideals are maximal: if $\mathfrak{a}$ were not maximal, then there were an ideal $\mathfrak{b}$ with $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq (1)$; this implies $\mathfrak{b} \mid \mathfrak{a}$ with $\mathfrak{b} \neq (1), \mathfrak{a}$.
- maximal ideals are irreducible: for $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ implies $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq (1)$.

It remains to show that, in our rings, prime ideals are maximal; note that this is not true in general rings. In fact we have to use Proposition 2.14 in the proof.

Proposition 2.15. *In rings of integers of qadratic number fields, prime ideals are maximal.*

Proof. Assume that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ and $\mathfrak{a} \nmid \mathfrak{b}$; then $\mathfrak{a} \mid \mathfrak{c}$, and since $\mathfrak{c} \mid \mathfrak{a}$ (to divide is to contain) we have $\mathfrak{a} = \mathfrak{c}$ and therefore $\mathfrak{b} = (1)$. □

Observe that from $\mathfrak{a} \mid \mathfrak{c}$ and $\mathfrak{c} \mid \mathfrak{a}$ we cannot conclude equality $\mathfrak{a} = \mathfrak{c}$: we do get $\mathfrak{a} = \mathfrak{c}\mathfrak{d}$ and $\mathfrak{c} = \mathfrak{a}\mathfrak{e}$, hence $\mathfrak{a} = \mathfrak{d}\mathfrak{e}\mathfrak{a}$. But without the cancellation law we cannot conclude that $\mathfrak{d}\mathfrak{e} = (1)$.

In $R = \mathbb{Z}[X]$, the ideal (X) is prime since $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$ is an integral domain; it is not maximal, since $\mathbb{Z}$ is not a field, and in fact we have $(X) \subset (2, X) \subset R$.

Now we can prove

Theorem 2.16. *Every nonzero ideal $\mathfrak{a}$ in the ring of integers $\mathcal{O}_K$ of a quadratic number field K can be written uniquely (up to order) as a product of prime ideals.*

Proof. We start with showing the existence of a factorization into irreducible ideals. If $\mathfrak{a}$ is irreducible, we are done. If not, then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$; if $\mathfrak{b}$ and $\mathfrak{c}$ are irreducible, we are done. If not, we keep on factoring. Since $N\mathfrak{a} = N\mathfrak{b}N\mathfrak{c}$ and $1 < N\mathfrak{b}$, $N\mathfrak{c} < N\mathfrak{a}$ etc. this process must terminate, since the norms are natural numbers and cannot decrease indefinitely.

Now we prove uniqueness. Assume that $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ are two decompositions of $\mathfrak{a}$ into prime ideals. We claim that $r = s$ and that we can reorder the $\mathfrak{q}_i$ in such a way that we have $\mathfrak{p}_i = \mathfrak{q}_i$ for $1 \le i \le r$. Since $\mathfrak{p}_1$ is prime, it divides some $\mathfrak{q}_j$ on the right hand side, say $\mathfrak{p}_1 \mid \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is irreducible, we must have equality $\mathfrak{p}_1 = \mathfrak{q}_1$, and the cancellation law yields $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. The claim now follows by induction. □

2.5 Decomposition of Primes

Now that we know that ideals in $\mathcal{O}_K$ can be factored uniquely into prime ideals, we have to come up with a description of these prime ideals. For quadratic (and, as we will see, also for cyclotomic) fields this is not hard.

Lemma 2.17. *Let $\mathfrak{p}$ be a prime ideal; then there is a unique prime number p such that $\mathfrak{p} \mid (p)$.*

Proof. We have $\mathfrak{p} \mid \mathfrak{p}\mathfrak{p}' = (N\mathfrak{p})$; decomposing $N\mathfrak{p}$ in $\mathbb{Z}$ into prime factors and using the fact that $\mathfrak{p}$ is prime shows that $\mathfrak{p}$ divides (hence contains) some ideal (p) for prime p. If $\mathfrak{p}$ would divide (hence contain) prime ideals (p) and (q) for different primes p and q, it would also contain 1, since p and q are coprime: this implies, by Bezout, the existence of $x, y \in \mathbb{Z}$ with $px + qy = 1$. □

If p is the prime contained in $\mathfrak{p}$, then we say that the prime ideal $\mathfrak{p}$ lies above p. Since (p) has norm p^2, we find that $N\mathfrak{p}$ equals p oder p^2.

Lemma 2.18. *If $\mathfrak{p}$ is an ideal in $\mathcal{O}_K$ with norm p, then it is prime.*

Proof. The ideal is clearly irreducible ($\mathfrak{p} = \mathfrak{a}\mathfrak{b}$ implies $p = N\mathfrak{p} = N\mathfrak{a} \cdot N\mathfrak{b}$), hence prime. □

For describing the prime ideals in quadratic number fields it is useful to have the notion of the discriminant. If $K = \mathbb{Q}(\sqrt{m}\,)$ with m squarefree, let $\{1, \omega\}$ denote an integral basis. We then define

$$\operatorname{disc} K = \left|\begin{smallmatrix} 1 & \omega \\ 1 & \omega' \end{smallmatrix}\right|^2 = (\omega - \omega')^2 = \begin{cases} m & \text{if } m \equiv \ \ 1 \bmod 4, \\ 4m & \text{if } m \equiv 2, 3 \bmod 4. \end{cases}$$

Theorem 2.19. *Let p be an odd prime, $K = \mathbb{Q}(\sqrt{m}\,)$ a quadratic number field, and $d = \operatorname{disc} K$ its discriminant.*

- *If $p \mid d$, then $p\mathcal{O}_K = (p, \sqrt{m}\,)^2$; we say that p is ramified in K.*
- *If $(d/p) = +1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ for prime ideals $\mathfrak{p} \neq \mathfrak{p}'$; we say that p splits (completely) in K.*
- *If $(d/p) = -1$, then $p\mathcal{O}_K$ is prime, and we say that p is inert in K.*

Proof. Assume first that $p \mid d$; since p is odd, we also have $p \mid m$. Now

$$(p, \sqrt{m}\,)^2 = (p^2, p\sqrt{m}, m) = (p)(p, \sqrt{m}, \frac{m}{p}) = (p),$$

since the ideal $(p, \sqrt{m}, \frac{m}{p})$ contains the coprime integers p and $\frac{m}{p}$, hence equals (1).

Next assume that $(d/p) = 1$; then $d \equiv x^2 \bmod p$ for some integer $x \in \mathbb{Z}$. Putting $\mathfrak{p} = (p, x + \sqrt{m}\,)$ we find

$$\begin{aligned} \mathfrak{p}\mathfrak{p}' &= (p^2, p(x + \sqrt{m}\,), p(x - \sqrt{m}\,), x^2 - m) \\ &= (p)(p, x + \sqrt{m}, x - \sqrt{m}, (x^2 - m)/p). \end{aligned}$$

Clearly $2\sqrt{m} = x + \sqrt{m} - (x - \sqrt{m}\,)$ and therefore $4m = (2\sqrt{m})^2$ are contained in the last ideal; since p and $4m$ are coprime, this ideal equals (1), and we have $\mathfrak{p}\mathfrak{p}' = (p)$. If we had $\mathfrak{p} = \mathfrak{p}'$, then it would follow that $4m \in \mathfrak{p}$ and $\mathfrak{p} = (1)$: contradiction.

Finally assume that $(d/p) = -1$. If there were an ideal $\mathfrak{p}$ of norm p, Proposition 2.8 would show that it has the form $\mathfrak{p} = (p, b + \omega)$ with $p \mid N(b + \omega)$. If $\omega = \sqrt{m}$, this means $b^2 - m \equiv 0 \bmod p$, hence $(d/p) = (4m/p) = (m/p) = +1$ in contradiction to our assumption. If $\omega = \frac{1}{2}(1 + \sqrt{m}\,)$, then $(2b + 1)^2 \equiv m \bmod p$, and this again is a contradiction. □

The description of all prime ideals above 2 is taken care of by the following

Exercise. Let $K = \mathbb{Q}(\sqrt{m}\,)$ be a quadratic number field, where m is squarefree.

- If $m \equiv 2 \bmod 4$ then $2\mathcal{O}_K = (2, \sqrt{m}\,)^2$.
- If $m \equiv 3 \bmod 4$ then $2\mathcal{O}_K = (2, 1+\sqrt{m}\,)^2$.
- If $m \equiv 1 \bmod 8$ then $2\mathcal{O}_K = \mathfrak{a}\mathfrak{a}'$, where $\mathfrak{a} = (2, \frac{1+\sqrt{m}}{2}\,)$ and $\mathfrak{a} \neq \mathfrak{a}'$.
- If $m \equiv 5 \bmod 8$ then $2\mathcal{O}_K$ is prime.

The two cases p odd and $p = 2$ can be subsumed into one by introducing the *Kronecker-Symbol* (d/p). This agrees with the Legendre symbol for odd primes p and is defined for $p = 2$ and $d \equiv 1 \bmod 4$ by $(d/2) = (-1)^{(d-1)/4}$; for $d \not\equiv 1 \bmod 4$ we put $(d/2) = 0$.

Before we go on, let us recall a few notions from algebra. A domain R is called a principal ideal domain (PID) if every ideal in R is principal. Every Euclidean ring (such as $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[X]$) is a PID, and every PID is a unique factorization domain (UFD). The knowledge that some ring $\mathcal{O}_K$ is a PID would allow us to prove results about the representation of primes by binary quadratic forms:

Proposition 2.20. *Assume that $\mathcal{O}_K$ is a PID, where $K = \mathbb{Q}(\sqrt{m}\,)$. Then every prime p with $(d/p) = +1$ can be written in the form $\pm p = x^2 - my^2$ if $m \equiv 2, 3 \bmod 4$, and in the form $\pm 4p = x^2 - my^2$ if $m \equiv 1 \bmod 4$.*

Proof. Assume that $(d/p) = +1$; then p splits in K, hence $p = \mathfrak{p}\mathfrak{p}'$ for prime ideals $\mathfrak{p}$, $\mathfrak{p}'$ of norm p. Since $\mathcal{O}_K$ is a PID, there is an $\alpha \in \mathcal{O}_K$ such that $\mathfrak{p} = (\alpha)$. Taking the norm show that $(N\alpha) = (p)$ as ideals, hence $N\alpha = \pm p$. The claim now follows by writing $\alpha = x + y\omega$, where $\{1, \omega\}$ is the standard integral basis of $\mathcal{O}_K$. □

If we could show that the rings of integers in $\mathbb{Q}(\sqrt{m}\,)$ for $m = -1$ and $m = -2$ were PIDs (actually this is easy to prove by showing they are Euclidean), this would imply

$$p \equiv 1 \bmod 4 \Longrightarrow p = x^2 + y^2,$$
$$p \equiv 1, 3 \bmod 8 \Longrightarrow p = x^2 + 2y^2,$$

as well as many similar results.

This stresses the importance of finding a method for determining when $\mathcal{O}_K$ is a PID. We will present such a method in the next two chapters: the main ingredients are the unit group and the ideal class group of a number field K.

Exercises

2.1 Compute the matrix M_α for $\alpha = a + b\omega + c\omega 2$ in the cubic number field $\mathbb{Q}(\omega)$ with $\omega^3 = 2$.

2.2 Show that every subgroup A of $\mathbb{Z}$ is automatically a subring and even an ideal in $\mathbb{Z}$, and that there is an $a \in \mathbb{Z}$ such that $A = a\mathbb{Z}$.

2.3 Let $n \in \mathbb{N}$ be a natural number. Find a basis for the ideal (n) in $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{m}\,)$ is a quadratic number field.

2.4 Show that $(3, 1 + \sqrt{-5}\,) = [3, 1 + \sqrt{-5}\,]$ in $R = \mathbb{Z}[\sqrt{-5}\,]$, i.e., that every R-linear combination $3\alpha + (1 + \sqrt{-5}\,)\beta$ with $\alpha, \beta \in R$ can already be written in the form $3a + (1 + \sqrt{-5}\,)b$ with $a, b \in \mathbb{Z}$.

2.5 Show that in $R = \mathbb{Z}[\sqrt{-5}\,]$ we have $R/(\sqrt{-5}\,) \simeq \mathbb{Z}/5\mathbb{Z}$ and deduce that $(\sqrt{-5}\,)$ is a maximal ideal.

2.6 Show that all ideals of prime norm p in $\mathcal{O}_K$ have the form $[p, a + \omega]$, where $p \mid N(a + \omega)$.

2.7 Show that the set of upper triangular 2×2-matrices with coefficients in some ring R is a subring, but not an ideal of the ring of all 2×2-matrices.

2.8 Consider the space S of all sequences of rational numbers. This is a ring with respect to pointwise addition and multiplication:

$$\begin{aligned}(a_1, a_2, a_3, \ldots) + (b_1, b_2, b_3, \ldots) &= (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots),\\ (a_1, a_2, a_3, \ldots) \cdot (b_1, b_2, b_3, \ldots) &= (a_1 b_1, a_2 b_2, a_3 b_3, \ldots).\end{aligned}$$

Show that the the following subsets of S actually are subrings:

1. the set N of sequences converging to 0;
2. the set D of sequences converging in $\mathbb{Q}$;
3. the set C of Cauchy sequences;
4. the set B of bounded sequences.

Observe that $N \subset D \subset C \subset B \subset S$. Determine which of these subrings are ideals in B (resp. C, D). Show that all of these rings contain zero divisors, and that N is maximal in C (so C/N is a field; actually $C/N \simeq \mathbb{R}$: this is one possible way of constructing the field of real numbers).