

代数系统与数论

代数系统与数论知识广泛应用于有限状态机、开关线路的计数、数据纠错、信息安全等领域。例如,在计算机和数据通信中,经常需要传递二进制数字信号,这种传递的距离一般很远,所以难免会出现错误。通常采用纠错码避免这种错误的发生,而构造纠错码的数学基础就是代数系统,设计纠错码中的一致校验矩阵需要用到代数系统中群的概念。另外,在群码的校正中要用到代数系统中的陪集。本章讲述代数系统的概念、性质、特异元素,并介绍重要而特殊的代数系统——群及其陪集,最后介绍数论基本知识及其在密码学中的应用。



5.1 代数系统的概念

由非空集合和该集合上的一个或多个运算组合的系统称为代数系统。在计算机科学中,常用代数系统描述可计算函数,研究运算的复杂性,分析程序设计语言的语义等。首先考察非空集合上的 n 元运算。

定义 5.1(n 元运算) 设 A 和 B 都是非空集合, n 是一个正整数,若 Φ 是 A^n 到 B 的一个映射,则称 Φ 是 A 到 B 的一个 n 元运算。当 $B=A$ 时,称 Φ 是 A 上的 n 元运算,简称 A 上的运算,并称该 n 元运算在 A 上是封闭的。

通常用 $\circ$ 、 $\cdot$ 、 $*$ 等运算符表示 n 元运算。例如, n 元运算 $f(a_1, a_2, \dots, a_n) = b$ 可简记为 $\circ(a_1, a_2, \dots, a_n) = b$, $n=1$ 时 $\circ(a_1) = b$ 是一元运算, $n=2$ 时 $\circ(a_1, a_2) = b$ 是二元运算;若 $f: s \times s \rightarrow s$ 是集合 S 上的二元运算,对任意 $x, y \in S$,如果 x 与 y 运算的结果是 z ,即 $f(x, y) = z$,该运算 $\circ$ 简记为 $x \circ y = z$ 。以下所涉及的 n 元运算主要是一元运算和二元运算。

例 5.1 以下是一元运算和二元运算的示例:

- (1) 求一个数的倒数是非零实数集 $\mathbf{R}^*$ 上的一元运算。
- (2) 有理数集 $\mathbf{Q}$ 上每一个数 a 映射成它的整数部分 $[a]$,或者将 $\mathbf{Q}$ 上的每一个数 a 映射成它的相反数 $-a$,这两个映射都是集合 $\mathbf{Q}$ 上的一元运算。
- (3) 在有理数集 $\mathbf{Q}$ 上,对任意两个数所进行的普通加法和乘法都是集合 $\mathbf{Q}$ 上的二元运算。
- (4) 非零实数集 $\mathbf{R}^*$ 上的乘法和除法都是 $\mathbf{R}^*$ 上的二元运算,而加法和减法不是。
- (5) S 是一个非空集合, S^S 是 S 到 S 上的所有函数的集合,则复合运算 $\circ$ 是

S^S 上的二元运算。

(6) 设 $M_n(\mathbf{R})$ 表示所有 n 阶 ($n \geq 2$) 实矩阵的集合, 即

$$M_n(\mathbf{R}) = \left\{ \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \mid a_{ij} \in \mathbf{R}, i, j = 1, 2, \dots, n \right\}$$

则矩阵加法和矩阵乘法都是 $M_n(\mathbf{R})$ 上的二元运算。

以上示例有一个共同的特征, 那就是其运算的结果都是落在原来的集合中, 称这种运算具有封闭性; 相反, 没有这种特征的运算就是不封闭的。例如, 设 $\mathbf{N}$ 是自然数集, $\mathbf{Z}$ 是整数集, 普通的减法是 $\mathbf{N} \times \mathbf{N}$ 到 $\mathbf{Z}$ 的运算, 但因为两个自然数相减可以不是自然数, 所以减法运算不是自然数集 $\mathbf{N}$ 上的闭运算。

若集合 $X = \{x_1, x_2, \dots, x_n\}$ 是有限集, X 上的一元运算和二元运算也可用运算表的形式给出。表 5.1 和表 5.2 分别是一元运算表和二元运算表。

表 5.1 一元运算表

S_i	$\circ(S_i)$
S_1	$\circ(S_1)$
S_2	$\circ(S_2)$
$\vdots$	$\vdots$
S_n	$\circ(S_n)$

表 5.2 二元运算表

$\circ$	S_1	S_2	$\cdots$	S_n
S_1	$S_1 \circ S_1$	$S_1 \circ S_2$	$\cdots$	$S_1 \circ S_n$
S_2	$S_2 \circ S_1$	$S_2 \circ S_2$	$\cdots$	$S_2 \circ S_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_n	$S_n \circ S_1$	$S_n \circ S_2$	$\cdots$	$S_n \circ S_n$

例 5.2 设集合 $B = \{0, 1\}$, 给出 B 的幂集 $P(B)$ 上求补运算 $\sim$ 和求对称差运算 $\oplus$ 的运算表, 其中全集是 B 。

解: 所求运算表如表 5.3 和表 5.4 所示。

表 5.3 求补运算表

S_i	$\sim S_i$
$\emptyset$	$\{0, 1\}$
$\{0\}$	$\{1\}$
$\{1\}$	$\{0\}$
$\{0, 1\}$	$\emptyset$

表 5.4 求对称差运算表

$\oplus$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0, 1\}$
$\emptyset$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0, 1\}$
$\{0\}$	$\{0\}$	$\emptyset$	$\{0, 1\}$	$\{1\}$
$\{1\}$	$\{1\}$	$\{0, 1\}$	$\emptyset$	$\{0\}$
$\{0, 1\}$	$\{0, 1\}$	$\{1\}$	$\{0\}$	$\emptyset$

定义 5.2(代数系统) 一个非空集合 A 连同若干个定义在该集合上的运算 $f_1, f_2, \dots, f_k$ 所组成的系统称为一个代数系统, 记为 $\langle A, f_1, f_2, \dots, f_k \rangle$ 。对给定的集合, 可以任意地在这个集合上规定运算, 使它成为代数系统。

例 5.3 由集合 B 的幂集 $P(B)$ 以及该幂集上的运算 $\cup, \cap, \sim$ 组成一个代数系统 $\langle P(B), \cup, \cap, \sim \rangle$, $B_1 \in P(B)$, B_1 的补集 $\sim B_1 = B - B_1$, 也常记为 $\bar{B}_1$ 。又如整数集 $\mathbf{Z}$ 以及 $\mathbf{Z}$ 上的普通加法运算组成一个代数系统 $\langle \mathbf{Z}, + \rangle$ 。

5.2 代数系统的运算及其性质

本节主要讨论一般二元运算的某些性质。

定义 5.3(交换律) 设 $*$ 是定义在集合 S 上的二元运算。如果对于任意的 $x, y \in S$, 都有 $x * y = y * x$, 则称二元运算 $*$ 是可交换的或满足交换律。

例 5.4 设 $\mathbf{Z}$ 是整数集, $\triangle, \star$ 分别是 $\mathbf{Z}$ 上的二元运算。其定义为: 对任意的 $a, b \in \mathbf{Z}$, $a \triangle b = ab - a - b$, $a \star b = ab - a + b$, $\mathbf{Z}$ 上的运算 $\triangle, \star$ 是否满足交换律?

解: 因为对 $\mathbf{Z}$ 中任意元素 a 和 b , $a \triangle b = ab - a - b = ba - b - a = b \triangle a$ 成立, 所以运算 $\triangle$ 满足交换律。

又因为对 $\mathbf{Z}$ 中的数 0 和 1, $0 \star 1 = 0 \times 1 - 0 + 1 = 1$, $1 \star 0 = 1 \times 0 - 1 + 0 = -1$, 所以, $0 \star 1 \neq 1 \star 0$, 从而运算 $\star$ 不满足交换律。

定义 5.4(结合律) 设 $*$ 是定义在集合 S 上的二元运算。如果对于 S 上的任意元素 x, y, z 都有 $(x * y) * z = x * (y * z)$, 则称二元运算 $*$ 是可结合的或满足结合律。

例 5.5 设 $\mathbf{Q}$ 是有理数集合, $\circ, *$ 分别是 $\mathbf{Q}$ 上的二元运算。其定义为: 对于任意的 $a, b \in \mathbf{Q}$, $a \circ b = a$, $a * b = a - 2b$, 证明运算 $\circ$ 满足结合律, 并举例说明运算 $*$ 不满足结合律。

解: 因为对任意的 $a, b, c \in \mathbf{Q}$ 都有

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

所以 $(a \circ b) \circ c = a \circ (b \circ c)$, 即运算 $\circ$ 满足结合律。

又因为对 $\mathbf{Q}$ 中的数 0 和 1 有

$$(0 * 0) * 1 = 0 * 1 = 0 - 2 = -2,$$

$$0 * (0 * 1) = 0 * (-2) = 0 - 2 \times (-2) = 4$$

所以 $(0 * 0) * 1 \neq 0 * (0 * 1)$, 从而运算 $*$ 不满足结合律。

说明: 在一个只满足结合律的二元运算表达式中, 可以去掉标记运算顺序的括号。例如, 实数集上的加法运算是可结合的, 所以表达式 $(x + y) + (u + v)$ 可简写为 $x + y + u + v$ 。

说明: 若 $\langle S, \circ \rangle$ 是代数系统, 其中 $\circ$ 是 S 上的二元运算且满足结合律, n 是正整数, $a \in S$, 那么, $a \circ a \circ a \cdots \circ a$ 是 S 中的一个元素, 称其为 a 的 n 次幂, 记为 a^n 。关于 a 的幂, 用数学归纳法不难证明以下公式:

$$a^m \circ a^n = a^{m+n}, (a^m)^n = a^{mn}$$

其中 m, n 为正整数。

定义 5.5(幂等律) 设 $*$ 是集合 S 上的二元运算。如果对于任意的 $x \in S$, 都有 $x * x = x$, 则称运算 $*$ 是幂等的或满足幂等律。

例 5.6 设 $\mathbf{Z}$ 是整数集, 在 $\mathbf{Z}$ 上定义两个二元运算 $\circ$ 和 $*$, 对于任意 $x, y \in \mathbf{Z}$, $x \circ y = \max(x, y)$, $x * y = \min(x, y)$, 验证运算 $\circ$ 和 $*$ 都是幂等的。

解: 对于任意的 $x \in \mathbf{Z}$, 有

$$x \circ x = \max(x, x) = x, x * x = \min(x, x) = x$$

因此运算 $\circ$ 和运算 $*$ 都是幂等的。

例 5.7 $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ 分别为整数集、有理数集、实数集; $\mathbf{M}_n(\mathbf{R})$ 为 n 阶实矩阵集合, $n \geq 2$; $P(B)$ 为幂集; A^A 为从 A 到 A 的函数, $|A| \geq 2$ 。这些集合上的相关运算是否满足交换律、

结合律、幂等律?

解: 以上集合上的相关运算的性质如表 5.5 所示。

表 5.5 例 5.7 集合上的相关运算的性质

集合	运算	交换律	结合律	幂等律
$\mathbf{Z}, \mathbf{Q}, \mathbf{R}$	普通加法(+)	是	是	否
	普通乘法($\times$)	是	是	否
$M_n(\mathbf{R})$	矩阵加法(+)	是	是	否
	矩阵乘法($\times$)	是	是	否
$P(B)$	并($\cup$)	是	是	是
	交($\cap$)	是	是	是
	相对补($-$)	否	否	否
	对称差($\oplus$)	是	是	否
A^A	函数复合	否	是	否

在表 5.5 中,对于任意的 $x, y, z \in \mathbf{Z}$,有

$$x + y = y + x \quad (\text{交换律})$$

$$(x + y) + z = x + (y + z) \quad (\text{结合律})$$

又如, B 是集合, $P(B)$ 是 B 的幂集,代数系统 $\langle P(B), \cup \rangle$ 和 $\langle P(B), \cap \rangle$ 中的 $\cup$ 、 $\cap$ 运算都满足交换律和结合律。

定义 5.6(分配律) 设 $\circ$ 、 $*$ 是定义在集合 S 上的两个二元运算。如果对于任意的 $x, y, z \in S$,都有

$$x \circ (y * z) = (x \circ y) * (x \circ z)$$

$$(y * z) \circ x = (y \circ x) * (z \circ x)$$

则称运算 $\circ$ 对运算 $*$ 是可分配的,也称运算 $\circ$ 对运算 $*$ 满足分配律。

例 5.8 设集合 $A = \{0, 1\}$,在 A 上定义两个二元运算 $\circ$ 和 $*$,如表 5.6 和表 5.7 所示。运算 $*$ 对运算 $\circ$ 和运算 $\circ$ 对运算 $*$ 分别是否可分配?

表 5.6 $\circ$ 运算表

$\circ$	0	1
0	0	1
1	1	0

表 5.7 $*$ 运算表

$*$	0	1
0	0	0
1	0	1

解: 容易验证运算 $*$ 对运算 $\circ$ 是可分配的,但运算 $\circ$ 对运算 $*$ 不满足分配律。因为 $1 \circ (0 * 1) = 1 \circ 1 = 1$,而 $(1 \circ 0) * (1 \circ 1) = 1 * 0 = 0$,所以 $\circ$ 对 $*$ 不满足分配律。

定义 5.7(吸收律) 设 $\circ$ 和 $*$ 是集合 S 上的两个可交换的二元运算,如果对任意 $x, y \in S$,都有

$$x * (x \circ y) = x, x \circ (x * y) = x$$

则称运算 $\circ$ 和 $*$ 满足吸收律。

例 5.9 讨论下列集合上的二元运算是否满足分配律和吸收律。

(1) 整数集 $\mathbf{Z}$ 、有理数集 $\mathbf{Q}$ 和实数集 $\mathbf{R}$ 。

(2) n 阶实矩阵集合 $M_n(\mathbf{R})$ 。

(3) 幂集 $P(B)$ 。

解：以上集合上的二元运算的性质如表 5.8 所示。

表 5.8 例 5.9 集合上的二元运算的性质

集 合	运 算	分 配 律	吸 收 律
$\mathbf{Z}, \mathbf{Q}, \mathbf{R}$	普通加法(+)与乘法($\times$)	$\times$ 对+可分配 +对 $\times$ 不可分配	否
$M_n(\mathbf{R})$	矩阵加法(+)与乘法($\times$)	$\times$ 对+可分配 +对 $\times$ 不可分配	否
$P(B)$	并($\cup$)与交($\cap$)	$\cup$ 对 $\cap$ 可分配 $\cap$ 对 $\cup$ 可分配	是
	交($\cap$)与对称差($\oplus$)	$\cap$ 对 $\oplus$ 可分配	否

在表 5.8 中,对任意 $C, D \in P(B)$,由集合相等及 $\cap$ 和 $\cup$ 的定义可得

$$C \cup (C \cap D) = C, C \cap (C \cup D) = C$$

因此, $\cap$ 和 $\cup$ 满足吸收律。

定义 5.8(单位元) 设 $\circ$ 是定义在集合 S 上的一个二元运算。如果有一个元素 $e_l \in S$,使得对任意元素 $x \in S$ 都有 $e_l \circ x = x$,则称 e_l 为 S 中关于运算 $\circ$ 的左单位元;如果有一个元素 $e_r \in S$,使得对任意元素 $x \in S$ 都有 $x \circ e_r = x$,则称 e_r 为 S 中关于运算 $\circ$ 的右单位元;如果 S 中有一个元素 e 既是左单位元又是右单位元,则称 e 是 S 中关于运算 $\circ$ 的单位元。

对给定的集合和运算,有些存在单位元,有些不存在单位元。

例 5.10 在整数集 $\mathbf{Z}$ 中加法的单位元是 0,乘法的单位元是 1;另外, $\mathbf{R}^*$ 是非零的实数集合, $\circ$ 是 $\mathbf{R}^*$ 上如下定义的二元运算:对任意的元素 $a, b \in \mathbf{R}^*$, $a \circ b = b$,则 $\mathbf{R}^*$ 中不存在右单位元;但对任意的 $a \in \mathbf{R}^*$,对所有的 $b \in \mathbf{R}^*$ 都有 $a \circ b = b$,所以, $\mathbf{R}^*$ 的任一元素 a 都是运算 $\circ$ 的左单位元, $\mathbf{R}^*$ 中的运算 $\circ$ 有无穷多个左单位元,没有右单位元和单位元。又如,在偶数集合中,普通乘法运算没有左单位元、右单位元和单位元。

定理 5.1 设 $*$ 是定义在集合 S 上的二元运算, e_l 和 e_r 分别是 S 中关于运算 $*$ 的左单位元和右单位元,则有 $e_l = e_r = e$,且 e 为 S 上关于运算 $*$ 的唯一的单位元。

证明: 因为 e_l 和 e_r 分别是 S 中关于运算 $*$ 的左单位元和右单位元,所以 $e_l = e_l * e_r = e_r$,把 $e_l = e_r$ 记为 e 。假设 S 中存在 e_l ,则有 $e_l = e * e_l = e$ 。所以, e 是 S 中关于运算 $*$ 的唯一单位元。

定义 5.9(零元) 设 $*$ 是定义在集合 S 上的一个二元运算。如果有一个元素 $\theta_l \in S$,使得对任意的元素 $x \in S$ 都有 $\theta_l * x = \theta_l$,则称 θ_l 为 S 关于运算 $*$ 的左零元;如果有一个元素 $\theta_r \in S$,使得对任意的元素 $x \in S$ 都有 $x * \theta_r = \theta_r$,则称 θ_r 为 S 关于运算 $*$ 的右零元;如果 S 中有一个元素 θ 既是左零元又是右零元,则称 θ 为 S 关于运算 $*$ 的零元。

例 5.11 整数集 $\mathbf{Z}$ 上普通乘法的零元是 0,加法没有零元;在集合 S 的幂集 $P(S)$ 中,运算 $\cup$ 的零元是 S ,运算 $\cap$ 的零元是 $\emptyset$;在非零的实数集 $\mathbf{R}^*$ 上定义运算 $*$,使得对任意的元素 $a, b \in \mathbf{R}^*$ 都有 $a * b = a$,那么, $\mathbf{R}^*$ 的任何元素都是运算 $*$ 的左零元,而 $\mathbf{R}^*$ 中运算 $*$ 没有右零元,也没有零元。

定理 5.2 设 $\circ$ 是集合 S 上的二元运算, θ_l 和 θ_r 分别是 S 中运算 $\circ$ 的左零元和右零元,则有 $\theta_l=\theta_r=\theta$ 且 θ 是 S 上关于运算 $\circ$ 的唯一零元。

定理 5.3 设 $\langle S, * \rangle$ 是一个代数系统,其中 $*$ 是 S 上的一个二元运算,且集合 S 中的元素个数大于1,若这个代数系统中存在单位元 e 和零元 θ ,则 $e \neq \theta$ 。

证明: 用反证法。若 $e=\theta$,那么对于任意的 $x \in S$,必有 $x=e*x=\theta*x=\theta=e$,于是 S 中的所有元素都相同,即 S 中只有一个元素,这与 S 中元素个数大于1矛盾。所以, $e \neq \theta$ 。

定义 5.10(逆元) 设 $\langle S, * \rangle$ 是代数系统,其中 $*$ 是 S 上的二元运算, $e \in S$ 是 S 中运算 $*$ 的单位元。对于 S 中任意元素 x ,如果有 S 中的元素 y_l 使 $y_l*x=e$,则称 y_l 为 x 的左逆元;若有 S 中的元素 y_r 使 $x*y_r=e$,则称 y_r 为 x 的右逆元;如果有 S 中的元素 y 既是 x 的左逆元又是 x 的右逆元,则称 y 是 x 的逆元。

例 5.12 设集合 $A=\{a_1, a_2, a_3, a_4, a_5, a_6\}$,定义在 A 上的二元运算 $*$ 的运算表如表5.9所示,试指出代数系统 $\langle A, * \rangle$ 中各元素的左、右逆元的情况。

表 5.9 定义在 A 上的二元运算 $*$ 的运算表

$*$	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_2	a_3	a_4	a_5
a_2	a_2	a_4	a_1	a_1	a_4
a_3	a_3	a_1	a_2	a_3	a_1
a_4	a_4	a_3	a_1	a_4	a_3
a_5	a_5	a_4	a_2	a_3	a_5

解: 由表5.9可知, a_1 是单位元, a_1 的逆元是 a_1 ; a_2 的左逆元和右逆元都是 a_3 ,即 a_2 和 a_3 互为逆元; a_4 的左逆元是 a_2 ,而右逆元是 a_3 , a_2 有两个右逆元 a_3 和 a_4 ; a_5 有左逆元 a_3 ,但 a_5 没有右逆元。

说明: 一般,对给定的集合和其上的一个二元运算来说,左逆元、右逆元、逆元和单位元、零元不同。如果单位元和零元存在,一定是唯一的;而左逆元、右逆元、逆元是与集合中某个元素相关的,一个元素的左逆元不一定是右逆元,一个元素的左逆元和右逆元可以不止一个,但一个元素若有逆元,则存在唯一的逆元。

定理 5.4 设 $\langle S, * \rangle$ 是一个代数系统,其中 $*$ 是定义在 S 上的一个可结合的二元运算, e 是该运算的单位元。对于 $x \in S$,如果存在左逆元 y_l 和右逆元 y_r ,则有 $y_l=y_r=y$,且 y 是 x 的唯一的逆元。

证明: 根据题意,

$$y_l=y_l*e=y_l*(x*y_r)=(y_l*x)*y_r=e*y_r=y_r$$

令 $y_l=y_r=y$,则 y 是 x 的逆元。假设 $y_1 \in S$ 也是 x 的逆元,则有

$$y_1=y_1*e=y_1*(x*y)=(y_1*x)*y=e*y=y$$

所以, y 是 x 的唯一的逆元。

由定理5.4可知,对于可结合的二元运算,元素 x 的逆元如果存在,则存在唯一的逆元。通常把 x 唯一存在的逆元记为 x^{-1} 。

定理 5.5 设 $\langle S, * \rangle$ 是代数系统, 其中 $*$ 是 S 上可结合的二元运算, S 有单位元 e 。若 S 中的每个元素都有右逆元, 则这个右逆元也是左逆元, 从而是该元素唯一的逆元。

证明: 对任一元素 $a \in S$, 由条件可设 $b, c \in S$, b 是 a 的右逆元, c 是 b 的右逆元。因为 $b * (a * b) = b * e = b$, 所以

$$e = b * c = (b * (a * b)) * c = b * ((a * b) * c) = b * (a * (b * c)) = b * (a * e) = b * a$$

因此, b 也是 a 的左逆元。从而由定理 5.4 知, b 是 a 的唯一逆元, 由 $a \in S$ 的任意性知定理 5.5 成立。

例 5.13 讨论下列集合关于二元运算的特异元素, 即单位元、零元、逆元情况。

(1) 集合 $\mathbf{N}$, 集合 $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$, 集合 $\mathbf{Q}, \mathbf{R}$ 。

(2) 集合 $M_n(\mathbf{R})$ 。

(3) 集合 $P(B)$ 。

解: 这些集合关于二元运算的特异元素如表 5.10 所示。

表 5.10 例 5.13 集合关于二元运算的特异元素

集合	运 算	单 位 元	零 元	逆 元
$\mathbf{N}$	普通加法(+)	0	无	0 的逆元为 0
$\mathbf{Z}, \mathbf{Q}, \mathbf{R}$	普通加法(+)	0	无	x 的逆元为 $-x$
$\mathbf{Q}, \mathbf{R}$	普通乘法($\times$)	1	0	x 的逆元为 x^{-1}
$M_n(\mathbf{R})$	矩阵加法(+) 矩阵乘法($\times$)	n 阶全零矩阵 n 阶全零矩阵	无 n 阶全零矩阵	x 的逆元为 $-x$ x 的逆元为逆矩阵(若 x 可逆)
$P(B)$	并($\cup$) 交($\cap$)	$\emptyset$ B	B $\emptyset$	$\emptyset$ 的逆元为 $\emptyset$ B 的逆元为 B

在表 5.10 中, $\mathbf{N}$ 和 $\mathbf{Z}$ 分别表示自然数集和整数集, $\times$ 为普通乘法, $+$ 为普通加法, 则代数系统 $\langle \mathbf{N}, + \rangle$ 有单位元 0 且只有 0 有逆元, 0 的逆元是 0, 其他自然数都没有加法逆元; 代数系统 $\langle \mathbf{Z}, + \rangle$ 中有单位元 0, 所有元素都有逆元, $\mathbf{Z}$ 中任何整数 x 关于加法运算的逆元是它的相反数 $-x$; $\langle \mathbf{Z}, \times \rangle$ 中 $\mathbf{Z}$ 关于乘法运算有单位元 1, 且只有 -1 和 1 有逆元, 分别是 -1 和 1。

说明: 若 $\langle S, \circ \rangle$ 是代数系统, 其中 $\circ$ 是有限非空集合 S 上的二元运算, 那么该运算的部分性质可以从运算表直接看出, 例如:

(1) 当且仅当运算表中每个元素都属于 S 时, 运算 $\circ$ 具有封闭性。

(2) 当且仅当运算表关于主对角线对称时, 运算 $\circ$ 具有可交换性。

(3) 当且仅当运算表主对角线上的元素与它所在的行(列)的表头相同时, 运算 $\circ$ 具有幂等性。

(4) S 关于运算 $\circ$ 有单位元 e , 当且仅当表头 e 所在的列与左边一列相同且表中左边一列 e 所在的行与表头一行相同。

(5) S 关于运算 $\circ$ 有零元 θ , 当且仅当表头 θ 所在的列和表中左边一列 θ 所在的行都是 θ 。

(6) 设 S 关于运算 $\circ$ 有单位元, 当且仅当位于 a 所在的行与 b 所在的列交叉点上的元素以及 b 所在的行与 a 所在的列交叉点上的元素都是单位元时, a 与 b 互为逆元。

代数系统 $\langle S, \circ \rangle$ 中一个元素是否有左逆元或右逆元也可以从运算表中观察出来, 但运算是否满足结合律在运算表上一般不易直接观察出来。

5.3 半群与含么半群

半群与含么半群是特殊的代数系统,在计算机科学领域中已得到了卓有成效的应用。

定义 5.11(半群) 设 $\langle S, * \rangle$ 是一个代数系统, $*$ 是 S 上的一个二元运算。如果运算 $*$ 是可结合的,即对任意的 $x, y, z \in S$,都有 $(x * y) * z = x * (y * z)$,则称代数系统 $\langle S, * \rangle$ 为半群。半群中的二元运算也叫乘法,运算的结果也叫积。

由定义 5.11 易得, $\langle \mathbf{N}, + \rangle$ 和 $\langle \mathbf{N}, \times \rangle$ 是半群,其中 $\mathbf{N}$ 是自然数集, $+$ 、 $\times$ 分别是普通的加法和乘法。设 A 是任一集合, $P(A)$ 是 A 的幂集,则 $\langle P(A), \cup \rangle$, $\langle P(A), \cap \rangle$ 都是半群。

例 5.14 设 $S = \{a, b, c\}$, S 上的二元运算 $\circ$ 的运算表如表 5.11 所示,验证 $\langle S, \circ \rangle$ 是半群。

表 5.11 S 上的二元运算 $\circ$ 的运算表

$\circ$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

解: 由表 5.11 知,运算 $\circ$ 在 S 上是封闭的,而且对任意 $x_1, x_2 \in S$ 有 $x_1 \circ x_1 = x_1$,所以 $\langle S, \circ \rangle$ 是代数系统,且 a, b, c 都是左单位元,从而对任意的 $x, y, z \in S$ 都有 $x \circ (y \circ z) = x \circ z = z = y \circ z = (x \circ y) \circ z$,因此,运算 $\circ$ 是可结合的, $\langle S, \circ \rangle$ 是半群。

例 5.15 设 k 是一个非负整数,集合定义为 $S_k = \{x \mid x \text{ 是整数且 } x \geq k\}$,那么, $\langle S_k, + \rangle$ 是半群,其中 $+$ 是普通的加法运算。

解: 因为 k 是非负整数,运算 $+$ 在 S_k 上是封闭的,且普通加法运算是可结合的,所以 $\langle S_k, + \rangle$ 是半群。

易知,代数系统 $\langle \mathbf{Z}, - \rangle$ 和 $\langle \mathbf{R} - \{0\}, / \rangle$ 都不是半群,这里 $-$ 和 $/$ 分别是普通的减法和除法。

定理 5.6 设 $\langle S, * \rangle$ 是半群, B 是 S 的非空子集,且二元运算 $*$ 在 B 上封闭,即对任意的 $a, b \in B$ 有 $a * b \in B$,那么, $\langle B, * \rangle$ 也是半群。通常称 $\langle B, * \rangle$ 是 $\langle S, * \rangle$ 的子半群。

证明: 因为运算 $*$ 在 S 上是可结合的,而 B 是 S 的非空子集且 $*$ 在 B 上是封闭的,所以 $*$ 在 B 上也是可结合的,因此, $\langle B, * \rangle$ 是半群。

例 5.16 设 $\cdot$ 表示普通的乘法运算,那么 $\langle \{-1, 1\}, \cdot \rangle$, $\langle [-1, 1], \cdot \rangle$ 和 $\langle \mathbf{Z}, \cdot \rangle$ 都是半群 $\langle \mathbf{R}, \cdot \rangle$ 的子半群。

解: 首先,运算 $\cdot$ 在 R 上是封闭的,且是可结合的,所以 $\langle \mathbf{R}, \cdot \rangle$ 是半群。其次,运算 $\cdot$ 在 $\{-1, 1\}$, $[-1, 1]$ 和 $\mathbf{Z}$ 上都是封闭的, $\{-1, 1\}$, $[-1, 1]$ 和 $\mathbf{Z}$ 都是 $\mathbf{R}$ 的非空子集,由定理 5.6 知 $\{-1, 1\}$, $[-1, 1]$ 和 $\langle \mathbf{Z}, \cdot \rangle$ 都是 $\langle \mathbf{R}, \cdot \rangle$ 的子半群。

定义 5.12(方幂) 半群 $\langle S, \circ \rangle$ 中的任一元素 a 的方幂 a^n 定义为 $a^1 = a$, $a^{n+1} = a^n \circ a$

(n 是大于或等于 1 的整数)。

可以证明,对于任意 $a \in S$ 和任意正整数 m, n 都有

$$a^m \circ a^n = a^{m+n}, (a^m)^n = a^{mn}$$

若 $a^2 = a$, 则称 a 为幂等元素。

定义 5.13(可交换半群) 若半群 $\langle S, \circ \rangle$ 的运算 $\circ$ 满足交换律, 则称 $\langle S, \circ \rangle$ 是一个可交换半群。

在可交换半群 $\langle S, \circ \rangle$ 中, 有 $(a \circ b)^n = a^n \circ b^n$, 其中 n 是正整数, $a, b \in S$ 。

定义 5.14(含幺半群) 含有单位元的半群称为含幺半群或独异点。

例 5.17 代数系统 $\langle \mathbf{R}, \cdot \rangle$ 是含幺半群, 其中 $\mathbf{R}$ 是实数集, $\cdot$ 是普通乘法, 这是因为 $\langle \mathbf{R}, \cdot \rangle$ 是半群, 且 1 是 $\mathbf{R}$ 关于运算 $\cdot$ 的单位元。代数系统 $\langle \{-1, 1\}, \cdot \rangle$ 和 $\langle \mathbf{Z}, \cdot \rangle$ 都是具有单位元 1 的半群, 因此它们都是含幺半群。另外, 设集合 $A = \{1, 2, 3, \dots\}$, 则 $\langle A, + \rangle$ 是半群但不含单位元, 所以它不是含幺半群。

定理 5.7 设 S 是至少有两个元素的有限集合, 且 $\langle S, * \rangle$ 是一个含幺半群, 则在关于运算 $*$ 的运算表中任何两行或两列都是不相同的。

证明: 假设 S 关于运算 $*$ 的单位元是 e 。对于任意 $a, b \in S$ 且 $a \neq b$, 总有

$$e * a = a \neq b = e * b, a * e = a \neq b = b * e$$

所以在运算 $*$ 表中不可能有两行和两列是相同的。

例 5.18 设 $\mathbf{Z}$ 是整数集合, m 是任意正整数, $\mathbf{Z}_m$ 是由模 m 的同余类组成的集合, 在 $\mathbf{Z}_m$ 上分别定义两个二元运算 $+_m$ 和 $\times_m$ 如下: 对任意的 $[i], [j] \in \mathbf{Z}_m$, $[i] +_m [j] = [(i + j) \pmod{m}]$, $[i] \times_m [j] = [(i \times j) \pmod{m}]$ 。证明 $m > 1$ 时在这两个二元运算的运算表中任何两行或两列都不相同。

证明: 考察非空集合 $\mathbf{Z}_m$ 上的二元运算 $+_m$ 和 $\times_m$ 。

(1) 由运算 $+_m$ 和 $\times_m$ 的定义易得, 它们在 $\mathbf{Z}_m$ 上都是封闭的且都是可结合的, 所以, $\langle \mathbf{Z}_m, +_m \rangle$ 和 $\langle \mathbf{Z}_m, \times_m \rangle$ 都是半群。

(2) 因为 $[0] +_m [i] = [i] = [i] +_m [0]$, 所以 $[0]$ 是 $\langle \mathbf{Z}_m, +_m \rangle$ 中的单位元; 因为 $[1] \times_m [i] = [i] = [i] \times_m [1]$, 所以 $[1]$ 是 $\langle \mathbf{Z}_m, \times_m \rangle$ 中的单位元。

由上可知, 代数系统 $\langle \mathbf{Z}_m, +_m \rangle$ 和 $\langle \mathbf{Z}_m, \times_m \rangle$ 都是含幺半群。从而由定理 5.7 知, $\mathbf{Z}_m$ 中的两个运算 $+_m, \times_m$ 的运算表的任何两行或两列都不相同。

表 5.12 和表 5.13 分别给出了 $m=4$ 时 $+_4$ 和 $\times_4$ 的运算表。在这两个运算表中没有两行或两列是相同的。

表 5.12 $+_4$ 运算表

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

表 5.13 $\times_4$ 运算表

$\times_4$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

定理 5.8 设 $\langle S, \circ \rangle$ 是含幺半群, 对于任意的 $x, y \in S$, 当 x, y 均有逆元时, 有

$$(1) (x^{-1})^{-1} = x.$$

$$(2) x \circ y \text{ 有逆元, 且 } (x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$

证明: (1) 因 x^{-1} 是 x 的逆元, 所以 $x^{-1} \circ x = x \circ x^{-1} = e$, 从而由逆元的定义及唯一性得 $(x^{-1})^{-1} = x$.

(2) 因为

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = x \circ (y \circ y^{-1}) \circ x^{-1} = x \circ e \circ x^{-1} = x \circ x^{-1} = e$$

同理可证 $(y^{-1} \circ x^{-1}) \circ (x \circ y) = e$, 所以由逆元的定义及唯一性得 $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

定义 5.15 (子含幺半群) 设 $\langle M, \circ \rangle$ 是含幺半群 $\langle S, \circ \rangle$ 的子半群, 且 $\langle S, \circ \rangle$ 的单位元 $e_s \in M$, 则 $\langle M, \circ \rangle$ 称为 $\langle S, \circ \rangle$ 的子含幺半群。

例 5.19 $\langle \mathbf{Z}, \circ \rangle$ 是含幺半群, $\mathbf{Z}$ 中所有幂等元的集合为 $M = \{x \mid x \in S \text{ 且 } x^2 = x\}$, 则 $\langle M, \circ \rangle$ 是 $\langle \mathbf{Z}, \circ \rangle$ 的子含幺半群。

证明: 显然, $\langle \mathbf{Z}, \circ \rangle$ 是含幺半群, 且满足交换律。设该含幺半群的单位元为 e , $M = \{x \mid x \in S \text{ 且 } x^2 = x\}$, 因为 $e^2 = e$, 所以 $e \in M$ 。又因为对任意 $a, b \in M$, 有

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

所以 $a \circ b \in M$, 从而运算 $\circ$ 在 M 上封闭。故 $\langle M, \circ \rangle$ 是 $\langle \mathbf{Z}, \circ \rangle$ 的子含幺半群。

5.4 群与子群

群的理论在数学和包括计算机科学在内的很多学科中发挥了重要的作用, 本节主要介绍群与子群的一些基本知识。

定义 5.16 (群) 设 $\langle G, \circ \rangle$ 是一个代数系统, 其中 G 是非空集合, $\circ$ 是 G 上的一个二元运算。如果 $\langle G, \circ \rangle$ 满足以下条件, 则称其为一个群。① 运算 $\circ$ 是封闭的; ② 运算 $\circ$ 是可结合的; ③ $\langle G, \circ \rangle$ 中有单位元 e ; ④ 对每个元素 $a \in G$ 都存在相应的逆元 a^{-1} 。

由以上定义可知: 群一定是含幺半群, 反之不一定成立。

例 5.20 若集合 $G = \{g\}$, 定义二元运算 $\circ$ 为 $g \circ g = g$, 则 $\langle G, \circ \rangle$ 是半群。事实上, 由运算 $\circ$ 的定义可得, $\langle G, \circ \rangle$ 满足群定义的条件①、②, 同时, g 是 $\langle G, \circ \rangle$ 的单位元, $g \in G$ 的逆元是 g , 所以 $\langle G, \circ \rangle$ 是群。

例 5.21 有理数集 $\mathbf{Q}$ 关于普通加法构成群 $\langle \mathbf{Q}, + \rangle$, 单位元是 0 , $a \in \mathbf{Q}$, a 的逆元是 $-a$; 类似地, 若 $\mathbf{Z}$ 是整数集, 则 $\langle \mathbf{Z}, + \rangle$ 是群, 但 $\langle \mathbf{Z}, \times \rangle$ 是只含单位元的半群而不是群。

例 5.22 设 $G = \{a, b, c\}$, 二元运算 $\circ$ 的运算表由表 5.14 给出, 则 $\langle G, \circ \rangle$ 是一个群。