- **Theorem 9.9:** Let $G=\langle a\rangle$ be a cyclic group. Then:
  (1) A **subgroup** of G is also a *cyclic group*.
  (2) If $G=\langle a\rangle$ is an infinite cyclic group, then every **subgroup** of G, except for $\{e\}$, is also an *infinite cyclic group*.
  (3) If $G=\langle a\rangle$ is an **n-order cyclic group**, then for every positive divisor d of n, G contains exactly one *subgroup of order d*.
- **Examples(1)** : $G=\langle Z,+\rangle$ is an infinite cyclic group. For any natural number $m\in N$, the m-th power of **1** is m, and the subgroup generated by m is mZ, where $m\in N$. That is,
  $\langle 0\rangle = \{ 0 \}=0Z$, $\langle 2\rangle = \{ 2k \mid k\in Z \} = 2Z$
  $\langle m\rangle = \{ mz \mid z\in Z \} = mZ, \quad m>0$

- **Example (2):** $G=Z_{12}$ is a cyclic group of order **12**. The positive divisors of **12** are **1**, **2**, **3**, **4**, **6**, and **12**. For each positive divisor ***d***, we construct a subgroup of order ***d***.
  - **Notes:**

  In the additive group modulo **12**, $<Z_{12},+>$, a nonempty subset H is a subgroup if and only if:

  ① It contains the identity element **0**.

  ② It is closed under addition modulo 12: if $a,b \in H$, then $(a + b)$ mod $12 \in H$.

  ③ It contains additive inverses: for every $a \in H$, $-a$ mod $12 \in H$.

- **Construct subgroups of Z_{12} by divisors of 12.**
  - **Order 1 subgroup:** <12> = <0> = {0}
  - **Order 2 subgroup:** Divide 12 by its divisor 2 to get the generator 6. <6> = { 0, 6 }
  - **Order 3 subgroup:** Divide 12 by 3 to get the generator 4. <4> = {0, 4, 8 }
  - **Order 4 subgroup:** Divide 12 by 4 to get the generator 3. <3> = {0, 3, 6, 9 }
  - **Order 6 subgroup:** Divide 12 by 6 to get the generator 2. <6> = {0, 2, 4, 6, 8, 10 }
  - **Order 12 subgroup:** Divide 12 by 12 to get the generator 1. <1> = Z_{12}
- **Verification of ⟨4⟩:** ① **Closure**: For any two elements in the set {0,3,6,9}, their sum is still in the set. ② **Inverses**: The inverse of 0 is 0(0+0=0). The inverse of 3 is 9(3+9=12≡0mod 12). The inverse of 6 is 6(6+6=12≡0mod 12). The inverse of 9 is 3(9+3=12≡0mod 12). All inverses are contained in the set.

- **Definition 9.20:** Let $S = \{ 1, 2, \ldots, n \}$, A bijective function $\sigma: S \to S$ is called a **permutation** of the set ***S***, and is referred to as an ***n-permutation***.

  An ***n***-permutation σ is usually written as: $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

- **Example:** $S = \{ 1, 2, 3, 4, 5 \}$, **then**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$

All are ***5-permutations*** on the set ***S***.

- A permutation is a **rearrangement of *n* group elements**. The ***n*!** possible arrangements correspond to ***n*!** ***permutations***, and the set of all such permutations is denoted by S_n.
- Under the operation of permutation composition (denoted $\circ$), S_n forms a group $< S_n, \circ >$, The identity permutation I_n serves as the identity element (neutral element) of the group. The inverse of a permutation σ is given by: $\boldsymbol{\sigma^{-1}} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$
- The group $< S_n, \circ >$ is called the **symmetric group of degree *n***, and any subgroup of S_n is called an ***n-permutation group***.

Notes:

- The symmetric group of degree *n*, denoted ***S_n*, contains all possible n! permutations** (arrangements) of ***n*** elements. These permutations preserve the group structure and represent mathematical symmetry.
- An *n*-permutation group is any specific set of permutations of ***n*** elements, its number of elements can be less than ***n***!, The group ***S_n* is the largest n-permutation group**.

- Permutations can be represented in several ways, including **two-line notation**, **cycle notation**, **matrix representation**, and **list notation**.
- A permutation $\boldsymbol{\sigma} \in \boldsymbol{S_6}$ can be written in ***two-line notation*** as: $\boldsymbol{\sigma} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} \\ \mathbf{1} & \mathbf{5} & \mathbf{2} & \mathbf{4} & \mathbf{3} & \mathbf{6} \end{pmatrix}$. This can also be expressed in ***cycle notation*** as: $\boldsymbol{\sigma} = (\mathbf{253})$, which means **2** maps to **5**, **5** maps to **3**, and **3** maps to **2**.
- If a cycle has length ***m***, then $\boldsymbol{\sigma}$ is called an ***m-cycle***, ***m*=2** it's called a ***transposition***, ***m*=1** it's the ***identity permutation***.
- **Any permutation** $\boldsymbol{\sigma}$ can be expressed as a product of ***disjoint cycles***.

  For example: $\boldsymbol{\sigma} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} \\ \mathbf{6} & \mathbf{5} & \mathbf{2} & \mathbf{4} & \mathbf{3} & \mathbf{1} \end{pmatrix} = (\mathbf{16})(\mathbf{253})$

- ***Identity Permutation***: A permutation that does not change the position of any element. It is denoted by ***e*** or ***id***.
  - **Example:** In S_3, the identity permutation is $e=(1)(2)(3)$.
- ***Transpositions***: A permutation that swaps exactly two elements while leaving all others unchanged. It is denoted as (ab) .
- ***Cycles***: A permutation that cycles a group of elements in a specific order, leaving all other elements unchanged. It is written (a1a2⋯ak) .
- ***Composition of Permutations***: The operation of applying two or more permutations in sequence, denoted by ∘. For example, **σ∘τ** means apply **τ** first, then **σ**.
  - **Example:** In S_3, if $\sigma=(123)$ and $\tau=(23)$, then $\sigma\circ\tau=(123)\circ(23)=(12)$.

- *Inverse Permutations*: A permutation that reverses the mapping of a given permutation, such that $\sigma\circ\sigma^{-1}=e$. It is denoted as σ^{-1} .
  - **Example:** In S_3, if $\sigma=(123)$,**then** $\sigma^{-1}=(132)$.
- **Example 1:** Let $S = \{1, 2, 3\}$, $\sigma=(123)$ and $\tau=(23)$, find the compositions $\sigma\circ\tau$ *and* $\tau\circ\sigma$.
  - **Solution 1:** To find the composition $\sigma\circ\tau$.

① Express τ : $\tau=(23)=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$.

② Apply σ to the result of τ, Using composition $(\sigma\circ\tau)(x)=\sigma(\tau(x))$:

$\sigma(\tau(1))=\sigma(1)=2$, $\sigma(\tau(2))=\sigma(3)=1$, $\sigma(\tau(3))=\sigma(2)=3$.

③ Final Result $\sigma\circ\tau=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(12)$.

- **Solution 2:** To find the composition $\boldsymbol{\tau\circ\sigma}$.

① Express $\boldsymbol{\sigma}$: $\boldsymbol{\sigma}$ =(123)= $\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$.

② Apply $\boldsymbol{\tau}$ to the result of $\boldsymbol{\sigma}$: Using composition $(\tau\circ\sigma)(x)=\tau(\sigma(x))$:

$\tau(\sigma(1))=\tau(2)=3,\ \ \tau(\sigma(2))=\tau(3)=2,\ \tau(\sigma(3))=\tau(1)=1.$

③ Final Result $\boldsymbol{\tau\circ\sigma} = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$= (13).

- The results of the compositions $\boldsymbol{\sigma\circ\tau}$ and $\boldsymbol{\tau\circ\sigma}$ are different, which shows that in the symmetric group S_3 , the composition of permutations is ***not commutative***, that is, $\boldsymbol{\sigma\circ\tau\neq\tau\circ\sigma}$.

TONGJI SEM 同济经管

- **Example:** Let S = {1, 2, 3}. The symmetric group of degree 3, S_3 = **{(1), (1 2), (1 3), (2 3), (1 2 3), (1 3 2)}**, has the following composition table under the operation ∘:

∘	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 2 3)	(1 3 2)	(1 3)	(2 3)
(1 3)	(1 3)	(1 3 2)	(1)	(1 2 3)	(2 3)	(1 2)
(2 3)	(2 3)	(1 2 3)	(1 3 2)	(1)	(1 2)	(1 3)
(1 2 3)	(1 2 3)	(2 3)	(1 2)	(1 3)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(1 3)	(2 3)	(1 2)	(1)	(1 2 3)

The results of **permutation operations** can be ***verified by checking the table***.

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

9.3.3 Rings and Fields

同济经管
TONGJI SEM

- Definition and Examples of Rings
- Operational Properties of Rings
- Subrings and Their Characterization
- Ring Homomorphisms
- Integral Domains and Fields

	Group	Ring
Definition	A set with a **single binary operation** that satisfies the properties of closure, associativity, identity element, and inverse element.	A set equipped with **two binary operations** (addition and multiplication) that satisfy specific properties.
Operations	A single operation (usually **addition or multiplication**)	**Addition and Multiplication**
Additive Structure	Ignore	Form an **Abelian group** (commutative group)
Multiplicative Structure	Form a **group**	Form a **semigroup**, not necessarily a group.
Identity Element	Requires an **identity element**	An additive identity **0** is required, while the multiplicative identity **1** is optional.
Commutativity	**Not necessarily commutative**; if it is commutative, it is called an Abelian group.	**Addition is commutative**, while multiplication is not necessarily commutative.

	Group	Ring
Example	(Z,+),(R*,·)	(Z)，(R[x])
Goal	Study of symmetry and transformations, abstract algebraic structures, and representation theory.	Study of structures with two operations, polynomial theory, and algebraic number theory.
Application	Physics (symmetry operations), Chemistry (molecular symmetry), Cryptography (encryption algorithms), Computer Science (graph theory)	Linear Algebra (matrix rings), Coding Theory, Computer Algebra, Quantum Mechanics

Understanding Symmetry in Groups:

(1) ***Symmetry*** refers to the property of an object remaining unchanged under certain operations. These operations can include rotations, reflections, translations, etc.

(2) ***Group symmetry*** refers to the invariance of an object under a set of operations that **satisfy the four fundamental properties** of a group: closure, associativity, existence of an identity element, and existence of inverse elements.

(3) The ***symmetry of cyclic groups*** (a special type of group) is reflected in structures with periodic repetition.

(4) Each ***permutation in the symmetric group*** S_n (a special group) can be viewed as a **symmetric transformation** of the positions of elements.

- **Example:** The symmetry group D_3 of an equilateral triangle with vertices A, B, and C includes the following transformations that illustrate group symmetry:

(1) A **120-degree clockwise rotation** corresponds to the cyclic permutation (ABC) in group D_3 .

(2) A **240-degree clockwise rotation** corresponds to the *cyclic permutation* (ACB) in group D_3 .

(3) A **reflection across the line connecting vertex A and the midpoint of the opposite side** corresponds to the ***transposition*** (BC) in group D_3 .

(4) A **reflection across the line connecting vertex B and the midpoint of the opposite side** corresponds to the ***transposition*** (AC) in group D_3 .

(5) A **reflection across the line connecting vertex C and the midpoint of the opposite side** corresponds to the ***transposition*** (AB) in group D_3 .

- **Definition 9.21:** Let <*R*,+,·> be an algebraic system, where *R* is a set, and + and · are binary operations. **If** the following conditions are satisfied:
  (1) <*R*,+> forms an Abelian group (commutative group) ,
  (2) <*R*,·> forms a semigroup,
  (3) Multiplication (·) is distributive over addition (+),

  then <*R*,+,·>is called a ***ring***.

Examples:

(1) The sets of integers, rational numbers, real numbers, and complex numbers form rings under the usual addition (+) and multiplication (·). They are called the ***ring of integers*** **Z**, the ***ring of rational numbers*** **Q**, the ***ring of real numbers*** **R**, and the ***ring of complex numbers*** **C**, respectively.

(2) The set $M_n(R)$ of all $n \times n$ real matrices (with $n \geq 2$) forms a ring under matrix addition and matrix multiplication, called the ***ring of n×n real matrices***.

(3) Let $Z_n=\{0,1,\ldots,n-1\}$, where $\oplus$ and $\otimes$ denote addition and multiplication modulo n, respectively. Then $\langle Z_n, \oplus, \otimes \rangle$ forms a ring called the ***ring of integers modulo n***.

(4) The power set $P(B)$ of a set B forms a ring under the symmetric difference operation $\oplus$ and the intersection operation $\cap$.

↳ Commutative, unital, and zero-divisor-free rings

- In a ring $<R,+,\cdot>$
  - If multiplication ($\cdot$) is commutative, then R is called a ***commutative ring***.
  - If there exists a multiplicative identity for $\cdot$, then R is called a ***ring with identity*** (or ***unit ring***).
  - If there exist elements a, $b \in R$ such that $a \neq 0$, $b \neq 0$, but $a \cdot b = 0$, then a is called a ***left zero divisor*** and b a ***right zero divisor*** in R.
  - A ring that contains no (left or right) zero divisors is called a ***domain without zero divisors***, or simply a ***domain***.

↳ Commutative, unital, and zero-divisor-free rings

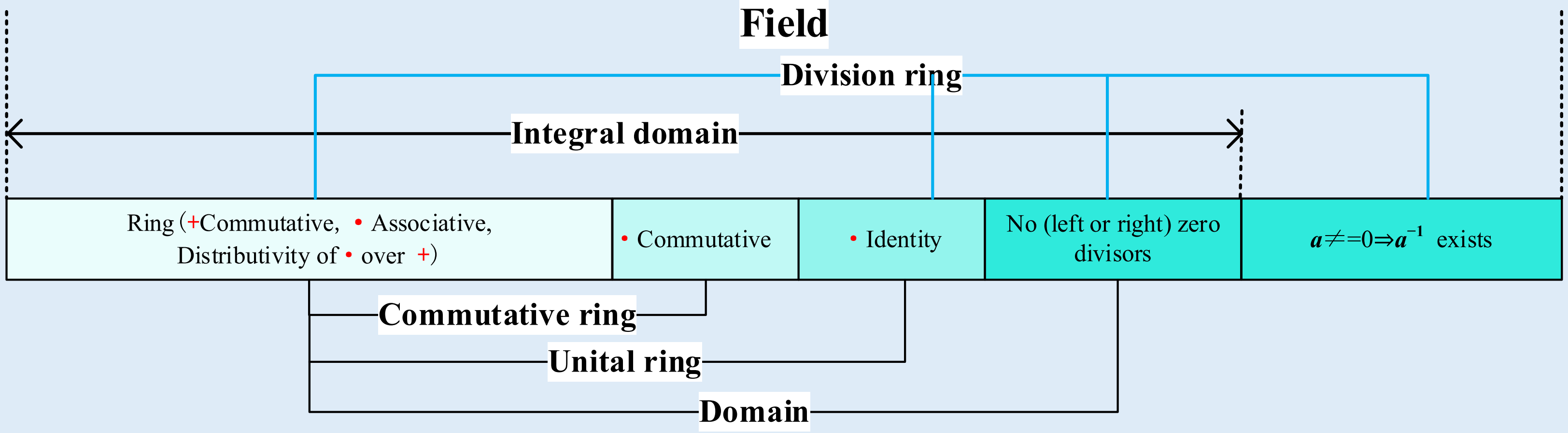
Ring	Commutative Ring	Ring with Identity	Integral Domain
$<Z,+,\cdot>$	√	multiplicative identity 1	√
$<Q,+,\cdot>$	√	multiplicative identity 1	√
$<R,+,\cdot>$	√	multiplicative identity 1	√
$<C,+,\cdot>$	√	multiplicative identity 1	√
$<M_n(\mathrm{R}),+,\cdot>$	No	With multiplicative identity: the identity matrix	There exist nonzero matrices A and B such that $A\cdot B = 0$.
$<Z_n,\oplus,\otimes>$	√	multiplicative identity 1	$\mathbb{Z}_6$ has zero divisors, since $2 \otimes 3 = 0$.

Definition 9.22:

(1) If the ring $<R,+,\cdot>$ is a **commutative ring**, has a **multiplicative identity**, and contains **no zero divisors**, then R is called an ***integral domain***.

(2) If the ring $<R,+,\cdot>$ has **at least two elements**, is a **ring with identity** and **has no zero divisors**, and for every $a \in R$ with $a \neq 0$, there exists $a^{-1} \in R$, then R is called a ***division ring***.

(3) If the ring $<R,+,\cdot>$ is both an **integral domain** and a **division ring**, then R is called a ***field***.



↳ Examples: Domains, Division Rings, and Fields

Ring	Commutative	Has Unity	No Zero Divisors	Integral Domain	Division Ring	Field
<Z,+, ·>	✓	Unity = 1	✓	✓	✗ Only ±1 invertible	✗
<Q, +, ·>	✓	Unity = 1	✓	✓	✓ All nonzero elements invertible	✓
<R,+, ·>	✓	Unity = 1	✓	✓	✓	✓
<C,+, ·>	✓	Unity = 1	✓	✓	✓	✓
<M_n(R) ,+, ·>	• Noncommutative	Unity = Identity Matrix	✗ $\exists A,B\neq 0, A \cdot B = 0$	✗	✗ nonzero matrix has no multiplicative inverse	✗
<Z_n,⊕,⊗>	✓	Unity = 1	$\mathbb{Z}_6$ has zero divisors, since 2 ⊗ 3 = 0	If n prime → ✓	If n prime → ✓	If n prime → ✓

- **Theorem 9.10:** Let <R,+,·> be a ring, then
  (1) $\forall a \in R,\ a \cdot 0 = 0 \cdot a = 0$.
  (2) $\forall a, b \in R,\ (-a)b = a(-b) = -(ab)$.
  (3) $\forall a, b \in R,\ (-a)(-b) = ab$.
  (4) $\forall a, b, c \in R,\ a(b-c) = ab-ac,\ \ (b-c)a = ba-ca$.
- **Example:** Let <R,+,·> be a ring, $\forall a, b \in R$, compute $(a+b)^3$ and $(a-b)^2$.
  - **Solve:** $(a+b)^3 = (a+b)(a+b)(a+b) = (a^2+ba+ab+b^2)(a+b)$

    $= a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3$

    $(a-b)^2 = (a-b)(a-b) = a^2-ba-ab-b(-b) = a^2-ba-ab+b^2$
  - When R is a commutative ring (i.e., $ab=ba$), it can be further simplified to:

    $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$

    $(a-b)^2 = a^2-2ab+b^2$

9.3.4 Lattices and Boolean Algebras

同济经管 TONGJI SEM

- Definition and Construction of Lattices
- Properties of Lattices - Principle of Duality
- Distributive Lattices, Bounded Lattices, Complemented Lattices

Characteristics	Set S	Partially Ordered Set $<S, \preccurlyeq>$
Definition	An ***unordered*** set of distinct elements.	A set S equipped with a binary relation that is ***reflexive***, ***antisymmetric***, and ***transitive***.
Relations between elements	There is ***no specific order*** relationship among the elements.	There is a ***partial order*** among the elements, not all elements are comparable.
Method of Representation	Represented using { }	Represented by a ***Hasse diagram*** or a directed graph.
Operations	Union (∪), intersection (∩), difference (\\), etc	Least upper bound, greatest lower bound, chain, antichain.
Example	{1,2,3}	$\{a,b,c\}$ equipped with the relations $a \le b$, $b \le c$

Reflexivity: For all $a \in S$, $a \preccurlyeq a$.

Antisymmetry: For all $a,b \in S$, if $a \preccurlyeq b$ *and* $b \preccurlyeq a$, *then* $a=b$.

Transitivity : For all $a,b,c \in S$, if $a \preccurlyeq b$ *and* $b \preccurlyeq c$, *then* $a \preccurlyeq c$.

- **Definition 9.23:** Let $<S,\preccurlyeq>$ be a partially ordered set. If $\forall x, y \in S$ the set $\{x,y\}$ has both a least upper bound and a greatest lower bound, then S is said to form a *lattice* under the partial order $\preccurlyeq$.
  - Due to the uniqueness of the least upper bound and greatest lower bound, finding the least upper bound and greatest lower bound of $\{x,y\}$ can be treated as *binary operations* $\vee$ and $\wedge$ on x and y , where $x \vee y$ denotes the least upper bound of x and y, and $x \wedge y$ denotes the greatest lower bound of x and y.

- **Note:**

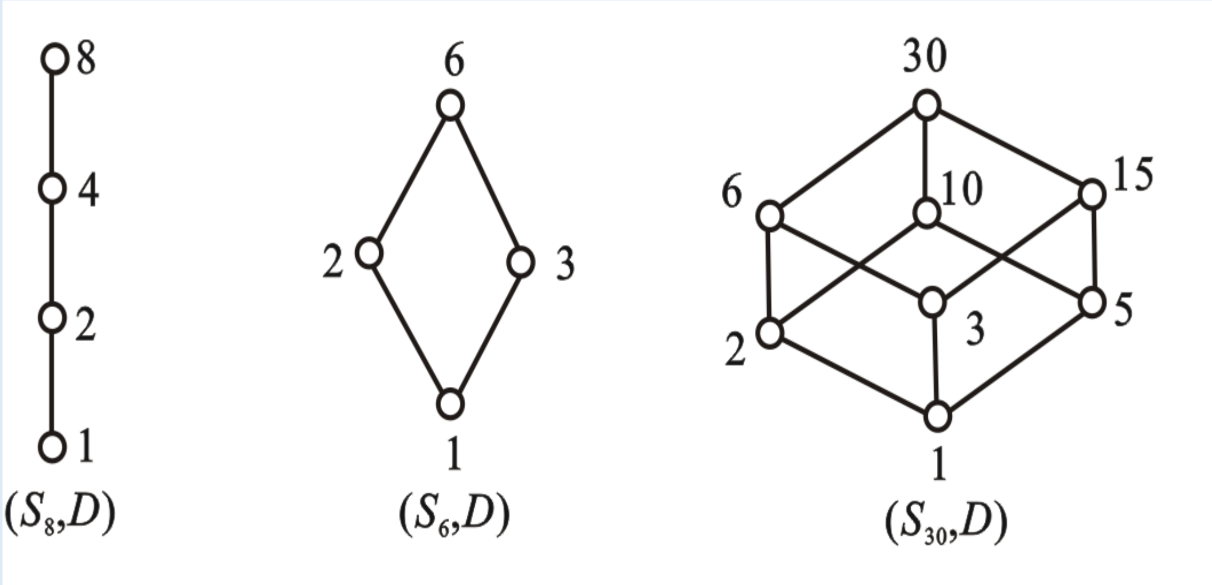
① The ***binary operations*** for least upper bound and greatest lower bound **(∨, ∧)** represent operations within the lattice only and have no other meanings.

② The lattice **<*L*,∧,∨>** constructed from a partially ordered set **<S,≼>** contains not only all elements of ***S*** but also ***additional elements*** needed to ensure that every pair ***x***, ***y*** has both a least upper bound and a greatest lower bound.

③ For any two elements ***x*** and ***y***, the least upper bound (***supremum x∨y***) is the smallest element among all upper bounds of **x** and **y**.

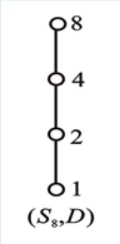
④ For any two elements **x** and **y**, the greatest lower bound (***infimum x∧y***) is the largest element among all lower bounds of ***x*** and ***y***.

- **Example:** Let n be a positive integer, and let S_n be the set of positive divisors of n. Let D denote the divisibility relation. Then the partially ordered set $<S_n,D>$ forms a *lattice*. $\forall x,y \in S_n$, $x \vee y$ is **lcm**(x,y), the least common multiple of x and y, and the meet $x \wedge y$ is **gcd**(x,y), the greatest common divisor of x and y.
  - Below are the *Hasse diagrams* of the lattices $<S_8,D>$, $<S_6,D>$ and $<S_{30},D>$.

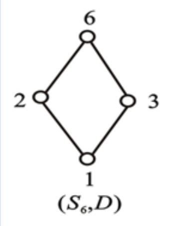


- **Note:**

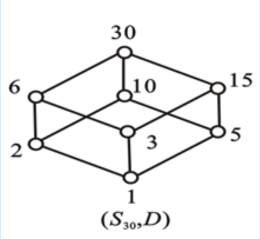
(1) For the lattice $<S_8,D>$, the set S_8={1,2,4,8} forms a **chain** under the divisibility relation D, each element divides the element above it, i.e., **1≤2≤4≤8.**



(2) For the lattice $<S_6,D>$, the set S_6={1,2,3,6} forms a **diamond structure** under D, both **2** and **3** are direct multiples of **1**, and **6** is the common multiple of 2 and **3**.



(3) For the lattice $<S_{30},D>$, the set S_{30}={1,2,3,5,6,10,15,30} forms a **cubic structure** under the divisibility relation D, edges between vertices represent divisibility, e.g., both **2** and **3** divide **6**, and both **2** and 5 divide **10**.



- **Example 1:** Determine whether the partially ordered set $<P(B),\subseteq>$ forms a lattice, where $P(B)$ is the power set of a set B.
  - **Solution :**

(1) ***Check the least upper bound***: For any two subsets $A,C\in P(B)$, define their least upper bound as $A\cup C$. Under the subset relation, any subset D that contains both A and C must satisfy $A\cup C\subseteq D$. Hence, $A\cup C$ is the least upper bound of A and C.

(2) ***Check the greatest lower bound***: For any two subsets $A,C\in P(B)$, C define their greatest lower bound as $A\cap C$. Under the subset relation, any subset E that is contained in both A and C must satisfy $E\subseteq A\cap C$. Thus, $A\cap C$ is the greatest lower bound of A and C.

(3) Since for any elements in $P(B)$, both the least upper bound $A\cup C$ and the greatest lower bound $A\cap C$ exist, the partially ordered set $<P(B),\subseteq>$ ***forms a lattice***.

- **Example 2:** Determine whether the partially ordered set **<Z, ≤ >** forms a lattice, where **Z** is the set of integers and **≤** is the less-than-or-equal-to relation.
  - **Solution:**

(1) For any two elements ***a*** and ***b*** in Z, the **least upper bound** is the greater of the two: $a \vee b = \max(a,b)$.

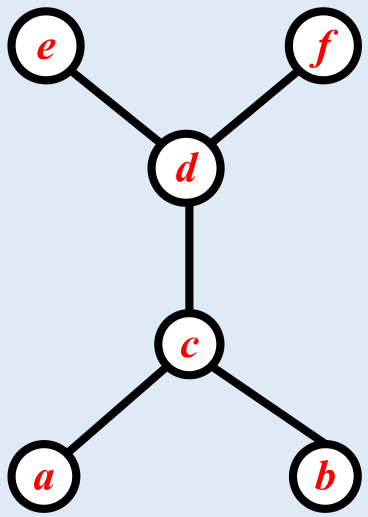
(2) For any two elements ***a*** and ***b*** in Z, the **greatest lower bound** is the smaller of the two: $a \wedge b = \min(a,b)$.

(3) Since these conditions hold for all pairs of integers ***a*** and ***b***, the partially ordered set ⟨Z,≤⟩ ***satisfies the definition of a lattice***.

- **Example 3:** Determine whether the structure forms a lattice based on the Hasse diagram of the partially ordered set.

- **Solution:**

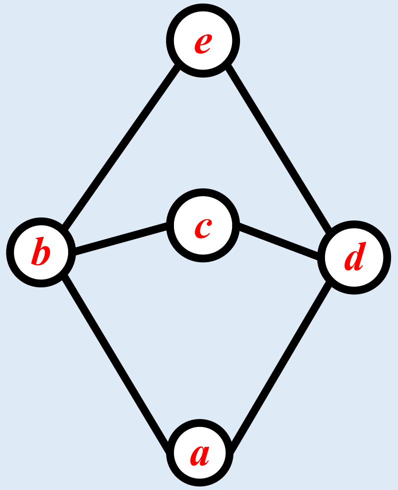
  (1) In diagram (**F1**), elements ***e*** and ***f*** have no common upper bound, so a least upper bound cannot be determined. Similarly, ***a*** and ***b*** have no common lower bound, so a **greatest lower bound cannot be determined**. Therefore, the structure ***does not form a lattice***.



(F1)

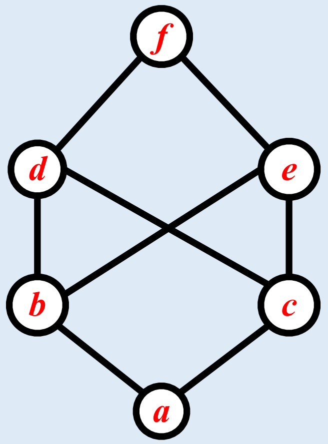
- **Solution:**

(2) In diagram (**F2**), ***c*** and ***e*** have no upper bounds, and there is no direct relationship between them. Therefore, a least (common) upper bound greater than both ***c*** and ***e*** cannot be found.The common lower bounds of ***c*** and ***e*** are ***b***, ***d***, and ***a***. Both ***b*** and ***d*** are greater than ***a***, and there is no direct partial order between ***b*** and ***d***. Thus, there is **no unique greatest common lower bound**. Hence, the structure ***does not form a lattice***.



(F2)

(3) In diagram (**F3**), the common lower bounds of ***d*** and ***e*** are ***a***, ***b***, and **c**. Both ***b*** and ***c*** are greater than ***a***, and there is no partial order between ***b*** and ***c***. Therefore, a **unique greatest lower bound cannot be determined**. As a result, the structure ***does not form a lattice***.



(F3)

↳ Dual statement & Principle of Duality in Lattices

- Let ***f*** be a statement involving elements of a lattice and the symbols $=, \preccurlyeq, \succcurlyeq$. Define ***f**** as the statement obtained by replacing $\preceq$ with $\succeq$, $\succeq$ with $\preceq$, $\vee$ with $\wedge$, and $\wedge$ with $\vee$ in ***f*** . The statement ***f**** is called the ***dual*** of ***f*** .

- **Principle of Duality for Lattices:**
  If a statement ***f*** is true for all lattices, then its dual statement ***f**** is also true for all lattices.

- **Example :** In a lattice, if the statement ***f*** : $(a \vee b) \wedge c \preccurlyeq c$ holds, then its dual statement ***f**** : $(a \wedge b) \vee c \succeq c$ also holds.

↳ Fundamental Properties of Lattice Operations

- **Theorem 9.11 :** Let ***v*** be a lattice. Then the operations $\vee$ and $\wedge$ satisfy the ***commutative***, ***associative***, ***idempotent***, and ***absorption*** laws, namely:
  (1) $\forall a,b\in L$, $a\vee b=b\vee a$ *and* $a\wedge b=b\wedge a$
  (2) $\forall a,b,c\in L$, $(a\vee b)\vee c=a\vee(b\vee c)$ and $(a\wedge b)\wedge c=a\wedge(b\wedge c)$
  (3) $\forall a\in L$, $a\vee a=a$ and $a\wedge a=a$
  (4) $\forall a,b\in L$, $a\vee(a\wedge b)=a$ *and* $a\wedge(a\vee b)=a$

Proof(1) : Commutative Law

- $a \vee b$ is the least upper bound of the set , $b \vee a$ is the least upper bound of the set $\{b,a\}$.
- Since $\{a, b\} = \{b, a\}$ we have $a \vee b = b \vee a$.
- By the **principle of duality**, it follows that $a \wedge b = b \wedge a$.
- Thus, the **commutative law** holds.

Proof(2) : Associative Law

- From the definition of the least upper bound, we have the following inequalities:

  $(a \vee b) \vee c \succcurlyeq a \vee b \succcurlyeq a$ ①

  $(a \vee b) \vee c \succcurlyeq a \vee b \succcurlyeq b$ ②

  $(a \vee b) \vee c \succcurlyeq c$ ③

- From ② and ③

  $(a \vee b) \vee c \succcurlyeq b \vee c$ ④

- Combining ① and ④ we obtain $(a \vee b) \vee c \succcurlyeq a \vee (b \vee c)$.
- Similarly, we can prove: $(a \vee b) \vee c \preccurlyeq a \vee (b \vee c)$.
- By the **antisymmetry** of the partial order, it follows that: $(a \vee b) \vee c = a \vee (b \vee c)$.
- By the **principle of duality**, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ can also be proved, that is, the *associative law holds*.

↳ Definition of a Lattice - Algebraic Perspective

- A lattice can be *characterized as an algebraic structure* with join ($\vee$) and meet ($\wedge$) operations satisfying commutativity, associativity, and absorption laws, *or as a poset* in which every pair of elements has a least upper bound and a greatest lower bound.
- **Definition 9.24：** Let $(S,*,\circ)$ be an **algebraic system** with two binary operations. If the operations $*$ and $\circ$ satisfy the **commutative law**, **associative law**, and **absorption law**, then a partial order $\preccurlyeq$ can be suitably defined on S such that $<S, \preccurlyeq>$ forms a *lattice*, and for all $a,b \in S$, we have: $\forall a,b \in S$, $a \wedge b = a * b$ and $a \vee b = a \circ b$.
- **Example：** Verify that the algebraic definition of a lattice and the order-theoretic definition are equivalent in characterizing the same lattice structure.

↳ Definition of a Lattice - Algebraic Perspective(e.g.)

① Let $S=\{0,1,2,3\}$, for any $a,b\in S$, *define* $a*b=min(a,b)$, $a\circ b=max(a,b)$.

② Define the *partial order* $\preceq$ by $a\preceq b$, if and only if $a*b=min(a,b)=a$ or $a\circ b=max(a,b)=b$.

③ *Reflexivity*: $a*a=min(a,a)=a$, $a\circ a=max(a,a)=a$, so reflexivity holds.

④ *Antisymmetry*: $a\preceq b$ means $a*b=a$ $(b*a=b)$, $*$ satisfy commutative $a*b=b*a$, obtain $a=b$, thus, antisymmetry holds.

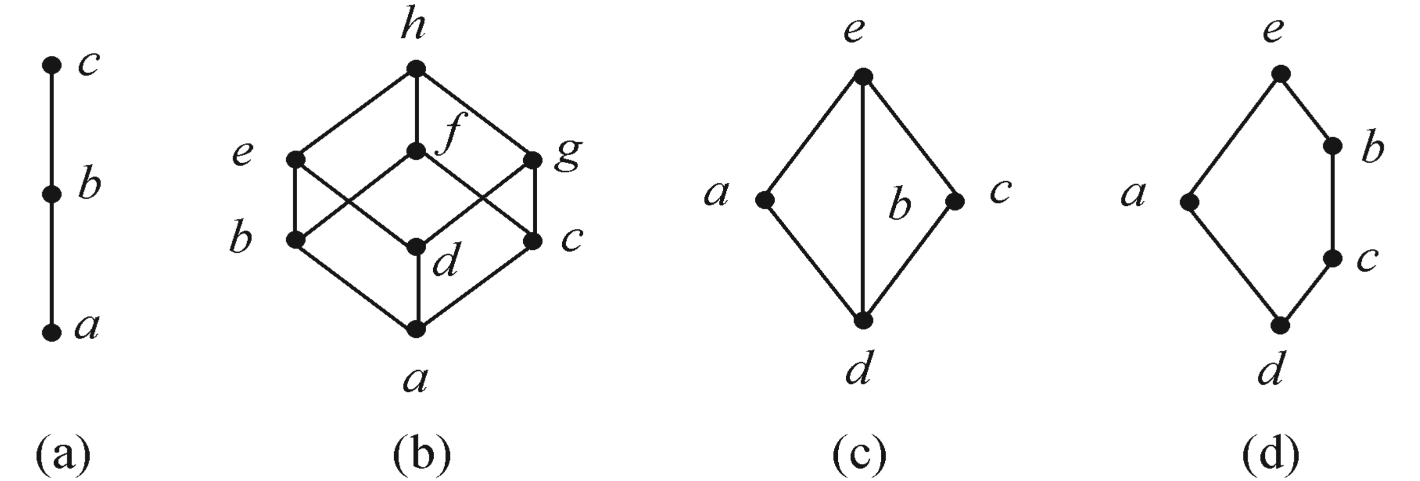
⑤ *Transitivity*: $a\preceq b(a*b=a)$, $b\preceq c(b*c=b)$, then using the associativity of $*$, $a*c=a*(b*c)=(a*b)*c=a*c=a$, transitivity holds.

⑥ Define the *greatest lower bound* $a\wedge b=a*b=min(a,b)$, for any $c\in S$, if $c\preceq a$ and $c\preceq b(c*a=c$ and $c*b=c)$, $c*(a*b)=c$,then $c\preceq(a*b)$, Hence, a greatest lower bound exists for any pair a, b.

⑦ Define the *least upper bound* $a\vee b=a\circ b=max(a,b)$, for any $c\in S$, if $a\preceq c$ and $b\preceq c(a\circ c=c$ and $b\circ c=c)$, $(a\circ b)\circ c=c$, then $(a\circ b)\preceq c$, Hence, a least upper bound exists for any pair a, b.

↳ Distributive lattice = lattice + distributive law

- **Definition 9.25:** Let $<L, \wedge, \vee>$ be a lattice. If for all $\forall a, b, c \in L$ we have $a\wedge(b\vee c) = (a\wedge b)\vee(a\wedge c)$, $a\vee(b\wedge c) = (a\vee b)\wedge(a\vee c)$, then L is called a ***distributive lattice***.
- **Example:** Identify which lattices in the diagram are **distributive lattices**.



Solution: (a) and (b) are distributive lattices, (c) and (d) are not.

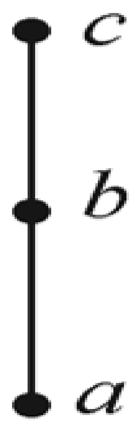
- **Solution:** Determine whether lattice **(a)** is a **distributive lattice**.

① The three elements a,b,c in the diagram form a simple chain $a \le b \le c$, where every pair of elements has a well-defined least upper bound and greatest lower bound.

② **Verify Distributive Law 1:** Since $b \le c$, we have $b \vee c = c$, so: $a \wedge (b \vee c) = a \wedge c = a$. Since $a \le b \le c$, we have $a \wedge b = a$, $a \wedge c = a$, so $(a \wedge b) \vee (a \wedge c) = a \vee a = a$. The identy $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ holds.

③ **Verify Distributive Law 2:** Since $b \le c$, we have $b \wedge c = b$, so $a \vee (b \wedge c) = a \vee b = b$. *Since* $a \le b \le c$, we have $a \vee b = b$, $a \vee c = c$, so $(a \vee b) \wedge (a \vee c) = b \wedge c = b$. Thus, the identity $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ holds.

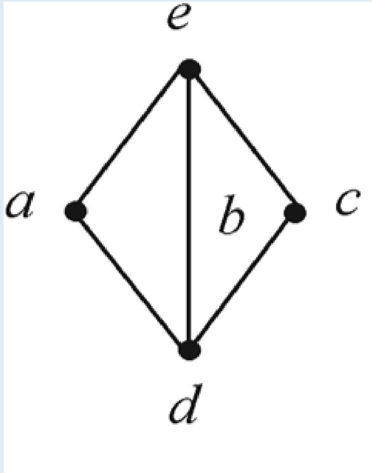
Therefore, lattice **(a)** *satisfies both distributive laws* and is a **distributive lattice**.



(a)

同济经管 TONGJI SEM

- **Solution:** Determine whether lattice **(c)** is a **distributive lattice**.



(c)

①The elements a,b,c,d,e satisfy the relations: $d\le a$, $d\le c$, $a\le e$, $c\le e$, $d\le b, b\le e$. Each pair of elements has a well-defined least upper bound and greatest lower bound.

②**Verify Distributive Law 1:** Since $b\vee c=e$, $a\wedge e=a$,we get $a\wedge(b\vee c)=a\wedge e=a$. Since $a\wedge b=d$, $a\wedge c=d$, we have $(a\wedge b)\vee(a\wedge c)=d\vee d=d$. Results: $a\wedge(b\vee c) \neq (a\wedge b)\vee(a\wedge c)$, so *Distributive Law 1 does not hold*.

③**Verify Distributive Law 2:** Since $b\wedge c=d$, $a\vee d=a$, we have $a\vee(b\wedge c)=a\vee d=a$. Since $a\vee b=e$, $a\vee c=e$, we have $(a\vee b)\wedge(a\vee c)=e\wedge e=e$. Results: $a\vee(b\wedge c)\neq(a\vee b)\wedge(a\vee c)$, so *Distributive Law 2 also does not hold*.

Since neither distributive law holds, *lattice (c) is not a distributive lattice*.

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

↳ Bounded lattice=lattice+greatest lower bound 0 +least upper bound 1

- **Definition 9.26 :** If there exists an element a in a lattice $<L, \wedge, \vee, >$ such that for $\forall b \in L$, $a \preccurlyeq b$ (or $b \preccurlyeq a$), then a is called the **greatest lower bound** (or **least upper bound**) of L.
  - If the ***greatest lower bound*** of L exists, it is unique and denoted by **0**.
  - If the ***least upper bound*** of L exists, it is also unique and denoted by **1**.
  - If both the greatest lower bound and the least upper bound exist in L, then v is called a ***bounded lattice***, denoted as $<L, \wedge, \vee, 0, 1>$.

↳ Examples of Determining Bounded Lattices

- **Example** (1) **:** A finite lattice $L=\{a_1,a_2,\ldots,a_n\}$ is a **bounded lattice**, where $a_1 \wedge a_2 \wedge \ldots \wedge a_n$ is the **greatest lower bound** (bottom element), and $a_1 \vee a_2 \vee \ldots \vee a_n$ is the **least upper bound** (top element) of L.

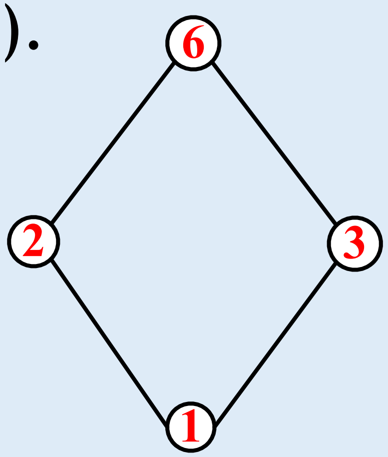
① Consider the finite lattice $L=\{1,2,3,6\}$, with the **divisibility relation** as the partial order. The ***meet operation*** $\wedge$ represents the **greatest common divisor** (GCD) of two elements, and the ***join operation*** $\vee$ represents the **least common multiple** (LCM).

② The **greatest lower bound** (GCD of all elements):

$1 \wedge 2 \wedge 3 \wedge 6 = 1$ — the GCD of all elements.

③ The **least upper bound** (LCM of all elements):

$1 \vee 2 \vee 3 \vee 6 = 6$ — the LCM of all elements.



↳ Examples of Determining Bounded Lattices

- **Example(2):** The power set lattice ***P*(*B*)** is a **bounded lattice**, even when ***B*** is an infinite set.

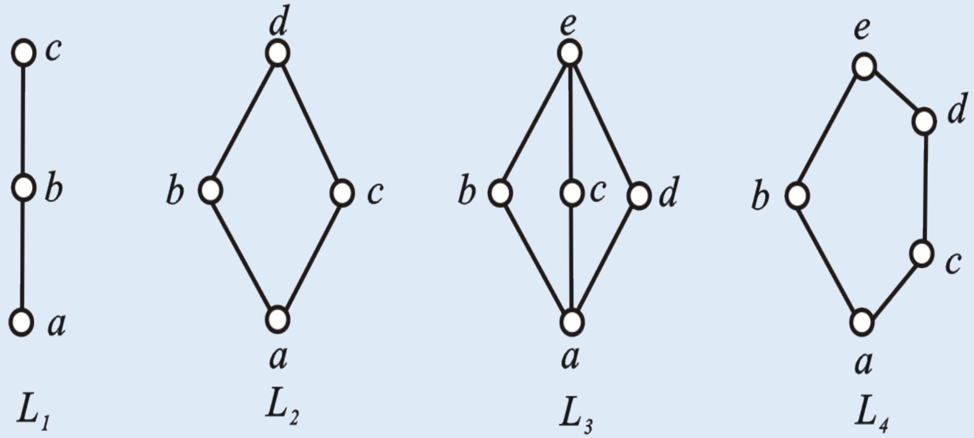
① The empty set **∅** is a subset of every set in ***P*(*B*)**, making it the ***greatest lower bound*** (bottom element) of all elements.

② The set ***B*** is a superset of every subset in ***P*(*B*)**, making it the ***least upper bound*** (top element).

③ Regardless of whether the set ***B*** is finite or infinite, the power set ***P*(*B*)** always has a well-defined **bottom element** (the empty set ∅) and **top element** (the set ***B***), and thus forms a ***bounded lattice*** **$\langle P(B), \subseteq, \cap, \cup, \emptyset, B \rangle$.**

- **Definition 9.27:** Let **<*L*,∧,∨,0,1>** be a **bounded lattice**, and let ***a***∈***L***. If there exists ***b***∈***L*** such that: ***a***∧***b*=0** and ***a***∨***b*=1**, then ***b*** is called a ***complement*** of ***a***.
  - The elements **0** (greatest lower bound) and **1** (least upper bound) are ***complements of each other***, and each has a **unique** complement.
  - Some elements may **not have any complements**, some may have **exactly one**, and some may have **more than one**.
  - If ***every element*** in the bounded lattice **<*L*,∧,∨,0,1>** ***has a complement***, then the lattice is called a ***complemented lattice***.

- **Example:** Find the complements of all elements in each of the following four lattices, and determine whether each lattice is a **complemented lattice.**

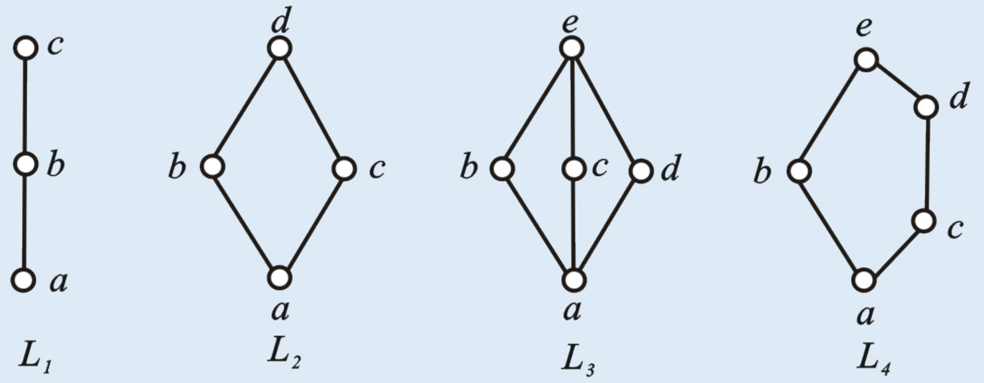


- **Solution:**

(1) In L_1 , $a \wedge c = a$ and $a \vee c = c$ (the maximum element), so a and c are complements of each other. However, b has *no complement*, so L_1 is **not a complemented lattice.**

(2) In L_2, a and d are complements of each other, and b and c are complements of each other. Therefore, L_2 **is a** ***complemented lattice***.

↳ Examples of Determining Complemented Lattices



(3) In L_3 , a and a are complements of each other. Element b has two complements: c, d. Element c has complements b and d. Element d has complements b and c. Therefore, L_3 is a ***complemented lattice***.

(4) In L_4 , a and e are complements of each other. Element b has complements c and d. Element c has complement b. Element d has complement b. Therefore, L_4 is a ***complemented lattice***.

↳ Definition of Boolean Lattice (Boolean Algebra)

- **Definition 9.28:** If a bounded lattice **<*L*,∧,∨,0,1>**⟩ is both **complemented** and **distributive**, then ***L*** is called a ***Boolean lattice*** or ***Boolean algebra***.
  - A ***distributive lattice*** must **satisfy the distributive laws**, that is, for all **a,b,c∈L** : **a∧(b∨c)=(a∧b)∨(a∧c)**) and **a∨(b∧c)=(a∨b)∧(a∨c).**
  - A ***complemented distributive lattice*** not only requires the existence of complements but also that each complement is **unique**.
  - In a **Boolean lattice (algebra)**, the operation of taking the ***complement*** can be regarded as a ***unary operation*** in Boolean algebra.
  - A Boolean algebra is typically denoted as **<*B*,∧,∨,′, 0, 1>**, where ′ ***′*** ′ represents the ***complement operation***.

同济经管 TONGJI SEM

- **Example:** Determine whether the power set lattice ***P***(***B***) is a **Boolean algebra**.
  - **Solution:**

(1) To determine whether *P*(*B*) is a *lattice*: For any two subsets $A,B \subseteq B$, both the **union** $A \cup B$(least upper bound) and the **intersection** $A \cap B$(greatest lower bound) exist and belong to ***P***(***B***), so the definition of a lattice is satisfied.

(2) To determine whether *P*(*B*) is a *distributive lattice*: For any three elements in ***P***(***B***), the operations of **union** $\cup$ and **intersection** $\cap$ satisfy the **distributive laws**, so the definition of a distributive lattice is fulfilled.

(3) To determine whether ***P*(*B*)** is a ***complemented lattice***: For every subset ***A*⊆*B***, there exists a **complement** A^c **=*B*-*A*** such that $A \cap A^c = \emptyset$ (the bottom element) and $A \cup A^c = B$ (the top element), satisfying the definition of a complemented lattice.

(4) To determine whether ***P*(*B*)** is a ***Boolean lattice***: Since ***P*(*B*)** is already known to be a **lattice**, a **distributive lattice**, and a **complemented lattice**, it follows that the power set lattice ***P*(*B*)** is a **Boolean lattice** (Boolean algebra).

- **Note:**

The ***uniqueness of complements*** in the Boolean lattice ***P*(*B*)** can be proven using the properties of Boolean algebra — namely, the **commutative**, **associative**, and **distributive** laws.

↳ Structure Theorem for Finite Boolean Algebras

- **Theorem 9.12:** Let L be a **finite Boolean algebra**. Then L contains 2^n elements for some $n \in N$, and L is ***isomorphic to the Boolean algebra*** $\langle P(S), \cap, \cup, \sim, \varnothing, S \rangle$, where S is a set with n elements.

- **Note:**

① An ***isomorphism*** between two Boolean algebras ***requires*** a **bijection** that preserves **meet** ($\wedge$), **join** ($\vee$), and **complement** operations, as well as the **zero** and **unit** elements.

② Up to isomorphism, there is *only one Boolean algebra* with 2^n elements.

↳ Structure Theorem for Finite Boolean Algebras

- **Note:**

③ Any finite Boolean algebra ***L*** is isomorphic to the power set algebra **<*P*(*S*),∩,∪,~,∅,*S*>** , where ***P*(*S*)** is the power set of an ***n***-element set ***S***. This ***intuitive model*** facilitates a better understanding and manipulation of Boolean algebra.

④ This theorem ***bridges*** abstract algebra (Boolean algebras) and set theory (power set algebras), enabling broad applications in **logic**, **computer science**, and **algebraic geometry**.

⑤ Understanding the ***algebraic structure*** and its **isomorphism** to ***set-theoretic models*** aids in simplifying logical expressions and optimizing algorithm design.

From lattices to Boolean algebra

Boolean Lattice (Boolean Algebra) $<B,\wedge,\vee,',0,1>$
- **Complemented lattice $<L,\wedge,\vee,0,1>$**
- **Distributive lattice $<L,\wedge,\vee,>$**

Complemented lattice $<L,\wedge,\vee,0,1>$
- **For all $a\in L$, there exists $b\in L$ such that $a\vee b=1$ and $a\wedge b=0$.**
- **Bounded lattice $<L,\wedge,\vee,0,1>$**

Bounded lattice $<L,\wedge,\vee,0,1>$
- **The set L has a least element 0 (infimum of L) and a greatest element 1 (supremum of L).**
- **Lattice $<L,\wedge,\vee>$**

Distributive lattice $<L,\wedge,\vee,>$
- **$\forall a,b,c\in L$, $a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)$ and $a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)$**
- **Lattice $<L,\wedge,\vee,>$**

Lattice $<L,\wedge,\vee,>$
- **$S\subseteq L$ and $<S,\preceq>\subseteq<L,\preceq>$** + Additional elements — The additional elements ensure that $<S,\preceq>$ is join and meet closed in L
- The poset $<S,\preceq>$ satisfies reflexivity, antisymmetry, and transitivity.

Objective :

Key Concepts :

Objective：

Key Concepts：