Chapter 4 : Ideals in number rings

One of the very first 'proofs' of Fermat's last theorem (FLT) was proposed by Lamé in 1847. This proof had the serious flaw that it was based on the assumption that the ring $\mathbb{Z}[\omega_n]$ of cyclotomic integers (ω_n being a primitive n-th root of unity) is a UFD. Unfortunately this is not true in general. Kummer later pointed this out and Cauchy discovered that the smallest n for which $\mathbb{Z}[\omega_n]$ is not a UFD is $n = 23$.

A great set-back to the mathematicians! But number rings are not as bad as they appeared at the first glance. Kummer himself proved that unique factorization in $\mathbb{Z}[\omega_n]$ is again restored in terms of what he called *ideal numbers*. Dedekind later reformulated Kummer's notion of ideal numbers to define what we now know as *ideals*. Thus ideals admit unique factorization in number rings. This is historically one of the main streams that led to the birth and development of modern algebraic number theory.

Ideals in a number ring indeed possess very rich structures. This chapter is an introduction to the theory of ideals in number rings. We prove that number rings are Dedekind domains (Definitions 2.9 and 2.24) and in any Dedekind domain unique factorization of ideals holds. We will also see how (ideals generated by) rational primes behave in number rings. I will also introduce two other important concepts (norm and class number) related to ideals in a number ring.

4.1 Unique factorization of ideals

In this section I denote by K an arbitrary number field of degree $d = [K : \mathbb{Q}]$ and $\mathfrak{O}_K$ the ring of integers of K (i.e., the integral closure of $\mathbb{Z}$ in K). As claimed above I start by showing that $\mathfrak{O}_K$ is a Dedekind domain (henceforth abbreviated as DD). I will use Definition 2.24 of Dedekind domains for this purpose. I proceed by proving a series of auxiliary results. First let me introduce a terminology. Let $\varphi : A \to B$ be a homomorphism of rings. If $\mathfrak{q}$ is a prime ideal of B, then the contraction $\mathfrak{p} := \varphi^{-1}(\mathfrak{q}) = \mathfrak{q}^c$ is a prime ideal of A (Exercise 1.2.6(a)). We say that $\mathfrak{q}$ lies above or over $\mathfrak{p}$. If $A \subseteq B$ and φ is the inclusion homomorphism, then $\mathfrak{p} = A \cap \mathfrak{q}$. For a number field K we consider the natural inclusion $\mathbb{Z} \hookrightarrow \mathfrak{O}_K$.

4.1 Lemma Let $\mathfrak{q}$ be a non-zero prime ideal of $\mathfrak{O}_K$. Then $\mathfrak{q}$ lies above a non-zero prime ideal of $\mathbb{Z}$. In particular, $\mathfrak{q}$ contains a rational prime.

Proof If $\mathfrak{q} \cap \mathbb{Z} = 0$, then both $\mathfrak{q}$ and 0 are prime ideals of $\mathfrak{O}_K$ that lie over the zero ideal of $\mathbb{Z}$. Since $0 \subseteq \mathfrak{q}$, it follows from Exercise 2.2.4(c) that $\mathfrak{q} = 0$, a contradiction. ◀

4.2 Corollary Let $\mathfrak{q}$ be a non-zero prime ideal of $\mathfrak{O}_K$. Then $\mathfrak{q}$ lies above a *unique* non-zero prime ideal of $\mathbb{Z}$. In other words $\mathfrak{q}$ contains a *unique* rational prime.

Proof $\mathfrak{p} := \mathfrak{q} \cap \mathbb{Z}$ is the unique prime ideal of $\mathbb{Z}$ over which $\mathfrak{q}$ lies. By Lemma 4.1 $\mathfrak{p} \neq 0$. ◀

We can in fact prove a more general result.

4.3 Lemma Let $\mathfrak{a}$ be a non-zero ideal of $\mathfrak{O}_K$. Then $\mathfrak{a}$ contains a non-zero rational integer.

Proof Take any non-zero $\alpha \in \mathfrak{a}$ and let $\alpha_1, \ldots, \alpha_r$ be the conjugates of α with $\alpha = \alpha_1$. Then $a := \mathrm{N}_{K|\mathbb{Q}}(\alpha) = (\alpha_1 \cdots \alpha_r)^s \in \mathbb{Z}$, where $s := [K : \mathbb{Q}(\alpha)] = d/r$ (See Equation 3.4). Certainly a is non-zero (since α_i are evidently non-zero). Now $\beta := \alpha_1^{s-1}(\alpha_2 \cdots \alpha_r)^s$ is an algebraic integer and being equal to a/α belongs to K, i.e., $\beta \in \mathbb{A} \cap K = \mathfrak{O}_K$. Thus $a = \alpha\beta \in \mathfrak{a}$. ◀

That $\mathfrak{O}_K$ is a free Abelian group of rank d has an important consequence.

4.4 Proposition The ring of integers $\mathfrak{O}_K$ of a number field K is Noetherian.

Proof Let $\alpha_1, \ldots, \alpha_d \in \mathfrak{O}_K$ constitute an integral basis of $\mathfrak{O}_K$, i.e., $\mathfrak{O}_K = \mathbb{Z}[\alpha_1, \ldots, \alpha_d]$, i.e., the ring homomorphism $\mathbb{Z}[X_1, \ldots, X_d] \to \mathfrak{O}_K$, $f(X_1, \ldots, X_d) \mapsto f(\alpha_1, \ldots, \alpha_d)$, is surjective. By Hilbert's basis theorem (Theorem 2.23) the polynomial ring $\mathbb{Z}[X_1, \ldots, X_d]$ is Noetherian and therefore $\mathfrak{O}_K$, being the quotient of a Noetherian ring (by the isomorphism theorem), is Noetherian too (Example 2.22). ◀

Thus all ideals of $\mathfrak{O}_K$ are finitely generated. This fact is also a direct consequence of the following result which investigates the $\mathbb{Z}$-module structure of non-zero ideals of $\mathfrak{O}_K$.

4.5 Proposition Every *non-zero* ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ is a free Abelian group (i.e., a $\mathbb{Z}$-module) of rank d.

Proof Let $\beta_1, \ldots, \beta_d$ be an integral basis of K. We now explicitly construct an integral basis (i.e., a $\mathbb{Z}$-basis) $\gamma_1, \ldots, \gamma_d$ of $\mathfrak{a}$. By Lemma 4.3 there is a rational integer $a \in \mathfrak{a}$. We can take $a > 0$ without loss of generality. Since $a\beta_i \in \mathfrak{a}$ for every $i = 1, \ldots, d$, we can choose the smallest positive integer a_{11} for which $\gamma_1 := a_{11}\beta_1 \in \mathfrak{a}$. More generally for every $i = 1, \ldots, d$ we choose $\gamma_i := a_{i1}\beta_1 + a_{i2}\beta_2 + \cdots + a_{ii}\beta_i \in \mathfrak{a}$ such that a_{ij} are rational integers and a_{ii} is positive and minimal. Since $\det(a_{ij})_{1 \leqslant i,j \leqslant d} = a_{11} \cdots a_{dd} \neq 0$ by construction, $\gamma_1, \ldots, \gamma_d$ form a $\mathbb{Q}$-basis of K. Therefore $\gamma_1, \ldots, \gamma_d$ are linearly independent over $\mathbb{Q}$ and hence over $\mathbb{Z}$. So it is sufficient to show that $\gamma_1, \ldots, \gamma_d$ generate $\mathfrak{a}$ as a $\mathbb{Z}$-module.

Take any $\alpha \in \mathfrak{a}$ and write $\alpha = b_1\beta_1 + \cdots + b_d\beta_d$ with $b_i \in \mathbb{Z}$. Euclidean division of b_d by a_{dd} gives $b_d = q_d a_{dd} + r_d$ for $q_d, r_d \in \mathbb{Z}$ with $0 \leqslant r_d < a_{dd}$. Now $\alpha - q_d\gamma_d = c_1\beta_1 + \cdots + c_{d-1}\beta_{d-1} + r_d\beta_d \in \mathfrak{a}$, where $c_j := b_j - q_d a_{dj} \in \mathbb{Z}$. The minimality of a_{dd} forces $r_d = 0$, i.e., $b_d = q_d a_{dd}$, i.e., $\alpha - q_d\gamma_d = c_1\beta_1 + \cdots + c_{d-1}\beta_{d-1} \in \mathfrak{a}$. The choice of $a_{d-1,d-1}$ now forces $c_{d-1} = q_{d-1}a_{d-1,d-1}$ for some $q_{d-1} \in \mathbb{Z}$. Proceeding in this way one can show that $\alpha = q_1\gamma_1 + \cdots + q_d\gamma_d$ with $q_i \in \mathbb{Z}$. ◀

The last proposition implies that every ideal in $\mathfrak{O}_K$ is generated (as an ideal, i.e., as an $\mathfrak{O}_K$-module) by at most d elements. We will later see that every ideal in $\mathfrak{O}_K$ is actually generated by at most *two* elements.

4.6 Theorem The ring of integers $\mathfrak{O}_K$ of a number field K is a Dedekind domain.

Proof We have seen that $\mathfrak{O}_K$ is Noetherian (Proposition 4.4) and integrally closed (Proposition 2.18). It then suffices to show that each non-zero prime ideal $\mathfrak{q}$ of $\mathfrak{O}_K$ is maximal. By Lemma 4.1 $\mathfrak{q}$ lies over a non-zero prime ideal $\mathfrak{p}$ of $\mathbb{Z}$. But then $\mathfrak{p}$ is maximal in $\mathbb{Z}$. Exercise 2.2.4(b) now completes the proof. ◀

Now we will derive the unique factorization theorem for ideals in a DD. It's going to be a long story. First recall that for two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring A the set-theoretic (inner) product $S := \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ is not, in general, an ideal of A. The ideal generated by S is called the product of $\mathfrak{a}$ and $\mathfrak{b}$ and is denoted by $\mathfrak{ab}$, i.e.,

$$\mathfrak{ab} := \left\{ \sum_{i=1}^{m} a_i b_i \mid m \in \mathbb{Z}_+, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

We always have $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$. However if $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime, i.e., if $\mathfrak{a} + \mathfrak{b} = A$, then $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. In a similar way we can define the product of finitely many ideals of A. This product is clearly associative and commutative. The power $\mathfrak{a}^m$ of an ideal $\mathfrak{a}$ of A, $m \in \mathbb{Z}_+$, is defined as the m-fold product of $\mathfrak{a}$. Let us adopt the convention that the empty product of ideals of A is A itself. For a principal ideal $\mathfrak{a} = Aa$ we have $\mathfrak{a}^m = Aa^m$.

4.7 Lemma Let A be a ring, $r \in \mathbb{N}$, $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ ideals of A, and $\mathfrak{p}$ a prime ideal of A such that $\mathfrak{p} \supseteq \mathfrak{a}_1 \cdots \mathfrak{a}_r$. Then $\mathfrak{p} \supseteq \mathfrak{a}_k$ for some $k \in \{1, \ldots, r\}$. In particular, if A is a Dedekind domain and $\mathfrak{a}_i$ are non-zero prime ideals, then $\mathfrak{p} = \mathfrak{a}_k$ for some $k \in \{1, \ldots, r\}$.

Proof The proof is obvious for $r = 1$. So assume that $r > 1$. If $\mathfrak{p} \not\supseteq \mathfrak{a}_i$ for all $i = 1, \ldots, r$, then for each i we can choose $a_i \in \mathfrak{a}_i \setminus \mathfrak{p}$ and see that $a_1 \cdots a_r \in \mathfrak{p}$, a contradiction, since $\mathfrak{p}$ is prime. The last statement follows from the fact that in a Dedekind domain every non-zero prime ideal is maximal. ◀

We now generalize the concept of ideals.

4.8 Definition Let A be an integral domain and $K := \mathrm{Q}(A)$. Then an A-submodule $\mathfrak{a}$ of K is called a fractional ideal of A, if $a\mathfrak{a} \subseteq A$ for some $0 \neq a \in A$.

Every ideal of A is evidently a fractional ideal of A and hence is often called an integral ideal of A. Conversely every fractional ideal of A contained in A is an integral ideal of A. The principal fractional ideal Ax is the A-submodule of K generated by $x \in K$. If A is a Noetherian domain, we have the following equivalent characterization of fractional ideals.

4.9 Lemma Let A be a Noetherian integral domain, $K := \mathrm{Q}(A)$ and $\mathfrak{a} \subseteq K$. Then $\mathfrak{a}$ is a fractional ideal of A, if and only if $\mathfrak{a}$ is a finitely generated A-submodule of K.

Proof [if] Let $\mathfrak{a} = Ax_1 + \cdots + Ax_m$, where $x_i = a_i/b_i$, $a_i, b_i \in A$, $b_i \neq 0$. Then $b_1 \cdots b_m \mathfrak{a} \subseteq A$.

[only if] Let $0 \neq b \in A$ be such that $b\mathfrak{a} \subseteq A$. It is easy to check that $b\mathfrak{a}$ is an (integral) ideal of A and is finitely generated, since A is Noetherian. Let $b\mathfrak{a} = Aa_1 + \cdots + Aa_m$, $a_i \in A$. Then $\mathfrak{a} = Ax_1 + \cdots + Ax_m$, where $x_i := a_i/b \in K$. ◀

We define the product of two fractional ideals $\mathfrak{a}, \mathfrak{b}$ of an integral domain A as we did for integral ideals:

$$\mathfrak{a}\mathfrak{b} := \left\{ \sum_{i=1}^{m} a_i b_i \mid m \in \mathbb{Z}_+, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

It is easy to check that $\mathfrak{a}\mathfrak{b}$ is again a fractional ideal of A. Let $\mathcal{F}$ denote the set of non-zero fractional ideals of A. The product of fractional ideals defines a commutative and associative binary operation on $\mathcal{F}$. The ideal A acts as a (multiplicative) identity in $\mathcal{F}$. A fractional ideal $\mathfrak{a}$ of A is called invertible, if $\mathfrak{a}\mathfrak{b} = A$ for some fractional ideal $\mathfrak{b}$ of A. We shall see shortly that if A is a DD, then every non-zero fractional ideal of A is invertible and, therefore, $\mathcal{F}$ is a group under multiplication of fractional ideals.

Fractional ideals often play an important role in analyzing the properties of integral ideals, for example, in proving the central theorem (Theorem 4.12) of this section. Before going directly to this theorem let us deduce some auxiliary results.

4.10 Lemma Let A be a Noetherian domain and $\mathfrak{a}$ an (integral) ideal of A. Then there exist prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of A each containing $\mathfrak{a}$ such that $\mathfrak{q}_1 \cdots \mathfrak{q}_r \subseteq \mathfrak{a}$.

Proof Let S be the set of ideals of A for which the claim does not hold. Assume that $S \neq \emptyset$. Since A is Noetherian, S contains a maximal element, say $\mathfrak{b}$. Clearly $\mathfrak{b}$ is a proper non-prime ideal of A. Then for some $a, b \notin \mathfrak{b}$ we have $ab \in \mathfrak{b}$. The ideals $\mathfrak{b}' := \mathfrak{b} + Aa$ and $\mathfrak{b}'' := \mathfrak{b} + Ab$ strictly contain $\mathfrak{b}$ and, therefore, by the maximality of $\mathfrak{b}$ are not in S, i.e, there exist prime ideals $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_s$ each containing $\mathfrak{b}'$ (and hence $\mathfrak{b}$) such that $\mathfrak{q}'_1 \cdots \mathfrak{q}'_s \subseteq \mathfrak{b}'$ and prime ideals $\mathfrak{q}''_1, \ldots, \mathfrak{q}''_t$ each containing $\mathfrak{b}''$ (and hence $\mathfrak{b}$) such that $\mathfrak{q}''_1 \cdots \mathfrak{q}''_t \subseteq \mathfrak{b}''$.

Moreover $(\mathfrak{q}_1' \cdots \mathfrak{q}_s')(\mathfrak{q}_1'' \cdots \mathfrak{q}_t'') \subseteq \mathfrak{b}'\mathfrak{b}'' = (\mathfrak{b} + Aa)(\mathfrak{b} + Ab) = \mathfrak{b}\mathfrak{b} + a\mathfrak{b} + b\mathfrak{b} + Aab \subseteq \mathfrak{b}$, since $ab \in \mathfrak{b}$, so that $\mathfrak{b} \notin S$, a contradiction. Thus S must be empty. ◀

Note that the condition "each containing $\mathfrak{a}$" was necessary in Lemma 4.10 in order to rule out the trivial possibility that $\mathfrak{q}_i = 0$ for some $i \in \{1, \ldots, r\}$.

4.11 Lemma Let A be a DD, $K := \mathrm{Q}(A)$ and $\mathfrak{q}$ a non-zero prime ideal of A. Define the set

$$\mathfrak{q}^{-1} := \{x \in K \mid x\mathfrak{q} \subseteq A\}\,.$$

Then:

(1) $\mathfrak{q}^{-1}$ is a fractional ideal of A.

(2) $A \subsetneqq \mathfrak{q}^{-1}$.

(3) $\mathfrak{q}\mathfrak{q}^{-1} = A$. In particular, every non-zero prime ideal in a DD is invertible.

Proof (1) Clearly $\mathfrak{q}^{-1}$ is an A-submodule of K and for each $0 \neq a \in \mathfrak{q}$ we have $a\mathfrak{q}^{-1} \subseteq \mathfrak{q}\mathfrak{q}^{-1} \subseteq A$.

(2) Since $1 \in \mathfrak{q}^{-1}$, we evidently have $A \subseteq \mathfrak{q}^{-1}$. In order to prove the strict inclusion we take any $0 \neq a \in \mathfrak{q}$ and consider the ideal $\mathfrak{a} := Aa$. By Lemma 4.10 there exist prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ each containing $\mathfrak{a}$ (and hence non-zero) such that $\mathfrak{q}_1 \cdots \mathfrak{q}_r \subseteq \mathfrak{a}$. We choose r to be minimal, so that $\mathfrak{a}$ does not contain the product of any $r-1$ of $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$. Now $\mathfrak{q}_1 \cdots \mathfrak{q}_r \subseteq \mathfrak{q}$ and hence by Lemma 4.7 $\mathfrak{q}_i = \mathfrak{q}$ for some i, say, $i = r$. Choose any $b \in \mathfrak{q}_1 \cdots \mathfrak{q}_{r-1} \setminus \mathfrak{a}$. Since $b \notin \mathfrak{a}$, we have $b/a \notin A$. On the other hand $b \in \mathfrak{q}_1 \cdots \mathfrak{q}_{r-1}$ and $\mathfrak{q} = \mathfrak{q}_r$, so that $(b/a)\mathfrak{q} \subseteq (1/a)(\mathfrak{q}_1 \cdots \mathfrak{q}_r) \subseteq (1/a)\mathfrak{a} = (1/a)(Aa) = A$, i.e., $b/a \in \mathfrak{q}^{-1} \setminus A$.

(3) By the definition of $\mathfrak{q}^{-1}$ it follows that $\mathfrak{q}\mathfrak{q}^{-1}$ is contained in and hence an integral ideal of A. Since $A \subseteq \mathfrak{q}^{-1}$, it follows that $\mathfrak{q} = \mathfrak{q}A \subseteq \mathfrak{q}\mathfrak{q}^{-1}$. Since $\mathfrak{q}$ is a maximal ideal, we then have $\mathfrak{q}\mathfrak{q}^{-1} = \mathfrak{q}$ or $\mathfrak{q}\mathfrak{q}^{-1} = A$. Assume that $\mathfrak{q}\mathfrak{q}^{-1} = \mathfrak{q}$. I claim that this assumption implies that $\mathfrak{q}^{-1} \subseteq A$, a contradiction to Part (2). So we must have $\mathfrak{q}\mathfrak{q}^{-1} = A$. Let $b \in \mathfrak{q}^{-1}$ and choose $0 \neq a \in \mathfrak{q}$. Then we have $ab \in \mathfrak{q}\mathfrak{q}^{-1} = \mathfrak{q}$ and therefore $ab^2 = (ab)b \in \mathfrak{q}$, $ab^3 = (ab^2)b \in \mathfrak{q}$ and so on. For each $m \in \mathbb{Z}_+$ define the ideal $\mathfrak{a}_m := \sum_{i=0}^{m} Aab^i$. Then $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ is an ascending chain of ideals in A. Since A is Noetherian, the chain must be stationary, i.e, for some $m \in \mathbb{N}$ we have $\mathfrak{a}_m = \mathfrak{a}_{m-1}$, i.e., $ab^m \in \sum_{i=0}^{m-1} Aab^i$, i.e., $ab^m = \sum_{i=0}^{m-1} a_i ab^i$ with $a_i \in A$. Since A is an integral domain and $a \neq 0$, we see that b is integral over A. Since A is integrally closed, $b \in A$. Therefore $\mathfrak{q}^{-1} \subseteq A$, as claimed. ◀

4.12 Theorem Let A be a DD. Then every non-zero ideal $\mathfrak{a}$ of A can be represented as a product of prime ideals of A. Moreover such a factorization of $\mathfrak{a}$ is unique up to permutations of the factors.

Proof If $\mathfrak{a} = A$, there is nothing to prove. So let $\mathfrak{a}$ be a proper ideal of A. I will first show that if $\mathfrak{a}$ contains a product of non-zero prime ideals, then $\mathfrak{a}$ *is* a product of prime ideals. By Lemma 4.10 we have prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$, $r \in \mathbb{N}$, of A each containing $\mathfrak{a}$, such that $\mathfrak{q}_1 \cdots \mathfrak{q}_r \subseteq \mathfrak{a}$. Let us choose r to be minimal and proceed by induction on r. If $r = 1$, $\mathfrak{a} = \mathfrak{q}_1$ is already prime. So take $r > 1$ and assume that if an ideal $\mathfrak{b}$ of A contains a product of $r-1$ or less non-zero prime ideals of A, then $\mathfrak{b}$ is a product of prime ideals. Let $\mathfrak{q}$ be a maximal ideal containing $\mathfrak{a}$. We then have $\mathfrak{q}_1 \cdots \mathfrak{q}_r \subseteq \mathfrak{a} \subseteq \mathfrak{q}$ and by Lemma 4.7 $\mathfrak{q} = \mathfrak{q}_i$ for some i, say, $i = r$. Now consider the fractional ideal $\mathfrak{b} := \mathfrak{a}\mathfrak{q}_r^{-1}$. Then $\mathfrak{b} \subseteq \mathfrak{q}_r\mathfrak{q}_r^{-1} = A$ and so $\mathfrak{b}$ is an integral ideal of A. Furthermore $\mathfrak{b} = \mathfrak{a}\mathfrak{q}_r^{-1} \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_r\mathfrak{q}_r^{-1} = (\mathfrak{q}_1 \cdots \mathfrak{q}_{r-1})A = \mathfrak{q}_1 \cdots \mathfrak{q}_{r-1}$, i.e, $\mathfrak{b}$ contains a product of $r-1$ non-zero prime ideals. By the induction hypothesis $\mathfrak{b}$ is a product of prime ideals, i.e., $\mathfrak{b} = \mathfrak{q}_1' \cdots \mathfrak{q}_s'$. But then $\mathfrak{a} = \mathfrak{a}A = \mathfrak{a}(\mathfrak{q}_r^{-1}\mathfrak{q}_r) = (\mathfrak{a}\mathfrak{q}_r^{-1})\mathfrak{q}_r = \mathfrak{b}\mathfrak{q}_r = \mathfrak{q}_1' \cdots \mathfrak{q}_s'\mathfrak{q}_r$ is also a product of prime ideals.

In order to prove the uniqueness of this product let $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_r = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ with prime ideals $\mathfrak{q}_i$ and $\mathfrak{p}_j$. Now $\mathfrak{q}_1 \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_r = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ and hence by Lemma 4.7 $\mathfrak{q}_1 = \mathfrak{p}_j$ for some $j \in \{1, \ldots, t\}$, say, $j = 1$. Then

$\mathfrak{q}_2 \cdots \mathfrak{q}_r = A\mathfrak{q}_2 \cdots \mathfrak{q}_r = (\mathfrak{q}_1^{-1}\mathfrak{q}_1)\mathfrak{q}_2 \cdots \mathfrak{q}_r = \mathfrak{q}_1^{-1}(\mathfrak{q}_1 \cdots \mathfrak{q}_r) = \mathfrak{p}_1^{-1}(\mathfrak{p}_1 \cdots \mathfrak{p}_t) = \mathfrak{p}_2 \cdots \mathfrak{p}_t$. Proceeding in this way shows the desired uniqueness. ◀

In the factorization of a non-zero ideal of a DD we do not rule out the possibility of repeated occurrences of factors. Taking this into account shows that every non-zero ideal $\mathfrak{a}$ in a DD A admits a *unique* factorization

$$\mathfrak{a} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

with *distinct* non-zero prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ and with exponents $e_1, \ldots, e_r \in \mathbb{N}$. Of course, uniqueness here is up to permutations of the indexes $1, \ldots, r$. This factorization can be extended to fractional ideals, but this time we have to allow non-positive exponents. First note that for integers $e_1, \ldots, e_r$ and non-zero prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of A the product $\mathfrak{a} := \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ is well-defined and is a fractional ideal of $\mathfrak{a}$. The converse is proved in the following corollary.

4.13 Corollary Every non-zero fractional ideal $\mathfrak{a}$ of a DD A admits a unique factorization of the form $\mathfrak{a} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ with non-zero prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of A and with exponents $e_i \in \mathbb{Z}$. Moreover for such a fractional ideal $\mathfrak{a}$ we have $\mathfrak{a}(\mathfrak{q}_1^{-e_1} \cdots \mathfrak{q}_r^{-e_r}) = A$.

Proof By definition there exists $0 \neq a \in A$ such that $a\mathfrak{a} \subseteq A$. But then $a\mathfrak{a} = (Aa)\mathfrak{a}$ is an integral ideal of A. We write $a\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{q}_i^{f_i}$ and $Aa = \prod_{i=1}^{r} \mathfrak{q}_i^{g_i}$ with $f_i, g_i \in \mathbb{Z}_+$. Since each non-zero prime ideal is invertible (Lemma 4.11(3)), it follows that $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{q}_i^{f_i - g_i}$. This proves the existence of a factorization of $\mathfrak{a}$. The proof for the uniqueness is left to the reader as an easy exercise. The last assertion follows from a repeated use of Lemma 4.11(3). ◀

The fractional ideal $\mathfrak{q}_1^{-e_1} \cdots \mathfrak{q}_r^{-e_r}$ in the last corollary is denoted by $\mathfrak{a}^{-1}$. We have $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{a}\mathfrak{a}^{-1} = A$. One can easily verify that $\mathfrak{a}^{-1}$ defined as above is equal to the set

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq A\}.$$

In fact, one can use the last equality as the definition for $\mathfrak{a}^{-1}$.

To sum up every non-zero fractional ideal of a DD A is invertible and thus the set $\mathcal{F}$ of all non-zero fractional ideals of A is a group as claimed earlier. The unit ideal A acts as the identity in $\mathcal{F}$.

As in every group we have the cancellation law(s) in $\mathcal{F}$.

4.14 Corollary Let A be a DD and $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ fractional ideals of A. If $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{c}$ and $\mathfrak{c} \neq 0$, then $\mathfrak{a} = \mathfrak{b}$. ◀

In view of unique factorization of ideals in A we can speak of the divisibility of integral ideals in A. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two integral ideals of A. We say that $\mathfrak{a}$ divides $\mathfrak{b}$ and write $\mathfrak{a} \mid \mathfrak{b}$, if $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ for some integral ideal $\mathfrak{c}$ of A. We will now show that the condition $\mathfrak{a} \mid \mathfrak{b}$ is equivalent to the condition $\mathfrak{a} \supseteq \mathfrak{b}$. Thus for ideals in a DD the term ‘divides’ is synonymous with ‘contains’.

4.15 Corollary Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral ideals of a DD A. Then $\mathfrak{a} \mid \mathfrak{b}$, if and only if $\mathfrak{a} \supseteq \mathfrak{b}$.

Proof [if] If $\mathfrak{a} \supseteq \mathfrak{b}$, we have $A = \mathfrak{a}^{-1}\mathfrak{a} \supseteq \mathfrak{a}^{-1}\mathfrak{b}$, i.e., $\mathfrak{c} := \mathfrak{a}^{-1}\mathfrak{b}$ is an integral ideal of A. Also $\mathfrak{b} = A\mathfrak{b} = (\mathfrak{a}\mathfrak{a}^{-1})\mathfrak{b} = \mathfrak{a}(\mathfrak{a}^{-1}\mathfrak{b}) = \mathfrak{a}\mathfrak{c}$.

[only if] If $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ for some integral ideal $\mathfrak{c}$, we have $\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{c} \subseteq \mathfrak{a}$. ◀

4.16 Corollary Let $\mathfrak{a} := \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ and $\mathfrak{b} := \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_r^{f_r}$ with $e_i, f_i \in \mathbb{Z}_+$ be the prime decompositions of two non-zero integral ideals of a DD A. Then $\mathfrak{a} \mid \mathfrak{b}$, if and only if $e_i \leqslant f_i$ for all $i = 1, \ldots, r$.

Proof [if] We have $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, where $\mathfrak{c} := \mathfrak{q}_1^{f_1 - e_1} \cdots \mathfrak{q}_r^{f_r - e_r}$ is an integral ideal of A.

[only if] Let $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ for some integral ideal $\mathfrak{c}$ of A. Clearly, $\mathfrak{c} \neq 0$ and we can write the prime decomposition $\mathfrak{c} = \mathfrak{q}_1^{l_1} \cdots \mathfrak{q}_r^{l_r} \mathfrak{q}_{r+1}^{l_{r+1}} \cdots \mathfrak{q}_{r+s}^{l_{r+s}}$ with $l_i \geqslant 0$. We have $\mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_r^{f_r} = \mathfrak{q}_1^{e_1 + l_1} \cdots \mathfrak{q}_r^{e_r + l_r} \mathfrak{q}_{r+1}^{l_{r+1}} \cdots \mathfrak{q}_{r+s}^{l_{r+s}}$. By unique factorization we have $f_1 = e_1 + l_1, \ldots, f_r = e_r + l_r$ and $l_{r+1} = \cdots = l_{r+s} = 0$. ◀

Thus as we pass from $\mathbb{Z}$ to $\mathfrak{O}_K$, the notion of unique factorization passes from the element level to the ideal level. Of course, if a DD is already a PID, these two concepts are equivalent. (Non-zero prime ideals in a PID are generated by prime elements.) A DD is in general not a PID. But a DD is not quite far away from a PID as the following two results justify.

4.17 Lemma For a non-zero ideal $\mathfrak{a}$ in a DD A there exists a non-zero ideal $\mathfrak{b}$ of A such that $\mathfrak{a}\mathfrak{b}$ is a principal ideal of A. Furthermore given any non-zero ideal $\mathfrak{c}$ of A the ideal $\mathfrak{b}$ can be so chosen that $\mathfrak{b} + \mathfrak{c} = A$.

Proof I start by proving the first statement. By Lemma 4.9 $\mathfrak{a}^{-1}$ is finitely generated as an A-module, say by $a_1/b_1, \ldots, a_t/b_t \in K := \mathrm{Q}(A)$ with $b_1, \ldots, b_t \neq 0$. Take $b := b_1 \cdots b_t$. Then $Ab = \langle b \rangle = A\langle b \rangle = (\mathfrak{a}\mathfrak{a}^{-1})\langle b \rangle = \mathfrak{a}\mathfrak{b}$, where $\mathfrak{b} := \mathfrak{a}^{-1}\langle b \rangle = \langle b_1 \cdots b_t \rangle (\sum_{i=1}^{t} Aa_i/b_i) \subseteq A$, i.e., $\mathfrak{b}$ is a non-zero integral ideal of A.

Now the second statement. For $\mathfrak{c} = A$ the ideal $\mathfrak{b}$ as found above will do. So assume that $\mathfrak{c} \subsetneqq A$. Let $\mathfrak{c} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ be the prime factorization of $\mathfrak{c}$ with $r, e_i \in \mathbb{N}$. Define $\mathfrak{C} := \mathfrak{q}_1 \cdots \mathfrak{q}_r$ and $\mathfrak{c}_i := \mathfrak{q}_1 \cdots \mathfrak{q}_{i-1}\mathfrak{q}_{i+1} \cdots \mathfrak{q}_r$. For every $i = 1, \ldots, r$ we have $\mathfrak{c}_i \supsetneqq \mathfrak{C}$, so that $\mathfrak{a}\mathfrak{c}_i \supsetneqq \mathfrak{a}\mathfrak{C}$, i.e., we can choose $b_i \in \mathfrak{a}\mathfrak{c}_i \setminus \mathfrak{a}\mathfrak{C}$. Set $b := \sum_{i=1}^{r} b_i$. Each $b_i \in \mathfrak{a}\mathfrak{c}_i \subseteq \mathfrak{a}$, so that $b \in \mathfrak{a}$, i.e., $\langle b \rangle \subseteq \mathfrak{a}$, i.e., $\langle b \rangle = \mathfrak{a}\mathfrak{b}$ for some non-zero ideal $\mathfrak{b}$ of A. It remains to show that $\mathfrak{b} + \mathfrak{c} = A$. Assume not, i.e., $\mathfrak{b} + \mathfrak{c}$ has a non-zero prime divisor. Since $\mathfrak{b} + \mathfrak{c} \supseteq \mathfrak{c}$, i.e., $(\mathfrak{b} + \mathfrak{c}) \mid \mathfrak{c}$, any prime ideal dividing $\mathfrak{b} + \mathfrak{c}$ must be a divisor of $\mathfrak{c}$ too. Let $\mathfrak{q}_i \mid (\mathfrak{b} + \mathfrak{c})$ for some $i \in \{1, \ldots, r\}$. We also have $(\mathfrak{b} + \mathfrak{c}) \mid \mathfrak{b}$, i.e., $\mathfrak{q}_i \mid \mathfrak{b}$, i.e., $\mathfrak{a}\mathfrak{q}_i \mid \mathfrak{a}\mathfrak{b} = \langle b \rangle$, i.e., $b \in \mathfrak{a}\mathfrak{q}_i$. But $b_j \in \mathfrak{a}\mathfrak{q}_i$ for all $j \neq i$ and so $b_i \in \mathfrak{a}\mathfrak{q}_i$. Also by choice $b_i \in \mathfrak{a}\mathfrak{c}_i$. Now $\mathfrak{q}_i$ and $\mathfrak{c}_i$ are relatively prime ideals and hence $\mathfrak{C} = \mathfrak{q}_i\mathfrak{c}_i = \mathfrak{q}_i \cap \mathfrak{c}_i$, i.e., $b_i \in (\mathfrak{a}\mathfrak{q}_i) \cap (\mathfrak{a}\mathfrak{c}_i) = \mathfrak{a}(\mathfrak{q}_i \cap \mathfrak{c}_i) = \mathfrak{a}\mathfrak{C}$, where the equality $(\mathfrak{a}\mathfrak{q}_i) \cap (\mathfrak{a}\mathfrak{c}_i) = \mathfrak{a}(\mathfrak{q}_i \cap \mathfrak{c}_i)$ follows from Exercise 4.1.2. But by choice $b_i \notin \mathfrak{a}\mathfrak{C}$, a contradiction. ◀

4.18 Proposition Every (integral) ideal in a DD A is generated by (at most) two elements. More precisely for a proper non-zero ideal $\mathfrak{a}$ of A and for any $0 \neq a \in \mathfrak{a}$ there exists $b \in \mathfrak{a}$ with $\mathfrak{a} = \langle a, b \rangle = \langle a \rangle + \langle b \rangle$.

Proof The first statement obviously holds for the zero ideal and the unit ideal. So let us prove the second statement. Since $\mathfrak{a} \supseteq \langle a \rangle$, we have $\mathfrak{a} \mid \langle a \rangle$, i.e., $\langle a \rangle = \mathfrak{a}\mathfrak{c}$ for some non-zero ideal $\mathfrak{c}$ of A. By Lemma 4.17 we can choose a non-zero ideal $\mathfrak{b}$ of A such that $\mathfrak{b} + \mathfrak{c} = A$ and $\mathfrak{a}\mathfrak{b}$ is the principal ideal $\langle b \rangle$ for some $b \in \mathfrak{a}$. But then $\langle a \rangle + \langle b \rangle = \mathfrak{a}\mathfrak{c} + \mathfrak{a}\mathfrak{b} = \mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}A = \mathfrak{a}$. ◀

Of course, a DD can be a UFD or even a PID. However, being a UFD is a necessary and sufficient condition for a DD to be a PID.

4.19 Proposition A Dedekind domain A is a UFD, if and only if A is a PID.

Proof [if] Every PID is a UFD (Theorem 1.12).

[only if] Let A be a UFD. In order to show that A is a PID it is sufficient (in view of Theorem 4.12) to show that every non-zero prime ideal $\mathfrak{q}$ of A is a principal ideal. Choose any non-zero $a \in \mathfrak{q}$. Then $\mathfrak{q} \supseteq \langle a \rangle$. Now a is a non-unit in A (since otherwise we would have $\mathfrak{q} = A$) and A is assumed to be a UFD. Thus we can write $a = uq_1 \cdots q_r$ for $r \in \mathbb{N}$, $u \in A^*$ and for prime elements q_i in A. Clearly each $\langle q_i \rangle$ is a non-zero prime ideal of A and $\langle a \rangle = \langle q_1 \rangle \cdots \langle q_r \rangle$. Therefore $\mathfrak{q} \supseteq \langle q_1 \rangle \cdots \langle q_r \rangle$ and hence by Lemma 4.7 $\mathfrak{q} = \langle q_i \rangle$ for some $i \in \{1, \ldots, r\}$. ◀

Exercises for Section 4.1

1. Let K be a field. Prove or disprove: $K[X,Y]$ is a DD.

2. Let $\mathfrak{a} := \mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_r^{e_r}$ and $\mathfrak{b} := \mathfrak{q}_1^{f_1}\cdots\mathfrak{q}_r^{f_r}$, $e_i, f_i \in \mathbb{Z}_+$, be the prime decompositions of two non-zero ideals $\mathfrak{a}$, $\mathfrak{b}$ of a DD A. Define the gcd and lcm of $\mathfrak{a}$ and $\mathfrak{b}$ as

$$\begin{aligned}\gcd(\mathfrak{a},\mathfrak{b}) &:= \mathfrak{q}_1^{\min(e_1,f_1)}\cdots\mathfrak{q}_r^{\min(e_r,f_r)},\\ \operatorname{lcm}(\mathfrak{a},\mathfrak{b}) &:= \mathfrak{q}_1^{\max(e_1,f_1)}\cdots\mathfrak{q}_r^{\max(e_r,f_r)}.\end{aligned}$$

Show that $\gcd(\mathfrak{a},\mathfrak{b}) = \mathfrak{a}+\mathfrak{b}$ and $\operatorname{lcm}(\mathfrak{a},\mathfrak{b}) = \mathfrak{a}\cap\mathfrak{b}$. Conclude that $\gcd(\mathfrak{a},\mathfrak{b})\operatorname{lcm}(\mathfrak{a},\mathfrak{b}) = (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}) = \mathfrak{a}\mathfrak{b}$. (**Remark:** If A is a general ring, we only have $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}) = \mathfrak{a}(\mathfrak{a}\cap\mathfrak{b})+\mathfrak{b}(\mathfrak{a}\cap\mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$.)

3. Let A be a DD and $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{b}$ non-zero ideals of A satisfying $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{b}^m$ for some $m \in \mathbb{N}$. Show that if $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, then $\mathfrak{a}_1 = \mathfrak{b}_1^m$ and $\mathfrak{a}_2 = \mathfrak{b}_2^m$ for some ideals $\mathfrak{b}_1$ and $\mathfrak{b}_2$ of A.

4. Let $A := \mathbb{Z}[\sqrt{-3}\,]$ and let $\mathfrak{a}$ be the ideal $\langle 2, 1+\sqrt{-3}\,\rangle$ in A. Show that $\mathfrak{a} \neq \langle 2\rangle$ and $\mathfrak{a}^2 = \langle 2\rangle\mathfrak{a}$. Explain why this example does not contradict Corollary 4.14.

5. Let A be a DD and $\mathfrak{a}$ a non-zero ideal of A. Show that:

(a) The number of ideals containing $\mathfrak{a}$ is finite.

(b) Every ideal of $A/\mathfrak{a}$ is principal.

6. Let A be an integral domain and $K := \mathrm{Q}(A)$. Show that:

(a) K is an A-module.

(b) If K is a fractional ideal of A, then $A = K$.

(c) If K is a number field, then K is not a fractional ideal of its ring of integers.

7. Let K be a number field, $\mathfrak{a}$ a non-zero ideal of $\mathfrak{O}_K$ and $\gamma \in K$. If $\gamma\mathfrak{a} \subseteq \mathfrak{a}$, show that $\gamma \in \mathfrak{O}_K$.

8. **(a)** Prove or disprove: Every UFD is a DD.

(b) Prove or disprove: Every PID is a DD.

9. (Linear congruence in a DD) Let A be a DD, $\mathfrak{a}$ a non-zero ideal of A and $\alpha, \beta \in A$. Prove that the congruence

$$\alpha x \equiv \beta \pmod{\mathfrak{a}} \tag{4.1}$$

is solvable for x, if and only if $\gcd(\langle\alpha\rangle, \mathfrak{a}) \mid \langle\beta\rangle$. In particular, if $\mathfrak{a} + \langle\alpha\rangle = A$, then the congruence (4.1) is solvable for x and the solution is unique modulo $\mathfrak{a}$. Moreover if $\mathfrak{a}$ is a non-zero prime ideal of A, then the congruence is solvable uniquely modulo $\mathfrak{a}$, if and only if $\alpha \notin \mathfrak{a}$.

10. (Chinese remainder theorem in a DD) Let A be a DD, $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ pairwise coprime non-zero ideals of A and $\alpha_1, \ldots, \alpha_r \in A$. Show that there is an $\alpha \in A$ unique modulo $\mathfrak{a}_1\cdots\mathfrak{a}_r$ satisfying the simultaneous congruences $\alpha \equiv \alpha_i \pmod{\mathfrak{a}_i}$ for all $i = 1, \cdots, r$.

4.2 Norms of ideals

In Section 3.2 we have introduced the concept of the norm of an algebraic number (or integer). Now we extend the definition to ideals in a number ring. As usual we will continue to work with a generic number field K of degree d with ring of integers $\mathfrak{O}_K$. Since we will in general not work with many number rings simultaneously, it would be harmless to abbreviate $\mathfrak{O}_K$ as $\mathfrak{O}$.

4.20 Definition Let $\mathfrak{a}$ be a non-zero ideal of $\mathfrak{O}$. The norm of $\mathfrak{a}$, denoted $\mathrm{N}(\mathfrak{a})$, is defined as the cardinality of the quotient ring $\mathfrak{O}/\mathfrak{a}$, i.e., $\mathrm{N}(\mathfrak{a})$ is the number of distinct cosets of $\mathfrak{a}$ in the additive group $\mathfrak{O}$. It is customary to define the norm of the zero ideal as zero.

For the simplest case $K = \mathbb{Q}$, i.e., $\mathfrak{O}_{\mathbb{Q}} = \mathbb{Z}$, every non-zero ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z} = \langle n \rangle$ for some $n \in \mathbb{N}$. The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}_n$. Thus $\mathrm{N}(\langle n \rangle)$ equals n and is finite. For a general K also $\mathrm{N}(\mathfrak{a})$ is finite for every ideal $\mathfrak{a}$ of $\mathfrak{O}_K$. This is immediate from the next proposition which gives an explicit formula for the norm of a non-zero ideal of $\mathfrak{O}_K$.

By Proposition 4.5 a non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}$ is a free $\mathbb{Z}$-module of rank d. In the proof of that proposition we constructed an integral basis $\gamma_1, \ldots, \gamma_d$ of $\mathfrak{a}$ of the form $\gamma_i = \sum_{j=1}^{i} a_{ij}\beta_j$ for all $i = 1, \ldots, d$, where $\beta_1, \ldots, \beta_d$ is a given integral basis of K. We selected $a_{ij} \in \mathbb{Z}$ with $a_{ii} > 0$ and minimal. With these notations we have:

4.21 Proposition $\mathrm{N}(\mathfrak{a}) = a_{11} \cdots a_{dd}$.

Proof I will show that the elements $\alpha_{r_1,\ldots,r_d} := \sum_{i=1}^{d} r_i\beta_i$, $r_i \in \mathbb{Z}$, $0 \leqslant r_i < a_{ii}$, constitute a complete residue system of $\mathfrak{O}$ modulo $\mathfrak{a}$.

Claim $\alpha_{r_1,\ldots,r_d}$ are distinct modulo $\mathfrak{a}$.

Let $\alpha_{r_1,\ldots,r_d} \equiv \alpha_{s_1,\ldots,s_d} \pmod{\mathfrak{a}}$. Then $\sum_{i=1}^{d}(r_i - s_i)\beta_i \equiv 0 \pmod{\mathfrak{a}}$, i.e., $\sum_{i=1}^{d}(r_i - s_i)\beta_i = \sum_{i=1}^{d} t_i\gamma_i$ for some $t_i \in \mathbb{Z}$. Substituting the values of γ_i in terms of β_i allows us to rewrite the last equality as $\sum_{i=1}^{d}(r_i - s_i)\beta_i = \sum_{i=1}^{d} u_i\beta_i$ for some integers u_i. Since $(\beta_1, \ldots, \beta_d)$ is a basis of $\mathfrak{O}$, we have $r_i - s_i = u_i$ for all $i = 1, \ldots, d$. In particular, $r_d - s_d = u_d = a_{dd}t_d$. Thus $a_{dd} \mid (r_d - s_d)$. Since $-a_{dd} < r_d - s_d < a_{dd}$, we must have $r_d - s_d = 0$, i.e., $r_d = s_d$. This implies that $u_d = a_{dd}t_d = 0$, i.e., $t_d = 0$. But then $r_{d-1} - s_{d-1} = u_{d-1} = a_{d-1,d-1}t_{d-1} + a_{d,d-1}t_d = a_{d-1,d-1}t_{d-1}$. As before we obtain $r_{d-1} = s_{d-1}$ and $t_{d-1} = 0$. Proceeding in this way shows that $r_i = s_i$ for all $i = 1, \ldots, d$. This proves the claim.

Claim Any $\xi \in \mathfrak{O}$ is congruent to some $\alpha_{r_1,\ldots,r_d}$.

Write $\xi = \sum_{i=1}^{d} v_i\beta_i$, $v_i \in \mathbb{Z}$. Euclidean division of v_d by a_{dd} gives $v_d = a_{dd}q_d + r_d$ with $0 \leqslant r_d < a_{dd}$. Then $\xi_1 := \xi - q_d\gamma_d - r_d\beta_d \in \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_{d-1}$. As above we then find $\xi_2 := \xi_1 - q_{d-1}\gamma_{d-1} - r_{d-1}\beta_{d-1} \in \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_{d-2}$ for integers q_{d-1} and r_{d-1} with $0 \leqslant r_{d-1} < a_{d-1,d-1}$. Proceeding in this way gives $\xi_d = 0$, so that $\xi = \left(\sum_{i=1}^{d} q_i\gamma_i\right) + \left(\sum_{i=1}^{d} r_i\beta_i\right) \equiv \alpha_{r_1,\ldots,r_d} \pmod{\mathfrak{a}}$. ◀

As in the case of $\mathfrak{O}$ one can show that the discriminant $\Delta(\alpha_1, \ldots, \alpha_d)$ is independent of the choice of the integral basis $(\alpha_1, \ldots, \alpha_d)$ of $\mathfrak{a}$ (See Corollary 3.20). One can then define $\Delta(\mathfrak{a}) := \Delta(\alpha_1, \ldots, \alpha_d)$ for any integral basis $(\alpha_1, \ldots, \alpha_d)$ of $\mathfrak{a}$. In view of Lemma 3.15 we then have:

4.22 Corollary For a non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}$ we have $\mathrm{N}(\mathfrak{a}) = \sqrt{\Delta(\mathfrak{a})/\Delta_K}$. ◀

4.23 Corollary For every non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}$ the quotient ring $\mathfrak{O}/\mathfrak{a}$ is a finite ring. In particular, for a non-zero prime (and hence maximal) ideal $\mathfrak{q}$ of $\mathfrak{O}$ the quotient ring $\mathfrak{O}/\mathfrak{q}$ is a finite field. ◀

We will study the norms of non-zero prime ideals of $\mathfrak{O}$ shortly. Before that let us look at some other properties of the norm function. First note that it is tempting to define the norm of an element $\alpha \in \mathfrak{O}$ to be the norm of the principal ideal $\langle \alpha \rangle = \mathfrak{O}\alpha$. It turns out that this new definition is (almost) the same as the old definition of $\mathrm{N}(\alpha)$. More precisely:

4.24 Proposition For any element $\alpha \in \mathfrak{O}$ we have $\mathrm{N}(\langle\alpha\rangle) = |\mathrm{N}(\alpha)|$.

Proof The result is obvious for $\alpha = 0$. So assume that $\alpha \neq 0$ and call $\mathfrak{a} := \langle\alpha\rangle$. Let $\beta_1, \ldots, \beta_d$ be an integral basis of $\mathfrak{O}$. It is a straightforward matter to check that $\alpha\beta_1, \ldots, \alpha\beta_d$ is an integral basis of $\mathfrak{a}$. Let $\sigma_1, \ldots, \sigma_d$ be the complex embeddings of K. Then $\Delta(\mathfrak{a})$ is the square of the determinant of the matrix $(\sigma_j(\alpha\beta_i)) = (\sigma_j(\alpha)\sigma_j(\beta_i)) = \begin{pmatrix} \sigma_1(\alpha) & 0 & \cdots & 0 \\ 0 & \sigma_2(\alpha) & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \sigma_n(\alpha) \end{pmatrix} (\sigma_j(\beta_i))$. It follows that $\Delta(\mathfrak{a}) = \mathrm{N}(\alpha)^2\Delta(\beta_1, \ldots, \beta_d) = \mathrm{N}(\alpha)^2\Delta_K$. Corollary 4.22 now completes the proof. ◀

4.25 Corollary For any $a \in \mathbb{Z}$ we have $\mathrm{N}(\mathfrak{O}a) = |a^d|$. ◀

An interesting generalization of Fermat's little theorem is the following.

4.26 Proposition Let $\mathfrak{q}$ be a non-zero prime ideal of $\mathfrak{O}$ and let $\alpha \in \mathfrak{O} \setminus \mathfrak{q}$. Then $\alpha^{\mathrm{N}(\mathfrak{q})-1} \equiv 1 \pmod{\mathfrak{q}}$.

Proof Let $\alpha_1, \ldots, \alpha_{\mathrm{N}(\mathfrak{q})}$ be a complete residue system of $\mathfrak{O}$ modulo $\mathfrak{q}$. We may take $\alpha_{\mathrm{N}(\mathfrak{q})} \equiv 0 \pmod{\mathfrak{q}}$. It is plain to check that $\alpha\alpha_1, \ldots, \alpha\alpha_{\mathrm{N}(\mathfrak{q})}$ is again a complete residue system of $\mathfrak{O}$ modulo $\mathfrak{q}$ with $\alpha\alpha_{\mathrm{N}(\mathfrak{q})} \equiv 0 \pmod{\mathfrak{q}}$. Therefore $\alpha^{\mathrm{N}(\mathfrak{q})-1}(\alpha_1 \cdots \alpha_{\mathrm{N}(\mathfrak{q})-1}) = (\alpha\alpha_1) \cdots (\alpha\alpha_{\mathrm{N}(\mathfrak{q})-1}) \equiv \alpha_1 \cdots \alpha_{\mathrm{N}(\mathfrak{q})-1} \pmod{\mathfrak{q}}$. Since $\mathfrak{q}$ is a prime ideal, $\alpha_1 \cdots \alpha_{\mathrm{N}(\mathfrak{q})-1} \notin \mathfrak{q}$, whence the result follows. ◀

We know that a non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}$ contains a non-zero rational integer (Lemma 4.3). $\mathrm{N}(\mathfrak{a})$ is also a rational integer. Let me now relate these two observations.

4.27 Lemma Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}$. Then $\mathrm{N}(\mathfrak{a}) \in \mathfrak{a}$.

Proof The result being obvious for the zero ideal, we consider $\mathfrak{a} \neq 0$ only. Again let $\alpha_1, \ldots, \alpha_{\mathrm{N}(\mathfrak{a})}$ constitute a complete residue system of $\mathfrak{O}$ modulo $\mathfrak{a}$. Then $1 + \alpha_1, \ldots, 1 + \alpha_{\mathrm{N}(\mathfrak{a})}$ is also a complete residue system of $\mathfrak{O}$ modulo $\mathfrak{a}$. Therefore, $\mathrm{N}(\mathfrak{a}) + (\alpha_1 + \cdots + \alpha_{\mathrm{N}(\mathfrak{a})}) = (1 + \alpha_1) + \cdots + (1 + \alpha_{\mathrm{N}(\mathfrak{a})}) \equiv \alpha_1 + \cdots + \alpha_{\mathrm{N}(\mathfrak{a})} \pmod{\mathfrak{a}}$, i.e., $\mathrm{N}(\mathfrak{a}) \equiv 0 \pmod{\mathfrak{a}}$. ◀

For non-zero prime ideals $\mathfrak{q}$ this lemma implies the following:

4.28 Corollary Let $\mathfrak{q}$ be a non-zero prime ideal of $\mathfrak{O}$. Then $\mathrm{N}(\mathfrak{q}) = p^f$ for some $f \in \mathbb{N}$, where p is the unique rational prime contained in $\mathfrak{q}$ (Corollary 4.2).

Proof By Corollary 4.23 $\mathfrak{O}/\mathfrak{q}$ is a finite field, i.e., $\mathrm{N}(\mathfrak{q}) = p^f$ for some $p \in \mathbb{P}$ and $f \in \mathbb{N}$. By Lemma 4.27 $p^f \in \mathfrak{q}$. Let $\mathfrak{q}$ contain the rational prime q. If $q \neq p$, then $\gcd(p^f, q) = 1$ (in $\mathbb{Z}$) implies that $\mathfrak{q}$ is the unit ideal, a contradiction. ◀

Lemma 4.27 has another important consequence.

4.29 Proposition Let $a \in \mathbb{N}$. Then there are only finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}$ with $\mathrm{N}(\mathfrak{a}) = a$.

Proof The ring $\mathfrak{O}/\langle a\rangle$ is finite (Corollary 4.23) and hence contains only finitely many ideals. Now use the one-to-one correspondence of the ideals of $\mathfrak{O}/\langle a\rangle$ with the ideals of $\mathfrak{O}$ containing $\langle a\rangle$ (or equivalently a). ◀

Since norm of elements of $\mathfrak{O}$ is multiplicative, it simply follows that norms of principal ideals of $\mathfrak{O}$ is also multiplicative. We will now show that this multiplicativity continues to hold for arbitrary ideals.

4.30 Proposition Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $\mathfrak{O}$. Then $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$.

Proof The proposition evidently holds for $\mathfrak{a} = 0$ and for $\mathfrak{a} = \mathfrak{O}$. So assume that $\mathfrak{a}$ is a non-zero proper ideal of $\mathfrak{O}$. We first prove the result when $\mathfrak{a} =: \mathfrak{q}$ is prime. Since $\mathrm{N}(\mathfrak{q}\mathfrak{b}) = [\mathfrak{O} : \mathfrak{q}\mathfrak{b}] = [\mathfrak{O} : \mathfrak{b}][\mathfrak{b} : \mathfrak{q}\mathfrak{b}] = \mathrm{N}(\mathfrak{b})[\mathfrak{b} : \mathfrak{q}\mathfrak{b}]$, it is sufficient to show that $\mathrm{N}(\mathfrak{q}) = [\mathfrak{b} : \mathfrak{q}\mathfrak{b}]$.

Let $n := \mathrm{N}(\mathfrak{q}) = [\mathfrak{O} : \mathfrak{q}]$ and let $\alpha_1, \ldots, \alpha_n$ be a complete residue system of $\mathfrak{O}$ modulo $\mathfrak{q}$. We will find $\beta \in \mathfrak{b}$ such that $\beta\alpha_1, \ldots, \beta\alpha_n$ is a complete residue system of $\mathfrak{b}$ modulo $\mathfrak{q}\mathfrak{b}$. First note that $\mathfrak{b} \supsetneqq \mathfrak{q}\mathfrak{b}$. We choose any $\beta \in \mathfrak{b} \setminus \mathfrak{q}\mathfrak{b}$ and want to show that this β has the desired property.

Claim $\beta\alpha_1, \ldots, \beta\alpha_n$ are distinct modulo $\mathfrak{q}\mathfrak{b}$.

Assume not, i.e., $\beta\alpha_i \equiv \beta\alpha_j \pmod{\mathfrak{q}\mathfrak{b}}$ for $i \neq j$, i.e., $\beta\gamma \in \mathfrak{q}\mathfrak{b}$, where $\gamma := \alpha_i - \alpha_j \notin \mathfrak{q}$. Since $\mathfrak{q}$ is maximal, $\mathfrak{q} + \langle\gamma\rangle = \mathfrak{O}$, i.e., $\gamma\delta \equiv 1 \pmod{\mathfrak{q}}$ for some $\delta \in \mathfrak{O}$. Also $\beta \in \mathfrak{b}$ and so $\beta(\gamma\delta - 1) \in \mathfrak{q}\mathfrak{b}$. But $\beta\gamma \in \mathfrak{q}\mathfrak{b}$ and hence $\beta\gamma\delta \in \mathfrak{q}\mathfrak{b}$, so that $\beta = \beta\gamma\delta - \beta(\gamma\delta - 1) \in \mathfrak{q}\mathfrak{b}$, a contradiction to the choice of β.

Claim Let $\xi \in \mathfrak{b}$. Then $\xi \equiv \beta\alpha_i \pmod{\mathfrak{q}\mathfrak{b}}$ for some i.

First note that $\mathfrak{b} \mid \mathfrak{q}\mathfrak{b} + \langle\beta\rangle$ and $\mathfrak{q}\mathfrak{b} + \langle\beta\rangle \mid \mathfrak{q}\mathfrak{b}$. Since $\mathfrak{q}$ is prime and $\mathfrak{q}\mathfrak{b} + \langle\beta\rangle \neq \mathfrak{q}\mathfrak{b}$, we must have $\mathfrak{b} = \mathfrak{q}\mathfrak{b} + \langle\beta\rangle$. Therefore $\xi \equiv \beta\alpha \pmod{\mathfrak{q}\mathfrak{b}}$ for some $\alpha \in \mathfrak{O}$. But $\alpha \equiv \alpha_i \pmod{\mathfrak{q}}$ for some i and $\beta \in \mathfrak{b}$, so that $\beta\alpha \equiv \beta\alpha_i \pmod{\mathfrak{q}\mathfrak{b}}$, i.e., $\xi \equiv \beta\alpha_i \pmod{\mathfrak{q}\mathfrak{b}}$ as claimed.

Now let us come to the general situation $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ for $r \in \mathbb{N}$ and for non-zero primes $\mathfrak{q}_i$. In order to show that $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$ we proceed by induction on r. For $r = 1$ we have the special case discussed above. So assume that $r > 1$ and that the result holds for all ideals $\mathfrak{a}$ having $r - 1$ (or less) prime ideals in the factorization. Then $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_r\mathfrak{b}) = \mathrm{N}(\mathfrak{q}_1)\,\mathrm{N}(\mathfrak{q}_2 \cdots \mathfrak{q}_r\mathfrak{b})$ (by the special case) $= \mathrm{N}(\mathfrak{q}_1)\,\mathrm{N}(\mathfrak{q}_2 \cdots \mathfrak{q}_r)\,\mathrm{N}(\mathfrak{b})$ (by induction) $= \mathrm{N}(\mathfrak{q}_1 \cdots \mathfrak{q}_r)\,\mathrm{N}(\mathfrak{b})$ (by the special case) $= \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$. ◀

The following immediate corollary often comes handy.

4.31 Corollary Let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero ideals of $\mathfrak{O}$. If $\mathfrak{a} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ is the factorization of $\mathfrak{a}$, then $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{q}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{q}_r)^{e_r}$. In particular, if $\mathfrak{a} \mid \mathfrak{b}$, then $\mathrm{N}(\mathfrak{a}) \mid \mathrm{N}(\mathfrak{b})$ (in $\mathbb{Z}$). ◀

Exercises for Section 4.2

1. Let $K := \mathbb{Q}(\sqrt{-5}\,)$. Compute the norms of the following ideals of $\mathfrak{O}_K$: $\langle\sqrt{-5}\,\rangle$, $\langle 1 + \sqrt{-5}\,\rangle$, $\langle 2, 1 + \sqrt{-5}\,\rangle$ and $\langle 3, 1 + \sqrt{-5}\,\rangle$.

2. (Generalized totient function) Let K be a number field and $\mathfrak{a}, \mathfrak{b}$ non-zero ideals of $\mathfrak{O} = \mathfrak{O}_K$.

   (a) Let $\alpha, \beta \in \mathfrak{O}$. Show that if $\alpha \equiv \beta \pmod{\mathfrak{a}}$, then $\gcd(\langle\alpha\rangle, \mathfrak{a}) = \gcd(\langle\beta\rangle, \mathfrak{a})$.

   (b) Let $\phi(\mathfrak{a})$ denote the number of cosets $\alpha + \mathfrak{a}$ such that $\gcd(\langle\alpha\rangle, \mathfrak{a}) = \langle 1\rangle$. Show that if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, then $\phi(\mathfrak{a}\mathfrak{b}) = \phi(\mathfrak{a})\phi(\mathfrak{b})$.

   (c) If $\mathfrak{q}$ is a non-zero prime ideal of $\mathfrak{O}$ and $e \in \mathbb{N}$, show that $\phi(\mathfrak{q}^e) = \mathrm{N}(\mathfrak{q})^e - \mathrm{N}(\mathfrak{q})^{e-1}$.

   (d) If $\mathfrak{a} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ with pairwise distinct non-zero prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ and with $e_1, \ldots, e_r \in \mathbb{N}$, show that $\phi(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}) \displaystyle\prod_{i=1}^{r} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{q}_i)}\right)$.

3. Let K be a number field and $\mathfrak{a}$ a non-zero ideal of $\mathfrak{O} = \mathfrak{O}_K$. Show that the $\phi(\mathfrak{a})$ cosets $\alpha + \mathfrak{a}$ with $\gcd(\langle\alpha\rangle, \mathfrak{a}) = \langle 1\rangle$ form an (Abelian) multiplicative group. We denote this group by $(\mathfrak{O}/\mathfrak{a})^*$. (**Remark:** $(\mathfrak{O}/\mathfrak{a})^*$ is the group of units of the quotient ring $\mathfrak{O}/\mathfrak{a}$.)

4. Show that if $\mathfrak{q}$ is a non-zero prime ideal of $\mathfrak{O}$, then the group $(\mathfrak{O}/\mathfrak{q})^*$ is cyclic.

4.3 Rational primes in number rings

The behavior of rational primes in number rings is an interesting topic of study in algebraic number theory. Recall from Exercise 3.1.6 that a rational prime p congruent to 3 modulo 4 continues to remain prime in the ring $\mathbb{Z}[\mathrm{i}] = \mathfrak{O}_{\mathbb{Q}(\mathrm{i})}$ of Gaussian integers, whereas 2 and primes congruent to 1 modulo 4 split non-trivially in $\mathbb{Z}[\mathrm{i}]$. We know that $\mathbb{Z}[\mathrm{i}]$ is a UFD. Thus splitting or remaining prime of $p \in \mathbb{P}$ makes sense in terms of factorization of p as an element in $\mathbb{Z}[\mathrm{i}]$. Unfortunately all number rings $\mathfrak{O}$ are not UFDs and so we have to talk in terms of the factorization of the ideal $\mathfrak{O}p$.

Let K be a number field of degree d and $\mathfrak{O} := \mathfrak{O}_K$. Consider a rational prime p and denote by $\langle p\rangle$ the ideal $\mathfrak{O}p$ generated by p in $\mathfrak{O}$. Let us use the symbol $\mathfrak{p}$ to denote the (prime) ideal of $\mathbb{Z}$ generated by p. Further let

$$\langle p\rangle = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} \tag{4.2}$$

be the prime factorization of $\langle p\rangle$ with $r \in \mathbb{N}$, with pairwise distinct non-zero prime ideals $\mathfrak{q}_i$ of $\mathfrak{O}$ and with $e_i \in \mathbb{N}$. For each i we have $\langle p\rangle \subseteq \mathfrak{q}_i$, i.e., $p \in \mathfrak{q}_i$, i.e., $\mathfrak{p} = \mathbb{Z} \cap \mathfrak{q}_i$ (Corollary 4.2), i.e., $\mathfrak{q}_i$ lies over $\mathfrak{p}$. Conversely if $\mathfrak{q}$ is an ideal of $\mathfrak{O}$ lying over $\mathfrak{p}$, then $p \in \mathfrak{q}$, i.e., $\langle p\rangle \subseteq \mathfrak{q}$, i.e., $\mathfrak{q} \mid \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$, i.e., $\mathfrak{q} = \mathfrak{q}_i$ for some $i = 1, \ldots, r$. Thus, $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are precisely all the prime ideals of $\mathfrak{O}$ that lie over $\mathfrak{p}$.

By Corollary 4.25 $\mathrm{N}(\langle p\rangle) = p^d$. By Corollary 4.31 each $\mathrm{N}(\mathfrak{q}_i)$ divides p^d and is again a power p^{d_i} of p.

4.32 Definition We define the ramification index of $\mathfrak{q}_i$ over p (or $\mathfrak{p}$) as $e(\mathfrak{q}_i/p) := e_i$. This is the largest $e \in \mathbb{N}$ such that $\mathfrak{q}_i^e$ divides (i.e., contains) $\langle p\rangle$. The integer d_i (where $\mathrm{N}(\mathfrak{q}_i) = p^{d_i}$) is called the inertial degree $d(\mathfrak{q}_i/p)$ of $\mathfrak{q}_i$ over p.

By the multiplicative property of norms we have

$$d = \sum_{i=1}^{r} e_i d_i = \sum_{i=1}^{r} e(\mathfrak{q}_i/p) d(\mathfrak{q}_i/p)\,. \tag{4.3}$$

Let me now introduce some common terms.

4.33 Definition If $r = d$, so that each $e_i = d_i = 1$, we say that the prime p (or $\mathfrak{p}$) splits completely in $\mathfrak{O}$. On the other extreme, if $r = 1$, $e_1 = 1$, $d_1 = d$, then $\langle p\rangle$ is prime in $\mathfrak{O}$ and we say that p is inert in $\mathfrak{O}$. Finally if $e_i > 1$ for some i, we say that the prime p ramifies in $\mathfrak{O}$. If $r = 1$ and $e_1 = d$ (so that $d_1 = 1$), then the prime p is said to be totally ramified in $\mathfrak{O}$.

The following important result is due to Dedekind. Its proof is long and complicated and is omitted here.

4.34 Theorem A rational prime p ramifies in $\mathfrak{O}_K$, if and only if p divides the discriminant Δ_K. In particular, there are only finitely many rational primes that ramify in $\mathfrak{O}_K$. ◀

Though this is not the case in general, let us assume that the ring $\mathfrak{O}$ is monogenic (i.e., $\mathfrak{O} = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathfrak{O}$) and try to compute the explicit factorization (4.2) of $\langle p\rangle$ in $\mathfrak{O}$. In this case $K = \mathbb{Q}(\alpha)$ and we denote by $f(X) \in \mathbb{Z}[X]$ the minimal polynomial of α. We then have $\mathfrak{O} = \mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/\langle f(X)\rangle$.

Let us agree to write the canonical image of any polynomial $g(X) \in \mathbb{Z}[X]$ in $\mathbb{F}_p[X] = \mathbb{Z}[X]/p\mathbb{Z}[X]$ as $\bar{g}(X)$. For the minimal polynomial $f(X) \in \mathbb{Z}[X]$ of α we factorize $\bar{f}(X)$ as

$$\bar{f}(X) = \bar{f}_1(X)^{e_1} \cdots \bar{f}_r(X)^{e_r}$$

with $r, e_1, \ldots, e_r \in \mathbb{N}$ and with pairwise distinct irreducible polynomials $\bar{f}_i \in \mathbb{F}_p[X]$. If $d_i := \deg \bar{f}_i$, then $\sum_{i=1}^r e_i d_i = d$. For each $i = 1, \ldots, r$ choose $f_i(X) \in \mathbb{Z}[X]$ whose reduction modulo p is $\bar{f}_i(X)$. Define the ideals

$$\mathfrak{q}_i := \langle p, f_i(\alpha) \rangle$$

of $\mathfrak{O}$. Since $\mathfrak{O} \cong \mathbb{Z}[X]/\langle f(X) \rangle$, we have $\mathfrak{O}/\langle p \rangle \cong \mathbb{Z}[X]/\langle p, f(X) \rangle \cong \mathbb{F}_p[X]/\langle \bar{f}(X) \rangle$ and $\mathfrak{O}/\mathfrak{q}_i = \mathfrak{O}/\langle p, f_i(\alpha) \rangle \cong \mathbb{Z}[X]/\langle p, f(X), f_i(X) \rangle \cong \mathbb{F}_p[X]/\langle \bar{f}_i(X) \rangle \cong \mathbb{F}_{p^{d_i}}$. Therefore $\mathfrak{q}_i$ are non-zero prime ideals of $\mathfrak{O}$. Moreover $\mathrm{N}(\mathfrak{q}_i) = p^{d_i}$. Thus $\mathrm{N}(\langle p \rangle) = p^d = p^{\sum_{i=1}^r e_i d_i} = \mathrm{N}(\mathfrak{q}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{q}_r)^{e_r} = \mathrm{N}(\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r})$. On the other hand $\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} = \prod_{i=1}^r \langle p, f_i(\alpha) \rangle^{e_i} \subseteq \langle p \rangle$, since $f(\alpha) = 0$ and $f(X) - \prod_{i=1}^r f_i(X)^{e_i} \in p\mathbb{Z}[X]$. Thus we must have $\langle p \rangle = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$, i.e., we have obtained the desired factorization of $\langle p \rangle$.

Let us now concentrate on an example of this explicit factorization.

4.35 Example Let $D \neq 0, 1$ be a square-free integer congruent to 2 or 3 modulo 4. If $K := \mathbb{Q}(\sqrt{D})$, then $\mathfrak{O} = \mathbb{Z}[\sqrt{D}]$ is monogenic. We take an odd rational prime p and compute the factorization of $\langle p \rangle$ in $\mathfrak{O}$. We have to factorize modulo p the polynomial $f(X) := \operatorname{minpoly}_{\sqrt{D}}(X) = X^2 - D$. We consider three cases separately based on the value of the Legendre symbol $\left(\frac{D}{p}\right)$.

Case 1: $\left(\frac{D}{p}\right) = 0$

In this case $p \mid D$, i.e., $\bar{f}(X) = X^2$. Then $\langle p \rangle = \mathfrak{q}^2$, where $\mathfrak{q} := \langle p, \sqrt{D} \rangle$. Thus p (totally) ramifies in $\mathfrak{O}$.

Case 2: $\left(\frac{D}{p}\right) = 1$

Since p is assumed to be an odd prime, the two square roots of D modulo p are distinct. Let δ be an integer with $\delta^2 \equiv D \pmod{p}$. Then $\bar{f}(X) = (X - \delta)(X + \delta)$. In this case $\langle p \rangle = \mathfrak{q}_1 \mathfrak{q}_2$, where $\mathfrak{q}_1 := \langle p, \sqrt{D} - \delta \rangle$ and $\mathfrak{q}_2 := \langle p, \sqrt{D} + \delta \rangle$. Thus p splits (completely) in $\mathfrak{O}$.

Case 3: $\left(\frac{D}{p}\right) = -1$

The polynomial $\bar{f}(X) = X^2 - D$ is irreducible in $\mathbb{F}_p[X]$ and hence $\langle p, f(\sqrt{D}) \rangle = \langle p, 0 \rangle = \langle p \rangle$ remains prime in $\mathfrak{O}$, i.e., p is inert in $\mathfrak{O}$.

Thus the quadratic residuosity of D modulo p dictates the behavior of the prime p in $\mathfrak{O}$.

Let us finally look at the fate of the even prime 2 in $\mathfrak{O}$. If D is even, then $\bar{f}(X) = X^2$ and if D is odd, then $\bar{f}(X) = (X + 1)^2$. In each case 2 ramifies in $\mathfrak{O}$.

Recall from Example 3.22 that $\Delta_K = 4D$. Thus we have a confirmation of the fact that a rational prime p ramifies in $\mathfrak{O}$, if and only if $p \mid \Delta_K$.

Cool! Now why don't you study the behavior of rational primes in $\mathfrak{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[(1 + \sqrt{D})/2]$, where $D \equiv 1 \pmod{4}$ is a square-free integer $\neq 0, 1$? More formally solve Exercise 4.3.2.

Exercises for Section 4.3

1. Let p be a rational prime $\equiv 1 \pmod 4$.

(a) Show that p splits in $\mathbb{Z}[\mathrm{i}]$. (**Hint:** Note that $\left(\frac{-1}{p}\right) = 1$. Now use Example 4.35.)

(b) Show that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. (**Hint:** $\mathbb{Z}[\mathrm{i}]$ is a PID.)

2. Let $D \neq 0, 1$ be a square-free integer, p a rational prime and $\mathfrak{O} = \mathfrak{O}_{\mathbb{Q}(\sqrt{D})}$. Prove the following assertions:

(a) If p is an odd prime, then:

p ramifies in $\mathfrak{O}$, if and only if $\left(\frac{D}{p}\right) = 0$.
p splits in $\mathfrak{O}$, if and only if $\left(\frac{D}{p}\right) = 1$.
p remains inert in $\mathfrak{O}$, if and only if $\left(\frac{D}{p}\right) = -1$.

(b) If $D \equiv 2, 3 \pmod 4$, then 2 ramifies in $\mathfrak{O}$.
If $D \equiv 1 \pmod 8$, then 2 splits in $\mathfrak{O}$.
If $D \equiv 5 \pmod 8$, then 2 remains inert in $\mathfrak{O}$.

3. Let $\alpha := 2^{1/3}$. Show that $\mathfrak{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$. (**Hint:** Look at the minimal polynomial of α^2.)

4. Let $K := \mathbb{Q}(2^{1/3})$.

(a) Find the smallest rational prime that ramifies in $\mathfrak{O}_K$.

(b) Find the smallest rational prime that does not ramify in $\mathfrak{O}_K$.

(c) Find the smallest rational prime that remains inert in $\mathfrak{O}_K$.

(d) Find the smallest rational prime that splits in $\mathfrak{O}_K$.

(**Remark:** You may use a computational number theory package (like PARI).)

5. Let p be an odd prime, $n \in \mathbb{N}$, ω_{p^n} a primitive p^n-th root of unity and $\mathfrak{O} = \mathfrak{O}_{\mathbb{Q}(\omega_{p^n})} = \mathbb{Z}[\omega_{p^n}]$. Show that the only rational prime that ramifies in $\mathfrak{O}$ is p. (**Hint:** Either use the unproven Theorem 4.34 in tandem with Exercise 3.3.3 or use Exercise 3.1.5(e).)

*** 6.** Let $n \in \mathbb{N}$, $n \geqslant 3$. Show that no rational prime remains inert in $\mathfrak{O}_{\mathbb{Q}(\omega_{2^n})} = \mathbb{Z}[\omega_{2^n}]$, where ω_{2^n} is a primitive 2^n-th root of unity. (**Hint:** Use the fact from elementary number theory that -1 is a quadratic residue modulo a (rational) prime p, if and only if $p = 2$ or $p \equiv 1 \pmod 4$.)

4.4 Ideal classes

A number ring $\mathfrak{O} = \mathfrak{O}_K$ is not necessarily a PID. We have seen, however, that $\mathfrak{O}$ is not far away from a PID in the sense that every ideal of $\mathfrak{O}$ is generated by at most two elements. There is another sense in which this comment holds. For this we look at the set $\mathcal{F} = \mathcal{F}_K$ of all non-zero fractional ideals of K. We proved that $\mathcal{F}$ is an (Abelian) group under multiplication. By Lemma 4.9 every fractional ideal $\mathfrak{a} \in \mathcal{F}$ is finitely generated as an $\mathfrak{O}$-module. Consider the set $\mathcal{P}$ of all principal fractional ideals of $\mathfrak{O}$, i.e., those $\mathfrak{a} \in \mathcal{F}$ that are cyclic $\mathfrak{O}$-modules, i.e., that are of the form $\mathfrak{O}x$ for some non-zero $x \in K = \mathrm{Q}(\mathfrak{O})$. It is evident that $\mathcal{P}$ is a subgroup of $\mathcal{F}$.

4.36 Definition The quotient group $\mathcal{F}/\mathcal{P}$ is called the class group of K (or of $\mathfrak{O}$) and is denoted by $\mathcal{H} = \mathcal{H}_K$. The cardinality of $\mathcal{H}$ is called the class number of K (or of $\mathfrak{O}$) and is denoted by $h = h_K$. The equivalence classes in $\mathcal{F}/\mathcal{P}$ are called ideal classes of K. Two (fractional) ideals $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}$ are called equivalent, if they belong to the same ideal class of K, or equivalently if $\mathfrak{a} = (\mathfrak{O}x)\mathfrak{b}$ for some $x \in K^*$.

I will now prove that the class number h_K is finite, i.e., in $\mathcal{F}$ the proportion of principal fractional ideals is positive (viz. non-zero). Obviously $\mathfrak{O}$ is a PID (or equivalently a UFD), if and only if $h_K = 1$. But in the general case there are not too many non-principal fractional ideals for each principal fractional ideal. This is the sense in which I said that the deviation of $\mathfrak{O}$ from a PID is not too much.

Let us now concentrate on the proof of the finiteness of the class number h. I start with a lemma.

4.37 Lemma For every non-zero integral ideal $\mathfrak{a}$ of $\mathfrak{O}$ there exists a non-zero $\alpha \in \mathfrak{a}$ with $|\mathrm{N}(\alpha)| \leqslant C_K \mathrm{N}(\mathfrak{a})$, where C_K is a constant that depends only on K.

Proof Choose an integral basis $\beta_1, \ldots, \beta_d$ of $\mathfrak{O}$ and denote $n := \mathrm{N}(\mathfrak{a})$ and $t := \left\lfloor n^{1/d} \right\rfloor$. Since $(t+1)^d > n$, the elements $\sum_{i=1}^d r_i \beta_i$, $r_i \in \mathbb{Z}$, $0 \leqslant r_i \leqslant t$, can not be all distinct modulo $\mathfrak{a}$. Thus there exists a non-zero $\alpha := \sum_{i=1}^d s_i \beta_i \in \mathfrak{a}$ with $s_i \in \mathbb{Z}$ and $|s_i| \leqslant t$. Let $\sigma_1, \ldots, \sigma_d$ denote the complex embeddings of K. Then $\sigma_j(\alpha) = \sum_{i=1}^d s_i \sigma_j(\beta_i)$, so that $|\sigma_j(\alpha)| \leqslant \sum_{i=1}^d |s_i||\sigma_j(\beta_i)| \leqslant t \sum_{i=1}^d |\sigma_j(\beta_i)|$. Therefore $|\mathrm{N}(\alpha)| = \prod_{j=1}^d |\sigma_j(\alpha)| \leqslant t^d C_K \leqslant n C_K = C_K \mathrm{N}(\mathfrak{a})$, where $C_K := \prod_{j=1}^d \sum_{i=1}^d |\sigma_j(\beta_i)|$. ◀

4.38 Corollary Every ideal class $\mathfrak{C}$ of K contains an integral ideal of norm $\leqslant C_K$, where C_K is a constant depending only on K.

Proof Choose any fractional ideal $\mathfrak{a}$ in the inverse class $\mathfrak{C}^{-1} \in \mathcal{H}$. By definition $\langle a \rangle \mathfrak{a} \subseteq A$ for some $0 \neq a \in \mathfrak{O}$. But then $\langle a \rangle \mathfrak{a}$ is an integral ideal of $\mathfrak{O}$ and also belongs to $\mathfrak{C}^{-1}$. Thus we may assume without loss of generality that $\mathfrak{a}$ itself is an integral ideal of $\mathfrak{O}$.

By Lemma 4.37 there exists a non-zero $\alpha \in \mathfrak{a}$ with $|\mathrm{N}(\alpha)| \leqslant C_K \mathrm{N}(\mathfrak{a})$ for some constant C_K depending only on K. Since $\alpha \in \mathfrak{a}$, we have $\mathfrak{a} \mid \langle \alpha \rangle$, i.e., $\langle \alpha \rangle = \mathfrak{a}\mathfrak{b}$ for some non-zero integral ideal $\mathfrak{b}$ of $\mathfrak{O}$. Now $\mathfrak{b} = \langle \alpha \rangle \mathfrak{a}^{-1} \in \mathfrak{C}$. Furthermore $\mathrm{N}(\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})/\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}\mathfrak{b})/\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\langle \alpha \rangle)/\mathrm{N}(\mathfrak{a}) = |\mathrm{N}(\alpha)|/\mathrm{N}(\mathfrak{a}) \leqslant C_K$. ◀

4.39 Theorem The class number $h = h_K$ of a number field K is finite.

Proof Assume not. Then by Corollary 4.38 there exists an infinite number of (non-zero) integral ideals of $\mathfrak{O}$ with norm $\leqslant C_K$, where C_K is a constant depending on K. But this contradicts Proposition 4.29. ◀

Determining the class number of a number field K is an interesting computational problem of algebraic number theory and involves a heavy usage of the theory developed throughout this chapter. The basic steps are as follows.

Step 1: Compute the constant $C_K = \prod_{j=1}^d \sum_{i=1}^d |\sigma_j(\beta_i)|$ of Lemma 4.37. By Corollary 4.38 it is sufficient to concentrate only on the non-zero integral ideals of $\mathfrak{O}$ with norm $\leqslant C_K$.

Step 2: For each rational prime $p \leqslant C_K$ compute all the prime ideals of $\mathfrak{O}$ which contain p. This can be done by computing the factorization of $\langle p \rangle$ in $\mathfrak{O}$. For the case that $\mathfrak{O}$ is monogenic this can be performed by the procedure described in Section 4.3.

Step 3: Combine the prime ideals of Step 2 to generate all the non-zero integral ideals of $\mathfrak{O}$ having norms $\leqslant C_K$. The theory of unique factorization of ideals and of multiplicative nature of norms helps here.

Step 4: Determine a maximal list L of pairwise non-equivalent ideals among those obtained in Steps 2 and 3. Then $h = |L|$.

4.40 Example Let us compute the class number of $K := \mathbb{Q}(\sqrt{-5})$. Since $-5 \equiv 3 \pmod 4$, we have $\mathfrak{O} := \mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$. The class of an ideal $\mathfrak{a}$ will be denoted by $[\mathfrak{a}]$ and equivalence of two ideals by $\mathfrak{a} \sim \mathfrak{b}$. These notations are as in the case of a general equivalence relation.

Step 1: Compute C_K.

The complex embeddings of K are $\sigma_1 = \mathrm{id}_K$ and $\sigma_2 : \sqrt{-5} \mapsto -\sqrt{-5}$. Thus $C_K = (1+\sqrt{5}\,)^2 = 10.472\ldots$. Thus it is sufficient to look at the non-zero integral ideals of $\mathfrak{O}$ of norms $\leqslant 10$.

Step 2: Factorize $\langle p \rangle$ for $p \in \{2, 3, 5, 7\}$.

We use the results of Example 4.35. The factorizations are listed in the following table.

p	Factorization of $\langle p \rangle$	Norm
2	$\langle 2 \rangle = \mathfrak{q}_2^2$, where $\mathfrak{q}_2 = \langle 2, 1+\sqrt{-5}\,\rangle$.	$\mathrm{N}(\mathfrak{q}_2) = 2$
3	$\left(\frac{-5}{3}\right) = \left(\frac{1}{3}\right) = 1$ and hence $\langle 3 \rangle = \mathfrak{q}_3\mathfrak{q}_3'$, where $\mathfrak{q}_3 = \langle 3, 1+\sqrt{-5}\,\rangle$ and $\mathfrak{q}_3' = \langle 3, -1+\sqrt{-5}\,\rangle$.	$\mathrm{N}(\mathfrak{q}_3) = \mathrm{N}(\mathfrak{q}_3') = 3$
5	$\langle 5 \rangle = \mathfrak{q}_5^2$, where $\mathfrak{q}_5 = \langle 5, \sqrt{-5}\,\rangle = \langle \sqrt{-5}\,\rangle$.	$\mathrm{N}(\mathfrak{q}_5) = 5$
7	$\left(\frac{-5}{7}\right) = \left(\frac{2}{7}\right) = (-1)^{(7^2-1)/8} = 1$ and therefore $\langle 7 \rangle = \mathfrak{q}_7\mathfrak{q}_7'$, where $\mathfrak{q}_7 = \langle 7, 3+\sqrt{-5}\,\rangle$ and $\mathfrak{q}_7' = \langle 7, -3+\sqrt{-5}\,\rangle$. (The square roots of -5 modulo 7 are ± 3.)	$\mathrm{N}(\mathfrak{q}_7) = \mathrm{N}(\mathfrak{q}_7') = 7$

It turned out that for each rational prime $p \leqslant 10$ the prime ideals of $\mathfrak{O}$ occurring in the factorization of $\langle p \rangle$ have prime norms p. This is not the general case however. For example, $\left(\frac{-5}{11}\right) = -1$, so that 11 remains inert in $\mathfrak{O}$, i.e., $\langle 11 \rangle$ is a prime ideal of $\mathfrak{O}$ and has norm $11^2 = 121$.

Step 3: Find non-prime ideals of norms $n \leqslant 10$.

n	Ideals of norm n
1	$\mathfrak{a}_1 = \mathfrak{O} = \langle 1 \rangle$
4	$\mathfrak{a}_4 = \mathfrak{q}_2^2$
6	$\mathfrak{a}_6 = \mathfrak{q}_2\mathfrak{q}_3$ and $\mathfrak{a}_6' = \mathfrak{q}_2\mathfrak{q}_3'$
8	$\mathfrak{a}_8 = \mathfrak{q}_2^3$
9	$\mathfrak{a}_9 = \mathfrak{q}_3^2$, $\mathfrak{a}_9' = \mathfrak{q}_3'^{\,2}$ and $\mathfrak{a}_9'' = \mathfrak{q}_3\mathfrak{q}_3'$
10	$\mathfrak{a}_{10} = \mathfrak{q}_2\mathfrak{q}_5$

Step 4: Find the list L of pairwise non-equivalent ideals of norms $\leqslant 10$.

This is the most non-trivial part of the whole business. Let us first insert in L all the ideals found in Steps 2 and 3, i.e., we start with with $L = (\mathfrak{a}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_3', \mathfrak{a}_4, \mathfrak{q}_5, \mathfrak{a}_6, \mathfrak{a}_6', \mathfrak{q}_7, \mathfrak{q}_7', \mathfrak{a}_8, \mathfrak{a}_9, \mathfrak{a}_9', \mathfrak{a}_9'', \mathfrak{a}_{10})$. We will later throw away one of $\mathfrak{a}$ and $\mathfrak{b}$ whenever we detect $\mathfrak{a} \sim \mathfrak{b}$.

Let us plan to keep $\mathfrak{a}_1 = \mathfrak{O}$ in L and throw away all other principal ideals from L. By simple inspection $\mathfrak{q}_5 = \langle \sqrt{-5}\,\rangle$, $\mathfrak{a}_4 = \langle 2 \rangle$ $\mathfrak{a}_9'' = \langle 3 \rangle$ are principal ideals. Let us now check if $\mathfrak{q}_2 = \langle a + b\sqrt{-5}\,\rangle$ for some $a, b \in \mathbb{Z}$. If so, then $|\mathrm{N}(a+b\sqrt{-5}\,)| = a^2 + 5b^2 = \mathrm{N}(\mathfrak{q}_2) = 2$. There are no integer values of a and b for which $a^2 + 5b^2 = 2$. Therefore $\mathfrak{q}_2$ is not principal. In a similar manner we see that $\mathfrak{q}_3, \mathfrak{q}_3', \mathfrak{q}_7, \mathfrak{q}_7', \mathfrak{a}_8, \mathfrak{a}_{10}$ are all non-principal. But $\mathfrak{a}_8 = \mathfrak{q}_2^3 = \langle 2 \rangle \mathfrak{q}_2 \sim \mathfrak{q}_2$ and $\mathfrak{a}_{10} = \mathfrak{q}_2\mathfrak{q}_5 = \langle \sqrt{-5}\,\rangle \mathfrak{q}_2 \sim \mathfrak{q}_2$. Thus the list L can be shortened to $(\mathfrak{a}_1, \mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_3', \mathfrak{a}_6, \mathfrak{a}_6', \mathfrak{q}_7, \mathfrak{q}_7', \mathfrak{a}_9, \mathfrak{a}_9')$.

In order to detect relations among the remaining members of L we look at principal ideals of $\mathfrak{O}$ having small norms, i.e., ideals of the form $\mathfrak{a}_{a,b} := \langle a + b\sqrt{-5}\,\rangle$ for integers a, b of small absolute values. We have $\mathrm{N}(\mathfrak{a}_{a,b}) = |\mathrm{N}(a + b\sqrt{-5}\,)| = a^2 + 5b^2$. Consider $a = 1$, $b = \pm 1$. Then $\mathrm{N}(\mathfrak{a}_{1,1}) = \mathrm{N}(\mathfrak{a}_{1,-1}) = 6$ and it is an easy check that $\mathfrak{a}_{1,1} \neq \mathfrak{a}_{1,-1}$. The only ideals of $\mathfrak{O}$ of norm 6 are $\mathfrak{a}_6$ and $\mathfrak{a}_6'$ and so they must be the same as $\mathfrak{a}_{1,1}$ and $\mathfrak{a}_{1,-1}$ (not necessarily in that order) and are therefore principal and should be discarded from L. Furthermore since $\mathfrak{q}_2^2$ is principal, we have $[\mathfrak{q}_2^2] = [\mathfrak{q}_2]^2 = [\mathfrak{O}]$, i.e., $[\mathfrak{q}_2^{-1}] = [\mathfrak{q}_2]^{-1} = [\mathfrak{q}_2]$. Hence, $\mathfrak{q}_3 = \mathfrak{q}_2^{-1}(\mathfrak{q}_2\mathfrak{q}_3) \sim \mathfrak{q}_2^{-1} \sim \mathfrak{q}_2$. Similarly $\mathfrak{q}_3' \sim \mathfrak{q}_2$. So we delete $\mathfrak{q}_3$ and $\mathfrak{q}_3'$ also from L.

Likewise looking at the ideals $\mathfrak{a}_{3,1}$ and $\mathfrak{a}_{3,-1}$ of norm 14 reveals that both $\mathfrak{q}_7$ and $\mathfrak{q}_7'$ are equivalent to $\mathfrak{q}_2$ and hence should be removed from L.

Finally consider the ideals $\mathfrak{a}_{2,1}$ and $\mathfrak{a}_{2,-1}$ of norm 9. All the ideals of $\mathfrak{O}$ of norm 9 are $\mathfrak{a}_9$, $\mathfrak{a}_9'$ and $\mathfrak{a}_9''$. But neither of $\mathfrak{a}_{2,1}$ and $\mathfrak{a}_{2,-1}$ can be equal to $\mathfrak{a}_9'' = \mathfrak{q}_3\mathfrak{q}_3' = \langle 3 \rangle$, since 3 is not associate to $2 \pm \sqrt{-5}$. Hence $\mathfrak{a}_{2,1}$ and $\mathfrak{a}_{2,-1}$ must be the same as the ideals $\mathfrak{a}_9$ and $\mathfrak{a}_9'$ (again not necessarily in that order), i.e., $\mathfrak{a}_9$ and $\mathfrak{a}_9'$ are both principal and should be rejected as candidates of L.

So we are left with a very short list $L = (\mathfrak{a}_1, \mathfrak{q}_2)$. Since $\mathfrak{q}_2$ has been shown to be non-principal, this is the desired list of pairwise non-equivalent ideals of norm $\leqslant 10$.

Thus the class number of $\mathbb{Q}(\sqrt{-5}\,)$ is 2. In particular, $\mathbb{Z}[\sqrt{-5}\,]$ is not a UFD (nor a PID nor an ED). In fact, 5 is the smallest of the square-free integers $D \geqslant 1$ for which $\mathfrak{O}_{\mathbb{Q}(\sqrt{-D}\,)}$ is not a UFD. On the other hand, 10 is the smallest of the square-free integers $D > 1$ for which $\mathfrak{O}_{\mathbb{Q}(\sqrt{D}\,)}$ is not a UFD. Both these assertions can be checked by routinely computing the class numbers of the fields $\mathbb{Q}(\sqrt{D}\,)$ for small (positive and negative) square-free integer values D. The table in the next page summarizes the class numbers h_+ and h_- respectively of $\mathbb{Q}(\sqrt{D}\,)$ and $\mathbb{Q}(\sqrt{-D}\,)$ for some small positive square-free integers D.[1]

It can be shown (not easily though) that the only square-free values of $D < 0$ for which the (imaginary) quadratic field $\mathbb{Q}(\sqrt{D}\,)$ is a UFD are $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$. Out of these the only values of D for which $\mathbb{Q}(\sqrt{D}\,)$ is also an ED are $-1, -2, -3, -7, -11$.

The list of ideals available from Steps 2 and 3 of the above procedure can be shortened and the subsequent Step 4 can be sped up considerably, if better values of the bound C_K of Lemma 4.37 can be made available. The way we proved Lemma 4.37 gave the formula $C_K = \prod_{j=1}^{d} \sum_{i=1}^{d} |\sigma_j(\beta_i)|$. While this value was theoretically sufficient for the proof of Theorem 4.39, exercising a little more care and involvement allows one to get better formulas for C_K. For example, the *Minkowski bound* allows us to choose the value

$$M_K = \frac{d!}{d^d}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|} \tag{4.4}$$

for a field K of degree d, signature (r_1, r_2) and discriminant Δ_K. For Example 4.40 this shows that it is sufficient to consider all ideals of norms $\leqslant M_K = 2.847\ldots$. This means that we could have started with $L = (\mathfrak{a}_1, \mathfrak{q}_2)$. Proving that $\mathfrak{q}_2$ is not principal would have been sufficient for computing $h = 2$.

[1] This table has been generated by post-processing the output of the following GP-PARI program:

```
for (D=2,1000, \
     if (issquarefree(D), \
          if ((D%4)==1, print1(D,quadclassunit(D)), print1(D,quadclassunit(4*D))); \
          print1 (” AND ”); \
          if ((–D%4)==1, print(–D,quadclassunit(–D)), print(–D,quadclassunit(–4*D)))))
```

The routine quadclassunit takes the discriminant as the input and produces the class number along with some other information. Well! GP-PARI, developed by Henri Cohen and his team, is indeed a very powerful and efficient package for computational algebraic number theory. It is downloadable freely from the Internet. Also look at Cohen's book on computational algebraic number theory (GTM #138, Springer-Verlag, 1993).

Table of class numbers: $h_+ = h_{\mathbb{Q}(\sqrt{D})}$ and $h_- = h_{\mathbb{Q}(\sqrt{-D})}$

D	h_+	h_-	D	h_+	h_-	D	h_+	h_-	D	h_+	h_-	D	h_+	h_-	D	h_+	h_-	D	h_+	h_-	D	h_+	h_-	D	h_+	h_-
1	–	1	110	2	12	221	2	16	334	1	12	446	1	32	559	2	16	670	2	12	782	2	24	897	4	16
2	1	1	111	2	8	222	2	12	335	2	18	447	2	14	561	2	16	671	2	30	785	6	16	898	6	12
3	1	1	113	1	8	223	3	7	337	1	8	449	1	20	562	2	8	673	1	12	786	6	16	899	6	14
5	1	2	114	2	8	226	8	8	339	2	6	451	2	6	563	1	9	674	4	24	787	1	5	901	4	24
6	1	2	115	2	2	227	1	5	341	1	28	453	1	12	565	2	12	677	1	30	789	1	32	902	2	28
7	1	1	118	1	6	229	3	10	345	2	8	454	1	14	566	1	30	678	2	20	790	2	16	903	4	16
10	2	2	119	2	10	230	2	20	346	6	10	455	4	20	569	1	32	679	2	18	791	4	32	905	4	24
11	1	1	122	2	10	231	4	12	347	1	5	457	1	8	570	4	16	681	1	20	793	4	8	906	6	28
13	1	2	123	2	2	233	1	12	349	1	14	458	2	26	571	1	5	682	2	12	794	2	42	907	1	3
14	1	4	127	1	5	235	6	2	353	1	16	461	1	30	573	1	16	683	1	5	795	4	4	910	8	16
15	2	2	129	1	12	237	1	12	354	2	16	462	4	8	574	6	16	685	2	12	797	1	30	911	1	31
17	1	4	130	4	4	238	2	8	355	2	4	463	1	7	577	7	8	687	2	12	798	4	16	913	1	12
19	1	1	131	1	5	239	1	15	357	2	8	465	2	16	579	4	8	689	4	40	799	8	16	914	4	36
21	1	4	133	1	4	241	1	12	358	1	6	466	2	8	581	1	28	690	4	16	802	2	12	915	4	8
22	1	2	134	1	14	246	2	12	359	3	19	467	1	7	582	4	16	691	1	5	803	2	10	917	1	20
23	1	3	137	1	8	247	2	6	362	2	18	469	3	16	583	2	8	694	1	10	805	2	16	919	1	19
26	2	6	138	2	8	249	1	12	365	2	20	470	2	20	586	2	18	695	2	24	806	2	28	921	1	20
29	1	6	139	1	3	251	1	7	366	2	12	471	2	16	587	1	7	697	6	8	807	2	14	922	2	18
30	2	4	141	1	8	253	1	4	367	1	9	473	3	12	589	1	16	698	2	26	809	1	32	923	2	10
31	1	3	142	3	4	254	3	16	370	4	12	474	2	20	590	2	20	699	2	10	811	1	7	926	1	40
33	1	4	143	2	10	255	4	12	371	2	8	478	1	8	591	2	22	701	1	34	813	1	12	929	1	36
34	2	4	145	4	8	257	3	16	373	1	10	479	1	25	593	1	24	703	2	14	814	2	12	930	4	24
35	2	2	146	2	16	258	2	8	374	2	28	481	2	16	595	4	4	705	2	24	815	2	30	933	1	16
37	1	2	149	1	14	259	2	4	377	2	16	482	2	20	597	1	12	706	4	24	817	5	12	934	3	26
38	1	6	151	1	7	262	1	6	379	1	3	483	4	4	598	2	8	707	2	6	818	4	28	935	4	28
39	2	4	154	2	8	263	1	13	381	1	20	485	2	20	599	1	25	709	1	10	821	1	30	937	1	20
41	1	8	155	2	4	265	2	8	382	1	8	487	1	7	601	1	20	710	2	32	822	2	20	938	2	16
42	2	4	157	1	6	266	2	20	383	1	17	489	1	20	602	2	24	713	1	24	823	1	9	939	4	8
43	1	1	158	1	8	267	2	2	385	2	8	491	1	9	606	2	12	714	4	24	826	2	12	941	1	46
46	1	4	159	2	10	269	1	22	386	2	20	493	2	12	607	1	13	715	4	4	827	1	7	942	2	12
47	1	5	161	1	16	271	1	11	389	1	22	494	2	28	609	2	16	717	1	16	829	1	22	943	4	16
51	2	2	163	1	1	273	2	8	390	4	16	497	1	24	610	4	12	718	1	12	830	2	20	946	2	16
53	1	6	165	2	8	274	4	12	391	2	14	498	2	8	611	2	10	719	1	31	831	2	28	947	1	5
55	2	4	166	1	10	277	1	6	393	1	12	499	5	3	613	1	10	721	1	16	834	2	16	949	2	12
57	1	4	167	1	11	278	1	14	394	2	10	501	1	16	614	1	34	723	4	4	835	2	6	951	2	26
58	2	2	170	4	12	281	1	20	395	2	8	502	1	14	615	4	20	727	5	13	838	1	14	953	1	32
59	1	3	173	1	14	282	2	8	397	1	6	503	1	21	617	1	12	730	12	12	839	3	33	955	2	4
61	1	6	174	2	12	283	1	3	398	1	20	505	4	8	618	2	12	731	4	12	842	6	26	957	2	16
62	1	8	177	1	4	285	2	16	399	8	16	506	6	28	619	1	5	733	3	14	843	2	6	958	1	16
65	2	8	178	2	8	286	2	12	401	5	20	509	1	30	622	1	12	734	1	40	849	1	28	959	4	36
66	2	8	179	1	5	287	2	14	402	2	16	510	4	16	623	2	22	737	1	20	851	2	10	962	4	28
67	1	1	181	1	10	290	4	20	403	2	2	511	2	14	626	4	36	739	1	5	853	1	10	965	2	44
69	1	8	182	2	12	291	4	4	406	2	16	514	4	16	627	4	4	741	2	24	854	2	44	966	4	24
70	2	4	183	2	8	293	1	18	407	2	16	515	2	6	629	2	36	742	2	8	857	1	32	967	1	11
71	1	7	185	2	16	295	2	8	409	1	16	517	1	12	631	1	13	743	1	21	858	4	16	969	2	24
73	1	4	186	2	12	298	2	6	410	4	16	518	2	16	633	1	20	745	2	16	859	1	7	970	4	12
74	2	10	187	2	2	299	2	8	411	2	6	519	2	18	634	2	14	746	2	26	861	2	24	971	1	15
77	1	8	190	2	4	301	1	8	413	1	20	521	1	32	635	2	10	749	1	32	862	1	8	973	1	12
78	2	4	191	1	13	302	1	12	415	2	10	523	1	5	638	2	20	751	1	15	863	1	21	974	1	36
79	3	5	193	1	4	303	2	10	417	1	12	526	1	12	641	1	28	753	1	12	865	2	16	977	1	20
82	4	4	194	2	20	305	2	16	418	2	8	527	2	18	642	2	16	754	4	20	866	2	44	978	2	24
83	1	3	195	4	4	307	1	3	419	1	9	530	4	28	643	1	3	755	2	12	869	1	32	979	4	8
85	2	4	197	1	10	309	1	12	421	1	10	533	2	12	645	2	16	757	1	10	870	8	16	982	5	10
86	1	10	199	1	9	310	2	8	422	1	10	534	2	20	646	8	16	758	1	22	871	2	22	983	1	27
87	2	6	201	1	12	311	1	19	426	2	24	535	2	14	647	1	23	759	4	24	874	6	20	985	6	24
89	1	12	202	2	6	313	1	8	427	6	2	537	1	12	649	1	20	761	3	40	877	1	10	986	4	44
91	2	2	203	2	4	314	2	26	429	2	16	538	2	10	651	4	8	762	2	12	878	1	20	987	4	8
93	1	4	205	2	8	317	1	10	430	2	12	541	1	10	653	1	14	763	2	4	879	2	22	989	1	36
94	1	8	206	1	20	318	2	12	431	1	21	542	1	24	654	2	28	766	1	24	881	1	40	991	1	17
95	2	8	209	1	20	319	2	10	433	1	12	543	2	12	655	2	12	767	2	22	883	1	3	993	3	12
97	1	4	210	4	8	321	3	20	434	4	24	545	2	32	658	4	8	769	1	20	885	2	24	994	8	16
101	1	14	211	1	3	322	4	8	435	4	4	546	4	24	659	3	11	770	4	32	886	1	18	995	2	8
102	2	4	213	1	8	323	4	4	437	1	20	547	1	3	661	1	18	771	2	6	887	1	29	997	1	14
103	1	5	214	1	6	326	3	22	438	4	8	551	2	26	662	1	22	773	1	26	889	1	16	998	1	26
105	2	8	215	2	14	327	2	12	439	5	15	553	1	8	663	4	16	777	4	16	890	4	24			
106	2	6	217	1	8	329	1	24	442	8	8	554	2	22	665	2	24	778	2	14	893	1	28			
107	1	3	218	2	10	330	4	8	443	3	5	555	4	4	667	2	4	779	2	10	894	6	28			
109	1	6	219	4	4	331	1	3	445	4	8	557	1	18	669	1	12	781	1	20	895	6	16			

Exercises for Section 4.4

1. Let h be the class number of a number field K and let $m \in \mathbb{N}$ be coprime to h. If $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero integral ideals of $\mathfrak{O}_K$ such that the ideal classes of $\mathfrak{a}^m$ and $\mathfrak{b}^m$ are the same, show that the ideal classes of $\mathfrak{a}$ and $\mathfrak{b}$ are also the same. (**Hint:** By Lagrange's theorem $\mathfrak{a}^h$ and $\mathfrak{b}^h$ are principal.) In particular, if $\mathfrak{a}^m$ is principal, then so is $\mathfrak{a}$.

2. Demonstrate that $\mathfrak{O}_K$ is a PID, if and only if all *prime* ideals of norms $\leqslant C_K$ are principal, where C_K is a constant depending on the field K.

3. Let $\mathfrak{a}$ be an integral ideal of $\mathfrak{O}_K$ and let $\alpha \in \mathfrak{a}$ satisfy $\mathrm{N}(\mathfrak{a}) = |\mathrm{N}(\alpha)|$. Show that $\mathfrak{a} = \langle \alpha \rangle$.

4. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two non-zero integral ideals of $\mathfrak{O}$.

(a) Show that $\mathfrak{a} \sim \mathfrak{b}$, if and only if there exist non-zero $\alpha, \beta \in \mathfrak{O}$ with $\langle \alpha \rangle \mathfrak{a} = \langle \beta \rangle \mathfrak{b}$.

* **(b)** Prove or disprove: $\mathfrak{a} \sim \mathfrak{b}$, if and only if there exists a non-zero $\gamma \in \mathfrak{O}$ with $\mathfrak{a} = \langle \gamma \rangle \mathfrak{b}$.

5. (a) Find all quadratic number fields K for which $-8 \leqslant \Delta_K \leqslant 13$.

(b) Using the Minkowski bound conclude that all the fields of Part (a) are UFDs.

6. Compute the class number of $\mathbb{Q}(\sqrt{-6}\,)$. (**Remark:** Use the formula for C_K as in Lemma 4.37.)

7. Show that the generalized Bachet equation $y^2 = x^3 - n$ has no (rational) integer solutions for $n = 6$. (**Hint:** Work in $\mathbb{Z}[\sqrt{-6}\,]$. Also look at Exercise 3.3.10.)

8. Compute the class number of $\mathbb{Q}(\sqrt{-23}\,)$. (**Remark:** You should better use the Minkowski bound.)