第三部分

代数结构

第七章 代数系统

7.1：代数运算的概念

- 定义7.1：设A是集合，函数 $f: A^n \to A$称为集合A上的n元代数运算，整数n称为运算的阶(Order)。

当n=1时，f:A→A称为集合A的一元运算；

当n=2时，f:A×A→A称为集合A中的二元运算。

- (1)一般，二元运算用算符 ∘,*,●,等符号，用中缀方式表示：$f(<a_1,a_2>)=a_3 \Rightarrow \circ(<a_1,a_2>)=a_3 \Rightarrow a_1 \circ a_2 = a_3$
- (2) $ran\ f \subseteq A$，即运算结果是A中的元素，称为运算的封闭性；
- (3)运算是函数，每一个自变元只有唯一的一个像。

7.1 代数运算的概念

- **例7-1：**

(1). $f: Z \to Z, \forall x \in Z, f(x) = -x;$

(2). $A = \{0,1\}, f: A \to A, \forall p \in A, f(p) = \neg p;$

(3). $f: R_{+} \to R_{+}, \forall x \in R_{+}, f(x) = \dfrac{1}{x};$

(4). $f: Z \times Z \to Z, \forall <x, y> \in Z^{2}, f(<x, y>) = x + y \setminus x - y \setminus x \times y;$

(5). $P(A)$为A的幂集。$f: P(A) \times P(A) \to P(A)$, f可为$\cup, \cap, -, \oplus;$

(6). $A = \{0,1\}, f: A \times A \to A$, f可为: $\wedge, \vee, \to, \leftrightarrow;$

(7). $A^{A} = \{f \mid f: A \to A\}$.($A$上所有函数的集合)

➢ **(4) 当A是有穷集合时，运算可以用运算表给出。**

7.2 代数运算的性质

- **定义7.2：设 $*,\circ$ 均为集合S上二元运算，**

(1)：若 $\forall x \forall y \forall z(x,y,z \in S \to x*(y*z)=(x*y)*z)$，则称“*”运算满足结合律；

(2)：若 $\forall x \forall y(x,y \in S \to x*y=y*x)$，则称“*”运算满足交换律；

(3)：若 $\forall x \forall y \forall z(x,y,z \in S \to x*(y\circ z)=(x*y)\circ(x*z))$，则称“*”运算对“∘”运算满足左分配律；若 $\forall x \forall y \forall z(x,y,z \in S \to (y\circ z)*x=(y*x)\circ(z*x))$，则称“*”运算对“∘”运算满足右分配律；若二者均成立，则称“*”运算对“∘”运算满足分配律；

(4)：设 $*,\circ$ 均可交换，若 $\forall x \forall y \in A$，有 $x*(x\circ y)=x, x\circ(x*y)=x$，则称“*”和“∘”运算满足吸收律；

(5)：若 $\forall x(x \in A, x*x=x)$，则称“*”运算满足幂等律。

7.2 代数运算的性质

- **例7-2：**（1）Z上的加，减，乘法是二元运算，且加法，乘法：结合律，交换律，乘法对加法，减法满足分配律，反之不满足；

（2）A的幂集P(A)上的二元运算：∪，∩满足交换律，结合律，吸收律，幂等律，且彼此之间满足分配律；

（3）设A={a，b}，A上的运算“*”和“o”满足如下运算表：

*	a	b
a	a	b
b	b	a

o	a	b
a	a	a
b	a	b

7.2 代数运算的性质

解：由运算表知：i)，*， o是可交换的；

ii)， *， o是可结合的；

iii)， o对*是可分配的；

iv)，*对o不可分配；

v)， *， o满足吸收律。

7.2 代数运算的性质

- **定义7.3：设*为集合S中的二元运算，如果存在 $e_r \in S(e_l \in S)$ 且对任意的元素 $x \in S$均有$x * e_r = x(e_l * x = x)$ 则称元素 $e_r(e_l)$ 为S中关于运算*的右幺元(左幺元)或右单位元(左单位元)。**
- **定理7.1：设*是集合S中的二元运算，且e_r与e_l分别是对于*的右幺元和左幺元，则 $e_r = e_l = e$，对任意元素$x \in S$有$x * e = e * x = x$，称元素e为关于运算*的幺元(Identity Elements)且唯一。**

证：$\because e_r$是$*$的右幺元 $\therefore e_l * e_r = e_l$， $\because e_l$是$*$的左幺元 $\therefore e_l * e_r = e_r$，

$\therefore e_r = e_l$，令$e = e_r = e_l$， 则有$x * e = e * x = x$，

设另有一幺元为右幺元e'，那么$e = e * e' = e'$

$\therefore e$对$*$是唯一的幺元。

7.2 代数运算的性质

- (1) 对于可交换的二元运算来说，左幺元都为右幺元，右幺元也为左幺元，即为幺元；
- (2) 幺元必须强调是针对某一个运算而言的。

- 例7-3：(1) R中的加法“+”运算：0是幺元；

(2) R中的乘法“×”运算：1是幺元；

(3) 全集E的子集的并“∪”运算：$\emptyset$是幺元；

(4) 全集E的子集的交“∩”运算：E是幺元；

(5) 命题集合中，析取“∨”运算：矛盾式是幺元；

(6) 命题集合中，合取“∧”运算：重言式是幺元；

(7) $A^A=\{f \mid f:A\to A\}$，A上的函数集合中，复合“∘”运算：I_A是幺元。

7.2 代数运算的性质

- **定义7.4：设*是S中的二元运算，如果存在** $\theta_r \in S(\theta_l \in S)$ **且对任意元素** $x \in S$ **均有** $x * \theta_r = \theta_r(\theta_l * x = \theta_l)$ **称元素** $\theta_r(\theta_l)$ **是S中关于运算*的右零元(左零元)。**
- **定理7.2：设*是S中的二元运算且** θ_r与θ_l **分别是对*的右零元和左零元，则** $\theta_r = \theta_l = \theta$ **，使对任意元素** $x \in S$, 有$x * \theta = \theta * x = \theta$ **，称元素**θ **是S中关于运算* 的零元(zero)且唯一。**

证： $\because \theta_r$是$*$的右零元 $\therefore \theta_l * \theta_r = \theta_r$， $\because \theta_l$是$*$的左零元

$\therefore \theta_l * \theta_r = \theta_l, \therefore \theta_r = \theta_l$，令$\theta = \theta_r = \theta_l$，则有$x * \theta = \theta * x = \theta$,

设另有一零元为右零元θ'，那么$\theta = \theta * \theta' = \theta'$

$\therefore \theta$对$*$是唯一的零元。

7.2 代数运算的性质

- 例7-4：(1)R中的加法“+”运算：无零元；

(2)R中的乘法“×”运算：0是零元；

(3)全集E的子集的并“∪”运算：E是零元；

(4)全集E的子集的交“∩”运算：$\emptyset$ 是零元；

(5)命题集合中，析取“∨”运算：重言式是零元；

(6)命题集合中，合取“∧”运算：矛盾式是零元；

(7)S={a，b，c}，S上的*运算的运算表如下：

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

则b是右零元，a是幺元。

7.2 代数运算的性质

- 定义7.5：设*是集合S中的二元运算，且S中对于*有e为幺元，x，y为S中元素，若x*y=e，那么称x为y的左逆元，y为x的右逆元，若x对于*运算既有左逆元又有右逆元，则称x是左，右可逆的，若x左右均可逆，则称x可逆。

➢ 显然，对于二元运算*，若*可交换，则任何左(右)可逆的元素均可逆。

- 定理7.3：设*是集合S中的一个可结合的二元运算，且S中对于*有e为幺元，若 $x \in S$ 是可逆的，则其左，右逆元相等，记为: x^{-1}，称为元素x对运算*的逆元(Inverse elements)且是唯一的。(x的逆元通常记为 x^{-1} ，但当运算为“加法运算”时，x的逆元可记为-x)。

7.2 代数运算的性质

证：设 x_r和x_l **分别是x对*运算的右逆元和左逆元，故有，** $x*x_r=x_l*x=e$**，由于*可结合，于是：**

$$x_l=x_l*e=x_l*(x*x_r)=(x_l*x)*x_r=e*x_r=x_r$$

假设 x_1^{-1},x_2^{-1}**均是x的逆元，则**

$$x_1^{-1}=x_1^{-1}*e=x_1^{-1}*(x*x_2^{-1})=(x_1^{-1}*x)*x_2^{-1}=e*x_2^{-1}=x_2^{-1}$$

$\therefore x^{-1}$唯一，即$x^{-1}*x=x*x^{-1}=e$

7.2 代数运算的性质

- 定理7.4：设*是集合S中的一个可结合的二元运算，且e为S中对于*的幺元，x有逆元 x^{-1}，则 $(x^{-1})^{-1}=x$

证：$(x^{-1})^{-1}=(x^{-1})^{-1}*e=(x^{-1})^{-1}*(x^{-1}*x)$

$=((x^{-1})^{-1}*x^{-1})*x=e*x=x$

➢ (1) $e^{-1}=e$；（2）并非每个元素均可逆。

- 例7-5：（1）N上的：“×”运算，只有1有逆元，“+”运算，只有0有逆元，总之，任何代数结构其幺元恒有逆元，为其自身；

(2) Z上，每个元素有“加法”逆元，只有1有“乘法”逆元；

(3) Q上，每个元素有“加法”逆元，除0外的每个元素有“乘法”逆元。

7.2 代数运算的性质

(4) P(A) 中，∪运算，幺元为 $\emptyset$，每个元素 $(B\neq\emptyset)$ 均无逆元，∩运算，幺元为A，每个元素 $(B\neq A)$ 均无逆元；

(5) 在集合 $A^A=\{f\mid f:A\to A\}$ 中，$\circ$ 为复合运算，I_A 为幺元，A中所有双射函数有逆元，所有单射函数有左逆元，所有满射函数有右逆元。

- **定理7.5：设*是S上的二元运算，e为幺元，θ为零元，并且|S|≥2，那么θ无左(右)逆元。**

证：先证 $\theta\neq e$，否则 $\theta=e$，则 S 中另有元素 a，a 不是幺元和零元，从而 $\theta=\theta*a=e*a=a$，与 a 不是零元矛盾 $\therefore\theta\neq e$。

再用反证法证 θ 无左(右逆元)，设 θ 的左(右逆元)为 x，那么

$\theta=x*\theta=e\quad(\theta=\theta*x=e)$，与 $\theta\neq e$ 矛盾，$\therefore$ 得证。

7.2 代数运算的性质

- (1) 左，右幺元，幺元，左，右零元，零元都是常元，依赖于运算；
- (2) 而逆元是对某个元素而言的，不是常元，不仅依赖于运算，而且依赖于是哪个元素的逆元。

- **定义7.6：** 设*是集合S中的二元运算，$a \in S, a \neq \theta$ 如果a满足，对任意 $x, y \in S$，均有：

$$a * x = a * y \Rightarrow x = y \qquad (1)$$

$$x * a = y * a \Rightarrow x = y \qquad (2)$$

则称元素a对*是可约(可消去)的(Cancelable)，当a满足(1)式，称a是左可约的，当a满足(2)式时，称a是右可约的。特别地，若对 $\forall x, y, z \in S$ 有

$$(x * y = x * z) \wedge x \neq \theta \Rightarrow y = z \quad (y * x = z * x) \wedge x \neq \theta \Rightarrow y = z$$

则称运算*满足消去律(可约律)。

7.2 代数运算的性质

- **定理7.6：若*是S中满足结合律的二元运算，且元素a有逆元(左，右逆元)，则a必定是可约的。**

证：设a的逆元为a^{-1}，对任意$x, y \in S$，设$a*x=a*y$可得

$a^{-1}*(a*x)=a^{-1}*(a*y) \quad \therefore x=y$

设$x*a=y*a$可得$(x*a)*a^{-1}=(y*a)*a^{-1} \quad \therefore x=y$

$\therefore a$是可约的

- **S是有穷集合时，二元运算可以用运算表给出，对应的运算性质也可从表中直接看出：**

(1)二元运算满足可交换性的充要条件是运算表关于主对角线对称；

(2)二元运算满足幂等性的充要条件是运算表上每个元素与它所在的行，列的表头元素相同；

7.2 代数运算的性质

(3) 二元运算有幺元的充要条件是该元素对应的依次与该表表头的行，列一致；

(4) 二元运算有零元的充要条件是该元素对应的行和列元素均与该元素相同；

(5) 二元运算中a与b互为逆元素的充要条件是运算表中位于a所在的行，b所在列的元素及b所在的行，a所在的列的元素都是幺元。

- **例7-6：** N_4是整数中模4同余产生的等价类集合，N_4 ={[0], [1], [2], [3]}，N_4上的运算$+_4, \times_4$定义为：

$$[m]+_4[n]=[(m+n)\bmod 4] \quad [m]\times_4[n]=[(m\times n)\bmod 4]$$

7.2 代数运算的性质

即：

$+_4$	**[0]**	**[1]**	**[2]**	**[3]**
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\times_4$	**[0]**	**[1]**	**[2]**	**[3]**
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

解：由表知：

$+_4$：**可交换（√），幂等（×），幺元（√ : [0]），零元（×），逆元（**$[0]^{-1}=[0],[2]^{-1}=[2],[1]^{-1}=[3]$**）**

$\times_4$：**可交换（√），幂等（×），幺元（√ : [1]），零元（√ : [0]），逆元（**$[1]^{-1}=[1],[3]^{-1}=[3]$**，[0]，[2]无逆元）**

7.3 代数系统

- **定义7.7：** 非空集合S和S上的k个一元或二元运算 $f_1, f_2, \cdots, f_k$ 组成的系统称为一个代数系统，记作 $< S, f_1, f_2, \cdots, f_k >$

例：(1)<N, +>，<Z, +, ×>，<R, +, ×>，<P(A), ∪, ∩, ~>都是代数系统；

(2)<N, −>，<Z, ÷>，<R, ÷>不是代数系统。

- **定义7.8：** 如果两个代数系统中运算的个数相同，对应的阶数相同，且代数常数的个数相同，则称这两个代数系统具有相同的构成成分，也称它们是同类型的代数系统。

例：$< P(A), \cup, \cap, \sim, A, \emptyset >$ 与 $< R, +, \times, -, 0, 1 >$ 同类型。

7.3 代数系统

- 定义7.9：设*是S上的n元运算(n=1, 2, ···)，$T \subseteq S$ 如果对任意元素 $x_1, x_2, \cdots, x_n \in T, *(x_1, x_2, \cdots, x_n) \in T$ 称*运算对T封闭(Closed)。

例：N上的加法运算对非负偶集封闭，而对非负奇数集不封闭。

- 定义7.10：设<S, *>是代数系统，如果有非空集合T满足：(1) $T \subseteq S$，(2) 运算*对T封闭；则称<T, *>为代数系统<S, *>的子代数系统，或子代数(Sub algebra)。

7.3 代数系统

- (1) 子代数仍是一个代数系统，*运算所满足的性质在子代数中仍满足；
- (2) T是S的子集，S中关于*运算的特殊元素，在T中未必有；
- (3) <S, *>为<S, *>的平凡子代数，若S中含有幺元e，<{e}, *>也叫做<S, *, e>的平凡子代数，若 $T \subset S$，则<T, *>为<S, *>的真子代数。

例：对<N, +>而言，设E为非负偶数集，则<E, +>为其子代数，<N, +>，<{0}, +>为其平凡子代数。

7.4 代数系统的同态与同构

- **定义7.11：**设<S,*>及<T,∘>均为代数系统，如果函数f:S→T对S中任何元素a，b有f(a*b)=f(a)∘f(b)则称函数f为(S到T的)同态映射，或同态(homomorphism)，当同态f为单射时，又称f为单一同态，同态f为满射时，又称f为满同态，同态f为双射时，又称f为同构映射，或同构(isomorphism)。

当<S,*>和<T,*>间存在同构映射时，称<S,*>，<T,*>同构，记为S≌T，当f为<S,*>到<S,*>的同态(同构)时，称f为S的自同态(自同构)。

f(a*b)=f(a)∘f(b)为同态f的同态方程。

7.4 代数系统的同态与同构

- **例7-7：** (1) 设f :R→R；$f(x)=e^x$，则f为<R, +>到<R, •>的单一同态，$\forall x\forall y\in R, f(x+y)=e^{x+y}=e^x\cdot e^y=f(x)\cdot f(y)$

若 $f:R\to R_+$，$f(x)=e^x$，则f为<R, +>到<R_+, •>的同构映射，即<R, +>与<R_+, •>同构；

(2) 设h:R→R，h(x)=2x，则h为<R, +>到<R, +>的自同态，$\because \forall x\forall y$，有$h(x+y)=2(x+y)=2x+2y=h(x)+h(y)$

h为R的自同构；

(3) 设A={a, b, c, d}, B={0, 1, 2, 3}, *，$+_4$ 定义如下：

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

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

7.4 代数系统的同态与同构

证明<A, *>与<B, $+_4$>同构。

证：设f:A→B，f(a)=0，f(b)=1，f(c)=2，f(d)=3
显然f是双射，*，$+_4$ 均是可交换的。

f(a*b)=f(b)=1　　f(a) $+_4$f(b)=0 $+_4$ 1=1

f(a*c)=f(c)=2　　f(a) $+_4$f(c)=0 $+_4$ 2=2

……

f(d*d)=f(c)=2　　f(d) $+_4$f(d)=3 $+_4$ 3=2

∴f是<A, *>到<B, $+_4$>的同构。

7.4 代数系统的同态与同构

- 定义7.12：设f为代数系统<S,*>到<T,ο>的同态映射，那么称f(S)为f的同态像(image under homomorphism)。
- 定理7.10：设f为代数系统<S,*>到<T,ο>的同态，那么同态像f(S)与ο构成<T,ο>的一个子代数

证明：只要证f(S)对运算ο封闭即可。

设a',b'为f(S)中任意两个元素，且f(a)=a'，f(b)=b'

则$a' \circ b' = f(a) \circ f(b) = f(a*b) \in f(S)$

∴f(S)对ο封闭，<f(S),ο>为<T,ο>的子代数。

7.4 代数系统的同态与同构

- 定理7.11：设f是代数系统<S, *>到<T, ο>(*, ο为二元运算)的满同态，那么

(1) 当运算*满足结合律，交换律时，T中运算ο也满足结合律，交换律；

(2) 如果<S, *>关于*有幺元e，那f(e)是<T, ο>中关于ο的幺元；

(3) 如果 x^{-1} 是<S, *>中元素x关于*的逆元，那么 $f(x^{-1})=(f(x))^{-1}$ 是<T, ο>中元素f(x)关于ο的逆元

(4) 如果<S, *>关于*有零元θ，那f(θ)是<T, ο>中关于ο的零元；

(5) 如果a是S中关于*的幂等元，那f(a)是<T, ο>中关于ο的幂等元；

7.4 代数系统的同态与同构

(6)如果a是S中关于*的(左，右)可约的，那f(a)是<T, o >中关于 o 的(左，右)可约的。

- (1)定理中满同态是必要条件，性质只在同态像上有效；
- (2)对于具有多个代数运算的两个同类型系统，同态是指相应的n个同态方程均成立；
- (3)同构映射是双射，所以不仅保持性质而且可逆，此时两个代数系统可视为一个，只是运算，元素符号不同。

- **定义7.13：** 如果f是代数系统<S, *>到<T, o >的同态，并且T中有幺元 e'，那么称下列集合为同态f的核(Kernel homomorphism)，记为K(f)。

$$K(f)=\{x \mid x \in S \wedge f(x)=e'\}$$

7.4 代数系统的同态与同构

- 定理7.12：设f是代数系统<S,*>到<T, o >的同态，如果$K(f)\neq\emptyset$，那么<K(f),*>为<S,*>的子代数

证：只要证明K(f)对*运算封闭即可。设K(f)中任意元素x，y，于是$f(x)=f(y)=e'$，考虑

$$f(x*y)=f(x)\circ f(y)=e'\circ e'=e' \quad \therefore x*y\in K(f)$$

那<K(f),*>为<S,*>的子代数。

➢ 一个同态映射f可导致两个子代数：<T, o >:<f(S), o >；<S,*>:<K(f),*>。