代数结构

Algebra Structures

内容提要

1. 运算及其性质
2. 代数系统
3. 群与子群
4. 阿贝尔群和循环群
5. 环与域
6. 格与布尔代数

1、运算及其性质

概念：

运算，封闭的，可交换的，可结合的，可分配的，吸收律，幂等的，幺元，零元，逆元，消去律

运算 对于集合 A，f 是从A^n到 A 的函数，称 f 为集合A上的一个n元运算。

注：函数f：$A^n \to B$，若$B \subseteq A$，称函数f在集合A上是封闭的。

运算实例：

(1) 加法和乘法是N上的二元运算，但减法和除法不是.

(2) 加法、减法和乘法都是Z上的二元运算，而除法不是.

(3) 乘法和除法都是R*上的二元运算，而加法和减法不是.

(4) 设M_n(R)表示所有n 阶($n\geq 2$)实矩阵的集合，即

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

则矩阵加法和乘法都是M_n(R)上的二元运算.

(5) S为任意集合，则∪、∩、－、⊕ 为$P(S)$上二元运算.

运算的表示

1. 算符

可以用$\circ$, $*$, $\cdot$, $\oplus$, $\otimes$,Δ 等符号表示二元或一元运算，称为算符.

2. 运算表：表示有穷集上的一元和二元运算

$\circ$	a_1	a_2	…	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	…	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	…	$a_2 \circ a_n$
.		…		
.		…		
.		…		
a_n	$a_n \circ a_1$	$a_n \circ a_2$	…	$a_n \circ a_n$

二元运算的运算表

	$\circ a_i$
a_1	$\circ a_1$
a_2	$\circ a_2$
.	.
.	.
.	.
a_n	$\circ a_n$

一元运算的运算表

运算表的实例

例 设 $S=P(\{a,b\})$，S上的$\oplus$和 $\sim$运算的运算表如下

$\oplus$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\varnothing$	$\{a.b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\varnothing$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\varnothing$

x	$\sim x$
$\varnothing$	$\{a,b\}$
$\{a\}$	$\{a\}$
$\{b\}$	$\{b\}$
$\{a,b\}$	$\varnothing$

运算的性质

交换律 (Commutative)

已知<A，*>，若∀x，y∈A，有x*y=y*x，称*在A上是可交换的。

例:判断相应的运算是否满足交换律。

(1) （Z，+）、（Z，-） （Z，×）

(2) 设<R，*>,*定义如下：a*b=a+b-ab

结合律(Associative)

已知<A，*>，若∀x，y，z∈A，有

x*（y*z）=（x*y）*z，

称*在A上是可结合的。

例:判断相应的运算是否满足结合律。

(1) （Z，+）、（Z，-） （Z，×）

(2) <A，*>，若∀a，b∈A，有a*b=b

幂等律(Idempotent)

已知〈A，*〉，若∀x∈A，x*x=x　　则称满足幂等律 。

例：已知集合s，〈 $\wp$（s），∪，∩〉，则∪，∩满足幂等律。

分配律(Distributive)

设<A，*，△>，若∀x，y，z∈A有：

x*(y△z)=（x*y）△（x*z）　；

(y△z)*x=(y*x)△(z*x)

称运算*对△是可分配的。

*	α	β
α	α	β
β	β	α

△	α	β
α	α	α
β	α	β

例：设A={α，β}，二元运算*，△定义如左：

问分配律成立否？

① 运算△对*是可分配的。

即：$x\triangle(y*z)=(x\triangle y)*(x\triangle z)$成立

证：当$x=\alpha$：　$x\triangle(y*z)=\alpha$

$(x\triangle y)*(x\triangle z)=\alpha$

当$x=\beta$：　$x\triangle(y*z)=y*z$

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

*	α	β
α	α	β
β	β	α

△	α	β
α	α	α
β	α	β

②、运算*对运算△不可分配

证：$\because \beta*(\alpha\triangle\beta)=\beta*\alpha=\beta$

$(\beta*\alpha)\triangle(\beta*\alpha)=\beta\triangle\alpha=\alpha$

吸收律(Absorbtive)

设$*, \Delta$是定义在集合A上的两个可交换二元运算，若对$\forall x, y \in A$, 都有：

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

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

则称运算$*$和Δ满足吸收律.

例：幂集P(S)上的运算$\cup$和$\cap$满足吸收律。

单位元（幺元）(Identity)

设*是A上二元运算， $e_l, e_r, e \in A$

若$\forall x \in A$，有$e_l * x = x$，称e_l为运算*的**左幺元**；

若$\forall x \in A$，有$x * e_r = x$，称e_r为运算*的**右幺元**

若e既是左幺元又是右幺元，称e为运算*的**幺元**

- $\forall x \in A$，有$e * x = x$，$x * e = x$

定理：设*是A上的二元运算，具有左幺元e_l，右幺元e_r，则$e_l=e_r=e$

证明：$e_r = e_l * e_r = e_l$

推论：二元运算的幺元若存在则唯一

证明：反证法：设有二个幺元e，e’；

则e=e*e’=e’

零元 (Zero)

设*是A上二元运算， θ_l， θ_r， $\theta \in A$

若$\forall x \in A$，有$\theta_l * x = \theta_l$ ，称θ_l为运算*的左零元；

若$\forall x \in A$，有$x * \theta_r = \theta_r$，称θ_r为运算*的右零元；

若θ既是左零元又是右零元，称θ为运算*的零元。

- $\forall x \in A$，有$\theta * x = x * \theta = \theta$

例：

a) 〈Z，x〉， Z为整数集

则幺元为1，零元为0

b) 〈$\wp$（A），∪，∩〉

对运算∪， ∅是幺元， A是零元

对运算∩， A是幺元，∅是零元。

c) 〈N，+〉

有幺元0，无零元。

例：代数A=〈{a，b，c，d}，*〉用下表定义：

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

左幺元　无

右幺元　a

左零元　a, b

右零元　无

定理：设*是A上的二元运算，具有左零元θ_l，右零元θ_r，则$\theta_l = \theta_r = \theta$

推论：二元运算的零元若存在则唯一。

逆元 (Inverse)

设*是A上的二元运算，e是运算*的幺元

若x*y=e那对于运算*，x是y的左逆元，y是x的右逆元

若x*y=e，y*x=e，则称x是y的逆元。记为y^{-1}

- 存在逆元(左逆无，右逆元）的元素称为可逆的（左可逆的，右可逆的）

例：

a)、代数 〈N，+〉 仅有幺元0，有逆元0，

b)、A=〈{a，b，c}，*〉由下表定义：

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

b是幺元，

a的右逆元为c，无左逆元，

b的逆元为b，

C无右逆元，左逆元为a

定理：对于可结合运算 o ，如果元素x有 左逆元 l ，右逆元r，则l=r=x^{-1}

证：　$l = l \circ e = l \circ (x \circ r)$

$= (l \circ x) \circ r = e \circ r = r$

∴逆元存在为r

推论：逆元若存在，则唯一

证：　若存在X的另一个逆元r^1；　则：

$r^1 = r^1 \circ e = r^1 \circ (x \circ r)$

$= (r^1 \circ x) \circ r = e \circ r = r$

消去律 (Cancellation Law)

已知<A，*>，若∀x，y，z∈A，有

(1) 若 x*y = x*z且 x ≠θ,则y=z；

(2) 若 y*x = z*x且 x ≠θ,则y=z；

那么称*满足消去律。

例: **(1) 整数集上的加法和乘法都满足消去律；**

(2) S ={1,2,3}, P(S)的交、并运算不满足消去律。

2、代数系统及同态

概念：

代数系统，子代数，积代数，同态，同构。

代数系统 设**A**为非空集合，**Ω**为**A**上运算的集合,称**<A,Ω >**为一个代数系统.

- 当$\Omega=\{f_1,\ldots,f_n\}$是有限时,代数系统常记为$<A,f_1,\ldots,f_n>$;
- 当A有限时,称<A,Ω>是有限代数系统。

例：

(1) **<N,＋>,<Z,＋,·>,<R,＋,·>**是代数系统，+和·分别表示普通加法和乘法。

(2) **<*P*(*S*),∪,∩,~>**是代数系统，∪和∩为并和交，~为绝对补。

构成代数系统的成分：

- 集合（也叫载体，规定了参与运算的元素）
- 运算（这里只讨论有限个二元和一元运算）
- 代数常数（通常是与运算相关的特异元素：如单位元等）

例如：代数系统<Z,+,0>：集合Z, 运算+, 代数常数0

代数系统<$P(S)$,∪,∩>：集合$P(S)$, 运算∪和∩，无代数常数

如果两个代数系统中运算的个数相同，对应运算的元数相同，且代数常数的个数也相同，则称它们是同类型的代数系统.

例：

$V_1=<\mathbf{R}, +, \cdot, 0, 1>$

$V_2=<M_n(\mathbf{R}), +, \cdot, \theta, E>$, θ为 n 阶全0矩阵，E为 n 阶单位矩阵

$V_3=<P(B), \cup, \cap, \varnothing, B>$

- V_1, V_2, V_3是同类型的代数系统，它们都含有2个二元运算, 2个代数常数.

设$V=<S, f_1, f_2, \ldots, f_k>$是代数系统，$B$是$S$的非空子集，如果$B$对$f_1, f_2, \ldots, f_k$都是封闭的，且$B$和$S$含有相同的代数常数，则称$<B, f_1, f_2, \ldots, f_k>$是$V$的子代数系统，简称子代数。

注：有时将子代数系统简记为B.

实例

N是<Z,＋>的子代数，N也是<Z,＋,0>的子代数

N–{0}是<Z,＋>的子代数，但不是<Z,＋,0>的子代数

几个术语

(1) 最大的子代数：就是V本身

(2) 最小的子代数：如果令V中所有代数常数构成的集合是B，且B对V中所有的运算都是封闭的，则B就构成了V的最小的子代数

(3) 最大和最小的子代数称为V 的平凡的子代数

(4) 若B是S的真子集，则B构成的子代数称为V的真子代数.

例 设$V=<Z,+,0>$,令 $nZ=\{nz \mid z\in Z\}$,n为自然数，则nZ是V的子代数

当$n=1$和0时，nZ是V的平凡的子代数，其他的都是V的非平凡的真子代数.

设$V_1=<A,\circ>$和$V_2=<B,*>$是同类型的代数系统，$\circ$和$*$为二元运算，在集合$A\times B$上如下定义二元运算$\blacksquare$，

$\forall <a_1,b_1>,<a_2,b_2>\in A\times B$，有

$$<a_1,b_1>\blacksquare<a_2,b_2>=<a_1\circ a_2,\ b_1*b_2>$$

称$V=<A\times B,\blacksquare>$为$V_1$与$V_2$的积代数，记作$V_1\times V_2$. 这时也称$V_1$和$V_2$为$V$的因子代数.

定理 设$V_1=<A,\circ>$和$V_2=<B,*>$是同类型的代数系统，$V_1\times V_2=<A\times B,\blacksquare>$是它们的积代数.

(1) 如果$\circ$和$*$运算是可交换（可结合、幂等）的，那么$\blacksquare$运算也是可交换（可结合、幂等）的

(2) 如果e_1和e_2（θ_1和θ_2）分别为$\circ$和$*$运算的单位元（零元），那么$<e_1,e_2>$（$<\theta_1,\theta_2>$）也是$\blacksquare$运算的单位元（零元）

(3) 如果x和y分别为$\circ$和$*$运算的可逆元素，那么$<x,y>$也是$\blacksquare$运算的可逆元素，其逆元就是$<x^{-1},y^{-1}>$

设V_1=<A,$\circ$>和V_2=<B,$*$>是同类型的代数系统，f:$A\to B$，

对$\forall x, y\in A$ 有 $f(x\circ y) = f(x)*f(y)$,

则称 f 是V_1到V_2的同态映射，简称同态 (Homomorphism) 。

特殊的同态

(1) f 如果是单射，则称为单同态(Monomorphism)。

(2) 如果是满射，则称为满同态 (Epimorphism)，这时称V_2是V_1的同态像， 记作$V_1\sim V_2$。

(3) 如果是双射，则称为同构 (Isomorphism)，也称代数系统V_1同构于V_2， 记作$V_1\cong V_2$ 。

(4) 如果V_1=V_2，则称作自同态(Endomorphism)。

实例

(1) 设V_1=<Z,+>, V_2=<Z_n,⊕>．其中Z为整数集，+为普通加法；Z_n={0,1,…,n–1}，⊕为模n加. 令

$$f: Z \to Z_n,\ f(x)=(x) \bmod n$$

那么 f 是V_1到V_2的满同态.

(2) 设V_1=<R,+>, V_2=<R*,·>，其中R和R*分别为实数集与非零实数集，+ 和 · 分别表示普通加法与乘法．令

$$f: R \to R^*,\ f(x)= e^x$$

则 f 是V_1到V_2的单同态.

(3) 设V=<Z,+>，其中Z为整数集，+为普通加法．$\forall a \in Z$，令

$$f_a: Z \to Z,\ f_a(x)=ax,$$

那么 f_a 是V的自同态；当a=±1时，称 f_a 为自同构；除此之外其他的 f_a 都是单自同态.