

离散数学

代数结构

9.2 代数系统

9.2 代数系统

- 代数系统定义
- 同类型与同种的代数系统
- 子代数
- 积代数
- 同态与同构

代数系统定义与实例

- 定义

- 非空集合 S 和 S 上 k 个一元或二元运算 f_1, f_2, \dots, f_k 组成的系统称为一个代数系统, 简称代数, 记做 $V = \langle S, f_1, f_2, \dots, f_k \rangle$ 。
- S 称为代数系统的载体, S 和运算叫做代数系统的成分。
- 有的代数系统定义指定了 S 中的特殊元素, 称为代数常数, 例如二元运算的单位元。有时也将代数常数作为系统的成分。

实例

- $\langle \mathbf{N}, + \rangle$, $\langle \mathbf{Z}, +, \cdot \rangle$, $\langle \mathbf{R}, +, \cdot \rangle$ 是代数系统,
+ 和 \cdot 分别表示普通加法和乘法。
- $\langle M_n(\mathbf{R}), +, \cdot \rangle$ 是代数系统,
+ 和 \cdot 分别表示 n 阶 ($n \geq 2$) 实矩阵的加法和乘法。
- $\langle \mathbf{Z}_n, \oplus, \otimes \rangle$ 是代数系统, $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$,
 \oplus 和 \otimes 分别表示模 n 的加法和乘法, $\forall x, y \in \mathbf{Z}_n$,
$$x \oplus y = (x + y) \bmod n, \quad x \otimes y = (xy) \bmod n$$
- $\langle P(S), \cup, \cap, \sim \rangle$ 也是代数系统,
 \cup 和 \cap 为并和交, \sim 为绝对补

同类型与同种代数系统

- 定义

(1) 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，则称它们是同类型的代数系统。

(2) 如果两个同类型的代数系统规定的运算性质也相同，则称为同种的代数系统。

例1 $V_1 = \langle \mathbf{R}, +, \cdot, 0, 1 \rangle$,

$V_2 = \langle M_n(\mathbf{R}), +, \cdot, \theta, E \rangle$, θ 为 n 阶全 0 矩阵, E 为 n 阶单位矩阵

$V_3 = \langle P(B), \cup, \cap, \emptyset, B \rangle$

同类型与同种代数系统（续）

V_1	V_2	V_3
+ 可交换, 可结合 • 可交换, 可结合 + 满足消去律 • 满足消去律 • 对+可分配 + 对• 不可分配 + 与• 没有吸收律	+ 可交换, 可结合 • 可交换, 可结合 + 满足消去律 • 满足消去律 • 对+可分配 + 对• 不可分配 + 与• 没有吸收律	∪ 可交换, 可结合 ∩ 可交换, 可结合 ∪ 不满足消去律 ∩ 不满足消去律 ∩ 对 ∪ 可分配 ∪ 对 ∩ 可分配 ∪ 与 ∩ 满足吸收律

- V_1, V_2, V_3 是同类型的代数系统
- V_1, V_2 是同种的代数系统
- V_1, V_2 与 V_3 不是同种的代数系统

子代数

- **定义** 设 $V = \langle S, f_1, f_2, \dots, f_k \rangle$ 是代数系统, B 是 S 的非空子集, 如果 B 对 f_1, f_2, \dots, f_k 都是封闭的, 且 B 和 S 含有相同的代数常数, 则称 $\langle B, f_1, f_2, \dots, f_k \rangle$ 是 V 的子代数系统, 简称 **子代数**。有时将子代数系统简记为 B 。
- **实例** \mathbb{N} 是 $\langle \mathbb{Z}, + \rangle$ 和 $\langle \mathbb{Z}, +, 0 \rangle$ 的子代数。 $\mathbb{N} - \{0\}$ 是 $\langle \mathbb{Z}, + \rangle$ 的子代数, 但不是 $\langle \mathbb{Z}, +, 0 \rangle$ 的子代数
- **说明:**
- 子代数和原代数是同种的代数系统
- 对于任何代数系统 V , 其子代数一定存在。

关于子代数的术语

- 最大的子代数 就是 V 本身。
- 如果 V 中所有代数常数构成集合 B ，且 B 对 V 中所有运算封闭，则 B 就构成了 V 的最小的子代数。
- 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2 设 $V = \langle \mathbb{Z}, +, 0 \rangle$ ，令 $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ ， n 为自然数，则 $n\mathbb{Z}$ 是 V 的子代数，当 $n = 1$ 和 0 时， $n\mathbb{Z}$ 是 V 的平凡子代数，其他的都是 V 的非平凡的真子代数。

积代数

定义 设 $V_1 = \langle S_1, \circ \rangle$ 和 $V_2 = \langle S_2, * \rangle$ 是代数系统，其中 \circ 和 $*$ 是二元运算。 V_1 与 V_2 的 **积代数** 是 $V = \langle S_1 \times S_2, \cdot \rangle$,

$$\forall \langle x_1, y_1 \rangle, \langle x_2, y_2 \rangle \in S_1 \times S_2,$$

$$\langle x_1, y_1 \rangle \cdot \langle x_2, y_2 \rangle = \langle x_1 \circ x_2, y_1 * y_2 \rangle$$

例3 $V_1 = \langle \mathbb{Z}, + \rangle$, $V_2 = \langle M_2(\mathbb{R}), \cdot \rangle$, 积代数 $\langle \mathbb{Z} \times M_2(\mathbb{R}), \circ \rangle$

$$\forall \langle z_1, M_1 \rangle, \langle z_2, M_2 \rangle \in \mathbb{Z} \times M_2(\mathbb{R}),$$

$$\langle z_1, M_1 \rangle \circ \langle z_2, M_2 \rangle = \langle z_1 + z_2, M_1 \cdot M_2 \rangle$$

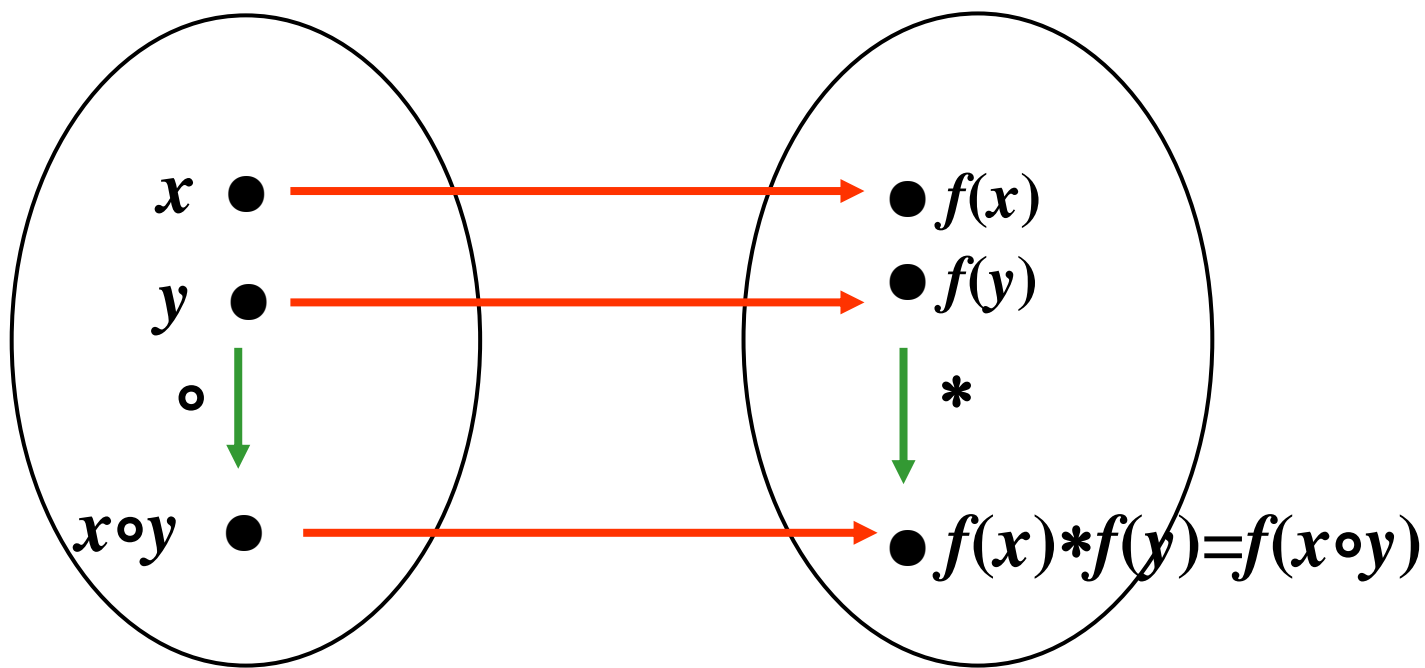
$$\langle 5, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \rangle \circ \langle -2, \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} \rangle = \langle 3, \begin{pmatrix} 2 & -1 \\ 2 & 0 \end{pmatrix} \rangle$$

积代数的性质

- 设 $V_1 = \langle S_1, \circ \rangle$ 和 $V_2 = \langle S_2, * \rangle$ 是代数系统，其中 \circ 和 $*$ 是二元运算。 V_1 与 V_2 的积代数是 $V = \langle S_1 \times S_2, \cdot \rangle$
 - (1) 若 \circ 和 $*$ 运算是可交换的，那么 \cdot 运算也是可交换的
 - (2) 若 \circ 和 $*$ 运算是可结合的，那么 \cdot 运算也是可结合的
 - (3) 若 \circ 和 $*$ 运算是幂等的，那么 \cdot 运算也是幂等的
 - (4) 若 \circ 和 $*$ 运算分别具有单位元 e_1 和 e_2 ，那么 \cdot 运算也具有单位元 $\langle e_1, e_2 \rangle$
 - (5) 若 \circ 和 $*$ 运算分别具有零元 θ_1 和 θ_2 ，那么 \cdot 运算也具有零元 $\langle \theta_1, \theta_2 \rangle$
 - (6) 若 x 关于 \circ 的逆元为 x^{-1} , y 关于 $*$ 的逆元为 y^{-1} ，那么 $\langle x, y \rangle$ 关于 \cdot 运算也具有逆元 $\langle x^{-1}, y^{-1} \rangle$

同态映射的定义

- **定义** 设 $V_1 = \langle S_1, \circ \rangle$ 和 $V_2 = \langle S_2, * \rangle$ 是代数系统，其中 \circ 和 $*$ 是二元运算。 $f: S_1 \rightarrow S_2$ ，且 $\forall x, y \in S_1, f(x \circ y) = f(x) * f(y)$ ，则称 f 为 V_1 到 V_2 的**同态映射**，简称**同态**。



更广泛的同态映射定义

- **定义** 设 $V_1 = \langle S_1, \circ, \cdot \rangle$ 和 $V_2 = \langle S_2, *, \diamond \rangle$ 是代数系统, 其中 \circ 、 $*$ 、 \cdot 和 \diamond 都是二元运算。 $f: S_1 \rightarrow S_2$, 且 $\forall x, y \in S_1$

$$f(x \circ y) = f(x) * f(y), \quad f(x \cdot y) = f(x) \diamond f(y)$$

则称 f 为 V_1 到 V_2 的**同态映射**, 简称**同态**。

- **定义** 设 $V_1 = \langle S_1, \circ, \cdot, \Delta \rangle$ 和 $V_2 = \langle S_2, *, \diamond, \nabla \rangle$ 是代数系统, 其中 \circ 和 $*$ 是二元运算。 Δ 和 ∇ 是一元运算, $f: S_1 \rightarrow S_2$, 且 $\forall x, y \in S_1$

$$f(x \circ y) = f(x) * f(y), \quad f(x \cdot y) = f(x) \diamond f(y), \quad f(\Delta x) = \nabla f(x)$$

则称 f 为 V_1 到 V_2 的**同态映射**, 简称**同态**。

特殊同态映射的分类

- 同态映射如果是单射，则称为**单同态**；
- 如果是满射，则称为**满同态**，这时称 V_2 是 V_1 的**同态像**，记作 $V_1 \sim V_2$ ；
- 如果是双射，则称为**同构**，也称代数系统 V_1 同构于 V_2 ，记作 $V_1 \cong V_2$ 。
- 对于代数系统 V ，它到自身的同态称为**自同态**。
- 类似地可以定义**单自同态**、**满自同态**和**自同构**。

例题

例1 $V=\langle \mathbf{R}^*, \cdot \rangle$, 判断下面的哪些函数是 V 的自同态?

$$(1) f(x)=|x| \quad (2) f(x)=2x \quad (3) f(x)=x^2$$

$$(4) f(x)=1/x \quad (5) f(x)=-x \quad (6) f(x)=x+1$$

解 (2), (5), (6) 不是自同态。

$$(1) \text{ 是同态, } f(x \cdot y) = |x \cdot y| = |x| \cdot |y| = f(x) \cdot f(y)$$

$$(3) \text{ 是同态, } f(x \cdot y) = (x \cdot y)^2 = x^2 \cdot y^2 = f(x) \cdot f(y)$$

$$(4) \text{ 是同态, } f(x \cdot y) = 1/(x \cdot y) = 1/x \cdot 1/y = f(x) \cdot f(y)$$

同态映射的实例

例2 设 $V = \langle \mathbb{Z}, + \rangle$, $\forall a \in \mathbb{Z}$, 令 $f_a: \mathbb{Z} \rightarrow \mathbb{Z}$, $f_a(x) = ax$ 那么 f_a 是 V 的自同态。

- 因为 $\forall x, y \in \mathbb{Z}$, 有

$$f_a(x+y) = a(x+y) = ax+ay = f_a(x)+f_a(y)$$

当 $a = 0$ 时称 f_0 为零同态;

当 $a = \pm 1$ 时, 称 f_a 为自同构;

除此之外其他的 f_a 都是单自同态。

同态映射的实例（续）

例3 设 $V_1 = \langle \mathbb{Q}, + \rangle$, $V_2 = \langle \mathbb{Q}^*, \cdot \rangle$, 其中 $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, 令

$$f: \mathbb{Q} \rightarrow \mathbb{Q}^*, f(x) = e^x$$

那么 f 是 V_1 到 V_2 的同态映射,

- 因为 $\forall x, y \in \mathbb{Q}$ 有

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

不难看出 f 是单同态。

同态映射的实例（续）

例4 $V_1 = \langle \mathbb{Z}, + \rangle$, $V_2 = \langle \mathbb{Z}_n, \oplus \rangle$, $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$, \oplus 是模 n 加。

令 $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$, $f(x) = (x) \bmod n$

则 f 是 V_1 到 V_2 的同态映射。

- $\forall x, y \in \mathbb{Z}$ 有

$$\begin{aligned} f(x+y) &= (x+y) \bmod n \\ &= (x) \bmod n \oplus (y) \bmod n \\ &= f(x) \oplus f(y) \end{aligned}$$

- 不难看出 f 是满同态。

同态映射的实例（续）

例5 设 $V = \langle \mathbb{Z}_n, \oplus \rangle$, \oplus 是模 n 加。可以证明恰有 n 个 V 的自同态 f_p :
 $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$

$$f_p(x) = (px) \bmod n, \quad p = 0, 1, \dots, n-1$$

例如 $n = 6$, 那么

f_0 为零同态;

f_1 与 f_5 为同构;

f_2 与 f_4 的同态像是 $\{0, 2, 4\}$;

f_3 的同态像是 $\{0, 3\}$ 。

同态映射保持运算的算律

设 V_1, V_2 是代数系统。 $\circ, *$ 是 V_1 上的二元运算， $\circ', *'$ 是 V_2 上对应的二元运算，如果 $f: V_1 \rightarrow V_2$ 是满同态，那么

- (1) 若 \circ 运算是可交换的（可结合、幂等的），则 \circ' 运算也是可交换的（可结合、幂等的）。
- (2) 若 \circ 运算对 $*$ 运算是可分配的，则 \circ' 运算对 $*$ '运算也是可分配的；若 \circ 和 $*$ 运算是可吸收的，则 \circ' 和 $*$ '运算也是可吸收的。

同态映射保持运算的特异元素

(3) 若 e 为 \circ 运算的单位元, 则 $f(e)$ 为 \circ' 运算的单位元。

(4) 若 θ 为 \circ 运算的零元, 则 $f(\theta)$ 为 \circ' 运算的零元。

(5) 设 $u \in V_1$, 若 u^{-1} 是 u 关于 \circ 运算的逆元, 则 $f(u^{-1})$ 是 $f(u)$ 关于 \circ' 运算的逆元。

同态映射的性质

- 说明：
- 上述性质仅在满同态时成立，如果不是满同态，那么相关性质在同态像中成立。
- 同态映射不一定能保持消去律成立。
- 例如 $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$ 是 $V_1 = \langle \mathbb{Z}, \cdot \rangle$ 到 $V_2 = \langle \mathbb{Z}_n, \otimes \rangle$ 的同态， $f(x) = (x) \bmod n$ ， V_1 中满足消去律，但是当 n 为合数时， V_2 中不满足消去律。

例题

- 例6 设 $V_1 = \langle \mathbb{Q}, + \rangle$, $V_2 = \langle \mathbb{Q}^*, \cdot \rangle$, 其中 \mathbb{Q} 为有理数集合, $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $+$ 和 \cdot 分别表示普通加法和乘法。证明不存在 V_2 到 V_1 的同构。

证 假设 f 是 V_2 到 V_1 的同构, 那么有 $f: V_2 \rightarrow V_1$, $f(1) = 0$ 。于是有

$$f(-1) + f(-1) = f((-1)(-1)) = f(1) = 0$$

从而 $f(-1) = 0$, 又有 $f(1) = 0$, 这与 f 的单射性矛盾。

问题？

