离散数学第四部分之一

代 数 系 统

由于数学和其他科学的发展，人们需要对若干不是数的事物，用类似普通计算的方法进行相似的计算。如矩阵、向量等。

研究代数系统的学科称为“近世代数”或“抽象代数”。

■ 代数运算

称自然数集合N上的加法“+”为运算，这是因为给定两个自然数a, b， 由加法“+”，可以得到唯一的自然数c = a + b。

加法“+”是函数吗？

N上的加法运算“+”本质上是一个N×N→N的函数

定义1：设A, B, C是非空集合，从A×B到C的一个函数f：A×B→C称为一个A×B到C的二元代数运算，简称二元运算。

代数运算

一个二元运算就是一个特殊的函数 ，该函数能够对 $a \in A$和$b \in B$进行运算，得到C中的一个元c ， 即 $o(a, b)=c$ 。

中缀方法表示为

$$a \circ b = c$$

例

判别下面的函数或表是否是二元运算：

（1）设A = {0, 1}， B = {1, 2}， C = {奇, 偶}，定义函数*：A×B→C，其中

* (0, 1) = 奇， * (0, 2) = 偶，

* (1, 1) = 偶， * (1, 2) = 奇。

分析 “*”是一个A×B到C的函数，因此，按定义，则“*”是一个A×B到C的运算。

运算表

- 当集合A和B有限时，一个A×B到C的代数运算，可以借用一个表，称为运算表（乘法表）来说明。
- 设“*”是A×B→C的运算，$A = \{a_1, a_2, \ldots, a_n\}$，$B = \{b_1, b_2, \ldots, b_m\}$，则运算“*”可用下表说明。

运算表

*	b_1	b_2	…	b_m
a_1	$a_1 * b_1$	$a_1 * b_2$	…	$a_1 * b_m$
a_2	$a_2 * b_1$	$a_2 * b_2$	…	$a_2 * b_m$
…	…	…	…	…
a_n	$a_n * b_1$	$a_n * b_2$	…	$a_n * b_m$

定义 2

设A_1, A_2, …, A_n, A是非空集合，$A_1 \times A_2 \times \ldots \times A_n$到A的一个函数(或函数)* ： $A_1 \times A_2 \times \ldots \times A_n \rightarrow A$ 称为一个$A_1 \times A_2 \times \ldots \times A_n$到A的n元代数运算，简称n元运算。当n = 1时，称为一元运算。

1元代数运算表

当元素有限时，一元运算也可以用运算表来说明。

设“*”是A到A的一元运算，其中 $A = \{a_1, a_2, \ldots, a_n\}$，则一元运算“*”可以用右表说明。

1元运算表

a	* (a)
a_1	* (a_1)
a_2	* (a_2)
…	…
a_n	* (a_n)

代数运算的特点：封闭性

定义3 如果“*”是A×A到A的二元运算，则称运算“*”对集合A是封闭的，或者称“*”是A上的二元运算。

定义 4：设“*”是一个$A_1 \times A_2 \times \ldots \times A_n$到A的n元代数运算，如果$A_1 = A_2 = \ldots = A_n = A$，则称代数运算“*”对集合A是封闭的，或者称“*”是A上的n元代数运算。

说　明

一般通常用大写的英文字母表示集合，用符号“+”、“-”、“*”、“/”、“∩”、“∪”、“∧”、“∨”、“┐”、“★”、“☆”、“o”、“⊕”、“+”、“×”、“÷”等抽象的符号来表示一个抽象的运算。

定义5

设A是非空集合，$*_1, *_2, \ldots, *_m$分别是定义在A上$k_1, k_2, \ldots, k_m$元封闭运算，k_i是正整数，$i = 1, 2, \ldots, m$。称集合A和$*_1, *_2, \ldots, *_m$所组成的系统称为代数系统，简称代数，记为$<A, *_1, *_2, \ldots, *_m>$。

当A是有限集合时，该代数系统称为有限代数系统，否则称为无限代数系统。

注意：判断集合A和其上的代数运算是否是代数系统，关键是判断两点：一是集合A非空，二是这些运算关于A是否满足封闭性。

例子

(1) R上的“+”、“×”运算；

解：构成一个代数系统〈R，+，×〉；

(2) P(S)上的“∩”、“∪”、“—”运算；

解：构成代数系统〈P(S),∩,∪,—〉，称集合代数；

(3) 含有n个命题变元的命题集合A与A上的“∧”、“∨”、“┐”运算；

解：构成代数系统〈A，∧，∨，┐〉，称之为命题代数。

同类型代数系统

定义 6 设<A, $*_1$, $*_2$, …, $*_m$ >和<B, o_1, o_2,…, o_m >是两个代数系统，若“o_i”和“$*_i$”都是k_i元运算，i = 1, 2, …, m，则称这两个代数同类型。

如：代数系统〈Z，+〉，〈Z，×〉，〈R，+〉，〈P(S)，∩〉，〈P(S)，∪〉都是同类型的代数系统。

代数系统〈Z，+，×〉、〈R，+，×〉、〈P(S)，∩，∪〉都是同类型的代数系统。

子代数

定义7 设$<A, *_1, *_2, \ldots, *_m>$是代数系统，如果：

（1）$B \subseteq A$并且$B \neq \varnothing$；

（2）$*_1, *_2, \ldots, *_m$都是B上的封闭运算。

则$<B, *_1, *_2, \ldots, *_m>$也是一个代数系统，称之为$<A, *_1, *_2, \ldots, *_m>$的子代数系统，简称子代数。又若$B \subset A$，则称$<B, *_1, *_2, \ldots, *_m>$是$<A, *_1, *_2, \ldots, *_m>$的真子代数。

子代数

子代数是抽象代数学中一个非常重要的概念，通过研究子代数的结构和性质，可以得到原代数系统的某些重要性质。如在群论中，通过研究子群可得群的某些性质。

注意：在后面章节中，将会学习半群、群、格、布尔代数等典型的代数系统。将子代数的概念应用到这些典型的代数系统，就会得到子半群、子群、子格、子布尔代数。因此，若没有比要，后面不再赘述某些典型代数系统中子代数的定义。

例4

在代数系统<Z, +>中，令

$$Q = \{5z \mid z \in Z\},$$

证明<Q, +>是<Z, +>的子代数。

分析 根据定义，只需证明两点：

（1）Q是非空子集；（2） “+”对集合Q封闭。

显然，集合Q非空。对任意$5z_1$，$5z_2 \in Q$，有

$$5z_1 + 5z_2 = 5(z_1 + z_2) \in Q,$$

因此“+”对集合Q封闭。

证明 略。

■ 二元运算律

例　设“+”是定义在自然数集合N上的普通加法运算，试回忆N上的加法运算“+”满足哪些运算性质？

分析　对任意 a, b, c∈N，有

(a + b) + c = a + (b + c)，即结合律成立；

a + b = b + a，即交换律成立；

对任意 x, y∈N，如果a + x = a + y，则x = y，即消去律成立；

0∈N，0 + 0 = 0，即0是幂等元，但其他自然数不是幂等元，即不满足幂等律。

结合律与交换律

定义 设<A, *>是二元代数系统，如果对任意a, b, c∈A，都有

$$(a*b)*c = a*(b*c)$$

则称“*”在A上是可结合的，或称满足结合律。

定义 设<A, *>是二元代数系统，如果对任意a, b∈A，都有

$$a*b = b*a$$

则称“*”在A上是可交换的，或称“*”满足交换律。

消去律

定义 设<A, *>是二元代数系统，元素a∈A，

（1）对任意x, y∈A，都有

如果a * x = a * y，那么x = y，

则称a在A中关于“*”是左可消去元；

（2）对任意x, y∈A，都有

如果x * a = y * a，那么x = y，

则称a在A中关于“*”是右可消去元；

消去律（续）

（3）如果a既是A左可消去元又是右可消去元，则称a是A的可消去元；

（4）若A中所有元素都是可消去元，则称“*”在A上可消去，或称“*”满足消去律。

幂等律

定义 设<A, *>是二元代数系统，若元素a∈A，满足

$$a*a = a,$$

则称a是A中关于“*”的一个幂等元，简称a为幂等元。若A中的每一个元素都是幂等元，则称“*”在A中是幂等的，或称“*”满足幂等律。

幂

设“*”是集合A上可结合的二元运算，a∈A，则a*a∈A，a*a*a∈A，…，由此，可以归纳定义a的正整数幂方：

$a^1 = a$，$a^2 = a*a$，$a^3 = a^2*a$，…，

$a^n = a^{n-1}*a$，…

对任意正整数n，m，有以下等式：

$a^n * a^m = a^{n+m}$，　　$(a^n)^m = a^{nm}$。

分配律

定义：设“*”、“o”是集合A上的二元运算，<A，*，o >是一个代数系统， 对任意a,b,c∈S，有

（1）ao(b*c)=(aob)*(aoc)，

则称运算“o”对“*”在S上满足左分配律(或第一分配律)；

（2) (b*c) oa=(boa)*(coa)，

则称运算“o”对“*”在S 上满足右分配律(或第二分配律)；

（3) 如果“o”对“*”既满足左分配律又满足右分配律，则称o”对“*”在S上满足分配律。

吸收律

定义　设“*”、“o”是集合A上的二元运算，<A, *, o >是一个代数系统，如果对任意x, y∈A，都有

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

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

则称“*”和“o”满足吸收律。

特殊元

在代数系统中，有些元素有特殊性质，叫特殊元。

例如在代数系统<N，×>中，其中N是自然数，“×”是普通乘法，0∈ N，并且对任意x∈ N，有

$$x\times 0=0\times x=0$$

1∈ N，并且对任意x∈ N，有

$$x\times 1=1\times x=x$$

幺元（单位元）

定义 设<A, *>是二元代数系统，

（1）若存在$e \in A$，对任意$a \in A$，都有

$$a * e = e * a = a,$$

则称e是A中关于运算“*”的一个幺元（单位元）

（2）若存在$e_l \in A$，使得对任意$a \in A$，都有

$$e_l * a = a,$$

则称e_l是A中关于运算“*”的一个左幺元（左单位元）

（3）若存在$e_r \in A$，使得对任意$a \in A$，都有

$$a * e_r = a,$$

称e_r是A中关于运算“*”的一个右幺元（右单位元）

例

下列代数系统是否存在幺元(左幺元或右幺元)，如果存在计算之。

（1）<R, + >，R是实数集，“+”是加法运算；

（2）<R^+, +>，R^+是正实数集，“+”是加法运算；

（3）<P(A×A), o>，其中P (A×A)表示集合A上的所有二元关系集合，运算“o”表示关系的复合；

（4）< A, *, o, ∧>，其中A = {a, b, c}，二元运算“*”,“o”,“∧”如表12.3.2、表12.3.3和表12.3.4分别所示。

例 （续）

表 12.3.2

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

表 12.3.3

○	a	b	c
a	b	a	a
b	b	b	b
c	a	c	c

表 12.3.4

∧	a	b	c
a	a	b	c
b	b	a	c
c	c	a	c

分析 可以直接通过定义计算幺元，即首先假设幺元存在，然后计算之，最后验证所计算的元是否是幺元。

例 （续）

（1）设x是<R, + >的幺元，则由定义，对任意a∈R，有

$$x + a = a,$$

让a = 1，有x + 1 = 1，则x = 0，x∈R。

这说明，如果<R, + >的幺元存在，那么幺元必是0。

对任意a∈R，0 + a = a + 0 = a，即验证可得，0是<R, + >的幺元。

例 （续）

（2）设x是$<R^+, +>$的幺元，对任意$a \in R^+$，有

$$x + a = a,$$

让$a = 1$，有$x + 1 = 1$，则$x = 0$，但$0 \notin R^+$。

这说明$<R^+, + >$不存在幺元。同理，左、右幺元也不存在。

例 （续）

（3）设X是< P(A×A), o>的幺元，对任意Y∈P(A×A)，有

$$XoY = Y,$$

让$Y = I_A$，则$XoI_A = I_A$，又$XoI_A = X$，因此$X = I_A$。

这说明，如果<P(A×A), o>的幺元存在，则幺元必是I_A。

对任意Y∈P(A×A)，

$$I_AoY = Y\ o\ I_A = Y,$$

即验证可得I_A是< P(A×A), o>的幺元。

例 （续）

（4）由于给出了运算表，因此可以根据运算表直接观察可得。

解（1）<R, +>中的幺元是0；

（2）<R^+, +>中无幺元；

（3）< P(A×A), o>中的幺元是恒等关系I_A；

（4）<A, *, o, ∧>中关于运算“*”有左幺元a和b，但无右幺元，因此无幺元，关于运算“o”无左幺元，但有右幺元b和c，因此无幺元；关于运算“o”有幺元a。

结论

（1）计算幺元可根据定义直接进行，即首先假设幺元存在，并根据定义计算，然后进行验证。

（2）可以直接从运算表中看出运算是否有左幺元或右幺元。具体方法是：

① 如果元素x所在的行上的元素与行表头完全相同，则x是一个左幺元；

② 如果元素x所在的列上的元素与列表头完全相同，则x是一个右幺元；

③同时满足①和②。

■ 零元

定义12.3.8 设<A, *>是一个二元代数系统，

（1）若存在$\theta \in A$，使得对任意$a \in A$，都有

$$a * \theta = \theta * a = \theta,$$

则称θ是A中关于运算“*”的一个零元；

（2）若存在$\theta_l \in A$，使得对任意$a \in A$，都有

$$\theta_l * a = \theta_l,$$

则称θ_l是A中关于运算“*”的一个左零元；

（3）若存在$\theta_r \in A$，使得对任意$a \in A$，都有

$$a * \theta_r = \theta_r,$$

则称θ_r是A中关于运算“*”的一个右零元。

■ 逆元

定义12.3.9 设<A, *>是二元代数系统，e是幺元，a∈A，若存在一个元素b∈A，

（1）使得： $a * b = b * a = e$，

则称a可逆，并称b是a的一个逆元，记为a^{-1}；

（2）使得： $b*a = e$，

则称a左可逆，并称b是a的一个左逆元，记为a_l^{-1}；

（3）使得： $a * b = e$，

则称a右可逆，并称b是a的一个右逆元，记为a_r^{-1}。

定理

设<A, *>是一个代数系统，“*” 满足结合律，a∈A，a可逆，则a是可消去元。

证明　记幺元为e，a的逆元为a^{-1}，设x、y是A中的对任意元素，假设

$$a * x = a * y。$$

由$a * x = a * y$，有

$$a^{-1} * (a * x) = a^{-1} * (a * y),$$

又结合律成立，所以有

$$(a^{-1} * a) * x = (a^{-1} * a) * y,$$

即$e * x = e * y$，可得

$$x = y$$

定理

设<A, *>是二元代数系统，

（1）如果<A, *>存在幺元，则幺元唯一；

（2）如果<A, *>存在幺元，则该幺元一定是左、右幺元；

（3）如果<A, *>存在左、右幺元，则该左、右幺元相等，且是幺元。

定理

证明（1）（反证法）设〈S,*〉存在两个以上的幺元，不妨假设e_1，e_2是〈S,*〉的两个幺元，

则对任意$x\in S$， $x*e_1=e_1*x=x$，此时，取$x=e_2$，

$$有 e_2*e_1=e_1*e_2=e_2 \qquad ①$$

则对任意$x\in S$，有$x*e_2=e_2*x=x$，此时，取$x=e_1$，

$$有 e_1*e_2=e_2*e_1=e_1 \qquad ②$$

由①、②可知

$$e_1=e_2,$$

即〈S,*〉的幺元是唯一的。

定理 （续）

（2）显然成立

（3）若e_l、e_r是〈S,*〉的左、右幺元，

则对任意$x\in S$，有$e_l*x=x$，此时，取$x=e_r$，有

$$e_l*e_r=e_r \qquad ①$$

则对任意$x\in S$，有$x*e_r=x$，此时，取$x=e_l$，有

$$e_l*e_r=e_l \qquad ②$$

由①、②可知

$$e_l=e_r,$$

即左、右幺元相等；显然可得 $e=e_l$。

定理

设<S,* >是二元代数系统，

（1）如果<A, *>存在零元，则零元唯一；

（2）如果<A, *>存在零元，则该零元一定是左、右零元；

（3）如果<A, *>存在左、右零元，则该左、右零元相等，且是零元。

分析 该定理的证明方法与定理12.3.2证明相似。

证明 略。

定理

设<A, *>是二元代数系统，“*”满足结合律且设e是幺元，则对任意a∈A，

（1）如果a存在逆元，则逆元唯一；

（2）如果a存在逆元，则该逆元一定是左、右逆元；

（3）如果a存在左、右逆元，则该左、右逆元相等，且是逆元。

分析 该定理的证明方法与定理12.3.2证明相似

定理 （续）

证明 （1）（反证法）设$a \in A$存在逆元，且不唯一，不妨设a_1，a_2都是a的逆元，则有

$$a * a_1 = a_1 * a = e,$$

$$a * a_2 = a_2 * a = e,$$

由于“*”满足结合律，所以有

$$a_1 = a_1 * e = a_1 * (a * a_2) = (a_1 * a) * a_2 = e * a_2 = a_2,$$ 即

$$a_1 = a_2$$

即a的逆元唯一；

定理 （续）

（2）由逆元、左逆元和右逆元的定义直接可得；

（3）设a∈A的左、右逆元分别是a_l^{-1}和a_r^{-1}，则有

$$a_l^{-1} * a = e，\ a*a_r^{-1} = e，$$

“*”满足结合律，所以有

$$\begin{aligned} a_r^{-1} &= e * a_r^{-1} \\ &= (a_l^{-1} * a) * a_r^{-1} \\ &= a_l^{-1} * (a * a_r^{-1}) \\ &= a_l^{-1} * e = a_l^{-1}, \end{aligned}$$

所以 $$a^{-1} = a_r^{-1} = a_l^{-1}$$

推论

设<A, *>是二元代数系统，“*”满足结合律，a, b∈A，

（1）如果a, b分别有逆元a^{-1}, b^{-1}，则 $(a*b)^{-1} = b^{-1}*a^{-1}$；

（2）如果a是左（或右）可逆的元素，则a是左（或右）可消去的元素；

（3）如果a是可逆的元素，则a是可消去的元素。

推论 （续）

分析 (1) 根据逆元的定义，只需证明

$$(a * b) * (b^{-1} * a^{-1})$$

$$= (b^{-1} * a^{-1}) * (a * b) = e;$$

同理，(2)和(3)可以直接根据消去元的定义证明。

推论 （续）

证明 (1) 由于“$*$”满足结合律，所以有

$(a * b) * (b^{-1} * a^{-1})$

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

$= a * e * a^{-1} = a * a^{-1} = e$，

$(b^{-1} * a^{-1}) * (a * b)$

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

$= b^{-1} * e * b = b^{-1} * b = e$，即

$$(a*b)^{-1} = b^{-1}*a^{-1}。$$

推论 （续）

（2）若a是左可逆的元素，设左逆元为a_l^{-1}，则对任意x, y∈A，如有a*x = a*y，则

$$a_l^{-1} * (a * x) = a_l^{-1} * (a * y),$$

即 $(a_l^{-1} * a) * x = (a_l^{-1} * a) * y,$

$$e * x = e * y，所以$$

$$x = y$$

则a是左可消去元。

同样可证，如果a是右可逆的，则a是右可消去元。

（3）由(2)和定理12.3.4直接可证。

例

设G = $\{f_{a,b}(x) = ax+b \mid a\neq 0, a, b\in R\}$，其中R是实数，“o”是G上关于函数的复合运算 。

（1）验证<G, o>是代数系统；

（2）如有幺元计算之；

（3）如有零元计算之；

（4）如有幂等元，计算出这些幂等元；

（5）说明G中的那些元有逆元，并计算这些元的逆元。

例 （续）：封闭性

分析 （1）要说明<G, o>是代数系统，只需要说明“o”对G封闭，即说明对任意$f_{a,b}$，$f_{c,d}\in G$，

$$f_{a,b}\circ f_{c,d}\in G,$$

又 $(f_{a,b}\circ f_{c,d})(x) = f_{c,d}(f_{a,b}(x))$

$= f_{c,d}(ax+b) = c(ax+b)+d$

$= cax+bc+d = f_{ca,bc+d}(x)$，即

$$f_{a,b}\circ f_{c,d} = f_{ca,bc+d},$$

显然$ca \neq 0$，故

$$f_{ca,bc+d}\in G,$$

所以“o”对G是封闭的，即〈G, o〉是代数系统。

例 （续）：幺元

（2）不妨假设幺元是$f_{c,d} \in G$，则对任意$f_{a,b} \in G$，有

$$f_{a,b} \circ f_{c,d} = f_{a,b}，又$$

$$f_{a,b} \circ f_{c,d} = f_{ca,\, bc+d}，则$$

$$f_{a,b} = f_{ca,\, bc+d}，$$

因此，对任意$x \in R$，有

$$f_{a,b}(x) = ax+b = f_{ca,\, bc+d}(x) = cax+bc+d，$$

特别取$x = 0$， $x = 1$，可得

$$bc+d = b，\quad ca = a。$$

由于$f_{a,b}$是G中的对任意元，取$a = 1$，$b = 2$，可得

$$c = 1，\quad d = 0。$$

例（续）：幺元

上面的分析说明，如果<G, o>有幺元，则此幺元必是$f_{1,0}$，所以需进一步验证$f_{1,0}$就是幺元。

即对任意$f_{a,b} \in G$，验证等式

$$f_{a,b} \circ f_{1,0} = f_{1,0} \circ f_{a,b} = f_{a,b}$$

显然此等式成立，所以$f_{1,0}$是幺元。

例（续）：零元

（3）按同样的思路，不妨假设零元是$f_{c,\ d}\in G$，由零元的定义，对任意 $f_{a,\ b}\in G$，有

$$f_{a,\ b}of_{c,\ d}=f_{c,\ d},$$

$$f_{a,\ b}of_{c,\ d}(x)=cax+bc+d=f_{c,\ d}(x)=cx+d,$$

取$x=0$，有 $bc=0$，

又$f_{a,\ b}$是对任意，取$b=1$，可得

$$c=0,$$

又$f_{c,\ d}\in G$，则$c\neq 0$， 矛盾，故$f_{c,\ d}$是零元不成立，故代数系统<G, o>没有零元。

例（续）：幂等元

（4）不妨假设幂等元是$f_{c,d} \in G$，有

$$f_{c,d} \circ f_{c,d} = f_{c,d},$$

$$f_{c,d} \circ f_{c,d}(x) = c^2x+cd+d = f_{c,d}(x) = cx+d,$$

取$x = 0$，有$cd = 0$，又$c \neq 0$，则

$$d = 0,$$

取$x = 1$，有$c^2+cd+d = c+d$，又$d = 0$，$c \neq 0$，则

$$c = 1。$$

因此，$f_{c,d} = f_{1,0}$，

又$f_{1,0} \circ f_{1,0} = f_{1,0}$，所以$f_{1,0}$是唯一幂等元。

例（续）：逆元

（5）对任意$f_{a,b}\in G$，不妨假设它的逆元为$f_{c,d}$，当然$f_{c,d}\in G$，有

$$f_{a,b}\circ f_{c,d} = f_{1,0},$$

$$f_{a,b}\circ f_{c,d}(x) = cax+bc+d = f_{1,0}(x) = x,$$

特别取$x = 0$，$x = 1$，可得

$$bc+d = 0,\quad ca = 1,$$

因为$a\neq 0$，显然$c = 1/a$，$d = -b/a$，故

$$f_{c,d} = f_{1/a,\,-b/a},$$

例（续）：逆元

同理，上面分析说明，如果$f_{a,\ b}$有逆元，则此逆元是$f_{1/a,\ -b/a}$，因此还需验证$f_{1/a,\ -b/a}$是$f_{a,\ b}$逆元，即验证等式

$$f_{a,\ b} \circ f_{1/a,\ -b/a} = f_{1/a,\ -b/a} \circ f_{a,\ b} = f_{1,0},$$

显然此等式成立，所以$f_{1/a,\ -b/a}$是$f_{a,\ b}$的逆元。

由$f_{a,\ b}$的对任意性，可得G中的任何一个元都有逆元。

结论

（1）<G, o >是代数系统；

（2）幺元是$f_{1,0}$；

（3）<G, o >中没有零元；

（4）<G, o >中唯一幂等元是$f_{1,0}$；

（5）<G, o >中对任意元$f_{a,b}$的逆元是$f_{1/a,-b/a}$。

■ 同态与同构

在现实社会中，存在着很多代数系统，但仔细分析这些众多的代数系统发现，有些代数系统，他们之间表面上似乎不相同，但他们实际上“相同”。

如有两个代数系统<{奇，偶}，*>和<{正，负}， o>，其运算“*”和“o”分别定义如下表

表 12.4.1

*	奇	偶
奇	奇	偶
偶	偶	偶

表 12.4.2

o	正	负
正	正	负
负	负	负

定义

设<A, *>和<B, o>为两个二元代数系统，ψ是A到B的函数。对任意x, y∈A，都有

$$\psi(x*y) = \psi(x) \circ \psi(y), \qquad (1)$$

则称ψ是从<A, *>到<B, o>的同态映射，称ψ(A)为同态象，其中ψ(A) = {ψ(x) | x∈A}。

如果存在一个从<A, *>到<B, o >的同态映射，则称<A, *>与<B, o >同态，记为<A, *>∽<B, o >。

当<A, *> = <B, o >时，称其同态为自同态。

定义 （续）

当同态映射ψ分别是单射、满射、双射时，分别称ψ是单一同态映射、满同态映射、同构映射。

如果存在一个从<A, *>到<B, o >的同构映射（单一同态映射、满同态映射），则称代数系统<A, *>与<B, o >同构（单一同态、满同态）。

用<A, *>≌<B, o >表示<A, *>与<B, o >同构。

同态与同构

同态与同构是代数系统中一个非常重要的概念，它体现了两个代数系统之间的某种联系，后面章节将会学习半群、群、格、布尔代数等典型的代数系统，那么将同态与同构的概念应用到这些典型的代数系统，就会得到半群、群、格、布尔代数的同态与同态。

例

设代数系统<Z, +>和<E, +>中，Z、E分别是整数集和偶数集，“+”是加法，证明<Z, +>≌<E, +>。

分析　证明两个代数系统同构，关键是找出同构映射。假设f是<Z, +>到<E, +>的同构映射，根据同构映射的定义，有

对任意$x, y \in Z$，$f(x + y) = f(x) + f(y)$，

特别取$x = 0$，$y = 0$，有

$f(0) = f(0 + 0) = f(0) + f(0)$，可得$f(0) = 0$。

例 （续）

对任意$n \in Z$， $f(n) = f(n-1+1) = f(n-1) + f(1)$， 可得递推公式如下：

$$f(n) = f(n-1) + f(1),$$

如果$f(1) > 0$，则$f(n)$是递增函数，

$$0 = f(0) < f(1) < f(2),$$

而f又是Z到E的双射，因此此时必有

$$f(1) = 2,$$

同理，如果$f(1) < 0$，可得 $f(1) = -2$。

根据以上分析可知，

对任意$n \in Z$， $f(n) = 2n$或$f(n) = -2n$，

例 （续）

以上说明，如果f是同构映射，则

$$f(n) = 2n或f(n) = -2n，$$

因此需进一步验证$f(n) = 2n$或$f(n) = -2n$是否是同构映射。

证明 对任意$n \in Z$，令$f(n) = 2n$，则显然f是Z到E的双射，又对任意$x，y \in Z$，有

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

因此f是同构映射，同理可证$f(n) = -2n$也是同构映射。故有$<Z, +> \cong <E, +>$。

定理

设ψ是<A, *>到<B, o >的同态映射，那么<ψ(A), o >是<B, o>的子代数。

分析 需证ψ(A) 非空，且运算“o”对ψ(A)封闭。

证明 由于A非空，所以显然ψ(A)为B的非空子集。

对任意x, y∈ψ(A)，存在a, b∈A，使得

$$\psi(a) = x，\ \psi(b) = y，有$$

$$x \circ y = \psi(a) \circ \psi(b) = \psi(a * b)，$$

因为a * b∈A，所以ψ(a * b) ∈ψ(A)，即

$$x \circ y \in \psi(A)，$$

故“o” ψ(A)对封闭，得证。

定理

设ψ是二元代数系统<A, *>到<B, o>的满同态，则：

（1）若“*”可交换，则“o”也可交换；

（2）若“*”可结合，则“o”也可结合；

（3）若e是<A, *>的幺元，则ψ(e)是<B, o>的幺元；

（4）若θ是<A, *>的零元，则ψ(θ)是<B, o>的零元；

定理 （续）

（5）若a是<A, *>的幂等元，则ψ(a)是<B, o>的幂等元；

（6）若x^{-1}是x在<A, *>中的逆元，则ψ(x^{-1})是ψ(x)在<B, o>中的逆元；

（7）若a是<A, *>的（左、右）可消去元，则ψ(a)是<B, o>的（左、右）可消去元。

定理 （续）

证明 （1）对任意x, y∈B，因为ψ是满射，所以存在a, b∈A，使得

$$\psi(a) = x, \quad \psi(b) = y,$$

因为运算“*”在A中可交换，则有

$$a * b = b * a, \quad \text{于是}$$

$$xoy = \psi(a)\, o\psi(b) = \psi(a * b) = \psi(b * a) = \psi(b)\, o\psi(a) = yox,$$

所以运算“o”在B中满足交换律。

（2）类似（1），略。

定理 （续）

（3）对任意x∈B，因为ψ是满射，所以存在a∈B，使得ψ(a) = x，又e是<A, *>的幺元，则有

a * e = e * a = a，于是

xoψ(e) = ψ(a) oψ(e)

= ψ(a * e) = ψ(a) = x，

ψ(e) ox = ψ(e) oψ(a)

= ψ(e * a) = ψ(a) = x，所以有

xoψ(e) = ψ(e) ox = x，

由x的对任意性，可知ψ(e)是<B, o>的幺元。

其它类似（3），略。

定理

设ψ是代数系统<A, $*_1$, $*_2$>到<B, o_1, o_2>的满同态，这里$*_i$和$_i$(i = 1, 2)均为二元运算，那么有

（1）若运算“$*_1$”对“$*_2$”在A中满足分配律，则“o_1”对“o_2”在B中也满足分配律；

（2）若运算“$*_1$”和“$*_2$”在A中满足吸收律，则“o_1”和“o_2”在B中也满足吸收律。

证明　定理的证明类似与定理12.4.2

同构关系

令P = {x| x是代数系统}，$\cong$ = {<x, y> | x, y∈P,且x与y同构}，则很容易证明$\cong$是P上等价关系，由该等价关系可以得到等价类，在同一个等价类的两个代数系统同构，它们在同构的意义下可以看作是相同的代数系统，具有完成相同的代数性质。称“$\cong$”为同构关系。

本章总结

- 代数系统的定义
- 代数系统中的特殊元素
- 计算代数系统中的特定元素