作业 2

2023 年 3 月 18 日

1. M 是一个非空集合, 设 $I = \{(a,b) \mid a,b \in M\}$. 证明, M 的一个关系决定了 I 的一个子集, I 的一个子集决定了 M 的一个关系, 不同的关系决定了 I 的不同子集.

证明. 设 $I' \subseteq I$. 设 $aRb \implies (a,b) \in I'$, $a\bar{R}b \implies (a,b) \notin I'$. 那么对于任意 $a,b \in M$, 要么 aRb, 要么 $a\bar{R}b$, 因为 (a,b) 要么 $(a,b) \in I'$, 要么 $(a,b) \notin I'$. 这就是说, I' 确实定义了一个关系 R.

给定一个 I' 我们能够确定一个 R. $(a,b) \in I' \implies aRb$, $(a,b) \notin I' \implies a\bar{R}b$. 这就确定了一个关系 R, 因为 (a,b) 要么 $(a,b) \in I'$, 要么 $(a,b) \notin I'$.

设有两个关系 $R_1 \neq R_2$. 那么存在 $(a,b) \in I$, 使得 $aR_1b, a\bar{R}_2b$ 成立, 或者 $a\bar{R}_1b, aR_2b$ 成立. 那么 R_1, R_2 分别确定的 I'_1, I'_2 一定不同因为 (a,b) 不会同时属于或者不属于 I'_1, I'_2 $\square$

2. 设 $G = \{(a,b) \mid a,b \in \mathbb{R}, a \neq 0\}$, 且 $\circ$ 的定义为 $(a,b) \circ (c,d) = (ac, ad+b)$ 证明 $(G, \circ)$ 是一个群. 如果是其是群, 其是否为交换群?

证明.

$$\begin{aligned}(a,b) \circ ((c,d) \circ (e,f)) &= (a,b) \circ (ce, cf+d) \\ &= (ace, a(cf+d)+b) \\ &= (ace, acf+ad+b)\end{aligned}$$

而

$$\begin{aligned}((a,b)\circ(c,d))\circ(e,f) &= (ac, ad+b)\circ(e,f)\\ &= (ace, acf+ad+b)\end{aligned}$$

可以知道

$$((a,b)\circ(c,d))\circ(e,f) = (a,b)\circ((c,d)\circ(e,f))$$

即, $\circ$ 满足结合律, G 是半群, 只需验证其具有左幺元和左逆元. 明显, $(1,0)$ 是左幺元.

$$\big(\frac{1}{c}, -\frac{d}{c}\big)(c,d) = \big(\frac{1}{c}\cdot c, \frac{1}{c}\cdot d + (-\frac{d}{c})\big) = (1,0)$$

故 $\left(\frac{1}{c}, -\frac{d}{c}\right)$ 是 (c,d) 的左逆元, 故 G 是群. □

3. 证明群 G 中 a, a^{-1}, cac^{-1} 的阶相等.

证明. 设 a 的阶为 n, $a^n = 1$ 因为

$$\begin{aligned}(a^{-1})^n a^n &= (a^{-1})^{n-1}a^{-1}aa^{n-1}\\ &= (a^{-1})^{n-1}1a^{n-1}\\ &= \dots\\ &= 1\end{aligned}$$

故 $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$, a^{-1} 的阶为 n.

$$\begin{aligned}(ca^{-1}c^{-1})^n &= ca^{-1}c^{-1}ca^{-1}c^{-1}(ca^{-1}c^{-1})^{n-2}\\ &= c(a^{-1})^2c^{-1}(ca^{-1}c^{-1})^{n-2}\\ &= \dots\\ &= c(a^{-1})^n c^{-1}\\ &= c1c^{-1}\\ &= 1\end{aligned}$$

那么 $ca^{-1}c^{-1}$ 也是 n 阶的. □

4. 设 a 是群 G 中的一个 n 阶群元, 证明

$$a^s = a^t \iff n \mid (s-t)$$

证明. "$\Rightarrow$": $a^s = a^t$ 可以推出 $a^{s-t} = 1$, 其中 a^{s-t} 定义为 $a^s(a^t)^{-1}$. 因为 a^{-1} 也是 n 阶元, 因此 $s-t$ 大于零或者小于零的时候, 下面结论均成立: 根据阶的定义, $s-t$ 一定被 n 整除.

"$\Leftarrow$": $n \mid (s-t)$, 那么设 $s = k_1 n + c, t = k_2 n + c$, 其中 $k_1, k_2, c \in \mathbb{Z}$, 则

$$a^s = a^{k_1 n + c} = a^{k_1 n} a^c = a^c = a^{k_2 n} a^c = a^{k_2 n + c} = a^t \qquad \square$$