# 代数学讲义

## 第二册　群的结构理论

**摘要**　本册共九章。从合成因子、可解群与幂零群出发，进一步构造直积、半直积与分裂扩张；再由集合截面推导交换核扩张的二余循环，证明扩张等价的分类，并计算循环中心扩张、二面体群、四元数群和补子群。第五章从群作用、循环型与中心化子出发，证明交错群单性，研究本原作用及其仿射结构。第六章给出不超过三十一阶及三十六阶群的分类，并处理多个一般阶族、子群与商群、幂映射、自同构和扩张的分裂；十六阶通过交换正规核、作用与进位参数完成去重；奇素数四次幂阶另给出十五类，并处理特征三例外。第七章从约化词构造自由群，证明生成元与关系的泛性质、Tietze 变换、自由积正规形与 Nielsen–Schreier 定理，推导子群秩公式、导出群的无限自由基及剩余有限性。第八章研究 Frattini 子群与 Burnside 基定理、Fitting 自中心化和 Fitting 列，并证明可解有限群的 Hall 与 Schur–Zassenhaus 定理。第九章从线性作用与群代数开始，证明 Maschke 定理及其逆、Schur 引理、等型分解与循环群的谱投影。以完全可约性作为本册终点；特征标、诱导表示及更深的组合群论另设后续专题。

中文讲义　审校版（2026 年 10 月 29 日）

# 目录

**记号与承接** **iv**

**1 正规列与合成因子** **1**
1.1 把一次取商接着做下去 . . . 1
1.2 商群的子群怎样回到原群 . . . 2
1.3 合成列的存在与加细 . . . 4
1.4 两个极大正规子群的交 . . . 5
1.5 Jordan–Hölder 定理 . . . 7
1.6 合成因子的具体计算 . . . 9
1.7 正规子群与商群的因子如何合并 . . . 11
1.8 无限群中存在性为何需要另作判断 . . . 12

**2 交换子与可解群** **14**
2.1 交换子怎样记录乘法次序 . . . 14
2.2 交换子群与交换化 . . . 15
2.3 可解性与导出列 . . . 16
2.4 可解群的合成因子 . . . 18
2.5 具体计算：从商群确定导出子群 . . . 18
2.6 上三角矩阵群的可解性 . . . 20
2.7 文献说明 . . . 22

**3 中心列与幂零群** **23**
3.1 中心的原像与上中心列 . . . 23
3.2 下中心列与满同态像 . . . 24
3.3 有限 $p$ 群的中心与幂零性 . . . 27
3.4 正规化子条件 . . . 27
3.5 有限幂零群与 Sylow 分解 . . . 28
3.6 三阶单位上三角群 . . . 29
3.7 可解与幂零的区别 . . . 30

**4 直积、半直积与群扩张** **31**
4.1 从唯一分解到乘法公式 . . . 31
4.2 外部半直积的构造 . . . 32
4.3 旋转、仿射变换与上三角矩阵 . . . 33
4.4 短正合列与分裂 . . . 35
4.5 交换核、集合截面与二余循环 . . . 36
4.6 截面变化与扩张等价 . . . 38
4.7 循环商的中心扩张：进位与模掉倍数 . . . 39
4.8 非平凡作用：二面体群与四元数群 . . . 41
4.9 补子群的变化与一余循环 . . . 42

**5 置换群与单群** **44**
5.1 作用、轨道与稳定子 . . . 44
5.2 陪集作用与子群的正规核 . . . 45
5.3 不交循环、阶与幂 . . . 46
5.4 符号与三循环生成 . . . 47
5.5 不动点与轨道计数 . . . 48
5.6 共轭类与中心化子的结构 . . . 49
5.7 交错群中共轭类的分裂 . . . 50
5.8 最小支撑与交错群的单性 . . . 52
5.9 对称群的正规子群与导出列 . . . 53

5.10 块、本原作用与极大子群 . . . 54
5.11 换位生成的图与传递性的边界 . . . 55
5.12 正规子群的轨道与仿射结构 . . . 56

**6 低阶群的结构与分类 59**
6.1 分类中的生成元、关系与计数 . . . 59
6.2 素数平方阶：两个模型与完整性 . . . 60
6.3 素数乘积阶：作用参数与同构类型 . . . 61
6.4 八阶交换群：先拆出循环因子 . . . 63
6.5 八阶非交换群：二阶元决定分岔 . . . 63
6.6 十二阶群：非正规 Sylow 子群产生忠实作用 . . . 66
6.7 素数立方阶：中央交换子与幂公式 . . . 69
6.8 立方阶的第一个非交换模型：三阶幺上三角群 . . . 70
6.9 立方阶的第二个非交换模型：循环核的分裂 . . . 70
6.10 奇素数立方阶的完整表 . . . 71
6.11 结构不变量：从分类表回到群本身 . . . 72
6.12 中心商上的交替形式与正规子群 . . . 74
6.13 八阶与十二阶的正规子群、商群和 Sylow 数据 . . . 75
6.14 立方阶模型的全部子群与扩张的两种核 . . . 77
6.15 阶 $2p^2$：二阶作用的特征空间 . . . 80
6.16 阶 $4p$：同一作用像的生成元更换 . . . 81
6.17 阶三倍素数平方的分类 . . . 82
6.18 六倍素数阶：平均二余循环与分裂 . . . 84
6.19 四次幂阶的入口：交换正规子群与进位坐标 . . . 85
6.20 十六阶群：十四个模型的完整分类 . . . 86
6.21 奇素数四次幂阶：十五种模型与特征三例外 . . . 90
6.22 二十四阶：正规三阶核与四点作用的分岔 . . . 94
6.23 三十阶：元素计数与十五阶正规核 . . . 96
6.24 三十六阶：线性作用与非正规九阶 Sylow 分支 . . . 96
6.25 按阶分类的边界与本章结论表 . . . 98

**7 自由群与生成元、关系 100**
7.1 形式字母、词与约化算法 . . . 100
7.2 自由群的构造与泛性质 . . . 101
7.3 循环约化、挠元与中心 . . . 102
7.4 正规闭包与表示式的准确含义 . . . 103
7.5 从正规形证明表示式：二面体群与交换化 . . . 104
7.6 Tietze 变换：更换表示而保持群 . . . 105
7.7 自由积及其交替正规形 . . . 106
7.8 边路径与生成树：只用组合定义 . . . 108
7.9 陪集图与闭路径群 . . . 109
7.10 生成树给出的自由基与 Nielsen–Schreier 定理 . . . 109
7.11 逐字重写公式与有限指数的秩 . . . 111
7.12 一个二指数子群：自由基与实际重写 . . . 111
7.13 二生成元自由群的导出群为何有无限秩 . . . 112
7.14 有限置换模型分离非平凡词 . . . 113
7.15 有限生成、Hopf 性与本章接口 . . . 115

**8 有限群结构工具：Frattini、Fitting 与 Hall 理论 116**
8.1 Frattini 子群与非生成元 . . . 116
8.2 有限 $p$ 群的 Frattini 子群 . . . 117
8.3 生成组计数与自同构的线性化 . . . 118
8.4 Frattini 论证与有限 Frattini 子群的幂零性 . . . 119
8.5 Fitting 子群的构造 . . . 119
8.6 有限可解群中的 Fitting 层 . . . 121
8.7 Fitting 列与可解群的幂零层数 . . . 122
8.8 Hall 子群与素数集分解 . . . 123

8.9 可解群的 Hall 子群存在性 . . . 124
8.10 Schur–Zassenhaus 的可解证明 . . . 126
8.11 条件的边界：Hall 失败与补群不唯一 . . . 126
8.12 本章工具之间的依赖关系 . . . 127

**9 有限群的线性表示与完全可约性 128**
9.1 线性作用、矩阵与表示的等价 . . . 128
9.2 群代数与线性延拓 . . . 129
9.3 不变子空间、商表示与分裂 . . . 130
9.4 Maschke 定理：把普通投影平均成等变投影 . . . 130
9.5 特征条件为何必要：增广映射的障碍 . . . 131
9.6 实数与复数域上的不变内积 . . . 132
9.7 Schur 引理与底域的作用 . . . 133
9.8 不可约分解的重数与典范等型分量 . . . 133
9.9 循环群的谱投影与交换群的不可约表示 . . . 134
9.10 从置换表示中取出一个不可约因子 . . . 135

# 记号与承接

本册承接第一册。前六章使用群与子群、陪集、Lagrange 定理、正规子群、商群，以及循环群的基本性质。第六章还使用第一册群论章已证明的 Sylow 子群存在、共轭与数目定理；有限 $p$ 群的中心及半直积性质在本册第三、四章证明。置换的符号沿用第一册线性代数章的定义；在具体例子中重新列出所用公式。

群的单位元为 $e$，整数加法群的单位元为 $0$。置换与映射均从右向左复合。$C_n$ 表示阶为 $n$ 的循环群；本册取模型 $C_n = \mathbb{Z}/n\mathbb{Z}$，其运算为加法。$S_n$ 表示集合 $\{1, \dots, n\}$ 上的置换群。$H \le G$ 表示子群，$H \trianglelefteq G$ 表示正规子群，允许 $H = G$；严格包含另以 $\subsetneq$ 或 $\supsetneq$ 表示。商群的单位元是分母子群本身。

第七章不预设拓扑学，以词和边路径构造自由群及其子群；第八章的 Hall 与 Schur–Zassenhaus 结论明确限定可解有限群；第九章另使用第一册的有限维线性代数。第四章的二余循环分类限于交换核和给定作用，并不覆盖一般非交换核扩张。

本册定理按章编号，章号从一重新开始。证明中给出的公式与映射采用本册的统一记号；文献说明列出实际参考的讲义节段。

# 1 正规列与合成因子

## 1.1 把一次取商接着做下去

第一册已经构造了商群。若 $N \trianglelefteq G$，投影 $q : G \to G/N$ 将 $N$ 中的元素识别为单位元。商群描述这次识别以后的运算，但 $N$ 内部仍有结构可研究。若再取 $K \trianglelefteq N$，便得到第二个商群 $N/K$。沿着子群列继续这一过程，就能比较群在不同层次上的因子。

**定义 1.1** (次正规列、正规列与加细)**.** 群 $G$ 的有限次正规列是一个子群列

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{e\}, \qquad G_{i+1} \trianglelefteq G_i \quad (0 \le i < r).$$

商群 $G_i/G_{i+1}$ 称为该列的因子。若每个 $G_i$ 都正规于 $G$，称该列为正规列。若每次包含都严格，称该列无重复，其长度为 $r$。平凡群的长度零的列只有一项 $G = \{e\}$，没有因子。

在原列的若干相邻项之间插入子群，保留所有原项，并使得到的列仍为次正规列，称为加细。若插入了至少一个不同于原有各项的子群，称为真加细。

在正规列中，$G_{i+1} \trianglelefteq G$。因而任取 $x \in G_i \subseteq G$，有

$$xG_{i+1}x^{-1} = G_{i+1},$$

所以正规列确实是次正规列。但次正规列中的正规条件只逐层施加，不能据此推出 $G_{i+2} \trianglelefteq G_i$。下面把这一点放在一个可以逐项计算的例子中。

**例 1.2** (正规性不传递)**.** 在 $S_4$ 中令

$$a = (12)(34), \qquad b = (13)(24), \qquad c = (14)(23), \qquad V = \{e, a, b, c\}.$$

每个置换都是两个不相交对换之积，故 $a^2 = b^2 = c^2 = e$。计算 $ab$ 和 $ba$ 在四个字母上的像，得到

| $x$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $ab(x)$ | 4 | 3 | 2 | 1 |
| $ba(x)$ | 4 | 3 | 2 | 1 |

所以$ab = ba = c.$

由结合律，

$$ac = a(ab) = b, \quad ca = (ab)a = b, \quad bc = b(ab) = a, \quad cb = (ab)b = a.$$

这给出完整的乘法表：

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

表内乘积仍在 $V$ 中，且每个元素的逆元仍在 $V$ 中；结合律来自 $S_4$。因此 $V$ 是交换子群。令 $H = \{e, a\}$。对 $v \in V, h \in H$，交换性给出 $vhv^{-1} = h$，故 $H \trianglelefteq V$。

任取 $\sigma \in S_4$。共轭公式为

$$\sigma(ij)\sigma^{-1} = (\sigma(i)\ \sigma(j)).$$

确实，左边把 $\sigma(i)$ 送到 $\sigma(j)$，把 $\sigma(j)$ 送到 $\sigma(i)$，并固定其余字母。因此

$$\sigma(ij)(k\ell)\sigma^{-1} = (\sigma(i)\ \sigma(j))(\sigma(k)\ \sigma(\ell)).$$

当 $i,j,k,\ell$ 是四个不同字母时，右边仍是 $a,b,c$ 中的一个，所以 $\sigma V\sigma^{-1} \subseteq V$。把 $\sigma$ 换成 $\sigma^{-1}$，得到 $\sigma^{-1}V\sigma \subseteq V$，两边再以 $\sigma$ 共轭，便有 $V \subseteq \sigma V\sigma^{-1}$。于是 $V \trianglelefteq S_4$。然而

$$(123)a(123)^{-1} = (23)(14) = c \notin H.$$

这说明 $H \trianglelefteq V \trianglelefteq S_4$，但 $H$ 不正规于 $S_4$。

**命题 1.3** (群阶与因子阶)**.** *若 $G$ 有限，则任意次正规列满足*

$$|G| = \prod_{i=0}^{r-1} |G_i/G_{i+1}|.$$

*若该列无重复，则 $2^r \le |G|$。*

*证明.* Lagrange 定理给出

$$|G_i/G_{i+1}| = [G_i : G_{i+1}] = \frac{|G_i|}{|G_{i+1}|}.$$

当 $r \ge 1$ 时，乘积逐项约去中间的群阶，得到

$$\prod_{i=0}^{r-1} |G_i/G_{i+1}| = \frac{|G_0|}{|G_1|}\frac{|G_1|}{|G_2|}\cdots\frac{|G_{r-1}|}{|G_r|} = \frac{|G|}{1} = |G|.$$

当 $r = 0$ 时，空乘积约定为 1，而此时 $G = \{e\}$，等式仍成立。若包含严格，各因子都有至少两个元素，故

$$|G| = \prod_{i=0}^{r-1} |G_i/G_{i+1}| \ge \prod_{i=0}^{r-1} 2 = 2^r.$$

□

## 1.2 商群的子群怎样回到原群

要判断一个因子能否继续分解，需要在商群的正规子群和原群的中间子群之间往返。为此，先把子群对应中的映射和逆映射写清楚。

**定理 1.4** (子群对应)**.** *设 $N \trianglelefteq G$，$q : G \to G/N$ 为投影 $q(g) = gN$。映射*

$$H \longmapsto H/N, \qquad U \longmapsto q^{-1}(U)$$

*在包含 $N$ 的子群 $H \le G$ 与子群 $U \le G/N$ 之间互逆，并保持包含关系。这里把 $H/N$ 看作 $G/N$ 中的子群。并且*

$$H \trianglelefteq G \quad\Longleftrightarrow\quad H/N \trianglelefteq G/N.$$

*若这两个正规条件成立，则映射*

$$\Phi : (G/N)/(H/N) \longrightarrow G/H, \qquad (gN)(H/N) \longmapsto gH$$

*是群同构。*

证明. 先检查对应的两个方向。若 $N \subseteq H \leq G$，则对 $h \in H$ 有 $hNh^{-1} = N$，故 $N \trianglelefteq H$。集合

$$H/N = \{hN : h \in H\}$$

是 $G/N$ 的子集，含单位元 $N$；对 $h_1, h_2 \in H$，

$$(h_1N)(h_2N)^{-1} = (h_1h_2^{-1})N \in H/N.$$

所以它是子群，且运算就是 $G/N$ 的运算限制。

若 $U \leq G/N$，则 $e \in q^{-1}(U)$，因为 $q(e) = N$ 是 $U$ 的单位元。对 $x, y \in q^{-1}(U)$，

$$q(xy^{-1}) = q(x)q(y)^{-1} \in U,$$

故 $xy^{-1} \in q^{-1}(U)$，这证明 $q^{-1}(U) \leq G$。又因 $n \in N$ 时 $q(n) = N \in U$，该子群包含 $N$。

接着检查互逆。对 $x \in G$，

$$\begin{aligned} x \in q^{-1}(H/N) &\iff xN = hN \text{ 对某个} h \in H \\ &\iff h^{-1}x \in N \text{ 对某个} h \in H \\ &\iff x \in H. \end{aligned}$$

最后一个等价的正向使用 $x \in hN \subseteq H$；反向可取 $h = x$。因此 $q^{-1}(H/N) = H$。若 $u \in U$，投影的满射性给出 $g \in G$ 使 $q(g) = u$，此时 $g \in q^{-1}(U)$，故 $u \in q(q^{-1}(U))$。另一个包含由逆像定义得到，于是

$$q(q^{-1}(U)) = U.$$

若 $H_1 \subseteq H_2$，则每个 $hN \in H_1/N$ 也属于 $H_2/N$。若 $U_1 \subseteq U_2$，则 $q(x) \in U_1$ 蕴含 $q(x) \in U_2$。这证明两个方向都保持包含。互逆性还说明严格包含对应于严格包含。

现在检查正规性。若 $H \trianglelefteq G$，则任取 $g \in G, h \in H$，

$$(gN)(hN)(gN)^{-1} = (ghg^{-1})N \in H/N.$$

故 $(gN)(H/N)(gN)^{-1} \subseteq H/N$。将 $g$ 换成 $g^{-1}$ 后共轭回来，得到相反包含，因而 $H/N \trianglelefteq G/N$。

反过来，若 $H/N \trianglelefteq G/N$，则同一公式说明

$$q(ghg^{-1}) \in H/N, \qquad ghg^{-1} \in q^{-1}(H/N) = H.$$

于是 $gHg^{-1} \subseteq H$。对 $g^{-1}$ 已得 $g^{-1}Hg \subseteq H$，故

$$H = g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}.$$

两个包含给出 $H \trianglelefteq G$。

最后证明所写的 $\Phi$ 是同构。首先，$gN = g'N$ 时 $g'^{-1}g \in N \subseteq H$，所以 $gH = g'H$。若改变外层陪集的代表，令

$$(gN)(H/N) = (g'N)(H/N),$$

则 $(g'^{-1}g)N \in H/N$，由刚证明的逆像等式可得 $g'^{-1}g \in H$，因此仍有 $gH = g'H$。这同时检查了两层代表的选择。

对 $g, k \in G$，

$$\begin{aligned} \Phi\big(((gN)(H/N))((kN)(H/N))\big) &= \Phi((gkN)(H/N)) \\ &= (gk)H = (gH)(kH). \end{aligned}$$

这等于两个像的乘积，故 $\Phi$ 是同态。每个 $gH$ 都是 $(gN)(H/N)$ 的像，所以满射。若两个像相同，则

$$gH = kH \implies k^{-1}g \in H \implies (k^{-1}g)N \in H/N$$

进而 $(gN)(H/N) = (kN)(H/N)$，所以单射。同态、单射、满射均已证明。 □

**推论 1.5** (单因子与极大正规子群)**.** *设 $N \trianglelefteq G$ 且 $N \neq G$。商群 $G/N$ 没有非平凡真正规子群，当且仅当不存在满足*

$$N \subsetneq K \subsetneq G, \qquad K \trianglelefteq G$$

*的子群。满足后一条件的 $N$ 称为 $G$ 的极大真正规子群。*

*证明.* 由定理 1.4，中间正规子群 $K$ 与商群的正规子群 $K/N$ 对应。因为对应互逆且保持严格包含，

$$N \subsetneq K \subsetneq G \quad \Longleftrightarrow \quad \{N\} \subsetneq K/N \subsetneq G/N.$$

故两边存在这类子群的条件等价，同时不存在的条件也等价。 □

“极大” 按包含关系理解：它只排除严格位于 $N$ 与 $G$ 之间的真正规子群，并不要求所有真正规子群都包含于 $N$。不同的极大真正规子群可以同时存在。

## 1.3 合成列的存在与加细

**定义 1.6** (单群与合成列)**.** 非平凡群 $S$ 称为单群，若它的正规子群只有 $\{e\}$ 与 $S$。各因子都是非平凡单群的有限次正规列称为合成列，相应因子称为合成因子。平凡群的长度零的列也称为合成列。

**引理 1.7** (素数阶群)**.** *若群 $P$ 的阶为素数 $p$，则 $P \cong C_p$，且 $P$ 是单群。*

*证明.* 取 $x \neq e$。由 Lagrange 定理，$|\langle x\rangle|$ 整除 $p$，又不等于 1，所以等于 $p$。因此 $\langle x\rangle = P$。定义

$$\alpha : \mathbb{Z}/p\mathbb{Z} \longrightarrow P, \qquad k + p\mathbb{Z} \longmapsto x^k.$$

若 $k - \ell = pt$，则 $x^k = x^\ell (x^p)^t = x^\ell$，故良定义；又有 $x^{k+\ell} = x^k x^\ell$，故保持运算。由 $x$ 生成 $P$ 可知满射。若 $x^k = x^\ell$，将 $k - \ell$ 除以 $p$ 写成 $pt + r$，其中 $0 \le r < p$，则 $x^r = e$。$x$ 的阶为 $p$，故 $r = 0$，得到 $k + p\mathbb{Z} = \ell + p\mathbb{Z}$，所以单射。

任意子群 $L \le P$ 的阶也整除 $p$，只能为 1 或 $p$，从而 $L = \{e\}$ 或 $L = P$。正规子群是子群，故 $P$ 单。 □

**命题 1.8** (合成列的极大性)**.** *无重复次正规列是合成列，当且仅当它没有真加细。这也等价于每个 $G_{i+1}$ 都是 $G_i$ 的极大真正规子群。*

*证明.* 在 $G_i \supsetneq G_{i+1}$ 之间只插入一个子群 $K$，需要满足

$$G_{i+1} \trianglelefteq K \trianglelefteq G_i, \qquad G_{i+1} \subsetneq K \subsetneq G_i.$$

因为原已有 $G_{i+1} \trianglelefteq G_i$，条件 $G_{i+1} \trianglelefteq K$ 对任何这样的中间子群都自动成立。推论 1.5 于是说明：能插入这样的 $K$，当且仅当 $G_i/G_{i+1}$ 不是单群。

还须排除一次插入多个子群的可能。若在这两个原项间有真加细

$$G_i \supsetneq K_1 \supsetneq \cdots \supsetneq K_t \supsetneq G_{i+1},$$

则 $K_1 \trianglelefteq G_i$，而 $G_{i+1} \trianglelefteq K_1$ 仍由原列的正规性限制得到。因此单独插入 $K_1$ 已可构成真加细。反之，插入一个子群就是一种真加细。逐个相邻区间应用这一结论，得到命题的三个条件等价。 □

**命题 1.9** (有限群合成列的存在)**.** *每个有限群都有合成列；有限群的任意无重复次正规列都可以加细成合成列。*

*证明.* 先对 $|G|$ 作强归纳，证明存在性。$|G| = 1$ 时使用长度零的列。设 $|G| > 1$，并已对阶小于 $|G|$ 的群证明结论。$G$ 的真正规子群集合含 $\{e\}$，非空；又因为 $G$ 有限，其子集只有有限多个，故可在真正规子群中选取阶最大的一个 $M$。

若有 $M \subsetneq K \subsetneq G$ 且 $K \trianglelefteq G$，则 $|M| < |K|$，与选择矛盾。因此 $M$ 是极大真正规子群，由推论 1.5，$G/M$ 单。又有 $|M| < |G|$，归纳假设给出

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_s = \{e\}$$

的一条合成列。在前面接上 $G$ 后，新的第一个因子是单群 $G/M$，其余因子就是原列因子，故得到 $G$ 的合成列。

再证明加细结论。若某个相邻因子不是单群，命题 1.8 给出一个可以插入的中间子群。每次插入使无重复列的长度增加 1，而命题 1.3 给出统一界 $2^r \le |G|$。所以不能无限插入。终止时每个因子都是单群，所得无重复列是合成列，并保留原列的所有不同子群。 □

若初始列含有重复项，可以先删除重复项，再应用命题加细。若坚持在列中保留同一子群的多次出现，则那些平凡因子仍会存在，按定义不能称为合成列。

## 1.4 两个极大正规子群的交

比较两条合成列时，第一步可能已经选了不同的极大真正规子群。以下引理给出两种选择之间的联系。

**引理 1.10.** *设 $M, N$ 是群 $G$ 的两个不同的极大真正规子群，令 $D = M \cap N$。则 $D \trianglelefteq G$，并且*

$$MN = NM = G, \qquad M/D \cong G/N, \qquad N/D \cong G/M.$$

*特别地，$D$ 在 $M, N$ 中都是极大真正规子群。本引理不要求 $G$ 有限。*

*证明.* 若 $M \subseteq N$，则由 $N \trianglelefteq G$、$N \neq G$ 及 $M$ 的极大性可得 $M = N$，矛盾。若 $N \subseteq M$，则由 $M \trianglelefteq G$、$M \neq G$ 及 $N$ 的极大性又得 $N = M$，仍矛盾。故存在

$$m_0 \in M \setminus N, \qquad n_0 \in N \setminus M.$$

因而 $D \subsetneq M$ 且 $D \subsetneq N$。对 $g \in G$，

$$gDg^{-1} = g(M \cap N)g^{-1} = (gMg^{-1}) \cap (gNg^{-1}) = M \cap N = D.$$

中间的集合等式来自共轭映射的双射性；因此 $D \trianglelefteq G$，也就正规于 $M, N$。

记 $MN=\{mn : m\in M, n\in N\}$。它含 $e$，而

$$(m_1n_1)(m_2n_2)=m_1(n_1m_2n_1^{-1})(n_1n_2)\in MN,$$
$$(mn)^{-1}=n^{-1}m^{-1}=(n^{-1}m^{-1}n)n^{-1}\in MN.$$

这里两处都用了 $M\trianglelefteq G$。因此 $MN$ 是子群。又对 $g\in G$，

$$g(mn)g^{-1}=(gmg^{-1})(gng^{-1})\in MN,$$

所以 $g(MN)g^{-1}\subseteq MN$；将 $g$ 换成 $g^{-1}$ 并共轭回来即得反向包含。因此 $MN\trianglelefteq G$。由于 $n_0\in MN\setminus M$，它严格包含 $M$；$M$ 的极大性给出 $MN=G$。此外

$$mn=n(n^{-1}mn)\in NM,\qquad nm=m(m^{-1}nm)\in MN,$$

故 $MN=NM$。

现在直接构造两个同构。定义

$$\alpha : M/D\longrightarrow G/N,\quad mD\longmapsto mN.$$

若 $mD=m'D$，则 $m'^{-1}m\in D\subseteq N$，所以 $mN=m'N$，故良定义。对 $m_1,m_2\in M$，

$$\alpha((m_1D)(m_2D))=(m_1m_2)N=(m_1N)(m_2N)=\alpha(m_1D)\alpha(m_2D).$$

若 $\alpha(mD)=\alpha(m'D)$，则 $m'^{-1}m\in N$，而此元素又在 $M$ 中，故属于 $D$，得到 $mD=m'D$。所以 $\alpha$ 单射。任取 $gN\in G/N$，由 $MN=G$ 可写 $g=mn$，其中 $m\in M, n\in N$，于是 $gN=mN=\alpha(mD)$，故满射。

第二个映射为

$$\beta : N/D\longrightarrow G/M,\quad nD\longmapsto nM.$$

若 $nD=n'D$，则 $n'^{-1}n\in D\subseteq M$，所以 $nM=n'M$，映射良定义；且

$$\beta((n_1D)(n_2D))=(n_1n_2)M=(n_1M)(n_2M)=\beta(n_1D)\beta(n_2D).$$

若 $nM=n'M$，则 $n'^{-1}n\in N\cap M=D$，得到 $nD=n'D$，故单射。由 $NM=G$，每个 $g$ 可写成 $nm$，于是 $gM=nM=\beta(nD)$，故满射。

$M,N$ 的极大性使 $G/M, G/N$ 都单，以上同构使 $M/D, N/D$ 都单。再由推论 1.5 分别在群 $M,N$ 内应用，$D$ 在两者中都是极大真正规子群。 □

图 1.1 的每条线段表示端点子群之间的包含关系，较大的子群画在上方；线旁写的是较大群除以较小群所得的因子。图中的同构交叉配对为

$$G/M\cong N/D,\qquad G/N\cong M/D.$$

它们比较的是商群，图本身并不声称 $M$ 与 $N$ 同构。

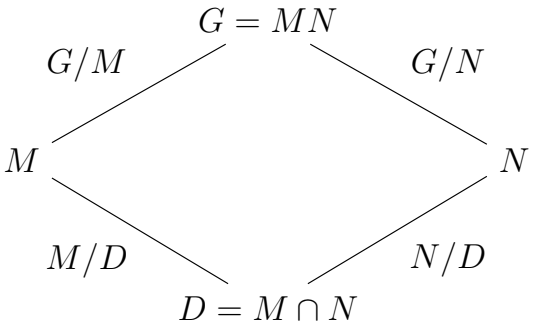



图 1.1: 极大正规子群的交

## 1.5　Jordan–Hölder 定理

先约定比较因子的记法。用 $[S]$ 表示群 $S$ 的同构类型：$[S] = [T]$ 的意思是 $S \cong T$。本章只比较有限条合成列中出现的群，无须把所有群的同构类型组成一个集合。多重集允许同一个类型出现多次；例如

$$\{[C_2], [C_2], [C_3]\}$$

中 $[C_2]$ 的重数为 2，$[C_3]$ 的重数为 1。两个多重集相等，是指每个类型的重数都相等。用 $\sqcup$ 表示把重数相加的合并，而不是去掉重复项的普通集合并。

若 $\mathcal{C}$ 是合成列 $G = G_0 \supsetneq \cdots \supsetneq G_r = \{e\}$，记

$$\mathcal{F}(\mathcal{C}) = \{[G_0/G_1], \ldots, [G_{r-1}/G_r]\}.$$

这是一个多重集，所含项的总数（计重数）为 $r$。

**定理 1.11** (Jordan–Hölder)**.** *有限群 $G$ 的任意两条合成列*

$$\mathcal{C}: \quad G = G_0 \supsetneq \cdots \supsetneq G_r = \{e\}, \qquad \mathcal{E}: \quad G = H_0 \supsetneq \cdots \supsetneq H_s = \{e\}$$

*满足 $\mathcal{F}(\mathcal{C}) = \mathcal{F}(\mathcal{E})$。因此 $r = s$；若 $r > 0$，还存在 $\{0, \ldots, r-1\}$ 的一个排列 $\pi$，使*

$$G_i/G_{i+1} \cong H_{\pi(i)}/H_{\pi(i)+1} \qquad (0 \le i < r).$$

*证明.* 对 $|G|$ 作强归纳。若 $|G| = 1$，无重复列只能是长度零的列，两边的因子多重集均为空。

设 $|G| > 1$，并假设结论对所有阶小于 $|G|$ 的群成立。令

$$M = G_1, \qquad N = H_1.$$

合成列的第一个因子 $G/M$ 与 $G/N$ 都单，故 $M, N$ 都是 $G$ 的极大真正规子群。把两列去掉第一项 $G$ 后分别记为 $\mathcal{C}_M, \mathcal{E}_N$；它们是 $M, N$ 的合成列。

若 $M = N$，则 $|M| < |G|$，归纳假设给出

$$\mathcal{F}(\mathcal{C}_M) = \mathcal{F}(\mathcal{E}_N).$$

因此

$$\begin{aligned} \mathcal{F}(\mathcal{C}) &= \{[G/M]\} \sqcup \mathcal{F}(\mathcal{C}_M) \\ &= \{[G/N]\} \sqcup \mathcal{F}(\mathcal{E}_N) = \mathcal{F}(\mathcal{E}). \end{aligned}$$

若 $M \neq N$，令 $D = M \cap N$。$D$ 有限，由命题 1.9 选定它的一条合成列

$$\mathcal{D}: \quad D = D_0 \supsetneq D_1 \supsetneq \cdots \supsetneq D_t = \{e\}.$$

$D = \{e\}$ 时允许 $t = 0$。引理 1.10 说明 $D$ 是 $M, N$ 中的极大真正规子群，故

$$\mathcal{C}'_M: \quad M \supsetneq D_0 \supsetneq \cdots \supsetneq D_t, \qquad \mathcal{E}'_N: \quad N \supsetneq D_0 \supsetneq \cdots \supsetneq D_t$$

分别是 $M, N$ 的合成列。由于 $|M|, |N| < |G|$，可分别比较

$$\mathcal{F}(\mathcal{C}_M) = \mathcal{F}(\mathcal{C}'_M) = \{[M/D]\} \sqcup \mathcal{F}(\mathcal{D}),$$

以及

$$\mathcal{F}(\mathcal{E}_N) = \mathcal{F}(\mathcal{E}'_N) = \{[N/D]\} \sqcup \mathcal{F}(\mathcal{D}).$$

于是

$$\begin{aligned}\mathcal{F}(\mathcal{C}) &= \{[G/M], [M/D]\} \sqcup \mathcal{F}(\mathcal{D}) \\ &= \{[N/D], [G/N]\} \sqcup \mathcal{F}(\mathcal{D}) \\ &= \{[G/N], [N/D]\} \sqcup \mathcal{F}(\mathcal{D}) \\ &= \mathcal{F}(\mathcal{E}).\end{aligned}$$

第二个等号使用引理中的两个同构，第三个等号只改变项的次序。这完成归纳。

最后从多重集相等推出定理所述的重排。两边项的总数相等，故 $r = s$。对每个出现的类型 $[S]$，把左列中该类型的指标按大小列为 $i_1, \ldots, i_u$，把右列中该类型的指标按大小列为 $j_1, \ldots, j_u$，令 $\pi(i_k) = j_k$。重数相等保证两列指标一样长；不同类型的指标集合互不相交，且它们并起来覆盖所有指标。因此这些对应合成一个排列，并使对应商群同构。 □

由此，有限群的合成因子多重集可以记为 $\mathcal{F}(G)$；合成列的长度记为 $\ell(G)$。这两个记号都与所选合成列无关，且 $\mathcal{F}(\{e\})$ 为空、$\ell(\{e\}) = 0$。

**命题 1.12** (同构保持合成因子)**.** *若有限群 $G, H$ 之间有同构 $f: G \to H$，则*

$$\mathcal{F}(G) = \mathcal{F}(H), \qquad \ell(G) = \ell(H).$$

*证明.* 取 $G$ 的合成列 $G = G_0 \supsetneq \cdots \supsetneq G_r = \{e_G\}$，令 $H_i = f(G_i)$。像包含单位元，并对乘积与逆元封闭，故是子群。$f$ 的双射性保证

$$H = H_0 \supsetneq \cdots \supsetneq H_r = \{e_H\}.$$

对 $x \in G_i, y \in G_{i+1}$，

$$f(x)f(y)f(x)^{-1} = f(xyx^{-1}) \in H_{i+1}.$$

每个 $H_i$ 的元素都可写成 $f(x)$；再以 $x^{-1}$ 代入得到反向包含，故 $H_{i+1} \trianglelefteq H_i$。定义

$$f_i: G_i/G_{i+1} \longrightarrow H_i/H_{i+1}, \qquad xG_{i+1} \longmapsto f(x)H_{i+1}.$$

若 $xG_{i+1} = yG_{i+1}$，则 $y^{-1}x \in G_{i+1}$，故 $f(y)^{-1}f(x) \in H_{i+1}$，两个像相同，所以良定义。且

$$f_i((xG_{i+1})(yG_{i+1})) = f(xy)H_{i+1} = (f(x)H_{i+1})(f(y)H_{i+1}).$$

每个 $h \in H_i$ 都是某个 $x \in G_i$ 的像，故 $f_i$ 满射。若 $f(x)H_{i+1} = f(y)H_{i+1}$，则 $f(y^{-1}x) \in f(G_{i+1})$；$f$ 单射，因而 $y^{-1}x \in G_{i+1}$，证明 $f_i$ 单射。

同构保持单群性：若 $\gamma: S \to T$ 是同构且 $L \trianglelefteq T$，则 $\gamma^{-1}(L) \trianglelefteq S$，因为

$$\gamma(sus^{-1}) = \gamma(s)\gamma(u)\gamma(s)^{-1} \in L \quad (s \in S,\ u \in \gamma^{-1}(L)),$$

反向包含由 $s^{-1}$ 得到。若 $S$ 单，这个逆像只能为 $\{e_S\}$ 或 $S$；用 $\gamma$ 的双射性，$L$ 只能为 $\{e_T\}$ 或 $T$，且 $T$ 非平凡。因此每个 $H_i/H_{i+1}$ 都单，所构造的列也是合成列。其因子逐个与 $G$ 的所选列同构，长度也相同，再用定理 1.11 即得结论。 □

## 1.6　合成因子的具体计算

**例 1.13** (循环群中的逐步取商)**.** 设 $n \geq 2$，取一个素因子分解

$$n = p_1 p_2 \cdots p_r.$$

允许素数重复。令 $C_n = \langle x \rangle$，并定义

$$d_0 = 1, \qquad d_i = p_1 \cdots p_i \ (1 \leq i \leq r), \qquad G_i = \langle x^{d_i} \rangle.$$

此处以乘法记号写循环群，只是将模型 $\mathbb{Z}/n\mathbb{Z}$ 中的 $k + n\mathbb{Z}$ 写成 $x^k$。因为 $d_i \mid n$，整数 $k > 0$ 满足 $(x^{d_i})^k = e$ 当且仅当 $n \mid d_i k$，也就是 $n/d_i \mid k$，所以

$$|G_i| = n/d_i.$$

又有 $x^{d_{i+1}} = (x^{d_i})^{p_{i+1}}$，故 $G_{i+1} \subseteq G_i$。循环群交换，所以这些子群都正规。两阶相除得到

$$|G_i/G_{i+1}| = \frac{n/d_i}{n/d_{i+1}} = p_{i+1}.$$

由引理 1.7，这些因子都是单群，因而

$$C_n = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_r = \{e\}$$

为合成列，其因子依次是 $C_{p_1}, \ldots, C_{p_r}$。

例如在 $C_{12} = \langle x \rangle$ 中，

$$C_{12} \supsetneq \langle x^2 \rangle \supsetneq \langle x^4 \rangle \supsetneq \{e\}$$

的各项阶为 $12, 6, 3, 1$，因子依次为 $C_2, C_2, C_3$；而

$$C_{12} \supsetneq \langle x^3 \rangle \supsetneq \langle x^6 \rangle \supsetneq \{e\}$$

的各项阶为 $12, 4, 2, 1$，因子依次为 $C_3, C_2, C_2$。两种分解次序不同，类型与重数相同。

**例 1.14** ($S_4$ 的两条合成列)**.** 先明确 $A_4$ 的定义。沿用第一册线性代数章 “排列符号与行列式” 的记号，

$$\operatorname{sgn}(\sigma) = (-1)^{N(\sigma)}, \qquad N(\sigma) = \#\{(i,j) : 1 \leq i < j \leq 4,\ \sigma(i) > \sigma(j)\}.$$

第一册 “排列符号的乘法性” 已证明

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau), \qquad \operatorname{sgn}((ij)) = -1.$$

因此 $\operatorname{sgn}: S_4 \to \{1,-1\}$ 是满同态。定义

$$A_4 = \ker(\operatorname{sgn}) = \{\sigma \in S_4 : \operatorname{sgn}(\sigma) = 1\}.$$

它是子群，因为 $\operatorname{sgn}(\sigma\tau^{-1}) = 1$ 对 $\sigma, \tau \in A_4$ 成立。又对 $g \in S_4, h \in A_4$，

$$\operatorname{sgn}(ghg^{-1}) = \operatorname{sgn}(g) \cdot 1 \cdot \operatorname{sgn}(g)^{-1} = 1,$$

故 $gA_4g^{-1} \subseteq A_4$；用 $g^{-1}$ 再得反向包含，所以 $A_4 \trianglelefteq S_4$。

设 $t = (12)$。乘以 $t$ 把符号 1 的置换双射到符号 $-1$ 的置换，其逆仍为乘以 $t$。$S_4$ 的元素数为 $4 \cdot 3 \cdot 2 \cdot 1 = 24$，故 $|A_4| = 12$。

例 1.2 中的 $a, b, c$ 都是两个对换之积，所以符号为 $(-1)^2 = 1$，从而 $V \subseteq A_4$。由 $V \trianglelefteq S_4$ 可得 $V \trianglelefteq A_4$。又因 $V$ 交换，$\langle a\rangle \trianglelefteq V$。所以

$$S_4 \supsetneq A_4 \supsetneq V \supsetneq \langle a\rangle \supsetneq \{e\}$$

是一条次正规列；各项阶为 $24, 12, 4, 2, 1$，因子阶依次为

$$2, \quad 3, \quad 2, \quad 2.$$

引理 1.7 说明每个因子均为单群，且依次同构于 $C_2, C_3, C_2, C_2$。因此它是合成列。

这些同构也可以在本例中直接看出。第一因子的同构为

$$S_4/A_4 \longrightarrow C_2, \qquad \sigma A_4 \longmapsto \begin{cases} 0 + 2\mathbb{Z}, & \operatorname{sgn}(\sigma) = 1, \\ 1 + 2\mathbb{Z}, & \operatorname{sgn}(\sigma) = -1. \end{cases}$$

同一陪集的两个代表之比在 $A_4$ 中，因而符号相同，故良定义；符号相乘对应模 2 相加，故保持运算。两个符号都出现，且符号相同的代表之比在 $A_4$，分别给出满射与单射。

令 $u = (123)$。由 $u = (13)(12)$ 可知 $u \in A_4$。$u$ 与 $u^2$ 都不在 $V$ 中，因为它们是 3-循环。因此 $V, uV, u^2V$ 是三个不同陪集：若 $uV = u^2V$，则 $u \in V$，矛盾。商群恰有三个元素，故它们列出了全部陪集；$u^3 = e$ 给出同构

$$C_3 \longrightarrow A_4/V, \qquad k + 3\mathbb{Z} \longmapsto u^kV.$$

代表相差 3 的倍数时像不变，指数相加给出乘法相容，而三个剩余类的像两两不同并遍历所有陪集，故该映射良定义且为双射同态。

$V/\langle a\rangle$ 的两个陪集为 $\langle a\rangle = \{e, a\}$ 和 $b\langle a\rangle = \{b, c\}$。映射

$$C_2 \longrightarrow V/\langle a\rangle, \qquad k + 2\mathbb{Z} \longmapsto b^k\langle a\rangle$$

由 $b^2 = e$ 保证良定义并保持运算；两个剩余类的像不同且覆盖商群，故为同构。最后的映射

$$C_2 \longrightarrow \langle a\rangle/\{e\}, \qquad k + 2\mathbb{Z} \longmapsto a^k\{e\}$$

由 $a^2 = e$ 保证良定义和乘法相容，由 $a \neq e$ 及 $\langle a\rangle = \{e, a\}$ 保证双射。

若把 $\langle a\rangle$ 换成 $\langle b\rangle$，仍有 $\langle b\rangle \trianglelefteq V$，且各项的阶不变，因此得到另一条合成列

$$S_4 \supsetneq A_4 \supsetneq V \supsetneq \langle b\rangle \supsetneq \{e\}.$$

$\langle a\rangle \neq \langle b\rangle$，因为 $a \neq b$，而两子群的唯一非单位元分别为 $a, b$。两条合成列都不是本章定义的正规列：例 1.2 已证明 $\langle a\rangle$ 不正规于 $S_4$；对另一条列，

$$(123)b(123)^{-1} = (21)(34) = a \notin \langle b\rangle.$$

这也具体说明，合成列所要求的是逐层正规。

**例 1.15** (相同合成因子不能恢复群)**.** 从例 1.14 的列中去掉 $S_4$，得到 $A_4$ 的合成列，因子多重集为

$$\mathcal{F}(A_4) = \{[C_3], [C_2], [C_2]\}.$$

例 1.13 给出

$$\mathcal{F}(C_{12}) = \{[C_2], [C_2], [C_3]\}.$$

然而两群不同构。$C_{12}$ 交换；在 $A_4$ 内取 $u = (123)$ 与 $v = (124)$，两者都是两个对换之积，所以属于 $A_4$，而

$$(uv)(1) = u(2) = 3, \qquad (vu)(1) = v(2) = 4.$$

故 $uv \neq vu$，$A_4$ 不交换。若存在同构 $f : C_{12} \to A_4$，则对任意 $y = f(s), z = f(t)$，

$$yz = f(st) = f(ts) = zy,$$

会迫使 $A_4$ 交换，产生矛盾。因此合成因子给出了群的不变量，但没有给出群的完全分类。

## 1.7 正规子群与商群的因子如何合并

Jordan–Hölder 定理允许先选一条便于计算的合成列。若已知一个正规子群 $N$，就可以分别处理 $N$ 与 $G/N$，再把两部分合并。

**定理 1.16** (合成因子与长度的可加性)**.** *设 $G$ 为有限群，$N \trianglelefteq G$。则*

$$\mathcal{F}(G) = \mathcal{F}(N) \sqcup \mathcal{F}(G/N), \qquad \ell(G) = \ell(N) + \ell(G/N).$$

*证明.* 若 $N = \{e\}$，映射 $g \mapsto g\{e\}$ 是同构：它保持乘法，每个陪集恰含一个元素，故双射。于是 $\mathcal{F}(G/N) = \mathcal{F}(G)$，而 $\mathcal{F}(N)$ 为空。若 $N = G$，则 $G/N$ 平凡，结论也成立。以下设 $\{e\} \subsetneq N \subsetneq G$。

取两条合成列

$$N = N_0 \supsetneq \cdots \supsetneq N_t = \{e\}, \qquad G/N = U_0 \supsetneq \cdots \supsetneq U_s = \{N\}.$$

令 $q : G \to G/N$ 为投影，$K_i = q^{-1}(U_i)$。子群对应给出

$$G = K_0 \supsetneq K_1 \supsetneq \cdots \supsetneq K_s = N.$$

对 $k \in K_i, x \in K_{i+1}$，

$$q(kxk^{-1}) = q(k)q(x)q(k)^{-1} \in U_{i+1},$$

因为 $U_{i+1} \trianglelefteq U_i$。因此 $kK_{i+1}k^{-1} \subseteq K_{i+1}$，再以 $k^{-1}$ 代入并共轭回来得到等号，故 $K_{i+1} \trianglelefteq K_i$。

对每个 $0 \le i < s$，定义

$$\psi_i : K_i/K_{i+1} \longrightarrow U_i/U_{i+1}, \qquad kK_{i+1} \longmapsto q(k)U_{i+1}.$$

若 $kK_{i+1} = k'K_{i+1}$，则 $k'^{-1}k \in K_{i+1} = q^{-1}(U_{i+1})$，所以 $q(k')^{-1}q(k) \in U_{i+1}$，两个像相同，故良定义。对 $k, h \in K_i$，

$$\begin{aligned}\psi_i((kK_{i+1})(hK_{i+1})) &= q(kh)U_{i+1} \\ &= (q(k)U_{i+1})(q(h)U_{i+1}),\end{aligned}$$

这证明保持运算。若像相同，则 $q(k'^{-1}k)\in U_{i+1}$，故 $k'^{-1}k\in K_{i+1}$，原陪集相同，得到单射。每个 $u\in U_i$ 可写为 $q(k)$，此时 $k\in K_i$，所以 $uU_{i+1}=\psi_i(kK_{i+1})$，得到满射。由此

$$K_i/K_{i+1}\cong U_i/U_{i+1}.$$

右侧是非平凡单群，左侧也是非平凡单群。

把提升得到的列与 $N$ 的列接在一起，得到

$$G=K_0\supsetneq\cdots\supsetneq K_s=N_0\supsetneq N_1\supsetneq\cdots\supsetneq N_t=\{e\}.$$

这是一条长度 $s+t$ 的合成列：上半段的因子逐个同构于 $G/N$ 所选列的因子，下半段就是 $N$ 所选列的因子。故这条列的因子多重集为 $\mathcal{F}(G/N)\sqcup\mathcal{F}(N)$。由定理 1.11，它等于 $\mathcal{F}(G)$；计数便得到长度等式。 □

**推论 1.17** (直积的合成因子)**.** *若 $A,B$ 为有限群，则*

$$\mathcal{F}(A\times B)=\mathcal{F}(A)\sqcup\mathcal{F}(B),\qquad \ell(A\times B)=\ell(A)+\ell(B).$$

*证明.* 令 $N=A\times\{e_B\}$。对 $(a,b)\in A\times B$ 和 $(x,e_B)\in N$，

$$(a,b)(x,e_B)(a,b)^{-1}=(axa^{-1},e_B)\in N.$$

再用 $(a,b)^{-1}$ 得到反向包含，所以 $N\trianglelefteq A\times B$。映射 $a\mapsto(a,e_B)$ 保持乘法，逆映射为 $(a,e_B)\mapsto a$，故 $N\cong A$。

商群的同构为

$$\rho:(A\times B)/N\longrightarrow B,\qquad (a,b)N\longmapsto b.$$

若 $(a,b)N=(a',b')N$，则 $(a'^{-1}a,b'^{-1}b)\in N$，故 $b=b'$，得到良定义；且

$$\rho(((a,b)N)((a',b')N))=bb'=\rho((a,b)N)\rho((a',b')N).$$

每个 $b$ 都是 $(e_A,b)N$ 的像，故满射。若两个像相等，则 $b=b'$，所以 $(a'^{-1}a,b'^{-1}b)=(a'^{-1}a,e_B)\in N$，原陪集相同，故单射。将 $N\cong A$ 与 $(A\times B)/N\cong B$ 代入定理 1.16 即得两式。 □

**例 1.18** (相同的长度来自不同的群)**.** $C_4$ 的列 $C_4\supsetneq\langle x^2\rangle\supsetneq\{e\}$ 有两个 $C_2$ 因子。直积公式给出 $C_2\times C_2$ 也有两个 $C_2$ 因子。两群均交换，但仍不同构：$C_4$ 中生成元 $x$ 的阶为 4，而对 $C_2\times C_2$ 的每个元素 $(u,v)$ 都有

$$2(u,v)=(2u,2v)=(0,0).$$

同构保持元素阶，因为 $f(x)^k=e$ 当且仅当 $f(x^k)=e$，由单射性又当且仅当 $x^k=e$。所以两群不可能同构。这说明即便限制到交换群，合成因子也不够恢复群。

## 1.8　无限群中存在性为何需要另作判断

有限群存在性证明使用了阶的严格下降。对无限群，严格子群可以与原群等势，所用论证不再成立。下面从最后一个因子直接判断一个无限群没有合成列。

**例 1.19** (整数加法群没有有限合成列)**.** 先求 $\mathbb{Z}$ 的子群。若 $H \le \mathbb{Z}$ 非零，取 $h \in H \setminus \{0\}$，则 $h$ 或 $-h$ 为正整数且属于 $H$。由良序原理，$H$ 的正整数中有最小者 $n$。对任意 $k \in H$，作带余除法

$$k = qn + r, \qquad 0 \le r < n.$$

因为 $r = k - qn \in H$，若 $r > 0$ 就与 $n$ 的最小性矛盾，故 $r = 0$。所以 $H \subseteq n\mathbb{Z}$；又因 $n \in H$，其所有整数倍都在 $H$ 中，故 $n\mathbb{Z} \subseteq H$，得到 $H = n\mathbb{Z}$。

对任意 $n \ge 1$，有

$$n\mathbb{Z} \supsetneq 2n\mathbb{Z} \supsetneq \{0\}.$$

第一个包含严格，因为 $n \notin 2n\mathbb{Z}$；第二个严格，因为 $2n \neq 0$。群 $n\mathbb{Z}$ 交换，故 $2n\mathbb{Z}$ 正规于其中。商群 $n\mathbb{Z}/\{0\}$ 因此有非平凡真正规子群 $2n\mathbb{Z}/\{0\}$，不是单群。

若 $\mathbb{Z}$ 有有限合成列，其最后的非零项必是某个 $n\mathbb{Z}$，接下来就是 $\{0\}$；最后因子恰为 $n\mathbb{Z}/\{0\}$，与它不单矛盾。所以 $\mathbb{Z}$ 没有有限合成列。

**例 1.20** (处处可取商仍不能到达合成列)**.** 对每个 $i \ge 0$，定义

$$\eta_i : 2^i\mathbb{Z}/2^{i+1}\mathbb{Z} \longrightarrow C_2, \qquad 2^i k + 2^{i+1}\mathbb{Z} \longmapsto k + 2\mathbb{Z}.$$

若代表相差 $2^{i+1}t$，则对应的整数 $k$ 相差 $2t$，故良定义。整数相加与模 2 相加相容，故保持运算。像覆盖两个剩余类；像相同意味着 $k - \ell$ 为偶数，也就是两个原陪集相同，因此它是同构。于是无限下降链

$$\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq 8\mathbb{Z} \supsetneq \cdots$$

的每个相邻商群都是单群 $C_2$。不过它没有有限步到达 $\{0\}$，所以不是定义 1.6 中的合成列。

事实上 $\bigcap_{i \ge 0} 2^i\mathbb{Z} = \{0\}$：0 属于每一项；若 $k \neq 0$，选 $i$ 使 $2^i > |k|$，则非零整数 $k$ 不可能是 $2^i$ 的倍数，故不在该交集中。即使无限链的交为零，也不能替代定义中有限长度这一要求。

## 文献说明

本章核读 Milne [1] 第六章 “Subnormal Series” 第 87–89 页，采用其中按有限群阶归纳证明 Jordan–Hölder 定理的路线。子群对应和商群同构在正文中直接构造；正规子群与商群的因子合并另列为定理并证明。置换符号的定义与乘法性承接第一册线性代数章，不依赖本册后面的置换群内容。

# 2　交换子与可解群

## 2.1　交换子怎样记录乘法次序

本章固定交换子的约定

$$[x,y]=xyx^{-1}y^{-1}.$$

它与另一种常见的约定 $x^{-1}y^{-1}xy$ 相差一个共轭；本章所有公式都只使用上式。由定义右乘 $yx$，得到

$$xy=[x,y]\,yx.$$

因此 $[x,y]=e$ 当且仅当 $x$ 与 $y$ 交换。交换子不是一个双线性符号；在非交换群中，交换子相乘时必须保留顺序。

**引理 2.1** (交换子恒等式)**.** *对群 $G$ 中任意 $x,y,z,t$，有*

$$[xy,z]=x[y,z]x^{-1}[x,z], \tag{2.1}$$

$$[x,yz]=[x,y]y[x,z]y^{-1}, \tag{2.2}$$

$$t[x,y]t^{-1}=[txt^{-1},tyt^{-1}]. \tag{2.3}$$

*本章只使用前两式和第三式的共轭形式，第二行的乘积顺序不可交换。*

*证明.* 第一式右边逐项展开：

$$\begin{aligned}x[y,z]x^{-1}[x,z]&=x(yzy^{-1}z^{-1})x^{-1}(xzx^{-1}z^{-1})\\&=xyzy^{-1}z^{-1}zx^{-1}z^{-1}\\&=xyzy^{-1}x^{-1}z^{-1}=[xy,z].\end{aligned}$$

第二式右边为

$$\begin{aligned}[x,y]y[x,z]y^{-1}&=(xyx^{-1}y^{-1})y(xzx^{-1}z^{-1})y^{-1}\\&=xyx^{-1}xzx^{-1}z^{-1}y^{-1}\\&=xyzx^{-1}z^{-1}y^{-1}=[x,yz].\end{aligned}$$

最后，

$$\begin{aligned}t[x,y]t^{-1}&=t(xyx^{-1}y^{-1})t^{-1}\\&=(txt^{-1})(tyt^{-1})(tx^{-1}t^{-1})(ty^{-1}t^{-1})\\&=[txt^{-1},tyt^{-1}].\end{aligned}$$

这里每次删去的相邻因子都是形如 $u^{-1}u$；没有交换任意两个不相邻的因子。 □

**命题 2.2** (交换子集合的共轭不变性)**.** *集合*

$$\mathcal{C}(G)=\{[x,y]:x,y\in G\}$$

*在 $G$ 的共轭下不变；即对 $t\in G$，有 $t\mathcal{C}(G)t^{-1}=\mathcal{C}(G)$。此外*

$$[x,y]^{-1}=[y,x].$$

证明. 共轭不变性是引理 2.1 的第三式：共轭后的元素仍属于 $G$，所以包含关系的一边成立；用 $t^{-1}$ 代替 $t$ 得反向包含。逆元直接计算：

$$[x,y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y,x].$$

□

## 2.2 交换子群与交换化

**定义 2.3** (导出子群与特征子群). 令

$$G' = [G,G] = \langle [x,y] : x,y \in G \rangle$$

为所有交换子生成的子群。若 $H \le G$ 且每一个 $\alpha \in \mathrm{Aut}(G)$ 都满足 $\alpha(H) = H$，称 $H$ 为 $G$ 的特征子群。令

$$G^{(0)} = G, \qquad G^{(i+1)} = (G^{(i)})' \quad (i \ge 0),$$

称 $G^{(0)} \supseteq G^{(1)} \supseteq \cdots$ 为导出列。

先证明导出子群确实给出一条正规列。对 $t \in G$ 和生成元 $[x,y]$，命题 2.2 给出

$$t[x,y]t^{-1} = [txt^{-1}, tyt^{-1}] \in G'.$$

共轭保持乘积和逆元，故 $tG't^{-1} \subseteq G'$；以 $t^{-1}$ 代入得到相反包含。因此 $G' \trianglelefteq G$。同理，每个 $G^{(i+1)}$ 正规于 $G^{(i)}$；事实上下面会看到它甚至特征于 $G$。

**命题 2.4** (导出子群的特征性与同态像). *$G'$ 是 $G$ 的特征子群，因而每个 $G^{(i)}$ 都是 $G$ 的特征子群。若 $f : G \to H$ 为同态，则*

$$f(G') = f(G)', \qquad f(G^{(i)}) = f(G)^{(i)} \quad (i \ge 0).$$

*特别地，若 $f$ 满射，则 $f(G^{(i)}) = H^{(i)}$。*

证明. 对 $x,y \in G$，同态保持乘法和逆元，所以

$$f([x,y]) = f(x)f(y)f(x)^{-1}f(y)^{-1} = [f(x),f(y)].$$

$G'$ 的元素是有限个交换子及其逆的乘积；因此它们的像都在 $f(G)'$ 中，得到 $f(G') \subseteq f(G)'$。反向地，$f(G)'$ 的每个生成元写成

$$[f(x),f(y)] = f([x,y]) \in f(G'),$$

故 $f(G)' \subseteq f(G')$，两边相等。

若 $\alpha \in \mathrm{Aut}(G)$，则 $\alpha(G') = \alpha(G)' = G'$，所以 $G'$ 特征。若 $K$ 特征于 $H$，$H$ 特征于 $G$，则 $\alpha \in \mathrm{Aut}(G)$ 限制为 $H$ 的自同构，而后者保持 $K$；故 $K$ 特征于 $G$。归纳得到每个 $G^{(i)}$ 特征于 $G$，因而正规于 $G$。

对 $i$ 作归纳。$i = 0$ 时 $f(G^{(0)}) = f(G) = f(G)^{(0)}$。若 $f(G^{(i)}) = f(G)^{(i)}$，把刚证明的等式应用于限制同态

$$f|_{G^{(i)}} : G^{(i)} \longrightarrow f(G^{(i)})$$

得到

$$f(G^{(i+1)}) = f((G^{(i)})') = f(G^{(i)})' = (f(G)^{(i)})' = f(G)^{(i+1)}.$$

这完成归纳。 □

**定理 2.5** (交换化的泛性质)**.** 商群 $G/G'$ 是交换群。若 $A$ 是交换群且 $f: G \to A$ 是同态，则存在唯一同态

$$\bar{f}: G/G' \longrightarrow A$$

使得 $f = \bar{f} \circ q$，其中 $q: G \to G/G'$ 是自然投影。也就是说，任意到交换群的同态都唯一地通过 $G/G'$ 因子化。

证明. 因所有交换子属于 $G'$，在商群中直接计算：

$$(xG')(yG') = xyG' = [x,y]yxG' = yxG' = (yG')(xG').$$

定义

$$\bar{f}(xG') = f(x).$$

若 $xG' = yG'$，则 $y^{-1}x \in G'$。$G'$ 由交换子生成，而 $A$ 交换，所以每个交换子在 $f$ 下都映到单位元：

$$f([u,v]) = f(u)f(v)f(u)^{-1}f(v)^{-1} = e_A.$$

因此 $G' \subseteq \ker f$，从而 $f(y^{-1}x) = e_A$，即 $f(x) = f(y)$；映射良定义。它保持运算：

$$\bar{f}((xG')(yG')) = \bar{f}(xyG') = f(xy) = f(x)f(y) = \bar{f}(xG')\bar{f}(yG').$$

代入 $q(x) = xG'$ 的定义可得 $\bar{f}(q(x)) = \bar{f}(xG') = f(x)$；对每个 $x \in G$ 都成立，故 $f = \bar{f} \circ q$。

若 $g: G/G' \to A$ 也满足 $f = g \circ q$，因 $q$ 满射，对任意 $xG'$ 有

$$g(xG') = g(q(x)) = f(x) = \bar{f}(q(x)) = \bar{f}(xG'),$$

故 $g = \bar{f}$。唯一性成立。 □

**命题 2.6** (交换商的判别)**.** 若 $N \trianglelefteq G$，则

$$G/N \text{ 交换} \quad \Longleftrightarrow \quad G' \subseteq N.$$

因而 $G'$ 是包含于 $G$ 的所有正规子群中使商群交换者的最小者。

证明. 令 $q: G \to G/N$ 为自然投影。对 $x, y \in G$，

$$\begin{aligned} q(x)q(y) = q(y)q(x) &\Longleftrightarrow q(xyx^{-1}y^{-1}) = N \\ &\Longleftrightarrow [x,y] \in N. \end{aligned}$$

若商群交换，所有交换子在 $N$ 中，故由生成定义 $G' \subseteq N$。反过来若 $G' \subseteq N$，每个 $[x,y] \in N$，上面等价链反向说明任意两个陪集交换。最后，$G' \trianglelefteq G$ 已在前面证明，所以它本身是这样的正规子群；任意另一个这样的 $N$ 都包含它。 □

## 2.3 可解性与导出列

**定义 2.7** (可解群与导出长度)**.** 若 $G$ 有一条有限次正规列（即每个下一项正规于当前项）

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{e\}, \qquad G_{i+1} \trianglelefteq G_i,$$

使每个因子 $G_i/G_{i+1}$ 都是交换群，称 $G$ 为可解群。若存在最小的 $d$ 使 $G^{(d)} = \{e\}$，称 $d$ 为 $G$ 的导出长度，记作 $\mathrm{dl}(G) = d$。平凡群的导出长度为 $0$。

**定理 2.8** (导出列判别)**.** *群 $G$ 可解，当且仅当存在非负整数 $r$ 使*

$$G^{(r)} = \{e\}.$$

*若 $G$ 可解，则导出长度是所有因子交换的有限次正规列长度的最小值，也等于其中正规列长度的最小值。*

*证明.* 若 $G^{(r)} = \{e\}$，由前面的特征性结论，

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(r)} = \{e\}, \qquad G^{(i+1)} \trianglelefteq G^{(i)}$$

是正规列。对每个 $i$，$(G^{(i)})' = G^{(i+1)}$，而命题 2.6 应用于 $G^{(i)}$ 和 $G^{(i+1)}$，给出

$$G^{(i)}/G^{(i+1)} \text{ 交换.}$$

故 $G$ 可解。

反向设 $G = G_0 \supseteq \cdots \supseteq G_r = \{e\}$ 是各因子交换的次正规列。证明

$$G^{(i)} \subseteq G_i \qquad (0 \le i \le r)$$

成立。$i = 0$ 时为等式。若 $G^{(i)} \subseteq G_i$，则 $G^{(i+1)}$ 由 $G^{(i)}$ 中元素的交换子生成，故

$$G^{(i+1)} \subseteq G_i'.$$

因 $G_i/G_{i+1}$ 交换，命题 2.6 给出 $G_i' \subseteq G_{i+1}$。于是 $G^{(i+1)} \subseteq G_{i+1}$。取 $i = r$，得到 $G^{(r)} \subseteq \{e\}$，所以 $G^{(r)} = \{e\}$。

这也证明了最小性：任意长度为 $r$ 的可解次正规列都迫使 $G^{(r)} = 1$，所以其长度不小于导出长度。而终止的导出列本身是一条因子交换的正规列，其长度就是导出长度，所以两个最小值都取到。 □

**命题 2.9** (导出长度的基本性质)**.** *若 $G$ 是非平凡可解群，则 $\mathrm{dl}(G) \ge 1$。若 $G$ 非平凡且交换，则 $\mathrm{dl}(G) = 1$。若 $N \trianglelefteq G$，则*

$$\mathrm{dl}(G/N) \le \mathrm{dl}(G), \qquad \mathrm{dl}(N) \le \mathrm{dl}(G).$$

*若 $G$ 与 $H$ 同构，则它们的导出长度相同。*

*证明.* $G^{(0)} = G \ne 1$，而交换群的第一导出群 $G' = 1$，所以前两句成立。商群部分由命题 2.4：若 $G^{(r)} = 1$，则

$$(G/N)^{(r)} = q(G^{(r)}) = 1.$$

子群部分先证明 $K^{(i)} \subseteq G^{(i)}$ 对 $K \le G$ 成立。初始为 $K \subseteq G$；若成立，则 $K^{(i+1)} = (K^{(i)})' \subseteq (G^{(i)})' = G^{(i+1)}$，因为 $K^{(i)}$ 是 $G^{(i)}$ 的子群。取 $K = N$ 即得。

若 $f : G \to H$ 是同构，命题 2.4 给出 $f(G^{(i)}) = H^{(i)}$。故一项为平凡群当且仅当对应项为平凡群，最小的指标相同。 □

**定理 2.10** (可解群的扩张判别)**.** *设 $N \trianglelefteq G$。则*

$$G \text{ 可解} \quad \Longleftrightarrow \quad N \text{ 与} G/N \text{ 都可解.}$$

*若 $\mathrm{dl}(N) \le a$ 且 $\mathrm{dl}(G/N) \le b$，则*

$$\mathrm{dl}(G) \le a + b.$$

证明. 先设 $G^{(r)}=1$。任意子群 $H\le G$ 满足 $H^{(i)}\subseteq G^{(i)}$，故 $H^{(r)}=1$，所以 $H$ 可解。令 $q:G\to G/N$，则

$$(G/N)^{(i)}=q(G^{(i)}),$$

故 $(G/N)^{(r)}=1$，商群可解。特别取 $H=N$，得到必要性。

反向，设 $N^{(a)}=1$ 且 $(G/N)^{(b)}=1$。由同态像公式，

$$q(G^{(b)})=(G/N)^{(b)}=1,$$

所以 $G^{(b)}\subseteq\ker q=N$。对包含关系连续取 $a$ 次交换子，得到

$$G^{(a+b)}=(G^{(b)})^{(a)}\subseteq N^{(a)}=1.$$

这里 $(G^{(b)})^{(a)}$ 表示从 $G^{(b)}$ 开始取 $a$ 次导出群，且由导出列递推定义它正是 $G^{(a+b)}$。由导出列判别，$G$ 可解且导出长度不超过 $a+b$。 □

## 2.4 可解群的合成因子

**引理 2.11** (交换单群). 非平凡交换单群恰为素数阶循环群。

证明. 设 $A$ 是非平凡交换单群，取 $a\neq e$。$\langle a\rangle$ 在交换群中正规且非平凡，单性给出 $\langle a\rangle=A$。若 $a$ 无限阶，则 $\langle a^2\rangle$ 是非平凡真子群；确实 $a\notin\langle a^2\rangle$，因为若 $a=(a^2)^k$，则 $a^{2k-1}=e$，与无限阶矛盾。故 $a$ 的阶为有限整数 $n$。

若 $n=uv$ 为合数分解，其中 $u,v>1$，则 $a^u$ 的阶为 $v$：$(a^u)^v=a^n=e$，且若 $(a^u)^k=e$，则 $n\mid uk$，因 $n=uv$ 得 $v\mid k$。于是 $\langle a^u\rangle$ 是非平凡真子群，矛盾。因此 $n=p$ 为素数，$A=\langle a\rangle\cong C_p$。

反之，若 $|P|=p$ 为素数，Lagrange 定理说明其子群阶只能为 1 或 $p$，故只有平凡子群和自身；$P$ 单。有限群阶为 $p$ 时任取非单位元便生成全群，因此 $P\cong C_p$ 且交换。 □

**定理 2.12** (有限可解群的素数阶因子). 有限群 $G$ 可解，当且仅当它的合成因子全为素数阶循环群。等价地，$G$ 有一条因子均为素数阶循环群的有限次正规列。

证明. 若 $G$ 可解，取任意合成列。每个列项是 $G$ 的子群，子群可解；每个合成因子是某个列项的商，而商群也可解。设 $S$ 是一个可解单群。$S'$ 是 $S$ 的正规子群，故 $S'=1$ 或 $S'=S$。第二种情形会使导出列从 $S$ 开始恒为 $S$，不可能到达 1；故 $S'=1$，$S$ 交换。引理 2.11 说明 $S\cong C_p$。

反之，若一条合成列的所有因子都为素数阶循环群，则每个因子交换，该列本身就是可解次正规列。由 Jordan–Hölder 定理，若说“合成因子全为”而没有指定列，所指性质与所选合成列无关。 □

## 2.5 具体计算：从商群确定导出子群

**例 2.13** ($S_3$ 的导出列). 符号同态 $\operatorname{sgn}:S_3\to C_2$ 的核为 $A_3$，而 $C_2$ 交换。由命题 2.6，

$$S_3'\subseteq A_3.$$

另一方面，按从右向左复合，$(12)^{-1}=(12)$、$(23)^{-1}=(23)$，所以

$$\begin{aligned}[(12),(23)] &= (12)(23)(12)(23)\\ &= (132).\end{aligned}$$

三循环 $(132)$ 生成 $A_3$，故 $A_3\subseteq S_3'$。于是 $S_3'=A_3$。由于 $A_3$ 交换，$A_3'=1$，因此

$$S_3^{(0)}=S_3,\qquad S_3^{(1)}=A_3,\qquad S_3^{(2)}=1,$$

导出长度为 2。

**例 2.14** (二面体群的导出群)**.** 令 $D_{2n}$ 为正 $n$ 边形的对称群，阶为 $2n$，取旋转 $r$ 与反射 $s$，满足

$$r^n=s^2=e,\qquad srs^{-1}=r^{-1}.$$

由定义

$$[s,r]=srs^{-1}r^{-1}=r^{-1}r^{-1}=r^{-2},$$

故 $\langle r^2\rangle\subseteq D_{2n}'$。

反向包含通过商群证明。$\langle r^2\rangle$ 在 $\langle r\rangle$ 中正规；又 $sr^2s^{-1}=r^{-2}\in\langle r^2\rangle$，所以它在 $D_{2n}$ 中正规。记商群中的像为 $\bar r=r\langle r^2\rangle$、$\bar s=s\langle r^2\rangle$。因 $r^2\in\langle r^2\rangle$，有 $\bar r^2=\bar e$，于是 $\bar r^{-1}=\bar r$。原关系变成

$$\bar s\bar r\bar s^{-1}=\bar r^{-1}=\bar r,$$

说明 $\bar r$ 与 $\bar s$ 交换。它们生成整个商群，所以商群交换；命题 2.6 给出 $D_{2n}'\subseteq\langle r^2\rangle$。因此

$$D_{2n}'=\langle r^2\rangle.$$

若 $n$ 为奇数，则存在整数 $u$ 使 $2u\equiv 1\pmod n$，从而 $r=(r^2)^u$，所以 $\langle r^2\rangle=\langle r\rangle$。若 $n$ 为偶数，$r^2$ 的阶为 $n/2$，所以 $\langle r^2\rangle$ 在旋转子群中指数为 2。当 $n\geq 3$ 时该导出群非平凡且循环，因而下一项为 1；于是 $D_{2n}$ 的导出长度为 2。小的退化情形为 $D_2\cong C_2$、$D_4\cong C_2\times C_2$，它们本身交换，导出长度为 1。

**例 2.15** (仿射群)**.** 设 $F$ 是域。所有

$$T_{a,b}:F\to F,\qquad x\longmapsto ax+b,\qquad a\in F^\times, b\in F$$

在复合下构成群 $\mathrm{Aff}(F)$。逐点计算得到

$$T_{a,b}T_{c,d}=T_{ac,ad+b},\qquad T_{a,b}^{-1}=T_{a^{-1},-a^{-1}b}.$$

映射

$$\lambda:\mathrm{Aff}(F)\to F^\times,\qquad T_{a,b}\longmapsto a$$

满足 $\lambda(T_{a,b}T_{c,d})=ac=\lambda(T_{a,b})\lambda(T_{c,d})$，是满同态。其核为

$$U=\{T_{1,b}:b\in F\},$$

而 $b\mapsto T_{1,b}$ 给出 $(F,+)\cong U$；因此商群交换，$\mathrm{Aff}(F)'\subseteq U$。

若 $|F|>2$，取 $a\in F^\times\setminus\{1\}$。由上面的复合和逆公式，

$$\begin{aligned}[T_{a,0},T_{1,b}] &= T_{a,0}T_{1,b}T_{a^{-1},0}T_{1,-b}\\ &= T_{1,ab}T_{1,-b}=T_{1,(a-1)b}.\end{aligned}$$

乘以非零元 $a-1$ 是 $F$ 上的双射，所以当 $b$ 遍历 $F$ 时，$(a-1)b$ 也遍历 $F$；每个平移都属于导出群。于是 $U \subseteq \mathrm{Aff}(F)'$，得到

$$\mathrm{Aff}(F)' = U, \qquad \mathrm{Aff}(F)'' = U' = 1.$$

若 $F = \mathbb{F}_2$，只有斜率 1，群本身就是平移群 $U \cong C_2$，所以第一导出群已经为 1。

## 2.6 上三角矩阵群的可解性

令 $B_n(F)$ 为可逆上三角矩阵群，令 $U_n(F)$ 为对角线全为 1 的上三角矩阵群。对角映射

$$\delta : B_n(F) \longrightarrow (F^\times)^n, \qquad A = (a_{ij}) \longmapsto (a_{11}, \ldots, a_{nn})$$

满足

$$(AB)_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki} = a_{ii} b_{ii},$$

因为 $a_{ik} = 0$（当 $k < i$）且 $b_{ki} = 0$（当 $k > i$），只有 $k = i$ 的项可能非零。因此 $\delta$ 是同态。对角矩阵

$$\mathrm{diag}(c_1, \ldots, c_n)$$

是任意 $(c_1, \ldots, c_n) \in (F^\times)^n$ 的原像，故 $\delta$ 满射；核正是 $U_n(F)$。由于 $(F^\times)^n$ 交换，$B_n(F)/U_n(F)$ 交换。

以下 $n \geq 1$。对每个整数 $k \geq 1$，令

$$J_k = \{A \in M_n(F) : a_{ij} = 0 \text{ unless } j - i \geq k\}, \qquad U_k = I + J_k.$$

这里 $J_1$ 是严格上三角矩阵集合，$k \geq n$ 时 $J_k = \{0\}$。因此 $U_1 = U_n(F)$，而过滤下标满足 $k \geq n$ 时 $U_k = \{I\}$。$J_k$ 是上三角矩阵环 $R$ 的加法子群。

**引理 2.16** (位置过滤)**.** *对正整数 $i, j$，有*

$$J_i J_j \subseteq J_{i+j}.$$

*若 $i + j \geq n$，则 $J_{i+j} = \{0\}$。*

*证明.* 取 $A \in J_i, B \in J_j$。矩阵乘积的 $(r, s)$ 项为

$$(AB)_{rs} = \sum_{t=1}^{n} a_{rt} b_{ts}.$$

若某项非零，则 $t - r \geq i$ 且 $s - t \geq j$，相加得 $s - r \geq i + j$。于是当 $s - r < i + j$ 时所有项均为零，故 $AB \in J_{i+j}$。若 $i + j \geq n$，对 $1 \leq r < s \leq n$ 有 $s - r \leq n - 1 < i + j$，而对角线下方本来为零，所以只有零矩阵满足条件。 □

**命题 2.17** (幂零上三角群的交换子过滤)**.** *对 $1 \leq i, j \leq n$，$U_i$ 与 $U_j$ 都是 $U_1$ 的正规子群，并且*

$$[U_i, U_j] \subseteq U_{i+j}.$$

*因此*

$$(U_1)^{(r)} \subseteq U_{2^r} \quad (r \geq 0),$$

*从而 $U_1$ 可解，且导出长度不超过 $\lceil \log_2 n \rceil$。*

证明. 先说明 $U_k$ 是群。若 $A, B \in J_k$，则

$$(I + A)(I + B) = I + (A + B + AB),$$

而 $A + B \in J_k$、$AB \in J_{2k} \subseteq J_k$，故乘积仍在 $I + J_k$。严格上三角矩阵满足 $A^n = 0$：矩阵乘积中每次非零位置至少向右移动一格，$n$ 次后不可能仍在 $1, \dots, n$ 的范围内。因此

$$(I + A)^{-1} = I - A + A^2 - \cdots + (-1)^{n-1} A^{n-1},$$

直接相乘时相邻项抵消，结果为 $I$；且每个 $A^m \in J_{mk} \subseteq J_k$，所以逆元仍在 $U_k$。

对 $X \in U_1$ 和 $I + A \in U_k$，写 $X = I + C$，其中 $C \in J_1$。下面先证明 $J_k$ 是上三角矩阵环的双边理想，再使用商环。对任意上三角矩阵 $P$，左右乘 $J_k$ 中的矩阵不会降低非零位置的差值：若 $A \in J_k$，则

$$(PA)_{rs} = \sum_t p_{rt} a_{ts} \neq 0 \implies s - r \geq (t - r) + k \geq k,$$

因为 $P$ 上三角时 $t - r \geq 0$；同理

$$(AP)_{rs} = \sum_t a_{rt} p_{ts} \neq 0 \implies s - r \geq k + (s - t) \geq k.$$

故 $PJ_k \subseteq J_k$ 且 $J_k P \subseteq J_k$，即 $J_k$ 是 $R$ 的双边理想。若 $X \in U_1$、$A \in J_k$，则 $X^{-1}$ 仍上三角，因而

$$X(I + A)X^{-1} = I + XAX^{-1} \in I + J_k.$$

再对 $X^{-1}$ 作同一计算，得到反向包含，所以 $U_k \trianglelefteq U_1$。

在商环 $R/J_{i+j}$ 中，若 $A \in J_i, B \in J_j$，引理给出 $AB = BA = 0$。因此

$$(I + A)(I + B) = I + A + B = (I + B)(I + A) \quad \text{在} R/J_{i+j} \text{ 中}.$$

这等价于交换子

$$(I + A)(I + B)(I + A)^{-1}(I + B)^{-1}$$

在商群中为单位元，也就是属于 $I + J_{i+j} = U_{i+j}$。所以 $[U_i, U_j] \subseteq U_{i+j}$。

最后对 $r$ 归纳。$r = 0$ 时 $(U_1)^{(0)} = U_1 = U_{2^0}$。若 $(U_1)^{(r)} \subseteq U_{2^r}$，则

$$(U_1)^{(r+1)} = ((U_1)^{(r)})' \subseteq [U_{2^r}, U_{2^r}] \subseteq U_{2^{r+1}}.$$

当 $2^r \geq n$ 时 $U_{2^r} = \{I\}$，故导出列终止。最小满足 $2^r \geq n$ 的整数为 $\lceil \log_2 n \rceil$。 □

**定理 2.18** (可逆上三角矩阵群可解). $B_n(F)$ 可解，并且

$$\mathrm{dl}(B_n(F)) \leq 1 + \lceil \log_2 n \rceil.$$

证明. 商群 $B_n(F)/U_n(F)$ 交换，而命题 2.17 说明 $U_n(F) = U_1$ 可解，导出长度不超过 $\lceil \log_2 n \rceil$。将 $N = U_n(F)$ 代入定理 2.10，得到

$$\mathrm{dl}(B_n(F)) \leq \mathrm{dl}(U_n(F)) + \mathrm{dl}(B_n(F)/U_n(F)) \leq \lceil \log_2 n \rceil + 1.$$

□

**例 2.19** (上三角群的低阶过滤)**.** 当 $n=4$ 时，$U_1$ 的元素形如

$$\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

而

$$U_2 = \left\{ \begin{pmatrix} 1 & 0 & b & c \\ 0 & 1 & 0 & e \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\}, \quad U_4 = \{I\}.$$

过滤给出

$$U_1' \subseteq U_2, \qquad U_1'' \subseteq U_4 = 1.$$

因此任何特征为零或正特征的域上，四阶单位上三角群的导出长度都不超过 2；结论没有除以 2 或使用特征零条件。

## 2.7　文献说明

本章交换子恒等式、导出列判别及可解群扩张性质核读 Milne [1] 第六章第 90–93 页；矩阵群部分使用位置过滤的直接证明。交换化的泛性质、仿射群例子和上三角矩阵的下标证明在本章独立写出。

# 3 中心列与幂零群

## 3.1 中心的原像与上中心列

可解群只要求因子群交换；幂零群要求这些因子还要由整个上方群的中心产生。这个附加条件可以用商群的中心逐层拉回原群来表达。

**定义 3.1** (中心与正规化子)**.** 群 $G$ 的中心定义为

$$Z(G)=\{z\in G : zg=gz \text{ 对所有} g\in G\}.$$

它是子群：$e$ 与所有元素交换；若 $z,w\in Z(G)$，由 $wg=gw$ 得 $w^{-1}g=gw^{-1}$，于是

$$(zw^{-1})g=z(gw^{-1})=g(zw^{-1})\qquad (g\in G).$$

故 $zw^{-1}\in Z(G)$。若 $H\le G$，其正规化子定义为

$$N_G(H)=\{g\in G : gHg^{-1}=H\}.$$

若 $g,k\in N_G(H)$，则

$$(gk)H(gk)^{-1}=g(kHk^{-1})g^{-1}=H.$$

由 $gHg^{-1}=H$ 两边以 $g^{-1}$ 共轭得 $g^{-1}Hg=H$；单位元也正规化 $H$。故 $N_G(H)$ 是子群。若 $h\in H$，则 $hHh^{-1}=H$，所以 $H\le N_G(H)$。

**定义 3.2** (上中心列与幂零类)**.** 令 $Z_0(G)=\{e\}$。假设 $Z_i(G)\trianglelefteq G$ 已定义，令

$$q_i : G\longrightarrow G/Z_i(G),\qquad q_i(g)=gZ_i(G),$$

并定义

$$Z_{i+1}(G)=q_i^{-1}\big(Z(G/Z_i(G))\big).$$

这称为 $G$ 的上中心列。若存在 $c\ge 0$ 使 $Z_c(G)=G$，称 $G$ 为幂零群；最小的这样的 $c$ 称为幂零类。平凡群的幂零类规定为 $0$。

要使定义递归合法，必须证明每个 $Z_i(G)$ 都正规。事实上它们将是特征子群。

**命题 3.3** (上中心列的特征性)**.** *对每个 $i\ge 0$，$Z_i(G)$ 是 $G$ 的特征子群，且*

$$x\in Z_{i+1}(G)\quad\Longleftrightarrow\quad [x,g]\in Z_i(G)\quad \text{对所有} g\in G.$$

*特别地，$Z_i(G)\trianglelefteq G$，定义中的每个商群都有意义。*

*证明.* 先证中心特征。若 $z\in Z(G)$，$\alpha\in \mathrm{Aut}(G)$，任取 $y\in G$ 并写成 $y=\alpha(x)$，则

$$\alpha(z)y=\alpha(z)\alpha(x)=\alpha(zx)=\alpha(xz)=\alpha(x)\alpha(z)=y\alpha(z).$$

所以 $\alpha(z)\in Z(G)$，得到 $\alpha(Z(G))\subseteq Z(G)$；对 $\alpha^{-1}$ 使用同一包含，得到等号。

归纳假设 $Z_i$ 特征。因为 $\alpha(Z_i)=Z_i$，公式

$$\bar{\alpha}: G/Z_i \longrightarrow G/Z_i, \qquad gZ_i \longmapsto \alpha(g)Z_i$$

是良定义的自同构：若 $gZ_i = hZ_i$，则 $h^{-1}g \in Z_i$，于是

$$\alpha(h)^{-1}\alpha(g) = \alpha(h^{-1}g) \in Z_i.$$

此外 $\bar{\alpha}((gZ_i)(hZ_i)) = \alpha(gh)Z_i = (\alpha(g)Z_i)(\alpha(h)Z_i)$，所以保持乘法；它的逆由 $\alpha^{-1}$ 给出。自同构保持中心，所以

$$\bar{\alpha}\big(Z(G/Z_i)\big) = Z(G/Z_i).$$

因此

$$\alpha(Z_{i+1}) = \alpha\big(q_i^{-1}(Z(G/Z_i))\big) = q_i^{-1}(Z(G/Z_i)) = Z_{i+1}.$$

归纳完成。

最后，$x \in Z_{i+1}$ 当且仅当 $xZ_i$ 属于 $G/Z_i$ 的中心。这等价于对每个 $g \in G$，

$$(xZ_i)(gZ_i) = (gZ_i)(xZ_i),$$

也等价于

$$(xgx^{-1}g^{-1})Z_i = Z_i,$$

即 $[x,g] \in Z_i$。 □

由命题可知 $Z_1(G) = Z(G)$。此外 $Z_i(G) \subseteq Z_{i+1}(G)$：若 $x \in Z_i$，则 $xZ_i$ 是商群单位元，必在其中心。故上中心列确实是递增列。

## 3.2 下中心列与满同态像

对两个子群 $A, B \leq G$，定义

$$[A,B] = \langle [a,b] : a \in A, b \in B \rangle.$$

这里的尖括号表示由所有这些交换子生成的子群，不表示交换子的集合本身。

**定义 3.4** (下中心列)**.** 令

$$\gamma_1(G) = G, \qquad \gamma_{i+1}(G) = [\gamma_i(G), G] \quad (i \geq 1).$$

称 $\gamma_1(G) \supseteq \gamma_2(G) \supseteq \cdots$ 为下中心列。

**引理 3.5** (下中心列的特征性与满同态像)**.** *每个 $\gamma_i(G)$ 是 $G$ 的特征子群，且*

$$\gamma_{i+1}(G) \subseteq \gamma_i(G).$$

*若 $f: G \to H$ 为满同态，则*

$$f(\gamma_i(G)) = \gamma_i(H) \quad (i \geq 1).$$

证明. 先证递降性。假设 $\gamma_i \trianglelefteq G$。若 $a \in \gamma_i$、$g \in G$，则

$$[a,g] = aga^{-1}g^{-1} = a(ga^{-1}g^{-1}).$$

因 $\gamma_i$ 正规，$ga^{-1}g^{-1} \in \gamma_i$；两因子都在 $\gamma_i$，故 $[a,g] \in \gamma_i$。生成这些交换子得到 $\gamma_{i+1} \subseteq \gamma_i$。

再证特征性。若 $\alpha \in \mathrm{Aut}(G)$，则

$$\alpha([\gamma_i, G]) = [\alpha(\gamma_i), \alpha(G)].$$

从 $\gamma_1 = G$ 开始归纳，假设 $\alpha(\gamma_i) = \gamma_i$，便有

$$\alpha(\gamma_{i+1}) = \alpha([\gamma_i, G]) = [\gamma_i, G] = \gamma_{i+1}.$$

所以每项特征，因而正规。

对满同态 $f$，先有 $f(\gamma_1(G)) = f(G) = H = \gamma_1(H)$。若 $f(\gamma_i(G)) = \gamma_i(H)$，则

$$\begin{aligned} f(\gamma_{i+1}(G)) &= f([\gamma_i(G), G]) \\ &= \langle f([a,g]) : a \in \gamma_i(G), g \in G \rangle \\ &= \langle [f(a), f(g)] : a \in \gamma_i(G), g \in G \rangle \\ &= \langle [u,v] : u \in \gamma_i(H), v \in H \rangle \\ &= [\gamma_i(H), H] = \gamma_{i+1}(H). \end{aligned}$$

第三个等号使用同态保持交换子，第四个等号使用 $f$ 对 $\gamma_i(G)$ 和 $G$ 的满射像分别为 $\gamma_i(H)$ 和 $H$。 □

**定理 3.6** (上、下中心列的等价判别)**.** 对每个整数 $c \geq 0$，有

$$Z_c(G) = G \quad \Longleftrightarrow \quad \gamma_{c+1}(G) = \{e\}.$$

因此 $G$ 幂零当且仅当其下中心列在有限步到达平凡群。

证明. 先设 $Z_c(G) = G$。我们证明

$$\gamma_i(G) \subseteq Z_{c+1-i}(G) \qquad (1 \leq i \leq c+1).$$

当 $i = 1$ 时这是 $G = Z_c(G)$。假设对某个 $1 \leq i \leq c$ 已有

$$\gamma_i \subseteq Z_{c+1-i}.$$

任取 $a \in \gamma_i$ 和 $g \in G$。由命题 3.3，

$$[a,g] \in Z_{c-i}.$$

因此所有生成元 $[a,g]$ 都在 $Z_{c-i}$，从而

$$\gamma_{i+1} = [\gamma_i, G] \subseteq Z_{c-i} = Z_{c+1-(i+1)}.$$

取 $i = c+1$ 得 $\gamma_{c+1} \subseteq Z_0 = \{e\}$。

反向设 $\gamma_{c+1} = \{e\}$。我们倒向证明

$$\gamma_{c+1-j} \subseteq Z_j \qquad (0 \leq j \leq c).$$

当 $j=0$ 时，$\gamma_{c+1}\subseteq Z_0$ 是假设。若对某个 $0\le j<c$ 有

$$\gamma_{c+1-j}\subseteq Z_j,$$

则任取 $a\in\gamma_{c-j}$ 和 $g\in G$，有

$$[a,g]\in[\gamma_{c-j},G]=\gamma_{c+1-j}\subseteq Z_j.$$

命题 3.3 的等价条件给出 $a\in Z_{j+1}$，所以

$$\gamma_{c-j}\subseteq Z_{j+1}.$$

令 $j=c$，得到 $G=\gamma_1\subseteq Z_c\subseteq G$，即 $Z_c=G$。 □

**推论 3.7** (基本封闭性)**.** *幂零群的子群、商群和有限直积仍幂零；幂零群可解。若 $G,H$ 的幂零类分别不超过 $c,d$，则 $G\times H$ 的幂零类不超过 $\max\{c,d\}$。*

*证明.* 若 $K\le G$，由交换子的生成定义归纳证明

$$\gamma_i(K)\subseteq\gamma_i(G).$$

初始为 $K\subseteq G$；若成立，则

$$\gamma_{i+1}(K)=[\gamma_i(K),K]\subseteq[\gamma_i(G),G]=\gamma_{i+1}(G).$$

所以 $\gamma_{c+1}(G)=1$ 蕴含 $\gamma_{c+1}(K)=1$。

商群结论由引理 3.5：若 $q:G\to G/N$ 满射且 $\gamma_{c+1}(G)=1$，则

$$\gamma_{c+1}(G/N)=q(\gamma_{c+1}(G))=1.$$

对直积，逐坐标计算

$$[(g_1,h_1),(g_2,h_2)]=([g_1,g_2],[h_1,h_2]).$$

归纳得到

$$\gamma_i(G\times H)=\gamma_i(G)\times\gamma_i(H).$$

一个包含方向来自右侧中任意交换子的坐标公式；反向方向则由嵌入

$$(a,e)=[(x,e),(y,e)]\quad(a=[x,y]),\qquad(e,b)=[(e,u),(e,v)]\quad(b=[u,v])$$

及生成性得到。故有限直积的下中心列在两个坐标同时终止时终止，类不超过各类的最大值。

若 $Z_c(G)=G$，则对每个 $i<c$，$Z_{i+1}/Z_i$ 是 $G/Z_i$ 的中心的子群，因而交换。列

$$G=Z_c\supseteq Z_{c-1}\supseteq\cdots\supseteq Z_0=1$$

的每个非平凡因子交换，删去重复项后是可解列。因此幂零群可解。 □

## 3.3 有限 $p$ 群的中心与幂零性

**定理 3.8** (有限 $p$ 群的中心非平凡)**.** *若 $P$ 是非平凡有限 $p$ 群，则 $Z(P) \neq \{e\}$。*

*证明.* $P$ 作用于自身，作用为共轭：$g \cdot x = gxg^{-1}$。轨道是共轭类。轨道大小由轨道–稳定子定理给出

$$|\operatorname{Orb}(x)| = [P : C_P(x)], \qquad C_P(x) = \{g \in P : gx = xg\}.$$

因为 $|P|$ 是 $p$ 的幂，每个轨道大小也是 $p$ 的幂。轨道大小为 1 的元素正是中心元素，所以类方程为

$$|P| = |Z(P)| + \sum_{j=1}^{m} [P : C_P(x_j)],$$

其中 $x_j$ 取非中心共轭类的代表。每一项和 $|P|$ 都被 $p$ 整除，故 $|Z(P)|$ 被 $p$ 整除。单位元在中心中，所以 $|Z(P)| \geq 1$；被 $p$ 整除便有 $|Z(P)| \geq p > 1$，中心非平凡。 □

**定理 3.9** (有限 $p$ 群幂零)**.** *每个有限 $p$ 群都是幂零群。*

*证明.* 对 $|P|$ 作归纳。平凡群满足 $Z_0(P) = P$，幂零类为 0。设 $P \neq 1$。由定理 3.8，$Z(P) \neq 1$，故

$$|P/Z(P)| < |P|.$$

归纳假设说明存在 $c \geq 0$ 使

$$\gamma_{c+1}(P/Z(P)) = 1.$$

投影 $q : P \to P/Z(P)$ 是满同态，由引理 3.5，

$$q(\gamma_{c+1}(P)) = \gamma_{c+1}(P/Z(P)) = 1.$$

因此 $\gamma_{c+1}(P) \subseteq \ker q = Z(P)$。于是

$$\gamma_{c+2}(P) = [\gamma_{c+1}(P), P] \subseteq [Z(P), P] = 1.$$

由定理 3.6，$P$ 幂零。 □

## 3.4 正规化子条件

幂零群的上中心列还控制任意真子群的正规化子。

**引理 3.10** (正规化子严格增大)**.** *若 $G$ 是非平凡幂零群，且 $H < G$，则*

$$H \subsetneq N_G(H).$$

*证明.* 取最小的 $j \geq 1$ 使 $Z_j(G) \not\subseteq H$。存在性来自 $Z_0 = 1 \subseteq H$ 和某个 $Z_c = G$；最小性给出

$$Z_{j-1}(G) \subseteq H.$$

取 $z \in Z_j(G) \setminus H$。任取 $h \in H$，由命题 3.3，

$$[z, h] \in Z_{j-1}(G) \subseteq H.$$

由交换子定义，

$$zhz^{-1} = [z, h]h \in H.$$

故 $zHz^{-1} \subseteq H$。同样对 $z^{-1} \in Z_j(G)$ 应用这个结论，得到 $z^{-1}Hz \subseteq H$；两边以 $z$ 共轭，得 $H \subseteq zHz^{-1}$。所以 $zHz^{-1} = H$，即 $z \in N_G(H) \setminus H$。 □

## 3.5 有限幂零群与 Sylow 分解

**定理 3.11** (有限幂零群的 Sylow 判别)**.** *有限群 $G$ 幂零，当且仅当每个 Sylow 子群正规；这又当且仅当 $G$ 是各 Sylow 子群的内部直积。*

*证明.* 先设 $G$ 幂零，取任意 Sylow $p$ 子群 $P$，令 $N = N_G(P)$。我们证明 $N_G(N) = N$。若 $g \in N_G(N)$，则 $gNg^{-1} = N$，而 $P \le N$，所以

$$gPg^{-1} \le gNg^{-1} = N.$$

$gPg^{-1}$ 与 $P$ 阶相同，且二者都是 $N$ 的 Sylow $p$ 子群。Sylow 共轭定理在 $N$ 内给出 $n \in N$，使

$$gPg^{-1} = nPn^{-1}.$$

于是

$$(n^{-1}g)P(n^{-1}g)^{-1} = P,$$

即 $n^{-1}g \in N_G(P) = N$，从而 $g \in N$。反向包含 $N \subseteq N_G(N)$ 总成立，故 $N_G(N) = N$。

若 $N < G$，正规化子条件将给出 $N < N_G(N)$，矛盾。因此 $N = G$，也就是 $P \trianglelefteq G$。$P$ 任意，所有 Sylow 子群正规。

反过来设所有 Sylow 子群 $P_1, \dots, P_s$ 正规。若 $i \neq j$, 则 $|P_i|$ 与 $|P_j|$ 互素, 因而 $P_i \cap P_j = 1$。任取 $a \in P_i, b \in P_j$。由于 $P_i$ 正规，

$$[a, b] = a(ba^{-1}b^{-1}) \in P_i;$$

由于 $P_j$ 正规，另一个改写给出

$$[a, b] = (aba^{-1})b^{-1} \in P_j.$$

故 $[a, b] \in P_i \cap P_j = 1$，即不同 Sylow 子群逐元素交换。

令 $Q_i = P_1 \cdots P_i$。由于不同 $P_i$ 的元素逐一交换，$Q_i$ 是子群；归纳地，若 $Q_{i-1}$ 已定义，则 $Q_{i-1}$ 与 $P_i$ 交换，且

$$Q_{i-1} \cap P_i = \{e\},$$

因为 $|Q_{i-1}|$ 只含 $p_1, \dots, p_{i-1}$ 这些素因子，而 $|P_i|$ 是 $p_i$ 的幂。故有限子群乘积公式给出

$$|Q_i| = \frac{|Q_{i-1}|\,|P_i|}{|Q_{i-1} \cap P_i|} = |Q_{i-1}|\,|P_i|.$$

特别地，$|Q_s| = \prod_i |P_i| = |G|$，所以 $Q_s = G$，且下述乘法映射满射。

于是乘法映射

$$\Phi : P_1 \times \cdots \times P_s \longrightarrow G, \qquad (x_1, \dots, x_s) \longmapsto x_1 \cdots x_s$$

是同态：两个坐标中的元素可以逐对交换，所以

$$\Phi(x_1, \dots, x_s)\Phi(y_1, \dots, y_s) = x_1y_1 \cdots x_sy_s = \Phi(x_1y_1, \dots, x_sy_s).$$

若 $s = 0$，则 $G$ 平凡，空直积也是平凡群。设 $s \ge 1$。若 $x_1 \cdots x_s = e$，则

$$x_s = (x_1 \cdots x_{s-1})^{-1} \in P_s \cap Q_{s-1} = \{e\}.$$

这里约定 $Q_0=\{e\}$。故 $x_s=e$；再有 $x_{s-1}\in P_{s-1}\cap Q_{s-2}=\{e\}$。如此递降至 $x_1=e$，得到核平凡。若两个元组像相同，它们之比在核中，因而两个元组相同，证明单射。结合前面的满射，$\Phi$ 是同构，得到内部直积分解。

最后，若 $G=P_1\times\cdots\times P_s$，每个 $P_i$ 是有限 $p_i$ 群，由定理 3.9 幂零；有限直积的幂零性由推论得到。因此 $G$ 幂零。 □

## 3.6　三阶单位上三角群

令

$$U_3(F)=\left\{u(a,b,c)=\begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix}:a,b,c\in F\right\}.$$

直接矩阵乘法给出

$$u(a,b,c)u(a',b',c')=u(a+a',b+b',c+c'+ab'),$$
$$u(a,b,c)^{-1}=u(-a,-b,ab-c).$$

将乘法公式逐次代入四个因子。前三个乘积的坐标依次为

$$u(a,b,c)u(a',b',c')=u(a+a',b+b',c+c'+ab'),$$
$$u(a+a',b+b',c+c'+ab')u(-a,-b,ab-c)=u(a',b',c'+ab'-a'b).$$

再乘以 $u(-a',-b',a'b'-c')$，得到

$$[u(a,b,c),u(a',b',c')]=u(0,0,ab'-a'b).$$

前两个坐标分别为 $a'$、$b'$，最后与 $(-a',-b')$ 相加成为 $0$；第三坐标为

$$(c'+ab'-a'b)+(a'b'-c')+a'(-b')=ab'-a'b.$$

因此所有交换子属于

$$C=\{u(0,0,c):c\in F\}.$$

反向地，取 $a=c$、$b=0$、$a'=0$、$b'=1$，则

$$[u(c,0,0),u(0,1,0)]=u(0,0,c),$$

所以每个 $C$ 中元素都是交换子，得到

$$U_3(F)'=C.$$

若 $u(a,b,c)$ 在中心中，则它与任意 $u(a',b',c')$ 交换，故

$$ab'-a'b=0\quad\text{对所有}a',b'\in F.$$

取 $(a',b')=(0,1)$ 得 $a=0$，取 $(1,0)$ 得 $b=0$；$c$ 任意。因此 $Z(U_3(F))=C$。矩阵 $u(0,0,c)$ 与所有元素交换，故 $C\subseteq Z(U_3(F))$，等号成立。

由导出群计算，$\gamma_2(U_3(F))=C$；因为 $C$ 位于中心，故

$$\gamma_3(U_3(F))=[C,U_3(F)]=1.$$

当 $F$ 非平凡时 $C\neq1$，所以幂零类恰为 $2$。若 $F=\mathbb{F}_p$，其阶为 $p^3$；该群也说明有限 $p$ 群的幂零类可以达到 $2$。

## 3.7 可解与幂零的区别

在 $S_3$ 中，中心元素的共轭类必须是单点。单位元以外的换位被共轭互相置换，三循环也被共轭互相置换；因此没有非单位元属于中心，得到

$$Z(S_3) = 1.$$

于是上中心列从 $Z_0 = 1$ 开始一直为 $1$，不能到达 $S_3$，所以 $S_3$ 不幂零。第二章已经计算

$$S_3' = A_3, \qquad A_3' = 1,$$

故 $S_3$ 可解。这给出可解群不必幂零的最小非交换例子。

还可以从扩张看出差别：

$$1 \longrightarrow A_3 \longrightarrow S_3 \longrightarrow C_2 \longrightarrow 1$$

的核和商群都是交换群，因而幂零；中间群却不幂零。若 $N \subseteq Z(G)$ 且 $G/N$ 的幂零类不超过 $c$，则满同态公式给出

$$\gamma_{c+1}(G) \subseteq N \subseteq Z(G),$$

再取交换子便有

$$\gamma_{c+2}(G) = [\gamma_{c+1}(G), G] = 1.$$

所以中心扩张至多使幂零类增加一层。

## 文献说明

本章核读 Milne [1] 第六章 “Nilpotent groups” 第 93–96 页，采用其上中心列、正规化子条件和有限幂零群 Sylow 判别的主线。中心列之间的等价性、有限 $p$ 群的类方程证明、$U_3(F)$ 的矩阵计算和中心扩张的类数上界均在正文中逐步写出。

# 4　直积、半直积与群扩张

本章先对任意群核建立直积与半直积；从集合截面和二余循环开始的扩张分类则假定核交换，并固定商在核上的作用。这里的扩张等价要求保持指定的核与商映射，条件强于中间群抽象同构。一般非交换核的因子集及其障碍不在本章建立；互素阶条件下的可解有限群分裂与补群共轭在第八章证明。

## 4.1　从唯一分解到乘法公式

第一章已经给出两个不能由合成因子区别的群：$C_4$ 与 $C_2 \times C_2$。更精确地说，它们都含有一个阶为 2 的正规子群，商群也都是 $C_2$。因此，指定核与商群以后，还必须描述它们如何组合。先研究存在一个子群与核互补的情形。

**定义 4.1** (补子群)**.** 设 $N \trianglelefteq G$。若 $H \leq G$ 满足

$$NH = G, \qquad N \cap H = \{e\},$$

称 $H$ 是 $N$ 在 $G$ 中的补子群。不同的补子群可以给出不同的分解坐标。

**命题 4.2** (唯一分解与共轭作用)**.** 设 $N \trianglelefteq G$，$H$ 是 $N$ 的补子群。则每个 $g \in G$ 唯一表示为 $nh$，其中 $n \in N, h \in H$。公式

$$\theta(h)(n) = hnh^{-1}$$

定义同态 $\theta : H \to \mathrm{Aut}(N)$，且

$$(nh)(mk) = n\theta(h)(m)hk.$$

称这种分解为内部半直积分解。

*证明.* $NH = G$ 保证存在性。若 $nh = mk$，则

$$m^{-1}n = kh^{-1} \in N \cap H = \{e\},$$

所以 $n = m$、$h = k$，表示唯一。

由 $N \trianglelefteq G$，共轭 $n \mapsto hnh^{-1}$ 将 $N$ 送到自身，且

$$h(n_1n_2)h^{-1} = (hn_1h^{-1})(hn_2h^{-1}).$$

其逆是以 $h^{-1}$ 共轭，故为自同构。对 $h, k \in H$、$n \in N$，

$$\theta(hk)(n) = hknk^{-1}h^{-1} = \theta(h)(\theta(k)(n)).$$

因此 $\theta(hk) = \theta(h)\theta(k)$。最后，

$$(nh)(mk) = n(hmh^{-1})hk = n\theta(h)(m)hk.$$

这从原群的乘法推导出坐标乘法。 □

## 4.2 外部半直积的构造

**定理 4.3** (半直积的群公理)**.** 给定群 $N, H$ 和同态 $\theta : H \to \mathrm{Aut}(N)$，在集合 $N \times H$ 上定义

$$(n,h)(m,k) = (n\theta(h)(m), hk).$$

这使它成为群，记为 $N \rtimes_\theta H$。单位元为 $(e_N, e_H)$，逆元为

$$(n,h)^{-1} = (\theta(h^{-1})(n^{-1}), h^{-1}).$$

证明. 自同构 $\theta(h)$ 将 $m$ 送到 $N$，故乘法封闭。对三个元素，左结合为

$$((n,h)(m,k))(l,t) = (n\theta(h)(m)\theta(hk)(l), (hk)t),$$

右结合为

$$\begin{aligned}(n,h)((m,k)(l,t)) &= (n\theta(h)(m\theta(k)(l)), h(kt)) \\ &= (n\theta(h)(m)\theta(h)\theta(k)(l), h(kt)).\end{aligned}$$

$N, H$ 各自结合，且 $\theta(hk) = \theta(h)\theta(k)$，所以两式相同。

因 $\theta(e_H) = \mathrm{id}_N$ 且 $\theta(h)(e_N) = e_N$，有

$$(e_N, e_H)(n,h) = (n,h), \qquad (n,h)(e_N, e_H) = (n,h).$$

记 $v = (\theta(h^{-1})(n^{-1}), h^{-1})$。左右乘分别得到

$$(n,h)v = (n\theta(h)\theta(h^{-1})(n^{-1}), e_H) = (e_N, e_H),$$

$$v(n,h) = (\theta(h^{-1})(n^{-1})\theta(h^{-1})(n), e_H) = (e_N, e_H).$$

群公理全部成立。 □

定义

$$i(n) = (n, e_H), \qquad j(h) = (e_N, h), \qquad \pi(n,h) = h.$$

则

$$i(n)i(m) = i(nm), \quad j(h)j(k) = j(hk), \quad \pi((n,h)(m,k)) = hk = \pi(n,h)\pi(m,k).$$

坐标相等说明 $i, j$ 单射；每个 $h$ 都是 $(e_N, h)$ 的像，说明 $\pi$ 满射。其核为 $i(N)$，所以 $i(N)$ 正规。又有

$$(n,h) = i(n)j(h), \qquad i(N) \cap j(H) = \{(e_N, e_H)\}.$$

因此 $j(H)$ 是 $i(N)$ 的补子群。所实现的共轭作用正是原给定作用：

$$j(h)i(n)j(h)^{-1} = (\theta(h)(n), e_H) = i(\theta(h)(n)).$$

**命题 4.4** (内部与外部构造相符)**.** 在命题 *4.2* 的条件下，映射

$$\Psi : N \rtimes_\theta H \longrightarrow G, \qquad (n,h) \longmapsto nh$$

是同构。

证明. 每个输入是确定的有序对，不涉及代表选择。乘法公式给出

$$\Psi((n,h)(m,k)) = n\theta(h)(m)hk = (nh)(mk) = \Psi(n,h)\Psi(m,k).$$

$NH = G$ 给出满射；若 $nh = mk$，唯一表示给出 $n = m, h = k$，所以单射。 □

**命题 4.5** (内部直积与平凡作用)**.** *在内部半直积分解中，以下条件等价：作用 $\theta$ 平凡；$N$ 与 $H$ 逐元素交换；$H \trianglelefteq G$。这些条件成立时 $\Psi : N \times H \to G$ 是直积同构。*

证明. $\theta(h)(n) = n$ 等价于 $hn = nh$，故前两项等价。若逐元素交换，任意 $g = nh$ 和 $k \in H$ 满足

$$gkg^{-1} = n(hkh^{-1})n^{-1} = hkh^{-1} \in H.$$

用 $g^{-1}$ 代入得反向包含，所以 $H \trianglelefteq G$。

若 $H \trianglelefteq G$，对 $n \in N, h \in H$，

$$[h,n] = h(nh^{-1}n^{-1}) \in H, \qquad [h,n] = (hnh^{-1})n^{-1} \in N.$$

故 $[h,n] \in H \cap N = 1$，二者交换。作用平凡时半直积乘法化为 $(n,h)(m,k) = (nm, hk)$；命题 4.4 给出直积同构。 □

这里比较的是给定两个子群与给定坐标的乘法；某个抽象群是否还具有其他直积分解，需要另行判断。

**命题 4.6** (改变核与商的坐标)**.** *设 $\theta : H \to \mathrm{Aut}(N)$、$\eta : K \to \mathrm{Aut}(M)$ 为作用。若同构 $\alpha : N \to M$、$\beta : H \to K$ 满足*

$$\alpha(\theta(h)(n)) = \eta(\beta(h))(\alpha(n)) \quad (h \in H, n \in N),$$

*则 $F(n,h) = (\alpha(n), \beta(h))$ 是 $N \rtimes_\theta H$ 到 $M \rtimes_\eta K$ 的同构。*

证明.

$$\begin{aligned} F((n,h)(m,k)) &= (\alpha(n)\alpha(\theta(h)(m)), \beta(h)\beta(k)) \\ &= (\alpha(n)\eta(\beta(h))(\alpha(m)), \beta(h)\beta(k)) \\ &= F(n,h)F(m,k). \end{aligned}$$

$\alpha, \beta$ 均为双射，其坐标乘积 $F$ 也是双射，逆映射为 $(u,v) \mapsto (\alpha^{-1}(u), \beta^{-1}(v))$。 □

## 4.3 旋转、仿射变换与上三角矩阵

在 $C_n = \mathbb{Z}/n\mathbb{Z}$ 上，$a \mapsto -a$ 是加法群自同构，平方为恒等。因此 $C_2$ 通过反演作用，得到

$$(a,\varepsilon)(b,\delta) = (a + (-1)^\varepsilon b, \varepsilon + \delta).$$

第一个坐标模 $n$，第二个坐标模 2。取 $r = (1,0)$、$s = (0,1)$，则

$$r^n = e, \qquad s^2 = e, \qquad srs^{-1} = r^{-1}.$$

每个元素唯一写为 $r^a s^\varepsilon$。若 $n \geq 3$，把正 $n$ 边形的顶点编号为 $j \in \mathbb{Z}/n\mathbb{Z}$，则 $(a,\varepsilon)$ 对顶点的作用为

$$j \longmapsto a + (-1)^\varepsilon j.$$

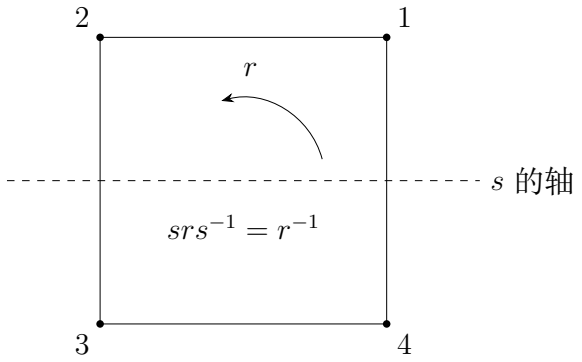



图 4.1: 正方形的旋转与反射

复合给出上述乘法。若这个作用为恒等，则代入 $j = 0$ 得 $a = 0$；代入 $j = 1$ 得 $(-1)^{\varepsilon} = 1 \pmod{n}$，因 $n \geq 3$，必有 $\varepsilon = 0$。故作用忠实。这些作用都是旋转或反射；任意平面等距对称由一个顶点的像与相邻方向确定，所以恰由这 $2n$ 个作用穷尽。该半直积即 $D_{2n}$。

图 4.1 中 $r$ 使 $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1$，$s$ 是关于水平轴的反射。因此 $s = (14)(23)$，直接按字母共轭得到

$$s(1234)s^{-1} = (4321) = (1432) = r^{-1}.$$

**例 4.7** (仿射群)**.** 取 $N = (F, +)$、$H = F^{\times}$，定义 $\theta(a)(b) = ab$。分配律给出加性，乘以 $a^{-1}$ 给出逆，且 $\theta(ac) = \theta(a)\theta(c)$。乘法为

$$(b, a)(d, c) = (b + ad, ac).$$

令 $T_{a,b}(x) = ax + b$，则

$$T_{a,b} \circ T_{c,d}(x) = acx + ad + b = T_{ac,b+ad}(x).$$

因此 $(b, a) \mapsto T_{a,b}$ 保持运算。若两个像相同，在 0 的值相同给出 $b = d$，在 1 的值相同给出 $a + b = c + d$，因而 $a = c$，所以单射。每个仿射变换都由这样的 $a, b$ 给出，故满射，得到

$$\mathrm{Aff}(F) \cong (F, +) \rtimes F^{\times}.$$

**例 4.8** (上三角群的分裂)**.** 令 $B_n(F)$ 为可逆上三角矩阵群，$U_n(F)$ 为单位上三角群，$T_n(F)$ 为可逆对角矩阵群。第二章的对角同态以 $U_n(F)$ 为核，故 $U_n(F) \trianglelefteq B_n(F)$。任取 $B = (b_{ij}) \in B_n(F)$，令

$$D = \mathrm{diag}(b_{11}, \ldots, b_{nn}), \qquad U = BD^{-1}.$$

$U$ 的对角线全为 1，故 $B = UD$，且 $U_n(F) \cap T_n(F) = \{I\}$。因此

$$B_n(F) \cong U_n(F) \rtimes T_n(F).$$

若 $D = \mathrm{diag}(d_1, \ldots, d_n)$，则

$$(DUD^{-1})_{ij} = d_i u_{ij} d_j^{-1}.$$

这明确给出作用。若 $n \geq 2$ 且 $|F| > 2$，可取 $d_1/d_2 \neq 1$，作用在 $u_{12} = 1$ 的矩阵上非平凡；若 $F = \mathbb{F}_2$，对角群平凡。这个边界不能从“上三角”三个字中省去。

## 4.4 短正合列与分裂

**定义 4.9** (扩张与截面)**.** 群的短正合列

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

表示 $i$ 是单同态、$\pi$ 是满同态，且 $\operatorname{im} i = \ker \pi$。称它为 $Q$ 通过 $N$ 的扩张。若存在同态 $s : Q \to G$ 满足 $\pi \circ s = \mathrm{id}_Q$，称扩张分裂，$s$ 称为同态截面。只满足这个右逆等式的集合映射称为集合截面。

核 $i(N)$ 正规于 $G$，因为 $\pi(gxg^{-1}) = \pi(g)e\pi(g)^{-1} = e$ 对 $x \in \ker\pi$ 成立，再以 $g^{-1}$ 共轭得到等号。以下的扩张分裂指这条带有指定 $i, \pi$ 的列分裂。

**定理 4.10** (分裂、补子群与半直积)**.** *短正合列分裂，当且仅当 $\ker\pi$ 在 $G$ 中有补子群。若 $s$ 为同态截面，定义*

$$\theta(x)(n) = i^{-1}\big(s(x)i(n)s(x)^{-1}\big).$$

*则 $\theta : Q \to \mathrm{Aut}(N)$ 为作用，映射*

$$F : N \rtimes_\theta Q \longrightarrow G, \qquad (n, x) \longmapsto i(n)s(x)$$

*为同构，且 $\pi F(n, x) = x$。*

*证明.* 若 $s$ 是截面，则 $s$ 单射：$s(x) = s(y)$ 蕴含 $x = \pi s(x) = \pi s(y) = y$。令 $H = s(Q)$，同态像是子群，且 $\pi|_H$ 与 $s$ 互逆。若 $s(x) \in \ker\pi$，则 $x = \pi s(x) = e$，所以 $s(x) = e$，得到 $H \cap \ker\pi = 1$。对任意 $g \in G$，

$$g = (gs(\pi(g))^{-1})s(\pi(g)), \qquad \pi(gs(\pi(g))^{-1}) = \pi(g)\pi(g)^{-1} = e.$$

故 $G = (\ker\pi)H$，$H$ 是补子群。

反之，若 $H$ 是补子群，$\pi|_H$ 的核为 $H \cap \ker\pi = 1$，所以单射；每个 $g = nh$ 满足 $\pi(g) = \pi(h)$，而 $\pi$ 满射，所以 $\pi|_H$ 满射。它的逆 $s$ 保持乘法：$s(x)s(y) \in H$ 且投影为 $xy$，由唯一性必等于 $s(xy)$。于是得到同态截面。

$\theta$ 是把命题 4.2 的共轭作用沿同构 $i : N \to \ker\pi$ 和 $s : Q \to H$ 运输回来，所以为作用。显式地，$s(xy) = s(x)s(y)$ 给出

$$i(\theta(xy)(n)) = s(x)s(y)i(n)s(y)^{-1}s(x)^{-1} = i(\theta(x)\theta(y)(n)).$$

$i$ 单射，故作用的乘法律成立。映射 $F$ 满足

$$\begin{aligned} F(n, x)F(m, y) &= i(n)s(x)i(m)s(x)^{-1}s(xy) \\ &= i(n\theta(x)(m))s(xy) = F((n, x)(m, y)). \end{aligned}$$

上面的分解保证满射。若 $i(n)s(x) = i(m)s(y)$，投影后得 $x = y$，再消去 $s(x)$ 得 $i(n) = i(m)$，所以 $n = m$，证明单射。 □

**例 4.11** (不分裂的循环扩张)**.** 设 $p$ 为素数。在加法群中定义

$$i : C_p \to C_{p^2}, \quad [b]_p \mapsto [pb]_{p^2}, \qquad \pi : C_{p^2} \to C_p, \quad [a]_{p^2} \mapsto [a]_p.$$

$i$ 的代表相差 $p$ 的倍数时像相差 $p^2$ 的倍数，故良定义；$[pb]_{p^2}=0$ 当且仅当 $p\mid b$，故单射。$\pi$ 良定义且满射，两者都保持加法，且 $\ker\pi=p\mathbb{Z}/p^2\mathbb{Z}=\operatorname{im} i$，所以短列正合。

若有同态截面，写 $s([1]_p)=[a]_{p^2}$。截面条件给出 $a\equiv 1 \pmod p$；同态性却给出

$$p[a]_{p^2}=s(p[1]_p)=s(0)=0,$$

所以 $p^2\mid pa$，即 $p\mid a$，矛盾。这个扩张不分裂。

## 4.5 交换核、集合截面与二余循环

现在固定短正合列

$$1\longrightarrow A\xrightarrow{i}G\xrightarrow{\pi}Q\longrightarrow 1,$$

其中 $A$ 交换，写成加法群。下文仍把 $G,Q$ 写成乘法群。选择归一化集合截面 $s:Q\to G$，即

$$\pi(s(x))=x,\qquad s(e)=e.$$

这只是每个纤维中选一个代表；有限 $Q$ 时是有限次选择，一般情形在第一册的选择公理框架下选取。

**命题 4.12** (商群在交换核上的作用)**.** *公式*

$$i(x\cdot a)=s(x)i(a)s(x)^{-1}$$

*给出 $Q$ 在 $A$ 上通过加法群自同构的作用。这个作用不依赖集合截面的选择。*

*证明.* 右侧投影为 $xe_Qx^{-1}=e_Q$，所以属于 $\ker\pi=\operatorname{im} i$；$i$ 单射使 $x\cdot a$ 唯一。共轭保持乘法，所以

$$i(x\cdot(a+b))=s(x)i(a)i(b)s(x)^{-1}=i(x\cdot a)i(x\cdot b)=i(x\cdot a+x\cdot b).$$

$i$ 单射，故 $a\mapsto x\cdot a$ 加性；逆共轭给出逆映射，所以它是加法群自同构。

若 $t(x)$ 是另一个提升，则 $t(x)s(x)^{-1}\in\ker\pi$，故可写 $t(x)=i(b)s(x)$。因 $A$ 交换，

$$t(x)i(a)t(x)^{-1}=i(b)\big(s(x)i(a)s(x)^{-1}\big)i(-b)=i(x\cdot a).$$

所以作用与提升无关。$s(x)s(y)$ 是 $xy$ 的一个提升，于是

$$i((xy)\cdot a)=s(x)s(y)i(a)s(y)^{-1}s(x)^{-1}=i(x\cdot(y\cdot a)).$$

$i$ 单射使 $(xy)\cdot a=x\cdot(y\cdot a)$。又由 $s(e)=e$ 得 $e\cdot a=a$，作用公理成立。 □

因 $s(x)s(y)s(xy)^{-1}$ 属于核，存在唯一 $c(x,y)\in A$ 满足

$$s(x)s(y)=i(c(x,y))s(xy).$$

每个 $g\in G$ 唯一写成 $i(a)s(x)$：投影确定 $x=\pi(g)$，然后 $gs(x)^{-1}$ 唯一确定 $a$。将群元素暂记为坐标 $(a,x)$，直接相乘得到

$$\begin{aligned}i(a)s(x)i(b)s(y)&=i(a)\big(s(x)i(b)s(x)^{-1}\big)s(x)s(y)\\&=i(a+x\cdot b+c(x,y))s(xy).\end{aligned}$$

所以坐标乘法为

$$(a,x)(b,y)=(a+x\cdot b+c(x,y),xy).\tag{4.1}$$

**定理 4.13** (二余循环与扩张的构造)**.** 上述 $c : Q \times Q \to A$ 满足归一化条件

$$c(e, x) = c(x, e) = 0$$

及二余循环等式

$$c(x, y) + c(xy, z) = x \cdot c(y, z) + c(x, yz). \tag{4.2}$$

反之，给定 $Q$ 在交换群 $A$ 上的作用和满足这些条件的 $c$，式 (4.1) 定义一个群，记为 $E_c$；它给出具有该指定作用的扩张

$$1 \longrightarrow A \xrightarrow{i_c} E_c \xrightarrow{\pi_c} Q \longrightarrow 1, \qquad i_c(a) = (a, e), \quad \pi_c(a, x) = x.$$

证明. 由 $s(e) = e$，

$$s(e)s(x) = s(x) = i(0)s(x), \qquad s(x)s(e) = s(x) = i(0)s(x),$$

唯一性给出归一化。原群结合律使 $(s(x)s(y))s(z) = s(x)(s(y)s(z))$。两边分别是

$$i(c(x, y) + c(xy, z))s(xyz)$$

和

$$i(x \cdot c(y, z) + c(x, yz))s(xyz),$$

消去末尾代表并用 $i$ 单射，得到 (4.2)。

反向构造中乘法封闭。三元乘积左结合的第一坐标为

$$a + x \cdot b + c(x, y) + (xy) \cdot d + c(xy, z),$$

右结合的第一坐标为

$$a + x \cdot b + (xy) \cdot d + x \cdot c(y, z) + c(x, yz).$$

等式 (4.2) 使二者相同，第二坐标都是 $xyz$，故结合。归一化给出

$$(0, e)(a, x) = (a, x) = (a, x)(0, e).$$

对 $(a, x)$，令

$$b = -x^{-1} \cdot a - x^{-1} \cdot c(x, x^{-1}).$$

则 $(a, x)(b, x^{-1})$ 的第一坐标为 $a + x \cdot b + c(x, x^{-1}) = 0$。代入 (4.2) 中的 $(x^{-1}, x, x^{-1})$ 得

$$c(x^{-1}, x) = x^{-1} \cdot c(x, x^{-1}).$$

因此反向乘积的第一坐标也为

$$b + x^{-1} \cdot a + c(x^{-1}, x) = 0,$$

第二坐标均为 $e$，所以 $(b, x^{-1})$ 是双侧逆元。

$i_c$ 满足 $(a, e)(b, e) = (a + b, e)$，且单射；$\pi_c$ 保持乘法，因每个 $x$ 有原像 $(0, x)$ 而满射，其核正是 $A \times \{e\} = \operatorname{im} i_c$。最后，

$$(0, x)(a, e) = (x \cdot a, x) = (x \cdot a, e)(0, x),$$

说明共轭在核上的作用正是 $a \mapsto x \cdot a$。 □

## 4.6 截面变化与扩张等价

若把 $s$ 改为另一个归一化截面 $s_b(x)=i(b(x))s(x)$，其中 $b:Q\to A$ 满足 $b(e)=0$，则

$$\begin{aligned}s_b(x)s_b(y)&=i(b(x)+x\cdot b(y))s(x)s(y)\\&=i(b(x)+x\cdot b(y)+c(x,y)-b(xy))s_b(xy).\end{aligned}$$

因此新二余循环为

$$c_b(x,y)=c(x,y)+b(x)+x\cdot b(y)-b(xy). \tag{4.3}$$

定义

$$(\delta b)(x,y)=b(x)+x\cdot b(y)-b(xy).$$

这是二上边界。这里的负号来自把旧代表 $s(xy)$ 改写为 $i(-b(xy))s_b(xy)$，不能省略。

**定义 4.14** (固定作用的二上同调群)**.** 固定作用 $Q\to\mathrm{Aut}(A)$。所有归一化二余循环在逐点相加下构成的群记为 $Z^2(Q,A)$；所有 $\delta b$（$b(e)=0$）构成的群记为 $B^2(Q,A)$。定义

$$H^2(Q,A)=Z^2(Q,A)/B^2(Q,A).$$

这些定义中的子群条件必须验证。二余循环等式在 $A$ 中是加法等式，故零函数、和、负函数均满足，归一化也保留，所以 $Z^2$ 是交换群。$b\mapsto\delta b$ 加性，故其像是加法子群。由 $b(e)=0$，

$$\delta b(e,x)=0+b(x)-b(x)=0,\qquad \delta b(x,e)=b(x)+x\cdot 0-b(x)=0.$$

再计算

$$\begin{aligned}\delta b(x,y)+\delta b(xy,z)&=b(x)+x\cdot b(y)+(xy)\cdot b(z)-b(xyz),\\ x\cdot\delta b(y,z)+\delta b(x,yz)&=b(x)+x\cdot b(y)+(xy)\cdot b(z)-b(xyz).\end{aligned}$$

所以 $B^2\subseteq Z^2$，商群有定义。

**定义 4.15** (扩张等价)**.** 两条扩张 $A\xrightarrow{i}G\xrightarrow{\pi}Q$ 与 $A\xrightarrow{i'}G'\xrightarrow{\pi'}Q$ 等价，是指存在同构 $F:G\to G'$ 满足

$$F\circ i=i',\qquad \pi'\circ F=\pi.$$

即下面的图交换：

$$\begin{array}{ccccccccc}1&\longrightarrow&A&\xrightarrow{i}&G&\xrightarrow{\pi}&Q&\longrightarrow&1\\&&\Vert&&\downarrow F&&\Vert&&\\1&\longrightarrow&A&\xrightarrow[i']{}&G'&\xrightarrow[\pi']{}&Q&\longrightarrow&1\end{array}$$

这里核 $A$ 和商 $Q$ 的标记固定；这比只要求中间群抽象同构更严格。

**定理 4.16** (交换核扩张的分类)**.** 固定 $Q$ 在 $A$ 上的作用。具有该作用的扩张等价类与 $H^2(Q,A)$ 的元素一一对应。扩张分裂当且仅当对应类为 0。

证明. 任意扩张选归一化截面，得到 $c$。由式 (4.3)，换截面只增加二上边界，故 $[c]$ 不变。若 $F$ 是扩张等价，$F\circ s$ 是另一条扩张的截面，且

$$F(s(x))F(s(y))=F(i(c(x,y))s(xy))=i'(c(x,y))F(s(xy)),$$

所以此截面的二余循环仍为 $c$，类对等价也不变。

还要把原扩张与坐标模型联系起来。映射

$$\Phi_s : E_c \longrightarrow G, \qquad (a,x) \longmapsto i(a)s(x)$$

由唯一坐标表示为双射；式 (4.1) 的推导给出

$$\Phi_s((a,x)(d,y)) = i(a + x\cdot d + c(x,y))s(xy) = \Phi_s(a,x)\Phi_s(d,y).$$

又有 $\Phi_s(a,e) = i(a)$、$\pi\Phi_s(a,x) = x$，所以它是扩张等价。

反过来，每个 $c \in Z^2$ 都给出扩张 $E_c$，故每个类都能实现。若 $c' = c + \delta b$，定义

$$F_b : E_{c'} \longrightarrow E_c, \qquad (a,x) \longmapsto (a + b(x), x).$$

比较乘法的第一坐标：

$$\begin{aligned} F_b((a,x)\cdot_{c'}(d,y))_1 &= a + x\cdot d + c'(x,y) + b(xy) \\ &= a + x\cdot d + c(x,y) + b(x) + x\cdot b(y), \\ (F_b(a,x)\cdot_c F_b(d,y))_1 &= a + b(x) + x\cdot(d + b(y)) + c(x,y). \end{aligned}$$

两式相同，第二坐标同为 $xy$，故 $F_b$ 为同态。它的逆为 $(a,x)\mapsto(a - b(x),x)$，所以双射。因 $b(e) = 0$，它在核上恒等，且保持投影，故为扩张等价。

还要证明等价不把不同的类混在一起。若 $F : E_{c'} \to E_c$ 是扩张等价，保持投影迫使

$$F(0,x) = (b(x),x), \qquad b(e) = 0.$$

保持核标记和乘法使

$$F(a,x) = F((a,e)(0,x)) = (a + b(x),x).$$

把 $(0,x)(0,y)$ 代入同态条件，得到

$$c'(x,y) + b(xy) = b(x) + x\cdot b(y) + c(x,y),$$

即 $c' = c + \delta b$。因此类相同当且仅当扩张等价。

若扩张有同态截面，其二余循环恒为 0，所以类为零。若 $[c] = 0$，可写 $c = \delta b$，用截面变化 $-b$ 得到 $c_{-b} = 0$；于是 $s_{-b}(x)s_{-b}(y) = s_{-b}(xy)$，新截面是同态，扩张分裂。 □

## 4.7 循环商的中心扩张：进位与模掉倍数

这一节设 $Q = C_m$, $m \ge 2$, 并假定作用平凡。由命题 4.12, 平凡作用等价于 $i(A) \subseteq Z(G)$：每个 $g = i(a)s(x)$ 在核上的共轭就是 $x$ 的作用。这样的扩张称为中心扩张。

令 $\bar t$ 是 $C_m$ 的生成元，取提升 $t \in G$，即 $\pi(t) = \bar t$。则存在唯一 $z \in A$ 使

$$t^m = i(z).$$

任意 $g \in G$ 唯一写为

$$i(a)t^r, \qquad a \in A, \quad 0 \le r < m.$$

因为投影先唯一确定 $r$，再由 $i$ 单射确定 $a$。定义进位函数

$$\kappa(r,s) = \left\lfloor \frac{r+s}{m} \right\rfloor \quad (0 \le r,s < m).$$

它只取 $0,1$。用 $i(A)$ 中心性计算

$$(i(a)t^r)(i(b)t^s) = i(a+b+\kappa(r,s)z)t^{r+s-m\kappa(r,s)}.$$

所以该扩张的二余循环为

$$c_z(\bar{t}^r,\bar{t}^s) = \kappa(r,s)z.$$

三项相加的总进位满足

$$\kappa(r,s)+\kappa((r+s) \bmod m,u) = \left\lfloor \frac{r+s+u}{m} \right\rfloor = \kappa(s,u)+\kappa(r,(s+u) \bmod m),$$

故 $c_z$ 确实满足二余循环等式；任何 $z\in A$ 都给出扩张 $E_{c_z}$。

**定理 4.17** (循环中心扩张的参数)**.** 固定平凡作用。上述扩张的等价类由

$$A/mA, \qquad mA=\{ma : a\in A\}$$

参数化；参数为 $z+mA$。因此

$$H^2(C_m,A)\cong A/mA.$$

扩张分裂当且仅当 $z\in mA$。

证明. 若另取提升 $t'=i(a)t$，中心性给出

$$(t')^m = i(ma)t^m = i(ma+z),$$

所以参数只增加 $mA$ 中的元素。所有扩张都由某个 $z$ 的进位坐标描述，前面的唯一表达与乘法计算给出到 $E_{c_z}$ 的等价。

若 $F:E_{c_z}\to E_{c_w}$ 是扩张等价，目标标准提升记作 $t_w$，则 $F(t_z)=i(a)t_w$，因为二者投影均为 $\bar{t}$。于是

$$i(z)=F(t_z^m)=F(t_z)^m=i(ma+w),$$

故 $z-w\in mA$。反之，若 $z=w+ma$，在目标中选新提升 $t'=i(a)t_w$，则 $(t')^m=i(z)$。以此提升给出的坐标映射

$$i(b)t_z^r \longmapsto i(b)(t')^r$$

保持核和投影；两边使用同一个进位参数 $z$，所以保持上面逐项写出的乘法。每个目标元在 $t'$ 坐标下唯一表示，因此它是双射，得到扩张等价。

为验证群同构的加法相容，映射 $z\mapsto[c_z]$ 加性，因为 $c_{z+w}=c_z+c_w$。它满射，因为每个扩张都具有进位坐标；其核由刚证明的等价判别恰为 $mA$。因此诱导 $A/mA\to H^2(C_m,A)$ 的双射同态，给出所述同构。

若 $z\in mA$，选 $a$ 使 $ma=-z$，则提升 $t'=i(a)t$ 满足 $(t')^m=e$。故 $\bar{t}^r\mapsto(t')^r$ 是良定义的同态截面。反之，同态截面给出一个 $m$ 次幂为 $e$ 的提升，必须满足 $z+ma=0$，所以 $z\in mA$。 □

**例 4.18** (两个阶四群来自两个扩张类)**.** 取 $A=C_2$、$m=2$，则 $2A=0$，所以 $A/2A=C_2$。$z=0$ 时乘法无进位，得到 $C_2\times C_2$；每个元素的二倍为零。

$z=1$ 时，令 $t=(0,\bar{t})$，则 $t^2=(1,e)\neq e$、$t^4=e$，而

$$e=(0,e),\quad t=(0,\bar{t}),\quad t^2=(1,e),\quad t^3=(1,\bar{t})$$

穷尽四个元素。因此 $k+4\mathbb{Z}\mapsto t^k$ 良定义、保持加法到乘法、满射，且四个剩余类像不同，所以为同构 $C_4\cong E_{c_1}$。两类不同，因为 $1\notin 2A$；中间群也不同构，因为一个有阶四元素，另一个没有。

**例 4.19** (无限循环核也有不分裂扩张)**.** 取 $A=\mathbb{Z}$、$z=1$，得到以 $\mathbb{Z}/m\mathbb{Z}$ 为参数集的中心扩张类中的一个。其模型为

$$0\longrightarrow\mathbb{Z}\xrightarrow{a\mapsto ma}\mathbb{Z}\xrightarrow{k\mapsto k+m\mathbb{Z}}C_m\longrightarrow 0.$$

中间群生成元 $t=1$ 的 $m$ 倍恰是核元素 $i(1)=m$，所以参数为 $1+m\mathbb{Z}$。它不分裂：若截面把 $1+m\mathbb{Z}$ 送到 $k\in\mathbb{Z}$，同态性迫使 $mk=0$，故 $k=0$，其投影不可能为 $1+m\mathbb{Z}$。这说明不分裂现象并不限于有限核。

## 4.8　非平凡作用：二面体群与四元数群

前面的循环中心扩张要求作用平凡。一个非平凡作用的完整计算能说明为什么不能把 $A/mA$ 公式无条件套用。

取 $A=\mathbb{Z}/4\mathbb{Z}$、$Q=\mathbb{Z}/2\mathbb{Z}$，令 $1\in Q$ 通过反演作用于 $A$。这一节 $Q$ 使用加法记号，二余循环公式中的 $xy$ 相应写成 $x+y$。归一化使 $c(0,x)=c(x,0)=0$，所以整个二余循环只由

$$k=c(1,1)\in\mathbb{Z}/4\mathbb{Z}$$

决定。对 $(1,1,1)$ 代入二余循环等式，得到 $k=-k$，即 $2k=0$，所以 $k=0$ 或 $2$。若三个指标中有一个为 $0$，则等式两边直接约为同一个值；故这两种 $k$ 都确实给出二余循环。

对任意归一化 $b:Q\to A$，有

$$\delta b(1,1)=b(1)-b(1)-b(0)=0.$$

所以 $B^2=0$，恰有两个扩张等价类，其乘法为

$$(a,\varepsilon)(b,\delta)=(a+(-1)^{\varepsilon}b+k\varepsilon\delta,\varepsilon+\delta \bmod 2).$$

第一坐标模 $4$，$\varepsilon,\delta$ 用 $0,1$ 代表。$k=0$ 是半直积 $C_4\rtimes C_2=D_8$。$k=2$ 时令 $r=(1,0)$、$s=(0,1)$，则

$$r^4=e,\qquad s^2=r^2,\qquad srs^{-1}=r^{-1}.$$

每个元素仍唯一写成 $r^as^{\varepsilon}$。对 $\varepsilon=1$ 的四个元素，

$$(a,1)^2=(a-a+2,0)=(2,0)\neq e.$$

因此没有位于非平凡商陪集中的阶二元素，扩张不能分裂。

这个群可以在复矩阵中明确实现。令 $\mathrm{i}^2=-1$，取

$$R=\begin{pmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{pmatrix},\qquad S=\begin{pmatrix}0&1\\-1&0\end{pmatrix}.$$

矩阵乘法给出 $R^2=S^2=-I$、$R^4=I$、$SRS^{-1}=R^{-1}$。故

$$(R^aS^{\varepsilon})(R^bS^{\delta})=R^{a+(-1)^{\varepsilon}b+2\varepsilon\delta}S^{\varepsilon+\delta \bmod 2}.$$

这恰好是 $k=2$ 的乘法，故 $(a,\varepsilon)\mapsto R^aS^\varepsilon$ 是同态。四个 $R^a$ 是不同的对角矩阵，四个 $R^aS$ 是不同的非零反对角矩阵，两个集合不交，所以此映射单射。其像是八个矩阵组成的群，定义为四元数群 $Q_8$，映射对这个像满射，所以给出 $E_{c_2}\cong Q_8$。

两种中间群也确实不同构：$Q_8$ 只有一个阶二元素 $r^2$；在 $D_8$ 中，$r^2$ 及四个 $r^as$ 都是阶二元素。群同构保持元素阶，所以不可能同构。这一对例子具有同一个核 $C_4$、同一个商 $C_2$，甚至同一个共轭作用；仍须用二余循环才能区别。

## 4.9 补子群的变化与一余循环

二余循环记录扩张能否分裂；扩张已经分裂以后，还可以问补子群有多少个。设

$$G=A\rtimes Q,\qquad (a,x)(b,y)=(a+x\cdot b,xy),$$

其中 $A$ 仍交换。任意同态截面都形如 $s_b(x)=(b(x),x)$。它保持乘法当且仅当

$$b(xy)=b(x)+x\cdot b(y). \tag{4.4}$$

这样的 $b$ 称为一余循环，所有这些函数的加法群记为 $Z^1(Q,A)$。将 $x=y=e$ 代入得 $b(e)=0$，所以无需另加归一化。这个集合确实是加法群。零函数满足式 (4.4)；若 $b,d$ 满足该式，则作用的加性给出

$$\begin{aligned}(b+d)(xy)&=b(x)+x\cdot b(y)+d(x)+x\cdot d(y)\\&=(b+d)(x)+x\cdot(b+d)(y),\\(-b)(xy)&=-b(x)+x\cdot(-b(y)).\end{aligned}$$

故它对和与负函数封闭，结合律与交换律由 $A$ 的逐点加法继承。

**命题 4.20** (补子群与一余循环)**.** *补子群与 $Z^1(Q,A)$ 一一对应；两个补子群由核 $A$ 中的元素共轭，当且仅当对应的一余循环之差形如*

$$d_a(x)=a-x\cdot a\qquad (a\in A).$$

*因此，核共轭意义下的补子群类由*

$$H^1(Q,A)=Z^1(Q,A)/\{d_a:a\in A\}$$

*参数化。*

*证明.* 补子群上投影是同构，故其逆唯一给出同态截面；反过来，同态截面的像是补子群，已由定理 4.10 证明。截面的坐标形式唯一，故与满足 (4.4) 的 $b$ 一一对应。

以核元素 $(a,e)$ 共轭，有

$$(a,e)(b(x),x)(a,e)^{-1}=(b(x)+a-x\cdot a,x).$$

所以共轭正对应于增加 $d_a$。若两条图像子群在此共轭下相同，每个投影 $x$ 的元素唯一，因此函数逐点相差 $d_a$，反向也由公式成立。

还须检查分母子群有定义。$d_a$ 满足

$$d_a(x)+x\cdot d_a(y)=a-x\cdot a+x\cdot(a-y\cdot a)=a-(xy)\cdot a=d_a(xy).$$

所以 $d_a\in Z^1$；并有 $d_{a+a'}=d_a+d_{a'}$。分母是加法子群，商群有定义。上述共轭判别说明商群元素恰好参数化核共轭类。 □

**例 4.21** (仿射群中的补子群是定点稳定子)**.** 设 $|F|>2$，取 $A=(F,+)$、$Q=F^{\times}$，作用为乘法。一余循环条件是

$$b(xy)=b(x)+xb(y).$$

因 $xy=yx$，交换 $x,y$ 得

$$(1-y)b(x)=(1-x)b(y).$$

选 $y\neq 1$，令 $a=b(y)/(1-y)$，便有 $b(x)=(1-x)a$。故每个一余循环都是某个 $d_a$，从而 $H^1(F^{\times},F)=0$。对应截面给出的仿射变换为

$$t\longmapsto xt+(1-x)a,$$

恰好固定 $a$。所有补子群由平移共轭。这从公式证明了不同原点给出共轭的伸缩子群。

## 文献说明

本章核读 Milne [1] 第三章第 46–49 页的半直积构造、二面体群与上三角群例子及作用坐标的同构判别。交换核扩张的二余循环、$H^2$ 分类、循环中心扩张的 $A/mA$ 参数和补子群的 $H^1$ 参数均在正文中从截面与乘法直接推导，不预先调用上同调分类定理。这里分类的是保持核与商标记的扩张等价类；任意抽象群的同构分类还须考虑核、商的自同构及不同正规子群的选择。

# 5 置换群与单群

前四章研究正规子群与商群如何分解、组合。本章改变观察方式：让群作用在一个集合上，把群元素转化为置换。轨道描述点怎样移动，稳定子记录哪些元素保持一点，块系则把子群包含关系表现为集合的分割。随后用循环型计算共轭类，证明交错群的单性，再回到可解群与半直积。

## 5.1 作用、轨道与稳定子

**定义 5.1** (左作用与忠实性)**.** 设 $G$ 为群，$X$ 为非空集合。左作用是映射 $G \times X \to X$，记为 $(g,x) \mapsto gx$，满足

$$ex = x, \qquad (gh)x = g(hx).$$

记 $\mathrm{Sym}(X)$ 为 $X$ 上所有双射在复合下组成的群。若只有单位元固定 $X$ 的每一点，称作用忠实；若任意两点可由一个群元素互相移动，称作用传递。

每个 $g$ 给出双射 $\lambda_g : x \mapsto gx$，因为

$$\lambda_{g^{-1}}\lambda_g(x) = g^{-1}(gx) = x, \qquad \lambda_g\lambda_{g^{-1}}(x) = x.$$

作用公理给出 $\lambda_{gh} = \lambda_g\lambda_h$，所以得到同态

$$\lambda : G \longrightarrow \mathrm{Sym}(X).$$

反过来，任意这样的同态以 $gx = \lambda(g)(x)$ 定义作用，因为同态保持单位元和乘法。忠实性恰好是 $\ker\lambda = 1$。

**定义 5.2** (轨道与稳定子)**.** 对 $x \in X$，定义

$$Gx = \{gx : g \in G\}, \qquad G_x = \{g \in G : gx = x\}.$$

前者称为 $x$ 的轨道，后者称为 $x$ 的稳定子。

关系 $y \sim x \iff y = gx$ 是等价关系：$x = ex$ 给出自反性；$y = gx$ 给出 $x = g^{-1}y$；$y = gx, z = hy$ 给出 $z = (hg)x$。因此轨道构成 $X$ 的分割。稳定子是子群：$e \in G_x$，且若 $g,h \in G_x$，则

$$(gh^{-1})x = g(h^{-1}x) = gx = x.$$

这里 $h^{-1}x = x$ 来自对 $hx = x$ 施加 $h^{-1}$。

**定理 5.3** (轨道与陪集的对应)**.** 映射

$$\Phi_x : G/G_x \longrightarrow Gx, \qquad gG_x \longmapsto gx$$

为双射，并满足 $\Phi_x(agG_x) = a\Phi_x(gG_x)$。若 $G$ 有限，则

$$|Gx| = [G : G_x] = \frac{|G|}{|G_x|}.$$

这里 $G/G_x$ 先指左陪集的集合，不假设它是商群。

证明. 若 $gG_x = hG_x$, 则 $h^{-1}g \in G_x$, 故 $h^{-1}gx = x$, 即 $gx = hx$, 证明良定义。反之, $gx = hx$ 给出 $h^{-1}g \in G_x$，所以陪集相同，证明单射。轨道定义保证每个点有原像，故满射。最后

$$\Phi_x(agG_x) = (ag)x = a(gx) = a\Phi_x(gG_x).$$

有限时用 Lagrange 定理计算陪集数，得到公式。 □

**命题 5.4** (稳定子的共轭与作用核)**.** 有 $G_{gx} = gG_xg^{-1}$。若作用传递，则

$$\ker\lambda = \bigcap_{g\in G} gG_xg^{-1}.$$

证明. 任取 $h \in G$,

$$h \in G_{gx} \iff hgx = gx \iff (g^{-1}hg)x = x \iff h \in gG_xg^{-1}.$$

作用核由固定每一点的元素组成，故为 $\bigcap_{y\in X} G_y$；传递时每个 $y$ 都等于某个 $gx$，代入刚证明的等式即得结论。 □

## 5.2 陪集作用与子群的正规核

设 $H \le G$。定义 $a(gH) = (ag)H$。若 $gH = g'H$，则 $g' = gh$ 对某个 $h \in H$ 成立，所以 $(ag')H = (agh)H = (ag)H$，作用良定义。单位元与乘法公理由 $e(gH) = gH$、$a(b(gH)) = (ab)(gH)$ 得到。它传递，且点 $H$ 的稳定子正是 $H$。

**定义 5.5** (正规核)**.** 定义 $H$ 在 $G$ 中的正规核为

$$\mathrm{core}_G(H) = \bigcap_{g\in G} gHg^{-1}.$$

**命题 5.6.** 正规核是包含于 $H$ 的最大正规子群，也是陪集作用的核。若 $[G:H] = m < \infty$，则

$$G/\mathrm{core}_G(H) \hookrightarrow S_m.$$

证明. 交集为子群，取 $g = e$ 得它包含于 $H$。对任意 $a \in G$,

$$a\Big(\bigcap_g gHg^{-1}\Big)a^{-1} = \bigcap_g (ag)H(ag)^{-1} = \bigcap_{u\in G} uHu^{-1},$$

因为 $g \mapsto ag$ 双射，所以正规。若 $N \trianglelefteq G$ 且 $N \le H$，则对每个 $g$，$N = gNg^{-1} \le gHg^{-1}$，故 $N \le \mathrm{core}_G(H)$。陪集作用的核由命题 5.4 给出。

编号陪集以后，作用给出 $\lambda : G \to S_m$。诱导映射

$$\bar\lambda : G/\mathrm{core}_G(H) \to S_m, \quad g\,\mathrm{core}_G(H) \mapsto \lambda(g)$$

良定义：两个代表之比在作用核中，像相同。记 $K = \mathrm{core}_G(H)$，则

$$\bar\lambda((gK)(hK)) = \lambda(gh) = \lambda(g)\lambda(h) = \bar\lambda(gK)\bar\lambda(hK),$$

所以保持乘法。若像为单位元，代表在作用核中，故商陪集为单位元，所以单射。 □

取 $H=1$，左乘作用忠实，得到有限群 $G$ 到 $S_{|G|}$ 的嵌入。这是 Cayley 定理。它证明每个有限群都能作为置换群研究，但寻找较小的忠实作用仍是另外的问题。

**推论 5.7** (最小素因子指数)**.** *设 $G$ 有限，$p$ 是整除 $|G|$ 的最小素数。若 $[G:H]=p$，则 $H \trianglelefteq G$。*

*证明.* 令 $K=\mathrm{core}_G(H)$。有 $K\le H$，且

$$[G:K]=p[H:K]\mid p!.$$

若 $[H:K]>1$，取其一个素因子 $q$。因 $[H:K]\mid|G|$，有 $q\ge p$；又 $q\mid p!$，所以 $q\le p$，必有 $q=p$。于是 $p^2\mid[G:K]\mid p!$。但 $1,\dots,p$ 中只有一个数含因子 $p$，且只含一次，矛盾。故 $[H:K]=1$，$H=K$ 正规。 □

## 5.3 不交循环、阶与幂

以下 $n\ge 2$，$S_n=\mathrm{Sym}(\{1,\dots,n\})$，从右向左复合。置换 $\sigma$ 的支撑为

$$\mathrm{supp}(\sigma)=\{a:\sigma(a)\neq a\}.$$

互异点 $a_0,\dots,a_{j-1}$ 的循环 $(a_0\ a_1\ \cdots\ a_{j-1})$ 把 $a_t$ 送到 $a_{t+1}$，下标模 $j$，并固定其他点；二循环称为换位。一循环记一个不动点。

**定理 5.8** (不交循环分解)**.** *每个 $\sigma\in S_n$ 都是不交循环的乘积。若计入不动点，其循环集合由 $\sigma$ 唯一确定，仅允许改变各循环的起点和循环书写次序。*

*证明.* 让 $\langle\sigma\rangle$ 作用于点集。对任一点 $a$，有限性给出整数 $r>s\ge 0$ 使 $\sigma^r(a)=\sigma^s(a)$。施加双射 $\sigma^{-s}$ 得 $\sigma^{r-s}(a)=a$，所以返回原点的正幂存在；取最小的正整数 $j$ 使 $\sigma^j(a)=a$。$a,\sigma(a),\dots,\sigma^{j-1}(a)$ 互异，否则对一个更短的正幂已有返回。带余除法使每个整数幂的像都属于这 $j$ 点，故它们恰好构成整个轨道。

在此轨道上，$\sigma$ 恰好是循环 $(a\ \sigma(a)\ \cdots\ \sigma^{j-1}(a))$。对所有轨道取这些循环。不同轨道不交，所以在任意点上只有本轨道的循环起作用，全部循环的乘积与 $\sigma$ 在每一点一致。不交循环可交换：任一点至多被其中一个循环移动，交换次序不改变像。

反过来，一个不交循环乘积的每个循环支撑恰是该置换的一个轨道。轨道唯一；每个轨道上的后继点由 $\sigma$ 决定，因而只剩起点和书写顺序的自由。 □

**命题 5.9** (循环型、元素阶与幂)**.** *设 $m_j$ 为 $\sigma$ 分解中长度为 $j$ 的循环数，包含 $m_1$ 个不动点。称 $1^{m_1}2^{m_2}\cdots n^{m_n}$ 为循环型，有*

$$\sum_{j=1}^{n} jm_j=n,\qquad \mathrm{ord}(\sigma)=\mathrm{lcm}\{j:m_j>0\}.$$

*若 $c$ 是 $j$ 循环，$k\in\mathbb{Z}$，则 $c^k$ 分成 $d=\gcd(j,k)$ 个长度 $j/d$ 的循环，约定 $\gcd(j,0)=j$。*

*证明.* 点集被各循环分割，得到第一式。$\sigma^k=e$ 当且仅当每个循环的 $k$ 次幂均恒等，等价于每个出现的长度都整除 $k$；最小正 $k$ 就是最小公倍数。

把 $c$ 的点编号为 $a_t$，$t\in\mathbb{Z}/j\mathbb{Z}$。$c^k$ 把指标 $t$ 变为 $t+k$。返回原点所需最小正步数 $l$ 满足 $j\mid lk$。写 $j=dj_0,k=dk_0$，$\gcd(j_0,k_0)=1$，则 $j\mid lk\iff j_0\mid l$，故轨道长为 $j_0=j/d$。$j$ 个点被分成 $j/(j/d)=d$ 个轨道。 □

**例 5.10** (在幂中分裂的循环)**.** 取 $\sigma = (123)(456)(78) \in S_8$。其阶为 $\operatorname{lcm}(3,2) = 6$，而

$$\sigma^2 = (132)(465), \qquad \sigma^3 = (78), \qquad \sigma^6 = e.$$

例如 $\sigma^2$ 在第一个轨道按 $1 \mapsto 3 \mapsto 2 \mapsto 1$ 运行，第二个轨道按 $4 \mapsto 6 \mapsto 5 \mapsto 4$ 运行，最后两个点固定。

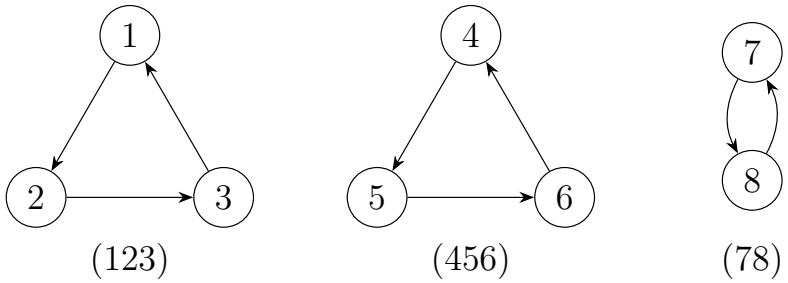



图 5.1: 不交循环给出的三个轨道

图 5.1 画的是 $\sigma$ 的箭头；求幂就是每次沿箭头多走相应步数。两个三点轨道长度相同，稍后将看到中心化子还可以整体交换它们。

## 5.4　符号与三循环生成

沿用第一册已证明的符号同态 $\operatorname{sgn} : S_n \to \{1, -1\}$；每个换位的符号为 $-1$，定义 $A_n = \ker \operatorname{sgn}$。为明确与循环分解的关系，对 $j \geq 2$ 先写出

$$(a_1\ a_2\ \cdots\ a_j) = (a_1 a_j)(a_1 a_{j-1}) \cdots (a_1 a_2). \tag{5.1}$$

右侧使 $a_1$ 先到 $a_2$，以后各换位不动 $a_2$；对 $2 \leq i < j$，$a_i$ 在遇到 $(a_1 a_i)$ 时变为 $a_1$，紧接着变为 $a_{i+1}$，以后不再改变；$a_j$ 最后变为 $a_1$。其余点固定，故等式逐点成立。一循环为单位元，符号为 $1$。因此

$$\operatorname{sgn}(\sigma) = \prod_{j} (-1)^{(j-1)m_j} = (-1)^{n - \sum_j m_j}.$$

特别地，$j$ 循环为偶置换当且仅当 $j$ 为奇数。式 (5.1) 说明换位生成 $S_n$；若一个置换写成 $l$ 个换位，符号必为 $(-1)^l$，所以不同写法的换位数具有相同奇偶性。

当 $n \geq 2$，$(12)$ 的符号为 $-1$，故符号满射。于是 $A_n \trianglelefteq S_n$、$[S_n : A_n] = 2$，且 $|A_n| = n!/2$。这里 $|S_n| = n!$ 来自依次选取 $\sigma(1), \ldots, \sigma(n)$ 的 $n, n-1, \ldots, 1$ 种可能。

**命题 5.11** (三循环生成)**.** *$A_n$ 由所有三循环生成；$n = 2$ 时把空生成集解释为平凡群。*

*证明.* 偶置换写成偶数个换位后，两两分组。两个相同换位相乘为 $e$；共享一点的不同换位适当命名为 $(ab)(bc)$，有

$$(ab)(bc) = (abc).$$

左边的逐点计算是 $a \mapsto a \mapsto b$、$b \mapsto c \mapsto c$、$c \mapsto b \mapsto a$，其余点固定。若两换位不交，则

$$(ab)(cd) = (acb)(acd).$$

为逐点核查后式，右边在 $a,b,c,d$ 上分别给出

$$a \mapsto c \mapsto b, \quad b \mapsto b \mapsto a, \quad c \mapsto d \mapsto d, \quad d \mapsto a \mapsto c.$$

即交换 $a,b$ 以及 $c,d$；其他点固定。因而每一组换位都是三循环乘积，每个偶置换均在三循环生成的群中。反向由三循环符号为 1 得生成群包含于 $A_n$。 □

## 5.5 不动点与轨道计数

**定理 5.12** (轨道计数公式)**.** 设有限群 $G$ 作用于有限非空集合 $X$，记 $X^g = \{x : gx = x\}$，轨道总数为 $r$。则

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

*证明.* 对集合 $\Omega = \{(g,x) \in G \times X : gx = x\}$ 双重计数。先固定 $g$，再固定 $x$，得到

$$|\Omega| = \sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|.$$

将右和按轨道 $O$ 分组。若 $x \in O$，定理 5.3 给出 $|G_x| = |G|/|O|$，因此

$$\sum_{x \in O} |G_x| = |O| \frac{|G|}{|O|} = |G|.$$

每个轨道贡献 $|G|$，故总和为 $r|G|$，两边除以 $|G|$ 即得公式。 □

**例 5.13** (正方形顶点染色)**.** 给正方形四个顶点各选 $q \geq 1$ 种颜色之一，允许同色。令 $X$ 为所有函数 $f : \{1,2,3,4\} \to \{1,\dots,q\}$。沿用第四章的 $D_8$ 顶点作用，定义

$$(gf)(v) = f(g^{-1}v).$$

有 $(gh)f(v) = f(h^{-1}g^{-1}v) = (g(hf))(v)$，故这是左作用。$gf = f$ 当且仅当 $f$ 在 $g$ 的每个顶点循环上为常值。因此若 $g$ 有 $c(g)$ 个循环（计入不动点），恰有 $q^{c(g)}$ 个染色被固定。

旋转 $r = (1234)$、反射 $s = (14)(23)$ 给出如下完整计数：

| 元素类型 | 个数 | 循环长度 | $\lvert X^g \rvert$ |
|---|---|---|---|
| $e$ | 1 | $1,1,1,1$ | $q^4$ |
| $r, r^3$ | 2 | $4$ | $q$ |
| $r^2$ | 1 | $2,2$ | $q^2$ |
| $s, r^2 s$ | 2 | $2,2$ | $q^2$ |
| $rs, r^3 s$ | 2 | $2,1,1$ | $q^3$ |

例如 $rs = (24)$、$r^3 s = (13)$，所以最后一行有两个不动顶点。旋转或反射后相同的染色属于同一轨道，轨道数为

$$\frac{q^4 + 2q^3 + 3q^2 + 2q}{8}.$$

$q = 2$ 时为 $(16 + 16 + 12 + 4)/8 = 6$。

## 5.6 共轭类与中心化子的结构

**命题 5.14** (共轭是重新标号)**.** 对 $\tau \in S_n$，

$$\tau(a_1\ \cdots\ a_j)\tau^{-1} = (\tau(a_1)\ \cdots\ \tau(a_j)).$$

两个置换在 $S_n$ 中共轭当且仅当它们循环型相同。

证明. 左侧把 $\tau(a_i)$ 先还原为 $a_i$，再送到 $a_{i+1}$，最后送到 $\tau(a_{i+1})$；对不在这些像点中的点，$\tau^{-1}$ 的像在原循环外，所以共轭后仍固定。于是得到公式。

共轭保持循环长，给出必要性。若循环型相同，将同长度循环逐一配对，按各自循环顺序把第 $t$ 点对应到第 $t$ 点，包括所有不动点。各循环分割点集，这定义一个双射 $\tau$。公式使它将源循环逐个共轭到目标循环，所以把整个置换共轭到目标。 □

记

$$C_{S_n}(\sigma) = \{\tau \in S_n : \tau\sigma = \sigma\tau\}$$

为中心化子。这里共轭作用是 $g \cdot x = gxg^{-1}$；$e \cdot x = x$，且 $(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1}$，所以满足作用公理。记群 $K$ 中的共轭类为

$$\mathrm{Cl}_K(x) = \{gxg^{-1} : g \in K\}.$$

中心化子是共轭作用下 $\sigma$ 的稳定子，故为子群，且共轭类大小为 $n!/|C_{S_n}(\sigma)|$。

**定理 5.15** (中心化子的坐标与阶)**.** 若 $\sigma$ 循环型为 $1^{m_1}\cdots n^{m_n}$，则

$$|C_{S_n}(\sigma)| = \prod_{j=1}^{n} j^{m_j} m_j!, \qquad |\,\mathrm{Cl}_{S_n}(\sigma)| = \frac{n!}{\prod_j j^{m_j} m_j!}.$$

更精确地，选定每个循环的起点以后，

$$C_{S_n}(\sigma) \cong \prod_{j:m_j>0} \big((C_j)^{m_j} \rtimes S_{m_j}\big),$$

其中 $S_{m_j}$ 通过置换坐标作用于 $(C_j)^{m_j}$。

证明. 把长度 $j$ 的第 $l$ 个循环写成点列 $a_{j,l,t}$，其中 $1 \le l \le m_j$、$t \in \mathbb{Z}/j\mathbb{Z}$，使

$$\sigma(a_{j,l,t}) = a_{j,l,t+1}.$$

若 $\tau\sigma = \sigma\tau$，则 $\tau(\sigma^t a) = \sigma^t \tau(a)$，所以 $\tau$ 将一个 $\sigma$ 轨道双射到另一个相同长度的轨道。对每个 $j$，它因而确定一个 $\pi_j \in S_{m_j}$。若

$$\tau(a_{j,l,0}) = a_{j,\pi_j(l),u_{j,\pi_j(l)}},$$

则交换关系迫使

$$\tau(a_{j,l,t}) = a_{j,\pi_j(l),t+u_{j,\pi_j(l)}}. \tag{5.2}$$

这里每个 $u_{j,l} \in C_j$ 是目标循环的平移量。

反过来，任取 $\pi_j$ 和 $u_{j,l}$，式 (5.2) 在每个轨道间给出双射，全部轨道不交，因此给出全点集的双射；它把 $t+1$ 变成 $t+1+u_{j,\pi_j(l)}$，与先平移再加 1 相同，所以与 $\sigma$ 交换。坐标唯一，故每个 $j$ 有 $j^{m_j}m_j!$ 种选择，不同 $j$ 独立，得到阶公式。

还要检验这里的半直积乘法。暂省略 $j$，用 $(u,\pi)$ 表示以上双射。两个双射复合使

$$a_{l,t} \longmapsto a_{\rho(l),t+v_{\rho(l)}} \longmapsto a_{\pi\rho(l),t+v_{\rho(l)}+u_{\pi\rho(l)}}.$$

定义 $\pi$ 对向量的作用为 $(\pi\cdot v)_k = v_{\pi^{-1}(k)}$，则 $k=\pi\rho(l)$ 时，上式平移量为 $u_k+(\pi\cdot v)_k$。因此坐标乘法为

$$(u,\pi)(v,\rho) = (u+\pi\cdot v, \pi\rho),$$

正是第四章的半直积。坐标作用保持加法，逆由 $\pi^{-1}$ 给出，且 $\pi\cdot(\rho\cdot v)=(\pi\rho)\cdot v$；各个 $j$ 上作用不交，最后取直积。 □

这个半直积常写为 $C_j \wr S_{m_j}$，称为这里的置换花环积；本章只使用上面已完全定义的坐标模型，不预设一般花环积理论。

**例 5.16** (两个等长循环可以互换)**.** 对 $\sigma=(123)(456)(78)$，定理给出

$$|C_{S_8}(\sigma)| = 3^2\cdot 2!\cdot 2 = 36, \qquad |\operatorname{Cl}_{S_8}(\sigma)| = \frac{40320}{36} = 1120.$$

除独立旋转两个三循环以外，$\tau=(14)(25)(36)$ 也与 $\sigma$ 交换，因为

$$\tau(123)\tau^{-1}=(456),\quad \tau(456)\tau^{-1}=(123),\quad \tau(78)\tau^{-1}=(78).$$

因此不能只把中心化子看成各个原循环生成的直积。

**例 5.17** ($S_4$ 的完整共轭表)**.** 4 的分拆恰为 $1+1+1+1, 2+1+1, 2+2, 3+1, 4$。代入中心化子公式得到

| 循环型 | 代表 | $\lvert C_{S_4}(\sigma)\rvert$ | 类大小 | sgn |
|---|---|---|---|---|
| $1^4$ | $e$ | 24 | 1 | $+1$ |
| $2\,1^2$ | $(12)$ | $2\cdot 2! = 4$ | 6 | $-1$ |
| $2^2$ | $(12)(34)$ | $2^2\cdot 2! = 8$ | 3 | $+1$ |
| $3\,1$ | $(123)$ | 3 | 8 | $+1$ |
| $4$ | $(1234)$ | 4 | 6 | $-1$ |

类大小之和 $1+6+3+8+6=24$，也与 $4!$ 相符。

## 5.7 交错群中共轭类的分裂

**引理 5.18** (指数二子群中的类分裂)**.** *设 $K$ 是有限群，$H\trianglelefteq K$、$[K:H]=2$，$x\in H$。$x$ 的 $K$ 共轭类在 $H$ 中或者仍为一个共轭类，或者分成两个等大的共轭类。分成两个当且仅当 $C_K(x)\le H$。*

*证明.* 取 $t\in K\setminus H$，则 $K=H\sqcup tH$，所以

$$\operatorname{Cl}_K(x) = \operatorname{Cl}_H(x)\cup t\operatorname{Cl}_H(x)t^{-1}.$$

第二部分恰是 $txt^{-1}$ 的 $H$ 共轭类：$tHt^{-1}=H$ 使 $t(hxh^{-1})t^{-1}=(tht^{-1})(txt^{-1})(tht^{-1})^{-1}$。两个 $H$ 轨道相交就相同，不相交就构成两个类；共轭 $y\mapsto tyt^{-1}$ 给出它们间的双射。

若 $C_K(x)$ 含 $c\notin H$，则 $t=hc$ 对某个 $h\in H$ 成立，故 $txt^{-1}=hxh^{-1}$，两个类相同。反之，若 $txt^{-1}=hxh^{-1}$，则 $h^{-1}t\in C_K(x)\setminus H$。因此一个类不分裂当且仅当中心化子含子群外元素，得到所述判别。 □

**定理 5.19** (交错群的分裂判别)**.** 设 $\sigma \in A_n$，计入不动点。它的 $S_n$ 共轭类分成两个 $A_n$ 共轭类，当且仅当所有循环长度均为奇数且彼此不同。

证明. 由引理，只需判定 $C_{S_n}(\sigma)$ 是否全由偶置换组成。

若分解含偶长度循环 $c$，则 $c$ 与 $\sigma$ 的所有不交循环交换，故 $c \in C_{S_n}(\sigma)$；但 $\operatorname{sgn}(c) = (-1)^{\operatorname{length}(c)-1} = -1$，类不分裂。

若没有偶长度，但某个奇数 $j$ 重复出现，取两个 $j$ 循环的点列 $a_0, \dots, a_{j-1}$、$b_0, \dots, b_{j-1}$。置换

$$t = \prod_{r=0}^{j-1} (a_r b_r)$$

交换这两个循环，固定其他点，故与 $\sigma$ 交换；它是 $j$ 个不交换位的乘积，符号为 $(-1)^j = -1$。这里 $j = 1$ 也包含两个不动点的换位。因此类仍不分裂。

若各长度为互异奇数，定理 5.15 的轨道置换 $\pi_j$ 都平凡，所以中心化子中的元素只能在每个循环内独立旋转，即为原循环各次幂的乘积。每个原循环符号为 1，其幂及乘积也为偶置换，故 $C_{S_n}(\sigma) \le A_n$，类分成两个。 □

**例 5.20** ($A_5$ 的全部共轭类)**.** 5 个点上的偶循环型只有 $1^5$、$2^2 1$、$31^2$、5。后一个型分裂，前两个非平凡型分别含重复长度 2、重复不动点 1，均不分裂。因而

| 循环型 | 代表 | $\lvert C_{S_5}(\sigma)\rvert$ | $\lvert C_{A_5}(\sigma)\rvert$ | $A_5$ 类大小 |
|---|---|---|---|---|
| $1^5$ | $e$ | 120 | 60 | 1 |
| $2^2 1$ | (12)(34) | 8 | 4 | 15 |
| $31^2$ | (123) | 6 | 3 | 20 |
| 5 | (12345) | 5 | 5 | 12 |
| 5 | (13524) | 5 | 5 | 12 |

未分裂的中心化子含奇置换，符号在其中满射，故与 $A_5$ 相交的阶恰减半。分裂的中心化子已包含于 $A_5$，阶不变。这说明表中每一列的来源。

还要确认两个五循环代表确实来自不同类。令 $c = (12345)$。把 $c$ 共轭为 $c^2 = (13524)$ 的一个置换为

$$u = (2354), \qquad ucu^{-1} = (13524).$$

$u$ 是奇置换。若还存在偶置换 $v$ 完成同一共轭，则 $u^{-1}v \in C_{S_5}(c) = \langle c \rangle \le A_5$，但 $u^{-1}v$ 为奇，矛盾。因此 $c, c^2$ 不在同一个 $A_5$ 类中。

表的类大小之和为 $1 + 15 + 20 + 12 + 12 = 60$。还可仅用这些数字证明 $A_5$ 单。正规子群 $N$ 是完整共轭类的并，包含 $e$，所以

$$|N| = 1 + 15a + 20b + 12d, \quad a, b \in \{0, 1\}, \quad d \in \{0, 1, 2\}.$$

将 $d = 0, 1, 2$ 分别代入，全部可能数为

| $d$ | $(a,b) = (0,0)$ | $(1,0)$ | $(0,1)$ | $(1,1)$ |
|---|---|---|---|---|
| 0 | 1 | 16 | 21 | 36 |
| 1 | 13 | 28 | 33 | 48 |
| 2 | 25 | 40 | 45 | 60 |

其中整除 60 的只有 $1, 60$。Lagrange 定理迫使 $N = 1$ 或 $A_5$。这为下一节的一般单性证明提供一个可独立核查的起点。

## 5.8 最小支撑与交错群的单性

**引理 5.21** (三循环在交错群中共轭)**.** 当 $n \geq 5$ 时，所有三循环在 $A_n$ 中共轭。

证明. 设三循环为 $c, d$，由循环型相同，存在 $\tau \in S_n$ 使 $\tau c \tau^{-1} = d$。若 $\tau$ 偶，已经完成。若 $\tau$ 奇，$d$ 的支撑外至少有两个点 $u, v$，取 $s = (uv)$。$s$ 与 $d$ 不交而交换，且 $s\tau$ 为偶，所以

$$(s\tau)c(s\tau)^{-1} = sds^{-1} = d.$$

□

**引理 5.22** (支撑的乘积上界)**.** 对 $\alpha, \beta \in S_n$，

$$\operatorname{supp}(\alpha\beta) \subseteq \operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta), \qquad \operatorname{supp}(\tau\alpha\tau^{-1}) = \tau(\operatorname{supp}(\alpha)).$$

证明. 若 $x$ 在右侧并集以外，则 $\alpha x = x = \beta x$，于是 $\alpha\beta x = x$，得到第一式。第二式来自

$$(\tau\alpha\tau^{-1})(x) \neq x \iff \alpha(\tau^{-1}x) \neq \tau^{-1}x.$$

□

**定理 5.23** (交错群的单性)**.** 当 $n \geq 5$ 时，$A_n$ 是非交换单群。

证明. 设 $1 \neq N \trianglelefteq A_n$。从有限非空集合 $N \setminus \{e\}$ 中，选支撑大小最小的 $\sigma$，记 $m = |\operatorname{supp}(\sigma)|$。置换不能只移动一点；只移动两点的置换为换位，是奇置换。因此 $m \geq 3$。

对任意三循环 $\tau$，交换子

$$\rho = [\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1})$$

属于 $N$，因为 $\tau \in A_n$ 且 $N$ 正规。它非单位当且仅当 $\sigma\tau\sigma^{-1} \neq \tau$。由支撑上界，$\rho$ 至多移动六点。

若 $m > 6$，取 $a$ 使 $b = \sigma(a) \neq a$，再取互异的 $c, d \notin \{a, b\}$，令 $\tau = (acd)$。共轭循环 $\sigma\tau\sigma^{-1}$ 的支撑包含 $b$，而 $\tau$ 的支撑不包含 $b$，故二者不同。于是 $e \neq \rho \in N$，支撑不超过 $6 < m$，与选择矛盾。故只需讨论 $m = 3, 4, 5, 6$。

若 $m = 3$，支撑上的无不动点置换只能是三循环，已经得到 $N$ 中的三循环。

若 $m = 4$，无不动点的循环长度分拆只有 4 或 $2 + 2$；四循环为奇，故 $\sigma = (ab)(cd)$。取支撑外一点 $u$，令 $\tau = (abu)$。因 $\sigma(u) = u$，

$$\sigma\tau\sigma^{-1} = (bau) = (aub) = \tau^{-1}, \qquad [\sigma, \tau] = \tau^{-2} = \tau.$$

这直接给出 $N$ 中支撑为 $3 < 4$ 的三循环，也与最小性矛盾。

若 $m = 5$，可能分拆只有 5 或 $3 + 2$；后者符号为 $-1$，因此 $\sigma = (abcdu)$。取 $\tau = (abc)$，则

$$\sigma\tau\sigma^{-1} = (bcd), \qquad [\sigma, \tau] = (bcd)(acb) = (adb).$$

最后一步的非固定点计算为 $a \mapsto c \mapsto d$、$d \mapsto d \mapsto b$、$b \mapsto a \mapsto a$；点 $c$ 先到 $b$ 再到 $c$，因而固定。得到一个支撑为 $3 < 5$ 的非单位元，矛盾。

若 $m = 6$，不含 1 的分拆为 $6, 4+2, 3+3, 2+2+2$；其中 6 与 $2+2+2$ 为奇，剩下两型。

第一型 $\sigma=(abc)(duv)$，取 $\tau=(abd)$。有

$$\sigma\tau\sigma^{-1}=(bcu),\qquad [\sigma,\tau]=(bcu)(adb)=(a\ d\ c\ u\ b).$$

最后的五循环按 $a\mapsto d\mapsto c\mapsto u\mapsto b\mapsto a$ 运行，故其支撑为 $5<6$，矛盾。

第二型 $\sigma=(abcd)(uv)$，取 $\tau=(abc)$，仍有

$$\sigma\tau\sigma^{-1}=(bcd),\qquad [\sigma,\tau]=(bcd)(acb)=(adb),$$

支撑为 $3<6$，再次矛盾。至此最小支撑元必为三循环。

正规性和引理 5.21 使 $N$ 包含全部三循环；命题 5.11 使 $N=A_n$。最后，$\alpha=(123)$、$\beta=(124)$ 均在 $A_n$ 中，而

$$(\alpha\beta)(1)=3,\qquad (\beta\alpha)(1)=4,$$

故群非交换。 □

这里的 $n\geq 5$ 同时用于两处：改变三循环共轭元的奇偶性时需要两个外部点；从双换位取得三循环时需要第五个点。$A_3\cong C_3$ 为交换单群，而 $A_4$ 有第一章构造的真正规子群 $V_4$，不能删掉次数条件。

## 5.9 对称群的正规子群与导出列

**引理 5.24** (对称群中心平凡)**.** *若 $n\geq 3$，则 $Z(S_n)=1$。*

*证明.* 设 $z$ 中心，则对任意互异的 $i,j$，共轭公式给出

$$(z(i)\ z(j))=z(ij)z^{-1}=(ij),$$

所以 $\{z(i),z(j)\}=\{i,j\}$。固定 $i$，取与它互异的 $j,k$，则

$$z(i)\in\{i,j\}\cap\{i,k\}=\{i\}.$$

故每个点均被固定，$z=e$。 □

**定理 5.25** (对称群的正规子群)**.** *若 $n\geq 5$，则 $S_n$ 的正规子群恰为 $1,A_n,S_n$。*

*证明.* 设 $N\trianglelefteq S_n$。交 $N\cap A_n$ 正规于 $A_n$，由单性为 1 或 $A_n$。若为 $A_n$，则 $N\supseteq A_n$。若 $N$ 还含一个奇置换 $t$，每个奇置换 $g$ 满足 $t^{-1}g\in A_n$，故 $g\in tA_n\subseteq N$，于是 $N=S_n$；不含奇置换则 $N=A_n$。

若 $N\cap A_n=1$，则 $\operatorname{sgn}|_N$ 核平凡，故单射，$|N|\leq 2$。若 $|N|=2$，写 $N=\{e,z\}$。任意 $g\in S_n$ 的共轭把 $N$ 送到自身，且不把 $z\neq e$ 送到 $e$，所以 $gzg^{-1}=z$。这使 $z\in Z(S_n)$，与引理矛盾。故 $N=1$。 □

**命题 5.26** (完美性与不可解性)**.** *若 $n\geq 5$，则*

$$A_n'=A_n,\qquad S_n'=A_n.$$

*因此 $A_n,S_n$ 都不可解。称满足 $G'=G$ 的群为完美群。*

证明. 第二章已证明导出子群特征，故 $A_n' \trianglelefteq A_n$。非交换性使某个交换子非单位，故 $A_n' \neq 1$；单性迫使 $A_n' = A_n$。其导出列恒为 $A_n \neq 1$，所以不可解。

符号商 $S_n/A_n \cong C_2$ 交换，第二章交换商判别给出 $S_n' \leq A_n$；另一方面，$A_n$ 内的交换子也是 $S_n$ 内的交换子，故 $A_n = A_n' \leq S_n'$。得到相等。于是 $S_n$ 导出列从第一步起恒为 $A_n$，也不终止。 □

**例 5.27** ($S_4$ 为何仍可解)**.** 沿用第一章的 $V = \{e, a, b, c\}$，其中

$$a = (12)(34), \quad b = (13)(24), \quad c = (14)(23).$$

第一章已逐项核对 $V \cong C_2 \times C_2$ 及 $V \trianglelefteq A_4 \trianglelefteq S_4$。现精确计算导出列。符号商交换，故 $S_4' \leq A_4$；而

$$[(12), (23)] = (12)(23)(12)(23) = (132) \in S_4'.$$

$S_4'$ 正规于 $S_4$，所有三循环在 $S_4$ 共轭，故 $S_4'$ 含所有三循环，等于 $A_4$。

商 $A_4/V$ 阶为 3，所以循环且交换，故 $A_4' \leq V$。取 $x = (123), y = (124)$，直接计算

$$[x, y] = (234)(142) = (12)(34) = a.$$

右侧在 $1, 2, 3, 4$ 上的像依次为 $2, 1, 4, 3$。用 $x$ 共轭有

$$xax^{-1} = (23)(14) = c, \qquad xcx^{-1} = (24)(13) = b.$$

正规性给出 $a, b, c \in A_4'$，所以 $A_4' = V$。$V$ 交换，故 $V' = 1$。最终

$$S_4^{(0)} = S_4, \quad S_4^{(1)} = A_4, \quad S_4^{(2)} = V, \quad S_4^{(3)} = 1,$$

导出长度为 3。$S_3$ 的导出长度为 2 已在第二章计算，$S_2 = C_2$ 的导出长度为 1。因此对 $n \geq 2$，$S_n$ 可解当且仅当 $n \leq 4$。

## 5.10 块、本原作用与极大子群

以下 $G$ 传递地作用于有限集合 $X$，$|X| \geq 2$。

**定义 5.28** (块与本原作用)**.** 非空子集 $B \subseteq X$ 称为块，若对每个 $g \in G$，要么 $gB = B$，要么 $gB \cap B = \varnothing$。单点和 $X$ 称为平凡块。若只有平凡块，称此传递作用为本原作用。

块条件比 “某个子集被某些元素保持” 更强：每个群元素都必须把它整体移到自身，或移到与它完全不交的地方。

**命题 5.29** (块的平移构成分割)**.** *若 $B$ 是块，则不同的平移 $gB$ 两两不交，全部平移覆盖 $X$，且 $G$ 置换这些块。反过来，若 $G$ 置换某个分割中的各部分，则每个部分都是块。有限时每块大小整除 $|X|$。*

证明. 若 $gB \cap hB \neq \varnothing$，施加 $h^{-1}$ 得 $h^{-1}gB \cap B \neq \varnothing$，块条件给出 $h^{-1}gB = B$，故 $gB = hB$。取 $b \in B$；传递性使每个 $x \in X$ 写成 $gb$，所以被某个 $gB$ 覆盖。$a(gB) = (ag)B$ 说明 $G$ 置换各部分。

反过来，同一分割中的两个部分相交就相同，而 $gB$ 仍为一个部分，恰是块条件。各平移通过双射 $g$ 与 $B$ 等势，若共有 $r$ 块，则 $|X| = r|B|$。 □

**定理 5.30** (含定点的块与中间子群)**.** 固定 $x \in X$。含 $x$ 的块与满足 $G_x \le H \le G$ 的子群一一对应，映射为

$$B \longmapsto G_B = \{g : gB = B\}, \qquad H \longmapsto Hx.$$

因而作用本原当且仅当 $G_x$ 是 $G$ 的极大真子群。

证明. 先给定块 $B \ni x$。集合稳定子 $G_B$ 为子群，因为 $eB = B$，且若 $gB = B = hB$，则 $h^{-1}B = B$，于是 $gh^{-1}B = B$。若 $g \in G_x$，则 $x = gx \in gB \cap B$，故 $gB = B$，得到 $G_x \le G_B$。

有 $G_B x \subseteq B$。对任意 $y \in B$，传递性给出 $g$ 使 $gx = y$。此时 $y \in gB \cap B$，块条件使 $g \in G_B$，故 $y \in G_B x$，得到 $B = G_B x$。

再给定 $G_x \le H \le G$，令 $B = Hx$。若 $gB \cap B \neq \varnothing$，则存在 $h_1, h_2 \in H$ 使 $gh_1 x = h_2 x$，因此

$$h_2^{-1} g h_1 \in G_x \le H, \qquad g = h_2 (h_2^{-1} g h_1) h_1^{-1} \in H.$$

于是 $gB = gHx = Hx = B$，证明 $B$ 是块。每个 $h \in H$ 保持 $Hx$，所以 $H \le G_B$；若 $g \in G_B$，则 $gx \in Hx$，写 $gx = hx$，得到 $h^{-1}g \in G_x \le H$，故 $g \in H$。因此 $G_B = H$，两映射互逆。

$H = G_x$ 对应 $\{x\}$；$H = G$ 对应 $X$。因此没有非平凡块，当且仅当没有严格中间子群。传递且 $|X| \ge 2$ 使 $G_x < G$，这就是极大真子群条件。 □

**推论 5.31** (素数次数与二重传递)**.** 传递作用的点数若为素数，则作用本原。二重传递作用也本原，其中二重传递指对任意有序互异点对 $(x, y)$、$(u, v)$，存在同一个 $g$ 使 $gx = u, gy = v$。

证明. 素数点数情形，块大小整除该素数，故只能为 1 或 $|X|$。

二重传递情形，若块 $B$ 含互异 $x, y$ 且 $B \neq X$，取 $z \notin B$。二重传递给出 $g$ 使 $gx = x, gy = z$。因 $x \in gB \cap B$，块条件使 $gB = B$，但 $z = gy \in gB$ 却不属于 $B$，矛盾。 □

## 5.11 换位生成的图与传递性的边界

**引理 5.32** (连通图的边换位)**.** 设有限无向图的顶点集为 $X$，边 $\{u, v\}$ 对应换位 $(uv)$。边换位生成的群，在每个连通分支上恰为全对称群；不同分支的这些对称群构成直积。特别地，图连通当且仅当边换位生成 $\mathrm{Sym}(X)$。

证明. 每个边换位只移动同一分支中的两个点，所以生成群保持每个分支。反过来，若 $a, b$ 属于同一分支，取简单路径

$$v_0 = a, v_1, \dots, v_r = b.$$

$r = 1$ 时 $(ab)$ 就是边换位。$r \ge 2$ 时令

$$w = (v_0 v_1)(v_1 v_2) \cdots (v_{r-2} v_{r-1}).$$

从右向左作用，$v_{r-1}$ 依次到 $v_{r-2}, \dots, v_0$，故 $w(v_{r-1}) = v_0$；简单路径使 $v_r$ 不在 $w$ 的支撑内，故 $w(v_r) = v_r$。共轭公式给出

$$w (v_{r-1} v_r) w^{-1} = (v_0 v_r) = (ab).$$

因此同一分支内任意两点的换位均已生成，它们生成该分支上的全部置换。

不同分支支撑不交，所以逐元素交换，交也平凡。任意保持每个分支的置换唯一由各分支上的限制决定，逐点相乘对应坐标相乘；因此生成群是这些对称群的直积。单点分支贡献平凡群。 □

**定理 5.33** (本原群含换位的判别)**.** 设 $G \le \mathrm{Sym}(X)$ 忠实本原地作用，且含一个换位，则 $G = \mathrm{Sym}(X)$。特别地，素数次数的传递置换群含换位时就是全对称群。

证明. 设换位为 $t = (ab)$。把所有 $gtg^{-1}$ 的两个支撑点作为边，构成顶点集为 $X$ 的图。共轭公式给出边 $\{ga, gb\}$。任意 $h \in G$ 将这条边送到 $\{hga, hgb\}$，仍为边；所以 $G$ 的每个元素都是图自同构，置换图的连通分支。

由命题 5.29，分支是块。图含边 $\{a, b\}$，其分支至少两点；本原性使这一分支等于 $X$，故图连通。所有边换位都在 $G$ 中，由上一引理生成整个 $\mathrm{Sym}(X)$。于是 $G$ 包含整个对称群，而原先已是其子群，所以相等。素数情形用推论 5.31。 □

**例 5.34** (传递且含换位仍可能不够)**.** 在 $S_4$ 中取

$$r = (1234), \qquad t = (24), \qquad G = \langle r, t \rangle.$$

有 $r^4 = t^2 = e$、$trt^{-1} = (1432) = r^{-1}$。关系 $tr = r^{-1}t$ 使每个乘积都可归到 $r^a t^\varepsilon$，$0 \le a < 4$、$\varepsilon \in \{0, 1\}$。四个 $r^a$ 不同，$t \notin \langle r \rangle$，故这八个元素不同，$|G| = 8$。它传递，因为包含四循环，也含换位 $t$；但 $|S_4| = 24$，所以 $G \ne S_4$。

$t$ 在 $G$ 中的共轭只有 $(24), (13)$：$r$ 共轭将二者互换，$t$ 共轭保持二者；生成元保持此二元集合，所以全部共轭都在其中，而两者均已出现。对应图有两个分支

$$B_1 = \{1, 3\}, \qquad B_2 = \{2, 4\}.$$

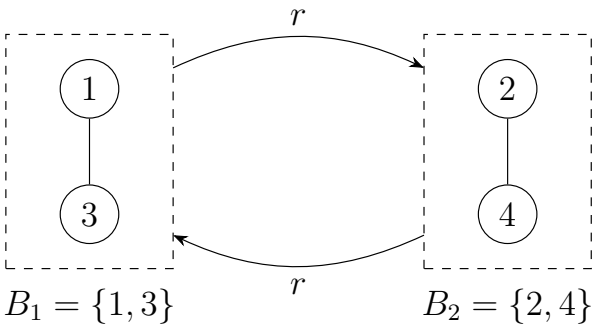



图 5.2: 换位共轭图的两个分支与块的交换

图 5.2 的两条实线恰是共轭换位对应的边。$rB_1 = B_2$、$rB_2 = B_1$，$t$ 保持两块，所以块系被 $G$ 保持；没有跨分支的边。这明确指出了上一证明中需要本原性的环节。

## 5.12 正规子群的轨道与仿射结构

**命题 5.35** (正规子群的轨道组成块系)**.** 设 $G$ 传递地作用于 $X$，$N \trianglelefteq G$。则 $N$ 的轨道组成被 $G$ 保持的分割，而且各轨道等大。若作用忠实且本原，则每个非平凡正规子群都传递。

证明. 对任意 $g \in G, x \in X$，

$$g(Nx) = \{gnx : n \in N\} = \{(gng^{-1})gx : n \in N\} = N(gx),$$

其中最后一步用 $gNg^{-1}=N$。故 $G$ 置换这些轨道。$G$ 在 $X$ 传递，使任意两个 $N$ 轨道由某个 $g$ 双射对应，因而等大。

若作用本原，轨道分割只能是单点分割或 $\{X\}$。若全是单点，则每个 $n\in N$ 固定每一点，忠实性使 $N=1$。所以非平凡 $N$ 必传递。 □

不能把“正规”省去。例如 $\langle(12)\rangle\le S_3$ 在三点上的轨道为 $\{1,2\},\{3\}$，大小不同。

**定义 5.36** (正则作用)**.** 忠实传递作用若一点的稳定子平凡，称为正则作用。由稳定子共轭公式，此时每一点的稳定子都平凡；对任意有序点对 $(x,y)$，传递性给出将 $x$ 送到 $y$ 的元素；若 $gx=hx=y$，则 $h^{-1}g\in G_x=1$，故 $g=h$，这样的元素唯一。

**定理 5.37** (交换正规子群迫使仿射形式)**.** *设有限群 $G\le \mathrm{Sym}(X)$ 忠实本原地作用于 $|X|\ge 2$ 的集合，且含非平凡交换正规子群 $N$。则存在素数 $p$ 和 $d\ge 1$，使*

$$|X|=p^d,\qquad N\cong (C_p)^d.$$

*选定一点 $x$ 与 $N$ 的一组 $\mathbb{F}_p$ 基以后，可以将 $X$ 识别为向量空间 $\mathbb{F}_p^d$，将 $G$ 识别为仿射群的子群*

$$N\rtimes G_x\ \le\ (\mathbb{F}_p^d,+)\rtimes \mathrm{GL}_d(\mathbb{F}_p).$$

*其中 $N$ 作用为全部平移，$G_x$ 的线性作用没有非零真不变子空间。*

*证明.* 命题 5.35 使 $N$ 传递。若 $n\in N$ 固定 $x$，任取 $y=mx$ $(m\in N)$，交换性给出

$$ny=nmx=mnx=mx=y.$$

所以 $n$ 固定全体点，由忠实性得 $n=e$。因此 $N$ 正则，映射 $N\to X, n\mapsto nx$ 为双射，$|N|=|X|$。

任何非平凡特征子群 $M$ 特征于 $N$，而 $N\trianglelefteq G$，所以 $M\trianglelefteq G$。它由本原性传递，因而 $Mx=X$。但 $N\to X$ 单射，$Mx=Nx$ 使 $M=N$，故 $N$ 没有非平凡真特征子群。

取整除 $|N|$ 的素数 $p$。Cauchy 定理给出一个阶 $p$ 元素。把 $N$ 改写为加法，集合

$$N[p]=\{a\in N: pa=0\}$$

是子群，因为 $p(a-b)=pa-pb=0$；它特征，因为 $p\alpha(a)=\alpha(pa)=0$，且对 $\alpha^{-1}$ 可得反向包含。它非平凡，所以 $N[p]=N$。由 $pa=0$，对 $k\in\mathbb{Z}$ 定义

$$[k]_p\,a=ka.$$

若 $k-l$ 是 $p$ 的倍数，则 $(k-l)a=0$，故标量乘法良定义。整数分配律给出两条分配律及标量结合律，$[1]_pa=a$，所以 $N$ 成为 $\mathbb{F}_p$ 向量空间。有限性使其有有限基，记维数 $d$，故 $|N|=p^d$、$N\cong(C_p)^d$。

令 $H=G_x$。正则性使 $N\cap H=1$。对任意 $g\in G$，传递性给出 $n\in N$ 使 $nx=gx$，于是 $n^{-1}g\in H$，得到 $G=NH$。第四章内部半直积定理给出 $G\cong N\rtimes H$，作用为共轭。每个 $h\in H$ 的共轭自同构 $\alpha_h$ 保持加法，且

$$\alpha_h(ka)=k\alpha_h(a),$$

故为 $\mathbb{F}_p$ 线性自同构。

此线性作用忠实：若 $h$ 与所有 $n\in N$ 交换，则对任意点 $nx$，

$$h(nx)=(hnh^{-1})(hx)=nx,$$

所以 $h=e$。选基给出单同态 $H\hookrightarrow \mathrm{GL}_d(\mathbb{F}_p)$。在 $a\leftrightarrow ax$ 的点坐标下（$a$ 是加法记号的 $N$ 元素），元素 $nh$ 将 $a$ 送到

$$a\longmapsto n+\alpha_h(a).$$

因为 $nh(ax)=n(hah^{-1})x$。这就是所述仿射作用，且半直积映射保持乘法、由唯一分解双射，故得到忠实仿射实现。

最后若 $0<W<N$ 是 $H$ 不变子空间，$N$ 交换使 $W$ 被 $N$ 共轭保持，又被 $H$ 保持；$G=NH$ 使 $W\trianglelefteq G$。非平凡正规子群必须传递，但正则点坐标下 $Wx$ 只有 $|W|<|N|=|X|$ 个点，矛盾。所以没有这样的子空间。 □

**例 5.38** (有限域上的一维仿射群)**.** 取素数 $p>2$，群 $\mathrm{Aff}(\mathbb{F}_p)=\{t\mapsto at+b : a\neq 0\}$ 具有交换正规平移子群。它实际上二重传递：给定 $x\neq y, u\neq v$，要求

$$ax+b=u,\qquad ay+b=v,$$

相减得到唯一解

$$a=\frac{v-u}{y-x}\neq 0,\qquad b=u-ax.$$

因此它本原，阶为 $p(p-1)$。$p=3$ 时阶为 $6$，忠实嵌入 $S_3$ 后阶相等，故为 $S_3$；$p=5$ 时阶为 $20$，小于 $|S_5|=120$，所以是真子群。它不含换位：非单位平移 $t\mapsto t+b$ 在五点上无不动点，而 $a\neq 1$ 时方程 $at+b=t$ 恰有一个解；换位却有三个不动点。

这也核对了定理 5.33 的条件：本原性本身不会迫使群是整个对称群，换位条件确实起作用。

## 文献说明

本章核读 Milne [1] 第四章第 57–62 页的群作用、轨道、稳定子与陪集模型，第 66–70 页的循环型、三循环生成和交错群单性，第 72–73 页的本原作用；另核对第 130 页习题 4-11、4-12 解答中的类分裂判别，以及第 122 页习题 56、第 123 页习题 59 的正规子群轨道问题。正文将中心化子进一步写成显式半直积坐标，完整证明分裂判别并列出 $A_5$ 共轭表；最小支撑证明的交换子逐个计算。轨道计数、图上的换位生成和交换正规子群导致仿射形式的结果，均在这里给出独立证明。本章不使用域扩张或 Galois 理论，相关根作用留到后续分册。

# 6 低阶群的结构与分类

本章把前面建立的群作用、有限 $p$ 群的中心、Sylow 理论与半直积用于分类；覆盖所有不超过三十一阶的群、三十六阶群，以及 $p^2$、$pq$、$p^3$、$p^4$、$2p^2$、$3p^2$、$4p$、$6p$ 等一般阶族，并对八阶、十二阶以及非交换奇素数立方阶模型继续求其子群结构。这里的“分类”包含三个任务：构造实际存在的模型；证明不同模型互不同构；证明任何满足条件的群都在列表中。仅列出群名不能完成第三个任务，写出生成关系也不能自动完成第一个任务。

## 6.1 分类中的生成元、关系与计数

**引理 6.1** (由唯一坐标构造同构)**.** *设 $G, H$ 为群，每个元素分别具有唯一表达式*

$$g = a_1^{i_1} \cdots a_s^{i_s}, \qquad h = b_1^{i_1} \cdots b_s^{i_s}, \qquad (i_1, \ldots, i_s) \in I.$$

*若两个群中的坐标乘法公式相同，则把第一种表达式送到第二种表达式的映射是群同构。*

*证明.* 定义 $\Phi(a_1^{i_1} \cdots a_s^{i_s}) = b_1^{i_1} \cdots b_s^{i_s}$。$G$ 中坐标的唯一性保证同一元素不会给出两个像，故映射良定义。$H$ 中坐标的唯一性保证不同坐标不对应同一像，故 $\Phi$ 单射；$H$ 中表达式的存在性保证满射。

若 $g, g'$ 的坐标分别为 $i, j$，共同的乘法公式给出乘积坐标 $M(i,j)$。于是 $\Phi(gg')$ 的坐标是 $M(i,j)$，$\Phi(g)\Phi(g')$ 的坐标也是 $M(i,j)$；唯一性给出两者相等。故 $\Phi$ 是同构。 □

**注 6.2.** 下面使用关系 $bab^{-1} = a^u$ 时，会先说明模型或坐标为何存在，再由 $ba = a^u b$ 推导乘法。因此不会把“生成元满足同样关系”直接当成“群已经同构”。关系可能不能唯一确定群，也可能迫使某个生成元的阶缩小。

**引理 6.3** (中心商循环的判别)**.** *若 $G/Z(G)$ 循环，则 $G$ 交换。*

*证明.* 取 $gZ(G)$ 为商群生成元。每个 $x \in G$ 都可写成 $x = g^i z$，其中 $i \in \mathbb{Z}$、$z \in Z(G)$。任取 $x = g^i z$、$y = g^j w$，利用 $z, w$ 与所有元素交换，得

$$xy = g^{i+j} zw = g^{j+i} wz = yx.$$

故 $G$ 交换。注意这里只要求模去整个中心后的商循环；一般正规子群的循环商不保证原群交换。 □

**引理 6.4** (本章使用的两个有限 $p$ 群事实)**.** *设 $|G| = p^n$，$n \geq 1$。则 $Z(G) \neq 1$；每个指数为 $p$ 的子群 $H$ 都正规。*

*证明.* 对共轭作用使用轨道–稳定子公式。任一共轭类大小为 $[G : C_G(g)]$，是 $p$ 的幂；大小为一恰当且仅当 $g \in Z(G)$。故类方程为

$$p^n = |Z(G)| + \sum_i p^{a_i}, \qquad a_i \geq 1,$$

其中和遍历非中央共轭类。因此 $p \mid |Z(G)|$，而中心包含单位，故 $|Z(G)| \geq p$。

指数为 $p$ 时，左陪集作用给出 $\rho: G \to S_p$，核 $K$ 包含在 $H$ 中。像的阶既整除 $p^n$ 又整除 $p!$，而 $p!$ 中素因子 $p$ 只出现一次，所以 $|\operatorname{im}\rho|$ 只能是一或 $p$。作用在 $p$ 个陪集上传递，其像的轨道有 $p$ 个元素，轨道–稳定子公式使 $p \mid |\operatorname{im}\rho|$，故像阶为 $p$。于是 $[G:K] = p = [G:H]$，结合 $K \le H$ 得 $K = H$，所以 $H$ 正规。这也为本章调用第五章最小素因子指数判据的所有 $p$ 群情形给出了独立短证明。 □

## 6.2 素数平方阶：两个模型与完整性

**定理 6.5.** *设 $p$ 是素数，$|G| = p^2$。则*

$$G \cong C_{p^2} \quad \text{或} \quad G \cong C_p \times C_p,$$

*且两者不同构。*

*证明.* 由引理 6.4，有限 $p$ 群的中心非平凡，所以 $|Z(G)|$ 是 $p$ 或 $p^2$。若为 $p$，则 $G/Z(G)$ 阶为 $p$，因而循环；引理 6.3 推出 $G$ 交换，与中心只有 $p$ 个元素矛盾。因此 $Z(G) = G$。

若有 $x \in G$ 的阶为 $p^2$，则 $G = \langle x\rangle$。否则每个非单位元阶为 $p$。取 $x \neq e$，再取 $y \notin \langle x\rangle$。定义

$$\Phi : (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow G, \qquad (\bar{i}, \bar{j}) \longmapsto x^i y^j.$$

因为 $x^p = y^p = e$，改变 $i, j$ 的整数代表元不改变像；交换性给出

$$x^i y^j x^k y^\ell = x^{i+k} y^{j+\ell},$$

所以 $\Phi$ 是同态。若 $x^i y^j = e$ 且 $\bar{j} \neq 0$，取整数 $t$ 使 $jt \equiv 1 \pmod p$，则

$$y = (y^j)^t = x^{-it} \in \langle x\rangle,$$

矛盾。因此 $\bar{j} = 0$，继而 $\bar{i} = 0$。这证明单射；定义域和值域均有 $p^2$ 个元素，故也满射。

两个模型存在，因为循环群和直积都已构造。它们不同构，因为第一个含阶 $p^2$ 元，第二个所有非单位元阶为 $p$。 □

**命题 6.6** (四阶群的完整分类)**.** *若 $|G| = 4$，则*

$$G \cong C_4 \quad \text{或} \quad G \cong C_2 \times C_2.$$

*证明.* 取 $g \neq e$。若 $|g| = 4$，则 $G = \langle g\rangle \cong C_4$。若不存在阶 4 元，则每个非单位元阶为 2。取 $x \neq e$，再取 $y \notin \langle x\rangle$。四个元素

$$e, \quad x, \quad y, \quad xy$$

互异并遍历 $G$。因为 $yx$ 也是不在 $\{e, x, y\}$ 中的元素，所以 $yx = xy$。于是

$$(\bar{i}, \bar{j}) \longmapsto x^i y^j$$

是 $C_2 \times C_2$ 到 $G$ 的双射同态。两种模型分别有阶 4 元和没有阶 4 元，故不同构。 □

**例 6.7.** 将同一论证取 $p = 3$，便得到九阶群只有 $C_9$ 和 $C_3^2$；这里不是额外引用，而是定理 6.5 的具体实例。

## 6.3 素数乘积阶：作用参数与同构类型

先补出本节所需的乘法群性质，以说明非平凡作用存在的依据。

**引理 6.8.** *域 $F$ 的乘法群的任意有限子群 $A$ 都是循环群。特别地，$\mathbb{F}_q^\times$ 在 $q$ 为素数时是阶 $q-1$ 的循环群。*

*证明.* 令 $d$ 为 $A$ 中所有元素阶的最小公倍数。对每个整除 $d$ 的素数 $\ell$，设 $\ell^{r_\ell}$ 是 $d$ 中的最高 $\ell$ 次幂。按最小公倍数的定义，有 $x_\ell \in A$ 的阶为 $\ell^{r_\ell} m_\ell$，其中 $\ell \nmid m_\ell$。于是 $y_\ell = x_\ell^{m_\ell}$ 的阶恰为 $\ell^{r_\ell}$。

$A$ 交换。两个交换元素 $u, v$ 若阶互素，记两阶为 $m, n$，则 $uv$ 的阶为 $mn$：若 $(uv)^k = e$，则 $u^k = v^{-k}$ 属于 $\langle u\rangle \cap \langle v\rangle$；交的元素阶同时整除两阶，因此交平凡，得到 $m \mid k, n \mid k$，故 $mn \mid k$。反过来，$(uv)^{mn} = u^{mn}v^{mn} = e$。逐个应用此论证，$\prod_\ell y_\ell$ 的阶为 $d$。所以 $d \le |A|$。

每个 $x \in A$ 都满足 $x^d = 1$，而域上的非零多项式 $T^d - 1$ 至多有 $d$ 个根：每找到一个根 $c$，多项式除法给出一个因子 $T - c$；不同根使剩余商仍在其余根处为零，逐次分解至多能做 $d$ 次，否则次数小于零。因此 $|A| \le d$。两边合并得 $|A| = d$，上面构造的阶 $d$ 元生成 $A$。 □

**定理 6.9** (阶 $pq$ 的分类)**.** *设 $p < q$ 为素数，$|G| = pq$。*

1. *若 $p \nmid (q-1)$，则 $G \cong C_{pq}$。*
2. *若 $p \mid (q-1)$，则恰有两个同构类型：$C_{pq}$ 和一个非交换的 $C_q \rtimes C_p$。*

*证明.* 设 $n_q$ 为 Sylow $q$ 子群个数。Sylow 定理给出 $n_q \mid p$ 且 $n_q \equiv 1 \pmod q$。因 $1 < p < q$，只能 $n_q = 1$。所以有正规子群 $N = \langle a\rangle$，$|a| = q$。任取 Sylow $p$ 子群 $H = \langle b\rangle$，$|b| = p$。两子群交平凡，且 $N$ 正规，故 $NH$ 是子群，阶为 $qp = |G|$。因此每个元素唯一写成

$$a^i b^j, \qquad i \in \mathbb{Z}/q\mathbb{Z},\ j \in \mathbb{Z}/p\mathbb{Z}.$$

共轭作用给出 $bab^{-1} = a^u$，其中 $u \in (\mathbb{Z}/q\mathbb{Z})^\times$。由 $b^p = e$，

$$a = b^p a b^{-p} = a^{u^p}, \qquad u^p \equiv 1 \pmod q.$$

反复使用 $ba = a^u b$ 得坐标乘法

$$(i, j)(k, \ell) = (i + u^j k,\ j + \ell). \tag{6.1}$$

第一坐标模 $q$，第二坐标模 $p$。

反过来，对每个满足 $u^p = 1$ 的非零剩余类 $u$，第四章的外部半直积构造保证式 (6.1) 在 $(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ 上定义一个群，且其阶确为 $pq$。引理 6.1 说明上面得到的任意 $G$ 都同构于对应模型。

$\mathrm{Aut}(C_q)$ 通过 $a \mapsto a^v$ 识别为 $\mathbb{F}_q^\times$，由引理 6.8 为阶 $q-1$ 的循环群。若 $p \nmid q-1$，没有阶为 $p$ 的元素，故 $u = 1$。此时模型是直积。元素 $(1,1)$ 的阶为 $pq$，因为它的 $k$ 次幂为 $(k,k)$，为单位当且仅当 $q \mid k$ 且 $p \mid k$。所以模型是 $C_{pq}$。

若 $p \mid q-1$，循环群 $\mathbb{F}_q^\times$ 有唯一的阶 $p$ 子群 $U$。$u \neq 1$ 时必生成 $U$，故至少存在一个非交换模型。若参数 $u, v$ 均生成 $U$，选 $r$ 满足

$$v^r = u, \qquad 1 \le r < p.$$

定义从 $u$ 模型到 $v$ 模型的映射

$$\Psi(i,j) = (i, rj).$$

因为 $r$ 模 $p$ 可逆，$\Psi$ 双射。由 $v^{rj} = u^j$，

$$\Psi\big((i,j)(k,\ell)\big) = (i + u^j k, r(j+\ell)) = \Psi(i,j)\Psi(k,\ell).$$

所以所有非平凡参数给出同一个同构类型。该模型不交换，因为

$$(0,1)(1,0) = (u,1), \qquad (1,0)(0,1) = (1,1),$$

且 $u \neq 1$。故它也不与循环模型同构。 □

**例 6.10** (阶 21 与阶 15)**.** 阶 21 时取 $p = 3, q = 7$。模 7 的 2 阶为 3，因为 $2^3 \equiv 1$ 而 $2, 2^2 \not\equiv 1$。故非交换模型可取

$$(i,j)(k,\ell) = (i + 2^j k, j + \ell), \quad i,k \in \mathbb{Z}/7\mathbb{Z},\ j,\ell \in \mathbb{Z}/3\mathbb{Z}.$$

参数 $4 = 2^2$ 给出同构模型，不能再算成第三种群。阶 15 时，$3 \nmid 5 - 1$，所以只有 $C_{15}$。

**推论 6.11.** *若 $q$ 为奇素数，则阶 $2q$ 的群只有 $C_{2q}$ 和 $D_{2q}$。*

*证明.* $\mathbb{F}_q^\times$ 中阶为 2 的唯一元素是 $-1$：若 $u^2 = 1$，域上 $(u-1)(u+1) = 0$，故 $u = 1$ 或 $-1$，且奇特征下二者不同。非平凡模型因此满足 $bab^{-1} = a^{-1}$，正是第四章构造的二面体群。两种群一个交换、一个不交换。 □

**命题 6.12** (平方阶与非交换素数乘积阶的子群)**.** *$C_{p^2}$ 有唯一阶 $p$ 子群，$C_p^2$ 有 $p+1$ 个阶 $p$ 子群。二者的全部子群都正规，任一阶 $p$ 子群的商都是 $C_p$。*

*若 $p < q$、$p \mid q-1$，令 $G = C_q \rtimes C_p$ 为非交换模型，$N = \langle a\rangle$、$H = \langle b\rangle$。则 $G$ 的真非平凡子群恰为 $N$ 以及 $q$ 个共轭的阶 $p$ 子群，正规子群恰为 $1, N, G$。此外*

$$Z(G) = 1, \qquad G' = N, \qquad G/N \cong C_p.$$

*证明.* 循环群子群由阶唯一决定，所以 $C_{p^2}$ 的结论成立。二维向量空间中每个非零向量生成一个阶 $p$ 子群，每个这样的子群有 $p-1$ 个非零向量，且不同子群非零部分不交；故数量为 $(p^2-1)/(p-1) = p+1$。两群交换，故所有子群正规；商阶为 $p$，因而循环。

在 $pq$ 阶模型中，Sylow $q$ 子群 $N$ 已知唯一。若 Sylow $p$ 子群也唯一，则 $N, H$ 同时正规，任取 $n \in N, h \in H$，交换子 $[n,h]$ 同时属于 $N, H$，故属于平凡交。这会使 $G = NH$ 交换，矛盾。因此 Sylow 数 $n_p \mid q$ 不能为一，只能为 $q$。Sylow 共轭定理说明所有阶 $p$ 子群为 $H$ 的共轭；它们都不正规。由 Lagrange 定理，真非平凡子群阶只能为 $p, q$，所以子群与正规子群列表完整。

写 $bab^{-1} = a^u$，$u \neq 1$ 且模 $q$ 阶为 $p$。若 $a^i b^j$ 中央，与 $a$ 交换先要求 $u^j = 1$，故 $j = 0$ (模 $p$)；再与 $b$ 交换要求 $(u-1)i = 0$ (模 $q$)，域中 $u-1$ 非零，故 $i = 0$。所以中心平凡。又 $[b,a] = a^{u-1}$ 生成 $N$，因为 $q$ 为素数且 $u - 1 \neq 0$；于是 $N \leq G'$。商 $G/N \cong C_p$ 交换给出反向包含 $G' \leq N$，所以 $G' = N$。 □

## 6.4 八阶交换群：先拆出循环因子

**命题 6.13.** 八阶交换群的同构类型恰为 $C_8, C_4\times C_2, C_2^3$。

证明. 若有阶 8 元，群循环。否则，若有阶 4 元 $a$，取 $b\notin\langle a\rangle$。由于指数为 2，$b^2\in\langle a\rangle$。$b^2$ 不能为 $a$ 或 $a^3$：这会使 $b^2$ 阶为 4，进而 $b$ 阶为 8。所以 $b^2=e$ 或 $a^2$。

若 $b^2=e$，令 $c=b$；若 $b^2=a^2$，令 $c=ba^{-1}$，交换性给出

$$c^2=b^2a^{-2}=e.$$

两种情况下 $c\notin\langle a\rangle$，否则 $b$ 也在其中。故 $\langle a\rangle\cap\langle c\rangle=1$，且两者相乘得到 8 个元素。坐标映射

$$C_4\times C_2\longrightarrow G,\qquad (\bar i,\bar j)\longmapsto a^ic^j$$

保持乘法、代表元独立且双射，故为同构。

若没有阶 4 元，所有非单位元阶为 2。取 $a\neq e$，再取 $b\notin\langle a\rangle$，则 $\langle a,b\rangle$ 含互异的 $e,a,b,ab$。取 $c\notin\langle a,b\rangle$，八个乘积 $a^ib^jc^k$ $(i,j,k\in\{0,1\})$ 互异：两个表达式相等时，移项会把 $c$ 放入 $\langle a,b\rangle$，除非 $k$ 相同；再依次消去 $b$、$a$。因此 $G\cong C_2^3$。

三个模型存在，且最大元素阶分别为 $8,4,2$，所以互不同构。 □

## 6.5 八阶非交换群：二阶元决定分岔

**定理 6.14.** 八阶群恰有五个同构类型：

$$C_8,\quad C_4\times C_2,\quad C_2^3,\quad D_8,\quad Q_8.$$

证明. 只需分类非交换群 $G$。由引理 6.4，有限 2 群中心非平凡，所以 $|Z(G)|$ 是 $2,4$ 或 $8$。后两种可能均被排除：中心阶为 8 就交换；中心阶为 4 则中心商阶为 2，由引理 6.3 仍交换。因此写

$$Z(G)=\{e,z\},\qquad z^2=e.$$

中心商阶为 4 且不能循环，故由定理 6.5

$$G/Z(G)\cong C_2^2.$$

取 $x,y$ 使 $xZ(G),yZ(G)$ 为商群的两个独立非零元素。商群中的基表示说明每个元素都能写成 $z^\epsilon x^iy^j$，其中 $\epsilon,i,j\in\{0,1\}$。若两个表达式相同，投到商群得 $i,j$ 分别相同，消去 $x^iy^j$ 后再由 $z$ 的阶得 $\epsilon$ 相同，故坐标唯一。若 $x,y$ 交换，这些表达式之间都交换，导致 $G$ 交换。因此 $[x,y]\neq e$。由于商群交换，$[x,y]\in Z(G)$，故

$$[x,y]=z,\qquad xy=z\,yx,\qquad x^2,y^2\in\{e,z\}.\tag{6.2}$$

第一种情形为 $x^2=y^2=z$。第四章的四元数模型有唯一坐标 $(-1)^\epsilon\mathbf{i}^i\mathbf{j}^j$，满足 $\mathbf{i}^2=\mathbf{j}^2=-1$、$\mathbf{ij}=(-1)\mathbf{ji}$。$G$ 中的坐标乘法完全由式 (6.2) 决定：相邻的 $y$ 移过 $x$ 产生一个 $z$，两次 $x$ 或两次 $y$ 也产生一个 $z$，且 $z$ 中央。写成公式为

$$(z^\epsilon x^iy^j)(z^\eta x^ky^\ell)=z^{\epsilon+\eta+jk+\lfloor(i+k)/2\rfloor+\lfloor(j+\ell)/2\rfloor}x^{\,i+k \bmod 2}y^{\,j+\ell \bmod 2}.$$

$z$ 的指数模 2。这也是四元数模型的乘法公式。因此引理 6.1 给出 $G\cong Q_8$。

第二种情形为 $x^2=e, y^2=z$。令 $r=y, s=x$，则 $r$ 阶为 4，$s$ 阶为 2，且

$$srs^{-1}=xyx^{-1}=zy=y^{-1}=r^{-1}.$$

若 $x^2=z, y^2=e$，令 $r=x, s=y$，由 (6.2) 得到相同关系。这两种情况下 $\langle r\rangle$ 阶为 4，$s\notin\langle r\rangle$；否则 $x,y$ 同在循环群中会交换。于是每个元素唯一为 $r^is^j$ $(0\le i<4, 0\le j<2)$，乘法为

$$(r^is^j)(r^ks^\ell)=r^{i+(-1)^jk}s^{j+\ell}.$$

这与二面体模型的乘法相同，故 $G\cong D_8$。

第三种情形为 $x^2=y^2=e$。令 $r=xy, s=x$。利用 $yx=zxy$，

$$r^2=x(yx)y=x(zxy)y=z,\qquad srs^{-1}=x(xy)x=yx.$$

又 $r^2=z$ 且 $z^2=e$，故 $r^{-1}=r^3=zr=zxy=yx$。因此 $r$ 阶为 4、$s$ 阶为 2，且 $srs^{-1}=r^{-1}$。$r,s$ 生成 $G$，因为 $x=s, y=sr$。由上一段的唯一坐标与乘法，再得 $G\cong D_8$。

这些情形穷尽 $x^2,y^2\in\{e,z\}$ 的四种组合。最后区分同构类型：三个交换群已由最大元素阶区分；$D_8, Q_8$ 均不交换，不能与前三者同构。在 $D_8$ 中，$r^2$ 与四个 $r^is$ 都为二阶元，其他非单位旋转阶为 4，所以二阶元恰有五个。在 $Q_8$ 中，$-1$ 是唯一二阶元，$\pm i,\pm j,\pm k$ 均平方为 $-1$。所以后二者也不同构。 □

**命题 6.15** (八阶五个模型的全部子群)**.** *沿用定理 6.14 的记号。五个模型的子群可以逐一列出如下；记号 $\langle X\rangle$ 表示由集合 $X$ 生成的子群。*

| 模型 $G$ | 阶 2 子群 | 阶 4 子群 | 子群总数 |
|---|---|---|---|
| $C_8=\langle a\rangle$ | $\langle a^4\rangle$ | $\langle a^2\rangle$ | 4 |
| $C_4\times C_2=\langle a,b\mid a^4=b^2=1,\ ab=ba\rangle$ | $\langle a^2\rangle,\langle b\rangle,\langle a^2b\rangle$ | $\langle a\rangle,\langle ab\rangle,\langle a^2,b\rangle$ | 8 |
| $C_2^3$ | 7 个 | 7 个 $C_2^2$ | 16 |
| $D_8=\langle r,s\mid r^4=s^2=1,\ srs=r^{-1}\rangle$ | $\langle r^2\rangle,\langle r^is\rangle$ $(0\le i<4)$ | $\langle r\rangle,\langle r^2,s\rangle,\langle r^2,rs\rangle$ | 10 |
| $Q_8$ | $\langle -1\rangle$ | $\langle i\rangle,\langle j\rangle,\langle k\rangle$ | 6 |

*除表中列出的子群外，每一行还包括平凡子群 1 与整个群 $G$；在 $C_8$ 一行，$\langle a^4\rangle$ 与 $\langle a^2\rangle$ 已包含全部真非平凡子群。*

*证明.* 先看循环群。$C_8$ 的子群与 8 的正因子一一对应，分别是

$$1,\quad \langle a^4\rangle,\quad \langle a^2\rangle,\quad \langle a\rangle.$$

对 $C_4\times C_2$，每个元素唯一写成 $a^ib^j$，其中 $0\le i<4$、$j\in\{0,1\}$。平方为

$$(a^ib^j)^2=a^{2i}.$$

所以非单位二阶元恰为 $a^2, b, a^2b$，从而得到表中的三个阶二子群。阶四元恰为 $a, a^3, ab, a^3b$；它们分别生成 $\langle a\rangle$ 与 $\langle ab\rangle$。最后，任何阶四子群若不含阶四元，就只能由两个独立二阶元生成；三阶二子群中只有

$$\langle a^2,b\rangle=\{1,a^2,b,a^2b\}$$

具有这种情形。由于子群阶只能为 $1,2,4,8$，列举已穷尽全部子群。

把 $C_2^3$ 看成三维向量空间 $V=\mathbb{F}_2^3$。子群对加法封闭，而 $\mathbb{F}_2$ 的标量只有 $0,1$，故子群恰为线性子空间。每个非零向量独自生成一条直线，所以一维子空间有 $2^3-1=7$ 个。为数二维

子空间，先数有序线性无关向量对：第一向量有 7 种选择，第二向量不能在第一向量生成的二元子空间中，故有 $8-2=6$ 种选择。每个二维子空间中第一向量有 3 种、第二向量有 2 种选择。因此二维子空间数为

$$\frac{7\cdot 6}{3\cdot 2}=7.$$

另有零空间与全空间，总计 $1+7+7+1=16$ 个子群。

对 $D_8$，每个元素唯一为 $r^i$ 或 $r^is$。其中 $r^2$ 是唯一的非单位旋转二阶元，而

$$(r^is)^2=r^isr^is=r^i(sr^i s)=r^ir^{-i}=1$$

说明四个反射也各自生成阶二子群。于是表中列出的五个阶二子群已经穷尽所有阶二子群。阶四子群若含 $r$，便是 $\langle r\rangle$；若含另一个阶四元 $r^3$，也因 $(r^3)^3=r$ 而回到该情形。剩下的阶四子群中每个非单位元阶为二；它必须含反射。若含两个不同反射，其乘积为非单位旋转，只能是 $r^2$；若只含一个反射，则至多含 $1,r^2$ 与这个反射，不能有四个元素。因此它必含 $r^2$ 以及两个反射。两个反射 $r^is, r^js$ 的乘积为 $r^{i-j}$；要使生成子群只有四个元素，必须 $i-j\equiv 2 \pmod 4$。因此只有

$$\langle r^2,s\rangle=\{1,r^2,s,r^2s\},\qquad \langle r^2,rs\rangle=\{1,r^2,rs,r^3s\}.$$

不存在其他阶四子群；加上 $1, D_8$ 后总数为 10。

最后在 $Q_8=\{\pm1,\pm i,\pm j,\pm k\}$ 中，$-1$ 是唯一二阶元，且每个 $\pm i,\pm j,\pm k$ 的平方都是 $-1$。因此三个阶四子群恰为 $\langle i\rangle,\langle j\rangle,\langle k\rangle$；任何含有其中一个四阶元的子群都已经包含相应的阶四子群，故不再产生新的真子群。连同 1 与 $Q_8$，总数为 6。 □

**例 6.16** (四元数中心的扩张不分裂)**.** 精确列

$$1\longrightarrow\{1,-1\}\longrightarrow Q_8\longrightarrow C_2^2\longrightarrow 1$$

没有补子群。先列出全部子群：非单位元除了 $-1$ 外都为四阶元，每个生成 $\langle i\rangle,\langle j\rangle,\langle k\rangle$ 中的一者。任意非平凡子群若含一个四阶元，就含其平方 $-1$；若不含四阶元，只能为 $\{1,-1\}$。阶四子群还必须循环，因为若不循环则为 $C_2^2$，会有三个二阶元，而 $Q_8$ 只有一个。因此全部子群正是图 6.1 中的六个。

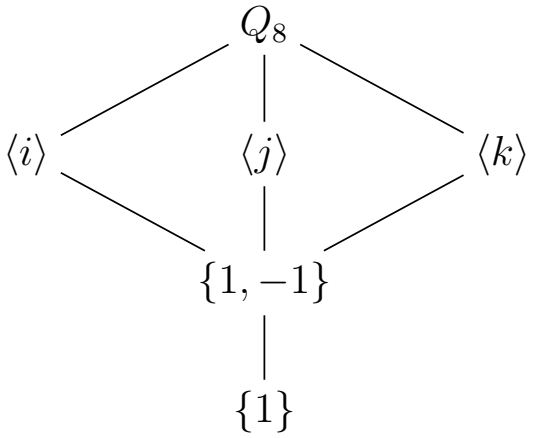



图 6.1: 四元数群的全部子群

图中每条线表示紧邻的真包含，下方的群包含于上方的群。若存在中心的补子群 $H$，则 $|H|=4$ 且 $H\cap\{1,-1\}=1$；但上面已经证明每个非平凡子群都含 $-1$，矛盾。这给出一个有完整模型的非分裂扩张。

## 6.6 十二阶群：非正规 Sylow 子群产生忠实作用

**引理 6.17.** *若 $|G|=12$，且 Sylow 3 子群不正规，则 $G\cong A_4$。*

*证明.* 取 Sylow 3 子群 $P$，令 $G$ 左乘作用在四个左陪集 $G/P$ 上，得到

$$\rho: G\longrightarrow \mathrm{Sym}(G/P)\cong S_4.$$

第五章已经证明作用核为 $\bigcap_{g\in G} gPg^{-1}$，因而是包含在 $P$ 中的正规子群。因 $|P|=3$，核只能为 1 或 $P$。若核为 $P$，则 $P$ 正规，与假设矛盾。所以 $\rho$ 单射，像是 $S_4$ 中的十二阶子群。

记 $K=\rho(G)$。其指数为 2，故正规。商群 $S_4/K$ 阶为 2，交换，所以 $S_4'\le K$。第五章已算出 $S_4'=A_4$：符号使导出群包含于 $A_4$，而换位的交换子给出三循环，三循环生成 $A_4$。因此 $A_4\le K$；两者阶均为 12，故 $K=A_4$。 □

**定理 6.18.** *十二阶群恰有五个同构类型：*

$$C_{12},\quad C_6\times C_2,\quad A_4,\quad S_3\times C_2,\quad T,$$

*其中 $T=C_3\rtimes C_4$ 的作用把 $C_4$ 的生成元送到 $C_3$ 的取逆自同构。*

*证明.* 若 Sylow 3 子群不正规，引理给出 $A_4$。以下设 $N=\langle a\rangle$ 为正规 Sylow 3 子群。取 Sylow 2 子群 $H$，则 $|H|=4$。$N\cap H=1$ 且 $NH=G$，所以 $G=N\rtimes H$。四阶群分类给出 $H\cong C_4$ 或 $C_2^2$。作用的值域为

$$\mathrm{Aut}(C_3)=\{1,\iota\}\cong C_2,\qquad \iota(a)=a^{-1}.$$

先设 $H=\langle b\rangle\cong C_4$。作用由 $b$ 的像确定，只能为 1 或 $\iota$。平凡作用给出 $C_3\times C_4\cong C_{12}$。非平凡作用给出 $T$，具体坐标为

$$T=(\mathbb{Z}/3\mathbb{Z})\times(\mathbb{Z}/4\mathbb{Z}),\qquad (i,j)(k,\ell)=(i+(-1)^j k,\ j+\ell).\tag{6.3}$$

这是合法的半直积，因为 $j\mapsto((-1)^j)$ 是从 $C_4$ 到 $\mathrm{Aut}(C_3)$ 的同态；所以 $T$ 确有 12 个元素，而不是仅由关系猜得的模型。

再设 $H\cong C_2^2$。平凡作用给出

$$C_3\times C_2^2\cong C_6\times C_2.$$

若作用 $\theta: H\to C_2$ 非平凡，其核有两个元素，写成 $\langle c\rangle$。取 $b\notin\ker\theta$，则 $H=\langle b\rangle\times\langle c\rangle$，$b$ 取逆 $a$、$c$ 固定 $a$。任意群元唯一为 $a^ib^jc^k$，其中 $0\le i<3$，$j,k\in\{0,1\}$。其乘法为

$$(a^ib^jc^k)(a^{i'}b^{j'}c^{k'})=a^{i+(-1)^j i'}b^{j+j'}c^{k+k'}.$$

所以坐标映射给出

$$G\cong(C_3\rtimes_{-1}C_2)\times C_2\cong S_3\times C_2.$$

最后一个同构可以具体取 $a \mapsto (123)$、$b \mapsto (12)$；这两个置换满足取逆关系，并生成 $S_3$。任何非平凡 $\theta$ 都可以选择上述 $b, c$，所以三个可能的非平凡同态并不产生三个不同构类型。

这已经证明列表完整，且五个模型均存在。下面证明互不同构。两个交换模型分别含有和不含有阶 12 元。其余三个不交换：$A_4$ 中 (123) 与 (124) 不交换；后两个模型的取逆作用非平凡。

$A_4$ 的阶 3 元恰为八个三循环，因为 $S_4$ 中阶 3 元必须具有一个三循环和一个不动点，其个数为 $4 \cdot 2 = 8$。另外两个非交换模型的三阶元都只能在正规 $C_3$ 中：三阶元投影到四阶补群后的阶同时整除 3 和 4，故像为单位。因此它们各只有两个三阶元，与 $A_4$ 不同构。

最后，$T$ 中的 $(0,1)$ 阶为 4，而 $S_3 \times C_2$ 的元素阶是两个分量阶的最小公倍数；$S_3$ 的元素阶仅为 $1, 2, 3$，故直积中元素阶只能是 $1, 2, 3, 6$，没有阶 4 元。所以最后两个模型也不同构。 □

**命题 6.19** (十二阶五个模型的全部子群)**.** 十二阶分类定理中的五个模型的子群如下。每一项只列出平凡子群与整个群之间的子群。

*(1)* $C_{12} = \langle r \rangle$：

$$\langle r^6 \rangle \cong C_2, \quad \langle r^4 \rangle \cong C_3, \quad \langle r^3 \rangle \cong C_4, \quad \langle r^2 \rangle \cong C_6.$$

因此共有 6 个子群。

*(2)* $C_6 \times C_2 \cong C_3 \times C_2^2$：有三个阶 2 子群、一个阶 3 子群、三个阶 6 子群以及一个 $C_2^2$ 子群，因此共有 10 个子群。

*(3)* $A_4$：有四个 $C_3$ 子群、三个阶 2 子群和一个正规子群 $V_4$，因此共有 10 个子群。

*(4)* $S_3 \times C_2 \cong D_{12} = \langle r, s \mid r^6 = s^2 = 1,\ srs = r^{-1} \rangle$：有一个 $C_2 = \langle r^3 \rangle$、六个反射 $C_2 = \langle r^i s \rangle$、一个 $C_3 = \langle r^2 \rangle$、一个 $C_6 = \langle r \rangle$、三个 $V_4$、两个 $S_3$；加上平凡子群与整个群，共有 16 个子群。

*(5)* $T = \langle a, b \mid a^3 = b^4 = 1,\ bab^{-1} = a^{-1} \rangle$：有唯一的 $C_2 = \langle b^2 \rangle$、唯一的 $C_3 = \langle a \rangle$、三个 $C_4$ 子群

$$\langle b \rangle, \qquad \langle ab \rangle, \qquad \langle a^2 b \rangle,$$

以及唯一的 $C_6 = \langle a, b^2 \rangle$，共有 8 个子群。

证明. $C_{12}$ 的子群由 12 的正因子唯一决定，故第一项直接由循环群子群定理得到。

对 $C_6 \times C_2 \cong C_3 \times V_4$，把两个直积分量识别为 $C_3 \times 1$ 与 $1 \times V_4$。设 $H$ 为子群，任取 $(x, y) \in H$。由 $x^3 = 1, y^2 = 1$，有

$$(x, y)^4 = (x, 1), \qquad (x, y)^3 = (1, y).$$

两个分量都在 $H$，且 $(x, y) = (x, 1)(1, y)$，从而

$$H = \big(H \cap (C_3 \times 1)\big)\big(H \cap (1 \times V_4)\big).$$

交平凡且两个因子相互交换，这个乘积是内部直积。第一交有 $1, C_3$ 两种可能；第二交有 1、三个阶二子群、$V_4$ 共五种可能。设 $V_4 = \langle u, v \rangle$，三个阶二子群为 $L_1 = \langle u \rangle, L_2 = \langle v \rangle, L_3 = \langle uv \rangle$。全部子群便是

$$1, \quad 1 \times L_i, \quad C_3 \times 1, \quad 1 \times V_4, \quad C_3 \times L_i, \quad C_3 \times V_4 \quad (1 \le i \le 3).$$

各交可由 $H$ 唯一恢复，故这些子群没有重复，总数 $2\cdot 5=10$。

在 $A_4$ 中，三个双换位生成三个阶二子群；八个三循环每两个互为逆元，生成四个阶三子群。它们可以取为

$$\langle(123)\rangle,\quad \langle(124)\rangle,\quad \langle(134)\rangle,\quad \langle(234)\rangle.$$

阶四子群中没有四阶元，故由四阶分类必须是 $V_4$；它的三个非单位元只能是全部三个双换位，所以这样的子群唯一。

还须排除阶六子群。若 $H\le A_4$ 阶为六，则其指数为二，故正规，$A_4/H$ 阶为二，因而 $A_4'\le H$。第五章算得 $A_4'=V_4$，于是 $4\mid |H|=6$，与 Lagrange 定理矛盾。子群阶只能是 $1,2,3,4,6,12$，故列表已穷尽，总数 $1+3+4+1+1=10$。

对 $D_{12}$，本章例 6.20 给出了它与 $S_3\times C_2$ 的显式同构。令 $R=\langle r\rangle$。若 $H\subseteq R$，则 $H$ 为

$$1,\quad \langle r^3\rangle,\quad \langle r^2\rangle,\quad R$$

之一。若 $H$ 含反射 $r^is$，令 $H\cap R=\langle r^d\rangle$，其中 $d\mid 6$。对任一另一个反射 $r^js\in H$，

$$(r^js)(r^is)=r^{j-i}\in H\cap R,$$

故 $d\mid j-i$。反过来，$r^{kd}(r^is)=r^{i+kd}s$ 都属于 $H$。因此

$$H=\{r^{kd}:0\le k<6/d\}\ \cup\ \{r^{i+kd}s:0\le k<6/d\}.$$

这还证明了：固定 $d$ 时，两个 $i$ 给出相同子群当且仅当它们模 $d$ 相同；不同 $d$ 则有不同旋转部分。阶为 $12/d$。逐个代入 $d=6,3,2,1$，分别得到六个阶二子群，三个

$$\langle r^3, r^is\rangle\cong V_4\quad (0\le i<3),$$

两个

$$\langle r^2, r^is\rangle\cong D_6\cong S_3\quad (0\le i<2),$$

以及整个群。第一组中 $r^3$ 中央、两个生成元均为二阶，且交平凡；第二组中 $r^2$ 为三阶、反射对它取逆，故有标明的同构。总数为 $4+6+3+2+1=16$。

最后在 $T$ 中置 $a=(1,0), b=(0,1)$，使用式 (6.3)。偶数第二坐标组成子群

$$K=\{a^ib^{2j}:0\le i<3,\ 0\le j<2\}=\langle a\rangle\times\langle b^2\rangle\cong C_6.$$

元素 $ab^2$ 阶为六，因为其 $m$ 次幂为 $a^mb^{2m}$，为单位恰在 $3\mid m$ 且 $2\mid m$ 时成立。故 $K$ 的子群正是 $1,\langle b^2\rangle,\langle a\rangle,K$。

对奇数 $j$，有

$$(a^ib^j)^2=a^i(b^ja^ib^{-j})b^{2j}=a^ia^{-i}b^2=b^2.$$

所以六个奇坐标元素都为四阶元。$g_i=a^ib$ 满足 $g_i^{-1}=g_i^3=a^ib^3$，故六个元素恰生成三个不同的 $\langle g_i\rangle$，$0\le i<3$。

设 $H$ 不包含在 $K$ 中，取其中一个奇坐标元素；换成它的逆元后可写为 $g_i\in H$，于是 $b^2\in H$。若 $H\cap K=\langle b^2\rangle$，任意奇坐标元素 $h\in H$ 都满足 $hg_i^{-1}\in H\cap K$，故

$$H=\{1,b^2,g_i,b^2g_i\}=\langle g_i\rangle.$$

若 $H\cap K$ 更大，由 $K$ 的子群列表及 $b^2\in H$ 可知只能 $H\cap K=K$。此时 $a\in H$，又 $b=a^{-i}g_i\in H$，故 $H=T$。因此没有其他子群，总计 $4+3+1=8$。 □

**例 6.20** (同一群的两种结构)**.** $S_3 \times C_2$ 也同构于 $D_{12}$。在直积中取

$$r = ((123), \bar{1}), \qquad s = ((12), \bar{0}).$$

$r$ 阶为 6，$s$ 阶为 2，且 $srs^{-1} = r^{-1}$。$s \notin \langle r \rangle$，因为 $\langle r \rangle$ 在 $S_3$ 分量中的像只含 $e, (123), (132)$。所以十二个 $r^i s^j$ 互异，构成全群，且乘法为二面体坐标公式。故该例不应被误算成第六种十二阶群。

## 6.7 素数立方阶：中央交换子与幂公式

下面固定 $p$ 为奇素数。先建立非交换 $p^3$ 阶群共享的结构，再区分两种模型。

**引理 6.21.** *设 $G$ 非交换且 $|G| = p^3$。则*

$$|Z(G)| = p, \qquad G/Z(G) \cong C_p^2, \qquad G' = Z(G).$$

*特别地，每个 $x \in G$ 满足 $x^p \in Z(G)$，且所有交换子都是中央元素。*

*证明.* 中心非平凡，阶为 $p, p^2$ 或 $p^3$。若中心阶为 $p^3$，则交换；若中心阶为 $p^2$，中心商阶为 $p$，由引理 6.3 仍交换。所以中心阶为 $p$。商群阶为 $p^2$，由定理 6.5 为交换群，并且不能循环，故为 $C_p^2$。

交换商说明 $G' \le Z(G)$。非交换性说明 $G' \neq 1$；而 $Z(G)$ 阶为素数，只能 $G' = Z(G)$。商群每个元素的 $p$ 次幂为单位，所以 $x^p \in Z(G)$。 □

**引理 6.22** (中央交换子下的乘积幂)**.** *若群中 $[x, y]$ 中央，则对正整数 $n$，*

$$(xy)^n = x^n y^n [y, x]^{n(n-1)/2}.$$

*因此在引理 6.21 的群中，幂映射*

$$P : G \longrightarrow Z(G), \qquad x \longmapsto x^p$$

*是群同态。*

*证明.* 置 $c = [y, x]$，于是 $yx = cxy$，且 $c$ 中央。先对 $n$ 归纳得 $y^n x = c^n x y^n$：$n = 1$ 就是定义；若对 $n$ 成立，则

$$y^{n+1}x = y(c^n x y^n) = c^n (yx) y^n = c^{n+1} x y^{n+1}.$$

再对乘积幂归纳。$n = 1$ 成立。若对 $n$ 成立，则

$$\begin{aligned} (xy)^{n+1} &= x^n y^n c^{n(n-1)/2} xy \\ &= x^n (y^n x) y \, c^{n(n-1)/2} \\ &= x^{n+1} y^{n+1} c^{n + n(n-1)/2} \\ &= x^{n+1} y^{n+1} c^{n(n+1)/2}. \end{aligned}$$

这证明公式。

在 $p^3$ 阶非交换群中，$c \in Z(G)$ 且 $c^p = e$。奇素数 $p$ 整除 $p(p-1)/2$，因此

$$(xy)^p = x^p y^p.$$

由引理 6.21，右侧属于 $Z(G)$，故 $P$ 是取值于中心的群同态。 □

**注 6.23.** $p$ 为奇数用在 $p \mid p(p-1)/2$。$p = 2$ 时乘积平方含有交换子修正项，不能删去。这正是后面分裂结论不能直接套用到 $Q_8$ 的原因。

## 6.8 立方阶的第一个非交换模型：三阶幺上三角群

**命题 6.24.** 设 $p$ 为奇素数，$|G| = p^3$，$G$ 非交换，且每个非单位元阶为 $p$。则 $G \cong U_3(\mathbb{F}_p)$。

证明. 由引理 6.21，取 $x, y$ 使 $xZ(G), yZ(G)$ 是 $G/Z(G)$ 的一组基。因为这些余类生成商，若 $x, y$ 交换，则它们与中央元素一起生成一个交换的 $G$，矛盾。因此

$$z = [x, y] \neq e.$$

$z$ 生成阶为 $p$ 的 $Z(G)$。每个元素唯一写成

$$x^i y^j z^k, \qquad i, j, k \in \{0, \dots, p-1\}.$$

存在性来自商群的基表示；若两个表达式相同，投到商群先得到 $i, j$ 模 $p$ 相同，再用 $z$ 的阶得到 $k$ 相同。

交换子约定给出 $xy = zyx$，即 $yx = z^{-1}xy$。中央性使反复交换合法，故

$$y^j x^{i'} = z^{-ji'} x^{i'} y^j.$$

于是

$$(x^i y^j z^k)(x^{i'} y^{j'} z^{k'}) = x^{i+i'} y^{j+j'} z^{k+k'-ji'}. \tag{6.4}$$

各指数模 $p$，因为题设给出 $x^p = y^p = z^p = e$。

在 $U_3(\mathbb{F}_p)$ 中取矩阵

$$X = I + E_{12}, \qquad Y = I + E_{23}, \qquad Z = I + E_{13}.$$

矩阵单位满足 $E_{12}E_{23} = E_{13}$，而反序乘积为零，所以 $XY = ZYX$。$Z$ 中央，且三个矩阵的 $p$ 次幂均为 $I$。每个 $X^i Y^j Z^k$ 的矩阵是

$$\begin{pmatrix} 1 & i & ij + k \\ 0 & 1 & j \\ 0 & 0 & 1 \end{pmatrix}.$$

三个参数唯一，且遍历所有幺上三角矩阵。因此这些矩阵也有式 (6.4) 的坐标乘法。引理 6.1 给出所求同构。

还需验证该模型确实满足“非单位元阶为 $p$”。任取严格上三角三阶矩阵 $N$，有 $N^3 = 0$。因 $p \geq 3$，$N^p = 0$；又二项式系数 $\binom{p}{k}$ $(1 \leq k < p)$ 在特征 $p$ 中为零，故

$$(I + N)^p = I + N^p = I.$$

非单位元阶整除素数 $p$，所以恰为 $p$。$X, Y$ 不交换，故模型非交换。 □

## 6.9 立方阶的第二个非交换模型：循环核的分裂

**命题 6.25.** 设 $p$ 为奇素数，$|G| = p^3$，$G$ 非交换且有阶 $p^2$ 元。则

$$G \cong M_p := C_{p^2} \rtimes C_p,$$

其中补群生成元对循环核生成元的作用为 $a \mapsto a^{1+p}$。

证明. 取 $|a|=p^2$，置 $N=\langle a\rangle$。$[G:N]=p$，由第五章最小素因子指数的正规性判据，$N$ 正规。这里所有素因子均为 $p$，满足该判据。

先证明存在阶为 $p$ 的元素 $b\notin N$。由引理 6.22，$P(x)=x^p$ 为同态，像包含 $a^p\neq e$，且包含在阶 $p$ 的中心中。因此像恰等于中心，核有 $p^2$ 个元素。$N$ 中被 $P$ 杀掉的元素恰为

$$e, a^p, a^{2p}, \dots, a^{(p-1)p},$$

仅有 $p$ 个。因此存在 $b\in\ker P\setminus N$。$b\neq e$ 且 $b^p=e$，所以 $|b|=p$。

$N\cap\langle b\rangle=1$，而两者乘积阶为 $p^3$，故 $G=N\rtimes\langle b\rangle$。写

$$bab^{-1}=a^u,\qquad u\in(\mathbb{Z}/p^2\mathbb{Z})^\times.$$

作用非平凡，否则 $a,b$ 交换并生成一个交换群。又因 $b^p=e$，有 $u^p\equiv 1 \pmod{p^2}$。把它模 $p$ 化简，并用 $\bar{u}^p=\bar{u}$，得 $\bar{u}=1$。所以

$$u=1+cp \pmod{p^2},\qquad c\not\equiv 0 \pmod{p}.$$

取 $r$ 使 $cr\equiv 1 \pmod{p}$，令 $b'=b^r$。$b'$ 仍生成同一补群；二项式展开给出

$$u^r=(1+cp)^r\equiv 1+crp\equiv 1+p \pmod{p^2}.$$

因此 $b'ab'^{-1}=a^{1+p}$。

反过来，$u_0=1+p$ 在模 $p^2$ 的单位群中阶恰为 $p$，因为

$$(1+p)^j\equiv 1+jp \pmod{p^2},$$

而 $1\le j<p$ 时右侧不为 1。所以此作用定义实际存在的半直积 $M_p$。其坐标及乘法为

$$M_p=(\mathbb{Z}/p^2\mathbb{Z})\times(\mathbb{Z}/p\mathbb{Z}),\qquad (i,j)(k,\ell)=(i+(1+p)^j k, j+\ell). \tag{6.5}$$

原群中每个元素唯一为 $a^i(b')^j$，且有同样乘法，故与模型同构。该模型的 $(1,0)$ 阶为 $p^2$，所以不与命题 6.24 的模型同构。 □

## 6.10 奇素数立方阶的完整表

**命题 6.26.** *阶为 $p^3$ 的交换群恰有三个同构类型：*

$$C_{p^3},\qquad C_{p^2}\times C_p,\qquad C_p^3.$$

*此结论对 $p=2$ 也成立。*

证明. 有阶 $p^3$ 元时群循环。否则，若存在 $|a|=p^2$，取 $b\notin\langle a\rangle$。商群阶为 $p$，所以 $b^p\in\langle a\rangle$。因为没有阶 $p^3$ 元，$b^{p^2}=e$，于是 $b^p$ 的阶整除 $p$。循环群 $\langle a\rangle$ 中这类元素恰为 $a^{pt}$，故 $b^p=a^{pt}$。令 $c=ba^{-t}$，由交换性，

$$c^p=b^pa^{-pt}=e.$$

$c\notin\langle a\rangle$，否则 $b$ 也在其中。因此 $\langle c\rangle$ 阶为 $p$、与 $\langle a\rangle$ 交平凡，两者乘积为 $G$，给出 $C_{p^2}\times C_p$。

若没有阶 $p^2$ 元，则每个非单位元阶为 $p$。取 $a\neq e$，再取 $b\notin\langle a\rangle$。若 $a^ib^j=e$ 且 $j$ 模 $p$ 非零，取 $jt\equiv 1 \pmod{p}$，由交换性有 $b=(b^j)^t=a^{-it}\in\langle a\rangle$，矛盾。因此 $j=0$，再由 $a$ 的阶得 $i=0$。所以 $a,b$ 生成的子群是含 $p^2$ 个元素的交换群。

再取 $c \notin \langle a,b\rangle$。若 $a^i b^j c^k = e$ 且 $k \neq 0$（模 $p$），取 $kt \equiv 1 \pmod p$，得到 $c = (a^{-i}b^{-j})^t \in \langle a,b\rangle$，矛盾。故 $k=0$，进而由上一段得到 $i=j=0$。映射

$$\mathbb{F}_p^3 \longrightarrow G, \qquad (i,j,k) \longmapsto a^i b^j c^k$$

因三生成元的 $p$ 次幂为一而良定义，因交换性而保持加法，因上述核计算而单射，因两端都有 $p^3$ 元素而满射。因此 $G \cong C_p^3$。

模型均存在，且最大元素阶分别是 $p^3, p^2, p$，所以互不同构。 □

**定理 6.27.** *若 $p$ 为奇素数，阶为 $p^3$ 的群恰有五个同构类型：*

$$C_{p^3}, \quad C_{p^2} \times C_p, \quad C_p^3, \quad U_3(\mathbb{F}_p), \quad M_p.$$

*证明.* 交换情形由命题 6.26 分类。非交换群没有阶为 $p^3$ 的元素，否则循环；因此非单位元阶只能为 $p$ 或 $p^2$。若全部为 $p$，由命题 6.24 得 $U_3(\mathbb{F}_p)$；若有阶 $p^2$ 元，由命题 6.25 得 $M_p$。

前三个群交换，后两个不交换；前三者已由最大元素阶区分，后两者也由是否存在阶 $p^2$ 元区分。所以五者互不同构，且所有模型均已构造。 □

**例 6.28** (阶 27)**.** 取 $p=3$，五种模型为

$$C_{27}, \quad C_9 \times C_3, \quad C_3^3, \quad U_3(\mathbb{F}_3), \quad M_3.$$

$M_3$ 的乘法中作用参数为 $1+3=4$（模 9），因为 $4^3 \equiv 1 \pmod 9$ 而 $4, 4^2 \neq 1$。$U_3(\mathbb{F}_3)$ 的所有非单位元阶为 3，$M_3$ 则含阶 9 元。它们都是幂零类为 2 的群，但幂零类并不能区分这两个同构类型。

## 6.11 结构不变量：从分类表回到群本身

**命题 6.29** (十二阶模型的独立不变量表)**.** *五个十二阶模型可以用下列不变量独立区分：*

| $G$ | $\lvert Z(G)\rvert$ | $\lvert G'\rvert$ | $\#\{g : \lvert g\rvert = 3\}$ | $\#\{g : \lvert g\rvert = 4\}$ |
|---|---|---|---|---|
| $C_{12}$ | 12 | 1 | 2 | 2 |
| $C_6 \times C_2$ | 12 | 1 | 2 | 0 |
| $A_4$ | 1 | 4 | 8 | 0 |
| $S_3 \times C_2$ | 2 | 3 | 2 | 0 |
| $T$ | 2 | 3 | 2 | 6 |

*这里第一列的 $\lvert G'\rvert = 1$ 表示导出群平凡，最后两列均不计单位元。*

*证明.* $C_{12}$ 的元素阶由循环群公式给出：阶 3 元有 $\varphi(3)=2$ 个，阶 4 元有 $\varphi(4)=2$ 个。$C_6 \times C_2$ 中元素阶为两个分量阶的最小公倍数；前一分量的阶只能为 $1,2,3,6$，后一分量的阶只能为 $1,2$，故没有阶 4 元，而阶 3 元恰来自 $C_6$ 的两个三阶元与 $C_2$ 的单位元。两者交换，故中心为自身、导出群平凡。

$A_4$ 的非单位元由三个双换位和八个三循环组成。三循环给出八个三阶元，没有四阶元；中心只有单位元：三循环与另一个三循环有不相交的三阶子群且不全交换，而三个双换位被 $(123)$ 共轭循环置换，故没有非单位双换位中央；更具体地 $[(123),(124)] = (12)(34) \neq 1$，共轭重新标号使任一三循环也不中央。第五章已经证明 $A_4' = V_4$，故导出群阶为 4。

$S_3 \times C_2$ 的中心是 $1 \times C_2$，所以中心阶为 2。阶 3 元只能由 $S_3$ 的两个三循环与第二分量单位元组成；两分量阶的最小公倍数不可能为 4。又

$$(S_3 \times C_2)' = S_3' \times 1 \cong C_3,$$

所以导出群阶为 3。

对 $T$, 正规核 $\langle a\rangle$ 给出两个非单位三阶元。若 $(i,j)$ 与 $(1,0)$ 交换, 由式 (6.3) 得 $(-1)^j = 1$, 故 $j = 0$ 或 2。再要求 $(i,j)$ 与 $(0,1)$ 交换，由

$$(i,j)(0,1) = (i,j+1), \qquad (0,1)(i,j) = (-i,j+1)$$

得 $2i = 0$（模 3），即 $i = 0$。与 $a, b$ 都交换的元素与它们的任意乘积都交换，所以这两个条件也充分。因此

$$Z(T) = \{(0,0),(0,2)\}, \qquad |Z(T)| = 2.$$

由

$$[(0,1),(1,0)] = (1,0)$$

可知 $\langle(1,0)\rangle \le T'$。另一方面，模去此子群的商为交换群 $C_4$，故 $T' \le \langle(1,0)\rangle$；两边合并得到 $|T'| = 3$。奇数 $j$ 时，上述子群计算已经给出 $(i,j)^2 = (0,2)$、$(i,j)^4 = (0,0)$，故六个元素均为四阶。偶数 $j$ 时元素位于循环群 $K \cong C_6$，阶整除六，不可能为四。因此四阶元恰有六个。表中关于 $T$ 的数据随即得到。 □

**命题 6.30.** *对奇素数 $p$，$M_p$ 满足*

$$Z(M_p) = M_p' = \langle a^p\rangle, \qquad M_p/Z(M_p) \cong C_p^2.$$

*其阶为 $p$ 的非单位元恰有 $p^2-1$ 个，阶为 $p^2$ 的元素恰有 $p^3-p^2$ 个。*

*证明.* 沿用式 (6.5)，把 $(i,j)$ 写为 $a^ib^j$。若它与 $a$ 交换，则

$$a^ib^jab^{-j}a^{-i} = a^{(1+p)^j} = a$$

要求 $(1+p)^j \equiv 1 \pmod{p^2}$，因此 $j = 0$（模 $p$）。接着 $a^i$ 与 $b$ 交换当且仅当

$$a^{(1+p)i} = a^i, \qquad p^2 \mid pi,$$

即 $p \mid i$。所以中心恰为 $\langle a^p\rangle$。

又

$$[b,a] = bab^{-1}a^{-1} = a^p.$$

所以 $\langle a^p\rangle \le M_p'$。模去此子群后，$a, b$ 的像阶均为 $p$ 且交换，故商群交换，推出反向包含。中心商有 $p^2$ 个元素，且两个生成元的像独立，所以为 $C_p^2$。

最后计算元素的 $p$ 次幂。由坐标乘法归纳，

$$(a^ib^j)^p = a^{\,i\sum_{t=0}^{p-1}(1+p)^{tj}}b^{pj}.$$

模 $p^2$ 有 $(1+p)^{tj} \equiv 1 + tjp$，因此

$$\sum_{t=0}^{p-1}(1+p)^{tj} \equiv p + jp\frac{p(p-1)}{2} \equiv p \pmod{p^2}.$$

于是 $(a^ib^j)^p = a^{ip}$，为单位当且仅当 $p \mid i$。满足条件的 $i$ 有 $p$ 个，$j$ 有 $p$ 个，故包括单位在内恰有 $p^2$ 个元素被 $p$ 次幂杀掉。去掉单位就是 $p^2-1$ 个阶 $p$ 元，余下 $p^3-p^2$ 个元素阶为 $p^2$。 □

## 6.12 中心商上的交替形式与正规子群

**命题 6.31.** 设 $G$ 非交换且 $|G|=p^3$，其中 $p$ 为奇素数。选 $x,y$ 使其余类生成 $V=G/Z(G)$，并令 $z=[x,y]$。把 $V$ 识别为二维 $\mathbb{F}_p$ 向量空间、把 $Z(G)=\langle z\rangle$ 识别为 $\mathbb{F}_p$ 的加法群。公式

$$[g,h]=z^{\beta(gZ(G),hZ(G))}$$

定义 $V$ 上一个非退化交替双线性形式，且

$$\beta((i,j),(k,\ell))=i\ell-jk.$$

$p$ 次幂还诱导一个线性映射 $V\to\mathbb{F}_p$，在 $U_3(\mathbb{F}_p)$ 中为零，在 $M_p$ 中非零。

证明. 若把 $g,h$ 换成 $gz^a,hz^b$，中央因子在交换子中全部抵消：

$$(gz^a)(hz^b)(gz^a)^{-1}(hz^b)^{-1}=ghg^{-1}h^{-1}.$$

所以 $\beta$ 与代表元选择无关。$z$ 阶为 $p$，故其指数在 $\mathbb{F}_p$ 中唯一。又因 $V\cong C_p^2$，其标量乘法由 $t(gZ(G))=g^tZ(G)$ 给出，整数 $t$ 改变 $p$ 的倍数不改变余类；这使加法群成为 $\mathbb{F}_p$ 向量空间。

写 $g=x^iy^jz^a,h=x^ky^\ell z^b$。因 $yx=z^{-1}xy$，

$$gh=x^{i+k}y^{j+\ell}z^{a+b-jk},\qquad hg=x^{i+k}y^{j+\ell}z^{a+b-\ell i}.$$

两式中的 $x,y$ 幂相同，即便指数超过 $p-1$ 也可相互消去，故

$$gh=z^{i\ell-jk}hg,\qquad [g,h]=z^{i\ell-jk}.$$

由这个坐标公式，$\beta$ 对两个变量分别线性，且 $\beta(v,v)=0$。若 $\beta((i,j),w)=0$ 对所有 $w$ 成立，先代 $w=(0,1)$ 得 $i=0$，再代 $w=(1,0)$ 得 $j=0$，故非退化。

已知 $P(g)=g^p$ 为中心值同态。若 $g$ 换成 $gz^a$，则

$$(gz^a)^p=g^pz^{ap}=g^p,$$

故 $P$ 降到 $V$；同态性给出加法性，$P(g^t)=P(g)^t$ 给出 $\mathbb{F}_p$ 标量相容性。因此降下的映射线性。$U_3(\mathbb{F}_p)$ 的元素 $p$ 次幂都为单位，故为零映射；$M_p$ 中 $P(a)=a^p\neq e$，故非零。 □

**推论 6.32.** 两个非交换 $p^3$ 阶群都恰有 $p^2+p-1$ 个共轭类；其中 $p$ 个类为单点，其余 $p^2-1$ 个类大小为 $p$。

证明. 中心的 $p$ 个元素各自形成单点类。固定 $g\notin Z(G)$，其余类 $v$ 非零。元素 $h$ 中心化 $g$ 当且仅当 $\beta(v,hZ(G))=0$。若 $v=(i,j)$ 且 $i\neq0$，则 $i\ell-jk=0$ 等价于 $\ell=ji^{-1}k$，恰有 $p$ 个解；若 $i=0$，则 $j\neq0$，方程要求 $k=0$，也恰有 $p$ 个解。因此 $C_G(g)$ 的中心商有 $p$ 个元素，而每个余类包含 $p$ 个元素，得到 $|C_G(g)|=p^2$。

轨道–稳定子公式给出共轭类大小 $[G:C_G(g)]=p$。非中心元素共 $p^3-p$ 个，故类数为 $(p^3-p)/p=p^2-1$；加上中央类就得到 $p^2+p-1$。 □

**命题 6.33.** 非交换 $p^3$ 阶群的正规子群恰为

$$1,\quad Z(G),\quad \text{全部}p+1\text{ 个阶}p^2\text{ 子群},\quad G.$$

阶 $p^2$ 子群与 $V=G/Z(G)$ 的一维子空间一一对应。

证明. 若 $H$ 阶为 $p^2$，则 $H$ 指数为最小素因子 $p$，所以正规。$G/H$ 阶为 $p$，交换，故 $G' = Z(G) \le H$。反过来，$V$ 的任意一维子空间 $L$ 是子群，其原像阶为 $p \cdot p = p^2$。子群对应给出双射。二维空间的非零向量有 $p^2 - 1$ 个，每条直线有 $p - 1$ 个非零向量，不同直线的非零向量不相交，所以直线数为

$$\frac{p^2 - 1}{p - 1} = p + 1.$$

若 $K$ 是阶为 $p$ 的正规子群，共轭定义同态 $G \to \mathrm{Aut}(K)$。其像阶整除 $p^3$，也整除 $|\mathrm{Aut}(C_p)| = p - 1$，故像平凡。因此所有 $G$ 元素与 $K$ 交换，得到 $K \le Z(G)$。两者阶相同，故 $K = Z(G)$。Lagrange 定理说明其他子群阶只可能为 $1, p^3$，对应列表中的两端；列表因而完整。 □

**注 6.34.** $U_3(\mathbb{F}_p)$ 与 $M_p$ 不仅中心阶、导出群阶、中心商相同，还具有相同的共轭类大小分布和上述正规子群结构。这些不变量依然不能判定同构；区分它们的是幂映射，而不是分类表的外观。中心商上的 $\beta$ 与 $P$ 将交换关系和幂关系分开记录，也把本章的具体分类接到第四章的扩张坐标。

## 6.13 八阶与十二阶的正规子群、商群和 Sylow 数据

**命题 6.35** (二面体群的子群、正规性与商)**.** 在 $D_{2n} = \langle r, s \mid r^n = s^2 = 1, srs = r^{-1} \rangle$ 中，全部子群恰为

$$R_d = \langle r^d \rangle \quad (d \mid n), \qquad H_{d,i} = \langle r^d, r^i s \rangle \quad (d \mid n,\ 0 \le i < d).$$

$R_d$ 阶为 $n/d$，全部正规，且 $D_{2n}/R_d \cong D_{2d}$。$H_{d,i}$ 阶为 $2n/d$；它正规当且仅当 $d = 1$ 或 $d = 2$。后一种情形的商为 $C_2$。这里 $D_2 = C_2$、$D_4 = C_2^2$ 按同一坐标模型解释。

证明. 令 $R = \langle r \rangle$。子群若包含于 $R$，由循环群子群定理恰为 $R_d$。否则取其中一个 $r^i s$，并写其与 $R$ 的交为 $R_d$。两个反射乘积为旋转的论证与十二阶情形完全一致，展开为

$$(r^j s)(r^i s) = r^{j-i} \in R_d \quad \Longleftrightarrow \quad d \mid j - i.$$

因此子群恰由 $R_d$ 与一个陪集 $R_d r^i s$ 构成；每部分各 $n/d$ 个元素。$i$ 模 $d$ 唯一，所以列表无重复。

$r$ 共轭固定 $R_d$，$s$ 把 $r^d$ 送到 $r^{-d}$，故 $R_d$ 正规。映射

$$D_{2n} \longrightarrow D_{2d}, \qquad r^i s^j \longmapsto (i \bmod d, j)$$

由二面体乘法公式为满同态，核恰为 $R_d$，得到所述商。

$H_{d,i}$ 的旋转部分已被共轭保持。对它的一个反射生成元，

$$r(r^i s)r^{-1} = r^{i+2} s, \qquad s(r^i s)s^{-1} = r^{-i} s.$$

要使第一个属于 $H_{d,i}$，必须 $d \mid 2$。若 $d = 1$ 或二，则又有 $d \mid 2i$，所以第二个也属于该子群；两个生成元 $r, s$ 的共轭均保持它，故正规。$d = 1$ 给全群；$d = 2$ 给指数二子群，其商为 $C_2$。 □

**命题 6.36** (八阶模型的正规子群与商)**.** 三个交换八阶模型的每个子群都正规。其商可由以下列表完全读出：

1. $C_8/\langle a^d \rangle \cong C_d$，$d \mid 8$。

2. 在 $C_4 \times C_2 = \langle a, b\rangle$ 中，模去 $\langle a^2\rangle$ 得 $C_2^2$；模去 $\langle b\rangle$ 或 $\langle a^2 b\rangle$ 得 $C_4$；模去任一阶四子群得 $C_2$。

3. $C_2^3/W \cong C_2^{3-\dim W}$。

$D_8$ 的正规子群恰为

$$1,\ \langle r^2\rangle,\ \langle r\rangle,\ \langle r^2, s\rangle,\ \langle r^2, rs\rangle,\ D_8.$$

模去 $\langle r^2\rangle$ 得 $C_2^2$，模去任一阶四子群得 $C_2$。$Q_8$ 的六个子群全部正规；模去中心得 $C_2^2$，模去任一阶四子群得 $C_2$。两端的商分别为原群与平凡群。

证明. 交换群的子群由共轭恒等而全部正规。循环商公式由 $a$ 的像阶为 $d$ 得到。对 $C_4 \times C_2$，模去 $\langle a^2\rangle$ 后 $a, b$ 的像均二阶且独立，故为 $C_2^2$；模去 $\langle b\rangle$ 后 $a$ 的像仍四阶并生成商；模去 $\langle a^2 b\rangle$ 后 $b$ 的像等于 $a^2$ 的像，而 $a^2$ 不在该二元核中，故 $a$ 的像仍四阶。任一阶四子群的商为二阶，故循环。向量空间商取一组 $W$ 的基再扩为全空间的基，剩下的基向量余类给出维数 $3 - \dim W$，所以第三式成立。

$D_8$ 的列表和商由命题 6.35 取 $n = 4$ 得到。$Q_8$ 的阶四子群指数二，故正规；中心与平凡子群、全群也正规，已有全部六个。模去中心后 $i, j$ 的像均为二阶，彼此交换且独立，所以商为 $C_2^2$；其余非平凡真商阶二，所以为 $C_2$。 □

**命题 6.37** (十二阶模型的正规子群与商). 前述全部子群列表中，正规者及其非平凡真商如下：

1. $C_{12}$ 的子群全正规，$C_{12}/\langle r^d\rangle \cong C_d$。

2. $C_3 \times V_4$ 的子群全正规，且

$$(C_3 \times V_4)/(B \times W) \cong (C_3/B) \times (V_4/W).$$

3. $A_4$ 的正规子群恰为 $1, V_4, A_4$，且 $A_4/V_4 \cong C_3$。

4. $D_{12}$ 的正规子群恰为

$$1,\ \langle r^3\rangle,\ \langle r^2\rangle,\ \langle r\rangle,\ \langle r^2, s\rangle,\ \langle r^2, rs\rangle,\ D_{12}.$$

其中分别模去三个非平凡旋转子群，得到 $S_3, C_2^2, C_2$；模去后面两个阶六子群都得到 $C_2$。

5. $T$ 的正规子群恰为

$$1,\ \langle b^2\rangle,\ \langle a\rangle,\ \langle a, b^2\rangle,\ T.$$

三个非平凡真商依次为 $S_3, C_4, C_2$。

证明. 第一、二项由交换性以及直积商映射给出；后者映射 $(x, y) \mapsto (xB, yW)$ 的核正是 $B \times W$。

在 $A_4$ 中，三个双换位被一个三循环共轭循环置换，所以三个阶二子群均不正规。四个阶三子群是 Sylow 子群，彼此共轭且有四个，所以也不正规。唯一阶四子群 $V_4$ 在任何自同构下不变，尤其正规。子群列表中已无其他阶，故正规列表穷尽；商阶为三，所以循环。

$D_{12}$ 的结论由二面体命题取 $n = 6$ 得到。$D_6 \cong S_3$ 的同构把三阶旋转送到 (123)、反射送到 (12)，六个唯一坐标相符；$D_4 \cong C_2^2$，因为旋转与反射均二阶且交换。

在 $T$ 中，$\langle b^2\rangle$ 中央；$\langle a\rangle$ 是半直积核；$K = \langle a, b^2\rangle$ 指数二，故三者正规。三个阶四子群不正规：用 $ab^i a^{-1}$ 的关系，特别是

$$aba^{-1} = a^2 b,$$

说明 $a$ 共轭把 $\langle b\rangle$ 送到另一个阶四子群；继续共轭依次得到全部三个，故没有一个固定。模去 $\langle b^2\rangle$，$a$ 的像三阶、$b$ 的像二阶且对 $a$ 取逆，所以商为 $S_3$；模去 $\langle a\rangle$ 得 $C_4$；模去 $K$ 得 $C_2$。这给出全部商。 □

**命题 6.38** (十二阶完整元素阶与 Sylow 数表)**.** *记 $n_2, n_3$ 为 Sylow 二子群、三子群的个数。以下每行的元素阶数之和加上单位元均为十二：*

| $G$ | $\nu_2$ | $\nu_3$ | $\nu_4$ | $\nu_6$ | $\nu_{12}$ | $n_2$ | $n_3$ |
|---|---|---|---|---|---|---|---|
| $C_{12}$ | 1 | 2 | 2 | 2 | 4 | 1 | 1 |
| $C_6 \times C_2$ | 3 | 2 | 0 | 6 | 0 | 1 | 1 |
| $A_4$ | 3 | 8 | 0 | 0 | 0 | 1 | 4 |
| $D_{12}$ | 7 | 2 | 0 | 2 | 0 | 3 | 1 |
| $T$ | 1 | 2 | 6 | 2 | 0 | 3 | 1 |

*证明.* $C_{12}$ 中阶 $d$ 的元素为 $r^{12k/d}$、$1 \le k \le d$ 且 $\gcd(k,d)=1$，逐个数 $d=2,3,4,6,12$ 得到第一行。$C_3 \times V_4$ 中，非单位二分量有三个；三分量非单位有两个；两个分量均非单位时阶为六，共 $2\cdot 3 = 6$ 个。交换群的 Sylow 子群唯一。

$A_4$ 的三双换位、八三循环已计数；唯一阶四子群为 Sylow 二子群，四个三阶子群为 Sylow 三子群。

$D_{12}$ 的旋转部分 $C_6$ 提供一个二阶、两个三阶、两个六阶元，六个反射再提供六个二阶元。阶四子群从全部子群表中有三个，三阶子群唯一，故 Sylow 数为三与一。

$T$ 的偶坐标部分为 $C_6$，提供与前述相同的旋转元素数；六个奇坐标元素全为四阶。三个四阶循环子群正是 Sylow 二子群；$\langle a\rangle$ 是唯一 Sylow 三子群。所有元素都已落在这两个坐标部分内，故表中没有未计入的元素。 □

## 6.14 立方阶模型的全部子群与扩张的两种核

**命题 6.39** (两种模型的全部子群)**.** *设 $p$ 为奇素数，$U = U_3(\mathbb{F}_p)$，$M = M_p$。两者都有 $p+1$ 个阶 $p^2$ 子群，且任意两个不同的阶 $p^2$ 子群交于中心。更精确地：*

1. *$U$ 的全部阶 $p^2$ 子群都同构于 $C_p^2$；阶 $p$ 子群有 $p^2+p+1$ 个，子群总数为 $p^2+2p+4$。*
2. *$M$ 的阶 $p^2$ 子群中，一个是 $C_p^2$，其余 $p$ 个是 $C_{p^2}$；阶 $p$ 子群有 $p+1$ 个，子群总数为 $2p+4$。*
3. *两者的正规子群数均为 $p+4$。非中心阶 $p$ 子群的正规化子阶为 $p^2$，每个这样的子群有 $p$ 个共轭子群。*

*证明.* 由命题 6.33，阶 $p^2$ 子群正是中心商 $V$ 中直线的原像，已有 $p+1$ 个。不同直线只交于零向量，取原像便得两个不同极大子群的交恰为 $Z(G)$。

先在 $U$ 中使用 $x = X, y = Y, z = [X,Y]$。全部直线可以无重复地写成

$$L_t = \mathbb{F}_p(1,t) \quad (t \in \mathbb{F}_p), \qquad L_\infty = \mathbb{F}_p(0,1).$$

对应的阶 $p^2$ 子群为

$$H_t = \langle xy^t, z\rangle, \qquad H_\infty = \langle y, z\rangle.$$

每个 $H$ 阶为 $p^2$，故交换；它的非单位元在 $U$ 中都为 $p$ 阶，故 $H \cong C_p^2$。全群有 $p^3-1$ 个非单位元，每个阶 $p$ 子群含 $p-1$ 个；两个不同的阶 $p$ 子群交平凡，因为它们的交阶只能为 1 或 $p$。因此这类子群数为

$$\frac{p^3-1}{p-1} = p^2+p+1.$$

若要逐个写出，可取中心 $\langle z\rangle$，以及

$$\langle xy^t z^c\rangle \quad (t,c\in\mathbb{F}_p), \qquad \langle yz^c\rangle \quad (c\in\mathbb{F}_p).$$

固定直线后，若两个所列生成元生成同一子群，存在 $1\le k<p$ 使其中一个为另一个的 $k$ 次幂；投到 $V$ 后，规范化的首个非零坐标都是一，故 $k=1$，再消去共同因子得 $c$ 相同。不同直线的子群在 $V$ 中像不同。所列数为 $1+p^2+p$，所以没有重复也没有遗漏。

再在 $M$ 中使用 $a,b$ 坐标。已知

$$(a^i b^j)^p = a^{ip}.$$

因而阶整除 $p$ 的元素恰组成

$$\Omega = \langle a^p, b\rangle.$$

这里 $ba^pb^{-1} = a^{p(1+p)} = a^p$，两个生成元均为 $p$ 阶，且由唯一坐标可见交平凡，故 $\Omega\cong C_p^2$。每个阶 $p$ 子群必须包含于 $\Omega$，它们恰为

$$\langle a^p\rangle, \qquad \langle ba^{pc}\rangle \quad (c\in\mathbb{F}_p),$$

共 $p+1$ 个。

$M$ 的中心为 $\langle a^p\rangle$，在商中采用 $aZ, bZ$ 为基。与 $\mathbb{F}_p(bZ)$ 对应的极大子群为 $\Omega$。其余直线为 $\mathbb{F}_p(aZ+tbZ)$，$t\in\mathbb{F}_p$。元素 $ab^t$ 投到相应直线，并满足 $(ab^t)^p = a^p \neq 1$，所以阶为 $p^2$。因此这些极大子群为

$$\langle ab^t\rangle \cong C_{p^2} \quad (t\in\mathbb{F}_p).$$

这恰给出其余 $p$ 个极大子群。Lagrange 定理限定子群阶为 $1, p, p^2, p^3$，所以分别把各阶计数相加，就得到命题中的两个总数。

正规子群的列表已由命题 6.33 给出，数量为 $1+1+(p+1)+1 = p+4$。设 $K=\langle g\rangle$ 为非中心阶 $p$ 子群。共轭给出

$$N_G(K) \longrightarrow \mathrm{Aut}(K), \qquad \ker = C_G(K).$$

像阶既整除 $|N_G(K)|$ 这个 $p$ 的幂，又整除 $p-1$，只能为一。因此 $N_G(K) = C_G(K) = C_G(g)$。推论 6.32 中已求得这个中心化子阶为 $p^2$，所以 $K$ 的共轭轨道大小为 $[G:N_G(K)] = p$。 □

**命题 6.40** (同一模型的不同扩张问题)**.** 设 $G$ 为两个非交换 $p^3$ 阶模型中的任一个。中心扩张

$$1 \longrightarrow Z(G) \longrightarrow G \longrightarrow C_p^2 \longrightarrow 1$$

均不分裂。但 $U$ 与 $M$ 都有别的分裂扩张表示：

$$U \cong C_p^2 \rtimes C_p, \qquad M \cong C_{p^2} \rtimes C_p.$$

不能仅凭中间群的名称判断一个扩张分裂；必须同时指定核与商映射。

证明. 若中心扩张有补子群 $H$,则 $H\cong C_p^2$,$G=Z(G)H$,$Z(G)\cap H=1$。对任意 $z_1h_1,z_2h_2\in G$,中心性与 $H$ 的交换性给出

$$(z_1h_1)(z_2h_2)=z_1z_2h_1h_2=z_2z_1h_2h_1=(z_2h_2)(z_1h_1).$$

于是 $G$ 交换，与模型的非交换性矛盾。因此两个中心扩张都不分裂。

在 $U$ 中置 $A=\langle X,Z\rangle$、$B=\langle Y\rangle$。$A\cong C_p^2$；由 $XY=ZYX$ 得

$$YXY^{-1}=Z^{-1}X,\qquad YZY^{-1}=Z.$$

所以 $Y$ 正规化 $A$，而 $X,Z$ 本已属于 $A$，故 $A\trianglelefteq U$。唯一坐标说明 $A\cap B=1$，且 $AB=U$。这给出第一个内部半直积；作用在基 $X,Z$ 下为

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

$M$ 的循环核 $\langle a\rangle$ 与补子群 $\langle b\rangle$ 已在构造时给出。它们相交平凡、阶乘积为 $p^3$、核正规，给出第二个内部半直积。两个结论使用的核阶均为 $p^2$，不是前面的阶 $p$ 中心。 □

**命题 6.41** (由交换与幂约束计算自同构的数量)**.** 对奇素数 $p$,

$$|\operatorname{Aut}(U_3(\mathbb{F}_p))|=p^2(p^2-1)(p^2-p),\qquad |\operatorname{Aut}(M_p)|=p^3(p-1).$$

证明. 先在 $U$ 中使用 $x,y,z=[x,y]$ 的唯一坐标。自同构在 $U/Z(U)$ 上诱导可逆矩阵

$$A=\begin{pmatrix}i&k\\j&\ell\end{pmatrix}.$$

$x,y$ 的像分别必为 $x^iy^jz^c,x^ky^\ell z^d$。交换子公式要求 $z$ 的像为 $z^{i\ell-jk}$。反过来，给任意可逆 $A$ 与 $c,d\in\mathbb{F}_p$，以上像满足三个生成元的 $p$ 次幂为一、$z$ 中央以及 $xy=zyx$ 的关系。

为说明这确实给出同态，把任意两个规范表达式相乘时，只须依次使用 $yx=z^{-1}xy$ 把所有 $x$ 移到左边，把 $z$ 移到右边，再把三指数模 $p$ 约化。这些操作在像中均合法，因此将规范表达式逐个代入像保持乘法。像在中心商上生成二维空间，$z$ 的像又生成中心，故像为全群；有限性使该同态为自同构。一个可逆矩阵的第一列可取任意非零向量，共 $p^2-1$ 种；第二列不能在第一列张成的直线上，共 $p^2-p$ 种；$c,d$ 各有 $p$ 种。因此得到第一个计数。

在 $M$ 中直接求 $a,b$ 的像。$a$ 阶为 $p^2$，故必有

$$a\longmapsto A=a^ib^j,\quad p\nmid i;\qquad b\longmapsto B=a^{pk}b^\ell,$$

其中 $i\in\mathbb{Z}/p^2\mathbb{Z}$，$j,k,\ell\in\mathbb{F}_p$。$b$ 的像必须为阶 $p$，其形式来自 $\Omega$ 的计算。由 $[b,a]=a^p$，像必须满足 $[B,A]=A^p$。中央交换子公式给出

$$[B,A]=a^{pi\ell},\qquad A^p=a^{pi},$$

因此 $pi(\ell-1)=0$（模 $p^2$），又 $i$ 模 $p$ 非零，故 $\ell=1$。

反过来，任取 $p\nmid i$ 与 $j,k\in\mathbb{F}_p$，上述 $A,B=a^{pk}b$ 满足

$$A^{p^2}=1,\quad B^p=1,\quad BAB^{-1}=A^{1+p}.$$

利用 $BA = A^{1+p}B$ 收集坐标可知 $a^r b^s \mapsto A^r B^s$ 为同态：乘积中的 $B^s A^t$ 被改写为 $A^{(1+p)^s t} B^s$，与式 (6.5) 完全相同。中心商上的矩阵为

$$\begin{pmatrix} \bar{i} & 0 \\ j & 1 \end{pmatrix},$$

行列式 $\bar{i} \neq 0$；而 $A^p = a^{ip}$ 生成中心。因此像包含中心并满射到中心商，进而等于全群。这给出自同构。$i$ 有 $p^2 - p$ 种，$j, k$ 各 $p$ 种，共 $(p^2 - p)p^2 = p^3(p-1)$ 种。 □

**引理 6.42** (交换核半直积的同构判据)**.** *设 $A, B$ 为交换群，$\theta : H \to \mathrm{Aut}(A)$、$\eta : K \to \mathrm{Aut}(B)$ 为作用。若同构*

$$f : A \rtimes_\theta H \longrightarrow B \rtimes_\eta K$$

*把指定核 $A \times \{e\}$ 送到 $B \times \{e\}$，则它在核与商上诱导同构 $\beta : A \to B$、$\gamma : H \to K$，且*

$$\beta\theta(h)\beta^{-1} = \eta(\gamma(h)) \qquad (h \in H).$$

*反过来，存在满足该式的 $\beta, \gamma$ 时，两个半直积同构。*

*证明.* 限制 $f$ 到核得到 $\beta$；对核取商得到 $\gamma$。将 $f(e,h)$ 唯一写成 $(c_h, \gamma(h))$。在目标群中共轭 $(b, e)$，由半直积乘法得到

$$(c_h, \gamma(h))(b, e)(c_h, \gamma(h))^{-1} = \big(c_h \eta(\gamma(h))(b) c_h^{-1}, e\big) = \big(\eta(\gamma(h))(b), e\big).$$

最后一步使用 $B$ 交换，所以核内的 $c_h$ 不影响作用。另一方面，在源群先共轭 $(a, e)$ 再施 $f$，结果为 $(\beta(\theta(h)(a)), e)$。同态保持共轭，令 $b = \beta(a)$ 比较便得所列等式。

反向定义 $F(a, h) = (\beta(a), \gamma(h))$。它是两个双射的乘积，故双射；且

$$\begin{aligned} F\big((a,h)(a',h')\big) &= \big(\beta(a)\beta(\theta(h)(a')), \gamma(h)\gamma(h')\big) \\ &= \big(\beta(a)\eta(\gamma(h))(\beta(a')), \gamma(h)\gamma(h')\big) \\ &= F(a,h)F(a',h'). \end{aligned}$$

因此 $F$ 为群同构。后续分类中，指定核通常是唯一 Sylow 子群，同构必然保持它；循环补群的生成元更换与向量核的换基，正分别对应 $\gamma$ 与 $\beta$。 □

## 6.15 阶 $2p^2$：二阶作用的特征空间

**定理 6.43.** *若 $p$ 为奇素数，则阶为 $2p^2$ 的群恰有五个同构类型：*

$$C_{2p^2}, \quad C_p^2 \times C_2, \quad D_{2p^2}, \quad D_{2p} \times C_p, \quad \mathrm{Dih}(C_p^2).$$

*最后一个模型为 $C_p^2 \rtimes C_2$，其中非单位二阶元对整个 $C_p^2$ 取逆。*

*证明.* Sylow 数 $n_p$ 满足 $n_p \mid 2$、$n_p \equiv 1 \pmod p$，因 $p \geq 3$，只能为一。故 Sylow $p$ 子群 $P$ 正规，阶为 $p^2$，已知交换。取 Sylow 二子群 $\langle b \rangle$，$b^2 = 1$。两因子交平凡，乘积阶为全群，所以

$$G = P \rtimes \langle b \rangle.$$

作用 $\alpha$ 满足 $\alpha^2 = I$。

若 $P=\langle a\rangle\cong C_{p^2}$，写 $\alpha(a)=a^u$。条件为 $u^2=1$（模 $p^2$）。$p$ 是奇数，所以 $p$ 不可能同时整除 $u-1,u+1$，否则会整除差二；而 $p^2\mid(u-1)(u+1)$，故 $p^2$ 必完全整除其中一个因子。因此 $u=1$ 或 $-1$。前者是循环直积 $C_{p^2}\times C_2\cong C_{2p^2}$，后者是二面体模型 $D_{2p^2}$。

若 $P\cong\mathbb{F}_p^2$，二在 $\mathbb{F}_p$ 中可逆。对任一向量 $v$ 定义

$$v_+=\frac{v+\alpha(v)}{2},\qquad v_-=\frac{v-\alpha(v)}{2}.$$

利用 $\alpha^2=I$ 逐项代入得 $\alpha(v_+)=v_+$、$\alpha(v_-)=-v_-$，且 $v=v_++v_-$。两特征空间的交为零：若 $w=\alpha(w)=-w$，则 $2w=0$，从而 $w=0$。所以

$$P=P_+\oplus P_-,\qquad \alpha|_{P_+}=I,\quad \alpha|_{P_-}=-I.$$

负特征空间维数只能为 $0,1,2$。选取各空间的基后，分别得到平凡作用、一个方向取逆、两个方向均取逆。对应模型正为 $C_p^2\times C_2, D_{2p}\times C_p, \mathrm{Dih}(C_p^2)$。更换基就是核的自同构，所以同一维数组合不会产生新的抽象同构类型。所有模型均由外部半直积存在。

最后区分五者。两个交换模型由是否存在阶 $p^2$ 元区分；三个非交换模型中，$D_{2p^2}$ 含阶 $p^2$ 元，而另外两个的奇阶元都在指数为 $p$ 的 $P$ 内，因此没有阶 $p^2$ 元。其余两者的二阶元个数不同：在向量坐标下，

$$(v,b)^2=(v+\alpha(v),1)=(2v_+,1).$$

故二阶元恰对应 $v_+=0$，数量为 $p^{\dim P_-}$，分别是 $p,p^2$。这完成去重。 □

**例 6.44** (十八阶五种模型)**.** 取 $p=3$，得到

$$C_{18},\quad C_3^2\times C_2,\quad D_{18},\quad S_3\times C_3,\quad \mathrm{Dih}(C_3^2).$$

最后两个模型的二阶元分别有三与九个；$D_{18}$ 则含九阶旋转。因此同阶、同样可解都不足以把它们认作同一个群。

## 6.16 阶 $4p$：同一作用像的生成元更换

**定理 6.45.** *设 $p\geq 5$ 为素数。若 $p\equiv 3\pmod 4$，阶 $4p$ 群恰有四种：*

$$C_{4p},\quad C_{2p}\times C_2,\quad D_{2p}\times C_2,\quad T_p.$$

*其中 $T_p=C_p\rtimes C_4$，四阶生成元对 $C_p$ 取逆。若 $p\equiv 1\pmod 4$，还多一个忠实作用模型*

$$\mathcal{F}_p=C_p\rtimes C_4,\qquad bab^{-1}=a^u,\quad |u|=4\ \text{于}\mathbb{F}_p^\times.$$

*这里符号 $\mathcal{F}_p$ 仅为该群名，域始终用 $\mathbb{F}_p$ 表示。*

*证明.* Sylow 数 $n_p\mid 4$ 且 $n_p\equiv 1\pmod p$。因 $p\geq 5$，$1,2,4$ 中只有一满足条件，所以 $P\cong C_p$ 正规。取 Sylow 二子群 $H$，$|H|=4$，与 $P$ 交平凡，乘积为全群。因此 $G=P\rtimes H$，$H=C_4$ 或 $V_4$。

自同构群 $\mathrm{Aut}(P)\cong\mathbb{F}_p^\times$ 循环，阶为 $p-1$。若 $H=\langle b\rangle=C_4$，作用由满足 $u^4=1$ 的参数确定。$u$ 的阶只能是 $1,2,4$，分别给平凡作用、取逆作用与忠实作用。阶四参数存在恰在

$4 \mid p-1$ 时成立：循环群中唯一阶四子群的两个生成元互为逆元。如果两个参数为 $u, v$ 且阶同为四，存在奇数 $r \in \{1,3\}$ 使 $v^r = u$。坐标映射

$$(i,j) \longmapsto (i, rj)$$

从 $u$ 模型到 $v$ 模型双射且保持乘法，因为 $v^{rj} = u^j$。所以忠实作用只有一个同构类型。阶二参数唯一为 $-1$，所以得到 $T_p$；平凡作用给出循环群 $C_{4p}$。

若 $H = V_4$，其像是循环群中指数至多二的子群，只能平凡或为 $\{1, -1\}$。平凡作用给出 $C_{2p} \times C_2$。非平凡时核为阶二子群，选取核的生成元 $c$ 及核外元素 $b$，则 $b$ 取逆、$c$ 平凡作用，故

$$C_p \rtimes (\langle b\rangle \times \langle c\rangle) \cong (C_p \rtimes \langle b\rangle) \times \langle c\rangle \cong D_{2p} \times C_2.$$

该同构在唯一坐标 $a^i b^j c^k$ 上保持乘法，因此不是单靠生成关系猜得的分解。选择不同的非平凡作用核，只相当于更换 $V_4$ 的基，不再产生新群。

两个交换模型分别有和没有阶 $4p$ 元。$D_{2p} \times C_2$ 没有四阶元，因为两分量阶的最小公倍数只能为 $1, 2, p, 2p$；$T_p, \mathcal{F}_p$ 都含四阶的 $b$。$T_p$ 的中心恰为 $\langle b^2\rangle$：与 $a$ 交换要求 $b$ 指数为偶数，与 $b$ 交换要求 $a$ 指数为零。$\mathcal{F}_p$ 与 $a$ 交换要求 $b$ 指数为零，再与 $b$ 交换要求 $a$ 指数为零，所以中心平凡。因此所有模型彼此不同构。 □

**例 6.46** (二十阶与二十八阶)**.** $p = 5$ 时有五种二十阶群：

$$C_{20}, \quad C_{10} \times C_2, \quad D_{10} \times C_2, \quad T_5, \quad \mathcal{F}_5.$$

在忠实模型中可以取 $u = 2$（模五），因为 $2^2 = -1$、$2^4 = 1$。$p = 7$ 时 $4 \nmid 6$，所以二十八阶只有前四种对应模型。$p = 3$ 不能代入本定理的 Sylow 正规性论证：此时 $n_3 = 4$ 也符合条件，正是十二阶分类中额外的 $A_4$ 分支。

## 6.17 阶三倍素数平方的分类

**定理 6.47.** *若 $p \geq 5$ 为素数，则阶 $3p^2$ 群有如下完整列表。*

1. *若 $p \equiv 2 \pmod 3$，共有三种：$C_{3p^2}$、$C_p^2 \times C_3$，以及 $C_p^2 \rtimes C_3$，后者的三阶作用为*

$$J_3 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

2. *若 $p \equiv 1 \pmod 3$，取 $\zeta \in \mathbb{F}_p^\times$ 阶为三。共有六种：循环核 $C_{p^2}$ 的平凡与非平凡三阶作用各一种；核 $C_p^2$ 上的作用可取*

$$I, \quad \mathrm{diag}(1, \zeta), \quad \zeta I, \quad \mathrm{diag}(\zeta, \zeta^{-1}),$$

*各一种。所有商与补群均为 $C_3$。*

*$p = 3$ 的阶二十七已由立方阶定理分类；$p = 2$ 的阶十二包含 $A_4$ 的例外，不能套用本定理。*

*证明.* $n_p \mid 3$、$n_p \equiv 1 \pmod p$，$p \geq 5$ 时只能 $n_p = 1$。取三阶 Sylow 补群便得 $G = P \rtimes C_3$，$P = C_{p^2}$ 或 $C_p^2$。

循环核的自同构对应模 $p^2$ 单位。三阶自同构存在恰在 $3 \mid p-1$：模 $p$ 化简的核由 $1+cp$ 组成，这个核阶为 $p$，所以三阶元素模 $p$ 仍为三阶。反过来，若 $u_0 \in \mathbb{F}_p^\times$ 阶三，取任一整数提升 $u$，令 $u^3 = 1 + kp$（模 $p^2$）；改成 $u + tp$ 后，其立方为

$$u^3 + 3u^2 tp \pmod{p^2}.$$

因 $3u^2$ 模 $p$ 可逆，唯一 $t$ 使 $k + 3u^2 t = 0$（模 $p$），故存在且唯一三次单位根提升。三个三次单位根中非平凡的两个互为逆，更换 $C_3$ 生成元使二者给出同构模型。因此循环核贡献一类或两类。

在 $P = \mathbb{F}_p^2$ 上，三阶作用 $T$ 满足 $T^3 = I$，且 $p \neq 3$。若 $p \equiv 1 \pmod 3$，多项式分解为三个不同线性因子

$$X^3 - 1 = (X-1)(X-\zeta)(X-\zeta^{-1}).$$

这里可用显式投影证明可对角化：对三个根 $\lambda$ 定义

$$\Pi_\lambda = \prod_{\mu \neq \lambda} \frac{T - \mu I}{\lambda - \mu}.$$

把 $\Pi_\lambda$ 对应的二次多项式记为

$$q_\lambda(X) = \prod_{\mu \neq \lambda} \frac{X - \mu}{\lambda - \mu}.$$

对任一根 $\nu \in \{1, \zeta, \zeta^{-1}\}$，逐项代入得 $q_\lambda(\nu) = 1$（$\nu = \lambda$）或 $0$（$\nu \neq \lambda$）。因此二次以下多项式 $\sum_\lambda q_\lambda(X) - 1$ 有三个不同的根，只能恒为零：若非零，依次除以三个不同的一次因子会使次数至少为三。代入 $T$ 得 $\sum_\lambda \Pi_\lambda = I$。又 $(T - \lambda I)\Pi_\lambda = 0$，因为其分子为 $T^3 - I$。故每个向量 $v$ 都是三个特征向量 $\Pi_\lambda v$ 之和。为证明这是直和，设 $\sum_\lambda v_\lambda = 0$，其中 $T v_\lambda = \lambda v_\lambda$。对任一固定的根 $\nu$ 作用 $\Pi_\nu$，有

$$0 = \sum_\lambda q_\nu(T) v_\lambda = \sum_\lambda q_\nu(\lambda) v_\lambda = v_\nu.$$

对三个 $\nu$ 分别使用该式，所有分量均为零。于是得到所需的特征空间直和。二维特征值无序对在交换两根及同时取逆下，恰有

$$(1,1), \quad (1,\zeta), \quad (\zeta,\zeta), \quad (\zeta,\zeta^{-1})$$

四种，给出定理所列矩阵。

若 $p \equiv 2 \pmod 3$，$X^2 + X + 1$ 没有根，否则一个非单位三次根会使 $3 \mid p-1$。两个互素因子 $X - 1$ 与 $X^2 + X + 1$ 给出

$$P = \ker(T - I) \oplus \ker(T^2 + T + I).$$

可由投影 $(I + T + T^2)/3$ 验证第一分量，剩余投影给第二分量。第二空间若非零不可能一维，因其上没有一维特征值，故为全部二维空间。任取 $v \neq 0$，则 $v, Tv$ 独立，在此基下 $T^2 v = -v - Tv$，矩阵即 $J_3$。因此只有 $I$ 与 $J_3$ 两类。$J_3^{-1}$ 与 $J_3$ 也相似：$v, T^{-1}v$ 是另一组同类基，故更换补群生成元不增加类型。

两种核类型由唯一 Sylow $p$ 子群区分。可分裂特征值情形的四种作用中，$I$ 的像平凡；$\mathrm{diag}(1,\zeta)$ 的固定空间一维；另外两种固定空间为零，但其中一个为标量变换、另一个有两个不同特征值。标量性与特征值重复次数在共轭和生成元取逆下不变，故四者不同构。不可分裂情形则由作用是否平凡区分。模型均由半直积构造存在，分类完成。 □

## 6.18 六倍素数阶：平均二余循环与分裂

**引理 6.48** (素数阶核与互素阶商的显式分裂)**.** *若 $N \trianglelefteq G$ 为 $p$ 阶循环群，$p \nmid |G/N| = m$，则精确列 $1 \to N \to G \to G/N \to 1$ 分裂。*

*证明.* 把 $N$ 识别为 $\mathbb{F}_p$ 加法群。核交换，故商 $Q = G/N$ 对核的共轭作用良定义：两个提升相差一个核元素，它在交换核上的共轭恒等。取单位处归一的集合截面，第四章的扩张坐标给出乘法

$$(a, q)(b, r) = (a + q \cdot b + f(q, r), qr),$$

其中 $f$ 归一且满足

$$f(q, r) + f(qr, s) = q \cdot f(r, s) + f(q, rs).$$

置 $S(q) = \sum_{s \in Q} f(q, s)$。固定 $q, r$ 并对 $s$ 求和，因为 $s \mapsto rs$ 为 $Q$ 的置换，得到

$$mf(q, r) + S(qr) = q \cdot S(r) + S(q).$$

$m$ 在 $\mathbb{F}_p$ 中可逆，故令 $t(q) = m^{-1} S(q)$，便有

$$f(q, r) = t(q) + q \cdot t(r) - t(qr).$$

又 $t(1) = 0$。把截面 $s(q)$ 改成 $(-t(q))s(q)$，其新二余循环为

$$f(q, r) - t(q) - q \cdot t(r) + t(qr) = 0.$$

所以新截面保持乘法、在商投影下为恒等，给出补子群。这是具体的截面计算，不需另引一般 Schur–Zassenhaus 定理。 □

**定理 6.49.** *设 $p \geq 5$ 为素数。阶 $6p$ 群都含正规 Sylow $p$ 子群，且为 $C_p \rtimes H$，$H = C_6$ 或 $S_3$。*

1. *$H = C_6$ 时，作用像阶 $d$ 可且只可取 $d \mid \gcd(6, p-1)$，每个 $d$ 给一个同构类型。*
2. *$H = S_3$ 时，作用平凡或通过符号商 $S_3/A_3 \cong C_2$ 取逆，共两类。*

*因此 $p \equiv 5 \pmod 6$ 时共四类，$p \equiv 1 \pmod 6$ 时共六类。*

*证明.* $p \geq 7$ 时 $n_p \mid 6$ 且 $n_p \equiv 1 \pmod p$，所以 $n_p = 1$；$p = 5$ 时后文定理 6.57 将独立证明存在正规十五阶循环子群，其五阶子群唯一而特征，故也正规于 $G$。引理 6.48 在 $m = 6$ 时适用，得到 $G = C_p \rtimes H$。商 $H$ 阶六，由 $pq$ 定理只有 $C_6, S_3$。

目标 $\mathrm{Aut}(C_p) = \mathbb{F}_p^\times$ 循环。对 $C_6$，生成元的像阶必须整除六与 $p-1$，每个允许阶 $d$ 的像子群在循环目标中唯一。$d = 1, 2$ 时生成元唯一；$d = 3, 6$ 时两个生成元互为逆，取 $C_6$ 生成元的逆便把二者互换。因此每个 $d$ 恰一个类型。

对 $S_3$，交换目标使作用消去 $S_3' = A_3$，故通过阶二交换化；只有平凡与取逆两种。同构保持唯一的 Sylow $p$ 核，并诱导商的同构。商 $C_6$ 与 $S_3$ 不同构，故两组不混同；第一组的作用像阶 $d$ 可由 $[G : C_G(C_p)]$ 恢复，第二组的平凡与非平凡作用也由该指数区分。所以列表无重复。

$p > 3$ 只能模六余一或五。余五时 $\gcd(6, p-1) = 2$，允许 $d = 1, 2$；余一时公因子为六，允许 $d = 1, 2, 3, 6$。各再加 $S_3$ 商的两类，即得四或六。 □

## 6.19 四次幂阶的入口：交换正规子群与进位坐标

**引理 6.50** (四次幂阶必有交换的指数 $p$ 子群)**.** *对任意素数 $p$，每个阶为 $p^4$ 的群都含有阶为 $p^3$ 的交换正规子群。*

*证明.* 若 $G$ 交换，只须找阶 $p^3$ 子群。更一般地，每个阶为 $p^n$ 的群都有每种阶 $p^k$ 的子群：对 $n$ 归纳，中心含有阶 $p$ 子群 $C$；在 $G/C$ 中取阶 $p^{k-1}$ 子群再取原像，便得阶 $p^k$ 子群。$k=0$ 时取平凡子群；中心中阶 $p$ 元由中心非平凡及 Cauchy 定理保证。因此交换情形已得结论。

以下 $G$ 非交换。中心阶不能是 $p^3$，否则中心商循环导致 $G$ 交换；也不能是 $p^4$，所以中心阶只可能是 $p$ 或 $p^2$。

若 $|Z(G)|=p^2$，商 $G/Z(G)$ 阶为 $p^2$，其中取一个阶 $p$ 子群 $\langle xZ(G)\rangle$。它的原像 $\langle Z(G),x\rangle$ 阶为 $p^3$。此群交换，因为元素均为 $zx^i$，中心因子和 $x$ 的幂彼此交换。

若 $|Z(G)|=p$，每个非中心 $x$ 的中心化子都包含 $\langle Z(G),x\rangle$，后者至少有 $p^2$ 个元素。因此 $|C_G(x)|$ 为 $p^2$ 或 $p^3$；不可能为 $p^4$，否则 $x$ 中央。假如所有非中心元素的中心化子都为 $p^2$ 阶，它们的共轭类便都为 $p^2$ 大小。然而非中心元素总数为

$$p^4-p=p(p^3-1),$$

不被 $p^2$ 整除，不可能分割成大小全为 $p^2$ 的类。故有某个 $x$ 的中心化子 $C$ 阶为 $p^3$。$Z(G)$ 与 $x$ 都属于 $Z(C)$，所以 $|Z(C)|\ge p^2$。若恰为 $p^2$，则 $C/Z(C)$ 为阶 $p$ 的循环群，中心商判别使 $C$ 交换，于是中心其实为全 $C$；若中心已经为 $p^3$，同样交换。因此 $C$ 为所求交换子群。

上述子群指数为 $p$，第五章最小素因子指数判据说明它正规。该判据在这里的假设满足，因为 $|G|$ 的唯一素因子为 $p$。 □

**命题 6.51** (交换核、循环素数阶商的完整坐标)**.** *设 $A$ 为交换群，用加法记号。设 $\alpha\in\mathrm{Aut}(A)$ 满足 $\alpha^p=\mathrm{id}$，$t\in A$ 满足 $\alpha(t)=t$。在 $A\times\{0,\dots,p-1\}$ 上定义*

$$(a,i)(b,j)=\left(a+\alpha^i(b)+\left\lfloor\frac{i+j}{p}\right\rfloor t,\ i+j \bmod p\right).$$

*它给出一个群 $E(A,\alpha,t)$，其中 $A\trianglelefteq E$、$E/A\cong C_p$。反过来，每个具有交换正规子群 $A$、商为 $C_p$ 的群都由此构造得到。*

*证明.* 置 $c(i,j)=\lfloor (i+j)/p\rfloor$。因为指标均在 $0,\dots,p-1$ 中，$c$ 为零或一。对三指标 $i,j,k$，有整数恒等式

$$c(i,j)+c(i+j \bmod p,k)=c(j,k)+c(i,j+k \bmod p)=\left\lfloor\frac{i+j+k}{p}\right\rfloor.$$

把 $i+j=pc(i,j)+(i+j \bmod p)$ 代入即得第一个等号的共同值；把 $j+k$ 分拆得到另一边。又 $\alpha^p=\mathrm{id}$、$\alpha(t)=t$，所以两种三重乘法的第一坐标分别归结为

$$a+\alpha^i(b)+\alpha^{i+j}(d)+\left\lfloor\frac{i+j+k}{p}\right\rfloor t.$$

第二坐标均为 $i+j+k \bmod p$，故结合律成立。单位为 $(0,0)$；$i=0$ 时逆元为 $(-a,0)$，$i>0$ 时逆元为

$$\big(-\alpha^{-i}(a+t),p-i\big).$$

把这两个表达式从左、右分别乘回，第一坐标都为零、第二坐标也为零，所以群公理全部成立。

置 $x=(0,1)$，则 $x^p=(t,0)$，且 $x(a,0)x^{-1}=(\alpha(a),0)$。第二坐标投影为到 $C_p$ 的满同态，核为 $A\times\{0\}$，故核正规且商为 $C_p$。

反过来，在给定群中取 $xA$ 生成 $G/A$。每个元素唯一为 $ax^i$，$0\le i<p$。令 $\alpha(a)=xax^{-1}$、$t=x^p\in A$。因 $A$ 交换，$\alpha^p$ 是 $t$ 的内部共轭，故为恒等；而 $x$ 与自己的 $p$ 次幂交换，故 $\alpha(t)=t$。移动 $x^ib=\alpha^i(b)x^i$ 并把 $x^{i+j}$ 约化，得到命题中的乘法。唯一坐标同构引理完成证明。 □

**注 6.52** (更换补元的精确影响)**.** 若保持 $A$ 不变，把 $x$ 改成 $sx$，$s\in A$，则作用仍为 $\alpha$，而

$$t\longmapsto t+N_\alpha(s),\qquad N_\alpha(s)=s+\alpha(s)+\cdots+\alpha^{p-1}(s).$$

这是把 $(sx)^p$ 逐次移动为 $s\alpha(s)\cdots\alpha^{p-1}(s)x^p$ 的结果。若再用 $\beta\in\mathrm{Aut}(A)$ 重新标记核，则

$$(\alpha,t)\longmapsto(\beta\alpha\beta^{-1},\beta(t)).$$

还可以把商生成元改为 $x^kA$，其中 $1\le k<p$。因 $k$ 模 $p$ 可逆，这仍生成 $G/A$；此时作用为 $\alpha^k$，而 $(x^k)^p=(x^p)^k$ 给出新进位 $kt$。两类更换合并为

$$x\longmapsto sx^k:\qquad(\alpha,t)\longmapsto\big(\alpha^k,\,kt+N_{\alpha^k}(s)\big).$$

核交换，故 $s$ 的内部共轭不改变 $\alpha^k$；逐次移动 $x^k$ 穿过 $s$，恰产生 $s,\alpha^k(s),\dots,\alpha^{(p-1)k}(s)$，所以以上进位公式包含了全部因子。下面的十六阶与奇素数四次幂阶分类使用这些变换逐项约化参数；不同交换核也可能产生同构的中间群，最后还须跨核去重。

## 6.20　十六阶群：十四个模型的完整分类

引理 6.50 把分类分成以下三支。箭头表示选择核后的分类步骤，不表示群同态。

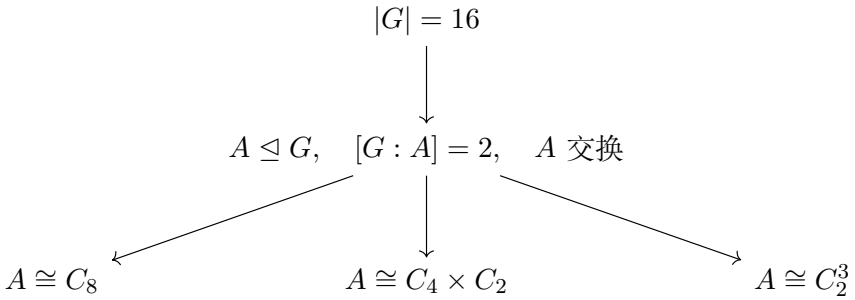



图 6.2: 十六阶分类的三个核分支；最后仍须跨分支去重。

**定理 6.53.** 十六阶群恰有十四个同构类型。五个交换模型为

$$C_{16},\quad C_8\times C_2,\quad C_4^2,\quad C_4\times C_2^2,\quad C_2^4.$$

九个非交换模型可取为

$$D_{16},\quad Q_{16},\quad SD_{16},\quad \mathcal{M}_{16},\quad D_8\times C_2,\quad Q_8\times C_2,\quad K_{16},\quad L_{16},\quad R_{16}.$$

这里后面的模型由以下坐标数据定义，名字只作为这些具体模型的缩写。

对四个具有循环八阶核的模型，取 $A=\mathbb{Z}/8\mathbb{Z}$，$p=2$，$\alpha(i)=ui$，用命题 *6.51* 构造：

| $G$ | $D_{16}$ | $Q_{16}$ | $SD_{16}$ | $\mathcal{M}_{16}$ |
|---|---|---|---|---|
| $u$ | 7 | 7 | 3 | 5 |
| $t$ | 0 | 4 | 0 | 0 |

作用参数 $u$ 用模八整数表示。另外三个新模型取 $A=\langle a\rangle\times\langle b\rangle\cong C_4\times C_2$，使用乘法记号列出作用与 $x^2$：

| $G$ | $\alpha(a)$ | $\alpha(b)$ | $x^2$ |
|---|---|---|---|
| $K_{16}$ | $a$ | $a^2b$ | 1 |
| $L_{16}$ | $a^{-1}$ | $b$ | $b$ |
| $R_{16}$ | $ab$ | $b$ | 1 |

每行的作用平方为恒等，$x^2$ 被作用固定，所以以上均为确有十六个元素的模型。

证明. 引理 6.50 给出八阶交换正规子群 $A$。它由八阶交换群分类只可能是 $C_8, C_4\times C_2, C_2^3$。取 $x\notin A$，记作用为 $\alpha$、$x^2=t$。只须按这三类核穷尽 $\alpha^2=1$、$\alpha(t)=t$ 的数据。

**第一类：** $A=C_8$。取 $A=\langle r\rangle$，$\alpha(r)=r^u$。$u$ 必为奇数，而 $1,3,5,7$ 的平方模八均为一，所以四种作用全部列出。$t$ 记为 $r^v$。固定条件为 $(u-1)v=0$（模八），更换 $x$ 为 $r^sx$ 则

$$v\longmapsto v+(1+u)s\pmod 8.$$

逐项求解得到

| $u$ | 允许的$v$ | $(1+u)\mathbb{Z}/8\mathbb{Z}$ | 可取的代表$v$ |
|---|---|---|---|
| 1 | $\mathbb{Z}/8\mathbb{Z}$ | $\{0,2,4,6\}$ | $0,1$ |
| 3 | $\{0,4\}$ | $\{0,4\}$ | 0 |
| 5 | $\{0,2,4,6\}$ | $\{0,2,4,6\}$ | 0 |
| 7 | $\{0,4\}$ | $\{0\}$ | $0,4$ |

$u=1,v=0$ 是 $C_8\times C_2$。$u=1,v=1$ 时 $x^2=r$，所以 $x$ 阶为十六并生成全群，即 $C_{16}$。其余四行正是定理给出的四个非交换循环核模型。这里每一次约化都是更换同一群的生成元，故没有失去同构类型。

**第二类：** $A=C_2^3$。把 $A$ 视为 $\mathbb{F}_2$ 三维空间。令 $N=\alpha-I$。由特征二及 $\alpha^2=I$，

$$N^2=0,\qquad \operatorname{im}N\subseteq\ker N.$$

秩 $r$ 因而满足 $r\le 3-r$，故 $r=0$ 或一。$r=0$ 时作用平凡；$t=0$ 给出 $C_2^4$，$t\neq 0$ 时取 $e_1=t$ 并扩为基，$x^2=e_1$ 使 $x$ 为四阶，另两基向量给出 $C_4\times C_2^2$。

$r=1$ 时取 $e_1$ 生成 $\operatorname{im}N$，再取 $e_2$ 满足 $Ne_2=e_1$，并取 $e_3\in\ker N$ 补足 $e_1$。于是

$$\alpha(e_1)=e_1,\quad \alpha(e_2)=e_2+e_1,\quad \alpha(e_3)=e_3.$$

$t$ 必在 $\ker N=\langle e_1,e_3\rangle$ 中，而 $N_\alpha=I+\alpha=N$，故更换 $x$ 可以消去 $t$ 的 $e_1$ 分量。只余 $t=0$ 或 $e_3$。

$t=0$ 时 $\langle e_1,e_2,x\rangle$ 有八个唯一坐标 $e_1^ie_2^jx^k$；这里暂把 $e_1,e_2$ 作为群元素使用乘法记号。$x,e_2$ 不交换，$(e_2x)^2=e_1$，且 $x$ 为二阶，故八阶分类给出 $D_8$。$e_3$ 中央，且由唯一坐标不在该子群中，所以全群为 $D_8\times C_2$。

$t=e_3$ 时，令 $a'=x$、$b'=e_1$、$y'=e_2$。由 $xe_2x^{-1}=e_2e_1$ 得

$$(a')^2=e_3,\qquad (b')^2=1,\qquad y'a'(y')^{-1}=b'a',\qquad (y')^2=1.$$

$e_1,e_3$ 中央，且 $e_1$ 独立于 $e_3$，所以 $\langle a',b'\rangle\cong C_4\times C_2$。$y'$ 在这个八阶子群外，故这些数据恰为 $R_{16}$ 的定义。两类非平凡作用已全部归入列表。

**第三类：** $A=C_4\times C_2$。用 $a,b$ 为规范生成元。任意自同构必且只可能写成

$$\alpha(a)=a^ub^v,\qquad \alpha(b)=a^{2w}b,\quad u\in\{1,3\},\quad v,w\in\{0,1\}.$$

理由是：四阶像的 $a$ 指数必须为奇数；$b$ 的像阶整除二，且不能在 $\langle a^2\rangle$ 中，否则像在 $A/\langle a^2\rangle$ 上不满。反过来，这些像在该商上独立，并含有 $a^2$，故生成 $A$。

在坐标 $(i,j)$ 中，上式为

$$\alpha(i,j)=(ui+2wj,vi+j).$$

再作用一次，第一坐标为 $(1+2wv)i$，第二坐标为 $j$。因此 $\alpha^2=I$ 当且仅当 $wv=0$；八个自同构中只有 $(v,w)=(1,1)$ 的两项被排除。

剩下六项中有两对共轭。设 $\alpha_1=(3,0,1)$，$\beta(a)=ab,\beta(b)=b$，则 $\beta^{-1}=\beta$，且

$$\beta\alpha_1\beta^{-1}(a)=\beta(a^{-1}a^2b)=a,\qquad \beta\alpha_1\beta^{-1}(b)=\beta(a^2b)=a^2b.$$

所以它与 $(1,0,1)$ 共轭。设 $\alpha_2=(3,1,0)$，$\gamma(a)=a,\gamma(b)=a^2b$，则 $\gamma^{-1}=\gamma$，且

$$\gamma\alpha_2\gamma^{-1}(a)=\gamma(a^{-1}b)=ab,\qquad \gamma\alpha_2\gamma^{-1}(b)=\gamma(a^2b)=b.$$

所以它与 $(1,1,0)$ 共轭。自同构由 $a,b$ 的像决定，上述两个等式分别验证了整个作用的共轭。因此只须以下四种作用。记 $N_\alpha(A)=\{s\alpha(s):s\in A\}$，此处使用乘法记号；相应的参数约化为

| $(\alpha(a),\alpha(b))$ | $\mathrm{Fix}(\alpha)$ | $N_\alpha(A)$ | $t$ 的代表 |
|---|---|---|---|
| $(a,b)$ | $A$ | $\langle a^2\rangle$ | $1,b,a$ |
| $(a,a^2b)$ | $\langle a\rangle$ | $\langle a^2\rangle$ | $1,a$ |
| $(ab,b)$ | $\langle a^2,b\rangle$ | $\langle a^2b\rangle$ | $1,b$ |
| $(a^{-1},b)$ | $\langle a^2,b\rangle$ | $1$ | $1,b,a^2$ |

下面补出表中除取商之外的两个约化。在第一行，模 $\langle a^2\rangle$ 有 $1,a,b,ab$；核自同构 $a\mapsto ab,b\mapsto b$ 把 $a$ 与 $ab$ 交换，故可留 $1,b,a$。第四行模范数不减少参数，但与作用交换的核自同构 $a\mapsto a,b\mapsto a^2b$ 把 $b$ 与 $a^2b$ 交换，故只留 $1,b,a^2$。第二、三行的固定群模范数群都为二阶，表中已列其两个余类代表。固定群与范数群逐项由

$$\alpha(i,j)=(ui+2wj,vi+j),\quad (i,j)+\alpha(i,j)=((1+u)i+2wj,vi)$$

求出，因此表中未隐藏其他参数。

第一行三个参数 $1,b,a$ 分别给出 $C_4\times C_2^2,C_4^2,C_8\times C_2$：前者 $x$ 独立二阶；中者 $x^2=b$，故 $a,x$ 为独立四阶生成元；后者 $x^2=a$，故 $x$ 为八阶并与独立的 $b$ 交换。

第二行 $t=1$ 是 $K_{16}$。$t=a$ 时，$x$ 阶八，$a=x^2$，且由 $xbx^{-1}=a^2b=x^4b$ 得

$$bxb^{-1}=x^5.$$

所以以 $x$ 为循环核生成元、$b$ 为补元，就是 $\mathcal{M}_{16}$。

第三行 $t=1$ 是 $R_{16}$。$t=b$ 时，$x^2=b$，并有 $xax^{-1}=ab=ax^2$，即 $xa=ax^3$。这给出 $axa^{-1}=x^{-1}$。令新核生成元为 $a'=x, b'=a^2$，新外元为 $y=a$，则

$$|a'|=4,\quad |b'|=2,\quad [a',b']=1,\quad ya'y^{-1}=(a')^{-1},\quad yb'y^{-1}=b',\quad y^2=b'.$$

唯一坐标保证 $\langle a',b'\rangle$ 为八阶，所以这是 $L_{16}$。

第四行 $t=1$ 时 $\langle a,x\rangle\cong D_8$，$b$ 为独立中央二阶元，故为 $D_8\times C_2$；$t=b$ 是 $L_{16}$；$t=a^2$ 时 $\langle a,x\rangle\cong Q_8$，$b$ 仍为独立中央二阶元，故为 $Q_8\times C_2$。至此所有数据都已构造、归入十四个候选模型。

还须证明候选模型互不同构，这由下一命题的不变量表完成；该表的计算只使用上述模型坐标，不再依赖分类结论。因此证明不存在循环论证。 □

**命题 6.54** (十六阶列表的去重证据)**.** 记 $\nu_d(G)=\#\{g\in G:|g|=d\}$，记

$$G^{(2)}=\langle g^2:g\in G\rangle$$

为所有平方生成的子群；这里不是导出群，也不是二阶元的集合。九个非交换模型的不变量为

| $G$ | $Z(G)$ | $\nu_2(G)$ | $\nu_8(G)$ | $G^{(2)}$ |
|---|---|---|---|---|
| $D_{16}$ | $C_2$ | 9 | 4 | $C_4$ |
| $Q_{16}$ | $C_2$ | 1 | 4 | $C_4$ |
| $SD_{16}$ | $C_2$ | 5 | 4 | $C_4$ |
| $\mathcal{M}_{16}$ | $C_4$ | 3 | 8 | $C_4$ |
| $D_8\times C_2$ | $C_2^2$ | 11 | 0 | $C_2$ |
| $Q_8\times C_2$ | $C_2^2$ | 3 | 0 | $C_2$ |
| $K_{16}$ | $C_4$ | 7 | 0 | $C_2$ |
| $L_{16}$ | $C_2^2$ | 3 | 0 | $C_2^2$ |
| $R_{16}$ | $C_2^2$ | 7 | 0 | $C_2^2$ |

九行互不相同，五个交换模型也彼此不同构。

证明. 先计算循环八阶核的四行。元素唯一为 $r^i$ 或 $r^ix$，且

$$(r^ix)^2=r^{(1+u)i+v},\qquad x^2=r^v.$$

旋转部分有一个二阶元 $r^4$、四个八阶元。外陪集元素不可能中央，因为它对 $r$ 的共轭为非恒等的 $r\mapsto r^u$。旋转 $r^i$ 中央恰在 $(u-1)i=0$（模八）时成立；$u=7,3$ 给中心 $\langle r^4\rangle$，$u=5$ 给中心 $\langle r^2\rangle$。

在 $D_{16}$ 外陪集的八个平方全为一，故新增八个二阶元；在 $Q_{16}$ 全为 $r^4$，故外面全为四阶。在 $SD_{16}$ 平方为 $r^{4i}$，四个为一、四个为 $r^4$。在 $\mathcal{M}_{16}$ 平方为 $r^{6i}$：$i=0,4$ 得一，$i=2,6$ 得 $r^4$，四个奇 $i$ 得阶四的旋转，故对应元素阶八。这给出前四行的 $\nu_2,\nu_8$。旋转的平方已生成 $\langle r^2\rangle$，外面的平方也在其中，所以四行的平方生成群均为 $C_4$。

$D_8$ 有包括单位在内六个平方为一的元素，$Q_8$ 有两个；乘上 $C_2$ 后分别有十二个与四个。扣除单位即得十一与三个二阶元。中心为两个因子中心的直积，均为 $C_2^2$；所有元素阶至多四，平方生成群均由第一个因子的唯一非平凡旋转平方生成，为 $C_2$。

后三个模型的核 $A = C_4 \times C_2$ 含三个二阶元，八个元素的平方都在 $\langle a^2\rangle$。因作用非平凡，外陪集无中央元素，中心恰为 $\mathrm{Fix}(\alpha)$，已在分类参数表中求出。外元素的平方分别为

| $G$ | $(a^i b^j x)^2$ |
|---|---|
| $K_{16}$ | $a^{2(i+j)}$ |
| $L_{16}$ | $b$ |
| $R_{16}$ | $a^{2i}b^i$ |

其中 $0 \le i < 4$、$0 \le j < 2$。在 $K$ 行，$i+j$ 偶数给四个单位平方；在 $L$ 行没有单位平方；在 $R$ 行，$i$ 偶数给四个单位平方。因此二阶元数为七、三、七。三个模型平方都阶至多二，所以没有八阶元；平方生成群由 $a^2$ 与外元素的平方生成，分别为 $\langle a^2\rangle, \langle a^2, b\rangle, \langle a^2, b\rangle$。这证明表中全部数据。

交换模型中，$C_{16}$ 含十六阶元，$C_8 \times C_2$ 的最大元素阶为八，另三者的最大元素阶为四、四、二。剩下两个四指数模型 $C_4^2, C_4 \times C_2^2$ 的二阶元数分别为 $2^2 - 1 = 3$ 与 $2^3 - 1 = 7$：一个坐标在 $C_4$ 中平方为一有两种选择，在 $C_2$ 中也有两种。于是五者彼此区分。交换性又把这五者与九个非交换模型区分开来。 □

## 6.21 奇素数四次幂阶：十五种模型与特征三例外

为避免同一个群的不同交换核导致重复，本节把类二与类三模型分开。下文的 $G^p = \langle g^p : g \in G\rangle$ 表示 $p$ 次幂生成的子群。所有坐标模型均使用命题 6.51，其中核 $A$ 用乘法记号，外元为 $x$，$x^p = t$。

**定理 6.55.** *对每个奇素数 $p$，阶 $p^4$ 的群恰有十五个同构类型，其中五个交换、六个幂零类二、四个幂零类三。*

*五个交换模型为*

$$C_{p^4}, \quad C_{p^3} \times C_p, \quad C_{p^2}^2, \quad C_{p^2} \times C_p^2, \quad C_p^4.$$

*六个类二模型为以下表格中的六行，每一行都定义一个群：*

| 记名 | $A$ | $\alpha(a)$ | $\alpha(b)$ | $t$ |
|---|---|---|---|---|
| $\mathcal{C}_p$ | $C_{p^3} = \langle a\rangle$ | $a^{1+p^2}$ | 无 $b$ | 1 |
| $\mathcal{U}_p$ | $U_3(\mathbb{F}_p) \times C_p$ | | | |
| $\mathcal{V}_p$ | $M_p \times C_p$ | | | |
| $\mathcal{K}_p$ | $C_{p^2} \times C_p = \langle a, b\rangle$ | $a$ | $a^p b$ | 1 |
| $\mathcal{E}_p$ | $C_{p^2} \times C_p = \langle a, b\rangle$ | $ab$ | $b$ | 1 |
| $\mathcal{H}_p$ | $C_{p^2} \times C_p = \langle a, b\rangle$ | $a^{1+p}$ | $b$ | $b$ |

*类三模型分为两种核类型。第一种取 $A = C_{p^2} \times C_p = \langle a, b\rangle$，定义*

$$D_p(d, s): \quad \alpha(a) = ab, \quad \alpha(b) = a^{pd}b, \qquad t = a^{ps}.$$

*这里 $d \in \mathbb{F}_p^\times$。若 $p \ge 5$，可且只可取 $(d, s) = (1, 0), (\epsilon, 0)$，$\epsilon$ 为任一非平方元。若 $p = 3$，可且只可取*

$$(d, s) = (1, 0), (2, 0), (2, 1).$$

*第二种取 $A = C_p^3 = \langle u, v, w\rangle$，定义*

$$J_p(e): \quad \alpha(u) = u, \quad \alpha(v) = uv, \quad \alpha(w) = vw, \qquad t = u^e.$$

*$p \ge 5$ 时取 $e = 0, 1$；$p = 3$ 时只取 $e = 0$。所以两种核合计总为四个类三模型。*

证明. 每个群由引理 6.50 有交换指数 $p$ 核，其类型为 $C_{p^3}$、$C_{p^2}\times C_p$、$C_p^3$。以下穷尽相应作用与进位参数；模型的存在均由进位坐标命题保证。

**循环核**。写 $\alpha(a)=a^u$，$\alpha^p=1$。模 $p$ 后 $\bar u^p=1$，而非零域元素满足 $\bar u^p=\bar u$，故 $u=1+pc+p^2d$。二项式展开给出

$$u^p\equiv 1+p^2c \pmod{p^3},$$

所以 $c=0$（模 $p$）。作用平凡时，更换外元使 $t$ 在 $A/A^p$ 中取零或一个非零代表，分别给 $C_{p^3}\times C_p$ 与 $C_{p^4}$。作用非平凡时，换 $x$ 为 $x^k$，$k\not\equiv 0 \pmod p$，可以把 $d$ 归一为一。固定点群为 $\langle a^p\rangle$，而范数为

$$N_\alpha(a^i)=a^{i\sum_{j=0}^{p-1}(1+p^2)^j}=a^{pi},$$

这里逐项展开为

$$\sum_{j=0}^{p-1}(1+p^2)^j\equiv\sum_{j=0}^{p-1}(1+jp^2)=p+p^2\frac{p(p-1)}{2}\equiv p \pmod{p^3}.$$

因为 $p$ 为奇素数，$(p-1)/2$ 为整数，最后一项被 $p^3$ 整除。于是范数像恰为 $\langle a^p\rangle$，等于固定点群；每个固定 $t=a^{pq}$ 都可把外元改成 $a^{-q}x$ 而消去，只得到 $\mathcal{C}_p$。

**混合核**。取 $A=C_{p^2}\times C_p$，用加法坐标 $(i,j)$，第一坐标模 $p^2$。任意自同构可写为

$$\beta(i,j)=(ri+phj,\ell i+zj),\quad r\in(\mathbb{Z}/p^2\mathbb{Z})^\times,\ z\in\mathbb{F}_p^\times,\quad h,\ell\in\mathbb{F}_p.$$

理由是阶整除 $p$ 的 $b$ 像第一坐标必须被 $p$ 整除；在 $A/pA$ 上可逆要求 $\bar r,z$ 非零。反过来，这些条件使两个像在该商上生成，并且 $\beta(a)^p=a^{pr}$ 生成 $pA$，所以整个像为 $A$。

若 $\alpha^p=I$，模 $p$ 的三角矩阵的两个对角元都满足 $\lambda^p=1$，故都为一。因此必有

$$\alpha(i,j)=((1+pc)i+pwj,vi+j),\qquad c,v,w\in\mathbb{F}_p.$$

置 $N=\alpha-I$，则逐次代入得到

$$N(i,j)=(pci+pwj,vi),\quad N^2(i,j)=(pwvi,0),\quad N^3=0.$$

反过来，每组 $(c,v,w)$ 都给 $\alpha^p=I$：$pN=0$、$\binom{p}{2}N^2=0$，所以 $(I+N)^p=I$。

现说明所有作用的约化。设 $R=\bar r$，共轭 $\alpha'=\beta\alpha\beta^{-1}$ 的参数满足

$$v'=zv/R,\qquad w'=Rw/z,\qquad c'=c+(hv-w'\ell)/R.$$

这来自分别比较 $\beta N$ 与 $N'\beta$ 的两个坐标；其第一坐标的 $i,j$ 系数为

$$p(Rc+hv),\ pRw,\qquad p(c'R+w'\ell),\ pw'z,$$

第二坐标的 $i$ 系数为 $zv$ 与 $v'R$。所以只要 $v$ 或 $w$ 非零，就能选 $h$ 或 $\ell$ 消去 $c$。更换商生成元 $x\mapsto x^k$ 则把作用改为

$$\alpha^k=I+kN+\binom{k}{2}N^2,\quad (v,w,c)\mapsto(kv,kw,kc+\tbinom{k}{2}vw).$$

因此全部非平凡作用可约化为

$$(c,v,w)=(1,0,0),\ (0,1,0),\ (0,0,1),\ (0,1,d),$$

最后一项 $d\neq 0$ 按平方类取值。具体说，核重标记保持 $vw$ 不变，商生成元更换使它乘 $k^2$；取 $R,z$ 使新 $v=1$，再消去 $c$，便得新 $w=k^2vw$。域的非零乘法群循环，平方子群指数二，故恰取 $d=1,\epsilon$ 两类。

范数的精确式为

$$N_\alpha = pI + \binom{p}{2}N + \binom{p}{3}N^2.$$

用 $\sum_{j=0}^{p-1} j=\binom{p}{2}$ 与 $\sum_{j=0}^{p-1}\binom{j}{2}=\binom{p}{3}$ 可得此式，后一个求和由三元子集中最大元素的选择数得到。$p\geq 5$ 时它简化为

$$N_\alpha(i,j)=(pi,0).$$

$p=3$ 时则为 $N_\alpha(i,j)=(3(1+vw)i,0)$。所以只有 $p=3, vw=-1$ 时范数像降为零。

把固定点条件 $vi=0$（模 $p$）、$ci+wj=0$（模 $p$）逐行求出，再模去范数像，得到

| $(c,v,w)$ | $\mathrm{Fix}(\alpha)$ | $t$ 代表 |
|---|---|---|
| $(0,0,0)$ | $A$ | $1,b,a$ |
| $(1,0,0)$ | $\langle a^p,b\rangle$ | $1,b$ |
| $(0,1,0)$ | $\langle a^p,b\rangle$ | $1,b$ |
| $(0,0,1)$ | $\langle a\rangle$ | $1,a$ |
| $(0,1,d)$ | $\langle a^p\rangle$ | $1\quad(p\geq 5)$ |
| $(0,1,1)$ | $\langle a^3\rangle$ | $1\quad(p=3)$ |
| $(0,1,2)$ | $\langle a^3\rangle$ | $1,a^3\quad(p=3)$ |

补充非零代表归一的依据：第一行在 $A/pA$ 上的三角自同构分为零、非零纯 $b$、首坐标非零三轨道。其余前三个非平凡作用的固定群模范数均为一维，逐一给出缩放映射如下。对 $(1,0,0)$，取 $\beta(a)=a,\beta(b)=b^q$；对 $(0,1,0)$ 和 $(0,0,1)$，取 $\beta(a)=a^q,\beta(b)=b^q$，其中整数 $q$ 的模 $p$ 余类任取非零值。代入共轭参数公式，这些 $\beta$ 均保持原作用。前三行的非零余类分别由 $b,b,a$ 生成，以上映射分别将其送到 $b^q,b^q,a^q$，所以每一行的所有非零余类确实落在一个轨道内。在最后一行，取 $z=R$、$h=d\ell$ 就保持该作用，且把 $a^p$ 送到 $(a^p)^R$，故所有非零参数等价。没有把非零轨道中的不同值另算模型。

还须跨行去重。平凡作用三项依次为 $C_{p^2}\times C_p^2, C_{p^2}^2, C_{p^3}\times C_p$。$(1,0,0), t=1$ 为 $M_p\times C_p=\mathcal{V}_p$，$t=b$ 为 $\mathcal{H}_p$。$(0,1,0), t=1$ 为 $\mathcal{E}_p$；$t=b$ 也为 $\mathcal{H}_p$：此时 $x^p=b$、$[x,a]=x^p$，改取循环核生成元 $a'=x$、中央元 $b'=a^p$、外元 $y=a^{-1}$，则

$$ya'y^{-1}=(a')^{1+p},\qquad y^p=(b')^{-1}.$$

再把 $b'$ 换成 $(b')^{-1}$，便是 $\mathcal{H}_p$ 的同一坐标。$(0,0,1), t=1$ 为 $\mathcal{K}_p$；$t=a$ 时 $x^p=a$，所以 $x$ 阶为 $p^3$，且 $[x,b]=x^{p^2}$。因而 $bxb^{-1}=x^{1-p^2}$，把 $b$ 换成 $b^{-1}$ 即得 $\mathcal{C}_p$。最后三行正是定理的 $D_p(d,s)$ 模型。

**初等交换核**。取 $A=\mathbb{F}_p^3$，仍记 $N=\alpha-I$。特征 $p$ 下 $I$ 与 $\alpha$ 交换，二项式系数的中间项被 $p$ 整除，所以

$$N^p=(\alpha-I)^p=\alpha^p-I=0.$$

先证明 $N^3=0$，以便后面的选基论证不预先使用待证的标准形。若 $N\neq 0$，令 $m$ 为 $N^m=0$ 的最小正整数；取 $w$ 使 $N^{m-1}w\neq 0$。向量

$$w, Nw, \ldots, N^{m-1}w$$

线性独立：若 $\sum_{i=0}^{m-1} c_i N^i w = 0$，先作用 $N^{m-1}$，得到 $c_0 N^{m-1} w = 0$，故 $c_0 = 0$；已知 $c_0, \dots, c_{j-1} = 0$ 时，作用 $N^{m-1-j}$ 得 $c_j N^{m-1} w = 0$，故 $c_j = 0$。归纳得所有系数为零。空间维数为三，所以 $m \le 3$，从而 $N^3 = 0$；$N = 0$ 时该结论也成立。

现在分三种情形。$N = 0$ 时为平凡作用。$N \neq 0, N^2 = 0$ 时，由 $\operatorname{im} N \subseteq \ker N$ 和秩–零度公式，若秩为 $r$，则 $r \le 3 - r$；非零性使 $r = 1$。取 $u \neq 0$ 生成 $\operatorname{im} N$，再取 $v$ 使 $Nv = u$，最后在二维的 $\ker N$ 中选 $w$ 补足 $u$。$v \notin \ker N$，所以 $u, v, w$ 为基，并有

$$Nu = 0, \quad Nv = u, \quad Nw = 0.$$

若 $N^2 \neq 0$，取 $w$ 使 $N^2 w \neq 0$，置 $u = N^2 w, v = Nw$。已证 $N^3 = 0$，所以对关系 $c_0 w + c_1 N w + c_2 N^2 w = 0$，先作用 $N^2$ 得 $c_0 = 0$，再作用 $N$ 得 $c_1 = 0$，最后得 $c_2 = 0$。故 $u, v, w$ 为基，且

$$Nu = 0, \quad Nv = u, \quad Nw = v.$$

平凡作用下范数为零，固定 $t = 0$ 或非零，分别给 $C_p^4$ 与 $C_{p^2} \times C_p^2$。秩一时范数也为零，因为 $pI = \binom{p}{2} N = 0$、$N^2 = 0$；固定空间为 $\langle u, w \rangle$。保持作用的基变换保留直线 $\operatorname{im} N = \langle u \rangle$，所以 $t$ 可取 $0, u, w$：在直线内缩放 $u$ 及 $v$；在线外则直接选 $w = t$。$t = 0$ 给 $\mathcal{U}_p$；$t = u$ 时 $x^p = u$、$[x, v] = u = x^p$。令 $a = x, b = v^{-1}$，则 $|a| = p^2, |b| = p$，且

$$bab^{-1} = v^{-1} x v = ux = x^{1+p} = a^{1+p}.$$

$\langle x, v \rangle$ 包含 $u = x^p$，其元素为 $x^i v^j$ $(0 \le i < p^2, 0 \le j < p)$，由原坐标的唯一性恰有 $p^3$ 个；它不含非平凡的 $w$ 幂。因此它是 $M_p$，并与独立中央的 $w$ 组成 $\mathcal{V}_p$；$t = w$ 时以 $a = x, b = u, y = v^{-1}$ 得

$$|a| = p^2, \quad |b| = p, \quad yay^{-1} = ab, \quad y^p = 1,$$

所以为 $\mathcal{E}_p$。

秩二时固定空间只有 $\langle u \rangle$。范数式在 $\mathbb{F}_p$ 上给

$$N_\alpha = 0 \quad (p \ge 5), \qquad N_\alpha = N^2 \quad (p = 3).$$

因此 $p \ge 5$ 时 $t = 0, u$ 两轨道（共同非零缩放三个基向量即可归一）；$p = 3$ 时范数像等于固定空间，$t$ 全部可消去。它们就是 $J_p(e)$ 的列表。

上述三个核的全部数据已进入定理列表。尚须证明没有剩余重复；下面两段分别完成类二与类三的去重。

六个非交换类二模型的中心、幂子群及其与导出群的交为

| $G$ | $Z(G)$ | $G^p$ | $\lvert G' \cap G^p \rvert$ |
|---|---|---|---|
| $\mathcal{C}_p$ | $C_{p^2}$ | $C_{p^2}$ | $p$ |
| $\mathcal{U}_p$ | $C_p^2$ | $1$ | $1$ |
| $\mathcal{V}_p$ | $C_p^2$ | $C_p$ | $p$ |
| $\mathcal{K}_p$ | $C_{p^2}$ | $C_p$ | $p$ |
| $\mathcal{E}_p$ | $C_p^2$ | $C_p$ | $1$ |
| $\mathcal{H}_p$ | $C_p^2$ | $C_p^2$ | $p$ |

逐项计算如下。循环核模型中与 $x$ 交换的核元素为 $\langle a^p \rangle$，外陪集不中央，导出群为 $\langle a^{p^2} \rangle$，$p$ 次幂生成 $\langle a^p \rangle$。$\mathcal{U}_p, \mathcal{V}_p$ 的数据由已算出的 $p^3$ 因子与一个独立中央 $C_p$ 得到。在 $\mathcal{K}_p$ 中中心为

$\langle a\rangle$，交换子 $[x,b]=a^p$，而 $p$ 次幂生成 $\langle a^p\rangle$。在 $\mathcal{E}_p$ 中中心为 $\langle a^p,b\rangle$，导出群为 $\langle b\rangle$，幂子群为 $\langle a^p\rangle$，两者独立。$\mathcal{H}_p$ 的中心为 $\langle a^p,b\rangle$，导出群为 $\langle a^p\rangle$，又 $a^p$ 和 $x^p=b$ 生成整个中心。所有模型的交换子均中央且阶 $p$，所以奇 $p$ 的乘积幂公式使 $p$ 次幂逐因子相乘；这证明上述幂子群没有遗漏额外生成元。六行各不相同，故六模型互不等价。

对类三的 $D,J$ 模型，$G'=N(A)$、$[G,G']=N^2(A)\neq 1$、下一次交换子为一，故幂零类恰为三。在 $D$ 中 $G'=\langle b,a^p\rangle$；若一个外元素含非零 $x^k$，它对 $b$ 的共轭乘上 $a^{pdk}\neq 1$，所以

$$C_G(G')=A\cong C_{p^2}\times C_p.$$

在 $J$ 中 $G'=\langle u,v\rangle$，非零 $x^k$ 把 $v$ 送到 $u^kv\neq v$，所以同样 $C_G(G')=A$，但此处 $A\cong C_p^3$。这个中心化子为特征子群，因为 $G'$ 特征，故任意自同构保持它。于是两类核绝不混同。

$D$ 模型之间的任何同构因此必须保持该核，已经证明的参数变换表明 $d$ 只会乘非零平方，所以两平方类不同。$p=3,d=2$ 时，对任一商生成元更换 $x\mapsto a_0x^k$，$k=1,2$，相应作用参数的乘积仍为 $2k^2=2$，范数仍为零。新的 $t$ 只经非零标量变为原 $t$ 的非零倍数，所以 $t=1$ 与 $t=a^3$ 不可能互换。$J$ 模型在 $p\geq 5$ 时 $e=0$ 的全群指数为 $p$，而 $e=1$ 含 $p^2$ 阶的 $x$：具体地，$1\leq k<p$ 时 $\alpha^k$ 的各次幂恰为 $\alpha$ 的各次幂的一次重排，所以 $N_{\alpha^k}=N_\alpha=0$。逐次移动外元给

$$(ax^k)^p=N_{\alpha^k}(a)+kt=kt$$

（此式核坐标用加法记号）。核内元素也全被 $p$ 次幂消去，因此 $e=0$ 时全群指数为 $p$；$e=1$ 时 $x^p=u\neq 1$，$x$ 阶为 $p^2$。这两个模型不同构。$p=3$ 本就只余一类。类三恰有四类。

五个交换模型的最大元素阶依次为 $p^4,p^3,p^2,p^2,p$；两个最大阶同为 $p^2$ 的模型中，阶整除 $p$ 的元素分别有 $p^2$ 与 $p^3$ 个，所以也不同构。交换性、幂零类二和类三把三组区分。最终类型总数为 $5+6+4=15$。 □

## 6.22 二十四阶：正规三阶核与四点作用的分岔

**定理 6.56.** 二十四阶群恰有十五个同构类型。其中十二个有正规 *Sylow* 三子群；它们均为 $C_3\rtimes P$，$P$ 为八阶群，作用数据如下。表中的 $K$ 为非平凡作用 $P\to\mathrm{Aut}(C_3)=C_2$ 的核。

| $P$ | 作用平凡的类型数 | 非平凡作用的核代表 |
|---|---|---|
| $C_8=\langle r\rangle$ | 1 | $\langle r^2\rangle\cong C_4$ |
| $C_4\times C_2=\langle a,b\rangle$ | 1 | $\langle a\rangle\cong C_4$；　$\langle a^2,b\rangle\cong V_4$ |
| $C_2^3$ | 1 | $C_2^2$ |
| $D_8=\langle r,s\rangle$ | 1 | $\langle r\rangle\cong C_4$；　$\langle r^2,s\rangle\cong V_4$ |
| $Q_8$ | 1 | $\langle i\rangle\cong C_4$ |

每个核代表给出一个非平凡作用类型，核外元素均对 $C_3$ 取逆。其余三个模型为

$$S_4,\qquad A_4\times C_2,\qquad B_{24}=Q_8\rtimes C_3,$$

其中 $C_3$ 的生成元按 $i\mapsto j\mapsto k\mapsto i$ 作用。

*证明.* 若 Sylow 三子群 $N$ 正规，取 Sylow 二子群 $P$，则 $N\cap P=1$、$NP=G$，得到半直积。作用像只可能是平凡群或 $C_2$，所以非平凡作用由一个指数二核 $K\leq P$ 唯一决定。

现逐行约化这些核。$C_8$ 只有一个指数二子群。$C_4\times C_2$ 的三个指数二子群已在八阶表中给出，两个循环的 $\langle a\rangle,\langle ab\rangle$ 被自同构 $a\mapsto ab,b\mapsto b$ 交换，非循环的 $\langle a^2,b\rangle$ 单独一类。$C_2^3$ 的

二维子空间都能选基再扩基，故任意两个被某个线性自同构互相送到。$D_8$ 的指数二子群为一个 $C_4$ 与两个 $V_4$；自同构 $r \mapsto r, s \mapsto rs$ 交换两个 $V_4$。$Q_8$ 的三个阶四循环子群被 $i, j, k$ 的循环置换交换。因此表中列出的恰为全部核轨道。

核的重标记若相差 $\beta \in \mathrm{Aut}(P)$，在半直积坐标中用 $(a, h) \mapsto (a, \beta(h))$ 即得同构。反过来，若两个中间群同构，其唯一 Sylow 三子群必彼此对应，Sylow 二子群的像可再经内部共轭调到所选 $P$，所以诱导 $P$ 的同构，且把

$$K = C_P(N)$$

送到另一作用核。因此不同的 $P$ 类型不能混同，同一行中 $C_4$ 与 $V_4$ 核也不能混同；平凡作用的核阶八，非平凡作用核阶四，更不能混同。故表中给出恰好 $2+3+2+3+2=12$ 个不同模型。

以下 Sylow 三子群不正规，所以有四个。共轭作用给出到 $S_4$ 的传递像。核 $L$ 包含于一个 Sylow 三子群的正规化子，其阶为 $24/4 = 6$；像阶又被四整除，故 $|L|$ 只能为 $1, 2, 3, 6$。$|L| = 3$ 时 $L$ 是正规 Sylow 三子群，矛盾。$|L| = 6$ 时，$L$ 中 Sylow 三子群的个数整除二且模三余一，所以为一。任一 $L$ 的自同构都把三阶子群送到三阶子群，故这个唯一子群 $Q$ 特征于 $L$。因 $L$ 是作用核而正规于 $G$，任意 $g \in G$ 的共轭在 $L$ 上限制为自同构，遂有 $gQg^{-1} = Q$。于是 $Q$ 是 $G$ 的正规 Sylow 三子群，仍矛盾。于是只余 $|L| = 1$ 或二。

若 $L = 1$，像阶二十四，故 $G \cong S_4$。若 $|L| = 2$，像是十二阶的 $S_4$ 子群，已知只能为 $A_4$。$L$ 二阶正规，共轭到 $\mathrm{Aut}(C_2) = 1$，所以 $L$ 中央。令 $P$ 为 $V_4 \trianglelefteq A_4$ 的原像，得八阶正规 Sylow 二子群，并取三阶补群 $C$，所以 $G = P \rtimes C_3$。

作用必须非平凡，否则 $C$ 正规。八阶五个模型中，$\mathrm{Aut}(C_8)$ 阶四，$\mathrm{Aut}(C_4 \times C_2)$ 阶八；$\mathrm{Aut}(D_8)$ 也阶八，因为 $r$ 的像有两个四阶生成元可选，$s$ 的像有四个反射可选，任意这样的选择均给自同构。因此这三类没有阶三作用。剩下 $P = C_2^3$ 或 $Q_8$。

在 $C_2^3$ 上，$\mathrm{Aut}(P) = \mathrm{GL}_3(\mathbb{F}_2)$ 阶为

$$(8-1)(8-2)(8-4) = 168.$$

三个因子依次为选第一个非零列、第二个不在第一列直线内、第三个不在前两列平面内的选择数。三在该阶数中只出现一次，所以任何阶三子群都是 Sylow 三子群，彼此共轭。取代表作用在一个二维子空间上循环置换三个非零向量，固定补出的一维空间。$V_4 \rtimes C_3 \cong A_4$：在 $A_4$ 中三个双换位被 (123) 循环共轭，核与补群交平凡、阶乘积十二。因此代表模型为 $A_4 \times C_2$。

在 $Q_8$ 上，$i$ 的像可取六个四阶元之一，$j$ 的像可取不在同一循环子群中的四个四阶元之一。任何这类像都有平方 $-1$ 且反交换，唯一四元数坐标表明它们定义自同构，故 $|\mathrm{Aut}(Q_8)| = 6 \cdot 4 = 24$。阶三子群仍均为 Sylow 三子群，彼此共轭；代表可取 $i \mapsto j \mapsto k \mapsto i$，得到 $B_{24}$。换掉 $C_3$ 的生成元只把作用生成元取逆，不增加类型。

两个非平凡半直积的 Sylow 三子群都不正规：若它与正规 $P$ 同时正规，则两者的交换子属于交，交平凡使二者相互中央化，与非平凡作用矛盾。故确实属于这一分支。$S_4$、$A_4 \times C_2$、$B_{24}$ 的 Sylow 二子群分别为 $D_8, C_2^3, Q_8$，彼此不同构；第一种可取由 (1234)、(13) 生成的二面体子群。它们也不可能与前十二个模型同构，因为 Sylow 三子群数不同。十五种已全部构造并去重。 □

## 6.23 三十阶：元素计数与十五阶正规核

**定理 6.57.** 阶为三十的群恰有四种：

$$C_{30}, \qquad S_3 \times C_5, \qquad D_{10} \times C_3, \qquad D_{30}.$$

证明. Sylow 数满足 $n_5 = 1$ 或六，$n_3 = 1$ 或十。若二者都不为一，不同五阶子群只有单位相交，不同三阶子群也只有单位相交，且三阶元不可能为五阶元，于是非单位元至少有

$$6(5-1) + 10(3-1) = 44 > 29,$$

矛盾。所以至少一个 Sylow 子群正规。

若五阶子群 $P$ 正规，取任意三阶子群 $Q$。共轭同态 $Q \to \mathrm{Aut}(P)$ 的像阶同时整除三与四，故平凡，$Q$ 中央化 $P$。$N = PQ$ 因 $P$ 正规而为子群，交平凡且相互交换，故 $N \cong C_5 \times C_3 \cong C_{15}$。其指数二，故正规。

若三阶子群 $Q$ 正规，取任意五阶子群 $P$。共轭同态 $P \to \mathrm{Aut}(Q)$ 的像阶同时整除五与二，亦平凡。于是 $N = QP \cong C_{15}$，仍由指数二而正规。两种分支均得十五阶循环正规核；它的三阶与五阶子群唯一，因而也都正规于全群。

取 Sylow 二子群 $\langle b \rangle$，与 $N$ 交平凡，故 $G = N \rtimes \langle b \rangle$。把 $N = C_3 \times C_5$，共轭保持每个唯一素数阶子群，在每个分量上的二阶作用只能为恒等或取逆：若模相应奇素数有 $u^2 = 1$，则 $(u-1)(u+1) = 0$，域中只能 $u = 1$ 或 $-1$。因此两个分量共有四种符号组合。全正给 $C_{30}$；只反转三阶分量给 $S_3 \times C_5$；只反转五阶分量给 $D_{10} \times C_3$；同时反转给 $D_{30}$。

后三者的中心阶分别为五、三、一。求法是：在核中，受取逆的奇阶分量只有单位被固定；外陪集任一元素在核上诱导同一个非平凡作用，故都不中央。第一个模型交换，后三者不交换，所以四者不同构。所有作用均由外部半直积构造存在，分类完成。 □

## 6.24 三十六阶：线性作用与非正规九阶 Sylow 分支

**定理 6.58.** 三十六阶群恰有十四个同构类型。十二个有正规 *Sylow* 三子群 $P$，它们均为 $P \rtimes H$，其中 $|P| = 9$、$|H| = 4$，作用代表如下。

1. $P = C_9$：$H = C_4$ 时其生成元作用为恒等或取逆；$H = V_4$ 时作用平凡或像为取逆二阶群。共四类。

2. $P = \mathbb{F}_3^2$，$H = C_4$：生成元作用为

$$I, \quad -I, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

   共四类。

3. $P = \mathbb{F}_3^2$，$H = V_4$：写 $H$ 的非平凡符号特征为 $\chi, \psi, \chi\psi$，平凡特征为 $1$，则二维表示的两条特征可取为

$$(1,1), \quad (1,\chi), \quad (\chi,\chi), \quad (\chi,\psi), \qquad \chi \neq \psi.$$

   共四类。

其余两个模型为

$$A_4 \times C_3, \qquad V_4 \rtimes C_9,$$

后一作用将九阶生成元送到 $V_4$ 的一个阶三自同构。

证明. 若 $P$ 正规，取 Sylow 二子群 $H$，便得 $G = P \rtimes H$。$P$ 为 $C_9$ 或 $C_3^2$，$H$ 为 $C_4$ 或 $V_4$。

$\mathrm{Aut}(C_9)$ 的六个元素由模九单位 $1, 2, 4, 5, 7, 8$ 给出。它们中阶整除四者只有 $1, -1$：单位群阶为六，若 $u^4 = 1$，则 $u$ 的阶同时整除四与六，故整除二，于是 $u^2 = 1$。由 $(u-1)(u+1) = 0$（模九）且三不同时整除两因子，必须有一个因子被九整除，得 $u = \pm 1$。故四阶循环作用只有两种；$V_4$ 的非平凡作用都具有一个阶二核，不同核被 $\mathrm{Aut}(V_4)$ 交换，所以也只有两种。这证明第一组穷尽。

在 $P = \mathbb{F}_3^2$、$H = C_4$ 时，作用 $T$ 满足 $T^4 = I$。对 $T^2$ 应用正负特征分解，有

$$P = \ker(T^2 - I) \oplus \ker(T^2 + I).$$

具体地，因 2 在 $\mathbb{F}_3$ 中可逆，对每个 $z \in P$ 置

$$z_+ = \frac{z + T^2 z}{2}, \qquad z_- = \frac{z - T^2 z}{2}.$$

由 $T^4 = I$，$T^2 z_+ = z_+$、$T^2 z_- = -z_-$，且 $z = z_+ + z_-$。两空间的交中若有 $y$，则 $T^2 y = y = -y$，故 $2y = 0$，从而 $y = 0$；这证明了所写直和。又 $T$ 与 $T^2 \pm I$ 交换，所以它保持两个核空间。在第一空间上 $T^2 = I$，用 $z \mapsto (z \pm Tz)/2$ 的相同投影公式，再按 $T$ 的正负特征分解；在第二空间上 $T^2 = -I$。后一空间不可能一维，因为 $\mathbb{F}_3$ 中没有平方为负一的数。因此若第二空间非零，它就是全部二维空间。任取 $v \neq 0$，$v, Tv$ 必独立，否则 $Tv = cv$ 导致 $c^2 = -1$；在基 $v, Tv$ 下 $T$ 正是矩阵 $J$。若第二空间为零，则 $T$ 在两个一维特征空间上取正或负，只给 $I, -I, \mathrm{diag}(1, -1)$ 三种。把循环生成元取逆不增加类型，因为 $J^{-1} = -J$ 与 $J$ 由基变换 $\mathrm{diag}(1, -1)$ 共轭。第二组因而穷尽。

$H = V_4 = \langle h_1, h_2 \rangle$ 时，两个作用交换且平方为一。先把 $h_1$ 分为正负特征空间；因 $h_2$ 与 $h_1$ 交换，它保持这两个空间，再在各空间内按 $h_2$ 分解。这样得到共同特征基，每条基线由一对正负号决定，恰是 $V_4$ 的四个符号特征。二维表示由两个允许重复的特征组成。更换二维基可以交换这两个特征，$\mathrm{Aut}(V_4)$ 则任意置换三个非平凡特征。于是：两个都平凡；一个平凡一个非平凡；两个相同非平凡；两个不同非平凡，恰为四种。这证明第三组穷尽。

还须说明十二者彼此不同构。同构保持唯一 Sylow 三子群的类型，以及 Sylow 二子群的类型，所以三大组之间不会混同。在第一组，相同 $H$ 的平凡与非平凡作用由中心化子 $C_H(P)$ 的阶区分。第二组四作用的

$$\big(|\operatorname{im}(H \to \mathrm{Aut}(P))|, \dim C_P(H)\big)$$

依次为 $(1,2), (2,0), (2,1), (4,0)$；第三组依次为 $(1,2), (2,1), (2,0), (4,0)$。每一组内这些数对不同。同构把 Sylow 二子群送到一个共轭 Sylow 子群，而共轭保持这些数对，故它们是所需的抽象群不变量。

最后假定 Sylow 三子群不正规，此时个数为四。其共轭作用在四点上传递，像阶整除 $\gcd(36, 24) = 12$ 又被四整除，故为四或十二。像阶四会使核阶九，成为正规 Sylow 三子群，矛盾。所以像阶十二，像为 $A_4$，核 $K$ 阶三。

共轭同态 $G \to \mathrm{Aut}(K) \cong C_2$ 在 $K$ 上平凡，故下降到 $G/K \cong A_4$。任一 $A_4 \to C_2$ 的同态必平凡：其像若非平凡，核便为六阶子群，而十二阶子群分类已证明 $A_4$ 不含这种子群。因此 $K \leq Z(G)$。

令 $N$ 为 $V_4 \trianglelefteq A_4$ 的原像，$|N| = 12$。取 $N$ 的 Sylow 二子群 $B$，则 $K$ 中央、$K \cap B = 1$、$KB = N$，所以 $N = K \times B$。从 $N/K \cong V_4$ 得 $B \cong V_4$，且直积分解表明 $B$ 是 $N$ 唯一 Sylow 二子群。因此 $B$ 特征于正规子群 $N$，故正规于 $G$。

取九阶 Sylow 三子群 $P$，得到 $G = B \rtimes P$。作用非平凡，否则 $P$ 正规。$\mathrm{Aut}(B) \cong S_3$：它任意置换三个非零向量，给出的六个置换均线性，故正是 $S_3$。作用像为阶三子群。若 $P = C_9$，其生成元映到一个阶三元素，两个可能生成元互为逆且在 $S_3$ 共轭，故只得一个 $V_4 \rtimes C_9$。若 $P = C_3^2$，非平凡同态的核为一维子空间，选核的基与补基后，作用只在补基方向非平凡，所以

$$G \cong (V_4 \rtimes C_3) \times C_3 \cong A_4 \times C_3.$$

这两个模型的 Sylow 三子群类型不同，故不同构；非平凡作用又保证它们的 Sylow 三子群不正规，与前十二者区分。十四种分类完成。 □

## 6.25 按阶分类的边界与本章结论表

本章的分类对象是明确列出的阶族。下表中的“完整”表示三个责任均已在正文完成：模型确实存在、任意该阶群都进入列表、列表中没有重复同构类型；它不表示任意阶的有限群都已分类。

| 群的阶 | 同构类型数 | 完成分类的主机制 |
|---|---|---|
| $p^2$ | 2 | 中心商与独立生成元 |
| $pq$ $(p<q)$ | 1 或2 | 唯一 Sylow 核与循环作用 |
| $p^3$ ($p$ 奇) | 5 | 中央交换子与幂映射 |
| 8 | 5 | 生成元平方的四种组合 |
| 12 | 5 | 陪集忠实作用或正规三阶核 |
| 16 | 14 | 八阶交换正规核及进位参数 |
| $p^4$ ($p$ 奇) | 15 | 三种交换核、范数、参数轨道与特征核 |
| $2p^2$ ($p$ 奇) | 5 | 二阶作用的正负特征空间 |
| $4p$ $(p \ge 5)$ | 4 或5 | 四阶作用的像与生成元替换 |
| $3p^2$ $(p \ge 5)$ | 3 或6 | 三阶作用的特征值与不可约多项式 |
| $6p$ $(p \ge 5)$ | 4 或6 | 平均二余循环消去扩张参数 |
| 24 | 15 | 正规三阶核或四点共轭作用 |
| 30 | 4 | Sylow 元素计数与十五阶正规核 |
| 36 | 14 | 二维线性作用或四点共轭作用 |

上述结果给出不超过三十一阶的逐阶完整分类。为防止把一般定理的例外阶漏掉，下面列出每一阶的同构类型数 $a(n)$：

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a(n)$ | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 5 | 2 | 2 | 1 | 5 | 1 | 2 | 1 | 14 |

| $n$ | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a(n)$ | 1 | 5 | 1 | 5 | 2 | 2 | 1 | 15 | 2 | 2 | 5 | 4 | 1 | 4 | 1 |

这里一阶群唯一；素数阶群由任一非单位元生成，因为该元素阶必须整除群阶且不为一。其余每个阶都属于表中的已证分类：四、九、二十五用平方阶；六、十、十四、十五、二十一、二十二、二十六用 $pq$；八、十二、十六、二十四、三十有专门定理；十八用 $2p^2$；二十、二十八用 $4p$；二十七用奇素数立方阶。这个逐项对应给出计数表的依据，而非另引数表。

例如阶九、十八、二十、二十七、二十八都已被这些定理覆盖。二十四阶与三十六阶的十五种、十四种模型已另列定理证明。定理 6.55 还独立完成了每个奇素数 $p$ 的 $p^4$ 阶十五种模型；连同十六阶十四种模型，四次幂阶现已全部覆盖。这不是由十六阶结果外推，而是对奇特征中的作用、范数与参数轨道另作计算。下面把其中使用的一般有限化步骤单独概括，以区别“给出候选数据”与“完成同构类型去重”。

**命题 6.59** (四次幂分类所用的有限化步骤)**.** *给定素数 $p$，阶 $p^4$ 群的分类可以化为有限个交换核上的自同构与进位参数问题：先取全部阶 $p^3$ 交换模型 $A$，再求*

$$\alpha \in \mathrm{Aut}(A), \quad \alpha^p = I, \qquad t \in \mathrm{Fix}(\alpha).$$

*这些有限数据通过命题 6.51 产生全部阶 $p^4$ 群；仅有此参数化还没有消除重复，十六阶与奇素数四次幂阶的分类定理分别完成了后续去重。*

*证明.* 引理 6.50 保证每个群都有这样的核 $A$，交换 $p^3$ 分类给出 $C_{p^3}, C_{p^2} \times C_p, C_p^3$ 三种核。每个群因此至少产生一组所列数据。反过来，满足两个条件的任何数据均由进位坐标命题构造出群，坐标数为 $p^3 \cdot p = p^4$。核为有限集合，故其置换只有有限个，自同构是其中保持运算的置换；每个固定点集合也有限，所以候选数据有限。

更换 $x$ 与核标记会改变 $t$ 与 $\alpha$；此外，同一个中间群可能含有不同类型的交换指数 $p$ 核。十六阶证明中 $\mathcal{M}_{16}$ 同时以 $C_8$ 核和 $C_4 \times C_2$ 核出现，就是实际例子。因此有限化必须接上逐项参数约化与跨核去重，才能得到分类定理。本章已对二与奇素数分别完成这一步；这里的有限化命题本身不承担去重结论。 □

**注 6.60** (有限模型验算的责任边界)**.** 本章的有限坐标模型可以逐元验证结合律、求中心、数子群与元素阶。这些验算能发现表格或坐标的错误，却不能替代“任意满足条件的群都进入列表”的证明；后者分别由 Sylow 论证、中心商论证以及交换正规核引理承担。相同不变量也不自动给同构：$U_3(\mathbb{F}_p)$ 与 $M_p$ 共有的中心与共轭类数据已提供反例。十六阶中 $Q_8 \times C_2$ 与 $L_{16}$ 的中心和元素阶分布相同，还必须使用平方生成子群区分。

## 文献说明

本章前半的分类路线核读 James S. Milne, *Group Theory*, Version 4.01 (2025)，第 48 页例 3.11、3.14–3.15，第 63 页例 4.21，第 82–84 页例 5.14、5.16–5.17。参照的是半直积与低阶分类的结构路线；本章重新给出坐标同构、中心商引理、中央交换子的幂公式、奇素数立方阶的两种模型及元素阶计数。后续各节的子群、正规商群、混合阶族、二十四与三十六阶、自同构计数及十六阶参数表，由正文列出的坐标、群作用和线性代数逐项推导；奇素数四次幂阶的部分还按三个交换核逐项计算了作用、范数、特征三例外与跨核去重。它们都是标准群论结论，这里不主张结果原创，也不把未核读的文献章节列为直接依据。本文的 $D_{2n}$ 表示阶 $2n$ 的二面体群，与该文献的 $D_n$ 记法不同。

# 7　自由群与生成元、关系

第六章把有限群压缩为生成元、作用与进位参数，但一个写出的关系式列表还不是分类证明。本章先建立更一般的语言：关系式究竟规定哪个群；如何证明一个候选群没有额外关系；如何从陪集计算子群的自由基。这里的“群的表示”指生成元与关系的表示式，写作 $\langle X \mid R\rangle$；线性表示 $G \to \mathrm{GL}(V)$ 是后续的另一主题。

## 7.1　形式字母、词与约化算法

**定义 7.1.** 给定集合 $X$，使用带标记的不交并

$$X^{\pm} = X \times \{+1, -1\}.$$

把 $(x,+1)$ 写为 $x$，把 $(x,-1)$ 写为 $x^{-1}$。这里 $x^{-1}$ 暂时只是形式符号；即使 $X$ 本身由群元素组成，两个标记仍区别对待。定义字母的逆 $(x^{\varepsilon})^{-1} = x^{-\varepsilon}$。一个词是有限序列 $w = \ell_1 \cdots \ell_n$，其中 $\ell_i \in X^{\pm}$；长度为 $n$。唯一的零长度词记为 $\epsilon$。连接记为 $uv$，逆词定义为

$$w^{-1} = \ell_n^{-1} \cdots \ell_1^{-1}.$$

没有相邻互逆字母的词称为约化词。一次消去删除相邻的一对 $\ell\ell^{-1}$。

不能仅由“反复消去直到不能消去”定义唯一的答案，因为可选的消去位置可能不止一个。我们先指定算法，再证明选择无关。

从空序列开始，由左到右读词。当前存储序列为 $s$，读到字母 $\ell$ 时：若 $s$ 的最后一个字母是 $\ell^{-1}$，就删除它；否则把 $\ell$ 接在末尾。每一步之后存储序列都约化：删除末字不会产生新的相邻位置；接上字母时算法已排除唯一可能产生的互逆对。最后得到的约化词记为 $R(w)$。

**引理 7.2** (读入互逆字母是互逆的操作)**.** *在约化词的集合上，记读入 $\ell$ 的操作为 $T_\ell$，则*

$$T_{\ell^{-1}} T_\ell(s) = s.$$

*于是，在任意词中插入或删除相邻互逆对，都不改变 $R(w)$。*

*证明.* 若 $s$ 不以 $\ell^{-1}$ 结尾，包括 $s = \epsilon$ 的情形，第一次操作把 $\ell$ 接上，第二次恰把这个新字母删除，恢复 $s$。

若 $s = t\ell^{-1}$，第一次操作得到 $t$。$t$ 不以 $\ell$ 结尾，否则 $s$ 不约化。因此第二次读入 $\ell^{-1}$ 时不会删除 $t$ 的末字，而是把 $\ell^{-1}$ 接回，得到 $s$。这证明等式。

设原词为 $u\ell\ell^{-1}v$。读完前缀 $u$ 时的存储序列是 $R(u)$。接下来的两步由刚证等式保持这一序列，再读相同的后缀 $v$，所得结果与读入 $uv$ 相同。所以

$$R(u\ell\ell^{-1}v) = R(uv).$$

插入是删除的逆过程，同样保持结果。　□

**定理 7.3** (约化词的唯一性)**.** 任意词经过有限次消去都能变成约化词；无论选择哪些消去位置，最后的约化词总是 $R(w)$。并且

$$R(R(u)v) = R(uv) = R(uR(v)). \tag{7.1}$$

证明. 每次消去使长度减少二，故任何持续消去的过程至多进行 $\lfloor |w|/2 \rfloor$ 步，并在没有互逆相邻对时停止。设终点为约化词 $z$。算法对一个已约化词逐字只作接入，所以 $R(z) = z$。引理7.2又表明每一步消去保持 $R$，故 $z = R(z) = R(w)$。这同时证明存在与唯一。

把 $u$ 中的一串消去放在连接词 $uv$ 的前缀中实行，便从 $uv$ 到 $R(u)v$；每一步仍是合法的相邻消去，故二者的 $R$ 相等。把 $v$ 内的消去放在后缀中实行，得到另一个等号。消去可以在前缀与后缀连接处产生新的互逆对，这不影响论证，因为此处仅声明两者最后的约化结果相同。 □

**例 7.4.** 对 $w = ab\,b^{-1}a^{-1}a\,b^{-1}$，依次删除 $bb^{-1}$、前面新相邻的 $aa^{-1}$，得到 $ab^{-1}$；若先删除原词第四、第五位置的 $a^{-1}a$，则得到 $abb^{-1}b^{-1}$，再删中间一对，也得 $ab^{-1}$。定理处理的是所有词和所有消去顺序，而不只这两种选法。

## 7.2 自由群的构造与泛性质

**定理 7.5.** 在 $X^{\pm}$ 上全部约化词组成的集合上定义

$$u \cdot v = R(uv).$$

它构成群 $F(X)$，单位元为 $\epsilon$，逆元为逆词。把 $x \in X$ 送到单字词 $x$ 的映射 $\iota : X \to F(X)$ 是单射，并具有如下性质：对任意群 $G$ 和集合映射 $f : X \to G$，存在唯一群同态 $\widehat{f} : F(X) \to G$，使 $\widehat{f} \circ \iota = f$。

证明. 对约化词 $u, v, t$，由式(7.1)，

$$(u \cdot v) \cdot t = R(R(uv)t) = R(uvt) = R(uR(vt)) = u \cdot (v \cdot t).$$

这证明结合律。连接空词不改变原词，且原词已约化，故 $\epsilon$ 为双侧单位元。逆词仍约化：它若有相邻互逆对，倒转并取逆后原词也有这样的对。$ww^{-1}$ 可从中间逐对删除直到空词，$w^{-1}w$ 也如此，所以它们约化后均为 $\epsilon$。这证明双侧逆元。不同 $x$ 给出不同的单字序列，故 $\iota$ 单射。

定义词的求值

$$\mathrm{ev}_f(\ell_1 \cdots \ell_n) = f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n}, \qquad \ell_i = x_i^{\varepsilon_i},$$

空词求值为 $e_G$。删除相邻 $\ell\ell^{-1}$ 不改变求值，因为对应两因子乘积为 $e_G$。故

$$\mathrm{ev}_f(R(w)) = \mathrm{ev}_f(w).$$

将求值限制在约化词上作为 $\widehat{f}$。对 $u, v \in F(X)$，

$$\widehat{f}(u \cdot v) = \mathrm{ev}_f(R(uv)) = \mathrm{ev}_f(uv) = \widehat{f}(u)\widehat{f}(v),$$

所以它是群同态，并在每个 $x$ 上等于 $f$。每个约化词都是单字生成元及其逆的乘积，同态在这些单字上的值已经被 $f$ 固定，因此没有第二个选择。 □

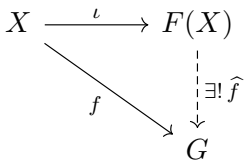



图 7.1: 上边是集合映射，竖边要求为群同态；任意生成元赋值唯一延拓。

**命题 7.6** (泛性质确定对象)**.** *若另一个群 $F'$ 与映射 $\iota' : X \to F'$ 有同样泛性质，则有唯一同构 $\alpha : F(X) \to F'$ 满足 $\alpha\iota = \iota'$。*

*证明.* 由两边的泛性质分别得 $\alpha : F(X) \to F'$、$\beta : F' \to F(X)$，满足 $\alpha\iota = \iota'$、$\beta\iota' = \iota$。于是 $\beta\alpha\iota = \iota$，而 $\mathrm{id}_{F(X)}\iota = \iota$。唯一性使 $\beta\alpha = \mathrm{id}_{F(X)}$。交换两群的角色得到 $\alpha\beta = \mathrm{id}_{F'}$，故 $\alpha$ 为同构；其唯一性已由第一边泛性质给出。 □

$X = \varnothing$ 时只有空词，故自由群平凡。$X = \{x\}$ 时约化词只能是 $x^n$，$n \in \mathbb{Z}$；因为正负字母若同时出现，两种符号首次交界处就可消去。映射 $n \mapsto x^n$ 因而给出 $\mathbb{Z} \cong F(\{x\})$。$X$ 至少有两个不同元素 $x, y$ 时，$xy$ 和 $yx$ 是不同约化词，故 $F(X)$ 非交换。

## 7.3 循环约化、挠元与中心

**定义 7.7.** 非空约化词若首字不等于末字的逆，称为*循环约化词*；空词也约定为循环约化。群中非单位元若有正整数次幂等于单位元，称为挠元；没有挠元的群称为无挠群。

**命题 7.8.** *每个非单位元 $w \in F(X)$ 都能写成*

$$w = tvt^{-1},$$

*其中 $v$ 是非空循环约化词，且所写连接本身已约化。对每个正整数 $k$，$w^k$ 的约化词为 $tv^kt^{-1}$，所以自由群无挠。*

*证明.* 从 $w$ 的首尾开始：若首字为 $\ell$、末字为 $\ell^{-1}$，剥去这两个字母，记录它们为外侧的共轭字母。中间词是原约化词的一段，仍约化。每次长度减少二，所以有限次后停止，得到 $tvt^{-1}$，其中 $v$ 的首尾不互逆或长度至多一。若原词非空，过程不能到空词：最后一次若从二字词到空词，该二字词就由互逆字母相邻组成，不约化。因此 $v$ 非空。原先剥离的字母按原顺序组成 $t$，故连接 $tvt^{-1}$ 与原约化词完全相同。

在乘积 $(tvt^{-1})^k$ 中，毗邻的 $t^{-1}t$ 消去，剩 $tv^kt^{-1}$。每一份 $v$ 内部约化；相邻两份的连接处不消去，因为 $v$ 循环约化；两端与 $t, t^{-1}$ 的接缝就是原词的接缝，也不消去。因此其长度为

$$2|t| + k|v| > 0.$$

由唯一性，它不等于空词，所以 $w^k \neq e$。 □

**命题 7.9.** *若 $x \in X$，则 $C_{F(X)}(x) = \langle x \rangle$。特别地，若 $|X| \geq 2$，则 $Z(F(X)) = \{e\}$。*

*证明.* $x$ 的整数幂当然与 $x$ 交换。反之，设约化词 $w$ 不是 $x$ 的幂。从 $w$ 中剥去开头与末尾全部 $x^{\pm 1}$ 字母，可唯一写成

$$w = x^r v x^s,$$

其中 $v$ 非空，首尾字母都不是 $x$ 或 $x^{-1}$，而 $r,s\in\mathbb{Z}$。于是群中

$$wxw^{-1}=x^{r}vx^{s}xx^{-s}v^{-1}x^{-r}=x^{r}vxv^{-1}x^{-r}.$$

最后的连接约化：$v$ 首尾都不涉及 $x$，排除了四个接缝的消去。其长度 $2|r|+2|v|+1$ 大于一，不可能等于单字词 $x$，所以 $w$ 不在中心化子中。

若 $x,y$ 是不同生成元，中心同时包含于 $\langle x\rangle$ 与 $\langle y\rangle$。非零幂 $x^{r}$ 和 $y^{s}$ 的约化词使用不同字母，不可能相等；两循环子群的交只有 $e$，故中心平凡。 □

## 7.4 正规闭包与表示式的准确含义

**引理 7.10.** *群 $K$ 中子集 $R$ 的正规闭包 $\langle\langle R\rangle\rangle_K$ 恰为所有有限乘积*

$$\prod_{i=1}^{t}u_i r_i^{\varepsilon_i}u_i^{-1},\qquad t\ge 0,\quad u_i\in K,\ r_i\in R,\ \varepsilon_i\in\{1,-1\}.$$

*空乘积为 $e$。*

*证明.* 所列集合 $N$ 含空乘积；连接两个有限乘积证明乘法封闭；一个乘积的逆按相反顺序排列各因子的逆，而

$$(ur^{\varepsilon}u^{-1})^{-1}=ur^{-\varepsilon}u^{-1},$$

仍是允许因子，所以 $N$ 是子群。对 $k\in K$，

$$k\left(\prod_i u_i r_i^{\varepsilon_i}u_i^{-1}\right)k^{-1}=\prod_i (ku_i)r_i^{\varepsilon_i}(ku_i)^{-1}\in N,$$

故 $N$ 正规。取 $t=1,u_1=e,\varepsilon_1=1$，知 $R\subseteq N$。任意包含 $R$ 的正规子群都包含每个共轭因子及其有限乘积，因而包含 $N$。所以 $N$ 正是最小的这样的正规子群。 □

**定义 7.11.** 给定字母集 $X$ 和 $F(X)$ 中的子集 $R$，定义

$$\langle X\mid R\rangle=F(X)/\langle\langle R\rangle\rangle_{F(X)}.$$

$X$ 称为生成元集，$R$ 中的词称为关系子。关系式 $u=v$ 表示收入关系子 $uv^{-1}$。一个群有这种商群同构，便称此为它的表示式。$X$ 和 $R$ 都有限时称为有限表示。

**定理 7.12** (表示式的泛性质)**.** *设 $P=\langle X\mid R\rangle$，$\bar{x}$ 是 $x$ 在商中的像。任意映射 $f:X\to G$ 唯一诱导同态 $P\to G$，当且仅当每个 $r\in R$ 在 $f$ 下求值为 $e_G$。*

*证明.* $f$ 首先唯一延拓为 $\widehat{f}:F(X)\to G$。它经商映射 $q:F(X)\to P$ 下降，当且仅当 $\langle\langle R\rangle\rangle\subseteq\ker\widehat{f}$：必要性由核直接得到；充分性下定义 $q(w)\mapsto\widehat{f}(w)$，若 $q(w)=q(w')$，则 $w'^{-1}w\in\langle\langle R\rangle\rangle\subseteq\ker\widehat{f}$，所以两像相同，映射良定义并保持乘法。核是正规子群，故 $\langle\langle R\rangle\rangle\subseteq\ker\widehat{f}$ 又等价于 $R\subseteq\ker\widehat{f}$。这正是所列关系求值为单位元。商群仍由所有 $\bar{x}$ 生成，因此这样的同态唯一。 □

由引理7.10，两个词 $u,v$ 在 $P$ 中相等，当且仅当 $uv^{-1}$ 在自由群中是关系子及其逆的有限个共轭的乘积。这里需要的是正规闭包：仅取 $R$ 生成的普通子群，通常不能形成商群。这个等价条件说明一个具体等式要有什么代数凭证；它本身不保证已经给出判定任意两个词相等的终止算法。

**命题 7.13.** 每个群都是自由群的商，并有一个可能无限的表示式。

证明. 取生成集 $X \subseteq G$，例如 $X = G$。包含映射延拓为满同态 $\pi : F(X) \to G$，因为它的像含 $X$，从而含整个 $G$。取 $R = \ker \pi$，它本来就正规，所以 $\langle\langle R \rangle\rangle = R$，第一同构定理给出结论。

也可以把关系子完全显式写出。对每个 $g \in G$ 引入符号 $t_g$，收入所有

$$t_g t_h t_{gh}^{-1} \qquad (g, h \in G).$$

所得群 $P$ 中有 $\bar{t}_g \bar{t}_h = \bar{t}_{gh}$。先取 $g = h = e_G$ 得 $\bar{t}_{e_G}^2 = \bar{t}_{e_G}$，左右消去可得 $\bar{t}_{e_G} = e_P$；再取 $h = g^{-1}$ 得 $\bar{t}_{g^{-1}} = \bar{t}_g^{-1}$。所以 $g \mapsto \bar{t}_g$ 是同态。反向映射由 $t_g \mapsto g$ 诱导，因为所有关系在 $G$ 中成立。两复合分别固定每个 $g$ 和每个生成元 $\bar{t}_g$，因此是恒等同态。于是 $P \cong G$。 □

## 7.5 从正规形证明表示式：二面体群与交换化

**例 7.14** (二面体关系为什么恰好给出二面体群)**.** 对 $n \geq 3$，置

$$P_n = \langle r, s \mid r^n = e,\ s^2 = e,\ srs^{-1} = r^{-1} \rangle.$$

我们证明它恰有 $2n$ 个元素，而不是只核验一个已知模型满足这些关系。

在 $P_n$ 中，$s^{-1} = s$，且 $sr = r^{-1}s$。对 $i \geq 0$ 作归纳，有 $sr^i = r^{-i}s$；对负整数 $i$，由 $sr^{-1} = rs$ 同样归纳，所以该式对全部 $i \in \mathbb{Z}$ 成立。因而

$$(r^i s^\varepsilon)(r^j s^\delta) = r^{i + (-1)^\varepsilon j} s^{\varepsilon + \delta}, \qquad \varepsilon, \delta \in \{0, 1\}.$$

$\varepsilon = 0$ 时只是相邻 $r$ 幂合并；$\varepsilon = 1$ 时使用刚证的移位公式。指数分别模 $n$ 与模二约化。所有生成元、逆元均在所列形内，而这些形在乘法下封闭，所以 $P_n$ 中每个元素均可写成 $r^i s^\varepsilon$，$0 \leq i < n$，共有至多 $2n$ 种。

反过来，在集合 $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ 上用上式的坐标乘法，第四章的半直积构造给出一个恰有 $2n$ 个元素的群。坐标元素 $(1, 0), (0, 1)$ 满足所列关系，且生成全群，所以由定理7.12有 $P_n$ 到该群的满同态。它的像有 $2n$ 个元素，迫使前面的至多 $2n$ 个正规形全部不同。满同态于是为同构，得到 $P_n \cong D_{2n}$。

**命题 7.15** (自由群与一般表示式的交换化)**.** 记 $\mathbb{Z}^{(X)}$ 为所有有限支撑的整数族 $(m_x)_{x \in X}$，按坐标相加。对词 $w$，记 $E_x(w)$ 为字母 $x$ 的正次数减负次数，置 $E(w) = (E_x(w))$。则

$$F(X)^{\mathrm{ab}} \cong \mathbb{Z}^{(X)}.$$

若 $P = \langle X \mid R \rangle$，则

$$P^{\mathrm{ab}} \cong \mathbb{Z}^{(X)} / \langle E(r) : r \in R \rangle,$$

右侧分母为加法子群，无需再取共轭。

证明. 消去一对互逆字母不改变任一指数和，所以 $E$ 在 $F(X)$ 上有定义，连接使指数和相加，故 $E$ 是同态；每个坐标单位向量是某个生成元的像，所以它满射。目标交换，故 $F(X)' \subseteq \ker E$，诱导满同态

$$\bar{E} : F(X)/F(X)' \to \mathbb{Z}^{(X)}.$$

反方向定义 $(m_x)\mapsto\prod_x \bar{x}^{m_x}$。支撑有限保证乘积有限，商群交换保证次序无关。坐标加法对应幂相加，故它是同态。与 $\bar{E}$ 的两复合分别固定所有坐标单位向量和所有 $\bar{x}$，于是分别恒等，得到第一个同构。

令 $N=\langle\langle R\rangle\rangle \trianglelefteq F(X)$。商映射 $q:F(X)\to F(X)/N$ 把交换子送到对应像的交换子，所以 $q(F(X)')\subseteq P'$；反过来，$P$ 中每个交换子可提升为 $F(X)$ 中某个交换子的像，所以 $P'=q(F(X)')$。因此

$$P/P'\cong F(X)/(F(X)'N).$$

在 $E$ 下，一个共轭关系子的像为

$$E(uru^{-1})=E(u)+E(r)-E(u)=E(r).$$

由正规闭包的乘积公式，$E(N)$ 恰为 $E(r)$ 生成的加法子群。对第一个同构再取这一子群的商，便得到第二个公式。 □

**例 7.16.** 二面体群的三个关系子可取 $r^n, s^2, srs^{-1}r$，它们的指数和向量为 $(n,0),(0,2),(2,0)$。故

$$D_{2n}^{\mathrm{ab}}\cong\begin{cases}C_2, & n\text{ 奇},\\ C_2\times C_2, & n\text{ 偶}.\end{cases}$$

当 $n$ 奇，$n$ 与二生成全部整数，使第一坐标被消去；当 $n$ 偶，第一坐标只被模二。这也从表示式重新得到第二章的交换化计算。

## 7.6 Tietze 变换：更换表示而保持群

**命题 7.17** (两类基本变换)**.** *下列变换保持所表示的群，并给出固定原生成元像的同构。*

1. *若 $s\in\langle\langle R\rangle\rangle_{F(X)}$，可在 $\langle X\mid R\rangle$ 中加入关系子 $s$；反过来，若某关系子已属于其余关系子的正规闭包，可删除它。*
2. *若 $t\notin X$，$w\in F(X)$，可加入新生成元 $t$ 及关系 $t=w$。反过来，若有定义关系 $t=w$，且 $w$ 不含 $t$，可在其余全部关系中把 $t$ 替为 $w$、$t^{-1}$ 替为 $w^{-1}$，再删除 $t$ 和这个定义关系。*

*证明.* 第一类中，因 $s\in\langle\langle R\rangle\rangle$，包含 $R\cup\{s\}$ 的最小正规子群仍是 $\langle\langle R\rangle\rangle$，两个商完全相同。删除是这一论证的反向使用。

第二类先看加入。设 $P=\langle X\mid R\rangle$，$Q=\langle X,t\mid R,tw^{-1}\rangle$。将 $x\mapsto\bar{x}\in P$、$t\mapsto w(\bar{X})$，所有 $Q$ 的关系都成立，故得同态 $\alpha:Q\to P$。将 $x\in X$ 送到其在 $Q$ 中的像，得 $\beta:P\to Q$。$\alpha\beta$ 固定 $P$ 的每个生成元，故为恒等；$\beta\alpha$ 固定 $Q$ 中的每个 $x$，并把 $t$ 送到 $w(\bar{X})=t$，故也为恒等。

一般的消元情况写成 $Q=\langle X,t\mid tw^{-1},S(X,t)\rangle$，并令

$$P=\langle X\mid S(X,w)\rangle.$$

代入 $t=w$ 给出 $Q\to P$。反向把 $X$ 送入 $Q$，因 $t=w$，$S(X,w)$ 与 $S(X,t)$ 在 $Q$ 内求值相同，故确实给出 $P\to Q$。两复合在 $X$ 上恒等，在 $t$ 上使用定义关系后也恒等。于是同样得到所需同构。 □

**定理 7.18** (有限表示的 Tietze 定理)**.** 两个有限表示所给出的群同构，当且仅当一个表示可经有限次上述基本变换和生成元重命名变为另一个。

证明. 每步保持群，所以充分性成立。证明必要性。设

$$P = \langle X \mid R \rangle, \qquad Q = \langle Y \mid S \rangle,$$

并给定同构 $\phi : P \to Q$。先重命名使 $X, Y$ 不交。对每个 $y \in Y$ 选 $X$ 中词 $u_y$，使其在 $P$ 中的像为 $\phi^{-1}(\bar{y})$；对每个 $x \in X$ 选 $Y$ 中词 $v_x$，使其在 $Q$ 中的像为 $\phi(\bar{x})$。这些选择存在，因为两边分别由 $X, Y$ 生成；两集合有限，所以只有有限次选择。

从 $P$ 出发，加入全部 $y$ 与定义关系 $y = u_y(X)$，得到

$$P_1 = \langle X, Y \mid R(X),\ y = u_y(X)\ (y \in Y) \rangle.$$

按刚证命题，$P_1 \cong P$。在此识别下，$y$ 代表 $\phi^{-1}(\bar{y})$。因此 $S(Y)$ 的每个关系在 $P_1$ 中成立，$x = v_x(Y)$ 也在 $P_1$ 中成立。由表示的定义，“一个词在群中为单位元” 恰指它属于所列关系的正规闭包，所以可以逐个把这些关系加入，得到共同的较大表示

$$K = \langle X, Y \mid R(X),\ y = u_y(X),\ S(Y),\ x = v_x(Y) \rangle.$$

另一方面，从 $Q$ 加入全部 $x = v_x(Y)$，得到

$$Q_1 = \langle X, Y \mid S(Y),\ x = v_x(Y) \rangle \cong Q.$$

在 $Q_1$ 中，$R(X)$ 成立，因为把 $x$ 换为 $\phi(\bar{x})$ 后，它就是 $\phi$ 送来的关系。关系 $y = u_y(X)$ 也成立，因为 $\phi(u_y(\bar{X})) = \bar{y}$。所以 $K$ 中的 $R(X)$ 和 $y = u_y(X)$ 都是 $Q_1$ 的关系的后果，可以从 $K$ 逐个删除。剩下 $Q_1$，再利用 $x = v_x(Y)$ 消去全部 $X$，便回到 $Q$。

上述过程只添加或删除 $|X| + |Y| + |R| + |S|$ 所控制的有限个生成元与关系，因此变换次数有限。这里没有声称能从两个未附同构的表示自动找出这些词；证明使用了给定同构 $\phi$。 □

**例 7.19** (两个二阶生成元与二面体表示)**.** 从 $\langle a, b \mid a^2 = e, b^2 = e, (ab)^n = e \rangle$ 加入 $r = ab$。由 $a^2 = e$ 得 $b = ar$，消去 $b$ 后，$b^2 = e$ 成为

$$(ar)^2 = e \quad \Longleftrightarrow \quad ara = r^{-1}.$$

因此得到 $\langle r, a \mid r^n = e, a^2 = e, ara = r^{-1} \rangle$。把 $a$ 重命名为 $s$，就是前节的 $D_{2n}$ 表示。转换时保留了 $a^2 = e$，所以从 $arar = e$ 到 $ara = r^{-1}$ 的左右乘法均合法。

## 7.7 自由积及其交替正规形

**定义 7.20.** 群 $A, B$ 的自由积是带同态 $i_A : A \to A * B$、$i_B : B \to A * B$ 的群，使给定任意 $\alpha : A \to G$、$\beta : B \to G$，都有唯一同态 $A * B \to G$ 在两因子上分别等于 $\alpha, \beta$。与直积不同，定义没有要求两因子的像彼此交换。

**定理 7.21** (交替正规形)**.** 自由积存在，两个自然映射均为单射。每个元素唯一写成

$$g_1 \cdots g_k,$$

其中每个 $g_i$ 为 $A$ 或 $B$ 的非单位元，相邻 $g_i$ 来自不同因子。单位元对应唯一的空序列。

证明. 先对 $A, B$ 的全部元素引入互不混同的符号，并各自加入乘法表关系。由表示的泛性质，所得群 $P$ 带有 $A, B$ 到它的同态，且具有所述泛性质：两因子的任意同态恰使各乘法表关系成立，进而唯一延拓到 $P$。故存在性已得。

任意词可以先在每个因子内部把相邻字母相乘，删除单位元；每步缩短因子项数，所以最终得到一个交替序列。这只证明存在，还须证明不同序列给出不同元素。

令 $W$ 为所有这种交替序列，包括空序列。对 $a \in A$，定义 $L_a : W \to W$：$a = e$ 时为恒等；$a \neq e$ 时，若序列为空或首项来自 $B$，就在前面接 $a$；若首项为 $c \in A \setminus \{e\}$，就把首项改为 $ac$，当 $ac = e$ 时删去这一首项。余下首项来自 $B$ 或序列为空，所以操作后仍在 $W$ 中。对 $b \in B$ 定义同样的 $L_b$。

验证同一因子内 $L_a L_{a'} = L_{aa'}$。任一参数为单位元时等式由定义成立。以下设 $a, a' \neq e$。若序列为空或首项来自 $B$，$L_{a'}$ 先接上 $a'$，$L_a$ 再将其合并为 $aa'$，乘积为单位元时删除，正与 $L_{aa'}$ 一致。若序列为 $cw'$、$c \in A \setminus \{e\}$，分两支：

1. 若 $a'c \neq e$，两步把首项合并为 $a(a'c) = (aa')c$，为单位元时删除。若 $aa' = e$，该值为 $c$，于是原序列被恢复，也与 $L_e$ 一致。
2. 若 $a'c = e$，第一步得到 $w'$，它为空或以 $B$ 开头；第二步接上 $a$。另一方面 $(aa')c = a$。若 $aa' \neq e$，$L_{aa'}$ 直接把首项合并为 $a$；若 $aa' = e$，则 $a = c$，恒等操作所得 $cw' = aw'$ 也相同。

这证明 $A$ 中的乘法关系。$B$ 的论证逐项相同，只需交换两个因子的名称。特别地，$L_a^{-1} = L_{a^{-1}}$，所以各操作都是双射，给出 $A \to \mathrm{Sym}(W)$ 和 $B \to \mathrm{Sym}(W)$ 的同态。由 $P$ 的泛性质，它们合成同态 $P \to \mathrm{Sym}(W)$。

若 $g_1 \cdots g_k$ 是交替序列，相应置换 $L_{g_1} \cdots L_{g_k}$ 作用在空序列上时，从最右边开始，依次把 $g_k, \ldots, g_1$ 接到前端；相邻因子不同，不发生合并，最后恰得原序列。因此两个交替序列若在 $P$ 中相等，对空序列的像也相等，迫使序列逐项相同。这证明唯一性。单项的非单位序列不能等于空序列，所以两因子到 $P$ 的映射均单射。 □

**推论 7.22.** 若 $A = \langle X \mid R \rangle$、$B = \langle Y \mid S \rangle$，且符号集 $X, Y$ 不交，则

$$A * B \cong \langle X \sqcup Y \mid R \cup S \rangle.$$

特别地，$F(X) * F(Y) \cong F(X \sqcup Y)$。

证明. 任意群中满足 $R \cup S$ 的赋值恰分成满足 $R$ 的 $X$ 赋值与满足 $S$ 的 $Y$ 赋值，即分别给出 $A, B$ 的同态。两种对象因而有相同泛性质；按定理7.5之后的双向复合证明，它们唯一同构。取 $R = S = \varnothing$ 得最后的结论。 □

**例 7.23** (有限阶生成元可以生成无限群)**.** 若 $A, B$ 都非平凡，选 $a \in A \setminus \{e\}$、$b \in B \setminus \{e\}$。$(ab)^k$ 对每个 $k \geq 1$ 都是长度 $2k$ 的交替正规形，所以 $ab$ 有无限阶；即使 $a, b$ 各自阶有限，这一结论仍成立。

对 $C_2 * C_2 = \langle a, b \mid a^2 = b^2 = e \rangle$，令 $r = ab, s = a$。交替正规形保证 $r$ 有无限阶；同时 $s^2 = e$ 且 $srs = r^{-1}$。每个交替词可改写为 $r^j$ 或 $r^j s$：偶数长度的词为 $(ab)^k$ 或 $(ba)^k = r^{-k}$；奇数长度的词为 $(ab)^k a = r^k s$ 或 $(ba)^k b = r^{-k-1} s$，后式使用 $b = ar = r^{-1} s$。两种形的乘法因此给出

$$C_2 * C_2 \cong \mathbb{Z} \rtimes C_2,$$

其中二阶元在 $\mathbb{Z}$ 上取负。这是无限二面体群。映射到半直积坐标的满同态与反向的 $r, s$ 赋值固定生成元，故确为同构。

**命题 7.24** (自由积中有限阶元素的位置)**.** *$A * B$ 的每个有限阶非单位元都共轭于某个因子的元素。*

*证明.* 设交替正规形为 $w = g_1 \cdots g_k$。若 $k \le 1$，已在因子中。若 $k \ge 2$ 且首尾属于不同因子，连接 $w$ 的任意正整数份时，每个接缝仍交替，所以 $w^m$ 长度为 $mk > 0$，它有无限阶。

若 $k \ge 2$ 且首尾同因子，则 $k$ 必为奇数，故 $k \ge 3$。共轭变为

$$g_1^{-1} w g_1 = g_2 \cdots g_k g_1.$$

合并最后两个同因子项；若乘积非单位，长度由 $k$ 减为 $k-1$；若乘积为单位，删除它们，长度减为 $k-2$。其余相邻项仍交替。不断重复这种缩短，有限次后得到长度至多一，或首尾属于不同因子的正规形。后一情况有无限阶，而共轭保持元素阶，所以有限阶非单位元只能落到前一情况的单项。 □

## 7.8 边路径与生成树：只用组合定义

下面只使用图的顶点、边和有限路径，不预设基本群或覆盖空间。图允许重边与自环；端点相同不表示边相同。每条几何边有两个形式方向 $e, \bar{e}$，满足 $\bar{\bar{e}} = e$，且 $e \ne \bar{e}$；自环的两个方向也须区别。记有向边的起点、终点为 $o(e), t(e)$，有 $o(\bar{e}) = t(e)$。

边路径 $p = e_1 \cdots e_k$ 要求 $t(e_i) = o(e_{i+1})$。允许各顶点处的空路径。逆路径为 $\bar{e}_k \cdots \bar{e}_1$。相邻 $e\bar{e}$ 可以删除，这保持路径的起终点。约化词唯一性的算法与证明原样适用：把每个互逆边对作为一对形式字母，且每次消去后路径仍合法。因此任意路径有唯一不回走的约化路径。

**定义 7.25.** 图连通，指任意两个顶点间都有有限边路径。连通图称为树，若从任一顶点出发的非空闭路径都能消去至少一对相邻互逆边；等价地，没有非空约化闭路径。包含原图全部顶点的树子图称为生成树。

**引理 7.26.** *树中任意两顶点间有唯一约化路径。任意连通图有生成树。在一般无限图的存在性证明中，我们使用选择公理；有限图不需要无限选择。*

*证明.* 在树中，连通性给出路径，约化后仍连接同样端点。若 $p, q$ 是同端点的约化路径，则 $pq^{-1}$ 是闭路径，其约化必须为空，否则违反树的定义。把 $p, q$ 当作有向边字母的约化词，$R(pq^{-1}) = \epsilon$ 给出它们在相应自由群中相等；唯一约化词定理于是使 $p = q$。

现在在连通图 $\Gamma$ 固定基点 $v_0$。对每个顶点 $v$ 定义 $d(v)$ 为从 $v_0$ 到 $v$ 的路径长度的最小值。连通性使这些长度组成非空的非负整数集，所以最小值存在。对每个 $v \ne v_0$，选一条从 $v$ 到某个距离为 $d(v)-1$ 顶点的边，称为 $v$ 的父边。这样的边存在：最短路径的倒数第二个顶点距离必须为 $d(v)-1$，否则会有更短路径。取全部父边及全部顶点为 $T$。不断沿父边行进使距离每次减少一，恰在 $d(v)$ 步后到基点，所以 $T$ 连通。

证明 $T$ 中没有非空约化闭路径。若有，从中取长度最短者 $p$。如果 $p$ 首尾两边互逆，剥去它们后是一个较短闭路径，其内部仍约化；所得路径不可能为空，因为原路径长二时已含相邻互逆边。因此最短性迫使首尾也不互逆。把 $p$ 的顶点按环状顺序观察，在其中选距离 $d$ 最大的顶点 $v$。$T$ 的每条边都连接距离相差一的两个顶点，故 $v$ 在环中的两个邻点距离都是 $d(v)-1$。但 $v$ 只选了一条通往低一层的父边；其他顶点所选的、连接到 $v$ 的父边都是从高一

层下来。所以这两次经过必是同一父边的相反方向，在环上立即回走，与 $p$ 在环状首尾处也不回走矛盾。因此 $T$ 是生成树。 □

**命题 7.27** (Cayley 图是一棵树)**.** *以 $F(X)$ 的元素为顶点，对每个 $g \in F(X), x \in X$ 放一条标 $x$ 的有向边 $g \to gx$，并给其逆方向标 $x^{-1}$。所得 Cayley 图是树。*

*证明.* 任意约化词 $\ell_1 \cdots \ell_k$ 给出从 $e$ 到它的逐字路径，所以图连通。从任一顶点出发，给定一个字母都有唯一标该字母的出边：正字母用所定义的边，负字母 $x^{-1}$ 用 $gx^{-1} \to g$ 的逆方向。因此相邻两步的标签互逆，当且仅当它们是同一条边的两个相反方向。

若有非空约化闭路径，从 $g$ 出发，标签组成非空约化词 $w$。闭合给出 $gw = g$，在群中左消去 $g$ 得 $w = e$，与非空约化词不等于空词矛盾。故无这种闭路径，图为树。 □

## 7.9 陪集图与闭路径群

**定义 7.28.** 设 $H \leq F(X)$。定义 Schreier 陪集图 $\Gamma_H$：顶点为右陪集 $Hg$；对每个顶点 $Hg$ 和每个 $x \in X$，放置一条正向边

$$(Hg, x) : Hg \longrightarrow Hgx,$$

逆边标 $x^{-1}$。边由“起点陪集、正标签”这对数据区分；即使端点相同，也不能合并不同边。基点取 $H$。

若 $Hg = Hg'$，存在 $h \in H$ 使 $g' = hg$，从而 $Hg'x = Hhgx = Hgx$，所以终点定义不依赖代表元。每个顶点有唯一的 $x$ 出边和唯一的 $x$ 入边，后者来自 $Hgx^{-1}$；这也保证从任意顶点读任意字母的路径唯一。对词 $w$，从 $Hg$ 读它的终点是 $Hgw$。特别地，图连通，因为从 $H$ 读 $g$ 就到 $Hg$。

固定顶点 $v_0$，把从 $v_0$ 出发并回到 $v_0$ 的路径，按插入、删除相邻 $e\bar{e}$ 视为等价；每类有唯一约化路径。以路径连接后约化为乘法，得到群 $\Pi(\Gamma, v_0)$。结合律、空路径与逆路径的验证完全由式(7.1)给出，且所有被连接的路径起终点相容。这里约定路径乘积先走左边一条，再走右边一条；它与路径标签词的书写次序一致。

**命题 7.29.** *读取标签给出群同构*

$$\lambda : \Pi(\Gamma_H, H) \xrightarrow{\sim} H.$$

*证明.* 闭路径的标签 $w$ 满足 $Hw = H$，等价于 $w \in H$。插入或删除一对互逆边只在标签词中插入或删除互逆字母，所以求出的自由群元素不变；连接路径对应词相乘，故 $\lambda$ 良定义且为同态。任意 $h \in H$ 的词从 $H$ 读起后回到 $H$，所以满射。

若一条闭路径标签在自由群中为 $e$,其标签词可以消去到空词。每当两个相邻标签为 $x, x^{-1}$ 或 $x^{-1}, x$ 时，唯一出边性质保证路径的这两步恰是同一边的相反方向，所以相同消去也能在边路径上实行。最终路径消为空路径，故原闭路径类为单位元。核平凡，得到单射。 □

## 7.10 生成树给出的自由基与 Nielsen–Schreier 定理

**定理 7.30** (图的闭路径群的显式自由基)**.** 设 $\Gamma$ 连通，固定基点 $v_0$ 和生成树 $T$。对每个顶点 $v$，记 $p_v$ 为 $T$ 中从 $v_0$ 到 $v$ 的唯一约化路径。对 $T$ 外的每条几何边选一个方向 $e$，令

$$\gamma_e = [p_{o(e)}\, e\, p_{t(e)}^{-1}].$$

则这些 $\gamma_e$ 构成 $\Pi(\Gamma, v_0)$ 的自由基。

证明. 记所选的非树有向边集为 $E_0$，为每个 $e \in E_0$ 引入自由字母 $z_e$。定义边的编码：树边的两个方向都编码为空词；$e \in E_0$ 编为 $z_e$，$\bar{e}$ 编为 $z_e^{-1}$。一条路径的编码是依次连接所有边编码后在 $F(\{z_e : e \in E_0\})$ 中求值。

相邻 $f\bar{f}$ 的编码或都为空，或为互逆字母，所以删除它们不改变编码。因此编码在闭路径类上给出同态

$$\Psi : \Pi(\Gamma, v_0) \to F(\{z_e : e \in E_0\}).$$

由自由群的泛性质，赋值 $z_e \mapsto \gamma_e$ 给出反向同态 $\Phi$。$p_{o(e)}$ 和 $p_{t(e)}$ 都只走树边，所以 $\Psi(\gamma_e) = z_e$。因此 $\Psi\Phi$ 固定所有自由生成元，是恒等。

还须证明 $\Phi\Psi$ 也是恒等，这一步同时承担“所列闭路径生成全部闭路径”的责任。给定闭路径 $q = f_1 \cdots f_k$，设依次经过顶点 $v_0, v_1, \ldots, v_k = v_0$。有

$$[q] = \prod_{i=1}^{k} [p_{v_{i-1}} f_i p_{v_i}^{-1}].$$

因为相邻因子之间的 $p_{v_i}^{-1} p_{v_i}$ 消为空路径，而开头和末尾的 $p_{v_0}$ 本身为空路径，乘积就恢复 $q$。

若 $f_i$ 是树边，$p_{v_{i-1}} f_i p_{v_i}^{-1}$ 是树中闭路径，约化后只能为空，所以该因子为单位元。若 $f_i = e \in E_0$，该因子是 $\gamma_e$。若 $f_i = \bar{e}$，其路径恰为 $p_{t(e)} \bar{e} p_{o(e)}^{-1}$，是定义 $\gamma_e$ 的路径的逆，故因子为 $\gamma_e^{-1}$。所以右侧正是先取编码再施 $\Phi$ 的结果，即 $\Phi\Psi([q]) = [q]$。

两个同态互逆。特别地，任何由 $\gamma_e^{\pm 1}$ 构成的非空约化词，其 $\Psi$ 像为对应 $z_e^{\pm 1}$ 的非空约化词，不会为单位元。这既证明生成性，也证明没有额外关系。 □

**推论 7.31** (Nielsen–Schreier)**.** 自由群的任意子群仍为自由群。更具体地，取 $\Gamma_H$ 的生成树 $T$，对每条正向非树边

$$e : (Ht) \xrightarrow{x} (Hu)$$

令 $t, u$ 为树路径 $p_{Ht}, p_{Hu}$ 的标签，则

$$s_e = txu^{-1} \tag{7.2}$$

构成 $H$ 的自由基。

证明. 图连通，故由引理7.26有生成树。定理7.30给出闭路径群的自由基，命题7.29把该群同构到 $H$。闭路径 $p_{Ht} e p_{Hu}^{-1}$ 的标签正是 $txu^{-1}$，所以其像给出所列自由基。

每条几何边都有唯一被定义为正向的方向，故可以统一选择这个方向，而不额外选择定向。对于树边，同样公式的值为 $e$；对于非树边，定理保证它非单位元，且不同非树边所得元素不会重复，否则两个自由生成元就有关系。 □

## 7.11 逐字重写公式与有限指数的秩

对每个陪集 $Hg$，记树路径的标签为 $\tau(Hg)$，特别地 $\tau(H)=e$。它是该陪集的一个代表，因为从 $H$ 读到的终点为 $H\tau(Hg)=Hg$。若树路径读过某个前缀，它仍是通往途中顶点的唯一树路径，故这些代表形成前缀封闭的词集。

设 $h=\ell_1\cdots\ell_k\in H$，置

$$t_i=\tau(H\ell_1\cdots\ell_i),\qquad t_0=t_k=e.$$

不必要求原来给出的 $h$ 的词约化。群内有望远镜式乘积

$$h=\prod_{i=1}^{k}t_{i-1}\ell_i t_i^{-1}. \tag{7.3}$$

右侧相邻的 $t_i^{-1}t_i$ 全部抵消，留下原词，故此式逐项成立。若 $\ell_i=x\in X$，该因子是相应正向边的 $s_e$；若 $\ell_i=x^{-1}$，则对应正向边从 $Ht_i$ 读 $x$ 到 $Ht_{i-1}$，其基元为 $t_ixt_{i-1}^{-1}$，而

$$t_{i-1}x^{-1}t_i^{-1}=(t_ixt_{i-1}^{-1})^{-1}.$$

树边的因子为单位元，非树边给出自由基元或其逆。这就是直接计算子群自由词的重写方法。

**定理 7.32** (Schreier 指数–秩公式)**.** *若 $F_r=F(\{x_1,\dots,x_r\}),1\le r<\infty$，且 $[F_r:H]=d<\infty$，则*

$$\operatorname{rank}H=1+d(r-1).$$

*这里秩为自由基的元素数。*

*证明.* 陪集图有 $d$ 个顶点。每个顶点、每个正生成元给出一条正向边，共 $dr$ 条几何边；自环仍算一条，重边分别计数，逆方向不另计。生成树恰有 $d-1$ 条几何边。证明这一计数：在树 $T$ 本身上实行引理7.26的父边构造，得到包含全部顶点的子树 $T_0\subseteq T$。每个非根顶点选一条父边，不同顶点的父边不同，因为一条边只有距离较远的端点能把它选为父边。因此 $T_0$ 有 $d-1$ 条边。若 $T$ 还有一条 $T_0$ 外的边 $e$，先沿 $e$，再沿 $T_0$ 中连接两端点的约化路径走回，便得非空约化闭路径：后一路径不含 $e$，所以在两个接缝都不会与 $e$ 消去；它内部本来就约化。这违反 $T$ 为树。因此 $T=T_0$，树边数确为 $d-1$。

非树边因此有 $dr-(d-1)=1+d(r-1)$ 条，正是前一定理给出的自由基大小。还须确认这个有限数不依赖自由基的选择。由命题7.15，若自由基大小为 $m$，交换化为 $\mathbb{Z}^m$，再模去全部二倍元素得到有 $2^m$ 个元素的 $\mathbb{F}_2$ 向量空间。不同有限 $m$ 给出不同的基数，而无限自由基的对应向量空间包含无限多个不同的坐标单位向量，不可能有有限基数。因此有限自由基的大小是群本身确定的不变量，所算数值确为秩。 □

当 $r=1$ 时公式给出秩一，与 $\mathbb{Z}$ 的非零有限指数子群都是 $d\mathbb{Z}$ 一致。若 $r\ge2$，有限指数子群的秩可以大于母群的秩；“子群需要的生成元不会更多”对于非交换群并不成立。

## 7.12 一个二指数子群：自由基与实际重写

设 $F=F(a,b)$，同态 $\eta:F\to C_2$ 由

$$\eta(a)=1,\qquad \eta(b)=0$$

给定，令 $H=\ker\eta$。由于 $\eta$ 满射，$F/H\cong C_2$，所以陪集恰为 $H, Ha$。图中每个顶点上的 $b$ 边是自环；两条正向 $a$ 边分别从 $H$ 到 $Ha$、从 $Ha$ 到 $H$，它们是不同几何边，而不是同一边的两个方向。

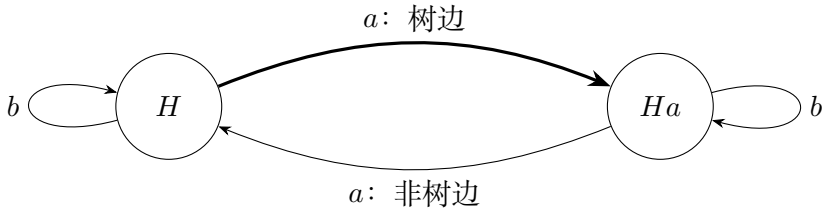



图 7.2: 两顶点、四条几何边；粗边构成生成树，余下三边给出三个自由基元。

选 $H\to Ha$ 的 $a$ 边为树，代表为 $e, a$。三个非树边依次给出

$$u=a^2,\qquad v=b,\qquad c=aba^{-1}.$$

例如从 $Ha$ 读 $a$ 回到 $H$，式(7.2)给出 $a\cdot a\cdot e^{-1}=a^2$；$Ha$ 上的 $b$ 自环给出 $aba^{-1}$。因此 $H$ 是以 $u, v, c$ 为自由基的三秩自由群，而不仅是由这三者生成。

对 $h=abab^{-1}a^{-1}a^{-1}$，逐字用式(7.3)计算：

| $i$ | $\ell_i$ | $t_{i-1}$ | $t_i$ | $t_{i-1}\ell_i t_i^{-1}$ |
|---|---|---|---|---|
| 1 | $a$ | $e$ | $a$ | $e$ |
| 2 | $b$ | $a$ | $a$ | $c$ |
| 3 | $a$ | $a$ | $e$ | $u$ |
| 4 | $b^{-1}$ | $e$ | $e$ | $v^{-1}$ |
| 5 | $a^{-1}$ | $e$ | $a$ | $u^{-1}$ |
| 6 | $a^{-1}$ | $a$ | $e$ | $e$ |

所以 $h=cuv^{-1}u^{-1}$。将右侧代回原字母，

$$(aba^{-1})a^2b^{-1}a^{-2}=abab^{-1}a^{-1}a^{-1},$$

与原词一致。这一次重写中，第五步是逆向走非树 $a$ 边，故产生 $u^{-1}$；它不能误按“当前代表乘负字母”直接读成一个新基元。

**例 7.33** (任意有限循环商的核)**.** 令 $r\ge 1, d\ge 1$，同态 $\eta: F(x_1,\dots,x_r)\to C_d$ 把 $x_1$ 送到 1，把其他生成元送到 0。核的陪集图有顶点 $H, Hx_1,\dots,Hx_1^{d-1}$，$x_1$ 边组成有向 $d$ 环，其他标签在各顶点成自环。取 $d$ 环中前 $d-1$ 条边为树，树代表为 $e, x_1,\dots,x_1^{d-1}$。所有非树边给出的自由基为

$$\{x_1^d\}\ \cup\ \{x_1^j x_i x_1^{-j} : 0\le j<d,\ 2\le i\le r\}.$$

第一项来自环的闭合边；其余来自各自环。非树边无一遗漏，所以这正是自由基，共 $1+d(r-1)$ 个。$d=1$ 时树没有边，上式恢复原自由基。

## 7.13 二生成元自由群的导出群为何有无限秩

**定理 7.34.** *$F=F(a,b)$ 的导出群 $F'$ 是可数无限秩自由群。它有显式自由基*

$$c_{m,n}=a^m b^n a b^{-n} a^{-m-1},\qquad m\in\mathbb{Z},\ n\in\mathbb{Z}\setminus\{0\}. \tag{7.4}$$

特别地，有限生成群的子群未必有限生成，有限生成群的导出群也未必有限生成。

证明. 由命题7.15，指数和同态

$$E : F \to \mathbb{Z}^2, \qquad a \mapsto (1,0), \quad b \mapsto (0,1)$$

的核恰为 $F'$。因此其右陪集由 $(m,n) \in \mathbb{Z}^2$ 标记，陪集图为整数格点图：正向 $a$ 边 $(m,n) \to (m+1,n)$，正向 $b$ 边 $(m,n) \to (m,n+1)$。

取生成树 $T$ 为所有竖边，加上水平轴 $n=0$ 上的全部横边。从原点到 $(m,n)$ 的树路径先沿水平轴走到 $(m,0)$，再竖走到 $(m,n)$，标签为 $a^m b^n$，其中负指数表示沿相应逆边行走。这些路径证明连通性。

还要验证没有非空约化闭路径。反设有，取长度最短的一条。如引理7.26的证明，最短性使它在环状首尾处也不回走。若路径经过非零高度，在所有经过的顶点中取 $|n|$ 最大者 $(m,n)$。此处没有横边，而沿竖线走向远离零的一侧会增大 $|n|$，违背最大性；所以进入和离开都必须使用朝零的一条竖边，方向相反，产生立即回走。若所有顶点高度为零，则路径全在水平轴；取横坐标最大的顶点，两侧邻点都必须是它左边的同一顶点，又使用同一条边回走。两种情况都矛盾，因此 $T$ 确为树。

非树边恰为高度 $n \neq 0$ 的正向横边。对这样的边，起点和终点的树代表分别为 $a^m b^n$、$a^{m+1} b^n$。由式(7.2)，对应基元为

$$(a^m b^n)\, a\, (a^{m+1} b^n)^{-1} = a^m b^n a b^{-n} a^{-m-1} = c_{m,n}.$$

Nielsen–Schreier 的显式基定理保证它们自由生成 $F'$。下标集合 $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ 是可数无限集，所以基可数无限。

最后证明这个群确实不能另由有限个元素生成。由自由基的交换化公式，$F'/F''$ 是以所有 $c_{m,n}$ 对应坐标为基的自由交换群。若取其中有限多个元素，它们的支撑的并仍有限，因此其整数线性组合不能得到这一并集外的任何坐标单位向量。所以该交换群不可能有限生成。一个有限生成群的任何商都由有限个生成元的像生成，故 $F'$ 本身也不可能有限生成。 □

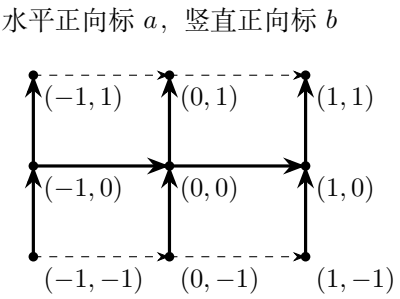



图 7.3: 整数陪集图的局部。完整图向四方无限延伸，所有非零高度的横边均在树外。

## 7.14 有限置换模型分离非平凡词

**定义 7.35.** 群 $G$ 称为剩余有限群，若对每个 $g \neq e$，存在有限群 $Q$ 及同态 $\rho : G \to Q$，使 $\rho(g) \neq e$。等价地，所有有限指数正规子群的交为 $\{e\}$。

等价性的证明如下。给定 $\rho$，其核正规，且 $G/\ker\rho \cong \operatorname{im}\rho$ 有限，故核为不含 $g$ 的有限指数正规子群。反过来，不含 $g$ 的有限指数正规子群 $N$ 给出有限商 $G/N$，自然映射的 $g$ 像不平凡。

**定理 7.36.** *任意自由群 $F(X)$ 都剩余有限。更精确地，长度 $L \geq 1$ 的非空约化词可以在 $S_{L+1}$ 中取得非单位像。*

*证明.* 设 $w = \ell_1 \cdots \ell_L$ 为约化词。目标置换按本册惯例从右向左作用，因此按相反次序记

$$d_j = \ell_{L+1-j} \qquad (1 \leq j \leq L).$$

在有限集合 $\Omega = \{0, 1, \ldots, L\}$ 上，对每个生成元 $x$ 规定一个部分映射 $\sigma_x$：若 $d_j = x$，规定

$$\sigma_x(j-1) = j;$$

若 $d_j = x^{-1}$，规定

$$\sigma_x(j) = j - 1.$$

其余点暂不规定。

必须证明这些规定对每个 $x$ 都构成部分单射。来源于不同位置、且同为正字母的规定，定义点与像点分别为不同的 $j-1$ 与 $j$；同为负字母也分别为不同的 $j$ 与 $j-1$，所以各自没有冲突。正位置 $p$ 与负位置 $q$ 若有相同定义点，须 $p - 1 = q$，即相邻子串 $d_q d_p = x^{-1}x$，与反向词仍约化矛盾。它们若有相同像点，须 $p = q - 1$，即 $d_p d_q = xx^{-1}$，同样矛盾。于是所有定义点不同、所有像点不同，规定确为从某子集 $D_x$ 到某子集 $I_x$ 的双射。

$|D_x| = |I_x|$，故补集 $\Omega \setminus D_x$ 与 $\Omega \setminus I_x$ 同基数。按自然数递增顺序逐一配对，就把部分映射延拓为整个 $\Omega$ 的置换 $\sigma_x$。未出现的生成元取恒等置换；实际出现的生成元有限，所以不涉及无限选择。由自由群泛性质，$x \mapsto \sigma_x$ 给出同态

$$\rho : F(X) \to \operatorname{Sym}(\Omega) \cong S_{L+1}.$$

若 $d_j = x$，按规定 $\rho(d_j)(j-1) = j$；若 $d_j = x^{-1}$，规定 $\sigma_x(j) = j-1$ 等价于 $\rho(d_j)(j-1) = \sigma_x^{-1}(j-1) = j$。于是

$$0 \xmapsto{\rho(\ell_L)} 1 \xmapsto{\rho(\ell_{L-1})} 2 \longmapsto \cdots \xmapsto{\rho(\ell_1)} L.$$

所以 $\rho(w)(0) = L \neq 0$，$\rho(w)$ 不是恒等置换。目标群有限，结论成立。 □

**例 7.37** (分离交换子而不靠交换商)**.** 取 $w = aba^{-1}b^{-1}$，它的所有指数和都为零，故在任何交换商中像都是单位元。但上述构造取反向字母 $b^{-1}, a^{-1}, b, a$，可在 $\{0,1,2,3,4\}$ 上用

$$\sigma_a = (0\ 3\ 4\ 2\ 1), \qquad \sigma_b = (0\ 1)(2\ 3)$$

完成所需部分置换，其中 $\sigma_b$ 固定四。逐点检查：$\sigma_b(1) = 0$、$\sigma_a(2) = 1$、$\sigma_b(2) = 3$、$\sigma_a(3) = 4$，对应四条规定。因而

$$0 \xmapsto{\sigma_b^{-1}} 1 \xmapsto{\sigma_a^{-1}} 2 \xmapsto{\sigma_b} 3 \xmapsto{\sigma_a} 4.$$

交换子在这一有限非交换商中被分离。这同时说明，仅计算交换化不能识别全部非平凡词。

## 7.15 有限生成、Hopf 性与本章接口

**定义 7.38.** 群 $G$ 称为 Hopf 群，若它的每个满自同态 $G \to G$ 都是同构。

**引理 7.39.** *若 $G$ 有有限生成集，则对每个正整数 $m$，$G$ 只有有限个指数为 $m$ 的子群。*

*证明.* 设 $G$ 由 $r$ 个元素生成。到有限群 $S_m$ 的同态由这 $r$ 个生成元的像决定，所以最多有 $(m!)^r$ 个。若 $H \le G$ 指数为 $m$，则 $G$ 在左陪集 $G/H$ 上左乘，选一个把陪集 $H$ 标为一点的编号，得到某个同态 $G \to S_m$。$H$ 正是该点稳定子的原像。每个同态至多给出 $m$ 个点稳定子原像，所以所有这样的 $H$ 总数至多 $m(m!)^r$，因而有限。 □

**定理 7.40.** *有限生成的剩余有限群都是 Hopf 群。因此有限秩自由群都是 Hopf 群。*

*证明.* 设 $\phi : G \to G$ 满射。若它不单射，选 $k \in \ker\phi \setminus \{e\}$。剩余有限性给出有限指数正规子群 $N \trianglelefteq G$，使 $k \notin N$。记 $[G:N] = m$。对 $i \ge 0$ 令

$$N_i = \phi^{-i}(N).$$

因 $\phi^i$ 满射，映射

$$G/N_i \longrightarrow G/N, \qquad gN_i \longmapsto \phi^i(g)N$$

良定义、满射且核平凡，所以是同构，$[G:N_i] = m$。由引理7.39，这些子群中有 $N_i = N_j$，其中 $0 \le i < j$。

对任意 $g \in G$，满射性给出 $a \in G$ 使 $\phi^i(a) = g$。于是

$$\begin{aligned} g \in N &\iff a \in \phi^{-i}(N) = N_i \\ &\iff a \in N_j \\ &\iff \phi^{j-i}(g) \in N. \end{aligned}$$

所以 $N = \phi^{-(j-i)}(N)$。但 $\phi(k) = e$ 且 $j - i \ge 1$，故 $\phi^{j-i}(k) = e \in N$，上式迫使 $k \in N$，矛盾。因此 $\ker\phi = \{e\}$，满自同态为同构。有限秩自由群有限生成，上一节证明它剩余有限，所以满足结论。 □

带合并自由积、HNN 扩张与 Britton 引理、一般 Reidemeister–Schreier 关系重写、群作用于树的结构定理，以及字问题不可判定性，尚未在本章建立，留待进一步的组合群论专题。本章对子群的完整自由基证明不依赖这些更深定理。

## 文献说明

自由群与表示式部分核读 Milne，*Group Theory*，Version 4.01 (2025)，第 31–37 页，命题 2.1–2.3、注 2.4、推论 2.5、定理 2.6 及命题 2.8、例 2.9–2.11；其中第 34 页只陈述子群自由和指数–秩公式，并未给证明，本章没有把这一陈述当作证明使用。

图的生成树和自由基路线另核读 Hatcher，*Algebraic Topology*，§1.A，第 84–86 页，命题 1A.1–1A.2、定理 1A.4；该作者公开单章 PDF 中分别为物理 64–66 页。导出群与剩余有限性的方向参看同节第 86 页习题 6、第 87 页习题 10–11（单章 PDF 物理 66–67 页）。本章把拓扑语言改写为边路径的组合论证，重新证明生成树、路径编码、子群同构及有限置换延拓，因而不预设基本群、同伦或覆盖空间。Tietze 变换、自由积的置换正规形与 Hopf 性亦在正文给出完整证明，结论均属标准群论，不主张结果原创。

# 8 有限群结构工具：Frattini、Fitting 与 Hall 理论

第六章的逐阶分类依赖 Sylow 理论和具体作用；第八章把其中反复出现的结构机制抽出来。第一部分研究 “哪些元素可以从生成集里删掉”，得到 Frattini 子群和 Burnside 基定理。第二部分把所有正规幂零子群合并成 Fitting 子群。第三部分在可解有限群中建立 Hall 子群的存在与共轭，最后证明正规 Hall 子群的分裂与补群共轭。每个定理都明确标出有限性、可解性和互素条件；这些条件不能在后续应用中无声省略。

## 8.1 Frattini 子群与非生成元

**定义 8.1.** 设 $G$ 为群。所有极大真子群的交称为 $G$ 的 Frattini 子群，记为

$$\Phi(G) = \bigcap_{M \max G} M.$$

若 $G$ 没有极大真子群，约定 $\Phi(G) = G$。元素 $x \in G$ 称为非生成元，若对任意子集 $S \subseteq G$，只要 $\langle S, x\rangle = G$，就已经有 $\langle S\rangle = G$。

**引理 8.2.** *有限群的每个真子群都包含在某个极大真子群中。因此有限群的 Frattini 子群是特征子群。*

*证明.* 若 $H < G$，考虑包含 $H$ 的真子群集合。它是有限集合，按阶取阶最大的成员 $M$。若 $M < K < G$，则 $|K| > |M|$，矛盾，所以 $M$ 极大。

任意自同构把极大真子群送到极大真子群。因此它把所有极大真子群的交送回自身，得到 $\alpha(\Phi(G)) = \Phi(G)$。 □

**定理 8.3** (Frattini 判据)**.** *对有限群 $G$ 和元素 $x \in G$，以下条件等价：*

1. *$x$ 是非生成元；*
2. *$x \in \Phi(G)$。*

*证明.* 先设 $x \in \Phi(G)$，且 $\langle S, x\rangle = G$。若 $\langle S\rangle \neq G$，由引理取一个包含它的极大真子群 $M$。由于 $x \in \Phi(G) \subseteq M$，便有 $\langle S, x\rangle \subseteq M < G$，矛盾。因此 $\langle S\rangle = G$，$x$ 是非生成元。

反过来设 $x \notin \Phi(G)$。按交的定义，存在极大真子群 $M$ 使 $x \notin M$。因为 $M$ 极大，$\langle M, x\rangle$ 严格包含 $M$，只能等于 $G$；但 $\langle M\rangle = M \neq G$。所以 $x$ 不是非生成元。 □

**推论 8.4.** *有限群 $G$ 的子集 $S$ 生成 $G$，当且仅当其像 $S\Phi(G)/\Phi(G)$ 生成商群 $G/\Phi(G)$。*

*证明.* 若 $\langle S\rangle = G$，商映射的像当然生成商群。反之，若 $S\Phi(G)/\Phi(G)$ 生成 $G/\Phi(G)$，则

$$\langle S, \Phi(G)\rangle = G.$$

若 $\langle S\rangle < G$，由引理存在极大真子群 $M$ 包含它；由于 $\Phi(G) \subseteq M$，商中 $S\Phi(G)/\Phi(G)$ 落在真子群 $M/\Phi(G)$ 内，不可能生成商群。故 $\langle S\rangle = G$。 □

**例 8.5.** 若 $n=\prod p_i^{a_i}$，则 $C_n$ 的极大子群为 $p_iC_n$，因而

$$\Phi(C_n)=\bigcap_i p_iC_n=\left(\prod_i p_i\right)C_n.$$

例如 $\Phi(C_{12})=6C_{12}=\{0,6\}$，而 $C_{12}/\Phi(C_{12})\cong C_6$。

## 8.2 有限 $p$ 群的 Frattini 子群

**引理 8.6.** *设 $P$ 为有限 $p$ 群。每个极大真子群 $M$ 都正规于 $P$，且 $[P:M]=p$。*

*证明.* 先证明有限 $p$ 群的正规化子条件：若 $H<P$，则 $H<N_P(H)$。对 $|P|$ 作归纳。$|P|=p$ 时，$H=1$，而 $N_P(1)=P$。对一般 $P\neq 1$，第三章已证 $Z(P)\neq 1$。若 $Z(P)\not\subseteq H$，取 $z\in Z(P)\setminus H$，则 $H<\langle H,z\rangle\le N_P(H)$。若 $Z(P)\subseteq H$，则 $|P/Z(P)|<|P|$，且 $H/Z(P)$ 为真子群。在 $P/Z(P)$ 中应用归纳，其正规化子的原像严格包含 $H$；由于 $Z(P)\le H$，等式 $g(H/Z(P))g^{-1}=H/Z(P)$ 等价于 $gHg^{-1}=H$，所以该原像就是 $N_P(H)$。因此条件成立。

对极大子群 $M$，正规化子条件给出 $M<N_P(M)\le P$，极大性迫使 $N_P(M)=P$，所以 $M\trianglelefteq P$。现在 $P/M$ 是非平凡 $p$ 群，并且没有非平凡真子群：任何这样的子群的原像都严格介于 $M$ 与 $P$ 之间。Cauchy 定理给出 $P/M$ 的阶 $p$ 子群，它只能等于整个 $P/M$。故 $[P:M]=p$。□

**定理 8.7** (Burnside 基定理)**.** *设 $P$ 为有限 $p$ 群，则*

$$\Phi(P)=P^p[P,P],$$

*其中 $P^p=\langle x^p:x\in P\rangle$，$[P,P]$ 为导出子群。因此 $P/\Phi(P)$ 是有限维 $\mathbb{F}_p$ 向量空间；若 $d(P)$ 表示 $P$ 的最小生成元数，则*

$$d(P)=\dim_{\mathbb{F}_p}P/\Phi(P).$$

*证明.* 令 $K=P^p[P,P]$。因为 $P^p$ 和 $[P,P]$ 都特征于 $P$，$K\trianglelefteq P$。在商群 $P/K$ 中，交换子和 $p$ 次幂都平凡，所以它是交换群且每个元素满足 $x^p=1$，即为 $\mathbb{F}_p$ 向量空间。

先证 $K\subseteq\Phi(P)$。由引理，每个极大子群 $M$ 正规且 $P/M$ 阶为 $p$，所以 $P/M\cong C_p$。它既交换又指数 $p$，故 $[P,P]\subseteq M$ 且 $P^p\subseteq M$。对所有极大 $M$ 取交，得 $K\subseteq\Phi(P)$。

反过来设 $x\notin K$。在向量空间 $V=P/K$ 中，$xK\neq 0$。取一个线性泛函 $\lambda:V\to\mathbb{F}_p$ 使 $\lambda(xK)=1$；把 $xK$ 扩充为一组基，再在该基上定义坐标投影。其核的逆像 $M$ 是 $P$ 的正规子群，且 $P/M\cong C_p$。因为 $x\notin M$，$M$ 是指数为 $p$ 的极大子群，于是 $x\notin\Phi(P)$。这证明反向包含，得到等式。

由 Frattini 判据，有限集 $S\subseteq P$ 生成 $P$ 当且仅当其像生成 $P/\Phi(P)$。向量空间的最小生成元数等于维数，故 $d(P)$ 等于该维数。□

**推论 8.8.** *有限 $p$ 群 $P$ 的子群 $H$ 等于 $P$，当且仅当 $H\Phi(P)=P$。特别地，若 $P$ 的元素 $x_1,\dots,x_d$ 在 $P/\Phi(P)$ 中构成基，则它们生成 $P$；任何生成集至少含 $d$ 个元素。*

*证明.* 若 $H\Phi(P)=P$，则商中 $H\Phi(P)/\Phi(P)$ 生成商群，故由 Frattini 判据 $H=P$。另一方向显然。□

**例 8.9** (阶 $p^3$ 群的最小生成元)**.** $C_{p^3}$ 的 Frattini 商为 $C_p$，所以最小生成元数为一。$C_{p^2}\times C_p$ 的 Frattini 商为 $C_p^2$，最小生成元数为二；$C_p^3$ 的 Frattini 子群为单位元，最小生成元数为三。这与第六章的三种交换模型一致。

## 8.3 生成组计数与自同构的线性化

**命题 8.10.** *设 $P$ 为有限 $p$ 群，$d=\dim_{\mathbb{F}_p} P/\Phi(P)$，$r\ge 0$。有序 $r$ 元生成组的数目为*

$$\begin{cases} 0, & r<d,\\ |\Phi(P)|^r\displaystyle\prod_{i=0}^{d-1}(p^r-p^i), & r\ge d. \end{cases}$$

*空乘积取一。因此 $P=1$ 时，对每个 $r\ge 0$ 都恰有一个有序 $r$ 元生成组。*

*证明.* 由 Burnside 基定理，$(x_1,\dots,x_r)$ 生成 $P$ 当且仅当其像生成 $V=P/\Phi(P)$。每个给定的商群 $r$ 元组都有 $|\Phi(P)|^r$ 个提升，且这些提升或者全生成 $P$，或者全不生成。

固定 $V$ 的一组基，把它的 $r$ 个向量写成一个 $d\times r$ 矩阵的列。列生成 $V$ 当且仅当矩阵的秩为 $d$，也即它的 $d$ 个行向量在 $\mathbb{F}_p^r$ 中线性无关。第一行有 $p^r-1$ 种选择；已选 $i$ 个独立行后，它们张成一个含 $p^i$ 个元素的子空间，下一行有 $p^r-p^i$ 种选择。因此独立行组数为 $\prod_{i=0}^{d-1}(p^r-p^i)$。若 $r<d$ 则不存在这样的矩阵。乘上提升数便得到结论。 □

**命题 8.11** (自同构作用的核)**.** *有限 $p$ 群 $P$ 的自同构在 Frattini 商上诱导同态*

$$\rho:\operatorname{Aut}(P)\longrightarrow \mathrm{GL}_d(\mathbb{F}_p).$$

*其核是 $p$ 群。因此 $\operatorname{Aut}(P)$ 的任何阶与 $p$ 互素的子群在 $P/\Phi(P)$ 上作用忠实。*

*证明.* $\Phi(P)$ 特征于 $P$，所以 $\rho$ 有定义。若 $P=1$，则 $\operatorname{Aut}(P)=1$，结论成立。以下设 $d\ge 1$，固定 $P/\Phi(P)$ 的有序基 $(\bar{x}_1,\dots,\bar{x}_d)$。记全部提升的集合为

$$\mathcal{X}=\{(x_1,\dots,x_d): x_i\Phi(P)=\bar{x}_i\}.$$

每个提升都生成 $P$，且 $|\mathcal{X}|=|\Phi(P)|^d$，是 $p$ 的幂。令 $K=\ker\rho$。由于 $K$ 在商上恒等，它逐坐标作用于 $\mathcal{X}$。若 $\alpha\in K$ 固定某个提升组，则它固定一组生成元。任意 $g\in P$ 都是这些生成元及其逆的乘积，故 $\alpha(g)=g$，即 $\alpha=\mathrm{id}$。所以每个稳定子都平凡，每个轨道的大小都是 $|K|$。轨道分割 $\mathcal{X}$，于是 $|K|\mid|\mathcal{X}|$，$K$ 为 $p$ 群。

若 $B\le\operatorname{Aut}(P)$ 且 $\gcd(|B|,p)=1$，则 $B\cap K$ 的阶既整除 $|B|$ 又是 $p$ 的幂，只能为一。因此 $\rho|_B$ 单射。 □

**注 8.12.** 一般不能把 $\rho$ 写成满射。例如 $P=C_{p^2}\times C_p$ 时，$P/\Phi(P)\cong\mathbb{F}_p^2$，但特征子群 $\{x\in P: x^p=1\}$ 在该商中的像是一条直线，每个诱导自同构都保持它；整个 $\mathrm{GL}_2(\mathbb{F}_p)$ 并不保持这条固定直线。具体地，用加法记号写 $P=\langle a\rangle\times\langle b\rangle$，$|a|=p^2$、$|b|=p$，则 $\Phi(P)=\langle pa\rangle$，上述像就是 $\langle b+\Phi(P)\rangle$。

## 8.4 Frattini 论证与有限 Frattini 子群的幂零性

**引理 8.13** (Frattini 论证)**.** 设 $G$ 为有限群，$N \trianglelefteq G$，$P$ 为 $N$ 的 *Sylow* $p$ 子群，则

$$G = N\,N_G(P).$$

这里的 *Frattini* 论证是一个关于正规子群中 *Sylow* 子群的结论，须与非生成元判据区分。

证明. 对 $g \in G$，正规性给出 $gPg^{-1} \le N$，其阶与 $P$ 相同，故也是 $N$ 的 Sylow $p$ 子群。由 $N$ 内的 Sylow 共轭性，存在 $n \in N$ 使

$$gPg^{-1} = nPn^{-1}.$$

因此 $n^{-1}g \in N_G(P)$，即 $g \in N\,N_G(P)$。反向包含因两个因子都属于 $G$ 而成立。 □

**定理 8.14.** 任意有限群 $G$ 的 *Frattini* 子群 $\Phi(G)$ 都幂零。

证明. 记 $D = \Phi(G)$。若 $D = 1$，结论成立。否则取任意素数 $p \mid |D|$ 及 $P \in \mathrm{Syl}_p(D)$。$D$ 特征于 $G$，特别是正规子群，Frattini 论证给出

$$G = D\,N_G(P).$$

由推论 8.4，子群 $H$ 满足 $H\Phi(G) = G$ 时必等于 $G$。应用于 $H = N_G(P)$，得到 $N_G(P) = G$，即 $P \trianglelefteq G$。所以 $D$ 的每个 Sylow 子群都正规于 $D$。有限群的幂零性判据遂给出 $D$ 幂零。 □

**命题 8.15** (Frattini 子群与商映射)**.** 若 $G$ 有限且 $N \trianglelefteq G$，则

$$\Phi(G)N/N \le \Phi(G/N).$$

若另外 $N \le \Phi(G)$，则有等式 $\Phi(G/N) = \Phi(G)/N$。

证明. 设 $\bar{M}$ 是 $G/N$ 的极大真子群。它的原像 $M$ 是包含 $N$ 的极大真子群：若 $M < K < G$，则 $N \le K$，子群对应给出 $\bar{M} < K/N < G/N$，与极大性矛盾。因此 $\Phi(G) \le M$，其像落在 $\bar{M}$ 中。对全部 $\bar{M}$ 取交便得到包含式；若 $G/N = 1$，包含式也成立。

若 $N \le \Phi(G)$，则 $G$ 的每个极大真子群都包含 $N$。子群对应因而在 $G$ 和 $G/N$ 的极大真子群之间给出双射。于是 $xN$ 属于 $\Phi(G/N)$ 当且仅当 $x$ 属于 $G$ 的全部极大真子群，即当且仅当 $x \in \Phi(G)$。这就是所求等式。 □

## 8.5 Fitting 子群的构造

**定义 8.16.** 有限群 $G$ 的 *Fitting* 子群定义为所有正规幂零子群的乘积：

$$F(G) = \prod \{N \trianglelefteq G : N \text{ 幂零}\}.$$

要使这个定义合法，必须证明有限个正规幂零子群的乘积仍为正规幂零子群。

**定理 8.17** (Fitting 乘积定理)**.** 设 $G$ 为有限群。若 $A, B \trianglelefteq G$ 且 $A, B$ 幂零，则 $AB$ 幂零。对每个素数 $p$，$AB$ 的 *Sylow* $p$ 子群等于 $P_A P_B$，其中 $P_A, P_B$ 分别是 $A, B$ 的 *Sylow* $p$ 子群；这些子群正规于 $G$。

证明. 有限幂零群是其 Sylow 子群的直积。因 $A$ 幂零，其 Sylow $p$ 子群 $P_A$ 唯一，故特征于 $A$；$A \trianglelefteq G$ 遂给出 $P_A \trianglelefteq G$。同理 $P_B \trianglelefteq G$。

$P_A, P_B$ 都正规于 $G$，故 $P_AP_B$ 是正规子群，且

$$|P_AP_B| = \frac{|P_A||P_B|}{|P_A \cap P_B|}$$

是 $p$ 的幂。记 $U = P_AP_B$。$AU/U$ 是 $A$ 的同态像，并且该同态的核包含 $P_A$，故 $|AU/U|$ 整除 $[A : P_A]$，不被 $p$ 整除。同理，$|BU/U|$ 不被 $p$ 整除。由于二者都是正规子群，它们的乘积就是商群

$$AB/U = (AU/U)(BU/U),$$

按乘积阶公式，其阶也不被 $p$ 整除。因此 $U$ 是 $AB$ 的 Sylow $p$ 子群。

最后说明不同素数的这些子群为什么交换。若 $U_p, U_q$ 分别是所构造的正规 $p$ 子群与正规 $q$ 子群，$p \neq q$，则

$$[U_p, U_q] \leq U_p \cap U_q = 1.$$

所以它们逐元素交换，且各因子的阶两两互素。乘法映射 $\prod_p U_p \to AB$ 是同态；其像的阶为 $\prod_p |U_p| = |AB|$，核为单位元。故 $AB$ 是这些 Sylow 子群的直积，因而幂零。 □

**推论 8.18.** *有限群 $G$ 有唯一最大的正规幂零子群 $F(G)$，且它包含每个正规幂零子群。$F(G)$ 是特征子群。*

证明. 有限群只有有限个子群，反复应用 Fitting 乘积定理，所有正规幂零子群的乘积仍正规幂零，并包含每一个。自同构把正规幂零子群置换，故把最大乘积固定。 □

**命题 8.19** (按素数分解 Fitting 子群)**.** *记 $O_p(G)$ 为有限群 $G$ 的最大正规 $p$ 子群，则*

$$F(G) = \prod_{p||G|} O_p(G).$$

*这个乘积是内部直积，并且 $\Phi(G) \leq F(G)$。若 $H \trianglelefteq G$，还有*

$$F(H) = H \cap F(G).$$

证明. 先说明 $O_p(G)$ 的存在。两个正规 $p$ 子群的乘积仍是正规子群，其阶由乘积阶公式知为 $p$ 的幂。有限群中反复取乘积，便得到包含所有正规 $p$ 子群的最大者 $O_p(G)$。它也是特征子群，因为自同构置换所有正规 $p$ 子群。

若 $p \neq q$，则 $[O_p(G), O_q(G)] \leq O_p(G) \cap O_q(G) = 1$。故乘积 $D = \prod_p O_p(G)$ 是正规幂零子群，$D \leq F(G)$。反过来，$F(G)$ 的 Sylow $p$ 子群唯一，特征于 $F(G)$，因而正规于 $G$，所以包含于 $O_p(G)$。将 $F(G)$ 的各 Sylow 因子相乘得 $F(G) \leq D$，于是等式成立。前一定理已证 $\Phi(G)$ 正规幂零，故其包含于 $F(G)$。

最后设 $H \trianglelefteq G$。因为 $F(H)$ 特征于 $H$，它正规于 $G$，又幂零，所以 $F(H) \leq H \cap F(G)$。另一方面，$H \cap F(G)$ 正规于 $H$，且是幂零群 $F(G)$ 的子群，因而幂零，所以 $H \cap F(G) \leq F(H)$。两向包含给出等式。 □

**命题 8.20** (商群中的 Fitting 子群)**.** *若 $N \trianglelefteq G$，则*

$$F(G)N/N \subseteq F(G/N).$$

*一般不能把这个包含关系改成等号。*

证明. $F(G)N/N$ 是 $G/N$ 的正规幂零子群，故包含于 $F(G/N)$。等号可能失败：在 $G = S_3$、$N = F(G) = A_3$ 时，左侧为平凡群，而 $F(G/N) = F(C_2) = C_2$。 □

## 8.6 有限可解群中的 Fitting 层

**引理 8.21.** *有限非平凡可解群 $G$ 的每个极小正规子群 $N$ 都是初等交换群 $C_p^d$，并且 $N \le F(G)$。*

证明. $N'$ 特征于 $N$，因而正规于 $G$。极小正规性给出 $N' = 1$ 或 $N' = N$。若 $N' = N$，则 $N^{(i)} = N$ 对所有 $i$ 成立。但由 $N \le G$ 和交换子的定义，逐次归纳有 $N^{(i)} \le G^{(i)}$。可解性给出某个 $r$ 使 $G^{(r)} = 1$，于是 $N \le 1$，矛盾。因此 $N' = 1$，即 $N$ 交换。

取素数 $p \mid |N|$。交换群 $N$ 的 Sylow $p$ 子群唯一，故特征于 $N$，从而正规于 $G$；极小正规性迫使该 Sylow 子群等于 $N$。所以 $N$ 是 $p$ 群。幂映射 $f : N \to N$，$x \mapsto x^p$ 是同态，像 $N^p$ 特征于 $N$。由 Cauchy 定理，存在阶为 $p$ 的非单位元，其属于 $\ker f$，所以

$$|N^p| = |N|/|\ker f| < |N|.$$

极小正规性随即给出 $N^p = 1$。用 $N$ 的群乘法作向量加法、用整数幂作 $\mathbb{F}_p$ 数乘，即得到有限维 $\mathbb{F}_p$ 向量空间。因此 $N \cong C_p^d$，$d \ge 1$。它交换所以幂零，故 $N \le F(G)$。 □

**定理 8.22** (有限可解群的 Fitting 自中心化)**.** *若 $G$ 为有限可解群，记 $F = F(G)$，则*

$$C_G(F) = Z(F).$$

*特别地，$C_G(F) \le F$。*

证明. 令 $C = C_G(F)$，$Z = Z(F)$。由于 $F$ 特征于 $G$，对任意 $g \in G$ 有

$$gCg^{-1} = C_G(gFg^{-1}) = C,$$

故 $C \trianglelefteq G$。$Z$ 特征于 $F$，也正规于 $G$。按中心的定义，

$$C \cap F = Z.$$

并且 $C$ 中每个元素都与 $Z \le F$ 中每个元素交换，所以 $Z \le Z(C)$。

若 $C > Z$，则非平凡正规子群 $C/Z$ 包含 $G/Z$ 的某个极小正规子群 $D/Z$：在所有满足 $1 < K/Z \le C/Z$ 且 $K/Z \trianglelefteq G/Z$ 的子群中取阶最小者即可。$G/Z$ 可解，由上一引理，$D/Z$ 初等交换，特别是交换群。于是

$$[D, D] \le Z, \qquad [Z, D] = 1.$$

这两式直接给出下中心列

$$\gamma_2(D) = [D, D] \le Z, \qquad \gamma_3(D) = [\gamma_2(D), D] = 1.$$

所以 $D$ 幂零，类至多为二。又 $D \trianglelefteq G$，故 $D \le F$。结合 $D \le C$，得到 $D \le C \cap F = Z$，与 $D/Z \ne 1$ 矛盾。因此 $C = Z$。 □

**推论 8.23** (共轭作用的两个忠实商)**.** *在上一条件下，共轭给出单同态*

$$G/Z(F) \hookrightarrow \mathrm{Aut}(F), \qquad G/F \hookrightarrow \mathrm{Out}(F).$$

*第二个同态的靶群为* $\mathrm{Out}(F) = \mathrm{Aut}(F)/\mathrm{Inn}(F)$。

*证明.* 同态 $\theta : G \to \mathrm{Aut}(F)$ 定义为 $\theta(g)(x) = gxg^{-1}$，其核是 $C_G(F) = Z(F)$，故第一式由第一同构定理得到。

复合同态 $G \to \mathrm{Out}(F)$ 在 $F$ 上平凡。若 $g$ 的像为单位元，则存在 $f \in F$，使 $gxg^{-1} = fxf^{-1}$ 对所有 $x \in F$ 成立。因而 $f^{-1}g \in C_G(F) = Z(F) \le F$，所以 $g \in F$。反之，$F$ 中元素的共轭在 $F$ 上当然是内自同构。因此这个复合同态的核恰为 $F$，得到第二式。 □

## 8.7 Fitting 列与可解群的幂零层数

**定义 8.24.** 对有限群 $G$，定义 $F_0(G) = 1$，并递归地令 $F_{i+1}(G)$ 为 $F(G/F_i(G))$ 在 $G$ 中的原像，即

$$F_{i+1}(G)/F_i(G) = F(G/F_i(G)).$$

这个递增列称为上 Fitting 列。若某个 $F_h(G) = G$，取最小的 $h$，称为 $G$ 的 Fitting 高度，记为 $h(G)$；约定 $h(1) = 0$。

**定理 8.25.** *有限群 $G$ 可解，当且仅当其上 Fitting 列最终到达 $G$。此时 $h(G)$ 等于所有正规列*

$$1 = N_0 \le N_1 \le \cdots \le N_r = G, \qquad N_i \trianglelefteq G,$$

*中每个因子 $N_{i+1}/N_i$ 都幂零时的最小长度 $r$。*

*证明.* 每个 $F_i(G)$ 都特征于 $G$。事实上，$F_0(G) = 1$ 特征；若 $F_i(G)$ 特征，$G$ 的任意自同构都诱导 $G/F_i(G)$ 的自同构，后者保持其 Fitting 子群，故保持该子群的原像 $F_{i+1}(G)$。

若 $G$ 可解而 $F_i(G) < G$，则 $G/F_i(G)$ 是非平凡可解群，含非平凡极小正规初等交换子群，所以它的 Fitting 子群非平凡。因此 $F_i(G) < F_{i+1}(G)$。群阶有限，这个严格增长不能无限持续，故某个 $F_h(G) = G$。反过来，若列到达 $G$，每个因子 $F_{i+1}(G)/F_i(G)$ 都幂零，因而可解；逐层用可解群的扩张仍可解，得到 $G$ 可解。

现在给定题设长度为 $r$ 的正规列，归纳证明 $N_i \le F_i(G)$。$i = 0$ 成立。若 $N_i \le F_i(G)$，则 $N_{i+1}F_i(G)/F_i(G)$ 是 $G/F_i(G)$ 的正规子群，并且是 $N_{i+1}/N_i$ 的同态像。后者幂零，故这个像也幂零，因而包含于 $F(G/F_i(G))$。取原像得 $N_{i+1} \le F_{i+1}(G)$。于是 $G = N_r \le F_r(G)$，故 $h(G) \le r$。而上 Fitting 列本身具有长度 $h(G)$ 且因子全幂零，所以最小长度恰为 $h(G)$。 □

**例 8.26** ($S_4$ 的三个幂零层)**.** 令

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

这是 $S_4$ 的正规 Klein 四元子群。$S_4$ 作用于三种无序配对

$$\{\{1,2\},\{3,4\}\}, \quad \{\{1,3\},\{2,4\}\}, \quad \{\{1,4\},\{2,3\}\}$$

得到同态 $\psi : S_4 \to S_3$。$(12)$ 诱导第二、三个配对的换位，$(123)$ 诱导三循环，故像为整个 $S_3$。逐项作用可见 $V \le \ker\psi$，而 $|\ker\psi| = 24/6 = 4 = |V|$，故 $\ker\psi = V$。

$S_3$ 无非平凡正规 2 子群：任何这样的子群必阶为二，但三个二阶子群彼此共轭，均不正规。因此 $\psi(O_2(S_4))=1$，从而 $O_2(S_4)\le V$；反向包含由 $V$ 本身正规且为 2 群得到。所以 $O_2(S_4)=V$。$S_4$ 的阶三子群共有四个，分别由四种三元支集上的三循环生成，故没有正规 Sylow 3 子群，$O_3(S_4)=1$。由命题 8.19，

$$F(S_4)=V.$$

同理 $F(S_3)=A_3$，而 $F(C_2)=C_2$。$\psi$ 的 $A_3$ 原像是 $A_4$：前者是指数二子群，且其元素在四个字母上的符号与诱导在三个配对上的符号一致，因为两个符号同态在生成 $S_4$ 的换位上都为 $-1$。所以

$$F_0(S_4)=1,\quad F_1(S_4)=V,\quad F_2(S_4)=A_4,\quad F_3(S_4)=S_4.$$

各因子依次为 $C_2^2, C_3, C_2$，故 $h(S_4)=3$。与之相比，$S_4$ 的导出列是 $S_4, A_4, V, 1$：$S_4'\le A_4$，而两个相交换位的交换子是三循环，三循环生成 $A_4$；$A_4'\le V$，且 $[(123),(124)]$ 是一个双换位，其在 $A_4$ 中的共轭包含 $V$ 的三个非单位元，故 $A_4'=V$。这两个长度在本例恰好相同，但定义分别衡量幂零因子与交换因子，不能混用。例如八阶二面体群 $D_8$ 本身幂零，所以 $h(D_8)=1$；而 $D_8'=\langle r^2\rangle\cong C_2$，$D_8''=1$，故其导出长度为二。

## 8.8 Hall 子群与素数集分解

**定义 8.27.** 设 $\pi$ 为一组素数，$\pi'$ 为其在全体素数中的补集。正整数 $n$ 的 $\pi$-部分定义为

$$n_\pi=\prod_{p\in\pi}p^{v_p(n)}.$$

阶的所有素因子都属于 $\pi$ 的有限群称为 $\pi$-群。有限群 $G$ 的子群 $H$ 称为 Hall $\pi$-子群，若 $H$ 是 $\pi$-群，且 $[G:H]$ 的所有素因子属于 $\pi'$；等价地，

$$|H|=|G|_\pi.$$

仅有 $\gcd(|H|,[G:H])=1$ 并不足以保证 $H$ 是指定素数集 $\pi$ 的 Hall 子群。例如 $1\le C_6$ 的阶与指数互素，但它不是 Hall $\{2\}$-子群。

**引理 8.28.** *设 $A\trianglelefteq E$ 为有限交换群，$Q=E/A$，且 $\gcd(|A|,|Q|)=1$。则存在子群 $H\le E$ 使 $E=AH$、$A\cap H=1$；所有这样的补子群彼此由 $A$ 中元素共轭。*

*证明.* 在 $A$ 上采用加法记号，在 $E$ 和 $Q$ 上采用乘法记号。取集合截面 $s:Q\to E$，满足 $s(1)=1$。定义

$$x\cdot a=s(x)as(x)^{-1},\qquad s(x)s(y)=c(x,y)s(xy).$$

改变 $s(x)$ 只会使其左乘 $A$ 中元素，而 $A$ 交换，所以第一式不依赖截面的选择。由第二式，$s(x)s(y)$ 与 $s(xy)$ 仅相差 $A$ 中元素，故 $x\cdot(y\cdot a)=(xy)\cdot a$；这确实定义 $Q$ 在 $A$ 上的作用。结合律 $(s(x)s(y))s(z)=s(x)(s(y)s(z))$ 分别展开为

$$\big(c(x,y)+c(xy,z)\big)s(xyz)=\big(x\cdot c(y,z)+c(x,yz)\big)s(xyz).$$

于是 $c$ 满足下述二余循环恒等式，且 $c(1,y)=c(x,1)=0$。

记 $m=|Q|$。由于 $\gcd(m,|A|)=1$，存在整数 $u,v$ 使 $um+v|A|=1$。Lagrange 定理给出 $|A|a=0$，所以 $u(ma)=a=m(ua)$。以下的 $m^{-1}a$ 指 $ua$，即乘以 $m$ 的自同构的逆，并非把 $A$ 的元素当作有理数相除。令

$$b(x)=|Q|^{-1}\sum_{z\in Q} z^{-1}\cdot c(z,x).$$

采用加法记号的二余循环恒等式

$$x\cdot c(y,z)+c(x,yz)=c(x,y)+c(xy,z).$$

于是，对 $x,y\in Q$，将第一项中的求和指标改为 $z=tx$，得到

$$\begin{aligned} x\cdot b(y)-b(xy)+b(x) &= |Q|^{-1}\sum_{t\in Q} t^{-1}\cdot\big(c(t,x)+c(tx,y)-c(t,xy)\big)\\ &= |Q|^{-1}\sum_{t\in Q} t^{-1}\cdot\big(t\cdot c(x,y)\big)=c(x,y). \end{aligned}$$

第二个等号正是二余循环恒等式的移项。具体地，第一项作 $z=tx$ 后，$x\cdot(z^{-1}\cdot a)=t^{-1}\cdot a$；然后将三个求和合并。由 $c(z,1)=0$ 还得 $b(1)=0$。

现在令 $t(x)=(-b(x))s(x)$。这里 $-b(x)$ 是 $A$ 中元素，视为 $E$ 中的因子。逐步计算

$$\begin{aligned} t(x)t(y) &= (-b(x))s(x)(-b(y))s(y)\\ &= \big(-b(x)-x\cdot b(y)+c(x,y)\big)s(xy)\\ &= (-b(xy))s(xy)=t(xy). \end{aligned}$$

故 $t:Q\to E$ 为同态，且商映射 $q:E\to Q$ 满足 $q\circ t=\mathrm{id}_Q$，所以 $t$ 单射。取 $H=t(Q)$。若 $h\in H\cap A$，则 $q(h)=1$，由单射性 $h=t(1)=1$。对任意 $e\in E$，令 $x=q(e)$，则 $et(x)^{-1}\in A$，故 $E=AH$。这证明了补群的存在，而不只证明一个共链恒等式。

设 $H,H'$ 为两个补群。商映射在它们上的限制都是到 $Q$ 的同构，其逆记为 $t,t'$。存在唯一函数 $d:Q\to A$ 使 $t'(x)=d(x)t(x)$。比较 $t'(xy)$ 与 $t'(x)t'(y)$，并利用 $t,t'$ 都是同态，得

$$d(xy)=d(x)+x\cdot d(y).$$

令 $a=|Q|^{-1}\sum_{x\in Q}d(x)$。对固定 $x$，由上式置换求和指标得

$$x\cdot a-a=|Q|^{-1}\sum_{y}(x\cdot d(y)-d(y))=|Q|^{-1}\sum_{y}(d(xy)-d(x)-d(y))=-d(x).$$

所以 $d(x)=a-x\cdot a$。在 $E$ 中计算

$$a\,t(x)\,a^{-1}=(a-x\cdot a)t(x)=d(x)t(x)=t'(x).$$

于是 $aHa^{-1}=H'$，证明共轭结论，并确定共轭的方向。 □

## 8.9 可解群的 Hall 子群存在性

**定理 8.29** (Hall 存在定理（可解情形）)**.** *设 $G$ 为有限可解群，$\pi$ 为任意素数集。则 $G$ 含有 Hall $\pi$-子群。*

证明. 对 $|G|$ 作归纳。$G=1$ 时取 $H=1$。设 $G\neq 1$，取极小正规子群 $N$。由引理，$N$ 是初等交换 $p$ 群。归纳假设 $G/N$ 有 Hall $\pi$-子群 $\bar{H}$，令 $H$ 为其在 $G$ 中的原像。

若 $p\in\pi$，则 $|H|$ 正好是 $|G|$ 的最大 $\pi$ 部分，$H$ 即 Hall $\pi$-子群。

若 $p\notin\pi$，则 $|N|$ 与 $|H/N|$ 互素。引理应用于 $N\trianglelefteq H$，给出补子群 $K$。因 $K\cong H/N$，其阶为 $|G|$ 的最大 $\pi$ 部分，故为 Hall $\pi$-子群。 □

**定理 8.30** (Hall 子群的共轭与包含)**.** *设 $G$ 为有限可解群，$\pi$ 为素数集。则：*

1. *任意两个 Hall $\pi$-子群共轭；*
2. *任意 $\pi$-子群都包含于某个 Hall $\pi$-子群。*

证明. 对 $|G|$ 作归纳，同时证明两条结论。$G=1$ 时二者均成立。设 $G\neq 1$，取极小正规子群 $N\cong C_p^d$，并记商映射为 $q:G\to G/N$。

先证明共轭性。设 $H,K$ 是 Hall $\pi$-子群。像 $q(H)$ 是 $\pi$-群，且

$$[G/N:q(H)]=[G:HN]\mid[G:H].$$

右侧是 $\pi'$-数，故 $q(H)$ 是 $G/N$ 的 Hall $\pi$-子群。同理 $q(K)$ 也是。由归纳假设存在 $\bar{g}\in G/N$ 使 $\bar{g}q(H)\bar{g}^{-1}=q(K)$。提升为 $g\in G$ 并将 $H$ 替换为 $gHg^{-1}$ 后，可设 $HN=KN=:E$。

若 $p\in\pi$，则 $HN$ 也是 $\pi$-群：它的阶为 $|H||N|/|H\cap N|$。但 $|H|=|G|_\pi$ 已是子群可能具有的最大 $\pi$-阶，故 $HN=H$。同理 $KN=K$。因此 $H=E=K$。

若 $p\notin\pi$，则 $H\cap N=K\cap N=1$，且 $NH=NK=E$。$N$ 交换，$|E/N|=|H|$ 与 $|N|$ 互素。由引理 8.28，$H,K$ 被 $N$ 中某元素共轭。与最初提升的 $g$ 合成，就得到原来两个 Hall 子群在 $G$ 中共轭。

再证明包含性。设 $L$ 是任意 $\pi$-子群。由归纳假设，$q(L)$ 包含在 $G/N$ 的某个 Hall $\pi$-子群 $\bar{E}$ 中，令 $E=q^{-1}(\bar{E})$。于是 $L\le E$，并且 $[G:E]$ 是 $\pi'$-数。

若 $p\in\pi$，则 $|E|=|N||\bar{E}|=|G|_\pi$，$E$ 就是所求 Hall 子群。

若 $p\notin\pi$，由交换互素分裂引理，存在补群 $K\le E$ 使 $E=NK$、$N\cap K=1$。其阶等于 $|G|_\pi$，故 $K$ 是 $G$ 的 Hall $\pi$-子群。这里不能直接断言 $L\le K$，需要在较小的群 $NL$ 中比较两个补群。令

$$K_0=(q|_K)^{-1}(q(L))=K\cap NL.$$

这一步的映射关系为

$$\begin{array}{ccc} K_0 & \hookrightarrow & K \\ {\scriptstyle q|_{K_0}}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle q|_K} \\ q(L) & \hookrightarrow & \bar{E}. \end{array}$$

两条竖箭头为同构，故从右下角先限制到 $q(L)$ 再取逆像，恰好得到左上角所需的子群；这也解释了为什么必须取 $K_0$，不能直接把 $L$ 当作 $K$ 的子群。因为 $q|_K:K\to\bar{E}$ 是同构，$|K_0|=|q(L)|=|L|$。此外 $q(K_0)=q(L)$，故 $NK_0=NL$。于是 $K_0$ 与 $L$ 都是 $NL$ 中 $N$ 的补群。再次应用引理，存在 $n\in N$ 使 $nLn^{-1}=K_0\le K$。所以

$$L\le n^{-1}Kn,$$

而 $n^{-1}Kn$ 仍是 Hall $\pi$-子群，包含性得证。 □

## 8.10 Schur–Zassenhaus 的可解证明

**定理 8.31** (Schur–Zassenhaus（可解版本）)**.** 设 $G$ 为有限可解群，$N \trianglelefteq G$，且 $\gcd(|N|, [G:N]) = 1$。则存在 $H \leq G$ 使

$$G = NH, \qquad N \cap H = 1.$$

任意两个这样的补子群彼此由 $N$ 中元素共轭。

证明. 令 $\pi$ 为 $|G/N|$ 的素数集。由于 $|N|$ 与 $|G/N|$ 互素，$|G/N|$ 是 $|G|$ 的全部 $\pi$ 部分，所以 $G$ 的 Hall $\pi$-子群 $H$ 存在。其阶为 $[G:N]$，故 $H \cap N = 1$；又 $|NH| = |N||H| = |G|$，于是 $G = NH$。

若 $H, K$ 都是补子群, 则二者都是 Hall $\pi$-子群。由 Hall 共轭定理, 存在 $g \in G$ 使 $gHg^{-1} = K$。写成 $g = nh$，其中 $n \in N$、$h \in H$（因为 $G = NH$）。由于 $h$ 规范化 $H$，有

$$gHg^{-1} = nhHh^{-1}n^{-1} = nHn^{-1} = K,$$

所以两个补子群事实上由 $N$ 中元素共轭。 □

**注 8.32.** 本章只证明 $G$ 可解时的 Schur–Zassenhaus。一般有限群的补群存在定理，以及在核或商可解时的补群共轭定理，需要另作证明；这里不能删去已经用于 Hall 归纳的可解性。将一般共轭结论再与奇数阶群可解定理联系，还涉及远超本章范围的结构理论。

## 8.11 条件的边界：Hall 失败与补群不唯一

**例 8.33** (不可解群中的 Hall 障碍)**.** 在 $A_5$ 中，若存在阶 15 的子群 $H$，则其 Sylow 5 子群 $P$ 在 $H$ 中正规，因为 $n_5(H) \mid 3$ 且 $n_5(H) \equiv 1 \pmod 5$，故 $n_5(H) = 1$。于是 $H \leq N_{A_5}(P)$。$S_5$ 中五循环共有 $5!/5 = 24$ 个，且都为偶置换；每个阶五子群包含四个五循环，不同阶五子群的非单位元互不相交。因此 $A_5$ 中 Sylow 5 子群数为 $24/4 = 6$，所以

$$|N_{A_5}(P)| = |A_5|/6 = 10,$$

不可能包含阶 15 的子群。这说明 $A_5$ 不含 Hall $\{3,5\}$-子群；可解性不能从 Hall 定理中删除。

**例 8.34** (互素条件失效)**.** 扩张

$$1 \longrightarrow C_p \longrightarrow C_{p^2} \longrightarrow C_p \longrightarrow 1$$

没有补子群：$C_{p^2}$ 的唯一阶 $p$ 子群正好是核，不能与核交为单位元。这里核与商阶不互素，正是第四章循环中心扩张中出现的不分裂例子。

**例 8.35** (补群可能很多但共轭)**.** 取 $\mathbb{F}_5$ 上的仿射群

$$G = \{x \mapsto ax + b : a \in \mathbb{F}_5^\times,\ b \in \mathbb{F}_5\}.$$

记仿射变换为 $(a, b)$，则 $(a,b)(c,d) = (ac, ad + b)$。平移子群 $N = \{(1, b) : b \in \mathbb{F}_5\}$ 正规，阶为五。点 $t \in \mathbb{F}_5$ 的稳定子为

$$H_t = \{(a, (1-a)t) : a \in \mathbb{F}_5^\times\},$$

阶为四，与 $N$ 交为单位元，故为补群。若 $s \neq t$，取 $a = 2$，则 $(2, (1-2)t)$ 固定 $t$ 而不固定 $s$，所以 $H_s \neq H_t$。对平移 $\tau_u = (1, u)$，逐项相乘得

$$\tau_u (a, (1-a)t) \tau_u^{-1} = (a, (1-a)(t+u)),$$

所以 $\tau_u H_t \tau_u^{-1} = H_{t+u}$。任意补群由 $N$ 中元素共轭于 $H_0$，因而恰为这五个 $H_t$ 之一。这个例子同时表明：补群可有多个，但互素条件下的核共轭类只有一个。

## 8.12 本章工具之间的依赖关系

Frattini 理论回答最小生成问题；Fitting 理论回答最大正规幂零部分；Hall 与 Schur–Zassenhaus 回答互素阶的正规核是否有补。它们的逻辑关系可以写成

$$\text{极大子群} \Longrightarrow \Phi(G) \Longrightarrow P/\Phi(P) \text{ 的线性化}$$

以及

$$\text{正规幂零子群乘积} \Longrightarrow F(G) \Longrightarrow C_G(F(G)) = Z(F(G)) \quad (G \text{ 可解}),$$

和

$$\text{极小正规初等交换子群} + \text{交换互素扩张分裂} \Longrightarrow \begin{array}{l}\text{Hall 存在、共轭、Schur–Zassenhaus} \\ \text{（可解情形）}\end{array}$$

下一章将在向量空间和群代数上建立线性表示。Burnside 基定理已经说明有限 $p$ 群的生成问题自然产生 $\mathbb{F}_p$ 向量空间；Fitting 与 Hall 理论则提供表示论中按正规层和互素层分解群的结构背景。

## 文献说明

本章所用 Sylow 理论及可解、幂零群的基础结论，可参照 James S. Milne，*Group Theory*，Version 4.01 (2025)，第 77–81 页及第 90–95 页；Frattini 论证见该书第 96 页命题 6.22。这里的 “Frattini 论证” 不能与 Frattini 子群的全部理论混称。该书这些页段不包含本章的 Fitting 与 Hall 定理，不将它们列作这两部分的出处。

本章将交换核的互素分裂写成显式共链平均，给出新截面的乘法和补群共轭的逐项计算；Hall 包含性另在 $NL$ 中比较补群。Fitting 自中心化通过 $C_G(F)/Z(F)$ 中的极小正规层证明。上述结论的证明责任均在正文承担；Hall 定理的可解性与互素分裂的互素性分别由 $A_5$ 和 $C_{p^2}$ 的反例标明。

# 9 有限群的线性表示与完全可约性

群的置换作用把群元素变成集合上的双射；线性表示要求这些双射同时保持向量空间运算。本章先说明群作用、矩阵与群代数模之间怎样相互转换，再证明两个决定分解理论的事实：在群阶可逆时，不变子空间总有不变补空间；在代数闭域上，不可约表示的自同态只有标量。所有向量空间均为有限维，所有群均为有限群，除非另有说明。底域记为 $k$；只有明确写出 $k=\mathbb{C}$ 或 “$k$ 代数闭” 时，才使用相应条件。

## 9.1 线性作用、矩阵与表示的等价

**定义 9.1.** 群 $G$ 在 $k$-向量空间 $V$ 上的表示是群同态

$$\rho : G \longrightarrow \mathrm{GL}_k(V).$$

其维数为 $\dim_k V$，其核为 $\{g : \rho(g)=\mathrm{id}_V\}$；核平凡时称为忠实表示。零空间上的表示允许存在，但不称为不可约表示。

写 $gv=\rho(g)v$ 后，同态条件等价于

$$g(hv)=(gh)v, \qquad 1v=v,$$

并要求 $v\mapsto gv$ 为线性映射。反过来，满足这些条件的线性作用中，$g$ 的作用以 $g^{-1}$ 的作用为逆，故确实取值于 $\mathrm{GL}_k(V)$。

**定义 9.2.** 表示 $(V,\rho)$ 到 $(W,\sigma)$ 的同态是满足

$$T\rho(g)=\sigma(g)T \qquad (g\in G)$$

的线性映射 $T:V\to W$，亦称交织映射。这些映射组成向量空间 $\mathrm{Hom}_G(V,W)$。若 $T$ 可逆，则称两个表示等价。

固定 $V$ 的基后，$\rho(g)$ 给出矩阵 $A_g$，满足 $A_{gh}=A_gA_h$。若新基向量的旧坐标构成矩阵 $B$ 的列，则 $v$ 的旧、新坐标满足 $[v]_{\mathrm{old}}=B[v]_{\mathrm{new}}$，因此

$$[\rho(g)v]_{\mathrm{new}}=B^{-1}A_gB[v]_{\mathrm{new}}.$$

故同一表示在不同基下的矩阵族相差同一个 $B$ 的同时共轭。只对每个 $g$ 分别找一个共轭矩阵，不能据此断定两个表示等价；交织映射必须对所有 $g$ 同时成立。

**例 9.3** (底域会改变表示)**.** 令 $C_p=\langle s\rangle$，$k$ 的特征为 $p$。在 $k^2$ 上取

$$\rho(s)=I+N, \qquad N=\begin{pmatrix}0&1\\0&0\end{pmatrix}.$$

因 $N^2=0$，二项式给出 $(I+N)^m=I+mN$。于是 $\rho(s)^p=I$，而 $1\le m<p$ 时 $mN\neq 0$，所以得到一个忠实的二维表示。另一方面，若 $a\in k^\times$ 满足 $a^p=1$，则 $(a-1)^p=a^p-1=0$，域中没有非零幂零元，故 $a=1$。因此在这个底域上，$C_p$ 的一维表示全部平凡。

## 9.2 群代数与线性延拓

**定义 9.4.** 群代数 $k[G]$ 是以符号 $\{e_g : g \in G\}$ 为基的 $k$-向量空间，其乘法由

$$e_g e_h = e_{gh}$$

双线性延拓而成。因此

$$\left(\sum_{g} a_g e_g\right)\left(\sum_{h} b_h e_h\right) = \sum_{x \in G}\left(\sum_{gh=x} a_g b_h\right) e_x.$$

单位元是 $e_1$。$k[G]$ 一般不交换，且作为向量空间的维数为 $|G|$。

结合律可以在基上验证：$(e_g e_h)e_t = e_{(gh)t} = e_{g(ht)} = e_g(e_h e_t)$；再对三个任意线性组合分别展开，三线性性便把结合律推广到整个群代数。

**命题 9.5** (表示与模的对应)**.** *给定 $G$ 在 $V$ 上的表示，公式*

$$\left(\sum_{g} a_g e_g\right) v = \sum_{g} a_g \rho(g) v$$

*唯一地使 $V$ 成为单位左 $k[G]$-模。反过来，任意单位左 $k[G]$-模的作用限制到 $e_g$，都给出 $G$ 的表示。两种构造互为逆；表示同态恰为 $k[G]$-模同态。*

*证明.* 记 $a = \sum_g a_g e_g$、$b = \sum_h b_h e_h$。直接展开得

$$(ab)v = \sum_{g,h} a_g b_h \rho(gh) v = \sum_{g,h} a_g b_h \rho(g)\rho(h) v = a(bv).$$

同时 $e_1 v = v$，对向量及系数的分配律由线性性成立，因此模的公理全部满足。因为 $e_g$ 是一组基，任意延拓都必须采用题设公式，故唯一。

反过来，$e_g e_{g^{-1}} = e_1$，所以 $e_g$ 在模上的作用可逆；$e_g e_h = e_{gh}$ 又给出群同态条件。这两个构造在每个 $e_g$ 上保持原作用，再由线性性在整个 $k[G]$ 上保持原作用，故互逆。最后，$T$ 与每个 $\rho(g)$ 交织，当且仅当它与每个线性组合的作用交织，这正是模同态条件。 □

**例 9.6** (左正则表示与置换表示)**.** 在 $k[G]$ 上令 $L(g)e_h = e_{gh}$，称为左正则表示。若 $L(g) = \mathrm{id}$，则 $e_g = L(g)e_1 = e_1$。基向量互异，故 $g = 1$，所以这个表示在任意底域上都忠实。

更一般地，若 $G$ 作用于有限集合 $X$，令 $k[X]$ 以 $\{e_x : x \in X\}$ 为基，并定义 $g e_x = e_{gx}$，便得到置换表示。向量 $v = \sum_x a_x e_x$ 被所有 $g$ 固定，当且仅当

$$a_{gx} = a_x \qquad (g \in G,\ x \in X).$$

因此系数恰在每条轨道上为常数，各轨道的向量和 $\sum_{x \in \mathcal{O}} e_x$ 构成固定子空间的一组基。特别地，

$$\dim_k k[X]^G = G \text{ 在 } X \text{ 上的轨道数.}$$

这个结论不要求 $|G|$ 在 $k$ 中可逆。

## 9.3 不变子空间、商表示与分裂

**定义 9.7.** 若子空间 $U \le V$ 满足 $\rho(g)U \subseteq U$ 对所有 $g$ 成立，则称 $U$ 为不变子空间。由于同时可取 $g^{-1}$，实际有 $\rho(g)U = U$。若 $V \neq 0$ 且不变子空间只有 $0, V$，则表示不可约。若 $V$ 是有限个不可约不变子空间的直和，则称其完全可约，也称半单。

若 $U$ 不变，则

$$g(v+U) = gv + U$$

定义 $V/U$ 的商表示。其良定义性来自：若 $v - v' \in U$，则 $g(v-v') \in U$。表示同态 $T : V \to W$ 的核与像都不变，因为 $T(gv) = gT(v)$。这些事实使向量空间的核、像和商同时成为表示范畴中的对象。

**命题 9.8** (分裂的三种写法)**.** *对不变子空间 $U \le V$，以下条件等价：*

1. *存在不变子空间 $W$ 使 $V = U \oplus W$；*
2. *存在 $G$-同态 $P : V \to U$ 使 $P|_U = \mathrm{id}_U$；*
3. *商映射 $q : V \to V/U$ 有 $G$-同态截面 $s : V/U \to V$，即 $q \circ s = \mathrm{id}_{V/U}$。*

*证明.* 若 $V = U \oplus W$，令 $P(u+w) = u$。因两个因子都不变，$P(g(u+w)) = P(gu+gw) = gu = gP(u+w)$，所以 $P$ 交织作用。限制 $q|_W : W \to V/U$ 为同构，其逆再与 $W \hookrightarrow V$ 复合便给出截面，故第一条推出其余两条。

若有第二条，令 $W = \ker P$，它不变。对任意 $v$，有

$$v = P(v) + (v - P(v)), \qquad P(v - P(v)) = P(v) - P(v) = 0.$$

故 $V = U + W$；若 $u \in U \cap W$，则 $u = P(u) = 0$，所以是直和。

若有第三条，令 $W = s(V/U)$，它不变。$q(s(\bar v)) = \bar v$ 说明 $s$ 单射。任意 $v$ 满足 $v - s(q(v)) \in U$，故 $V = U + W$。若 $s(\bar v) \in U$，则 $\bar v = q(s(\bar v)) = 0$，所以交为零。第三条也推出第一条。 □

取一个普通向量空间补空间 $W_0$，不预设它不变。适配分解 $V = U \oplus W_0$ 的矩阵为

$$\rho(g) = \begin{pmatrix} A_g & B_g \\ 0 & D_g \end{pmatrix}.$$

$\rho(gh) = \rho(g)\rho(h)$ 中的右上块给出

$$B_{gh} = A_g B_h + B_g D_h.$$

因此商与子空间上的两个表示 $D_g, A_g$ 本身并不决定整个表示；右上块还记录扩张数据。寻找不变补空间，就是寻找合适的补空间变化以同时消去全部 $B_g$。下一节的平均投影将直接完成这件事。

## 9.4 Maschke 定理：把普通投影平均成等变投影

**定理 9.9** (Maschke)**.** *设 $|G| \cdot 1_k \neq 0$，即 $k$ 的特征不整除 $|G|$。则任意有限维 $G$-表示的每个不变子空间都有不变补空间。因此任意有限维表示都完全可约。*

*证明.* 设 $U \le V$ 不变。先取 $U$ 的一组基，扩充为 $V$ 的一组基，再把补充的基向量都映到零，得到普通线性投影 $P_0 : V \to U$，满足 $P_0|_U = \mathrm{id}_U$。由于域中的非零元素可逆，可以定义

$$P = \frac{1}{|G|} \sum_{g \in G} \rho(g) P_0 \rho(g)^{-1}.$$

逐项验证这个平均映射具有所需性质。

首先，$P_0(\rho(g)^{-1}v) \in U$，而 $\rho(g)U = U$，所以每个求和项都落在 $U$，于是 $P(V) \subseteq U$。对 $u \in U$，也有 $\rho(g)^{-1}u \in U$，所以

$$\rho(g) P_0 \rho(g)^{-1} u = \rho(g)\rho(g)^{-1}u = u.$$

取平均得 $P(u) = u$。这还给出 $P^2(v) = P(P(v)) = P(v)$。

其次，对任意 $h \in G$，用 $t = hg$ 重排求和指标，得

$$\begin{aligned} \rho(h) P \rho(h)^{-1} &= \frac{1}{|G|} \sum_{g \in G} \rho(hg) P_0 \rho((hg)^{-1}) \\ &= \frac{1}{|G|} \sum_{t \in G} \rho(t) P_0 \rho(t^{-1}) = P. \end{aligned}$$

故 $P$ 为 $G$-同态。由命题 9.8，$V = U \oplus \ker P$ 是不变直和。

最后对维数归纳以得到完全可约性。零空间为空直和。非零表示若不可约便已完成；否则选 $0 < U < V$，刚才得到 $V = U \oplus W$，两个非零因子的维数都小于 $\dim V$。分别应用归纳，得到各自的不可约直和分解，合起来就是 $V$ 的不可约分解。 □

**注 9.10.** 平均之后得到投影，并不是因为“若干投影的平均仍为投影”：这个说法一般不成立。此处的理由是每项都把 $V$ 映入同一个 $U$，且在 $U$ 上恒等，所以平均映射也满足这两条，进而满足 $P^2 = P$。这是证明中不能省掉的检查。

## 9.5 特征条件为何必要：增广映射的障碍

**定理 9.11** (群代数的半单性判据)**.** *有限群 $G$ 的所有有限维 $k$-表示都完全可约，当且仅当 $|G| \cdot 1_k \neq 0$。*

*证明.* 充分性已由 Maschke 定理证明。为证必要性，设 $|G| \cdot 1_k = 0$。定义增广映射

$$\varepsilon : k[G] \to k, \qquad \varepsilon\left(\sum_{g} a_g e_g\right) = \sum_{g} a_g,$$

并在 $k$ 上取平凡 $G$-作用。左乘 $h$ 只是把基指标置换，所以 $\varepsilon(hv) = \varepsilon(v)$，故 $\varepsilon$ 是满的 $G$-同态，$I = \ker \varepsilon$ 是不变子空间。

若 $I$ 有不变补空间，则由命题 9.8 存在 $G$-同态 $s : k \to k[G]$，使 $\varepsilon s = \mathrm{id}_k$。写 $s(1) = \sum_g a_g e_g$。因为 $k$ 上作用平凡，这个向量必须被全部左乘固定。由正则作用的传递性，所有 $a_g$ 相同，记为 $a$。但这给出

$$1 = \varepsilon(s(1)) = \varepsilon\left(a \sum_{g} e_g\right) = a|G| = 0,$$

矛盾。因此 $I$ 没有不变补空间。

还需说明这也排除了完全可约性本身。若一个表示已是不可约直和 $V = S_1 \oplus \cdots \oplus S_r$，对任意不变子空间 $U$，从这些因子中取一个极大的子集合 $J$ 使 $U \cap \bigoplus_{j\in J} S_j = 0$。若某个 $S_i$ 不包含于 $U + \bigoplus_{j\in J} S_j$，则它与该不变子空间的交是零，因 $S_i$ 不可约；于是可将 $i$ 加入 $J$，矛盾。故所有 $S_i$ 都包含于该和中，从而 $V = U \oplus \bigoplus_{j\in J} S_j$。这证明完全可约表示的每个不变子空间都有补空间。应用于 $k[G]$ 和 $I$，即知 $k[G]$ 不是完全可约表示。 □

**例 9.12** (二维的非分裂模型)**.** 仍取特征 $p$ 下的 $C_p$ 表示 $\rho(s) = I + N$，$Ne_2 = e_1$、$Ne_1 = 0$。子空间 $U = ke_1$ 不变。任意一维补空间都可写成 $k(ae_1 + e_2)$。若它不变，则存在 $\lambda \in k$ 使

$$\rho(s)(ae_1 + e_2) = (a+1)e_1 + e_2 = \lambda(ae_1 + e_2).$$

比较 $e_2$ 系数得 $\lambda = 1$，再比较 $e_1$ 系数得 $a + 1 = a$，矛盾。子表示 $U$ 与商表示 $V/U$ 都平凡，但整个表示不是它们的直和。这也给出了上一节矩阵右上块无法同时消去的具体例子。

## 9.6 实数与复数域上的不变内积

**命题 9.13.** *若 $k = \mathbb{R}$ 或 $\mathbb{C}$，则有限群的每个有限维表示都存在不变正定内积。在复数情形约定内积对第一个变量线性、对第二个变量共轭线性。*

*证明.* 固定一组基，取普通正定内积 $\langle\ ,\ \rangle_0$。定义

$$\langle v, w\rangle_G = \frac{1}{|G|}\sum_{g\in G}\langle \rho(g)v, \rho(g)w\rangle_0.$$

线性、共轭对称性及相应的共轭线性逐项成立。若 $v \neq 0$，则每个 $\rho(g)v \neq 0$，所以每一项 $\langle \rho(g)v, \rho(g)v\rangle_0 > 0$，平均仍严格为正。对 $h \in G$，作 $t = gh$ 的指标替换得

$$\langle \rho(h)v, \rho(h)w\rangle_G = \frac{1}{|G|}\sum_{g}\langle \rho(gh)v, \rho(gh)w\rangle_0 = \langle v, w\rangle_G.$$

因此内积不变。 □

若 $U$ 不变，$v \in U^{\perp}$，则对任意 $u \in U$，

$$\langle \rho(g)v, u\rangle_G = \langle v, \rho(g)^{-1}u\rangle_G = 0,$$

所以 $U^{\perp}$ 也不变，给出 $V = U \oplus U^{\perp}$。这证明实、复情形下 Maschke 的另一条路线。

在这个内积的正交规范基中，不变性逐项等价于

$$A_g^{*}A_g = I$$

(实数域中 $*$ 为转置)。所以有限群的复表示都等价于酉表示，实表示都等价于正交表示。这里的正交补取决于选取的不变内积；不能由补空间存在便声称补空间唯一。

## 9.7 Schur 引理与底域的作用

**定理 9.14** (Schur 引理)**.** 设 $V, W$ 为非零不可约 $k$-表示，则任意非零 $T \in \mathrm{Hom}_G(V,W)$ 都为同构。因此 $\mathrm{End}_G(V)$ 是除环。若 $k$ 代数闭，则

$$\mathrm{End}_G(V) = k\,\mathrm{id}_V, \qquad \dim_k \mathrm{Hom}_G(V,W) = \begin{cases} 1, & V \cong W, \\ 0, & V \not\cong W. \end{cases}$$

这些结论本身不需要 $|G|$ 在 $k$ 中可逆。

证明. $\ker T$ 与 $\mathrm{im}\, T$ 都不变。$T \neq 0$ 使 $\ker T \neq V$、$\mathrm{im}\, T \neq 0$，不可约性因而给出 $\ker T = 0$、$\mathrm{im}\, T = W$。故 $T$ 双射。其逆也交织作用：由 $T\rho(g) = \sigma(g)T$ 左右乘以 $T^{-1}$ 得 $\rho(g)T^{-1} = T^{-1}\sigma(g)$。所以 $\mathrm{End}_G(V)$ 中每个非零元素都有该环中的乘法逆，成为除环。

再设 $k$ 代数闭。任取 $A \in \mathrm{End}_G(V)$。因 $V$ 非零且有限维，特征多项式有根 $\lambda \in k$，所以 $\ker(A - \lambda I) \neq 0$。映射 $A - \lambda I$ 仍为 $G$-自同态；若非零，则按前半部分必为同构，与其核非零矛盾。因此 $A = \lambda I$。

若 $V \not\cong W$，任何非零交织映射都会给出同构，所以同态空间为零。若 $V \cong W$，固定一个同构 $T_0 : V \to W$。任意 $T$ 满足 $T_0^{-1}T \in \mathrm{End}_G(V) = kI$，故 $T = \lambda T_0$，同态空间维数为一。 □

**例 9.15** (实不可约不意味着自同态只有实标量)**.** 令 $C_3 = \langle s \rangle$ 在 $\mathbb{R}^2$ 上作用为

$$R = \rho(s) = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

直接相乘得 $R^2 + R + I = 0$、$R^3 = I$。若有不变实直线，则 $R$ 在该直线上有实特征值 $\lambda$，满足 $\lambda^2 + \lambda + 1 = 0$；该式的判别式为 $-3$，无实根，所以表示实不可约。

记 $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$，则 $R = -\frac{1}{2}I + \frac{\sqrt{3}}{2}J$。实矩阵与 $R$ 交换当且仅当与 $J$ 交换。对 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$，计算 $AJ = JA$ 得 $d = a$、$c = -b$。因此

$$\mathrm{End}_{C_3}(\mathbb{R}^2) = \{xI + yJ : x, y \in \mathbb{R}\} \cong \mathbb{C}.$$

同构由 $x + iy \mapsto xI + yJ$ 给出，因为 $J^2 = -I$。这个除环包含非实标量的自同态，说明 Schur 引理的标量结论必须保留底域条件。

## 9.8 不可约分解的重数与典范等型分量

**定理 9.16.** 设 $k$ 代数闭且 $|G| \cdot 1_k \neq 0$。若

$$V \cong \bigoplus_{i=1}^{r} S_i^{\oplus m_i},$$

其中 $S_i$ 两两不等价且不可约，$m_i > 0$，则

$$m_i = \dim_k \mathrm{Hom}_G(S_i, V).$$

所以不可约因子的同构类型及各重数唯一。每个类型的等型分量

$$V[S_i] = \sum \{U \le V : U \text{ 不变且} U \cong S_i\}$$

不依赖某次分解中的因子选择，并且 $V = \bigoplus_i V[S_i]$。

证明. 选定一次不可约直和分解，并令 $\pi_{j,\ell}$ 为投影到第 $j$ 种类型的第 $\ell$ 个副本的映射。由于每个因子都不变，这些投影都是 $G$-同态。一个 $G$-同态 $T : S_i \to V$ 由全部分量 $\pi_{j,\ell} T$ 唯一确定；反过来，任意给定这些分量，把它们分别包含回 $V$ 再相加就得到 $T$。所以

$$\mathrm{Hom}_G(S_i, V) \cong \bigoplus_{j=1}^{r} \mathrm{Hom}_G(S_i, S_j)^{\oplus m_j}.$$

由 Schur 引理，$j \neq i$ 的项为零，$j = i$ 的每一项为一维，故维数为 $m_i$。右侧原来的内在同态空间与所选分解无关，因此重数唯一。若另一个不可约类型 $T$ 出现在其他分解中，则 $\mathrm{Hom}_G(T, V) \neq 0$，按同样的分量论证，$T$ 必与某个 $S_i$ 等价，所以类型也没有遗漏。

记所选分解中第 $i$ 种类型的全部因子之和为 $V_i$。若 $U \le V$ 且 $U \cong S_i$，则对每个 $j \neq i$，投影 $\pi_{j,\ell}|_U$ 为不同不可约表示间的同态，必为零。因此 $U \le V_i$，故 $V[S_i] \le V_i$。反过来，$V_i$ 的每个副本本身属于定义 $V[S_i]$ 时的求和集合，所以 $V_i \le V[S_i]$。两者相等，且各 $V_i$ 的和是直和，得到结论。 □

**推论 9.17.** 在同样的域与群阶条件下，若 $V \cong \bigoplus_i S_i^{\oplus m_i}$、$W \cong \bigoplus_i S_i^{\oplus n_i}$，允许某些重数为零，则

$$\dim_k \mathrm{Hom}_G(V, W) = \sum_i m_i n_i, \qquad \mathrm{End}_G(V) \cong \prod_i M_{m_i}(k)$$

（第二式为代数同构，但依赖各副本间同构的选择）。特别地，$\dim_k \mathrm{End}_G(V) = \sum_i m_i^2$。

证明. 将同态同时按源和靶的直和分量分块。不同类型间的块全为零，同类型的每个块是一个固定同构的标量倍。所以第 $i$ 种类型贡献一个 $n_i \times m_i$ 标量矩阵，共 $m_i n_i$ 个自由参数。当源靶相同时，复合的分块公式恰为标量矩阵乘法，各类型互不混合，故自同态代数为题设矩阵代数的直积。 □

**注 9.18.** 等型分量唯一，并不意味着其中每个不可约副本唯一。以平凡作用的 $k^2$ 为例，它整体就是唯一的等型分量，而每条直线都是一个不可约副本。只要选两条不同直线就能得到一次直和分解。因此唯一性应表述为同构类型与重数唯一，以及等型分量作为子空间唯一。

## 9.9 循环群的谱投影与交换群的不可约表示

**定理 9.19**（循环群的显式分解）. 令 $C_n = \langle s \rangle$，在 $\mathbb{C}$ 上取 $\zeta = \exp(2\pi i/n)$。对任意表示 $\rho : C_n \to \mathrm{GL}(V)$，定义

$$E_j = \frac{1}{n} \sum_{a=0}^{n-1} \zeta^{-ja} \rho(s)^a, \qquad 0 \le j < n.$$

则 $E_j$ 的像恰为 $\rho(s)$ 的 $\zeta^j$-特征子空间，且

$$E_j E_\ell = \delta_{j\ell} E_j, \qquad \sum_{j=0}^{n-1} E_j = I.$$

因此 $V = \bigoplus_{j=0}^{n-1} E_j V$，而 $C_n$ 的不可约复表示恰为 $n$ 个一维表示 $s \mapsto \zeta^j$。

证明. 记 $A=\rho(s)$，则 $A^n=I$。在求和中将指数 $a+1$ 按模 $n$ 替换为 $b$；因 $\zeta^{jn}=1$，得到

$$AE_j=\frac{1}{n}\sum_{a=0}^{n-1}\zeta^{-ja}A^{a+1}=\frac{\zeta^{j}}{n}\sum_{b=0}^{n-1}\zeta^{-jb}A^{b}=\zeta^{j}E_j.$$

所以 $E_jV$ 包含于 $\zeta^j$-特征子空间。反之，若 $Av=\zeta^{\ell}v$，则

$$E_jv=\frac{1}{n}\sum_{a=0}^{n-1}\zeta^{(\ell-j)a}v=\begin{cases}v, & j=\ell,\\ 0, & j\neq\ell.\end{cases}$$

后一等号的理由是：若 $q=\zeta^{\ell-j}\neq 1$，则 $(1-q)\sum_{a=0}^{n-1}q^a=1-q^n=0$，而 $1-q\neq 0$ 可逆；若 $q=1$，则和为 $n$。特别地，$E_j$ 在自身像上恒等，且在 $E_\ell V$ 上为零，得到投影乘法式，并证明其像恰为相应特征子空间。

再直接求和，

$$\sum_{j}E_j=\frac{1}{n}\sum_{a=0}^{n-1}\left(\sum_{j=0}^{n-1}\zeta^{-ja}\right)A^a=I;$$

因为 $a=0$ 时内和为 $n$，其他 $a$ 时由同一几何级数计算为零。于是 $v=\sum_j E_jv$，各像张成 $V$。若 $\sum_j v_j=0$ 且 $v_j\in E_jV$，施以 $E_\ell$ 得 $v_\ell=0$，所以和为直和。

每个特征子空间上的 $s$ 都是标量作用，因此其中任意直线都不变。若 $V$ 不可约，它只能是某个特征子空间中的一条直线，故一维。反过来每个 $s\mapsto\zeta^j$ 都给出一维表示，并且不同 $j$ 的表示不等价：一维基变换不会改变标量。 □

**命题 9.20.** *有限交换群的每个不可约复表示都是一维表示，因而由群同态 $G\to\mathbb{C}^\times$ 给出。*

证明. 设 $V$ 不可约。交换性给出 $\rho(g)\rho(h)=\rho(h)\rho(g)$，所以每个 $\rho(g)$ 都属于 $\mathrm{End}_G(V)$。由 Schur 引理，$\rho(g)=\lambda_g I$。于是 $V$ 的任意子空间都不变，不可约性迫使 $\dim_{\mathbb{C}}V=1$。同态条件化为 $\lambda_{gh}=\lambda_g\lambda_h$、$\lambda_1=1$，故 $g\mapsto\lambda_g$ 是所述群同态。反过来任意这样的群同态显然定义一维不可约表示。 □

## 9.10　从置换表示中取出一个不可约因子

**例 9.21** ($S_3$ 的二维标准表示)**.** 让 $S_3$ 置换 $\mathbb{C}^3$ 的坐标基，令

$$L=\mathbb{C}(e_1+e_2+e_3),\qquad U=\{x_1e_1+x_2e_2+x_3e_3 : x_1+x_2+x_3=0\}.$$

两者都不变。若 $a(e_1+e_2+e_3)\in U$，则 $3a=0$，故 $a=0$；维数又分别为一和二，所以 $\mathbb{C}^3=L\oplus U$。在 $U$ 上选基 $u=e_1-e_3$、$v=e_2-e_3$。对 $s=(12)$、$t=(123)$，逐个作用得

$$su=v,\quad sv=u,\qquad tu=v-u,\quad tv=-u.$$

所以矩阵为

$$S=\begin{pmatrix}0&1\\1&0\end{pmatrix},\qquad T=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}.$$

相乘可核查 $S^2=I$、$T^3=I$、$STS=T^{-1}$。

为证不可约，若存在不变直线，它在 $S$ 下也不变，故由 $S^2 = I$，必为 $S$ 的某条特征直线。$S$ 的两条特征直线恰为 $\mathbb{C}(u+v)$、$\mathbb{C}(u-v)$。但

$$T(u+v) = -2u + v \notin \mathbb{C}(u+v), \qquad T(u-v) = v \notin \mathbb{C}(u-v).$$

因此两条都不在 $T$ 下不变，矛盾。二维空间没有其他非零真子空间，故 $U$ 不可约。这里直接检查不变直线，没有预先借用尚未证明的特征标判据。

本章只把有限群表示的分解基础建立起来。正则表示中各不可约表示的重数、不可约表示的总数、特征标正交关系、诱导与限制，以及模表示的更深结构，都尚未由上述结果自动完成；后续将分别证明。尤其不能仅凭 $S_3$ 已找到两个一维表示和一个二维表示，就宣布它们已经穷尽，穷尽性还需要正则表示或特征标的维数公式。

## 文献说明

线性表示、群代数与 Maschke 定理的路线核读 James S. Milne，*Group Theory*，Version 4.01 (2025)，第 101–106 页。本章逐项展开平均投影的像、限制、幂等性与等变性，并用增广映射证明特征条件的必要性。Schur 引理与等型分解在正文独立证明，不以模的 Jordan–Hölder 定理代替重数唯一性的证明。循环群的谱投影直接通过有限几何级数计算；实 $C_3$ 与模 $C_p$ 的例子分别说明底域与特征不能从结论中略去。

# 参考文献

[1] James S. Milne. *Group Theory*. Version 4.01, 2025. https://www.jmilne.org/math/CourseNotes/GT.pdf

[2] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2002. 作者公开单章文本, 第 1 章, §1.A. https://pi.math.cornell.edu/~hatcher/AT/ATch1.pdf