Modules and classification of finitely generated modules over a PID

- Fields $\subset$ vector spaces

  Rings $\subset$ modules (模)

Definition Let R be a ring. A (left) R-module (R-左模) is an abelian group M equipped with an "R-action" on M: $R \times M \longrightarrow M$, satisfying

$$(a, m) \longmapsto a \cdot m$$

(0) $1_R \cdot m = m$

(1) $(r+s) \cdot m = r \cdot m + s \cdot m$

(2) $r \cdot (m+n) = r \cdot m + r \cdot n$

(3) $r \cdot (s \cdot m) = (rs) \cdot m$.

A right R-module is an abelian group N with a right R-action

$$N \times R \longrightarrow N \quad , \text{ satisfying analogues of (0) (1) (2) above,}$$

$$(n, a) \longmapsto n \cdot a$$

and $(3)_R$ $(n \cdot s) \cdot r = n \cdot (sr)$.

Remark: If R is commutative, then there is no difference between left/right R-modules

- A (left) R-submodule (R-左子模) is an abelian subgroup $N \subseteq M$

  s.t. $\forall r \in R$, $r \cdot N \subseteq N$.

Examples: ① If $R = F$ is a field, then F-modules = F-vector spaces.

② If $I \subseteq R$ is a left ideal, then I is a left R-submodule of R (b/c $\forall r \in R$, $r \cdot I \subseteq I$)

Conversely, a left R-submodule of R is a left ideal.

③ A $\mathbb{Z}$-module is just an abelian group G

b/c $\forall n \in \mathbb{Z}_{\geq 0}$, $n \cdot g = \underbrace{g + \cdots + g}_{n} \in G$ & $(-n) \cdot g = -n \cdot g$.

A $\mathbb{Z}$-submodule is an abelian subgroup of G.

④ If M_i $(i \in I)$ are left R-modules, define their

direct product (直积) to be $\prod_{i \in I} M_i = \{ (m_i)_{i \in I} ; m_i \in M_i \}$

$\cup|$

direct sum (直和) to be $\bigoplus_{i \in I} M_i = \{ (m_i)_{i \in I} ; m_i \in M_i,$ all but finitely many m_i is zero $\}$

or $M_1 \oplus M_2$

⑤ $R^{\oplus m} = \underbrace{R \oplus \cdots \oplus R}_{m}$ free R-module of rank m.

⑥ If $S \xrightarrow{\varphi} R$ is a ring homomorphism, the we may naturally view an R-module M as an S-module, by $s \cdot m := \varphi(s) \cdot m$

Definition Let R be a ring and let M and N be left R-modules

① An R-module homomorphism (R-模同态) is an abelian group homomorphism $\phi : M \to N$ satisfying $\forall r \in R, m \in M \Rightarrow r\phi(m) = \phi(r \cdot m)$.

Write $\mathrm{Hom}_R(M, N)$ for the set of such homomorphisms; it is naturally an abelian group.

- When R is commutative, $\mathrm{Hom}_R(M, N)$ is also an R-module

$$(r \cdot \phi)(m) := r \cdot \phi(m) = \phi(r \cdot m).$$ (Think: why need R to be commutative.)

Example: $\{ \mathbb{Z}\text{-module homomorphisms} \} \leftrightarrow \{ \text{abelian group homomorphisms} \}$.

② Say ϕ is an R-module isomorphism (R-模同构) if it is a homomorphism + bijection.

③ If $\phi : M \to N$ is an R-module homomorphism, then

- $\ker \phi = \phi^{-1}(0)$ is the kernel of ϕ
- $\mathrm{Im}\, \phi = \phi(M)$ is the image of ϕ

} both are R-modules

Rmk: ϕ injective $\Leftrightarrow \ker\phi = \{0\}$ or just write $\ker\phi = 0$.

④ If $N \subseteq M$ is an R-submodule, define the quotient R-module (R-商模)

$$M/N := \{m+N \ ; m \in M\}, \qquad r\cdot(m+N) := rm+N.$$

Isomorphism Theorems for R-modules (omit)

Theorem (Jordan-Hölder) Let R be a ring and M an R-module. Assume that we are given two chains of R-submodules $0 = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_m = M$ and $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = N$

Then setting $A'_{ij} := A_{i-1} + (A_i \cap B_j)$ and $B'_{ij} = B_{j-1} + (A_i \cap B_j)$,

we refine the two chains by A'_{ij} and B'_{ij} and that $A'_{ij}/A'_{ij-1} \cong B'_{ij}/B'_{i-1,j}$. □

Definition M a left R-module. $A \subseteq M$ subset.

$$RA := \{r_1a_1 + \cdots + r_na_n \mid n \geq 0, r_1, \cdots, r_n \in R, a_1, \cdots, a_n \in A\}$$

is the submodule of M generated by A

When $A = \{a_1, \cdots, a_n\}$, $RA = \text{Image}\left(\phi : R^{\oplus n} \longrightarrow M,\ (r_1, \cdots, r_n) \longmapsto r_1a_1 + \cdots + r_na_n\right)$

We say a submodule $N \subseteq M$ (possibly $N = M$) is finitely generated (有限生成的) if

$\exists$ finite set $A \subseteq N$ s.t. $N = RA$.

say ——— is cyclic if $\exists\, m \in N$ s.t. $N = Rm = \{rm \mid r \in R\}$

say M is free of rank n (自由的, 秩为 n) if there exists $a_1, \cdots, a_n \in M$

s.t. $\forall\, m \in M$ can be written uniquely as $m = r_1a_1 + \cdots + r_na_n$ with $r_1, \cdots, r_n \in R$

This is equivalent to $R^{\oplus n} \simeq M$

Remark: If M is (finitely generated) by $a_1, \cdots, a_n \in M$, then

we get $\phi: R^{\oplus n} \twoheadrightarrow M$

$$(r_1, \cdots, r_n) \longmapsto r_1 a_1 + \cdots + r_n a_n$$

We are interested in "relations among $a_1, \cdots, a_n$" e.g. $b_{j1} a_1 + \cdots + b_{jn} a_n = 0$ for some $b_{ji} \in R$

or equivalently $\ker \phi$.

To specify an R-module homomorphism $\psi: M \to L$, it is enough to specify $\psi(a_i)$ for each a_i satisfying $b_{j1}\psi(a_1) + \cdots + b_{jn}\psi(a_n) = 0$.

(Nice situation: $\ker \phi$ is also a finitely generated R-modules $\rightsquigarrow$ say M is finitely presented)

i.e. there are essentially finitely many such relations. (有限多现象的)

Key example: Let F be a field, V an F-vector space $\circlearrowleft T$ F-linear operator

Then we define an $F[x]$-module structure on V by

$$(a_0 + a_1 x + \cdots + a_n x^n) \cdot v := a_0 v + a_1 T(v) + a_2 T^2(v) + \cdots + a_n T^n(v)$$

$$\rightsquigarrow \left\{ \begin{array}{l} F\text{-vector space } V \text{ with} \\ \text{an } F\text{-linear operator } T \end{array} \right\} \longleftrightarrow \left\{ F[x]\text{-module } V \right\}$$

Similarly $\{T\text{-stable subspaces } W \subseteq V\} \longleftrightarrow \{F[x]\text{-submodule } W \subseteq V\}$

Remark: V finite F-dimensional $\Rightarrow$ V is a fin. gen $F[x]$-module, But not conversely.

Classification of finitely generated R-modules where R is a PID

Lemma. R integral domain, $M \simeq R^{\oplus n}$. Then any $n+1$ elements in M are linearly dependent,

i.e. $\forall x_1, \cdots, x_{n+1} \in M$, $\exists a_1, \cdots, a_{n+1} \in R$ not all zero, s.t. $a_1 x_1 + \cdots + a_{n+1} x_{n+1} = 0$

Proof: Set $F = \mathrm{Frac}(R)$. It is clear that $\exists a_1', \cdots, a_{n+1}' \in F$ not all zero s.t.

$$a_1' x_1 + \cdots + a_{n+1}' x_{n+1} = 0$$

Multiply this by d = product of denominators of all a_i'. ✓ □

From now on, R is a PID

Theorem 1. Let M be a free R-module of rank n, and N be a submodule of M. Then

(1) N is free of rank n ($n \le m$)

(2) There exists a basis $y_1, \cdots, y_m$ of M so that $a_1 y_1, \cdots, a_n y_n$ is a basis of N and $a_1, \cdots, a_n \in R \setminus \{0\}$ satisfy $a_1 | a_2 | \cdots | a_n$.

Proof: If $N = \{0\}$, the theorem is trivial.

Now assume $N \neq 0$ (First we determine a_1)

(Idea: Say $M \simeq R^{\oplus m}$. Then each $x \in N$ can be written as $(x_1, \cdots, x_m)$

$\rightsquigarrow$ want to find the "minimal possible" $\gcd(x_1, \cdots, x_m)$.)

Fix an isomorphism $M \simeq R^{\oplus m}$ $\rightsquigarrow$ $\pi_i : M \to R$ taking the i^{th} coordinate.

For each homomorphism $\varphi : M \to R$, $\varphi(N)$ is an R-submodule of R, i.e. an ideal of R.

Consider $\{\varphi(N) \mid \varphi \in \mathrm{Hom}_R(M,R)\}$; it contains a maximal possible ideal $(a_1) \subseteq R$

Say for $\varphi_1 \in \mathrm{Hom}_R(M,R)$, $\varphi_1(y) = a_1$ for some $y \in N$

($(a_1) \neq (0)$ b/c $\exists\, x \in N$ with nonzero coordinates $(x_1, \cdots, x_m)$.)

Claim: For any $\varphi' \in \mathrm{Hom}_R(M,R)$, $a_1 | \varphi'(y)$

Pf: otherwise, say $d = \gcd(a_1, \varphi'(y)) = r_1 a_1 + r_2 \varphi'(y) = (r_1 \varphi_1 + r_2 \varphi')(y)$

contradicting with the maximality of (a_1)

In particular, for $\pi_1, \cdots, \pi_m$, $\pi_i(y) = a_1 b_i$ i.e. $y = (a_1 b_1, \cdots, a_1 b_m)$ ← all coordinates are divisible by a_1

$a_1 \cdot \varphi(b_1, \cdots, b_m) = \varphi(a_1 b_1, \cdots, a_1 b_m) = \varphi(y) = a_1$

$\Rightarrow \varphi(\underbrace{b_1, \cdots, b_m}_{y_1}) = 1$

Claim ① $M = Ry_1 \oplus \ker\varphi$

② $N = Ra_1y_1 \oplus (N \cap \ker\varphi)$

Proof: ① $M \xrightarrow{\varphi} R$, y_1 (a section). Such a surjective map admits a section, i.e. $\forall r \in R$, $\varphi(ry_1) = r$.

In this situation, we get $M \simeq R\cdot y_1 \oplus \ker\varphi$

$\forall m \in M$, $m = \underbrace{\varphi(m)\cdot y_1}_{\text{multiple of } y_1} + \underbrace{(m - \varphi(m)y_1)}_{\hookrightarrow \text{belongs to } \ker\varphi}$

$\varphi(m - \varphi(m)y_1) = \varphi(m) - \varphi(m)\underbrace{\varphi(y_1)}_{=1} = 0.$

Yet $Ry_1 \cap \ker\varphi = \{ ry_1, \text{ s.t. } \varphi(ry_1) = 0 \} = 0.$

② $\forall x \in N$, $x = \underbrace{\varphi(x)\cdot y_1}_{\text{in } Ra_1y_1} + \underbrace{(x - \varphi(x)y_1)}_{\hookrightarrow \text{as } \varphi(x)y_1 \in Ra_1y_1 \subseteq N \Rightarrow \text{belongs to } N\cap\ker\varphi}$

$\Rightarrow N = Ra_1y_1 \oplus (N \cap \ker\varphi)$

Thus we are reduced to $N \cap \ker\varphi \subseteq \ker\varphi$.

First prove (1): $N = R\cdot a_1y_1 \oplus \underbrace{(N\cap\ker\varphi)}_{\text{!!}\ N_1} \subseteq M$

Applying the same argument to $N_1 \subseteq M$, ... ← not $\ker\varphi$ (b/c not knowing $\ker\varphi$ is free yet)

Continue this way, by lemma, must stop before the $(m+1)^{th}$ step.

Now, prove (2): Reduce to $N \cap \ker\varphi \subseteq \ker\varphi$ ← free by (1)

By induction, we get $N = R\cdot a_1y_1 \oplus R\cdot a_2y_2 \oplus \cdots \oplus Ra_ny_n$ with $a_2 \mid a_3 \mid \cdots \mid a_n$.

$\cap\!\!|$

$M = Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_m.$

Remains to check $a_1 \mid a_2$. If not, $d = \gcd(a_1, a_2) = a_1r_1 + a_2r_2$

Consider $\varphi' : M \longrightarrow R$

$y_1 \longmapsto r_1$

$y_2 \longmapsto r_2$

$y_i \longmapsto 0$ other i

$\Rightarrow \varphi'(a_1y_1 + a_2y_2) = d$ contradicting the maximality of $\varphi(N)$.

Theorem (Fundamental theorem of modules over a PID)

Let R be a PID and M a finitely generated R-module.

Then $M \simeq R^{\oplus r} \oplus R/(a_1) \oplus \cdots \oplus R/(a_n)$, with $a_1 | a_2 | \cdots | a_n$ $a_i \in R$

Such $r, a_1, \cdots, a_n$ are unique (up to associates)

In particular, M is torsion-free $\Leftrightarrow$ M is free

↳ means $0 \neq m \in M$ and $r \neq 0 \Rightarrow r \cdot m \neq 0$.

Corollary: * Classification of finitely generated abelian groups

* Jordan normal form / rational normal form.

Proof of the theorem As M is finitely generated, $\exists$ a surjective homomorphism

$$\varphi : R^{\oplus m} \twoheadrightarrow M$$

Then $\ker \varphi \leq R^{\oplus m}$ is a submodule.

Apply theorem above $\Rightarrow \exists$ a "new basis" $y_1, \cdots, y_m$ of $R^{\oplus m}$ s.t. $\ker\varphi = \langle a_1 y_1, \cdots, a_n y_n \rangle$

Then $$M = \frac{Ry_1 \oplus \cdots \oplus Ry_m}{Ra_1y_1 \oplus \cdots \oplus Ra_ny_n} \simeq R/(a_1)\cdot y_1 \oplus \cdots \oplus R/(a_n)\cdot y_n \oplus R^{\oplus(m-n)}$$

Now, uniqueness:

- **A different form of the classification theorem.**

Fact: For $a \in R$ (nonzero, nonunit), if it factors as $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ in R (PID $\Rightarrow$ UFD)

then $R/(a) = R/(p_1^{\alpha_1}) \times \cdots \times R/(p_r^{\alpha_r})$ by Chinese remainder theorem.

So any finitely generated R-module M can be written as

$$M \simeq R^{\oplus r} \oplus R/(p_1^{\alpha_{11}}) \oplus \cdots \oplus R/(p_1^{\alpha_{1s_1}}) \oplus R/(p_2^{\alpha_{21}}) \oplus \cdots$$

(Reassembly this back gives $a_1 = p_1^{\max\{\alpha_{11} \cdots \alpha_{1s_1}\}} \cdot p_2^{\max\{\cdots\}} \cdots$

$a_2 = p_1^{2^{\text{nd}}\text{ largest in } \{\alpha_{11} \cdots \alpha_{1s_1}\}} p_2^{\cdots} \cdots$)

Will prove: r, $p_1, p_2, \cdots$, $\{\alpha_{11} \geq \alpha_{12} \geq \cdots \geq \alpha_{1s_1}\}$, $\{\alpha_{21} \geq \cdots \geq \alpha_{2s_2}\}$, $\cdots$ are unique.

Lemma. $p, q \in R$ prime elements $(p) \neq (q)$, $r, s \in \mathbb{N}$

(1) If $M \simeq R$, then $M/p^r M \simeq R/(p^r)$

(2) If $M \simeq R/(p^s)$, then $M/p^r M \simeq R/(p^{\min\{r,s\}})$

(1,2)' If $M \simeq R/(p^s)$ (allowing $s=\infty$), $p^r M/p^{r+1}M = \begin{cases} \text{trivial if } s \geq r \\ R/(p) \text{ otherwise} \end{cases}$

(3) If $M \simeq R/(q^s)$, then $M/p^r M = (0)$

(note: $M/p^r M \simeq R/(p^r, q^s)R = 0$,

as $(p) \neq (q) \Rightarrow 1 \quad 1 = ap + bq \Rightarrow 1 - (ap+bq)^{r+s-1} = p^r * + q^s *$)

Applying this lemma to M, writing $F_i := R/(p_i)$ a field,

$$\left.\begin{aligned} \dim_{F_i}\left(M/p_i M\right) &= r + \#\{\alpha_{ij} \mid j=1,\cdots s_i, \alpha_{ij} \geq 1\} \\ \dim_{F_i}\left(p_i M/p_i^2 M\right) &= r + \#\{\alpha_{ij} \mid j=1,\cdots,s_i, \alpha_{ij} \geq 2\} \\ &\cdots\cdots \end{aligned}\right\} \Rightarrow \text{From this, we determine the numbers } r, \alpha_{ij}.$$