第二讲半群、幺半群与群

陈建文

February 14, 2023

定义1. 代数系$(S,\circ)$称为一个半群，如果二元代数运算“$\circ$”满足结合律，即$\forall a,b,c\in S$，

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

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。

证明. $e_r=e_l\circ e_r=e_l$ □

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，$S^S=\{f|f:S\to S\}$，则S^S对映射的合成构成了一个以I_S为单位元的幺半群$(S^S,\circ,I_S)$，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}。

证明. $a_r = e \circ a_r = (a_l \circ a) \circ a_r = a_l \circ (a \circ a_r) = a_l \circ e = a_l$ □

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$\forall a \in G \exists b \in G b \circ a = a \circ b = e$。

群G中的"$\circ$"运算通常称为乘法，$a \circ b$简写为ab。a的逆元记为a^{-1}。

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，记为$|G|$。如果G含有无穷多个元素，则称G为无限群。

定义10. 设$a, b \in Z$，如果存在$q \in Z$使得$a = qb$，则称b整除a，记为$b|a$。

定义11. 设$a, b \in Z$，$b > 0$，$a = qb + r$，$q \in Z$，$0 \le r < b$，则称r为a除以b所得到的余数，记为$a \bmod b$。

定义12. 设$a, b, n \in Z$，$n > 0$，如果$a \bmod n = b \bmod n$，则称a与b模n同余，记为$a \equiv b \pmod n$。

定理3. $\forall a, b, n \in Z, n > 0, a \equiv b \pmod n$等价于$n|(a - b)$。

定理4. *1.* $\forall a \in Z, a \equiv a \pmod{n}$;

2. $\forall a, b \in Z$，如果$a \equiv b \pmod{n}$，则$b \equiv a \pmod{n}$;

3. $\forall a, b, c \in Z$，如果$a \equiv b \pmod{n}$并且$b \equiv c \pmod{n}$，则$a \equiv c \pmod{n}$;

4. $\forall a, b, k \in Z$，如果$a \equiv b \pmod{n}$，则$a + k \equiv b + k \pmod{n}$;

5. $\forall a, b, c, d \in Z$，如果$a \equiv b \pmod{n}$并且$c \equiv d \pmod{n}$，则$a + c \equiv b + d \pmod{n}$;

6. $\forall a, b, k \in Z$，如果$a \equiv b \pmod{n}$，则$ak \equiv bk \pmod{n}$;

7. $\forall a, b, c, d \in Z$，如果$a \equiv b \pmod{n}$并且$c \equiv d \pmod{n}$，则$ac \equiv bd \pmod{n}$

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

定义13. 设$n \in Z$，$n > 0$，$\forall x \in Z$，定义$[x] = \{y | y \equiv x \pmod{n}\}$，称为整数集$Z$上在模$n$同余的等价关系下的一个等价类。

例. 模4同余关系的所有等价类为：

$[0] = \{\cdots, -8, -4, 0, 4, 8, \cdots\}$

$[1] = \{\cdots, -7, -3, 1, 5, 9, \cdots\}$

$[2] = \{\cdots, -6, -2, 2, 6, 10, \cdots\}$

$[3] = \{\cdots, -5, -1, 3, 7, 11, \cdots\}$

定理5. 设$n \in Z$，$n > 0$，$\forall x, y \in Z$，$[x] = [y]$当且仅当$x \equiv y \pmod{n}$。

证明. $\Rightarrow$

$x \in [x] = [y] \Rightarrow x \equiv y (\mathrm{mod} n)$。

$\Leftarrow$

$t \in [x] \Leftrightarrow t \equiv x \pmod{n} \Leftrightarrow t \equiv y \pmod{n} \Leftrightarrow t \in [y]$。 □

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。

证明. $\forall i, j, i', j' \in Z$，如果$[i] = [i']$，$[j] = [j']$，则$[i + j] = [i' + j']$，这验证了“+”为一个运算。

$\forall i, j, k \in Z$，$([i] + [j]) + [k] = [i + j] + [k] = [(i + j) + k]$，$[i] + ([j] + [k]) = [i] + [j + k] = [i + (j + k)]$，$([i] + [j]) + [k] = [i] + ([j] + [k])$，这验证了加法运算+满足结合律。

$\forall i \in Z$，$[0] + [i] = [i] + [0] = [i]$，这验证了$[0]$为单位元。

$\forall i \in Z$，$[n - i] + [i] = [i] + [n - i] = [n] = [0]$，这说明$[i]$有逆元。

以上验证了Z_n对于加法运算“+”构成一个群。 □

例. 设$Z'_n = \{0, 1, 2, \cdots, n-1\}$，在$Z'_n$上定义运算”$\oplus$”如下：$i \oplus j = (i + j) \bmod n$，则$(Z'_n, \oplus)$构成一个群。

证明. $\forall a, b, c \in Z'_n, (a \oplus b) \oplus c = a \oplus (b \oplus c)$

$((a + b) \bmod n + c) \bmod n = (a + (b + c) \bmod n) \bmod n$

$((a + b) \bmod n + c) \bmod n = (a + b + c) \bmod n$

$(a + (b + c) \bmod n) \bmod n = (a + b + c) \bmod n$

$0 \oplus a = (0 + a) \bmod n = a$

如果$a \neq 0$，则$(n - a) \oplus a = (n - a + a) \bmod n = 0$；$0 \oplus 0 = (0 + 0) \bmod n = 0$。 □

设用n个二进制位表示一个整数x，x的补码定义为

如果$x \geq 0$，则x的补码为x的原码；

如果$x < 0$，则x的补码为$x + 2^n$的原码。

例：设用8个二进制位表示一个整数，计算7和-7的补码。

解：

因为$7 \geq 0$，因此7的补码为7的原码，即7的补码为00000111。

因为$-7 < 0$，因此-7的补码为$-7 + 2^8$的原码，即-7的补码为11111001。

-7的补码还可以这样求解：先计算7的原码，得到00000111，然后取反加1，得到-7的补码为11111001。

例：设用8个二进制位表示一个整数，计算-128的补码。

解：因为$-128 < 0$，因此-128的补码为$-128 + 2^8$的原码，即-128的补码为10000000。同样的，-128的补码还可以这样求解：先计算128的原码，得到10000000，然后取反加1，得到-128的补码为10000000。

如果用n个二进制位表示一个整数，用补码表示的数字的范围为$-2^{n-1} \sim 2^{n-1} - 1$。对于补码而言，如果首位为0，其表示的是大于等于0的整数，如果首位为1，其表示的是负数。

例：如果用8个二进制位表示一个整数，00001010为哪个整数的补码？10001010为哪个整数的补码?

解：因为00001010的首位为0，它为一个大于等于0的整数的补码，这个整数为10。因为10001010的首位为1，它为一个负数的补码，这个负数为$138 - 2^8 = -118$。

计算机中普遍采用补码表示数字的原因是对于负数的加法可以采用与自然数的加法一样的加法器。下面简略介绍其思想。

设x和y为任意的两个整数，分以下4种情况讨论：

$x \geq 0$，$y \geq 0$：此时x的补码为x的原码，y的补码为y的原码，按照自然数相加计算得到$x + y$，恰为$x + y$的补码。

$x < 0$，$y \geq 0$：此时x的补码为$x + 2^n$的原码，y的补码为y的原码，按照自然数相加计算得到$x + 2^n + y = (x + y) + 2^n$。如果$x + y < 0$，则得到的恰为$x + y$的补码；如果$x + y \geq 0$,计算结果的第$n$位（从最右边数起，依次为第0位，第1位，$\cdots$，第$n-1$位，第$n$位）会自动抛掉。

$x \geq 0$，$y < 0$：此时x的补码为x的原码，y的补码为$y + 2^n$的原码，按照自然数相加计算得到$x + (y + 2^n) = (x + y) + 2^n$。如果$x + y < 0$，则得到的恰为$x + y$的补码；如果$x + y \geq 0$,计算结果的第$n$位会自动抛掉。

$x < 0$，$y < 0$：此时x的补码为$x + 2^n$的原码，y的补码为$y + 2^n$的原码，按照自然数相加计算得到$(x + 2^n) + (y + 2^n) = (x + y) + 2^n + 2^n$，计算结果的第$n$位会自动抛掉，于是最终得到的计算结果为$(x + y) + 2^n$，恰为$x + y$的补码。

定义14. 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中有一个左单位元e，即$\forall a \in G\ e \circ a = a$；

III. $\forall a \in G \exists b \in G b \circ a = e$，其中$e$为*II*中的同一个左单位元素。

在群$(G, \circ)$中，$\forall a, b \in G, a \circ b$简写为$ab$。

定理6. 设G为一个群，则$\forall a, b \in G$，如果$ba = e$，则$ab = e$。

证明. 在
$$ba = e$$
的两边同时右乘以b得
$$(ba)b = eb$$
从而
$$b(ab) = b$$
在G中存在c使得$cb = e$，于是
$$c(b(ab)) = cb$$
所以
$$ab = e$$
□

定理7. 设G为一个群，则G的左单位元e也是右单位元。

证明. $\forall a \in G$，设$b \in G$，$ba = e$，则$ae = a(ba) = (ab)a = ea = a$，所以$e$也是右单位元。 □

定理8. 设a与b为群G的任意两个元素，则$(a^{-1})^{-1} = a$，$(ab)^{-1} = b^{-1}a^{-1}$。

证明. 由
$$aa^{-1} = e$$
得
$$(a^{-1})^{-1} = a$$
由
$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = e$$
得
$$(ab)^{-1} = b^{-1}a^{-1}$$
□

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。

解. 设S为一切形如
$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, a, b \in N$$
的2×2矩阵之集，则S对矩阵的乘法构成一个半群。

$\forall d \in N$，2×2矩阵
$$\begin{bmatrix} 1 & 0 \\ d & 0 \end{bmatrix}$$
为右单位元素。于是，$(S, *)$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。

证明. 如果$\forall x,y\in S$，$(a\circ b)\circ x=(a\circ b)\circ y$，由结合律知$a\circ(b\circ x)=a\circ(b\circ y)$，由$a$为左消去元知$b\circ x=b\circ y$，由$b$为左消去元知$x=y$，这证明了$a\circ b$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。

证明. (1)$\forall(x_1,x_2),(y_1,y_2),(z_1,z_2)\in M$，

$$\begin{aligned}
&((x_1,x_2)\circ(y_1,y_2))\circ(z_1,z_2)=(x_1y_1+2x_2y_2,x_1y_2+x_2y_1)\circ(z_1,z_2)\\
=&(x_1y_1z_1+2x_2y_2z_1+2x_1y_2z_2+2x_2y_1z_2,x_1y_1z_2+2x_2y_2z_2+x_1y_2z_1+x_2y_1z_1)\\
&(x_1,x_2)\circ((y_1,y_2)\circ(z_1,z_2))=(x_1,x_2)\circ(y_1z_1+2y_2z_2,y_1z_2+y_2z_1)\\
=&(x_1y_1z_1+2x_1y_2z_2+2x_2y_1z_2+2x_2y_2z_1,x_1y_1z_2+x_1y_2z_1+x_2y_1z_1+2x_2y_2z_2)\\
&((x_1,x_2)\circ(y_1,y_2))\circ(z_1,z_2)=(x_1,x_2)\circ((y_1,y_2)\circ(z_1,z_2))
\end{aligned}$$

这验证了"$\circ$"运算满足结合律。

$$\forall(x,y)\in M,(1,0)\circ(x,y)=(x,y)\circ(1,0)=(x,y)$$

这验证了$(1,0)$为"$\circ$"运算的单位元。

于是，M对"$\circ$"运算构成一个幺半群。

(2) $\forall(y_1,y_2),(z_1,z_2)\in M$，如果$(x_1,x_2)\circ(y_1,y_2)=(x_1,x_2)\circ(z_1,z_2)$，则$(x_1y_1+2x_2y_2,x_1y_2+x_2y_1)=(x_1z_1+2x_2z_2,x_1z_2+x_2z_1)$，

当$(x_1,x_2)\neq 0$时，以下证明关于y_1和y_2的线性方程组

$$\begin{cases}x_1y_1+2x_2y_2=x_1z_1+2x_2z_2\\x_1y_2+x_2y_1=x_1z_2+x_2z_1\end{cases}$$

即

$$\begin{cases}x_1y_1+2x_2y_2=x_1z_1+2x_2z_2\\x_2y_1+x_1y_2=x_2z_1+x_1z_2\end{cases}$$

有唯一解$y_1=z_1,y_2=z_2$，因此(x_1,x_2)是左消去元。

以上线性方程组系数矩阵的行列式

$$\begin{vmatrix}x_1&2x_2\\x_2&x_1\end{vmatrix}=x_1^2-2x_2^2\neq 0$$

这是因为如果$x_1^2-2x_2^2=0$，则$x_1^2=2x_2^2$，此时如果$x_2=0$，则$x_1=0$，与$(x_1,x_2)\neq 0$矛盾；如果$x_2\neq 0$，则$(\frac{x_1}{x_2})^2=2$，与x_1和x_2都为整数矛盾。

(3)$\forall (x_1, x_2), (y_1, y_2) \in M$,

$$\begin{aligned}
(x_1, x_2) \circ (y_1, y_2) &= (x_1 y_1 + 2x_2 y_2, x_1 y_2 + x_2 y_1) \\
(y_1, y_2) \circ (x_1, x_2) &= (y_1 x_1 + 2y_2 x_2, y_1 x_2 + x_1 y_2) \\
(x_1, x_2) \circ (y_1, y_2) &= (y_1, y_2) \circ (x_1, x_2)
\end{aligned}$$

这证明了“$\circ$”运算满足交换律。 □

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

证明. 设$(S, \circ)$为有限半群，$x \in S$。由S为有限半群知，存在正整数i和j，使得$x^i = x^j$。不妨设$j > i$。$\forall m \in Z^+$，如果$m \geq j$，则$x^m = x^{m-j}x^j = x^{m-j}x^i = x^{m-(j-i)}$。取正整数$n$，使得$(n+1)(j-i) \geq j$，则$x^{2n(j-i)} = x^{n(j-i)}$，于是$(x^{n(j-i)})^2 = x^{n(j-i)}$。 □

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。

证明. $\forall (a, b), (c, d), (e, f) \in S$,

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

这验证了“$\circ$”运算满足结合律。

$\forall (c, d) \in S, (1, 0) \circ (c, d) = (1 \cdot c, 1 \cdot d + 0) = (c, d)$，这验证了$(1, 0)$为$\circ$运算的左单位元。

$\forall (c, d) \in S, (1/c, -d/c) \circ (c, d) = (1, 0)$,这验证了$(1/c, -d/c)$为$(c, d)$关于左单位元$(1, 0)$的左逆元。 □

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。

证明. 对任意的$x_1 \in U_n$，$x_2 \in U_n$，则$x_1^n = 1$，$x_2^n = 1$，从而$(x_1 x_2)^n = 1$，即$x_1 x_2 \in U_n$。

结合律显然成立。

$1^n = 1$，从而$1 \in U_n$。$\forall x \in U_n, 1 \cdot x = x$，这说明1为左单位元。

$\forall x \in U_n$，则$x^n = 1$，从而$(\frac{1}{x})^n = 1$，即$\frac{1}{x} \in U_n$。$\frac{1}{x} \cdot x = 1$说明$\frac{1}{x}$为x关于左单位元1的左逆元。

以上验证了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。

证明. 易验证G对矩阵的乘法满足封闭性。

结合律显然成立。

$\begin{bmatrix}1&0\\0&1\end{bmatrix}$为左单位元。

$\begin{bmatrix}1&0\\0&1\end{bmatrix}$的左逆元为$\begin{bmatrix}1&0\\0&1\end{bmatrix}$，$\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$的左逆元为$\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$，$\begin{bmatrix}1&0\\0&-1\end{bmatrix}$的左逆元为$\begin{bmatrix}1&0\\0&-1\end{bmatrix}$，$\begin{bmatrix}-1&0\\0&1\end{bmatrix}$的左逆元为$\begin{bmatrix}-1&0\\0&1\end{bmatrix}$。

以上验证了G对矩阵的乘法构成一个群。

□