离散数学

西安交通大学
计算机学院

第七章 格与布尔代数

§1.格

§2.布尔代数

§ 1.格

- 格的定义
- 格的性质
- 模格
- 分配格
- 有界格和有补格

§ 1.格

定义1.格(lattice)

设 (L, ∗, ⊕)是代数系统， ∗ 和 ⊕ 是 L上的两个二元运算。若∗ 运算和 ⊕ 运算满足

(1) 结合律：$(a*b)*c=a*(b*c)$, $(a\oplus b)\oplus c=a\oplus(b\oplus c)$；

(2) 交换律： $a*b=b*a$, $a\oplus b=b\oplus a$；

(3) 幂等律： $a*a=a$, $a\oplus a=a$；

(4) 吸收律： $a*(a\oplus b)=a$, $a\oplus (a*b)=a$；

则称 (L, ∗, ⊕)是格(**代数格**)。

注：•验证格要先验证两个二元运算∗ 和 ⊕ 的封闭性；

•从格的定义可以看到格这种代数系统和环、域这些代数系统有着很大的不同。

•格中的两个二元运算的性质具有**对称性**。即一个运算所具有的性质，另一个也有，反之亦然。这正是格这种代数系统的特点。格中的许多性质均与此种特点有关。

例1. 集合代数$(2^X, \cap, \cup)$ 是格。

由第三章知$\cap$和$\cup$都是2^X上的二元运算，由第三章§2定理2知：

(1) $\cap$和$\cup$运算分别满足结合律；

(2) $\cap$和$\cup$运算分别满足交换律；

(3) $\cap$和$\cup$运算分别满足幂等律；

(4) $\cap$和$\cup$运算分别满足吸收律；

所以，由格的定义知 $(2^X, \cap, \cup)$是格。

例2. 命题代数(**P**, $\wedge$,$\vee$) 是格 。$\wedge$和$\vee$可看作是**P**上的两个二元运算;

(1)结合律：$(p\wedge q)\wedge r \Leftrightarrow p\wedge(q\wedge r)$， $(p\vee q)\vee r \Leftrightarrow p\vee(q\vee r)$；

(2)交换律：$p\wedge q \Leftrightarrow q\wedge p$， $p\vee q \Leftrightarrow q\vee p$；

(3)幂等律：$p\wedge p \Leftrightarrow p$， $p\vee p \Leftrightarrow p$；

(4)吸收律：$p\wedge(p\vee q) \Leftrightarrow p$， $p\vee(p\wedge q) \Leftrightarrow p$；

所以，由格的定义知(**P**, $\wedge$,$\vee$)是格。

例3. $(I,\ *,\ \oplus)$是格。I是整数集合，$*$和$\oplus$是I上的取小、取大运算。即 $\forall a,b\in I$, $a*b=\min\{a,b\}$，$a\oplus b=\max\{a,b\}$ 。

于是$*$和$\oplus$都是I上的二元运算，$(I, *, \oplus)$ 是代数系统。

(1)结合律：由于 $\forall a,b,c\in I$，有

$$(a * b) * c=\min\{\min\{a,b\},c\}=\min\{a,b,c\}$$

$$a * (b * c)=\min\{a,\min\{b,c\}\}=\min\{a,b,c\}$$

所以 $(a * b) * c= a * (b * c)$

又有 $(a \oplus b) \oplus c=\max\{\max\{a,b\},c\}=\max\{a,b,c\}$

$$a \oplus (b \oplus c)=\max\{a,\max\{b,c\}\}=\max\{a,b,c\}$$

所以 $(a \oplus b) \oplus c= a \oplus (b \oplus c)$

故 $*$ 运算和 $\oplus$ 运算满足结合律；

(2)交换律： 由于 $\forall a,b \in I$，有

$$a * b=\min\{a,b\}=\min\{b,a\}=b * a$$

$$a \oplus b=\max\{a,b\}=\max\{b,a\}=b \oplus a$$

故 $*$ 运算和 $\oplus$ 运算满足交换律；

(3)幂等律：由于 $\forall a \in I$，有

$$a * a=\min\{a,a\}= a$$

$$a \oplus a=\max\{a,a\}=a$$

故 $*$ 运算和 $\oplus$ 运算满足幂等律;

(4)吸收律：由于 $\forall a,b \in I$，有

$$a*(a\oplus b)=\min\{a, \max\{a,b\}\}=a$$

$$a\oplus(a*b)=\max\{a,\min\{a,b\}\}=a$$

故 $*$ 运算和 $\oplus$ 运算满足吸收律;

所以，由格的定义知$(I, *, \oplus)$是格。

定理1. 设$(L, *, \oplus)$是格。则$\forall a,b \in L$，

$$a*b=a \Leftrightarrow a\oplus b=b \quad 。$$

[证]. 先证$\Rightarrow$):

$$\begin{aligned} a\oplus b &= (a*b)\oplus b && (\text{条件：} a*b=a) \\ &= b\oplus(b*a) && (\text{交换律}) \\ &= b && (\text{吸收律}) \end{aligned}$$

次证$\Leftarrow$):

$$\begin{aligned} a*b &= a*(a\oplus b) && (\text{条件：} a\oplus b=b) \\ &= a && (\text{吸收律}) \quad 。 \end{aligned}$$

定义7. 上确界 下确界

（least upper bound, greatest lower bound）

设$(A,\leq)$是半序集，$B\subseteq A$， $z_0\in A$ 。则我们称

(1)z_0是B的上确界

$\Leftrightarrow(\forall x\in B)(x\leq z_0)\wedge(\forall z\in A)((\forall x\in B)(x\leq z)\Rightarrow z_0\leq z)$；

(2)z_0是B的下确界

$\Leftrightarrow(\forall x\in B)(z_0\leq x)\wedge(\forall z\in A)((\forall x\in B)(z\leq x)\Rightarrow z\leq z_0)$；

(3)上确界即是最小上界，记为LUB(B);

下确界即是最大下界，记为GLB(B)。

定理2. 设(L, $*$, $\oplus$)是格。定义二元关系 $\preccurlyeq' \subseteq L\times L$ 如下：

$\forall a,b\in L$，$a\preccurlyeq' b \Leftrightarrow a*b=a$ 那么

(1)$\preccurlyeq'$是L上的一个半序关系 ，(L, $\preccurlyeq'$) 是一个半序集;

(2)对于任何一对元素$a,b\in L$，其上、下确界都存在，且

$$LUB(\{a,b\})= a\oplus b$$

$$GLB (\{a,b\})= a*b$$ 。

[证].(1) $\preccurlyeq'$**是**L上的一个半序关系

① $\preccurlyeq'$是自反的：$\forall a\in L$， $a*a=a$ (幂等律)

$\Rightarrow a\preccurlyeq' a$;

②$\preccurlyeq'$是反对称的：$\forall a,b\in L$，

$a\preccurlyeq' b \wedge b\preccurlyeq' a\Rightarrow a*b=a \wedge b*a=b$

$\Rightarrow a*b=a \wedge a*b=b$ (交换律)

$\Rightarrow a=a*b \wedge a*b=b$ (等号交换律)

$\Rightarrow a=b$ (等号传递律)；

③ $\preccurlyeq'$是传递的：$\forall a,b,c \in L$，

$a \preccurlyeq' b \wedge b \preccurlyeq' c \Rightarrow a*b=a \wedge b*c=b$

$$\begin{aligned} \Rightarrow a*c &= (a*b)*c && (a*b=a) \\ &= a*(b*c) && (\text{结合律}) \\ &= a*b && (b*c=b) \\ &= a && (a*b=a) \end{aligned}$$

$\Rightarrow a \preccurlyeq' c$；

(2)对于任何一对元素$a,b \in L$， 其上、下确界都存在。

① $\forall a,b \in L$，$LUB(\{a,b\})= a \oplus b$：

$a \preccurlyeq' a \oplus b$, $b \preccurlyeq' a \oplus b$：

$a*(a\oplus b)=a$ (吸收律)

$\Rightarrow a\preccurlyeq' a\oplus b$；

$b*(a\oplus b)=b*(b\oplus a)$ (交换律)

$=b$ (吸收律)

$\Rightarrow b\preccurlyeq' a\oplus b$；

$a\preccurlyeq' c \wedge b\preccurlyeq' c \Rightarrow a\oplus b\preccurlyeq' c$：

$a\preccurlyeq' c \wedge b\preccurlyeq' c$

$\Rightarrow a*c=a \wedge b*c=b$

$\Rightarrow a\oplus c=c \wedge b\oplus c=c$ (定理1)

$\Rightarrow (a\oplus b)\oplus c= a\oplus (b\oplus c)$ (结合律)

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

$= c$ $(a\oplus c=c)$

$\Rightarrow (a\oplus b)*c= a\oplus b$ (定理1)

$\Rightarrow a\oplus b\preccurlyeq' c$；

②$\forall a,b \in L$，GLB({a,b})= a*b：

$a*b \preccurlyeq' a$, $a*b \preccurlyeq' b$：

$$(a*b)*a = a*(b*a) \qquad \text{(结合律)}$$
$$= a*(a*b) \qquad \text{(交换律)}$$
$$= (a*a)*b \qquad \text{(结合律)}$$
$$= a*b \qquad \text{(幂等律)}$$

$\Rightarrow a*b \preccurlyeq' a$；

$$(a*b)*b = a*(b*b) \qquad \text{(结合律)}$$
$$= a*b \qquad \text{(幂等律)}$$

$\Rightarrow a*b \preccurlyeq' b$；

$c\preccurlyeq' a \wedge c\preccurlyeq' b \Rightarrow c\preccurlyeq' a * b$：

$$c\preccurlyeq' a \wedge c\preccurlyeq' b$$

$$\Rightarrow c*a=c \wedge c*b=c$$

$$\Rightarrow c*(a*b) =(c*a)*b \qquad \text{(结合律)}$$

$$=c*b \qquad (c*a=c)$$

$$=c \qquad (c*b=c)$$

$$\Rightarrow c\preccurlyeq' a*b$$ 。

注：$\preccurlyeq'$称为是由$*$运算诱导出的L上的半序关系， 称$\preccurlyeq'$是与格$(L, *, \oplus)$伴随的关系； $(L, \preccurlyeq')$称为是与格$(L, *, \oplus)$伴随集；

根据定理1,半序关系$\preccurlyeq'$也可由$\oplus$运算诱导出来；

$\forall a,b\in L$， $a\preccurlyeq' b \Leftrightarrow a*b=a \Leftrightarrow a\oplus b=b$ 。

引理1. 设(L, $\preccurlyeq$)是一半序集，$\preccurlyeq$是L上的半序关系。则$\forall a,b,c\in L$

(1) $GLB(\{GLB(\{a,b\}),c\})=GLB(\{a,b,c\})$

(2) $GLB(\{a,GLB(\{b,c\})\})=GLB(\{a,b,c\})$

(3) $LUB(\{LUB(\{a,b\}),c\})=LUB(\{a,b,c\})$

(4) $LUB(\{a,LUB(\{b,c\})\})=LUB(\{a,b,c\})$

［证］. 只证(1) ,(3)

(1)令：$x = GLB(\{GLB(\{a,b\}),c\})= GLB(\{z,c\})$

$y =GLB(\{a,b,c\})$, $z= GLB(\{a,b\})$;

①$x\preccurlyeq y$：

由$x\preccurlyeq z\preccurlyeq a$, $x\preccurlyeq z\preccurlyeq b$, $x\preccurlyeq c$， 有$x\preccurlyeq a$, $x\preccurlyeq b$, $x\preccurlyeq c$， 有$x\preccurlyeq y$ (下确界y的最大性);

② $y\preccurlyeq x$：

由$y\preccurlyeq a$, $y\preccurlyeq b$, $y\preccurlyeq c$， 有$y\preccurlyeq z$ (下确界z的最大性), $y\preccurlyeq c$，有$y\preccurlyeq x$ (下确界x的最大性) ;

所以，由半序关系$\preccurlyeq$的反对称性，得到 $x = y$ ；

(3)令：$x = \mathrm{LUB}(\{\mathrm{LUB}(\{a,b\}),c\}) = \mathrm{LUB}(\{z,c\})$

$y = \mathrm{LUB}(\{a,b,c\})$, $z = \mathrm{LUB}(\{a,b\})$；

①$x \preccurlyeq y$：

由$a \preccurlyeq y$, $b \preccurlyeq y$, $c \preccurlyeq y$， 有$z \preccurlyeq y$ (上确界z的最小性), $c \preccurlyeq y$，有$x \preccurlyeq y$ (上确界x的最小性)；

②$y \preccurlyeq x$：

由$a \preccurlyeq z \preccurlyeq x$, $b \preccurlyeq z \preccurlyeq x$, $c \preccurlyeq x$， 有$a \preccurlyeq x$, $b \preccurlyeq x$, $c \preccurlyeq x$， 有$y \preccurlyeq x$ (上确界y的最小性)；

所以，由半序关系$\preccurlyeq$的反对称性，得到 $x = y$ 。

定理3. 设(L, $\preccurlyeq$)是一半序集，$\preccurlyeq$是L上的半序关系。如果对于任何一对元素其上、下确界都存在，即

$$\forall a,b\in L,\quad LUB(\{a,b\})\in L,\quad GLB(\{a,b\})\in L,$$

则 可以定义L上的两个二元运算

$$*, \oplus : L\times L\to L \qquad 如下：$$

$$\forall a,b\in L,\quad a*b=GLB(\{a,b\}),\ a\oplus b=LUB(\{a,b\})$$

那么

(1) (L, $*$, $\oplus$)是格；

(2)格(L, $*$, $\oplus$)的伴随关系$\preccurlyeq'$与原半序关系$\preccurlyeq$重合(相等) 。

[证].首先，(L, $*$, $\oplus$)是代数系统

①后者唯一：由第四章§6定理2知上、下确界若存在必唯一，因而 $*$, $\oplus$的运算结果是唯一的；

②封闭性：由已知条件和两个运算的定义可知

离散数学

定理2. 设(A,≤)是半序集,B⊆A。若B有上(下)确界，则必是唯一的。

[证].仿定理1可证。留给学者。

注：•最大(小)元一定是极大(小)元;
　　极大(小)元不一定是最大(小)元;
　　极大(小)元存在不一定有最大(小)元;
　•最大(小)元一定是上(下)确界;
　　上(下)确界不一定是最大(小)元;
　　上(下)确界存在不一定有最大(小)元;
　•上(下)确界一定是上(下)界;
　　上(下)界不一定是上(下)确界;
　　上(下)界存在不一定有上(下)确界;
　•讨论B的上(下)确界的前提是B的上(下)界存在;

$\forall a,b \in L \qquad a*b=GLB(\{a,b\}) \in L$，

$\qquad\qquad\qquad\;\; a \oplus b=LUB(\{a,b\}) \in L$；

故 $*$ 运算和 $\oplus$ 运算是封闭的；

(1) $(L, *, \oplus)$是格

①结合律：根据引理1的(1),(2)，由于 $\forall a,b,c \in L$，有

$(a * b) * c= GLB(\{GLB(\{a,b\}),c\})= GLB(\{a,b,c\})$

$a * (b * c)= GLB(\{a, GLB(\{b,c\})\})= GLB(\{a,b,c\})$

所以 $(a * b) * c= a * (b * c)$

又根据引理1的(3),(4)，由于 $\forall a,b,c \in L$，有

$(a \oplus b) \oplus c= LUB(\{LUB(\{a,b\}),c\})= LUB(\{a,b,c\})$

$a \oplus (b \oplus c)= LUB(\{a, LUB(\{b,c\})\})= LUB(\{a,b,c\})$

所以 $(a \oplus b) \oplus c= a \oplus (b \oplus c)$

故 $*$ 运算和 $\oplus$ 运算满足结合律；

②交换律： 由于 $\forall a,b \in L$，有

$$a * b = GLB(\{a,b\}) = GLB(\{b,a\}) = b * a$$

$$a \oplus b = LUB(\{a,b\}) = LUB(\{b,a\}) = b \oplus a$$

故 $*$ 运算和 $\oplus$ 运算满足交换律；

③幂等律：由于 $\forall a \in L$，有

$$a * a = GLB(\{a,a\}) = a$$

$$a \oplus a = LUB(\{a,a\}) = a$$

故 $*$ 运算和 $\oplus$ 运算满足幂等律;

④吸收律：由于 $\forall a,b \in L$，有

$$a*(a\oplus b) = GLB(\{a, LUB(\{a,b\})\}) = a \quad (\text{因} a \preccurlyeq LUB(\{a,b\}))$$

$$a\oplus(a*b) = LUB(\{a, GLB(\{a,b\})\}) = a \quad (\text{因} GLB(\{a,b\}) \preccurlyeq a)$$

故 $*$ 运算和 $\oplus$ 运算满足吸收律;

所以，由格的定义知 $(L, *, \oplus)$ 是格。

(2) $\preccurlyeq' = \preccurlyeq$

$\forall a,b \in L$，$(a,b) \in \preccurlyeq' \Leftrightarrow a \preccurlyeq' b$

$\Leftrightarrow a * b = a$ (定理2的定义)

$\Leftrightarrow GLB(\{a,b\}) = a$ (定理3的定义)

$\Leftrightarrow a \preccurlyeq b$ (因 $GLB(\{a,b\}) \preccurlyeq b$)

$\Leftrightarrow (a,b) \in \preccurlyeq$

所以 $\preccurlyeq' = \preccurlyeq$ 。

定义1′.(半序格)

设$(L,\preccurlyeq)$ 是半序集，$\preccurlyeq$是L上的半序关系。若L中任意两个元素都有上、下确界存在，即

$$\forall a,b\in L,\quad LUB(\{a,b\})\in L,\quad GLB(\{a,b\})\in L,$$

则称$(L,\preccurlyeq)$ 是格(半序格)。

例4. $(2^X,\subseteq)$是(半序)格

包含关系$\subseteq$是集合上的半序关系(第三章§1定理1)；

其次$\forall A,B\in 2^X$，都有

$LUB(\{A,B\})=A\cup B\in 2^X$ (第三章§2定理2(3)(3′))；

$GLB(\{A,B\})=A\cap B\in 2^X$ (第三章§2定理2(3)(3″))；

所以，根据定义1′可知，$(2^X,\subseteq)$是格。

注：•由于定义1和定义1′的等价性，以后关于格，既可以用 $(L, *, \oplus)$ 表示，也可以用 $(L, \preccurlyeq)$ 表示；

•当用 $(L, *, \oplus)$表示格时，半序关系$\preccurlyeq$是用 $a * b=a$ 或 $a \oplus b=b$ 定义的；

•当用$(L, \preccurlyeq)$ 表示格时，两个运算是用 $a * b = GLB\{a,b\}$ 及 $a \oplus b = LUB\{a,b\}$ 定义的；

•更多的时候则用$(L, \preccurlyeq, *, \oplus)$ 表示格，即将格中的代数性质和序性质都表示出来，这样就将格的性质描述的比较全面了；

例如 $(2^X, \cap, \cup)$是格，$(2^X, \subseteq)$也是格，且是同一个格，因此通常用$(2^X，\subseteq，\cap，\cup)$表示这个格。

定理4.设$(L, \preccurlyeq, *, \oplus)$ 是格。则$\forall a,b\in L$，

$$a \preccurlyeq b \Leftrightarrow a*b=a \Leftrightarrow a\oplus b=b \text{。}$$

[证]**.** 根据定理2的注， 有

$$a \preccurlyeq' b \Leftrightarrow a*b=a \Leftrightarrow a\oplus b=b$$

根据定理3， 有

$$\preccurlyeq' = \preccurlyeq$$

因此， 得到

$$a \preccurlyeq b \Leftrightarrow a*b=a \Leftrightarrow a\oplus b=b \text{。}$$

例5. (N, GCD, LCM)是格；且其伴随关系是整除关系‘|’。

这里： N 为自然数集合，$\forall a,b \in N$,

GCD{a,b}= a和b最大公约数

LCM{a,b}= a和b最小公倍数

由于两个自然数的最大公约数和最小公倍数是唯一的，且为自然数，故$*$ 和 $\oplus$ 是N上的两个二元运算。

(1)$\forall a,b,c \in N$，由于有

GCD{GCD{a,b},c}=GCD{a,b,c}=GCD{a,GCD{b,c}}

LCM{LCM{a,b},c}= LCM{a,b,c}＝LCM{a, LCM{b,c}}

故GCD运算和GCD运算满足结合律。

(2)$\forall a,b \in N$，由于有

$$GCD\{a,b\} = GCD\{b,a\}$$

$$LCM\ \{a,b\} = LCM\ \{b,a\}$$

故GCD运算和LCM运算满足交换律。

(3)$\forall a \in N$，由于有

$$GCD\{a,a\} = a$$

$$LCM\{a,a\} = a$$

故GCD运算和LCM运算满足幂等律。

(4)$\forall a,b \in N$，由于有

$$GCD\{a, LCM\{a,b\}\} = a$$

$$LCM\{a, GCD\{a,b\}\} = a$$

故GCD运算和LCM运算满足吸收律。

由格的定义1知 (N, GCD, LCM)是格(代数格)。

根据定理2，其伴随关系 $\preccurlyeq' \subseteq N \times N$的定义 如下：

$\forall a,b \in N$，$a \preccurlyeq' b \Leftrightarrow GCD\{a,b\}=a \Leftrightarrow LCM\{a,b\}=b$

从而可得 $a \preccurlyeq' b \Leftrightarrow a \mid b \Leftrightarrow$ a整除b 。

因此，格(N, GCD, LCM)的伴随关系$\preccurlyeq'$就是N上的整除关系‘|’。

例6. (N, |)是格；由关系 ‘|’ 诱导出的运算是GCD, LCM 。N 为自然数集合，‘|’是N上的整除关系。

(1)自反性：$\forall a \in N, \exists 1 \in N, a=a \times 1 \Rightarrow a \mid a$；

(2)反对称性：$\forall a,b \in N$，

$a \mid b \wedge b \mid a$

$\Rightarrow \exists r,k \in N,\ b=a \times r \wedge a=b \times k$

$\Rightarrow a=b$ (因$a=b \times k=(a \times r) \times k=a \times (r \times k) \Rightarrow r \times k=1 \Rightarrow r=k=1$)；

(3)传递性：$\forall a,b,c\in N$，

$a|b\wedge b|c$

$\Rightarrow \exists r,k\in N,\ b=a\times r\wedge c=b\times k$

$\Rightarrow \exists (r\times k)\in N,\ c=b\times k=(a\times r)\times k=a\times(r\times k)$

$\Rightarrow a|c$；

其次，要证 N中任意两个元素的上、下确界都存在。即 $\forall a,b\in L$，$LUB(\{a,b\})=LCM\{a,b\}\in N$

$GLB(\{a,b\})=GCD\{a,b\}\in N$

任何两个自然数a,b的最大公约数GCD{a,b}，最小公倍数LCM{a,b}都存在唯一且是自然数。因此，只须证明 $\forall a,b\in N$，$LUB(\{a,b\})=LCM\{a,b\}$

$GLB(\{a,b\})=GCD\{a,b\}$

即可。

(1)GLB({a,b})＝GCD{a,b}。设α= GCD{a,b}

(a)下界：由于α是a，b的最大公约数，于是有$\alpha|a$ 且$\alpha|b$，故α是a，b的一个下界；

(b)最大性：若β是a，b另一下界，则有$\beta|a$且$\beta|b$，故β是a，b的一个公约数。由最大公约数的定义知有$\beta|\alpha$，故α是a，b的最大下界。

由(a) (b)可知GLB{a,b}= GCD{a,b}。

(2) LUB({a,b})＝LCM{a,b}。设γ = LCM{a,b}

(a)上界：由于γ是a，b的最小公倍数，于是有$a|\gamma$ 且$b|\gamma$，故γ是a，b的一个上界；

(b)最小性：若δ 是a，b另一上界，则有$a|\delta$且$b|\delta$，故δ是a，b的一个公倍数。由最小公倍数的定义知有$\gamma|\delta$，故γ是a，b的最小上界。

由(a) (b)可知LUB{a,b}= LCM{a,b}。

由格的定义1′知(N, |)是格(半序格) 。

由定理3，由 ‘|’诱导出的N上的两个二元运算 $*$, $\oplus$: $L\times L\rightarrow L$ 的定义如下：

$$\forall a,b\in L,\quad a*b=GLB(\{a,b\}),\ a\oplus b=LUB(\{a,b\})$$

而由上面的证明可知 $a*b=GCD\{a,b\}$, $a\oplus b=LCM\{a,b\}$。

因此，由关系‘|’诱导出的两个运算就是GCD, LCM 。

注：•由例5和例6可知，如果将求最大公约数和求最小公倍数作为N上的两个二元运算，则其伴随关系就是N上的整除关系。因此，根据定理2可知，整除关系是半序关系，且任两个元素的上确界就是它们的最小公倍数，任两个元素的下确界就是它们的最大公约数;

•反之，若在N上定义一个整除关系，则此关系是一个半序关系，且任两个元素的上确界就是它们的最小公倍数，任两个元素的下确界就是它们的最大公约数。由其诱导出的两个二元运算就是求最大公约数和求最小公倍数.因此，根据定理3可知，这两个二元运算满足结合律、交换律、幂等律、吸收律;

•这两个例子验证了定义1和定义1′的等价性;

•通常将此格记为(N, | , GCD, LCM).

对偶原理(duality principle):

设 $(L,\preccurlyeq,*,\oplus)$是格，$\succcurlyeq$ 是$\preccurlyeq$的逆关系。则

(1)在格$(L,\preccurlyeq,*,\oplus)$中实行：

将 $\preccurlyeq$换成$\succcurlyeq$；将 $*$ 换成 $\oplus$；将 $\oplus$ 换成 $*$；

得到的$(L,\succcurlyeq,\oplus,*)$仍是一格；

(2)若T是原格中某个已经证明的定理，那么在定理T的条件和结论中实行：

将 $\preccurlyeq$换成$\succcurlyeq$；将 $*$ 换成 $\oplus$；将 $\oplus$ 换成 $*$；

由此所得到的新的定理T′在原格中仍然成立。

[证]. 格中的对偶原理实质上来源于两个二元运算 $*$ 和 $\oplus$ 所具有的结合律、交换律、幂等律、吸收律的对称性以及半序关系$\preccurlyeq$和其逆关系$\succcurlyeq$的对称性。

注：•格$(L,\succcurlyeq,\oplus,*)$称为原格$(L,\preccurlyeq,*,\oplus)$的对偶格。实际上，它们互为对偶；

•定理T′称为原定理T的对偶定理。实际上，它们互为对偶；

定理5.(运算的保序性)

设$(L,\preccurlyeq,*,\oplus)$是格。$\forall a,b,c\in L$，

(1)$a\preccurlyeq b\Rightarrow a*c\preccurlyeq b*c$；

(2)$a\preccurlyeq b\Rightarrow a\oplus c\preccurlyeq b\oplus c$；

[证]. 只证(1)

$(a*c)*(b*c)=(a*b)*(c*c)$　(*的结合律、交换律)

$=(a*b)*c$　(*的幂等律)

$=a*c$　(由条件$a\preccurlyeq b$从定理4)

$\Rightarrow a*c\preccurlyeq b*c$　(定理4)

定理6.(分配不等式)

设$(L,\preccurlyeq,*,\oplus)$是格。$\forall a,b,c\in L$，

(1)$a\oplus(b*c)\preccurlyeq(a\oplus b)*(a\oplus c)$；

(2)$(a*b)\oplus(a*c)\preccurlyeq a*(b\oplus c)$。

[证]. 只证(1)

由上确界是上界的性质得：$a\preccurlyeq a\oplus b$，$a\preccurlyeq a\oplus c$

由下确界的最大性得：$a\preccurlyeq(a\oplus b)*(a\oplus c)$ ①

又由下确界是下界、上确界是上界的性质得：

$b*c\preccurlyeq b\preccurlyeq a\oplus b$，$b*c\preccurlyeq c\preccurlyeq a\oplus c$

由半序关系$\preccurlyeq$的传递性得：$b*c\preccurlyeq a\oplus b$，$b*c\preccurlyeq a\oplus c$

再次由下确界的最大性得：

$b*c\preccurlyeq(a\oplus b)*(a\oplus c)$ ②

最后由①、②，**利用**上确界的最小性得：

$a\oplus(b*c)\preccurlyeq(a\oplus b)*(a\oplus c)$。

定理7.(模不等式)

设$(L,\preccurlyeq,*,\oplus)$是格。$\forall a,b,c\in L$，

(1) $(a*b)\oplus(a*c)\preccurlyeq a*(b\oplus(a*c))$；

(2) $a\oplus(b*(a\oplus c))\preccurlyeq(a\oplus b)*(a\oplus c)$ 。

[证]. 只证(1)

由下确界是下界、上确界是上界的性质得：

$a*b\preccurlyeq a$ ，$a*b\preccurlyeq b\preccurlyeq b\oplus(a*c)$

由半序关系$\preccurlyeq$的传递性得：$a*b\preccurlyeq b\oplus(a*c)$

由下确界的最大性得：

$a*b\preccurlyeq a*(b\oplus(a*c))$ ①

同理，由下确界是下界、上确界是上界的性质得：

$a * c \preccurlyeq a$ ，$a * c \preccurlyeq b \oplus (a * c)$

由下确界的最大性得：

$a * c \preccurlyeq a * (b \oplus (a * c))$ ②

最后由① 、②，利用上确界的最小性得：

$(a * b) \oplus (a * c) \preccurlyeq a * (b \oplus (a * c))$ 。

定义2.模律(modular law)

设$(X,*,\oplus)$是代数系统。$*$和$\oplus$是X上的两个二元运算。若$\forall a,b,c\in L$，都有

(1) $(a*b)\oplus(a*c)=a*(b\oplus(a*c))$

(2) $(a\oplus b)*(a\oplus c)=a\oplus(b*(a\oplus c))$

则称$*$运算和$\oplus$运算满足模律。

定义3.模格(modular lattice)

设$(L,\preccurlyeq,*,\oplus)$是格。若$*$运算和$\oplus$运算满足模律，则称$(L,\preccurlyeq,*,\oplus)$为模格。

定理8. 设(L,$\preccurlyeq$,$*$,$\oplus$)是格。(L,$\preccurlyeq$,$*$,$\oplus$)是模格$\Leftrightarrow \forall$a,b,c$\in$L，

$$a \preccurlyeq c \Rightarrow a \oplus (b * c) = (a \oplus b) * c \quad 。$$

[证]. $\Rightarrow$)：

(L,$\preccurlyeq$,$*$,$\oplus$)是模格

$\Rightarrow a \oplus (b * (a \oplus c)) = (a \oplus b) * (a \oplus c)$ (模律2))

$\Rightarrow a \oplus (b * c) = (a \oplus b) * c$ (定理4： $a \preccurlyeq c \Rightarrow a \oplus c = c$)

$\Leftarrow$)：只证模律2)

$a \preccurlyeq a \oplus c$ (上确界是上界)

$\Rightarrow a \oplus (b * (a \oplus c)) = (a \oplus b) * (a \oplus c)$

(利用条件： $a \preccurlyeq c \Rightarrow a \oplus (b * \mathbf{c}) = (a \oplus b) * \mathbf{c}$)

所以，(L,$\preccurlyeq$,$*$,$\oplus$)是模格。

例7. $(2^X, \subseteq, \cap, \cup)$是模格

由例1已知$(2^X, \subseteq, \cap, \cup)$是格。其次$\forall A,B,C \in 2^X$,

$A \subseteq C$

$\Rightarrow A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (分配律)

$= (A \cup B) \cap C$ $(A \subseteq C \Rightarrow A \cup C = C)$

所以，根据定理8可知，$(2^X, \subseteq, \cap, \cup)$是模格。

例8.如图1所示的$(L,\preccurlyeq)$是模格。

根据定义1′易知$(L,\preccurlyeq)$是格。

它有12个序组：

$a_0 \preccurlyeq a_0$， $a_0 \preccurlyeq a_1$， $a_0 \preccurlyeq a_2$，

$a_0 \preccurlyeq a_3$， $a_0 \preccurlyeq a_4$， $a_1 \preccurlyeq a_1$，

$a_2 \preccurlyeq a_2$， $a_2 \preccurlyeq a_1$， $a_3 \preccurlyeq a_3$，

$a_3 \preccurlyeq a_1$， $a_4 \preccurlyeq a_4$， $a_4 \preccurlyeq a_1$，

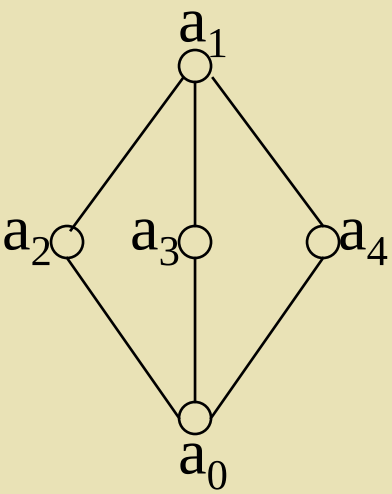

图1

在这些序组下， 定理8的充分必要条件：

$$a \preccurlyeq c \Rightarrow a \oplus (b * c) = (a \oplus b) * c$$

中b有5个取值，共计需验证12×5=60个等式。

象征性的验证一个等式： $a_0 \preccurlyeq a_1$， $b= a_4$， 这时

$$a \oplus (b * c)= a_0 \oplus (a_4 * a_1)= a_0 \oplus a_4= a_4$$

$$(a \oplus b) * c= (a_0 \oplus a_4) * a_1= a_4 * a_1= a_4$$

即 $a \oplus (b * c)= (a \oplus b) * c$

所以，根据定理8可知，如图1所示的$(L,\preccurlyeq)$是模格。

例9.如图2所示的$(L,\preccurlyeq)$不是模格。

根据定义1′易知$(L,\preccurlyeq)$是格。

但是，在序组$b_2 \preccurlyeq b_3$下，取

$b= b_4$，这时

$$a \oplus (b * c)= b_2 \oplus (b_4 * b_3)$$

$$= b_2 \oplus b_0= b_2$$

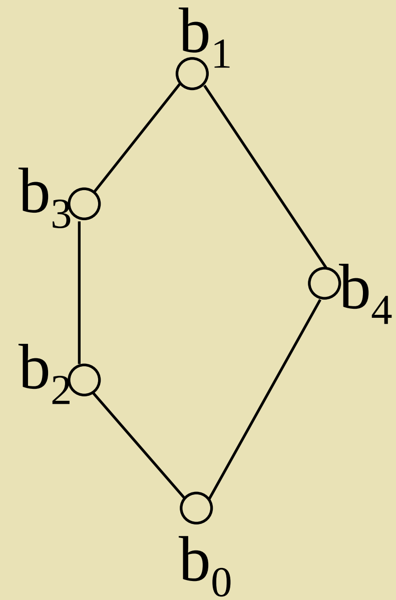

图2

$$(a \oplus b) * c= (b_2 \oplus b_4) * b_3= b_1 * b_3= b_3$$

即　$a \oplus (b * c) \neq (a \oplus b) * c$

所以，根据定理8可知，如图1所示的$(L,\preccurlyeq)$不是模格。

定义4. 分配格(distributive lattice)

设$(L,\preccurlyeq,*,\oplus)$是格。若$*$运算和$\oplus$运算满足分配律，即$\forall a,b,c\in L$，

(1) $a * (b \oplus c) = (a * b) \oplus (a * c)$；

(2) $a \oplus (b * c) = (a \oplus b) * (a \oplus c)$；

则称$(L,\preccurlyeq,*,\oplus)$ 是分配格。

例10. $(2^X, \subseteq, \cap, \cup)$是分配格。

由例1已知$(2^X, \subseteq, \cap, \cup)$是格。

其次，由第三章§2定理2(7)知，$\cap$运算和$\cup$运算满足分配律，即 $\forall A,B,C\in 2^X$，有:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

所以，由定义4知$(2^X, \subseteq, \cap, \cup)$是分配格。

例11. (N, | , GCD, LCM)是分配格。

由例5和例6已知(N, | , GCD, LCM)是格。

其次，GCD运算和LCM运算满足分配律，即$\forall a,b,c \in N$，有:

(1)GCD{a,LCM{b,c}}=LCM{GCD{a,b},GCD{a,c}}；

(2)LCM{a,GCD{b,c}}=GCD{LCM{a,b},LCM{a,c}}；

只证(1)

设：α＝GCD{a,LCM{b,c}}= GCD{a, γ}

β = LCM{GCD{a,b},

GCD{a,c}} = LCM{δ,λ}

其中：γ = LCM{b,c}，δ = GCD{a,b}， λ = GCD{a,c}

先证：$\alpha|\beta$

设$b=b_1d$，$c=c_1d$，于是有$\gamma = LCM\{b,c\} = b_1c_1d$ (并且$GCD\{b_1, c_1\}=1$)。

又由 $\alpha = GCD\{a, \gamma\}$，有$\alpha|a$， $\alpha|\gamma$，故可设$\alpha = b_2c_2d'$ (这里$b_2|b_1$，$c_2|c_1$， $d'|d$，且$GCD\{b_2, c_2\}=1$)，从而有

$a = \alpha\cdot a_1 = b_2c_2d'\cdot a_1$， $b=b_1d= b_2d'\cdot b'$，$c=c_1d = c_2d'\cdot c'$，

所以 $\delta = GCD\{a,b\}= b_2d'\cdot GCD\{c_2\cdot a_1,b'\}= b_2d'\cdot\delta'$

$\lambda = GCD\{a,c\}= c_2d'\cdot GCD\{b_2\cdot a_1,c'\}= c_2d'\cdot\lambda'$

故此 $\beta= LCM\{\delta , \lambda\}$

$= b_2c_2d'\cdot LCM\{\delta',\lambda'\}$ (因为 $GCD\{b_2, c_2\}=1$)

$= b_2c_2d'\cdot\beta ' = \alpha\cdot\beta '$

所以$\alpha|\beta$；

次证：$\beta|\alpha$

$(\delta|a\wedge\delta|b)\wedge(\lambda|a\wedge\lambda|c)$

(因$\delta = GCD\{a,b\}$，$\lambda = GCD\{a,c\}$)

$\Rightarrow(\delta|a\wedge\lambda|a)\wedge(\delta|b\wedge\lambda|c)$ ($\wedge$的结合律、交换律)

$\Rightarrow LCM\{\delta,\lambda\}|a \wedge LCM\{\delta,\lambda\}| LCM\{b,c\}$

(最小公倍数的最小性、保序性)

$\Rightarrow\beta|a\wedge\beta|\gamma$ (因 $\beta=LCM\{\delta,\lambda\}$，$\gamma = LCM\{b,c\}$)

$\Rightarrow\beta|GCD\{a, \gamma\}$ (最大公约数的最大性)

$\Rightarrow\beta|\alpha$ (因$\alpha=GCD\{a, \gamma\}$)；

最后，由‘|’是半序关系，具有反对称性可知

$\alpha=\beta$

所以，由定义4知(N, | , GCD, LCM)是分配格。证明完毕。

例12. 例8图1所示的格(L,≼)不是分配格 。

因为 $a\oplus(b*c)$

$=a_2\oplus(a_3*a_4)$

$=a_2\oplus a_0$

$=a_2$

$(a\oplus b)*(a\oplus c)$

$=(a_2\oplus a_3)*(a_2\oplus a_4)$

$=a_1*a_1$

$=a_1$

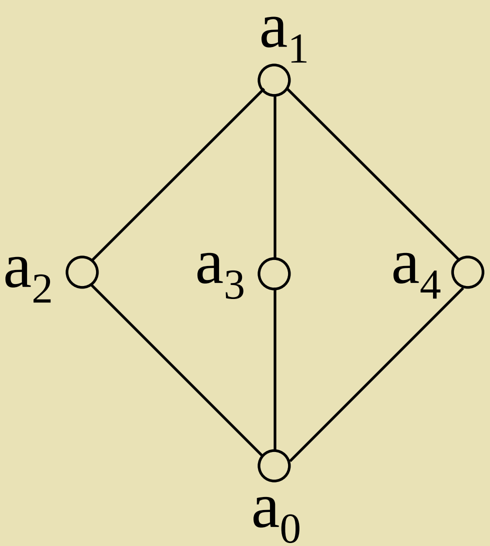

图1

即 $a\oplus(b*c)\neq(a\oplus b)*(a\oplus c)$

所以，根据定义4知(L,≼)不是分配格 。

例13. 例9图2所示的格(L,≼)不是分配格 。

因为 $a\oplus(b*c)$

$=b_2\oplus (b_3*b_4)$

$=b_2\oplus b_0$

$=b_2$

$(a\oplus b)*(a\oplus c)$

$=(b_2\oplus b_3)*(b_2\oplus b_4)$

$=b_3 *b_1$

$=b_3$

即 $a\oplus (b*c)\neq(a\oplus b)*(a\oplus c)$

所以，根据定义4知(L,≼)不是分配格 。

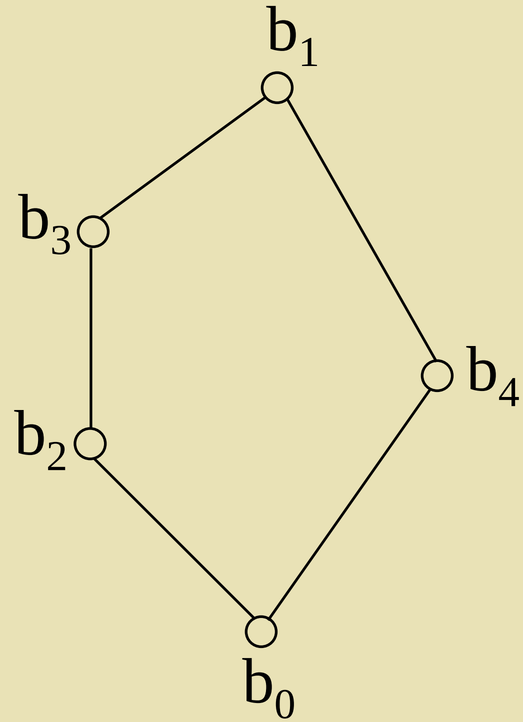

图2

结论. 一个格不是分配格$\Leftrightarrow$

它有与图1或图2所示的格同构的子格；

或者：

一个格是分配格$\Leftrightarrow$

它没有与图1和图2所示的格同构的子格。

定理9.分配格一定是模格。即

$(L,\preccurlyeq,*,\oplus)$是分配格$\Rightarrow(L,\preccurlyeq,*,\oplus)$是模格。

[证]. $\forall a,b,c\in L$， $a\oplus(b*c)$

$=(a\oplus b)*(a\oplus c)$ (分配律)

$=(a\oplus b)*c$ $(a\preccurlyeq c\Rightarrow a\oplus c=c)$

所以，由模格的定义3可知， $(L,\preccurlyeq,*,\oplus)$是模格。

定理10.分配格一定有消去律。即

若$(L,\preccurlyeq,*,\oplus)$是分配格，则 $\forall a,b,c\in L$，

$$\left.\begin{array}{l} a*b=a*c \\ a\oplus b=a\oplus c \end{array}\right\}\Rightarrow b=c$$

[证]. $\forall a,b,c\in L$，$b=b*(b\oplus a)$ (吸收律)

$=b*(a\oplus b)$ (交换律)

$=b*(a\oplus c)$ (条件：$a\oplus b=a\oplus c$)

$=(b*a)\oplus(b*c)$ (分配律)

$=(a*b)\oplus(b*c)$ (交换律)

$=(a*c)\oplus(b*c)$ (条件：$a*b=a*c$)

$=(a\oplus b)*c$ (分配律)

$=(a\oplus c)*c$ ($a\oplus b=a\oplus c$)

$=c$ (吸收律)

所以，结论成立。

定理11.全序格一定是分配格。即， 若$(L,\preccurlyeq,*,\oplus)$是格，并且$\preccurlyeq$是$L$上的全序关系，则$(L,\preccurlyeq,*,\oplus)$是分配格。

[证]. 由条件知$\preccurlyeq$是L上的全序关系，故L中任两元素均是可比较的。因此$\forall a,b,c\in L$， 3个元素之间的全序关系有3!=6种情况，这6种情况按全序关系可合并为如下的4种情况：

(1) $a\preccurlyeq b$且$a\preccurlyeq c$ (包含$a\preccurlyeq b\preccurlyeq c$, $a\preccurlyeq c\preccurlyeq b$)

(2) $b\preccurlyeq a$且$c\preccurlyeq a$ (包含$b\preccurlyeq c\preccurlyeq a$, $c\preccurlyeq b\preccurlyeq a$)

(3) $b\preccurlyeq a\preccurlyeq c$

(4) $c\preccurlyeq a\preccurlyeq b$

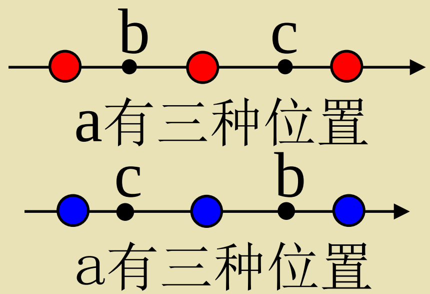

图3

在每种情况下 都易证分配律是成立的。例如：

(1) 当$a \preccurlyeq b$且$a \preccurlyeq c$时有

$a * (b \oplus c) = a$ （由定理4，因为$a \preccurlyeq b \preccurlyeq b \oplus c$）

$= a \oplus a$ （幂等律）

$= (a * b) \oplus (a * c)$ （由定理4，因为$a \preccurlyeq b, a \preccurlyeq c$）；

$a \oplus (b * c) = b * c$ （从$a \preccurlyeq b, a \preccurlyeq c$可知a是 b和c的一个下界，于是由b和c的下确界 $b * c$的最大性可得$a \preccurlyeq b * c$ ）

$= (a \oplus b) * (a \oplus c)$ （因为$a \preccurlyeq b, a \preccurlyeq c$）；

(3) 当$b \preccurlyeq a \preccurlyeq c$时有

$a * (b \oplus c) = a$ （由定理4，因为$a \preccurlyeq c \preccurlyeq b \oplus c$）

$= b \oplus a$ （由定理4，因为$b \preccurlyeq a$）

$= (a * b) \oplus (a * c)$ （由定理4，因为$b \preccurlyeq a, a \preccurlyeq c$）；

$a \oplus (b * c) = a$ （由定理4，因为$b * c \preccurlyeq b \preccurlyeq a$）

$= a * c$ （由定理4，因为$a \preccurlyeq c$）

$= (a \oplus b) * (a \oplus c)$ （因为$b \preccurlyeq a, a \preccurlyeq c$）；

所以由分配格的定义4知是分配格。

例14. (X,≤, min, max)是分配格。

这里：X＝[0,1]为实数闭区间，

≤为实数间的小于或等于关系。

由于 $\forall a,b\in X$，有

$$\left.\begin{array}{l} GLB\{a,b\} = \min\{a,b\}\in X \\ LUB\{a,b\} = \max\{a,b\}\in X \end{array}\right\}(\text{存在})$$

故定义1′可知(X, ≤)是格。

因此，格上的两个运算为：$\forall a,b\in X$，

$a*b = \min\{a,b\}$，$a \oplus b = \max\{a,b\}$ 。

由于任意两个实数均能比较大小，故此格中的半序关系≤为全序关系。由定理11知格(X, ≤, ∗, ⊕)是分配格， 记其为(X, ≤, min, max)。

定义5. 有界格(bounded lattice)

存在着最小元和最大元的格称为有界格。即

设 (L , ≼, ∗, ⊕)是格，若

$$(\exists x_0 \in L)(\forall a \in L)(x_0 \preccurlyeq a) \wedge (\exists y_0 \in L)(\forall a \in L)(a \preccurlyeq y_0)$$

，则称格(L , ≼, ∗, ⊕)是有界格。

注：•格中的最小元x_0 **通常记为0；格中的最大元**y_0 **通常记为1；**

• $(\forall a \in L)(\mathbf{0} \preccurlyeq a \preccurlyeq \mathbf{1})$；

•有界格通常记为(L,≼,∗,⊕,**0**,**1**)**。**

例15. (2^X ,⊆,∩ ,∪,∅,X)是有界格。 根据例1已知(2^X ,⊆,∩ ,∪)是格；又由于∀A∈2^X ,

有∅⊆A，故∅∈2^X存在是此格的最小元；

有A⊆X，故X∈2^X存在是此格的最大元；

因此，根据定义5可知，(2^X ,⊆,∩ ,∪,∅,X)是有界格。

例16. ([0,1],≤, min, max,0,1)是有界格。

例14已证([0,1],≤, min, max)是格，而且这是一个无限格。由于在此格中有最小元0，有最大元1，故此由有界格的 定义5知([0,1],≤, min, max,0,1)是有界格。

注：•这说明有限格一定是有界格；但无限格不一定是有界格。无限格也可能是有界格；因此无限格不是有界格的必然否决条件。

例17. (N, | , GCD, LCM)不是有界格。

由例5和例6已知(N, | , GCD, LCM)是格，而且这是一个无限格。 这不是有界格，因为在此格中无最大元。

定义6. 有补格(complemented lattice)

每个元素都有补元存在的有界格称为有补格。即设 (L , ≼, ∗, ⊕ ,**0**,**1**)是有界格，若

$$(\forall a \in L)(\exists b \in L)((a * b = \mathbf{0}) \wedge (a \oplus b = \mathbf{1})),$$

则称有界格(L , ≼, ∗, ⊕ ,**0**,**1**)是有补格。

注：•对于元素$a \in L$，若存在着元素$b \in L$，使得

$a * b = \mathbf{0}$ 且$a \oplus b = \mathbf{1}$

则称b是a的补元(complement element)。 a的补元通常记为a′,于是有a′=b或b=a′，并且$a * a' = \mathbf{0}$ 且$a \oplus a' = \mathbf{1}$ (互补律)；

•若b是a的补元，则显然a也是b的补元，从而a与b互为补元，即补元是相互的；

•群无补元，只有逆元。因为它只有一个运算。

例18. (S_{24}, | , GCD, LCM,1,24)不是有补格。

这里：S_{24}是由24的所有乘法因子所组成的集合。

由右图可知 (S_{24}, | , GCD, LCM, 1, 24) 是格(|是半序，任意两个元素的上下确界存在，就是LCM和GCD)。而且它是一个有界格，其最大元为24，最小元为1。

此格中各元的补元如下表：

元素	1	2	3	4	6	8	12	24
补元	24	无	8	无	无	3	无	1

表1

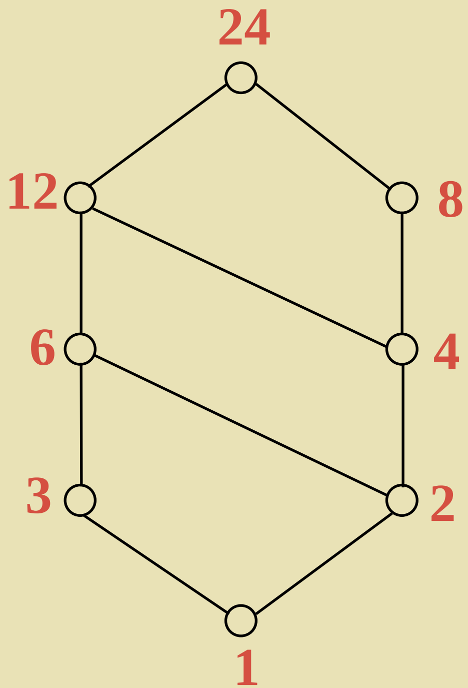

图4

例19.例8图1所示的格(L,≼)是有补格 。

由例8已知右图是格。并且此格显然是有界格，其最小元是a_0，最大元是a_1。

此格中各元的补元如下表：

元素	a_0	a_1	a_2	a_3	a_4
补元	a_1	a_0	a_3 a_4	a_2 a_4	a_2 a_3

表2

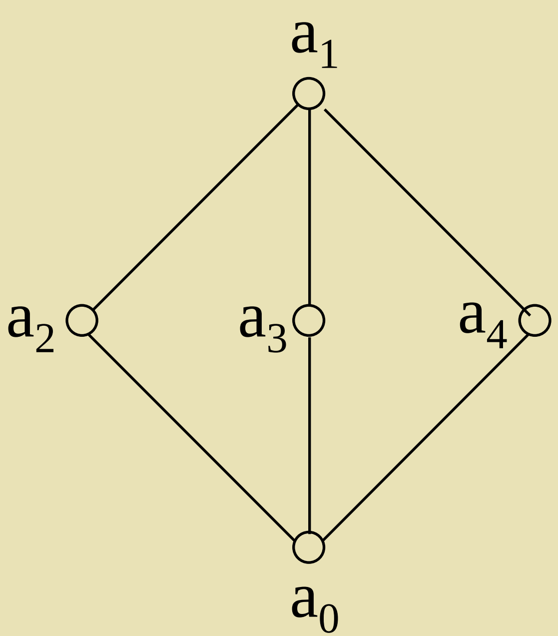

图1

例20. $(2^X, \subseteq, \cap, \cup, \varnothing, X)$是有补格。

由例15已知$(2^X, \subseteq, \cap, \cup, \varnothing, X)$是有界格。 最小元为$\varnothing$， 最大元为X 。 由例10已知此格是分配格。

根据第一章§2定理2(2)知：$\forall A \in 2^X$，$\exists A' \in 2^X$，使

$$A \cap A' = \varnothing \quad 且 \quad A \cup A' = X$$

故在此格中每个元素均有唯一的补元，由有补格的定义6知此格是有补格。

注： •有界格中，每个元素的补元不一定是唯一的;

•由例18知：当补元唯一时，有界格似乎同时是分配格;

由例19知：当补元不唯一时，有界格似乎同时不是分配格。

定理12.有界的分配格中补元是唯一的。即

设(L , $\preccurlyeq$, $*$, $\oplus$,**0**,**1**)是有界的分配格。对任意元素$a\in L$，若a有补元，则a的补元是唯一的。

[证]. $\forall a\in L$，$\exists b,c\in L$

b是a的补元 $\wedge$ c是a的补元

$\Rightarrow(a*b=\mathbf{0}=a*c)\wedge(a\oplus b=\mathbf{1}=a\oplus c)$

$\Rightarrow b=c$ (根据定理10：分配格有消去律)

注：• 有界格在有分配律时，补元有唯一性；但并不能保证补元的存在性；只有在有补的分配格中，补元才是唯一存在的；

•在有补的分配格中，每个元素的补元是唯一存在的。因此可以将对每个元素的求补定义为格L上的一个一元运算，通常将这个运算记为 $'$: $L\to L$,

$\forall x\in L$, $(x)'=x'$

•因此，今后 将有补的分配格记为：(L , $\preccurlyeq$, $*$, $\oplus$, $'$, **0**,**1**)

例如 $(2^X, \subseteq, \cap, \cup, ', \varnothing, X)$是有补的分配格，即集合代数。

离散数学

- 第七章　格

  到此已经结束！