Chapter3 Rings and Modules

Contents

1 Definiton of ring

1.1 Basic Motivation:End(G)

The basic motivation of introduction of ring is the $\mathrm{Hom}_{\mathbf{Ab}}(G,G)$(or simply $\mathrm{End}(G)$), that is, the set of all endmorphism over an abelian group G. We can define the so called addition over this set as follows:

$$(\forall f,g \in \mathrm{End}(G) : (f+g)(a) = f(a) + g(a)$$

It's easy to show that $\mathrm{End}(G)$ forms an abelian group if G is abelian. One thing to rememebr is that not any general group G satisfies $\mathrm{End}(G)$ is an abelian group. The key point is that the above-defined $f+g$ might not be a group homomorphism if G is not abelian:

$$\begin{aligned}
&(\forall f,g \in \mathrm{End}(G), a,b \in G) : \\
&\qquad (f+g)(a+b) = f(a+b) + g(a+b) \\
&\qquad\qquad = f(a) + f(b) + g(a) + g(b) \\
&\qquad\qquad \xlongequal{G\ is\ abelian} f(a) + g(a) + f(b) + g(b) \\
&\qquad\qquad = (f+g)(a) + (f+g)(b)
\end{aligned}$$

In conclusion, $\mathrm{End}(G)$ forms an abelian group under homomorphism addition. However, there is another type of operation: **Composition of homomorphisms**

$$(f,g \in \mathrm{End}(G)) : (f \circ g)(a) = f(g(a))$$

Thus, there are two kinds of different operations within set $\mathrm{End}(G)$. That's the basic motivation of a new algebra structure, called **ring**.

1.2 Definition of ring

A ring $(R,+,)$ is an **abelian group** $(R,+)$ endowed with a second binary operation(often omit this dot notion), satisfying of its own the requirements of being associative and having a two-sided identity:

- **Associativity**: $(\forall r,s,t \in R) : \quad (rs)t = r(st)$

- **Existence of Identity**: $(\exists 1_R \in R)(\forall r \in R): \quad 1_R r = r 1_R = r$

  Also, there are laws combining two different operations, called **distributive law**:

- $(\forall r, s, t \in R): \quad r(s+t) = rs + rt, (r+s)t = rt + st$

The operation $+$ and $\cdot$ are called addition and multiplication resepctively.

Here are one point to note : Within this book, a ring is always to be considered have **multiplication identity**. Some other definition may not require a ring to have an identity.

Examples

- **Trivial ring**. There is only one element $\{0\}$, which is the addition identity.
- **Integer ring**. $(\mathbb{Z}, +, \times)$ forms a ring, where addition and multiplication are naturally integer addition and multiplication.
- **Modular ring**. The addition group $\mathbb{Z}/n\mathbb{Z}$ forms a ring. The addition and multiplication is modular addition and multiplication.
- **Matrix ring**. All square matrix of order n forms a ring, the addition and multiplication are matrix addition and multiplication.

1.3 Rings with special properties

1.3.1 Commutative ring

Definition 1. *(Commutative Ring) A ring R is commutative, if multiplication is commutative, that is*

$$(\forall r, s \in R): \quad rs = sr$$

R is called commutative ring under in such case.

In our examples, $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ are commutative rings. But matrix ring is not.

1.3.2 Zero divisors and Integral domain

Definition 2. *(zero-devisor) Let R be a ring, and an element $r \in R$ is a left(resp.right) zero-divisor, if*

$$(\exists s \in R, s \neq 0): \quad rs = 0 (sr = 0)$$

The following proposition depicts the property of a zero-divisor:

Proposition 1. *Let R be a ring and $r \in R$ is an element. The following statements are equavialent:*

- *r is **not** a left zero divisor.*
- *Function: $f: R \longrightarrow R, a \mapsto ra$ is injective.*

It is easy to prove the proposition and the right zero divisor case. By the definiton of R, we give the following definiton of integral domain:

Definition 3. *A ring R is called an integral domain, if it is **commutative** and has no zero-divisors, i.e.*

$$(\forall a, b \in R) \quad ab = 0 \Longrightarrow a = 0 \text{ or } b = 0$$

According to the definiton of integral domain and the property of zero-divisors We have the cancellation law holds:

(Cancellation) If R is an integral domain, then:

$$(\forall a, b, c \in R, a \neq 0): \quad ab = ac \Longrightarrow b = c$$

That is, in integral domain we can simply cut off the same component in a multiplication expression, which is the same as we do in group.

Examples $\mathbb{Z}$ is an integral domain. However, both $Z/n\mathbb{Z}$ and matrix ring are not integral domain in general case. For example, in matrix ring of order 2, we have:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

In $\mathbb{Z}/6\mathbb{Z}$, we have $[2]_6 \times [3]_6 = [0]_6$. Thus $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain. However, there is a class of n that makes $\mathbb{Z}/n\mathbb{Z}$ integral domain, in particular, they are actually field.

1.3.3 Unit and division ring

Definition 4. *Let R be a ring and an element $r \in R$. r is called a left(resp. right) unit if*

$$\exists v \in R, uv = 1(resp.\ vu = 1)$$

r is an unit if it is both left and right side unit.

Similar to zero divisor, we given a depiction of unit as the following proposition:

Proposition 2. *Let R be a ring and $r \in R$.*

- *r is a left unit $\Longleftrightarrow f : R \longrightarrow R, a \mapsto ra$ is surjective*
- *r is a left unit $\Longrightarrow r$ is not a right zero-divisor*
- *The inverse of two-sided unit is unique*
- *The set of all two-sided unit forms a group.*

Proof. The proof of above propositions are easy. For the third proposition we could actually prove that if r is a two sided unit, then the left-inverse and right inverse equals.

$$u = u1 = u(rv) = (ur)v = 1v = v$$

That's why we can use the word *inverse* to denote both left and right inverse. □

Definition 5. *(division ring and field) A division ring is a ring in which every non-zero element is an unit. A field is a non-zero commutative division ring.*

It's obviously that both $\mathbb{Q}, \mathbb{R}$ are fields. The following theorem implies a class of special modular group:

Theorem 1. *$\mathbb{Z}/n\mathbb{Z}$ is field if and only if n is a prime.*

Hint. We only need to show that $[a]_n$ is unit if and only if $\gcd(a, n) = 1$.

Theorem 2. *R is a finite commutative ring, then R is field if and ony if R is integral domain.*

Hint. Field is naturally an integral domain. If R is an integral domain, prove that each $r \in R$ is unit by considering the left multiplication function. It must map some element to 1 since R is finite and this map is injective. More specificly, one injective map from a finite set to iteself must be surjective

1.4 Other examples of rings

1.4.1 Polynomial rings

Let R be a ring and define a polynomial $f(x)$ over R as the following form:

$$f(x) = \sum_{i \geq 0} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots$$

Note that each $f(x)$ only has finitely many summation. The set of all $f(x)$ is a ring, called Polynomial ring over R, denoted as $R[x]$.

Definition 6. *(Degree of polynomial) Let $f(x) \in R[x]$, the degree of $f(x)$, denoted as $degf$, is the maximum n such that $a_n \neq 0$. Typically we define $degr = 0, r \in R$ and $deg0 = -\infty$.*

When R is an integral domain, $R[x]$ is also an integral domain. And the following equation holds:

$$\deg(fg) = \deg f + \deg g$$

1.4.2 Monoid rings

Monoid rings is a ring constructed from a monoid and a ring. Here is the definition:

Definition 7. *(Monoid rings) Let R be a ring and M a monoid, then consider all the following linear combinations:*

$$\sum_{m\in M} a_m \cdot m, a_m \in R$$

Where only finitely many $a_m \neq 0$. The addition and multiplication are defined as follows:

$$\sum_{m\in M} a_m \cdot m + \sum_{m\in M} b_m \cdot m = \sum_{m\in M} (a_m + b_m) \cdot m$$
$$(\sum_{m\in M} a_m \cdot m)(\sum_{m\in M} b_m \cdot m) = \sum_{m\in M} (\sum_{m_1 m_2 = m} a_{m_1} b_{m_2}) m$$

Under this definition, it's easy to show that all combination forms a ring. It is called Monoid rings, denoted as $R[M]$. Actually, the polynomial ring is a special case of general monoid ring, where we take $M = \{1, x, x^2, x^3, \dots\}$.

2 Category Ring

2.1 Ring homomorphism

A ring homomorphism is a function between two rings that maintains two operations: $\cdot$ and $+$, that is:

Definition 8. *Let R, S be rings, a function $f : R \to S$ is a ring homomorphism, if:*

- $(\forall a, b \in R) : \quad f(a + b) = f(a) + f(b)$
- $(\forall a, b \in R) : \quad f(ab) = f(a)f(b)$
- $f(1_R) = 1_S$

Since f is a function maintains $+$, it is basically a group homomorphism of the underlying abelian group. Thus, it naturally has: $f(0_R) = 0_S$. However, the second axiom does not induce the third one. That is: a function maintains both $\cdot$ and $+$ might be send identity to identity. For example:

$$f : \mathbb{Z} \to \mathbb{Z}, a \mapsto 0$$

is a function maintaining both addition and multiplication. But it is not a ring homomorphism since it does not meet the third requirements.

Proposition 3. *Let R, S be non-zero rings, $f : R \to S$ is a ring homomorphim, the following statement is true:*

- *If $r \in R$ is an unit, then $f(r)$ is an unit in S, $f(r)^{-1} = f(r^{-1})$*
- *If $r \in R$ is a zero-divisor, then $f(r)$ might not be a zero-divisor as $f(r)$ might be zero.*
- *The composition of ring homomorphism is still a ring homorphism.*

2.2 Category Ring

The category "Ring" consists all rings, and the morphism set between two objects is the ring homomorphisms.

There are some interesting results in **Ring**: $\{0\}$ is a final object in **Ring** but not a initial object. The reason is that the identity in $\{0\}$ is exactly its zero, which means $\{0\}$ only has a ring homomorphism to itself. $(\mathbb{Z}, \cdot, +)$ is an initial object in **Ring**: any homomorphism $f : \mathbb{Z} \to R$ is uniquely determined by $f(1)$, i.e $f(n) = nf(1) = n1_R$.

The following proposition describes the universal property of polynomial ring on $\mathbb{Z}$:

Theorem 3. *Let A be a finite set: $A = \{a_1, a_2, \dots, a_k\}$. Consider a new category $\mathscr{R}_A$: The object of $\mathscr{R}_A$ is (j, R), where R is a ring, and j is a set-function from A to R.*

$$j : A \to R$$

The morphism from object (j_1, R_1) to (j_2, R_2) is the following diagram:

$$\begin{tikzcd} R_1 \arrow[r, "\varphi"] & R_2 \\ A \arrow[u, "j_1"] \arrow[ur, "j_2"'] & \end{tikzcd}$$

Then $(\mathbb{Z}[x_1, x_2, \dots, x_k], \iota)$ is an initial object in $\mathscr{R}_A$, where $\iota(a_i) = x_i, i = 1, 2, \dots, k$.

Proof. The proof this this theorem is pretty straight forward. We need to show for each (j, R) in $\mathscr{R}_A$, the following diagram is true: To prove this, one itutive way is to map each polynomial to its coresponding "value": x_i is replaced as $j(a_i)$, and the whole polynomial forms a linear summation of multiplication consists of $j(a_i)$. The uniqueness is determined by the property of homomorphism.

For each object (R, j), we need to show the following diagram holds:

$$\begin{tikzcd} \mathbb{Z}[x_1, x_2, \dots, x_k] \arrow[r, "\exists!\varphi"] & R \\ A \arrow[u, "\iota"] \arrow[ur, "j"'] & \end{tikzcd}$$

For a fixed object (R, j), define φ as follows:

$$\begin{aligned} \varphi(\sum_i a_i x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}) &= \sum_i \varphi(a_i)\varphi(x_1)^{i_1}\varphi(x_2)^{i_2} \cdots \varphi(x_k)^{i_k} \\ &= \sum_i (a_i 1_R)\varphi(\iota(a_1))^{i_1}\varphi(\iota(a_2))^{i_2} \cdots \varphi(\iota(a_k))^{i_k} \\ &= \sum_i (a_i 1_R)(j(a_1))^{i_1}(j(a_2))^{i_2} \cdots (j(a_k))^{i_k} \end{aligned}$$

In the above construction, we do not only present a ring homomorphim that maps from $\mathbb{Z}[x_1, x_2, \dots, x_k]$ to R, but also shows the uniqueness by using the fact that R must maintains both addition and multiplication. Thus φ is unique. The key to the proof is that the fact that $\mathbb{Z}$ is initial in **Ring**. □

2.3 Monomorphism and Epimorphism

2.3.1 Monomorphism

Definition 9. *(Kernel of ring homomorphim) Let R, S be rings and f a ring homomorphism from R to S, define kernel of this homomorphism as:*

$$\ker f = \{r \in R \mid f(r) = 0_S\}$$

Theorem 4. *(Equavalence of ring monomorphism) Let f be a ring homomorphism from R to S, the following statements are equavalent:*

1. *f is monomorphism*
2. $\ker f = \{0_R\}$
3. *f is injective as set-function*

Proof. (1) ⇒ (2) Consider the following diagram:

□

2.3.2 Epimorphism

Definition 10. *A ring homomorphism $f : R \to S$ is a ring homomorphism, if and only if for any ring T and ring homomorphism $S \to T, \varphi_1, \varphi_2$:*

$$f \circ \varphi_1 = f \circ \varphi_2 \Longrightarrow \varphi_1 = \varphi_2$$

That is, the following commutative diagram

$$\begin{tikzcd} R \arrow[r, "f"] & S \arrow[r, shift left, "\varphi_1"] \arrow[r, shift right, "\varphi_2"'] & T \end{tikzcd}$$

indicates $\varphi_1 = \varphi_2$.