Chapter 2

Ideals

For the whole chapter, K is a number field of degree n and $\mathcal{O} = \mathcal{O}_K$ is its ring of integers.

2.1 Introduction

Historically, experience with unique prime factorization of integers led mathematicians in the early days of algebraic number theory to a general intuition that factorization of algebraic integers into primes should also be unique. A likely reason for this misconception is the actual definition of what is a prime number. The familiar definition is that a prime number is a number which is divisible only by 1 and itself. Since units in $\mathbb{Z}$ are ± 1, this definition can be rephrased as: if $p = ab$, then one of a or b must be a unit. Equivalently over $\mathbb{Z}$, a prime number p satisfies that if $p|ab$, then $p|a$ or $p|b$. However, these two definitions are not equivalent anymore over general rings of integers. In fact, the second property is actually stronger, and if one can get a factorization with "primes" satisfying this property, then factorization will be unique, which is not the case for "primes" satisfying the first property. To distinguish these two definitions, we say in modern terminology that a number satisfying the first property is *irreducible*, while one satisfying the second property is *prime*.

Consider for example $\mathbb{Z}[\sqrt{-6}]$. We have that

$$6 = 2 \cdot 3 = -\sqrt{-6}\sqrt{-6}.$$

We get two factorizations into irreducibles (we have a factorization but it is not unique). However this is not a factorization into primes, since $\sqrt{-6}$ divides $2 \cdot 3$ but $\sqrt{-6}$ does not divide 2 and does not divide 3 either. So in the case where primes and irreducibles are different, we now have to think what we are looking for when we say factorization. When we attempt to factorize an element x in a domain D, we naturally mean proper factors a, b such that $x = ab$, and if either

of these factors can be further decomposed, we go on. That means, we look for writing

$$x = a_1 a_2 \dots a_n$$

into factors that cannot be reduced any further. The definition of irreducible captures what it means for the factorization to terminate: one of the term has to be a unit.

Thus what we are interested in is to understand the factorization into *irreducibles* inside rings of integers. Before starting, let us make a few more remarks. Note first that this factorization into irreducibles may not always be possible in general rings, since the procedure may continue indefinitely. However the procedure does stop for rings of integers. This comes from the fact that rings of integers are, again in modern terminology, what we call *noetherian rings*. The big picture can finally be summarized as follows:

- In general rings, factorization even into irreducibles may not be possible.
- In rings of integers, factorization into irreducibles is always possible, but may not be unique.
- For rings of integers which furthermore have a generalized Euclidean division, then the notions of prime and irreducible are equivalent, thus factorization is unique.

Let us now get back to the problem we are interested in, namely, factorization into product of irreducibles in rings of integers.

Example 2.1. Let $K = \mathbb{Q}(\sqrt{-5})$ be a quadratic number field, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, since $d \equiv 3 \pmod 4$. Let us prove that we do not have a unique factorization into product of irreducibles in $\mathbb{Z}[\sqrt{-5}]$. We have that

$$21 = 7 \cdot 3 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

with $3, 7, 1 \pm 2\sqrt{-5}$ irreducible. Let us show for example that 3 is irreducible. Let us write

$$3 = \alpha\beta,\ \alpha, \beta \in \mathcal{O}_K.$$

We need to see that either α or β is a unit (that is an invertible element of $\mathcal{O}_K$). The norm of 3 is given by

$$9 = \mathrm{N}_{K/\mathbb{Q}}(3) = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\mathrm{N}_{K/\mathbb{Q}}(\beta),$$

by multiplicativity of the norm. By Corollary 1.10, we know that $N_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\beta) \in \mathbb{Z}$. Thus we get a factorization of 9 in $\mathbb{Z}$. There are only two possible factorizations over the integers:

- $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$, $\mathrm{N}_{K/\mathbb{Q}}(\beta) = \pm 9$ (or vice versa): by Corollary 1.11, we know that the element of $\mathcal{O}_K$ of norm ± 1 is a unit, and we are done.

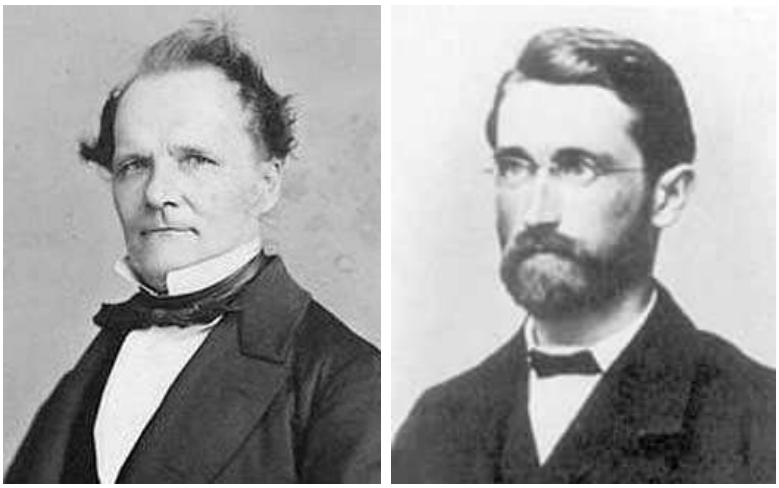

Figure 2.1: Ernst Kummer (1810-1893) and Richard Dedekind (1831-1916)

- $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 3$, $\mathrm{N}_{K/\mathbb{Q}}(\beta) = \pm 3$ (or vice versa): however, we will now show that there is no element of $\mathcal{O}_K$ with norm ± 3. Let us indeed assume that there exists $a + b\sqrt{-5} \in \mathcal{O}_K$, $a, b \in \mathbb{Z}$ such that

  $$\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2 = \pm 3.$$

  We can check that this equation has no solution modulo 5, yielding a contradiction.

On the other hand, we will see that the ideal $21\mathcal{O}_K$ can be factorized into 4 prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ such that

$$7\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2,\ 3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_4,\ (1+2\sqrt{5})\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_3,\ (1-2\sqrt{5})\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_4,$$

namely

$$21\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4.$$

After the realization that uniqueness of factorization into irreducibles is unique in some rings of integers but not in others, the mathematician Kummer had the idea that one way to remedy to the situation could be to work with what he called *ideal numbers*, new structures which would enable us to regain the uniqueness of factorization. Ideals numbers then got called *ideals* by another mathematician, Dedekind, and this is the terminology that has remained. Ideals of $\mathcal{O}$ will the focus of this chapter.

Our goal will be to study ideals of $\mathcal{O}$, and in particular to show that we get a unique factorization into a product of prime ideals. To prove uniqueness, we need to study the arithmetic of non-zero ideals of $\mathcal{O}$, especially their behaviour under multiplication. We will recall how ideal multiplication is defined, which

will appear to be commutative and associative, with $\mathcal{O}$ itself as an identity. However, inverses need not exist, so we do not have a group structure. It turns out that we can get a group if we extend a bit the definition of ideals, which we will do by introducing *fractional ideals*, and showing that they are invertible.

2.2 Factorization and fractional ideals

Let us start by introducing the notion of norm of an ideal. We will see that in the case of principal ideals, we can relate the norm of the ideal with the norm of its generator.

Definition 2.1. Let I be a non-zero ideal of $\mathcal{O}$, we define the norm of I by

$$N(I) = |\mathcal{O}/I|.$$

Lemma 2.1. *Let I be a non-zero ideal of $\mathcal{O}$.*

1. *We have that*
$$N(\alpha\mathcal{O}) = |N_{K/\mathbb{Q}}(\alpha)|,\ \alpha \in \mathcal{O}.$$

2. *The norm of I is finite.*

Proof. 1. First let us notice that the formula we want to prove makes sense, since $N(\alpha) \in \mathbb{Z}$ when $\alpha \in \mathcal{O}_K$, thus $|N(\alpha)|$ is a positive integer. By Proposition 1.12, $\mathcal{O}$ is a free Abelian group of rank $n = [K : \mathbb{Q}]$, thus there exists a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$ of $\mathcal{O}$, that is $\mathcal{O} = \mathbb{Z}\alpha_1 \oplus \cdots \mathbb{Z}\alpha_n$. It is now a general result on free Abelian groups that if H is as subgroup of G, both of same rank, with $\mathbb{Z}$-bases $x_1, \dots, x_r$ and $y_1, \dots, y_r$ respectively, with $y_i = \sum_j a_{ij}x_j$, then $|G/H| = |\det(a_{ij})|$. We thus apply this theorem in our case, where $G = \mathcal{O}$ and $H = \alpha\mathcal{O}$. Since one basis is obtained from the other by multiplication by α, we have that

$$|\mathcal{O}/\alpha\mathcal{O}| = |\det(\mu_\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|.$$

2. Let $0 \neq \alpha \in I$. Since I is an ideal of $\mathcal{O}$ and $\alpha\mathcal{O} \subset I$, we have a surjective map
$$\mathcal{O}/\alpha\mathcal{O} \to \mathcal{O}/I,$$
so that the result follows from part 1.

□

Example 2.2. Let $K = \mathbb{Q}(\sqrt{-17})$ be a quadratic number field, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$. Then

$$N(\langle 18\rangle) = 18^2.$$

Starting from now, we need to build up several intermediate results which we will use to prove the two most important results of this section. Let us begin with the fact that prime is a notion stronger than maximal. You may want to recall what is the general result for an arbitrary commutative ring and compare with respect to the case of a ring of integers (in general, maximal is stronger than prime).

Proposition 2.2. *Every non-zero prime ideal of $\mathcal{O}$ is maximal.*

Proof. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$. Since we have that

$$\mathfrak{p} \text{ is a maximal ideal of } \mathcal{O} \iff \mathcal{O}/\mathfrak{p} \text{ is a field},$$

it is enough to show that $\mathcal{O}/\mathfrak{p}$ is a field. In order to do so, let us consider $0 \neq x \in \mathcal{O}/\mathfrak{p}$, and show that x is invertible in $\mathcal{O}/\mathfrak{p}$. Since $\mathfrak{p}$ is prime, $\mathcal{O}/\mathfrak{p}$ is an integral domain, thus the multiplication map $\mu_x : \mathcal{O}/\mathfrak{p} \mapsto \mathcal{O}/\mathfrak{p}$, $z \mapsto xz$, is injective (that is, its kernel is 0). By the above lemma, the cardinality of $\mathcal{O}/\mathfrak{p}$ is finite, thus μ_x being injective, it has to be also bijective. In other words μ_x is invertible, and there exists $y = \mu_x^{-1}(1) \in \mathcal{O}/\mathfrak{p}$. By definition, y is the inverse of x. □

To prove the next result, we need to first recall how to define the multiplication of two ideals.

Definition 2.2. If I and J are ideals of $\mathcal{O}$, we define the multiplication of ideals as follows:

$$IJ = \left\{ \sum_{finite} xy,\ x \in I,\ y \in J \right\}.$$

Example 2.3. Let $I = (\alpha_1, \alpha_2) = \alpha_1\mathcal{O} + \alpha_2\mathcal{O}$ and $J = (\beta_1, \beta_2) = \beta_1\mathcal{O} + \beta_2\mathcal{O}$, then

$$IJ = (\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2).$$

Lemma 2.3. *Let I be a non-zero ideal of $\mathcal{O}$. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathcal{O}$ such that*

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset I.$$

Proof. The idea of the proof goes as follows: we want to prove that every non-zero ideal I of $\mathcal{O}$ contains a product of r prime ideals. To prove it, we define a set $\mathcal{S}$ of all the ideals which do not contain a product of prime ideals, and we prove that this set is empty. To prove that this set is empty, we assume by contradiction that $\mathcal{S}$ does contain at least one non-zero ideal I. From this ideal, we will show that we can build another ideal I_1 such that I is strictly included in I_1, and by iteration we can build a sequence of ideals strictly included in each other, which will give a contradiction.

Let us now proceed. Let $\mathcal{S}$ be the set of all ideals which do not contain a product of prime ideals, and let I be in $\mathcal{S}$. First, note that I cannot be prime (otherwise I would contain a product of prime ideals with only one ideal, itself).

By definition of prime ideal, that means we can find $\alpha, \beta \in \mathcal{O}$ with $\alpha\beta \in I$, but $\alpha \notin I$, $\beta \notin I$. Using these two elements α and β, we can build two new ideals

$$J_1 = \alpha\mathcal{O} + I \supsetneq I, \;\; J_2 = \beta\mathcal{O} + I \supsetneq I,$$

with strict inclusion since $\alpha, \beta \notin I$.

To prove that J_1 or J_2 belongs to $\mathcal{S}$, we assume by contradiction that none are. Thus by definition of $\mathcal{S}$, there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset J_1$ and $\mathfrak{q}_1 \ldots \mathfrak{q}_s \subset J_2$. Thus

$$\mathfrak{p}_1, \ldots, \mathfrak{p}_r\mathfrak{q}_1, \ldots, \mathfrak{q}_s \subset J_1J_2 \subset I$$

where the second inclusion holds since $\alpha\beta \in I$ and

$$J_1J_2 = (\alpha\mathcal{O} + I)(\beta\mathcal{O} + I) = \alpha\beta\mathcal{O} + \alpha I + \beta I + I^2 \in I$$

But $\mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset I$ contradicts the fact that $I \in \mathcal{S}$. Thus J_1 or J_2 is in $\mathcal{S}$.

Starting from assuming that I is in $\mathcal{S}$, we have just shown that we can find another ideal, say I_1 (which is either J_1 or J_2), such that $I \subsetneq I_1$. Since I_1 is in $\mathcal{S}$ we can iterate the whole procedure, and find another ideal I_2 which strictly contains I_1, and so on and so forth. We thus get a strictly increasing sequence of ideals in $\mathcal{S}$:

$$I \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$$

Now by taking the norm of each ideal, we get a strictly decreasing sequence of integers

$$N(I) > N(I_1) > N(I_2) > \ldots,$$

which yields a contradiction and concludes the proof. □

Note that an ideal I of $\mathcal{O}$ is an $\mathcal{O}$-submodule of $\mathcal{O}$ with scalar multiplication given by $\mathcal{O} \times I \to I$, $(a, i) \mapsto ai$. Ideals of $\mathcal{O}$ are not invertible (with respect to ideal multiplication as defined above), so in order to get a group structure, we extend the definition and look at $\mathcal{O}$-submodules of K.

Definition 2.3. A fractional ideal I is a finitely generated $\mathcal{O}$-module contained in K.

Let $\alpha_1, \ldots, \alpha_r \in K$ be a set of generators for the fractional ideal I as $\mathcal{O}$-module. By Corollary 1.5, we can write $\alpha_i = \gamma_i/\delta_i$, $\gamma_i, \delta_i \in \mathcal{O}$ for $i = 1, \ldots, r$. Set

$$\delta = \prod_{i=1}^{r} \delta_i.$$

Since $\mathcal{O}$ is a ring, $\delta \in \mathcal{O}$. By construction, $J := \delta I$ is an ideal of $\mathcal{O}$. Thus for any fractional ideal $I \subset \mathcal{O}$, there exists an ideal $J \subset \mathcal{O}$ and $\delta \in \mathcal{O}$ such that

$$I = \frac{1}{\delta} J.$$

This yields an equivalent definition of fractional ideal.

Definition 2.4. An $\mathcal{O}$-submodule I of K is called a fractional ideal of $\mathcal{O}$ if there exists some non-zero $\delta \in \mathcal{O}$ such that $\delta I \subset \mathcal{O}$, that is $J = \delta I$ is an ideal of $\mathcal{O}$ and $I = \delta^{-1} J$.

It is easier to understand the terminology "fractional ideal" with the second definition.

Examples 2.4.
1. Ideals of $\mathcal{O}$ are particular cases of fractional ideals. They may be called integral ideals if there is an ambiguity.
2. The set
$$\frac{3}{2}\mathbb{Z} = \left\{ \frac{3x}{2} \in \mathbb{Q} \mid x \in \mathbb{Z} \right\}$$
is a fractional ideal.

It is now time to introduce the inverse of an ideal. We first do it in the particular case where the ideal is prime.

Lemma 2.4. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$. Define*
$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subset \mathcal{O}\}.$$
1. *$\mathfrak{p}^{-1}$ is a fractional ideal of $\mathcal{O}$.*
2. *$\mathcal{O} \subsetneq \mathfrak{p}^{-1}$.*
3. *$\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$.*

Proof. 1. Let us start by showing that $\mathfrak{p}^{-1}$ is a fractional ideal of $\mathcal{O}$. Let $0 \neq a \in \mathfrak{p}$. By definition of $\mathfrak{p}^{-1}$, we have that $a\mathfrak{p}^{-1} \subset \mathcal{O}$. Thus $a\mathfrak{p}^{-1}$ is an integral ideal of $\mathcal{O}$, and $\mathfrak{p}^{-1}$ is a fractional ideal of $\mathcal{O}$.

2. We show that $\mathcal{O} \subsetneq \mathfrak{p}^{-1}$. Clearly $\mathcal{O} \subset \mathfrak{p}^{-1}$. It is thus enough to find an element which is not an algebraic integer in $\mathfrak{p}^{-1}$. We start with any $0 \neq a \in \mathfrak{p}$. By Lemma 2.3, we choose the smallest r such that
$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a)\mathcal{O}$$
for $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ prime ideals of $\mathcal{O}$. Since $(a)\mathcal{O} \subset \mathfrak{p}$ and $\mathfrak{p}$ is prime, we have $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i by definition of prime. Without loss of generality, we can assume that $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Hence $\mathfrak{p}_1 = \mathfrak{p}$ since prime ideals in $\mathcal{O}$ are maximal (by Proposition 2.2). Furthermore, we have that
$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a)\mathcal{O}$$
by minimality of r. Hence we can find $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ but not in $(a)\mathcal{O}$.

We are now ready to show that we have an element in $\mathfrak{p}^{-1}$ which is not in $\mathcal{O}$. This element is given by ba^{-1}.

- Using that $\mathfrak{p} = \mathfrak{p}_1$, we thus get $b\mathfrak{p} \subset (a)\mathcal{O}$, so $ba^{-1}\mathfrak{p} \subset \mathcal{O}$ and $ba^{-1} \in \mathfrak{p}^{-1}$.

- We also have $b \notin (a)\mathcal{O}$ and so $ba^{-1} \notin \mathcal{O}$.

This concludes the proof that $\mathfrak{p}^{-1} \neq \mathcal{O}$.

3. We now want to prove that $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$. It is clear from the definition of $\mathfrak{p}^{-1}$ that $\mathfrak{p} = \mathfrak{p}\mathcal{O} \subset \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}^{-1}\mathfrak{p} \subset \mathcal{O}$. Since $\mathfrak{p}$ is maximal (again by Proposition 2.2), $\mathfrak{p}\mathfrak{p}^{-1}$ is equal to $\mathfrak{p}$ or $\mathcal{O}$. It is now enough to prove that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ is not possible. Let us thus suppose by contradiction that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Let $\{\beta_1, \ldots, \beta_r\}$ be a set of generators of $\mathfrak{p}$ as $\mathcal{O}$-module, and consider again $d := ab^{-1}$ which is in $\mathfrak{p}^{-1}$ but not in $\mathcal{O}$ (by the proof of 2.). Then we have that

$$d\beta_i \in \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p} \text{ and } d\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}.$$

Since $d\mathfrak{p} \subset \mathfrak{p}$, we have that

$$d\beta_i = \sum_{j=1}^{r} c_{ij}\beta_j \in \mathfrak{p},\ c_{ij} \in \mathcal{O},\ i = 1, \ldots, r,$$

or equivalently

$$0 = \sum_{j=1, j\neq i}^{r} c_{ij}\beta_j + \beta_i(c_{ii} - d),\ i = 1, \ldots, r.$$

The above r equations can be rewritten in a matrix equation as follows:

$$\underbrace{\begin{pmatrix} c_{11} - d & c_{1r} \\ c_{21} & c_{2r} \\ \vdots & \vdots \\ c_{r1} & c_{rr} - d \end{pmatrix}}_{C} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{pmatrix} = \mathbf{0}.$$

Thus the determinant of C is zero, while $\det(C)$ is an equation of degree r in d with coefficients in $\mathcal{O}$ of leading term ± 1. By Proposition 1.13, we have that d must be in $\mathcal{O}$, which is a contradiction.

□

Example 2.5. Consider the ideal $\mathfrak{p} = 3\mathbb{Z}$ of $\mathbb{Z}$. We have that

$$\mathfrak{p}^{-1} = \{x \in \mathbb{Q} \mid x \cdot 3\mathbb{Z} \subset \mathbb{Z}\} = \{x \in \mathbb{Q} \mid 3x \in \mathbb{Z}\} = \frac{1}{3}\mathbb{Z}.$$

We have

$$\mathfrak{p} \subset \mathbb{Z} \subset \mathfrak{p}^{-1} \subset \mathbb{Q}.$$

We can now prove that the fractional ideals of K form a group.

Theorem 2.5. *The non-zero fractional ideals of a number field K form a multiplicative group, denoted by I_K.*

Proof. The neutral element is $\mathcal{O}$. It is enough to show that every non-zero fractional ideal of $\mathcal{O}$ is invertible in I_K. By Lemma 2.4, we already know this is true for every prime (integral) ideals of $\mathcal{O}$.

Let us now show that this is true for every integral ideal of $\mathcal{O}$. Suppose by contradiction that there exists a non-invertible ideal I with its norm $N(I)$ minimal. Now I is included in a maximal integral $\mathfrak{p}$, which is also a prime ideal. Thus

$$I \subset \mathfrak{p}^{-1}I \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O},$$

where last equality holds by the above lemma. Let us show that $I \neq \mathfrak{p}^{-1}I$, so that the first inclusion is actually a strict inclusion. Suppose by contradiction that $I = \mathfrak{p}^{-1}I$. Let $d \in \mathfrak{p}^{-1}$ but not in $\mathcal{O}$ and let $\beta_1, \ldots, \beta_r$ be the set of generators of I as $\mathcal{O}$-module. We can thus write:

$$d\beta_i \in \mathfrak{p}^{-1}I = I,\ dI \subset \mathfrak{p}^{-1}I = I.$$

By the same argument as in the previous lemma, we get that d is in $\mathcal{O}$, a contradiction. We have thus found an ideal with $I \subsetneq \mathfrak{p}^{-1}I$, which implies that $N(I) > N(\mathfrak{p}^{-1}I)$. By minimality of $N(I)$, the ideal $\mathfrak{p}^{-1}I$ is invertible. Let $J \in I_K$ be its inverse, that is $J\mathfrak{p}^{-1}I = \mathcal{O}$. This shows that I is invertible, with inverse $J\mathfrak{p}^{-1}$.

If I is a fractional ideal, it can be written as $\frac{1}{d}J$ with J an integral ideal of $\mathcal{O}$ and $d \in \mathcal{O}$. Thus dJ^{-1} is the inverse of I. □

We can now prove unique factorization of integral ideals in $\mathcal{O} = \mathcal{O}_K$.

Theorem 2.6. *Every non-zero integral ideal I of $\mathcal{O}$ can be written in a unique way (up to permutation of the factors) as a product of prime ideals.*

Proof. We thus have to prove the existence of the factorization, and then the unicity up to permutation of the factors.

Existence. Let I be an integral ideal which does not admit such a factorization. We can assume that it is maximal among those ideals. Then I is not prime, but we will have $I \subset \mathfrak{p}$ for some maximal (hence prime) ideal. Thus $I\mathfrak{p}^{-1} \subset \mathcal{O}$ is an integral ideal and $I \subsetneq I\mathfrak{p}^{-1} \subset \mathcal{O}$, which strict inclusion, since if $I = I\mathfrak{p}^{-1}$, then it would imply that $\mathcal{O} = \mathfrak{p}^{-1}$. By maximality of I, the ideal $I\mathfrak{p}^{-1}$ must admit a factorization

$$I\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r$$

that is

$$I = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r,$$

a contradiction.

Unicity. Let us assume that there exist two distinct factorizations of I, that is

$$I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

where $\mathfrak{p}_i$, $\mathfrak{q}_j$ are prime ideals, $i = 1, \ldots, r$, $j = 1, \ldots, s$. Let us assume by contradiction that $\mathfrak{p}_1$ is different from $\mathfrak{q}_j$ for all j. Thus we can choose $\alpha_j \in \mathfrak{q}_j$ but not in $\mathfrak{p}_1$, and we have that

$$\prod \alpha_j \in \prod \mathfrak{q}_j = I \subset \mathfrak{p}_1,$$

which contradicts the fact that $\mathfrak{p}_1$ is prime. Thus $\mathfrak{p}_1$ must be one of the $\mathfrak{q}_j$, say $\mathfrak{q}_1$. This gives that

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

We conclude by induction. □

Example 2.6. In $\mathbb{Q}(i)$, we have

$$(2)\mathbb{Z}[i] = (1+)^2\mathbb{Z}[i].$$

Corollary 2.7. *Let I be a non-zero fractional ideal. Then*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_s^{-1},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are prime integral ideals. This factorization is unique up to permutation of the factors.

Proof. A fractional ideal can be written as $d^{-1}I$, $d \in \mathcal{O}$, I an integral ideal. We write $I = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ and $d\mathcal{O} = \mathfrak{q}_1 \cdots \mathfrak{q}_n$. Thus

$$(d\mathcal{O})^{-1} I = \mathfrak{p}_1 \cdots \mathfrak{p}_t \mathfrak{q}_q^{-1} \cdots \mathfrak{q}_n^{-1}.$$

It may be that some of the terms will cancel out, so that we end up with a factorization with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$. Unicity is proved as in the above theorem. □

2.3 The Chinese Theorem

We have defined in the previous section the group I_K of fractional ideals of a number field K, and we have proved that they have a unique factorization into a product of prime ideals. We are now interested in studying further properties of fractional ideals. The two main properties that we will prove are the fact that two elements are enough to generate these ideals, and that norms of ideals are multiplicative. Both properties can be proved as corollary of the Chinese theorem, that we first recall.

Theorem 2.8. *Let $I = \prod_{i=1}^m \mathfrak{p}_i^{k_i}$ be the factorization of an integral ideal I into a product of prime ideals $\mathfrak{p}_i$ with $\mathfrak{p}_i \neq \mathfrak{p}_j$ of $i \neq j$. Then there exists a canonical isomorphism*

$$\mathcal{O}/I \to \prod_{i=1}^m \mathcal{O}/\mathfrak{p}_i^{k_i}.$$

Corollary 2.9. *Let $I_1, \ldots, I_m$ be ideals which are pairwise coprime (that is $I_i + I_j = \mathcal{O}$ for $i \neq j$). Let $\alpha_1, \ldots, \alpha_m$ be elements of $\mathcal{O}$. Then there exists $\alpha \in \mathcal{O}$ with*

$$\alpha \equiv \alpha_i \mod I_i,\ i = 1, \ldots, m.$$

Proof. We can write $I_i = \prod \mathfrak{p}_{ij}^{n_{ij}}$. By hypothesis, no prime ideal occurs more than once as a $\mathfrak{p}_{ij}$, and each congruence is equivalent to the finite set of congruences

$$\alpha \equiv \alpha_i \mod \mathfrak{p}_{ij}^{n_{ij}},\ i, j.$$

Now write $I = \prod I_i$. Consider the vector $(\alpha_1, \ldots, \alpha_m)$ in $\prod_{i=1}^m \mathcal{O}/I_i$. The map

$$\mathcal{O}/I = \mathcal{O}/\prod I_i \to \prod_{i=1}^m \mathcal{O}/I_i$$

is surjective, thus there exists a preimage $\alpha \in \mathcal{O}$ of $(\alpha_1, \ldots, \alpha_m)$. □

Corollary 2.10. *Let I be a fractional ideal of $\mathcal{O}$, $\alpha \in I$. Then there exists $\beta \in I$ such that*

$$(\alpha, \beta) =< \alpha, \beta >= \alpha\mathcal{O} + \beta\mathcal{O} = I.$$

Proof. Let us first assume that I is an integral ideal. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the prime factors of $\alpha\mathcal{O} \subset I$, so that I can be written as

$$I = \prod_{i=1}^m \mathfrak{p}_i^{k_i},\ k_i \geq 0.$$

Let us choose β_i in $\mathfrak{p}_i^{k_i}$ but not in $\mathfrak{p}_i^{k_i+1}$. By Corollary 2.9, there exists $\beta \in \mathcal{O}$ such that $\beta \equiv \beta_i \mod \mathfrak{p}_i^{k_i+1}$ for all $i = 1, \ldots, m$. Thus

$$\beta \in I = \prod_{i=1}^m \mathfrak{p}_i^{k_i}$$

and $\mathfrak{p}_i^{k_i}$ is the exact power of $\mathfrak{p}_i$ which divides $\beta\mathcal{O}$. In other words, $\beta\mathcal{O}I^{-1}$ is prime to $\alpha\mathcal{O}$, thus $\beta\mathcal{O}I^{-1} + \alpha\mathcal{O} = \mathcal{O}$, that is

$$\beta\mathcal{O} + \alpha I = I.$$

To conclude, we have that

$$I = \beta\mathcal{O} + \alpha I \subset \beta\mathcal{O} + \alpha\mathcal{O} \subset I.$$

If I is a fractional ideal, there exists by definition $d \in \mathcal{O}$ such that $I = \frac{1}{d}J$ with J an integral ideal. Thus $d\alpha \in J$. By the first part, there exists $\beta \in J$ such that $J = (d\alpha, \beta)$. Thus

$$I = \alpha\mathcal{O} + \frac{\beta}{d}\mathcal{O}.$$

□

We are now left to prove properties of the norm of an ideal, for which we need the following result.

Proposition 2.11. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ and $n > 0$. Then the $\mathcal{O}$-modules $\mathcal{O}/\mathfrak{p}$ and $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ are (non-canonically) isomorphic.*

Proof. We consider the map

$$\phi : \mathcal{O} \to \mathfrak{p}^n/\mathfrak{p}^{n+1},\ \alpha \mapsto \alpha\beta$$

for any β in $\mathfrak{p}^n$ but not in $\mathfrak{p}^{n+1}$. The proof consists of computing the kernel and the image of ϕ, and then of using one of the ring isomorphism theorems. This will conclude the proof since we will prove that $ker(\phi) = \mathfrak{p}$ and ϕ is surjective.

- Let us first compute the kernel of ϕ. If $\phi(\alpha) = 0$, then $\alpha\beta = 0$, which means that $\alpha\beta \in \mathfrak{p}^{n+1}$ that is $\alpha \in \mathfrak{p}$.

- Given any $\gamma \in \mathfrak{p}^n$, by Corollary 2.9, we can find $\gamma_1 \in \mathcal{O}$ such that

  $$\gamma_1 \equiv \gamma \mod \mathfrak{p}^{n+1},\ \gamma_1 \equiv 0 \mod \beta\mathcal{O}\mathfrak{p}^{-n},$$

  since $\beta\mathcal{O}\mathfrak{p}^{-n}$ is an ideal coprime to $\mathfrak{p}^{n+1}$. Since $\gamma \in \mathfrak{p}^n$, we have that γ_1 belongs to $\beta\mathcal{O}\mathfrak{p}^{-n} \cap \mathfrak{p}^n = \beta\mathcal{O}$ since $I \cap J = IJ$ when I and J are coprime ideals. In other words, $\gamma_1/\beta \in \mathcal{O}$. Its image by ϕ is

  $$\phi(\gamma_1/\beta) = (\gamma_1/\beta)\beta \mod \mathfrak{p}^{n+1} = \gamma.$$

  Thus ϕ is surjective.

□

Corollary 2.12. *Let I and J be two integral ideals. Then*

$$\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J).$$

Proof. Let us first assume that I and J are coprime. The chinese theorem tells us that

$$\mathcal{O}/IJ \simeq \mathcal{O}/I \times \mathcal{O}/J,$$

thus $|\mathcal{O}/IJ| = |\mathcal{O}/I||\mathcal{O}/J|$. We are left to prove that $\mathrm{N}(\mathfrak{p}^k) = \mathrm{N}(\mathfrak{p})^k$ for $k \geq 1$, $\mathfrak{p}$ a prime ideal. Now one of the isomorphism theorems for rings allows us to write that

$$\mathrm{N}(\mathfrak{p}^{k-1}) = |\mathcal{O}/\mathfrak{p}^{k-1}| = \left|\frac{\mathcal{O}/\mathfrak{p}^k}{\mathfrak{p}^{k-1}/\mathfrak{p}^k}\right| = \frac{|\mathcal{O}/\mathfrak{p}^k|}{|\mathfrak{p}^{k-1}/\mathfrak{p}^k|}.$$

By the above proposition, this can be rewritten as

$$\frac{|\mathcal{O}/\mathfrak{p}^k|}{|\mathcal{O}/\mathfrak{p}|} = \frac{\mathrm{N}(\mathfrak{p}^k)}{\mathrm{N}(\mathfrak{p})}.$$

Thus $\mathrm{N}(\mathfrak{p}^k) = \mathrm{N}(\mathfrak{p}^{k-1})\mathrm{N}(\mathfrak{p})$, and by induction on k, we conclude the proof. □

Example 2.7. In $\mathbb{Q}(i)$, we have that $(2)\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i]$ and thus

$$4 = N(2) = N(1+i)^2$$

and

$$N(1+i) = 2.$$

Definition 2.5. If $I = J_1 J_2^{-1}$ is a non-zero fractional ideal with J_1, J_2 integral ideals, we set

$$\mathrm{N}(I) = \frac{\mathrm{N}(J_1)}{\mathrm{N}(J_2)}.$$

This extends the norm N into a group homomorphism $\mathrm{N} : I_K \to \mathbb{Q}^\times$. For example, we have that $\mathrm{N}\left(\frac{2}{3}\mathbb{Z}\right) = \frac{2}{3}$.

The main definitions and results of this chapter are

- Definition of fractional ideals, the fact that they form a group I_K.
- Definition of norm of both integral and fractional ideals, and that the norm of ideals is multiplicative.
- The fact that ideals can be uniquely factorized into products of prime ideals.
- The fact that ideals can be generated with two elements: $I = (\alpha, \beta)$.