第14章 代数系统

1

代数系统

- 代数系统又称为代数结构。简单说，代数系统就是集合与集合上运算的合成体
- 代数系统对于可计算模型研究、抽象数据结构、形式语言理论、程序设计语言语义分析等都有着深远的影响。

2

主要内容

- 二元运算
- 代数系统
- 特异元

3

二元运算

- n元代数运算：设S,G是非空集合，映射f：$S^n \to G$ 称为从S到G的n元代数运算，简称n元运算(n-ary Operation).
  - ✓ 当n = 1时，称为一元运算； Ex. y=f(x)=2x, x∈S,y∈G
  - ✓ 当n = 2时，称为二元运算; Ex. z =f(x,y)= x+y, x,y∈S,z∈G

例：设集合S={*a,b,c,d*}。定义从S到S的一个二元运算“•” 用表表示为：

f(a,a)= a, f(a,b)= a, f(a,c)= a, f(a,d)= a
f(b,a)= a, f(b,b)= b, f(b,c)= c, f(b,d)= d
f(c,a)= a, f(b,b)= c, f(c,c)= b, f(c,d)= d
f(d,a)= a, f(b,b)= d, f(d,c)= c, f(d,d)= b

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

4

二元运算的性质

定义14-1：

- 设“·”是一个从S到G的二元运算，如果

① 对任意的a, b∈S，都有 a·b∈S，即G⊆S, 则称“·”是S上的二元运算, 并称“·”在S上是封闭的;

- 进一步, 设“·”是S上的一个二元运算

② 对任意的a, b∈S，都有a·b = b·a，则称“·”在S上是可交换的，或称满足交换律。

③ 对任意的a, b，c∈S，都有 (a·b)·c = a·(b·c), 则称“·”在S上是可结合的，或称满足结合律。

④ 对任意的a∈S，满足a·a = a，则称“·”是 幂等的，或称满足幂等律。

5

消化二元运算的几个性质： 封闭性，交换性，结合性，幂等性并完成下表

集合	运算	封闭	交换	结合	幂等
自然数集	+ * -				
整数集	+ * -				
正整数集	+ * - /				
实数集	+ * -				
正实数集	+ * - /				
2^A幂集	∪和∩				
命题集合	∧和∨				

6

二元运算的性质

- 定义在自然数集N上的加法和乘法运算:
  - ✓ 满足封闭性、交换律和结合律，但不满足幂等性
- 定义在实数集R上的加法和乘法运算:
  - ✓ 满足封闭性、交换律和结合律；但不满足幂等性
- 定义在2^A幂集上运算∪和∩:
  - ✓ 满足封闭性、交换律、结合律和幂等性
- 定义在命题集合上运算∧和∨
  - ✓ 满足封闭性、交换律、结合率和幂等性

7

二元运算的性质

定义14-2： 设“*”，“·” 是集合S上的两个二元运算，对 ∀a,b,c∈S，

① 若 a·(b*c)=(a·b)*(a·c) 且 (b*c)·a=(b·a)*(c·a)，则称“·”对“*”在S上满足分配律。

- ✓ 乘法对加法在实数集R/整数集Z/自然数集N上满足分配律

② 若“*”、“·”满足交换律，且 a·(a*b)=a 且 a*(a·b)=a，则称运算“*”与“·”满足 吸收律。

- ✓ 在幂集2^A上，∪和∩是相互可分配的，并且满足吸收律
- ✓ 在命题集合上, ∧和∨是相互可分配的，并且满足吸收律

8

二元运算的性质

例：设运算“∨”、“∧”分别是实数集R上的最大值和最小值二元运算，即对任意的a,b∈R，a∨b=max(a,b)，a∧b=min(a,b)，试判断运算“∨”与“∧”是否满足分配律和吸收律。

分配率：需判断 对任意的a,b,c∈R

$a \vee (b \wedge c) \stackrel{?}{=} (a \vee b) \wedge (a \vee c)$

$(b \wedge c) \vee a \stackrel{?}{=} (b \vee a) \wedge (c \vee a)$

$a \wedge (b \vee c) \stackrel{?}{=} (a \wedge b) \vee (a \wedge c)$

$(b \vee c) \wedge a \stackrel{?}{=} (b \wedge a) \vee (c \wedge a)$

6 种情况
a>b>c, a>c>b
b>a>c, b>c>a
c>a>b, c>b>a

吸收率需判断：对任意的a,b∈R

$a \vee (a \wedge b) \stackrel{?}{=} a$； $a \wedge (a \vee b) \stackrel{?}{=} a$

2 种情况
a> b
b>a

二元代数系统

- **定义14-3：设S是一个非空集合，$f_1,f_2,\ldots,f_m$分别是定义在S上的封闭二元运算，称集合S 和 运算$f_1,f_2,\ldots,f_m$所组成的系统为一个二元代数系统，简称代数，记为<S，$f_1, f_2,\ldots,f_m$ >。**
- **判断集合S及某些二元运算是否可组成二元代数系统，关键是判断两点：**
  - **① 集合S 是否 非空；**
  - **② 二元运算关于S 是否 满足封闭性。**

二元代数系统的特异元
--幺元，零元，幂等元

定义14-4：设〈S,*〉是个二元代数系统

1）**若 ∃e ∈ S，使得对 ∀a ∈ S，都有：a*e = e*a = a，**
则称e为 二元代数系统〈S,*〉的单位元或幺元；
✓ **0 为〈R, +〉的单位元；1 为〈R, ×〉的单位元**

2）**若 ∃θ∈S, 使得 对 ∀a∈S, 都有：a*θ = θ*a = θ，**
则称θ为二元代数系统〈S,*〉 的零元；
✓ **0 为〈R, ×〉的零元**

3）**若 ∃a∈S，有a*a = a，则称a是二元代数系统〈S,*〉的幂等元。**
✓ **0，1 为〈R, ×〉的幂等元**
✓ **0 为〈R, - 〉，〈R, + 〉的幂等元**

自学 幺元，零元，幂等元的定义， 并完成下表

代数系统	幺元/单位元	零元	幂等元
< N,+ >			
< Z, * >			
< Z, - >			
< R, + >			
< R-{0}, / >			
< R, - >			
<2^A, ∪>			
<2^A, ∩ >			
<{0,1}, ∨ >			
<{0,1}, ∧ >			

设二元代数系统<A，*>，其中A={a，b，c, d}，二元运算* 结果见下表

问：

1. “*” 满足交换律，结合律，幂等律吗?
2. 幺元是 a ；
3. 零元是 无 ；
4. 幂等元是 a,b,d 。

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

13

二元代数系统的特异元 --逆元

定义14-5： 设〈S,*〉是一个二元代数系统，e是〈S,*〉的幺元，若对 a∈S，∃b∈S，使得：a*b=b*a=e，则称 b是a的逆元，记为$b=a^{-1}$，也称a为可逆元（同样，a也称为b的逆元，记为$a=b^{-1}$，也称b为可逆的）

幺元的逆元是它本身

例：<S={a,b,c,d}, * >的可逆元有_____；

a, b, c, d

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

在一个代数系统中，并不是每个元都是可逆的。

如〈R,*〉的 0

14

请思考

在一个代数系统〈S,*〉中

1. 如果存在幺元，幺元是否唯一
2. 如果存在零元，零元是否唯一?
2. 若存在可逆元，其逆元是否唯一?

15

二元代数系统的特异元

定理14-1 设〈S,*〉是一个二元代数系统：

1）若〈S,*〉存在幺元，则该幺元唯一；

2）若〈S,*〉存在零元，则该零元唯一；

3）若“*”满足结合律且〈S,*〉存在幺元，则对∀a∈S，若a存在逆元，则逆元唯一。

用来判断不满足结合律

证明：（反证法）

1) 设〈S,*〉含有幺元e_1，e_2，根据定义 $e_1 = e_1*e_2=e_2$，因此，幺元唯一。

2) 设S中有两个零元θ_1和θ_2， 由定义有 $\theta_1=\theta_1*\theta_2=\theta_2$，故 零元唯一。

3）设 e是〈S,*〉的幺元，且元素a有两个逆元b_1，b_2，则有

$b_1=b_1*e= b_1*(a*b_2) = (b_1*a)*b_2=e*b_2=b_2$， 因此，逆元唯一。

16

DMS Chapter 14 代数系统

二元代数系统的特异元

定义14-6： 设<S，·>是一个二元代数系统，其幺元为e。对a∈S， 若存在 b∈S，使 b·a=e，则称b是a的**左逆元**；若存在 c∈S，使 a·c=e，则称c是a的**右逆元**。

例： <S={a,b,c,d}, * >中，b的左逆元为 无 ，右逆元为 c ， c的左逆元为 b ，右逆元为 d 。

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

若 "·" 满足结合律，且一个元既有左逆元又有右逆元，则其左右逆元必相等且等于其逆元

也可用来判断不满足结合律

该代数系统满足结合律吗？

DMS Chapter 14 代数系统

总结

1. 代数系统〈S,*〉
   集合S 与 其上运算 * 的 结合体
2. 二元运算的4个性质
   封闭性， 结合律， 交换律， 幂等律
3. 四种特异元
   1. 幺元， 若有，一定唯一
   2. 零元， 若有，一定唯一
   3. 幂等元，
   4. 可逆元，若 "*" 满足结合律， 有唯一逆元

第15章 半群与群

1

主要内容

- 广群、半群、含幺半群及群
- 半群与子半群
- 群与子群
- 元素的周期与循环群
- 交换群（Abel群）
- 同态与同构

2

广群、半群、含幺半群及群

定义14-7:

- ✓ 广群：含一个二元运算的代数系统<S，*>称为广群； （闭）
- ✓ 半群： 若<S，*>为广群，且“*”在S上满足结合率，则称<S，*>为半群； （闭、结）
- ✓ 含幺半群：若<S，*>是半群，且存在幺元 e，则称<S，*>是含幺半群，常记为<S，*，e>； （闭、结、幺）
- ✓ 群：如果<S，*>是含幺半群，且每个元素都有逆元，则称<S，*>为 群。（闭、结、幺、逆）

群⊂含幺半群⊂半群⊂广群

3

广群、半群、含幺半群及群

例： 设k∈Z，令集合$S_k=\{x|(x\in Z)\wedge(x\geq k)\}$， “+”是一个普通的加法运算，试判断<$S_k$，+>是否是一个广群，半群，含幺半裙，群?

1. 判断封闭性
   - ① 若k<0，运算“+”在S_k上不封闭;
   - ② 若k ≥ 0，运算“+”在S_k上是封闭的

   故 k ≥ 0时，<S_k，+>是广群。
2. 判断结合性:

   k ≥ 0时， “+” 在S_k 上满足结合律， 故 k ≥ 0时，<S_k，+>是半群。
3. 判断是否有幺元:

   k =0时，有幺元 e=0，故 k = 0时，<S_k，+>是含幺半群。
4. 判断是否每个元可逆:

   k=0时，除了0，其他元均不可逆 ，故 k = 0时，<S_k，+>不是群。

4

广群、半群、含幺半群及群

- 含 +, × 的广群 (封) 通常为半群（封，结）
  - <R, ×>，<Q, ×>，<N, +> 等;
- 含 -, ÷ 的广群 不是半群
  - ✓ <Q-{0}, ÷>, <Z, ->, <Q, - >等 是广群，但不是半群;

一些典型的(含幺)半群

- <Z,+>,<N,+>,<R,+>, <Q,+>,是含幺半群;
  - ✓ 0是幺元，也是唯一的幂等元，无零元；满足结合律和交换律
- <Z,×>, <N,×>, <R,×>, <Q,×>是含幺半群;
  - ✓ 1是幺元，0是零元，1和0都是幂等元；满足结合律和交换律
- <Z^+,+>,<Q^+,+>, <Z^-,+>,< <Q^-,+>等 是半群，但不是含幺半群;
  - ✓ 无幺元，无幂等元，无零元；满足结合律和交换律
- <Q^+,×>, <Z^+,×>等是含幺半群，
  - ✓ 幺元为1，无零元，1是幂等元；满足结合律和交换律

一些典型的(含幺)半群

设$M_n(R)$为n×n实数矩阵集合，+和·分别是矩阵的加法和乘法运算，则

- <$M_n(R)$, + > 是含幺半群，
  - ✓ 幺元为零矩阵；也是唯一的幂等元；无零元；
  - ✓ 满足结合律和交换律
- <$M_n(R)$, · >是含幺半群，
  - ✓ 幺元为单位矩阵，零元为零矩阵，单位矩阵和零矩阵都是幂等元。
  - ✓ 满足结合律和交换律

一些典型的(含幺)半群

设A为任意集合，则<2^A,∩>和<2^A,∪>都是含幺半群，

- <2^A,∪>的幺元为Φ；零元为A。
- <2^A,∩>的幺元为A；零元为Φ。
- 满足结合律，交换律和幂等律

一些典型的(含幺)半群

例：设A＝{a, b, c, …, z}，由A中有限个元素组成的序列称为A上的字符串，不包含任何字符的字符串称为空串，用ε表示，

令 A^*＝{x | x是A上的字符串}

$A^+=A^*-\varepsilon$

设二元运算“o”为：αoβ为两个字符串的连接，即对任意两个字符串α、β，αoβ为将字符串α写在字符串β的左边而得到的字符串。

问： <A^*,o>, <A^+,o> 是否是含幺半群，若是，求其幺元。

幂运算

- 设<S,*>是一个半群，由于 * 满足结合律，故可定义幂运算，即对∀x∈S，定义：

  $x^1=x$,

  $x^2=x*x$,

  $x^3=x*x^2=x^2*x=x*x*x$,

  ……

  $x^n=x^{n-1}*x=x*x^{n-1}$

- 若进一步，<S,*>是含幺半群，设其单位元为e，可定义：

  $x^0=e$

幂运算

- 定理14-2 设<S，*>是半群，$a\in S$，m和n是正整数，则
  ① $a^m*a^n=a^{m+n}$
  ② $(a^m)^n=a^{mn}$

- 当<S，*>是含幺半群时，上述结论对任意非负整数m和n都成立。
  ① $a^m*a^n=a^{m+n}$
  ② $(a^m)^n=a^{mn}$

幂运算

定理14-3 设<S，*>是半群，如果S是有限集，则<S，*>必有幂等元，即 必有a∈S，满足 $a^2=a$。

注意：如果S不是有限集，则不一定有幂等元。

如： <Z^+, +> 是半群， 但Z^+不是有限集， 没有幂等元

<Z, +> 是半群， 但Z不是有限集， 有幂等元0

含幺半群至少有一个幂等元----幺元

含幺半群至少有一个可逆元-----幺元

(含幺)子半群

定义14-8

①如果<S,*>是半群，T是S的非空子集，且“*”在T上是封闭的，则<T,*>是半群，并称<T,*>是半群<S,*>的子半群；

②如果<S,*,e>是含幺半群，T⊆S，e∈T，且“*”在T上是封闭的，则<T,*>是含幺半群，称<T,*,e>是<S,*,e>的含幺子半群。

例：代数系统 <[0，1]，×>，<Z，×>，<R^+，×>都是<R，×>的子半群。

<[10，20]，×> 不是半群，故不是<R，×>的子半群，

(含幺)子半群

例 设<S，*>是一个可交换的含幺半群，M是它的所有的等幂元构成的集合，则<M，*>是<S，*>的一个含幺子半群。

证明：

(1) 子集： 显然，M⊆S；

(2) <M，*> 封闭： 设任意 a，b∈M，

a*b = (a*a)*(b*b) = a*a*b*b

= (a*b)*(a*b)

所以 a*b∈M，即运算“*”关于集合M是封闭的。

(3) M含幺： <S，*>是含幺半群，所以幺元e是等幂元，即有 e∈M；

由(1)、(2)、(3)知： <M，*>是<S，*>的一个含幺子半群。

群

如果<G，*>是含幺半群，且每个元素都是可逆元，则称<G，*>为 群。（闭、结、幺、逆），|G|称为群的阶

- <Z,+> 是含幺半群； 因每个整数*a* 都有逆元 –*a*，故<Z,+>是群，通常称为整数加群
- <R,+>： 实数加群
- <Q,+>： 有理数加群；
- <R-{0}, ×>是实数乘群；

为什么要去掉0？

Your turn

1. 已知代数系统<A,$>是群，定义二元运算 # 为：

x#y = xay， a ∈A

1） 试判断运算 # 在A上是否 满足封闭性，结合律，是否有幺元（若有，请表达出来），是否每元可逆（若可逆，写出逆元的表达式）

2） <A, # >是否为群？

群

例： 设 S={1，3，4，5，9}， 在S上定义运算#， $ 为：

模11乘 运算

∀x，y∈S， x#y = ((x%11) * (y%11))%11 = （x*y）%11

∀x，y∈S， x$y = ((x%11) + (y%11))%11 = （x+y）%11

模11加 运算

这里 +, * 为普通加和普通乘， %为求模运算

问： <S, #>， <S, $> 是否为群?

S = {1,2,3,5,10} 呢?

S = {0,1,2,3,4, 5,6,7,8,9,10}呢?

典型群—剩余类加群

➢ 剩余类加群

设Z_k表示整数集Z上的模k剩余类（模k同余等价类）集合，即

Z_k={[0]，[1]，[2]，…，[k-1]}

在Z_k上定义运算⊕和⊗如下：

[i]⊕[j]=[(i+j)%k]， i,j ∈{0,1,..,k-1}

[i]⊗[j]=[(ij)%k]

则<Z_k，⊕>是群，常被称为剩余类加群。[0]是⊕的幺元， 每元[i]的逆元是[k-i]。

剩余类乘半群

<Z_k，⊗>只是含幺半群，[1]是它的幺元，但不是群，因[0]无逆元，

已有证明：当k是素数时，<Z_k-{[0]}，⊗>是群。

典型群—剩余类加群

➢<Z_k-{[0]}，⊗>是不是群呢? 不一定!

➢如， Z_4-{[0]}={[1]，[2]，[3]}，

[2]⊗[2]=[0] ∉ Z_4-{[0]}， 不封闭

∴ <Z_4-{[0]}，⊗> 不是群。

➢又如，Z_5-{[0]}={[1]，[2]，[3]，[4]}

其运算表如右图，

运算是封闭的，可结合的;

[1]是幺元，[1]、[4]的逆元是自身，[2]和[3]互为逆元;

因此<Z_5-{[0]}，⊗>是群。

⊗	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

典型群—n次对称群

➢ n次对称群/ n阶置换群

设基数为n的集合A上的全体置换构成集合S_n， “∘” 是复合运算，则<S_n，∘> 是群，常称为n次对称群/ n阶置换群

证明：

1）封闭： S_n中两个置换的复合仍然是A上的一个置换，所以运算是封闭的;

2）结合律：由于函数的复合是可结合的，所以置换的复合也是可结合的;

3）含幺： S_n中存在幺置换(单位置换) e = （1），使对 ∀σ∈S_n，e∘σ=σ∘e=σ ， 所以e = （1）是幺元;

4）每元可逆：每个置换σ都有逆σ^{-1}。$\sigma\circ\sigma^{-1}=\sigma^{-1}\circ\sigma=(1)$

群的性质

① 若<G，*>是群，则运算 * 满足消去律；

➢ 即 a*b = a*c ⇔ b=c； b*a = c*a ⇔ b=c

② 群的运算表中同一行(列)没有相同的值；

③ 群<G，*>中除幺元 e 外无其它幂等元；

反证法：设a≠e，a*a = a

a*a = a ⇒ a*a = a*e ⇒ a = e， 与假定a≠e矛盾

④ 阶大于1的群<G，*>没有零元； （用反证法）

证：假设有零元 z，任取 $a \neq b$， 则有 $a*z = b*z = z \Rightarrow a = b$，与 $a \neq b$ 矛盾

⑤ <G，*>中的任意两个元素a, b，都有 $(a*b)^{-1} = b^{-1}*a^{-1}$。

证：$(a*b)*(a*b)^{-1}=e \Rightarrow a^{-1} * (a*b)*(a*b)^{-1}=a^{-1} \Rightarrow b^{-1}*b*(a*b)^{-1}=b^{-1}*a^{-1}$

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

子群

➢ 定义15.1 设<G，*>是一个群，S是G的一个非空子集，若<S，*> 也是群，则称<S，*>是<G，*>的一个子群。

➢ 对任意的群<G，*>，都有两个子群

① 幺元子群<{e}，*>

② 群自身<G，*>，

平凡子群

➢ 若<S,*>是<G，*>的子群，且非平凡子群，则称<S，*>为<G，*>的真子群。

子群

➢ 定理15-3 设 <S,*>是 群<G,*>的子群，则：

(1) 子群<S，*>的幺元 e_S 与群<G，*>的幺元e_G相同；

(2) 对∀a∈S，a在S中的逆元a_S^{-1}就是a在G中的逆元a_G^{-1}。

定理15-4 设<G，*>是一个群，S是G的一个非空子集，则<S，*> 是<G，*>的子群的充要条件是：

对∀a，b∈S，有$a*b^{-1}$∈S

Your turn

1 设 <G, *>是群，其中 G={0,1,2,3,4,5, … , 999} “*” 为 模1000加 运算，H = {0，2，4, 6, …，996,998]}，

试证明<H，*> 是 <G，* > 的子群。

2. 已知 <G，*>是群， $<S_1, *>$，$<S_2, *>$ 均为<G，*>的子群， $S=S_1 \cap S_2$， 试证明<S，*> 是 <G，*>的子群。