有限群的经典表示论初步

戚天成 ✉

复旦大学 数学科学学院

2023 年 10 月 31 日

有限群表示论起源于 1896 年 Richard Dedekind(德国, 1831-1916) 和 Ferdinand Georg Frobenius(德国, 1849-1917) 的通信中, 由后者系统发展. 再由 Frobenius 的学生 Issai Schur(1875-1941) 显著地改进与简化了该理论. 这份笔记的目的是用结合代数观点简短有力地介绍有限群的经典表示论的基本概念和思想, 内容主要由以下两部分构成:

(1) 介绍群的表示的基本概念及其基本例子, 我们指出群的表示本质上就是群代数上的模结构, 等价的群表示对应同构的群代数上的模. 第一部分的主定理是 Maschke 定理, 它表明当有限群的表示的基域特征不整除该群的阶时, 任何表示都是一些不可约表示的直和, 所以这时要研究群的表示, 只需搞清楚不可约表示以及不可约表示间的联系即可. 用模的语言来说, 当基域的特征不整除群的阶时, 群代数是 Artin 半单环, 其上任何非零模完全可约, 于是只需搞清楚群代数上的不可约模以及不可约模之间的同态即可.

(2) 介绍群表示的特征标的概念和基本性质, 特征标作为精巧的数值不变量, 它不仅易计算把握, 且承载了充分多的表示信息. 例如, 我们会说明复数域上任意两个有限维表示等价当且仅当它们特征标一致 (见 [推论2.15]). 并且有限维复表示的不可约性可通过计算特征标复内积判别 (见 [推论2.16]), 这与第一部分提到的研究群复表示的根本任务是研究不可约表示以及不可约表示间的联系呼应. 并且用特征标理论不仅可证明对任给阶为两个不同素数正整数幂乘积的群不是单群 (见 [推论2.34]), 也可给出 Burnside 定理一个较为简单证明.

由于水平有限, 虽然我全力以赴, 但还是无法避免笔记中存在不足与错误, 欢迎指出, 谢谢.

1 基本概念

在有限群的 Sylow 定理学习中我们看到群作用是强有力的工具, 通过把群作用到某个集合上就足以反映出很多信息. 在环的结构理论中, 任何一个含幺环 R 上的左 R-模 M 就是环 R 的一个表示对象, 模本来就可以看成把环作用到某个 Abel 群上的产物. 通过模论工具我们可以得到环的大量结构信息. 而接下来我们将介绍的群表示, 它是把群线性地作用到线性空间上, 当作用在有限维线性空间上时, 群表示会把每个群中元素对应到一个具体的矩阵, 使得我们可以用线性代数的工具去认识群.

1.1 群的表示

Definition 1.1 (群的表示)**.** 设 G 是群, V 是域 $\Bbbk$ 上线性空间, 称群同态 $\rho: G \to GL(V)$ 是**群 G 在 V 上的一个 $\Bbbk$-线性表示**, 简称为 G 在 $\Bbbk$ 上的**表示**, 其中 $GL(V)$ 表示 V 上可逆线性变换全体构成的群. 这里的线性空间 V 称为表示 ρ 的**表示空间**. 当 ${}_{\Bbbk}V$ 是有限维空间时, 称表示 ρ **有次数 $\dim_{\Bbbk}V$**, 这时也称 ρ 是 G 的**有限维表示**. 当 ${}_{\Bbbk}V$ 作为线性空间维数不是有限时, ρ 为 G 的**无限维表示**.

有了群表示的概念, 随之而来的第一个问题是其存在性问题. 下面的例子给出一个平凡的表示.

Example 1.2 (平凡表示)**.** 设 G 是群, V 是域 $\Bbbk$ 上线性空间, 我们总有平凡群同态 $\rho: G \to GL(V), g \mapsto \mathrm{id}_V$. 称该表示 ρ 为 G 的**平凡表示**.

任给域 $\Bbbk$ 上的代数 A 以及左 A-模 M, M 总有天然的 $\Bbbk$-线性结构并且我们都可以通过 $a \in A$ 在 M 上决定的左乘变换给出 M 上的 $\Bbbk$-线性变换. 现在我们把目光聚焦在群代数上的模的情形, 把群的表示和群代数上的模联系起来. 我们马上会看到, 有一个群表示本质上与有一个群代数上的模是一样的.

Example 1.3. 设 G, H 是群, $\Bbbk$ 是域, 则有 $\Bbbk$-代数同构: $\Bbbk(G \times H) \cong \Bbbk G \otimes_{\Bbbk} \Bbbk H$.

Proof. 首先有标准 $\Bbbk$-线性映射 $\psi: \Bbbk(G \times H) \to \Bbbk G \otimes_{\Bbbk} \Bbbk H, (g, h) \mapsto g \otimes h$, 不难看出 ψ 是 $\Bbbk$-代数同态. 其次, 通过 $\Bbbk$-平衡映射

$$\Bbbk G \times \Bbbk H \to \Bbbk(G \times H), (\sum_{g \in G} a_g g, \sum_{h \in H} b_h h) \mapsto \sum_{(g,h) \in G \times H} a_g b_h (g, h)$$

可诱导 $\Bbbk$-双线性映射 $\varphi: \Bbbk G \otimes_{\Bbbk} \Bbbk H \to \Bbbk(G \times H)$ 满足 $\varphi(g \otimes h) = (g, h)$, 易验证 ψ 与 φ 互为逆映射. □

Example 1.4. 设 G 是群, $\Bbbk G$ 是群代数, 那么对任何群代数 $\Bbbk G$ 上的左模 M, M 有自然的 $\Bbbk$-线性结构, 即对每个 $x \in M$ 与 $c \in \Bbbk$, 定义 $cx = (c1_G)x$. 并且每个 g 都给出了 M 上的可逆 $\Bbbk$-线性变换 $\rho(g): M \to M, x \mapsto gx$, 因此我们得到映射 $\rho: G \to GL(M), g \mapsto \rho(g)$, 它明显是群同态, 故 ρ 是群 G 的一个表示.

事实上, 如果我们有了群 G 在 $\Bbbk$ 上的一个表示 $\rho: G \to GL(V)$, V 有天然的左 $\Bbbk G$-模结构

$$\left(\sum_{g \in G} a_g g\right) v = \sum_{g \in G} a_g \rho(g)(v), \forall v \in V, \sum_{g \in G} a_g g \in \Bbbk G.$$

所以一个群 G 的 $\Bbbk$-线性表示所承载的信息和一个群代数 $\Bbbk G$ 上的左模所载有的信息一致. 群代数 $\Bbbk G$ 上的左模自然会反映群 G 本身的一些信息, 以 $\Bbbk G$ 本身为例：对有限群 G, 有 $\dim_{\Bbbk} \Bbbk G = |G|$. 当群 G 有非平凡挠元 $g \neq 1_G$ 时, 群代数 $\Bbbk G$ 会有零因子, 具体地, 设 g 有阶 t, 那么 $(1_G - g)(1_G + g + \cdots + g^{t-1}) = 1_G - g^t = 0$.

Definition 1.5 (忠实表示)**.** 设 G 是群, V 是域 $\Bbbk$ 上线性空间, 如果群的表示 $\rho: G \to GL(V)$ 满足 $\mathrm{Ker}\rho = \{1_G\}$, 即 ρ 是单同态, 则称该表示是**忠实的**. 忠实表示意味着对每个 $g \neq 1_G \in G$, g 在线性空间 V 上的作用一定会使 V 中某个元素变动.

对每个群的表示 $\rho: G \to GL(V)$, 它可天然诱导单群同态 $\overline{\rho}: G/\mathrm{Ker}\rho \to GL(V)$, 所以从每个群的表示出发都可以产生一个忠实表示 $\overline{\rho}: G/\mathrm{Ker}\rho \to GL(V)$. 对任何群我们也可以构造它的忠实表示.

Example 1.6 (正则表示)**.** 设 $V = \Bbbk G$ 是群代数, 则有忠实表示 $\rho: G \to GL(V), g \mapsto g_l$, 其中 g_l 指 g 决定的左乘变换. 我们把该表示 ρ 称为群 G 的**正则表示**.

Definition 1.7 (表示的等价性)**.** 设 G 是群, $\Bbbk$ 是域, $\rho : G \to GL(V)$ 和 $\rho' : G \to GL(V')$ 均为群的表示, 如果存在线性同构 $f : V \to V'$ 使得下图对所有的 $g \in G$ 交换, 则称这两个表示是**等价的**.

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ {\scriptstyle \rho(g)}\downarrow & & \downarrow{\scriptstyle \rho'(g)} \\ V & \xrightarrow{f} & V' \end{array}$$

根据表示等价性的定义, 如果 $\rho : G \to GL(V)$ 和 $\rho' : G \to GL(V')$ 这两个表示等价, 即存在线性同构 $f : V \to V'$ 使得 $f\rho(g) = \rho'(g)f, \forall g \in G$, 那么 $f : V \to V'$ 给出左 $\Bbbk G$-模同构. 反之, 如果我们有两个同构的左 $\Bbbk G$-模 V, V', 设 $f : V \to V'$ 是 $\Bbbk G$-模同构, $\rho : G \to GL(V)$ 是 V 上 $\Bbbk G$-模结构给出的表示, $\rho' : G \to GL(V')$ 是 V' 上 $\Bbbk G$-模结构给出的表示, 那么 $f : V \to V'$ 是使得下图交换的线性同构.

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ {\scriptstyle \rho(g)}\downarrow & & \downarrow{\scriptstyle \rho'(g)} \\ V & \xrightarrow{f} & V' \end{array}$$

根据上面的讨论, 我们便看到下述命题成立.

Proposition 1.8. 设 G 是群, $\Bbbk$ 是域, $\rho : G \to GL(V)$ 和 $\rho' : G \to GL(V')$ 均为群的表示. 那么这两个表示等价的充要条件是用 ρ, ρ' 分别赋予 V, V' 左 $\Bbbk G$-模结构后, 作为左 $\Bbbk G$-模有同构 $V \cong V'$.

在本节最后, 用范畴语言来更严格地叙述群的表示与群代数上的模本质上一样. 为此, 引入

Definition 1.9 (群表示范畴)**.** 给定群 G 以及域 $\Bbbk$, 通过如下方式来定义范畴 $\mathrm{Rep}_{\Bbbk}(G)$: 定义对象类 $\mathrm{obRep}_{\Bbbk}(G)$ 为 G 在 $\Bbbk$ 上的线性表示 $\rho : G \to GL(V)$ 全体, 对任意两个群表示 $\rho : G \to GL(V)$ 和 $\rho' : G \to GL(V')$, 若线性映射 $f : V \to V'$ 使得下图对所有的 $g \in G$ 交换, 则称 f 是**表示 ρ 到 ρ' 的态** (或**态射**).

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ {\scriptstyle \rho(g)}\downarrow & & \downarrow{\scriptstyle \rho'(g)} \\ V & \xrightarrow{f} & V' \end{array}$$

记 $\mathrm{Hom}_{\mathrm{Rep}_{\Bbbk}(G)}(\rho, \rho')$ 为 ρ 到 ρ' 的所有态构成的集合. 于是可天然地定义表示间态的合成. 进而可得范畴 $\mathrm{Rep}_{\Bbbk}(G)$. 称为群 G 在 $\Bbbk$ 上的**表示范畴**. 记 $\mathrm{rep}_{\Bbbk}(G)$ 为群 G 在 $\Bbbk$ 上所有有限维表示构成的全子范畴.

Theorem 1.10. 给定群 G 以及域 $\Bbbk$, 那么有范畴同构 $\Bbbk G\text{-Mod} \cong \mathrm{Rep}_{\Bbbk}(G)$.

Proof. 对每个左 $\Bbbk G$-模 V, 可在 [例1.4] 意义下得到表示 $\rho : G \to GL(V)$, 记之为 FV. 任意两个 $\Bbbk G$-模之间的模同态 $f : V \to V'$, 可对应表示之间的态 $f : V \to V'$, 记为 $F(f)$. 由此得到函子 $F : \Bbbk G\text{-Mod} \to \mathrm{Rep}_{\Bbbk}(G)$. 对每个群的表示 $\rho : G \to GL(V)$, 根据之前的讨论, 可为 V 赋予天然的左 $\Bbbk G$-模结构, 记该左模为 $H(\rho)$. 表示间的态 f 明显给出群代数上左模之间的模同态 $H(f)$. 这定义出函子 $H : \mathrm{Rep}_{\Bbbk}(G) \to \Bbbk G\text{-Mod}$. 于是可直接验证 F 和 H 满足 $FH = 1_{\Bbbk G\text{-Mod}}, HF = 1_{\mathrm{Rep}_{\Bbbk}(G)}$ □

1.2 群的矩阵表示

如果群 G 在域 $\Bbbk$-上有一个次数为 $n \geq 1$ 有限维表示 $\rho : G \to GL(V)$, 那么每个 $g \in G$ 它都会对应一个 $\mathrm{M}_n(\Bbbk)$ 中的可逆矩阵. 具体地, 取定 V 的基 $B = \{u_1, ..., u_n\}$, 那么考虑每个 $\varphi \in \mathrm{End}_{\Bbbk}(V)$ 在这个基下表示矩阵 A, 即满足等式 $(\varphi(u_1), ..., \varphi(u_n)) = (u_1, ..., u_n)A$ 的矩阵 A, 我们可以得到 $\Bbbk$-代数同构

$$T : \mathrm{End}_{\Bbbk}(V) \to \mathrm{M}_n(\Bbbk), \varphi \mapsto A,$$

那么 T 自然把可逆线性变换全体 $GL(V)$ 映至可逆阵全体 $GL_n(\Bbbk)$, 并且把 T 限制在 $GL(V)$ 上就给出了群同构 $GL(V) \cong GL_n(\Bbbk)$, 所以通过下述同态列的合成 $\rho_B = T|\rho : G \to GL_n(\Bbbk)$

$$G \xrightarrow{\quad\rho\quad} GL(V) \xrightarrow{\quad T|\quad} GL_n(\Bbbk)$$

我们便可把每个群中元素 g 对应到可逆矩阵 $\rho_B(g)$. 那么 $g \in G$ 在 V 上的线性作用可由可逆阵 $\rho_B(g)$ 在 $\Bbbk^n$ 上的数乘作用描述. 这就引出了矩阵表示的概念.

Definition 1.11 (矩阵表示)**.** 设 G 是群, $\Bbbk$ 是域, $n \geq 1$, 称群同态 $\rho : G \to GL_n(\Bbbk)$ 为群 G 的 n **次矩阵表示**.

Example 1.12. 设 G 是群, $\Bbbk$ 是域, $\rho : G \to GL_n(\Bbbk)$ 为群 G 的 n 次矩阵表示. 那么 $\varphi : G \to \Bbbk^*, g \mapsto \det\rho(g)$, 这里 $\det\rho(g)$ 指 n 阶矩阵 $\rho(g)$ 的行列式, 是 G 的 1 次表示.

根据有限维线性变换和它在一给定基下表示矩阵的关系, 我们看到

Lemma 1.13. 设群 G 在域 $\Bbbk$-上有一个次数为 $n \geq 1$ 有限维表示 $\rho : G \to GL(V)$, 取定 V 的基 $B = \{u_1, ..., u_n\}$, 并设 $\eta_B : V \to \Bbbk^n$ 是满足 $\eta_B(u_i) = e_i, 1 \leq i \leq n$ 的线性同构, 其中 $e_i \in \Bbbk^n$ 是第 i 个标准单位列向量, 那么对由 B 诱导的矩阵表示 $\rho_B : G \to GL_n(\Bbbk)$, 有下图对所有 $g \in G$ 交换.

$$\begin{array}{ccc} V & \xrightarrow{\rho(g)} & V \\ {\scriptstyle\eta_B}\downarrow & & \downarrow{\scriptstyle\eta_B} \\ \Bbbk^n & \xrightarrow{\rho_B(g)} & \Bbbk^n \end{array}$$

线性代数中更一般的结果如下, 它的证明也是平凡的.

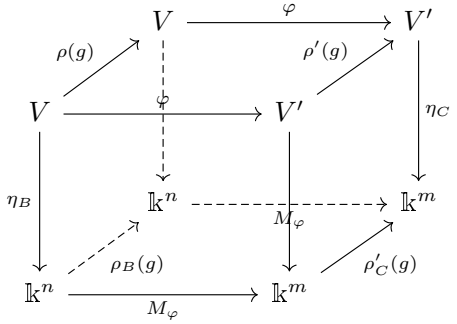
Lemma 1.14. 设 V 是域 $\Bbbk$ 上 n 维线性空间, V' 是域 $\Bbbk$ 上 m 维线性空间, 取定 V 的基 $B = \{u_1, ..., u_n\}$, 并设 $\eta_B : V \to \Bbbk^n$ 是满足 $\eta_B(u_i) = e_i, 1 \leq i \leq n$ 的线性同构, 其中 $e_i \in \Bbbk^n$ 是第 i 个标准单位列向量. 类似地, 取定 V' 的一个基 C, 可得线性同构 $\eta_C : V' \to \Bbbk^m$. 对任何线性映射 $\varphi : V \to V'$, 设 M_φ 是 φ 在基 B, C 下的表示矩阵, 那么下图交换

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & V' \\ {\scriptstyle\eta_B}\downarrow & & \downarrow{\scriptstyle\eta_C} \\ \Bbbk^n & \xrightarrow{M_\varphi} & \Bbbk^m \end{array}$$

根据前面的讨论, 给定一个次数是 n 的有限维表示 $\rho : G \to GL(V)$, 通过取定 V 的一个基 $B = \{u_1, ..., u_n\}$, 可产生一个群 G 的矩阵表示 $\rho_B : G \to GL_n(\Bbbk)$. 如果我们通过另一个 V 的基 $C = \{v_1, ..., v_n\}$ 来产生矩阵表示 $\rho_C : G \to GL_n(\Bbbk)$, 设基 B 到 C 的过渡矩阵是 $P \in GL_n(\Bbbk)$, 即 $(v_1, ..., v_n) = (u_1, ..., u_n)P$, 那么 $\rho_C(g) = P^{-1}\rho_B(g)P, \forall g \in G$. 这时我们可以对所有的 $g \in G$ 找到一个公共的可逆阵 P 使得对 $\rho_B(g)$ 作用 P 决定的相似变换后得到矩阵 $\rho_C(g)$. 这就引出了两个矩阵表示等价的概念.

Definition 1.15 (矩阵表示的等价)**.** 设 $\rho_1, \rho_2 : G \to GL_n(\Bbbk)$ 均为群 G 在 $\Bbbk$ 上的矩阵表示, 如果存在可逆阵 P 使得 $\rho_1(g) = P^{-1}\rho_2(g)P, \forall g \in G$, 称这两个矩阵表示是**等价的**, 记作 $\rho_1 \sim \rho_2$. 易知矩阵表示的等价作为群 G 在 $\Bbbk$ 上的矩阵表示全体构成的集合上的二元关系是等价关系.

从 [引理1.13] 以及 [引理1.14] 我们可以看到对任何两个群 G 在 $\Bbbk$ 上的有限维表示 $\rho : G \to GL(V)$ 和 $\rho' : G \to GL(V')$, 其中 $\dim_{\Bbbk} V = n, \dim_{\Bbbk} V' = m$, 只要 V 和 V' 之间有个左 $\Bbbk G$-模同态 $\varphi : V \to V'$, 就会产生下述交换图**:**



其中 B 是 V 取定的基, C 是 V' 取定的基. 进而我们看到等价的有限维群表示它们在给定基下决定的矩阵表示也等价. 反过来, 如果两个有限维表示 $\rho : G \to GL(V)$ 和 $\rho' : G \to GL(V')$ 满足 $n = m$ 且它们在给定基下决定的矩阵表示等价, 我们仍可构造上述形式的交换图. 总结一下, 我们得到

Proposition 1.16. 给定群 G 在 $\Bbbk$ 上的有限维表示 $\rho : G \to GL(V)$ 和 $\rho' : G \to GL(V')$, 其中 $\dim_{\Bbbk} V = n, \dim_{\Bbbk} V' = m$, 取定 V 的基 B, V' 的基 C, 并设 $\rho_B : G \to GL_n(\Bbbk), \rho'_C : G \to GL_m(\Bbbk)$ 是相应矩阵表示. 那么 ρ 和 ρ' 是等价的群表示当且仅当 $n = m$ 且 ρ_B 和 ρ'_C 是等价的矩阵表示.

Example 1.17 (置换表示)**.** 给定群 G 在集合 $\{1, 2, ..., n\}$ 上的一个作用, 它诱导群同态 $\pi : G \to S_n$ 使得 $\pi(g)(i) = gi, \forall i \in \{1, 2, ..., n\}$. 下面我们用群同态 $\pi : G \to S_n$ 来产生一个群 G 的有限维表示. 设 V 是域 $\Bbbk$ 上的 n 维线性空间, 取定 V 的基 $B = \{u_1, ..., u_n\}$. 那么对每个 $g \in G$, 通过定义 $\rho(g)(u_i) = u_{\pi(g)(i)} = u_{gi}$ 可唯一决定一可逆线性变换 $\rho(g) : V \to V$, 于是我们得到群同态 $\rho : G \to GL(V)$, 它给出群 G 一个次数为 n 的 $\Bbbk$-线性表示, 称为 G 的**置换表示**. 可以看到每个 $\rho(g)$ 在基 B 上的作用无非是把 $u_1, ..., u_n$ 进行重排, 因此 $\rho(g)$ 在 B 下的表示矩阵是置换矩阵.

Example 1.18 (表示的张量积)**.** 设群 G 有表示 $\rho : G \to GL(V)$ 和 $\rho' : G \to GL(V')$, 对每个 $g \in G$, 有线性同构 $\rho(g) : V \to V$ 以及 $\rho'(g) : V' \to V'$, 于是得到线性同构 $\rho(g) \otimes \rho'(g) : V \otimes_{\Bbbk} V' \to V \otimes_{\Bbbk} V'$. 通过定义 $\rho \otimes \rho' : G \to GL(V \otimes_{\Bbbk} V'), g \mapsto \rho(g) \otimes \rho'(g)$, 我们得到群同态 $\rho \otimes \rho'$, 称为**表示 ρ, ρ' 的张量积**. 如果 V 是 G 的 n 次表示, V' 是 G 的 m 次表示, 这里 n, m 是正整数, 那么表示的张量积 $\rho \otimes \rho'$ 是 nm 次表示. 若取定 V 的基 $B = \{u_1, ..., u_n\}$, V' 的基 $C = \{v_1, ..., v_m\}$, 设 $\rho(g)$ 在 B 下的表示矩阵是 $\rho_B(g)$, $\rho'(g)$ 在 C 下的表示矩阵是 $\rho_C(g)$, 那么 $(\rho \otimes \rho')(g)$ 在基 $\{u_1 \otimes v_1, u_1 \otimes v_2, ..., u_1 \otimes v_m, ..., u_n \otimes v_1, ..., u_n \otimes v_m\}$ 下的表示矩阵是矩阵 $\rho_B(g)$ 和 $\rho_C(g)$ 的 Kronecker 积 $\rho_B(g) \otimes \rho_C(g)$. 用模的语言来说, 表示的张量积对应的是对左 $\Bbbk G$-模 V, V', 在 $V \otimes_{\Bbbk} V'$ 上通过 $g(v \otimes v') = gv \otimes gv'$ 赋予 $V \otimes_{\Bbbk} V'$ 一个左 $\Bbbk G$-模结构.

1.3 完全可约性

设 G 是群, 我们已经看到群 G 在域 $\Bbbk$ 上的表示 $\rho: G \to GL(V)$ 本质上就是一个群代数 $\Bbbk G$ 上的模结构. 那么我们可以把模论的观点与工具带进群表示论来研究群的表示.

Definition 1.19 (不变子空间)**.** 设 $\rho: G \to GL(V)$ 是群 G 在域 $\Bbbk$ 上的表示, 若 V 的线性子空间 U 满足 $\rho(g)U \subseteq U, \forall g \in G$, 称 U 是 V 的 $\rho(G)$**-不变子空间**或 G**-不变子空间**.

根据 $\rho(G)$-不变子空间的定义可以看到, 对群 G 在域 $\Bbbk$ 上的表示 $\rho: G \to GL(V)$, V 的子集 U 是 $\rho(G)$-不变子空间的充要条件是将 V 视作左 $\Bbbk G$-模后 U 是 V 的子模. 因为 $\rho(g)$ 是 V 上可逆线性变换, 因此 $\rho(g)|_U$ 一定是 U 上单线性变换, 而每个 $x \in U$ 满足 $x = \rho(g)\rho(g^{-1})x$, 其中 $\rho(g^{-1})x \in U$, 所以 $\rho(g)$ 限制在 U 上可得 U 上可逆线性变换. 我们通过 $\rho(G)$-不变子空间来引入子表示的概念.

Definition 1.20 (子表示)**.** 设 $\rho: G \to GL(V)$ 是群 G 在域 $\Bbbk$ 上的表示, 若 V 的线性子空间 U 是 $\rho(G)$-不变子空间, 那么每个 $\rho(g)|_U : U \to U$ 是可逆线性变换, 因此可得群同态 $\rho|_U : G \to GL(U), g \mapsto \rho(g)|_U$, 称 $\rho|_U : G \to GL(U)$ 是 ρ **的子表示**. 子表示本质上就是一个 $\Bbbk G$-子模结构.

子表示无非是通过群代数上模的子模去认识群的表示. 完全类似地我们可以用商模去研究群的表示.

Definition 1.21 (商表示)**.** 设 $\rho: G \to GL(V)$ 是群 G 在域 $\Bbbk$ 上的表示, 若 V 的线性子空间 U 是 $\rho(G)$-不变子空间, 即 U 是 V 作为左 $\Bbbk G$-模的子模, 那么我们得到商模 V/U, 于是得到表示 $\rho|_{V/U} : G \to GL(V/U), g \mapsto g_l$, 这里 g_l 表示 $g \in G$ 所决定的商模 V/U 上的左乘变换, 称表示 $\rho|_{V/U}$ 是 ρ 的**商表示**.

如果 $\rho: G \to GL(V)$ 是群 G 在域 $\Bbbk$ 上的有限维表示, $\dim_{\Bbbk} V = n$ 且有子表示 $\rho|_U : G \to GL(U)$. 设 U 有基 $\{u_1, ..., u_r\}$, 并将其扩充为 V 的一个基 $B = \{u_1, ..., u_n\}$, 那么 $\rho(g)$ 在基 B 下的表示矩阵 $\rho_B(g)$ 是具有下述形式的分块矩阵.

$$\rho_B(g) = \begin{pmatrix} M_{11} & M_{12} \\ 0 & M_{22} \end{pmatrix}, M_{11} \in \mathrm{M}_r(\Bbbk), M_{12} \in \Bbbk^{r\times(n-r)}, M_{22} \in \mathrm{M}_{n-r}(\Bbbk).$$

特别地, 当 U 是 V 作为 $\Bbbk G$-模的一个直和因子, 即存在子模 U' 使得 $V = U \oplus U'$ 时, 取 U 的基 $\{u_1, ..., u_r\}$ 以及 U' 的基 $\{u_{r+1}, ..., u_n\}$ 来得到 V 的基 $B = \{u_1, ..., u_n\}$, 那么 $\rho(g)$ 在基 B 下的表示矩阵 $\rho_B(g)$ 是分块对角阵, 即上述分块矩阵的子矩阵 $M_{12} = 0$, 这样的矩阵具有更简单的形式. 因此我们可以把模的直和分解理论带进群表示论来把一个表示分解为一些尽可能简单的表示加以研究.

Definition 1.22 (表示的直和)**.** 设 $\rho: G \to GL(V)$ 是群 G 在域 $\Bbbk$ 上的表示, 若 V 作为左 $\Bbbk G$-模可以分解为有限个子模的直和, 设为 $V = U_1 \oplus U_2 \oplus \cdots \oplus U_m$, 记 $\rho_i = \rho|_{U_i}$ 是 ρ 的子表示, 我们称表示 ρ 是**子表示** $\rho_1, \rho_2, ..., \rho_m$ **的直和**, 记作 $\rho = \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_m$.

根据表示直和的定义我们知道表示的直和分解对应于群代数上模的直和分解. 如果表示 $\rho: G \to GL(V)$ 对应的左 $\Bbbk G$-模 V 是不可约模, 称该表示是**不可约的**. 若 V 是完全可约左 $\Bbbk G$-模, 称该表示是**完全可约的**.

下面的结果被称为 Maschke 定理. 该定理在复数域上的特殊情形由 H. Maschke(德国, 1853-1908), 呈现的版本由 L.E.Dickson(美国, 1874-1954) 先注意到.

Maschke's Theorem. 设 G 是有限群, 对任何域 $\Bbbk$, 只要 $\mathrm{char}\Bbbk \nmid |G|$, 那么 G 在域 $\Bbbk$ 上的表示 $\rho: G \to GL(V)(V \neq 0)$ 都是完全可约的. 特别地, 对满足 $\mathrm{char}\Bbbk \nmid |G|$ 的域 $\Bbbk$, 群代数 $\Bbbk G$ 是 Artin 半单代数.

Proof. 只需证任何左 $\Bbbk G$-模 V 的子模 U 是直和因子. 设 U_0 是 U 作为线性子空间的直和补, 即作为 $\Bbbk$-线性空间有直和分解 $V = U \oplus U_0$. 设 $p_0 : V \to U$ 是 V 作为线性空间在子空间 U 上的标准投射, 命

$$p = \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} p_0 \rho(g),$$

则 $p : V \to U$ 是满左 $\Bbbk G$-模同态且 $p|_U = \mathrm{id}_U$, 故 U 作为 $\Bbbk G$-子模是直和因子. □

Corollary 1.23 (群代数的半单性)**.** 设 G 是有限群, $\Bbbk$ 是域, 那么群代数 $\Bbbk G$ 半单的充要条件是 $\mathrm{char}\Bbbk \nmid |G|$.

Proof. 充分性由 Maschke 定理即得. 必要性：如果 $\mathrm{char}\Bbbk$ 整除 $|G|$, 那么 $z = \sum_{g \in G} g \neq 0$ 满足 $z^2 = |G|z = 0$ 以及 $zx = xz, \forall x \in G$, 因此 $z \in \mathrm{Jac}(\Bbbk G)$. 由 Wedderburn-Artin 定理知这说明 $\Bbbk G$ 不是 Artin 半单环. 但条件说群代数 $\Bbbk G$ 作为一个 Artin 环是半单的, 这就得到了矛盾. □

Maschke 定理的意义在于它告诉我们, 要研究有限群 G 在满足特征不整除 G 的阶的域上的表示, 只需要把不可约表示研究清楚即可, 因为完全可约模总可以分解为一些不可约模的直和.

Application 1.24 ($\mathbb{Z}G$ 半单)**.** 设 G 是有限群, 则 $\mathbb{Z}G$ 是 Artin 半单环.

Proof. 根据 Maschke 定理, 只要素数 p 不整除 $|G|$, 群代数 $\mathbb{F}_p G$ 半单, 其中 $\mathbb{F}_p$ 是 p 元有限域, 所以此时 $\mathrm{Jac}(\mathbb{F}_p G) = 0$. 对任给素数 p, 都有自然的满环同态

$$\alpha_p : \mathbb{Z}G \to \mathbb{F}_p G, \sum_{g \in G} b_g g \mapsto \sum_{g \in G} \overline{b_g} g,$$

易知 $\alpha_p(\mathrm{Jac}\mathbb{Z}G) \subseteq \mathrm{Jac}(\mathbb{F}_p G)$, 当素数 p 不整除 $|G|$ 时, 上述包含关系右端是 0, 由此可知对每个 $x = \sum_{g \in G} b_g g \in \mathrm{Jac}\mathbb{Z}G$, 并且每个系数 b_g 可以被无穷多素数整除, 这迫使 $x = 0$. 所以 $\mathrm{Jac}\mathbb{Z}G = 0$. 记 $m = |G|$, 那么 $\mathbb{Z}^m$ 到 $\mathbb{Z}G$ 有自然的满 $\mathbb{Z}$-模同态, 这表明 $\mathbb{Z}G$ 是左、右 Artin 环. 于是我们看到 $\mathbb{Z}G$ 是 Artin 半单环. □

1.4 模论的应用

我们已经引入过将群 G 的表示 $\rho : G \to GL(V)$ 视作群代数 $\Bbbk G$ 上的模的观点. 因此我们可以把模论工具引入到群表示论中. 例如 Artin 半单代数的不可约模同构类只有有限多个, 转换成群表示的语言就是

Proposition 1.25. 设 G 是有限群, $\Bbbk$ 是域, 满足 $\mathrm{char}\Bbbk \nmid |G|$. 那么 G 的不可约表示等价类只有有限多个.

对 $\Bbbk$-代数 A 上的左模 V, Krull-Schmidt 定理告诉我们只要 V 有合成列 (例如 V 是非零有限维模), 那么 V 可分解为有限个不可分模的直和, 并且这样的直和分解在不计次序和同构意义下唯一. 具体地, 若 ${}_A V \neq 0$ 有合成列, 则存在不可分子模 $V_1, ..., V_m \neq 0$ 使得 $V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$. 若还存在不可分子模 $W_1, ..., W_s$ 使得 $V = W_1 \oplus W_2 \oplus \cdots \oplus W_s$, 那么 $s = m$ 并且存在 $\sigma \in S_m$ 使得 $V_i \cong W_{\sigma(i)}, \forall 1 \leq i \leq m$. 现在我们设 G 是有限群, 域 $\Bbbk$ 满足 $\mathrm{char}\Bbbk \nmid |G|$, 那么 $A = \Bbbk G$ 是有限维半单代数, 对任何非零有限维模 ${}_A V$, 它可分解为有限个不可约子模的直和, 设为 $V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$, 其中每个 V_i 不可约, 由于不可约模一定不可分, 所以 ${}_A V$ 的不可约子模直和分解在不计次序和同构意义下唯一. 现在我们可以设有限维模 V 有不可约分解

$$V = V_1^{(1)} \oplus \cdots \oplus V_1^{(m_1)} \oplus V_2^{(1)} \oplus \cdots \oplus V_r^{(1)} \oplus \cdots \oplus V_r^{(m_r)},$$

其中每个 $V_i^{(k)}$ 是不可约模, 对每个 $1 \leq i \leq r$, 有 $V_i^{(k)} \cong V_i^{(l)}, \forall k, l \in \{1, 2, ..., m_i\}$, 只要 $i \neq j$, 就有 $V_i^{(k)} \ncong V_j^{(l)}$. 那么正整数序列 $m_1, ..., m_r$ 和正整数序列 $\dim_{\Bbbk} V_1^{(1)}, \dim_{\Bbbk} V_2^{(1)}, ..., \dim_{\Bbbk} V_r^{(1)}$ 被 V 唯一确定. 记左 A-模 V 给出群 G 的有限维表示为 $\rho : G \to GL(V)$, ρ_i 为 $V_i^{(1)}$ 决定的不可约表示, 称 ρ_i 是 ρ 的**不可约成分**, m_i 是 ρ_i 的**重数**. 现在我们取 $V = \Bbbk G$, 那么一样可设它有不可约分解 $V = V_1^{(1)} \oplus \cdots \oplus V_1^{(m_1)} \oplus V_2^{(1)} \oplus \cdots \oplus V_r^{(1)} \oplus \cdots \oplus V_r^{(m_r)}$ 满足之前我们假定的条件, 记每个 $V_i^{(1)}$ 作为左 $\Bbbk G$-模的自同态环是 Δ_i, 那么 Δ_i 是域 $\Bbbk$ 上的可除代数并且当 $\Bbbk$ 是代数闭域时, 下面的引理表明有代数同构 $\Delta_i \cong \Bbbk$.

Lemma 1.26. 设 $\Bbbk$ 是代数闭域, A 是 $\Bbbk$-代数, ${}_AM$ 是有限维不可约模, 则有 $\Bbbk$-代数同构 $\mathrm{End}_A(M) \cong \Bbbk$.

Proof. 这时 $\mathrm{End}_A(M)$ 是有限维 $\Bbbk$-可除代数, 而 $\Bbbk$ 是代数闭域, 故每个 $\varphi \in \mathrm{End}_A(M)$ 在 $\Bbbk$ 上最小多项式是一次的, 设为 $x - \lambda_\varphi$, 那么 $\varphi = \lambda_\varphi \mathrm{id}_M$, 由此可见 $\Bbbk \mapsto \mathrm{End}_A(M), a \mapsto a\mathrm{id}_M$ 是 $\Bbbk$-代数同构. □

于是由反代数同构 $\Bbbk G \cong \mathrm{End}_{\Bbbk G}(\Bbbk G) = \mathrm{End}_{\Bbbk G}(V)$ 以及 $\Bbbk$-线性同构

$$\mathrm{End}_{\Bbbk G}(V) \cong \prod_{i=1}^{r} \prod_{j=1}^{r} \mathrm{Hom}_{\Bbbk G}(V_i^{(1)}, V_j^{(1)})^{m_i m_j} \cong \prod_{i=1}^{r} \mathrm{End}_{\Bbbk G}(V_i^{(1)})^{m_i^2} = \prod_{i=1}^{r} \Delta_i^{m_i^2}$$

得到 $|G| = \dim_{\Bbbk} \Bbbk G = \sum_{i=1}^{r} m_i^2 \dim_{\Bbbk} \Delta_i$. 我们把上述讨论总结为下面的推论.

Corollary 1.27. 设 G 是有限群, 群代数 $\Bbbk G$ 半单, 并设 $V = \Bbbk G$ 作为左 $\Bbbk G$-模有不可约分解

$$\Bbbk G = V_1^{(1)} \oplus \cdots \oplus V_1^{(m_1)} \oplus V_2^{(1)} \oplus \cdots \oplus V_r^{(1)} \oplus \cdots \oplus V_r^{(m_r)},$$

其中每个 $V_i^{(k)}$ 是不可约模, 对每个 $1 \leq i \leq r$, 有 $V_i^{(k)} \cong V_i^{(l)}, \forall k, l \in \{1, 2, ..., m_i\}$, 只要 $i \neq j$, 就有 $V_i^{(k)} \ncong V_j^{(l)}$. 若记 $\Delta_i = \mathrm{End}_{\Bbbk G}(V_i^{(1)})$, 那么 $|G| = \dim_{\Bbbk} \Bbbk G = \sum_{i=1}^{r} m_i^2 \dim_{\Bbbk} \Delta_i$. 若进一步要求 $\Bbbk$ 是代数闭域, 则 $|G| = \sum_{i=1}^{r} m_i^2$.

我们再指出对上述不可约分解 $V = V_1^{(1)} \oplus \cdots \oplus V_1^{(m_1)} \oplus V_2^{(1)} \oplus \cdots \oplus V_r^{(1)} \oplus \cdots \oplus V_r^{(m_r)}$, 可直接验证 $\Bbbk$-代数同构 $\mathrm{End}_{\Bbbk G}(V) \cong \mathrm{End}_{\Bbbk G}((V_1^{(1)})^{m_1} \oplus \cdots (V_r^{(1)})^{m_r}) \cong \mathrm{End}_{\Bbbk G}(V_1^{(1)})^{m_1} \times \cdots \mathrm{End}_{\Bbbk G}(V_r^{(1)})^{m_r}$, 记 $\Delta_i = \mathrm{End}_{\Bbbk G} V_i^{(1)}$ 是域 $\Bbbk$ 上的有限维可除代数, 那么有 $\Bbbk$-代数同构

$$\mathrm{End}_{\Bbbk G}(V) \cong \mathrm{M}_{m_1}(\Delta_1) \times \cdots \times \mathrm{M}_r(\Delta_r),$$

于是得到 $\Bbbk$-代数同构 $\Bbbk G \cong \mathrm{M}_{m_1}(\Delta_1^{op}) \times \cdots \times \mathrm{M}_r(\Delta_r^{op})$. 我们把刚刚的讨论总结为

Corollary 1.28. 设 G 是有限群, 群代数 $\Bbbk G$ 半单, 并设 $\Bbbk G$ 作为左 $\Bbbk G$-模有不可约分解

$$\Bbbk G = V_1^{(1)} \oplus \cdots \oplus V_1^{(m_1)} \oplus V_2^{(1)} \oplus \cdots \oplus V_r^{(1)} \oplus \cdots \oplus V_r^{(m_r)},$$

其中每个 $V_i^{(k)}$ 是不可约模, 对每个 $1 \leq i \leq r$, 有 $V_i^{(k)} \cong V_i^{(l)}, \forall k, l \in \{1, 2, ..., m_i\}$, 只要 $i \neq j$, 就有 $V_i^{(k)} \ncong V_j^{(l)}$. 若记 $\Delta_i = \mathrm{End}_{\Bbbk G}(V_i^{(1)})$, 那么有 $\Bbbk$-代数同构 $\Bbbk G \cong \mathrm{M}_{m_1}(\Delta_1^{op}) \times \cdots \times \mathrm{M}_r(\Delta_r^{op})$. 这时同样可得 $|G| = \sum_{i=1}^{r} m_i^2 \dim_{\Bbbk} \Delta_i$. 若进一步要求 $\Bbbk$ 是代数闭域, 则代数同构 $\Delta_i \cong \Bbbk$ 表明 $\Delta_i = \Delta_i^{op}$, 从而有代数同构

$$\Bbbk G \cong \mathrm{M}_{m_1}(\Bbbk) \times \cdots \times \mathrm{M}_r(\Bbbk).$$

下面我们再把有限群的共轭类和群代数的中心联系起来.

Proposition 1.29. 设 G 是有限群, 共轭类全体是 $C_1=\{1_G\}, C_2, ..., C_r$, 对每个 $1\le i\le r$, 置 $c_i=\sum\limits_{g\in C_i} g$, 那么 $\{c_1, ..., c_r\}$ 是群代数 $\Bbbk G$ 中心 $Z(\Bbbk G)$ 作为 $\Bbbk$-线性空间的一个基, 特别地, $\dim_{\Bbbk} Z(\Bbbk G)=r$ 为共轭类个数.

Proof. 易见 $\{c_1, ..., c_r\}$ 是线性无关的, 只要证每个 $c_i\in Z(\Bbbk G)$ 以及任何 $c\in Z(\Bbbk G)$ 可被 $\{c_1, ..., c_r\}$ 线性表出即可. 任取 $g\in G$, 有 $gc_ig^{-1}=\sum\limits_{g_i\in C_i} gg_ig^{-1}=c_i$, 所以 $c_i\in Z(\Bbbk G)$. 对每个 $c\in Z(\Bbbk G)$, 设

$$c=\sum_{g\in G}\alpha_g g, \alpha_g\in\Bbbk,$$

那么 $c=hch^{-1}, \forall h\in G$, 由此可见 $\alpha_{hgh^{-1}}=\alpha_g, \forall h\in G$. 这蕴含 c 可被 $\{c_1, ..., c_r\}$ 线性表出. □

若设 Artin 半单代数 A 的极小左理想分解为 $A=I_1\oplus\cdots\oplus I_m$, 那么每个不可约左 A-模都同构于某个 I_k, 把这一观察和前面的讨论结合便有

Corollary 1.30. 设 G 是有限群, $\Bbbk$ 是代数闭域且群代数 $\Bbbk G$ 半单, $V=\Bbbk G$ 作为左 $\Bbbk G$-模有不可约分解

$$V=V_1^{(1)}\oplus\cdots\oplus V_1^{(m_1)}\oplus V_2^{(1)}\oplus\cdots\oplus V_r^{(1)}\oplus\cdots\oplus V_r^{(m_r)},$$

其中每个 $V_i^{(k)}$ 是不可约模, 对每个 $1\le i\le r$, 有 $V_i^{(k)}\cong V_i^{(l)}, \forall k, l\in\{1, 2, ..., m_i\}$, 只要 $i\ne j$, 就有 $V_i^{(k)}\ncong V_j^{(l)}$. 那么群 G 的共轭类总数 $\dim_{\Bbbk} Z(\Bbbk G)=r$ 就是 $\Bbbk G$ 上不可约模同构类总数.

Proof. 此时 $\Bbbk G\cong \mathrm{M}_{m_1}(\Bbbk)\times\cdots\times \mathrm{M}_r(\Bbbk)$, 再由 $Z(\Bbbk G)\cong Z(\mathrm{M}_{m_1}(\Bbbk))\times\cdots\times Z(\mathrm{M}_r(\Bbbk))$ 便知. □

Example 1.31 (置换群 S_n 的不可约复表示和整数拆分)**.** 对有限群 G, [推论1.30] 说 $\mathbb{C}G$ 上不可约模同构类总数恰是 G 共轭类数目. 当我们取 $G=S_n$ 为 n 次对称群时, S_n 中两个元素共轭当且仅当它们有相同的型 (回忆置换 $\sigma\in S_n$ 的型如下定义：当 σ 分解为不相交轮换分解后, 记 $\{1, 2, ..., n\}$ 中被 σ 作用固定不同的元素数目是 α_1, 不相交轮换分解中长度为 $i(2\le i\le n)$ 的轮换数目是 α_i, 称形式记号 $[1^{\alpha_1}2^{\alpha_2}\cdots n^{\alpha_n}]$ 是置换 σ 的**型**), 而置换 $\sigma\in S_n$ 的型 $[1^{\alpha_1}2^{\alpha_2}\cdots n^{\alpha_n}]$ 对应正整数 n 的拆分 $n=\alpha_1 1+\alpha_2 2+\cdots+\alpha_n n$(即把正整数 n 分解成一些正整数的和, 分解中数字 1 出现 α_1 次, 数字 $i(2\le i\le n)$ 出现 α_i 次), 我们把正整数 n 的拆分数记作 $p(n)$(例如, $p(1)=1, p(2)=2, p(3)=3, p(4)=5$), 那么 $p(n)$ 也就是 S_n 共轭类的数目. 所以 $\mathbb{C}S_n$ 不可约模同构类, 或者说 S_n 的不可约复表示等价类, 数目是 $p(n)$.

Example 1.32 (有限 Abel 群的不可约表示)**.** 设 $\Bbbk$ 是代数闭域, G 是有限 Abel 群, 那么 $\Bbbk G$ 是交换代数. 考虑 $\Bbbk G$ 上任何不可约左模 M, 它是有限维模, 由 [引理1.26] 知 M 上任何一个自同态是 $\Bbbk$ 中元素决定的数乘作用. 而 $\Bbbk G$ 的交换性使得每个 $g\in G$ 决定的 M 上左乘变换是左 $\Bbbk G$-模同态, 于是 M 的左 $\Bbbk G$-子模等价于 M 的 $\Bbbk$-线性子空间. 这一观察意味着 M 作为不可约左 $\Bbbk G$-模是 1 维的. 故

有限 Abel 群在代数闭域上的不可约表示都是 1 次的.

在 [推论1.30] 中我们看到只要代数闭域 $\Bbbk$ 的特征不整除有限群的阶 $|G|$, 那么有限群 G 在代数闭域 $\Bbbk$ 上的不可约表示等价类数恰好就是 G 的共轭类总数. 当 G 是有限 Abel 群时, 它的共轭类数目恰好是 $|G|$, 因此

对有限 Abel 群 G 和代数闭域 $\Bbbk$, 只要 $\mathrm{char}\Bbbk\nmid G$, 那么 G 的不可约表示等价类恰好 $|G|$ 个.

Example 1.33 (一般有限群的不可约表示构造)**.** 对含幺环 R, S 之间的保幺环同态 $\alpha : R \to S$, 我们可以使用 α 为每个左 S-模 M 赋予自然的左 R-模结构：$rx = \alpha(r)x, \forall r \in R, x \in M$. 如果 α 是满环同态, 易知 ${}_SM$ 是不可约模蕴含配备 α 诱导的 R-模 ${}_RM$ 也不可约. 应用这个观点于群的表示理论, 我们对每个有限群 G, 关于它的换位子群 $[G, G]$ 作商可得一有限 Abel 群 $\overline{G} = G/[G, G]$, 并且标准投射 $\pi : G \to \overline{G}$ 是满群同态, 它诱导满环同态 $\alpha : \Bbbk G \to \Bbbk\overline{G}, \sum\limits_{g\in G} a_g g \mapsto \sum\limits_{g\in G} a_g \pi(g)$, 由此能够从每个不可约 $\Bbbk\overline{G}$-模产生不可约左 $\Bbbk G$-模结构. 用群表示的语言说, 我们可以从有限 Abel 群 $\overline{G}$ 的不可约表示出发构造有限群 G 的不可约表示.

2 特征理论

虽然群的矩阵表示使得我们可以通过分析具体的对象结构来了解抽象的群, 但是对高阶群, 它的矩阵表示或是置换表示难以具体分析处理. 例如对充分大的正整数 n, 置换群 S_n 中每个元素的不相交轮换分解可能基本无法手算. 这时我们需要更精巧的数值不变量, 使得不通过复杂计算也能在一些具体处理问题的场合能为我们提供一些有用的信息. 大量实践经验表明特征标 (见 [定义2.1]) 所载有的表示信息在应用中卓有成效. 并且, 我们会说明对有限群的任意两个不可约复表示, 这两个复表示等价的充要条件是它们的特征标相同 (见 [推论2.15]). 并且有限维复表示的不可约性可通过计算特征标复内积判别 (见 [推论2.16]).

2.1 基本性质

Definition 2.1 (类函数, 特征标)**.** 设 G 是群, $\Bbbk$ 是域.

- 若函数 $f : G \to \Bbbk$ 在群 G 的每个共轭类上取值是常值的, 即 $f(gxg^{-1}) = f(x), \forall x, g \in G$, 则称 f 是一个**类函数**. 易见 G 的类函数全体关于通常加法和乘法构成含幺交换环, 称为 G 的**类函数环**.
- 若 $\rho : G \to GL(V)$ 是次数为 $n \geq 1$ 的有限维表示, 称 $\chi : G \to \Bbbk, g \mapsto \mathrm{tr}\rho(g)$ 为该表示的**特征标**. 不可约表示的特征称为**不可约特征标**. 称 ρ 的次数为该特征标的**次数**. 当 $\Bbbk = \mathbb{C}$ 时, 称 χ 是**复特征标**.

有时为了突出 χ 是表示 ρ 的特征标, 我们会把特征标记作 χ_ρ. 从特征的定义可以看到群表示的特征标是群上一个类函数. 群 G 两个等价的有限维表示特征标一致. 下面是关于有限维表示特征标的一些简单事实.

Example 2.2 (平凡表示特征标)**.** 设 $\rho : G \to GL(V)$ 是群 G 的 n 次平凡表示, 则该表示的特征标

$$\chi(g) = n1_\Bbbk, \forall g \in G.$$

Example 2.3 (子表示直和特征标)**.** 设 $\rho : G \to GL(V)$ 是群 G 的 $n \geq 1$ 次表示, 如果 ρ 是子表示 $\rho_1, \rho_2, ..., \rho_m$ 的直和, 即 $\rho = \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_m$, 若记 χ_i 是子表示 ρ_i 的特征标, 那么明显有 $\chi = \sum\limits_{i=1}^{m} \chi_i$.

Example 2.4 (商表示特征标)**.** 设 $\rho : G \to GL(V)$ 是群 G 的 $n \geq 1$ 次表示, 如果 U 是 V 的 $\Bbbk G$-子模, 设 ρ_U 和 $\rho_{V/U}$ 是相应子表示与商表示, 那么 $\chi_\rho = \chi_{\rho_U} + \chi_{\rho_{V/U}}$.

Example 2.5 (表示张量积的特征标)**.** 设群 G有有限维表示 $\rho : G \to GL(V)$ 和 $\rho' : G \to GL(V')$, 它们次数均正. 在 [例1.18] 中我们已经看到若取定 V 的基 $B = \{u_1, ..., u_n\}$, V' 的基 $C = \{v_1, ..., v_m\}$, 设 $\rho(g)$ 在 B 下的表示矩阵是 $\rho_B(g)$, $\rho'(g)$ 在 C 下的表示矩阵是 $\rho_C(g)$, 那么 $(\rho \otimes \rho')(g)$ 在基 $\{u_1 \otimes v_1, u_1 \otimes v_2, ..., u_1 \otimes v_m, ..., u_n \otimes v_1, ..., u_n \otimes v_m\}$ 下的表示矩阵是矩阵 $\rho_B(g)$ 和 $\rho_C(g)$ 的 Kronecker 积 $\rho_B(g) \otimes \rho_C(g)$. 于是 $\chi_{\rho\otimes\rho'} = \chi_\rho \chi_{\rho'}$.

2.2 复特征标

实际应用中我们更感兴趣复特征标, 它性质丰富. 例如对有限群 G 的 n 次复表示 $\rho: G \to GL(V)$, 每个 $\rho(g)$ 的特征值总是单位根, 进而 $\chi_\rho(g)$ 为一些单位根之和. 现在我们来看一些复特征标的基本性质.

Lemma 2.6. 设 G 是有限群, 它的**指数**是 m, 即全体元素阶的最小公倍数是 m. 那么对任何一个群 G 的 n 次复表示 ρ, 对每个 $g \in G$, $\rho(g)$ 在某个基下表示矩阵是由一些 m 次本原单位根构成的对角阵. 即 $\rho(g)$ 在某个基下表示矩阵形如 $\mathrm{diag}\{\omega_1, ..., \omega_n\}$, 其中每个 ω_i 是某个 m 次本原单位根. 于是 $\chi_\rho(g) = \sum_{i=1}^{n} \omega_i$.

Proof. 注意线性变换 $\rho(g)$ 在 $\mathbb{C}$ 上的最小多项式整除 $x^m - 1$, 故其最小多项式无重根且特征值均为 m 次本原单位根, 这表明线性变换 $\rho(g)$ 在 $\mathbb{C}$ 上可对角化且相似于一个主对角线都是 m 次本原单位根的对角阵. □

Remark 2.7. 上述引理表明对有限群 G 的任何有限维复表示 ρ, $\chi_\rho(g)$ 总是一些单位根的和, 而单位根总是代数整数 (回忆 $\alpha \in \mathbb{C}$ 被称为**代数数**, 如果 α 是某个首一整系数多项式的根), 而有限个代数整数的和仍是代数整数 (一般地, 对含幺交换环的扩环链 $R \subseteq E$, E 中所有在 R 上的整元, 即满足某个 R 上首一多项式的元素, 构成的集合总是 E 的子环, 称为 R 在 E 中的**整闭包**), 所以 $\chi_\rho(g)$ 是代数整数.

上述引理说有限群 G 它的任何 n 次复表示的特征标均是一些 m 次本原单位根的和, 这里 m 是 G 的指数. 于是对任何 n 次复表示 $\rho: G \to GL(V)$, 有 $|\chi_\rho(g)| \leq n$. 不等式中等号成立当且仅当存在 m 次本原单位根 ω 使得 $\rho(g) = \omega \mathrm{id}_V$. 充分性明显, 必要性：设 $\rho(g)$ 在某个基下表示矩阵形如 $\mathrm{diag}\{\omega_1, ..., \omega_n\}$, 其中每个 ω_i 是某个 m 次本原单位根. 那么 $\chi_\rho(g) = \sum_{i=1}^{n} \omega_i$ 且 $|\sum_{i=1}^{n} \omega_i| = n$ 迫使所有 ω_i 具有相同方向, 即都相同, 设 ω_i 的公共值是 ω, 那么我们便得到 $\rho(g) = \omega \mathrm{id}_V$. 我们把刚刚的讨论总结为

Proposition 2.8. 设 G 是有限群, 它的指数是 m, $\rho: G \to GL(V)$ 是 n 次复表示. 那么对每个 $g \in G$, 有 $|\chi_\rho(g)| \leq n$. 等号成立当且仅当存在 m 次本原单位根 ω 使得 $\rho(g) = \omega \mathrm{id}_V$. 特别地, 如果 $\chi_\rho(g) = n$, 那么 $\rho(g) = \mathrm{id}_V$. 也就是说我们可以直接从有限群 G 的复特征标 χ 在元素 g 上的取值读出 $\rho(g)$ 是否是恒等映射!

根据上述命题, 对有限群 G 的 n 次复表示 $\rho: G \to GL(V)$, 那些满足 $|\chi_\rho(g)| = n$ 的元素 g 对应了某个 m(m 表示群的指数) 次本原单位根诱导的数乘变换 $\rho(g) = \omega \mathrm{id}_V$. 同时也看到 $\{g \in G | \chi_\rho(g) = n\} = \mathrm{Ker}\rho$, 也称 $\{g \in G | \chi_\rho(g) = n\}$ 为**该特征标的核**, 记作 $\mathrm{Ker}\chi_\rho$. 我们也引入

$$Z(\chi_\rho) = \{g \in G | \text{特征标} |\chi_\rho(g)| = n\} = \{g \in G | \text{存在} m \text{次本原单位根} \omega \text{使得} \rho(g) = \omega \mathrm{id}_V\}$$

这也是群 G 的正规子群, 并且包含 $\mathrm{Ker}\chi_\rho = \mathrm{Ker}\rho$. 通过满群同态 $Z(\chi_\rho) \to U(m), g \mapsto \omega$, 这里 $\rho(g) = \omega \mathrm{id}_V$, 我们看到 $Z(\chi_\rho)/\mathrm{Ker}\rho$ 是循环群.

Example 2.9 (对偶表示)**.** 设有限群 G有 n 次复表示 $\rho: G \to GL(X)$, 那么可如下在 $X^* = \mathrm{Hom}_{\mathbb{C}}(X, \mathbb{C})$ 上赋予左 $\mathbb{C}G$-模结构：$g\varphi: X \to \mathbb{C}, x \mapsto \varphi(g^{-1}x)$, 于是得到 G 的表示 $\rho^*: G \to GL(X^*)$, 称为 G 关于 ρ 的**对偶表示**. 在 [引理2.6] 中我们看到对每个 $g \in G$, 可选取 X 的一个基 B 使得 $\rho(g)$ 在 B 下的表示矩阵形如 $\mathrm{diag}\{\omega_1, ..., \omega_n\}$, 其中每个 ω_i 是某个 m 次本原单位根, m 是 G 的指数, 考虑 B 对应的 X^* 中对偶基 B^*, 容易验证 $\rho^*(g)$ 在 B^* 下表示矩阵是 $\mathrm{diag}\{\overline{\omega_1}, ..., \overline{\omega_n}\}$, 所以 $\chi_\rho(g^{-1}) = \chi_{\rho^*}(g) = \overline{\chi_\rho(g)}, \forall g \in G$.

2.3 第一正交关系

固定有限群 G, 设 $\{\rho_1, \rho_2, ..., \rho_r\}$ 是 G 在 $\mathbb{C}$ 上不可约表示等价类的一个代表元集, ρ_i 的表示空间是 W_i, χ_i 是 ρ_i 的特征标. 那么 $\{W_1, ..., W_r\}$ 是 $\mathbb{C}G$ 上所有不可约模同构类的一个代表元集. 对每个 G 的有限维表示 $\rho : G \to GL(V)$, 我们已经看到 V 作为完全可约左 $\mathbb{C}G$-模可分解为一些不可约模的直和, 可设

$$V = V_1^{(1)} \oplus \cdots \oplus V_1^{(m_1)} \oplus V_2^{(1)} \oplus \cdots \oplus V_r^{(1)} \oplus \cdots \oplus V_r^{(m_r)},$$

其中每个 $V_i^{(k)}$ 是不可约模, 对每个 $1 \le i \le r$, $V_i^{\ell} \cong W_i, \forall 1 \le \ell \le m_i$, 这里 $m_1, ..., m_r$ 由 V 决定. 进而得到 $\mathbb{C}G$-模同构 $V \cong W_1^{m_1} \oplus W_2^{m_2} \oplus \cdots \oplus W_r^{m_r}$. 从 [例2.3] 可知 $\chi_\rho = \sum_{i=1}^{r} m_i \chi_i$. 接下来我们来说明 $\{\chi_1, ..., \chi_r\}$ 作为复线性空间 $\mathbb{C}^G = \{f : G \to \mathbb{C}\}$ 的子集线性无关. 一旦说明这一点我们马上得到

有限群 G 的两个有限维复表示等价当且仅当它们有相同的特征标.

我们通过证明下面的定理来得到特征标集 $\{\chi_1, ..., \chi_r\}$ 的 $\mathbb{C}$-线性无关性.

Theorem 2.10 (第一正交关系)**.** 设 G是有限群, $\Bbbk$ 的特征零的代数闭域. $\{\rho_1, \rho_2, ..., \rho_r\}$ 是 G 在 $\Bbbk$ 上不可约表示等价类的一个代表元集, ρ_i 的表示空间是 W_i, χ_i 是 ρ_i 的特征标. 那么对每个 $g \in G$, 有

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_j(g^{-1}) = \frac{1}{|G|}\sum_{g\in G}\chi_i(g^{-1})\chi_j(g) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

为了看到上述定理成立, 对有限群 G 的有限维表示 $\rho : G \to GL(V), \dim_{\Bbbk} V = n$, 设线性作用的不动点集

$$V^G = \{x \in V | gx = x, \forall g \in G\},$$

易见 V^G 是 V 作为左 $\Bbbk G$-模的一个子模, 并且 char$\Bbbk$=0 使得可构造满 $\Bbbk G$-模同态

$$p : V \to V^G, x \mapsto \frac{1}{|G|}\sum_{g\in G} gx$$

使得对标准嵌入 $i : V^G \to V$ 有 $pi = \mathrm{id}_{V^G}$, 因此 p 是 V 在直和因子 V^G 上的投射. 我们把 p 视作 V 上线性变换 $\tilde{p} : V \to V$ 并设 $\dim_{\Bbbk} V^G = t$, 那么可取 V 的一个基 B 使得 $\tilde{p} : V \to V$ 在 B 下的表示矩阵为

$$\begin{pmatrix} I_t & 0 \\ 0 & 0 \end{pmatrix},$$

所以 $\mathrm{tr}(\tilde{p}) = \dim_{\Bbbk} V^G$. 另一方面, 由 p 的定义可以看出 $\tilde{p} = (1/|G|)\sum_{g\in G} \rho(g)$, 对该等式两边取迹得

$$\tilde{p} = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g),$$

总结一下, 得到

Lemma 2.11. 对有限群 G 的有限维表示 $\rho : G \to GL(V), \dim_{\Bbbk} V = n$, 设线性作用的不动点集 $V^G = \{x \in V | gx = x, \forall g \in G\}$, 那么 $\dim_{\Bbbk} V^G = (1/|G|)\sum_{g\in G}\chi_\rho(g)$.

对群 G 上任意两个左 $\Bbbk G$-模 X,Y, 可如下赋予 $\mathrm{Hom}_{\Bbbk}(X,Y)$ 一个左 $\Bbbk G$-模结构：对每个 $g\in G$, $\varphi\in \mathrm{Hom}_{\Bbbk}(X,Y)$, 定义 $g\varphi: X\to Y, x\mapsto g\varphi(g^{-1}x)$. 那么 $\mathrm{Hom}_{\Bbbk}(X,Y)$ 给出群 G 的一个表示.

Example 2.12. 设 G 是群, X,Y 是左 $\Bbbk G$-模, 则 $\mathrm{Hom}_{\Bbbk}(X,Y)^G=\mathrm{Hom}_{\Bbbk G}(X,Y)$.

通过取对偶基容易验证下述经典同构.

Lemma 2.13. 设 G 是群, X,Y 是左 $\Bbbk G$-模, 那么 $X\otimes_{\Bbbk} Y$ 上通过表示的张量积可知有一个左 $\Bbbk G$-模结构 (见 [例1.18]), 对 $\mathrm{Hom}_{\Bbbk}(X,Y), X^*=\mathrm{Hom}_{\Bbbk}(X,\Bbbk)$ 通过前面的方式赋予左 $\Bbbk G$-模结构 (其中 $\Bbbk$ 上左模结构平凡), 则有左 $\Bbbk G$-模同构 $X^*\otimes_{\Bbbk} Y\cong \mathrm{Hom}_{\Bbbk}(X,Y)$.

现在我们把上述引理具体到有限维复表示的场景, 对有限维非零左 $\mathbb{C}G$-模 X,Y, 由模同构 $X^*\otimes_{\mathbb{C}} Y\cong \mathrm{Hom}_{\mathbb{C}}(X,Y)$ 知它们对应的表示有相同的特征标, 设 ρ_X,ρ_Y 分别是模 X,Y 对应的复表示. 从 [例2.5] 看到 $X^*\otimes_{\mathbb{C}}Y$ 的特征标由 $\chi_{\rho_X^*}\chi_{\rho_Y}$ 给出, 而 [例2.9] 中已说明 $\chi_{\rho_X^*}=\overline{\chi_{\rho_X}}$, 所以 $\mathrm{Hom}_{\mathbb{C}}(X,Y)$ 对应的表示的特征标是 $\overline{\chi_{\rho_X}}\chi_{\rho_Y}$. 因此由 $\mathrm{Hom}_{\mathbb{C}}(X,Y)^G=\mathrm{Hom}_{\mathbb{C}G}(X,Y)$ 以及 $\dim_{\mathbb{C}}\mathrm{Hom}_{\mathbb{C}}(X,Y)^G=(1/|G|)\sum_{g\in G}\overline{\chi_{\rho_X}(g)}\chi_{\rho_Y}(g)$ 知

Proposition 2.14. 设有限群 G 有有限维复表示 $\rho_X: G\to GL(X), \rho_Y: G\to GL(Y)$, 其中 $X,Y\neq 0$. 那么

$$\dim_{\mathbb{C}}\mathrm{Hom}_{\mathbb{C}G}(X,Y)=\frac{1}{|G|}\sum_{g\in G}\overline{\chi_{\rho_X}(g)}\chi_{\rho_Y}(g)=\frac{1}{|G|}\sum_{g\in G}\chi_{\rho_X}(g^{-1})\chi_{\rho_Y}(g)=\frac{1}{|G|}\sum_{g\in G}\chi_{\rho_X}(g)\chi_{\rho_Y}(g^{-1}).$$

现在我们可以给出 [定理2.10] 的证明：对不可约模同构类代表元集 $\{W_1,...,W_r\}$, 有

$$\dim_{\mathbb{C}G}\mathrm{Hom}_{\mathbb{C}G}(W_i,W_j)=\frac{1}{|G|}\sum_{g\in G}\overline{\chi_i(g)}\chi_j(g).$$

当 $i=j$ 时, [引理1.26] 说上式等号左边的维数是 1. 当 $i\neq j$ 时, 明显 $\mathrm{Hom}_{\mathbb{C}G}(W_i,W_j)=0$, 证毕.

对有限群 G, 在复线性空间 $\mathbb{C}^G$ 上, 对每个 $\varphi,\psi\in\mathbb{C}^G$, 通过定义

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

可赋予 $\mathbb{C}^G$ 复内积结构. 那么 [定理2.10] 无非是说不可约特征标集 $\{\chi_1,...,\chi_r\}$ 是两两正交且长度是 1 的向量集, 这也是为什么我们称该定理体现的是“正交关系”. 特别地, 我们得到 $\{\chi_1,...,\chi_r\}$ 是 $\mathbb{C}$-线性无关的.

Corollary 2.15. 有限群 G 的两个有限维复表示等价当且仅当它们有相同的特征标.

该推论表明有限群 G 的有限维复表示的特征标承载了复表示结构上的所有信息. 此外, 引入复内积语言后, 任何有限维表示的特征标在该复内积下的长度可由不可约分解中的“重数”表示. 具体地, 有

Corollary 2.16 (复表示的不可约性关于内积的判别)**.** 设有限群 G 有有限维复表示 $\rho: G\to GL(V)$, 并设有 $\mathbb{C}G$-模同构 $V\cong W_1^{m_1}\oplus W_2^{m_2}\oplus\cdots\oplus W_r^{m_r}(m_1,...,m_r$ 由 V 决定), 其中 $\{W_1,...,W_r\}$ 是 $\mathbb{C}G$-不可约模同构类代表元集, 它们对应的不可约表示特征标集设为 $\{\chi_1,...,\chi_r\}$. 我们有 $\chi_\rho=\sum_{i=1}^r m_i\chi_i$, 并且 $\langle\chi_\rho,\chi_\rho\rangle=\sum_{i=1}^r m_i^2$. 特别地, ρ 是不可约复表示当且仅当 $\langle\chi_\rho,\chi_\rho\rangle=1$. 若取 $V=\mathbb{C}G$, 那么 $\langle\chi_\rho,\chi_\rho\rangle=|G|$(回忆 [推论1.27]).

因为有限维复表示 χ_ρ 关于自己的复内积由定义是

$$\langle\chi_\rho,\chi_\rho\rangle=\frac{1}{|G|}\sum_{g\in G}\overline{\chi_\rho(g)}\chi_\rho(g),\forall g\in G,$$

特征标相当于算有限维线性空间上线性变换的迹, 它的计算并不需要把线性变换所有特征值解出, 因此计算复特征标的复内积在实际计算中是可行的. 前面提到有限群的元素个数可通过计算 $\mathbb{C}G$ 对应的复表示特征标自身和自身的内积得到, 任何有限维复表示的不可约性判别也可由复特征标内积计算得到. 所以有限群的特征标理论不止步于理论本身的优美与重要研究意义, 也具有很高的应用价值. 若有限群 G 的共轭类全体是 $\{C_1,...,C_r\}$, $\{\chi_1,...,\chi_r\}$ 是不可约复表示等价类的一个代表元集 $\{\rho_1,...,\rho_r\}$ 所对应的复特征标 (我们已经从 [推论1.30] 中看到 r 就是 $\mathbb{C}G$ 上所有不可约模等价类的数目), 每个 χ_i 可视作共轭类上的函数, 于是得到下表

	C_1	C_2	$\cdots$	C_r
χ_1	$\chi_1(C_1)$	$\chi_1(C_2)$	$\cdots$	$\chi_1(C_r)$
χ_2	$\chi_2(C_1)$	$\chi_2(C_2)$	$\cdots$	$\chi_2(C_r)$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
χ_r	$\chi_r(C_1)$	$\chi_r(C_2)$	$\cdots$	$\chi_r(C_r)$

称为群 G 的**复特征标表**. 设 $C_1=\{1_G\}$, 则特征标表 C_1 所在的列, 各元素 $\chi_i(C_1)$ 就是 ρ_i 的次数. 我们也指出特征标表实际上也给我们提供了一个复方阵

$$\begin{pmatrix} \chi_1(C_1) & \chi_1(C_2) & \cdots & \chi_1(C_r) \\ \chi_2(C_1) & \chi_2(C_2) & \cdots & \chi_2(C_r) \\ \vdots & \vdots & & \vdots \\ \chi_r(C_1) & \chi_r(C_2) & \cdots & \chi_r(C_r) \end{pmatrix} \in \mathrm{M}_r(\mathbb{C}).$$

下面应用特征标的复内积来导出有限群所有不可约复表示维数的平方和就是群的阶, 也就是说特征标表第一列的平方和, 即 $\sum\limits_{i=1}^{r}(\chi_i(C_1))^2(C_1=\{1_G\})$, 是 $|G|$.

在 [例1.6] 中引入了正则表示, 它相当于是对群 G 利用群代数上的模结构给出一个表示. 在 [推论1.27] 中我们也看到若有限群 G 与代数闭域 $\Bbbk$ 使 $\mathrm{char}k\nmid|G|$, 则考察正则表示对应的不可约模直和分解 $\Bbbk G\cong W_1^{m_1}\oplus W_2^{m_2}\oplus\cdots\oplus W_r^{m_r}$, 其中 $\{W_1,...,W_r\}$ 是 $\Bbbk G$-不可约模同构类代表元集, 会得到 $|G|=\sum\limits_{i=1}^{r}m_i^2$, 即正则表示的不可约表示直和分解中所有重数平方和给出群的阶. 下面我们说明当 $\Bbbk=\mathbb{C}$ 时每个 $m_i=\dim_{\Bbbk}W_i$, 即有限群 G 的正则表示的不可约表示直和分解中, 每个 W_i 对应表示 ρ_i 的重数 m_i 恰是 W_i 作为复线性空间的维数, 进而知群的阶 $|G|$ 就是所有 W_i 作为复线性空间的维数平方和.

Lemma 2.17. 设 G 是有限群, $\{W_1,...,W_r\}$ 是 $\mathbb{C}G$-不可约模同构类代表元集, 并设有 $\mathbb{C}G$-模同构 $\Bbbk G\cong W_1^{m_1}\oplus W_2^{m_2}\oplus\cdots\oplus W_r^{m_r}$, 那么对每个 $1\le i\le r$, 有 $m_i=\dim_{\mathbb{C}}W_i$. 进而 $|G|=\sum\limits_{i=1}^{r}(\dim_{\mathbb{C}}W_i)^2$.

Proof. 记 W_i 对应的不可约表示为 ρ_i, 其特征标是 χ_i, 正则表示仍记为 $\rho:G\to GL(\mathbb{C}G)$. 那么 [推论2.16] 说 $\chi_\rho=\sum\limits_{i=1}^{r}m_i\chi_i$, 从而对每个 i 有 $\langle\chi_\rho,\chi_i\rangle=m_i$. 另一方面, 由正则表示的定义不难看到 $\chi_\rho(g)=0,\forall g\ne1_G\in G$ 以及 $\chi_\rho(1_G)=|G|$. 所以

$$m_i=\langle\chi_\rho,\chi_i\rangle=\frac{1}{|G|}\sum_{g\in G}\overline{\chi_\rho(g)}\chi_i(g)=\frac{1}{|G|}\overline{\chi_\rho(1_G)}\chi_i(1_G)=\chi_i(1_G)=\dim_{\mathbb{C}}W_i.$$

□

在 [例1.32] 中我们看到有限 Abel 群 G 在代数闭域 $\Bbbk$ 上的不可约表示都是 1 次的, 所以群代数 $\Bbbk G$ 上的不可约模都是 1 维的. 下面我们用刚刚得到的事实给出一个有限群交换性的刻画.

Application 2.18 (有限群交换性刻画)**.** 设 G 是有限群, 则 G 交换的充要条件是任何不可约左 $\mathbb{C}G$-模都是 1 维的, 即任何不可约复表示都是 1 次的. 因此我们可以读特征标表第一列元素来判别有限群的交换性. 例如对称群 S_3 的共轭类总数是 $p(3)=3$(回忆 [例1.31]), 所以可设 S_3 的一个不可约复表示代表元集是 $\{\rho_1,\rho_2,\rho_3\}$, ρ_i 的次数是 m_i, 那么 $6=|S_3|=m_1^2+m_2^2+m_3^2$ 表明 S_3 存在次数高于 1 的不可约表示, 事实上求解上式的正整数解便知在等价意义下 S_3 有两个 1 次不可约表示和一个 2 次不可约表示. 这就反映了 S_3 是非交换的.

Proof. 只需说明充分性：如果任何不可约左 $\mathbb{C}G$-模都是 1 维的, 那么 [引理2.17] 表明 G 的共轭类总数就是 $|G|$, 这迫使群 G 每个元素所在的共轭类是单点集, 进而知 G 是交换群. □

2.4 第二正交关系

在 [定理2.10] 中我们得到了复特征标的第一正交关系, 本节我们介绍另一种正交关系, 它不仅指出复特征标表不同的列是正交的, 也为我们提供了用复特征标计算有限群中一给定元素所在共轭类元素数目的公式 (见 [定理2.19]).

对有限群 G, 设 G 的共轭类全体是 $\{C_1,...,C_r\}$, $\{W_1,...,W_r\}$ 是 $\mathbb{C}G$-不可约模同构类代表元集, 它们对应的不可约表示特征标集设为 $\{\chi_1,...,\chi_r\}$. 我们有下述特征标表

	C_1	C_2	$\cdots$	C_r
χ_1	$\chi_1(C_1)$	$\chi_1(C_2)$	$\cdots$	$\chi_1(C_r)$
χ_2	$\chi_2(C_1)$	$\chi_2(C_2)$	$\cdots$	$\chi_2(C_r)$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
χ_r	$\chi_r(C_1)$	$\chi_r(C_2)$	$\cdots$	$\chi_r(C_r)$

前面提到过我们可以把特征标表视作一个 r 阶复方阵

$$\begin{pmatrix} \chi_1(C_1) & \chi_1(C_2) & \cdots & \chi_1(C_r) \\ \chi_2(C_1) & \chi_2(C_2) & \cdots & \chi_2(C_r) \\ \vdots & \vdots & & \vdots \\ \chi_r(C_1) & \chi_r(C_2) & \cdots & \chi_r(C_r) \end{pmatrix}.$$

回忆不可约特征标的第一正交关系 (见 [定理2.10]) 表明

$$\frac{1}{|G|}\sum_{k=1}^{r}|C_k|\chi_i(C_k)\overline{\chi_j(C_k)}=\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)}=\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_j(g^{-1})=\begin{cases}1, & i=j\\ 0, & i\neq j\end{cases}.$$

作复方阵

$$A=\frac{1}{\sqrt{|G|}}\begin{pmatrix} \chi_1(C_1)\sqrt{|C_1|} & \chi_1(C_2)\sqrt{|C_2|} & \cdots & \chi_1(C_r)\sqrt{|C_r|} \\ \chi_2(C_1)\sqrt{|C_1|} & \chi_2(C_2)\sqrt{|C_2|} & \cdots & \chi_2(C_r)\sqrt{|C_r|} \\ \vdots & \vdots & & \vdots \\ \chi_r(C_1)\sqrt{|C_1|} & \chi_r(C_2)\sqrt{|C_2|} & \cdots & \chi_r(C_r)\sqrt{|C_r|} \end{pmatrix},$$

那么 A 的行向量是两两正交的单位复向量, 所以 A 是酉矩阵, 这说明 A 的列向量全体也是两两正交的单位向量. 于是我们得到了下述定理.

Theorem 2.19 (第二正交关系)**.** 设 G 是有限群, G 的共轭类全体是 $\{C_1,...,C_r\}$, $\{W_1,...,W_r\}$ 是 $\mathbb{C}G$-不可约模同构类代表元集, 它们对应的不可约表示特征标集设为 $\{\chi_1,...,\chi_r\}$. 那么
(1) 对每个共轭类 C_k, 有 $\sum\limits_{i=1}^{r}\overline{\chi_i(g)}\chi_i(g)=|G|/|C_k|, \forall g\in C_k$. 特别地, 对任何 $g\in G$, g 所在的共轭类元素个数是 $|G|/(\sum\limits_{i=1}^{r}|\chi_i(g)|^2)$, 这给出了用特征标计算共轭类元素个数的公式.
(2) 设 $a,b\in G$ 是不共轭的两个元素, 那么 $\sum\limits_{i=1}^{r}\overline{\chi_i(a)}\chi_i(b)=0$. 特别地, 复特征标表中任意两个不同的列作为 $\mathbb{C}^r$ 中列向量 (在标准复内积下) 正交.

[引理1.26] 表明代数闭域 $\Bbbk$ 上代数上的有限维不可约表示的自同态都是基域内某个元素的数乘, 因此对有限群 G 的不可约表示 $\rho_1,...,\rho_r$(设对应的不可约 $\Bbbk G$ 模分别为 $W_1,...,W_r$) 内固定的 ρ_i, 只要 $c\in Z(\Bbbk G)$, c 决定的左乘变换对应 W_i 上模自同态. 这一观察使我们看到：

Lemma 2.20. 设 G 是有限群, $c\in Z(\mathbb{C}G)$, 那么对任何 G 的不可约复表示 $\rho: G\to GL(V)$ 有

$$\tilde{\rho}(c)=\frac{\tilde{\chi}_\rho(c)}{\dim_{\mathbb{C}}V}\mathrm{id}_V,$$

这里 $\tilde{\rho}:\mathbb{C}G\to \mathrm{End}_{\mathbb{C}}V$ 的 ρ 的线性延拓, $\tilde{\chi}_\rho:\mathbb{C}G\to\mathbb{C}$ 是 χ_ρ 的线性延拓.

下述观察是之后证明 Burnside 定理所需必要准备.

Corollary 2.21. 设 G 是有限群, 设 G 的共轭类全体是 $\{C_1,...,C_r\}, C_1=\{1\}$, $\{W_1,...,W_r\}$ 是 $\mathbb{C}G$-不可约模同构类代表元集, 它们对应的不可约表示特征标集设为 $\{\chi_1,...,\chi_r\}$. 那么对任给 $g_j\in C_j$ 与特征标 χ_i 有

$$\frac{|C_j|\chi_i(g_j)}{\chi_i(1)}=\frac{|C_j|\chi_i(g_j)}{\dim_{\mathbb{C}}W_i}$$

是代数整数.

Proof. 沿用 [命题1.29] 中的记号, 对每个 $1\le i\le r$, 置 c_i 是共轭类 c_i 中所有元素的和, 那么 $\{c_1,...,c_r\}$ 是 $Z(\mathbb{C}G)$ 的一个基, 那么对任给正整数 $1\le s,t\le r$, 存在整数 $m_{stl}(1\le l\le r)$ 使得

$$c_sc_t=\sum_{l=1}^{r}m_{stl}c_l,$$

两边作用 W_i 对应不可约表示的线性延拓 $\tilde{\rho}_i:\mathbb{C}G\to\mathbb{C}$ 和 χ_i 的线性延拓 $\tilde{\chi}_i:\mathbb{C}G\to\mathbb{C}$ 可得

$$\frac{|C_s|\chi_i(g_s)}{\chi_i(1)}\frac{|C_t|\chi_i(g_t)}{\chi_i(1)}=\left(\sum_{l=1}^{r}m_{stl}|C_l|\chi_i(g_l)\right)/\chi_i(1).$$

对条件中固定的指标 i 和每个正整数 $1\le j\le r$, 记 $u_j=|C_j|\chi_i(g_j)/\chi_i(1)$, 补充定义 $u_0=1$ 并作考虑 $\mathbb{C}$ 作为 $\mathbb{Z}$-模的子模 $M=\mathbb{Z}u_0+\mathbb{Z}u_1+\cdots+\mathbb{Z}u_r$, 那么 M 是有限生成 $\mathbb{Z}$-模且对每个 u_j 有 $u_jM\subseteq M$. □

2.5 Burnside 定理

W. Burnside(英国, 1852-1927) 于 1904 年利用有限群表示论的工具证明了下述定理.

Burnside's Theorem. 设 p,q 是素数, $a,b\in\mathbb{N}$, 那么阶为 p^aq^b 的群是可解群.

本节的目标是证明上述定理, 首先我们回顾可解群的基本概念与性质. 若群 G 存在正规列

$$G=G_1\trianglerighteq G_2\trianglerighteq G_3\trianglerighteq\cdots\trianglerighteq G_s\trianglerighteq G_{s+1}=\{1_G\}$$

满足每个商因子 G_i/G_{i+1} 是 Abel 群, 则称 G 是**可解群**. 否则称该群**不可解**. 可解群的"可解"一词来源便是它在多项式根式求解问题上起到至关重要的作用——特征为零的域 F 上次数不低于 1 的多项式方程 $f(x)=0$ 可根式求解的充要条件是该多项式的 Galois 群是可解群. 让我们来回顾一些可解群的基本例子.

Example 2.22. 若单群 G 是可解群, 则 G 是 Abel 群. 故交错群 $A_n(n\geq 5)$ 不可解.

Remark 2.23. 这一观察表明 Burnside 定理成立意味着非交换有限单群的阶至少被三个不同的素数整除.

Example 2.24. 设 n 是正整数, 则当 $n\leq 4$ 时对称群 S_n 可解, 当 $n\geq 5$ 时对称群 S_n 不可解.

Proof. S_1 与 S_2 的可解性是明显的. S_3 有正规列 $S_3\trianglerighteq A_3\trianglerighteq\{(1)\}$, 它的两个商因子都是 Abel 群, 所以 S_3 也是可解群. 当 $n=4$ 时, 记 $K=\{(1),(12)(34),(14)(23),(24)(13)\}$, 可直接验证 K 是 S_4 的正规子群 (注意 4 阶群都交换, K 是 Abel 群), 所以 S_4 有正规列 $S_4\trianglerighteq A_4\trianglerighteq K\trianglerighteq\{(1)\}$, 它每个商因子都是 Abel 群, 所以 S_4 是可解群. 最后我们来看 $n\geq 5$ 的情形, 假设 S_n 可解, 那么有商因子都是 Abel 群的正规列 $S_n\trianglerighteq G_2\trianglerighteq G_3\trianglerighteq\cdots\trianglerighteq G_s\trianglerighteq\{(1)\}$, 那么存在正整数 $i\geq 2$ 使得 $G_i\neq S_n$, 设 l 是使得 $G_l\neq S_n$ 的最小正整数, 因为 $n\geq 5$ 时 S_n 的正规子群只有 $S_n,A_n,\{(1)\}$, 所以 $G_l=A_n$ 或 $\{(1)\}$, 但 G_{l-1}/G_l 是交换群, 所以 $G_l=A_n$. 因为 A_n 不是交换群, 所以存在正整数 $l+1\leq t\leq s$ 使得 $G_t\neq A_n$, 设 t 是满足条件的最小正整数, 那么由 A_n 是单群知 $G_t=\{(1)\}$, 于是 $G_{t-1}/G_t\cong A_n$ 非交换, 矛盾. 所以当 $n\geq 5$ 时 S_n 不是可解群. □

Remark 2.25. 这里关于 $n\geq 5$ 时 S_n 的正规子群只有 $S_n,A_n,\{(1)\}$ 可如下证明: 设 N 是 S_n 的一个正规子群, 如果 $N\subseteq A_n$, 那么由 A_n 是单群知 $N=\{(1)\}$ 或 A_n. 下设 $N\nsubseteq A_n$. 首先 $N\cap A_n=\{(1)\}$ 或 A_n, 如果 $A_n\subseteq N$, 那么由 $N\neq A_n$ 知 $N=S_n$. 如果 $N\cap A_n=\{(1)\}$, 那么由 $|N|>1$ 知 $NA_n=S_n$, 从而 $|N|=2$, 但当 $n\geq 5$ 时, S_n 不存在阶为 2 的正规子群, 矛盾.

Example 2.26. 称群 G 是**幂零群**, 如果群 G 存在中心正规列, 即有正规列

$$G=G_1\trianglerighteq G_2\trianglerighteq G_3\trianglerighteq\cdots\trianglerighteq G_s\trianglerighteq G_{s+1}=\{1_G\}$$

满足每个商因子 $G_i/G_{i+1}\subseteq Z(G/G_{i+1})$. 从该定义立即看到幂零群是可解群且任何 Abel 群是幂零群.

对群 G, 我们也将 G 的换位子群记作 G' 或 $G^{(1)}$, 将 G' 的换位子群记作 G'' 或 $G^{(2)}$, 递归地可以定义 $G^{(k)}=(G^{(k-1)})',k\geq 2$, 称 $G^{(k)}$ 为 G 的 k **次导群**. G 的零次导群定义为 G 本身. 下面是可解群的一个等价刻画, 我们将使用它去证明任何一个可解群的商群还是可解群.

Proposition 2.27. 给定群 G, 那么 G 可解的充要条件是存在正整数 k 使得 $G^{(k)}=\{1_G\}$.

Proof. 充分性：如果存在正整数 k 使得 $G^{(k)}=\{1_G\}$, 那么 G 有正规列 $G=G^{(0)}\trianglerighteq G^{(1)}\trianglerighteq\cdots\trianglerighteq G^{(k-1)}\trianglerighteq G^{(k)}=\{1_G\}$, 且该正规列每个商因子是交换群, 所以 G 可解. 必要性：假设 G 可解, 即有正规列 $G=G_1\trianglerighteq G_2\trianglerighteq G_3\trianglerighteq\cdots\trianglerighteq G_s\trianglerighteq G_{s+1}=\{1_G\}$. 如果 $s=1$, 结论直接成立, 下设 $s\geq 2$. 因为 G/G_2 是交换群, 所以 $G_2\supseteq G^{(1)}$. 假设对正整数 $1\leq i\leq s-1$ 有 $G_{i+1}\supseteq G^{(i)}$, 那么 G_{i+1}/G_{i+2} 为交换群表明 $G_{i+2}\supseteq G'_{i+1}\supseteq (G^{(i)})'=G^{(i+1)}$, 故归纳地我们得到 $G_{s+1}\supseteq G^{(s)}$, 因此取 $k=s$ 得到 $G^{(k)}=\{1_G\}$. □

Remark 2.28. 通过该命题立即得到可解群的子群都可解. 事实上也可以得到可解群的同态像都可解. 具体地, 给定可解群 G, 如果群 K 满足存在 G 到 K 的满群同态 $f:G\to K$, 那么 K 也是可解群. 我们断言对任何满群同态 $f:G\to K$ 必有 $f(G^{(i)})=K^{(i)},\forall i\geq 1$, 下面对正整数 i 作归纳. 当 $i=1$ 时, 群同态 f 将任何一个 G 的换位子映为 K 的一个换位子, 所以 $G^{(1)}\subseteq f^{-1}(K^{(1)})$, 于是 $f(G^{(1)})\subseteq K^{(1)}$. 反之, 因为 f 是满射, 所以 $f(G^{(1)})$ 包含任何一个 K 的换位子, 于是 $f(G^{(1)})\supseteq K^{(1)}$, 从而 $f(G^{(1)})=K^{(1)}$, 所以 $i=1$ 时结论成立. 假设结论对正整数 i 成立, 即 $f(G^{(i)})=K^{(i)}$, 那么对满群同态 $\tilde{f}:G^{(i)}\to K^{(i)},x\mapsto f(x)$ 应用 $i=1$ 时已证明的结论可得 $f(G^{(i+1)})=f((G^{(i)})')=(K^i)'=K^{(i+1)}$. 故由数学归纳原理知断言成立. 当 G 是可解群时, 由可解性的导群刻画知存在正整数 s 使得 $G^{(s)}=\{1_G\}$, 所以 $K^s=\{1_K\}$, 这说明 K 也是可解群. 特别地, 我们得到对可解群 G 的任何正规子群 N, G/N 也是可解群.

Corollary 2.29. 设 G 是群, 且有正规子群 N, 那么 G 是可解群的充要条件是 G/N 与 N 可解.

Proof. 根据前面的讨论, 只需再验证充分性. 由条件, N 有正规列 $N=N_1\trianglerighteq N_2\trianglerighteq\cdots\trianglerighteq N_s\trianglerighteq\{1_G\}$ 满足每个商因子是 Abel 群, G/N 有正规列 $G/N=\overline{G_1}\trianglerighteq\overline{G_2}\trianglerighteq\cdots\trianglerighteq\overline{G_t}\trianglerighteq\overline{1_G}$ 满足每个商因子是 Abel 群. 由子群对应定理, 存在 G 的子群 $G_i\supseteq N$ 使得 $G_i/N=\overline{G_i},\forall 1\leq i\leq t$. 易见子群列 $G=G_1\supseteq G_2\supseteq\cdots\supseteq G_t\supseteq N\supseteq N_2\supseteq\cdots\supseteq N_s\supseteq\{1_G\}$ 是正规列且每个商因子是 Abel 群, 故 G 是可解群. □

Example 2.30. 设 p 是素数, 那么 p-群是可解群.

Proof. 设该群的阶 $|G|=p^n$, 我们对正整数 n 作归纳. 当 $n=1$ 时, G 是 p 阶循环群, 有正规列 $G\trianglerighteq\{1_G\}$, 该正规列唯一的商因子交换, 结论成立. 下设结论对不超过 n 的正整数成立, 现考虑 p^{n+1} 阶群 G, 因为 p-群的中心非平凡, 所以 $Z(G)$ 也是 p-群, 设 $|Z(G)|=p^m,1\leq m\leq n+1$, 当 $m=n+1$ 时, 有 $Z(G)=G$, 即 G 是交换群, 此时有正规列 $G\trianglerighteq\{1_G\}$, 商因子同构于 G 为交换群. 如果 $1\leq m\leq n$, 那么 $G/Z(G)$ 与 $Z(G)$ 都是 p-群, 由归纳假设可知它们都是可解群, 所以 G 可解. □

接下来回到 Burnside 定理的准备中, 首先我们需要:

Lemma 2.31. 设 χ 是有限群 G 的某个不可约复表示 $\rho:G\to GL(V)$ 的特征标. 那么 G 的共轭类 C 满足 $|C|$ 与 $\chi(1)=\dim_{\mathbb{C}}V$ 互素, 那么对任给 $g\in C$ 有 $\chi(g)=0$ 或 $\rho(g)\in\mathbb{C}\mathrm{id}_V$.

Proof. 由条件知存在整数 m,l 使得 $m\chi(1)+l|C|=1$, 所以等式两边同时除以 $\chi(1)$ 并乘上 $\chi(g)$ 可得等式

$$\frac{\chi(g)}{\chi(1)}=l|C|\frac{\chi(g)}{\chi(1)}+m\chi(g),g\in C.$$

在 [推论2.21] 中我们看到对 $g\in C$ 有 $|C|\chi(g)/\chi(1)$ 是代数整数, 因此由 $\chi(g)$ 本身也是代数整数立即得到 $\chi(g)/\chi(1)$ 是代数整数. 设 $\chi(g)=\omega_1+\cdots+\omega_n$ 是 n 个 ℓ 次本原单位根的和 (回忆 [引理2.6]), 考虑 ℓ 次本原单位根 $\zeta_n=e^{2\pi i/\ell}$ 生成的 ℓ 次分圆域 $\mathbb{Q}(\zeta_\ell)$, 那么有有限扩张 $\mathbb{Q}(\zeta_\ell)\supseteq\mathbb{Q}$, 并且它是 Galois 扩张 (原因是 ζ_ℓ 在 $\mathbb{Q}$

上的最小多项式在 $\mathbb{Q}(\zeta_\ell)$ 上分裂). 考虑该域扩张的 Galois 群 $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_\ell)=\{\sigma\in\mathrm{Aut}\mathbb{Q}(\zeta_\ell)|\sigma(q)=q,\forall q\in\mathbb{Q}\}$. 注意到 $\chi(g)/\chi(1)\in\mathbb{Q}(\zeta_\ell)$, 并且对任何 $\sigma\in\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_\ell)$ 总有 $\sigma(\chi(g))$ 是 n 个 ℓ 次本原单位根的和. 现作

$$N=\prod_{\sigma\in\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_\ell)}\sigma\left(\frac{\chi(g)}{\chi(1)}\right),$$

那么 $\tau(N)=N,\forall\tau\in\mathrm{Aut}\mathbb{Q}(\zeta_\ell)$. 前面提到分圆域 $\mathbb{Q}(\zeta_\ell)$ 是 $\mathbb{Q}$ 的有限 Galois 扩张, 因此 $\mathbb{Q}(\zeta_\ell)$ 中关于 $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_\ell)$ 中所有元素作用不动的元素在 $\mathbb{Q}$ 中, 于是上面构造的 N 在 $\mathbb{Q}$ 中. N 作为有限个代数整数之积依然是代数整数, 结合它是有理数以及 $\mathbb{Q}\supseteq\mathbb{Z}$ 是整闭扩张可得 $N\in\mathbb{Z}$. 注意到对每个 $\sigma\in\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_\ell)$ 有 $\sigma(\chi(g)/\chi(1))$ 是模长不超过 1 非复数, 所以 $|N|=0$ 或 1. 如果 $N=0$, 那么 $\chi(g)=0$. 如果 $|N|=1$, 那么 [命题2.8] 表明存在 ℓ 次本原单位根 ω 使得 $\rho(g)=\omega\mathrm{id}_V$. 因此对固定的 $g\in C$ 有 $\chi(g)=0$ 或 $\rho(g)\in\mathbb{C}\mathrm{id}_V$. □

Remark 2.32. 这里回忆证明过程中涉及到的 Galois 理论的概念和相关性质. 对有限扩张 $E\supseteq F$, 总有 $|\mathrm{Aut}_F E|\leq[E:F]$. 如果等号成立, 则称该域扩张 $E\supseteq F$ 为 **Galois 扩张**. 设域扩张 $E\supseteq F$ 是有限扩张, 那么该域扩张 Galois 扩张的充要条件是对任给 $c\in E-F$, 存在 $\sigma\in\mathrm{Aut}_F E$ 使得 $\sigma(c)\neq c$. 设域扩张 $E\supseteq F$ 是有限扩张, 那么 $E\supseteq F$ 是 Galois 扩张的充要条件是存在 $\alpha\in E$ 使得 $E=F[\alpha]$ 且 α 在 F 上的首一最小多项式在 $E[x]$ 中可以分解为两两互异的一次多项式乘积, 即能够在 E 上分裂且没有重根.

Theorem 2.33. 设 G 是有限单群, 那么不存在 G 的共轭类 C 使得 $|C|$ 为某个素数的正整数幂.

Proof. 如果 G 是 Abel 群, 结论明显成立. 下设 G 非交换, 我们用反证法证明结论. 假设存在素数 p 与 G 的共轭类 C 使得 $|C|=p^\ell$, 其中 ℓ 是某个正整数. 设 G 有不可约复表示 $\{\rho_1,...,\rho_r\}$, 对应特征标集 $\{\chi_1,...,\chi_r\}$, 并记 $\rho_i(1)=n_i$. 我们不妨设 ρ_1 是平凡表示 $\rho_1:G\to GL(\mathbb{C}),g\mapsto\mathrm{id}_{\mathbb{C}}$, 那么 $n_1=1$ 且 $\chi_1(g)=1,\forall g\in G$.

Claim. 存在正整数 $2\leq j\leq r$ 使得 p 整除 n_j.

若不然, 只要正整数 i 满足 p 不整除 n_i, 那么 $|C|$ 与 $\chi_i(1)$ 互素, 于是应用 [引理2.31] 得到对 $g\in C$ 有 $\chi_i(g)=0$ 或 $\rho_i(g)\in\mathbb{C}\mathrm{id}$. 假设存在 $g\in C$ 使得 $\chi_i(g)\neq0$, 那么 $N=\{g\in G|\rho_i(g)\in\mathbb{C}\mathrm{id}\}$ 是 G 的非平凡正规子群, 由 G 是单群迫使 $N=G$, 所以 $G\cong\rho_i(G)$ 为 Abel 群, 这与条件矛盾, 所以 $\chi_i(g)=0,\forall g\in C$. 由特征标理论的第二正交关系 (回忆 [定理2.19]), 对 $g\in C$ 与 1 这两个不共轭的元素有

$$0=\sum_{i=1}^{r}\overline{\chi_i(1)}\chi_i(g)=\sum_{i=1}^{r}n_i\chi_i(g)=\chi_1(1)=1,$$

矛盾. 断言得证, 即有某个 n_j 能够被素数 p 整除. 依然考虑第二正交关系导出的等式

$$1+\sum_{i=2}^{r}n_i\chi_i(g)=0,g\in C.$$

通过前面证明断言的讨论我们知道上式那些满足 p 不整除 n_i 的项满足 $\chi_i(g)=0$, 因此由每个 $\chi_i(g)$ 是代数整数知上式蕴含 $1/p$ 是代数整数. 这与 $\mathbb{Q}\supseteq\mathbb{Z}$ 是整闭扩张矛盾. □

Corollary 2.34. 设 p,q 是不同的素数, $a,b\in\mathbb{N}_{\geq1}$, 那么阶为 p^aq^b 的群不是单群.

Proof. 设 G 是满足条件的有限群, 取 G 的一个 Sylow p-子群 P, 那么由 P 是 p-群知其中心 $Z = Z(P)$ 非平凡, 取 $z \neq 1 \in Z$, 那么 z 在群 G 中的中心化子 $C(z) \supseteq P$, 这意味着指数 $[G : C(z)]$(也是元素 z 所在的共轭类元素数目) 是素数 q 的幂次. 如果 $[G : C(z)] > 1$, 那么由 [定理2.33] 知 G 不是单群. 如果 $[G : C(z)] = 1$, 那么 $z \in Z(G)$, 于是 $Z(G) \neq 1$. 如果 $Z(G) \neq G$, 那么由 $Z(G)$ 是 G 的非平凡正规子群知 G 不是单群. 如果 $Z(G) = G$, 那么 G 作为阶不是素数正整数幂的 Abel 群自然不是单群. □

Remark 2.35. 该推论的意义是要寻找非交换的有限单群, 只需从阶至少含三个不同素因子的群里找.

现在我们可以正式地给出 Burnside 定理的证明: 对 $n = |G|$ 作归纳, 当 $n = 1$ 时结论直接成立. 假设结论对阶不超过 $n - 1(n \geq 1)$ 的群成立, 那么对 $n = p^a q^b$ 的有限群 G, 如果 a 与 b 中有一个为零, 那么 [例2.30] 保证了 G 可解. 下设 a, b 均不为零, 这时 [推论2.34] 保证了 G 存在正规子群 N 满足 $1 \subsetneq N \subsetneq G$, N 与 G/N 的阶都具备一个素数的自然数幂乘上一个素数的自然数幂的形式, 并且阶严格小于 n, 故对 N 和 G/N 应用归纳假设得到 $N, G/N$ 是可解群. 最后应用 [推论2.29] 得到 G 是可解群.

之前已经提到, Bernside 定理在有限单群分类问题中的基本意义是它告诉我们要寻找非交换有限单群只需从阶至少有三个不同素因子的群中找. 下述定理是有限单群分类问题中里程碑式的成果.

Feit-Thompson Theorem. 奇数阶单群可解, 因此任何奇数阶单群同构于奇素数阶循环群.

该定理由 W. Feit(美国, 1930-2004) 与 J. G. Thompson(美国, 1932-) 于 1963 年证明, 论文长达 255 页.