有限群表示论初步

李从辉

liconghui@swjtu.edu.cn

目　录

第一章　表示的基本概念

1.1　群与群的置换表示

1.1.1. 历史上, **群** (group) 的概念是 E. Galois 为解决高次方程根式求解问题而引入的. 对一元二次方程, 我们有求根公式, 这个公式用系数的加减乘除和开方运算给出方程的全部根. 对一元三次和四次方程, 也有类似的公式. 一般地, 设有多项式

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \quad n > 0, a_n \neq 0.$$

方程 $f(x) = 0$ 可根式求解是指可用 $a_0, a_1, \ldots, a_n$ 经加减乘除和开方运算得到的公式表示出 $f(x) = 0$ 的所有根. 对方程 $f(x) = 0$, Galois 定义了一个群 $\mathrm{Gal}(f)$, 称为 $f(x)$ 的 **Galois 群**, 并证明了以下结论:

方程 $f(x) = 0$ 可根式求解当且仅当 $\mathrm{Gal}(f)$ 是可解群.

例如, 对于 n **次一般方程** (即系数 $a_0, a_1, \ldots, a_n$ 是一般符号)$f(x) = 0$, Galois 证明了 $\mathrm{Gal}(f) \cong \mathcal{S}_n$ 为 n 阶对称群且 $\mathcal{S}_n (n \geq 5)$ 不可解, 于是 5 次及以上一般方程不可根式求解.

1.1.2. Galois 使用的群是具体的置换群, 后来数学家引入了抽象群的概念. 群论研究的一个课题是分类所有的群, 即列举出所有不同构的群.

设 G 是一个群, N 是 G 的一个正规子群, 则称 G 是 N 和 $S := G/N$ 的一个**扩张** (extension). 设 S 是一个非平凡群, 若 S 只有 1 和 S 这两个正规子群, 则称 S 是一个**单群** (simple group). 设 G 是一个群, G 的一个**合成列** (composition series) 是指 G 的一系列子群

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{r-1} \trianglelefteq G_r = G$$

使得对每个 $i = 1, 2, \ldots, r$, G_{i-1} 是 G_i 的正规子群且 G_i/G_{i-1} 是单群; 单群 $S_i := G_i/G_{i-1} (i = 1, 2, \ldots, r)$ 称为 G 的**合成因子** (composition factors). 注意到: 合成列不唯一, 但合成因子与合成列无关. 从合成列可以看出: G_1 是 G_0 和 S_1 的一个扩张, G_2 是 G_1 和 S_2 的一个扩张, $\ldots$, $G = G_r$ 是 G_{r-1} 和 S_r 的一个合成. 所以从理论上来说, 分类所有群需要解决两个问题: (1) 群扩张问题; (2) 单群分类.

1.1.3. 有限单群分类 (Classification of the finite simple groups, 简称为 CFSG) 在上世纪八九十年代宣告完成, 这是上世纪最重要和最宏大的数学成果之一. 根据有限单群分类定理, 任意单群都是如下的群之一:

(1) 素数阶循环群 C_p;

(2) 交错单群 A_n;

(3) 李型单群;

(4) 26 个散在单群.

其中, 交换单群必定是素数阶循环群, 其他三类都是非交换单群. 有限单群分类定理的证明由 100 余篇论文组成, 篇幅超过 10000 页. 目前, 由 Gorenstein, Lyons 和 Solomon 撰写的统一证明尚未完成; 他们的证明目前已出版 9 卷, 计划占用 11 卷, 总篇幅也有几千页.

1.1.4. 读者已经在近世代数课程上学习过群的基本概念. 若 H 是群 G 的一个 (正规) 子群, 我们记为 $H \leq G$ $(H \trianglelefteq G)$. 设 $H \leq G$, 则集合

$$gH := \{gh \mid h \in H\}, \quad Hg := \{hg \mid h \in H\}, \quad g \in G$$

分别称为 H 在 G 中的**左陪集**和**右陪集**, H 在 G 中所有左 (右) 陪集的集合记为 G/H $(H\backslash G)$. 左陪集 gH 中的任意元素 gh 都称为 gH 的一个代表元, H 在 G 的任意完全左陪集代表元集记为 $[G/H]$; 通常将 H 的代表元取为 1. 我们有:

(1) $g_1H = g_2H$ 当且仅当 $g_2^{-1}g_1 \in H$;

(2) 对任意 $g \in G$, $H \to gH$, $h \mapsto gh$ 都是双射, 且当 H 有限时有 $|gH| = |H|$;

(3) G 可分解为无交并 $G = \dot{\cup}_{g\in[G/H]} gH$;

(4) 若 G 是有限群, 则 $|G| = |G/H||H|$.

对右陪集有类似结论. 群 G 的子群 N 是 G 的正规子群有如下等价的定义方式

(i) 对任意 $g \in G$ 和 $n \in N$ 都有 ${}^g n := gng^{-1} \in N$.

(ii) 对任意 $g \in G$ 都有 ${}^g N (:= \{gng^{-1} \mid n \in N\}) \subseteq N$.

(iii) 对任意 $g \in G$ 都有 ${}^g N = N$.

(iv) 对任意 $g \in G$ 都有 $gN = Ng$.

由上述最后一条可知, 若 $N \trianglelefteq G$, 则 $G/N = N\backslash G$. 设 $N \trianglelefteq G$, 则集合 G/N 上定义的乘法

$$(g_1N)(g_2N) := (g_1g_2)N$$

是良定义的, 即与陪集代表元的选取无关. 可以验证: G/N 关于上述乘法构成一个群, 称为 G 的一个**商群**, 其单位元为 $1 \in G$ 的陪集 N, $gN \in G/N$ 的逆元为 $g^{-1}N$. 常使用 bar convention 来表示商群: 记 $\bar{G} := G/N$, 记 $\bar{g} := gN$ (注意这个符号没有包含正规子群 N, 因而需在指定正规子群 N 或 N 可从上下文确定的意义下使用); 在这种符号下有:

(a) $g_1g_2^{-1} \in N \Leftrightarrow \bar{g_1} = \bar{g_2} \Leftrightarrow g_2^{-1}g_1 \in N$.

(b) $\bar{g_1}\bar{g_2} = \overline{g_1g_2}$.

(c) $\bar{g}^{-1} = \overline{g^{-1}}$.

(d) $\bar{g} = \bar{1} \Leftrightarrow g \in N$.

1.1.5. 读者已经在近世代数课程中学习过群同态和群同构的概念. 这里回顾一下群同态基本定理. 设 $\varphi\colon G \to H$ 是一个群同态, 则有**群同态第一基本定理**:

$$\operatorname{Ker}\varphi \trianglelefteq G, \quad G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi.$$

设 $\varphi\colon G \to H$ 是一个满同态, 则有**群同态第二基本定理**: 映射

$$\begin{aligned} \{G \text{ 的包含 } \operatorname{Ker}\varphi \text{ 的子群}\} &\to \{\text{H 的子群}\} \\ K &\mapsto \varphi(K) \end{aligned}$$

是一个保持包含关系的一一对应; 在这个对应下有 $K \trianglelefteq G$ 当且仅当 $\varphi(K) \trianglelefteq H$, 且此时有

$$G/K \cong H/\varphi(K).$$

若 $N \trianglelefteq G$ 且 φ 是自然满同态 $G \to G/N,\ g \mapsto \bar{g}$, 则第二同态基本定理可表述如

下: 映射

$$\{G \text{ 的包含 } N \text{ 的子群}\} \to \{\text{G/N 的子群}\}$$
$$K \mapsto K/N$$

是一个一一对应; 在这个对应下有 $K \trianglelefteq G$ 当且仅当 $K/N \trianglelefteq G/N$, 且此时有

$$G/K \cong (G/N)/(K/N).$$

继续考虑自然同态 $\varphi\colon G \to G/N$, 若 $H \leq G$ 但 H 不一定包含 N 时, 有**群同态第三基本定理**:

$$\varphi(H) = HN/H \cong H/H \cap N.$$

1.1.6. 设 G 是一个群, G 的**导群** (derived subgroup) 是由形如 $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$ $(g_1, g_2 \in G)$ 的所有元素生成的子群, 记为 $G' = [G, G]$, 即

$$G' = \langle [g_1, g_2] \mid g_1, g_2 \in G \rangle$$

元素 $[g_1, g_2]$ 称为 g_1, g_2 的**交换子**; 显然 $[g_1, g_2] = 1$ 当且仅当 g_1, g_2 相乘课交换. 可归纳地定义**高阶导群**:

$$G^{(0)} = G,\ G^{(1)} = G',\ \ldots,\ G^{(n)} = (G^{(n-1)})',\ \ldots$$

对有限群 G, 若存在一个自然数 n 使得 $G^{(n)} = 1$, 则称 G 为**可解群** (solvable group). 由定义, 交换群显然都是可解群.

1.1.7 命题. *设 G 是一个群, G' 是 G 的导群, 则*

(1) G' 是 G 的正规子群;

(2) G/G' 是一个交换群;

(3) G' 是使得商群交换的最小正规子群, 即若 $N \trianglelefteq G$ 使得 G/N 交换, 则必有 $G' \leq N$.

1.1.8 命题. *设 G 是一个群, $N \trianglelefteq G$, 则 G 可解当且仅当 N 和 G/N 都可解.*

1.1.9. 容易证明: 交换单群一定是素数阶循环群. 由上面的性质可以得到: *非交换单群一定不可解*或等价地*可解群一定不是非交换单群*. 所以寻找非交换单群, 首先必须排除可解群. 可解群的判定和性质是群论的重要课题. 这里列举两个著

名结果.

Burnside p^aq^b 定理 若群 G 的阶为 $p^aq^b(p,q$ 为素数, $a,b\in\mathbb{N})$, 则 G 可解.

Feit-Thompson 定理 所有其数阶群都可解.[1]

由以上两个结果可得: 非交换单群的阶必为偶数且可被至少 3 个素数整除.

1.1.10. 群表示论的思想是将抽象群和一类具体群做比较, 比较的方式是通过群同态. 根据用来做比较的具体群的不同就有不同的群表示论, 例如: 对称群对应群的**置换表示**和**群在集合上的作用**); 一般线性群对应群的**群的线性表示**和**群在线性空间上的作用**. 群的线性表示是我们课程的研究对象, 常简称为群的表示.

群表示有很多重要应用: Burnside p^aq^b 定理; Feit-Thompson 奇阶群可解定理; 有限单群分类定理; 等等. **本课程讨论线性表示的基本概念和结果, 作为应用, 我们将用表示论的方法证明 Burnside p^aq^b 定理**.

1.1.11. 对任意集合 Ω, 记 $\mathcal{S}_\Omega$ 为 Ω 上的对称群 (由 Ω 上所有一一变换组成的群); 若 $|\Omega|=n$, 则 $\mathcal{S}_\Omega\cong\mathcal{S}_n$. 群 G 的**置换表示** (permutation representation) 是指 G 到某个对称群 $\mathcal{S}_\Omega$ 的群同态

$$\rho\colon G\to\mathcal{S}_\Omega.$$

回顾一下, **群 G 在集合 Ω 上的作用** (actions of groups on sets) 是指一个映射

$$G\times\Omega\to\Omega,\quad (g,x)\mapsto g.x$$

且满足

$$g_1.(g_2.x)=(g_1g_2).x,\ 1_G.x=x,\ \forall g_1,g_2\in G,\forall x\in\Omega.$$

群的置换表示与群在集合上的作用一一对应. 具体来说, 若 $\rho\colon G\to\mathcal{S}_\Omega$ 是 G 的一个置换表示, 则可定义 G 在集合 Ω 上的一个作用

$$g.x=\rho(g)(x),\quad \forall g\in G,\ \forall x\in\Omega;$$

反过来, 若有群 G 在集合 Ω 上的一个作用, 则可定义 G 的一个置换表示

$$\rho\colon\ G\to\mathcal{S}_\Omega,\ g\mapsto(x\mapsto g.x).$$

注意, 上面群在集合上的作用是**左作用** (left action), 类似地还可以定义**右作用**

[1] W. Feit, J. Thompson, Solvability of groups of odd order, Pacific J. Math. 13 (1963), 775–1029.

(right action); 以下若无特别说明, 群在集合上的作用都是指左作用. 当 G 作用在集合 Ω 上时, 称 Ω 是一个 **G-集合** (G-set).

1.1.12. 设 G 是一个群，Ω 是一个 G-集合.

对任意 $x \in \Omega$, Ω 的子集

$$\mathcal{O}_G(x) := \{g.x \mid g \in G\}$$

称为 x 在 G 作用下的**轨道** (orbit). 轨道的大小也称为**轨道的长度**. G 在 Ω 上所有轨道的集合记为 $G\backslash\Omega$. 轨道中的任意元素称为这个轨道的**代表元** (representative); 从每一个轨道任取一个代表元组成的集合称为一个**完全代表元集** (complete set of representatives), 记为 $[G\backslash\Omega]$; 注意完全代表元集不唯一, $[G\backslash\Omega]$ 表示任意完全代表元集, 通常使用这个符号时, 所讨论的概念都是**良定义**的 (well defined), 即与代表元集的选取无关. 对 G 在 Ω 上的右作用, 有类似的概念和符号 Ω/G, $[\Omega/G]$.

若群 G 在集合 Ω 上的作用只有一个轨道, 则称 G 在 Ω 上的作用是**传递**的 (transitive). 群 G 在集合 Ω 上作用传递的一个等价描述是: *对任意 $x, y \in \Omega$, 存在 $g \in G$ 使得 $y = g.x$.* 若 $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$ 是 G 在 Ω 上的所有轨道, 则有无交并

$$\Omega = \mathcal{O}_1 \mathbin{\dot\cup} \mathcal{O}_2 \mathbin{\dot\cup} \cdots \mathbin{\dot\cup} \mathcal{O}_k.$$

因此, 群的置换表示可归结为传递置换表示.

对 $x \in \Omega$, 子群 $G_x = \{g \in G \mid g.x = x\}$ 称为 G 在 x 处的**稳定化子** (stabilizer). 若对任意 $x \in \Omega$ 都有 $G_x = 1$, 则称 G 在 Ω 上的作用是**半正则**的 (semi-regular); 若 G 在 Ω 上的作用既是半正则的又是传递的, 则称该作用是**正则**的 (semi-regular).

设 G 在 Ω 上的作用对应置换表示 $\rho\colon G \to \mathcal{S}_\Omega$, 则 ρ 的核 $\ker\rho$ 也称为 G 在 Ω 上作用的**核** (kernel); 由定义, $\ker\rho = \bigcap_{x\in\Omega} G_x$; 若 $\ker\rho = 1$, 则称 G 在 Ω 上的作用是**忠实**的 (faithful). *半正则作用都是忠实的.*

1.1.13 例. 设 G 是一个群, H 是 G 的一个子群.

(1) H 在 G 上的**左乘作用** (left multiplication action) 定义如下:

$$H \times G \to G,\ (h, g) \mapsto hg;$$

左乘作用是半正则的, 从而是忠实的; $g \in G$ 在左乘作用下的轨道为

$$Hg := \{hg \mid h \in H\},$$

称为 H 在 G 中的**右陪集** (right coset); 所有轨道的集合为

$$H\backslash G = \{Hg \mid g \in G\};$$

左乘作用的完全代表元集记为 $[H\backslash G]$. 同理可以定义 H 在 G 上的**右乘作用** (right multiplication action), 并且有相应的左陪集 gH, 左陪集集合 G/H 和左陪集完全代表元集 $[G/H]$.

(2) (**Cayley 定理**) 任意群 G 都是某个对称群的子群.

(3) G 在 G/H 上有一个左乘作用:

$$G \times G/H \to G/H,\ (g, xH) \mapsto gxH,$$

这个作用是传递的, 其核为 $\bigcap_{x\in G} {}^xH$. 类似地, G 可右乘作用在 $H\backslash G$ 上.

(4) 设 K 是 G 的一个子群且 H 正规化 K(即 $H \le N_G(K)$: ${}^hK = K$, $\forall h \in H$). 则 H 在 K 上的**共轭作用** (conjugacy action) 定义为:

$$H \times K \to K,\ (h, x) \mapsto {}^hx := hxh^{-1};$$

对 $x \in K$, x 在 H 作用下的稳定化子为

$$C_H(x) := \{h \in H \mid hx = xh\}.$$

例如当 $K \trianglelefteq G$, $H = G$ 时, G 通过共轭作用在 N 上. 当 $H = K = G$ 时, 共轭作用的轨道称为 G 的**共轭类** (conjugacy class), 此时共轭表示的核为 $Z(G)$.

1.1.14 例. 二面体群的一个置换表示; $D_6 \cong \mathcal{S}_3$.

1.1.15. 设 G 是一个群. 为比较 G 的两个置换表示, 引入置换表示的映射概念. 设 Ω 和 Λ 是两个 G-集合.

若 Ω 到 Λ 的映射 σ 满足

$$\sigma(g.x) = g.\sigma(x),\ \forall x \in \Omega,$$

则称 σ 是 G-集合 Ω 到 Λ 的一个 **G-映射** (G-map); 若 σ 还是一个双射, 则称 σ 是一个 **G-同构** (G-isomorphism) 或**置换 (表示) 同构** (isomorphism of permutation representations). 若存在 G-集合 Ω 到 G-集合 Λ 的 G-同构, 则称 Ω 和 Λ 是 **(G-)**

同构或**置换同构**的.

两个 G-同构的集合可认为是一样的: 不仅元素之间一一对应, G-的作用也一一对应, 从而与置换表示相关的概念都是一样的. 设 Ω 和 Λ 是 G-同构的. 则 Ω 和 Λ 的轨道一一对应, 对应的轨道长度也是一样的; G 在 Ω 上是传递的当且仅当 G 在 Λ 上也是传递的; Ω 和 Λ 的对应元素具有相同的稳定化子; G 在 Ω 上是 (半) 正则的当且仅当 G 在 Λ 上也是 (半) 正则的; G 在 Ω 上的核等域 G 在 Λ 上的核; G 在 Ω 上是忠实的当且仅当 G 在 Λ 上也是忠实的; 等等.

1.1.16 命题. *设群 G 传递地作用在集合 Ω 上, 任取 $x \in \Omega$, 则有置换表示同构:*

$$G/G_x \to \Omega,\ gG_x \mapsto g.x.$$

1.1.17 命题. *设 Ω 是一个 G-集合且 G 和 Ω 都是有限的.*

(1) (轨道-稳定化子定理, orbit-stabilizer theorem) 对任意 $x \in \Omega$, 记 $\mathcal{O}_G(x)$ 为 x 在 G 下的轨道, 则有

$$|G| = |G_x||\mathcal{O}_G(x)|.$$

(2) 设 G 在 Ω 上的所有轨道为 $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$, 任取 $x_i \in \Omega_i$, 则有

$$|\Omega| = |G|/|G_{x_1}| + |G|/|G_{x_2}| + \cdots + |G|/|G_{x_k}|.$$

(3) (类公式, class fumula) 设 G 的所有共轭类为 $C_1, C_2, \ldots, C_k$, 任取 $x_i \in C_i$, 则有

$$|G| = |G|/|C_G(x_1)| + |G|/|C_G(x_2)| + \cdots + |G|/|C_G(x_k)|.$$

1.1.18 定理 (Sylow 定理)**.** *设 G 是一个群, p 是一个素数, $|G| = n = p^a n_0$ 且 $(n_0, p) = 1$.*

(1) 存在 G 的子群 P 使得 $|P| = p^a$, 这样的子群称为 G 的 Sylow p-子群.

(2) 设 P 是 G 的一个 Sylow p-子群, Q 是 G 的一个 p-子群, 则存在 $g \in G$ 使得 ${}^gQ \le P$. 特别地, G 的所有 Sylow p-子群都共轭.

(3) 设 $\mathrm{Syl}_p(G)$ 为 G 的所有 Sylow p-子群组成的集合, 则有

$$|\mathrm{Syl}_p(G)| \mid n_0, \quad |\mathrm{Syl}_p(G)| \equiv 1 \mod p.$$

1.1.19 命题. *设 P 是一个 p-群.*

(1) 若 $P \neq 1$, 则 $Z(P) \neq 1$.

(2) P 是可解的[2]*.*

习 题

1.1.1. 证明 1.1.4 和 1.1.5 中的所有论断.

1.1.2. 设 G 是一个群, S 是 G 的一个子集. 由 S 中元素通过乘法和求逆得到的所有元素组成的集合构成 G 的一个子群, 称为由 S 生成的子群, 记为

$$\langle S \rangle = \langle s \mid s \in S \rangle.$$

证明: $\langle S \rangle$ 是 G 中包含 S 的最小子群.

1.1.3. 设 G 是一个群, $N \leq G$, 且 N 有 G 的子集 S 生成. 证明: 若对任意 $s \in S$ 和 $g \in G$ 都有 ${}^g s \in N$, 则 $N \trianglelefteq G$.

1.1.4. 设 G 是一个群, $g_1, g_2, g \in G$, 证明: ${}^g[g_1, g_2] = [{}^g g_1, {}^g g_2]$.

1.1.5. 设 $\varphi\colon G \to H$ 是一个群同态, 证明:

(1) 对任意 $g_1, g_2 \in G$ 都有 $\varphi([g_1, g_2]) = [\varphi(g_1), \varphi(g_2)]$;

(2) $\varphi(G^{(n)}) = \varphi(G)^{(n)}$.

1.1.6. 设 G 是一个群, $N \trianglelefteq G$, $H \leq G$. 证明: $(HN/N)^{(n)} \cong H^{(n)}N/N$.

1.1.7. 设 $G = \mathcal{S}_4$, 试计算 G 的各阶导群 $G^{(1)}, G^{(2)}, \ldots$

1.1.8. 证明置换表示和群在集合上的作用一一对应; 参见 1.1.11.

1.1.9. 设 G 是一个有限群, Ω 是一个 G-集合. 证明: 若 G 在 Ω 上的作用是半正则的, 则 G 在 Ω 上的每个轨道长度都是 $|G|$; 若 G 在 Ω 上的作用是正则的, 则 $|\Omega| = |G|$.

[2] 实际上 P 是幂零的 (nilpotent), 幂零是比可解更强的条件.

1.2　环与代数的表示和模

1.2.1. 假定读者已经掌握近世代数中关于环的基本概念. 类似于群表示, 也可以考虑 "环的表示": 将一般抽象的环与某类具体的环做比较. 这类具体的环通常选取为交换群的自同态环. 设 V 是一个交换群, 则 V 的所有群自同态构成的集合 $\mathrm{End}_{\mathrm{ab}}(V)$ 关于如下定义的加法和乘法 $(\sigma,\tau\in\mathrm{End}_{\mathrm{ab}}(V))$

$$\sigma+\tau\colon\ V\to V,\ v\mapsto\sigma(v)+\tau(v);$$
$$\sigma\tau\colon\ V\to V,\ v\mapsto\sigma(\tau(v))$$

构成一个含幺环, 其中幺元为 V 的恒等变换 Id_V. **环**[3]**A 的表示**是指保幺元的环同态

$$\rho\colon\ A\to\mathrm{End}_{\mathrm{ab}}(V),$$

其中 V 是一个交换群.

1.2.2. 类似于群的置换表示和群在集合上的作用, 环的表示也对应环在交换群上的作用. 设 A 是一个环, V 是一个交换群. **A 在交换群 V 上的一个作用** (action of A on an abelian group) 是指有一个映射

$$A\times V\to V,\quad (a,v)\mapsto a.v$$

且满足对任意 $a,a_1,a_2\in A,u,v\in V$ 都有[4]

$$a.(u+v)=a.u+a.v,$$
$$(a_1+a_2).v=a_1.v+a_2.v,$$
$$a_1.(a_2.v)=(a_1a_2).v,$$
$$1_A.v=v;$$

此时, 我们也说 V 是一个 **A-模** (A-module)[5]. 注意到上述第一个条件说明任意 $a\in A$ 在 V 上的作用都是一个交换群自同态. 请读者自己验证: **环 A 的表示和 A 的模一一对应**.

上述模的概念也称为左模, 类似可定义右模的概念. 对交换环 R, 左 R-模和

[3]若无特别说明, 本文中的环都是含幺环.

[4]这四条要求加上交换群定义的四条要求就是通常模定义的八条要求.

[5]即 "作用" 和 "模" 是等同的概念, 后面考虑的群 G 在 R-模上的作用和 R 上的 G-模也是等同的概念.

右 R-模的概念是一样的.

1.2.3. 设 A 是一个环, U,V 都是 A-模.

设有映射 $\sigma\colon U\to V$. 若 σ 满足

$$\sigma(u_1+u_2)=\sigma(u_1)+\sigma(u_2),\ \sigma(au)=a\sigma(u),\ \forall u,u_1,u_2\in U,a\in A,$$

则称 σ 是一个 **A-模同态** (homomorphism of A-modules 或 A-homomorphism). 注意到模同态定义等价于:

$$\sigma(a_1u_1+a_2u_2)=a_1\sigma(u_1)+a_2\sigma(u_2),\ \forall a_1,a_2\in A,\forall u_1,u_2\in U.$$

当 $\sigma\colon U\to V$ 是 A-模同态时, 上述性质还可推广到任意的 A-线性组合 $a_1u_1+a_2u_2+\cdots+a_nu_n$ ($a_i\in A,\ u_i\in U$):

$$\sigma(a_1u_1+a_2u_2+\cdots+a_nu_n)=a_1\sigma(u_1)+a_2\sigma(u_2)+\cdots+a_n\sigma(u_n).$$

若 σ 既是一个 A-模同态, 又是一个双射, 则称 σ 是一个 **A-模同构** (isomorphism of A-modules 或 A-isomorphism); A-模同态 σ 是 A-模同构当且仅当存在 A-模同态 $\tau\colon V\to U$ 使得 $\sigma\tau=\mathrm{Id}_V$ 且 $\tau\sigma=\mathrm{Id}_U$. 若存在 U 到 V 的 A-模同构, 则称 U 和 V 是**同构**的, 记为 $U\cong V$, 此时也称 U,V 对应的表示是同构的.

将 U 到 V 的所有 A-模同态构成的集合记为 $\mathrm{Hom}_A(U,V)$, 且当 $U=V$ 时, 记为 $\mathrm{End}_A(V):=\mathrm{Hom}_A(V,V)$. 设 $\sigma\colon U\to V$ 是一个 A-模同态, 定义中的条件

$$\sigma(u_1+u_2)=\sigma(u_1)+\sigma(u_2),\ \forall u_1,u_2\in U$$

说明 σ 是一个交换群同态, 定义中的条件

$$\sigma(au)=a\sigma(u),\ \forall u\in U,a\in A$$

说明 σ 与 A 的作用 (A 的作用是交换群自同态) 可交换. 设 A-模 U,V 对应的 A 的表示分别为 $\rho_U\colon A\to\mathrm{End}_{\mathrm{ab}}(U)$ 和 $\rho_V\colon A\to\mathrm{End}_{\mathrm{ab}}(V)$, 则由定义有

$$\mathrm{Hom}_A(U,V)=\{\sigma\in\mathrm{Hom}_{\mathrm{ab}}(U,V)\mid\sigma\circ\rho_U(a)=\rho_V(a)\circ\sigma,\forall a\in A\};$$

特别地, 当 $U=V$ 时有

$$\mathrm{End}_A(V)=\{\sigma\in\mathrm{End}_{\mathrm{ab}}(V)\mid\sigma\circ\rho_V(a)=\rho_V(a)\circ\sigma,\forall a\in A\}.$$

集合 $\mathrm{Hom}_A(U,V)$ 关于如下加法

$$\sigma+\tau\colon u\mapsto\sigma(u)+\tau(u),\ \sigma,\tau\in\mathrm{Hom}_A(U,V)$$

构成一个交换群. 当 $U=V$ 时, $\mathrm{End}_A(V):=\mathrm{Hom}_A(V,V)$ 关于上述加法和映射合成作为乘法构成一个环, 称为 V 的**同态环** (endomorphism ring). 若 $A=R$ 是一个交换环, 则 $\mathrm{Hom}_R(U,V)$ 关于上述加法和如下 R-作用

$$r\sigma\colon\ u\mapsto r\sigma(u),\ r\in R,\sigma\in\mathrm{Hom}_R(U,V)$$

构成一个 R-模.

1.2.4. 设 A 是一个环, V 是一个 A-模.

若 V 的子集 U 关于加法构成 V 的子群且在 A 的作用下封闭, 则 U 关于 V 中的加法和 A-作用也是一个 A-模, 称为 V 的一个 **A-子模** (A-submodule)[6].

设 U,W 都是 V 的子模, 则它们的交 $U\cap W$ 与**和** (sum)

$$U+W=\{u+w\mid u\in U,w\in W\}$$

也都是 V 的子模. 交与和的构造还可以推广到任意多个子模的情形. 设 $V_i,i\in I$ 是 V 的一族 A-子模[7]. 则子模 $V_i,i\in I$ 的交仍是 V 的子模. 子模 $V_i,i\in I$ 的**和** (sum) 定义为

$$\sum_{i\in I}V_i:=\left\{v_{i_1}+v_{i_2}+\cdots+v_{i_k}\mid i_j\in I,v_{i_j}\in V_{i_j}\right\},$$

读者可验证, 这也是 V 的子模.

对 V 的子集 Ω, 集合

$$\mathrm{Span}_A(\Omega):=\left\{\sum_{i=1}^n a_ix_i\mid n\in\mathbb{N},a_i\in A,x_i\in\Omega\right\}$$

是 V 的一个 A-子模, 称为**由 Ω 生成的子模**. 上述子模也记为 $A\Omega$ 或 $\sum_{x\in\Omega}Ax$. 当 $V=\mathrm{Span}_A(\Omega)$ 时, 称 Ω 是 V 的一组生成元, V 由 Ω 生成; 若 V 可由某个有限集 Ω 生成, 称 V 是一个**有限生成 A-模**.

只含有零元素的模称为**零模**, 也记为 0. 若 V 只有 0 和 V 两个子模, 则称 V 是一个**单模** (simple module). 由一个元素生成的模称为**循环模** (cyclic module). 若循环模 V 由元素 v 生成, 我们记为 $V=Av$. 单模一定是循环模 (事实上单模可由其中任意非零元素生成).

[6]如果可以从上下文确定所讨论的环 A, 相关概念中常将 “A-” 省略, 如将 A-模简称为模, A-模同态简称为模同态, 将 A-子模简称为子模, 等等; 以下不再一一说明.

[7]这里, I 是一个 (不一定有限) 集合, 称为这族 A-模的**指标集** (index set).

1.2.5 例. (1) 对域 F 上的模就是 F-线性空间 (linear space), 子模就是线性子空间 (linear subspace), 模同态就是线性映射 (linear map 或 linear homomorphism). 所以, 模可看成线性空间的一种推广.

(2) 整数环 $\mathbb{Z}$ 上的模就是交换群; 事实上, 任意交换群 V 上有唯一的 $\mathbb{Z}$-模结构:

$$n.v = \underbrace{v+v+\cdots+v}_{n\text{ 个 }v},\ (-n).v = -(n.v), \quad \forall n \in \mathbb{N}, v \in V.$$

$\mathbb{Z}$-模的子模就是交换群的子群, 模同态就是交换群同态. 设 U, V 都是交换群 ($\mathbb{Z}$-模). 所有交换群同态构成的集合 $\mathrm{Hom}_{\mathrm{ab}}(U,V)$ 常记为 $\mathrm{Hom}_{\mathbb{Z}}(U,V)$; 类似地, 交换群自同态环 $\mathrm{End}_{\mathrm{ab}}(V)$ 常记为 $\mathrm{End}_{\mathbb{Z}}(V)$. 注意到 V 上有一个 $\mathrm{End}_{\mathbb{Z}}(V)$-模结构.

(3) 设 A 是一个环, V 是一个 A-模. 则 $\mathrm{End}_A(V)$ 是一个环且 V 有一个 $\mathrm{End}_A(V)$-模结构. 由定义, V 上的 A-作用和 $\mathrm{End}_A(V)$-作用是交换的.

(4) 环 A 关于环的加法和 A 在自身上的左乘构成一个 A-模, 称为 A 的**正则模** (regular module). 正则模的子模就是 A 的左理想. 类似地, 环 A 关于环的加法和 A 在自身上的右乘构成一个右 A-模, 称为 A 的右正则模; 右正则模的子模就是 A 的右理想.

(5) 设 A 是一个环, V 是一个 A-模, I 是 A 的一个理想, 则

$$IV := \left\{ \sum_{i=1}^{n} a_i v_i \mid n \in \mathbb{Z}_{>0}, a_i \in I, v_i \in V \right\}$$

是 V 的一个子模.

1.2.6. 设 R 是一个交换环. 环 R 在 R-模上的作用也常称为 R-数乘.

若集合 A 上定义有加法, 乘法和 R-数乘, 且 A 关于加法和 R-数乘构成一个 R-模, 关于加法和乘法构成一个环, 并满足

$$r(ab) = (ra)b = a(rb),\ \forall r \in R, a, b \in A,$$

则称 A 是一个 **R-代数** (R-algebra). 对环 A, 以下两个条件等价:

(1) A 是一个 R-代数;

(2) 存在一个保幺元的环同态 $R \to Z(A)$.

乘法交换的 R-代数称为交换 R-代数.

设 A 是一个 R-代数. 在上述环同态 $R\to Z(A)$ 下, R 的像为 $R\cdot 1_A$. A 上的 R-数乘等于 $R\cdot 1_A$ 按 A 中的乘法作用在 A 上. 因此, A 的所有左理想, 右理想和理想都是 A 的 R-子模. 若 B 是 A 的一个子集, 且 B 关于 A 的加法, 乘法和 R-数乘构成一个 R-代数, 则称 B 是 A 的一个 **R-子代数**.

若 R 是一个域且 R-代数 A 作为 R-线性空间是有限维的, 则称 A 是一个有限维 R-代数.

注意到, *任意环 A 都可看成 $\mathbb{Z}$-代数*, 其上的 $\mathbb{Z}$-模结构是唯一的. 因此, 以后的所有叙述都将对 R-代数进行, 当 $R=\mathbb{Z}$ 时就是关于一般环的结论.

1.2.7 例. 设 R 是一个交换环.

(1) 设 V 是一个 R-模, 则 $\mathrm{End}_R(V)$ 关于 1.2.3 中定义的 R-数乘, 加法和映射合成作为乘法构成一个 R-代数, 称为 V 的 **R-自同态代数** (R-endomorphism algebra).

(2) 类似于域上一元多项式的定义, 可定义 R 上的一元多项式

$$f(x)=a_nx^n+\cdots+a_1x+a_0,\quad a_0,a_1,\ldots,a_n\in R,$$

并定义多项式的加法, 乘法和 R-数乘. 记 R 上的所有一元多项式构成的集合为 $R[x]$, 则 $R[x]$ 关于多项式的加法, 乘法和 R-数乘构成一个交换 R-代数.

(3) 类似于域上矩阵的概念, 可定义 R 上的矩阵, 并定义矩阵的加法, 乘法和 R-数乘等概念. 记 R 上所有 n 阶方阵的集合为 $M_n(R)$, 则 $M_n(R)$ 关于矩阵加法, 乘法和 R-数乘构成一个 R-代数. 域上矩阵相关的大部分概念, 如果涉及到加法, 乘法和数乘, 基本都可以推广到 $M_n(R)$ 上; 如果涉及到域上的非零数, 则需要将非零数换成 R 中的可逆元 (域上的所有非零数都是可逆元), 如将某一行乘以域中的非零数的初等变换, 应改成乘以 R 中的可逆元. 在 $M_n(R)$ 上可以按照域上相同的方式定义行列式函数; 还可以定义伴随矩阵, 并有

$$AA^*=A^*A=I_n.$$

从而有 $A\in M_n(R)$ 可逆当且仅当 $|A|\in R^\times$.

1.2.8. 类似于群和环的情形, 我们也有代数的表示, 即将一般的代数与一类具体的代数进行比较, 通常用来比较的这类代数就是交换环上模的自同态代数. 设 R

是一个交换环, A 是一个 R-代数.

代数 A 的 **(R-) 表示** (R-representation) 指的是保幺元的 R-代数同态

$$\rho\colon\ A \to \mathrm{End}_R(V),$$

其中, V 是一个 R-模.

同样地, 我们还有 R-代数 A 的作用的概念, 也就是 A-模的概念. **代数 A 的模就是 A 作为环的模**. 设 V 是一个 A-模, 则 R 通过映射 $R \to R{\cdot}1_A \subseteq Z(A) \subseteq A$ 在 V 上有一个作用, 从而 V 上有 R-模结构, 并且 A 的作用保持这个 R-模结构 (即对任意 $a \in A$, $(v \mapsto a.v) \in \mathrm{End}_R(V)$), 这样就得到 A 的一个 R-表示

$$\rho\colon\ A \to \mathrm{End}_R(V),\ a \mapsto (v \mapsto a.v).$$

反过来, 设有 A 的一个 R-表示 $\rho\colon A \to \mathrm{End}_R(V)$, 则可给出 V 上的一个 A-模结构[8]. 所以, **代数 A 的表示与 A 的模一一对应**.

代数 A 的模同态就是作为环 A 的模同态. 设 U, V 都是 A-模且 $\sigma\colon U \to V$ 是一个 A-模同态, 则 $\sigma \in \mathrm{End}_R(V)$. 设 $\rho_U\colon A \to \mathrm{End}_R(U)$ 和 $\rho_V\colon A \to \mathrm{End}_R(V)$ 是 U, V 对应的表示, 则

$$\mathrm{Hom}_A(U,V) = \{\sigma \in \mathrm{Hom}_R(U,V) \mid \sigma \circ \rho_U(a) = \rho_V(a) \circ \sigma, \forall a \in A\};$$

特别地, 当 $U = V$ 时有

$$\mathrm{End}_A(V) = \{\sigma \in \mathrm{End}_R(V) \mid \sigma \circ \rho_V(a) = \rho_V(a) \circ \sigma, \forall a \in A\}.$$

注意到, $\mathrm{Hom}_A(U,V)$ 是 $\mathrm{Hom}_R(U,V)$ 的一个 R-子模; $\mathrm{End}_A(V)$ 是 $\mathrm{End}_R(V)$ 的一个 R-子代数.

1.2.9 例. 设 R 是一个交换环.

(1) 设 V 是一个 R-模. 则 V 是一个 $\mathrm{End}_R(V)$-模.

(2) 设 n 是一个正整数, R^n 是 R 上所有 n 元组的集合, 则 R^n 是一个 R-模. 将 R^n 中的元素写成列向量的形式, 则 $M_n(R)$ 可通过左乘作用到 R^n 上, 此时 R^n 称为一个 $M_n(R)$-模. 类似地, 若将 R^n 中的元素写成行向量的形式, 则 $M_n(R)$ 可通过右乘作用到 R^n 上, 此时 R^n 称为一个右 $M_n(R)$-模.

[8]注意到 V 上由 A-作用诱导的 R-模结构与 V 上本来的 R-模结构是一样的.

(3) 设 F 是一个域, V 是一个 F-线性空间, $\mathcal{A}$ 是 V 上的一个 F-线性映射. 映射

$$\rho_{\mathcal{A}}\colon\ F[x] \to \mathrm{End}_F(V),\ f(x) \mapsto f(\mathcal{A})$$

给出了 F-代数 $F[x]$ 的一个 F-表示, 而 V 成为一个 $F[x]$-模. 此时, V 的 $F[x]$-子模就是 V 的 $\mathcal{A}$-不变子空间; $\mathrm{End}_{F[x]}(V)$ 由 V 上所有与 $\mathcal{A}$ 交换的线性变换组成.

若无特殊说明, 以后都假定 R 是一个交换环.

1.2.10. 设 A 是一个 R-代数, V 是一个 A-模, U 是 V 的一个 A-子模. 若 $v_1, v_2 \in V$ 满足:

$$v_1 - v_2 \in U,$$

则称 v_1, v_2 **模** U **同余**, 记为 $v_1 \equiv v_2 \mod U$. 可验证 (留给读者): 模 U 同余是一个等价关系, 且 $v \in V$ 的等价类为

$$v + U = \{v + u \mid u \in U\}.$$

将模 U 同余关系下所有等价类的集合记为

$$V/U := \{v + U \mid v \in V\}.$$

在 V/U 上定义加法和 A-作用如下

$$(v_1 + U) + (v_2 + U) = (v_1 + v_2) + U, \quad v_1, v_2 \in V;$$
$$a(v + U) = av + U, \quad a \in A, v \in V.$$

则可验证 (留给读者): V/U 关于上述加法和 A-作用构成一个 A-模, 称为 V 关于 U 的**商模** (quotient module). 当子模 U 固定时, 也常将商模 V/U 记为 $\bar{V}$, 将商模中的元素 $v + U$ 记为 $\bar{v}$; 在这种记号下, 商模的加法和 A-作用可表示为

$$\bar{v}_1 + \bar{v}_2 = \overline{v_1 + v_2}, \quad a\bar{v} = \overline{av};$$

且有

$$\bar{v_1} = \bar{v_2} \Leftrightarrow v_1 - v_2 \in U, \quad \bar{v} = 0 \Leftrightarrow v \in U.$$

1.2.11. 设 A 是一个 R-代数, $\sigma\colon U \to V$ 是一个 A-模同态. 定义:

$$\mathrm{Ker}\,\sigma = \{u \in U \mid \sigma(u) = 0\}, \quad \mathrm{Im}\,\sigma = \{\sigma(u) \mid u \in U\};$$

可以验证, $\operatorname{Ker}\sigma$ 是 U 的子模, 称为 σ 的**核** (kernel); $\operatorname{Im}\sigma$ 是 V 的子模, 称为 σ 的**像** (image).

例如, 若 U 是 A-模 V 的一个子模, 则**自然同态** (natural homomorphism)

$$\pi\colon\ V \to V/U,\ v \mapsto v+U,$$

的核为 $\operatorname{Ker}\pi = U$. 这说明, 任意子模都是某个同态的核.

1.2.12 定理 (同态基本定理)**.** *设 A 是一个 R-代数.*

(1) 设 $\sigma\colon U \to V$ 是一个 A-模同态, 则有 A-模同构

$$U/\operatorname{Ker}\sigma \cong \operatorname{Im}\sigma,\ u+\operatorname{Ker}\sigma \mapsto \sigma(u).$$

(2) 设 $\sigma\colon U \to V$ 是一个满的 A-模同态, 则映射

$$\begin{aligned}\{U \text{ 的包含 } \operatorname{Ker}\sigma \text{ 的子模}\} &\to \{V \text{ 的子模}\}\\ U_0 &\mapsto \sigma(U_0)\end{aligned}$$

是一个保持包含关系的一一对应, 且有

$$U/U_0 \cong V/\sigma(U_0).$$

特别地, 若 U 是一个 A-模, K 是 U 的一个子模, $\sigma\colon U \to U/K$ 是自然同态 $u \mapsto \bar{u}$, 则映射

$$\begin{aligned}\{U \text{ 的包含 } K \text{ 的子模}\} &\to \{U/K \text{ 的子模}\}\\ U_0 &\mapsto U_0/K\end{aligned}$$

是一个保持包含关系的一一对应, 且有

$$U/U_0 \cong (U/K)/(U_0/K).$$

(3) 设 U 是一个 A-模, K 是 U 的一个子模, $\sigma\colon U \to U/K$ 是自然同态 $u \mapsto \bar{u}$. 对 U 的任意 (不一定包含 K 的) 子模 W, 有

$$\sigma(W)(W+K)/K \cong W/W\cap K.$$

注. 由定理 1.2.12, 所有模同态 $\sigma\colon U \to V$ 都可以分解为

$$U \longrightarrow U/\ker\sigma \cong \operatorname{Im}\sigma \hookrightarrow V.$$

在此意义下, 所有模同态 “都是” 自然同态.

1.2.13. 设 R 是任意交换幺环, A 是一个 R-代数, V 是一个 A-模. 对任意 $v \in V$, 记

$$\mathrm{Ann}_A(v) := \{a \in A \mid a.v = 0\},$$

则 $\mathrm{Ann}_A(v)$ 是 A 的一个左理想, 称为 v 在 A 中的**零化子** (annihilator). 注意到有 A-模同构

$$A/\operatorname{Ann}_A(v) \cong Av,$$

其中, $Av = \{av \mid a \in A\}$ 是由 v 生成的 V 的 A-子模. 记

$$\mathrm{Ann}_A(V) := \bigcap_{v \in V} \mathrm{Ann}_A(v),$$

则 $\mathrm{Ann}_A(V)$ 是 A 的一个理想, 称为 V 在 A 中的**零化子**.

1.2.14. 设 A 是一个 R-代数, V 是一个 A-模.

若存在 $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in V$ 满足:

(1) $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ 是 **A-线性无关**的 (A-linear independent), 即由

$$a_1\varepsilon_1 + a_2\varepsilon_2 + \cdots + a_n\varepsilon_n = 0, \quad a_i \in A,\ i = 1, 2, \ldots, n$$

可推出 $a_1 = a_2 = \cdots = a_n = 0$;

(2) 任意 $v \in V$ 都是 $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ 的 **A-线性组合** (A-linear combination), 即存在 $a_1, a_2, \ldots, a_n \in A$ 使得

$$v = a_1\varepsilon_1 + a_2\varepsilon_2 + \cdots + a_n\varepsilon_n;$$

则称 $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ 是 V 的一组**基** (basis), 称 V 是一个 **(有限生成的) 自由 A-模** ((finitely generated) free A-module). V 中任意元素可由其基唯一地线性表示. 自由模是线性空间最直接的推广.

例如, 集合

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A\}$$

关于如下加法和 A-作用

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$
$$a.(a_1, a_2, \ldots, a_n) = (aa_1, aa_2, \ldots, aa_n),$$

构成一个自由 A-模, 其一组基为

$$\varepsilon_1=(1,0,\ldots,0),\ \varepsilon_2=(0,1,\ldots,0),\ \ldots,\ \varepsilon_n=(0,\ldots,0,1).$$

自由模还可以推广到一般 (不一定有限生成) 的情形. 设 Ω 是 V 的一个 (不必有限) 子集. 若 Ω 中任意有限子集都是 A-线性无关的, 则称 Ω 是 A-线性无关的. 若 Ω 线性无关且 V 中任意元素都可以表示为 Ω 中有限个元素的 A-线性组合, 也就是说 V 可由 Ω 生成或 $V=A\Omega$, 则称 Ω 是 V 的一组基. 具有基的 A-模称为自由 A-模.

1.2.15. 设 A 是一个 R-代数, $\Omega=\{\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n\}$ 是一个集合. 记 $F_A(\Omega)$ 为所有如下**形式和** (formal sum)[9]

$$a_1\varepsilon_1+a_2\varepsilon_2+\cdots+a_n\varepsilon_n,\quad a_i\in A$$

的集合. 我们将 $\varepsilon_i\in\Omega$ 与形式和 $0\cdot\varepsilon_1+\cdots+0\cdot\varepsilon_{i-1}+1\cdot\varepsilon_i+0\cdot\varepsilon_{i+1}+\cdots+0\cdot\varepsilon_n$ 等同, 从而可将 Ω 看成 $F_A(\Omega)$ 的一个子集. 更一般的, 在书写 $F_A(\Omega)$ 中元素时常将系数为 0 的项 $0\cdot\varepsilon_i$ 省略, 特别地, 其零元 $0\cdot\varepsilon_1+0\cdot\varepsilon_2+\cdots+0\cdot\varepsilon_n$ 简记为 0. 此外, 系数 1 也常省略. 在 $F_A(\Omega)$ 上定义加法和 A-作用如下:

$$\sum_{i=1}^m a_i\varepsilon_i+\sum_{i=1}^m b_i\varepsilon_i=\sum_{i=1}^m(a_i+b_i)\varepsilon_i,\quad a_i,b_i\in A;$$
$$a\left(\sum_{i=1}^m a_i\varepsilon_i\right)=\sum_{i=1}^m aa_i\varepsilon_i,\quad a,a_i\in A.$$

可以验证: $F_A(\Omega)$ 关于上述加法和 A-作用构成一个自由 A-模, 且 Ω 为 $A\Omega$ 的一组 A-基, 称为**由集合 Ω 张成的自由 A-模** (free A-module spanned by the set Ω). 这个构造还可推广到 Ω 为任意集合的情形: 令 $F_A(\Omega)$ 是所有 Ω 中有限个元素形式和的集合, 则上述讨论全部都成立. 也常将 $F_A(\Omega)$ 记为 $A\Omega$, 且当 $\Omega=\{\varepsilon\}$ 是单点集时, 也将 $F_A(\Omega)$ 记为 $A\varepsilon$.

1.2.16 定理. *设 R 是一个交换环, V 是一个有限生成自由 R-模. 则 V 的任意基所含元素个数相同, 称为 V 的*秩 *(rank), 记为* $\mathrm{rank}_R V$.

[9]这里, 形式和的含义是: $a_1\varepsilon_1+a_2\varepsilon_2+\cdots+a_m\varepsilon_m=b_1\varepsilon_1+b_2\varepsilon_2+\cdots+b_m\varepsilon_m$ 当且仅当 $a_i=b_i$, $i=1,2,\ldots,m$.

1.2.17. 设 A 是一个 R-代数, V 是一个有限秩的自由 R-模. 设 A 在 V 上有一个作用, 即 V 是一个 A-模, 记对应的表示为

$$\rho\colon A \to \mathrm{End}_R(V).$$

固定 V 的一组 R-基 $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$, 则有一个 R-代数同构

$$\mathrm{End}_R(V) \to M_n(R),\ \sigma \mapsto X_\sigma,$$

其中 X_σ 是 σ 在基 $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ 下的矩阵, 即

$$\sigma(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) := (\sigma(\varepsilon_1), \sigma(\varepsilon_2), \ldots, \sigma(\varepsilon_n)) = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)X_\sigma.$$

将 ρ 与上述同构合成得到一个 R-代数同态

$$X_\rho\colon\ A \to M_n(R),\ a \mapsto X_\rho(a) := X_{\rho(a)},$$

称为由表示 ρ 或 A-模 V 给出的 A 的 **(R-) 矩阵表示**. 取 V 不同的基, 给出的矩阵表示之间是共轭的, 即若 X'_ρ 是 ρ 的另一个矩阵表示, 则存在可逆矩阵 $T \in \mathrm{GL}_n(R)$ 使得 $X'_\rho(a) = TX_\rho(a)T^{-1}, \forall a \in A$; 这里, $\mathrm{GL}_n(R)$ 为 R 上所有 n 阶可逆方阵的集合, 即

$$\mathrm{GL}_n(R) = \{A \in M_n(R) \mid \det(A) \in R^\times\}.$$

反过来, 给定 A 的一个矩阵表示 $X\colon\ A \to M_n(R)$, 可以构造一个自由 R-模 V 和一个 A 的表示 $\rho\colon A \to \mathrm{End}_R(V)$ 使得 ρ 对应的矩阵表示就是 X.

习 题

若无特殊说明, R 是一个交换环.

1.2.1. 设 V 是交换群, 证明: $\mathrm{End}_{\mathbb{Z}}(V)$ 关于同态的加法和合成构成一个环.

1.2.2. 证明: R-代数 A 的表示和 A-模一一对应; 参见 1.2.8.

1.2.3. 设 A 是 R-代数, $\sigma\colon U \to V$ 是 A-模同态. 证明: σ 是 A-模同构当且仅当存在 A-模同态 $\tau\colon V \to U$ 使得 $\sigma\tau = \mathrm{Id}_V$ 且 $\tau\sigma = \mathrm{Id}_U$.

1.2.4. 设 A 是 R-代数, U, V 都是 A-模. 证明: $\mathrm{Hom}_A(U, V)$ 是 $\mathrm{Hom}_R(U, V)$ 的一个 R-子模, $\mathrm{End}_A(V)$ 是 $\mathrm{End}_R(V)$ 的 R-子代数.

1.2.5. 验证 1.2.10 中的所有细节.

1.2.6. 设 A 是 R-代数, $\sigma\colon V \to W$ 是一个 A-模同态. 证明: $\operatorname{Ker}\sigma$ 是 V 的子模, $\operatorname{Im}\sigma$ 是 W 的子模.

1.2.7. 设 A 是 R-代数, $\sigma\colon V \to W$ 是一个 A-模同态. 证明: 若 U 是 V 的 A-子模且满足 $U \subseteq \operatorname{Ker}\sigma$, 则映射

$$V/U \to W,\ v + U \mapsto \sigma(v)$$

是 A-模同态.

1.2.8. 证明: 任意循环模 (从而单模) 必同构于正则模的某个商模.

1.2.9. 设 A 是 R-代数, S 是 A-模, 则 S 是单模当且仅当 S 可由其中的任意非零元素生成.

1.2.10. 设 F 是域, n 是正整数, $M_n(F)$ 左乘作用在 F^n 上, 证明: F^n 是一个单 $M_n(F)$-模.

1.3 群的线性表示

若无特殊说明, 本节中 R 是一个交换环.

1.3.1. 设 G 是一个群.

G 的一个 R-**表示** (R-representation) 或 G 在 R 上的一个表示是指一个群同态:

$$\rho\colon G \to \mathrm{GL}_R(V),$$

其中 V 是一个 R-模, $\mathrm{GL}_R(V)$ 是 V 上所有 R-模自同构 (可逆的 R-模同态) 的集合. 若 $R = F$ 是域, $\mathrm{GL}_F(V)$ 是 V 上所有 F-线性自同构 (即可逆 F-线性变换) 的集合. 群的这种表示称为**线性表示** (linear representation); 若无特殊说明, 群的表示都指线性表示.

设 V 是一个 R-模, 若映射

$$G \times V \to V, \quad (g, v) \mapsto g.v$$

满足对任意 $g, g_1, g_2 \in G, v, v_1, v_2 \in V, r_1, r_2 \in R$ 都有

$$
\begin{aligned}
g.(r_1v_1 + r_2v_2) &= r_1g.v_1 + r_2g.v_2, \\
g_1.(g_2.v) &= (g_1g_2).v, \\
1_G.v &= v,
\end{aligned}
$$

则称上述映射给出了 G **在** R**-模** V **上的一个作用** (action of G on an R-module), 此时也称 V 是 R **上的一个** G**-模** (G-module over R)[10].

请读者验证: **群** G **的** R**-线性表示与** R **上的** G**-模一一对应**.

1.3.2. 设 G 是一个群.

设 V 是一个 R-模. $\mathrm{GL}_R(V)$ 是 $\mathrm{End}_R(V)$ 的一个子集, 因而群的表示 $\rho\colon G \to \mathrm{GL}_R(V)$ 给出一个集合间映射

$$G \to \mathrm{End}_R(V).$$

上述映射左边的群 G 上只有乘法, 为与右边 $\mathrm{End}_R(V)$ 上的加法和数乘对应, 可在 G 的元素上做形式的加法和数乘, 这样就得到所谓的群代数.

在下述形式和

$$\sum_{g\in G} a_g g,\ \ a_g \in R,$$

的集合 RG 上定义加法, R-数乘和乘法如下

$$
\begin{aligned}
\sum_{g\in G} a_g g + \sum_{g\in G} b_g g &= \sum_{g\in G} (a_g + b_g) g, \\
c.\left(\sum_{g\in G} a_g g\right) &= \sum_{g\in G} c a_g g, \\
\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) &= \sum_{g\in G}\left(\sum_{x,y\in G, xy=g} a_x b_y\right) g;
\end{aligned}
$$

则可验证, RG 关于上述运算构成一个 R-代数, 称为群 G 在 R 上的**群代数** (group algebra). 作为 R-模时, RG 是一个自由 R-模且 G 是 RG 的一组 R-基.

给定 G 的一个 R-线性表示

$$\rho\colon G \to \mathrm{GL}_R(V),$$

[10] 即 G 在 R-模上的作用与 R 上的 G-模是等同的概念.

通过线性扩张可得到一个保幺元的 R-代数同态:

$$\tilde{\rho}\colon\ RG \to \mathrm{End}_R(V),\ \sum_{g\in G} a_g g \mapsto a_g\rho(g),$$

也就是群代数 RG 的一个表示. 反之, 给定群代数 RG 的一个表示

$$\tilde{\rho}\colon RG \to \mathrm{End}_R(V),$$

限制到 G 上就得到 G 的一个 R-线性表示 (注意: $\tilde{\rho}$ 保幺元!)

$$\rho = \tilde{\rho}|_G\colon G \to \mathrm{GL}_R(V).$$

因此: **群 G 的 R-线性表示与群代数 RG 的表示一一对应**.

结合 R-代数的表示和模的关系, 可知以下概念之间一一对应:

$$\begin{array}{ccc} G \text{ 的 } R\text{-线性表示} & \Longleftrightarrow & RG \text{ 的表示} \\ \Updownarrow & & \Updownarrow \\ R \text{ 上的 } G\text{-模} & \Longleftrightarrow & RG \text{ 的模} \end{array}$$

我们将根据需要在这几种概念之间自由切换.

1.3.3. 设 G 是一个群, U, V 都是 RG-模, $\rho_U\colon G \to \mathrm{GL}_R(U)$ 和 $\rho_V\colon G \to \mathrm{GL}_R(V)$ 是 U, V 对应的表示, 则

$$\mathrm{Hom}_{RG}(U,V) = \{\sigma \in \mathrm{Hom}_R(U,V) \mid \sigma\circ\rho_U(g) = \rho_V(g)\circ\sigma, \forall g \in G\};$$

特别地, 当 $U = V$ 时有

$$\mathrm{End}_{RG}(V) = \{\sigma \in \mathrm{End}_R(V) \mid \sigma\circ\rho_V(g) = \rho_V(g)\circ\sigma, \forall g \in G\}.$$

1.3.4 例. 设 G 是一个群. 将 R 看成正则 R-模, 则 R-代数同构 $R \cong \mathrm{End}_R(R)$ 诱导群同构

$$R^\times \cong \mathrm{GL}_R(R).$$

所以, G 在 R-模 R 上的表示等同于群同态

$$G \to R^\times.$$

这样的表示称为 G 在 R 上的**秩 1 表示**或 1 **维表示** (特别是当 $R = F$ 为域时).

群 G 必有如下的一维表示[11]:

$$G \to R^{\times},\ g \mapsto 1_R,$$

称为 G 在 R 上的**主表示** (principal representation) 或**平凡表示** (trivial representation), 对应的模称为**平凡模** (trivial module).

若 $R = \mathbb{C}$ 是复数域, 一维表示 $\rho\colon G \to \mathbb{C}^{\times}$ 的取值 $\rho(g), g \in G$ 都是单位根. 当 $G = C_n = \langle g \rangle$ 为 n 阶循环群时, G 在 $\mathbb{C}$ 上的一维表示 ρ 由 $\rho(g) = e^{\frac{2k\pi \mathrm{i}}{n}} (0 \leq k \leq n-1)$ 决定, 因此 n 阶循环群恰有 n 个不同的 1 维 $\mathbb{C}$-表示.

若 $G = \mathcal{S}_n$ 是 n 阶对称群, **符号表示** (sign representation)

$$\mathrm{sign}:\ \mathcal{S}_n \to R^{\times}, \sigma \mapsto \begin{cases} 1, & \sigma \text{ 是偶置换;} \\ -1, & \sigma \text{ 是奇置换,} \end{cases}$$

是一个一维表示.

1.3.5 例. 设 G 是一个群, Ω 是一个 G-集合.

(1) 群 G 在 Ω 上的作用诱导自由 R-模 $R\Omega$ 上的一个 RG-模结构, 在此结构下, 我们称 $R\Omega$ 为 G 的一个**置换模** (permutation module).

(2) 设 $\mathcal{O}$ 是 G 在 Ω 上的一个长度有限的轨道, 令 $\hat{\mathcal{O}} = \sum_{x \in \mathcal{O}} x$, 则 $R\hat{\mathcal{O}} := \mathrm{Span}_R(\hat{\mathcal{O}})$ 是 $R\Omega$ 的一个平凡子模.

(3) $\mathcal{S}_n$ 的自然模.

(4) 当 G 左乘作用在 $\Omega = G$ 时, 所得置换模就是 RG 的正则模, 对应的表示称为 G 在 R 上的**正则表示** (regular representation).

(5) 假设 G 在 Ω 上的作用是传递的, $x \in \Omega$, x 在 G 作用下的稳定化子为 H, 则有 RG-模同构 $R(G/H) \cong R\Omega$.

1.3.6. 设 V 是一个秩为 n 的自由 R-模, 取定 V 的一组 R-基, 则 V 的任意 R-模同态可以用一个 R 上的 n 阶方阵表示, 且这个对应给出 R-代数同构

$$\mathrm{End}_R(V) \cong M_n(R);$$

[11] 任意代数不一定有一维表示.

参见1.2.17. 上述 R-代数同构给出群同构

$$\mathrm{GL}_R(V) \cong \mathrm{GL}_n(R).$$

设 $\rho\colon G \to \mathrm{GL}_R(V)$ 是 G 的一个 R-表示且 V 是秩为 n 的自由 R-模. 取定 V 的一组 R-基, 将 ρ 与上面的同构 $\mathrm{GL}_R(V) \cong \mathrm{GL}_n(R)$ 合成给出 G 的一个所谓**矩阵表示** (matrix representation):

$$X_\rho:\ G \to \mathrm{GL}_n(R).$$

取 V 不同的基, 给出的矩阵表示之间是共轭的, 即若 X'_ρ 是 ρ 的另一个矩阵表示, 则存在可逆矩阵 $T \in \mathrm{GL}_n(R)$ 使得 $X'_\rho(g) = TX_\rho(g)T^{-1}, \forall g \in G$. 反之, 给定 G 的一个矩阵表示 X, 可以构造一个 RG-模 V, 使得 X 是给出 V 的一个矩阵表示. 矩阵表示是给出群的线性表示的常用方法.

1.3.7 例. 设 $G = C_p = \langle g \rangle$ 为 p 阶循环群, F 是一个特征为 p 的域. 则

$$X:\ G \to \mathrm{GL}_2(F),\ g^a \mapsto \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}[12].$$

是 G 的一个矩阵表示.

1.3.8 例. 设 $G = \langle g \mid g^2 = 1 \rangle$ 是二阶循环群, F 是一个特征不为 2 的域, V 是一个 2 维 FG-模, 且在 V 的基 $\varepsilon_1, \varepsilon_2$ 下对应的矩阵表示为

$$X:\ G \to \mathrm{GL}_2(F),\ g \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

请读者验证: V 的全部 FG-子模为 0, $F\varepsilon_1$, $F\varepsilon_2$, V.

[12]这个二阶矩阵中的整数 $1, a$ 看成 $\mathbb{F}_p$ 中的元素

1.3.9 例. 映射

$$\begin{aligned} X\colon\quad \mathcal{S}_3 &\to \mathrm{GL}_2(R)\\ (123) &\mapsto \begin{bmatrix} 0 & -1\\ 1 & -1\end{bmatrix}\\ (12) &\mapsto \begin{bmatrix} 0 & 1\\ 1 & 0\end{bmatrix}\end{aligned}$$

是 $\mathcal{S}_3$ 的一个矩阵表示.

习 题

1.3.1. 设 G 是群, 请验证以下概念之间一一对应: G 的 R-线性表示; R 上的 G-模; RG 的表示; RG 的模.

1.3.2. 将 R 看成正则 R-模, 证明: 有 R-代数同构 $R \cong \mathrm{End}_R(R)$, $r \mapsto (x \mapsto rx)$.

1.3.3. 验证例 1.3.8 中的论断.

1.3.4. 设 $G = \langle x, y \mid x^2 = y^2 = 1 = [x, y]\rangle$ 为 Klein 四群, F 是特征为 2 的无限域. 对任意 $\lambda \in F$, 令 U_λ 是一个 2 维 FG-模且在 U_λ 的基 $\varepsilon_1^\lambda, \varepsilon_2^\lambda$ 下的矩阵表示为

$$X_\lambda\colon\ G \to \mathrm{GL}_2(F),\ x \mapsto \begin{bmatrix} 1 & 1\\ 0 & 1\end{bmatrix},\ y \mapsto \begin{bmatrix} 1 & \lambda\\ 0 & 1\end{bmatrix}.$$

(1) 验证上述 X_λ 确实给出了 FG 的一个矩阵表示.

(2) 求 U_λ 的全部 FG-子模.

(3) 证明: 若 $\sigma\colon U_\lambda \to U_\mu$ 是 FG-模同态, 则 σ 在 U_λ 的基 $\varepsilon_1^\lambda, \varepsilon_2^\lambda$ 和 U_μ 的基 $\varepsilon_1^\mu, \varepsilon_2^\mu$ 下的矩阵必形如 $\begin{bmatrix} a & b\\ 0 & a\end{bmatrix}$, $a, b \in F$.

(4) 证明: 若 $\lambda \neq \mu$, 则 $U_\lambda \ncong U_\mu$, 从而 G 在域 F 上有无限多个不同构的 2 维表示.

1.3.5. 设 p 是素数, F 是特征为 p 的域, $G = \langle g \mid g^p = 1\rangle$ 是 p 阶循环群, V 是 p

维 FG-模且在 V 的基 $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ 下的矩阵表示为

$$X\colon\ G \to \mathrm{GL}_p(F),\ g \mapsto \begin{bmatrix} 1 & 1 & & \\ & 1 & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{bmatrix}.$$

验证上述 X 确实给出了 FG 的矩阵表示, 并求 V 的所有 FG-子模.

第二章　模的基本理论

2.1　直和, 幂等元, 块

本节中我们假设 R 是一个交换幺环, A 是一个 R-代数.

2.1.1. 设 n 个 A-模 $V_1, V_2, \dots, V_n$. 则笛卡尔积

$$V_1 \times V_2 \times \cdots \times V_n = \{(v_1, v_2, \dots, v_n) \mid v_i \in V_i\}$$

关于逐项的加法和 A-作用

$$(v_1, v_2, \dots, v_n) + (v_1', v_2', \dots, v_n') = (v_1 + v_1', v_2 + v_2', \dots, v_n + v_n'),$$
$$a.(v_1, v_2, \dots, v_n) = (av_1, av_2, \dots, av_n),$$

构成一个 A-模 (验证留给读者), 称为 $V_1, V_2, \dots, V_n$ 的**外直和** (external direct sum), 记为 $V_1 \oplus V_2 \oplus \cdots \oplus V_n$.

设 V 是一个 A-模, $V_1, V_2, \dots, V_k$ 是 V 的 A-子模. 如果 $V_1 + V_2 + \cdots + V_k$ 中的任意向量 v 都能唯一地表示为

$$v = v_1 + v_2 + \cdots + v_k \ (v_i \in V_i,\ i = 1, 2, \dots, k),$$

则称 $V_1 + V_2 + \cdots + V_k$ 为 $V_1, V_2, \dots, V_k$ 的**内直和** (internal direct sum), 记为

$$V_1 + V_2 + \cdots + V_k = V_1 \oplus V_2 \oplus \cdots \oplus V_k.$$

请读者验证: $V_1 + V_2 + \cdots + V_k$ 是内直和还有以下两个等价描述:

(1) 0 的表示法唯一, 即由

$$0 = v_1 + v_2 + \cdots + v_k \quad (v_i \in V_i,\ i = 1, 2, \dots, k)$$

可得 $v_1 = v_2 = \cdots = v_k = 0$;

(2) 对任意 $i=1,2,\ldots,k$ 都有 $V_i\cap\left(\sum_{j=1,j\neq i}^{k}V_j\right)=0$.

若 $V_1+V_2+\cdots+V_k$ 是内直和且 $V=V_1+V_2+\cdots+V_k$, 则称 V 可分解为子模 $V_1,V_2,\ldots,V_k$ 的直和, 记为 $V=V_1\oplus V_2\oplus\cdots\oplus V_k$, 并称 V_i 是 V 的**直和项** (direct summand).

前面外直和与内直和用了相同的符号, 事实上两者也可等同起来. 设有 n 个 A-模 $V_1,V_2,\ldots,V_n$, 在外直和 $V_1\oplus V_2\oplus\cdots\oplus V_n$ 中取子模

$$\tilde{V}_i:=\{(v_1,v_2,\ldots,v_n)\in V_1\oplus V_2\oplus\cdots\oplus V_n\mid v_j=0,\forall j\neq i\},$$

则 $V_1\oplus V_2\oplus\cdots\oplus V_n$ 可分解为 $\tilde{V}_1,\tilde{V}_2,\ldots,\tilde{V}_n$ 的内直和. 反过来, 若 A-模 V 可分解为子模 $V_1,V_2,\ldots,V_k$ 的直和 $V=V_1\oplus V_2\oplus\cdots\oplus V_k$, 则 V 同构于 $V_1,V_2,\ldots,V_k$ 的外直和. 验证的细节留给读者. 因此以后不再区分外直和与内直和, 都统称为**直和** (direct sum).

2.1.2. 直和的概念如果推广到任意多个 A-模的情形, 会出现直积与直和两种不同的构造. 首先注意到 A-模 $V_1,V_2,\ldots,V_n$ 的笛卡尔积 $V_1\times V_2\times\cdots\times V_n$ 中的元素 $(v_1,v_2,\ldots,v_n)$ 可等同于函数

$$f\colon\{1,2,\ldots,n\}\to\coprod_{1\le i\le n}V_i,$$

(其中 $\coprod$ 表示集合的无交并), 且这个函数 f 应满足 $f(i)\in V_i$. 直接推广这个构造得到的是直积.

设 $V_i,i\in I$ 是一族 A-模. 则集合

$$\prod_{i\in I}V_i:=\left\{f:I\to\coprod_{i\in I}V_i\mid f(i)\in V_i,\forall i\in I\right\}$$

关于逐项加法和 A-作用

$$\begin{aligned}f+g:\quad & I\to\coprod_{i\in I}V_i,\ i\mapsto f(i)+g(i),\\ af:\quad & I\to\coprod_{i\in I}V_i,\ i\mapsto af(i).\end{aligned}$$

构成一个 A-模 (验证留给读者), 称为 $V_i,i\in I$ 的**直积** (direct product). 读者还

可以验证

$$\bigoplus_{i\in I} V_i = \left\{ f \in \prod_{i\in I} V_i \,\middle|\, \text{只有有限多个 } i \text{ 使得 } f(i) \neq 0 \right\}$$

是 $\prod_{i\in I} V_i$ 的一个子模, 称为 $V_i, i \in I$ 的**外直和** (external direct sum). 当 I 是有限集时, 直积与直和的概念是一样的.

设 V 是一个 A-模, $V_i, i \in I$ 是 V 的一族 A-子模. 如果 $\sum\limits_{i\in I} V_i$ 中的任意向量 v 都能唯一地表示为

$$v = \sum_{i\in I} v_i \ (v_i \in V_i,\ i \in I,\ \text{且只有有限多个 } v_i \text{ 不等于零}),$$

则称 $\sum\limits_{i\in I} V_i$ 为 $V_i, i \in I$ 的**内直和** (internal direct sum), 记为

$$\sum_{i\in I} V_i = \bigoplus_{i\in I} V_i.$$

请读者验证: $\sum\limits_{i\in I} V_i$ 是内直和还有以下两个等价描述:

(1) 0 的表示法唯一, 即由

$$0 = \sum_{i\in I} v_i \ (v_i \in V_i,\ i \in I,\ \text{且只有有限多个 } v_i \text{ 不等于零})$$

可得 $v_i = 0,\ i \in I$;

(2) 对任意 $i \in I$ 都有 $V_i \cap \left(\sum\limits_{i\neq j\in I} V_j \right) = 0$.

若 $\sum\limits_{i\in I} V_i$ 是内直和且 $V = \sum\limits_{i\in I} V_i$, 则称 V 可分解为子模 $V_i, i \in I$ 的直和, 记为 $V = \bigoplus_{i\in I} V_i$, 并称每个 V_i 是 V 的**直和项** (direct summand).

与 I 有限的情况类似地, 在同构意义下, 外直和与内直和可以等同起来, 统称为直和(direct sum).

若 A-模 V 不能分解为若干真子模的直和, 则称 V 是**不可分解**的 (indecomposable). 对表示论中常见的情形, A 的表示可归结为不可分解模的研究. 单模一定是不可分解模, 但不可分解模不一定是单模.

2.1.3 例. 任意自由模都同构于若干个正则模的直和. 事实上, 若 V 是一个自由

A-模, Ω 是 V 的一组基, 则

$$V \cong \bigoplus_{x\in\Omega} A_x,$$

其中 A_x 同构于正则模 A. 当 $|\Omega| = n$ 有限时, 也将上式右边记为 $A\oplus A\oplus\cdots\oplus A$ (n 个 A 的直和), 并简记为 $A^{\oplus n}$ 或 A^n.

2.1.4. 设 V 是一个 A-模, 且 V 有直和分解 $V = U \oplus W$, 其中 U, W 都是 V 的 A-子模. 可以验证映射

$$\mathcal{P}_{U\oplus W\to U}\colon\ V \to V,\ v = u + w(u \in U, w \in W) \mapsto u$$

是一个 A-模同态, 称为 V 关于直和分解 $V = U \oplus W$ 到 U 的**投影映射**.

R-代数 A 中满足 $e^2 = e$ 的元素称为 A 中的**幂等元**. 设 V 是一个 A-模, 则 R-代数 $\mathrm{End}_A(V)$ 中的幂等元也称为**幂等变换**. 可以验证: 上面的 $\mathcal{P}_{U\oplus W\to U}$ 就是幂等变换. 此外, 还可验证: $\mathcal{P}_{U\oplus W\to U}\mathcal{P}_{U\oplus W\to W} = \mathcal{P}_{U\oplus W\to W}\mathcal{P}_{U\oplus W\to U} = 0$.

2.1.5 定理. *设 V 是一个 A-模, $\sigma \in \mathrm{End}_A(V)$. 则 σ 是投影映射当且仅当 σ 是 $\mathrm{End}_A(V)$ 中的幂等元.*

2.1.6. 对 $e \in A$, 若 $e^2 = e$, 则称 e 是 A 的一个**幂等元** (idempotent). 显然 0 和 1 都是幂等元. 当 e 是一个幂等元时, $1-e$ 也是幂等元, 且满足 $e(1-e) = (1-e)e = 0$ 和 $1 = e+(1-e)$, 于是有 $A = Ae\oplus A(1-e)(A = eA\oplus(1-e)A)$, 从而 Ae (eA) 是左 (右) 正则模的直和项. 反之, 正则模 A 的任意直和分解 $A = A_1 \oplus A_2$ 都给出幂等元 e, f 满足 $1 = e + f$ 和 $ef = fe = 0$.

若 A 的两个幂等元 e, f 满足 $ef = fe = 0$, 则称 e, f 是**正交的** (orthogonal). 若干正交幂等元的和仍然是幂等元. 若幂等元 e 不能分解为两个正交非零幂等元之和, 则称 e 是**本原**的 (primitive).

令 e 为一个幂等元, 若 $e = \sum\limits_{i=1}^{n} e_i$ 且 e_i 是两两正交的非零幂等元, 则称 $e = \sum\limits_{i=1}^{n} e_i$ 是 e 的一个**幂等元分解** (idempotent decomposition). 若 e 的正交分解 $e = \sum\limits_{i=1}^{n} e_i$ 中每个 e_i 都是本原的, 则称这个分解是 e 的一个**本原幂等元分解** (primitive idempotent decomposition).

2.1.7 命题. *设 e 是 A 的一个幂等元.*

(1) 映射

$$e = e_1 + e_2 + \cdots + e_n \mapsto Ae = Ae_1 \oplus Ae_2 \oplus \cdots \oplus Ae_n$$

是 e 的所有幂等元分解到 Ae 的所有直和分解的一个一一对应.

(2) e 是本原的当且仅当 Ae 是不可分解的.

(3) 正则模 A 的直和分解与 1_A 的幂等元分解一一对应.

类似的结论对右 A-模 eA 也成立.

2.1.8. 接下来考虑代数的直积 (直和).

设 $A_1, A_2, \ldots, A_n$ 都是 R-代数. 集合

$$A := A_1 \times A_2 \times \cdots \times A_n$$

在逐项加法, 乘法和 R-作用下构成一个 R-代数, 其单位元为 $(1_{A_1}, 1_{A_2}, \ldots, 1_{A_n})$. 上述 R-代数 A 称为 $A_1, A_2, \ldots, A_n$ 的外直积或外直和. 将每个 A_i 都等同为 A 的子集, 则可验证 A_i 是 A 的双边理想. 记

$$b_i = (0, \ldots, 0, 1_{A_i}, 0, \ldots, 0),$$

则 b_i 是 A 的幂等元, $b_i \in Z(A)$, $1_A = b_1 + b_2 + \cdots + b_n$ 且对任意 $i \neq j$ 都有 $b_i b_j = 0$.

类似于模的情形, 对 R-代数 A 的任意双边理想 B, C, 可以定义双边理想的和 $B + C$ 以及双边理想的直和 $B \oplus C$, 且类似的等价条件也成立; 双边理想的和与直和还可以推广到任意有限多个双边理想的情况. 设 R-代数 A 可分解为双边理想 $A_1, A_2, \ldots, A_n$ 的直和:

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_n.$$

令 $1_A = b_1 + b_2 + \cdots + b_n$, 则可验证: b_i 都是 A 的幂等元, $b_i \in Z(A)$ 且对任意 $i \neq j$ 都有 $b_i b_j = 0$. 进一步地, 每个 A_i 都是一个 R-代数, 其单位元为 b_i. 我们称 A 是 $A_1, A_2, \ldots, A_n$ 的内直积或内直和, 并且使用 $A = A_1 \times A_2 \times \cdots \times A_n$ 的符号.

与模的情况类似, 在同构意义下, 我们将代数的外直积 (和) 与内直积 (和) 等同, 简称为直积 (和). 对于代数的情形, 习惯上更倾向于使用直积的术语并使

用 $A_1 \times A_2 \times \cdots \times A_n$ 的符号而不用 $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ 的符号.

2.1.9. A 的中心 $Z(A)$ 的幂等元称为 A 的**中心幂等元** (central idempotent). 对 A 的任意中心幂等元 b, $Ab = bAb = AbA$ 是 A 的双边理想, 同时 Ab 也是一个 R-子代数, 其幺元为 b. 若干正交中心幂等元的和仍是中心幂等元. 若 A 的中心幂等元 b 不能分解为两个正交非零中心幂等元之和, 则称 b 是一个**本原中心幂等元** (primitive central idempotent). 若 A 的中心幂等元 b 可写成 A 的若干正交 (本原) 中心幂等元的和 $b = b_1 + b_2 + \cdots + b_n$, 则这样的分解称为 b 的 **(本原) 中心幂等元分解** ((primitive) central idempotent decomposition).

2.1.10 例. 对 R-代数 $M_n(R)$, I_n 是其单位元. 设

$$e_i = \mathrm{diag}\{0, \ldots, 1, \ldots, 0\}, \text{ (只有第 } i \text{ 个位置为 1, 其余位置都为 0).}$$

则单位元有一个幂等元分解

$$I_n = e_1 + e_2 + \cdots + e_n.$$

以下假设 $R = F$. 则上式还是一个本原幂等元分解, 对应的 $M_n(F)$-模分解为

$$M_n(F) = M_n(F)e_1 \oplus M_n(F)e_2 \oplus \cdots \oplus M_n(F)e_n,$$

其中每个 $M_n(F)e_i$ 都同构于 F^n. 任取可逆矩阵 $u \in M_n(F)$, 则可得到另一个本原幂等元分解

$$I_n = ue_1u^{-1} + ue_2u^{-1} + \cdots + ue_nu^{-1}.$$

注意到 e_i 不是中心幂等元. 事实上, I_n 是 $M_n(F)$ 中唯一的非零中心幂等元, 因而是本原中心幂等元.

2.1.11 引理. *设 b 是 A 的一个中心幂等元. 映射*

$$b = b_1 + b_2 + \cdots + b_n \mapsto Ab = Ab_1 \times Ab_2 \times \cdots \times Ab_n$$

是 b 的所有中心幂等元分解到 Ab 的所有双边理想直积分解的一个一一对应. 特别地, b 是一个本原中心幂等元当且仅当 Ab 作为双边理想是不可分解的.

2.1.12 定理. *设 A 的单位元 1_A 有一个本原中心幂等元分解*

$$1_A = b_1 + b_2 + \cdots + b_n.$$

(1) A *的所有本原中心幂等元为* $b_1, b_2, \cdots, b_n$.
(2) $1_A = b_1 + b_2 + \cdots + b_n$ *是* 1_A *唯一的本原中心幂等元分解.*
(3) A *可唯一地分解为不可分解双边理想的直积*

$$A = Ab_1 \times Ab_2 \times \cdots \times Ab_n.$$

(4) A *的任意中心幂等元都是若干* b_i *的和.*

2.1.13. 设 A 的单位元 1_A 有一个本原中心幂等元分解. 则上述定理中的 Ab_i 称为 A 的**块** (block), b_i 称为块 Ab_i 的**块幂等元** (block idempotent); 也经常将 b_i 称为一个块. A 的分解

$$A = Ab_1 \times Ab_2 \times \cdots \times Ab_n$$

称为 A 的**块分解**.

设 A 有一个块分解 $A = Ab_1 \times Ab_2 \times \cdots \times Ab_n$. 任意 A-模 V 有一个直和分解 $V = b_1V \oplus b_2V \oplus \cdots \oplus b_nV$, 其中每个 b_iV 都可看成 Ab_i-模; 如果存在 $i = 1, 2, \ldots, n$ 使得 $b_iV = V$ 且对任意 $j \neq i$ 都有 $b_jV = 0$, 则称 V 是属于块 Ab_i 的, 并记为 $V \in Ab_i$. 例如, 任意不可分解 A-模都属于 A 的某个块; 特别地, 任意单 A-模都可以看成 A 的某个块的单模. 反过来, 任意 Ab_i 的模也可看成 A 的模. 这样, A 的表示的研究可分解为每个块的表示的研究.

习 题

2.1.1. 请验证 2.1.1 和 2.1.2 中的所有论断.

2.1.2. 证明: 直和满足交换律和结合律, 即对任意 A-模 U, V, W 有

$$U \oplus V \cong V \oplus U, \ (U \oplus V) \oplus W \cong U \oplus (V \oplus W).$$

2.1.3. 设 U_i, $i \in I$ 和 V 都是 A-模, 则有

$$\mathrm{Hom}_A\left(\bigoplus_{i\in I} U_i, V\right) \cong \prod_{i\in I} \mathrm{Hom}_A(U_i, V);$$
$$\mathrm{Hom}_A\left(V, \bigoplus_{i\in I} U_i\right) \cong \prod_{i\in I} \mathrm{Hom}_A(V, U_i).$$

2.1.4. 证明: 单模都是不可分解模. 试举例说明不可分解模不一定是单模.

2.1.5. (**模律** (modular law)) 设 A-模 $V = V_0 + V_1$, 其中 V_0, V_1 都是 V 的子模. 若 U 是 V 的一个子模且满足 $V_0 \subseteq U$, 则有 $U = V_0 + (V_1 \cap U)$; 进一步地, 若 $V = V_0 \oplus V_1$, 则 $U = V_0 \oplus (V_1 \cap U)$.

2.1.6. 设 V 是一个 A-模, 证明以下论断.

(1) 对任意幂等元 $e \in \mathrm{End}_A(V)$, $eV = \mathrm{Im}(e)$ 是 V 的一个 A-子模, 且有

$$V = eV \oplus (1-e)V.$$

(2) 映射

$$\mathrm{Id}_V = e_1 + e_2 + \cdots + e_n \;\mapsto\; V = e_1V \oplus e_2V \oplus \cdots \oplus e_nV$$

是 Id_V 在 $\mathrm{End}_A(V)$ 中的所有幂等元分解到 V 的所有直和分解的一个一一对应.

(3) 有 R-代数同构 $e\,\mathrm{End}_A(V)e \cong \mathrm{End}_A(eV)$.

(4) e 在 $\mathrm{End}_A(V)$ 中本原当且仅当 eV 是不可分解的.

2.1.7. 证明: 习题1.3.4和1.3.5中的模都是不可分解的.

2.2 张量积与双模

本节总假设 R 是一个交换幺环.

2.2.1. 设 A 是一个 R-代数, U 是一个右 A-模, V 是一个 A-模, W 是一个 R-模[1]. 若映射

$$\varphi\colon U \times V \to W$$

满足对任意 $u, u_1, u_2 \in U, v, v_1, v_2 \in V, a \in A$ 和 $r_1, r_2 \in R$ 都有

$$\varphi(r_1u_1 + r_2u_2, v) = r_1\varphi(u_1, v) + r_2\varphi(u_2, v),^{2}$$
$$\varphi(u, r_1v_1 + r_2v_2) = r_1\varphi(u, v_1) + r_2\varphi(u, v_2),$$
$$\varphi(ua, v) = \varphi(u, av),$$

[1] 当 $R = \mathbb{Z}$, 即 A 是一个环时, W 就是一个交换群.

则称 φ 是一个 **A-平衡映射** (A-balanced map). 当 $A=R$ 时, R-平衡映射就是 R-双线性映射, 特别地, 定义中的第三条可由前三条推出.

2.2.2 定义. 设 A 是一个 R-代数, U 是一个右 A-模, V 是一个 A-模. 则 U,V 的**张量积**是一个二元组 (T,φ), 其中 T 是一个 R-模, $\varphi\colon U\times V\to T$ 是一个 A-平衡映射, 且对任意 A-平衡映射 $\psi\colon U\times V\to W$ 都有唯一的 R-模同态 $\psi_0\colon T\to W$ 使得 $\psi=\psi_0\circ\varphi$, 即有如下交换图

$$\begin{tikzcd} & T \arrow[d, "\psi_0"] \\ U\times V \arrow[ur, "\varphi"] \arrow[r, "\psi"'] & W. \end{tikzcd}$$

2.2.3 定理. *设 A 是一个 R-代数, U 是一个右 A-模, V 是一个 A-模. 则 U,V 的张量积存在且在同构的意义下唯一. 进一步地, 若 (T_1,φ_1) 和 (T_2,φ_2) 都是 U,V 的张量积, 则存在唯一的 R-模同构 $\psi\colon T_1\to T_2$ 使得以下图表交换*

$$\begin{tikzcd} & T_1 \arrow[d, "\psi"] \\ U\times V \arrow[ur, "\varphi_1"] \arrow[r, "\varphi_2"'] & T_2. \end{tikzcd}$$

2.2.4. 设 A 是一个 R-代数, U 是一个右 A-模, V 是一个 A-模, (T,φ) 是 U,V 的张量积. 记 $(u,v)(u\in U,v\in V)$ 在映射 φ 下的像为 $u\otimes v$, 在此符号下, 有如下性质

$$\begin{aligned}(r_1u_1+r_2u_2)\otimes v&=r_1(u_1\otimes v)+r_2(u_2\otimes v),\\ u\otimes(r_1v_1+r_2v_2)&=r_1(u\otimes v_1)+r_2(u\otimes v_2),\\ u.a\otimes v&=u\otimes a.v.\end{aligned}$$

特别地, T 上的 R-模结构满足

$$r(u\otimes v)=ru\otimes v=u\otimes rv.$$

由上面定理的证明过程知, T 由元素 $u\otimes v(u\in U,v\in V)$ 生成, 即 T 中元素形如

$$\sum_{i=1}^n u_i\otimes v_i,\quad u_i\in U,v_i\in V.$$

将 φ 称为自然映射, 在不致引起误解时常省略自然映射, 而将 T 称为 U, V 的张量积, 并记为 $U \otimes_A V$.

接下来给出张量积的基本性质. 首先考虑双模的张量积.

2.2.5. 设 A, B 都是 R-代数. 若 V 即是左 A-模又是右 B-模, 满足

$$a(vb) = (av)b, \quad \forall a \in A, b \in B, v \in V,$$

且 A 在 V 上诱导的 R-模结构和 B 在 V 上诱导的 R-模结构相同, 即

$$rv = vr, \quad \forall r \in R, v \in V,$$

则称 V 是一个 (A, B)**-双模** ((A,B)-bimodule). 可类似地定义双模同态和双模同构. 例如, R-代数 A 上的乘法给出 A 上一个 (A, A)-双模结构.

2.2.6 命题. *设 A, B, C 都是 R-代数, U 是 (A, B)-双模, V 是 (B, C)-双模. 则 $U \otimes_B V$ 上有一个 (A, C)-双模结构:*

$$a.(u \otimes v).c = au \otimes vc.$$

2.2.7 命题. *设 A, B 都是 R-代数, V 是一个 (A, B)-双模. 则有 (A, B)-双模同构*

$$A \otimes_A V \cong V, \ a \otimes v \mapsto av,$$
$$V \otimes_B B \cong V, \ v \otimes b \mapsto vb.$$

2.2.8 命题. *设 A, B, C, D 都是 R-代数, U 是一个 (A, B)-模, V 是一个 (B, C)-双模, W 是一个 (C, D)-双模. 则有 (A, D)-双模同构*

$$U \otimes_B (V \otimes_C W) \cong (U \otimes_B V) \otimes_C W, \ u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w.$$

2.2.9 命题. *设 A, B, C 都是 R-代数, $U, U_i, i \in I$ 都是 (A, B)-双模, $V, V_j, j \in J$ 都是 (B, C)-双模. 则有 (A, C)-双模同构*

$$\left(\bigoplus_{i \in I} U_i\right) \bigotimes_B V \cong \bigoplus_{i \in I} (U_i \otimes_B V), \quad U \bigotimes_B \left(\bigoplus_{j \in J} V_j\right) \cong \bigoplus_{j \in J} (U \otimes_B V_j).$$

2.2.10 命题. 设 A 是一个 R-代数, U 是一个右 A-模, V 是一个 A-模. 若 U 是一个自由右 A-模且 $\mathcal{B}$ 是 U 的一组基, 则 $U\otimes_A V$ 的元素可唯一地表示为 $\sum\limits_{i=1}^{n} u_i\otimes v_i$, 其中 $u_i, i=1,2,\ldots,n$ 是 $\mathcal{B}$ 中若干两两不同的元素, $v_i\in V, i=1,2,\ldots,n$. 若 V 是一个自由 A-模, 类似结论成立.

2.2.11 推论. 设 U,V 是两个自由 R-模, $\mathcal{B},\mathcal{C}$ 分别为 U,V 的一组基. 则 $U\otimes_R V$ 也是一个自由 R-模且 $\mathcal{B}\otimes\mathcal{C}=\{x\otimes y\mid x\in\mathcal{B}, y\in\mathcal{C}\}$ 是 $U\otimes_R V$ 的一组基.

2.2.12 推论. 设 S 是 R 的一个子环且 $1_R\in S$. 若 V 是一个自由 S-模且 $\mathcal{B}$ 是 V 的一组 S-基, 则 $R\otimes_S V$ 是一个自由 R-模且 $\{1\otimes x\mid x\in\mathcal{B}\}$ 是 $R\otimes_S V$ 的一组基.

2.2.13. 设 A,B 都是 R-代数.

在张量积 $A\otimes_R B$ 上定义乘法如下 (请读者验证乘法是良定义的):

$$(a_1\otimes b_1)(a_2\otimes b_2)=a_1a_2\otimes b_1b_2.$$

则 $A\otimes_R B$ 关于 R-乘法, 加法和上述乘法构成一个 R-代数.

设 U 是一个 A-模, V 是一个 B-模, 则 $U\otimes_R V$ 上有一个 $A\otimes_R B$-模结构: 对任意 $a\in A, b\in B, u\in U, v\in V$, 定义

$$(a\otimes b)(u\otimes v)=au\otimes bv.$$

2.2.14. 引入反代数的概念, 可将代数的右模看成反代数的左模, 反之亦然; 进一步地, 还可以将双模看成代数张量积的左模.

设 A 是一个 R-代数. A 的**反代数** (opposite algebra) A^{op} 定义如下:

- 作为集合, $A^{\mathrm{op}}=A$;
- A^{op} 的加法和 R-作用与 A 的相同;
- A^{op} 的乘法 $\circ$ 定义为 $a\circ b=ba, a,b\in A^{\mathrm{op}}$.

请读者自己验证, A^{op} 关于加法, R-作用和乘法确实构成一个 R-代数.

设 A 是一个 R-代数, V 是一个 A-模 (右 A-模), 则 V 可看成右 A^{op}-模

(A^{op}-模). 若 U,V 都是右 A-模, 则 U 到 V 所有右 A-模同态构成的集合记为 $\mathrm{Hom}_{A^{\mathrm{op}}}(U,V)$.

若 A,B 都是 R-代数, 则任意 (A,B)-双模 V 上有一个 $A\otimes_R B^{\mathrm{op}}$-模结构: 对任意 $a\in A,b\in B,v\in V$, 定义

$$(a\otimes b).v=a.v.b.$$

反过来, 任意 $A\otimes_R B^{\mathrm{op}}$-模也可看成一个 (A,B)-双模.

一种自然地出现双模的情形如下: 设 A 是一个 R-代数, V 是一个 A-模, $B=\mathrm{End}_A(V)^{\mathrm{op}}$, 则 V 上有一个 (A,B)-双模结构.

2.2.15. 设 A,B,C 都是 R-代数.

设 U 是一个 (A,B)-双模, V 是一个 (A,C)-双模. 则 $\mathrm{Hom}_A(U,V)$ 上有一个 (B,C)-双模结构:

$$b.f.c:\ U\to V,u\mapsto f(ub)c,\quad \forall b\in B,c\in C,f\in\mathrm{Hom}_A(U,V).$$

类似地, 若 U 是一个 (B,A)-双模, V 是一个 (C,A)-双模. 则 $\mathrm{Hom}_{A^{\mathrm{op}}}(U,V)$ 上有一个 (C,B)-双模结构:

$$c.f.b:\ U\to V,u\mapsto cf(bu),\quad \forall b\in B,c\in C,f\in\mathrm{Hom}_A(U,V).$$

2.2.16 定理. *设 A 是一个 R-代数.*

(1) 对任意 A-模 V 都有 A-模同构 $\mathrm{Hom}_A(A,V)\cong V$, $\sigma\mapsto\sigma(1)$.

(2) 有 R-代数同构 $\mathrm{End}_A(A)\cong A^{\mathrm{op}}$, $\sigma\mapsto\sigma(1)$, 其逆映射为 $a\mapsto(x\mapsto xa)$.

2.2.17 定理. *设 A,B,C,D 都是 R-代数, U 是一个 (A,B)-双模, V 是一个 (B,C)-双模, W 是一个 (A,D)-双模. 则有 (C,D)-双模同构*

$$\mathrm{Hom}_A(U\otimes_B V,W)\cong\mathrm{Hom}_B(V,\mathrm{Hom}_A(U,W)),\ \sigma\mapsto(v\mapsto(u\mapsto\sigma(u\otimes v))).$$

2.2.18. 为考虑 Frobenius 互反律, 首先引入更广的限制和诱导概念. 设 $\alpha\colon A\to B$ 是一个保幺元的 R-代数同态.

则任意 B-模 V 都有一个 A-模结构:

$$a.v=\alpha(a)v,\quad \forall a\in A, v\in V,$$

这个模结构称为 V **(经 α) 的限制** (restriction of V via α), 记为 $\mathrm{Res}_\alpha V$ 或在不会引起混淆时记为 $\mathrm{Res}_A^B V$. 类似地, 在右模和双模上也有经 α 的限制. 例如, B 上有一个左 A-模结构, 也有一个右 A-模结构, 还有 (A,B)-双模结构, (B,A)-双模结构, 以及 (A,A)-双模结构. 此外, 有以下的 A-模同构:

$$\mathrm{Res}_A^B V\cong B\otimes_B V\cong \mathrm{Hom}_B(B,V),$$

其中, 第二项和第三项中的 B 分别看成 (A,B)-双模和 (B,A)-双模.

考虑两种特殊 α 下的限制. 首先, 若 A 是 B 的子代数, $1_B\in A$ 且 $\alpha\colon A\to B$ 是 R-代数嵌入, $\mathrm{Res}_A^B V$ 就是将 B 在 V 上的作用限制到子代数 A 上. 反过来, 若 α 是满同态, 则任意 B-模等同于可被 $\mathrm{Ker}\,\alpha$ 零化的 A-模.

设 U 是一个 A-模, 则 $B\otimes_A U$ 上有一个 B-模结构, 称为 U 通过 α 的**诱导**, 记为 $\mathrm{Ind}_\alpha U$ 或在不会引起混淆时记为 $\mathrm{Ind}_A^B U$. 前面群代数模的限制和诱导就是这里的特例, 即考虑的是嵌入 $\alpha\colon RH\to RG$. 除了上面的诱导概念外, 还有**余诱导** (coinduction) 的概念: U 的余诱导模是指 B-模 $\mathrm{Hom}_A(B,U)$ (这里 B 看成一个 (A,B)-双模).

2.2.19 命题. *设 $\alpha\colon A\to B$ 是一个保幺元的 R-代数同态. 则对任意 A-模 U 和 B-模 V 都有*

$$\mathrm{Hom}_B(B\otimes_A U,V)\cong \mathrm{Hom}_A(U,\mathrm{Res}_A^B V);$$
$$\mathrm{Hom}_A(\mathrm{Res}_A^B V,U)\cong \mathrm{Hom}_B(V,\mathrm{Hom}_A(B,U)).$$

习 题

2.2.1. 设 A 是一个 (不一定交换的) R-代数, 则可类似地定义 A 上的矩阵. 记所有 A 上的 $m\times n$ 矩阵的集合为 $M_{m,n}(A)$, 并在 $m=n$ 时记为 $M_n(A)$. 证明: 有 R-代数同构 $M_n(A)^{\mathrm{op}}\cong M_n(A^{\mathrm{op}})$.

2.2.2. 设 R 是任意交换幺环, A 是一个 R-代数, I 是 A 的理想. 证明下述论断.

(1) 可将 A/I-模等同于可被 I 零化的 A-模.

(2) 设 V 是一个 A/I-模, 则 V 作为 A/I-模的子模就是 V 作为 A-模的子模.

(3) 设 V 是一个 A/I-模, 则 V 作为 A/I-模是单的当且仅当 V 作为 A-模是单的.

(4) 设 V 是一个 A/I-模, 则 V 作为 A/I-模是不可分解的当且仅当 V 作为 A-模是不可分解的.

2.2.3. 设 R 是任意交换幺环, G 是一个群, $N \lhd G$.

(1) 证明: 可将 G/N 的 R-表示等同于 N 作用平凡的 G 的 R-表示.

(2) 证明: 若 V 是一个 $R(G/N)$-模, 则 V 作为 $R(G/N)$-模的子模就是 V 作为 RG-模的子模.

(3) 证明: 若 V 是一个 $R(G/N)$-模, 则 V 作为 $R(G/N)$-模是单的当且仅当 V 作为 RG-模是单的.

(4) 证明: 若 V 是一个 $R(G/N)$-模, 则 V 作为 $R(G/N)$-模是不可分解的当且仅当 V 作为 RG-模是不可分解的.

(5) 自然映射

$$\pi\colon\ G \to G/N,\ g \mapsto \bar{g}$$

诱导一个 R-代数同态 (仍记为 π)

$$\pi\colon\ RG \to RG/N.$$

求这个 R-代数同态 π 的核.

2.3 群代数模的构造: 张量积与同态, 限制与诱导

在本节中, 假设 R 是任意交换环.

2.3.1. 若 G, H 都是群, 则有 R-代数 $RG \otimes_R RH$; 这个 R-代数仍是群代数, 事实上, 有 R-代数同构

$$R(G \times H) \cong RG \otimes_R RH, \quad (g, h) \mapsto g \otimes h.$$

所以, 若 V 是一个 RG-模, W 是一个 RH-模, $V \otimes_R W$ 上有一个 $R(G \times H)$-模结构.

设 G 是一个群, V, W 都是 RG-模. 则张量积 $V \otimes_R W$ 上有一个 $RG \otimes_R RG$-模结构. 经 R-代数同态

$$RG \to RG \otimes_R RG, \quad g \mapsto g \otimes g$$

限制可得到 $V \otimes_R W$ 的一个 RG-模结构: 对任意 $v \in V, w \in W$ 和任意 $g \in G$ 有

$$g.(v \otimes w) = gv \otimes gw.$$

2.3.2. 设 G 是一个群. G 的**反群** (opposite group) G^{op} 定义如下:

- 作为集合, $G^{\mathrm{op}} = G$;
- G^{op} 的乘法 $\circ$ 定义为 $g \circ h = hg, g, h \in G^{\mathrm{op}}$.

可验证有 R-代数同构:

$$RG^{\mathrm{op}} \cong (RG)^{\mathrm{op}}.$$

群 G 到 G^{op} 有一个群同构: $g \mapsto g^{-1}$; 这个群同构诱导 R-代数同构:

$$RG \cong RG^{\mathrm{op}}.$$

对任意右 RG-模 V, 经上述 R-代数同构, V 有一个 RG-模结构

$$g.v = v.g^{-1}, \ \forall g \in G, v \in V;$$

反之任意 RG-模也有一个右 RG-模结构.

2.3.3. 设 G, H 都是群. 则任意 (RG, RH)-双模都可以看成一个 $R(G \times H^{\mathrm{op}})$-模; 实际上, (RG, RH)-双模等同于 $RG \otimes_R (RH)^{\mathrm{op}}$-模且 $RG \otimes_R (RH)^{\mathrm{op}} \cong R(G \times H^{\mathrm{op}})$. 当 $G = H$ 时, (RG, RG)-双模 V 上还有一个 RG-模结构, 即可通过 R-代数同态

$$RG \to RG \otimes_R (RG)^{\mathrm{op}}, \quad g \mapsto g \otimes g^{-1},$$

给出 V 上一个 RG-模结构: 对任意 $g \in G, v \in V$ 有

$$g.v = gvg^{-1}.$$

例如, RG 上有左正则 RG-模结构, 右正则 RG-模结构, (RG, RG)-双模结构, 也有如下的 RG-模结构:

$$g.x = gxg^{-1}, \ \forall\, g \in G, \forall\, x \in RG.$$

2.3.4. 设 A 是一个 R-代数, V, W 都是 A-模. 由 2.2.15, $\mathrm{Hom}_R(V, W)$ 上有一个 (A, A)-双模结构: 对任意 $f \in \mathrm{Hom}_R(V, W)$ 和任意 $a, b \in A$ 有

$$a.f.b\colon v \mapsto bf(av);$$

而 V 的**对偶** (dual) $V^* := \mathrm{Hom}_R(V, R)$ 上有一个右 A-模结构: 对任意 $f \in V^*$ 和任意 $a \in A$ 有

$$f.a\colon u \mapsto f(au).$$

设 G 是一个群, 现在考虑 $A = RG$ 的情形. 设 V, W 都是 RG-模. 则 $\mathrm{Hom}_R(V, W)$ 上有一个 (RG, RG)-双模结构. 此外, 将 $\mathrm{Hom}_R(V, W)$ 上的 (RG, RG)-双模结构经 R-代数同态

$$RG \to RG \otimes_R (RG)^\circ, \quad g \mapsto g \otimes g^{-1}$$

限制可得到 $\mathrm{Hom}_R(V, W)$ 上的一个 RG-模结构, 即对任意 $f \in \mathrm{Hom}_R(V, W)$ 和任意 $g \in G$ 有

$$g.f\colon v \mapsto gf(g^{-1}v).$$

实际上, 这是2.3.3的特例 (将2.3.3里的 V 取为这里的 $\mathrm{Hom}_R(V, W)$).

对偶 $V^* := \mathrm{Hom}_R(V, R)$ 上的右 RG-模结构经 R-代数同态

$$RG \to RG^\circ, \quad g \mapsto g^{-1}$$

限制可得到一个 RG-模结构: 对任意 $f \in \mathrm{Hom}_R(U, V)$ 和任意 $g \in G$ 有

$$g.f\colon u \mapsto f(g^{-1}u).$$

对偶 V^* 上的 RG-模结构也可看成上一段 $\mathrm{Hom}_R(V, W)$ 的特例.

注. 当 G 是一个群, V, W 都是 RG-模时, $V \otimes_R W$, $\mathrm{Hom}_R(V, W)$ 和 V^* 上有如上定义的几种模结构; 以后的相关叙述, 读者需注意讨论的是哪种模结构, 有时需从上下文自行判断.

2.3.5 定理. *设 A 是一个 R-代数, U, V 都是 A-模, 且 U, V 至少有一个是有限秩自由 R-模. 则有 (A, A)-双模同构*

$$U^* \otimes_R V \cong \mathrm{Hom}_R(U, V), \; f \otimes v \mapsto (u \mapsto f(u)v).$$

当 G 是一个群且 $A = RG$ 时, 上述同构还是 RG-模同构.

2.3.6. 设 G 是一个群, $H \leq G$. 任意 RG-模 V 都可看成 RH-模, 称为 V 的一个**限制** (restriction), 记为 $\operatorname{Res}_H^G V$. 设 U 是一个 RH-模, 将 RG 看成一个 (RG, RH)-双模, 则 RG-模 $RG \otimes_{RH} U$ 称为 V 的一个**诱导** (induction), 记为 $\operatorname{Ind}_{RH}^{RG} U$, 当 R 固定时, 也简记为 $\operatorname{Ind}_H^G U$. 设 $[G/H]$ 是 H 在 G 的一个左陪集完全代表元集. 则 $[G/H]$ 是 RG 作为自由右 RH-模的一组基. 于是作为 R-模有

$$\operatorname{Ind}_H^G U = RG \otimes_{RH} U = \bigoplus_{g \in [G/H]} g \otimes U,$$

其中 $g \otimes U = \{g \otimes u \mid u \in U\}$ 作为 R-模同构于 U; 进一步地, 若 U 是有限生成自由 R-模, 则

$$\operatorname{rank}_R \left(\operatorname{Ind}_H^G U\right) = |G : H| \operatorname{rank}_R U.$$

在上面的分解下, G 在 $\operatorname{Ind}_H^G U$ 上的作用可以描述如下: 对任意 $x \in G$ 和 $g \otimes u \in g \otimes U$ 有

$$x.(g \otimes u) = g' \otimes hu,$$

其中 $xg = g'h, g' \in [G/H], h \in H$. 于是 G 在集合

$$\{g \otimes U \mid g \in [G/H]\}$$

上有一个作用: $x(g \otimes U) = g' \otimes U$; 这个作用是传递的且 $\operatorname{Stab}_G(1 \otimes U) = H$.

2.3.7 命题. *设 G 是一个群, H 是 G 的一个子群. 若 V 是一个 RG-模且有一个 R-子模 U 使得 V 是 R-子模 $\{gU \mid g \in G\}$ 的直和且 $H = \operatorname{Stab}_G(U)$, 则 $V \cong \operatorname{Ind}_H^G U$.*

2.3.8 例. 设 G 是一个群, Ω 是一个 G-集合, $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$ 是 G 在 Ω 上的全部轨道. 则置换模 $R\Omega$ 可分解为

$$R\Omega = R\mathcal{O}_1 \oplus R\mathcal{O}_2 \oplus \cdots \oplus R\mathcal{O}_k.$$

对任意轨道 $\mathcal{O}_i$, 任取 $\omega \in \mathcal{O}_i$ 并记 $H = \operatorname{Stab}_G(x)$, 则有 $R\mathcal{O}_i \cong \operatorname{Ind}_H^G R$. 于是置换模是若干诱导模的直和. 作为一种特殊情况, 考虑 G 在 $\Omega = G$ 上的左乘作用, 则可得 $RG \cong \operatorname{Ind}_1^G R$.

2.3.9 命题. *设 G 是一个群, $H \leq K \leq G$, V 是一个 RG-模, U 是一个 RH-模,*

则有

$$\operatorname{Ind}_K^G \operatorname{Ind}_H^K U \cong \operatorname{Ind}_H^G U, \quad \operatorname{Res}_H^K \operatorname{Res}_K^G V \cong \operatorname{Res}_H^G V.$$

2.3.10 命题. 设 G 是一个群, $H \leq G$, V 是一个 RG-模, U 是一个 RH-模, 则有

$$\operatorname{Ind}_H^G U \otimes_R V \cong \operatorname{Ind}_H^G (U \otimes_R \operatorname{Res}_H^G V).$$

本节最后介绍诱导与限制的两个重要性质: Frobenius 互反律与 Mackey 公式.

2.3.11 引理. 设 G 是一个群, $H \leq G$. 则对任意 RH-模 U 都有

$$\operatorname{Ind}_H^G U \cong \operatorname{Hom}_{RH}(RG, U).$$

即群代数的诱导和余诱导是同构的.

2.3.12 定理 (Frobenius 互反律)**.** 设 G 是一个群, $H \leq G$, 则对任意 RG-模 V 和任意 RH-模 U, 都有

$$\operatorname{Hom}_{RG}(\operatorname{Ind}_H^G U, V) \cong \operatorname{Hom}_{RH}(U, \operatorname{Res}_H^G V);$$
$$\operatorname{Hom}_{RG}(V, \operatorname{Ind}_H^G U) \cong \operatorname{Hom}_{RH}(\operatorname{Res}_H^G V, U).$$

2.3.13. 设 H, K 都是群, Ω 是一个集合, 若 H 在 Ω 上有一个左作用, K 在 Ω 上有一个右作用, 且满足

$$(h.x).k = h.(x.k), \quad \forall h \in H, k \in K, x \in \Omega,$$

则称 Ω 是一个 (H, K)-**双集** (biset). (H, K)-双集与 $H \times K$-集合一一对应:

$$(h, k).x = h.x.k^{-1}, \quad \forall h \in H, k \in K, x \in \Omega.$$

上述作用下所有轨道的集合记为 $H \backslash \Omega / K$, 任意一个完全代表元集记为 $[H \backslash \Omega / K]$.

设 G 是一个群, H, K 都是 G 的子群. 则群 $H \times K$ 在 G 上有一个作用

$$(h, k).x = hxk^{-1}, \quad \forall h \in H, k \in K, x \in G.$$

这个作用的轨道称为 (H,K)-**双陪集**. 元素 g 所在的双陪集为

$$HgK = \{hgk \mid h \in H, k \in K\}.$$

所有双陪集的集合 $H\backslash G/K$ 构成 G 的一个划分, 任意一个 (H,K)-双陪集完全代表元集记为 $[H\backslash G/K]$.

2.3.14 引理. *设 G 是一个群, H,K 都是 G 的子群.*

(1) H 可通过左乘作用在 G/K 上, 且这个作用所有轨道的集合 $H\backslash(G/K)$ 与 $H\backslash G/K$ 有一个一一对应: $H(gK) \mapsto HgK$.

(2) 在 (1) 中的对应下, 可将 $gK \in G/K$ 在 H 左乘作用下的轨道记为 HgK/K, 且有 H-集合同构

$$HgK/K \cong H/(H \cap {}^gK),$$

从而 HgK 是 $|H : H \cap {}^gK|$ 个 K-左陪集的并.

(3) K 可通过右乘作用在 $H\backslash G$ 上, 且这个作用所有轨道的集合 $(H\backslash G)/K$ 与 $H\backslash G/K$ 有一个一一对应: $(Hg)K \mapsto HgK$.

(4) 在 (3) 中的对应下, 可将 $Hg \in H\backslash G$ 在 K 右乘作用下的轨道记为 $H\backslash GHgK$, 且有右 K-集合同构

$$H\backslash HgK \cong (H^g \cap K)\backslash K,$$

从而 HgK 是 $|K : H^g \cap K|$ 个 H-右陪集的并.

2.3.15 引理. *设 G 是一个群, H,K 都是 G 的子群.*

(1) 作为 (RH,RK)-双模有 $RG = \bigoplus\limits_{g\in[H\backslash G/K]} R[HgK]$.

(2) 有 (RH,RK)-双模同构 $R[HgK] \cong RH \otimes_{R(H\cap {}^gK)} R[gK]$.

2.3.16. 设 G 是一个群, $H \leq G$.

对任意 RH-模 V 和 $g \in G$, V 的**共轭** ${}^gV$ 是一个 $R({}^gH)$-模, 其中 ${}^gV$ 作为 R-模与 V 相同, 而 ${}^gH$ 在 ${}^gV$ 上的作用定义如下:

$${}^gh.v = hv, \quad \forall\, h \in H, v \in V.$$

特别地, 若 $N \lhd G$ 且 V 是一个 RN-模, 则 ${}^gV$ 也是一个 RN-模 (${}^gN = N$), 按照

定义, N 在 ${}^gV$ 上的作用如下:

$$n.v = ({}^{g^{-1}}n)v, \quad \forall\, n \in N, v \in V.$$

在诱导模中, 共轭模会自然地出现. 设 U 是一个 RH-模, 则作为 R-模有

$$\operatorname{Ind}_H^G U = \bigoplus_{g \in [G/H]} g \otimes U.$$

则 $g \otimes U$ 上有一个 $R({}^gH)$-模结构

$${}^gh(g \otimes u) = g \otimes h.U,$$

且有 $R({}^gH)$-模同构 $g \otimes U \cong {}^gU$.

2.3.17 定理 (Mackey 公式)**.** *设 G 是一个群, H, K 都是 G 的子群. 则对任意 RK-模 U 有 RH-模同构*

$$\operatorname{Res}_H^G \operatorname{Ind}_K^G U \cong \bigoplus_{g \in [H\backslash G/K]} \operatorname{Ind}_{H\cap {}^gK}^H \operatorname{Res}_{H\cap {}^gK}^{{}^gK} {}^gU.$$

习 题

以下设 G 是一个有限群.

2.3.1. 对任意 RG-模 V, 记

$$V^G = \{v \in V \mid g.v = v,\ \forall g \in G\}.$$

(1) 证明: 对任意 RG-模 V, V^G 是 V 的一个 R-子模.

(2) 证明: 对任意 RG-模 V, W 有 $\operatorname{Hom}_R(V, W)^G = \operatorname{Hom}_{RG}(V, W)$.

2.3.2. 设 U, V 都是 RG-模, 且 U, V 至少有一个是有限秩自由 R-模, 证明: 有 RG-模同构 $(U \otimes_R V)^* \cong U^* \otimes_R V^*$.

2.3.3. 设 U, V, W 都是 RG-模, 且 U, V, W 都是有限秩自由 R-模, 证明: 有 R-模同构 $\operatorname{Hom}_{RG}(U \otimes_R V, W) \cong \operatorname{Hom}_{RG}(U, V^* \otimes_R W)$.

2.3.4. 设 $H \le G$, U 是一个 RH-模, 证明: 若 U 作为 RH-模可由 d 个元素生成, 则 $\operatorname{Ind}_H^G U$ 作为 RG-模也可由 d 个元素生成.

2.3.5. 设 $H \leq G$, V 是一个 RG-模, U 是一个 RH-模, 证明: 有 RG-模同构

$$\operatorname{Ind}_H^G U^* \cong \left(\operatorname{Ind}_H^G U\right)^*, \quad \operatorname{Res}_H^G V^* \cong \left(\operatorname{Res}_H^G V\right)^*.$$

2.3.6. 对 Frobenius 互反律 2.3.12 的两个同构式, 试分别写出一对具体的同构映射.

2.3.7. 设 $H \leq G$, 记 $[G/H]$ 是 H 在 G 中的一个左陪集完全代表元集, 则

$$\left\{t^{-1} \mid t \in [G/H]\right\}$$

是 H 在 G 中的一个右陪集代表元集.

2.3.8. 设 H, K 都是 G 的子群, $g \in G$. 证明:

$$|G:K| = \sum_{g \in [H\backslash G/K]} |H : H \cap {}^gK|;$$

$$|G:H| = \sum_{g \in [H\backslash G/K]} |K : H^g \cap K|.$$

2.3.9. 设 U 是一个 RG-模, $g \in G$, 证明: ${}^gU \cong U$.

2.3.10. 设 $K \leq H \leq G$, V 是一个 RH-模, U 是一个 RK-模, $g \in G$. 证明:

$$\operatorname{Res}_{{}^gK}^{{}^gH} {}^gV \cong {}^g\left(\operatorname{Res}_K^H V\right), \quad \operatorname{Ind}_{{}^gK}^{{}^gH} {}^gU \cong {}^g\left(\operatorname{Ind}_K^H U\right).$$

2.3.11. 设 $H \leq G$, U 是一个 RH-模, 证明: U 是 $\operatorname{Res}_H^G \operatorname{Ind}_H^G U$ 的一个直和项.

2.3.12. 设 $N \trianglelefteq G$, V 是一个 RN-模, 证明: G 的每个 (N,N)-双陪集都是 N 在 G 中的左陪集, 也是 N 在 G 中的右陪集, 且有

$$\operatorname{Res}_N^G \operatorname{Ind}_N^G V \cong \bigoplus_{g \in [G/N]} {}^gV.$$

2.3.13. 设 $H, K \leq G$ 满足 $G = HK$, 证明: 对任意 RK-模 V 都有

$$\operatorname{Res}_H^G \operatorname{Ind}_K^G V \cong \operatorname{Ind}_{H\cap K}^H \operatorname{Res}_{H\cap K}^K V.$$

2.3.14. 设 $H, K \leq G$, 证明: 对任意 RH-模 U 和 RK-模 V 都有

$$\operatorname{Ind}_H^G U \otimes_R \operatorname{Ind}_K^G V \cong \bigoplus_{t \in [H\backslash G/K]} \operatorname{Ind}_{H\cap {}^tK}^G \left(\operatorname{Res}_{H\cap {}^tK}^H U \otimes_R \operatorname{Res}_{H\cap {}^tK}^{{}^tK} {}^tV\right).$$

2.4 PID 上的有限生成模及应用

本节首先讨论**主理想整环** (principal ideal domain, 简写为 PID) 上有限生成模的结构定理; 然后给出以下三方面的应用: 有限生成交换群的结构, 有限维线性空间上线性变换的结构, 循环 p-群在特征为 p 的域上的不可分解模的分类. 假定读者已掌握主理想整环的基本概念及其上的唯一因子分解定理.

2.4.1 定理. *设 R 是一个主理想整环, V 是一个有限秩自由 R-模. 则 V 的任意 R-子模 U 都是有限秩自由 R-模且 $\mathrm{rank}_R U \le \mathrm{rank}_R V$.*

2.4.2 推论. *设 R 是一个主理想整环, V 是一个 R-模. 若 V 可由 n 个元素生成, 则 V 的任意子模可由不超过 n 个元素生成.*

2.4.3. 设 R 是任意交换幺环, A 是一个 R-代数, V 是一个 A-模. 若 $v \in V$ 满足 $\mathrm{Ann}_A(v) \ne 0$ ($\mathrm{Ann}_A(V)$ 的定义参见 1.2.13), 即存在 $0 \ne a \in A$ 使得 $a.v = 0$, 则称 v 是一个**扭元** (torsion element). 若 R 是整环, 则 R-模 V 中所有扭元组成的集合构成一个 R-子模, 称为 V 的**扭子模** (torsion submodule), 记为 $T(V)$. 若 $T(V) = 0$, 则称 V 是**无扭**的 (torsionless).

2.4.4 定理. *设 R 是一个主理想整环, V 是一个有限生成 R-模.*

(1) V 是自由的当且仅当 V 是无扭的.

(2) $V/T(V)$ 是一个有限秩自由 R-模.

(3) 存在 V 的有限秩自由子模 F 使得 $V = T(V) \oplus F$.

2.4.5. 设 R 是一个交换环, V 是一个 R-模. 对任意 $r \in R$,

$$\mathrm{Ann}_V(r) = \{v \in V \mid r.v = 0\};$$

是 V 的一个子模, 称为 r 的**零化子模** (submodule annihilated by r); 此外, $rV := \{rv \mid v \in V\}$ 也是 V 的一个子模.

设 R 是一个主理想整环, V 是一个 R-模. 对 R 中的素元 p(等价于不可约

元), 记

$$V(p) := \bigcup_{i=1}^{+\infty} \mathrm{Ann}_V(p^i),$$

则 $V(p)$ 是 V 的一个 R-子模; 若 $V = V(p)$, 则称 V 是一个 **p-准素模**.

本节以后的内容中, 我们总假定 R 是一个主理想整环.

2.4.6 命题. *设 V 是一个 R-模. 若 $a = bc \in R$, $b, c \in R$ 且 b 与 c 互素, 则*

$$\mathrm{Ann}_V(a) = \mathrm{Ann}_V(b) \oplus \mathrm{Ann}_V(c).$$

2.4.7 定理. *设 V 是一个有限生成 R-模. 若 $\mathrm{Ann}_R(V) = (r)(r \in R)$ 且*

$$r = up_1^{e_1}p_2^{e_2}\cdots p_s^{e_s},$$

其中, $u \in R^\times$, $p_1, p_2, \ldots, p_s$ 是 R 中两两不相伴的素元, $e_i \in \mathbb{N}$, 则

$$V = \bigoplus_{i=1}^{s} V(p_i),$$

其中 $V(p) = \mathrm{Ann}_V(p_i^{e_i})$.

2.4.8 定理. *设 V 是一个有限生成 R-模.*

(1) V 同构于一个有限生成自由模 F 和若干循环模

$$R/(p_1^{n_{11}}), \ldots, R/(p_1^{n_{1l}}), R/(p_2^{n_{21}}), \ldots, R/(p_2^{n_{2l}}), \ldots, R/(p_k^{n_{k1}}), \ldots, R/(p_k^{n_{kl}})$$

的直和, 其中 $p_1, p_2, \ldots, p_k$ 是两两不相伴的素元, $n_{i1} \geq \cdots \geq n_{il} \geq 0$. 自由模 F 的秩 $\mathrm{rank}_R F$ 和理想 $(p_1^{n_{11}}), \ldots, (p_1^{n_{1l}}), (p_2^{n_{21}}), \ldots, (p_2^{n_{2l}}), \ldots, (p_k^{n_{k1}}), \ldots, (p_k^{n_{kl}})$ 由 V 唯一决定.

(2) V 同构于一个有限生成自由模 F 和若干循环模 $R/(r_1), R/(r_2), \ldots, R/(r_l)$ 的直和, 其中 $r_l \mid r_{l-1} \mid \cdots \mid r_1$. 自由模 F 的秩 $\mathrm{rank}_R F$ 和理想 $(r_1), (r_2), \ldots, (r_l)$ 由 V 唯一决定.

2.4.9. 上述定理称为**主理想整环上有限生成模的结构定理**. 定理中的 $r_1, r_2, \ldots, r_l$

称为 V 的**不变因子**, 而

$$p_1^{n_{11}},\dots,p_1^{n_{1l}},p_2^{n_{21}},\dots,p_2^{n_{2l}},\dots,p_k^{n_{k1}},\dots,p_k^{n_{kl}}$$

称为 V 的**初等因子**. 由中国剩余定理有

$$R/(r_i)\cong R/(p_1^{n_{1i}})\oplus R/(p_2^{n_{2i}})\oplus\cdots\oplus R/(p_k^{n_{ki}}).$$

因此, 不变因子和初等因子之间相互决定 (在忽略相伴意义下), 它们之间的关系由 r_i 的素因子标准分解

$$r_i=u_ip_1^{n_{1i}}p_2^{n_{2i}}\cdots p_k^{n_{ki}},\ i=1,2,\dots,l$$

给出. 上述定理说明主理想整环上有限生成模 V 在同构意义下由自由模 $V/T(V)$ 的秩和 V 的初等因子 (或不变因子) 决定.

2.4.10. 将主理想整环上有限生成模的结构定理应用到 $\mathbb{Z}$-模上, 可以得到有限生成交换群的结构定理: 设 V 是一个有限生成交换群, 则

(1) 有同构

$$V\cong\mathbb{Z}^r\oplus\mathbb{Z}/(p_1^{n_{11}})\oplus\cdots\oplus\mathbb{Z}/(p_1^{n_{1l}})\oplus\cdots\oplus\mathbb{Z}/(p_k^{n_{k1}})\oplus\cdots\oplus\mathbb{Z}/(p_k^{n_{kl}}),$$

其中 $p_1,p_2,\dots,p_k$ 是两两不同的素数, $n_{i1}\geq\cdots\geq n_{il}\geq 0$;

(2) 有同构

$$V\cong\mathbb{Z}^r\oplus\mathbb{Z}/(m_1)\oplus\mathbb{Z}/(m_2)\oplus\cdots\oplus\mathbb{Z}/(m_l),$$

其中 $m_l\mid m_{l-1}\mid\cdots\mid m_1$.

2.4.11. 设 F 是一个域, V 是一个有限维 F-线性空间, $\mathcal{A}\in\mathrm{End}_F(V)$, 则 V 上有一个 $F[x]$-模结构:

$$f(x).v=f(\mathcal{A})(v),\ \forall f(x)\in F[x],v\in V.$$

将主理想整环上有限生成模的结构定理应用到这个模结构上, 就给出线性变换 $\mathcal{A}$ 的结构: V 同构于以下直和

$$F[x]/(p_1(x)^{n_{11}})\oplus\cdots\oplus F[x]/(p_1(x)^{n_{1l}})\oplus\cdots\oplus F[x]/(p_l(x)^{n_{k1}})\oplus\cdots\oplus F[x]/(p_k(x)^{n_{kl}}),$$

其中, $p_1(x),\dots,p_k(x)$ 是两两不同的首一不可约多项式, $n_{i1}\geq\cdots\geq n_{il}\geq 0$; 注意到 V 是有限维的, 所以上述直和中没有自由 $F[x]$-模. 请读者自行写出 V 的初等因子和不变因子.

考查上述分解中的任意直和项 $F[x]/(p_i(x)^{n_{ij}})$. 记

$$f(x) = p_i(x)^{n_{ij}} = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

其中 $n = \deg f(x)$. 于是

$$\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$$

是 $F[x]/(p_i(x)^{n_{ij}})$ 的一组基且有

$$\mathcal{A}(\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}) = (\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}) \begin{bmatrix} 0 & 0 & \cdots & \cdots & -a_0 \\ 1 & 0 & \cdots & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

上式右边的 $n \times n$ 方阵就是 $\mathcal{A}$ 在基 $\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ 下的矩阵, 这个矩阵称为多项式 $f(x)$ 的**有理块**.

对 V 的每个直和项, 都选取如上形式的基, 合起来得到 V 的一组基, 则 $\mathcal{A}$ 在这组基下的矩阵是一个由有理块构成的准对角矩阵, 称为 $\mathcal{A}$ 的**有理标准形**.

2.4.12. 设 F 是一个代数封闭域 (即任意 F 上的多项式都可以分解为一次因式乘积, 例如复数域 $\mathbb{C}$ 就是一个代数封闭域), 则 F 上的不可约多项式都是一次的. 设 V 是 F 上的有限维线性空间, $\mathcal{A} \in \mathrm{End}_F(V)$. 则 V 同构于一个直和

$$F[x]/((x-\lambda_1)^{n_{11}}) \oplus \cdots \oplus F[x]/((x-\lambda_1)^{n_{1l}}) \oplus \cdots \oplus F[x]/((x-\lambda_k)^{n_{k1}}) \oplus \cdots \oplus F[x]/((x-\lambda_k)^{n_{kl}}).$$

考虑其中任意分量; 为方便计, 将其简记为 $F[x]/((x-\lambda)^n)$. 于是

$$\bar{1}, \overline{x-\lambda}, \ldots, \overline{(x-\lambda)^{n-1}}$$

是 $F[x]/((x-\lambda)^n)$(不同于 2.4.11 中) 的一组基且有

$$\mathcal{A}(\bar{1}, \overline{x-\lambda}, \ldots, \overline{(x-\lambda)^{n-1}}) = (\bar{1}, \overline{x-\lambda}, \ldots, \overline{(x-\lambda)^{n-1}}) \begin{bmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & \lambda \end{bmatrix}.$$

上式右边的矩阵称为特征值为 λ 的 n 阶 **Jordan 块**. 令一方面注意到 $\mathcal{A}$ 在基

$\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ 下的矩阵为有理块

$$\begin{bmatrix} 0 & 0 & \cdots & \cdots & -(-\lambda)^n \\ 1 & 0 & \cdots & \cdots & -n(-\lambda)^{n-1} \\ 0 & 1 & 0 & \cdots & -\binom{n}{2}(-\lambda)^{n-2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & n\lambda \end{bmatrix}.$$

上述 Jordan 块和有理块是同一个线性变换在不同基下的矩阵, 因而是相似的.

对 V 的每个直和项, 都选取如上形式的基, 合起来得到 V 的一组基, 则 $\mathcal{A}$ 在这组基下的矩阵是一个由 Jordan 块构成的准对角矩阵, 称为 $\mathcal{A}$ 的 **Jordan 标准形**.

2.4.13 定理. *设 F 是一个域, V 是一个有限维 F-线性空间, 对 $\mathcal{A} \in \mathrm{End}_F(V)$, 以下叙述等价.*

(1) $\mathcal{A}$ 可对角化.

(2) $\mathcal{A}$ 的最小多项式可在 $F[x]$ 中分解为一次因式的乘积且没有重根.

(3) $\mathcal{A}$ 的某个零化多项式可在 $F[x]$ 中分解为一次因式的乘积且没有重根.

2.4.14 (循环 p-群的表示)**.** 设 $P = \langle g \rangle$ 是一个 p^m 阶循环群, F 是一个特征为 p 的域, 我们考虑 P 的 F-表示, 即群代数 FP 的模. 只考虑有限生成模, 这可归结为不可分解模的研究. 定义一个 F-代数同态如下

$$\rho\colon\ F[x] \to FP,\ x \mapsto 1 - g.$$

首先注意到 ρ 是满射, 事实上, $g = \rho(1-x)$, 从而 $g^i = \rho((1-x)^i)$. 于是由同态基本定理知 ρ 诱导一个 F-代数同构

$$\bar{\rho}\colon F[x]/\operatorname{Ker}\rho \cong FP.$$

又注意到 $\rho(x^{p^m}) = (1-g)^{p^m} = 1-g^{p^m} = 0$, 所以 $x^{p^m} \in \operatorname{Ker}\rho$. 而 $\dim_F F[x]/(x^{p^m}) = p^m = \dim_F FP = \dim_F F[x]/\operatorname{Ker}\rho$, 从而 $\operatorname{Ker}\rho = (x^{p^m})$, 于是上面的同构可写为

$$F[x]/(x^{p^m}) \cong FP,\ \bar{x} \mapsto 1 - g.$$

在此同构下, 可将 FP-模等同于 $F[x]/(x^{p^m})$-模. 而在自然同态

$$\pi\colon F[x] \to F[x]/(x^{p^m})$$

下, 任意 $F[x]/(x^{p^m})$-模 V 可看成一个可被 x^{p^m} 零化的 $F[x]$-模; 反过来, 若 $F[x]$-模 V 可被 x^{p^m} 零化, 则 V 也可看成 $F[x]/(x^{p^m})$-模. 所以可将 $F[x]/(x^{p^m})$-模等同于可被 x^{p^m} 零化的 $F[x]$-模, 且若 V 是这样的模, 则 V 作为 $F[x]/(x^{p^m})$-模的子模就是 V 作为 $F[x]$-模的子模, V 作为 $F[x]/(x^{p^m})$-模是单 (不可分解) 的当且仅当 V 作为 $F[x]$-模是单 (不可分解) 的. 应用主理想整环上有限生成模的结构定理, $F[x]$ 的不可分解模必同构于 $F[x]/(g(x))$ 的形式. 若 $F[x]$-模 $F[x]/(g(x))$ 可被 x^{p^m} 零化, 则必有 $g(x) \mid x^{p^m}$. 所以不可分解 $F[x]/(x^{p^m})$-模必同构于以下之一

$$V_1 = F[x]/(x),\ V_2 = F[x]/(x^2),\ \ldots,\ V_{p^m} = F[x]/(x^{p^m}).$$

注意在前面的同构

$$F[x]/(x^{p^m}) \cong FP,\ \bar{x} \mapsto 1 - g$$

下, $g \in P$ 在 V_i 上的作用等于用 $1 - x$ 去乘, 从而 g 在 V_i 的基 $\bar{1}, \bar{x}, \ldots, \bar{x}^{i-1}$ 下的矩阵为

$$\begin{bmatrix} 1 & & & \\ -1 & 1 & & \\ & \ddots & \ddots & \\ & & -1 & 1 \end{bmatrix}_{i\times i}, \quad \text{(其中空白处都为 0)}.$$

习 题

2.4.1. 设 R 是一个主理想整环, 证明: 循环 R-模必形如 $R/(a)\,(a \in R)$ 且

$$\mathrm{Ann}_R(R/(a)) = (a).$$

2.4.2. 设 R 是任意交换幺环, A 是 R-代数, $\alpha\colon U \to V$ 和 $\beta\colon V \to U$ 都是 A-模同态. 证明: 若 $\beta \circ \alpha = \mathrm{Id}_U$, 则 α 是单射, β 是满射, 且有

$$V = \mathrm{Ker}\,\beta \oplus \mathrm{Im}\,\alpha.$$

第三章　半单, 常表示与特征标

本章中若无特殊说明, 总假定 G 是一个有限群.

3.1　半单模与半单代数, Mascheke 定理

本节讨论半单模的定义和性质, 半单代数的定义和结构 (Wedderburn 定理), 这个过程中会给出具有基础性作用的 Schur 引理, 最后给出域上群代数半单的充要条件 (Maschke 定理). 本节中假设 R 是任意交换幺环.

3.1.1 引理. *设 A 是一个 R-代数, V 是一个 A-模, 且 $V = \sum_{i\in I} S_i$, 其中每个 S_i 都是单模. 则对 V 的任意子模 U, 存在 I 的一个子集 I_U 使得*

$$V = U \oplus \left(\bigoplus_{i\in I_U} S_i\right);$$

特别地, V 是若干单模的直和且 V 的任意子模都是 V 的直和项.

3.1.2 定理. *设 A 是一个 R-代数, V 是一个 A-模, 则以下叙述等价.*

(1) V 是若干单模的直和.

(2) V 是若干单模的和.

(3) V 的任意子模都是 V 的直和项.

3.1.3. 设 A 是一个 R-代数, 满足上述定理条件的 A-模称为**半单模** (semisimple module). 由定义立得如下性质:

(1) 半单模的 (直) 和仍是半单模;

(2) 半单模的子模和商模都是半单模.

3.1.4 定理. *设 A 是一个 R-代数, $V=\bigoplus_{i\in I}\left(\bigoplus_{j\in J_i} V_{ij}\right)$ 是一个半单 A-模, 其中 V_{ij} 都是单 A-模且 $V_{ij}\cong V_{i'j'}$ 当且仅当 $i=i'$. 令 $V_i=\bigoplus_{j\in J_i} V_{ij}$ 且 $S_i=V_{i1}$. 则以下成立.*

(1) 有直和分解 $V=\bigoplus_{i\in I} V_i$.

(2) V 的任意单子模 W 都同构于某个 S_i, 且此时 W 包含在 V_i 中. 从而, V_i 是 V 的所有同构于 S_i 的单子模之和.

(3) 对任意 $i\neq j$ 都有 $\mathrm{Hom}_A(V_i,V_j)=0$.

3.1.5. 上述定理中的 V_i 称为 V 的**齐性分支** (homogeneous components), 直和分解 $V=\bigoplus_{i\in I} V_i$ 称为 V 的**齐性分解** (homogeneous decomposition). 由上述定理, 半单模 V 的齐性分解不依赖于 V 分解为单模的直和.

3.1.6 定理 (Schur 引理)**.** *设 A 是一个 R-代数. 对任意单 A-模 S, $\mathrm{End}_A(S)$ 是一个可除 R-代数; 若 T 是一个不同构于 S 的单 A-模, 则 $\mathrm{Hom}_A(S,T)=0$. 进一步地, 若 $R=F$ 是一个代数封闭域, 则 $\mathrm{End}_A(S)\cong F$.*

3.1.7 引理. *设 A 是一个 R-代数, 若 A-模 V 有直和分解 $V=V_1\oplus V_2\oplus\cdots\oplus V_n$ 且对任意 i,j 都有 $V_i\cong V_j$, 则有 R-代数同构 $\mathrm{End}_A(V)\cong M_n(\mathrm{End}_A(V_1))$.*

3.1.8 定理. *设 A 是一个 R-代数, $V=\bigoplus_{i\in I}\left(\bigoplus_{j\in J_i} V_{ij}\right)$ 是一个半单 A-模, 其中 V_{ij} 都是单 A-模且 $V_{ij}\cong V_{i'j'}$ 当且仅当 $i=i'$. 令 $V_i=\bigoplus_{j=1}^{n_i} V_{ij}$. 则 $\mathrm{End}_A(V)=\prod_{i=1}^{m}\mathrm{End}_A(V_i)$ 且 $\mathrm{End}_A(V_i)\cong M_{n_i}(D_i)$, 其中 $D_i=\mathrm{End}_A(V_{i1})$.*

3.1.9 注. 设 A 是一个 R-代数, V 是半单 A-模且 V 可分解为有限多个单模的

直和. 则由上述定理知, 在 V 分解为单模直和的任意分解式中, 同构于给定单模 S 的直和项的个数与 V 的分解式无关, 这个个数称为单模 S 在 V 的**重数**.

3.1.10 定理. *设 A 是一个 R-代数, 以下等价.*

(1) A 作为 A-模是半单的.

(2) 每个 A-模都是半单的.

(3) 每个有限生成 A-模都是半单的.

3.1.11. 满足上述条件的 R-代数称为是**(左) 半单**的 ((left) semisimple). 显然, 半单代数的商代数仍是半单的. 类似可定义右半单, 下面的定理说明左半单和右半单是一样的.

3.1.12 引理. *设 D 是一个可除 R-代数, 则以下结论成立.*

(1) $M_n(D)$ 是一个单 R-代数 (只有 0 和自身两个理想的代数称为单代数), 从而是不可分解 R-代数.

(2) $M_n(D)$ 是半单的且在同构意义下只有唯一单模.

3.1.13 定理. *(Wedderburn-Artin) 设 A 是一个半单 R-代数, 则以下成立.*

(1) 在同构意义下, A 只有有限多个单模 $S_1, S_2, \cdots, S_k$, 记 S_i 对应的齐性分量为 A_i, 则每个 A_i 都是 A 的双边理想, 且有直积分解 $A = A_1 \times A_2 \times \cdots \times A_k$.

(2) $A \cong \prod\limits_{i=1}^{k} M_{n_i}(D_i)$, 其中 $D_i = \mathrm{End}_A(S_i)^{\mathrm{op}}$.

(3) 在 (2) 中的同构下, $A_i \cong M_{n_i}(D_i)$, 从而 $A_1, A_2, \ldots, A_k$ 是 A 的所有块, S_i 可看成 A_i 的唯一单模且 S_i 作为 A_i 和 A 的直和项的重数等于 $n_i = \dim_{D_i} S_i$.

3.1.14 命题. *设 F 是一个代数封闭域, A 是一个有限维半单 F-代数.*

(1) $A \cong \prod\limits_{i=1}^{k} M_{n_i}(F)$, 从而 $\dim_F A = \sum\limits_{i=1}^{k} n_i^2$.

(2) A 任意单模的维数等于其重数, $\dim_F A$ 等于其所有单模维数的平方和.

(3) A 的单模个数等于 $\dim_F Z(A)$, 其中 $Z(A)$ 是 A 的中心.

3.1.15 定理 (Mascheke 定理). 设 F 是一个域, 则群代数 FG 半单当且仅当 $\operatorname{char} F \nmid |G|$.

3.1.16. 常表示与模表示

3.1.17. 设 R 是任意交换环. 对群 G 的任意子集 C, 记 $\hat{C} = \sum\limits_{x \in C} x$ 为 C 中元素在 RG 中的形式和. 当 C 是 G 的共轭类时, $\hat{C}$ 称为一个共轭类和.

3.1.18 命题. 设 R 是一个交换环, 则群代数 RG 的中心 $Z(RG)$ 是一个自由 R-模, 且 G 的共轭类和是 $Z(RG)$ 的一组 R-基. 特别地, 若 F 是一个域, $\dim_F Z(FG)$ 等于 G 的共轭类个数.

3.1.19 定理. 单 $\mathbb{C}G$-模个数等于 G 的共轭类个数.

习 题

3.1.1. 设 A 是一个 R-代数, 证明: $M_n(A)$ 的所有理想都形如 $M_n(I)$, 其中 I 是 A 的理想.

3.1.2. 设 D 是一个可除 R-代数, 证明: $M_n(D)$ 是半单的且在同构意义下只有唯一单模.

3.1.3. 设 D_1, D_2 是两个可除 R-代数, 证明: $M_{n_1}(D_1) \cong M_{n_2}(D_2)$ 的充要条件是 $D_1 \cong D_2$ 且 $n_1 = n_2$.

3.1.4. 设 G 是一个交换群. 证明: $\mathbb{C}G \cong \mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C}$.

3.1.5. 若 $G = \langle g \rangle$ 是一个 n 阶循环群, 证明: $\mathbb{C}G$ 的所有本原中心幂等元为

$$b_k = \frac{1}{n} \sum_{i=0}^{n-1} \zeta^{-ki} g^i, \quad k = 0, 1, \ldots, n-1,$$

其中 $\zeta = e^{\frac{2\pi \mathrm{i}}{n}}$.

3.1.6. 设 $G = \langle g \rangle$ 是一个 3 阶循环群, $\mathbb{R}$ 是实数域, 试求 $\mathbb{R}G$ 的所有单模.

3.1.7. 设 $H \leq G$, F 是一个域且 F 的特征不整除 $|G:H|$, U 是一个 FG-模, V 是一个 FH-模.

(1) 证明: 若 $\mathrm{Res}_H^G U$ 是半单的, 则 U 是半单的.

(2) 证明: 若 V 是半单的且 $H \trianglelefteq G$, 则 $\mathrm{Ind}_H^G V$ 是半单的.

3.2 特征标

3.2.1. 设 $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ 是群 G 的一个复表示, 其中 V 是一个有限维 $\mathbb{C}$-线性空间. 表示 ρ 或 $\mathbb{C}G$-模 V 提供的**特征标** (character)[1]是 G 上的复值函数

$$\chi\colon\ G \to \mathbb{C},\ g \mapsto \mathrm{tr}(\rho(g)),$$

即 $\chi(g)$ 为线性变换 $\rho(g)$ 的迹; 为表达 χ 与 ρ 和 V 的关系, 也将 χ 记为 χ_ρ 或 χ_V. $\mathbb{C}G$-模 V 的维数 $\dim_{\mathbb{C}} V$ 称为特征标 χ 的**次数** (degree); 显然, χ 的次数等于 $\chi(1)$. 单模的特征标称为**不可约特征标** (irreducible character). 不可约特征标对应的表示也称为**不可约表示**. 若 $\mathbb{C}G$ 的所有单模为 $S_1, S_2, \ldots, S_k$, 且其所提供的特征标分别为 $\chi_1, \chi_2, \ldots, \chi_k$, 则有

$$|G| = \sum_{i=1}^{k} \chi_i(1)^2.$$

利用上述公式可找出小阶群的不可约特征标次数, 例如 $\mathcal{S}_4$.

3.2.2 命题. *设 $\rho\colon G \to \mathrm{GL}_{\mathbb{C}}(V)$ 是群 G 的一个复表示, χ 是 ρ 的特征标. 设 $g, h \in G$.*

(1) 若 g 是一个 n 阶元素, 则 $\chi(g)$ 是若干 n 次单位根的和.

(2) $|\chi(g)| \leq \chi(1)$, 且等号成立当且仅当 $\rho(g)$ 是一个数乘.

(3) $\chi(g) = \chi(1)$ 当且仅当 $g \in \mathrm{Ker}\,\rho$.

(4) $\chi(g^{-1}) = \overline{\chi(g)}$ 是 $\chi(g)$ 的复共轭.

(5) $\chi(hgh^{-1}) = \chi(g)$.

3.2.3. 类函数, 类函数空间 $\mathrm{CF}_{\mathbb{C}}(G)$, 这是一个 $\mathbb{C}$-线性空间. 特征标是类函数.

[1]文献中也常将特征标称为指标.

特征标表. 特征标表是一个方形.

3.2.4 例. (1) 1 维表示. 其中平凡模提供的特征标称为**主特征标**, 记为 1_G.
(2) 置换模的特征标.
(3) 正则模 $\mathbb{C}G$ 的特征标为

$$\chi_{\mathbb{C}G}(g) = \begin{cases} |G|, & g = 1; \\ 0, & g \neq 1. \end{cases}$$

(4) $\mathcal{S}_3$ 的一个二维表示.

3.2.5 命题. *设 U, V 都是有限维 $\mathbb{C}G$-模.*
(1) 若 $U \cong V$, 则 $\chi_U = \chi_V$.
(2) 直和 $U \oplus V$ 提供的特征标为 $\chi_U + \chi_V$.
(3) 张量积 $U \otimes_{\mathbb{C}} V$ 提供的特征标为 $\chi_U \cdot \chi_V$.
(4) 对偶模 V^* 提供的特征标 χ_{V^*} 为

$$\chi_{V^*}(g) = \chi_V(g^{-1}) = \overline{\chi_V(g)}, \ \forall\, g \in G.$$

(5) 同态模 $\mathrm{Hom}_{\mathbb{C}}(U, V)$ 提供的特征标为 $\chi_{U^*} \cdot \chi_V$, 即对任意 $g \in G$ 都有

$$\chi_{\mathrm{Hom}_{\mathbb{C}}(U,V)}(g) = \chi_{U^*}(g)\chi_V(g) = \chi_U(g^{-1})\chi_V(g) = \overline{\chi_U(g)}\chi_V(g).$$

3.2.6. 设 $H \leq G$, U 是一个 $\mathbb{C}G$-模, V 是一个 $\mathbb{C}H$-模, 记 U, V 提供的特征标分别为 χ, ψ. 我们将限制模 $\mathrm{Res}_H^G U$ 提供的特征标记为 $\mathrm{Res}_H^G \chi$, 将诱导模 $\mathrm{Ind}_H^G V$ 提供的特征标记为 $\mathrm{Ind}_H^G \psi$. $\mathbb{C}G$-模的一些基本性质可以用特征标的语言来表述.
(1) 设 $H \leq K \leq G$, χ 是某个 $\mathbb{C}G$-模的特征标, ψ 是某个 $\mathbb{C}H$-模的特征标, 则有

$$\mathrm{Ind}_K^G \mathrm{Ind}_H^K \psi = \mathrm{Ind}_H^G \psi, \quad \mathrm{Res}_H^K \mathrm{Res}_K^G \chi = \mathrm{Res}_H^G \chi.$$

(2) 设 $H \leq G$, χ 是某个 $\mathbb{C}G$-模的特征标, ψ 是某个 $\mathbb{C}H$-模的特征标, 则有

$$\left(\mathrm{Ind}_H^G \psi\right) \chi = \mathrm{Ind}_H^G \left(\psi \,\mathrm{Res}_H^G \chi\right).$$

(3) (Mackey 公式) 设 $H, K \leq G$, V 是一个 $\mathbb{C}G$-模且其提供的特征标为 ψ, 则有

$$\mathrm{Res}_H^G \mathrm{Ind}_K^G \psi = \sum_{t \in [H\backslash G/K]} \mathrm{Ind}_{H\cap {}^tK}^H \mathrm{Res}_{H\cap {}^tK}^{{}^tK} {}^t\psi,$$

其中 ${}^t\psi$ 是 $\mathbb{C}{}^tK$-模 ${}^tV$ 的特征标.

下面给出诱导特征标的计算方法.

3.2.7 命题. 设 $H \leq G$, V 是一个 $\mathbb{C}H$-模, 且 V 提供特征标 χ, 则

$$(\mathrm{Ind}_H^G \chi)(g) = \sum_{t \in [G/H]} \chi^\circ(t^{-1}gt) = \frac{1}{|H|} \sum_{t \in G} \chi^\circ(t^{-1}gt),$$

其中 $\chi^\circ(g) = \begin{cases} \chi(g), & g \in H; \\ 0, & g \notin H. \end{cases}$

为给出 Frobenius 互反律的特征标版本, 需要一些准备工作.

3.2.8. 设 R 是一个交换环, U 是 RG-模. 记 U 在 G 下的不动点集为 $U^G = \{u \in U \mid gu = u, \forall g \in G\}$, 即 U^G 是 U 中最大的平凡 RG-子模.

3.2.9 命题. 设 R 是一个交换环且 $|G|$ 在 R 中可逆, U 是一个 RG-模. 则群代数中的元素 $\frac{1}{|G|}\sum\limits_{g \in G} g$ 在 U 上的作用

$$\frac{1}{|G|}\sum_{g \in G} g\colon\ U \to U,\ u \mapsto \frac{1}{|G|}\sum_{g \in G} gu$$

是一个 RG-模同态且是 U 到 U^G 的投影, 从而 U^G 是 U 作为 RG-模的直和项. 当 $R = \mathbb{C}$ 时, 有

$$\mathrm{tr}_U\left(\frac{1}{|G|}\sum_{g \in G} g\right) = \dim_{\mathbb{C}} U^G.$$

3.2.10. 类函数空间上的一个内积 $\langle \chi, \psi \rangle_G$ 如下

$$\langle \chi, \psi \rangle = \frac{1}{|G|}\sum_{g \in G} \overline{\chi(g)}\psi(g).$$

上述内积对第二个变量是线性的, 对第一个变量是共轭线性的, 还满足共轭对称性. $\langle \chi\phi, \psi \rangle_G = \langle \chi, \phi^*\psi \rangle_G$. 对任意特征标 χ, ψ, $\langle \chi, \psi \rangle_G$ 是实数.

3.2.11 命题. 设 R 是一个交换环, U,V 都是 RG-模. 则

$$\mathrm{Hom}_R(U,V)^G = \mathrm{Hom}_{RG}(U,V),$$

且当 $R=\mathbb{C}$ 时, 有

$$\mathrm{tr}_{\mathrm{Hom}_{\mathbb{C}}(U,V)}\left(\frac{1}{|G|}\sum_{g\in G} g\right) = \dim_{\mathbb{C}} \mathrm{Hom}_{RG}(U,V),$$

且若 U,V 提供的特征标分别为 χ,ψ, 则有

$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}G}(U,V) = \langle \chi,\psi\rangle.$$

3.2.12 定理 (Frobenius 互反律)**.** 设 $H\le G$, χ 是某个 $\mathbb{C}G$-模的特征标, ψ 是某个 $\mathbb{C}H$-模的特征标, 则有

$$\langle \mathrm{Ind}_H^G \psi,\chi\rangle_G = \langle \psi, \mathrm{Res}_H^G \chi\rangle_H;$$
$$\langle \mathrm{Res}_H^G \chi,\psi\rangle_G = \langle \chi, \mathrm{Ind}_H^G \psi\rangle_H.$$

习 题

3.2.1. 设 R 是任意交换幺环, 记所有 G 到 R 的类函数构成的集合为 $\mathrm{CF}_R(G)$. 对 G 的任意共轭类 C, 定义

$$\chi_C\colon\ G\to R,\ g\mapsto \begin{cases} 1, & g\in C;\\ 0, & g\notin C.\end{cases}$$

(1) 证明: $\chi_C\in \mathrm{CF}_R(G)$.

(2) 证明: 若 G 的全部共轭类为 $C_1,C_2,\dots,C_k$, 则 $\chi_{C_1},\chi_{C_2},\dots,\chi_{C_k}$ 是 $\mathrm{CF}_R(G)$ 的一组 R-基, 从而 $\mathrm{CF}_R(G)$ 是一个自由 R-模.

3.2.2. 设 K 是一个域, V 是一个有限维 K-线性空间, $\varepsilon_1,\varepsilon_2,\dots,\varepsilon_n$ 是 V 的一组基. 设 $\mathcal{A}\in \mathrm{End}_K(V)$ 在基 $\varepsilon_1,\varepsilon_2,\dots,\varepsilon_n$ 下的矩阵为 A. 证明: $\mathcal{A}$ 的对偶变换

$$\mathcal{A}^*\colon\ V^*\to V^*,\ f\mapsto f\circ\mathcal{A}$$

在 V^* 的对偶基 $\varepsilon_1^*,\varepsilon_2^*,\dots,\varepsilon_n^*$ 下的矩阵为 A^t.

3.2.3. 设 G 是一个群.

(1) 对 $g \in G$, 证明: $g \in Z(G)$ 当且仅当对 G 的任意不可约特征标 χ 都有 $|\chi(g)| = \chi(1)$.

(2) 证明: 若 G 有一个忠实的单复表示, 则 G 的中心是循环的.

3.2.4. [1, p.52, 7].

3.3 正交关系与中心幂等元

3.3.1 定理 (第一正交关系)**.** 设 S,T 是两个单 $\mathbb{C}G$-模, 则

$$\langle \chi_S, \chi_T \rangle = \begin{cases} 1, & 若\ S \cong T; \\ 0, & 否则. \end{cases}$$

3.3.2 推论. 所有不可约特征标构成类函数空间的一组基.

3.3.3 推论. 设 $S_1, S_2, \ldots, S_k$ 是所有不同构的单 $\mathbb{C}G$-模. 设 V 是一个有限维 $\mathbb{C}G$-模, 则 $\langle \chi_V, \chi_{S_i} \rangle$ 等于 S_i 在 V 中的重数.

3.3.4 注. 设 $S_1, S_2, \ldots, S_k$ 是所有不同构的单 $\mathbb{C}G$-模, $\chi_1, \chi_2, \ldots, \chi_k$ 为对应的不可约特征标. 由 §3.1 的结果知道, S_i 在 $\mathbb{C}G$ 中的重数等于 $\dim_{\mathbb{C}} S_i$. 用特征标的语言可将这个结果重新叙述为:

$$\langle \chi_{\mathbb{C}G}, \chi_i \rangle = \chi_i(1), \quad \chi_{\mathbb{C}G} = \sum_{i=1}^{k} \chi_i(1)\chi_i, \quad |G| = \sum_{i=1}^{k} \chi_i(1)^2.$$

3.3.5 推论. 设 U,V 是两个 $\mathbb{C}G$-模, 则 $U \cong V$ 当且仅当 $\chi_U = \chi_V$.

3.3.6 推论. 设 U,V 是两个 $\mathbb{C}G$-模. 则 $\langle \chi_U, \chi_V \rangle$ 是一个非负整数, $\langle \chi_V, \chi_V \rangle$ 是一个正整数, 且 $\langle \chi_V, \chi_V \rangle = 1$ 当且仅当 V 是单模.

3.3.7 推论 (第二正交关系)**.** 设 $\chi_1, \chi_2, \ldots, \chi_k$ 是 G 的所有不可约特征标, 则对

任意 $g, h \in G$ 都有

$$\sum_{i=1}^{k} \chi_i(g)\overline{\chi(h)} = \begin{cases} |C_G(g)|, & \text{若 } g, h \text{ 共轭;} \\ 0, & \text{否则.} \end{cases}$$

3.3.8 例. 运用第二正交关系计算最后一个不可约特征标.

接下来计算群代数的中心幂等元.

3.3.9. 设 $\rho_1, \rho_2, \ldots, \rho_k$ 是 G 的全部不可约表示, 其次数分别为 $n_1, n_2, \ldots, n_k$. 对每个 $i = 1, 2, \ldots, k$, 表示 $\rho_i \colon G \to \mathrm{GL}_{n_i}(\mathbb{C})$ 都可以扩充为一个代数同态

$$\rho_i\colon\ \mathbb{C}G \to M_{n_i}(\mathbb{C}).$$

在差一个表示同构的意义下, 代数同态 ρ_i 与同构

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$$

合成后的映射

$$\tilde{\rho}_i\colon\ M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C}) \to M_{n_i}(\mathbb{C})$$

就是到第 i 个分量的投影. 设不可约表示 ρ_i 对应的中心幂等元为 e_i, 则 e_i 由以下性质决定

$$\rho_i(e_i) = I_{n_i}, \quad \rho_j(e_i) = 0,\ \forall j \neq i.$$

3.3.10 命题. 设 ρ 是 G 的不可约表示, 其提供的不可约特征标为 χ. 则对任意 $x \in Z(\mathbb{C}G)$ 有

$$\rho(x) = \frac{\mathrm{tr}(\rho(x))}{\chi(1)} \cdot I_{\chi(1)};$$

进一步地, 若 $x = \sum\limits_{g \in G} a_g g$, 则

$$\rho(x) = \frac{\sum\limits_{g \in G} a_g \chi(g)}{\chi(1)} \cdot I_{\chi(1)}.$$

3.3.11 定理. 设 $\chi_1, \chi_2, \ldots, \chi_k$ 是 G 的全部不可约特征标, 对应的本原中心幂等

元分别为 $e_1, e_2, \ldots, e_k$, 则有

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g.$$

习 题

3.3.1. [1, p.51, 4].

3.3.2. [1, p.51, 3].

3.3.3. [1, p.51, 5].

3.3.4. [1, p.52, 8].

3.3.5. [1, pp.52–53, 9].

3.3.6. [1, p.53, 11].

3.3.7. 设 Ω 是 G-集合.

(1) 证明: 若 G 在 Ω 上的作用是传递的, 则平凡 $\mathbb{C}G$-模在置换模 $\mathbb{C}\Omega$ 中的重数为 1.

(2) 证明: G 在 Ω 上的轨道数量等于平凡 $\mathbb{C}G$-模在置换模 $\mathbb{C}\Omega$ 中的重数, 即

$$|G \backslash \Omega| = \langle \chi_{\mathbb{C}\Omega}, 1_G \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\mathbb{C}\Omega}(g) = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_\Omega(g)|.$$

3.3.8. 设 Ω 是传递的 G-集合, $|\Omega| > 1$, 若对任意 $\omega_1 \neq \omega_2$ 和任意 $\omega_1' \neq \omega_2'$ 都存在 $g \in G$ 使得 $g.(\omega_1, \omega_2) = (\omega_1', \omega_2')$, 则称 G 在 Ω 上是 **2-传递的**. 证明: G 在 Ω 上的作用是 2-传递的当且仅当 G 在 Ω 上是传递的且对任意 $\omega \in \Omega$, $\operatorname{Stab}_G(\omega)$ 在 $\Omega - \{\omega\}$ 上都是传递的.

3.3.9. 设 Ω 是传递的 G-集合. 证明: 置换模 $\mathbb{C}\Omega$ 有 $\mathbb{C}G$-模直和分解

$$\mathbb{C}\Omega \cong \mathbb{C} \oplus V,$$

其中 $\mathbb{C}$ 是 G 的平凡模; 且若 $|\Omega| \geq 2$, 则 V 是单 $\mathbb{C}G$-模当且仅当 G 在 Ω 上是 2-传递的.

3.3.10. 考虑对称群 $\mathcal{S}_n$ 在集合 $\Omega = \{1, 2, \ldots, n\}$ 上的自然作用. 证明: 置换 $\mathbb{C}\mathcal{S}_n$-模 $\mathbb{C}\Omega$ 可分解为

$$\mathbb{C}\Omega \cong \mathbb{C} \oplus V,$$

其中 $\mathbb{C}$ 是 $\mathcal{S}_n$ 的平凡模且 V 是一个单 $\mathbb{C}\mathcal{S}_n$-模.

3.4 整性与不可约特征标次数

3.4.1. 设 S 是一个含幺交换环, R 是 S 的子环且 $1_S \in R$. 对 $s \in S$, 若存在首一多项式 $f(x) \in R[x]$ 使得 $f(s) = 0$, 则称 s 是 R 上的**整元素** (integral element), 此时我们也说 s 是 R **上整的**或 s **在** R **上整** (integral over R). 若 S 中所有元素都是 R 上的整元素, 则称 S 是 R **上整的** (integral over R). 在 $\mathbb{Z}$ 上整的复数称为**代数整数**, 例如单位根都是代数整数.

3.4.2 命题. *设 S 是一个含幺交换环, R 是 S 的子环且 $1_S \in R$. 对 $s \in S$, 以下条件等价.*

(1) s 是 R 上的整元素.

(2) $R[s]$ 是有限生成 R-模.

(3) S 有子环 T 满足 $R[s] \subseteq T$ 且 T 作为 R-模是有限生成的.

(4) 存在一个忠实的 $R[s]$-模 V 且 V 作为 R-模是有限生成的.

3.4.3 推论. *设 S 是一个含幺交换环, R 是 S 的子环且 $1_S \in R$. 则 S 中在 R 上整的元素关于加法, 减法和乘法封闭, 从而 S 中所有在 R 上整的元素构成 S 的一个包含 R 的子环 (称为 R 在 S 中的**整闭包**).*

3.4.4 命题. *$\mathbb{Z}$ 在 $\mathbb{Q}$ 中的整闭包就是 $\mathbb{Z}$, 即在 $\mathbb{Z}$ 上整的有理数就是整数. (因此, 整数又称为有理整数.)*

3.4.5 命题. *对 G 的任意特征标 χ 和任意 $g \in G$, $\chi(g)$ 都是代数整数.*

3.4.6. 将群代数 $\mathbb{Z}G$ 看成 $\mathbb{C}G$ 的子环. 以后将 $\mathbb{Z}$ 与 $\mathbb{Z} \cdot 1_G$ 等同, 看成是 $\mathbb{Z}G$ 和

$\mathbb{C}G$ 的交换子环. 此外还可以将 $\mathbb{C}$ 与 $\mathbb{C}\cdot 1_G$ 等同, 看成 $\mathbb{C}G$ 的交换子环, 这个子环包含 $\mathbb{Z}\cdot 1_G$.

3.4.7 命题. *群代数 $\mathbb{Z}G$ 的含有 1_G 的交换子环都是 $\mathbb{Z}$ 上整的; 特别地, 中心 $Z(\mathbb{Z}G)$ 在 $\mathbb{Z}$ 上整.*

3.4.8 推论. *设 $C_1, C_2, \ldots, C_k$ 是 G 的全部共轭类. 则对任意代数整数 $\lambda_1, \lambda_2, \ldots, \lambda_k$, $\sum_{i=1}^{k} \lambda_i \hat{C}_k \in Z(\mathbb{C}G)$ 都是 $\mathbb{Z}$ 上整的.*

3.4.9 注. 环同态下的整元素.

3.4.10 定理. *G 的任意不可约特征标次数都整除 $|G|$.*

3.5 特征标表的例子

3.5.1 引理. *设 G 是一个群, 则 G 是交换群当且仅当所有单 $\mathbb{C}G$-模都是一维的.*

3.5.2 例. 循环群

3.5.3 定理. *设 G, H 都是群, $S_1, S_2, \ldots, S_k$ 是 $\mathbb{C}G$ 的全部不同构单模, $T_1, T_2, \ldots, T_l$ 是 $\mathbb{C}H$ 的全部不同构单模, 则 $S_i \otimes_{\mathbb{C}} T_j (i = 1, 2, \ldots, k, j = 1, 2, \ldots, l)$ 是 $\mathbb{C}(G \times H)$ 的全部不同构单模, 且 $S_i \otimes_{\mathbb{C}} T_j$ 提供的特征标为*

$$\chi_{S_i \otimes_{\mathbb{C}} T_j} \colon\ G \times H \to \mathbb{C},\ (g, h) \mapsto \chi_{S_i}(g)\chi_{T_j}(h).$$

3.5.4 例. $C_2 \times C_2$.

3.5.5. 设有群同态 $\alpha \colon G \to H$. 若有 H 的表示 $\rho \colon H \to \mathrm{GL}_R(V)$, 则合成 $\rho \circ \alpha \colon G \to \mathrm{GL}_R(V)$ 是 G 的一个表示, 称为 ρ 的一个**提升** (lift or inflation).

3.5.6 命题. 设 G 是群, G' 是 G 的导群, 则 G 的一维复表示就是 G/G' 的不可约表示的提升.

3.5.7 例. D_8 和 Q_8.

3.5.8 猜想. *Huppert* 猜想.

习 题

3.5.1. 设 $C_1, C_2, \ldots, C_k$ 是群 G 的全部共轭类, $D_1, D_2, \ldots, D_l$ 是群 H 的全部共轭类, 证明:

$$C_i \times D_j,\ i = 1, 2, \ldots, k,\ j = 1, 2, \ldots, l$$

是群 $G \times H$ 的全部共轭类.

3.6 Burnside $p^a q^b$ 定理

3.6.1 引理. 设 χ 是 G 的不可约特征标, C 是 G 的共轭类, $x \in C$, 则 $\frac{|C|\chi(x)}{\chi(1)}$ 是代数整数.

3.6.2 引理. 设 ρ 是 G 的不可约复表示, χ 是由 ρ 提供的特征标, C 是 G 的共轭类且满足 $(\chi(1), |C|) = 1$. 则对 $x \in C$, $\rho(x)$ 是数乘变换或 $\chi(x) = 0$.

3.6.3 引理. 设 ρ 是 G 的复表示, 则

$$Z_\rho(G) := \{g \in G \mid \rho(g) \text{ 是数乘变换.}\}$$

是 G 的正规子群.

3.6.4 引理. 设 G 是非交换单群, 则平凡表示是 G 唯一的一维表示, 且若 ρ 是 G 的非平凡不可约复表示, 则 $Z_\rho(G) = 1$.

3.6.5 引理. 设 G 是非交换单群, C 是 G 的任意非平凡共轭类, 则 $|C|$ 不是素数的方幂.

3.6.6 定理 (Burnside)**.** 设 $|G| = p^a q^b (p, q$ 都是素数$)$, 则 G 可解.

参考文献

[1] P. Webb, A Course in Finite Group Representation Theory, Cambridge University Press 2016.