

Chapter 4

模 I: 基本性质

定义 4.1 模: R 为有单位元交换环, $(M, +)$ 为交换群, 数乘: $R \times M \rightarrow M, (r, m) \mapsto rm$ 满足

$$(1) (r + t)m = rm + tm$$

$$(2) (rt)m = r(tm)$$

$$(3) r(m_1 + m_2) = rm_1 + rm_2$$

$$(4) 1m = m$$

则称 M 为 R 上的模, 记作 $R - \text{mod} \equiv \{R \text{ 上的模}\}$.

\therefore 域是一种特殊的环, \therefore 向量空间是一种特殊的模.

$$0m = 0.$$

证: $0m + 0m = (0 + 0)m = 0m \implies 0m = 0.$ □

$$r0 = 0.$$

证: $r0 + r0 = r(0 + 0) = r0 \implies r0 = 0.$ □

$$(-r)m = r(-m) = -(rm).$$

证: $(-r)m + rm = (-r + r)m = 0m = 0 \implies (-r)m = -rm.$

$r(-m) + rm = r(m + (-m)) = r0 = 0 \implies r(-m) = -rm.$ □

$\forall r \in R$, 可构造映射 $\bar{r} : M \rightarrow M, m \mapsto rm$. \bar{r} 是 M 上的群同态, 又称自同态, 记作 $\bar{r} \in \text{End}(M) \equiv \{M \text{ 上的自同态}\}$, $\text{End}(M)$ 关于同态的加法、复合成环, 其单位元为 M 上的恒等映射, 1_M , 故还可构造映射 $\phi : R \rightarrow \text{End}(M), r \mapsto \bar{r}$.

证: $\bar{r}(m + n) = r(m + n) = rm + rn = \bar{r}(m) + \bar{r}(n)$, 即映射 \bar{r} 下保持运算结构, 故得证. □

例 4.1: 在交换群 $(G, +)$ 上定义 $1a = a, 2a = a + a, \dots, na = \overbrace{a + \dots + a}^{n \text{ 个 } a \text{ 相加}}, -a = -1a, -2a = (-a) + (-a),$
 $-na = \overbrace{(-a) + \dots + (-a)}^{n \text{ 个 } (-a) \text{ 相加}},$ 数乘 $\alpha : \mathbb{Z} \times G \rightarrow G, (n, a) \mapsto na$, 满足

(1) α 是映射

4. 模 I: 基本性质

$$(2) (n+m)a = na + ma$$

$$(3) (nm)a = n(ma)$$

$$(4) n(a+b) = na + nb$$

证: (1) na 的定义依赖于 G 中的运算, 而运算的本质是卡氏积至原集合的映射, 有唯一的结果, 故得证.

$$(2) (n+m)a = \overbrace{a+\cdots+a}^{(n+m)\text{个}a\text{相加}} = \overbrace{a+\cdots+a}^{n\text{个}a\text{相加}} + \overbrace{a+\cdots+a}^{m\text{个}a\text{相加}} = na + ma.$$

$$(3) (nm)a = \overbrace{a+\cdots+a}^{nm\text{个}a\text{相加}} = \overbrace{\overbrace{a+\cdots+a}^{m\text{个}a\text{相加}} + \cdots + \overbrace{a+\cdots+a}^{m\text{个}a\text{相加}}}^{n\text{组}} = \overbrace{ma+\cdots+ma}^{n\text{个}ma\text{相加}} = n(ma).$$

$$(4) n(a+b) = \overbrace{(a+b)+\cdots+(a+b)}^{n\text{个}(a+b)\text{相加}} = \overbrace{a+\cdots+a}^{n\text{个}a\text{相加}} + \overbrace{b+\cdots+b}^{n\text{个}b\text{相加}} = na + nb.$$

(5) 由定义显然. □

故 $M \in \mathbb{Z} - \text{mod}$. □

例 4.2: \forall 交换群 $(G, +)$, $G \in \mathbb{Z} - \text{mod}$. □

例 4.3: $R \in R - \text{mod}$, 其中的数乘即 R 中的乘法. □

例 4.4: $\mathbb{Z}_p = \frac{\mathbb{Z}}{p} = \{[0], \cdots, [p-1]\}$, $(\mathbb{Z}_p, +)$ 是交换群, 故 $\mathbb{Z}_p \in \mathbb{Z} - \text{mod}$.

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}, n[k] = \overbrace{[k]+\cdots+[k]}^{n\text{个}[k]\text{相加}} = [nk],$$

注意到 $[2] \neq [0]$, $3 \neq 0$, 但 $3[2] = [6] = [0]$, 即非零元素的卡氏积在数乘映射下得到零元素, 这意味着非零的单个元素不再线性无关.

实际上, \mathbb{Z}_p 中无线性无关元素. □

例 4.5: $R^n = \{(r_1, \cdots, r_n) \mid r_i \in R\} \in R - \text{mod}$, 其中 $(r_1, \cdots, r_n) + (l_1, \cdots, l_n) = (r_1 + l_1, \cdots, r_n + l_n)$, $r(r_1, \cdots, r_n) = (rr_1, \cdots, rr_n)$. □

定义 4.2 子模: $\emptyset \neq S \subseteq M$, 若在 M 的运算下, S 是 R 上的模, 则称 S 为 M 的子模.

定理 4.1 判定子模的方法(课本定理4.1): $\emptyset \neq S \subseteq M$ 是 M 的子模 $\iff \forall u, v \in S, \forall r, t \in R, ru + tv \in S$ (即线性运算封闭).

定理 4.2 (课本定理4.2): $S, T \subseteq M$ 是 M 的子模, 则 $S \cap T$ 为 M 的子模, $S + T \equiv \{u + v \mid u \in S, v \in T\}$ 为 M 的子模.

定理 4.3: $R \in R - \text{mod}$, R 的子模即 R 上的理想.

证: 设 S 为 R 的子模, 则

4. 模 I: 基本性质

(1) $\emptyset \neq S \subseteq R$

(2) $\forall u, v \in S, \forall r, t \in R, ru + tv \in S$. 特别地, 令 $t = 0$, 则 $ru \in S$

故 S 为 R 的理想. □

定义 4.3 生成子模和生成集: $\emptyset \neq S \subseteq M \in R - \text{mod}$, S 的生成子模为 $\langle\langle S \rangle\rangle \equiv$ 包含 S 的最小子模 \equiv 包含 S 的所有子模的交 $= \{\sum_{i=1}^n r_i u_i \mid r_i \in R, u_i \in S, n \in \mathbb{Z}^+\}$, 其中称 S 为生成集.

$\forall M \in R - \text{mod}$, 都有生成集, $\therefore M = \langle\langle M \rangle\rangle$.

定义 4.4 有限生成模: 生成集由有限个元素构成的生成模.

定义 4.5 循环模: 生成集由一个元素构成的生成模.

例 4.6: $R \in R - \text{mod}$ 是一个循环模, $\therefore R = \langle\langle 1 \rangle\rangle = \{r1 \mid r \in R\}$. □

有限生成模的子模未必是有限生成的, 即有限生成的性质未必会由模遗传至其子模.

例 4.7: 多项式环 $R = F[x_1, \dots, x_n, \dots] \equiv \left\{ \sum_{k_i=0}^N a_{i_1, \dots, i_n} x_{i_1}^{k_1} \cdots x_{i_n}^{k_n} \mid a_{i_1 \dots i_n} \in F, N_i \in \mathbb{Z}^+ \right\}$, $R \in R - \text{mod}$ 且 $R = \langle\langle 1 \rangle\rangle$.

假设 S 是有限生成的, $S = \langle\langle f_1, \dots, f_m \rangle\rangle$, $f_i = \sum_{j_1, \dots, j_m=0}^{N_i} a_{i_1, \dots, i_n}^{j_1, \dots, j_n} x_{i_1}^{j_1} \cdots x_{i_n}^{j_n}$ 是有限个变元的有限次多项式, 故 S 无法生成无限个变元的无限次多项式, 即 S 并非有限生成的. □

定义 4.6 线性无关: $\emptyset \neq S \subseteq M$, 若 $\sum_{i=1}^n r_i u_i = 0$ 其中 $u_i \in S, r_i \in R \forall i \implies r_1 = \dots = r_n = 0$, 则称 S 线性无关.

在模中, 线性无关元素未必存在, 如例 ?? 中 \mathbb{Z}_p 无线性无关元素.

在向量空间中, 我们有: u, v 线性相关 $\iff \exists$ 不全为零的 $r, t \in R$, s.t. $ru + tv = 0$, 不妨设 $r \neq 0$, 则 $ru = -tv \implies u = -\frac{t}{r}v$.

在模中, 上述说法未必成立: u, v 线性相关 $\iff \exists$ 不全为零的 r, t , s.t. $ru + tv = 0$, (不妨设 $r \neq 0$.) 则 $ru = -tv$, 但由于未必能找到 r 的逆元, 所以未必有 $u = -\frac{t}{r}v$. 故在模中, 线性相关元素未必能相互表示, 即一个线性相关元素未必能由与其线性相关的元素线性表示.

定义 4.7 自由模: $M \in R - \text{mod}$, $M = \langle\langle \mathcal{B} \rangle\rangle$ 且 \mathcal{B} 线性无关, 则称 M 为自由模, \mathcal{B} 为 M 的基.

定理 4.4 (课本定理4.3): $\emptyset \neq \mathcal{B} \subseteq M$ 是 M 的基, 则 $\forall v \in M$, v 可由 \mathcal{B} 中的元素唯一地线性表示.

定理 4.5 (课本定理4.4): \mathcal{B} 是 M 的基 $\iff \mathcal{B}$ 为 M 的极小生成集且为 M 的极大线性无关集.

例 4.8: $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$, $\mathbb{Z}_6 = \langle\langle [1] \rangle\rangle = \langle\langle [5] \rangle\rangle$,

$\therefore 0[1] = [0], 1[1] = [1], 2[1] = [2], 3[1] = [3], 4[1] = [4], 5[1] = [5]$,

$0[5] = [0], 1[5] = [5], 2[5] = [10] = [4], 3[5] = [15] = [3], 4[5] = [20] = [2], 5[5] = [25] = [1]$.

故 \mathbb{Z}_6 的表示不唯一. □

4. 模 I: 基本性质

$M \in R - \text{mod}$, 但 M 的子模未必自由.

例 4.9: $R = \mathbb{Z} \times \mathbb{Z} = \{(n, m) \mid n, m \in \mathbb{Z}\}$, 其中 $(n, m)(k, l) = (nk, ml)$, $(n, m) + (k, l) = (n + k, m + l)$ 是仅为交换环 (而非域), $R \in R - \text{mod}$, $R = \langle\langle(1, 1)\rangle\rangle = \{r(1, 1) \mid r \in R = \mathbb{Z} \times \mathbb{Z}\}$, $\therefore R$ 自由.

但子模 $S = \mathbb{Z} \times \{0\} = \{(n, 0) \mid n \in \mathbb{Z}\}$, $\because \forall n \neq 0, (n, 0)(0, 1) = (0, 0)$, \therefore 无线性无关元, 从而非自由. \square

定义 4.8 模同态: $M, N \in R - \text{mod}$, 映射 $\tau : M \rightarrow N$, 若 $\forall u, v \in M, r, t \in R, \tau(ru + tv) = r\tau(u) + t\tau(v)$, 则 τ 为 M 到 N 的模同态, 记作 $\tau \in \text{hom}(M, N) = \{M \text{ 到 } N \text{ 的模同态}\}$.

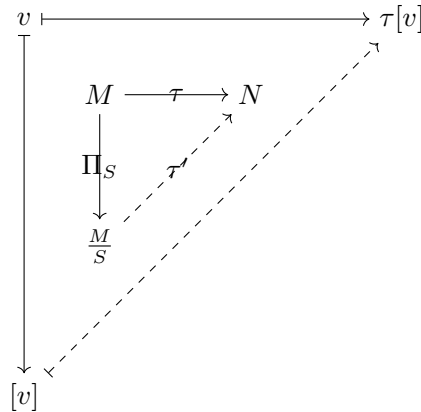
取 $r = t = 1$, 则 $\forall u, v \in M, \tau(u + v) = \tau(u) + \tau(v)$, 故 τ 为群同态.

定理 4.6 (课本定理4.6): (1) $\ker \tau \equiv \{v \in M \mid \tau(v) = 0\}$ 是 M 的子模. τ 单射 $\iff \ker \tau = \{0\}$.

(2) $\text{Im } \tau \equiv \{\tau(v) \mid v \in M\}$ 是 N 的子模. τ 满射 $\iff \text{Im } \tau = N$.

定义 4.9 商模: S 是 M 的子模, 商群 $\equiv \{[v] \mid v \in M\}$.

$[u] + [v] = [u + v]$, $r[u] = [ru]$ 是合法运算, \because 结果与代表元选取无关.



$\Pi_S : M \rightarrow \frac{M}{S}, v \mapsto [v]$, 且满足

(1) Π_S 满射.

(2) $\ker \Pi_S = S$.

定理 4.7 同态第一基本定理: 若 $S \subseteq \ker \tau$, 则 $\exists! \tau'$, s.t. $\tau = \tau' \circ \Pi_S$.

$$\ker \tau' = \frac{\ker \tau}{S}.$$

定理 4.8 同构第一基本定理: 若 $S = \ker \tau$, 则 $\tau' = \frac{\ker \tau}{S} = \{[0]\}$, 即 τ' 单射.

$\because \text{Im } \tau' = \text{Im } \tau$, \therefore 若进一步有 τ , 则 τ' 同构.