群与 Galois 理论
作业 2

陈宏泰
清华大学数学科学系
cht24@mails.tsinghua.edu.cn

2025 年 10 月 22 日

目录

A. 对称群 $\mathfrak{S}_n$ 中的计算

A1)

解：由上课命题知, $\mathfrak{S}_n$ 可以由 $\{(1,k) \mid k=2,\cdots,n\}$ 或者 $\{(k,k+1) \mid k=1\cdots,n-1\}$ 生成. 于是有 $|S|_{\min} \leq n-1$.

下面说明 $|S|$ 不能小于等于 $n-2$: 假设 $|S|=n-2$, 那么可以定义集合 $N=\{1,2,\cdots,n\}$ 中的等价关系“$\sim$”:

$$i \sim j \Leftrightarrow \exists\, \sigma \in \langle S\rangle,\ \text{s.t.}\ \sigma(i)=j.$$

可知 $\mathfrak{S}_n$ 能够被 S 生成 $\Rightarrow$ 集合 N 仅有一个等价类. 于是考察 N 中的等价类.

任取 $i_1 \in N$, 如果 $\exists\,(i_1,i_2) \in S, i_1 \neq i_2 \in N$, 那么知 $i_1 \sim i_2$. 如果不存在, 那么 i_1 无法与其他元素置换, 那么知 N 有超过一个等价类, 矛盾. 如果是前一种情况, 则继续. 如果 $\exists\,(i_k,i_3) \in S, k=1,2, i_k \neq i_3 \in S$, 那么 $i_k \sim i_3$. 如果不存在, 那么 i_1,i_2 无法与其他元素置换, 那么知 N 有超过一个等价类, 矛盾. 以此类推, 如果出现不存在的情况, 结论成立. 如果都存在, 那么 i_1 的等价类中至多有 $(n-2)+1=n-1$ 个元素, 因为 S 中每个对换至多向等价类中增加一个元素. 那么 N 中仍然会剩余一个元素不在此等价类中, 即 N 中有超过一个等价类, 矛盾.

如果 $|S| \leq n-2$ 以上过程都能导出矛盾. 综上, $|S|$ 的最小值是 $n-1$. □

注：用图论的观点来看, $n-2$ 条线无法连接 n 个点并使之连通.

A2)

证明：假设 $|i_0-j_0|$ 与 n 互素, 不妨设 $i_0<j_0$, 设 $m=j_0-i_0$, 则 m 与 n 互素. 对换 (i_0,j_0) 可以写作 (i_0,i_0+m).

通过以下变换:

$$(1,2,\cdots,n)^{-k}(i_0,i_0+m)(1,2,\cdots,n)^k,$$

可以得到所有形如 $(i_0+k,i_0+k+m), k\in\mathbb{Z}$ 的对换, 其中可以利用 $i_0+k \equiv j \pmod n, j \in S$, 将 i_0+k 与 j 等同起来. 由于 m 与 n 互素, 存在整数 a 与 b, s.t. $am+bn=1$. 于是又可以通过

$$\begin{aligned}&(i_0+(a-1)m,i_0+am)(i_0+(a-2)m,i_0+(a-1)m)\cdots(i_0,i_0+m)\\&(i_0+m,i_0+2m)\cdots(i_0+(a-1)m,i_0+am),\end{aligned}$$

得到 $(i_0,i_0+am)=(i_0,i_0+1)$. 又可以通过

$$(1,2,\cdots,n)^{1-i_0}(i_0,i_0+1)(1,2,\cdots,n)^{i_0-1},$$

得到 $(1,2)$, 由上课命题知 $\{(1,2),(1,2,\cdots,n)\}$ 生成 $\mathfrak{S}_n$, 于是 $S_4=\{(i_0,j_0),(1,2,\cdots,n)\}$ 生成 $\mathfrak{S}_n$. □

A3)

证明： 假设 $\mathfrak{A}_n, n \geq 5$ 有两个不同的三循环 $\alpha = (i_1, i_2, i_3), \beta = (j_1, j_2, j_3)$.

如果 $\{i_1, i_2, i_3\} \cap \{j_1, j_2, j_3\} = \emptyset$, 那么由

$$\begin{aligned}\beta =&(i_1, j_1, j_2)(i_2, j_1, j_3)(i_3, j_1, j_3)\alpha(i_3, j_3, j_1)(i_2, j_3, j_1)(i_1, j_2, j_1)\\ =&((i_1, j_1, j_2)(i_2, j_1, j_3)(i_3, j_1, j_3))\alpha((i_1, j_1, j_2)(i_2, j_1, j_3)(i_3, j_1, j_3))^{-1},\end{aligned}$$

知 α 与 β 共轭.

如果 $\{i_1, i_2, i_3\} \cap \{j_1, j_2, j_3\} \neq \emptyset$, 且如果有一个相同的元素, 不妨设 $i_1 = j_1$, 那么由

$$\begin{aligned}\beta &= (i_3, j_3)(i_2, j_2)\alpha(i_2, j_2)(i_3, j_3)\\ &= ((i_2, j_2)(i_3, j_3))\alpha((i_2, j_2)(i_3, j_3))^{-1},\end{aligned}$$

知 α 与 β 共轭.

如果有两个相同的元素, 不妨设 $i_1 = j_1, i_2 = j_2$ 或者 $i_1 = j_1, i_2 = j_3$. 当 $i_1 = j_1, i_2 = j_3$ 时, 有

$$\begin{aligned}\beta &= (i_1, i_2)(i_3, j_2)\alpha(i_3, j_2)(i_1, i_2)\\ &= ((i_1, i_2)(i_3, j_2))\alpha((i_1, i_2)(i_3, j_2))^{-1},\end{aligned}$$

知 α 与 β 共轭. 当 $i_1 = j_1, i_2 = j_2$ 时, 由 $n \geq 5$ 知, 存在 $k \in \{1, 2, \cdots, n\} \backslash \{i_1, i_2, i_3, j_3\}$, 那么有

$$\begin{aligned}\beta &= (i_3, j_3, k)\alpha(i_3, k, j_3)\\ &= (i_3, j_3, k)\alpha(i_3, j_3, k)^{-1},\end{aligned}$$

知 α 与 β 共轭.

综上, $\mathfrak{A}_n, n \geq 5$ 中的任意两个三循环共轭. □

注： 可以直接通过 3-循环在 $\mathfrak{S}_n$ 共轭性质进行证明, 但需要注意共轭元是否在 $\mathfrak{A}_n$ 中. 如果不在其中, 则需要引入一个与 β 不交的对换来保证, 而由于 $n \geqslant 5$, 一定能取到这样的对换.

A4)

证明： 由课上命题已知, $\mathfrak{A}_5$ 可以由 3-循环子集生成. 下面说明任意一个 3-循环可以由双对换生成: 设 $\alpha = (i, j, k)$, 则 $\exists\, l \neq m \in \{1, 2, 3, 4, 5\} \backslash \{i, j, k\}$, 那么有

$$\alpha = (i, j)(j, k) = (i, j)(l, m)(l, m)(j, k) = ((i, j)(l, m))((l, m)(j, k)),$$

于是 $\mathfrak{A}_5$ 可以由双对换生成. □

A5)

证明： a) 如果 $y \in G$ 是一个 3 阶元素, 则 y 是一个 3-循环. 充分性: 不妨设 $y = (i, j, 5)$, 其中 $i \in \{1, 2\}, j \in \{3, 4\}$.($j \in \{1, 2\}, i \in \{3, 4\}$ 时同理) 则

$$xy = (12)(34)(i, j, 5) = (12)(k, j, 5, i) = (l, i, k, j, 5),$$

其中 $k \in \{1, 2\} \backslash \{i\}, l \in \{3, 4\} \backslash \{j\}$. 从而 xy 是一个 5-循环, $\mathrm{ord}(xy) = 5$.

必要性: 如果 y 的两个不动点不是一个在 $\{1, 2\}$ 中, 另一个在 $\{3, 4\}$ 中, 那么 y 的两个不动点要么都在 $\{1, 2\}$ 中, 要么都在 $\{3, 4\}$ 中. 不妨设 y 的两个不动点都在 $\{1, 2\}$ 中, 于是 y 与 (12) 交换, 那么由 $xy = (12)(34)y$, 知 $(xy)^5 = (12)^5((34)y)^5$. 显然 $(12)^5 = (12)$, $((34)y)^5 \neq (12)$. 于是 $(xy)^{-5} \neq 1$, $\mathrm{ord}(xy) \neq 5$, 矛盾.

b) 显然有 u 的阶为 2 $\Leftrightarrow u = (ij)(kl)$, 其中 i, j, k, l 互不相同. v 的阶为 3 $\Leftrightarrow v$ 为 3-循环. 由 a) 知

$$\mathrm{ord}(uv) = 5 \ \Leftrightarrow v \text{ 的两个不动点一个在 } \{i, j\} \text{ 中, 另一个在 } \{k, l\} \text{ 中.}$$

对 X 中元素计数, u 有 $\frac{C_5^2 C_3^2}{2} = 15$ 种取法, 而对于每个 u, v 有 $2 \times 2 \times 2 = 8$ 种取法, 故 X 中共有 $15 \times 8 = 120$ 个元素, $|X| = 120$.

c) 定义 $\mathbf{Aut}(G)$ 在 X 上的作用为:

$$\begin{aligned} &\mathbf{Aut}(G) \times X \to X \\ &\quad (\varphi, (u, v)) \mapsto \varphi \cdot (u, v) = (\varphi(u), \varphi(v)), \end{aligned}$$

由于 $\varphi \in \mathbf{Aut}(G)$ 是一个同构, 故 $\mathrm{ord}(\varphi(u)) = \mathrm{ord}(u)$,$\mathrm{ord}(\varphi(v)) = \mathrm{ord}(v)$,$\mathrm{ord}(\varphi(u)\varphi(v)) = \mathrm{ord}(\varphi(uv)) = \mathrm{ord}(uv)$. 于是 $\varphi \cdot (u, v) \in X$. $\forall\ \varphi, \psi \in \mathbf{Aut}(G)$, 有

$$(\varphi \cdot \psi) \cdot (u, v) = (\varphi\psi(u), \varphi\psi(v)) = \varphi \cdot (\psi \cdot (u, v)),$$

又 $\mathbf{Aut}(G)$ 中单位元 1, 满足 $1(u, v) = (u, v)$, 于是 $\mathbf{Aut}(G)$ 在 X 上的作用是群作用.

$\forall\ (u, v) \in X$, 若 $\varphi \cdot (u, v) = (u, v)$, 则 $\varphi(u) = u, \varphi(v) = v$. 考虑 $S = \langle u, v \rangle$, 由于 $u, v, uv \in S$ 的阶分别为 2,3,5, 故 $\mathrm{lcm}(2, 3, 5) = 30 \big| |S|$. 又 $|S| \big| |G|$, 而 $|G| = 60$, 故 $|S| = 30$ 或者 60. 知 S 是 G 的一个正规子群, 所以 v 的共轭类也在 S 中. 由 A3) 知, $\mathfrak{A}_5$ 中所有 3-循环构成一个共轭类, 故 S 包含所有 3-循环. 由于 3-循环生成 $\mathfrak{A}_5 = G$, 故 $S = G$. 于是 φ 在作用在 $S = G$ 上是恒等映射, 从而 $\mathbf{Aut}(G)$ 在 X 上的作用是自由的.

据此, 有 $|\mathbf{Aut}(G)| \leq |X| = 120$. 由于 $\mathbf{Aut}(G)$ 包含 $\mathfrak{S}_5$, 从而 $\mathbf{Aut}(G) = \mathfrak{S}_5$. □

注： 如果知道 B 题的结论, 则可以直接利用 $\mathfrak{A}_5$ 是单群与 Lagrange 定理来证明 A5)c).

A6)

证明： 令 $G = \mathfrak{A}_4$.

a) 假设 $x = (12)(34) \in G, y \in G$ 是一个 3-循环. 则 xy 是一个 3-循环. 不妨设 $y = (i, j, k)$, 其中 $i \neq j \in \{1, 2\}, k \in \{3, 4\}$.($i \neq j \in \{3, 4\}, k \in \{1, 2\}$ 时同理) 则

$$xy = (12)(34)(i, j, k) = (34)(12)(i, j)(j, k) = (34)(j, k) = (l, k, j),$$

其中 $l \in \{3, 4\}\backslash\{k\}$. 从而 xy 是一个 3-循环, $\mathrm{ord}(xy) = 3$.

b) 令 $X = \{(u, v) \in G \times G \mid u, v, uv\text{的阶分别为 }2,3,3\}$.

显然有 u 的阶为 $2 \Leftrightarrow u = (ij)(kl)$, 其中 i, j, k, l 互不相同. v 的阶为 $3 \Leftrightarrow v$ 为 3-循环. 由 a) 知 $\mathrm{ord}(uv) = 3$, 对 X 中元素计数, u 有 $C_4^2/2 = 3$ 种取法, 而对于每个 u, v 有 $2 \times C_4^3 = 8$ 种取法, 故 X 中共有 $3 \times 8 = 24$ 个元素, $|X| = 24$.

c) 定义 $\mathbf{Aut}(G)$ 在 X 上的作用为:

$$\begin{aligned} \mathbf{Aut}(G) \times X &\to X \\ (\varphi, (u, v)) &\mapsto \varphi \cdot (u, v) = (\varphi(u), \varphi(v)), \end{aligned}$$

由于 $\varphi \in \mathbf{Aut}(G)$ 是一个同构, 故 $\mathrm{ord}(\varphi(u)) = \mathrm{ord}(u)$,$\mathrm{ord}(\varphi(v)) = \mathrm{ord}(v)$,$\mathrm{ord}(\varphi(u)\varphi(v)) = \mathrm{ord}(\varphi(uv)) = \mathrm{ord}(uv)$. 于是 $\varphi \cdot (u, v) \in X$. $\forall\ \varphi, \psi \in \mathbf{Aut}(G)$, 有

$$(\varphi \cdot \psi) \cdot (u, v) = (\varphi\psi(u), \varphi\psi(v)) = \varphi \cdot (\psi \cdot (u, v)),$$

又 $\mathbf{Aut}(G)$ 中单位元 1, 满足 $1(u, v) = (u, v)$, 于是 $\mathbf{Aut}(G)$ 在 X 上的作用是群作用.

$\forall\ (u, v) \in X$, 若 $\varphi \cdot (u, v) = (u, v)$, 则 $\varphi(u) = u, \varphi(v) = v$, 考虑 $S = \langle u, v \rangle$, 由于 $u, v, uv \in S$ 的阶分别为 2,3,3, 故 $\mathrm{lcm}(2, 3) = 6 \big| |S|$. 又 $|S| \big| |G|$, 而 $|G| = 12$, 故 $|S| = 6$ 或者 12. 首先注意到 $1, u, v, v^2, uv, (uv)^2$ 互不相同, 而以 a) 中的 u, v 为例, 有

$$vu = (i, j, k)(12)(34) = (i, j)(j, k)(12)(34) = (i, j)(j, k, l)(12) = (i, j)(k, l, j, i) = (k, l, i),$$

其中 $l \in \{3, 4\}\backslash\{k\}$. 显然 $vu \neq uv$ 且 $vu \neq (uv)^2$. 于是 $|S| > 6$. 从而 $|S| = 12$, 则 $S = G$. 于是 φ 在作用在 $S = G = \mathfrak{A}_4$ 上是恒等映射, 从而 $\mathbf{Aut}(G)$ 在 X 上的作用是自由的.

据此, 有 $|\mathbf{Aut}(G)| \leq |X| = 24$. 由于 $\mathbf{Aut}(G)$ 包含 $\mathfrak{S}_4$, 从而 $\mathbf{Aut}(\mathfrak{A}_4) = \mathfrak{S}_4$. □

A7)

证明： 令 $G = \mathfrak{S}_4$.

a) 假设 $x = (12) \in G, y \in G$ 是一个 3 阶元素, 则 y 是一个 3-循环. 下面证明: xy 的阶为 4, 当且仅当 y 的不动点在 $\{1, 2\}$ 之中. 充分性: 不妨设 $y = (i, 3, 4)$, 其中 $i \in \{1, 2\}$.($y = (i, 4, 3)$ 时同理) 则

$$xy = (12)(i, 3, 4) = (j, i, 3, 4),$$

其中 $j \in \{1, 2\}\backslash\{i\}$. 从而 xy 是一个 4-循环, $\mathrm{ord}(xy) = 4$.

必要性: 如果 y 的不动点在 $\{1,2\}$ 中, 那么 y 的不动点在 $\{3,4\}$ 中. 不妨设 $y=(1,2,i)$, 其中 $i\in\{3,4\}$,($y=(2,1,i)$ 时同理) 则

$$xy=(12)(1,2,i)=(12)(12)(2,i)=(2,i),$$

那么由 $\mathrm{ord}(xy)=2$, 矛盾.

b) 令 $X=\{(u,v)\in G\times G \mid u,v,uv\text{的阶分别为 2,3,4}\}$.

显然有 u 的阶为 $2\Leftrightarrow u=(ij)$, 其中 i,j 互不相同. v 的阶为 $3\Leftrightarrow v$ 为 3-循环. 由 a) 知

$$\mathrm{ord}(uv)=4\ \Leftrightarrow v\text{ 的不动点在 }\{i,j\}\text{ 中}.$$

对 X 中元素计数, u 有 $C_4^2=6$ 种取法, 而对于每个 u, v 有 $2\times 2=4$ 种取法, 故 X 中共有 $6\times 4=24$ 个元素, $|X|=24$.

c) 定义 $\mathbf{Aut}(G)$ 在 X 上的作用为:

$$\begin{aligned}\mathbf{Aut}(G)\times X&\to X\\(\varphi,(u,v))&\mapsto\varphi\cdot(u,v)=(\varphi(u),\varphi(v)),\end{aligned}$$

由于 $\varphi\in\mathbf{Aut}(G)$ 是一个同构, 故 $\mathrm{ord}(\varphi(u))=\mathrm{ord}(u)$,$\mathrm{ord}(\varphi(v))=\mathrm{ord}(v)$,$\mathrm{ord}(\varphi(u)\varphi(v))=\mathrm{ord}(\varphi(uv))=\mathrm{ord}(uv)$. 于是 $\varphi\cdot(u,v)\in X$. $\forall\ \varphi,\psi\in\mathbf{Aut}(G)$, 有

$$(\varphi\cdot\psi)\cdot(u,v)=(\varphi\psi(u),\varphi\psi(v))=\varphi\cdot(\psi\cdot(u,v)),$$

又 $\mathbf{Aut}(G)$ 中单位元 1, 满足 $1(u,v)=(u,v)$, 于是 $\mathbf{Aut}(G)$ 在 X 上的作用是群作用.

$\forall\ (u,v)\in X$, 若 $\varphi\cdot(u,v)=(u,v)$, 则 $\varphi(u)=u,\varphi(v)=v$. 考虑 $S=\langle u,v\rangle$, 由于 $u,v,uv\in S$ 的阶分别为 2,3,4, 故 $\mathrm{lcm}(2,3,4)=12\big||S|$. 又 $|S|\big||G|$, 而 $|G|=24$, 故 $|S|=12$ 或者 24. 知 S 是 G 的一个正规子群, 所以 v 的共轭类也在 S 中. 而 $\mathfrak{S}_4$ 中所有 3-循环构成一个共轭类, 故 S 包含所有 3-循环. 又 $1,u,uv,(uv)^2,(uv)^3\in S$, 互不相同, 于是 $|S|>12$. 故 $|S|=24,S=G$. 于是 φ 在作用在 $S=G=\mathfrak{S}_4$ 上是恒等映射, 从而 $\mathbf{Aut}(G)$ 在 X 上的作用是自由的.

据此, 有 $|\mathbf{Aut}(G)|\le|X|=24$. 由于 $\mathbf{Aut}(G)$ 包含 $\mathfrak{S}_4$, 从而 $\mathbf{Aut}(\mathfrak{S}_4)=\mathfrak{S}_5$. □

A8)

证明：一方面, $\mathbf{Aut}(\mathfrak{S}_4)$ 包含 $\mathfrak{S}_4$ 的内自同构群 $\mathbf{Int}(\mathfrak{S}_4)$, 而 $\mathfrak{S}_4$ 的中心是一个平凡群, 故 $\mathfrak{S}_4\cong\mathbf{Int}(\mathfrak{S}_4)/Z(\mathfrak{S}_4)=\mathbf{Int}(\mathfrak{S}_4)\triangleleft\mathbf{Aut}(\mathfrak{S}_4)$.

另一方面, $\forall\ \varphi\in\mathbf{Aut}(\mathfrak{S}_4)$, 下面说明其将对换映射到对换: 设 $\sigma=(i,j)$ 是一个对换, 由 $\sigma^2=1$ 知, $\varphi(\sigma)^2=1$, 故 $\varphi(\sigma)$ 的可能类型只有三种: 单位元, 对换, 双对换. 如果 $\varphi(\sigma)$ 是单位元, 则 φ 不是单射, 矛盾. 如果 $\varphi(\sigma)$ 是双对换, 不妨设 $\varphi(\sigma)=(k,l)(m,n)$, 那么取

$$\rho=\begin{pmatrix}k&l&m&n\\i&j&p&q\end{pmatrix},$$

其中 $p,q\in\{1,2,3,4\}\backslash\{i,j\}$, 则有

$$\varphi(\rho\sigma\rho^{-1})=\varphi(\rho)\varphi(\sigma)\varphi(\rho)^{-1}=(i,j)(p,q),$$

但 $\rho\sigma\rho^{-1}=(k,l)$ 是一个对换, 故 σ 将所有对换映射到双对换. 但两者的数量不同, 与 φ 是自同构矛盾. 于是 $\varphi(\sigma)$ 是一个对换, 即得 φ 将对换映射到对换. 又由于对换生成 $\mathfrak{S}_4$, 故 φ 也将偶置换映射到偶置换, 所以 $\varphi\in\mathbf{Aut}(\mathfrak{A}_4)$. 于是 $\mathbf{Aut}(\mathfrak{S}_4)\subset\mathbf{Aut}(\mathfrak{A}_4)=\mathfrak{S}_4$.

综上, 有 $\mathbf{Aut}(\mathfrak{S}_4)=\mathfrak{S}_4$. $\square$

注： 对于所有 $n\geqslant 3, n\neq 6$ 的情况, 都可以使用以上的方法证明 $\mathbf{Aut}(\mathfrak{S}_4)=\mathbf{Aut}(\mathfrak{A}_4)=\mathfrak{S}_4$.

B. 交替群 $\mathfrak{A}_n$ $(n \geqslant 5)$ 是单群

B0)

解： $\mathfrak{A}_3$ 的正规子群有 $\{e\}, \mathfrak{A}_3$.

$\mathfrak{A}_4$ 的正规子群有 $\{e\}, \{e, (12)(34), (13)(24), (14)(23)\}, \mathfrak{A}_4$. □

B1)

证明： B1-1) 注意到

$$\tau = (34)(25)\sigma(25)(34) = ((34)(25))\sigma((34)(25))^{-1},$$

于是 σ 与 τ 在 $\mathfrak{A}_5$ 中共轭.

特别地, $\sigma\tau = (152)$ 是一个 3-循环.

B1-2) 注意到

$$\tau = (123)\sigma(123) = (123)\sigma(123)^{-1},$$

于是 σ 与 τ 在 $\mathfrak{A}_5$ 中共轭.

特别地, $\tau\sigma^2 = (253)$ 是一个 3-循环.

B1-3) 只需要证明 N 中有一个 3-循环即可, 由 $\mathfrak{A}_5$ 中所有 3-循环共轭可知 N 包含所有 3-循环. 而 $\mathfrak{A}_5$ 中的元素只有单位元, 3-循环, 双对换, 5-循环四种可能的类型. 由 N 非平凡可知, 如果 N 中有一个 3-循环, 结论成立. 如果 N 中有一个双对换, 由 B1-1) 知 N 中有一个 3-循环, 结论成立. 如果 N 中有一个 5-循环, 由 B1-2) 知 N 中有一个 3-循环, 结论成立. 综上, N 包含所有的 3-循环, 从而, $\mathfrak{A}_5$ 是单群。 □

B2)

证明： B2-1) 对于 $\mathfrak{A}_5$ 中单位元 1, 共轭类元素个数为 1. 对于 3-循环, 由 A3) 知共轭类元素个数为 $C_5^3 \times 2 = 20$.

对于双对换, 任取两个不同的双对换 $\sigma = (i_1, i_2)(i_3, i_4), \tau = (j_1, j_2)(j_3, j_4)$, 取

$$\rho = \begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 \\ j_1 & j_2 & j_3 & j_4 & j_5 \end{pmatrix}$$

其中 i_5, j_5 分别为 $\{1,2,3,4,5\} \backslash \{i_1, i_2, i_3, i_4\}, \{1,2,3,4,5\} \backslash \{j_1, j_2, j_3, j_4\}$, 则 $\tau = \rho\sigma\rho^{-1}$. 如果 ρ 是奇置换, 则取 $\rho' = (i_1, i_2)\rho$, 则 ρ' 是偶置换, 且 $\tau = \rho'\sigma(\rho')^{-1}$; 如果 ρ 是偶置换, 则直接取 $\rho' = \rho$. 于是 σ 与 τ 在 $\mathfrak{A}_5$ 中共轭. 于是双对换构成一个共轭类. 对于双对换, 共轭类有 $\frac{C_5^2 C_3^2}{2} = 15$ 个元素.

对于 5-循环, 共轭类元素个数为 $(5-1)! = 24$. 设 $\tau = (12345), \sigma$ 是两个不同的 5-循环, 则存在 $\rho \in \mathfrak{S}_5$, 使得 $\sigma = \rho\tau\rho^{-1} = (\rho(1), \rho(2), \rho(3), \rho(4), \rho(5))$. 可知 σ 与 τ 在 $\mathfrak{A}_5$ 中共轭的充

分必要条件是 ρ 的逆序数为偶数, 同时, 这样的 ρ 有 60 个, 生成的 σ 有 $60/5=12$ 个. 同理可知对应 ρ 的逆序数为奇数的 5-循环 ς 也为一个共轭类. 这两个共轭类的元素数量都为 12.

综上, $\mathfrak{A}_5$ 的共轭类有 5 个, 并且每个共轭类中的元素个数分别为 1,12,12,15 和 20.

B2-2) 如果子群 $N \subset \mathfrak{A}_5$ 在 $\mathfrak{A}_5$ 的共轭下不变, 那么共轭类要么全部包含在 N 中, 要么全部不包含在 N 中. 由 B2-1) 知, $\mathfrak{A}_5$ 的共轭类大小分别为 1,12,12,15,20. 进行组合, 有 $|N|$ 可能的取值为 1,13,16,21,25,28,33,36,40,45,48 和 60

B2-3) 假设 N 是 $\mathfrak{A}_5$ 的一个非平凡正规子群.

由 B2-2) 知 $|N|$ 的可能取值为 13,16,21,25,28,33,36,40,45 和 48. 由于 N 是 $\mathfrak{A}_5$ 的子群, 故 $|N|\big|60$. 于是 $|N|$ 的可能取值为 2,3,4,5,6,10,15,20 和 30. 综上, N 的阶数没有可能的取值, 故 $\mathfrak{A}_5$ 没有非平凡子群, $\mathfrak{A}_5$ 是单群. $\square$

B3)

证明： B3-1)

如果存在 $\sigma \in N-\{1\}$, 使得 $\sigma(n)=n$, 可以将 σ 看作 $\mathfrak{A}_{n-1}$ 中的一个元素. $\forall\ \rho \in \mathfrak{A}_{n-1}$, 由 $\mathfrak{A}_{n-1} \subset \mathfrak{A}_n$ 知, 可以将 ρ 看作 $\mathfrak{A}_n$ 中的一个元素, 其中 $\rho(n)=n$.

考虑集合 $S_n=\{\rho\sigma^k\rho^{-1} \mid \sigma \neq 1, k \in \mathbb{Z}, \rho \in \mathfrak{A}_{n-1}\} \subset \mathfrak{A}_{n-1}$. 容易验证, S_n 是 $\mathfrak{A}_{n-1}$ 的一个正规子群. 由 $\mathfrak{A}_{n-1}$ 的单群性质, 知 $S_n=\mathfrak{A}_{n-1}$. 同时, 由于 N 是 $\mathfrak{A}_n$ 的正规子群, $\rho\sigma\rho^{-1} \in N$, 从而 $S_n \subset N$. 于是 $S_n=\mathfrak{A}_{n-1}$ 是 N 的子群.

而 $\forall\ k \in \{1,2,\cdots,n-1\}, \exists\ \varsigma \in \mathfrak{A}_{n-1}, \text{s.t. } \varsigma(k)=k$, 因为所有 3-循环在 $\mathfrak{A}_{n-1}$ 中. 用完全相同的方法可以证明, $S_k=\{\varsigma \mid \varsigma(k)=k\} \simeq \mathfrak{A}_{n-1} \subset N$ 是 N 的子群. 于是知道 $\mathfrak{A}_n$ 中的每个 3-循环都在 N 中, 从而 $N=\mathfrak{A}_n$.

提示： n 只是一个 symbol.

B3-2)

注意到 $\tau\sigma\tau^{-1}\sigma \in N$

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

而由 B3-1) 知, 不存在 $\rho \in N-\{1\}$, 使得 $\rho(n)=n$. 所以 $\tau\sigma\tau^{-1}\sigma=1$.

B3-3)

首先，由 B3-1) 知，不存在 $k \in \{1,2,\cdots,n\}$，使得 $\sigma(k)=k$. 又由于 B3-2) 知 $\tau\sigma\tau^{-1}\sigma=1$,

考虑 σ^2, 如果 $\exists\ m \notin \{i,j,n,\sigma(n)\}, \text{s.t. } \sigma(m) \notin \{i,j,n,\sigma(n)\}$, 那么

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

那么, $\sigma^2(m)=\tau^{-1}(m)=m$, 得出 σ^2 有不动点, 即 $\sigma^2=1$.

如果 $\forall\ m \notin \{i,j,n,\sigma(n)\}, \sigma(m) \in \{i,j,n,\sigma(n)\}$, 并且容易观察到此时 $n \leqslant 7$(并不需要用到). 那么由于 $n \geqslant 6$, 必定 $\exists\ m \notin \{i,j,n,\sigma(n)\}, \text{s.t. } \sigma(m) \neq n$. 那么取 $i',j', \text{s.t. } m,\sigma(m) \notin \{i',j'\}$. 那么归为上一种情况, 知 $\sigma^2=1$.

由此可知, $\sigma^{-1}\tau\sigma\tau^{-1}=1$, 于是有 $\tau\sigma=\sigma\tau$. 固定 i,j 后, 有

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

可知 $\sigma(i),\sigma(j)\in\{i,j,n,\sigma(n)\}$. 显然有 $\sigma(i)\neq i,\sigma(n)$, $\sigma(j)$ 同理. 而如果 $\sigma(i)=n$, 那么 $\tau\sigma(i)=\tau(n)=\sigma(n)=\sigma(j)$, 矛盾. 故 $\sigma(i)=j$, 同理 $\sigma(j)=i$, 即 $\sigma:\{i,j\}\to\{i,j\}$.

注：做法过于多样.

B3-4)

由于 B3-3), $\sigma:\{i,j\}\to\{i,j\}$, 由于 $n\geqslant 6$, 可知一定存在 $j'\in\{1,2,\cdots,n\}\backslash\{i,j,n,\sigma(n)\}$, 同样有 $\sigma:\{i,j'\}\to\{i,j'\}$, 可知 $\sigma(i)=i,\forall i\notin\{n,\sigma\}$, 故 $\sigma=\{n,\sigma(n)\}$, 从而矛盾.

综上, $\mathfrak{A}_\mathfrak{n}$ 是单群.

□

B4)

证明：考虑 $G\cap\mathfrak{A}_n$, 则 $\forall\, g\in G\cap\mathfrak{A}_n,\forall\,\sigma\in\mathfrak{A}_n$, 有

$$\sigma g\sigma^{-1}\in G,\quad \sigma g\sigma^{-1}\in\mathfrak{A}_n,$$

则 $G\cap\mathfrak{A}_n$ 是 $\mathfrak{A}_n$ 的一个正规子群. 由 $\mathfrak{A}_n$ 的单群性质, 知 $G\cap\mathfrak{A}_n=\{1\}$ 或者 $\mathfrak{A}_n$.

如果 $G\cap\mathfrak{A}_n=\mathfrak{A}_n$, 则 $\mathfrak{A}_n\subset G$, $|G|\geqslant|\mathfrak{A}_n|=\frac{1}{2}n!$. 又由 $|G|\big||\mathfrak{S}_n|$ 知, $G=\mathfrak{A}_n$. 如果 $G\cap\mathfrak{A}_n=\{1\}$, 则 G 中所有非单位元元素都是奇置换, 故 $|G|\leqslant 2$, 否则两个奇置换的乘积为偶置换. 由于 G 非平凡, 故 $|G|=2$, 则 $G=\{1,\tau\}$, 其中 τ 是一个奇置换. $\forall\,\sigma\in\mathfrak{S}_n$, 有

$$\sigma\tau\sigma^{-1}\in G.$$

因为 τ 是奇置换, 故 $\sigma\tau\sigma^{-1}$ 也是奇置换, 于是 $\sigma\tau\sigma^{-1}=\tau$. 由此可知 τ 与 $\mathfrak{S}_n$ 中所有元素交换, 故 τ 在 $\mathfrak{S}_n$ 的中心中. 由于 $n\geqslant 3$, 故 $\mathfrak{S}_n$ 的中心为平凡群, 则 $\tau=1$, 矛盾.

综上, $G=\mathfrak{A}_n$. □

B5)

证明：首先有

$$((12)(34))((13)(24))=(14)(23),$$
$$((12)(34))((14)(23))=(13)(24),$$
$$((13)(24))((14)(23))=(12)(34).$$

于是 $(12)(34),(13)(24),(14)(23)$ 在 N 中乘法封闭且阶都为 2. 故 N 是 $\mathfrak{S}_n$ 的子群. 由于 $\mathfrak{S}_n$ 中的共轭作用保持置换的型不变, 而 N 中的非单位元元素都是 (2,2)-型置换, 故 N 在 $\mathfrak{S}_n$ 的共轭作用下不变, 于是 N 是 $\mathfrak{S}_n$ 的正规子群. $N\lhd\mathfrak{A}_4$ 同理可证.

考虑 $\mathfrak{S}_4$ 在集合

$$X = \{\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}$$

上的作用, 定义 π 在 X 上的作用为: $\pi \cdot \{\{a,b\},\{c,d\}\} = \{\{\pi(a),\pi(b)\},\{\pi(c),\pi(d)\}\}$.

这是对 X 中 3 个元素的置换, 因此得到一个群同态 $\varphi : \mathfrak{S}_4 \to \mathfrak{S}_3$. 由于 $\mathfrak{S}_3$ 能被一个 2-循环和一个 3-循环生成, 而 $\varphi((12)) = (\{\{1,4\},\{2,3\}\},\{\{1,3\},\{2,4\}\})$, $\varphi((123)) = (\{\{1,2\},\{3,4\}\},\{\{1,4\},\{2,3\}\},\{\{1,3\},\{2,4\}\})$, 这两个 3-循环能够生成 $\mathfrak{S}_3$, 故 φ 是满同态.

下面求 $\ker\varphi$. 容易观察到 φ 将 $\mathfrak{S}_4$ 中相同的型映到 $\mathfrak{S}_3$ 中相同的型上. 因此, 通过计算, $\ker\varphi$ 中元素的型只能是 (1),(2,2). 显然, φ 的核中包含单位元和所有 (2,2)-型置换, 即 $\ker\varphi = N$.

由第一同构定理, 有 $\mathfrak{S}_4/N \simeq \mathfrak{S}_3$. □

注：可以定义自然的群同态 φ:

$$\begin{aligned} \mathfrak{S}_3 &\to \mathfrak{S}_4/N \\ \sigma &\mapsto \sigma N. \end{aligned}$$

再证明这是一个群同构.

B6)

证明：考虑 $\mathfrak{S}_n$ 作用在左陪集集合 $\mathfrak{S}_n/H$ 上, 定义作用为:

$$\begin{aligned} \mathfrak{S}_n \times \mathfrak{S}_n/H &\to \mathfrak{S}_n/H \\ (\sigma, \tau H) &\mapsto \sigma\cdot\tau H = (\sigma\tau)H, \end{aligned}$$

这是一个群作用. 由此得到一个群同态 $\varphi : \mathfrak{S}_n \to \mathfrak{S}_{|\mathfrak{S}_n/H|}$. 由于 $|\mathfrak{S}_n/H| = \frac{|\mathfrak{S}_n|}{|H|} = \frac{n!}{|H|} = d$, 故 φ 可以看作 $\mathfrak{S}_n \to \mathfrak{S}_d$ 的一个群同态.

下面求 $\ker\varphi$. $\forall\ \sigma \in \ker\varphi$, 有 $\sigma\cdot\tau H = \tau H, \forall\ \tau H \in \mathfrak{S}_n/H$, 则 $\sigma\tau H = \tau H$, 即 $\tau^{-1}\sigma\tau \in H, \forall\ \tau \in \mathfrak{S}_n$. 取 $\tau = 1$, 则 $\sigma \in H$. 于是 $\ker\varphi \subset H$, 从而 $\ker\varphi < H$.

我们熟知群同态的核为正规子群, 所以由 B5) 知 $\ker\varphi \in \{1, \mathfrak{A}_n, \mathfrak{S}_n\}$. 又由 $H \neq \mathfrak{A}_n, \mathfrak{S}_n$, 所以 $\ker\varphi = 1$. 从而 φ 是单映射, 推出 $d \geqslant n$. □

B7)

证明：构造地, 定义群同态 φ:

$$\begin{aligned} \mathfrak{S}_n &\to \mathfrak{A}_{n+2} \\ \sigma &\mapsto \begin{cases} \sigma, & \text{如果 } \sigma \text{ 是偶置换}, \\ \sigma(n+1, n+2), & \text{如果 } \sigma \text{ 是奇置换}. \end{cases} \end{aligned}$$

容易验证这的确是一个单的群同态.

假设存在这样的单同态 $\varphi : \mathfrak{S}_n \to \mathfrak{A}_{n+1}$, 知 $\mathfrak{S}_n$ 可以视作 $\mathfrak{A}_{n+1}$ 的一个子群, 故 $|\mathfrak{S}_n| \big| |\mathfrak{A}_{n+1}|$. 推出 $2 \mid n+1$, 从而当 n 为偶数时不成立. 当 $n = 3$ 时, $|\mathfrak{S}_3| = 6, |\mathfrak{A}_4| = 12$, 但是 $\mathfrak{A}_{n+1}$ 没有阶为 6 的子群, 矛盾.

记 $G = \varphi(\mathfrak{S}_n)$, 考虑群同态 ψ:

$$\mathfrak{A}_{n+1} \to \mathfrak{A}_{n+1}/G$$
$$\sigma \mapsto \sigma G$$

由于 $|\mathfrak{A}_{n+1}| = \frac{1}{2}(n+1)!$, $|\mathfrak{A}_{n+1}/G| = \frac{n+1}{2}$, 知 ψ 一定不是单同态. 于是 $\ker\psi \neq 1$, 又 $\ker\psi$ 是 $\mathfrak{A}_{n+1}$ 的正规子群, 故 $\ker\psi = 1$ 或者 $\mathfrak{A}_{n+1}$. 于是 $\ker\psi = \mathfrak{A}_{n+1}$. 由此得到 $\mathfrak{A}_{n+1} \subset G$, 矛盾.

所以不存在这样的单同态 $\varphi : \mathfrak{S}_n \to \mathfrak{A}_{n+1}$. □