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:

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

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 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.*

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

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*

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

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 $deg f$, is the maximum n such that $a_n \neq 0$. Typically we define $deg r = 0, r \in R$ and $deg 0 = -\infty$.*

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: · 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 · 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: $A = \{a_1, a_2, \ldots, a_k\}$. 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 $(\mathbb{Z}[x_1, x_2, \ldots, x_k], \iota)$ is an initial object in $\mathscr{R}_A$, where $\iota(a_i) = x_i, i = 1, 2, \ldots, k$.

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 ituitive 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:

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

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 $\mathbb{Z}[x_1, x_2, \ldots, x_k]$ 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) $\Rightarrow$ (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 $\varphi_1 = \varphi_2$.

3 Ideals and quotients: remarks and examples

Most of contents used in this section would assume R is a commutative ring. We would explicitly point it out if R is non-commutative.

Definition 11. *(Principle Ideal) Ra is a left-side ideal, and aR is a right-side ideal. If R is commutative, then Ra is a two-sided ideal, called principle ideal generated by a, denoted as (a).*

Let $S = \{a_1, a_2, \dots a_k\}$, the ideal generated by S is the minimal ideal that contains S. It is easy to prove that the ideal generated by S is:

$$(a_1) + (a_2) + \dots + (a_k) = \{\sum_{i=1}^{k} r_i a_i \mid r_i \in R\}$$

And this ideal is denoted as $(a_1, a_2, \dots, a_k)$. If k is finite, then $(a_1, a_2, \dots, a_k)$ is called *finitely-generated.* A special class of ring that widely used in algebraic geometry is as follows:

Definition 12. *A commutative ring R is called Noetherian if every ideal is finitely generated.*

Definition 13. *An integral domain R is called principle ideal domain(PID), if every ideal of R is principle ideal.*

It's that PID is a special case of Noetherian ring. There are some basic facts that we know as follows:

1. $\mathbb{Z}$ is a PID.
2. If k is a field, then the polynomial ring $k[x]$ is a PID.
3. $\mathbb{Z}[x]$ is not PID, for example, ideal $(2, x)$ is not a principle ideal.

Both $\mathbb{Z}$ and $k[x]$ are *Euclidean domain*, namely, it means a domain where the Euclidean algorithm holds. $\mathbb{Z}[x]$, however, are not that special, but it is an UFD, which stands for *Unique Factorization Domain.*

3.1 Quotient of polynomial ring

This section considers a special quotient of polynomial ring $R[x]$. Let $f(x) \in R[x]$ be a *monic* polynomial, i.e. the leading coefficient of $f(x)$ needs to be exactly 1. Then for each $g(x) \in R[x]$, there exists unique $h(x), r(x) \in R[x]$, such that:

$$g(x) = h(x)f(x) + r(x), \deg r(x) < \deg f(x)$$

This is basically what Euclidean algorithm tells us, but note that this might not be true if $f(x)$ is not monic. For example, consider $\mathbb{Z}[x]$, and $f(x) = 2x + 1$. Then

$$x + 1 = (2x + 1) \times 1 + (-x)$$

Addmiting the above equations, we continue by considering the principle ideal $(f(x))$, and quotient $R[x]/(f(x))$. $R[x]/(f(x))$ consists of all cosets such that:

$$R[x]/(f(x)) = \{r(x) + (f(x)) \mid r(x) \in R[x]\}$$

Considering the following fact:

$$g(x) = f(x)g(x) + r(x) \Rightarrow g(x) + (f(x)) = r(x) + (f(x))$$

This means:

$$R[x]/(f(x)) = \{\overline{r(x)} \mid \deg r(x) < \deg f(x)\}$$

Thus, we basically view $R[x]/(f(x))$ (in group concept) as addtiion group consists of all polynomials with degree less than $\deg f(x)$. More formly, that is:

$$R[x]/(f(x)) \cong R^{\oplus d}$$

where d is the degree of $f(x)$. The isomorphism φ would be:

$$\varphi(\overline{r(x)}) = \varphi(\sum_{i=0}^{d-1} r_i x^i) = (r_0, r_1, \ldots, r_{d-1})$$

It's basically naive to verify this function is indeed a group homomorphism between two abelian groups. One of most trivial examples would be:

$$R[x]/(x-a) \cong R$$

One more complex example is considering $f(x)$ with degree of 2, for example:

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{R}^2$$

The isomorphism, as explained, is $\varphi(a_0 + a_1x) = (a_0, a_1)$. However, in what condition does this isomorphism is also a ring homomorphism? This typically requires:

$$\varphi((a_0 + a_1x)(b_0 + b_1x)) = \varphi(a_0 + a_1x)\varphi(b_0 + b_1x)$$

Note that $\varphi(a_0b_0 + (a_0b_1 + a_1b_0)x + a_1b_1x^2) = \varphi((a_0b_0 - a_1b_1) + (a_0b_1 + a_1b_0)x + (a_1b_1)(x^2+1)) = (a_0b_0 - a_1b_1, a_0b_1 + a_1b_0)$, thus we must have

$$(a_0b_0 - a_1b_1, a_0b_1 + a_1b_0) = (a_0, b_0)(a_1, b_1)$$

Conversely, if we define multiplication over $\mathbb{R}^2$ as above, $\mathbb{R}^2$ does form a ring. And this ring, is exactly isomorphic to $\mathbb{C}$.

3.2 Prime ideal and maximal ideal

There are actually two equavalent definitions of prime ideal and maximal ideal.

Definition 14. *Let $I \neq (1)$ be an ideal of a commutative ring R.*

1. *I is a prime ideal, if R/I is an integral domain*
2. *I is a maximal ideal, if R/I is a field*

The equavalent definitions would be:

Definition 15. *Let $I \neq (1)$ be an ideal of a commutative ring R.*

1. *I is a prime ideal, if $ab \in I \Rightarrow a \in I$ or $b \in I$*
2. *I is a maximal ideal, if for any ideal $J \subseteq R$, $I \subseteq J \Rightarrow I = J$ or $J = R$.*

There is no difficulty to prove these two definitions equals to each other. But it seems more reasonable if we call the second group definition and the first group 'properties'.

According to the definition, one obvious fact would be maximal ⇒ prime since R/I is a field induces R/I is an integral domain. Further more, the following theorem extends this relationship between prime ideal and maximal ideal:

Theorem 5. *If R is a PID, then an ideal $I \neq R$ is prime if and only if I is maximal.*

Proof. We only prove prime ⇒ maximal. If $I = (a)$ is prime, consider another ideal $J = (b)$ that contains I, then we have $a \in J = (b)$. Thus, there exists $c \in R$, such that $a = bc$. Note that $bc = a \in I$ and I is prime. This indicates $b \in I$ or $c \in I$. If $b \in I$, we have $(b) \subseteq I$ and $(b) = I$. If $c \in I$, we further have some d and $c = da$. Then:

$$a = bc = bda \overset{!}{\Longrightarrow} 1 = bd \quad (R \text{ is integral domain})$$

b is an unit and $J = (b) = R$. In conclusion, J is either I or R. I is maximal according to the definition. □

The set of all prime ideals of R is called the *spectrum* of R.

4 Modules over ring

4.1 Definition of R-module

Conceptually, an R-module is a ring action on an abelian group M, by action, we mean a ring homomorphism from R to $\mathrm{End}_{\mathrm{Ab}}(M)$. And one element $r \in R$ acts on one element $m \in M$ actually means the target ring endmorphism maps m.

Definition 16. *Let R be a ring, an abelian gorup M is said to be a left R-module, if there exists one function:*

$$R \times M \to M, (r, m) \mapsto rm$$

such that, $\forall r, s \in R, m, n \in M$:

- $r(m + n) = rm + rn$
- $(r + s)m = rm + sm$
- $(rs)m = r(sm)$
- $1m = m$

Similarly we can define the structure of right-R-module. If R is commutative, both left-R-module and right-R-module are exactly the same. We will call R-module and ommit "left" for simplicity.

There are many examples of R-module. For example, any abelian group is actually one $\mathbb{Z}$-module. A special class of R-module, endowed with ring structure, is R-algebra. Check the textbook for more details.

4.2 Category R-Mod

Definition 17. *Let M, N be R-modules, one function φ from M to N is called R-module homomorphism if it is an abelian and maintain module structure:*

- $(\forall m_1, m_2 \in M): \quad \varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$
- $(\forall r \in R, m \in M): \quad \varphi(rm) = r\varphi(m)$

All R-modules endowed with R-module homomorphism forms a category, called R-Mod. There are similarities between R-Mod and Ab, one particular example is that $\mathrm{Hom}_{R-Mod}(M, N)$ is also an abelian group and actually an R-module if R is commutative.

4.3 Submodule and quotients

Conceptually, a submodule is a subset that maintains module structure. The formal definition is as follows:

Definition 18. *Let M be R-module, a submodule $N \subsetneqq M$ is a subgroup of abelian group M and for each $r \in R, n \in N$, $rn \in N$.*

Thus, a left ideal of R can be viewed as a submodule of R. Obviously, let $r \in R$ be a fixed element, then rM is a submodule of M(if R is commutative). Let I be an ideal of R, then the set $IM = \{rm \mid r \in I, m \in M\}$ is also a submodule of M.

Let N be a submodule of M, since N is a subgroup of M in abelian conception, there is naturally one quotient group: M/N. The question is, how to construct an R-module structure over this quotien group? One intuitive way is:

$$(\forall r \in R, m + N \in M/N): \quad r(m + N) := rm + N$$

This definition is well-defined: if $m_1 + N = m_2 + N$ then $m_1 - m_1 \in N$, and $r(m_1 - m_2) \in N$ according to the definition of submodule. Thus $rm_1 + N = rm_2 + N$. It's also easy to verify this "action" meets the requirements of an R-modules.

Abelian group M/N endowed with "ring action" defined above has a module structure, it is called quotient module M by N.

The universal property of M/N is similar to group and ring counterparts, as follows:

Theorem 6. *Let M be one R-module and N a submodule of M, if P is another R-module with an R-module homomorphism such that $N \subseteq \ker\varphi$. Then the following diagram is commutative:*