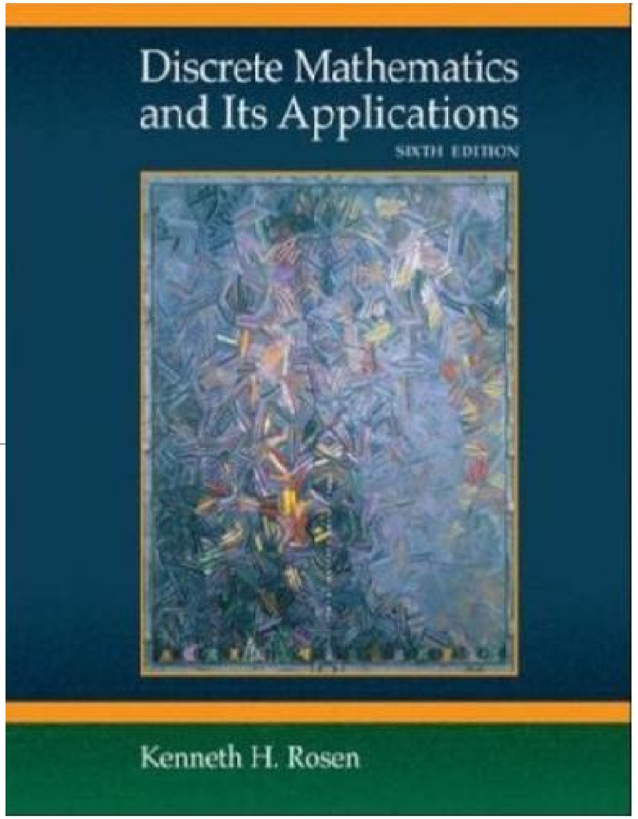
Discrete Mathematics



Jidong Yuan

yuanjd@bjtu.edu.cn

SD 404

Algebraic Structure

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

Review

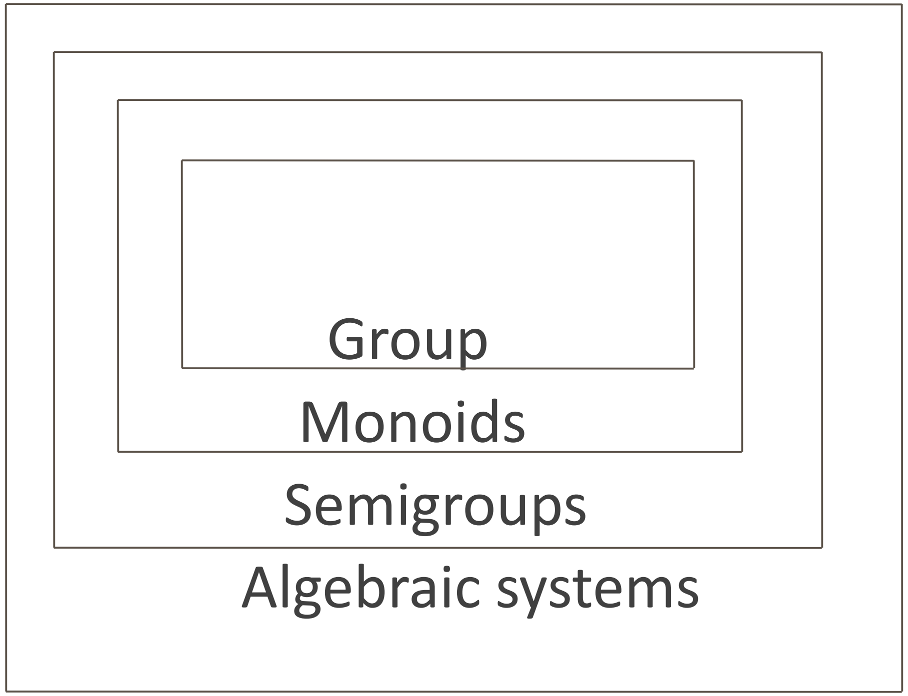
- Algebraic system <A, ∘>
  - ✓3 properties
    - Closure
    - Commutativity
    - Associativity
  - ✓3 constants
    - Identity
    - Zero
    - Inverse
  - ✓2 special algebraic systems
    - Semigroup
    - Monoid
  - ✓2 relations
    - Homomorphism
    - Isomorphism

Group

Definition:

- An algebraic system $<G, *>$ is said to be a **group** if the following conditions are satisfied.

1) $*$ is a closed operation.
2) $*$ is an associative operation.
3) There is an identity in G.
4) Every element in G has inverse in G.



Example:

- $<\mathbf{Z}, +>$ is a group.
- $<\mathbf{Z}^+, +>$ is not a group.

Example 1

- Determine whether <**R**, ·> is a group. What about <**R** - {0}, ·>? Prove your conclusion.

1. Closure: We know that, product of two nonzero real numbers is again a nonzero real number .

$$ab \in \mathbf{R} - \{0\} \text{ for } \forall a, b \in \mathbf{R} - \{0\}.$$

2. Associativity: We know that multiplication of real numbers is associative.

$$(ab)c = a(bc) \quad \text{for } \forall a, b, c \in \mathbf{R} - \{0\}.$$

3. Identity : We have $1 \in \mathbf{R} - \{0\}$ and $1 \cdot a = a \cdot 1 = a$ for $\forall a \in \mathbf{R} - \{0\}$.

4. Inverse: To $\forall a \in \mathbf{R} - \{0\}$, we have $1/a \in \mathbf{R} - \{0\}$ such that

$$a(1/a) = 1$$ i.e., Each element in **R** - {0} has an inverse.

Exercise 1

- Let $a * b = ab/2$. Show that $<\mathbf{R}^+, *>$ is a group.

Finite Group

- **Finite Group**: Let $<G, *>$ be a group, if G is a finite set then $<G, *>$ is called a finite group.

- **Order of a group**: The number of elements in a group is called order of the group, denoted by $|G|$.

- **Infinite Group:** Let $<G, *>$ be a group, if G is a infinite set then $<G, *>$ is called a infinite group.

Exercise 2

- Let G={0, 1}, $*$ be an operation defined on G as follows. Show that <G, $*$> is a group.

*	0	1
0	0	1
1	1	0

- In a group with 2 elements, each element is its own inverse.

Theorems

- In a group $<G, *>$ the following properties hold

1. Zero doesn't exist.
2. Inverse of an element is unique.
3. Cancellation laws hold

$$a * b = a * c \Rightarrow b = c \quad \text{(left cancellation law)}$$

$$a * c = b * c \Rightarrow a = b \quad \text{(Right cancellation law)}$$

4. $(a^{-1})^{-1}=a$

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

5. $a * x = b$ has a unique solution in G.

$y * a = b$ has a unique solution in G.

Theorem 1

- Zero doesn't exist in groups.

Proof:

Assume θ is the zero in group $<G, *>$.

$\forall a \in G, \theta * a = a * \theta = \theta.$

θ doesn't have an inverse, which contradicts the fact that $<G, *>$ is a group.

Theorem 2

- Inverse of each element in a group is unique.

Proof:

Assume a has two inverses a_1 and a_2.

Theorem 3

- Cancellation laws hold in a group.

$a * b = a * c \rightarrow\ b = c$ (left cancellation law)

$a * c = b * c \rightarrow\ a = b$ (Right cancellation law)

Proof:

Theorem 4

- $\forall a, b \in G$ in a group $<G, *>$,

  $(a^{-1})^{-1}=a$

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

Proof:

Theorem 5

- Let $<G, *>$ be a group, and let a and b be elements of G. Then

  $a * x = b$ has a unique solution in G.

  $y * a = b$ has a unique solution in G.

Proof:

Subgroup

Definition:

- Let $<G, *>$ be a group, and let H be a subset of G such that:

✓(a) The identity e of $<G, *>$ belongs to H.

✓(b) If a and b belong to H, then $a * b \in H$.

✓(c) If $a \in H$, then $a^{-1} \in H$.

Then $<H, *>$ is called a **subgroup** of $<G, *>$.

- Let $<G, *>$ be a group. Then $<G, *>$ and $<\{e\}, *>$ are subgroups of G, called the **trivial subgroups** of G.

Example:

- $<\mathbf{Z}, +>$ and $<\mathbf{Q}, +>$ are subgroups of the group $<\mathbf{R}, +>$.

Example 2

- Let $H=\{x|x=2n, n \in \mathbf{Z}\}$, show that $<H, +>$ is a subgroup of $<\mathbf{Z}, +>$.

✓(a) The identity e of $<G, *>$ belongs to H.

✓(b) If a and b belong to H, then $a * b \in H$.

✓(c) If $a \in H$, then $a^{-1} \in H$.

Theorem 6

- Let $<G, *>$ be a group, and $<H, *>$ be a subgroup of $<G, *>$. Then the identity e of $<G, *>$ is also the identity of $<H, *>$.

Proof:

For $\forall a \in H, a \in G$.

$a * e = e * a = a$.

Thus, e is the identity of $<H, *>$.

Theorem 7

- A necessary and sufficient condition for a nonempty subset H of a group $<G, *>$ to be a subgroup is that for $\forall a, b \in H \rightarrow a * b^{-1} \in H$.

Proof:

(1) If $<H, *>$ is a subgroup of $<G, *>$,

$b \in H$, then $b^{-1} \in H$. $a \in H$, then $a * b^{-1} \in H$.

(2) $\forall a, b \in H \rightarrow a * b^{-1} \in H$, then $\forall a \in H \rightarrow a * a^{-1} \in H$.

$a \in H \subseteq G$, then $a * a^{-1} = e \in H$.

$e \in H$, $\forall a \in H$, then $e * a^{-1} = a^{-1} \in H$.

$\forall a, b \in H$, $b^{-1} \in H$, then $a * (b^{-1})^{-1} \in H$.

✓(a) The identity e of $<G, *>$ belongs to H.

✓(b) If a and b belong to H, then $a * b \in H$.

✓(c) If $a \in H$, then $a^{-1} \in H$.

Exercise 3

- Let $<G, *>$ be a group. $<H_1, *>$ and $<H_2, *>$ are two subgroups of G. Show that $< H_1 \cap H_2, *>$ is also a subgroup of G.

A necessary and sufficient condition for a nonempty subset H of a group $<G, *>$ to be a subgroup is that for $\forall a, b \in H \rightarrow a * b^{-1} \in H$.

Isomorphism of Groups

Example:

- Two groups <**R**, +> and <**R**$^+$, ·>. Let f : **R** → **R**$^+$ be defined by $f(x) = e^x$. Show that f is an isomorphism.

Proof:

- If $f(a) = f(b)$, so that $e^a = e^b$, then $a = b$. Thus f is one to one.
- If $a \in$ **R**$^+$, then $\log a \in$ **R** and $f(\log a) = e^{\log a} = a$, so f is onto.
- $f(a + b) = e^{a+b} = e^a \cdot e^b = f(a)f(b)$.

✓Define a function $f : S \to T$ with domain S.
✓Show that f is one-to-one.
✓Show that f is onto.
✓$f(a * b) = f(a) \circ f(b)$.