第七章 群环域理论

回顾

- 运算
  - 封闭性
  - 二元运算，n元运算
- 代数系统
  - $\langle S, f_1, f_2, \cdots, f_m \rangle$
  - 同类型的代数系统
  - 子代数系统
- 代数系统的基本性质
  - 结合律
  - 交换律
  - 分配律
  - 吸收律
  - 等幂律与等幂元
  - 可约律与可约元
  - 幺元或单位元
  - 零元
  - 逆元

回顾

- 同态
  - 定义：$\langle X, \odot \rangle \simeq \langle Y, * \rangle$：

    $$(\exists f)(f: X \to Y \wedge (\forall x_1)(\forall x_2)(x_1, x_2 \in X \to f(x_1 \odot x_2) = f(x_1) * f(x_2)))$$

  - 性质：“保持运算”
- 同构
  - 定义：$\langle X, \odot \rangle \cong \langle Y, * \rangle$

    $(\exists f)(f \in Y^X \wedge f$为双射$\wedge f$为从$\langle X, \odot \rangle$到$\langle Y, * \rangle$的同态映射
  - 性质：“彼此相通”

回顾

- 同余关系
  - 定义
  - 性质
- 商代数
  - 定义
  - 性质
- 积代数
  - 定义
  - 性质

主要内容

- 半群和独异点的定义及性质
- 半群和独异点的同态与同构
- 积半群
- 群的基本定义与性质
- 置换群和对称群
- 子群与陪集
- 群的同态与同构
- 环与域

7.1.1 半群和独异点的定义及性质

- **定义7.1.1** 给定$\langle S, \odot \rangle$，若$\odot$满足结合律，则称$\langle S, \odot \rangle$为半群。
  - 可见，半群就是由集合及其上定义的一个可结合的二元运算组成的代数结构。
- **定义7.1.2** 给定$\langle M, \odot \rangle$，若$\langle M, \odot \rangle$是半群且$\odot$有幺元或$\odot$满足结合律且拥有幺元，则称$\langle M, \odot \rangle$为独异点。
  - 可以看出，独异点是含有幺元的半群。因此有些著作者将独异点叫做含幺半群。有时为了强调幺元e，独异点表示为$\langle M, \odot, e \rangle$。


代数系统
⟨S, ⊙⟩
⊙可结合
半群
⟨S, ⊙⟩
有幺元e
独异点
⟨S, ⊙, e ⟩

- 例7.1.1 给定$\langle N,+\rangle$和$\langle N,\times\rangle$，其中N为自然数集合，+和×为普通加法和乘法。
  - 易知$\langle N,+\rangle$和$\langle N,\times\rangle$都是半群，而且还是独异点。因为0是+的幺元，1是×的幺元。
- 如果半群$\langle S,\odot\rangle$中的集合S是有限的，则称半群为有限半群。对于有限半群可以给出下面有趣定理：

- **定理7.1.1** $\langle S, \odot \rangle$为有限半群$\Rightarrow (\exists x)(x \in S \wedge x \odot x = x)$
- 本定理告诉我们，有限半群存在等幂元。
- 证明：因为$\odot$是可结合的，所以对任意的$x \in S$, 有

$$x \odot x = x^2 \in S \quad \text{(封闭性)}$$

$$x^2 \odot x = x^3 \in S$$

$$\cdots$$

因为S是有限集，必存在$j > i$使得$x^j = x^i$

令$p = j - i$,则$x^j = x^i = x^p \odot x^i$

所以，对于$q \geq i$，有

$$x^q = x^i \odot x^{q-i} = x^p \odot x^i \odot x^{q-i} = x^p \odot x^q$$

即 $x^q = x^p \odot x^q$ (1)

因为$p \geq 1$,故总有$k \geq 1$,使得$kp \geq i$.

对于$x^{kp} \in S$,则由(1)有

$$x^{kp} = x^p \odot x^{kp} = x^p \odot \left(x^p \odot x^{kp}\right) =$$
$$x^{2p} \odot x^{kp} = \cdots = x^{kp} \odot x^{kp}$$

因此，存在$y = x^{kp} \in S$,使得$y \odot y = y$

即y是等幂元.

- 定义7.1.3 给定半群 $\langle S, \odot \rangle$，若$\odot$是可交换的，则称$\langle S, \odot \rangle$是可交换半群。类似地可定义可交换独异点$\langle M, \odot, e \rangle$。
- 例7.1.2 给定$\langle P(S), \cup \rangle$和$\langle P(S), \cap \rangle$，其中$P(S)$是集合$S$的幂集，$\cap$和$\cup$为集合上的并与交运算。
  - 可知$\langle P(S), \cup \rangle$和$\langle P(S), \cap \rangle$都是可交换半群。
  - 不仅如此，它们还都是可交换独异点，因为$\varnothing$与S分别是它们的幺元。

- 定义7.1.4 给定半群$\langle S, \odot\rangle$和$g \in S$，以及自然数集合N，则

  g为$\langle S, \odot\rangle$的生成元：

  $$(\forall x)(x \in S \rightarrow (\exists n)(n \in N \wedge x = g^n))$$

  此时也说，元素g生成半群$\langle S, \odot\rangle$，而且称该半群为循环半群。

- 类似地定义独异点$\langle M, \odot, e\rangle$的生成元$g$和循环独异点，并且规定$g^0=e$。

- **定理7.1.2** 每个循环独异点$\langle M, \odot, e\rangle$都是可交换的。
- 证明：设$\langle M, \odot, e\rangle$是由$g$生成的，对于任意的$x, y \in M$，存在$a, b \in N$，使

$$x = g^a, y = g^b$$

$$x \odot y = g^a \odot g^b = g^{a+b}$$

$$y \odot x = g^b \odot g^a = g^{b+a}$$

显然$x \odot y = y \odot x$，因此$\langle M, \odot, e\rangle$是可交换的

- 将生成元的概念加以推广便得出生成集的概念。

- **定义7.1.5** 给定半群$\langle S, \odot \rangle$及$G \subseteq S$，则
- G为$\langle S, \odot \rangle$的**生成集**：

$$(\forall a)(a \in S \rightarrow a = \odot(G)) \wedge \min |G|$$
$$G \subseteq S$$

- 这里$\odot(G)$表示用G中的元素经$\odot$的复合而生成的元素。
- 类似地定义独异点$\langle M, \odot, e \rangle$的生成集。
- **例7.1.3** 给定$\langle N, + \rangle$，其中N是自然数集合，+为普通加法
  - $\langle N, + \rangle$ 是无穷循环独异点，0是幺元，1是生成元。

- 例7.1.4 令半群$\langle S, \odot \rangle$，其中$S = \{a, b, c, d\}$，$\odot$定义如表7.1.1，试证明生成集$G = \{a, b\}$

表7.1.1

$\odot$	a	b	c	d
a	d	c	b	a
b	b	b	b	b
c	c	c	c	c
d	a	b	c	d

- 解：由表7.1.1可以看出：

$$a^1 = a$$

$$b^1 = b$$

$$a \odot a = a^2 = d$$

$$a \odot b = c$$

- 即集合$\{a, b\}$可以生成集合$\{a, b, c, d\}$.

表7.1.1

$\odot$	a	b	c	d
a	d	c	b	a
b	b	b	b	b
c	c	c	c	c
d	a	b	c	d

- 定义7.1.6 给定半群$\langle S, \odot\rangle$及非空集合$T \subseteq S$，若T对$\odot$封闭，则称$\langle T, \odot\rangle$为$\langle S, \odot\rangle$的子半群。
- 类似地定义独异点$\langle M, \odot, e\rangle$的子独异点$\langle P, \odot, e\rangle$，应注意的是$e \in P$。
- 定理7.1.3 给定半群$\langle S, \odot\rangle$及任意$a \in S$，则$\langle \{a, a^2, a^3, \cdots\}, \odot\rangle$是循环子半群。
- 证明：因为$\langle S, \odot\rangle$是半群，所以，对任意

  $a \in S, a \odot a \in S$(封闭性), 即$a^2 \in S$,于是

  $a^2 \odot a \in S$,...$a^i \in S$, $i \in Z_+$

  即$\{a, a^2, a^3, \cdots\} \subseteq S$, 并且$a$是生成元，

  于是$\langle \{a, a^2, a^3, \cdots\}, \odot\rangle$是循环子半群

- **定理7.1.4** 给定可交换独异点$\langle M, \odot, e\rangle$，若$P$为其等幂元集合，则$\langle P, \odot, e\rangle$为子独异点。
- 证明：$e \in P$是明显的，并且$P \subseteq M$是显然的

  令$a, b \in P$,则有$a \odot a \in P$和$b \odot b \in P$

  于是有

$$\begin{aligned}(a \odot b) \odot (a \odot b) &= (a \odot b) \odot (b \odot a)\\ &= a \odot (b \odot b) \odot a\\ &= a \odot b \odot a\\ &= (a \odot a) \odot b\\ &= a \odot b \in P\end{aligned}$$

  即$\odot$对P是封闭的，得证.

- **定理7.1.5** 设$\langle M, \odot, e\rangle$为独异点，则关于$\odot$的运算表中任两列或任两行均不相同。
- 证明：因为对任意的$a, b \in M$且$a \neq b$时，总有
- $$e \odot a = a \neq b = e \odot b$$
- 和 $$a \odot e = a \neq b = b \odot e$$
- 因此在$\odot$的运算表中不可能有两列和两行是相同的.

- **定理7.1.6** 给定独异点$\langle M, \odot, e\rangle$，对任意$a, b \in M$且$a$，$b$均有逆元，则
  - (1) $(a^{-1})^{-1} = a$。
  - (2) $a \odot b$有逆元，且$(a \odot b)^{-1} = b^{-1} \odot a^{-1}$。
    - 证明: 1) $(a \odot b) \odot (b^{-1} \odot a^{-1})$

$$= a \odot (b \odot b^{-1}) \odot a^{-1}$$

$$= a \odot e \odot a^{-1}$$

$$= a \odot a^{-1} = e$$

2) $(b^{-1} \odot a^{-1}) \odot (a \odot b)$

$$= b^{-1} \odot (a^{-1} \odot a) \odot b$$

$$= b^{-1} \odot e \odot b$$

$$= b^{-1} \odot b = e$$

7.1.2 半群和独异点的同态与同构

- 定义7.2.1 给定两个半群$\langle S, \odot\rangle$与$\langle T, *\rangle$，则$\langle S, \odot\rangle \simeq \langle T, *\rangle$:

$$(\exists f)(f \in T^S \wedge (\forall x)(\forall y)(x, y \in S \rightarrow f(x \odot y) = f(x) * f(y))$$

- 并称f为从$\langle S, \odot\rangle$到$\langle T, *\rangle$的半群同态映射。
- 由定义可以知道，半群同态映射f可以不是惟一的。

- 与前面定义类似，根据半群同态映射f是单射(一对一)、满射、双射，把半群同态映射f分别定义半群单一同态映射、半群满同态映射和半群同构映射。
- 如果两个半群，存在一个同构映射，则称一个半群同构于另一个半群。
- 由于代数结构之间的满同态具有保持运算的各种性质，对于半群满同态当然完全适用。

- 下面给出一个半群同态保持等幂性的定理。
- 定理7.2.1 如果f为从$\langle S, \odot\rangle$到$\langle T, *\rangle$的半群同态映射，对任意$a \in S$且$a \odot a = a$，则

$$f(a) * f(a) = f(a)。$$

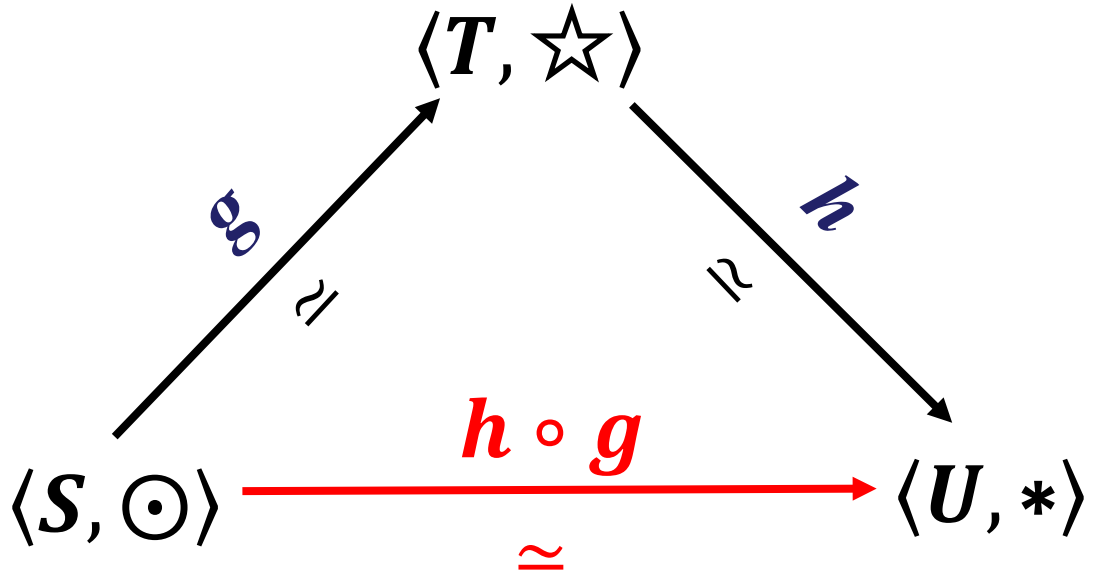
- 证明：因为对任意$a \in S$且$a \odot a = a$

而f是同态映射，即有

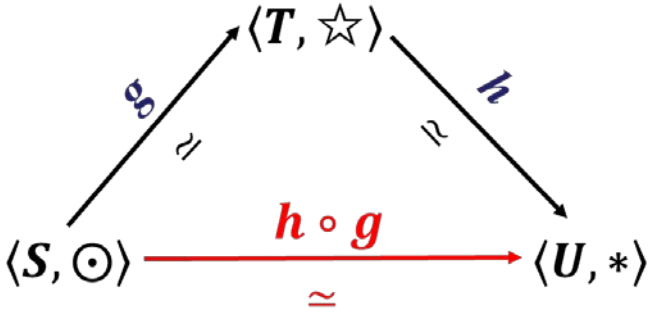
$$f(a \odot a) = f(a) = f(a) * f(a)$$

即等幂性保持.

- 由于半群同态映射是个函数，因此可对半群同态映射进行复合运算，从而产生新的半群同态映射。请看如下定理：
- **定理7.2.2** 如果g是从$\langle S, \odot\rangle$到$\langle T, \star\rangle$的半群同态映射，h是从$\langle T, \star\rangle$到$\langle U, *\rangle$的半群同态映射，则$h \circ g$是从$\langle S, \odot\rangle$到$\langle U, *\rangle$的半群同态映射。



- **定理7.2.2** 如果g是从$\langle S,\odot\rangle$到$\langle T,\star\rangle$的半群同态映射，h是从$\langle T,\star\rangle$到$\langle U,*\rangle$的半群同态映射，则$h\circ g$是从$\langle S,\odot\rangle$到$\langle U,*\rangle$的半群同态映射。



- 证明：对任意$x,y\in S$,有

$$(h\circ g)(x\odot y)$$
$$=h(g(x\odot y)) \quad /^*g\in T^S\text{且是同态}*/$$
$$=h(g(x)\star g(y))$$
$$=h(g(x))*h(g(y)) \quad /^*h\in U^T\text{且是同态}*/$$

即$(h\circ g)\in U^S$是同态.

- 定义7.2.2 若g是从$\langle S,\odot\rangle$到$\langle S,\odot\rangle$的半群同态映射，则称g为半群自同态映射；若g是从$\langle S,\odot\rangle$到$\langle S,\odot\rangle$的半群同构映射，则称g为半群自同构映射。
- 定理7.2.3 给定半群$\langle S,\odot\rangle$，如果$A=\{g\mid g$为$\langle S,\odot\rangle$到$\langle S,\odot\rangle$的半群自同态映射$\}$且$\circ$是函数复合运算，则$\langle A,\circ\rangle$为半群。
- 该定理是明显的，由前一个定理知$\circ$在A上是封闭的，函数的复合运算是可结合的。

- 由于恒等映射idA是复合运算$\circ$的幺元，因此可得下面定理：
- 定理7.2.4 给定半群$\langle S, \odot\rangle$，若$B=\{h|h$为$\langle S, \odot\rangle$到$\langle S, \odot\rangle$的半群自同构映射$\}$，$\circ$为函数复合运算，则$\langle B, \circ, idA\rangle$是独异点。
- 定理7.2.5 给定半群$\langle S, \odot\rangle$，又$\langle S^S, \circ\rangle$是从$S$到$S$的所有函数在复合运算$\circ$下构成的函数半群，则存在从$\langle S, \odot\rangle$到$\langle S^S, \circ\rangle$的半群同态映射$g$，或者说$\langle S, \odot\rangle$半群同态于$\langle S^S, \circ\rangle$。
- 但该半群同态映射是射入的.

- 例7.2.1 给定半群$\langle S, \odot\rangle$，其中$S = \{a, b, c\}$，$\odot$定义由表7.2.1所示。今定义$g \in (S^S)^S$，$g(a) = f_a$，$g(b) = f_b$，$g(c) = f_c$，这里f_a，f_b，$f_c \in S^S$，并且

表7.2.1

$\odot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

- $f_a(a) = a$ $f_a(b) = b$ $f_a(c) = c$
- $f_b(a) = b$ $f_b(b) = c$ $f_b(c) = a$
- $f_c(a) = c$ $f_c(b) = a$ $f_c(c) = b$

- 显然，S^S中有$3^3 = 27$个元素，且$\langle S^S, \circ\rangle$是独异点。根据定理7.2.5可知，$g$是从$\langle S, \odot\rangle$到$\langle S^S, \circ\rangle$的半群同态映射。

- 上面介绍半群同态及有关定理。接着讨论独异点之间的同态及其有关定理。

- 定义7.2.3 给定独异点$\langle M,\odot,e_M\rangle$和$\langle T,*,e_T\rangle$，则$\langle M,\odot,e_M\rangle \simeq \langle T,*,e_T\rangle$：

$$(\exists g)(g \in T^M \wedge (\forall x)(\forall y)(x,y \in M \rightarrow g(x \odot y) = g(x) * g(y)) \wedge g(e_M) = e_T)$$

- 并称g为从$\langle M,\odot,e_M\rangle$到$\langle T,*,e_T\rangle$的独异点同态映射。
- 注意，独异点同态区别半群同态就在于保持幺元，即$g(e_M) = e_T$。因此，半群同态未必是独异点同态，反之都真。

- 例7.2.2 给定独异点$\langle N,+,0\rangle$和$\langle S,*,e\rangle$，其中N为自然数集合，+为一般加法，0为幺元，$S=\{e,0,1\}$，*定义如表7.2.2，e为幺元，又有映射$g\in S^N$：

$$g(i)=\begin{cases}0 & i\neq 0\\ 1 & i=0\end{cases}$$

表7.2.2

*	e	0	1
e	e	0	1
0	0	0	0
1	1	0	1

- 试问g是否为$\langle N,+,0\rangle$到$\langle S,*,e\rangle$的独异点同态映射？

- 给定独异点$\langle N,+,0\rangle$和$\langle S,*,e\rangle$
- $g(i)=\begin{cases}0 & i\neq 0\\ 1 & i=0\end{cases}$
- 证明：

  对任何$i,j\in N$和$i\neq 0,j\neq 0$, 则$i+j\neq 0$,

  于是有$g(i+j)=0$

  $$g(i)*g(j)=0$$

  满足运算的像等于像的运算，

  但是$g(0)=1\neq e$,所以g不是独异点同态映射.

- 例7.2.3 给定独异点$\langle R,+,0\rangle$和$\langle R,\times,1\rangle$，其中$R$是实数集合，+和×是一般加法和乘法，0和1分别为它们的幺元。令$f \in R^R$：

  $f(x) = a^x$其中$a > 0$，$x \in R$
- 问f是否为从$\langle R,+,0\rangle$到$\langle R,\times,1\rangle$的独异点同态映射？
- 证明：因为对任何$x, y \in R$,

  $$f(x+y) = a^{x+y} = a^x \times a^y = f(x) \times f(y)$$

  /*满足运算的像等于像的运算*/

  又$f(0) = a^0 = 1$ /*1是×的幺元*/

  即f是独异点同态映射.

- 定理7.2.6 给定独异点$\langle M,\odot\rangle$，则存在$T\subseteq M^M$，使$\langle M,\odot\rangle\cong\langle T,\circ\rangle$。
- 本定理表明，一个独异点可与复合运算下的一个函数独异点同构。
- 证明：由定理7.2.5 $\langle S,\odot\rangle$半群同态于$\langle S^S,\circ\rangle$，有$\langle M,\odot\rangle\simeq\langle M^M,\circ\rangle$，下面证明存在同态映射$g$，并且$g$是双射
- 令$g:M\to M^M$是$\langle M,\odot\rangle$与$\langle M^M,\circ\rangle$的同态映射，则$g(M)$是M在同态映射g作用下的像，
- 显然$g(M)\subseteq M^M$，且g是$\langle M,\odot\rangle$到$\langle g(M),\circ\rangle$的满同态

- 又因为$\langle M, \odot \rangle$为独异点，故其运算表中的任两行和任两列均不相同，因此，任意的$a, b \in M$，且$a \neq b$，有$g(a) \neq g(b)$，因此g又是单射

- 故g是从$\langle M, \odot \rangle$到$\langle g(M), \circ \rangle$的同构映射.
- 取$T = g(M)$,则有$\langle M, \odot \rangle \cong \langle T, \circ \rangle$.

• 7.1.3 积半群

- 把积代数方法应用于特殊一类代数结构——半群，便产生积半群。
- 定义7.3.1 给定两个半群<S，⊙>和<T，*>。称<$S\times T$，⊗>为<S，⊙>和<T，*>的积半群，其中$S\times T$为集合S与T的笛卡儿积，运算⊗定义如下：
- $\langle s_1, t_1\rangle \otimes \langle s_2, t_2\rangle = \langle s_1 \odot s_2, t_1 * t_2\rangle$，其中$s_1, s_2 \in S$，$t_1, t_2 \in T$
- 由于运算⊗是经⊙和*定义的，易知，积半群是个半群。

- 不难证明下列定理：
- 定理**7.3.1** 若半群<S，⊙>和<T，*>是可交换的，则<$S\times T$，⊗>也是可交换的。
- 定理**7.3.2** 给定半群<S，⊙>和<T，*>，且e_1和e_2分别是它们的幺元，则积半群<$S\times T$，>含有幺元<e_1，e_2>。换言之，若<S，⊙，e_1>和<T，*，e_2>是独异点，则<$S\times T$，⊗，<e_1，e_2>>是独异点。

- 定理7.3.3 给定半群<S，$\odot$>和<T，*>，且θ_1和θ_2分别为它们的零元，
- 则积半群<$S\times T$，$\otimes$>含有零元<θ_1，θ_2>。
- 定理7.3.4 给定半群<S，$\odot$>和<T，*>，且$s\in S$ 的逆元s^{-1}，$t\in T$的逆元t^{-1}，则积半群<$S\times T$，$\otimes$>中<s，t>的逆元是<s^{-1}，t^{-1}>。

总结

- 半群和独异点
  - 定义及性质
  - 同态与同构

作业

- **P174: 2,3,4,5**