第十六章 半群与独异点

- 半群、独异点的定义与性质
  - 半群与独异点的定义
  - 半群与独异点的性质
- 半群、独异点的子代数、积代数、商代数
  - 子半群与子独异点
  - 半群与独异点的直积
  - 商半群与商独异点
- 半群与独异点的同态
  - 独异点的表示定理
- 学习要点与基本要求
- 实例分析

半群与独异点的定义

定义 一个代数系统$<S, *>$，其中S是非空集合，$*$是S上的一个二元运算，

半群： 运算$*$是可结合的

独异点： (1)运算$*$是可结合的

(2) 存在单位元

说明： 任何半群都可以扩张成独异点

表示式中可以省略运算符

半群与独异点的举例

- $<Z^+,+>$是半群， $+$是普通加法；
- $<N,+>$，$<Z,+>$，$<Q,+>$，$<R,+>$是独异点；
- 设$n \in Z^+$, $<M_n(R),+>$和$<M_n(R),\cdot>$都是独异点；
- $<P(B),\oplus>$为独异点，其中$\oplus$为集合的对称差运算；
- $<Z_n, +_n>$为独异点，其中$Z_n=\{0,1,\ldots,n-1\}$, $+_n$为模n加法；
- $<A^A,\circ>$为独异点，其中$\circ$为函数的复合运算；
- $<R^*,\circ>$为半群,其中R^*为非零实数集合,

$$\forall x,y \in R^*, x \circ y = y$$

半群与独异点性质

- 幂运算的定义

半群　　　　　　　　独异点

$a^1=a$　　　　　　　　$a^0=e$

$a^{n+1}=a^n a$

- 性质：　如，<N,+>，$m^3=m+m+m=3m$

（1）定理1　幂运算的等式

$a^n a^m=a^{n+m}$　　　　　　$(a^n)^m=a^{nm}$

（2）结合律

（3）有限半群必存在幂等元（证明见后）

（4）独异点运算表中任何两行或两列都是不相同的。

实例1

例1 $V=<S,*>$为半群，任取$a,b\in S$, 如果$ab=ba$, 则有$a=b$，证明

(1) V 中成立幂等律

(2) $\forall a,b\in V,\ aba=a$

(3) $\forall a,b,c\in V,\ abc=ac$

证 (1) $(aa)a=a(aa)\Rightarrow aa=a$

(2) $(aba)a=ab(aa)=aba$

$a(aba)=(aa)ba=aba$

故$(aba)a=a(aba)\Rightarrow aba=a$

(3) $(abc)(ac)=(ab)(cac)=abc$

$(ac)(abc)=(aca)(bc)=abc$

故$(abc)(ac)=(ac)(abc)\Rightarrow abc=ac$

实例2

例2 设集合$S_k=\{x|x\in I, x\geq k\}$，$k\geq 0$，验证$< S_k,+>$是一个半群，其中+是普通的加法运算。

解 $\forall x,y\in S_k$，$x\geq k$，$y\geq k$，$k\geq 0$，有$x+y\geq k$，

所以运算+是在S_k上封闭的。

已知普通加法运算是可结合的。

所以$< S_k,+>$是一个半群。

思考： 若没有条件$k\geq 0$，$< S_k,+>$一定是半群吗？为什么？

实例3

例3 设$S=\{a,b,c\}$，在S上的一个二元运算Δ定义如表所示。验证$<S, \Delta>$是一个半群。

Δ	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

解 从表中可知运算Δ是封闭的。

a,b和c都是左幺元。

$\forall x,y,z \in S$，有

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

因此，运算Δ在S上是可结合的。

故$<S, \Delta>$是一个半群。

子半群、子独异点

定义：

子半群： 半群的子代数

子独异点： 独异点T的子代数

子半群、子独异点*B*的判别：

（1）非空子集*B*,

（2）*B* 对于*V* 中的运算（含0元运算）封闭.

定理2 若干子半群的非空交集仍为子半群；

若干子独异点的交集仍为子独异点.

子集B生成的子半群<B>

定义： $V=\langle S,*\rangle$为半群, $B\subseteq S$,包含B 的最小的半群称为由B生成的子半群，记作$\langle B\rangle$.

$\langle B\rangle=\cap\{A \mid A$是$S$的子半群，$B\subseteq A\}$

$$\langle B\rangle=\bigcup_{n\in Z^+} B^n,\quad B^n=\{b_1b_2\cdots b_n \mid b_i\in B, i=1,2,\cdots,n\}$$

实例

例4 $V=<Z,+>$半群，$B=\{4,6\}$,

$<B>=\{\ 4i+6j \mid i,j \in N,\ i$ 和j 不同时为0 $\}$

$=\{\ 4,6,8,10,12,14,16,\ldots\} = 2Z^{+}-\{2\}$

例5 Σ有穷字母表，Σ^{+}为非空字的集合, Σ^{*}为字的集合。

$a_1a_2\ldots a_n = b_1b_2\ldots b_n \Leftrightarrow a_1=b_1,\ a_2=b_2,\ \ldots,\ a_n=b_n$

每个字可以唯一分解为Σ中的元素之积

Σ^{+}上的连接运算满足结合律，$V=<\Sigma^{+},\cdot>$构成半群，

称为Σ上的自由半群，Σ为这个自由半群的生成元集，

即$<\Sigma>=V$.

如果包含空串则Σ^{*}构成自由独异点.

半群独异点的直积、商代数、同态

- 半群与独异点的直积
  - 半群的直积仍是半群
  - 独异点的直积仍是独异点
- 半群与独异点的商代数
  - 半群$<A,\circ>$, 商半群$<A/R,\bar{\circ}>$
  - 独异点$<A,\circ,e>$，商独异点$<A/R,\bar{\circ},[e]>$
- 半群与独异点的同态和同构
  - 半群$f(xy)=f(x)f(y)$
  - 独异点$f(xy)=f(x)f(y)$, $f(e)= e'$

半群的同态性质

定理3 设$V=<S,*>$为半群，$V'=<S^S,\circ>$，$\circ$为合成，则V'也是半群，且存在V到V'的同态.

证： $f_a:S\to S$, $f_a(x)=a*x$

$f_a\in S^S$, 且$\{f_a \mid a\in S\}\subseteq S^S$,

令ϕ：$S\to S^S$, $\phi(a)=f_a$,

$\phi(a*b)=f_{a*b}$, $\phi(a)\circ\phi(b)=f_a\circ f_b$

为证同态只需证明$f_{a*b}=f_a\circ f_b$

$\forall x\in S$，$f_{a*b}(x)=(a*b)*x=a*b*x$

$f_a\circ f_b(x)=f_a(f_b(x))=f_a(b*x)=a*(b*x)=a*b*x$

独异点的表示定理

定理4 设$V=<S,*,e>$为独异点，则存在$T\subseteq S^S$, 使得

$<S,*,e>$同构于$<T,\circ,I_S>$

证： 令 ϕ：$S\to S^S$, $\phi(a) = f_a$, 则

$\phi(a*b) = \phi(a)\circ\phi(b)$

$\phi(e) = f_e = I_S$,

ϕ为独异点V 到$<S^S,\circ,I_S>$的同态

$\phi(a) = \phi(b) \Rightarrow f_a=f_b \Rightarrow \forall x\in S(a*x=b*x)$

$\Rightarrow a*e = b*e \Rightarrow a=b$, ϕ为单射

令$T=\phi(S)$，则$T\subseteq S^S$, 且$\phi:S\to T$ 为双射，

$<S,*,e>\cong<T,\circ,I_S>$

实例

例6 $S = Z_3 = \{ 0, 1, 2 \}$，独异点 $V = <S,\oplus,0>$,

$S^S = \{ f_0, f_1, f_2, \ldots, f_{26} \}$，其中

$f_0 = \{<0,0>,<1,1>,<2,2>\}$ $\quad$ $f_0(x) = 0 \oplus x = x$

$f_1 = \{<0,1>,<1,2>,<2,0>\}$ $\quad$ $f_1(x) = 1 \oplus x$

$f_2 = \{<0,2>,<1,0>,<2,1>\}$ $\quad$ $f_2(x) = 2 \oplus x$

$\phi: S \to S^S$, $\phi(0) = f_0$, $\phi(1) = f_1$, $\phi(2) = f_2$

$T = \phi(S) = \{f_0, f_1, f_2\} \subseteq S^S$,即$<S,\oplus,0>$同构于$<T, \circ, I_S>$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\circ$	f_0	f_1	f_2
f_0	f_0	f_1	f_2
f_1	f_1	f_2	f_0
f_2	f_2	f_0	f_1

学习要点与基本要求

- 掌握判别半群、独异点的方法
- 半群、独异点的性质
- 作业：习题十六：2,3,7,10,11,12
- 阅读：十六章 16.2节 有穷自动机

实例分析

例题1 设独异点V＝<S,•,e>，其中

$$S=\left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| \ a,d\in R\right\}$$

•为矩阵乘法，e= $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$，令 $T=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| \ a\in R\right\}$

证明<T, •>是独异点，但不是V的子独异点。

证： T$\subseteq$ S，且T对矩阵乘法是封闭的，

所以<T,•>是V＝<S,•>的子半群。 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$是<T,•>的幺元。

所以<T,•>是一个独异点。

因为V的幺元$\notin T$，所以<T, •>不是V 的子独异点。

实例分析

例题2 设$V_1=<S_1,\circ>$，$V_2=<S_2,*>$是半群(或独异点),

证明$<S_1\times S_2,\bullet>$是半群（或独异点）。

证 $\forall<a,b>,<c,d>\in S_1\times S_2$,则$a\in S_1,c\in S_1,b\in S_2, d\in S_2$,

$<a,b>\bullet<c,d>=<a\circ c, b*d>$,

因为$\circ$在S_1上封闭，$*$在S_2上封闭,

所以$a\circ c\in S_1,b*d\in S_2$，那么$<a,b>\bullet<c,d>\in S_1\times S_2$,

所以$\bullet$在$S_1\times S_2$,上封闭。

（接上页）

任取$<a,b>,<c,d>,<u,v>\in S_1\times S_2$

$(<a,b>\bullet<c,d>)\bullet<u,v>$

$=<a\circ c,b*d>\bullet<u,v>$

$=<(a\circ c)\circ u,(b*d)*v>$

$=<a\circ c\circ u,b*d*v>$（$\circ$和$*$分别在S_1,S_2上可结合）

$<a,b>\bullet(<c,d>\bullet<u,v>)$

$=<a,b>\bullet(<c\circ u,d*v>)$

$=<a\circ(c\circ u),b*(d*v)>$

$=<a\circ c\circ u,b*d*v>$

所以$(<a,b>\bullet<c,d>)\bullet<u,v>=<a,b>\bullet(<c,d>\bullet<u,v>)$

因此$<S_1\times S_2,,\bullet>$是半群。

（接上页）

如果$<S_1,\circ>$，$<S_2,*>$是独异点，设e_1,e_2分别是$<S_1,\circ>$和$<S_2,*>$的幺元，有

$e_1\in S_1$, $e_2\in S_2$，则$<e_1,e_2>\in S$

$\forall<x,y>\in S$，有

$<x,y>\bullet<e_1,e_2>=<x\circ e_1, y*e_2>=<x,y>$

$<e_1,e_2>\bullet<x,y>=<e_1\circ x, e_2*y>=<x,y>$

所以$<e_1,e_2>$是$<S_1\times S_2,\bullet>$的幺元。

故$<S_1\times S_2,\bullet>$是独异点。

实例分析

例题3 设Z是整数集，$m \in Z^+$，Z_m是由模m的同余类组成的同余类集, $Z_m=\{[0], [1], \ldots, [m-1]\}$，在$Z_m$上定义 $+_m$ 和$\times_m$分别如下：

对于任意的$[i],[j] \in Z_m$

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

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

试证明在这两个二元运算的运算表中任何两行或两列都不相同。

[分析] 只需证明$<Z_m,+_m>$和$<Z_m,\times_m>$是独异点。

例题3（接上页）

证明：考察代数系统$<Z_m,+_m>$和$<Z_m,\times_m>$。

（1）对于$\forall[i],[j]\in Z_m$，则$i,j\in Z$，

$[i]+_m[j]=[(i+j)\bmod m]$，$[i]\times_m[j]=[(i\times j)\bmod m]$

由于$i+j\in Z$，$i\times j\in Z$，所以

$(i+j)\bmod m<m$，$(i\times j)\bmod m<m$

即$[(i+j)\bmod m]\in Z_m$，$[(i\times j)\bmod m]\in Z_m$

即$[i]+_m[j]\in Z_m$，$[i]\times_m[j]\in Z_m$

故$+_m$和$\times_m$在Z_m上都是封闭的。

例题3（接上页）

（2）验证可结合性

对于任意$[i],[j],[k]\in Z_m$,

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

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

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

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

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

$+_m$满足结合律。因此$<Z_m,+_m>$是半群。

同理$([i]\times_m[j])\times_m[k]=[i]\times_m([j])\times_m[k])=[(i\times j\times k)(\bmod m)]$

即$\times_m$是可结合的。故代数系统$<Z_m,\times_m>$是半群。

例题3（接上页）

(3) 验证幺元

因为$[0] +_m [i]=[(0+i)\text{mod } m]=[i \text{ mod } m]=[i]$,

$[i] +_m [0]=[(i+0)\text{mod } m]=[i \text{ mod } m]=[i]$,

即$[0] +_m [i]= [i] +_m [0]=[i]$，

所以，$[0]$是$<Z_m, +_m>$中的幺元。

同理$[1] \times_m [i]= [i] \times_m [1]=[i]$，

所以，$[1]$是$<Z_m,\times_m>$中的幺元。

故$< Z_m,+_m>$和$< Z_m,\times_m>$都是独异点。命题得证。

例题3（接上页）

给定m=5，那么$+_5$和$\times_5$的运算表分别如下表所示。

$+_5$	[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]

$\times_5$	[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]

有限半群存在幂等元

定理 设$<S,*>$是一个半群，如果S是有限集，则必有$a\in S$，使得$a*a=a$。

证明 因为$<S,*>$是半群，$\forall b\in S$，必有

$$b^2=b*b\in S$$

$$b^3= b^2*b=b* b^2\in S$$

因为S是有限集，所以必定存在$j>i$，使得$b^i= b^j$。

令$p=j-i$，有$b^j = b^p* b^i \Leftrightarrow b^i= b^p* b^i$，（周期性）

因此有$b^q= b^p* b^q$，$q\geq i$。

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

有限半群存在幂等元（续）

对于$b^{kp} \in S$，有

$b^{kp} = b^p * b^{kp}$

$= b^p * (b^p * b^{kp})$

$= b^{2p} * b^{kp}$

$= \dots$

$= b^{kp} * b^{kp} = b^{kp}$

这就证明了在S中存在元素$a = b^{kp}$，使得$a*a=a$。

独异点运算表的特点

定理 设 $<S, *>$ 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 设 S 中关于运算 $*$ 的幺元是 e。

$\forall x,y \in S$ 且 $x \neq y$，有

$$e * x \neq e * y$$

所以 x,y 对应的列不同。

$$x * e \neq y * e$$

所以 x,y 对应的行不同。

所以，在 $*$ 的运算表中不可能有两行或两列是相同的。