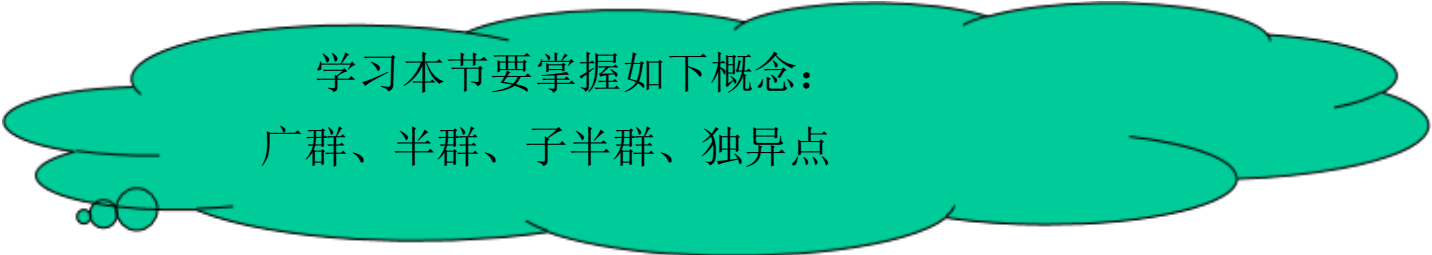


5-3 半群

半群是一种特殊的代数系统，它在形式语言、自动机等领域中，都有具体的应用。



学习本节要掌握如下概念：
广群、半群、子半群、独异点

一、广群

定义5-3.1 一个代数系统 $\langle S, * \rangle$ ，其中 S 是非空集合， $*$ 是 S 上的一个二元运算，如果运算 $*$ 是封闭的，则称代数结构 $\langle S, * \rangle$ 为广群。

二、半群

定义5-3.2 一个代数系统 $\langle S, * \rangle$ ，其中 S 是非空集合， $*$ 是 S 上的一个二元运算，如果：

- (1) 运算 $*$ 是封闭的；
- (2) 运算 $*$ 是可结合的，即对任意的 $x, y, z \in S$ ，满足

$$(x*y)*z = x*(y*z)$$

则称代数结构 $\langle S, * \rangle$ 为半群。

例题1 设集合 $S_k = \{x | x \in I \wedge x \geq k\}, k \geq 0$, 那么 $\langle S_k, + \rangle$ 是一个半群, 其中 $+$ 是普通的加法运算。

解

因为运算 $+$ 在 S_k 上是封闭的, 而且普通加法运算是可结合的。所以, $\langle S_k, + \rangle$ 是一个半群。

在例题1中, $k \geq 0$ 这个条件是重要的, 否则, 如果 $k < 0$, 则运算 $+$ 在 S_k 上将是不封闭的。

190页 (1) 对于正整数 k , $N_k=\{0,1,2,\cdots,k-1\}$, 设 $*_k$ 是 N_k 上的一个二元运算, 使得 $a*_kb$ =用 k 除 $a\cdot b$ 所得的余数, 这里 $a, b\in N_k$ 。

a) 当 $k=4$ 时, 试造出 $*_k$ 的运算表。

b) 对于任意正整数 k , 证明 $\langle N_k, *_k \rangle$ 是一个半群。

解 a) 当 $k=4$ 时, $*_k$ 的运算表如下:

$*_k$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

b) 对于任意的 $a, b \in \mathbf{N}_k$, $a *_k b = a \cdot b - nk = r$, $0 \leq r \leq k-1$,

所以运算 $*_k$ 在 \mathbf{N}_k 上是封闭的。

对于任意的 $a, b, c \in \mathbf{N}_k$, 有

$$(a *_k b) *_k c = (a \cdot b - n_1 k) \cdot c - n_2 k = r_1 \quad 0 \leq r_1 \leq k-1$$

$$= a \cdot b \cdot c - k(n_1 c + n_2)$$

$$a *_k (b *_k c) = a \cdot (b \cdot c - n_3 k) - n_4 k = r_2 \quad 0 \leq r_2 \leq k-1$$

$$= a \cdot b \cdot c - k(n_3 a + n_4)$$

可见 r_1 和 r_2 都是 $a \cdot b \cdot c$ 用 k 除所得的余数, 所以 $r_1 = r_2$ 。所

以 $(a *_k b) *_k c = a *_k (b *_k c)$, 即 $*_k$ 满足结合律。

因此, $\langle \mathbf{N}_k, *_k \rangle$ 是半群。

例题2 设 $S=\{a,b,c\}$ ，在 S 上的一个二元运算 Δ 定义如表5-3.1

所示。表5-3.1:

Δ	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

验证 $\langle S, \Delta \rangle$ 是一个半群。

解 从表5-3.1中可知运算 Δ 是封闭的，同时a, b和c都是左么元。所以，对于任意的 $x, y, z \in S$ ，都有

$$x \Delta (y \Delta z) = x \Delta z = z = y \Delta z = (x \Delta y) \Delta z$$

因此， $\langle S, \Delta \rangle$ 是半群。

明显地，代数系统 $\langle I_+, - \rangle$ 和 $\langle R, / \rangle$ 都不是半群，这里， $-$ 和 $/$ 分别是普通的减法和除法。

练习 设 $*$ 是实数集 \mathbf{R} 上的运算，其定义如下：

$$a*b=a+b+2ab$$

1)求 $2*3$ ， $3*(-5)$ 和 $7*1/2$ 。

2) $\langle \mathbf{R}, * \rangle$ 是半群吗？ $*$ 可交换吗？

3)求 \mathbf{R} 中关于 $*$ 的幺元（单位元）。

4) \mathbf{R} 中哪些元素有逆元，逆元素是什么？

解 1) $2*3=17$ ， $3*(-5)=-32$ ， $7*1/2=14.5$

2)运算 $*$ 在 \mathbf{R} 上是封闭的。

对任意 $a, b, c \in \mathbf{R}$,

$$(a*b)*c=(a+b+2ab)*c=a+b+2ab+c+2(a+b+2ab)c$$

$$=a+b+c+2ab+2ac+2bc+4abc$$

$$a*(b*c)=a*(b+c+2bc)=a+b+c+2bc+2a(b+c+2bc)$$

$$=a+b+c+2ab+2ac+2bc+4abc$$

所以 $(a*b)*c = a*(b*c)$ 。因此 $\langle \mathbf{R}, * \rangle$ 是半群。 $*$ 可交换。

3) \mathbf{R} 中关于 $*$ 的幺元是 0 。

4) \mathbf{R} 中除 $-1/2$ 外所有元素都有逆元， a 的逆元素是 $-a/(1+2a)$ 。

练习 设 $S=\{a, b\}$, S^S 是从 S 到 S 的所有函数的集合, \circ 是函数的复合运算,
写出运算 \circ 的运算表, 证明 $\langle S^S, \circ \rangle$ 是半群。

解 $|S^S| = |S|^{|S|} = 2^2 = 4$

$S^S = \{f_1, f_2, f_3, f_4\}$

其中 $f_1: a \rightarrow a$

$b \rightarrow a$

$f_2: a \rightarrow a$

$b \rightarrow b$

$f_3: a \rightarrow b$

$b \rightarrow a$

$f_4: a \rightarrow b$

$b \rightarrow b$

$f_1 \circ f_1: a \rightarrow a$

$= f_1 \quad b \rightarrow a$

$f_1 \circ f_2: a \rightarrow a$

$= f_1 \quad b \rightarrow a$

$f_1 \circ f_3: a \rightarrow a$

$= f_1 \quad b \rightarrow a$

$f_1 \circ f_4: a \rightarrow a$

$= f_1 \quad b \rightarrow a$

$f_2 \circ f_1: a \rightarrow a$

$= f_1 \quad b \rightarrow a$

$f_2 \circ f_2: a \rightarrow a$

$= f_2 \quad b \rightarrow b$

$f_2 \circ f_3: a \rightarrow b$

$= f_2 \quad b \rightarrow a$

$f_2 \circ f_4: a \rightarrow b$

$= f_4 \quad b \rightarrow b$

$f_3 \circ f_1: a \rightarrow b$

$= f_4 \quad b \rightarrow b$

$f_3 \circ f_2: a \rightarrow b$

$= f_3 \quad b \rightarrow a$

$f_3 \circ f_3: a \rightarrow a$

$= f_2 \quad b \rightarrow b$

$f_3 \circ f_4: a \rightarrow a$

$= f_1 \quad b \rightarrow a$

$f_4 \circ f_1: a \rightarrow b$

$= f_4 \quad b \rightarrow b$

$f_4 \circ f_2: a \rightarrow b$

$= f_4 \quad b \rightarrow b$

$f_4 \circ f_3: a \rightarrow b$

$= f_4 \quad b \rightarrow b$

$f_4 \circ f_4: a \rightarrow b$

$= f_4 \quad b \rightarrow b$

运算 \circ 的运算表如下:

\circ	f_1	f_2	f_3	f_4
f_1	f_1	f_1	f_1	f_1
f_2	f_1	f_2	f_2	f_4
f_3	f_4	f_3	f_2	f_1
f_4	f_4	f_4	f_4	f_4

由表中可看到运算 \circ 在

S^S 上是封闭的, 由第4章知
函数的复合运算满足结合律,
因此 $\langle S^S, \circ \rangle$ 是半群。

子半群

定理5-3.1 设 $\langle S, * \rangle$ 为一半群, $B \subseteq S$ 且 $*$ 在 B 上封闭, 那么 $\langle B, * \rangle$ 也是一个半群, 称为 $\langle S, * \rangle$ 的子半群。

□ 证明思路: 结合律在 B 上仍成立。 □

证明 因为 $*$ 在 S 上是可结合的, 而 $B \subseteq S$ 且 $*$ 在 B 上封闭, 所以 $*$ 在 B 上也是可结合的, 因此, $\langle B, * \rangle$ 也是一个半群。

证明 $\langle B, * \rangle$ 是 $\langle S, * \rangle$ 的子半群, 只须证明运算 $*$ 在 B 上是封闭的。

例题3 设 \cdot 表示普通的乘法运算, 那么 $\langle [0,1], \cdot \rangle$ 、 $\langle [0,1), \cdot \rangle$ 和 $\langle I, \cdot \rangle$ 都是 $\langle R, \cdot \rangle$ 的子半群。

解 首先, 运算 \cdot 在 R 上是封闭的, 且是可结合的, 所以 $\langle R, \cdot \rangle$ 是一个半群。其次, 运算 \cdot 在 $[0, 1]$ 、 $[0, 1)$ 和 I 上都是封闭的, 且 $[0, 1] \subset R$, $[0, 1) \subset R$, $I \subset R$ 。因此, 由定理5-3.1可知 $\langle [0,1], \cdot \rangle$ 、 $\langle [0,1), \cdot \rangle$ 和 $\langle I, \cdot \rangle$ 都是 $\langle R, \cdot \rangle$ 的子半群。

练习 若 $\langle S, * \rangle$ 是半群, $a \in S$, $M = \{a^n | n \in \mathbb{N}\}$, 证明
 $\langle M, * \rangle$ 是 $\langle S, * \rangle$ 的子半群。

证明 只须证明运算 $*$ 在 M 上是封闭的。

任取 $a^n, a^m \in M$,

$$\begin{aligned} a^n * a^m &= (a^n * a) * a^{m-1} \\ &= a^{n+1} * a^{m-1} \\ &= (a^{n+1} * a) * a^{m-2} \\ &= a^{n+2} * a^{m-2} \\ &= \dots \\ &= a^{n+m} \in M \end{aligned}$$

所以 $\langle M, * \rangle$ 是 $\langle S, * \rangle$ 的子半群。

即有限半群中
存在等幂元。

定理 5-3.2 设代数结构 $\langle S, * \rangle$ 为一个半群，
如果 S 是一个有限集合，则必有 $a \in S$ ，使得 $a * a = a$ 。

□ **证明思路：** 因 $\langle S, * \rangle$ 是半群，对于任意 $b \in S$ ，由于 $*$ 的封闭性可知

$$b * b \in S \quad \text{记 } b^2 = b * b$$

$$b^2 * b = b * b^2 \in S \quad \text{记 } b^3 = b^2 * b = b * b^2$$

.....

$b, b^2, b^3, \dots, b^i, \dots, b^q, \dots, b^j$ (最多有 $|S|$ 个不同元素)

因**S**是一个有限集合，所以必存在 $j > i$ ，使得

$$b^i = b^j$$

令 $p = j - i$ 即 $j = p + i$ 代入上式: $b^i = b^p * b^i$

所以, $b^q = b^p * b^q \quad i \leq q$

因为 $p \geq 1$ 所以总可以找到 $k \geq 1$ ，使得 $kp \geq i$ ，

对于 $b^{kp} \in S$ ，就有 $b^{kp} = b^p * b^{kp} = b^p * (b^p * b^{kp})$

$$= b^{2p} * b^{kp} = b^{2p} * (b^p * b^{kp}) = \dots = b^{kp} * b^{kp} \quad \square$$

这就证明了在S中存在元素 $a = b^{kp}$ ，使得 $a * a = a$

再看190页 (1) 对于正整数 k , $N_k=\{0,1,2,\cdots,k-1\}$, 设 $*_k$ 是 N_k 上的一个二元运算, 使得 $a*_kb$ =用 k 除 $a\cdot b$ 所得的余数, 这里 $a, b\in N_k$ 。我们已经证明了 $\langle N_k, *_k \rangle$ 是一个半群。

当 $k=4$ 时, $*_k$ 的运算表如下:

$*_k$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

找出 $\langle N_k, *_k \rangle$ 中的等幂元。

0和1都是等幂元。

例题2 设 $S=\{a,b,c\}$ ，在 S 上的一个二元运算 Δ 定义如表5-3.1所示。表5-3.1:

Δ	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

验证 $\langle S, \Delta \rangle$ 是一个半群。

前面已验证 $\langle S, \Delta \rangle$ 是一个半群。这里a, b, c都是等幂元。

三、独异点

定义5-3.3 设代数结构 $\langle S, * \rangle$ 为半群, 若 $\langle S, * \rangle$ 含有关于 $*$ 运算的么元, 则称它为独异点(*monoid*), 或含么半群。

例如, 代数系统 $\langle \mathbf{R}, + \rangle$ 是一个独异点, 因为 $\langle \mathbf{R}, + \rangle$ 是一个半群, 且 0 是 \mathbf{R} 中关于运算 $+$ 的么元。另外, 代数系统 $\langle \mathbf{I}, \cdot \rangle, \langle \mathbf{I}_+, \cdot \rangle, \langle \mathbf{R}, \cdot \rangle$ 都是具有么元 1 的半群, 因此它们都是独异点。

代数系统 $\langle \mathbf{N} - \{0\}, + \rangle$ 虽是一个半群, 但关于运算 $+$ 不存在么元, 所以, 这个代数系统不是独异点。

有代数系统 $\langle S, * \rangle$, 其中 $S = \{a, 0, 1\}$, 运算 $*$ 由下表定义, 证明 $\langle S, * \rangle$ 是独异点。

$*$	a	0	1
a	a	0	1
0	0	0	1
1	1	0	1

证明 1) 运算 $*$ 是封闭的。

2) 对于任意 $x, y \in S$,

$$(x*y)*a = x*y \quad x*(y*a) = x*y$$

$$(x*y)*0 = 0 \quad x*(y*0) = x*0 = 0$$

$$(x*y)*1 = 1 \quad x*(y*1) = x*1 = 1$$

所以运算 $*$ 是可结合的。

3) a 是 S 中关于运算 $*$ 的幺元。

因此 $\langle S, * \rangle$ 是独异点。

表中任何两
行或两列都
是不同的。

定理5-3.3 设 $\langle S, *, e \rangle$ 是一个独异点,则在关于运算 $*$ 的运算表中任何两行或两列都是不相同的。

□ **证明:** 因 S 中关于 $*$ 运算的幺元是 e , 因为对于任意的元素 $a, b \in S$, 且 $a \neq b$ 时, 总有

$$e * a = a \neq b = e * b$$

和 $a * e = a \neq b = b * e$

所以, 在的运算表中不可能有两行或两列是相同的。

□

例题4: 因设 I 是整数集合, m 是任意正整数, Z_m 是由模 m 的同余类组成的同余类集, 在 Z_m 上定义两个二元运算 $+_m$ 和 \times_m 分别如下: 对于任意的 $[i], [j] \in Z_m$

$$[i] +_m [j] = [(i+j) \pmod m]$$

$$[i] \times_m [j] = [(i \times j) \pmod m]$$

试证明在这两个二元运算的运算表中任何两行或两列都是不相同的。

证明: 考察代数结构 $\langle Z_m, +_m \rangle$ 和 $\langle Z_m, \times_m \rangle$, 只须证明 $\langle Z_m, +_m \rangle$ 和 $\langle Z_m, \times_m \rangle$ 都是独异点。先分三步证明 $\langle Z_m, +_m \rangle$ 是独异点, 再利用定理5-3.3的结论:

- 1) 根据运算定义, 证明两个运算在 Z_m 上封闭;
- 2) 根据运算定义, 证明两个运算满足结合律;
- 3) 根据运算定义, 证明 $[0]$ 是 $\langle Z_m, +_m \rangle$ 的幺元, $[1]$ 是 $\langle Z_m, \times_m \rangle$ 的幺元。

本例题的实例见 表5-3.2和表5-3.3

(1)由运算 $+_m$ 和 \times_m 的定义, 可知它们在 Z_m 上都是封闭的。

(2)对于任意 $[i], [j], [k] \in Z_m$

$$([i] +_m [j]) +_m [k] = [i] +_m ([j] +_m [k])$$

$$= [(i+j+k) \pmod m]$$

$$([i] \times_m [j]) \times_m [k] = [i] \times_m ([j] \times_m [k])$$

$$= [(i \times j \times k) \pmod m]$$

即运算 $+_m$ 和 \times_m 都是可结合的。

(3)因为 $[0] +_m [i] = [i] +_m [0] = [i]$, 所以, $[0]$ 是 $\langle Z_m, +_m \rangle$ 中的幺元。因为 $[1] \times_m [i] = [i] \times_m [1] = [i]$, 所以 $[1]$ 是 $\langle Z_m, \times_m \rangle$ 中的幺元。

因此, 代数系统 $\langle Z_m, +_m \rangle$, $\langle Z_m, \times_m \rangle$ 都是独异点。由定理**5-3.3**可知, 这两个运算的运算表中任何两行或两列都不相同。

上例中,如果给定 $m=5$, 那么, $+_5$ 和 \times_5 的运算表分别如表 5-3.2 和表 5-3.3 所示。

表 5-3.2

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

表 5-3.3

\times_5	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

显然, 上述运算表中没有两行或两列是相同的。

定理5-3.4 设 $\langle S, *, e \rangle$ 是一个独异点,如果对于任意 $a, b \in S$, 且 a, b 均有逆元, 则

a) $(a^{-1})^{-1} = a$

b) $(a*b)^{-1}$ 有逆元, 且 $(a*b)^{-1} = b^{-1} * a^{-1}$ 。

□ **证明:** a) 因 a^{-1} 和 a 为互为逆元, 直接得到结论。

b) 必须证明两种情况:

$$(a*b) * [b^{-1} * a^{-1}] = e$$

和 $[b^{-1} * a^{-1}] * (a*b) = e$

利用结合律容易得出。

□