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 $\phi(i, i+1) = (a_i, a_{i+1}), \phi(i+1, i+2) = (a_{i+1}, a_{i+2})$.

证明. 注意到 $(i, i+1)(i+1, i+2) = (i, i+1, i+2)$ 是三轮换, 故 $(\alpha, \beta)(\delta, \gamma)$ 是三轮换, 进而容易看出. □

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 $\phi \in \mathrm{Inn}(G)$.

证明. 由 (1.1) 可以证明, 存在 $a_1, \ldots, a_n$, 使得 $\{a_1, \ldots, a_n\} = \{1, \ldots, n\}$, 使得 $f(i, i+1) = (a_i, a_{i+1})$ 对所有 i 成立. 此时取 $\tau \in S_n$ 满足 $\tau(i) = a_i$, 此时 $\tau^{-1}(a_i, a_{i+1})\tau = (i, i+1)$. 由 S_n 可以被对换生成, 故 f 等于 τ 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:

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

证明. 显然, 在 S_{n-2} 中考虑 $(2, i)$ 的共轭作用, 其中 $3 \leq i \leq n-2$ 至少存在 $n-3$ 个不同的共轭于 $(12)(34)\ldots(2k-3, 2k-2)$, 进而若上述等式成立, 则 $n - 3 \leq k$, 进而 $k \leq 3$ 而 $n \leq 6$. 此时, 通过直接的计算就可以得证. □

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 一定是 S_n 中全体对换构成的共轭类.

证明. 由 (1.3) 得到. □

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.

证明. 由 (1.4), 若 $f \in \mathrm{Aut}(S_n)$, 则 f 将全体对换构成的共轭类映为全体对换构成的共轭类, 进而由 (1.2), 则 $f \in \mathrm{Inn}(S_n)$. □

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.

证明. 利用 Sylow 第三定理得到. □

问题 (2.2):请证明: (2.1) 中的三种情况不会同时发生.

证明. 若这三种情况同时发生, 则 G 中至少包含 $q(p-1)$ 个不同的 p 阶元, $r(q-1)$ 个不同的 q 阶元, $pq(r-1)$ 个不同的 r 阶元. 但是 $q(p-1)+r(q-1)+pq(r-1) > pqr$ 矛盾, 故而三者不能同时成立. □

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.

证明. 由 Sylow 第三定理得到. □

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.

证明. 此时, 对 $g \in G$, 则 $gNg^{-1} = N$, 进而 $gPg^{-1} \subset N$ 也是 N 的 Sylow-p 子群. 由 P 在 N 中正规, 则 N 中只有唯一 Sylow-p 子群, 进而 $gPg^{-1} = P$. □

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.

证明. 由 (2), 若 G 不包含正规的 Sylow-r 子群, 则 G 包含一个正规的 Sylow-q 子群或一个正规的 Sylow-p 子群, 记为 N. 此时 $G/N = pr$ 或 qr, 故由 (2.3), 则 G/N 包含一个正规的 Sylow-r 子群. 取 G 的正规子群 H, 使得 H/N 是 G/N 的 Sylow-r 子群, 则 $|H| = pr$ 或 qr. 由 (2.3), 则 H 包含正规的 Sylow-r 子群 P. 由 (2.4), 则 P 在 G 中正规. □

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.

证明. 利用 Sylow 第三定理得到. □

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 $G \to S_8$.

证明. 由 (3.1) 立刻得到. □

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) $G \subset A_8$.

证明. 由 7 整除 336, 故 G 中包含一个 7 阶元, 而 S_8 中的 7 阶元只有 7-轮换, 故 G 中包含一个 7-轮换, 进而 $G \cap A_8 \neq 0$. 由 G 是单群, 而 $G \cap A_8$ 是 G 的正规子群, 故 $G \subset A_8$. □

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 $0,1,2,3,4,5,6$.

证明. 注意到 $(1,2,3,4,5,6,7)^k = (1, 1+k \mod 7, 1+2k \mod 7, \ldots, 1+6k \mod 7)$, 而 $f(1,2,3,4,5,6,7)f^{-1} = (f(1), f(2), \ldots, f(7))$, 故而容易看出. □

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.

证明. 由 (3.4), 则 $|N_{S_8}(P)| = 42$. 考虑 $f(i) = 6i + 1$, 则 $(1,7)(2,6)(3,5)(4) \in N_{S_8}(P)$ 而这是偶置换, 故 $|N_{A_8}(P)| = |N_{S_8}(P) \cap A_8| = 21$. 另一方面 $N_G(P) = 42$, 故而得证. □

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.

证明. 略. □

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) $g \in Z(P)$.

证明. 显然 (2) 可以推出 (1). 反之, 当 $P \in C_G(g)$, 则显然 $g \in N_G(P)$. 由 P 是 $N_G(P)$ 中唯一的 Sylow-p 子群, 故 $g \in P$, 进而得证. □

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:$|X| \equiv -1 \mod p$.

证明. 考虑 P 在 X 上的共轭作用, 记 $Y = X - (Z(P) \cap X)$, 则 Y 在 P 的作用下不变. 由 (4.1), 则 Y 中不存在 P 的不动点, 进而 $|Y| \equiv 0 \mod p$. 注意到 $Z(P) \cap X \cup \{e\}$, 是 $Z(P)$ 中所有 p 阶元生成的子群, 故 $|Z(p) \cap X \cup \{e\}| = p^r$, 进而 $Z(p) \cap X \equiv p^r - 1 \equiv -1 \mod p$ □

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

证明. G 的每个 p 阶子群都恰有 $p-1$ 个 p 阶元, 故由 (4.2), 则 $r_1(p-1) \equiv -1 \mod p$, 进而 $r_1 \equiv 1 \mod p$. □

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

证明. 考虑 $N_G(H)$ 在 H 的所有 G-共轭上的作用. 由 G 是 p^n 阶群, 则所有 H 的 G-共轭的数量为 $[G : N_G(H)]$ 也是 p 的幂. 注意到 H 是 $N_G(H)$ 共轭作用的不动点, 因而 $N_G(H)$ 的共轭作用至少还有 $p-1$ 个不动点. 进而存在 $g \in G - N_G(H)$ 使得 $hgHg^{-1}h^{-1} = gHg^{-1}$ 对所有 $h \in N_G(H)$ 成立, 此时 $(g^{-1}hg)H(g^{-1}hg)^{-1} = H$, 故 $g^{-1}hg \in N_G(H)$ 对所有 $h \in N_G(H)$ 成立, 进而 $g \in N_G(N_G(H))$. 此时, 若 $H = N_G(H)$, 则 $g \in N_G(H) = H$, 则矛盾. □

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 $a \equiv 1 \mod p$.

证明. 记 $N = N_G(H)$. 由 (4.4), 则所有包含 H 的 p^{s+1} 阶子群都被包含于 N, 进而这样的子群数量等于 N/H 中的 p 阶子群数量, 进而由 (4.3) 得到. □

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

证明. 由 (4.4), 则 H_1, H_2 都是正规的, 进而 $H_1 \cap H_2$ 也是正规的. 由第 1 次习题课的 (2.3), 此时 $H_2/H_1 \cap H_2 \to G/H_1$ 是单射, 则 $[H_2 : H_1 \cap H_2] \leq p$. 由 $H_1 \neq H_2$, 则 $|H_1 \cap H_2| = p^{n-2}$. 此时 $G/H_1 \cap H_2$ 是 p^2 阶群. 注意到 p^2 阶群只有 $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ 和 $\mathbb{Z}/p^2\mathbb{Z}$, 而后者只有一个 p 阶子群, 故而得到 (2). □

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 $b \equiv 1 \mod p$.

证明. 提示所述已经足够详细, 不再赘述. □

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

证明. 记 $H_1,\dots,H_{r_s}$ 是 G 的所有 p^s 阶子群, 其中 H_i 被包含在 a_i 个 p^{s+1} 阶子群中. 记 $N_1,\dots,N_{r_{s+1}}$ 是 G 的所有 p^{s+1} 阶子群, 其中 N_j 包含 b_j 个 p^s 阶子群. 则 $\sum\limits_{i=1}^{r_s} a_i = \sum\limits_{j=1}^{r_{s+1}} b_j$. 由 (4.5) 和 (4.7), 则 $r_s \equiv \sum\limits_{i=1}^{r_s} a_i \equiv \sum\limits_{j=1}^{r_{s+1}} \equiv r_{s+1} \mod p$. 故而由 (4.3) 得到. □

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 $e_1 = (1,0,\dots,0), e_2 = (0,1,\dots,0),\dots,e_n = (0,0,\dots,1)$. 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 $2 \le i \le n$ 成立.
问题 (5.1):<u>请求出</u> $\mathrm{GL}_n(\mathbb{F}_p)$ 和 $\mathrm{B}_n(\mathbb{F}_p), \mathrm{U}_n(\mathbb{F}_p)$ 的阶数.

证明. 由题前的事实 $|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{\frac{n(n-1)}{2}} \prod\limits_{k=1}^{n}(p^k-1)$. 而不难算出由 $|\mathrm{U}_n(\mathbb{F}_p)| = p^{\frac{n(n-1)}{2}}$, 而 $|\mathrm{B}_n(\mathbb{F}_p)| = p^{\frac{n(n-1)}{2}}(p-1)^n$. □

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

证明. 由 (5.1), 以及 $N_{\mathrm{GL}_n(K)}(\mathrm{U}_n(K)) = \mathrm{B}_n(K)$ 容易计算得出. □

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 $A = f(g)$.(我认为这一事实只在 $n = 2$ 时成立, 但我没有仔细验证)
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
$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\frac{(p-1)(p-2)}{2}$	$p(p+1)$
$\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$	$\frac{p(p-1)}{2}$	$p(p-1)$

证明. 只有第四行是非平凡的.$g = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$, 其中 $f(t) = t^2 + at + b$ 在 $\mathbb{F}_p$ 中没有根, 直接计算知 $g^2 + ag + bI_2 = 0$. 考虑 $L = \mathbb{F}_p I_2 + \mathbb{F}_p g$, 则 L 构成一个具有 p^2 个元素的域, 且 $|L \cap \mathrm{GL}_2(\mathbb{F}_p)| = |C_{\mathrm{GL}_2(\mathbb{F}_p)}(g)| = p^2 - 1$. 故 g 的共轭类中的元素个数为 $\frac{p(p-1)(p^2-1)}{p^2-1} = p(p-1)$. 为求这样共轭类的数目, 只需求在 $\mathbb{F}_p$ 中无根的首一二次多项式的数目.$\mathbb{F}_p$ 上的首一二次多项式共有 p^2 个. 而若 f 有根, 则 $f = (t-a)(t-b)$, 其中 $a, b \in \mathbb{F}_p$, 故这样的多项式有 $p^2 - p - \frac{p(p-1)}{2} = \frac{p(p-1)}{2}$ 个. □