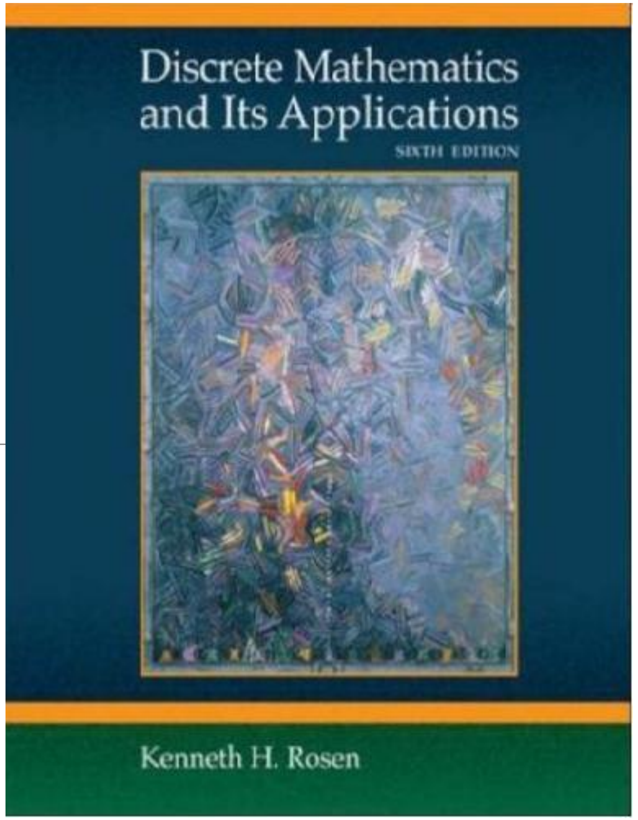
北京交通大學

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
  - 6 special algebraic systems
    - Semigroup
    - Monoid
    - Group
    - Abelian Group
    - Cyclic Group
    - Permutation Group
  - 2 relations
    - Homomorphism
    - Isomorphism

Coset

Definition:

- If $<H, *>$ is a subgroup of $<G, *>$ and $a \in G$ then the set

$Ha = \{h * a | h \in H\}$ is called a right coset of H in G.

$aH = \{a * h | h \in H\}$ is called a left coset of H in G.

Example:

✓ $<\mathbf{Z}, +>$ is a subgroup of $<\mathbf{R}, +>$.

✓ $2.5 \in \mathbf{R}$

✓ $\{a + 2.5 | a \in \mathbf{Z}\}$ is a right coset of **Z** in **R**.

✓ $\{2.5 + a | a \in \mathbf{Z}\}$ is a left coset of **Z** in **R**.

Exercise 1

- Let S={1, 2, 3}, <S_3, ∘> is a group. Determine all the left cosets of H = {p_1, p_3} in S_3.

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

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

Equivalence Relation

- $<H, *>$ is a subgroup of $<G, *>$. $R=\{(a, b) \mid a, b \in G$ and $a^{-1} * b \in H\}$ is an equivalence relation on G.

Proof:

✓Reflexivity:

For $\forall a \in G$, $a^{-1} \in G$. $a^{-1} * a = e \in H$. Thus $(a, a) \in R$.

✓Symmetry:

For $\forall (a, b) \in R$, $a^{-1} * b \in H$. H is a group, thus $(a^{-1} * b)^{-1} = b^{-1} * a \in H$, $(b, a) \in R$.

✓Transitivity:

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

$(a^{-1} * b) * (b^{-1} * c) \in H$. Thus $a^{-1} * c \in H$, $(a, c) \in R$.

Equivalence Classes

- $<H, *>$ is a subgroup of $<G, *>$. $R=\{(a,b) \mid a, b \in G \text{ and } a^{-1} * b \in H\}$ is a equivalence relation on G.

For $\forall a \in G$, *if* $[a]_R = \{x \mid x \in G \text{ and } (a, x) \in R\}$, $[a]_R = aH$.

Proof:

$b \in [a]_R$ if and only if $(a, b) \in R$.

$$
\begin{aligned}
[a]_R &= \{b \mid a^{-1} * b \in H, a, b \in G\} \\
&= \{b \mid a^{-1} * b = h, h \in H, a, b \in G\} \\
&= \{b \mid b = a * h, h \in H, a, b \in G\} \\
&= aH
\end{aligned}
$$

Coset:

If $<H, *>$ is a subgroup of $<G, *>$ and $a \in G$ then the set:

$Ha = \{h * a \mid h \in H\}$ is called a right coset of H in G.

$aH = \{a * h \mid h \in H\}$ is called a left coset of H in G.

Properties of Cosets

- Let <H, $*$> be a subgroup of <G, $*$> . Then the left (right) cosets of H form a partition of G. i.e., the union of all left (right) cosets of a subgroup H is equal to G.
- Any two left (right) cosets of H in G are either identical or disjoint.

$$G = \bigcup_{i=1}^{k} [a_i]_R = \bigcup_{i=1}^{k} a_i H$$

- $|a_1H| = |a_2H| = |a_3H| = \ldots = |a_kH| = |H|$

Lagrange's theorem

- The order of each subgroup of a finite group is a divisor of the order of the group.
- If $<H, *>$ is a subgroup of $<G, *>$, $|G|=n$, $|H|=m$, then $m|n$.

Proof:

Since $<G, *>$ is a finite group, H is finite.

Therefore, the number of cosets of H in G is finite.

Let $a_1H, a_2H, \ldots, a_kH$ be the distinct left cosets of H in G.

$|G|=|a_1H|+|a_2H|+|a_3H|+\ldots+|a_kH|$

Since $|a_1H|=|a_2H|=|a_3H|=\ldots=|a_kH|=|H|$

$|G|=k|H|$

Corollary

- Every group with an order of a prime number can not have other subgroups other than two trivial subgroups .

Exercise 2

- Group <$\mathbf{Z}_4$, $+_4$>. Let $G = \mathbf{Z}_4$. Determine all the left cosets of $H = \{[0]\}$ in G.

$+_m$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Exercise 3

- Group <$\mathbf{Z}_4$, $+_4$>. Let $G = \mathbf{Z}_4$. Determine all the left cosets of H = {[0], [1], [2], [3]} in G.

$+_m$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]