抽象代数

《代数学 (三)》书后题答案

Solution Manual

Lucian

Version 1.7, July 20, 2026

前言

这是笔者第二次修抽象代数这门课。第一次低估课程难度了，期中考试前两天才开始学，然后发现学不明白，内容太多了，就退课了。

有一说一，这门课很美，美到有时候我会有一种错觉，觉得这门课是我转来数院的意义。尽管它很难，难到让我对基础数学望而却步。

以后笔者的方向将与这门课再无瓜葛，相信绝大多数的读者也是这样。笔者在这里祝愿大家都能在这门课里获得一些来自头脑风暴或是逻辑诡变的快乐。

虽世殊事异，所以兴怀，其致一也。

顺颂时祺，愿诸事顺遂。

我是北京大学 23 级数院本科生，笔名荒糖，如果大家发现手册中的勘误等等，可以通过如下邮箱联系我，未经许可不可借此资料获利；或许你仍会烦恼，但愿你终将自由如风！

- **Email:** 2300011821@stu.pku.edu.cn, 947216434@qq.com

这个方框用于突出解答手册中的题目描述，为区分每一道习题及其对应解答提供清晰的视觉提示。

这个方框用于呈现重要引理、中间结论或关键推导过程，以辅助习题的求解。

这个方框用于提供额外说明、见解或对问题及解答的补充性解释与澄清。

目录

1 再探群、环、域 **2**

1.1 运算与运算法则 . . . 2
1.2 半群与群 . . . 7
1.3 环与域 . . . 10
1.4 整数模 n 的剩余类环 . . . 16

2 群的基本性质与作用 **19**

2.1 对称群和交错群 . . . 19
2.2 子群与同态 . . . 23
2.3 循环群 . . . 35
2.4 群在集合上的作用 . . . 45
2.5 陪集、指数、*Lagrange* 定理 . . . 49
2.6 轨道长度和类方程 . . . 53
2.7 正规子群与商群 . . . 57
2.8 同态基本定理 . . . 63
2.9 自由群 . . . 68

3 群的结构 **73**

3.1 群的直积 . . . 73
3.2 Sylow 定理 . . . 79
3.3 有限交换群的结构 . . . 88
3.4 可解群 . . . 97
3.5 Jordan-Holder 定理 . . . 102

1 再探群、环、域

1.1 运算与运算法则

1. 判断下列论断是否正确，若正确，给出简要证明，否则举反例说明：

(1) 设 $\mathbb{R}^+$ 是所有正实数构成的集合，

$$\begin{aligned}\mathbb{R} &\longrightarrow \mathbb{R}^+,\\ y &\longmapsto y^2\end{aligned}$$

是一个映射；

(2) 在 $\mathbb{R}$ 中，对任意 $x, y \in \mathbb{R}$，定义

$$xRy \Longleftrightarrow |x-y| \leqslant 3,$$

关系 R 是一个等价关系；

(3) 在 $\mathbb{Z}$ 中，对任意 $m, n \in \mathbb{Z}$，定义

$$mRn \Longleftrightarrow 2 \nmid m-n,$$

关系 R 不是一个等价关系；

(4) 在 n 阶复矩阵集合 $\mathbb{C}^{n\times n}$ 中，对任意 $M, N \in \mathbb{C}^{n\times n}$，定义

$$MRN \Longleftrightarrow \text{存在} P, Q \in \mathbb{C}^{n\times n}\text{，使得} M = PNQ,$$

关系 R 是一个等价关系；

(5) 一个非空集合上的关系可以同时是等价关系和偏序关系。

解

(1) 该论断不正确。

因为 $0 \in \mathbb{R}$，但

$$0^2 = 0 \notin \mathbb{R}^+.$$

因此，对应法则 $y \mapsto y^2$ 不能将定义域 $\mathbb{R}$ 中的每一个元素都对应到陪域 $\mathbb{R}^+$ 中，故它不是从 $\mathbb{R}$ 到 $\mathbb{R}^+$ 的映射。

(2) 该论断不正确。

关系 R 不具有传递性。例如，取

$$x = 0, \qquad y = 2, \qquad z = 4.$$

则

$$|x-y| = 2 \leqslant 3, \qquad |y-z| = 2 \leqslant 3,$$

所以 xRy 且 yRz；但是

$$|x-z| = 4 > 3,$$

故 $x \not R z$。因此 R 不是等价关系。

(3) 该论断正确。

对任意 $m \in \mathbb{Z}$，都有

$$m - m = 0, \qquad 2 \mid 0.$$

因此

$$2 \nmid m - m$$

不成立，即 $m \not R\, m$。所以关系 R 不具有自反性，从而不是等价关系。

(4) 该论断不正确。

取

$$M = 0, \qquad N = I_n.$$

令

$$P = 0, \qquad Q = I_n,$$

则

$$M = 0 = 0 \cdot I_n \cdot I_n = PNQ,$$

故 MRN。

但是不可能存在 P, Q 使得

$$I_n = P0Q.$$

于是 $N \not R\, M$，说明关系 R 不具有对称性，故它不是等价关系。

(5) 该论断正确。

设 X 是任意非空集合，在 X 上定义恒等关系

$$\Delta_X = \{(x, x) \mid x \in X\},$$

即

$$x \Delta_X y \iff x = y.$$

等号关系具有自反性、对称性和传递性，故 Δ_X 是等价关系；同时，等号关系也具有自反性、反对称性和传递性，故 Δ_X 是偏序关系。

□

2. 设 A, B 是两个集合，$f\colon A \to B$ 和 $g\colon B \to A$ 是映射。如果

$$gf = \mathrm{id}_A,$$

那么称 g 为 f 的一个左逆映射；如果

$$fg = \mathrm{id}_B,$$

那么称 g 为 f 的一个右逆映射。如果 g 既是 f 的左逆映射，又是 f 的右逆映射，那么称 g 为 f 的逆映射。证明：

(1) f 有左逆映射当且仅当 f 是单射，f 有右逆映射当且仅当 f 是满射，从而 f 有逆映射当且仅当 f 是双射；

(2) 若 f 有左逆映射 g，同时又有右逆映射 h，则 $g = h$。

解

(1) 若 $gf = \mathrm{id}_A$，则

$$f(x) = f(y) \Longrightarrow x = gf(x) = gf(y) = y,$$

故 f 为单射。反之，若 f 为单射，定义

$$g(f(x)) = x,$$

并在 $B \setminus f(A)$ 上任意定义 g，则 $gf = \mathrm{id}_A$。

若 $fg = \mathrm{id}_B$，则对任意 $y \in B$，

$$y = fg(y) \in f(A),$$

故 f 为满射。反之，若 f 为满射，对每个 $y \in B$ 任取 $x_y \in f^{-1}(y)$，令 $g(y) = x_y$，则 $fg = \mathrm{id}_B$。

因此，f 有逆映射当且仅当 f 是双射。

(2) 由

$$gf = \mathrm{id}_A, \qquad fh = \mathrm{id}_B,$$

可得

$$g = g\,\mathrm{id}_B = g(fh) = (gf)h = \mathrm{id}_A\, h = h.$$

□

3. 设 A, B 是两个有限集合，$|A| = m$，$|B| = n$，证明：

(1) 映射 $f\colon A \to B$ 的个数为 n^m；

(2) 若 $f\colon A \to B$ 为单射，则有 $m \leqslant n$；进一步地，若 $m \leqslant n$，则从 A 到 B 的单射个数为

$$n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!};$$

(3) 若 $f\colon A \to B$ 为满射，则有 $m \geqslant n$；进一步地，若 $m \geqslant n$，则从 A 到 B 的满射个数为

$$\sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} j^m;$$

(4) 设 $m = n$，则从 A 到 B 的单射也是满射，从 A 到 B 的满射也是单射，从而从 A 到 B 的单射或满射都是双射。

解

(1) 对 A 中每个元素，其像均有 n 种选择，且各元素的选择相互独立，故映射总数为

$$n^m.$$

(2) 若 f 为单射，则 A 中的 m 个元素有互不相同的像，故

$$m \leqslant n.$$

当 $m \leqslant n$ 时，依次选择 A 中各元素的像，选择数为

$$n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!}.$$

(3) 若 f 为满射，则 B 中每个元素至少有一个原像，故

$$m \geqslant n.$$

当 $m \geqslant n$ 时，由容斥原理，满射个数为

$$n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \cdots = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} j^m.$$

(4) 设 $m=n$。若 f 为单射，则 $f(A)$ 含有 n 个元素，而 $f(A)\subseteq B$ 且 $|B|=n$，故

$$f(A)=B,$$

所以 f 为满射。

若 f 为满射，则 B 中每个元素至少有一个原像。由于 A 与 B 的元素个数相等，故每个元素恰有一个原像，所以 f 为单射。

因此，当 $m=n$ 时，单射、满射与双射三者等价。

□

4. 在 $\mathbb{Z}$ 中，考虑如下定义的两个等价关系 $\sim_1$ 和 $\sim_2$。对任意 $m,n\in\mathbb{Z}$，定义

$$m\sim_1 n \iff 6\mid m-n, \qquad m\sim_2 n \iff 2\mid m-n.$$

(1) 描述 $\sim_1$ 诱导的 $\mathbb{Z}$ 的划分 $\mathbb{Z}_6$ 和 $\sim_2$ 诱导的 $\mathbb{Z}$ 的划分 $\mathbb{Z}_2$；

(2) 以上两个划分中，是否存在一个比另一个更细？为什么？

解

(1) 有

$$\mathbb{Z}_6=\{[0]_6,[1]_6,[2]_6,[3]_6,[4]_6,[5]_6\}, \qquad [r]_6=r+6\mathbb{Z},$$

以及

$$\mathbb{Z}_2=\{[0]_2,[1]_2\}, \qquad [r]_2=r+2\mathbb{Z}.$$

(2) $\mathbb{Z}_6$ 比 $\mathbb{Z}_2$ 更细。事实上，

$$[0]_6,[2]_6,[4]_6\subseteq[0]_2, \qquad [1]_6,[3]_6,[5]_6\subseteq[1]_2.$$

这也可由

$$6\mid m-n \Longrightarrow 2\mid m-n$$

直接得到。

□

5. 判断以下给出的集合上的运算是否满足结合律或者交换律。若答案为否，请举例说明原因：

集合	运算
$\mathbb{Z}$	$a*b=a-b$
$\mathbb{Z}^+$	$a*b=2^{ab}$
$\mathbb{C}^{2\times2}$	$M*N=MN-NM$

解

(1) 在 $\mathbb{Z}$ 上，运算既不满足结合律，也不满足交换律。例如，

$$(0*0)*1=-1, \qquad 0*(0*1)=1,$$

且

$$1*0=1, \qquad 0*1=-1.$$

(2) 在 $\mathbb{Z}^+$ 上，运算满足交换律，因为

$$a * b = 2^{ab} = 2^{ba} = b * a.$$

但不满足结合律，例如

$$(1 * 2) * 2 = 4 * 2 = 2^8, \qquad 1 * (2 * 2) = 1 * 16 = 2^{16}.$$

(3) 在 $\mathbb{C}^{2\times 2}$ 上，运算既不满足结合律，也不满足交换律。令

$$M = E_{11}, \qquad N = E_{12}, \qquad P = E_{21}.$$

则

$$(M * N) * P = E_{11} - E_{22}, \qquad M * (N * P) = 0,$$

故结合律不成立；又

$$N * P = E_{11} - E_{22}, \qquad P * N = E_{22} - E_{11},$$

故交换律不成立。

□

6. 设

$$A = \mathbb{Q} \setminus \{-1\},$$

对于 $a, b \in A$，定义

$$a \circ b = a + b + ab.$$

证明 $\circ$ 是集合 A 上的运算，且满足交换律和结合律。进一步判断 A 中是否有单位元，元素是否都有逆元；若有，求出 $a \in A$ 的逆元。

解 注意到

$$(a \circ b) + 1 = (a + 1)(b + 1) \neq 0,$$

故 $a \circ b \neq -1$，所以 $\circ$ 是 A 上的运算。

交换律显然成立。又

$$(a \circ b) \circ c = a + b + c + ab + ac + bc + abc = a \circ (b \circ c),$$

故结合律成立。

由

$$a \circ 0 = a$$

知单位元为 0。设 a 的逆元为 b，则

$$a + b + ab = 0,$$

从而

$$b = -\frac{a}{a+1}.$$

该元素属于 A，故每个 $a \in A$ 都有逆元

$$a^{-1} = -\frac{a}{a+1}.$$

□

7. 考虑 $\mathbb{Q}$ 上的等价关系

$$u \sim v \iff u - v \in \mathbb{Z}.$$

证明 $\mathbb{Q}$ 上的加法与等价关系 $\sim$ 相容。

解 若

$$u_1 \sim u_2, \qquad v_1 \sim v_2,$$

则

$$u_1 - u_2 \in \mathbb{Z}, \qquad v_1 - v_2 \in \mathbb{Z}.$$

因此

$$(u_1 + v_1) - (u_2 + v_2) = (u_1 - u_2) + (v_1 - v_2) \in \mathbb{Z},$$

故

$$u_1 + v_1 \sim u_2 + v_2.$$

所以 $\mathbb{Q}$ 上的加法与 $\sim$ 相容。 □

1.2 半群与群

1. 设 S 为幺半群，$a, b \in S$，若 ab 可逆，是否有 a 和 b 均可逆？证明或举出反例。

解 不一定。设 V 是以 $\{e_1, e_2, \ldots\}$ 为基的无限维向量空间，在 $\mathrm{End}(V)$ 中定义

$$a(e_1) = 0, \qquad a(e_{n+1}) = e_n, \qquad b(e_n) = e_{n+1}.$$

则

$$ab = \mathrm{id}_V,$$

故 ab 可逆；但 a 不为单射，b 不为满射，因而 a, b 均不可逆。 □

2. 设 S 为幺半群，$a_1, a_2, \ldots, a_m \in S$ 且两两可交换，证明 $a_1 a_2 \cdots a_m$ 可逆当且仅当 $a_1, a_2, \ldots, a_m$ 均可逆。

解 若各 a_i 均可逆，则

$$(a_1 a_2 \cdots a_m)^{-1} = a_m^{-1} \cdots a_2^{-1} a_1^{-1},$$

故其乘积可逆。

反之，设

$$p = a_1 a_2 \cdots a_m$$

可逆。固定 i，令

$$b_i = \prod_{j \neq i} a_j.$$

由各元素两两可交换，有 $p = a_i b_i = b_i a_i$。于是

$$a_i (b_i p^{-1}) = p p^{-1} = 1, \qquad (p^{-1} b_i) a_i = p^{-1} p = 1.$$

故 a_i 可逆。由于 i 任意，所有 a_i 均可逆。 □

3. 设 A 是一个非空集合，其上有一个运算，e_l（或 e_r）$\in A$。若对任意 $a \in A$，均有

$$e_l a = a \qquad (\text{或} ae_r = a),$$

则称 e_l（或 e_r）为 A 的一个左（或右）单位元。对于 $a \in A$，若存在 $b \in A$ 使得

$$ba = e_l \qquad (\text{或} ab = e_r),$$

则称 b 为 a 的一个左（或右）逆元。

(1) 若 A 中运算满足结合律，存在左单位元，且 A 中每个元素都有左逆元，证明 A 是一个群；

(2) 若 A 中运算满足结合律，存在右单位元，且 A 中每个元素都有右逆元，证明 A 是一个群。

解

(1) 设 e 为左单位元。对任意 $a \in A$，取 $b, c \in A$ 使得

$$ba = e, \qquad cb = e.$$

则

$$c = ce = c(ba) = (cb)a = ea = a,$$

故 $ab = cb = e$。进而

$$ae = a(ba) = (ab)a = ea = a.$$

因此 e 是单位元，且 b 是 a 的逆元，故 A 是群。

(2) 设 e 为右单位元。对任意 $a \in A$，取 $b, c \in A$ 使得

$$ab = e, \qquad bc = e.$$

则

$$c = ec = (ab)c = a(bc) = ae = a,$$

故 $ba = bc = e$。进而

$$ea = (ab)a = a(ba) = ae = a.$$

因此 e 是单位元，且 b 是 a 的逆元，故 A 是群。

□

4. 设 G 为具有一个运算的非空集合，已知该运算满足结合律，并且对于 G 中任意两个元素 a, b，方程

$$ax = b \qquad \text{和} \qquad xa = b$$

都在 G 中有解，证明 G 是一个群。

解 固定 $a \in G$，取 $e_l, e_r \in G$ 使得

$$e_l a = a, \qquad ae_r = a.$$

对任意 $x \in G$，分别取 $u, v \in G$ 使得 $au = x$、$va = x$，则

$$e_l x = e_l(au) = (e_l a)u = x,$$

且

$$xe_r = (va)e_r = v(ae_r) = x.$$

故 e_l 是左单位元，e_r 是右单位元，从而

$$e_l = e_l e_r = e_r.$$

记公共单位元为 e。

对任意 $a \in G$，取 $x, y \in G$ 使得

$$ax = e, \qquad ya = e.$$

则

$$y = ye = y(ax) = (ya)x = ex = x.$$

因此每个元素都有逆元，故 G 是群。 □

5. 设 G 是一个群，$a, b \in G$，如果

$$aba^{-1} = b^r,$$

其中 r 是一个整数，证明对任意正整数 i，有

$$a^i b a^{-i} = b^{r^i}.$$

解 对 i 作归纳。当 $i = 1$ 时结论即为已知条件。

若

$$a^i b a^{-i} = b^{r^i},$$

则

$$a^{i+1} b a^{-(i+1)} = a(a^i b a^{-i})a^{-1} = a b^{r^i} a^{-1} = (aba^{-1})^{r^i} = (b^r)^{r^i} = b^{r^{i+1}}.$$

故对任意正整数 i，均有

$$a^i b a^{-i} = b^{r^i}.$$

□

6. 设 G 是一个群，如果对于任意 $a, b \in G$ 都有

$$(ab)^2 = a^2 b^2,$$

证明 G 为交换群。

解 由题设

$$abab = aabb.$$

两边左乘 a^{-1}、右乘 b^{-1}，得

$$ba = ab.$$

由于 a, b 任意，故 G 为交换群。 □

7. 设 $n \geqslant 3$，在 n 元对称群 S_n 中找两个元素 σ, τ，使得

$$\sigma\tau \neq \tau\sigma.$$

由此可知 S_n 不是交换群。

解 取

$$\sigma = (12), \qquad \tau = (23).$$

则

$$(\sigma\tau)(1)=2,\qquad (\tau\sigma)(1)=3,$$

故

$$\sigma\tau\neq\tau\sigma.$$

因此当 $n\geqslant 3$ 时，S_n 不是交换群。 □

1.3 环与域

1. 设 R 为交换环，对于任意 $a,b\in R$，定义

$$a\oplus b=a+b-1,\qquad a\odot b=a+b-ab.$$

证明 R 在运算 $\oplus,\odot$ 下也构成一个交换环。

解 首先，显然 $a\oplus b, a\odot b\in R$。

对于运算 $\oplus$，有

$$(a\oplus b)\oplus c=a+b+c-2=a\oplus(b\oplus c),$$

且

$$a\oplus b=b\oplus a.$$

又

$$a\oplus 1=a,$$

故 $\oplus$ 的零元为 1；并且

$$a\oplus(2-a)=1,$$

故 a 关于 $\oplus$ 的负元为 $2-a$。因此 $(R,\oplus)$ 为交换群。

对于运算 $\odot$，由 R 的乘法交换律，

$$a\odot b=b\odot a.$$

又

$$(a\odot b)\odot c=a+b+c-ab-ac-bc+abc=a\odot(b\odot c),$$

故 $\odot$ 满足结合律。

最后，

$$\begin{aligned}a\odot(b\oplus c)&=a+(b+c-1)-a(b+c-1)\\&=2a+b+c-ab-ac-1\\&=(a\odot b)\oplus(a\odot c).\end{aligned}$$

由交换律，另一侧分配律也成立。

因此 R 在运算 $\oplus,\odot$ 下构成交换环。

也可以定义

$$\varphi\colon R\to R,\qquad \varphi(a)=1-a.$$

则

$$\varphi(a\oplus b)=\varphi(a)+\varphi(b),\qquad \varphi(a\odot b)=\varphi(a)\varphi(b).$$

因此新定义的两个运算实际上只是通过双射 $a\mapsto 1-a$ 将原来的加法和乘法重新表示出来。

□

2. 设 R 为环，定义

$$a-b=a+(-b),$$

证明：对于任意 $a,b,c\in R$，有

$$-(a+b)=(-a)+(-b)=-a-b,$$

$$-(a-b)=(-a)+b,$$

$$-(ab)=(-a)b=a(-b),$$

$$(-a)(-b)=ab,$$

$$a(b-c)=ab-ac.$$

解 由加法逆元的唯一性及分配律，

$$(a+b)+[(-a)+(-b)]=0,$$

故

$$-(a+b)=(-a)+(-b)=-a-b.$$

又

$$-(a-b)=-[a+(-b)]=(-a)+b.$$

由于

$$ab+(-a)b=(a-a)b=0,$$

且

$$ab+a(-b)=a(b-b)=0,$$

故

$$-(ab)=(-a)b=a(-b).$$

于是

$$(-a)(-b)=-[a(-b)]=-(-ab)=ab.$$

最后，

$$a(b-c)=a[b+(-c)]=ab+a(-c)=ab-ac.$$

□

3. 设 R 为环，$a,b\in R$，且 a,b 可交换，证明二项式定理：对任意正整数 n，

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

解 对 n 作归纳。当 $n=1$ 时显然成立。

假设结论对 n 成立，则由 $ab=ba$，

$$\begin{aligned}(a+b)^{n+1}&=(a+b)^n(a+b)\\&=\sum_{k=0}^{n}\binom{n}{k}a^{n+1-k}b^k+\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1}\\&=\sum_{k=0}^{n+1}\left[\binom{n}{k}+\binom{n}{k-1}\right]a^{n+1-k}b^k\\&=\sum_{k=0}^{n+1}\binom{n+1}{k}a^{n+1-k}b^k.\end{aligned}$$

故结论对任意正整数 n 成立。 □

4. 给出一个没有乘法消去律的环的例子。

解 取环 $\mathbb{Z}_6$。由于

$$2 \cdot 1 = 2 \cdot 4 = 2 \pmod 6,$$

但

$$1 \neq 4,$$

故 $\mathbb{Z}_6$ 中乘法消去律不成立。 □

5. 证明整环中有消去律。

解 设 R 为整环，$a, b, c \in R$，且 $a \neq 0$。若

$$ab = ac,$$

则

$$a(b - c) = 0.$$

由于整环无零因子且 $a \neq 0$，故

$$b - c = 0,$$

即

$$b = c.$$

同理可证右消去律。 □

6. 设 R 为环，$a \in R$，$a \neq 0$，且存在 $b \in R$，$b \neq 0$ 使得

$$aba = 0,$$

证明 a 是 R 的一个左零因子或右零因子。

解 若 $ab = 0$，由于 $b \neq 0$，故 a 是左零因子。
若 $ab \neq 0$，则

$$(ab)a = 0,$$

故 a 是右零因子。 □

7. 设 R 为有限环，$a, b \in R$ 且

$$ab = 1,$$

证明

$$ba = 1.$$

解 考虑映射

$$L_a \colon R \to R, \qquad x \mapsto ax.$$

由 $ab = 1$，对任意 $x \in R$，

$$x = abx = a(bx),$$

故 L_a 为满射。由于 R 有限，L_a 也是单射。

又

$$a(ba) = a = a \cdot 1,$$

故由单射性得

$$ba = 1.$$

□

8. 设 R 为环，$a, b \in R$ 且

$$ab = 1, \qquad ba \neq 1,$$

证明有无穷多个 $x \in R$ 满足

$$ax = 1.$$

解 令

$$c = 1 - ba \neq 0.$$

则

$$ac = a - aba = 0, \qquad cb = b - bab = 0.$$

对 $n = 0, 1, 2, \ldots$，令

$$x_n = b + ca^n.$$

则

$$ax_n = ab + aca^n = 1.$$

下面证明 x_n 两两不同。若 $m < n$ 且 $x_m = x_n$，则

$$ca^m = ca^n.$$

两边右乘 b^n，利用 $a^k b^k = 1$，得

$$cb^{n-m} = c.$$

但 $cb = 0$，故左边为 0，从而 $c = 0$，矛盾。

因此 $\{x_n\}_{n \geqslant 0}$ 两两不同，故满足 $ax = 1$ 的 x 有无穷多个。 □

9. 设 R 为环，$a \in R$。如果存在正整数 n 使得

$$a^n = 0,$$

就称 a 为幂零元。证明若 a 为幂零元，则 $1 - a$ 可逆。

解 设 $a^n = 0$，则

$$(1 - a)(1 + a + \cdots + a^{n-1}) = 1 - a^n = 1,$$

且

$$(1 + a + \cdots + a^{n-1})(1 - a) = 1 - a^n = 1.$$

故

$$(1 - a)^{-1} = 1 + a + \cdots + a^{n-1}.$$

□

10. 设 R 为环，$a,b\in R$。设 $1-ab$ 可逆，证明 $1-ba$ 也可逆并求出

$$(1-ba)^{-1}.$$

解 令

$$c=(1-ab)^{-1}.$$

则

$$(1-ab)c=c(1-ab)=1.$$

直接计算得

$$(1-ba)(1+bca)=1,$$

且

$$(1+bca)(1-ba)=1.$$

因此

$$\boxed{(1-ba)^{-1}=1+b(1-ab)^{-1}a}.$$

□

11. 证明有限整环是域。

解 设 R 为有限整环，$a\in R$，$a\neq 0$。考虑映射

$$f\colon R\to R,\qquad x\mapsto ax.$$

若 $ax=ay$，则

$$a(x-y)=0.$$

由 R 无零因子知 $x=y$，故 f 为单射。由于 R 有限，f 也是满射，故存在 $b\in R$ 使

$$ab=1.$$

因此每个非零元素均可逆，故 R 是域。 □

12. 设 R 为除环，$a,b\in R$ 且 $ab\neq 0,1$，证明华罗庚等式

$$a-\big(a^{-1}+(b^{-1}-a)^{-1}\big)^{-1}=aba.$$

解 由 $ab\neq 0,1$，各逆元均存在。注意

$$\begin{aligned}a^{-1}+(b^{-1}-a)^{-1}&=(b^{-1}-a)^{-1}\big((b^{-1}-a)+a\big)a^{-1}\\&=(b^{-1}-a)^{-1}b^{-1}a^{-1}.\end{aligned}$$

故

$$\big(a^{-1}+(b^{-1}-a)^{-1}\big)^{-1}=ab(b^{-1}-a)=a-aba.$$

于是

$$a-\big(a^{-1}+(b^{-1}-a)^{-1}\big)^{-1}=aba.$$

□

13. 设 R 为一个无零因子环，$e \in R$ 满足对所有 $a \in R$ 有

$$ea = a,$$

证明 e 为 R 的单位元。

解 取 $a = e$，得

$$e^2 = e.$$

于是对任意 $a \in R$，

$$(ae - a)e = ae^2 - ae = 0.$$

因 $e \neq 0$ 且 R 无零因子，故

$$ae - a = 0,$$

即 $ae = a$。结合已知 $ea = a$，故 e 为单位元。 □

14. 设 D 是一个整环，在 D 中解方程

$$x^2 = 1.$$

解 由

$$x^2 - 1 = (x - 1)(x + 1) = 0,$$

且 D 无零因子，故

$$x - 1 = 0 \quad \text{或} \quad x + 1 = 0.$$

因此

$$\boxed{x = 1 \quad \text{或} \quad x = -1}.$$

□

15. 设 R 为环，若 $u \in R$ 存在右逆元但不唯一，证明 u 有无穷多个右逆元。

解 取 $v \in R$ 使

$$uv = 1.$$

由于右逆元不唯一，必有

$$vu \neq 1.$$

令

$$c = 1 - vu \neq 0.$$

则

$$uc = u - uvu = 0.$$

对 $n = 0, 1, 2, \ldots$，令

$$v_n = v + cu^n.$$

则

$$uv_n = uv + ucu^n = 1,$$

故 v_n 均为 u 的右逆元。

若 $m < n$ 且 $v_m = v_n$，则

$$cu^m = cu^n.$$

右乘 v^n，得

$$cv^{n-m} = c.$$

但

$$cv = (1 - vu)v = 0,$$

故 $c = 0$，矛盾。因此 v_n 两两不同，故 u 有无穷多个右逆元。 □

1.4 整数模 n 的剩余类环

1. 证明在 p 元域 $\mathbb{Z}_p$ 中有

$$(a+b)^{p^k} = a^{p^k} + b^{p^k},$$

其中 $a, b \in \mathbb{Z}_p$，k 为任意正整数。

解 由于对 $1 \leqslant j \leqslant p-1$，

$$p \mid \binom{p}{j},$$

故在 $\mathbb{Z}_p$ 中

$$(a+b)^p = a^p + b^p.$$

反复应用此式即得

$$(a+b)^{p^k} = \left(a^{p^{k-1}} + b^{p^{k-1}}\right)^p = a^{p^k} + b^{p^k}.$$

□

2. 给出一个有限非交换群 G，使得对于任意 $a \in G$ 均有

$$a^4 = e.$$

解 取四元数群

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

它是非交换群，例如

$$ij = k, \qquad ji = -k.$$

又其中每个元素的阶均为 $1, 2$ 或 4，故对任意 $a \in Q_8$，

$$a^4 = e.$$

□

四元数群 Q_8：

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\},$$

其中乘法满足

$$i^2 = j^2 = k^2 = -1,$$

以及

$$ij = k, \qquad jk = i, \qquad ki = j,$$

交换次序则变号：

$$ji = -k, \qquad kj = -i, \qquad ik = -j.$$

3. 求出方程

$$x^2 - 1 = 0$$

在环 $\mathbb{Z}_{360}$ 中的全部解。

解 方程等价于

$$360 \mid (x-1)(x+1).$$

由于

$$360 = 8 \cdot 9 \cdot 5,$$

先分别考虑这三个因子。

模 8 时，

$$x^2 \equiv 1 \pmod 8$$

当且仅当 x 为奇数。

又因为

$$\gcd(x-1, x+1) \mid 2,$$

所以 3 和 5 不可能同时整除 $x-1$ 与 $x+1$。因此

$$9 \mid (x-1) \quad 或 \quad 9 \mid (x+1),$$

以及

$$5 \mid (x-1) \quad 或 \quad 5 \mid (x+1).$$

即

$$x \equiv \pm 1 \pmod 9, \qquad x \equiv \pm 1 \pmod 5.$$

将四种情况直接合并，可得

$$x \equiv 1, 19, 26, 44 \pmod{45}.$$

再要求 x 为奇数，在 $0 \leqslant x < 360$ 中得到

$$\boxed{x = \overline{1}, \overline{19}, \overline{71}, \overline{89}, \overline{91}, \overline{109}, \overline{161}, \overline{179}, \overline{181}, \overline{199}, \overline{251}, \overline{269}, \overline{271}, \overline{289}, \overline{341}, \overline{359}}.$$

□

4. 证明群 $U(3^5)$ 中一定有一个元素 g，使得 $U(3^5)$ 中每个元素都是 g 的幂。这个结论对群 $U(2^5)$ 是否正确？

解 有

$$|U(3^5)| = \varphi(3^5) = 162.$$

取 $g = 2$。由

$$2^{54} \equiv 82 \neq 1 \pmod{243}, \qquad 2^{81} \equiv -1 \neq 1 \pmod{243},$$

而 $2^{162} \equiv 1 \pmod{243}$，故

$$o(2) = 162.$$

因此

$$U(3^5) = \langle 2 \rangle.$$

对 $U(2^5) = U(32)$，结论不成立。事实上 $|U(32)| = 16$，而对任意奇数 a 都有

$$a^8 \equiv 1 \pmod{32}.$$

故其中不存在阶为 16 的元素，所以 $U(32)$ 不是循环群。 □

5. 在 $\mathbb{Z}_{29}$ 中计算

$$\overline{28}^{960}.$$

解 由于

$$\overline{28} = \overline{-1},$$

故

$$\overline{28}^{960} = \overline{(-1)^{960}} = \boxed{\overline{1}}.$$

□

2 群的基本性质与作用

2.1 对称群和交错群

1. 设 $n \geqslant 3$，$\sigma \in S_n$ 且

$$\sigma \neq \mathrm{id}_{[n]},$$

证明存在 $\tau \in S_n$ 使得

$$\sigma\tau \neq \tau\sigma.$$

解 由于 $\sigma \neq \mathrm{id}_{[n]}$，存在 i 使

$$\sigma(i) = j \neq i.$$

因 $n \geqslant 3$，可取 $k \neq i, j$。令

$$\tau = (jk).$$

则

$$(\sigma\tau)(i) = \sigma(i) = j,$$

而

$$(\tau\sigma)(i) = \tau(j) = k.$$

由于 $j \neq k$，故

$$\sigma\tau \neq \tau\sigma.$$

□

2. 设 $n \geqslant 3$，$\sigma = (12\cdots n)$，k 为正整数，计算 σ^k。进一步地，对任意 $\tau \in S_n$，若 τ 与 σ 可交换，证明 τ 为 σ 的幂。

解 对任意 i，

$$\sigma^k(i) \equiv i + k \pmod{n}.$$

若

$$\tau\sigma = \sigma\tau,$$

则

$$\tau\sigma\tau^{-1} = \sigma.$$

另一方面，由轮换的共轭公式，

$$\tau\sigma\tau^{-1} = (\tau(1)\ \tau(2)\ \cdots\ \tau(n)).$$

故

$$(\tau(1)\ \tau(2)\ \cdots\ \tau(n)) = (1\ 2\ \cdots\ n).$$

设

$$\tau(1) = \sigma^r(1).$$

由于同一个轮换从任意位置开始书写均相同，由 $(1\,2\,\cdots\,n) = \big(\sigma^r(1)\,\sigma^r(2)\,\cdots\,\sigma^r(n)\big)$，必有

$$\tau(i) = \sigma^r(i), \qquad i = 1, \ldots, n.$$

因此

$$\boxed{\tau = \sigma^r}.$$

□

3. 证明：如果一个置换是不相交的等长度的轮换的乘积，那么该置换一定可以写为一个轮换的幂。

解 设

$$\sigma = (a_{11}\cdots a_{1m})(a_{21}\cdots a_{2m})\cdots(a_{r1}\cdots a_{rm}).$$

令

$$\tau = (a_{11}\ a_{21}\cdots a_{r1}\ a_{12}\ a_{22}\cdots a_{r2}\ \cdots\ a_{1m}\ a_{2m}\cdots a_{rm}).$$

则 τ^r 将每个 a_{ij} 映为 $a_{i,j+1}$，故

$$\boxed{\sigma = \tau^r}.$$

□

4. 把 S_9 中元素

$$(147)(789)(39)(942)(356)$$

写成不相交轮换的乘积。

解 按从右向左作用计算各元素的像：

$$1 \mapsto 4 \mapsto 2 \mapsto 3 \mapsto 5 \mapsto 6 \mapsto 1,$$

以及

$$7 \mapsto 8 \mapsto 9 \mapsto 7.$$

故

$$\boxed{(147)(789)(39)(942)(356) = (142356)(789)}.$$

□

5. 找出 S_8 中与

$$\sigma = (123)(45) \in S_8$$

交换的所有元素。

解 设 $\tau \in S_8$ 与 σ 交换，则

$$\tau\sigma\tau^{-1} = \sigma.$$

由轮换的共轭公式，

$$\tau\sigma\tau^{-1} = (\tau(1)\,\tau(2)\,\tau(3))(\tau(4)\,\tau(5)).$$

因此

$$(\tau(1)\,\tau(2)\,\tau(3))(\tau(4)\,\tau(5)) = (123)(45).$$

由不相交轮换分解的唯一性，必有

$$\{\tau(1),\tau(2),\tau(3)\} = \{1,2,3\}, \qquad \{\tau(4),\tau(5)\} = \{4,5\}.$$

故由第 2 题结论，τ 在 $\{1,2,3\}$ 上只能是

$$(123)^i, \qquad i = 0,1,2,$$

在 $\{4,5\}$ 上只能是

$$(45)^j, \qquad j = 0,1,$$

而在固定点集合 $\{6,7,8\}$ 上可以任意置换。

因此所有满足条件的元素恰为

$$\boxed{\tau=(123)^i(45)^j\rho,\qquad i=0,1,2,\quad j=0,1,\quad \rho\in S_{\{6,7,8\}}}.$$

共有 $3\cdot 2\cdot 3!=36$ 个。 □

6. 设 p 为素数，$\sigma\in S_p$ 且 σ 不是恒等变换，若 σ^p 为恒等变换，证明 σ 是一个 p-轮换。

解 由 $\sigma^p=\mathrm{id}$，知

$$o(\sigma)\mid p.$$

又 $\sigma\neq\mathrm{id}$，且 p 为素数，故

$$o(\sigma)=p.$$

将 σ 写成不相交轮换之积，则其阶为各轮换长度的最小公倍数。因 $o(\sigma)=p$，且所有轮换长度均不超过 p，故其中必有一个长度为 p 的轮换。因此 σ 本身就是一个 p-轮换。 □

6. 设 p 为素数，$\sigma\in S_p$ 且 σ 不是恒等变换，若 σ^p 为恒等变换，证明 σ 是一个 p-轮换。

解 将 σ 写成不相交轮换之积。设其中一个非平凡轮换的长度为 r。

由于

$$\sigma^p=\mathrm{id},$$

所以该 r-轮换的 p 次方也是恒等变换，从而

$$r\mid p.$$

又 p 为素数，且 $r>1$，故

$$r=p.$$

由于 σ 不是恒等变换，它至少含有一个非平凡轮换，因此必含有一个 p-轮换。而 $\sigma\in S_p$，这个 p-轮换已经包含全部 p 个元素，故

$$\boxed{\sigma\text{ 是一个}p\text{-轮换}}.$$

□

7. 给出交错群 A_5 中置换的型，求 A_5 中与 (12345) 共轭的所有元素，并证明 A_5 中型为 1^12^2 的置换彼此共轭。

解 A_5 中置换的型共有

$$1^5,\qquad 1^23,\qquad 1^12^2,\qquad 5.$$

设 $\sigma=(12345)$。由

$$\tau\sigma\tau^{-1}=(\tau(1)\,\tau(2)\,\tau(3)\,\tau(4)\,\tau(5)),\qquad \tau\in A_5,$$

经验证可得与 σ 共轭的 12 个元素为

$$(12345),(12453),(12534),(13254),$$
$$(13425),(13542),(14235),(14352),$$
$$(14523),(15243),(15324),(15432).$$

设 α,β 均为型 $1^1 2^2$ 的置换。它们在 S_5 中共轭，故存在 $\rho \in S_5$ 使

$$\rho\alpha\rho^{-1} = \beta.$$

若 ρ 为偶置换，则已经得到结论。若 ρ 为奇置换，设

$$\alpha = (ab)(cd),$$

则 (ab) 与 α 可交换，且 $\rho(ab) \in A_5$。于是

$$\rho(ab)\alpha(\rho(ab))^{-1} = \rho\alpha\rho^{-1} = \beta.$$

故型为 $1^1 2^2$ 的置换在 A_5 中彼此共轭。 □

为什么 (12354) 不与 (12345) 在 A_5 中共轭？

设

$$\sigma = (12345), \qquad \rho = (45).$$

则由共轭公式，

$$\rho\sigma\rho^{-1} = (\rho(1)\,\rho(2)\,\rho(3)\,\rho(4)\,\rho(5)) = (12354).$$

所以 (12354) 与 (12345) 在 S_5 中共轭。

但 $\rho = (45)$ 是奇置换，因此 $\rho \notin A_5$。进一步地，若存在 $\tau \in A_5$ 使

$$\tau\sigma\tau^{-1} = (12354),$$

则

$$\tau\sigma\tau^{-1} = \rho\sigma\rho^{-1},$$

从而

$$\rho^{-1}\tau\,\sigma = \sigma\,\rho^{-1}\tau.$$

即 $\rho^{-1}\tau$ 与 σ 可交换。

由前面的结论，与 $\sigma = (12345)$ 可交换的元素都是 σ 的幂，故

$$\rho^{-1}\tau = \sigma^k,$$

于是

$$\tau = \rho\sigma^k.$$

由于 ρ 是奇置换，而 σ^k 是偶置换，所以 τ 必为奇置换，这与 $\tau \in A_5$ 矛盾。

因此

$$\boxed{(12354) \text{ 与} (12345) \text{ 在} A_5 \text{ 中不共轭.}}$$

这说明 S_5 中所有 5-轮换虽然彼此共轭，但在 A_5 中会分裂成两个共轭类，每个共轭类含 12 个元素。

8. 交错群 A_n 中两个型相同的置换是否一定在 A_n 中共轭？

解 不一定。例如在 A_5 中，

$$(12345), \qquad (13524) = (12345)^2$$

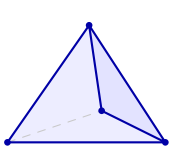
均为 5-轮换，因而型相同。

但由第 7 题中 (12345) 的共轭类可知，

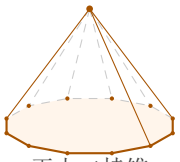
$$(13524)$$

不在其共轭类中，故二者在 A_5 中不共轭。 □

9. 求正四面体和正十二棱锥的对称群。



正四面体



正十二棱锥

解 正四面体的任意对称变换都对应于其 4 个顶点的一个置换，且任意顶点置换均可由唯一的对称变换实现，故其对称群为

$$\boxed{S_4}.$$

正十二棱锥的顶点保持不动，其对称变换完全由底面的正十二边形决定，故其对称群为

$$\boxed{D_{12}},$$

其阶为 24。 □

10. 在二面体群 D_4 中找 3 个元素 a, b, c 满足

$$ab = bc,$$

但是 $a \neq c$。

解 设

$$D_4 = \langle r, s \mid r^4 = e,\ s^2 = e,\ srs = r^{-1} \rangle.$$

取

$$a = r^3, \qquad b = s, \qquad c = r.$$

由

$$sr = r^{-1}s = r^3 s,$$

有

$$ab = r^3 s = sr = bc,$$

而

$$a = r^3 \neq r = c.$$

□

2.2 子群与同态

1. 设 H 是群 G 的非空子集，在 G 中定义关系 $\sim$：对任意 $a, b \in G$，

$$a \sim b \iff ab^{-1} \in H.$$

证明 $\sim$ 是 G 上的等价关系当且仅当 $H \leqslant G$。

解 若 $H \leqslant G$，则

$$aa^{-1} = e \in H,$$

故 $\sim$ 自反。若 $a \sim b$，则

$$ba^{-1} = (ab^{-1})^{-1} \in H,$$

故 $\sim$ 对称。若 $a \sim b,\ b \sim c$，则

$$ac^{-1} = (ab^{-1})(bc^{-1}) \in H,$$

故 $\sim$ 传递。因此 $\sim$ 是等价关系。

反之，设 $\sim$ 是等价关系。任取 $x, y \in H$，则

$$x \sim e, \qquad y \sim e.$$

由对称性，$e \sim y$；再由传递性，

$$x \sim y,$$

故

$$xy^{-1} \in H.$$

由子群判定法（定理 2.2.1），$H \leqslant G$。 □

2. 考虑整数加法群 $\mathbb{Z}$，设 $H \leqslant \mathbb{Z}$。

(1) 证明：若 $m, n \in H$，则 $\gcd(m, n) \in H$；

(2) 证明存在一个整数 $m \in \mathbb{Z}$，使得

$$H = m\mathbb{Z};$$

(3) 设 $m_1, m_2, \ldots, m_k$ 为两两不同的 k 个非零整数，证明

$$m_1\mathbb{Z} \cap m_2\mathbb{Z} \cap \cdots \cap m_k\mathbb{Z} = \operatorname{lcm}(m_1, m_2, \ldots, m_k)\mathbb{Z},$$

其中 $\operatorname{lcm}(m_1, m_2, \ldots, m_k)$ 表示 $m_1, m_2, \ldots, m_k$ 的最小公倍数；

(4) 任取无穷多个两两不同的整数 $\{m_k\}_{k\in\mathbb{N}}$，利用（3）中结论证明

$$\bigcap_{k\in\mathbb{N}} m_k\mathbb{Z} = \{0\}.$$

解

(1) 由 Bézout 等式，存在 $s, t \in \mathbb{Z}$ 使

$$\gcd(m, n) = sm + tn.$$

因 H 为加法子群，故 $\gcd(m, n) \in H$。

(2) 若 $H = \{0\}$，取 $m = 0$ 即可。

若 $H \neq \{0\}$，取 H 中最小的正整数 m。显然

$$m\mathbb{Z} \subseteq H.$$

任取 $a \in H$，由带余除法

$$a = qm + r, \qquad 0 \leqslant r < m.$$

于是

$$r = a - qm \in H.$$

由 m 的最小性知 $r = 0$，故 $m \mid a$。因此

$$H = m\mathbb{Z}.$$

(3) 对任意 $x \in \mathbb{Z}$，

$$x \in \bigcap_{i=1}^{k} m_i\mathbb{Z} \iff m_i \mid x \quad (i = 1, \dots, k)$$
$$\iff \operatorname{lcm}(m_1, \dots, m_k) \mid x.$$

故

$$m_1\mathbb{Z} \cap \cdots \cap m_k\mathbb{Z} = \operatorname{lcm}(m_1, \dots, m_k)\mathbb{Z}.$$

(4) 令

$$L_n = \operatorname{lcm}(m_1, m_2, \dots, m_n).$$

由（3），若

$$x \in \bigcap_{k\in\mathbb{N}} m_k\mathbb{Z},$$

则对任意 n 均有

$$L_n \mid x.$$

由于 m_k 两两不同，而一个非零整数只有有限多个因数，故 L_n 无界。

若 $x \neq 0$，取 n 使 $L_n > |x|$，则不可能有 $L_n \mid x$，矛盾。因此 $x = 0$，故

$$\bigcap_{k\in\mathbb{N}} m_k\mathbb{Z} = \{0\}.$$

□

3. 设 $n \geqslant 3$，在对称群 S_n 中令

$$\sigma = (12\cdots n), \qquad \tau = (12),$$

证明

$$S_n = \langle \sigma, \tau \rangle.$$

解 由共轭公式，

$$\sigma^k \tau \sigma^{-k} = (\sigma^k(1)\, \sigma^k(2)).$$

因此

$$(12), (23), \dots, (n-1\, n) \in \langle \sigma, \tau \rangle.$$

而任意置换都可以写成相邻对换

$$(12), (23), \dots, (n-1\, n)$$

的乘积，故

$$S_n = \langle \sigma, \tau \rangle.$$

□

4. 证明：若 n 为大于 2 的偶数，则

$$A_n = \langle (123), (23\cdots n) \rangle;$$

若 n 为大于 2 的奇数，则

$$A_n = \langle (123), (12\cdots n) \rangle.$$

解 先注意 A_n 可由

$$(123),(124),\ldots,(12n)$$

生成。因此只需证明题中给出的两个元素能生成这些 3-轮换。

（1）n 为偶数。

令

$$\sigma=(23\cdots n),\qquad H=\langle(123),\sigma\rangle.$$

由共轭公式，

$$\sigma^k(123)\sigma^{-k}=(1\,\sigma^k(2)\,\sigma^k(3)),$$

故

$$(123),(134),(145),\ldots,(1\,n-1\,n)\in H.$$

又

$$(1\,k\,k+1)(12k)=(12\,k+1),$$

所以由归纳法得到

$$(123),(124),\ldots,(12n)\in H.$$

因此

$$A_n\subseteq H.$$

而 (123) 与 $(23\cdots n)$ 均为偶置换，故 $H\subseteq A_n$。于是

$$A_n=\langle(123),(23\cdots n)\rangle.$$

（2）n 为奇数。

令

$$\sigma=(12\cdots n),\qquad H=\langle(123),\sigma\rangle.$$

由共轭公式，

$$\sigma^k(123)\sigma^{-k}=(k+1\,k+2\,k+3),$$

其中各数字模 n 理解。因此

$$(123),(234),(345),\ldots,(n-2\,n-1\,n)\in H.$$

由

$$(234)(123)(234)^{-1}=(134),$$

从而

$$(134)(123)=(124),$$

故 $(124)\in H$。

若已有 $(12k)\in H$，其中 $k\geqslant 4$，则

$$(k-1\,k\,k+1)(12k)(k-1\,k\,k+1)^{-1}=(12\,k+1).$$

故归纳得到

$$(123),(124),\ldots,(12n)\in H.$$

于是 $A_n\subseteq H$。

又因为 n 为奇数，$(12\cdots n)$ 为偶置换，故 $H\subseteq A_n$。因此

$$A_n=\langle(123),(12\cdots n)\rangle.$$

□

为什么 A_n 可由 $(123),(124),\dots,(12n)$ 生成？
记

$$H=\langle (123),(124),\dots,(12n)\rangle.$$

由于 A_n 可由所有 3-轮换生成，只需说明任意 3-轮换均属于 H。
首先，对任意互异的 $i,j\neq 1,2$，

$$(1ij)=(12j)(12i)^{-1}\in H.$$

进一步地，对任意互异的 i,j,k，

$$(ijk)=(1ij)(1jk)\in H.$$

因此所有 3-轮换均属于 H，从而

$$A_n\subseteq H.$$

另一方面，$(123),(124),\dots,(12n)$ 本身都是偶置换，故

$$H\subseteq A_n.$$

所以

$$\boxed{A_n=\langle (123),(124),\dots,(12n)\rangle.}$$

5. 考虑 2 阶整系数方阵的集合 $\mathbb{Z}^{2\times 2}$，其上运算为矩阵乘法。

(1) 证明 $A\in\mathbb{Z}^{2\times 2}$ 可逆当且仅当

$$|\det A|=1;$$

(2) 设所有满足 $|\det A|=1$ 的整数 2 阶方阵构成的集合为 $\mathrm{GL}_2(\mathbb{Z})$，证明 $\mathrm{GL}_2(\mathbb{Z})$ 关于矩阵乘法构成一个群，并且该群可以由

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

生成。

解

(1) 若 A 在 $\mathbb{Z}^{2\times 2}$ 中可逆，设其逆为 B，则

$$\det A\det B=1.$$

因两者均为整数，故

$$\det A=\pm 1.$$

反之，若 $\det A=\pm 1$，则

$$A^{-1}=\frac{1}{\det A}A^{*}$$

仍为整系数矩阵，故 A 可逆。

(2) 由

$$\det(AB)=\det A\det B,\qquad \det(A^{-1})=(\det A)^{-1},$$

知 $\mathrm{GL}_2(\mathbb{Z})$ 关于矩阵乘法构成群。

记

$$U=\begin{pmatrix}1&1\\0&1\end{pmatrix},\quad L=\begin{pmatrix}1&0\\1&1\end{pmatrix},\quad D=\begin{pmatrix}1&0\\0&-1\end{pmatrix}.$$

则 $U^{\pm1}, L^{\pm1}$ 分别对应整倍的初等行变换，且

$$UL^{-1}U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

结合 D 还可实现两行交换及变号。

任取

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

由 $\det A = \pm 1$ 知

$$\gcd(a, c) = 1.$$

利用辗转相除法，通过上述初等行变换可将第一列化为

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

于是可将 A 化为

$$\begin{pmatrix} 1 & q \\ 0 & \pm 1 \end{pmatrix},$$

再利用 U 的适当整数次幂及 D 即可化为单位矩阵。

因此任意 $A \in \mathrm{GL}_2(\mathbb{Z})$ 都可由 U, L, D 的乘积表示，即

$$\mathrm{GL}_2(\mathbb{Z}) = \langle U, L, D \rangle.$$

□

6. 已知定义在 $\mathbb{R} \cup \{\infty\}$ 上的函数

$$f(x) = \frac{1}{x}, \qquad g(x) = \frac{x-1}{x},$$

考虑这两个函数生成的 $\mathbb{R} \cup \{\infty\}$ 的全变换群 $S_{\mathbb{R}\cup\{\infty\}}$ 的子群 H，其中的运算是函数复合。证明

$$H \cong S_3.$$

解 直接计算得

$$f^2 = \mathrm{id}, \qquad g^3 = \mathrm{id}, \qquad fg = g^{-1}f.$$

因此 H 中任意元素均可写成

$$g^i \quad 或 \quad g^i f, \qquad i = 0, 1, 2,$$

故 $|H| \leqslant 6$。

又 $g \neq \mathrm{id}$，$g^2 \neq \mathrm{id}$，且

$$fg \neq gf,$$

故 $f \notin \langle g \rangle$。因此

$$\mathrm{id}, g, g^2, f, gf, g^2 f$$

两两不同，从而

$$|H| = 6.$$

又 H 非交换，故

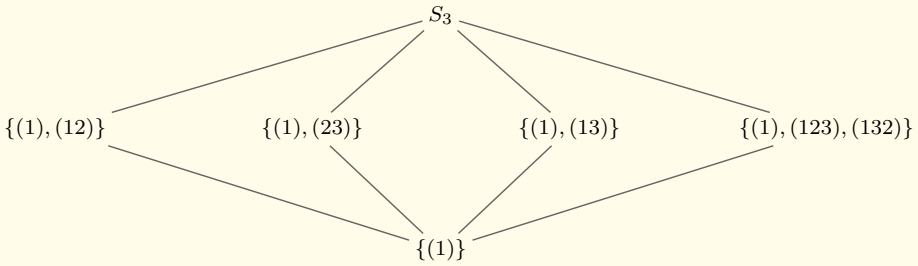
$$\boxed{H \cong S_3}.$$

□

7. 如果 G 是一个有限群，我们可以构造 G 的子群图，这个图的点是 G 的子群。任给两个不同子群 H 和 K，存在一条连接 H 和 K 的线段当且仅当 $H < K$，且不存在其他子群 L 满足 $H < L < K$。如果 $H < K$，我们通常将 H 放在较低的位置，K 放在较高的位置。例如，以下给出 $\mathbb{Z}_3$ 的子群图：



以及 S_3 的子群图：



试画出 $\mathbb{Z}_{12}$ 和 D_4 的子群图。

解 **（1）$\mathbb{Z}_{12}$ 的子群图。**

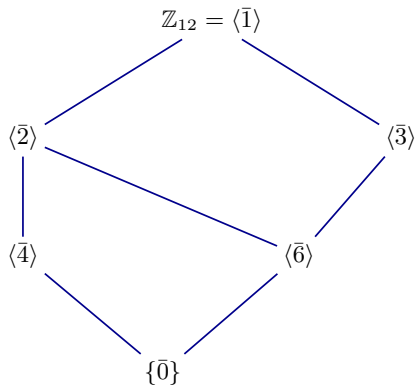
采用加法记号。循环群的每个子群仍为循环群，并且对 12 的每个正因数，$\mathbb{Z}_{12}$ 恰有一个相应阶数的子群。因此全部子群为

$$\begin{aligned}
\langle\bar{1}\rangle &= \mathbb{Z}_{12},\\
\langle\bar{2}\rangle &= \{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\bar{10}\},\\
\langle\bar{3}\rangle &= \{\bar{0},\bar{3},\bar{6},\bar{9}\},\\
\langle\bar{4}\rangle &= \{\bar{0},\bar{4},\bar{8}\},\\
\langle\bar{6}\rangle &= \{\bar{0},\bar{6}\}, \qquad \{\bar{0}\}.
\end{aligned}$$

其中

$$\langle\bar{a}\rangle \leqslant \langle\bar{b}\rangle \quad\Longleftrightarrow\quad b \mid a.$$

去掉所有由传递性得到的包含关系，子群图为



（2）D_4 的子群图。

沿用表示

$$D_4 = \langle r, s \mid r^4 = e,\ s^2 = e,\ srs = r^{-1}\rangle.$$

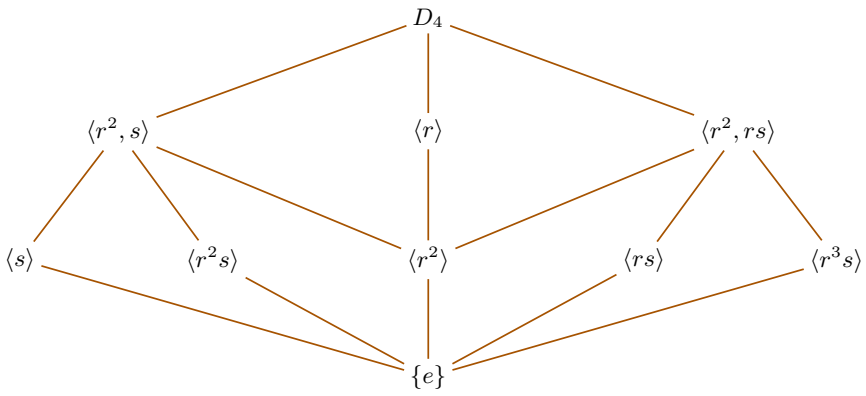
它的三个 4 阶子群为

$$\langle r\rangle = \{e, r, r^2, r^3\},$$
$$\langle r^2, s\rangle = \{e, r^2, s, r^2 s\},$$
$$\langle r^2, rs\rangle = \{e, r^2, rs, r^3 s\};$$

五个 2 阶子群为

$$\langle r^2\rangle, \quad \langle s\rangle, \quad \langle rs\rangle, \quad \langle r^2 s\rangle, \quad \langle r^3 s\rangle.$$

由拉格朗日定理，子群的阶只能为 $1, 2, 4, 8$。若一个 4 阶子群含有 4 阶元素，它只能是 $\langle r\rangle$；否则它由 r^2 和一对相差 r^2 的反射组成。因此上面已经列出了全部子群。根据这些子群之间的直接包含关系，得到



□

8. 设 G 是群，$K, L \leqslant G$，证明

$$KL \leqslant G$$

当且仅当

$$KL = LK.$$

解 先设 $KL \leqslant G$。任取 $l \in L$, $k \in K$，由于

$$k^{-1}l^{-1} \in KL,$$

且 KL 对取逆封闭，故

$$lk = (k^{-1}l^{-1})^{-1} \in KL.$$

所以 $LK \subseteq KL$。同理 $KL \subseteq LK$，故

$$KL = LK.$$

反之，设 $KL = LK$。任取 $k_1l_1, k_2l_2 \in KL$。由于

$$l_1k_2 \in LK = KL,$$

可写为 $l_1k_2 = k_3l_3$，其中 $k_3 \in K$, $l_3 \in L$。于是

$$(k_1l_1)(k_2l_2) = k_1k_3l_3l_2 \in KL.$$

又

$$(kl)^{-1} = l^{-1}k^{-1} \in LK = KL.$$

故 KL 对乘法和取逆封闭，因此

$$KL \leqslant G.$$

□

9. 证明定理 2.2.2：
设

$$\sigma\colon G \to G'$$

为同态，则有：

(1) 设 e 为 G 的单位元，则

$$\sigma(e) = e',$$

其中 e' 为 G' 的单位元；

(2) 对任意 $g \in G$，

$$\sigma(g^{-1}) = \sigma(g)^{-1};$$

(3) 对任意 $S \subseteq G$，令

$$\sigma(S) = \{\sigma(a) \mid a \in S\}.$$

若 $H \leqslant G$，则

$$\sigma(H) \leqslant G',$$

特别地，

$$\sigma(G) \leqslant G';$$

(4) 对任意 $S' \subseteq \sigma(G)$，令

$$\sigma^{-1}(S') = \{g \in G \mid \sigma(g) \in S'\}.$$

若 $H' \leqslant \sigma(G)$，则

$$\sigma^{-1}(H') \leqslant G.$$

解

(1) 由

$$\sigma(e) = \sigma(e^2) = \sigma(e)^2,$$

消去 $\sigma(e)$ 得

$$\sigma(e) = e'.$$

(2) 由

$$e' = \sigma(e) = \sigma(gg^{-1}) = \sigma(g)\sigma(g^{-1}),$$

故

$$\sigma(g^{-1}) = \sigma(g)^{-1}.$$

(3) 任取 $\sigma(a), \sigma(b) \in \sigma(H)$，则

$$\sigma(a)\sigma(b)^{-1} = \sigma(ab^{-1}) \in \sigma(H),$$

因为 $ab^{-1} \in H$。由子群判定法，

$$\sigma(H) \leqslant G'.$$

取 $H = G$ 即得

$$\sigma(G) \leqslant G'.$$

(4) 任取 $a, b \in \sigma^{-1}(H')$，则

$$\sigma(a), \sigma(b) \in H'.$$

因 $H' \leqslant \sigma(G)$，

$$\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} \in H'.$$

故

$$ab^{-1} \in \sigma^{-1}(H').$$

由子群判定法，

$$\sigma^{-1}(H') \leqslant G.$$

□

10. 确定对称群 S_n 到 2 阶群

$$\mu_2 = \{1, -1\}$$

的所有同态。

解 设

$$\varphi\colon S_n \to \mu_2$$

为同态。由于 S_n 中任意两个对换共轭，而 μ_2 为交换群，故所有对换在 φ 下的像相同，记为 $c \in \mu_2$。

又 S_n 由对换生成，所以 φ 完全由 c 决定。

若 $c = 1$，则 φ 为平凡同态；若 $c = -1$，则

$$\varphi(\sigma) = \begin{cases} 1, & \sigma \text{ 为偶置换}, \\ -1, & \sigma \text{ 为奇置换}, \end{cases}$$

即符号同态。

因此，当 $n \geqslant 2$ 时，所有同态为

$$\boxed{\text{平凡同态或符号同态}}.$$

□

11. 证明 S_4 的子群

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$$

与 μ_4 不同构。

解 V_4 中任意元素 x 均满足

$$x^2 = (1).$$

若 $V_4 \cong \mu_4$，则 μ_4 中任意元素 y 也应满足

$$y^2 = 1.$$

但 $i \in \mu_4$，且

$$i^2 = -1 \neq 1.$$

矛盾。因此

$$\boxed{V_4 \ncong \mu_4}.$$

□

12. 设 G 为群，G 上的变换 σ 定义为对任意 $a \in G$，

$$\sigma(a) = a^{-1}.$$

证明 σ 为 G 的自同构当且仅当 G 是交换群。

解 首先

$$\sigma^2(a) = (a^{-1})^{-1} = a,$$

故 σ 为双射。

σ 为同态当且仅当对任意 $a, b \in G$，

$$\sigma(ab) = \sigma(a)\sigma(b).$$

即

$$b^{-1}a^{-1} = a^{-1}b^{-1},$$

这等价于

$$ab = ba.$$

因此 σ 为自同构当且仅当 G 为交换群。 □

13. 求有理数加法群 $(\mathbb{Q}, +)$ 的自同构群。

解 设

$$\sigma \in \mathrm{Aut}(\mathbb{Q}, +),$$

令

$$\sigma(1) = r.$$

则 $r \neq 0$。对任意

$$x = \frac{m}{n} \in \mathbb{Q},$$

有

$$n\sigma(x) = \sigma(nx) = \sigma(m) = mr,$$

故

$$\sigma(x) = rx.$$

反之，对任意 $r \in \mathbb{Q}^\times$，

$$\sigma_r(x) = rx$$

显然是 $(\mathbb{Q}, +)$ 的自同构。

因此

$$\boxed{\mathrm{Aut}(\mathbb{Q}, +) = \{\sigma_r : x \mapsto rx \mid r \in \mathbb{Q}^\times\} \cong \mathbb{Q}^\times.}$$

这里 $\mathbb{Q}^\times$ 表示所有非零有理数在乘法下构成的群。 □

14. 证明实数加法群与正实数乘法群同构。

解 定义

$$\varphi\colon (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot), \qquad \varphi(x) = e^x.$$

则

$$\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y),$$

故 φ 为同态。

又 e^x 在 $\mathbb{R}$ 上严格单调，且对任意 $y>0$，

$$y = e^{\ln y},$$

故 φ 为双射。因此

$$\boxed{(\mathbb{R},+) \cong (\mathbb{R}_{>0},\cdot)}.$$

□

15. 设

$$\sigma\colon G \to G'$$

为群同态，$H \leqslant G$，$K = \operatorname{Ker}\sigma$，证明

$$\sigma^{-1}(\sigma(H)) = HK,$$

并且

$$HK \leqslant G.$$

解 任取 $x \in \sigma^{-1}(\sigma(H))$，则存在 $h \in H$ 使

$$\sigma(x) = \sigma(h).$$

于是

$$\sigma(h^{-1}x) = e',$$

故 $h^{-1}x \in K$，从而

$$x \in HK.$$

所以

$$\sigma^{-1}(\sigma(H)) \subseteq HK.$$

反之，若 $x = hk \in HK$，其中 $h \in H,\ k \in K$，则

$$\sigma(x) = \sigma(h)\sigma(k) = \sigma(h),$$

故

$$x \in \sigma^{-1}(\sigma(H)).$$

因此

$$\boxed{\sigma^{-1}(\sigma(H)) = HK}.$$

又由定理 2.2.2，

$$\sigma(H) \leqslant \sigma(G),$$

故

$$\sigma^{-1}(\sigma(H)) \leqslant G.$$

于是

$$\boxed{HK \leqslant G}.$$

□

2.3 循环群

1. 群 S_5 中元素的阶有哪几种？S_{10} 中元素的阶最大是多少？

解 置换的阶等于其不相交轮换长度的最小公倍数。由 5 的各个分拆可得

$$\boxed{S_5 \text{ 中元素的阶为} 1,2,3,4,5,6}.$$

对于 S_{10}，若轮换中出现长度至少为 6 的轮换，则由

$$10,\quad 9+1,\quad 8+2,\quad 7+3,\quad 6+4,\quad \dots$$

可知其阶至多为 21。若所有轮换长度均不超过 5，含有 5-轮换时，剩余 5 个元素取 3-轮换和 2-轮换可得

$$\operatorname{lcm}(5,3,2)=30;$$

若不含 5-轮换，则阶至多为

$$\operatorname{lcm}(1,2,3,4)=12.$$

因此

$$\boxed{S_{10} \text{ 中元素的最大阶为} 30},$$

例如 $(12345)(678)(9\,10)$ 的阶为 30。 □

2. 证明不存在恰有两个 2 阶元素的群。

解 反设群 G 恰有两个 2 阶元素 a,b。

若 $ab=ba$，则

$$(ab)^2=a^2b^2=e,$$

且 $ab\neq e,a,b$，故 ab 是第三个 2 阶元素，矛盾。

若 $ab\neq ba$，则

$$(aba)^2=e.$$

又 $aba\neq a$，否则 $a=b$；且 $aba\neq b$，否则 $ab=ba$。故 aba 是第三个 2 阶元素，仍矛盾。

因此不存在恰有两个 2 阶元素的群。 □

3.

(1) 求出加法群 $\mathbb{Z}_{12}$ 的所有生成元，并确定它的自同态集合 $\operatorname{End}(\mathbb{Z}_{12})$；

(2) 证明对任意正整数 m,n，存在 $\mathbb{Z}_m$ 到 $\mathbb{Z}_n$ 的满同态当且仅当

$$n \mid m.$$

解

(1) $\overline{k}$ 为 $\mathbb{Z}_{12}$ 的生成元当且仅当 $(k,12)=1$，故所有生成元为

$$\boxed{\overline{1},\overline{5},\overline{7},\overline{11}}.$$

任意同态由 $\overline{1}$ 的像唯一决定，因此

$$\boxed{\operatorname{End}(\mathbb{Z}_{12})=\{\varphi_k \mid k\in\mathbb{Z}_{12}\},\qquad \varphi_k(\overline{x})=\overline{kx}.}$$

(2) 若 $\varphi\colon \mathbb{Z}_m \to \mathbb{Z}_n$ 为满同态，则 $\varphi(\overline{1}) = \overline{a}$ 必为 $\mathbb{Z}_n$ 的生成元，故 $(a, n) = 1$。又

$$\overline{0} = \varphi(\overline{m}) = m\varphi(\overline{1}) = \overline{ma},$$

所以 $n \mid ma$，从而 $n \mid m$。

反之，若 $n \mid m$，定义

$$\varphi\colon \mathbb{Z}_m \to \mathbb{Z}_n, \qquad \varphi(\overline{x}) = \overline{x}.$$

则 φ 良定义且为满同态。

□

4. 证明：若

$$\exp(G) = 2,$$

则 G 为交换群。

解 由 $\exp(G) = 2$，对任意 $a, b \in G$ 均有

$$a^2 = b^2 = (ab)^2 = e.$$

于是

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

故 G 为交换群。 □

5. 证明偶数阶有限群中必有 2 阶元素。

解 设 G 为偶数阶有限群。若 G 中没有 2 阶元素，则对任意 $a \neq e$，

$$a \neq a^{-1}.$$

因此 $G \setminus \{e\}$ 中的元素可以两两配成

$$\{a, a^{-1}\},$$

故 $|G| - 1$ 为偶数，从而 $|G|$ 为奇数，矛盾。

因此存在 $a \neq e$ 使

$$a = a^{-1},$$

即

$$a^2 = e.$$

故 a 为 2 阶元素。 □

6. 设 G 为群，$a, b \in G$，证明

$$o(ab) = o(ba).$$

解 注意到

$$ba = a^{-1}(ab)a,$$

故 ab 与 ba 共轭。共轭元素的阶相同，因此

$$\boxed{o(ab) = o(ba)}.$$

□

7. 在群 $\mathrm{GL}_2(\mathbb{Q})$ 中令

$$A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\qquad B=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix},$$

计算 $o(A)$、$o(B)$ 和 $o(AB)$。

解 直接计算

$$A^2=-I,\qquad A^4=I,$$

故

$$o(A)=4.$$

又

$$B^2=\begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix},\qquad B^3=I,$$

故

$$o(B)=3.$$

而

$$AB=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},$$

所以

$$(AB)^n=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\neq I\qquad (n\geqslant 1).$$

因此

$$\boxed{o(A)=4,\qquad o(B)=3,\qquad o(AB)=\infty}.$$

□

8. 设 G 为交换群，证明 G 中所有有限阶元素构成 G 的一个子群。

解 设 $a,b\in G$ 均为有限阶元素，且

$$a^m=e,\qquad b^n=e.$$

由于 G 交换，

$$(ab^{-1})^{mn}=a^{mn}b^{-mn}=e.$$

故 ab^{-1} 也是有限阶元素。

由子群判定法，所有有限阶元素构成 G 的一个子群。 □

9. 设群 G 只有有限个子群，证明 G 是有限群。

解 对任意 $g\in G$，循环子群 $\langle g\rangle$ 必为有限群；否则若 $\langle g\rangle$ 为无限循环群，则

$$\langle g\rangle,\langle g^2\rangle,\langle g^3\rangle,\dots$$

给出无穷多个不同的子群，矛盾。

又 G 只有有限个子群，因而只有有限个循环子群。由于

$$G = \bigcup_{g \in G} \langle g \rangle,$$

G 是有限个有限集合之并，故 G 为有限群。 □

10. 证明 A_4 没有 6 阶子群。

解 反设存在 $H \leqslant A_4$，且 $|H| = 6$，我们知道 A_4 中有 1、2、3 阶元素。

由前题知，H 中存在一个 2 阶元素，记为 a。又 A_4 中只有 3 个 2 阶元素，而 H 有 5 个非单位元，故 H 中必有一个 3 阶元素 b。

令

$$K = \langle b \rangle = \{e, b, b^2\}.$$

由于 $|H| = 6$，故

$$H = K \cup aK.$$

又 $ba \notin K$，故 $ba \in aK$，从而

$$aba \in K.$$

由于 aba 也是 3 阶元素，故

$$aba = b \qquad 或 \qquad aba = b^2.$$

若 $aba = b$，则 $ab = ba$，于是

$$(ab)^6 = e, \qquad (ab)^2 \neq e, \qquad (ab)^3 \neq e,$$

故 ab 为 6 阶元素，这与 A_4 中元素的阶只有 $1, 2, 3$ 矛盾。

因此

$$aba = b^2.$$

于是

$$(ab)^2 = abab = b^2 b = e,$$

故 ab 是另一个 2 阶元素，且 $ab \neq a$。因此 H 至少含两个不同的 2 阶元素。

而 A_4 中三个 2 阶元素

$$(12)(34), \qquad (13)(24), \qquad (14)(23)$$

中任意两个的乘积恰为第三个，故 H 必包含它们全部。因此

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \leqslant H.$$

由 Lagrange 定理应有

$$4 \mid 6,$$

矛盾。

故

$$\boxed{A_4 \text{ 没有6 阶子群}}.$$

□

11. 设 g 为群 G 中的 rs 阶元素，其中

$$\gcd(r,s)=1.$$

证明存在 $a,b\in G$ 使得

$$g=ab,\qquad o(a)=r,\qquad o(b)=s,$$

且 a,b 都是 g 的幂。

解 由 $\gcd(r,s)=1$，存在整数 u,v 使

$$su+rv=1.$$

令

$$a=g^{su},\qquad b=g^{rv}.$$

则

$$ab=g^{su+rv}=g.$$

又由 $su+rv=1$ 知

$$\gcd(u,r)=1,\qquad \gcd(v,s)=1.$$

因此

$$o(a)=\frac{rs}{\gcd(rs,su)}=r,\qquad o(b)=\frac{rs}{\gcd(rs,rv)}=s.$$

故结论成立。 □

12. 设 $\sigma\in S_n$，σ 的阶为素数 p，证明 σ 为若干个互不相交的长为 p 的轮换之积。

解 将 σ 写成不相交轮换之积。设其中非平凡轮换的长度分别为

$$r_1,r_2,\dots,r_k.$$

则

$$o(\sigma)=\operatorname{lcm}(r_1,\dots,r_k)=p.$$

由于 p 为素数，故每个 r_i 都只能等于 p。

因此 σ 是若干个互不相交的 p-轮换之积。 □

13. 设 G 为群，$g\in G$，正整数 k 与 $o(g)$ 互素，证明

$$x^k=g$$

在 $\langle g\rangle$ 中恰有一个解。

解 记

$$n=o(g).$$

设 $x=g^m$，则

$$x^k=g\iff g^{km}=g\iff km\equiv 1\pmod{n}.$$

由于

$$\gcd(k,n)=1,$$

同余方程

$$km\equiv 1\pmod{n}$$

有唯一解 $m \pmod n$。因此 $x = g^m$ 在 $\langle g \rangle$ 中恰有一个解。 □

14. 证明有理数加法群的任一有限生成子群都是循环群。

解 设

$$H = \langle q_1, q_2, \ldots, q_n \rangle \leqslant \mathbb{Q}, \qquad q_i = \frac{a_i}{b_i}.$$

取

$$d = \operatorname{lcm}(b_1, \ldots, b_n),$$

则可写成

$$q_i = \frac{c_i}{d}, \qquad c_i \in \mathbb{Z}.$$

令

$$c = \gcd(c_1, \ldots, c_n).$$

由 Bézout 等式，

$$H = \left\langle \frac{c}{d} \right\rangle.$$

故 H 为循环群。 □

15. 设 G 是有限生成的交换群，如果 G 的每个生成元的阶都有限，证明 G 为有限群。

解 设

$$G = \langle g_1, g_2, \ldots, g_n \rangle, \qquad o(g_i) = m_i < \infty.$$

由于 G 为交换群，每个元素均可写成

$$g_1^{a_1} g_2^{a_2} \cdots g_n^{a_n}.$$

又可将各指数分别模 m_i 化简，因此可取

$$0 \leqslant a_i < m_i.$$

故

$$|G| \leqslant m_1 m_2 \cdots m_n < \infty.$$

所以 G 为有限群。 □

16. 设 $H \leqslant G$，$g \in G$。若

$$o(g) = n, \qquad g^m \in H, \qquad \gcd(n, m) = 1,$$

证明 $g \in H$。

解 由 $\gcd(n, m) = 1$，存在 $u, v \in \mathbb{Z}$ 使

$$um + vn = 1.$$

因此

$$g = g^{um+vn} = (g^m)^u (g^n)^v = (g^m)^u \in H.$$

故 $g \in H$。 □

17. 设 p 为奇素数，m 为正整数，证明 $U(p^m)$ 为循环群。若 $p=2$，结论是否正确？

解 已知 $U(p)$ 为循环群，取 a 使 $\overline{a}$ 生成 $U(p)$，故 a 模 p 的阶为 $p-1$。

在 a 与 $a+p$ 中至少有一个数 g 满足

$$g^{p-1}\not\equiv 1 \pmod{p^2}.$$

事实上，若 $a^{p-1}\equiv 1 \pmod{p^2}$, 则由二项式定理，

$$(a+p)^{p-1}\equiv 1-pa^{p-2}\not\equiv 1 \pmod{p^2}.$$

又因 $g\equiv a \pmod{p}$，故 g 模 p 的阶仍为 $p-1$。

于是可写

$$g^{p-1}=1+cp,\qquad p\nmid c.$$

反复利用二项式定理可得

$$g^{(p-1)p^{r-1}}\equiv 1+c_rp^r \pmod{p^{r+1}},\qquad p\nmid c_r.$$

特别地，

$$g^{(p-1)p^{m-2}}\not\equiv 1 \pmod{p^m}.$$

另一方面，g 在 $U(p^m)$ 中的阶为 $p-1$ 的倍数，且由 Lagrange 定理整除

$$|U(p^m)|=p^{m-1}(p-1).$$

因此只能有

$$o(g)=p^{m-1}(p-1).$$

故

$$U(p^m)=\langle g\rangle,$$

所以 $U(p^m)$ 为循环群。

当 $p=2$ 时结论一般不成立。例如

$$U(8)=\{\overline{1},\overline{3},\overline{5},\overline{7}\},$$

且

$$\overline{3}^2=\overline{5}^2=\overline{7}^2=\overline{1}.$$

因此 $U(8)$ 中没有 4 阶元素，故 $U(8)$ 不是循环群。 □

18. 设 G 为 n 阶循环群，m 为正整数，求方程 $x^m=e$ 在 G 中解的个数。

解 设 $G=\langle a\rangle$，则 G 中每个元素都唯一写成 $x=a^k$，其中 $0\leqslant k\leqslant n-1$。于是

$$x^m=e\Longleftrightarrow a^{mk}=e\Longleftrightarrow n\mid mk.$$

令 $d=\gcd(m,n)$，写成 $m=dm_1$、$n=dn_1$，其中 $\gcd(m_1,n_1)=1$。则

$$n\mid mk\Longleftrightarrow dn_1\mid dm_1k\Longleftrightarrow n_1\mid m_1k\Longleftrightarrow n_1\mid k.$$

因此在 $0\leqslant k\leqslant n-1$ 中，k 必须为

$$0,n_1,2n_1,\ldots,(d-1)n_1,$$

恰有 d 个。

故方程 $x^m=e$ 在 G 中恰有

$$\boxed{\gcd(m,n)}$$

个解。 □

19. 设 G 为循环群，分别就 G 无限或有限时给出 G 的自同态环（由此也可以得到 G 的自同构群）。

解 设 $G=\langle g\rangle$。任一自同态均由 g 的像唯一确定。

若 G 为无限循环群，则对任意 $k\in\mathbb{Z}$，

$$\varphi_k(g^r)=g^{kr},$$

且所有自同态均如此。因此

$$\boxed{\mathrm{End}(G)\cong\mathbb{Z}}.$$

其中 φ_k 为自同构当且仅当 $k=\pm1$，故

$$\boxed{\mathrm{Aut}(G)\cong\mathbb{Z}_2}.$$

若 $|G|=n$，则 k 只需模 n 考虑，因此

$$\boxed{\mathrm{End}(G)\cong\mathbb{Z}_n}.$$

而 φ_k 为自同构当且仅当

$$\gcd(k,n)=1,$$

故

$$\boxed{\mathrm{Aut}(G)\cong U(n)}.$$

□

20. 求二面体群 D_4 的自同构群。

解 写成

$$D_4=\langle r,s\mid r^4=s^2=e,\ srs=r^{-1}\rangle.$$

自同构必须将 r 映为 4 阶元素，故

$$r\longmapsto r^{\pm1}.$$

而 s 必须映为某个反射，故

$$s\longmapsto r^js,\qquad j=0,1,2,3.$$

这 $2\cdot4=8$ 种选择均给出自同构。

令

$$\alpha:r\mapsto r,\quad s\mapsto rs,$$

$$\beta:r\mapsto r^{-1},\quad s\mapsto s.$$

则

$$\alpha^4=\beta^2=\mathrm{id},\qquad \beta\alpha\beta=\alpha^{-1},$$

且 α,β 生成全部自同构。因此

$$\boxed{\mathrm{Aut}(D_4)\cong D_4}.$$

□

21. 举例说明不同构的群可以有同构的自同构群。

解 取

$$G=\mathbb{Z}_3,\qquad H=\mathbb{Z}_4.$$

显然

$$G \ncong H.$$

但

$$\mathrm{Aut}(\mathbb{Z}_3) \cong U(3) \cong \mathbb{Z}_2,$$

且

$$\mathrm{Aut}(\mathbb{Z}_4) \cong U(4) \cong \mathbb{Z}_2.$$

故

$$\boxed{\mathrm{Aut}(\mathbb{Z}_3) \cong \mathrm{Aut}(\mathbb{Z}_4)}.$$

□

22. 设 G 是群，对任一正整数 k，定义

$$G^k = \{g^k \mid g \in G\},$$

证明：

(1) 若 G 交换，则

$$G^k \leqslant G;$$

(2) G 是循环群当且仅当 G 的任一子群都是某个 G^k。

解

(1) 任取 $a^k, b^k \in G^k$。由于 G 交换，

$$a^k(b^k)^{-1} = a^k b^{-k} = (ab^{-1})^k \in G^k.$$

由子群判定法，$G^k \leqslant G$.

(2) 先设 $G = \langle g \rangle$ 为有限循环群，$|G| = n$。循环群的任一子群均形如 $H = \langle g^d \rangle$，其中 $d \mid n$。于是

$$G^d = \{g^{dt} \mid t \in \mathbb{Z}\} = \langle g^d \rangle = H.$$

反之，设 G 的任一子群都等于某个 G^k。

首先，由

$$\{e\} = G^N$$

对某个正整数 N 成立，知对任意 $x \in G$，

$$x^N = e.$$

故 G 中所有元素的阶均为 N 的因数，因此可以取一个阶最大的元素 $a \in G$，记

$$o(a) = n.$$

由题设，存在正整数 k 使

$$\langle a \rangle = G^k.$$

由于 $a \in G^k$，存在 $b \in G$ 使

$$a = b^k.$$

于是

$$o(a) = \frac{o(b)}{\gcd(o(b), k)}.$$

由 $o(a)$ 的最大性知 $o(b) \leqslant n = o(a)$，故必有

$$o(b) = n, \qquad \gcd(n, k) = 1.$$

下面证明对任意 $x \in G$ 都有

$$\gcd(k, o(x)) = 1.$$

否则存在素数 p 同时整除 k 和 $o(x)$。于是 $\langle x \rangle$ 中存在一个 p 阶元素 y。由于 $\gcd(n, k) = 1$，有

$$p \nmid n.$$

注意任意形如 G^r 的子群在共轭下保持不变，因为

$$zg^r z^{-1} = (zgz^{-1})^r \in G^r.$$

而 $\langle a \rangle$、$\langle y \rangle$ 都是某个 G^r，故

$$yay^{-1} \in \langle a \rangle, \qquad aya^{-1} \in \langle y \rangle.$$

于是

$$aya^{-1}y^{-1} \in \langle a \rangle \cap \langle y \rangle.$$

由于

$$\gcd(n, p) = 1,$$

有

$$\langle a \rangle \cap \langle y \rangle = \{e\}.$$

故

$$ay = ya.$$

因此

$$o(ay) = np > n,$$

与 n 是最大元素阶矛盾。

所以对任意 $x \in G$，

$$\gcd(k, o(x)) = 1.$$

又

$$x^k \in G^k = \langle a \rangle.$$

由第 16 题的结论可得

$$x \in \langle a \rangle.$$

由于 x 任意，

$$G = \langle a \rangle.$$

故 G 为循环群。

严格来说，若题目中的“循环群”包括无限循环群，则第（2）问原文需要补充条件。因为若

$$G = \langle g \rangle \cong \mathbb{Z}$$

为无限循环群，则对任意正整数 k，

$$G^k = \langle g^k \rangle \neq \{e\},$$

所以平凡子群 $\{e\}$ 不是任何 G^k。
因此正向命题应理解为有限循环群的情形。

□

2.4 群在集合上的作用

1. 设 X 是所有实函数构成的集合，对任意 $a \in \mathbb{R}^*$，$f(x) \in X$，证明

$$a \circ f(x) = f(ax)$$

给出实数域的乘法群 $\mathbb{R}^*$ 在集合 X 上的作用。

解 对任意 $f \in X$，

$$1 \circ f(x) = f(x).$$

又对任意 $a, b \in \mathbb{R}^*$，

$$a \circ (b \circ f)(x) = (b \circ f)(ax) = f(abx) = (ab) \circ f(x).$$

故满足群作用的两个条件，因此 $\mathbb{R}^*$ 在 X 上有一个作用。 □

2. 设 $\mathcal{H}$ 为上半复平面

$$\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\},$$

对于

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

和 $z \in \mathcal{H}$，令

$$\gamma \circ z = \frac{az + b}{cz + d}.$$

证明这是群 $\mathrm{SL}_2(\mathbb{R})$ 在集合 $\mathcal{H}$ 上的一个作用，并求该作用的轨道个数。

解 由于 $ad - bc = 1$，直接计算得

$$\mathrm{Im}\,\frac{az + b}{cz + d} = \frac{\mathrm{Im}\, z}{|cz + d|^2} > 0,$$

故 $\gamma \circ z \in \mathcal{H}$。

单位矩阵显然满足

$$I \circ z = z.$$

又由分式线性变换的直接复合可得，对任意 $\gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{R})$，

$$\gamma_1 \circ (\gamma_2 \circ z) = (\gamma_1 \gamma_2) \circ z.$$

故这确实定义了 $\mathrm{SL}_2(\mathbb{R})$ 在 $\mathcal{H}$ 上的作用。

下面证明该作用传递。任取

$$z = x + yi \in \mathcal{H}, \qquad y > 0,$$

取

$$\gamma = \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

则

$$\gamma \circ i = \frac{\sqrt{y}\, i + x/\sqrt{y}}{1/\sqrt{y}} = x + yi = z.$$

因此任意 $z \in \mathcal{H}$ 都与 i 位于同一轨道中，所以该作用只有一个轨道：

$$\boxed{\text{轨道个数为1}}.$$

□

3. 设 G 为群，证明 G 在自身上的共轭作用传递当且仅当

$$G = \{e\}.$$

解 在共轭作用下，

$$g \circ x = gxg^{-1}.$$

特别地，对任意 $g \in G$，

$$g \circ e = geg^{-1} = e.$$

因此 e 的轨道为

$$\mathrm{Orb}(e) = \{e\}.$$

若共轭作用传递，则 e 的轨道必须等于整个 G，故

$$G = \{e\}.$$

反之，若 $G = \{e\}$，则显然只有一个轨道，因此共轭作用传递。 □

4. 设

$$V = \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

证明

$$V \leqslant \mathrm{GL}_2(\mathbb{R}).$$

令

$$M = \{(1,0), (1,1), (0,1), (-1,1), (-1,0), (-1,-1), (0,-1), (1,-1)\}$$

是实平面 $\mathbb{R}^2$ 的子集。对任意 $g \in V, \alpha \in M$，定义

$$\rho(g, \alpha) = \alpha g^T,$$

其中 g^T 是矩阵 g 的转置。证明 ρ 是一个群作用，并求出该作用下的轨道。

解 显然 $I \in V$，且

$$A^2 = B^2 = C^2 = I, \qquad AB = BA = C,$$

其余乘积也均属于 V，故

$$V \leqslant \mathrm{GL}_2(\mathbb{R}).$$

又

$$\rho(I, \alpha) = \alpha,$$

且对任意 $g, h \in V$，

$$\rho(g, \rho(h, \alpha)) = (\alpha h^T) g^T = \alpha (gh)^T = \rho(gh, \alpha).$$

故 ρ 是群作用。

V 的作用即分别改变两个坐标的符号，因此共有三个轨道：

$$\mathrm{Orb}(1,0) = \{(1,0), (-1,0)\},$$

$$\mathrm{Orb}(0,1) = \{(0,1), (0,-1)\},$$

$$\mathrm{Orb}(1,1) = \{(1,1), (-1,1), (-1,-1), (1,-1)\}.$$

□

5. 记实数域上 n 维向量空间 $\mathbb{R}^n$ 的所有 k 维子空间构成的集合为

$$\mathrm{Gr}(k,n),$$

称为 Grassmann（格拉斯曼）流形。对任意 $\varphi \in \mathrm{GL}_n(\mathbb{R})$，$W \in \mathrm{Gr}(k,n)$，定义

$$\varphi \circ W = \{\varphi(\alpha) \mid \alpha \in W\}.$$

证明这给出了群 $\mathrm{GL}_n(\mathbb{R})$ 在 $\mathrm{Gr}(k,n)$ 上的一个传递作用。

解 由于 φ 为可逆线性变换，若 $\dim W = k$，则

$$\dim \varphi(W) = k,$$

故 $\varphi \circ W \in \mathrm{Gr}(k,n)$。

又

$$I \circ W = W,$$

且

$$\varphi \circ (\psi \circ W) = (\varphi\psi) \circ W,$$

故这确实定义了一个群作用。

任取 $W_1, W_2 \in \mathrm{Gr}(k,n)$，分别取基

$$w_1, \ldots, w_k, \qquad v_1, \ldots, v_k,$$

并将它们分别扩充为 $\mathbb{R}^n$ 的一组基。定义可逆线性变换 φ 将第一组基逐一映到第二组基，则

$$\varphi(W_1) = W_2.$$

因此该作用是传递的。 □

6.

(1) 证明：对任意 $\varphi \in \mathrm{Aut}(S_n)$，若对任意对换 $\sigma \in S_n$，$\varphi(\sigma)$ 仍为一个对换，则

$$\varphi \in \mathrm{Inn}(S_n);$$

(2) 证明：若 $n \neq 2, 6$，则对任意 $\varphi \in \mathrm{Aut}(S_n)$ 和对换 $\sigma \in S_n$，$\varphi(\sigma)$ 都是一个对换；并由此证明

$$\mathrm{Aut}(S_n) \cong S_n;$$

(3) 当 $n = 2$ 或 6 时，结论 $\mathrm{Aut}(S_n) \cong S_n$ 是否成立？为什么？

解

(1) 对 $i = 2, \ldots, n$，记

$$t_i = (1i), \qquad \tau_i = \varphi(t_i).$$

由假设，τ_i 都是对换；又因为 φ 为单射，它们两两不同。当 $i \neq j$ 时，$t_i t_j$ 是一个 3-轮换，故

$$o(\tau_i \tau_j) = o\big(\varphi(t_i t_j)\big) = 3.$$

两个不同对换的乘积为 3 阶元素，当且仅当这两个对换恰有一个公共字母。因此 $\tau_2,\dots,\tau_n$ 对应于完全图中一族两两相交的边。

若 $n\geqslant 5$，这族边至少有 4 条，故它们必有一个公共端点：否则其中三条边只能组成一个三角形，而不可能再有第四条不同的边与三边同时相交。于是存在互不相同的 $a,b_2,\dots,b_n\in\{1,\dots,n\}$，使得

$$\tau_i=(a\,b_i),\qquad i=2,\dots,n.$$

当 $n=4$ 时，三条两两相交的边还可能组成三角形；但在这种情形下 τ_2,τ_3,τ_4 只生成一个 S_3，而 t_2,t_3,t_4 生成 S_4，与 φ 为自同构矛盾。因此它们仍有公共端点。$n=3$ 时结论直接成立；$n=2$ 时 $\mathrm{Aut}(S_2)=\{\mathrm{id}\}$，结论也显然成立。

定义 $\pi\in S_n$ 为

$$\pi(1)=a,\qquad \pi(i)=b_i\quad(2\leqslant i\leqslant n).$$

则

$$\varphi((1i))=(a\,b_i)=\pi(1i)\pi^{-1}.$$

而 $(12),(13),\dots,(1n)$ 生成 S_n，所以对所有 $\sigma\in S_n$，

$$\varphi(\sigma)=\pi\sigma\pi^{-1}.$$

故 φ 是内自同构，即

$$\boxed{\varphi\in\mathrm{Inn}(S_n)}.$$

(2) 自同构保持元素的阶及共轭关系。设 σ 是一个对换，则 $\varphi(\sigma)$ 是一个非平凡的 2 阶元素，因而其轮换型为

$$2^k1^{\,n-2k},$$

即 k 个不相交对换的乘积，其中 $1\leqslant k\leqslant\lfloor n/2\rfloor$。

自同构还保持共轭类的大小。事实上，若 σ 的共轭类为

$$\mathrm{Cl}(\sigma)=\{g\sigma g^{-1}\mid g\in S_n\},$$

则

$$\begin{aligned}\varphi\big(\mathrm{Cl}(\sigma)\big)&=\{\varphi(g)\varphi(\sigma)\varphi(g)^{-1}\mid g\in S_n\}\\&=\mathrm{Cl}\big(\varphi(\sigma)\big).\end{aligned}$$

由于 φ 是双射，这两个共轭类所含元素个数相同。

S_n 中的对换共有

$$\binom{n}{2}=\frac{n(n-1)}{2}$$

个。下面计算轮换型为 $2^k1^{\,n-2k}$ 的元素个数：先从 n 个字母中选出 $2k$ 个，再将它们分成 k 个不计次序的二元组，故共有

$$\binom{n}{2k}\frac{(2k)!}{2^k k!}=\frac{n!}{2^k k!(n-2k)!}$$

个。于是 σ 与 $\varphi(\sigma)$ 的共轭类大小相等给出

$$\frac{n(n-1)}{2}=\frac{n!}{2^k k!(n-2k)!}.$$

约去 $n(n-1)$，得到

$$\frac{(n-2)!}{(n-2k)!}=2^{k-1}k!.\tag{*}$$

若 $k=2$，左边为 $(n-2)(n-3)$，在 $n=4$ 时等于 2，而在 $n\geqslant 5$ 时至少为 6，不可能等于 4。

若 $k=3$，式 (*) 仅在 $n=6$ 时成立，因为此时

$$4\cdot 3\cdot 2\cdot 1=24=2^2\cdot 3!,$$

而左边随 n 严格递增。若 $k\geqslant 4$，左边在 $n=2k$ 时已经至少为 $(2k-2)!$，且

$$(2k-2)!>2^{k-1}k!,$$

故也无解。

所以除 $(n,k)=(6,3)$ 外，必有 $k=1$。特别地，当 $n\neq 2,6$ 时，每个自同构都把对换映为对换。由第（1）问，

$$\mathrm{Aut}(S_n)=\mathrm{Inn}(S_n).$$

最后考虑满同态

$$\begin{aligned} S_n &\longrightarrow \mathrm{Inn}(S_n),\\ \pi &\longmapsto \left(\tau\mapsto \pi\tau\pi^{-1}\right). \end{aligned}$$

当 $n\geqslant 3$ 时，只有恒等置换与 S_n 的每个对换都交换，所以该同态的核为 $\{e\}$，从而它也是单射。因此

$$\boxed{\mathrm{Aut}(S_n)=\mathrm{Inn}(S_n)\cong S_n}\qquad (n\neq 2,6).$$

(3) 当 $n=2$ 时，$S_2\cong\mathbb{Z}_2$，且其唯一非恒等元素必须被任意自同构固定，故

$$\mathrm{Aut}(S_2)=\{\mathrm{id}\}.$$

于是

$$\boxed{\mathrm{Aut}(S_2)\ncong S_2}.$$

当 $n=6$ 时，结论也不成立。由 S_6 的例外外自同构定理，S_6 存在外自同构，并且

$$|\mathrm{Aut}(S_6)|=1440.$$

而

$$|S_6|=6!=720.$$

同构的有限群必有相同的阶，故

$$\boxed{\mathrm{Aut}(S_6)\ncong S_6}.$$

□

2.5 陪集、指数、*Lagrange* 定理

1. 设 $\mathbb{R}^+$ 为所有正实数在通常数的乘法下构成的群，求 $\mathbb{R}^+$ 在实数域的乘法群 $\mathbb{R}^*$ 中的指数。

解 记 $[\mathbb{R}^*:\mathbb{R}^+]$ 表示 $\mathbb{R}^+$ 在 $\mathbb{R}^*$ 中的左陪集个数，任取 $a\in\mathbb{R}^*$。

若 $a>0$，则 $a\in\mathbb{R}^+$,，从而 $a\mathbb{R}^+=\mathbb{R}^+$.

若 $a<0$，则 $a\mathbb{R}^+=\{ax\mid x>0\}=\mathbb{R}^-$,，其中 $\mathbb{R}^-$ 表示所有负实数构成的集合。

因此 $\mathbb{R}^*=\mathbb{R}^+\cup\mathbb{R}^-$, 且两个左陪集分别为 $\mathbb{R}^+,-\mathbb{R}^+$.

故

$$\boxed{[\mathbb{R}^*:\mathbb{R}^+]=2}.$$

□

2. 证明不存在恰有两个指数为 2 的子群的群。

解 反设群 G 中存在恰有两个指数为 2 的子群，记为 $H, K \leqslant G$，且 $H \neq K$。

令

$$M = (H \cap K) \cup ((G \setminus H) \cap (G \setminus K)).$$

下面证明 M 是 G 的一个指数为 2 的子群，从而得到矛盾。

首先证明 M 是子群。

显然 $e \in H \cap K \subseteq M$。任取 $x, y \in M$，若 $x, y \in H \cap K$，则 $xy \in H \cap K \subseteq M$；若 $x, y \in (G \setminus H) \cap (G \setminus K)$，下面证明 $xy \in H \cap K$：

因为 $[G : H] = 2$，所以 H 的两个左陪集为 H 与 $G \setminus H$。又因为 $x \notin H$，有 $xH = G \setminus H$。由于 $x^{-1} \notin H$，故 $x^{-1}H = G \setminus H = xH$。于是存在 $h \in H$ 使得 $x^{-1} = xh$，从而 $x^2 = h^{-1} \in H$。

又因为 $y \notin H$，存在 $h_1 \in H$ 使得 $y = xh_1$。因此

$$xy = x^2 h_1 \in H.$$

同理可得

$$xy \in K.$$

故

$$xy \in H \cap K \subseteq M.$$

另外，若 $x \in H \cap K$，$y \in (G \setminus H) \cap (G \setminus K)$，则因为 H, K 均为子群，有

$$xy \notin H, \qquad xy \notin K,$$

故

$$xy \in (G \setminus H) \cap (G \setminus K) \subseteq M.$$

所以 M 对乘法封闭。

若 $x \in M$，则显然 x^{-1} 与 x 在 H、K 中的所属情况相同，因此 $x^{-1} \in M$。

故

$$M \leqslant G.$$

下面证明 M 的指数为 2。

由于 $H \neq K$，存在

$$a \in H \setminus K.$$

则

$$a \notin M,$$

因为 a 在 H, K 中的所属情况不同。

又任取 $g \notin M$，则 g 必在一个子群中而不在另一个子群中。因此 gM 是 M 的补集。

所以 M 在 G 中只有两个左陪集：

$$M, \qquad G \setminus M.$$

故

$$[G : M] = 2.$$

于是 M 是 G 的另一个指数为 2 的子群。

又显然 $M \neq H$，$M \neq K$，因此 G 至少有三个指数为 2 的子群：

$$H, \quad K, \quad M,$$

与假设矛盾。

因此不存在恰有两个指数为 2 的子群的群。 □

3. 设 G 为群，$H, K \leqslant G$，证明 $H \cap K$ 的任一左陪集都是 H 的一个左陪集与 K 的一个左陪集的交。

解 设 $a(H \cap K)$ 是 $H \cap K$ 的任一左陪集。

因为 $H \cap K \subseteq H$ 且 $H \cap K \subseteq K$，所以有

$$a(H \cap K) \subseteq aH \cap aK.$$

反过来，任取 $x \in aH \cap aK$。

则存在 $h \in H$，$k \in K$，使得 $x = ah = ak$。左乘 a^{-1}，得到 $h = k$。

于是该元素同时属于 H 与 K，即 $h \in H \cap K$。因此 $x = ah \in a(H \cap K)$。

所以

$$aH \cap aK = a(H \cap K).$$

故 $H \cap K$ 的任一左陪集都是 H 的一个左陪集与 K 的一个左陪集的交。 □

4. 设 G 为群，$H, K \leqslant G$，且 $[G : H]$ 和 $[G : K]$ 均有限，证明 $[G : H \cap K]$ 有限。

解 设 $[G : H] = m$，$[G : K] = n$。

考虑映射

$$\varphi : G/(H \cap K) \to G/H \times G/K, \qquad \varphi(g(H \cap K)) = (gH, gK).$$

下面证明 φ 为单射。

若

$$\varphi(g(H \cap K)) = \varphi(g'(H \cap K)),$$

则有 $gH = g'H$ 且 $gK = g'K$。

由陪集相等的性质，$g^{-1}g' \in H$ 且 $g^{-1}g' \in K$，故 $g^{-1}g' \in H \cap K$。

因此

$$g(H \cap K) = g'(H \cap K),$$

所以 φ 是单射。

由于 G/H 和 G/K 均为有限集，$G/H \times G/K$ 也是有限集。

而 $G/(H \cap K)$ 可单射到有限集 $G/H \times G/K$，故 $G/(H \cap K)$ 有限。

因此

$$[G : H \cap K] < \infty.$$

□

5. 设 G 为群，$H, K \leqslant G$，$a, b \in G$，证明：若 $Ha = Kb$，则 $H = K$。

解 由

$$Ha = Kb,$$

右乘 a^{-1}，得

$$H = Kba^{-1}.$$

令 $c = ba^{-1}$，则 $H = Kc$。

因为 $e \in H$，所以 $e \in Kc$。故存在 $k \in K$，使得 $e = kc$。
于是 $c = k^{-1} \in K$。
因此 $Kc = K$，从而

$$H = Kc = K.$$

故 $H = K$。 □

6. 设 $H = \{z \in \mathbb{C} \mid |z| = 1\}$，给出 H 在群 $\mathbb{C}^*$ 中的左陪集的几何解释。

解 任取 $z \in \mathbb{C}^*$，其左陪集为 $zH = \{zw \mid |w| = 1\}$。
对于任意 $zw \in zH$，有

$$|zw| = |z||w| = |z|.$$

因此

$$zH = \{u \in \mathbb{C}^* \mid |u| = |z|\}.$$

所以 H 在 $\mathbb{C}^*$ 中的左陪集在几何上表示为：以原点为圆心、半径为 $|z|$ 的圆。
因此 $\mathbb{C}^*$ 被 H 的左陪集划分成所有以原点为中心的同心圆。 □

7. 设 H, K 是群 G 的两个子群，对于 $g \in G$，集合 $HgK = \{hgk \mid h \in H, k \in K\}$ 称为 G 关于子群 H 和 K 的一个双陪集，证明：
(1) G 可以写成关于子群 H 和 K 的双陪集的不交并；
(2) 若 H, K 均有限，则

$$|HgK| = |H|[K : K \cap g^{-1}Hg] = |K|[H : H \cap gKg^{-1}].$$

解 (1) 先证明任意两个双陪集要么相等，要么不交。
设

$$Hg_1K \cap Hg_2K \neq \varnothing.$$

则存在 $x \in G$，使得

$$x = h_1g_1k_1 = h_2g_2k_2,$$

其中 $h_1, h_2 \in H$，$k_1, k_2 \in K$。
于是

$$g_2 = h_2^{-1}h_1g_1k_1k_2^{-1}.$$

令 $h = h_2^{-1}h_1 \in H$，$k = k_1k_2^{-1} \in K$，则 $g_2 = hg_1k$。
因此

$$Hg_2K = H(hg_1k)K.$$

由于 H, K 是子群，有 $Hh = H$，$kK = K$，故

$$Hg_2K = Hg_1K.$$

所以若两个双陪集有公共元素，则它们相等。
又因为任意 $g \in G$ 都属于双陪集 HgK，故所有双陪集覆盖 G。
因此 G 可以写成双陪集的不交并。
(2) 注意到

$$HgK = \bigcup_{k \in K} Hgk.$$

下面判断两个集合 Hgk_1 与 Hgk_2 何时相等。

有

$$Hgk_1 = Hgk_2$$

当且仅当

$$gk_1k_2^{-1}g^{-1} \in H.$$

这等价于

$$k_1k_2^{-1} \in g^{-1}Hg.$$

由于 $k_1, k_2 \in K$，故等价于

$$k_1k_2^{-1} \in K \cap g^{-1}Hg.$$

因此不同的 Hgk 恰好对应于 K 关于子群 $K \cap g^{-1}Hg$ 的不同左陪集。
所以 HgK 中不同的集合 Hgk 的个数为

$$[K : K \cap g^{-1}Hg].$$

每个 Hgk 都是 H 的一个左陪集，因此大小为 $|H|$。
故

$$|HgK| = |H|[K : K \cap g^{-1}Hg].$$

同理，将 HgK 看成右陪集的并，可得

$$|HgK| = |K|[H : H \cap gKg^{-1}].$$

因此

$$\boxed{|HgK| = |H|[K : K \cap g^{-1}Hg] = |K|[H : H \cap gKg^{-1}]}.$$

□

2.6 轨道长度和类方程

1. 设 $G \leqslant S_n$，证明
(1) $G \cap A_n \leqslant G$;
(2) 如果 G 中有奇置换，那么 G 中奇偶置换的个数相等。

解 (1) 由于 $G, A_n \leqslant S_n$，只需证明 $G \cap A_n$ 对群运算封闭。任取 $\sigma, \tau \in G \cap A_n$，则 $\sigma, \tau \in G$，故 $\sigma\tau^{-1} \in G$。又因为 $\sigma, \tau \in A_n$，且 A_n 为子群，所以 $\sigma\tau^{-1} \in A_n$。
因此 $\sigma\tau^{-1} \in G \cap A_n$，故

$$G \cap A_n \leqslant G.$$

(2) 设 $\alpha \in G$ 为奇置换。定义映射

$$\varphi : G \cap A_n \to G \setminus A_n, \qquad \varphi(\sigma) = \alpha\sigma.$$

由于 α 为奇置换，而 σ 为偶置换，所以 $\alpha\sigma$ 为奇置换，故 φ 定义良好。
若 $\varphi(\sigma_1) = \varphi(\sigma_2)$，则 $\alpha\sigma_1 = \alpha\sigma_2$，从而 $\sigma_1 = \sigma_2$，故 φ 为单射。
任取 $\tau \in G \setminus A_n$，则 τ 为奇置换。因为奇置换乘奇置换为偶置换，所以

$$\alpha^{-1}\tau \in G \cap A_n.$$

并且

$$\varphi(\alpha^{-1}\tau) = \tau.$$

故 φ 为双射。因此 G 中奇置换与偶置换的个数相等。 □

2. 设 n 为奇数，G 为 $2n$ 阶群，证明 G 有指数为 2 的子群。

解 对 G 中任意元素 g，定义映射

$$f_g : G \to G, \qquad x \mapsto gx.$$

将 G 中元素编号为 $1, 2, \ldots, 2n$，则每个 f_g 都对应于 S_{2n} 中的一个置换。

令

$$G_0 = \{g \in G \mid f_g \text{ 为偶置换}\}.$$

下面证明 G_0 是 G 的指数为 2 的子群。

我们知道偶置换的乘积、逆均为偶置换，故 G_0 为 G 的子群，即 $G_0 \leqslant G$，下面证明 $[G : G_0] = 2$。

因为 $|G| = 2n$，取 $g \in G$，且 $g \neq e$ 且 $o(g) = 2$（我们知道偶数阶群都有二阶元素），考虑对应的置换 f_g。

由于

$$f_g(f_g(x)) = g^2 x = x,$$

所以 f_g 的轮换分解中只有二轮换，又因为我们可以知道 f_g 没有不动点，因此 f_g 可表示为 n 个不相交二轮换的乘积。因为 n 为奇数，故 f_g 是奇置换。

于是 G 中存在使 f_g 为奇置换的元素。

由第一题可知，在置换群

$$\{f_g \mid g \in G\}$$

中，奇置换与偶置换的个数相等。

又因为

$$g \mapsto f_g$$

是一一对应，所以 G 中满足 f_g 为偶置换的元素个数等于满足 f_g 为奇置换的元素个数。

因此

$$|G_0| = \frac{|G|}{2} = n.$$

故

$$[G : G_0] = \frac{|G|}{|G_0|} = 2.$$

所以 G 存在指数为 2 的子群。 □

3. 设 $\sigma = (12\cdots n) \in S_n$，求 σ 在 S_n 中的中心化子 $C_{S_n}(\sigma)$。

进一步地，设 $\sigma \in S_n$ 的型为 $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$，求 σ 在 S_n 中的中心化子的阶以及与 σ 共轭的置换个数。

解 先考虑 $\sigma = (12\cdots n)$。

设 $\tau \in C_{S_n}(\sigma)$，则

$$\tau\sigma = \sigma\tau.$$

设 $\tau(1) = i$，则

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

因此 τ 完全由 $\tau(1)$ 决定。

而 $\tau(1)$ 有 n 种取法，分别对应

$$\tau = \sigma^k, \qquad k = 0, 1, \ldots, n-1.$$

故

$$\boxed{C_{S_n}(\sigma) = \langle\sigma\rangle},$$

且

$$|C_{S_n}(\sigma)| = n.$$

一般地，设 σ 的型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$。若 τ 与 σ 可交换，则 τ 必须将 σ 的同长度轮换互相置换。

对于长度为 i 的轮换：

- λ_i 个轮换之间可以任意交换，有 $\lambda_i!$ 种；
- 每个轮换内部可以循环移动，有 i^{λ_i} 种。

因此

$$\boxed{|C_{S_n}(\sigma)| = \prod_{i=1}^{n} i^{\lambda_i}\lambda_i!}.$$

由共轭类大小公式，

$$|\operatorname{Cl}(\sigma)| = \frac{|S_n|}{|C_{S_n}(\sigma)|}.$$

由于 $|S_n| = n!$，故与 σ 共轭的置换个数为

$$\boxed{\frac{n!}{\prod_{i=1}^{n} i^{\lambda_i}\lambda_i!}}.$$

□

4. 设群 G 作用在集合 M 上，定义

$$M_0 = \{x \in M \mid g \circ x = x,\ \forall g \in G\}$$

为作用的不动点构成的集合。证明：若 G 为 p 群，则有

$$|M| \equiv |M_0| \pmod{p}.$$

解 将 M 分解为 G 的各个轨道的不交并。若 $x \in M_0$，则其轨道只有一个元素；若 $x \notin M_0$，则由轨道–稳定子定理，

$$|G \circ x| = [G : G_x] > 1.$$

由于 G 为 p 群，$[G : G_x]$ 是 p 的幂，故此时 $p \mid |G \circ x|$。

因此，除不动点外，其余各轨道的大小均为 p 的倍数，从而

$$|M| = |M_0| + \sum_{\substack{\text{非平凡}\\ \text{轨道}O}} |O| \equiv |M_0| \pmod{p}.$$

□

5. 设 H 是有限群 G 的真子群，证明：

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

进一步地，若 G 为无限群，该结论是否成立？请证明或举出反例。

解 先设 G 为有限群。令

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

为 H 的正规化子，则 H 的不同共轭子群个数为 $k = [G : N_G(H)]$。由于 $H \leqslant N_G(H)$，有

$$k \leqslant [G : H] = \frac{|G|}{|H|}.$$

每个共轭子群都有 $|H|-1$ 个非单位元，而所有共轭子群都含单位元，故

$$\left|\bigcup_{g\in G} gHg^{-1}\right| \leqslant 1+k(|H|-1) \leqslant 1+\frac{|G|}{|H|}(|H|-1).$$

于是

$$\left|\bigcup_{g\in G} gHg^{-1}\right| \leqslant |G|+1-[G:H].$$

因为 $H<G$，故 $[G:H]\geqslant 2$，从而

$$\left|\bigcup_{g\in G} gHg^{-1}\right| \leqslant |G|-1<|G|.$$

因此

$$G \neq \bigcup_{g\in G} gHg^{-1}.$$

当 G 为无限群时，结论有可能成立。

取 G 为自然数集 $\mathbb{N}$ 上所有有限支撑置换构成的群，即每个 $\sigma\in G$ 只移动有限多个元素。令 $H=\{\sigma\in G\mid \sigma(1)=1\}$，则 $H<G$。

任取 $\sigma\in G$。由于 σ 只有有限个非不动点，可取 $m\in\mathbb{N}$ 使 $\sigma(m)=m$。再取 $g\in G$ 使 $g(1)=m$，则

$$gHg^{-1}=\{\tau\in G\mid \tau(m)=m\}.$$

故 $\sigma\in gHg^{-1}$。由于 σ 任意，

$$G=\bigcup_{g\in G} gHg^{-1}.$$

所以无限群时原结论有可能成立。 □

6. 写出对称群 S_5 的类方程。

解 S_5 中两个置换共轭当且仅当它们的轮换型相同，因此各轮换型分别构成一个共轭类。

各类的代表元及元素个数为：

轮换型	代表元	元素个数
1^5	(1)	1
$1^3 2$	(12)	$\binom{5}{2}=10$
$1\,2^2$	$(12)(34)$	$5\cdot 3=15$
$1^2 3$	(123)	$\binom{5}{3}\cdot 2=20$
$2\,3$	$(123)(45)$	$\binom{5}{3}\cdot 2=20$
$1\,4$	(1234)	$\binom{5}{4}\cdot 3!=30$
5	(12345)	$4!=24$

故 S_5 的类方程为

$$\boxed{120=1+10+15+20+20+30+24}.$$

□

2.7 正规子群与商群

1. 举例说明若 $H \trianglelefteq K$ 且 $K \trianglelefteq G$，则不一定有 $H \trianglelefteq G$。

解 取 $G = S_4$，

$$K = \{e, (12)(34), (13)(24), (14)(23)\},$$

并令 $H = \{e, (12)(34)\}$。

由于 K 为交换群，故 $H \trianglelefteq K$。又共轭保持轮换型，所以 K 在 S_4 的共轭下保持不变，故 $K \trianglelefteq S_4$。

但

$$(123)(12)(34)(123)^{-1} = (14)(23) \notin H,$$

故 $H \not\trianglelefteq S_4$。 □

2. 设 G 为群且 $H, K \trianglelefteq G$，证明 $HK \trianglelefteq G$。

解 任取 $h \in H, k \in K$。由于 $H \trianglelefteq G$，有 $k^{-1}hk \in H$，故 $hk = k(k^{-1}hk) \in KH$，所以 $HK \subseteq KH$。同理 $KH \subseteq HK$，从而 $HK = KH$。

因此由 $HK = KH$ 可知 $HK \leqslant G$。

又对任意 $g \in G$，

$$g(HK)g^{-1} = (gHg^{-1})(gKg^{-1}) = HK,$$

故 $HK \trianglelefteq G$。 □

3. 设 S 为群 G 的非空子集，令

$$C_G(S) = \{x \in G \mid xa = ax,\ \forall a \in S\}, \qquad N_G(S) = \{x \in G \mid xS = Sx\}.$$

$C_G(S)$ 和 $N_G(S)$ 分别称为 S 在 G 中的中心化子和正规化子。

(1) 证明 $C_G(S)$ 和 $N_G(S)$ 都是 G 的子群；

(2) 证明 $C_G(S) \leqslant N_G(S)$；

(3) 设 $n \geqslant 2$，记 $G = \mathrm{GL}_n(\mathbb{R})$ 中上三角形矩阵构成的子群为 B，上三角形且对角线元素全为 1 的矩阵构成的子群为 U，证明

$$N_G(U) = B, \qquad N_G(B) = B.$$

解

(1) 任取 $x, y \in C_G(S)$。对任意 $a \in S$，有 $ya = ay$，故 $y^{-1}a = ay^{-1}$，于是

$$(xy^{-1})a = x(ay^{-1}) = a(xy^{-1}).$$

所以 $xy^{-1} \in C_G(S)$，由子群判定法得 $C_G(S) \leqslant G$。

注意 $xS = Sx$ 等价于 $xSx^{-1} = S$。若 $x, y \in N_G(S)$，则 $y^{-1}Sy = S$，从而

$$xy^{-1}S(xy^{-1})^{-1} = x(y^{-1}Sy)x^{-1} = xSx^{-1} = S.$$

故 $xy^{-1} \in N_G(S)$，所以 $N_G(S) \leqslant G$。

(2) 若 $x \in C_G(S)$，则对任意 $a \in S$ 有 $xa = ax$，所以 $xS = Sx$，即 $x \in N_G(S)$。故

$$C_G(S) \leqslant N_G(S).$$

(3) 记 $V_i = \mathrm{span}\{e_1, \dots, e_i\}$，$i = 1, \dots, n$。

先证明 $N_G(U) = B$。对任意 $b \in B$，直接计算可知 $bUb^{-1} = U$，故 $B \subseteq N_G(U)$。

反之，设 $g \in N_G(U)$。注意 V_1 恰为 U 中所有矩阵的公共不动点空间，且递归地

$$V_i = \{v \in \mathbb{R}^n \mid (u - I)v \in V_{i-1},\ \forall u \in U\}.$$

由 $gUg^{-1} = U$，依次可得 $gV_i = V_i$，$i = 1, \dots, n$。因此 g 的矩阵必为上三角矩阵，即 $g \in B$。故

$$N_G(U) = B.$$

再证明 $N_G(B) = B$。显然 $B \subseteq N_G(B)$。若 $g \in N_G(B)$，则 $gBg^{-1} = B$。而 U 恰为 B 中所有特征值均为 1 的矩阵，共轭不改变特征值，故 $gUg^{-1} = U$。于是 $g \in N_G(U) = B$。

因此

$$\boxed{N_G(U) = B, \qquad N_G(B) = B}.$$

□

4. 考虑正方形的对称群，即二面体群

$$D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\},$$

其中 r 为逆时针旋转 $\pi/2$ 角度，s 为关于一条对角线的反射。记

$$V = \{e, r^2, s, sr^2\}, \qquad H = \{e, s\}.$$

证明：$V \trianglelefteq D_4$，$H \trianglelefteq V$，但是 H 不是 D_4 的正规子群。

解 由于 $|D_4| = 8$，$|V| = 4$，故 $[D_4 : V] = 2$，所以 $V \trianglelefteq D_4$。

同理，$|V| = 4$，$|H| = 2$，故 $[V : H] = 2$，所以 $H \trianglelefteq V$。

但由 $srs = r^{-1}$ 可得 $rsr^{-1} = sr^2 \notin H$，故

$$\boxed{H \not\trianglelefteq D_4}.$$

□

5. 给出二面体群 D_{10} 的全部正规子群。

解 写成

$$D_{10} = \langle r, s \mid r^{10} = e,\ s^2 = e,\ srs = r^{-1} \rangle.$$

首先，$\langle r \rangle$ 是 10 阶循环群，其全部子群为 $\{e\}$、$\langle r^5 \rangle$、$\langle r^2 \rangle$ 和 $\langle r \rangle$。对 $d = 1, 2, 5, 10$，有

$$r\langle r^d \rangle r^{-1} = \langle r^d \rangle, \qquad s\langle r^d \rangle s^{-1} = \langle r^{-d} \rangle = \langle r^d \rangle,$$

故这些子群均为 D_{10} 的正规子群。

再令

$$E = \langle r^2, s \rangle = \{r^{2j}, sr^{2j} \mid 0 \leqslant j \leqslant 4\},$$

$$O = \langle r^2, sr \rangle = \{r^{2j}, sr^{2j+1} \mid 0 \leqslant j \leqslant 4\}.$$

二者均有 10 个元素，故在 D_{10} 中的指数均为 2，从而 $E, O \trianglelefteq D_{10}$。

下面证明没有其他正规子群。设 $N \trianglelefteq D_{10}$。若 $N \subseteq \langle r \rangle$，则 N 只能是上述四个循环子群之一。

若 $N \not\subseteq \langle r\rangle$，则存在某个反射 $sr^i \in N$。由正规性，$r(sr^i)r^{-1} = sr^{i-2} \in N$，于是

$$(sr^{i-2})(sr^i) = r^2 \in N.$$

若 i 为偶数，则 $s = (sr^i)r^{-i} \in N$，故 $E \leqslant N$；若 i 为奇数，则 $sr = (sr^i)r^{1-i} \in N$，故 $O \leqslant N$。由于 $|E| = |O| = 10$ 而 $|D_{10}| = 20$，由 Lagrange 定理，N 只能等于 E、O 或 D_{10}。

因此，D_{10} 的全部正规子群为

$$\boxed{\{e\},\quad \langle r^5\rangle,\quad \langle r^2\rangle,\quad \langle r\rangle,\quad \langle r^2, s\rangle,\quad \langle r^2, sr\rangle,\quad D_{10}}.$$

□

6. 设 G 为一个群，H 为 G 的一个阶为 m 的子群。

(1) 证明：若 H 是 G 的唯一一个阶为 m 的子群，那么 $H \trianglelefteq G$；

(2) 如果 $H \trianglelefteq G$，H 是否为 G 的唯一一个阶为 m 的子群？如果正确，请给出证明；如果错误，请给出一个反例。

解

(1) 任取 $g \in G$，共轭子群 gHg^{-1} 与 H 元素个数相同，故 $|gHg^{-1}| = m$。由 H 是唯一的 m 阶子群，必有 $gHg^{-1} = H$。因此

$$\boxed{H \trianglelefteq G}.$$

(2) 不一定。取 Klein 四元群

$$V_4 = \{e, a, b, c\},$$

其中 $a^2 = b^2 = c^2 = e$。由于 V_4 为交换群，其所有子群均为正规子群。

但 $\{e, a\}$、$\{e, b\}$、$\{e, c\}$ 都是 V_4 的 2 阶子群。因此正规子群不一定是同阶子群中唯一的。

□

Klein 四元群： Klein 四元群通常记作 V_4，是一个 4 阶非循环交换群，可以写成

$$V_4 = \{e, a, b, c\},$$

其中

$$a^2 = b^2 = c^2 = e, \qquad ab = c, \quad bc = a, \quad ca = b.$$

在置换群 S_4 中，一个典型的 Klein 四元群为

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

此外，

$$V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2,$$

因此 V_4 是 4 阶群中除 $\mathbb{Z}_4$ 外的另一种同构类型。

7. 设有限群 G 在集合 M 上的作用传递，$N \trianglelefteq G$，证明 N 在 M 上的同样作用下每个轨道长度均相等。

解 任取 $x, y \in M$。由于 G 的作用传递，存在 $g \in G$ 使 $y = g \circ x$。记 N 经过 x 的轨道为 $\mathrm{Orb}_N(x) = \{n \circ x \mid n \in N\}$，则

$$\begin{aligned}\mathrm{Orb}_N(y) &= \{n \circ (g \circ x) \mid n \in N\} \\ &= \{g \circ ((g^{-1}ng) \circ x) \mid n \in N\} \\ &= g \circ \mathrm{Orb}_N(x),\end{aligned}$$

其中最后一个等号利用了 $g^{-1}Ng = N$。

由于 $z \mapsto g \circ z$ 是 M 上的双射，故 $|\mathrm{Orb}_N(y)| = |\mathrm{Orb}_N(x)|$。因此 N 在 M 上的所有轨道长度均相等。□

8. 设 G 是有限群，$N \trianglelefteq G$，且 $|N|$ 与 $|G/N|$ 互素。对于 $a \in G$，若 $o(a) \mid |N|$，证明 $a \in N$。

解 设 $o(aN) = m$。由于 $(aN)^{o(a)} = N$，故 $m \mid o(a)$，从而 $m \mid |N|$。另一方面，由 Lagrange 定理，$m \mid |G/N|$。因为 $\gcd(|N|, |G/N|) = 1$，所以 $m = 1$，即 $aN = N$。因此 $a \in N$。□

9. 设 G 为一个群，证明 G 的任意指数有限的子群都包含一个在 G 中指数有限的正规子群。

解 设 $H \leqslant G$ 且 $[G : H] < \infty$。由于 $H \leqslant N_G(H)$，故 $[G : N_G(H)] \leqslant [G : H] < \infty$，所以 H 只有有限个不同的共轭子群，记为 $H_1, H_2, \ldots, H_r$。

令

$$K = \bigcap_{i=1}^{r} H_i = \bigcap_{g \in G} gHg^{-1}.$$

由于每个 H_i 与 H 共轭，故 $[G : H_i] = [G : H] < \infty$。反复利用有限指数子群之交仍为有限指数子群，可得 $[G : K] < \infty$。

又因为 H 是这些共轭子群之一，所以 $K \leqslant H$。对任意 $x \in G$，

$$xKx^{-1} = \bigcap_{g \in G} (xg)H(xg)^{-1} = \bigcap_{g \in G} gHg^{-1} = K.$$

因此 $K \trianglelefteq G$。故 H 包含一个在 G 中指数有限的正规子群 K。□

10. 设 A, B, C 是群 G 的子群，并且 $A \leqslant B$，证明：

(1) $AC \cap B = A(B \cap C)$；

(2) 若还有 $A \cap C = B \cap C$ 和 $AC = BC$，则有 $A = B$。

解

(1) 若 $x \in AC \cap B$，则 $x = ac$，其中 $a \in A$, $c \in C$。因 $A \leqslant B$ 且 $x \in B$，有 $c = a^{-1}x \in B$，故 $c \in B \cap C$，从而 $x \in A(B \cap C)$。反之，若 $x = ac \in A(B \cap C)$，则 $a, c \in B$，故 $x \in B$，又 $x \in AC$，所以 $x \in AC \cap B$。因此 $AC \cap B = A(B \cap C)$。

(2) 已知 $A \leqslant B$，只需证 $B \leqslant A$。任取 $b \in B$，则 $b \in BC = AC$，故 $b = ac$，其中 $a \in A$, $c \in C$。又 $a, b \in B$，故 $c = a^{-1}b \in B \cap C = A \cap C$，于是 $c \in A$，从而 $b = ac \in A$。因此 $A = B$。

□

11. 证明群的 2 阶正规子群必在群的中心里。

解 设 $H=\{e,a\}\trianglelefteq G$。任取 $g\in G$，由正规性知 $gag^{-1}\in H$。又 $gag^{-1}\neq e$，故 $gag^{-1}=a$，即 $ga=ag$。因此 $a\in Z(G)$，从而 $H\leqslant Z(G)$。 □

12. 设 $n\geqslant 5$，证明 A_n 是 S_n 的唯一非平凡正规子群。

解 由定理 2.7.3 的证明，A_n 为单群。设 $N\trianglelefteq S_n$ 是非平凡真正规子群，则 $N\cap A_n\trianglelefteq A_n$，故 $N\cap A_n=\{e\}$ 或 A_n。

若 $N\cap A_n=A_n$，则 $A_n\leqslant N<S_n$。因 $[S_n:A_n]=2$，故 $N=A_n$。

若 $N\cap A_n=\{e\}$，则 N 中所有非单位元均为奇置换。任取 $\sigma\in N\setminus\{e\}$，有 $\sigma^2\in N\cap A_n=\{e\}$。若 $\tau\in N\setminus\{e\}$，则 $\sigma\tau\in N\cap A_n=\{e\}$，故 $\tau=\sigma^{-1}=\sigma$。于是 $|N|=2$。由第 11 题，$N\leqslant Z(S_n)$。但 $n\geqslant 5$ 时 $Z(S_n)=\{e\}$，矛盾。

因此只能有 $N=A_n$，故 A_n 是 S_n 的唯一非平凡真正规子群。 □

13. 证明有限群 G 是二面体群的充要条件是 G 可由两个 2 阶元素生成。（这里 A_4 的 4 阶子群 V_4 也看成 4 阶二面体群。）

解 若 $G=D_n$，设 r 为旋转，s 为反射，则 s 与 rs 均为 2 阶元素，且 $r=(rs)s$，故 $D_n=\langle s,rs\rangle$。

反之，设 $G=\langle a,b\rangle$，其中 $o(a)=o(b)=2$，令 $r=ab$，$o(r)=n$。则 $b=ar$，且 $ara=ba=r^{-1}$，故 $G=\langle r,a\rangle$，每个元素均可写成 r^i 或 r^ia 的形式。

又 $a\notin\langle r\rangle$，否则 $G=\langle r\rangle$ 为循环群，却含有两个不同的 2 阶元素，矛盾。因此 $\langle r\rangle$ 与 $\langle r\rangle a$ 不相交，$|G|=2n$。于是 $G=\langle r,a\mid r^n=a^2=e,\ ara=r^{-1}\rangle$，故 G 为二面体群。 □

14. 设 G 为一个有限群，其类方程为 $20=1+4+5+5+5$。

(1) G 中有没有 5 阶子群？如果有，是不是 G 的正规子群？

(2) G 中有没有 4 阶子群？如果有，是不是 G 的正规子群？

解 由类方程 $20=1+4+5+5+5$ 可知，$|G|=20$，G 中除单位元 $\{e\}$ 外，有一个大小为 4 的共轭类和三个大小为 5 的共轭类。对任意 $x\in G$，由轨道—稳定子定理，

$$|\operatorname{Cl}(x)|=[G:C_G(x)]=\frac{|G|}{|C_G(x)|},$$

其中 $\operatorname{Cl}(x)$ 表示 x 的共轭类。

(1) 取大小为 4 的共轭类中的元素 x。由上式有 $[G:C_G(x)]=4$，故 $|C_G(x)|=5$。因此 $C_G(x)$ 本身就是一个 5 阶子群，所以 G 中存在 5 阶子群。

下面证明它是正规子群。因为 $x\in C_G(x)$ 且 $x\neq e$，由 Lagrange 定理，$o(x)\mid 5$，故 $o(x)=5$，从而 $C_G(x)=\langle x\rangle$。记 $H=\langle x\rangle=\{e,x,x^2,x^3,x^4\}$。

对任意 $k=1,2,3,4$，由于 H 是循环群，H 中每个元素都与 x^k 交换，因此 $H\leqslant C_G(x^k)$。于是 $5=|H|\mid|C_G(x^k)|$。另一方面，$C_G(x^k)\leqslant G$，故 $|C_G(x^k)|\mid 20$，所以 $|C_G(x^k)|$ 只能为 $5,10$ 或 20。因此 x^k 的共轭类大小只能为 $4,2$ 或 1。

但由题给类方程，非单位元的共轭类大小只有 4 或 5，不存在大小为 2 的共轭类；又大小为 1 的共轭类只有 $\{e\}$，而 $x^k\neq e$。故 x,x^2,x^3,x^4 的共轭类大小都为 4。

题给类方程中只有一个大小为 4 的共轭类，因此 x, x^2, x^3, x^4 都属于这个共轭类。该共轭类恰有 4 个元素，故它就是

$$\{x, x^2, x^3, x^4\} = H \setminus \{e\}.$$

所以任意 $g \in G$ 共轭都把 $H \setminus \{e\}$ 映到自身，同时 $geg^{-1} = e$，从而 $gHg^{-1} = H$。因此 $H \trianglelefteq G$。

故 G 中有 5 阶子群，并且这个 5 阶子群是正规子群。

(2) 取任意一个大小为 5 的共轭类中的元素 y。由 $[G : C_G(y)] = 5$，有 $|C_G(y)| = 4$，所以 $C_G(y)$ 是一个 4 阶子群。因此 G 中存在 4 阶子群。

下面证明 $C_G(y)$ 不是正规子群。若 $C_G(y) \trianglelefteq G$，因为 $y \in C_G(y)$，所以对任意 $g \in G$，都有 $gyg^{-1} \in C_G(y)$。因此 y 的整个共轭类都包含在 $C_G(y)$ 中。然而 y 的共轭类有 5 个元素，而 $|C_G(y)| = 4$，不可能包含这 5 个不同的元素，矛盾。因此 $C_G(y)$ 不是 G 的正规子群。

故 G 中有 4 阶子群，并且上述 4 阶子群不是正规子群。

□

15. 设 G 和 G' 为两个群，N 和 N' 分别为 G 和 G' 的正规子群，判断以下说法是否正确，证明或给出反例：

(1) 若 $G \cong G'$ 且 $N \cong N'$，则有 $G/N \cong G'/N'$；

(2) 若 $N \cong N'$ 且 $G/N \cong G'/N'$，则有 $G \cong G'$；

(3) 若 $G \cong G'$ 且 $G/N \cong G'/N'$，则有 $N \cong N'$。

解 三种说法均不正确。下面均取阿贝尔群，因此所取子群都是正规子群。

(1) 取 $G = G' = \mathbb{Z}_4 \times \mathbb{Z}_2$，并令 $N = \langle (2,0) \rangle$，$N' = \langle (0,1) \rangle$。显然 $N \cong N' \cong \mathbb{Z}_2$，且 $G \cong G'$。

在 G/N 中，

$$2\big((1,0) + N\big) = (2,0) + N = N,$$

故 $(1,0) + N$ 的阶为 2；同理 $(0,1) + N$ 和 $(1,1) + N$ 的阶也均为 2。因此 G/N 的三个非单位元的阶都为 2，故 $G/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$。

另一方面，在 G'/N' 中，$(1,0) + N'$ 的阶为 4，因为 $(2,0) \notin N'$，而 $(4,0) = (0,0) \in N'$。又 $|G'/N'| = 4$，故 $G'/N' \cong \mathbb{Z}_4$。

因此 $G/N \ncong G'/N'$，所以 (1) 错误。

(2) 取 $G = \mathbb{Z}_4$，$N = \langle 2 \rangle = \{0, 2\}$；取 $G' = \mathbb{Z}_2 \times \mathbb{Z}_2$，$N' = \langle (1,0) \rangle$。则 $N \cong N' \cong \mathbb{Z}_2$。

又 $|G/N| = |G'/N'| = 2$，而 2 阶群都同构于 $\mathbb{Z}_2$，故 $G/N \cong G'/N' \cong \mathbb{Z}_2$。

但是 $G = \mathbb{Z}_4$ 中有 4 阶元素，而 $G' = \mathbb{Z}_2 \times \mathbb{Z}_2$ 中每个非单位元的阶都是 2，所以 $G \ncong G'$。

因此 (2) 错误。

(3) 取 $G = G' = \mathbb{Z}_4 \times \mathbb{Z}_2$，并令 $N = \langle (1,0) \rangle$，$N' = \langle (2,0), (0,1) \rangle$。

其中 $N \cong \mathbb{Z}_4$，而

$$N' = \{(0,0), (2,0), (0,1), (2,1)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2,$$

故 $N \ncong N'$。

但是 $|G| = 8$，且 $|N| = |N'| = 4$，所以 $|G/N| = |G'/N'| = 2$。因此 $G/N \cong G'/N' \cong \mathbb{Z}_2$。

于是 $G \cong G'$ 且 $G/N \cong G'/N'$，但 $N \ncong N'$，所以 (3) 错误。

□

2.8 同态基本定理

1. 设群 G 恰有两个自同构，证明 G 为交换群。

解 对任意 $g\in G$，定义内自同构 $\varphi_g: G\to G$ 为 $\varphi_g(x)=gxg^{-1}$。对任意 $g,h\in G$，有

$$\varphi_g=\varphi_h \iff gxg^{-1}=hxh^{-1}\quad(\forall x\in G)\iff h^{-1}g\in Z(G).$$

因此，$\varphi_g=\varphi_h$ 当且仅当 $gZ(G)=hZ(G)$，故 G 的内自同构个数等于 $[G:Z(G)]$。

由于 G 恰有两个自同构，而内自同构都是 G 的自同构，所以 $[G:Z(G)]\leqslant 2$。

若 $[G:Z(G)]=1$，则 $G=Z(G)$，从而 G 为交换群。

若 $[G:Z(G)]=2$，取 $a\notin Z(G)$，则 G 的两个关于 $Z(G)$ 的陪集为 $Z(G)$ 和 $aZ(G)$。任取 $x,y\in G$。若其中一个属于 $Z(G)$，则 $xy=yx$；若二者都不属于 $Z(G)$，则可写成 $x=az_1,\ y=az_2$，其中 $z_1,z_2\in Z(G)$，于是

$$xy=az_1az_2=a^2z_1z_2=a^2z_2z_1=az_2az_1=yx.$$

因此任意两个元素均可交换，即 $G=Z(G)$，这与 $[G:Z(G)]=2$ 矛盾。

故只能有 $[G:Z(G)]=1$，所以 G 为交换群。 □

2. 证明阶大于 2 的有限群至少有两个自同构。

解 恒等映射 id_G 总是 G 的一个自同构。下面证明还存在一个非恒等自同构。

若 G 不是交换群，则存在 $g\notin Z(G)$。定义 $\varphi_g(x)=gxg^{-1}$，则 φ_g 是内自同构。若 $\varphi_g=\mathrm{id}_G$，则对任意 $x\in G$ 都有 $gxg^{-1}=x$，即 $gx=xg$，从而 $g\in Z(G)$，矛盾。因此 φ_g 是非恒等自同构。

下面设 G 为交换群。此时映射 $\iota: G\to G$，$\iota(x)=x^{-1}$ 是自同构，因为

$$\iota(xy)=(xy)^{-1}=y^{-1}x^{-1}=x^{-1}y^{-1}=\iota(x)\iota(y),$$

且 $\iota^2=\mathrm{id}_G$。若存在 $x\in G$ 使 $x^{-1}\neq x$，则 ι 是所需的非恒等自同构。

最后只需考虑对任意 $x\in G$ 都有 $x^{-1}=x$ 的情形，此时每个元素都满足 $x^2=e$。取 G 的一个极小生成集 $\{a_1,\dots,a_r\}$。由于每个生成元的阶都为 2，每个元素均可写成 $a_1^{\varepsilon_1}\cdots a_r^{\varepsilon_r}$，其中 $\varepsilon_i\in\{0,1\}$。这种表示是唯一的：否则两种不同表示相乘后将得到一个非空的生成元乘积等于 e，从而其中某个生成元可由其余生成元表示，与生成集的极小性矛盾。

若 $r=1$，则 $G=\{e,a_1\}$，与 $|G|>2$ 矛盾，故 $r\geqslant 2$。定义映射 $\alpha: G\to G$，交换 a_1,a_2，并固定其余生成元，即

$$\alpha\left(a_1^{\varepsilon_1}a_2^{\varepsilon_2}a_3^{\varepsilon_3}\cdots a_r^{\varepsilon_r}\right)=a_1^{\varepsilon_2}a_2^{\varepsilon_1}a_3^{\varepsilon_3}\cdots a_r^{\varepsilon_r}.$$

由表示的唯一性，α 定义良好；又因 G 为交换群且各元素的指数均按模 2 相加，所以 α 是同态。并且 $\alpha^2=\mathrm{id}_G$，故 α 为自同构。由于 $\alpha(a_1)=a_2\neq a_1$，它不是恒等自同构。

综上，阶大于 2 的有限群至少有两个自同构。 □

3. 设 G 为群，H,K 都是 G 的正规子群且 $H\cap K=\{e\}$，证明 H 与 K 之间元素的乘法可交换。

解 任取 $h\in H,\ k\in K$，考虑元素 $hkh^{-1}k^{-1}$。

由于 $K\trianglelefteq G$，有 $hkh^{-1}\in K$；又 $k^{-1}\in K$，故 $hkh^{-1}k^{-1}\in K$。

另一方面，由于 $H\trianglelefteq G$，有 $kh^{-1}k^{-1}\in H$；又 $h\in H$，故 $hkh^{-1}k^{-1}=h(kh^{-1}k^{-1})\in H$。

因此 $hkh^{-1}k^{-1}\in H\cap K=\{e\}$，从而 $hkh^{-1}k^{-1}=e$。于是 $hk=kh$。

由于 $h\in H$ 和 $k\in K$ 是任意的，故 H 中任一元素都与 K 中任一元素可交换。 □

4. 设 G 为有限群，$H \leqslant G$ 且 $[G:H]=n>1$，证明 G 必有一个指数整除 $n!$ 的非平凡正规子群，或者 G 同构于 S_n 的一个子群。

解 令 $X=\{gH \mid g\in G\}$ 为 H 的所有左陪集组成的集合，则 $|X|=[G:H]=n$。群 G 按左乘作用在 X 上，即 $g\cdot(xH)=(gx)H$。由此得到同态

$$\varphi: G \longrightarrow S_X \cong S_n, \qquad \varphi(g)(xH)=gxH.$$

令 $N=\ker\varphi$，则 $N\trianglelefteq G$。若 $g\in N$，则 g 固定每一个左陪集，特别地，$gH=H$，故 $g\in H$。因此 $N\leqslant H$。又因 $[G:H]=n>1$，所以 $H<G$，从而 $N<G$。

在 N 的左陪集与 $\varphi(G)$ 的元素之间定义映射 $gN\mapsto\varphi(g)$。因为

$$\varphi(g)=\varphi(h)\Longleftrightarrow\varphi(h^{-1}g)=\mathrm{id}_X\Longleftrightarrow h^{-1}g\in N\Longleftrightarrow gN=hN,$$

所以该映射为双射，故 $[G:N]=|\varphi(G)|$。由于 $\varphi(G)\leqslant S_n$，由 Lagrange 定理有 $|\varphi(G)|\mid n!$，因而 $[G:N]\mid n!$。

若 $N\neq\{e\}$，则 N 是指数整除 $n!$ 的非平凡正规子群；若 $N=\{e\}$，则 φ 为单射，故 $G\cong\varphi(G)\leqslant S_n$。结论得证。 □

5. 证明下列对应定理：设 G 是群，$N\trianglelefteq G$。记 $\mathcal{M}$ 为 G 中包含 N 的所有子群的集合，$\overline{\mathcal{M}}$ 为 $\overline{G}=G/N$ 的所有子群的集合，即

$$\mathcal{M}=\{M\mid N\leqslant M\leqslant G\}, \qquad \overline{\mathcal{M}}=\{\overline{M}\mid \overline{M}\leqslant\overline{G}=G/N\}.$$

则映射

$$\pi:\mathcal{M}\longrightarrow\overline{\mathcal{M}}, \qquad M\longmapsto\overline{M}=M/N$$

为双射，且对于任意 $M_1,M_2,M\in\mathcal{M}$，有：

(1) $M_1\leqslant M_2$ 当且仅当 $\overline{M_1}\leqslant\overline{M_2}$；

(2) 若 $M_1\leqslant M_2$，则 $[M_2:M_1]=[\overline{M_2}:\overline{M_1}]$；

(3) $\overline{\langle M_1,M_2\rangle}=\langle\overline{M_1},\overline{M_2}\rangle$；

(4) $\overline{M_1\cap M_2}=\overline{M_1}\cap\overline{M_2}$；

(5) $M\trianglelefteq G$ 当且仅当 $\overline{M}\trianglelefteq\overline{G}$，且此时 $G/M\cong\overline{G}/\overline{M}$。

解 记自然映射 $q:G\to\overline{G}$ 为 $q(g)=gN$，并记 $\overline{g}=gN$。

首先证明 π 是双射。若 $M\in\mathcal{M}$，则 $N\leqslant M$，且由 $N\trianglelefteq G$ 可知 $N\trianglelefteq M$，所以 M/N 是 G/N 的子群，故 π 定义良好。

反之，对任意 $\overline{L}\leqslant\overline{G}$，令

$$\lambda(\overline{L})=q^{-1}(\overline{L})=\{g\in G\mid\overline{g}\in\overline{L}\}.$$

若 $x,y\in\lambda(\overline{L})$，则 $\overline{xy^{-1}}=\overline{x}\,\overline{y}^{-1}\in\overline{L}$，故 $xy^{-1}\in\lambda(\overline{L})$，所以 $\lambda(\overline{L})\leqslant G$。又对任意 $n\in N$，有 $\overline{n}=\overline{e}\in\overline{L}$，故 $N\leqslant\lambda(\overline{L})$，从而 $\lambda(\overline{L})\in\mathcal{M}$。

对任意 $M\in\mathcal{M}$，有 $M\leqslant q^{-1}(M/N)$。若 $g\in q^{-1}(M/N)$，则存在 $m\in M$ 使 $\overline{g}=\overline{m}$，于是 $m^{-1}g\in N\leqslant M$，故 $g\in M$。因此 $\lambda(\pi(M))=q^{-1}(M/N)=M$。另一方面，由 q 的满射性，有 $\pi(\lambda(\overline{L}))=q(q^{-1}(\overline{L}))=\overline{L}$。所以 π 与 λ 互为逆映射，π 为双射。

下面证明各项性质。

(1) 若 $M_1\leqslant M_2$，则每个 $mN\in M_1/N$ 都属于 M_2/N，故 $\overline{M_1}\leqslant\overline{M_2}$。

反之，若 $\overline{M_1} \leqslant \overline{M_2}$，任取 $x \in M_1$，则 $\overline{x} \in \overline{M_2}$，故存在 $y \in M_2$ 使 $\overline{x} = \overline{y}$。于是 $y^{-1}x \in N \leqslant M_2$，从而 $x \in M_2$。因此 $M_1 \leqslant M_2$。

(2) 设 $M_1 \leqslant M_2$。在 M_2 关于 M_1 的左陪集与 $\overline{M_2}$ 关于 $\overline{M_1}$ 的左陪集之间定义

$$xM_1 \longmapsto \overline{x}\,\overline{M_1}.$$

由于 $N \leqslant M_1$，对任意 $x, y \in M_2$，有

$$xM_1 = yM_1 \Longleftrightarrow y^{-1}x \in M_1 \Longleftrightarrow \overline{y}^{-1}\overline{x} \in \overline{M_1} \Longleftrightarrow \overline{x}\,\overline{M_1} = \overline{y}\,\overline{M_1}.$$

因此上述对应定义良好且为双射，故 $[M_2 : M_1] = [\overline{M_2} : \overline{M_1}]$。

(3) 因为 $M_i \leqslant \langle M_1, M_2\rangle$，由 (1) 有 $\overline{M_i} \leqslant \overline{\langle M_1, M_2\rangle}$，其中 $i = 1, 2$。故

$$\langle \overline{M_1}, \overline{M_2}\rangle \leqslant \overline{\langle M_1, M_2\rangle}.$$

反之，$\langle M_1, M_2\rangle$ 中的任一元素均可写成 $x_1x_2\cdots x_r$，其中每个 x_i 属于 M_1 或 M_2。于是 $\overline{x_1x_2\cdots x_r} = \overline{x_1}\,\overline{x_2}\cdots\overline{x_r} \in \langle \overline{M_1}, \overline{M_2}\rangle$，故反向包含也成立。因此

$$\overline{\langle M_1, M_2\rangle} = \langle \overline{M_1}, \overline{M_2}\rangle.$$

(4) 由 $M_1 \cap M_2 \leqslant M_i$，有 $\overline{M_1 \cap M_2} \leqslant \overline{M_1} \cap \overline{M_2}$。

反之，若 $\overline{x} \in \overline{M_1} \cap \overline{M_2}$，则存在 $a \in M_1$、$b \in M_2$，使 $\overline{x} = \overline{a} = \overline{b}$。于是 $a^{-1}x, b^{-1}x \in N$。由于 $N \leqslant M_1 \cap M_2$，可得 $x \in M_1$ 且 $x \in M_2$，故 $x \in M_1 \cap M_2$。因此 $\overline{x} \in \overline{M_1 \cap M_2}$，从而

$$\overline{M_1 \cap M_2} = \overline{M_1} \cap \overline{M_2}.$$

(5) 若 $M \trianglelefteq G$，则对任意 $\overline{g} \in \overline{G}$ 和 $\overline{m} \in \overline{M}$，有 $\overline{g}\,\overline{m}\,\overline{g}^{-1} = \overline{gmg^{-1}} \in \overline{M}$，故 $\overline{M} \trianglelefteq \overline{G}$。

反之，若 $\overline{M} \trianglelefteq \overline{G}$，则对任意 $g \in G$、$m \in M$，有 $\overline{gmg^{-1}} \in \overline{M}$。故存在 $m' \in M$ 使 $\overline{gmg^{-1}} = \overline{m'}$，于是 $(m')^{-1}gmg^{-1} \in N \leqslant M$，从而 $gmg^{-1} \in M$。因此 $gMg^{-1} \leqslant M$；将 g 换为 g^{-1} 可得反向包含，故 $gMg^{-1} = M$，即 $M \trianglelefteq G$。

此时定义

$$\Phi : G/M \longrightarrow \overline{G}/\overline{M}, \qquad \Phi(gM) = \overline{g}\,\overline{M}.$$

由于

$$gM = hM \Longleftrightarrow h^{-1}g \in M \Longleftrightarrow \overline{h}^{-1}\overline{g} \in \overline{M} \Longleftrightarrow \overline{g}\,\overline{M} = \overline{h}\,\overline{M},$$

所以 Φ 定义良好且为单射。又每个 $\overline{g}\,\overline{M} \in \overline{G}/\overline{M}$ 都是 $\Phi(gM)$，故 Φ 为满射。并且

$$\Phi((gM)(hM)) = \Phi(ghM) = \overline{gh}\,\overline{M} = (\overline{g}\,\overline{M})(\overline{h}\,\overline{M}),$$

所以 Φ 是同构，故 $G/M \cong \overline{G}/\overline{M}$。

□

6. 设 $N \trianglelefteq G$，$|N| = n$，$[G : N] = m$，且 m 与 n 互素，证明 G 的阶为 n 的正规子群一定为 N。

解 设 $K \trianglelefteq G$ 且 $|K| = n$。由于 $K, N \trianglelefteq G$，故 $KN \leqslant G$。由子群乘积的阶数公式，

$$[KN : N] = \frac{|KN|}{|N|} = \frac{|K|}{|K \cap N|} = [K : K \cap N].$$

因此 $[KN:N] \mid |K| = n$。另一方面，由 $N \leqslant KN \leqslant G$，有

$$[G:N] = [G:KN][KN:N],$$

故 $[KN:N] \mid [G:N] = m$。

由于 m 与 n 互素，只能有 $[KN:N] = 1$，从而 $KN = N$，于是 $K \leqslant N$。又 $|K| = |N| = n$，故 $K = N$。

因此，G 的阶为 n 的正规子群一定为 N。 □

7. 设 σ 是群 G 到交换群 H 的一个群同态，$N \leqslant G$ 且 $\ker\sigma \subseteq N$，证明 $N \trianglelefteq G$。

解 任取 $g \in G$ 和 $a \in N$。由于 H 为交换群，有

$$\sigma(gag^{-1}a^{-1}) = \sigma(g)\sigma(a)\sigma(g)^{-1}\sigma(a)^{-1} = e_H.$$

故 $gag^{-1}a^{-1} \in \ker\sigma \subseteq N$。又 $a \in N$，所以 $gag^{-1} = (gag^{-1}a^{-1})a \in N$。因此 $gNg^{-1} \leqslant N$。

将 g 换为 g^{-1}，可得 $g^{-1}Ng \leqslant N$，两边同时被 g 共轭，得到 $N \leqslant gNg^{-1}$。所以 $gNg^{-1} = N$。

由于 $g \in G$ 任意，故 $N \trianglelefteq G$。 □

8. 设 G 为单群，且存在 G 到群 H 的满同态，证明 H 为单群或者 H 为单位元群。

解 设 $\sigma : G \to H$ 为满同态。由于 $\ker\sigma \trianglelefteq G$，而 G 为单群，故 $\ker\sigma = \{e_G\}$ 或 $\ker\sigma = G$。

若 $\ker\sigma = G$，则对任意 $g \in G$ 都有 $\sigma(g) = e_H$，故 $\sigma(G) = \{e_H\}$。又 σ 为满同态，所以 $H = \{e_H\}$，即 H 为单位元群。

若 $\ker\sigma = \{e_G\}$，则 σ 为单射；结合满射性，σ 是同构。任取 $L \trianglelefteq H$，则 $\sigma^{-1}(L) \trianglelefteq G$。由 G 为单群，$\sigma^{-1}(L) = \{e_G\}$ 或 $\sigma^{-1}(L) = G$。由于 σ 为满射，分别得到 $L = \{e_H\}$ 或 $L = H$。因此 H 没有非平凡真正规子群，即 H 为单群。

综上，H 为单群或者 H 为单位元群。 □

9. 证明有限 p-群的非正规子群的个数一定是 p 的倍数。

解 把 G 的非正规子群按照共轭关系分类，即称两个子群 H, K 属于同一类，如果存在 $g \in G$ 使得 $K = gHg^{-1}$。于是所有非正规子群被分成若干个互不相交的共轭类。

任取一个非正规子群 H。先计算与 H 共轭的子群个数。对任意 $g_1, g_2 \in G$，有

$$g_1Hg_1^{-1} = g_2Hg_2^{-1} \iff g_2^{-1}g_1H(g_2^{-1}g_1)^{-1} = H \iff g_2^{-1}g_1 \in N_G(H).$$

因此，不同的共轭子群与 $N_G(H)$ 在 G 中的不同陪集一一对应，所以与 H 共轭的子群共有 $[G:N_G(H)]$ 个。

由于 H 不是正规子群，存在 $g \in G$ 使 $gHg^{-1} \neq H$，故 $N_G(H) \neq G$。设 $|G| = p^r$。由 Lagrange 定理，$|N_G(H)| = p^s$，其中 $s < r$，因而

$$[G:N_G(H)] = p^{r-s},$$

这是 p 的倍数。

所以，每一个非正规子群的共轭类所含子群的个数都是 p 的倍数。所有非正规子群的个数等于这些共轭类大小之和，因此也是 p 的倍数。 □

10. 设 G 为有限群，$\alpha \in \mathrm{Aut}(G)$，令 $I = \{g \in G \mid \alpha(g) = g^{-1}\}$，证明：

(1) 若 $|I| > \dfrac{3}{4}|G|$，则 G 交换；

(2) 若 $|I| = \dfrac{3}{4}|G|$，则 G 有一个指数为 2 的交换正规子群。

解 首先我们注意到，对任意 $x, y \in I$，有

$$xy \in I \iff \alpha(xy) = (xy)^{-1} \iff x^{-1}y^{-1} = y^{-1}x^{-1} \iff xy = yx.$$

也就是说，若 $x, y \in I$，则 $xy \in I$ 当且仅当 x 与 y 可交换。

固定 $x \in I$，令 $I_x = \{y \in I \mid xy \in I\}$。由上述事实，$I_x = I \cap C_G(x)$。

下面估计 $|I_x|$。若 $y \in I \setminus I_x$，则 $xy \notin I$。左乘映射 $y \mapsto xy$ 是单射，故它把 $I \setminus I_x$ 单射地映入 $G \setminus I$。因此

$$|I| - |I_x| = |I \setminus I_x| \leqslant |G \setminus I| = |G| - |I|,$$

从而

$$|I_x| \geqslant 2|I| - |G|.$$

(1) 设 $|I| > \dfrac{3}{4}|G|$。对任意 $x \in I$，有

$$|C_G(x)| \geqslant |I_x| \geqslant 2|I| - |G| > \frac{1}{2}|G|.$$

若 $C_G(x)$ 是 G 的真子群，则 $[G : C_G(x)] \geqslant 2$，从而 $|C_G(x)| \leqslant \dfrac{1}{2}|G|$，矛盾。因此 $C_G(x) = G$，即 $x \in Z(G)$。

由于 $x \in I$ 任意，故 $I \subseteq Z(G)$。于是 $|Z(G)| \geqslant |I| > \dfrac{1}{2}|G|$。同理，$Z(G)$ 不可能是 G 的真子群，因此 $Z(G) = G$，所以 G 为交换群。

(2) 设 $|I| = \dfrac{3}{4}|G|$。先证明 I 中存在非中心元素。

反设 $I \subseteq Z(G)$。此时任取 $x, y \in I$，都有 $xy = yx$，由开头的关键事实可得 $xy \in I$。又 $e \in I$，且若 $x \in I$，则

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

故 $x^{-1} \in I$。因此 $I \leqslant G$。

但此时 $[G : I] = |G|/|I| = 4/3$，不是整数，与 Lagrange 定理矛盾。因此可以取 $x \in I \setminus Z(G)$。

令 $H = C_G(x)$。由于 $x \notin Z(G)$，故 $H < G$，于是 $|H| \leqslant \dfrac{1}{2}|G|$。另一方面，

$$|I_x| \geqslant 2|I| - |G| = 2 \cdot \frac{3}{4}|G| - |G| = \frac{1}{2}|G|.$$

又 $I_x = I \cap H \subseteq H$，所以

$$\frac{1}{2}|G| \leqslant |I_x| \leqslant |H| \leqslant \frac{1}{2}|G|.$$

因此以上各处均取等号，即 $|H| = \dfrac{1}{2}|G|$ 且 $I_x = H$。于是 $H \subseteq I$，并且 $[G : H] = 2$。由指数为 2 的子群必为正规子群，得 $H \trianglelefteq G$。

最后证明 H 为交换群。任取 $a, b \in H$。由于 H 是子群，有 $ab \in H$；又 $H \subseteq I$，故 $a, b, ab \in I$。由开头的关键事实，$ab \in I$ 蕴含 $ab = ba$。因此 H 为交换群。

所以 H 是 G 的一个指数为 2 的交换正规子群。

□

2.9 自由群

1. 证明四元数群 Q 的每个子群都是正规子群，但 Q 不是交换群。（这样的群称为 Hamilton（哈密顿）群。）

解 写成 $Q=\{\pm1,\pm i,\pm j,\pm k\}$，其中 $i^2=j^2=k^2=-1$，$ij=k$，$ji=-k$。

Q 的全部子群为

$$\{1\},\quad \{1,-1\},\quad \langle i\rangle=\{\pm1,\pm i\},\quad \langle j\rangle=\{\pm1,\pm j\},\quad \langle k\rangle=\{\pm1,\pm k\},\quad Q.$$

事实上，-1 是 Q 中唯一的 2 阶元素；若一个真子群含有 i,j,k 中两类不同的元素，则它也含有这两个元素的乘积，从而包含 Q 的全部元素，矛盾。因此上述子群已经包含了 Q 的所有子群。

其中 $\{1\}$ 和 Q 显然正规，$\{1,-1\}\leqslant Z(Q)$，故也是正规子群；其余三个 4 阶子群在 Q 中的指数均为 2，所以都是正规子群。因此 Q 的每个子群都是正规子群。

但 $ij=k$，而 $ji=-k$，故 $ij\neq ji$，所以 Q 不是交换群。 □

2. 求群 $G=\langle a,b\mid a^3=b^9=e,\ a^{-1}ba=b^{-1}\rangle$ 的阶，并确定群 G。

解 由 $a^{-1}ba=b^{-1}$，有

$$a^{-2}ba^2=a^{-1}b^{-1}a=(a^{-1}ba)^{-1}=b.$$

继续共轭一次，得到 $a^{-3}ba^3=a^{-1}ba=b^{-1}$。另一方面，由 $a^3=e$，有 $a^{-3}ba^3=b$，故 $b=b^{-1}$，即 $b^2=e$。

又 $b^9=e$，而 $b^2=e$ 蕴含 $b^9=b$，所以 $b=e$。因此 $G=\langle a\rangle$，且 $a^3=e$，从而 $|G|\leqslant 3$。

设 $\bar a$ 是 $\mathbb{Z}_3$ 的生成元。令 $a\mapsto\bar a$，$b\mapsto e$，则这些元素满足题中全部定义关系，因而得到满同态 $G\to\mathbb{Z}_3$。所以 $|G|\geqslant 3$。

综上，$|G|=3$，且 $G\cong\mathbb{Z}_3$。 □

3. 求群 $G=\langle a,b\mid ab^2=b^3a,\ ba^3=a^2b\rangle$ 的阶，并确定群 G。

解 令 $x=a^{-1}$。由题中两个关系分别得到

$$x^{-1}b^2x=b^3,\qquad b^{-1}x^2b=x^3.$$

由第二个关系，对任意整数 r，都有 $b^{-1}x^{2r}b=x^{3r}$。因此

$$b^{-1}x^8b=x^{12},\qquad b^{-2}x^8b^2=x^{18},\qquad b^{-3}x^8b^3=x^{27}.$$

由第一个关系可得 $xb^3=b^2x$，取逆后得到 $b^{-3}x^{-1}=x^{-1}b^{-2}$。于是

$$\begin{aligned}x^{27}&=b^{-3}x^8b^3\\&=(b^{-3}x^{-1})x^8(xb^3)\\&=x^{-1}b^{-2}x^8b^2x\\&=x^{-1}x^{18}x=x^{18}.\end{aligned}$$

故 $x^9=e$。

再由 $b^{-1}x^2b=x^3$，有

$$b^{-2}x^4b^2=b^{-1}x^6b=x^9=e,$$

所以 $x^4=e$。由于 $\gcd(4,9)=1$，元素 x 的阶同时整除 4 和 9，故 $x=e$。于是 $a=x^{-1}=e$。

将 $a=e$ 代入 $ab^2=b^3a$，得到 $b^2=b^3$，故 $b=e$。因此 $G=\{e\}$，即 $|G|=1$。 □

4. 求群 $G=\langle a,b\mid a^6=e,\ a^3=b^2,\ b^{-1}ab=a^{-1}\rangle$ 的阶。

解 由 $b^{-1}ab=a^{-1}$ 也有 $ba=a^{-1}b$。因此可将任意字中的 b 移到所有 a 的右边；再利用 $b^2=a^3$ 和 $a^6=e$，可知 G 的每个元素均可写成 a^r 或 a^rb，其中 $0\leqslant r\leqslant 5$。故 $|G|\leqslant 12$。

下面证明这 12 个形式确实不会因定义关系而进一步合并。在 S_7 中取

$$A=(123)(45)(67),\qquad B=(23)(4657).$$

直接计算可得

$$A^6=e,\qquad A^3=(45)(67)=B^2,\qquad B^{-1}AB=A^{-1}.$$

因此赋值 $a\mapsto A$、$b\mapsto B$ 诱导满同态 $G\to\langle A,B\rangle$。

元素 A 的阶为 6，且 $B\notin\langle A\rangle$，因为 B 在 $\{1,2,3\}$ 上的限制为对换，而 A 的任意幂在该集合上的限制只能是单位元或 3-轮换。因此 $\langle A\rangle$ 与 $\langle A\rangle B$ 不相交，故 $\langle A,B\rangle$ 至少含有 A^r,A^rB 这 12 个不同元素。

于是 $|G|\geqslant 12$。结合 $|G|\leqslant 12$，得到 $|G|=12$。 □

5. 设

$$G=\langle a,b,c\mid a^2=b^2=c^2=e,\ ac=ca,\ (ab)^3=(bc)^3=e\rangle,$$

证明 $G\cong S_4$。

解 由 $a^2=b^2=c^2=e$ 以及 $(ab)^3=(bc)^3=e$，可得

$$aba=bab,\qquad bcb=cbc.$$

令 $H=\langle a,b\rangle$，并记 $d=ab$。因为 $d^3=e$、$a^2=e$ 且 $ada=d^{-1}$，所以 H 的每个元素都可写成 d^i 或 d^ia，其中 $0\leqslant i\leqslant 2$。故 $|H|\leqslant 6$。

令 $R=\{e,c,cb,cba\}$，并令 $X=H\cup Hc\cup Hcb\cup Hcba$。利用 $ac=ca$、$aba=bab$ 和 $bcb=cbc$，可得下表：

u	ua	ub	uc
e	a	b	c
c	ac	cb	e
cb	cba	c	$b(cb)$
cba	cb	$a(cba)$	$b(cba)$

例如，$cba\cdot b=cbab=caba=a(cba)$，且 $cba\cdot c=cbac=cbca=bcba=b(cba)$。

表中每个元素都属于 X，所以 X 在右乘 a,b,c 下保持不变。又 $e\in X$，而 G 由 a,b,c 生成，故 $G=X$。因此

$$|G|\leqslant 4|H|\leqslant 24.$$

现定义

$$\varphi:G\longrightarrow S_4,\qquad \varphi(a)=(12),\quad \varphi(b)=(23),\quad \varphi(c)=(34).$$

这三个置换均为对换，(12) 与 (34) 可交换，而 $(12)(23)$ 和 $(23)(34)$ 均为 3 阶元素，所以它们满足 G 的全部定义关系。因此 φ 是定义良好的群同态。

又因为相邻对换 $(12),(23),(34)$ 生成 S_4，故 φ 为满同态，从而 $|G|\geqslant|S_4|=24$。结合前面的 $|G|\leqslant 24$，有 $|G|=24$。于是 φ 是双射，故 $G\cong S_4$。 □

6. 证明 $S_4 = \langle a, b \mid a^2 = b^3 = (ab)^4 = e \rangle$。

解 令

$$\Gamma = \langle a, b \mid a^2 = b^3 = (ab)^4 = e \rangle.$$

先证明 $|\Gamma| \leqslant 24$。令 $c = ab$，则 $c^4 = e$，并且 $b = ac$，故 $\Gamma = \langle a, c \rangle$，且 $a^2 = c^4 = (ac)^3 = e$。

令 $x = c^2$，$y = ac^2a$。显然 $x^2 = y^2 = e$。由 $(ac)^3 = e$，有 $(ac)^2 = (ac)^{-1} = c^{-1}a$，从而 $aca = c^{-1}ac^{-1}$。因此

$$y = ac^2a = (aca)^2 = c^{-1}ac^{-2}ac^{-1}.$$

于是利用 $c^{-2} = c^2$，得到

$$xy = c^2y = cac^{-2}ac^{-1} = cac^2ac^{-1} = cyc^{-1}.$$

所以 xy 与 y 共轭，故 $(xy)^2 = e$。又 x, y 均为 2 阶元素，因而 $xy = (xy)^{-1} = yx$。

于是 $V = \{e, x, y, xy\}$ 是 Γ 的一个子群，且 $|V| \leqslant 4$。又

$$axa = y, \qquad aya = x, \qquad a(xy)a = xy,$$

以及

$$cxc^{-1} = x, \qquad cyc^{-1} = xy, \qquad c(xy)c^{-1} = y.$$

故 V 在 a, c 的共轭下均保持不变。由于 $\Gamma = \langle a, c \rangle$，所以 $V \trianglelefteq \Gamma$。

在商群 Γ/V 中，记 $aV = \bar{a}$、$cV = \bar{c}$，则 $\bar{a}^2 = \bar{c}^2 = V$，且 $(\bar{a}\,\bar{c})^3 = V$。令 $d = \bar{a}\,\bar{c}$，则 $\bar{a} = d\bar{c}$，并且 $\bar{c}d\bar{c} = d^{-1}$。因此 Γ/V 的每个元素均可写成 d^i 或 $d^i\bar{c}$，其中 $0 \leqslant i \leqslant 2$。故 $[\Gamma : V] \leqslant 6$，从而

$$|\Gamma| = |V|[\Gamma : V] \leqslant 4 \cdot 6 = 24.$$

现在取 S_4 中的置换 $A = (12)$、$B = (234)$。则 $A^2 = B^3 = e$，且 $AB = (1234)$，故 $(AB)^4 = e$。又

$$BAB^{-1} = (13), \qquad B^2AB^{-2} = (14),$$

所以 $\langle A, B \rangle$ 包含 $(12), (13), (14)$，从而 $\langle A, B \rangle = S_4$。

因此赋值 $a \mapsto A$、$b \mapsto B$ 诱导满同态 $\Gamma \to S_4$，故 $|\Gamma| \geqslant 24$。结合前面所得 $|\Gamma| \leqslant 24$，可知该满同态为同构。因此

$$S_4 \cong \langle a, b \mid a^2 = b^3 = (ab)^4 = e \rangle.$$

□

7. 证明 $A_4 = \langle a, b \mid a^2 = b^3 = (ab)^3 = e \rangle$。

解 令

$$\Gamma = \langle a, b \mid a^2 = b^3 = (ab)^3 = e \rangle.$$

先证明 $|\Gamma| \leqslant 12$。由 $(ab)^3 = e$，有 $(ab)^2 = (ab)^{-1} = b^{-1}a$，故 $abab = b^{-1}a$，从而

$$aba = b^{-1}ab^{-1}.$$

令 $x = a$，$y = bab^{-1}$。则 $x^2 = y^2 = e$，并且

$$xy = abab^{-1} = b^{-1}ab^{-2} = b^2ab^{-2}.$$

因此 xy 是 a 的共轭元，也满足 $(xy)^2 = e$。于是 $xy = (xy)^{-1} = yx$，所以 $V = \{e, x, y, xy\}$ 是一个阶至多为 4 的子群。

共轭变换 $v \mapsto bvb^{-1}$ 依次将

$$x \longmapsto y, \qquad y \longmapsto xy, \qquad xy \longmapsto x.$$

故 $bVb^{-1} = V$。又 $a = x \in V$，所以 $aVa^{-1} = V$。由于 $\Gamma = \langle a, b\rangle$，可知 $V \trianglelefteq \Gamma$。

在 Γ/V 中，$aV = V$，故 Γ/V 由 bV 生成；又 $(bV)^3 = V$，所以 $[\Gamma : V] \leqslant 3$。因此

$$|\Gamma| = |V|[\Gamma : V] \leqslant 4 \cdot 3 = 12.$$

现在取 A_4 中的置换 $A = (12)(34)$、$B = (123)$。则 $A^2 = B^3 = e$，且 $AB = (243)$，故 $(AB)^3 = e$。

又

$$BAB^{-1} = (14)(23), \qquad B^2AB^{-2} = (13)(24),$$

所以 $\langle A, B\rangle$ 包含 Klein 四元群

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

由于 B 的阶为 3，且 $\langle B\rangle \cap V_4 = \{e\}$，故 V_4, V_4B, V_4B^2 是三个互不相同的陪集。因此 $\langle A, B\rangle$ 至少有 12 个元素。又 $\langle A, B\rangle \leqslant A_4$ 且 $|A_4| = 12$，故 $\langle A, B\rangle = A_4$。

因此赋值 $a \mapsto A$、$b \mapsto B$ 诱导满同态 $\Gamma \to A_4$。结合 $|\Gamma| \leqslant 12 = |A_4|$，可知该满同态为同构。因此

$$A_4 \cong \langle a, b \mid a^2 = b^3 = (ab)^3 = e\rangle.$$

□

8. 证明四元数群

$$Q = \langle a, b \mid a^4 = b^4 = e,\ a^2 = b^2,\ b^{-1}ab = a^{-1}\rangle.$$

解 令

$$\Gamma = \langle a, b \mid a^4 = b^4 = e,\ a^2 = b^2,\ b^{-1}ab = a^{-1}\rangle.$$

先证明 $|\Gamma| \leqslant 8$。由 $b^{-1}ab = a^{-1}$，可得 $a = ba^{-1}b^{-1}$；两边取逆，得到 $bab^{-1} = a^{-1}$，即

$$ba = a^{-1}b.$$

因此可以不断把字中的 b 移到所有 a 的右边，所以 Γ 的每个元素均可写成 a^rb^s 的形式。

再由 $b^2 = a^2$，可以将 b 的指数化为 0 或 1；由 $a^4 = e$，可以将 a 的指数化为 $0, 1, 2, 3$。因此每个元素均可写成

$$a^r \quad 或 \quad a^rb, \qquad 0 \leqslant r \leqslant 3,$$

故 $|\Gamma| \leqslant 8$。

写四元数群为 $Q = \{\pm 1, \pm i, \pm j, \pm k\}$。取 $A = i$、$B = j$，则 $A^4 = B^4 = 1$，$A^2 = B^2 = -1$，并且

$$B^{-1}AB = j^{-1}ij = -i = i^{-1}.$$

因此赋值 $a \mapsto i$、$b \mapsto j$ 诱导同态 $\Gamma \to Q$。由于 i, j 生成整个四元数群，该同态为满同态，所以 $|\Gamma| \geqslant |Q| = 8$。

结合 $|\Gamma| \leqslant 8$，可知该满同态为同构。因此

$$Q \cong \langle a, b \mid a^4 = b^4 = e,\ a^2 = b^2,\ b^{-1}ab = a^{-1}\rangle.$$

□

9. 证明

$$\langle a, b \mid abab^{-1} = e\rangle \cong \langle u, v \mid u^2v^2 = e\rangle.$$

解 记

$$G = \langle a, b \mid abab^{-1} = e \rangle, \qquad H = \langle u, v \mid u^2v^2 = e \rangle.$$

定义 $\varphi : G \to H$，使得 $\varphi(a) = uv$、$\varphi(b) = v^{-1}$。由于

$$\varphi(abab^{-1}) = (uv)v^{-1}(uv)v = u^2v^2 = e,$$

故 φ 是定义良好的群同态。

反过来，定义 $\psi : H \to G$，使得 $\psi(u) = ab$、$\psi(v) = b^{-1}$。由于

$$\psi(u^2v^2) = (ab)^2b^{-2} = abab^{-1} = e,$$

故 ψ 也是定义良好的群同态。

在生成元上有

$$\psi\varphi(a) = \psi(uv) = abb^{-1} = a, \qquad \psi\varphi(b) = \psi(v^{-1}) = b,$$

以及

$$\varphi\psi(u) = \varphi(ab) = uvv^{-1} = u, \qquad \varphi\psi(v) = \varphi(b^{-1}) = v.$$

因此 $\psi\varphi = \mathrm{id}_G$ 且 $\varphi\psi = \mathrm{id}_H$，所以 φ 与 ψ 互为逆同构。故

$$\langle a, b \mid abab^{-1} = e \rangle \cong \langle u, v \mid u^2v^2 = e \rangle.$$

□

10. 设 F 为自由群，G, H 是群，$\sigma : F \to G$ 是同态，$\tau : H \to G$ 是满同态，证明存在同态 $\rho : F \to H$，使得 $\sigma = \tau\rho$。（本习题的结论常被称为自由群的投射性。）

解 设 X 是自由群 F 的一组自由生成元。由于 $\tau : H \to G$ 为满同态，对每个 $x \in X$，都可以选取 $h_x \in H$，使得

$$\tau(h_x) = \sigma(x).$$

定义映射 $f : X \to H$ 为 $f(x) = h_x$。由自由群的定义，f 唯一地延拓为群同态 $\rho : F \to H$，且对任意 $x \in X$ 都有 $\rho(x) = h_x$。

于是对每个自由生成元 $x \in X$，有

$$(\tau\rho)(x) = \tau(\rho(x)) = \tau(h_x) = \sigma(x).$$

同态 $\tau\rho$ 与 σ 在自由生成集 X 上取值相同，因此它们在整个 F 上相同。故

$$\sigma = \tau\rho.$$

□

3 群的结构

3.1 群的直积

1. 设群 $B \cong C$，证明对任意群 A，有 $A \times B \cong A \times C$。反之是否成立？

解 设 $\varphi : B \to C$ 为同构。定义 $F : A \times B \to A \times C$ 为 $F(a,b) = (a, \varphi(b))$。由直积的运算定义，

$$\begin{aligned} F\big((a_1,b_1)(a_2,b_2)\big) &= (a_1a_2, \varphi(b_1b_2)) \\ &= (a_1a_2, \varphi(b_1)\varphi(b_2)) = F(a_1,b_1)F(a_2,b_2). \end{aligned}$$

所以 F 是同态。又其逆映射为 $(a,c) \mapsto (a, \varphi^{-1}(c))$，故 F 为同构，即 $A \times B \cong A \times C$。

但是，对于固定的群 A，由 $A \times B \cong A \times C$ 不一定能推出 $B \cong C$。例如，取

$$A = \{(x_1, x_2, \ldots) \mid x_i \in \mathbb{Z}_2\},$$

运算为各分量分别模 2 相加，并取 $B = \{0\}$、$C = \mathbb{Z}_2$。

定义映射

$$\Psi : A \times C \longrightarrow A, \qquad \Psi\big((x_1, x_2, \ldots), c\big) = (c, x_1, x_2, \ldots).$$

由于两边的运算都是按分量相加，Ψ 保持运算；又其逆映射为 $(y_1, y_2, \ldots) \mapsto ((y_2, y_3, \ldots), y_1)$，故 Ψ 是同构。因此 $A \times B \cong A \cong A \times C$，但 B 为单位元群，C 为 2 阶群，所以 $B \ncong C$。

注意，若要求对每一个群 A 都有 $A \times B \cong A \times C$，则取 A 为单位元群便得到 $B \cong C$；上述反例说明的是不能从某一个这样的同构中消去因子 A。 □

2. 设 G_1 和 G_2 都是非单位循环群，证明：若 G_1 和 G_2 中至少有一个为无限循环群，则 $G_1 \times G_2$ 不是循环群。

解 不妨设 G_1 为无限循环群，分别记 G_1, G_2 的单位元为 e_1, e_2。反设 $G_1 \times G_2 = \langle (x,y) \rangle$。

由于直积中的每个元素都是 (x,y) 的某个整数次幂，分别考察两个分量可得 $G_1 = \langle x \rangle$、$G_2 = \langle y \rangle$。因此 x 的阶为无穷，且由 G_2 非平凡可知 $y \neq e_2$。

另一方面，$(e_1, y) \in G_1 \times G_2$，故存在整数 k，使得

$$(e_1, y) = (x,y)^k = (x^k, y^k).$$

比较第一分量，得 $x^k = e_1$。由于 x 的阶为无穷，只能有 $k = 0$；再比较第二分量，得 $y = y^0 = e_2$，矛盾。

因此 $G_1 \times G_2$ 不是循环群。 □

3. 若定理 3.1.2 中有限群 G_1 和 G_2 的阶不互素，结论如何？

定理 3.1.2： 设有限群 G_1 和 G_2 的阶互素，则 $G_1 \times G_2$ 的子群一定形如 $H_1 \times H_2$，其中 $H_1 \leqslant G_1$、$H_2 \leqslant G_2$。

解 若两群的阶不互素，上述结论一般不成立。

取 $G_1 = G_2 = \mathbb{Z}_2$，其阶均为 2，并令 $K = \{(0,0), (1,1)\}$。由于 $(1,1) + (1,1) = (0,0)$，故 $K = \langle (1,1) \rangle$ 是 $G_1 \times G_2$ 的一个 2 阶子群。

假设存在 $H_1 \leqslant G_1$、$H_2 \leqslant G_2$，使得 $K = H_1 \times H_2$。由 $(1,1) \in K$，可得 $1 \in H_1$ 且 $1 \in H_2$，所以 $H_1 = H_2 = \mathbb{Z}_2$。于是 $K = \mathbb{Z}_2 \times \mathbb{Z}_2$ 应有 4 个元素，与 $|K| = 2$ 矛盾。

因此 K 不能写成上述形式，说明定理中的互素条件不能省去。

□

4. 设 G_1 和 G_2 为有限群，若 $G_1 \times G_2$ 为循环群，证明 G_1 和 G_2 都是循环群且阶互素。

解 设 $G_1 \times G_2 = \langle (a,b) \rangle$，分别记 G_1, G_2 的单位元为 e_1, e_2。

任取 $x \in G_1$，由于 $(x, e_2) \in G_1 \times G_2$，存在整数 r 使得 $(x, e_2) = (a,b)^r = (a^r, b^r)$，故 $x = a^r$。因此 $G_1 = \langle a \rangle$。同理，$G_2 = \langle b \rangle$，所以两个群都是循环群。

记 $m = |G_1| = o(a)$、$n = |G_2| = o(b)$。由于 $(a,b)^r = (e_1, e_2)$ 当且仅当 $m \mid r$ 且 $n \mid r$，故 $o((a,b)) = \operatorname{lcm}(m,n)$。另一方面，$(a,b)$ 生成整个直积，其阶为 $|G_1 \times G_2| = mn$。因此

$$mn = \operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)},$$

从而 $\gcd(m,n) = 1$，即 G_1 与 G_2 的阶互素。 □

5. 设 $N_1 \trianglelefteq G_1$、$N_2 \trianglelefteq G_2$，证明 $N_1 \times N_2 \trianglelefteq G_1 \times G_2$，且

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2).$$

解 记 $N = N_1 \times N_2$，有 $N \leqslant G_1 \times G_2$。任取 $g = (g_1, g_2) \in G_1 \times G_2$，由 N_1, N_2 的正规性，

$$gNg^{-1} = (g_1 N_1 g_1^{-1}) \times (g_2 N_2 g_2^{-1}) = N_1 \times N_2 = N.$$

故 $N_1 \times N_2 \trianglelefteq G_1 \times G_2$。

定义映射

$$\Phi : (G_1 \times G_2)/N \longrightarrow (G_1/N_1) \times (G_2/N_2), \qquad \Phi((g_1,g_2)N) = (g_1N_1, g_2N_2).$$

先检查其定义良好性与单射性。对任意 $(g_1,g_2), (h_1,h_2) \in G_1 \times G_2$，有

$$\begin{aligned}(g_1,g_2)N = (h_1,h_2)N &\iff (h_1^{-1}g_1, h_2^{-1}g_2) \in N_1 \times N_2 \\ &\iff g_1N_1 = h_1N_1 \text{ 且 } g_2N_2 = h_2N_2.\end{aligned}$$

因此，同一陪集得到相同的像，不同陪集得到不同的像，故 Φ 定义良好且为单射。又任意 (g_1N_1, g_2N_2) 都是 $\Phi((g_1,g_2)N)$，所以 Φ 为满射。

最后，设 $g = (g_1,g_2)$、$h = (h_1,h_2)$，则

$$\begin{aligned}\Phi((gN)(hN)) &= (g_1h_1N_1, g_2h_2N_2) \\ &= (g_1N_1, g_2N_2)(h_1N_1, h_2N_2) = \Phi(gN)\Phi(hN).\end{aligned}$$

故 Φ 为同态，从而为同构，即得所证结论。 □

6. 设 G 为一个群，且有 $A \trianglelefteq G$ 和 $B \trianglelefteq G$，证明

$$AB/(A \cap B) \cong (AB/A) \times (AB/B).$$

解 记 $P = AB$、$N = A \cap B$。由于 $A, B \trianglelefteq G$，有 $AB = BA$，故 $P \leqslant G$；并且 A, B, N 都是 P 的正规子群。

定义映射

$$\Phi : P/N \longrightarrow (P/A) \times (P/B), \qquad \Phi(xN) = (xA, xB).$$

对任意 $x, y \in P$，有

$$\begin{aligned}xN = yN &\iff y^{-1}x \in A \cap B \\ &\iff xA = yA \text{ 且 } xB = yB.\end{aligned}$$

因此 Φ 定义良好且为单射。又

$$\Phi((xN)(yN)) = (xyA, xyB) = (xA, xB)(yA, yB) = \Phi(xN)\Phi(yN),$$

故 Φ 是同态。

下面证明满射性。任取 $(xA, yB) \in (P/A)\times(P/B)$，由 $P = AB$，可写 $x = a_1b_1$、$y = a_2b_2$，其中 $a_1, a_2 \in A$、$b_1, b_2 \in B$。在 P/A 中 $a_1A = A$，故 $xA = b_1A$；在 P/B 中 $b_2B = B$，故 $yB = a_2B$。于是

$$\Phi((a_2b_1)N) = (b_1A, a_2B) = (xA, yB).$$

因此每一对陪集都有原像，Φ 为满射。

综上，Φ 为同构，故 $AB/(A\cap B) \cong (AB/A)\times(AB/B)$。 □

7. 设 H, K, L 都是 G 的正规子群，满足

$$G = HKL = \{abc \mid a \in H,\ b \in K,\ c \in L\}$$

和

$$H \cap (KL) = K \cap (HL) = L \cap (HK) = \{e\},$$

证明 $G \cong H \times K \times L$。

解 首先，由 $H \cap K \subseteq H \cap (KL) = \{e\}$，有 $H \cap K = \{e\}$。同理，$H \cap L = K \cap L = \{e\}$。

任取 $h \in H$、$k \in K$。由 H, K 的正规性，有 $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$，且 $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$。故 $hkh^{-1}k^{-1} \in H \cap K = \{e\}$，从而 $hk = kh$。同理，H 与 L、K 与 L 之间的元素也可交换。

定义映射

$$\Phi : H \times K \times L \longrightarrow G, \qquad \Phi(h, k, l) = hkl.$$

利用不同子群之间的元素可交换，得到

$$\begin{aligned}\Phi\big((h_1, k_1, l_1)(h_2, k_2, l_2)\big) &= h_1h_2k_1k_2l_1l_2 \\ &= (h_1k_1l_1)(h_2k_2l_2) \\ &= \Phi(h_1, k_1, l_1)\Phi(h_2, k_2, l_2).\end{aligned}$$

所以 Φ 是同态。由 $G = HKL$，每个 $g \in G$ 都可写成 hkl，故 Φ 为满射。

若 $\Phi(h, k, l) = e$，即 $hkl = e$，则 $h = (kl)^{-1} \in H \cap (KL) = \{e\}$，所以 $h = e$。于是 $kl = e$，从而 $k = l^{-1} \in K \cap L = \{e\}$，故 $k = l = e$。因此 $\ker\Phi = \{(e, e, e)\}$，Φ 为单射。

综上，Φ 为同构，故 $G \cong H \times K \times L$。 □

8. 设 H, K 是有限群 G 的正规子群，满足 $G = HK$ 且 H 与 K 的阶互素，证明 G 的任意子群 L 可以写成 $L = (H \cap L)(K \cap L)$。

解 记 $m = |H|$、$n = |K|$。由 Lagrange 定理，$|H \cap K|$ 同时整除 m, n，而 $\gcd(m, n) = 1$，故 $H \cap K = \{e\}$。

任取 $h \in H$、$k \in K$，由 H, K 的正规性，有 $hkh^{-1}k^{-1} \in H \cap K = \{e\}$，所以 $hk = kh$。

现任取 $x \in L$。由 $G = HK$，可写 $x = hk$，其中 $h \in H$、$k \in K$。下面证明 h, k 都属于 L。

由 $\gcd(m, n) = 1$，存在整数 r, s 使 $rm + sn = 1$。又由 Lagrange 定理，$h^m = k^n = e$。利用 h, k 可交换，得到

$$x^{sn} = (hk)^{sn} = h^{sn}k^{sn} = h^{1-rm} = h.$$

因为 $x \in L$ 且 L 是子群，所以 $h = x^{sn} \in L$；于是 $k = h^{-1}x \in L$。因此 $h \in H \cap L$、$k \in K \cap L$，从而 $x \in (H \cap L)(K \cap L)$。这就证明了 $L \subseteq (H \cap L)(K \cap L)$。

反之，$H\cap L$ 和 $K\cap L$ 都包含在子群 L 中，故其元素的乘积仍属于 L，即 $(H\cap L)(K\cap L)\subseteq L$。综上，$L=(H\cap L)(K\cap L)$。 □

9. 设群 G_1 和 G_2 都是非单位元群，证明：若 $G_1\times G_2$ 的每个子群一定为 $H_1\times H_2$，其中 $H_1\leqslant G_1$、$H_2\leqslant G_2$，则 G_1 和 G_2 中每个元素的阶都有限，并且对任意 $a\in G_1$ 和 $b\in G_2$，$o(a)$ 与 $o(b)$ 互素。

解 分别记 G_1,G_2 的单位元为 e_1,e_2。任取 $a\in G_1$、$b\in G_2$，考虑循环子群 $L=\langle(a,b)\rangle$。由假设，可写 $L=H_1\times H_2$。因为 $(a,b)\in L$，所以 $a\in H_1$、$b\in H_2$，从而 $(a,e_2)\in L$。

因此存在整数 t，使得

$$(a,e_2)=(a,b)^t=(a^t,b^t),\qquad \text{即}\qquad a^{t-1}=e_1,\quad b^t=e_2.$$

先证明所有元素的阶都有限。若 G_1 中存在无限阶元素 a，则取 $b\in G_2\setminus\{e_2\}$。由上述关系 $a^{t-1}=e_1$，只能有 $t=1$；但此时 $b=b^t=e_2$，矛盾。因此 G_1 中每个元素的阶都有限。交换两个群的地位，同理可知 G_2 中每个元素的阶也都有限。

再任取 $a\in G_1$、$b\in G_2$，记 $m=o(a)$、$n=o(b)$。由上述关系，存在整数 t 使 $m\mid(t-1)$ 且 $n\mid t$。令 $d=\gcd(m,n)$，则 d 同时整除 $t-1$ 和 t，因而 $d\mid t-(t-1)=1$。故 $d=1$，即 $o(a)$ 与 $o(b)$ 互素。 □

10. 设 n 为奇数，证明 $D_{2n}\cong D_n\times\mathbb{Z}_2$。

解 写

$$D_{2n}=\langle r,s\mid r^{2n}=s^2=e,\ srs^{-1}=r^{-1}\rangle,$$

其中 r 是 $2n$ 阶旋转，s 是反射。令 $H=\langle r^2,s\rangle$、$K=\langle r^n\rangle$。

由 $sr^2s^{-1}=r^{-2}$，可将 H 中的元素写成

$$H=\{r^{2i},r^{2i}s\mid 0\leqslant i<n\}.$$

这 $2n$ 个元素互不相同，故 $|H|=2n$。又 r^2 的阶为 n，且 $s^2=e$、$sr^2s^{-1}=(r^2)^{-1}$，所以将 D_n 的旋转、反射生成元分别映到 r^2,s，得到满同态 $D_n\to H$。两群的阶均为 $2n$，故此同态为同构，即 $H\cong D_n$。

另一方面，$K=\{e,r^n\}\cong\mathbb{Z}_2$。元素 r^n 与 r 可交换，并且 $sr^ns^{-1}=r^{-n}=r^n$，故 $K\leqslant Z(D_{2n})$。由于 H 中的旋转恰为 r 的偶数次幂，而 n 为奇数，所以 $r^n\notin H$，从而 $H\cap K=\{e\}$。

又因 n 为奇数，$(n+1)/2$ 是整数，且

$$r=(r^2)^{(n+1)/2}r^n\in HK.$$

同时 $s\in H\subseteq HK$。由于 $K\leqslant Z(D_{2n})$，HK 是子群；它包含生成元 r,s，故 $D_{2n}=HK$。

最后定义 $\Phi:H\times K\to D_{2n}$ 为 $\Phi(h,k)=hk$。因为 K 中的元素与 H 中的元素可交换，Φ 保持乘法，故为同态；由 $D_{2n}=HK$，它是满射。若 $\Phi(h,k)=e$，则 $h=k^{-1}\in H\cap K=\{e\}$，故 $h=k=e$，所以 Φ 也是单射。

因此 Φ 为同构，从而

$$D_{2n}\cong H\times K\cong D_n\times\mathbb{Z}_2.$$

□

11. 设 φ 是 K 在 H 上的一个同构作用，由 φ 构造的半直积为 $H\rtimes_\varphi K$。若 K （即 $\{e_H\}\times K$）是 $H\rtimes_\varphi K$ 的正规子群，证明 φ 一定是平凡的同构作用，且 $H\rtimes_\varphi K=H\times K$。

解 在外半直积中，将 K 认同为子群 $\{e_H\}\times K$。其乘法为

$$(h_1,k_1)(h_2,k_2)=\big(h_1\varphi(k_1)(h_2),\,k_1k_2\big).$$

任取 $h \in H$、$k \in K$。由于 $(h, e_K)^{-1} = (h^{-1}, e_K)$，所以

$$(h, e_K)(e_H, k)(h, e_K)^{-1} = \big(h\varphi(k)(h^{-1}),\, k\big).$$

由 $\{e_H\}\times K$ 的正规性，上式属于 $\{e_H\}\times K$，故其第一分量必须为 e_H，即 $h\varphi(k)(h^{-1}) = e_H$。于是 $\varphi(k)(h^{-1}) = h^{-1}$，两边取逆，得 $\varphi(k)(h) = h$。

因为 $h \in H$、$k \in K$ 任意，故每个 $\varphi(k)$ 都是 H 上的恒等自同构，即 φ 为平凡作用。此时半直积的乘法化为

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2),$$

恰为直积的乘法。因此 $H \rtimes_\varphi K = H \times K$。 □

12. 设 m, n 为正整数，A 为一个 m 阶循环群，B 为一个 n 阶循环群，则半直积 $A \rtimes B$ 在同构意义下有多少种可能？

解 若 $m = 1$ 或 $n = 1$，则半直积分别同构于 B 或 A，所以只有一种可能。以下设 $m, n > 1$，并记 $A = \langle a\rangle$、$B = \langle b\rangle$。

一个半直积 $A \rtimes B$ 由一个同构作用 $\varphi : B \to \mathrm{Aut}(A)$ 决定。由于 $B = \langle b\rangle$ 是循环群，φ 完全由 $\varphi(b)$ 决定。

又因为 $A = \langle a\rangle$ 是 m 阶循环群，A 的任意自同构都由生成元 a 的像唯一决定。若 $\varphi(b)(a) = a^r$，则 a^r 必须仍为 A 的生成元，所以 $\gcd(r, m) = 1$。因此可以把 $\mathrm{Aut}(A)$ 与单位群

$$U_m = (\mathbb{Z}/m\mathbb{Z})^\times$$

对应起来，其中整数 r 对应自同构 $a \mapsto a^r$。

由于 $b^n = e_B$，而 φ 是群同态，所以

$$\varphi(b)^n = \varphi(b^n) = \varphi(e_B) = \mathrm{id}_A\,.$$

另一方面，由 $\varphi(b)(a) = a^r$，逐次作用可得

$$\varphi(b)^2(a) = \varphi(b)(a^r) = \varphi(b)(a)^r = a^{r^2},$$

一般地有 $\varphi(b)^k(a) = a^{r^k}$。特别地，$\varphi(b)^n(a) = a^{r^n}$。

因此 $\varphi(b)^n = \mathrm{id}_A$ 等价于它固定生成元 a，即

$$a^{r^n} = a \iff a^{r^n - 1} = e \iff m \mid (r^n - 1) \iff r^n \equiv 1 \pmod m.$$

反过来，若 $\gcd(r, m) = 1$ 且 $r^n \equiv 1 \pmod m$，则令 $\varphi(b)(a) = a^r$，便可以定义一个同态 $\varphi : B \to \mathrm{Aut}(A)$。因此，所有可能的同构作用恰好与

$$X = \{r \in U_m \mid r^n = 1\}$$

中的元素对应。

对给定的 $r \in X$，相应的半直积可以写成

$$G_r = \langle a, b \mid a^m = b^n = e,\ bab^{-1} = a^r\rangle.$$

不过，不同的 r 不一定给出不同构的群。例如，若用 B 的另一个生成元 b^t 代替 b，其中 $\gcd(t, n) = 1$，则

$$b^t a b^{-t} = a^{r^t}.$$

所以参数 r 会变为 r^t，而所得半直积并没有改变同构类型。也就是说，r 与 r^t（$\gcd(t, n) = 1$）应视为同一种情况。

因此，若令 $U_n = (\mathbb{Z}/n\mathbb{Z})^\times$ 作用在 $X = \{r \in U_m \mid r^n = 1\}$ 上：

$$t \cdot r = r^t \qquad (t \in U_n,\ r \in X),$$

则半直积 $A \rtimes B$ 的同构类型与该作用的轨道一一对应。

进一步地，两个元素 $r, s \in X$ 属于同一轨道，当且仅当它们在 U_m 中生成同一个循环子群。因此，半直积的同构类型个数等于 U_m 中阶整除 n 的循环子群的个数，即

$$\boxed{\#\{C \leqslant U_m \mid C \text{ 为循环群且} |C| \mid n\}.}$$

下面将它写成具体的计数形式。对每个正整数 d，记

$$c_d(m) = |\{r \in U_m \mid o(r) = d\}|,$$

即 U_m 中阶恰为 d 的元素个数。

若一个循环子群 $C \leqslant U_m$ 的阶为 d，则 C 恰有 $\phi(d)$ 个生成元，即恰有 $\phi(d)$ 个阶为 d 的元素。反过来，每个阶为 d 的元素都唯一生成一个 d 阶循环子群。因此，U_m 中 d 阶循环子群的个数为

$$\frac{c_d(m)}{\phi(d)}.$$

而这里只允许循环子群的阶 d 整除 n，所以半直积 $A \rtimes B$ 在同构意义下的可能数目为

$$\boxed{\sum_{d \mid n} \frac{c_d(m)}{\phi(d)}.}$$

例如，当 $m = 7, n = 3$ 时，U_7 中满足 $r^3 = 1$ 的元素为 $1, 2, 4$。其中 1 生成单位子群，而 $\langle 2 \rangle = \langle 4 \rangle = \{1, 2, 4\}$，所以共有两个满足条件的循环子群。因此此时半直积在同构意义下共有两种可能。 □

第 12 题所用的补充同构判别。固定正整数 m, n，设 $r, s \in U_m$ 且 $r^n = s^n = 1$。对于

$$G_r = \langle a, b \mid a^m = b^n = e,\ bab^{-1} = a^r \rangle,$$

有

$$G_r \cong G_s \iff \langle r \rangle = \langle s \rangle \text{ 于} U_m \iff \exists\, t \in \mathbb{Z},\ \gcd(t, n) = 1,\ s \equiv r^t \pmod{m}.$$

这里要求 $\langle r \rangle$ 与 $\langle s \rangle$ 是 U_m 中同一个子群，而不只是抽象同构。

上述同构判别的一般必要性是额外的理论结果，此处引用而不证明；不能仅凭更换生成元所证明的充分性，就断言已经完成同构类型的去重。相关结果见 B. G. Basmaji，*On the Isomorphisms of Two Metacyclic Groups*，Proc. Amer. Math. Soc. **22** (1969), 175–182。

3.2 Sylow 定理

1. 给出 S_4 的一个 Sylow 2-子群和一个 Sylow 3-子群。

解 由于 $|S_4| = 24 = 2^3 \cdot 3$，故 Sylow 2-子群的阶为 8，Sylow 3-子群的阶为 3。

令 $r = (1234)$、$s = (13)$，并令 $P = \langle r, s\rangle$。有 $o(r) = 4$、$o(s) = 2$，且

$$srs^{-1} = (13)(1234)(13) = (1432) = r^{-1}.$$

因此利用 $sr = r^{-1}s$，P 中任意元素都可以写成 r^i 或 r^is 的形式，其中 $0 \leqslant i \leqslant 3$。又 $s \notin \langle r\rangle$，所以 $\langle r\rangle$ 与 $\langle r\rangle s$ 是两个不同的陪集，从而 $|P| = 2|\langle r\rangle| = 8$。因此

$$\boxed{\langle (1234), (13)\rangle}$$

是 S_4 的一个 Sylow 2-子群。

另一方面，$Q = \langle (123)\rangle$ 的阶为 3，故

$$\boxed{\langle (123)\rangle}$$

是 S_4 的一个 Sylow 3-子群。 □

2. 设 G 为有限群，$N \trianglelefteq G$，P 为 N 的一个 Sylow p-子群，证明 $G = N_G(P)N$。

解 任取 $g \in G$。由于 $N \trianglelefteq G$，有 $gNg^{-1} = N$。又 $P \leqslant N$，故 $gPg^{-1} \leqslant N$，且 $|gPg^{-1}| = |P|$。因此 gPg^{-1} 也是 N 的一个 Sylow p-子群。

由 Sylow 定理，N 的任意两个 Sylow p-子群在 N 中共轭，所以存在 $n \in N$，使得

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

于是

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

故 $n^{-1}g \in N_G(P)$。记 $x = n^{-1}g$，则 $g = nx$，其中 $n \in N$、$x \in N_G(P)$，所以 $G \subseteq NN_G(P)$。

又因为 $N \trianglelefteq G$，对任意 $x \in N_G(P)$、$n \in N$，有 $x^{-1}nx \in N$，从而 $nx = x(x^{-1}nx) \in N_G(P)N$。因此 $NN_G(P) = N_G(P)N$。

故 $G \subseteq N_G(P)N$。反向包含显然成立，因此

$$\boxed{G = N_G(P)N}.$$

□

3. 设 p 为素数，写出 p 元域上 n 级一般线性群 $\mathrm{GL}_n(\mathbb{Z}_p)$ 的一个 Sylow p-子群。

解 先计算 $\mathrm{GL}_n(\mathbb{Z}_p)$ 的阶。构造一个可逆矩阵时，第一列可以任取非零向量，有 $p^n - 1$ 种选择；第二列不能属于第一列张成的子空间，有 $p^n - p$ 种选择；依此类推，故

$$|\mathrm{GL}_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}).$$

将各因子中的 p 的幂提出，得到

$$|\mathrm{GL}_n(\mathbb{Z}_p)| = p^{1+2+\cdots+(n-1)}(p^n - 1)(p^{n-1} - 1)\cdots(p - 1).$$

因为每个 p^k-1 都不能被 p 整除，所以 $|\mathrm{GL}_n(\mathbb{Z}_p)|$ 中 p 的最高次幂为

$$p^{1+2+\cdots+(n-1)}=p^{\frac{n(n-1)}{2}}.$$

现令 U 为所有对角元均为 1 的上三角矩阵组成的集合，即

$$U=\left\{\begin{pmatrix}1 & a_{12} & a_{13} & \cdots & a_{1n}\\ 0 & 1 & a_{23} & \cdots & a_{2n}\\ \vdots & \ddots & \ddots & \ddots & \vdots\\ 0 & \cdots & 0 & 1 & a_{n-1,n}\\ 0 & \cdots & \cdots & 0 & 1\end{pmatrix}\middle|\ a_{ij}\in\mathbb{Z}_p\right\}.$$

两个这样的矩阵相乘仍是这种形式，而其逆矩阵也仍是对角元全为 1 的上三角矩阵，故 $U\leqslant \mathrm{GL}_n(\mathbb{Z}_p)$。

矩阵中严格位于主对角线上方的位置共有 $\dfrac{n(n-1)}{2}$ 个，每个位置都有 p 种选择，所以

$$|U|=p^{\frac{n(n-1)}{2}}.$$

这正是 $|\mathrm{GL}_n(\mathbb{Z}_p)|$ 中 p 的最高次幂。因此

$$\boxed{U=\{(a_{ij})\in\mathrm{GL}_n(\mathbb{Z}_p)\mid a_{ii}=1,\ a_{ij}=0\ (i>j)\}}$$

是 $\mathrm{GL}_n(\mathbb{Z}_p)$ 的一个 Sylow p-子群。 □

4. 求 S_5 的 Sylow 5-子群的个数，并写出一个这样的子群。

解 由于

$$|S_5|=5!=120=5\cdot 24,$$

故 S_5 的 Sylow 5-子群的阶为 5。因此每个 Sylow 5-子群都是由一个 5-轮换生成的循环群。

先计算 S_5 中 5-轮换的个数。一个 5-轮换可由 $1,2,3,4,5$ 的一个排列写成，而循环表示中

$$(a_1a_2a_3a_4a_5)=(a_2a_3a_4a_5a_1)=\cdots$$

这 5 种写法表示同一个轮换，所以 5-轮换共有

$$\frac{5!}{5}=4!=24$$

个。

另一方面，每个 5 阶循环群有 $\phi(5)=4$ 个生成元，即其中 4 个非单位元都是 5-轮换，而且不同的 Sylow 5-子群除单位元外没有公共元素。因此 Sylow 5-子群的个数为

$$\frac{24}{4}=6.$$

例如，

$$\boxed{\langle(12345)\rangle=\{e,(12345),(13524),(14253),(15432)\}}$$

就是 S_5 的一个 Sylow 5-子群。 □

5. 设 G 为有限群，且 G 有一个非平凡的循环 Sylow 2-子群，证明 G 有指数为 2 的子群。

解 设 $P=\langle a\rangle$ 是 G 的一个非平凡循环 Sylow 2-子群，并设 $|P|=2^r$，其中 $r\geqslant 1$。由于 P 是 Sylow 2-子群，可以写 $|G|=2^rm$，其中 m 为奇数。

考虑 G 在自身上的左乘作用。对每个 $g \in G$，令

$$\lambda_g : G \longrightarrow G, \qquad \lambda_g(x) = gx.$$

则每个 λ_g 都是 G 上的一个置换，并且 $g \mapsto \lambda_g$ 给出一个同态 $\lambda : G \to S_{|G|}$。

再与置换的符号同态复合，得到

$$\varepsilon : G \longrightarrow \{1, -1\}, \qquad \varepsilon(g) = \operatorname{sgn}(\lambda_g).$$

下面证明 ε 不是平凡同态。

考察 Sylow 2-子群的生成元 a。由于 $o(a) = 2^r$，置换 $\lambda_a : x \mapsto ax$ 的每一个轨道都为

$$x,\ ax,\ a^2x, \ldots, a^{2^r-1}x,$$

所以 λ_a 是若干个长度为 2^r 的不相交轮换的乘积。这样的轮换共有

$$\frac{|G|}{2^r} = m$$

个。

一个长度为 2^r 的轮换的符号为 $(-1)^{2^r-1} = -1$。又 m 为奇数，因此

$$\varepsilon(a) = \operatorname{sgn}(\lambda_a) = (-1)^m = -1.$$

所以 ε 的像中既有 1 又有 -1，即 ε 为满同态。

令 $H = \ker \varepsilon$。由于 $\operatorname{Im} \varepsilon = \{1, -1\}$ 有两个元素，故 G 被分成 H 与任意一个映到 -1 的元素所在的两个陪集，因此

$$[G : H] = 2.$$

所以 G 存在一个指数为 2 的子群。 □

6. 设 $N \trianglelefteq G$ 且 N 为 p-群，证明 G 的所有 Sylow p-子群都包含 N。

解 任取 G 的一个 Sylow p-子群 P。由于 $N \trianglelefteq G$，故 $NP \leqslant G$。

又因为 N 和 P 都是 p-群，设 $|N| = p^r$、$|P| = p^s$。由子群乘积的阶数公式，

$$|NP| = \frac{|N||P|}{|N \cap P|}$$

也是 p 的幂，因此 NP 是 G 的一个 p-子群。

但 P 是 Sylow p-子群，即它的阶已经是 $|G|$ 中所能出现的最大的 p 的幂。又 $P \leqslant NP$，所以只能有 $NP = P$。

于是 $N \leqslant P$。

□

7. 设 $N \trianglelefteq G$，P 是 G 的一个 Sylow p-子群，证明 $N \cap P$ 是 N 的 Sylow p-子群且 PN/N 是 G/N 的 Sylow p-子群。

解 设 $|G| = p^a m$、$|N| = p^b n$，其中 $p \nmid m, n$。由于 P 是 G 的 Sylow p-子群，故 $|P| = p^a$。

因为 $N \trianglelefteq G$，所以 $PN \leqslant G$。设 $|P \cap N| = p^c$。由 $P \cap N \leqslant N$，有 $c \leqslant b$。另一方面，由子群乘积的阶数公式，

$$|PN| = \frac{|P||N|}{|P \cap N|} = \frac{p^a \cdot p^b n}{p^c} = p^{a+b-c} n.$$

由于 $PN \leqslant G$，由 Lagrange 定理有 $|PN| \mid |G|$，故 $a + b - c \leqslant a$，即 $c \geqslant b$。因此 $c = b$。

于是 $|P\cap N|=p^b$，正好是 $|N|$ 中 p 的最高次幂，所以 $P\cap N$ 是 N 的 Sylow p-子群。

再看商群 G/N。由于 $N\trianglelefteq G$，有 $PN/N\leqslant G/N$，并且

$$|PN/N|=[PN:N]=[P:P\cap N]=\frac{p^a}{p^b}=p^{a-b}.$$

另一方面，

$$|G/N|=\frac{|G|}{|N|}=p^{a-b}\frac{m}{n},$$

而 $p\nmid m,n$，故 p^{a-b} 正是 $|G/N|$ 中 p 的最高次幂。因此 PN/N 是 G/N 的 Sylow p-子群。 □

8. 设 H 是 G 的一个 Sylow p-子群，$K=N_G(H)$，$L=N_G(K)$，证明 $K=L$。

解 由 $K=N_G(H)$ 的定义，对任意 $k\in K$ 都有 $kHk^{-1}=H$，故 $H\trianglelefteq K$。又由于 H 是 G 的 Sylow p-子群且 $H\leqslant K\leqslant G$，所以 H 也是 K 的 Sylow p-子群。

因为 $H\trianglelefteq K$，所以 H 是 K 的唯一 Sylow p-子群。

现任取 $g\in L=N_G(K)$。由 $gKg^{-1}=K$，且 $H\leqslant K$，可知 $gHg^{-1}\leqslant K$。又 $|gHg^{-1}|=|H|$，故 gHg^{-1} 也是 K 的 Sylow p-子群。由唯一性，

$$gHg^{-1}=H.$$

因此 $g\in N_G(H)=K$，从而 $L\leqslant K$。

另一方面，每个子群都包含在自己的正规化子中，所以 $K\leqslant N_G(K)=L$。因此 $K=L$。 □

9. 设 K 是 G 的一个 Sylow p-子群，$K\ntrianglelefteq G$，证明存在 G 的子群 H 使得 $H\cap K$ 不是 H 的 Sylow p-子群。

解 由于 $K\ntrianglelefteq G$，存在 $g\in G$ 使得 $gKg^{-1}\neq K$。令 $H=gKg^{-1}$，则 $H\leqslant G$，且 H 与 K 共轭，所以 $|H|=|K|$。特别地，H 本身是一个 p-群。

由于 $H\neq K$，有 $H\cap K<H$。而 H 是 p-群，所以 H 自身就是 H 的 Sylow p-子群。由于 $H\cap K$ 是 H 的真子群，其阶严格小于 $|H|$，故 $H\cap K$ 不是 H 的 Sylow p-子群。

因此存在所要求的子群 H。 □

10. 证明非交换 6 阶群同构于 S_3。

解 设 G 为非交换 6 阶群。由于 $|G|=6=2\cdot 3$，由 Sylow 定理，Sylow 3-子群的个数 n_3 满足 $n_3\mid 2$ 且 $n_3\equiv 1\pmod 3$，故 $n_3=1$。因此 G 有唯一的 Sylow 3-子群 P，且 $P\trianglelefteq G$。

取 $P=\langle a\rangle$，则 $o(a)=3$。再取一个 Sylow 2-子群 $Q=\langle b\rangle$，则 $o(b)=2$。由于 $P\trianglelefteq G$，有 $bab^{-1}\in P$。共轭不改变元素的阶，所以 bab^{-1} 仍为 3 阶元素，从而 $bab^{-1}=a$ 或 a^{-1}。

若 $bab^{-1}=a$，则 $ab=ba$。又 $P\cap Q=\{e\}$，且 $P\trianglelefteq G$，所以 $PQ\leqslant G$，并且

$$|PQ|=\frac{|P||Q|}{|P\cap Q|}=3\cdot 2=6.$$

因此 $G=PQ$。此时 G 由可交换的 a,b 生成，故 G 为交换群，与假设矛盾。所以只能有

$$bab^{-1}=a^{-1}.$$

在 S_3 中令 $r=(123)$、$s=(12)$，则 $r^3=s^2=e$ 且 $srs^{-1}=r^{-1}$。因此赋值 $r\mapsto a$、$s\mapsto b$ 给出一个同态 $\varphi:S_3\to G$。

由于 $a,b\in\operatorname{Im}\varphi$，而 $G=\langle a,b\rangle$，故 φ 为满同态。又 $|S_3|=|G|=6$，所以 φ 为同构。因此

$$G\cong S_3.$$

□

11. 证明 72 和 180 阶群不是单群。

解 先设 $|G|=72=2^3\cdot 3^2$。由 Sylow 定理，Sylow 3-子群的个数 n_3 满足 $n_3\mid 8$ 且 $n_3\equiv 1\pmod 3$，故 $n_3=1$ 或 4。

若 $n_3=1$，则唯一的 Sylow 3-子群为非平凡真正规子群，故 G 不是单群。

若 $n_3=4$，反设 G 为单群。令 G 以共轭作用在这 4 个 Sylow 3-子群组成的集合上，得到同态 $\varphi:G\to S_4$。该作用不是平凡作用，否则每个 Sylow 3-子群都在共轭下不变，从而正规，与 $n_3=4$ 矛盾。因此 $\ker\varphi\neq G$。由 G 为单群，只能有 $\ker\varphi=\{e\}$，故 G 可嵌入 S_4。但 $|G|=72>|S_4|=24$，矛盾。因此 72 阶群不是单群。

下面设 $|G|=180=2^2\cdot 3^2\cdot 5$，反设 G 为单群。Sylow 5-子群的个数满足 $n_5\mid 36$ 且 $n_5\equiv 1\pmod 5$，故 $n_5=1,6$ 或 36。由于 G 为单群，$n_5\neq 1$。

若 $n_5=6$，则 G 以共轭作用在这 6 个 Sylow 5-子群上，得到非平凡同态 $\varphi:G\to S_6$。由单群性，φ 必为单射。再考虑符号同态 $\operatorname{sgn}:S_6\to\{\pm1\}$。复合映射 $\operatorname{sgn}\circ\varphi:G\to\{\pm1\}$ 必为平凡同态，否则其核将是 G 的指数为 2 的非平凡真正规子群，与单群矛盾。因此 $\varphi(G)\leqslant A_6$。但

$$[A_6:\varphi(G)]=\frac{360}{180}=2,$$

故 $\varphi(G)\trianglelefteq A_6$。由 A_6 为单群，矛盾。

故只能有 $n_5=36$。此时不同的 Sylow 5-子群交于 $\{e\}$，所以它们一共含有 $36(5-1)=144$ 个非单位元。

再看 Sylow 3-子群。其个数 n_3 满足 $n_3\mid 20$ 且 $n_3\equiv 1\pmod 3$，故 $n_3=1,4$ 或 10。由单群性 $n_3\neq 1$。若 $n_3=4$，同样利用共轭作用可得到单射 $G\to S_4$，但 $180>24$，矛盾。因此 $n_3=10$。

若这 10 个 Sylow 3-子群两两交于 $\{e\}$，则它们共有 $10(9-1)=80$ 个非单位元。由于 3-元素与 5-元素不可能相同，此时 G 至少有 $144+80=224$ 个非单位元，与 $|G|=180$ 矛盾。因此存在两个不同的 Sylow 3-子群 P,Q，使得 $R=P\cap Q\neq\{e\}$。由于 $|P|=|Q|=9$ 且 $P\neq Q$，故 $|R|=3$。

群 P,Q 都是 9 阶群，因而是交换群，所以 $R\trianglelefteq P$ 且 $R\trianglelefteq Q$。于是 $P,Q\leqslant N_G(R)$。记 $M=N_G(R)$，则 P,Q 是 M 中两个不同的 Sylow 3-子群。因此 M 的 Sylow 3-子群个数至少为 4，从而

$$[M:P]\geqslant 4,\qquad |M|\geqslant 4\cdot 9=36.$$

故 $[G:M]\leqslant 180/36=5$。

由于 G 为单群而 R 是非平凡真子群，R 不可能正规，所以 $[G:N_G(R)]>1$。令 $t=[G:N_G(R)]$，则 $2\leqslant t\leqslant 5$。G 以共轭作用在 R 的 t 个共轭子群上，得到非平凡同态 $G\to S_t$。由单群性该同态必须为单射，但

$$|G|=180>|S_t|\geqslant|S_5|=120$$

应改为 $|S_t|\leqslant 120$，故不可能有单射。矛盾。

因此 180 阶群也不是单群。 □

12. 证明 455 阶群一定是循环群。

解 设 $|G|=455=5\cdot 7\cdot 13$。

先考察 Sylow 13-子群。其个数 n_{13} 满足 $n_{13}\mid 35$ 且 $n_{13}\equiv 1\pmod{13}$。35 的正因子为 $1,5,7,35$，其中只有 1 模 13 余 1，故 $n_{13}=1$。因此 Sylow 13-子群 P_{13} 唯一，且 $P_{13}\trianglelefteq G$。

同理，Sylow 7-子群的个数 n_7 满足 $n_7\mid 65$ 且 $n_7\equiv 1\pmod 7$。65 的正因子为 $1,5,13,65$，其中也只有 1 模 7 余 1，故 $n_7=1$。因此 $P_7\trianglelefteq G$。

由于 $|P_7|=7$、$|P_{13}|=13$，二者交为 $\{e\}$。又二者都是正规子群，所以任取 $x\in P_7$、$y\in P_{13}$，有 $xyx^{-1}y^{-1}\in P_7\cap P_{13}=\{e\}$，故 $xy=yx$。因此 $H=P_7P_{13}\cong P_7\times P_{13}$，且 $|H|=91$。因为 P_7,P_{13} 都是素数阶循环群且 $7,13$ 互素，所以 H 是 91 阶循环群。

任取 G 的一个 Sylow 5-子群 P_5，则 $|P_5|=5$。由于 $P_7\trianglelefteq G$，共轭给出同态

$$P_5\longrightarrow \mathrm{Aut}(P_7).$$

而 $P_7\cong\mathbb{Z}_7$，故 $|\mathrm{Aut}(P_7)|=6$。上述同态的像的阶既整除 5 又整除 6，所以像只能为单位元。因此 P_5 中每个元素都与 P_7 中每个元素交换。

同理，由 $|\mathrm{Aut}(P_{13})|=12$ 且 $\gcd(5,12)=1$，可知 P_5 中每个元素也都与 P_{13} 中每个元素交换。因此 P_5 与整个 $H=P_7P_{13}$ 逐元素交换。

又 $H\trianglelefteq G$，且 $H\cap P_5=\{e\}$，所以 $HP_5\leqslant G$，并且

$$|HP_5|=\frac{|H||P_5|}{|H\cap P_5|}=91\cdot 5=455=|G|.$$

故 $G=HP_5$。由于 H 与 P_5 逐元素交换，

$$G\cong H\times P_5\cong\mathbb{Z}_{91}\times\mathbb{Z}_5.$$

又 $\gcd(91,5)=1$，所以 $\mathbb{Z}_{91}\times\mathbb{Z}_5\cong\mathbb{Z}_{455}$。

因此 G 为循环群。 □

13. 设 $p<q<r$ 为素数，证明 pqr 阶群有唯一的 r 阶子群。

解 设 $|G|=pqr$，记 Sylow r-子群的个数为 n_r。由 Sylow 定理，$n_r\mid pq$ 且 $n_r\equiv 1\pmod r$。因为 $p,q<r$，所以 n_r 不可能等于 p 或 q，故只需排除 $n_r=pq$ 的可能。

反设 $n_r=pq$。每个 Sylow r-子群的阶均为素数 r，两个不同的 Sylow r-子群只能交于 $\{e\}$，故这些子群一共含有 $pq(r-1)$ 个非单位元。因此除去这些元素和单位元后，G 中至多还剩

$$pqr-1-pq(r-1)=pq-1$$

个非单位元。

下面考察 Sylow q-子群的个数 n_q。若 $n_q>1$，由 $n_q\equiv 1\pmod q$，必有 $n_q\geqslant q+1$。不同的 Sylow q-子群也只能交于 $\{e\}$，故至少有

$$(q+1)(q-1)=q^2-1$$

个非单位的 q-元素。但 $q>p$，所以 $q^2-1>pq-1$，与上面的计数矛盾。因此 $n_q=1$。

于是 G 的 Sylow q-子群 Q 唯一，故 $Q\trianglelefteq G$。任取一个 Sylow r-子群 R，由于 $Q\trianglelefteq G$，有 $QR\leqslant G$，且 $Q\cap R=\{e\}$，所以 $|QR|=qr$。

在群 QR 中，Sylow r-子群的个数整除 q 且模 r 余 1。由于 $q<r$，只能为 1，故 $R\trianglelefteq QR$。于是 $Q\leqslant N_G(R)$。

另一方面，由 $n_r=pq$，利用共轭作用有

$$[G:N_G(R)]=n_r=pq,$$

故 $|N_G(R)|=r$。但 $Q\leqslant N_G(R)$ 且 $|Q|=q$，这与 Lagrange 定理矛盾。

因此 $n_r\neq pq$，只能有 $n_r=1$。故 G 有唯一的 r 阶子群。 □

14. 把 D_n 看成是 S_n 的子群，证明 $D_n\leqslant A_n$ 当且仅当 $n\equiv 1\pmod 4$。进一步地，设 p 为素数且 $p\equiv 3\pmod 4$，证明 A_p 无 $2p$ 阶子群。

解 把 D_n 看成正 n 边形在顶点集 $\{1,\dots,n\}$ 上的置换群。记 $r=(12\cdots n)$ 为旋转，s 为一个反射，则 $D_n=\langle r,s\rangle$。

首先，r 是一个 n-轮换，可以写成 $n-1$ 个对换的乘积，所以 r 为偶置换当且仅当 $n-1$ 为偶数，即 n 为奇数。因此若 n 为偶数，则 $r\notin A_n$，从而 $D_n\not\leqslant A_n$。

以下设 n 为奇数。此时任一反射固定一个顶点，并将其余 $n-1$ 个顶点两两交换，所以 s 是 $\dfrac{n-1}{2}$ 个互不相交对换的乘积。因此

$$s\in A_n \iff \frac{n-1}{2}\text{ 为偶数} \iff n\equiv 1 \pmod 4.$$

当 $n\equiv 1 \pmod 4$ 时，生成元 r,s 都是偶置换，故 $D_n=\langle r,s\rangle\leqslant A_n$；反之，若 $D_n\leqslant A_n$，则 r,s 都必须为偶置换，由上面的讨论必有 $n\equiv 1 \pmod 4$。因此

$$D_n\leqslant A_n \iff n\equiv 1 \pmod 4.$$

下面设 $p\equiv 3 \pmod 4$ 为素数。反设 A_p 有一个 $2p$ 阶子群 H。由 Sylow 定理，H 的 Sylow p-子群个数 n_p 满足 $n_p\mid 2$ 且 $n_p\equiv 1 \pmod p$，故 $n_p=1$。记这个唯一的 Sylow p-子群为 $P=\langle a\rangle$，则 $P\trianglelefteq H$。

由 Cauchy 定理，H 中存在一个 2 阶元素 b。因为 p 为奇数，故 $b\notin P$。又 $P\trianglelefteq H$，所以存在整数 t 使 $bab^{-1}=a^t$。由 $b^2=e$，

$$a=b^2ab^{-2}=a^{t^2},$$

故 $t^2\equiv 1 \pmod p$，即 $t\equiv\pm 1 \pmod p$。

若 $t\equiv 1 \pmod p$，则 $ab=ba$。但 a 是 S_p 中的一个 p-轮换，与 a 交换的置换都是 a 的幂，即 $C_{S_p}(a)=\langle a\rangle$，于是 $b\in\langle a\rangle=P$，矛盾。因此只能有 $bab^{-1}=a^{-1}$。

这说明 $H=\langle a,b\rangle$ 在 p 个点上的作用正是二面体群 D_p 的作用，其中 a 为旋转，b 为反射。由前面已经证明的结论，因为 $p\equiv 3 \pmod 4$，有 $D_p\not\leqslant A_p$，这与 $H\leqslant A_p$ 矛盾。

因此 A_p 不存在 $2p$ 阶子群。 □

15. 设群 G 的阶为 $n=p^rm$，其中 p 为素数且 $p\nmid m$，$r>0$，证明对于任意正整数 $k\leqslant r$，G 的 p^k 阶子群的个数模 p 余 1。

解 记 a_k 为 G 的 p^k 阶子群的个数，并约定 $a_0=1$。我们证明 $a_k\equiv a_{k-1} \pmod p$，从而逐次得到 $a_k\equiv 1 \pmod p$。

先说明两个计数事实。

第一，若有限群 M 的阶能被 p 整除，则 M 的 p 阶子群个数模 p 余 1。事实上，考虑

$$X=\{(x_1,\dots,x_p)\in M^p \mid x_1x_2\cdots x_p=e\}.$$

任意给定前 $p-1$ 个分量，最后一个分量唯一确定，故 $|X|=|M|^{p-1}\equiv 0 \pmod p$。循环群 C_p 通过循环移动分量作用在 X 上。非平凡轨道的大小都是 p，所以 $|X|$ 模 p 等于不动点个数。不动点恰为 $(x,\dots,x)$，其中 $x^p=e$。因此满足 $x^p=e$ 的元素个数能被 p 整除。

设 M 中 p 阶子群的个数为 c。不同的 p 阶子群除单位元外互不相交，而每个这样的子群有 $p-1$ 个非单位元，所以满足 $x^p=e$ 的元素共有 $1+(p-1)c$ 个。因此 $1+(p-1)c\equiv 0 \pmod p$，即 $c\equiv 1 \pmod p$。

第二，任一非平凡有限 p-群 K 的指数为 p 的子群个数模 p 余 1。记这个个数为 $d(K)$。把 $\mathbb{Z}_p$ 写成加法群，所有同态 $K\to\mathbb{Z}_p$ 构成一个有限的 $\mathbb{Z}_p$-向量空间，设其维数为 $s\geqslant 1$，故共有 p^s 个同态。每个非零同态都是满同态，其核是 K 的一个指数为 p 的子群；反过来，每个指数为 p 的子群都是某个满同态 $K\to\mathbb{Z}_p$ 的核，并且对应恰好 $p-1$ 个非零同态。因此

$$d(K)=\frac{p^s-1}{p-1}=1+p+\cdots+p^{s-1}\equiv 1 \pmod p.$$

现固定 $1\leqslant k\leqslant r$，考虑所有有序对

$$\Omega_k=\{(H,K)\mid H\leqslant K\leqslant G,\ |H|=p^{k-1},\ |K|=p^k\}.$$

先固定第二个分量 K。此时 H 恰为 K 的指数为 p 的子群。由上面的第二个计数事实，每个这样的 K 所对应的 H 的个数都模 p 余 1。因此

$$|\Omega_k| \equiv a_k \pmod{p}.$$

再固定第一个分量 H。若 $H \leqslant K$ 且 $|K:H| = p$，则 $H \trianglelefteq K$，故 $K \leqslant N_G(H)$，而 K/H 是 $N_G(H)/H$ 的一个 p 阶子群。反之，$N_G(H)/H$ 的每个 p 阶子群的原像都是一个包含 H 的 p^k 阶子群。因此，包含 H 的 p^k 阶子群的个数，正好等于 $N_G(H)/H$ 的 p 阶子群个数。

由于 $k-1 < r$，H 不是 G 的 Sylow p-子群。取一个包含 H 的 Sylow p-子群 P。有限 p-群满足正规化子条件，所以 $H < N_P(H)$，从而 $p \mid [N_G(H):H]$。因此由第一个计数事实，$N_G(H)/H$ 的 p 阶子群个数模 p 余 1。

所以对每一个 p^{k-1} 阶子群 H，包含它的 p^k 阶子群个数都模 p 余 1，从而

$$|\Omega_k| \equiv a_{k-1} \pmod{p}.$$

比较两种计数方式，得到 $a_k \equiv a_{k-1} \pmod{p}$。由于 $a_0 = 1$，逐次可得

$$a_k \equiv a_{k-1} \equiv \cdots \equiv a_0 = 1 \pmod{p}.$$

因此，对于任意 $1 \leqslant k \leqslant r$，$G$ 的 p^k 阶子群的个数模 p 余 1。 □

16. 设有限群 G 的阶为 n，且对 n 的每个正因子 m，群 G 有唯一的 m 阶子群，证明 G 为循环群。

解 设

$$n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$$

为 n 的素因数分解。对每个 i，由假设，G 有唯一的 $p_i^{a_i}$ 阶子群 P_i，它就是 G 的唯一 Sylow p_i-子群，因此 $P_i \trianglelefteq G$。

先证明每个 P_i 都是循环群。更一般地，设 P 是一个 p^a 阶子群。由题设，对每个 $0 \leqslant k \leqslant a$，$G$ 有唯一的 p^k 阶子群，因此 P 中也只有一个 p^k 阶子群。

对 a 作归纳。当 $a = 1$ 时，P 为素数阶群，故为循环群。设结论对 p^{a-1} 阶群成立。令 M 为 P 中唯一的 p^{a-1} 阶子群，则由归纳假设 M 为循环群。

取 $x \in P \setminus M$。若 $o(x) = p^k$，其中 $k < a$，则 $\langle x \rangle$ 是一个 p^k 阶子群。而 M 为循环群，所以 M 中存在一个 p^k 阶子群；由题设的唯一性，这个子群只能是 $\langle x \rangle$。于是 $\langle x \rangle \leqslant M$，从而 $x \in M$，矛盾。因此 $o(x) = p^a$，故 $P = \langle x \rangle$。所以每个 P_i 都是循环群。

下面证明不同的 P_i 之间元素可交换。若 $i \neq j$，任取 $x \in P_i$、$y \in P_j$。由于 $P_i, P_j \trianglelefteq G$，有

$$xyx^{-1}y^{-1} \in P_i \cap P_j.$$

而 $|P_i|$ 与 $|P_j|$ 互素，所以 $P_i \cap P_j = \{e\}$。因此 $xyx^{-1}y^{-1} = e$，即 $xy = yx$。

于是 $P_1, \ldots, P_s$ 两两逐元素可交换，且它们的阶两两互素。因此 $P_1 P_2 \cdots P_s$ 是子群，并且

$$|P_1 P_2 \cdots P_s| = |P_1||P_2| \cdots |P_s| = n = |G|.$$

故 $G = P_1 P_2 \cdots P_s$。

对每个 i 取生成元 x_i，即 $P_i = \langle x_i \rangle$，令 $x = x_1 x_2 \cdots x_s$。由于各 x_i 两两可交换且阶两两互素，

$$o(x) = \prod_{i=1}^{s} o(x_i) = \prod_{i=1}^{s} p_i^{a_i} = n.$$

因此 $\langle x \rangle$ 有 n 个元素，只能等于 G。故 G 为循环群。 □

17. 设 p 为一个素数，求 S_p 的 Sylow p-子群的个数，并证明 Wilson 定理

$$(p-1)! \equiv -1 \pmod{p}.$$

解 由于 $|S_p| = p!$，而 $p^2 \nmid p!$，所以 S_p 的 Sylow p-子群的阶为 p。因此每个 Sylow p-子群都是由一个 p-轮换生成的循环群。

先计算 S_p 中 p-轮换的个数。一个 p-轮换可写成 $(a_1 a_2 \cdots a_p)$，共有 $p!$ 种排列写法；但循环移动

$$(a_1 a_2 \cdots a_p) = (a_2 \cdots a_p a_1) = \cdots$$

给出同一个轮换，每个轮换恰有 p 种这样的写法。因此 p-轮换的个数为

$$\frac{p!}{p} = (p-1)!.$$

每个 p 阶循环子群有 $p-1$ 个非单位元，而这 $p-1$ 个非单位元全都是 p-轮换。不同的 p 阶子群除单位元外没有公共元素。因此 S_p 的 Sylow p-子群个数为

$$n_p = \frac{(p-1)!}{p-1} = (p-2)!.$$

另一方面，由 Sylow 定理，$n_p \equiv 1 \pmod{p}$，所以

$$(p-2)! \equiv 1 \pmod{p}.$$

两边同乘 $p-1$，得到

$$(p-1)! = (p-1)(p-2)! \equiv (-1) \cdot 1 = -1 \pmod{p}.$$

这正是 Wilson 定理。 □

18. 设 G 为一个有限群，p 为一个整除 $|G|$ 的素数，N 为 G 的一个正规子群，且 $p \nmid [G:N]$，证明对 G 的任意 Sylow p-子群 P，均有 $P \leqslant N$。

解 任取 G 的一个 Sylow p-子群 P，设 $|P| = p^k$。考虑自然同态

$$\pi : G \longrightarrow G/N, \qquad \pi(g) = gN.$$

则 $\pi(P) \leqslant G/N$。设 $|P \cap N| = p^j$，其中 $0 \leqslant j \leqslant k$。

对任意 $x, y \in P$，有

$$\pi(x) = \pi(y) \Longleftrightarrow xN = yN \Longleftrightarrow y^{-1}x \in N.$$

又因为 $x, y \in P$，所以 $y^{-1}x \in P$，故

$$\pi(x) = \pi(y) \Longleftrightarrow y^{-1}x \in P \cap N \Longleftrightarrow x(P \cap N) = y(P \cap N).$$

因此 $\pi(P)$ 中的元素与 P 关于 $P \cap N$ 的左陪集一一对应，从而

$$|\pi(P)| = [P : P \cap N] = \frac{|P|}{|P \cap N|} = p^{k-j}.$$

另一方面，$\pi(P) \leqslant G/N$，由 Lagrange 定理，

$$p^{k-j} = |\pi(P)| \mid |G/N| = [G:N].$$

但题设 $p \nmid [G:N]$，所以只能有 $k - j = 0$，即 $j = k$。于是 $|P \cap N| = |P|$。

由于 $P \cap N \leqslant P$，故 $P \cap N = P$，从而

$$P \leqslant N.$$

因此 G 的任意 Sylow p-子群都包含于 N。 □

3.3 有限交换群的结构

1. 证明 Lagrange 定理的逆对有限交换群成立，即设 G 为 n 阶交换群，d 为正整数且 $d \mid n$，则 G 有 d 阶子群。

解 对 n 作归纳。$n=1$ 时结论成立。设结论对阶小于 n 的有限交换群成立，现设 $|G|=n$。

若 $d=1$，则 $\{e\}$ 即为所求子群。以下设 $d>1$，取素数 $p \mid d$。由于 $d \mid n$，故 $p \mid |G|$，由 Cauchy 定理，存在 $a \in G$ 使 $o(a)=p$。令 $N=\langle a\rangle$，则 $|N|=p$。

因为 G 为交换群，所以 $N \trianglelefteq G$，且 G/N 仍为交换群。又 $|G/N|=n/p<n$，并且 $d/p \mid n/p$，由归纳假设，G/N 有一个 d/p 阶子群 $\overline{H}$。

设 $\pi: G \to G/N$ 为自然同态，令 $H=\pi^{-1}(\overline{H})$，则 $H \leqslant G$。由于 $\overline{H}$ 中的每个元素都是 N 的一个陪集，而每个陪集有 p 个元素，所以

$$|H| = |N|\,|\overline{H}| = p \cdot \frac{d}{p} = d.$$

因此 H 就是所求的 d 阶子群，归纳完成。 □

2. 设 G 为有限交换 p-群，n 为正整数且 $p \nmid n$，证明对任意 $a \in G$，方程 $x^n=a$ 在群 G 中有解。

解 设 $|G|=p^r$。因为 $p \nmid n$，所以 $\gcd(n,p^r)=1$，由 Bézout 等式，存在整数 u,v 使 $nu+p^rv=1$。

任取 $a \in G$，由 Lagrange 定理，$a^{p^r}=e$。令 $x=a^u \in G$，则

$$x^n = a^{un} = a^{1-p^rv} = a(a^{p^r})^{-v} = a.$$

因此 $x=a^u$ 就是方程 $x^n=a$ 的一个解。 □

3. 给出 360 阶交换群的所有可能的初等因子组和不变因子组，并给出所有互不同构的 360 阶交换群。

解 由于 $360=2^3\cdot 3^2\cdot 5$，由有限交换群结构定理，任一 360 阶交换群都同构于其 Sylow 2-子群、Sylow 3-子群和 Sylow 5-子群的直积。

其中，8 阶交换群有 $\mathbb{Z}_8$、$\mathbb{Z}_2\times\mathbb{Z}_4$、$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ 三种可能；9 阶交换群有 $\mathbb{Z}_9$、$\mathbb{Z}_3\times\mathbb{Z}_3$ 两种可能；5 阶群只能为 $\mathbb{Z}_5$。因此共有 $3\cdot 2=6$ 种初等因子组。

以下将不变因子按 $d_1 \mid d_2 \mid \cdots \mid d_t$ 排列。求不变因子时，将各素数对应的初等因子分别从小到大排列，在左侧补 1 使各组长度相同，再将同一位置的数相乘。这样合并是因为互素阶循环群的直积仍为循环群。

例如，对于初等因子组 $(2,4,3,3,5)$，三组分别写成 $(2,4)$、$(3,3)$、$(1,5)$，按位置相乘得到 $(2\cdot3\cdot1, 4\cdot3\cdot5)=(6,60)$。

全部结果如下：

初等因子组	不变因子组	对应的群
$(8,9,5)$	(360)	$\mathbb{Z}_{360}$
$(8,3,3,5)$	$(3,120)$	$\mathbb{Z}_3\times\mathbb{Z}_{120}$
$(2,4,9,5)$	$(2,180)$	$\mathbb{Z}_2\times\mathbb{Z}_{180}$
$(2,4,3,3,5)$	$(6,60)$	$\mathbb{Z}_6\times\mathbb{Z}_{60}$
$(2,2,2,9,5)$	$(2,2,90)$	$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{90}$
$(2,2,2,3,3,5)$	$(2,6,30)$	$\mathbb{Z}_2\times\mathbb{Z}_6\times\mathbb{Z}_{30}$

由有限交换群结构定理的唯一性，不同的初等因子组对应不同构的群。因此上表恰为所有互不同构的 360 阶交换群，共 6 个。 □

4. 给出所有互不同构的 16 阶交换群，并给出其中恰有 3 个 2 阶元素的群。

解 由有限交换群结构定理，任一 16 阶交换群都可写成 $\mathbb{Z}_{2^{a_1}} \times \cdots \times \mathbb{Z}_{2^{a_t}}$，其中 $a_i \geqslant 1$ 且 $a_1 + \cdots + a_t = 4$。整数 4 的无序分拆为 4、3 + 1、2 + 2、2 + 1 + 1、1 + 1 + 1 + 1，因此共有 5 种同构类型。

下面计算各群中 2 阶元素的个数。在每个非平凡循环 2-群中，满足 $x^2 = e$ 的元素恰有两个，即单位元和唯一的 2 阶元素。因此，若一个群是 t 个非平凡循环 2-群的直积，则满足 $x^2 = e$ 的元素共有 2^t 个；除去单位元后，恰有 $2^t - 1$ 个 2 阶元素。

故全部群及其 2 阶元素个数如下：

群	2 阶元素的个数
$\mathbb{Z}_{16}$	1
$\mathbb{Z}_2 \times \mathbb{Z}_8$	3
$\mathbb{Z}_4 \times \mathbb{Z}_4$	3
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$	7
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	15

因此，恰有 3 个 2 阶元素的群为 $\mathbb{Z}_2 \times \mathbb{Z}_8$ 和 $\mathbb{Z}_4 \times \mathbb{Z}_4$。 □

5. 证明 $175 = 5^2 \cdot 7$ 阶群和 $20449 = 11^2 \cdot 13^2$ 阶群一定交换，并给出所有互不同构的 175 阶和 20449 阶群。

解

(1) 设 $|G| = 175 = 5^2 \cdot 7$，记 Sylow 5-子群和 Sylow 7-子群的个数分别为 n_5, n_7。

由 Sylow 定理，$n_5 \mid 7$ 且 $n_5 \equiv 1 \pmod 5$。由于 $7 \not\equiv 1 \pmod 5$，故 $n_5 = 1$。又 $n_7 \mid 25$ 且 $n_7 \equiv 1 \pmod 7$，而 25 的正因子 $1, 5, 25$ 中只有 1 满足此同余式，故 $n_7 = 1$。

因此，Sylow 子群 P_5, P_7 都是正规子群。它们的阶互素，故 $P_5 \cap P_7 = \{e\}$，且

$$|P_5P_7| = \frac{|P_5||P_7|}{|P_5 \cap P_7|} = 25 \cdot 7 = 175,$$

所以 $G = P_5P_7$。

任取 $x \in P_5$、$y \in P_7$，由两个子群的正规性，$xyx^{-1}y^{-1} \in P_5 \cap P_7 = \{e\}$，故 $xy = yx$。因此 $G \cong P_5 \times P_7$。又素数平方阶群与素数阶群都是交换群，所以 P_5, P_7 都交换，从而 G 为交换群。

其中 P_5 只能同构于 $\mathbb{Z}_{25}$ 或 $\mathbb{Z}_5 \times \mathbb{Z}_5$，而 $P_7 \cong \mathbb{Z}_7$。因此所有可能为

$$\mathbb{Z}_{25} \times \mathbb{Z}_7 \cong \mathbb{Z}_{175},$$
$$\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_5 \times \mathbb{Z}_{35}.$$

这两个群的初等因子组不同，故不同构。因此共有 2 种同构类型。

(2) 设 $|G| = 20449 = 11^2 \cdot 13^2$，记 Sylow 11-子群和 Sylow 13-子群的个数分别为 n_{11}, n_{13}。

由 Sylow 定理，$n_{11} \mid 169$ 且 $n_{11} \equiv 1 \pmod{11}$。所以 n_{11} 只能为 $1, 13, 169$；由于 $13 \equiv 2 \pmod{11}$、$169 \equiv 4 \pmod{11}$，故 $n_{11} = 1$。

同理，$n_{13} \mid 121$ 且 $n_{13} \equiv 1 \pmod{13}$。所以 n_{13} 只能为 $1, 11, 121$；由于 $11 \not\equiv 1 \pmod{13}$、$121 \equiv 4 \pmod{13}$，故 $n_{13} = 1$。

因此，Sylow 子群 P_{11}, P_{13} 都是正规子群。它们的阶互素，故 $P_{11} \cap P_{13} = \{e\}$；又其阶的乘积等于 $|G|$，所以 $G = P_{11}P_{13}$。与 (1) 中相同，由正规性及交为 $\{e\}$ 可知两个子群之间的元素可交换，从而 $G \cong P_{11} \times P_{13}$。

由于 $|P_{11}| = 11^2$、$|P_{13}| = 13^2$，二者都是素数平方阶群，故都是交换群。因此 G 为交换群。

其中 P_{11} 只能同构于 $\mathbb{Z}_{121}$ 或 $\mathbb{Z}_{11}\times\mathbb{Z}_{11}$，$P_{13}$ 只能同构于 $\mathbb{Z}_{169}$ 或 $\mathbb{Z}_{13}\times\mathbb{Z}_{13}$。将两种选择分别组合，得到全部 4 种同构类型：

$$\mathbb{Z}_{121}\times\mathbb{Z}_{169}\cong\mathbb{Z}_{20449},$$
$$\mathbb{Z}_{121}\times\mathbb{Z}_{13}\times\mathbb{Z}_{13}\cong\mathbb{Z}_{13}\times\mathbb{Z}_{1573},$$
$$\mathbb{Z}_{11}\times\mathbb{Z}_{11}\times\mathbb{Z}_{169}\cong\mathbb{Z}_{11}\times\mathbb{Z}_{1859},$$
$$\mathbb{Z}_{11}\times\mathbb{Z}_{11}\times\mathbb{Z}_{13}\times\mathbb{Z}_{13}\cong\mathbb{Z}_{143}\times\mathbb{Z}_{143}.$$

这四个群的初等因子组两两不同，故它们两两不同构。

□

6. 设 A,B,C 均为有限交换群且 $A\times B\cong A\times C$，证明 $B\cong C$。

解 由有限交换群结构定理，有限交换群的同构类型由其初等因子组唯一确定。

对任意有限交换群 X、素数 p 和正整数 r，记 $c_{p,r}(X)$ 为 X 的初等因子组中 p^r 出现的次数。将 A,B 各自分解为素数幂阶循环群的直积，再将这些因子合在一起，就得到 $A\times B$ 的初等因子分解。因此

$$c_{p,r}(A\times B)=c_{p,r}(A)+c_{p,r}(B).$$

同理，$c_{p,r}(A\times C)=c_{p,r}(A)+c_{p,r}(C)$。

由于 $A\times B\cong A\times C$，由初等因子组的唯一性，对所有 p,r 都有

$$c_{p,r}(A)+c_{p,r}(B)=c_{p,r}(A)+c_{p,r}(C).$$

消去两边相同的整数 $c_{p,r}(A)$，得到 $c_{p,r}(B)=c_{p,r}(C)$。因此 B,C 的初等因子组相同，故 $B\cong C$。 □

7. 设 p 为素数，求群 $\mathbb{Z}_p\times\mathbb{Z}_p$ 的自同构群 $\mathrm{Aut}(\mathbb{Z}_p\times\mathbb{Z}_p)$。

解 将 $V=\mathbb{Z}_p\times\mathbb{Z}_p$ 写成加法群，并看成域 $\mathbb{Z}_p$ 上的二维向量空间。

若 $\alpha:V\to V$ 为群同态，则 $\alpha(u+v)=\alpha(u)+\alpha(v)$。由反复相加可得，对任意整数 t，有 $\alpha(tu)=t\alpha(u)$。因此对任意 $\lambda\in\mathbb{Z}_p$，都有 $\alpha(\lambda u)=\lambda\alpha(u)$，所以 α 为线性映射。反之，线性映射保持加法，因而也是群同态。

取标准基 $e_1=(1,0)^{\mathsf{T}}$、$e_2=(0,1)^{\mathsf{T}}$。设 $\alpha(e_1)=(a,c)^{\mathsf{T}}$、$\alpha(e_2)=(b,d)^{\mathsf{T}}$，则

$$\alpha\begin{pmatrix}x\\y\end{pmatrix}=x\alpha(e_1)+y\alpha(e_2)=\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}.$$

因此每个群同态唯一对应一个 2×2 矩阵，且它是自同构当且仅当对应矩阵可逆，即 $ad-bc\neq0$。

又同态的复合对应矩阵的乘法，所以这个对应给出群同构

$$\boxed{\mathrm{Aut}(\mathbb{Z}_p\times\mathbb{Z}_p)\cong\mathrm{GL}_2(\mathbb{Z}_p).}$$

可逆矩阵的第一列可以任取非零向量，有 p^2-1 种选择；第二列不能属于第一列张成的一维子空间，而该子空间有 p 个向量，所以第二列有 p^2-p 种选择。因此

$$\left|\mathrm{Aut}(\mathbb{Z}_p\times\mathbb{Z}_p)\right|=(p^2-1)(p^2-p)=p(p-1)^2(p+1).$$

□

8. 设 $m\geqslant n$ 为正整数，p 为素数，求群 $\mathbb{Z}_{p^m}\times\mathbb{Z}_{p^n}$ 的各阶循环子群的个数。进一步地，求该群的各阶子群的个数。

解 记 $A=\mathbb{Z}_{p^m}$、$B=\mathbb{Z}_{p^n}$、$G=A\times B$，均采用加法记号。由 Lagrange 定理，G 的子群的阶只能为 p^k，其中 $0\leqslant k\leqslant m+n$。

(1) **各阶循环子群的个数。**

对 $k \geqslant 0$，记 E_k 为满足 $p^k x = 0$ 的元素 $x \in G$ 的个数。在 A 中，方程 $p^k u = 0$ 有 $p^{\min(k,m)}$ 个解；在 B 中有 $p^{\min(k,n)}$ 个解。因此

$$E_k = p^{\min(k,m)+\min(k,n)}.$$

特别地，$E_0 = 1$。当 $k \geqslant 1$ 时，阶恰为 p^k 的元素个数为 $E_k - E_{k-1}$。

每个 p^k 阶循环子群恰有 $\phi(p^k) = p^{k-1}(p-1)$ 个生成元，而每个 p^k 阶元素唯一生成一个这样的子群。因此，记 c_k 为 p^k 阶循环子群的个数，则

$$c_k = \frac{E_k - E_{k-1}}{p^{k-1}(p-1)} \qquad (k \geqslant 1).$$

代入 E_k 并化简，得到

$$\boxed{c_k = \begin{cases} 1, & k = 0, \\ p^{k-1}(p+1), & 1 \leqslant k \leqslant n, \\ p^n, & n < k \leqslant m, \\ 0, & k > m. \end{cases}}$$

其中最后一种情形也可直接看出：G 中每个元素都满足 $p^m x = 0$，故不存在阶大于 p^m 的循环子群。

(2) **各阶子群的个数。**

记 s_k 为 G 的 p^k 阶子群的个数。对 $0 \leqslant i \leqslant m$、$0 \leqslant j \leqslant n$，分别记 A_i、B_j 为 A、B 中唯一的 p^i 阶、p^j 阶子群。

设 $\pi_A : G \to A$ 为第一分量投影。任意子群 $H \leqslant G$ 唯一确定两个整数 i, j，使

$$\pi_A(H) = A_i, \qquad H \cap (\{0\} \times B) = \{0\} \times B_j.$$

固定 $u \in A_i$，选取 $(u, v) \in H$。对任意 $v' \in B$，有 $(u, v') \in H$ 当且仅当 $(0, v' - v) \in H$，即 $v' - v \in B_j$。因此，所有与 u 配成 H 中元素的第二分量恰为陪集 $v + B_j$，共有 p^j 个。于是 $|H| = p^{i+j}$。

下面固定 i, j，计算满足上述两个条件的子群数。对这样的子群 H，定义 $f_H : A_i \to B/B_j$ 为 $f_H(u) = v + B_j$，其中 $(u, v) \in H$。由上面的陪集描述，f_H 与 v 的选取无关，故定义良好。又由 H 对加法封闭，有 $f_H(u + u') = f_H(u) + f_H(u')$，所以 f_H 是群同态。

反之，给定同态 $f : A_i \to B/B_j$，令

$$H_f = \{(u, v) \in A_i \times B \mid v + B_j = f(u)\}.$$

由 f 保持加法及逆元，H_f 是子群。每个 $f(u)$ 都有代表元，故 $\pi_A(H_f) = A_i$；又 $f(0) = B_j$，所以 $H_f \cap (\{0\} \times B) = \{0\} \times B_j$。由每个第二分量集合恰为相应陪集，还可得 $H_{f_H} = H$、$f_{H_f} = f$。

因此，固定 i, j 后，所求子群数等于同态 $A_i \to B/B_j$ 的个数。由于 A_i 为 p^i 阶循环群，一个同态由生成元的像唯一决定，该像只需满足 $p^i \bar{v} = 0$。而 B/B_j 为 p^{n-j} 阶循环群，满足此条件的元素有 $p^{\min(i,n-j)}$ 个，故这样的子群恰有 $p^{\min(i,n-j)}$ 个。

若要求 $|H| = p^k$，则 $i + j = k$，所以 $\max(0, k-m) \leqslant j \leqslant \min(k, n)$。每个子群唯一确定 i, j，从而

$$\begin{aligned} s_k &= \sum_{j=\max(0,k-m)}^{\min(k,n)} p^{\min(k-j,n-j)} \\ &= \sum_{j=\max(0,k-m)}^{\min(k,n)} p^{\min(k,n)-j}. \end{aligned}$$

分别按 $k \leqslant n$、$n < k \leqslant m$、$m < k \leqslant m+n$ 计算这个等比数列的和，得到

$$\boxed{s_k = \begin{cases} \dfrac{p^{k+1}-1}{p-1}, & 0 \leqslant k \leqslant n, \\ \dfrac{p^{n+1}-1}{p-1}, & n < k \leqslant m, \\ \dfrac{p^{m+n-k+1}-1}{p-1}, & m < k \leqslant m+n. \end{cases}}$$

□

9. 证明有限生成交换群是有限群当且仅当它的一组生成元均为有限阶元素。

解 若 G 为有限群，则由 Lagrange 定理，G 中每个元素的阶都有限，因而任一组生成元均为有限阶元素。

反之，由有限生成性，可从题设的生成元中选出有限个 $a_1, \ldots, a_t$，仍生成整个 G。记 $o(a_i) = n_i < \infty$。由于 G 为交换群，每个元素都可以整理成 $a_1^{r_1} \cdots a_t^{r_t}$ 的形式。再利用 $a_i^{n_i} = e$，可将各指数分别按模 n_i 化简。因此

$$G = \{a_1^{r_1} \cdots a_t^{r_t} \mid 0 \leqslant r_i < n_i,\ 1 \leqslant i \leqslant t\}.$$

这些乘积至多有 $n_1 \cdots n_t$ 个，所以 $|G| \leqslant n_1 \cdots n_t < \infty$。故 G 为有限群。 □

10. 分类 75 阶群，并证明交换的 75 阶群有 2 个，非交换的 75 阶群唯一。

解 以下分类均在同构意义下进行。设 $|G| = 75 = 3 \cdot 5^2$。由 Sylow 定理，Sylow 5-子群的个数 n_5 满足 $n_5 \mid 3$ 且 $n_5 \equiv 1 \pmod 5$，故 $n_5 = 1$。记这个唯一的 Sylow 5-子群为 P，则 $P \trianglelefteq G$。

取一个 Sylow 3-子群 $Q = \langle c \rangle$，则 $o(c) = 3$。由于 $P \cap Q = \{e\}$，且 $P \trianglelefteq G$，有 $PQ \leqslant G$，并且 $|PQ| = |P||Q| = 75$，故 $G = PQ$。因此 $G \cong P \rtimes Q$，其作用由共轭自同构 $T : P \to P$，$T(x) = cxc^{-1}$ 决定。由 $c^3 = e$，有 $T^3 = \mathrm{id}_P$。

因为 $|P| = 25$，所以 P 为交换群，且 $P \cong \mathbb{Z}_{25}$ 或 $\mathbb{Z}_5 \times \mathbb{Z}_5$。下面分别讨论。

(1) $P \cong \mathbb{Z}_{25}$。

此时 $|\mathrm{Aut}(P)| = \phi(25) = 20$。由于 $T^3 = \mathrm{id}_P$，T 的阶整除 3；又 $T \in \mathrm{Aut}(P)$，由 Lagrange 定理，T 的阶也整除 20。因 $\gcd(3, 20) = 1$，只能有 $T = \mathrm{id}_P$。

因此作用平凡，半直积为直积，故

$$G \cong \mathbb{Z}_{25} \times \mathbb{Z}_3 \cong \mathbb{Z}_{75}.$$

(2) $P \cong \mathbb{Z}_5 \times \mathbb{Z}_5$。

将 P 看成 $\mathbb{Z}_5$ 上的二维向量空间，并采用加法记号。由第 7 题，T 为可逆线性变换，且 $T^3 = I$。

若 $T = I$，则作用平凡，故

$$G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_5 \times \mathbb{Z}_{15}.$$

以下设 $T \neq I$，证明所有这样的非平凡作用都给出同一种半直积。

取 $u \in P$ 使 $Tu \neq u$，令 $v = (T - I)u \neq 0$。利用 $T^3 = I$，得到

$$(T^2 + T + I)v = (T^2 + T + I)(T - I)u = (T^3 - I)u = 0.$$

下面证明 v, Tv 线性无关。若二者线性相关，则因 $v \neq 0$，存在 $\lambda \in \mathbb{Z}_5$ 使 $Tv = \lambda v$。代入上式，得到 $(\lambda^2 + \lambda + 1)v = 0$，从而 $\lambda^2 + \lambda + 1 = 0$。

但这个等式蕴含 $(2\lambda+1)^2=-3=2$，而 $\mathbb{Z}_5$ 中的平方只有 $0,1,4$，不可能等于 2，矛盾。因此 v, Tv 构成 P 的一组基。

在这组基下，$T(v)=Tv$，且 $T(Tv)=T^2v=-v-Tv$，所以 T 的矩阵为

$$T_0=\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}.$$

这说明，每个满足 $T^3=I$、$T\neq I$ 的作用，经适当换基后都成为同一个作用。

具体地，设 $S:P\to\mathbb{Z}_5^2$ 将 v, Tv 分别映到标准基，则 $ST=T_0S$，从而 $ST^j=T_0^jS$。定义

$$F:P\rtimes_T\mathbb{Z}_3\longrightarrow\mathbb{Z}_5^2\rtimes_{T_0}\mathbb{Z}_3,\qquad F(x,\bar{j})=(Sx,\bar{j}).$$

由于 S 为双射，F 也是双射；又由半直积的乘法，

$$\begin{aligned}F\big((x,\bar{j})(y,\bar{k})\big)&=F(x+T^jy,\overline{j+k})\\&=(Sx+T_0^jSy,\overline{j+k})\\&=F(x,\bar{j})F(y,\bar{k}),\end{aligned}$$

所以 F 为同构。因此所有非平凡作用所给出的半直积彼此同构。

另一方面，直接计算可得 $T_0^2+T_0+I=0$，故 $T_0^3=I$；又 $T_0\neq I$。因此 $\theta(\bar{1})=T_0$ 确实定义了一个非平凡作用 $\theta:\mathbb{Z}_3\to\mathrm{GL}_2(\mathbb{Z}_5)$。相应的半直积

$$G_0=(\mathbb{Z}_5\times\mathbb{Z}_5)\rtimes_\theta\mathbb{Z}_3$$

的阶为 $25\cdot3=75$。由于作用非平凡，第二因子的生成元不与第一因子的所有元素交换，故 G_0 非交换。

综上，75 阶群共有 3 种同构类型：$\mathbb{Z}_{75}$、$\mathbb{Z}_5\times\mathbb{Z}_{15}$ 以及上述 G_0。前两个群交换，且前者有 75 阶元素，后者的元素阶均整除 15，所以二者不同构；第三个群非交换，并且非交换的同构类型唯一。 □

11. 分类 12 阶群。

解 设 $|G|=12=2^2\cdot3$，记 Sylow 3-子群的个数为 n_3。由 Sylow 定理，$n_3\mid4$ 且 $n_3\equiv1\pmod3$，故 $n_3=1$ 或 4。

(1) $n_3=1$。

记唯一的 Sylow 3-子群为 $N=\langle a\rangle$，则 $N\trianglelefteq G$。取一个 Sylow 2-子群 P，由 $|N|=3$、$|P|=4$，有 $N\cap P=\{e\}$ 且 $|NP|=12$，所以 $G=NP\cong N\rtimes P$。

由于 $\mathrm{Aut}(N)$ 只有恒等自同构和反演自同构 $a\mapsto a^{-1}$，共轭作用 $\theta:P\to\mathrm{Aut}(N)$ 或为平凡作用，或为满同态。

若作用平凡，则 $G\cong N\times P$。又 4 阶群只有 $\mathbb{Z}_4$ 和 $\mathbb{Z}_2\times\mathbb{Z}_2$ 两种，故得到两个交换群

$$\mathbb{Z}_3\times\mathbb{Z}_4\cong\mathbb{Z}_{12},\qquad\mathbb{Z}_3\times\mathbb{Z}_2\times\mathbb{Z}_2\cong\mathbb{Z}_6\times\mathbb{Z}_2.$$

以下设作用非平凡。若 $P=\langle b\rangle\cong\mathbb{Z}_4$，则其生成元必须诱导反演自同构，故得到

$$\Gamma=\langle a,b\mid a^3=b^4=e,\ bab^{-1}=a^{-1}\rangle\cong\mathbb{Z}_3\rtimes\mathbb{Z}_4,$$

其中 $\mathbb{Z}_4$ 的生成元按反演作用于 $\mathbb{Z}_3$。这个半直积确实有 12 个元素，且由 $bab^{-1}\neq a$ 可知它非交换。

若 $P\cong\mathbb{Z}_2\times\mathbb{Z}_2$，则 $\ker\theta$ 有两个元素。取其非单位元为 c，再取 $b\in P\setminus\ker\theta$，便有 $P=\langle b,c\rangle$，其中 $b^2=c^2=e$、$bc=cb$，并且 $bab^{-1}=a^{-1}$、$cac^{-1}=a$。

令 $r=ac$、$s=b$。由于 a,c 可交换且阶分别为 $3,2$，故 $o(r)=6$，并且

$$srs^{-1}=b(ac)b^{-1}=a^{-1}c=r^{-1}.$$

又 $c=r^3$、$a=r^4$，所以 r,s 生成 G。因此将二面体群 D_6 的旋转、反射生成元分别映到 r,s，得到满同态 $D_6\to G$。两群的阶均为 12，故 $G\cong D_6$。

(2) $n_3=4$。

令 Ω 为这 4 个 Sylow 3-子群组成的集合。共轭作用给出同态 $\varphi: G\to \mathrm{Sym}(\Omega)\cong S_4$。

任取 $P\in\Omega$。由 Sylow 子群彼此共轭，P 的轨道为整个 Ω，其稳定子为 $N_G(P)$，故 $[G:N_G(P)]=4$，从而 $|N_G(P)|=3$。又 $P\leqslant N_G(P)$，所以 $N_G(P)=P$。

$\ker\varphi$ 中的元素固定所有 Sylow 3-子群，特别地固定 P，故 $\ker\varphi\leqslant P$。由于 $|P|=3$，只能有 $\ker\varphi=\{e\}$ 或 P。若 $\ker\varphi=P$，则 $P\trianglelefteq G$，与 $n_3=4$ 矛盾。因此 φ 为单射。

不同的 3 阶子群除单位元外不相交，所以 G 有 $4(3-1)=8$ 个 3 阶元素。它们在 φ 下的像是 S_4 中 8 个不同的 3-轮换，而 S_4 中恰有 $\binom{4}{3}\cdot 2=8$ 个 3-轮换。因此 $\varphi(G)$ 包含全部 3-轮换，从而包含由它们生成的 A_4。又 $|\varphi(G)|=12=|A_4|$，故 $\varphi(G)=A_4$，即 $G\cong A_4$。

综上，12 阶群共有以下 5 种同构类型：

$$\boxed{\mathbb{Z}_{12},\quad \mathbb{Z}_6\times\mathbb{Z}_2,\quad D_6,\quad \Gamma,\quad A_4.}$$

其中两个交换群不同构，因为前者有 12 阶元素，后者没有。三个非交换群中，A_4 的 Sylow 3-子群不正规，而另外两个群的 Sylow 3-子群正规；D_6 和 Γ 的 Sylow 2-子群又分别同构于 $\mathbb{Z}_2\times\mathbb{Z}_2$ 和 $\mathbb{Z}_4$，故也不同构。 □

12. 作为所学知识的一个应用，本习题证明在同构意义下 56 阶群共有 13 个。

(1) 证明同构意义下，56 阶交换群共有 3 个；

(2) 证明每个 56 阶群或者有一个正规的 Sylow 2-子群，或者有一个正规的 Sylow 7-子群；

(3) 对每一个 8 阶群 P，构造（在同构意义下）所有的满足以下条件的 56 阶非交换群：

(i) 所有 Sylow 2-子群同构于 P；

(ii) Sylow 7-子群为正规子群；

(4) 证明：若一个 56 阶群中的 Sylow 7-子群不是正规子群，则其 Sylow 2-子群同构于 $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$；

(5) 证明在同构意义下，Sylow 7-子群不是正规子群的 56 阶群只有一个。

解 以下分类均在同构意义下进行，以 D_4 表示 8 阶二面体群，Q 表示四元数群。

(1) 由 $56=2^3\cdot 7$ 及有限交换群结构定理，56 阶交换群是一个 8 阶交换群与 $\mathbb{Z}_7$ 的直积。8 阶交换群有 $\mathbb{Z}_8$、$\mathbb{Z}_4\times\mathbb{Z}_2$、$\mathbb{Z}_2^3$ 三种，故恰有

$$\boxed{\mathbb{Z}_{56},\qquad \mathbb{Z}_{28}\times\mathbb{Z}_2,\qquad \mathbb{Z}_{14}\times\mathbb{Z}_2\times\mathbb{Z}_2.}$$

它们的初等因子组不同，所以两两不同构。

(2) 设 $|G|=56$，Sylow 7-子群的个数为 n_7。由 Sylow 定理，$n_7\mid 8$ 且 $n_7\equiv 1\pmod 7$，故 $n_7=1$ 或 8。

若 $n_7=1$，则 Sylow 7-子群正规。若 $n_7=8$，由于不同的 7 阶子群除单位元外互不相交，它们共含有 $8(7-1)=48$ 个 7 阶元素。

任一 Sylow 2-子群有 8 个元素，其中元素的阶均为 2 的幂，故不含上述 48 个元素。因此每个 Sylow 2-子群都恰好等于剩下的 $56-48=8$ 个元素组成的集合。于是 Sylow 2-子群唯一，因而正规。

(3) **先把问题化为作用的分类。**

设 Sylow 7-子群 $N=\langle z\rangle \trianglelefteq G$，取一个 Sylow 2-子群 P。由 $N\cap P=\{e\}$ 且 $|NP|=56$，有 $G=NP\cong N\rtimes_\theta P$。

因为 $|\operatorname{Aut}(N)|=6$，而 $|\theta(P)|=[P:\ker\theta]$ 整除 8，同时又整除 6，故 $|\theta(P)|=1$ 或 2。N 的唯一 2 阶自同构是反演 $z\mapsto z^{-1}$：事实上，若 $z\mapsto z^a$ 的平方为恒等自同构，则 $a^2\equiv 1\pmod 7$，故 $a\equiv\pm1\pmod 7$。

因此每个作用都由一个同态 $\chi:P\to\mathbb{Z}_2$ 决定，其中 $\theta(u)(z)=z^{(-1)^{\chi(u)}}$。记相应的半直积为 $\Gamma(P,\chi)$，其乘法明确为

$$(z^i,u)(z^j,v)=\big(z^{\,i+(-1)^{\chi(u)}j},uv\big).$$

每个这样的构造都有 56 个元素，且第一因子是正规的 Sylow 7-子群。

若 $\beta\in\operatorname{Aut}(P)$ 且 $\chi'\circ\beta=\chi$，则由上述乘法，$(z^i,u)\mapsto(z^i,\beta(u))$ 是 $\Gamma(P,\chi)\to\Gamma(P,\chi')$ 的同构。因此可通过更换 P 的生成元，合并等价的作用。对于非零同态 χ，它在核上取 0、在其余元素上取 1，故由其核唯一确定。

列出所有 8 阶群。交换的情形为 $\mathbb{Z}_8$、$\mathbb{Z}_4\times\mathbb{Z}_2$、$\mathbb{Z}_2^3$。若 P 非交换，则它不能含有 8 阶元素，也不能所有元素都满足 $x^2=e$，否则由 $xy=(xy)^{-1}=y^{-1}x^{-1}=yx$ 可知它交换。因此存在 4 阶元素 u。

取 $v\notin\langle u\rangle$。由于 $\langle u\rangle$ 的指数为 2，它正规，且 $P=\langle u,v\rangle$、$v^2\in\langle u\rangle$。共轭不能使 u 不变，否则 u,v 可交换，故 $vuv^{-1}=u^{-1}$。写 $v^2=u^j$，由于 v 与自身的平方可交换，得 $u^j=u^{-j}$，所以 $j\equiv 0$ 或 $2\pmod 4$。这两种情形分别给出 D_4 和 Q。

因此所有 8 阶群恰为 $\mathbb{Z}_8$、$\mathbb{Z}_4\times\mathbb{Z}_2$、$\mathbb{Z}_2^3$、$D_4$、$Q$。其中 D_4 有 5 个 2 阶元素，Q 只有 1 个，故二者不同构。下面逐一确定 χ。

$P=\mathbb{Z}_8=\langle u\rangle$。只有一个非零同态，即 $\chi(u)=1$。零同态给出交换群，故这里有 1 个非交换群。

$P=\mathbb{Z}_4\times\mathbb{Z}_2=\langle u\rangle\times\langle v\rangle$。非零同态由 $(\chi(u),\chi(v))=(1,0),(0,1),(1,1)$ 给出。它们的核分别为 $\langle u^2,v\rangle\cong\mathbb{Z}_2^2$、$\langle u\rangle\cong\mathbb{Z}_4$、$\langle uv\rangle\cong\mathbb{Z}_4$。自同构 $u\mapsto uv,\ v\mapsto v$ 交换后两个核，故后两个作用等价。因而可取 $(0,1)$、$(1,0)$ 为代表，得到 2 个非交换群。

$P=\mathbb{Z}_2^3$。将 P 看成 $\mathbb{Z}_2$ 上的三维向量空间。任一非零 χ 的核为二维子空间，取其一组基 v,w，再取 u 使 $\chi(u)=1$，便有 $(\chi(u),\chi(v),\chi(w))=(1,0,0)$。因此所有非零作用等价，得到 1 个非交换群。

$P=D_4=\langle u,v\mid u^4=v^2=e,\ vuv^{-1}=u^{-1}\rangle$。三个非零同态的取值仍为 $(0,1),(1,0),(1,1)$，对应的核分别为 $\langle u\rangle\cong\mathbb{Z}_4$、$\langle u^2,v\rangle\cong\mathbb{Z}_2^2$、$\langle u^2,uv\rangle\cong\mathbb{Z}_2^2$。自同构 $u\mapsto u,\ v\mapsto uv$ 交换后两个核，故可取 $(0,1)$、$(1,0)$ 为非零作用的代表。零作用给出 $\mathbb{Z}_7\times D_4$，它也非交换，因此这里共有 3 个非交换群。

$P=Q=\langle i,j\rangle$。任一非零同态的核为 Q 的一个 4 阶子群，即 $\langle i\rangle$、$\langle j\rangle$、$\langle k\rangle$ 之一。循环置换 i,j,k 给出 Q 的自同构，故这三个核彼此等价。因此非零作用只有一种，可取 $(\chi(i),\chi(j))=(1,0)$。加上零作用给出的 $\mathbb{Z}_7\times Q$，这里共有 2 个非交换群。

因此，满足本问条件的全部非交换群可由下表构造，表中每个取值代表一个群 $\Gamma(P,\chi)$：

P	χ 在上述生成元上的取值	个数
$\mathbb{Z}_8$	1	1
$\mathbb{Z}_4\times\mathbb{Z}_2$	$(0,1),\ (1,0)$	2
$\mathbb{Z}_2^3$	$(1,0,0)$	1
D_4	$(0,0),\ (0,1),\ (1,0)$	3
Q	$(0,0),\ (1,0)$	2

最后验证这些代表互不同构。不同的 P 给出不同的 Sylow 2-子群同构类型，因此对应的群不同构。对于固定的 P，零作用使 $N\leqslant Z(G)$，非零作用则不满足此性质，故两者不同构。

还需区分 $\mathbb{Z}_4\times\mathbb{Z}_2$ 和 D_4 情形中的两种非零作用。由于 N 是唯一的 Sylow 7-子群，同构必将它映到对应的 Sylow 7-子群，并将其中心化子映到对应的中心化子。而由乘法定义，

$$C_{\Gamma(P,\chi)}(N)=N\times\ker\chi.$$

两种作用的核分别同构于 $\mathbb{Z}_4$ 和 $\mathbb{Z}_2^2$，所以对应中心化子的 Sylow 2-子群不同构，从而原群也不同构。

因此本问恰有 $1+2+1+3+2=9$ 个非交换群。连同 (1) 中的 3 个交换群，Sylow 7-子群正规的情形共有 12 个群。

(4) 设 G 的 Sylow 7-子群不正规。由 (2)，其 Sylow 2-子群 P 唯一，故 $P \trianglelefteq G$。取 Sylow 7-子群 $R=\langle c\rangle$，则 $G=PR\cong P\rtimes R$。

令 $T: P\to P$ 为共轭自同构 $T(x)=cxc^{-1}$，则 $T^7=\mathrm{id}_P$。若 $T=\mathrm{id}_P$，则 R 与 P 逐元素可交换，因而 R 在 P 和 R 的共轭下都不变，从 $G=PR$ 得 $R\trianglelefteq G$，矛盾。因此 $T\neq\mathrm{id}_P$。

把 T 看成 P 上的置换。由于 $T^7=\mathrm{id}_P$，每个轨道的大小为 1 或 7。它固定单位元，又不是恒等置换，而 $|P|=8$，所以其余 7 个非单位元恰构成一个轨道。自同构保持元素的阶，故这 7 个元素的阶相同。

由 Cauchy 定理，P 中存在 2 阶元素，所以每个非单位元都为 2 阶。于是任取 $x,y\in P$，有 $xy=(xy)^{-1}=y^{-1}x^{-1}=yx$，故 P 交换。由有限交换群结构定理，

$$P\cong\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2.$$

(5) 记 $V=\mathbb{Z}_2^3$，将其看成三维向量空间。由 (4)，所求群必为 $V\rtimes_T\mathbb{Z}_7$，其中 $\mathbb{Z}_7$ 的生成元作用为一个 7 阶线性自同构 T。

先构造一个这样的群。在 $\mathbb{Z}_2$ 上取

$$T_0=\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}.$$

直接计算有 $T_0^3=T_0+I$。由于运算在特征为 2 的域上进行，

$$T_0^7=T_0(T_0^3)^2=T_0(T_0+I)^2=T_0^3+T_0=I.$$

又 $T_0\neq I$，故 T_0 可逆且其阶为 7。因此 $G_0=V\rtimes_{T_0}\mathbb{Z}_7$ 是一个 56 阶群。

其中的 Sylow 7-子群不正规。否则它与正规子群 V 的交为单位元，两个正规子群之间的元素应逐元素可交换，迫使作用 T_0 为恒等映射，矛盾。

下面证明唯一性。由向量空间的加法群自同构就是线性自同构，有 $\mathrm{Aut}(V)\cong\mathrm{GL}_3(\mathbb{Z}_2)$，并且

$$|\,\mathrm{GL}_3(\mathbb{Z}_2)|=(2^3-1)(2^3-2)(2^3-2^2)=7\cdot6\cdot4=168.$$

所以任一 7 阶自同构 T 生成的 $\langle T\rangle$ 都是 $\mathrm{GL}_3(\mathbb{Z}_2)$ 的 Sylow 7-子群。由 Sylow 子群的共轭性，存在 $S\in\mathrm{GL}_3(\mathbb{Z}_2)$，使 $S\langle T\rangle S^{-1}=\langle T_0\rangle$。因此存在 $t\in\{1,\dots,6\}$，使 $STS^{-1}=T_0^t$。

定义

$$F: V\rtimes_T\mathbb{Z}_7\longrightarrow V\rtimes_{T_0}\mathbb{Z}_7,\qquad F(x,\overline{j})=(Sx,\overline{tj}).$$

因为 S 可逆且 t 与 7 互素，F 为双射。又 $ST^j=T_0^{tj}S$，故

$$\begin{aligned}F\big((x,\overline{j})(y,\overline{k})\big)&=F(x+T^jy,\overline{j+k})\\&=(Sx+T_0^{tj}Sy,\overline{t(j+k)})\\&=F(x,\overline{j})F(y,\overline{k}).\end{aligned}$$

因此 F 为同构，证明这一情形只有 G_0 一种同构类型。

综上，56 阶群在同构意义下共有 $3+9+1=13$ 个，其中交换群有 3 个，非交换群有 10 个。 □

3.4 可解群

1. 设 G 为群，$N \trianglelefteq G$ 且 $N \cap G^{(1)} = \{e\}$，证明 $N \leqslant Z(G)$。

解 任取 $g \in G$、$a \in N$，考虑换位子 $[g,a] = gag^{-1}a^{-1}$。由于 $N \trianglelefteq G$，有 $gag^{-1} \in N$；又 $a^{-1} \in N$，故 $[g,a] \in N$。

另一方面，$G^{(1)}$ 由 G 的所有换位子生成，故 $[g,a] \in G^{(1)}$。于是 $[g,a] \in N \cap G^{(1)} = \{e\}$，从而 $gag^{-1}a^{-1} = e$，即 $ga = ag$。

因为 $g \in G$、$a \in N$ 任意，所以 N 中每个元素都与 G 中所有元素交换，即 $N \leqslant Z(G)$。 □

2. 设 H 和 K 都是群 G 的正规子群，且 G/H 与 G/K 都可解，证明群 $G/(H \cap K)$ 也可解。

解 记 $L = H \cap K$，则 $L \trianglelefteq G$。设自然满同态分别为 $\pi_H : G \to G/H$、$\pi_K : G \to G/K$。

满同态把导群映到目标群的导群：因为 $f([x,y]) = [f(x), f(y)]$，而目标群中的每个元素都有原像，所以目标群中的每个换位子也都是原群中某个换位子的像。逐次应用这一事实，对任意 $i \geqslant 0$，有

$$\pi_H(G^{(i)}) = (G/H)^{(i)}, \qquad \pi_K(G^{(i)}) = (G/K)^{(i)},$$

其中约定 $G^{(0)} = G$。

由于 G/H 和 G/K 都可解，可取足够大的整数 t，使 $(G/H)^{(t)} = \{H\}$ 且 $(G/K)^{(t)} = \{K\}$。于是 $G^{(t)} \leqslant \ker \pi_H = H$，同时 $G^{(t)} \leqslant \ker \pi_K = K$，故 $G^{(t)} \leqslant H \cap K = L$。

再考虑自然满同态 $\pi_L : G \to G/L$，同理有

$$(G/L)^{(t)} = \pi_L(G^{(t)}) = \{L\}.$$

因此 $G/L = G/(H \cap K)$ 可解。 □

3. 设 p 为素数，群 G 的阶为 p^3，证明：若 G 为非交换群，则 $G^{(1)} = Z(G)$。

解 由有限 p-群的类方程，非中心共轭类的大小均为 p 的倍数，所以 $|Z(G)| \equiv |G| \equiv 0 \pmod p$。又 G 非交换，故 $Z(G) \neq G$，于是 $|Z(G)| = p$ 或 p^2。

若 $|Z(G)| = p^2$，则 $G/Z(G)$ 的阶为 p，因而是循环群。取 $aZ(G)$ 为其生成元，则任意 $x, y \in G$ 均可写成 $x = a^i z_1$、$y = a^j z_2$，其中 $z_1, z_2 \in Z(G)$。于是

$$xy = a^i z_1 a^j z_2 = a^{i+j} z_1 z_2 = a^{i+j} z_2 z_1 = yx,$$

这与 G 非交换矛盾。因此 $|Z(G)| = p$。

此时 $G/Z(G)$ 的阶为 p^2，由素数平方阶群必交换，知 $G/Z(G)$ 为交换群。所以对任意 $x, y \in G$，有 $[x,y]Z(G) = Z(G)$，即 $[x,y] \in Z(G)$。因此 $G^{(1)} \leqslant Z(G)$。

又 G 非交换，故至少有一个换位子不是单位元，从而 $G^{(1)} \neq \{e\}$。由于 $|Z(G)| = p$，其非平凡子群只能是自身，故 $G^{(1)} = Z(G)$。 □

4. 设 G 为 p-群，$N \trianglelefteq G$ 且 $|N| = p$，证明 $N \leqslant Z(G)$。

解 由于 $|N| = p$，N 为循环群。它的一个自同构由生成元的像唯一决定，而生成元可映到任意非单位元，所以 $|\operatorname{Aut}(N)| = p - 1$。

任取 $g \in G$。由 $N \trianglelefteq G$，共轭映射 $\alpha_g : N \to N$，$\alpha_g(x) = gxg^{-1}$ 是 N 的自同构。

因为 G 为 p-群，可设 $o(g)=p^s$，其中 $s\geqslant 0$。对任意 $x\in N$，有

$$\alpha_g^{p^s}(x)=g^{p^s}xg^{-p^s}=x,$$

故 $o(\alpha_g)\mid p^s$。另一方面，$\alpha_g\in \mathrm{Aut}(N)$，由 Lagrange 定理，$o(\alpha_g)\mid p-1$。由于 $\gcd(p^s,p-1)=1$，只能有 $o(\alpha_g)=1$，即 $\alpha_g=\mathrm{id}_N$。

因此对任意 $g\in G$、$x\in N$，都有 $gxg^{-1}=x$，即 $gx=xg$。故 $N\leqslant Z(G)$。 □

5. 设 G 为群，若 $G^{(1)}/G^{(2)}$ 和 $G^{(2)}/G^{(3)}$ 都是循环群，证明 $G^{(2)}=G^{(3)}$。

解 先说明循环群的自同构群是交换群。设 $C=\langle c\rangle$，任取 $\alpha,\beta\in\mathrm{Aut}(C)$，写 $\alpha(c)=c^r$、$\beta(c)=c^s$，则 $\alpha\beta(c)=c^{rs}=c^{sr}=\beta\alpha(c)$。由于两个同态在生成元上相同，故 $\alpha\beta=\beta\alpha$。

令 $D=G^{(2)}/G^{(3)}$。共轭将换位子映为换位子，逐次应用可知 $G^{(2)},G^{(3)}$ 都在 G 的共轭下保持不变。因此共轭给出同态

$$\theta: G\longrightarrow \mathrm{Aut}(D),\qquad \theta(g)(uG^{(3)})=gug^{-1}G^{(3)}.$$

由题设，D 为循环群，所以 $\mathrm{Aut}(D)$ 交换。于是对任意 $x,y\in G$，有

$$\theta([x,y])=\theta(x)\theta(y)\theta(x)^{-1}\theta(y)^{-1}=\mathrm{id}_D\,.$$

因此 $G^{(1)}\leqslant \ker\theta$。这说明对任意 $h\in G^{(1)}$、$u\in G^{(2)}$，都有 $huh^{-1}u^{-1}\in G^{(3)}$。

现考虑 $E=G^{(1)}/G^{(3)}$，并用上横线表示模 $G^{(3)}$ 的陪集。上面的结论恰好说明 $D\leqslant Z(E)$，即 $G^{(2)}$ 中元素的像都位于 E 的中心。

又因为 $G^{(1)}/G^{(2)}$ 为循环群，取 $aG^{(2)}$ 为其生成元。任取 $x,y\in G^{(1)}$，可写成 $x=a^iu$、$y=a^jv$，其中 $i,j\in\mathbb{Z}$、$u,v\in G^{(2)}$。由于 $\overline{u},\overline{v}\in Z(E)$，有

$$\overline{x}\,\overline{y}=\overline{a}^{\,i+j}\overline{u}\,\overline{v}=\overline{a}^{\,i+j}\overline{v}\,\overline{u}=\overline{y}\,\overline{x}.$$

所以 E 为交换群，即对任意 $x,y\in G^{(1)}$，都有 $[x,y]\in G^{(3)}$。而这些换位子生成 $G^{(2)}$，故 $G^{(2)}\leqslant G^{(3)}$。结合导列本身满足 $G^{(3)}\leqslant G^{(2)}$，得到 $G^{(2)}=G^{(3)}$。 □

6. 证明不存在群 G 使得 $G^{(1)}\cong S_3$，也不存在群 G 使得 $G^{(1)}\cong S_4$。

解 先确定 S_3,S_4 及 A_4 的导群。

对 $n=3,4$，由符号同态可知每个换位子都是偶置换，所以 $S_n^{(1)}\leqslant A_n$。另一方面，

$$[(12),(23)]=(12)(23)(12)(23)=(132).$$

由于导群为正规子群，且所有 3-轮换在 S_n 中彼此共轭，所以 $S_n^{(1)}$ 包含所有 3-轮换。又 3-轮换生成 A_n，故 $S_3^{(1)}=A_3$、$S_4^{(1)}=A_4$。

再令 $V_4=\{e,(12)(34),(13)(24),(14)(23)\}$。双对换经共轭后仍为双对换，故 $V_4\trianglelefteq A_4$。又 A_4/V_4 的阶为 3，所以它交换，从而 $A_4^{(1)}\leqslant V_4$。另一方面，

$$[(123),(124)]=(12)(34)\in A_4^{(1)}.$$

用 (123) 及其平方共轭这个元素，分别得到 (14)(23) 和 (13)(24)，所以 V_4 的全部元素都属于 $A_4^{(1)}$。因此 $A_4^{(1)}=V_4$。

若存在 G 使 $G^{(1)}\cong S_3$，由于同构把导群映到导群，有 $G^{(2)}\cong A_3$、$G^{(3)}=\{e\}$。因此

$$G^{(1)}/G^{(2)}\cong\mathbb{Z}_2,\qquad G^{(2)}/G^{(3)}\cong\mathbb{Z}_3.$$

这两个商群均为循环群，由第 5 题，应有 $G^{(2)}=G^{(3)}$，但它们的阶分别为 3 和 1，矛盾。

若存在 G 使 $G^{(1)} \cong S_4$，同理有 $G^{(2)} \cong A_4$、$G^{(3)} \cong V_4$。所以 $G^{(1)}/G^{(2)}$ 的阶为 $24/12 = 2$，$G^{(2)}/G^{(3)}$ 的阶为 $12/4 = 3$，两者也都是循环群。再次由第 5 题，得到 $G^{(2)} = G^{(3)}$，与它们的阶分别为 12 和 4 矛盾。

因此这两种群 G 都不存在。 □

7. 设 G 为群，$H \leqslant G$ 且 $G^{(1)} \subseteq H$，证明 $H \trianglelefteq G$。

解 任取 $g \in G$、$h \in H$，有 $[g,h] = ghg^{-1}h^{-1} \in G^{(1)} \subseteq H$。又 $h \in H$，故 $ghg^{-1} = [g,h]h \in H$。因此 $gHg^{-1} \subseteq H$。

将 g 换为 g^{-1}，得到 $g^{-1}Hg \subseteq H$，两边再被 g 共轭，得 $H \subseteq gHg^{-1}$。因此 $gHg^{-1} = H$。

由于 $g \in G$ 任意，故 $H \trianglelefteq G$。 □

8. 群 G 的子群 H 称为特征子群，若对任意 $\alpha \in \mathrm{Aut}(G)$ 有 $\alpha(H) = H$。如果 H 是 G 的特征子群，则记为 $H \sqsubset G$。

(1) 证明：若 $H \sqsubset G$，则有 $H \trianglelefteq G$；

(2) 证明群 G 的中心 $Z(G)$ 和导群 $G^{(1)}$ 为 G 的特征子群；

(3) 设 G 的子群 H 和 K 满足 $H \sqsubset K$、$K \sqsubset G$，证明 $H \sqsubset G$；

(4) 设 G 的子群 H 和 K 满足 $H \sqsubset K$、$K \trianglelefteq G$，证明 $H \trianglelefteq G$。

解

(1) 任取 $g \in G$，共轭映射 $\alpha_g(x) = gxg^{-1}$ 是 G 的自同构。由于 $H \sqsubset G$，有 $gHg^{-1} = \alpha_g(H) = H$。因此 $H \trianglelefteq G$。

(2) 任取 $\alpha \in \mathrm{Aut}(G)$。

先考察中心。任取 $z \in Z(G)$、$x \in G$。由 α 为满射，存在 $y \in G$ 使 $x = \alpha(y)$，于是

$$\alpha(z)x = \alpha(z)\alpha(y) = \alpha(zy) = \alpha(yz) = x\alpha(z).$$

故 $\alpha(z) \in Z(G)$，从而 $\alpha(Z(G)) \subseteq Z(G)$。对 α^{-1} 同样有 $\alpha^{-1}(Z(G)) \subseteq Z(G)$，再作用 α 得 $Z(G) \subseteq \alpha(Z(G))$。因此 $\alpha(Z(G)) = Z(G)$，即 $Z(G) \sqsubset G$。

再考察导群。对任意 $x, y \in G$，有

$$\alpha([x,y]) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1} = [\alpha(x), \alpha(y)] \in G^{(1)}.$$

由于 $G^{(1)}$ 由换位子生成，故 $\alpha(G^{(1)}) \subseteq G^{(1)}$。对 α^{-1} 应用同一结论，可得反向包含。因此 $\alpha(G^{(1)}) = G^{(1)}$，即 $G^{(1)} \sqsubset G$。

(3) 任取 $\alpha \in \mathrm{Aut}(G)$。由 $K \sqsubset G$，有 $\alpha(K) = K$，所以限制映射 $\alpha|_K : K \to K$ 是 K 的自同构。再由 $H \sqsubset K$，有 $\alpha(H) = (\alpha|_K)(H) = H$。因此每个 G 的自同构都保持 H 不变，故 $H \sqsubset G$。

(4) 任取 $g \in G$。由于 $K \trianglelefteq G$，有 $gKg^{-1} = K$，故共轭映射 $x \mapsto gxg^{-1}$ 限制在 K 上是 K 的自同构。再由 $H \sqsubset K$，该自同构保持 H 不变，故 $gHg^{-1} = H$。因此 $H \trianglelefteq G$。

□

9. 证明对任意正整数 n，有 $G^{(n)} \trianglelefteq G$。

解 先归纳证明：对任意正整数 n，$G^{(n)}$ 都是 G 的特征子群。

当 $n=1$ 时，由第 8 题，$G^{(1)}$ 是 G 的特征子群。假设 $G^{(n)}$ 是 G 的特征子群，将同一结论用于群 $G^{(n)}$，可知 $G^{(n+1)}=(G^{(n)})^{(1)}$ 是 $G^{(n)}$ 的特征子群。再由特征子群关系的传递性，$G^{(n+1)}$ 也是 G 的特征子群。归纳完成。

任取 $g\in G$，共轭映射 $x\mapsto gxg^{-1}$ 是 G 的自同构，因此保持 $G^{(n)}$ 不变，即 $gG^{(n)}g^{-1}=G^{(n)}$。所以对任意正整数 n，都有 $G^{(n)}\trianglelefteq G$。 □

10. 设 H,K 都是可解群，证明 H,K 的半直积 $H\rtimes_\varphi K$ 也是可解群。

解 记 $G=H\rtimes_\varphi K$，并令 $H_0=H\times\{e_K\}$。考虑投影 $\pi:G\to K$，$\pi(h,k)=k$。由半直积的乘法，π 是满同态，且 $\ker\pi=H_0$，所以 $H_0\trianglelefteq G$，并且 $H_0\cong H$。

由 H,K 可解，可取正整数 r,s，使 $H^{(r)}=\{e_H\}$、$K^{(s)}=\{e_K\}$。

由于同态保持换位子，且满同态使目标群的每个换位子都有原像，故 $\pi(G^{(1)})=K^{(1)}$。逐次应用这一事实，得到 $\pi(G^{(s)})=K^{(s)}=\{e_K\}$，因此 $G^{(s)}\leqslant\ker\pi=H_0$。

若两个群满足 $A\leqslant B$，则 A 中的换位子也是 B 中的换位子，所以 $A^{(1)}\leqslant B^{(1)}$；逐次取导群，同样有 $A^{(i)}\leqslant B^{(i)}$。将此用于 $G^{(s)}\leqslant H_0$，并利用 $H_0\cong H$，得到

$$G^{(r+s)}=(G^{(s)})^{(r)}\leqslant H_0^{(r)}=\{e_G\}.$$

因此 $G^{(r+s)}=\{e_G\}$，故 $H\rtimes_\varphi K$ 为可解群。 □

11. 设 G 是群，$N\trianglelefteq G$ 且 $N\neq G$。如果在 N 和 G 之间没有其他真正规子群，即对任意满足 $N\leqslant H\leqslant G$ 的正规子群 $H\trianglelefteq G$，都有 $H=N$ 或 $H=G$，则称 N 是 G 的极大正规子群。

(1) 设 $N\trianglelefteq G$，证明 N 是 G 的极大正规子群当且仅当 G/N 是单群；

(2) 设 G 是有限群，$G\neq\{e\}$，证明 G 有极大正规子群；

(3) 设 G 是有限群，证明 G 可解当且仅当存在 G 的子群列

$$G=G_0\trianglerighteq G_1\trianglerighteq\cdots\trianglerighteq G_s=\{e\},$$

使得对任意 $0\leqslant i\leqslant s-1$，$G_i/G_{i+1}$ 都是素数阶循环群。

解

(1) 由对应定理，G 中包含 N 的正规子群与 G/N 的正规子群通过 $H\mapsto H/N$ 一一对应。其中，N 对应单位元子群 $\{N\}$，G 对应整个商群 G/N。

因此，N 是 G 的极大正规子群，当且仅当 $N\neq G$，且 G/N 的正规子群只有 $\{N\}$ 和 G/N。这恰好表示 G/N 非平凡且没有非平凡真正规子群，即 G/N 是单群。

(2) 因为 $G\neq\{e\}$，所以 $\{e\}$ 是 G 的真正规子群，故真正规子群的集合非空。又 G 有限，所以可以从中选取一个阶最大的子群，记为 N。

若 $H\trianglelefteq G$ 且 $N\leqslant H<G$，则由 N 的选取，有 $|H|\leqslant|N|$；而 $N\leqslant H$ 又给出 $|N|\leqslant|H|$，故 $|N|=|H|$，从而 $H=N$。

因此，包含 N 的正规子群只能是 N 或 G，即 N 是 G 的极大正规子群。

(3) **必要性**。设 G 为有限可解群，对 $|G|$ 作归纳。若 $G=\{e\}$，取 $s=0$ 即可。以下设 $G\neq\{e\}$，并假设结论对阶小于 $|G|$ 的有限可解群成立。

由 (2)，取 G 的一个极大正规子群 N。由于 $N^{(j)} \leqslant G^{(j)}$，所以 N 可解。又自然满同态 $\pi : G \to G/N$ 满足 $\pi(G^{(j)}) = (G/N)^{(j)}$，故 G/N 也可解。由 (1)，G/N 为非平凡单群。

下面说明，非平凡的有限可解单群一定是素数阶循环群。记 $S = G/N$。由于 $S^{(1)} \trianglelefteq S$，由单群性，只能有 $S^{(1)} = \{e_S\}$ 或 $S^{(1)} = S$。若 $S^{(1)} = S$，则逐次取导群得到 $S^{(j)} = S \neq \{e_S\}$，与 S 可解矛盾。因此 $S^{(1)} = \{e_S\}$，即 S 交换。

任取 $a \in S \setminus \{e_S\}$，由于 S 交换，$\langle a \rangle$ 是非平凡正规子群，故由单群性有 $S = \langle a \rangle$。若 $|S|$ 为合数，则循环群 S 有非平凡真子群，该子群又正规，与单群性矛盾。因此 $|S|$ 为素数，即 G/N 是素数阶循环群。

由于 $N < G$，有 $|N| < |G|$，且 N 可解，由归纳假设，N 存在一条相邻商群均为素数阶循环群的子群列。将 G 添在这条子群列的最前面，再利用 $N \trianglelefteq G$ 以及 G/N 为素数阶循环群，便得到所求子群列。

充分性。设存在题述子群列。由于 G_i/G_{i+1} 为交换群，G_i 中的每个换位子都属于 G_{i+1}，所以 $G_i^{(1)} \leqslant G_{i+1}$。约定 $G^{(0)} = G$，归纳证明 $G^{(i)} \leqslant G_i$。当 $i = 0$ 时成立；若 $G^{(i)} \leqslant G_i$，则

$$G^{(i+1)} = (G^{(i)})^{(1)} \leqslant G_i^{(1)} \leqslant G_{i+1}.$$

因此 $G^{(s)} \leqslant G_s = \{e\}$，即 $G^{(s)} = \{e\}$，所以 G 可解。

□

3.5 Jordan-Holder 定理

1. 设 F 为域，$G=\mathrm{Aff}(F)$ 为域 F 上的仿射群，令

$$G_1=\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\,\middle|\, b\in F\right\}.$$

证明 $G_1\trianglelefteq G$，并求出次正规群列 $G\trianglerighteq G_1\trianglerighteq\{I\}$ 的因子群组。

解 记 $T(a,b)=\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}$，则 $G=\{T(a,b)\mid a\in F^\times,\ b\in F\}$，且

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

特别地，$T(1,b)T(1,d)=T(1,b+d)$，$T(1,b)^{-1}=T(1,-b)$，故 $G_1\leqslant G$。

任取 $T(a,b)\in G$、$T(1,t)\in G_1$，有

$$T(a,b)T(1,t)T(a,b)^{-1}=T(1,at).$$

由于 $a\neq 0$，当 t 遍历 F 时，at 也遍历 F，所以 $T(a,b)G_1T(a,b)^{-1}=G_1$。因此 $G_1\trianglelefteq G$。

又 $T(a,b)G_1=\{T(a,b+at)\mid t\in F\}$，所以两个这样的陪集相同，当且仅当它们的第一参数 a 相同。因此映射

$$G/G_1\longrightarrow F^\times,\qquad T(a,b)G_1\longmapsto a$$

是双射；由上述乘法公式，它保持乘法，故 $G/G_1\cong(F^\times,\cdot)$。

另一方面，$b\mapsto T(1,b)$ 是加法群 $(F,+)$ 到 G_1 的同构。因此该次正规群列的因子群组为

$$\boxed{\big((F^\times,\cdot),\ (F,+)\big).}$$

□

2. 设 G 为群，$H\leqslant G$，且

$$G=G_0\trianglerighteq G_1\trianglerighteq\cdots\trianglerighteq G_t=\{e\}$$

是 G 的一个次正规群列。对 $0\leqslant i\leqslant t$，令 $H_i=H\cap G_i$，证明

$$H=H_0\trianglerighteq H_1\trianglerighteq\cdots\trianglerighteq H_t=\{e\}$$

是 H 的次正规群列，且对任意 $0\leqslant i<t$，因子群 H_i/H_{i+1} 同构于 G_i/G_{i+1} 的子群；并由此证明可解群的子群也可解。

解 由定义，$H_0=H$、$H_t=\{e\}$。任取 $h\in H_i$、$x\in H_{i+1}$，由 $G_{i+1}\trianglelefteq G_i$，有 $hxh^{-1}\in G_{i+1}$；又 $h,x\in H$，故 $hxh^{-1}\in H$。因此 $hH_{i+1}h^{-1}\subseteq H_{i+1}$，将 h 换为 h^{-1} 可得反向包含，故 $H_{i+1}\trianglelefteq H_i$。

固定 i，定义

$$\varphi_i:H_i/H_{i+1}\longrightarrow G_i/G_{i+1},\qquad \varphi_i(hH_{i+1})=hG_{i+1}.$$

对任意 $h,k\in H_i$，由于 $k^{-1}h\in H$，有

$$\begin{aligned}hG_{i+1}=kG_{i+1}&\iff k^{-1}h\in H\cap G_{i+1}=H_{i+1}\\&\iff hH_{i+1}=kH_{i+1}.\end{aligned}$$

因此 φ_i 定义良好且为单射。由陪集乘法，它也是同态，故 H_i/H_{i+1} 同构于 G_i/G_{i+1} 的子群。

若 G 可解，可取上述次正规群列使各因子群 G_i/G_{i+1} 都交换。于是各 H_i/H_{i+1} 也交换，所以 H 有因子群均交换的有限次正规群列，故 H 可解。 □

3. 设 G 为群，$N \trianglelefteq G$，且

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_t = \{e\}$$

是 G 的一个次正规群列。对 $0 \leqslant i \leqslant t$，令 $N_i = NG_i/N$，证明

$$G/N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_t = \{N\}$$

是 G/N 的次正规群列，且对任意 $0 \leqslant i < t$，因子群 N_i/N_{i+1} 同构于 G_i/G_{i+1} 的商群；并由此证明可解群的商群也可解。

解 记自然满同态为 $\pi : G \to G/N$，则 $N_i = \pi(G_i)$，特别地 $N_0 = G/N$、$N_t = \{N\}$。由 $G_{i+1} \trianglelefteq G_i$，任取 $g \in G_i$，有

$$\pi(g)\pi(G_{i+1})\pi(g)^{-1} = \pi(gG_{i+1}g^{-1}) = \pi(G_{i+1}),$$

所以 $N_{i+1} \trianglelefteq N_i$，从而所得群列为次正规群列。

固定 i，定义

$$\psi_i : G_i/G_{i+1} \longrightarrow N_i/N_{i+1}, \qquad \psi_i(gG_{i+1}) = (gN)N_{i+1}.$$

若 $gG_{i+1} = hG_{i+1}$，则 $h^{-1}g \in G_{i+1}$，故 $\pi(h)^{-1}\pi(g) \in N_{i+1}$，所以两者有相同的像。因此 ψ_i 定义良好；由陪集乘法，它是同态，又由 $N_i = \pi(G_i)$ 可知它为满射。

它的核为

$$K_i = \ker \psi_i = \big(G_i \cap NG_{i+1}\big)/G_{i+1}.$$

两个元素在 ψ_i 下有相同的像，当且仅当它们属于 K_i 的同一个陪集。因此 ψ_i 诱导双射同态

$$(G_i/G_{i+1})/K_i \cong N_i/N_{i+1}.$$

故 N_i/N_{i+1} 同构于 G_i/G_{i+1} 的商群。

若 G 可解，可取上述群列的各因子群均交换。交换群的商群仍交换，所以各 N_i/N_{i+1} 都交换，从而 G/N 可解。 □

4. 设 F 为域，形如

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \qquad a, b, c \in F$$

的 3 阶上三角形矩阵称为域 F 上的 Heisenberg（海森伯）矩阵。令 $G = \mathrm{Heis}(F)$ 是所有这样的矩阵在矩阵乘法下构成的群，证明 G 的导群就是其中心 $Z(G)$，并且 G 是零幂群。

解 记题中矩阵为 $X(a, b, c)$。直接计算得

$$X(a, b, c)X(a', b', c') = X(a + a', b + b' + ac', c + c'),$$

且 $X(a, b, c)^{-1} = X(-a, ac - b, -c)$。以 $[x, y] = xyx^{-1}y^{-1}$ 表示换位子，进一步计算得到

$$[X(a, b, c), X(a', b', c')] = X(0, ac' - a'c, 0).$$

因此 $X(a, b, c)$ 位于中心，当且仅当对所有 $a', c' \in F$ 都有 $ac' - a'c = 0$。分别取 $(a', c') = (0, 1)$、$(1, 0)$，得到 $a = c = 0$；反之，$a = c = 0$ 时该条件成立。所以

$$Z(G) = \{X(0, b, 0) \mid b \in F\}.$$

由换位子公式，所有换位子都属于 $Z(G)$，故 $G^{(1)} \leqslant Z(G)$。另一方面，任取 $b \in F$，有

$$X(0, b, 0) = [X(b, 0, 0), X(0, 0, 1)] \in G^{(1)}.$$

因此 $Z(G)\leqslant G^{(1)}$，从而 $G^{(1)}=Z(G)$。

由 $[G,G]\leqslant Z(G)$ 且 $[G,Z(G)]=\{I\}$，群列 $G\trianglerighteq Z(G)\trianglerighteq\{I\}$ 是中心群列，故 G 为零幂群。又 $[X(1,0,0),X(0,0,1)]=X(0,1,0)\neq I$，所以它的零幂类恰为 2。 □

5. 证明群 A_4、S_4 和 S_3 都是可解群但不是零幂群。

解 令 $V_4=\{e,(12)(34),(13)(24),(14)(23)\}$。由已求得的导群，$S_4^{(1)}=A_4$、$A_4^{(1)}=V_4$，而 V_4 交换；另有 $S_3^{(1)}=A_3$，且 A_3 交换。因此这三个群的导列都在有限步后达到单位元群，故它们都可解。

下面考察它们的中心。由 $Z(S_n)=\{e\}$（$n\geqslant 3$），知 $Z(S_3)=Z(S_4)=\{e\}$。对于 A_4，与 (123) 交换的 S_4 中置换必须固定 4，并且在 $\{1,2,3\}$ 上是 (123) 的幂，故 $C_{S_4}((123))=\langle(123)\rangle$。同理，$C_{S_4}((124))=\langle(124)\rangle$。于是

$$Z(A_4)\leqslant\langle(123)\rangle\cap\langle(124)\rangle=\{e\}.$$

所以这三个非平凡群的中心都平凡。

而非平凡零幂群的中心必非平凡：在一条中心群列中，最靠近单位元群的非平凡项与整个群的换位子都为单位元，故该项包含于中心。因此 A_4,S_4,S_3 都不是零幂群。 □

6. 证明零幂群的子群和商群也是零幂群。反之，设 N 是群 G 的正规子群，若 N 和 G/N 都是零幂群，G 是否为零幂群？给出证明或反例。

解 设 G 为零幂群，取其一条中心群列

$$G=C_0\trianglerighteq C_1\trianglerighteq\cdots\trianglerighteq C_c=\{e\},\qquad [G,C_i]\leqslant C_{i+1}\quad(0\leqslant i<c).$$

这里各 C_i 都是 G 的正规子群。

若 $H\leqslant G$，令 $H_i=H\cap C_i$，则 $H_0=H$、$H_c=\{e\}$，且各 H_i 都是 H 的正规子群。对任意 $h\in H$、$x\in H_i$，有 $[h,x]\in H$ 且 $[h,x]\in C_{i+1}$，所以 $[H,H_i]\leqslant H_{i+1}$。因此 $H=H_0\trianglerighteq\cdots\trianglerighteq H_c=\{e\}$ 为中心群列，故 H 零幂。

若 $N\trianglelefteq G$，记自然满同态为 $\pi:G\to G/N$，令 $\overline{C}_i=\pi(C_i)=NC_i/N$。各 $\overline{C}_i$ 都正规，且

$$[G/N,\overline{C}_i]=\pi([G,C_i])\leqslant\pi(C_{i+1})=\overline{C}_{i+1}.$$

因此 $G/N=\overline{C}_0\trianglerighteq\cdots\trianglerighteq\overline{C}_c=\{N\}$ 是中心群列，故 G/N 零幂。

反向结论不成立。取 $G=S_3$、$N=A_3$，则 $N\cong\mathbb{Z}_3$、$G/N\cong\mathbb{Z}_2$，二者都是交换群，因而零幂；但由第 5 题，S_3 不是零幂群。 □

7. 群 G 的无重复正规群列称为主群列，若它的任意两项之间都不能再插入其他的 G 的正规子群。证明有限群一定有主群列，并且也有类似的 Jordan–Hölder 定理。

解 主群列的各项都要求是整个 G 的正规子群。由于有限群只有有限多个子群，在所有无重复正规群列中选取一条长度最大的，便不能再插入其他正规子群，因此它是主群列。

类似的 Jordan–Hölder 定理为：**有限群的任意两条主群列长度相同，且其因子群经过适当重排后逐个同构。**下面对 $|G|$ 作归纳证明。

当 $G=\{e\}$ 时结论成立。现设 $G\neq\{e\}$，取两条主群列，并从单位元群向上排列。记它们的第一个非平凡项分别为 A,B，则 A,B 都是 G 的极小非平凡正规子群。

若 $A=B$，则这两条群列在 A 以上的部分投影到 G/A 后，都是 G/A 的主群列。由 $|G/A|<|G|$ 及归纳假设，两者长度和因子群组相同；再在最前面补上共同的因子 A，即得结论。

以下设 $A\neq B$。因为 $A\cap B\trianglelefteq G$，由极小性可知 $A\cap B=\{e\}$。又 $AB\trianglelefteq G$，且映射 $b\mapsto bA$、$a\mapsto aB$ 分别给出同构

$$AB/A\cong B,\qquad AB/B\cong A.$$

这里每个映射都为满同态，并由 $A\cap B=\{e\}$ 得到单射性。

在 A 与 AB 之间没有其他 G 的正规子群。事实上，若 $A\leqslant M\leqslant AB$ 且 $M\trianglelefteq G$，则对 $m=ab\in M$，由 $a\in A\leqslant M$ 得 $b\in M\cap B$，所以 $M=A(M\cap B)$。而 $M\cap B\trianglelefteq G$，由 B 的极小性，只能有 $M\cap B=\{e\}$ 或 B，故 $M=A$ 或 AB。同理，在 B 与 AB 之间也不能再插入 G 的正规子群。

选取 G/AB 的一条主群列，将其各项取原像，得到从 AB 到 G 的群列。分别在其下端补上 $\{e\}<A<AB$ 和 $\{e\}<B<AB$，便得到 G 的两条主群列。这两条群列的前两个因子群分别同构于

$$A,\ B \qquad 和 \qquad B,\ A,$$

其余因子群相同，因此它们等长且因子群组相同。

最后，在 G/A 中应用归纳假设，可知原来的第一条主群列与新构造的经过 A 的主群列等长且因子群组相同；在 G/B 中同理比较第二条群列。结合上面的比较，即得原来两条主群列的长度相同，因子群经过重排后逐个同构。 □

8. 群 G 的正规子群 N 称为 G 的极小正规子群，若 $N\neq\{e\}$ 且 N 不真包含 G 的非平凡正规子群（例如单群的极小正规子群就是它本身）。假设群 G 有主群列，证明它的主群列的每个因子群都是 G 的某个商群的极小正规子群。

解 设 $G=G_0>G_1>\cdots>G_s=\{e\}$ 为主群列，其中每个 $G_i\trianglelefteq G$。固定 $0\leqslant i<s$，则 G_i/G_{i+1} 是 G/G_{i+1} 的非平凡正规子群。

若 L 是 G/G_{i+1} 的正规子群，且 $\{G_{i+1}\}\leqslant L\leqslant G_i/G_{i+1}$，取自然满同态 $\pi:G\to G/G_{i+1}$，令 $M=\pi^{-1}(L)$。由对应定理，$M\trianglelefteq G$，并且 $G_{i+1}\leqslant M\leqslant G_i$。

因为主群列的相邻两项之间不能插入其他 G 的正规子群，所以 $M=G_{i+1}$ 或 G_i。相应地，$L=\{G_{i+1}\}$ 或 G_i/G_{i+1}。

因此 G_i/G_{i+1} 是商群 G/G_{i+1} 的极小正规子群，结论成立。 □

9. 证明有合成群列的群一定有主群列。

解 设 G 有一条长度为 r 的合成群列。先证明：G 的任意无重复正规群列的长度都不超过 r。对 r 作归纳。

若 $r=0$，则 $G=\{e\}$，结论成立。设 $r>0$，记给定合成群列中紧接 G 的一项为 M，则 $M\trianglelefteq G$，G/M 是单群，而 M 有长度为 $r-1$ 的合成群列。

任取一条无重复正规群列 $G=N_0>N_1>\cdots>N_t=\{e\}$。考虑它在 M 中的交和在 G/M 中的像：

$$N_0\cap M\geqslant\cdots\geqslant N_t\cap M,\qquad N_0M/M\geqslant\cdots\geqslant N_tM/M.$$

第一条群列的各项都正规于 M，删去重复项后，由归纳假设，严格下降的次数至多为 $r-1$。第二条群列的各项都正规于单群 G/M，故只能是整个 G/M 或单位元群，因此严格下降至多一次。

而每次 $N_i>N_{i+1}$，至少有上述两条群列中的一条发生严格下降。否则，若交和像都相同，任取 $x\in N_i$，由像相同可取 $y\in N_{i+1}$ 使 $xM=yM$。于是

$$y^{-1}x\in N_i\cap M=N_{i+1}\cap M\leqslant N_{i+1},$$

从而 $x\in N_{i+1}$，与 $N_i>N_{i+1}$ 矛盾。因此 $t\leqslant(r-1)+1=r$，归纳完成。

于是 G 的无重复正规群列的长度有有限上界。选取其中长度最大的一条，若还能在相邻两项之间插入 G 的正规子群，就会得到更长的无重复正规群列，矛盾。因此所选群列是主群列。 □

10. 设 $n\geqslant3$，试给出对称群 S_n 的所有合成群列和主群列。

解 合成群列只要求每一项正规于前一项，且各因子群为非平凡单群；主群列则要求每一项都正规于整个 S_n，并且不能再插入这样的正规子群。分三种情形讨论。

(1) $n=3$。S_3 的唯一非平凡真正规子群为 A_3，且 A_3 的阶为 3。因此唯一的合成群列和主群列都是

$$S_3 \trianglerighteq A_3 \trianglerighteq \{e\},$$

因子群依次为 $\mathbb{Z}_2, \mathbb{Z}_3$。

(2) $n=4$。令 $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$。

S_4 的共轭类由轮换型决定，其大小为 $1, 3, 6, 6, 8$。在 A_4 中，三个双对换彼此共轭，而每个 3-轮换的中心化子阶为 3，故其共轭类大小为 4。因此 A_4 的共轭类大小为 $1, 3, 4, 4$。

正规子群必须是包含单位元的共轭类之并，且其阶整除群阶。检查这些可能的大小，得到 S_4 的正规子群恰为 $\{e\}, V_4, A_4, S_4$，A_4 的正规子群恰为 $\{e\}, V_4, A_4$。

所以合成群列的前两步必须为 $S_4 \trianglerighteq A_4 \trianglerighteq V_4$。$V_4$ 的三个 2 阶子群为

$$T_1 = \langle (12)(34) \rangle, \qquad T_2 = \langle (13)(24) \rangle, \qquad T_3 = \langle (14)(23) \rangle.$$

它们都正规于 V_4，因此全部合成群列恰为

$$\boxed{S_4 \trianglerighteq A_4 \trianglerighteq V_4 \trianglerighteq T_i \trianglerighteq \{e\}, \qquad i = 1, 2, 3.}$$

因子群依次为 $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2$。

但 T_1, T_2, T_3 在 S_4 中彼此共轭，均不正规于 S_4，故不能加入主群列。由上述正规子群列表，唯一的主群列为

$$\boxed{S_4 \trianglerighteq A_4 \trianglerighteq V_4 \trianglerighteq \{e\},}$$

因子群依次为 $\mathbb{Z}_2, \mathbb{Z}_3, V_4$。这里 V_4 不是单群，说明主群列的因子群不必是单群。

(3) $n \geqslant 5$。由已证结论，S_n 的唯一非平凡真正规子群为 A_n，且 A_n 为单群。因此唯一的合成群列和主群列都是

$$\boxed{S_n \trianglerighteq A_n \trianglerighteq \{e\},}$$

因子群依次为 $\mathbb{Z}_2, A_n$。

□

11. 证明有限 p-群为零幂群。

解 先说明非平凡有限 p-群的中心非平凡。由类方程，每个非中心共轭类的大小都是大于 1 的 p 的幂，故 $|Z(P)| \equiv |P| \equiv 0 \pmod{p}$。又中心包含单位元，所以 $|Z(P)| \geqslant p$。

现设 $|G| = p^r$。若 $r = 0$，则结论成立。以下设 $r > 0$，从 $Z_0 = \{e\}$ 开始，递归定义 Z_{i+1} 为自然映射 $G \to G/Z_i$ 下中心 $Z(G/Z_i)$ 的原像，即

$$Z_{i+1}/Z_i = Z(G/Z_i).$$

由中心为正规子群及正规子群的原像仍正规，可知各 $Z_i \trianglelefteq G$。只要 $Z_i \neq G$，商群 G/Z_i 就是非平凡有限 p-群，其中心非平凡，所以 $Z_{i+1} > Z_i$。

由于 $|G| = p^r$，每次严格增大都使阶至少增大 p 倍，故至多经过 r 步便有 $Z_c = G$。又由定义，Z_{i+1}/Z_i 位于 G/Z_i 的中心，所以

$$\{e\} = Z_0 \leqslant Z_1 \leqslant \cdots \leqslant Z_c = G$$

是一条中心群列。因此 G 为零幂群。 □

12. 设 G 是有限群，证明下列陈述等价：

(1) G 是零幂群；

(2) 对 G 的任意非平凡真子群 H，有 $H < N_G(H)$；

(3) G 的每个 Sylow 子群在 G 中正规；

(4) G 是其 Sylow 子群的直积；

(5) G 的每个极大子群在 G 中正规。

解 若 $G = \{e\}$，各条件均成立。以下设 $G \neq \{e\}$，先证明 (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1)，再证明 (2) $\Rightarrow$ (5) $\Rightarrow$ (3)。

(1) $\Rightarrow$ (2)。取 G 的一条升序中心群列 $\{e\} = Z_0 \leqslant Z_1 \leqslant \cdots \leqslant Z_c = G$，其中 $[G, Z_i] \leqslant Z_{i-1}$。设 $H < G$，取最小的 i 使 $Z_i \not\subseteq H$，则 $Z_{i-1} \leqslant H$。

选取 $x \in Z_i \setminus H$。对任意 $h \in H$，有 $xhx^{-1}h^{-1} \in Z_{i-1} \leqslant H$，所以 $xHx^{-1} \subseteq H$。对 $x^{-1} \in Z_i$ 同理可得反向包含，故 $xHx^{-1} = H$。因此 $x \in N_G(H) \setminus H$，从而 $H < N_G(H)$。

(2) $\Rightarrow$ (3)。任取 Sylow p-子群 P，令 $K = N_G(P)$。则 $P \trianglelefteq K$，且 P 也是 K 的 Sylow p-子群，所以它是 K 的唯一 Sylow p-子群。

若 $g \in N_G(K)$，则 gPg^{-1} 仍为 K 的 Sylow p-子群，由唯一性有 $gPg^{-1} = P$，故 $g \in K$。因此 $N_G(K) = K$。

又 $P \leqslant K$，故 $K \neq \{e\}$。若 $K < G$，由 (2) 应有 $K < N_G(K)$，矛盾。因此 $K = G$，即 $P \trianglelefteq G$。

(3) $\Rightarrow$ (4)。设 $|G| = p_1^{a_1} \cdots p_s^{a_s}$，分别记各 Sylow 子群为 $P_1, \ldots, P_s$。它们都正规，且阶两两互素，所以 $P_i \cap P_j = \{e\}$（$i \neq j$）。由正规性，$[P_i, P_j] \leqslant P_i \cap P_j = \{e\}$，故不同因子之间的元素可交换。

逐次利用子群乘积的阶数公式及各阶互素，得到

$$|P_1 \cdots P_s| = \prod_{i=1}^{s} |P_i| = |G|.$$

所以 $G = P_1 \cdots P_s$。乘法映射 $P_1 \times \cdots \times P_s \to G$ 是满同态，且两边的阶相同，故为同构。这就证明了 (4)。

(4) $\Rightarrow$ (1)。由第 11 题，每个 P_j 都零幂。取各 P_j 的升序中心群列，并在较短的群列末端重复 P_j，使它们有相同长度 c，记为 $\{e\} = C_{j,0} \leqslant \cdots \leqslant C_{j,c} = P_j$。

在直积 $G = P_1 \times \cdots \times P_s$ 中令 $C_i = \prod_{j=1}^{s} C_{j,i}$。由于直积中的换位子按分量计算，$[G, C_i] \leqslant C_{i-1}$，故 $\{e\} = C_0 \leqslant \cdots \leqslant C_c = G$ 是中心群列。因此 G 零幂。

(2) $\Rightarrow$ (5)。设 M 为极大子群。若 $M = \{e\}$，则它正规。若 $M \neq \{e\}$，由 (2) 有 $M < N_G(M) \leqslant G$，再由极大性可知 $N_G(M) = G$，故 $M \trianglelefteq G$。

(5) $\Rightarrow$ (3)。任取 Sylow p-子群 P，反设 P 不正规，则 $N_G(P) < G$。由于 G 有限，可取极大子群 M 使 $N_G(P) \leqslant M < G$。由 (5)，$M \trianglelefteq G$。

任取 $g \in G$，由 $P \leqslant M$ 及 M 的正规性，有 $gPg^{-1} \leqslant M$。P 和 gPg^{-1} 都是 M 的 Sylow p-子群，所以存在 $m \in M$，使 $gPg^{-1} = mPm^{-1}$。于是 $m^{-1}g \in N_G(P) \leqslant M$，从而 $g \in M$。

这对任意 $g \in G$ 都成立，故 $G = M$，矛盾。因此 $P \trianglelefteq G$，即得 (3)。综上，五个条件等价。 □