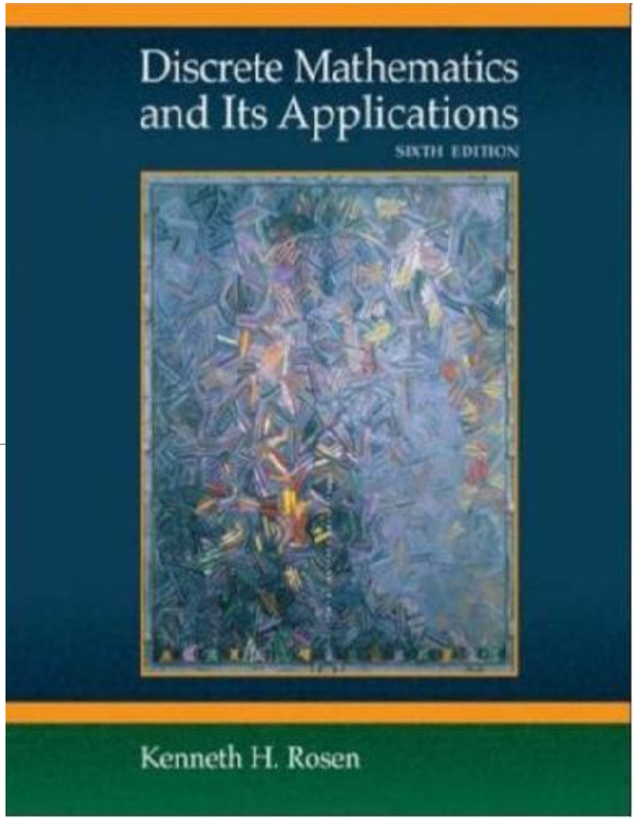
Discrete Mathematics



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**
- Ring and Field
- Lattice
- Boolean algebra

Review

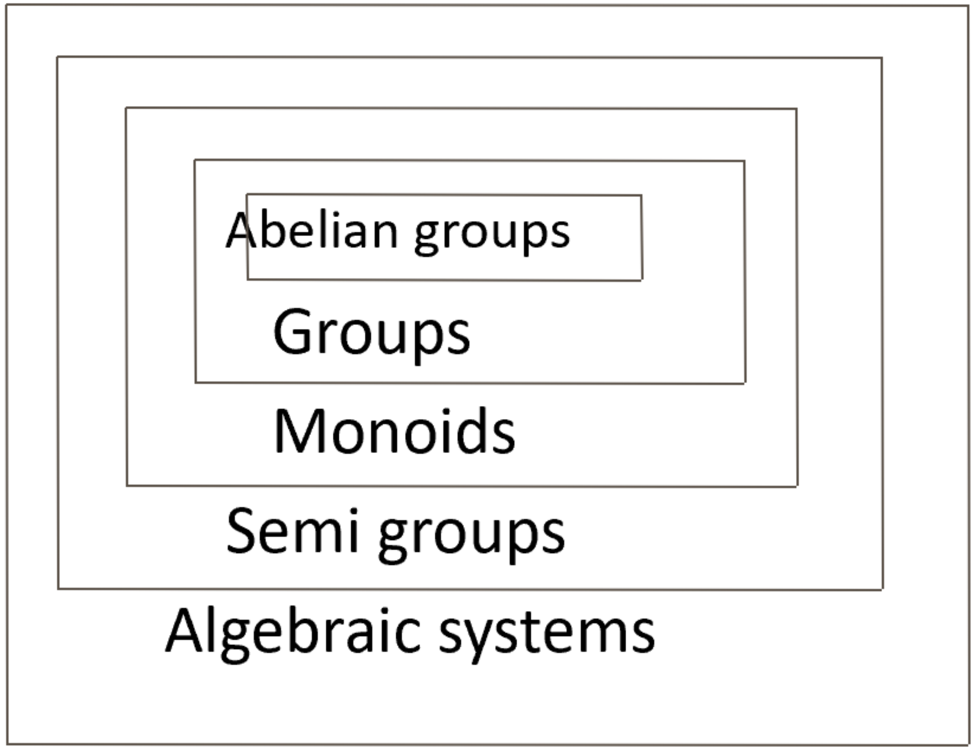
- Algebraic system <A, ∘>
  - ✓ 3 properties
    - Closure
    - Commutativity
    - Associativity
  - ✓ 3 constants
    - Identity
    - Zero
    - Inverse
  - ✓ 3 special algebraic systems
    - Semigroup
    - Monoid
    - Group
  - ✓ 2 relations
    - Homomorphism
    - Isomorphism

Abelian Group

Definition:

- An algebraic system <G, $*$> is said to be an **Abelian 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.
5) $*$ is a commutative operation.



Example:

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

× ∃ identity

Exercise 1

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

① $a * b = \frac{ab}{2} \in R^+$

② $(a*b)*c = \frac{ab}{2} * c = \frac{abc}{2\times 2} = \frac{a}{2} \cdot (\frac{bc}{2}) = a*(\frac{bc}{2}) = a*(b*c)$

③ $2*a = \frac{2a}{2} = a$, $a*2 = \frac{a2}{2} = a$, $2 \to$ identity

④ $a * a^{-1} = \frac{aa^{-1}}{2} = 2$ $a^{-1} = \frac{4}{a} \in R^+$

⑤ $a * b = \frac{ab}{2} = \frac{ba}{2} = b*a$

Modulo Systems

- Let m be a positive integer. For any two positive integers a and b operation $+_m$ is defined as follows:

$a +_m b = r$, where r is the remainder obtained by dividing $(a+b)$ with m.

i.e. $a + b \equiv r \pmod{m}$

- Let $\mathbf{Z}_4=\{0, 1, 2, 3\}$, show that $\langle \mathbf{Z}_4, +_4 \rangle$ is an Abelian group.

$+_m$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

closed

$(a +_m b) +_m c \qquad a +_m (b +_m c)$

0

1 3 2 2 0 0

$a +_m b = b +_m a$

Cont.

- Let $\mathbf{Z}_4$={0, 1, 2, 3}, show that <$\mathbf{Z}_4$, $+_4$> is an Abelian group.

$+_m$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Theorem 1

- A necessary and sufficient condition for a group $<G, *>$ to be an Abelian group is that for $\forall a, b \in G$, $(a * b) * (a * b) = (a * a) * (b * b)$.

Proof:

(1) If $<G, *>$ is an Abelian group, then

$(a * b) * (a * b) = a * (b * a) * b = a * (a * b) * b = (a * a) * (b * b)$

(2) If $\forall a, b \in G$, $(a * b) * (a * b) = (a * a) * (b * b)$

$(a * b) * (a * b) = a * (b * a) * b$

$(a * a) * (b * b) = a * (a * b) * b$

$b * a = a * b$

Cyclic Group

- Suppose that <G, $*$> is a group, and let $a \in G$. For $n \in \mathbf{Z}^+$, we define the powers of a recursively as follows:

$a^0 = e$, $a^1 = a$, $a^n = a^{n-1} * a$, $n \geq 2$.

- A group is called a **cyclic group** if all of its elements are the powers of one of its elements. The element is called a **generator**.

Example 1

- Let A={0°, 60°, 120°, 180°, 240°, 300°}, representing different angles that one geometric figure on the plane rotates clockwise around its center. $*$ is a binary operation on A. $a * b$ is defined as the angle after the figure rotates a and b continuously. Determine whether <A, $*$> is a cyclic group or not.

$*$	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

Cont.

*	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

60

Theorem 1

- Every cyclic group must be an abelian group.

proof:

Let $<G, *>$ be a cyclic group, and a be the generator.

For $\forall x, y \in G$, there must be $r, s \in \mathbf{Z}$, such that $x=a^r$, $y=a^s$.

$$x * y = a^r * a^s = a^{r+s} = a^s * a^r = y * x$$

Permutation

Definition:

- Let S be a nonempty set, a bijection on S is called a permutation of S.

Example:

- Let S={1, 2, 3}

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Permutation Composition

Definition:

- Composition of two permutations $p_1 \circ p_2$ on a group S is defined as doing p_2 permutation on S first and then doing p_1 permutation.

Example:

- Let S={1, 2, 3}

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

- $p_2 \circ p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = p_5$

Permutation Composition

- The set of all permutations of n elements is denoted by S_n, $<S_n, \circ>$ is a group of order $n!$ under the operation of composition.

Proof:

- (1) Closure

For $\forall p_1, p_2 \in S_n$, for $\forall a, b \in S$ and $a \neq b$.

Assume that after p_2, $p_2(a)=c$, $p_2(b)=d$. The we have $c, d \in S$ and $c \neq d$.

Assume that after p_1, $p_1(c)=e$, $p_1(d)=f$. The we have $e, f \in S$ and $e \neq f$.

$p_1 \circ p_2$ maps any two different elements in S to two different elements in S.

Thus $p_1 \circ p_2$ is also a permutation of S, $p_1 \circ p_2 \in S_n$.

北京交通大学

Permutation Composition

- The set of all permutations of n elements is denoted by S_n, $<S_n, \circ>$ is a group of order $n!$ under the operation of composition.

Proof:

- (2) Associativity

For $\forall p_1, p_2, p_3 \in S_n$, for $\forall x \in S$, Assume $p_3(x)=y$, $p_2(y)=z$, $p_1(z)=w$.

$p_1 \circ (p_2 \circ p_3)(x) = p_1(p_2 \circ p_3(x)) = p_1(p_2(p_3(x))) = w.$

$(p_1 \circ p_2) \circ p_3(x) = (p_1 \circ p_2)(p_3(x)) = p_1(p_2(p_3(x))) = w.$

$p_1 \circ (p_2 \circ p_3) = (p_1 \circ p_2) \circ p_3.$

Permutation Composition

- The set of all permutations of n elements is denoted by S_n, $<S_n, \circ>$ is a group of order $n!$ under the operation of composition.

Proof:

- (3) Identity

There is a permutation p_e in S_n such that for $\forall x \in S$, $p_e(x)=x$.

Then for $\forall p_a \in S_n$, for $\forall x \in S$, $p_a \circ p_e = p_e \circ p_a = p_a$.

Thus p_e is the identity of $<S_n, \circ>$.

Permutation Composition

- The set of all permutations of n elements is denoted by S_n, $<S_n, \circ>$ is a group of order n! under the operation of composition.

Proof:

- (4) Inverse

For $\forall p_a \in S_n$, for $\forall x \in S$, assume $p_a(x)=y$.

Then there must be a permutation p_b such that $p_b(y)=x$.

$$p_a \circ p_b = p_b \circ p_a = p_e$$

Permutation Group

Definition:

- Any subgroup of $<S_n, \circ>$ is a **permutation group** on S.

Example:

- Let S={1, 2, 3}, list all permutation groups on S.

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Cont.

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$\circ$	p_1	p_2	p_3	p_4	p_5	p_6
p_1						
p_2						
p_3						
p_4						
p_5						
p_6						

Cont.

- Let S={1, 2, 3}, list all permutation groups on S.

$\circ$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_4	p_1	p_2	p_6	p_5
p_4	p_4	p_3	p_6	p_5	p_1	p_2
p_5	p_5	p_6	p_2	p_1	p_4	p_3
p_6	p_6	p_5	p_4	p_3	p_2	p_1

✓(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 $a^{-1} \in H$.

✓identity: p_1
✓ ${p_1}^{-1} = p_1$
✓ ${p_2}^{-1} = p_2$
✓ ${p_3}^{-1} = p_3$
✓ ${p_4}^{-1} = p_5$
✓ ${p_6}^{-1} = p_6$

Permutation groups: <S_n, $\circ$>, <{ p_1}, $\circ$>, <{ p_1, p_2}, $\circ$>, <{ p_1, p_3}, $\circ$>, <{ p_1, p_6}, $\circ$>, <{ p_1, p_4, p_5}, $\circ$>