Lecture Notes On Abstract Algebra (Week 7)

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

Contents

1 Lecture 12 (Oct 17, 2023): Homomorphism of Modules, Direct Sum

1.1 Homomorphism of Modules

Definition 1.1. *Let M and N be R-modules. A map $f : M \to N$ is called a* **homomorphism** *of R-modules* (R-模同态) *if*

1. $f(m + m') = f(m) + f(m')$,
2. $f(rm) = rf(m)$

for all $r \in R$ and $m, m' \in M$.

An R-module homomorphism is also called an *R-homomorphism*, or *R-linear map*.

Example 1.1. 1. For an R-module M and any $m \in M$, the map

$$\begin{aligned} \tau_m : R &\to M \\ r &\mapsto rm \end{aligned}$$

is an R module homomorphism.

2. Let M be an R-module and N be a submodule of M. There is a canonical homomorphism from M onto M/N, sending $m \in M$ to $\overline{m} = m + N$.

Remark 1.1. Let $f : M \to N$ be a homomorphism of R-modules. Then $f(0)) = 0$ and $f(-m) = -f(m)$ for all $m \in M$.

An injective homomorphism of R-modules is called a *monomorphism* (单同态). A surjective homomorphism of R-modules is called an *epimorphism* (满同态). A bijective homomorphism of R-modules is called an *isomorphism* (同构). Two R-modules M and N are called isomorphic, denoted by $M \cong N$, if there is an isomorphism from M to N. One can easily prove that the relation "isomorphic" is an equivalence relation between R-modules.

We use $\underline{\mathrm{Hom}_R(M,N)}$ or simply $\mathrm{Hom}(M,N)$ to denote the set of all R-homomorphisms from M to N. One can see that $\mathrm{Hom}(M,N)$ becomes an abelian group in an obvious way. *If R is commutative, the additive group* $\mathrm{Hom}(M,N)$ *endowed with an R-module structure* given by

$$(rf)(m) = f(rm), \forall m \in M.$$

If R is not commutative, we note in general "rf" is additive but not necessarily R-linear.

A homomorphism from M to M is also called an **endomorphism** (自同态) on M. And $\mathrm{Hom}_R(M,M)$ is also denoted by $\mathrm{End}_R(M)$.

One can check that $\mathrm{End}_R(R) \cong R$ and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/(m,n)\mathbb{Z}$.

The module $\mathrm{Hom}_R(M,R)$ is called the **dual module** (对偶模) of M, denoted by M^*. For a vector space V over a field F, $V^* = \mathrm{Hom}_F(V,F)$ is just the *dual space* of V.

The **image** (像) of a R-module homomorphism $f : M \to N$ is defined by

$$\mathrm{im}\, f = f(M) = \{f(m) \mid m \in M\}.$$

The **kernel** (核) of f is

$$\ker f = \{m \in M \mid f(m) = 0\}.$$

Proposition 1.1. *Let $f : M \to N$ be a homomorphism of R-modules. Then* $\ker f$ *is a submodule of M and* $\mathrm{im}\, f$ *is a submodule of N.*

Just as the cases for groups and rings, we have the same theorems of homomorphisms for modules. We list them below for references. Their proofs are similar to that of the homomorphism theorem on rings.

Theorem 1.1 (Fundamental Theorem of Homomorphisms of Modules). *Let $f : M_1 \to M_2$ be a homomorphism of R-modules. Then f induces a natural isomorphism:*

$$\overline{f} : M_1/\ker f \to \mathrm{im} f = f(M_1)$$
$$a + \ker f \mapsto f(a).$$

In particular, if f is an epimorphism, then $M_1/\ker f \cong M_2$.

Example 1.2. Let F be a field and $V = F^n$ the vector space of column vectors. Let

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & & \vdots & \vdots \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

be an $n \times n$ matrix. For $\alpha \in F^n$, define

$$\mathbf{T}(\alpha) = A\alpha.$$

If $\alpha = (a_1, a_2, \ldots, a_n)^T$, then $\mathbf{T}(\alpha) = (0, a_1, a_2, \ldots, a_{n-1})$, which is a kind of shift of the coordinates. Consequently $\mathbf{T}$ is a linear transformation and F^n becomes an $F[\lambda]$-module via $\mathbf{T}$. The $F[\lambda]$-module structure on F^n is defined as follows: for $f(\lambda) \in F[\lambda]$ and $\alpha \in F^n$,

$$f(\lambda)\alpha = f(\lambda) \circ \alpha = f(\mathbf{T})(\alpha) = f(A)\alpha,$$

where the last operation is the multiplication of matrices.

Take $e = (1, 0, 0, \ldots, 0)^T$. Then $\mathbf{T}^i(e)$ is the unit vector whose i-th coordinate is 1 and other coordinates are 0. Hence the vectors $e, \mathbf{T}(e), \mathbf{T}^2(e), \ldots, \mathbf{T}^{n-1}(e)$ are linearly independent over F, equivalently, $e, \lambda e, \lambda^2 e, \cdots, \lambda^{n-1}e$ are linearly independent over F. Since $\dim_F F^n = n$ and $\mathbf{T}^n(e) = \lambda^n e = 0$, we have

$$\begin{aligned} F^n &= \{a_0 e + a_1 \mathbf{T}(e) + a_2 \mathbf{T}^2(e) + \cdots + a_{n-1}\mathbf{T}^{n-1}(e) \mid a_0, a_1, \ldots, a_{n-1} \in F\} \\ &= Fe + F\mathbf{T}(e) + F\mathbf{T}^2(e) + \cdots + F\mathbf{T}^{n-1}(e) \\ &= F[\lambda]e. \end{aligned}$$

Hence F^n is a cyclic $F[\lambda]$-module (F^n is a cyclic space with respect to $\mathbf{T}$).

Consider the map

$$\begin{aligned} \tau : F[\lambda] &\to F^n \\ f(\lambda) &\mapsto f(\lambda)e = f(A)e. \end{aligned}$$

One can see that

(i) τ is an epimorphism of $F[\lambda]$-modules;

(ii) $\ker \tau = (\lambda^n)$.

By the Fundamental Theorem of Homomorphisms of Modules, we have

$$F^n \cong F[\lambda]/(\lambda^n).$$

Clearly

$$F[\lambda]/(\lambda^n) = \{a_0 + a_1\overline{\lambda} + \cdots + a_{n-1}\overline{\lambda}^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\}.$$

Here $\overline{\lambda} = \lambda \bmod (\lambda^n)$ denotes the image of $\lambda \in F[\lambda]$ in the quotient ring $F[\lambda]/(\lambda^n)$. The $F[\lambda]$-module action on $F[\lambda]/(\lambda^n)$ is essentially the multiplication in $F[\lambda]$ modulo (λ^n):

$$f(\lambda) \circ \overline{g(\lambda)} = \overline{f(\lambda)g(\lambda)}.$$

The isomorphism from $F[\lambda]/(\lambda^n)$ to F^n which is induced by τ is given by

$$\begin{aligned} \overline{\tau} : F[\lambda]/(\lambda^n) &\to F^n \\ \overline{f(\lambda)} &\mapsto f(\lambda)e. \end{aligned}$$

In particular, $\overline{1} \mapsto e$.

If we identify F^n with $F[\lambda]/(\lambda^n)$, the module action on F^n which is defined via $\mathbf{T}$ can be described by the ordinary multiplication of polynomials. In other words, the multiplication of matrices can be interpreted as the multiplication of polynomials.

1.2 Isomorphism Theorems for Modules

Theorem 1.2 (**First Isomorphism Theorem for Modules**). *Let $f : M_1 \to M_2$ be an epimorphism of R-modules (denoted by $M_1 \twoheadrightarrow R_2$) and let N be a submodule of M_1 containing* $\ker f$. *Then $f(N)$ is a submodule of M_2 and*

$$\begin{aligned} \eta : M_1/N &\to M_2/f(N) \\ a+N &\mapsto f(a)+f(N). \end{aligned}$$

is an isomorphism from M_1/N to $M_2/f(N)$.

Corollary 1.1. *Let N, H be two submodules of M, and $N \subseteq H$, then*

$$M/H \cong M/N \Big/ H/N.$$

Theorem 1.3 (**Second Isomorphism Theorem for Modules**). *Let N, H be submodules of R-module M. Then*

$$\begin{aligned} (N+H)/N &\to H/(N \cap H) \\ a+N &\mapsto a+N\cap H, \quad a \in H \end{aligned}$$

is an isomorphism of R-modules. That is, $(N+H)/N \cong H/(N \cap H)$.

Example 1.3. Take $\mathbb{Z}$-module $M = \mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$. Then

$$H = \mathbb{Z} \text{ and } N = (2+3i)\mathbb{Z}[i]$$

are submodules of M. One can see that

(1) $H = \langle 1 \rangle$ is cyclic as a $\mathbb{Z}$-module; and

(2) $N = (2+3i) \neq \langle 2+3i \rangle = (2+3i)\mathbb{Z}$ and N is not cyclic as a $\mathbb{Z}$-module, even if N is cyclic as a $\mathbb{Z}[i]$-module.

We have

$$H + N = \{a + (2+3i)b(i) \mid a \in \mathbb{Z}, b(i) \in \mathbb{Z}[i]\} = \mathbb{Z}[i] = \langle 1, i \rangle,$$

since $i = -5 + (2+3i)(1-i) \in H+N$.

Notice $13 = (2+3i)(2-3i)$. If $(2+3i)(a+bi) = n \in \mathbb{Z}$ with $a, b \in \mathbb{Z}$, then $n = (2a-3b)+(3a+2b)i$ and hence $2b = -3a$. This implies that $a = 2m, b = -3m$ for some $m \in \mathbb{Z}$. Consequently $n = 13m$. We have

$$H \cap N = \langle 1 \rangle \cap (2+3i) = \langle 13 \rangle = 13\mathbb{Z}.$$

By the Second Isomorphism Theorem for modules,

$$\mathbb{Z}[i]/(2+3i) \cong \mathbb{Z}/13\mathbb{Z}.$$

This means that the quotient module $\mathbb{Z}[i]/(2+3i)$ is finite with 13 elements.

The above homomorphism theorems can be also formulated in the following form.

1. (*The First Isomorphism Theorem*) Let $f : M \to N$ be an epimorphism of R-modules.Then

$$M/\ker f \cong N.$$

2. (*The Second Isomorphism Theorem*) Let $M_1 \subseteq M_2$ be submodules of the R-module M. Then M_2/M_1 is also a submodule of M/M_1 and

$$(M/M_1) \,/\, (M_2/M_1) \cong M/M_2.$$

3. (*The Third Isomorphism Theorem*) Let M_1 and M_2 be submodules of the R-module M. Then

$$(M_1 + M_2)/M_1 \cong M_2/M_1 \cap M_2.$$

Exercises

1. Is a submodule of a cyclic module over a ring still cyclic?
2. Show that any irreducible module is cyclic and any nonzero element is a generator.
3. Let $\mathfrak{a}$ be an ideal of a ring R and M an R-module. Define

$$\mathfrak{a}M = \left\{ \sum_{i=1}^{n} a_i m_i \mid a_i \in \mathfrak{a}, m_i \in M, i = 1, 2, \ldots, n \right\}.$$

   (1) Show that $\mathfrak{a}M$ is a submodule of M.

   (2) Suppose $\mathfrak{a}M = 0$. Show that M becomes an $R/\mathfrak{a}$ via the following well-defined scalar multiplication:

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

   where $\overline{r} \in R/\mathfrak{a}$ and $m \in M$.

   (3) Show that $M/\mathfrak{a}M$ can be naturally regarded as an $R/\mathfrak{a}$-module.

4. An endomorphism of an irreducible module must be an isomorphism or zero map.
5. Let M be an irreducible module. Then $\mathrm{Emd}(M)$ is a division ring. (*Schur's Lemma*)
6. Let M be an R-module and $m \in M$. Define $\mathrm{ann}(m) = \{x \in R \mid xm = 0\}$.

   (a) Show that $\mathrm{ann}(m)$ is a left-ideal of R. It is called the annihilator (or order) of m.

   (b) If $M = Rm$ is irreducible, then $\mathrm{ann}(m)$ is a maximal left ideal of R.

   (c) Show that the cyclic module $Rm \cong R/\mathrm{ann}(m)$ as R-modules. This shows that basically the only cyclic modules are of the form R/I.

7. Let M be an R-module and $m \in M$. Show that $\mathrm{End}_R(R) \cong R$ and $\mathrm{Hom}_R(R, M) \cong M$.
8. Let M be a finitely generated R-module and N a submodule. Then M/N is also a finitely generated R-module.
9. Let f be a homomorphism of R-module M into some other R-module and N a submodule of M. Then

$$\#\,(M/N) = \#\,(f(M)/f(N))\,\#\,(\ker f/(N \cap \ker f))$$

   in the sense that if two of the quotients are finite, so is the third and the equality holds.

10. Let $T(x, y, z) = (y, z, -x)$ be the linear transformation via which $\mathbb{R}^3$ becomes a $\mathbb{R}[\lambda]$-module. Determine all submodules of $\mathbb{R}^3$.

1.3 Direct Sum of Modules

Let $M_1, M_2, \ldots, M_n$ be R-modules. The direct sum of the abelian groups $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ has a natural R-module structure:

$$r(a_1, a_2, \ldots, a_n) = (ra_1, ra_2, \ldots, ra_n),$$

where $r \in R$, $a_i \in M_i$, $1 \leq i \leq n$. This module is called the **direct sum** of the R-module $M_1, M_2, \ldots, M_n$, still denoted by $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ or $\oplus_{i=1}^n M_i$.

If we take

$$M_i' = \{(0, 0, \ldots, 0, a_i, 0, \ldots, 0) \mid a_i \in M_i\},$$

one can see that M_i' is a submodule of $\oplus_{i=1}^n M_i$ and M_i is isomorphic to M_i' as R-module.

Example 1.4. The direct sum $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ is a finite $\mathbb{Z}$-module with 6 elements. Actually, we have a $\mathbb{Z}$-module isomorphism:

$$\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$
$$a \bmod 6 \mapsto (a \bmod 2, a \bmod 3).$$

Example 1.5. The abelian group

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

has a natural R-module structure. Actually, R^n is a direct sum of n copies of R: $R^n = R \oplus R \oplus \cdots \oplus R$.

Theorem 1.4. *Let $M_1, M_2, \ldots, M_n$ be submodules of an R-module M. If*

1. $M = \sum_{i=1}^n M_i$; *and*
2. $M_i \cap \left(\sum_{j \neq i} M_j \right) = \{0\}$ *for $i = 1, 2, \ldots, n$,*

then there is an isomorphism of R-modules

$$\bigoplus_{i=1}^n M_i \to M$$
$$(a_1, a_2, \ldots, a_n) \mapsto a_1 + a_2 + \cdots + a_n.$$

In this case, we say the sum $M = \sum_{i=1}^n M_i$ is a direct sum and write $M = \bigoplus_{i=1}^n M_i$. Furthermore, each submodule M_i is called a **direct summand** (直和项) *of M.*

Corollary 1.2. *Let $M_1, M_2, \ldots, M_n$ be submodules of an R-module M such that $M = M_1 + M_2 + \cdots + M_n$. TFAE*

1. $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$.
2. *Every element $m \in M$ can be written in a unique manner as $m = m_1 + m_2 + \cdots + m_n$, where $m_i \in M_i, i = 1, 2, \ldots, n$.*
3. *If $m_1 + m_2 + \cdots + m_n = 0$ with $m_i \in M_i, i = 1, 2, \ldots, n$, then $m_i = 0$ for all i.*

4. For $1 \le i \le n$, $M_i \cap \left(\sum_{j \neq i} M_j \right) = \{0\}$.

Remark 1.2. All concepts and statements on direct sum of modules are almost the same as those of vector spaces.

Clearly, $\{0\}$ and M are submodule of M. They are called *trivial modules*. If M can be written as a direct sum of two nontrivial submodules, then M is called *decomposable* (可分解的). Otherwise, M is called **indecomposable** (不可分解模).

Example 1.6.
1. Assume the ring R has an impotent $e \neq 0, 1$ (i.e. $e^2 = e$). As an R-module, R is decomposable: $R = Re \oplus R(1-e)$.
2. As a $\mathbb{Z}$-module, $\mathbb{Z}/6\mathbb{Z}$ is decomposable: $\mathbb{Z}/6\mathbb{Z} = 2\mathbb{Z}/6\mathbb{Z} \oplus 3\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. But $\mathbb{Z}/4\mathbb{Z}$ is indecomposable.
3. Let π be an irreducible element in R. Then $R/(\pi^n)$ is an indecomposable R-module for every positive integer n.

Exercise Let $M_1, M_2, \ldots, M_n$ be submodules of M. Denote the identity map on S by 1_S. For $1 \le i \le n$, the natural embedding $M_i \to M$ is denoted by ι_i and there exist module homomorphism $p_i : M \to M$ such that

(1) $\mathrm{im}(p_i) = M_i$;

(2) $p_1 + p_2 + \cdots + p_n = 1_M$ and

(3) $p_i \circ \iota_i = 1_{M_i}$.

Show that $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

2 Lecture 13 (Oct 19, 2023): Free Modules

2.1 Torsion Elements

Definition 2.1. *Let M be an R-module and let $\alpha \in M$. We define the* **annihilator** (零化子) *of α in R as*

$$\mathrm{ann}(\alpha) = \{r \in R \mid r\alpha = 0\}.$$

One can easily see that ann(α) is a left ideal of R. In the case of $\mathbb{Z}$-modules (abelian groups), ann(α) is generated by the order of α. Hence, sometimes ann(α) is also called the *order ideal* of α.

Example 2.1. Let M be a $\mathbb{Z}$-module and $\alpha \in M$. Then $\mathrm{ann}(\alpha) = (d)$ for some nonnegative integer. If $d = 0$, then x is an element of infinite order as an element in the abelian group M. If $d > 0$, then x is an element of order d.

Example 2.2. Let V be a vector space of dimension n over a field F and $\mathbb{T}$ a linear transformation on V. Then V becomes an $F[\lambda]$-module via $\mathbb{T}$. Let $\varphi(\lambda)$ be the characteristic polynomial of $\mathbb{T}$. By Hamilton-Cayley Theorem, $\varphi(\mathbb{T}) = 0$. It follows that $\varphi(\lambda)\alpha = 0$ holds for all $\alpha \in V$ and hence $\mathrm{ann}(\alpha) \neq 0$. Thus $\mathrm{ann}(\alpha) = (m_\alpha(\lambda)) \neq 0$ for some monic polynomial $m_\alpha(\lambda)$, where $m_\alpha(\lambda) \mid \varphi(\lambda)$.

Proposition 2.1. *Let M be an R-module and $\alpha \in M$. There is an R-module isomorphism:*

$$R\alpha = \langle \alpha \rangle \cong R/\mathrm{ann}(\alpha).$$

If $\mathrm{ann}(\alpha) \neq \{0\}$, α is called a **torsion element** (扭元) of M. A torsion element in M is an element that can be annihilated by a nonzero element in R. If α is not a torsion element, then $R\alpha \cong R$.

The torsion part of M is defined by

$$\begin{aligned}\mathrm{Tor}(M) &= \text{the set of all torsion elements in } M \\ &= \{\alpha \in M \mid r\alpha = 0 \text{ for some } r \in R^*\} \\ &= \{\alpha \in M \mid \mathrm{ann}(\alpha) \neq 0\}.\end{aligned}$$

If $\mathrm{Tor}(M) = M$, then M is called a **torsion module** (扭模) over R. If $\mathrm{Tor}(M) = 0$, then M is called **torsion-free** (无扭的).

M is a torsion module if and only if all elements of M are torsion.

Example 2.3. Every finite abelian group is a torsion $\mathbb{Z}$-module.

In general, $\mathrm{Tor}(M)$ is not a submodule of M. For example, the additive group $\mathbb{Z}/6\mathbb{Z}$ is a module over the ring $\mathbb{Z}/6\mathbb{Z}$. Since

$$\begin{aligned}&\mathrm{ann}(\overline{0}) = (\overline{1}),\\ &\mathrm{ann}(\overline{2}) = \mathrm{ann}(\overline{4}) = (\overline{3}),\\ &\mathrm{ann}(\overline{3}) = (\overline{2}),\\ &\mathrm{ann}(\overline{1}) = \mathrm{ann}(\overline{5}) = (\overline{0}),\end{aligned}$$

we have $\mathrm{Tor}(\mathbb{Z}/6\mathbb{Z}) = \{\overline{0}, \overline{2}, \overline{3}, \overline{4}\}$, which is not a submodule of $\mathbb{Z}/6\mathbb{Z}$.

Proposition 2.2. *Let M be a module over an integral domain. Then $\mathrm{Tor}(M)$ is a submodule and $M/\mathrm{Tor}(M)$ is torsion-free.*

The proof is clear.

Problem Let V be a vector space of dimension n over a field F. A linear transformation $\mathbb{T}$ on V gives an $F[\lambda]$-module structure on V as follows:

$$g(\lambda)\alpha = g(\mathbb{T})(\alpha),$$

where $g(\lambda) \in F[\lambda]$, $\alpha \in V$.

1. Show that $\mathrm{ann}(\alpha) = (f_\alpha(\lambda))$, where $f_\alpha(\lambda)$ is the monic polynomial with smallest degree such that $g(\mathbb{T})(\alpha) = 0$. Deduce that $f_\alpha(\lambda)$ is a divisor of the characteristic polynomial of $\mathbb{T}$.
2. Show that the cyclic $F[\lambda]$-module $F[\lambda]\alpha$ is an F-module generated by $\{\mathbb{T}^k\alpha \mid k \geq 0\}$.
3. Show that $\mathbb{T}\,|_{F[\lambda]\alpha}$, the restriction of $\mathbb{T}$ on the subspace $F[\lambda]\alpha$, induces a linear transformation. Deduce that $\dim_F F[\lambda]\alpha = \deg f_\alpha(\lambda)$, where $f_\alpha(\lambda)$ is the polynomial described above. More precisely, $f_\alpha(\lambda)$ is the characteristic polynomial of the linear transformation $\mathbb{T}\,|_{F[\lambda]\alpha}$.
4. Show that V is a torsion $F[\lambda]$-module.

5. Define the annihilator of V by

$$\mathrm{ann}(V) = \{f(\lambda) \in F[\lambda] \mid f(\lambda)\alpha = 0 \text{ for all } \alpha \in V\}.$$

Show that $\mathrm{ann}(V) = (m(\lambda))$, where $m(\lambda)$ is the minimal polynomial of $\mathbb{T}$.

2.2 Free Modules

Definition 2.2. *Let M be an R-module.*

1. *A collection of elements $x_1, x_2, \ldots, x_n$ in M is said to be* **linearly independent** (线性无关) *if $\sum_{i=1}^n a_i x_i = 0$ for some $a_1, a_2, \ldots, a_n \in R$ implies that $a_i = 0$ for all i.*

2. *If M can be generated by a linearly independent generating set, then M is called a* **free R-module** (自由模) *and the elements in a linearly independent generating set form a base or a* **basis** (基) *of M over R.*

Remark 2.1. A infinite collection of elements is called linearly independent if any sub-collection of finite elements is linearly independent.

Remark 2.2. A module over a field is free.

$$\boxed{x_1, x_2, \ldots, x_n \text{ are linearly independent} \Longrightarrow \sum_{i=1}^n Rx_i = \bigoplus_{i=1}^n Rx_i.}$$

The zero module is conventional considered as a free module. We can also define a free module with an infinity generating set.

Example 2.4. Let V be an n-dimensional vector space over a number field F. Then V is a free F-module and a basis of V as F-vector space is naturally a basis as F-module.

Example 2.5. For a ring R, as a module over itself, it admits a basis, consisting of the identity 1. More generally, let

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in R^n = R \oplus R \oplus \cdots \oplus R, \ i = 1, 2, \ldots, n.$$

They form a basis of R^n. Hence R^n is a free module.

Example 2.6.

1. The additive group $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ can be seen as a $\mathbb{Z}$-module or a $\mathbb{Z}_2$-module. Neither $\overline{0}$ nor $\overline{1}$ in $\mathbb{Z}_2$ can be part of a basis over $\mathbb{Z}$. However, $\{\overline{1}\}$ form a basis for $\mathbb{Z}_2$ over $\mathbb{Z}_2$. Hence $\mathbb{Z}_2$ is a free $\mathbb{Z}_2$-module.

2. As a $\mathbb{Z}$-module, $\mathbb{Q}$ is not free, since any two rational number are $\mathbb{Z}$-linearly dependent. But $\mathbb{Q}$ is a free $\mathbb{Q}$-module: $\mathbb{Q} = \langle 1 \rangle = \mathbb{Q}1$.

Remark 2.3.

1. Every element appears in a basis of a free R-module must be torsion-free.

2. If R has no zero divisors, then every free module over R is torsion-free.

   But the converse is not true. For example, the addition group $\mathbb{Q}$ is a torsion-free $\mathbb{Z}$-module. But $\mathbb{Q}$ is not free, since every pair of elements in $\mathbb{Q}$ are linearly dependent.

3. Unlike vector spaces, not all modules posses bases. To see this, note that the annihilator of an element in a basis must be 0.

4. Let R be a ring and I an ideal of R. Then R/I is a R-module, also an R/I-module. As an R/I-module, R/I is free; as an R-module, R/I is not free, except $I = \{0\}$.

Corollary 2.1. *If M is a free R-module with a basis $x_1, x_2, \ldots, x_n$, then*

$$M = Rx_1 \oplus Rx_2 \oplus \cdots \oplus Rx_n.$$

Consequently $M \cong R^n$.

Theorem 2.1. *Let M be a free module over a commutative ring R with a basis $x_1, x_2, \ldots, x_n$, and $\mathfrak{a}$ an ideal of R. Consider*

$$\mathfrak{a}M = \mathfrak{a}x_1 + \mathfrak{a}x_2 + \cdots + \mathfrak{a}x_n = \left\{ a_1x_1 + \cdots + a_nx_n \,\middle|\, a_i \in \mathfrak{a}, i = 1, 2, \ldots, n \right\}.$$

(1) Then $\mathfrak{a}M$ is a submodule of M and each $\mathfrak{a}x_i$ is a submodule of Rx_i.

(2) We have a natural R-module isomorphism

$$M/\mathfrak{a}M \cong \bigoplus_{i=1}^{n} Rx_i/\mathfrak{a}x_i,$$

which is induced by the epimorphism

$$\begin{aligned} M = Rx_1 \oplus \cdots \oplus Rx_n &\to Rx_1/\mathfrak{a}x_1 \oplus \cdots \oplus Rx_n/\mathfrak{a}x_n \\ a_1x_1 + \cdots + a_nx_n &\mapsto (a_1x_1 \bmod \mathfrak{a}x_1, \ldots, a_nx_n \bmod \mathfrak{a}x_n). \end{aligned}$$

(3) The quotient group $M/\mathfrak{a}M$ can be regarded as an $R/\mathfrak{a}$-module and the above isomorphism is an isomorphism as $R/\mathfrak{a}$-module. In particular, $M/\mathfrak{a}M$ is a free $R/\mathfrak{a}$-module with a basis $\overline{x}_1, \ldots, \overline{x}_n$, where $\overline{x}_i = x_i + \mathfrak{a}M$.

In virtue of Theorem 2.1, we can prove the following result by taking $\mathfrak{a}$ to be a maximal ideal and reducing to the case of vector spaces.

Corollary 2.2. *If R is commutative, then $R^m \cong R^n$ if and only if $m = n$.*

Proof. Let $\mathfrak{a}$ be a maximal ideal of R and let $\phi : R^m \to R^n$ be an isomorphism. The First Isomorphism Theorem shows ϕ induces an isomorphism

$$R^m/\mathfrak{a}R^m \cong R^n/\mathfrak{a}R^n.$$

But Theorem 2.1 implies that

$$R^m/\mathfrak{a}R^m \cong \bigoplus_{i=1}^{m} Re_i/\mathfrak{a}e_i \cong F^m,$$

where $F = R/\mathfrak{a}$ is a field. Similarly $R^n/\mathfrak{a}R^n \cong F^n$. Hence $F^m \cong F^n$, yielding $m = n$. □

Corollary 2.2 shows, if M is a free module with finitely many elements in a basis over a commutative ring, then any two bases of M have the same cardinality, which is called the **rank** (秩) of M.

Remark 2.4. 1. If M is a module over a field F with finitely many generators. Then M is a free F-module with a finite basis and any two bases have the same cardinality, say n. In this case, n is just the dimension of M as an k-vector space. In other words, the rank of M is just the dimension of M as an F-vector space.

2. If M is a free module over a noncommutative ring R with bases B and B', then does $\#(B) = \#(B')$?

   In general the answer is NO. If interested, please refer to the following significant work on this question:

   - P. M. Cohn, Some remarks on the invariant basis property, *Topology* 5 (1966), 215-228.

Exercises

1. Is a submodule of a torsion module over a ring still torsion?
2. Is a submodule of a finitely generated module over a ring still finitely generated?
3. Is a submodule of a free module over a ring still free?
4. Is a submodule of a torsion-free module over a ring still torsion-free?
5. How about the quotient ring case of the above problems?
6. Let M_1 and M_2 are submodules of an R-module M such that $M = M_1 \oplus M_2$. Show that $M/M_1 \cong M_2$ and $M/M_2 \cong M_1$ as R-modules.
7. Let M, N be R-modules and let $f : M \to N$, $g : N \to M$ be R-homomorphisms such that $f \circ g = \mathrm{id}_N$. Show that $M = \ker(f) \oplus \mathrm{im}(g)$.
8. Let N be a submodule of some left R-module M and $\mathfrak{a}$ a left ideal of M. Define
$$\mathfrak{a}N = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_i \in \mathfrak{a}, x_i \in N, i = 1, 2, \ldots, n \right\}.$$
   Show that $\mathfrak{a}N$ is a submodule of M.
9. Let M be a free R-module with a basis $x_1, x_2, \ldots, x_n$ and $\mathfrak{a}$ an ideal of M.
   (a) Show that $Rx_i/\mathfrak{a}x_i \cong R/\mathfrak{a}$ as R-module and $Rx_i/\mathfrak{a}x_i$ is a free $A/\mathfrak{a}$-module, $i = 1, 2, \ldots, n$.
   (b) Show that $M/\mathfrak{a}M \cong \bigoplus_{i=1}^{n} Rx_i/\mathfrak{a}x_i$ as R-module.
   (c) If R is commutative, then every basis of M has n elements. We call n the *rank* of M.
10. Let M be a nonzero R-module. Show that M is finitely generated if and only if M is isomorphic to a quotient of R^n for some $n > 0$.
11. Let N be a direct summand of a finitely generated module M. Show that N is finitely generated.
12. Let M be a finitely generated R-module and $\phi : M \to R^n$ an epimorphism. Show that $\ker \phi$ is finitely generated.
13. Show that two free modules whose generating sets have the same cardinality are isomorphic.
14. Let k be a field and $m(\lambda)$ be a polynomial of degree n in $k[\lambda]$. Set $M = k[\lambda]/(m(\lambda))$. Show that
   (a) M is a cyclic torsion $k[\lambda]$-module; and
   (b) M is a free k-module of rank n.
15. Let V be a vector space of dimension n over k and $\mathbb{T}$ a linear transformation on V. Then V becomes a $k[\lambda]$-module via $\mathbb{T}$. Let $f(\lambda)$ be the characteristic polynomial of $\mathbb{T}$ and let $M = k[\lambda]/(f(\lambda))$.

(a) Show that V is a cyclic $k[\lambda]$-module if and only if the minimal polynomial of $\mathbb{T}$ is $f(\lambda)$.

(b) Show that V and M are isomorphic as k-module.

(c) Explain that V and M are not necessarily isomorphic as $k[\lambda]$-module. And when?

16. Let R be a PID and M a module over R.

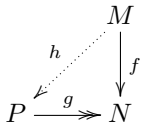
(a) Let $x \in M, a \in R$ and $\mathrm{ann}(x) = (d)$. Show that $\mathrm{ann}(ax) = \left(\frac{d}{(a,d)}\right)$. In particular, if $(a, d) = 1$, then $\mathrm{ann}(ax) = \mathrm{ann}(x)$.

(b) Let $M = \langle x \rangle$ be a cyclic module and $\mathrm{ann}(x) = (d)$ with $d = d_1 d_2, (d_1, d_2) = 1$. Show that there exist $y, z \in M$ such that $\mathrm{ann}(y) = (d_1)$, $\mathrm{ann}(z) = (d_2)$ and $M = \langle y \rangle \oplus \langle z \rangle$.

(c) Let $M = \langle y, z \rangle$, where $y, z \in M$ and $\mathrm{ann}(y) = (d_1), \mathrm{ann}(z) = (d_2)$. Show that $M = \langle x \rangle$ for some $x \in M$ such that $\mathrm{ann}(x) = (d_1 d_2)$.

(d) Let $M = \langle y \rangle \oplus \langle z \rangle$ and $\mathrm{ann}(y) = (d_1)$, $\mathrm{ann}(z) = (d_2)$. Show that $\mathrm{ann}(y + z) = (d)$, where d is a least common multiple of d_1, d_2. Is it true that $M = \langle y + z \rangle$?

17. A left module M over a ring R is called *projective* (投射模), if for every R-homomorphism $f : M \to N$ and every R-epimorphism $g : P \twoheadrightarrow N$, there exists an R-homomorphism $h : M \to P$ such that $f = g \circ h$. That is, there exists an homomorphism h which makes the following diagram commute.



In other words, M is a projective module, if given an epimorphism $g : P \to N$, every homomorphism $f : M \to N$ can be factored through g as $f = g \circ h$ for some h.

(a) Every free module is projective.

(b) If $e = e^2$ is an idempotent in the ring R, then Re is a projective left module over R.

(c) Every module over a field (or division ring) is projective.

(d) A module M is projective, if whenever M is a quotient of a module P, there exists a module N such that the direct sum $M \oplus N \cong P$.

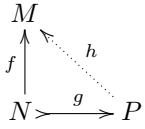
(e) A module is projective if and only if it is a direct summand of a free module.

18. An R-module M is projective if and only if there exists a set $\{a_i \in M \mid i \in I\}$ and a set $\{f_i \in \mathrm{Hom}(M, R) \mid i \in I\}$ such that for every $x \in M$, $f_i(x)$ is only nonzero for finitely many i, and $x = \sum f_i(x) a_i$.

19. (a) Show that $\mathbb{Z}$ is a module over the ring $\mathbb{Z} \oplus \mathbb{Z}$ with respect to the scalar multiplication defined by $(a \oplus b) \cdot x = ax$.

(b) Show that $\mathbb{Z}$ is projective but not free as a module over $\mathbb{Z} \oplus \mathbb{Z}$ defined above.

20. An R-module M is called *injective* (内射模), if for every R-homomorphism $f : N \to M$ and every R-monomorphism $g : N \rightarrowtail P$, there exists an R-homomorphism $h : P \to M$ such that $f = h \circ g$. That is, the following diagram is commutative.



(a) The rationals $\mathbb{Q}$ and the quotient module $\mathbb{Q}/\mathbb{Z}$ are injective $\mathbb{Z}$-modules.

(b) The factor group $\mathbb{Z}/n\mathbb{Z}$ for $n > 1$ is injective as a $\mathbb{Z}/n\mathbb{Z}$-module, but not injective as a $\mathbb{Z}$-module.

(c) Every vector space over a field is an injective module.

(d) A left module M is injective, if whenever M is a submodule of some left R-module P, there exists another submodule N of P such that $P = M \oplus N$.

Homework Exercise 7, 12, 19, 20, 22, 23, 24 on page 177-179.