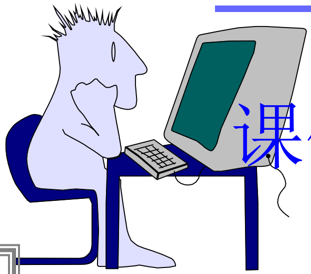
离散数学

主讲：李淑琴

Lishuqin2005@bistu.edu.cn



课件邮箱：lisanshuxue2012@126.com

密码：lssx2012

考试、课时、答疑安排

- 课时安排

  授课　：32学时

  考试方式

  笔试闭卷(选修)

  成绩评定：平时30%，考试70%

- 每周周五前交作业，全能扫描王扫描为.pdf格式上传到课堂，课码：GWEPD4

- 答疑安排

  周三、周五全天　健翔桥**3-221**教研室

前言：

人们研究和考察现实世界中的各种现象或过程，往往要借助于某些数学工具。如：

代数学中，用正整数集合上的加法描述累计数；

集合间的“并”“交”描述单位与单位之间的关系；

微积分学中，用导数来描述质点运动的速度；用定积分来计算面积、体积等

针对某个具体问题选用适宜的数学结构去进行较为确切地描述，就是所谓的“数学模型”

或者说数学模型就是对于一个特定的对象为了一个特定目标，根据特有的内在规律，做出一些必要的简化假设，运用适当的数学工具，得到的一个数学结构。数学结构可以是数学公式，算法、表格、图示等。

在此我们研究一类特殊的数学结构--------由集合上定义若干个运算组成的系统，我们称为**代数系统**，也称为**代数结构**。

第五章　代数系统的基本概念

- 二元运算及其性质
- 代数系统
- 代数系统的同态和同构

第五章　代数系统的基本概念

- 二元运算及其性质
- 代数系统
- 代数系统的同态和同构

5.1 二元运算及其性质

定义. 设A， B,C是非空集合,从A×B到C的映射（或函数）

$$f: A\times B\text{->}C$$

称为A×B到C的二元函数。

例如： (1)设A={0,1}，B={1,2}，C={奇，偶}，定义映射*，*（0,1）=偶，*（0,2）=偶，*（1,1）=奇，*（1,2）=奇

（2）一架售货机，只接收五角和一元硬币，对应的商品有纯净水、矿泉水和橘子汁。当人们投入上述硬币的任何两枚时，自动售货机供应相应的商品。

5.1 二元运算及其性质

定义： n元运算

.设A为集合,n为正整数,则函数

$$f: A\times A\ldots\ldots\times A \to A$$

称为A上的一个n元运算,简称为n元运算.n也称为运算的阶。

集合上的运算，其运算结果都是在原来的集合S中，具有这种特征的运算是封闭的，简称闭运算。

5.1 二元运算及其性质

定义. 一元运算

设A是非空集合,从A.到A的映射（或函数）

f: A->A

称为A上的一元运算。

例如:

1. 一元运算

A.在实数集R上,求一个数的相反数;

B.在非零实数集R*上求一个数的倒数;

C.在幂集合P(A)上,如果规定全集为A,那么求集合的绝对补运算可以看作是P(A)上的一元运算.

5.1 二元运算及其性质

定义.二元运算

设A是非空集合,从A×A到A的映射（或函数）

$$f: A\times A \to A$$

称为A上的二元运算。

(1)自然数集合N上的乘法是N上的二元运算,但除法不是.

(2)整数集合Z上的加法、减法和乘法是Z上的二元运算,而除法不是.

(3)非零实数集R*上的乘法和除法都是R*上的二元运算,而加法、减法不是.

(4)设$M_n(R)$表示所有n阶实矩阵的集合(n≥2),即

$$M_n(\mathbf{R}) = \left\{ \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \vdots & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \middle| a_{ij} \in \mathbf{R} \right\}$$

则矩阵加法和乘法都是$M_n(R)$上的二元运算,

(5)A为任意集合,则∪,∩,—,⊕为A的幂集P(A)上的二元运算,

(6)S为集合, S^S是S上的所有函数的集合,则合成运算.是 S^S上的二元运算.

定义.三元运算

设A是非空集合,从A×A ×A到A的映射（或函数）

$$f: A\times A \times A \to A$$

称为A上的三元运算。

例如.三元运算

在空间直角坐标系中求某一点(x,y,z)的坐标在x轴上的投影可以看作是实数集R上的三元运算 $f(<x,y,z>) = x$,因为参加运算的是有序的3个实数,而结果也是实数.

使用算符表示n元运算

若$f(<S,T,\cdots;a_n>)=b$,则可记为

$$\circ(S,T,\cdots;a_n)=b$$

通常用$\circ$,$*$,$\cdot$,...等符号表示二元运算

前缀表示法:

$\circ(a)=b$　　一元运算,

$\circ(S,T)=b$　　二元运算,

$\circ(S,T,a_3)=b$　　三元运算.

二元运算的中缀表示法：

$$x \circ y = z$$

如果集合A是有穷集,A上的一元和二元运算也可以用运算表给出.表5,1和5.2是一元和二元运算表的一般形式

表 5.1

a_i	$\circ(a_i)$
a_1	$\circ(a_1)$
a_2	$\circ(a_2)$
$\vdots$	$\vdots$
a_n	$\circ(a_n)$

表 5.2

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	$\cdots$	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	$\cdots$	$a_2 \circ a_n$
$\vdots$		$\vdots$		
a_n	$a_n \circ a_1$	$a_n \circ a_2$	$\cdots$	$a_n \circ a_n$

例5.2 设$A=\{1,2\}$,给出$P(A)$上的运算~和$\oplus$的运算表,其中全集为A.

解 所求的运算表如表5.3、表5.4所示.

表 5-3

a_i	$\sim a_i$
$\varnothing$	$\{1,2\}$
$\{1\}$	$\{2\}$
$\{2\}$	$\{1\}$
$\{1,2\}$	$\varnothing$

表 5-4

$\oplus$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\varnothing$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\varnothing$	$\{1,2\}$	$\{2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\varnothing$	$\{1\}$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	$\varnothing$

例5.3 设A={1,2,3,4},定义A上二元运算如下：

$$x \circ y = (xy) \bmod 5,\ \forall x,y \in A$$

$\circ$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

二元运算的性质

定义 交换律

设$\circ$为A上的二元运算,如果对任意的$x,y \in A$都有

$$x \circ y = y \circ x$$

则称运算$\circ$在A上是可交换的,或者说.在A上适合交换律.

例如,实数集上的加法和乘法都是可交换的,但减法不可交换, 在幂集P(A)上的$\cup,\cap,\oplus$都是可交换的,但相对补不是可交换的.

定义　结合律

设$\circ$为A上的二元运算,如果对任意的$x,y,z \in A$都有

$$(x \circ y) \circ z = x \circ (y \circ z),$$

则称运算$\circ$在A上是可结合的,或者说.在A上适合结合律.

普通的加法和乘法在N,Z,Q,R上都是可结合的,$\cup$,$\cap$,$\oplus$在幂集P(A)上也是可结合的.矩阵加法和乘法在$M_n(R)$上是可结合的,其中矩阵加法还是可交换的,但矩阵乘法不是可交换的.

定义 幂等律

设$\circ$为A上的二元运算,如果对任意的$x \in A$都有

$$x \circ x = x$$

则称该运算$\circ$适合幂等律,也可以说A中的全体元素都是幂等元.

例如，幂集P(A)上$\cup$和$\cap$适合幂等律,但对称差不适合幂等律（除非$P(A)=\varnothing$）,$\varnothing$是运算$\oplus$的幂等元.

定义　分配律.

设$\circ$和$*$是A上的两个二元运算,如果对任意的$x,y,z\in A$有

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

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

则称运算$*$对$\circ$是可分配的,也称$*$对$\circ$适合分配律.

例如,在实数集上普通乘法对加法是可分配的,在n阶实矩阵的集合$M_n(R)$上矩阵乘法对矩阵加法是可分配的,而在幂集P(A)上$\cup$和$\cap$是互相可分配的.

定义　吸收律

设$\circ$和$*$是A上的两个可交换的二元运算,如果对任意的$x,y\in A$都有

$$x*(x\circ y)=x,$$

$$x\circ(x*y)=x,$$

则称$\circ$和$*$满足**吸收律**.

例如,在幂集$P(A)$上$\cup$和$\cap$是满足**吸收律**的.

例2：设集合A={a,b},定义在A上的一个二元运算*、∘如表所示，指出这两个运算的性质

*	a	b	
a	a	b	
b	b	a	

∘	a	b
a	a	a
b	a	b

解： *是可交换，可结合。

∘ 也是可交换，可结合，幂等律

∘ 对*满足分配律，但是*对∘ 不满足分配律

左幺元,右幺元,幺元

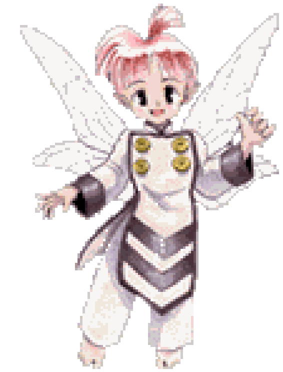
定义 左幺元 右幺元 幺元

设 $\circ$ 为A上的二元运算,如果存在元素 e_l (或 e_r) $\in A$ 使得对任何 $x \in A$, 都有

$$e_l \circ x = x \quad (\text{或} x \circ e_r = x)$$

则称 e_l(或 e_r)是A中关于运算 $\circ$ 的一个左幺元(或右幺元).若 $e \in A$ 关于 $\circ$ 既是左幺元, 又是右幺元,则称e为A上关于运算 $\circ$ 的幺元.

$$\exists e \in A, \quad \forall x \in A (x * e = e * x = x)$$



谁是幺元?

自然数集合上的加法运算的幺元是谁?

自然数集合上的乘法运算的幺元是谁?

在$M_n(R)$上,矩阵加法的幺元是谁?

在$M_n(R)$上,矩阵乘法的幺元是谁?

在幂集$P(A)$上,$\cup$运算的幺元是谁?

在幂集$P(A)$上,$\cap$运算的幺元是谁?

在命题集合中,析取运算的幺元是谁?

在命题集合中,合取运算的幺元是谁?

例：设集合A={a,b,c,d },定义在A上的一个二元运算,*如表所示：试指出代数系统<A,*>中的幺元。

*	a	b	c	d
a	a	b	c	d
b	b	a	d	d
c	c	a	a	d
d	d	d	d	d

左幺元,右幺元,幺元

定理

设$\circ$为A上的二元运算, e_l, e_r分别为运算$\circ$的左幺元和右幺元,则有

$$e_l = e_r = e.$$

且e为A上关于运算$\circ$的唯一的幺元.

证明： 因为 $e_l = e_l \circ e_r$, $e_l \circ e_r = e_r$

所以 $e_l = e_r$

把$e_l = e_r$记作e.假设A中存在幺元e',则有

$$e' = e \circ e' = e$$

所以,e是A中关于运算$\circ$的唯一的幺元.

左零元,右零元,零元

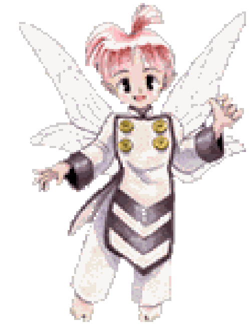
定义: 左零元　右零元　零元

设∘为A上的二元运算,若存在元素θ_l(或θ_r)$\in A$使得对任意的$x\in A$有

$$\theta_l \circ x = \theta_l \text{（或} x \circ \theta_r = \theta_r\text{）}$$

则称θ_l(或θ_r)是A上关于运算∘的左零元(或右零元)若 $\theta\in A$关于运算∘既是左零元,又是右零元,则称θ 为A上关于运算∘的零元.

$$\exists\theta\in A,\quad \forall x\in A(x*\theta = \theta*x = \theta)$$



谁是零元?

自然数集合上的加法运算的零元是谁?

自然数集合上的乘法运算的零元是谁?

在$M_n(R)$上,矩阵加法的零元是谁?

在$M_n(R)$上,矩阵乘法的零元是谁?

在幂集P(A)上,$\cup$运算的零元是谁?

在幂集P(A)上,$\cap$运算的零元是谁?

在命题集合中,析取运算的零元是谁?

在命题集合中,合取运算的零元是谁?

例：设集合A={a,b,c,d },定义在A上的一个二元运算*如表所示：试指出代数系统<A,*>中的零元。

*	a	b	c	d
a	a	b	c	d
b	b	a	d	d
c	c	a	a	d
d	d	d	d	d

定理:

设$\circ$为A上的二元运算, θ_l,θ_r分别为运算$\circ$的左零元和右零元,则有

$$\theta_l = \theta_r = \theta$$

且θ为A上关于运算$\circ$的唯一的零元.

左逆元、右逆元、逆元

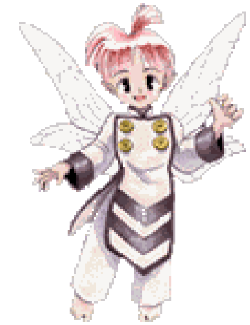
定义5.10 左逆元、右逆元、逆元

设$\circ$为A上的二元运算,$e \in A$为运算$\circ$的幺元.对于任意的$x \in A$,如果存在$y_l \in A$(或$y_r \in A$)使得

$$y_l \circ x = e(\text{或} x \circ y_r = e)$$

则称y_l(或y_r)是x的左(或右)逆元,若$y \in A$既是x的左逆元,又是x的右逆元,则称y是x的逆元.

注意：逆元是与集合中的某个元素相关。



每个元素的逆元?

自然数集每个元素关于加法运算的逆元?

整数集每个元素关于加法运算的逆元?

$M_n(R)$上，每个矩阵元素关于乘法的逆元?

$M_n(R)$上，每个矩阵元素关于矩阵加法的逆元?

在幂集P(A)上，每个元素关于$\cup$运算的逆元?

在幂集P(A)上,每个元素关于$\cap$运算的逆元?

例：设集合 S={a,b,c,d,e},定义在 S 上的一个二元运算

如表所示：试指出代数系统<S,>中的左、右逆元。

*	a	b	c	d	e
a	**a**	**b**	**c**	**d**	**e**
b	**b**	**d**	**a**	**c**	**d**
c	**c**	**a**	**b**	**a**	**b**
d	**d**	**a**	**c**	**d**	**c**
e	**e**	**d**	**a**	**c**	**e**

解：a是幺元；a的逆元为a；

b的左逆元c,d；右逆元为c；

c的左逆元b,e；右逆元为b,d；

d的左逆元c；右逆元为b；

e的左逆元无；右逆元为c；

结论:

1）一个元素的左逆元不一定等于该元素的右逆元；

2）一个元素可以有左逆元没有右逆元；也可以只有右逆元而没有左逆元；

3）一个元素的左逆元（或右逆元）可以不唯一；

定理

设$\circ$为A上可结合的二元运算,e为该运算的幺元.对于$x \in A$如果存在左逆元x_l和右逆元x_r,则有 $x_l = x_r$, 且x的逆元唯一.通常把这个唯一的逆元记作 x^{-1}

证明: $y_l = y_l \circ e = y_l \circ (x \circ y_r)$

$= (y_l \circ x) \circ y_r = e \circ y_r = y_r$.

令$y_l = y_r = y$,假设$y' \in A$是x的逆元,则有

$y' = y' \circ e = y' \circ (x \circ y) = (y' \circ x) \circ y = e \circ y = y$.

由这个定理可知,对于可结合的二元运算来说,元素x的逆元如果存在则是唯一的..

定理5.1.4

设$\circ$为A上可结合的二元运算,e为该运算的幺元.对于$x \in A$如果存在逆元x^{-1} ,则$(x^{-1})^{-1}=x$

)

定理:

设<A,*>是一个代数系统,且集合A中元素的个数大于1.如果该代数系统中存在幺元e和零元θ,则$\theta \neq$e,且θ无左（右）逆元。

证明：

用反证法，设θ=e，那么对于任意$x \in A$,必有

$x=e*x=\theta*x=\theta=e$

于是，A中所有元素都是相同的，这与A中含有多个元素相矛盾。

再用反证法，设θ有右（或左）逆元x，那么

$\theta=\theta*x=e$ 与$\theta \neq$e矛盾。故θ无左（右）逆元。得证。

定义5.1.6 元素可约的

设$\circ$为A上的二元运算,如果对$a\in A, a\neq \theta$, 如果a满足以下条件

(1)若$a\circ y = a\circ z$,则$y = z$,

(2)若$y \circ a = z \circ a$,则$y = z$

就称元素a对运算$\circ$是可约的。(1)中a为左可约的; (2) 中a为右可约的

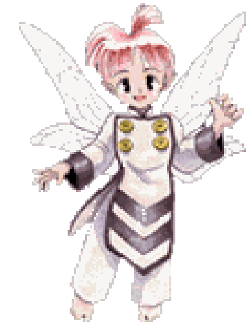
定义 消去律

设$\circ$为A上的二元运算,如果对任意的$x,y,z\in A$满足以下条件

(1)若$x\circ y = x\circ z$且x不是零元,则$y = z$,

(2)若$y\circ x = z\circ x$ 且x不是零元,则$y = z$

就称运算$\circ$满足消去律



满足消去律吗?

整数集合上加法?

满足

整数集合上乘法?

满足

幂集P(A)上∪运算?

不满足

幂集P(A)上∩运算?

不满足

幂集P(A)上⊕运算? 满足

$\forall A, B, C \in P(S)$都有

$$A \oplus B = A \oplus C \Rightarrow B = C$$

$$B \oplus A = C \oplus A \Rightarrow B = C$$

定理

设$\circ$是S上满足结合律的二元运算,且元素a有逆元（左逆元，右逆元）,则a必定是可约的（左可约的，右可约的）。

例1： 对于下面给定的集合和该集合上的二元关系，指出该运算的性质，并求出它的幺元，零元和所有可逆元素的逆元。

（1）正整数集合中的任意x，y满足

$$x * y = \mathrm{lcm}(x,y),$$

即求x和y的最小公倍数

（2）有理数集合中的任意x，y满足

$$x * y = x + y - xy$$

解 (1) $*$ 运算可交换，可结合，是幂等的.

$\forall x \in \mathbf{Z}^{+}$，$x * 1 = x$，$1 * x = x$，1 为单位元.

不存在零元.

只有 1 有逆元，是它自己，其它正整数无逆元.

(2) $*$ 运算满足交换律，因为对 $\forall x, y \in \mathbf{Q}$，

$$x * y = x + y - xy = y + x - yx = y * x$$

(2) * 运算满足交换律，因为对 $\forall x,y\in\mathbf{Q}$,

$$x*y=x+y-xy=y+x-yx=y*x$$

* 运算满足结合律，因为对 $\forall x,y,z\in\mathbf{Q}$,

$$(x*y)*z=(x+y-xy)*z=x+y+z-xy-xz-yz+xyz$$
$$x*(y*z)=x*(y+z-yz)=x+y+z-xy-xz-yz+xyz$$

所以

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

* 运算不满足幂等律，因为 $2\in\mathbf{Q}$，但

$$2*2=2+2-2\times2=0\neq2$$

* 运算满足消去律.因为 $\forall x,y,z\in Q, x\neq 1$(1 为零元),有

$$
\begin{aligned}
& x*y=x*z \\
\Rightarrow\ & x+y-xy=x+z-xz \\
\Rightarrow\ & (y-z)=x(y-z) \\
\Rightarrow\ & y=z \qquad (x\neq 1)
\end{aligned}
$$

由于 * 是可交换的,右消去律显然成立.

$\forall x\in Q$ 有

$$x*0=x=0*x$$

0 是 * 运算的单位元.

$\forall x \in \mathbf{Q}$ 有

$$x * 1 = 1 = 1 * x$$

1 是 $*$ 运算的零元.

$\forall x \in \mathbf{Q}$,欲使 $x * y = 0$ 和 $y * x = 0$ 成立,即

$$x + y - xy = 0,$$

解得

$$y = \frac{x}{x-1} \qquad (x \neq 1)$$

从而有 $x^{-1} = \dfrac{x}{x-1} \quad (x \neq 1)$.

例2：设集合A={a,b,c },定义在A上的一个二元运算*、°、.如表所示,

（1）指出这三个运算的性质

(2)分别求出它们的幺元，零元和所有可逆元素的逆元。

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

°	a	b	c
a	a	b	c
b	b	b	b
c	c	b	c

.	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

∘	a	b	c
a	a	b	c
b	b	b	b
c	c	b	c

·	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

运算	结合律	交换律	幂等律	消去律	幺元	零元	a逆元	b逆元	c逆元
*	Y	Y	N	Y	a	无	a	c	b
∘	Y	Y	Y	N	a	b	a	无	无
·	Y	N	Y	N	无	无	无	无	无

<A,*>是一个代数系统,*是A上的一个二元运算，那么该运算的有些性质可以从运算表中直接看出。即：

1.运算*具有封闭性，当且仅当运算表中每个元素都属于A。

2.运算*具有可交换性，当且仅当运算表 关于主对角线是对称的。

3.运算*具有等幂性，当且仅当运算表的主对角线上每一个元素与它所在行（列 ）的表头元素相同。

4.A关于*有零元，当且仅当该元素所对应的行和列中的元素都与该元素相同。

5. A中关于*有幺元，当且仅当该元素所对应的行和列依次与运算表的行和列相一致。

6.设A中有幺元，a和b互逆，当且仅当位于a所在行，b所在列的元素以及b所在行，a所在的元素都是幺元。

第五章　代数系统的一般性质

- 二元运算及其性质
- 代数系统
- 代数系统的同态和同构

5.2 代数系统

定义5.2.1 **代数系统(代数结构)**

非空集合A和A上的k个运算$f_1,f_2,\ldots,f_k$(其中f_i为n_i元运算,$i=1,2,\ldots,k$)组成的系统称为一个**代数系统**,简称**代数**,记作

$$\langle A, f_1,f_2,\ldots,f_k \rangle.$$

例如,常见的几个代数系统:

(1) $\langle N, + \rangle$,$\langle Z, +,\ ; \rangle$,$\langle R, +,\ \cdot, \rangle$都是代数系统,其中+为普通加法, 为普通乘法

(2) $\langle M_n(R), +, \cdot\rangle$是代数系统,其中＋和 分别表示矩阵加法和矩阵乘法.

(3) $\langle P(A), \cap, \cup, \sim\rangle$也是代数系统,它包含两个二元运算和一个一元运算.

(4) $\langle Z_n, \oplus, \otimes\rangle$是代数系统，其中

$$\mathbf{Z}_n = \{0, 1, \cdots, n-1\},$$

$\oplus$和$\otimes$分别表示模 n 的加法和乘法,对于 $\forall x, y \in \mathbf{Z}_n$

$$x \oplus y = (x+y) \bmod n, \quad x \otimes y = (xy) \bmod n$$

定义：　代数常数(特异元素)

二元运算的幺元或零元,对系统性质起着重要的作用,称之为系统的**特异元素**,或**代数常数**.

$$<Z,+,0>$$

$$<P(A),\cup,\cap,\phi,A>$$

定义5.2.2: 同类型的代数系统

如果两个代数系统中运算的个数相同，对应的阶数也相同，且代数常数的个数也相同。则称这两个代数系统具有相同的构成成分，也称他们是同类型的代数系统.

例:幂集代数和实数代数

$<P(A),\cap,\cup,\sim,A,\varnothing>$ 与 $<R,+,\times,-,0,1>$

定义5.2.3 闭运算

设*是S上的n元运算， $T \subseteq S$,如果对于任意元素$x_1,x_2,\ldots x_n \in T$,$*(x_1,x_2,\ldots x_n) \in T$,称运算*对T封闭。

子代数系统、子代数

定义5.2.4　子代数系统

设<S, * >是代数系统,如果

(1)　（1）$T \subseteq S$且$T \neq \varnothing$,

(2)　（2）运算*对T封闭的, 则称<T, * >是<S, * >的**子代数系统**,简称**子代数**.

注意：S和T不一定含有相同的代数常数,

例如.<N, + ,0>是<Z, + ,0>的子代数,因为N对加法封闭,且它们都具有相同的代数常数0.

<N-{0}, + >是<Z, + >的子代数,但不是<Z, + ,0>的子代数.因为代数常数0不出现在N-{0}中.

平凡的子代数、真子代数

对任何代数系统$<S, * >$,其子代数定存在.

最大的子代数就是$<S,*>$本身.

最小的子代数是 $<\{e\},*>$.

这种最大与最小的子代数称为S的平凡的子代数.

如果S的子代数$< T, * >$满足$T\subset S$,则称T是S的真子代数.

例5.5 设$V=<Z,+,0>$,令,

$$nZ=\{nz|z\in Z\}$$ n为自然数

那么,证明, nZ是V的子代数.

证明: 任取nZ中的两个元素nz_1和nz_2,

$nz_1, nz_2 \in Z$.则有

$$nz_1 + nz_2 = n(z_1 + z_2) \in nZ,$$

即nZ对+运算是封闭的. 并且$0=n\ 0\in nZ$. 所以,nN是$<Z,+,0>$的子代数. 证毕.

当n=1时,nZ就是V本身,当n=0时,$0Z=\{0\}$是V的最小的子代数,而其他的子代数都是V的非平凡的真子代数.

第五章　代数系统的一般性质

- 二元运算及其性质
- 代数系统及其子代数和积代数
- 代数系统的同态和同构

5.3 代数系统的同态与同构

定义5.15 同态

设$V_1=<S,\circ>$,$V_2=<T,*>$是代数系统,$\circ$和$*$是二元运算,如果存在映射: $\varphi:S\to T$满足对任意的$x,y\in S$有

$$\varphi(x\circ y)=\varphi(x)*\varphi(y),$$

则称φ是V_1到V_2的同态映射,简称同态.

助记: 运算的像等于像的运算

例1: $V_1=<Z,+>$, $V_2=<Z_n,\oplus>$,其中＋为普通加法,$\oplus$为模n加法,即$\forall x,y\in Z_n$有

$$x\oplus y=(x+y)_{\mathrm{mod}\ n},$$

这里$Z_n=\{0,1,\ldots,n-1\}$. 令

$$\varphi:Z\to Z_n,\ \varphi(x)=(x)_{\mathrm{mod}\ n},$$

则φ是V1到V2的同态.

解: 因为对任意$x,y\in Z$有

$$\varphi(x+y)=(x+y)\mathrm{mod}\ n=(x)\mathrm{mod}\ n\oplus(y)\mathrm{mod}\ n$$
$$=\varphi(x)\oplus\varphi(y)$$

例2:

令$\varphi: R \to R^+$, $\varphi(x)=e^x$,那么φ是$\langle R, +\rangle$到$\langle R^+, \cdot\rangle$的同态映射.

解:　　因为 对任意$x,y \in R$,

$$\varphi(x+y)=e^{x+y}=e^x\ e^y=\varphi(x)\ \varphi(y)$$

所以φ是$\langle R, +\rangle$到$\langle R^+, \cdot\rangle$的同态

注意：有一个代数系统到另一个代数系统可能存在多于一个的同态。

同态 同构

定义 满同态 单同态 同构 自同态自同构

设φ是$V_1=<S,\circ>$到$V_2=<T,*>$的同态,如果φ是满射的,则称φ为V_1到V_2的满同态,记作 $V_1 \overset{\varphi}{\sim} V_2$.

如果φ是单射的,则称φ为V_1到V_2的单同态.

如果φ是双射的,则称φ为V_1到V_2的同构,记作 $V_1 \overset{\varphi}{\cong} V_2$.

如果φ为V_1到V_1的同态(或同构),则称φ为V_1的自同态(自同构).

例4

(1)$V=<R,+>$,令 $f:R\to R$, $f(x)=2x$, $\forall x\in R$,

证明f是V到自身的同构。

证明：

(1) 任取$x,y\in R$有

$f(x+y)=2(x+y)=2x+2y=f(x)+f(y)$,

所以f是V到自身的同态,这时也称为V的自同态.

(2) 因为任取$x,y\in R$且$x\neq y$，有$2x\neq 2$，即$f(x)\neq f(y)$,
所以f是单射；

(3) 任取$t\in R$，存在$t/2\in R$，有 $f(t/2)=t$, 所以f是满射；

综合上述3点，所以f是V到自身的同构映射。

例5:

设 f: R->R 定义为对任意的x ∈R

$$f(x)=5^x$$

那么， f是从〈R,+> 到〈R, ·>的一个单同态。

解： 因为对任意的x1,x2∈R 且x1≠ x2

$$f(x1)=5^{x1} \neq 5^{x2} = f(x2)$$

所以f是从〈R,+> 到〈R, ·>的一个单射

又因为

$$f(x+y)=5^{x+y} =5^x \cdot 5^y =f(x) \cdot f(y)$$

所以f是从〈R,+> 到〈R, ·>的一个单同态。

设 A={a,b,c,d},在 A 上定义二元运算如下表所示。又设 B={$\alpha,\beta,\gamma,\delta$},在 B 上定义二元运算如下表所示。证明<A, ★>于<B, *>同构。

★	a	b	c	d
a	a	b	c	d
b	b	a	a	c
c	b	d	d	c
d	a	b	c	d

*	α	β	γ	δ
α	α	β	γ	δ
β	β	α	α	γ
γ	β	δ	δ	γ
δ	α	β	γ	δ

证明：考查映射 f，使得

f(a)= α ; f(b)= β ; f(c)= γ ; f(d)= δ ;

g(a)= δ ; g(b)= γ ;g(c)= β ; g(d)= α ;

小结：

- 两个代数系统同构，它们之间的同构映射可以不唯一。
- 形式上不同的代数系统，如果它们同构，则可抽象地把它们看成是本质上相同的代数系统，所不同的只是使用的符号不同。

定义5.3.2 同态象

设φ是$V_1=<S,*>$到$V_2=<T,\circ>$的同态映射,则称$<\varphi(S),\circ>$是V_1在φ下的**同态象**.

定理5.3.1:

设φ是$V_1=<S,*>$到$V_2=<T,\circ>$的同态映射,那么同态象$\varphi(S)$与$\circ$构成$<T,\circ>$的一个子代数系统.

定理5.3.2:

设f是V_1=<S,*>到V_2=<T,∘>的满同态映射，(*,∘均为二元运算）那么

（1）当运算*满足结合律、交换律时，T也满足结合律、交换律；

（2）如果<S,*>关于*有幺元e,那么f(e)是<T,∘>中关于∘的幺元.

（3）如果x^{-1}是<S,*>中元素关于*的逆元,那么

$f(x^{-1})=(f(x))^{-1}$是<T,∘>中元素f(x)关于∘的逆元.

(4)如果<S,*>关于*有零元θ,那么$f(\theta)$是<T,∘>中关于∘的零元. （作业）

定义5.3.3 同态核

设φ是V_1=<S,*>到V_2=<T,∘>的同态,并且T中有幺元e’,那么称下列集合为同态φ的**核**，记为K(f).

$$K(f)=\{x \mid x \in S且f(x)=e'\}$$

定理5.3.3:

设φ是V1=<S,*>到V2=<T,∘>的同态,如果K(f) ≠∅，那么<K(f),*>为<S, * >的子代数系统.

一般的代数系统的同态

定义5.15的同态概念可以推广到一般的代数系统中去.

设$V_1=\langle S, \circ, * \rangle$, $V_2=\langle T, \circ', *' \rangle$是代数系统, 其中$\circ, *, \circ', *'$都是二元运算. 如果$\varphi: S \to T$满足以下条件:$\forall x,y \in S$有

(1) $\varphi(x \circ y) = \varphi(x) \circ' \varphi(y)$,

(2) $\varphi(x * y) = \varphi(x) *' \varphi(y)$,

则称φ是V_1到V_2的同态映射,简称同态.

例如，

$V_1=\langle Z,+,\cdot\rangle$, $V_2=\langle Z_n,\oplus,\odot\rangle$,其中$+$, $\cdot$为普通的加法和乘法. $\oplus$为模n加法, $\odot$为模n乘法.即对任意$x,y\in Z_n$有

$$x\oplus y=(x+y)_{\mathrm{mod}\ n}$$

$$x\odot y=(xy)_{\mathrm{mod}n}$$

令$\varphi:Z\to Z_n$, $\varphi(x)=(x)_{\mathrm{mod}\ n}$,那么易证

$$\varphi(x+y)=(x+y)_{\mathrm{mod}\ n}=(x)_{\mathrm{mod}\ n}\oplus(y)_{\mathrm{mod}\ n}$$
$$=\varphi(x)\oplus\varphi(y)$$

$$\varphi(x\cdot y)=(xy)_{\mathrm{mod}\ n}=(x)_{\mathrm{mod}\ n}\odot(y)_{\mathrm{mod}\ n}$$
$$=\varphi(x)\odot\varphi(y)$$

所以φ是V_1到V_2的同态,且是满同态.

具有一元运算的代数系统中的同态

设$V_1=<S,\circ,\triangle>$, $V_2=<T,*,\triangle'>$是代数系统,其中$\circ$,$*$是二元运算,$\triangle$和$\triangle'$是一元运算.如果映射

$\varphi: S \to T$满足以下条件

(1)$\forall x,y \in S$,有$\varphi(x\circ y)=\varphi(x)*\varphi(y)$,

(2)$\forall x \in S$,有$\varphi(\triangle(x))=\triangle'(\varphi(x))$,

则称 φ是V_1到V_2的同态.

例如：

$V_1 = \langle R, +, - \rangle$, $V_2 = \langle R^+, \cdot, ^{-1} \rangle$,其中+，·为普通加法和乘法，$-x$表示求$x$的相反数，$x^{-1}$表示求$x$的倒数.

令$\varphi: R \rightarrow R^+$ $\varphi(x) = e^x$,那么有

$\forall x, y \in R$,

$$\varphi(x+y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y),$$

$\forall x \in R$,

$$\varphi(-x) = e^{-x} = (e^x)^{-1} = (\varphi(x))^{-1},$$

所以，φ 是V_1到V_2的同态.

具有代数常数的代数系统之间的同态

设V_1 =< S ,∘,k_1>,V_2=<T,*, k_2 >是代数系统,其中∘,*为二元运算, $k_1 \in S$,$k_2 \in T$是代数常数.如果$\varphi : S \to T$满足以下

条件:

(1)$\forall x,y \in S$,有$\varphi(x \circ y)=\varphi(x)*\varphi(y)$,

(2)$\varphi(k_1)= k_2$,

则称φ是V_1到V_2的同态.

例如：

$V_1 = \langle Z, +, 0 \rangle$， $V_2 = \langle Z_n, \oplus, 0 \rangle$其中＋是普通加法，$\oplus$是模n加法，令

$$\varphi: Z \to Z_n \text{，□ } \varphi(x) = (x)_{\bmod n}\text{，}$$

则有

$$\forall x, y \in Z,\ \varphi(x+y) = (x+y)_{\bmod n}$$

$$= (x)_{\bmod n} \oplus (y)_{\bmod n}$$

$$= \varphi(x) \oplus \varphi(y),$$

$$\varphi(0) = (0)_{\bmod n} = 0,$$

所以φ是V_1到V_2的同态.

设$V_1 = \langle S, \circ, * \rangle$, , $V_2 = \langle T, \circ', *' \rangle$是具有两个二元运算的代数系统, φ 是V_1到V_2的同态,φ具有以下性质:

(1)若$\circ$(或$*$)是可交换的(可结合的或幂等的),则 $\circ'$(或$*'$)在$\varphi(S)$中也是可交换的(可结合的或幂等的).

(2)若$\circ$对$*$是可分配的,则$\circ'$ 对$*'$在$\varphi(S)$中也是可分配的.

(3)若$\circ$和$*$是可吸收的,则$\circ'$和$*'$ 在$\varphi(S)$中也是可吸收的.

(4)若e是S中关于$\circ$运算的幺元,θ是S中关于$\circ$运算的零元,那么$\varphi(e)$和$\varphi(\theta)$分别是$\varphi(S)$中关于$\circ'$运算的幺元和零元. 对于$x\in S$,如果x^{-1}是x的关于$\circ$运算的逆元,则$\varphi(x^{-1})$是$\varphi(x)$关于$\circ'$运算的逆元.

例：代数系统$<\{0,1\},\vee>$是否与代数系统$<N,+>$同态？如果同态，求出同态像和同态核。

解：作映射$f:N\rightarrow\{0,1\}$

另$f(0)=0, f(n)=1$（n不为0）