代数系统

由集合上定义若干个运算而组成的系统我们通常称它为代数系统。它在计算机科学中有着广泛的应用。

第五章 代数结构

- 代数结构是一类特殊的数学结构，它由集合上定义若干个运算而组成系统。本章主要讲授运算的性质及一些具有特殊性质的代数系统。
- 重点是群、同态与同构。要求能够掌握各种代数系统的特性，能够证明一个代数系统是群，并能够证明两个代数系统是同态或同构的。

学习《代数结构》这一章的要求

一、学习目的与要求

本章从一般代数系统的引入出发，研究一些特殊的代数系统中运算的性质。通过本章的学习使学生了界代数系统的结构与性质。

二、知识点

1．代数系统的引入，运算的性质：封闭性、结合性、分配性、交换性；

2．主要的代数系统：广群、半群、独异点、群、子群；代数系统之间的关系；

3．交换群和循环群；

4．陪集、拉格朗日定理；

5．同态映射、同构映射；

6．环、同态象、域。

三、要求

1．识记

运算的封闭性、交换性、结合性，幺元、零元、逆元、等幂元的识别。

2．领会

广群、半群、独异点、群、子群；代数系统之间的关系，主要的性质定理及其证明。

学时分配

学时	内　　容
2	5-1 代数系统的引入 5-2 运算及其性质
2	5-3 半群
2	5-4 群和子群
2	5-5 阿贝尔群和循环群
2	5-6 置换群与伯恩赛德定理
2	5-7 陪集与拉格朗日定理
4	5-8 同态与同构
2	5-9 环与域

本章将从一般代数系统的引入出发，研究一些特殊的代数系统，而这些代数系统中的运算具有某些性质，从而确定了这些代数系统的数学结构。

5-1 代数系统的引入

一、集合上的运算及封闭性

一元运算：

$$f_1: a \to \frac{1}{a}, a \in R, a \neq 0$$

$$f_2: x \to [x], x \in R$$

$$f_3: a \to -a, a \in R$$

以上运算都是集合R上的一元运算。

将R上的每两个数映射成R中的一个数。

二元运算：$f_4: a,b \to a+b, \quad a,b \in R$

可看作：$f_4: R^2 \to R$

$$f_5: a,b \to a \cdot b, \quad a,b \in R$$

三元运算：f_6：三种颜色→三种颜色混合色

A→A A是各种颜色的集合。

这些例子的共同特征就是运算结果还在原来的集合中。称具有这种特征的运算是封闭的，简称闭运算。

很容易举出不封闭运算的例子：一架自动售货机，能接受一角硬币和二角伍分硬币，而所对应的商品是桔子水(瓶)、可口可乐(瓶)和冰淇淋(杯)。当人们投入上述硬币的任何两枚时，自动售货机将按表5-1.1所示的供应相应的商品。

表格左上角的记号 * 可以理解为一个二元运算的运算符。这个例子中的二元运算 * 就是集合{一角硬币，二角伍分硬币}上的不封闭运算。

表 5-1.1

*	一角硬币	二角伍分硬币
一角硬币	桔子水	可口可乐
二角伍分硬币	可口可乐	冰淇淋

运算结果不在集合
{一角硬币，二角伍分硬币}中

设A={红色，黄色，蓝色}

f_7：三种颜色→三种颜色混合色

f_7是不封闭的。

f_8是I上的除法运算，f_8是不封闭的。

定义5-1.1 如果 * 为A^n到B的一个函数，则称 * 为集合A上的n元运算（*operater*）。如果 $B \subseteq A$，则称 该n元运算在A上封闭。

二、代数系统

定义5-1.2 一个非空集合**A**连同若干个定义在该集合上的运算 $f_1,f_2,\cdots,f_k$ 所组成的系统称为一个代数系统（代数结构），记为$<A, f_1,f_2,\cdots,f_k>$。

定义5-1.2‘ 代数结构是由以下三个部分组成的数学结构：

（1）非空集合S，称为代数结构的载体。

（2）载体S上的若干运算。

（3）一组刻划载体上各运算所满足性质的公理。

代数结构常用一个多元序组<S，*，Δ，…>来表示，其中S是载体,*,Δ，…为各种运算。有时为了强调S有某些元素地位特殊,也可将它们列入这种多元序组的末尾。

如正整数集合 I_+ 以及在该集合上的普通加法运算“+”组成一个代数系统 $\langle I_+, + \rangle$。又如，一个有限集 S，由 S 的幂集 $\mathscr{P}(S)$ 以及在该幂集上的集合运算“$\cup$”、“$\cap$”、“$\sim$”组成一个代数系统 $\langle \mathscr{P}(S), \cup, \cap, \sim \rangle$。虽然，有些代数系统具有不同的形式，但是，它们之间可能有一些共同的运算规律。

例如，考察代数系统$\langle I, +\rangle$，这里I是整数集合，$+$是普通的加法运算。很明显，在这个代数系统中，关于加法运算，具有以下三个运算规律，即对于任意的$x, y, z \in I$，有

(1) $x+y \in I$　　(封闭性)

(2) $x+y=y+x$　　(交换律)

(3) $(x+y)+z=x+(y+z)$　　(结合律)

容易找到与$\langle I, +\rangle$具有相同运算规律的一些代数系统，如表5-1.2所示。

表　5-1.2

	$\langle I, \cdot\rangle$	$\langle R, +\rangle$	$\langle \mathscr{P}(S), \cup\rangle$	$\langle \mathscr{P}(S), \cap\rangle$
集合	I 为整数集合	R 为实数集合	$\mathscr{P}(S)$是S的幂集	$\mathscr{P}(S)$是S的幂集
运算	$\cdot$ 为普通乘法	$+$为普通加法	$\cup$ 为集合的"并"	$\cap$ 为集合的"交"
封闭性	$x \cdot y \in I$	$x+y \in R$	$A \cup B \in \mathscr{P}(S)$	$A \cap B \in \mathscr{P}(S)$
交换律	$x \cdot y = y \cdot x$	$x+y=y+x$	$A \cup B = B \cup A$	$A \cap B = B \cap A$
结合律	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	$(x+y)+z = x+(y+z)$	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$

虽然集合不同，运算不同，但是它们是一些具有共同运算规律的运算，研究 $<I，+>$就相当于研究$<I，*>$，$<R，+>$，$<\wp(S)，\cup>$，$<\wp(S)，\cap>$

5-2 运算及其性质

在前面考察几个具体的代数系统时，已经涉及到我们所熟知的运算的某些性质。下面，着重讨论一般二元运算的一些性质。

一、封闭性

定义5-2.1

设*是定义在集合A上的二元运算，如果对于任意的$x,y\in A$，都有$x*y\in A$，则称二元运算*在A上是封闭的。

例题1 设$A=\{x|x=2^n,n\in N\}$,问乘法运算是否封闭？对加法运算呢？

解 对于任意的$2^r,2^s\in A$，r，$s\in N$，因为$2^r\cdot 2^s=2^{r+s}\in A$所以乘法运算是封闭的。而对于加法运算是不封闭的，因为至少有$2+2^2=6\notin A$

二、可交换性

定义5-2.2

设*是定义在集合A上的二元运算，如果对于任意的x,y∈A，都有x*y=y*x，则称二元运算*在A上是可交换的。

例题2 设Q是有理数集合，Δ是Q上的二元运算，对任意的a,b∈R，a Δ b=a+b-a·b，问运算Δ是否可交换。

解 因为

a Δ b=a+b-a·b=b+a-b·a=b Δ a

所以运算Δ 是可交换的。

三、可结合性

定义5-2.3

设*是定义在集合A上的二元运算，如果对于任意的$x, y, z \in A$，都有$(x*y)*z=x*(y*z)$，则称二元运算*在A上是可结合的。

例如**R**上的加法运算和乘法运算都是可结合运算，**R**上的减法运算和除法运算都是不可结合运算

例题3 设A是一个非空集合，★是A上的二元运算，对于任意$a,b \in A$,有$a★b=b$，证明★是可结合运算。

证明 因为对于任意的$a,b,c \in A$

$(a★b)★c=b★c=c$

而 $a★(b★c)=a★c=c$

所以$(a★b)★c=a★(b★c)$

四、可分配性

定义5-2.4　设*，Δ是定义在集合A上的二元运算，如果对于任意的x, y, z∈A，都有

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

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

则称运算*在A上对运算Δ是可分配的。

例题4　设集合 $A=\{\alpha,\beta\}$，在 A 上定义两个二元运算 $*$ 和 Δ 如表5-2.1所示。运算 Δ 对于运算 $*$ 可分配吗？运算 $*$ 对于运算 Δ 呢？

表　5-2.1

*	α	β
α	α	β
β	β	α

Δ	α	β
α	α	α
β	α	β

解　容易验证运算 Δ 对于运算 $*$ 是可分配的。但是运算 $*$ 对于运算 Δ 是不可分配的，因为

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

而

$$(\beta*\alpha)\Delta(\beta*\beta)=\beta\Delta\alpha=\alpha.$$

验证运算△对于运算*是可分配的。

从*和△的运算表中可以看出*和△两种运算都是可交换的。

故只须验证 $\alpha\triangle(\alpha*\alpha)=(\alpha\triangle\alpha)*(\alpha\triangle\alpha)$

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

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

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

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

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

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

五、吸收律

定义5-2.5　设*，Δ是定义在集合A上的两个可交换二元运算，如果对于任意的$x,y\in A$，都有

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

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

则称运算*和运算Δ满足吸收律。

例题5 设集合N为自然数全体，在N上定义两个二元运算*和★，对于任意$x,y\in N$，有

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

$$x★y=\min(x,y)$$

验证运算*和★的吸收律。

解 对于任意$a,b\in N$

$$a*(a★b)=\max(a,\min(a,b))=a$$

$$a★(a*b)=\min(a,\max(a,b))=a$$

因此，*和★满足吸收律。

六、等幂律

定义5-2.6

设*是定义在集合A上的一个二元运算，如果对于任意的$x \in A$，都有$x*x=x$，则称二元运算*在A上是等幂的。

例题6 设$\wp(S)$是集合S的幂集，在$\wp(S)$上定义的两个二元运算，集合的“并”运算$\cup$和集合的“交”运算$\cap$，验证是$\cup$、$\cap$等幂的。

解

对于任意的$A \in \wp(S)$，有$A \cup A=A$和$A \cap A=A$，因此运算$\cup$和$\cap$都满足等幂律。

小结 运算及其性质

定义5-2.1~6 设*和Δ为集合A上的二元运算：

若$\forall x\forall y(x,y\in A\rightarrow x*y\in A)$，

则称*在A上封闭。

若$\forall x\forall y(x,y\in A\rightarrow x*y= y*x)$，

则称*满足交换律。

若$\forall x\forall y\forall z(x,y,z\in A\rightarrow x*(y*z)=(x*y)*z)$，

则称 * 满足结合律。

若$\forall x\forall y\forall z(x,y,z\in A\rightarrow x*(y\Delta z)=(x*y)\Delta(x*z))$，

则称*对Δ满足分配律。

若$\forall x\forall y(x,y\in A\rightarrow x*(x\Delta y)=x, x\Delta(x*y)=x)$，

则称*和Δ满足吸收律。

若$\forall x(x\in A\rightarrow x*x=x)$，

则称*满足等幂律。

七、幺元

定义5-2.7 设*为集合A上的二元运算：

若 $\exists e_l \forall x(e_l,x \in A \rightarrow e_l * x = x)$,则称e_l为A中的左幺元。

若 $\exists e_r \forall x(e_r,x \in A \rightarrow x * e_r = x)$,则称e_r为A中的右幺元。

若 $\exists e \forall x(e,x \in A \rightarrow e * x = x * e = x)$,则称e为A中的幺元。

见P-180页例题7。

例题**7** 设集合**S=**{α，β，γ，δ}，在**S**上定义的两个二元运算*和★ 如表**5-2.2**所示。试指出左幺元或右幺元。

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

★	α	β	γ
		δ	
α	α	β	δ	γ
β	β	α	γ	δ
γ	γ	δ	α	β
δ	δ	δ	β	γ

解 由表**5-2.2**可知β，δ 都是S中关于运算*的左幺元，而α是S中关于运算★的右幺元。

定理5-2.1 代数结构<A，*>有关于 * 运算的幺元e，当且仅当它同时有关于 * 运算的左幺元e_l和右幺元e_r。并且其所含幺元是唯一的,即$e_l = e_r = e$ 。

证明：先证左幺元e_l=右幺元e_r=e

$$e_l = e_l * e_r = e_r = e$$

再证幺元e是唯一的

设还有一个幺元e’ ∈A,则

$$e' = e' * e = e$$

八、零元

定义5-2.8 如果 $\theta_l \in A$，满足:对一切$x \in A$，都有

$$\theta_l * x = \theta_l$$

则称元素θ_l 为左零元。

如果$\theta_r \in A$，满足:对一切$x \in A$，都有

$$x * \theta_r = \theta_r$$

则称元素θ_r 为右零元。

如果$\theta \in A$且对任意$x \in A$，都有

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

则称元素θ为代数结构$<A, *>$ (关于 * 运算) 的零元 (*zero*)。

例题8 表5-2.3定义的二元运算

例题**8** 设集合**S={**浅色，深色**}**，定义在**S**上的一个二元运算*

如表**5-2.3**所示。试指出零元和幺元。

*	浅色	深色
浅色	浅色	深色
深色	深色	深色

表5-2.3

解

深色是**S**中关于运算*的零元，浅色是**S**中关于运算*的幺元。

定理5-2.2 代数结构<A，*>有关于 * 运算的零元θ，当且仅当它同时有关于 * 运算的左零元θ_l和右零元θ_r。并且其所含零元是唯一的,即$\theta_l=\theta_r=\theta$。

□ 证明：先证左零元θ_l=右零元θ_r=θ

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

再证零元θ是唯一的

设还有一个幺元 θ’ ∈A,则

$$\theta' =\theta' * \theta = \theta$$ □

定理5-2.3 如果代数结构<A，*>有关于 * 运算的零元θ 和幺元e，且集合A中元素个数大于2，则θ≠e 。

□ 证明：用反证法：

反设幺元e =零元θ ，则对于任意x∈A，必有

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

于是，推出A中所有元素都是相同的，矛盾。

□

九、逆元

定义5-2.9 设代数结构<A，*，e>中* 为二元运算，e为么元，a,b 为A中元素,若b*a＝e，那么称b为a的左逆元，a为b的右逆元。若a*b＝b*a＝e，那么称a(b)为b(a)的逆元（*inverse elements*）。

x的逆元通常记为x^{-1};但当运算被称为“加法运算”（记为+）时，x的逆元可记为-x 。

一般地，一个元素的**左逆元**不一定等于它的**右逆元**。一个元素可以有**左逆元**不一定有**右逆元**。甚至一个元素的**左（右）逆元**不一定是唯一的。

P-182页例题9 ：先找出幺元，再根据幺元所在的行和列找出左、右逆元。

例题**9** 设集合**S={**α，β，γ，δ，ζ **},**定义在**S**上的一个二元运算*如表**5-2.4**所示。

试指出代数系统**<S,*>**中各个元素的左、右逆元情况。

表 5-2.4

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

解 α是幺元；β的左逆元和右逆元都是γ；即β和γ互为逆元；δ的左逆元是γ而右逆元是β；β有两个左逆元γ和δ；ζ的右逆元是γ，但ζ没有左逆元。

定理5-2.4 设<A, *>有么元e，且运算 * 满足结合律,那么当A中元素x有左逆元*l*及右逆元r时,l = r,它们就是x的逆元。并且每个元素的逆元都是唯一的。

□ 证明：先证左逆元=右逆元

设a,b,c，且b是a的左逆元， c是b的左逆元。

因为： （b*a）*b =e *b = b

所以： e=c*b = c * (（b*a）*b)

= (c *（b*a）) *b

= (（c *b ）*a) *b

= (（e ）*a) *b =a*b (b也是a的右逆元)

再证逆元是唯一的

设a有两个逆元b_1和b_2，则有

$$b_1 = b_1 * e = b_1 * (a * b_2)$$

$$= (b_1 * a) * b_2$$

$$= e * b_2 = b_2$$ □

例题**10** 试构造一个代数系统，使得其中只有一个元素具有逆元。

解

设$m,n\in I,T=\{x|x\in I,m\leqslant x\leqslant n\}$,那么，代数系统$<T,max>$中有一个幺元是**m**,且只有**m**有逆元，因为$m=max(m,m)$。

例题**11** 对于代数系统$<R,\cdot>$，这里**R**是实数的全体，是普通的乘法运算，是否每个元素都有逆元。

解

该代数系统中的幺元是**1**，除了零元素**0**外，所有的元素都有逆元。

例题12 对于代数系统$<N_k,+_k>$，这里$N_k=\{0,1,2,\ldots,k-1\}$，$+_k$是定义在N_k上的模k加法运算，定义如下：

对于任意$x,y\in N_k$

$$x+_k y=\begin{cases} x+y & \text{若 } x+y<k \\ x+y-k & \text{若 } x+y\geq k \end{cases}$$

试问是否每个元素都有逆元。

解

可以验证，$+_k$是一个可结合的二元运算，N_k中关于运算$+_k$的幺元是**0**，N_k中的每一个元素都有唯一的逆元，即**0**的逆元是**0**，每个非零元素**x**的逆元是**k-x**。

十、从运算表中看运算具有的性质

1）运算*具有封闭性，当且仅当运算表中的每个元素都属于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的每一元素与它所在行（列）的表头元素相同。

4）A中关于运算*具有零元，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中关于运算*具有幺元，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中关于运算*具有幺元，a和b互逆，当且仅　当位于a所在行和b所在列的元素及b所在行和a 所在列的元素都是幺元。