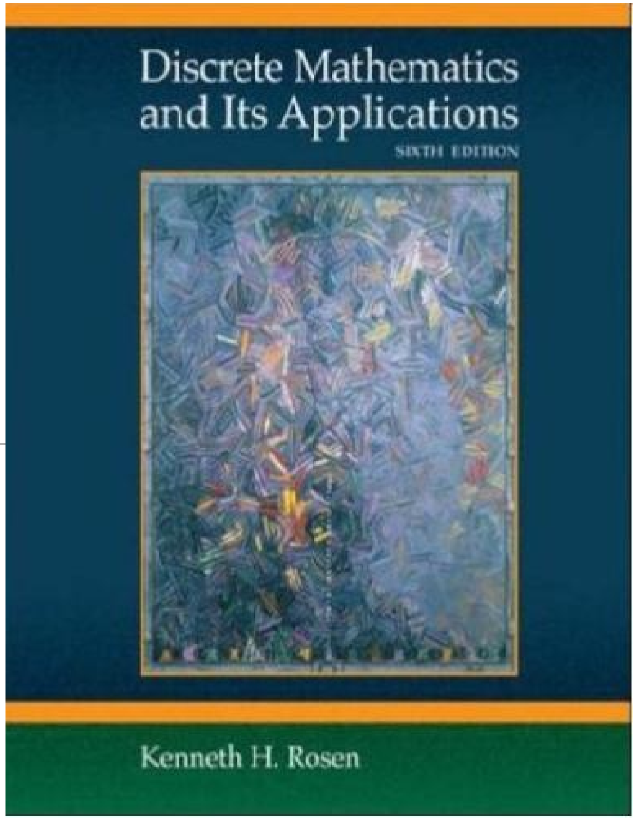
Discrete Mathematics

Jidong Yuan

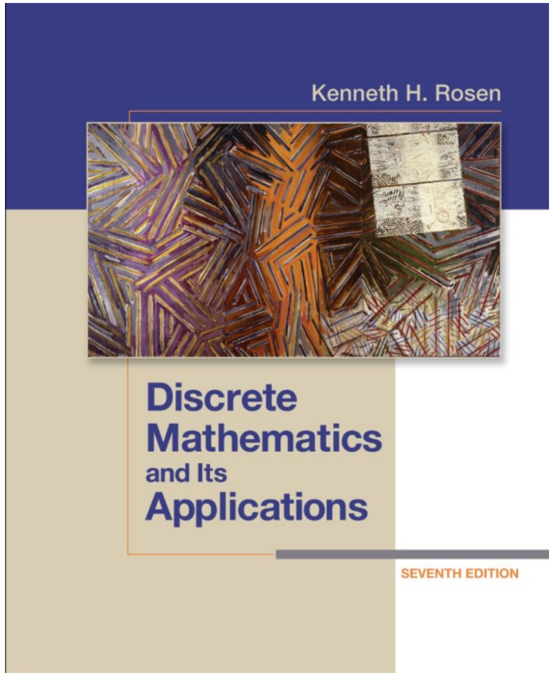
yuanjd@bjtu.edu.cn

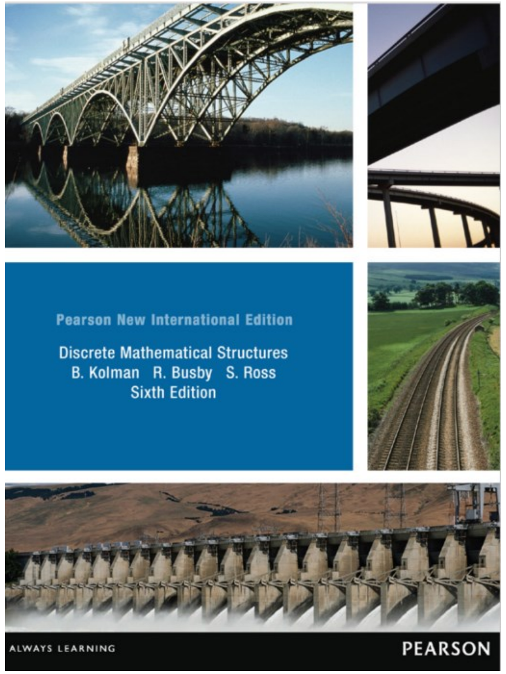
SD 404



Administrivia

- Textbook:
  - ✓Bernard Kolman, Robert C. Busby, Sharon Cutler Ross. Discrete Mathematical Structures (6th Edition). 2013.
  - ✓Kenneth H. Rosen. *Discrete Mathematics and Its Applications, 7th Edition*. McGraw Hill, 2012.
- Topic Covered:
  - ✓Algebraic Structure
  - ✓Graph Theory
- Homework 50% + Exam 50%
- English Learning





Algebraic Structure

- **Outline:**
- **Introduction to Algebraic Structure**
- Homomorphism and Isomorphism
- Semigroup and Monoid
- Group and Subgroup
- Abel group and Cyclic group
- Ring and Field
- Lattice
- Boolean algebra

Binary/Unary Operation

Definition:

- An operation that combines two objects is a **binary operation**.
- An operation that requires only one object is a **unary operation**.
- Every operation is a function.

Example:

- Subtraction and addition between any two members in set **R** are binary operations on set **R**.
- For any $a \in \mathbf{R}$, $a \to \frac{1}{a}$ and $a \to [a]$ are unary operations on set **R**.

Closed Operation

Definition:

- The binary operator ∘ is said to be a **closed operation** on a non empty set A, if $\forall a, b \in A, a \circ b \in A$.

Example:

- Subtraction is closed on **Z**.
- Subtraction is not closed on $\mathbf{Z}^+$.
- Addition is not closed on the set of odd integers.
- Multiplication is closed on the set of odd integers.

Exercise 1

$2-3$ $2/3$

- Are addition, multiplication, subtraction, division closed operations on set **N**?
- Are addition, multiplication, subtraction, division closed operations on set **Z**?

$2/3$

- Are addition, multiplication, subtraction, division closed operations on set **R***?

$2-3$

- Let set $S=P(\{a, b\})$, are $\cap$ and $\cup$ closed operations on set S?

- Let $A=\{1, 2, 3,\ldots, 10\}$, are the following binary operations $\circ$ closed?
  - $x \circ y = max(x, y)$
  - $x \circ y = min(x, y)$

Binary Operation Properties

- Commutativity

If $\forall a, b \in S, a \circ b = b \circ a$, then $\circ$ is commutative.

- Associativity

If $\forall a, b, c \in S, (a \circ b) \circ c = a \circ (b \circ c)$, then $\circ$ is associative.

Example 1

- Join and meet for Boolean matrices are commutative operations.

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

- Matrix multiplication is not a commutative operation.

$$AB \neq BA.$$

- Set union is an associative operation.

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

Exercise 2

- Let $\circ$ be a binary operation on set **Z** such that $a \circ b = a + b - 3ab$, find out if $\circ$ has the properties of commutativity and associativity.

➢ commutative:

$$a \circ b = a + b - 3ab = b + a - 3ba = b \circ a$$

➢ associative:

$$(a \circ b) \circ c = (a + b - 3ab) + c - 3(a + b - 3ab)c$$

$$= a + b - 3ab + c - 3ac - 3bc + 9abc$$

$$= a + b + c - 3ab - 3ac - 3bc + 9abc$$

$$= a + (b + c - 3bc) - 3a(b + c - 3bc)$$

$$= a \circ (b \circ c)$$

Algebraic System

Definition:

- A set A with one or more operations defined on it is called an algebraic system, denoted by $<A, f_1, f_2, f_3,\ldots, f_k>$.

Example:

- $<N, +>$, $<Z, +, -->$, $<R, +, \cdot, -->$
- $<P(S), \cup, \cap>$

Algebraic Constants

- Identity
- Zero
- Inverse

Identity

Definition:

- For an algebraic system <*A*, ∘>, an element *e* in *A* is said to be an identity element of *A* if $a \circ e = e \circ a = a$ for all $a \in A$.

Example:

- Identity for < **N**, *max* > is 0.
- There is no identity for < **N**, *min* >.
- < **R**, + >, < ~~**R**, -~~>, < **R**, · >, < **R**, ~~*max*~~ >, < **R**, ~~*min*~~ >, < **R**, |*x*-*y*| >.

0 1 ~~0~~ 没有

Exercise 3

- Let<*A*, *> be a algebraic system, *A*={*a*, *b*, *c*}, * is a binary operation on *A*. Operation relations are shown in the following tables. Determine whether there is identity in <*A*, *> .

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

a

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

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

a

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

a

Theorem 1

- If e is an identity for a binary operation $\circ$, then e is unique.

Proof:

✓Assume another object i also has the identity property, so $x \circ i = i \circ x = x$.

✓Then $e \circ i = e$, but since e is an identity for $\circ$, $i \circ \mathrm{e} = \mathrm{e} \circ i = i$.

✓Thus, $i = e$.

✓Therefore there is at most one object with the identity property for $\circ$.

Zero

Definition:

- For an algebraic system $<A, \circ>$, an element θ in A is said to be a zero element of A if $a \circ \theta = \theta \circ a = \theta$ for all $a \in A$.

Example:

- Zero for $<\mathbf{N}, min>$ is 0
- Zero for $<\mathbf{Z}^+, min>$ is 1
- $<\mathbf{R}, \cancel{+}>$, $<\mathbf{R}, \cancel{-}>$, $<\mathbf{R}, \cdot>$, $<\mathbf{R}, \cancel{max}>$, $<\mathbf{R}, \cancel{min}>$, $<\mathbf{R}, \cancel{|x-y|}>$.
- *

*	*a*	*b*
a	*a*	*b*
b	*b*	*b*

Theorem 2

- If Θ is a zero for a binary operation $\circ$, then Θ is unique.

Proof:

- ✓Assume another object i also has the zero property, so $x \circ i = i \circ x = i$.
- ✓Then $\Theta \circ i = i$, but since Θ is a zero for $\circ$, $i \circ \Theta = \Theta \circ i = \Theta$.
- ✓Thus, $i = \Theta$.
- ✓Therefore there is at most one object with the zero property for $\circ$.

Inverse

Definition:

- For an algebraic system $<A, \circ>$, if it has an identity e, we say y is a inverse of x if $x \circ y = y \circ x = e$.
- Apparently, if y is a inverse of x, then x is a inverse of y.
- e is a inverse of itself.

Example:

- Let $m, n \in \mathbf{Z}$, $A=\{x \mid x \in \mathbf{Z}, m \leq x \leq n\}$, in algebraic system $<A, \max>$:

✓identity: m m

✓zero: n n $\max(x, m) = x = m$

✓Which elements are invertible? m

Theorem 3

- If $\circ$ is an associative operation and x has an inverse y, then y is unique.
- **Proof:**

✓ Let w be another inverse of x.

✓ $w \circ x = x \circ y = e$

✓ $w = w \circ e$

✓ $\quad = w \circ (x \circ y)$

✓ $\quad = (w \circ x) \circ y$

✓ $\quad = e \circ y$

✓ $\quad = y$

北京交通大學

Exercise 4

0

- For algebraic system <**R**, ·>, does every element in the system has a inverse?

- Let<*A*, *> be a algebraic system, *A*={*a*, *b*, *c*}. Operation relations are shown in the following tables. Find out the inverse of each element.

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

a bc

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

a, bb

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

a

Operation table

- Let<A, *> be a algebraic system, A={a, b, c}. Operation relations are shown in the following tables.

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

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

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

✓Closure: every element in the table belongs to A.

✓Commutativity: symmetric about the diagonal.

✓Identity: a , a , a

✓Zero: X , c , X

✓Inverse: a bc , ab ; X

Exercise 5

- Let $<Q, \circ>$ be a algebraic system, $\forall x, y \in Q$, $x \circ y = x+y+2xy$
- (a) Is $<Q, \circ>$ commutative? ✓
- (b) Is $<Q, \circ>$ associative? ✓
- (c) Find out the identity of the algebraic system if it exists. 0
- (d) Find out the zero of the algebraic system if it exists. $-\frac{1}{2}$
- (c) Find out inverses of every invertible element.

$$x = -\frac{y}{1+2y} \quad y \neq -\frac{1}{2}$$