0.1 群的生成组

定义 0.1

设 S 是群 G 的非空子集, 以 $\langle S\rangle$ 表示 G 的包含 S 的最小子群, 即 S **生成的子群**. 显然,$\langle S\rangle$ 是 G 中所有包含 S 的子群之交, 即 $\langle S\rangle = \bigcap\limits_{S<H} H$.

笔记 由命题????知 $\langle S\rangle = \bigcap\limits_{S<H} H$ 是一个群, 故上述定义是良定义的.

定理 0.1

设 S 是群 G 的非空子集,S^{-1} 是 S 中所有元素的逆元构成的集合, 则

$$\langle S\rangle = \{x_1x_2\cdots x_m \mid x_i \in S\cup S^{-1}, 1 \leqslant i \leqslant m, m \in \mathbb{N}\}.$$

进而若 S 在群 H 中, 则 $S \subseteq H$.

证明 令 $\bar{S} = \{x_1x_2\cdots x_m \mid x_i \in S\cup S^{-1}, 1 \leqslant i \leqslant m, m \in \mathbb{N}\}$. 由 $\langle S\rangle$ 为子群且 $S \subseteq \langle S\rangle$ 知 $S^{-1} \subseteq \langle S\rangle$, 因而 $S \subseteq \bar{S} \subseteq \langle S\rangle$. 又 $\langle S\rangle$ 是含 S 的最小子群, 故只需证明 $\bar{S}$ 为子群, 则 $\bar{S} \supseteq \langle S\rangle$.

设 $x_1x_2\cdots x_m \in \bar{S}$,$y_1y_2\cdots y_n \in \bar{S}$, 于是 $y_i^{-1} \in S\cup S^{-1}(1 \leqslant i \leqslant m)$, 则有

$$(x_1x_2\cdots x_m)(y_1y_2\cdots y_n)^{-1} = x_1x_2\cdots x_m y_n^{-1}y_{n-1}^{-1}\cdots y_2^{-1}y_1^{-1} \in \bar{S},$$

因而 $\bar{S}$ 为 G 的子群, 故 $\bar{S} = \langle S\rangle$.

□

定义 0.2

若 S 为群 G 的子集且 $G = \langle S\rangle$, 则称 S 为 G 的**生成组**. 若 G 有一个含有限个元素的生成组, 则称 G 是**有限生成的**.

若 $G = \langle a\rangle$ 为循环群, 则 a 本身就是生成组, 这时称 a 为 G 的**生成元**.

定义 0.3 (全变换群/置换群)

设 X 是非空集合. 以 S_X 表示 X 的所有可逆变换 (即 X 到 X 的一一对应) 的集合, 则 S_X 对变换的乘法构成一个群, id_X 为左幺元, f^{-1} 为 f 的左逆元. S_X 称 X 的**全变换群**.S_X 的子群称为 X 上的**变换群**.

如果集合 X 所含元素的个数 $|X| = n < +\infty$. 此时 S_X 记为 S_n, 称为 n 个文字的**对称群**或 n 个文字的**置换群**, 也称为 n **阶置换群**, 其元素称为**置换**.

定义 0.4

假定集合 $X = \{1, 2, \cdots, n\}$, 记 S_n 为 X 的对称群, 设 $\sigma \in S_n$, 则 $\sigma(1), \sigma(2), \cdots, \sigma(n)$ 是 $1, 2, \cdots, n$ 的一个排列. 常用下面记法:

$$\sigma = \begin{pmatrix} 1 & 2 & & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

更一般地, 若 $i_1, i_2, \cdots, i_n$ 是 $1, 2, \cdots, n$ 的一个排列, 则可记

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$$

易知 S_n 中有 $n!$ 个元素, S_n 中一个元素可以有 $n!$ 种表示法.

例如, $\sigma \in S_3$, 满足 $\sigma(1)=2, \sigma(2)=3, \sigma(3)=1$, 则可记

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \cdots$$

♣

定理 0.2

设 n 个不定元 $x_1, x_2, \cdots, x_n$ 的多项式

$$A = \prod_{1 \leqslant i<j \leqslant n} (x_i - x_j) \in \mathbb{C}[x_1, x_2, \cdots, x_n].$$

记 S_n 为 $\{1,2,\cdots,n\}$ 的对称群, 对于 $\sigma \in S_n$, 令

$$A_\sigma = \prod_{1 \leqslant i<j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)}),$$

则 $A_\sigma = \pm A$. 若 $A_\sigma = A$, 则称 σ 为**偶置换**, 并记 $\mathrm{sgn}\sigma = 1$; 若 $A_\sigma = -A$, 则称 σ 为**奇置换**, 并记 $\mathrm{sgn}\sigma = -1$, $\mathrm{sgn}\sigma$ 称为 σ 的**符号**. 故有 sgn 是 S_n 到 $\{-1,1\}$ 的同态且

$$A_\sigma = \mathrm{sgn}\sigma A.$$

令 A_n 为 S_n 中偶置换集合, 即

$$A_n \triangleq \{\sigma \in S_n | \mathrm{sgn}\sigma = 1\},$$

则 A_n 为 S_n 的子群.A_n 称为 n 个文字的**交错群**或**交代群**, 也称为 n **阶交错群**或**交代群**.

♡

证明 先证明 $A_\sigma = \pm A$. 注意到 A 中没有 $x_i - x_j$ 的重因式, 因而只需说明 A_σ 中没有重因式即可. 设有 $\{\sigma(i), \sigma(j)\} = \{\sigma(k), \sigma(l)\}$, 则有如下两种可能:

(1) $\sigma(i) = \sigma(k), \sigma(j) = \sigma(l)$, 则有 $i = k, j = l$;

(2) $\sigma(i) = \sigma(l), \sigma(j) = \sigma(k)$, 则有 $i = l, j = k$,

因而都有 $\{i, j\} = \{k, l\}$, 由此知 $A_\sigma = \pm A$.

事实上, 若 $\tau, \sigma \in S_n$, 则有

$$A_{\sigma\tau} = \prod_{1 \leqslant i<j \leqslant n} (x_{\sigma\tau(i)} - x_{\sigma\tau(j)}).$$

将 $A_{\sigma\tau}$ 与 A_σ 进行比较. 若 $\tau(i) < \tau(j)$, 则 $x_{\sigma\tau(i)} - x_{\sigma\tau(j)}$ 仍是 A_σ 中一个因子; 若 $\tau(i) > \tau(j)$, 则 $x_{\sigma\tau(j)} - x_{\sigma\tau(i)} = -(x_{\sigma\tau(i)} - x_{\sigma\tau(j)})$ 为 A_σ 中一因子, 因而将 A_σ 变成 $A_{\sigma\tau}$ 时改变因子符号的次数与将 A 变成 A_τ 时改变因子符号的次数相同, 因而有

$$A_{\sigma\tau} = \mathrm{sgn}\tau \cdot \prod_{1 \leqslant i<j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)}) = \mathrm{sgn}\sigma\mathrm{sgn}\tau A.$$

于是

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}\sigma\mathrm{sgn}\tau, \quad \forall \sigma, \tau \in S_n.$$

故 sgn 是 S_n 到 $\{-1,1\}$ 的同态. 又注意到 $\mathrm{sgn}\tau^{-1} = \mathrm{sgn}\tau, \forall \tau \in S_n$, 故

$$\mathrm{sgn}(\sigma\tau^{-1}) = \mathrm{sgn}\sigma\mathrm{sgn}\tau^{-1} = \mathrm{sgn}\sigma\mathrm{sgn}\tau = 1 \Longrightarrow \sigma\tau^{-1} \in A_n, \quad \forall \sigma, \tau \in A_n.$$

由此知 A_n 为 S_n 的子群.

□

例题 0.1 设 σ 是 S_n 中任一奇置换, 则有 $S_n = A_n \cup \sigma A_n$, 故 $[S_n : A_n] = 2$.

证明

□

例题 0.2 设 $G = S_3$, 又 $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$,$b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, 则 $S_3 = \langle \{a, b\} \rangle$.

证明 事实上, 设 $G_1 = \langle a \rangle$, 注意到

$$a^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, a^2 = (a^{-1})^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},$$

故由定理 0.1知 $G_1 = \{a, a^{-1}\}$. 从而 G_1 为 S_3 的 2 阶子群且 $b \notin G_1$, 于是 $G_1 \subset \langle\{a,b\}\rangle$. 设 $\langle\{a,b\}\rangle$ 的阶为 n, 则由 Lagrange 定理知 $2 \mid n$ 且 $2 < n$. 又因为 $\langle\{a,b\}\rangle$ 是 G 的子群, 所以由 Lagrange 定理知 $n \mid 6$. 因而有 $n = 6$, 由此知 $S_3 = \langle\{a,b\}\rangle$.

□

定义 0.5

设集合 $\{i_1, i_2, \cdots, i_r\}$ 为集合 $\{1, 2, \cdots, n\}$ 的子集. 若 $\sigma \in S_n$ 满足

$$\begin{aligned} \sigma(i_j) &= i_{j+1}, \quad 1 \leqslant j \leqslant r-1, \\ \sigma(i_r) &= i_1, \\ \sigma(k) &= k, \quad k \notin \{i_1, i_2, \cdots, i_r\}, \end{aligned}$$

则称 σ 为一个**长为 r 的轮换**或 **r 轮换**, 这时记 $\sigma = (i_1 i_2 \cdots i_r)$. 特别地, 将 2 轮换 (ij) 称为**对换**. 将 S_n 中的幺元 id 记为长为 1 的轮换, 即 $\mathrm{id} = (i), i = 1, 2, \cdots, n$

若 $\sigma = (i_1 i_2 \cdots i_r)$ 与 $\sigma = (j_1 j_2 \cdots j_s)$ 是两个轮换且

$$\{i_1, i_2, \cdots, i_r\} \bigcap \{j_1, j_2, \cdots, j_s\} = \varnothing,$$

则称 σ 与 σ 为**不相交的轮换**.

显然, 一个 r 轮换 $(i_1 i_2 \cdots i_r)$ 有 r 种不同的表示,

$$(i_1 i_2 \cdots i_r) = (i_2 i_3 \cdots i_r i_1) = \cdots = (i_r i_1 \cdots i_{r-1}).$$

♣

命题 0.1

(1) $[(i_1 i_1')(i_2 i_2') \cdots (i_r i_r')]^{-1} = (i_r i_r')(i_{r-1} i_{r-1}') \cdots (i_1 i_1')$.

(2) $(i_1 i_2 \cdots i_r)^{-1} = (i_r i_{r-1} \cdots i_1)$. 特别地,$(i_1 i_2)^{-1} = (i_2 i_1) = (i_1 i_2)$.

(3) 任何两个不相交的轮换的乘积是可以交换的.

(4) $(kl)(ka \cdots b)(lc \cdots d) = (ka \cdots blc \cdots d)$, 其中 $a, \cdots, b, c, \cdots, d, k, l$ 为互不相同的正整数.

(5) $(kl)(ka \cdots blc \cdots d) = (ka \cdots b)(lc \cdots d)$, 其中 $a, \cdots, b, c, \cdots, d, k, l$ 为互不相同的正整数.

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

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

(7) 任何轮换 $(i_1 i_2 \cdots i_r)$ 可写成如下对换之积

$$(i_1 i_2 \cdots i_r) = (i_1 i_2)(i_2 i_3) \cdots (i_{r-1} i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_2).$$

♠

证明

(1)

(2)

(3) 设 $\sigma = (i_1\ i_2\ \cdots\ i_r)$ 与 $\tau = (j_1\ j_2\ \cdots\ j_s)$ 是两个不相交的轮换,a 是 X 中的任意一个数.

(a) 如果 $a \neq i_k, j_l (k = 1, 2, \cdots, r; l = 1, 2, \cdots, s)$, 则

$$\sigma\tau(a) = \sigma(a) = a,$$
$$\tau\sigma(a) = \tau(a) = a,$$

所以 $\sigma\tau(a) = \tau\sigma(a)$.

(b) 如果 $a = i_k(1 \leqslant k \leqslant r)$, 则 $a, \sigma(a) \neq j_l(l = 1, 2, \cdots, s)$. 从而

$$\begin{aligned}\sigma\tau(a) &= \sigma(a),\\ \tau\sigma(a) &= \tau(\sigma(a)) = \sigma(a),\end{aligned}$$

所以 $\sigma\tau(a) = \tau\sigma(a)$.

(c) 同理可证, 如果 $a = j_l(1 \leqslant l \leqslant s)$, 也有 $\sigma\tau(a) = \tau\sigma(a)$.

这就证明了结论.

(4)

(5)

(6) 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

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

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

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

(7) 由对换的定义可得

$$\begin{aligned}(i_1 i_2)(i_2 i_3)\cdots(i_{r-1} i_r)(i_r) &= i_1,\\ (i_1 i_2)(i_2 i_3)\cdots(i_{r-1} i_r)(k) &= k, \quad k \notin \{i_1, i_2, \cdots, i_r\}.\end{aligned}$$

故 $(i_1 i_2 \cdots i_r) = (i_1 i_2)(i_2 i_3)\cdots(i_{r-1} i_r)$.

再利用数学归纳法证明任何轮换 $(i_1 i_2 \cdots i_r)$ 可写成如下对换之积

$$(i_1 i_2 \cdots i_r) = (i_1 i_r)(i_1 i_{r-1})\cdots(i_1 i_2). \tag{1}$$

当 $r = 2$ 时,(1)式显然成立. 假设定理对 $r-1(r \geqslant 3)$ 成立, 并记 $a = (i_1 i_2 \cdots i_r)$, 于是有

$$(i_1 i_r)(i_1 i_{r-1})\cdots(i_1 i_3)(i_1 i_2) = (i_1 i_3 \cdots i_r)(i_1 i_2) = a'.$$

当 $j \neq i_k$ 时,$a'(j) = j = a(j)$;

当 $j = i_k(k \geqslant 3)$ 时,$a'(j) = (i_1 i_3 \cdots i_r)(j) = a(j)$;

当 $j = i_1$ 时,$a'(i_1) = (i_1 i_3 \cdots i_r)(i_2) = i_2 = a(i_1)$;

当 $j = i_2$ 时,$a'(i_2) = (i_1 i_3 \cdots i_r)(i_1) = i_3 = a(i_2)$.

综上知 $a = a'$. 故知式(1)成立.

□

定理 0.3 (Ruffini 定理)

设 $a \in S_n$ 且 $a = \sigma_1\sigma_2\cdots\sigma_k$, 其中,$\sigma_i$ 为 r_i 轮换且当 $i \neq j$ 时,σ_i 与 σ_j 不相交,$1 \leqslant i, j \leqslant k$, 则 a 的阶为 $r_1, r_2, \cdots, r_k$ 的最小公倍数 $[r_1, r_2, \cdots, r_k]$. 进而 σ_i 的阶为 r_i.

♡

证明 证法一:设 $m = [r_1, r_2, \cdots, r_s]$. 由命题 0.1(3)知不相交轮换的乘积是可以互相交换的, 因此

$$\sigma^m = (\sigma_1\sigma_2\cdots\sigma_s)^m = \sigma_1^m\sigma_2^m\cdots\sigma_s^m = (1),$$

从而 $\mathrm{ord}\sigma \mid m$.

另一方面, 设 $\sigma_1=(i_1\ i_2\ \cdots\ i_{r_1})$, 则对任意的 $i_j\in\{i_1,i_2,\cdots,i_{r_1}\}$, 由于 $\sigma_1,\sigma_2,\cdots,\sigma_s$ 为互不相交的轮换, 因此

$$\sigma_1^{\mathrm{ord}\sigma}(i_j)=\sigma_1^{\mathrm{ord}\sigma}\sigma_2^{\mathrm{ord}\sigma}\cdots\sigma_s^{\mathrm{ord}\sigma}(i_j)=\sigma^{\mathrm{ord}\sigma}(i_j)=i_j.$$

由此推出 $\sigma_1^{\mathrm{ord}\sigma}=(1)$, 从而 $r_1\mid\mathrm{ord}\sigma$. 同理可证 $r_i\mid\mathrm{ord}\sigma(i=1,2,\cdots,s)$. 于是

$$m=[r_1,r_2,\cdots,r_s]\mid\mathrm{ord}\sigma.$$

所以

$$\mathrm{ord}\sigma=[r_1,r_2,\cdots,r_s].$$

证法二: 对因子个数 k 用数学归纳法证明. 当 $k=1$ 时,$a=(i_1i_2\cdots i_{r_1})$ 是一个轮换. 对任何 $s(1\leqslant s\leqslant r_1)$ 有

$$a^s(j)=j,\quad j\neq i_1,i_2,\cdots,i_{r_1},$$

而

$$a^s(i_j)=\begin{cases} i_{s+j}, & j+s\leqslant r_1,\\ i_{s+j-r_1}, & j+s>r_1,\end{cases}$$

于是当 $s<r_1$ 时,$a^s\neq\mathrm{id}$, 而当 $s=r_1$ 时,$a^{r_1}=\mathrm{id}$, 故 a 的阶为 r_1. 由此可知 σ_i 的阶为 r_i.

设 $k-1(k\geqslant 2)$ 时定理成立. 设 $a=\sigma_1\sigma_2\cdots\sigma_k$, 令

$$a_1=\sigma_2\sigma_3\cdots\sigma_k,$$

于是由归纳假设知 a_1 的阶为 $[r_2,r_3,\cdots,r_k]$. 因为 σ_1 与 $\sigma_j(j=2,\cdots,n)$ 不相交, 所以可设 $\sigma_2,\sigma_3,\cdots,\sigma_k$ 中包含的文字 (作用的对象) 为 $\{i_{r_1+1},i_{r_1+2},\cdots,i_t\}$,$\sigma_1$ 中的文字 (作用的对象) 为 $\{i_1,i_2,\cdots,i_{r_1}\}$.

若 $j\neq i_l(1\leqslant l\leqslant t)$, 则 $\sigma_1(j)=a_1(j)=j$, 故 $\sigma_1a_1(j)=a_1\sigma_1(j)=j$.

若 $j=i_l$ 且 $1\leqslant l\leqslant r_1$, 则 $a_1(j)=j$,$\sigma_1(j)=i_{l'}$,$l'\leqslant r_1$, 因而 $a_1\sigma_1(j)=i_{l'}=\sigma_1a_1(j)$.

若 $j=i_l$ 且 $t\geqslant l\geqslant r_1+1$, 则 $\sigma_1(i_l)=i_l$,$a_1(i_l)=i_{l'}(t\geqslant l'\geqslant r_1+1)$, 故有 $a_1\sigma_1(j)=i_{l'}=\sigma_1a_1(j)$.

总之有 $a_1\sigma_1=\sigma_1a_1$.

又设 $\beta\in\langle\sigma_1\rangle\cap\langle a_1\rangle$. 由定理 0.1知 $\beta=f_1f_2\cdots f_m$, 其中 $f_i\in\left\{\sigma_1,\sigma_1^{-1}\right\}\cap\left\{a_1,a_1^{-1}\right\}$, $m\in\mathbb{N}$.

若 $j\neq i_l(1\leqslant l\leqslant t)$, 则 $\beta(j)=j$.

若 $j=i_l(1\leqslant l\leqslant r_1)$, 由 $\beta\in\langle a_1\rangle$, 则 $\beta(j)=j$. 若 $j=i_l(t\geqslant l\geqslant r_1+1)$, 由 $\beta\in\langle\sigma_1\rangle$, 则 $\beta(j)=j$.

故 $\beta=\mathrm{id}$, 即有 $\langle\sigma_1\rangle\cap\langle a_1\rangle=\{\mathrm{id}\}$.

设 m 为 $a=a_1\sigma_1$ 的阶, 则再由 $a_1\sigma_1=\sigma_1a_1$ 可得

$$a^m=a_1^m\sigma_1^m=\sigma_1^ma_1^m=\mathrm{id}.$$

因此 $\sigma_1^m=a_1^{-m}\in\langle\sigma_1\rangle\cap\langle a_1\rangle$. 又由 $\langle\sigma_1\rangle\cap\langle a_1\rangle=\{\mathrm{id}\}$ 知 $\sigma_1^m=a_1^{-m}=\mathrm{id}$, 从而 m 是 σ_1,a_1 的阶的公倍数, 即 $m\mid r_1$,$m\mid[r_2,\cdots,r_k]$. 再设 n 也是 r_1,$[r_2,\cdots,r_k]$ 的公倍数, 则

$$\sigma_1^n=a_1^n=\mathrm{id}\Longrightarrow a^n=\sigma_1^na_1^n=\mathrm{id}.$$

故 $m\mid n$. 因而 $a=\sigma_1a_1$ 的阶为 $[r_1,[r_2,\cdots,r_k]]=[r_1,r_2,\cdots,r_k]$.

□

定理 0.4

(1) 任意 n 阶置换 $a\in S_n$ 一定可写成互不相交的轮换之积. 即存在互不相交的轮换 $\sigma_1,\sigma_2,\cdots,\sigma_r$, 使得

$$a=\sigma_1\sigma_2\cdots\sigma_r. \tag{2}$$

(2) 设 σ 为一个 n 阶置换, 由定理 0.4(1)可设 σ 可表为不相交轮换 (包括 1 轮换) 的乘积

$$\sigma=\sigma_1\sigma_2\cdots\sigma_s,$$

在集合 $X=\{1,2,\cdots,n\}$ 中, 规定关系 “$\sim$” :

$$k\sim l\iff r\in\mathbb{Z},\ \sigma^r(k)=l.$$

(i) 证明: $\sim$ 是 X 的一个等价关系;

(ii) 证明: $k \sim l$ 的充分必要条件是 k 与 l 属于 σ 的同一个轮换. 进而 X 的所有等价类为

$$\{k \in \mathbb{N} \mid k \in \sigma_i\}, \quad i = 1, 2, \cdots, s.$$

(3) 如果不考虑因子的次序和乘积中 1 轮换的个数, 则分解式(2)是唯一的.

注 在(2)定义的等价关系下, 对于置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 6 & 8 & 9 & 1 & 7 & 10 & 4 & 5 \end{pmatrix},$$

由于

$$\sigma = (1\ 3\ 6)(4\ 8\ 10\ 5\ 9)(2)(7),$$

所以集合 X 的所有等价类为

$$[2] = \{2\}, \quad [7] = \{7\}, \quad [1] = \{1, 3, 6\}, \quad [4] = \{4, 5, 8, 9, 10\}.$$

证明

(1) 证法一:对 X 的元素个数 n 用数学归纳法. 当 $n = 1$ 时,1 阶置换只有 $a = (1)$, 已经是轮换, 因此结论对 $n = 1$ 成立. 假定结论对 $n - 1$ 成立, 考察 n 阶置换

$$a = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}.$$

(a) 如果 $i_n = n$, 即

$$a = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & n \end{pmatrix}.$$

令

$$a_1 = \begin{pmatrix} 1 & 2 & \cdots & n-1 \\ i_1 & i_2 & \cdots & i_{n-1} \end{pmatrix},$$

则 a_1 是一个 $n - 1$ 阶置换. 由归纳假设,a_1 可表为一些不相交轮换的乘积

$$a_1 = \sigma_1 \sigma_2 \cdots \sigma_s.$$

将 σ_i 看作 n 阶置换, 即得

$$a = \sigma_1 \sigma_2 \cdots \sigma_s \cdot (n) = \sigma_1 \sigma_2 \cdots \sigma_s.$$

(b) 如果 $i_n \neq n$, 则有某个 $k (1 \leqslant k \leqslant n - 1)$, 使得 $i_k = n$. 令

$$\beta = (i_k\ i_n) a = \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{k-1} & i_n & i_{k+1} & \cdots & i_{n-1} & n \end{pmatrix}.$$

由 (a) 所证,β 可表为一些不相交轮换的乘积. 设

$$\beta = a_1 a_2 \cdots a_s,$$

其中,$a_1, a_2, \cdots, a_s$ 为互不相交的轮换, 则

$$a = (i_k\ i_n) a_1 a_2 \cdots a_s.$$

如果每个 a_i 都不与 $(i_k\ i_n)$ 相交, 则

$$a = (i_k\ i_n) a_1 a_2 \cdots a_s$$

为不相交轮换的乘积. 如果有某个 a_i 与 $(i_k\ i_n)$ 相交, 则至多有一个 a_i 与 $(i_k\ i_n)$ 相交. 不妨设 $a_1 = (i_n\ a\ \cdots\ b)$, 则

$$a = (i_k\ i_n)(i_n\ a\ \cdots\ b) a_2 a_3 \cdots a_s$$

$$= (i_k\, i_n\, a\ \cdots\ b)a_2a_3\cdots a_s$$

为不相交轮换的乘积. 从而由归纳法知结论成立.

证法二:设 $a \in S_n$, 令 $\bar{F}_a = \{j \mid a(j) \neq j\}$. 显然有

$$\bar{F}_{\mathrm{id}} = \varnothing. \tag{3}$$

当 $a \neq \mathrm{id}$ 时,

$$|\bar{F}_a| \geqslant 2 \tag{4}$$

当且仅当 a 为对换时, 式(4)中等号成立. 下面不妨设 $a \neq \mathrm{id}$. 证明存在轮换 σ_1 满足

$$\begin{cases} \bar{F}_a = \bar{F}_{\sigma_1} \cup \bar{F}_{\sigma_1^{-1}a}, \\ \bar{F}_{\sigma_1} \cap \bar{F}_{\sigma_1^{-1}a} = \varnothing. \end{cases} \tag{5}$$

因 $a \neq \mathrm{id}$, 故由式(4)知有 $i_1 \in \bar{F}_a$. 令

$$i_2 = a(i_1), \quad i_3 = a(i_2), \quad \cdots, \quad i_k = a(i_{k-1}),$$

则 $i_1 \neq i_2$. 由于 $\bar{F}_a$ 是有限集, 故存在 $r \geqslant 3$, 使得 $i_1, i_2, \cdots, i_{r-1}$ 互不相同, 而 $i_r = i_t (1 \leqslant t \leqslant r-1)$. 现证 $t = 1$. 若不然, 则有

$$a(i_{t-1}) = i_t = i_r = a(i_{r-1}).$$

于是

$$i_{t-1} = i_{r-1},$$

即有 $t = r$, 矛盾, 故 $t = 1$. 令 $\sigma_1 = (i_1 i_2 \cdots i_{r-1})$, 显然

$$\sigma_1(i_k) = a(i_k),\ 1 \leqslant k \leqslant r-1, \quad \bar{F}_{\sigma_1} = \{i_1, i_2, \cdots, i_{r-1}\} \subseteq \bar{F}_a.$$

再令 $a_1 = \sigma_1^{-1}a$, 若 $l \notin \bar{F}_a$, 则 $l \notin \bar{F}_{\sigma_1^{-1}}$, 故 $a_1(l) = l (l \notin \bar{F}_{a_1})$, 因而 $\bar{F}_{a_1} \subseteq \bar{F}_a$. 于是 $\bar{F}_{a_1} \cup \bar{F}_{\sigma_1} \subseteq \bar{F}_a$. 反之, 若 $l \notin \bar{F}_{a_1} \cup \bar{F}_{\sigma_1}$, 则有 $a_1(l) = \sigma_1(l) = l$, 故 $a(l) = a_1\sigma_1^{-1}(l) = l$, 即 $l \notin \bar{F}_a$. 于是式(5)中第一个等式成立.

设 $i_k \in \bar{F}_{\sigma_1}$, 则有 $a_1(i_k) = \sigma_1^{-1}a(i_k) = \sigma_1^{-1}\sigma_1(i_k) = i_k$, 即 $i_k \notin \bar{F}_{a_1} = \bar{F}_{\sigma_1^{-1}a}$. 故(5)式中第二个等式也成立.

若 $a \neq \sigma_1$, 则 $\bar{F}_{\sigma_1^{-1}a} \neq \bar{F}_{\mathrm{id}} = \varnothing$. 从而 $\bar{F}_{\sigma_1^{-1}a} \neq \bar{F}_a$, 否则由(5)式知 $\bar{F}_{\sigma_1} = \varnothing$, 即 $\sigma_1 = \mathrm{id}$, 这与 $i_1, i_2, \cdots, i_{r-1}$ 互不相同矛盾! 再对 $\sigma_1^{-1}a$ 用上述方法同理可得另一轮换 $\sigma_2 = (j_1 j_2 \cdots j_{l-1})$, 使得

$$\bar{F}_{\sigma_2} = \{j_1, j_2, \cdots, j_{l-1}\} \subseteq \bar{F}_{\sigma_1^{-1}a}, \tag{6}$$

并且

$$\begin{cases} \bar{F}_{\sigma_1^{-1}a} = \bar{F}_{\sigma_2} \cup \bar{F}_{\sigma_2^{-1}\sigma_1^{-1}a}, \\ \bar{F}_{\sigma_2} \cap \bar{F}_{\sigma_2^{-1}\sigma_1^{-1}a} = \varnothing. \end{cases}$$

若 $a \neq \sigma_1\sigma_2$, 则同理有 $\bar{F}_{\sigma_2^{-1}\sigma_1^{-1}a} \neq \bar{F}_{\sigma_1^{-1}a}$. 从而 $\bar{F}_{\sigma_2^{-1}\sigma_1^{-1}a} \subset \bar{F}_{\sigma_1^{-1}a} \subset \bar{F}_a$. 由(5)式和(6)式知

$$\{i_1, i_2, \cdots, i_{r-1}\} \cap \{j_1, j_2, \cdots, j_{l-1}\} = \bar{F}_{\sigma_1} \cap \bar{F}_{\sigma_2} = \varnothing,$$

故 σ_1 与 σ_2 为不相交的轮换. 继续做下去. 由于 $\bar{F}_a$ 是有限的, 最后有 $s \in \mathbb{N}$, 使得互不相交的轮换 $\sigma_1, \sigma_2, \cdots, \sigma_s$ 满足

$$\bar{F}_{\sigma_s^{-1}\sigma_{s-1}^{-1}\cdots\sigma_1^{-1}a} = \varnothing,$$

即 $\sigma_s^{-1}\sigma_{s-1}^{-1}\cdots\sigma_1^{-1}a = \mathrm{id}$, 因而

$$a = \sigma_1\sigma_2\cdots\sigma_s,$$

即 S_n 中任何元素可表为互不相交的轮换之积.

(2) (i) 设 $\operatorname{ord}\sigma = m$, 对 $\forall j, k, l \in X$.

因为 $\sigma^m(j) = (1)j = j$, 所以 $j \sim j$, 于是 $\sim$ 具有反身性;

如果 $k \sim l$, 则存在 $r \in \mathbb{Z}$, 使 $\sigma^r(k) = l$, 于是 $\sigma^{-r}(l) = k$, 从而 $l \sim k$, 这说明 $\sim$ 具有对称性;

如果 $j \sim k, k \sim l$, 则存在 $r_1, r_2 \in \mathbb{Z}$, 使 $\sigma^{r_1}(j) = k, \sigma^{r_2}(k) = l$, 于是 $\sigma^{r_1+r_2}(j) = l$, 从而 $j \sim l$, 这说明 $\sim$ 具有传递性.

这就证明了 $\sim$ 是 X 的一个等价关系.

(ii) **必要性**: 设 $k \sim l$, 则存在 $r \in \mathbb{Z}$, 使 $\sigma^r(k) = l$. 设 k 属于轮换 σ_i, 则

$$l = \sigma^r(k) = (\sigma_1\sigma_2\cdots\sigma_s)^r(k) = \sigma_1^r\sigma_2^r\cdots\sigma_s^r(k) = \sigma_i^r(k),$$

即 l 也属于轮换 σ_i, 从而 k 与 l 属于 σ 的同一个轮换.

充分性: 如果 k 与 l 属于 σ 的同一个轮换 σ_i, 则必有 $r \in \mathbb{Z}$, 使 $\sigma_i^r(k) = l$, 从而

$$l = \sigma_i^r(k) = \sigma_1^r\sigma_2^r\cdots\sigma_s^r(k) = (\sigma_1\sigma_2\cdots\sigma_s)^r(k) = \sigma^r(k),$$

所以 $k \sim l$.

(3) 设 σ 为任一 n 阶置换,

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s = \delta_1\delta_2\cdots\delta_t.$$

是 σ 的两个表为不相交轮换 (包括 1 轮换) 的乘积的分解式, 则 σ 在集合 $X = \{1, 2, \cdots, n\}$ 上规定关系 "$\sim$"

$$k \sim l \iff r \in \mathbb{Z},\ \sigma^r(k) = l.$$

由定理 0.4(2)(ii)知, 在此等价关系之下, 集合 X 的等价类的个数等于 σ 分解为不相交轮换 (包括 1 轮换) 的乘积的因子数, 所以 $s = t$. 又由定理 0.4(2)(ii)知,X 的一个等价类由属于 σ 的同一个轮换中的元素组成. 因此, 适当交换因子的次序, 可使 σ_i 与 δ_i 含有 X 的同一个等价类 X_i 中的元素. 从而, 对任意的 $x \in X$, 如果 $x \notin X_i$, 则有

$$\sigma_i(x) = x = \delta_i(x).$$

如果 $x \in X_i$, 也有

$$\sigma_i(x) = \sigma_1\sigma_2\cdots\sigma_s(x) = \sigma(x) = \delta_1\delta_2\cdots\delta_s(x) = \delta_i(x).$$

因此 $\sigma_i = \delta_i (i = 1, 2, \cdots, s)$. 这就证明了分解的唯一性.

□

推论 0.1

(1) 任何置换都可写成对换之积. 并且令 $S = \{(1i) \mid 2 \leqslant i \leqslant n\}$, 则有 $S_n = \langle S \rangle$.

(2) 将一个置换写成对换的乘积, 所用对换个数的奇偶性是唯一的.

注 由定理 0.4(1)和命题 0.1(7)知, 任何置换至少可分解成两个不同的对换之积 (这里 (1) 中只证明了其中一种).

证明

(1) 由定理 0.4(1)知任何置换可分解为不相交的轮换之积, 又由命题 0.1(7)知任何轮换可分解为对换之积, 故任何置换都可分解为对换之积.

事实上,

$$(ij) = (1i)(1j)(1i). \tag{7}$$

由定理 0.4(1)知 $\forall a \in S_n$ 一定可写成轮换之积, 从而由命题 0.1(7)知 a 可写成对换之积. 再利用(7)式知 a 可写成 S 中元素之积, 再由定理 0.1可知 $a \in \langle S \rangle$, 即 $\langle S \rangle \supseteq S_n$. 又显然有 $\langle S \rangle \subseteq S_n$, 故 $\langle S \rangle = S_n$.

(2) 设 σ 为任一 n 阶置换, 并设 σ 已表为 s 个不相交轮换 (包括 1 轮换) 之积:$\sigma = \tau_1\tau_2\cdots\tau_s$. 定义

$$\mathcal{N}(\sigma) = (-1)^{n-s}.$$

显然 $\mathcal{N}(\sigma)$ 由 σ 唯一确定. 设 (ab) 为任一对换, 考察乘积 $(ab)\sigma$. 下证

$$\mathcal{N}((ab)\sigma) = -\mathcal{N}(\sigma). \tag{8}$$

如果 a, b 处于 σ 的同一个轮换

$$\tau_1 = (ac_1c_2\cdots c_kbd_1d_2\cdots d_h)$$

中, 则由命题 0.1(5)知

$$(ab)\sigma = (ac_1c_2\cdots c_k)(bd_1d_2\cdots d_h)\tau_2\tau_3\cdots\tau_s.$$

从而

$$\mathcal{N}((ab)\sigma) = (-1)^{n-s-1} = -\mathcal{N}(\sigma).$$

如果 a, b 分别处于 σ 的两个不同轮换

$$\tau_1 = (ac_1c_2\cdots c_k), \quad \tau_2 = (bd_1d_2\cdots d_h)$$

中, 则由命题 0.1(4)知

$$(ab)\sigma = (ac_1c_2\cdots c_kbd_1d_2\cdots d_h)\tau_3\tau_4\cdots\tau_s.$$

从而

$$\mathcal{N}((ab)\sigma) = (-1)^{n-s+1} = -\mathcal{N}(\sigma).$$

故(8)式成立.

设 σ 可分别表示为 h 个对换和 k 个对换的乘积

$$\sigma = (a_1b_1)(a_2b_2)\cdots(a_hb_h) = (c_1d_1)(c_2d_2)\cdots(c_kd_k),$$

则由(8)式可得

$$\mathcal{N}(\sigma) = \mathcal{N}(\sigma\cdot(1)) = \mathcal{N}((a_1b_1)(a_2b_2)\cdots(a_hb_h)\cdot(1)) = (-1)^h\mathcal{N}((1)) = (-1)^h.$$

由(8)式同理可得

$$\mathcal{N}(\sigma) = (-1)^k.$$

因此 $(-1)^h = (-1)^k$, 所以 h 与 k 有相同的奇偶性.

□

推论 0.2

(1) 对换都是奇置换.

(2) 置换是偶 (奇) 置换当且仅当其可表示为偶 (奇) 数个对换之积.

(3) 轮换是奇 (偶) 置换当且仅当其长度为偶 (奇) 数.

(4) 任何两个偶 (奇) 置换之积是偶置换.

(5) 一个偶置换与一个奇置换之积是奇置换.

(6) 一个偶 (奇) 置换的逆置换仍是一个偶 (奇) 置换.

(7) 置换 σ 与 σ^{-1} 具有相同的奇偶性.

♡

证明

(1) 由定理 0.2中奇置换定义知对换显然都是奇置换.

(2) 设 $\sigma \in S_n$, 则由推论 0.1知 $\sigma = \sigma_1\sigma_2\cdots\sigma_k$, 其中 σ_i 都是对换. 又注意到对换 $\sigma_i = (ij)$ 都是奇置换, 故 $\mathrm{sgn}\sigma_i = -1$. 由定理 0.2知 sgn 是 S_n 到 $\{-1, 1\}$ 的同态, 因此

$$\mathrm{sgn}\sigma = \mathrm{sgn}(\sigma_1\sigma_2\cdots\sigma_k) = (\mathrm{sgn}\sigma_1)(\mathrm{sgn}\sigma_2)\cdots(\mathrm{sgn}\sigma_k) = (-1)^k.$$

故 σ 是奇置换当且仅当 $\mathrm{sgn}\sigma = (-1)^k = -1$ 当且仅当 k 为奇数;
σ 是偶置换当且仅当 $\mathrm{sgn}\sigma = (-1)^k = 1$ 当且仅当 k 为偶数.

(3) 设 r 轮换 $(i_1i_2,\cdots i_r)$, 则由命题 0.1(7)知

$$(i_1i_2\cdots i_r) = (i_1i_r)(i_1i_{r-1})\cdots(i_1i_2).$$

由定理 0.2知 sgn 是 S_n 到 $\{-1, 1\}$ 的同态, 因此

$$\mathrm{sgn}(i_1i_2\cdots i_r) = \mathrm{sgn}(i_1i_r)\cdot\mathrm{sgn}(i_1i_{r-1})\cdots\mathrm{sgn}(i_1i_2) = (-1)^{r-1}.$$

故 $(i_1 i_2, \cdots i_r)$ 为偶置换当且仅当 $\mathrm{sgn}(i_1 i_2 \cdots i_r) = (-1)^{r-1} = 1$ 当且仅当 r 是奇数;
若 $(i_1 i_2, \cdots i_r)$ 为奇置换当且仅当 $\mathrm{sgn}(i_1 i_2 \cdots i_r) = (-1)^{r-1} = -1$ 当且仅当 r 是偶数;

(4)

(5)

(6)

(7) 如果 σ 可表示为 k 个对换的乘积

$$\sigma = (i_1\ j_1)(i_2\ j_2)\cdots(i_k\ j_k),$$

则

$$\sigma^{-1} = (i_k\ j_k)(i_{k-1}\ j_{k-1})\cdots(i_1\ j_1)$$

也可表示为 k 个对换的乘积. 所以 σ 与 σ^{-1} 具有相同的奇偶性.

□

定理 0.5

设 S_X 是置换群, 则有以下结论

(1) 若 S_X 中存在奇置换, 则 S_X 中奇置换的个数与偶置换的个数相同. 特别地, 在全体 n 阶置换 S_n 中, 奇置换与偶置换各有 $\frac{n!}{2}$ 个, 进而 $|A_n| = \frac{n!}{2}$.

(2) S_X 中所有偶置换的集合 H 是 S_X 的子群.

♡

证明

(1) 设 S_X 中有奇置换. 由于 S_X 是置换群, 所以 $(1) \in S_X$, 而 (1) 为偶置换. 所以 S_X 中既有奇置换又有偶置换. 以 O 与 E 分别表示 S_X 中奇置换与偶置换的集合. 设 σ 为 S_X 的任一奇置换, 则由推论 0.2(4)和推论 0.2(5)可得

$$\sigma O = \{\sigma\delta \mid \delta \in O\} \subseteq E,$$
$$\sigma E = \{\sigma\tau \mid \tau \in E\} \subseteq O.$$

因此

$$|O| = |\sigma O| \leqslant |E|, \quad |E| = |\sigma E| \leqslant |O|,$$

由此得 $|O| = |E|$. 这就证明了结论.

(2) 因 $(1) \in G$ 为偶置换, 所以 $(1) \in H$, 从而 H 非空. 又由推论 0.2(4)知两个偶置换的乘积仍是偶置换, 所以 H 关于置换的乘积封闭. 从而由命题**????**知 H 为 G 的子群.

□

例题 0.3 把下列置换分别写成不相交的轮换的乘积和对换的乘积, 并计算置换的奇偶性:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 5 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 1 & 5 & 3 \end{pmatrix}.$$

解 注意到

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 5 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix} = (1\ 6)(2\ 4\ 5).$$

再由命题 0.1(7)知

$$(1\ 6)(2\ 4\ 5) = (1\ 6)(2\ 4)(4\ 5) \quad \text{or} \quad (1\ 6)(2\ 5)(2\ 4).$$

故由推论 0.2(2)知这个置换是奇置换.

□