

# 离散数学



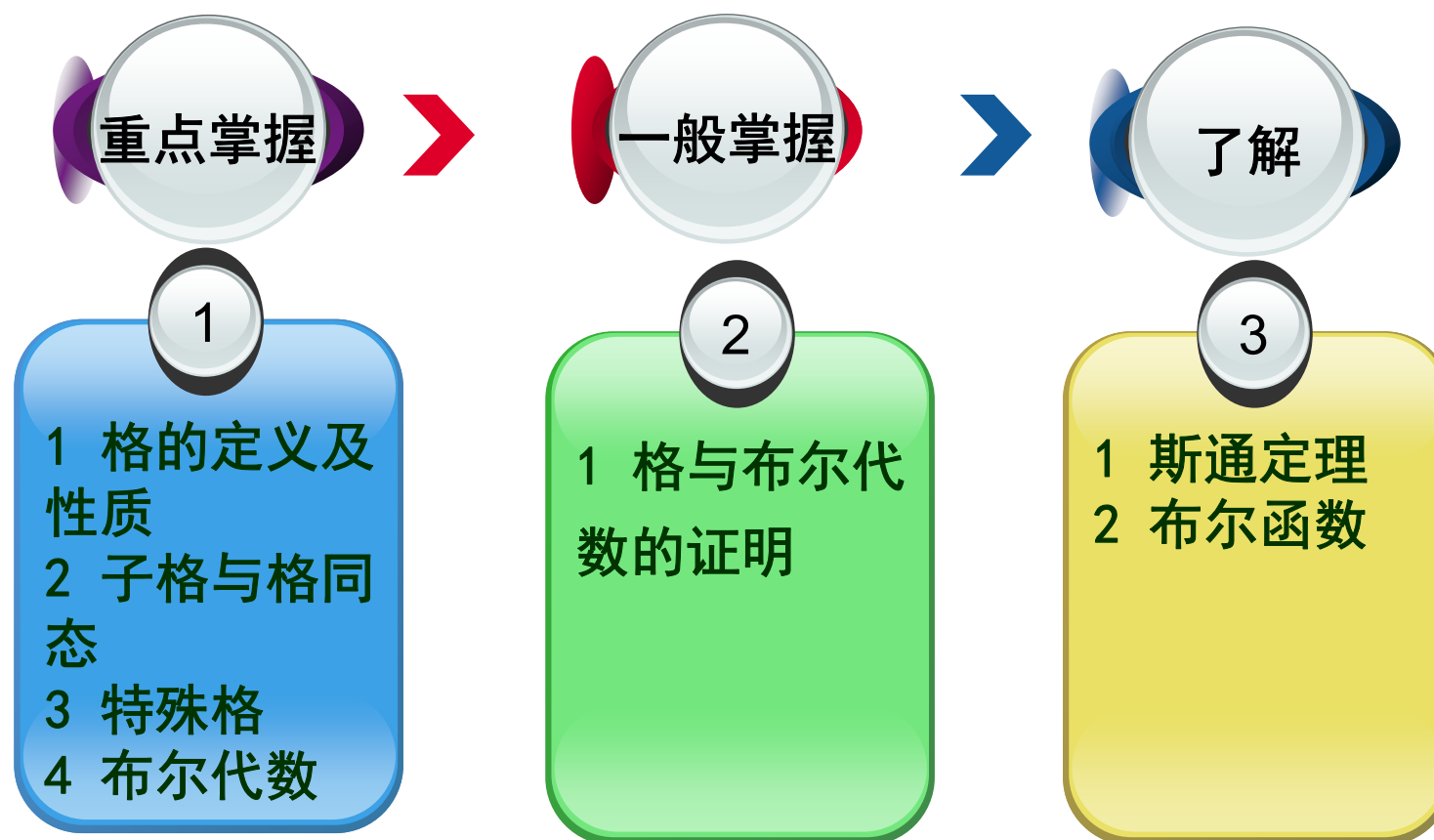
西北工业大学

2022年6月1日 星期三

## 第13章 格与布尔代数

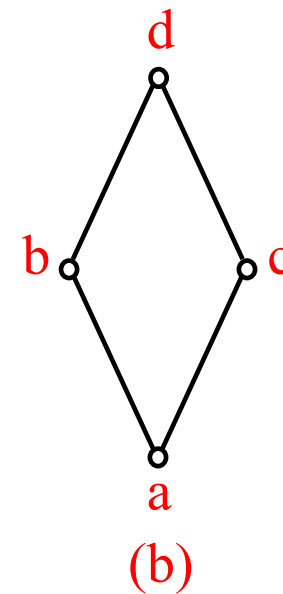
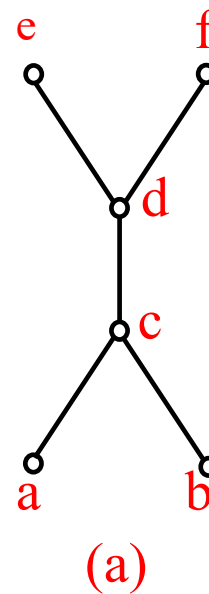
- 1 偏序格与代数格
- 2 格的性质
- 3 子格与格同态
- 4 特殊格
- 5 布尔代数

## 13.1 本章学习要求



## 偏序格

比较右边两个哈  
斯图的不同？



## 定义13.2.1

设 $\langle L, \leq \rangle$ 是一个偏序集，如果对任意 $a, b \in L$ ， $\{a, b\}$ 都有最大下界和最小上界存在，则称 $\langle L, \leq \rangle$ 是**格**，简称 $L$ 是**格**。若 $L$ 为有限集，则称格 $\langle L, \leq \rangle$ 为**有限格**。

暂且把由偏序关系定义的格称为**偏序格**

## 保交与保联

在格 $\langle L, \leq \rangle$ 中，任取 $a, b \in G$ ，则 $\{a, b\}$ 的最大下界和最小上界都是惟一存在的，且均属于 $L$ 。

用 $a \wedge b$ 表示 $\{a, b\}$ 的最大下界，称为 $a$ 与 $b$ 的**保交**，用 $a \vee b$ 表示 $\{a, b\}$ 的最小上界，称为 $a$ 与 $b$ 的**保联**，即

$$a \wedge b = \text{GLB}\{a, b\}, \quad a \vee b = \text{LUB}\{a, b\}$$

也可用 $\cap$ 和 $\cup$ 、 $\cdot$ 和 $+$ 、 $*$ 和 $\oplus$ 分别表示保交和保联

## 例13.2.1

- (1) 考虑偏序集 $\langle \mathbb{Z}^+, D \rangle$ ，其中 $\mathbb{Z}^+$ 是正整数， $D$ 是一个整除关系，问此偏序集 $\langle \mathbb{Z}^+, D \rangle$ 是否是一个格？
- (2) 设 $A$ 是一个集合， $P(A)$ 是 $A$ 的幂集，是集合上的包含关系，问此偏序集 $\langle P(A), \subseteq \rangle$ 是否是一个格？
- (3) 考虑偏序集 $\langle S_n, D \rangle$ ，其中 $D$ 是一个整除关系， $S_n$ 是 $n$ 的所有因子的集合，问此偏序集 $\langle S_n, D \rangle$ 是否是一个格？
- (4) 所有的全序集 $\langle L, \leq \rangle$ 都是格？

## 例13.2.1

**分析** 判断一个偏序集 $\langle L, \leq \rangle$ 是否是格，要对 $L$ 的所有2元素子集看它是否都有最大下界和最小上界

**解** (1) 对 $a, b \in \mathbb{Z}^+$ ，有

$$a \wedge b = \text{GLB}\{a, b\} = \text{GCD}\{a, b\} \in \mathbb{Z}^+$$

GCD表示 $\{a, b\}$ 的最大公因子。

$$a \vee b = \text{LUB}\{a, b\} = \text{LCM}\{a, b\} \in \mathbb{Z}^+$$

LCM表示 $\{a, b\}$ 的最小公倍数。

所以， $\langle \mathbb{Z}^+, D \rangle$ 是一个格。



## 例13.2.1 (续)

(2) 对  $S_1, S_2 \in P(S)$ , 有

$$S_1 \wedge S_2 = \text{GLB}\{S_1, S_2\} = S_1 \cap S_2 \in P(S)$$

$$S_1 \vee S_2 = \text{LUB}\{S_1, S_2\} = S_1 \cup S_2 \in P(S)$$

所以,  $\langle P(S), \cap, \cup \rangle$  是一个格。

(3) 由(1)可知:  $\langle S_n, D \rangle$  一定是一个格。

举例如下:

当  $n = 6$  和  $n = 24$  时, 有  $\langle S_6, D \rangle$  和  $\langle S_{24}, D \rangle$  是格。

此时  $S_6 = \{1, 2, 3, 6\}$ ,

$S_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$ ,

## 例13.2.1 (续)

对 $a, b \in S_6$  (或 $S_{24}$ ), 有

$$a \wedge b = \text{GLB}\{a, b\}$$

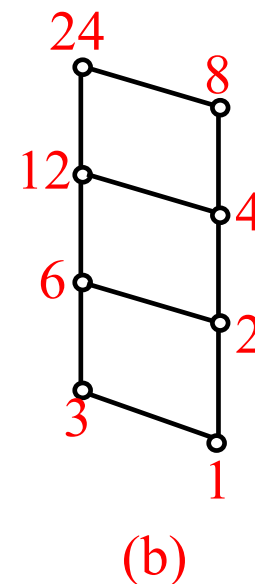
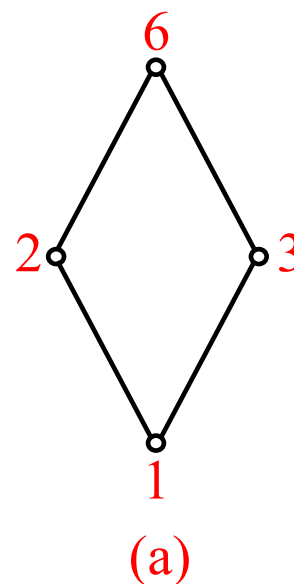
$$= \text{GCD}\{a, b\} \in S_6 \text{ (或 } S_{24})$$

$$a \vee b = \text{LUB}\{a, b\}$$

$$= \text{LCM}\{a, b\} \in S_6 \text{ (或 } S_{24})$$

对应的Hasse图如图 (a)

和图 (b) 所示。



## 例13.2.1 (续)

(4) 因为在全序集 $\langle L, \leq \rangle$ 中, 对任意 $a, b \in L$ , 都有 $a \leq b$ 或 $b \leq a$ 成立。

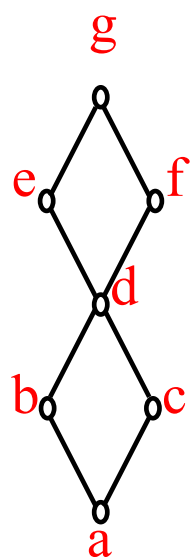
若 $a \leq b$ 成立, 则 $\{a, b\}$ 有最大下界为 $a$ , 最小上界为 $b$ ;

若 $b \leq a$ 成立, 则 $\{a, b\}$ 有最大下界为 $b$ , 最小上界为 $a$ ;

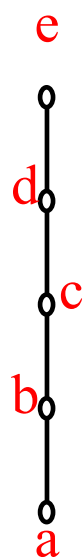
故 $\langle L, \leq \rangle$ 是一个格。

## 例13.2.2

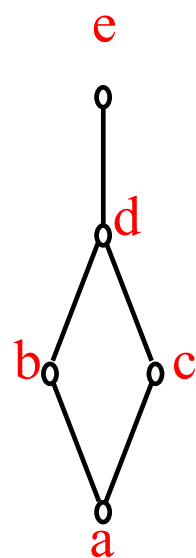
判断哈斯图如下图所示的几个偏序集是否是格。



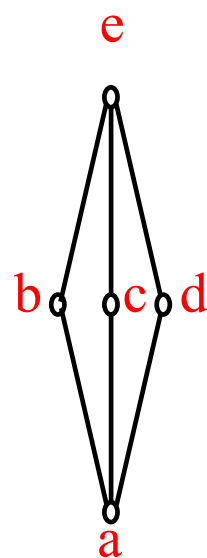
(a)



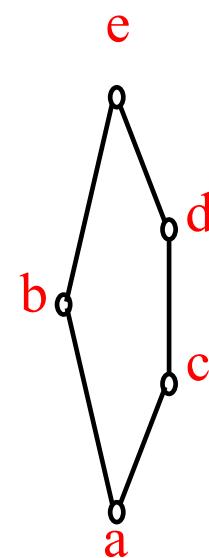
(b)



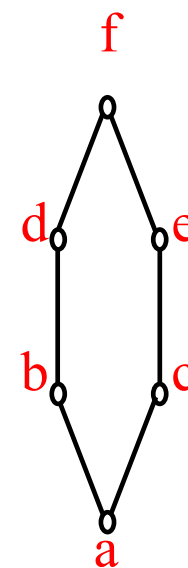
(c)



(d)

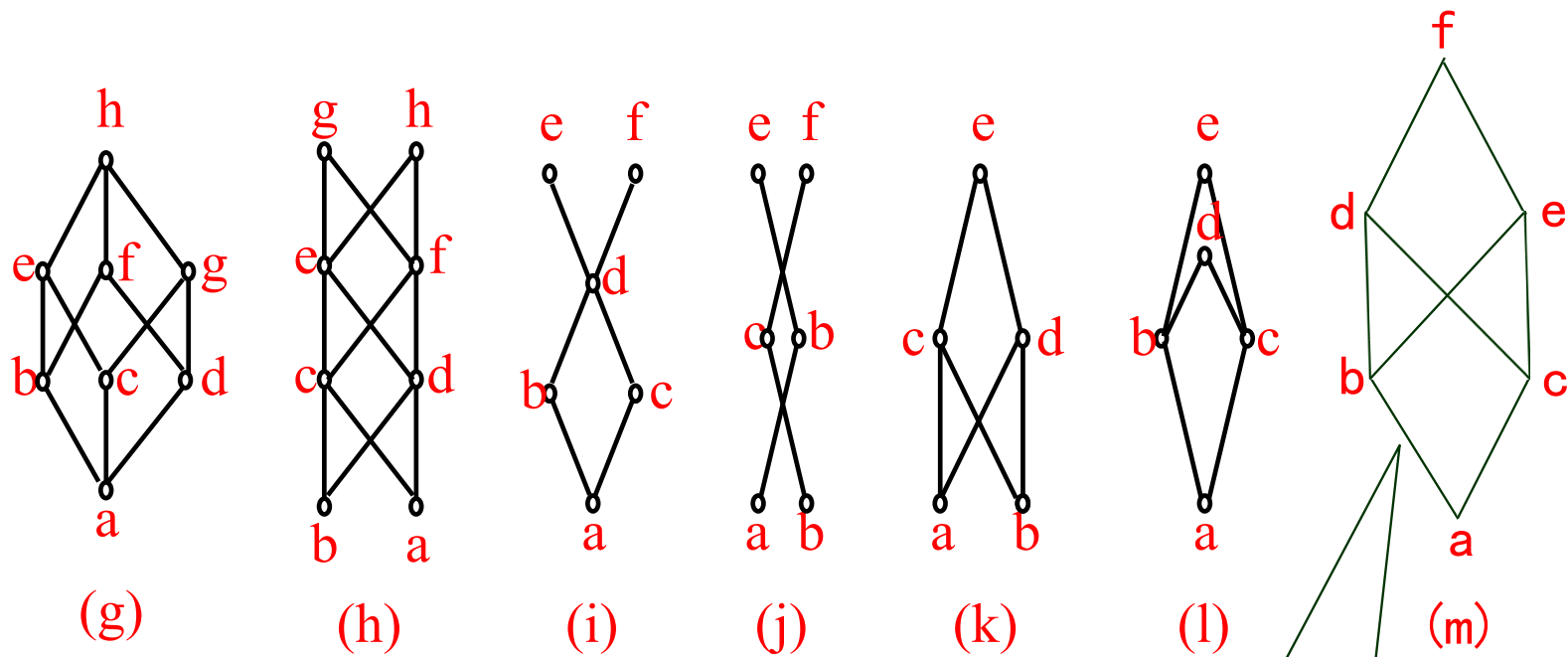


(e)



(f)

# 例13.2.2 (续)



b和c不存在最小上界  
d和e不存在最大下界

## 定义13.2.2

设 $\langle L, \wedge, \vee \rangle$ 是具有两个二元运算的代数系统，如果运算 $\wedge$ 和 $\vee$ 满足**交换律、结合律和吸收律**，则称 $\langle L, \wedge, \vee \rangle$ 为**格**。

把由代数系统定义的格称为**代数格**。

## 定理13.2.1

---

偏序格与代数格是等价的。

**注意：**偏序格与代数格等价，今后就不再区分偏序格与代数格了，而把它们统称为格。

## 自然运算与自然偏序

任何偏序格 $\langle L, \leq \rangle$ 都存在两个二元运算——保交( $\wedge$ )和保联( $\vee$ ), 称之为格 $\langle L, \leq \rangle$ 的**自然运算**;

代数格 $\langle L, \wedge, \vee \rangle$ 都可以得到一个偏序关系  $\leq$ , 称之为格 $\langle L, \wedge, \vee \rangle$ 的**自然偏序**。



## 对偶格

对于集合 $L$ 的任何偏序关系“ $\leq$ ”，其逆关系“ $\geq$ ”也是集合 $L$ 上的偏序关系；

对 $L$ 的任意子集 $T$ ， $T$ 在偏序集 $\langle L, \leq \rangle$ 中的最大下界和最小上界分别是 $\langle L, \geq \rangle$ 中的最小上界和最大下界。

因此偏序集 $\langle L, \leq \rangle$ 是格当且仅当 $\langle L, \geq \rangle$ 是格，我们称此两个格为**对偶格**；

格 $\langle L, \leq \rangle$ 的保联运算与保交运算分别是对偶格 $\langle L, \geq \rangle$ 的保交运算和保联运算。

## 对偶原理

对于格 $\langle L, \leq \rangle$ 的任何命题，将保联运算与保交运算分别换成对偶格 $\langle L, \geq \rangle$ 的保交运算和保联运算，将命题中的“ $\leq$ ”换成对偶格 $\langle L, \geq \rangle$ 中的“ $\geq$ ”，得到的一个关于对偶格 $\langle L, \geq \rangle$ 中的命题，称这个命题为**对偶命题**。

容易证明，关于格 $\langle L, \leq \rangle$ 的任何真命题，其对应的对偶命题在对偶格 $\langle L, \geq \rangle$ 中也是真命题，把这个原理称为**对偶原理**。

## 性质13.2.1

设 $\langle L, \leq \rangle$ 是格, “ $\geq$ ” 是 “ $\leq$ ” 的逆关系。则对任意 $a, b, c, d \in L$ , 有

(1) **自反性:**  $a \leq a; \quad a \geq a$

(2) **反对称性:**  $a \leq b \text{ 且 } b \leq a \Rightarrow a = b$

$$a \geq b \text{ 且 } b \geq a \Rightarrow a = b$$

(3) **传递性:**  $a \leq b \text{ 且 } b \leq c \Rightarrow a \leq c;$

$$a \geq b \text{ 且 } b \geq c \Rightarrow a \geq c$$

(4)  $a \wedge b \leq a; \quad a \vee b \geq a$

(5)  $c \leq a \text{ 且 } c \leq b \Rightarrow c \leq a \wedge b;$

$$c \geq a \text{ 且 } c \geq b \Rightarrow c \geq a \vee b$$

## 性质13.2.1 (续)

(6) **交换律**:  $a \wedge b = b \wedge a$ ;  $a \vee b = b \vee a$ 。

(7) **结合律**:  $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ ;

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

(8) **吸收律**:  $a \wedge (a \vee b) = a$ ;

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

(9) **幂等律**:  $a \wedge a = a$ ;  $a \vee a = a$

(10)  $a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$

## 性质13.2.1 (续)

$$(11) \quad a \leq b \text{ 且 } c \leq d \Rightarrow a \wedge c \leq b \wedge d;$$

$$a \leq b \text{ 且 } c \leq d \Rightarrow a \vee c \leq b \vee d$$

$$(12) \quad \text{保序性: } a \leq b \Rightarrow a \wedge c \leq b \wedge c;$$

$$a \leq b \Rightarrow a \vee c \leq b \vee c$$

$$(13) \quad \text{分配不等式:}$$

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c);$$

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

$$(14) \quad \text{模不等式:}$$

$$a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$$

## 定义13.2.3

设代数系统 $\langle L, \wedge, \vee \rangle$ 是一个格， $S \subseteq L$ ，若 $S$ 满足：

- (1)  $S \neq \Phi$ ；
- (2) 运算 $\wedge$ 和 $\vee$ 对子集 $S$ 都是封闭的；

则称 $\langle S, \wedge, \vee \rangle$ 是 $\langle L, \wedge, \vee \rangle$ 的**子格**，简称 $S$ 是 $L$ 的子格。

## 定义13.2.4

设 $\langle L, \leq \rangle$ 是一个格， $S \subseteq L$ ，若 $S$ 满足：

(1)  $S \neq \Phi$ ；

(2) 对任意 $a, b \in S$ ， $\langle L, \leq \rangle$ 的保交和保联运算都有

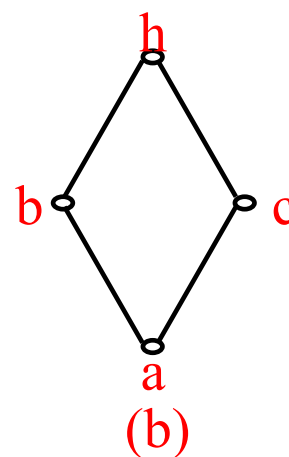
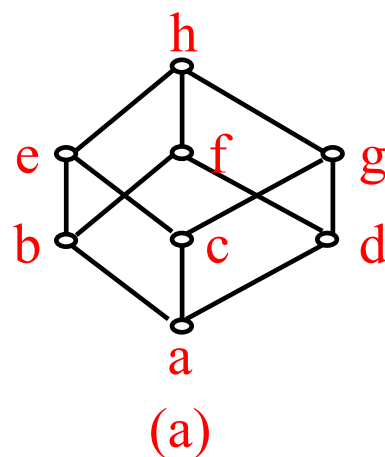
$$a \wedge b = \text{GLB}\{a, b\} \in S,$$

$$a \vee b = \text{LUB}\{a, b\} \in S,$$

则称 $\langle S, \leq \rangle$ 是 $\langle L, \leq \rangle$ 的一个子格，简称 $S$ 是 $L$ 的子格。

## 例13.2.5

在如下图 (a) 所示的偏序格  $\langle L, \leq \rangle$  中, 考虑如下子集:  $B_1 = \{a, b, g, h\}$ ,  $B_2 = \{a, b, c, d\}$ ,  $B_3 = \{a, b, c, h\}$ , 问  $B_1, B_2, B_3$  中那些是  $\langle L, \leq \rangle$  的子格?





## 例13.2.5 (续)

**分析** 显然 $B_1, B_2, B_3$ 都是 $L$ 的非空子集,  $B_1$ 是 $L$ 的子格;  $B_2$ 的2元素子集 $\{b, c\}$ 的最小上界 $e$ 不在 $B_2$ 中, 因此 $B_2$ 不是 $L$ 的子格;  $B_3$ 的2元素子集 $\{b, c\}$ 的最小上界 $e$ 不在 $B_3$ 中, 因此 $B_3$ 不是 $L$ 的子格。

**注意**, 偏序集 $\langle B_3, \leq \rangle$ 的哈斯图如上图 (b) 所示, 因此 $\langle B_3, \leq \rangle$ 是格。即存在子集关于偏序能构成格, 但不是子格, 主要原因是它们的保交或保联运算不一样。

**解**  $B_1$ 是 $L$ 的子格,  $B_2, B_3, B_4$ 都不是 $L$ 的子格。

## 例13.2.5

设 $\langle L, \leq \rangle$ 是一个格,  $a \in L$ , 令 $S = \{x \mid x \in L, x \leq a\}$ , 则 $S$ 是 $L$ 的子格。

**证明** 因为 $a \leq a$ , 所以 $a \in S$ , 即 $S$ 是非空子集。

对任意 $x, y \in S$ , 由 $x \leq a, y \leq a$ , 可知

$x \wedge y = \text{GLB}\{x, y\} \leq a$ , 即 $x \wedge y = \text{GLB}\{x, y\} \in S$

$x \vee y = \text{LUB}\{x, y\} \leq a$ , 即 $x \vee y = \text{LUB}\{x, y\} \in S$

故 $S$ 是 $L$ 的子格。

## 定义13.2.5

设 $\langle L, \wedge, \vee \rangle$ 和 $\langle S, *, \oplus \rangle$ 是两个格， $f$ 是 $L$ 到 $S$ 的映射。如果对任意 $x, y \in L$ ，都有

$$f(x \wedge y) = f(x) * f(y), \quad f(x \vee y) = f(x) \oplus f(y)$$

则称 $f$ 为从格 $\langle L, \wedge, \vee \rangle$ 到格 $\langle S, *, \oplus \rangle$ 的格同态映射，简称格同态。

如果 $f$ 是格同态，当 $f$ 分别是单射、满射和双射时， $f$ 分别称为单一格同态、满格同态和格同构。

## 定理13.2.3 (保序定理)

设 $\langle L_1, \wedge_1, \vee_1 \rangle$ 和 $\langle L_2, \wedge_2, \vee_2 \rangle$ 是两个格，对应的偏序关系为 $\leq_1$ 、 $\leq_2$ ，则有：

(1) 如 $f: L_1 \rightarrow L_2$ 是格同态，则对任意 $a, b \in L_1$ ，

$$a \leq_1 b \Rightarrow f(a) \leq_2 f(b);$$

(2) 如 $f: L_1 \rightarrow L_2$ 是格同构，则对任意 $a, b \in L_1$ ，

$$a \leq_1 b \Leftrightarrow f(a) \leq_2 f(b)。$$

**证明** (1) 对任意 $a, b \in L_1$ ，若 $a \leq_1 b$ ，则有

$$a \wedge_1 b = a, \text{ 由同态式知:}$$

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

所以 $f(a) \leq_2 f(b)$ 。

## 定理13.2.3 (续)

(2) “ $\Rightarrow$ ”：若 $f$ 是格同构，则 $f$ 是格同态。由(1)知：对任意 $a, b \in L_1$ ,

$$a \leq_1 b \Rightarrow f(a) \leq_2 f(b)。$$

“ $\Leftarrow$ ”：对任意 $a, b \in L_1$ ，有

$$f(a) \leq_2 f(b) \Rightarrow f(a) \wedge_2 f(b) = f(a)$$

于是，由同态式知

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

因 $f$ 是单射，故有

$$a \wedge_1 b = a$$

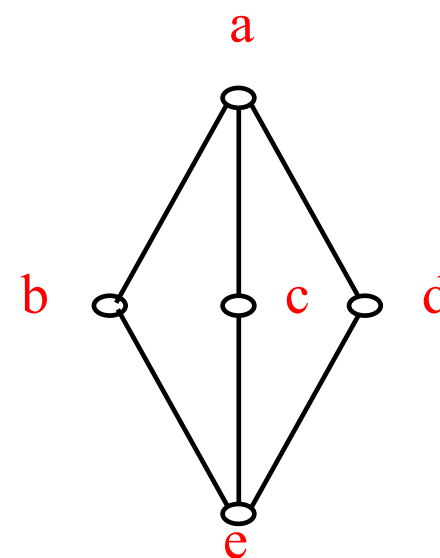
所以， $a \leq_1 b$ 。

## 例13.2.6

设 $\langle L, \leq \rangle$ 是格，其中 $L = \{a, b, c, d, e\}$ ，它的Hasse图如右图所示。 $\langle P(L), \subseteq \rangle$ 也是一个格。作映射 $f: L \rightarrow P(L)$ ，使得对任意 $x \in L$ ，有

$$f(x) = \{y \mid y \in L, y \leq x\}$$

试证明： $f$ 是保序映射，但不是格同态。



## 例13.2.6 (续)

**分析** 要证明 $f$ 是保序映射，必须验证：对任意 $x, y \in L$ ,  $x \leq y$   
 $f(x) \subseteq f(y)$ 。而证明 $f$ 不是格同态，只需要找到一对 $x, y \in L$ ,  
使得

$$f(x \vee y) \neq f(x) \cup f(y)。$$

**证明** 容易验证 $f$ 是保序映射。

对于 $b, d \in L$ , 有 $b \vee d = a$ ,  $f(b \vee d) = f(a) = L$ , 而

$$f(b) \cup f(d) = \{b, e\} \cup \{d, e\} = \{b, d, e\}$$

所以,  $f(b \vee d) \neq f(b) \cup f(d)$ , 即 $f$ 不是格同态。

## 定义13.2.6

设 $\langle L, \wedge, \vee \rangle$ 是一个格，如果对任意 $a, b, c \in L$ ，都有

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

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

即运算满足分配律，则称 $\langle L, \wedge, \vee \rangle$ 是一个**分配格**。



## 定理13.2.4

所有链都是分配格。

**证明** 设 $\langle L, \leq \rangle$ 是链，因此 $\langle L, \leq \rangle$ 是格，任取 $a, b, c \in L$ ，只有以下两种情况：

(1)  $a$ 是三者中最大的，即 $b \leq a, c \leq a$ ；

(2)  $a$ 不是三者中最大的，即 $a \leq b$ 或 $a \leq c$ 。

在情况(1)中， $b \vee c \leq a$ ，故 $a \wedge (b \vee c) = b \vee c$ 。

显然， $a \wedge b = b, a \wedge c = c$ 。所以

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

## 定理13.2.4 (续)

在情况(2)中,  $a \leq b \vee c$ , 而  $a \wedge b = a$  或  $a \wedge c = a$ , 从而  
 $(a \wedge b) \vee (a \wedge c) = a$ , 所以

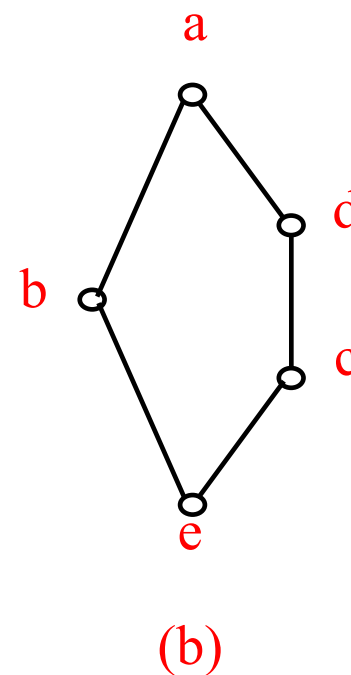
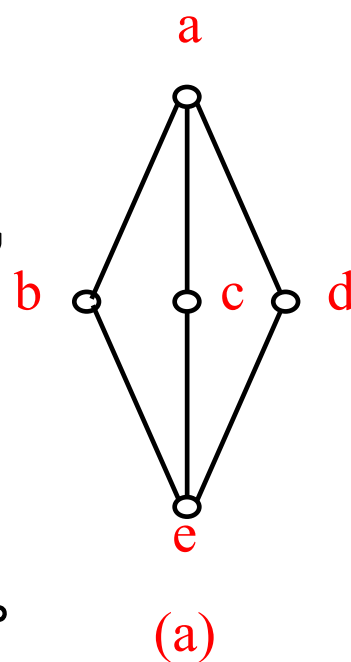
$$(a \wedge b) \vee (a \wedge c) = a = a \wedge (b \vee c)$$

所以  $\langle L, \leq \rangle$  是分配格。

## 例13.2.8

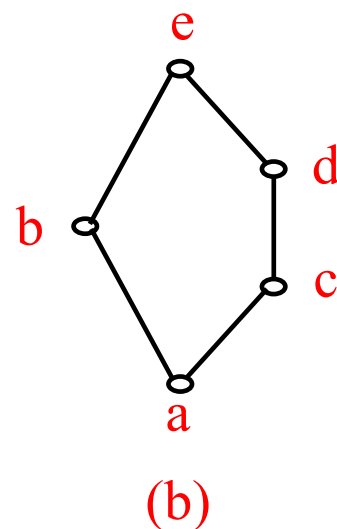
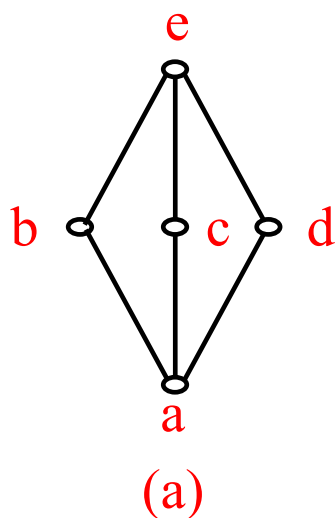
右图所示的两个格都不是分配格。

**分析** 由于链是分配格，因此在同一条链上的元素都满足分配等式，最有可能不满足分配等式的元素不在同一条链上。选取b, c, d来验证即可。



## 定理13.2.5

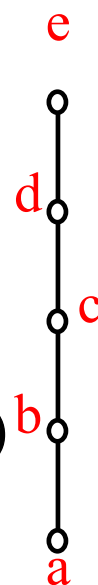
一个格是分配格的充分必要条件是该格中没有任何子格与下图中的两个五元素格中的任何一个同构。



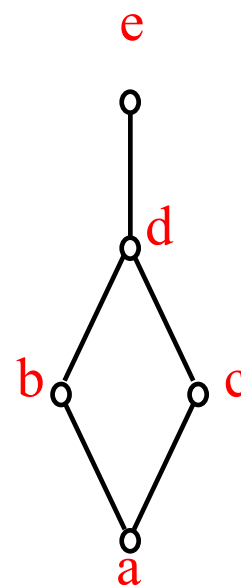
## 性质13.2.2

(1) 四个元素以下的格都是分配格；

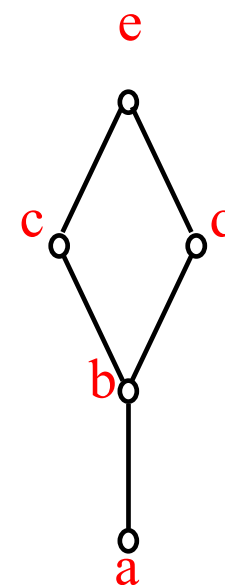
(2) 五个元素的格仅有两个格是非分配格，其余三个格(右图 (a), (b) 和 (c)) 都是分配格。



(a)



(b)



(c)

## 定理13.2.6

设 $\langle L, \wedge, \vee \rangle$ 是分配格, 对于任何 $a, x, y \in L$ ,  
如果 $a \wedge x = a \wedge y$ 且 $a \vee x = a \vee y$ , 则 $x = y$ 。

$$\begin{aligned} \text{证明 } x &= x \wedge (a \vee x) && \text{(吸收律)} \\ &= x \wedge (a \vee y) && \text{(已知 } a \vee x = a \vee y \text{)} \\ &= (x \wedge a) \vee (x \wedge y) && \text{(分配律)} \\ &= (a \wedge y) \vee (x \wedge y) && \text{(已知 } a \wedge x = a \wedge y \text{)} \\ &= y \wedge (a \vee x) && \text{(交换律, 分配律)} \\ &= y \wedge (a \vee y) && \text{(已知 } a \vee x = a \vee y \text{)} \\ &= y && \text{(吸收律)} \end{aligned}$$

## 定义13.2.8

设 $\langle L, \leq \rangle$ 是一个格，若存在元素 $a \in L$ ，使得对任意 $x \in L$ ，都有：

$$a \leq x \text{ (或 } x \leq a),$$

则称 $a$ 为格 $\langle L, \leq \rangle$ 的**全下界** (或**全上界**)，分别记为 $0$  (或 $1$ )，具有全上界和全下界的格称为**有界格**。

显然，对任意 $x \in L$ ，有

$$1 \wedge x = x \wedge 1 = x, \quad 1 \vee x = x \vee 1 = 1$$

$$0 \wedge x = x \wedge 0 = 0, \quad 0 \vee x = x \vee 0 = x$$

## 有限格与有界格

若 $\langle L, \leq \rangle$ 是有限格，设 $L = \{a_1, a_2, \dots, a_n\}$ ，由于运算“ $\wedge$ ”和“ $\vee$ ”满足结合律，所以有

$$((a_1 \wedge a_2) \wedge \dots \wedge a_n) = a_1 \wedge a_2 \wedge \dots \wedge a_n$$

$$((a_1 \vee a_2) \vee \dots \vee a_n) = a_1 \vee a_2 \vee \dots \vee a_n$$

此时， $a_1 \wedge a_2 \wedge \dots \wedge a_n$ 和 $a_1 \vee a_2 \vee \dots \vee a_n$ 分别是格 $L$ 的全下界和全上界，即有

$$a_1 \wedge a_2 \wedge \dots \wedge a_n = 0$$

$$a_1 \vee a_2 \vee \dots \vee a_n = 1$$

所以，**有限格一定是有界格。**



## 定理13.2.8

---

在格 $\langle L, \leq \rangle$ 中，全下界和全上界分别是集合 $L$ 的最小元和最大元，由于最大元和最小元的惟一性，有下面的定理：

**定理13.2.8** 设 $\langle L, \leq \rangle$ 是一个格，若格 $\langle L, \leq \rangle$ 的全上界和全下界存在，则必惟一。

## 定义13.2.9

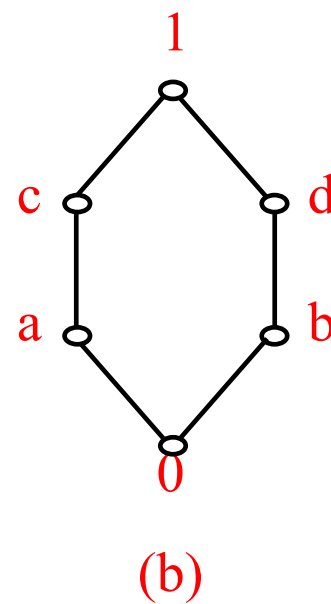
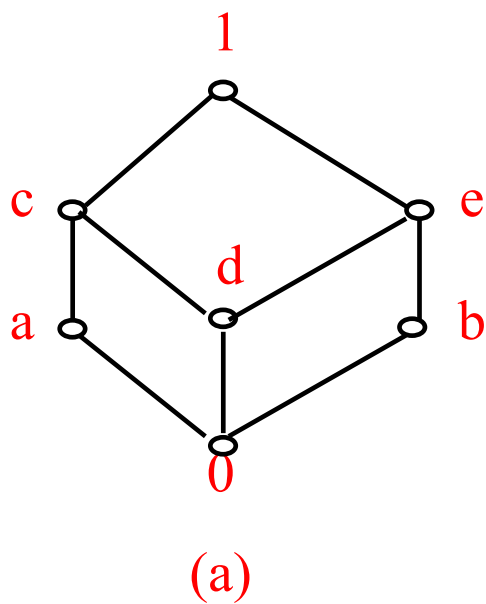
设 $\langle L, \wedge, \vee \rangle$ 为有界格，1和0分别为它的全上界和全下界， $a \in L$ 。如果存在 $b \in L$ ，使得

$$a \wedge b = 0, a \vee b = 1,$$

则称 $b$ 为 $a$ 的补元，记为 $a'$ 。若有界格 $\langle L, \wedge, \vee \rangle$ 中的所有元素都存在补元，则称 $\langle L, \wedge, \vee \rangle$ 为有补格。

## 例13.2.9

如下图有界格，求其所有元素的补元(如果有的话)。



## 例13.2.9 (续)

**解** 对于图a

$$\begin{aligned}0' &= 1, \quad 1' = 0, \\a' &= e, \quad b' = c, \\c' &= b, \quad e' = a, \\d &\text{无补元}.\end{aligned}$$

对于图b

$$\begin{aligned}0' &= 1, \quad 1' = 0, \\a' &= d, \quad a' = c, \\b' &= d, \quad b' = c, \\c' &= a, \quad c' = b, \\d' &= a, \quad d' = b\end{aligned}$$

则图a不是有补格，图b是有补格。

## 定理13.2.9

在有界分配格(既是有界格又是分配格, 简称为有界分配格) $\langle L, \wedge, \vee \rangle$ 中, 如元素 $a \in L$ 有补元存在, 则此元素的补元必惟一。

**证明** 设 $a$ 有两个补元 $b$ 和 $c$ , 由补元的定义知

$$a \wedge b = 0 = a \wedge c, \quad a \vee b = 1 = a \vee c$$

由定理13.2.6知,  $b = c$ 。

**推论13.2.1** 在有补分配格(既是有补格又是分配格, 简称为有补分配格) $\langle L, \wedge, \vee \rangle$ 中, 每个元素都存在惟一的补元。

## 定理13.2.10

设 $\langle L, \wedge, \vee \rangle$ 是有补分配格, “ $\leq$ ”是该格的自然偏序, 则对任意 $a, b \in L$ , 都有

$$(1) \quad (a')' = a; \quad (\text{对合律})$$

$$(2) \quad (a \wedge b)' = a' \vee b',$$

$$(a \vee b)' = a' \wedge b'; \quad (\text{De Morgan律})$$

$$(3) \quad a \leq b \Leftrightarrow b' \leq a';$$

$$(4) \quad a \leq b \Leftrightarrow a \wedge b' = 0 \Leftrightarrow a' \vee b = 1.$$

## 格的应用

例 某公司用信息流的格模型来控制敏感信息，公司的每个部门都具有序偶 $\langle A, C \rangle$ 表示安全类型，其中A是权限级别，C是种类。这里，权限级别A可以是0(公开), 1(内部), 2(秘密), 3(绝密)；种类C是集合{东北虎, 大熊猫, 金丝猴}的子集(这些作为项目的代码)。

问：

- (1) 信息允许从  $\langle 1, \{\text{东北虎}, \text{金丝猴}\} \rangle$  流向  $\langle 2, \{\text{金丝猴}\} \rangle$  吗？
- (2) 信息允许从  $\langle 2, \{\text{东北虎}\} \rangle$  流向  $\langle 3, \{\text{东北虎}, \text{大熊猫}\} \rangle$  吗？
- (3) 信息允许从  $\langle 1, \{\text{东北虎}, \text{金丝猴}\} \rangle$  流向哪些安全类型？
- (4) 信息允许哪些安全类型流向  $\langle 2, \{\text{大熊猫}, \text{金丝猴}\} \rangle$ ？

## 格的应用（续）

**分析** 从权限级别和种类容易得到两个格

$\langle \{0, 1, 2, 3\}, \leq \rangle$  和

$\langle P\{\text{东北虎}, \text{大熊猫}, \text{金丝猴}\}, \subseteq \rangle$

构造信息流向格如下：

$\langle A_1, C_1 \rangle \text{流向} \langle A_2, C_2 \rangle \Leftrightarrow A_1 \leq A_2 \text{ 且 } C_1 \subseteq C_2$



## 定义13.3.1

称有补分配格 $\langle L, \wedge, \vee \rangle$ 为**布尔格**。

在有补分配格中每个元都有补元而且补元惟一，可以将求元素的补元作为一种一元运算，则此布尔格 $\langle L, \wedge, \vee \rangle$ 可记为 $\langle L, \wedge, \vee, ', 0, 1 \rangle$ ，此时，称 $\langle L, \wedge, \vee, ', 0, 1 \rangle$ 为布尔代数。因此有：

**定义13.3.2** 一个布尔格 $\langle L, \wedge, \vee \rangle$ 称为**布尔代数**。若一个布尔代数的元素个数是有限的，则称此布尔代数为**有限布尔代数**，否则称为**无限布尔代数**。

## 布尔代数

布尔代数是具有补分配格，有补分配格 $\langle L, \wedge, \vee \rangle$ 必须满足它是格、有全上界和全下界、分配律成立、每个元素都有补元存在。显然，全上界1和全下界0可以用下面的同一律来描述：

同一律：

在L中存在两个元素0和1，使得对任意 $a \in L$ ，有

$$a \wedge 1 = a, a \vee 0 = a。$$

## 布尔代数

补元的存在可以用下面的互补律来描述。

**互补律**：对任意  $a \in L$ ，存在  $a' \in L$ ，使得

$$a \wedge a' = 0, a \vee a' = 1。$$

格可以用交换律、结合律、吸收律来描述。

因此，一个有补分配格就必须满足交换律、结合律、吸收律、分配律、同一律、互补律。

另外，可以证明，由交换律、分配律、同一律、互补律可以得到结合律、吸收律。所以布尔代数有下面的**等价定义**：

## 定义13.2.3

设 $\langle B, \wedge, \vee \rangle$ 是代数系统，其中 $\wedge$ 、 $\vee$ 是 $B$ 中的二元运算，如果对任意 $a, b, c \in B$ ，满足

(1) **交换律**： $a \wedge b = b \wedge a$ ,  $a \vee b = b \vee a$ ;

(2) **分配律**： $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ ,  
 $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ ;

(3) **同一律**：在 $B$ 中存在两个元素 $0$ 和 $1$ ，使得对任意 $a \in B$ ，有

$$a \wedge 1 = a, a \vee 0 = a;$$

(4) **互补律**：对任意 $a \in B$ ，存在 $a' \in B$ ，使得

$$a \wedge a' = 0, a \vee a' = 1。$$

则称 $\langle B, \wedge, \vee \rangle$ 为**布尔代数**。

## 定义13.2.3 (续)

---

通常将布尔代数 $\langle B, \wedge, \vee \rangle$ 记为 $\langle B, \wedge, \vee, ', 0, 1 \rangle$ 。为方便起见，也简称B是布尔代数。

## 定义13.2.4

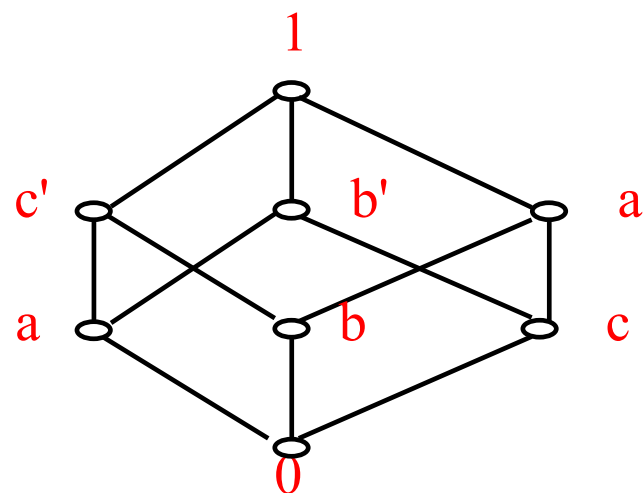
设 $\langle B, \wedge, \vee, ', 0, 1 \rangle$ 是布尔代数， $S$ 是 $B$ 的非空子集，如果运算 $\wedge, \vee$ 和 $'$ 都对 $S$ 是封闭的，则称 $\langle S, \wedge, \vee, ', 0, 1 \rangle$ 为 $\langle B, \wedge, \vee, ', 0, 1 \rangle$ 的子布尔代数，简称 $S$ 为 $B$ 的子布尔代数。

显然，对任意布尔代数 $\langle B, \wedge, \vee, ', 0, 1 \rangle$ ，子集 $\{0, 1\}$ 和 $B$ 总能构成 $B$ 的子布尔代数，这两个子布尔代数称为 $\langle B, \wedge, \vee, ', 0, 1 \rangle$ 的平凡子布尔代数。

## 例13.3.1

考察下图所示的布尔代数 $\langle B, \wedge, \vee, ', 0, 1 \rangle$ 。

$S_1 = \{a, a', 0, 1\}$ ,  $S_2 = \{a, b', c, 0\}$ ,  $S_3 = \{a, b, 0, 1\}$ , 试问 $S_1, S_2, S_3$ 能否构成 $B$ 的子布尔代数?



## 例13.3.1 (续)

**分析** 对集合中的所有元素验证3个运算 $\wedge$ ,  $\vee$ ,  $'$ 都封闭, 且 $0, 1 \in S$ 即是子布尔代数, 否则不是。

**解** 由于 $S_1$ 对运算 $\wedge$ 、 $\vee$ 和  $'$  都是封闭的, 所以 $S_1$ 能构成 $B$ 的子布尔代数。

$S_2$ 仅对运算 $\wedge$ 和 $\vee$ 封闭, 而对运算 $'$ 不封闭, 所以 $S_2$ 只能构成 $B$ 的子格, 而不能构成 $B$ 的子布尔代数。

由于 $S_3$ 对运算 $\vee$ 不是封闭的, 所以 $S_3$ 既不能构成 $B$ 的子格, 也不能构成 $B$ 的子布尔代数。并且 $S_3$ 不能构成布尔代数



## 定义13.2.5

设 $\langle B_1, \wedge, \vee, ', 0, 1 \rangle$ 和 $\langle B_2, \wedge, \vee, \neg, \alpha, \beta \rangle$ 是两个布尔代数， $f$ 是 $L$ 到 $S$ 的映射。如果对任意 $x, y \in B_1$ ，都有

$$f(x \wedge y) = f(x) \wedge f(y),$$

$$f(x \vee y) = f(x) \vee f(y)$$

$$f(x') = \neg f(x),$$

$$f(0) = \alpha, \quad f(1) = \beta$$

则称 $f$ 为从布尔代数 $\langle B_1, \wedge, \vee, ', 0, 1 \rangle$ 到 $\langle B_2, \wedge, \vee, \neg, \alpha, \beta \rangle$ 的**布尔同态映射**，简称**布尔同态**。

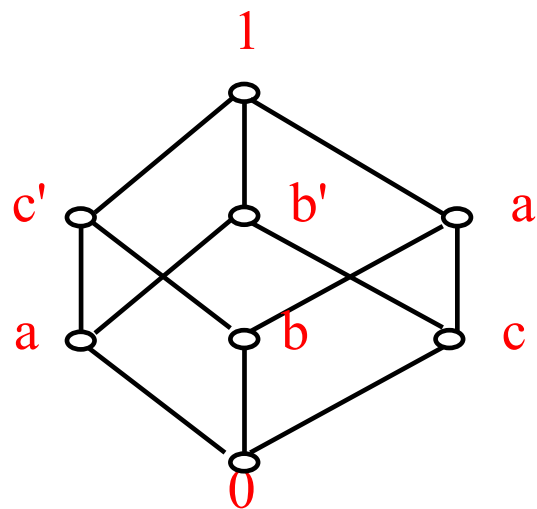
## 定义13.2.5 (续)

---

如果 $f$ 是格同态，当 $f$ 分别是单射、满射和双射时， $f$ 分别称为单一布尔同态、满布尔同态和布尔同构。

## 例13.3.2

试证明下图所示的布尔代数与集合代数 $\langle P(A), \cap, \cup, -, \Phi, A \rangle$ 同构，其中 $A = \{1, 2, 3\}$ 。



## 例13.3.2 (续)

**分析** 构造一个双射函数，对集合中的所有元素验证3个运算 $\wedge$ ,  $\vee$ ,  $'$ 都满足同态式。

**证明** 作映射 $f: B \rightarrow P(A)$ 为：

$$f(0) = \Phi, f(a) = \{1\}, f(b) = \{2\}, f(c) = \{3\}$$

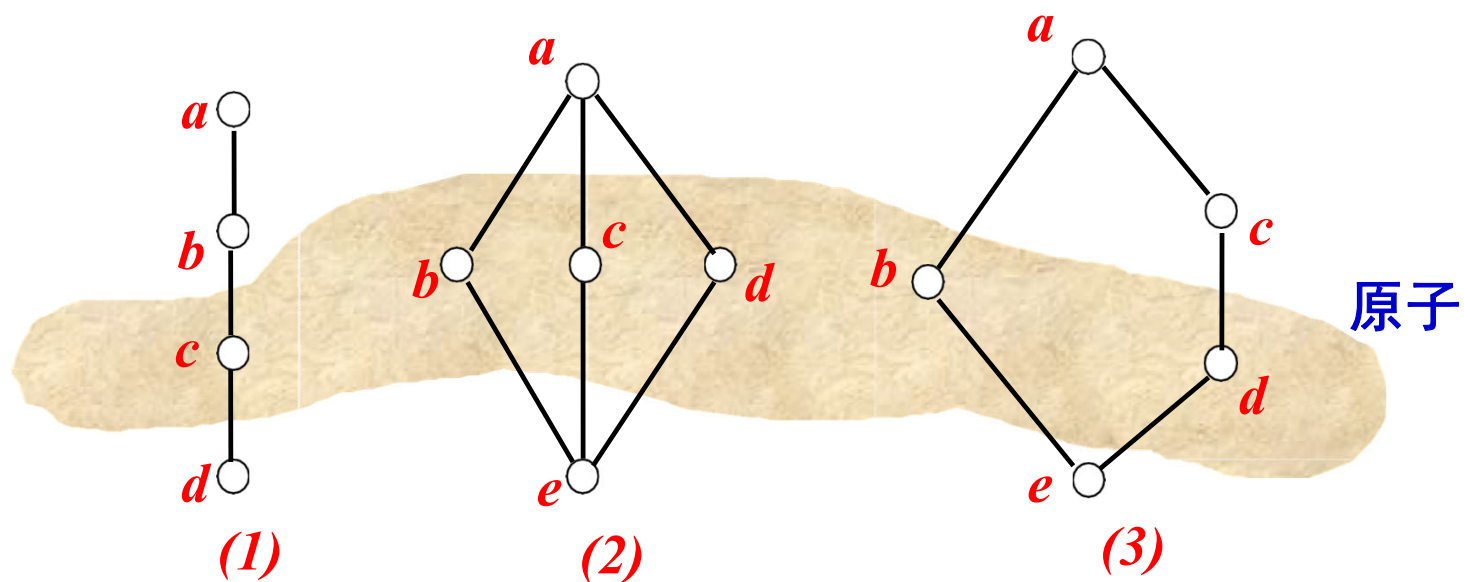
$$f(a') = \{2, 3\}, f(b') = \{1, 3\}, f(c') = \{1, 2\}, f(1) = \{1, 2, 3\}$$

显然 $f$ 是双射，容易验证 $f$ 对3个运算 $\wedge$ ,  $\vee$ ,  $'$ 都满足同态式，因此 $f$ 是布尔同构，即这两个布尔代数同构。

## 格中的原子

- 定义：设 $L$ 是格， $L$ 中有最小元(全下界) $0$ ，给定元素  
 $a \neq 0$ ，若 $\forall b \in L$ ，有：  
$$0 < b \leq a \Rightarrow b = a$$
  
则称 $a$ 是 $L$ 中的原子  
(原子是覆盖最小元的那些元素。)
- 设 $a, b$ 是格 $L$ 中的原子，若 $a \neq b$ ，则 $a \wedge b = 0$ 
  - 假设 $a \wedge b \neq 0$ ，注意： $a \wedge b \leq a$ 且 $a \wedge b \leq b$ ，由原子的定义：  
 $a \wedge b = a, a \wedge b = b, \therefore a = b$ ，矛盾。

## 格中的原子



## 有限布尔代数的表示定理

---

- 任一有限布尔代数 $B$ 同构于 $B$ 中所有的原子构成的集合 $A$ 的幂集代数系统 $P(A)$ 。

$$\text{即 } (B, \wedge, \vee, ', 0, 1) \cong (P(A), \cap, \cup, \sim, \emptyset, A)$$

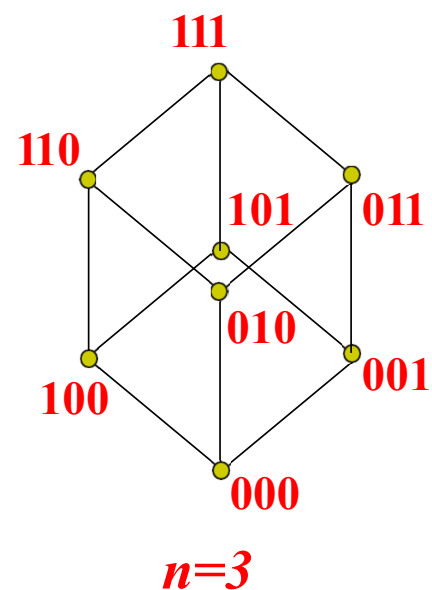
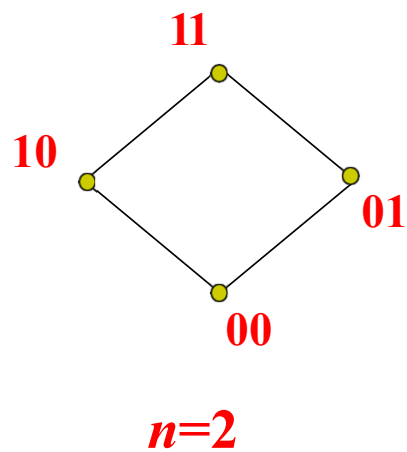
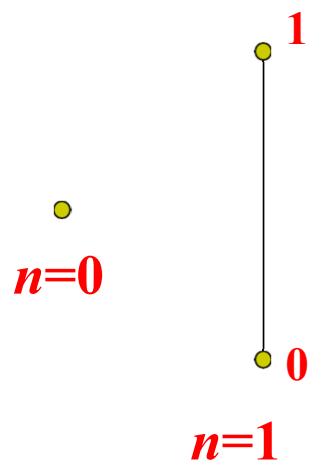
## 有限布尔代数基数是2的整数次幂

- 任何有限布尔代数的基数为 $2^n$ ,  $n$ 是自然数。
  - 设 $B$ 是有限代数系统,  $A$ 是 $B$ 中所有原子的集合。  
则:  $B \cong P(A)$ ,  $\therefore |B| = |P(A)| = 2^{|A|}$
- 等势的有限布尔代数均同构

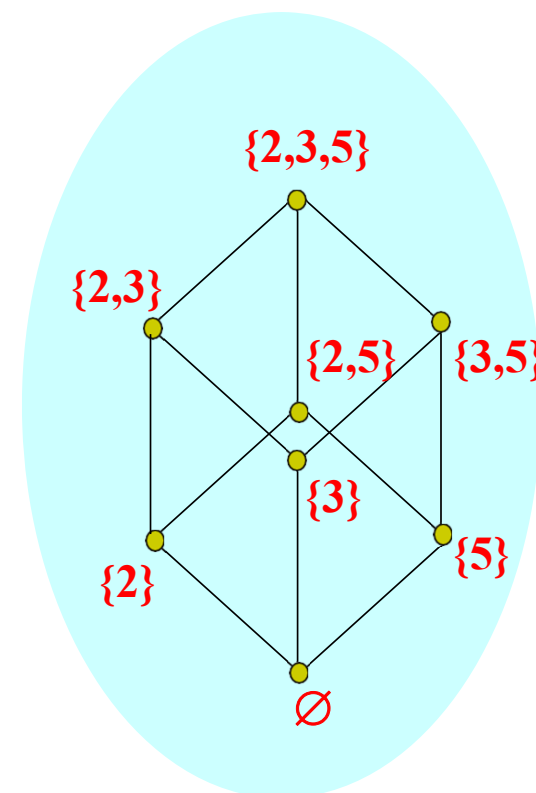
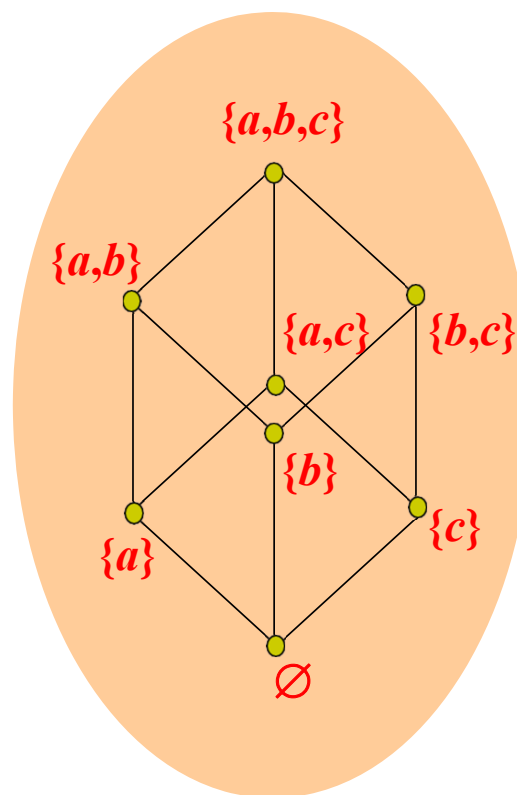
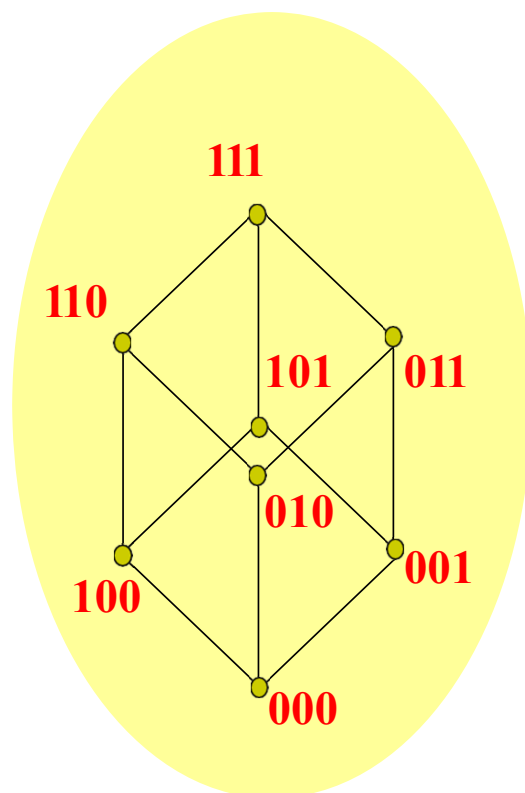


# 最小的几个有限布尔代数

与含 $n$ 个元素的集合的幂集代数系统同构的布尔代数记为 $B_n$ 。



# Hasse Diagrams of Isomorphic Lattices



## $B_n$ as Product of $n$ $B$ 's

---

- $B_1, (\{0,1\}, \wedge, \vee, 1, 0, ')$ , is denoted as  $B$ .
- For any  $n \geq 1$ ,  $B_n$  is the product  $B \times B \times \dots \times B$  of  $B$ ,  $n$  factors, where  $B \times B \times \dots \times B$  is given the product partial order.

**Product partial order:**

$x \leq y$  if and only if  $x_k \leq y_k$  for all  $k$ .

# Hasse Diagrams of $B_n$

