可对角化 $\Leftrightarrow$ minimal polynomial splits and no multiple roots.

不可对角化，如何分类？！ V, W F-linear spaces

首先定义分类：

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "\varphi"'] & V \arrow[d, "\varphi"] \\ W \arrow[r, "S"] & W \end{tikzcd}$$

若存在 φ: $V \cong W$

使得 $S\circ\varphi = \varphi T$，则称 $(V, T) \sim (W, S)$

与 $F[\lambda]$-module 分类的关系：

回顾：$F[\lambda]$-module. V F-linear space

$$F[\lambda] \times V \to V$$
$$(f, v) \mapsto f\cdot g$$

当 $f \in F$ 时 $f\cdot v$ 是原本的 F-linear space 结构

$$(f\cdot g)v = f\cdot(g\cdot v)$$
$$(f+g)v = f\cdot v + g\cdot v$$
$$f(v_1 + v_2) = fv_1 + fv_2$$
$$1\cdot v = v$$

$F[\lambda]$-module 同构

$\varphi: V \longrightarrow W$ 双射

$\varphi(f \cdot v) = f(\varphi(v))$

$\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$

定理: $\{(V, T) \mid V.\ F\text{-linear space}.\ T: V \to V\}$

$\longrightarrow \{F[\lambda]\text{-module } V\}$

$(V, T) \longmapsto F[\lambda] \times V \to V$

$(f(\lambda), v) \longmapsto f(T)(v)$

$\left(V, \begin{array}{l} T: V \to V \\ v \mapsto \lambda \cdot v \end{array}\right) \longleftarrow\!\shortmid\ F[\lambda]\text{-module } V$

是互逆的双射.

且 $(V, T) \sim (W, S)$

当且仅当 $V \cong W$ as $F[\lambda]$-module

如果 $\dim_F V = n < +\infty$，也等价于

$S = \varphi T \varphi^{-1}$，或者取基后 $[S]_C = P \cdot [T]_B P^{-1}$

$P = [\varphi]_B^C$

即：$\{A \in M_n(F)\} \big/ A_1 \underset{\text{相似}}{\sim} A_2$.

更一般的，对环 R，定义 R-module

$$R \times M \to M \quad (r, m) \mapsto r \cdot m$$

$$M \times M \to M \quad (m_1, m_2) \mapsto m_1 + m_2$$

$(M, +, 0, \cdot)$ $\quad 0 + m = m + 0 = m$

$\exists -m$, s.t. $m + (-m) = 0$

$$(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$$

$$(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$$

$$r(m_1 + m_2) = r \cdot m_1 + r \cdot m_2$$

$$1 \cdot m = m.$$

例：$\mathbb{Z}/n\mathbb{Z}$ 是 $\mathbb{Z}$-mod

$F[t]$-module 分类. $F[t]=R$ ring

例子: R 本身. $R\times R\to R$

$R^n=R\times\cdots\times R$. 称为 R 自由模.

子模: M. R-mod. $N\subset M$.

① N 加法封闭

② R-数乘封闭.

例: $I\subset R$, $I=\{f(x)\cdot h(x)\mid h(x)\in F[x]\}$

(记作 $(f(x))$)

则 I 是 R 的子模.

定义 (理想) $I\subset R$ 是 R 的子模.

商模: $N\subset M$, 子模.

$\forall m\in M$, $m+N=\{m+n\mid n\in N\}$

$M/N=\{m+N\mid m\in M\}$

M/N 有 R-模结构, $r\cdot(m+N)=r\cdot m+N$

$(m_1+N)+(m_2+N)=(m_1+m_2)+N$

例: $n\mathbb{Z} \subset \mathbb{Z}$ $\quad$ $\mathbb{Z}$-子模

$\quad \overset{\shortparallel}{\{nk \mid k \in \mathbb{Z}\}}$

$\mathbb{Z}/n\mathbb{Z}$ $\quad$ $\mathbb{Z}$-模.

例: $(V, T \in \mathrm{End}_F(V)) \longrightarrow F[x]\text{-mod } V.$

T 不变子空间 $W \longrightarrow F[x]$-子模

V/W 商空间, $\longrightarrow F[x]$-商模

$\tilde{T}: V/W \to V/W$

例: $f(x) \in F[x]$. $\quad F[x]/(f(x))$ as

$F[x]$-mod.

恢复出 $V = F[x]/(f(x))$ 的 F-线性空间

结构以及 $T: V \to V$

$$v \mapsto x \cdot v$$

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

则 V 有基 $\underbrace{1, x, \cdots, x^{n-1}}$ $\leftarrow B$

(证明用到带余除法)

$$T(1, x, \cdots, x^{n-1}) = (x, x^2, \cdots, x^n)$$

$$= (1, x, \cdots, x^{n-1}) \cdot \begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & \vdots \\ 0 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & & & 1 & -a_{n-1} \end{bmatrix}$$

$$[T]_B^B = \begin{bmatrix} \quad \end{bmatrix} \leftarrow A.$$

T 的特征多项式为??

2种方法：一：直接算 $f_T(x) = \det(\lambda I - A)$

二. 求 T 的极小多项式.

$g(T) = 0 \Leftrightarrow g(x) \cdot 1 = 0$ in $F[x]/(f(x))$

$\Leftrightarrow g(x) \in (f(x))$

$\Leftrightarrow g(x) = h(x) \cdot f(x)$

$\mathrm{Ann}(T) = (f(x)) \Rightarrow$ 极小多项式为 $f(x)$

模同态，R-线性映射

$\varphi: M_1 \to M_2$

$\varphi(m_1+m_2) = \varphi(m_1)+\varphi(m_2)$

$\varphi(r\cdot m) = r\cdot\varphi(m)$

性质：① $\ker\varphi \subset M_1$ 子模

$\operatorname{Im}\varphi \subset M_2$ 子模.

② φ 单 $\Leftrightarrow \ker\varphi = \{0\}$

③ φ 双射 $\Rightarrow \varphi^{-1}$ R-线性

例子：$N \subset M$ 子模

$\pi: M \to M/N$ R-线性. 满.

$m \mapsto m+N$

第一同构定理：

$\varphi: M_1 \to M_2$. 则 $M_1/\ker\varphi \cong \operatorname{Im}\varphi$.

证明：

$$\begin{tikzcd} M_1 \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & M_2 \\ & M_1/\ker\varphi \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}$$

$$\tilde{\varphi}(m+\ker\varphi) = \varphi(m)$$

验证良定，R-线性. 且 $\ker\tilde{\varphi} = 0$.

子模对应定理.

$\varphi: M \to N$ 满，R-线性.

则 $\left\{ L \,\middle|\, \begin{array}{l} L \subset N \\ R\text{-子模} \end{array} \right\} \longrightarrow \left\{ \tilde{L} \,\middle|\, \begin{array}{l} \ker\varphi \subset \tilde{L} \subset M \\ \tilde{L}\ R\text{-子模} \end{array} \right\}$

$$L \longmapsto \varphi^{-1}(L)$$

是一个一一对应，且有 $\tilde{L}/\ker\varphi \cong L$

先了解 $F[t]$ 作为环的基本性质.

Euclidean domain R

$\exists\ s: R-\{0\} \to \mathbb{Z}_{\geq 0}$ s.t.

$\forall f, g \in R,\ g \neq 0$, 有 $q, r \in R$.

$f = g \cdot q + r,\quad r = 0$ or $s(r) < s(g)$

s 称作 size function.

例: $F[x],\ s(f) = \deg f$.

$\mathbb{Z},\ s(n) = |n|$.

主定理: R Euclidean domain, 则

R 上的有限生成 R-mod 有分类.

用于 $F[x]$, 有 $(V, T \in \mathrm{End}_F(V))$ 的分类.

用于 $\mathbb{Z}$, 有 有限 abelian group 的分类.

环的理想

定义 $I \subset R$，满足 ① 加法封闭 ② 乘法吸收. $\underbrace{\text{① 加法封闭 ② 乘法吸收}}_{R\text{ 的 }R\text{-子模}}$

I 中.

例子：上次的 T 的 annilinator.

$\mathrm{Ann}(T) = \{ f(x) \in F[x] \mid f(T) = 0 \}$

$\mathrm{Ann}(T) \subset F[x]$ 是理想.

性质：R 是 Euclidean domain. 则

理想 $I \subset R$，$I = (a) = \{ ab \mid b \in R \}$

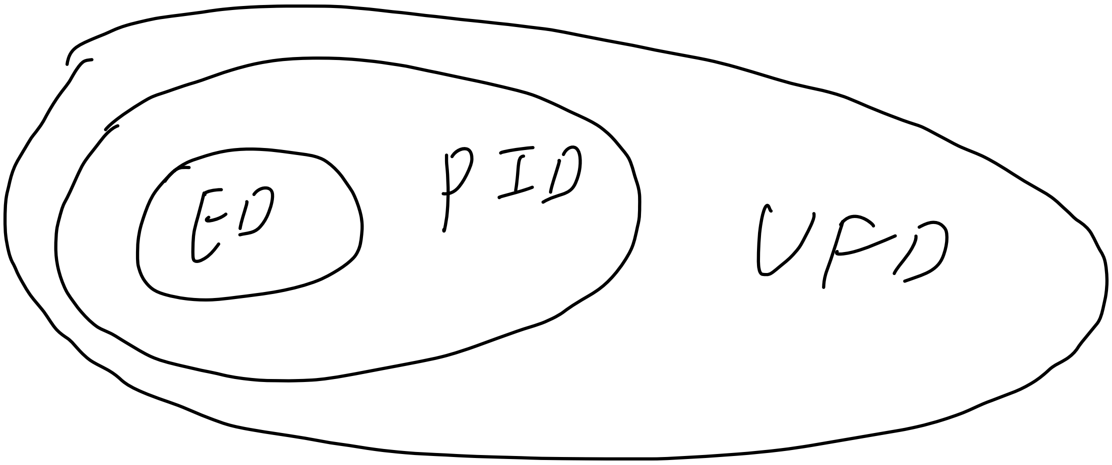
证明：若 $I \neq 0$，找 I 中 size 最小的非零元 a，则 $I = (a)$

上次一样 · · · · · · · · · · · □

定义：(PID) 主理想整环 R.

理想 $I \subset R$ 均为 $I = (a) = \{ab \mid b \in R\}$

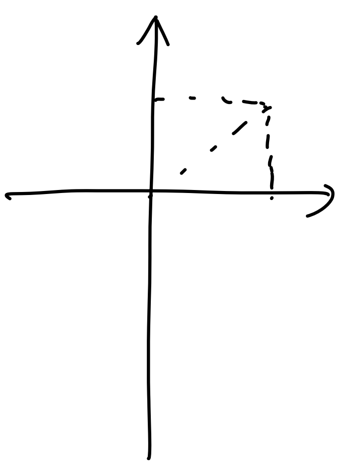
$\square$

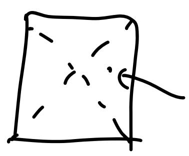


主定理对 PID 也对.

更多例子：ED：$\mathbb{Z}[\sqrt{-1}] = \{a+b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$

$$\delta(a+b\sqrt{-1}) = \sqrt{a^2+b^2}$$





正方形上任一点到顶点的最短距离 < 边长

$\mathbb{Z}[w]$ $\quad w = \frac{1+\sqrt{-3}}{2}$

定义：有限生成模.

有限生成模的子模仍然有限生成吗？？

不一定. $R=F[x_1,x_2 \dots x_n \dots]$

$(x_1, x_2 \dots x_n \dots) = I \subset R$

I 不是有限生成的.

引入条件：Noetherian.

定义：R 的理想作为 R-模有限生成

推论：任意有限生成的 R-模的子模有限生成.

考虑 M 的生成元组 $m_1, m_2, \dots m_n$, 则有

R-线性满射 $R^n \to M$

性质：$\varphi: M \to N$ 满射，$\ker\varphi = L$，则

① M 有限生成 $\Rightarrow$ N 有限生成.

② L，N 有限生成 $\Rightarrow$ M 有限生成

证明：① $R^n \to M \xrightarrow{\varphi} N$

满射的复合仍然是满射

② 取 L 的生成元 $l_1, l_2 \cdots l_k$

取 N 的生成元 $n_1, n_2 \cdots n_s$

则 $n_1 \cdots n_s$ 有原像 $m_1 \cdots m_s$.

Claim：$l_1, l_2 \cdots l_k, m_1 \cdots m_s$ 生成 M.

$\forall\ m \in M$，$\varphi(m) = \sum_{i=1}^{s} r_i n_i$

则 $\varphi(m - \sum_{i=1}^{s} r_i m_i) \in \ker\varphi$

$\Rightarrow m - \sum_{i=1}^{s} r_i m_i \in \mathrm{Span}_R(l_1 \cdots l_k)$

$\square$

回到 $\varphi: R^n \to M$ 满，R-线性.

$N \subset M$ 子模. R Noetherian $\Rightarrow N$ 有限生成

证明：$\tilde{N} = \varphi^{-1}(N) \subset R^n$. 只用证 $\tilde{N}$ 有限生成.

对 n 归纳.

$\tilde{N} \subset R^n$. 拆成

$$f: R^n \to R^{n-1}, \quad \ker f \cong R.$$

则有 $f|_{\tilde{N}}: \tilde{N} \to f(\tilde{N})$ 满，

$$\ker(f|_{\tilde{N}}) = \tilde{N} \cap \ker f \subseteq R \text{ 的子模}$$

Noether　　　　　　归纳假设 $n-1$

所以 $\tilde{N} \cap \ker f$ 有限生成，$f(\tilde{N})$ 有限生成

$\Rightarrow \tilde{N}$ 有限生成.　　　　　□.

更多的，R 主理想环，$\tilde{N}$ 生成元个数可取得小于等于 n.

R Noetherian.

M 有限生成. $\varphi: R^n \to M$ 满射.

$\ker\varphi$ 也有限生成: $f: R^m \to R^n$.

$\mathrm{Im} f = \ker\varphi$.

$M \cong R^n / \mathrm{Im} f$. 也称为 $\mathrm{coker} f$.

R^n 生成元, R^m 表达了生成元之间的 R-线性关系.

研究 $f \in \mathrm{Hom}_R(R^m, R^n)$ 即可.

取 R^n 的一组基 $e_1, \dots, e_n$. C

R^m 的一组基 $v_1, \dots, v_m$. B

则 $[f]_B^C = ([f(v_1)]_C, \dots, [f(v_m)]_C) \in M_{n\times m}(R)$.

若 $C' = C \cdot P$. $B' = B \cdot Q$.

则 $[f]_{C'}^{B'} = P^{-1} [f]_B^C \cdot Q$

R PID or Euclidean domain.

对 $A \in M_{n\times m}(R)$ 作行列变换.

定理: R PID. 则 $\exists\ P \in GL_n(R)$.
$Q \in GL_m(R)$, s.t. $P^{-1}AQ = \begin{bmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_l & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}$

且 $d_1 \mid d_2 \mid d_3 \mid \cdots \mid d_l$

$\left(d_i \mid d_{i+1} \iff \exists\ r_i,\ \text{s.t.}\ d_{i+1} = r_i \cdot d_i. \right)$

且 (d_i) 由 A 唯一确定.

(称为 Smith 标准型, d_i 称为不变因子)

推论: R PID, M 有限生成 R-模, 则
M 同构于循环模的直和.

证明: $M \cong R^n / \operatorname{Im} f$

$\cong \bigoplus_{i=1}^{l} R/(d_i) \oplus R^{n-l}$

$\square$

用在 $(V, T\in \mathrm{End}_F(V))$ $\dim V<+\infty$ 上.

则 $l=n$. 否则 $\dim_F V \geq \dim_F F[x]=+\infty$.

$d_1,\dots,d_r$ 也称为 T 的不变因子.

性质: d_r 是 T 的极小多项式.

$T_i: V_i \to V_i$, 极小多项式 m_i.

证明: 用引理: $T=T_1\oplus T_2: V_1\oplus V_2 \to V_1\oplus V_2$

的极小多项式 $m(x)$. 有

$$(m)=(m_1)\cap(m_2).$$

(或者 $m=\mathrm{l.c.m}(m_1,m_2)$)

引理证明: 代入 $\mathrm{Ann}(T)$ 的定义 $\square$.

$\boxed{\text{重新证明 } d_r \text{ splits, separated} \Rightarrow T \text{ 可对角化.}}$

推论: $A_1, A_2\in M_n(F)$ 相似, 当且仅当

A_1, A_2 对应的不变因子相同.

(极小多项式是其中一个不变量).

主定理

证明：存在性：

先证

R Euclidean domain 的情形.

$$A=(a_{ij})\in M_{n\times m}(R)$$

Step 1: Switch row or column, s.t.

$$s(a_{11})=\min_{i,j}\{s(a_{ij})\mid a_{ij}\neq 0\}$$

$a_{11}\mid a_{1i}$ eliminate a_{1i}

Step 2: $a_{11}\nmid a_{1i}$ $i>1$

$$a_{1i}=q a_{11}+r, \quad s(r)<s(a_{11})$$

$$A'=A\cdot\begin{bmatrix} 1 & \cdots 0 \cdots 0 & -q & 0 & 0 \\ & 1 \ddots & 0 & & 0 \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}=\begin{bmatrix} a_{11} & \cdots & r & \\ a_{21} & & \vdots & \cdots \\ \vdots & & \vdots & \\ a_{n1} & & \vdots & \end{bmatrix}$$

$$A'=(a'_{ij}) \quad \min\{s(a'_{ij})\mid a'_{ij}\neq 0\}$$

$$<s(a_{11})$$

finite steps

$$\begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & & & \\ \vdots & & * & \\ a_{n1} & & & \end{bmatrix}$$

Similarly
row reduction

$$\begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & X & \\ 0 & & & \end{bmatrix} = A$$

Step 3: If $a_{11} \nmid x_{ij}$,

$$\begin{bmatrix} 1 & & 1 & \\ & \ddots & & \\ & & & 1 \end{bmatrix} \cdot A = \begin{bmatrix} a_{11} & x_{i2} & x_{i3} & \cdots & x_{ij} & \cdots & x_{in} \\ 0 & & & & & & \\ \vdots & & & X & & & \\ 0 & & & & & & \end{bmatrix}$$

repeat step 2 strictly descrease

$$\min \{ s(a_{ij}) \mid a_{ij} \neq 0 \}$$

After finitely many steps

$$A = \begin{pmatrix} a_{11} & 0 \cdots 0 \\ 0 & \\ \vdots & X \\ 0 & \end{pmatrix}$$

$$\underline{a_{11} \mid x_{ij}}$$

By induction $\Rightarrow$ $A = \left[\begin{array}{ccc|c} d_1 & & & \\ & d_2 & & 0 \\ & & \ddots & \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right]$

$$d_1 \mid d_2 \mid \cdots \mid d_r$$

In general $R = PID$

Step 1: Switching rows or columns.

s.t. $a_{11} \neq 0$

If $\underline{a_{11} \nmid a_{1i}}$. $i \geq 2$. (a_{1i}) is not a proper subset of (a_{11})

Choose $(d) = (a_{11}, a_{1i})$

$mk + nl = 1$

$d = k a_{11} + l a_{1i}$ $k, l \in R.$

$a_{11} = m d,$ $m, n \in R$

$a_{1i} = n d$

$$\underbrace{A \cdot \begin{array}{c} \\ \\ \\ \text{i-th row} \rightarrow \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{cccccc} & & & \overset{\text{i-th column}}{\downarrow} & & \end{array} \\ \begin{bmatrix} k & & & -n & & \\ 0 & 1 & & & & \\ \vdots & & \ddots & & & \\ 0 & & & 1 & & \\ l & & & m & & \\ 0 & & & & 1 & \\ \vdots & & & & & \ddots \\ 0 & & & & & & 1 \end{bmatrix}\end{array}}_{\text{Invertible}} = \begin{bmatrix} d & \cdots \\ \vdots & \ddots \\ \vdots & & \ddots \\ \vdots & & & \ddots \end{bmatrix} =$$

$$A = \begin{pmatrix} \underline{a_{11}} & & \underline{a_{1i}} \\ & & \\ & & \end{pmatrix}$$

$(d) \supsetneq a_{11},$ $A' = (a'_{ij})$

$(a'_{11}) \supsetneq (a_{11})$

If $a_{11} \mid a_{1i}$, $\underline{\text{eliminate}}$ a_{1i}

repeat $(a_{11}) \subsetneq (a_{11}') \subsetneq (a_{11}'') \cdots$

ascending chain of principal ideals

terminates after finite steps

$$\Rightarrow A \longrightarrow \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & X & \\ 0 & & & \end{bmatrix}$$

$a_{11} \nmid x_{ij}$

Similarly

$$\begin{bmatrix} a_{11} & x_{i2} & \cdots & x_{ij} & \cdots \\ 0 & & & & \\ \vdots & & X & & \\ 0 & & & & \end{bmatrix}$$

ascending chain of principal ideals

$$A \to \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & X & \\ 0 & & & \end{bmatrix} \quad a_{11} \mid x_{ij}$$

Induction $\Rightarrow$ $A \to \left[\begin{array}{ccc|ccc} d_1 & & & & & \\ & \ddots & & & 0 & \\ & & d_2 & & & \\ \hline & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{array}\right]$

$\boxed{\text{唯一性证明稍后.}}$

Ex: $\underline{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}}$ $\left\langle m_1, m_2 \,\middle|\, \begin{array}{l} 2m_1 = 0 \\ 3m_2 = 0 \end{array} \right\rangle$

$$\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \to \begin{bmatrix} 2 & 3 \\ 0 & 3 \end{bmatrix}$$

$$\to \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix} \to \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 \\ 3 & -6 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & -6 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$$

$$(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$
$$\cong \mathbb{Z}/6\mathbb{Z}$$

R-module M_1, M_2

Direct sum. $M_1 \oplus M_2 = (M_1 \times M_2,$
(外直和)

$r \cdot (m_1, m_2) = (r m_1, r m_2))$

R-module homomorphism.

$$\begin{tikzcd} M_1 \arrow[r, "f_1"] & N \\ M_2 \arrow[ur, "f_2"'] & \end{tikzcd}$$

$$\begin{tikzcd} M_1 \arrow[r, "i_1"', "\text{injective}"] & M_1 \oplus M_2 \arrow[r, "\exists! f"] & N \\ M_2 \arrow[ur, "i_2", "\text{injective}"'] & & \end{tikzcd}$$

s.t. $f_1 = f \circ i_1$

$f_2 = f \circ i_2$

$f(m_1, m_2) = f_1(m_1) + f_2(m_2)$

universal property

内直和. $M_1 \subset M$, $M_2 \subset M$ submodules

(Defn) ① M_1, M_2 generates M.

$\forall\, m \in M$, $m = m_1 + m_2$

$m_i \in M_i$

② $M_1 \cap M_2 = \{0\}$

$\Rightarrow \forall\ m = m_1 + m_2$

m_1, m_2 determined by m.

$m = m_1 + m_2 = m_1' + m_2'$

$\underline{m_1 - m_1'} = \underline{m_2' - m_2} \in M_1 \cap M_2$

$M_1 \to M, \quad M_2 \to M$ R-homomorphism

$\underline{M_1 \oplus M_2} \xrightarrow{f} \underline{M}.$

① f surjective

② f injective

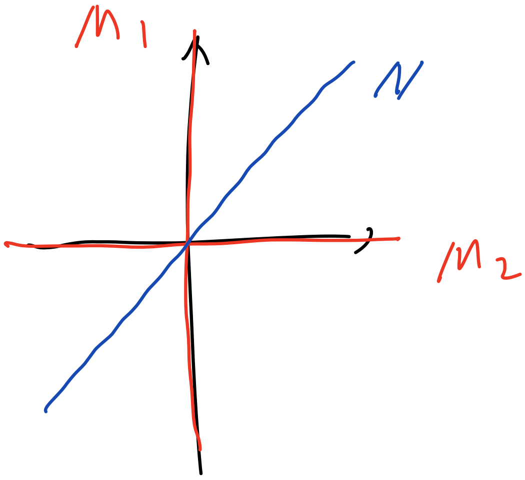
$\Rightarrow$ $\underline{f \text{ isomorphism}}$

$$\boxed{M \cong M_1 \oplus M_2}$$

容易犯错： $\underline{M_1 \oplus M_2 = M}$

$N \subset M$ submodule

$\underline{(M_1 \oplus M_2) \cap N \neq (M_1 \cap N) \oplus (M_2 \cap N)}$



$N_1 \subset M_1$, $\quad N_2 \subset M_2$.

$N_1 \oplus N_2 \subset M_1 \oplus M_2$, $\quad M_1 \oplus M_2 / N_1 \oplus N_2$

$$= (M_1 / N_1) \oplus (M_2 / N_2)$$

例子： $R=\mathbb{Z}$. M f.g. R-module.

M "$+, 0, -$", $\Rightarrow$ 唯一确定 $r\cdot m$

$r = \underbrace{1+1+\cdots+1}_{r个}$, $r\cdot m = \underbrace{m+\cdots+m}_{r个}$

可验证如此定义的 $r\cdot m$ 满足结合，分配律.

$\Rightarrow$ M. "$+, 0, -$" Abelian group 阿贝尔群.

均为 $\mathbb{Z}$-模

有限生成阿贝尔群： $\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$

$\mathbb{Z}$ 的理想均为 (n). ($\mathbb{Q}$ 不是)

此时循环模 $\mathbb{Z}/I$, $I=(0), (n)\cdots$

也称为循环群.

$$\underbrace{M \cong \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_r \oplus (\mathbb{Z})^{n-r}}$$

如何由 M 的 $\mathbb{Z}$-模结构恢复出 $d_1, \cdots, d_r$.
$n-r$.

不断利用子模，商模的构造.

首先 $\mathbb{Z}/d\mathbb{Z}$ 是否可再分解.

例:

$$\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$n+6\mathbb{Z} \mapsto (n+3\mathbb{Z},\ n+2\mathbb{Z})$$

$d = d_1 d_2$. $\quad g.c.d.(d_1, d_2) = 1$.

$\mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ 单、满

一般的 均有 中国剩余定理:

$d = p_1^{a_1} \cdots p_s^{a_s}$ $\quad p_j$ 互不相同的素数.

$$\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1} \oplus \cdots \oplus \mathbb{Z}/p_s^{a_s}$$

$$\begin{cases} d_r = p_1^{a_1^r} \cdots\cdots p_s^{a_s^r} \\ d_{r-1} = p_1^{a_1^{r-1}} \cdots p_s^{a_s^{r-1}} \\ \vdots \\ d_1 \cdots - \quad - \end{cases}$$

p_j 素数.

$a_j^{i+1} \geq a_j^i \geqslant 0$

引入 Torsion. $\overset{\text{Torsion}}{\cdot}$free 来分类

Torsion :

$$\{ m \in M \mid \exists\, a \in \mathbb{Z},\ a \neq 0,\ a \cdot m = 0 \}$$

$$\mathrm{Ann}(m) = \{ a \in \mathbb{Z} \mid a \cdot m = 0 \}$$

$$M_{tor} = \{ m \in M \mid m \text{ torsion} \}$$

验证 M_{tor} 是 submodule.

$a_1 m_1 = 0$, $a_2 m_2 = 0 \Rightarrow \underline{a_1 a_2 (m_1 + m_2) = 0}$

$a \cdot m = 0 \Rightarrow a \cdot (b \cdot m) = 0$

$$\left(M \cong \underbrace{\bigoplus \mathbb{Z}/d_i\mathbb{Z}}_{M_{tor}} \quad \underbrace{\oplus\ \mathbb{Z}^{n-r}} \right)$$

性质: $M = \underbrace{\left(\bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}\right)} \oplus \mathbb{Z}^{n-r}$

则 $M_{tor} = \bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$

如何确定 $n-r$ ($\mathbb{Z}^{n-r}$ 不能作为 M 的子集被唯一确定).

$M/M_{tor} \cong \mathbb{Z}^{n-r}$

有用的构造: $I \subset R$ ideal, 则

$IM = \{\sum_{i\,有限} a_i m_i \mid a_i \in I,\ m_i \in M\}$

是 M 的子模.

M/IM 有自然的 R/I-module 结构.

$r \cdot \bar{m} = \overline{rm}$ (验证 well-defined)

$I(M_1 \oplus M_2) = (IM_1) \oplus (IM_2)$

$(M_1 \oplus M_2)/I(M_1 \oplus M_2) = (M_1/IM_1) \oplus (M_2/IM_2)$

R/I -module isomorphism.

Cor: $\mathbb{Z}^n \cong \mathbb{Z}^m$, then $n=m$.

pf: p prime number. $I = (p)$.

$\underline{R^n/IR^n} \cong R^m/IR^m$ as R/I-modules

as R/I-vector spaces

$||$

$\underline{(R/I)^n}$ $\dim = n = m$

$R^n = ((R \oplus R) \oplus R) \oplus R \cdots$

Ex: $\underline{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}}$ $\quad \langle m_1, m_2 \mid 2m_1 = 0,\ 3m_2 = 0 \rangle$

$$\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \to \begin{bmatrix} 2 & 3 \\ 0 & 3 \end{bmatrix}$$

$$\to \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix} \to \begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 \\ 3 & -6 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & -6 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$$

$$(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$
$$\cong \mathbb{Z}/6\mathbb{Z}$$

In general $\quad R = PID$

R domain $\Rightarrow$ M_{tor} is a submodule

$m_1 + m_2$, $\quad r_1 m_1 = 0$, $r_2 m_2 = 0$ $\quad r_i \neq 0$

$r_1 r_2 \neq 0$, $(r_1 r_2)(m_1 + m_2) = 0$.

$$M = \underbrace{R/(d_1) \oplus \cdots \oplus R/(d_r)}_{M_1} \oplus \underbrace{R^k}_{M_2}$$

$m = m_1 + m_2$. $\quad m_i \in M_i$

$m \in M_{tor}$

$r \neq 0$, $r \cdot m = 0 \Rightarrow r \cdot m_1 = 0$

$r \cdot m_2 = 0$

$\Rightarrow m_2 = 0 \quad (R^k = R \oplus \cdots \oplus R)$

$M_{tor} \subset M_1$

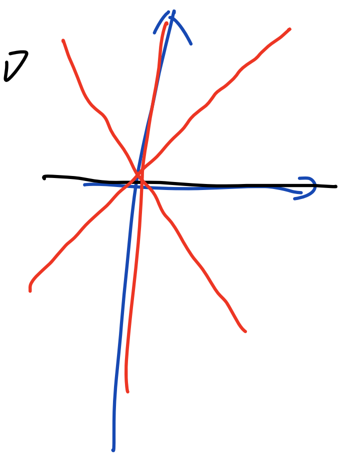
$\forall m_1$, $d_r \cdot m_1 = 0 \Rightarrow M_1 \subset M_{tor}$

$$\Rightarrow \quad M_{tor} = M_1$$

$$\Rightarrow \quad R^k \cong M / M_{tor}$$

k is determined by M.

$$\begin{tikzcd} 0 \arrow[r] & \underbrace{M_{tor}} \arrow[r] & M \arrow[r] & R^k \arrow[r] \arrow[l, bend left] & 0 \end{tikzcd}$$



Ex: $$M = \underbrace{\mathbb{Z}/2\mathbb{Z}}_{M_1} \oplus \underbrace{\mathbb{Z}}_{M_2}$$

$$M_2' = \langle (\bar{1}, 1) \rangle$$

$$= \{ (n \cdot \bar{1}, n) \mid n \in \mathbb{Z} \}$$

$M_2' \cong \mathbb{Z}$. $\quad \underline{M_2' \neq M_2}$

$$M = M_1 \oplus M_2'$$

How to determine

$$M_{tor} \cong R/(d_1) \oplus R/(d_2) \cdots \oplus R/(d_r)$$

$$d_1 \mid d_2 \cdots \mid d_r$$

$$\boxed{(d_1) \neq R}$$

$d_1 \cdots d_r$ are uniquely determined by M. (M_{tor})

Defn: M generated by one element. call M a cyclic R-module

$$R \to M \to 0$$

$$M \cong R/I.$$

Prop:

R PID, Assume $M \cong R/(d)$

$\underline{d \neq 0}$, $d = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$

$n_i \geq 1$. p_i prime element

$(p_1) \cdots (p_k)$ distinct. ($p_1 \cdots p_k$ are not associates to each other)

$$R/(d) \cong R/(p_1^{n_1}) \oplus R/(p_2^{n_2}) \cdots \oplus R/(p_k^{n_k})$$

pf: Recall chinese remainder Thm:

R ring, I, J ideals. $I + J = R$

① $IJ = I \cap J$.

② $R/I \cap J \cong R/I \times R/J$

$$\begin{aligned} R &\to R/I \times R/J \\ r &\mapsto (\bar{r}, \bar{\bar{r}}) \end{aligned}$$

Apply CRT: $I = (p_1^{n_1})$,

$J = (p_2^{n_2} \cdots p_k^{n_k})$

$I + J = (q)$. $\underset{\sim}{q} = g.c.d(\underline{p_1^{n_1}}, \underline{p_2^{n_2} \cdots p_k^{n_k}})$

$q = 1$, or $I + J = R$

$I \cap J = (d)$

ring iso

$\Rightarrow R/(d) \cong R/(p_1^{n_1}) \times R/(p_2^{n_2} \cdots p_k^{n_k})$

$\cong R/(p_1^{n_1}) \oplus R/(p_2^{n_2} \cdots p_k^{n_k})$

R-module isom

induction $= R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_k^{n_k})$

Back to $\underset{\sim}{M} \cong R/(d_1) \oplus \cdots \oplus R/(d_r)$

$d_r = p_1^{n_{1r}} p_2^{n_{2r}} \cdots p_k^{n_{kr}}$ $n_{ir} \geq 1$

$d_{r-1} = p_1^{n_{1(r-1)}} p_2^{n_{2(r-1)}} \cdots p_k^{n_{k(r-1)}}$ $p_1 \cdots p_k$ prime

$n_{ir} \geq n_{i(r-1)} \geq 0$

$\vdots$

$$d_1 = p_1^{n_{11}} p_2^{n_{21}} \cdots p_k^{n_{k1}}$$

$$\begin{array}{l} n_{ir} \geq n_{i(r-1)} \geq n_{i(r-2)} \cdots \geq n_{i1} \geq 0 \\ \ \ \mathbin{\rotatebox[origin=c]{90}{$\geq$}} \\ \ \ 1 \end{array}$$

不变因子.

$d_1 \cdots d_r$ are called invariant factors of M

$p_i^{n_{ij}}$ $\quad n_{ij} \geq 1$ $\quad \cdots$ elementary divisors of M

计重数 $\qquad$ 初等因子.

Prop: Elementary divisors determine the corresponding invariant factors.

$$M \cong R/(p_1^{n_{1r}}) \oplus R/(p_1^{n_{1(r-1)}}) \oplus \cdots$$
$$\oplus R/(p_2^{n_{2r}}) \oplus R/(p_2^{n_{2(r-1)}}) \cdots$$

$\cdots$

$\oplus R/(p_k^{n_{kr}}) \oplus \cdots$

n_{ij} are determined by M.

Defn (p-torsion part) p prime element of R

$M(p) = p$-torsion submodule

$= \{ m \in M \mid \exists n \in \mathbb{Z}_{\geq 1},\ p^n \cdot m = 0 \}$

$M(p)$ is a submodule. $m_1, m_2 \in M(p)$

$p^{n_1} m_1 = 0$. $p^{n_2} \cdot m_2 = 0$

$p^{n_1+n_2}(m_1+m_2) = 0 \Rightarrow m_1+m_2 \in M(p)$

$p^{n_1}(rm_1) = r \cdot (p^{n_1} \cdot m_1) = 0 \Rightarrow r \cdot m_1 \in M(p)$

Prop: In the decomposition above.

$M \cong M(p_1) \oplus M(p_2) \cdots \oplus M(p_k)$

Pf: If $m = m_1 + m_2 + \cdots + m_k \in M(p_1)$

$m_i \in \underline{R/(p_i^{n_{ir}})} \oplus \cdots \oplus \underline{R/(p_i^{n_{i1}})}$

$p_1^n \cdot m = 0, \Rightarrow p_1^n \cdot m_i = 0$

<u>If $i \geq 2$</u>, $p_1^n \cdot (m_{ir} + m_{ir-1} + \cdots + m_{i1})_{=0}$

$m_{ij} \in R/(p_i^{n_{ij}})$

$p_1^n \cdot m_{ij} = 0, \Rightarrow m_{ij} = \overline{r_{ij}} \in R/(p_i^{n_{ij}})$

$r_{ij} \in R$

$p_1^n \cdot r_{ij} \in (p_i^{n_{ij}})$

$\underline{p_1^n} r_{ij} = \underline{p_i^{n_{ij}}} \cdot r$

$\Rightarrow p_i^{n_{ij}} \mid r_{ij}$

$\Rightarrow m_{ij} = 0$

$$M = M_{(p)} \cong R/(p^{n_1}) \oplus \cdots \oplus R/(p^{n_r})$$

$$n_1 \geq n_2 \cdots \geq n_r \geq 1$$

Ex: $\mathbb{Z}$-module. $M \cong \mathbb{Z}/(p^2) \oplus \mathbb{Z}/(p) \oplus \mathbb{Z}/(p)$

p can kill this part.

Defn: p prime element

$$M[p] = \{ m \in M \mid p \cdot m = 0 \}$$

submodule

In the example: $\mathbb{Z}/(p^2) \oplus \mathbb{Z}/(p) \oplus \mathbb{Z}/(p)$

$$m = m_1 + m_2 + m_3$$

$p m_1 = 0$, $p m_2 = 0$, $p m_3 = 0$

$m_1 = \overline{r_1} \in \mathbb{Z}/(p^2)$. $r_1 \in \mathbb{Z}$

$p m_1 = 0 \iff p r_1 \in (p^2)$

$p^2 \mid p \cdot r_1 \iff p \mid r_1$

$\mathbb{Z}/(p^2)[p] \cong \underline{\mathbb{Z}/p\mathbb{Z}}$

$M[p] \cong \underline{(\mathbb{Z}/p\mathbb{Z})^3}$

$M[p]$ has $\mathbb{Z}/p\mathbb{Z}$ - module. structure

In general. $\underline{M[p]}$ has a $R/(p)$-module structure

Define

$\forall m \in M[p]$, $\overline{r} \cdot m = rm$ (well-defined)

R PID. $R/(p)$ field

$\underline{\dim_{R/(p)} M[p]}$ is determined by M.

$$M = R/(p^{n_1}) \oplus R/(p^{n_2}) \cdots \oplus R/(p^{n_r})$$

$$n_1 \geq n_2 \cdots \geq n_r \geq 1$$

Prop: $M[p] \cong \underbrace{R/(p) \oplus \cdots \oplus R/(p)}_{r \text{ copies}}$

$$\left(\underline{R/(p^n)}^{\,n \geq 1} [p] \cong R/(p) \right)$$

Cor: $\dim_{\underset{\sim}{R/(p)}} M[p] = r$ (r is the number of n_i s.t. $n_i \geq 1$)

$$IM = \left\{ \sum r_i m_i \,\middle|\, r_i \in I,\ m_i \in M \right\}$$

$(p)M = pM$ submodule of M.

In $M = \mathbb{Z}/(p^2) \oplus \mathbb{Z}/(p) \oplus \mathbb{Z}/(p)$

$pM \cong \mathbb{Z}/(p)$

In general, $p \in R$. prime

$\dim_{R/(p)} (pM)[p]$ = number of n_i s.t. $n_i \geq 2$.

$\dim_{R/(p)} (p^2M)[p]$ . . . . $n_i \geq 3$.

$r \in R$

multiplication by r

$0 \to M[r] \to M \xrightarrow{r\cdot} M$

$\ker(r\cdot) = M[r]$

$\operatorname{Im}(r\cdot) = rM$

$R/(p) \cong (p^{k-1})/(p^k) \to R/(p^k) \xrightarrow{p} pR/(p^k) \subset R/(p^k)$

$$\begin{gathered} \| \\ R/(p^{k-1}) \end{gathered}$$

$$0 \to R/(p) \to R/(p^k) \to R/(p^{k-1}) \to 0$$

No isomorphism $R/(p^k) \not\cong R/(p) \oplus R/(p^{k-1})$

Defn: M torsion-free $M_{tor} = 0$

Cor: M f.g. R PID.

M torsion free $\iff$ M free.

$R = \mathbb{Z}$ $\qquad$ $R = F[t]$ F field

$R = \mathbb{Z}$. Structure Thm for f.g. abelian groups

Thm: M f.g. abelian group

M is the direct sum of cyclic groups. $C_{d_1} \oplus C_{d_2} \cdots \oplus C_{d_r} \oplus \mathbb{Z}^l$

$2 \le d_1 \mid d_2 \cdots \mid d_r$. $l \ge 0$

$d_1 \ldots d_r$, l determined by M.

M finite. $M_{(p)}$ p-sylow subgroup of M.

$\underline{R = F[t]}$ V F-vector space. $T: V \to V$ linear

$(V, T) \sim (V', T')$ equivalent

iff $\exists f$ F-isomorphism.

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "T"'] & V' \arrow[d, "T'"] \\ V \arrow[r, "f"] & V' \end{tikzcd}$$

$T'(f(v)) = f(T(v))$

Prop: T has matrix $[T]_B$ under basis B of V

$\dim_F V$ finite

T' $\quad [T]_{B'} \cdots \cdot B'$ of V'

$(V,T) \sim (V',T')$ iff $\exists P \in GL(n,F)$

s.t. $P[T]_B P^{-1} = [T']_{B'}$

Pf: If $(V,T) \sim (V',T')$

$f(B)$ is a basis for V'

$[T]_B = [T']_{f(B)}$ is similar

to $[T']_{B'}$

If $[T]_B$ is similar to $[T']_{B'}$

Define $f: V \to V'$ by matrix P.

under basis B, B' $\quad [f]_B^{B'} = P$

Prop: (V,T) defines a $F[t]$-module structure on V. $t \cdot v = T(v)$

$$p(t) \cdot v = (p(T))(v)$$

$(V,T) \sim (V',T')$ is equivalent to

V is isomorphic to V' as $F[t]$-module

相似类

Cor: $\dim V = n$ $\{$ similar classes in $M_n(F)$ $\}$

$\longleftrightarrow$ $\{ \dim_F V = n$, $F[t]$-module isomorphism classes $\}$.

$T: V \to V$ $\dim V = n$. $B = (v_1, \ldots, v_n)$ basis of V

$$T(v_1, \cdots, v_n) = (T(v_1), \cdots, T(v_n))$$

$$= (v_1 \cdots v_n) \cdot [T]_B$$

$[T]_B = (a_{ij})$ $\quad a_{ij} \in F$

$v_1 \cdots v_n$ generate V as F-module

$F[t]$-module.

$$\ker f \xrightarrow{g} (F[t])^n \xrightarrow{f} V \to 0$$

$$?? = (F[t])^n$$

$$t \cdot (v_1 \cdots v_n) = (v_1 \cdots v_n) \cdot A$$

$$t \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = A^T \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

$$(tI - A^T) \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\begin{cases} (t-a_{11})\cdot v_1 - a_{21}v_2 - a_{31}v_3 - \cdots - a_{n1}v_n = 0 \\ -a_{12}v_1 + (t-a_{22})v_2 \cdots\cdots - a_{n2}v_n = 0 \\ \vdots \end{cases}$$

$F[t]$. row. column reduction

$$\underbrace{(tI - A^T)}_{(tI-A)} \sim \begin{bmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}$$

$d_1 \mid d_2 \cdots \mid d_r \in F[t]$

$$\Rightarrow V \cong F[t]/(d_1) \oplus \cdots \oplus F[t]/(d_r) \oplus \underbrace{(F[t])^{n-r}}_{\dim_F = +\infty}$$

$\Rightarrow n = r$

$$\begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{bmatrix}$$

$d_1 \mid d_2 \cdots \mid d_n$

d_i monic

d_i invariant factors of $T: V \to V$

---- elementary divisor

t

$F[t]/(d_i)$, $d_i = t^k + a_{k-1} t^{k-1} + \cdots + a_0$

has F-basis. $(1, t, t^2, \ldots, t^{k-1})$

$\quad\quad v_1 \quad v_2 \quad \cdots \quad v_k$

$$t \cdot (v_1 \cdots v_k) = (v_1 \cdots v_k) \cdot \begin{bmatrix} 0 & 0 & & -a_0 \\ 1 & 0 & & -a_1 \\ 0 & 1 & & \vdots \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 1 & -a_{k-1} \end{bmatrix}.$$

有理标准型.