

Chapter 1

Rings

Example 1

1. $(\mathbb{Z}, +, \cdot)$
2. All fields, such as $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$, are rings.
3. Let R be a commutative ring, then $R[X]$, the set of polynomials with coefficients in R , is again a ring, e.g. $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, and $\mathbb{R}[X]$.
4. For any ring R and for any $n \in \mathbb{N}$, the set of all square n -by- n matrices with entries from R , forms a ring with matrix addition and matrix multiplication as operations. If $n = 1$, this matrix ring is isomorphic to R itself. For $n > 1$ (and R not a zero ring), this matrix is noncommutative. More concretely, $\text{Mat}_{3 \times 3}(\mathbb{R})$ is a noncommutative ring.

1.1 No idea yet

Definition 1 (Fractional Ideal)

Let A be an [integral domain](#).

1. A [fractional ideal](#) of A is an [A-submodule](#) $I \subset \text{Quot}(A)$ such that $dI \subset A$ for some [denominator](#) $d \in A \setminus \{0\}$.
2. A [principal fractional ideal](#) is a [fractional ideal](#) of the form $(r) = rA = \{ar \mid a \in A\}$

Example 2

- All ordinary ideals $I \subset A$ are also fractional ideals with denominator $d = 1$, and are often referred to as [integral ideals](#).

- The subset

$$\frac{3}{25}\mathbb{Z} = \left\{ \frac{3n}{25} \in \mathbb{Q} \mid n \in \mathbb{Z} \right\} \subset \mathbb{Q} \quad (1.1)$$

is a principal fractional ideal of \mathbb{Z}

Example 3

The subset

$$\mathbb{Z} \left[\frac{1}{2} \right] = \left\{ a_0 + a_1 \frac{1}{2} + a_2 \frac{1}{2^2} + \cdots + a_n \frac{1}{2^n} \mid a_0, \dots, a_n \in \mathbb{Z} \subset \mathbb{Q} \right\} \quad (1.2)$$

is not a fractional ideal, because the denominators are not bounded.

Lemma 1.1 If $I \subset \text{Quot}(A)$ is an A -submodule and $d \in \text{Quot}(A)$, then $dI \subset \text{Quot}(A)$ is also an A -module. Thus $I \subset K$ is a fractional ideal if and only if $I = \frac{1}{d}J$ for some $d \in A \setminus \{0\}$ and some integral ideal $J \subset A$ (just take d a denominator of I and $J = dI$).

Lemma 1.2 Let A be an integral domain and denote its field of fraction with $\text{Quot}(A) = K$.

1. If $I \subset K$ is a finitely generated A -submodule, then I is a fractional ideal.
2. Conversely, if A is noetherian and $I \subset K$ is a fractional ideal, then I is a finitely generated A -module.
3. If $I, J \subset K$ are fractional ideals, then $I \cap J, I + J, IJ \subset K$ are also fractional ideals.
4. If $I, J \subset K$ are fractional ideals and $J \neq 0$, then the generalized ideal quotient

$$(I : J) := \{x \in K \mid xJ \subset I\} \quad (1.3)$$

is also a fractional ideal. Moreover, it satisfies $(I : J)J \subset I$.

The nonzero fractional ideals form an abelian semigroup with neutral element A with respect to the multiplication. We will now show that, if A is a Dedekind domain, every nonzero fractional ideal has an inverse hence they form an abelian group $\text{Id}(A)$.

Definition 2

Let A be an integral domain. A fractional ideal $I \subset K$ is invertible if $IJ = A$ for some fractional ideal J called the inverse of I .

The following result shows characterizes invertible fractional ideals and their inverses (which are unique).

Lemma 2.1 A fractional ideal I is invertible if and only if $I(A : I) = A$, in which case $I^{-1} := (A : I)$ is the unique inverse.

The main result of this section is to prove that, in a Dedekind domain, every nonzero ideal is invertible. To this aim we need first a technical result.

Lemma 2.2 Let A be a Dedekind domain and $I \subset A$ a nonzero integral ideal. Then there are not necessarily distinct nonzero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset A$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset I$.

Let

$$\Sigma = \{I \neq \{0\} \mid I \subset A \text{ ideal. } I \text{ does not contain any product of nonzero prime ideals.}\} \quad (1.4)$$

If $\Sigma \neq \emptyset$, let $I \in \Sigma$ be a maximal element which must exist since A is noetherian. In particular, I is not prime, i.e. there exists $a, b \in A \setminus I$ with $a \cdot b \in I$.

Because of the maximality of I , the ideals $I + (a), I + (b) \supsetneq I$ don't lie in I , i.e. there exists nonzero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n, \mathfrak{q}_1, \dots, \mathfrak{q}_m$ such that

$$\mathfrak{p}_1, \dots, \mathfrak{p}_n \subseteq I + (a) \quad (1.5)$$

$$\mathfrak{q}_1, \dots, \mathfrak{q}_m \subseteq I + (b). \quad (1.6)$$

We have

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq (I + (a))(I + (b)) \subseteq I \quad (1.7)$$

which is a contradiction. Hence $\Sigma = \emptyset$.

Theorem 2.1 Let A be a Dedekind domain, I a nonzero ideal, and \mathfrak{p} a prime ideal such that $I \subseteq \mathfrak{p}$. Set

$$\mathfrak{p}^{-1} := (A : \mathfrak{p}) = \{x \in \text{Quot}(A) \mid x\mathfrak{p} \subseteq A\}. \quad (1.8)$$

Then, $I \subsetneq \mathfrak{p}^{-1}I \subseteq A$. In particular, $A \subsetneq \mathfrak{p}^{-1}$ and $\mathfrak{p}^{-1}\mathfrak{p} = A$, i.e. \mathfrak{p} is invertible.

Corollary 1 Let A be a Dedekind domain and

$$\text{Id}(A) = \{I \subseteq K \mid I \text{ is a nonzero fractional ideal.}\} \quad (1.9)$$

1. Every nonzero fractional ideal $I \in Id(A)$ is invertible. In particular, $Id(A)$ is an abelian group with respect to the product of ideals, and the trivial ideal $(1) = A$ as neutral element.
2. Moreover, the map

$$\varphi : K^* \rightarrow Id(A), \quad \frac{a}{b} \mapsto \left(\frac{a}{b}\right) = \left\{ \frac{ac}{b} \mid c \in A \right\} \subseteq K, \quad (1.10)$$

is a group homomorphism, whose image is the subgroup P_A of nonzero principal fractional ideals.

Definition 3

The (ideal) class group of a Dedekind domain A is the quotient $Cl(A) = Id(A)/P_A$ which is naturally an abelian group.

Remark 1 Two crucial objects in the study of a Dedekind domain A are the group of units A^* and the class group $Cl(A)$.

1. For example, A is a principal ideal domain if and only if the class group is trivial.
2. In general, it is immediate that the kernel of φ is the set of units A^* . Hence there is an exact sequence of abelian groups

$$1 \rightarrow A^* \rightarrow K^* \rightarrow Id(A) \rightarrow Cl(A) \rightarrow 0. \quad (1.11)$$

1.2 Chapter 5

How to compute the prime factorization $I = \mathfrak{p}_1^{r_1} \cdot \dots \cdot \mathfrak{p}_n^{r_n}$ of a nonzero ideal in a Dedekind domain $I \subseteq A$?

One idea is to find a smaller Dedekind subring $A' \subseteq A$ where we can compute these factorizations and then

1. Factorize $I \cap A' \subseteq A' \Rightarrow I \cap A' = \tilde{\mathfrak{p}}_1^{s_1} \cdot \dots \cdot \tilde{\mathfrak{p}}_k^{s_k}$.
2. Factorize $\tilde{\mathfrak{p}}_i^{s_i} \cdot A \subseteq A \Rightarrow \tilde{\mathfrak{p}}_1^{s_1} \cdot A = \prod_{j=1}^{N_i} \mathfrak{p}_{i,j}^{e_{i,j}}$.
3. For each $\mathfrak{p}_{i,j}$ find the right exponent, i.e. smallest k such that $I \subseteq \mathfrak{p}_{i,j}^k$ ($k \leq s_i \cdot e_{i,j}$).

Another approach is

1. list all prime ideals $\mathfrak{p} \subseteq A, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \dots$
2. localize at \mathfrak{p}_1 , compute $r_1 = v_{\mathfrak{p}_1}(I \cdot A_{\mathfrak{p}_1})$ check if $I = \mathfrak{p}_1^{r_1}$
3. If not, then compute again
4. jadajadajada

Definition 4

The spectrum of a ring A is

$$\text{Spec}(A) = \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ prime ideal}\}. \quad (1.12)$$

Definition 5

Let A be a Dedekind domain, $K = \text{Quot}(A)$ its field of fraction, L/K a finite separable field extension, and $B = \bar{A}$ the integral closure of A in L .

Moreover, let $\mathfrak{p} \subset A$ and $\mathfrak{q} \subset B$ be two prime ideals. We say that \mathfrak{q} lies over \mathfrak{p} if $\mathfrak{q} \mid \mathfrak{p}B$, i.e. $\mathfrak{q} \cap A = \mathfrak{p}$. In this case, define

1. $e_{\mathfrak{q}|\mathfrak{p}} = v_{\mathfrak{q}}(\mathfrak{p}B) \in \mathbb{Z}_{\geq 0}$ the ramification index of \mathfrak{q} over \mathfrak{p} .

Example 4

Consider $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, so that $B = \mathcal{O}_L = \mathbb{Z}[i]$. For a nonzero prime ideal $\mathfrak{p} = (p) \subseteq \mathbb{Z}$.

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

Example 5

Let $\alpha := \sqrt[3]{2}$. Consider a Dedekind domain $A := \mathbb{Z}$, $K := \text{Quot}(A)$, $L := \mathbb{Q}(\alpha)$, and $B := \mathcal{O}_K$ the integral closure of \mathbb{Z} in $\mathbb{Q}(\alpha)$.

Take a prime ideal $(2) \subseteq A$, then $(2)\mathcal{O}_K$