Lecture Notes On Abstract Algebra (Week 8)

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

Contents

1 Lecture 14 (Oct 24, 2023): Finitely Generated Modules over a PID

In the following lectures on module theory, all rings are always assumed to be PID, unless otherwise specified. And we are interested in the structure of finitely generated modules over a PID.

First, recall a result in last lecture.

Theorem 1.1. *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

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

(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 $\overline{m}_i = x_i + \mathfrak{a}M$.

Assume M is a free module over a PID R with a basis $x_1, x_2, \ldots, x_n$. Let p be an irreducible element of R. Then $(p) = Rp$ is a maximal ideal of R and Theorem 1.1 shows that there is a canonical R-isomorphism

$$M/pM \cong \bigoplus_{i=1}^{n} Rx_i/Rpx_i \cong (R/Rp)^n.$$

This is also an isomorphism of (R/Rp)-vector space. Hence n, the cardinality of the base set, is uniquely determined. In other words, every basis has exactly n elements. We call n the **rank** of M, denoted by $\operatorname{rank}(M) = n$. The zero module is always assumed to be free of rank 0.

Before establishing the coarse structure of a finitely generated module (Theorem 1.2), we need some preparations.

Lemma 1.1. *A submodule of a free module over a PID is still free with smaller rank.*

Proof. Let M be a free R-module with rank n and N a submodule. Let $x_1, x_2, \ldots, x_n$ be a basis of M and set

$$N_r = N \cap \langle x_1, x_2, \ldots, x_r \rangle$$

for $i = 1, 2, \ldots, n$. We claim that N_r is free of rank $\leq r$. In particular, $N_n = N$ is free of rank $\leq n$.

Let

$$I_r = \{a_r \in R \mid a_1x_1 + a_2x_2 + \cdots + a_rx_r \in N \text{ for some } a_1, a_2, \ldots, a_r \in R\}.$$

Then I_r is an ideal of R, thus principal, say $I_r = (d_r)$ for some $d_r \in R$.

For $r = 1$, we have $N_1 = \langle d_1x_1 \rangle$. If $d_1 = 0$, then $N_1 = 0$ is free of rank 0. If $d_1 \neq 0$, then d_1x_1 is linearly independent and N_1 is free of rank 1.

Assume inductively that N_r is free of rank $\leq r$. Since $I_{r+1} = (d_{r+1})$, there exist $b_1, b_2, \ldots, b_r \in R$ such that

$$\varepsilon = b_1x_1 + b_2x_2 + \cdots + b_rx_r + d_{r+1}x_{r+1} \in N.$$

For any $\alpha = a_1x_1 + a_2x_2 + \cdots + a_rx_r + a_{r+1}x_{r+1} \in N_{r+1}$, $a_{r+1} \in (d_{r+1})$, i.e., there exists some $a \in R$ such that $a_{r+1} = ad_{r+1}$. Then $\alpha - a\varepsilon \in N_r$. It follows $N_{r+1} = N_r + \langle \varepsilon \rangle$.

If $d_{r+1} = 0$, then $N_{r+1} = N_r$ and hence N_{r+1} is free of rank $< r + 1$.

If $d_{r+1} \neq 0$, we have $\operatorname{ann}(\varepsilon) = 0$ and $N_r \cap \langle \varepsilon \rangle = 0$, since $x_1, x_2, \ldots, x_{r+1}$ are linearly independent. Hence $N_{r+1} = N_r \oplus \langle \varepsilon \rangle \cong N_r \oplus R$. It follows that N_{r+1} is free of rank $\leq r + 1$. □

Remark 1.1.

1. The proof of Lemma 1.1 shows that $N_r = N \cap \langle x_1, x_2, \ldots, x_r \rangle = \langle y_1, y_2, \ldots, y_r \rangle$, where

   $$y_r = a_{1r}x_1 + a_{2r}x_2 + \cdots + a_{rr}x_r, \quad r = 1, 2, \ldots, n.$$

   In particular, $N = \langle y_1, y_2, \ldots, y_n \rangle$. In terms of the language of matrices, we can formally write

   $$(y_1, y_2, \ldots, y_n) = (x_1, x_2, \ldots, x_n) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}.$$

   The element d_r in the proof is just a_{rr}. If $N_r = N_{r+1}$ happens, or equivalently $a_{r+1,r+1} = d_{r+1} = 0$, then we may take $y_{r+1} = 0$, and the $(r+1)$-th column of the matrix $(a_{ij})_{n \times n}$ on the right-hand side is zero.

2. Lemma 1.1 is not true if R is not a domain. For example, let $R = M = \mathbb{Z}/4\mathbb{Z}$. Then M is a free R-module of rank 1. Take $N = 2M = \{\overline{0}, \overline{2}\} = \langle \overline{2} \rangle$. The submodule N is not free, since $\overline{2}$ is not linearly independent.

3. Lemma 1.1 is also true for the case of infinity rank.

Corollary 1.1. *A submodule of a finitely generated module over a PID is also finitely generated.*

Proof. Let M be an R-module generated by $x_1, x_2, \dots, x_n$ and let N be a submodule. Define

$$\tau : R^n \to M$$
$$(a_1, \dots, a_n) \mapsto a_1x_1 + \cdots + a_nx_n$$

Then τ is an epimorphism of R-modules. Let $N' = \tau^{-1}(N)$ be the inverse image of N in R^n. By Lemma 1.1, N' is free of rank $\leq n$. Take a basis $y_1, y_2, \dots, y_r$ of N'. Then $\tau(y_1), \tau(y_2), \dots, \tau(y_r)$ form a generator of N. Consequently N is finitely generated. □

Remark 1.2.

1. Every submodule of a finitely generated module over a Noetherian ring is also finitely generated. Corollary 1.1 is a direct consequence of this general result.
2. We can mimic the proof of Lemma 1.1 to give a direct proof of Corollary 1.1. But the sum $N_{r+1} = N_r + \langle \varepsilon \rangle$ may not be a direct sum.

Lemma 1.2. *A finitely generated torsion-free module over a PID is free.*

Proof. Let R be a PID and assume M is a torsion-free R-module with a generating set $S = \{x_1, x_2, \dots, x_n\}$. Then S has a maximal linearly independent subset, say $\{x_1, x_2, \dots, x_m\}$ $(m \leq n)$, for simplicity. Clearly the submodule $\langle x_1, x_2, \dots, x_m \rangle$ is free of rank m.

If $m = n$, then $M = \langle x_1, x_2, \dots, x_n \rangle$ is already free of rank n. We next assume $m < n$.

For $i = m + 1, \dots, n$, the subset $\{x_1, x_2, \dots, x_m, x_i\}$ is linearly dependent over R. Hence there exist $a_{i1}, a_{i2}, \dots, a_{im}, b_i \in R$, not all zero, such that

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{im}x_m + b_ix_i = 0.$$

Thus $b_ix_i \in \langle x_1, x_2, \dots, x_m \rangle$. We claim $b_i \neq 0$. Otherwise, $a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{im}x_m = 0$ and $a_{i1}, a_{i2}, \dots, a_{im}$ are not all zero. This contradicts to the linearly independency of $\{x_1, x_2, \dots, x_m\}$.

Take $b = b_{m+1}b_{m+2} \cdots b_n$. Then $b \neq 0$ and $bM = Rbx_1 + Rbx_2 + \cdots + Rbx_n \subseteq \langle x_1, x_2, \dots, x_m \rangle$. By Lemma 1.1, the submodule bM is free.

Consider the map $\tau_b : M \to bM$ given by $\tau_b(x) = bx$. It's obvious that τ_b is an epimorphism of R-modules. On the other hand, τ_b is injective, since M is torsion-free. This means that τ_b is an isomorphism and then M is free. □

Remark 1.3.

1. If we drop the "finitely generated" hypothesis, a torsion-free module may not be free. A counterexample is given by the $\mathbb{Z}$-module $\mathbb{Q}$. Two rational numbers are always $\mathbb{Z}$-dependent.
2. Lemma 1.2 is easy to prove when the PID is a field. For general PID R, we can embed R into its quotient field to achieve another proof of the lemma.

Recall that

$$\mathrm{Tor}(M) = \{x \in M \mid ax = 0 \text{ for some nonzero element } a \in R\}.$$

The following coarse structure theorem (Theorem 1.2) shows a finitely generated module over a PID can decompose into torsion part and torsion-free part. And the torsion-free part is actually free by the above discussion.

Theorem 1.2. *Let R be a PID and M a finitely generated module over R. Then $M/\mathrm{Tor}(M)$ is free and*

$$M = \mathrm{Tor}(M) \oplus N,$$

where N is a free submodule of M such that $N \cong M/\mathrm{Tor}(M)$. In particular, the rank of such a module N is uniquely determined by M.

Proof. Firstly, we claim that $M/\mathrm{Tor}(M)$ is torsion-free.

Actually, let $\overline{x} \in M/\mathrm{Tor}(M)$ denote the residue class of x modulo $\mathrm{Tor}(M)$. If $a\overline{x} = 0$ for some nonzero $a \in R$, then $ax \in \mathrm{Tor}(M)$ and there exists a nonzero element $b \in R$ such that $bax = 0$. But $ba \neq 0$. It follows that x is torsion and $x \in \mathrm{Tor}(M)$, i.e. $\overline{x} = 0$.

Secondly, $M/\mathrm{Tor}(M)$ is obviously finitely generated. Thus, $M/\mathrm{Tor}(M)$ is free of finite rank, by Lemma 1.2. Hence there exists an isomorphism $\eta : M/\mathrm{Tor}(M) \to R^m$, where m is the rank of $M/\mathrm{Tor}(M)$. Clearly, m is uniquely determined by M.

Now, for $1 \leq i \leq m$, take any $x_i \in M$ satisfying

$$\eta(\overline{x}_i) = e_i = (0, \ldots, 0, 1, 0 \cdots, 0) \in R^m.$$

Then $\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_m$ form a basis of $M/\mathrm{Tor}(M)$. Consequently $x_1, x_2, \ldots, x_m$ are linearly independent and $N = \sum Rx_i = \langle x_1, x_2, \ldots, x_m \rangle \cong R^m$ is a free submodule of M with rank m.

Let $\alpha \in M$. Since $\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_m$ generate $M/\mathrm{Tor}(M)$, there exist $a_1, a_2, \ldots, a_m$ such that $\overline{\alpha} = a_1\overline{x}_1 + a_2\overline{x}_2 + \cdots + a_m\overline{x}_m$. Thus $\alpha - (a_1x_1 + a_2x_2 + \cdots + a_mx_m) = \gamma \in \mathrm{Tor}(M)$, i.e. $\alpha = \gamma + (a_1x_1 + a_2x_2 + \cdots + a_mx_m)$. This means $M = \mathrm{Tor}(M) + N$. Since N has no nonzero torsion element, we have $\mathrm{Tor}(M) \cap N = \{0\}$. Therefore $M = \mathrm{Tor}(M) \oplus N$. □

Exercises

1. Let I be an ideal of a ring R. Show that I is a free R-module if and only if it is a principal ideal generated by $\alpha \in R$ which is not a zero divisor.

2. Show that a commutative ring R with identity such that every finitely generated module is free is a field.

3. Let V be a free module over a ring R with a finite basis. Prove or disprove:

   (a) Every set of generating set contains a basis.

   (b) Every linearly independent set can be extended to a basis.

   (c) $\mathrm{Tor}(V) = 0$.

4. Let M be a module over a UFD R and $x \in M$. Assume $\mathrm{ann}(x) = (p^n)$ for some irreducible element p and positive integer n. Show that

   (a) $\mathrm{ann}(p^m x) = (p^{n-m})$ for $0 \leq m \leq n$;

   (b) $\mathrm{ann}(ax) = (p^n)$ for every element a in R with $\gcd(a, p) = 1$.

5. Let $M = \langle x_1, x_2, \ldots, x_n \rangle$ be a finitely generated R-module. Define the *annihilator* of M by

   $$\mathrm{ann}(M) = \{a \in R \mid am = 0 \text{ for all } m \in M\}.$$

   Then $\mathrm{ann}(M)$ is an ideal of R and $\mathrm{ann}(M) = \mathrm{ann}(x_1) \cap \mathrm{ann}(x_2) \cap \cdots \cap \mathrm{ann}(x_n)$.

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

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

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

   (c) Let $M = \langle y, z \rangle$, where $y, z \in M$ and $\operatorname{ann}(y) = (d_1), \operatorname{ann}(z) = (d_2)$, $(d_1, d_2) = 1$. Show that $M = \langle x \rangle$ for some $x \in M$ such that $\operatorname{ann}(x) = (d_1 d_2)$.

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

7. A nonzero R-module M is called a *prime module* if the annihilator $\operatorname{ann}(M) = \operatorname{ann}(N)$ for any nonzero submodule N of M.

   (a) For a prime module M, show that $\operatorname{ann}(M)$ is a prime ideal in R.

   (b) Let I be an ideal of R. Show that R/I is a prime module over R if and only if I is a prime ideal in R.

8. Show that every finitely generated projective module over a PID is free.

9. Embedding an integral domain into its field of fractions to rewrite the proof of Lemma 1.2.

10. Let
$$M = \{(x_1, x_2, x_3) \in \mathbb{Z}^3 \mid x_1 + 2x_2 + 3x_3 = 0, 3x_1 + 8x_2 + 15x_3 = 0\}.$$
    Show that M is a free submodule of the $\mathbb{Z}$-module $\mathbb{Z}^3$ and find a basis.

2 Lecture 15 (Oct 26, 2023): Structure of Finitely Generated Modules over a PID

The explicit structure theorem for finitely generated modules over a principal ideal domain usually appears in the following two forms.

2.1 Primary Decomposition Theorem

When a vector space over a field F has a finite generating set, then one may extract from it a basis consisting of a finite number n of vectors, and the space is therefore isomorphic to F^n. The corresponding statement with the F generalized to a principal ideal domain (PID) R is no longer true, as a finitely generated module over R need not have any basis. However such a module is still isomorphic to a quotient of some module R^n with n finite. To see this it suffices to construct a homomorphism that sends the elements of the canonical basis R^n to the generators of the module, and take the quotient by its kernel (see the proof of Theorem 1.2). By changing the choice of generating set, one can in fact describe the module as the quotient of some R^n by a particularly simple submodule, and this is the structure theorem.

For an R-module M, we define
$$\operatorname{ann}(M) = \{r \in R \mid rx = 0 \text{ for all } x \in M\}.$$

One can see that

(1) $\operatorname{ann}(M)$ is an ideal of R;

(2) $\operatorname{ann}(M) = \bigcap_{i=1}^{n} \operatorname{ann}(x_i)$, if $M = \langle x_1, \dots, x_n \rangle$. In particular, if $M = \langle x \rangle$, then $\operatorname{ann}(M) = \operatorname{ann}(x)$.

Let R be a PID and M a module over R. For $x \in M$, consider the cyclic module $Rx = \langle x \rangle$ over a PID, the annihilator $\operatorname{ann}(x) = \operatorname{ann}(Rx) = \{r \in R \mid rx = 0\}$ is an ideal of R. Since R is principal, $\operatorname{ann}(x) = (\varphi)$ for some φ in R and we have an R-module isomorphism

$$Rx \cong R/(\varphi).$$

If $\varphi = 0$, then x is linearly independent and $Rx \cong R$. Thus Rx is free of rank 1.

If $\varphi \neq 0$, then Rx is torsion and Rx is isomorphic to $R/(\varphi)$ as R-modules. Since R is a UFD, we have a prime decomposition

$$\varphi = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s},$$

where $p_1, p_2, \dots, p_r$ are irreducible elements and $r_1, r_2, \dots, r_s > 0$. Consequently there is a prime ideal decomposition: $(\varphi) = (p_1)^{r_1}(p_2)^{r_2} \cdots (p_s)^{r_s} = (p_1^{r_1})(p_2^{r_2}) \cdots (p_s^{r_s})$. By Chinese Reminder Theorem (CRT), we have

$$Rx \cong R/(\varphi) \cong R/\left(p_1^{r_1}\right) \oplus R/\left(p_2^{r_2}\right) \oplus \cdots \oplus R/\left(p_s^{r_s}\right).$$

Notice that a direct summand of the form $R/(p^r)$ is an indecomposable R-module, where $r > 0$ and p is irreducible (hence prime). Thus we decompose Rx into a direct sum of indecomposable submodules. This result can be generalized to all finitely generated modules over a PID.

Theorem 2.1 (**Primary Decomposition**). *Let R be a PID and M a finitely generated module over R. Then there exist linearly independent elements $v_1, v_2, \dots, v_m$ and torsion elements x_{ij} such that*

$$M = (Rv_1 \oplus Rv_2 \oplus \cdots \oplus Rv_m) \oplus \bigoplus_{i=1}^{s} (Rx_{i1} \oplus Rx_{i2} \oplus \cdots \oplus Rx_{in_i})$$

and $\operatorname{ann}(x_{ij}) = (p_i^{e_{ij}})$ for $i = 1, 2, \dots, s$ and $j = 1, 2, \dots, n_i$, where $p_1, p_2, \dots, p_s$ are prime elements of R which are not mutually associate, and $e_{i1} \leq e_{i2} \leq \cdots \leq e_{in_i}$. In other words, there is an R-module isomorphism

$$M \cong R^m \oplus \bigoplus_{i=1}^{s} \left(R/(p_i^{e_{i1}}) \oplus R/(p_i^{e_{i2}}) \oplus \cdots \oplus R/(p_i^{e_{in_i}})\right), \tag{1}$$

where the summands $R/(p_i^{e_{ij}})$ are indecomposable.

Furthermore, the integers m and e_{ij} are uniquely determined by M and $p_1, p_2, \dots, p_s$ are unique up to ordering and multiplication by units.

> 设 R 是 PID, M 为有限生成 R-模. 则在 M 中有线性无关元 $v_1, v_2, \dots, v_m$ 和扭元 x_{ij} 使得
>
> $$M = (Rv_1 \oplus Rv_2 \oplus \cdots \oplus Rv_m) \oplus \bigoplus_{i=1}^{s} (Rx_{i1} \oplus Rx_{i2} \oplus \cdots \oplus Rx_{in_i}),$$
>
> 其中 $\operatorname{ann}(x_{ij}) = (p_i^{e_{ij}})$, $p_1, p_2, \dots, p_s$ 为互不相伴的素元, $e_{i1} \leq e_{i2} \leq \cdots \leq e_{in_i}$.
> 换言之, 我们有 R-模同构:
>
> $$M \cong R^m \oplus \bigoplus_{i=1}^{s} \left(R/(p_i^{e_{i1}}) \oplus R/(p_i^{e_{i2}}) \oplus \cdots \oplus R/(p_i^{e_{in_i}})\right),$$
>
> 其中每个直和因子 $R/(p_i^{e_{ij}})$ 都不可分解.
> 并且, m 和 e_{ij} 是由 M 唯一决定的, $p_1, p_2, \dots, p_s$ 在相伴和不计顺序的情况下也是唯一的.

All $p_i^{e_{i1}}, p_i^{e_{i2}}, \dots p_i^{e_{in_i}}$ in (1), $i = 1, 2, \dots s$, which are determined by the torsion part $\operatorname{Tor}(M)$, are called the **elementary divisors** (初等因子) of M.

Proof. By Theorem 1.2, $M = \operatorname{Tor}(M) \oplus N$ with $N \cong R^m$ for some nonnegative integer m. The rank m is uniquely determined by M. So we only need to focus on the torsion part of M.

Assume M is a finitely generated torsion nonzero R-module. That is, $\operatorname{Tor}(M) = M$. Hence $\operatorname{ann}(M) = \{r \in R \mid rx = 0, \forall x \in M\} = (\phi)$ for some element $\phi \notin R^*$. Actually, if $M = \langle x_1, x_2, \dots, x_n \rangle$, then $\operatorname{ann}(M) = \bigcap_{i=1}^n \operatorname{ann}(x_i) \neq 0$.

For a prime element p in R and a positive integer α, define the p^α-torsion part of M by

$$M[p^\alpha] = \{x \in M \mid p^\alpha x = 0\}.$$

It's clear that $M[p^\alpha]$ is a submodule of M and $x \in M[p^\alpha]$ if and only if $\operatorname{ann}(x) \supseteq (p^\alpha)$. Moreover, $M[p^\alpha] \neq 0$ if and only $p \mid \phi$.

Let $\phi = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$, where $p_1, p_2, \dots, p_s$ are all distinct prime divisors of ϕ. Write $p_i^* = \frac{\phi}{p_i^{\beta_i}}$. Then $\gcd(p_1^*, p_2^*, \dots, p_s^*) = 1$ or $(p_1^*) + (p_2^*) + \cdots + (p_s^*) = (1)$, and there exist $a_1, a_2, \dots, a_s \in R$ such that

$$a_1 p_1^* + a_2 p_2^* + \cdots + a_s p_s^* = 1.$$

For $x \in M$, we have $x = a_1 p_1^* x + a_2 p_2^* x + \cdots + a_s p_s^* x$ and $a_i p_i^* x \in M[p_i^{\beta_i}]$ for $i = 1, 2, \dots, s$. Hence $M = M[p_1^{\beta_1}] + M[p_2^{\beta_2}] + \cdots + M[p_s^{\beta_s}]$. Let $x_1 + x_2 + \cdots + x_s = 0$ and each $x_i \in M[p_i^{\beta_i}]$. Taking module action on the left by p_i^*, we have $p_i^* x_i = 0$, since $p_j^{\beta_j} \mid p_i^*$ for all $j \neq i$. But $\gcd(p_i, p_i^*) = 1$. There exist $a, b \in R$ such that $a p_i^{\beta_i} + b p_i^* = 1$. It follows that $x_i = (a p_i^{\beta_i} + b p_i^*) x_i = a p_i^{\beta_i} x_i + b p_i^* x_i = 0$. Hence

$$M = M[p_1^{\beta_1}] \oplus M[p_2^{\beta_2}] \oplus \cdots \oplus M[p_s^{\beta_s}].$$

It remains to show that each $M[p^\beta]$ can be decomposed as a direct sum of a series of indecomposable cyclic modules (in a unique way). Set $N = M[p^\beta]$.

Clearly, N is also finitely generated, say $N = \langle x_1, x_2, \dots, x_r \rangle$. We use induction on the number r of generators.

If $r = 1$, then N is cyclic and $N = \langle x_1 \rangle \cong R/(p^\beta)$ is already indecomposable.

Notice that $\operatorname{ann}(N) = \bigcap_{i=1}^r \operatorname{ann}(x_i)$. If we write $\operatorname{ann}(x_i) = (p^{e_i})$, then $\beta = \max\{e_1, e_2, \dots, e_r\}$. We must have one among the generators whose annihilator is (p^β). Without loss of generality we may assume $\operatorname{ann}(x_1) = (p^\beta)$. Consider $\overline{N} = N/\langle x_1 \rangle$. Then $\overline{N} = \langle \overline{x_2}, \dots, \overline{x_r} \rangle$ has $r - 1$ generators and $\operatorname{ann}(\overline{N}) = (p^{\beta_1})$

with $\beta_1 \leq \beta$. By induction, $\overline{N}$ is a direct sum of a series of indecomposable cyclic modules. That is, $\overline{N} = \langle z_1 \rangle \oplus \langle z_2 \rangle \oplus \cdots \oplus \langle z_\ell \rangle$ for some $z_1, z_2, \ldots, z_\ell \in \overline{N}$ and each $\langle z_i \rangle$ is indecomposable. In virtue of the following Lemma 2.1, we have $y_1, y_2, \ldots, y_\ell \in N$ such that $\overline{y}_i = z_i$ for $i = 1, 2, \ldots, r$, and

$$N = \langle x_1 \rangle \oplus \langle y_1 \rangle \oplus \cdots \oplus \langle y_\ell \rangle,$$

where $\langle x_1 \rangle, \langle y_1 \rangle, \ldots, \langle y_\ell \rangle$ are indecomposable and they are isomorphic to an R-module of the form $R/(p^e)$.

The uniqueness of the decomposition comes from another form of structure theorem as in Theorem 2.2. □

Lemma 2.1. *Let M be a torsion module over a PID R and let $x_0 \in M$ be an element in R such that $\operatorname{ann}(x_0) = \operatorname{ann}(M) = (p^n)$, where p is a prime element and n is a positive integer. Set $\overline{M} = M/\langle x_0 \rangle$.*

1. *For any $\alpha \in \overline{M}$, there exists $y \in M$ such that $\overline{y} = \alpha$ and $\operatorname{ann}(y) = \operatorname{ann}(\alpha)$.*

2. *If $\overline{M} = \langle \alpha_1 \rangle \oplus \langle \alpha_2 \rangle \oplus \cdots \oplus \langle \alpha_r \rangle$, then for each $\alpha_i \in \overline{M}$, there exists a representative $y_i \in M$ such that $\overline{y_i} = \alpha_i, \operatorname{ann}(y_i) = \operatorname{ann}(\alpha_i)$ and $M = \langle x_0 \rangle \oplus \langle y_1 \rangle \oplus \cdots \oplus \langle y_r \rangle$.*

Proof. (1) Let $\alpha \in \overline{M}$ and $\operatorname{ann}(\alpha) = (p^m)$, $1 \leq m \leq n$. Taking any $y_0 \in M$ such that $\overline{y_0} = \alpha$, we have $\operatorname{ann}(y_0) = (p^s)$ with $1 \leq m \leq s \leq n$. Since $p^m \overline{y_0} = 0$, there exist nonnegative integer $t \leq n$ and $q \in R$ such that

$$p^m y_0 = p^t q x_0, \ \gcd(p, q) = 1.$$

But $\operatorname{ann}(p^m y_0) = (p^{s-m})$, $\operatorname{ann}(p^t q x_0) = \operatorname{ann}(p^t x_0) = (p^{n-t})$. We have $s - m = n - t$, yielding $t = m + (n - s) \geq m$.

Now take $y = y_0 - p^{t-m} q x_0$. Then $\overline{y} = \overline{y_0} = \alpha$ and $p^m y = 0$. Thus $(p^m) \subseteq \operatorname{ann}(y)$. If $(p^m) \subsetneq \operatorname{ann}(y)$, then $p^{m-1} y = 0$, yielding $p^{m-1} y_0 \in \langle x_0 \rangle$ or $p^{m-1} \overline{y_0} = 0$ in $\overline{M}$. This implies $s < m$, contradicting to the choice of s. Hence $\operatorname{ann}(y) = (p^m) = \operatorname{ann}(\alpha)$.

(2) Assume $\overline{M} = \langle \alpha_1 \rangle \oplus \langle \alpha_2 \rangle \oplus \cdots \oplus \langle \alpha_r \rangle$ for some $\alpha_1, \alpha_2, \ldots, \alpha_r \in \overline{M}$. Then we can choose a representative $y_i \in M$ for each α_i such that $\overline{y_i} = \alpha_i$ and $\operatorname{ann}(y_i) = \operatorname{ann}(\alpha_i)$.

Let $x \in M$. Then $\overline{x} = \sum_{i=1}^r a_i \alpha_i$ for some $a_1, a_2, \ldots, a_r \in R$. It follows that $x - \sum_{i=1}^r a_i y_i = a_0 x_0$ for some $a_0 \in R$. That is, $x = a_0 x_0 + \sum_{i=1}^r a_i y_i$. This means $M = \langle x_0 \rangle + \langle y_1 \rangle + \cdots + \langle y_r \rangle$.

Now let $0 = b x_0 + b_1 y_1 + \cdots + b_r y_r$ for some $b, b_1, \ldots, b_r \in R$. Then taking modulo, we have $b_1 \alpha_1 + \cdots + b_r \alpha_r = 0$ in $\overline{M}$, yielding $b_i \alpha_i = 0$ for each i. It follows $b_i \in \operatorname{ann}(\alpha_i) = \operatorname{ann}(y_i)$ and hence $b_i y_i = 0$ for each i, which implies $b x_0 = 0$. So $M = \langle x_0 \rangle \oplus \langle y_1 \rangle \oplus \cdots \oplus \langle y_r \rangle$.

□

Remark 2.1. The elementary divisors of a finitely generated module over a PID are only determined by its torsion part.

Remark 2.2.
1. Let p be an irreducible element. A torsion module M is called a **p-module** (p-模) if $\operatorname{ann}(M) = (p^n)$ for some positive inter n. Recall in group theory, a *p-group* (p-群) is a finite group of order p^n for some positive integer n.

2. For an irreducible element p in R, $M[p^n] \subseteq M[p^{n+1}]$ for all $n \geq 1$. Set $M[p^\infty] = \bigcup_{n \geq 1} M[p^n]$. It's easy to see that $M[p^\infty]$ is a p-submodule of M, which is called the *p-part* of M. If M is a finitely generated torsion module, one can see that $M[p_i^\infty] = M[p_i^n]$ for some positive integer n.

3. In the proof of Theorem 2.1, we can choose y_i so that $\operatorname{ann}(y_i) = \operatorname{ann}(z_i)$. Hence each $\langle y_i \rangle \cong \langle z_i \rangle \cong R/\operatorname{ann}(y_i)$. So the exponent of the annihilator of each component can be inductively arranged in decreasing order.

4. The first step of proving Theorem 2.1 is to decompose a finitely generated module as a direct sum of distinct p-modules. Then every p-modules can be decomposed into a series of indecomposable cyclic p-module. The proof of Theorem 2.1 includes three parts.

   (i) $M = R^m \oplus \operatorname{Tor}(M)$ for some nonnegative integer m.

   (ii) If $M = \operatorname{Tor}(M)$, then $M = \oplus_p M[p^\infty]$, where p ranges over all prime elements of R and almost all $M[p^\infty]$ are zero. Actually, $M[p^\infty] \neq 0$ if and only if p is an irreducible divisor of ϕ, where $(\phi) = \operatorname{ann}(M)$.

   (iii) Each nonzero module $M[p^\infty]$ can be decomposition into a series of indecomposable p-modules: $M[p^\infty] = \langle \alpha_1 \rangle \oplus \langle \alpha_2 \rangle \oplus \cdots \oplus \langle \alpha_s \rangle$ and each $\langle \alpha_i \rangle \cong R/(p^{e_i})$ for some $e_i > 0$.

5. Theorem 2.1 shows that a finitely generated p-module M is isomorphic to a module of the form

$$R/(p^{e_1}) \oplus R/(p^{e_2}) \oplus \cdots \oplus R/(p^{e_r})$$

   in a unique way, where $1 \leq e_1 \leq e_2 \leq \cdots \leq e_r$. We called $(p^{e_1}, p^{e_2}, \ldots, p^{e_r})$ the **type** of M. For example, $R/(p) \oplus R/(p) \oplus R/(p^2)$ is a module of (p, p, p^2)-type.

In particular, the Primary Decomposition Theorem shows

Corollary 2.1. *Every finitely generated module over a PID is a direct sum of cyclic modules.*

We can get more information from the Primary Decomposition Theorem.

Corollary 2.2. *Let R be a PID and M a finitely generated torsion module over R. Let*

$$p_1^{e_{11}}, \ldots p_1^{e_{1n_1}}, \ldots, p_s^{e_{s1}}, \ldots p_s^{e_{sn_s}}$$

be the elementary divisors of M and $e_{i1} \leq e_{i2} \leq \cdots \leq e_{in_i}$ for all $1 \leq i \leq s$. Then

$$\operatorname{Tor}(M) = (p_1^{e_{1n_1}} \cdots p_s^{e_{sn_s}}).$$

Corollary 2.3. *Let R be a PID and let M, N be two finitely generated torsion modules over R. Then M and N are isomorphic over R if and only if they have the same elementary divisors.*

2.2 Invariant Factor Decomposition Theorem

We have proved the

Primary Decomposition Theorem (Theorem 2.1) Every finitely generated module M over a principal ideal domain R is isomorphic to one of the form

$$R^m \bigoplus_i \left(R/(p_i^{e_{i1}}) \bigoplus R/(p_i^{e_{i2}}) \bigoplus \cdots \bigoplus R/(p_i^{e_{in_i}}) \right),$$

where the summands $R/(p_i^{e_{ij}})$ are indecomposable, each p_i is distinct prime elements of R and $e_{i1} \leq e_{i2} \leq \cdots \leq e_{in_i}$. The integer m is uniquely determined by M and the elementary divisors $p_i^{e_{ij}}$ are unique up to ordering and multiplication by units.

Assume $\mathrm{Tor}(M) = M$ and $\mathrm{ann}(M) = (\phi)$, where $\phi = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ is a prime decomposition of d. Using the Primary Decomposition Theorem, decompose (torsion module) M into a direct sum of p-submodules $M[p_1^{\beta_1}], M[p_2^{\beta_2}], \cdots, M[p_s^{\beta_s}]$, and then decompose each $M[p_i^{\beta_i}]$ into a direct sum of cyclic submodules of annihilator $p_i^{e_{ij}}$, $j = 1, 2, \ldots, n_j$. That is,

$$M[p_i^\infty] = M[p_i^{\beta_i}] \cong R/\left(p_i^{e_{i1}}\right) \oplus R/\left(p_i^{e_{i2}}\right) \oplus \cdots \oplus R/\left(p_i^{e_{in_i}}\right)$$

with $0 \le e_{i1} \le e_{i2} \le \cdots \le e_{in_i}$. We visualize these direct summands symbolically as described by the following diagram:

$$\begin{array}{ll} p_i\text{−part} & \text{exponents in decreasing order} \\ M[p_1^\infty]: & t_{1n} \ge t_{1,n-1} \ge \cdots \ge t_{11} \\ M[p_2^\infty]: & t_{2n} \ge t_{2,n-1} \ge \cdots \ge t_{21} \\ \vdots & \qquad\vdots \\ M[p_s^\infty]: & t_{sn} \ge t_{s,n-1} \ge \cdots \ge t_{s1} \end{array}$$

A horizontal row describes the type of the module with respect to the prime at the left (actually, $n = \max\{n_1, n_2, \ldots, n_s\}$). For example, the first row comes from the p_1-part: $M[p_1^\infty] \cong R/(p_1^{t_{11}}) \oplus R/(p_1^{t_{12}}) \oplus \cdots \oplus R/(p_1^{t_{1n}})$. The exponents t_{ij} are arranged in decreasing order for each fixed i. Some t_{ij} may be zero. We add minimal number of zeros as entries at each tail to form a array as below.

$$\begin{array}{cccc} t_{1n} & t_{1,n-1} & \cdots & t_{11} \\ t_{2n} & t_{2,n-1} & \cdots & t_{21} \\ \vdots & \vdots & & \vdots \\ t_{sn} & t_{s,n-1} & \cdots & t_{s1} \end{array}$$

Here $t_{ij} = 0$ or $t_{ij} = e_{ij'}$ for some $1 \le j' \le n_i$. In other word, some of the exponents t_{ij} may be zero, but the last column is nonzero. Let

$$d_i = p_1^{t_{1i}} p_2^{t_{2i}} \cdots p_s^{t_{si}},$$

correspond to the $(n+1-i)$-th column of the above array of exponents for $i = 1, 2, \ldots, n$ (This is what we did in Linear Algebra to reconstruct the invariant factors from the elementary divisors of a λ-matrix). The direct sum of the cyclic modules represented by the i-th column is then isomorphic to $R/(d_{n+1-i})$, by Chinese Remainder Theorem. For example, the first column corresponds to

$$R/(p_1^{t_{1n}}) \oplus R/(p_2^{t_{2n}}) \oplus \cdots \oplus R/(p_s^{t_{sn}}) \cong R/(d_n).$$

Thus we get a direct sum decomposition

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_n) \tag{2}$$

with $d_1 \mid d_2 \mid \cdots \mid d_n$.

Example 2.1. Let $p_1, p_1^2,\ p_2, p_2, p_2^3,\ p_3^2, p_3^{2023}$ be the elementary divisors of M. Then we construct the following array:

$$\begin{array}{ccc} p_1^2 & p_1^1 & p_1^0 \\ p_2^3 & p_2^1 & p_2^1 \\ p_3^{2023} & p_3^2 & p_3^0. \end{array}$$

So $d_1 = p_2,\ d_2 = p_1 p_2 p_3^2,\ d_3 = p_1^2 p_2^3 p_3^{2023}$.

Next we show that these d_i are essentially unique, which implies that the elementary factors in Theorem 2.1 are uniquely determined.

Actually, we remark

$$\operatorname{ann}(M) = \bigcap_{i=1}^{n} \operatorname{ann}\left(R/(d_i)\right) = \bigcap_{i=1}^{n} (d_i) = (d_n).$$

It follows that (d_n) is uniquely determined by M. Because $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$ with $M_i \cong R/(d_i)$ for each i, we have

$$\overline{M} = M/M_n \cong M_1 \oplus M_2 \oplus \cdots \oplus M_{n-1} \cong R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_{n-1}).$$

This is a direct sum decomposition of $\overline{M}$ as (2) and $\overline{M}$ has only $n-1$ direct summands. By induction, the principal ideals $(d_1), (d_2), \ldots, (d_{n-1})$ are also uniquely determined.

So we establish the following

Theorem 2.2 (**Invariant Factor Decomposition**). *Let R be a PID and M a finitely generated module over R. Then there exist linearly independent elements $v_1, v_2, \ldots, v_m$ and torsion elements $z_1, z_2, \ldots, z_n$ such that*

$$M = (Rv_1 \oplus Rv_2 \oplus \cdots \oplus Rv_m) \bigoplus (Rz_1 \oplus Rz_2 \oplus \cdots \oplus Rz_n)$$

and $\operatorname{ann}(z_i) = (d_i)$ for $i = 1, 2, \ldots, n$, together with the property $d_1 \mid d_2 \mid \cdots \mid d_n$.

In other words, every finitely generated module M over a principal ideal domain R is isomorphic to a unique one of the form

$$R^m \oplus R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_n)$$

where $0 \neq (d_i) \neq R$ and $d_1 \mid d_2 \mid \cdots \mid d_n$. The number m and the nonzero ideals (d_i) are uniquely determined by M.

设 R 是 PID, M 为有限生成 R-模. 则在 M 中存在线性无关元 $v_1, v_2, \ldots, v_m$ 和扭元 z_1, z_2, $\ldots$, z_n, 使得

$$M = (Rv_1 \oplus Rv_2 \oplus \cdots \oplus Rv_m) \bigoplus (Rz_1 \oplus Rz_2 \oplus \cdots \oplus Rz_n),$$

其中 $\operatorname{ann}(z_i) = (d_i)$, 且 $d_1 \mid d_2 \mid \cdots \mid d_n$.
换言之, M 和如下的 R-模同构:

$$R^m \oplus R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_n),$$

其中 $0 \neq (d_i) \neq R$, 且 $d_1 \mid d_2 \mid \cdots \mid d_n$.
并且, m 和非零理想 (d_i) 由 M 唯一决定.

The nonzero elements $d_1, d_2, \ldots, d_n$ determined by the torsion part $\operatorname{Tor}(M)$ are called a collection of **invariant factors** (不变因子) of M. They form a complete set of invariants for the module and are uniquely determined up to multiplication by units.

Remark 2.3. The invariant factors of a finitely generated module over a PID are determined by its torsion part.

Example 2.2. Let

$$\lambda, \lambda^2,\ \lambda - 1, (\lambda-1)^3,\ \lambda^2 - 2, \lambda^2 - 2, \lambda^2 - 2, (\lambda^2 - 2)^{2023}$$

be the elementary divisors of a $\mathbb{Q}[\lambda]$-module. Then its invariant factors are

$$d_1 = d_2 = \lambda^2 - 2,\ d_3 = \lambda(\lambda-1)(\lambda^2-2),\ d_4 = \lambda^2(\lambda-1)^3(\lambda^2-2)^{2023}.$$

Theorem 2.3. *Two finitely generated torsion modules over a PID are isomorphic if and only if they have the same elementary divisors up to units and ordering, or equivalently they have the same invariant divisors up to units and ordering.*

The next theorem is included for completeness. It is called the *invariant factor theorem* for free modules.

Theorem 2.4. *Let R be a PID and M a free module of rank m over R, and let N be a nonzero submodule with $\operatorname{rank}(N) = n$. Then there exists a basis $x_1, x_2, \dots, x_m$ of M and non-zero elements $d_1, d_2, \dots, d_n \in R$ such that $d_1 \mid d_2 \mid \cdots \mid d_n$ and $d_1x_1, d_2x_2, \dots, d_nx_n$ form a basis of N. Furthermore, The sequence of ideals $(d_1), (d_2), \dots, (d_n)$ is uniquely determined by the preceding conditions.*

The ideals $(d_1), (d_2), \dots, (d_n)$ in Theorem 2.4 are the invariants of N in M.

We formulate a proof of Theorem 2.4 by considering N as a submodule of $M = R^m$, and applying the method of row and column operations to get a desired basis. In this context, we make some further comments which may serve to illustrate Theorem 2.4. By *row operations* we mean: interchanging two rows; adding a multiple of one row to another; multiplying a row by a *unit* in the ring. The *column operations* are defined in the similar way. These row and column operations correspond to multiplying with the so-called elementary matrices in the ring. Theorem 2.4 is an immediate consequence of the following

Lemma 2.2. *Let A be a non-zero $m \times m$ matrix whose entries are in a PID R. Then with a finite number of row and column operations, it is possible to bring the matrix to the diagonal form*

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & d_n & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} = \operatorname{diag}(d_1, d_2, \dots, d_n, 0 \cdots, 0), \tag{3}$$

where $d_1d_2\cdots d_n \neq 0$ and $d_1|d_2|\cdots|d_n$. And the ideals $(d_1), (d_2), \dots, (d_n)$ are uniquely determined subject to the preceding conditions.

Proof of Theorem 2.4 Let $\varepsilon_1, \dots, \varepsilon_m$ be a basis of M. Since submodule N is also free, we can choose arbitrary basis $\eta_1, \dots, \eta_n$ for N with $n \le m$. Expressing each η_i as a linear combination of $\varepsilon_1, \dots, \varepsilon_m$, we get a formal expression

$$(\eta_1, \dots, \eta_n, 0, \dots, 0) = (\varepsilon_1, \dots, \varepsilon_m)A,$$

where A is an $m \times m$ matrix over R. By Lemma 2.2, we have invertible matrices P and Q such that $PAQ = \operatorname{diag}(d_1, \dots, d_r, 0, \dots, 0)$ with $d_1 \cdots d_n \neq 0$. Thus

$$\begin{aligned}(\eta_1, \dots, \eta_n, 0, \dots, 0)Q &= (\varepsilon_1, \dots, \varepsilon_m)P^{-1} \cdot PAQ \\ &= (\varepsilon_1, \dots, \varepsilon_m)P^{-1} \cdot \operatorname{diag}(d_1, \dots, d_r, 0, \dots, 0).\end{aligned} \tag{4}$$

Now set

$$(y_1, \dots, y_m) = (\eta_1, \dots, \eta_n, 0, \dots, 0)Q \quad \text{and} \quad (x_1, \dots, x_m) = (\varepsilon_1, \dots, \varepsilon_m)P^{-1}.$$

Then $y_1, \dots, y_m$ generate N and $x_1, \dots, x_m$ is a basis of M. Furthermore, (4) implies that $r = n$ and $y_1 = d_1x_1, \dots, y_n = d_nx_n, y_{n+1} = \cdots = y_m = 0$. This shows that $d_1x_1, \dots, d_nx_n$ form a basis of N.

If we take R to be the polynomial ring $k[\lambda]$ over a field k, then (3) is just the *Smith Normal Form*. This is the canonical form of a λ-matrix as we discussed in Linear Algebra.

Remark 2.4. The Primary Decomposition Theorem (Theorem 2.1) and Invariant Factor Decomposition Theorem (Theorem 2.2) are essentially equivalent because of the Chinese Remainder Theorem.

Taking $R = \mathbb{C}[x]$ yields the fundamental theorem of Jordan Canonical Form on matrices and taking $R = \mathbb{Z}$ yields the fundamental theorem of finitely generated abelian groups.

Exercises

1. Let R be a PID and M a module over R. For $x, y \in M$, show that Rx is isomorphic to Ry as R-modules if and only if $\operatorname{ann}(x) = \operatorname{ann}(y)$.

2. Let A be an $m \times n$ matrix M over a PID R. Give an existential argument that there are invertible $m \times m$ matrix P and invertible $n \times n$ matrix Q, such that PAQ is diagonal.

3. Given a row vector $v = (x_1, \dots, x_{n-1}, x_n) \in \mathbb{Z}^n$ with $\gcd(x_1, \dots, x_{n-1}, x_n) = 1$, Show that there exists an $n \times n$ integer matrix P with determinant ± 1 such that $vP = (0, \dots, 0, 1)$.

4. Given a row vector $v = (x_1, \dots, x_{n-1}, x_n) \in \mathbb{Z}^n$ with $\gcd(x_1, \dots, x_{n-1}, x_n) = 1$, show that there exists an $n \times n$ integer matrix P with determinant ± 1 whose bottom row is v.

5. Let $A = (a_{ij})_{n \times n} \in M_n(\mathbb{Z})$ be a matrix with $\det A \neq 0$ and M the submodule generated by the row vectors of A over $\mathbb{Z}$.

   (a) Show that M is a free module of rank n over $\mathbb{Z}$.

   (b) Show that the index $[\mathbb{Z}^n : M]$ of subgroup M in $\mathbb{Z}^n$ is $|\det A|$.

2.3 Quiz 3

1. (8分) 设 S 为交换(幺)环, R 为 S 的子环, 于是 S 自然成为一个 R-模, 其模作用就是环中的乘法. 若 S 是一个秩为 n 的 R 上的自由模, 证明: S 同构于矩阵环 $\mathrm{M}_n(R)$ 的一个子环(即存在从 S 到 $\mathrm{M}_n(R)$ 的单同态).

2. (12分) 已知 $\mathbb{R}^3$ 上的线性变换 $\mathbb{T}$ 由 $\mathbb{T}(x, y, z) = (x + z, y, y + z)$ 给出, $m(\lambda)$ 为 $\mathbb{T}$ 的极小多项式. 通过 $\mathbb{T}$, $\mathbb{R}^3$ 以标准的方式成为一个 $\mathbb{R}[\lambda]$-模.

   (1) 求 $m(\lambda)$.

   (2) 设 $v \in \mathbb{R}^3, v \neq (x, 0, z)$. 证明: 作为 $\mathbb{R}[\lambda]$-模, $\mathbb{R}[\lambda]v = \langle v \rangle$ 与 $\mathbb{R}[\lambda]/(m(\lambda))$ 同构.

   (3) 证明: $\mathbb{R}^3$ 为循环 $\mathbb{R}[\lambda]$-模.

Homework Exercise 1, 3, 4, 5, 6, 20 on page 209-210.