Semigroup and Groups

9.1 二元运算/Binary Operations Revisited

9.2 半群/Semigroups

9.3 乘积半群与商半群/Products and Quotients of Semigroups

9.4 群Groups

9.5 乘积群与商群Products and Quotients of Groups

Mathematical Structures

Mathematical structure（数学结构）

- A collection of objects with operations defined on them and the accompanying properties form a mathematical structure or system.
- 具有某些运算性质的对象的集合构成了一个数学结构或系统（S，$*_1$，$*_2$，…）。

Example 1

- The collection of sets with the operations of union, intersection, and complement and their accompanying properties is a (discrete) mathematical structure. We denote this structure by [sets, $\cup$, $\cap$, $\overline{}$].

Example 2

- The collection of 3×3 matrices with the operations of addition, multiplication, and transpose is a mathematical structure denoted by [3×3 matrices, $+$, $*$, ^{T}].

Closure（封闭）

- A structure is closed with respect to an operation if that operation always produces another member of the collection of objects.

Examples

- The structure [5×5 matrices, $+$, $*$, ^{T}] is closed with respect to addition because the sum of two 5×5 matrices is another 5×5 matrix.
- 矩阵结构+, $*$, ^{T}--封闭
- The structure [odd integers, $+$, $*$] is not closed with respect to addition.
  - The sum of two odd integers is an even integer.
  - This structure does have the closure property for multiplication, since the product of two odd numbers is an odd number.
  - 奇整数，+， 不封闭
  - 奇整数， $*$， 封闭

Binary operation（二元运算）

- An operation that combines two objects is a binary operation.（结合2个对象的是二元运算）
- An operation that requires only one object is a unary operation.（一元运算）
- Binary operations often have similar properties, as we have seen earlier.
- Example
  - (a) Set intersection is a binary operation since it combines two sets to produce a new set.
  - Producing the transpose of matrix is a unary operation.
  - 集合转置——一元运算
  - 集合交并补，整数+，-，＊二元运算

Commutative （交换律）

Common properties have been given names.

For example, if the order of the objects does not affect the outcome of a binary operation, we say that the operation is commutative.

That is, if $x \square y = y \square x$, where □ is some binary operation, □ is commutative .

Commutative （交换律）

Example

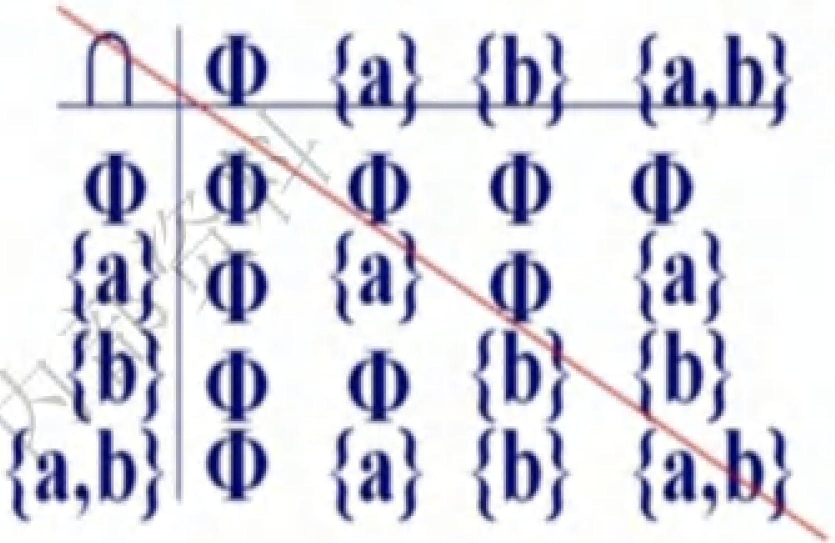
(a) Join and meet for Boolean matrices are commutative operations（布尔矩阵的并和交运算）.

$\boldsymbol{A} \vee \boldsymbol{B} = \boldsymbol{B} \vee \boldsymbol{A}$ and $\boldsymbol{A} \wedge \boldsymbol{B} = \boldsymbol{B} \wedge \boldsymbol{A}$.

(b) Ordinary matrix multiplication is not a commutative operation（普通矩阵的乘积运算）

$\boldsymbol{A} * \boldsymbol{B} \neq \boldsymbol{B} * \boldsymbol{A}$.

(c)集合的交运算



∩	Φ	{a}	{b}	{a,b}
Φ	Φ	Φ	Φ	Φ
{a}	Φ	{a}	Φ	{a}
{b}	Φ	Φ	{b}	{b}
{a,b}	Φ	{a}	{b}	{a,b}

Note

- An operation has a property means the statement of the property is true when the operation is used with any objects in the structure.
  - If there is even one case when the statement is not true, the operation does not have that property.

一个运算具有某种性质是指该结构中的任何对象做该运算时命题为真，否则如果存在一个对象做该运算后命题为假，则该运算不具有该性质。

Associative（结合律）

If □ is a binary operation, then □ is associative or has the associative property

$(x \square y) \square z= x \square (y \square z)$

设□是A上的二元运算，如果任意x,y,z∈*A*,都有
则称□在A上是可结合的

Associative（结合律）

- Example
  - Set union is an associative operation, since (A ∪ B) ∪ C = A ∪(B ∪ C) is always true.

结合律

若□ 是可结合的运算，元素x 的□运算，通常可以写成乘幂的形式。如下：

$x \square x = x^2$ ，$x^2 \square x = x^3$

$x^m \square x^n = x^{m+n}$

比如： 对于加法 $1+1+1 = 1^3$

对于乘法 $1*1*1 = 1^3$

Distributive property（分配律）

- If a mathematical structure has two binary operations, say □and ∇, a distributive property has the following pattern:

$$x \ \square \ (y \nabla z) = (x \ \square \ y) \nabla (x \ \square \ z).$$

$$(y \nabla z) \ \square \ x = (y \ \square \ x) \nabla (z \ \square \ x).$$

— □ 对 ∇ 可分配

- Example
  - (a) 实数的乘法对加法可分配

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

  - (b) The structure [sets, ∪, ∩, ¯] has two distributive properties: $\boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C}) = (\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C})$ and $\boldsymbol{A} \cap (\boldsymbol{B} \cup \boldsymbol{C}) = (\boldsymbol{A} \cap \boldsymbol{B}) \cup (\boldsymbol{A} \cap \boldsymbol{C})$.

De Morgan’s laws（德.摩根定理）

- Several of the structures we have seen have a unary operation and two binary operations.
- 一元运算 为 ∗ , 二元运算为 □和 ∇. 则 De Morgan ‘s laws 为

  $(x \square y)^{*} = x^{*} \nabla y^{*}$ and $(x \nabla y)^{*} = x^{*} \square y^{*}$.
- Example 9
  - (a) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ and $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.
  - (b) The structure [real numbers, +, $*$, $\sqrt{\ }$] does not satisfy De Morgan's laws. since $\sqrt{x+y} \neq \sqrt{x} * \sqrt{y}$

Identity for an operation（单位元）

- A structure with a binary operation □ may contain a distinguished object *e*, with the property $x \square e = e \square x = x$ for all *x* in the collection.
  - We call *e* an identity（单位元或幺元） for □.
  - an identity for an operation must be unique（单位元唯一）.

Theorem 1

- If e is an identity for a binary operation □, then e is unique.
- Proof （反证法证明单位元唯一）
  - Assume another object i also has the identity property, so $x \square i = i \square x = x$.
  - Then $e \square i = e$, but since e is an identity for □, $i \square e = e \square i = i$.
  - Thus, $i = e$.
  - There is at most one object with the identity property for □.

Example 10

- For [$n \times n$ matrices, +, $*$, ^{T}] ,$\mathbf{I}_n$ is the identity for matrix multiplication and the $n \times n$ zero matrix is the identity for matrix addition.
- 矩阵乘法单位元 为 单位矩阵$\boldsymbol{I}_n$。
- 矩阵加法单位元 为 零矩阵。

Inverse（逆元）

- If a binary operation □ has an identity *e*, we say *y* is a □ -inverse of *x* if
- *x* □ *y*=*y* □ *x*=*e* ， x和y互为逆元

Theorem 2 --（逆元唯一性）

-

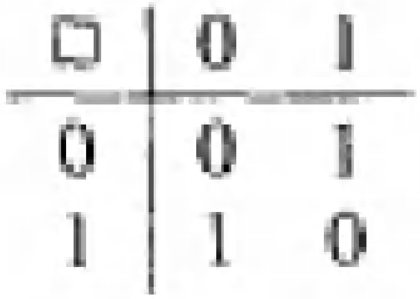
- If □ is an associative operation and x has a □-inverse y, then y is unique.
- Proof
  - Assume there is another □ -inverse for x, say z.
  - Then $(z \square x) \square y = e \square y = y$
  - and $z \square (x \square y) = z \square e = z$.
  - Since □ is associative, $(z \square x) \square y = z \square (x \square y)$ and so $y=z$.

Example 11

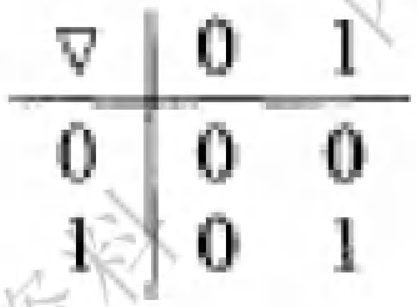
- (a) In the structure [3 × 3 matrices, +, *,^{T}] each matrix $A = [\ a_{ij}\ ]$ has a +-inverse, or additive inverse, $-A = [\ -a_{ij}\ ]$. (每个矩阵A = [a_{ij}] 有一个矩阵加法逆, $-A$ = [- a_{ij}].)
- (b) In the structure [integers, +, *], only the integers l and -l have multiplicative inverses. (结构中, 只有1和-1有乘法逆).

Example 12

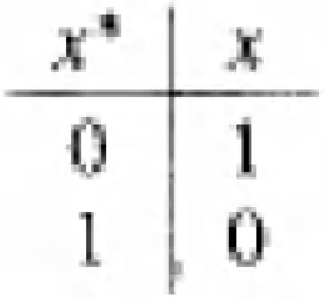
- Let □ ,∇ and ∗ be defined for the set {0, l} by the following tables.



□	0	1
0	0	1
1	1	0



∇	0	1
0	0	0
1	0	1



x^*	x
0	1
1	0

Thus 1 □ 0 = l, 0 ∇ 1 = 0, and 1 ∗ = 0. Determine if each of the following is true for [{0, l}, □, ∇, ∗].

(a) □ is commutative.

(b) ∇ is associative.

(c) De Morgan's laws hold.

(d) Two distributive properties hold for the structure.

Example 12

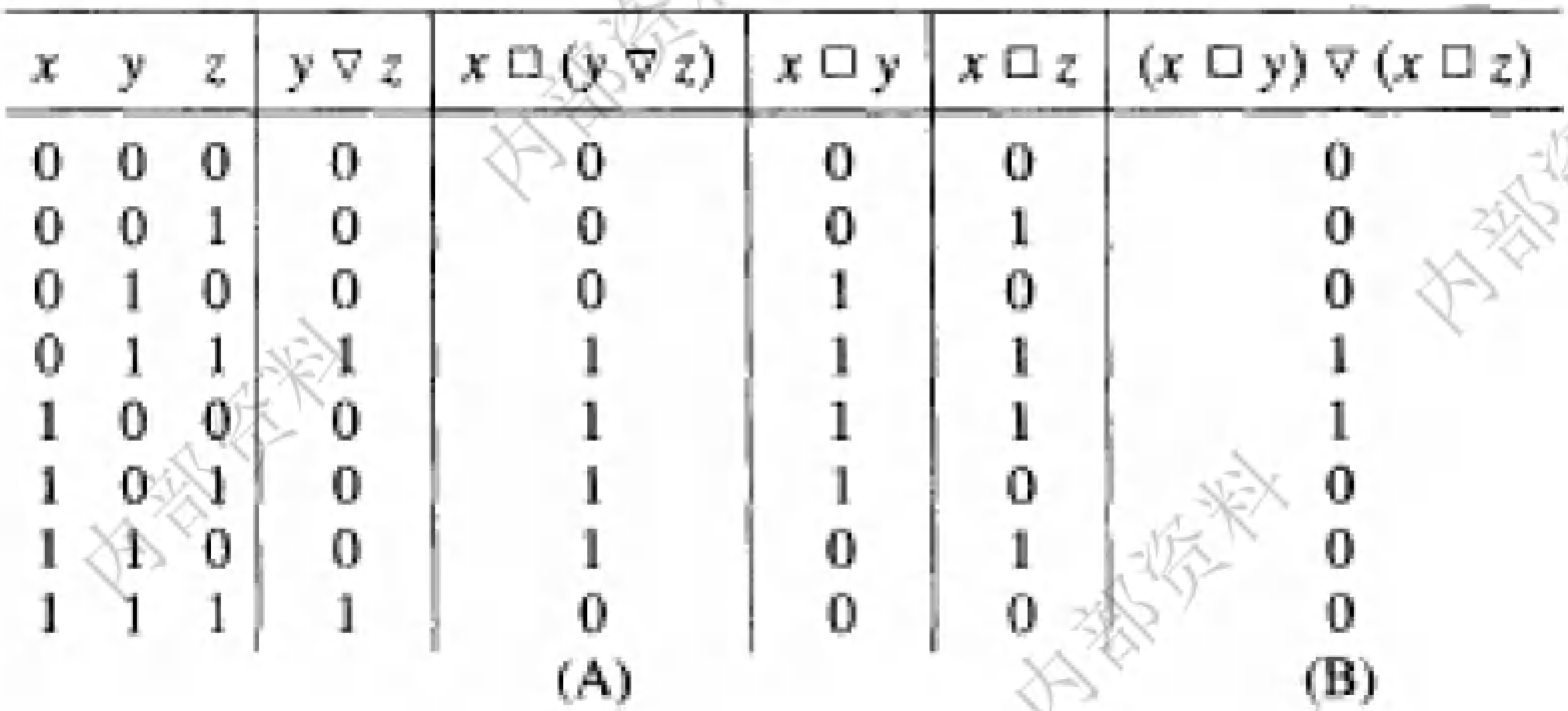
- Solution
  - (a) The statement *x* □ *y* = *y* □ *x* must be true for all choices of *x* and *y*. Since both 0 □ l and l □ 0 are l, □ is commutative.(运算表以主对角线对称)
  - (b) The eight possible cases to be checked are left as an exercise. ∇
  - (c) (0 □ 0) ∗ =0 ∗ = l   0 ∗ ∇ 0 ∗ =1 ∇ 1= l.

    (0 □ 1) ∗ =1 ∗ = 0   0 ∗ ∇ 1 ∗ =1 ∇ 0= 0.

    (1 □ 1) ∗ =0 ∗ = l   1 ∗ ∇ 1 ∗ =0 ∇ 0= 0.

  The last pair shows that De Morgan's laws do not hold in this structure.

- (d) One possible distributive property is $x \,\square\, (y \nabla z) = (x \,\square\, y) \nabla (x \,\square\, z)$.
  - all possible cases must be checked.
  - We can show it in a table.



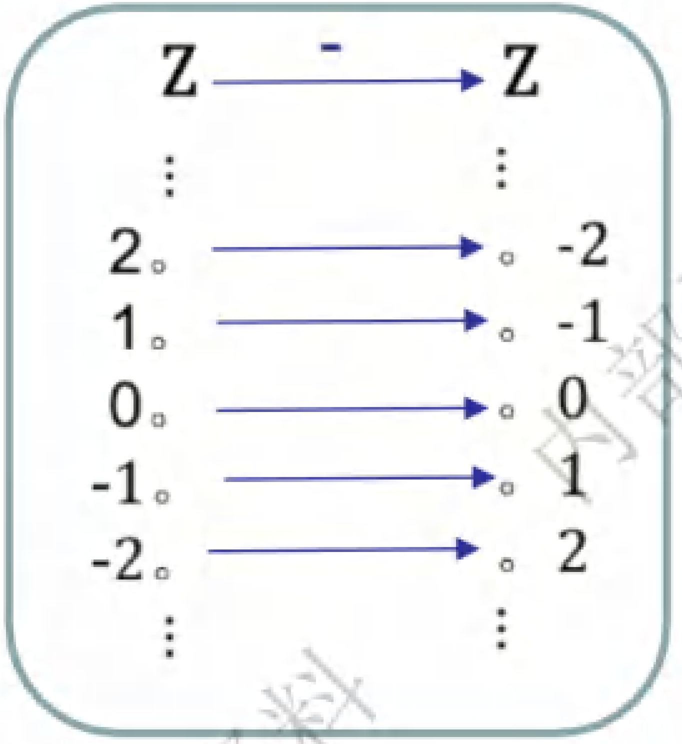
x	y	z	$y \nabla z$	$x \square (y \nabla z)$	$x \square y$	$x \square z$	$(x \square y) \nabla (x \square z)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	0	0
1	1	0	0	1	0	1	0
1	1	1	1	0	0	0	0
				(A)			(B)

Binary Operations

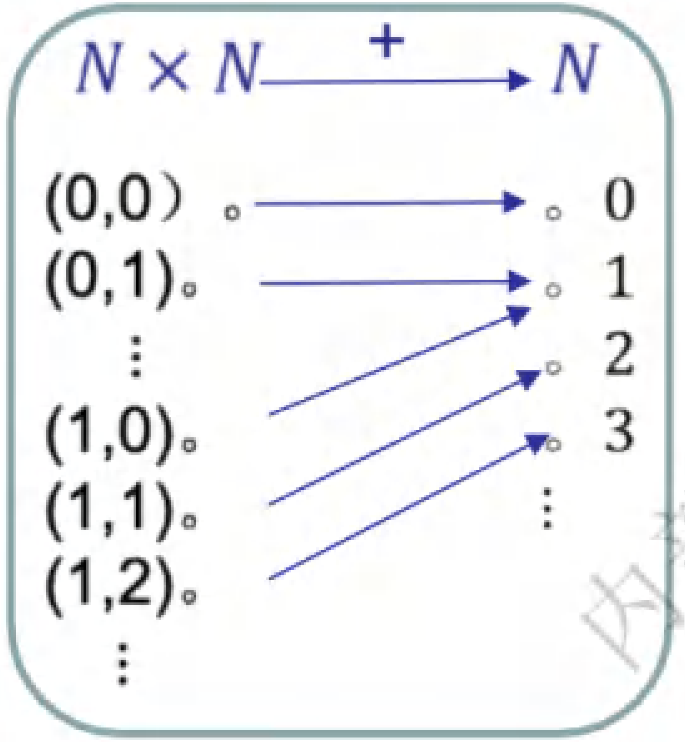
- Definition
- Properties of Binary Operations

例：

整数集合上的相反数运算



自然数集合上的加法运算



集合中任何一个或两个元素都可以进行运算，且运算的结果唯一

Binary operations(二元运算)

- A binary operation on a set *A* is an everywhere defined function f:$A\times A \to A$.

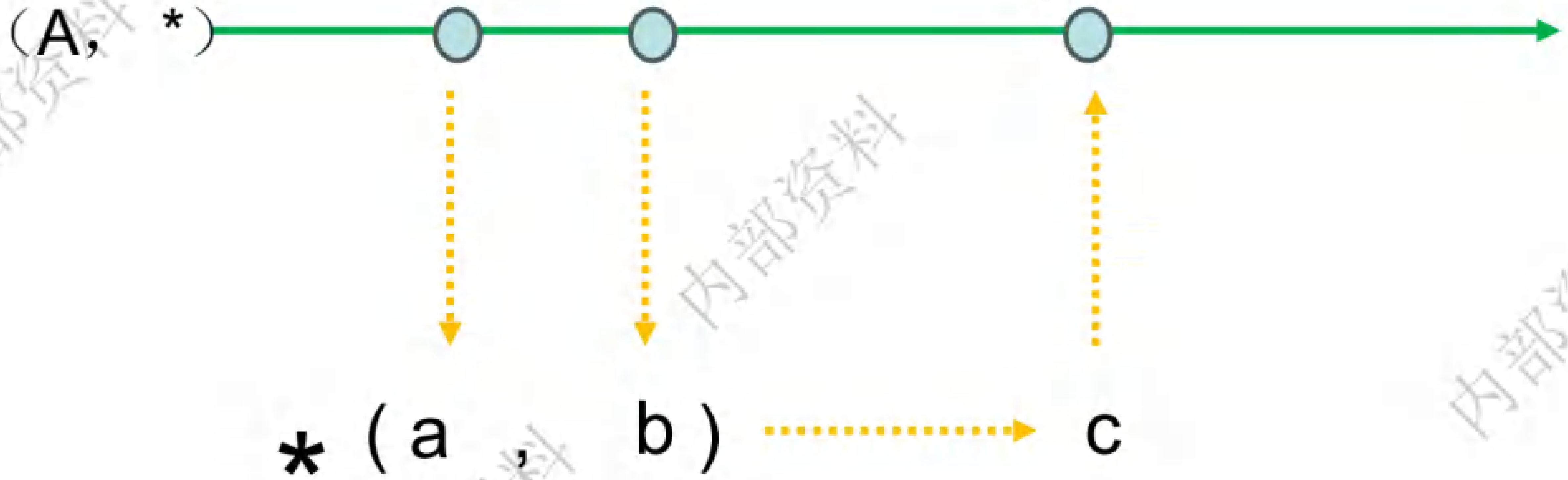
Note

- It's customary to denote binary operations by a symbol such as $*$, instead of f, and to denote the element assigned to (a, b) by $a * b$ [instead of $*(a, b)$].
- A is *closed*(封闭的) *under the operation* $*$, if a and b are elements in A, $a * b \in A$.

1.处处有定义
2.封闭---运算结果属于A
3.运算结果唯一 -----函数性质

A={ a , b , c, ...}

$f: A \times A \rightarrow A$



（A，*）

$*$ (a , b) c

Example 1,2

- Let $A = \mathsf{Z}$. Define $a * b$ as $a + b$.
  - $*$ is a binary operation on Z.
- Let $A = \mathsf{R}$. Define $a * b$ as a/b.
  - $*$ is not a binary operation.
  - For example, $3 * 0$ is not defined.

Example 3

- Let A = Z^+. Define $a * b$ as a-b.
  - $*$ is not a binary operation .
  - it does not assign an element of A to every ordered pair of elements of A; for example,$2 * 5 \notin A$.

不封闭

Example 4

- Let A = Z. Define $a * b$ as a number less than both a and b.
  - $*$ is not a binary operation, since it does not assign a *unique* element of A to each ordered pair of elements of A; for example, $8 * 6$ could be 5, 4, 3, l, and so on.
  - in this case, $*$ would be a relation from $A \times A$ to A, but not a function

不唯一

Example 5,6

- Let A = Z. Define $a * b$ as max{a, b}.(∗表示最大值)
  - ∗ is a binary operation; for example,2 ∗ 4 = 4, -3 ∗(-5)=-3.
- Let A = P(S), for some set S. If V and W are subsets of S, define $V * W$ as $V \cup W$.
  - ∗ is a binary operation on A.
  - if we define $V *' W$ as $V \cap W$, then ∗' is another binary operation on A.

Note: It's possible to define many binary operations on the same set.

Example 7,8

- Let M be the set of all $n \times n$ Boolean matrices for a fixed n. Define $A * B$ as $A \vee B$
  - $*$ is a binary operation.
  - This is also true of $A \vee B$.
- Let L be a lattice. Define $a * b$ as $a \vee b$.
  - $*$ is a binary operation on L.
  - This is also true of $a \vee b$

Table-运算表

If $A = \{a_l, a_2, \ldots, a_n\}$ is a *finite* set(有穷集), we can define a binary operation on A by means of a table

$\circ$	a_1	a_2	…	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	…	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	…	$a_2 \circ a_n$
·		· · ·		
·		· · ·		
·		· · ·		
a_n	$a_n \circ a_1$	$a_n \circ a_2$	…	$a_n \circ a_n$

	$\circ a_i$
a_1	$\circ a_1$
a_2	$\circ a_2$
·	·
·	·
·	·
a_n	$\circ a_n$

运算表的实例

例4 $A = P(\{a, b\})$, ⊕, ~分别为对称差和绝对补运算
（$\{a,b\}$为全集）

⊕ 的运算表

⊕	$\varnothing$ $\{a\}$ $\{b\}$ $\{a,b\}$
$\varnothing$ $\{a\}$ $\{b\}$ $\{a,b\}$	$\varnothing$ $\{a\}$ $\{b\}$ $\{a,b\}$ $\{a\}$ $\varnothing$ $\{a.b\}$ $\{b\}$

~ 的运算表

x	$\sim x$
$\varnothing$	$\{a,b\}$
$\{a\}$	$\{b\}$
$\{b\}$	$\{a\}$
$\{a,b$	$\varnothing$

运算表的实例（续）

例5 $Z_5 = \{ 0, 1, 2, 3, 4 \}$, $\oplus$, $\otimes$ 分别为模 5 加法与乘法

$\oplus$ 的运算表

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

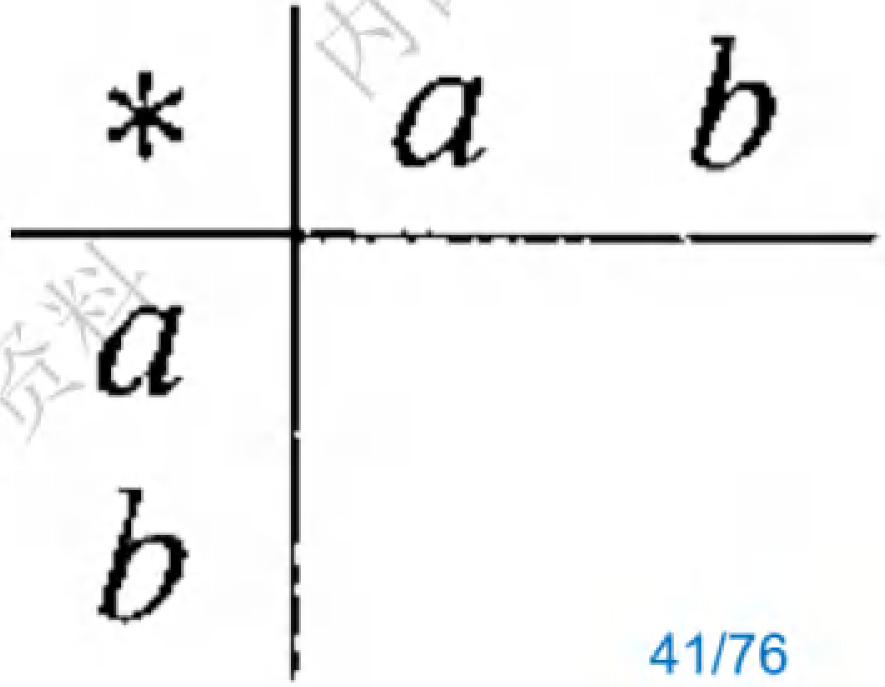
$\otimes$ 的运算表

$\otimes$	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

How many operations?

- If $A = \{a, b\}$, how many binary operations can be defined on A.
  - Every binary operation $*$ on A can be described by a table

There are $2 \cdot 2 \cdot 2 \cdot 2 = 2^4$ or 16 ways to complete the table.



$*$	a	b
a		
b		

Properties of Binary Operations 二元运算性质

- For all elements *a*, *b*, and *c* in *A*
- Commutative(交换律)

  $a * b = b * a$
- Associative(结合律)

  $a *(b * c) = (a * b) * c$
- Idempotent(等幂律)

  $a * a = a$

Idempotent(等幂律)

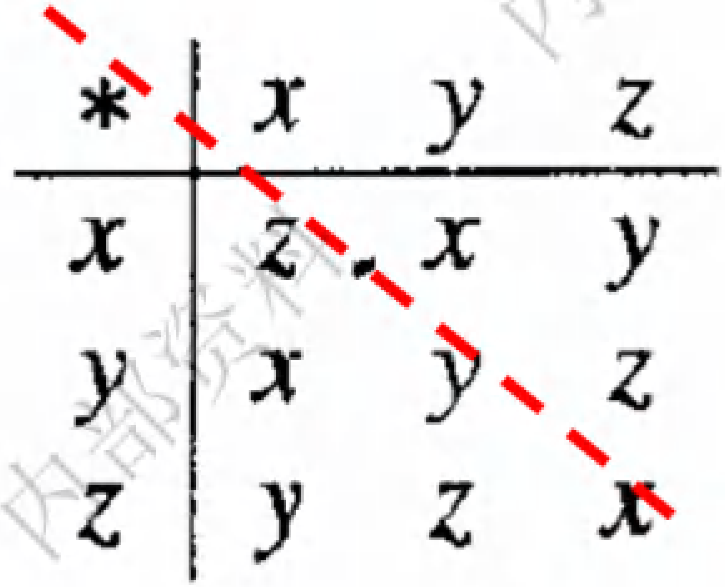
- 推广有限项：$a * a * a....a * = a$

Commutative - 交换律

- A binary operation on a set *A* is said to be *commutative* if $a \ast b = b \ast a$ for all elements *a* and *b* in *A*.
- Example:
- The binary operation of addition on Z is commutative.（实数加法可交换）
- The binary operation of subtraction on Z is not commutative（实数减法不可交换）, since $2-3 \neq 3-2$.

Commutative

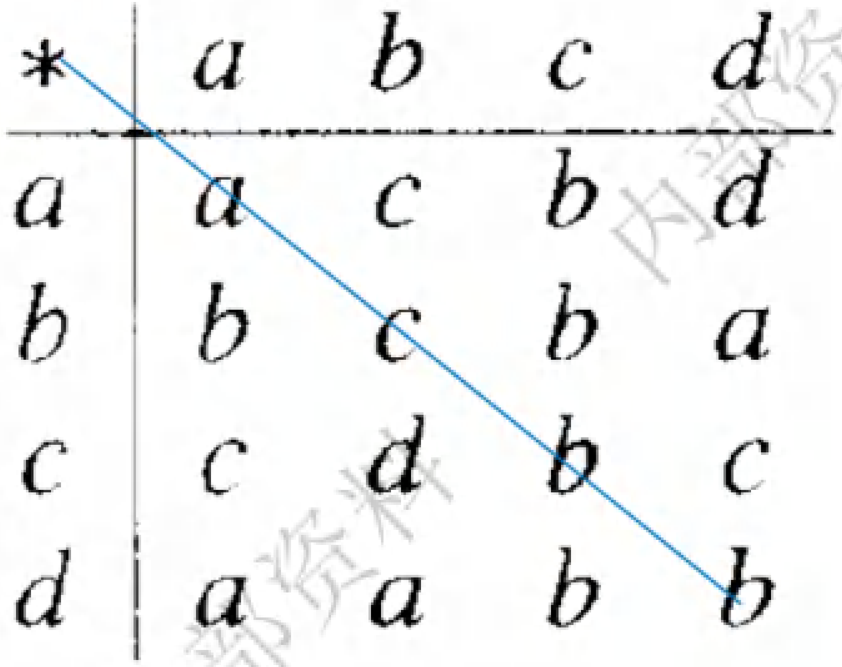
- A binary operation that is described by a table is commutative
  - if and only if
- The entries in the table are symmetric with respect to the main diagonal.



*	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

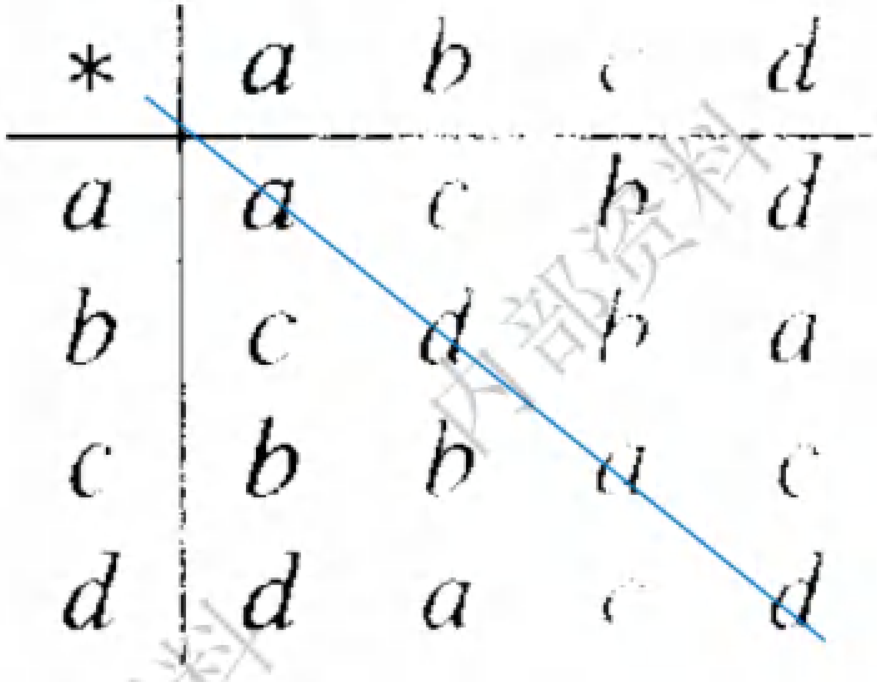
Example 12

- Which of the fol1owing binary operations on *A* = {*a*, *b*, *c*, *d*} are commutative?



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

(a) ×



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

(b) √

Associative - 结合律

- A binary operation $*$ on a set A is said to be associative if $a *(b * c) = (a * b) * c$ for all elements a, b, and c in A.
- *推广到n项结合成立*
- Example:
- The binary operation of addition on Z is associative.（实数加法可结合）

  $a+(b+c)=(a+b)+c$
- The binary operation of subtraction on Z is not associative（实数减法不可结合）, since $2-(3-5) \neq (2-3)-5$.

Example 15

- Let L be a lattice. The binary operation defined by $a * b = a \wedge b$ is （*定义为格的交运算），
  - *commutative* （交换）
  - *associative*. （结合）
  - It also satisfies the *idempotent* （等幂） property $a \wedge a = a$.

Example 16

- Let $*$ be a binary operation on a set A, and suppose that $*$ satisfies the following properties for any a, b, and c in A:
  - $a = a * a$ Idempotent property
  - $a * b = b * a$ Commutative property
  - $a *(b * c) = (a * b) * c$ Associative property

Define a relation $\leq$ on A by：

$a \leq b$ if and only if $a = a * b$.

Show that： $(A, \leq)$ is a poset, and for all a, b in A, GLB(a, b) = a*b.

Example 16（续）

Show that (A, ≤) is a poset, and for all a, b in A, GLB(a, b) = a*b.

思路：

条件：集合A上的二元运算∗，**满足交换，结合，等幂。定义关系“≤”，** $a \le b$，**当且仅当** $a = a * b$

证明 (A, ≤) 是偏序集, 且GLB(a, b) = a ∗ b.

1）要证偏序：自反，反对称，传递

2）求最大下界： GLB(a, b) = a*b

$\leq$ is reflexive（自反的）

$a \leq b$ if and only if $a = a * b$

- Since $a = a * a$,
  - $a \leq a$ *for* all a *in* A, and
  - $\leq$ is reflexive.

$a = a * a$ Idempotent

$a * b = b * a$ Commutative

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

$\leq$ is antisymmetric（反对称）

- $a \leq b$ if and only if $a = a * b$

- Now suppose that
  - $a \leq b$ and $b \leq a.$
  - Then, by definition and property 2, ——交换性
  - $a = a * b = b * a = b,$
  - so $a = b.$
  - Thus $\leq$ is antisymmetric.

$\leq$ is transitive

- $a \leq b$ if and only if $a = a * b$

- If $a \leq b$ and $b \leq c$,
  - then $a = a * b = a *(b * c) = \underline{(a * b)} * c = \underline{a} * c$,
  - so $a \leq c$ and
  - $\leq$ is transitive.

GLB： $a*b = a \wedge b$, for all a and b in A

$a \leq b$ if and only if $a = a * b$

先证是下界，
再证是最大下界

- We have
  - $a * b = a *(b * b) =(a * b) * b$,
  - so $a * b \leq b$.
  - In a similar way $a * b \leq a$.
  - so $a * b$ is a lower bound for a and b.
- Now, if $c \leq a$ and $c \leq b$.
  - then $c = c * a$ and $c = c * b$ by definition.
  - Thus $c = (c * a) * b = c *(a * b)$.
  - so $c \leq a * b$.
  - This shows that $a * b$ is the greatest lower bound of a and b.

特异元素及性质-小结

定义 设$\circ$ 为A上二元运算

单位元 e, $\forall a \in A$, $e \circ a = a \circ e = a$

零元 θ $\forall a \in A$, $\theta \circ a = a \circ \theta = \theta$

等幂元a $a \in A$, $a \circ a = a$

可逆元x （逆元 y） $x \in A$, $\exists y \in A$, $x \circ y = y \circ x = e$

特异元素的性质

单位元以及零元的唯一性

如果 $|A| > 1$, $e \neq \theta$

可结合的运算逆元唯一性： x的逆元标记为 x^{-1}

例

说明哪些运算是可结合的，可交换的，幂等的?
求出每个运算的单位元，零元，所有可逆元素的逆元

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

∘	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

•	a	b	c
a	a	b	c
b	b	c	c
c	c	c	c

解 (1) ∗满足交换、结合律；∘满足结合、幂等律；
•满足交换、结合律.

(2) ∗的单位元为 *b*, 没零元， $a^{-1} = c, b^{-1} = b, c^{-1} = a$

∘的单位元和零元都不存在，没有可逆元素.

•的单位元为 *a*， 零元为*c*, $a^{-1}=a$. *b*, *c*不可逆.

特异元素实例总结

集合	运算	单位元	零元	逆元
Z, Q, R	普通加法+	0	无	X 的逆元 $-x$
	普通乘法×	1	0	X 的逆元 x^{-1} (x^{-1}属于给定集合)
$M_n(R)$	矩阵加法+	n阶全0矩阵	无	X逆元$-X$
	矩阵乘法×	n阶单位矩阵	n阶全0矩阵	X的逆元 X^{-1} （X是可逆矩阵）
$P(B)$	并∪	$\varnothing$	B	$\varnothing$ 的逆元为 $\varnothing$
	交∩	B	$\varnothing$	B 的逆元为 B
	对称差⊕	$\varnothing$	无	X 的逆元为 X

Homework

- 9.1作业
- 20， 24
- 28, 32