离散数学

（第 3 版）

智能科学与技术学院 2024 级

目录

目录

12.1 二元运算及其性质

定义 1.1.1

设 S 为集合，函数 $f : S \times S \to S$ 称为 S 上的二元运算，简称为二元运算 .

12.1 二元运算及其性质

定义 1.1.1

设 S 为集合，函数 $f : S \times S \to S$ 称为 S 上的二元运算，简称为二元运算.

例如，$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, f(\langle x, y \rangle) = x + y$ 就是自然数集 $\mathbb{N}$ 上的二元运算，即普通的加法运算.

12.1 二元运算及其性质

定义 1.1.1

设 S 为集合，函数 $f : S \times S \to S$ 称为 S 上的二元运算，简称为 二元运算 .

例如，$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, f(\langle x, y \rangle) = x + y$ 就是自然数集 $\mathbb{N}$ 上的二元运算，即普通的加法运算.

普通的减法不是自然数集 $\mathbb{N}$ 上的二元运算，因为两个自然数相减可能得负数，而负数不是自然数. 这时也称 $\mathbb{N}$ 对减法运算 不封闭 .

12.1 二元运算及其性质

定义 1.1.1

设 S 为集合，函数 $f : S \times S \to S$ 称为 S 上的二元运算，简称为 二元运算 .

例如，$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, f(\langle x, y \rangle) = x + y$ 就是自然数集 $\mathbb{N}$ 上的二元运算，即普通的加法运算.

普通的减法不是自然数集 $\mathbb{N}$ 上的二元运算，因为两个自然数相减可能得负数，而负数不是自然数. 这时也称 $\mathbb{N}$ 对减法运算 不封闭 .

验证一个运算是否为集合 S 上的二元运算主要考虑以下两点.

1. S 中任何两个元素都可以进行这种运算，且运算的结果是唯一的.
2. S 中任何两个元素的运算结果都属于 S，即 S 对该运算是 封闭 的.

12.1 二元运算及其性质

定义 1.1.1

设 S 为集合，函数 $f : S \times S \to S$ 称为 S 上的二元运算，简称为 二元运算 .

例如，$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, f(\langle x, y \rangle) = x + y$ 就是自然数集 $\mathbb{N}$ 上的二元运算，即普通的加法运算.

普通的减法不是自然数集 $\mathbb{N}$ 上的二元运算，因为两个自然数相减可能得负数，而负数不是自然数. 这时也称 $\mathbb{N}$ 对减法运算 不封闭 .

验证一个运算是否为集合 S 上的二元运算主要考虑以下两点.

1. S 中任何两个元素都可以进行这种运算，且运算的结果是唯一的.
2. S 中任何两个元素的运算结果都属于 S，即 S 对该运算是 封闭 的.

例如，实数集 $\mathbb{R}$ 上不可以定义除法运算，因为 $0 \in \mathbb{R}$，而 0 不能做除数. 但在 $\mathbb{R}^* = \mathbb{R} - \{0\}$ 上就可以定义除法运算了，因为 $\forall x, y \in \mathbb{R}^*$，都有 $x/y \in \mathbb{R}^*$.

例 1.1.1

1. 自然数集 $\mathbb{N}$ 上的加法和乘法是 $\mathbb{N}$ 上的二元运算，而减法和除法不是.

例 1.1.1

1. 自然数集 $\mathbb{N}$ 上的加法和乘法是 $\mathbb{N}$ 上的二元运算，而减法和除法不是.
2. 整数集 $\mathbb{Z}$ 上的加法、减法和乘法都是 $\mathbb{Z}$ 上的二元运算，而除法不是.

例 1.1.1

1. 自然数集 $\mathbb{N}$ 上的加法和乘法是 $\mathbb{N}$ 上的二元运算，而减法和除法不是.
2. 整数集 $\mathbb{Z}$ 上的加法、减法和乘法都是 $\mathbb{Z}$ 上的二元运算，而除法不是.
3. 非零实数集 $\mathbb{R}^*$ 上的乘法和除法都是 $\mathbb{R}^*$ 上的二元运算，而加法和减法不是，因为两个非零实数相加或相减可能得 0.

例 1.1.1

1. 自然数集 $\mathbb{N}$ 上的加法和乘法是 $\mathbb{N}$ 上的二元运算，而减法和除法不是.
2. 整数集 $\mathbb{Z}$ 上的加法、减法和乘法都是 $\mathbb{Z}$ 上的二元运算，而除法不是.
3. 非零实数集 $\mathbb{R}^*$ 上的乘法和除法都是 $\mathbb{R}^*$ 上的二元运算，而加法和减法不是，因为两个非零实数相加或相减可能得 0.
4. 设 $M_n(\mathbb{R})$ 表示所有 $n(\geqslant 2)$ 阶实矩阵的集合，即

$$M_n(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \middle| a_{ij} \in \mathbb{R}, 1 \leqslant i, j \leqslant n \right\},$$

则矩阵加法和乘法都是 $M_n(\mathbb{R})$ 上的二元运算.

例 1.1.1

1. 自然数集 $\mathbb{N}$ 上的加法和乘法是 $\mathbb{N}$ 上的二元运算，而减法和除法不是.
2. 整数集 $\mathbb{Z}$ 上的加法、减法和乘法都是 $\mathbb{Z}$ 上的二元运算，而除法不是.
3. 非零实数集 $\mathbb{R}^*$ 上的乘法和除法都是 $\mathbb{R}^*$ 上的二元运算，而加法和减法不是，因为两个非零实数相加或相减可能得 0.
4. 设 $M_n(\mathbb{R})$ 表示所有 $n(\geqslant 2)$ 阶实矩阵的集合，即

$$M_n(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \middle| a_{ij} \in \mathbb{R}, 1 \leqslant i, j \leqslant n \right\},$$

   则矩阵加法和乘法都是 $M_n(\mathbb{R})$ 上的二元运算.
5. S 为任意集合，则 $\cup, \cap, -, \oplus$ 为 S 的幂集 $P(S)$ 上的二元运算，这里 $\cup$ 和 $\cap$ 是初级并和初级交.

例 1.1.1

1. 自然数集 $\mathbb{N}$ 上的加法和乘法是 $\mathbb{N}$ 上的二元运算，而减法和除法不是.
2. 整数集 $\mathbb{Z}$ 上的加法、减法和乘法都是 $\mathbb{Z}$ 上的二元运算，而除法不是.
3. 非零实数集 $\mathbb{R}^*$ 上的乘法和除法都是 $\mathbb{R}^*$ 上的二元运算，而加法和减法不是，因为两个非零实数相加或相减可能得 0.
4. 设 $M_n(\mathbb{R})$ 表示所有 $n(\geqslant 2)$ 阶实矩阵的集合，即

$$M_n(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \middle| a_{ij} \in \mathbb{R}, 1 \leqslant i, j \leqslant n \right\},$$

   则矩阵加法和乘法都是 $M_n(\mathbb{R})$ 上的二元运算.
5. S 为任意集合，则 $\cup, \cap, -, \oplus$ 为 S 的幂集 $P(S)$ 上的二元运算，这里 $\cup$ 和 $\cap$ 是初级并和初级交.
6. S 为集合，S^S 为 S 上的所有函数的集合，则函数的复合运算 $\circ$ 为 S^S 上的二元运算.

通常用 $\circ, *, \cdot$ 等符号表示二元运算，称为算符. 设 $f : S \times S \to S$ 是 S 上的二元运算，对任意的 $x, y \in S$，如果 x 与 y 的运算结果是 z，即

$$f(\langle x, y \rangle) = z,$$

那么可以利用算符 $\circ$ 简记为

$$x \circ y = z.$$

通常用 $\circ, *, \cdot$ 等符号表示二元运算，称为算符. 设 $f : S \times S \to S$ 是 S 上的二元运算，对任意的 $x, y \in S$，如果 x 与 y 的运算结果是 z，即

$$f(\langle x, y \rangle) = z,$$

那么可以利用算符 $\circ$ 简记为

$$x \circ y = z.$$

例 1.1.2

设 $\mathbb{R}$ 为实数集，定义 $\mathbb{R}$ 上的二元运算 $*$ 如下.

$$\forall x, y \in \mathbb{R},\ x * y = x.$$

计算 $3 * 4, (-5) * 0.2, 0 * \frac{1}{2}$.

解

$3 * 4 = 3, (-5) * 0.2 = -5, 0 * \frac{1}{2} = 0.$ □

一元运算

定义 1.1.2

设 S 为集合，函数 $f : S \to S$ 称为 S 上的一个一元运算，简称为一元运算.

一元运算

定义 1.1.2

设 S 为集合，函数 $f : S \to S$ 称为 S 上的一个一元运算，简称为一元运算.

例 1.1.3

1. 求一个数的相反数是整数集 $\mathbb{Z}$、有理数集 $\mathbb{Q}$ 和实数集 $\mathbb{R}$ 上的一元运算.
2. 求一个数 x 的倒数 $\frac{1}{x}$ 是非零有理数集 $\mathbb{Q}^*$、非零实数集 $\mathbb{R}^*$ 上的一元运算.
3. 求一个复数的共轭复数是复数集 $\mathbb{C}$ 上的一元运算.
4. 在幂集 $P(S)$ 上，如果规定全集为 S，则求集合的绝对补运算 $\sim$ 是 $P(S)$ 上的一元运算.
5. 设 S 为集合，令 A 为 S 上所有双射函数的集合，$A \subseteq S^S$，则求一个双射函数的反函数为 A 上的一元运算.
6. 在 $n(\geqslant 2)$ 阶实矩阵的集合 $M_n(\mathbb{R})$ 上，求一个矩阵的转置矩阵是 $M_n(\mathbb{R})$ 上的一元运算.

与二元运算一样，也可以使用算符来表示一元运算. 若 $f : S \to S$ 为 S 上的一元运算，则 $f(x) = y$ 可以用算符 $\circ$ 记作 $\circ(x) = y$ 或 $\circ x = y$, 其中 x 为参加运算的元素，y 为运算的结果.

例如，x 的相反数 $-x$、集合 X 的绝对补集 $\sim X$ 都是上述表示形式，其中 $-$ 和 $\sim$ 都是算符.

与二元运算一样,也可以使用算符来表示一元运算. 若 $f : S \to S$ 为 S 上的一元运算,则 $f(x) = y$ 可以用算符 $\circ$ 记作 $\circ(x) = y$ 或 $\circ x = y$, 其中 x 为参加运算的元素,y 为运算的结果.

例如,x 的相反数 $-x$、集合 X 的绝对补集 $\sim X$ 都是上述表示形式,其中 $-$ 和 $\sim$ 都是算符.

表 1.1.1

a_i	$\circ a_i$
a_1	$\circ a_1$
a_2	$\circ a_2$
$\vdots$	$\vdots$
a_n	$\circ a_n$

表 1.1.2

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	$\cdots$	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	$\cdots$	$a_2 \circ a_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	$a_n \circ a_1$	$a_n \circ a_2$	$\cdots$	$a_n \circ a_n$

对于有穷集 S 上的一元和二元运算,除了可以使用函数 f 的表达式表示以外,还可以用运算表表示. 表 1.1.1 和表 1.1.2 是一元运算表和二元运算表的一般形式,其中 $a_1, a_2, \cdots, a_n$ 是 S 中的元素,$\circ$ 为算符.

例 1.1.4

设 $S = \{1, 2\}$, 给出 $P(S)$ 上的运算 $\sim$ 和 $\oplus$ 的运算表, 其中全集为 S.

例 1.1.4

设 $S=\{1,2\}$,给出 $P(S)$ 上的运算 $\sim$ 和 $\oplus$ 的运算表,其中全集为 S.

解

所求的运算表如表 1.1.3 和表 1.1.4 所示.

表 1.1.3

X	$\sim X$
$\varnothing$	$\{1,2\}$
$\{1\}$	$\{2\}$
$\{2\}$	$\{1\}$
$\{1,2\}$	$\varnothing$

表 1.1.4

$\oplus$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\varnothing$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\varnothing$	$\{1,2\}$	$\{2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\varnothing$	$\{1\}$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	$\varnothing$

例 1.1.5

设 $S = \{1, 2, 3, 4\}$, 定义 S 上的二元运算 $\circ$ 如下.

$$x \circ y = xy \mod 5, \ \forall x, y \in S.$$

求运算 $\circ$ 的运算表.

例 1.1.5

设 $S=\{1,2,3,4\}$，定义 S 上的二元运算 $\circ$ 如下.

$$x \circ y = xy \mod 5,\ \forall x, y \in S.$$

求运算 $\circ$ 的运算表.

解

$xy \mod 5$ 表示 xy 除以 5 的余数，其运算表如下所示.

表 1.1.5

$\circ$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

交换律

定义 1.1.3

设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x, y \in S$ 都有

$$x \circ y = y \circ x,$$

那么称运算 $\circ$ 在 S 上是可交换的，或者说运算 $\circ$ 在 S 上满足交换律.

交换律

定义 1.1.3

设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x, y \in S$ 都有

$$x \circ y = y \circ x,$$

那么称运算 $\circ$ 在 S 上是可交换的，或者说运算 $\circ$ 在 S 上满足交换律.

例如，实数集上的加法和乘法是可交换的，但减法不可交换.

幂集 $P(S)$ 上的 $\cup, \cap$ 和 $\oplus$ 都是可交换的，但是相对补运算不可交换.

$n(\geqslant 2)$ 阶实矩阵集合 $M_n(\mathbb{R})$ 上的矩阵加法是可交换的，但矩阵乘法不是可交换的.

A^A 上函数的复合运算不是可交换的，因为一般地说，$f \circ g \neq g \circ f$.

结合律

定义 1.1.4

设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x, y, z \in S$ 都有

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

那么称运算 $\circ$ 在 S 上是可结合的，或者说运算 $\circ$ 在 S 上满足结合律.

结合律

定义 1.1.4

设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x, y, z \in S$ 都有

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

那么称运算 $\circ$ 在 S 上是 可结合 的，或者说运算 $\circ$ 在 S 上满足 结合律 .

普通的加法和乘法在自然数集 $\mathbb{N}$、整数集 $\mathbb{Z}$、有理数集 $\mathbb{Q}$、实数集 $\mathbb{R}$ 和复数集 $\mathbb{C}$ 上都是可结合的.

矩阵的加法和乘法是可结合的，集合的 $\cup, \cap$ 和 $\oplus$ 运算是可结合的，还有函数的复合运算是可结合的.

对于满足结合律的二元运算，在一个只由该运算的算符连接起来的表达式中，可以把所有表示运算顺序的括号去掉.

例如，加法在实数集上是可结合的，对于任意实数 x, y, z 和 u，可以写

$$(x + y) + (z + u) = x + y + z + u.$$

幂等律

定义 1.1.5

设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x \in S$ 都有

$$x \circ x = x,$$

那么称运算 $\circ$ 满足幂等律.

幂等律

定义 1.1.5

设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x \in S$ 都有

$$x \circ x = x,$$

那么称运算 $\circ$ 满足幂等律.

如果 S 中的某些 x 满足 $x \circ x = x$，则称 x 为运算 $\circ$ 的幂等元.

易见，如果 S 上的二元运算满足幂等律，那么 S 中的所有元素都是幂等元.

对于任何集合 X，有 $X \cup X = X$ 和 $X \cap X = X$，集合的并和交运算满足幂等律，

$\oplus$ 运算和 $-$ 运算一般不满足幂等律，但 $\emptyset$ 是幂等元.

普通数的加法和乘法不满足幂等律，但 0 是加法的幂等元，0 和 1 是乘法的幂等元.

分配律

定义 1.1.6

设 $\circ$ 和 $*$ 是 S 上的两个二元运算，如果对任意的 $x, y, z \in S$ 有

$$x * (y \circ z) = (x * y) \circ (x * z), \qquad \text{(左分配律)}$$
$$(y \circ z) * x = (y * x) \circ (z * x), \qquad \text{(右分配律)}$$

那么称运算 $*$ 对 $\circ$ 是可分配的，或者说 $*$ 对 $\circ$ 满足分配律 .

分配律

定义 1.1.6

设 $\circ$ 和 $*$ 是 S 上的两个二元运算，如果对任意的 $x, y, z \in S$ 有

$$x * (y \circ z) = (x * y) \circ (x * z), \qquad \text{(左分配律)}$$
$$(y \circ z) * x = (y * x) \circ (z * x), \qquad \text{(右分配律)}$$

那么称运算 $*$ 对 $\circ$ 是可分配的，或者说 $*$ 对 $\circ$ 满足分配律.

实数集 $\mathbb{R}$ 上的乘法对加法是可分配的，在 $n(\geqslant 2)$ 阶实矩阵的集合 $\boldsymbol{M}_n(\mathbb{R})$ 上，矩阵乘法对于矩阵加法也是可分配的，而在幂集 $P(S)$ 上 $\cup$ 和 $\cap$ 互相可分配.

使用归纳法不难证明，若 $*$ 对 $\circ$ 运算分配律成立，则 $*$ 对 $\circ$ 运算广义分配律也成立，即 $\forall x, y_1, y_2, \cdots, y_n \in S$ 有

$$x * (y_1 \circ y_2 \circ \cdots \circ y_n) = (x * y_1) \circ (x * y_2) \circ \cdots \circ (x * y_n),$$
$$(y_1 \circ y_2 \circ \cdots \circ y_n) * x = (y_1 * x) \circ (y_2 * x) \circ \cdots \circ (y_n * x).$$

吸收律

定义 1.1.7

设 $\circ$ 和 $*$ 是 S 上两个可交换的二元运算，如果对于任意的 $x, y \in S$ 都有

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

那么称 $\circ$ 和 $*$ 满足吸收律.

吸收律

定义 1.1.7

设 $\circ$ 和 $*$ 是 S 上两个可交换的二元运算，如果对于任意的 $x, y \in S$ 都有

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

那么称 $\circ$ 和 $*$ 满足吸收律.

例如，幂集 $P(S)$ 上的 $\cup$ 和 $\cap$ 运算满足吸收律，即 $\forall A, B \in P(S)$ 有

$$A \cup (A \cap B) = A,$$
$$A \cap (A \cup B) = A.$$

单位元

定义 1.1.8

设 $\circ$ 为 S 上的二元运算，如果存在 $e_l \in S$(或 $e_r \in S$)，使得对任何 $x \in S$ 都有 $e_l \circ x = x$ (或 $x \circ e_r = x$)，那么称 e_l(或 e_r)是 S 中关于 $\circ$ 运算的一个*左单位元*(或*右单位元*). 若 e 关于 $\circ$ 运算既是左单位元又是右单位元，则称 e 为 S 上关于 $\circ$ 运算的*单位元*. 单位元也可以称作*幺元*.

单位元

定义 1.1.8

设 $\circ$ 为 S 上的二元运算，如果存在 $e_l \in S$(或 $e_r \in S$)，使得对任何 $x \in S$ 都有 $e_l \circ x = x$ (或 $x \circ e_r = x$)，那么称 e_l(或 e_r)是 S 中关于 $\circ$ 运算的一个*左单位元*(或*右单位元*). 若 e 关于 $\circ$ 运算既是左单位元又是右单位元，则称 e 为 S 上关于 $\circ$ 运算的*单位元*. 单位元也可以称作*幺元*.

在 $\mathbb{N}$ 上，0 是加法单位元，1 是乘法单位元. 在 $M_n(\mathbb{R}), n \geqslant 2$, 上全 0 的 n 阶矩阵是矩阵加法单位元，而 n 阶单位矩阵是矩阵乘法单位元. 在幂集 $P(S)$ 上，$\emptyset$ 是 $\cup$ 运算单位元，S 是 $\cap$ 运算单位元. $\emptyset$ 也是对称差运算 $\oplus$ 的单位元，相对补运算无单位元. 在 A^A 上，恒等函数 I_A 是函数复合运算的单位元.

单位元

定义 1.1.8

设 $\circ$ 为 S 上的二元运算，如果存在 $e_l \in S$(或 $e_r \in S$)，使得对任何 $x \in S$ 都有 $e_l \circ x = x$ (或 $x \circ e_r = x$)，那么称 e_l(或 e_r)是 S 中关于 $\circ$ 运算的一个*左单位元*(或*右单位元*). 若 e 关于 $\circ$ 运算既是左单位元又是右单位元，则称 e 为 S 上关于 $\circ$ 运算的*单位元*. 单位元也可以称作*幺元*.

在 $\mathbb{N}$ 上，0 是加法单位元，1 是乘法单位元. 在 $M_n(\mathbb{R}), n \geqslant 2$, 上全 0 的 n 阶矩阵是矩阵加法单位元，而 n 阶单位矩阵是矩阵乘法单位元. 在幂集 $P(S)$ 上，$\emptyset$ 是 $\cup$ 运算单位元，S 是 $\cap$ 运算单位元. $\emptyset$ 也是对称差运算 $\oplus$ 的单位元，相对补运算无单位元. 在 A^A 上，恒等函数 I_A 是函数复合运算的单位元.

考虑 $\mathbb{R}^*$，定义二元运算 $\circ$:$\forall a, b \in \mathbb{R}^*, a \circ b = a$, 则不存在 $e \in \mathbb{R}^*$ 使得 $\forall b \in \mathbb{R}^*$ 有 $e \circ b = b$，故 $\circ$ 运算无左单位元. 但对每一个 $a \in \mathbb{R}^*$，对任意 $b \in \mathbb{R}^*$ 都有 $b \circ a = b$，所以 $\mathbb{R}^*$ 中的每一个元素 a 都是 $\circ$ 运算的右单位元. $\mathbb{R}^*$ 中有无数多个右单位元，但任何右单位元都不是左单位元，故 $\mathbb{R}^*$ 中没有关于 $\circ$ 运算的单位元.

单位元

定理 1.1.1

设 $\circ$ 为 S 上的二元运算，e_l 和 e_r 分别为 $\circ$ 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 $\circ$ 运算唯一的单位元.

单位元

定理 1.1.1

设 $\circ$ 为 S 上的二元运算，e_l 和 e_r 分别为 $\circ$ 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 $\circ$ 运算唯一的单位元.

证明.

因为 e_r 为右单位元，所以 $e_l \circ e_r = e_l$；同理，由 e_l 为左单位元知，$e_l \circ e_r = e_r$.
由此可见，$e_l = e_r$.
将 $e_l = e_r$ 记作 e，则知 e 是 S 中的单位元. 假设 e' 也是 S 中的单位元，则有

$$e' = e \cdot e' = e,$$

所以 e 是 S 中关于 $\circ$ 运算的唯一的单位元. □

零元

定义 1.1.9

设 $\circ$ 为 S 上的二元运算，若存在 $\theta_l \in S$(或 $\theta_r \in S$)，使得对于任意的 $x \in S$ 有

$$\theta_l \circ x = \theta_l \text{ (或 } x \circ \theta_r = \theta_r\text{)},$$

则称 θ_l(或 θ_r)是 S 上关于 $\circ$ 运算的 *左零元* (或 *右零元*). 若 $\theta \in S$ 关于 $\circ$ 运算既是左零元又是右零元，则称 θ 为 S 上关于 $\circ$ 运算的 *零元* .

零元

定义 1.1.9

设 $\circ$ 为 S 上的二元运算，若存在 $\theta_l \in S$(或 $\theta_r \in S$)，使得对于任意的 $x \in S$ 有

$$\theta_l \circ x = \theta_l \text{ (或 } x \circ \theta_r = \theta_r\text{)},$$

则称 θ_l(或 θ_r)是 S 上关于 $\circ$ 运算的 *左零元* (或 *右零元*). 若 $\theta \in S$ 关于 $\circ$ 运算既是左零元又是右零元，则称 θ 为 S 上关于 $\circ$ 运算的 *零元* .

例如，自然数集 $\mathbb{N}$ 上 0 是普通乘法的零元，而加法没有零元.

$M_n(\mathbb{R}), n \geqslant 2$, 上矩阵乘法的零元是全 0 的 n 阶矩阵，而矩阵加法没有零元.

在幂集 $P(S)$ 上 $\cup$ 运算的零元是 S，$\cap$ 运算的零元是 $\emptyset$，而对称差运算 $\oplus$ 没有零元.

零元

定义 1.1.9

设 $\circ$ 为 S 上的二元运算，若存在 $\theta_l \in S$(或 $\theta_r \in S$)，使得对于任意的 $x \in S$ 有

$$\theta_l \circ x = \theta_l \text{ (或 } x \circ \theta_r = \theta_r\text{)},$$

则称 θ_l(或 θ_r)是 S 上关于 $\circ$ 运算的 *左零元* (或 *右零元*). 若 $\theta \in S$ 关于 $\circ$ 运算既是左零元又是右零元，则称 θ 为 S 上关于 $\circ$ 运算的 *零元* .

例如，自然数集 $\mathbb{N}$ 上 0 是普通乘法的零元，而加法没有零元.

$M_n(\mathbb{R}), n \geqslant 2$, 上矩阵乘法的零元是全 0 的 n 阶矩阵，而矩阵加法没有零元.

在幂集 $P(S)$ 上 $\cup$ 运算的零元是 S，$\cap$ 运算的零元是 $\emptyset$，而对称差运算 $\oplus$ 没有零元.

在 $\mathbb{R}^*$ 上如果定义运算 $\circ$，使得对任意的 $a, b \in \mathbb{R}^*$ 有 $a \circ b = a$, 那么 $\mathbb{R}^*$ 中的任何元素都是关于 $\circ$ 运算的左零元，但没有右零元，从而也没有零元.

零元(续)

与定理 1.1.1 类似,可以证明下面的定理.

定理 1.1.2

设 $\circ$ 为 S 上的二元运算,θ_l 和 θ_r 分别为 $\circ$ 运算的左零元和右零元,则有

$$\theta_l = \theta_r = \theta,$$

且 θ 是 S 上关于 $\circ$ 运算的唯一的零元.

零元(续)

与定理 1.1.1 类似,可以证明下面的定理.

定理 1.1.2

设 $\circ$ 为 S 上的二元运算,θ_l 和 θ_r 分别为 $\circ$ 运算的左零元和右零元,则有

$$\theta_l = \theta_r = \theta,$$

且 θ 是 S 上关于 $\circ$ 运算的唯一的零元.

定理 1.1.3

设 $\circ$ 为 S 上的二元运算,e 和 θ 分别为 $\circ$ 运算的单位元和零元. 如果 S 至少有两个元素,那么 $e \neq \theta$.

零元(续)

与定理 1.1.1 类似,可以证明下面的定理.

定理 1.1.2

设 $\circ$ 为 S 上的二元运算,θ_l 和 θ_r 分别为 $\circ$ 运算的左零元和右零元,则有

$$\theta_l = \theta_r = \theta,$$

且 θ 是 S 上关于 $\circ$ 运算的唯一的零元.

定理 1.1.3

设 $\circ$ 为 S 上的二元运算,e 和 θ 分别为 $\circ$ 运算的单位元和零元. 如果 S 至少有两个元素,那么 $e \neq \theta$.

证明.

用反证法. 假设 $e = \theta$,则 $\forall x \in S$ 有

$$x = x \circ e = x \circ \theta = \theta,$$

与 S 中至少含有两个元素矛盾. □

逆元

定义 1.1.10

设 $\circ$ 为 S 上的二元运算，e 为 $\circ$ 运算的单位元，对于 $x \in S$，如果存在 $y_l \in S$(或 $y_r \in S$)，使得

$$y_l \circ x = e \text{ (或 } x \circ y_r = e),$$

那么称 y_l(或 y_r)是 x 的*左逆元*(或*右逆元*). 若 $y \in S$ 既是 x 的左逆元又是 x 的右逆元，则称 y 是 x 的*逆元*. 如果 x 的逆元存在，那么称 x 是*可逆*的.

逆元

定义 1.1.10

设 $\circ$ 为 S 上的二元运算，e 为 $\circ$ 运算的单位元，对于 $x \in S$，如果存在 $y_l \in S$(或 $y_r \in S$)，使得

$$y_l \circ x = e \text{ (或 } x \circ y_r = e),$$

那么称 y_l(或 y_r)是 x 的*左逆元*(或*右逆元*). 若 $y \in S$ 既是 x 的左逆元又是 x 的右逆元，则称 y 是 x 的*逆元*. 如果 x 的逆元存在，那么称 x 是*可逆*的.

在 $\mathbb{N}$ 上只有 0 有加法逆元，就是 0 自己.

在 $\mathbb{Z}$ 上加法的单位元是 0. 对任何整数 x，它的加法逆元都存在，即相反数 $-x$.

在 $n(\geqslant 2)$ 阶实矩阵集 $M_n(\mathbb{R})$ 上，n 阶全 0 矩阵是矩阵加法的单位元. 对任何 n 阶实矩阵 $\boldsymbol{M}$，$-\boldsymbol{M}$ 是 $\boldsymbol{M}$ 的加法逆元，而 n 阶单位矩阵是 $\boldsymbol{M}_n(\mathbb{R})$ 上关于矩阵乘法的单位元. 只有 n 阶实可逆矩阵 $\boldsymbol{M}$ 存在乘法逆元 $\boldsymbol{M}^{-1}$.

在幂集 $P(S)$ 上，对于 $\cup$ 运算，$\emptyset$ 为单位元. 只有 $\emptyset$ 有逆元，就是它本身，其他的元素都没有逆元. 类似地，对于 $\cap$ 运算，S 为单位元，也只有 S 有逆元，即 S 本身，其他元素都没有逆元.

定理 1.1.4

设 $\circ$ 为 S 上可结合的二元运算，e 为该运算的单位元，如果 $x \in S$ 存在左逆元 y_l 和右逆元 y_r，那么有

$$y_l = y_r = y,$$

且 y 是 x 的唯一的逆元.

定理 1.1.4

设 $\circ$ 为 S 上可结合的二元运算，e 为该运算的单位元，如果 $x \in S$ 存在左逆元 y_l 和右逆元 y_r，那么有

$$y_l = y_r = y,$$

且 y 是 x 的唯一的逆元.

证明.

由 $y_l \circ x = e$ 和 $x \circ y_r = e$ 得

$$y_l = y_l \circ e = y_l \circ (x \circ y_r) = (y_l \circ x) \circ y_r = e \circ y_r = y_r.$$

令 $y_l = y_r = y$，则 y 是 x 的逆元. 假设 y' 也是 x 的逆元，则

$$y' = y' \circ e = y' \circ (x \circ y) = (y' \circ x) \circ y = e \circ y = y,$$

所以 y 是 x 的唯一的逆元. □

定理 1.1.4

设 $\circ$ 为 S 上可结合的二元运算，e 为该运算的单位元，如果 $x \in S$ 存在左逆元 y_l 和右逆元 y_r，那么有

$$y_l = y_r = y,$$

且 y 是 x 的唯一的逆元.

证明.

由 $y_l \circ x = e$ 和 $x \circ y_r = e$ 得

$$y_l = y_l \circ e = y_l \circ (x \circ y_r) = (y_l \circ x) \circ y_r = e \circ y_r = y_r.$$

令 $y_l = y_r = y$，则 y 是 x 的逆元. 假设 y' 也是 x 的逆元，则

$$y' = y' \circ e = y' \circ (x \circ y) = (y' \circ x) \circ y = e \circ y = y,$$

所以 y 是 x 的唯一的逆元. □

由定理 1.1.4 可知，对于可结合的二元运算来说，可逆的元素 x 只有唯一的逆元，通常把它记作 x^{-1}.

消去律

定义 1.1.11

设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x, y, z \in S$，以下条件成立：

1. 若 $x \circ y = x \circ z$ 且 $x \neq \theta$，则 $y = z$；
2. 若 $y \circ x = z \circ x$ 且 $x \neq \theta$，则 $y = z$；

那么称 $\circ$ 运算满足 *消去律*，其中 *(1)* 称作 *左消去律*，*(2)* 称作 *右消去律*.

消去律

定义 1.1.11

设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x, y, z \in S$，以下条件成立：

1. 若 $x \circ y = x \circ z$ 且 $x \neq \theta$，则 $y = z$；
2. 若 $y \circ x = z \circ x$ 且 $x \neq \theta$，则 $y = z$；

那么称 $\circ$ 运算满足 *消去律*，其中 *(1)* 称作 *左消去律*，*(2)* 称作 *右消去律*.

注意被消去的 x 不能是运算的零元 θ.

整数集合上的加法和乘法都满足消去律.

幂集 $P(S)$ 上的并和交运算一般不满足消去律. $\forall A, B, C \in P(S)$，由 $A \cup B = A \cup C$ 不一定能得到 $B = C$.

消去律

定义 1.1.11

设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x, y, z \in S$，以下条件成立：

1. 若 $x \circ y = x \circ z$ 且 $x \neq \theta$，则 $y = z$；
2. 若 $y \circ x = z \circ x$ 且 $x \neq \theta$，则 $y = z$；

那么称 $\circ$ 运算满足 *消去律*，其中 *(1)* 称作 *左消去律*，*(2)* 称作 *右消去律*.

注意被消去的 x 不能是运算的零元 θ.

整数集合上的加法和乘法都满足消去律.

幂集 $P(S)$ 上的并和交运算一般不满足消去律. $\forall A, B, C \in P(S)$，由 $A \cup B = A \cup C$ 不一定能得到 $B = C$.

但对称差运算满足消去律. $\oplus$ 运算不存在零元，$\forall A, B, C \in P(S)$，都有

$$A \oplus B = A \oplus C \Rightarrow B = C,$$
$$B \oplus A = C \oplus A \Rightarrow B = C.$$

例 1.1.6

对于下面给定的集合和该集合上的二元运算，指出该运算的性质，并求出它的单位元、零元和所有可逆元素的逆元.

1. $\mathbb{Z}^+,\ \forall x, y \in \mathbb{Z}^+,\ x * y = \mathrm{lcm}(x, y)$，即求 x 和 y 的最小公倍数.
2. $\mathbb{Q},\ \forall x, y \in \mathbb{Q},\ x * y = x + y - xy.$

例 1.1.6

对于下面给定的集合和该集合上的二元运算，指出该运算的性质，并求出它的单位元、零元和所有可逆元素的逆元.

1. $\mathbb{Z}^+,\ \forall x, y \in \mathbb{Z}^+,\ x * y = \mathrm{lcm}(x, y)$，即求 x 和 y 的最小公倍数.
2. $\mathbb{Q},\ \forall x, y \in \mathbb{Q},\ x * y = x + y - xy.$

解

(1) $*$ 运算可交换，可结合，是幂等的.

$\forall x \in \mathbb{Z}^+, x * 1 = x, 1 * x = x,$ 故 1 为单位元.

不存在零元.

只有 1 有逆元，是它自己，其他正整数无逆元.

例 1.1.6

对于下面给定的集合和该集合上的二元运算，指出该运算的性质，并求出它的单位元、零元和所有可逆元素的逆元.

1. $\mathbb{Z}^+,\ \forall x, y \in \mathbb{Z}^+,\ x * y = \mathrm{lcm}(x, y)$，即求 x 和 y 的最小公倍数.
2. $\mathbb{Q},\ \forall x, y \in \mathbb{Q},\ x * y = x + y - xy.$

解

(1) $*$ 运算可交换，可结合，是幂等的.

$\forall x \in \mathbb{Z}^+, x * 1 = x, 1 * x = x,$ 故 1 为单位元.

不存在零元.

只有 1 有逆元，是它自己，其他正整数无逆元.

(2) $*$ 运算满足交换律，因为 $\forall x, y \in \mathbb{Q}$，有

$$x * y = x + y - xy = y + x - yx = y * x.$$

$*$ 运算满足结合律，因为 $\forall x, y, z \in \mathbb{Q}$，有

$$(x * y) * z = (x + y - xy) * z = x + y + z - xy - xz - yz + xyz,$$
$$x * (y * z) = x * (y + z - yz) = x + y + z - xy - xz - yz + xyz,$$

例1.1.6(续)

所以 $(x * y) * z = x * (y * z)$.

$*$ 运算不满足幂等律,因为 $2 \in \mathbb{Q}$,但

$$2 * 2 = 2 + 2 - 2 \times 2 = 0 \neq 2.$$

$*$ 运算满足消去律. 因为 $\forall x, y, z \in \mathbb{Q}$, 当 $x \neq 1$(1 为零元,见后)时,若 $x * y = x * z$,则有 $x + y - xy = x + z - xz$,即 $(y - z) = x(y - z)$,故有 $y = z$,所以左消去律成立. 由于 $*$ 是可交换的,所以右消去律也成立.

例1.1.6(续)

所以 $(x * y) * z = x * (y * z)$.

$*$ 运算不满足幂等律,因为 $2 \in \mathbb{Q}$,但

$$2 * 2 = 2 + 2 - 2 \times 2 = 0 \neq 2.$$

$*$ 运算满足消去律. 因为 $\forall x, y, z \in \mathbb{Q}$, 当 $x \neq 1$(1 为零元,见后)时,若 $x * y = x * z$,则有 $x + y - xy = x + z - xz$,即 $(y - z) = x(y - z)$,故有 $y = z$,所以左消去律成立. 由于 $*$ 是可交换的,所以右消去律也成立.

$\forall x \in \mathbb{Q}$,有 $x * 0 = x = 0 * x$, 故 0 是 $*$ 运算的单位元.

$\forall x \in \mathbb{Q}$,有 $x * 1 = 1 = 1 * x$, 故 1 是 $*$ 运算的零元.

$\forall x \in \mathbb{Q}$,欲使 $x * y = 0$ 和 $y * x = 0$ 成立,即

$$x + y - xy = 0,$$

解得

$$y = \frac{x}{x - 1}, \ x \neq 1.$$

从而知,$x \neq 1$ 时 x 可逆,$x^{-1} = \frac{x}{x-1}$. □

例 1.1.7

设 $A = \{a, b, c\}$, A 上的二元运算 $*, \circ, \cdot$ 如下表所示. 分别说明 3 个运算是否满足交换律、结合律、消去律和幂等律，并求出单位元、零元和可逆元素的逆元.

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

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

$\cdot$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

例 1.1.7

设 $A = \{a, b, c\}$, A 上的二元运算 $*, \circ, \cdot$ 如下表所示. 分别说明 3 个运算是否满足交换律、结合律、消去律和幂等律, 并求出单位元、零元和可逆元素的逆元.

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

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

$\cdot$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

解

$*$ 运算满足交换律、结合律和消去律, 不满足幂等律. 单位元是 a, 没有零元, 且 $a^{-1} = a, b^{-1} = c, c^{-1} = b$.

$\circ$ 运算满足交换律、结合律和幂等律, 不满足消去律. 单位元是 a, 零元是 b. 只有 a 有逆元, $a^{-1} = a$.

$\cdot$ 运算不满足交换律, 满足结合律和幂等律, 不满足消去律. 没有单位元, 没有零元, 没有可逆元素. □

12.2 代数系统

定义 1.2.1

非空集合 S 和 S 上 k 个一元或二元运算 $f_1, f_2, \cdots, f_k$ 组成的系统称作一个 代数系统，简称为 代数，记作 $\langle S, f_1, f_2, \cdots, f_k \rangle$.

12.2 代数系统

定义 1.2.1

非空集合 S 和 S 上 k 个一元或二元运算 $f_1, f_2, \cdots, f_k$ 组成的系统称作一个 代数系统，简称为 代数，记作 $\langle S, f_1, f_2, \cdots, f_k \rangle$.

例如，$\langle \mathbb{N}, + \rangle, \langle \mathbb{Z}, +, \cdot \rangle, \langle \mathbb{R}, +, \cdot \rangle$ 都是代数系统，其中 $+$ 和 $\cdot$ 分别表示普通加法和乘法.

$\langle M_n(\mathbb{R}), +, \cdot \rangle$ 是代数系统，其中 $+$ 和 $\cdot$ 分别表示 $n(\geqslant 2)$ 阶实矩阵的加法和乘法.

$\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ 是代数系统，其中 $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$，$\oplus$ 和 $\otimes$ 分别表示模 n 加法和模 n 乘法，即 $\forall x, y \in \mathbb{Z}_n$，

$$x \oplus y = (x + y) \mod n, \quad x \otimes y = xy \mod n.$$

$\langle P(S), \cup, \cap, \sim \rangle$ 也是代数系统，其中含有两个二元运算 $\cup$ 和 $\cap$ 以及一个一元运算 $\sim$.

在某些代数系统中存在着一些特定的元素，它们对该系统的一元或二元运算起着重要的作用，如二元运算的单位元和零元.

在某些代数系统中存在着一些特定的元素，它们对该系统的一元或二元运算起着重要的作用，如二元运算的单位元和零元.

在定义代数系统时，如果把含有这样的特定元素也作为系统的性质，例如，规定系统的二元运算必须含有单位元，那么在这种情况下称这些元素为该代数系统的 特异元素 或 代数常数 .

在某些代数系统中存在着一些特定的元素，它们对该系统的一元或二元运算起着重要的作用，如二元运算的单位元和零元.

在定义代数系统时，如果把含有这样的特定元素也作为系统的性质，例如，规定系统的二元运算必须含有单位元，那么在这种情况下称这些元素为该代数系统的 特异元素 或 代数常数 .

有时为了强调某个代数系统是含有代数常数的系统，也可以把这些代数常数列到系统的表达式中. 例如，$\langle \mathbb{Z}, + \rangle$ 中的 $+$ 运算有单位元 0，为了强调 0 的存在，将 $\langle \mathbb{Z}, + \rangle$ 记作 $\langle \mathbb{Z}, +, 0 \rangle$. 又如 $\langle P(S), \cup, \cap, \sim \rangle$ 中的 $\cup$ 和 $\cap$ 运算存在单位元 $\emptyset$ 和 S，当规定 $\emptyset$ 和 S 是该系统的代数常数时，也可将它记为 $\langle P(S), \cup, \cap, \sim, \emptyset, S \rangle$. 当然，在不发生混淆的情况下，为了叙述的简便也常用集合的名字来标记代数系统. 例如，上述代数系统可以简记为 $\mathbb{Z}$ 和 $P(S)$.

在某些代数系统中存在着一些特定的元素，它们对该系统的一元或二元运算起着重要的作用，如二元运算的单位元和零元.

在定义代数系统时，如果把含有这样的特定元素也作为系统的性质，例如，规定系统的二元运算必须含有单位元，那么在这种情况下称这些元素为该代数系统的 特异元素 或 代数常数 .

有时为了强调某个代数系统是含有代数常数的系统，也可以把这些代数常数列到系统的表达式中. 例如，$\langle \mathbb{Z}, + \rangle$ 中的 $+$ 运算有单位元 0，为了强调 0 的存在，将 $\langle \mathbb{Z}, + \rangle$ 记作 $\langle \mathbb{Z}, +, 0 \rangle$. 又如 $\langle P(S), \cup, \cap, \sim \rangle$ 中的 $\cup$ 和 $\cap$ 运算存在单位元 $\emptyset$ 和 S，当规定 $\emptyset$ 和 S 是该系统的代数常数时，也可将它记为 $\langle P(S), \cup, \cap, \sim, \emptyset, S \rangle$. 当然，在不发生混淆的情况下，为了叙述的简便也常用集合的名字来标记代数系统. 例如，上述代数系统可以简记为 $\mathbb{Z}$ 和 $P(S)$.

定义 1.2.2

如果两个代数系统中运算的个数相同，对应运算的元数相同，且代数常数的个数也相同，那么称这两个代数系统 具有相同的构成成分 ，也称它们是 同类型 的代数系统.

例如，

$$V_1 = \langle \mathbb{R}, +, \cdot, -, 0, 1 \rangle,$$
$$V_2 = \langle P(B), \cup, \cap, \sim, \emptyset, B \rangle,$$

是同类型的代数系统，它们都含有两个二元运算、一个一元运算和两个代数常数.

例如，

$$V_1 = \langle \mathbb{R}, +, \cdot, -, 0, 1 \rangle,$$
$$V_2 = \langle P(B), \cup, \cap, \sim, \emptyset, B \rangle,$$

是同类型的代数系统，它们都含有两个二元运算、一个一元运算和两个代数常数. 同类型的代数系统仅仅是具有相同的构成成分，不一定具有相同的运算性质. 上述的 V_1 和 V_2 是同类型的代数系统，但它们的运算性质却很不一样，如表 1.2.1 所示. 如果同类型的两个代数系统具有共同的运算性质，那么称它们是 *同种的* .

表 1.2.1

V_1	V_2
$+$ 和 $\cdot$ 可交换，可结合	$\cup$ 和 $\cap$ 可交换，可结合
$\cdot$ 对 $+$ 可分配	$\cup$ 和 $\cap$ 互相可分配
$+$ 和 $\cdot$ 不满足幂等律	$\cup$ 和 $\cap$ 都满足幂等律
$+$ 和 $\cdot$ 不满足吸收律	$\cup$ 和 $\cap$ 都满足吸收律
$+$ 和 $\cdot$ 都满足消去律	$\cup$ 和 $\cap$ 一般不满足消去律

在规定了一个代数系统的构成成分，即集合、运算以及代数常数以后，如果再对这些运算所遵从的算律加以限制，那么满足这些条件的代数系统就具有完全相同的性质，从而构成了一类特殊的代数系统.

在规定了一个代数系统的构成成分，即集合、运算以及代数常数以后，如果再对这些运算所遵从的算律加以限制，那么满足这些条件的代数系统就具有完全相同的性质，从而构成了一类特殊的代数系统.

例如，代数系统 $V = \langle S, \circ \rangle$，其中 $\circ$ 是一个可结合的二元运算，就代表了一类特殊的代数系统——半群. 如 $\langle \mathbb{Z}, + \rangle, \langle \mathbb{R}, + \rangle, \langle M_n(\mathbb{R}), \cdot \rangle, \langle P(B), \cup \rangle$ 等都是半群.

在规定了一个代数系统的构成成分，即集合、运算以及代数常数以后，如果再对这些运算所遵从的算律加以限制，那么满足这些条件的代数系统就具有完全相同的性质，从而构成了一类特殊的代数系统.

例如，代数系统 $V = \langle S, \circ \rangle$，其中 $\circ$ 是一个可结合的二元运算，就代表了一类特殊的代数系统——半群. 如 $\langle \mathbb{Z}, + \rangle, \langle \mathbb{R}, + \rangle, \langle M_n(\mathbb{R}), \cdot \rangle, \langle P(B), \cup \rangle$ 等都是半群.

又如代数系统 $V = \langle S, \circ, * \rangle$，其中 $\circ$ 和 $*$ 是二元运算，并满足交换律、结合律、幂等律和吸收律，那么代表了另一类特殊的代数系统——格. 实际中的代数系统 $\langle \mathbb{Z}^+, \mathrm{lcm}, \gcd \rangle, \langle P(B), \cup, \cap \rangle$ 等都是格，这里的 lcm 和 $\gcd$ 分别表示求两个正整数的最小公倍数和最大公因数的运算.

在规定了一个代数系统的构成成分，即集合、运算以及代数常数以后，如果再对这些运算所遵从的算律加以限制，那么满足这些条件的代数系统就具有完全相同的性质，从而构成了一类特殊的代数系统.

例如，代数系统 $V = \langle S, \circ \rangle$，其中 $\circ$ 是一个可结合的二元运算，就代表了一类特殊的代数系统——半群. 如 $\langle \mathbb{Z}, + \rangle, \langle \mathbb{R}, + \rangle, \langle M_n(\mathbb{R}), \cdot \rangle, \langle P(B), \cup \rangle$ 等都是半群.

又如代数系统 $V = \langle S, \circ, * \rangle$，其中 $\circ$ 和 $*$ 是二元运算，并满足交换律、结合律、幂等律和吸收律，那么代表了另一类特殊的代数系统——格. 实际中的代数系统 $\langle \mathbb{Z}^+, \mathrm{lcm}, \gcd \rangle, \langle P(B), \cup, \cap \rangle$ 等都是格，这里的 lcm 和 $\gcd$ 分别表示求两个正整数的最小公倍数和最大公因数的运算.

从代数系统的构成成分和遵从的算律出发，将代数系统分类，然后研究每一类代数系统的共同性质，并将研究的结果运用到具体的代数系统中去，这种方法就是抽象代数的基本方法，也是代数结构课程的主要内容.

在规定了一个代数系统的构成成分，即集合、运算以及代数常数以后，如果再对这些运算所遵从的算律加以限制，那么满足这些条件的代数系统就具有完全相同的性质，从而构成了一类特殊的代数系统.

例如，代数系统 $V = \langle S, \circ \rangle$，其中 $\circ$ 是一个可结合的二元运算，就代表了一类特殊的代数系统——半群. 如 $\langle \mathbb{Z}, + \rangle, \langle \mathbb{R}, + \rangle, \langle M_n(\mathbb{R}), \cdot \rangle, \langle P(B), \cup \rangle$ 等都是半群.

又如代数系统 $V = \langle S, \circ, * \rangle$，其中 $\circ$ 和 $*$ 是二元运算，并满足交换律、结合律、幂等律和吸收律，那么代表了另一类特殊的代数系统——格. 实际中的代数系统 $\langle \mathbb{Z}^+, \mathrm{lcm}, \gcd \rangle, \langle P(B), \cup, \cap \rangle$ 等都是格，这里的 lcm 和 gcd 分别表示求两个正整数的最小公倍数和最大公因数的运算.

从代数系统的构成成分和遵从的算律出发，将代数系统分类，然后研究每一类代数系统的共同性质，并将研究的结果运用到具体的代数系统中去，这种方法就是抽象代数的基本方法，也是代数结构课程的主要内容.

由已知的代数系统可以通过系统的方法构成新的代数系统，即子代数和积代数. 这些代数系统能够保持或者基本上保持原有代数系统的良好性质.

子代数

定义 1.2.3

设 $V = \langle S, f_1, f_2, \cdots, f_k \rangle$ 是代数系统，$B \subseteq S$，如果 B 对运算 $f_1, f_2, \cdots, f_k$ 都是封闭的，且 B 和 S 含有相同的代数常数，那么称 $\langle B, f_1, f_2, \cdots, f_k \rangle$ 是 V 的子代数系统，简称为子代数. 有时将子代数系统简记为 B.

子代数

定义 1.2.3

设 $V = \langle S, f_1, f_2, \cdots, f_k \rangle$ 是代数系统，$B \subseteq S$，如果 B 对运算 $f_1, f_2, \cdots, f_k$ 都是封闭的，且 B 和 S 含有相同的代数常数，那么称 $\langle B, f_1, f_2, \cdots, f_k \rangle$ 是 V 的子代数系统，简称为子代数. 有时将子代数系统简记为 B.

例如，$\mathbb{N}$ 是 $\langle \mathbb{Z}, + \rangle$ 的子代数，因为 $\mathbb{N}$ 对加法运算 $+$ 是封闭的. $\mathbb{N}$ 也是 $\langle \mathbb{Z}, +, 0 \rangle$ 的子代数，因为 $\mathbb{N}$ 对加法运算 $+$ 封闭，且 $\mathbb{N}$ 中含有代数常数 0. $\mathbb{N} - \{0\}$ 是 $\langle \mathbb{Z}, + \rangle$ 的子代数，但不是 $\langle \mathbb{Z}, +, 0 \rangle$ 的子代数，因为 $\langle \mathbb{Z}, +, 0 \rangle$ 的代数常数 $0 \notin \mathbb{N} - \{0\}$.

从子代数定义不难看出，子代数和原代数不仅具有相同的构成成分，是同类型的代数系统，而且对应的二元运算都具有相同的运算性质.

子代数

定义 1.2.3

设 $V = \langle S, f_1, f_2, \cdots, f_k \rangle$ 是代数系统，$B \subseteq S$，如果 B 对运算 $f_1, f_2, \cdots, f_k$ 都是封闭的，且 B 和 S 含有相同的代数常数，那么称 $\langle B, f_1, f_2, \cdots, f_k \rangle$ 是 V 的子代数系统，简称为子代数. 有时将子代数系统简记为 B.

例如，$\mathbb{N}$ 是 $\langle \mathbb{Z}, + \rangle$ 的子代数，因为 $\mathbb{N}$ 对加法运算 $+$ 是封闭的. $\mathbb{N}$ 也是 $\langle \mathbb{Z}, +, 0 \rangle$ 的子代数，因为 $\mathbb{N}$ 对加法运算 $+$ 封闭，且 $\mathbb{N}$ 中含有代数常数 0. $\mathbb{N} - \{0\}$ 是 $\langle \mathbb{Z}, + \rangle$ 的子代数，但不是 $\langle \mathbb{Z}, +, 0 \rangle$ 的子代数，因为 $\langle \mathbb{Z}, +, 0 \rangle$ 的代数常数 $0 \notin \mathbb{N} - \{0\}$.

从子代数定义不难看出，子代数和原代数不仅具有相同的构成成分，是同类型的代数系统，而且对应的二元运算都具有相同的运算性质.

对任何代数系统 $V = \langle S, f_1, f_2, \cdots, f_k \rangle$，其子代数一定存在. 最大子代数就是 V 本身. 如果 V 中所有代数常数构成的集合对 V 中所有的运算都是封闭的，那么它构成了 V 的最小子代数. 这种最大和最小子代数称为 V 的平凡子代数.

若 B 是 S 的真子集，则 B 构成的子代数称为 V 的真子代数.

例 1.2.1

设 $V = \langle \mathbb{Z}, +, 0 \rangle$, 令

$$n\mathbb{Z} = \{nz | z \in \mathbb{Z}\},\ n \text{ 为自然数},$$

则 $n\mathbb{Z}$ 是 V 的子代数.

例 1.2.1

设 $V = \langle \mathbb{Z}, +, 0 \rangle$, 令

$$n\mathbb{Z} = \{nz | z \in \mathbb{Z}\},\ n \text{ 为自然数},$$

则 $n\mathbb{Z}$ 是 V 的子代数.

证明.

任取 $n\mathbb{Z}$ 中的两个元素 $nz_1, nz_2, z_1, z_2 \in \mathbb{Z}$, 则有

$$nz_1 + nz_2 = n(z_1 + z_2) \in n\mathbb{Z},$$

即 $n\mathbb{Z}$ 对 $+$ 运算是封闭的.

又

$$0 = n \cdot 0 \in n\mathbb{Z},$$

所以, $n\mathbb{Z}$ 是 V 的子代数.

当 $n = 1$ 或 $n = 0$ 时, $n\mathbb{Z}$ 是 V 的平凡子代数, 其他都是 V 的非平凡的真子代数. □

积代数

定义 1.2.4

设 $V_1 = \langle A, \circ \rangle$ 和 $V_2 = \langle B, * \rangle$ 是同类型的代数系统，$\circ$ 和 $*$ 为二元运算，在集合 $A \times B$ 上定义二元运算 $\cdot$ 如下.

$$\forall \langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \in A \times B,$$

有

$$\langle a_1, b_1 \rangle \cdot \langle a_2, b_2 \rangle = \langle a_1 \circ a_2, b_1 * b_2 \rangle,$$

称 $V = \langle A \times B, \cdot \rangle$ 为 V_1 与 V_2 的积代数，记作 $V_1 \times V_2$. 这时也称 V_1 和 V_2 为 V 的因子代数.

易见积代数与它的因子代数是同类型的代数系统.

例 1.2.2

设 V_1 和 V_2 分别为模 *3* 加法和模 *2* 加法的代数系统，即 $V_1 = \langle \mathbb{Z}_3, \oplus_3 \rangle$，$V_2 = \langle \mathbb{Z}_2, \oplus_2 \rangle$，给出 $V_1 \times V_2$ 的运算表，并说明它的运算是否满足交换律与结合律，是否具有单位元.

例 1.2.2

设 V_1 和 V_2 分别为模 3 加法和模 2 加法的代数系统，即 $V_1 = \langle \mathbb{Z}_3, \oplus_3 \rangle$，$V_2 = \langle \mathbb{Z}_2, \oplus_2 \rangle$，给出 $V_1 \times V_2$ 的运算表，并说明它的运算是否满足交换律与结合律，是否具有单位元.

解

运算表如下表所示.

$\oplus$	$\langle 0,0 \rangle$	$\langle 0,1 \rangle$	$\langle 1,0 \rangle$	$\langle 1,1 \rangle$	$\langle 2,0 \rangle$	$\langle 2,1 \rangle$
$\langle 0,0 \rangle$	$\langle 0,0 \rangle$	$\langle 0,1 \rangle$	$\langle 1,0 \rangle$	$\langle 1,1 \rangle$	$\langle 2,0 \rangle$	$\langle 2,1 \rangle$
$\langle 0,1 \rangle$	$\langle 0,1 \rangle$	$\langle 0,0 \rangle$	$\langle 1,1 \rangle$	$\langle 1,0 \rangle$	$\langle 2,1 \rangle$	$\langle 2,0 \rangle$
$\langle 1,0 \rangle$	$\langle 1,0 \rangle$	$\langle 1,1 \rangle$	$\langle 2,0 \rangle$	$\langle 2,1 \rangle$	$\langle 0,0 \rangle$	$\langle 0,1 \rangle$
$\langle 1,1 \rangle$	$\langle 1,1 \rangle$	$\langle 1,0 \rangle$	$\langle 2,1 \rangle$	$\langle 2,0 \rangle$	$\langle 0,1 \rangle$	$\langle 0,0 \rangle$
$\langle 2,0 \rangle$	$\langle 2,0 \rangle$	$\langle 2,1 \rangle$	$\langle 0,0 \rangle$	$\langle 0,1 \rangle$	$\langle 1,0 \rangle$	$\langle 1,1 \rangle$
$\langle 2,1 \rangle$	$\langle 2,1 \rangle$	$\langle 2,0 \rangle$	$\langle 0,1 \rangle$	$\langle 0,0 \rangle$	$\langle 1,1 \rangle$	$\langle 1,0 \rangle$

$V_1 \times V_2$ 中的 $\oplus$ 运算满足交换律、结合律，单位元是 $\langle 0,0 \rangle$. □

定理 1.2.1

设 $V_1 = \langle A, \circ \rangle$ 和 $V_2 = \langle B, * \rangle$ 是同类型的代数系统，$V_1 \times V_2 = \langle A \times B, \cdot \rangle$ 是它们的积代数.

1. 如果 $\circ$ 和 $*$ 运算是可交换(可结合、幂等)的，那么 $\cdot$ 运算也是可交换(可结合、幂等)的；
2. 如果 e_1 和 e_2(θ_1 和 θ_2)分别为 $\circ$ 和 $*$ 运算的单位元(零元)，那么 $\langle e_1, e_2 \rangle$ ($\langle \theta_1, \theta_2 \rangle$) 也是 $\cdot$ 运算的单位元(零元)；
3. 如果 x 和 y 分别为 $\circ$ 和 $*$ 运算的可逆元素，那么 $\langle x, y \rangle$ 也是 $\cdot$ 运算的可逆元素，其逆元就是 $\langle x^{-1}, y^{-1} \rangle$.

定理 1.2.1

设 $V_1 = \langle A, \circ \rangle$ 和 $V_2 = \langle B, * \rangle$ 是同类型的代数系统，$V_1 \times V_2 = \langle A \times B, \cdot \rangle$ 是它们的积代数.

1. 如果 $\circ$ 和 $*$ 运算是可交换(可结合、幂等)的，那么 $\cdot$ 运算也是可交换(可结合、幂等)的；
2. 如果 e_1 和 e_2(θ_1 和 θ_2)分别为 $\circ$ 和 $*$ 运算的单位元(零元)，那么 $\langle e_1, e_2 \rangle$ ($\langle \theta_1, \theta_2 \rangle$) 也是 $\cdot$ 运算的单位元(零元)；
3. 如果 x 和 y 分别为 $\circ$ 和 $*$ 运算的可逆元素，那么 $\langle x, y \rangle$ 也是 $\cdot$ 运算的可逆元素，其逆元就是 $\langle x^{-1}, y^{-1} \rangle$.

证明.

这里只证明 (1) 中的结合律，(2) 中的单位元.

(1) 任取 $\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle, \langle a_3, b_3 \rangle \in V_1 \times V_2$，

$$
\begin{aligned}
&(\langle a_1, b_1 \rangle \cdot \langle a_2, b_2 \rangle) \cdot \langle a_3, b_3 \rangle \\
=\ &\langle a_1 \circ a_2, b_1 * b_2 \rangle \cdot \langle a_3, b_3 \rangle \\
=\ &\langle (a_1 \circ a_2) \circ a_3, (b_1 * b_2) * b_3 \rangle \\
=\ &\langle a_1 \circ (a_2 \circ a_3), b_1 * (b_2 * b_3) \rangle \\
=\ &\langle a_1, b_1 \rangle \cdot \langle a_2 \circ a_3, b_2 * b_3 \rangle \\
=\ &\langle a_1, b_1 \rangle \cdot (\langle a_2, b_2 \rangle \cdot \langle a_3, b_3 \rangle).
\end{aligned}
$$

(2) 任取 $\langle a, b \rangle \in V_1 \times V_2$，

$$
\begin{aligned}
\langle a, b \rangle \cdot \langle e_1, e_2 \rangle &= \langle a \circ e_1, b * e_2 \rangle = \langle a, b \rangle, \\
\langle e_1, e_2 \rangle \cdot \langle a, b \rangle &= \langle e_1 \circ a, e_2 * b \rangle = \langle a, b \rangle,
\end{aligned}
$$

因此 $\langle e_1, e_2 \rangle$ 是关于 $\cdot$ 运算的单位元. □

积代数的定义可以推广到具有多个运算的同类型的代数系统.

在具有两个不同二元运算的情况下,使用与定理 1.2.1 中类似的方法不难证明:积代数也保留因子代数中的分配律和吸收律等性质. 但是消去律是一个例外. 请看下面的例子.

积代数的定义可以推广到具有多个运算的同类型的代数系统.
在具有两个不同二元运算的情况下,使用与定理 1.2.1 中类似的方法不难证明:积代数也保留因子代数中的分配律和吸收律等性质. 但是消去律是一个例外. 请看下面的例子.

例 1.2.3

设 $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$,其中 n 是正整数, $V_1 = \langle \mathbb{Z}_4, \otimes_4 \rangle$, $V_2 = \langle \mathbb{Z}_3, \otimes_3 \rangle$ 分别表示模 4 乘法和模 3 乘法的代数系统,那么 V_1 和 V_2 中的运算都满足消去律. 考虑积代数 $\langle V_1 \times V_2, \otimes \rangle$,这里的 $\otimes$ 运算不满足消去律. 因为在 $V_1 \times V_2$ 中有

$$\langle 2, 0 \rangle \otimes \langle 0, 2 \rangle = \langle 0, 0 \rangle = \langle 2, 0 \rangle \otimes \langle 0, 0 \rangle,$$

且 $\langle 2, 0 \rangle$ 不是零元,如果 $\otimes$ 运算满足消去律,那么在上式中用消去律将 $\langle 2, 0 \rangle$ 消去,就得到 $\langle 0, 2 \rangle = \langle 0, 0 \rangle$,显然这是矛盾的. □

12.3 同态与同构

在同种的代数系统中，有些系统在结构上更为相似，甚至完全一样. 例如，$V_1 = \langle \mathbb{Z}_3, \oplus_3 \rangle$, $V_2 = \langle A, \oplus_6 \rangle$，其中 $\mathbb{Z}_3 = \{0, 1, 2\}$, $A = \{0, 2, 4\}$，$\oplus_3$ 和 $\oplus_6$ 分别表示模 3 加法和模 6 加法. 这两个代数系统的运算表如表 1.3.1 和表 1.3.2 所示.

表 1.3.1

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

表 1.3.2

$\oplus_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

12.3 同态与同构

在同种的代数系统中，有些系统在结构上更为相似，甚至完全一样. 例如，$V_1 = \langle \mathbb{Z}_3, \oplus_3 \rangle$, $V_2 = \langle A, \oplus_6 \rangle$，其中 $\mathbb{Z}_3 = \{0, 1, 2\}$, $A = \{0, 2, 4\}$，$\oplus_3$ 和 $\oplus_6$ 分别表示模 3 加法和模 6 加法. 这两个代数系统的运算表如表 1.3.1 和表 1.3.2 所示.

表 1.3.1

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

表 1.3.2

$\oplus_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

把表 1.3.1 中的 1 和 2 分别替换成 2 和 4，就可以得到表 1.3.2. 这个替换可以表示成函数：

$$f = \{\langle 0, 0\rangle, \langle 1, 2\rangle, \langle 2, 4\rangle\}.$$

在双射函数 f 的作用下，代数系统 V_1 转换成了 V_2. 直观上它们具有同样的结构，都是抽象代数系统 $\{a, b, c\}$ 的实例.

同态

定义 1.3.1

设 $V_1 = \langle A, \circ \rangle$ **和** $V_2 = \langle B, * \rangle$ **是同类型的代数系统**, $f : A \to B$, **且** $\forall x, y \in A$ **有**

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

则称 f **是** V_1 **到** V_2 **的** 同态映射 , **简称为** 同态 .

同态

定义 1.3.1

设 $V_1 = \langle A, \circ \rangle$ 和 $V_2 = \langle B, * \rangle$ 是同类型的代数系统，$f : A \to B$，且 $\forall x, y \in A$ 有

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

则称 f 是 V_1 到 V_2 的同态映射，简称为同态.

根据同态映射的性质可以将同态分为单同态、满同态和同构，即：同态映射 f 如果是单射，那么称作单同态；如果是满射，那么称作满同态，这时称 V_2 是 V_1 的同态像；如果 f 是双射，那么称作同构，也称代数系统 V_1 同构于 V_2，记作 $V_1 \cong V_2$.

如果同态映射 f 是 V 到 V 的，那么称 f 为自同态.

类似地，可以定义单自同态、满自同态和自同构.

同态映射 f 具有许多良好的性质. 设 f 是 $V_1 = \langle A, \circ \rangle$ 到 $V_2 = \langle B, * \rangle$ 的同态映射.

首先, 如果 $\circ$ 运算具有交换律、结合律、幂等律等, 那么在同态像 $f(V_1)$ 中, $*$ 运算也具有相同的算律(注意, 消去律可能有例外).

同态映射 f 具有许多良好的性质. 设 f 是 $V_1 = \langle A, \circ \rangle$ 到 $V_2 = \langle B, * \rangle$ 的同态映射.

首先,如果 $\circ$ 运算具有交换律、结合律、幂等律等,那么在同态像 $f(V_1)$ 中,$*$ 运算也具有相同的算律(注意,消去律可能有例外).

此外,同态映射 f 恰好把 V_1 的单位元 e_1 映射到 V_2 的单位元 e_2,即 $f(e_1) = e_2$.

同样对于零元和可逆元也有

$$f(\theta_1) = \theta_2,\ f(x^{-1}) = f(x)^{-1}.$$

同态映射 f 具有许多良好的性质. 设 f 是 $V_1 = \langle A, \circ \rangle$ 到 $V_2 = \langle B, * \rangle$ 的同态映射.

首先,如果 $\circ$ 运算具有交换律、结合律、幂等律等,那么在同态像 $f(V_1)$ 中,$*$ 运算也具有相同的算律(注意,消去律可能有例外).

此外,同态映射 f 恰好把 V_1 的单位元 e_1 映射到 V_2 的单位元 e_2,即 $f(e_1) = e_2$.

同样对于零元和可逆元也有

$$f(\theta_1) = \theta_2,\ f(x^{-1}) = f(x)^{-1}.$$

上述关于同态映射的定义可以推广到具有有限多个运算的代数系统. 例如,对于具有两个二元运算的代数系统 $V_1 = \langle A, \circ_1, \circ_2 \rangle$ 和 $V_2 = \langle B, *_1, *_2 \rangle, f : A \to B$,如果 $\forall x, y \in A$,有

$$f(x \circ_1 y) = f(x) *_1 f(y),$$
$$f(x \circ_2 y) = f(x) *_2 f(y),$$

那么 f 是 V_1 到 V_2 的同态映射.

例 1.3.1

(1) **设代数系统** $V_1 = \langle \mathbb{Z}, + \rangle$, $V_2 = \langle \mathbb{Z}_n, \oplus \rangle$, **其中** $\mathbb{Z}$ **为整数集合**, $+$ **为普通加法**; $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$, $\oplus$ **为模** n **加法. 令**

$$f : \mathbb{Z} \to \mathbb{Z}_n,\ f(x) = x \mod n,$$

那么 f **是** V_1 **到** V_2 **的满同态. 事实上, 显然** f **是满射, 且** $\forall x, y \in \mathbb{Z}$ **有**

$$f(x+y) = (x+y) \mod n = (x \mod n) \oplus (y \mod n) = f(x) \oplus f(y).$$

例 1.3.1

(1) 设代数系统 $V_1 = \langle \mathbb{Z}, + \rangle$, $V_2 = \langle \mathbb{Z}_n, \oplus \rangle$, 其中 $\mathbb{Z}$ 为整数集合, $+$ 为普通加法; $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$, $\oplus$ 为模 n 加法. 令

$$f : \mathbb{Z} \to \mathbb{Z}_n,\ f(x) = x \mod n,$$

那么 f 是 V_1 到 V_2 的满同态. 事实上, 显然 f 是满射, 且 $\forall x, y \in \mathbb{Z}$ 有

$$f(x+y) = (x+y) \mod n = (x \mod n) \oplus (y \mod n) = f(x) \oplus f(y).$$

(2) 设 $V_1 = \langle \mathbb{R}, + \rangle$, $V_2 = \langle \mathbb{R}^*, \cdot \rangle$, 其中 $\mathbb{R}$ 和 $\mathbb{R}^*$ 分别为实数集与非零实数集, $+$ 和 $\cdot$ 分别表示普通加法与乘法. 令

$$f : \mathbb{R} \to \mathbb{R}^*,\ f(x) = \mathrm{e}^x,$$

则 f 是 V_1 到 V_2 的单同态.
事实上, 易见 f 是单射, 且 $\forall x, y \in \mathbb{R}$ 有

$$f(x+y) = \mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y = f(x) \cdot f(y).$$

例1.3.1(续)

(3) 设 $V = \langle \mathbb{Z}, + \rangle$, 其中 $\mathbb{Z}$ 为整数集, $+$ 为普通加法. $\forall a \in \mathbb{Z}$, 令

$$f_a : \mathbb{Z} \to \mathbb{Z},\ f_a(x) = ax,$$

那么 f_a 是 V 的自同态.

例1.3.1(续)

(3) 设 $V = \langle \mathbb{Z}, + \rangle$, 其中 $\mathbb{Z}$ 为整数集, $+$ 为普通加法. $\forall a \in \mathbb{Z}$, 令

$$f_a : \mathbb{Z} \to \mathbb{Z},\ f_a(x) = ax,$$

那么 f_a 是 V 的自同态.

事实上, 因为 $\forall x, y \in \mathbb{Z}$, 有

$$\begin{aligned} f_a(x+y) &= a(x+y) \\ &= ax + ay \\ &= f_a(x) + f_a(y), \end{aligned}$$

即 $f_a(x+y) = f_a(x) + f_a(y)$.

当 $a = 0$ 时称 f_0 为零同态; 当 $a = \pm 1$ 时, f_a 是自同构; 除此之外, 其他的 f_a 都是单自同态. □

例 1.3.2

设 $V = \langle \mathbb{Z}_n, \oplus \rangle$, 其中 $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$, $\oplus$ 为模 n 加法. 证明恰有 n 个 V 的自同态.

例 1.3.2

设 $V = \langle \mathbb{Z}_n, \oplus \rangle$, 其中 $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$, $\oplus$ 为模 n 加法. 证明恰有 n 个 V 的自同态.

证明.

先证存在着 n 个 V 的自同态. 令

$$f_p : \mathbb{Z}_n \to \mathbb{Z}_n,\ f_p(x) = px \mod n,\ p = 0, 1, \cdots, n-1,$$

则 f_p 是 V 的自同态, 因为 $\forall x, y \in \mathbb{Z}_n$ 有

$$\begin{aligned} f_p(x \oplus y) &= p(x \oplus y) \mod n \\ &= (px \mod n) \oplus (py \mod n) \\ &= f_p(x) \oplus f_p(y). \end{aligned}$$

由于 p 有 n 种取值, 不同的 p 确定了不同的映射 f_p, 所以存在 n 个 V 的自同态.

例1.3.2(续)

下面证明任何 V 的自同态都是上述 n 个自同态中的一个. 设 f 是 V 的自同态, 且 $f(1)=i, i\in\{0,1,\cdots,n-1\}$. 需证明 $\forall x\in\mathbb{Z}_n$, 有 $f(x)=ix \mod n$, 即 $f=f_i$. 事实上, 若 $x\in\{1,2,\cdots,n-1\}$, 则有

$$
\begin{aligned}
f(x) &= f(\underbrace{1\oplus 1\oplus\cdots\oplus 1}_{x\text{个}1}) \\
&= \underbrace{f(1)\oplus f(1)\oplus\cdots\oplus f(1)}_{x\text{个}f(1)} \\
&= \underbrace{i\oplus i\oplus\cdots\oplus i}_{x\text{个}i} \\
&= ix \mod n.
\end{aligned}
$$

例1.3.2(续)

下面证明任何 V 的自同态都是上述 n 个自同态中的一个. 设 f 是 V 的自同态, 且 $f(1)=i, i\in\{0,1,\cdots,n-1\}$. 需证明 $\forall x\in\mathbb{Z}_n$, 有 $f(x)=ix \mod n$, 即 $f=f_i$. 事实上, 若 $x\in\{1,2,\cdots,n-1\}$, 则有

$$\begin{aligned} f(x) &= f(\underbrace{1\oplus 1\oplus\cdots\oplus 1}_{x\text{个}1}) \\ &= \underbrace{f(1)\oplus f(1)\oplus\cdots\oplus f(1)}_{x\text{个}f(1)} \\ &= \underbrace{i\oplus i\oplus\cdots\oplus i}_{x\text{个}i} \\ &= ix \mod n. \end{aligned}$$

另外, 也有

$$\begin{aligned} f(0) &= f((n-1)\oplus 1) = f(n-1)\oplus f(1) \\ &= (i(n-1) \mod n)\oplus i = in \mod n \\ &= 0 = i\cdot 0 \mod n. \end{aligned}$$

一个进程代数的描述实例

下面介绍代数系统在计算机科学中的一个重要的研究领域——进程代数(process algebra).

例 1.3.3

利用进程代数可以对使用通信实现交互的并发系统建模,*20* 世纪 *80* 年代发展起来的通信系统演算(*Calculus of Communicating Systems*, *CCS*)便是这方面的典型代表.

一个进程代数的描述实例

下面介绍代数系统在计算机科学中的一个重要的研究领域——进程代数 (process algebra).

例 1.3.3

利用进程代数可以对使用通信实现交互的并发系统建模, *20* 世纪 *80* 年代发展起来的通信系统演算(*Calculus of Communicating Systems*, *CCS*)便是这方面的典型代表.

下面是一个自动售货机的例子. 简单起见, 这里假设该售货机只为顾客提供咖啡和茶. 系统中的进程由动作 *coin*, *coffee* 和 *tea* 构成.

为了更好地描述交互, 通常将动作细分为互补的输入和输出动作. 例如, 如果 *coin*, *coffee* 和 *tea* 分别表示"接收硬币""取走咖啡"和"取走茶", 那么对应的输出动作 $\overline{coin}$, $\overline{coffee}$ 和 $\overline{tea}$ 将分别表示"投入硬币""提供咖啡"和"提供茶".

除了输入和输出动作外, 还有一个特别的动作, 即外部不可见的动作, 笼统地用 τ 表示.

一个进程代数的描述实例(续)

这些动作构成原子进程. 自动售货机 M 的进程可以定义为$!\mathrm{coin}.(\overline{\mathrm{coffee}}+\overline{\mathrm{tea}})$, 购买咖啡的顾客 C 的进程可以定义为 $!\overline{\mathrm{coin}}.\mathrm{coffee}$, 这里符号"!"表示其后的进程可以重复执行, 符号"+"表示在该符号前后两个进程中选择一个执行.
自动售货机 M 与顾客 C 的交互可以用下面的进程描述.

$$\mathrm{M}|\mathrm{C}=!\mathrm{coin}.(\overline{\mathrm{coffee}}+\overline{\mathrm{tea}})|!\overline{\mathrm{coin}}.\mathrm{coffee}$$

该进程在顾客投入硬币、自动售货机接收硬币后, 转化为进程

$$(\overline{\mathrm{coffee}}+\overline{\mathrm{tea}})|!\mathrm{coin}.(\overline{\mathrm{coffee}}+\overline{\mathrm{tea}})|\mathrm{coffee}|!\overline{\mathrm{coin}}.\mathrm{coffee}$$

进而, 在自动售货机提供咖啡、顾客取走咖啡后, 系统还原为进程 M|C.
另外, 也可以在 M|C 外加上约束$(\mathrm{new\ coin},\mathrm{coffee},\mathrm{tea})$, 即$(\mathrm{new\ coin},\mathrm{coffee},\mathrm{tea})(\mathrm{M}|\mathrm{C})$, 该约束限定 coin, coffee, tea 等动作只能在系统 M|C 内部发生.

一个进程代数的描述实例(续)

利用这些算子,加上表示空进程的零元算子 0,可以构造出 CCS 的所有进程. 进程集合 A 和给定的 A 上的算子构成了代数系统——CCS.

更明确地,CCS 中有 6 个算子:$0, ., +, |, (\text{new}\ \tilde{a})$ 和!,具体说明如下.

$0 :\to A$,称作空进程,表示进程终止.

$. : A \times A \to A$ 称作顺序,运算结果得到的 $a.b$ 是个组合进程,a 后面顺序执行 b.

$+ : A \times A \to A$,称作选择,$a + b$ 表示在 a 与 b 中选择一个进程来执行,同时放弃另外一个.

$| : A \times A \to A$,称作并行,$a|b$ 是把 a 与 b 的并行执行看成一个新进程,当一个分支有输出动作,另外一个分支有同名的输入动作时,两个分支可以通信.

$(\text{new}\ \tilde{a}) : A \to A$,称作限制,表示动作集合 $\tilde{a}$ 里的动作不能与外界交互.

$! : A \to A$,称作重复,表示可以不断执行.

所有进程及算子构成进程代数 $\langle A, 0, ., +, |, (\text{new}\ \tilde{a}), ! \rangle$.

为使得表达式更为简洁,上述算子的优先级规定如下.

$$. > | > +, ! > | > +, (\text{new}\ \tilde{a}) > | > +$$

一个进程代数的描述实例(续)

设 x, y, z 是 CCS 中的任意进程，可以证明进程代数 CCS 的一些主要算律.
选择运算满足交换律和结合律，即 $x + y = y + x, (x + y) + z = x + (y + z)$.
并行运算满足交换律和结合律，即 $x|y = y|x, (x|y)|z = x|(y|z)$.
0 是 $+$ 和 $|$ 运算的单位元，即

$$0 + x = x, \quad x + 0 = x, \quad x|0 = x, \quad 0|x = x.$$

利用进程代数可以分析通信并发系统的性质，也可以通过互模拟来研究系统之间行为的等价性，从而在保证系统性能的前提下进一步简化系统，实现预定的设计目标.