

Chapter 6

主理想整环上的模

定义 6.1 主理想整环(PID): 每个理想均由一个元素生成的整环.

例 6.1: $\mathbb{Z}, \mathbb{C}[x]$ 为 PID. □

PID 必诺特.

\mathbb{R} 为整环, $a, b, r, s \in R$,

(1)

定义 6.2 整除: 若 $\exists x \in R$, s.t. $s = xr$, 则称 r 整除 s , 记作 $r \mid s$.

(2)

定义 6.3 单位: R 中的可逆元.

例 6.2: \mathbb{Z} 中, 1 和 -1 为单位.

若 F 为域, 则 $F^* \equiv F - \{0\}$ 中的元素均为单位. □

(3)

定义 6.4 素元: $0 \neq q \in R$, 若 $p \mid ab \implies p \mid a$ 或 $p \mid b$, 则称 p 为素元.

(4)

定义 6.5 不可约元: $0 \neq r \in R$, 若 $r = ab \implies a$ 或 b 为单位, 则称 r 为不可约元.

(5)

定义 6.6 互素: a 与 b 无非单位公因子, 则称 a 与 b 互素.

注意:

- 单位必素, 必不可约.

证: 设 $0 \neq r \in R$ 为单位, 则必 $\exists a$ 的逆 a^{-1} .

若 $r \mid ab$, 则 $\because (ar^{-1})r = a, (br^{-1})r = b, \therefore r$ 为素元.

若 $r = ab$, 则 $\because (r^{-1}a)b = r^{-1}(ab) = r^{-1}r = 1$, 即 b 可逆, 逆元为 $r^{-1}a$, $\therefore r$ 为不可约元. \square

- 整环中, 素元不可约, 反之未必.

证: 设 $p \neq 0$ 为素元且 $p = ab$.

显然 $p \mid ab$, 又 $\because p$ 为素元, $\therefore p \mid a$ 或 $p \mid b$.

不妨 $p \mid a$, 则 $\exists x \in R$, s.t. $a = px$

$\implies p = ab = pxb \implies p(1 - xb) = 0$.

$\because p \neq 0$ 且 R 为整环 (即 R 无零因子), $\therefore 1 - xb = 0 \implies xb = 1 \implies b$ 为单位, 故 p 为不可约元. \square

例 6.3: (不可约元非素的例子) $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ 为整环.

$9 = 3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, 其中 3 不可约 (证略), $3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$, 但 $3 \nmid (2 + \sqrt{-5}), 3 \nmid (2 - \sqrt{-5}) \implies 3$ 非素. \square

- 非整环中, 素元未必不可约.

例 6.4: $(\mathbb{Z}_6, +, \cdot)$ 非整环, $[2]$ 为素元, 但 $[2] = [2][4]$, $[2]$ 和 $[4]$ 均非单位 $\implies [2]$ 可约. \square

定理 6.1 (课本定理0.29): R 为 PID, $a, b \in R$, 则 a 与 b 互素 $\iff \exists r, t \in R$, s.t. $ra + tb = 1$.

证: “ \implies ”: 令 R 的理想 $I = \langle a, b \rangle$.

$\because R$ 是主理想, $\therefore I$ 可由一个元素生成, 设 $I = \langle c \rangle$, 其中 $c \in R$.

又 $\because a \in I, b \in I, \therefore c \mid a, c \mid b \implies c$ 为 a 和 b 的公因子,

$\because a, b$ 互素, $\therefore c$ 为单位, 即 $\exists c^{-1} \in R$, s.t. $1 = c^{-1}c \in I$.

$\because 1 \in I, \therefore 1 = ra + tb$.

“ \Leftarrow ”: 取 c 为 a 和 b 的公因子, $a = cx, b = cy$.

$\because 1 = ra + tb = rcx + tcy = c(rx + ty), \therefore c \mid 1 \implies c$ 可逆, 即 c 为单位. \square

有算法可以在给定 a, b 下找到 s, t , 此处不赘述.

定理 6.2 (课本定理0.29): R 是 PID, $\forall 0 \neq r \in R, r = up_1 \cdots p_n$ 且该分解式唯一, 其中 u 为单位, p_i 是 R 中的不可约元, $n \in \mathbb{Z}^+$.

证: $\forall 0 \neq r \in R$, 首先分解出 r 中的可逆因子, $r = ur'$, 其中 u 为单元, $r' = u^{-1}r$ 非单元.

若 r' 不可约, 则得证;

若 r' 可约, 则 $r' = r_1 r_2$, 其中 r_1, r_2 均非单位.

若 r_1, r_2 均不可约, 则得证;

否则不妨 r_2 可约, 则 $r_2 = r_3 r_4$.

重复如上分解操作, 可得 $r' = r_1 r_2 = r_1 (r_3 r_4) = (r_1 r_3)(r_5 r_6) = (r_1 r_3 r_5)(r_7 r_8) = \cdots$,

同时得到升链 $\langle r' \rangle \subseteq \langle r_2 \rangle \subseteq \langle r_4 \rangle \subseteq \cdots$.

又 $\because R$ 为 PID, $\therefore R$ 诺特 \implies 上述升链有限长, 即上述分解式中不可约元个数有限, 故最终得 $r = u^{-1}p_1 \cdots p_n$.

下证上述分解唯一: 假设 r' 有两个不可约元分解式 $r' = p_1 \cdots p_n$ 和 $r' = q_1 \cdots q_m$.

首先消去相同的不可约元, 留下 $p_i \neq q_j \forall i, j$, 等式两边不可能均为非单位的不同不可约元的乘积, 故必消得 $1 =$

1. \square

定义 6.7 挠元(Torsion): $M \in R - \text{mod}$, $v \in M$, 若 $\exists 0 \neq r \in R$, s.t. $rv = 0$, 则称 v 为 M 的挠元.

定义 6.8 挠模: 所有元素均为挠元的模.

定义 6.9 无挠: 若一模无非零挠元, 则称该模无挠.

与线性无关类似, 若 $0 \neq v \in M$, $r \in R$, $rv = 0$, 且 M 无挠, 则 $r = 0$.

定义 6.10 挠子模: $M_{\text{tor}} = \{v \in M \mid v \text{ 为挠元}\}.$

$\because 0$ 为 M 的挠元, $0 \in M_{\text{tor}}$, $\therefore M_{\text{tor}} \neq \emptyset$.

若 R 交换, 则 M_{tor} 为 M 的子模.

证: $\forall u, v \in M_{\text{tor}}$, $\exists 0 \neq r_1, r_2 \in R$, s.t. $r_1 u = 0$, $r_2 v = 0$.

$\forall s, t \in R$, $(r_1 r_2)(su + tv) = r_2 s(r_1 u) + r_1 t(r_2 v) = r_2 s \cdot 0 + r_1 t \cdot 0 = 0 + 0 = 0$ 且 $r_1 r_2 \neq 0 \implies (su + tv) \in M_{\text{tor}}$, 故得证. \square

$\frac{M}{M_{\text{tor}}}$ 无挠.

证: 假设 $[0] \neq [v] \in \frac{M}{M_{\text{tor}}}$ 为挠元, 则 $\exists 0 \neq r \in R$, $r[v] = [rv] = [0] = M_{\text{tor}} \implies rv \in M_{\text{tor}} \implies v \in M_{\text{tor}} \implies [v] = M_{\text{tor}} = [0]$, 与假设矛盾, 故假设错误, 得证. \square

定义 6.11 零化子: $v \in M \in R - \text{mod}$, v 的零化子 $\text{ann}(v) \equiv \{r \in R \mid rv = 0\} \subseteq R$.

N 是 M 的子模, 则 $\text{ann}(N) = \{r \in R \mid rN \equiv \{rv \mid v \in N\} = \{0\}\} \subseteq R$.

$\text{ann}(v)$ 是 R 的理想.

证: $\forall s, t \in \text{ann}(v)$, $sv = tv = 0 \implies sv - tv = (s - t)v = 0 \implies s - t \in \text{ann}(v)$.

$\forall r \in R$, $(rs)v = r(sv) = r \cdot 0 = 0 \implies rs \in \text{ann}(v)$.

综上, 得证. \square

同理, $\text{ann}(N)$ 也是 R 的理想

定义 6.12 阶: 若 R 为 PID, 则 $\text{ann}(v), \text{ann}(N)$ 均为主理想, 其生成元分别称为 v 和 N 的阶.

定理 6.3 (课本定理6.5): R 为 PID, $M \in R - \text{mod}$ 自由, 则 M 的子模均自由.

证: (不严谨的证明, 仅针对 M 有限生成 (的特殊情况) 且自由.

设 $M = \langle \langle v_1, \dots, v_n \rangle \rangle = \{\sum_{i=1}^n r_i v_i \mid r_i \in R\}$, 其中 $\{v_1, \dots, v_n\}$ 线性无关.

$\forall v \in M$, $v = \sum_{i=1}^n r_i v_i$ 展开唯一, 定序后, $M \longleftrightarrow R^n$, $v \longleftrightarrow \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$ 模同构.

设 S 是 R^n 的子模, 取 R 的理想 $I_k = \{r_k \in R \mid \exists a_1, \dots, a_{k-1} \in R, \text{ s.t. } (a_1, \dots, a_{k-1}, r_k, 0, \dots, 0) \in S\}$.

$\because R$ 为 PID, $\therefore I_k$ 由一个元素生成, 设 $I_k = \langle r_k \rangle$, 其中 $r_k \neq 0, k = 1, \dots, n$.

取 $u_k = (a_1^k, \dots, a_{k-1}^k, r_k, 0, \dots, 0) \in S, S = \langle u_1, \dots, u_n \rangle$ (下证) 且显然 $\{u_1, \dots, u_n\}$ 线性无关.

取 $(b_1, \dots, b_n) \in S$, 若 $b_n \neq 0$, 则 $b_n \in I_n = \langle r_n \rangle \implies \exists x_n \in R, \text{ s.t. } b_n = x_n r_n \implies (b_1, \dots, b_n) - x_n b_n = (\dots, 0)$, 重复如上操作, 最终可将 (b_1, \dots, b_n) 用 $\{u_1, \dots, u_n\}$ 表示.

故得证. \square

定理 6.4 (课本定理6.6): R 为 PID, $M \in R - \text{mod}$ 有限生成, 则 M 自由 $\iff M$ 无挠.

证: “ \implies ”: 设 $M = \langle \langle v_1, \dots, v_n \rangle \rangle$ 且 $\{v_1, \dots, v_n\}$ 线性无关.

$\forall v \in V, v = \sum_{i=1}^n r_i v_i$.

若 $rv = 0$, 则 $r(\sum_{i=1}^n r_i v_i) = \sum_{i=1}^n (rr_i) v_i = 0$.

$\because \{v_1, \dots, v_n\}$ 线性无关, $\therefore rr_1 = \dots = rr_n = 0$.

$\because R$ 为整环 (无零因子), \therefore 若 $r \neq 0$, 则 $r_1 = \dots = r_n = 0 \implies v = 0$, 故 M 无挠.

“ \impliedby ”: 设 $M = \langle \langle u_1, \dots, u_m \rangle \rangle$.

不妨设 u_1, \dots, u_k 是其中最大的线性无关组, 即 $\forall i = k+1, \dots, m, \{u_1, \dots, u_k, u_i\}$ 线性相关

$\implies \exists$ 不全为零的 $a_{i1}, \dots, a_{ik}, a_i$, s.t. $a_{i1}u_1 + \dots + a_{ik}u_k + a_i u_i = 0$.

显然 $a_i \neq 0$ (否则 $a_{i1}u_1 + \dots + a_{ik}u_k = 0 \implies a_{i1} = \dots = a_{ik} = 0$, 矛盾) $\implies a_i u_i = -(a_{i1}u_1 + \dots + a_{ik}u_k)$.

令 $a = a_{k+1} \dots a_m$.

$\because R$ 为整环 (无零因子), $\therefore a \neq 0$,

$aM = \langle \langle au_1, \dots, au_k, au_{k+1}, \dots, au_m \rangle \rangle \subseteq \langle \langle u_1, \dots, u_k \rangle \rangle$,

$\because \{u_1, \dots, u_k\}$ 线性无关, $\therefore \langle \langle u_1, \dots, u_k \rangle \rangle$ 是自由模.

$\because R$ 为 PID, 自由具有遗传性, $\therefore aM$ 自由.

构造映射 $\tau: M \rightarrow aM, v \mapsto av$.

(1) τ 线性.

(2) $\because M$ 无挠且 $a \neq 0, \therefore \ker \tau = \{v \in M \mid av = 0\} = \{0\}$, 即 τ 单射.

(3) τ 满射.

故 τ 同构 $\implies M$ 也自由.

综上, 得证. \square

$\because M$ 自由, $\therefore M = \langle \langle v_1, \dots, v_n \rangle \rangle$ 且 $\{v_1, \dots, v_n\}$ 线性无关 $\implies \langle \langle v_i \rangle \rangle \cap \langle \langle v_j \rangle \rangle = \{0\} \forall i \neq j$

$\implies M = \langle \langle v_1 \rangle \rangle \oplus \dots \oplus \langle \langle v_n \rangle \rangle$.

定理 6.5 (课本定理6.8): R 是 PID, $M \in R - \text{mod}$ 有限生成, 则 $M = M_{\text{free}} \oplus M_{\text{tor}}$, 其中 $M_{\text{free}} \approx \frac{M}{M_{\text{tor}}}$.

证: M_{tor} 为挠子模且 $\frac{M}{M_{\text{tor}}}$ 无挠.

$\because \Pi: M \rightarrow \frac{M}{M_{\text{tor}}}, u \mapsto [u]$ 满同态且 M 有限生成, 由引理 6.1 得 $\frac{M}{M_{\text{tor}}}$ 有限生成.

又 $\because \frac{M}{M_{\text{tor}}}$ 无挠, $\therefore \frac{M}{M_{\text{tor}}}$ 自由.

取 $\frac{M}{M_{\text{tor}}} = \langle \langle [u_1], \dots, [u_t] \rangle \rangle$, 其中 $\{[u_1], \dots, [u_t]\}$ 线性无关. 下证 $\{u_1, \dots, u_t\}$ 线性无关:

证: 若 $\sum_{i=1}^t r_i u_i = 0$, 则 $\Pi\left(\sum_{i=1}^t r_i u_i\right) = \sum_{i=1}^t r_i \Pi(u_i) = \sum_{i=1}^t r_i [u_i] = [0]$.

又 $\because \{[u_1], \dots, [u_t]\}$ 线性无关, $\therefore r_1 = \dots = r_t = 0 \implies \{u_1, \dots, u_t\}$ 线性无关. \square

故 $\langle\langle u_1, \dots, u_t \rangle\rangle$ 为自由模, 记作 M_{free} .

确定了 M_{free} 和 M_{tor} 后, 下面来证 $M = M_{\text{free}} \oplus M_{\text{tor}}$:

$$\forall v \in M, \Pi(v) = [v] \in \frac{M}{M_{\text{tor}}} = \langle\langle [u_1], \dots, [u_t] \rangle\rangle \implies \Pi(v) = [v] = \sum_{i=1}^t l_i [u_i].$$

$$\text{令 } u = \sum_{i=1}^t l_i u_i \in M_{\text{free}}, \text{ 则 } \Pi(u) = \Pi\left(\sum_{i=1}^t l_i u_i\right) = \sum_{i=1}^t l_i \Pi(u_i) = \sum_{i=1}^t l_i [u_i] = \Pi(v).$$

$$\Pi(v - u) = \Pi(v) - \Pi(u) = [0] \implies v - u \in \ker \Pi = M_{\text{tor}}.$$

$$\text{于是 } v = u + (v - u), \text{ 其中 } u \in M_{\text{free}}, v - u \in M_{\text{tor}} \implies M = M_{\text{free}} + M_{\text{tor}}.$$

$$\text{取 } w \in M_{\text{free}} \cap M_{\text{tor}}, \text{ 则 } w \in M_{\text{free}} \iff w = \sum_{i=1}^t \alpha_i u_i,$$

$$\text{且 } w \in M_{\text{tor}} \iff \Pi(w) = 0$$

$$\implies 0 = \Pi(w) = \Pi\left(\sum_{i=1}^t \alpha_i u_i\right) = \sum_{i=1}^t \alpha_i \Pi(u_i) \implies \alpha_1 = \dots = \alpha_t = 0 \implies w = 0 \implies M_{\text{free}} \cap M_{\text{tor}} = \{0\}.$$

综上, 得证. □

引理 6.1: $\tau: M \rightarrow N$ 满同态, 若 M 有限生成, 则 N 有限生成.

证: $\because \tau: M \rightarrow N$ 满同态, $\therefore \forall w \in N, \exists u \in M, \text{ s.t. } w = \tau(u)$,

$$\text{又 } \because M \text{ 有限生成, 设 } M = \langle\langle v_1, \dots, v_k \rangle\rangle, \therefore u = \sum_{i=1}^k r_i u_i \implies \tau(u) = \tau\left(\sum_{i=1}^k r_i u_i\right) = \sum_{i=1}^k r_i \tau(u_i),$$

故 $N = \langle\langle \tau(u_1), \dots, \tau(u_k) \rangle\rangle$, 即 N 有限生成. □

至此, $M_{\text{free}} = \langle\langle u_1, \dots, u_t \rangle\rangle = \langle\langle u_1 \rangle\rangle \oplus \dots \oplus \langle\langle u_t \rangle\rangle$ 已拆解到位. 那么能否以及如何继续拆解 M_{tor} 呢?

定理 6.6 (课本定理6.10): R 为 PID, $M \in R - \text{mod}$ 为挠模且 $\text{ann}(M) = \langle\langle \mu \rangle\rangle$, 其中 $\mu = up_1^{e_1} \dots p_m^{e_m}$, u 为单位, p_i 均不可约且互不相等, $e_i \in \mathbb{Z}^+$,

则 $M = M_{p_1} \oplus \dots \oplus M_{p_m}$, 其中 $M_{p_i} = \{v \in M \mid p_i^{e_i} v = 0\}$ 是阶为 $p_i^{e_i}$ (即 $\text{ann}(M_{p_i}) = \langle p_i^{e_i} \rangle$) 的准素子模.

证: 不失一般性, 设 $\mu = pq$, 其中 p 与 q 互素, 要证 $M = M_p \oplus M_q$, 其中 $M_p = \{v \mid pv = 0\}$, $M_q = \{v \mid qv = 0\}$.

$$\because p \text{ 与 } q \text{ 互素}, \therefore \exists r, t \in R, \text{ s.t. } rp + tq = 1.$$

$$\forall v \in M, v = 1v = (rp + tq)v = (rp)v + (tq)v,$$

$$q(rp)v = (qrp)v = (rpq)v = r(pq)v = r\mu v.$$

$$\text{又 } \because \langle\langle \mu \rangle\rangle \text{ 为零化子}, \therefore q(rpv) = r\mu v = 0 \implies rpv \in M_q,$$

同理, $tqv \in M_p$, 故 $M = M_p + M_q$.

$$\text{若 } v \in M_p \cap M_q, \text{ 则 } v \in M_p \iff pv = 0,$$

$$\text{且 } v \in M_q \iff qv = 0$$

$$\implies v = 1v = (rp + tq)v = rpv + tqv = r \cdot 0 + t \cdot 0 = 0 + 0 = 0 \implies M_p = M_q = \{0\}.$$

$$\because M_p = \{v \mid pv = 0\}, \therefore \text{ann}(M_p) = \langle p \rangle, \text{ 易推广得 } M_{p_i} = \langle p_i^{e_i} \rangle.$$

综上, 得证. □

然后准素子模能否及如何进一步分解呢?

定理 6.7 (课本定理6.11): R 为 PID, $M \in R - \text{mod}$ 有限生成且为挠模, $\text{ann}(M) = \langle p^e \rangle$, 其中 p 不可约, $e \in \mathbb{Z}^+$,

则 $M = \langle\langle v_1 \rangle\rangle \oplus \dots \oplus \langle\langle v_n \rangle\rangle$, 其中 $\text{ann}(v_i) = \langle p^{e_i} \rangle$, 且 $e = e_1 \geq \dots \geq e_n$.

证: (存在性证明) 不失一般性, 只需证 M 由两个元素生成时, 定理成立, 即可由数学归纳法推广到一般情况.

$$\text{设 } M = \langle\langle u_1, u_2 \rangle\rangle \text{ 且 } u_1, u_2 \neq 0, \text{ann}(M) = \{r \in R \mid rM = \{0\}\} = \langle p^e \rangle.$$

$$\because u_1 \in M, \therefore p^e u_1 = 0 \implies p^e \in \text{ann}(u_1),$$

同理, $p^e \in \text{ann}(u_2)$.

若 $\text{ann}(u_1) = \langle b_1 \rangle$, 则 $\because p$ 不可约, $\therefore b_1 \mid p^e \implies b_1 = p^{l_1}, l_1 \leq e$,

同理, 若 $\text{ann}(u_2) = \langle b_2 \rangle$, 则 $b_2 = p^{l_2}, l_2 \leq e$.

假设 $l_1 < e, l_2 < e$, 令 $l = \max\{l_1, l_2\}$, 则 $p^e \nmid p^l$ 且 $p^l \in \text{ann}(M)$, 与 $\text{ann}(M) = \langle p^e \rangle$ 矛盾, 故假设错误, l_1, l_2 中至少有一个 $= e$.

不妨设 $l_1 = e$ 即 $\text{ann}(u_1) = \langle p^e \rangle$.

$M = \langle \langle u_1, u_2 \rangle \rangle \implies M = \langle \langle u_1 \rangle \rangle + \langle \langle u_2 \rangle \rangle$,

若 $\langle \langle u_1 \rangle \rangle \cap \langle \langle u_2 \rangle \rangle = \{0\}$, 则 $M = \langle \langle u_1 \rangle \rangle \oplus \langle \langle u_2 \rangle \rangle$, 得证.

若 $\langle \langle u_1 \rangle \rangle \cap \langle \langle u_2 \rangle \rangle \neq \{0\}$, 则 $\exists 0 \neq r \in R$, s.t. $ru_2 \in \langle \langle u_1 \rangle \rangle$.

取 R 的理想 $J = \{r \in R \mid ru_2 \in \langle \langle u_1 \rangle \rangle\}$.

$\because R$ 为 PID, $\therefore J$ 由一个元素生成, 设 $J = \langle \langle t \rangle \rangle$.

$\because p^e u_2 = 0, \therefore p^e \in J \implies t \mid p^e$.

又 $\because p$ 不可约, $\therefore t = p^{e_2}$, 其中 $e_2 \leq e$.

又 $\because J = \{r \in R \mid ru_2 \in \langle \langle u_1 \rangle \rangle\} = \langle \langle t \rangle \rangle, \therefore p^{e_2} u_2 \in \langle \langle u_1 \rangle \rangle$, 即 $\exists \alpha \in R$, s.t. $p^{e_2} u_2 - \alpha u_1 = 0$

$\implies p^{e-e_2}(p^{e_2} u_2 - \alpha u_1) = 0 \implies p^e u_2 - p^{e-e_2} \alpha u_1 = 0$.

又 $\because p^e u_2 = 0, \therefore p^{e-e_2} \alpha u_1 = 0 \implies p^{e-e_2} \alpha \in \text{ann}(u_1)$.

又 $\because \text{ann}(u_1) = \langle p^e \rangle, \therefore p^e \mid p^{e-e_2} \alpha \implies p^{e_2} \mid \alpha \implies \exists \beta \in R$, s.t. $\alpha = \beta p^{e_2}$,

回代到 $p^{e_2} u_2 - \alpha u_1 = 0$ 得 $p^{e_2} u_2 - p^{e_2} \beta u_1 = 0 \implies p^{e_2}(u_2 - \beta u_1) = 0$.

令 $w = u_2 - \beta u_1$, 则 $M = \langle \langle u_1, w \rangle \rangle$, 且 $\langle \langle u_1 \rangle \rangle \cap \langle \langle w \rangle \rangle = \{0\}$ (下证),

证: 设 $v \in \langle \langle u_1 \rangle \rangle \cap \langle \langle w \rangle \rangle$, 则 $v \in \langle \langle u_1 \rangle \rangle$,

且 $v \in \langle \langle w \rangle \rangle \implies \exists r \in R, v = rw$

$\implies v = rw = ru_2 - r\beta u_1 \in \langle \langle u_1 \rangle \rangle$.

$\because r\beta u_1 \in \langle \langle u_1 \rangle \rangle, \therefore ru_2 \in \langle \langle u_1 \rangle \rangle \implies r \in J \implies \exists r_1$, s.t. $r = tr_1 = p^{e_2} r_1$,

回代得 $v = rw = p^{e_2} r_1 u_2 - p^{e_2} r_1 \beta u_1 = r_1 p^{e_2} u_2 - r_1 (\beta p^{e_2}) u_1 = r_1 (p^{e_2} u_2 - \alpha u_1) = r_1 \cdot 0 = 0 \implies \langle \langle u_1 \rangle \rangle \cap \langle \langle w \rangle \rangle = \{0\}$. □

故 $M = \langle \langle u_1 \rangle \rangle \oplus \langle \langle w \rangle \rangle$, 其中 u_1 的阶为 p^{e_1} , w 的阶为 p^{e_2} , $e_2 \leq e_1 = e$. □

总结定理 6.5, 6.6 和 6.7, 可得:

定理 6.8 (课本定理6.12): R 为 PID, $M \in R - \text{mod}$ 有限生成,

则 $M = M_{\text{free}} \oplus M_{\text{tor}}$, 其中 $M_{\text{free}} \approx \frac{M}{M_{\text{tor}}}$.

若 $\text{ann}(M_{\text{tor}}) = \langle \mu \rangle$, 其中 $\mu = up_1^{e_1} \cdots p_n^{e_n}$, u 为单位, p_i 不可约且互不相等, $e_i \in \mathbb{Z}^+$,

则 $M_{\text{tor}} = M_{p_1} \oplus \cdots \oplus M_{p_n}$, 其中 $M_{p_i} = \{v \in M_{\text{tor}} \mid p_i(v) = 0\}$ 即 $\text{ann}(M_{p_i}) = \langle p_i^{e_i} \rangle$,

$M_{p_i} = \langle \langle v_{i1} \rangle \rangle \oplus \cdots \oplus \langle \langle v_{it_i} \rangle \rangle$, 其中 $\text{ann}(v_{ij}) = \langle p_i^{e_{ij}} \rangle$, $e_i = e_{i1} \geq \cdots \geq e_{it_i}$.

$$\text{故 } M = \overbrace{\left(\bigoplus_{i=1}^m \langle \langle u_i \rangle \rangle \right)}^{M_{\text{free}}} \oplus \overbrace{\left[\bigoplus_{i=1}^n \left(\bigoplus_{j=1}^{t_i} \langle \langle v_{ij} \rangle \rangle \right) \right]}^{M_{\text{tor}}}.$$

由定理 6.7, $M_{\text{tor}} = \bigoplus_{ij} \langle v_{ij} \rangle$, 其中 $\text{ann}(v_{ij}) = \langle p_i^{e_{ij}} \rangle$, $e_{i1} \geq \cdots \geq e_{it_i}$. 这里,

$$\begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1t_1} \\ v_{21} & v_{22} & \cdots & v_{2t_2} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nt_n} \end{pmatrix}$$

生成了 M_{tor} , 其阶为

定义 6.13 初等因子: M 的初等因子:

$$\begin{pmatrix} p_1^{e_{11}} & p_1^{e_{12}} & \cdots & p_1^{e_{1t_1}} \\ p_2^{e_{21}} & p_2^{e_{22}} & \cdots & p_2^{e_{2t_2}} \\ \vdots & \vdots & \ddots & \vdots \\ p_n^{e_{n1}} & p_n^{e_{n2}} & \cdots & p_n^{e_{nt_n}} \end{pmatrix}.$$

此外, 还定义了

定义 6.14 不变因子: M 的不变因子:

$$\begin{aligned} q_1 &= \prod_i p_i^{e_{1i}}, \\ q_2 &= \prod_i p_i^{e_{2i}}, \\ &\vdots, \\ q_t &= \prod_i p_i^{e_{ti}}. \end{aligned}$$