第三次作业.

1. $f: X \to Y$ 映射. $T_1, T_2 \subseteq Y$ 为两个子集.

(1) $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$

(2) $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$

元素 $\in$ 集合. 集合 $\subseteq$ 集合.

证. (1). "$\supseteq$" $\because T_1 \subseteq T_1 \cup T_2$ $\therefore f^{-1}(T_1) \subseteq f^{-1}(T_1 \cup T_2)$. 同理 $f^{-1}(T_2) \subseteq f^{-1}(T_1 \cup T_2)$

$\therefore f^{-1}(T_1) \cup f^{-1}(T_2) \subseteq f^{-1}(T_1 \cup T_2)$

$f^{-1}(x)$ 是集合

"$\subseteq$" $\forall x \in f^{-1}(T_1 \cup T_2)$ 则 $\exists y \in T_1 \cup T_2$ s.t. $f(x) = y$

$\because y \in T_1 \cup T_2$ 则 $y \in T_1$ 或 $y \in T_2$

如果 $y \in T_1$ 则 $f(x) \in T_1$ $\therefore x \in f^{-1}(T_1)$

如果 $y \in T_2$ 同理 $x \in f^{-1}(T_2)$ $\therefore x \in f^{-1}(T_1)$ 或 $x \in f^{-1}(T_2)$

$\therefore f^{-1}(T_1 \cup T_2) \subseteq f^{-1}(T_1) \cup f^{-1}(T_2)$

综上 $f^{-1}(T_1) \cup f^{-1}(T_2) = f^{-1}(T_1 \cup T_2)$

(2) "$\supseteq$" $\because T_1 \cap T_2 \subseteq T_1$ $\therefore f^{-1}(T_1 \cap T_2) \subseteq f^{-1}(T_1)$ 同理 $f^{-1}(T_1 \cap T_2) \subseteq f^{-1}(T_2)$

$\therefore f^{-1}(T_1 \cap T_2) \subseteq f^{-1}(T_1) \cap f^{-1}(T_2)$

"$\supseteq$" $\forall x_0 \in f^{-1}(T_1) \cap f^{-1}(T_2)$ 即 $x_0 \in f^{-1}(T_1)$ 且 $x_0 \in f^{-1}(T_2)$

$\because x \in f^{-1}(T_1)$ 则 $\exists y_1 \in T_1$ s.t. $f(x) = y_1$, 同理 $\exists y_2 \in T_2$ s.t. $f(x) = y_2$.

$\because f$ 为映射 $\therefore f(x) = y_1 = y_2$ $\therefore f(x) \in T_1 \cap T_2$ $\therefore x \in f^{-1}(T_1 \cap T_2)$

$\therefore f^{-1}(T_1) \cap f^{-1}(T_2) \subseteq f^{-1}(T_1 \cap T_2)$

综上 $f^{-1}(T_1) \cap f^{-1}(T_2) = f^{-1}(T_1 \cap T_2)$ □.

2. 映射 $f: X \to Y$, $g: Y \to Z$, $h = g \circ f$ 为复合映射.

(1) h 单 $\Rightarrow$ f 单　　(2) h 满 $\Rightarrow$ g 满.

证. (1). $\forall x_1, x_2 \in X$ 如果 $f(x_1) = f(x_2)$ 则 $h(x_1) = g\circ f(x_1) = g(f(x_1)) = g(f(x_2)) = g\circ f(x_2) = h(x_2)$ 由于 h 单 $\therefore x_1 = x_2$ $\therefore f$ 单.

(2). $\forall z \in Z$ $\because h$ 满 $\therefore \exists x \in X$ s.t. $z = h(x) = g\circ f(x) = g(f(x))$

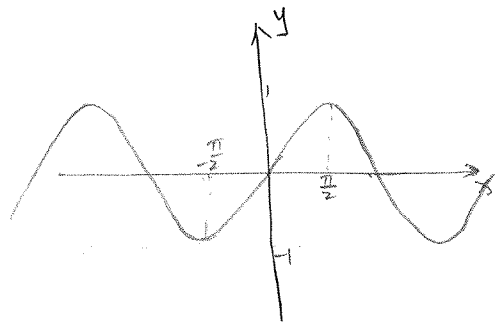
令 $y = f(x)$ 则 $y \in Y$ 且 $g(y) = z$ 即 $\exists y \in Y$ s.t. $g(y) = z$ $\therefore g$ 满.

3. $f(x) = \sin x$, 定义域为 $\mathbb{R}$.

(1) $\forall y \in [-1, 1]$ 求 $f^{-1}(\{y\})$

(2) 求由 f 诱导一等价关系一商集.

(3). 刻画映射分解式.



解 (1). $\forall y \in [-1, 1]$ $\exists!\, x_0 \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ s.t. $y = f(x_0)$

且 $f(x_0) = \sin x_0 = \sin(2k\pi + x_0) = \sin((2k+1)\pi - x_0) = y$ 对 $\forall k \in \mathbb{Z}$ 成立

$\therefore f^{-1}(\{y\}) = \{2k\pi + x_0, (2k+1)\pi - x_0 \mid k \in \mathbb{Z}\} = \{k\pi + (-1)^k x_0 \mid k \in \mathbb{Z}\}$

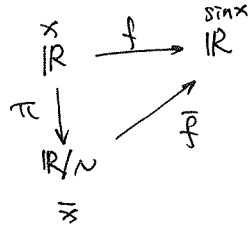
(2) 由 f 诱导的等价关系 $\sim_f$ 满足 $x \sim_f x' \iff f(x) = f(x')$.

由(1)可知 $x \sim_f x' \iff x' = k\pi + (-1)^k x$ $(k \in \mathbb{Z})$

则 $\forall x \in \mathbb{R}$ $\overline{x} = \{x' \in \mathbb{R} \mid x' = k\pi + (-1)^k x,\ k \in \mathbb{Z}\}$ 不妨取代表元 $x \in [-\frac{\pi}{2}, \frac{\pi}{2}]$

$\therefore$ 商集为 $\mathbb{R}/\sim_f = \{\overline{x} \mid -\frac{\pi}{2} \le x \le \frac{\pi}{2}\}$

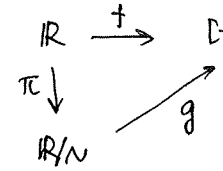
(3).



其中 $\bar{f}: \mathbb{R}/\sim \to \mathbb{R}$, $\bar{x} \mapsto \sin x$ 且 $\bar{f}\circ\pi = f$

且 如果 $\bar{f}(\overline{x_1}) = \bar{f}(\overline{x_2})$ 即 $\sin x_1 = \sin x_2$ 即 $x_1 \sim_f x_2$

$\therefore \overline{x_1} = \overline{x_2}$ $\therefore \bar{f}$ 为单射.



选 $\mathbb{R} \xrightarrow{f} [-1,1]$ 易知 f 为满射 则 g 为双射. ($g: \mathbb{R}/\sim \to [-1,1]$, $\bar{x} \mapsto \sin x$)

易证 g 为单射 且 $\because g\circ\pi = f$ 由 f 满和 2(2) 可知 g 满

$\therefore g$ 为双射,

4. (P30. 2) $\forall (x,y), (x',y') \in \mathbb{R}^2$ 二元关系满足 $P(x,y) \sim P(x',y') \Leftrightarrow x'-x \in \mathbb{Z},\ y'-y \in \mathbb{Z}$.

证明 $\sim$ 是等价关系，且商集是环面.

证. (1). ① 反身性：$\forall (x,y) \in \mathbb{R}^2$ $\because x-x=0 \in \mathbb{Z},\ y-y=0 \in \mathbb{Z}$ $\therefore P(x,y) \sim P(x,y)$

② 对称性：如果 $P(x,y) \sim P(x',y')$ 则 $x-x' \in \mathbb{Z} \Rightarrow x'-x \in \mathbb{Z}$. 同理 $y'-y \in \mathbb{Z}$.

$\therefore P(x',y') \sim P(x,y)$ 即 $P(x,y) \sim P(x',y') \Rightarrow P(x',y') \sim P(x,y)$

③ 传递性：如果 $P(x,y) \sim P(x',y')$, $P(x',y') \sim P(x'',y'')$ 则 $x-x' \in \mathbb{Z},\ x'-x'' \in \mathbb{Z}$

不妨设 $x-x'=m$, $x'-x''=n$ 则 $x-x''=m+n \in \mathbb{Z}$ 同理 $y-y'' \in \mathbb{Z}$

$\therefore P(x,y) \sim P(x'',y'')$. 即 $P(x,y) \sim P(x',y')$, $P(x',y') \sim P(x'',y'') \Rightarrow P(x,y) \sim P(x'',y'')$.

(2). $\forall (x,y) \in \mathbb{R}^2$ $\overline{(x,y)} := \{(x',y') \in \mathbb{R}^2 \mid x-x' \in \mathbb{Z},\ y-y' \in \mathbb{Z}\}$

(不妨取代表元 $(x,y) \in [0,1) \times [0,1)$) 则商集 $\mathbb{R}^2/\sim = \{\overline{(x,y)} \mid (x,y) \in \mathbb{R}^2\}$.

实际上可构造 $\mathbb{R}^2/\sim \xrightarrow{f} [0,1) \times [0,1)$ 一双射

$\overline{(x,y)} \longmapsto (x-\lfloor x \rfloor,\ y-\lfloor y \rfloor)$ (注 $\lfloor x \rfloor := n$ 满足 $n \le x < n+1$ 且 $n \in \mathbb{Z}$)

f良定义：首先 $0 \le x-\lfloor x \rfloor < 1$, $0 \le y-\lfloor y \rfloor < 1$ $\therefore (x-\lfloor x \rfloor,\ y-\lfloor y \rfloor) \in [0,1) \times [0,1)$

若 $\overline{(x,y)} = \overline{(x',y')}$ 即 $P(x,y) \sim P(x',y')$ 则 $x-x' \in \mathbb{Z},\ y-y' \in \mathbb{Z}$.

$\therefore f(\overline{(x,y)}) - f(\overline{(x',y')}) = (x-\lfloor x \rfloor,\ y-\lfloor y \rfloor) - (x'-\lfloor x' \rfloor,\ y'-\lfloor y' \rfloor)$

$= (x-x'-\lfloor x \rfloor+\lfloor x' \rfloor,\ y-y'-\lfloor y \rfloor+\lfloor y' \rfloor)$

$\because 0 \le x-\lfloor x \rfloor < 1$, $0 \le x'-\lfloor x' \rfloor < 1$ $\therefore 0 \le |(x-\lfloor x \rfloor) - (x-\lfloor x' \rfloor)| < 1$

又 $\because x-x' \in \mathbb{Z}$, $\lfloor x \rfloor, \lfloor x' \rfloor \in \mathbb{Z}$ $\therefore x-x'-\lfloor x \rfloor+\lfloor x' \rfloor \in \mathbb{Z}$

$\therefore x-\lfloor x \rfloor+\lfloor x' \rfloor-x'=0$ 同理 $\because y-y'+\lfloor y' \rfloor-\lfloor y \rfloor=0$

$\therefore f(\overline{(x,y)}) = f(\overline{(x',y')})$ 即 f良定义.

f是双射：若 $\exists\ \overline{(x,y)}, \overline{(x',y')} \in \mathbb{R}^2/\sim$ s.t. $f(\overline{(x,y)}) = f(\overline{(x',y')})$

则 $x-\lfloor x \rfloor = x'-\lfloor x' \rfloor$ $y-\lfloor y \rfloor = y'-\lfloor y' \rfloor$

$\therefore x-x' \in \mathbb{Z}$. $y-y' \in \mathbb{Z}$ $\therefore \overline{(x,y)} = \overline{(x',y')}$ 即 f单.

显然 对 $\forall\ (x,y) \in [0,1) \times [0,1)$ $f(\overline{(x,y)}) = (x,y)$ 即 f满.

综上 f为双射 即 $[0,1) \times [0,1)$ 可以几何地表示为环面上一个点集.

(验证 $[0,1) \times [0,1) \longrightarrow [0,1] \times [0,1]/\sim$ 为双射 即 $[0,1] \times [0,1]/\sim$ 为环面)

5 (P30, 3) 证明 2元、3元、4元集 分别有 2、5、15个不同商集.

证. 设 2元集 $A=\{a,b\}$ 来定义等价关系 $\sim_1 := \{(a,a),(b,b)\}$

则商集 $A/\sim_1 = \{\{a\},\{b\}\}$. 或定义等价关系 $\sim_2 := \{(a,a),(b,b),(a,b),(b,a)\}$

则商集 $A/\sim_2 = \{\{a,b\}\}$ 易可验证 其余二元关系均不是等价关系.

∴ 有2个不同商集.

实际上. 集合^{A}有多少不同商集 相当于 A 有多少种 划分. 下面从划分角度证明.

设 3元集 $A=\{a,b,c\}$

$P_1 = \{\{a,b,c\}\}$ $P_2 = \{\{a,b\},\{c\}\}$. $P_3 = \{\{a,c\},\{b\}\}$.

~~$P_4 = \{\{a\},\{b\},\{c\}\}$~~ 易得$P_4 = \{\{b,c\},\{a\}\}$ 且$P_4 = \{\{a\},\{b\},\{c\}\}$

∴ 有5个不同商集.

设 4元集 $A=\{a,b,c,d\}$ 划分可能性如下.

$P_1 = \{\{a,b,c,d\}\}$ $P_2 = \{\{a,b,c\},\{d\}\}$. $P_3 = \{\{a,c,d\},\{b\}\}$.

$P_4 = \{\{a,b,d\},\{c\}\}$. $P_5 = \{\{a,b\},\{c,d\}\}$ $P_6 = \{\{a,c\},\{b,d\}\}$

$P_7 = \{\{a,d\},\{b,c\}\}$. $P_8 = \{\{a,b\},\{c\},\{d\}\}$. $P_9 = \{\{a,c\},\{b\},\{d\}\}$.

$P_{10} = \{\{a,d\},\{b\},\{c\}\}$. $P_{11} = \{\{a\},\{b,c,d\}\}$ $P_{12} = \{\{a\},\{b,c\},\{d\}\}$

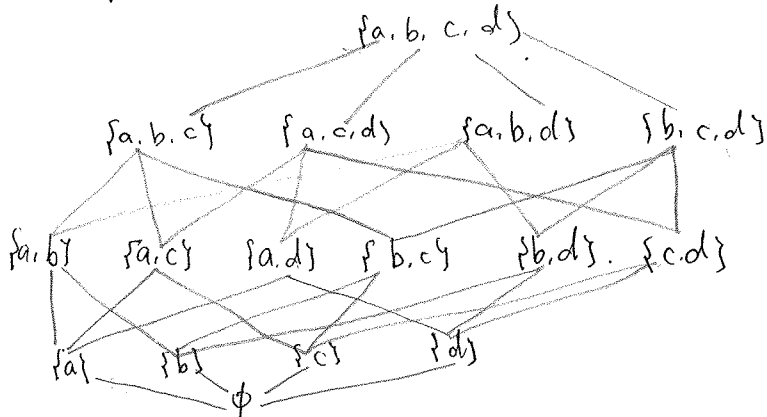
$P_{13} = \{\{a\},\{b,d\},\{c\}\}$. $P_{14} = \{\{a\},\{c,d\},\{b\}\}$. $P_{15} = \{\{a\},\{b\},\{c\},\{d\}\}$.

∴ 有15个不同商集.

设 k元集 有 B_k 个不同商集 (划分) 则 (n+1)元集 有 $B_{n+1} = 1 + \sum_{k=1}^{n} \binom{n}{k} B_k$ 个不同划分. $(k\le n)$

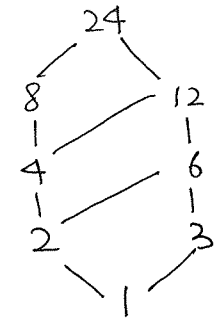
6. (P31, 5) 画偏序集 Hasse 图解.

1) $\mathcal{P}(\{a,b,c,d\})$



2) 24 的全体因子

24 的全体因子为 $\{1,2,3,4,6,8,12,24\}$



置换.

1. 定义：设 X 为有限集，如果 $\sigma: X \to X$ 为双射，则称 σ 为 X 上的一个置换.

设 $|X|=n$ 且 $X=\{1,2,\cdots n\}$ 记：$S_n=\{\sigma: X\to X \mid \sigma$ 为双射$\}$ 则 $|S_n|=n!$

一般地 $\forall \sigma\in S_n$. σ 表示为 $\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$ 其中 $\sigma(k)=i_k$ $(k=1,\cdots n)$

一般对置换的复合简记为乘法 (ie $\forall \sigma,\tau\in S_n$. $\sigma\circ\tau =: \sigma\tau$)

记 $\sigma^k=\sigma\cdot\sigma\cdots\sigma$ (k个复合). 设 k 是使得 $\sigma^k=id_X(=e)$ 的最小正整数. 称 k 为 σ 的阶.

注：1) $\forall \sigma,\tau\in S_n$ $\sigma\tau$ 未必一定等于 $\tau\sigma$ (交换律不一定成立).

2) $\forall \sigma_1,\sigma_2,\sigma_3\in S_n$. $\sigma_1(\sigma_2\sigma_3)=(\sigma_1\sigma_2)\sigma_3$ 结合律成立 (由映射性质自然).

3) 特记 $e:=\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}$ ie. $e=id_X$ 称 e 为 S_n 的单位元.

4) $\forall \sigma\in S_n$ $\exists \sigma^{-1}\in S_n$ s.t. $\sigma\sigma^{-1}=\sigma^{-1}\sigma=e$ (有逆元) (双射有逆).

2. 循环：$\sigma\in S_n$ 称为一个循环，如果 $\exists r\in \mathbb{Z}_{\geq 2}$ 和 $i_1,i_2\cdots i_r\in\{1,2\cdots n\}$

s.t. $\sigma(i_1)=i_2$, $\sigma(i_2)=i_3$ $\cdots$ $\sigma(i_{r-1})=i_r$ $\sigma(i_r)=\sigma(i_1)$

且 $\forall j\in\{1,2\cdots n\}\setminus\{i_1,\cdots i_r\}$ $\sigma(j)=j$.

此时记 $\sigma=(i_1 i_2\cdots i_r)$ 且 $\sigma^k(i_s)=\begin{cases} i_{s+k} & (s+k\leq r)\\ i_{s+k-r} & (s+k>r)\end{cases}$ $(\forall k=1,2\cdots r)$

Prop. 设循环 $\sigma=(i_1 i_2\cdots i_k)$ 则 σ 的阶为 k.

两个循环不相交：设 $\sigma=(i_1,\cdots i_r)$, $\tau=(j_1,\cdots j_t)$ 是两个循环.

如果 $i_\alpha\neq j_\beta$ 对 $\forall \alpha=1,2\cdots r$, $\beta=1,2\cdots t$ 均成立.

则称循环 σ,τ 不相交.

Thm. $\forall$非置换 $\sigma\in S_n$ $\exists$ 不相交的循环 $\sigma_1,\sigma_2\cdots\sigma_s$ s.t. $\sigma=\sigma_1\sigma_2\cdots\sigma_s$ 且在不考虑顺序的情况下次分解性一.

设 σ_i 的阶为 k_i 则 σ 的阶为 $\mathrm{lcm}(k_1,k_2\cdots k_s)$.

$\varepsilon_\sigma=(-1)^{\sum_{i=1}^{s}(k_i-1)}$

3. 对换：长度为 2 的循环称为对换.

Thm. $\forall$置换 均可分解为若干对换的乘积. 且对换个数保证奇偶性不变.

4. 置换的符号 $\forall \sigma\in S_n$ 如果 σ 可分解为奇数个对换的乘积. 称 σ 为奇置换. 记 $\varepsilon_\sigma=-1$

如果 σ --- 偶数 --- 称 σ 为偶置换. 记 $\varepsilon_\sigma=1$

置换.

eg1: $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\5&4&1&7&3&6&2\end{pmatrix}$ 求逆，阶和符号.

解 $\sigma^{-1}=\begin{pmatrix}1&2&3&4&5&6&7\\3&7&5&2&1&6&4\end{pmatrix}$

$\sigma=(153)(247)$ ∴阶为 $\operatorname{lcm}(3,3)=3$

符号为 $\varepsilon_\sigma=(-1)^{(3-1)+(3-1)}=(-1)^4=1$ ∴σ为偶置换.

$\sigma=(15)(35)(24)(47)=(13)(35)(27)(24)$

eg2. $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\5&6&4&7&2&1&3\end{pmatrix}$ 求阶和符号.

解 $\sigma=(1526)(347)$ ∴阶为 $\operatorname{lcm}(4,3)=12$

$=(15)(25)(26)(34)(47)$ 符号为 $\varepsilon_\sigma=(-1)^{4-1+3-1}=-1$ ∴σ为奇置换.

$=(16)(12)(15)(37)(34)$

eg3. 设 $A_n=\{\tau\in S_n \mid \varepsilon_\tau=1\}$ 为全体偶置换组成的集合.

求 A_n 的基数.

解：首先 $|S_n|=n!$

定义映射 $\varphi: A_n \longrightarrow S_n\setminus A_n$ (左集).

$\tau \longmapsto (12)\tau$

良定义显然.

$\forall \tau_1,\tau_2\in A_n$. 如果 $\varphi(\tau_1)=\varphi(\tau_2)$ 即 $(12)\tau_1=(12)\tau_2$ 则 $(12)(12)\tau_1=(12)(12)(\tau_1)$

$\Rightarrow ((12)(12))\tau_1=((12)(12))\tau_2 \Rightarrow \tau_1=\tau_2$ ∴ φ为单射.

$\forall\ \sigma\in S_n\setminus A_n$ 即σ为置换且非偶置换 ∴σ为奇置换 ∴$(12)\sigma\in A_n$

则 $\varphi((12)\sigma)=(12)(12)\sigma=\sigma$ 即σ有原像$(12)\sigma$ ∴ φ为满射.

$\therefore |A_n|=|S_n\setminus A_n|=\frac{n!}{2}$ □.

~~注：$(i_1 i_2\cdots i_s)=$~~

~~$(i_1 i_2)(i_2 i_3)\cdots(i_{s-1} i_s)$~~

~~$(i_1 i_2)(i_1 i_3)\cdots(i_1 i_s)$~~

~~$(i_1 i_2)(i_2 i_3)\cdots(i_{s-1} i_s)$~~

注. $(i_1 i_2\cdots i_s)=(i_1 i_s)(i_1 i_{s-1})\cdots(i_1 i_2)$

…

例子. $\forall \sigma \in S_n$ 和 $(i_1 i_2 \cdots i_k) \in S_n$ $(k \geq 2)$ 求证

$$\sigma \circ (i_1 i_2 \cdots i_k) \circ \sigma^{-1} = (\sigma(i_1)\ \sigma(i_2) \cdots \sigma(i_k))$$

证明：对 $\forall j \in \{1,2,\cdots n\}$ 要么 $j \in \{i_1, \cdots i_k\}$ 要么 $j \in \{1,2,\cdots n\} \setminus \{i_1, \cdots i_k\}$.

如果 $j \in \{i_1, \cdots i_k\}$ 不妨设 $j = i_s$ $(1 \leq s \leq k)$ 则：

$$\sigma \circ (i_1 i_2 \cdots i_k)(j) = \sigma\big((i_1 i_2 \cdots i_k)(i_s)\big) = \begin{cases} \sigma(i_{s+1}) & (s = 1,2 \cdots k-1) \\ \sigma(i_1) & (s = k) \end{cases}$$

$$(\sigma(i_1)\ \sigma(i_2) \cdots \sigma(i_k)) \circ \sigma(j) = (\sigma(i_1) \cdots \sigma(i_k))(\sigma(i_s)) = \begin{cases} \sigma(i_{s+1}) & (s = 1,2 \cdots k-1) \\ \sigma(i_1) & (s = k) \end{cases}$$

$\therefore \sigma \circ (i_1 i_2 \cdots i_k)(j) = (\sigma(i_1)\ \sigma(i_2) \cdots \sigma(i_k)) \circ \sigma(j)$

如果 $j \in \{1,2,\cdots n\} \setminus \{i_1, i_2, \cdots i_k\}$ 则 $\sigma(i_1 i_2 \cdots i_k)(j) = \sigma(j)$

且 $(\sigma(i_1) \cdots \sigma(i_k)) \circ \sigma(j) = \sigma(j)$ $(\because \sigma(j) \notin \{\sigma(i_1), \sigma(i_2), \cdots \sigma(i_k)\})$

$\therefore \sigma \circ (i_1 i_2 \cdots i_k)(j) = (\sigma(i_1)\ \sigma(i_2) \cdots \sigma(i_k)) \circ \sigma(j)$

由 j 任意性： $\sigma \circ (i_1 i_2 \cdots i_k) = (\sigma(i_1) \cdots \sigma(i_k)) \circ \sigma$

$\therefore \sigma (i_1 i_2 \cdots i_k) \sigma^{-1} = (\sigma(i_1)\ \sigma(i_2) \cdots \sigma(i_k))$ □

例子. 设 $a, b, c \in \mathbb{Z}$ 求 $ax + by = c$ 一个整数解.

解：设 $g = \gcd(a,b)$ 如果 $g \nmid c$ 则该方程无整数解.

如果 $g \mid c$ 不妨设 $c = d \cdot g$ $(d \in \mathbb{Z})$

由 Bézout's 关系 对于 $a, b \in \mathbb{Z}$. 于 $\alpha, \beta \in \mathbb{Z}$ s.t. $a\alpha + b\beta = g$

则 $x = d\alpha$, $y = d\beta$ 是方程一组解.

设 $(\tilde{x}, \tilde{y})$ 是该方程另一组解. 即 $a\tilde{x} + b\tilde{y} = c = g \cdot d$ 不妨设 $a' = \frac{a}{g}$, $b' = \frac{b}{g} \in \mathbb{Z}$

则 $a'\tilde{x} + b'\tilde{y} = d = a'x + b'y \Rightarrow a'(\tilde{x} - x) = b'(y - \tilde{y})$ $\because \gcd(a', b') = 1$

$\therefore a' \mid y - \tilde{y}$ 且设 $y - \tilde{y} = a' \cdot k$ $(k \in \mathbb{Z})$ 同理 $b' \mid \tilde{x} - x$ 且 $\tilde{x} - x = b' \cdot k$

$\therefore \begin{cases} \tilde{y} = y - a' \cdot k \\ \tilde{x} = x + b'k \end{cases}$ 则 $\begin{cases} x = d\alpha + k\frac{b}{g} \\ y = d\beta - k\frac{a}{g} \end{cases}$ 是方程全体整数解 (其中 $k \in \mathbb{Z}$).

eg6. 扩展欧几里德算法求 $\gcd(a,b)=ua+vb$. (Extended Euclidean Algorithm)

解：$r_0 = 1\cdot a + 0\cdot b = u_0 a + v_0 b$

$r_1 = 0\cdot a + 1\cdot b = u_1 a + v_1 b$.

$r_2 = r_0 - q_1 r_1 = u_2 a + v_2 b = (u_0 - q_1 u_1)a + (v_0 - q_1 v_1)b$.

$\vdots$

$r_{i+1} = r_{i-1} - q_i r_i = u_{i+1} a + v_{i+1} b = (u_{i-1} - q_i u_i)a + (v_{i-1} - q_i v_i)b$.

$\vdots$

$r_k = r_{k-2} - q_{k-1} r_{k-1} = u_k a + v_k b = (u_{k-2} - q_{k-1} u_{k-1})a + (v_{k-2} - q_{k-1} v_{k-1})b$

$r_{k+1} = r_{k-1} - q_k r_k = 0$

(要求 $0 \le r_{i+1} < |r_i|$ 对 $i = 0, 1, 2 \cdots k$ 均成立则 q_i 唯一确定)

则 $\gcd(a,b) = r_k = u_k a + v_k b$

其中 u_k. v_k 满足递推关系 $\begin{cases} u_{i+1} = u_{i-1} - q_i u_i \\ u_0 = 1 \\ u_1 = 0 \end{cases}$ $\begin{cases} v_{i+1} = v_{i-1} - q_i v_i \\ v_0 = 0 \\ v_1 = 1 \end{cases}$