Discrete Mathematics 2025 Spring

同济经管 TONGJI SEM

魏可佶 kejiwei@tongji.edu.cn

CAMEA 中国高质量MBA教育认证 AACSB ACCREDITED EQUIS ACCREDITED

- 9.1 Binary Operations and Their Properties
- 9.2 Algebraic Systems
- 9.3 Several Typical Algebraic Systems

9.3.1 Semigroups and Idempotent Elements

- Definition and Examples of Semigroups and Idempotent Elements
- Exponentiation (Power Operations) in Semigroups and Idempotent Elements

- **Definition 9.13 :**

(1) Let V=<S,∘> be an algebraic system, where ∘ is a binary operation. If the operation ∘ is associative, then V is called a ***semigroup***.

(2) Let V=<S,∘> be a semigroup. If there exists an element $e \in S$ that serves as the identity element with respect to the operation ∘, then V is called a ***monoid*** (also known as a **unital semigroup**). To emphasize the existence of the identity element e, the monoid is sometimes denoted as <S,∘,e>.

(3) If the binary operation ∘ in the semigroup V=<S,∘> (V=<S,∘,e>) is commutative, then V is called a ***commutative semigroup.***

- **Note:** ① A semigroup is an algebraic system that satisfies the associative law. ② To verify whether a system is a semigroup, the key points are to check the **closure** of the operation and the **associative law** .

(1) $<Z^+,+>$, $<N,+>$, $<Z,+>$, $<Q,+>$, $<R,+>$ are ***semigroups***, where **+** is ordinary addition. Among them, all except **$<Z^+,+>$** are ***monoids***.

Note: The set of positive integers $<Z^+, +>$ satisfies the associative law but lacks an additive identity (zero), so it is **not** a monoid. The others all have an identity element (zero) and are monoids.

(2) Let ***n*** be a positive integer greater than 1. Both $<M_n(R),+>$ and $<M_n(R),\cdot>$ are ***semigroups and monoids***, where **+** and **·** denote matrix addition and matrix multiplication, respectively.

Note: The identity element for + is the zero matrix, and the identity element for · is the identity matrix.

(3) $<P(B),\oplus>$ is a ***semigroup and also a monoid***, where $\oplus$ denotes the symmetric difference operation on sets.

Note: The symmetric difference identity element in the power set ***P*(*B*)** is the empty set $\varnothing$.

(4) $<Z_n, \oplus>$ is a ***semigroup and also a monoid***, where $Z_n=\{0,1, \dots, n-1\}$ and $\oplus$ denotes addition modulo n.

Note: Modular addition over the set Z_n has the identity element **0**.

(5) $<A^A, \circ>$ is a ***semigroup and also a monoid***, where $\circ$ is the composition of functions.

Note: The set of all functions from A to A, denoted A^A, has the identity element id_A, i.e., $id_A(x)=x$.

(6) $<R^*, \circ>$ is a ***semigroup***, where R^* is the set of nonzero real numbers, and the operation $\circ$ is defined by: $\forall x, y \in R^*$, $x \circ y = y$.

Note: According to the operation definition, for any $x, e \in R^*$, we have $x \circ e = e$. To satisfy $x \circ e = x$, we must have $e = x$. Since x is arbitrary, this means there is no unique $e \in R^*$ satisfying this condition. Therefore, $<R^*, \circ>$ satisfies the associative law but has no identity element, so it is a semigroup but ***not a monoid***.

- Let $V=<S, \circ>$ be a **semigroup** , for any $x \in S$, define :

$$x^1 = x$$

$$x^{n+1} = x^n \circ x \qquad n \in Z^+$$

- In a **monoid** $V=<S,\circ,e>$, for any $x \in S$, define :

$$x^0=e,$$

$$x^{n+1}=x^n \circ x \qquad n \in N$$

- **Power operation rules:**

$$x^n \circ x^m = x^{n+m}$$

$$(x^n)^m= x^{nm} \qquad m, n \in Z^+$$

- **Proof method:** Mathematical induction.

9.3 Several Typical Algebraic Systems

- 9.3.1 Semigroups and Idempotent Elements
- 9.3.2 Groups
- 9.3.3 Rings and Fields
- 9.3.4 Lattices and Boolean Algebras

9.3.2 Groups

- Definition and Determination of Groups
- Klein Four-Group
- Commutative Groups (Abelian Groups)
- Infinite Groups, Finite Groups, Order of a Group
- Exponentiation in Groups, Order of Elements and Generators
- Group Equations
- Groups and Subgroups
- Generated Subgroups, Cyclic Groups
- Permutation Groups

- **Definition 9.14:** Let $<G,\circ>$ be an algebraic system, where $\circ$ is a binary operation. If the operation $\circ$ is associative, there exists an identity element $e \in G$, and for every element $x \in G$, there exists an inverse element $x^{-1} \in G$, then G is called a ***group***.
- **Note:**
  - A group is essentially a monoid (a semigroup with identity) in which ***every element has an inverse***.
  - To verify that an algebraic system is a group, one must ***check***: ① **Closure**, ② **Associativity**, ③ **Existence of an identity element**, ④ **Existence of inverses.**

■ **Examples:**

(1) $<Z,+>$, $<Q,+>$, $<R,+>$ are all *groups*, $<Z^+,+>$ and $<N,+>$ are *not groups*.

(2) $<M_n(R),+>$ is a *group*, whereas $<M_n(R),\cdot>$ is *not a group*.

(3) $<P(B),\oplus>$ is a *group*, where $\oplus$ denotes the symmetric difference operation.

(4) $<Z_n,\oplus>$ is a *group*, where $Z_n=\{0,1,\ldots,n-1\}$, $\oplus$ denotes addition modulo n.

9.3.2 Groups

Group Identification

	Algebraic System	Closure	Associativity	Identity Element	Inverse Element	Group ?
1	$\langle \mathbf{Z},+\rangle$	Satisfy	Satisfy	0	Exist	Yes
2	$\langle \mathbf{Q},+\rangle$	Satisfy	Satisfy	0	Exist	Yes
3	$\langle \mathbf{R},+\rangle$	Satisfy	Satisfy	0	Exist	Yes
4	$\langle \mathbf{Z}^+,+\rangle$	Satisfy	Satisfy	Identity$0 \notin Z^+$	Does not exist	No
5	$\langle \mathbf{N},+\rangle$	Satisfy	Satisfy	Identity$0 \notin N+$	Does not exist	No
6	$\langle \mathbf{M}_n(\mathbf{R}),+\rangle$	Satisfy	Satisfy	0-Matix	A real matrix **A** has an additive inverse **−A**.	Yes
7	$\langle \mathbf{M}_n(\mathbf{R}),\ .\rangle$	Satisfy	Satisfy	I	Only full-rank (nonsingular) matrices have a multiplicative inverse.	No
8	$\langle \mathbf{P}(\mathbf{B}),\oplus\rangle$	Satisfy	Satisfy	$\emptyset$	Itself	Yes
9	$\langle \mathbf{Z}_n,\oplus\rangle$	Satisfy	Satisfy	0	Exist	Yes

- Let $G = \{e, a, b, c\}$, and let the binary operation $\circ$ on G be defined by the following table:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The operation table has the following characteristics:

- ***Symmetry*** - the operation is commutative.
- The ***main diagonal elements*** are all the identity element ***e***.
- Each element composed with itself equals the identity element ***e*** (i.e., each element is its ***own inverse***).
- For any **two elements** among ***a***, ***b***, ***c*** , their operation result ***equals the third element***.

Such a group $\langle G,\circ\rangle$ is generally called the ***Klein four-group.***

- If the binary operation $\circ$ in the group $\langle G,\circ\rangle$ is commutative, then **G** is called a **commutative group** or ***Abelian group***.
- If the group $\langle G,\circ\rangle$ has infinitely many elements, it is called an ***infinite group***, otherwise, it is a ***finite group***.
- For a finite group $\langle G,\circ\rangle$, the number of elements is called the ***order of the group***, denoted as $|G|$.
- **Example1 :**
  - **<Z,+>** and **<R,+>** are **infinite groups.**
  - $<Z_n,\oplus>$ is a **finite group** and is a group of order ***n*** .
  - The **Klein four-group** is a group of order 4.
  - All of the above groups are **commutative (Abelian) groups**.

- **Example 2:** The set of invertible real $n \times n$ matrices (for $n \geq 2$) under matrix multiplication forms a *non-commutative group*.
- **Note:**

① The product AB of two invertible $n \times n$ matrices is also an *invertible* $n \times n$ matrix.

② Matrix multiplication is ***associative***.

③ Any invertible $n \times n$ matrix A has the ***identity matrix*** I.

④ Every invertible $n \times n$ matrix A has an ***inverse matrix*** A^{-1}.

⑤ For two invertible $n \times n$ real matrices A and B, generally $AB \neq BA$(*non-commutativity*).

- **Definition 9.15:** Let G be a group with operation $\circ$, and let $x \in G$, $n \in Z$. The *n-th* power of x, denoted x^n, is defined as:
  - For **positive** integers n, $x^{n+1} = x^n \circ x$.
  - For **zero** , $x^0 = e$ (the identity element)) .
  - For **negative** integers $-n$, $x^{-n} = (x^{-1})^n$, where x^{-1} is the inverse of x in the group G , it satisfies $x \cdot x^{-1} = e$.
- **Example :**
  - In $<Z_3, \oplus>$ we have $2^{-3} = (2^{-1})^3 = 1^3 = 1 \oplus 1 \oplus 1 = 0$.(the identity element of the modulo 3 addition group is **0**, and the inverse of element **2** is **1**)
  - In $<Z, +>$ we have $(-2)^{-3} = ((-2)^{-1})^3 = 2^3 = 2+2+2 = 6$.(the identity element of the integer addition group is 0, and the inverse of element −2 is 2)

In the integer multiplication group $<Z, \cdot>$, **what is** $(-2)^{-3} =$?

- **Definition 9.16:** Let G be a group, and let $x \in G$. The smallest positive integer k such that $x^k = e$ is called the ***order*** (**or** ***period***) of x, denoted by $|x| = k$. We say that x is an element of order k (also called a **k-th power element**). If no such positive integer k exists, then x is called an ***element of infinite order***.

- **Note:**

  ① The order of an element reflects that after applying the group operation k times, the element x returns to the identity element e.

  ② The identity element e in any group G always has order 1.

- **Example:**

(1) In <Z_6,⊕>, **2** and **4** are elements of *order 3*, **3** is an element of *order 2*, **1** and **5** are elements of *order 6*, and **0** is an element of *order 1*.

Note: The identity element of the additive group modulo **6** is **0**, and elements **2** and **4** return to the identity after three applications of addition modulo **6**.

(2) In <Z,+>, 0 is an element of *order 1*, and all other integers have *no (finite) order*.

- **Theorem 9.3** : Let G be a group. Then the power operations in G satisfy:
  (1) $\forall x \in G$, $(x^{-1})^{-1} = x$.
  (2) $\forall x, y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$.
  (3) $\forall x \in G$, $x^n x^m = x^{n+m}$, $n, m \in Z$.
  (4) $\forall x \in G$, $(x^n)^m = x^{nm}$, $n, m \in Z$.
  (5) If G is an abelian (commutative) group, then $(xy)^n = x^n y^n$ (since the binary operation in an abelian group is commutative).
- **Proof** (1): $(x^{-1})^{-1}$ is the inverse of x^{-1}, and x is also the inverse of x^{-1}. By the uniqueness of the inverse, the equation is proved.
- **Proof** (2) : $(y^{-1}x^{-1})(xy)= y^{-1}(x^{-1}x)y = y^{-1}y = e$, and similarly, $(xy)(y^{-1}x^{-1})=e$, therefore $y^{-1}x^{-1}$ is the inverse of xy . By the uniqueness of the inverse, the equation is proved.

Explanation:

- The proofs for (3) (4) (5) : Use mathematical induction to prove that the equation holds for natural numbers ***n*** and ***m***, and then discuss the cases where ***n*** or ***m*** are negative numbers.
- The result in (2) can be extended to the case of finitely many elements, that is, $(x_1 x_2 \dots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \dots x_2^{-1} x_1^{-1}$.
- Equation (5) holds only for abelian (commutative) groups. If ***G*** is a non-abelian (non-commutative) group, then $(xy)^n = \underbrace{(xy)(xy)\dots(xy)}_{n}$.

同济经管 TONGJI SEM

- **Theorem 9.4 :** Let G be a group. For all $\forall a,b\in G$, the equations $ax=b$ and $ya=b$ *have solutions* in G, and the solutions are unique.
- **Proof:** $a^{-1}b$ is the unique solution to the equation $ax=b$.

  ① Substitute $a^{-1}b$ into the left-hand side: $a\,(a^{-1}b) = (a\,a^{-1})\,b = eb = b$ so $a^{-1}b$ is indeed a solution.

  ② Assume c is a solution to $ax = b$, then $ac = b$, hence $c = ec = (a^{-1}a)c = a^{-1}(ac) = a^{-1}b$. Therefore, the uniqueness of the solution is proved.
- Similarly, we can prove that ba^{-1} is the unique solution to the equation $ya = b$.

- **Note:**

  ① Group equations can be used to ***find elements*** in a given group ***G*** that satisfy certain specific relations.

  ② They allow for a ***deeper understanding of the internal structure*** of the group (such as subgroups, homomorphisms, isomorphisms, and automorphisms).

  ③ They can be applied in areas such as ***describing point movements*** in space, cryptographic computations, and the symmetries of quantum systems.

- **Example:** Let the group G=<$P(\{a,b\}),\oplus$>, where $\oplus$ denotes the symmetric difference. We are to solve the group equations:

  (1) $\{a\}\oplus X=\varnothing$ and (2) $Y\oplus\{a,b\}=\{b\}$

- **Solution:**
  - **Equation (1): $\{a\}\oplus X=\varnothing$**

    ①The identity element of G is the empty set $\varnothing$, since for any set A, $A\oplus\emptyset=A$. ② In the symmetric difference group, **every element is its own inverse**, because: $A\oplus A=\emptyset\Rightarrow A^{-1}=A$.③ Therefore: $X=\{a\}^{-1}\oplus\varnothing=\{a\}\oplus\varnothing=\{a\}$.
  - **Equation (2): $Y\oplus\{a,b\}=\{b\}$.**

    To isolate Y, multiply both sides by the inverse of $\{a,b\}$ (which is itself):

    $Y=\{b\}\oplus\{a,b\}^{-1}=\{b\}\oplus\{a,b\}=\{a\}$
  - **Final Answers: $X=\{a\}$, $Y=\{a\}$**

- **Theorem 9.5:** Let G be a group. Then the cancellation laws hold in G, that is, for any $a,b,c \in G$
  - (1) $ab=ac$, **then** $b=c$.
  - (2) $ba=ca$, **then** $b=c$.
- **Proof:**
  (1) $ab=ac \Rightarrow a^{-1}(ab)=a^{-1}(ac) \Rightarrow (a^{-1}a)b=(a^{-1}a)c \Rightarrow b=c$
  (2) Similarly, it can be proved.
- **Example:** Let $G=\{a_1, a_2, \ldots, a_n\}$ be a group of order n , Define $a_iG =\{ a_i a_j \mid j =1,2, \ldots , n \}$, Prove that $a_iG = G$.

- **Example:** Let $G=\{a_1, a_2, \ldots, a_n\}$ be a group of order n， Define $a_iG=\{a_i\, a_j \mid j=1,2, \ldots, n\}$, prove that $a_iG = G$.
- **Explanation:**

① a_iG is the set formed by multiplying a_i with every element in G.

② $a_iG = G$ means the two sets contain the same elements.

③ Although the order of elements may change due to multiplication by a_i , the structure and operational properties of a_iG and G remain unchanged — that is, a_iG is isomorphic to G.

④ The symmetry of the group ensures that the action of any single element on the group structure is uniform — no element can independently alter the overall structure of the group.

- **Proof:** The group G satisfies closure, associativity, the existence of an identity element, and the existence of inverses. To prove $a_iG = G$, we need to show both $a_iG \subseteq G$ and $a_iG \supseteq G$, i.e., that a_iG is simply a rearrangement (permutation) of G.

①By the closure property of the group, the product $a_i\, a_j$ is still in G, so $a_iG \subseteq G$.

②For any element $a_i \in G$, we can write $a_j = a_i\,(a_i^{-1}\, a_j\,)$, i.e., in the form a_ia_k . Because of the existence of inverses and closure, this means for any $a_j \in G$, there exists some $a_k \in G$ such that $a_j = a_ia_k$.

③ For any element $a_i\, a_j$, we have $a_i\, a_j = a_i(a_i^{-1}a_k\,) = a_k \in G$, so $a_iG \supseteq G$ *holds*.

④ Since both $a_iG \subseteq G$ and $a_iG \supseteq G$ hold, we conclude that $a_iG = G$.

- Let the group **G** have elements **{e,a,b,c}**, where **e** is the identity element. The ***multiplication operation rules*** are:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Compute aG

$\cdot$	e	a	b	c
$a \cdot x$	a	e	c	b

The set $aG = \{a,e,c,b\}$ is a permutation of the group G .

- **Theorem 9.6:** Let G be a finite group. Then in the ***operation table*** of G, each row and each column is a ***complete permutation*** of the elements of G, and the permutations in different rows (or columns) are all distinct.
- **Note:**

  ① Only the ***three conditions*** of closure, identity element, and inverses among the four group axioms are necessary to guarantee this result.

  ② The ***associative law*** is a property concerning ternary operations, and it cannot be directly reflected in the binary operation table.

- **Example:** Analyze the following operation table and determine whether it satisfies the necessary conditions of a group.

	a	b	c	d
a	b	c	d	a
b	b	a	c	d
c	c	d	b	a
d	d	b	a	c

(1)

	a	b	c	d
a	a	b	c	d
b	c	d	a	b
c	b	c	d	a
d	d	a	b	c

(2)

	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

(3)

Algebraic Structures and Their Properties

Algebra or Subalgebra System	Structure	Closure	Associativity	Identity element	Inverse element
Semigroup	Binary operation ∘ on the set S	Holds on S	Holds on S		
Subsemigroup	Binary operation ∘ on the subset $T \subseteq S$	Holds on T	Holds on T		
Monoid	Binary operation ∘ on the set M	Holds on M	Holds on M	unit $e \in M$	
Submonoid	Binary operation ∘ on the subset $N \subseteq M$	Holds on N	Holds on N	$e \in N$	
Group	Binary operation ∘ on the set G	Holds on G	Holds on G	$e \in G$	Each element in G exist
Subgroup	Binary operation ∘ on the subset $H \subseteq G$	Holds on H	Holds on H	$e \in H$	Each element in H exist

- **Definition 9.17:** Let ***G*** be a group, and let ***H*** be a **nonempty subset** of ***G*** .
  - If ***H***, under the operation inherited from ***G*** , forms a group, then H is called a ***subgroup*** of ***G*** , denoted ***H≤G***.
  - If ***H*** is a subgroup of ***G*** and H⊊G, then ***H*** is called ***a proper subgroup*** of ***G***, denoted ***H<G***.
  - Every group ***G*** has subgroups. Both ***G*** itself and the set **{*e*}**(where e is the identity element of ***G***) are subgroups of ***G***, and they are called the ***trivial subgroups*** of ***G***.

同济经管 TONGJI SEM

- **Example:**

  For any natural number n, the set *n*Z is a subgroup of the additive group of integers **<Z,+>** .When ***n*≠1**, ***n*Z** is a **proper subgroup** of **Z**.

- **Notes:**
  - The notation ***n*Z** denotes the set of all integer multiples of ***n***, it is a subset of **Z**, and the subgroup **< *n*Z,+>** satisfies the conditions of closure, associativity, existence of the identity element, and existence of inverses.
  - Each natural number ***n*** corresponds to a unique subgroup ***n*Z**. In particular, **0Z**, which contains only the zero element **{0}**, is a **trivial subgroup** of **<Z,+>**.

- **Theorem 9.7 :** Let G be a group and H be a nonempty subset of G. If for any $x,y \in H$, we have $xz= xy^{-1} \in H$, then H is a *subgroup* of G.
  - **Closure Proof:** By the given condition, $xy^{-1}\in H$. Let $y^{-1}=z$ where $z\in H$, then we have $y^{-1}=z$ and $xz=xy^{-1}$. Thus, for any $x,y\in H$, we have $xz\in H$ (because $xz= xy^{-1} \in H$).
  - **Identity Proof:** By the given condition, for any $x,y\in H$, we have $xy^{-1}\in H$. Let $y=x\in H$, then $xx^{-1}\in H$, where e is the identity element of G, we conclude that $e\in H$.
  - **Inverse Proof:** We have already proven that $e\in H$. By the given condition, for any $x\in H$, we have $ex^{-1}\in H$, so $x^{-1}\in H$ holds.

- **Definition 9.8 :**

  Let G be a group. For any $a \in G$, define $H = \{a^k \mid k \in Z\}$, then H is a subgroup of G, called the ***subgroup generated by a***, and is denoted by $<a>$.

- **Proof:**

  Since $a \in <a>$ we know that $<a> \neq \varnothing$.

  Let $a^m, a^l \in <a>$, be arbitrary. Then:

  $$a^m(a^l)^{-1} = a^m a^{-l} = a^{m-l} \in <a>.$$

  By **Theorem 9.7** (the subgroup criterion), we conclude that $<a> \leq G$.

- **Example:**

(1) For the additive group $<Z,+>$, the subgroup generated by 2 is $<2> = \{ 2k \mid k \in Z \} = 2Z$.

(2) In the group $\langle Z_6, \oplus \rangle$, the subgroup generated by 2 is $\langle 2 \rangle = \{0,2,4\}$. Similarly, $<3> = \{ 0, 3\}$, $<1> = <5> = \{ 0, 1, 2, 3, 4, 5\} = Z_6$, $<0> = \{ 0\}$, $<4> = \{ 0, 2, 4 \}$.

(3) The Klein four-group $G=\{e,a,b,c\}$ has the following subgroups generated by each element:

$<e> = \{ e \}$, $<a> = \{ e, a \}$, $<b> = \{ e, b \}$, $<c> = \{ e, c \}$.

- **Definition 9.19:** Let G be a group. If there exists $a \in G$ such that $G = \{ a^k \mid k \in Z \}$, then G is called a *cyclic group*, denoted by $G = \langle a \rangle$, and a is called a *generator* of G .
  - If $G=\langle a \rangle$, and a is an element of order n, then G is called an *n-order cyclic group*, i.e., $G = \{ a^0=e, a^1, a^2, \dots , a^{n-1} \}$.
  - If a is an element of infinite order, then G is called an *infinite cyclic group*, i.e., $G = \{ a^{\pm 0}=e, a^{\pm 1}, a^{\pm 2}, \dots \}$.
- **Examples of Cyclic Groups:**

  (1) The additive group of integers $G = \langle Z,+ \rangle = \langle 1 \rangle = \langle -1 \rangle$, is a typical **infinite cyclic group**, with **2 generators**.

  (2) The additive group modulo **6** $G = \langle Z_6, \oplus \rangle = \langle 1 \rangle = \langle 5 \rangle$, is a **finite cyclic group** with **6** elements, and it has **2 generators**.

■ *n*-order Cyclic Groups & Infinite Cyclic Groups:

① In any cyclic group, $a^0=e$ for all elements a.

② The periodicity of a cyclic group of order n implies that its generator satisfies $a^n=e$ (the identity element). The properties $a^0=e$ and $a^n=e$ are fundamental to cyclic groups, ensuring both ***closure and periodicity***.

③ All cyclic groups of the ***same order are isomorphic***.

- **Theorem 9.8:** Let $G=<a>$ be a cyclic group.

  (1) If G is an infinite cyclic group, then G has exactly ***two generators***, namely a and a^{-1}.

  (2) If G is an n-order cyclic group, then G contains $\varphi(n)$ *generators*, where $\varphi(n)$ denotes Euler's totient function, i.e., the number of positive integers less than n that are coprime to n.

  (3) For any natural number r less than n and coprime to n, a^r is a *generator* of the n-order cyclic group G.