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



第六章 几个典型的代数系统

6.1 半群与独异点

定义 6.1 设$\circ$是集合S上的二元运算($\Leftrightarrow$封闭)的代数系统,

(1) 若S是代数系统, 且$\circ$ 是可结合的,

则称 $<S, \circ>$为半群(semigroup);

定义6.2 若S是半群, 且存在 $e\in S$为运算 $\circ$ 的单位元,

则称 $<S, \circ, e>$为独异点(monoid), 也称幺半群/盟;

定义 6.5 若S是独异点, 且每一元素都有逆元,

则称 $<S, \circ, e>$为群(group)。 ■

由上述定义有:

$\{$群$\}\subset\{$独异点$\}\subset\{$半群$\}\subset\{$代数系统(广群)$\}$。

例6.1

(1) N, Z, Q, R关于普通加法和乘法都可以构成半群和独异点; $<Z^+, +>$关于普通乘法可以构成半群和独异点, 而关于普通加法只能构成半群。

(2) 设$n \geq 2$, n阶实矩阵$M_n(R)$关于矩阵加法或矩阵乘法都能构成半群和独异点。

(3) 幂集P(B)关于集合的并、交和对称差运算都可以构成半群和独异点。

(4) A^A关于函数的合成运算构成了半群和独异点。

(5) $A = \{a_1, a_2, \cdots, a_n\}$, $n \in Z^+$, $\circ$ 为A上的二元运算。

$\forall a_i, a_j \in A$有$a_i \circ a_j = a_i$ (左零元), 则A关于$\circ$运算构成半群.

定义 设$V = \langle S, \circ\rangle$ 是半群, $\forall x \in S, n \in Z^+$,

定义x 的n次**幂**x^n 为

$$\begin{cases} x^1 = x, & \\ x^{n+1} = x^n \circ x, & n \in Z^+。 \end{cases} \blacksquare$$

例 在半群$\langle Z, +\rangle$中, $\forall x \in Z$, x的n次幂是

$$\underbrace{x + x + \cdots + x}_{n个x} = nx;$$

- 而在半群$\langle P(B), \oplus\rangle$中, $\forall x \in P(B)$, x 的n 次幂是

$$\underbrace{x \oplus x \oplus \cdots \oplus x}_{n个x} = \begin{cases} \varnothing, & n为偶数; \\ x, & n为奇数。 \end{cases}$$

- 半群中元素的幂运算遵从下面的规律。

定理a 设$V = \langle S, \circ \rangle$是半群, $\forall\, x, y \in S$有

(1) $x^n \circ x^m = x^{n+m}$； 其中$n, m \in Z^+$。

Omit! 证 (1) 固定n, 施归纳于m。

- 若$m = 1$, 则 $x^n \circ x^1 = x^n \circ x = x^{n+1}$。
- 假设对$m = k$有$x^n \circ x^k = x^{n+k}$成立,
- 则对$m = k + 1$有

$$x^n \circ x^{k+1} = x^n \circ (x^k \circ x) = (x^n \circ x^k) \circ x = x^{n+k} \circ x$$

$$= x^{n+k+1} = x^{n+(k+1)},$$

- 根据数学归纳法, 对一切$n, m \in Z^+$, 结论为真。▮

Omit! (2) $(x^n)^m = x^{nm}$，其中n, m $\in Z^+$。

证 (2) 固定n, 施归纳于m。

- $m = 1$时有 $(x^n)^1 = x^{n \cdot 1}$。
- 假设当$m = k$时有$(x^n)^k = x^{nk}$成立,
- 则$m = k + 1$时有

$$(x^n)^{k+1} = (x^n)^k \circ (x^n)^1 = x^{nk} \circ x^n$$

$$= x^{nk+n} \qquad \text{/*由(1)}$$

$$= x^{n(k+1)},$$

根据数学归纳法, 对一切n, m $\in Z^+$, 结论为真。 ▮

- 可以将x的n次幂的概念从半群推广到独异点。
- 在独异点$V = \langle S, \circ, e\rangle$中,

  $\forall x \in S, n \in N$, x的n次幂是:

  $$x^0 = e, \qquad \text{/*对比定义6.2}$$

  $$x^{n+1} = x^n \circ x, \qquad n \in N。$$

- 不难证明定理a 的结论在独异点中也成立,

  只是n, m 不仅限于正整数, 也可以是0。

- 下面考虑半群和独异点T的子代数。 /*定义15.11
- 子代数对所有运算封闭, 尤其是零元运算(常数)。

定义 半群S的子代数叫做S的子半群。

独异点T的子代数叫做T的子独异点。

例 6.2 设 $A = \{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in R\}$, 则A关于矩阵乘法构成半群 $\langle A, \cdot \rangle$, 且它是 $\langle M_2(R), \cdot \rangle$的子半群。

令$V = \langle A, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \rangle$, 则V是一个独异点, 单位元$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

但它不是独异点$\langle M_2(R), \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$的子独异点。

因为$M_2(R)$中关于·运算的单位元$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin A$。

- 半群与独异点的积代数 称为积半群 和 积独异点。
- 有关积代数的定理和性质

  都可以用于积半群与积独异点。　　/*特例
- 类似地, 可以把一般代数系统的 同态的概念用到半群和独异点上,

  对半群和独异点也是正确的。　　/*特例