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 $S=\bigcap\limits_{S<H} H$.

♣

笔记 由命题????知 $S=\bigcap\limits_{S<H} H$ 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, 则

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

♡

证明 令 $\bar{S}=\{x_1x_2\cdots x_m \mid x_i\in S\cup S^{-1}, 1\leqslant i\leqslant m, m\in\mathbf{N}\}$. 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

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

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**.

♣

例题 0.1 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 0.3

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 $\sigma=(i_1i_2\cdots i_r)$. 特别地, 将 2 轮换 (ij) 称为**对换**.

若 $\sigma=(i_1i_2\cdots i_r)$ 与 $\tau=(j_1j_2\cdots j_s)$ 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 τ 为**不相交的轮换**.

显然, 一个 r 轮换 $(i_1i_2\cdots i_r)$ 有 r 种不同的表示,

$$(i_1i_2\cdots i_r)=(i_2i_3\cdots i_ri_1)=\cdots=(i_ri_1\cdots i_{r-1}).$$

命题 0.1

设 $\sigma\in S_n$ 且 $\sigma=(i_1i_1')(i_2i_2')\cdots(i_ri_r')$, 则 $\sigma^{-1}=(i_ri_r')(i_{r-1}i_{r-1}')\cdots(i_1i_1')$.

证明

□

定理 0.2

设 $a\in S_n$ 且 $a=\sigma_1\sigma_2\cdots\sigma_k$, 其中,$\sigma_i$ 为 r_i 轮换: 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 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 $f_i\in\left\{\sigma_1,\sigma_1^{-1}\right\}\cap\left\{a_1,a_1^{-1}\right\}$, $m\in\mathbf{N}$.

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 0.3

(1) 任何轮换 $(i_1i_2\cdots i_r)$ 可写成如下对换之积

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

(2) 若把 S_n 中的幺元 id 记为长为 1 的轮换, 即 $\mathrm{id}=(i)$, 则 $\forall a\in S_n$, 一定可写成互不相交的轮换之积.

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

证明

(1) 利用数学归纳法证明任何轮换 $(i_1i_2\cdots i_r)$ 可写成如下对换之积

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

当 $r=2$ 时,(1)式显然成立. 假设定理对 $r-1(r\geqslant 3)$ 成立, 并记 $a=(i_1i_2\cdots i_r)$, 于是有

$$(i_1i_r)(i_1i_{r-1})\cdots(i_1i_3)(i_1i_2)=(i_1i_3\cdots i_r)(i_1i_2)=a'.$$

当 $j\neq i_k$ 时,$a'(j)=j=a(j)$;

当 $j=i_k(k\geqslant 3)$ 时,$a'(j)=(i_1i_3\cdots i_r)(j)=a(j)$;

当 $j=i_1$ 时,$a'(i_1)=(i_1i_3\cdots i_r)(i_2)=i_2=a(i_1)$;

当 $j=i_2$ 时,$a'(i_2)=(i_1i_3\cdots i_r)(i_1)=i_3=a(i_2)$.

综上知 $a=a'$. 故知式(1)成立, 故任何轮换可写成 S 中元素之积.

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

$$\bar{F}_{\mathrm{id}}=\varnothing. \tag{2}$$

当 $a\neq\mathrm{id}$ 时,

$$|\bar{F}_a|\geqslant 2 \tag{3}$$

当且仅当 a 为对换时, 式(3)中等号成立. 下面不妨设 $a\neq\mathrm{id}$. 证明存在轮换 σ_1 满足

$$\begin{cases}\bar{F}_a=\bar{F}_{\sigma_1}\cup\bar{F}_{\sigma_1^{-1}a},\\ \bar{F}_{\sigma_1}\cap\bar{F}_{\sigma_1^{-1}a}=\varnothing.\end{cases} \tag{4}$$

因 $a\neq\mathrm{id}$, 故由式(3)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 $\sigma_1=(i_1i_2\cdots i_{r-1})$, 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(4)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(4)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(4)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 $\sigma_2=(j_1j_2\cdots j_{l-1})$, 使得

$$\bar{F}_{\sigma_2}=\{j_1,j_2,\cdots,j_{l-1}\}\subseteq\bar{F}_{\sigma_1^{-1}a}, \tag{5}$$

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(4)式和(5)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 n, 使得互不相交的轮换 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 满足

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

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

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

即 S_n 中任何元素可表为互不相交的轮换之积, 故定理成立.

(3) 事实上,

$$(ij) = (1i)(1j)(1i). \tag{6}$$

由结论 (2) 知 $\forall a \in S_n$ 一定可写成轮换之积, 从而由结论 (1) 知 a 可写成对换之积. 再利用(6)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 $\langle S\rangle = S_n$.

□

推论 0.1

对换都是奇置换, 并且奇置换可表示为奇数个对换之积, 偶置换可表示为偶数个对换之积.
进而长度为奇数的轮换都是奇置换, 长度为偶数的轮换都是偶置换.

证明 由定理**??**中奇置换定义知对换显然都是奇置换. 设 $\sigma \in S_n$, 则由定理 0.3(3)知 $\sigma = \tau_1\tau_2\cdots\tau_k$, 其中 τ_i 都是对换. 又注意到对换 $\tau_i = (ij)$ 都是奇置换, 故 $\mathrm{sgn}\tau_i = -1$. 由定理**??**知 sgn 是 S_n 到 $\{-1, 1\}$ 的同态, 因此

$$\mathrm{sgn}\sigma = \mathrm{sgn}(\tau_1\tau_2\cdots\tau_k) = (\mathrm{sgn}\tau_1)(\mathrm{sgn}\tau_2)\cdots(\mathrm{sgn}\tau_k) = (-1)^k.$$

若 σ 是奇置换, 则 $\mathrm{sgn}\sigma = (-1)^k = -1$, 即 k 为奇数.

若 σ 是偶置换, 则 $\mathrm{sgn}\sigma = (-1)^k = 1$, 即 k 为偶数.

设 r 轮换 $(i_1i_2, \cdots i_r)$, 则由定理 0.3(1)知

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

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

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

若 r 是奇数, 则 $\mathrm{sgn}(i_1i_2\cdots i_r) = (-1)^r = -1$, 即 $(i_1i_2, \cdots i_r)$ 为奇置换.

若 r 是偶数, 则 $\mathrm{sgn}(i_1i_2\cdots i_r) = (-1)^r = 1$, 即 $(i_1i_2, \cdots i_r)$ 为偶置换.

□