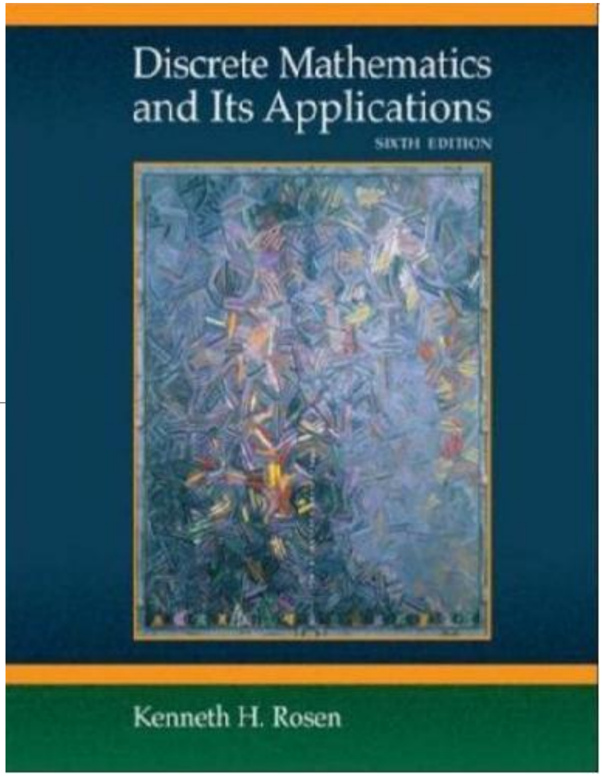
Discrete Mathematics



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
- Ring and Field
- **Lattice**
- Boolean algebra

Review

- Algebraic system <A, ∘> or $<S, \triangle, *>$
- 4 properties
  - Closure
  - Commutativity
  - Associativity
  - Distributivity
- ✓3 constants
  - Identity
  - Zero
  - Inverse
- ✓9 special algebraic systems
  - Semigroup
  - Monoid
  - Group
  - Abelian Group, Cyclic Group, Permutation Group
  - Coset
  - Ring and Field
- ✓2 relations
  - Homomorphism
  - Isomorphism

Lattice

- A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a **lattice**.
- upper bound -> 公倍数， lower bound -> 公约数

- Let $(L, \preccurlyeq)$ be a lattice. We denote lub($\{a, b\}$) by $a \vee b$ and call it the join of a and b. Similarly, we denote glb($\{a, b\}$) by $a \wedge b$ and call it the meet of a and b. Then $<L, \vee, \wedge>$ is the corresponding algebraic system of $(L, \preccurlyeq)$.

Hasse Diagram

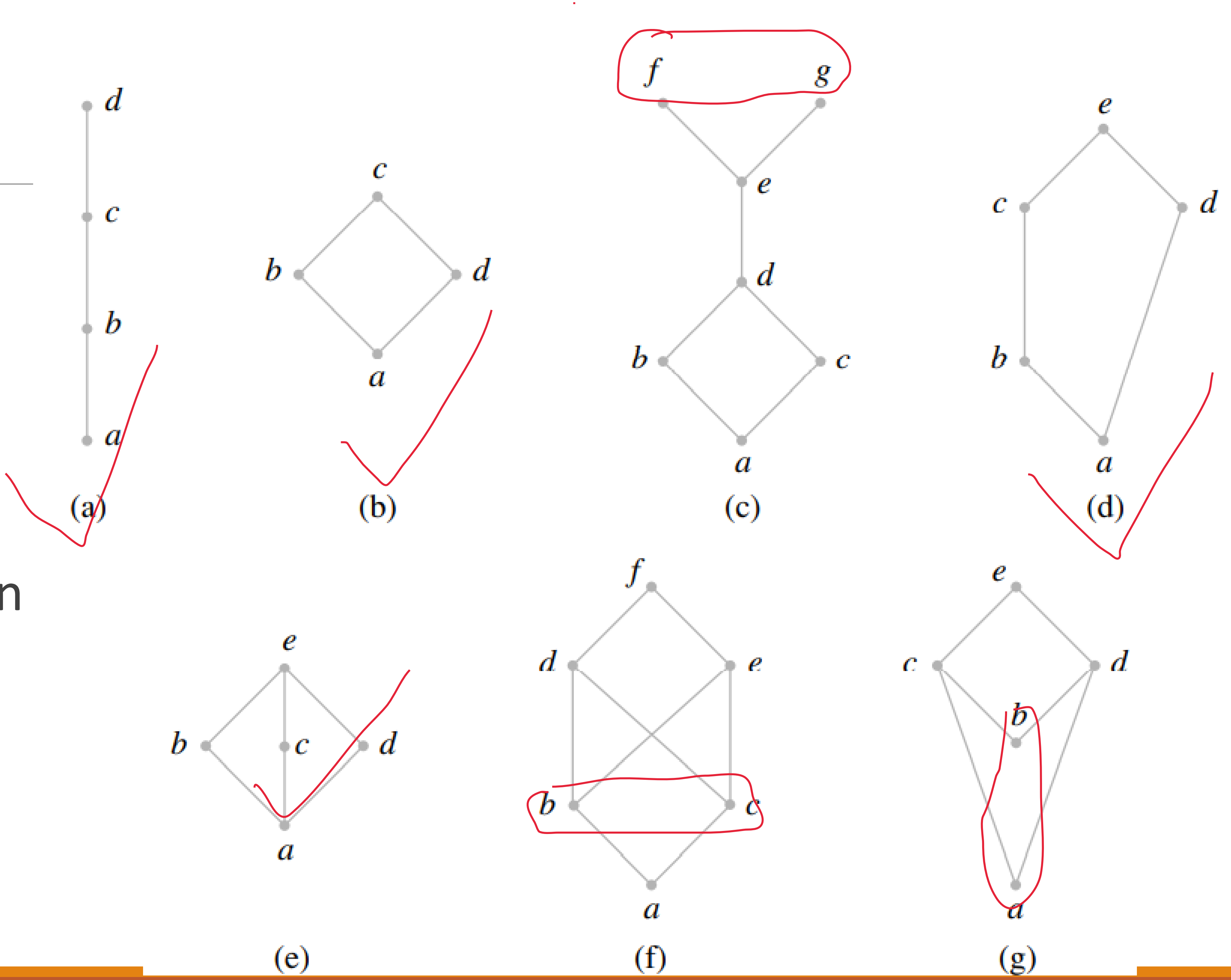
A **Hasse diagram** is a graphical rendering of a partially ordered set displayed via the cover relation of the partially ordered set with an implied upward orientation. A point is drawn for each element of the poset, and line segments are drawn between these points according to the following two rules:

- 1. If $x \preccurlyeq y$ in the poset, then the point corresponding to x appears lower in the drawing than the point corresponding to y.

- 2. The line segment between the points corresponding to any two elements x and y of the poset is included in the drawing iff x covers y or y covers x.

Example 1

- Which of the following Hasse diagrams represent lattices?



reduce redundant information

Example 2

- Let $S=\{a,b\}$, draw the Hasse diagram of lattice $(P(S), \subseteq)$ and the operation tables of $\vee$ and $\wedge$.

$\vee$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$

$\wedge$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a,b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$

Sublattice

Definition:

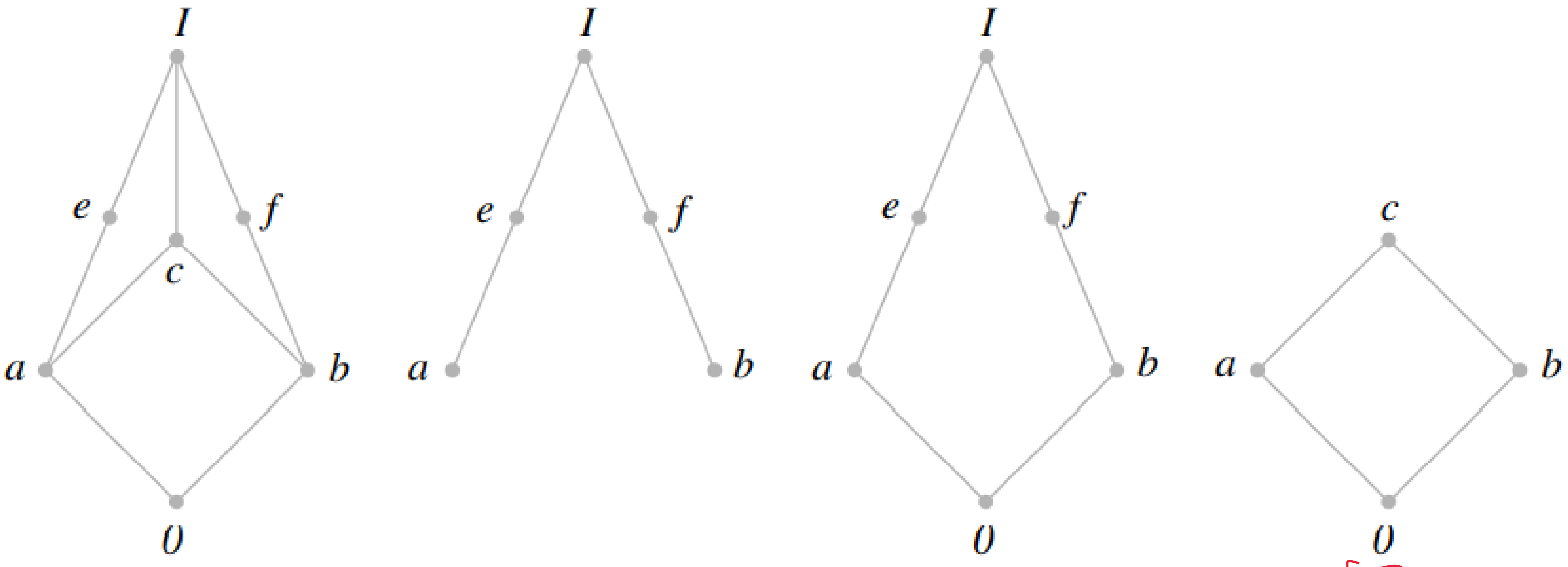
- Let $(L, \preccurlyeq)$ be a lattice. A nonempty subset S of L is called a **sublattice** of L if $a \vee b \in S$ and $a \wedge b \in S$ whenever $a \in S$ and $b \in S$. 并不代表lattice+ nonempty subset = sublattice

Example:

- Let E^+ be the set of all positive even integers, then $(E^+, |)$ is a sublattice of $(\mathbf{Z}^+, |)$.

Example 3

- Consider the lattice $(L, \preccurlyeq)$ shown in Figure (a). Which one is its sublattice?



(a) (b) (c) (d)

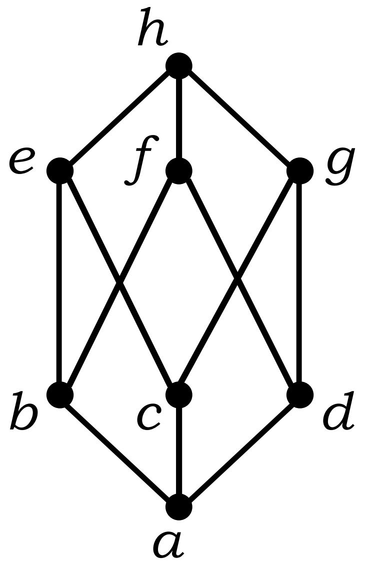
Example 4

- Let (L, ≼) be a lattice shown in the figure, L={a, b, c, d, e, f, g, h}.

✓ Let L_1={h, e, c, g}

✓ Let L_2={a, b, f, d}

✓ Let L_3={a, b, d, e, f, g, h}



- Let (L, ≼) be a lattice, S be a nonempty subset of L. Then (S, ≼) must be a poset, but not necessarily a lattice.

- Even if (S, ≼) is lattice, it is not necessarily a sublattice of (L, ≼)

Theorems of Lattice (1)

- Let $(L, \preccurlyeq)$ be a lattice. $<L, \vee, \wedge>$ is the corresponding algebraic system of $(L, \preccurlyeq)$. For $\forall a, b \in L$,

✓ $a \preccurlyeq a \vee b$, $b \preccurlyeq a \vee b$, $a \wedge b \preccurlyeq b$, $a \wedge b \preccurlyeq a$ (upper bound property)

✓ $a \vee b = b$ iff $a \preccurlyeq b$ iff $a \wedge b = a$ (equal property)

上界大于任意元素
下界小于任意元素
最小上界小于任意上界
最大下界大于任意下界

Cont.

- $a \vee b = b$ if and only if $a \preccurlyeq b$.
- $a \wedge b = a$ if and only if $a \preccurlyeq b$.
- $a \wedge b = a$ if and only if $a \vee b = b$.
- Proof:

Suppose that $a \vee b = b$. Since a $\preccurlyeq a \vee b = b$, we have $a \preccurlyeq b$.

Conversely, if $a \preccurlyeq b$, then, since $b \preccurlyeq b$, b is an upper bound of a and b;

so by definition of least upper bound we have $a \vee b \preccurlyeq b$. Since $a \vee b$ is an upper bound, $b \preccurlyeq a \vee b$, so $a \vee b = b$.

Theorems of Lattice (2)

Let $(L, \preccurlyeq)$ be a lattice. $<L, \vee, \wedge>$ is the corresponding algebraic system of $(L, \preccurlyeq)$. For $\forall a, b, c, d \in L$,

同增同减

- 1. If $a \preccurlyeq b$, then

(a) $a \vee c \preccurlyeq b \vee c$. (b) $a \wedge c \preccurlyeq b \wedge c$.

- 2. $a \preccurlyeq c$ and $b \preccurlyeq c$ if and only if $a \vee b \preccurlyeq c$.
- 3. $c \preccurlyeq a$ and $c \preccurlyeq b$ if and only if $c \preccurlyeq a \wedge b$.
- 4. If $a \preccurlyeq b$ and $c \preccurlyeq d$, then (递推性)

(a) $a \vee c \preccurlyeq b \vee d$. (b) $a \wedge c \preccurlyeq b \wedge d$.

Cont.

- 4. If $a \preccurlyeq b$ and $c \preccurlyeq d$, then

(a) $a \vee c \preccurlyeq b \vee d$. (b) $a \wedge c \preccurlyeq b \wedge d$.

- Proof:

$b \preccurlyeq b \vee d$, $a \preccurlyeq b$, so $a \preccurlyeq b \vee d$.

$d \preccurlyeq b \vee d$, $c \preccurlyeq d$, so $c \preccurlyeq b \vee d$.

So $b \vee d$ is an upper bound of a and c.

By the definition of lub, we have $a \vee c \preccurlyeq b \vee d$.

Cont.

- 1. If $a \preccurlyeq b$, then

(a) $a \vee c \preccurlyeq b \vee c$. (b) $a \wedge c \preccurlyeq b \wedge c$.

- 4. If $a \preccurlyeq b$ and $c \preccurlyeq d$, then

(a) $a \vee c \preccurlyeq b \vee d$. (b) $a \wedge c \preccurlyeq b \wedge d$.

- Proof:

Replace d in 4(a)(b) with c.

Theorems of Lattice (3)

Let $(L, \preccurlyeq)$ be a lattice. $<L, \vee, \wedge>$ is the corresponding algebraic system of $(L, \preccurlyeq)$. For $\forall a, b, c \in L$,

- **1. Idempotent Properties:** (a) $a \vee a = a$ (b) $a \wedge a = a$
- **2. Commutative Properties:** (a) $a \vee b = b \vee a$ (b) $a \wedge b = b \wedge a$
- **3. Associative Properties:**

(a) $a \vee (b \vee c) = (a \vee b) \vee c$ (b) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

- **4. Absorption Properties:**

满不满足分配率

(a) $a \vee (a \wedge b) = a$ (b) $a \wedge (a \vee b) = a$

Cont.

- **3. Associative Properties**

(a) $a \vee (b \vee c) = (a \vee b) \vee c$ (b) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

- Proof:

From the definition of lub, we have $a \preccurlyeq a \vee (b \vee c)$ and $b \vee c \preccurlyeq a \vee (b \vee c)$.

Moreover, $b \preccurlyeq b \vee c$ and $c \preccurlyeq b \vee c$, so, by transitivity, $b \preccurlyeq a \vee (b \vee c)$ and $c \preccurlyeq a \vee (b \vee c)$.

Thus $a \vee (b \vee c)$ is an upper bound of a and b, so $a \vee b \preccurlyeq a \vee (b \vee c)$

Since $a \vee (b \vee c)$ is an upper bound of $a \vee b$ and c, we obtain $(a \vee b) \vee c \preccurlyeq a \vee (b \vee c)$.

Similarly, $a \vee (b \vee c) \preccurlyeq (a \vee b) \vee c$. By the antisymmetry of $\preccurlyeq$, $a \vee (b \vee c) = (a \vee b) \vee c$.

Cont.

- **4. Absorption Properties**

(a) $a \vee (a \wedge b) = a$ (b) $a \wedge (a \vee b) = a$

- Proof:

Since $a \wedge b \preccurlyeq a$ and $a \preccurlyeq a$, we see that a is an upper bound of $a \wedge b$ and a.

So $a \vee (a \wedge b) \preccurlyeq a$.

By the definition of lub, we have $a \preccurlyeq a \vee (a \wedge b)$.

So $a \vee (a \wedge b) = a$.

Example 5

Let $<A, \vee, \wedge>$ be an algebraic system. $\vee$ and $\wedge$ are binary operations with absorption properties. Show that $\vee$ and $\wedge$ have idempotent properties.

- Proof:

By the definition of absorption property, for $\forall a, b \in A$,

$a \vee (a \wedge b) = a$ (1),

$a \wedge (a \vee b) = a$ (2).

Replace b in (1) with $a \vee b$, we have $a \vee (a \wedge (a \vee b)) = a$.

According to (2) $a \vee (a \wedge (a \vee b)) = a \vee a = a$.

Similarly, $a \wedge a = a$.

Exercise 1

- Let $(L, \preccurlyeq)$ be a lattice. For $\forall a, b, c \in L$, show that

$a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c)$.

$(a \wedge b) \vee (a \wedge c) \preccurlyeq a \wedge (b \vee c)$.

Isomorphism of Lattices

- Let $(L_1, \preccurlyeq_1)$ and $(L_2, \preccurlyeq_2)$ be two lattices, the corresponding algebraic systems are $< L_1, \vee_1, \wedge_1>$ and $< L_2, \vee_2, \wedge_2>$ respectively. If there is a bijection $f: L_1 \to L_2$, such that for $\forall a, b \in L_1$,

$$f(a \vee_1 b) = f(a) \vee_2 f(b)$$

$$f(a \wedge_1 b) = f(a) \wedge_2 f(b),$$

then we say f is a isomorphism from $< L_1, \vee_1, \wedge_1>$ to $< L_2, \vee_2, \wedge_2>$.

$(L_1, \preccurlyeq_1)$ and $(L_2, \preccurlyeq_2)$ isomorphic lattices.

Example 6

- Let E^+ be the set of positive even integers, show that $(\mathbf{Z}^+, \leq)$ and $(E^+, \leq)$ are isomorphic lattices.

Exercise 2

- Let $A = \{1, 2, 3, 6\}$, $S=\{a, b\}$, show that $(A, |)$ and $(P(S), \subseteq)$ are isomorphic lattice.

Define $f : A \to P(S)$ as:

$f(1) = \emptyset$, $f(2) = \{a\}$, $f(3) = \{b\}$, $f(6) = \{a, b\}$.

then it is easily seen that f is a one-to-one correspondence.

Bounded Lattice

Definition:

- A lattice $(L, \preccurlyeq)$ is said to be **bounded** if it has a greatest element and a least element.

Example:

- $(\mathbf{Z}^+, \mid)$
- $(\mathbf{Z}, \leq)$
- $(P(S), \subseteq)$

Example 1

- Let $(L, \preccurlyeq)$ be a finite lattice, $L = \{a_1, a_2, \ldots, a_n\}$. Then $(L, \preccurlyeq)$ is a bounded lattice.
- **Proof:**

The greatest element is $a_1 \vee a_2 \vee \cdots \vee a_n$.

The least element is $a_1 \wedge a_2 \wedge \cdots \wedge a_n$.

Distributive Lattice

Definition:

- A lattice $(L, \preccurlyeq)$ is called **distributive** if for any elements a, b, and c in L we have the following distributive properties:

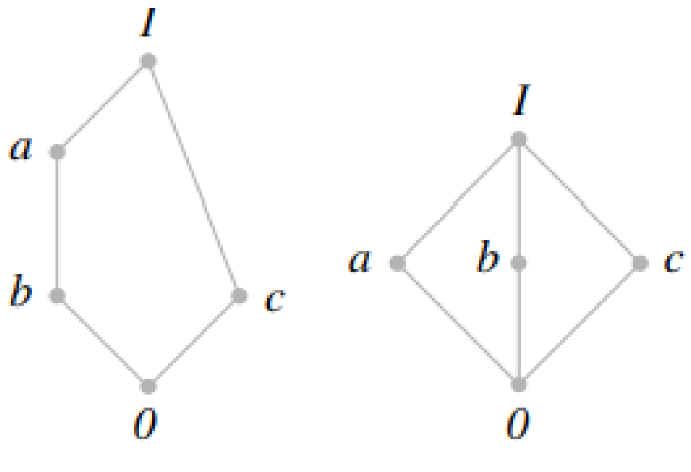
1. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
2. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Example:

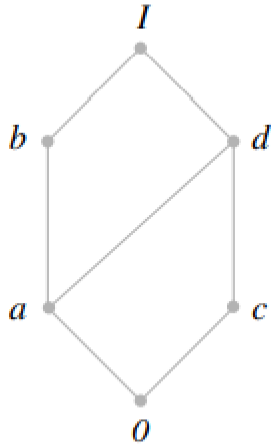
- $(P(S), \subseteq)$

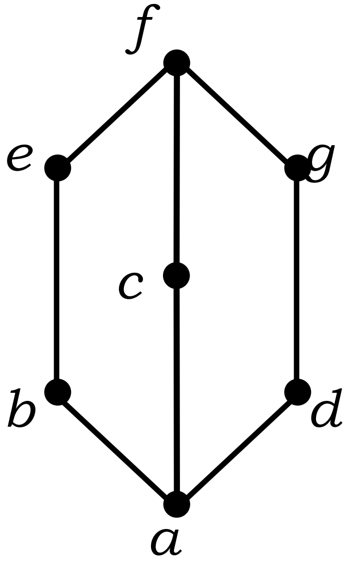
Example 2

- Show that the lattices are nondistributive.



(a) (b)





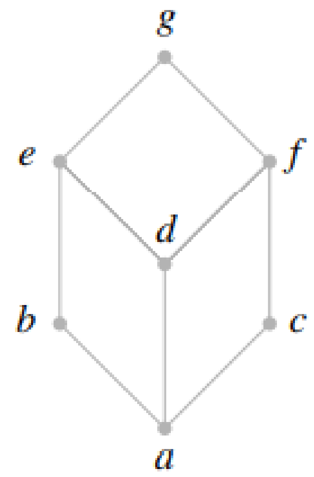
- (a) $a \wedge (b \vee c) = a \wedge I = a$; $(a \wedge b) \vee (a \wedge c) = b \vee 0 = b$.
- (b) $a \wedge (b \vee c) = a \wedge I = a$; $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$.
- Conclusion: A lattice is nondistributive if and only if it contains a **sublattice** that is isomorphic to one of the two lattices.

Complement

- Let L be a bounded lattice with greatest element I and least element 0, and let $a \in L$. An element $a' \in L$ is called a **complement** of a if

$$a \vee a' = I \text{ and } a \wedge a' = 0.$$

- If b is a complement of a, then a is a complement of b.
- $0' = I$ and $I' = 0$.
- An element can have multiple complements or no complement.



Complemented Lattice

Definition:

- A bounded lattice L is called **complemented** if every element in L has at least one complement in L.

Example:

- $(P(S), \subseteq)$ is a **complemented** lattice, since if $A \in L$, then its set complement $\bar{A}$ has the properties $A \vee \bar{A} = S$ and $A \wedge \bar{A} = \emptyset$. That is, the set complement is also the complement in the lattice L.

Example 3

- Let n be a positive integer and let D_n be the set of all positive divisors of n. Determine whether $(D_{20}, |)$ and $(D_{30}, |)$ is a complemented lattice, respectively.

Theorem 1

- Let L be a bounded distributive lattice. If a complement exists, it is unique.

Proof:

Let b, c be two complements of a.

Then $a \wedge b = 0$, $a \wedge c = 0$; $a \vee b = I$, $a \vee c = I$.

$b = b \vee 0 = b \vee (a \wedge c)$

$c = c \vee 0 = c \vee (a \wedge b)$