学科与专题介绍

有限群 (V)

Jean-Pierre Serre

第七章 转移

7.1 定义

设 G 为群，H 为 G 中具有有限指标的子群，$X=G/H$ 是 H 左陪集的集合. 对每个 $x\in X$, 在 G 中选取 x 的代表元 $\bar{x}$. 群 G 作用在 X 上. 若 $s\in G$ 而 $x\in X$, G 中元素 $s\bar{x}$ 在 X 中的象就是 sx. 若 $\overline{sx}$ 表示 sx 的代表元，则有 $h_{s,x}\in H$ 使 $s\bar{x}=\overline{sx}h_{s,x}$. 令

$$\mathrm{Ver}(s)=\prod_{x\in X}h_{s,x}\ \ (\mathrm{mod}(H,H)),$$

其中乘积是在群 $H^{ab}=H/(H,H)$ 中来计算的.

定理 7.1 (Schur) 上面定义的映射 $\mathrm{Ver}: G\to H^{ab}$ 是同态，而且它不依赖于代表元组 $\{\bar{x}\}_{x\in X}$ 的选取.

先来证明映射 Ver 的定义没有歧义. 为此，设 $\{\bar{x}'\}_{x\in X}$ 是另一组代表元，来计算由 $\bar{x}'$ 决定的乘积 $\mathrm{Ver}'(s)$. 元素 $\bar{x}'\in G$ [1] 在 X 中的象为 x, 因此存在 $h_x\in H$ 使 $\bar{x}'=\bar{x}h_x$. 由于

$$\begin{aligned}s\bar{x}'&=s\bar{x}h_x=\overline{sx}h_{s,x}h_x\\&=\overline{sx}h_{sx}h_{sx}^{-1}h_{s,x}h_x\\&=(\overline{sx})'h_{sx}^{-1}h_{s,x}h_x,\end{aligned}$$

又由于 H^{ab} 是交换群，从而 [2]

$$\begin{aligned}\mathrm{Ver}'(s)&=\prod h_{sx}^{-1}h_{s,x}h_x\ \ (\mathrm{mod}(H,H))\\&=(\prod h_{sx})^{-1}\prod h_{s,x}\prod h_x\ \ (\mathrm{mod}(H,H)),\end{aligned}$$

然而，当 x 取遍 X 时，sx 也取遍 X, 故 $\prod h_{sx}=\prod h_x$, 从而

$$\mathrm{Ver}'(s)=\prod h_{s,x}=\mathrm{Ver}(s)\ \ (\mathrm{mod}(H,H)),$$

所以映射 Ver 的定义没有歧义.

现在来证明它是一个同态. 设 $s,t\in G$, 则

$$st\bar{x}=s\overline{tx}h_{t,x}=\overline{stx}h_{s,tx}h_{t,x},$$

原题: Groupes Finis. 译自: http://arxiv.org/math.GR/0503154.

1) 原文为 $\bar{x}'\in X$.—— 译注

2) 下面用了简化记号，所有乘积都是对 $x\in X$ 来求的.—— 译注

由于 H^{ab} 是交换群，从而

$$\begin{aligned}\mathrm{Ver}(st) &= \prod h_{s,tx}h_{t,x} \ (\mathrm{mod}(H,H)) \\ &= \prod h_{s,tx}\prod h_{t,x} \ (\mathrm{mod}(H,H)).\end{aligned}$$

然而，当 x 取遍 X 时，tx 也取遍 X，故 $\prod h_{s,tx}=\prod h_{s,x}$. 从而 $\mathrm{Ver}(st)=\prod h_{s,x}\prod h_{t,x}=\mathrm{Ver}(s)\mathrm{Ver}(t)\ (\mathrm{mod}(H,H))$. ■

由于 H^{ab} 是交换群，同态 Ver 诱导了 G^{ab} 到 H^{ab} 的一个同态 (还记作 Ver)，称为 **转移**.

注 对于同构来说，转移是一个 *函子*，就是说，如果 σ 是群对 (G,H) 到群对 (G',H') 上的同构，则下图交换：

$$\begin{array}{ccc} G^{ab} & \xrightarrow{\ \sigma\ } & G'^{ab} \\ {\scriptstyle \mathrm{Ver}}\downarrow & & \downarrow{\scriptstyle \mathrm{Ver}} \\ H^{ab} & \xrightarrow[\ \sigma\ ]{} & H'^{ab} \end{array}$$

(只须证明，若 $\{\bar{x}\}$ 是 G/H 的代表元组，则 $\{\sigma(\bar{x})\}$ 是 G'/H' 的代表元组.)

特别，若取 $G=G'$, $H=H'$ 以及 $\sigma(x)=gxg^{-1}$，其中 $g\in N_G(H)$，这证明了同态 $\mathrm{Ver}: G^{ab}\to H^{ab}$ 的象集包含于 H^{ab} 中在 $N_G(H)$ 作用下不变的元素所组成的集合内.

7.2 转移的计算

设 H 是 G 的有限指标子群，令 $X=G/H$. 元素 $s\in G$ 作用在 X 上，设 C 是 s 在 G 中生成的循环子群，那么 C 将 X 分解成一些轨道 O_α. 设 $f_\alpha=|O_\alpha|$ 而 $x_\alpha\in O_\alpha$，则有 $s^{f_\alpha}x_\alpha=x_\alpha$. 如果 g_α 是 x_α 的代表元，那么就有

$$s^{f_\alpha}g_\alpha=g_\alpha h_\alpha,\quad \text{其中}\, h_\alpha\in H.$$

命题 7.2 $\mathrm{Ver}(s)=\prod_\alpha h_\alpha=\prod_\alpha g_\alpha^{-1}s^{f_\alpha}g_\alpha\ \ (\mathrm{mod}\,(H,H))$.[1)]

元素 s^ig_α, $0\le i<f_\alpha$，可以取为 X 的一个代表元组. 如果 $x\in X$ 的代表元形如 $s^{f_\alpha-1}g_\alpha$，则 H 中相应的元素 $h_{s,x}$ 就等于 h_α，而其余的 $h_{s,x}$ 都等于 1. 由此即得命题. ■

推论 7.3 *设 φ 是 H^{ab} 到 A 的同态. 假定对于 H 中的两个元素 h,h'，只要它们在 G 中共轭，就有 $\varphi(h)=\varphi(h')$. 那么，对 $h\in H$，有*

$$\varphi(\mathrm{Ver}(h))=\varphi(h)^n,$$

其中 $n=(G:H)$.

实际上，我们有 $\varphi(\mathrm{Ver}(h))=\prod_\alpha\varphi(g_\alpha^{-1}h^{f_\alpha}g_\alpha)$. 由于元素 $g_\alpha^{-1}h^{f_\alpha}g_\alpha$ 与 h^{f_α} 在 G 中共轭，因此有

$$\varphi(\mathrm{Ver}(h))=\prod_\alpha\varphi(h^{f_\alpha})=\prod_\alpha\varphi(h)^{f_\alpha}.$$

于是，可由等式 $\sum_\alpha f_\alpha=\sum_\alpha|O_\alpha|=|X|=n$ 导出结果. ■

1) 注意，如果 s 属于 G 的中心，则 $g_\alpha^{-1}s^{f_\alpha}g_\alpha=s^{f_\alpha}$. 于是，这个公式导出 $\mathrm{Ver}(s)=\prod_\alpha s^{f_\alpha}=s^n\ (\mathrm{mod}\,(H,H))$，其中 $n=\sum_\alpha f_\alpha=(G:H)$. 下面命题 7.6 的证明要用到这一事实. —— 译注

因为 $H \subset G$, 所以有一个自然的同态 $H^{ab} \to G^{ab}$.

推论 7.4 *复合同态* $G^{ab} \xrightarrow{\mathrm{Ver}} H^{ab} \longrightarrow G^{ab}$ *就是* $s \mapsto s^n$.

这由命题直接推出，因为有

$$g_\alpha^{-1} s^{f_\alpha} g_\alpha = s^{f_\alpha} \pmod{(G,G)} \quad \text{以及} \quad \sum_\alpha f_\alpha = |X| = n. \qquad \blacksquare$$

推论 7.5 *若 G 为交换群，则 $\mathrm{Ver}: G \to H$ 由 $s \mapsto s^n$ 给出.*

7.3 使用转移的实例

7.3.1 第一例 (Gauss)

固定一个素数 $p \neq 2$.

设 $G = \mathbf{F}_p^*$, $H = \{\pm 1\}$. 那么， H 在 G 中的指标为 $(p-1)/2$, 对 $x \in \mathbf{F}_p^*$ 转移公式为 $\mathrm{Ver}(x) = x^{(p-1)/2}$. 由于这就是 *Legendre* 符号 $(\frac{x}{p})$, 所以这就提供了计算 $(\frac{x}{p})$ 的一个方法.

取 $S = \{1, 2, \ldots, (p-1)/2\}$ 为 $X = G/H$ 的代表元组. 设 $x \in G$, $s \in S$. 如果 $xs \in S$, 则 $h_{s,x}$ 取值为 1, 否则取值为 -1. 因此，令

$$\varepsilon(x,s) = \begin{cases} 1 & \text{若 } xs \in S, \\ -1 & \text{若 } xs \notin S, \end{cases}$$

则有 $\mathrm{Ver}(x) = \prod_{s \in S} \varepsilon(x,s)$ (*Gauss* 引理).

例如，对 $p \neq 2$ 来计算 $(\frac{2}{p})$. 设 $p = 1 + 2m$, 则

$$\left(\frac{2}{p}\right) = (-1)^{m/2} \qquad \text{若 } m \text{ 为偶数},$$

$$\left(\frac{2}{p}\right) = (-1)^{(m+1)/2} \qquad \text{若 } m \text{ 为奇数}.$$

由此得出

$$p \equiv 1 \pmod 8 \Longrightarrow \left(\frac{2}{p}\right) = +1,$$

$$p \equiv 3 \pmod 8 \Longrightarrow \left(\frac{2}{p}\right) = -1,$$

$$p \equiv 5 \pmod 8 \Longrightarrow \left(\frac{2}{p}\right) = -1,$$

$$p \equiv 7 \pmod 8 \Longrightarrow \left(\frac{2}{p}\right) = +1.$$

这些可以归结为： $(\frac{2}{p}) = +1 \Longleftrightarrow p \equiv \pm 1 \pmod 8$.

7.3.2 第二例

命题 7.6 *若群 G 没有挠元，并且包含一个与 $\mathbb{Z}$ 同构的有限指标子群 H, 则 G 本身也与 $\mathbb{Z}$ 同构.*

有必要的话，将 H 换成它的共轭子群之交，[1] 就可以假设 H 为 G 的正规子群. 群

1) H 的共轭子群之交是 $H \cong \mathbb{Z}$ 的子群，因此它或者同构于 $\mathbb{Z}$, 或者为平凡群. 因为 H 只有有限个共轭子群，因此这个交在 G 中的指标有限，所以不会是平凡群. —— 译注

G 作用在 H 上,[1] 因此有同态 $\varepsilon: G \to \mathrm{Aut}(H) = \{\pm 1\}$. 设 ε 的核为 G'. 那么, 由于 H 为交换群, 故通过内自同构作用于自身时是平凡作用, 从而 $H \subset G'$. 因为 G' 平凡作用于 H 上, 故 H 还含于 G' 的中心. 因此, 转移同态 $\mathrm{Ver}: G'^{ab} \to H^{ab} = \mathbb{Z}$ 就等于 $x \mapsto x^n$, 其中 $n = (G' : H)$.[2] 设 Φ 为 $\mathrm{Ver}: G' \to H^{ab}$ 的核, 则由于 H 同构于 $\mathbb{Z}$, 因而 $\Phi \cap H = \{1\}$, 从而 Φ 是有限子群, 既然 G 没有挠元, 故有 $\Phi = \{1\}$. 因此, G' 同构于 $\mathbb{Z}$. 如果 G 同构于 G', 那就证完了.[3]

如果不然, 则有 $(G : G') = 2$,[4] $G' \cong \mathbb{Z}$, 并且群 G/G' 通过同态 $y \mapsto y^{\pm 1}$ 作用在 G' 上. 因此, 设 $x \in G - G'$ 使得对某个 $y \in G'$ 有 $xyx^{-1} = y^{-1}$. 由于 G' 在 G 中的指标为 2, 故 $x^2 \in G'$. 那么, 取 $y = x^2$ 就得到 $xx^2x^{-1} = x^{-2}$, 从而 $x^2 = x^{-2}$. 由于 G 没有挠元, 故 $x = 1$. 因此, G 同构于 $\mathbb{Z}$. ■

注 对于非交换的自由群有一个类似的结果 (Stallings-Swan), 但却非常艰深. 参考: J. R. Stallings, On torsion-free groups with infinitely many ends, Ann. Math. 88 (1968), 312–334; R. Swan, Groups of cohomological dimension one, J. Algebra 12 (1969), 585–610.

7.4 Sylow 子群中的转移

定理 7.7 *设 H 为群 G 的 Sylow p–子群, A 为交换 p–群, $\varphi: H \to A$ 为同态. 那么*

(1) *φ 可以扩张为 G 到 A 的同态之充要条件是: 若 $h, h' \in H$ 在 G 中共轭, 则 $\varphi(h) = \varphi(h')$.*

(2) *如果这一条件满足的话, 则扩张是唯一决定的, 并由公式 $s \mapsto \varphi(\mathrm{Ver}(s))^{1/n}$ 给出, 其中 $n = (G : H)$, 由于 n 与 p 互素, 这个表达式是有意义的.*

(1) 必要性: 设 $\tilde{\varphi}$ 为 φ 在 G 上的扩张, 若 $h \in H$, $g \in G$ 使 $g^{-1}hg \in H$, 则由于 A 交换, 故有

$$\varphi(g^{-1}hg) = \tilde{\varphi}(g)^{-1}\varphi(h)\tilde{\varphi}(g) = \varphi(h).$$

充分性: 由于 n 与 p 互素, A 为 p–群, 故 $\varphi(\mathrm{Ver}(s))^{1/n}$ 有意义 (对每个 $a \in A$, 存在唯一一个 $b \in A$ 使 $b^n = a$[5]). 根据推论 7.3, 映射 $s \mapsto \varphi(\mathrm{Ver}(s))^{1/n}$ 就满足要求.

(2) 当 $p' \neq p$ 时, φ 在 G 的 Sylow p'–子群上必定等于 1, 所以扩张是唯一决定的. ■

定理 7.8 *设 H 为 G 的交换 Sylow p–子群, N 是 H 在 G 中的正规化子. 那么, 同态 $\mathrm{Ver}: G^{ab} \to H^{ab} = H$ 的象集由 H 中在 N 作用下不动的元素组成 (即, H 中属于 N 的中心的元素).*

---

1) 通过内自同构的共轭作用. —— 译注

2) 不清楚为什么转移同态具有这种形式. 但由于 H 含于 G' 的中心, 故若 $x \in H$ 时, 根据命题 7.2 之脚注, 就有 $\mathrm{Ver}(x) = x^n$. 既然 H 为无限循环群, 故 $x \neq 1$ 时, 有 $x^n \neq 1$. 这就导出下面的事实: $\Phi \cap H = \{1\}$. 这个等式又说明 Φ 中的两个元素不会属于 H 的同一个陪集, 因此 Φ 必为有限集. —— 译注

3) 也可直接证明 $G = G'$. 用反证法, 如果不然, 则有 $x \in G$ 使 $\varepsilon(x) = -1 \in \mathrm{Aut}(H) = \{\pm 1\}$, 即 $\varepsilon(x)$ 是由 $y \mapsto y^{-1}$ 给出的 H 的自同构. 于是对所有 $y \in H$ 都有 $xyx^{-1} = y^{-1}$. 既然 H 为 G 的正规子群, 故 $x^m \in H$, 其中 $m = (G : H)$. 由 $xx^mx^{-1} = x^{-m}$ 推出 x 是 G 中的挠元, 故 $x = 1$, 矛盾. —— 译注

4) 如果不然, 则 $G \neq G'$. 故 $\varepsilon: G \to \mathrm{Aut}(G) = \{\pm 1\}$ 为满射, 所以 $(G : G') = 2$. —— 译注

5) 由于 A 为交换 p–群而 n 与 p 互素, 所以 $a \mapsto a^n$ 是 A 的自同构, 特别是双射. —— 译注

由 §7.1 最后的注记已经知道， Ver 的象集含在 $H^N=\{h\in H\,|\,nhn^{-1}=h,\forall n\in N\}$ 内. 下面证明它们实际上相等. 我们有 $N\supset H$, 且由于 H 为 Sylow p-子群，故 $(N:H)$ 与 p 互素. 用公式

$$\varphi(h)=\Big(\prod_{n\in N/H}nhn^{-1}\Big)^{1/(N:H)}$$

定义一个同态 $\varphi:H\to H^N$. 注意，我们确实有 $\prod_{n\in N/H}nhn^{-1}\in H^N$, 因为若 $n'\in N$, 则有

$$n'\Big(\prod_{n\in N/H}nhn^{-1}\Big)n'^{-1}=\prod_{n\in N/H}n'nhn^{-1}n'^{-1}=\prod_{n\in N/H}nhn^{-1}.$$

此外，由于 H 交换，所以，若 $h,h'\in H$ 在 G 中共轭，它们就在 N 中共轭 (参阅 §2.4 [1])，从而有 $\varphi(h)=\varphi(h')$. 根据推论 7.3, 对 $h\in H$, 有

$$\varphi(\mathrm{Ver}(h))=\varphi(h)^n.$$

由于对 $h\in H^N$, 有 $\varphi(h)=h$, 又由于 $\mathrm{Ver}(h)\in H^N$, 故对 $h\in H^N$ 有

$$\mathrm{Ver}(h)=\varphi(\mathrm{Ver}(h))=\varphi(h)^n.$$

即，若 $h\in H^N$, 则 $\mathrm{Ver}(h)=h^n$.

由于 H^N 是 p-群而 n 与 p 互素，对 H^N 的元素取 n 次幂就可得到 H^N 中所有的元素，因此有 $\mathrm{Im}(\mathrm{Ver})=H^N$. ■

定理 7.9 *设 H 为 G 的交换 Sylow p-子群， H 不等于 $\{1\}$. 假定 G 的商群都不是 p 阶循环群. 设 N 是 H 在 G 中的正规化子. 那么*

(1) H 在 N 作用下不动的元素集合 H^N 等于 $\{1\}$.

(2) 若 r 为 H 的秩 (生成元的最少个数), 那么存在一个不等于 p 的素数 l, 它既整除 $(N:H)$, 也整除 $\prod_{i=1}^{r}(p^i-1)$.

(1) 如果 $H^N\neq\{1\}$, 则有一个非平凡同态 $\mathrm{Ver}:G\to H^N$. [2] 因为 H^N 是 p-群，由此可以得到 G 的一个 p 阶循环商群.

(2) 设 H_p 是 H 中满足 $x^p=1$ 的元素组成的子群，这是 $\mathbf{F}_p$ 上的 r 维向量空间 (因为 $H=\prod_{i=1}^{r}(\mathbb{Z}/p^{n_i}\mathbb{Z})$). 由 (1) 知， N 在 H_p 上的作用是非平凡的，这就定义了 $\mathrm{Aut}(H_p)\cong\mathbf{GL}_r(\mathbb{Z}/p\mathbb{Z})$ 的一个子群 Φ. 如果 l 是 Φ 的阶的一个素因子，则 l 除尽 N/H 的阶，因为 Φ 是 N/H 的商群 (实际上， Φ 通过 N 在 H 上的作用来定义，由于 H 为交换群，它平凡作用于自身，因此 Φ 实际上通过 N/H 的作用来定义 [3])． 因为 p 不整除 N/H 的阶，故有 $l\neq p$. 又因为 Φ 是 $\mathbf{GL}_r(\mathbb{Z}/p\mathbb{Z})$ 的子群，故 l 整除 $\mathbf{GL}_r(\mathbb{Z}/p\mathbb{Z})$ 的阶，即 $p^{r(r-1)/2}\prod_{i=1}^{r}(p^i-1)$. 证毕. ■

推论 7.10 *若 $p=2$, 那么子群 H 不是循环群.*

---

1) 推论 2.13.—— 译注

2) 定理 7.8 说明这是一个满同态.—— 译注

3) N 共轭作用在 H 上，因此也作用在 H_p 上. 这诱导了一个同态 $N\to\mathrm{Aut}(H_p)$. 既然 H 交换，它在 H_p 上的作用是平凡的，故 H 包含在上述同态的核内. 这就诱导了一个同态 $N/H\to\mathrm{Aut}(H_p)$, 而它的象就是 Φ, 故 Φ 是 N/H 的商群.—— 译注

实际上，定理 7.9 推出 $r \geq 2$,[1] 但这一结果也可直接证明：假定 Sylow 2−子群 H 为循环群，设 h 为它的一个生成元. 群 G 通过平移作用在自身上. 那么，元素 h 将 G 分解为 $|G/H|$ 条轨道. 对 $x \in G$, x 在 G 上平移作用的效果相当于 G 上的一个置换，将 x 指派上这个置换的符号，就得到从 G 到 $\{\pm 1\}$ 的同态. 若 $|H| = 2^n$, 则 h 由奇数个 (确切地说，是 $|G/H|$ 个) 形如 $(x, hx, \ldots, h^{2^n-1}x)$ 的轮换 [2] 组成. 每个这样的轮换符号都为 -1, 从而 h 的符号为 -1. 于是，这就给出了从 G 到 $\{\pm 1\}$ 的一个非平凡同态,[3] 矛盾.

■

注 定理 7.9 证明了以下结果：设 H 为 G 的交换 Sylow p−子群，而 G 没有 p 阶循环商群，则 $N_G(H) \neq H$ (否则 $H^N = H \neq \{1\}$).

7.5 应用：不超过 2000 的奇数阶单群

下面来证明不存在群 G 使得 $G = (G, G)$, 并且 $|G|$ 为 ≤ 2000 的奇数.

根据 Burnside 定理 (参阅附录之定理 A.21),[4] $|G|$ 至少有 3 个素因子. 若 p^α 是它的最小素数幂因子，则有 $p^{3\alpha} < 2000$. 于是，只有 5 种可能性： $p^\alpha = 3, 5, 7, 9$ 或 11.

$p^\alpha = 3$ 的情况

群 G 有一个 3 阶的 Sylow 3−子群，它是循环群，从而是交换群. 设 N 是它的正规化子. 根据定理 7.9, 存在不等于 3 的素数 l, 它除尽 $|N|$ 与 $p - 1 = 2$. 由于 $|N|$ 为奇数，这是不可能的.

$p^\alpha = 5$ 的情况

用与上面类似的方法排除.

$p^\alpha = 9$ 的情况

同样地，注意到 Sylow 3−子群的阶为 3^2, 因此是交换群. 在此情形中， $r = 1$ 或 2, 用类似的论证即可排除这种情形.

$p^\alpha = 7$ 的情况

根据定理 7.9, 必有素数 l 除尽奇数 $|N|$ 与 $p - 1 = 6$. 因此， 3 整除 $|G|$. 由于前面已排除了 $p^\alpha = 3$ 或 9 的情况，故必有 3^3 整除 $|G|$. 根据 Burnside 定理，有不等于 3 与 7 的素数 q 整除 G 的阶. 因此 $|G| \geq 3^3 \cdot 7 \cdot q^\beta$, 并且 $q^\beta \geq 11$ (因为若 $q = 5$, 已经考虑过的情况说明必有 $\beta \geq 2$). 但由于 $3^3 \cdot 7 \cdot 11 > 2000$, 这是不可能的.

$p^\alpha = 11$ 的情况

将定理 7.9 应用于 Sylow 11−子群，知道有素数 l 整除 $|N|$ 与 $p - 1 = 10$. 根据前一种情形，必有 $|G| \geq 11 \cdot 5^2 \cdot q^\beta$, 且 $q^\beta \geq 13$. 这是不可能的. ■

7.6 应用：阶数不超过 200 的非交换单群

在本节中，总假定 $|G| \leq 200$.

---

1) 此时有 $\prod_{i=1}^{r}(2^i - 1) \geq l > 1$. 故 $r \geq 2$.—— 译注
2) 原文为 cycle, 亦译作 "循环","圈" 等等.—— 译注
3) 这说明 $\{\pm 1\}$ 是 G 的 2 阶商群.—— 译注
4) 也可见定理 5.4.—— 译注

命题 7.1 (1) 假定 $G=(G,G)$ 且 $G\neq\{1\}$, 则 G 的阶为 60, 120, 168 或者 180.
(2) 若 G 为非交换单群, 则 G 的阶为 60 或 168, 并且 G 同构于 A_5 或 $\mathbf{PSL}_2(\mathbf{F}_7)$.

(1) 由前节的结果, G 的阶为偶数. 又由于推论 7.10 断言不存在循环的 Sylow 2–子群, 因此 G 的阶还能被 4 整除.

Sylow 2–子群 H 阶为 4 的情形

那么, 它必是 $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. 设 $N=N_G(H)$, 则 N 非平凡地作用在 H 上 (由于 $H^N=\{1\}$, 见定理 7.9), 从而有一个非平凡的同态 $N\to\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})$ (这个群的阶为 6). 如果 N 映为 $\mathrm{Aut}(H)$ 的一个 2 阶子群, 则 $H^N\cong\mathbb{Z}/2\mathbb{Z}$ (要证明这一点, 只需考虑 $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ 的自同构). 因此, 3 整除 N 的阶, 故也整除 G 的阶. 从而, 有 5 种可能性:

• $|G|=4\cdot3\cdot13$: 设 H 为 Sylow 13–子群, N 是它的正规化子. 那么, $(G:N)$ 是 G 的 Sylow 13–子群的个数, 故 $(G:N)\equiv1\,(\mathrm{mod}\,13)$. 由于 $(G:N)$ 除尽 $4\cdot3=12$, 这推出 $(G:N)=1$, 故 H 是正规子群, 这是不可能的.

• $|G|=4\cdot3\cdot11$: 设 H 为 Sylow 11–子群, N 是它的正规化子. 那么, $(G:N)$ 整除 $4\cdot3=12$, 且 $(G:N)\equiv1\,(\mathrm{mod}\,11)$. 因此, 或者 $(G:N)=1$, 或者 $(G:N)=12$. 前一种情况不可能, 后一种情况推出 $N=H$, 从而 $H^N=H$ (由于 H 为交换群), 这也不可能 (见定理 7.4).

• $|G|=4\cdot3\cdot7$: 设 H 为 Sylow 7–子群, N 是它的正规化子. 那么, $(G:N)$ 整除 12, 且 $(G:N)\equiv1\,(\mathrm{mod}\,7)$. 因此, $(G:N)=1$, 这是不可能的.

• 还剩下两种情形: $|G|=4\cdot3\cdot5=60$ 或 $|G|=4\cdot3^2\cdot5=180$ (其余的情况可排除, 因为那时 $|G|>200$).

Sylow 2–子群 H 阶为 8 的情形

有两种可能性: $|G|=8\cdot3\cdot5$ 或 $|G|=8\cdot3\cdot7$, 其它情形给出的 $|G|$ 的阶都太大了. 同理, 考虑阶就可将 $|H|>8$ 的情形排除. 这就证明了 (1).

(2) 考虑 $|G|=4\cdot3^2\cdot5$ 与 $|G|=8\cdot3\cdot5$ 的情形: 设 H 为 Sylow 5–子群, N 是它的正规化子. 那么, $(G:N)\equiv1\,(\mathrm{mod}\,5)$, 并且 $(G:N)$ 除尽 $4\cdot3^2$ (第一种情况) 或者 $8\cdot3$ (后一种情况). 在两种情况中, 都只有 $(G:N)=6$ 这一种可能性. 设 X 为 G 的 Sylow 5–子群的集合. 群 G 可嵌入到 X 的置换群内, 也就是 S_6 内. [1] 因为 G 是单群, 它实际上嵌入到了 A_6 内. [2] 然而 A_6 的阶为 360, G 的阶为 120 或 180. 若 $1<m<6$, 则群 A_6 没有指标为 m 的子群 (这里是 3 与 2 的情形), 因为否则 A_6 可以嵌入到 S_m 内, 由于 $|A_6|>|S_m|$, 这是不可能的. 因此, 不超过 200 的非交换单群的阶只有可能是 $4\cdot3\cdot5=60$ 与 $8\cdot3\cdot7=168$.

60 阶与 168 阶单群的结构

60 阶 设 H 为 G 的 Sylow 2–子群, N 是 H 的正规化子, 那么 H 不能是循环群 (推论 7.10), 因此 3 整除 $|N|$ (定理 7.9), 故 12 整除 $|N|$ 而 $N\neq G$, 从而 $|N|=12$. 由此

1) 通过共轭, G 作用于 X 上. 这给出了从 G 到 S_6 (X 的置换群) 的非平凡同态. 既然 G 为单群, 这必然是一个单同态, 也就是嵌入. —— 译注
2) 如果 G 不包含在 A_6 内, 则 $G\cap A_6$ 是 G 的指标为 2 的子群, 从而为正规子群. —— 译注

G/N 的阶为 5, 故有 G 到 $\mathcal{S}_5$ 的非平凡同态. 因为 G 是单群, 所以这将 G 嵌入到 $\mathcal{A}_5$ 中, 比较阶数可知 $G = \mathcal{A}_5$.

168 阶 设 H 为 G 的 Sylow 7–子群, N 是它的正规化子. 那么 $(G:N)$ 整除 $8\cdot 3$, 且 $(G:N) \equiv 1 \pmod 7$. 因为 $N \neq G$, 故有 $(G:N) = 8$, 从而 $|N| = 21$. 考虑正合列 $\{1\} \to H \to N \to N/H \to \{1\}$. 由于 H 的阶与 N/H 的阶互素, 故群 N 是 H 与 N/H 的半直积 (参考 §4.4). 于是, 群 N 有两个生成元: 一个是 H 的生成元 α, 满足 $\alpha^7 = 1$; 另一个是 N/H 的生成元 β, 满足 $\beta^3 = 1$. H 的自同构 $x \mapsto \beta x \beta^{-1}$ 的阶为 3, 因此, 它或者是 $x \mapsto x^2$, 或者是 $x \mapsto x^{-3}$. [1] 如果必要的话, 将 β 换成 β^{-1}, 总可假定这个自同构为 $x \mapsto x^2$. 因此, 有 $\beta\alpha\beta^{-1} = \alpha^2$.

设 X 为 G 的 Sylow 7–子群的集合. 那么, H 作用在 X 上, 而 H 自己在看作 X 的元素时, 在这个作用下稳定. 将这个元素记为 ∞, 则有 $X = \{\infty\} \cup X_0$, 且 $|X_0| = 7$. 群 H 自由作用在 X_0 上 (因为 H 是 7 阶循环群). [2] 元素 β 作用在 X 上, 且由于 $\beta \in N$, 所以 ∞ 在它的作用下稳定. 因为 $\beta^3 = 1$, 故存在 $x_0 \in X_0$ 使 $\beta x_0 = x_0$. [3] 那么

$$X = \{x_0, \alpha x_0, \ldots, \alpha^6 x_0, \infty\}.$$

将 X 等同于 $\mathbf{P}_1(\mathbf{F}_7)$, 并将 $\alpha^i x_0$ 等同于 i.

元素 α 以如下方式作用在 $\mathbf{P}_1(\mathbf{F}_7)$ 上: 若 $i < 6$, 则 $\alpha(i) = i+1$, 又 $\alpha(6) = 0$, $\alpha(\infty) = \infty$. 元素 β 的作用为: $\beta(\infty) = \infty$, $\beta(0) = 0$, 又由 $\beta\alpha = \alpha^2\beta$ 推知对每个 i 有 $\beta(i+1) = \beta(i)+2$ 及 $\beta(i) = 2i$. 这样, α 在 $\mathbf{P}_1(\mathbf{F}_7)$ 上的作用相当于平移变换, β 的作用相当于伸缩变换. 设 C 为 β 在 N 中生成的循环子群, 而 M 是它在 G 中的正规化子. 由于 C 是 G 的 Sylow 3–子群, 定理 7.9 说明 2 整除 $|M|$. 群 M 非平凡地作用在 C 上 (定理 7.9), 故存在 γ 使 $\gamma C \gamma^{-1} = C$, 且 $\gamma\beta\gamma^{-1} = \beta^{-1}$. 因为 $\gamma \notin C$, 且 $\gamma \neq \alpha^n$ (因为 $\alpha \notin M$), 故可选取 γ 使其阶为 2^n.

元素 γ 将 C 的轨道变为 C 的轨道, 因此 $\gamma(\{0,\infty\}) = \{0,\infty\}$. γ 在 X 上的作用是没有不动点的, 因为如若不然, 则 γ 属于 H 的某个共轭子群的正规化子, 于是属于 N 的某个共轭子群, 但这与 2 不整除 $|N|$ 的事实矛盾. 因此必有 $\gamma(0) = \infty$, $\gamma(\infty) = 0$. 因为 ∞ 在 γ^2 作用下不动, 故有 $\gamma^2 \in N$. [4] 由于 γ 是偶数阶的, 所以 $\gamma^2 = 1$. 因此, γ 置换两条轨道 $\{1,2,4\}$ 与 $\{3,6,5\}$. 令 $\gamma(1) = \lambda$, 则 λ 等于 3, 6 或 5. 因为 $\gamma\beta = \beta^{-1}\gamma$, 故有 $\gamma(2i) \equiv \gamma(i)/2 \pmod 7$. 因此 $\gamma(i) = \lambda/i$, 从而 γ 是一个射影变换, 即 $\gamma \in \mathbf{PGL}_2(\mathbf{F}_7)$. 因为 $-\lambda$ 是完全平方, 设 $\mu^2 = -\lambda$, 则有

$$\gamma(i) = \frac{-\mu}{\mu^{-1} i}.$$

因此, $\det\gamma = +1$, 故 $\gamma \in \mathbf{PSL}_2(\mathbf{F}_7)$.

---

1) 原文是 $x \mapsto x^{-2}$.—— 译注

2) $\alpha \in H$ 可以看作 X_0 上的一个置换, 因为它是 7 阶元, 所以它只能是一个长度为 7 的轮换 (cycle). 于是, H 中每个非单位元都是长度为 7 的轮换, 即在 X_0 上没有不动点.—— 译注

3) 由 $\beta^3 = 1$ 知 β 或者是一个 3 元轮换, 或者是两个 3 元轮换之积. 故一定有 $x_0 \in X_0$ 不出现在 β 的轮换分解中, 即有 $\beta x_0 = x_0$.—— 译注

4) 原文为 $\gamma \in N$.—— 译注

然而 α,β 与 γ 生成了群 G. 实际上，设 G' 是由这些元素生成的 G 的子群. 那么，G' 包含 N 与偶数阶元素 γ. 如果 $G' \neq G$, 则 G' 的指标为 2 或 4, 这样 G 就可以嵌入到 $\mathcal{A}_2$ 或 $\mathcal{A}_4$ 中，而这是不可能的. 因此 $G = G'$. 我们有一个单同态 $G \to \mathbf{PSL}_2(\mathbf{F}_7)$. 由于这两个群的阶数相同，所以它是一个同构. ■

附录 特征标理论

A.1 表示与特征标

设 G 为群，K 为域. V 为 K 上的有限 n 维向量空间. 从定理 A.2 起，假定 $K = \mathbb{C}$, 且 G 为有限群.

定义 A.1 *从 G 到 $\mathbf{GL}(V)$ 的一个给定同态 ρ 就称为 G 在 V 中的一个线性表示. V 的维数称为表示的次数.*

注 (1) 这样就可按以下方式定义一个 G 在 V 上的作用：对 $x \in V, s \in G$, 令 $s.x = \rho(s)(x)$.

(2) 对给定的 ρ, V 称为 G 的表示空间，或简称为 G 的表示，常常将 ρ 写作 ρ_V.

如果同态 ρ_1 与 ρ_2 相应的 G 的表示为 V_1 与 V_2, 则可定义：

- V_1 与 V_2 的直和 $V_1 \oplus V_2$: 相应的表示 $\rho : G \to \mathbf{GL}(V_1 \oplus V_2)$ [1] 定义为 $\rho(s) = \rho_1(s) \oplus \rho_2(s)$. 如果在 $V = V_1 \oplus V_2$ 中选取与直和分解相容的基底，则在此基底中 $\rho(s)$ 可用以下矩阵来表示：

$$\begin{pmatrix} A_1(s) & 0 \\ 0 & A_2(s) \end{pmatrix},$$

其中 $A_i(s)$ 是 $\rho_i(s)$ 在 V_i 的相应基底下之矩阵表示.

- 张量积 $V_1 \otimes V_2$: 对 $x \in V_1$ 与 $y \in V_2$, $\rho(s)(x \otimes y) = \rho_1(s)(x) \otimes \rho_2(s)(y)$.
- V_1 的对偶 V_1^*: 对 $l \in V_1^*$, $x \in V_1$, $\rho(s).l(x) = l(\rho_1(s^{-1}).x)$.
- $\mathrm{Hom}(V_1, V_2)$, 可将它与 $V_1^* \otimes V_2$ 等同：对 $x \in V_1$, $h \in \mathrm{Hom}(V_1, V_2)$, $\rho(s).h(x) = \rho_2(s)h(\rho_1(s^{-1}).x)$.

还可定义其他一些对象.

表示的特征标

设 V 是向量空间，给定了一组基 $(e_i)_{1 \le i \le n}$. 设 ρ 是 V 到自身的线性变换，在这组基下的矩阵表示为 $a = (a_{ij})$, 用 $\mathrm{Tr}(\rho) = \sum_i a_{ii}$ 来记矩阵 a 的迹 (它不依赖于基底的选取).

现在，如果 V 是有限群 G 的表示，则可在 G 上定义一个取值在 K 中的函数 χ_V 如下：

$$\chi_V(s) = \mathrm{Tr}(\rho_V(s)),$$

其中 ρ_V 是与表示 V 相应的同态. 函数 χ_V 称为表示 V 的*特征标*.

注 $\chi_V(1) = \dim V$.

1) 原文为 $\rho : G \to V_1 \oplus V_2$.—— 译注

命题 A.1

- χ_V 是中心函数，即对 $s,t\in G$, $\chi_V(sts^{-1})=\chi_V(t)$.
- $\chi_{V_1\oplus V_2}=\chi_{V_1}+\chi_{V_2}$,
- $\chi_{V_1\otimes V_2}=\chi_{V_1}\chi_{V_2}$,
- $\chi_{V^*}(s)=\chi_V(s^{-1})$, 对 $s\in G$,
- $\chi_{\mathrm{Hom}(V_1,V_2)}(s)=\chi_{V_1}(s^{-1})\chi_{V_2}(s)$, 对 $s\in G$.

下面总假定 $K=\mathbb{C}$, 且 G 为有限群. 设 V 是 G 的表示. 令

$$V^G=\{x\in V\mid s.x=x,\forall s\in G\};$$

又，对 $x\in V$, 令

$$\pi(x)=\frac{1}{|G|}\sum_{s\in G}s.x.$$

那么， $\pi(x)\in V^G$, 且若 $x\in V^G$, 则 $\pi(x)=x$. 这证明了 π 是 V 到 V^G 上的投影算子. 映射 π 与 G 的元素是交换的，即对 $s\in G$ 有 $\pi(s.x)=s.\pi(x)$, 因此有

$$V=V^G\oplus\ker\pi.$$

取一个与此分解相容的基底，则 π 的矩阵表示是

$$\begin{pmatrix}1&0&\cdots&\cdots&\cdots&0\\0&\ddots&\ddots&&&\vdots\\\vdots&\ddots&1&\ddots&&\vdots\\\vdots&&\ddots&0&\ddots&\vdots\\\vdots&&&\ddots&\ddots&0\\0&\cdots&\cdots&\cdots&0&0\end{pmatrix}$$

由此得到

定理 A.2 $\dim V^G=\mathrm{Tr}(\pi)=\frac{1}{|G|}\sum_{s\in G}\chi_V(s)$.

推论 A.3 设 $0\longrightarrow V'\longrightarrow V\xrightarrow{f}V''\longrightarrow 0$ 是 G 的表示组成的正合列，[1] 那么，V''^G 中的每个元素都是某个 V^G 中元素的象.

若 $x''\in V''^G$, 由正合性， f 为满射，故存在 $x\in V$ 使 $f(x)=x''$. 那么， $\pi(x)\in V^G$, 且 $f(\pi(x))=\pi(f(x))=\pi(x'')=x''$. ■

推论 A.4 [2] 若 V' 是 V 的向量子空间，它在 G 的作用下稳定. 那么，存在 V' 在 V 中的补子空间，它在 G 的作用下也稳定.

设 $V''=V/V'$. 考虑正合列

$$0\longrightarrow\mathrm{Hom}(V'',V')\longrightarrow\mathrm{Hom}(V'',V)\longrightarrow\mathrm{Hom}(V'',V'')\longrightarrow 0.$$

1) 表示的正合列是向量空间的正合列，其中的线性映射与 G 的每个元素都交换. —— 译注
2) 这个推论有时称作 Maschke 定理. —— 译注

设 $x \in \mathrm{Id}_{V''} \in \mathrm{Hom}(V'', V'')$, 则 x 在 G 作用下不变. 因此, 由推论 A.3, 存在 $\varphi : V'' \to V$, 它在 G 作用下不变并且映为 x. 因此, 若 $v \in V''$, $s \in G$, 则有

$$(s^{-1}.\varphi)(v) = \varphi(v) = s^{-1}.\varphi(sv),$$

故有 $s.\varphi(v) = \varphi(s.v)$, 从而 φ 与 G 交换.

若 $p : V \to V''$ 为投影同态, 则由 $p \circ \varphi = x = \mathrm{Id}''_V$ 知 φ 是 p 的截口, 故有 $V = V' \oplus \mathrm{Im}\varphi$, 且 $\mathrm{Im}\varphi$ 在 G 的作用下稳定. ■

定义 A.2 设 $\rho : G \to \mathrm{GL}(V)$ 是 G 的线性表示. 如果 $V \neq 0$, 并且除了 0 与 V 之外, 没有其它的向量子空间在 G 的作用下稳定, 就称 ρ 为不可约表示.

那么, 有下面的

定理 A.5 . 每个表示都是不可约表示的直和.

对表示 V 的维数作归纳法来证明.

若 $\dim V \leq 1$, 结论显然成立. 如若不然, 则或者 V 不可约, 或者它有一个 $\neq 0$ 与 V 的真子空间在 G 作用下稳定. 在后一种情形, 根据推论 A.4, 存在一个直和分解 $V = V' \oplus V''$, 使得 $\dim V' < \dim V$, $\dim V'' < \dim V$, 且 V' 与 V'' 都在 G 作用下稳定. 对 V' 与 V'' 应用归纳假设, 知道它们都是不可约表示的直和, 所以 V 也是. ■

注 上面的直和分解并不是唯一的. 例如, 若 G 平凡作用于 V 上, 只要将 V 写成一些直线的直和就将 V 分解成了不可约表示的直和. 如果 $\dim V \geq 2$, 这样的分解当然是很多的.

A.2 正交关系

定理 A.6 (Schur) 设 $\rho_1 : G \to \mathbf{GL}(V_1)$ 与 $\rho_2 : G \to \mathbf{GL}(V_2)$ 是 G 的两个不可约表示, f 是 V_1 到 V_2 的同态, 使得对每个 $s \in G$ 都有 $\rho_2(s) \circ f = f \circ \rho_1(s)$. 那么,

(1) 若 V_1 与 V_2 不同构, 则 $f = 0$.

(2) 若 $V_1 = V_2$, $\rho_1 = \rho_2$, 则 f 是伸缩变换.

(1) 若 $x \in \ker f$, 则对每个 $s \in G$ 都有 $(f \circ \rho_1(s)).x = (\rho_2(s) \circ f).x = 0$. 因此, $\ker f$ 在 G 作用下稳定. 由于 V_1 不可约, 故或者 $\ker f = 0$, 或者 $\ker f = V_1$. 在前一种情形 f 为单射, 后一种情形 f 为零映射. 同理, $\mathrm{Im} f$ 在 G 作用下稳定, 故 $\mathrm{Im} f = 0$ 或者 V_2. 因此, 若 $f \neq 0$, 则 $\ker f = 0$, 且 $\mathrm{Im} f = V_2$, 于是 f 是 V_1 到 V_2 上的同构. 这就证明了 (1).

(2) 现在, 设 $V_1 = V_2$ 且 $\rho = \rho_1 = \rho_2$, 又设 $\lambda \in \mathbb{C}$ 是 f 的一个特征值. 令 $f' = f - \lambda$, 则 f' 不是单射. 此外又有 $\rho(s) \circ f' = \rho(s) \circ (f - \lambda) = f' \circ \rho(s)$, 故由第一部分的证明知道 $f' = 0$, 故 f' 为伸缩变换. ■

特征标的正交性

设 f 与 g 是定义在 G 上的函数. [1] 令

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{s \in G} f(s) g(s^{-1}),$$

1) 取值在 $\mathbb{C}$ 中. —— 译注

这是一个标量积.

注 如果 g 是特征标, 则有 $g(s^{-1})=\overline{g(s)}$. [1] 因此 $\langle f,g\rangle$ 可以写成一个 Hermite 内积:

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

定理 A.7 (特征标的正交性) 设 V 与 V' 是两个不可约表示, χ 与 χ' 为相应的特征标. 那么

$$\langle\chi,\chi'\rangle=\begin{cases}1, & \text{若 } V=V' \text{ 且 } \chi=\chi',\\ 0, & \text{若 } V \text{ 与 } V' \text{ 不同构.}\end{cases}$$

• 考虑 $W=\mathrm{Hom}\,(V,V)$, 这是 G 的一个表示. 设 $\varphi\in W$, 则 φ 在 G 作用下稳定, 当且仅当对每个 $s\in G$ 有 $\varphi\circ s=s\circ\varphi$. 设 W^G 是 V 的 G 不变自同态 (即在 G 作用下稳定) 的集合. 由 Schur 引理知道 $\dim W^G=1$, 因此由定理 A.2 有

$$1=\frac{1}{|G|}\sum_{s\in G}\chi_W(s),$$

然而 $\chi_W(s)=\chi(s)\chi(s^{-1})$, 因此 $\langle\chi,\chi\rangle=1$.

• 如果 V 与 V' 不同构, 令 $W=\mathrm{Hom}\,(V,V')$, 又令 W^G 为 V 到 V' 的 G 不变同态的集合. Schur 引理说明 $\dim W^G=0$, 从而 $\langle\chi,\chi'\rangle=0$. ■

推论 A.8 G 的互不相同的不可约表示的特征标在 $\mathbb{C}$ 上是线性无关的 (它们称为 G 的不可约特征标).

这个定理也使我们能够证明 G 的特征标 "刻划了" 它的表示.

定理 A.9 设 V 是 G 的表示, 特征标为 χ_V. 设 $V=\oplus_{i=1}^{p}V_i$ 是将 V 分解为不可约表示 V_i 的直和, V_i 相应的特征标为 χ_{V_i}. 那么, 如果 W 是不可约表示, 特征标为 χ_W, 则与 W 同构的 V_i 之数目为 $\langle\chi_V,\chi_W\rangle$.

我们有

$$\chi_V=\sum_{i=1}^{p}\chi_{V_i},$$

$$\langle\chi_V,\chi_W\rangle=\sum_{i=1}^{p}\langle\chi_{V_i},\chi_W\rangle.$$

然而, 由前一定理, 根据 V_i 是否与 W 同构, $\langle\chi_{V_i},\chi_W\rangle$ 的取值为 1 或 0, 由此得到结论. ■

推论 A.10

• 与 W 同构的 V_i 之数目与特定的分解无关 (在这种意义下, 分解是唯一的).

• 具有相同特征标的两个表示相互同构.

1) 设 g 是表示 ρ 的特征标, 即 $g(s)=\mathrm{Tr}\,(\rho(s))$. 如果 $\lambda_1,\ldots,\lambda_n$ 是 $\rho(s)$ 的特征值, 则 $\lambda_1^{-1},\ldots,\lambda_n^{-1}$ 是 $\rho(s^{-1})$ 的特征值. 注意到 $\rho(s)$ 是有限阶矩阵, 因此 $\lambda_1,\ldots,\lambda_n$ 都是单位根, 故有 $\lambda_i^{-1}=\overline{\lambda_i}$, $1\le i\le n$. 从而 $g(s^{-1})=\sum_i\lambda_i^{-1}=\sum_i\overline{\lambda_i}=\overline{g(s)}$.—— 译注

• 若 $(W_i)_{1\le i\le m}$ 是 G 的全部不可约表示，则 G 的每个表示 V 都同构于一个直和 $\oplus n_iW_i$，其中 $n_i=\langle\chi_V,\chi_{W_i}\rangle$，而 $n_iW_i=W_i\oplus\cdots\oplus W_i$ (n_i 个因子).

A.3 特征标与中心函数

现在，来求不可约表示的数目 h (在相差一个同构的意义下)，也就是求不可约特征标的数目.

一个定义在 G 上取值在 $\mathbb{C}$ 中的函数，如果在 G 的每个共轭类上都取常值，则称为中心函数，所有中心函数的集合组成了一个 $\mathbb{C}$ 上的向量空间 $\mathcal{C}$，它的维数就等于 G 的共轭类的个数.

定理 A.11 *G 的不可约特征标 $(\chi_1,\ldots,\chi_h)$ 组成了 $\mathcal{C}$ 的一组基 (特别，h 就是 G 的共轭类的个数).*

证明这个定理要用到下面的

引理 A.12 *设 V 是不可约表示，特征标为 χ；又设 n 为 V 的维数 (即 $n=\chi(1)$). 设 $f\in\mathcal{C}$，用下式定义一个 V 上的自同态 π_f:*

$$\pi_f=\sum_{s\in G}f(s^{-1})\rho_V(s).$$

那么，π_f 是一个伸缩变换，伸缩系数为

$$\lambda=\frac{1}{n}\sum_{s\in G}f(s^{-1})\chi(s)=\frac{|G|}{n}\langle f,\chi\rangle.$$

若 $t\in G$，则由于 f 为中心函数，因此有

$$\pi_f.t=\sum_{s\in G}f(s^{-1})\rho_V(st)=\sum_{s\in G}f(u^{-1})\rho_V(tu),$$

其中 $u=t^{-1}st$，从而 $\pi_f.t=t.\pi_f$. 根据定理 A.6,π_f 是伸缩变换，又

$$\mathrm{Tr}\,(\pi_f)=n\lambda=\sum_{s\in G}f(s^{-1})\chi(s),$$

因此 $\lambda=\frac{|G|}{n}\langle f,\chi\rangle$. ■

现在可以来证明定理 A.11 了：假如 (χ_i) 不组成 $\mathcal{C}$ 的基底，则存在一个非零的 $f\in\mathcal{C}$ 与所有 χ_i 正交. 因此，上面的引理说明，对每个不可约表示，π_f 都是零，从而，对每个表示 (将其分解成直和),π_f 也是零. 现在，对一个特殊的表示来计算 π_f: 设 V 是 $|G|$ 维空间，有一组基底 $(e_s)_{s\in G}$，用下式定义一个 G 在 V 上的作用 ρ:

$$\rho(s).e_t=e_{st}.$$

这样定义的表示称为 G 的 *正则表示* (它的特征标记为 r_G. 若 $s\neq 1$，则 $r_G(s)=0$，而 $r_G(1)=|G|$). 对这个表示来计算 π_f，则有 $\pi_f=\sum_{s\in G}f(s^{-1})\rho(s)$，因此 $\pi_f(e_1)=\sum_{s\in G}f(s^{-1})e_s$ (因为 $e_{1.s}=e_s$). 如果 π_f 是零，则对每个 $s\in G$ 有 $f(s^{-1})=0$ (因为 $(e_s)_{s\in G}$ 组成一组基)，从而 f 是零，这与假设矛盾. ■

注 若 W 是一个不可约表示，那么正则表示中含有 n 个 W ($n = \dim W$). 实际上，若 χ 是 W 的特征标，则

$$\langle r_G, \chi \rangle = \frac{1}{|G|} \sum_{s \in G} r_G(s^{-1})\chi(s) = \chi(1) = \dim W.$$

因此 $r_G = \sum_{i=1}^{h} \chi_i(1)\chi_i$, 其中 χ_i 都是不可约特征标. 特别

$$r_G(1) = |G| = \sum_{i=1}^{h} \chi_i(1)\chi_i(1).$$

于是，若 $n_i = \chi_i(1)$, 则有

$$|G| = \sum_{i=1}^{h} n_i^2.$$

A.4 特征标的例子

我们来对 $n \leq 4$ 决定群 $\mathcal{A}_n$ 或者 $\mathcal{S}_n$ 的不可约特征标.

(1) 平凡情形： $\mathcal{S}_1 = \mathcal{A}_1 = \mathcal{A}_2 = \{1\}$, 此时只有一个不可约特征标： $\chi = 1$.

(2) 在群 $\mathcal{S}_2 = \{1, s\}$ (其中 $s^2 = 1$) 的情形，每个不可约特征标都是 1 次的 (这是因为，例如， $|\mathcal{S}_2| = 2 = \sum n_i^2$, 其中 n_i 是不可约特征标 χ_i 的次数), 所以有两个不可约特征标：

	1	s
χ_1	1	1
χ_2	1	-1

(3) 群 $\mathcal{A}_3 = \{1, t, t^2 \mid t^3 = 1\}$ 为 3 阶循环群. 由 $|\mathcal{A}_3| = 3 = \sum n_i^2$ 推出有 3 个 1 次不可约表示，它们的特征标如下：

	1	t	t^2
χ_1	1	1	1
χ_2	1	ρ	ρ^2
χ_3	1	ρ^2	ρ

其中 ρ 是 $\neq 1$ 的三次单位根.

(4) 对称群 $\mathcal{S}_3$ 就是二面体群 $\mathcal{D}_3$, 它有 3 个共轭类 $1, s, t$, 满足关系 $s^2 = 1, t^3 = 1, sts^{-1} = t^{-1}$. 两个 1 次不可约特征标由 1 与置换的符号给出. 此外，有 $\chi_1 + \chi_2 + n_3\chi_3 = r_{\mathcal{S}_3}$ 及 $\sum n_i^2 = |\mathcal{S}_3| = 6 = 2 + n_3^2$, 因此， $n_3 = 2$ 而 χ_3 的次数为 2.

然后，由

$$(\chi_1 + \chi_2 + 2\chi_3)(s) = r_{\mathcal{S}_3}(s) = 0$$

推出 $\chi_3(s) = 0$; 又由

$$(\chi_1 + \chi_2 + 2\chi_3)(t) = r_{\mathcal{S}_3}(t) = 0$$

推出 $\chi_3(t) = -1$. 因此，有

	1	s	t
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

如果将 $\mathcal{S}_3$ 看作为等边三角形的对称群，也可直接求出 χ_3. 于是，s 可以看作是对于一条直线的对称变换，相应的矩阵为 $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$，因此它的迹为 0; 而 t 可以看作为旋转 $2\pi/3$ 角度的变换，因此它的迹为 $2\cos(2\pi/3) = -1$.

(5) 群 $\mathcal{A}_4$ 的阶为 12, 有 4 个共轭类，代表元分别为 $1, s, t, t'$, 其中 s 的阶为 2 ($s = (a,b)(c,d)$),t 的阶为 3 ($t = (a,b,c)$) 而 $t' = t^2$. 已经有了 $\mathcal{A}_4$ 的 3 阶商群的 3 个表示. 此外，有 $\chi_1 + \chi_2 + \chi_3 + n_4\chi_4 = r_{\mathcal{A}_4}$ 及 $\sum n_i^2 = |\mathcal{A}_4| = 12$. 由此得到特征标表：

	1	s	t	t'
χ_1	1	1	1	1
χ_2	1	1	ρ	ρ^2
χ_3	1	1	ρ^2	ρ
χ_4	3	-1	0	0

如果将 $\mathcal{A}_4$ 看作正四面体的对称群，也可直接求出 χ_4. 于是，s 可以看作相对于连接两对边中点直线的对称变换. 在适当的基底下，它的矩阵表示为

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

因此. 它的迹为 -1. 此外，t 可解释为在一圆周上作轮换置换，因此，它的迹为 0.

这个结果也可用另一种方式得到：如果 W 是一维不可约表示，而 V 是不可约表示，那么 $V \otimes W$ 也是不可约表示. 特别，$\chi_4\chi_2$ 是不可约表示，考虑到次数，它必定等于 χ_4, 由此推出 $\chi_4(t) = \chi_4(t') = 0$.

练习 用同样的方法可以求出群 $\mathcal{S}_4$ 的特征标表. $\mathcal{S}_4$ 有 5 个共轭类，代表元为 $1, \sigma, s, t, \tau$, 其中 $\sigma = (a,b)$, $s = (a,b)(c,d)$, $t = (a,b,c)$, 而 $\tau = (a,b,c,d)$. 求出下表：

	1	σ	s	t	τ
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_4	3	1	-1	0	-1
χ_5	3	-1	-1	0	1

A.5 整性

设 G 为有限群，ρ 是 G 的表示，χ 是它的特征标.

命题 A.13 *χ 的取值都是代数整数.*

(复数 x 称为一个 *代数整数*, 是指存在整数 $n>0$ 与 $a_0,\dots,a_{n-1}\in\mathbb{Z}$, 使得

$$x^n+a_{n-1}x^{n-1}+\cdots+a_0=0.$$

所有代数整数的集合组成了 $\mathbb{C}$ 的一个子环.)

证明 群 G 为有限群, 所以, 有整数 $p>0$ 使对所有 $s\in G$ 都有 $s^p=1$, 从而对每个 s 都有 $\rho(s^p)=\rho(s)^p=1$. 若 λ 是 $\rho(s)$ 的特征值, 则 λ^p 是 $\rho(s)^p$ 的特征值, 因此 $\lambda^p=1$. $\rho(s)$ 的每个特征值都是代数整数, 而 $\chi(s)$ 是 $\rho(s)$ 的迹, 也就是 $\rho(s)$ 的所有特征值之和, 所以也是代数整数. ■

注 对每个 $s\in G$, $\rho(s)$ 都可对角化. 事实上, ρ 是 G 到 $\mathbf{GL}_n(\mathbb{C})$ 的映射, 对每个 $s\in G$, 矩阵 $\rho(s)$ 都相似于一个 Jordan 矩阵 J_s, 它是一个分块对角矩阵, 每块都形如

$$\begin{pmatrix}\lambda & 1 & \cdots & \times\\ & \ddots & \ddots & \vdots\\ & & \ddots & 1\\ & & & \lambda\end{pmatrix}$$

所以, $\rho(s)^p$ 相似于一个分块对角阵, 其每块都形如:

$$\begin{pmatrix}\lambda^p & p\lambda^{p-1} & \cdots & \times\\ & \ddots & \ddots & \vdots\\ & & \ddots & p\lambda^{p-1}\\ & & & \lambda^p\end{pmatrix}.$$

然而 $\rho(s)^p=1$, 这只有当 J_s 本身是对角阵时才能成立, 证毕. ■

(另证: 对 s 生成的循环群应用定理 A.5.)

下面来说明, 如何从群特征标的信息得出关于群本身的信息. 先给出以下的

命题 A.14 *设 G 是群, $G\neq\{1\}$. 那么, G 是单群的充要条件是: 对每个不等于 1 的不可约特征标 χ 及每个 $s\in G-\{1\}$ 都有*

$$\chi(s)\neq\chi(1).$$

设 $(\lambda_i)_{1\le i\le n}$ 为 $\rho(s)$ 的特征值. 已经看到 λ_i 都是单位根, 故 $|\lambda_i|=1$. 因为 $\chi(s)=\lambda_1+\cdots+\lambda_n$ 而 $\chi(1)=n$, 所以 $\chi(s)=\chi(1)=n$ 当且仅当每个 $\lambda_i=1$.[1] 因此, $\chi(s)=n$ 当且仅当 $s\in\ker\rho$.

现在, 假设 G 是单群, 则 $\ker\rho$ 是 G 的正规子群, 故等于 $\{1\}$ 或 G. 因此, 若对某个 $s\in G-\{1\}$ 有 $\chi(s)=\chi(1)$, 则 $\rho=\mathrm{Id}$, 从而 $\chi=1$. 反过来, 若 G 不是单群, 设 N 为 G 的一个非平凡正规子群. 设 χ' 为 G/N 的非平凡特征标, 相应的表示为 ρ'. 那么

$$G\longrightarrow G/N\xrightarrow{\rho'}\mathbf{GL}_n(\mathbb{C})$$

1) 这用到以下的初等结果: 若 $\alpha_1,\dots,\alpha_n\in\mathbb{C}$ 都是单位模长, 而 $|\alpha_1+\cdots+\alpha_n|=n$, 则 $\alpha_1=\cdots=\alpha_n=1$. —— 原注

定义了 G 的一个表示 ρ, 它的特征标 $\chi \neq 1$, 并且有 $s \in G - \{1\}$ 满足 $\chi(s) = \chi(1)$. ■

现在来推广命题 A.13.

定理 A.15 *设 ρ 为群 G 的不可约表示, 特征标为 χ. 若 f 为 G 上的中心函数, 它取值都是代数整数. 令 $n = \chi(1)$, 则 $n^{-1}\sum_{s\in G} f(s)\chi(s)$ 也是代数整数.*

只要对那些在一个共轭类上取值为 1、在其余共轭类上取值为 0 的函数来证明本定理就可以了. 若 $s \in G$, 用 $Cl(s)$ 来记 s 的共轭类, 而 $c(s)$ 表示 $Cl(s)$ 的基数. 设 G 上的函数 f_s 在 $Cl(s)$ 上取值为 1, 在其它共轭类上取值为 0, 则由于 χ 为中心函数, 故有

$$\frac{1}{n}\sum_{t\in G} f_s(t)\chi(t) = \frac{1}{n}\sum_{t\in Cl(s)} \chi(t) = \frac{c(s)\chi(s)}{n}.$$

因此, 证明下面的定理就行了:

定理 A.16 *在定理 A.15 的假设条件及上述记号下, 对每个 $s \in G$, $\frac{c(s)\chi(s)}{n}$ 都是代数整数.*

设 X 为 G 上取值在 $\mathbb{Z}$ 中的中心函数之集合. 这是由 f_s 生成的 $\mathbb{Z}$ 上的自由模. X 上有一个自然的环结构, 其乘法运算为 *卷积*, $(f, g) \mapsto f * g$, 定义如下:

$$f * g(s) = \sum_{uv=s} f(u)g(v).$$

可以验证, 环 X 是结合且交换的, 而 "Dirac 函数" f_1 是环的单位元.

对 $f \in X$, 我们配上一个自同态 $\rho(f) = \sum f(s)\rho(s)$. 根据引理 A.12,$\rho(f)$ 是伸缩变换, 即可看 $\mathbb{C}$ 中的元素. 这样就得到一个映射 $\tilde{\rho} : X \to \mathbb{C}$, 它是一个环同态 (由公式 $\rho(f * f') = \rho(f).\rho(f')$ 推出). 因此, X 的象集 $\tilde{\rho}(X)$ 是 $\mathbb{C}$ 的子环, 而作为 $\mathbb{Z}$ 上的模它是有限型的. 用标准的证法即可推出这个环中的元素都是代数整数. 由于 $\frac{c(s)\chi(s)}{n}$ 等于 $\tilde{\rho}(f_s)$, 定理得证. ■

推论 A.17 *表示 ρ 的次数整除群的阶.*

实际上, 设 $n = \chi(1)$, 又用 $f(s) = \chi(s^{-1})$ 定义 G 上的函数 f. 那么, f 满足定理 A.15 的假设条件, 因此, $n^{-1}\sum_{s\in G} \chi(s^{-1})\chi(s)$ 是代数整数. 然而, $n^{-1}\sum_{s\in G} \chi(s^{-1})\chi(s) = |G|/n$ 是 $\mathbb{Q}$ 中的元素, 而 $\mathbb{Q}$ 中在 $\mathbb{Z}$ 上整的元素只能是 $\mathbb{Z}$ 中的元素, 因此, n 整除 $|G|$. ■

推论 A.18 *设 χ 为群 G 的 n 次不可约特征标, $s \in G$. 如果 $c(s)$ 与 n 互素, 则 $\frac{\chi(s)}{n}$ 是一个代数整数. 此外, 若 $\chi(s) \neq 0$, 则与 $\chi(s)$ 相应的 $\rho(s)$ 为伸缩变换.*

如果 $c(s)$ 与 n 互素, 则根据 Bézout 定理, 存在两个整数 $a, b \in \mathbb{Z}$, 使 $ac(s) + bn = 1$. 因此,

$$\frac{\chi(s)}{n} = \frac{ac(s)\chi(s)}{n} + b\chi(s).$$

根据命题 A.13,$\chi(s)$ 是代数整数, 根据定理 A.16, $\frac{c(s)\chi(s)}{n}$ 也是, 这就证明了推论中的第一个断言. 第 2 个断言则要用到以下的

引理 A.19 *若 $\lambda_1, \ldots, \lambda_n$ 都是单位根, 并且 $(\lambda_1 + \cdots + \lambda_n)/n$ 是代数整数, 那么, 或者 $\lambda_1 + \cdots + \lambda_n = 0$, 或者所有 λ_i 都相等.*

引理的证明 如果 λ 为单位根，则它在 $\mathbb{Z}$ 上的极小方程形如 $x^p-1=0$, 因此， λ 的每个共轭数也是单位根. (复习一下，若 $z\in\mathbb{C}$ 为代数数，则 z 的极小方程的根就称为 z 的共轭数.) 设 $z=(\lambda_1+\cdots+\lambda_n)/n$, 则由假设 z 是一个代数数，并且 z 的每个共轭数 z' 都可写为 $(\lambda_1'+\cdots+\lambda_n')/n$, 其中 λ_i' 都是单位根，因此， $|z'|\leq 1$. 将所有 z 的共轭数之乘积记作 Z, 则 $|Z|\leq 1$. 此外， Z 是有理数 (除了相差一个符号之外，它是 z 的极小多项式的常数项), 又是代数整数 (它是代数整数的乘积), 因而， $Z\in\mathbb{Z}$. 如果 $Z=0$, z 有一个共轭数为 0, 因此 $z=0$; 如果 $|Z|=1$, 则 z 的每个共轭数都是单位模长的，因此 $|z|=1$, 故所有 λ_i 之和模长为 n, 所以它们必定都相等 (参考命题 A.14 之注). ■

回到推论的第 2 个断言. 设 (λ_i) 为 $\rho(s)$ 的特征值，它们都是单位根，且 $\chi(s)=\mathrm{Tr}(\rho(s))=\sum\lambda_i$, 故结论可由引理推出. ■

A.6 应用: Burnside 定理

沿用前一节的记号.

定理 A.20 *设 s 是 $G-\{1\}$ 的元素， p 为素数. 假定 $c(s)$ (G 中与 s 共轭的元素个数) 是 p 的方幂. 那么，存在 G 的正规子群 N, $N\neq G$, 使得 s 在 G/N 中的象属于 G/N 的中心.*

设 r_G 为正则表示的特征标 (参阅 A.3 节). 当 $s\neq 1$ 时， $r_G(s)=0$. 此外， $r_G=\sum n_\chi\chi$ (对所有不可约特征标求和), 其中 $n_\chi=\chi(1)$. 因此有 $\sum\chi(1)\chi(s)=0$, 或者写作 $1+\sum_{\chi\neq 1}\chi(1)\chi(s)=0$, 从而有 $\sum_{\chi\neq 1}\frac{\chi(1)\chi(s)}{p}=-\frac{1}{p}$. 由于 $-\frac{1}{p}$ 不是代数整数，所以存在不等于 1 的不可约特征标 χ, 使得 $\frac{\chi(1)\chi(s)}{p}$ 不是代数整数. 特别有， $\chi(s)\neq 0$, 且 p 不整除 $\chi(1)$, 从而 $c(s)$ 与 $\chi(1)$ 互素. 根据推论 A.18, 如果与 χ 相应的 G 的表示是 ρ, 则 $\rho(s)$ 是伸缩变换. 那么，若令 $N=\ker\rho$, 则群 N 是不等于 G 的正规子群. 另一方面， G/N 可以与 ρ 在 $\mathbf{GL}_n(\mathbb{C})$ 中的象等同，而 s 在 ρ 之下的象则是伸缩变换，因此属于 G/N 的中心. ■

现在可以推出

定理 A.21 (Burnside) *设 p 与 q 为素数，则每个阶为 $p^\alpha q^\beta$ 的群都是可解群.*

不妨假定 α 与 β 都非零 (否则 G 为幂零群), 对 $|G|$ 作归纳法来证明本定理.

存在 $s\in G-\{1\}$, 使 q 不整除 $c(s)$. 实际上， $G=\{1\}\cup\{Cl(s)\}$, 其中 $Cl(s)$ 是不同于 1 的共轭类. 因此， $|G|=1+\sum|Cl(s)|=1+\sum c(s)$. 由于 q 整除 $|G|$, 故存在 s 使 q 不整除 $c(s)$. 然而， $c(s)$ 整除 $|G|$, 故 $c(s)$ 是 p 的方幂. 根据前一定理，存在 G 的正规子群 N, $N\neq G$, 使得 s 在 G/N 中的象属于 G/N 的中心. 若 $N\neq\{1\}$, 对 N 与 G/N 应用归纳假设，知道它们都是可解群，因此 G 也是可解群. 如果 $N=\{1\}$, 则 G 的中心 C 包含 s, 因而非平凡. 对 C 与 G/C 应用归纳假设，即可推出 G 是可解群. ■

A.7 Frobenius 定理的证明

设 G 为有限群， H 是 G 的子群. H"不与它的共轭子群相交", 就是说，对所有 $g\in G-H$,

$$H\cap gHg^{-1}=\{1\},$$

参见 §6.2.

定理 A.22 (Frobenius) 设 $N = \{1\} \cap \{G - \cup_{g\in H} gHg^{-1}\}$, 则 N 是 G 的正规子群, 并且 G 是 H 与 N 的半直积.

证明的要点在于说明 H 的线性表示可以扩张到整个 G 上. 首先证明下面的

引理 A.23 设 f 是 H 上的中心函数, 那么, 存在唯一一个 G 上的中心函数 $\tilde{f}$, 它满足下面两个条件:

(1) $\tilde{f}$ 是 f 的扩张, 即, 若 $h \in H$, 则 $\tilde{f}(h) = f(h)$.

(2) 若 $x \in N$, 则 $\tilde{f}(x) = f(1)$, 即 $\tilde{f}$ 在 N 上取常值.

这个结果是容易的: 若 $x \notin N$, 则 x 可写成 ghg^{-1}, 使 $g \in G$, $h \in H$, 于是可令 $\tilde{f}(x) = f(h)$. 这个定义不依赖于 g, h 的选取, 因为, 如果 $g'h'g'^{-1} = ghg^{-1}$, 则有 $g'^{-1}ghg^{-1}g' = h'$, 因此, 或者 $h = h' = 1$, 或者 $g'^{-1}g \in H$. 在后一情形, h 与 h' 在 H 中是共轭的, 而由于 f 为中心函数, 故有 $f(h) = f(h')$. ■

下面, 我们用记号 $\langle \alpha, \beta\rangle_G$ 来表示相对于 G 的标量积 $\frac{1}{|G|}\sum_{s\in G}\alpha(s^{-1})\beta(s)$; 类似地, 用 $\langle \alpha, \beta\rangle_H$ 来表示相对于 H 的标量积. 如果 F 为 G 上的函数, 则用 F_H 来表示它在 H 上的限制.

引理 A.24 设 f 与 $\tilde{f}$ 如前面引理所述, 又设 θ 为 G 上的中心函数. 则有

$$\langle \tilde{f}, \theta\rangle_G = \langle f, \theta_H\rangle_H + f(1)\langle 1, \theta\rangle_G - f(1)\langle 1, \theta_H\rangle_H. \tag{A.1}$$

我们来证明这个等式. 如果 $f = 1$, 则 $\tilde{f} = 1$, 因此等式肯定成立. 因此, 由于线性的缘故, 只要对满足条件 $f(1) = 0$ 的函数 f 来验证 (A.1) 就可以了. 那么, 若令 $\mathcal{R}$ 为 H 左陪集的一个代表元组, 则当 r 取遍 $\mathcal{R}$ 时, rHr^{-1} 给出 H 的互不相同的共轭子群. 又, H 中每个 (不等于 1 的) 元素的共轭都可唯一地写作 rhr^{-1}, 使 $r \in \mathcal{R}$, $h \in H$. 由于

$$\langle \tilde{f}, \theta\rangle_G = \frac{1}{|G|}\sum_{s\in G}\tilde{f}(s^{-1})\theta(s),$$

而 $\tilde{f}$ 在 H 的共轭元素之外取值都是零, 所以, 上面的讨论说明

$$\langle \tilde{f}, \theta\rangle_G = \frac{1}{|G|}\sum_{(r,h)\in\mathcal{R}\times H}\tilde{f}(h^{-1})\theta(h) = \langle f, \theta\rangle_H,$$

后一等式是由于 $|G| = |H|\cdot|\mathcal{R}|$. ■

特殊情形 若 $\theta = 1$, 则有 $\langle \tilde{f}, 1\rangle_G = \langle f, 1\rangle_H$.[1] 因此, 映射 $f \mapsto \tilde{f}$ 是等距变换, 换句话说, 有 $\langle \tilde{f}_1, \tilde{f}_2\rangle_G = \langle f_1, f_2\rangle_H$. 实际上, 若令 $f_1^*(s) = f_1(s^{-1})$, 则有[2]

$$\frac{1}{|G|}\sum_{s\in G}\tilde{f}_1(s^{-1})\tilde{f}_2(s) = \langle \tilde{f}_1\tilde{f}_2^*, 1\rangle_G.$$

1) 原文为 $\langle \tilde{f}, 1\rangle_G = \langle f, 1\rangle_G$.—— 译注

2) 原文为 $\frac{1}{|G|}\sum_{s\in G}\tilde{f}_1(s^{-1})f_2(s) = \langle f_1^*\tilde{f}_2, 1\rangle_G$.—— 译注

又因为 $\widetilde{f_1 f_2} = \tilde{f}_1 \tilde{f}_2$, 故有 [1)]

$$\langle \tilde{f}_1, \tilde{f}_2 \rangle_G = \langle \tilde{f}_1 \tilde{f}_2^*, 1 \rangle_G = \langle f_1 f_2^*, 1 \rangle_H = \langle f_1, f_2 \rangle_H.$$

由此导出

命题 A.25 *若 χ 为 H 的特征标, θ 是 G 的特征标, 则 $\langle \tilde{\chi}, \theta \rangle_G$ 是整数.*

只要证明 (A.1) 式右边的每一项都是整数, 但这是显然的. ■

设 $\theta_1, \ldots, \theta_n$ 是 G 的全部互不相同的特征标, 则有 $\tilde{\chi} = \sum c_i \theta_i$, 并且由前面证明的结果, 知道每个 $c_i \in \mathbb{Z}$.

命题 A.26 *假设 χ 不可约, 则 c_i 中只有一个等于 1, 其余等于 0.*

(换句话说, $\tilde{\chi}$ 是 G 的不可约特征标.)

实际上, $\langle \tilde{\chi}, \tilde{\chi} \rangle_G = \langle \chi, \chi \rangle_H = 1 = \sum c_i^2$, 因此, 有某个 c_{i_0} 的平方等于 1, 其余的 c_i 等于 0. 如果 $c_{i_0} = -1$, 则有 $\tilde{\chi} = -\theta_{i_0}$, 然而 $\tilde{\chi}(1) = \chi(1) > 0$, 又 $\theta_{i_0}(1) > 0$, 这是不可能的. 因此必有 $c_{i_0} = 1$, 即 $\tilde{\chi} = \theta_{i_0}$. ■

推论 A.27 *如果 χ 是 H 的特征标, 则 $\tilde{\chi}$ 是 G 的特征标.*

如果将 χ 分解为不可约特征标之和, 结果就可由前面命题导出. ■

现在来证明 A.22. 选取 H 的一个表示 ρ, 要求它的核平凡, 例如, 可取正则表示. 设 χ 是 ρ 的特征标, 由推论 A.27, $\tilde{\chi}$ 是 G 的特征标, 设 $\tilde{\rho}$ 是相应于 $\tilde{\chi}$ 的 G 的表示. 如果 s 与 $H - \{1\}$ 中的某个元素共轭, 则 $\tilde{\rho}(s) \neq 1$. 另一方面, 若 $s \in N$, 则有 $\tilde{\chi}(s) = \chi(1) = \tilde{\chi}(1)$, 从而, 由命题 A.14 证明中的方法, 可知 $\tilde{\rho}(s) = 1$. 因此有 $N = \ker \tilde{\rho}$, 这证明了 N 是 G 的正规子群. ■

参考文献 (略)

(全文完)

(赵曼菲 译 姚景齐 校)

****

(上接 352 页)

Aumann: 伦理中立意味着对策理论家不需要提倡实现对策论的规范规定了. 对策论是关于自私的理论. 就象是我建议研究战争一样, 对策论研究自私性. 显然, 研究战争不等于提倡战争; 类似地, 研究自私性不是支持自私自利. 细菌学家不提倡疾病, 然而他们研究疾病. 对 "理性" 方式在精神上的还是伦理上是正确的, 对策论没有发表任何言论. 它仅仅表明理性的 —— 利己主义的 —— 实体将做些什么; 不是从伦理上说他们 "应该" 做什么. 如果我们希望我们的世界更美好, 我们最好关注一下理性动机将会把我们带往何处.

Hart: 对于我们这个迷人的访谈, 这是个非常好的结论. 谢谢您!

Aumann: 也谢谢 你, Sergiu, 为您在这个令人愉快的访谈中的出色表现.

参考文献 (略)

(全文完)

(孙连菊 译 陆柱家 校)

1) 原文为 $\langle \tilde{f}_1, \tilde{f}_2 \rangle_G = \langle \tilde{f}_1^* \tilde{f}_2, 1 \rangle_G = \langle f_1^* f_2, 1 \rangle_H = \langle f_1, f_2 \rangle_H$. —— 译注