§7. 对称群与对称多项式.

$A\neq\phi$.

$S_A := \{\sigma: A\to A \mid \sigma$ 为双射$\}$ 在映射复合下构成群

$(S_A,\circ)$: A的对称群　　注: S_A 中单位元为恒等映射.

性质: 若 $\#A=\#B>0$, 则 $(S_A,\circ)\cong(S_B,\circ)$.

Pf: 取双射 $f: A \xrightarrow{\sim} B$. 则 $\sigma\mapsto f\circ\sigma\circ f^{-1}$ 给出同构映射. □

定义: $\forall n\geq 1$. 称 $S_n := S_{\{1,2,\cdots,n\}}$ 为 n 阶对称群

称 S_n 中的元素为 $\{1,2,\cdots,n\}$ 的置换 (或排列, permutation)

例: S_1 $\{1\}\to\{1\}$, $1\mapsto 1$

S_2 $\{1,2\}\to\{1,2\}$

$\mathrm{id}\begin{cases}1\mapsto 1\\ 2\mapsto 2\end{cases}$　　$\tau\begin{cases}1\mapsto 2\\ 2\mapsto 1\end{cases}$

S_3 : $\{1,2,3\}\to\{1,2,3\}$

$1\longrightarrow a$
$2\longrightarrow b$
$3\longrightarrow c$

$\{a,b,c\}$ 为 $\{1,2,3\}$ 的一个排列

共6种排列. $\Rightarrow$ $\#S_3=3!=6$.

命题: (1) $\#S_n=n!$

(2) $\forall n\geq 3$, S_n 为非交换的.

(1) 由排列数性质可得.

(2). $n\geq 3$　$\sigma(1)=2$, $\sigma(2)=3$, $\sigma(3)=4$, $\cdots$, $\sigma(n-1)=n$, $\sigma(n)=1$

$\tau(1)=2$, $\tau(2)=1$, $\tau(3)=3$, $\cdots$ $\tau(n-1)=n-1$ $\tau(n)=n$

$\Rightarrow$ $\sigma\tau(1)=3$, $\tau\sigma(1)=1$ $\Rightarrow$ $\sigma\tau\neq\tau\sigma$ $\Rightarrow$ S_n 不交换

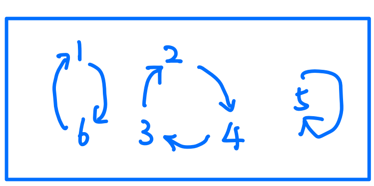
简化表达: $\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}$

$$\sigma^{-1}=\begin{pmatrix}\sigma(1), & \sigma(2), & \cdots, & \sigma(n)\\ 1, & 2, & \cdots, & n\end{pmatrix}\overset{列}{=}\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma^{-1}(1) & \sigma^{-1}(2), & \cdots, & \sigma^{-1}(n)\end{pmatrix}$$

例如: $\sigma=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$　$\sigma^{-1}=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}^{-1}=\begin{pmatrix}2&3&4&1\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$

进一步简化:

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

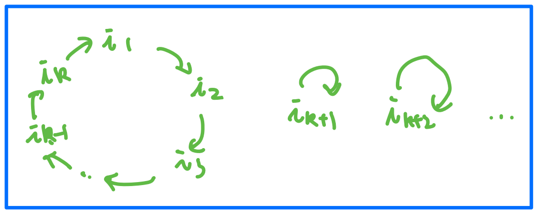


$\boxed{\begin{matrix}1\mapsto 6\mapsto 1\\ 2\mapsto 4\mapsto 3\mapsto 2\\ 5\mapsto 5\end{matrix}}$

16
243
5

∀取$\{1,\cdots,n\}$中k个元素$i_1,\cdots,i_k$ 考虑如下置换，

$$\begin{aligned} i_1 &\mapsto i_2 \\ i_2 &\mapsto i_3 \\ &\vdots \\ i_{k-1} &\mapsto i_k \\ i_k &\mapsto i_1 \\ j &\mapsto j \quad (\forall j \notin \{i_1,\cdots,i_k\}) \end{aligned}$$



将其记为 $(i_1, i_2, \cdots, i_k)$，称其为 k轮换 (k-cycle)

若 k=2，则称 (i_1, i_2) 为对换 (transposition)

若 k=1，则其为 S_n 中的单位元

性质： $(i_1\, i_2, \cdots, i_k)^{-1} = (i_k\, i_{k-1} \cdots i_1)$

定义：若 $\{i_1,\cdots,i_k\} \cap \{j_1,\cdots,j_l\} = \phi$，则称 $(i_1,\cdots,i_k)$ 与 $(j_1,\cdots,j_l)$ 不相交，否则称它们相交

例：$\begin{pmatrix}1&2&3&4&5&6\\6&4&2&3&5&1\end{pmatrix} = (16)(243)$

定理 (1) σ_1, σ_2 = 不相交的两轮换 ⇒ $\sigma_1\sigma_2 = \sigma_2\sigma_1$

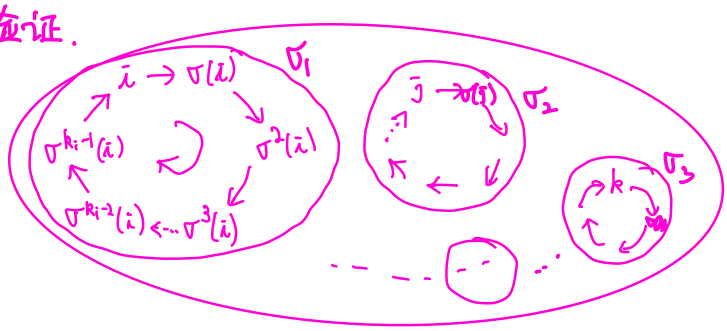
(2) $\forall \sigma \in S_n$ ∃两两不交的轮换 $\sigma_1, \sigma_2, \cdots, \sigma_s$ s.t.

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

且表达在去除1轮换下唯一.

Pf：(1) 直接验证.

(2)、存在性：



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

唯一性：$\sigma = \sigma'$ ⇔ $D_\sigma = D_{\sigma'}$ ⇔ σ 与 σ' 箭头相同.

例：$(15)(24)(13) = (135)(24)$

$(1234)(3456)(5678) = (123)(45)(678)$

例：

$S_2 = \{1,$
$\quad (12)\}$

$2 = 1+1 \quad 1^2$
$\;\; = 2 \quad 2^1$

$S_3 = \{1,$
$\quad (12), (13), (23),$
$\quad (123), (132)\}$

$3 = 1+1+1 \quad 1^3$
$\;\; = 2+1 \quad 1^1 2^1$
$\;\; = 3 \quad 3^1$

$S_4 = \{1,$
$\quad (12), (13), (14), (23), (24), (34)$
$\quad (123)\,(132), (124), (142), (134), (143), (234), (243)$
$\quad (1234), (1243), (1324), (1342), (1423), (1432)$
$\quad (12)(34), (13)(24), (14)(23)\}$

$4 = 1+1+1+1 \quad 1^4$
$\;\; = 2+1+1 \quad 1^2 2^1$
$\;\; = 3+1 \quad 1^1 3^1$
$\;\; = 4 \quad 4^1$
$\;\; = 2+2 \quad 2^2$

$$n = \underbrace{1+\cdots+1}_{\lambda_1} + \underbrace{2+\cdots+2}_{\lambda_2} + \cdots + \underbrace{n+\cdots+n}_{\lambda_n} \qquad \lambda_1, \cdots, \lambda_n \geq 0$$

$\hookrightarrow$ n 的一个拆分，记为 $(i_1, i_2, \cdots, i_n)$

分拆函数

$$P(n) := \# \{ \underbrace{(\lambda_1, \cdots, \lambda_n)}_{\hookrightarrow\ n\text{ 的一个分拆 (partition)}} \mid \lambda_i \geq 0,\ \sum_{i=1}^{n} i\lambda_i = 0 \}$$

例：$P(2) = 2$，$P(3) = 3$，$P(4) = 5$

定义：$\sigma\in S_n$ 若 σ 写为两两不交的轮换乘积中 k 轮换的个数为 λ_k ($k=1$, $\lambda_1=\#\{1,\dots,n\}^{\sigma}$)，则称 **σ 的型** 为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ （对应一个拆分，型的总数为分拆函数）

性质：1) $\forall\, \sigma,\sigma'\in S_n$

σ 与 σ' 共轭 $\Longleftrightarrow$ σ 与 σ' 有相同的型.

2) S_n 中恰有 $p(n)$ 个共轭类

Pf: • $\forall\, \sigma=(i_1\cdots i_k)(j_1\cdots j_l)\cdots$

$$\tau\sigma\tau^{-1}=\big(\tau(i_1),\dots,\tau(i_k)\big)\cdot\big(\tau(j_1)\cdots\tau(j_l)\big)\cdots$$

• $\forall\, \sigma=(i_1\cdots i_k)(j_1\cdots j_l)\cdots$

$\sigma'=(i_1'\cdots i_k')(j_1'\cdots j_l')\cdots$

令 $\tau=\begin{pmatrix} i_1 & \cdots & i_k & j_1 & \cdots & j_l & \cdots \\ i_1' & \cdots & i_k' & j_1' & \cdots & j_l' & \cdots \end{pmatrix}$ 则 $\tau\sigma\tau^{-1}=\sigma'$

奇置换与偶置换

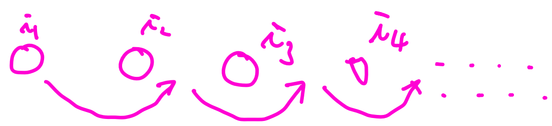
命题: 1) $(i_1,\cdots,i_k)=(i_1\, i_k)(i_1\, i_{k-1})\cdots(i_1\, i_2)$

2) S_n 由对换生成.

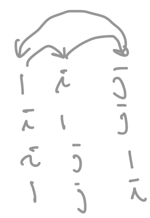
3) 更一般地, S_n 可由 $(12),(13),\cdots,(1n)$ 生成.

或由 $(12),(23),\cdots,(n-1,n)$ 生成.

Pf: (1)



$$(i_1\, i_k)(i_1, i_{k-1})\cdots(i_1\, i_2)\,(j) = \begin{cases} j & \forall j\notin\{i_1,\cdots,i_k\} \\ (i_1\, i_k)\cdots(i_1\, i_{l+1})(i_1, i_l)(j)=i_{l+1} & j=i_l \\ (i_1\, i_k)(j)=i_1 & j=i_k \end{cases}$$



$$= (i_1,\cdots,i_k)(j)$$

(2). $$(i\,j)=(1\,i)(1\,j)(1\,i)\overset{i<j}{=}(i,i+1)(i+1,i+2)\cdots(j-2,j-1)(j-1,j)(j-2,j-1)\cdots(i+1,i+2)(i,i+1)$$

注: 表达不唯一!

定理: 将一个置换写成对换乘积时, 对换个数的奇偶性不依赖于写法.

定义: 偶置换 (even permutation) := 偶数个对换的乘积

奇置换 (odd permutation) := 奇数个对换的乘积

性质: 1) 奇奇=偶; 奇偶=奇; 偶偶=偶.

2) $\sigma\in S_n$ 的型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ $\Rightarrow$ σ 与 $\sum_{i=1}^{n}\lambda_i(i-1)$ 有相同的奇偶性.

Pf: k 轮换可写为 $k-1$ 个对换的乘积. □

推论: $\exists!$ 群同态 $\varepsilon: S_n\to\{\pm1\}$ s.t. ε(对换) $=-1$

Pf: ε(奇置换) $:=-1$ $\quad$ ε(偶置换) $=1$ □

定义: $n(\sigma) := \#\{(ij) \mid \sigma(i) > \sigma(j) \ \& \ i<j\}$

↳ 置换 σ 的交错数

性质: σ 可写为 $n(\sigma)$ 个对换的乘积.

Pf: 对 $n(\sigma)$ 归纳.

(1) $n(\sigma)=0$ ✓ 设 $n(\sigma)<k \Rightarrow$ ✓

若 $n(\sigma)=k>0$ 则 $\exists i$ s.t. $\sigma(i)>\sigma(i+1)$ (否则 $\sigma=(1)$)

$$\tau := (\sigma(i)\ \sigma(i+1))\cdot\sigma = \begin{pmatrix} 1 & \cdots & i-1 & i & i+1 & i+2 & \cdots & n \\ \sigma(1) & \cdots & \sigma(i-1) & \sigma(i+1) & \sigma(i) & \sigma(i+2) & \cdots & \sigma(n) \end{pmatrix}$$

则 $n(\tau) = n(\sigma)-1 = k-1$. $\Rightarrow$ τ 可写为 $k-1$ 个对换之积

$\Rightarrow$ $\sigma = (\sigma(i)\,\sigma(i+1))\tau$ 可写为 k 个对换之积.

注: $\sigma\cdot(i,i+1) = \begin{pmatrix} 1 & \cdots & i & i+1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(i+1) & \sigma(i) & \cdots & \sigma(n) \end{pmatrix} \Rightarrow n(\sigma(i,i+1)) = n(\sigma) \pm 1.$

$\equiv n(\sigma)+1 \mod 2$

定理证明: 仅需证明若 $\sigma=(i_1\, j_1)(i_2\, j_2)\cdots(i_m\, j_m)$, 则 $m \equiv n(\sigma) \mod 2$.

$\Rightarrow$ $\sigma = (k_1,k_1+1)(k_2,k_2+1)\cdots(k_{m'},k_{m'}+1)$ $\quad (m \equiv m' \mod 2)$

$\Rightarrow$ $0 = n\big(\sigma(k_{m'},k_{m'}+1)\cdots(k_2,k_2+1)(k_1,k_1+1)\big)$

$= n(\sigma)+m' \mod 2$

$\Rightarrow$ $m \equiv m' \equiv n(\sigma) \mod 2$ ✓

§7.2.2. 交错群

定义：$A_n := \ker \varepsilon = \{偶置换\} < S_n$

↳ n阶交错群 (alternating group)

性质：1) $A_n \trianglelefteq S_n$ $\quad \# A_n = \frac{n!}{2}$

2) $K_4 := \{(1), (12)(34), (13)(24), (14)(23)\} \trianglelefteq S_4$

($\Rightarrow K_4 \trianglelefteq A_4$)

Pf: 1) 奇偶=偶，偶·偶=偶 $\Rightarrow$ ✓

2) 直接验证 $K_4 < S_n$，而 K_4 为全体 $1^4, 2^2$ 型置换

K_4 关于共轭封闭.

定义：若群 $G \neq 1$ 无非平凡正规子群，则称 G 为单群 (Simple group)

例：$G \neq 1$ 交换 则 G 单 $\Leftrightarrow$ $\# G$ 为素数.

$\Leftarrow$) ✓

$\Rightarrow$) $\forall g \in G \setminus \{1\} \Rightarrow \langle g \rangle \overset{\{1\}}{\underset{\neq}{\trianglelefteq}} G \Rightarrow G = \langle g \rangle \quad \forall p \mid \# G$ (素)

$\Rightarrow \langle g^{\frac{\# G}{p}} \rangle \underset{\neq}{\trianglelefteq} G \Rightarrow g^{\frac{\# G}{p}} = 1 \Rightarrow \# G = p.$

定理：A_n $(n \geq 5)$ 为单群.

有限单群分类定理 (Classification theorem of the finite simple groups)

- 素数阶循环群
- 交错群 A_n $(n \geq 5)$
- 李型单群 (Simple gps of Lie type)
  ↳ ABCD / EFG
- 26个散在单群

- 1955 → 2004
- 100作者 500篇 1万页
- A_5 最小非交换单群

$\forall f: \mathbb{Z}^n \to \mathbb{Z}.\ \forall \sigma \in S_n.\ \sigma(f)(x_1,\cdots,x_n) := f(x_{\sigma(1)},\cdots,x_{\sigma(n)})$

$\Rightarrow \sigma(f): \mathbb{Z}^n \to \mathbb{Z}.$

例: $n=3,\ \sigma=(123)\quad f = x_3^2 - x_1 \Rightarrow \sigma(f) = x_1^2 - x_2$

引理: 1) $\sigma = 1 \Rightarrow \sigma(f) = f$

2) $(\sigma\tau)(f) \Rightarrow \sigma(\tau(f))$ $\Big\}$ $S_n \curvearrowright Map(\mathbb{Z}^n, \mathbb{Z})$

3) σ 为 $\mathbb{Z}$-线性. 即

$\sigma(f+g) = \sigma(f) + \sigma(g),\ \sigma(cf) = c\sigma(f)$ $\Big\}$ 作用为 $\mathbb{Z}$-线性.

Pf: 1), 3) 显然

2): $\tau(f)(x) = f(x_{\tau(1)},\cdots,x_{\tau(n)})$

$\Rightarrow \sigma(\tau(f))(x) = f(x_{\sigma(\tau(1))},\cdots,x_{\sigma(\tau(n))}) = f(x_{\sigma\tau(1)},\cdots,x_{\sigma\tau(n)})$

$= (\sigma\tau)(f)$ □

定理: $\forall n \geq 2$、$\exists!$ 非平凡群同态 $\varepsilon: S_n \to \{\pm 1\}$. s.t. ε(对换) $= -1$.

Pf: (存在性) $\Delta(x_1,\cdots,x_n) := \prod_{1\le i<j\le n} (x_i - x_j)$ 则 $\forall$ 对换 τ

$\tau\Delta = -\Delta.$

$\forall \sigma \in S_n. \Rightarrow \exists i$ s.t. σ 为 i 个对换乘积

$\Rightarrow \sigma\Delta = (-1)^i \Delta$

$\Rightarrow \varepsilon(\sigma) := (-1)^i$ 良定义 (不依赖于 i 的选取)

$\sigma\tau(\Delta) = \sigma(\tau(\Delta)) \Rightarrow \varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau).$

$\Rightarrow \varepsilon$ 为群同态.

(唯一性) $(ij) = (1i)(1j)(1i) \Rightarrow \varepsilon((ij)) = \varepsilon((1j))$

$(1j) = (2j)(12)(2j) \Rightarrow \varepsilon((1j)) = \varepsilon((12))$ $\Big\}$

$\Rightarrow \varepsilon((ij)) = \varepsilon((12)).$

ε 非平凡 $\Rightarrow \varepsilon((12)) = -1$ (否则 $\varepsilon(\sigma) = 1\ \forall\sigma$)

$\Rightarrow \varepsilon((ij)) = -1 \Rightarrow \checkmark.$

§ 对称多项式

定义: 称 $f\in R[x_1,\cdots,x_n]$ 为对称多项式, 若 $\forall\sigma\in S_n$, 皆有
$$f(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)}) = f(x_1,\cdots,x_n)$$
即 $\sigma(f)=f$, $\forall\sigma\in S_n$.

例: 1) $x_1^k+\cdots+x_n^k$

2) $F(x)=(x-x_1)(x-x_2)\cdots(x-x_n) = x^n - s_1x^{n-1}+s_2x^{n-2}+\cdots+(-1)^n s_n$.

韦达定理 $\Rightarrow$
$$\left.\begin{aligned}
s_1 &= x_1+x_2+\cdots+x_n\\
s_2 &= \sum_{1\le i<j\le n} x_ix_j\\
&\vdots\\
s_k &= \sum_{1\le i_1<i_2<\cdots<i_k\le n} x_{i_1}x_{i_2}\cdots x_{i_k}\\
&\vdots\\
s_n &= x_1x_2\cdots x_n
\end{aligned}\right\}\text{初等对称多项式}$$

定理: 任意对称多项式均为初等对称多项式的多项式.

i.e. $\forall f$ 对称 $\exists g$ s.t. $f(x_1\cdots x_n)=g(s_1,\cdots,s_n)$.

定理: $s_1,s_2,\cdots,s_n$ 代数独立.

即 $f\in R[x]\setminus\{0\}\Rightarrow f(s_1,\cdots,s_n)\neq 0$. 也说明 g 的选取唯一.

Pf: 反证. 设 n 为最少的变元数使得结论不成立.

设 $f\neq 0$ 为次数最小的非零多项式使得 $f(s_1,\cdots,s_n)=0$.
$$f = f_0(s_1,\cdots,s_{n-1}) + f_1(s_1,\cdots,s_{n-1})s_n+\cdots+f_d(s_1,\cdots,s_{n-1})s_n^d$$
$\Rightarrow f_0\neq 0$ (否则 $x_n\mid f$ $\left(\psi:=\frac{f}{x_n}\right)\Rightarrow \psi(s_1,\cdots,s_n)=0$ ↯)

$\overset{x_n=0}{\Rightarrow}$ $0=f((s_1)_0,\cdots,(s_{n-1})_0,0)=f_0((s_1)_0,\cdots,(s_{n-1})_0)$ ↯ (与 n 的最小性)

定义：称 $D_f = D(x_1,\cdots,x_n) = \prod\limits_{i<j}(x_i-x_j)^2$ 为 $f(x)=(x-x_1)\cdots(x-x_n)$ 的判别式.

例 1). $f = x^2+bx+c \Rightarrow D_f = b^2-4c$

2). $f = x^3+ax+b \Rightarrow D_f = -4a^3-27b^2$