第十讲近世代数基本概念

陈建文

December 23, 2024

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。

定义3. 设$(S,\circ)$为一个半群，$B\subseteq S$，如果B对S中的“$\circ$”运算也构成一个半群，则称B为S的一个子半群。

定义4. 如果一个半群只包含有限个元素，则称之为有限半群。

定义5. 设$(S,\circ)$为一个代数系。如果存在一个元素$e_l\in S$，使得$\forall a\in S$，

$$e_l\circ a=a$$

则称e_l为“$\circ$”运算的左单位元素；如果存在一个元素$e_r\in S$，使得$\forall a\in S$，

$$a\circ e_r=a$$

则称e_r为“$\circ$”运算的右单位元素；如果存在一个元素$e\in S$，使得$\forall a\in S$，

$$e\circ a=a\circ e=a$$

则称e为“$\circ$”运算的单位元素。

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6. 有单位元素的半群称为幺半群。

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7. 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。

定义8. 如果一个幺半群只包含有限个元素，则称之为有限幺半群。

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$(S^S, \circ, I_S)$，它是不可交换的幺半群。

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9. 设$(M, \circ, e)$为一个幺半群，$P \subseteq M$。如果$e \in P$且P为M的子半群，则称P为M的子幺半群。

定义10. 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11. 每个元素都有逆元素的幺半群称为群。

定义12. 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13. 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，$Sym(S) = S_n$。

定义14. 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15. 设$(G, \circ)$为一个群，$S \subseteq G$，如果S对G中的“$\circ$”运算也构成一个群，则称S为G的一个子群。

定义16. 设R为一个非空集合，R中有两个代数运算，一个叫做加法并用“$+$”表示，另一个叫做乘法并用“$\circ$”表示，如果

（*1*）$(R,+,0)$为一个*Abel*群：

I.$\forall a,b,c\in R(a\circ b)\circ c=a\circ(b\circ c)$；

II.$\forall a\in R0+a=a+0=a$；

III.$\forall a\in R\exists b\in Rb+a=a+b=0$，$a$的逆元记为$-a$；

IIII.$\forall a,b\in Ra+b=b+a$。

（*2*）$(R,\circ)$为一个半群：$\forall a,b,c\in R(a\circ b)\circ c=a\circ(b\circ c)$

（*3*）乘法对加法满足左、右分配律：$\forall a,b,c\in R$

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

则称代数系$(R,+,\circ,0)$为一个环（*ring*）。

在环R中，$a\circ b$简写为ab。

例. 整数集合Z对通常数的加法和乘法构成一个环$(Z,+,\cdot,0)$，称为整数环。

定义17. 设$(R,+,\circ,0)$为一个环，$S\subseteq R$，如果S对R的加法和乘法也构成一个环，则称S为R的一个子环。

定义18. 一个环称为一个体，如果它满足以下两个条件：

（*1*）它至少含有一个非零元素；

（*2*）非零元素的全体对乘法构成一个群。

定义19. 如果一个体中的乘法满足交换律，则称之为域。

定义20. 有理数集Q、实数集R、复数集C对通常的乘法和加法都构成域。

定义21. 设$(F,+,\circ,0,1)$为一个体（域），$E\subseteq F$，如果E对F的加法和乘法也构成一个体（域），则称E为F的一个子体（域）。

定义22. 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23. 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24. 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. $\forall a,b\in Z,(a+b) \bmod n=(a \bmod n+b \bmod n) \bmod n$；

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

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

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

定义25. 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$x \equiv y \pmod{n}$。

定义26. 设$\cong$为代数系$(X, \circ)$上的等价关系。$\forall a, a', b, b' \in X$，如果$a \cong a'$且$b \cong b'$，则必有$a \circ b \cong a' \circ b'$，则称$\cong$为$X$上的同余关系。常用$\equiv$表示同余关系。

定理6. $\cong$为代数系$(X, \circ)$上的同余关系，等价于$\forall a, a', b \in X$，如果$a \cong a'$，则必有$a \circ b \cong a' \circ b$且$\forall a, b, b' \in x$，如果$b \cong b'$，则$a \circ b \cong a \circ b'$。

定理7. 设$\cong$为代数系$(X, \circ)$上的一个等价关系。$\forall [a], [b] \in X/\cong$，定义$[a] \cdot [b] = [a \circ b]$，则$\cdot$为$X/\cong$上的二元代数运算当且仅当$\cong$为同余关系。

证明. 设“$\cdot$”为$X/\cong$上的等价关系。$\forall a, a', b, b' \in X$，如果$a \cong a'$且$b \cong b'$，则$[a] = [a']$，$[b] = [b']$，于是$[a] \cdot [b] = [a'] \cdot [b']$，$[a \circ b] = [a' \circ b']$，于是$a \circ b \cong a' \circ b'$，从而$\cong$为代数系$(X, \circ)$上的同余关系。

设$\cong$是代数系$(X, \circ)$的同余关系，则$\forall a, a', b, b' \in X$，如果$[a] = [a']$，$[b] = [b']$，则$a \cong a'$，$b \cong b'$，从而$a \circ b \cong a' \circ b'$，故$[a \circ b] = [a' \circ b']$，即“$\cdot$”的定义与运算对象$[a]$与$[b]$的表示形式无关，从而是代数运算。 □

定义27. 设$(S, \circ)$，$(S', *)$为两个半群。如果存在一个双射$\phi : S \to S'$，使得$\forall a, b \in S$，

$$\phi(a \circ b) = \phi(a) * \phi(b),$$

则称半群S与S'同构，记为$S \cong S'$。ϕ称为从S到S'的一个同构。

定义28. 设$(M, \circ, e)$，$(M', *, e')$为两个幺半群。如果存在一个双射$\phi : M \to M'$，使得$\forall a, b \in M$，

$$\phi(a \circ b) = \phi(a) * \phi(b),$$

则称幺半群M与M'同构，记为$M \cong M'$。ϕ称为从M到M'的一个同构。

定理8. 设ϕ是从幺半群$(M, \circ, e)$到$(M', *, e')$的同构，则$\phi(e) = e'$。

定义29. 设$(S, \circ)$，$(S', *)$为两个半群。如果存在一个映射$\phi : S \to S'$，使得$\forall a, b \in S$，

$$\phi(a \circ b) = \phi(a) * \phi(b),$$

则称半群S与S'同态。ϕ称为从S到S'的一个同态。如果ϕ为单射，则称ϕ为从S到S'的单同态；如果ϕ为满射，则称ϕ为从S到S'的满同态。

定义30. 设$(M,\circ,e)$，$(M',*,e')$为两个幺半群。如果存在一个映射$\phi: M \to M'$，使得$\phi(e)=e'$，$\forall a,b\in M$，

$$\phi(a\circ b)=\phi(a)*\phi(b),$$

则称幺半群M与M'同态。ϕ称为从M到M'的一个同态。如果ϕ为单射，则称ϕ为从M到M'的单同态；如果ϕ为满射，则称ϕ为从M到M'的满同态。

例. 设$(Z,\cdot,1)$为整数的乘法幺半群。令$\phi: Z\to Z$，$\forall z\in Z, \phi(z)=0$，则$\phi$不是从$Z$到$Z$的同态，因为$\phi(1)=0\neq 1$。

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$(Z'_n,\oplus)$构成一个幺半群。

证明. $\forall a,b,c\in Z'_n, (a\oplus b)\oplus c = a\oplus(b\oplus c)$
即：$((a+b) \bmod n + c) \bmod n = (a+(b+c) \bmod n) \bmod n$
这是因为$((a+b) \bmod n + c) \bmod n = (a+b+c) \bmod n$，
并且$(a+(b+c) \bmod n) \bmod n = (a+b+c) \bmod n$。
$0\oplus a = (0+a) \bmod n = a$

□

令$f: Z\to Z'_n$，$\forall x\in Z, f(x)=x \bmod n$，则$f$为从$(Z,+)$到$(Z'_n,\oplus)$的同态，这是因为$\forall a,b\in Z, f(a+b)=(a+b) \bmod n, f(a)\oplus f(b)=(a \bmod n)\oplus(b \bmod n)=((a \bmod n)+(b \bmod n)) \bmod n$，$f(a+b)=f(a)\oplus f(b)$。

定理9 (幺半群的同态基本定理)**.** 设ϕ为幺半群$(M,\circ,e)$到幺半群$(M',*,e')$的同态，则

1. 同态像$\phi(M)$为M'的一个子幺半群。

2. 由ϕ确定的等价关系E_ϕ($\forall x,y\in M, xE_\phi y$当且仅当$\phi(x)=\phi(y)$)为同余关系，$\forall [a],[b]\in M/E_\phi$，$[a]\cdot[b]=[a\circ b]$为$M/E_\phi$上的二元代数运算，$(M/E_\phi,\cdot,[e])$为幺半群。

3. 存在唯一的M/E_ϕ到M'的单同态$\bar{\phi}$使得$\phi=\bar{\phi}\circ\gamma$，其中$\gamma$为从$M$到$M/E_\phi$的映射，$\forall x\in M$，$\gamma(x)=[x]$。$\gamma$为从$M$到$M/E_\phi$的同态，称为从$M$到$M/E_\phi$的自然同态。

4. $M/E_\phi\cong\phi(M)$。

证明. 1.由于ϕ为幺半群同态，所以$\phi(e)=e'$，故$e'\in\phi(M)$。其次，$\forall t_1,t_2\in\phi(M)$，$\exists s_1,s_2\in M$使得$\phi(s_1)=t_1,\phi(s_2)=t_2$，故$t_1*t_2=\phi(s_1)*\phi(s_2)=\phi(s_1\circ s_2)\in\phi(M)$，故$(\phi(M),*,e')$为$M'$的子幺半群。

3. 首先证明γ为从M到M/E_ϕ的同态，即要证（1）$\gamma(e)=[e]$为M/E_ϕ的单位元；（2）$\forall x,y\in M, \gamma(x\circ y)=\gamma(x)*\gamma(y)$。（1）显然成立。（2）即要证$\forall x,y\in M, [x\circ y]=[x]\cdot[y]$，这也是显然成立的。如果同态$\bar{\phi}$满足$\phi=\bar{\phi}\circ\gamma$，则必有$\forall x\in M, \bar{\phi}\circ\gamma(x)=\phi(x)$，即$\bar{\phi}([x])=\phi(x)$。定义$\bar{\phi}: M/E_\phi\to M'$，$\forall [x]\in M/E_\phi, \bar{\phi}([x])=\phi(x)$，则$\bar{\phi}$为从$M/E_\phi$到$M'$的同态，这是因为$\bar{\phi}([x]\cdot[y])=\bar{\phi}([x\circ y])=\phi(x\circ y)=\phi(x)*\phi(y)=\bar{\phi}([x])*\bar{\phi}([y])$。$\bar{\phi}$为从$M/E_\phi$到$M'$的单射，这是因为$\forall x,y\in M$，如果$\bar{\phi}([x])=\bar{\phi}([y])$，则$\phi(x)=\phi(y)$，从而$xE_\phi y$，故$[x]=[y]$。这证明了$\bar{\phi}$为从$M/E_\phi$到$M'$的单同态。显然这样的单同态是唯一的。

4.$\bar{\phi}$为从M/E_ϕ到$\phi(M)$的满射，所以为同构。 □

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。