离散数学

西安交通大学
计算机学院

离散数学

第六章 代数系统

§1.代数系统的基本概念

§2.代数系统的同态和同构

§3.半群与单子

§4.群

§5.环

§6.域

离散数学

§1.代数系统的基本概念

- 代数系统
- 代数系统的基本性质
- 子代数系统

离散数学

§1.代数系统的基本概念

代数系统有两层含义，一层是代数，一层是系统。代数的实质是运算与比较，运算与比较的概念我们在上二章已经定义过了，比较则牵扯到半序关系；而系统的含义则是集成，即将若干相关联的部分构成一个整体。代数系统就是将一个非空集合以及这个集合上的若干个运算、关系集成在一起成为一个整体。

这相当于面向对象的程序设计中的捆绑思想。其实代数系统的许多概念都已渗透到计算机科学的各个方面了

离散数学

定义1. 代数系统　代数结构(algebra structure)

一个代数系统(代数结构，简称代数)A是如下的一个有序元组：

$A=(X, R_1, R_2, \ldots, R_m)$

其中：

(1)$X\neq\varnothing$是一个任意集合；

(2)$R_1, R_2, \ldots, R_m$, 是X上的m个运算($m\geq 1$)；

注：•当X是有限集合时，称A为有限代数系统；

•当X是无限集合时，称A为无限代数系统；

•在一个代数系统中运算的集合不能是空的，必须至少有一个X上的运算。代数系统中各个运算的元(阶)数可能是不一样的，即每个运算都有自己的运算元数；

•对于运算我们主要讨论运算的封闭性；另外还要讨论运算的许多性质；

•我们离散数学研究的代数系统主要包含一些以一元、二元为主的运算。

离散数学

例1. (I,+), (I, ×) ,(I,+,×)都是代数系统。

这里：I是整数集合：+和×是整数的加法和乘法。

由于两个整数之和仍为整数，且结果唯一，即∀a, b，a∈I∧b∈I⇒a+b∈I，满足封闭性，故+是I上的二元运算。

由于两个整数之积仍为整数，且结果唯一，即∀a, b，a∈I∧b∈I⇒a×b∈I，满足封闭性，故×是I上的二元运算。

由代数系统的定义知(I,+), (I, ×) ,(I,+,×)分别都是代数系统。

(I, ÷) 是代数系统吗?

例2. (Ω, o)是代数系统。

这里：X={a,b}，设$\Omega=\{f \mid f:X\to X\}$，则

$\Omega=\{f_1, f_2, f_3, f_4\}$ 。

其中：$f_1:\begin{cases} f_1(a)=a \\ f_1(b)=b \end{cases}$ $f_2:\begin{cases} f_2(a)=a \\ f_2(b)=a \end{cases}$ $f_3:\begin{cases} f_3(a)=b \\ f_3(b)=b \end{cases}$ $f_4:\begin{cases} f_4(a)=b \\ f_4(b)=a \end{cases}$

o运算是函数的复合运算 $o:\Omega\times\Omega\to\Omega$ 其运算可列表如下：

由表1可以看出 Ω^2中的任意一个元素的象仍在Ω中，且象是唯一的，即$\forall f, g$，$f\in\Omega\wedge g\in\Omega\Rightarrow f\circ g\in\Omega$ ，满足封闭性。故o是Ω上的一个二元运算。

离散数学

表1称为Ω上二元运算o的运算表。

由代数系统的定义知，(Ω, o)是代数系统。

o	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_2	f_2	f_2
f_3	f_3	f_3	f_3	f_3
f_4	f_4	f_3	f_2	f_1

表 1

例3. (X,*)是代数系统。

这里： X = { a,b,c,d }，定义运算 $*: X^2 \to X$ 如表2所示：

由表2可以看出X^2中的任意一个元素的象仍在X中，且象是唯一的，即

$\forall a, b$，$a \in X \wedge b \in X \Rightarrow a*b \in X$

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

表 2

满足封闭性，故*确实是X上的一个二元运算。

由代数系统的定义知，(X,*)是代数系统。

例4. (1)$(2^X, \cap, \cup)$是代数系统。

这里：X是任意非空的集合，2^X是X的幂集，$\cap$和$\cup$是集合的交和并。

由于X中任意两个子集之交仍为X的子集，且结果唯一，即 $\forall A,B$，$A\in 2^X \wedge B\in 2^X \Rightarrow A\cap B\in 2^X$，满足封闭性，故$\cap$是$2^X$ 上的二元运算。

由于X中任意两个子集之并仍为X的子集，且结果唯一，即 $\forall A,B$，$A\in 2^X \wedge B\in 2^X \Rightarrow A\cup B\in 2^X$，满足封闭性，故$\cup$是$2^X$上的二元运算。

由代数系统的定义知$(2^X, \cap, \cup)$是代数系统。

(2)集合代数$(2^X, \cap, \cup, ')$是代数系统。

另外，'是集合的补。由于X中任意一个子集之补仍为X的子集，且结果唯一，即 $\forall A$，$A \in 2^X \Rightarrow A' \in 2^X$，满足封闭性，故 ' 是$2^X$ 上的一元运算。

由代数系统的定义知$(2^X, \cap, \cup, ')$是代数系统。

例5.时钟代数(X, σ)是代数系统。

这里：$X=\{a_1, a_2, a_3, \ldots, a_n\}$，定义运算 $\sigma: X \to X$

$$\sigma(a_i)=\begin{cases} a_{i+1} & \text{当} a_i \neq n \\ a_1 & \text{当} a_i = n \end{cases}$$

(参见图1)。

显然，由于X中任意一个元素之象仍为X的元素，且结果唯一，即 $\forall a$，$a \in X \Rightarrow \sigma(a) \in X$，满足封闭性，故σ是X上的一元运算。

由代数系统的定义知(X, σ)是代数系统。

离散数学

代数系统的性质一般是由代数系统中所具有的运算的个数，每个运算的元数，以及每个运算所具有的性质决定的。因此研究一个代数系统，主要是研究代数系统中每个运算所具有的性质。

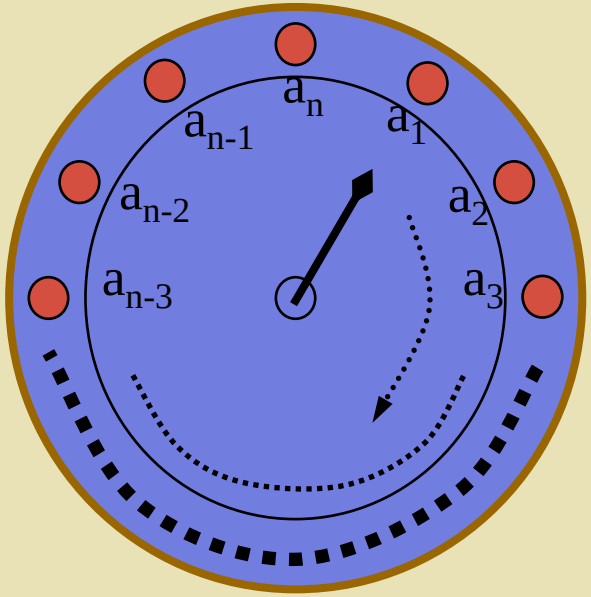

图1

离散数学

定义2.结合律　交换律(associative law,commutative law)

设(X, *)是任一代数系统， *是X上的二元运算。则我们称

(1)*运算满足结合律

$\Leftrightarrow(\forall x\in X)(\forall y\in X)(\forall z\in X)((x*y)*z=x*(y*z))$；

(2)*运算满足交换律$\Leftrightarrow(\forall x\in X)(\forall y\in X)(x*y=y*x)$。

注：•当一个二元运算满足结合律时，在运算表达式中运算的先后次序与运算的结果无关；

•当一个二元运算满足交换律时，在运算表达式中运算对象的位置顺序与运算的结果无关；

•由此可见，结合律改变的是运算的先后次序；交换律改变的是运算对象的位置顺序。前者是对运算符而言；后者是对运算对象而言。为此二元运算的结合律和交换律是两个根本不同的概念。

离散数学

例6.在代数系统(I,+,×)中，二元运算加法+和乘法×都满足结合律和交换律。

例7.在代数系统 $(2^X, \cap, \cup)$ 中，二元运算交∩和并∪都满足结合律和交换律。

例8.在代数系统(I,-)中，减法运算-不满足结合律和交换律。这里：I是整数集合，“－”是整数减法。

由于两个整数之差仍为整数，且结果唯一，即$\forall a, b$，$a\in I\wedge b\in I\Rightarrow a-b\in I$，满足封闭性, 故“-”是I上的二元运算。

由代数系统的定义知 (I, -)是代数系统。

但是，取$1,2,3\in I$，由于

$(3-2)-1=0\neq 2=3-(2-1)$

$3-2=1\neq -1=2-3$

故在此代数系统中，减法运算-不满足结合律，也不满足交换律。

离散数学

定义3.幺元　零元(identity element,zero element)

设 (X, *)是代数系统，* 是X上的二元运算， $x_0 \in X$ 。则我们称

(1)x_0是关于*运算的幺元$\Leftrightarrow(\forall x\in X)(x_0*x=x*x_0=x)$；

(2)x_0是关于*运算的零元$\Leftrightarrow(\forall x\in X)(x_0*x=x*x_0=x_0)$。

注：• 通常将幺元记为 e ； 含有幺元e的代数系统(X, *), 通常记作(X, * , e)； 即　　$(\forall x\in X)(e * x=x * e =x)$ ；

• 在同时具有幺元和零元的代数系统中，通常将幺元记为1，将零元记为 0；即

$(\forall x\in X)(1 * x=x * 1 =x)$；　$(\forall x\in X)(0 * x=x * 0 = 0)$。

离散数学

例9. 在代数系统 (I,+, ×) 中，加法+的幺元是 0，乘法×的幺元是 1。

例10. 在代数系统 (2^X,∩,∪) 中，交∩的幺元是X，并∪的幺元是∅。

例11.在代数系统(I,+,×)中，关于加法+无零元，乘法×的零元是 0 。

例12.在代数系统(2^X,∩,∪,)中，∩的零元是 ∅ ，∪的零元是 X 。

离散数学

定理1.幺元、零元的唯一性

设 (X, *) 是代数系统，* 是X上的二元运算。则

(1)若关于 *运算的幺元存在，则必是唯一的；

(2)若关于 *运算的零元存在，则必是唯一的。

[证].（采用逻辑法）只证幺元的唯一性

e_1是*运算的幺元 $\wedge$ e_2是*运算的幺元

$\Rightarrow(\forall x\in X)(x * e_1=x)\wedge(\forall x\in X)(e_2 * x=x)$,

$\Rightarrow(e_2 * e_1= e_2)\wedge(e_2 * e_1=e_1)$

$\Rightarrow e_1 = e_2$

所以，幺元是唯一的。

离散数学

定义4. 逆元　可逆性(inverse element,invertibility)

设(X, *, e)是代数系统，*是X上的二元运算，e是关于*运算有幺元。

(1)对于某一元素$x \in X$, 若存在着某个元素$y \in X$ ，使得

$$x*y = y*x = e$$

则称y是x关于*运算的逆元，并称x关于*运算是可逆的(invertible)，同时称x是关于*运算的可逆元；

(2)我们称：

*运算在X上是可逆的

$\Leftrightarrow (\forall x \in X)(\exists y \in X)(x*y=y*x=e)$

$\Leftrightarrow$X中的每个元素都是关于*运算的可逆元 。

离散数学

注：• 幺元和零元是对整个代数系统而言。即在一个代数系统中，对某个二元运算来说，只可能有一个幺元，同样也只可能有一个零元。

•而逆元是对代数系统中的每个元素而言的。现在讨论的是X中的某个元素对某个二元运算是否有逆元的问题。当然关于逆元的讨论，只能在二元运算有幺元的前提下进行，即幺元的存在是讨论逆元的先决条件，否则逆元问题无从谈起。

•从定义4可以看出，如果y是x的逆元，则x也是y的逆元。这两者的关系是同时成立的。另外如果x有逆元存在，则称x是可逆元。当知道x有逆元存在时，并不一定知道x的逆元究竟是谁。 因此可逆元的概念是元素本身的性质，而逆元的概念则是两个元素之间的关系，并且这两个元素可能是相同的，也可能是不相同的。

离散数学

例13. 在代数系统$(I,+,\times)$中

(1)加法+的幺元是0，0的逆元是其本身。每个元素关于＋都有逆元。$\forall a\in I$，a的逆元是-a ；

(2)乘法×的幺元是1，1的逆元是其本身。除了1和-1以外，每个元素关于×都无逆元。

例14. 在代数系统$(2^X,\cap,\cup)$中

(1)$\cap$的幺元是X，X的逆元是其本身。除X外每个元素关于$\cap$都无逆元 ；

(2)$\cup$的幺元是$\varnothing$，$\varnothing$的逆元是其本身。除$\varnothing$外每个元素关于$\cup$都无逆元。

离散数学

定理2. 逆元的唯一性

设(X，*，e)是代数系统，*是X上的二元运算并且满足结合律，e是幺元。对任何元素$x\in X$，若x的逆元存在，则必是唯一的。

[证].设y_1 ，$y_2\in X$ 都是x的逆元，则

$$\begin{aligned} y_1 &= e*y_1 \\ &= (y_2*x)*y_1 && (y_2\text{是}x\text{的逆元}) \\ &= y_2*(x*y_1) && (\text{结合律}) \\ &= y_2*e && (y_1\text{是}x\text{的逆元}) \\ &= y_2 \end{aligned}$$

注：•对任何元素$x\in X$，若x的逆元存在唯一，则将其逆元记为x^{-1}。于是，就有

$$x*x^{-1}=x^{-1}*x=e \quad ;$$

•若*运算不满足结合律，则逆元未必是唯一的。

离散数学

例15. 设X={a,b,c,d,e,f,g}，*是X上的二元运算，*运算的运算表如下表3。

从表3可知，(X，*) 是代数系统，a是关于*运算的幺元。由于有

b*e=e*b=a

b*f=f*b=a

b*g=g*b=a

故e, f和g均为b的逆元，即b的逆元不唯一。原因在于*运算不满足结合律。

*	a	b	c	d	e	f	g
a	a	b	c	d	e	f	g
b	b	b	b	b	a	a	a
c	c	b	b	b	a	a	a
d	d	b	b	b	a	a	a
e	e	a	a	a	e	e	e
f	f	a	a	a	e	e	e
g	g	a	a	a	e	e	e

表3

离散数学

注：•因此当代数系统中的二元运算不满足结合律时，逆元的情况变得极为复杂；

•结合律的验证有时是十分困难的。上百个成员的代数，验证结合律，其工作量即使对于一般计算机也是很困难的，有上亿次的计算量。

定义5.消去律(cancellation law)

设(X, *)是代数系统，*是X上的二元运算。

称 *运算满足消去律⇔

a) $(\forall x \in X)(\forall y \in X)(\forall z \in X)(x * y = x * z \Rightarrow y = z)$

b) $(\forall x \in X)(\forall y \in X)(\forall z \in X)(y * x = z * x \Rightarrow y = z)$;

注：• 当*及Δ运算满足交换律时，a)、b)两式中只要有一式成立即有 *及Δ运算满足消去律。

离散数学

例16. 在代数系统(I,+,×)中，加法+满足消去律；乘法×不满足消去律。

对加法+而言，当 a+b=a+c 时，等式两边同时加上-a，就有 b=c。另一式同理可得；

对乘法×而言，取a=0,b=1,c=2，于是有 $a \times b = a \times c$，但 $b \neq c$，故乘法不满足消去律；

例17.在代数系统 $(2^X, \cap, \cup)$中，∩和∪都不满足消去律。

设X={a,b,c,d}，S_1={a,b}, S_2={b,c}, S_3={b}, S_4 ={a,b,c}，则$S_1, S_2 S_3, S_4 \in 2^X$。

由于 $S_1 \cap S_3$ ={b}= $S_2 \cap S_3$，但$S_1 \neq S_2$，故∩不满足消去律。

由于 $S_1 \cup S_4$={a,b,c}= $S_2 \cup S_4$ ，但$S_1 \neq S_2$，故∪不满足消去律。

定义6. 分配律(distributive law)

设$(X,*,\Delta)$是代数系统，$*$和Δ是X上的两个二元运算。

(1) 称$*$运算对Δ运算满足分配律$\Leftrightarrow$

a) $(\forall x\in X)(\forall y\in X)(\forall z\in X)$

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

b) $(\forall x\in X)(\forall y\in X)(\forall z\in X)$

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

(2) 称运算Δ对运算$*$满足分配律$\Leftrightarrow$

a) $(\forall x\in X)(\forall y\in X)(\forall z\in X)$

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

b) $(\forall x\in X)(\forall y\in X)(\forall z\in X)$

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

离散数学

例18. 在代数系统$(I, +, \times)$中

(1) 乘法对加法满足分配律。因为 $\forall a, b, c \in I$，有

$$a\times(b+c)=(a\times b)+(a\times c);$$

(2) 加法对乘法不满足分配律。因为对于$2, 3, 5 \in I$，有

$$(2\times 3)+5=11\neq 56=(2+5)\times(3+5)\ 。$$

例19. 在代数系统$(2^X, \cap, \cup)$中

(1) $\cap$对$\cup$满足分配律，因为 $\forall A,B,C \in 2^X$，有

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C);$$

(2) $\cup$对$\cap$满足分配律，因为 $\forall A,B,C \in 2^X$，有

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)。$$

注：• 以上两例的两个二元运算都满足交换律，因此两个等式只要有一个成立即可。

离散数学

定义7. 反身律　鞋袜律

设$(X,*,^{\clubsuit})$是代数系统，$*$是X上的二元运算，$^{\clubsuit}$是X上的一元运算。

(1) 称$^{\clubsuit}$运算满足反身律$\Leftrightarrow(\forall x\in X)((x^{\clubsuit})^{\clubsuit}=x)$ ；

(2) 称$^{\clubsuit}$运算关于$*$运算满足鞋袜律

$\Leftrightarrow(\forall x\in X)(\forall y\in X)((x*y)^{\clubsuit}=y^{\clubsuit}*x^{\clubsuit})$ 。

离散数学

例20. 在代数系统(Σ^*, o, v)中，Σ^*是Σ上字的全体集合，o是两个字的毗连(concatenation)运算，v是一个字的逆置(倒置(inverse))运算。例如，取$\Sigma=\{a,b\}$,字

α=abaaaaabbbbbb，β=abbbbaa，则有

α o β=abaaaaabbbbbb o abbbbaa

=abaaaaabbbbbbabbbbaa

α^v=bbbbbbaaaaaba

于是v运算满足反身律：$(\alpha^v)^v=\alpha$

v运算关于o运算满足鞋袜律：$(\alpha \text{ o } \beta)^v=\beta^v \text{ o } \alpha^v$ 。

注：• (Σ^*, o, v)是代数系统在§3还要讨论；

•一个字$\alpha \in \Sigma^*$称为是一个迴文(palindromes)$\Leftrightarrow \alpha^v=\alpha$ 。

离散数学

定义8. 反身律 de Morgan律

设$(X,*,\Delta,\clubsuit)$是代数系统，$*$和Δ是X上的两个二元运算，$\clubsuit$是X上的一元运算。

(1) 称$\clubsuit$运算满足反身律$\Leftrightarrow(\forall x\in X)((x^{\clubsuit})^{\clubsuit}=x)$;

(2) 称$\clubsuit$运算关于$*$运算和Δ运算满足de Morgan律$\Leftrightarrow$

a) $(\forall x\in X)(\forall y\in X)((x*y)^{\clubsuit}=x^{\clubsuit}\Delta y^{\clubsuit})$;

b) $(\forall x\in X)(\forall y\in X)((x\Delta y)^{\clubsuit}=x^{\clubsuit}*y^{\clubsuit})$ 。

例21. 在代数系统$(2^X,\cap,\cup,')$中

(1)′ 满足反身律，因为 $\forall A\in 2^X$，有$(A')'=A$

(2)′关于$\cap$和$\cup$满足de Morgan律，因为 $\forall A,B\in 2^X$，有 $(A\cap B)'=A'\cup B'$ ， $(A\cup B)'=A'\cap B'$ 。

离散数学

定义9. 子代数系统(subalgebra system)

设$A=(X,O_1,O_2,\ldots,O_m)$是代数系统，其中$O_1,O_2,\ldots,O_m$是X上的m个运算，其元数分别为$p_1, p_2, \ldots, p_m$。若有子集$S\subseteq X$且$S\neq\varnothing$，对A中的每一个运算O_i，有其子关系O_{si}，使得O_{si}也是S上的P_i元运算，从而使得

$(S, O_{S1}, O_{S2}, \ldots, O_{Sm})$也构成一代数系统，则我们称此代数系统是A的子代数系统，记为

$$A_s=(S, O_1, O_2, \ldots, O_m) \quad 。$$

注：•子代数系统的概念将贯穿于本章。因为每个非空集合总有非空子集存在，因此每遇到一类代数系统就会遇到同类子代数系统的问题。

•由于子代数系统中的运算就是原来那个代数系统中相应运算的子关系。因此经常将子代数系统中的运算符用原来那个代数系统中的运算符来表示。

•这也是“运算符是任意的”的一种具体体现（‘重载’概念）。

•验证子代数系统必须验证条件：1°$S\subseteq X$； 2° $S\neq\varnothing$ ； 3°封闭性。

离散数学

例22. $(S_1,*_1)$是$(X,*)$的子代数系统

$(S_2,*_2)$不是$(X,*)$的子代数系统

这里X={a,b,c,d}，S_1={a,b}，S_2={c,d}是X的两个子集；*是X上的一个二元运算，其运算表见表4，已知(X，*)是代数系统。由表4取出*运算对应于子集S_1和S_2的子关系$*_1$和$*_2$如表5及表6所示。

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

表4

$*_1$	a	b
a	a	b
b	a	b

表5

$*_2$	c	d
c	b	a
d	b	a

表6

离散数学

由表5知$*_1$是S_1上的二元运算，因此$(S_1,*_1)$是$(X, *)$的子代数系统。

由表6知$*_2$不是S_2上的二元运算（不满足封闭性），因此$(S_2,*_2)$不是$(X, *)$的子代数系统。

例23. $(N,+, \times)$、$(I, +, \times)$、$(Q, +, \times)$都是$(R, +, \times)$的子代数系统

在代数系统 $(R,+,\times)$中，$+, \times$对自然数集N、整数集I、有理数集Q都是封闭的，故$(N,+, \times)$、$(I, +, \times)$、$(Q, +, \times)$都是$(R, +, \times)$的子代数系统。

离散数学

例24. (E, +, ×)是(I, +, ×)的子代数系统

(O, +, ×)不能构成(I, +, ×)的子代数系统

在代数系统 (I, +, ×)中，取I的两个子集如下：

E={x:x是偶数}，O={y:y是奇数}

由于任意两个偶数之和仍为偶数，任意两个偶数之积仍为偶数，故+, ×对I的偶数子集E是封闭的。

因此(E, +, ×)是(I, +, ×)的子代数系统。

由于任意两个奇数之积是奇数，故×对I的奇数子集O是封闭的。但是任意两个奇数之和是偶数，故+对I的奇数子集O是不封闭的。

因此不存在+的子关系是O上的二元运算。故虽有×的子关系是O上的二元运算，但(O, +, ×)仍不能构成(I, +, ×)的子代数系统.

离散数学

定理3. 遗传性定理

设(X，*)是代数系统，*是X上的二元运算。(S，*)是(X，*)的子代数系统。则

(1)*运算在X上有结合律⇒ *运算在S上有结合律；

(2)*运算在X上有交换律⇒ *运算在S上有交换律。

[证]. 只证(1)

对于任何元数$a,b,c\in S$，由于$S\subseteq X$，所以$a,b,c\in X$。而*运算在X上有结合律，因此有

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

但由于(S，*)是(X，*)的子代数系统，*运算关于S封闭，$(a*b)*c, a*(b*c)\in S$，因此上述等式在S上也是成立的。这说明*运算在S上也有结合律。

注：•其实，其它许多性质，诸如消去律、分配律、de morgan律等等，在其各自所在类的代数系统与其子代数系统间，都有遗传性定理成立！我们不再证明，以后有时会直接应用到。

§2.代数系统的同态和同构

- 代数系统间的同态
- 代数系统间的同构关系

离散数学

§2.代数系统的同态和同构

例1. $(2^A,\cup)$是代数系统

这里A={a}，$\cup$是2^A上的并运算，其运算表见表1 。

$\cup$	$\varnothing$	A
$\varnothing$	$\varnothing$	A
A	A	A

表1

例2. (B,$\vee$)是代数系统

这里B={0,1}，$\vee$是B上的或运算，其运算表见表2 。

$\vee$	0	1
0	0	1
1	1	1

表2

注：•由例1和例2可以看到，在这两个代数系统中，虽然集合不同，运算不同，但这两个二元运算的运算表却如此相似，如用$\cup$代替$\vee$，用$\varnothing$代替0，用A代替1，那么就会得到两张完全一样的运算表；反之也一样。这说明这两个代数系统除符号外，没有实质上的不同。研究两个代数系统间的这种结构相似性、相同性是我们本节的任务。

离散数学

定义1.同类型（same type）

称两个代数系统

$A=(X,O_1,O_2,\cdots,O_m)$和$B=(Y,O'_1,O'_2,\cdots,O'_n)$

是同类型的代数系统⇔

(1) m = n；

(2)O_i运算和相对应的O'_i运算的元数相同（ i= 1, ⋯,m ）。

例3. $(I, +,\times)$ 和$(2^X, \cap, \cup)$是两个同类型的代数系统

因为这两个代数系统都具有两个运算，且＋和∩都是二元运算， ×和∪也都是二元运算。

例4. $(2^X, \cap, \cup,')$ 和$(B, *,\oplus,^-)$是两个同类型的代数系统

因为这两个代数系统都具有三个运算，且∩和*， ∪和⊕也都是二元运算，′和-都是一元运算。

离散数学

定义2.同态(homomorphism)

称两个同类型的代数系统

$A=(X,O_1,O_2,\cdots,O_m)$和$B=(Y,O'_1,O'_2,\cdots,O'_m)$

是同态的⇔存在着一个函数 h：$X\to Y$　　使得：

对任何一对运算O_i和O'_i（$i=1,\cdots,m$）（设其元数为p_i），都满足如下的**同态公式**：

$$\forall(x_1,x_2,\ldots,x_{pi})\in X$$

$$h(O_i(x_1,x_2,\ldots,x_{pi}))=O'_i(h(x_1),h(x_2),\ldots,h(x_{pi}))\quad ①$$

注：• 称函数 h 是保持运算的；并称函数 h 为从A到B的同态函数，记为h：A~B；称两代数系统A与B同态，记为A ~ B；

• h对O_i和O'_i保持运算的含义是指在 h 的作用下，**元素运算结果的象等于元素象的运算结果。**

离散数学

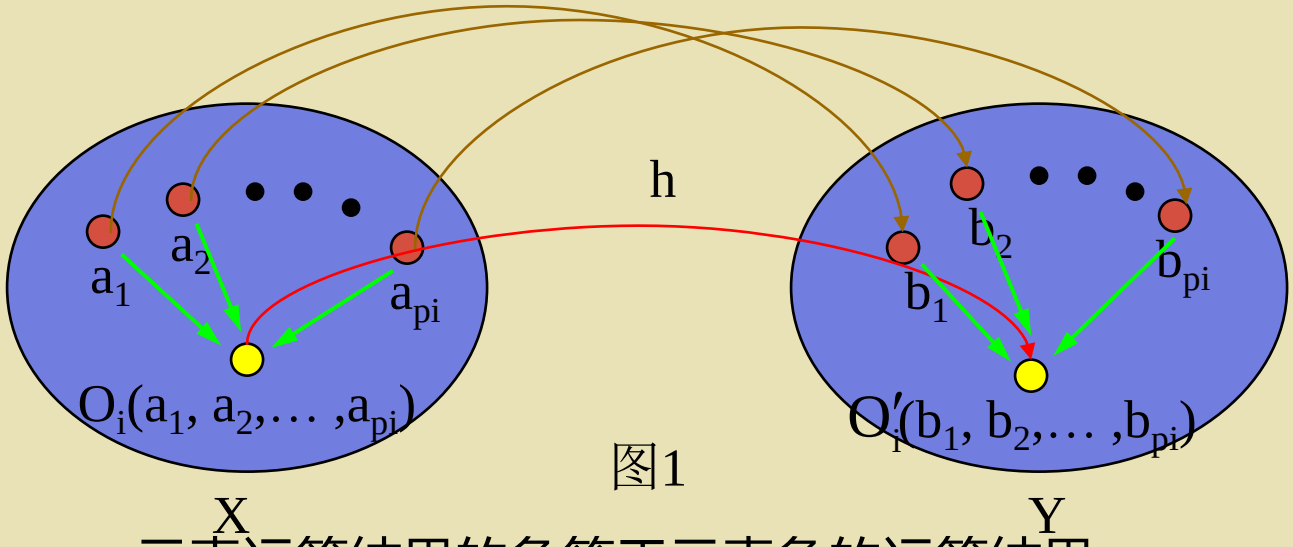

图1

元素运算结果的象等于元素象的运算结果

离散数学

定义3.同态象 单同态 满同态

设代数系统$A=(X,O_1,O_2,\cdots,O_m)$同态于代数系统$B=(Y,O'_1,O'_2,\cdots,O'_m)$，其同态函数为 h：$X\to Y$ 。

(1)称X在h下的象集$h(X)\subseteq Y$与B的所有运算一起组成的 $C=(h(X),O'_1,O'_2,\cdots,O'_m)$是A的同态象；

(2)若h是单射函数，则称h是从A到B的单同态函数并称C为A的单同态象；

(3)若h是满射函数，则称h是从A到B的满同态函数；并称 B为A的满同态象(这时有$h(X)=Y$,$C=B$) 。

例5.代数系统$(N, +)$与代数系统$(N_m, +_m)$是满同态的

这里N是自然数集合,＋是自然数加法， 故$(N, +)$是代数系统；

$N_m=\{[0]_m, [1]_m, \ldots, [m-1]_m\}$，二元运算$+_m$定义如下：

$\forall [i]_m, [j]_m \in N_m$，

$$[i]_m +_m [j]_m = [(i+j) \bmod m]_m$$

由于$0 \le (i+j) \bmod m < m$，因此运算结果唯一，且$[(i+j) \bmod m]_m \in N_m$，满足封闭性。故$+_m$是$N_m$上的二元运算，故$(N_m, +_m)$是代数系统；

离散数学

定义函数 $h: N \to N_m$ 使得

$\forall i \in N, h(i) = [i \bmod m]_m$

$\forall i,j \in N$，有

$h(i+j) = [(i+j) \bmod m]_m$

$= [(i \bmod m + j \bmod m) \bmod m]_m$

$= [i \bmod m]_m +_m [j \bmod m]_m$

$= h(i) +_m h(j)$

故 h 对+和$+_m$满足同态公式；

对任意元素$[i]_m \in N_m$，当然有$i \in N$，使得 $h(i) = [i]_m$

故h是满射的；

由定义2和3知，h 是从$(N, +)$到$(N_m, +_m)$的满同态函数，即$(N_m, +_m)$是$(N, +)$的满同态象。

离散数学

例6.代数系统(N,+)与代数系统(X,×)是满同态的

这里N是自然数集合,＋是自然数加法， 故(N, +)是代数系统;

X={1, -1}，×是整数乘法，其运算表如下：

×	1	-1
1	1	-1
-1	-1	1

表3

故，显然(X , ×)是代数系统;

定义函数 h：N →X 使得

h(2m)=1，h(2m+1)=-1

于是有

$$h(2m+2n)=h(2(m+n))=1=1\times 1= h(2m)\times h(2n)$$

$$h(2m+2n+1)=h(2(m+n)+1)=-1=1\times(-1)$$

$$= h(2m)\times h(2n+1)$$

$$h(2m+1+2n+1)=h(2(m+n+1))=1= (-1)\times(-1)$$

$$= h(2m+1)\times h(2n+1)$$

离散数学

故 h 对+和×满足同态公式；

并且h 显然是从 N 到 X 的满射函数；

由定义2和3可知，h 是从(N, +)到(X , ×)的满同态函数，即(X , ×)是(N, +)的满同态象。

注：•由例1和例2 可以看到$(N_m , +_m)$和(X , ×) 都是(N, +) 的满同态象。由此可知，一个代数系统的满同态象可以是各种各样的代数系统。

离散数学

定理1. 设代数系统$A=(X,O_1,O_2,\cdots,O_m)$同态于代数系统$B=(Y, O_1', O_2', \cdots, O_m')$，其同态函数为$h: X\to Y$。则A的同态象$C=(h(X), O_1', O_2', \cdots, O_m')$是B的子代数系统。

[证].只须证B的每个运算$O_i'(1\le i\le m)$（设其元数为p_i）在$h(X)$上都是封闭的即可。

对于任何元素$y_1, y_2, \ldots, y_{pi}\in h(X)$，由于$h(X)$是X的象集，故存在着其原象$x_1, x_2, \ldots, x_{pi}\in X$，使得

$$h(x_1)=y_1, h(x_2)=y_2, \ldots, h(x_{pi})=y_{pi}$$

离散数学

于是 $O_i'(y_1, y_2, \ldots, y_{pi})$

$= O_i'(h(x_1), h(x_2), \ldots, h(x_{pi}))$

$= h(O_i(x_1, x_2, \ldots, x_{pi}))$ （同态公式）

$= h(x)$ （O_i运算在X上是封闭的，故可设 $O_i(x_1, x_2, \ldots, x_{pi}) = x \in X$）

$\in h(X)$

所以O_i'运算是封闭的；于是由子代数系统的定义可知A的同态象C是B的子代数系统。

离散数学

定理2.同态遗传定理

设(X，*)和(Y，o) 是两个代数系统，* 和 o 分别是X和Y上的二元运算，h 是从(X，*)到(Y，o)

的满同态函数，那么：

(1)*运算满足结合律⇒ o运算满足结合律；

(2)*运算满足交换律⇒ o运算满足交换律；

(3)e是关于*运算的幺元⇒ h(e) 是关于o运算的幺元；

(4)0是关于*运算的零元⇒ h(0) 是关于o运算的零元；

(5)x关于 *运算有逆元x^{-1}⇒ h(x) 关于o运算的逆元是h(x^{-1})，即 $[h(x)]^{-1} = h(x^{-1})$。

注：•遗传性有三种

（1）定义遗传：

例如，我们定义

$$x \vee y = \max(x, y), \quad x \wedge y = \min(x, y)$$

则求大，求小的对称性就转变为运算$\vee$和$\wedge$的交换律；

又例如，当我们定义

$$[i]_m +_m [j]_m = [(i+j) \bmod m]_m$$

时，普通自然数加法的结合律，交换律实际上已自动遗传给模m加运算$+_m$了；

(2)子代数遗传（参见§1定理3）；

离散数学

(3)同态遗传(即本定理)；

•同态遗传对研究新代数的性质，尤其是结合律很重要

从定理3可见，当(Y，o)是(X，*)的满同态象时，如果对(Y, o)的性质不了解，则可通过满同态函数将(X，*)上的性质带到(Y, o)中去。因此在研究一个新代数系统时，首先应考虑它是否与已有的代数系统同态(甚或后面的同构)，若某个新的代数系统与原有的熟知的代数系统间有这种同态（同构）关系，则对新的代数系统来说，研究起它来就容易的多了；

•实际上，有时定义遗传和子代数遗传可以归结为同态遗传。

离散数学

[证].只证(1), (3), (5),

(1)对于任何元素y_1， y_2, $y_3 \in$Y，由于h是满射，故存在着其原象x_1， x_2, $x_3 \in$X，使得

$h(x_1)=y_1$, $h(x_2)=y_2$, $h(x_3)=y_3$,于是

$$(y_1 \circ y_2) \circ y_3$$

$$= (h(x_1) \circ h(x_2)) \circ h(x_3)$$

$$= h(x_1 * x_2) \circ h(x_3) \quad \text{(同态公式)}$$

$$= h((x_1 * x_2) * x_3) \quad \text{(同态公式)}$$

$$= h(x_1 * (x_2 * x_3)) \quad \text{(*运算的结合律)}$$

$$= h(x_1) \circ h(x_2 * x_3) \quad \text{(同态公式)}$$

$$= h(x_1) \circ (h(x_2) \circ h(x_3)) \quad \text{(同态公式)}$$

$$= y_1 \circ (y_2 \circ y_3)$$

所以o运算满足结合律;

(3) 令$e' = h(e) \in Y$。对于任何元素$y \in Y$，由于h是满射，故存在着其原象$x \in X$，使得

$h(x) = y$，于是

$$
\begin{aligned}
& e' \circ y \\
=\ & h(e) \circ h(x) \\
=\ & h(e * x) && \text{（同态公式）} \\
=\ & h(x) && \text{（e是关于*运算的幺元）} \\
=\ & y \\
=\ & h(x) \\
=\ & h(x * e) && \text{（e是关于*运算的幺元）} \\
=\ & h(x) \circ h(e) && \text{（同态公式）} \\
=\ & y \circ e'
\end{aligned}
$$

即$e' \circ y = y \circ e' = y$，所以$e' = h(e)$是关于o运算的幺元；

(5) 令$e' = h(e) \in Y$。对于任何元素$x \in X$， 由于存在着其逆元$x^{-1} \in X$，故此 $h(x)$， $h(x^{-1}) \in Y$，于是有

$h(x) \circ h(x^{-1})$

$= h(x * x^{-1})$ （同态公式）

$= h(e)$ （x^{-1} 是x关于 $*$ 运算的逆元）

$= e'$

$= h(e)$

$= h(x^{-1} * x)$ （x^{-1} 是x关于 $*$ 运算的逆元）

$= h(x^{-1}) \circ h(x)$ （同态公式）

即 $h(x) \circ h(x^{-1}) = h(x^{-1}) \circ h(x) = e'$

所以$h(x)$关于$\circ$运算的逆元是$h(x^{-1})$，即

$[h(x)]^{-1} = h(x^{-1})$ 。

离散数学

定义4.同构(isomorphism)

设代数系统$A=(X,O_1,O_2,\cdots,O_m)$同态于代数系统$B=(Y,O'_1,O'_2,\cdots,O'_m)$，其同态函数为 h：$X\to Y$ 。若h还是双射函数，则称h是从A到B的同构函数,记为h：$A\cong B$；并且这时我们称A和B同构,记为$A\cong B$ 。

注：•同态和同构概念要求两个代数系统必须是同类型的

从定义2,4可知，论及两个代数系统间的同态和同构，必须在两个同类型的代数系统之间讨论，即两个代数系统中运算的个数必须一样多，且对应的运算的元数也必须相同，否则同态和同构就无从谈起；

•同构概念要求两个集合必须是等势的(即$|X|=|Y|$)

代数系统间的同构要求有一个双射函数存在，因此如果两个代数系统同构，那么这两个代数系统的集合的势是一样的，故有限代数系统绝对不会和无限代数系统同构。同时这个双射函数还要对每一对相应的运算满足同态公式，这样两个代数系统才能同构。

离散数学

- 同构概念是双向的、相互的、可逆的

由于两个代数系统间的同构函数 h 是双射函数，因此 h 的逆函数 h^{-1} 存在，可以证明 h^{-1}是从Y 到 X 的双射函数且对A和B的每一对相应的运算都满足同态公式，故 h^{-1} 是从B 到A 的同构函数。因此对同构而言，两个代数系统若同构，则是互相同构的。

- 同态概念是单方向的、不可逆的

因此，同构实际上是一种特殊的同态。同态的概念和同构的概念不同，同构是无方向性的，即对两个同构的代数系统来说是相互同构。但同态是有方向性的，从A到B有同态函数存在，从 B到A就未必有同态函数存在，即同态的概念不可逆。另外当 h 是满同态函数时，A的同态象就是B。

离散数学

例8. 集合代数$(2^X, \cap, \cup, ')$与布尔代数$(B, \wedge, \vee, \neg)$是同构的。

这里$X=\{a\}$，$2^X=\{\varnothing, X\}$, $B=\{0,1\}$，其运算表如下：

$\cap$	$\varnothing$	X
$\varnothing$	$\varnothing$	$\varnothing$
X	$\varnothing$	X

表4

$\cup$	$\varnothing$	X
$\varnothing$	$\varnothing$	X
X	X	X

表5

	$'$
$\varnothing$	X
X	$\varnothing$

表6

$\wedge$	0	1
0	0	0
1	0	1

表7

$\vee$	0	1
0	0	1
1	1	1

表8

	$\neg$
0	1
1	0

表9

构造自然映射　$h: 2^X \to B$　使得

$h(\varnothing)=0, h(X)=1$，则容易验证h满足同态公式

离散数学

对任何的$C \subseteq X$, $h(C') = \neg h(C)$（一元同态公式）；

对任何的$C_1, C_2 \subseteq X$,

$$\left.\begin{array}{l} h(C_1 \cap C_2) = h(C_1) \wedge h(C_2) \\ h(C_1 \cup C_2) = h(C_1) \vee h(C_2) \end{array}\right\} \text{(二元同态公式);}$$

并且，显然 h 是双射函数；

因此h是从$(2^X, \cap, \cup, ')$到$(B, \wedge, \vee, \neg)$的同构函数，即$(2^X, \cap, \cup, ')$与$(B, \wedge, \vee, \neg)$同构。

同时有h^{-1}：$B \to 2^X$, $h^{-1}(0) = \varnothing$, $h^{-1}(1) = X$。

显然 h^{-1} 是从 B 到 2^X 的双射函数；

同上可证 h^{-1} 满足同态公式；

因此 h^{-1} 是从$(B, \wedge, \vee, \neg)$到$(2^X, \cap, \cup, ')$的同构函数，即$(B, \wedge, \vee, \neg)$与$(2^X, \cap, \cup, ')$同构。

这是一对具体的集合代数与布尔代数同构的例子。

离散数学

例9. (N, +)和(E, +)同构

这里：N 是自然数集合, +是自然数加法，故(N, +)是代数系统；E 是N中偶数集合, +是自然数加法,故(E, +)是代数系统；

这两个代数系统是同类型的，都只有一个二元运算；

取函数 h：$N \to E$，$h(i)=2i \quad (\forall i \in N)$；

显然h是双射函数；

$\forall i,j \in N$ 有：

$h(i+j)=2(i+j)=2i+2j=h(i)+h(j)$

故h满足同态公式；

于是, h是从(N,+)到(E,+)的同构函数, 即(N,+)和(E,+)同构。

同时有h^{-1}：$E \to N$, $h^{-1}(i)=i/2$ $(\forall i \in E)$；

显然h^{-1}是双射函数；

$\forall i,j \in E$ 有：

$$h^{-1}(i+j)=(i+j)/2=i/2+j/2=h^{-1}(i)+h^{-1}(j)$$

故h^{-1} 满足同态公式；

于是, h^{-1}是从(E,+)到(N,+)的同构函数, 即(E,+)和(N,+)同构。

离散数学

例10. $(R, +)$和$(R^+, \times)$同构

这里：R是实数集合，+是实数加法，（R, ＋）是代数系统；R^+是正实数集合，×是实数乘法，$(R^+, \times)$是代数系统；

这是两个同类型的代数系统，都只有一个二元运算；

取函数 h：$R \to R^+$，$h(\alpha)= e^{\alpha}$。

单射：$h(\alpha)= h(\beta) \Rightarrow e^{\alpha} = e^{\beta} \Rightarrow \ln e^{\alpha} = \ln e^{\beta} \Rightarrow \alpha= \beta$；

满射：对任何$c \in R^+$，由于$c>0$，故可取$\alpha=\ln c$，则

$h(\alpha)= e^{\alpha} = e^{\ln c} = c$；

故所以h是双射函数；

离散数学

$\forall \alpha,\beta \in R$ 有:

$$h(\alpha+\beta)=e^{\alpha+\beta}=e^{\alpha}\times e^{\beta}=h(\alpha)\times h(\beta)$$

故h满足同态公式;

由定义4知, h是从$(R,+)$到$(R^+,\times)$的同构函数，即$(R,+)$和$(R^+,\times)$同构。

同时有h^{-1}：　$R^+ \rightarrow R$, $h^{-1}(\alpha)=\ln\alpha$ 。

同理可证 h^{-1}是双射函数;

且$\forall \alpha$，$\beta \in R^+$ 有:

$$h^{-1}(\alpha\times\beta)=\ln(\alpha\times\beta)=\ln\alpha+\ln\beta=h^{-1}(\alpha)+h^{-1}(\beta)$$

故h^{-1}满足同态公式;

由定义4可知，h^{-1}是从$(R^+,\times)$到$(R,+)$的同构函数, 即$(R^+,\times)$和$(R,+)$同构。

离散数学

定理3. 代数系统间的同构关系≅是X上的等价关系。

其中：X={A:A是代数系统}。

[证].(以下都以仅含一个二元运算的代数系统为例)

由等价关系的定义知要证≅是

(1)自反的：这点可由幺函数来保证；

对于任何代数系统A=(X,*), 有幺函数

I:X →X 使得 ∀a∈X , I(a)=a 。

幺函数是双射函数；

∀a,b∈X ,I(a * b)=a*b=I(a)*I(b), 满足同态公式；

故I： A≅A ； 故A≅A 。

离散数学

(2)对称的：这点可由逆函数来保证；

对于任何两个代数系统A=(X,*)，B=(Y, Δ),

若有A≅B，则有同构函数h：A≅B 。

从而h：X→Y ；

h是双射函数；

h满足同态公式：∀a,b∈X ,h(a＊b)=h(a)Δh(b) ；

于是有逆函数h^{-1}存在 h^{-1} ： Y→X ；

h^{-1}是双射函数(参见第三章§1定理1)；

并且对任何元素c,d∈Y,都存在着a,b∈X ,使得h(a)=c，h(b)=d ，从而$h^{-1}(c)=a$，$h^{-1}(d)=b$，于是有

$h^{-1}(c\Delta d)$

$= h^{-1}(h(a)\Delta h(b))$

$= h^{-1}(h(a * b))$ （h满足同态公式）

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

$=I(a * b)$ （h^{-1}是h的逆函数）

$=a * b$

$= h^{-1}(c) * h^{-1}(d)$

所以h^{-1}满足同态公式；

所以h^{-1}：$B \cong A$；所以 $B \cong A$；

(3)传递的：这点可由复合函数来保证。

对于任何三个代数系统A=(X,*)，B=(Y, Δ), 以及C=(Z,♣), 若有$A \cong B$，且 $B \cong C$，则有同构函数：

h：$A \cong B$， g：$B \cong C$。

从而有函数h：$X \to Y$， g：$Y \to Z$，

h,g都是双射函数；

离散数学

h ,g都满足同态公式：

$\forall a,b\in X$,$h(a*b)=h(a)\Delta h(b)$

$\forall c,d\in Y$,$g(c\Delta d)=g(c)\clubsuit g(d)$ ；

于是有复合函数 goh： $X\to Z$，

goh是双射函数(参见第三章§2定理1)；

并且对任何元素$a,b\in X$,我们有

$(goh)(a*b)$

$= g(h(a*b))$

$= g(h(a)\Delta h(b))$ (h满足同态公式)

$= g(h(a))\clubsuit g(h(b))$ (g满足同态公式)

$=(goh)(a)\clubsuit(goh)(b)$

所以goh满足同态公式；

所以goh： $A\cong C$； 所以 $A\cong C$ 。

离散数学

§3.半群

- 半群的基本概念
- 交换半群与含幺半群
- 循环半群
- 子半群

§3.半群

定义1.半群(semigrop)

设(X, *)是代数系统，* 是X上的二元运算。若 *运算满足结合律，则称(X, *)为半群。

注：•半群就是具有结合律的代数系统；

•验证半群的要点是验证运算的(1)封闭性；(2)结合律。

例1. (I,×)是半群

这里：I 是整数集合， ×是整数乘法。

由 §1的例1. (1)我们已知(I,×)是代数系统；

由算术知识知整数乘法×满足结合律，即∀a, b, c∈I ，

(a×b)×c= a×(b×c) ；

由半群的定义知(I,×)是半群。

例2. $(M_{n\times n}, \times)$是半群

这里： $M_{n\times n}$是n 阶实(方)矩阵的全体， $\times$是矩阵乘法。

由线性代数知两个n阶实(方)矩阵相乘仍为n阶实(方)矩阵，且结果唯一，即 $\forall A,B$，

$$A\in M_{n\times n}\wedge B\in M_{n\times n}\Rightarrow A\times B\in M_{n\times n}$$

满足封闭性，故$\times$是$M_{n\times n}$上的二元运算；

由线性代数知矩阵乘法满足结合律即$\forall A, B, C\in M_{n\times n}$，

$(A\times B)\times C= A\times(B\times C)$ ；

由半群的定义知$(M_{n\times n}, \times)$是半群。

例3. $(N_m, \times_m)$是半群

这里： $N_m=\{[0]_m, [1]_m, \ldots, [m-1]_m\}$， $\times_m$定义如下

$\forall [i]_m, [j]_m \in N_m$，

$$[i]_m \times_m [j]_m = [(i \times j) \bmod m]_m$$

由于$0 \le (i \times j) \bmod m < m$，因此运算结果唯一，且$[(i \times j) \bmod m]_m \in N_m$，满足封闭性。故$\times_m$是$N_m$上的二元运算，通常称为$N_m$上的**模乘运算**；

由于$\forall [i]_m, [j]_m, [k]_m \in N_m$，有：

$$\begin{aligned}
&([i]_m \times_m [j]_m) \times_m [k]_m \\
&= [(i \times j) \bmod m]_m \times_m [k]_m \\
&= [((i \times j) \bmod m \times k) \bmod m]_m \\
&= [(i \times j \times k) \bmod m]_m
\end{aligned}$$

离散数学

$$
\begin{aligned}
&[\,i\,]_m \times_m ([\,j\,]_m \times_m [\,k\,]_m) \\
&= [\,i\,]_m \times_m [(j \times k) \bmod m]_m \\
&= [(i \times (j \times k) \bmod m) \bmod m]_m \\
&= [(i \times j \times k) \bmod m]_m
\end{aligned}
$$

故有：

$$([\,i\,]_m \times_m [\,j\,]_m) \times_m [\,k\,]_m = [\,i\,]_m \times_m ([\,j\,]_m \times_m [\,k\,]_m)$$

由结合律的定义知$\times_m$满足结合律；

由半群的定义知$(N_m, \times_m)$是半群。

例4. $(2^X, \cap)$是半群

这里： X 为非空集合，2^X是 X 的幂集， ∩是2^X上的集合交运算。

由第一章集合 § 2定义2(1)知，∩是2^X上的二元运算；

由第一章集合 § 2定理2(6)知， ∩满足结合律 ；

由半群的定义知$(2^X, \cap)$是半群。

例5. $(P[x], \times)$是半群

这里： $P[x]$ 是实系数多项式的全体， ×是多项式的乘法。

由于两个多项式之积仍为多项式，且结果唯一，故×是满足封闭性，故是$P[x]$上的二元运算；

由于实数乘法和加法分别满足结合律，故多项式乘法满足结合律，由半群的定义知$(P[x], \times)$是半群。

离散数学

例6. (X^X, o)是半群(参见§1例2)

这里：$X=\{a,b\}$，$X^X=\{f \mid f: X \to X\}=\Omega$，则

由§1例2我们已知(X^X, o)是代数系统；

由第三章函数§2.函数的复合知函数的复合运算o满足结合律；

由半群的定义知(X^X, o)是半群，这里

$\forall x \in X$，$(f_2 \circ f_3)(x)=f_2(f_3(x))$。

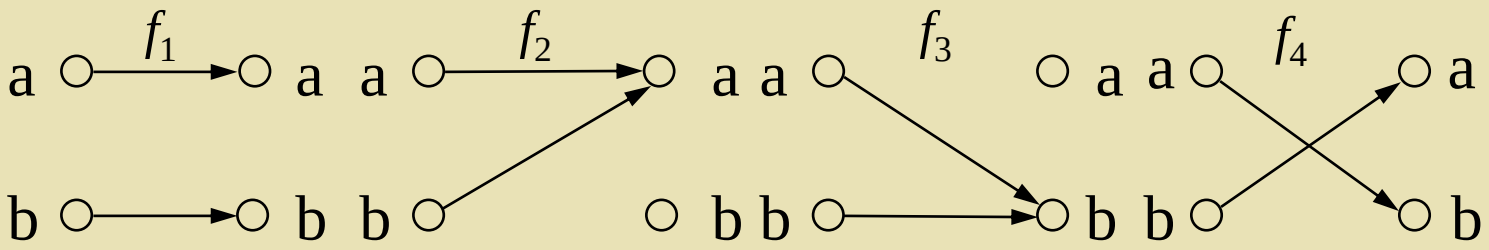

图1

离散数学

定义2. 交换半群 含幺半群

设(X，*)是半群。

(1)若*运算满足交换律，则称(X，*)是交换半群。

(2)若X关于*运算有幺元，则称(X，*)是含幺半群或者单子。

(3)若*运算满足交换律同时X关于*运算又有幺元，则称(X，*)是交换含幺半群或交换单子。

例7. 在前面所举的半群的例子中：

(1)(I，×)是交换含幺半群，幺元是1；

(2)($M_{n\times n}$，×)不是交换半群，但是是含幺半群，幺元是单位矩阵E；

(3)(N_m，$\times_m$)是交换含幺半群，幺元是$[1]_m$；

(4)(2^X，∩)是交换含幺半群，幺元是X；

(5)(P[x]，×)是交换含幺半群，幺元是1；

(6)(X^X，o)不是交换半群，但是含幺半群，幺元是幺函数 f_1 。

定义3.元素的乘幂

设(X，∗)是代数系统，∗是 X 上的二元运算。X 中元素的乘幂定义如下：∀x∈ X，

$x^1 = x$；

$x^{m+1} = x^m * x$ (m ∈ N)。

例9. 在代数系统(N，+)中，1∈N，于是有：

$1^1 = 1, 1^2 = 2, 1^3 = 1^2+1 = 2+1 = 3, \ldots, 1^n = n, \ldots$

例10. 在代数系统$(2^X, \cap)$中，$A \in 2^X$，于是有：

$A^1=A, A^2=A\cap A=A, A^3=A^2\cap A=A\cap A=A,\ldots,$

$A^n=A^{n-1}\cap A =A\cap A=A,\ldots$

离散数学

定理1. 指数律

设(X，*)是半群。任取 $x \in X$ ， $\forall m、n \in N$，有

(1)$x^m * x^n = x^{m+n} = x^n * x^m$;

(2)$(x^m)^n = x^{m\,n} = (x^n)^m$ 。

[证].采用归纳法

(1)固定m,选取n为归纳变元。

当n=1时，由定义3知有$x^m * x^1 = x^{m+1}$;

当n=k时，设有$x^m * x^k = x^{m+k}$;

当n=k+1时，有$x^m * x^{k+1} = x^m * (x^k * x)$ （定义3）

$= (x^m * x^k) * x$ （结合律）

$= x^{m+k} * x$ （归纳假设）

$= x^{m+(k+1)}$ （定义3）

故对任意的$m、n \in N$，有 $x^m * x^n = x^{m+n}$ 。

(2)当n=1时，由定义3知$(x^m)^1 = x^m = x^{m\times 1}$；

当n=k时，设有$(x^m)^k = x^{mk}$；

当n=k+1时，有$(x^m)^{k+1} = (x^m)^k * x^m$ （定义3）

$= x^{mk} * x^m$ （归纳假设）

$= x^{mk+m}$ （根据(1)）

$= x^{m(k+1)}$

故对任意的m、n∈N，有 $(x^m)^n = x^{mn}$ 。

定义4.循环半群(cyclic semigroup)

设(X，*)是半群。若存在着元素 $x_0 \in X$，使得

$(\forall x \in X)(\exists n \in N)(x = x_0^n)$

则称(X，*)为循环半群；同时称 x_0 是该循环半群的生成元(generating element)。

例11. 在$(N,+)$, $(N,\times)$, $(N_5,+_5)$这三个代数系统中：

(1)$(N,+)$ 是循环半群，生成元是1；

(2)$(N,\times)$不是循环半群，因为它无生成元；

(3)$(N_5,+_5)$是循环半群，其中$[1]_5$，$[2]_5$，$[3]_5$，$[4]_5$都是它的生成元，即$(N_5,+_5)$的生成元不唯一。

定理2. 循环半群一定是交换半群。

[证].设$(X,*)$是循环半群，生成元是$x_0\in X$。于是，

对任何元素$x, y\in X$,存在着自然数m，n∈N，使得$x=x_0^m$, $y=x_0^n$,从而

$$x*y=x_0^m*x_0^n$$
$$=x_0^n*x_0^m \qquad \text{(定理1的(1))}$$
$$=y*x$$

故*运算满足交换律；即$(X,*)$是交换半群。

离散数学

注：•定理2说明循环半群一定是交换半群；

•但是，交换半群未必都是循环半群。

例12. $(N_5, \times_5)$不是循环半群

取交换含幺半群$(N_5, \times_5)$(参见例7(3))，其幺元是$[1]_5$，其运算表见表1。由表1知$(N_5, \times_5)$确实是交换半群(因其运算表是对称的)。

但$(N_5, \times_5)$不是循环半群。因为N_5中的$[0]_5$无法表示成任何元素的乘幂。

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

表1

注：•这里，我们将$N_5=\{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$简化表示为本$N_5=\{0, 1, 2, 3, 4\}$。

离散数学

定义5.子半群(sub-semigroup)

设 (X，*)是半群，S⊆X且S≠∅。若(S，*)是(X，*)的子代数系统，并且(S，*)也构成半群,则称(S，*)是(X，*)的子半群。

注：•子半群的概念是子代数系统概念在半群这种代数系统中的具体体现。

•由本章§1的定理3知，若代数系统中的二元运算满足结合律，则子代数系统中的二元运算也满足结合律，因此**半群的子代数系统就是这个半群的子半群**。

•因此，验证子半群与验证子代数系统一样，必须验证条件：1°S⊆X； 2° S≠∅ ； 3°封闭性。

离散数学

- 第六章 代数系统
  前三节结束！