第二讲半群、幺半群与群

陈建文

October 11, 2022

定义1. 设“$\circ$”为非空集合S上的一个二元代数运算。如果$\forall a,b,c \in S$，

$$(a \circ b) \circ c = a \circ (b \circ c)$$

则称集合S对“$\circ$”运算形成一个半群（*semigroup*），并记为$(S, \circ)$。

例. 正整数集合Z_+对“$+$”运算构成一个半群。

$\forall a,b,c \in Z_+ (a+b)+c = a+(b+c)$

定义2. 如果一个半群中的二元代数运算满足交换律，则称此半群为交换半群。

例. 设S为一切形如

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, a, b \in N$$

的2×2矩阵之集，则S对矩阵的乘法构成一个不可交换的半群。

$\forall d \in N$，2×2矩阵

$$\begin{bmatrix} 1 & d \\ 0 & 0 \end{bmatrix}$$

为左单位元素。于是，$(S, *)$有无穷多个左单位元素，然而它却没有右单位元素。

定理1. 设$(S, \circ)$为一个代数系，如果二元代数运算$\circ$既有左单位元e_l，又有右单位元e_r，则$e_l = e_r$，从而有单位元且单位元是唯一的。

定义3. 有单位元素的半群称为独异点*(monoid)*，或称为幺半群。

例. 自然数集合N对加法运算“$+$”构成幺半群，单位元为0。正整数集合Z_+对乘法运算“$\times$”构成幺半群，单位元为1。

例. 设S为任意一个非空集合，则$(2^S, \cup, \phi)$和$(2^S, \cap, S)$都为幺半群。

定义4. 如果一个幺半群中的二元代数运算满足交换律，则称此幺半群为交换幺半群。

例. 设S为非空集合，$M(S) = \{f | f : S \to S\}$，则$M(S)$对映射的合成构成了一个以$I_S$为单位元的幺半群$(M(S), \circ, I_S)$，它是不可交换幺半群。

例. 设M_n为所有$n \times n$实矩阵构成的集合，则M_n对矩阵的乘法构成了一个以I_n为单位元的幺半群$(M_n, *, I_n)$。

定义5. 设$(S, \circ, e)$为一个幺半群，$a \in S$。如果存在$a_l \in S$使得$a_l \circ a = e$，则称a_l为a的左逆元素；如果存在$a_r \in S$使得$a \circ a_r = e$，则称a_r为a的右逆元素；如果存在$b \in S$使得$b \circ a = a \circ b = e$，则称$b$为$a$的逆元素。

定理2. 如果幺半群$(S, \circ, e)$中的元素a既有左逆元素a_l，又有右逆元素a_r，则$a_l = a_r$。于是，a有逆元素且a的逆元素是唯一的，记为a^{-1}。

定义6. 每个元素都有逆元素的幺半群称为群。

定义7. 设G为一个非空集合，“$\circ$”为G上的一个二元代数运算。如果下列各个条件成立，则称G对“$\circ$”运算构成一个群（*group*）：

I. “$\circ$”运算满足结合律，即$\forall a, b, c \in G\ (a \circ b) \circ c = a \circ (b \circ c)$；

II. 对“$\circ$”运算，G中有一个单位元e，即$\forall a \in G\ e \circ a = a \circ e = a$；

III. 对G中的每个元素，关于$\circ$运算有一个逆元，即$\forall a \in G \exists b \in G b \circ a = a \circ b = e$。

例. 整数集合Z,有理数集合Q，实数集合R，复数集合C对通常的加法运算构成群；非零有理数集合Q^*，非零实数集合R^*，非零复数集合C^*对通常的乘法运算构成群。

定义8. 如果一个群中的二元代数运算满足交换律，则称此群为交换群，又称为*Abel*群。

例. 设S为一个非空集合，从S到S的所有双射构成的集合对映射的合成构成一个群，称为S上的对称群，记为$Sym(S)$。当$S = \{1, 2, \cdots, n\}$时，$Sym(S) = S_n$。

例. 设M_n为所有可逆$n \times n$实矩阵构成的集合，则M_n对矩阵的乘法构成了一个以I_n为单位元的群$(M_n, *, I_n)$。

定义9. 群$(G, \circ)$称为有限群，如果G为有限集。G的基数称为群G的阶。如果G含有无穷多个元素，则称G为无限群。

定义10. 设$a, n \in Z$，$n > 0$，$a = bn + r$，$0 \le r < n$，则称r为a除以n所得到的余数，记为$a \mod n$。

定义11. 设$a, b, n \in Z$，$n > 0$，如果$a \mod n = b \mod n$，则称a与b模n同余，记为$a \equiv b(\mod n)$。

定理3. $\forall a, b \in Z, a \equiv b(\mod n)$等价于$n|(a - b)$。

定理4. *1.* $\forall a \in Z, a \equiv a(\mod n)$；

2. $\forall a, b \in Z$，如果$a \equiv b(\mod n)$，则$b \equiv a(\mod n)$；

3. $\forall a, b, c \in Z$，如果$a \equiv b(\mod n)$并且$b \equiv c(\mod n)$，则$a \equiv c(\mod n)$；

4. $\forall a, b, k \in Z$，如果$a \equiv b(\mod n)$，则$a + k \equiv b + k(\mod n)$；

5. $\forall a, b, c, d \in Z$，如果$a \equiv b(\mod n)$并且$c \equiv d(\mod n)$，则$a + c \equiv b + d(\mod n)$；

6. $\forall a, b, k \in Z$，如果$a \equiv b(\mod n)$，则$ak \equiv bk(\mod n)$；

7. $\forall a,b,c,d \in Z$，如果$a \equiv b(\mod n)$并且$c \equiv d(\mod n)$，则$ac \equiv bd(\mod n)$

8. $\forall a,b \in Z$，$ab(\mod n) = (a \mod n)(b \mod n)(\mod n)$。

定义12. 设$n \in Z$，$n > 0$，$\forall x \in Z$，定义$[x] = \{y | y \equiv x(\mod n)\}$。

定理5. 设$n \in Z$，$n > 0$，$\forall x \in z$，$[x] = [y]$当且仅当$x \equiv y(\mod n)$。

例. 设$Z_n = \{[0],[1],\cdots,[n-1]\}$为整数集$Z$上在模$n$同余的等价关系下所有等价类之集，在$Z_n$上定义加法运算"+"如下：$\forall [i],[j] \in Z_n, [i]+[j] = [i+j]$，则$(Z_n,+)$构成一个交换群;

在Z_n上定义加法运算"$*$"如下：$\forall [i],[j] \in Z_n, [i]*[j] = [i*j]$，则$(Z_n,*)$构成一个交换幺半群;

课后作业题:

练习1. 给出一个半群，它有无穷多个右单位元素。

练习2. 设$(S,\circ)$为一个半群，$a \in S$称为左消去元素，如果$\forall x,y \in S$，有$a \circ x = a \circ y$，则一定有$x = y$。试证：如果a和b均为左消去元，则$a \circ b$也是左消去元。

练习3. 设Z为整数集合，$M = Z \times Z$。在M上定义二元运算$\circ$如下:

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

试证:

(1)M对上述定义的代数运算构成一个幺半群。

*(2)*如果$(x_1,x_2) \neq (0,0)$，则(x_1,x_2)是左消去元。

*(3)*运算"$\circ$"满足交换率。

练习4. 证明：有限半群中一定有一个元素a使得$a \circ a = a$。

练习5. 设R为实数集合，$S = \{(a,b) | a \neq 0, a,b \in R\}$。在$S$上利用通常的加法和乘法定义二元运算"$\circ$"如下:

$$(a,b) \circ (c,d) = (ac, ad+b)$$

验证$(S,\circ)$为群。

练习6. n次方程$x^n = 1$的根称为n次单位根，所有n次单位根之集记为U_n。证明：U_n对通常的复数乘法构成一个群。

练习7. 令

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

试证：G对矩阵乘法构成一个群。