Chapter 1

Rings

Definition 1 (Ring)
A ring is a set equipped with two binary operations "$+$" (addition) and "$\cdot$" (multiplication) satisfying the following three sets of axioms, called the ring axioms.

Remark 1
- A nonzero commutative ring in which every nonzero element has a multiplicative inverse is a field.
- A structure with the same axiomatic definition but omitting the requirement of a multiplicative identity is called a rng.

Example 1
1. $(\mathbb{Z}, +, \cdot)$
2. All fields, such as $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$, are rings.
3. The zero ring, denoted $\{0\}$ with the operations $0 + 0 = 0$ and $0 \cdot 0 = 0$ is a commutative ring.
4. 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 $\mathbb{R}[X]$.
5. For any ring R and for any $n \in \mathbb{N}$, the set of all square n-by-n matricies 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 Integral Domain

Integral domains are generalization of the ring of integers and provide a natural setting for studying divisibility. In an integral domain, every nonzero element a has the cancellation property, that is, if $a \neq 0$, an equality $ab = ac$ implies $b = c$.

Definition 2
An integral domain R is a nonzero commutative ring in which the product of any two nonzero elements is nonzero, i.e. for all $a, b \in R \setminus \{0\}$ it is $a \cdot b \neq 0$. Equivalently:

1. An integral domain R is a nonzero commutative ring with no nonzero zero divisors, i.e. there exists no element $a \in R \setminus \{0\}$ such that $a \cdot x = 0$ for some $x \in R$.
2. An integral domain R is a commutative ring in which the zero ideal $\{0\}$ is a prime ideal.
3. An integral domain R is a nonzero commutative ring for which every nonzero element is cancellable under multiplication, i.e. if $a \in R \setminus \{0\}$, an equality $ab = ac$ implies $b = c$.
4. An integral domain R is a ring for which the set of nonzero elements is a commutative monoid under multiplication.
5. An integral domain R is a nonzero commutative ring in which for every nonzero element r, the function that maps each element x of the ring to the product xr is injective. Elements r with this property are called regular, so it is equivalent to require that every nonzero element of the ring be regular.
6. An integral domain R is a ring that is isomorphic to a subring of a field.

Example 2

1. $\mathbb{Z}$.
2. Every field such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ are integral domains.

1.2 Unique Factorization Domain

A unique factorization domain (UFD) or factorial ring is an integral domain in which every nonzero non-unit element can be written as a product of prime elements, uniquely up to order and units. Therefore, in a unique factorization domain a statement analogous to the fundamental theorem of arithmetic holds.

Definition 3
A unique factorization domain is an integral domain R in which every nonzero element can be written as a product of unit and prime elements of R.

1.3 Noetherian Ring

1.4 Dedekind Domain

1.5 Principal Ideal Domain

A principal ideal domain (PID) is an in which every ideal is principal, i.e., can be generated by a single element. Thus, principal ideal domains are structures that behave somewhat like the integers, with respect to divisibility as firstly, any element of a principal ideal domain has a unique decomposition into prime elements, and secondly, any two elements of a principal ideal domain have a greatest common divisor.

Chapter 2

something

2.1 No idea yet

Definition 4 (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 3

- All ordinary ideals $I \subset A$ are also fractional ideals with denominator $d = 1$, and are often referred to as integral ideals.
- The subset
$$\frac{3}{25}\mathbb{Z} = \left\{ \frac{3n}{25} \in \mathbb{Q} \,\middle|\, n \in \mathbb{Z} \right\} \subset \mathbb{Q} \tag{2.1}$$
is a principal fractional ideal of $\mathbb{Z}$

Example 4
The subset
$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ a_0 + a_1\frac{1}{2} + a_2\frac{1}{2^2} + \cdots + a_n\frac{1}{2^n} \,\middle|\, a_0, \ldots, a_n \in \mathbb{Z} \subset \mathbb{Q} \right\} \tag{2.2}$$
is not a fractional ideal, because the denominators are not bounded.

Lemma 4.1 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 4.2 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
$$(I : J) := \{\, x \in K \mid xJ \subset I \,\} \tag{2.3}$$
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 forme an abelian group $Id(A)$.

Definition 5
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 5.1 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 5.2 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 $\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_n \subset I$.

Let

$$\Sigma = \{\, I \neq \{0\} \mid I \subset A \text{ ideal. } I \text{ does not contain any product of nonzero prime ideals.} \}. \tag{2.4}$$

If $\Sigma \neq \varnothing$, 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 maximility 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

$$\mathfrak{p}_1, \dots, \mathfrak{p}_n \subseteq I + (a) \tag{2.5}$$
$$\mathfrak{q}_1, \dots, \mathfrak{q}_n \subseteq I + (b). \tag{2.6}$$

We have

$$\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_n \cdot \mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_m \subseteq (I + (a))(I + (b)) \subseteq I \tag{2.7}$$

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

Theorem 5.1 Let A be a Dedekind domain, I a nonzero ideal, and $\mathfrak{p}$ a prime ideal such that $I \subseteq \mathfrak{p}$. Set

$$\mathfrak{p}^{-1} := (A : \mathfrak{p}) = \{x \in \mathrm{Quot}(A) \mid x\mathfrak{p} \subseteq A\}. \tag{2.8}$$

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

$$Id(A) = \{I \subseteq K \mid I \text{ is a nonzero fractional ideal.}\}. \tag{2.9}$$

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

$$\varphi : K^* \to Id(A), \quad \frac{a}{b} \mapsto \left(\frac{a}{b}\right) = \left\{ \frac{ac}{b} \middle| c \in A \right\} \subseteq K, \tag{2.10}$$

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

Definition 6
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 2 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
$$1 \to A^* \to K^* \to Id(A) \to Cl(A) \to 0. \tag{2.11}$$

2.2 Divisibility and unique factorization of ideals

Theorem 6.1 Let $I \subseteq K = \mathrm{Quot}(A)$ be a nonzero fractional ideal of A.

1. There exist an integer $n \in \mathbb{N}_0$, distinct nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq A$, and integers $r_1, \ldots, r_n \in \mathbb{Z} \setminus \{0\}$ such that
$$I = \mathfrak{p}_1^{r_1} \cdot \ldots \cdot \mathfrak{p}_n^{r_n} \tag{2.12}$$
with the convention that the empty product $n = 0$ is A, and $\mathfrak{p}^{-r} := \left(\mathfrak{p}^{-1}\right)^r$ for any nonzero $r \in \mathbb{N}$.
2. The decomposition is unique up to permutation of the factors.
3. $I \subseteq A$ if and only if $r_1, \ldots, r_n \geq 0$.

Corollary 2 the chinese remainder theorm.

Definition 7
For every nonzero prime ideal $\mathfrak{p} \subseteq A$, we define $v_{\mathfrak{p}}(I) \in \mathbb{Z}$ as the exponent of $\mathfrak{p}$ in the unique factorization of I into a product prime ideals.

2.3 The case of local Dedekind domains

Definition 8
A ring A is called local if it contains a unique maximal ideal $\mathfrak{m}$. Sometimes one says that the pair $(A, \mathfrak{m})$ is a local ring.

2.4 Chapter 5

How to compute the prime factorization $I = \mathfrak{p}_1^{r_2} \cdot \ldots \cdot \mathfrak{p}_n^{r_n}$ 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 $I \cap A' \subseteq A' \Rightarrow I \cap A' = \tilde{\mathfrak{p}}_1^{s_1}, \cdot \ldots \cdot \tilde{\mathfrak{p}}_k^{s_k}$.
2. Factorize $\tilde{\mathfrak{p}}_i^{s_i} \cdot A \subset A \Rightarrow \tilde{\mathfrak{p}}_1^{s_1} \cdot A = \prod_{j=1}^{N_i} \mathfrak{p}_{i,j}^{e_{i,j}}$.
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 approch is

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

Definition 9
The spectrum of a ring A is

$$\mathrm{Spec}(A) = \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ prime ideal}\}. \tag{2.13}$$

Lemma 9.1 In the $AKLB$-setting, let $\mathfrak{p} \subseteq A$ and $\mathfrak{q} \subseteq B$ be prime ideals. Then the following holds.

1. $\mathfrak{q}$ divides $\mathfrak{p}B$ if and only if $\mathfrak{p} = \mathfrak{q} \cap A$.
2. Given $\mathfrak{p}$, there is always such a $\mathfrak{q}$.

1. We have

$$\begin{aligned}
&\mathfrak{q} \mid \mathfrak{p}B && && (2.14)\\
\iff &\mathfrak{p}B \subseteq \mathfrak{q} && \text{there is a lemma for this} && (2.15)\\
\iff &\mathfrak{p} \subseteq \mathfrak{p}B \cap A \subseteq \mathfrak{q} \cap A && && (2.16)\\
\iff &\mathfrak{p} = \mathfrak{q} \cap A && && (2.17)
\end{aligned}$$

Definition 10
Let A be a Dedekind domain, $K = \text{Quot}(A)$ its field of fraction, L/K a finite separable field extension, and $B = \overline{A}$ 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. $e_{\mathfrak{q}|\mathfrak{p}} = v_{\mathfrak{q}}(\mathfrak{p}B) \in \mathbb{Z}_{>0}$ the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$.

Example 5
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. $p\mathbb{Z}[i] = \mathfrak{q}^2 = (1+i)^2$ for $p = 2$, i.e. $(2) \subseteq \mathbb{Z}$ is ramified (with ramification index $e_{\mathfrak{q}|\mathfrak{p}} = 2$). The residue class field $\mathbb{F}_{\mathfrak{q}} \cong \mathbb{F}_2$, hence

Example 6
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 $(2)\mathcal{O}_K$

Theorem 10.1 Let A be a ring and let $B = A[\alpha]$, and let $f(X) \in A[X]$ be the minimal polynomial of α. Moreover, let $\mathfrak{p} \subseteq A$ be a nonzero prime ideal and $g_1(X), \ldots, g_r(X) \in A[X]$ monic such that

$$\overline{f(X)} = \overline{g_1(X)}^{e_1} \cdot \ldots \cdot \overline{g_r(X)}^{e_r} \mod p \in A/\mathfrak{p}[X] = \mathbb{F}_p[X]. \tag{2.18}$$

Then,

$$\mathfrak{p}B = \prod_{i=1}^{r} Q_i^{e_i} \qquad \text{with } Q_i = (\mathfrak{p}, g_i(\alpha)) \subseteq B \tag{2.19}$$

is the prime factorization of $\mathfrak{p}B$.

Example 7
Let $D \in \mathbb{Z}$ be squarefree with $D \equiv 2, 3 \mod 4$ and $L = \mathbb{Q}(\sqrt{D})$, such that $B = O_L = \mathbb{Z}[\sqrt{D}]$ with the minimal polynomial $f(X) = X^2 - D \in \mathbb{Z}[X]$.

Let $p \in \mathbb{Z}$ be a prime number and look for the factorization of $pB = p\mathcal{O}_L = p\mathbb{Z}[\sqrt{D}]$.
Case A: If $p \neq 2$ consider the factorization of $X^2 - D \in \mathbb{Z}/p\mathbb{Z}[X] = \mathbb{F}_p[X]$.
Case A1: If $p \mid D$ then $\overline{f(X)} = X^2$, so $pB = (p, \sqrt{D})^2$, with $B/(p, \sqrt{p}) \cong \mathbb{F}_p[X]/(X) \cong \mathbb{F}_p$.

Example 8
Denote $\alpha = \sqrt[3]{2}$ and let $A := \mathbb{Z}$,

2.5 Ramification

Definition 11 (Ramification Index)
Let K be an algebraic number field of degree n. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Let p be a rational prime lying below P. Then the unique positive integer e such that

$$\mathfrak{p}^e \mid (p),\, \mathfrak{p}^{e+1} \not\mid (p) \tag{2.20}$$

is called the ramification index of $\mathfrak{p}$ in K and is written $e_K(\mathfrak{p})$.