近世代数作业 1

cycleke

November 23, 2020

Contents

1 课后习题 1

1.1 第 3 题 1

1.2 第 4 题 1

1.3 第 5 题 2

1.4 第 6 题 2

1.5 第 7 题 3

1.6 第 9 题 3

2 思考题 4

2.1 思考题 1 4

1 课后习题

1.1 第 3 题

证. 因为 $(S,\circ)$ 是一个半群，所以 $\circ$ 符合交换律，即

$$
\begin{aligned}
&\because (a\circ b)\circ x = (a\circ b)\circ y\\
&\therefore a\circ(b\circ x) = a\circ(b\circ y)
\end{aligned}
$$

又有 a 和 b 为左消去元，那么有：

$$
\begin{aligned}
&a\circ(b\circ x) = a\circ(b\circ y)\\
\Rightarrow &b\circ x = b\circ y \text{ (消去 a)}\\
\Rightarrow &x = y \text{ (消去 b)}
\end{aligned}
$$

所以 $a\circ b$ 为左消去元。 [证毕]

1.2 第 4 题

1. 证. 首先证明 $(M,\circ)$ 是一个半群，即 $\circ$ 符合交换律。

$$
\begin{aligned}
&\forall(x_1,x_2),(y_1,y_2),(z_1,z_2)\in M,\\
&((x_1,x_2)\circ(y_1,y_2))\circ(z_1,z_2)\\
=&(x_1y_1+2x_2y_2,x_1y_2+x_2y_1)\circ(z_1,z_2)\\
=&((x_1y_1+2x_2y_2)\times z_1+2(x_1y_2+x_2y_1)\times z_2,(x_1y_1+2x_2y_2)\times z_2+(x_1y_2+x_2y_1)\times z_1)\\
=&(x_1y_1z_1+2x_1y_2z_2+2x_2y_1z_2+2x_2y_2z_1,x_1y_1z_2+x_1y_2z_1+x_2y_1z_1+2x_2y_2z_2)
\end{aligned}
$$

$$
\begin{aligned}
&(x_1,x_2)\circ((y_1,y_2)\circ(z_1,z_2))\\
=&(x_1,x_2)\circ(y_1z_1+2y_2z_2,y_1z_2+y_2z_1)\\
=&(x_1\times(y_1z_1+2y_2z_2)+2x_2\times(y_1z_2+y_2z_1),x_1\times(y_1z_2+y_2z_1)+x_2\times(y_1z_1+2y_2z_2))\\
=&(x_1y_1z_1+2x_1y_2z_2+2x_2y_1z_2+2x_2y_2z_1,x_1y_1z_2+x_1y_2z_1+x_2y_1z_1+2x_2y_2z_2)\\
\therefore&((x_1,x_2)\circ(y_1,y_2))\circ(z_1,z_2)=(x_1,x_2)\circ((y_1,y_2)\circ(z_1,z_2))
\end{aligned}
$$

再证明 $(M,\circ)$ 是一个幺半群，即存在幺元。

$$
\begin{aligned}
&\forall(x_1,x_2)\in M,\\
&(1,0)\circ(x_1,x_2)=(1\times x_1+2\times0\times x_2,1\times x_2+0\times x_1)=(x_1,x_2)
\end{aligned}
$$

$$
(x_1,x_2)\circ(1,0)=(x_1\times1+2\times x_2\times0,x_1\times0+x_2\times1)=(x_1,x_2)
$$

$\therefore (1,0)$是$(M,\circ)$的一个幺元

综上所述，$(M,\circ)$ 是一个幺半群。 [证毕]

2. 证.

$$
\begin{aligned}
&\forall (x_1,x_2),(y_1,y_2),(z_1,z_2) \in M, s.t.(x_1,x_2) \neq (0,0)\\
&\quad (x_1,x_2)\circ(y_1,y_2) = (x_1,x_2)\circ(z_1,z_2)\\
&\Rightarrow \begin{cases} x_1y_1 + 2x_2y_2 &= x_1z_1 + 2x_2z_2 \\ x_1y_2 + x_2y_1 &= x_1z_2 + x_2z_1 \end{cases} \Rightarrow \begin{cases} x_1(y_1 - z_1) + 2x_2(y_2 - z_2) = 0 & ① \\ x_2(y_1 - z_1) + x_1(y_2 - z_2) = 0 & ② \end{cases}\\
&① \times x_2 - ② \times x_1 \Rightarrow (2x_2^2 - x_1^2)(y_2 - z_2) = 0\\
&② \times 2x_2 - ① \times x_1 \Rightarrow (2x_2^2 - x_1^2)(y_1 - z_1) = 0
\end{aligned}
$$

若 $2x_2^2 - x_1^2 = 0$，则有 $x_1 = \pm\sqrt{2}x_2$，又因为 $x_1,x_2 \in Z$，所以 $x_1 = x_2 = 0$，这与 $(x_1,x_2) \neq (0,0)$ 矛盾。
所以 $2x_2^2 - x_1^2 \neq 0 \Rightarrow \begin{cases} y_2 - z_2 = 0 \\ y_1 - z_1 = 0 \end{cases} \Rightarrow \begin{cases} y_2 = z_2 \\ y_1 = z_1 \end{cases} \Rightarrow (y_1,y_2) = (z_1,z_2)$，
所以 (x_1,x_2) 为左消去元。 [证毕]

3. 证.

$$(x_1,x_2)\circ(y_1,y_2) = (x_1y_1 + 2x_2y_2, x_1y_2 + x_2y_1) = (y_1,y_2)\circ(x_1,x_2)$$

所以 $\circ$ 符合交换律。 [证毕]

1.3 第 5 题

证. 有错误。步骤 $x^{2(n-k)}x^k = x^{n-k}x^k \Rightarrow x^{2(n-k)} = x^{n-k}$ 成立的条件为 x^k 为半群 $(S,\circ)$ 的右消去元，但是没证明 x^k 为右消去元，所以有错。 [证毕]

1.4 第 6 题

证. 设有限半群 $(S,\circ), |S| = n$。
若 $\nexists a \in S, a\circ a = a$，则 $\exists 2 \leq m \leq n, a_1\circ a_1 = a_2, a_2\circ a_2 = a_3, \cdots, a_m\circ a_m = a_1$，进而有：

$$
\begin{aligned}
a_1\circ(a_1\circ a_2\circ\cdots\circ a_m) &= (a_1\circ a_1)\circ(a_2\circ\cdots\circ a_m)\\
&= a_2\circ(a_2\circ\cdots\circ a_m)\\
&\cdots
\end{aligned}
$$

$$
\begin{aligned}
&= a_m \circ a_m \\
&= a_1
\end{aligned}
$$

设 $A = a_1 \circ a_2 \circ \cdots \circ a_m$，因为 $(S, \circ)$ 为半群，所以 $A \in S$，进而有

$$
\begin{aligned}
& a_1 \circ A = a_1 \circ a_1 \circ a_2 \circ \cdots \circ a_m = a_1 \\
\Rightarrow\ & (a_1 \circ a_1) \circ A = a_1 \circ a_1 \\
\Rightarrow\ & a_2 \circ A = a_2 \\
\cdots & \\
\Rightarrow\ & a_m \circ A = a_m \\
\Rightarrow\ & a_{m-1} \circ a_m \circ A = a_{m-1} \circ a_m \circ A \\
\cdots & \\
\Rightarrow\ & a_1 \circ a_2 \circ \cdots \circ a_m \circ A = a_1 \circ a_2 \circ \cdots \circ a_m \\
\Rightarrow\ & A \circ A = A
\end{aligned}
$$

这与 $\nexists a \in S, a \circ a = a$ 矛盾，所以 $\exists a \in S, a \circ a = a$，命题得证。 [证毕]

1.5 第 7 题

证.

$$
\begin{aligned}
& \forall a, b, c \in M \\
& \quad (a * b) * c \\
& = (a \circ m \circ b) * c \\
& = (a \circ m \circ b) \circ m \circ c \\
& = a \circ m \circ (b \circ m \circ c) \\
& = a * (b * c)
\end{aligned}
$$

所以 $(M, *)$ 是一个半群。
若 $(M, *)$ 为一个幺半群，设其幺元为 e'，则有

$$\forall a \in M, a * e' = a \Rightarrow a \circ m \circ e' = a \Rightarrow m \circ e' = e$$

所以当 m 在 $(M, \circ)$ 中存在逆元素 m^{-1} 时，$(M, *, e^{-1})$ 为幺半群。 [证毕]

1.6 第 9 题

证. 对 $\forall A, B, C \in 2^S$，有

$$(A \Delta B) \Delta C = (A \bigcap B^C \bigcap C^C) \bigcup (A^C \bigcap B \bigcap C^C) \bigcup (A^C \bigcap B^C \bigcap C) = A \Delta (B \Delta C)$$

所以 $(2^S, \Delta)$ 是一个半群。
因为 $\forall A \in 2^S, A\Delta\emptyset = \emptyset\Delta A = A$，所以 $(2^S, \Delta, \emptyset)$ 为幺半群。
因为 $\forall A \in 2^S, A\Delta A = \emptyset$，所以 $A^{-1} = A$，所以 $(2^S, \Delta)$ 为群。 [证毕]

2 思考题

2.1 思考题 1

设 $Z_n = \{[0], [1], \cdots, [n-1]\}$ 是整数集合 Z 上在模 n 的同余关系之下的等价类之集合。在 Z_n 上定义乘法"$\times$"，$\forall [i], [j] \in Z_n, [i] \times [j] = [i \times j]$。
现证明 $\times$ 为 Z_n 的一个二元运算：

证.

$$\forall k \in [i], l \in [j]$$
$$[k] = [i], [l] = [j], [k] \times [l] = [i] \times [j]$$
$$[k] \times [l] = [k \times l], [i] \times [j] = [i \times j]$$

所以只需证 $[k\times l] = [i\times j]$。由于 $n|(k-i), n|(l-j)$，所以不妨设 $k = i+an, l = j + bn, a, b \in Z$。所以 $k \times l - i \times j = n(abn + aj + bi) \Rightarrow n|(k \times l - i \times j) \Rightarrow [k \times l] = [i \times j]$。 [证毕]

又因为 $\forall [i], [j], [k] \in Z_n$,

$$([i] \times [j]) \times [k] = [i \times j \times k]$$
$$[i] \times ([j] \times [k]) = [i \times j \times k]$$
$$\therefore ([i] \times [j]) \times [k] = [i] \times ([j] \times [k])$$

所以 $(Z_n, \times)$ 是一个半群。其中显然 $(Z_1, \times)$ 有一个单位元 $[0]$。
若要构造具有 $n(n \geq 2)$ 个左（或右）单位元的半群，则有如下构造方法：
设

$$S = \{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} | a, b \in Z_n\}$$

在 S 上定义乘法 $\times$，规则使用一般矩阵的乘法，不过将自然数的乘法变为 Z_n 上的乘法。不难得出 $\forall d \in Z_n, \begin{pmatrix} [1] & d \\ 0 & 0 \end{pmatrix}$ 是 $(S, \times)$ 的左单元元素。又因为 $|Z_n| = n$，所以 $(S, \times)$ 有 n 个左单元元素。

同理可以构造

$$S' = \{\left(\begin{array}{cc} a & 0 \\ b & 0 \end{array}\right) | a, b \in Z_n\}$$

$(S', \times)$ 有 n 个右单元元素。