# 第六章 代数系统(algebra system)

§1.代数系统的基本概念

§2.代数系统的同态和同构

§3.半群与单子

§4.群

§5.环

§6.域

§7.同余关系（*）

# §1.代数系统的基本概念

- 代数系统
- 代数系统的基本性质
- 子代数系统

## §1.代数系统的基本概念

定义1.运算(operation)

对于任何自然数n≥1，n元运算$f$ 是一个从n维叉积$X^n$到X的函数。

即 $f$： $X^n \to X$ 。

<u>n元运算$f$的封闭性</u>：对于任何n个元素$x_1, x_2, \dots, x_n$,

$$x_1, x_2, \dots, x_n \in X \Rightarrow f(x_1, x_2, \dots, x_n) \in X \text{ ，}$$

或者 $(x_1, x_2, \dots, x_n) \in X^n \Rightarrow f(x_1, x_2, \dots, x_n) \in X$ 。

例子.集合的余运算 $':2^X \to 2^X$ 是一元运算；

集合的交，并运算 $\cap, \cup : 2^X \times 2^X \to 2^X$ 是二元运算。

## 定义2.代数系统　代数结构(algebra structure)

一个代数系统(代数结构，简称代数)A是如下的一个有序元组：

$$A=(X,O_1 , O_2 ,\ldots, O_m , R_1 , R_2 ,\ldots, R_n , c_1 , c_2 ,\ldots, c_l )$$

其中:

(1)$X\neq\varnothing$是一个任意集合,称为母集或承载子(carrier)；

(2)$O_1 , O_2 ,\ldots, O_m$是X上的m个运算($m\geq1$)；

(3)$R_1 , R_2 ,\ldots, R_n$是X上的n个(序)关系($n\geq0$)；

(4)$c_1 , c_2 ,\ldots, c_l \in X$是X中的$l$个特殊元素($l\geq0$),称为常项(constants)。

注：●当X是有限集合时，称A为有限代数系统;

●当X是**无**限集合时，称A为**无**限代数系统;

●在一个代数系统中运算的集合不能是空的，**必须至少**有一个X上的运算。代数系统中**各**个运算的元(阶)数可能是不一**样**的，即每个运算都有自**己**的运算元数。

**例1. (I,+), (I, ×) ,(I,+,×), (I,+, ×, ≤, 0,1)都是代数系统。**

**这里：I是整数集合：+和×是整数的加法和乘法。小于等于关系≤是I上的二元关系(半序)，0,1∈I是I上的两个特殊元素。**

例2. (Ω, o)是代数系统。这里： X={a,b}，

设 $\Omega=\{ f \mid f:X\to X \}$，则 $\Omega=\{f_1, f_2, f_3, f_4\}$ 。

其中

$$f_1:\begin{cases} f_1(a)=a \\ f_1(b)=b \end{cases} \quad f_2:\begin{cases} f_2(a)=a \\ f_2(b)=a \end{cases} \quad f_3:\begin{cases} f_3(a)=b \\ f_3(b)=b \end{cases} \quad f_4:\begin{cases} f_4(a)=b \\ f_4(b)=a \end{cases}$$

o运算是函数的复合运算，

$o:\Omega\times \Omega \to \Omega$

其运算可列表如表1所示：

| o | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
| $f_2$ | $f_2$ | $f_2$ | $f_2$ | $f_2$ |
| $f_3$ | $f_3$ | $f_3$ | $f_3$ | $f_3$ |
| $f_4$ | $f_4$ | $f_3$ | $f_2$ | $f_1$ |

**表 1**

例3. (X,* )是代数系统。这里： $X = \{ a,b,c,d \}$，

定义运算 $* : X^2 \to X$，如表2所示。

| * | a | b | c | d |
|---|---|---|---|---|
| **a** | **a** | **b** | **c** | **d** |
| **b** | **a** | **b** | **c** | **d** |
| **c** | **d** | **c** | **b** | **a** |
| **d** | **d** | **c** | **b** | **a** |

表 **2**

例4. (1)($2^X$, ∩, ∪)是代数系统。 这里X是任意非空的集合，$2^X$是X的幂集， ∩和∪是集合的交和并。

(2)集合代数($2^X$, ∩, ∪, ′)是代数系统。这里′是集合的余。

……

例5.时钟代数(X, σ)是代数系统。

这里：$X=\{a_1, a_2, a_3, \ldots, a_n\}$，定义运算 $\sigma: X \to X$

$$\sigma(a_i)=\begin{cases} a_{i+1} & 当\ a_i \neq n \\ a_1 & 当\ a_i = n \end{cases}。$$

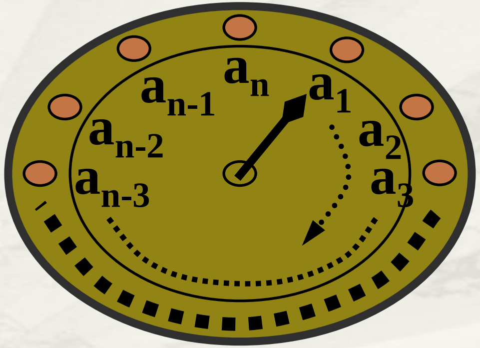



图1

## **定义3.**结合律　交换律(associative law,commutative law)

设( X, ∗ )是任一代数系统， ∗是X上的二元运算。则 称

(1)∗运算满足结合律

$$\Leftrightarrow(\forall x\in X)(\forall y\in X)(\forall z\in X)((x * y) * z = x * (y* z))$$ ；

(2)∗运算满足交换律$\Leftrightarrow(\forall x\in X)(\forall y\in X)(x* y= y * x )$ 。

注：结合律改变的是运算的先后次序；交换律改变的是运算对象的位置顺序。前者是对运算符而言；后者是对运算对象而言。

**例6.**代数系统$(I,+,\times)$中，二元运算$+$和$\times$的性质如何？

**例7.**代数系统 $(2^X, \cap , \cup)$ 中，二元运算$\cap$和$\cup$的性质如何？

**例8.**代数系统$(I,-)$中，减法运算$-$的性质如何？

## 定义4.幺元　零元(identity element,zero element)

设 (X, $*$ )是代数系统，$*$ 是X上的二元运算， $x_0 \in X$ 。则 称

(1)$x_0$是**关于$*$运算的幺元**$\Leftrightarrow(\forall x\in X)(x_0*x=x*x_0=x)$ ；

(2)$x_0$是**关于$*$运算的零元**$\Leftrightarrow(\forall x\in X)(x_0*x=x*x_0=x_0)$ 。

注: • 通常将幺元记为 e ； 含有幺元e的代数系统(X, $*$ ), 通常记作(X, $*$ , e ) ；

即　$(\forall x\in X)(e*x=x*e=x)$ ；

• 在同时具有幺元和零元的代数系统中， 通常将幺元记为1，将零元记为 0 ； 即 $(\forall x\in X)(1*x=x*1=x)$ ；　$(\forall x\in X)(0*x=x*0=0)$ 。

**例9.** 代数系统 (I,+, ×) 中，关于+的幺元、×的幺元？

……

**例10.** 代数系统 ( $2^X$,∩,∪) 中，关于∩的幺元、∪的幺元？

……

**例11.**代数系统(I,+,×)中，关于+的零元、×的零元？

……

**例12.**代数系统($2^X$,∩,∪,)中，关于∩的零元、∪的零元？



……

**定理1.幺元、零元的唯一性**

设 (X, *) 是代数系统，* 是X上的二元运算。则

(1)若关于 *运算的幺元存在，则必是唯一的；

(2)若关于 *运算的零元存在，则必是唯一的。

## [证].（采用逻辑法）只证幺元的唯一性

$e_1$是*运算的幺元 $\wedge$ $e_2$是*运算的幺元

$\Rightarrow(\forall x\in X)(x * e_1=x)\wedge(\forall x\in X)(e_2 * x=x)$,

$\Rightarrow(e_2 * e_1= e_2)\wedge(e_2 * e_1=e_1)$ (因 $e_1, e_2\in X$都是X的普通一元；

据普遍性 特殊化：$\forall xA(x)\Rightarrow A(y)$ 及

合成律： $(p\to q)\wedge(r\to s)\Rightarrow p\wedge r\to q\wedge s$)

$\Rightarrow(e_1=e_2 * e_1)\wedge(e_2 * e_1= e_2)$

(交换律：$p\wedge q\Leftrightarrow q\wedge p$，以及=的对称性)

$\Rightarrow e_1=e_2$ (=的传递性)

所以，幺元是唯一的。

# 填空题 1分

设置

此题未设置答案，请点击右侧设置按钮

设$X=Q\backslash\{1\}$，其中Q是有理数集合，X上的二元运算*定义为：$\forall a, b \in X, a*b=a+b-a\cdot b$，

则在代数系统$<X,*>$中，幺元是[填空1]，零元是 [填空2]

正常使用填空题需3.0以上版本雨课堂

作答

## 定义5.逆元　可逆性(inverse element,invertibility)

设(X,*,e)是代数系统，*是X上的二元运算，e是关于*运算有幺元。

(1)对于某一元素$x \in X$, 若存在着某个元素$y \in X$ ,使得

$$x*y=y*x=e$$

则称$y$是$x$关于*运算的逆元，并称$x$关于*运算是可逆的(invertible)，同时称$x$是关于*运算的可逆元；

(2) 称*运算在X上是可逆的

$$\Leftrightarrow (\forall x \in X)(\exists y \in X)(x*y=y*x=e)$$

$\Leftrightarrow$X中的每个元素都是关于*运算的可逆元 。

例13. 在代数系统$(I, +, \times)$中

(1)加法+的幺元是0，每个元素关于+的逆元是什么？

(2)乘法×的幺元是1，每个元素关于+的逆元是什么？

例14. 在代数系统$(2^X, \cap, \cup)$中

(1)$\cap$的幺元是X，每个X的子集关于$\cap$的逆元是什么？

(2)$\cup$的幺元是$\varnothing$，每个X的子集关于$\cup$的逆元是什么？

## 定理2.逆元的唯一性

设(X，*, e)是代数系统，*是X上的二元运算并且满足结合律，e是幺元。对任何元素$x \in X$，若$x$的逆元存在，则必是唯一的。

# 定理2.逆元的唯一性

[证].设$y_1, y_2 \in X$ 都是$x$的逆元，则

$y_1$=e*$y_1$

=$(y_2*x)*y_1$ ($y_2$是$x$的逆元)

=$y_2*(x*y_1)$ (结合律)

=$y_2$*e ($y_1$是$x$的逆元)

=$y_2$

注：●对任何元素$x \in X$，若$x$的逆元存在唯一，则将其逆元记为$x^{-1}$。

于是，就有 $x*x^{-1}=x^{-1}*x=e$ ；

●若*运算不满足结合律，则逆元未必是唯一的。

例15. 设X={a,b,c,d,e,f,g}，*是X上的二元运算，*运算的运算表如表3，各个元素的逆元是？

| * | a | b | c | d | e | f | g |
|---|---|---|---|---|---|---|---|
| a | a | b | c | d | e | f | g |
| b | b | b | b | b | a | a | a |
| c | c | b | b | b | a | a | a |
| d | d | b | b | b | a | a | a |
| e | e | a | a | a | e | e | e |
| f | f | a | a | a | e | e | e |
| g | g | a | a | a | e | e | e |

表3

注：●因此当代数系统中的二元运算不满足结合律时，**逆**元的**情况变**得**极**为复**杂**;

●结合律的**验**证有时是**十**分**困难**的。上**百**个成**员**的代数，**验**证结合律，其**工**作量即使对于**一般**计算机也是**很困难**的，有上**亿**次的计算量。

# 填空题 0.5分

设置

此题未设置答案，请点击右侧设置按钮

设$X=Q\setminus\{1\}$，其中Q是有理数集合，X上的二元运算*定义为： $\forall a$，$b \in X$, $a*b=a+b-a\cdot b$，

则在代数系统$<X,*>$中，每个元素的逆元是[填空1]。

正常使用填空题需3.0以上版本雨课堂

作答

## 定义6.消去律(cancellation law)

消去律有三种形式：

(1)设(X, $*$)是代数系统，$*$是X上的二元运算。

称 $*$运算满足消去律$\Leftrightarrow$

a) $(\forall x\in X)(\forall y\in X)(\forall z\in X)(x * y = x * z \Rightarrow y = z)$

b) $(\forall x\in X)(\forall y\in X)(\forall z\in X)(y * x = z * x \Rightarrow y = z)$;

## 定义6.消去律(cancellation law)

(1)……

(2)设(X, $*$,0)是代数系统，$*$是X上的二元运算， 0是零元。称 $*$运算满足消去律$\Leftrightarrow$

a) $(\forall x\in X)(\forall y\in X)(\forall z\in X)(x\neq 0\wedge x * y = x * z\Rightarrow y = z)$

b) $(\forall x\in X)(\forall y\in X)(\forall z\in X)(x\neq 0\wedge y * x = z * x\Rightarrow y = z)$;

## 定义6.消去律(cancellation law)

(1) (2)……

(3)设(X,∗, Δ)是代数系统，∗, Δ都是X上的二元运算。

称 ∗及Δ运算满足消去律⇔

a) $(\forall x\in X)(\forall y\in X)(\forall z\in X)$

$$(x * y = x * z \wedge x \,\Delta\, y = x \,\Delta\, z \Rightarrow y = z)$$

b)$(\forall x\in X)(\forall y\in X)(\forall z\in X)$

$$(y * x = z * x \wedge y \,\Delta\, x = z \,\Delta\, x \Rightarrow y = z)。$$

例16.在代数系统$(I,+,\times)$中，加法+满足消去律(1)；乘法×不满足消去律(1)，但满足消去律(2) 。

例17.在代数系统 $(2^X,\cap,\cup)$中， $\cap$和$\cup$都不满足消去律(1) ，但满足消去律(3) 。

## 定义7. 分配律(distributive law)

设(X,*, Δ)是代数系统，*和Δ是X上的两个二元运算。

(1)称*运算对Δ运算满足分配律⇔

a) $(\forall x \in X)(\forall y \in X)(\forall z \in X)$

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

b) $(\forall x \in X)(\forall y \in X)(\forall z \in X)$

$$( ( y \,\Delta\, z ) * x = ( y * x ) \,\Delta (z * x ));$$

## 定义7. 分配律(distributive law)

(1) ……

(2) 称运算$\Delta$对运算$*$满足分配律$\Leftrightarrow$

a) $(\forall x\in X)(\forall y\in X)(\forall z\in X)$

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

b) $(\forall x\in X)(\forall y\in X)(\forall z\in X)$

$$((y*z)\,\Delta\,x = (y\,\Delta\,x)*(z\,\Delta\,x))$$ 。

例18.在代数系统$(I,+,\times)$中

(1)乘法对加法满足分配律吗？

(2)加法对乘法满足分配律吗？

例19.在代数系统$(2^X,\cap,\cup)$中

(1)$\cap$对$\cup$满足分配律吗？

(2)$\cup$对$\cap$满足分配律吗？

## 定义8.反身律　鞋袜律

设(X,*,$^{\clubsuit}$)是代数系统，*是X上的二元运算，$^{\clubsuit}$是X上的一元运算。

(1)称$^{\clubsuit}$运算满足反身律$\Leftrightarrow(\forall x\in X)((x^{\clubsuit})^{\clubsuit} = x)$；

(2)称$^{\clubsuit}$运算关于*运算满足鞋袜律

$$\Leftrightarrow(\forall x\in X)(\forall y\in X)((x * y)^{\clubsuit} = y^{\clubsuit} * x^{\clubsuit})$$ 。

例20. 在代数系统$(\Sigma^*, o, v)$中，$\Sigma^*$是$\Sigma$上字的全体集合， o是两个字的毗连(concatenation)运算， $v$是一个字的逆置(倒置(inverse))运算。例如，取$\Sigma=\{a,b\}$,字

$\alpha$=abaaaaabbbbb，$\beta$=abbbbaa, 则有

$\alpha$ o $\beta$=abaaaaabbbbb o abbbbaa

=abaaaaabbbbbabbbbaa

$\alpha^v$=bbbbbaaaaaba

于是$v$运算满足反身律： $(\alpha^v)^v=\alpha$

$v$运算关于o运算满足鞋袜律： $(\alpha \circ \beta)^v=\beta^v \circ \alpha^v$ 。

注: •一个字$\alpha\in \Sigma^*$称为是一个迴文(palindromes)$\Leftrightarrow \alpha^v=\alpha$ 。

## 定义9. 反身律 de Morgan律

设(X,∗, Δ, ♣)是代数系统，∗和Δ是X上的两个二元运算，♣是X上的一元运算。

(1) 称♣运算满足反身律⇔$(\forall x \in X)((x^{♣})^{♣} = x)$；

(2) 称♣运算关于∗运算和Δ运算满足de Morgan律⇔

a) $(\forall x \in X)(\forall y \in X)((x * y)^{♣} = x^{♣} \Delta y^{♣})$ ；

b) $(\forall x \in X)(\forall y \in X)((x \Delta y)^{♣} = x^{♣} * y^{♣})$ 。

例21. 在代数系统 $(2^X,\cap,\cup,')$ 中

(1) $'$ 满足反身律，因为 $\forall A\in 2^X$，有 $(A')'=A$

(2) $'$ 关于 $\cap$ 和 $\cup$ 满足de Morgan律。

## 定义10.子代数系统(subalgebra system)

设A=(X,$O_1$,$O_2$,…,$O_m$)是代数系统，其中$O_1$,$O_2$,…,$O_m$是X上的m个运算，其元数分别为$p_1$ , $p_2$ , … , $p_m$ 。若有子集S⊆X且S≠∅，对A中的每一个运算$O_{i}$, 有其子关系$O_{si} \subseteq O_i$ ，使得$O_{si}$也是S上的$P_i$元运算(**$O_{si}=O_i \cap (S^{Pi} \times ?)$**)，从而使得(S, $O_{S1}$, $O_{S2}$ , …, $O_{Sm}$ )也构成一代数系统，则 称此代数系统是A的子代数系统，记为

$A_s$=(S, $O_1$, $O_2$ , … ,$O_m$ ) 。

例22. $X=\{a,b,c,d\}$，$S_1=\{a,b\}$，$S_2=\{c,d\}$是X的两个子集，

$(S_1,*_1)$是$(X,*)$的子代数系统？

$(S_2,*_2)$是$(X,*)$的子代数系统？

| * | a | b | c | d |
|---|---|---|---|---|
| a | a | b | c | d |
| b | a | b | c | d |
| c | d | c | b | a |
| d | d | d | b | a |

表4

| $*_1$ | a | b |
|---|---|---|
| a | a | b |
| b | a | b |

表5

| $*_2$ | c | d |
|---|---|---|
| c | b | a |
| d | b | a |

表6

例23. $(N,+,\times)$、$(I,+,\times)$、$(Q,+,\times)$都是$(R,+,\times)$的子代数系统吗？

例24. 在代数系统 $(I,+,\times)$中，取I的两个子集如下：

$E=\{x:x$是偶数$\}$，$O=\{y:y$是奇数$\}$

$(E,+,\times)$是$(I,+,\times)$的子代数系统吗？

$(O,+,\times)$能构成$(I,+,\times)$的子代数系统吗？

## 定理3.遗传性定理

设(X，*)是代数系统，*是X上的二元运算。(S，*)是(X，*)的子代数系统。则

(1)*运算在X上有结合律$\Rightarrow$ *运算在S上有结合律；

(2)*运算在X上有交换律$\Rightarrow$ *运算在S上有交换律。

[证].只证(1)

对于任何元素$a,b,c\in S$，由于$S\subseteq X$，所以$a,b,c\in X$。而*运算在X上有结合律，因此有 $(a*b)*c=a*(b*c)$。

由于(S，*)是(X，*)的子代数系统，*运算关于S封闭，$(a*b)*c\in S$, $a*(b*c)\in S$，因此上述等式在S上也是成立的。这说明*运算在S上也有结合律。

# §2.代数系统的同态和同构

- 代数系统间的同态
- 代数系统间的同构关系

# §2.代数系统的同态和同构

例1. $(2^A,\cup)$是代数系统。

这里$A=\{a\}$，$\cup$是$2^A$上的并运算。

| $\cup$ | $\varnothing$ | $A$ |
|---|---|---|
| $\varnothing$ | $\varnothing$ | $A$ |
| $A$ | $A$ | $A$ |

例2. $(B,\vee)$是代数系统。

这里$B=\{0,1\}$，$\vee$是$B$上的或运算 。

| $\vee$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

## 定义1.同类型(same type)

称两个代数系统

$A=(X,O_1,O_2,\ldots,O_m)$和$B=(Y,O_1',O_2',\ldots,O_n')$

是同类型的代数系统⇔

(1) $m = n$;

(2)$O_i$运算和相对应的$O_i'$运算的元数相同 ( $i= 1, \cdots,m$ )。

例3. $(I, +,\times)$ 和$(2^X, \cap, \cup)$是两个同类型的代数系统。

例4. $(2^X, \cap, \cup,')$ 和$(B, *,\oplus,^-)$是两个同类型的代数系统 。

## 定义2.同态(homomorphism)

称两个同类型的代数系统

$A=(X,O_1,O_2,\ldots,O_m)$和$B=(Y,O'_1,O'_2,\ldots,O'_m)$

是同态的⇔存在着一个函数 h：X→Y 使得：

对任何一对运算$O_i$和 $O'_i$( i= 1, ⋯,m ) (其元数为$p_i$ )，都满足如下的同态公式：

$\forall(x_1,x_2,\ldots,x_{pi})\in X^{pi}$

$$h(O_i(x_1,x_2,\ldots,x_{pi}))=O'_i(h(x_1),h(x_2),\ldots,h(x_{pi})) \quad ①$$

注：● 称**函**数 h 是**保持**运算的；并称**函**数 h 为从A到B的同**态函**数，

记为h：A~B；称两代数系统A与B同**态**，记为A ~ B；

● h对$O_i$和 $O_i'$**保持**运算的含义是**指**在 h 的作用下，元素运算结**果**的象等于元素象的运算结**果**。

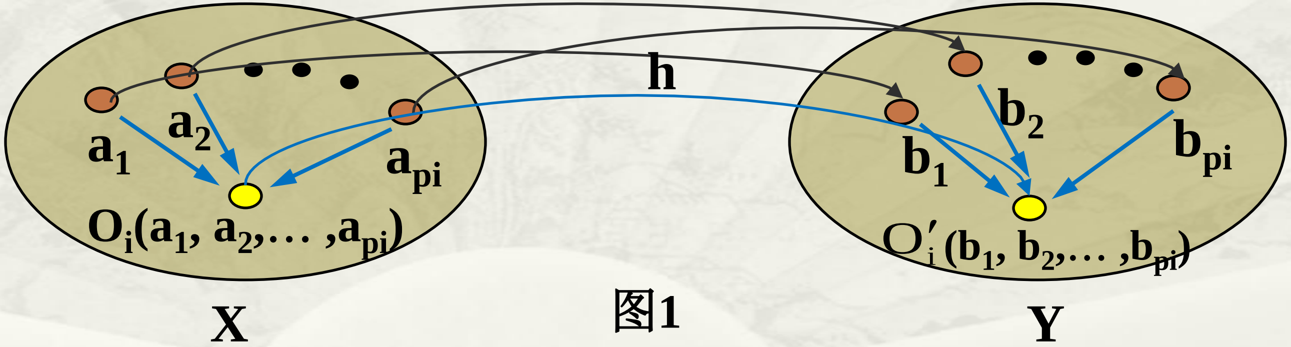



图1

元素运算结**果**的象等于元素象的运算结**果**

## 定义3.同态象  单同态  满同态

设代数系统$A=(X,O_1,O_2,\cdots,O_m)$同态于代数系统$B=(Y,O_1',O_2',\cdots,O_m')$，其同态函数为 $h: X\to Y$ 。

(1)称X在h下的象集$h(X)\subseteq Y$与B的所有运算一起组成的

$C=(h(X),O_1',O_2',\cdots,O_m')$是A的同态象；

(2)若h是单射函数，则称h是从A到B的单同态函数并称C为A的单同态象；

(3)若h是满射函数，则称h是从A到B的满同态函数；并称 B为A的满同态象(这时有h(X)=Y ,C=B) 。

例5.代数系统(N, +)与代数系统($N_m$ , $+_m$ )是满同态的。

$N_m=\{[0]_m , [1]_m ,...,[m-1]_m\}$，二元运算$+_m$定义如下：

$\forall [i]_m,[j]_m \in N_m$ ,　　　　$[ i ]_m +_m [ j ]_m = [(i+j) \bmod m]_m$，

……

例6.代数系统(N,+)与代数系统(X,×)是满同态的。

这里N是自然数集合,＋是自然数加法。

X={1, -1}，×是整数乘法，其运算表如下：

| × | 1 | -1 |
|---|---|---|
| 1 | 1 | -1 |
| -1 | -1 | 1 |

……

定理1. 设代数系统$A=(X,O_1,O_2,\cdots,O_m)$同态于代数系统

$B=(Y,O'_1,O'_2,\cdots,O'_m)$，其同态函数为 h：$X\to Y$ 。则A的同态

象 $C=(h(X),O'_1,O'_2,\cdots,O'_m)$是B的子代数系统。

[证].只须证B的每个运算 $O'_i(1\le i\le m)$(设其元数为$p_i$ )在h(X)上

都是封闭的即可。

对于任何元素$y_1$， $y_2, \ldots, y_{pi} \in \mathbf{h}(X)$，由于$\mathbf{h}(X)$是X的象集，故存在着其原象$x_1$， $x_2, \ldots, x_{pi} \in X$，使得

$$\mathbf{h}(x_1) = y_1,\ \mathbf{h}(x_2) = y_2,\ \ldots, \mathbf{h}(x_{pi}) = y_{pi}$$

于是 $O'_i(y_1,\ y_2, \ldots, y_{pi})$

$=O'_i(\mathbf{h}(x_1), \mathbf{h}(x_2), \ldots, \mathbf{h}(x_{pi}))$

$=\mathbf{h}(O_i(x_1, x_2, \ldots, x_{pi}))$　　　（同态公式）

$=\mathbf{h}(x)$　　　（$O_i$运算在X上是封闭的，故可设 $O_i(x_1, x_2, \ldots, x_{pi})=x\in X$）

$\in \mathbf{h}(X)$

该运算是封闭的；于是由子代数系统的定义可知A的同态象C是B的子代数系统。

# 定理2.同态遗传定理

设(X，$*$)和(Y，o) 是两个代数系统，$*$ 和 o 分别是X和Y上的二元运算，h 是从(X，$*$ )到(Y，o )的满同态函数，那么：

(1)$*$运算满足结合律$\Rightarrow$ o运算满足结合律；

(2)$*$运算满足交换律$\Rightarrow$ o运算满足交换律；

(3)e是关于$*$运算的幺元$\Rightarrow$ h(e) 是关于o运算的幺元；

(4)0是关于$*$运算的零元$\Rightarrow$ h(0) 是关于o运算的零元；

(5)$x$关于 $*$运算有逆元$x^{-1} \Rightarrow$ h($x$) 关于o运算的逆元是 h($x^{-1}$),

即 $[h(x)]^{-1} = h(x^{-1})$ 。

注：(1)定义**遗**传：例如， 定义$x\vee y=\max(x, y)$，$x\wedge y=\min(x, y)$

则**求**大，**求**小的对称性就**转变**为运算$\vee$和$\wedge$的交**换**律;

**又**例如，当 定义 $[i]_m +_m [j]_m = [(i+j) \bmod m]_m$

时，自然数加法的结合律、交**换**律实**际**上**已**自**动遗**传给运算$+_m$了；

(2)子代数**遗**传(**参**见§1定理3)；

(3)同**态遗**传(即本定理)；

[证].只证(1), (3), (5),

(1)对于任何元素$y_1, y_2, y_3 \in$ Y，由于h是满射，故存在着其原象$x_1, x_2, x_3 \in$ X，使得 $h(x_1)=y_1$, $h(x_2)=y_2$, $h(x_3)=y_3$,于是

$(y_1 \circ y_2) \circ y_3$

$=(h(x_1) \circ h(x_2)) \circ h(x_3)$

$= h(x_1 * x_2) \circ h(x_3)$ (同态公式)

$= h((x_1 * x_2) * x_3)$ (同态公式)

$= h(x_1 * (x_2 * x_3))$ (∗运算的结合律)

$= h(x_1) \circ h(x_2 * x_3)$ (同态公式)

$= h(x_1) \circ (h(x_2) \circ h(x_3))$ (同态公式)

$= y_1 \circ (y_2 \circ y_3)$ 所以o运算满足结合律；

(3)令$e' = h(e) \in Y$。对于任何元素$y \in Y$，由于h是满射，故存在着其原象$x \in X$，使得 $h(x) = y$，于是

$$
\begin{aligned}
& e' \circ y \\
&= h(e) \circ h(x) \\
&= h(e * x) && \text{(同态公式)} \\
&= h(x) && \text{(e是关于*运算的幺元)} \\
&= y \\
&= h(x) \\
&= h(x * e) && \text{(e是关于*运算的幺元)} \\
&= h(x) \circ h(e) && \text{(同态公式)} \\
&= y \circ e'
\end{aligned}
$$

即 $e' \circ y = y \circ e' = y$，所以$e' = h(e)$是关于o运算的幺元；

(5)令$e' = h(e) \in Y$。对于任何元素$x \in X$， 由于存在着其逆元$x^{-1} \in X$，故此 $h(x), h(x^{-1}) \in Y$，于是有

$h(x) \circ h(x^{-1})$

$= h(x * x^{-1})$ (同态公式)

$= h(e)$ ( $x^{-1}$ 是$x$关于 $*$ 运算的逆元)

$= e'$

$= h(e)$

$= h(x^{-1} * x)$ ($x^{-1}$ 是$x$关于 $*$ 运算的逆元)

$= h(x^{-1}) \circ h(x)$ (同态公式)

即 $h(x) \circ h(x^{-1}) = h(x^{-1}) \circ h(x) = e'$

所以$h(x)$关于o运算的逆元是$h(x^{-1})$ ,即 $[h(x)]^{-1} = h(x^{-1})$ 。

## 定义4.同构(isomorphism)

设代数系统$A=(X,O_1,O_2,\cdots,O_m)$同态于代数系统$B=(Y, O'_1, O'_2,\ldots,O'_m)$，其同态函数为 $h: X\to Y$ 。若h是双射函数，则称h是从A到B的同构函数,记为$h: A\cong B$ ；并且这时 称A和B同构,记为$A\cong B$ 。

注：●同**态**和同构概念要**求**两个代数系统**必须**是同类**型**的。

●同构概念要**求**两个集合**必须**是等**势**的(即 $\overline{\overline{X}}=\overline{\overline{Y}}$或$|X|=|Y|$ )。

●同构概念是**双向**的、相**互**的、可**逆**的。

●同**态**概念是单方**向**的、不可**逆**的。

例7.集合代数$(2^X,\cap,\cup,',\subseteq,\varnothing,X)$与布尔代数

$(B, *,\oplus,^-, \preccurlyeq,0,1)$是同构的，

这里：$X=\{a_1, a_2, \ldots,a_n\}$， $B=\{S:S=\bigoplus_{a\in C} a \wedge C\subseteq X\}$。

……

例8.集合代数$(2^X, \cap, \cup, ', \varnothing, X)$与布尔代数$(B, \wedge, \vee, \neg, 0, 1)$是同构的。 这里$X=\{a\}$, $2^X=\{\varnothing, X\}$, $B=\{0,1\}$，其运算表如下：

| $\cap$ | $\varnothing$ | X |
|---|---|---|
| $\varnothing$ | $\varnothing$ | $\varnothing$ |
| X | $\varnothing$ | X |

表4

| $\cup$ | $\varnothing$ | X |
|---|---|---|
| $\varnothing$ | $\varnothing$ | X |
| X | X | X |

表5

| | $'$ |
|---|---|
| $\varnothing$ | X |
| X | $\varnothing$ |

表6

| $\wedge$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

表7

| $\vee$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

表8

| | $\neg$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

表9

……

构造自然映射　h：$2^X \to B$　使得

$h(\varnothing)=0, h(X)=1$，

则容易验证h是同构函数……。

同时　$h^{-1}$：$B \to 2^X$

$h^{-1}(0)=\varnothing$ , $h^{-1}(1)=X$。

$h^{-1}$ 是从$(B, \wedge, \vee, \neg, 0, 1)$到$(2^X, \cap, \cup, ', \varnothing, X)$的同构函数，即$(B, \wedge, \vee, \neg, 0, 1)$与$(2^X, \cap, \cup, ', \varnothing, X)$同构。

例9. (N, +)和(E, +)同构。

取函数 h：$N \rightarrow E$，$h(i)=2i \quad (\forall i \in N)$

……。

例10. $(R, +)$和$(R^{+}, \times)$同构。

取函数 h：$R \rightarrow R^{+}$，$h(\alpha)= e^{\alpha}$

……。

# 不同构的例子

## **定理3.**代数系统间的同构关系≅是X上的等价关系。

其中：X={A**:**A是代数系统}。

[证].(以下都以仅含一个二元运算的代数系统为例)

由等价关系的定义知要证≅是

(1)自反的：这点可由幺函数来保证；

对于任何代数系统A=(X,*),有幺函数 I**:X** →X

使得 ∀a∈X **,** I(a)=a 。

幺函数是双射函数；

∀a,b∈X ,I(a * b)=a*b=I(a)*I(b),满足同态公式；

故I：A≅A；故A≅A 。

(2)对称的：这点可由逆函数来保证；

对于任何两个代数系统A=(X,*), B=(Y, Δ),

若有A ≅ B，则有同构函数h：A ≅ B 。

从而h：X→Y ；

h是双射函数；

h满足同态公式：$\forall a,b \in X$ ,h(a * b)=h(a)Δh(b) ；

于是有逆函数$h^{-1}$存在 $h^{-1}$ ：Y→X ；

$h^{-1}$是双射函数(参见第三章§1定理1)；

……

并且对任何元素$c,d\in Y$,都存在着$a,b\in X$ ,使得$h(a)=c$， $h(b)=d$ ，从而$h^{-1}(c)=a$， $h^{-1}(d)=b$ ，于是有

$$
\begin{aligned}
& h^{-1}(c\Delta d) \\
&= h^{-1}(h(a)\Delta h(b)) \\
&= h^{-1}(h(a*b)) && \text{（h满足同态公式）} \\
&=(h^{-1}\circ h)(a*b) \\
&=I(a*b) && \text{（}h^{-1}\text{是h的逆函数）} \\
&=a*b \\
&= h^{-1}(c)*h^{-1}(d)
\end{aligned}
$$

所以$h^{-1}$满足同态公式； 所以$h^{-1}$ ：$B\cong A$；所以 $B\cong A$；

(3)传递的：这点可由复合函数来保证。

对于任何三个代数系统A=(X,*), B=(Y, Δ),以及C=(Z,♣),若有

A≅B，且 B≅ C，则有同构函数：

h：A≅ B， g：B≅ C 。

从而有函数h：$X\rightarrow Y$， g：$Y\rightarrow Z$，

h,g都是双射函数；

h ,g都满足同态公式：

$\forall a,b\in X, h(a * b)=h(a)\Delta h(b)$

$\forall c,d\in Y, g(c\Delta d)=g(c)\clubsuit g(d)$； ……

…… 于是有复合函数 goh： X→Z,

goh是双射函数(参见第三章§2定理1)；

并且对任何元素$a,b\in X$ , 有

$(goh)(a * b)$

$= g(h(a * b))$

$= g(h(a)\Delta h(b))$ (h满足同态公式)

$= g(h(a))\clubsuit g(h(b))$ (g满足同态公式)

$=(goh)(a)\clubsuit(goh)(b)$

所以goh满足同态公式；

所以goh： A≅C ；所以 A≅C。

# §3.半群与单子

- 半群的基本概念
- 交换半群与含幺半群(单子)
- 循环半群
- 子半群

# §3.半群与单子

**定义1.**半群(semigrop)

设(X, ∗)是代数系统，∗ 是X上的二元运算。若 ∗运算满足结合律，则称(X, ∗ )为半群。

注：•半群就是具有结合律的代数系统;

•验证半群的要点是验证运算的

(1)封闭性；(2)结合律。

**例1. (I,×)是半群。**

**这里：I 是整数集合， ×是整数乘法。由 § 1的例1. (1) 已知(I,×)是代数系统；**

**由算术知识知整数乘法×满足结合律，即**

$\forall a, b, c \in I$ ， **(a×b)×c= a×(b×c)** ；

**由半群的定义知(I,×)是半群。**

**例2.** $(M_{n\times n}, \times)$是半群。

这里：$M_{n\times n}$是n 阶实(方)矩阵的全体，$\times$是矩阵乘法。

**例3.** $(2^X, \cap)$是半群。

这里：X 为非空集合，$2^X$是 X 的幂集，$\cap$是$2^X$上的集合交运算。

**例4.**$(N_m, \times_m)$是半群。 这里：

$N_m=\{[0]_m, [1]_m, \ldots, [m-1]_m\}$， $\times_m$定义如下

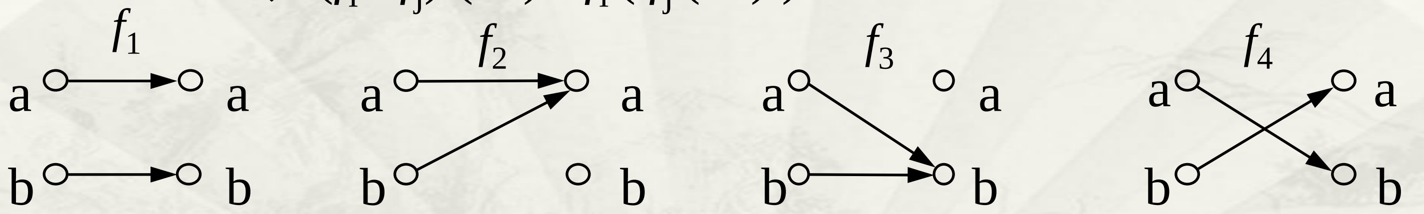
$\forall [i]_m, [j]_m \in N_m$，

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

**例5.** $(P[x], \times)$是半群。这里： $P[x]$ 是实系数多项式的全体，$\times$是多项式的乘法。

**例6.** $(X^X, \circ)$是半群(参见§1例2)。 这里：$X=\{a,b\}$，$X^X=\{f \mid f:X\rightarrow X\}=\Omega$，则由§1例2 已知$(X^X, \circ)$是代数系统；由第五章函数§2.函数的复合知函数的复合运算$\circ$满足结合律；由半群的定义知$(X^X, \circ)$是半群，

这里 $\forall x\in X$，$(f_i \circ f_j)(x)=f_i(f_j(x))$。




| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
| $f_2$ | $f_2$ | $f_2$ | $f_2$ | $f_2$ |
| $f_3$ | $f_3$ | $f_3$ | $f_3$ | $f_3$ |
| $f_4$ | $f_4$ | $f_3$ | $f_2$ | $f_1$ |

半群例子： 设(S, *)是半群，X={f | f:S →S}，定义X上的运算Δ如下：

$\forall f,g \in X$， $\forall x \in S$，  $(f \Delta g)(x) = f(x)*g(x)$。

则(X, Δ)是半群。

## **定义2.**单子(monoid)。 设(X，*)是半群。

(1)若*运算满足交换律，则称(X，*)是交换半群。

(2)若X关于*运算有幺元，则称(X，*)是含幺半群或者单子。

(3)若*运算满足交换律同时X关于*运算又有幺元，则称(X，*)是交换含幺半群或交换单子。

**例7. (I，×)是交换含幺半群吗？幺元是什么？**

**$(M_{n\times n}$，×)是交换半群吗？是含幺半群吗？幺元是什么？**

**$(N_m$，$\times_m)$是交换含幺半群，幺元是什么？**

**$(2^X$，∩)是交换含幺半群吗？幺元是什么？**

**(P[$x$]，×)是交换含幺半群吗？幺元是什么？**

**$(X^X$，o)是交换半群吗？是含幺半群吗？幺元是什么？**

**例8.** 自由单子(free monoid)($\Sigma^*$, o)。设Σ是一有限集，称为字母表(alphabet)，任一元素$a\in\Sigma$称为字母(alpha)。则$\Sigma^*$是Σ上字的全体集合，

$$\Sigma^* = \{\Lambda\}\cup\Sigma\cup\Sigma^2\cup\Sigma^3\cup\ldots\cup\Sigma^n\cup\ \ldots \quad (\Lambda\text{称为空字})$$

其任何元素 $w\in\Sigma^*$称为一个字(word)；必有 $k\in N$ ,使得$w\in\Sigma^k$，从而

$$w = (a_{i1}, a_{i2}, a_{i3}, \ldots, a_{ik}) = a_{i1}\, a_{i2}\, a_{i3} \ldots a_{ik} \qquad \text{这里} a_{ij}\in\Sigma\ \ (1\le j\le k)\ 。$$

o是Σ上字的毗连或并置(concatenation)运算，

1）对任何两个字$w_1, w_2\in\Sigma^*$，

$$w_1 \circ w_2 = w_1 w_2 \in \Sigma^*$$

仍是Σ上的一个字，且结果唯一，满足封闭性，故o是$\Sigma^*$上的二元运算；

2）对任何三个字$w_1, w_2, w_3 \in \Sigma^*$，

$$(w_1 \circ w_2) \circ w_3 = w_1 w_2 \circ w_3 = w_1 w_2 w_3$$

$$w_1 \circ (w_2 \circ w_3) = w_1 \circ w_2 w_3 = w_1 w_2 w_3$$

$$(w_1 \circ w_2) \circ w_3 = w_1 \circ (w_2 \circ w_3)$$

所以 o运算具有结合律；

3）对任何字$w \in \Sigma^*$，

$$\Lambda \circ w = w \circ \Lambda = w$$

所以$\Sigma^*$关于o运算具有幺元，是空字$\Lambda$；

4）对任何两个字$w_1, w_2 \in \Sigma^*$，一般地

$$w_1 \circ w_2 \neq w_2 \circ w_1$$

所以o运算不具有交换律；

因此，$(\Sigma^*, \circ)$是一个含幺半群， 称为**自由单子**。它将在计算机编译系统中应用到。

但$(\Sigma^*, \circ)$不是一个交换半群。

自由单子的一个例子如下，若取$\Sigma=\{a,b\}$,则

$\Sigma^*=\{\Lambda$,a,b,aa,ab,ba,bb,aaa,aab,aba,abb,baa,

bab,bba,bbb,aaaa,aaab,aaba,aabb, … …}。

## 定义3.元素的乘幂

设(X，*)是代数系统，*是 X 上的二元运算。X 中元素的乘幂定义如下：$\forall x \in X$,

$x^{1} = x$；

$x^{m+1} = x^{m} * x \ (m \in N)$。

例9. 在代数系统(N，+)中，$1\in N$，于是有：

$1^1 = 1,\ 1^2 = 2,\ 1^3 = 1^2 + 1 = 2 + 1 = 3,\ \ldots,\ 1^n = n,\ \ldots$

例10. 在代数系统($2^X$，$\cap$)中，$A\in 2^X$，于是有：

$A^1=A,\ A^2=A\cap A=A,\ A^3=A^2\cap A=A\cap A=A, \ldots,$

$A^n=A^{n-1}\cap A =A\cap A=A, \ldots$

## **定理1.** 指数律

设(X，∗)是半群。任取 $x\in X$， $\forall m$、$n\in N$，有

(1)$x^m * x^n = x^{m+n} = x^n * x^m$；

(2)$(x^m)^n = x^{mn} = (x^n)^m$ 。

[证].采用归纳法

(1)固定m,选取n为归纳变元。

当n=1时，由定义3知有$x^m * x^1 = x^{m+1}$；

当n=k时， 设有$x^m * x^k = x^{m+k}$；

当n=k+1时， 有$x^m * x^{k+1} = x^m * (x^k * x)$ （定义3）

$= (x^m * x^k) * x$ （结合律）

$= x^{m+k} * x$ （归纳假设）

$= x^{m+(k+1)}$ （定义3）

故对任意的m、n∈N，有 $x^m * x^n = x^{m+n}$ 。

(2)当n=1时，由定义3知$(x^{m})^{1} = x^{m} = x^{m\times 1}$；

当n=k时，设有$(x^{m})^{k}= x^{m k}$；

当n=k+1时，有$(x^{m})^{k+1} = (x^{m})^{k} * x^{m}$ (定义3)

$= x^{mk} * x^{m}$ (归纳假设)

$= x^{mk+m}$ (根据(1))

$= x^{m(k+1)}$

故对任意的m、n∈N，有 $(x^{m})^{n} = x^{m n}$ 。

## 定义4.循环半群（cyclic semigroup）

设（X，∗）是半群。若存在着元素 $x_0 \in X$ ，使得

$$(\forall x \in X)(\exists n \in N)(x = x_0^n)$$

则称（X，∗）为循环半群；同时称 $x_0$ 是该循环半群的生成元（generating element）。

**例11.** 在$(N,+)$,$(N,\times)$,$(N_5 ,+_5)$这三个代数系统中：

(1)$(N,+)$ 是循环半群，生成元是1；

(2)$(N, \times)$不是循环半群，因为它无生成元；

(3)$(N_5 , +_5)$是循环半群，其中$[1]_5$，$[2]_5$，$[3]_5$，$[4]_5$都是它的生成元，即$(N_5 , +_5)$的生成元不唯一。

(4) )$(N_6 , +_6)$?

## 定理2. 循环半群一定是交换半群。

[证].设(X,$*$)是循环半群，生成元是$x_0 \in X$ 。于是，

对任何元素$x$，$y \in X$,存在着自然数m，$n \in N$，使得

$x = x_0^m$，$y = x_0^n$，从而

$$x * y = x_0^m * x_0^n$$

$$= x_0^n * x_0^m \qquad \text{（定理1的(1)）}$$

$$= y * x$$

故$*$运算满足交换律；即(X, $*$)是交换半群。

## **例12.** $(N_5, \times_5)$不是循环半群

取交换含幺半群$(N_5, \times_5)$(参见例7(3))，其幺元是$[1]_5$，其运算表见表1。由表1知$(N_5, \times_5)$确实是交换半群(因其运算表是对称的)。

但$(N_5, \times_5)$不是循环半群。因为$N_5$中的$[0]_5$无法表示成任何元素的乘幂。

| $\times_5$ | 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 |

**表1**

注：•这里，将$N_5=\{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$简化表示为$N_5=\{0, 1, 2, 3, 4\}$。

## 半群例子：设(S, *)是有限半群，那么S中存在着幂等元。

## **定义5.**子半群(sub-semigroup)

设 (X，$*$)是半群，$S \subseteq X$且$S \neq \varnothing$。若(S，$*$ )是(X，$*$)的子代数系统，并且(S，$*$)也构成半群,则称(S，$*$)是(X，$*$)的子半群。

注：●子**半群**的概念是子代数系统概念在**半群**这种代数系统中的**具**体体现。

●由本章§1的定理3**知**，若代数系统中的二元运算满足结合律，则子代数系统中的二元运算也满足结合律，因此**半群**的子代数系统就是这个**半群**的子**半群**。

●因此，**验**证子**半群**与**验**证子代数系统一**样**，**必须验**证条件：

1°$S \subseteq X$；

2° $S \neq \varnothing$ ；

3°**封**闭性。