0.1 有限单群

定义 0.1 (有限单群)

若有限群 G 无非平凡的正规子群, 则称 G 为**有限单群**.

定理 0.1

设 G 为 Abel 群且 $G \neq \{e\}$,e 为 G 的幺元, 则 G 为单群的充分必要条件是 G 的阶为素数. 这时 G 必为循环群.

证明 由命题???? Abel 群 G 的任何子群都是 G 的正规子群, 故 Abel 群 G 为单群当且仅当 G 无非平凡子群.

若 G 是有限阶的, 当 G 的阶为素数时, 由命题??知 G 只有平凡子群. 当 G 无非平凡子群时, 若 G 的阶不是素数, 又 $G \neq \{e\}$, 故 $|G|$ 是不为 1 的合数. 由因式分解定理知存在素数 p 以及正整数 m, l, 使 $|G| = p^l m$ 且 $(p, m) = 1$. 从而 m, l 不同时为 1, 否则与 $|G|$ 不为素数矛盾! 故 $|G| > p$. 由 Sylow 第一定理知 G 中一定有 p 阶子群 H, 而 $1 < p < |G|$, 故 H 必是 G 的非平凡子群, 矛盾! 因此 G 无非平凡子群当且仅当 G 的阶为素数. 此时, 由命题??知 $\forall a \in G$ 且 $a \neq e$ 有 $G = \langle a \rangle$.

若 G 是无限阶的, 则 $\langle a \rangle \lhd G(\forall a \in G, a \neq e)$. 若 $\langle a \rangle$ 是有限阶的, 则 $\langle a \rangle$ 是非平凡的. 若 $\langle a \rangle$ 是无限阶的, 则 $\langle a^2 \rangle$ 是非平凡的, 因为 $a, -a \notin \langle a^2 \rangle$. 即任何无限阶的 Abel 群都有非平凡的正规子群. 故此时 G 必不是单群.

□

命题 0.1

对任意 r 轮换 $(i_1 i_2 \cdots i_r)$ 和 $\sigma \in S_n$, 都有

$$\sigma\left(i_1 i_2 \cdots i_r\right) \sigma^{-1} = \left(\sigma\left(i_1\right) \sigma\left(i_2\right) \cdots \sigma\left(i_r\right)\right).$$

证明 对 $\forall l \in \{1, 2, \cdots, n\}$, 若 $l \notin \{i_1, i_2, \cdots, i_r\}$, 则

$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1}(\sigma(l)) = \sigma(i_1 i_2 \cdots i_r)(l) = \sigma(l) = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r))(\sigma(l)).$$

若 $l \in \{i_1, i_2, \cdots, i_r\}$, 设 $l = i_j, j \in \{1, 2, \cdots, r\}$, 则

$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1}(\sigma(i_j)) = \sigma(i_1 i_2 \cdots i_r)(i_j) = \sigma(i_{j+1}) = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r))(\sigma(i_j)),\ j = 1, 2, \cdots, r-1;$$
$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1}(\sigma(i_r)) = \sigma(i_1 i_2 \cdots i_r)(i_r) = \sigma(i_1) = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r))(\sigma(i_r)).$$

故

$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1}(\sigma(l)) = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r))(\sigma(l)),\ \forall l \in \{i_1, i_2, \cdots, i_r\}.$$

即

$$\sigma(i_1 i_2 \cdots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r)).$$

□

定理 0.2

(1) 当 $n \geqslant 3$ 时,A_n 由所有的 3 轮换生成, 即 $A_n = \langle\{(ijk)\}\rangle$;

(2) 当 $n \geqslant 5$ 时, 任意 3 轮换 (ijk) 在 A_n 中的共轭类由所有的 3 轮换构成, 即 $C_{(ijk)} = \{(i'j'k')\}$.

证明

(1) 由推论??知 $a \in A_n$ 当且仅当 a 可表示为偶数个对换之积. 由推论??知

$$\langle\{(ijk)\}\rangle = \{(i_1 j_1 k_1)\cdots(i_m j_m k_m) \mid i_s, j_s, k_s \in \{1, 2, \cdots, n\}, 1 \leqslant s \leqslant m, m \in \mathbf{N}\}.$$

设 i, j, k, l 且互不相等. 由

$$(ij)(ij) = \mathrm{id}, \quad (ij)(ik) = (ikj),$$

$$(ik)(jl)=(ik)(ij)(ij)(jl)=(ijk)(jli)$$

知 A_n 中元素都可写成 3 轮换之积, 因此 $A_n \subseteq \langle\{(ijk)\}\rangle$.

设 $(i_1j_1k_1)\cdots(i_mj_mk_m)\in\langle\{(ijk)\}\rangle$, 则由定理**????**知

$$(i_sj_sk_s)=(i_sk_s)(i_sj_s),\quad s=1,2,\cdots,m.$$

故 $(i_1j_1k_1)\cdots(i_mj_mk_m)$ 可写成偶数个对换之积, 故 $(i_1j_1k_1)\cdots(i_mj_mk_m)\in A_n$. 因此 $\langle\{(ijk)\}\rangle\subseteq A_n$. 故 $A_n=\langle\{(ijk)\}\rangle$.

(2) $\forall\sigma\in S_n$, 由命题 0.1知

$$\sigma(ijk)\sigma^{-1}=(\sigma(i)\sigma(j)\sigma(k)). \tag{1}$$

于是 $C_{(ijk)}\subseteq\{(i'j'k')\}$. 反之, 对任意 3 轮换 $(i'j'k')$, 当 $n\geqslant 5$ 时, 首先 $\exists\sigma\in S_n$, 使 $\sigma(i)=i',\sigma(j)=j',\sigma(k)=k'$. 若 $\sigma\in A_n$, 则由(1)式可得

$$(i'j'k')=(\sigma(i)\sigma(j)\sigma(k))=\sigma(ijk)\sigma^{-1}\in C_{(ijk)}.$$

若 $\sigma\notin A_n$, 由 $n\geqslant 5$ 有 $i_1,i_2\notin\{i,j,k\}$. 故由推论**??**知 $\sigma(i_1i_2)\in A_n$. 再由命题 0.1知

$$(i'j'k')=(\sigma(i)\sigma(j)\sigma(k))=((\sigma(i_1i_2)(i))(\sigma(i_1i_2)(j))(\sigma(i_1i_2)(k)))=\sigma(i_1i_2)(ijk)(\sigma(i_1i_2))^{-1}\in C_{(ijk)}.$$

即仍有 $(i'j'k')\in C_{(ijk)}$. 综上知 $C_{(ijk)}=\{(i'j'k')\}$.

□

定理 0.3

当 $n\geqslant 5$ 时,A_n 是非 Abel 有限单群.

证明 对 $\alpha\in S_n$, 令 $\bar F_\alpha=\{j\mid\alpha(j)\neq j\}$. 显然有

(1) $\bar F_\alpha=\{i,j\}$ 当且仅当 $\alpha=(ij)$;

(2) $\bar F_\alpha=\{i,j,k\}$ 当且仅当 $\alpha=(ijk)$或$(ijk)^{-1}$;

(3) 对 $\forall\alpha\in A_n$ 且 $\alpha\neq\mathrm{id}$, 又由推论**??**知 α 可写成偶数个对换之积, 从而一定有 $|\bar F_\alpha|\geqslant 3$.

设 $H\lhd A_n$ 且 $H\neq\{\mathrm{id}\}$. 取 $\tau\in H$, 使

$$|\bar F_\tau|=\min\{|\bar F_\alpha|\mid\alpha\in H,\alpha\neq\mathrm{id}\}. \tag{2}$$

显然 $|\bar F_\tau|\geqslant 3$. 若 $|\bar F_\tau|=3$, 则 τ 是 3 轮换. 显然 $\tau\in H$, 由正规子群定义和定理**????**知

$$\alpha\tau\alpha^{-1}\in H,\ \forall\alpha\in A_n\implies C_\tau=\{\alpha\tau\alpha^{-1}\mid\alpha\in A_n\}\subseteq H.$$

再由定理 0.2知

$$A_n=\langle\{(ijk)\}\rangle=C_\tau\subseteq H,$$

故 $H=A_n$. 这就证明了 A_n 为有限单群,A_n 的阶不是素数, 由定理 0.1知 A_n 不是 Abel 群.

若 $|\bar F_\tau|>3$. 由定理**????**, 可将 τ 分解为不相交轮换之积, 分两种情况讨论. 一种在分解中只出现对换, 另一种在分解中有长度大于 2 的轮换.

1. 若 τ 可分解为互不相交的对换之积, 又由最开始得到的情况 (1)知 τ 不可能是对换, 故可设 $\tau=(i_1i_2)(i_3i_4)\cdots$ 且 $i_1,i_2,i_3,i_4,\cdots$ 互不相同. 由 $n\geqslant 5$ 有 $j\neq i_1,i_2,i_3,i_4$, 令 $\phi=(i_3i_4j)$, 则由推论**??**知 $\phi\in A_n$. 由 $H\lhd A_n$ 有 $\tau_1=\tau^{-1}(\phi\tau\phi^{-1})\in H$. 于是由命题 0.1可得

$$\tau_1=(\tau^{-1}\phi\tau)\phi^{-1}=(\tau^{-1}(i_3)\tau^{-1}(i_4)\tau^{-1}(j))(i_4i_3j)=(i_4i_3\tau^{-1}(j))(i_4i_3j).$$

若 $j\notin\bar F_\tau$, 即 $\tau(j)=\tau^{-1}(j)=j$. 则有

$$\tau_1=(i_4i_3j)(i_4i_3j)=(i_3i_4j),$$

这时 $|\bar F_{\tau_1}|=|\{i_3,i_4,j\}|=3<|\bar F_\tau|$, 这与(2)式中 $|\bar F_\tau|$ 的最小值定义矛盾!

若 $j\in\bar F_\tau$, 则 $\tau=(i_1i_2)(i_3i_4)\cdots\left(j\tau^{-1}(j)\right)\cdots$ 且 $i_1,i_2,i_3,i_4,j,\tau^{-1}(j)$ 互不相同. 由 $j\neq i_1,i_2,i_3,i_4$ 知 $|\bar F_\tau|\geqslant 5$,

又 τ 可写成对换之积, 故 $|\bar{F}_\tau|$ 必为偶数, 因此 $|\bar{F}_\tau| \geqslant 6$. 此时由命题 0.1可得

$$\begin{aligned}\tau_1 &= (i_4 i_3 \tau^{-1}(j))(i_4 i_3 j) = (i_3 j)(i_4 \tau^{-1}(j)) \\ &= \left(i_4 \tau^{-1}(j)\right)(i_4 i_3)(i_4 j)(i_4 i_3) \\ &= \left(i_4 \tau^{-1}(j)\right)\left((i_4 i_3)(i_4 i_3)^{-1}\right) \\ &= \left(i_4 \tau^{-1}(j)\right)(((i_4 i_3)(i_4))((i_4 i_3)(j))) \\ &= \left(i_4 \tau^{-1}(j)\right)(i_3 j).\end{aligned}$$

于是

$$|\bar{F}_{\tau_1}| = |\{i_3, i_4, j, \tau^{-1}(j)\}| = 4 < |\bar{F}_\tau|.$$

这也(2)式中 $|\bar{F}_\tau|$ 的最小值定义矛盾! 因而 $\tau = (i_1 i_2)(i_3 i_4)\cdots$ 是不可能的.

2. 设 τ 的分解中有长度大于 2 的轮换, 即

$$\tau = (i_1 i_2 i_3 \cdots)\cdots.$$

因为 $(i_1 i_2 i_3 i_4)$ 为奇置换, 故 $\tau \neq (i_1 i_2 i_3 i_4)$, 由此知 $|\bar{F}_\tau| > 4$, 即 $|\bar{F}_\tau| \geqslant 5$. 因而有 $j,k \in \bar{F}_\tau$. 令 $\phi = (i_3 j k), \tau_1 = \tau^{-1}\phi\tau\phi^{-1}$, 由 $H \lhd A_n$ 有 $\tau_1 = \tau^{-1}(\phi\tau\phi^{-1}) \in H$. 于是由命题 0.1可得

$$\tau_1 = (\tau^{-1}\phi\tau)\phi^{-1} = (\tau^{-1}(i_3)\tau^{-1}(j)\tau^{-1}(k))(j i_3 k) = (i_2 \tau^{-1}(j)\tau^{-1}(k))(j i_3 k).$$

由 $j,k \in \bar{F}_\tau$ 知

$$\bar{F}_{\tau_1} = \left\{i_2, i_3, j, k, \tau^{-1}(j), \tau^{-1}(k)\right\} \subseteq \bar{F}_\tau.$$

注意到

$$\tau_1(i_1) = \tau^{-1}\phi\tau\phi^{-1}(i_1) = \tau^{-1}\phi\tau(i_1) = \tau^{-1}\phi(i_2) = \tau^{-1}(i_2) = i_1,$$

即 $i_1 \notin \bar{F}_{\tau_1}$, 则有 $\bar{F}_{\tau_1} \subset \bar{F}_\tau$, 亦即 $|\bar{F}_{\tau_1}| < |\bar{F}_\tau|$. 这也(2)式中 $|\bar{F}_\tau|$ 的最小值定义矛盾! 故 $|\bar{F}_\tau| = 3$.
因而 $H = A_n$, 即 A_n 为单群.

□

命题 0.2

对于 $n \leqslant 4, A_n$ 的结构为

(1) $A_1 = A_2 = \{\mathrm{id}\}$;

(2) $A_3 = \langle(123)\rangle$ 为三阶循环群;

(3) A_4 的阶为 $12, A_4$ 含有一个非平凡的正规子群

$$\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}.$$

此群与 **Klein 四元数群**同构, 也记为 K_4, 而且 K_4 也是 S_4 的正规子群.

♠

证明

□