离散数学

Discrete Mathematics

吴梅红

厦门大学计算机科学系

E-mail: wmh@xmu.edu.cn

5.3 代数系统的同态和同构

- 同态映射是研究代数系统之间相互关系的有力工具。
- 元素运算 的像 等于 元素像 的运算

  是函数与运算的重要联系。

定义 5.16 设$V_1 = \langle A, \circ_1, \circ_2, \ldots, \circ_r \rangle$, $V_2 = \langle B, *_1, *_2, \ldots, *_r \rangle$ 是同类型的代数系统。对于$i = 1, 2, \ldots, r$, $\circ_i$ 和$*_i$是k_i元运算。函数$\varphi: A \to B$, 如果对所有的运算$\circ_i$, $*_i$ 都有

$$\varphi(\circ_i (x_1, x_2, \ldots, x_{ki})) = *_i (\varphi(x_1), \varphi(x_2), \ldots, \varphi(x_{ki}))$$

$$\forall\ x_1, x_2, \ldots, x_{ki} \in A,$$

则称φ是代数系统V_1到V_2的同态映射, 简称同态。▌

- 同态是保持两个同类型代数系统之间运算的映射。
- 对于二元 $\circ$, $*$, 一元 Δ, $\underline{\Delta}$和零元运算 a, a_* , 上述定义中的等式可分别表示为:

$$\varphi(x \circ y) = \varphi(x) * \varphi(y), \qquad \forall x, y \in A,$$

$$\varphi(\Delta x) = \underline{\Delta}\varphi(x), \qquad \forall x \in A,$$

$$\varphi(a) = a_* 。 \qquad /*零元运算, 对应常元$$

- 代数系统V_1中的元素先进行V_1中运算然后再取像,
  与V_1中的元素先取像再进行V_2中相应的运算,
  其运算结果是一样的。
- 或者说V_1和V_2中相对应的元素分别经过相对应运算后的结果仍然保持对应关系。

- 凡能满足定义所给出的条件的函数，都是一个从V_1到V_2的同态。因此从一个代数系统到另一个代数系统可有多个同态(homomorphrism)映射。

例 5.10 设代数系统 $V_1 = \langle Z, + \rangle$, $V_2 = \langle Z_n, \oplus \rangle$,

这里 $Z_n = \{0, 1, \ldots, n - 1\}$, $\oplus$为模n加法。

定义 $\varphi: Z \to Z_n$, $\varphi(x) = (x) \bmod n$,

则 φ为V_1到V_2的同态。 因为 $\forall x, y \in Z$有

$\varphi(x + y)$

$= (x + y) \bmod n = (x) \bmod n \oplus (y) \bmod n$

$= \varphi(x) \oplus \varphi(y)$。

定义 5.17 设$V_1 = <A, \circ_1, \circ_2, \ldots, \circ_r>$, $V_2 = <B, *_1, *_2, \ldots, *_n>$ 是同类型的代数系统。对于$i = 1, 2, \ldots, r$, $\circ_i$ 和$*_i$是k_i元运算。函数$\varphi: A \to B$是从V_1 到V_2 的同态, 则$\varphi(A)$关于V_2中的运算构成V_2的子代数, 称为V_1在φ下的同态像。

例 5.11 设$V_1 = <R, +, 0>$, $V_2 = <R, \cdot, 1>$, 其中R为实数集, +和·分别为普通加法和乘法。

令 $\varphi: R \to R$, $\varphi(x) = e^x$, $\forall x \in R$,

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

φ为V_1到V_2的同态，在φ下的同态像为 $<R^+, \cdot, 1>$, 是$<R, \cdot, 1>$的子代数。 ■

定义5.18 设$V_1 = \langle A, \circ_1, \circ_2, \ldots, \circ_r \rangle$, $V_2 = \langle B, *_1, *_2, \ldots, *_n \rangle$ 是同类型的代数系统, $\varphi: A \to B$是V_1到V_2的同态。

(1) 若$\varphi: A \to B$是满射, 则称φ是满同态(epimorphism),

记为$V_1 \sim V_2$。

f^*满同态 $A \to \varphi(A)$

(2) 若$\varphi: A \to B$是单射, 则称φ是单同态(monomorphism)

(3) 若$\varphi: A \to B$双射, 则称φ是同构(isomorphism),

$V_1 \overset{\varphi}{\cong} V_2$,

记为 这时也称V_1同构于V_2。

(4) 若$V_1 = V_2$, 则称φ是自同态。

若φ 又是双射的则称φ是自同构。

- 如果代数系统V_1同构于V_2, 从抽象代数的观点看, 它们是没有区别的, 是同一个代数系统。

- 同构关系是等价关系, 即自反、对称和可传递。

例 5.12 设$V = <Z, +>$, $c \in Z$ 。定义 $\varphi_a: Z \to Z$,

$\varphi_a(x) = ax$, $\forall x \in Z$, $ax \in Z$ 。 则 $\forall x, y \in Z$ 有

$$\varphi_a(x + y) = a(x + y) = ax + ay = \varphi_a(x) + \varphi_a(y),$$

φ_a 是V上的自同态。

- 当$a = 0$时, $\forall x \in Z$有$\varphi_0(x) = 0$, 称φ_0是零同态。/*单位元

  它不是单同态也不是满同态。

- 当$a = \pm 1$时, 有 $\varphi_1(x) = x$, $\varphi_{-1}(x) = -x$, $\forall x \in Z$。

  φ_1 和 φ_{-1} 是V上的两个自同构。

- 当 $a \neq \pm 1, 0$ 时, $\forall x \in Z$ 有

  $\varphi_a(x) = ax$, φ_a 是V上的单自同态。

例5.12.2 设Σ是有穷字母表, Σ*为Σ上有限长度的串的集合,

空串$\Lambda \in \Sigma^*$。

Σ*和串的连接运算构成代数系统$<\Sigma^*, \circ, \Lambda>$。

令 $\varphi: \Sigma^* \to N$, $\forall w \in \Sigma^*$, $\varphi(w) = |w|$,

则 $\forall w_1, w_2 \in \Sigma^*$ 有

$$\varphi(w_1 \circ w_2) = |w_1 \circ w_2| = |w_1| + |w_2| = \varphi(w_1) + \varphi(w_2),$$

且有 $\varphi(\Lambda) = 0$,

所以 φ是$<\Sigma^*, \circ, \Lambda>$ 到 $<N, +, 0>$的同态, 且为满同态。

- 当Σ 中只含一个字母时, φ为同构。 ■
- 下面讨论同态的性质。

- 不同的代数系统可能具有一些 共同的性质。
- 我们不必一个一个地去研究各个代数系统，

  而是列出一组性质 (如 封闭性、可结合性、有单位元、有零元、每个元有逆元等), 把这一组性质看作是公理, 研究满足这些公理的抽象的代数系统。
- 由这些公理推导出的任何有效的结论 (定理),

  对于满足这组公理的任何代数系统将都是成立的。
- 形象地说, 一个代数系统的同态像可以看作是

  抽去该系统中某些元素的次要特性的情况下,

  对该系统的一种 粗糙描述。

定理 5.5 设$V_1 = \langle A, \circ_1, \circ_2, \ldots, \circ_r \rangle$, $V_2 = \langle B, *_1, *_2, \ldots, *_r \rangle$

是同类型的代数系统。$\varphi: A \to B$是从V_1到V_2的满同态，

$\circ_i$, $\circ_j$是V_1中的两个二元运算。 /*或令$B = \varphi(A)$

(1) 若 $\circ_i$ 是可交换的(或可结合的, 幂等的),

则 $*_i$ 也是可交换的(或可结合的, 幂等的)。

证 $\forall x, y, z \in B$, 因φ是满同态, 所以存在$a, b, c \in A$使得

$$\varphi(a) = x,\ \ \varphi(b) = y,\ \ \varphi(c) = z。$$

$$(x *_i y) *_i z = (\varphi(a) *_i \varphi(b)) *_i \varphi(c) = \varphi(a \circ_i b) *_i \varphi(c)$$

$$= \varphi((a \circ_i b) \circ_i (c)) = \varphi(a \circ_i (b \circ_i c)) = \varphi(a) *_i \varphi(b \circ_i c)$$

$$= \varphi(a) *_i (\varphi(b) *_i \varphi(c)) = x *_i (y *_i z)$$ /*可结合

(2) 若 $\circ_i$ 对 $\circ_j$ 是可分配的, 则 $*_i$ 对 $*_j$ 也是可分配的。

(3) 若 $\circ_i$, $\circ_j$ 是可吸收的, 则 $*_i$, $*_j$ 也是可吸收的。

(4) 若e (或θ)是V_1 中关于 $\circ_i$ 运算的单位元(或零元),

则φ(e)(或φ(θ))是V_2中关于 $*_i$ 运算的单位元(或零元)。

(5) 若$\circ_i$ 是含有单位元的运算, $u^{-1} \in A$是u关于$\circ_i$ 运算的

逆元, 则$\varphi(u^{-1})$是φ(u)关于$*_i$ 运算的逆元, $\varphi(u)^{-1} = \varphi(u^{-1})$.

证 $\varphi(u) *_i \varphi(u^{-1}) = \varphi(u \circ_i u^{-1}) = \varphi(e)$。

$\varphi(u^{-1}) *_i \varphi(u) = \varphi(u^{-1} \circ_i u) = \varphi(e)$。

由逆元的惟一性, 知$\varphi(u^{-1})$是φ(u)关于$*_i$ 运算的逆元。

- 同态保持运算，满同态能保持运算的性质。

- 定理5.5中 φ为满同态的条件很重要。
- 定理5.5 说明与代数系统 V_1 相联系的一些重要公理, 如交换律、结合律、分配律、同一律和可逆律, 在V_1的任何同态像(特别同构像)中能够被保持下来。
- 但V_2 具有的性质未必在V_1中成立。 即 满同态 对 保持性质 是 单向的。
- 需要指出的是, 若φ: $V_1 \to V_2$ 不是一个满同态, 则定理5.5所列出的性质不一定成立。因为这时在V_2 中存在某些元素, 它们不是V_1中任何元素的像。
- 当φ不是满同态时, 定理的结论仅在V_1的同态像φ(A)中成立。研究下面 反例5.13和例5.14。

表5.8

*	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

V_1

∘	0	1	2	3
0	0	1	1	0
1	1	1	2	1
2	1	2	3	2
3	0	1	2	3

V_2

反例 5.13 设代数系统$V_1 = \langle A, *\rangle$, $V_2 = \langle B, \circ\rangle$, 其中 $A = \{a, b, c, d\}$, $B = \{0, 1, 2, 3\}$。*和∘运算由运算表5.8所示, 对称可交换。定义函数$\varphi: A \to B$, $\varphi(a) = 0$, $\varphi(b) = 1$, $\varphi(c) = 0$, $\varphi(d) = 1$。可以验证φ是V_1到V_2的同态。

V_1在φ下的同态像是$\langle\{0, 1\}, \circ\rangle$。不难证明$V_1$的*运算满足结合律, 但$V_2$的∘运算却不满足结合律, 因为有

$(1 \circ 0) \circ 2 = 1 \circ 2 = 2$ 和 $1 \circ (0 \circ 2) = 1 \circ 1 = 1$

例 5.14 设代数系统 $V = <A, \bullet>$, 其中 $A = \{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} | a, d \in R\}$, $\bullet$为矩阵乘法。定义函数 $\varphi: A \to A$,

$\varphi(\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $\forall \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in A$。$\varphi$是A上的自同态,

但不是A上的满自同态, 因为任取$\begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix}$, $\begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix} \in A$有

$$\varphi(\begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix} \bullet \begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix}) = \varphi(\begin{pmatrix} a_1a_2 & 0 \\ 0 & d_1d_2 \end{pmatrix}) = \begin{pmatrix} a_1a_2 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\varphi(\begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix}) \bullet \varphi(\begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix}) = \begin{pmatrix} a_1 & 0 \\ 0 & 0 \end{pmatrix} \bullet \begin{pmatrix} a_2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1a_2 & 0 \\ 0 & 0 \end{pmatrix},$$

所以 $\varphi(\begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix} \bullet \begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix}) = \varphi(\begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix}) \bullet \varphi(\begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix})$。

V在φ下的同态像是$<B, \bullet>$, 其中 $B = \{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} | a \in R\}$。

- 考虑V中关于$\bullet$运算的单位元$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, φ将它映到$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$,

但$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$不是V中的单位元, 而是同态像$<B, \bullet>$的单位元.

- 满同态映射可以 保持代数系统V_1中的许多性质，如交换律、结合律、幂等律、分配律、吸收律等，
- 但对消去律不一定为真。

反例 5.14.2 $V_1 = \langle Z, \bullet\rangle$, $V_2 = \langle Z_6, \otimes\rangle$为代数系统，其中

$Z_6 = \{0, 1, \ldots, 5\}$, $\otimes$为模6乘法。令 $\varphi: Z \to Z_6$。

$\varphi(x) = (x) \bmod 6$, $\forall x \in Z$, 则φ是V_1 到 V_2 的满同态。

- 不难看到，普通乘法•在Z上满足消去律，
- 而 模6乘法$\otimes$ 在Z_6上 不满足消去律。

考虑等式 $2 \otimes 3 = 2 \otimes 0$,

若成立消去律就得到 $3 = 0$, 显然是不对的。

- 子代数概念为我们

  由已知代数系统 作新的代数系统提供了一条思路。

- 积代数和商代数是 构造新系统的两个主要手段。

- **5.2**节提供构造结构更复杂 且保持原代数系统中运算性质的新代数系统 -- 积代数。

***** Omit !** 利用商集和代数系统上的同余关系等概念,

可以构造结构更简单 且保持原代数系统中运算性质的新代数系统 -- 商代数。