第四次习题课.

- 置换: $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}$

- 逆序: 若 $i<j$ 有 $\pi(i)>\pi(j)$ 则称 $(\pi(i),\pi(j))$ 为一个逆序对

- 逆序数: $inv(\pi)=|\{(i,j) \mid i<j \text{ 且 } \pi(i)>\pi(j)\}|$

例: $\pi=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$

逆序集: $\{(4,3),(4,2),(4,1),(3,2),(3,1),(2,1),(5,1)\}$

$inv(\pi)=7$

- 符号: $sgn(\pi)=(-1)^{inv(\pi)}$

定义一致

奇置换 → 符号 -1 可以写成奇数个对换之积.

偶置换 → 符号 $+1$. 可以写成偶数个对换之积.

- 命题: 一次对换改变了置换逆序数的奇偶性.

证: ① 相邻对换 $\sigma=(\pi(p),\pi(p+1))$

$\begin{pmatrix} 1 & 2 & \cdots & p & p+1 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(p) & \pi(p+1) & \cdots & \pi(n) \end{pmatrix}$

若 $\pi(p)<\pi(p+1)$, 则对换 σ 增加一个逆序

若 $\pi(p)>\pi(p+1)$, 则对换 σ 减少一个逆序.

$\Rightarrow$ 逆序数奇偶性改变.

② 先证: 任意对换可以表示为奇数个相邻对换的乘积.

(p,q) $(1\le p<q\le n)$ 共 $2(q-p)-1$ 步

$(p,q)=(p,p+1)(p+1,p+2)\cdots(q-1,q)$

$\cdot(q-2,q-1)\cdots(p,p+1)$

$\Rightarrow$ 回到情形①去考虑. $\Rightarrow$ 逆序数奇偶性改变.

命题2: 任何置换都可以通过有限次对换变为恒同置换
并且对换形式不唯一.

证: 归纳法.

① $n=2$ $(12)(21)=e$

② 假设命题对任意 $n-1$ 长的置换成立.

则对 $\sigma=\sigma(1)\sigma(2)\cdots\sigma(n)$

$\exists\ p$, s.t. $\sigma(p)=n$ 则对换 $\sigma(p)$ 与 $\sigma(n)$ 可得

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

$\Rightarrow \tilde{\sigma} \in S_{n-1}$

$\Rightarrow$ 由归纳假设 $\tilde{\sigma}$ 可通过有限次对换变为 e

$\Rightarrow \sigma=(\sigma(p),\sigma(n))\cdot\tilde{\sigma}$ 亦成立.

综上, 命题得证.

命题3: 设 $\pi=\pi_1\cdots\pi_k$ 为一个对换乘积分解. 则 $sgn(\pi)=(-1)^{inv(\pi)}=(-1)^k$

即 $inv(\pi)$ 与 k 奇偶性相同.

证: 注: $inv(e)=0$ 为偶数.

由于命题2.

任意 π 可以连续地通过对换 $\pi_1,\cdots\pi_k$ 变为 e

而由命题1, 每次对换会改变逆序数的奇偶性

$\Rightarrow (-1)^0=(-1)^k sgn(\pi)$ $\Rightarrow sgn(\pi)=(-1)^k$

例: $\pi=\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}=(1,n)(2,n-1)\cdots(i,n-i)$

$inv(\pi)=1+2+\cdots+(n-1)=\frac{(n-1)n}{2}$

n 偶: $k=\frac{n}{2}$ $\Rightarrow sgn(\pi)=(-1)^{\frac{n}{2}}$

n 奇: $k=\frac{n-1}{2}$ $\Rightarrow sgn(\pi)=(-1)^{\frac{n-1}{2}}$

$$\operatorname{sgn}(\pi)=\left((-1)^{n+1}\right)^{\frac{n}{2}}=(-1)^{\frac{n}{2}} \quad (n \text{ 偶})$$

$$\operatorname{sgn}(\pi)=\left((-1)^{n}\right)^{\frac{n+1}{2}}=(-1)^{\frac{n+1}{2}} \quad (n \text{ 奇}).$$

命题4: 当 $n\geq 3$ 时，证明任何偶置换都可以写成 3-循环的乘积.

证: $\pi=\tau_1\tau_2\cdots\tau_{2m-1}\tau_{2m}$，其中 τ_i 为对换.

考虑两个相邻的对换 $\tau_{2j-1}\tau_{2j}$ $1\leq j\leq m$

现证 $\tau_{2j-1}\tau_{2j}$ 可以写成 3-循环之积.

设 $\tau_{2j-1}=(s,t)$ $\tau_{2j}=(s',t')$

① 若 $\{s,t\}\cap\{s',t'\}=\varnothing$

则 $(s,t)(s',t')=(s,t)(t,s')(t,s')(s',t')$

$=(s,t,s')(t,s',t')$ (s,t,t').

$\cdots s\cdots t\cdots s'\cdots t'\to\cdots t\cdots s\cdots t'\cdots s'$ $\cdots s\cdots t\cdots s'\cdots t'\cdots\to\cdots t\cdots s'\cdots s\cdots t'\cdots$

$\to\cdots t\cdots s\cdots t'\cdots s'\cdots$

② 若 $\{s,t\}\cap\{s',t'\}\neq\varnothing$

若 $s=s'$ 则 $(s,t)(s,t')=(s,t',t)$

若 $s=t'$ 则 $(s,t)(s',s)=(s,s',t)$

若交集中元素为 t 同理可得

综上，由于每对相邻对换可化为 3-循环之积 $\Rightarrow$ 命题成立.

命题5: S_n 中任何置换都可写成对换.

$(1,2),(1,3),(1,4)\cdots(1,n-1),(1,n)$ 的乘积.

证: 由于 引理6.20 (讲义)

任何置换可写成若干对换之积.

而 $(i,j)=(1,i)(1,j)(1,i)$

$\Rightarrow$ 命题成立

$1\cdots i\cdots j\longrightarrow 1\cdots j\cdots i$

$\searrow\ i\cdots 1\cdots j\longrightarrow i\cdots j\cdots 1\to 1\cdots j\cdots i$

中国剩余定理：

中国的古代数学典集《孙子算经》中有：

"今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？"

$\Leftrightarrow$ 同余方程组：

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \quad (*)$$

方程(*)的系统解法：秦九韶《数书九章·大衍求一术》

现代数学家程大位：《孙子歌诀》

"三人同行七十希，五树梅花廿一支，七子团圆正半月，除百零五便得知."

$r_3 \times 70 + r_5 \times 21 + r_7 \times 15 = r \times 105 + x$. $\Rightarrow x$ 即为所求.

设 $\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_m \pmod{n_m} \end{cases}$

假设 $n_1, n_2, \cdots, n_m$ 任意两两互素.

则对 $\forall\, a_1, a_2, \cdots, a_m \in \mathbb{Z}$

方程组有解

且可如下构造得到：

设 $N = n_1 \cdot n_2 \cdots n_m$ 并对 $\forall i \in \{1, 2, \cdots m\}$

设 $N_i = \dfrac{N}{n_i}$

设 $t_i = N_i^{-1}$ 即 $N_i \cdot t_i \equiv 1 \pmod{n_i}$

则方程组的通解形式为：

$$x = a_1 t_1 N_1 + a_2 t_2 N_2 \cdots + a_m t_m N_m + kN \quad (k \in \mathbb{Z})$$

在模 N 意义下方程组只有一个解 $x = \sum_{i=1}^{m} a_i t_i N_i$

例：$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$

$N = 3\times5\times7 = 105$

$N_1 = 35 \quad N_2 = 21 \quad N_3 = 15$

$t_1 = 2 \quad t_2 = 1 \quad t_3 = 1$

$N_i \cdot t_i \equiv 1 \pmod{n_i}$

$N_i \cdot t_i \equiv 0 \pmod{n_j} \quad j \neq i$

因为 $N_i = n_1 \cdots \hat{n_i} \cdots n_j \cdots n_m$.

$$70 = 2\times35 \equiv \begin{cases} 1 \pmod 3 \\ 0 \pmod 5 \\ 0 \pmod 7 \end{cases}$$

$$21 = 1\times21 \equiv \begin{cases} 0 \pmod 3 \\ 1 \pmod 5 \\ 0 \pmod 7 \end{cases}$$

$$15 = 1\times15 \equiv \begin{cases} 0 \pmod 3 \\ 0 \pmod 5 \\ 1 \pmod 7 \end{cases}$$

$\Rightarrow$ 将原方程的余数相应乘到这三个基础解上再相加

$$\Rightarrow 2\times70 + 3\times21 + 2\times15 \equiv \begin{cases} 2\times1+3\times0+2\times0 \equiv 2 \pmod 3 \\ 2\times0+3\times1+2\times0 \equiv 3 \pmod 5 \\ 2\times0+3\times0+2\times1 \equiv 2 \pmod 7 \end{cases}$$

$\Rightarrow x = 233 + k\times105 \quad (k\in\mathbb{Z})$