1.1. 集合、映射、等价关系.

△

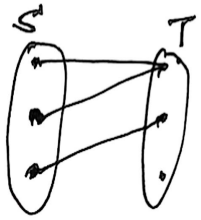
映射: $\varphi: S \longrightarrow T$

$a \longmapsto \varphi(a)$

[well defined]

对S中的"任意"一个元素 a

"唯一"确定一个元素与之对应.



单射: $\varphi: S \to T$ 是一个映射.

(1) 对S中的任意两个不同元素 x_1, x_2, 都有 $\varphi(x_1) \neq \varphi(x_2)$

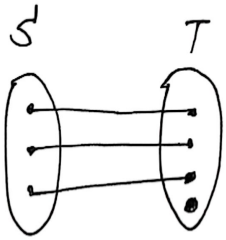
⇕

(2) 对T中的 $\forall$ 若 $\varphi(x_1) = \varphi(x_2)$ 则必有 $x_1 = x_2$

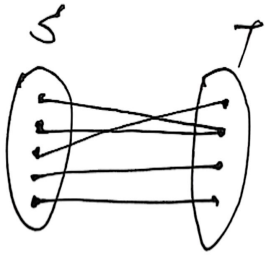
[像相同, 则原像相同]

⇕

(3) $\ker(\varphi) = 0$, $\ker(\varphi) = \{a \mid \varphi(a) = 0\}$



满射: T中任意元素在S中都有原像



1. 证明: 自反性(反身性)

$a \sim a \Leftrightarrow a \sim a$

对称性: $a \sim b \Leftrightarrow n \mid a-b$ ⇕ 故 $b \sim a \Leftrightarrow n \mid b-a$

传递性: $a \sim b,\ b \sim c \Rightarrow a \sim c$

$(n \mid a-b,\ n \mid b-c \Rightarrow n \mid a-c)$ □

2. 证明:

自反性: aRa $(\forall a)$ ✓

对称性: $aRb \Rightarrow bRa$ $(\exists \lambda \in I,\ a, b \in S_\lambda)$

传递性 $aRb,\ bRc \Rightarrow aRC$ $(\exists \lambda \in I\ a, b \in S_\lambda,\ \exists \gamma \in I\ b, c \in R_\gamma$ 故 $\lambda = \gamma$ $a, b, c \in S_\lambda)$

□

3. 证明：由 $f: S \to S$ 的双射，$g: S \to S$ 是 f 的逆映射，即 $f^{-1} = g$.

若在 S 中有 $g(x) = g(y)$，即 $f^{-1}(x) = f^{-1}(y)$ 由 f 是双射，得 $x = y$. 故 g 是单射.

对任给的一个元素 $x \in S$. 即有 $g \cdot (f^{-1}(x)) = x$. 故 $f(x)$ 为 x 在 g 下的原像

故 g 是满射，因此 g 是双射. 由命题 1.1.2. (g 可逆 $\Leftrightarrow$ g 双射)

故 g 可逆. 由 $g \circ f = f^{-1} \circ f = id_S$，$f \circ g = f \circ f^{-1} = id_S$

故 $g^{-1} = f$. 得证. □

4. 证明：
- 自反性：$S \sim S$ $(f(s) = f(s))$
- 对称性：$S \sim S' \Rightarrow S' \sim S$ $(f(s) = f(s'))$
- 传递性：$S \sim S'$，$S' \sim S''$，故有 $f(s) = f(s') = f(s'')$

因此有 $S \sim S''$.

等价类：S 的等价类 $\bar{S} = \{a \mid f(a) = f(s)\} = f^{-1}(\{S\})$

5. 证明：
- 自反性：$(a,b) \sim (a,b)$ $(\because ab = ba)$
- 对称性：$(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$ $(\because ad = bc)$
- 传递性：$(a,b) \sim (c,d)$，$(c,d) \sim (e,f)$ 故 $ad = bc$，$cf = de$

故 $adf = bcf$，$bcf = bde \Rightarrow adf = bde$

$\Rightarrow af = be$

得 $(a,b) \sim (e,f)$ □

6. 证明：对于任意 $x \in S$，由对称性，若 xRy，则 yRx.

问题出在：存在这样的 y 吗？(y 不一定存在)

即 $\{x\}$ 自己形成一个等价关系的一个等价类. □

$R = \{\{x\}, \{y,z\}, \{a,b,c\}, \{g\}, \{f\}\}$

7: ①. 对称性 + 传递性 $\not\Rightarrow$ 自反性. (见6题)

~~$A=\{1,2,3\}$~~ $A=\{a,b,c\}$. $R=\{(a,a),(b,b),(a,b),(b,a)\}$

R中有对称性,有传递性. 但没有自反性. 没有 (c,c)

②. 自反性 + 传递性 $\not\Rightarrow$ 对称性.

"$\geq$"

($a\geq a$, $a\geq b$, $b\geq c \Rightarrow a\geq c$), 但 $a\geq b$, 得不到 $b\geq a$

③. 自反性 + 对称性 $\not\Rightarrow$ 传递性

(未指定关系)

令 S 是所有英文单词组成的集合, a, b 代表两个单词

定义 aRb: a,与 b 中具有相同的字母)

则 aRa, $aRb\Rightarrow bRc$. 但 aRb, $bRc \not\Rightarrow$ @. aRC.

(例: $a=$ math $b=$ combinatorics $C=$ zoo)

□

1.2 代数运算、代数系

1. 整数集Z对于数的减法组成代数系.

(1) 不满足交换律 $(a\circ b=b\circ a)$

$2-3\neq 3-2$

(2) 不满足结合律 $(a\circ b)\circ c=a\circ(b\circ c)$

$(a-b)-c=a-b-c\neq a-(b-c)$

(3) 单位元 不存在, $(e\circ s=s\circ e=s)$

(4) 逆元 不存在.

□

2. (1) 交换律成立 $a\cdot b=a+b+ab=b\cdot a$

(2) 结合律成立

$(a\cdot b)\cdot c=(a+b+ab)\cdot c=a+b+ab+c+ac+bc+abc$

$a\cdot(b\cdot c)=a\cdot(b+c+bc)=a+b+c+bc+ab+ac+abc$

(3) 单位元: $e=0$

$e\cdot a=e+a+ea=a\Rightarrow e=0$

(4) 逆元: ~~存在~~ 不一定存在.

若存在逆元, $\forall a\in R$. $a\cdot b=a+b+ab=0\Rightarrow b=-\frac{a}{1+a}$

故当 $a\neq -1$ 时存在逆元.

□

3. $A\cdot X=\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a+c&b+d\\a&b\end{pmatrix}$

$X\cdot A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}=\begin{pmatrix}a+b&a\\c+d&c\end{pmatrix}$

若 $A\cdot X=X\cdot A$ 则: $b=c$, $a=c+d$.

故条件为 $\begin{cases}a=c+d\\b=c\end{cases}$

□

4. 由代数系的定义，需证明：

① S非空，显然 $X=\begin{pmatrix}0&0\\0&0\end{pmatrix}\in S$，或 $E=\begin{pmatrix}1&0\\0&1\end{pmatrix}\in S$.

② 二元运算封闭 $(S\times S\to S)$ 即封闭性，亦即：

若 $X_1\in S$，$X_2\in S$，有 $X_1X_2\in S$.

由 $(X_1X_2)A=X_1(X_2A)=X_1(AX_2)=(X_1A)X_2=(AX_1)X_2=A(X_1X_2)$

（矩阵乘法的结合律）

故 $X_1X_2\in S$.

③ 满足交换律（$X_1,X_2\in S$，有 $X_1X_2=X_2X_1$）

首先显然有 X_1X_2，$X_2X_1\in S$

由第3题可设 $X_1=\begin{pmatrix}a&b\\b&a-b\end{pmatrix}$，$X_2=\begin{pmatrix}x&y\\y&x-y\end{pmatrix}$

故 $X_1X_2=\begin{pmatrix}a&b\\b&a-b\end{pmatrix}\begin{pmatrix}x&y\\y&x-y\end{pmatrix}=\begin{pmatrix}ax+by&ay+b(x-y)\\bx+y(a-b)&by+(a-b)(x-y)\end{pmatrix}$

$X_2X_1=\begin{pmatrix}x&y\\y&x-y\end{pmatrix}\begin{pmatrix}a&b\\b&a-b\end{pmatrix}=\begin{pmatrix}ax+by&xb+y(a-b)\\ya+(x-y)b&by+(x-y)(a-b)\end{pmatrix}$

④ 满足结合律：（$X_1X_2X_3\in S$，有 $(X_1X_2)X_3=X_1(X_2X_3)$）

由矩阵乘法本身便具有结合律，故代数系统亦具有结合律 □

⑤ 单位元 $E=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ 都有 $EA=AE$，故 $E\in S$.

对 $\forall X\in S$，$X=\begin{pmatrix}a&b\\b&a-b\end{pmatrix}$ 故 $EX=\begin{pmatrix}a&b\\b&a-b\end{pmatrix}=XE$

⑥ 没有逆元（零元没有逆元：$X=\begin{pmatrix}0&0\\0&0\end{pmatrix}$）

注：若可表为，都分元素有逆元

$\begin{pmatrix}a&b\\b&a-b\end{pmatrix}\begin{pmatrix}x&y\\y&x-y\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ 得 $\begin{cases}ax+by=1\\ay+b(x-y)=0\end{cases}$ 解方程组

$$\begin{cases}a=\dfrac{y-x}{y^2+y-x}\\[2ex] b=\dfrac{y}{y^2+y-x}\end{cases}$$

□

1.3 整数系

1. (1) 由 $ac \equiv bc \pmod n$，故 $n \mid (ac-bc) = c(a-b)$

由于 $(c,n)=1$，故 $n \mid (a-b)$ 得证

(2) 由 $a \equiv b \pmod n$ 故 $n \mid a-b$，即 $a-b = mn$ 对某个 $m \in \mathbb{Z}$

故 $(a-b)k = ak-bk = m \cdot nk$，因此 $ak \equiv bk \pmod{nk}$ $k \in \mathbb{N}$

(3) 由题意：$a = x_1 d$ $b = x_2 d$ $n = x_3 d$ 对某些 $x_1, x_2, x_3 \in \mathbb{Z}$.

故由 $a \equiv b \pmod n$ ~~$(a-b) \mid n$~~ $n \mid (a-b)$ 即.

$x_3 d \mid (x_1 - x_2) d$ 即 $x_3 \mid x_1 - x_2$ 故 $\frac{n}{d} \mid \left(\frac{a}{d} - \frac{b}{d}\right)$ 得证 □

2. (1) 在 $\mathbb{Z}/2\mathbb{Z}$ 中 $\bar{1}+\bar{1}=\bar{0}$，$\bar{3}\cdot\bar{5}=\bar{1}$，$\bar{2}+\bar{5}=\bar{1}$.

(2) 在 $\mathbb{Z}/32\mathbb{Z}$ 中 $\bar{1}+\bar{1}=\bar{2}$，$\bar{3}\cdot\bar{5}=\bar{0}$，$\bar{2}+\bar{5}=\bar{1}$.

(3) 在 $\mathbb{Z}/7\mathbb{Z}$ 中 $\bar{1}+\bar{1}=\bar{2}$，$\bar{3}\cdot\bar{5}=\bar{1}$，$\bar{2}+\bar{5}=\bar{0}$ □

3. (1) 在 $\mathbb{Z}/5\mathbb{Z}$ 中 $\bar{2}+\bar{3}=\bar{0}$，$\bar{2}\cdot\bar{2}=\bar{4}$，$\bar{2}\cdot\bar{3}=\bar{1}$

$\bar{2}$ 在 $\mathbb{Z}/5\mathbb{Z}$ 中有乘法逆元为 $\bar{3}$.

(2) 在 $\mathbb{Z}/4\mathbb{Z}$ 中 $\bar{2}+\bar{3}=\bar{1}$，$\bar{2}\cdot\bar{2}=\bar{0}$，$\bar{2}\cdot\bar{3}=\bar{2}$

$\bar{2}$ 在 $\mathbb{Z}/4\mathbb{Z}$ 中~~有逆~~无关于乘法的逆元，(因为 $(2,4)=2$) 不互素.

(3) 在 $\mathbb{Z}/2\mathbb{Z}$ 中 $\bar{2}+\bar{3}=\bar{1}$，$\bar{2}\cdot\bar{2}=\bar{0}$，$\bar{2}\cdot\bar{3}=\bar{0}$.

$\bar{2}$ 在 $\mathbb{Z}/2\mathbb{Z}$ 中无关于乘法的逆元 $\bar{2}$ 在 $\mathbb{Z}/2\mathbb{Z}$ 中为零元. □

4. ~~$(\mathbb{Z}/12\mathbb{Z})^*$~~ $(\mathbb{Z}/12\mathbb{Z})^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$.

乘法逆元分别为：$\bar{1}, \bar{5}, \bar{7}, \bar{11}$，即自身. $\bar{1}\cdot\bar{1}=\bar{1}$，$\bar{5}\cdot\bar{5}=\bar{1}$，... □

5. $(\mathbb{Z}/7\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

乘法逆元分别为 $\bar{1}, \bar{4}, \bar{5}, \bar{2}, \bar{3}, \bar{6}$，

即：$\bar{1}\cdot\bar{1}=\bar{1}$，$\bar{2}\cdot\bar{4}=\bar{1}$，$\bar{3}\cdot\bar{5}=\bar{1}$，$\bar{6}\cdot\bar{6}=\bar{1}$

□

6. trivial and bored

由命题 1.3.5, $(m,n)=1$, 则 $\varphi(mn)=\varphi(m)\varphi(n)$, $\boxed{(m,n\neq 1)}$

由命题 1.3.6, p 是素数, $k\in\mathbb{N}_0$, 则 $\varphi(p^k)=p^k-p^{k-1}$.

$\varphi(1)=0$
$\varphi(2)=1$
$\varphi(3)=2$
$\varphi(4)=2$
$\varphi(5)=4$
$\varphi(6)=2$
$\varphi(7)=6$
$\varphi(8)=4$
$\varphi(9)=6$
$\varphi(10)=4$

$\varphi(11)=10$
$\varphi(12)=4$
$\varphi(13)=12$
$\varphi(14)=6$
$\varphi(15)=8$
$\varphi(16)=8$
$\varphi(17)=16$
$\varphi(18)=6$
$\varphi(19)=18$
$\varphi(20)=8$

$\varphi(21)=12$
$\varphi(22)=10$
$\varphi(23)=22$
$\varphi(24)=8$
$\varphi(25)=20$
$\varphi(26)=12$
$\varphi(27)=18$
$\varphi(28)=12$
$\varphi(29)=28$
$\varphi(30)=8$