第二章 群作用

2.1 群作用

采用最原始的置换群定义来替代现代的抽象公理化群的定义有不少优势，也有一些不足. 在置换群中总有一个被置换的集合，而这一集合往往是研究群的工具. 例如，如果置换集的文字数为 n，那么由 Lagrange 定理知群阶整除 n 个文字对称群的群阶 $|S_n|=n!$.

群作用的基本思想是：借助置换群的某些优势来处理抽象群. 群作用既是一种构造子群与正规子群的重要工具，也是一种非常有效的计算工具，且可籍此证明某些群论定理，或求解某些涉及对称的组合问题.

定义 1 设 Ω 是非空集合，其元素称为文字，G 是群. 如果对每一个 $g\in G$，$\alpha\in\Omega$，都存在唯一确定的 $g\cdot\alpha\in\Omega$ 且满足如下条件

(1) $1\cdot\alpha=\alpha$ 对所有的 $\alpha\in\Omega$；　　(2) $(gh)\cdot\alpha=g\cdot(h\cdot\alpha)$ 对所有的 $\alpha\in\Omega, g,h\in G$.

则称**群 G 作用在集合 Ω 上**，也称“$\cdot$”是群 G 在 Ω 上的一个**作用**.

通常将 Ω 称为文字集，里边的元素称为**文字**，用小写希腊字母 α,β,γ 表示，群 G 中的元素称为**元**，用小写英文字母 g,h 等表示，群 G 的单位元与单位子群，都记为 1，文字集 Ω 上的恒等置换记为 id_Ω，$g\cdot\alpha$ 也课采用乘积的记号记为 $g\alpha$.

为叙述方便，若非特别指出，我们总是约定 G 是一个群，Ω 是一个非空集合.

群作用的原型是置换群，每一个置换群 S_Ω 自然定义了群 S_Ω 在 Ω 上的一个群作用.

设 G 是集 Ω 上全对称群 S_Ω 的子群，那么对任一 $g\in G,\alpha\in\Omega$，可以规定 $g\cdot\alpha:=g(\alpha)$，即群元 $g\in G$ 在文字 $\alpha\in\Omega$ 上的作用规定为置换 $g\in S_\Omega$ 在 α 上的作用.

对称群 S_Ω 的单位元 $1=\mathrm{id}_\Omega$ 是 Ω 上的恒等置换，保持每一个文字 α 不变，故 $1\cdot\alpha=\mathrm{id}_\Omega(\alpha)=\alpha$ 对所有的 $\alpha\in\Omega$，即群作用的定义条件(1)成立；

由群 S_Ω 中的乘法是映射的合成知定义条件(2)也成立.

所以集 Ω 上的置换群 G 自然的定义了群 G 在 Ω 上的一个群作用.■

定义 2 群 G 在 Ω 上的群作用称为**忠实的**是指：如果 $g\cdot\alpha=\alpha,\forall\alpha\in\Omega$，则 $g=1$.

根据定义，一个群作用是忠实的，当且仅当诱导出 Ω 上恒等变换的唯一元是单位元.

例 1 (1) 规定 G 在 Ω 上的**平凡作用**为：$g\cdot\alpha=\alpha,\forall\alpha\in\Omega,g\in G$. 则：群作用忠实 $\Leftrightarrow G$ 是单位群.

(2) 单位群在任一非空集合 Ω 的作用总是平凡的，也是忠实的.

(3) G 在 $\Omega=G$ 上的共轭作用规定为: $g\cdot x:=gxg^{-1},\forall g,x\in G$, 则: 群作用平凡 $\Leftrightarrow$ G 是交换群.

定义 3 设 G 作用在 Ω 上, 规定**群作用的核**为 $\{g\in G\mid g\cdot\alpha=\alpha,\forall\alpha\in\Omega\}$, 表示群 G 中与单位元 1 的作用一样固定 Ω 中所有文字的元所成子群, 这里称元 $g\in G$ **固定**文字 α 是指 $g\cdot\alpha=\alpha$.

一个群作用是忠实的, 当且仅当群作用的核是单位子群.

定理 1 设 G 作用在 Ω 上, 则群作用的核 $N=\{g\in G\mid g\cdot\alpha=\alpha,\forall\alpha\in\Omega\}$ 是群 G 的一个正规子群.

证明 由群作用的定义条件(1)知 $1\cdot\alpha=\alpha,\forall\alpha\in\Omega$, 这表明 $1\in N$, 故 N 非空.

任取 $x,y\in N$, 则 $x\cdot\alpha=\alpha,y\cdot\alpha=\alpha,\forall\alpha\in G$. 由群作用的定义条件(2)知

$$x^{-1}\cdot\alpha=x^{-1}\cdot(x\cdot\alpha)=(x^{-1}x)\cdot\alpha=1\cdot\alpha=\alpha,\forall\alpha\in\Omega,$$

于是 $(x^{-1}y)\cdot\alpha=x^{-1}\cdot(y\cdot\alpha)=x^{-1}\cdot\alpha=\alpha,\forall\alpha\in\Omega$, 所以 $x^{-1}y\in N$. 于是 N 是 G 的子群.

任取 $x\in N,g\in G$, 则对任一 $\alpha\in\Omega$ 有 $g\cdot\alpha\in\Omega$, 由 $x\in N$ 知 $x\cdot(g\cdot\alpha)=g\cdot\alpha$, 于是

$$(g^{-1}xg)\cdot\alpha=g^{-1}\cdot(x\cdot(g\cdot\alpha))=g^{-1}\cdot(g\cdot\alpha)=(g^{-1}g)\alpha=1\cdot\alpha=\alpha,$$

所以 $g^{-1}xg\in N$, 故 N 是 G 的正规子群.■

对有限群来说, 在某种意义下内部作用是最重要的群作用. 例如, 群 G 有两种重要的方式作用于自身.

(1) **左正则作用**是指群 G 在 $\Omega=G$ 自身上的左乘作用, 定义为: $g\cdot x=gx,\forall x,g\in G$. 直接验证知其满足群作用的定义条件, 作用核为单位子群:

$$\{g\in G\mid g\cdot x=x,\forall x\in G\}=\{g\in G\mid gx=x,\forall x\in G\}=1.$$

即: 左正则作用是忠实的.

(2) **共轭作用**是指群 G 在 $\Omega=G$ 自身上的共轭作用, 定义为: $g\cdot x=gxg^{-1},\forall x,g\in G$. 直接验证知其满足群作用的定义条件, 作用核恰为群的中心:

$$\{g\in G\mid g\cdot x=x,\forall x\in G\}=\{x\in G\mid gxg^{-1}=x,\forall x\in G\}=\{x\in G\mid gx=xg,\forall x\in G\}=\mathbf{Z}(G).$$

下面再给出较常见的其它群作用.

(3) 设 X 是群 G 的子集且 $g\in G$, 规定 $gX:=\{gx\mid x\in X\}$, 规定 ***G* 在其幂集 $P(G)$ 上的作用**为

$$g\cdot X=gX,\forall g\in G,X\subseteq G,$$

直接验证知其确实是群作用. 作用核为单位子群, 即该作用是忠实的:

$$\{g\in G\mid g\cdot X=X,\forall X\subseteq G\}=\{g\in G\mid gX=X,\forall X\subseteq G\}=1.$$

(4) 设 $H \le G$，令 $\Omega = \{xH \mid x \in G\}$ 为 H 在 G 中的全部左陪集所成集，规定 G 在 Ω 上的左乘作用为

$$g \cdot xH = gxH, \forall x, g \in G.$$

直接验证知其确实是群作用. 作用的核为

$$\{g \in G \mid g \cdot xH = xH, \forall x \in G\} = \{g \in G \mid gxH = xH, \forall x \in G\}$$

$$= \{g \in G \mid x^{-1}gx \in H, \forall x \in G\} = \{g \in G \mid g \in xHx^{-1}, \forall x \in G\} = \bigcap_{x \in G} xHx^{-1},$$

恰为与 H 共轭的全部子群的交，记为 $\mathrm{core}_G(H)$.

需要注意的是，通常情形下对右陪集所成集来说，如下两种方式未必定义了群作用:

(1) $g \cdot Hx = Hxg, \forall x, g \in G$；　　(2) $g \cdot Hx = Hgx, \forall x, g \in G$.

定理 2 设**群 G 作用在集 Ω 上**. 对任一 $g \in G$，定义 $\pi_g : \Omega \to \Omega$ 为 $\pi_g(\alpha) := g \cdot \alpha, \forall \alpha \in \Omega$，则 $\pi_g \in S_\Omega$，定义映射 $\theta : G \to S_\Omega$ 为 $\theta(g) = \pi_g, \forall g \in G$，则 θ 是从**群 G 到对称群 S_Ω 的群同态**，且**同态核恰为群作用的核**.

证明 (1) π_g 是集合 Ω 上的双射. (在群作用 $G \curvearrowright \Omega$ 下，每一群元自然诱导出 Ω 上的一个置换.)

π_g 单: 若 $\alpha, \beta \in \Omega$ 使得 $\pi_g(\alpha) = \pi_g(\beta)$，由 π_g 的定义知 $g \cdot \alpha = g \cdot \beta$，于是

$$\alpha = 1 \cdot \alpha = (g^{-1}g) \cdot \alpha = g^{-1} \cdot (g \cdot \alpha) = g^{-1} \cdot (g \cdot \beta) = (g^{-1}g) \cdot \beta = 1 \cdot \beta = \beta.$$

π_g 满: $\forall \beta \in \Omega$，令 $\alpha = g^{-1} \cdot \beta \in \Omega$，则

$$\pi_g(\alpha) = \pi_g(g^{-1} \cdot \beta) = g \cdot (g^{-1} \cdot \beta) = (gg^{-1}) \cdot \beta = 1 \cdot \beta = \beta.$$

(2) $\theta : G \to S_\Omega$ 是群同态，即 $\theta(gh) = \theta(g)\theta(h)$，或者等价地 $\pi_{gh} = \pi_g \pi_h, \forall g, h \in G$. 任取 $\alpha \in \Omega$，有

$$\pi_{gh}(\alpha) = (gh) \cdot \alpha = g \cdot (h \cdot \alpha) = \pi_g(h \cdot \alpha) = \pi_g(\pi_h(\alpha)) = (\pi_g \pi_h)(\alpha).$$

于是有 $\theta(gh) = \pi_{gh} = \pi_g \pi_h = \theta(g)\theta(h), \forall g, h \in G$.

(3) 也可先证明(2)，然后由群作用的定义条件(1)知 $\pi_1 = \mathrm{id}_\Omega$ 是集 Ω 上的恒等变换，然后对任一 $g \in G$，由 $\pi_g \pi_{g^{-1}} = \pi_1 = \mathrm{id}_\Omega = \pi_{g^{-1}} \pi_g$ 推得 $\pi_g \in S_\Omega$.

(4) 对任一 $g \in G$，$g \in \ker\theta \Leftrightarrow \mathrm{id}_\Omega = \theta(g) = \pi_g \Leftrightarrow g \cdot \alpha = \alpha, \forall \alpha \in \Omega \Leftrightarrow g$ 含于作用核.■

习题 设有群同态 $\theta : G \to S_\Omega$，规定群 G 在 Ω 上的群作用为:

$$g \cdot \alpha := (\theta(g))(\alpha), \forall g \in G, \alpha \in \Omega,$$

验证如上规定确实是一个群作用, 且群作用的核恰为同态核.

推论 1 设群 G 作用在集 Ω 上的核为 K, 则 $K \lhd G$ 且 G/K 与 S_Ω 的某个子群同构.

证明 令 $\theta: G \to S_\Omega$ 如引理 2. 由作用核恰为同态核知 $K = \ker\theta \lhd G$, 由同构定理 A 知

$$G/K = G/\ker\theta \cong \theta(G) \le S_\Omega,$$

即 G/K 与 S_Ω 的某个子群同构.■

定义 4 如果群 $G \neq 1$, 并且 G 只有平凡的正规子群 1 与 G 自身, 就称 G 是一个**单群**.

定理 3 设 G 是有限群, 则: G 是交换单群 $\Leftrightarrow$ G 是素数阶群.

证明 "$\Leftarrow$" 设 G 是素数 p 阶群, 由 Lagrange 定理知其子群阶整除群阶 p, 因此 G 仅有两个子群: 1 与 G 自身, 故 G 只有平凡的正规子群, 确实为单群.

"$\Rightarrow$" 如果 G 是交换单群, 则 $G \neq 1$, 任取一个非单位元 $a \in G$, 则由 G 交换知 $\langle a \rangle$ 是群 G 的一个非单位正规子群, 由 G 单知 $G = \langle a \rangle$ 循环. 如果 $o(a) = n$ 不是素数, 则 $n = rs$, 其中整数 r, s 满足 $1 < r, s < n$, 此时 $\langle a^r \rangle$ 是 G 的一个 s 阶非平凡正规子群, 矛盾! 所以 G 是素数阶群.■

单群是有限群的基本构建块, 找出所有的非交换单群是 20 世纪群论研究的中心课题. 为了寻找单群, 如果有一些好的非单性判别准则来排除某些群的单性, 进而缩小寻找范围是非常有用的. 因此, 我们认为, 凡是能导出群的某个非平凡正规子群存在性的定理可视为"好的"定理. 按此标准, 如下结论可以视为一个"好定理":

定理 4 设 $H \le G$ 且 $|G:H| = n < \infty$, 则

(1) 存在 $N \lhd G$ 使得 $N \le H$ 且 $|G:N| \mid n!$.　　(2) 如果 $n > 1$ 且 $|G| \nmid n!$, 则 G 不是单群.

证明 令 G 左乘作用于左陪集集合 $\Omega = \{xH \mid x \in G\}$ 上, 设 N 是作用核. 由推论 1 知 G/N 同构于 S_Ω 的某个子群. 由 $|\Omega| = |G:H| = n$ 知 $|S_\Omega| = n!$, 由 Lagrange 定理知 $|G:N| = |G/N| \mid n!$.

此时有 $N \subseteq H$: 任取 $x \in N$, 由 $H \in \Omega$ 知 $x \in xH = x \cdot H = H$.

为证明 G 不是单群, 只需证明 N 是 G 的非平凡正规子群. 由 $n > 1$ 知 $H < G$, 再由 $N \subseteq H$ 知 $N < G$. 若 $N = 1$, 则 $|G| = |G:N| \mid n!$, 与已知 $|G| \nmid n!$ 矛盾!■

为了利用定理 4 作为非单性准则, 我们需要寻找 G 的指数较小的子群. 第三章讨论的 Sylow 定理就是寻找子群的强有力技术.

推论 2 如果有限群 G 的子群 H 的指数 $|G:H| = p$ 是群阶 $|G|$ 的最小素因子, 则 $H \lhd G$.

证明 令 G 左乘作用于左陪集集合 $\Omega=\{xH\mid x\in G\}$ 上，设 N 是作用核.

法 1: 令 $m:=|H:N|$. 则 $|G:N|=|G:H|\cdot|H:N|=pm$，由定理 4 知 $pm\mid p!=p(p-1)!$，于是 $m\mid(p-1)!$，故 m 的素因子 q 均小于 p，由 Lagrange 定理知 q 整除群阶 $|G|$，这与 p 是 $|G|$ 的最小素因子矛盾！因此 m 没有素因子，即 $m=1$，所以 $H=N\lhd G$.

法 2: 由推论 1 知 G/N 同构于 S_p 的某子群，于是 $|G/N|\,\big|\,|S_p|=p!$，注意到 $|G/N|$ 的最小素因子大于等于 $|G|$ 的最小素因子 p，所以 $|G/N|=p$，故 $p=|G/N|=|G:N|=|G:H|\cdot|H:N|=p|H:N|$，于是 $|H:N|=1$，故 $H=N\lhd G$.■

特别地，在有限群中，指数为 2 的子群一定正规，奇数阶群的指数为 3 的子群必然正规.

注意，即使 G 是无限群，但 $|G:H|$ 有限时，定理 4 依然成立.

推论 3 *若 G 具有指数有限的子群 H，则存在 G 的含于 H 中且指数有限的正规子群 N.*

证明 令 G 左乘作用于左陪集集合 $\Omega=\{xH\mid x\in G\}$ 上，设 N 是作用核. 由推论 1 知 G/N 同构于 S_Ω 的某个子群 K. 此时 $N=\mathrm{core}_G(H)=\bigcap\limits_{x\in G}xHx^{-1}\le H$ 且 $|G:N|=|K|$ 整除 $|G:H|!$ 有限.■

推论 3 可用于将无限群的问题转化为对应的有限群问题. 比如 G 有限，$U\le V\le G$，由 Lagrange 定理知 $|G:U|=|G:V|\cdot|V:U|$. 下面设 G 无限但 $|G:U|<\infty$，$U\le V\le G$，那么依然成立 $|G:U|=|G:V|\cdot|V:U|$. 为什么呢？利用推论 3 可以得到 G 的含于 U 且指数有限的正规子群 N. 令 $\overline{G}:=G/N,\overline{U}:=U/N,\overline{V}:=V/N$ 分别是 G, U, V 在自然同态 $G\to G/N$ 下的像，由 $\overline{G}$ 有限知 $|\overline{G}:\overline{U}|=|\overline{G}:\overline{V}|\cdot|\overline{V}:\overline{U}|$. 再由子群对应定理知:

$$|\overline{G}:\overline{U}|=|G:U|,|\overline{G}:\overline{V}|=|G:V|,|\overline{V}:\overline{U}|=|V:U|,$$

于是得到我们需要的结论.

下面的定理给出了如前所讨论正规子群 N 的一些更精确的信息.

定理 5 *设 H 是群 G 的子群，令 G 左乘作用于 H 的左陪集集合的核为 N. 则*

(1) $N=\bigcap\limits_{x\in G}xHx^{-1}$;　　(2) *若 $M\lhd G$ 且 $M\le H$，则 $M\le N$.*

证明 设 $x,g\in G$，则

$$g\cdot(xH)=xH\Leftrightarrow gxH=xH\Leftrightarrow gx\in xH\Leftrightarrow g\in xHx^{-1}.$$

故

$$g\in G\text{ 在作用核 }N\text{ 中}\Leftrightarrow gxH=xH,\forall x\in G\Leftrightarrow gxHx^{-1}=xHx^{-1},\forall x\in G$$

$$\Leftrightarrow g \in xHx^{-1}, \forall x \in G \Leftrightarrow g \in \bigcap_{x\in G} xHx^{-1},$$

即 $N = \bigcap_{x\in G} xHx^{-1}$.

若 $M \lhd G$ 且 $M \le H$，则 $M = xMx^{-1} \subseteq xHx^{-1}$，故 $M \subseteq \bigcap_{x\in G} xHx^{-1} = N$.■

定理 5 中，N 是 G 的含于 H 中的极大正规子群，称为 H 在 G 中的**核**，也记为 $N = \mathrm{Core}_G(H)$. 即 $\mathrm{Core}_G(H) = \bigcap_{x\in G} xHx^{-1}$.

群作用也可以造出一些未必正规的子群. 设群 G 作用在 Ω 上且 $\alpha \in \Omega$，规定

$$G_\alpha := \{g \in G \mid g\cdot\alpha = \alpha\}$$

是 G 中固定文字α的所有元所成集，称为 α 在 G 中的**稳定子群**，直接验证知 G_α 确实是 G 的子群.

练习： 证明 G_α 是 G 的子群.

2.2 基本计数原理

定义 1 称群 G 在 Ω 上的作用**可迁**，若对任意给定的 $\alpha, \beta \in \Omega$，均存在 $g \in G$ 使得 $g\cdot\alpha = \beta$.

例如，群 G 在集合 G 上的左乘作用可迁，群 G 在子群 H 在 G 中的全部左陪集上的左乘作用可迁. 一般来说，G 在其自身上的共轭作用是不可迁的，这是因为当 $x, y \in G$ 的阶不同时，不可能存在 $g \in G$ 使得 $gxg^{-1} = y$.(元素 g 的共轭作用定义了群 G 的一个自同构 $\sigma_g : G \to G, x \mapsto gxg^{-1}, \forall x \in G$，保持元素的阶.)

定义 2 设群 G 作用在集 Ω 上，规定 $\alpha \in \Omega$ 在 G 作用下的**轨道**为 $\mathcal{O}_\alpha = \{g\cdot\alpha \mid g \in G\}$，也称 $\mathcal{O}_\alpha$ 为 **G－轨道.**

定理 1 设群 G 作用于集合 Ω 上，则作用下的全部轨道构成 Ω 的一个**划分**，即

(1) Ω 是所有轨道的并，即 $\Omega = \bigcup_{\alpha\in\Omega} \mathcal{O}_\alpha$；　　(2) 任意两个不同的轨道均不相交.

证明 (1) 由 $1\cdot\alpha = \alpha$ 知 $\alpha \in \mathcal{O}_\alpha$，故 $\Omega = \bigcup_{\alpha\in\Omega} \mathcal{O}_\alpha$.

(2) 先证明若 $\gamma \in \mathcal{O}_\alpha$，则 $\mathcal{O}_\gamma = \mathcal{O}_\alpha$. 由 $\gamma \in \mathcal{O}_\alpha$ 可设 $\gamma = x\cdot\alpha$，其中 $x \in G$. 此时对任一 $g \in G$ 有

$$g\cdot\gamma = g\cdot(x\cdot\alpha) = gx\cdot\alpha \in \mathcal{O}_\alpha.$$

所以 $\mathcal{O}_\gamma \subseteq \mathcal{O}_\alpha$. 另一方面，由 $\gamma = x\cdot\alpha$ 知 $\alpha = x^{-1}\cdot\gamma$，于是 $\alpha \in \mathcal{O}_\gamma$，因而 $\mathcal{O}_\alpha \subseteq \mathcal{O}_\gamma$，故 $\mathcal{O}_\gamma = \mathcal{O}_\alpha$.

如果两个轨道的交非空：$\mathcal{O}_\alpha \cap \mathcal{O}_\beta \neq \varnothing$，任取 $\gamma \in \mathcal{O}_\alpha \cap \mathcal{O}_\beta$，则 $\mathcal{O}_\alpha = \mathcal{O}_\gamma = \mathcal{O}_\beta$，故(2)成立.■

文字集在群作用下得到文字集的轨道划分，它类似于子群对群的陪集划分. 不过二者并不完全一致.

设 $H \le G$，令 H 左乘作用于 G 上，此时包含 $g \in G$ 的轨道恰为右陪集 Hg.

若规定 H 在 G 上的作用为: $\forall g\in G, h\in H$, $h\cdot g\coloneqq gh^{-1}$, 则

$$1\cdot g\coloneqq g1^{-1}=g,\ h_1\cdot(h_2\cdot g)\coloneqq h_1\cdot\left(gh_2^{-1}\right)=gh_2^{-1}h_1^{-1}=g\left(h_1h_2\right)^{-1}=\left(h_1h_2\right)\cdot g,$$

这表明如上确实规定了 H 在 G 上的一个作用, 此时包含 $g\in G$ 的轨道恰为左陪集 gH:

$$\mathcal{O}_g=\left\{h\cdot g\middle|h\in H\right\}=\left\{gh^{-1}\middle|h\in H\right\}=gH^{-1}=gH.$$

群作用的一个重要应用是计数, 其关键是下面的定理.

定理 2 设群 G 作用在集合 Ω 上, $\alpha\in\Omega$ 所在的轨道为 $\mathcal{O}_\alpha$, 相应的稳定子群为 $H\coloneqq G_\alpha$, 则 $\mathcal{O}_\alpha$ 与 G_α 在 G 中的左陪集集合之间有一个双射: $\mathcal{O}_\alpha\leftrightarrow\left\{xH\middle|x\in G\right\}$.

证明 构造映射 $f:\mathcal{O}_\alpha\to\left\{xH\middle|x\in G\right\}$ 如下. 任取 $\beta\in\mathcal{O}_\alpha$, 则存在 $x\in G$ 使得 $\beta=x\cdot\alpha$, 规定 $f(\beta)=xH$.

首先验证映射是良定的. 需要证明每一个文字 $\beta\in\mathcal{O}_\alpha$ 在映射 f 下的像是唯一确定的, 与使得 $\beta=x\cdot\alpha$ 的 $x\in G$ 无关. 换而言之, 若 $\beta=y\cdot\alpha$, 需要证明 $xH=yH$, 或者等价地 $y^{-1}x\in H=G_\alpha$. 由 $x\cdot\alpha=\beta=y\cdot\alpha$ 知

$$y^{-1}x\cdot\alpha=y^{-1}\cdot(x\cdot\alpha)=y^{-1}\cdot(y\cdot\alpha)=\left(y^{-1}y\right)\cdot\alpha=1\cdot\alpha=\alpha,$$

所以 $y^{-1}x\in H$, 故 $xH=yH$.

f 满: 对任一左陪集 xH, 有 $f(x\cdot\alpha)=xH$.

f 单: 设 $\beta,\gamma\in\mathcal{O}_\alpha$ 使得 $f(\beta)=f(\gamma)$, 由 $\beta,\gamma\in\mathcal{O}_\alpha$ 知 $\beta=x\cdot\alpha,\gamma=y\cdot\alpha$ 对适当的 $x,y\in G$. 由 f 的定义知 $xH=f(x\cdot\alpha)=f(\beta)=f(\gamma)=f(y\cdot\alpha)=yH$, 所以 $y=xh$ 对某 $h\in H$, 故

$$\gamma=y\cdot\alpha=xh\cdot\alpha=x\cdot(h\cdot\alpha)=x\cdot\alpha=\beta.\blacksquare$$

如下结论是定理 2 的重述, 我们称为“基本计数原理”, 或者 FCP.

推论 1(基本计数原理 FCP) 设群 G 作用在集合 Ω 上, $\alpha\in\Omega$. 则

(1) $\left|\mathcal{O}_\alpha\right|=\left|G:G_\alpha\right|$;　　(2) 如果 G 有限, 则 $\left|\mathcal{O}_\alpha\right|=|G|/\left|G_\alpha\right|$. 特别地, 轨道长度是群阶的因子.

作为第一个应用, 我们利用 FCP 得到共轭类的一些信息.

推论 2 群 G 的元 g 所在共轭类 $\mathrm{Cl}(g)$ 的**长度**为 $\left|\mathrm{Cl}(g)\right|=\left|G:\mathbf{C}_G(g)\right|$. 特别地, 有限群任一共轭类的长度整除群阶.

证明 令群 G 共轭作用于自身, 则 g 所在轨道为 $\mathrm{Cl}(g)$, 稳定子群为 $\mathbf{C}_G(g)$, 由 FCP 即得.$\blacksquare$

例 1 如果有限群 G 的非单位元均共轭，则 $|G|\le 2$.

证明 设 $n=|G|>1$，则 G 的全部非单位元作成长度为 $n-1$ 的共轭类，由推论 2 知 $n-1\mid n$，于是 $n\ge 2(n-1)$，得 $n\le 2$.■

令人惊奇的是，存在无限群使得其所有非单位元均共轭. 如下结论是推论 4.12 的一个推广.

定理 3(Landau) 若有限群 G 有 k 个共轭类，则存在界 $B(k)$ 使得 $|G|\le B(k)$. 或者等价地，恰有 k 个共轭类的有限群个数有限.

我们需要先证明一个引理.

引理 1 已知正整数 k 与数 A，如下方程正整数解的个数有限：$\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_k}=A$.

证明 若 $A\le 0$，则如上方程的正整数解数为 0，有限.

下设 $A>0$. 不妨设 x_k 是所有 $x_i\,(1\le i\le k)$ 中最小者，则 $\frac{1}{x_k}\ge\frac{1}{x_i}$ 对所有的 i，故 $\frac{k}{x_k}\ge\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_k}=A$，所以 $1\le x_k\le k/A$，即 x_k 仅有限多个.

若 $k=1$ 则证明完毕. 下设 $k>1$，对 k 用数学归纳法.

对每一个可能的 k 值，由归纳假设知 $\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_{k-1}}=A-\frac{1}{x_k}$ 的正整数解数有限，故原方程的正整数解数有限.■

定理 3 的证明 设 G 的 k 个共轭类的长度为 $|\mathrm{Cl}(g_i)|=c_i$，又设 $|\mathbf{C}_G(g_i)|=x_i, 1\le i\le k$，则有类方程:

$$|G|=c_1+c_2+\cdots+c_k,$$

由 $|G|=|\mathrm{Cl}(g_i)|\cdot|\mathbf{C}_G(g_i)|=c_ix_i$ 知 $c_i=|G|/x_i$，代入类方程，则有 $\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_k}=1$，由引理 1 知该方程仅有限多组解，于是存在一个仅依赖于 k 的正整数 $B(k)$ 使得 $x_i\le B(k), 1\le i\le k$. 设单位元所在共轭类为 $\mathrm{Cl}(g_1)$，则有 $|G|=x_1\le B(k)$.■

例 2(第一届丘成桐大学生数学竞赛试题) 设 G 是一个非 Abel 的有限群，用 $c(G)$ 表示群 G 的共轭类的类数，定义 $\bar{c}(G)=\frac{c(G)}{|G|}$. 证明 $\bar{c}(G)\le\frac{5}{8}$，并举一个使得等号成立的群例.

证明 (1) 由 G 非 Abel 知其中心 $\mathbf{Z}(G)$ 是 G 的真子群.

若$\left[G:\mathbf{Z}(G)\right]=p$是素数, 则$G/\mathbf{Z}(G)$是素数$p$阶循环群, 于是存在$a\in G$使得$G/\mathbf{Z}(G)=\left\langle a\mathbf{Z}(G)\right\rangle$, 于是$G$中元均形如$a^kc$, 其中$c\in\mathbf{Z}(G)$, 故 G是交换群, 与G非 Abel 矛盾!

因此$\left[G:\mathbf{Z}(G)\right]\notin\{1,2,3\}$, 故$\left[G:\mathbf{Z}(G)\right]\geq 4$, 于是$\left|\mathbf{Z}(G)\right|\leq\frac{1}{4}|G|$.

注意到群G中中心元以外的元所在共轭类至少有两个元素, 此时G的中心元构成$\left|\mathbf{Z}(G)\right|$个共轭类, 剩下的$c(G)-\left|\mathbf{Z}(G)\right|$个共轭类中元的个数不少于$2\left[c(G)-\left|\mathbf{Z}(G)\right|\right]$, 于是$|G|\geq\left|\mathbf{Z}(G)\right|+2\left[c(G)-\left|\mathbf{Z}(G)\right|\right]$, 故

$$c(G)\leq\frac{1}{2}|G|+\frac{1}{2}\left|\mathbf{Z}(G)\right|\leq\frac{1}{2}|G|+\frac{1}{2}\times\frac{1}{4}|G|=\frac{5}{8}|G|,$$

所以$\bar{c}(G)=\dfrac{c(G)}{|G|}\leq\dfrac{5}{8}$.

(2) 考虑四元数群

$$\mathrm{Q}_8=\left\{I_2,\begin{pmatrix}&1\\-1&\end{pmatrix},\begin{pmatrix}\mathrm{i}&\\&-\mathrm{i}\end{pmatrix},\begin{pmatrix}&-\mathrm{i}\\-\mathrm{i}&\end{pmatrix},-I_2,-\begin{pmatrix}&1\\-1&\end{pmatrix},-\begin{pmatrix}\mathrm{i}&\\&-\mathrm{i}\end{pmatrix},-\begin{pmatrix}&-\mathrm{i}\\-\mathrm{i}&\end{pmatrix}\right\}\subseteq\mathrm{GL}(\mathbb{C},2),$$

如果记$1=I_2,i=\begin{pmatrix}&1\\-1&\end{pmatrix},j=\begin{pmatrix}\mathrm{i}&\\&-\mathrm{i}\end{pmatrix},k=\begin{pmatrix}&-\mathrm{i}\\-\mathrm{i}&\end{pmatrix},\mathrm{Q}_8=\{1,i,j,k,-1,-i,-j,-k\}$, 且满足如下关系

$$i^2=j^2=k^2=-1,ij=k,jk=i,ki=j,ji=-k,,kj=-i,ik=-j,$$

而这些关系都可以由如下三个关系导出:

$$i^4=j^4=1,ij=ji^3$$

Q_8的群阶为 8, $\mathbf{Z}(G)=\{1,-1\}$, G恰有 5 个共轭类.■

2.3　若干范例

在群作用之下, 将一个集合划分为若干轨道并的重要范例是**群共轭作用于自身**. 此时每一个轨道称为一个**共轭类**. 注意元$x\in G$的共轭类恰含一个元当且仅当$x\in\mathbf{Z}(G)$. 我们有时候也考虑群G共轭作用于某个子群集的情形, 此时就有子群共轭类的概念.

下面给出一些稳定子群与轨道计算的具体例子.

例 1 (1) 群 ***G* 共轭作用于自身**.

若$x\in G$, 则

$$G_x=\left\{g\in G\middle|g\cdot x=x\right\}=\left\{g\in G\middle|gxg^{-1}=x\right\}=\left\{g\in G\middle|gx=xg\right\}=\mathbf{C}_G(x).$$

即x的**稳定子群**G_x恰为x在G中的**中心化子**$\mathbf{C}_G(x)$. 而x所在的**轨道**

$$\mathcal{O}_x=\left\{g\cdot x\middle|g\in G\right\}=\left\{gxg^{-1}\middle|g\in G\right\}=\mathrm{Cl}(x)$$

恰为**共轭类** $\mathrm{Cl}(x)=\left\{gxg^{-1}\middle|g\in G\right\}$.

由基本计数原理知 $\left|\mathrm{Cl}(x)\right|=\left|\mathcal{O}_x\right|=\dfrac{|G|}{|G_x|}=\dfrac{|G|}{\left|\mathbf{C}_G(x)\right|}$，或者等价地 $|G|=\left|\mathrm{Cl}(x)\right|\cdot\left|\mathbf{C}_G(x)\right|$，特别地每一个共轭类的长度都是群阶的因子.

(2) 设群 ***G*** **共轭作用于** ***G*** **的全部子集所成集**.

若 $X\subseteq G$，则

$$G_X:=\left\{g\in G\middle|g\cdot X=X\right\}=\left\{g\in G\middle|gXg^{-1}=X\right\}=\mathbf{N}_G(X),$$

即 X 的稳定子群恰为 X 在 G 中的**正规化子** $\mathbf{N}_G(X)=\left\{g\in G\middle|gXg^{-1}=X\right\}=\left\{g\in G\middle|gX=Xg\right\}$. 而 X 所在的**轨道**

$$\mathcal{O}_X=\left\{g\cdot X\middle|g\in G\right\}=\left\{gXg^{-1}\middle|g\in G\right\}$$

恰为子集 X 的**共轭类**.

特别地，如果 X 是 G 的子群，由基本计数原理知 G 中 X 的共轭子群的个数为 $\left|\mathcal{O}_X\right|=\dfrac{|G|}{|G_X|}=\dfrac{|G|}{\left|\mathbf{N}_G(X)\right|}$.

练习题：设 $X\lhd H\leq G$，则

[1] $X\leq\mathbf{N}_G(X)$ 且 $X\lhd\mathbf{N}_G(X)$；

[2] $H\leq\mathbf{N}_G(X)$，即 X 的正规化子 $\mathbf{N}_G(X)$ 是 G 的使得 X 在其中正规的最大子群.

(3) 设**群** ***G*** **左乘作用于子群** ***H*** **在** ***G*** **中的全部左陪集所成集** $\Omega=\left\{xH\middle|x\in G\right\}$.

此时 xH 的稳定子群为 xHx^{-1}. 特别地，H 的稳定子群为 H 自身.

若 $xH\in\Omega$，则

$$G_{xH}=\left\{g\in G\middle|g\cdot xH=x\right\}=\left\{g\in G\middle|gxH=xH\right\}=\left\{g\in G\middle|x^{-1}gx\in H\right\}=\left\{g\in G\middle|g\in xHx^{-1}\right\}$$

即 xH 的**稳定子群** G_{xH} 恰为 H 的共轭子群. 此时群作用是可迁的，恰由一个轨道. 群作用的核是所有稳定子群的公共交 $\mathrm{core}_G(H)=\bigcap\limits_{x\in H}xHx^{-1}$.

总结例 1 的结论，就有下面的定理.

定理 1 设 G 是有限群，$H\leq G$，则

(1) x 的共轭类长度为 $\mathrm{Cl}(x)=\left|G:\mathbf{C}_G(x)\right|$；　　(2) H 的共轭子群个数为 $\left|G:\mathbf{N}_G(x)\right|$.

例 2 设 H 与 K 都是群 G 的有限子群, 则 $|HK|=\dfrac{|H|\cdot|K|}{|H\cap K|}$.

证明 令 H 左乘作用在 $\Omega:=\{xK\,|\,x\in G\}$ 上, 由 $HK=\bigcup\limits_{k\in K}Hk$ 知 HK 恰为 K 所在轨道 $\mathcal{O}_K$ 中左陪集的不相交并. 注意到每一个左陪集均含 $|K|$ 个元, 故 $|HK|=|\mathcal{O}_K||K|$.

在群作用下, $K\in\Omega$ 的稳定子群为

$$\{x\in H\,|\,xK=K\}=\{x\in H\,|\,x\in K\}=H\cap K.$$

由 FCP 知 $|\mathcal{O}_K|=|H|/|H\cap K|$, 故 $|HK|=|\mathcal{O}_K||K|=\dfrac{|H|\cdot|K|}{|H\cap K|}$.■

例 3. 设 H 是有限群 G 的真子群, 则 H 的所有共轭子集的并是 G 的真子集. 或者等价地, 存在 G 中的元 g 不含于 H 的任一共轭.

提示 与 H 共轭的子群数 $|G:\mathbf{N}_G(H)|\le|G:H|$, 共轭子群有公共的单位元, 对 G 的元素计数.

证明 设 $H_1=H,H_2,\cdots,H_k$ 是与 H 共轭的全部子群, 则 $k=|G:\mathbf{N}_G(H)|$, 由 $H\le\mathbf{N}_G(H)$ 知

$$k=|G:\mathbf{N}_G(H)|\le|G:H|,$$

于是

$$\left|\bigcup_{i=1}^k H_i\right|\le 1+\left|\bigcup_{i=1}^k(H_i-\{1\})\right|\le 1+\sum_{1\le i\le k}|H_i-\{1\}|=1+\sum_{1\le i\le k}(|H|-1)$$

$$=1+k(|H|-1)\le 1+|G:H|(|H|-1)=|G|-|G:H|+1<|G|-1+1=|G|,$$

最后一个小于号是由 $H<G$ 知 $|G:H|>1$, 于是有 $\left|\bigcup_{i=1}^k H_i\right|<|G|$, 即 $\bigcup_{i=1}^k H_i$ 是 G 的真子集.■

群 G 的全部真子群所成集关于集合的包含作成一个偏序集, 该偏序集中的极大元, 即 G 的真子群中极大者称为 G 的**极大子群**. 换而言之, 即满足如下条件的 H:

$$H<G\text{ 且满足条件 }"H\le K<G\Rightarrow H=K".$$

例 4. 如果群 G 的任意两个极大子群都共轭, 则 G 为循环群.

证明 任取 G 的一个极大子群 H.

(1) 设 $g\in G$, 则 gHg^{-1} 是 G 的极大子群: 由 $|gHg^{-1}|=|H|<|G|$ 知 $gHg^{-1}<G$. 设 $gHg^{-1}\le K<G$, 则有 $g^{-1}(gHg^{-1})g\le g^{-1}Kg<g^{-1}Gg$, 即 $H\le g^{-1}Kg<G$, 由 H 极大知 $H=g^{-1}Kg$, 即 $gHg^{-1}=K$.

(2) 由题设知 G 的极大子群均与 H 共轭, 再由(1)知与 H 共轭的均为 G 的极大子群, 于是 G 的全部极大子群恰为与真子群 H 共轭的全部子群.

由例 1 知存在某元 $a\in G$ 不含于 H 共轭子群之并, 于是 a 也不含于 G 的任一极大子群.

若 $G\neq\langle a\rangle$, 由 G 有限知 $\langle a\rangle$ 含于 G 的某极大子群 M, 于是 a 含于极大子群 M, 矛盾! 故 $G=\langle a\rangle$ 循环.■

事实上, 如上证明中的(1)不是必需的, 我们也可以给出如下证明:

证明 2 任取 G 的一个极大子群 H, 由例 1 知存在某元 $a\in G$ 不含于 H 共轭子群之并, 断言 $G=\langle a\rangle$:

反证. 若 $G\neq\langle a\rangle$, 则 $\langle a\rangle$ 是 G 的真子群, 由 G 有限知 $\langle a\rangle$ 含于某极大子群 M, 由题设知 M 与 H 共轭, 于是 a 含于 H 共轭子群之并, 与 a 的选取矛盾! ■

例 5. N/C 定理 设 $H\leq G$, 则 $\mathbf{N}_G(H)/\mathbf{C}_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的某个子群.

证明 规定映射

$$\sigma:\mathbf{N}_G(H)\to\mathrm{Aut}(H),\ g\mapsto\left(\sigma_g\in\mathrm{Aut}(H):h\mapsto ghg^{-1},\forall h\in H\right),$$

由 $H\lhd\mathbf{N}_G(H)$ 知对每一个 $g\in\mathbf{N}_G(H)$ 均有 $\sigma_g\in\mathrm{Aut}(H)$, 因此映射 σ 良定. 而且

$$\sigma_{g_1g_2}h=g_1g_2h(g_1g_2)^{-1}=g_1\left(g_2hg_2^{-1}\right)g_1^{-1}=\sigma_{g_1}\left(\sigma_{g_2}(h)\right)=\left(\sigma_{g_1}\sigma_{g_2}\right)(h)$$

表明 σ 是群同态, 同态核为

$$\ker\sigma=\left\{g\in\mathbf{N}_G(H)\middle|\sigma_g=\mathrm{id}_H\right\}=\left\{g\in\mathbf{N}_G(H)\middle|ghg^{-1}=h,\forall h\in H\right\}$$

$$=\mathbf{C}_{\mathbf{N}_G(H)}(H)=\mathbf{C}_G(H)\cap\mathbf{N}_G(H),$$

注意到显然有 $\mathbf{C}_G(H)\leq\mathbf{N}_G(H)$, 所以 $\ker\sigma=\mathbf{C}_G(H)$, 由同构定理 A 知

$$\mathbf{N}_G(H)/\mathbf{C}_G(H)\cong\sigma\left(\mathbf{N}_G(H)\right)\leq\mathrm{Aut}(H).\blacksquare$$

2.4 轨道计数

现在来看 FCP 另一种重要的应用: 计算群作用的轨道个数. 为此给出一些新的定义.

定义 1 群 G 作用在集 Ω 上的**置换特征标**, 是 G 上的一个取值为整数的函数:

$$\chi(g):=\left|\left\{\alpha\in\Omega\middle|g\cdot\alpha=\alpha\right\}\right|,\forall g\in G.$$

对任一 $g\in G$, $\chi(g)$ 的值恰为"***g* 固定文字的个数**".

例 1 (1) 有限群 G 的左正则作用的置换特征标为: $\chi(g)=\begin{cases}0, & \text{若 } g\neq 1,\\ |G|, & \text{若 } g=1\end{cases}$.

(2) G 共轭作用于自身的置换特征标为: $\chi(g)=\left|\mathbf{C}_G(g)\right|, \forall g\in G$.

轨道计数的关键是如下定理.

定理 1(Cauchy-Frobenius) 设有限群 G 作用在有限集 Ω 上, 则轨道数 $n=\dfrac{1}{|G|}\sum\limits_{x\in G}\chi(x)$.

注记 **群作用的轨道数恰为置换特征标的平均值.**

证明 令 $S=\{(\alpha,g)\mid \alpha\in\Omega, g\in G, g\cdot\alpha=\alpha\}$, 用两种不同的方式对 S 计数.

对每一个 $\alpha\in\Omega$, 固定 α 的元 $\{g\mid g\in G, g\cdot\alpha=\alpha\}$ 构成稳定子群 G_α, 恰有 $|G_\alpha|$ 个 $(\alpha,g)\in S$, 故

$$|S|=\sum_{\alpha\in\Omega}\left|\{g\mid g\in G, g\cdot\alpha=\alpha\}\right|=\sum_{\alpha\in\Omega}|G_\alpha|=\sum_{\alpha\in\Omega}\frac{|G|}{|\mathcal{O}_\alpha|}.$$

对每一个 $g\in G$, g 固定的文字 α 的个数为 $\chi(g)$, 恰有 $\chi(g)$ 个 $(\alpha,g)\in S$, 故 $|S|=\sum\limits_{g\in G}\chi(g)$, 因此

$$n=\sum_{\alpha\in\Omega}\frac{1}{|\mathcal{O}_\alpha|}=\frac{1}{|G|}|S|=\frac{1}{|G|}\sum_{g\in G}\chi(g).\blacksquare$$

Burnside 在 1897 年证明了该引理并且给出了轨道计数的公式, 而历史上, Cauchy 在 1845 年, Frobenius 在 1887 年已经发现了这一结论.

推论 1 设有限群 G 可迁地作用在有限集 $\Omega(|\Omega|>1)$ 上, 则存在 $g\in G$ 不固定 Ω 中任一文字.

证明 由群作用可迁知轨道数为 1, 即置换特征标的平均值为 1. 注意到 $\chi(1)=|\Omega|>1$, 因而一定存在某个 $g\in G$ 使得其置换特征标的值低于平均值, 即 $\chi(g)<1$, 由置换特征标的定义知 $\chi(g)$ 是非负整数, 故 $\chi(g)=0$, 即存在 $g\in G$ 不固定 Ω 中任一文字.$\blacksquare$

习题二

1 设有限群 G 可迁的作用在集 Ω 上. 由此规定 G 在集 $\Omega\times\Omega$ 上的一个作用为

$$g\cdot(\alpha,\beta):=(g\cdot\alpha, g\cdot\beta), \forall\alpha,\beta\in\Omega, g\in G.$$

证明: G 在 $\Omega\times\Omega$ 上的轨道数与 G_α 在 Ω 上的轨道数相同.

2 若按 4.1 规定的作用 G 在集 $\{(\alpha,\beta)\mid\alpha,\beta\in\Omega,\alpha\neq\beta\}$ 上可迁, 则称群 G 在集 Ω 上的作用**二重可迁**. 证明: 群 G 在集 Ω 上的二重可迁 $\Leftrightarrow\dfrac{1}{|G|}\sum\limits_{g\in G}\chi(g)^2=2$. 其中 χ 是 G 在集 Ω 上作用相应的置换特征标. 这里不需假设 G 在集 Ω 上的作用可迁.

3 设 H, K 都是群 G 的有限子群. 证明 $|HgK| = \dfrac{|H||K|}{|H \cap gKg^{-1}|}$.

注记: 形如 HgK 的子集称为**双陪集**.

4 设 G 是有限群, $\varphi: G \to H$ 是满同态, $g \in G$. 证明: $|\mathbf{C}_G(g)| \geq |\mathbf{C}_H(\varphi(g))|$.

提示: 证明 $\mathbf{C}_H(\varphi(g))$ 在 G 中的原像的共轭类长度 $\leq |\ker\varphi|$.

5 设 G 是有限群. 证明: G 中任取两个元可交换相乘的概率为 $\dfrac{k}{|G|}$, 其中 k 为 G 的共轭类数. (两个元允许相等, 它们是随机选取的.)

6 对正六面体, 用 n 种不同的颜色对顶点着色, 有多少种着色方案? 如果对面进行着色呢?

7 用 5 种不同颜色的珠子做一串 6 颗珠子的项链, 有多少种不同的方案?

第三章 Sylow 定理

迄今为止，我们研究了子群的许多性质，但是并没有给出寻找或者构造子群的有力技术. 如果有限群 G 的阶为 n，子群 H 的阶为 m, Lagrange 定理告知我们，子群阶整除群阶，即 $m\mid n$. 反之，是否对每一个整除群阶 n 的正整数因子 m, G 都具有一个 m 阶子群呢? 如果 G 是循环群, Abel 群甚至幂零群时，此结论为真. 不过一般来说，这一结论是不成立的，比如 12 阶群

$$A_4=\{(1),(12)(34),(13)(24),(14)(23),(123),(124),(132),(134),(142),(143),(234),(243)\}$$

没有 6 阶子群!

例 证明 12 阶群 A_4 没有 6 阶子群.

证明 反证. 若有 6 阶子群 N，则指数为 2 从而正规，且 $|G/N|=2$. 任取 $g\in A_4$，在 2 阶商群 G/N 中，$(gN)^2=N$，于是有 $g^2\in N$，直接计算得

$$\{g^2\mid g\in A_4\}=\{(1),(123),(124),(132),(134),(142),(143),(234),(243)\},$$

这与 $\{g^2\mid g\in A_4\}\subseteq N$ 矛盾!■

注记 如果 G/N 是素数 p 阶群，则 $g^p\in N,\forall g\in G$：在 p 阶商群中有 $g^pN=(gN)^p=N$.

Sylow 定理的主要结论是 Lagrange 定理的部分逆：如果素数幂 m 是群阶的因子时，则存在 m 阶子群. 这一结论也称为“**有限群论基本定理**”，事实上, Sylow 定理将告知我们更多的子群信息.

3.1 Sylow 存在性定理

定理 1 设 $n=p^am$，其中 p 为素数, m 是正整数，则 $C_n^{p^a}\equiv m(\mathrm{mod}\,p)$.

证明 (1) 由数论知 $p\mid C_p^i,(1\le i\le p-1)$：

由组合数 $C_p^i=\dfrac{p!}{i!(p-1)(p-2)\cdots(p-i)}$ 是整数知，$i!(p-1)(p-2)\cdots(p-i)\mid p!$ 再由 $p\mid p!$ 以及 p 与 $1,2,\cdots,p-1$ 均互素知 $(p,i!(p-1)(p-2)\cdots(p-i))=1$，所以 $p\cdot i!(p-1)(p-2)\cdots(p-i)\mid p!$，故

$$p\mid C_p^i\,(1\le i\le p-1);$$

(2) $(x+1)^p\equiv x^p+1\Rightarrow(x+1)^{p^2}\equiv\left[(x+1)^p\right]^p\equiv\left(x^p+1\right)^p\equiv x^{p^2}+1(\mathrm{mod}\,p)$

$$\Rightarrow\cdots\Rightarrow(x+1)^{p^a}\equiv\left[(x+1)^{p^{a-1}}\right]^p\equiv\left(x^{p^{a-1}}+1\right)^p\equiv x^{p^a}+1(\mathrm{mod}\,p)$$

$$\Rightarrow (x+1)^n=\left[(x+1)^{p^a}\right]^m\equiv\left(x^{p^a}+1\right)^m \bmod p,$$

左端$(x+1)^n$中x^{p^a}的系数为$C_n^{p^a}$，右端$\left(x^{p^a}+1\right)^m$中x^{p^a}的系数为m，所以$C_n^{p^a}\equiv m(\bmod p)$.■

下面来证明 Sylow 存在性(Existence)定理，也称 Sylow E 定理.

定理 2(Sylow 存在性定理) 设G是p^am阶有限群，其中素数$p\nmid m$，则G存在p^a阶子群.

证明(Wielandt) 令$\Omega=\left\{X\subseteq G\middle||X|=p^a\right\}$是$G$的全体$p^a$元子集所成集，由定理 1 知

$$|\Omega|=C_n^{p^a}\equiv m\neq 0(\bmod p).$$

令G左乘作用在集Ω上. 注意到$|g\cdot X|=|gX|=|X|=p^a,\forall g\in G,X\in\Omega$，根据群作用的定义直接验证知其确实是群作用. 此时Ω分解为有限个轨道的并. 由$p\nmid|\Omega|$知至少有一个轨道$\mathcal{O}_X$的长度不是p的倍数，其中$X\in\Omega$. 由基本计数原理 FCP 知$|G|=|\mathcal{O}_X|\cdot|G_X|$，其中$G_X=\{g\in G|gX=X\}$是$X$的稳定子群.

由$p^a\big||G|=|\mathcal{O}_X|\cdot|G_X|$，$p\nmid|\mathcal{O}_X|\Rightarrow(p,|\mathcal{O}_X|)=1$知$p^a\big||G_X|$，故$p^a\le|G_X|$.

固定$x\in X$，由G_X是X的稳定子群知$G_Xx\subseteq X$，故$|G_X|=|G_Xx|\le|X|=p^a$.

综上知$|G_X|=p^a$，故G_X是G的一个p^a阶子群.■

如下是徐明曜教材《有限群初步》给出的定理与证明:

Sylow 定理 设G是p^am阶有限群，其中p是素数，m是正整数，允许$p|m$.

则G中p^a阶子群数$n_{p^a}(G)\equiv1(\bmod p)$，特别地$G$中存在$p^a$阶子群.

证明 令$\Omega=\left\{X\subseteq G\middle||X|=p^a\right\}$是$G$的全体$p^a$元子集所成集，则$|\Omega|=C_{p^am}^{p^a}$. 令$G$左乘作用于集$\Omega$上，$\Omega$分解为轨道$\mathcal{O}_i(1\le i\le k)$的不交并，取各轨道的代表元$M_i$($G$的一个$p^a$元子集)，相应稳定子群为$G_i$，则

$$|\Omega|=\sum_{1\le i\le k}|\mathcal{O}_i|,|G|=|\mathcal{O}_i|\cdot|G_i|,G_iM_i=M_i,$$

(1) 阶$|G_i|=p^{b_i}$，其中$0\le b_i\le a$. 由$G_iM_i=M_i$知每一M_i都是G_i的右陪集之并，故$|G_i|$整除$|M_i|=p^a$.

(2) $|G_i|<p^a\Leftrightarrow|\mathcal{O}_i|\equiv0(\bmod pm),|G_i|=p^a\Leftrightarrow|\mathcal{O}_i|=m$：由$p^am=|G|=|\mathcal{O}_i|\cdot|G_i|$. 从而有

$$|\Omega|=\sum_{1\le i\le k}|\mathcal{O}_i|\equiv\sum_{|\mathcal{O}_i|=m}|\mathcal{O}_i|(\bmod pm).$$

(3) 长度为m的轨道$\mathcal{O}_i$的个数 = p^a阶子群的个数$n_{p^a}(G)$.

设$|\mathcal{O}_i|=m$，由$p^am=|G|=|\mathcal{O}_i|\cdot|G_i|$知$|G_i|=p^a$，由$G_iM_i=M_i$知$M_i=G_im_i$对任一$m_i\in M_i$. 此时

$$\mathcal{O}_i=\left\{gM_i\middle|g\in G\right\}=\left\{gm_i^{-1}M_i\middle|g\in G\right\}=\left\{gm_i^{-1}G_im_i\middle|g\in G\right\}.$$

这表明每一个长度为 m 的轨道 $\mathcal{O}_i$ 都是一个 p^a 阶子群 $m_i^{-1}G_im_i$ 的全体左陪集的并.

如果有两个 p^a 阶子群 H 与 K 使得 $\mathcal{O}_i$ 是 H 的左陪集的并, 也是 K 的左陪集的并, 注意到 H 与 K 都是 $\mathcal{O}_i$ 中唯一包含单位元的文字, 所以有 $H=K$, 这也表明 $\mathcal{O}_i$ 中有唯一的 p^a 阶子群 H 使得 $\mathcal{O}_i$ 是 H 的左陪集的并.

反之, 对 G 的任一 p^a 阶子群, 该子群在 G 中的全体左陪集也是 G 作用在 Ω 上的一个长度为 m 的轨道.如果两个 p^a 阶子群 H 与 K 构造出来的轨道 $\mathcal{O}_H=\mathcal{O}_K$, 那么 $H\in\mathcal{O}_H=\mathcal{O}_K$, 而轨道 $\mathcal{O}_K$ 作为 K 的左陪集的并, 唯一包含单位元的文字为 K, 又 H 也是包含单位元的文字, 所以 $H=K$.

这样就得到了长度为 m 的轨道集与 p^a 阶子群集的一个双射, 由此即得.

(4) 将(3)的结论代入(2)得 $|\Omega|\equiv\sum_{|\mathcal{O}_i|=m}|\mathcal{O}_i|=n_{p^a}(G)m\pmod{pm}$

(5) 对 p^am 阶循环群 C, 它恰有唯一的 p^a 阶子群, 即 $n_{p^a}(C)=1$, 由(4)知 $|\Omega_C|\equiv n_{p^a}(C)m=m\pmod{pm}$, 注意到 C 的 p^a 元子集个数 $|\Omega_C|$ 与 G 的 p^a 元子集个数 $|\Omega|$ 相同, 所以 $n_{p^a}(G)m\equiv|\Omega|=|\Omega_C|\equiv m\pmod{pm}$. 故

$$n_{p^a}(G)\equiv1\pmod{p}.\blacksquare$$

注记 (1) 两个证明的群作用基本一样.

(2) 证明 1 的关键: 存在某个轨道的长度不为 p 的倍数, 其代表元的稳定子群恰为所需.

(3) 证明 2 更细致的分析了轨道的长度与相应稳定子群的阶:

稳定子群的阶均为素数幂;

构建了长度为 m 的轨道集与 p^a 阶子群集的一个双射;

一个精致的小技巧.

下面给出一个不用群作用, 仅用归纳法的证明.

预备引理 如果素数 p 整除有限 Abel 群 G 的阶, 则 G 中有 p 阶元.

证明 任取 Abel 群 G 的一个真子群 H, 如果 $p\big||H|$, 对 H 用归纳法即得.

否则设 $(p,|H|)=1$, 对 G/H 用归纳法知其存在 p 阶元 aH, 即 $a\notin H$ 但 $h:=a^p\in H$, 设 $|H|=s$, 整数 u,v 使得 $up+vs=1$.

由 $(a^s)^p=(a^p)^s=h^s=1$ 知 a^s 的阶为 1 或者 p.

若 a^s 的阶为 1，则 $a^s=1$，于是 $a=a^1=a^{pu+sv}=a^{pu}a^{sv}=a^{up}=\left(a^p\right)^u=h^u\in H$，矛盾于 $a\notin H$！

所以 a^s 是群 G 的 p 阶元. ■

Sylow 定理的归纳法证明 对群 G 的阶 $|G|=p^an$ 用归纳法，其中 $(p,n)=1$. 如果群 G 含有一个指数与 p 互素的真子群 H，则 $|H|=p^am$，其中 $(m,p)=1$，且 $m<n$，对 H 用归纳法即得.

下设 G 的任一真子群的指数均为 p 之倍数，考虑群 G 的类方程

$$|G|=|\mathbf{Z}(G)|+\sum_{1\le i\le s}|\mathrm{Cl}(x_i)|=|\mathbf{Z}(G)|+\sum_{1\le i\le s}|G:\mathbf{C}_G(x_i)|,$$

其中 $x_1,\cdots,x_s$ 是群 G 的非中心元的共轭类代表系. 此时 $p\|G|,|G:\mathbf{C}_G(x_i)|=|\mathrm{Cl}(x_i)|,1\le i\le s$，于是 p 整除群中心的阶 $|\mathbf{Z}(G)|$，由预备引理知 Abel 群 $\mathbf{Z}(G)$ 具有某个 p 阶元 x.

若 $G=\langle x\rangle$，结论显然成立.

若 $G\neq\langle x\rangle$，对 $p^{a-1}m$ 阶群 $G/\langle x\rangle$ 用归纳法知其存在某个 p^{a-1} 阶子群 $H/\langle x\rangle$，其中 $H\le G$，显然 H 是 G 的 p^a 阶子群. ■

我们在后面将证明，条件 $p\nmid m$ 不是必需的，事实上若 p 是素数且 $p^a\|G|$ 时，G 总有 p^a 阶子群.

定义 1 设 G 是 p^am 阶有限群，其中素数 $p\nmid m$，则 G 的 p^a 阶子群称为 G 的 **Sylow $p-$ 子群**. G 的全体 Sylow $p-$ 子群所成集合记为 $\mathrm{Syl}_p(G)$.

Sylow 定理 2 即：对任一有限群 G 与素数 p，$\mathrm{Syl}_p(G)\neq\varnothing$. 若 $p\nmid|G|$，则单位子群是 Sylow $p-$ 子群，此时仍有 $\mathrm{Syl}_p(G)\neq\varnothing$.

推论 1(Cauchy) 如果素数 p 整除有限群 G 的阶，则 G 中有 p 阶元.

证明 任取 $P\in\mathrm{Syl}_p(G)$，由 $p\|G|$ 知 $P>1$. 任取 P 的一个非单位元 x，由元素 x 的阶整除子群 P 的阶知 $o(x)=p^s$ 对某个正整数 s，此时 $x^{p^{s-1}}$ 是 G 的一个 p 阶元.■

可能无限的群 P 称为 $p-$ 群，如果 P 的全部阶有限元素的阶都是 p 的方幂，其中 p 是素数.

推论 2 设 G 是有限群. 则：G 是 $p-$ 群 $\Leftrightarrow|G|$ 为素数 p 的方幂.

证明 "$\Leftarrow$" 设 $|G|$ 是素数 p 的方幂，则任一元的阶整除群阶 $|G|$，也是 p 的方幂，故为 $p-$ 群.

"⇒"设有限群 G 是 $p-$群，若 $|G|$ 不是素数 p 的方幂，则 $|G|$ 有素因子 $q\neq p$，由 Cauchy 定理知 G 有 q 阶元，与 G 是 $p-$群矛盾!■

3.2 Sylow D 与 C 定理

有限群 G 的 Sylow $p-$子群是一个 $p-$子群，且由 Lagrange 定理知 G 不存在阶更高的 $p-$子群，因而是其极大 $p-$子群. 事实上，G 的极大 $p-$子群恰为 G 的 Sylow $p-$子群. 这正是下面的 Sylow "Development" 定理，简称 Sylow D 定理.

定理 1(Sylow D) 设 P 是有限群 G 的 $p-$子群，则存在 $S\in \mathrm{Syl}_p(G)$ 使得 $P\leq S$.

我们在后面再证明 Sylow D 定理，这里先考虑对固定的素数 p，G 的不同 Sylow $p-$子群之间的关系. G 的子群成为 Sylow $p-$子群是子群阶的一个条件，因而 Sylow $p-$子群的共轭仍然是 Sylow $p-$子群. 不平凡的事实是任两个 Sylow $p-$子群都共轭. 这一事实称为 Sylow 共轭"Conjugacy"定理或者 Sylow C 定理.

定理 2(Sylow C) 设 G 是有限群，则 $\mathrm{Syl}_p(G)$ 恰构成 G 的子群的一个共轭类，即 Sylow $p-$子群均共轭.

Sylow D 与 Sylow C 定理可以组合为一个定理.

定理 3 设 G 是有限群，P 是 G 的一个 $p-$子群，$S\in \mathrm{Syl}_p(G)$，则 $P\leq xSx^{-1}$ 对某个 $x\in G$.

证明 令 P 左乘作用在 $\Omega=\{xS\,|\,x\in G\}$ 上，则作用将 Ω 分解为若干轨道之并. 由 FCP 定理，每一轨道长度均为素数 p 的方幂，由 $S\in \mathrm{Syl}_p(G)$ 知 $p\nmid |\Omega|=|G:S|$. 如果 Ω 的每一个轨道长度 $|\mathcal{O}_\alpha|$ 均大于 1，则由 $|\mathcal{O}_\alpha|$ 是 p 的方幂知其也是 p 的倍数，于是 $|\Omega|$ 也是 p 的倍数，矛盾! 所以 Ω 至少有一个轨道长为 1.

不妨设 $\{xS\}$ 是 Ω 的长为 1 的轨道，则 P 再在 xS 上的左乘作用平凡，即 $yxS=xS,\forall y\in P$，两端同时右乘 x^{-1} 得 $yxSx^{-1}=xSx^{-1},\forall y\in P$，或者等价地 $y\in xSx^{-1},\forall y\in P$，所以 $P\leq xSx^{-1}$，证明完毕.■

注记 在定理 3 中，取 P 为 G 的 Sylow $p-$子群，则 P 与 S 均共轭，得到 Sylow 共轭定理.

注意到 $S\in \mathrm{Syl}_p(G)$ 时 $xSx^{-1}\in \mathrm{Syl}_p(G)$，故 $P\leq xSx^{-1}$ 即 Sylow 发展定理.

定义 设 G 是有限群，令 $n_p(G):=|\mathrm{Syl}_p(G)|$ 表示 G 的 Sylow $p-$子群的个数.

因为 G 的全部 Sylow $p-$子群作成子群的一个共轭类，于是有如下结论.

推论 1 设 G 是有限群，$P\in \mathrm{Syl}_p(G)$，则 $n_p(G)=|G:\mathbf{N}_G(P)|$，特别地 $n_p(G)\big||G:P|$.

证明 令 G 共轭作用于 $\mathrm{Syl}_p(G)$ 上，由 Sylow 共轭定理知作用可迁，故 P 所在的轨道 $\mathcal{O}_P=\mathrm{Syl}_p(G)$，而 P 的稳定子群 $G_P=\mathbf{N}_G(P)$，由 FCP 知 $n_p(G)=\left|\mathrm{Syl}_p(G)\right|=\left|G:\mathbf{N}_G(P)\right|$.

由 $P\le\mathbf{N}_G(P)$ 知 $\left|G:\mathbf{N}_G(P)\right|\left|G:P\right|$，所以 $n_p(G)\left|G:P\right|$ ■

推论 2 设 G 是有限群，$S\in\mathrm{Syl}_p(G)$，则如下条件等价:

(1) $S\lhd G$;　　(2) S 是群 G 唯一的 Sylow $p-$子群;

(3) G 的任一 $p-$子群均含于 S;　　(4) S char G.

证明 $(1)\Rightarrow(2)$ 因为 $S\lhd G$，故 $\mathbf{N}_G(S)=G$，由推论 1 知 $\left|\mathrm{Syl}_p(G)\right|=\left|G:\mathbf{N}_G(S)\right|=1$，故 S 是群 G 唯一的 Sylow $p-$子群.

或: 设 $P\in\mathrm{Syl}_p(G)$，由定理 2 知存在 $x\in G$ 使得 $P=xSx^{-1}$，再由 $S\lhd G$ 知 $xSx^{-1}=S$，所以 $P=xSx^{-1}=S$.

$(2)\Rightarrow(3)$ 设 P 是 G 的 $p-$子群，由定理 3 知 $P\le xSx^{-1}$ 对某 $x\in G$，由 $\left|xSx^{-1}\right|=\left|S\right|$ 知 $xSx^{-1}\in\mathrm{Syl}_p(G)$，再由 S 是唯一的 Sylow $p-$子群知 $xSx^{-1}=S$，故 $P\le xSx^{-1}=S$.

$(3)\Rightarrow(4)$ $\forall\sigma\in\mathrm{Aut}(G)$，由 $\left|\sigma(S)\right|=\left|S\right|$ 是 p 的幂知 $\sigma(S)\in\mathrm{Syl}_p(G)$，由(3)知 $\sigma(S)\subseteq S$，故 S char G.

$(4)\Rightarrow(1)$ 显然. ■

由推论 1，若 $\left|G\right|=p^am$，则 $n_p(G)\left|m\right.$. 例如，若 $\left|G\right|=360=2^3\cdot3^2\cdot5$，则由推论 1 知，$G$ 的 9 阶 Sylow $3-$子群的个数是 $\left|G\right|/3^2=2^3\cdot5$ 的因子，形如 $2^i\cdot5^j,0\le i\le3,0\le j\le1$.

事实上我们有进一步的结论，进一步限制了 Sylow $p-$子群的个数 $n_p(G)$ 的取值可能.

定理 4(Sylow 计数定理) 设 G 是有限群，则 $n_p(G)\equiv1(\mathrm{mod}\,p)$，即 $p\left|n_p(G)-1\right.$.

进而，若 $p^e\le\left|S:S\cap T\right|,\forall S\ne T\in\mathrm{Syl}_p(G)$，则 $n_p(G)\equiv1(\mathrm{mod}\,p^e)$，即 $p^e\left|n_p(G)-1\right.$.

即，不同 Sylow 子群交在 Sylow 子群中的最小指数整除 $n_p(G)-1$.

例如，应用推论 1 与定理 4，则 360 阶群的 9 阶子群的个数 $n_3(G)$ 必为 1, 4, 10, 40 之一.

进而，注意到 4 与 40 模 9 的余数不为 1，如果 $n_3(G)\in\{4,40\}$，则 $3^2\nmid n_3(G)-1$，于是由定理 4 知存在 $S,T\in\mathrm{Syl}_3(G)$ 使得 $9>\left|S:S\cap T\right|=\dfrac{9}{\left|S\cap T\right|}$，所以 $\left|S\cap T\right|=3$，即存在交非平凡的两个 Sylow 子群 S,T.

为证明定理，需要先证明一个引理.

引理 1 设 G 是有限群，$S\in \mathrm{Syl}_p(G)$，则

(1) $S\in \mathrm{Syl}_p\left(\mathbf{N}_G(S)\right), S\lhd \mathbf{N}_G(S)$，即 S 是 $\mathbf{N}_G(S)$ 唯一的 Sylow $p-$ 子群;

(2) 如果 P 是 $\mathbf{N}_G(S)$ 的 $p-$ 子群，则 $P\le S$.

证明 (1) 由 $S\in \mathrm{Syl}_p(G)$ 知 S 是 G 的极大 $p-$ 子群，又显然 $S\le \mathbf{N}_G(S)$，所以 S 也是 $\mathbf{N}_G(S)$ 的极大 $p-$ 子群，故 $S\in \mathrm{Syl}_p\left(\mathbf{N}_G(S)\right)$. 由 $\mathbf{N}_G(S)$ 的定义知 $S\lhd \mathbf{N}_G(S)$;

(2) 由 $S\in \mathrm{Syl}_p\left(\mathbf{N}_G(S)\right), S\lhd \mathbf{N}_G(S)$ 与推论 2 知 $P\le S$.

另一证法 由 $P\le \mathbf{N}_G(S)$ 知 $PS=SP$，故 $PS\le G$. 再由 $|PS|=\dfrac{|S||P|}{|S\cap P|}=|S|\cdot|P:S\cap P|$ 知 PS 是 G 的 $p-$ 子群. 由 S 是 G 的极大 $p-$ 子群与 $S\le PS$ 知 $PS=S$，所以 $P\le S$.■

定理 4 的证明 设 $P\in \mathrm{Syl}_p(G)$，令 P 共轭作用于 $\mathrm{Syl}_p(G)$，直接验证知作用良定. 在此作用下 $n_p(G)$ 元集 $\mathrm{Syl}_p(G)$ 分解为若干轨道之并，$\{P\}$ 显然是一个长度为 1 的 $P-$ 轨道. 为了证明 $n_p(G)\equiv 1\left(\mathrm{mod}\, p^e\right)$，只需证明其它轨道的长度均被 p^e 整除:

任取 $P\ne S\in \mathrm{Syl}_p(G)$，令 $\mathcal{O}_S$ 为 $\mathrm{Syl}_p(G)$ 中含 S 的轨道，则 S 的稳定子群为

$$\left\{x\in P\middle| x\cdot S=S\right\}=\left\{x\in P\middle| xSx^{-1}=S\right\}=\left\{x\in P\middle| x\in \mathbf{N}_G(S)\right\}=\mathbf{N}_P(S),$$

由 FCP 知 $\left|\mathcal{O}_S\right|=\left|P:\mathbf{N}_P(S)\right|$.

注意到 $\mathbf{N}_P(S)\le \mathbf{N}_G(S)$ 是 $p-$ 子群，由引理 1 知 $\mathbf{N}_P(S)\le S$，又 $\mathbf{N}_P(S)\le P$，故 $\mathbf{N}_P(S)\le S\cap P$，又显然有 $S\cap P\le \mathbf{N}_P(S)$，故 $\mathbf{N}_P(S)=S\cap P$.

所以 $\left|\mathcal{O}_S\right|=\left|P:\mathbf{N}_P(S)\right|=|P:S\cap P|$ 是 p^e 的倍数. 故 $n_p(G)\equiv 1\left(\mathrm{mod}\, p^e\right)$，由整数 $e\ge 1$ 知 $n_p(G)\equiv 1(\mathrm{mod}\, p)$.■

3.3 pq, p^2q, p^3q 阶群的 Sylow 子群

我们下面应用 Sylow 定理来分析 pq, p^2q, p^3q 阶群的 Sylow 子群，其中 p, q 均为素数.

定理 1 设 $|G|=pq, p>q$ 均为素数.

(1) G 的 Sylow $p-$ 子群正规，或者等价地，G 的 p 阶子群正规.

(2) 若 G 非交换，则: $q\,|\,p-1$ 且 G 恰有 p 个 Sylow $q-$ 子群;

(3) 若 G 是交换群, 则 G 循环.

证明 (1) 由推论 1 得 $n_p(G)=q$ 或 1, 又由 Sylow 计数定理知 $n_p(G)=1(\mathrm{mod}\,p)$, 故由 $p>q$ 知 $n_p(G)=1$, 即 G 的 Sylow $p-$子群正规. 或: 由 Sylow $p-$子群 P 在群 G 中的指数 q 是 $|G|$ 的最小素因子知 $P\triangleleft G$.

(2) 令 $P\in \mathrm{Syl}_p(G)$, 由(1)知 $P\triangleleft G$, 如果 G 的 Sylow $q-$子群 Q 也正规, 由 $P\cap Q=1$ 知 G 为 Abel 群, 矛盾! 于是 G 的 Sylow $q-$子群不正规, 即 $n_q(G)\neq 1$, 由推论 3.2.1 知 $n_q(G)=p$, 再由 Sylow 计数定理知 $n_q(G)\equiv 1(\mathrm{mod}\,q)$, 所以 $q|p-1$.

(3) 由 Cauchy 推论知 G 中存在 p 阶元 x 与 q 阶元 y, 由 G 交换知 $o(xy)=pq$, 所以 $G=\langle xy\rangle$ 循环.■

定理 1 允许存在 pq 阶非 Abel 群, 其中 $q|p-1$. 事实上确实可以构造出这样的 pq 阶非 Abel 群, 且这样的群在同构的意义下是唯一的, 参阅习题 13.

定理 2 设 $|G|=p^2q$, 其中 $p\neq q$ 为互异素数. 则 G 的 Sylow $p-$子群或 $q-$子群正规, 等价地 $n_p(G)=1$ 或 $n_q(G)=1$.

证明 由推论 3.2.1 知 $n_q(G)\in\{1,p,p^2\}, n_p(G)=\{1,q\}$. 下设 $n_q(G)>1$, 需要证明 $n_p(G)=1$.

若 $n_q(G)=p$, 由 Sylow 计数定理知 $q|n_q(G)-1=p-1$, 特别地 $p>q$. 此时如果 $n_p(G)=q$, 那么由 Sylow 计数定理知 $p|n_p(G)-1=q-1$, 于是 $p<q$, 矛盾! 所以 $n_p(G)=1$.

若 $n_q(G)=p^2$, 对 G 中元计数.

G 的任两个不同的 Sylow $q-$子群的交是两个不同的 q 阶子群的交, 必为单位子群, 于是 p^2 个 Sylow $q-$子群共 $p^2(q-1)$ 个 q 阶元. 记 G 剩下的 $p^2q-p^2(q-1)=p^2$ 个元所成子集为 X, 设 $S\in\mathrm{Syl}_p(G)$, 由 S 不含 q 阶元知 $S\subseteq X$, 再由 $|S|=p^2=|X|$ 知 $S=X$, 即 G 的 Sylow $p-$子群唯一, 恰为 $S=X$, 正规.■

定理 3 设 $|G|=p^3q$, 其中 $p\neq q$ 为互异素数. 则必成立如下之一:

(1) G 有正规的 Sylow $p-$子群, 或者等价地 $n_p(G)=1$;

(2) G 有正规的 Sylow $q-$子群, 或者等价地 $n_q(G)=1$;

(3) $p=2, q=3$ 且 $|G|=24$.

证明 设(1)(2)不成立, 证明(3)即可. 设 $n_p(G)\neq 1$ 且 $n_q(G)\neq 1$, 由推论 3.2.1, 有

$$n_p(G)=q \text{ 且 } n_q(G)\in\{p,p^2,p^3\}.$$

由 Sylow 计数定理知 $p\mid n_p(G)-1=q-1$, 再由 $p\neq q$ 知 $p<q$.

若 $n_q(G)=p$, 由 Sylow 计数定理知 $q\mid p-1$, 再由 $p\neq q$ 知 $p>q$, 矛盾于 $p<q$!

若 $n_q(G)=p^3$, 如定理 2 对 G 计数知, G 有 $p^3(q-1)$ 个 q 阶元, 剩余的 p^3 个元恰构成 G 唯一的 p^3 阶 Sylow $p-$子群, 得 $n_p(G)=1$, 矛盾!

若 $n_q(G)=p^2$, 由 Sylow 计数定理知 $q\mid p^2-1$, 由 q 是素数知 $q\mid p-1$ 或者 $q\mid p+1$.

若 $q\mid p-1$ 则 $p>q$, 矛盾于 $p<q$!

故 $q\mid p+1$, 此时有 $p<q\leq p+1$, 由 p,q 均素数知 $p=2,q=3$, 此时 $|G|=2^3\cdot 3=24$. ■

一个自然的问题是, 是否存在 24 阶群使得其 Sylow $2-,3-$子群均不正规? 定理 3 并没有回答这一问题. 在有限群论中, 人们能证明一个一般性的结果, 给出证明不成立例外情形的一个较小列表. 那么例外情形是否存在? 这不仅仅是证明不够完美的小缺陷. 事实上 24 阶对称群 S_4 正是定理 3 的第三种情形的群例, 且是同构意义下唯一的群例.

$$S_4=\left\{\begin{array}{l}(1),(12),(13),(14),(23),(24),(12)(34),(13)(24),(14)(23)\\(34),(123),(132),(124),(142),(134),(143),(234),(243),\\(1234),(1243),(1324),(1342),(1423),(1432)\end{array}\right\}$$

S_4 有 4 个 Sylow $3-$子群

$$H_1=\{(1),(123),(132)\},H_2=\{(1),(124),(142)\},H_3=\{(1),(134),(143)\},H_4=\{(1),(234),(243)\},$$

有 3 个互为共轭的 Sylow $2-$子群(均同构于二面体群 D_8):

$$K_1=\{(1),(12)(34),(14)(23),(13)(24),(12),(34),(1324),(1423)\},$$

$$K_2=\{(1),(12)(34),(14)(23),(13)(24),(13),(24),(1234),(1432)\},$$

$$K_3=\{(1),(12)(34),(14)(23),(13)(24),(14),(23),(1243),(1342)\}.$$

3.4 群的单性判定

我们现在希望利用 Sylow 定理与其它群的性质证明某个指定合数阶的群不是单群.

我们先回忆 2.1 节定理 4 的结论及其证明.

设 H 是群 G 的指数大于 $n>1$ 的子群. 令群 G 左乘作用在 n 元集 $\Omega=\{aH\,|\,a\in G\}$ 上, 则作用的核为

$$\mathrm{Core}_G(H)=\bigcap_{x\in G}xHx^{-1},$$

它是群 G 含于 H 的极大正规子群. 自然诱导出一个从 G 到对称群 S_n 的群同态:

$$\sigma:G\to S_n,\ g\mapsto(\sigma_g:aH\mapsto gaH,\forall aH\in\Omega),\forall g\in G,$$

由同构定理 A 有 $G/\mathrm{Core}_G(H)\cong S_n$ 的某子群. 令 $N=\mathrm{Core}_G(H)=\bigcap_{x\in G}xHx^{-1}$, 我们可以得到如下定理:

定理 1 设 H 是群 G 的指数 $n>1$ 的子群, 则

(1) 存在 $N=\bigcap_{x\in G}xHx^{-1}\lhd G$ 使得 $N\le H$ 且 $|G:N|\,|\,n!$.

(2) 如果 $|G|\nmid n!$, 则 N 是 G 的非平凡正规子群, 于是 G 不是单群;

(3) 如果 G 是单群, 则 G 同构于 S_n 的某子群.

如下定理可以视为定理 1, 推论 3.2.1 与 Sylow 计数定理的结合.

定理 2 设 $|G|=p^am$, 其中整数 $a>0,m>1$, 素数 $p\nmid m$. 如果 G 是单群, 则 $n:=n_p(G)$ 满足如下条件:

(1) $n>1$; (2) $n\,|\,m$; (3) $n\equiv1(\mathrm{mod}\,p)$; (4) $|G|\,|\,n!$.

证明 任取 $P\in\mathrm{Syl}_p(G)$.

由 G 是单群知其 Sylow $p-$子群作为 G 的非平凡子群不正规, 于是 $P\le\mathbf{N}_G(P)<G$, 由推论 3.2.1 知 $n=|G:\mathbf{N}_G(P)|>1$, $n=|G:\mathbf{N}_G(P)|\,|\,|G:P|=m$, 再由 Sylow 计数定理得(3).

注意到 $n=|G:\mathbf{N}_G(P)|>1$, 因为 G 是单群, 由定理 1 (3)知 G 同构于 S_n 的某子群, 故 $|G|\,|\,n!$.■

例 1 设 $|G|=1,000,000=2^6\cdot5^6$, 则 G 不是单群.

证明 反证, 设 G 是单群, 则由定理 2 知

$$n_5(G)>1,\ n_5(G)\,|\,2^6\Rightarrow n_5(G)\in\{1,2,4,8,16\},\ n_5(G)\equiv1(\mathrm{mod}\,5).$$

于是 $n_5(G)=16$, 由定理 2(4)知 $|G|=2^6\cdot5^6\,|\,16!$, 这与整除 16!的 5 的最高幂次为 5^3 矛盾! ■

例 2 设 $|G|=8000=2^6\cdot5^3$, 则 G 不是单群.

证明 反证, 设 G 为单群, 则由定理 2 知 $n_5(G)=16$. 由于 $16\equiv1(\mathrm{mod}\,5^2)$ 不成立, 由 Sylow 计数定理知存在两个互异的 $S,T\in\mathrm{Syl}_5(G)$ 使得 $5^2>|S:S\cap T|$, 故 $|S:S\cap T|=5$ 是 S 的最小素因子, 所以 $S\cap T\lhd S$, 同理

$S\cap T\lhd T$. 令 $H=\mathbf{N}_G(S\cap T)$, 于是 $S\cap T$ 是 H 的 25 阶正规子群. 而由 G 单知 $S\cap T$ 不是 G 的正规子群, 故 $H<G$.

此时 $S,T\le H$, 即 H 有两个互异的 Sylow $5-$子群, $n_5(H)>1$. 又 $n_5(H)\equiv 1(\mathrm{mod}\,5)$ 且 $n_5(H)\big||H|$, 所以 $n_5(H)=2^4$, 于是 $2^4\big||H|$. 又 $S\le H$ 知 $5^3\big||H|$, 于是 $2^4 5^3\big||H|$, 得 $|G:H|\le 2^2$, 由定理 2(4)知 $|G|\big|4!$, 矛盾!■

例 3 (2010 丘成桐大学生数学竞赛团体赛)证明 150 阶群不是单群.

证明 反证. 设 150 阶群 G 单. 注意到 $150=2\cdot 3\cdot 5^2$, 由定理 2 知

$$n_5(G)\big|6\Rightarrow n_5(G)\in\{1,2,3,6\},\ n_5(G)\equiv 1(\mathrm{mod}\,5),\ n_5(G)>1,$$

所以 $n_5(G)=6$.

如果任意两个不同 Sylow $5-$子群的交均平凡, 则 6 个 Sylow $5-$子群共含 G 的 $6\times 24=145$ 个元. 由 G 单知其至少有 3 个 2 阶 Sylow $2-$子群, 于是 G 至少有 3 个 2 阶元, 因而是 G 恰有 $150-145-3=2$ 个 3 阶元, 所以 G 有唯一 3 阶子群 P, 此时 $P\lhd G$, 这与 G 单矛盾!

于是存在两个不同的 Sylow $5-$子群 P 与 Q, 其交 H 为 5 阶子群, 是 P 与 Q 的正规子群(H 在 P 与 Q 中的指数为 $|P|=|Q|=5^2$ 的最小素因子), 因而 H 在 G 中的正规化子 $\mathbf{N}_G(H)$ 含 P 与 Q, 于是 $\mathbf{N}_G(H)$ 的 Sylow $5-$子群数 $n_5(\mathbf{N}_G(H))>1$, 由 Sylow 计数定理知 $n_5(\mathbf{N}_G(H))\ge 6$. 另一方面, 显然有 $\mathrm{Syl}_5(\mathbf{N}_G(H))\subseteq\mathrm{Syl}_5(G)$, 因而 $n_5(\mathbf{N}_G(H))\le n_5(G)=6$, 故 $n_5(\mathbf{N}_G(H))=6$, 于是 $6\big|\mathbf{N}_G(H)|$. 又 $|P|=5^2\big|\mathbf{N}_G(H)|$, 所以 $6\cdot 25\big|\mathbf{N}_G(H)|$, 再由 $|\mathbf{N}_G(H)|\big||G|=150$ 知 $\mathbf{N}_G(H)=G$, 于是 $H\lhd G$, 这与 G 单矛盾! ■

证明 2 反证. 设 150 阶群 G 单. 注意到 $150=2\cdot 3\cdot 5^2$, 由定理 2 知

$$n_5(G)\big|6\Rightarrow n_5(G)\in\{1,2,3,6\},\ n_5(G)\equiv 1(\mathrm{mod}\,5),\ n_5(G)>1,$$

所以 $n_5(G)=6$, 于是由定理 2(4)知 $150=|G|\big|6!=720$, 矛盾!■

例 4 设 $|G|=12376=2^3\cdot 3^3\cdot 11$, 则 G 不是单群.

证明 反证, 设 G 是单群, 则由定理 2 知:

$$n_{11}(G)\big|2^3 3^3=216\Rightarrow n_{11}(G)\in\{1,2,4,8,3,12,24,9,18,36,72,27,54,108,216\},$$

$$n_{11}(G)>1,\ n_{11}(G)\equiv 1(\mathrm{mod}\,11),$$

故 $n_{11}(G)=12=2^2\cdot 3$.

只需找出 G 的一个真子群 H 使得指数 $n=[G:H]<11$, 则由定理 2 知 $|G|\big|n!$, 与 $11\big||G|$ 矛盾!

任取 $S\in \mathrm{Syl}_{11}(G)$，则 $|G:\mathbf{N}_G(S)|=n_{11}(G)=2^2\cdot 3$，故 $|\mathbf{N}_G(S)|=|G|/2^2 3=2\cdot 3^2\cdot 11$.

由“N/C 定理”知 $\mathbf{N}_G(S)/\mathbf{C}_G(S)$ 同构于 $\mathrm{Aut}(S)$ 的某子群，而 $|\mathrm{Aut}(S)|=\varphi(11)=10$，由 Lagrange 定理知 $|\mathbf{N}_G(S):\mathbf{C}_G(S)|\,|10$，由 $|\mathbf{N}_G(S)|=2\cdot 3^2\cdot 11$ 知 $|\mathbf{C}_G(S)|=2\cdot 3^2\cdot 11$ 或 $3^2\cdot 11$，特别地 $3^2\,||\mathbf{C}_G(S)|$.

令 $P\in \mathrm{Syl}_3(\mathbf{C}_G(S))$，则 $|P|=3^2$，由 G 单知 $\mathbf{N}_G(P)<G$. 下面证明 $|G:\mathbf{N}_G(P)|<11$ 即可!

由 $P\in \mathrm{Syl}_3(\mathbf{C}_G(S))$ 知 $P\le \mathbf{C}_G(S)$，故 $S\le \mathbf{C}_G(P)\le \mathbf{N}_G(P)$，所以 $11=|S|\,||\mathbf{N}_G(P)|$.

由 Sylow D 定理知 9 阶子群 P 含于 G 的某 27 阶 Sylow $3-$子群 Q，由 $|Q:P|=3$ 是 $|Q|$ 的最小素因子知 $P\lhd Q$，于是 $Q\le \mathbf{N}_G(P)$ 从而 $3^3=|Q|\,||\mathbf{N}_G(P)|$.

由 $11|\mathbf{N}_G(P)|$ 与 $3^3\,||\mathbf{N}_G(P)|$ 得 $3^3\cdot 11\,||\mathbf{N}_G(P)|$，此时 $|G:\mathbf{N}_G(P)|\le 2^3<11$，证毕. ■

3.5 有限 p 群

Sylow 存在性定理保证了有限群中某些 $p-$子群的存在性，自然有必要研究这些子群的性质. 目前已知大量的有限 $p-$群，我们仅考虑一些最重要的例子.

引理 1 设有限 $p-$群 P 作用在集合 Ω 上的不动点子集为

$$\Omega_0=\{\alpha\in\Omega\,|\,x\cdot\alpha=\alpha,\forall x\in P\},$$

则 $|\Omega|\equiv|\Omega_0|\pmod p$. 即作用集与不动点子集的势模 p 同余.

证明 不动点子集 Ω_0 即长度为 1 的轨道中的文字所成集，故 $\Omega-\Omega_0$ 是长度大于 1 的轨道的并，由 FCP 定理知任一轨道 $\mathcal{O}_\alpha$ 的长度 $|\mathcal{O}_\alpha|=|P|/|G_\alpha|$ 都素数幂 $|P|$ 的因子，所以长度大于 1 的轨道 $|\mathcal{O}_\alpha|$ 的长度都是 p 的倍数:

$$|\Omega|=|\Omega_0|+|\Omega-\Omega_0|=|\Omega_0|+\sum_{|\mathcal{O}_\alpha|>1}|\mathcal{O}_\alpha|=|\Omega_0|+\sum_{|\mathcal{O}_\alpha|>1}|P|/|P_\alpha|\equiv|\Omega_0|\pmod p.\blacksquare$$

定理 1 设 N 是有限 $p-$群 P 的正规且非单位子群，则 $N\cap\mathbf{Z}(P)>1$. 特别地，任一非平凡有限 $p-$群都有非平凡的中心元.

证明 因为 $N\lhd P$，故可令 P 共轭地作用在 N 上，此时作用的不动点集

$$\{x\in N\,|\,x\cdot g=x,\forall g\in P\}=\{x\in N\,|\,g^{-1}xg=x,\forall g\in P\}=N\cap\mathbf{Z}(P).$$

由引理 1 知 $|N\cap\mathbf{Z}(P)|\equiv|N|\equiv 0\pmod p$，又 $1\in N\cap\mathbf{Z}(P)$，故 $N\cap\mathbf{Z}(P)>1$.

令 $N=P>1$，则 $\mathbf{Z}(P)=P\cap\mathbf{Z}(P)>1$，即：任一非平凡有限 $p-$群 P 都有非平凡的中心元. ■

推论 1 有限 $p-$群 P 是单群，则 $|P|=p$.

证明 由定理 1 知 $1<\mathbf{Z}(P)\lhd P$，由 P 单知 $P=\mathbf{Z}(P)$ 从而 Abel，再由 P 单知 $|P|=p$.■

推论 2 设 P 是有限非平凡 $p-$群，则 P 有一个指数为 p 的子群，且这样的子群均正规.

证明 P 非平凡，即 $P>1$. 由 P 有限知可选取 P 的一个极大正规子群 N，即 $N\lhd P, N<P$，且不存在 P 的正规子群 M 使得 $N<M<P$. 由子群对应定理知 P/N 是单群，于是由推论 1 知 $|P:N|=p$. 任取 P 的指数为 p 的子群，由指数是 $|P|$ 的最小素因子知该子群正规.■

给定有限 $p-$群 P，由推论 2 可找出指数为 p 的正规子群 P_1，然后对 P_1 找出其指数为 p 的正规子群 P_2，如此继续下去可知对 $|P|$ 的任一因子，P 均具有给定因子阶的子群. 结合 Sylow E 定理，得到如下推论.

推论 3 如果 p^e 是有限群 G 的阶的素数幂因子，则 G 具有 p^e 阶子群.■

例 1 (1) 设 G 是有限群，则 $G/\mathbf{Z}(G)$ 不能是循环群，特别地 $\mathbf{Z}(G)$ 在群 G 中的指数不能是素数；

(2) p^2 阶的有限群 P 都是 Abel 群，同构于 $\mathbb{Z}_{p^2}$ 或 $\mathbb{Z}_p\times\mathbb{Z}_p$.

证明 (1) 反证. 如果 $G/\mathbf{Z}(G)$ 是循环群，设 $G/\mathbf{Z}(G)=\langle g\mathbf{Z}(G)\rangle$，则 $x\mathbf{Z}(G), y\mathbf{Z}(G)\in\langle g\mathbf{Z}(G)\rangle$，$\forall x,y\in G$，不妨设 $x\mathbf{Z}(G)=g^i\mathbf{Z}(G), y\mathbf{Z}(G)=g^j\mathbf{Z}(G)$，则 $x=g^iz_1, y=g^jz_2$ 对某 $z_1,z_2\in\mathbf{Z}(G)$，此时

$$xy=g^iz_1\cdot g^jz_2=g^{i+j}z_1z_2=g^{i+j}z_2z_1=g^jz_2\cdot g^iz_1=yx,$$

所以 G 是交换群，于是 $\mathbf{Z}(G)=G$，与 $|G:\mathbf{Z}(G)|=p$ 是素数矛盾!

如果 $|G:\mathbf{Z}(G)|=p$ 是素数，则 $G/\mathbf{Z}(G)$ 是素数阶群，循环，矛盾! 所以 $|G:\mathbf{Z}(G)|$ 不能是素数.

(2) 由 Lagrange 定理知 $|\mathbf{Z}(P)|=1, p$ 或 p^2，由定理 1 知 $|\mathbf{Z}(P)|>1$，由(1)知 $|\mathbf{Z}(P)|\neq p$，故 $|\mathbf{Z}(P)|=p^2=|P|$，所以 $P=\mathbf{Z}(P)$ 是交换群. 由第二章 Abel $p-$群的结构定理知 P 同构于 $\mathbb{Z}_{p^2}$ 或 $\mathbb{Z}_p\times\mathbb{Z}_p$.■

例 2 (2018 年丘成桐大学生数学竞赛个人赛) 证明 99 阶群都是 Abel 群.

证明 设 G 是 $99=3^2\cdot11$ 阶群，由推论 3.2.1 与 Sylow 计数定理知 $n_{11}(G)\big|9$ 且 $n_{11}(G)\equiv1(\mathrm{mod}11)$，所以 $n_{11}(G)=1$，于是 G 存在唯一的 Sylow $11-$子群 $P\lhd G$. 同理，$n_3(G)\big|11$ 且 $n_3(G)\equiv1(\mathrm{mod}3)$ 从而 $n_3(G)=1$，G 存在唯一的 Sylow $3-$子群 $Q\lhd G$，由 $(|P|,|Q|)=(11,9)=1$ 知 $P\cap Q=1$，于是 $|PQ|=\dfrac{|P||Q|}{|P\cap Q|}=99=|G|$，故 $G=P\times Q$.

11 阶群 P 是素数阶循环群, 由例 1(2)知 9 阶群 Q 交换, 所以 $G=P\times Q$ 是交换群.■

有限非平凡 $p-$ 群有非平凡的中心是非常重要且极具威力的一个结论. 它的另一个应用是 $p-$ 群中正规化子的增长性.

定理 2 设 H 是有限 $p-$ 群 P 的真子群, 则 $H<\mathbf{N}_P(H)$.

证明 注意到 $\mathbf{N}_P(H)=\{x\in P\mid xHx^{-1}=H\}$, $\mathbf{Z}(P)=\{x\in P\mid xyx^{-1}=y,\forall y\in P\}$, 显然 $\mathbf{Z}(P),H\le\mathbf{N}_P(H)$.

如果 $\mathbf{Z}(P)$ 不包含在 H 中, 则存在 $x\in\mathbf{Z}(P)-H\subseteq\mathbf{N}_P(H)-H$, 于是 $H<\mathbf{N}_P(H)$.

下设 $\mathbf{Z}(P)\subseteq H$. 此时 $H/\mathbf{Z}(P)<P/\mathbf{Z}(P)$, 由 $\mathbf{Z}(P)>1$ 知 $P/\mathbf{Z}(P)$ 是阶比 P 小的 $p-$ 群. 对 $|P|$ 用归纳法, 由归纳假设知 $H/\mathbf{Z}(P)<\mathbf{N}_{P/\mathbf{Z}(P)}\left(H/\mathbf{Z}(P)\right)$, 由子群对应定理知存在 P 的某个包含 $\mathbf{Z}(P)$ 的子群 M 使得 $\mathbf{N}_{P/\mathbf{Z}(P)}\left(H/\mathbf{Z}(P)\right)=M/\mathbf{Z}(P)$.

此时 $H/\mathbf{Z}(P)\lhd M/\mathbf{Z}(P)$ 从而有 $H\lhd M$, 且 $H/\mathbf{Z}(P)<M/\mathbf{Z}(P)$ 表明 $H<M$, 所以 $H<M\subseteq\mathbf{N}_P(H)$. ■

推论 4 设 P 是有限 $p-$ 群, 则 P 的极大子群均正规且在 P 中的指数为 p.

证明 设 H 是 P 的一个极大子群. 由定理 2 知 $H<\mathbf{N}_P(H)$, 由 H 极大知 $\mathbf{N}_P(H)=P$, 故 $H\lhd P$. 因为 H 是 P 的极大子群, 由子群对应定理知 $p-$ 群 P/H 不含真子群, 阶为素数 p, 所以 $[P:H]=|P/H|=p$.■

定理 3 设 $|G|=p^aq$, 其中 p 与 q 是互异素数且整数 $a>0$, 则 G 不是单群.

证明 反证. 设 G 是单群, 由定理 3.4.2 知 $n_p(G)=q$ 且 $p\mid q-1$.

(1) 如果 $S\cap T=1,\forall S\ne T\in\mathrm{Syl}_p(G)$. 对 G 中元计数: G 的 q 个 Sylow $p-$ 子群有 $q\left(p^2-1\right)+1$ 个 $p-$ 元素, 于是剩余的 $q-1$ 个元与单位元构成唯一的 Sylow $q-$ 子群, 得 $n_q(G)=1$, 与 G 是单群矛盾!

(2) 于是存在 $S\ne T\in\mathrm{Syl}_p(G)$ 使得 $S\cap T>1$, 选取 $S,T\in\mathrm{Syl}_p(G)$ 使得 $|S\cap T|$ 最大. 令 $N=\mathbf{N}_G(S\cap T)$, 由 $S\cap T<S$ 与定理 2 知 $S\cap T<\mathbf{N}_S(S\cap T)=S\cap\mathbf{N}_G(S\cap T)=S\cap N$. 同理有 $S\cap T<T\cap N$.

(3) 如果 N 是 $p-$ 群, 由 Sylow D 定理知 N 含于某 $P\in\mathrm{Syl}_p(G)$, 此时 $S\cap P\supseteq S\cap N>S\cap T$, 由 $S\cap T$ 的阶极大性知 $P=S$. 同理得 $P=T$, 于是 $S=T$, 与 $S\ne T$ 的选取条件矛盾!

(4) 于是 N 不是 $p-$ 群, 故 $q\|N|$. 设 q 阶子群 $Q\in\mathrm{Syl}_q(N)$, 而 $S\in\mathrm{Syl}_p(N)$ 知 $|S|=p^a$, 因此有 $Q\cap S=1$ 且 $|QS|=|Q||S|/|Q\cap S|=|Q||S|=qp^a=|G|$, 故 $G=QS$.

(5) 此时，$\forall g=xy\in G$，其中 $x\in Q\subseteq N=\mathbf{N}_G\left(S\cap T\right), y\in S$，有

$$gSg^{-1}=xySy^{-1}x^{-1}=x\left(ySy^{-1}\right)x^{-1}=xSx^{-1}\supseteq x\left(S\cap T\right)x^{-1}=S\cap T,$$

所以 $1<S\cap T\subseteq \bigcap\limits_{g\in G} gSg^{-1}=\mathrm{core}_G\left(S\right)\lhd G$，于是单群 G 有非平凡正规子群 $\mathrm{core}_G\left(S\right)$，矛盾！故 G 不为单群.■

事实上还有比定理 3 更一般的结论, W.Burnside 的证明了:

$$\text{如果}\left|G\right|=p^aq^b\text{，其中 }p,q\text{ 是素数，}a,b\in\mathbb{Z}_{\geq 0}\text{，则 }G\text{ 为单群}\Leftrightarrow\left|G\right|\text{ 为素数.}$$

这就是著名的“p^aq^b – 定理”，它也可以视为有限群特征标理论的一个重要应用.

在定理 3 的证明中，我们通过分析极大 Sylow 交获得了 $\mathrm{cors}_G\left(S\right)$(其中 $S\in\mathrm{Syl}_p\left(G\right)$)的某些信息. 下面给出极小 Sylow 交与 $\mathrm{cors}_G\left(S\right)$ 关系的某些结论. 我们知道 $\mathrm{cors}_G\left(S\right)$ 是 G 的含于 S 的最大正规子群，是 S 的全部共轭的交，即 G 的全部 Sylow p – 子群的交. 问题是 $\mathrm{cors}_G\left(S\right)$ 是否恰为两个 Sylow p – 子群的交？我们发现虽然一般情形下此结论不成立，但是当 S 是 Abel 群该结论为真.

记群 G 的全部 Sylow p – 子群的交为 $\mathbf{O}_p\left(G\right)$，即

$$\mathbf{O}_p\left(G\right):=\bigcap_{g\in G} gSg^{-1}=\bigcap_{P\in\mathrm{Syl}_p(G)} P=\cap\mathrm{Syl}_p\left(G\right)=\mathrm{cors}_G\left(S\right),$$

则它是有限群 G 唯一最大的正规 p – 子群.

定理 4 设 G 是有限群，p – 子群 $P\lhd G$，则 $P\leq\mathbf{O}_p\left(G\right)\lhd G$.

证明 任取 $x\in G$，$S\in\mathrm{Syl}_p\left(G\right)$，则

$$x\mathbf{O}_p\left(G\right)x^{-1}=x\left(\bigcap_{g\in G} gSg^{-1}\right)x^{-1}=\bigcap_{g\in G} xgSg^{-1}x^{-1}=\bigcap_{gx\in G}\left(xg\right)S\left(xg\right)^{-1}=\mathbf{O}_p\left(G\right),$$

所以 $\mathbf{O}_p\left(G\right)\lhd G$；

由 Sylow C 定理知 $P\subseteq gSg^{-1}$ 对某 $g\in G$，由 $P\lhd G$ 知 $P=g^{-1}Pg\subseteq g^{-1}\left(gSg^{-1}\right)g=S$，由 S 的任意性知 P 含于所有 Sylow p – 子群中，即 $P\subseteq\mathbf{O}_p\left(G\right)$.■

定理 5 设 G 是有限群，设 $S,T\in\mathrm{Syl}_p\left(G\right)$ 使得 $S\cap T$ 具有极小的阶. 如果 $N\leq S\cap T$ 使得 $N\lhd S, N\lhd T$，则 $N\leq\mathbf{O}_p\left(G\right)$.

证明 注意到 $\mathbf{O}_p\left(G\right)=\cap\mathrm{Syl}_p\left(G\right)$，只需证明 $N\leq P,\forall P\in\mathrm{Syl}_p\left(G\right)$.

任取 $P\in\mathrm{Syl}_p\left(G\right)$，令 $M=\mathbf{N}_G\left(N\right)$. 由 $N\lhd T$ 知 $T\leq M$，于是 $T\in\mathrm{Syl}_p\left(M\right)$，由定理 3.2.3 知存在某个元

$m\in M$ 使得 $m(P\cap M)m^{-1}\le T$，即 $mPm^{-1}\cap M\le T$，又由 $N\lhd S$ 知 $S\le M$，故有

$$mPm^{-1}\cap S=mPm^{-1}\cap(M\cap S)=(mPm^{-1}\cap M)\cap S\le T\cap S.$$

注意到 $S\cap T$ 的阶是 Sylow 交中极小者，故 $mPm^{-1}\cap S=T\cap S\ge N$，于是 $N\le mPm^{-1}$.

最后，注意到 $m\in M=\mathbf{N}_G(N)$，故 $N=m^{-1}Nm\le P$，正是所需.■

定理 6(Brodkey) 设 G 是有限群，$S\in\mathrm{Syl}_p(G)$ 是 Abel 群，则存在 $T\in\mathrm{Syl}_p(G)$ 使得

$$S\cap T=\mathbf{O}_p(G).$$

证明 选取 $T\in\mathrm{Syl}_p(G)$ 使得 $S\cap T$ 具有极小的阶，由 Sylow 共轭定理知 T 与 Abel 群 S 共轭，故 T 是 Abel 群，所以 $S\cap T\lhd S, S\cap T\lhd T$，由定理 5 知 $S\cap T\le\mathbf{O}_p(G)$.

另一方面，由 $S,T\in\mathrm{Syl}_p(G)$ 知 $\mathbf{O}_p(G)=\cap\mathrm{Syl}_p(G)\le S\cap T$. 所以 $S\cap T=\mathbf{O}_p(G)$.■

3.6 交错群的单性及其推论

引理 1 (1) 如果 $\alpha=(i_1i_2\cdots i_s)\cdots(k_1\cdots k_t),\beta=(j_1j_2\cdots j_s)\cdots(l_1\cdots l_t)\in S_n$ 具有相同的不相交轮换分解式，则存在 $\tau\in S_n$ 使得 $\tau\alpha\tau^{-1}=\beta$.

(2) 设 $\alpha,\beta\in S_n$，则：α,β 具有相同的不相交轮换分解式 $\Leftrightarrow\exists\tau\in S_n$ 使得 $\tau\alpha\tau^{-1}=\beta$.

证明 (1) 先考虑 $\alpha=(i_1i_2\cdots i_s),\beta=(j_1j_2\cdots j_s)$ 的简单情形，令 $\tau=\begin{pmatrix}\cdots & i_1 & i_2 & \cdots & i_s & \cdots\\ \cdots & j_1 & j_2 & \cdots & j_s & \cdots\end{pmatrix}$，则

$$\tau\alpha\tau^{-1}=\begin{pmatrix}\cdots & i_1 & i_2 & \cdots & i_s & \cdots\\ \cdots & j_1 & j_2 & \cdots & j_s & \cdots\end{pmatrix}(i_1i_2\cdots i_s)\begin{pmatrix}\cdots & i_1 & i_2 & \cdots & i_s & \cdots\\ \cdots & j_1 & j_2 & \cdots & j_s & \cdots\end{pmatrix}^{-1}=(j_1j_2\cdots j_s),$$

类似地，对引理中 $\alpha=(i_1i_2\cdots i_s)\cdots(k_1\cdots k_t),\beta=(j_1j_2\cdots j_s)\cdots(l_1\cdots l_t)\in S_n$ 的一般情形，令

$$\tau=\begin{pmatrix}\cdots & i_1 & i_2 & \cdots & i_s & \cdots\\ \cdots & j_1 & j_2 & \cdots & j_s & \cdots\end{pmatrix}\cdots\begin{pmatrix}\cdots & k_1 & k_2 & \cdots & k_t & \cdots\\ \cdots & l_1 & l_2 & \cdots & l_t & \cdots\end{pmatrix},$$

则 $\tau\alpha\tau^{-1}=\beta$.

(2) 由(1)，只需证明 $\tau\alpha\tau^{-1}$ 与 α 的不相交轮换分解式相同即可.

不妨设 α 的不相交轮换分解式为 $\alpha=(i_1i_2\cdots i_r)\cdots(k_1\cdots k_s)\cdots(l_1\cdots l_t)$，直接计算有

$$\tau\alpha\tau^{-1}\left(\tau\left(k_x\right)\right)=\tau\alpha\left[\tau^{-1}\left(\tau\left(k_x\right)\right)\right]=\tau\alpha\left(k_x\right)=\tau\left(k_{x+1}\right),1\le x\le s-1,$$

$$\tau\alpha\tau^{-1}\left(\tau\left(k_s\right)\right)=\tau\alpha\left[\tau^{-1}\left(\tau\left(k_s\right)\right)\right]=\tau\alpha\left(k_s\right)=\tau\left(k_1\right),$$

由此得 $\tau\alpha\tau^{-1}=\left(\tau\left(i_1\right)\tau\left(i_2\right)\cdots\tau\left(i_r\right)\right)\cdots\left(\tau\left(k_1\right)\cdots\tau\left(k_s\right)\right)\cdots\left(\tau\left(l_1\right)\cdots\tau\left(l_t\right)\right)$ 与 α 的不相交轮换分解式相同.■

定理 1 (1) 设 $N=\{1,x\}$ 是群 G 的 2 阶正规子群, 则 $N\subseteq\mathbf{Z}(G)$, 即 2 阶正规子群必然含于中心;

(2) 设 $n\ge 4$, 则 $\mathbf{Z}\left(A_n\right)=\mathbf{Z}\left(S_n\right)=1$, 特别地 A_n,S_n 没有 2 阶正规子群.

证明 (1) 任取 $g\in G$, 由 N 正规知 $x^g=g^{-1}xg\in N$ 是 2 阶元, 所以 $g^{-1}xg=x$, 即 $xg=gx$, 所以 $N\subseteq\mathbf{Z}(G)$.

(2) 任取 $1\ne\alpha\in S_n$, 将 α 分解为不相交轮换的乘积后, 不妨设 $\alpha=(12\cdots)\cdots$, 令 $\beta=(23)$, 则

$$\beta\alpha\beta^{-1}=(13\cdots)\cdots\ne\alpha,$$

所以 $\alpha\notin\mathbf{Z}\left(S_n\right)$, 故 $\mathbf{Z}\left(S_n\right)=1$.

任取 $1\ne\alpha\in A_n$, 将 α 分解为不相交轮换的乘积后, 其形状为如下两种情形之一:

[1] 如果 α 的分解式中有对换, 不妨设 $\alpha=(12)\cdots$, 令 $\beta=(123)\in A_n$, 则 $\beta\alpha\beta^{-1}=(23)\cdots\ne\alpha$.

[2] 如果 α 的分解式中没有对换, 不妨设 $\alpha=(123\cdots)\cdots$, 令 $\beta=(12)(34)\in A_n$, 则 $\beta\alpha\beta^{-1}=(214)\cdots\ne\alpha$.

此即中存在 $\beta\in A_n$, 使得 $\beta\alpha\beta^{-1}\ne\alpha$, 故 $\alpha\notin\mathbf{Z}\left(A_n\right)$.

所以 $n\ge 4$ 时 $\mathbf{Z}\left(A_n\right)=1$.■

定理 2 $n\ge 5$ 时, A_n 是单群.

证明 (1) 先证明 $n\ge 4$ 时, A_n 可由全体 3 – 轮换生成, 即 $n\ge 4$ 时:

$$A_n=\left\langle(abc)\middle|a,b,c\in\{1,2,\cdots,n\}\text{ 互异}\right\rangle.$$

注意到对任意两个不同对换的乘积有

$(ac)(ab)=(abc)$, 不同的对换有共同字母时, 其乘积恰为 3 – 轮换

$$(ab)(cd)=(ab)\left[(ac)(ca)\right](cd)=\left[(ab)(ac)\right]\left[(ca)(cd)\right]=(acb)(cda),$$

不同的对换没有共同字母时, 其乘积是 3 – 轮换之积

其中不同的字母 a,b,c,d 表示集合 $\{1,2,\cdots,n\}$ 中不同的文字.

每一个 $\alpha \in A_n$ 都是偶数个对换的乘积, 再利用上面两个式子就可以写成若干个 3 – 轮换之积了.

反之, 每一个 3 – 轮换都是偶置换, 从而有 $\left\langle (abc) \middle| a,b,c \in \{1,2,\cdots,n\} \text{ 互异} \right\rangle \subseteq A_n$.

(2) 如果 $1 \neq N \lhd A_n$, 则 N 含有 3 – 轮换.

设 $\alpha \in N$ 是 N 中变动文字数最少的非恒等置换, 下证 α 变动的文字数恰为 3, 于是 α 是一个 3 – 轮换.

讨论 α 的不相交轮换分解式:

[1] α 不能是两个不相交对换的乘积.

反证, 不妨设不相交对换的乘积 $\alpha = (12)(34) \in N$, 由 $n \geq 5$ 可取 $\beta = (345) \in A_n$, 由 $N \lhd A_n$ 知

$$\alpha\left(\beta\alpha^{-1}\beta^{-1}\right) = (12)(34)(345)(12)(34)(354) = (345) \in N,$$

与 α 变动文字数的最少性矛盾!

[2] α 不能是更多个不相交对换的乘积.

反证, 不妨设 $\alpha = (12)(34)(56)\cdots$, 令 $\beta = (123)$, 由 $N \lhd A_n$ 知

$$\alpha\left(\beta\alpha^{-1}\beta^{-1}\right) = \left[(12)(34)(56)\cdots\right](123)\left[(12)(34)(56)\cdots\right](132) = (13)(24) \in N$$

变动的文字数少于 α, 与 α 变动文字数的最少性矛盾!

由[1][2]知, α 的不相交轮换分解式中最长轮换因子的长度 ≥ 3.

若 α 不是 3 – 轮换, 将 α 最长轮换因子写在最前面, 分两种情形讨论:

[3] 若 α 形如 $\alpha = (123)(45\cdots)\cdots$, 由 α 是偶置换知其变动文字数 ≥ 6, 令 $\beta = (234)$, 则

$$\alpha\left(\beta\alpha^{-1}\beta^{-1}\right) = \left[(123)(45\cdots)\cdots\right](234)\left[(132)(54\cdots)\cdots\right](243) = (15324) \in N$$

变动的文字数少于 α, 矛盾!

[4] 若 α 形如 $\alpha = (1234\cdots)\cdots$, 由 α 是偶置换知其变动文字数 ≥ 5, 令 $\beta = (132)$, 则

$$\alpha\left(\beta\alpha^{-1}\beta^{-1}\right) = \left[(1234\cdots)\cdots\right](132)\left[(4321\cdots)\cdots\right](123) = (143) \in N,$$

变动的文字数少于 α, 矛盾!(实际计算时分两种情形: $\alpha = (1234)\cdots$)与 $\alpha = (1234\cdots k)\cdots$)

综上, α 是一个 3 – 轮换.

(3) N 包含所有 3 – 轮换. 不妨设 $\alpha = (123) \in N$, 则对任意的 3 – 轮换 (ijk), 令 $\beta = \begin{pmatrix} 1 & 2 & 3 & \cdots \\ i & j & k & \cdots \end{pmatrix}$, 则

$$\beta\alpha\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & \cdots \\ i & j & k & \cdots \end{pmatrix}(123)\begin{pmatrix} i & j & k & \cdots \\ 1 & 2 & 3 & \cdots \end{pmatrix} = (ijk) \in N.$$

综上，$n\geq 5$时，A_n的非单位正规子群 N 包含所有3－轮换，而由(1)知 A_n 可由全体3－轮换生成，所以 $N=A_n$，即 A_n 的正规子群均平凡，所以 A_n 是单群.■

证明 2(Isaacs 代数学 P78) 首先考虑 $n=5$ 的情形. A_5 中置换的轮换结构为

$$1^5, 1^1\cdot 2^2, 1^2\cdot 3^1, 5^1,$$

这些元素的个数分别为 $1, C_5^4\cdot 3=15, C_5^3\cdot 2=20, P_5^5/5=24$.

设 N 是 A_5 的真正规子群，证明 $N=1$ 即得结论.

若 $3\|N|$，则由 $|A_5|=2^2\cdot 3\cdot 5$ 知 N 包含 A_5 的一个 Sylow 3－子群，由 A_5 的 Sylow 3－子群均共轭及 N 正规知 N 包含 A_5 的全部 Sylow 3－子群，于是 N 包含 A_5 的 20 个 3 阶元，再由 N 含单位元知 $|N|>20$，由 Lagrange 定理知 $|N|=30$. 类似地若 $5\|N|$，可得 N 包含 A_5 的 24 个 5 阶元且 $|N|=30$.

由上面的推导知，如果 3 或者 5 是正规子群 $|N|$ 阶的因子，都将得到 $|N|=30$，且 N 包含 20 个 3 阶元与 24 个 5 阶元，这是不可能的!

因此 N 只能是 A_5 的一个2－子群. 由定理 2(2)知 $|N|\neq 2$，所以 $|N|=4$，此时 N 是 A_5 唯一的 Sylow 2－子群，不可能包含 A_5 的 15 个 2 阶元!

综上知 $|N|=1$，故 A_5 是单群.

下设 $n\geq 6$，对 n 用归纳法来证明 A_n 为单群. 此时 A_{n-1} 是单群，设 N 是 A_n 的真正规子群. 令 A_n 自然地作用在集合 $\Omega=\{1,2,\ldots,n\}$ 上，令 H 是文字 $n\in\Omega$ 的稳定子群，则 $H=A_{n-1}$ 是单群. 由 $N\lhd A_n$ 知 $N\bigcap H\lhd H$，于是 $N\bigcap H=1$ 或 H.

若 $N\bigcap H=H$，则 $H\leq N$，由 $N\lhd A_n$ 知 $gHg^{-1}\leq N, \forall g\in A_n$，注意到每一个 gHg^{-1} 都是文字 $g(\alpha)$ 在 A_n 中的稳定子群，因此 N 包含 A_n 的全部单个点的稳定子群，特别地 N 包含所有形如两个对换乘积的元，故 $N=A_n$，矛盾!

下设 $N\bigcap H=1$. 若 $N\neq 1$，取 N 中的非单位元 x. 此时 x 要么包含一个长度 $m\geq 3$ 的轮换，要么是一些不相交对换的乘积. 即 x 形如

$$(12)(34)\cdots \text{或} (123\cdots)\cdots$$

令 $y=(356)x(356)^{-1}\in N$，则 $y=(12)(54)\cdots$ 或 $(125\cdots)\cdots$，此时总有 $x\neq y$ 且 $y^{-1}x$ 固定文字 1. 若 H 固定文字

$\alpha\in\Omega$，设 $g(1)=\alpha$，则 $1\neq g\left(y^{-1}x\right)g^{-1}\in N\cap H$，这与 $N\cap H=1$ 矛盾!■

定义 (1) 群 G 的**换位子群**(或导群)定义为: $G'\coloneqq\left\langle aba^{-1}b^{-1}\middle|a,b\in G\right\rangle$. 进而递归定义 $G^{(n)}\coloneqq\left(G^{(n-1)}\right)'$, $n\geq 2$, 称 $G^{(n)}$ 是群 G 的 ***n* 次换位子群**.

(2) 如果存在正整数 n 使得 $G^{(n)}=1$，则称 G 是**可解群**.

性质 (1) $G'\lhd G$;

(2) G 是交换群 $\Leftrightarrow G'=1$;

(3) 设 $N\lhd G$，则 G/N 是交换群 $\Leftrightarrow G'\leq N$.

定理 3 (1) 若 $n\geq 5$，则 S_n 恰有 3 个正规子群: $1, A_n, S_n$.

(2) 设 $n\geq 2$，则 $S_n'=A_n$.

(3) 若 $n\geq 5$，则 S_n 不可解.

证明 (1) 设 $N\lhd S_n$，则 $N\cap A_n\lhd A_n$，由 $A_n\,(n\geq 5)$ 单知 $N\cap A_n=A_n$ 或 1，于是 $A_n\leq N$ 或者 $N\cap A_n=1$.

若 $A_n\leq N$，由 $2=\left|S_n:A_n\right|=\left|S_n:N\right|\cdot\left|N:A_n\right|$ 知 $N=S_n$ 或 A_n.

若 $N\cap A_n=1$，则由 $\left|S_n\right|\geq\left|NA_n\right|=\dfrac{\left|N\right|\left|A_n\right|}{\left|N\cap A_n\right|}=\left|N\right|\left|A_n\right|$ 知 $\left|N\right|\leq\left|S_n:A_n\right|=2$.

若 $\left|N\right|=2$，与定理 2 矛盾! 所以 $\left|N\right|=1$，于是 $N=1$.

(2) 若 $n\geq 2$，$S_n'=\left\langle\alpha\beta\alpha^{-1}\beta^{-1}\middle|\alpha,\beta\in S_n\right\rangle$，注意到 S_n 中每个置换与其逆元有相同的奇偶性，故 $\alpha\beta\alpha^{-1}\beta^{-1}$ 都是偶置换，所以 $S_n'\leq A_n$.

S_2 是 2 阶循环群，交换，此时 $S_2'=1=A_2$.

对 6 阶群 S_3: $(132)=(123)(12)(132)(12)\in S_3'$，$(123)=(132)^{-1}\in S_3'$，表明 $A_3\subseteq S_3'$. 由 $S_3'\leq A_3$ 知 $S_3'=A_3$.

对 12 阶群 S_4，类似于 S_3 知 8 个 3 – 轮换均含于 S_4'. 进而

$$(13)(24)=(13)(1234)(13)(4321)\in S_4',$$

类似可证任两个不相交对换的乘积均含于 S_4'，表明 $A_4\subseteq S_4'$. 由 $S_4'\leq A_4$ 知 $S_3'=A_3$.

若 $n\geq 5$，由(1)知 S_n 的正规子群恰有 $1, A_n, S_n$，由 $S_n'\leq A_n$ 知 $S_n'=A_n$ 或 1，再由 S_n 非交换知 $S_n'>1$，所以 $S_n'=A_n$.

(3) 若 $n\geq 5$，由(2)知 $S_n'=A_n$，而由 A_n 是非交换的单群知 $A_n'=A_n$，所以 S_n 不可解.■

例 1 (2020 全国大学生数学竞赛决赛) 证明 180 阶群不是单群.

证明 反证. 设 G 是 $180=2^2\cdot 3^2\cdot 5$ 阶单群.

由系列 Sylow 计数定理知 G 的 Sylow 3－子群个数 $n_3(G)$ 满足

$$n_3(G)>1, n_3(G)\big|2^2\cdot 5, n_3(G)\equiv 1(\mathrm{mod}\,3),$$

所以 $n_3(G)=4$ 或 10.

如果 $n_3(G)=4$，即 G 有 4 个 Sylow 子群，考虑 G 在 $\mathrm{Syl}_3(G)$ 上的共轭作用，由 G 单知作用核为单位子群，于是 G 同构于 S_4 的某子群，比较阶知这是不可能的. 所以 $n_3(G)=10$.

如果 G 有两个不同的 Sylow 3－子群 S 与 T 的交不是单位子群：$D:=S\cap T>1$，由 S 与 T 的阶为 9 知 D 的阶为 3，且由 D 在 S 与 T 的指数为 3 知 $D\lhd S, D\lhd T$，令 $N:=\mathbf{N}_G(D)$，则 $S,T\leq \mathbf{N}_G(D)$ 且 S,T 是 $\mathbf{N}_G(D)$ 的 Sylow 3－子群，于是 N 中 Sylow 3－子群的个数 $n_3(N)>1$. 由系列 Sylow 计数定理知

$$n_3(N)\equiv 1(\mathrm{mod}\,3), n_3(N)\big||N:S|,$$

于是 $n_3(N)\geq 4$ 且与 3 互素. 由 $n_3(N)\big||N|$ 与 $|S|\big||N|$ 知 $|N|\geq 36$，于是 $|G:N|\leq 5$. 考虑 G 在 N 的左陪集集合上的作用知 G 同构于 $S_{|G:N|}$ 的某个子群，但是 $|G|=180>5!\geq\left|S_{|G:N|}\right|$，矛盾!

所以 G 的任意两个不同的 Sylow 3－子群的交都是平凡的.

由系列 Sylow 计数定理知 G 的 Sylow 5－子群个数 $n_5(G)$ 满足

$$n_5(G)>1, n_5(G)\big|2^2\cdot 3^2, n_5(G)\equiv 1(\mathrm{mod}\,5),$$

所以 $n_5(G)=6$ 或 36.

如果 $n_5(G)=36$，注意到任意两个不同的 Sylow 5－子群的交都是单位子群，此时 G 的 10 个 Sylow 3－子群与 36 个 Sylow 5－子群至少包含 $10\cdot(9-1)+36\cdot(5-1)+1=225$ 个元素，矛盾!

所以 $n_5(G)=6$，考虑 G 在 6 元集 $\mathrm{Syl}_5(G)$ 上的共轭作用，由 G 单知作用核为单位子群，于是 G 同构于 S_6 的某子群，不妨设 $G\leq S_6$.

如果 G 中有奇置换, 则 $1<\left|G:G\cap A_6\right|=\left|GA_6:A_6\right|\le\left|S_6:A_6\right|=2$, 即 $G\cap A_6$ 是 G 的指数为 2 的子群, 在 G 中正规, 与 G 单矛盾!

所以 G 中仅含偶置换, 但此时 $\left|A_6:G\right|=\left|A_6\right|/\left|G\right|=2$, 从而 G 是 A_6 的正规子群, 这与 A_6 单矛盾!■

习题三

1 设 $S\in\mathrm{Syl}_p(G)$. 证明 $S\cap N\in\mathrm{Syl}_p(N)$. 特别地, 若 N 是 $p-$ 群, 则 $N\le S$.

注记: 由如上习题, 任一正规 $p-$ 子群均含于 $\mathrm{core}_G(S)$, 而 $\mathrm{core}_G(S)$ 是 G 的唯一的极大正规 $p-$ 子群, 记为 $\mathbf{O}_p(G)$.

2 设 G 是有限群, $\varphi:G\to H$ 是满的群同态.

(1) 若 $P\in\mathrm{Syl}_p(G)$, 证明 $\varphi(P)\in\mathrm{Syl}_p(H)$.

(2) 若 $Q\in\mathrm{Syl}_p(H)$, 证明存在 $P\in\mathrm{Syl}_p(G)$ 使得 $Q=\varphi(P)$.

(3) 证明 $n_p(H)\le n_p(G)$.

3 设 H 是有限群 G 的子群, 证明 $n_p(H)\le n_p(G)$.

4 设 H 是有限群 G 的子群, 且 $\mathbf{C}_G(x)\le H,\forall x\in H-\{1\}$. 证明: $\gcd\left(\left|H\right|,\left[G:H\right]\right)=1$.

提示: 选取 $P\in\mathrm{Syl}_p(H)$, 证明 $P\in\mathrm{Syl}_p(G)$.

注记: G 的阶与指数互素的子群称为 G 的 Hall 子群.

5 设设 H 是有限群 G 的子群, $P\in\mathrm{Syl}_p(H)$. 若 $\mathbf{N}_G(P)\le H$, 证明 $P\in\mathrm{Syl}_p(G)$.

6 设有限群 $G>1, P\le\mathrm{Aut}(G)$ 是 $p-$ 子群. 证明存在 G 的非平凡 Sylow $q-$ 子群 Q 使得

$$\sigma(Q)=Q,\forall\sigma\in P.$$

提示: 分别考虑 p 整除与不整除群阶两种情形.

7 设 $\left|G\right|=p^2q^2$, 其中 $p>q$ 均为素数. 若 $\left|G\right|\ne 36$, 证明 G 有正规的 Sylow $p-$ 子群.

8 设 $P\in\mathrm{Syl}_p(G)$. 证明 $\mathbf{N}_G(\mathbf{N}_G(P))=\mathbf{N}_G(P)$.

9 若 $\left|G\right|=pqr$, 其中 p,q,r 均为素数, 证明 G 不是单群.

10 若 $\left|G\right|\le 100$ 是非 Abel 单群, 证明 $\left|G\right|=60$.(可以应用 p^aq^b- 定理)

注记: 确实存在 60 阶单群 A_5.

11 若 G 是 60 阶单群, 证明 G 同构于 S_5 的子群. 若 G_1, G_2 都是 60 阶单群, 证明 $G_1 \cong G_2$.

提示: 证明 G 有指数为 5 的子群. 若 $n_2(G)=5$ 是容易的. 设 $n_2(G)=15$, 证明存在两个 Sylow $2-$ 子群 S 与 T 的交 $D=S\bigcap T$ 是 2 阶群. 考虑 $\mathbf{N}_G(D)$.

12 若 $|G|=280$, 证明 G 不是单群.

13 设素数 p 与 q 满足 $q|p-1$, 构造 pq 阶非 Abel 群如下. 设 P 是素数 p 阶循环群, 令 Q 是 $\mathrm{Aut}(P)$ 的 q 阶自同构. 对 $\forall a\in P, \sigma\in Q$, 规定集合 P 上的置换 $\varphi_{a,\sigma}$ 为:

$$\varphi_{a,\sigma}: x\mapsto (xa)\sigma, \forall x\in P,$$

令 $G=\left\{\varphi_{a,\sigma}\middle| a\in P, \sigma\in Q\right\}$ 是集 P 上对称群的子集合. 证明 G 是 pq 阶非 Abel 群.

14 设 $|G|=p(p+1)$, 其中 p 是素数. 证明 G 或者有 p 阶或者有 $p+1$ 阶正规子群.

提示: 若 $n_p(G)>1$, 取 $x\in G$ 使得 $o(x)\neq 1, p$. 证明 $|\mathbf{C}_G(x)|=p+1$, 然后对元素计数.

15 群 G 的子群 X 称为一个**平凡交集**, **T.I.集**, 若对任一 $g\in G$, 或 $X^g=X$ 或 $X^g\bigcap X=1$. 设 $P\in \mathrm{Syl}_p(G)$ 且 P 是 G 的一个 T.I.集, $H\leq G, Q\in \mathrm{Syl}_p(H)$. 证明 Q 是 H 的一个 T.I.集.

16 设 G 是有限群. 令 $f_n(G)=\left|\left\{x\in G\middle| x^n=1\right\}\right|, n\in\mathbb{N}$. Frobenius 定理表明当 $n|G$ 时 $n|f_n(G)$. 试证明 n 是素数时定理为真.

17 设 $|G|=p^a(kp+1)$, 其中 p 是素数且 $0<k\leq p+1$. 设 $S\in \mathrm{Syl}_p(G)$, 证明 S 是 G 的极大子群或者 $S\lhd G$.

提示: 若 $r\equiv 1\equiv s \pmod p$ 且 $r>1, s>1$, 则 $rs\geq (p+1)^2$.

18 设有限群 P 的阶为 p^2, 其中 p 为素数. 证明 P 是 Abel 群.

19 设有限群 G 的 Sylow 子群均正规.

(1) 若 $P\in \mathrm{Syl}_p(G)$, 证明 $\mathbf{Z}(P)\leq \mathbf{Z}(G)$; (2) 若 $1<N\lhd G$, 证明 $N\bigcap \mathbf{Z}(G)>1$.

注记: 满足习题 5.19 的群称为幂零群. 第八章将定义无限幂零群. 习题(2)在无限情形也成立.

20 设 P 是有限 $p-$ 群, 设 $A\lhd P$ 是 P 的 Abel 正规子群中极大者. 证明 $A=\mathbf{C}_P(A)$.

提示: 令 $C=\mathbf{C}_P(A)$ 且设 $C>A$. 证明 C/A 有一个 p 阶子群 $B/A\lhd P/A$. 再证明 B 是 Abel 群.