习题课讲义：

1) 偏序集与偏序关系

设 R 为集合 A 上的偏序关系，则 R 满足：

① 自反性，$\forall x\in A$，xRx

② 反对称性：$\forall x,y\in A$，xRy 且 $yRx \Rightarrow x=y$

③ 传递性：$\forall x,y,z\in A$，xRy 且 $yRz \Rightarrow xRz$

称 (A, R) 为偏序结构，一般我们用 $\le$ 来记偏序关系

在偏序集中，我们可以定义：设 $x\in A$

① 如果不存在 $y\in A$ 满足 $y\neq x$ 且 $y\geq x$ $(y\le x)$，则称 x 为极大元 (极小元)

② 如果对 $\forall y\in A$ 都有 $y\le x$ $(x\le y)$，则称 x 为最大元 (最小元)

③ 设 $B\subseteq A$. 如果 $\forall y\in B$ 都有 $y\le x$ $(x\le y)$，则称 x 为 B 的上界 (下界)

④ 设 $B\subseteq A$. 如果 $\forall a,b\in B$ 都满足要么 $a\le b$ 要么 $b\le a$ (即 a,b 可比较) 则称 B 为 A 的全序子集

注 (1) 一个偏序集 A 中可能不存在极大元，并且即使极大元存在也不一定是唯一的.

例：集合 $\mathbb{R}$ 对实数的大小关系 $\le$ 不存在极大元.

集合 $\{6,8,3,4,2,1\}$ 对于整除关系存在两个极大元 6 与 8，但有唯一的极小元且为最小元.

(2) 偏序集 A 的子集 B 的上界不一定存在且即使存在也不一定在 B 中.

例：$\mathbb{R}$ 的子集 $(0,+\infty)$ 不存在上界. 设 $A=\{24,12,6,8,4,3,2,1\}$

$B=\{6,8,4,3,2,1\}$，则 24 为 B 的上界 但 $24\notin B$.

命题1 有限非空偏序集一定存在极大元。

(证明一) 我们利用反证法来证明：

设 S 为非空有限偏序集且 $\leq$ 为偏序关系. 假设 S 中不存在极大元. 由于 S 非空，任取 $x_1 \in S$. 因为 S 中不存在极大元，所以 x_1 不是 S 的极大元，即存在 $x_2 \in S$ 满足 $x_2 \neq x_1$ 且 $x_1 \leq x_2$. 又因为 x_2 也不是极大元，则存在 $x_3 \in S$ 满足 $x_3 \neq x_2$ 且 $x_2 \leq x_3$. 如此重复该过程可构造一列互不相同的元素：$x_1 \lneq x_2 \lneq x_3 \lneq x_4 \lneq \cdots \lneq x_n \lneq \cdots$

这与 S 为有限集矛盾！

(证明二) 利用数学归纳法证明：对 S 的元素个数 n 作归纳

1) 当 $n=1$ 时，S 中的唯一元素为 S 的极大元，命题成立.

2) 假设命题对 $n=k$ 成立. 下面考虑 $n=k+1$ 情形. 任取 S 中一个元素 x. 考虑 $S' = S \setminus \{x\}$. 则 $|S'| = k$. 由归纳假设，S' 中存在极大元 $y \in S' \subseteq S$. 下面分两种情形讨论：(i) $y \leq x$，则 x 为 S 的极大元（否则存在 $z \in S'$，满足 $z \geq x \Rightarrow z \geq y$，与 y 为 S' 中极大元矛盾！）

(ii) x 与 y 不可比或 $x \leq y$，则 y 为 S 的极大元.

命题二 设 S 为有限非空偏序集. 如果 x 为 S 的唯一极大元，则 x 为 S 的最大元.

证明 $\forall y \in S$，我们要证 $y \leq x$. 因为 x 为 S 的极大元. 则有要么 $y \leq x$ 要么 y 与 x 不可比较. 设 $T = \{y \in S \mid y 与 x 不可比较\}$. 下面只需证明 T 为空集. 否则 T 中存在极大元 y_0. 下面说明 y_0 也是 S 的极大元. $\forall z \in S \setminus T$，如果 $z \geq y_0$，则有 $x \geq y_0$，这与 x 与 y_0 不可比较矛盾. 于是 y_0 为 S 的极大元 但 $y_0 \neq x$，这与 x 是 S 的唯一极大元矛盾！

2) 中国剩余定理

在中国的古代数学典集《孙子算经》中有这么一个问题。

"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？"

用现代的数学语言来描述该问题为：设 x 为未知整数，x 为如下同余方程组的解：

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

求 x？ 更一般地，我们可以考虑同余方程组。

$$\begin{cases} x \equiv a_1 \mod p_1 \\ x \equiv a_2 \mod p_2 \\ \vdots \\ x \equiv a_m \mod p_m \end{cases}$$

其中 $p_1, \cdots, p_m$, $a_1, \cdots, a_m \in \mathbb{Z}$ 且有 $p_1, p_2, \cdots, p_m$ 两两互素

方程 (*) 的系统解法是秦九韶在《数书九章·大衍求一术》中给出的。"大衍求一术"是中国古算中最独创性的成就之一。

明代著名数学家程大位在其《算法统宗》中用一首歌诀来给出了 (*) 的解答：《孙子歌》

三人同行七十稀；
五树梅花廿一枝；
七子团圆正半月，
除百零五便得知。

$$2\times 70 + 3\times 21 + 2\times 15 = 233\ (-105-105 = 23)$$

辗转相除法(扩展欧几里得算法): 任给两个整数 $a,b \in \mathbb{Z}$, 存在 $s,t \in \mathbb{Z}$ 满足

$$\gcd(a,b) = s\cdot a + t\cdot b$$

<u>例子</u> $a=3$, $b=35$ $\quad \gcd(3,35)=1$

$$\left.\begin{aligned} 35 &= 11\times 3 + 2 \\ 3 &= 1\times 2 + \underline{\underline{1}} \\ 2 &= 2\times 1 + 0 \end{aligned}\right\} \text{反代回去} \quad \begin{aligned} 1 &= 3 - 1\times 2 \\ &= 3 - 1\times(35 - 11\times 3) \\ &= 3 + 11\times 3 - 1\times 35 \\ &= 12\times 3 - 1\times 35 \end{aligned}$$

可得 $s=12$, $t=-1$

$$(**)\begin{cases} x \equiv a_1 \mod p_1 \\ x \equiv a_2 \mod p_2 \\ \vdots \\ x \equiv a_m \mod p_m \end{cases}$$

我们分两步讨论:

① $$(***)\begin{cases} x \equiv 1 \mod p_1 \\ x \equiv 0 \mod p_2 \\ \vdots \\ x \equiv 0 \mod p_m \end{cases}$$

因为 $p_1,\dots,p_m$ 两两互素, 则有 $\gcd(p_1, p_2p_3\cdots p_m)=1$

由扩展欧几里得算法可求得 $s_1, t_1 \in \mathbb{Z}$ 满足:

$$s_1p_1 + t_1p_2p_3\cdots p_m = 1$$

取 $x = t_1p_2p_3\cdots p_m$, 则 x 满足 $(***)$

$$= 1 - s_1p_1$$

类似地 可以求解如下方程组: $$(***)_i\begin{cases} x \equiv 1 \mod p_i \\ x \equiv 0 \mod p_j \end{cases} \quad j \in \{1,2,\dots,m\}\setminus\{i\}$$

因为 $\gcd(p_i, \prod_{j\neq i} p_j)=1$, 由扩展欧几里得算法可得: $\boxed{s_ip_i + t_i\prod_{j\neq i} p_j = 1}$

即求得 $x_i \in \mathbb{Z}$ 满足 $(***)_i$

$$x_i = t_i\prod_{j\neq i} p_j$$

② $\begin{cases} x \equiv a_1 \mod p_1 \\ x \equiv a_2 \mod p_2 \\ \vdots \\ x \equiv a_m \mod p_m \end{cases}$ 的解可表为 $a_1 x_1 + a_2 x_2 + \cdots + a_m x_m + k\prod_{i=1}^{m} p_i$

我们来考虑开始的同余方程组: $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases}$

① $\begin{cases} x_1 \equiv 1 \mod 3 \\ x \equiv 0 \mod 5 \\ x \equiv 0 \mod 7 \end{cases}$ $\quad 12 \times 3 - 1 \times 5 \times 7 = 1$

$x_1 = -35$

也可以将 x_1 调为正解, 即 $\underline{-23} \times 3 + \underline{2} \times 35 = 1$

$\boxed{x_1 = 70}$

② $\begin{cases} x_2 \equiv 0 \mod 3 \\ x_2 \equiv 1 \mod 5 \\ x_2 \equiv 0 \mod 7 \end{cases}$ $\quad -4 \times 5 + \underline{1} \times 3 \times 7 = 1$

$\boxed{x_2 = 21}$

③ $\begin{cases} x_3 \equiv 0 \mod 3 \\ x_3 \equiv 0 \mod 5 \\ x_3 \equiv 1 \mod 7 \end{cases}$ $\quad -2 \times 7 + 1 \times 3 \times 5 = 1$

$\boxed{x_3 = 15}$

$x = 2x_1 + 3x_2 + 2x_3$

$= 2 \times 70 + 3 \times 21 + 2 \times 15 = 233 \Longrightarrow 233 - 2 \times 105$

$= \boxed{23}$

置换的逆序数与符号

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

称 $(\pi(i), \pi(j))$ 为一对逆序 若 $i<j$ 但 $\pi(i)>\pi(j)$.

π 的所有逆序构成一个集合，其集合的元素个数称为 π 的逆序数 记为 $inv(\pi)$

例.

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

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

则 $inv(\sigma) = 7$. 定义: $sgn(\pi) = (-1)^{inv(\pi)}$.

我们将证明这个符号定义与通过对换个数来定义符号的方法是一致的.

命题1. 一次对换改变逆序数的奇偶性.

证. 情形一. 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 $\pi(p)$ 与 $\pi(p+1)$, 逆序数增加1

若 $\pi(p) > \pi(p+1)$, 则对换 $\pi(p)$ 与 $\pi(p+1)$, 逆序数减少1.

所以对于相邻对换, 逆序数奇偶性改变, 即 $sgn(\pi)$ 变号

$sgn(\sigma\pi) = -sgn(\pi)$

情形二. 因为任意对换可以表示为奇数个相邻对换乘积.
每个相邻对换改变逆序数奇偶性1次, 所以奇数次改变奇偶性等价于1次奇偶性改变.

①

$1\ 2\ 3\ 4 \to 4\ 2\ 3\ 1$

$\to 2\ 1\ 3\ 4 \to 2\ 3\ 1\ 4 \to 2\ 3\ 4\ 1 \to 2\ 4\ 3\ 1 \to 4\ 2\ 3\ 1$

命题2. 任何置换都可以通过有限次对换变为恒同置换，并且对换方式不唯一。

证. (归纳法)

1) $n=2$ $(12)\underbrace{(12)}_{1\text{次对换}}=e$

2) 假设结论对 $n-1$ 个元素的置换成立. 因为 $(\pi(1),\cdots\pi(n))$ 中必有某个 $\pi(p)=n$，则对换 $\pi(p)$ 与 $\pi(n)$，得到

$$\underbrace{\pi(1),\cdots,\pi(p-1)\ \pi(n)\ \pi(p+1),\cdots,\pi(n-1)}, n$$

前 $n-1$ 个元素为 $n-1$ 个元素 $\{1,2\cdots n-1\}$ 的置换，由归纳假设，存在有限个对换将其变为 $12\cdots n-1$. 由此命题得证.

命题3 $\pi=\pi_1\cdots,\pi_k$ 为一个对换乘积分解.

则 $sgn(\pi)=(-1)^{inv(\pi)}=(-1)^k$. 即 k 的奇偶性与逆序数奇偶性相同.

证明: 注意 $inv(e)=0$ 为偶的.

π 可以连续地通过对换 $\pi_1,\cdots,\pi_k$ 变为 e

每次对换改变逆序数的奇偶性. 即有

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

例1.

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

① n 为偶数 $sgn(\sigma)=(-1)^{\frac{n}{2}}$

② n 为奇数 $sgn(\sigma)=(-1)^{\frac{n-1}{2}}$

$n : n-1$

$n-1 : n-2$

$\vdots$

$2 : 1$

逆序数 $inv(\sigma)=1+2+\cdots+n-1=\frac{(n-1)n}{2}$

$sgn(\sigma)=(-1)^{\frac{(n-1)n}{2}}$

$+ - - + + - - +$

②

例2. 当$n\geq 3$时，证明任何偶置换都可以写成3-循环的乘积

证明： $\pi=\tau_1\tau_2\cdots\tau_{2m-1}\tau_{2m}$

τ_i 为对换

考察相邻两个对换 $\tau_{2j-1}\tau_{2j}$，$j=1,2,\cdots,m$，只需证 $\tau_{2j-1}\tau_{2j}$ 可以写成

3-循环乘积。可以设 $\tau_{2j-1}=(s,t)$，$\tau_{2j}=(s',t')$

情况1： $\{s,t\}\cap\{s',t'\}=\phi$ 则

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

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

情况2： $\{s,t\}\cap\{s',t'\}\neq\phi$.

若 $s=s'$，则 $(s,t)(s,t')=(s,t',t)$

若 $s=t'$，则 $(s,t)(s',s)=(s,s',t)$

由于每对 $\tau_{2j-1}\tau_j$ 都可以写成3-循环乘积，则 π 亦可以。□

例3. S_n中任何置换都可以写成对换

$(12),(13),(1,4),\cdots,(1,n-1),(1,n)$

的乘积

证明： 任何置换 π 皆可写成若干对换的乘积，又注意到

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

所以任何置换皆可表为 $(1,2),\cdots,(1,n)$ 的乘积

③