

1, 试确定实数域 $\mathbb{R}$ 上一般线性群 $GL_2(\mathbb{R})$ 中

由元素 $A = \begin{pmatrix} 2 & 3 \\ -1 & -1 \end{pmatrix}$ 所生成的循环群,

解: $A = \begin{pmatrix} 2 & 3 \\ -1 & -1 \end{pmatrix},$

$$A^2 = \begin{pmatrix} 2 & 3 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix},$$

$$A^n = \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -E,$$

因此 $A^4 = -A, A^5 = -A^2, A^6 = -A^3 = E,$

故在群 $GL_2(\mathbb{R})$ 中由 A 生成的循环群为 $\langle A \rangle = \{E, A, A^2, A^3, A^4, A^5\},$

2, 设 G 是群, 对属于群 G 的任意 a, b , 试证明 ab 与 ba 的阶相同,

证明: 若 $(ab)^n = e$, 则 $b = b(ab)^n = (ba)^n b$, 从而 $(ba)^n = e$,

3, 试证明 S_3 是阶数最小的非交换群,

证明: 因为 1, 2, 3, 5 阶群为循环群, 因而是交换群,

4 阶群有两种: 一种是循环群, 另一种与 K_4 同构, 它们都是交换群,

而 S_3 是 6 阶非交换群, 所以 S_3 是阶数最小的非交换群

4, 设 G 是交换群, 试证明 G 中全体有限阶元素构成 G 的一个子群,

证明: 设 $S = \{a \in G \mid a \text{ 的阶有限}\}$, 显然 e 属于 S , 即 S 不是空集,

设属于 S 的任意 a, b 的阶分别为 m, n ,

又因 G 为交换群, 因此 $(a^{-1}b)^{mn} = (a^{-1})^{mn}(b)^{mn} = e$,

从而 $a^{-1}b$ 也为有限阶元, 即 $a^{-1}b$ 属于 S ,

故 G 中全体有限阶元素构成 G 的一个子群,

5, 试证明群 G 仅有平凡子群的充分必要条件是 $G=\{e\}$ 或 G 是素数阶循环群,

证明: 充分性, 若 $G=\{e\}$, 显然 G 仅有平凡子群;

若 G 是素数阶循环群, 则 G 的子群的阶数只能为 1 或 $|G|$,

从而 G 仅有平凡子群,

必要性, 若 $G \neq \{e\}$, 则存在 a 属于 $G, a \neq e, \langle a \rangle$ 是 G 的子群且 $\langle a \rangle \neq \{e\}$,

所以 $\langle a \rangle = G$,

设 a 的阶为 n , 若素数 $p|n$, 则 $a^{\frac{n}{p}}$ 的阶为 $p, \langle a^{\frac{n}{p}} \rangle$ 是 G 的子群, $\langle a^{\frac{n}{p}} \rangle \neq \{e\}$,

所以 $\langle a^{\frac{n}{p}} \rangle = G, G$ 是 p 阶群,

6, 试证明 6 阶群 G 必有 3 阶子群,

证明: G 的元素的阶仅可能是 1, 2, 3, 6,

若 G 中单位元以外的元素阶都为 2, 则 G 是一个阿贝尔群,

对 G 中非单位元 a_1, a_2 , 设 $a_1 a_2 = a_3$, 则 $\{e, a_1, a_2, a_3\}$ 构成 G 的一个四阶子群,

这与 G 的阶为 6 矛盾,

若 G 中存在 3 阶元素 a 或 6 阶元素 b , 则 G 中存在 3 阶子群 $\{e, a, a^2\}$ 或 $\{e, b^2, b^4\}$

7, 试证明循环群 $\langle a \rangle$ 的商群是循环群,

且商群的生成元是 $\langle a \rangle$ 的生成元所在的左陪集,

证明: 设 $\langle a \rangle$ 的正规子群为 $\langle a^r \rangle$, 商群为 $\langle a \rangle / \langle a^r \rangle$, 设 $a^t \langle a^r \rangle$ 属于 $\langle a \rangle / \langle a^r \rangle$,

则 $a^t \langle a^r \rangle = (a \langle a^r \rangle)^t$, 即 $\langle a \rangle / \langle a^r \rangle$ 是循环群, 生成元为 $a \langle a^r \rangle = \bar{a}$,

8, 设 $G = \langle a \rangle$ 是循环群, a 的阶为 15, 求子群 $H = \langle a^6 \rangle$ 的所有左陪集,

解: a^6 的阶为 $\frac{15}{(6,15)} = 5$, 即 H 是 5 阶子群, 所以 H 的左陪集共有 3 个: H, aH, a^2H

9, 求剩余类加法群 Z_6 中各元素的阶, 并找出 Z_6 的所有子群,

解: Z_6 的元素 $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ 的阶依次为 1, 6, 3, 2, 3, 6,

Z_6 的子群是循环群,

因此 Z_6 的 1 阶子群为 $\{\bar{0}\}$, 2 阶子群为 $\langle \bar{3} \rangle$, 3 阶子群为 $\langle \bar{2} \rangle = \langle \bar{4} \rangle$, 6 阶子群为 Z_6

10, 试找出 Z_3 和 Z_4 的所有子群,

解: Z_3 的子群有 $\{\bar{0}\}, Z_3$

Z_4 的子群有 $\{\bar{0}\}, \{\bar{0}, \bar{2}\}, Z_4$

11, 如果群 G 只含有限多个子群, 试证明 G 是有限群,

证明: 若 G 有无限阶元素 a , 则 $\langle a \rangle \cong Z$, 而 Z 有无穷多个子群 nZ , 这与 G 只含有限多个子群矛盾, 因此, G 中元素的阶都是有限的,

因为 G 的循环子群的个数也有限, 且 $G = \bigcup_{a \in G} \langle a \rangle$

所以存在有限个元 $a_1, a_2, \dots, a_n$, 使得 $G = \bigcup_{1 \leq i \leq n} \langle a_i \rangle$

而每个 $\langle a_i \rangle$ 均为有限群, 从而 G 是有限群,

12, 设 a 的阶为 18, 求 $\langle a^3 \rangle \cap \langle a^{10} \rangle$ 的生成元,

解: $\langle a^3 \rangle \cap \langle a^{10} \rangle$ 的生成元是 $a^r, r = [3, 10] = 30, a^{30} = a^{12},$

a^{12} 的阶为 $\frac{18}{(12, 18)} = 3, \langle a^{12} \rangle$ 的生成元有 $a^{12}, a^{24},$

习题 1 设 G 是群, a, b 都属于 G , 试证明 a 与 a^{-1} 的阶相同, aba^{-1} 与 b 的阶相同

证明: 若 a 的阶为 m, a^{-1} 的阶为 $n,$

则 $a^m = e, a^{-m} = e$, 从而 $n|m$, 同理 $m|n$, 所以 $n=m$,

设 aba^{-1} 与 b 的阶分别为 m 和 $n,$

则 $(aba^{-1})^m = e, ab^ma^{-1} = e, b^m = e$, 从而 $n|m$, 同理 $m|n$, 所以 $n=m$,

习题 2 设 G 是群, a 是 3 阶元素, 属于 G 的 b 满足 $ab = b^2a$, 求 b 的阶,

解: 由 $ab = b^2a$ 知 $b^{-1}ab = ba$, 从而 ba 阶为 3, $e = (ba)^3 = b^7,$

则 b 的阶为 1 或 7,

习题 3 设群同态映射 $\varphi: G \rightarrow G'$, G 的元素 a 的阶为 n , 试证明 $\varphi(a)$ 的阶整除 n ,

证明: 由群同态基本定理知 $\varphi(a)^n = \varphi(a^n) = \varphi(e) = e'$, 则 $\varphi(a)$ 的阶整除 n ,

习题 4 设 G 是交换群, 属于 G 的 a_i 的阶为 m_i , ($i=1, 2, \dots, n$)

若 m_i 彼此互素, 则 $a_1 + a_2 + \dots + a_n$ 的阶为 $m_1 m_2 \dots m_n$,

证明: 对 n 用数学归纳法,

当 $n=2$ 时, 因为 m_1, m_2 互素, 所以 $\langle a_1 \rangle \cap \langle a_2 \rangle = \{0\}$, 从而, $a_1 + a_2$ 的阶为 $m_1 m_2$

假设结论对 $n-1$ 成立, 那么 $a_1 + a_2 + \dots + a_{n-1}$ 的阶为 $m_1 m_2 \dots m_{n-1}$,

显然, m_n 与 $m_1 m_2 \dots m_{n-1}$, 互素,

因此, $(a_1 + a_2 + \dots + a_{n-1}) + a_n$ 的阶为 $m_1 m_2 \dots m_{n-1} m_n$,

习题 5 设 a 的阶为 18, 求群 $\langle a^{12} \rangle$ 的元素,

解: 设 n 是正整数, 若 a 是无限阶元素, 则由 $a^k = a^l$, 可以推出 $k=l$,

则 $\langle a^n \rangle = \{e, a^n, a^{-n}, a^{2n}, a^{-2n}, \dots\}$ 是无限群,

若 a 是有限阶元素, 设 a 的阶为 m , 则 a^n 的阶为 $t = \frac{m}{(m,n)}$,

因此, $\langle a^n \rangle = \{e, a^n, a^{2n}, \dots, a^{(t-1)n}\}$, $\langle a^{12} \rangle = \{e, a^{12}, a^{24}\}$,

习题 6 求非零有理数乘法群中每个元素的阶,

解: 设 n, m 属于 $\mathbb{Z}$, $n \neq 0$, 若 $\frac{m}{n}$ 的阶为 r , 即 $\left(\frac{m}{n}\right)^r = 1$,

则 $\frac{m}{n} = 1, r=1$ 或 $\frac{m}{n} = -1, r=2$ 或 $\frac{m}{n} \neq \pm 1, \frac{m}{n}$ 为无限阶元素,

习题 7 设 G 是交换群, a, b 都属于 G , a, b 的阶分别为 12, 9, 求 a^5 和 $a^6 b$ 的阶,

解: a^5 的阶为 $\frac{12}{(12,5)} = 12$, a^6 的阶为 2, $a^6 b$ 的阶为 18,

习题 8 在群 $\{GL_2(R); \times\}$ 中, $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, 计算 A, B 及 AB 的阶,

解: 因为 $A^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$, $A^3 = E$ 、 $B^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $AB = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $(AB)^2 = -E$,

所以 A 的阶为 3, B 的阶为无限, AB 的阶为 4,

习题 9 设群 G 的阶为 n, 若 m, n 互素,

试证明对属于群 G 的任意 a, 方程 $x^m = a$ 有唯一解,

证明: 由 m, n 互素可知存在属于 Z 的 s, t, 使得 $ms + nt = 1$,

则 $a = a^{ms+nt} = a^{ms} = (a^s)^m$, 即 a^s 是一个解,

若存在另一个解 b, 则 $a = (a^s)^m = b^m$,

从而 $(a^s b^{-1})^m = e$, $a^s b^{-1}$ 的阶为 m, n 的公因子,

因为 m, n 互素, 所以 $a^s b^{-1}$ 的阶为 1, $a^s = b$, 即 $x^m = a$ 有唯一解,

习题 10 设 H 是 G 的子群, H 在 G 中的指数有限,

试证明若 H 元素的阶都是有限的, 则 G 的元素的阶是有限的,

证明: 若 a 属于 $(G-H)$, 因为 H 在 G 中的指数有限,

所以 $aH, a^2H, \dots, a^mH, \dots$ 中必有两个是相等的,

设 $a^i H = a^j H$, (其中 $i > j$), 则属于 H 的 a^{i-j} 是有限阶元素,

从而 a 是有限阶元素, G 的所有元素的阶是有限的

习题 11 设 G 是非交换群,

试证明存在属于 G 的 a, b, 使得 a, b, e 互不相等, 且 $ab = ba$,

证明: 在 G 中存在阶大于 2 的元素 a (否则 G 是交换群), 即 $a \neq a^{-1}$,

令 $b = a^{-1}$, 则 a, b 为所求,

习题 12 判断 Z_5^* 是否是循环群,

解: Z_5^* 是 4 阶群, 它的元素 $\bar{1}, \bar{2}, \bar{3}, \bar{4}$ 的阶分别为 1, 4, 4, 2,

因此, $Z_5^* = \langle \bar{2} \rangle = \langle \bar{3} \rangle$ 是循环群

习题 13 设 a 是群 G 的任意元素，试证明

(1) 若 a 是 n 阶元素，则 $\langle a^s \rangle = \langle a^t \rangle \Leftrightarrow (s, n) = (t, n)$ ；

(2) 若 a 是无限阶元素，则 $\langle a^s \rangle = \langle a^t \rangle \Leftrightarrow s = \pm t$ ，

证明: (1) a^s, a^t 的阶分别为 $\frac{n}{(n,s)}, \frac{n}{(n,t)}$ ， $\langle a \rangle$ 的 r 阶子群是唯一的，

因此 $\langle a^s \rangle = \langle a^t \rangle \Leftrightarrow (s, n) = (t, n)$ ，

(2) 充分性是显然的，下面证明必要性

无限阶循环群 $\langle a \rangle$ 的子群为有限群 $\{e\}$ 或无限群，

因此，若 $\langle a^s \rangle$ 是有限群，则 $a^s = a^t = e$ ，即 $s = t = 0$ ；

若 $\langle a^s \rangle$ 是无限群，则 $\langle a^s \rangle$ 的生成元只能是 a^s 和 a^{-s} ，因此， $s = \pm t$ ，

习题 14 设 G 是群， a, b 是 G 的阶互素的两个元素，

试证明若 $ab = ba$ ，则 $\langle a, b \rangle = \langle ab \rangle$ ，

证明: 显然 $\langle ab \rangle$ 包含于 $\langle a, b \rangle$ ，下证反包含关系成立，

设 a, b 的阶分别为 m, n ，因为 m, n 互素，因此存在 s, t ，使得 $ms + nt = 1$ ，

从而 $a = a^{ms+nt} = a^{nt} = (ab)^{nt}$ 属于 $\langle ab \rangle$ ，

同理可得 b 属于 $\langle ab \rangle$ ，所以 $\langle a, b \rangle$ 包含于 $\langle ab \rangle$ ，

习题 15 设 $H = \langle a^s \rangle, K = \langle a^t \rangle$ 是 $G = \langle a \rangle$ 的子群，试证明 $H \cap K = \langle a^{[s,t]} \rangle$ ，

证明: 显然， $\langle a^{[s,t]} \rangle$ 包含于 $\langle a^s \rangle \cap \langle a^t \rangle$ ，

因为循环群的交还是循环群，设 $H \cap K$ 的生成元是 a^r ，

则 r 是 s 和 t 的公倍数，即 $H \cap K$ 包含于 $\langle a^{[s,t]} \rangle$ ，从而 $H \cap K = \langle a^{[s,t]} \rangle$ ，

习题 16 设 a 的阶为 18，求 $\langle a^{14} \rangle \cap \langle a^{10} \rangle$ 的生成元，

解: 由上题， $\langle a^{14} \rangle \cap \langle a^{10} \rangle$ 的生成元是 $a^r, r = [14, 10] = 70, a^{70} = a^{16}$ ，

所以 $\langle a^{14} \rangle \cap \langle a^{10} \rangle$ 的生成元为 a^{16} ，

习题 17 设属于 S_n 的 σ 是长度为 t 的轮换，试证明 σ 的阶为 t ，

证明： 设 $\sigma = (i_1, i_2, \dots, i_t)$ ，则当 $r=1, \dots, t-1$ 时， $\sigma^r(i_1) = i_{r+1}$ ， $\sigma^r \neq (1)$ ，而 $\sigma^t = (1)$ ，所以 σ^n 的阶为 t ，

习题 18 设 σ 属于 S_n ，如果 σ 是不相交轮换的合成 $\sigma = \sigma_1 \sigma_2 \cdots \sigma_s$ ，

其中 σ_i 是长度为 t_i 的轮换，试证明 σ 的阶为 $t_1, t_2, \dots, t_s$ 的最小公倍数，

证明： 对 s 用数学归纳法，

若 $s=2$ ，由 σ_1, σ_2 ，互不相交可知 $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$ ，且 $\langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle = \{(1)\}$ ，

根据[第二章命题 5.2]可知 σ 的阶为 $[t_1, t_2]$ ，

假设结论对 s 成立，

令 $\sigma_0 = \sigma_1 \sigma_2 \cdots \sigma_s$ ， $\sigma = \sigma_0 \sigma_{s+1}$ ，则 $\sigma_0 \sigma_{s+1} = \sigma_{s+1} \sigma_0$ ，且 $\langle \sigma_0 \rangle \cap \langle \sigma_{s+1} \rangle = \{(1)\}$ ，

因此 σ 的阶为 $[[t_1, \dots, t_s], t_{s+1}] = [t_1, \dots, t_s, t_{s+1}]$ ，

习题 19 将下列置换表示成不相交轮换的合成，并求其阶，

(1)(16243)(532)； (2)(672)(5326)(127)，

解： 因为 $(16243)(532) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$

所以 $(16243)(532) = (1625)(34)$ ，阶为 4，

$(672)(5326)(127) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 3 & 4 & 5 & 6 & 1 \\ 6 & 7 & 2 & 4 & 3 & 5 & 1 \\ 7 & 2 & 6 & 4 & 3 & 5 & 1 \end{pmatrix}$

所以 $(672)(5326)(127) = (17)(365)$ ，阶为 6，

习题 20 S_4 中有多少个 4 阶元？设 $\sigma = (243)$ 属于 S_4 ，求 $\langle \sigma \rangle$ ，

解： (1) 是 1 阶元；

(12)，(13)，(14)，(23)，(24)，(34) 是 2 阶元；

(123)，(132)，(124)，(142)，(134)，(143)，(234)，(243) 是 3 阶元；

(1234)，(1243)，(1324)，(1342)，(1423)，(1432) 是 4 阶元；

(12)(34)，(13)(24)，(14)(23) 是 2 阶元，

因为 $\sigma = (243)$ 是 3 阶元，所以 $\langle \sigma \rangle = \{(1), (243), (234)\}$ ，

习题 21 设 σ 是长度为 5 的轮换，已知 $\sigma^3=(53241)$ ，求 $\sigma, \sigma^{-1}, \sigma^4, \langle \sigma \rangle$ ，

解：若 $\sigma=(i_1 i_2 \cdots i_t)$ 的长度为 t ，则 σ 的阶为 t ， $\sigma^{-1}=(i_t i_{t-1} \cdots i_1)$ ，

那么 $(\sigma^3)^2=\sigma^5\sigma=\sigma$ ，计算得 $\sigma=(13452)$ ，

从而 $\sigma^{-1}=(12543)$ ，

$\sigma^4=\sigma^5\sigma^{-1}=\sigma^{-1}=(12543)$ ，

$\langle \sigma \rangle=\{(1), (13452), (14235), (15324), (12543)\}$ ，

习题 22 证明当且仅当 $(a, n)=1$ 时， $\bar{a}$ 是 Z_n 的生成元，

证明 1: Z_n 的生成元为 $\bar{1}$ ，而 $\bar{a}=a\bar{1}$ ，因此命题成立，

证明 2: 必要性，设 $(a, n)=d$ ，则 $\frac{n}{d}\bar{a}=\frac{n}{d}\overline{a}=\frac{a}{d}\bar{n}=\bar{0}$ ，即 $\bar{a}$ 的阶是 $\frac{n}{d}$ 的因数

又因为 $\bar{a}$ 是 Z_n 的生成元，所以 $\bar{a}$ 的阶是 n ，从而 $d=1$ ，

充分性，设 $\bar{a}$ 的阶是 m ，则 $\bar{0}=m\bar{a}=\overline{ma}$ ，即 $n|ma$ ，由 $(a, n)=1$ 得 $n|m$ ，

从而 $m=n$ ，即 $\bar{a}$ 是 Z_n 的生成元，

习题 23 求循环群 Z_{10} 的生成元个数

解： Z_{10} 是 10 阶循环群，

因此它的生成元个数为欧拉函数 $\varphi(10)=4$ (小于 10 与 10 互素的元素的个数)

习题 24 分别求循环群 Z_{15} 的生成元个数和子群个数，

解：小于 15 与 15 互素的正整数有 1, 2, 4, 7, 8, 11, 13, 14，

生成元个数共 8 个，

15 的正因数有 1, 3, 5, 15，子群个数共 4 个，

习题 25 求 Z_{pq} 的生成元的个数，其中 p, q 是互不相同的素数

解： Z_{pq} 的生成元个数为 $\varphi(pq)$ ，

而小于 pq 且与 pq 互素的正整数有 $(p-1) \cdot (q-1)$ 个，

习题 26 求 Z_{p^k} 的生成元的个数，其中 p 是素数，是正整数，

解: Z_{p^k} 的生成元个数为 $\varphi(p^k)$ ，而小于 p^k 且与 p^k 互素的正整数有 $p^{k-1}(p-1)$ 个

习题 27 证明 A_4 没有 6 阶子群，

证明 1: 若 A_4 有 6 阶子群，则这个 6 阶子群有一个 3 阶子群，

设其为 $\{(1), (123), (132)\}$ ，其他 3 个元素为 2 阶元素，

因此，6 阶子群为 $\{(1), (123), (132), (12)(34), (13)(24), (14)(23)\}$ ，

它包含一个 4 阶子群，矛盾，所以 A_4 没有 6 阶子群，

证明 2: 若 A_4 有 6 阶子群 H ，

则 $\frac{|A_4|}{|H|} = 2$ ，从而 H 是正规子群且对任意 aH 有 $(aH)^2 = H$ ，即 a^2 属于 H ，

从而

$\{a^2 | a \in A_4\} = \{(1), (132), (123), (124), (142), (134), (143), (234), (243)\} \subseteq H$

矛盾，

习题 28 求 A_4 的所有子群和正规子群，

证明: 1 阶子群为 $\{(1)\}$ ；

2 阶子群为 $\{(1), (12)(34)\}, \{(1), (13)(24)\}, \{(1), (14)(23)\}$ ；

3 阶子群为 $\{(1), (123), (132)\}, \{(1), (124), (142)\}, \{(1), (134), (143)\},$

$\{(1), (234), (243)\}$

4 阶子群只能含 1, 2 阶元素，

因此 4 阶子群为 $\{(1), (12)(34), (13)(24), (14)(23)\}$ ；

没有 6 阶子群；

12 阶子群为 A_4 ，

正规子群有 $\{(1)\}, \{(1), (12)(34), (13)(24), (14)(23)\}, A_4$ ，

习题 29 证明不存在恰有两个 2 阶元素的群，

证明: 假设属于 G 的 a, b 是群 G 的两个 2 阶元，则 aba^{-1} 的阶为 2，

若 $aba^{-1}=a$ ，则 $ab=a^2, a=b$ ，矛盾，

若 $aba^{-1}=b$ ，则 ab 的阶为 2，从而 $ab=a$ 或 b ，但是无论哪种情况都与已知矛盾，
所以不存在恰有两个 2 阶元素的群，

习题 30 确定 1, 2, 3, 4, 5, 6, 7 阶同构群，

证明: 因为素数阶群是循环群，

所以 2, 3, 5, 7 阶群分别同构于 Z_2, Z_3, Z_5 ，和 Z_7 ，

1 阶群只有一个，

4 阶群是交换群，

若存在 4 阶元素，则为循环群，同构于 Z_4 ；

若不存在 4 阶元素，

则单位元以外的每个元素阶均为 2，同构于克莱因四元素群，

对于 6 阶群，

若存在 6 阶元素，则为循环群，同构于 Z_6 ；

若不存在阶为 6 的元素，则必存在一个 3 阶元素 a 和一个 2 阶元素 b ，

则这个 6 阶群为 $G=\{e, a, a^2, b, ba, ba^2\}=\langle a, b \rangle$ ，

若 $ab=ba$ ，则 ab 的阶为 6，矛盾，所以 $ab=ba^2$ ，

在 G 和 S_3 之间定义映射 φ ，使得 $\varphi(a)=(123), \varphi(b)=(12)$ ，则 φ 是同构映射，

因此，6 阶群有两类， Z_6 和 S_3

习题 31 证明 $\text{Aut}(S_3) \cong S_3$ ，

证明: 因为 S_3 中心为 $\{(1)\}$ ，根据[参见习题 2, 4 题 10] $\text{Int}(S_3) \cong S_3$ ，

确定 $\text{Aut}(S_3)$ 中的元素，仅需要考虑 S_3 的生成元，

而 $S_3=\langle (12), (13) \rangle$ 且 $(12), (13)$ 的阶都为 2，它们同构像的阶只能为 1 或 2，

所以可能的像有 $(1), (12), (13), (23)$ ，那么 $\text{Aut}(S_3)$ 最多有 $P_4^2=6$ 个元素，

又因 $\text{Int}(S_3)$ 包含于 $\text{Aut}(S_3)$ ，所以 $\text{Aut}(S_3)=\text{Int}(S_3) \cong S_3$

习题 32 设 $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$

关于矩阵的乘法运算是群，试找出与 G 同构的置换群，

解: 因为 4 阶群分为循环群和克莱因四元群两类，又因为 G 不是循环群，因此 G 同构于置换群 $\{(1), (12)(34), (13)(24), (14)(23)\}$ ，

习题 33 设 G 是交换群，且 G 中所有元素有最大阶 n ，

试证明 G 中每个元素的阶都是 n 的因数，

证明: 设 a 的阶为 n , b 的阶为 m ，若 m 不是 n 的因数，则存在素数 p ，使得 $n = p^l s$, $m = p^k t$, $(p, s) = (p, t) = 1$ ，其中 $k > l$ ，

因为 a^{p^l} , b^t 的阶分别为 s , p^k ，则 $a^{p^l} b^t$ 的阶为大于 n 的 sp^k ，矛盾，

因此， G 中每个元素的阶都是 n 的因数，

习题 34 设 G 是有限交换群， n 是 G 的所有元素阶的最小公倍数，

试证明在 G 中存在 n 阶元素，

证明: 设 a 是最大阶元素，由上题即可得证，

习题 35 设 G 是有限交换群，

试证明当且仅当对任意正整数 m , $x^m = e$ 在 G 中最多有 m 个解时， G 是循环群

证明: 充分性，设 $|G| = n$ ，由习题 33 知，

G 中存在阶为 m 的元素 a ，且 m 是所有元素阶的最小公倍数，得 $m \leq n$ ，

对属于群 G 的任意 b ，有 $b^m = e$ ，即 $x^m = e$ 有 n 个解，得 $n \leq m$ ，

因此 $n = m$, $G = \langle a \rangle$ 是循环群，

必要性，设 $|G| = n$, $G = \langle a \rangle$ ，若 a^r 是 $x^m = e$ 的解，则 $a^{rm} = e$ ，

从而 $n \mid rm$, $\frac{n}{(m,n)} \mid r \frac{m}{(m,n)}$ ，进而 $\frac{n}{(m,n)} \mid r$ ，

这说明 a^r 属于 $\langle a^{\frac{n}{(m,n)}} \rangle$ ，而 $\langle a^{\frac{n}{(m,n)}} \rangle$ 中含有 (m, n) 个元素，

所以 $x^m = e$ 的解的个数不超过 $(m, n) \leq m$ ，

习题 36 设 G 是有限生成的交换群，

如果 G 的每个元素的阶都有限，试证明 G 是有限群，

证明： 设 $G = \langle a_1, a_2, \dots, a_n \rangle$ ， a_i 的阶为 m_i ，

则 $G = \{a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} \mid 0 \leq k_i \leq m_i, i=1, 2, \dots, n\}$ 是有限群，

习题 37 设 G 是循环群， H 是 G 的 n 阶子群，试证明 $H = \{a \in G \mid a^n = e\}$ ，

证明： 显然 H 包含于 $\{a \in G \mid a^n = e\}$ ，

若 m 是 n 的因数，则 H 有 m 阶子群，

若 c 属于 $\{a \in G \mid a^n = e\}$ ，则 c 的阶为 n 的因数，设为 m ，则 $\langle c \rangle$ 是 m 阶子群，

循环群的 m 阶子群是唯一的，

所以 $\langle c \rangle$ 是 H 的子群，从而 c 属于 H ， $\{a \in G \mid a^n = e\}$ 包含于 H ，

故 $H = \{a \in G \mid a^n = e\}$

习题 38 证明无限循环群的自同构群是 2 阶循环群；

n 阶循环群的自同构群是阶为 $\varphi(n)$ 的交换群，其中 $\varphi(n)$ 是欧拉函数，

证明： 设 φ 是循环群 $G = \langle a \rangle$ 的自同构，则 $\varphi(a)$ 是群 G 的生成元，

事实上，对属于 G 的任意 b ，存在属于 $\mathbb{Z}$ 的 r ，使得 $\varphi^{-1}(b) = a^r$ ，

从而 $b = \varphi(a^r) = (\varphi(a))^r$ ，

注意到，若属于 G 的 b 也是 G 的生成元，则映射 $\varphi: a^r \rightarrow b^r$ 是 G 的自同构，

根据上面的论述可知，循环群的自同构群是由生成元决定的，

无限循环群有两个生成元 a 和 a^{-1} ，因此自同构为 $\varphi_1: a^r \rightarrow a^r$ 和 $\varphi_2: a^r \rightarrow a^{-r}$ ，

无限循环群的自同构群是 2 阶循环群，

在 n 阶循环群 $G = \langle a \rangle$ 中，当且仅当 $(r, n) = 1$ 时， a^r 是 G 的生成元，

令 R 是小于 n 且与 n 互素的正整数集合，

因此自同构为 $\varphi_r: a^s \rightarrow a^{sr}$ ，其中 r 属于 R ，

即 n 阶循环群的自同构群是阶为 $\varphi(n)$ 的交换群，

习题 39 证明 12 阶循环群的自同构群同构于 K_4 ,

证明: 由上题知

12 阶循环群的自同构群 $\{\varphi_r: a^s \rightarrow a^{sr}, r \in R = \{1, 5, 7, 11\}\}$ 是 4 阶交换群,

且 φ_r 的阶都为 2,

所以 12 阶循环群的自同构群同构于 K_4 ,

习题 40 无限循环群的自同构群与 3 阶循环群的自同构群同构,

证明: 由习题 38 知

无限循环群的自同构群是 2 阶循环群, 3 阶循环群的自同构群是 2 阶循环群,

因此它们同构,

习题 41 求 $\text{Aut}(\mathbb{Z})$,

解: $\mathbb{Z}$ 是无限循环群, 由习题 38 知

自同构为 $\varphi_1: m \rightarrow m$ 和 $\varphi_2: m \rightarrow -m$, $\text{Aut}(\mathbb{Z}) = \{\varphi_1, \varphi_2\}$,