X 集合

$Sym(X) = \{\sigma \mid \sigma: X \to X$ 双射$\}$　　$(Sym(X), \circ)$ 成群

幺元 $id_X: X \to X$ 恒等映射　　$(\sigma_1 \circ \sigma_2)(x) = \sigma_1(\sigma_2(x)), \forall x \in X$

逆元 逆映射

$X = \{1, 2, \cdots, n\}$　$Sym(X) = S_n$.

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

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}$

$|S_1| = 1$　$S_2 = \left\{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\}$

非支轨 ←　$S_3 = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{\tau}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\}$

轮换　$\sigma = (a_1, a_2, \cdots, a_m)$　X 上两两不同的元.

$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3, \cdots, \sigma(a_{m-1}) = a_m, \sigma(a_m) = a_1.$

$\forall x \in X - \{a_1, a_2, \cdots, a_m\},\ \sigma(x) = x.$

$\tau = (1, 2, 3)$ 阶?　$\eta = (1, 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\tau^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$

$\tau^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\eta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

τ 是 3 阶元.

$H=\langle\tau\rangle=\{(1),(1,2,3),(1,3,2),\mathrm{id}\}\lhd S_3$

$\eta\circ\tau\circ\eta^{-1}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\tau^2\in H.$

其他2个元素也可验证.

$S_3=\langle\{\tau,\eta\}\rangle$ $\quad |H|=3.\ |\eta H|=3.\ \eta\notin H\ \ H\cup\eta H=S_3.$

$\tau\circ\eta\neq\eta\circ\tau$ $\quad S_3$：不交换

$\eta\circ\tau\circ\eta^{-1}=\tau^2$ $\quad \tau\circ\eta\circ\tau\circ\eta^{-1}\circ\tau=\tau\circ\tau^2\circ\tau=\tau^4=\tau.$

S_3的全体子群 $\quad |S_3|=6.$ Lagrange $\Rightarrow$ 无4,5阶

1阶：$\{\mathrm{id}\}$

2阶：$\{\mathrm{id},(1,2)\},\{\mathrm{id},(2,3)\},\{\mathrm{id},(3,1)\}$

3阶：$H=\{\mathrm{id},(1,2,3),(1,3,2)\}$

6阶：S_3

定义 看X上的对称群$\mathrm{Sym}(X)$，若$(a_1,\cdots,a_m)$是X上两两不同的元素 $(b_1,\cdots,b_k)$

且$a_i\neq b_j,\ \forall i,j$，则称轮换$(a_1,\cdots,a_m)$和$(b_1,\cdots,b_k)$是不相交的.

$(a_1,\cdots,a_m)(b_1,\cdots b_k)=(b_1,\cdots,b_k)(a_1,\cdots,a_m)$

eg. S_7

$(1,2,3)=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&4&5&6&7\end{pmatrix}$

$(4,5,6)=\begin{pmatrix}1&2&3&4&5&6&7\\1&2&3&5&6&4&7\end{pmatrix}$

没有公共的发生变动的元素.

$(1,2,3)(4,5,6)=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&5&6&4&7\end{pmatrix}$

$=$

$(4,5,6)(1,2,3)=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&5&6&4&7\end{pmatrix}$

// 双射也称为置换

$\forall \sigma \in Sym(X)$, $M(\sigma) = \{x \mid x \in X, \sigma(x) \neq x\}$

对 $\sigma_1, \sigma_2 \in Sym(X)$, 若 $M(\sigma_1) \cap M(\sigma_2) = \emptyset$, 则 $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

不相交的轮换乘法可交换

定理. S_n 中任一置换可写成若干个两两不相交的轮换的乘积(复合), 且在不计次序的情况下, 分解是惟一的.

eg. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 6 & 7 & 4 & 5 & 8 \end{pmatrix}$

$= (1,2,3)(4,6)(5,7)(8)$

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

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

$Sym(X)$ 中, $\sigma \in Sym(X)$, 任取 $x \in X$, $x \mapsto \sigma(x) \mapsto \sigma^2(x) \mapsto \cdots$

x 所在的轮换 $\exists k \in \mathbb{Z}^+$, s.t. $\sigma^k(x) = x$. $\forall i \in \{1, \cdots, k-1\}$, $\sigma^i(x) \neq x$.

$(x, \sigma(x), \sigma^2(x), \cdots, \sigma^{k-1}(x))$.

$\sigma \in Sym(X)$

定义等价关系 $(X, \sim)$ $i \sim j \Leftrightarrow \exists l \in \mathbb{Z}$, s.t. $j = \sigma^l(i)$

全体和 x 等价的元素

等价关系唯一, 等价类确定, 分解惟一.

$(1,2,3) = (1,2)(2,3)$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ 先

$(1,2,3,4) = (1,2,3)(3,4)$ $(1,2,3,4)$ 首尾相连

$= (1,2)(2,3)(3,4)$

$(a_1, a_2, \cdots, a_m) = (a_1, a_2)(a_2, a_3), \cdots (a_{m-1}, a_m)$

命题. 任一置换都能写成对换的乘积(复合)

S_n中的对换 (i,j) $(i\neq j)$ $C_n^2=\frac{n(n-1)}{2}$个. → 全需要吗?

命题. S_n可以由下面$n-1$个对换来生成: $(1,2)(2,3),\cdots(i,i+1),\cdots,(n-1,n)$

eg. $(1,3)=(1,2)(2,3)(1,2)=(1,3)$

$(1,4)=(1,3)(3,4)(1,3)=(1,2)(2,3)(1,2)(3,4)(1,2)(2,3)(1,2)$

$(i,j)(j,k)(i,j)=(i,k)$ i,j,k互不相同. 但k差得多, 可插入j缩小差距.

思考

命题. S_n可以由下面2个元素生成: $(1,2),(1,2,\cdots,n)$

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

$S_n=\{1,2,3,\cdots,n\}$ 上的双射全体

$(a_1,a_2,\cdots,a_m)$ 是两两不同的元素.

$\sigma=(a_1,a_2,\cdots,a_m)$ $\sigma(a_1)=a_2,\ \sigma(a_2)=a_3,\cdots,\sigma(a_{m-1})=a_m,\ \sigma(a_m)=a_1$

$\forall i\in\{a_1,\cdots,a_m\},\ \sigma(i)=i.$

任何一个置换都能写成不相交的轮换的乘积

$(1\ 2\ 3)(4\ 5)$ ← 不相交

相交：$(1\ 2\ \underline{3})(\underline{3}\ 4\ 5)$

eg $\begin{pmatrix}1&2&3&4&5&6&7&8\\4&7&6&8&2&3&5&1\end{pmatrix}=(1\ 4\ 8)(2\ 7\ 5)(3\ 6)$

轮换可写成对换乘积. 故置换也可写成对换乘积.

$(1,2,3)=(1,2)(2,3)$

$(1,2,3,4)=(1,2)(2,3)(3,4)$

$(a_1,a_2,\cdots,a_m)=(a_1,a_2)(a_2,a_3)\cdots(a_{m-1},a_m)$

对换写法不唯一. $(1,2)(2,3)(1,2)=(1,3)$

$\sigma=(a_1,b_1)(a_2,b_2)\cdots(a_m,b_m)=(c_1,d_1)(c_2,d_2)\cdots(c_k,d_k)$

m和k同奇偶.

判断：$(1,2)(3,4)(2,3)\neq(1,4)(2,3)(3,4)(1,2)$

I_n 单位矩阵 //交换2行(k×某一行, k×某行+另一行)

由 I_n 若干次交换2行/列 → 置换矩阵 每行/列必有且仅有1个1.

(1)

$\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\begin{pmatrix}0&1\\1&0\end{pmatrix}$

(1,2)

$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$ 交换1,2行 → $\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$ 交换2,3行 (1,2) → $\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$ (3 2 1) 交换2,3列 → $\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}$ (3 1 2)

$\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$ (2 3) $\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}$ (1 3)

对应 S_3.

有些书上：

$A'_{(i,j)}=\begin{cases}1, & j=\sigma(i)\\ 0, & j\neq\sigma(i)\end{cases}$

对 $\sigma\in S_n$，如下定义 n 阶矩阵 A

$$A_{(i,j)}=\begin{cases}1, & i=\sigma(j)\\ 0, & i\neq\sigma(j)\end{cases}$$

即：(1) $\forall j\in\{1,2,\cdots,n\}$ $A_{(\sigma(j),j)}=1$

(2) $\forall 1\le i,j\le n$, $i\neq\sigma(j)$, $A_{(i,j)}=0$.

A 是由 σ 确定的置换矩阵

事实. 定义 $f:S_n\to M_n(\mathbb{Z})$ $f(\sigma)=\sigma$ 确定的置换矩阵.

则 f 是同态，即 $f(\sigma\circ\tau)=f(\sigma)f(\tau)$

（$\circ$：复合　　$f(\sigma)f(\tau)$：矩阵乘法）

证：记 $A=f(\sigma)$, $B=f(\tau)$, $C=f(\sigma\circ\tau)$，欲证 $C=AB$

$$C_{(i,j)}=\begin{cases}1, & i=(\sigma\circ\tau)(j)=\sigma(\tau(j))\\ 0, & i\neq\sigma(\tau(j))\end{cases}$$

对 (i,j)，$(AB)_{(i,j)}=\sum_{l=1}^{n}A_{(i,l)}B_{(l,j)}=A_{(i,\tau(j))}B_{(\tau(j),j)}$ // $\forall l\neq\tau(j)$. $B_{(l,j)}=0$.

$=A_{(i,\tau(j))}=\begin{cases}1, & i=\sigma(\tau(j))\\ 0, & i\neq\sigma(\tau(j))\end{cases}$ // $A=f(\sigma)$

$=C_{(i,j)}$

(i,j) 任意性，$C=AB$. #

$f(ab)=f(a)f(b)$

$f(a_1\cdots a_m)=f(a_1)f(a_2)\cdots f(a_m)$

$\det(AB)=\det(A)\det(B)$

接着证 k,m 同奇偶：

设 $\sigma=(a_1,b_1)(a_2,b_2)\cdots(a_m,b_m)$

$f(\sigma)=f((a_1,b_1))f((a_2,b_2))\cdots f((a_m,b_m))$

$|f(\sigma)|=|f((a_1,b_1))|\cdots|f((a_m,b_m))|=(-1)^m$

若 $\sigma=(c_1,d_1)\cdots(c_k,d_k)$　　$|f(\sigma)|=(-1)^k$

$(-1)^m=(-1)^k$.　　$k\equiv m\pmod 2$

对 $\sigma \in S_n$.

记 $T(\sigma)=\{(i,j) \mid 1\le i<j\le n,\ \sigma(i)>\sigma(j)\}$ = σ 的全体逆序对

若 $\sigma=(a_1,b_1)\cdots(a_m,b_m)$

则 $m \equiv |T(\sigma)| \pmod 2$

$|T(\sigma\tau)| = |T(\sigma)| + |T(\tau)| \pmod 2$

一个置换若能写成奇数个对换的乘积，就叫奇置换；

偶　　偶

$n!$个

// S_n 中奇/偶置换对半开

子群的陪集　子群

$A_1=S_1$

定义. $A_n=\{\sigma \mid \sigma\in S_n,\ \sigma$ 是偶置换$\}$，则 $A_n \le S_n$，称为 n 次交代群.

$A_n \le S_n$.

$\sigma, \tau \in A_n$

$\sigma=(a_1,b_1)\cdots(a_m,b_m)$，$2|m$

$\tau=(c_1,d_1)\cdots(c_k,d_k)$，$2|k$.

$\sigma\tau=(a_1,b_1)\cdots(a_m,b_m)(c_1,d_1)\cdots(c_k,d_k)$

$m+k$ 个对换，$2|(m+k)$

$\sigma^{-1}=(a_m,b_m)(a_{m-1},b_{m-1})\cdots(a_1,b_1)$

$(i,j)(i,j)=1_n$.

考虑对换 $(1,2)$：$\begin{cases}\forall \sigma\in A_n,\ (1,2)\sigma \text{ 是奇置换}\\ \forall \tau\in S_n-A_n,\ (1,2)\tau \text{ 是偶置换}\end{cases}$

$S_n = A_n \cup \underbrace{(1,2)A_n}_{\text{全体奇置换}}$　　$n\ge 2$，$|A_n|=\frac{n!}{2}$

当 $n \geq 5$ 时，A_n 的正规子群只有 $\{1\}$ 和 A_n.

// ≥5次的一元多次方程无求根公式

G 是群，$a \in G$

$\begin{cases} \forall k \in \mathbb{Z}^+,\ a^k \neq |_G \\ \exists k \in \mathbb{Z}^+,\ s.t.\ a^k = |_G.\quad m = \min\{k \mid k \in \mathbb{Z}^+, a^k = |_G\} \quad o(a) = m. \quad |\langle a \rangle| = m = o(a) \end{cases}$

G 是有限群

$a \in G$，则 a 是有限阶的，$o(a) = m$，$|\langle a \rangle| = m$. $m \mid |G|$ // Lagrange：子群阶 $\mid |G|$.

对换 $(i,j)(i,j) = id$

$(1,2,3)$ $(1,2,3)(1,2,3) = (1,3,2)$

$(1,2,3)(1,2,3)(1,2,3) = (1,3,2)(1,2,3) = id$

轮换 $(a_1, a_2, \cdots, a_m)$ 阶为 m

// 1次：$a_1 \to a_2$　2次：$a_1 \to a_3$，3次：$a_1 \to a_4$，……，$m-1$次：$a_1 \to a_m$，m次 $a_1 \to a_1$.

$\sigma \in S_n$，将 σ 写成不相交的轮换之积

$\sigma = \tau_1 \tau_2 \cdots \tau_k$，每 τ_i 是轮换，两两不相交.

设 τ_i 长度为 d_i，$o(\sigma) = lcm(d_1, d_2, \cdots, d_k)$

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

3　4　2　$o(\sigma) = lcm(3,4,2) = 12$.

// 仅一个直能相接，可以收掉

eg. $\sigma = (1,2,3)(3,4,5,6)$　不满足不相交

$o(\sigma) = lcm(3,4) = 12$ ✗

$\sigma = (1,2,3,4,5,6)$　$o(\sigma) = 6$ ✓

证明：

$\sigma = \tau_1\tau_2\cdots\tau_k$，$\tau_i$ 两两不相交（有交换律 $\tau_i\circ\tau_j = \tau_j\circ\tau_i$，$\forall i,j$）

$\sigma^m = \tau_1^m\cdots\tau_k^m$

$\sigma^m = id \Leftrightarrow \forall i,\ \tau_i^m = id \quad (o(\tau_i) = d_i)$

$\Leftrightarrow \forall i : d_i \mid m$

$\Leftrightarrow lcm(d_1,\cdots,d_k) \mid m.$

计算题：置换的乘积（复合）

不相交的轮换分解

置换的阶

预告 ☆ Sylow定理 内容+证明

G有限群，$H \le G$，$|H| \mid |G|$

反过来，对 $|G|$ 的因子 $d \mid |G|$，G是否有阶数为d的子群？ 一般有反例。

eg. A_4 没有6阶子群。$|A_4| = \frac{4!}{2} = 12$

$12 = 2^2 \times 3$　2,4 3 素数幂因子有子群

个数 $\equiv 1 \pmod 2$　个数 $\equiv 1 \pmod 3$