Algebraic Number Theory, a Computational Approach

William Stein

June 9, 2019

Chapter 1

Unique Factorization of Ideals

Unique factorization into irreducible elements frequently fails for rings of integers of number fields. In this chapter we will deduce a central property of the ring of integers $\mathcal{O}_K$ of an algebraic number field, namely that every nonzero *ideal* factors uniquely as a products of prime ideals. Along the way, we will introduce fractional ideals and prove that they form a free abelian group under multiplication. Factorization of *elements* of $\mathcal{O}_K$ (and much more!) is governed by the class group of $\mathcal{O}_K$, which is the quotient of the group of fractional ideals by the principal fractional ideals (see Chapter **??**).

Exercise 1.0.1. This exercise illustrates the failure of unique factorization in the ring $\mathcal{O}_K$ of integers of $K = \mathbb{Q}(\sqrt{-5})$.

1. Give an element $\alpha \in \mathcal{O}_K$ that factors in two distinct ways into irreducible elements.

2. Observe explicitly that the (α) factors uniquely, i.e., the two distinct factorization in the previous part of this problem do not lead to two distinct factorization of the ideal (α) into prime ideals.

[*Hint*: $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.]

1.1 Dedekind Domains

Recall (Corollary **??**) that we proved that the ring of integers $\mathcal{O}_K$ of a number field is noetherian as follows. As we saw before using norms, the ring $\mathcal{O}_K$ is finitely generated as a module over $\mathbb{Z}$, so it is certainly finitely generated as a ring over $\mathbb{Z}$. By the Hilbert Basis Theorem (Theorem **??**), $\mathcal{O}_K$ is noetherian.

If R is an integral domain, the *field of fractions* $\mathrm{Frac}(R)$ of R is the field of all equivalence classes of formal quotients a/b, where $a, b \in R$ with $b \neq 0$, and $a/b \sim c/d$ if $ad = bc$. For example, the field of fractions of $\mathbb{Z}$ is (canonically isomorphic to) $\mathbb{Q}$ and the field of fractions of $\mathbb{Z}[(1+\sqrt{5})/2]$ is $\mathbb{Q}(\sqrt{5})$. The field of fractions of the ring $\mathcal{O}_K$ of integers of a number field K is just the number field K (see Lemma **??**).

Example 1.1.1. We compute the fraction fields mentioned above.

```
Frac(ZZ)
```

```
Rational Field
```

In `Sage` the `Frac` command usually returns a field canonically isomorphic to the fraction field (not a formal construction).

```
K.<a> = QuadraticField(5)
OK = K.ring_of_integers(); OK
```

```
Maximal Order in Number Field in a with defining polynomial x^2 - 5
```

```
OK.basis()
```

```
[1/2*a + 1/2, a]
```

```
Frac(OK)
```

```
Number Field in a with defining polynomial x^2 - 5
```

The fraction field of an *order* – i.e., a subring of $\mathcal{O}_K$ of finite index – is also the number field again.

```
O2 = K.order(2*a); O2
```

```
Order in Number Field in a with defining polynomial x^2 - 5
```

```
Frac(O2)
```

```
Number Field in a with defining polynomial x^2 - 5
```

Remark 1.1.2. Note that in computers `1/2 * x` means the same as `(1/2)*x`. For more information about the order of operations in programming see `http://en.wikipedia.org/wiki/Order_of_operations`. In `Sage` the `^` symbol is replaced with python's exponentiation `**` at execution.[1]

Definition 1.1.3 (Integrally Closed)**.** An integral domain R is *integrally closed in its field of fractions* if whenever α is in the field of fractions of R and α satisfies a monic polynomial $f \in R[x]$, then $\alpha \in R$.

For example, every field is integrally closed in its field of fractions, as is the ring $\mathbb{Z}$ of integers. However, $\mathbb{Z}[\sqrt{5}]$ is not integrally closed in its field of fractions, since $(1+\sqrt{5})/2$ is integrally over $\mathbb{Z}$ and lies in $\mathbb{Q}(\sqrt{5})$, but not in $\mathbb{Z}[\sqrt{5}]$

Proposition 1.1.4. *If K is any number field, then $\mathcal{O}_K$ is integrally closed. Also, the ring $\overline{\mathbb{Z}}$ of all algebraic integers (in a fixed choice of $\overline{\mathbb{Q}}$) is integrally closed.*

Proof. We first prove that $\overline{\mathbb{Z}}$ is integrally closed. Suppose $\alpha \in \overline{\mathbb{Q}}$ is integral over $\overline{\mathbb{Z}}$, so there is a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \overline{\mathbb{Z}}$ and $f(\alpha) = 0$. The a_i all lie in the ring of integers $\mathcal{O}_K$ of the number field $K = \mathbb{Q}(a_0, a_1, \ldots a_{n-1})$, and $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module, so $\mathbb{Z}[a_0, \ldots, a_{n-1}]$ is finitely generated as a $\mathbb{Z}$-module. Since $f(\alpha) = 0$, we can write α^n as a $\mathbb{Z}[a_0, \ldots, a_{n-1}]$-linear combination of α^i for $i < n$, so the ring $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ is also finitely generated as a $\mathbb{Z}$-module. Thus $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module because it is a submodule of a finitely generated $\mathbb{Z}$-module, which implies that α is integral over $\mathbb{Z}$.

Without loss we may assume that $K \subset \overline{\mathbb{Q}}$, so that $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K$. Suppose $\alpha \in K$ is integral over $\mathcal{O}_K$. Then since $\overline{\mathbb{Z}}$ is integrally closed, α is an element of $\overline{\mathbb{Z}}$, so $\alpha \in K \cap \overline{\mathbb{Z}} = \mathcal{O}_K$, as required. $\square$

Exercise 1.1.5. Prove that $\overline{\mathbb{Z}}$ is not noetherian.

[*Hint*: Find an ascending chain of ideals generated by prime fractional powers that does not stabilize.]

Definition 1.1.6 (Dedekind Domain)**.** An integral domain R is a *Dedekind domain* if it is noetherian, integrally closed in its field of fractions, and every nonzero prime ideal of R is maximal.

Exercise 1.1.7. Let K be a field.

(a) Prove that the polynomial ring $K[x]$ is a Dedekind domain.

[1] Another source for order of operations specific to python is `https://docs.python.org/2/reference/expressions.html#operator-precedence`.

(b) Is $\mathbb{Z}[x]$ a Dedekind domain?

The ring $\mathbb{Z} \oplus \mathbb{Z}$ is not a Dedekind domain because it is not an integral domain. The ring $\mathbb{Z}[\sqrt{5}]$ is not a Dedekind domain because it is not integrally closed in its field of fractions. The ring $\mathbb{Z}$ is a Dedekind domain, as is any ring of integers $\mathcal{O}_K$ of a number field, as we will see below. Also, any field K is a Dedekind domain, since it is an integral domain, it is trivially integrally closed in itself, and there are no nonzero prime ideals so the condition that they be maximal is empty.

Exercise 1.1.8. In Proposition 1.1.4 we showed that $\overline{\mathbb{Z}}$ is integrally closed in its field of fractions. Prove that and every nonzero prime ideal of $\overline{\mathbb{Z}}$ is maximal. Together with Exercise 1.1.5, this shows $\overline{\mathbb{Z}}$ is not a Dedekind domain only because it is not noetherian.

Exercise 1.1.9. Show that Dedekind domains are closed under localization. This means the following: given any nonzero prime $\mathfrak{p}$ in R, the *localization* $R_\mathfrak{p}$ of R at $\mathfrak{p}$ is the ring formed by inverting all elements of R not contained in $\mathfrak{p}$. Thus $R_\mathfrak{p}$ is a subring of the field of fractions K of R which contains R. For example, $\mathbb{Z}_{(2)}$ is the localization of $\mathbb{Z}$ at the prime ideal (2). Note $\mathbb{Z}_{(2)}$ contains $\frac{1}{3}$ but not $\frac{1}{2}$. This exercise will show $R_\mathfrak{p}$ is again a Dedekind domain. In general, any element of $R_\mathfrak{p}$ can be written as a quotient $\frac{a}{b}$ for some $a \in R$ and $b \in R \setminus \mathfrak{p}$.

[*Hint*: It is a standard fact of localizations that the set of prime ideals in $R_\mathfrak{p}$ is in bijection with the set of prime ideals of R contained in $\mathfrak{p}$. Use this to show $R_\mathfrak{p}$ is noetherian and all prime ideals of $R_\mathfrak{p}$ are maximal. It remains to show $R_\mathfrak{p}$ is integrally closed. Let $\alpha \in K$ satisfy a monic polynomial with coefficients in $R_\mathfrak{p}$. By clearing denominators show that $s\alpha \in R$ for some $s \in R \setminus \mathfrak{p}$.]

Proposition 1.1.10. *The ring of integers $\mathcal{O}_K$ of a number field is a Dedekind domain.*

Proof. By Proposition 1.1.4, the ring $\mathcal{O}_K$ is integrally closed, and by Proposition **??** it is noetherian. Suppose that $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$. Let $\alpha \in \mathfrak{p}$ be a nonzero element, and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Then

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

so $a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha) \in \mathfrak{p}$. Since f is irreducible, a_0 is a nonzero element of $\mathbb{Z}$ that lies in $\mathfrak{p}$. Every element of the finitely generated abelian group $\mathcal{O}_K/\mathfrak{p}$ is killed by a_0, so $\mathcal{O}_K/\mathfrak{p}$ is a finite set. Since $\mathfrak{p}$ is prime, $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. Every finite integral domain is a field (see Exercise 1.1.11), so $\mathfrak{p}$ is maximal, which completes the proof. $\square$

Exercise 1.1.11. Prove that every finite integral domain is a field.

1.2 Factorization of Ideals

If I and J are ideals in a ring R, the product IJ is the ideal *generated by* all products of elements in I with elements in J:

$$IJ = (ab : a \in I, b \in J) \subset R.$$

Note that the set of all products ab, with $a \in I$ and $b \in J$, need not be an ideal, so it is important to take the ideal generated by that set.

Exercise 1.2.1. Give an example of two ideals I, J in a commutative ring R whose product is *not* equal to the set $\{ab : a \in I, b \in J\}$.

Exercise 1.2.2. Suppose R is a principal ideal domain. Is it always the case that

$$IJ = \{ab : a \in I, b \in J\}$$

for all ideals I, J in R?

Definition 1.2.3 (Fractional Ideal)**.** A *fractional ideal* is a nonzero $\mathcal{O}_K$-submodule I of K that is finitely generated as an $\mathcal{O}_K$-module.

Exercise 1.2.4. Is the set $\mathbb{Z}\left[\frac{1}{2}\right]$ of rational numbers with denominator a power of 2 a fractional ideal?

We will sometimes call a genuine ideal $I \subset \mathcal{O}_K$ an *integral ideal*. The notion of fractional ideal makes sense for an arbitrary Dedekind domain R – it is an R-module $I \subset K = \mathrm{Frac}(R)$ that is finitely generated as an R-module.

Example 1.2.5. We multiply two fractional ideals in `Sage`:

```
K.<a> = NumberField(x^2 + 23)
I = K.fractional_ideal(2, 1/2*a - 1/2)
J = I^2
I
```

```
Fractional ideal (2, 1/2*a - 1/2)
```

```
J
```

```
Fractional ideal (4, 1/2*a + 3/2)
```

```
I*J
```

```
Fractional ideal (1/2*a + 3/2)
```

Since fractional ideals I are finitely generated, we can clear denominators of a generating set to see that there exists some nonzero $\alpha \in K$ such that

$$\alpha I = J \subset \mathcal{O}_K,$$

with J an integral ideal. Thus dividing by α, we see that every fractional ideal is of the form

$$aJ = \{ab : b \in J\}$$

for some $a \in K$ and integral ideal $J \subset \mathcal{O}_K$.

For example, the set $\frac{1}{2}\mathbb{Z}$ of rational numbers with denominator 1 or 2 is a fractional ideal of $\mathbb{Z}$.

Theorem 1.2.6. *The set of fractional ideals of a Dedekind domain R is an abelian group under ideal multiplication with identity element R.*

Note that fractional ideals are nonzero by definition, so it is not necessary to write "nonzero fractional ideals" in the statement of the theorem. We will *only* prove Theorem 1.2.6 in the case when $R = \mathcal{O}_K$ is the ring of integers of a number field K. The general case can be found in many algebraic number theory books such as [Mar77, Ch. 3]. Before proving Theorem 1.2.6 we prove a lemma. For the rest of this section $\mathcal{O}_K$ is the ring of integers of a number field K.

Definition 1.2.7 (Divides for Ideals)**.** Suppose that I, J are ideals of $\mathcal{O}_K$. Then we say that I *divides* J if $I \supset J$.

To see that this notion of divides is sensible, suppose $K = \mathbb{Q}$, so $\mathcal{O}_K = \mathbb{Z}$. Then $I = (n)$ and $J = (m)$ for some integer n and m, and I divides J means that $(n) \supset (m)$, i.e., that there exists an integer c such that $m = cn$, which exactly means that n divides m, as expected.

Lemma 1.2.8. *Suppose I is a nonzero ideal of $\mathcal{O}_K$. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_n \subset I$, i.e., I divides a product of prime ideals.*

Proof. Let S be the set of nonzero ideals of $\mathcal{O}_K$ that do not satisfy the conclusion of the lemma. The key idea is to use that $\mathcal{O}_K$ is noetherian to show that S is the empty set. If S is nonempty, then since $\mathcal{O}_K$ is noetherian, there is an ideal $I \in S$ that is maximal as an element of S. If I were prime, then I would trivially contain a product of primes, so we may assume that I is not prime. Thus there exists $a, b \in \mathcal{O}_K$ such that $ab \in I$ but $a \notin I$ and $b \notin I$. Let $J_1 = I + (a)$ and $J_2 = I + (b)$. Then neither J_1 nor J_2 is in S, since I is maximal, so both J_1 and J_2 contain a product of prime ideals, say $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset J_1$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset J_2$. Then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset J_1 J_2 = I^2 + I(b) + (a)I + (ab) \subset I,$$

so I contains a product of primes. This is a contradiction, since we assumed $I \in S$. Thus S is empty, which completes the proof. □

We are now ready to prove the theorem.

Proof of Theorem 1.2.6. Note that we will *only* prove Theorem 1.2.6 in the case when $R = \mathcal{O}_K$ is the ring of integers of a number field K.

The product of two fractional ideals is again finitely generated, so it is a fractional ideal, and $I\mathcal{O}_K = I$ for any ideal I, so to prove that the set of fractional ideals under multiplication is a group it suffices to show the existence of inverses. We will first prove that if $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}$ has an inverse, then we will prove that all nonzero integral ideals have inverses, and finally observe that every fractional ideal has an inverse. (Note: Once we know that the set of fractional ideals is a group, it will follows that inverses are unique; until then we will be careful to write "an" instead of "the".)

Suppose $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$. We will show that the $\mathcal{O}_K$-module

$$I = \{a \in K : a\mathfrak{p} \subset \mathcal{O}_K\}$$

is a fractional ideal of $\mathcal{O}_K$ such that $I\mathfrak{p} = \mathcal{O}_K$, so that I is an inverse of $\mathfrak{p}$.

For the rest of the proof, fix a nonzero element $b \in \mathfrak{p}$. Since I is an $\mathcal{O}_K$-module, $bI \subset \mathcal{O}_K$ is an $\mathcal{O}_K$ ideal, hence I is a fractional ideal. Since $\mathcal{O}_K \subset I$ we have $\mathfrak{p} \subset I\mathfrak{p} \subset \mathcal{O}_K$, hence since $\mathfrak{p}$ is maximal, either $\mathfrak{p} = I\mathfrak{p}$ or $I\mathfrak{p} = \mathcal{O}_K$. If $I\mathfrak{p} = \mathcal{O}_K$, we are done since then I is an inverse of $\mathfrak{p}$. Thus suppose that $I\mathfrak{p} = \mathfrak{p}$. Our strategy is to show that there is some $d \in I$, with $d \notin \mathcal{O}_K$. Since $I\mathfrak{p} = \mathfrak{p}$, such a d would leave $\mathfrak{p}$ invariant, i.e., $d\mathfrak{p} \subset \mathfrak{p}$. Since $\mathfrak{p}$ is a finitely generated $\mathcal{O}_K$-module we will see that it will follow that $d \in \mathcal{O}_K$, a contradiction.

By Lemma 1.2.8, we can choose a product $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, with m minimal, with

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m \subset (b) \subset \mathfrak{p}.$$

If no $\mathfrak{p}_i$ is contained in $\mathfrak{p}$, then we can choose for each i an $a_i \in \mathfrak{p}_i$ with $a_i \notin \mathfrak{p}$; but then $\prod a_i \in \mathfrak{p}$, which contradicts that $\mathfrak{p}$ is a prime ideal. Thus some $\mathfrak{p}_i$, say $\mathfrak{p}_1$, is contained in $\mathfrak{p}$, which implies that $\mathfrak{p}_1 = \mathfrak{p}$ since every nonzero prime ideal is maximal. Because m is minimal, $\mathfrak{p}_2 \cdots \mathfrak{p}_m$ is not a subset of (b), so there exists $c \in \mathfrak{p}_2 \cdots \mathfrak{p}_m$ that does not lie in (b). Then $\mathfrak{p}(c) \subset (b)$, so by definition of I we have $d = c/b \in I$. However, $d \notin \mathcal{O}_K$, since if it were then c would be in (b). We have thus found our element $d \in I$ that does not lie in $\mathcal{O}_K$.

To finish the proof that $\mathfrak{p}$ has an inverse, we observe that d preserves the finitely generated $\mathcal{O}_K$-module $\mathfrak{p}$, and is hence in $\mathcal{O}_K$, a contradiction. More precisely, if $b_1, \ldots, b_n$ is a basis for $\mathfrak{p}$ as a $\mathbb{Z}$-module, then the action of d on $\mathfrak{p}$ is given by a matrix with entries in $\mathbb{Z}$, so the minimal polynomial of d has coefficients in $\mathbb{Z}$ (because d satisfies the minimal polynomial of ℓ_d, by the Cayley-Hamilton theorem – here we also use that $\mathbb{Q} \otimes \mathfrak{p} = K$, since $\mathcal{O}_K/\mathfrak{p}$ is a finite set). This implies that d is integral over $\mathbb{Z}$, so $d \in \mathcal{O}_K$ since $\mathcal{O}_K$ is by definition the set of elements of K that are integral over $\mathbb{Z}$.

So far we have proved that if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then

$$\mathfrak{p}^{-1} = \{a \in K : a\mathfrak{p} \subset \mathcal{O}_K\}$$

is the inverse of $\mathfrak{p}$ in the monoid of nonzero fractional ideals of $\mathcal{O}_K$. As mentioned after Definition 1.2.3, every nonzero fractional ideal is of the form aI for $a \in K$ and I an integral ideal, so since (a) has inverse $(1/a)$, it suffices to show that every integral ideal I has an inverse. If not, then there is a nonzero integral ideal I that is maximal among all nonzero integral ideals that do not have an inverse. Every ideal is contained in a maximal ideal, so there is a nonzero prime ideal $\mathfrak{p}$ such that $I \subset \mathfrak{p}$. Multiplying both sides of this inclusion by $\mathfrak{p}^{-1}$ and using that $\mathcal{O}_K \subset \mathfrak{p}^{-1}$, we see that

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

If $I = \mathfrak{p}^{-1}I$, then arguing as in the proof that $\mathfrak{p}^{-1}$ is an inverse of $\mathfrak{p}$, we see that each element of $\mathfrak{p}^{-1}$ preserves the finitely generated $\mathbb{Z}$-module I and is hence integral. But then $\mathfrak{p}^{-1} \subset \mathcal{O}_K$, which, upon multiplying both sides by

$\mathfrak{p}$, implies that $\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^{-1} \subset \mathfrak{p}$, a contradiction. Thus $I \neq \mathfrak{p}^{-1}I$. Because I is maximal among ideals that do not have an inverse, the ideal $\mathfrak{p}^{-1}I$ does have an inverse J. Then $\mathfrak{p}^{-1}J$ is an inverse of I, since $(J\mathfrak{p}^{-1})I = J(\mathfrak{p}^{-1}I) = \mathcal{O}_K$. □

We can finally deduce the crucial Theorem 1.2.9, which will allow us to show that any nonzero ideal of a Dedekind domain can be expressed uniquely as a product of primes (up to order). Thus unique factorization holds for ideals in a Dedekind domain, and it is this unique factorization that initially motivated the introduction of ideals to mathematics over a century ago.

Theorem 1.2.9. *Suppose I is a nonzero integral ideal of $\mathcal{O}_K$. Then I can be written as a product*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

of prime ideals of $\mathcal{O}_K$, and this representation is unique up to order.

Proof. Suppose I is an ideal that is maximal among the set of all ideals in $\mathcal{O}_K$ that cannot be written as a product of primes. Every ideal is contained in a maximal ideal, so I is contained in a nonzero prime ideal $\mathfrak{p}$. If $I\mathfrak{p}^{-1} = I$, then by Theorem 1.2.6 we can cancel I from both sides of this equation to see that $\mathfrak{p}^{-1} = \mathcal{O}_K$, a contradiction. Since $\mathcal{O}_K \subset \mathfrak{p}^{-1}$, we have $I \subset I\mathfrak{p}^{-1}$, and by the above observation I is strictly contained in $I\mathfrak{p}^{-1}$. By our maximality assumption on I, there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $I\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Then $I = \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_n$, a contradiction. Thus every ideal can be written as a product of primes.

Suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$. If no $\mathfrak{q}_i$ is contained in $\mathfrak{p}_1$, then for each i there is an $a_i \in \mathfrak{q}_i$ such that $a_i \notin \mathfrak{p}_1$. But the product of the a_i is in $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, which is a subset of $\mathfrak{p}_1$, which contradicts that $\mathfrak{p}_1$ is a prime ideal. Thus $\mathfrak{q}_i = \mathfrak{p}_1$ for some i. We can thus cancel $\mathfrak{q}_i$ and $\mathfrak{p}_1$ from both sides of the equation by multiplying both sides by the inverse. Repeating this argument finishes the proof of uniqueness. □

Exercise 1.2.10. Factor the ideal (10) as a product of primes in the ring of integers of $\mathbb{Q}(\sqrt{11})$. You are allowed to use a computer, as long as you show the commands you use. [*Hint*: In `Sage`, an ideal `I` can be factored using `I.factor()`.]

Theorem 1.2.11. *If I is a fractional ideal of $\mathcal{O}_K$ then there exists prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$, unique up to order, such that*

$$I = (\mathfrak{p}_1 \cdots \mathfrak{p}_n)(\mathfrak{q}_1 \cdots \mathfrak{q}_m)^{-1}.$$

Proof. We have $I = (a/b)J$ for some $a, b \in \mathcal{O}_K$ and integral ideal J. Applying Theorem 1.2.9 to (a), (b), and J gives an expression as claimed. For uniqueness, if one has two such product expressions, multiply through by the denominators and use the uniqueness part of Theorem 1.2.9. □

Example 1.2.12. The ring of integers of $K = \mathbb{Q}(\sqrt{-6})$ is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$. We have

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

If $ab = \sqrt{-6}$, with $a, b \in \mathcal{O}_K$ and neither a unit, then $\mathrm{Norm}(a)\,\mathrm{Norm}(b) = 6$, so without loss $\mathrm{Norm}(a) = 2$ and $\mathrm{Norm}(b) = 3$. If $a = c + d\sqrt{-6}$, then $\mathrm{Norm}(a) = c^2 + 6d^2$; since the equation $c^2 + 6d^2 = 2$ has no solution with $c, d \in \mathbb{Z}$, there is no element in $\mathcal{O}_K$ with norm 2, so $\sqrt{-6}$ is irreducible. Also, $\sqrt{-6}$ is not a unit times 2 or times 3, since again the norms would not match up. Thus 6 cannot be written uniquely as a product of irreducibles in $\mathcal{O}_K$. Theorem 1.2.11, however, implies that the principal ideal (6) can, however, be written uniquely as a product of prime ideals. An explicit decomposition is

$$(6) = (2, 2 + \sqrt{-6})^2 \cdot (3, 3 + \sqrt{-6})^2, \tag{1.1}$$

where each of the ideals $(2, 2 + \sqrt{-6})$ and $(3, 3 + \sqrt{-6})$ is prime. We will discuss algorithms for computing such a decomposition in detail in Chapter **??**. The first idea is to write $(6) = (2)(3)$, and hence reduce to the case of writing the (p), for $p \in \mathbb{Z}$ prime, as a product of primes. Next one decomposes the finite (as a set) ring $\mathcal{O}_K/p\mathcal{O}_K$.

The factorization (1.1) can be compute using `Sage` as follows:

```
K.<a> = NumberField(x^2 + 6); K
```

```
Number Field in a with defining polynomial x^2 + 6
```

```
K.factor(6)
```

```
(Fractional ideal (2, a))^2 * \
(Fractional ideal (3, a))^2
```

Exercise 1.2.13. Let $\mathcal{O}_K$ be the ring of integers of a number field. Let F_K denote the abelian group of fractional ideals of $\mathcal{O}_K$.

(a) Prove that F_K is torsion free.

(b) Prove that F_K is not finitely generated.

(c) Prove that F_K is countable.

(d) Conclude that if K and L are number fields, then there exists some (non-canonical) isomorphism of groups $F_K \approx F_L$.

SOLUTION

Exercise 1.2.14. Give an example of each of the following, with proof:

(a) A non-principal ideal in a ring.

(b) A module that is not finitely generated.

(c) The ring of integers of a number field of degree 3.

(d) An order in the ring of integers of a number field of degree 5.

(e) The matrix on K of left multiplication by an element of K, where K is a degree 3 number field.

(f) An integral domain that is not integrally closed in its field of fractions.

(g) A Dedekind domain with finite cardinality.

(h) A fractional ideal of the ring of integers of a number field that is not an integral ideal.

SOLUTION

Bibliography

[Mar77] Daniel A. Marcus, *Number Fields*, Universitext (1979), Springer, 1977.