Lecture Notes On Abstract Algebra (Week 6)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

Contents

1 Lecture 10 (Oct 10, 2023): Noetherian Rings and Artinian Rings

1.1 Noetherian Ring

The Noetherian property is central in ring theory and in areas that make heavy use of rings, such as algebraic geometry. The reason behind this is that the Noetherian property is in some sense the ring-theoretic analogue of finiteness. For example, the fact that polynomial rings over a field are Noetherian allows one to prove that any infinite set of polynomial equations can be replaced with a finite set with the same solutions.

We say a ring R satisfies the *ascending chain condition* (ACC) on ideals (理想的升链条件), if every ascending chain of ideals terminates. That is, given any chain of ideals of R:

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_k \subseteq \cdots,$$

there exists an n such that

$$I_n = I_{n+1} = \cdots.$$

A ring R is called **Noetherian** (Noether环) if it satisfies ACC (ascending chain condition) on ideals.

Example 1.1. Any principal ideal domain, such as the integers, is Noetherian since every ideal is generated by a single element. This includes PIDs and Euclidean domains.

Example 1.2. The ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$ is not Noetherian: let I_n be the ideal of all continuous functions f such that $f(x) = 0$ for all $x \geq n$. The sequence of ideals $I_0, I_1, I_2, \cdots$ is an ascending chain that does not terminate.

Theorem 1.1. *Let R be a ring. TFAE (The following are equivalent):*

1. *The ring R is Noetherian.*
2. *The ring R satisfies the maximal condition on ideals (i.e. every non-empty set of ideals that is partially ordered by inclusion has a maximal element).*
3. *Every ideal of R is finitely generated.*

Example 1.3. 1. *A unique factorization domain (UFD) is not necessarily a Noetherian ring.* A UFD does satisfy a weaker condition: the ascending chain condition on principal ideals. For example, the ring of polynomials over a field in infinitely many variable $F[x_1, x_2, \cdots]$ is a UFD that is non-noetherian (see explanation in the following example).

2. *A subring of a Noetherian ring is not necessarily Noetherian.* For example, take a polynomial ring over a field F in infinitely many indeterminates, $F[x_1, x_2, \cdots]$. The quotient field $F(x_1, x_2, \cdots)$ is then Noetherian, but the subring $F[x_1, x_2, \cdots]$ is not, since there is an infinite ascending chain of ideals which never stabilizes:

$$(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots$$

We have many ways to construct Noetherian rings.

Theorem 1.2. *1. If R is noetherian, the quotient ring R/I is Noetherian for any ideal I of R.*

2. (Hilbert's Basis Theorem, 1890) *If R is commutative noetherian ring with identity, so is $R[x]$.*

3. If R is commutative Noetherian ring with identity, so is $M_n(R)$ for all $n \geq 1$.

4. If R is not Noetherian, then $M_n(R)$ is not Noetherian.

Proof of Hilbert's Basis Theorem Suppose $\mathfrak{a} \subseteq R[x]$ is not a finitely generated ideal. Then we can recursively find a sequence of polynomials $f_0, f_1, \ldots$ such that if $\mathfrak{b}_n$ is the ideal generated by $f_0, \ldots, f_{n-1}$ then $f_n \in \mathfrak{a} \setminus \mathfrak{b}_n$ is of minimal degree. It is clear that $\deg(f_0), \deg(f_1), \ldots$ is a non-decreasing sequence of positive integers. Let a_n be the leading coefficient of f_n and let $\mathfrak{b}$ be the ideal in R generated by $a_0, a_1, \ldots$. Since R is Noetherian the chain of ideals

$$(a_0) \subseteq (a_0, a_1) \subseteq (a_0, a_1, a_2) \subseteq \cdots$$

must terminate. Thus $\mathfrak{b} = (a_0, \ldots, a_{N-1})$ for some integer N. So in particular,

$$a_N = \sum_{i<N} u_i a_i, \ u_i \in R.$$

Now consider

$$g = \sum_{i<N} u_i x^{\deg(f_N)-\deg(f_i)} f_i,$$

whose leading term is equal to that of f_N; moreover, $g \in \mathfrak{b}_N$. However, $f_N \notin \mathfrak{b}_N$, which means that $f_N - g \in \mathfrak{a} \setminus \mathfrak{b}_N$ has degree less than f_N, contradicting the minimality.

Remark 1.1. *Hilbert's Basis Theorem is also true even if R is not commutative*: if R is a Noetherian ring, then $R[X]$ is a Noetherian ring. The proof is the same, only all ideals being replaced by left ideals or right ideals.

Corollary 1.1. *1. If R is a noetherian ring with identity, so is the polynomial ring $R[x_1, x_2, \cdots, x_n]$.*

2. Let F be a field, then $F[x_1, x_2, \cdots, x_n]$ is Noetherian.

Remark 1.2. This corollary can be translated into algebraic geometry as follows: every algebraic set over a field can be described as the set of common roots of finitely many polynomial equations.

Example 1.4. As a consequence of the Hilbert basis theorem, the coordinate ring of an affine variety is a Noetherian ring.

A subring of a finitely generated ring may not be finitely generated. For example, the polynomial ring $F[x, y]$ over a field F is Noetherian (by Hilbert's basis theorem), but the subring generated by $\{xy^i \mid i \geq 0\}$ is not finitely generated over F, hence not Noetherian.

1.2 Artin Ring

In 1921, Emmy Noether introduced the ACC for the first time in mathematics literature. Emil Artin formulated the DCC (descending chain condition) in 1927, which provided a minimum condition to complement the maximum condition given by the ACC.

A ring is called **Artinian** (Artin环) if it satisfies the *descending chain condition* (DCC, 降链条件) on ideals; that is, given any chain of ideals:

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_k \supseteq \cdots,$$

there exists an n such that

$$I_n = I_{n+1} = \cdots.$$

Example 1.5. 1. All rings with a finite number of ideals, like $\mathbb{Z}/n\mathbb{Z}$ for $n > 0$, and fields are Artinian and Noetherian.

2. Let F be a field. Then $F[x]/(x^n)$ is an Artin ring for $n > 0$, since it has $n + 1$ ideals.

3. The ring $\mathbb{Z}$ is Noetherian, but not Artinian.

Theorem 1.3. *A ring is Artinian if and only if it satisfies the minimum condition on ideals, i.e. every non-empty set of ideals that is partially ordered by inclusion has a minimal element.*

Proposition 1.1. *Every prime ideal of a commutative Artin ring is maximal.*

Proof. Let $\mathfrak{p}$ be a prime ideal in an Artin ring R. We need to show that $(a) + \mathfrak{p} = R$ for any element $a \in R \setminus \mathfrak{p}$.

Since R is Artinian, the chain $(a)+\mathfrak{p} \supseteq (a^2)+\mathfrak{p} \supseteq \cdots$ must stabilize. That is, $(a^n)+\mathfrak{p} = (a^{n+1})+\mathfrak{p} = (a^{n+2}) + \mathfrak{p} = \cdots$ for some positive integer n. In particular, $a^n \in (a^{n+1}) + \mathfrak{p}$. Hence there exist $b \in R$ and $c \in \mathfrak{p}$ such that $a^n = a^{n+1}b + c$. It follows $a^n(1 - ab) \in \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal and $a \notin \mathfrak{p}$, we must have $1 - ab \in \mathfrak{p}$. Now $1 = ab + (1 - ab) \in (a) + \mathfrak{p}$ and thus $(a) + \mathfrak{p} = R$. □

As an immediate consequence, we have

Corollary 1.2. *An Artinian integral domain is a field.*

Theorem 1.4. *A commutative ring is Artinian if and only if it is Noetherian and every prime ideal is maximal.*

A ring is called a **local ring** (局部环) if it has only one maximal ideal. For example, $\mathbb{Z}/p^2\mathbb{Z}$ is a local ring, where p is a prime.

Theorem 1.5. *Every commutative Artin ring is a direct sum of finite number of commutative Artin local rings.*

The *Artin-Wedderburn Theorem* states that a semisimple Artin ring R is isomorphic to a direct sum of finitely many $n_i \times n_i$ matrix rings over division rings D_i, for some integers n_i, both of which are uniquely determined up to permutation of the index i.

Exercises

1. Which of the following rings are Noetherian?
   (a) The ring of rational functions of z having no pole on the circle $|z| = 1$.
   (b) The ring of power series in z with a positive radius of convergence.
   (c) The ring of power series in z with an infinite radius of convergence.
   (d) The ring of polynomials in z whose first k derivatives vanish at the origin, where k is a fixed integer.
   (e) The ring of polynomials in z, w all of whose partial derivatives with respect to w vanish for $z = 0$.
2. Is a subring of a Artin ring still Artinian?
3. Is a homomorphic image of a Artin ring still Artinian?
4. An prime ideal $\mathfrak{m}$ of R is called *minimal* if there exists no proper prime ideal containing in $\mathfrak{m}$. For example, the zero ideal is minimal in an integral domain. Show that there is only a finite number of minimal primes in a commutative noetherian ring.
5. Let R be a domain. If R is Artinian, then R is a field.
6. Show that a commutative Artin ring has only finitely many prime (maximal) ideals.
7. Let R be a local ring and $x \in R$. Show that either x or $1 - x$ is a unit. Is the converse true?
8. Let R be a commutative Noetherian local ring with maximal ideal $\mathfrak{m}$. Show that
$$\bigcap_{i=1}^{\infty} \mathfrak{m}^i = (0).$$
9. We say that a chain of prime ideals of the form $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ has length n. That is, the length is the number of strict inclusions, not the number of primes. The *Krull dimension* of a commutative ring R is the supremum of the lengths of all chains of prime ideals. Then the Krull dimension of a field is 0, the Krull dimension of $\mathbb{Q}[x]$ is 1, but the Krull dimension of $\mathbb{Z}[x]$ is 2. Generally, the polynomial $F[x_1, x_2, \cdots, x_n]$ has Krull dimension n, where F is a field. Show that an integral domain is a field if and only if its Krull dimension is zero.
10. Show that a commutative local ring has Krull dimension 0 if and only if every element of its maximal ideal is nilpotent.

1.3 Direct Sum of Rings

Given rings $R_1, R_2, \cdots, R_n$, the (external) **direct sum** ((外)直和) $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ is the cartesian product set $R_1 \times R_2 \times \cdots \times R_n$ endowed with addition and multiplication defined by

$$(r_1, r_2, \cdots, r_n) + (s_1, s_2, \cdots, s_n) = (r_1 + s_1, r_2 + s_2, \cdots, r_n + s_n)$$

and

$$(r_1, r_2, \cdots, r_n) \times (s_1, s_2, \cdots, s_n) = (r_1 s_1, r_2 s_2, \cdots, r_n s_n),$$

where the operation in the i-th coordinate position is the relevant operation in R_i. It can be checked that this is a ring.

Example 1.6.

1. The (external) direct sum of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. It's a commutative ring with 6 elements. The ring $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ has zero divisors:

$$(1 \bmod 2, 0) \times (0, 1 \bmod 3) = (0, 0).$$

2. The direct sum $R \oplus R \oplus \cdots \oplus R$ of n copies of R can be viewed as the ring of function on a set of n elements (such as $\{1, 2, \ldots, n\}$) with values in R: an element $(x_1, x_2, \ldots, x_n) \in R \oplus R \oplus \cdots \oplus R$ can be identified with the function f given by $f(i) = x_i$. Addition and multiplication of functions are given as usual by operating on their values.

3. If $R_1, R_2, \cdots, R_n$ are all commutative, so is $R_1 \oplus R_2 \oplus \cdots \oplus R_n$.

4. If each R_i is a ring with identity 1_i, then $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ is also a ring with identity $(1_1, 1_2, \cdots, 1_n)$.

Let $S_1, S_2, \cdots, S_n$ be a finite sequence of subrings of R (not necessarily having the identity). We have the (external) direct sum $S = S_1 \oplus S_2 \oplus \cdots \oplus S_n$. If the natural map

$$\varphi : S \to R$$
$$(x_1, x_2, \cdots, x_n) \mapsto x_1 + x_2 + \cdots + x_n$$

is an isomorphism of rings from S to R, R is said to be a **internal direct sum** (内直和) of $S_1, S_2, \cdots, S_n$. And each S_i is called a *direct summand* (直和因子) of R. In this case we write $R = S_1 \oplus S_2 \oplus \cdots \oplus S_n$.

As in the case of vector spaces or groups, a ring R is a direct of its subrings $R_1, R_2, \cdots, R_n$ if and only if every element $x \in R$ can be written as the sum of the form $x = x_1 + x_2 + \cdots + x_n$ in a unique way with $x_i \in R_i$.

Exercises

1. Let $R \cong R_1 \oplus R_2 \oplus \cdots \oplus R_n$ be an isomorphism of rings. Show that $R^\times \cong R_1^\times \otimes R_2^\times \otimes \cdots \otimes R_n^\times$ is an isomorphism of multiplicative groups.

2. Is there a ring isomorphism from $\mathbb{Z}/p^2\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$? why? Here p is a prime.

3. Is there a ring isomorphism from $\mathbb{Z}/p^2\mathbb{Z}$ to $\mathbb{F}_{p^2}$? Here p is a prime and $\mathbb{F}_{p^2}$ is a finite field with p^2 elements.

2 Lecture 11 (Oct 12, 2023): CRT, Basic Concepts on Module

2.1 Chinese Remainder Theorem

Chinese Remainder Theorem, ancient theorem that gives the conditions necessary for multiple equations to have a simultaneous integer solution. The theorem has its origin in the work of the 4th/5th-century Chinese mathematician Sun Zi, although the complete theorem was first given in 1247 by Qin Jiushao (秦九韶).

Chinese Remainder Theorem (for Commutative Rings) Let R be a commutative ring and let $I_1, I_2, \cdots, I_k$ be ideals of R that are pairwise coprime (meaning $I_i + I_j = (1)$ for all $i \neq j$). Then the quotient ring R/I is isomorphic to the direct sum $R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_k$ via the epimorphism

$$\begin{aligned} \varphi : R &\to R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_k \\ x &\mapsto (x + I_1, x + I_2, \cdots, x + I_k), \end{aligned}$$

with $I = \ker \varphi = I_1 \cap I_2 \cap \cdots \cap I_k$. That is,

$$R/(I_1 \cap I_2 \cap \cdots \cap I_k) \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_k.$$

Proof. It's routine to check that φ is a homomorphism of rings and clearly $\ker \varphi = I_1 \cap I_2 \cap \cdots \cap I_k$. So we only need to show that φ is surjective.

We first show that there exists an element $a_1 \in R$ such that $\varphi(a_1) = (1, 0, \cdots, 0)$. For $j \geq 2$, since $I_1 + I_j = (1)$, we have $u_j \in I_1, v_j \in I_j$ such that $u_j + v_j = 1$. Set $a_1 = v_2 v_3 \cdots v_k$. Then $a_1 = (1 - u_2)(1 - u_3) \cdots (1 - u_k) \equiv 1 \pmod{I_1}$, and $a_1 \equiv 0 \pmod{I_j}$ for all $j \geq 2$. Hence $\varphi(a_1) = (1, 0, \cdots, 0)$ as required.

Similarly, for $2 \leq j \leq k$, we can construct $a_j \in R$ such that $\varphi(a_j) = (0, \cdots, 0, 1, 0, \cdots, 0)$, whose entries are zero except the j-th coordinate.

Now for $(x_1 + I_1, x_2 + I_2, \cdots, x_k + I_k) \in R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_k$, take $x = a_1 x_1 + a_2 x_2 + \cdots + a_k x_k$. One can check that $\varphi(x) = (x_1 + I_1, x_2 + I_2, \cdots, x_k + I_k)$. Hence φ is surjective. □

The Chinese Remainder Theorem (CRT) in commutative ring theory is a generalization of the so called *Sun Zi Theorem* (孙子定理) in elementary number theory. The earliest known statement of the Sun Zi Theorem originates in the following problem appeared in the 4th/5th-century book *Sun Zi Suan Jing* (《孙子算经》) by the Chinese mathematician Sun Zi (孙子):

> There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?
>
> (有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二. 问物几何?)

This problem is reduced to solve a system of simultaneous linear congruence equations:

$$x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}.$$

The answer is $x = 23 + 105n$, $n \geq 0$. If we restrict the solution in the range $[0, 104]$, the answer is 23.

Actually, Sun Zi Theorem asserts that if the n_i are pairwise coprime positive integers, and if $a_1, a_2, \cdots, a_k$ are integers such that $0 \leq a_i < n_i$ for every i, then there is one and only one integer

x, such that $0 \leq x < N$ and the remainder of the Euclidean division of x by n_i is a_i for every i, where $N = n_1 n_2 \cdots n_k$. For example, the above problem is essentially illustrated by the isomorphism

$$\varphi : \mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}.$$

Sun Zi Theorem may be restated as follows in term of congruences:

If n_i are pairwise coprime integers, and if $a_1, \cdots, a_k$ are arbitrary integers, then the system of congruences

$$\begin{cases} x \equiv a_1 \,(\mathrm{mod}\ n_1), \\ x \equiv a_2 \,(\mathrm{mod}\ n_2), \\ \qquad \vdots \\ x \equiv a_k \,(\mathrm{mod}\ n_k) \end{cases}$$

has a unique solution modulo N for $N = n_1 n_2 \cdots n_k$.

Actually, the solution can be described as follows:

$$x \equiv \sum_{i=1}^{k} a_i t_i N_i (\mathrm{mod}\, N),$$

where $N_i = \frac{N}{n_i}$, $t_i \equiv N_i^{-1} (\mathrm{mod}\, N)$.

In terms of the language in ring theory, the theorem is often restated as: if the n_i are pairwise coprime, the map

$$x \,\mathrm{mod}\ N \ \mapsto\ (x \,\mathrm{mod}\ n_1, x \,\mathrm{mod}\ n_2, \cdots, x \,\mathrm{mod}\ n_k)$$

defines a ring isomorphism

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

between the ring of integers modulo N and the direct product of the rings of integers modulo the n_i. This means that for doing a sequence of arithmetic operations in $\mathbb{Z}/N\mathbb{Z}$, one may do the same computation independently in each $\mathbb{Z}/n_i\mathbb{Z}$ and then get the result by applying the isomorphism (from the right to the left). This may be much faster than the direct computation if N and the number of operations are large. This is widely used, under the name multi-modular computation, for linear algebra over the integers or the rational numbers.

Exercises

1. Give a direct proof that $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.
2. There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?
3. Let n be a positive integer having at least two distinct prime divisors. Explain why the ring $\mathbb{Z}/n\mathbb{Z}$ is not a domain via the Chinese Remainder Theorem.

4. Let $R_1, R_2, \cdots, R_n$ be rings. We define the *direct sum* $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$ as for monoids and groups. More precisely, the underlying set is $R_1 \times R_2 \times \cdots \times R_n$. Addition, multiplication, 0 and 1 are defined by

$$\begin{aligned}(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) &= (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)\\ (a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) &= (a_1 b_1, a_2 b_2, \cdots, a_n b_n)\\ 0 &= (0_1, 0_2, \cdots, 0_n)\\ 1 &= (1_1, 1_2, \cdots, 1_n),\end{aligned}$$

where 0_i and 1_i are the zero and unit of R_i. Verify R is a ring. Show that the units of R are the elements $(u_1, u_2, \cdots, u_n)$, u_i a unit of R_i. Note that $U(R)$ denotes the group of units of R. Show that $U(R) = U(R_1) \otimes U(R_2) \otimes \cdots \otimes U(R_n)$, the direct product of the groups $U(R_i)$, and that $|U(R)| = \prod |U(R_i)|$.

5. Use the Chinese Remainder Theorem to show that if I_1 and I_2 are relatively prime ideals, then $R/I_1 I_2 \cong R/I_1 \oplus R/I_2$. Deduce that if m and n are relatively prime integers then

$$\mathbb{Z}/(mn) \cong \mathbb{Z}/(m) \oplus \mathbb{Z}/(n)$$

as rings.

6. Let R be a commutative ring and $I_1, I_2, \cdots, I_k$ ideals of R that are pairwise coprime. Let $I = I_1 \cap I_2 \cap \cdots \cap I_k$. Show that

$$(R/I)^\times \cong (R/I_1)^\times \otimes (R/I_2)^\times \otimes \cdots \otimes (R/I_k)^\times$$

as groups.

7. Deduce from Problem 5 that if m and n are relatively prime integers then $\varphi(mn) = \varphi(m)\varphi(n)$, where φ is the Euler φ-function. Show that if $p$is a prime then $\varphi(p^n) = p^n - p^{n-1}$. Hence prove that

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = n \prod_{p|n} (1 - \frac{1}{p}),$$

where $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ with distinct primes p_i and $e_i \geq 1$.

8. What are the last two digits of 77^{2023}?

2.2 Basic Concepts on Module

Note that the following rings involved are not necessarily commutative.

Definition 2.1 (**Left modules**). *Let R be a ring. A* **left R-module** *(or a left module over R)* (左R-模) *is an abelian group M together with a map $(a, m) \mapsto a \cdot m$ of $R \times M$ into M, called the* scalar multiplication *or the* structure map*, such that*

1. $1 \cdot m = m$;
2. $a \cdot (m + n) = a \cdot m + a \cdot n$;
3. $(a + b) \cdot m = a \cdot m + b \cdot m$;

4. $(ab) \cdot m = a \cdot (b \cdot m)$

for $m, n \in M$ *and* $a, b \in R$.

This definition is somewhat familiar to us, as we can see in the following example of vector spaces.

Remark 2.1. 1. The map $R \times M \to M$ is also called *module multiplication* or *module action*.

2. If no confusion exists, the module action $a \cdot m$ is simply denoted by am.

3. When an abelian group M becomes an R-module, we may also say M has an *R-module structure*.

Example 2.1. 1. Every abelian group is naturally a left $\mathbb{Z}$-module.

A $\mathbb{Z}$-module structure is essentially an abelian group structure.

2. Let F be a field. A vector space over F is a F-module.

3. A ring R is naturally an R-module and every left ideal is a left R-module.

Example 2.2. The abelian group

$$R^n = \underbrace{R \times R \times \cdots \times R}_{n \text{ pieces}}$$

is a left R-module if we let

$$a(a_1, a_2, \ldots, a_n) = (aa_1, aa_2, \ldots, aa_n),$$

where $a, a_1, \ldots, a_n \in R$. In particular, R is a left R-module.

Example 2.3. Let F be a number field, V be a vector space over F and $\mathbf{T}$ be a linear transformation on V. Let λ be an indeterminate. One can make V into a $F[\lambda]$-module by letting $g(\lambda)v = g(\mathbf{T})v$:

$$(a_0 + a_1\lambda + \cdots + a_m\lambda^m)v = a_0v + a_1(\mathbf{T}(v)) + \cdots + a_m(\mathbf{T}^m(v)),$$

where $a_0, a_1, \ldots, a_m \in F$. In this case, we say V becomes a $F[\lambda]$-module via T. Notice the above $F[\lambda]$-module structure of V dependents on T.

A vector space over F has an $F[\lambda]$-module structure via a linear transformation.

Example 2.4. Recall that $\mathrm{M}_n(R)$ denotes the ring of $n \times n$ matrices over R. One can see that $\mathrm{M}_n(R)$ has a natural (left) R-module structure, given by scalar multiplication:

$$r \cdot (a_{ij})_{n\times n} = (ra_{ij})_{n\times n}.$$

Example 2.5. Let R be the ring of $n \times n$ matrices over some commutative ring A. Let M be the abelian group of column n-vectors in A^n. Then M can be made into a left R-module by using the matrix multiplication as the scalar multiplication.

A^n has a natural $\mathrm{M}_n(A)$-module structure.

Remark 2.2. 1. Let M be an R-module and $\underline{\mathrm{End}(M)}$ the ring of group homomorphism on M.

For $r \in R$, it induces an endomorphism (自同態) on the additive group M:

$$\tau_r : M \to M$$
$$m \mapsto rm.$$

And we have a ring homomorphism

$$\tau : R \to \mathrm{End}(M)$$
$$r \mapsto \tau_r.$$

Conversely, a ring homomorphism from R to $\mathrm{End}(M)$ will gives an R-module structure on M: if $\varphi : R \to \mathrm{End}(M)$ is a ring homomorphism, then $r \cdot m = \varphi(r)(m)$ gives a module action.

Endowing an R-module structure on $M \iff$ giving a ring homomorphism from R to $\mathrm{End}(M)$.

2. When a ring A becomes an R-module, we say A is an R-algebra, or A is an **algebra** (代数) over R. For example, the matrix ring $\mathrm{M}_n(R)$ is an R-module, hence an R-algebra. If R is a subring of some ring A. The multiplication in A induces a natural R-scalar multiplication on A. Then A becomes an R-algebra.

Proposition 2.1. *Let M be a left R-module. Then*

1. $0_R m = 0_M$;
2. $a0_M = 0_M$;
3. $(-a)m = -(am) = a(-m)$ *and in particular* $(-1)m = -m$

for all $m \in M$ and $a \in R$.

The notion of *right R-module* is dual to that of the left R-module.

Definition 2.2 (Right modules)**.** *Let R be a ring. A* **right R-module** *(or* right module over R*)* (右R-模) *is an abelian group M together with a map $(m, r) \mapsto mr$ of $M \times R$ into M satisfying the following properties:*

1. $m1 = m$;
2. $(m + n)a = ma + na$;
3. $m(a + b) = ma + mb$;
4. $m(ab) = (ma)b$

for $m, n \in M$ and $a, b \in R$.

Every property that a left module might possess has a corresponding property regarding the right modules. Hence, every statement regarding the left modules will not be repeated for the right modules again.

Definition 2.3. *Let M be a module over R. We say that N is a* **submodule** (子模) *(over R) if N is an subgroup of M such that $rn \in N$ for all $r \in R$ and $n \in N$.*

Remark 2.3. A nonempty subset M of R is a left-submodule over R if and only if M is a left-ideal of R. Similarly, a subgroup of an abelian group is a $\mathbb{Z}$-submodule.

Proposition 2.2. *A subset N of M is an R-submodule of M if and only if the following conditions are satisfied:*

1. $N \neq \emptyset$;
2. $n + n' \in N$;
3. $rn \in N$ *for all* $r \in R$ *and* $n, n' \in N$.

$$\boxed{\emptyset \neq N \subseteq M \text{ is a submodule} \iff x + y, rx \in N \text{ for all } x, y \in N \text{ and } r \in R.}$$

Example 2.6. Let V be a vector space over a field F and W a nonempty subset of V. Then V has a F-module structure. For a linear transformation $\mathbf{T}$, according to Example 2.3, V becomes a $F[\lambda]$-module. We have

1. W is a F-submodules $\Leftrightarrow$ W is a subspace;
2. W is a $F[\lambda]$-submodule $\Leftrightarrow$ W is a $\mathbf{T}$-invariant subspace.

An R-module M always has two trivial submodules: $\{0\}$ and M. We say that M is **irreducible** (不可约模) if $M \neq \{0\}$ and its only submodules are $\{0\}$ and M. An irreducible module is also called *simple* (单模).

Proposition 2.3. *Let $\{N_i\}_{i \in I}$ be a family of submodules of the R-module M.*

1. *The intersection*
$$\bigcap_{i \in I} N_i$$
is a submodule of M.

2. *Define*
$$\sum_{i \in I} N_i = \{m_{i_1} + m_{i_2} + \cdots + m_{i_s} \mid m_{i_j} \in N_{i_j}, i_1, i_2, \ldots, i_s \in I\}.$$
It is a submodule of M, called the **sum** (和) *of $N_i, i \in I$.*

One can see that $\sum_{i \in I} N_i$ is the smallest submodule of M containing every N_i, $i \in I$. If the index set I is finite, then $\sum_{i=1}^{s} N_i$ is also written as $N_1 + N_2 + \cdots + N_s$.

Let S be a subset of an R-module M. Define

$$\langle S \rangle = \{x_1 s_1 + x_2 s_2 + \cdots x_n s_n \mid x_1, x_2, \ldots x_n \in R, s_1, s_2, \ldots, s_n \in S\}.$$

It's easy to check that $\langle S \rangle$ is a (left-)submodule of M. We call $\langle S \rangle$ the **submodule generated by** S (由S生成的子模). Clearly $\langle S \rangle$ is the smallest submodule containing S. If $M = \langle S \rangle$, we say that S is a **generating set** (生成元集) of M, or S generates the module M over R. If $S = \{m_1, m_2, \ldots, m_r\}$ is a finite set, we use $\langle m_1, m_2, \ldots, m_r \rangle$ to denote $\langle S \rangle$. An elements of $\langle m_1, m_2, \ldots, m_r \rangle$ is a linear combination of $m_1, m_2, \ldots, m_r$ over R. Hence we may write $\langle m \rangle = Rm$ and

$$\langle m_1, m_2, \ldots, m_r \rangle = Rm_1 + Rm_2 + \cdots + Rm_r.$$

If M can be generated by a finite set, we say that M is a **finitely generated** module over R (R上的有限生成模). In particular, if M can be generated by one element, i.e. $M = \langle m \rangle$ for some $m \in M$, then M is called **cyclic** (循环模). Every finitely generated R-module is a sum of cyclic module: $\langle m_1, m_2, \ldots, m_r \rangle = \langle m_1 \rangle + \langle m_2 \rangle + \cdots + \langle m_r \rangle$.

Example 2.7. For any ring R (with identity), it is a cyclic R-module, since $R = R1 = \langle 1 \rangle$. If I be an ideal of R, then the quotient ring $R/I = R\overline{1}$ is also a cyclic module.

Finitely generated $\mathbb{Z}$-module = Finitely generated abelian group

A submodule N of an R-module M is a normal (additive) subgroup of M. It corresponds to an abelian quotient group M/N. The R-module structure on M naturally induces an R-module structure on $M/N = \{\overline{m} \mid m \in M\}$:

$$r \cdot \overline{m} = \overline{rm}.$$

One can check that this action is well-defined and then becomes a R-module action. The R-module M/N is called the **quotient module** (商模) of M modulo N. We may also write

$$M/N = \{x + N \mid x \in M\}.$$

The following result is analogue to the same statements in the quotient group G/H and quotient ring R/I.

Theorem 2.1. *Every submodule of the quotient module M/N must be of the form H/N, where H is a submodule of M containing N. In particular, there is an inclusion-preserving one-to-one correspondence between the submodules of M containing N and submodules of M/N.*

Exercises

1. Let V be an n-dimensional vector space over $\mathbb{C}$ and $\mathbf{T}$ a linear transformation. Then V becomes a $\mathbb{C}[\lambda]$-module via $\mathbf{T}$. If a Jordan block

$$T = \begin{pmatrix} 2 & 0 & \cdots & 0 & 0 \\ 1 & 2 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 2 \end{pmatrix}$$

   is a representing matrix of $\mathbf{T}$ with respect to some basis, determinant all $\mathbb{C}[\lambda]$-submodules of V.

2. Determine all $\mathbb{R}[x]$-submodules of the quotient module $\mathbb{R}[x]/(x^3 + x - 2)$.

Homework Exercise 32 on page 133. Exercise 33 on page 161. Exercise 1, 5, 10, 11 on page 177-178.