注：关于良定义

$$f: \mathbb{Q} \longrightarrow \mathbb{Z}$$
$$\frac{a}{b} \mapsto b$$

其中 $a, b \in \mathbb{Z}$, $b \neq 0$

$f(\frac{1}{2}) = 2$, $f(\frac{2}{4}) = 4$ f不是映射

定义：设 $a, b \in \mathbb{Z}$, $b \neq 0$

如果 $c \in \mathbb{Z}$ 满足 $c|a$ 和 $c|b$

则称 c 是 a, b 的公因子

设 d 是 a, b 的公因子，且

$\forall$ a, b 的公因子 c，都有 $c|d$

则称 d 是 a, b 的最大公因子

记为 gcd(a, b)

gcd — greatest common divisor.

例：gcd(12, 18) = 6 或 -6 ①

$$g: \mathbb{Q} \longrightarrow \mathbb{Z}$$
$$\frac{a}{b} \mapsto b$$

其中 $a, b \in \mathbb{Z}$, $b \neq 0$, $\gcd(a, b) = 1$

$f(\frac{1}{2}) = 2$, $f(\frac{-1}{2}) = -2$. f不是映射

$$h: \mathbb{Q} \longrightarrow \mathbb{Z}$$
$$\frac{a}{b} \mapsto b$$

其中 $a, b \in \mathbb{Z}$, $b \neq 0$, $\gcd(a, b) = 1$

h是映射.

§4.6 序关系

定义：设 $\leqslant$ 是集合 S 上的二元关系

如果 "$\leqslant$" 满足

(1) 自反律. $\forall a \in S$, $a \leqslant a$

(ii) 反对称　设 $a, b \in S$

如果 $a \leqslant b$ 和 $b \leqslant a$，则 $a = b$

(iii) 传递．设 $a, b, c \in S$

如果 $a \leqslant b$ 和 $b \leqslant c$，则 $a \leqslant c$．

例：在 $\mathbb{Z}$ 上 "$\leqslant$" 和 "$\geqslant$" 都是序关系

例：在 $\mathbb{Z}^+$ 上，整除 "$|$" 是序关系

验证：(i) 自反律．$\forall a \in \mathbb{Z}^+$，$a|a$

(ii) 设 $a, b \in \mathbb{Z}^+$，$a|b$ 和 $b|a$

则 $\exists x, y \in \mathbb{Z}^+$ 使得

$b = xa$，$a = yb \Rightarrow a = xya$

$\Rightarrow xy = 1 \Rightarrow x = y = 1$.

$\Rightarrow a = b$.

反对称律成立

(iii) 设 $a, b, c \in \mathbb{Z}^+$，$a|b$，$b|c$

则 $\exists x, y \in \mathbb{Z}^+$

$b = xa$，$c = yb$

$\Rightarrow c = (xy)a \Rightarrow a|c$.

传递律成立

定义：设 $\leqslant$ 是集合 S 上的序关系

如果 $\forall a, b \in S$.

$a \leqslant b$ 或 $b \leqslant a$

则称 $a = b$．则称为偏序

例："$\leqslant$" 是 $\mathbb{Z}$ 上全序，"$|$" 是 $\mathbb{Z}^+$ 上偏序

定义：设 $\leqslant$ 是 S 上的序关系，$a \in S$

(i) 如果不存在 $b \in S$ 使得

$a \leqslant b$ 且 $a \neq b$

则称 a 是 S 上关于 "$\leqslant$" 的极大元

(ii) 如果 $\forall b \in S$, $b \leq a$

则称 $a \in S$ 中关于"$\leq$"最大元

类似地可以定义极小元和最小元

例：设 $S = \{a, b, c\}$,

T = S 中所有子集的集合

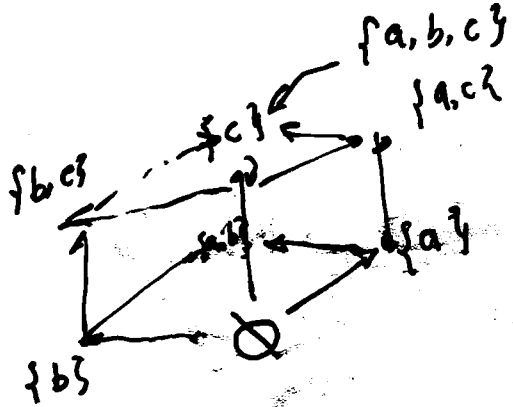
$T^\circ = T \setminus \{S\}$

则 "$\subset$" 是 T 和 T_0 上的序关系

S 是 T 中关于 "$\subset$" 最大元

$\{a,b\}, \{b,c\}, \{c,a\}$ 是 T_0 中关于 "$\subset$" 极大元。

把 "$\subset$" 记为 "$\longrightarrow$"



例：设 $a, b \in \mathbb{Z}^+$.

$S = \{c \in \mathbb{Z}^+ \mid c|a, c|b\}$

则 $gcd(a,b) \in \mathbb{Z}^+$ 是 S 上关于 "|" 的最大元

例 定义：设 $a, b \in \mathbb{Z} \setminus \{0\}$

$m \in \mathbb{Z}$. 如果 $a|m$ 和 $b|m$,

则称 m 是 a, b 的公倍式

设 l 是 a, b 的公倍式. 如果

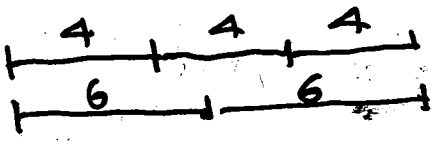
$\forall$ a, b 的公倍式 m, $l|m$. 则

称 l 是 a、b 的最小公倍式

记为 lcm(a, b)

lcm — least common multiple

例如 lcm(4, 6) = 12



例：设 $a, b \in \mathbb{Z}^+$.

$T = \{ m \in \mathbb{Z}^+ \mid m$ 是 a, b 的公倍式$\}$

则 lcm(a,b) 是 T 中关于"|"的最小元.

§5 置换

记号：设 S 是集合，则 S 的势记为 card(S) 或 |S|

设 X 是集合且 $|X| = n$.

不妨设 $X = \{1, 2, \cdots, n\}$

$S_n = \{ \sigma : X \to X \mid \sigma$ 是双射$\}$

σ 可以表示为 $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$

其中 $i_1, i_2, \cdots, i_n \in X$, 两两不同.

$\sigma(1) = i_1, \sigma(2) = i_2, \cdots, \sigma(n) = i_n$.

$|S_n| = n!$

注：如果 $\sigma, \tau \in S_n$, 则 $\sigma \circ \tau \in S_n$ [命题3.2]

为了符号简洁

$\sigma \circ \tau$ 记为 $\sigma\tau$.

由定理3.2 设 $\sigma, \tau, \delta \in S_n$

$(\sigma\tau)\delta = \sigma(\tau\delta)$ 结合律成立

记恒同映射 $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ 为 e

由补充3. page 3 的例子

$\forall \sigma \in S_n$, $\sigma e = e\sigma = \sigma$.

由定理3.1. 设 $\sigma \in S_n$. 则 $\sigma^{-1} \in S_n$

于是: $\forall \sigma, \tau, \delta \in S_n$

① 封闭性: $\sigma\tau \in S_n$

② 结合律 $(\sigma\tau)\delta = \sigma(\tau\delta)$

③ "乘法"单位. 记 $\sigma e = e\sigma = \sigma$

④ 可逆元: $\sigma^{-1} \in S_n$

S_n 中的元素称为置换.

例。在 S_4 中. 设

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

计算 $\sigma\tau$ 和 $\tau\sigma$

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

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

于是 $\sigma\tau \neq \tau\sigma$.

记号 设 $\sigma \in S_n$, $\sigma^0 = e$

设 $k \in \mathbb{Z}^+$

$$\sigma^k = \underbrace{\sigma \cdots \sigma}_{k}$$

$$\sigma^{-k} = \underbrace{\sigma^{-1} \cdots \sigma^{-1}}_{k}$$

自己验证: $\forall i, j \in \mathbb{Z}$ $\sigma^{i+j} = \sigma^i\sigma^j$

$(\sigma^i)^j = \sigma^{ij}$

注：设 $\sigma, \tau \in S_n$.

$$(\sigma\tau)^2 = (\sigma\tau)(\sigma\tau) = \sigma(\tau\sigma)\tau$$

一般 $\neq \sigma^2\tau^2$

$$(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$$ （穿衣脱衣）

§5.2 置换的阶.

引理5.1. 设 $\sigma \in S_n$. 则 $\exists m \in \mathbb{Z}^+$, 使得

$$\sigma^m = e$$

证：考虑序列

$$\sigma, \sigma^2, \sigma^3, \cdots \in S_n$$

则 $\exists i, j \in \mathbb{Z}^+$, $i < j$ 使得

$$\sigma^i = \sigma^j$$

$\Rightarrow \sigma^{j-i} = e$. 令 $m = j - i$ 即可.

定义：设 $\sigma \in S_n$, 极小的正整数 k 使得 $\sigma^k = e$. 称为 σ 的阶 order. 记为 $\mathrm{ord}(\sigma)$

注：设 $\sigma \in S_n$. 则 $\mathrm{ord}(\sigma) = 1 \Leftrightarrow \sigma = e$.

例：设 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$. 求 $\mathrm{ord}(\sigma)$

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

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

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

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

$\Rightarrow \mathrm{ord}(\sigma) = 3$

引理 5.2 设 $\sigma \in S_n$, $\mathrm{ord}(\sigma)=k$, $m\in\mathbb{Z}$

则 $\sigma^m = e \iff k \mid m$

证: "$\Leftarrow$" 设 $m=qk$, $q\in\mathbb{Z}$

$$\sigma^m = \sigma^{qk} = (\sigma^k)^q = e^q = e$$

[注: $e^{-1}=e$]

"$\Rightarrow$" 由带余除法

$m = qk + r$, $q\in\mathbb{Z}$, $r\in\{0,1,\cdots,k-1\}$

$$e = \sigma^m = \sigma^{qk+r} = \sigma^{qk}\sigma^r = \sigma^r$$

$\because \mathrm{ord}(\sigma)=k \therefore r=0 \Rightarrow k\mid m$ ☒

定义: 设 $i_1,\cdots,i_k \in X$ 两两不同

$\pi \in S_n$. 如果

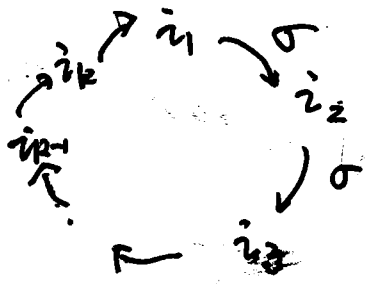
$\pi(i_1)=i_2$, $\pi(i_2)=i_3$, $\cdots$ $\pi(i_{k-1})=\pi(i_k)$

$\pi(i_k)=i_1$

且 $\forall j \in X\setminus\{i_1,\cdots i_k\}$ ⑦

有 $\pi(j)=j$

则称 π 是一个作用于 X 的 cycle



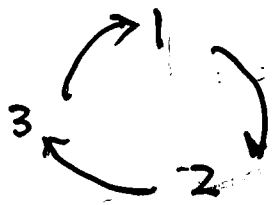
称 k 是 π 的长度

记 $\pi = (i_1 i_2 \cdots i_k)$

注: $\pi = (i_1 i_2 \cdots i_k) = (i_2 i_3 \cdots i_k i_1) = \cdots = (i_k i_1 i_2 \cdots i_{k-1})$

例: 求 (123) 的阶

$\mathrm{ord}(123) = 3$



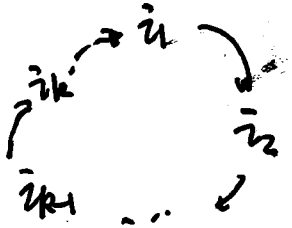
注: $\pi = (i_1, i_2, \cdots i_k)$

则 $\pi: \{i_1 \cdots i_k\} \to \{i_1, \cdots i_k\}$ 是双射

$\forall m\in\mathbb{Z}$ π^m 也是 且 $\forall j \in X\setminus\{i_1\cdots i_k\}$, $\pi^m(j)=j$

引理5.3 设 $\sigma=(i_1,\cdots,i_k)$. 则

$$k=\mathrm{ord}(\sigma).$$



证: $\forall\, m\in\{1,2,\cdots,k-1\}$

$$\sigma^m(i_1)=i_{1+m}\neq i_1$$

$$\Rightarrow \sigma^m\neq e.$$

$$\sigma^k(i_1)=\sigma(\sigma^{k-1}(i_1))=\sigma(i_k)=i_1$$

$\sigma=(i_2\cdots i_k i_1)\Rightarrow \sigma^k(i_2)=i_2$

类似地可知 $\sigma^k(i_j)=i_j$, $\forall j\in\{1,\cdots k\}$

定义: 设 $\sigma=(i_1,\cdots,i_k)$, $\tau=(j_1,\cdots,j_l)$

是 S_n 中两个轮换. 如果

$$\{i_1,\cdots,i_k\}\cap\{j_1,\cdots,j_l\}=\Phi$$

则称 σ,τ 互不相交

例: 设 $\sigma=(123)$, $\tau=(45)\in S_7$ ⑤

计算 $\sigma\tau$ 和 $\tau\sigma$

$$\sigma\tau=(123)(45)=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&5&4&6&7\end{pmatrix}$$

$$\tau\sigma=(45)(123)=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&5&4&6&7\end{pmatrix}.$$

引理5.4 设 $\sigma,\tau\in S_n$ 是两个互不

相交的循环. 则 $\sigma\tau=\tau\sigma$.

证: 设 $\sigma=(i_1,\cdots,i_k)$, $\tau=(j_1,\cdots,j_l)$

$I=\{i_1,\cdots,i_k\}$, $J=\{j_1,\cdots,j_l\}$

$M=X\setminus(I\cup J)$

$\forall\, m\in M$ $\quad\sigma\tau(m)=\sigma(m)=m$

同理 $\tau\sigma(m)=m$.

$\forall\, i\in I$. $\quad\sigma\tau(i)=\sigma(i)$

$\tau\sigma(i)=\tau(\sigma(i))=\sigma(i)$

$(\because \sigma(i)\in I)$

同理 $\Rightarrow \sigma\tau(i)=\tau\sigma(i)$.

则 $\forall j \in J$, $\sigma\tau(j) = \tau\sigma(j)$.

$\Rightarrow \sigma\tau = \tau\sigma$ ☒

例：设 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 4 & 5 & 7 & 6 & 1 & 8 \end{pmatrix}$

把 σ 写成若干互不相交的循环之积

解 $\sigma = (198)(23)(67)$

定理5.1 设 $\sigma \in S_n$ 则 σ 可以写成若干个互不相交的循环之积

证：设 $I_\sigma = \{i \in X \mid \sigma(i) \neq i\}$.

我们对 $|I_\sigma|$ 归纳

注意到 $|I_\sigma| \neq 1$. 这是因为 σ 是双射

若 $I_\sigma = \{i_1, i_2\}$. 则 $\sigma(i_1) = i_2$ 且

$\sigma(i_2) = i_1$. 且 $\forall j \in X \setminus I_\sigma$

$\sigma(j) = j$.

于是 $\sigma = (i_1, i_2)$.

设 $|I_\sigma| = k > 2$ 且 $|I_\sigma| < k$ 时结论成立

设 $i_1 \in I_\sigma$. $\because \sigma^{ord(\sigma)}(i_1) = i_1$

$\because \exists\, k \in \mathbb{Z}^+$ 使得

$\sigma^k(i_1) = i_1$ 且 $\forall\, m \in \{1, 2, \cdots k-1\}$, $\sigma^m(i_1) \neq i_1$

于是 $i_2 := \sigma(i_1)$, 则 $\sigma(i_2) = \sigma^2(i_1)$

$\cdots i_k = \sigma(i_{k-1}) = \sigma^{k-1}(i_1)$

则 $\pi = (i_1, i_2, \cdots i_k)$ 是一个循环

令 $J = X \setminus \{i_1, i_2, \cdots, i_k\}$

τ: $X \to X$

$i \mapsto i_1$, $i \in \{i_1, i_2, \cdots i_k\}$

$j \mapsto \sigma(j)$ $j \in J$.

下面验证：

$$\sigma = \pi \cdot \tau \qquad (*)$$

$\forall i \in \{i_1, \cdots i_k\}$, $\pi\tau(i) = \pi(i) = \sigma(i)$

$\forall j \in J$ $\quad \pi \cdot \tau(j) = \tau(j) = \sigma(j)$

于是 $(*)$ 成立.

且 $|I_\tau| < k$

于是 τ 是若干互不相交的循环不动

且每个循环只与 J 中元素有关

于是 σ 是若干互不相交循环之积. 因

定理5.2 设 $\sigma \in S_n$ 且

$$\sigma = \pi_1 \cdots \pi_s$$

其中 $\pi_1, \cdots, \pi_s$ 是两两互不相交

的循环. 则 $\mathrm{ord}(\sigma) = \mathrm{lcm}(\mathrm{ord}(\pi_1), \cdots, \mathrm{ord}(\pi_s))$

证: 设 $k_i = \mathrm{ord}(\pi_i)$ $i = 1, \cdots s$

$k = \mathrm{ord}(\pi)$, $l = \mathrm{lcm}(k_1, \cdots, k_s)$.

则 $\exists q_i \in \mathbb{Z}^+$, $l = q_i k_i$, $i = 1, \cdots s$.

$$\begin{aligned}\sigma^l &= (\pi_1 \cdots \pi_s)^l \\ &= \pi_1^l \cdots \pi_s^l \qquad (\text{引理5.4}) \\ &= \pi_1^{k_1 q_1} \cdots \pi_s^{k_s q_s} \qquad (\text{引理5.2}) \\ &= e.\end{aligned}$$

假设 $k < l$. 则 $\exists i \in \{1, \cdots s\}$

$k_i \nmid l$

不妨设 $i = 1$. 由带余除法

$k = q m_1 k_1 + r_1$, $m_1 \in \mathbb{Z}^+$, $r_1 \in \{1, 2, \cdots k_1\}$

$$\sigma^k = \pi_1^k \pi_2^k \cdots \pi_s^k = \pi_1^{r_1} \pi_2^k \cdots \pi_s^k$$

$\because \pi_1^{r_1} \neq e \quad \therefore \exists j \in I_{\pi_1}$

使得 $\pi_1^{r_1}(j) \neq j$

$j = \sigma^k(j) = \pi_1^{r_1}(j) \neq j \quad \rightarrow\leftarrow$. 因

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

求 $\mathrm{ord}(\sigma)$

解: $\sigma = \underbrace{(134689)}_{\pi_1}\underbrace{(25107)}_{\pi_2}$

$\mathrm{ord}(\sigma) = \mathrm{lcm}(\mathrm{ord}(\pi_1), \mathrm{ord}(\pi_2))$

$= \mathrm{lcm}(6,4) = 12.$

§5.3 置换的符号

定义: 长度为2的循环 (i_1, i_2) 称为对换.

注: $(i_1,i_2)(i_1,i_2) = e$

例: 设 $k>1$, 证明

$\underbrace{(i_1, i_2, \cdots, i_k)}_{\sigma} = \underbrace{(i_1,i_k)\cdots(i_1,i_3)(i_1,i_2)}_{\tau}$

证: 设 $s \in \{1,2,\cdots k-1\}$

$\sigma(i_s) = i_{s+1}$, $\tau(i_s) = i_{s+1}$

$\sigma(i_k) = i_1$, $\tau(i_k) = i_1$

$\forall j \in X \setminus \{i_1, i_2, \cdots, i_k\}$

$\sigma(j) = j$, $\tau(j) = j$

于是 $\sigma = \tau$ ▨

注: 由定理5.1和上例可知 $\forall \sigma \in S_n \setminus \{e\}$, σ 是若干对换之积.

例: 把 $\sigma = \begin{pmatrix} 1&2&3&4&5&6 \\ 2&4&3&1&6&5 \end{pmatrix}$ 把 σ 写成若干对换之积.

证: $\sigma = (124)(56)$

$= (41)(21)(56)$

$\sigma = (41)(54)(21)(54)(56)$

引理5.5 设 $\alpha, \beta \in S_n$ 是两个对换且 $\alpha \neq \beta$. 令 $\alpha = (st)$ 则存在两个对换 α', β'

满足：$\alpha'(s) \neq s$，$\beta'(s) = s$，$\beta\alpha = \alpha'\beta'$.

证：设 $\beta = (uv)$

情形1 $\{s,t\} \cap \{u,v\} = \varnothing$

~~$\alpha\beta = \beta\alpha$~~ $\beta\alpha = \alpha\beta$ (引理5.4)

令 $\alpha' = \alpha$，$\beta' = \beta$ 即可

情形2 $u = s$. 则 $v \neq t$. $v \neq s$

$\beta\alpha = (sv)(st) = (st)(vt)$

$s \to t$，$t \to v$，$v \to s$

令 $\alpha' = \alpha$，$\beta' = (vt)$

情形3 $u = t$，则 $v \neq s$，$v \neq t$

$\beta\alpha = (vt)(st) = (sv)(vt)$

$s \to v$，$t \to s$，$v \to t$ ☒

引理5.6 设 $\tau_1, \cdots \tau_k$ 是对换

且 $e = \tau_1 \cdots \tau_k$

则 k 是偶数

证：$k \neq 1$. 若 $k = 2$. 则结论成立

设 $k > 2$. 我们证明，e 可写成 $k-2$ 个对换之积.

设 $\tau_k = (st)$. 由引理5.5

$\exists\ \tau'_{k-1}, \tau'_k$ 对换 使得

$\tau'_k(s) = s$，$\tau'_{k-1}(s) \neq s$，$\tau_{k-1}\tau_k = \tau'_{k-1}\tau'_k$

$e = \tau_1 \cdots \tau_{k-2}\tau'_{k-1}\tau'_k$

如果 $\tau_{k-2}\tau'_{k-1} = e$. 则 e 是 $k-2$ 个对换之积

否则 $\tau_{k-2} \neq \tau'_{k-1}$. 又于 τ_{k-2}, τ'_{k-1} 用引理5.5

$\exists\ \tau'_{k-2}, \tau''_{k-1}$ 对换 使得

$\tau''_{k-1}(s) = s$，$\tau'_{k-2}(s) \neq s$. $\tau_{k-2}\tau'_{k-1} = \tau'_{k-2}\tau''_{k-1}$

$e = \tau_1 \cdots (\tau_{k-3}\tau'_{k-2})\tau''_{k-1}\tau'_k$

由此从右到左推理，

或者得到 e 可写成 $k-2$ 对换之积

或者 $e=\delta_1\delta_2\cdots\delta_k$

其中 $\delta_1,\delta_2,\cdots\delta_k$ 是对换且

$\delta_2(s)=\cdots=\delta_k(s)=s$，$\delta_1(s)\neq s$

但 $\delta_1\neq\delta_2$

$s=e(s)=\delta_1(s)\neq s$ $\rightarrow\leftarrow$

于是 $e=\delta_1\cdots\delta_{k-2}$，$\delta_1,\cdots\delta_{k-2}$ 是对换

$\Rightarrow$ k 是偶数 ☒

定理5.3 设 $\sigma\in S_n\setminus\{e\}$，

$\sigma=\lambda_1\cdots\lambda_k=\mu_1\cdots\mu_m$

其中，$\lambda_1,\cdots,\lambda_k,\mu_1,\cdots,\mu_m$ 是对换

则 k 和 m 有相同的奇偶性

证：$\because \lambda_1\cdots\lambda_k=\mu_1\cdots\mu_m$ ⑬

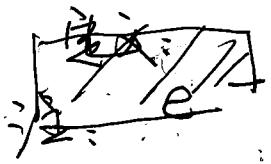
$\therefore e=(\lambda_1\cdots\lambda_k)^{-1}\mu_1\cdots\mu_m$

$\therefore e=\lambda_k\cdots\lambda_1\mu_1\cdots\mu_m$

$=\lambda_k\cdots\lambda_1\mu_1\cdots\mu_m$ (引理5.6)

$\Rightarrow$ $k+m$ 是偶数 (引理5.6)

$\Rightarrow$ k,m 有共同的奇偶性 ☒



定义：设 $\sigma\in S_n$，σ 的符号定义为

1，如果 σ 是偶数个对换之积

否则，符号定义为 -1，σ 的符号记

为 ε_σ

推论5.1 设 $\sigma\in S_n$ 且

$\sigma=\pi_1\cdots\pi_s$

其中 $\pi_1,\cdots,\pi_s$ 是互不相交的循环

则 $\varepsilon_\sigma=(-1)^{\sum_{i=1}^{s}[\mathrm{ord}(\pi_i)-1]}$

证: π_i 是 $\mathrm{ord}(\pi_i)-1$ 个对换之积

$\Rightarrow \sigma$ 是 $\sum_{i=1}^{s}[\mathrm{ord}(\pi_i)-1]$ 个对换之积. 证毕

例: 求 $\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11\\11&5&4&2&3&10&7&6&8&1&9\end{pmatrix}$

奇偶性符号.

解: $\sigma=(1,11,9,8,6,10)(2,5,3,4)$

6 4

$\mathrm{ord}(\sigma)=12$. $\varepsilon_\pi=(-1)^{5+3}=1$

注: $e=(12)(12)$ 是 $\pi_e=1$

注: 当 $\varepsilon_\sigma=1$ 时 σ 称为偶置换

$\varepsilon_\sigma=-1$ 时 ... 奇置换.

~~§6 整数的最大公因子~~

§6 辗转相除 (14)

设 $a,b\in\mathbb{Z}$, $b\neq 0$ 求 a,b 的

最大公因子. $\gcd(a,b)$

设 $r_0=a$, $r_1=b$

由带余除法:

$r_0=q_1r_1+r_2$. $q_2=\mathrm{quo}(r_0,r_1)$, $r_2=\mathrm{rem}(r_0,r_1)$

如果 $r_2=0$, 则 $r_1\mid r_0$. $\Rightarrow r_1=\gcd(r_0,r_1)$

否则 $r_0=q_3r_2+r_3$ $q_3=\mathrm{quo}(r_0,r_2)$, $r_3=\mathrm{rem}(r_1,r_2)$

设 $r_3\neq 0$

$r_2=q_4r_3+r_4$ $q_4=\mathrm{quo}(r_2,r_3)$, $r_4=\mathrm{rem}(r_2,r_3)$

$\vdots$

我们有 $r_2>r_3>\cdots$

正整数序列

有限步后必然终止

于是 $\exists\ k \in \mathbb{Z}^+$

$$r_{k-2} = q_k r_{k-1} + r_k \qquad q_k = quo(r_{k-2}, r_{k-1}),\ r_k = rem(r_{k-2}, r_{k-1}) \neq 0$$

但是 $r_{k-1} = q_{k+1} r_k$, $q_{k+1} \in \mathbb{Z}^+$

断言: $gcd(r_{i-2}, r_{i-1}) = gcd(r_{i-1}, r_i)$

$i = 2, 3, \cdots, k$

断言的证明

设 $x = gcd(r_{i-2}, r_{i-1}), > 0$

$y = gcd(r_{i-1}, r_i) > 0$

由 $r_{i-2} = q_i r_{i-1} + r_i$

~~$r_{i-1} = q_{i+1} r_i + r_{i+1}$~~

$x \mid r_{i-1}$, $x \mid r_{i-1} \Rightarrow x \mid r_i$

(引理 4.2)

$y \mid r_{i-1}$, $y \mid r_i$

于是 x 是 r_{i-1} 和 r_i 的公因子.

$\Rightarrow x \mid y$ (最大公因子的定义)

类似地. $y \mid r_{i-1}$, $y \mid r_i \Rightarrow y \mid r_{i-2}$

$\Rightarrow y$ 是 r_{i-2}, r_{i-1} 的最大公因子

$\Rightarrow y \mid x$.

由 $x \mid y$. $y \mid x$, $x > 0$, $y > 0$ 可知 $x = y$.

于是 $gcd(a, b) = gcd(r_0, r_1) =$

$= gcd(r_1, r_2) = \cdots = gcd(r_{k-1}, r_k) = r_k$.

定理 6.1 设 $a, b \in \mathbb{Z}$, $b \neq 0$

则 (i) $gcd(a, b)$ 存在

(ii) $\exists\ u, v \in \mathbb{Z}$, 使得

$$ua + vb = gcd(a, b)$$

(Bezout's relation)

证：(i) 由辗转相除法（Euclid's 算法）可知.

(ii) 设 $g=\gcd(a,b)$.

由辗转相除法可知. $g=r_k$

于是 $g=r_{k-2}+(-q_k)r_{k-1}$

$\because\quad r_{k-3}=q_{k-1}r_{k-2}+r_{k-1}$

$\therefore\quad g=r_{k-2}+(-q_k)[r_{k-3}-q_{k-1}r_{k-2}]$

$$=\underbrace{(-q_k)}_{u_{k-2}}r_{k-3}+\underbrace{(1+q_kq_{k-1})}_{v_{k-2}}r_{k-2}$$

即 $g=u_{k-2}r_{k-3}+v_{k-2}r_{k-2}$

由 $r_{k-4}=q_{k-2}r_{k-3}+r_{k-2}$

可知 $g=u_{k-2}r_{k-3}+v_{k-2}(r_{k-4}-q_{k-2}r_{k-3})$

$$=\underbrace{(u_{k-2}-q_{k-2}v_{k-2})}_{v_{k-3}}r_{k-3}+\underbrace{v_{k-2}}_{u_{k-3}}r_{k-4}$$

反向观察辗转相除法.

由归纳可知. 当 $u_k, v_k\in\mathbb{Z}$

使得 $u_kr_0+v_1r_1=g$

令 $u=u_1,\quad v=v_1.$

$$ua+vb=g.$$

例：计算 95 和 57 的最大公因子.

解 $r_0=95,\quad r_1=57$

$$95=1\cdot57+38$$
$$57=1\cdot38+19$$
$$38=2\cdot19$$
$$\Rightarrow \gcd(95,57)=19.$$

再求 $u,v\in\mathbb{Z}$ 使得

$$u\cdot95+v\cdot57=19.$$

$57 - 1 \cdot 38 = 19$

$57 - (95 - 57) = 19$

$\Rightarrow 1)\ 95 + 2 \cdot 57 = 19$

$u = -1, \quad v = 2$