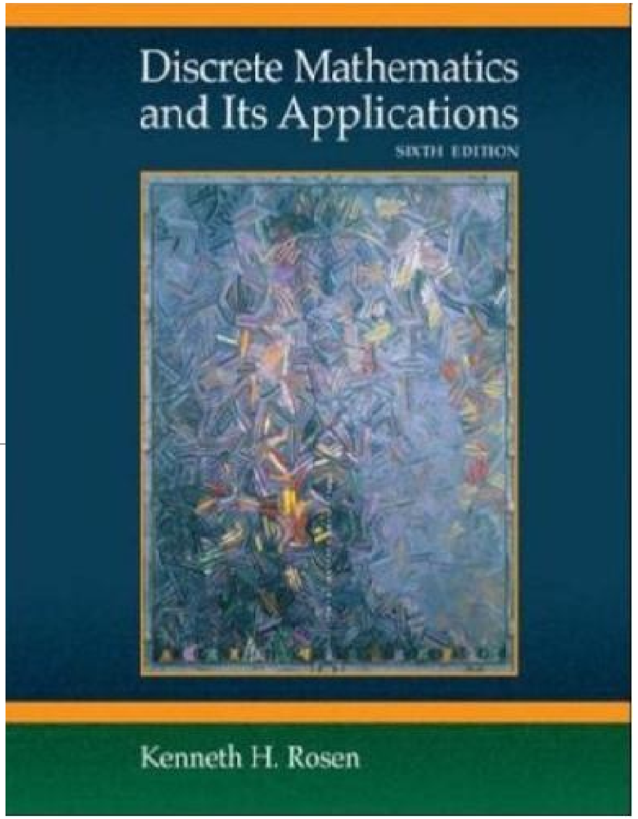
Discrete Mathematics

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

Semigroup

Definition:

- Let <S, $*$> be a algebraic system. S is a nonempty set, $*$ is a binary operation defined on S. <S, $*$> is a semigroup if

(1) $*$ is closed on set S;

(2) $*$ is associative.

- Example:
- <$\mathbf{Z}^+$, +> is a semigroup.
- <$P(S)$, $\cup$> is a semigroup.
- <**Z**, -> is not a semigroup. $(0-1)-2 = -3 \neq 1 = 0-(1-2)$
- <**R**, /> is not a semigroup. $(a/b)/c \neq a/(b/c)$

Exercise 1

- Let set $S = \{a, b, c\}$, $\triangle$ is a binary operation on set S defined by the following table. Show that $\langle S, \triangle \rangle$ is a semigroup.

$\triangle$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

$(\boxed{x} \triangle \boxed{y}) \triangle \boxed{z}$

$= y \triangle z = z$

$x \triangle (y \triangle z)$

$= x \triangle z = z$

操作都为前者，或者都为后者

Monoid

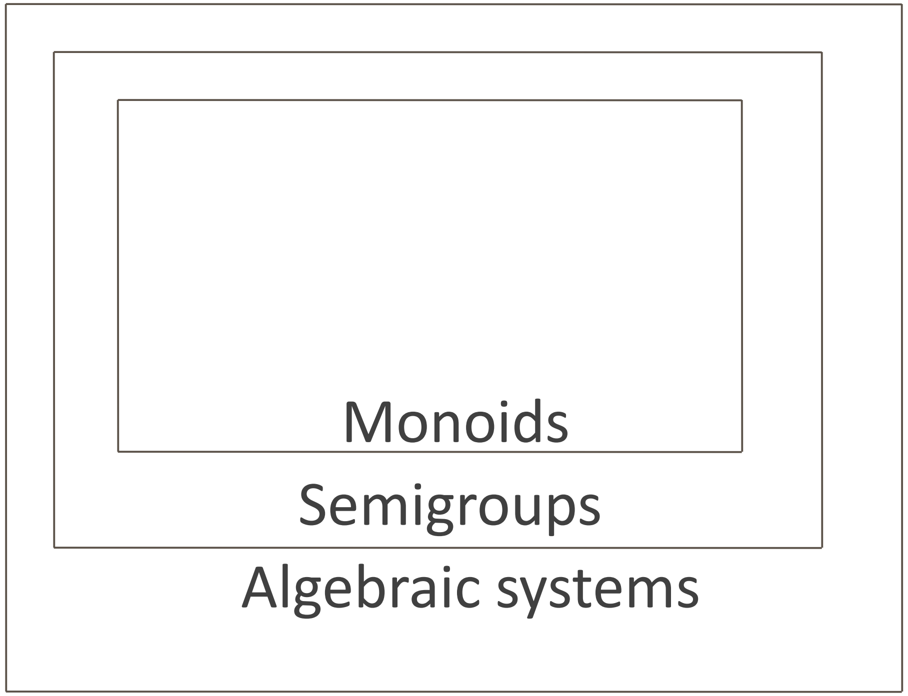
Definition:

- An algebraic system <*S*, ∗> is said to be a monoid if :

(1)∗ is a closed operation on *S*.

(2)∗ is an associative operation on *S*.

(3)There is an identity in *S*.



Example:

- <**R**, +>, <**R**, ·>, <**Z**, ·> are monoids
- <*P*(*S*), ∪> is a monoid. ∅
- <**N**-{0}, +> is not a monoid.

Exercise 2

- Let $A = \{a, b\}$. Which of the following tables define a semigroup on A? Which define a monoid on A?

*	a	b
a	a	b
b	a	a

b * b * b

*	a	b
a	a	b
b	b	b

✓

*	a	b
a	a	a
b	b	b

前者或后者

*	a	b
a	b	b
b	a	a

b * b * b

Exercise 3

- Determine whether the algebraic is a semigroup, a monoid, or neither. If it is a monoid, specify the identity. If it is a semigroup or a monoid, determine if it is commutative.
- <$\mathbf{Z}^+$, max> true, 1, true
- <$\mathbf{Z}^+$, $*$> where $a * b$ is defined as a. true, false, false
- <$P(S)$, $\cap$> true, S, true
- <$\mathbf{Z}$, $*$>, where $a * b = a + b - ab$. true, 0, true

Subsemigroup

Definition:

- Let $<S, *>$ be a semigroup and let T be a nonempty subset of S. If T is closed under operation $*$, then $<T, *>$ is also a semigroup, called a subsemigroup of $<S, *>$.

Example:

- $<[0, 1], \cdot>$, $<[0, 1), \cdot>$ and $<\mathbf{Z}, \cdot>$ are subsemigroups of $<\mathbf{R}, \cdot>$.
- $<$even integers, $\cdot>$ is a subsemigroup of $<\mathbf{Z}, \cdot>$.

Submonoid

Definition:

- Let $<S, *>$ be a monoid with identity e, and let T be a nonempty subset of S. If T is closed under the operation $*$ and $e \in T$, then $<T, *>$ is called a submonoid of $<S, *>$.

Example:

- If $T=\{e\}$, then $<T, *>$ is a submonoid of $<S, *>$.
- $<$even integers, $\cdot>$ is not a submonoid of $<\mathbf{Z}, \cdot>$.

Exercise 2

- (a) $a \in \mathbf{R}$, and $T = \{a^i \mid i \in \mathbf{Z}^+\}$, prove that $<T, \cdot>$ is a subsemigroup of $<\mathbf{R}, \cdot>$.

prove closed t1 * t2 belong to T

T is the subset of R

- (b) $a \in \mathbf{R}$, and $T = \{a^i \mid i \in \mathbf{N}\}$, prove that $<T, \cdot>$ is a submonoid of $<\mathbf{R}, \cdot>$.

prove closed , subset and
1 belong to T.

Homomorphism

Definition:

- Let $<S, *>$ and $<T, \circ>$ be two algebraic systems. A function $f : S \to T$ is called a homomorphism from $<S, *>$ to $<T, \circ>$ if for $\forall a, b \in S, f(a * b) = f(a) \circ f(b)$.
- $<S, *>$ is homomorphic to $<T, \circ>$, denoted by $S \sim T$.
- There can be more than one homomorphisms from one algebraic system to another.

Isomorphism

Definition:

- Let $<S, *>$ and $<T, \circ>$ be two algebraic systems. A function $f : S \to T$ is called an Isomorphism from $<S, *>$ to $<T, \circ>$ if it is a one-to-one correspondence(bijection) from S to T , and if for $\forall a, b \in S, f(a * b) = f(a) \circ f(b)$.
- $<S, *>$ and $<T, \circ>$ are isomorphic, denoted by $S \cong T$.

Procedure of proving $<S, *>$ and $<T, \circ>$ are isomorphic:

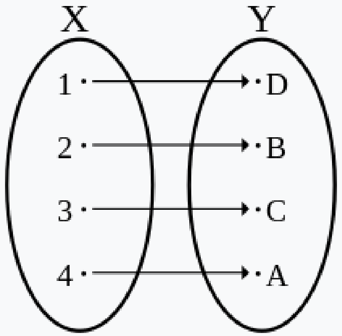
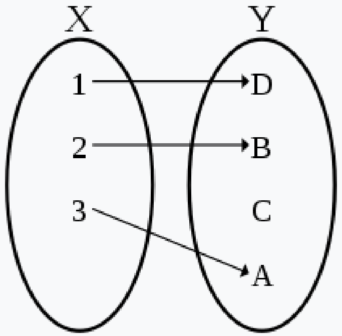
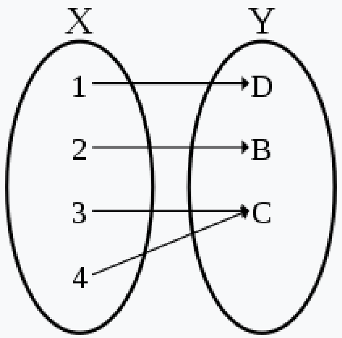
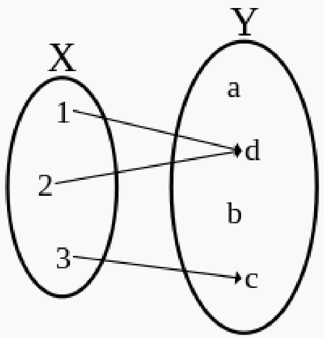
✓Define a function $f : S \to T$ with domain S.

✓Show that f is one-to-one (injection).

✓Show that f is onto (surjection).

✓$f(a * b) = f(a) \circ f(b)$.

Injective, Surjective and Bijective Function

	surjective	non-surjective
injective	 bijective	 injective-only
non-injective	 surjective-only	 general

- The function is **injective**, or **one-to-one**, if each element of the codomain is mapped to by *at most one* element of the domain.
- The function is **surjective**, or **onto**, if each element of the codomain is mapped to by *at least one* element of the domain.
- The function is **bijective** (**one-to-one and onto, one-to-one correspondence, or invertible**) if each element of the codomain is mapped to by *exactly one* element of the domain.

Example 1

- Let T be the set of all even integers. Show that the semigroups <**Z**, +> and <T, +> are isomorphic.

- We define the function $f : \mathbf{Z} \to T$ by $f(a) = 2a$.
- We now show that f is one to one as follows. Suppose that $f(a_1) = f(a_2)$. Then $2a_1 = 2a_2$, so $a_1 = a_2$. Hence f is one to one.
- We next show that f is onto. Suppose that b is any even integer. Then $a = b/2 \in \mathbf{Z}$ and $f(a) = f(b/2) = 2(b/2) = b$, so f is onto.
- We have $f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b)$.

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

Exercise 3

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

- Prove that <**R**$^+$, ·> and <**R**, +> are isomorphic.

- We define the function $f : \mathbf{R}^+ \to \mathbf{R}$ by $f(a) = \log a$.
- We now show that f is one to one as follows. Suppose that $f(a_1) = f(a_2)$. Then $\log a_1 = \log a_2$, so $a_1 = a_2$. Hence f is one to one.
- We next show that f is onto. Suppose that b is any real number. Then $a = e^b \in \mathbf{R}^+$ and $f(a) = f(e^b) = \log e^b = b$, so f is onto.
- We have $f(a \cdot b) = \log a \cdot b = \log a + \log b = f(a) + f(b)$.

Exercise 4

- Let $S = \{a, b, c\}$ and $T = \{x, y, z\}$. Show that $<S, *>$ and $<T, *>$ are isomorphic.

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

$*$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

2

a — y

b — x/z

Theorem 1

- Let $<S, *>$ and $<T, \circ>$ be monoids with identities e and e', respectively. Let $f : S \rightarrow T$ be an isomorphism. Then $f(e) = e'$.
- **Proof:**

Homomorphism

Let b be any element of T. Since f is a bijection, there is an element a in S such that $f(a) = b$.

Then $a = a * e$, $b = f(a) = f(a * e) = f(a) \circ f(e) = b \circ f(e)$.

Similarly, since $a = e * a$, $b = f(e) \circ b$.

Thus for any $b \in T$, $b = b \circ f(e) = f(e) \circ b$, which means that $f(e)$ is an identity for T. Thus since the identity is unique, it follows that $f(e) = e'$.

Example 2

- Let T be the set of all even integers. Determine the semigroups $(\mathbf{Z}, \cdot)$ and $(T, \cdot)$ are isomorphic or not.

No. Since **Z** has an identity and T does not.

是　　　　不一定有

- NOTE: If $<S, *>$ and $<T, \circ>$ are semigroups such that S has an identity and T does not, it then follows from Theorem 1 that $<S, *>$ and $<T, \circ>$ cannot be isomorphic.

Theorem 2

- If f is a isomorphism from a commutative semigroup $<S, *>$ to a semigroup $<T, \circ>$, then $<T, \circ>$ is also commutative.
- **Proof:**

Let t_1 and t_2 be any elements of T.

Then there exist s_1 and s_2 in S with $t_1 = f(s_1)$ and $t_2 = f(s_2)$.

Therefore, $t_1 \circ t_2 = f(s_1) \circ f(s_2) = f(s_1 * s_2) = f(s_2 * s_1) = f(s_2) \circ f(s_1) = t_2 \circ t_1$.

Hence $<T, \circ>$ is also commutative.