↳ Special Elements in Binary Operations: The Identity Element

- **Definition 9.5:** Let $\circ$ be a binary operation on S.

(1) If there exists an element e_l (or e_r) $\in S$, such that for all $x \in S$

$$e_l \circ x = x \quad (\text{ or } \quad x \circ e_r = x),$$

then e_l (or e_r) is called the ***left identity element*** (or ***right identity element***) of S with respect to the operation $\circ$.

(2) If $e \in S$ is both a left identity and a right identity under $\circ$, then e is called the ***identity element*** (or **unit element**) of S with respect to the operation $\circ$.

- **Note:**

An identity (or unit) element is a ***special element*** under the given operation $\circ$ that does **not change other elements** when the operation is applied.

- **Definition 9.6:** Let $\circ$ be a binary operation on S.

  (1) If there exists an element θ_l (or θ_r)$\in S$, such that for all $x\in S$ we have $\theta_l \circ x = \theta_l$ (or $x \circ \theta_r = \theta_r$), then θ_l (or θ_r) is called the ***left zero element*** (or ***right zero element***) of S with respect to the operation $\circ$.

  (2) If an element $\theta \in S$ is both a left zero element and a right zero element under $\circ$, then θ is called the ***zero element*** of S with respect to the operation $\circ$.

- **Note:** A zero element is a ***special element*** that ***"absorbs" other elements*** when combined with them under a specific binary operation, always producing itself as the result.

- **Definition 9.7:** Let e be the identity (unit) element of S with respect to the operation $\circ$.

(1) For any $x \in S$, if there exists y_l (or y_r) $\in S$ such that

$$y_l \circ x = e \ (\text{or } x \circ y_r = e),$$

then y_l (or y_r) is called the ***left inverse*** (or ***right inverse***) of x.

(2) If $y \in S$ is both the left inverse and the right inverse of x, then y is called the ***inverse*** of x.

(3) If the inverse of x exists, then x is said ***to be invertible***.

↳ Special Elements in Binary Operations(e.g.)

Set	Operations	identity element	Zero element	Inverse
Z, Q,R	+	0	NO	$-x$
	×	1	0	x^{-1}
M_n(R)	+	θ	NO	$-X$
	×	E	θ	X^{-1} （X is an invertible matrix）
$P(B)$	$\cup$	$\varnothing$	B	$\varnothing$
	$\cap$	B	$\varnothing$	B
	$\oplus$	$\varnothing$	NO	X

- **Membership of the *Multiplicative Inverse* x^{-1}:**
  - In the set of integers **Z**, *only 1 and −1 have multiplicative inverses within Z*, the multiplicative inverses of all other integers do **not** belong to **Z**.
  - In the set of rational numbers **Q**, *all nonzero elements have multiplicative inverses*, and these inverses also belong to **Q**.
  - In the set of real numbers **R**, *all nonzero elements have multiplicative inverses*, and these inverses also belong to **R**.

↳ Uniqueness of the Identity Element Theorem

- **Theorem 9.1:** Let $\circ$ be a binary operation on S. If e_l and e_r are the left identity and right identity elements of S with respect to $\circ$, respectively, then we have $e_l = e_r = e$, and e is the ***unique identity element*** of S under $\circ$.
- **Proof:**

  ①By the definition of the left identity, we have $e_l \cdot e_r = e_r$. By the definition of the right identity, we have $e_l \cdot e_r = e_l$.

  ②Combining these two equations, we get $e_l = e_l \cdot e_r = e_r$.

  ③We denote $e_l = e_r$ as e. Now, suppose e' is also an identity element of S, then $e' = e \circ e' = e$.

  ④Therefore, the identity element e is unique.
- Similarly, one can prove the ***uniqueness theorem for the zero element***.

↳ Uniqueness of the Identity Element Theorem

- **Theorem 9.2:** Let $\circ$ be an associative binary operation on S, and let e be the identity element under this operation. For any $x \in S$, if there exists a left inverse y_l and a right inverse y_r , then $y_l = y_r = y$, and y is the *unique inverse* of x.
- **Proof:**

  ① Since $y_l \circ x = e$ and $x \circ y_r = e$,we have $y_l = y_l \circ e = y_l \circ (x \circ y_r)$
  $= (y_l \circ x) \circ y_r = e \circ y_r = y_r$.

  ② Let $y_l = y_r = y$, then y is an inverse of x.

  ③ Now, suppose $y' \in S$ also an inverse of x, then $y' = y' \circ e = y' \circ (x \circ y)$
  $= (y' \circ x) \circ y = e \circ y = y$.

  ④ Therefore, y s the unique inverse of x.

- **Note:** For *associative binary operations*, an invertible element x has a *unique inverse*, denoted as x^{-1}.

- **Definition 9.8:** Let $\circ$ be a binary operation on V, if $\forall\, x, y, z \in V$,
  If $x \circ y = x \circ z$, and x is not a zero element, then $y = z$ (Left cancellation).
  If $y \circ x = z \circ x$, and x is not a zero element, then $y = z$ (Right cancellation).
  then the operation $\circ$ is said to satisfy the ***cancellation law*** .
- **Examples:**
  (1) Z, Q, R satisfy the cancellation law under ordinary addition and multiplication.
  (2) $M_n(R)$ satisfies the cancellation law under matrix addition, but does not satisfy the cancellation law under matrix multiplication.
  (3) Z_n satisfies the cancellation law under addition modulo n, it also satisfies the cancellation law under multiplication modulo n when n is prime. However, when n is composite, multiplication modulo n does not satisfy the cancellation law.
  (4) Set union and intersection do not satisfy the cancellation law. For example, $\{1\}\cup\{1,2\}=\{2\}\cup\{1,2\}$, but $\{1\}\neq\{2\}$.

- **Example:** Let $\circ$ be a binary operation on **Q**, defined by,

$$\forall x,\ y \in \mathbf{Q},\quad x \circ y = x+y+2xy,$$

(1) Determine whether the operation $\circ$ satisfies the commutative law and the associative law, and explain why.

(2) Find the identity element, the zero element, and the inverse elements (for all invertible elements) under the operation .

- **Solution (1):**

① The $\circ$ operation is commutative. For any $x,\ y \in \mathbf{Q}$,

$$x \circ y = x+y+2xy = y+x+2yx = y \circ x\ .$$

② The $\circ$ operation is associative. For any $x,\ y,\ z \in \mathbf{Q}$,

$$\begin{aligned}(x \circ y) \circ z &= (x+y+2xy) + z + 2(x+y+2xy)\,z \\ &= x+y+z+2xy+2xz+2yz+4xyz\end{aligned}$$

$$\begin{aligned}x \circ (y \circ z) &= x + (y+z+2yz) + 2x(y+z+2yz) \\ &= x+y+z+2xy+2xz+2yz+4xyz\end{aligned}$$

■ Solution (2):

- Find the identity element e :

  ① Assume that the identity element and the zero element under the $\circ$ operation are e and θ, respectively. For any x, we have $x\circ e = x$, then $x+e+2xe = x \Rightarrow e = 0$. ② Since the $\circ$ operation is commutative, 0 is the identity element (unit element).

- Find the zero element θ :

  ① For any x, we have $x \circ \theta = \theta \circ x = \theta$, that is $x+\theta+2x\theta = \theta \Rightarrow x+2x\theta = 0 \Rightarrow \theta = -1/2$. ② $-1/2$ zero element.

- Find the inverse y :

  ① Let y be the inverse of x. Then we have $x \circ y = e = 0$,that is $x+y+2xy = 0$.

  ② $y = -\frac{x}{2x+1}$, this means that every x （$x \neq -\frac{1}{2}$ ） has an inverse y.

- **Example:** Here are three operation tables:
  - **(1)** Identify which operations are **commutative**, **associative**, and **idempotent**.
  - **(2)** Find the **identity element**, **zero element**, and the **inverse** of all invertible elements for each operation.

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

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

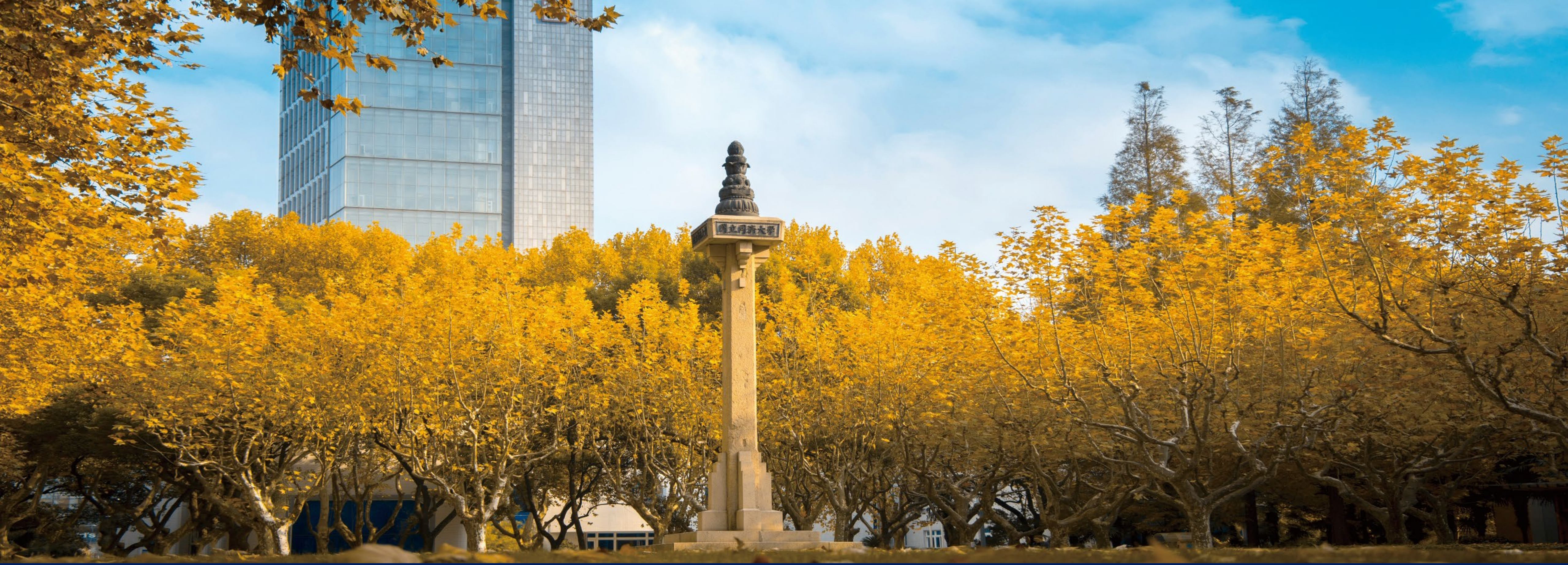
$\bullet$	a	b	c
a	a	b	c
b	b	c	c
c	c	c	c

- **Solve (1)** : ① $*$ satisfies the commutative law and associative law. ② $\circ$ satisfies the associative law and idempotent law. ③ $\bullet$ satisfies the **commutative law** and **associative law**.
- **Solve (2)** : ① $*$ the identity element is b, no zero element， $a^{-1}=c$, $b^{-1}=b$, $c^{-1}=a$. ② $\circ$ there is no identity element and no zero element, there are no invertible elements. ③ $\bullet$ the identity element is a， the zero element is c， $a^{-1}=a$． b, c are not invertible.

9.1 Binary Operations and Their Properties

Objective：

Key Concepts：



Discrete Mathematics 2025 Spring

魏可佶 kejiwei@tongji.edu.cn

- 9.2.1 Definition and Examples of Algebraic Systems
- 9.2.2 Subalgebraic Systems and Product Algebraic Systems
- 9.2.3 Homomorphisms and Isomorphisms of Algebraic Systems

↳ The subject matter of algebra and its process of abstraction

- ***Algebra*** (in the broad sense), as a major branch of mathematics, studies various algebraic structures as well as related operations, equations, and theories. The objects of algebra are not limited to numbers, but extend to all kinds of abstract structures.
- The development of algebra is a gradual process of ***abstraction and systematization*** — from the basic concepts in elementary algebra (such as addition, multiplication, variables, and polynomials), to linear algebra (vectors, matrices, and determinants), and then to the more abstract structures of higher algebra (such as groups, rings, and fields). It represents humanity's continuous pursuit and exploration of the unknown.

- An *algebraic structure* (or type of algebraic system) is an **abstract mathematical concept** used to describe operations defined on one or more sets, along with their (abstract) properties. These operations must satisfy specific rules and axioms. Examples include algebraic structures such as groups, rings, and fields.
- An *algebraic system* is a concrete realization or **instance of an algebraic structure**,consisting of a specific set and concrete operations defined on that set.
  - **For example:**
    - Addition on the set of *natural numbers* $\mathbb{N}$.
    - Addition and multiplication on the *set of integers* $\mathbb{Z}$.
    - Addition and multiplication on the *set of real numbers* $\mathbb{R}$.
    - Addition and multiplication on the set of ***n*-order** ($n \geq 2$) *real matrices* $M_n(\mathbb{R})$.
    - Addition and multiplication modulo *n* on *the set* $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.
    - Union,intersection,and absolute complement on the *power set* $\mathcal{P}(S)$ of a set S.

↳The formal definition of an algebraic system

- **Definition 9.9:** A non-empty set S together with k operations f_1, f_2, … , f_k (where each f_i n_i-**ary** operation, i=1,2,…,k) forms a system called an ***algebraic system*** (or simply, an **algebra**), denoted as **$<S, f_1, f_2, …, f_k>$**.
- **Examples:**
  - $<N, +>$, $<Z, +, \cdot>$, $<R, +, \cdot>$ are algebraic systems, where + and · represent the usual addition and multiplication.
  - $<M_n(R), +, \cdot>$ is an algebraic system, where + and · denote addition and multiplication of $n \times n$ ($n \geq 2$) real matrices.
  - $<Z_n, \oplus, \otimes>$ is an algebraic system, $Z_n = \{0, 1, …, n-1\}$, $\oplus$ and $\otimes$ denote addition and multiplication modulo n, for $x, y \in Z_n$, $x \oplus y = (x + y) \bmod n$, $x \otimes y = (xy) \bmod n$.
  - $<P(S), \cup, \cap, \sim>$ is also an algebraic system, $\cup$ and $\cap$ are union and intersection, and ~ is the absolute complement.

↳ The constituent elements of an algebraic system

(1) A ***basic set*** **(carrier set)** that contains all the elements.For example, in the ring of integers, the set is the set of all integers **Z** .

(2) ***Operations*** defined on the set. Common operations include unary and binary operations.

(3) Some algebraic systems require the definition of certain ***special elements or algebraic constants*** (such as the **zero element** or **identity element** for a binary operation). For example, the element **0** in integer addition, or the element **1** in integer multiplication.

(4) Certain operations may require the existence of ***inverse elements***. For example, for an integer n, its additive inverse is $-n$.

(5) An algebraic system typically comes with a set of ***axioms*** that must be satisfied, such as the associative law, commutative law, and distributive law.

- **Note:** In addition to these basic components, different algebraic structures (such as groups, rings, fields, vector spaces) also have their own ***specific components and axioms*** that must be satisfied.
- **Example:**
  - **<Z, + >**has the identity element **0**,and can also be written as <Z, + ,0 >.
  - **<*P*(*S*),∪,∩,~>** the identity elements for ∪ and ∩ are the empty set ∅ and the universal set ***S*** , respectively. It can also be written as <*P*(*S*),∪,∩,~, ∅ , *S* >.

- 9.2.1 Definition and Examples of Algebraic Systems
- 9.2.2 Subalgebraic Systems and Product Algebraic Systems
- 9.2.3 Homomorphisms and Isomorphisms of Algebraic Systems