问题 (1): 在本系列问题中, 我们将证明, 对 $n \geq 3$, 当 $n \neq 6$, 则 $S_n \cong \mathrm{Aut}(S_n)$.

问题 (1.1): 对 $\phi \in \mathrm{Aut}(S_n)$,请证明: 若 $\phi(i, i+1) = (\alpha, \beta), \phi(i+1, i+2) = (\gamma, \delta)$, 则存在 a_i, a_{i+1}, a_{i+2}, 使得 $\phi(i, i+1) = (a_i, a_{i+1}), \phi(i+1, i+2) = (a_{i+1}, a_{i+2})$.

提示: 注意到对于对换 (ij) 和 (kl), 其乘积 $(ij)(kl)$ 的阶为 3 当且仅当 (ij),(kl) 形如 (ab),(bc).(此时其乘积 $(ab)(bc) = (bca)$ 是三轮换)

问题 (1.2): 对 $\phi \in \mathrm{Aut}(S_n)$,请证明: 若 ϕ 将对换映射为对换, 则 $\phi \in \mathrm{Inn}(G)$.

提示: 对 $\sigma \in S_n$, 其在轮换上的共轭作用是 $\sigma(i_1, i_2, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k))$. 利用 (1.2), 则存在 $a_1, \ldots, a_n$, 使得 $\phi(i, i+1) = (a_i, a_{i+1})$ 对所有 $1 \leq i \leq n-1$ 成立, 且 a_i 两两不同. 取 $\sigma \in S_n$, 使得 $\sigma(i) = a_i$, 则 $\phi(i, i+1) = \sigma(i, i+1)\sigma^{-1}$. 由于 $(i, i+1)$ 构成 S_n 的生成元, 故 ϕ 等于 σ 的共轭作用.

问题 (1.3): 当 $n \geq 3$, $2k \leq n$, 请证明: 当 $k > 1$, 则以下组合数等式只在 $k = 3$, $n = 6$ 时成立:

$$\frac{1}{(k-1)!}\binom{n-2}{2}\binom{n-4}{2}\cdots\binom{n+2-2k}{2} = k$$

提示: 等式的左侧是 S_{n-2} 中置换 $(12)(34)\ldots(2k-3, 2k-2)$ 所在共轭类的元素个数. 对 $3 \leq i \leq n-2$, 考虑对换 $(2, i)$ 在 $(12)(34)\ldots(2k-3, 2k-2)$ 上的共轭作用, 则至少存在 $n-3$ 个不同的置换存在于这一共轭类中. 因此若等式成立, 则 $n-3 \leq k$. 而 $2k \leq n$, 故 $n \leq 6$, 进而只需验证有限多个例子便足矣.

问题 (1.4): 当 $n \geq 3$, 若 C 是 S_n 中的共轭类, 满足:

(1) C 中元素都是 2 阶的.

(2) $|C| = \binom{n}{2}$

请证明: 当 $n \neq 6$, 则 C 是 S_n 中全体对换构成的共轭类.

提示: 注意到 S_n 中的二阶元一定形如若干不交对换的乘积, 因而由二阶元构成的共轭类一定是某个 $(12)(34)\ldots(2k-1, 2k)$ 所在的共轭类. 这样的共轭类中元素个数为 $\frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n+2-2k}{2}$. 而由对换构成的共轭类中元素个数为 $\binom{n}{2}$. 由 (1.3), 则 $n \neq 6$ 时对换的共轭类大小与其它二阶元构成的共轭类的大小都不相同.

问题 (1.5):请证明: 共轭作用诱导的映射 $S_n \to \mathrm{Aut}(S_n)$ 是群同构.

提示: 利用 (1.4), 说明 $n \neq 6$ 时,$f \in \mathrm{Aut}(S_n)$ 一定将对换映射为对换.

问题 (2): 在本系列问题中, 我们将研究阶为 pqr 的群的结构, 其中 $p < q < r$ 都是素数.

问题 (2.1): 若 G 是 pqr 阶群, 其中 $p < q < r$ 都是素数,请证明 如下事实:

(1) 若 G 不包含正规的 Sylow-p 子群, 则 G 至少包含 q 个 Sylow-p 子群.

(2) 若 G 不包含正规的 Sylow-q 子群, 则 G 至少包含 r 个 Sylow-q 子群.

(3) 若 G 不包含正规的 Sylow-r 子群, 则 G 至少包含 pq 个 Sylow-r 子群.

提示: 利用 Sylow 第三定理.

问题 (2.2):请证明: (2.1) 中的三种情况不会同时发生.

提示:G 的不同的 Sylow 子群间的交集一定是平凡的, 因此当上诉三种情况同时发生, 则 G 中的元素个数将会超过 pqr.

问题 (2.3):请证明: 若 G 是 pq 阶群, 其中 $p < q$ 都是素数, 则 G 一定包含一个正规的 Sylow-q 子群.

提示: 利用 Sylow 第三定理.

问题 (2.4):请证明: 对群 G 及素数 p, 若 P 是 G 的 Sylow-p 子群, 且存在 G 的正规子群 N, 使得 P 是 N 的正规子群, 则 P 是 G 的正规子群.

提示: 利用 Sylow 第二定理.

问题 (2.5):请证明: 若 G 是 pqr 阶群, 其中 $p < q < r$ 都是素数, 则 G 一定包含一个正规的 Sylow-r 子群.

提示: 由 (2.2), 若 G 不包含正规的 Sylow-r 子群, 则一定包含正规的 Sylow-p 子群或正规的 Sylow-q 子群. 考虑该子群的商群, 将问题化归为 G 只有两个素因数的情形.

问题 (3): 本系列问题中, 我们将证明 336 阶单群不存在.

补充说明: 证明 336 阶群不是单群是 2020 年北京大学某抽象代数班的期中考试试题, 因难度较高而在北京大学校内一时广为人知. 事实上, 证明 336 阶群不是单群的方法可以推广至所有 $p^3 - p$ 阶群上, 其中 p 是素数. 如果你想沉浸式地体验这道题的难度, 你可以选择不看下面的小问, 直接尝试证明 336 阶单群不存在.

问题 (3.1):请证明: 对 336 阶群 G, 若 G 不包含正规的 Sylow-7 子群, 则 G 恰有 8 个 Sylow-7 子群.

提示: 利用 Sylow 第三定理.

问题 (3.2): 对 336 阶单群 G, 记其全部 Sylow-7 子群的集合为 $\mathcal{P}$. 请证明: G 在 $\mathcal{P}$ 上的共轭作用诱导嵌入 $G \to S_8$.

提示: G 在 $\mathcal{P}$ 上的作用诱导同态 $\phi : G \to S_8$. 由 G 是单群, 则 $\mathrm{Ker}(\phi) = G$ 或 $\mathrm{Ker}(\phi) = 0$. 利用 Sylow 第二定理说明不可能有 $\mathrm{Ker}(\phi) = G$.

问题 (3.3): 对 336 阶单群 G, 通过 (3.2) 将 G 看作 S_8 的子群, 请证明 如下事实成立:

(1) G 中包含一个 7-轮换, 进而 $G \cap A_8 \neq 0$.

(2) $G \subset A_8$.

提示: 由 Cauchy 定理,G 中存在 7 阶元. 而 S_8 中的 7 阶元只有 7-轮换.7-轮换一定数域 A_8, 故 $G \cap A_8 \neq 0$. 注意到 $G \cap A_8$ 是 G 的正规子群. 由 G 是单群, 则要么 $G \cap A_8 = 0$, 要么 $G \cap A_8 = G$.

问题 (3.4): 记 H 是由 7-轮换 $(1, 2, 3, 4, 5, 6, 7)$ 生成的子群, 请证明:

$$N_{S_8}(H) = \left\{ f \in S_8 : \text{存在} a \in \mathbb{F}_7^\times, b \in \mathbb{F}_7, \text{使得} f(i) \equiv ai + b \mod 7, \text{且} f(8) = 8 \right\}$$

这里取 $\mathbb{Z}/7\mathbb{Z}$ 的代表元为 $1,2,3,4,5,7$ 而不是 $0,1,2,3,4,5,6$.

提示: 注意到 $(1,2,3,4,5,6,7)^k = (1 \mod 7, 1+k \mod 7, 1+2k \mod 7, \ldots, 1+6k \mod 7)$. 而对于 $\sigma \in S_8$, 则 $\sigma \in N_{S_8}(H)$ 当且仅当存在 $k \in \mathbb{Z}$, 使得 $\sigma(1,2,3,4,5,6,7)\sigma^{-1} = (\sigma(1), \sigma(2), \ldots, \sigma(7)) = (1,2,3,4,5,6,7)^k$.

问题 (3.5): 对 336 阶单群 G, 若 P 是 G 的 Sylow-7 子群, 请证明: $N_G(P)$ 不可能被嵌入到 $N_{A_8}(P)$ 中, 因此 G 不存在.

提示: 考虑 $f = (17)(26)(35)$, 则 $f \in N_{S_8}(P)$, 而 $f \notin A_8$, 进而 $N_{A_8}(P)$ 是 $N_{S_8}(P)$ 的真子群. 然而 $|N_G(P)| = |N_{S_8}(P)| = 42$.

问题 (3.6):请将 上述证明过程推广至阶为 $p^3 - p$ 的群, 其中 p 是素数.

问题 (4): 本系列问题中, 我们将证明 Sylow 第三定理的一个加强. 对 $p^n m$ 阶的群 G, 其中 m, p 互素, 记 r_s 是 G 中 p^s 阶群的数目, 其中 $s \leq n$, 则 $r_s \equiv 1 \mod p$.

问题 (4.1):请证明: 若 P 是 G 的 Sylow-p 子群, 对 $g \in G$, 若 g 是 p-阶元, 则下列条件等价:

(1) $P \subset C_G(g)$.

(2) $g \in Z(P)$.

提示: 若 $P \subset C_G(g)$, 则 $g \in N_G(P)$, 但是 P 是 $N_G(P)$ 的唯一 Sylow-p 子群.

问题 (4.2): 若 P 是 G 的 Sylow-p 子群, 记 X 是 G 中所有 p 阶元构成的集合, 考虑 P 在 X 上的共轭作用,请证明:$|X| \equiv -1 \mod p$.

提示: 由 (4.1), 当 $g \notin Z(P)$, 则 $C_P(g)$ 是 P 的真子群, 进而 g 在 P 共轭作用下的轨道长度被 p 整除, 故 $|X| \equiv Z(P) \cap X \mod p$.

问题 (4.3): 在 (4) 中的条件下,请证明:$r_1 \equiv 1 \mod p$.

提示: 每个 p 阶子群恰有 $p-1$ 个不同的 p 阶元, 利用 (4.2) 的结果.

问题 (4.4): 若 G 是 p^n 阶群, H 是 G 的真子群, 请证明: $H \neq N_G(H)$.

提示: 考虑 $N_G(H)$ 在 H 的所有 G-共轭上的共轭作用. 该作用的不同点数量一定被 p 整除, 而 H 是该作用的不同点, 故一定存在 $g \in G - N_G(H)$, 使得 gHg^{-1} 也是不动点, 即 $hgHg^{-1}h^{-1} = gHg^{-1}$ 对所有 $h \in N_G(H)$ 成立. 此时 $(g^{-1}hg)H(g^{-1}hg)^{-1} = H$ 对所有 $h \in N_G(H)$ 成立, 故 $g \in N_G(N_G(H))$, 请由此推出矛盾.

问题 (4.5): 在 (4) 中的条件下,请证明: 若 H 是 G 的 p^s 阶子群, 且 H 恰好被包含于 a 个 p^{s+1} 阶子群中, 则 $a \equiv 1 \mod p$.

提示: 若 K 是包含 H 的 p^{s+1} 阶子群, (4.4) 说明 H 是 K 的正规子群, 进而 $K \subset N_G(H)$, 故包含 H 的 p^{s+1} 阶子群数量等于商群 $N_G(H)/H$ 中的 p 阶子群数量.

问题 (4.6): 对 $n \geq 2$, 若 G 是 p^n 阶群,H_1, H_2 是 G 的两个不同的 p^{n-1} 阶子群,请证明如下事实成立:

(1) $H_1 \cap H_2$ 是 G 的 p^{n-2} 阶正规子群.

(2) $G/(H_1 \cap H_2) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

提示: 对于 (1), 由第 1 次习题课的 (2.3), 则 $[H_2 : H_1 \cap H_2] \leq p$, 进而 $[G : H_1 \cap H_2] \leq p^2$. 对于 (2), 你可以直接用到如下事实:$p^2$ 阶群只有 $\mathbb{Z}/p^2\mathbb{Z}$ 和 $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, 而前者只有唯一 p 阶子群.

问题 (4.7): 在 (4) 中的条件下, 请证明: 若 H 是 G 的 p^{s+1} 解子群, 且 H 恰好包含 b 个 p^s 阶子群, 则 $b \equiv 1 \mod p$.

提示: 利用 (4.6) 证明, 若 H_1, H_2 是 H 的两个不同的 p^s 阶子群, 则恰好有 $p+1$ 个 p^s 阶子群包含 $H_1 \cap H_2$. 进一步, 若 H_3 不在上述 $p+1$ 个子群之列, 则恰好有 p 个 p^s 阶子群包含 $H_1 \cap H_3$ 却不包含 $H_1 \cap H_2$, 因为同时包含 $H_1 \cap H_3$ 和 $H_1 \cap H_2$ 的子群只有 H_1.

问题 (4.8): 在 (4) 中的条件下, 请证明: $r_s \equiv 1 \mod p$.

提示: 利用 (4.5) 和 (4.7), 将 (4.3) 的结果归纳地提升至任意幂次.

问题 (5): 本系列问题中, 我们将研究 $\mathrm{GL}_n(\mathbb{F}_p)$ 的 Sylow-p 子群.

在下面的问题中, 你可以用到如下事实: 对 $V = \mathbb{F}_p^n$, 我们记 $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$. 则对 $g \in \mathrm{M}_n(\mathbb{F}_p)$, 有 $g \in \mathrm{GL}_n(\mathbb{F}_p)$ 当且仅当 $ge_1 \neq 0$, 且 $ge_i \notin \mathbb{F}_p ge_1 + \mathbb{F}_p ge_2 + \cdots + \mathbb{F} ge_{i-1}$ 对所有 $2 \leq i \leq n$ 成立.

问题 (5.1):请求出 $\mathrm{GL}_n(\mathbb{F}_p)$ 和 $\mathrm{B}_n(\mathbb{F}_p), \mathrm{U}_n(\mathbb{F}_p)$ 的阶数.

提示: 对 $A \in \mathrm{M}_n(F)$, 记 A 的列向量分别是 $v_1, v_2, \ldots, v_n$, 则 A 可逆当且仅当 $v_k \notin \mathbb{F}_p v_1 + \cdots + \mathbb{F}_p v_{k-1}$ 对所有 k 成立. 当 $v_1, \ldots, v_k$ 已经取定, 则 $v_{k+1} \notin \mathbb{F}_p v_1 + \cdots + \mathbb{F}_p v_k$ 的取法恰有 $p^n - p^k$ 种.

问题 (5.2):请求出 $\mathrm{GL}_n(\mathbb{F}_p)$ 的 Sylow-p 子群以及其 Sylow-p 子群的个数.

提示: 利用第 2 次习题课的 (3.8).

补充说明: 本问题说明, 我们可以构造地证明 $\mathrm{GL}_n(\mathbb{F}_p)$ 的 Sylow-p 子群的存在性. 它给出了证明一般的有限群 G 存在 Sylow-p 子群的一种证明方法. 考虑 G 在自身上的平移作用, 则得到嵌入 $G \to S_n$ (Caley 定理). 而 S_n 通过置换矩阵 $\sigma \mapsto w_\sigma$ 可以嵌入 $\mathrm{GL}_n(\mathbb{F}_p)$. 进而只需如下命题便可以得到 Sylow 第一定理: 对有限群 G 及子群 H, 若 G 存在 Sylow-p 子群, 则 H 也存在 Sylow-p 子群——这个命题可以这样证明: 考虑 H 在陪集空间 G/P 上的共轭作用, 则 gP 的轨道长度为 $H/H \cap gPg^{-1}$. 因此只需证明存在一条轨道, 其长度与 p 互素即可. 然而 $|G/P|$ 与 p 互素, 故而这样的轨道是必然存在的.

问题 (6): 本问题中, 我们将研究 $\mathrm{GL}_2(\mathbb{F}_p)$ 的共轭类.
在本问题中, 你可以用到如下的事实: 对 $g \in \mathrm{GL}_2(\mathbb{F}_p)$, 记 $f_g(t) = \det(tI - g) = t^2 + at + b$, 则:

(1) 若 $f_g(t)$ 在 $\mathbb{F}_p$ 中没有根, 则 g 共轭于 $\left(\begin{smallmatrix} 0 & -b \\ 1 & -a \end{smallmatrix}\right)$.

(2) 若 $f_g(t)$ 在 $\mathbb{F}_p$ 中有两个不同的根 x, y, 则 g 共轭于 $\left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$.

(3) 若 $f_g(t)$ 在 $\mathbb{F}_p$ 中有两个重根 x, 则 g 共轭于 $\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right)$ 或 $\left(\begin{smallmatrix} x & 1 \\ 0 & x \end{smallmatrix}\right)$.

进一步地, 你可以利用以下的事实: 对 $g \in \mathrm{GL}_2(\mathbb{F}_p)$, 若 $g \notin \mathbb{F}_p^\times I_2$, 则对 $A \in \mathrm{M}_n(\mathbb{F}_p)$, 有 $gA = Ag$ 当且仅当存在多项式 $f(X) \in \mathbb{F}_p[X]$, 使得 $A = f(g)$.
请你验证 下面的表格是正确的:

共轭类形式	共轭类个数	共轭类中元素个数
$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$p-1$	1
$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$p-1$	p^2-1
$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\frac{(p-1)(p-2)}{2}$	$p(p+1)$
$\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$	$\frac{p(p-1)}{2}$	$p(p-1)$