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 $f_1, f_2, \ldots, f_k$ 组成的系统称为一个代数系统, 简称代数，记做 $V=<S, f_1, f_2, \ldots, f_k>$。

- 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

- $<\mathbf{N},+>$, $<\mathbf{Z},+,\cdot>$, $<\mathbf{R},+,\cdot>$是代数系统，
  $+$ 和 $\cdot$ 分别表示普通加法和乘法。
- $<M_n(\mathbf{R}),+,\cdot>$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。
- $<\mathbf{Z}_n,\oplus,\otimes>$是代数系统，$\mathbf{Z}_n=\{0, 1, \ldots, n-1\}$，
  $\oplus$ 和 $\otimes$ 分别表示模 n 的加法和乘法，$\forall x,y\in \mathbf{Z}_n$，
  $x\oplus y = (x+y) \bmod n$，$x\otimes y = (xy) \bmod n$
- $<P(S),\cup,\cap,\sim>$ 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

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

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$V=<S, f_1, f_2, \ldots, f_k>$ 是代数系统，B 是 S 的非空子集，如果 B 对 $f_1, f_2, \ldots, f_k$ 都是封闭的，且 B 和 S 含有相同的代数常数，则称 $<B, f_1, f_2, \ldots, f_k>$ 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 N是<Z,+> 和<Z,+,0>的子代数。 N–{0}是<Z,+>的子代数，但不是<Z,+,0>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的平凡的子代数。
- 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=<Z,+,0>，令 $nZ = \{ nz \mid z \in Z\}$，$n$ 为自然数，则 nZ 是 V 的子代数，当 $n = 1$ 和 0 时，nZ 是 V 的平凡的子代数，其他的都是 V 的非平凡的真子代数。

积代数

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

$\forall <x_1, y_1>, <x_2, y_2>\in S_1\times S_2$,

$<x_1,y_1>\cdot<x_2,y_2>=<x_1\circ x_2, y_1 * y_2>$

例3 $V_1=<Z,+>$, $V_2=<M_2(R),\cdot>$, 积代数$<Z\times M_2(R),\circ>$

$\forall <z_1,M_1>, <z_2,M_2>\in Z\times M_2(R)$,

$<z_1,M_1>\circ<z_2,M_2> = <z_1+z_2, M_1\cdot M_2>$

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

积代数的性质

- 设 $V_1 = <S_1,\circ>$和 $V_2 = <S_2,*>$是代数系统，其中 $\circ$ 和 $*$是二元运算。V_1 与 V_2 的积代数是 $V=<S_1\times S_2,\cdot>$

  (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

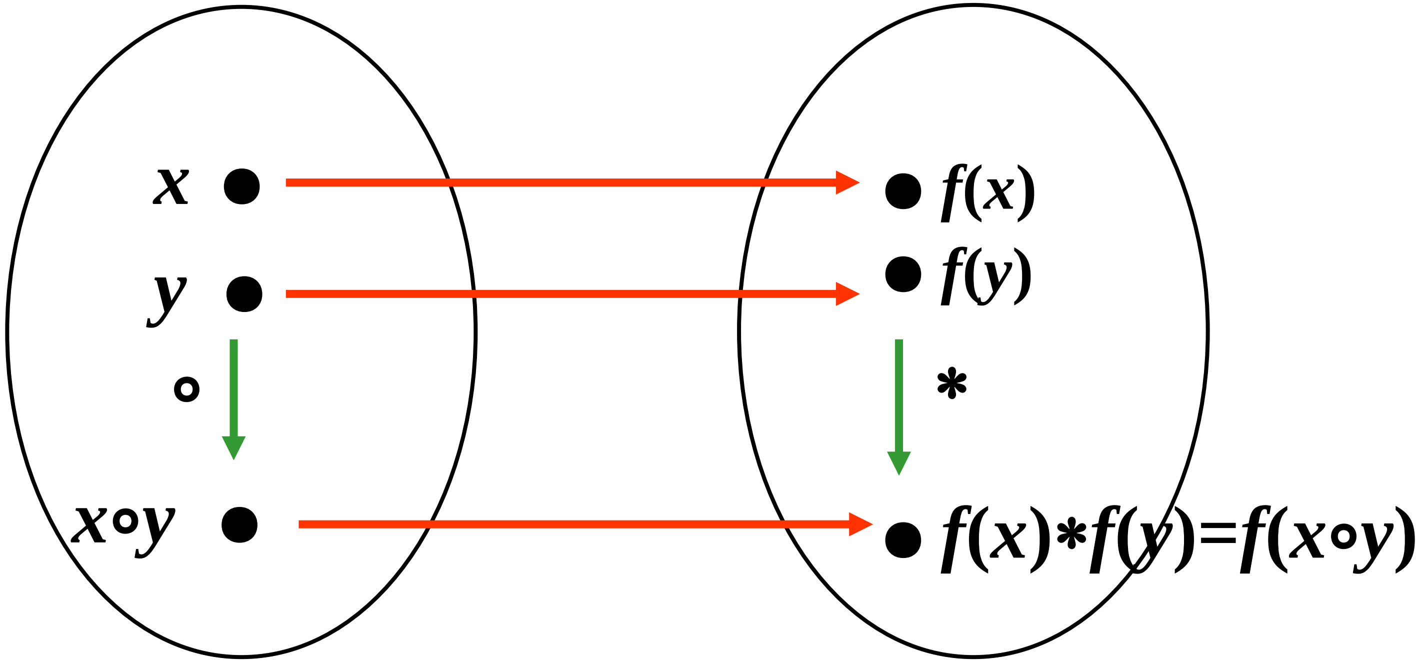
  (4) 若 $\circ$ 和 $*$ 运算分别具有单位元 e_1 和 e_2，那么$\cdot$ 运算也具有单位元 $<e_1,e_2>$

  (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$<\theta_1,\theta_2>$

  (6) 若 x 关于 $\circ$ 的逆元为 x^{-1}, y 关于 $*$ 的逆元为 y^{-1}，那么$<x,y>$关于$\cdot$ 运算也具有逆元$<x^{-1},y^{-1}>$

同态映射的定义

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

  $$f(x\circ y)=f(x)*f(y)\text{，}\quad f(x\cdot y)=f(x)\Diamond f(y)$$

  则称 f 为V_1到 V_2 的同态映射，简称同态。

- 定义 设 $V_1=<S_1,\circ,\cdot,\Delta>$和 $V_2=<S_2,*,\Diamond,\nabla>$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=<R*,·>, 判断下面的哪些函数是V 的自同态?

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

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

解 (2) , (5), (6) 不是自同态。

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

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

(4) 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=<Z,+>，$\forall a \in$Z，令 f_a：Z→Z，f_a(x)=ax，那么 f_a是V的自同态。

- 因为$\forall x,y \in$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=<Q,+>, V_2= <Q*,·>，其中Q*= Q–{0}，令

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

那么 f 是V_1到V_2的同态映射，

- 因为$\forall x, y \in$ 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=<Z,+>，V_2=<Z_n,⊕ >，Z_n={0,1, … , n-1}, ⊕是模 n 加。

令 f：$Z \to Z_n$，$f(x) = (x) \bmod n$

则 f 是V_1到 V_2 的同态映射。

- $\forall x, y \in Z$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=<Z_n,⊕>，⊕是模 n 加。 可以证明恰有 n 个V 的自同态f_p: $Z_n \to Z_n$， $f_p(x) = (px) \bmod n$，$p = 0,1, \ldots, n-1$

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： $V_1\to V_2$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 $f : Z \to Z_n$ 是 $V_1=<Z,\cdot>$ 到 $V_2=<Z_n,\otimes>$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=<Q,+>，V_2=<Q*,·>，其中 Q 为有理数集合，Q*=Q–{0}，+ 和 · 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：$V_2 \to V_1$， $f(1)=0$。 于是有

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

从而 $f(-1)=0$，又有 $f(1)=0$，这与 f 的单射性矛盾。

问题？