Structure Theorem of Sub-Modules of Free Modules of Finite Rank over PID

Jiang-Hua Lu

The University of Hong Kong

Monday March 3, 2025

In this file:

1. Sub-modules of finite rank free modules over PIDs;

Recall: Let R be any commutative ring (not necessarily a PID).

- An R-module is said to be free if it has a basis, i.e., a linearly independent generating set.
- If $M \neq 0$ is a free and finitely generated R-modules, then all bases of M have the same finite cardinality, called the rank of M.
- A free R-module M of rank n is isomorphic to R^n.

We now look at sub-modules of R^n. Why?

Question: Assume M is a finitely generated R-module, and has no torsion. Is M a free R-module?

Ex: $R = \mathbb{C}[x]$, $M = \mathbb{C}[x]/\langle x \rangle$ as an R-module. is torsion.

$$x \cdot (f + \langle x \rangle) = 0$$

Ex: let $R = \mathbb{Z}[x]$. $M = 2R + xR \subseteq R$ as a module of R is ~~not~~ free.

In general, if $I \subset R$ is an ideal of R regarded as an R-module. If free w/ basis basis $\mathcal{B}$,

For any $b_1, b_2 \in \mathcal{B}$, $b_1 b_2 - b_2 b_1 = 0$

so $|\mathcal{B}| = 1$, so I must be principal.

If R is an ID, then I is free $\iff$ I is principal.

Let R be any commutative ring.

Lemma. An R-module M is finitely generated if and only if

$$M \cong R^n/N$$

for some integer $n \geq 1$ and some sub-module N of R^n.

Pf: Assume M is generated by $s_1, \cdots, s_n \in M$.
Then we have an R-mod. homomorphism

$$R^n \xrightarrow{\varphi} M, \quad (r_1, \cdots, r_n) \mapsto r_1 s_1 + \cdots + r_n s_n$$

which is also surjective. So

$$R^n/\ker\varphi \xrightarrow{\cong} M$$

is an R-mod. isomorphism

Examples of R-submodules of R^n:

1) $I_1 \times \cdots \times I_n \subset R^n$

$\{ (x_1, \cdots x_n) : x_i \in I_i \}$

If R is a PID, then $I_i = a_i R$,

so $I_1 \times \cdots \times I_n = a_1 R \times \cdots \times a_n R$

Examples of sub-modules of free modules

Let R be a PID and let $A = (a_{ij}) \in M_{m,n}(R)$. Identifying

$$R^n \cong M_{n,1}(R) \quad \text{and} \quad R^m \cong M_{m,1}(R),$$

we have the R-module map

$$L_A : R^n \longrightarrow R^m,\ L_A(x) = Ax.$$

Thus we have the sub-modules $\mathrm{Ker}(L_A) \subset R^n$ and $\mathrm{Im}(L_A) \subset R^m$.

What does Smith Normal Form Theorem tell us about $\mathrm{Ker}(L_A) \subset R^n$ and $\mathrm{Im}(L_A) \subset R^m$?

Let $P = (P_1, \cdots, P_m)$, $Q = (g_1, \cdots, g_n)$

Then $\{P_1, \cdots, P_m\}$ is an R-basis of R^m

$\{g_1, \cdots g_n\}$ is an R-basis of R^n

so $Ax = 0 \iff PDQ^{-1}x = 0 \iff DQ^{-1}x = 0$ ($Q^{-1}x = x'$)

$$\iff \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_s & \\ & & & 0 \cdots 0 \end{pmatrix} \begin{pmatrix} x_1' \\ \vdots \\ x_n' \end{pmatrix} = 0 \iff \begin{matrix} d_1 x_1' = 0 \\ \vdots \\ d_s x_s' = 0 \end{matrix}$$

$$\iff x' = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x_{s+1} \\ \vdots \\ x_n \end{pmatrix}$$

$$\iff x = Qx' = (g_1, \cdots g_n) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x_{s+1}' \\ \vdots \\ x_n' \end{pmatrix} = x_{s+1}' g_{s+1} + \cdots + x_n' g_n$$

Thus $\ker A$ = the sub-module generated $g_{s+1}, \cdots g_n$

Consider $\operatorname{Im} A \subset R^m$.

$A = PDQ^{-1} \iff AQ = PD = (P_1, \cdots, P_m) \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_s \\ & 0 & \end{pmatrix}$

$= (d_1 P_1, \cdots d_s P_s, 0, \cdots 0)$

So $\operatorname{Im} A$ is the sub module generated by

$d_1 P_1, \cdots, d_s P_s$.

Note that $(P_1, \cdots P_s, P_{s+1}, \cdots P_m)$ is a basis of R^m

Structure theorem for sub-modules of free finite rank modules over PIDs.

Let R be a PID, F a free R-module of rank n, and $N \subset F$ a sub-module.

Theorem

1. *There exist a basis $\{v_1, \ldots, v_n\}$ of F, an integer $0 \leq s \leq n$, and non-zero elements $d_1, \ldots d_s \in R$ with $d_1 | d_2 | \cdots | d_s$, such that $\{d_1 v_1, d_2 v_2, \ldots, d_s v_s\}$ is a basis of N.*
2. *The integer s is unique and the elements $d_1, d_2, \ldots, d_s$ are unique up to associates. Moreover, s and $d_1, d_2, \ldots, d_s$ are independent of the choice of the basis $\{v_1, v_2, \ldots, v_n\}$ of F.*

The integer s is called the rank of N, and the elements $d_1, d_2, \ldots, d_s$ the invariant factors of N.

Corollary. Any sub-module of a free module of n rank over a PID is again free and of rank $r \leq n$.

Prepare for the proof:

Proposition. Let R be a PID, and let F be a free R-module of rank n. Then any sub-module N of F is generated by a subset with no more than n elements.

Induction on n.

Proof. Tutorial.

Remark. Assumption that R is a PID is necessary for proposition.

Proof of Structure theorem for sub-modules of free finite rank modules over PIDs

Let R be a PID, F a free R-module of rank n, $N \subset F$ an R-submodule.

- Let $\{g_1, \ldots, g_s\}$ be a generating set for N of minimum cardinality, where $s \leq n$.
- Let $\{e_1, \ldots, e_n\}$ be a basis of F and write

$$(g_1, \ldots, g_s) = (e_1, \ldots, e_n)A$$

  where $A \in M_{n,s}(R)$.
- Apply the Smith Normal Form Theorem to A:

$$PAQ = \begin{pmatrix} D \\ 0 \end{pmatrix}_{s \times s}$$

  where $P \in GL(n, R)$, $Q \in GL(s, R)$, $D = \mathrm{diag}(d_1, \ldots, d_s)$, and

$$d_1 | d_2 | \cdots | d_s \in R.$$

- Note that $s \geq \mathrm{rank}(A)$.

- Rewrite $PAQ = \begin{pmatrix} D \\ 0 \end{pmatrix}$ as

$$(g_1, \ldots, g_s)Q = (e_1, \ldots, e_n)P^{-1}\begin{pmatrix} D \\ 0 \end{pmatrix},$$

and set

$$(v_1, \ldots, v_n) = (e_1, \ldots, e_n)P^{-1}, \qquad (w_1, \ldots, w_s) = (g_1, \ldots, g_s)Q.$$

.

- One then has $(w_1, \ldots, w_s) = (d_1 v_1, \ldots, d_s v_s)$.
- As Q is invertible, $\{w_1, \ldots, w_s\}$ is a generating set of N.
- Minimality of s implies that $d_j \neq 0$ for any $1 \leq j \leq s$, so $\{w_1, \ldots, w_s\}$ is a linearly independent set.
- Thus $\{w_1, \ldots, w_s\}$ is a basis for N.

- The integer s, being the minimal size of all the generating sets of N, is independent of the choices of the basis $\{v_1, \ldots, v_n\}$ of F.
- Suppose that $\{u_1, \ldots, u_n\}$ is another basis of F and $c_1, \ldots, c_s \in R$ are such that $c_i | c_j$ for $1 \leq i < j \leq s$ and that $\{c_1 u_1, \ldots, c_s u_s\}$ is a basis of N.
- Let $X \in GL(n, R)$ and $Y \in GL(s, R)$ be such that

$$(u_1, \ldots, u_n) = (v_1, \ldots, v_n)X^{-1},$$
$$(c_1 u_1, \ldots, c_s u_s) = (d_1 v_1, \ldots, d_s v_s)Y.$$

Then

$$X \begin{pmatrix} D \\ 0 \end{pmatrix} Y = \begin{pmatrix} C \\ 0 \end{pmatrix}.$$

- By Smith Normal Form Theorem, c_j and d_j are associates for all j.

Q.E.D.