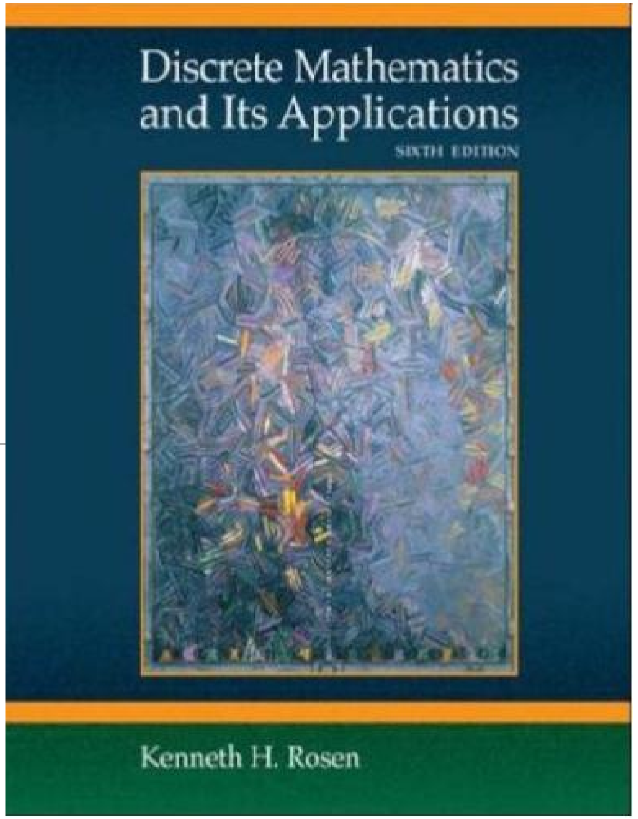
北京交通大學

Discrete Mathematics



Jidong Yuan

yuanjd@bjtu.edu.cn

SD 404

Algebraic Structure

- **Outline:**
- Introduction to Algebraic Structure
- Semigroup and Monoid
- Group and Subgroup
- Abelian Group, Cyclic Group and Permutation Group
- Coset
- **Ring and Field**
- Lattice
- Boolean algebra

Review

- Algebraic system <A, ∘>
  - ✓ 3 properties
    - Closure
    - Commutativity
    - Associativity
  - ✓ 3 constants
    - Identity
    - Zero
    - Inverse
  - ✓ 7 special algebraic systems
    - Semigroup
    - Monoid
    - Group
    - Abelian Group
    - Cyclic Group
    - Permutation Group
    - Coset
  - ✓ 2 relations
    - Homomorphism
    - Isomorphism

Ring

Definition:

- Let $<S, \triangle, *>$ be a algebraic system with two binary operations. $<S, \triangle, *>$ is said to be a **Ring** if the following conditions are satisfied.

(1) $<S, \triangle>$ is an Abelian group.

(2) $<S, *>$ is a semigroup.

(3) $*$ is distributive over $\triangle$.

- Distributive property

Let $\triangle$ and $*$ are binary operations defined on set S, for $\forall a, b, c$, if

$\boldsymbol{a * (b \triangle c) = (a * b) \triangle (a * c)}$ and $\boldsymbol{(b \triangle c) * a = (b * a) \triangle (c * a)}$

Then $*$ is distributive over $\triangle$.

北京交通大学

Ring Cont.

Example:

- Determine whether $<\mathbf{R}, +, \cdot>$ is a ring or not.

- Let $<S, \triangle, *>$ be a ring,

✓ if $*$ is communitive, then $<S, \triangle, *>$ is a **communitive ring**.

✓ if $<S, *>$ has a identity (monoid), then $<S, \triangle, *>$ is a **ring with identity**.

Example 1

- $\mathbf{Z}_n$={[0], [1], [2], [3],…,[n-1]}, define [a] + [b] = [a + b], [a] · [b] = [a · b]. Show that <$\mathbf{Z}_n$, +, ·> is a communitive ring with identity.

Example 2

- Let $<A, \triangle, *>$ be a ring, e be the identity of $<A, \triangle>$, a^{-1} denotes the inverse of a on $<A, \triangle>$. For $\forall a, b, c \in A$, show that

(1) $a * e = e * a = e$

(2) $a * b^{-1} = a^{-1} * b = (a * b)^{-1}$

Example 2 Cont.

- Let $<A, \triangle, *>$ be a ring, e be the identity of $<A, \triangle>$, a^{-1} denotes the inverse of a on $<A, \triangle>$. For $\forall a, b, c \in A$, show that

(3) $a^{-1} * b^{-1} = a * b$

Field

Definition:

- Let <S, △, ∗> be an algebraic system with two binary operations. <S, △, ∗> is said to be a **Field** if the following conditions are satisfied.

(1) <S, △> is an Abelian group.

(2) <S – {θ}, ∗> is an Abelian group.

(3) ∗ is distributive over △.

Example:

- <**R**, +, ·>
- <**Z**, +, ·>

Example 3

- Let <A, +, ·> be a algebraic system, A are the following sets:

(1) $A=\{x \mid x \geq 0, x \in \mathbf{Z}\}$

(2) $A=\{x \mid x = a/b, a, b \in \mathbf{Z}^+, a \neq b\}$

(3) $A=\{x \mid x = a + b\sqrt{3}, a, b \in \mathbf{Q}\}$

Is <A, +, ·> a field?

Example 4

- Is ring $<\mathbf{Z}_4, +, \cdot>$ a field? What about $<\mathbf{Z}_5, +, \cdot>$?

- Ring $<\mathbf{Z}_n, +, \cdot>$ is a field when n is a prime number.