离散数学 II Discrete Mathematics II

封筠

fengjun@stdu.edu.cn

20-11



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。它是近 世代数研究对象,是研究各种数学分支 与许多实际问题的重要理论基础。它在 计算机科学中有着广泛的应用。



代数系统

代数系统通常包括半群、群、环、域、格和布尔代数等不同代数结构的内容。起源与发展(两位怀才不遇的天才数学家):

- 法国的伽罗瓦(Evariste Galois)
- 挪威的阿贝尔(Abel)



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。
- 在计算机科学中,如程序理论与数据结构以及编码理论等都有着广泛的应用。



第五章 代数结构

- 本章主要讨论群、环和域等代数系统。
- 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解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。 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。

第五章 学时安排(14学时,共7讲)

学时	教学内容
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 群与子群
2	5-5 阿贝尔群和循环群
2	5-7 陪集与拉格朗日定理
2	5-8 同态与同构 (上)
2	5-8 同态与同构 (下)
	5-9 环与域

5-1 代数系统的引入

本节要熟悉下列概念(3个):

集合A上的n元运算、

n元运算在集合A上封闭、

代数系统 (代数结构)

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: $f_4: \mathbb{R}^2 \to \mathbb{R}$ $f_5: a, b \to a \bullet b, \quad a, b \in \mathbb{R}$

三元运算: f_6 : 三种颜色 \rightarrow 三种颜色混合色 $A\rightarrow A$ 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。

不封闭运算举例: 自动售货机

*	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



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An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。

例题 设 $A=\{1, 2, 3, 4\}$,定义A上的二元运算如下:

$$x \circ y = (x \cdot y) \mod 5, \forall x, y \in A$$

求。的运算表。

解 运算表如下所示,可知该运算是封闭的。

0	1	2	3	4	
1	1	2	3	4	
2	2	4	1	3	
3	3	1	4	2	
4	4	3	2	1	

练习: 178页(1)

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 $f_1, f_2, ..., f_k$ 所组成的系统称为一个代数系统(代数结构),记为<A, $f_1, f_2, ..., f_k >$ 。

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A, 称为代数结构的载体。
- (2) 载体A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<A,*, Δ ,…>来表示,其中 A是载体,*, Δ ,…为各种运算。有时为了强调A有某些地位特殊的元素,也可将它们列入这种多元序组的末尾。

代数系统举例:
$$< I_+, +>$$
 $< \wp(S), \cup, \cap, \sim>$

虽然一些代数系统具有不同的形式,但是它们之间可能存在一些共同的运算规律。

例如:代数系统 $< I_+, +>$ 具有以下三个运算规律(对于任意的 $x, y, z \in I_+$):

$$(1) x + y \in I_{+}$$
 (封闭性)

(2)
$$x + y = y + x$$
 (交換律)

(3)
$$(x + y) + z = x + (y + z)$$
 (结合律)

与 $< I_+, +>$ 具有相同运算规律的代数系统如P177 表5-1.2。

表	5_1	. 2	
700			

	$\langle I, \cdot \rangle$	⟨R, +⟩	$\langle \mathscr{S}(S), \; U \rangle$	⟨ ୬ ⟨Ṣ⟩, ⋂⟩
集合	I 为整数集合	R为实数集合	9(8)是8的幂集	9(S)是S的幂集
运算	• 为普通乘法	+为普通加法	U 为集合的"并"	∩ 为集合的"交"
封闭性	$x \cdot y \in I$	$x+y\in R$	$A \cup B \in \mathscr{F}(\mathcal{S})$	$A \cap B \in \mathscr{P}(S)$
交換律	$x \cdot y = y \cdot x$	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 + > > < $\wp(S)$ \cap > \circ

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 (如封闭性、交换律、结合律)。本节将 着重讨论一般二元运算的一些性质。 ●学习本节要熟悉如下术语(15个): 封闭的、可交换的、可结合的、可分配的、 吸收律、等幂的、 左幺元、 右幺元、 幺元、 左零元、 右零元、 零元、左逆元、 右逆元、 逆元

●要求:

掌握4个定理

一、二元运算的性质

1、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 $A=\{x|x=2^n,n\in\mathbb{N}\}$,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 $2+2^2 = 6 \notin A$ 。

2、交换律

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 $x,y \in A$,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, \triangle 是Q上的二元运算,对任意的 $a,b \in Q$, $a \triangle b = a + b - a b$,问运算 \triangle 是否可交换。

解因为

a △ b=a+b-a b=b+a-b a=b △ a 所以运算 △ 是可交换的。

3、结合律

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∈A,有a★b=b,证明★是可结合运算。

4、分配律

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 $x,y,z\in A$,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A是可分配的。

例如幂集 ℘(S)上的∪和∩运算是互相可 分配的。 例题4 设集合 $A=\{\alpha,\beta\}$,在A上定义两个二元运算*和 \triangle 如下表所示。问运算 \triangle 对于运算*可分配吗?运算*对于运算 \triangle 可分配吗?

*	α	β
α	α	β
β	β	α

Δ	α	β
α	α	α
β	α	β

解验证运算△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
$$\alpha \triangle (\alpha^*\alpha) = (\alpha \triangle \alpha)^* (\alpha \triangle \alpha)$$

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

$$\alpha\triangle(\alpha^*\alpha) = \alpha\triangle\alpha = \alpha \qquad (\alpha\triangle\alpha)^*(\alpha\triangle\alpha) = \alpha^*\alpha = \alpha$$

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

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

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

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

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

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

但是运算*对于运算△是不可分配的。 因为:

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

而

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

5、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。

例如幂集 ℘(S)上的 ∪ 和 ∩ 运算满足吸收 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∈N,有

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

$$x \neq y = min(x,y)$$

验证运算*和★的吸收律。

解 对于任意a,b∈N

$$a*(a \bigstar b)=max(a,min(a,b))=a$$

 $a \bigstar (a*b)=min(a,max(a,b))=a$

因此,*和★满足吸收律。

6、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 ℘(S)是集合S的幂集,在 ℘(S)上定义的两个二元运算,集合的"并"运算∪和集合的"交"运算∩,验证是∪、∩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。

但 \oplus 不符合等幂律。 因为 若 $A \neq \phi$,则 $A \oplus A \neq A$

运算律小结

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 $\forall x \forall y \forall z (x,y,z \in A \rightarrow x*(y \Delta z) = (x*y) \Delta (x*z),$ $(y \Delta z)*x = (y*x) \Delta (z*x))$,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∈A \rightarrow x*x=x),则称*满足等幂律。

二、二元运算的特异元素

1、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∃e \forall x(e,x∈A→e*x=x*e=x),则称e为A中的 幺元。 例题7 设集合 $S=\{\alpha, \beta, \gamma, \delta\}$,在S上定义的两个二元运算*和★ 如下表所示。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

解由上表可知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。 39 例如,在幂集 $\wp(S)$ 上, ∪运算的幺元是 \varnothing , ∩运算的幺元是S。

对于给定的集合和运算有的存在幺元,有的不存在幺元。

例如, \mathbf{R}^* 是非零实数集, Δ 是 \mathbf{R}^* 上的二元运算, $\forall \mathbf{a}, \mathbf{b} \in \mathbf{R}^*$,有a $\Delta \mathbf{b} = \mathbf{a}$,则不存在 $\mathbf{e}_{\mathbf{l}}$ 使得对所有的 $\mathbf{b} \in \mathbf{R}^*$ 都有 $\mathbf{e}_{\mathbf{l}}\Delta \mathbf{b} = \mathbf{b}$,所以,运算 Δ 没有左幺元。但对 $\forall \mathbf{a} \in \mathbf{R}^*$,对所有 $\mathbf{b} \in \mathbf{R}^*$ 都有 $\mathbf{b} \Delta \mathbf{a} = \mathbf{b}$,所以任意 \mathbf{R}^* 的元素a都是运算 Δ 的右幺元。 \mathbf{R}^* 有无数个右幺元,但没有左幺元及幺元。

定理5-2.1 代数结构<A,*>同时有关于*运算的左幺元 e_l 和右幺元 e_r ,则满足 $e_l=e_r=e$,且所含幺元e是唯一的。

□ 证明: 先证左幺元e_l=右幺元e_r=e

2、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6 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, 为右零元。

如果θ∈A且对任意x∈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)。

42

例题8 设集合S={浅色,深色},定义在S上的一个二元运算*如下表所示。试指出零元和幺元。

*	浅色	深色
浅色	浅色	深色
深色	深色	深色

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。

例如,在幂集 $\wp(S)$ 上, ∪运算的零元是 S , ∩运算的零元是∅。

对于给定的集合和运算有的存在零元,有的不存在零元。

例如,R*是非零实数集, Δ 是R*上的二元运算, $\forall a,b \in R*$,满足a $\Delta b=a$,则R*的任何元素都是关于 Δ 的左零元,R*中没有右零元,也没有零元。

定理5-2.2 代数结构<A,*>同时有关于*运算的左零元 θ_l 和右零元 θ_r ,则满足 θ_l = θ_r = θ ,且其所含零元是唯一的。

□ 证明: 先证左零元 θ_l =右零元 θ_r = θ $\theta_l = \theta_l * \theta_r = \theta$ 再证零元 θ 是唯一的
设还有一个零元 $\theta' \in A$,则

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1,则 $\theta \neq e$ 。

□ 证明:用反证法:

反设幺元e =零元 θ ,则对于任意 $x \in A$,必有

$$\mathbf{x} = \mathbf{e} * \mathbf{x} = \mathbf{\theta} * \mathbf{x} = \mathbf{\theta} = \mathbf{e}$$

于是,推出A中所有元素都是相同的,矛盾。

3、逆元

定义5-2.9 设代数结构<A,*,e>中*为二元运算,e为幺元,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。

例如,在整数集Z中,加法幺元为0,对任何整数x,它的加法逆元都存在,即它的相反数-x。因为x+(-x)=0,(-x)+x=0,而非负整数集关于加法运算只有0有逆元0,其他正整数都无加法逆元。

对于给定的集合和二元运算来说,逆元和幺元、零元不同。如果幺元和零元存在,一定是唯一的,而逆元是与集合中的某个元素相关的,有的元素有逆元,有的元素没有逆元,不同的元素则对应着不同的逆元。

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。

例题9 设集合 $S=\{\alpha,\beta,\gamma,\delta,\xi\}$,定义在S上的一个二元运算*如下表所示。试指出代数系统 < S,*>中各个元素的左、右逆元情况。

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

解 先找出幺元,再根据幺元所在的行和列找出左、右逆元。 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,若A中每个元素x有左逆元l,则任何元素x存在右逆元r,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: $e=c*b=c*(\underline{(b*a)*b})$ = (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b₁和b₂,则有

$$\mathbf{b}_{1} = \mathbf{b}_{1} * \mathbf{e} = \mathbf{b}_{1} * \underline{(\mathbf{a} * \mathbf{b}_{2})}$$

$$= \underline{(\mathbf{b}_{1} * \mathbf{a})} * \mathbf{b}_{2}$$

$$= \mathbf{e} * \mathbf{b}_{2} = \mathbf{b}_{2}$$

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 \leq x \leq 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,·>, 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 $N_k=\{0,1,2,...,k-1\}$, $+_k$ 是定义在 N_k 上的模k加法运算,定义如下: 对于任意 $x,y\in N_k$

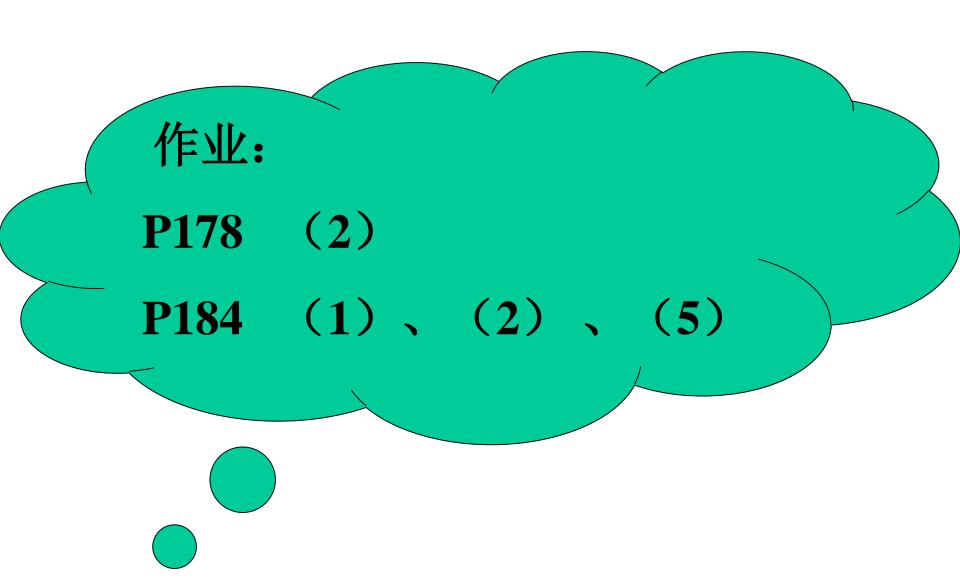
$$x +_k y = \begin{cases} x+y & \text{若}x+y < k \\ x+_k y = \begin{cases} x+y-k & \text{若}x+y \geqslant k \\ \text{试问是否每个元素都有逆元。} \end{cases}$$

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。

4、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。



The End