第三次习题课

一、作业三的解析及需要注意的问题

映射的三个基本要素：①定义域 ②值域 ③映射规则 $x \longmapsto f(x)$.

定义（左逆、右逆与逆）

设映射 $f: X \longrightarrow Y$，映射 $g: Y \longrightarrow X$ 称为 f 的 $\begin{cases} \text{一个左逆，若 } g\circ f = e_X. \\ \text{一个右逆，若 } f\circ g = e_Y. \\ \text{逆 若 } g\circ f = e_X \text{ 且 } f\circ g = e_Y. \end{cases}$

引理 $f: X \longrightarrow Y$ 存在 $\begin{cases} \text{左逆} \Longleftrightarrow f \text{ 是单射.} \\ \text{右逆} \Longleftrightarrow f \text{ 是满射.} \\ \text{逆} \Longleftrightarrow f \text{ 是双射.} \end{cases}$ （留作思考题，因已证）

eg1. $f: \mathbb{N} \longrightarrow \mathbb{N}$ 是否有右逆？给出 f 的两个左逆.
$\quad n \longmapsto n^2$

解：由于 f 不是满射，如 $f^{-1}(2) = \phi$，$\therefore f$ 不存在右逆。

f 的两个左逆：$f_1: \mathbb{N} \longrightarrow \mathbb{N}$ s.t. $f(n) = \begin{cases} m & n = m^2\ (\exists m \in \mathbb{N}) \\ 1 & n \neq m^2\quad \forall m \in \mathbb{N} \end{cases}$

$f_2: \mathbb{N} \longrightarrow \mathbb{N}$ s.t. $f(n) = \begin{cases} m & n = m^2 \text{ for some } m \in \mathbb{N} \\ 2 & n \neq m^2\quad \forall m \in \mathbb{N} \end{cases}$

eg2. 对映射 $f: X \longrightarrow Y$，$g: Y \longrightarrow X$，定义 $G(f) = \{(x, f(x)) \mid x \in X\}$
$H(g) = \{(g(y), y) \mid y \in Y\}$.

证明：f 是 g 的逆映射 $\Longleftrightarrow G(f) = H(g)$.

证明："$\Longrightarrow$" 设 f 是 g 的逆映射，则 $g\circ f = e_X$ 且 $f\circ g = e_Y$.

任取 $(x, f(x)) \in G(f)$，则 $f(x) \in Y$ 且 $g(f(x)) = (g\circ f)(x) = e_X(x) = x$，

故 $(x, f(x)) = (g(f(x)), f(x)) \in H(g)$，所以 $G(f) \subseteq H(g)$；

任取 $(g(y), y) \in H(g)$，则 $g(y) \in X$ 且 $f(g(y)) = (f\circ g)(y) = e_Y(y) = y$，

故 $(g(y), y) = (g(y), f(g(y))) \in G(f)$，所以 $H(g) \subseteq G(f)$.

综上可知 $H(g) = G(f)$.

"$\Longleftarrow$" 设$G(f)=H(g)$，要证f是g的逆映射，只需证明$g\circ f=e_X$且$f\circ g=e_Y$.

对$\forall x\in X$，$(x,f(x))\in G(f)=H(g)$，故$\exists\,(g(y),y)\in H(g)$ s.t.

$(x,f(x))=(g(y),y)$ 故$x=g(y)$且$f(x)=y$. 于是有 $x=g(y)=(g\circ f)(x)$

对任意的$x\in X$成立. 从而$g\circ f=e_X$.

对$\forall y\in Y$，$(g(y),y)\in H(g)=G(f)$，故$\exists\,(x,f(x))\in G(f)$ s.t

$(g(y),y)=(x,f(x))$ 故$y=f(x)$且$x=g(y)$. 所以 $y=f(g(y))=(f\circ g)(y)$

对$\forall y\in Y$成立. 从而$f\circ g=e_Y$. 故f是g的逆映射.

hw2. $|S|=m$，$|T|=n$. S,T为两个非空集合.

(1) 任意给定S中的元素，该元素映到T的方式有n种，故S到T：n^m个.

(2) 双射条件：$m=n$　　　双射个数：$n!=m!$

单射条件：$m\le n$　　　单射个数：$n(n-1)\cdots(n-m+1)=A_n^m$

满射条件：$m\geq n$

满射个数：(容斥原理)

$|S|=m$，$|T|=n$，$m\geq n$. 设$T=\{t_1,\cdots,t_n\}$，I是从S到T的非满射的映射的集合，则从S到T的满射的个数为$n^m-|I|$.

设$I_i=\{f:S\longrightarrow T \mid t_i\notin \operatorname{Im} f\}$

则$I=I_1\cup\cdots\cup I_n$.

根据容斥原理：$$I=\sum_{i=1}^{n}|I_i|-\sum_{1\le i<j\le n}|I_i\cap I_j|+\cdots+(-1)^{k-1}\sum_{1\le i_1<i_2<\cdots<i_n\le n}|I_{i_1}\cap\cdots\cap I_{i_k}|+\cdots+(-1)^n|I_1\cap\cdots\cap I_n|.$$

注意到 $I_{i_1}\cap\cdots\cap I_{i_k}=\{f:S\longrightarrow T \mid t_{i_1},\cdots,t_{i_k}\notin \operatorname{Im} f\}$

是从S到$T\setminus\{t_{i_1},\cdots,t_{i_k}\}$的所有映射的集合.

于是$|I_{i_1}\cap\cdots\cap I_{i_k}|=(n-k)^m$

从而 $$\sum_{1\le i_1<\cdots<i_k\le n}|I_{i_1}\cap\cdots\cap I_{i_k}|=\binom{n}{k}(n-k)^m$$

于是 $|I| = \binom{n}{1}(n-1)^m - \binom{n}{2}(n-2)^m + \cdots + (-1)^{k-1}\binom{n}{k}(n-k)^m + \cdots + (-1)^{n-1}\binom{n}{n}(n-n)$

$$= \sum_{k=1}^{n} (-1)^{k-1}\binom{n}{k}(n-k)^m$$

故满射个数为

$$n^m - \sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}(n-k)^m$$

$$= n^m + \sum_{k=1}^{n}(-1)^{k}\binom{n}{k}(n-k)^m$$

$$= \sum_{k=0}^{n}(-1)^{k}\binom{n}{k}(n-k)^m$$

$$= \sum_{k=0}^{n-1}(-1)^{k}\binom{n}{k}(n-k)^m$$

等价关系的三个条件：$\begin{cases} \text{反身性} \\ \text{对称性} \\ \text{传递性} \end{cases}$

eg3. 任给一个映射 $f: X \to Y$，我们可以定义 X 上的一个等价关系：

$$x_1 \sim_f x_2 \Longleftrightarrow f(x_1) = f(x_2)$$ [可以验证 $\sim_f$ 是一个等价关系]

对任意的 $x \in X$，x 的等价类为 $\bar{x} = \{x' \in X \mid f(x') = f(x)\}$.

商集 $X/\sim_f$ 是 X 中等价类的集合，其中的每个元素为集合，即 $X/\sim_f = \{\bar{x} : x \in X\}$.

自然映射 $\pi: X \longrightarrow X/\sim_f$; $\quad x \longmapsto \bar{x}$

商映射：$\bar{f}: X/\sim_f \longrightarrow Y$; $\quad \bar{x} \longmapsto f(x)$.

1) $\bar{f}$ 是良定义的或 $\bar{f}$ 的定义是合理的：$\forall\ \bar{x}_1 = \bar{x}_2 \Longrightarrow \bar{f}(x_1) = \bar{f}(x_2)$

或

$\forall\ x' \in \bar{x} \Longrightarrow f(x) = f(x')$

2) $\bar{f}$ 是单射：$\bar{f}(\bar{x}_1) = \bar{f}(\bar{x}_2) \Longrightarrow f(x_1) = f(x_2) \Longrightarrow x_1 \sim x_2$ 即 $\bar{x}_1 = \bar{x}_2$.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "\pi"'] & Y \\ & X/\sim_f \arrow[u, "\bar{f}"'] \end{tikzcd}$$

$f = \bar{f} \circ \pi$ 映射的分解

hw4. 设 $C=\{(x,y)\in\mathbb{R}^2 \mid x^2+y^2=1\}$

$$f:[0,2\pi]\longrightarrow C$$
$$\theta \longmapsto (\cos\theta,\ \sin\theta)$$

[$\sim_f$ 是由映射 f 诱导的等价关系]

证: $\alpha\sim_f\beta \Longleftrightarrow f(\alpha)\sim_f f(\beta)\quad \forall\ \alpha,\beta\in[0,2\pi]$

(1) $\forall\ \alpha,\beta\in(0,2\pi)$, 若 $f(\alpha)=f(\beta)$ 即 $\begin{cases}\cos\alpha=\cos\beta\\ \sin\alpha=\sin\beta\end{cases}$

$\Longrightarrow \alpha=\beta$ 则 $\bar{\alpha}=\{\alpha\}$.

(2) $f(0)=f(2\pi)=(1,0)$ $\therefore \{0,2\pi\}\subset\bar{0}$

又 $\forall\ \alpha\in(0,2\pi)$ $\cos\alpha\neq 1 \Longrightarrow f(\alpha)\neq(1,0)$ $\therefore \{0,2\pi\}=\bar{0}$.

eg4. 设 $\sim$ 是集合 X 上的一个等价关系, 且 $f:X\to Y$ 是一个映射, 满足

$$x\sim x' \Longrightarrow f(x)=f(x')\qquad (*)$$

1) 证明 f 与 $\sim$ 的相容性条件允许定义一个从 $X/\sim$ 到 Y 的诱导映射 $\bar{f}:\bar{x}\longrightarrow f(x)$, 它给出了分解式 $f=\bar{f}\circ\pi$ 且 $\bar{f}$ 不一定是单射.

2) 给出 $\bar{f}$ 成为单射的条件并证明之。

证明: 首先证明 $\bar{f}:\ X/\sim \longrightarrow Y$ 是良定义的: 若 $\bar{x}_1=\bar{x}_2$, 则
$$\bar{x}\longmapsto f(x)$$

$x_1\sim x_2$, 由相容性条件 $(*)$

$f(x_1)=f(x_2)$, 故 $\bar{f}(\bar{x}_1)=\bar{f}(\bar{x}_2)$ 即 $\bar{f}$ 是良定义的。

对 $\forall\ x\in X$, $(\bar{f}\circ\tilde{\pi})(x)=\bar{f}(\tilde{\pi}(x))=\bar{f}(\bar{x})=f(x)$, 故 $\bar{f}\circ\tilde{\pi}=f$, 分解成立.

下面说明 $\bar{f}$ 不一定是单射.

若令 $X=\{1,2,3\}$, $Y=\{1\}$, $X/\sim=\{\{1,2\},\{3\}\}$, $f:X\longrightarrow Y$

则 f 与 $\sim$ 满足 $(*)$.

注意到 $\bar{1}\neq\bar{3}$, 但 $\bar{f}(\bar{1})=\bar{f}(\bar{3})=1$, 故 $\bar{f}$ 不是单射, 即一般情况下, $\bar{f}$ 不一定是单射。

2) $\bar{f}$是单射的充要条件是 $\sim = \sim_f$，即 $\forall x_1, x_2 \in X$，总有

$$x_1 \sim x_2 \Longleftrightarrow f(x_1)=f(x_2).$$

为区别 $\sim$ 与 $\sim_f$，记 $X/\sim_f = \{\bar{\bar{x}} \mid x \in X\}$，即 $\bar{\bar{x}} = \{x' \in X \mid f(x')=f(x)\}$.

并记
$$\bar{\bar{f}}: X/\sim_f \longrightarrow Y, \quad \bar{\bar{x}} \longmapsto f(x)$$
则 $\bar{\bar{f}}$是单射.

定义：
$$g: X/\sim \longrightarrow X/\sim_f, \quad \bar{x} \longmapsto \bar{\bar{x}}$$

我们断言g是良定义的：对 $\forall \bar{x}_1 = \bar{x}_2$
即 $x_1 \sim x_2$.

由(*)，$f(x_1)=f(x_2)$，故由 $\sim_f$ 的定义，$\bar{\bar{x}}_1 = \bar{\bar{x}}_2$，即$g$是良定义的.

显然g是满射且有分解 $\bar{f} = \bar{\bar{f}} \circ g$. 由于$\bar{\bar{f}}$是单射，故$\bar{f}$是单射的充要条件是$g$是单射.

$$\begin{tikzcd}
\underset{(\bar{x})}{X/\sim} \arrow[rr, "\bar{f}"] \arrow[dr, "g"'] & & \overset{f(x)}{Y} \\
& \underset{(\bar{\bar{x}})}{X/\sim_f} \arrow[ur, "\bar{\bar{f}}"'] &
\end{tikzcd}$$

而g单 $\Longleftrightarrow X/\sim = X/\sim_f$
$\Longleftrightarrow \sim = \sim_f$.

可数集

集合论是数理逻辑的一个分支，由德国数学家 Cantor 创立.

比较两个有限集合元素个数的大小有两种方法：

① 先数出每个集合中的元素个数，然后比较两个数的大小；

② 如果从集合A到集合B存在单射，则集合A中的元素个数必然不多于集合B中的元素个数。

对于两个无穷集合，无法用①比较集合的大小，解决办法是用集合间的映射，即方法②，所以说集合间的映射比集合元素的个数计算更基本。

以集合($\mathbb{Z}_+$)为参照物。

定义：称集合A是可数的，如果存在双射 $\varphi: A \longrightarrow \mathbb{Z}_+$.

（一般来说，称集合A，B"个数相同"，若存在双射 $\varphi: A \longrightarrow B$）.

eg5. 整数是可数的.

证明：构造 $f: \mathbb{Z} \longrightarrow \mathbb{Z}_+$，其中 $f(x) = \begin{cases} 2x & x>0 \\ -2x+1 & x\le 0 \end{cases}$. 显然$f$是双射.

故$\mathbb{Z}$是可数集。

eg6. 有理数集是可数的.

证明：首先证明任何有理数集合$\mathbb{Q}^+$是可数的，注意到$\forall$正有理数均可写成 $\frac{m}{n}$ $(m,n\in\mathbb{Z}^+)$的形式

	1	2	3	4		
1	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{5}{1}$	$\frac{6}{1}$
2	$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$	$\frac{5}{2}$	
3	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$		
4	$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$		

下面证明$\mathbb{Q}$是可数集，由于$\mathbb{Q}^+$可数，故存在双射 $f: \mathbb{Z}^+ \longrightarrow \mathbb{Q}^+$

定义：$g: \mathbb{Z}^+ \longrightarrow \mathbb{Q}$ s.t. $g(n) = \begin{cases} 0 & n=1 \\ -f(\frac{n-1}{2}) & n\text{为}\ge 3\text{的奇数} \\ f(\frac{n}{2}) & n\text{为偶数} \end{cases}$

可验证g为双射. 故$\mathbb{Q}$为可数集。

eg7. $\mathbb{R}$不是可数集.

证：反证法：若$\mathbb{R}$是可数集，则存在$\mathbb{Z}^+$到$\mathbb{R}$的双射，从而存在$\mathbb{Z}^+$到$[0,1)$的满射.

下证不存在$\mathbb{Z}^+$到$[0,1)$的满射，从而$\mathbb{R}$不可数。

假若$f:\mathbb{Z}^+\longrightarrow[0,1)$是满射，由于$[0,1)$中的任一实数均可唯一地表示

$n\in\mathbb{Z}^+$，可记 $f(n)=0.a_{n1}a_{n2}a_{n3}\cdots$

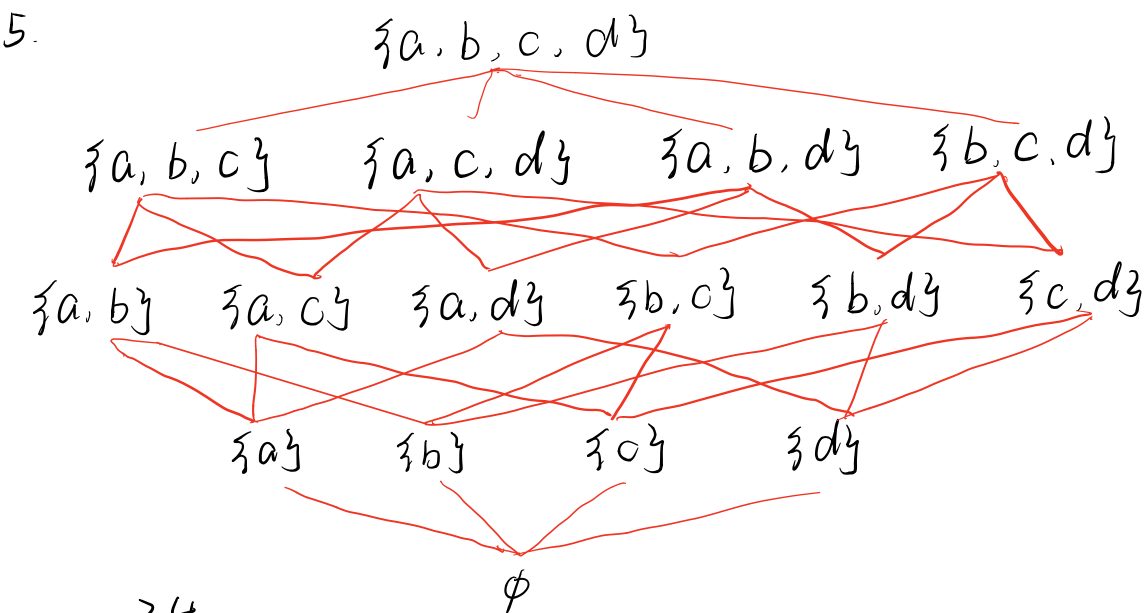
$$\begin{array}{ccc}
1 & \longrightarrow & 0.a_{11}a_{12}a_{13}\cdots \\
2 & \longrightarrow & 0.a_{21}a_{22}a_{23}\cdots \\
3 & \longrightarrow & 0.a_{31}a_{32}a_{33}\cdots \\
\vdots & & \vdots
\end{array}$$

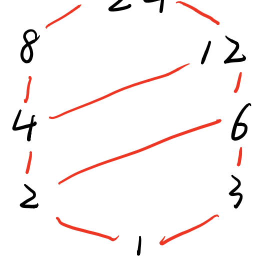
令 $b=0.b_1b_2b_3\cdots$ 其中 $b_i=\begin{cases}0 & 若\ a_{ii}\neq 0\\ 1 & 若\ a_{ii}=0\end{cases}$ 则 $b\in[0,1)$ 且 $b\notin Im(f)$.

故f不是满射，矛盾。

hw4. 集合A有多少不同商集相当于A有多少种划分。

hw5.





二、作业四的解析及需要注意的问题

hw3. 任何S_n中置换都可以写成至多$n-1$个对换的乘积。

证：任何S_n中置换均可以写成互不相交循环的乘积. $\pi=\pi_1\pi_2\cdots\pi_m$,

并且有 $\sum_{i=1}^{m} l_i \le n$. 其中l_i为循环π_i的长度，而且每个循环π_i均可以写成l_i-1个对换的乘积，所以π可以写成 $\sum_{i=1}^{m}(l_i-1)=\sum_{i=1}^{m} l_i - m$

$\le n-m \le n-1$ 个对换.

hw4. 讲义命题6.19. (只需证 $\tau\sigma\tau^{-1}=(\tau(i_1)\tau(i_2)\cdots\tau(i_k))$)

hw1. $\forall\, \sigma\in S_n\setminus\{e\}$, σ是有限个两两互不相交的长度大于1的循环之积。

任何一个循环都是若干个对换之积。

奇偶置换的定义.

$\sigma_1=\underbrace{(1246)}_{\tau_1}\underbrace{(35)}_{\tau_2}$ $\quad$ $\mathrm{ord}(\sigma_1)=\mathrm{lcm}(\mathrm{ord}(\tau_1),\mathrm{ord}(\tau_2))=4.$

τ_1可分解成$4-1$个对换乘积，τ_2可分解成$2-1$个对换乘积.

$\therefore\ \varepsilon_{\sigma_1}=\varepsilon_{\tau_1}\varepsilon_{\tau_2}=(-1)^{4-1}(-1)^{2-1}=1.$

hw2. 证：$\varepsilon_\pi=\varepsilon_{\pi_1}\varepsilon_{\pi_2}\cdots\varepsilon_{\pi_m}$
$=(-1)^{l_1-1}(-1)^{l_2-1}\cdots(-1)^{l_m-1}$

hw5. 解：$253=1\times253+0\times161=r_0$

$161=0\times253+1\times161=r_1$

$92=253-1\times161=r_0-q_1r_1=r_2$

$69=161-1\times92=r_1-q_2r_2=r_3$

$23=92-1\times69=r_2-q_3r_3=r_4=\gcd(161,253).$

$0=69-3\times23=r_3-q_4r_4$

$v_0=1,\quad v_1=0,\quad v_2=v_0-q_1v_1=1\quad v_3=v_1-q_2v_2=-1\quad v_4=v_2-q_3v_3=2$

$u_0=0,\quad u_1=1\quad u_2=u_0-q_1u_1=-1\quad u_3=u_1-q_2u_2=2\quad u_4=u_2-q_3u_3=-3.$

$\therefore\ \gcd(161,253)=23=253\times2+161\times(-3)$

$\mathrm{lcm}(161,253)=\dfrac{161\times253}{23}=1771=161\times11=253\times7$ $\quad$ $\begin{cases}u=-3+11k\\ v=2-7k\end{cases}$ 均满足.

eg8. 证明如下结论

(1) $\gcd(ma, mb) = m\gcd(a,b)$

(2) 若 $\gcd(a,b)=1$，则 $\gcd(ab,m)=\gcd(a,m)\gcd(b,m)$.

证：(1) Method 1：设 $g=\gcd(a,b)$. $a=n_1 g$，$b=n_2 g$ 其中 $\gcd(n_1,n_2)=1$.

则 $ma=n_1 mg$，$mb=n_2 mg \Longrightarrow \gcd(ma,mb)=mg$

$=m\gcd(a,b)$.

Method 2：设 $g=\gcd(a,b)$ $\because g\mid a$，$g\mid b$ $\therefore mg\mid ma$，$mg\mid mb$.

即 mg 是 ma，mb 的公因子

$\exists u,v\in\mathbb{Z}$, s.t. $ua+vb=g \Longrightarrow uma+vmb=mg$

任取 ma，mb 的公因子 d，$d\mid ma$，$d\mid mb \Longrightarrow d\mid mg$.

$\therefore mg=\gcd(ma,mb)$

(2) 设 $g=\gcd(ab,m)$，$g_1=\gcd(a,m)$，$g_2=\gcd(b,m)$ 下证 $g=g_1g_2$

一方面 $g_1\mid a$，$g_2\mid b \Longrightarrow g_1g_2\mid ab$

$\because \gcd(a,b)=1$ $\therefore \gcd(g_1,g_2)=1$ $\therefore g_1\mid m$，$g_2\mid m \Longrightarrow g_1g_2\mid m$

即 g_1g_2 是 ab，m 的公因子，$\therefore g_1g_2\mid g$.

另一方面. $\exists u_1,u_2,v_1,v_2\in\mathbb{Z}$ s.t. $u_1a+v_1m=g_1$，$u_2b+v_2m=g_2$

$\therefore g_1g_2=u_1u_2ab+(v_1v_2m+v_1u_2b+u_1v_2a)m$

$\because g\mid ab$，$g\mid m$ $\therefore g\mid g_1g_2$ 因此 $g=g_1g_2$

注：① $g_1\mid m$，$g_2\mid m \xRightarrow{\gcd(g_1,g_2)=1} g_1g_2\mid m$ eg. $6\mid 12$，$4\mid 12$，但 $24\nmid 12$

② 若 $\gcd(a,b)\neq 1$ 则 (2) 中等式不一定成立.

eg. $a=2$，$b=4$，$m=6$ $\gcd(ab,m)=\gcd(8,6)=2$ $\gcd(a,m)\gcd(b,m)$

$=2\times 2=4$