

## 第二讲半群、么半群与群

陈建文

October 14, 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 $2 \times 2$ 矩阵之集，则 $S$ 对矩阵的乘法构成一个不可交换的半群。

$\forall d \in N$ ,  $2 \times 2$ 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*)，或称为么半群。

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

**例.** 设 $S$ 为任意一个集合，则 $(2^S, \cup, \phi)$ 和 $(2^S, \cap, S)$ 都为么半群。

**定义4.** 如果一个么半群中的二元代数运算满足交换律，则称此么半群为交换么半群。

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

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

**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 $S = \{1, 2, \dots, n\}$ 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 $a, b \in Z$ ,  $b > 0$ ,  $a = qb + r$ ,  $q \in Z$ ,  $0 \leq r < b$ , 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 $a \equiv b \pmod{n}$ 。

**定义13.**

**定理3.**  $\forall a, b \in Z, a \equiv b \pmod{n}$ 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.  $\forall a, b \in Z, ab \pmod{n} = (a \pmod{n})(b \pmod{n}) \pmod{n}$ 。

**定义14.** 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。

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

**例.** 设  $Z_n = \{[0], [1], \dots, [n-1]\}$  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  $Z_n$  上定义乘法运算 “\*” 如下:  $\forall [i], [j] \in Z_n, [i] * [j] = [i * j]$ , 则  $(Z_n, *)$  构成一个交换幺半群;

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,  $\dots$ , 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15.** 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. 对 $G$ 中的每个元素, 关于 $\circ$ 运算有一个左逆元, 即 $\forall a \in G \exists b \in G b \circ a = e$ , 其中 $e$ 为II中的同一个左单位元素。

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

**定理6.** 设 $G$ 为一个群, 则 $\forall a \in G$ ,  $a$ 的左逆元也是 $a$ 的右逆元。

证明.  $\forall a \in G$ , 设 $a_l$ 为 $a$ 的一个左逆元, 则

$$a_l a = e$$

两边同时右乘以 $a_l$ 得

$$(a_l a) a_l = e a_l$$

从而

$$a_l (a a_l) = a_l$$

两边同时左乘以 $a_l$ 的左逆元得

$$a a_l = e$$

□

**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 $a_l$ 为 $a$ 的左逆元, 则 $a e = a(a_l a) = (a a_l) a = e a = a$ , 所以 $e$ 也是右单位元。 □

在群 $(G, \circ)$ 中,  $a$ 得逆元记为 $a^{-1}$ 。

**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。

**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。