第16章

环 与 域

应用广泛的群和半群，都是只含有一个二元运算的代数系统。但是，在实际问题中，许多代数系统都包含多个运算。如数集、矩阵集、多项式集都有加法和乘法运算，集合有并、交、补等运算，命题有非、合取、析取等运算。如果按照运算的性质进行组合与分类，这些代数系统有着各种类别。

这一章考虑的是具有两个运算的典型代数系统：环和域。这两种代数系统不仅在理论上较重要，而且在应用上也是值得研究的，比如，环在计算机科学的很多领域，诸如编码理论的研究中起着重要作用。

16.1 环的定义及其性质

定义 16.1 设 $\langle R,+,*\rangle$ 是含有两个二元运算的代数系统。如果满足

①$\langle R,+\rangle$ 是交换群；

②$\langle R,*\rangle$ 是半群；

③$\forall a,b,c\in R$，$a*(b+c)=(a*b)+(a*c)$，$(b+c)*a=(b*a)+(b*c)$；

则称 $\langle R,+,*\rangle$ 是**环**。

【例 16.1】 在数的加法“+”和乘法“*”运算下，整数集 **Z** 构成整数环 $\langle \mathbf{Z},+,*\rangle$。已经知道 $\langle \mathbf{Z},+\rangle$ 满足条件①，$\langle \mathbf{Z},*\rangle$ 满足条件②，并且数的乘法关于加法满足左分配律和右分配律。

同样，有理数集 **Q** 关于加法和乘法运算构成有理数环 $\langle \mathbf{Q},+,*\rangle$，实数集 **R** 则构成实数环 $\langle \mathbf{R},+,*\rangle$。■

【例 16.2】 设 $P(X)=\{P_n(x)\mid n\in \mathbf{N}\}$ 是定义在实数集上的多项式集合

$$P_n(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$$

和

$$P_n(x)=b_0x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m$$

是其中两个多项式。定义多项式加法“+”和乘法“·”运算如下：

设 $n\geqslant m$，则 $Pn(x)+Pm(x)=g_n(x)=c_0x^n+c_1x^{n-1}+\cdots+c_{n-1}x+c_n$，其中

$$C_i=\begin{cases}a_i & \text{当 } m<i\leqslant n\\ a_i+b_i & \text{当 } 0\leqslant i\leqslant m\end{cases}$$

$P_n(x)\cdot P_m(x)=Q_{m+n}(x)=d_0x^{m+n}+d_1x^{m+n-1}+\cdots+d_{n+n}$，其中

$$d_i=\sum_{\substack{0\leqslant t+s\leqslant i\\ 0\leqslant t\leqslant n,0\leqslant m\leqslant s}} a_t b_s$$

由于多项式的加法和乘法运算实质上仍由数的加法和乘法运算实现，易知 $\langle P(x),+\rangle$ 满足封闭、可结合、幺元为 $P_n(x)=0$，$P_n(x)$ 的逆元为 $-P_n(x)$，因而是加群。而 $\langle P(x),\cdot\rangle$ 满足封闭性、可结合，并且有幺元 $P_n(x)=1$，因而是含幺乘群。至于乘法关于加法的分配律，可由数的运算性质得到。因此，$\langle P(x),+,\cdot\rangle$ 是环，称为**多项式环**。■

【例 16.3】 已证明 $\langle \mathbf{Z}_m,\oplus\rangle$ 是模 m 剩余类加群，$\langle \mathbf{Z}_m,\otimes\rangle$ 是剩余类乘半群。至于$\otimes$关于$\oplus$的分配性，任取 $[i],[j],[k]\in\mathbf{Z}_m$，那么

$$[i]\otimes([j]\oplus[k])=[ij+ik]=[ij]\oplus[ik]=([i]\otimes[j])\oplus([i]\otimes[k])$$

即$\otimes$关于$\oplus$的左分配律成立。同样，可以证明右分配律成立。综上所述，$\langle \mathbf{Z}_m,\oplus,\otimes\rangle$ 是环，称为**（模 m）剩余类环**。特别地，当 $m=2$ 时，称为**布尔环**。■

在环 $\langle R,+,*\rangle$ 中，为方便起见，约定加法幺元记为 θ，元 b 的加法逆元记为 $-b$，并且 $a+(-b)=a-b$。注意，这里并未定义新运算“$-$”，$a-b$ 只是 $a+(-b)$ 的一种缩写形式，在下面定理中它确实与数的减法有相同之处。

定理 16.1（移项法则） 设 $\langle R,+,*\rangle$ 是环，$a,b,c\in R$，则下面两条等价：

①$a+b=c$　　②$a+b-c=\theta$

【证明】 ①⇒②　在①式两端同时加上 $-c$，可得 $(a+b)+(-c)=c-c=\theta$，即 $a+b-c=\theta$。

②⇒①　在②式两端同时加 c 即得①式。

定理 16.2 设 $\langle R,+,*\rangle$ 是环，$a,b,c\in R$，则

①$a*\theta=\theta*a=\theta$（加法幺元是乘法零元）

②$a*(-b)=-(a*b)=(-a)*b$

③$(-a)*(-b)=a*b$

④$a*(b-c)=(a*b)-(b*c)$

⑤$(b-c)*a=(b*a)-(c*a)$

【证明】 ①因为 $a*\theta=a*(\theta+\theta)=(a*\theta)+(a*\theta)$，由移项法则 $a*\theta=\theta$。同样，可得 $\theta*a=\theta$。

②因为 $(a*(-b))+(a*b)=a*(-b+b)=a*\theta=\theta$，所以 $a*(-b)=-(a*b)$。同理，$(a*b)+((-a)*b)=(a-a)*b=\theta$，所以 $(-a)*b=-(a*b)$。

③利用②式的结果，$((-a)*(-b)-(a*b)=((-a)*(-b)+((-a)*b)=(-a)*(-b+b)=(-a)*\theta=\theta$，但是，$-(a*b)$ 又是 $a*b$ 的逆，根据群 $\langle R,+\rangle$ 中逆的唯一性，$a*b=(-a)*(-b)$。

④$a*(b-c)=a*(b+(-c))=(a*b)+(a*(-c))=(a*b)-(a*c)$。

⑤式可同样证明。■

这个定理表明，普通环的运算性质在很多方面类似于数的运算性质，但是在某些方面它们却有不同。例如在模 m 剩余类环 $\langle \mathbf{Z}_m,\oplus,\otimes\rangle$ 中，我们特别注意到一种情况：当 $[i]\neq[0]$，$[j]\neq[0]$ 时，却可能 $[i]\otimes[j]=[0]$。例如在 $\langle \mathbf{Z}_6,\oplus,\otimes\rangle$ 中，$[2]\otimes[3]=[0]$，$[4]\otimes[3]=[0]$。

定义 16.2 设 $\langle R,+,*\rangle$ 是环，$a,b\in R$。如果 $a\neq\theta$ 且 $b\neq\theta$，而 $a*b=\theta$，则称 a 和 b 是 R 中的**零因子**。

【例 16.4】 模 m 剩余类环 $\langle \mathbf{Z}_m,\oplus,\otimes\rangle$ 没有零因子，当且仅当 m 是素数。因为当 m 是合数时，必有 $a\geqslant 2$，$b\geqslant 2$ 使 $m=ab$，从而 $[a]\otimes[b]=[m]=[0]$，而且 $[a]$ 和 $[b]$ 都是零因子。当 m 是素数时，不存在 $a\geqslant 2$ 和 $b\geqslant 2$ 使 $m=ab$，因而无零因子。■

【例 16.5】 n 阶矩阵集 M_n 关于矩阵加法“+”和矩阵乘法“·”分别构成群和半群，并且由线性代数只是知道，矩阵乘法关于加法是可分配的，因而 $\langle \mathbf{Z}_n, +, \cdot \rangle$ 是环，称为 n 阶矩阵环。在 n 阶矩阵环中存在着零因子。例如当 $n=2$ 时，

$$\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

■

16.2 整环与域

定义 16.3 设 $\langle R, +, * \rangle$ 是环

①如果 $*$ 可交换，则称 R 为**交换环**。

②如果 $\langle R, * \rangle$ 有幺元，则称 R 为**含幺环**。

③如果①和②成立且无零因子，则称 R 为**整环**。

显然，整数环 $\langle \mathbf{Z}, +, * \rangle$ 是整环。当 m 是质数时，剩余类环 $\langle \mathbf{Z}_m, \oplus, \otimes \rangle$ 是整环。如果 M_n 是由 n 阶满秩阵构成的集合，那么 n 阶满秩阵环 $\langle M_n, \oplus, \otimes \rangle$ 也是整环。在环中无零因子与消去律是等价的。

定理 16.3 设 $\langle R, +, * \rangle$ 是环，则 R 中无零因子，当且仅当对任何 $a, x, y \in R$，当 $a \neq 0$ 时，由 $a * x = a * y$，必然得到 $x = y$（或由 $x * a = y * a$ 得到 $x = y$）。

【证明】 如果 R 中无零因子，则当 $a * x = a * y$ 时，$(a * x) - (a * y) = \theta$，即 $a * (x - y) = \theta$。由于 $a \neq \theta$，因而 $x - y = \theta$，即 $x = y$。同理，由 $x * a = y * a$ 可以得出 $x = y$。

反过来，设由 $a * x = a * y$ 必然得出 $x = y$ 的结论，如果 R 中存在 b 和 c 使 $b * c = \theta$，那么由 $b * c = \theta = b * \theta$ 就导出 $c = \theta$。这说明 R 中必无零因子。 ■

在环中也有子环的概念。

定义 16.4 设 $\langle R, +, * \rangle$ 是环，S 是 R 的非空子集，如果 $\langle S, +, * \rangle$ 也是环，则称 S 是 R 的**子环**。

例如，整数环 $\langle \mathbf{Z}, +, * \rangle$ 是实数环 $\langle \mathbf{R}, +, * \rangle$ 的子环，$\langle \{[0], [2], [4]\}, \oplus, \otimes \rangle$ 是模 6 剩余类环 $\langle \mathbf{Z}_6, \oplus, \otimes \rangle$ 的子环。

两个环之间也有着同态和同构的概念。

定义 16.5 设 $\langle S, +, * \rangle$ 和 $\langle T, \oplus, \otimes \rangle$ 是两个环，$f: S \to T$ 是映射。如果对任意 $a, b \in S$，都有

$$f(a + b) = f(a) \oplus f(b)$$
$$f(a * b) = f(a) \otimes f(b)$$

则称 f 是环 $\langle S, +, * \rangle$ 到环 $\langle T, \oplus, \otimes \rangle$ 的环同态映射，$f(S)$ 为 S 的**同态像**。当 f 是满射时，称 f 为**满同态**；当 f 是双射时，称 f 是**环同构映射**。

【例 16.6】 存在整数环 $\langle \mathbf{Z}, +, * \rangle$ 到模 m 剩余类环 $\langle \mathbf{Z}_m, \oplus, \otimes \rangle$ 的同态，因为可以定义映射 $f: \mathbf{Z} \to \mathbf{Z}_m$ 如下：使对所有 $x \in \mathbf{Z}$。

$$f(x) = x \bmod m$$

在此映射下，设 $a, b \in \mathbf{Z}$，由同余的性质，有

$$[a + b] = [a] \oplus [b]$$
$$[ab] = [a] \otimes [b]$$

所以 $\langle \mathbf{Z}, +, * \rangle \sim \langle \mathbf{Z}_6, \oplus, \otimes \rangle$。 ■

类似于群的同态的讨论，容易证明下面的定理：

定理 16.4 设 f 是环 $\langle S,+,*\rangle$ 到环 $\langle T,\oplus,\otimes\rangle$ 的环同态映射，则

①如果 θ 和 e 分别是 S 中的加法幺元和乘法幺元，则 $f(\theta)$ 和 $f(e)$ 分别是 $f(S)$ 中的$\oplus$幺元和$\otimes$幺元。

②对 $a\in S$，如果 $-a$（或 a^{-1}）是 a 的加法（或乘法）逆元，则 $f(-a)$（或 $f(a^{-1})$）是 $f(S)$ 中的$\oplus$（或$\otimes$）逆元。

③$\langle S,\oplus,\otimes\rangle$ 也是环。

【证明】 留作练习。 ■

定义 16.6 设 $\langle R,+,*\rangle$ 是环，如果 $\langle R,+\rangle$ 和 $\langle R-\{\theta\},*\rangle$ 都是交换群，则称 $\langle R,+,*\rangle$ 是**域**。

$\langle R,+,*\rangle$、有理数环 $\langle \mathbf{Q},+,*\rangle$、剩余类环 $\langle \mathbf{Z}_p,\oplus,\otimes\rangle$（其中 p 是素数）都是域的例子。但是，整数环 $\langle \mathbf{Z},+,*\rangle$、$m$ 为合数时的模 m 剩余类环 $\langle \mathbf{Z}_6,\oplus,\otimes\rangle$ 都不是域，因为这时 $\langle \mathbf{Z}-\{0\},*\rangle$ 和 $\langle \mathbf{Z}_m-\{[0]\},\otimes\rangle$ 都不是群。

为方便起见，一般把域中的加法幺元记为 θ，把乘法幺元记为 e。从域的定义看，它是在整环的基础增加了除 θ 之外每元都有乘法逆元的条件。因此，一般来说，整环不是域，然而，当环的元素个数有限时，情况就不同了。

定理 16.5 有限整环 $\langle R,+,*\rangle$ 必是域。

【证明】 根据整环的定义，只需证明 R 中每个非零元都有逆元。为此，设 $R=\{a_1,a_2,\cdots,a_n\}$。任取 $r\in R$ 且 $r\neq\theta$，构造集合 $rR=\{r*a_1,r*a_2,\cdots,r*a_n\}$。由于 R 中无零因子，因此 rR 中的元素互不相同，并且由于乘法运算的封闭性可知 $R=rR$，于是 $e\in rR$；这说明必有 $ra_i=e$，即 $r^{-1}=a_i$。由此可知，$\langle R,+,*\rangle$ 是域。 ■

习题十六

1. 设 S 是由有限个实数组成的非空集合。证明：$\langle S,+,\times\rangle$ 不是环，其中“+”和“×”是实数的加法和乘法运算。
2. 在 $\langle \mathbf{Z}_{15},\oplus,\otimes\rangle$ 中求出满足方程 $x^2-[1]=[0]$ 的全部根。
3. 设 A 依次为下列数集合，试确定 $\langle A,+,\times\rangle$ 是否成环、整环或域。
   (1) $A=\{x\mid x\in\mathbf{Z}\text{ 且 }x\geqslant 0\}$
   (2) $A=\{a+b\sqrt{3}\mid a,b\in\mathbf{Q}\}$
   (3) $A=\{x\mid(\exists y)[y\in\mathbf{Z}\wedge x=2y]\}$
   (4) $A=\{a/b\mid a,b\text{ 为正整数，且 }(a,b)=1\}$
4. 设 a,b 是交换环 $\langle R,+,*\rangle$ 中任意两个元素。证明：对任何正整数 n 以下成立。
   (1) $(a*b)^n=a^n*b^n$
   (2) $(a+b)^n=\sum_{i=1}^{n}C_n^i a^i*b^{n-1}$
5. 证明定理 16.4。
6. 设 $\langle S,+,*\rangle$ 是环 $\langle R,+,*\rangle$ 的一个子环。证明：S 中的零元（加法幺元）必是 R 的零元；如果 S 有乘法幺元 e，则 e 也是 R 的乘法幺元。
7. 设 $\langle R,+,*\rangle$ 为环，且 R 中每个元都是乘法幂等元。证明：
   (1) 对任何 $a\in R$，$a+a=\theta$。
   (2) $\langle R,+,*\rangle$ 为交换环。

第17章

格与布尔代数

布尔代数是人们利用数学方法研究人类思想规律的一项重要成果。由于他的两种运算与并联电路和串联电路的密切关系，布尔代数在逻辑电路设计和开关网络研究中有着广泛的应用，是计算机科学必需的基础知识。从系统的角度看，布尔代数是一类特殊的格代数。本章将从格的代数定义和偏序定义出发，研究格系统的各种性质，建立布尔代数的基本理论。

17.1 格的定义与性质

设 A 是集合，则代数系统 $\langle 2^A, \cup, \cap \rangle$ 中集合运算 $\cap$ 和 $\cup$ 都满足幂等律、可换律、可结合律、吸收律和分配律等。

如果设 $\wp$ 为命题的集合，则代数系统 $\langle \wp, \vee, \wedge \rangle$ 中逻辑运算 $\vee$ 和 $\wedge$ 也适合幂等律、交换律、结合律、吸收律和分配律等。

这两类不同的代数系统从运算性质上看，具有相当的一致性。现在以这样的代数系统为对象，从运算性质着眼进行抽象，提取它们的共性，得到“格”的概念。为书写简便起见，本章用 $\vee$ 和 $\wedge$ 表示格的两个运算，它们不表示狭义的逻辑运算符。

定义 17.1 设 $\langle L, \vee, \wedge \rangle$ 是一个代数系统。如果 $\vee$ 和 $\wedge$ 满足

①交换律：$a \vee b = b \vee a$，$a \wedge b = b \wedge a$

②结合律：$a \vee (b \vee c) = (a \vee b) \vee c$，$a \wedge (b \wedge c) = (a \wedge b) \wedge c$

③吸收律：$a \vee (b \wedge a) = a$，$a \wedge (a \vee b) = a$

则称 $\langle L, \vee, \wedge \rangle$ 为一个**代数格**。

由代数格的定义可知，集合代数系统 $\langle 2^A, \cup, \cap \rangle$ 和命题逻辑系统 $\langle \wp, \vee, \wedge \rangle$ 都是典型的格例子。在代数格的定义中，只列出了运算满足的三个条件，实际上由这些条件还可导出运算的幂等性。

定理 17.1 幂等律 设 $\langle L, \vee, \wedge \rangle$ 是一个代数格，$a \in L$，则必有

$$a \vee a = a, \quad a \wedge a = a$$

【证明】 $a \vee a = a \vee (a \wedge (a \vee a)) = a$ （吸收律）

在上两式中，把 $\vee$ 换成 $\wedge$，把 $\wedge$ 换成 $\vee$ 后，可以证明 $a \wedge a = a$。 ■

对于逻辑代数系统，我们曾从蕴涵与等价的角度定义过命题之间的关系。同样，在集合

代数系统中引入过包含和相等关系，从而在元素之间建立了序关系。下面从偏序的角度来定义格系统。

定义 17.2 设$\leqslant$是集合L上的一个偏序。如果对所有$a, b\in L$，子集$\{a, b\}$在L中都有一个最大下界和一个最小上界，则称$\langle L,\leqslant\rangle$为一个**偏序格**。$a$和$b$的最大下界记为$\text{glb}(a, b)$，最小上界记为$\text{lub}(a, b)$。

从定义可知，有限偏序集$\langle L,\leqslant\rangle$不一定能成为格；要成为格，它必须有一个最大元和一个最小元，这容易从它对应的Hasse图中看出来。

【例 17.1】 图17-1中列出了6个有限偏序集对应的Hasse图，图17-1a～d对应的偏序集满足偏序格的条件；而图17-1e～f对应的偏序集中没有最大元和最小元，因此不能构成偏序格。■

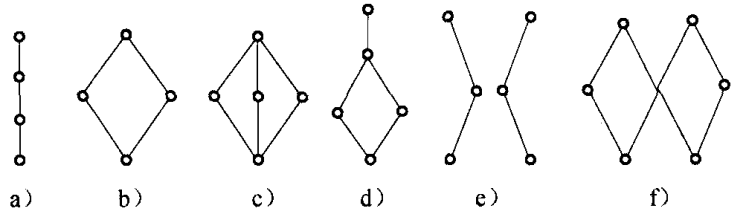


图 17-1

【例 17.2】 在偏序集$\langle 2^A,\subseteq\rangle$中，任何两个元素$X, Y\in 2^A$，都有$\text{lub}(X, Y)=X\cup Y$，$\text{glb}(X, Y)=X\cap Y$，因此满足偏序格的条件。以后，将简称$\langle 2^A,\subseteq\rangle$为幂集格。■

同时，我们注意到$\langle 2^A,\cup,\cap\rangle$还是一个代数格。尽管在$2^A$上定义了两个表面上不同的系统，但它们在本质上确实一样的。下面，要把代数格和偏序格联系起来，证明两种格的定义在本质上是一样的。

定理 17.2 设$\langle L,\vee,\wedge\rangle$是一个代数格。定义格上的自然偏序“$\leqslant$”如下：$a\leqslant b$，当且仅当$a\wedge b=a$，则$\langle L,\leqslant\rangle$是一个偏序格。

【证明】 首先证明$\langle L,\leqslant\rangle$是偏序集。

由于$a\wedge a=a$（幂等律），因此$a\leqslant a$，即“$\leqslant$”具有自反性。

设$a\leqslant b$且$b\leqslant a$，则由“$\leqslant$”的定义

$$\begin{aligned} a &= a\wedge b && (a\leqslant b)\\ &= b\wedge a && (\text{交换律})\\ &= b && (b\leqslant a)\end{aligned}$$

即反对称性成立。

再设$a\leqslant b$，$b\leqslant c$，那么

$$\begin{aligned} a\wedge c &= (a\wedge b)\wedge c && (\text{由 } a\leqslant b)\\ &= a\wedge(b\wedge c) && (\text{结合律})\\ &= a\wedge b && (\text{由 } b\leqslant c)\\ &= a && (\text{由 } a\leqslant b)\end{aligned}$$

即有$a\leqslant c$，传递性成立。

其次，证明对任意$x, y\in L$，$\{x, y\}$在L中有最大下界和最小上界。由于

$$x\wedge(x\wedge y)=x\wedge y \qquad (\text{结合律，幂等律})$$

所以，$x\wedge y\leqslant x$。同理可得$x\wedge y\leqslant y$。这说明$x\wedge y$是$\{x, y\}$的一个下界。现在设c是x和y的任一下界，即$c\leqslant x$且$c\leqslant y$，那么

$$\begin{aligned} c \wedge (x \wedge y) &= (c \wedge x) \wedge y \qquad \text{（结合律）} \\ &= c \wedge y \\ &= c \end{aligned}$$

这说明 $c \leqslant x \wedge y$，从而知道，$\text{glb}(x, y) = x \wedge y$。

类似地，可以证明 $\text{lub}(x, y) = x \vee y$，只需在上述证明中把 $\wedge$ 换成 $\vee$，把 $\vee$ 换成 $\wedge$ 即可。（证明中利用了 $a \leqslant b$ 的另一等价定义，即 $a \leqslant b$ 当且仅当 $a \vee b = b$，其证明留作练习。）■

为便于叙述，将把 $x \leqslant y$，读做“x 小于等于 y”，把 $x < y$ 读做“x 小于 y”。

定理 17.3　设 $\langle L, \leqslant \rangle$ 是一个偏序格。在格上定义运算“$\vee$”和“$\wedge$”如下：$a \wedge b = \text{glb}(a, b)$，$a \vee b = \text{lub}(a, b)$，则 $\langle L, \vee, \wedge \rangle$ 是一个代数格。

【证明】 从运算和的定义可以看出，它们满足交换律、结合律和幂等律。现证明吸收律成立。事实上，由 $\text{glb}(a, b) \leqslant a \leqslant \text{lub}(a, b)$，可以看出

$$a \wedge (a \wedge b) = \text{glb}(a, \text{lub}(a, b)) = a$$

$$a \vee (a \vee b) = \text{lub}(a, \text{glb}(a, b)) = a$$

由此可知，$\langle L, \vee, \wedge \rangle$ 是代数格。■

上面两个定理说明，格的两种定义是完全等价的。以后将不特别加以区分，而是根据需要采用相应的定义来说明问题。

17.2　子格与格同态

利用代数系统的方法讨论格，能够自然地引入子格和格同态。与其他代数系统一样，格也有着它的子系统。

定义 17.3　设 $\langle L, \vee, \wedge \rangle$ 是格，S 是 L 的非空子集。如果对任何 $a, b \in S$，$a \wedge b$ 与 $a \vee b$ 都在 S 中，则称 S 是 L 的**子格**，记为 $\langle S, \vee, \wedge \rangle$。

【例 17.3】 设图 17-2 是格 $\langle L, \vee, \wedge \rangle$ 对应的 Hasse 图，$S_1 = \{a, b, c, f\}$，$S_2 = \{a, c, d, f\}$，那么 $\langle S_1, \vee, \wedge \rangle$ 不是 $\langle L, \vee, \wedge \rangle$ 的子格。因为尽管 $\langle S_1, \vee, \wedge \rangle$ 自身可以成格，但是 $b \wedge c = e$，不在 S_1 中。

通过考察可以知道，$\langle S_2, \vee, \wedge \rangle$ 是 $\langle L, \vee, \wedge \rangle$ 的子格，因为它满足子格的条件。■

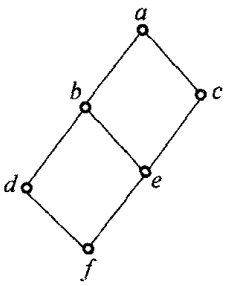


图　17-2

在上一节中看到，格上的一些关系式常常是成对出现的，这种情况在集合论和数理逻辑中是普遍的现象，其中起根本作用的是所谓格的对偶原理。

定义 17.4　设 $\langle L, \leqslant \rangle$ 和 $\langle L, \leqslant' \rangle$ 是两个偏序格，如果偏序关系 $\leqslant'$ 是 $\leqslant$ 的逆关系，则称这两个偏序格是**互为对偶的格**。

【例 17.4】 设 L 是由 18 的正因子组成的集合，则 L 关于整除关系构成 $\langle L, | \rangle$。整除关系的逆关系是倍数关系。设倍数关系用“$\|\|$”表示，那么 $\langle L, \|\| \rangle$ 是格，并和 $\langle L, | \rangle$ 互为对偶。■

在两个互为对偶的格中，任何两个元素在一个格中的最大下界必是对偶格中的最小上界，反过来也一样。推而广之，在一个格中的最大（小）元必是对偶格中的最小（大）元，换句话说，两个对偶格的 Hasse 图是相互颠倒的。

从代数格的角度看，互为对偶的两个格，它们的运算也刚好是互换的。例如，对于例 17.4 中的格 $\langle L, | \rangle$，它对应的代数格中的运算时分别求最大公约数和最小公倍数；而格 $\langle L, \|\| \rangle$ 对应的代数格中的运算恰分别是求最小公倍数和最大公约数，这就是说，求一个

格的对偶格，可通过交换该格两个运算而得到。

为叙述完整起见，设一个格中的最大元用1表示，最小元用0表示。现在定义对偶公式如下：

定义 17.5 设〈L，$\vee$，$\wedge$〉是一个格，E是格中的一个公式。将E中的0和1互换，$\vee$和$\wedge$互换后得到的新公式E^*称为E的**对偶公式**。

显然，在一个格中公式E的对偶公式E^*也是对偶格中的一个公式，因此，只需考虑在一个格中互为对偶的公式就行了。

对偶原理 设X和Y是格〈L，$\vee$，$\wedge$〉上的两个公式，X^*和Y^*是相对应的对偶公式。如果$X=Y$，那么$X^*=Y^*$。

由对偶公式的定义知道，对偶原理是正确的。在应用对偶原理时，下面的序关系式更常用。

定理 17.4 设X和Y是格〈L，$\vee$，$\wedge$〉上的两个公式，$\preccurlyeq$是对应的偏序。如果$X\preccurlyeq Y$，则必$Y^*\preccurlyeq X^*$。

【证明】 根据偏序的定义和对偶原理，

$$\begin{aligned} X\preccurlyeq Y &\Leftrightarrow X\wedge Y=X && \text{（偏序定义）}\\ &\Leftrightarrow X^*\vee Y^*=X^* && \text{（对偶原理）}\\ &\Leftrightarrow Y^*\preccurlyeq X^* && \text{（偏序定义）} \end{aligned}$$

■

作为对偶原理的应用，下面将证明在格中普遍成立的一些结论。

定理 17.5 设〈L，$\vee$，$\wedge$〉为格，$\preccurlyeq$是对应的偏序，a，b，c，$d\in L$，则

①$a\preccurlyeq b\Rightarrow a\vee c\preccurlyeq b\vee c$　　②$a\preccurlyeq b\Rightarrow a\wedge c\preccurlyeq b\wedge c$

③$a\preccurlyeq b$，$c\preccurlyeq d\Rightarrow a\wedge c\preccurlyeq b\wedge d$　　④$a\preccurlyeq b$，$c\preccurlyeq d\Rightarrow a\vee c\preccurlyeq b\vee d$

⑤$a\preccurlyeq b$，$a\preccurlyeq c\Rightarrow a\preccurlyeq b\wedge c$　　⑥$a\preccurlyeq c$，$b\preccurlyeq c\Rightarrow a\vee b\preccurlyeq c$

【证明】

①$a\preccurlyeq b\Rightarrow a\vee b=b\Rightarrow(a\vee c)\vee(b\vee c)=b\vee c\Rightarrow a\vee c\preccurlyeq b\vee c$

②$a\preccurlyeq b\Rightarrow a\wedge b=a\Rightarrow(a\wedge c)\wedge(b\wedge c)=a\wedge c\Rightarrow a\wedge c\preccurlyeq b\wedge c$

③$a\preccurlyeq b$，$c\preccurlyeq d\Rightarrow a\wedge c\preccurlyeq b\wedge c$，$b\wedge c\preccurlyeq b\wedge d$　（由②）

$\Rightarrow a\wedge c\preccurlyeq b\wedge d$

⑤$a\preccurlyeq b$，$a\preccurlyeq c\Rightarrow a\wedge a\preccurlyeq b\wedge c$　（由③）

$\Rightarrow a\preccurlyeq b\wedge c$

④和⑥留作练习。 ■

在一般格中分配律不成立，但格的两个运算之间却存在稍弱形式的准分配关系。

定理 17.6 设〈L，$\vee$，$\wedge$〉为格，$\preccurlyeq$是对应的偏序，a，b，c，$d\in L$，则

① $a\vee(b\wedge c)\preccurlyeq(a\vee c)\wedge(a\vee c)$

② $(a\wedge b)\vee(a\wedge c)\preccurlyeq a\wedge(b\vee c)$

【证明】 根据定理17.5，只要证明①成立即可。

由于$a\preccurlyeq a\vee b$，$a\preccurlyeq a\vee c$，根据定理17.5第⑤式得

$$a\preccurlyeq(a\vee b)\wedge(a\vee c) \tag{17-1}$$

因为$b\preccurlyeq a\vee b$，$c\preccurlyeq a\vee c$，根据定理17.5第③式得

$$b\wedge c\preccurlyeq(a\vee b)\wedge(a\vee c) \tag{17-2}$$

根据定理17.5第⑥式，由（A）和（B）可得

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

■

在代数系统中同态是重要的概念，对于格也是如此。在格中同态不仅与运算有关，还和

对应的偏序有关。

定义 17.6　设 $\langle L, \vee, \wedge\rangle$ 和 $\langle P, \oplus, \otimes\rangle$ 是两个格，f 是 L 到 P 的映射。如果对任何 $a, b\in L$，有

$$f(a \vee b) = f(a) \oplus f(b)$$
$$f(a \wedge b) = f(a) \otimes f(b)$$

则称 f 是从格 $\langle L, \vee, \wedge\rangle$ 到 $\langle P, \oplus, \otimes\rangle$ 的**格同态**；特别地，当 f 是双射时，称为**格同构**。

【例 17.5】　设 D_6 表示 6 的正因子集，那么，因子格 $\langle D_6, |\rangle$ 和幂集格 $\langle 2^{\{a,b\}}, \subseteq\rangle$ 之间可建立同态关系。

定义映射 $f: D_6 \to 2^{\{a,b\}}$，使得 $f(1)=\varnothing$，$f(2)=\{a\}$，$f(3)=\{b\}$，$f(6)=\{a, b\}$，可以验证 f 满足格同态的定义。注意 $\langle D_6, |\rangle$ 对应的运算是 lcm 和 gcd，$\langle 2^{\{a,b\}}, \subseteq\rangle$ 对应的运算为 $\cup$ 和 $\cap$。下面是一些验证数据：

$$f(\mathrm{lcm}(1,3)) = f(3) = \{b\} = \varnothing \cup \{b\} = f(1) \cup f(3)$$
$$f(\gcd(2,6)) = f(2) = \{a\} = \{a\} \cap \{a,b\} = f(2) \cap f(6)$$
$$f(\mathrm{lcm}(2,3)) = f(6) = \{a,b\} = \{a\} \cup \{b\} = f(2) \cup f(3)$$
$$f(\gcd(2,3)) = f(1) = \varnothing = \{a\} \cap \{b\} = f(2) \cap f(3)$$

其余情况可以类似地一一验证。 ■

不仅如此，f 还是双射，$\langle D_6, |\rangle$ 和 $\langle 2^{\{a,b\}} \subseteq\rangle$ 是同构的两个格。事实上，这两个格对应的 Hasse 图是完全一致的。

定理 17.7（**保序定理**）　f 是从格 $\langle L, \vee, \wedge\rangle$ 到格 $\langle P, \oplus, \otimes\rangle$ 的同态，两个格上的偏序分别是 $\leqslant$ 和 $\subseteq$。对 $a, b\in L$，如果 $a\leqslant b$，则必然 $f(a)\subseteq f(b)$。

【证明】　$a\leqslant b$，所以 $a\wedge b=a$。利用格同态定义

$$f(a) = f(a \wedge b) = f(a) \otimes f(b)$$

于是得

$$f(a)\subseteq f(b)$$ ■

这个保序定理的意义是明显的。对于例 17.5 中的 $\langle D_6, |\rangle$ 和 $\langle 2^{\{a,b\}}, \subseteq\rangle$ 来说，设 m，$n\in D_6$，则只要 $m|n$，就能得到 $f(m)\subseteq f(n)$ 的结论。然而，当一个由格 L 到格 P 的映射 f 满足保序性时，并不能保证 f 是格同态。下面举一个简单的例子。

【例 17.6】　设 $L=\{1, 2, 3, 12\}$。在格 $\langle L, |\rangle$ 和格 $\langle 2^L, \subseteq\rangle$ 之间构造映射 $f: L\to 2^L$ 使得对每个 $x\in L$，$f(x)=\{y \mid y\in L \text{ 且 } y|x\}$。易知 $f(1)=1$，$f(2)=\{1, 2\}$，$f(3)=\{1, 3\}$，$f(12)=\{1, 2, 3, 12\}$，并且容易验证当 $x|y$ 时，$f(x)\subseteq f(y)$，所以 f 是保序映射。

但是，f 却不是格同态。因为容易算出 $f(\mathrm{lub}(2, 3))=f(12)=\{1, 2, 3, 12\}$，但是 $f(2)\cup f(3)=\{1, 2, 3\}$，这说明 $f(\mathrm{lub}\ (2, 3))\neq f(2)\cup f(3)$，所以 f 不是从 $\langle L, |\rangle$ 和 $\langle 2^L, \subseteq\rangle$ 的格同态。 ■

由这个例子可以看出，保序与格同态不能等同。然而这对于格同构就不一样了。

定理 17.8　双射 $f: L\to P$ 为格 $\langle L, \vee, \wedge\rangle$ 到格 $\langle P, \oplus, \otimes\rangle$ 的格同构的充分必要条件是：对任意的 $a, b\in L$，$a\leqslant b\Leftrightarrow f(a)\subseteq f(b)$，其中 $\leqslant$ 和 $\subseteq$ 分别是格 L 和 P 对应的偏序。

【证明】　当 f 是 L 到 P 的格同构时，它必须满足保序定理，因此保序为必要条件是成立的。

至于充分条件，只需证明由 $a\leqslant b\Leftrightarrow f(a)\subseteq f(b)$ 能导出 $f(a\vee b)=f(a)\oplus f(b)$ 和 $f(a\wedge b)=f(a)\otimes f(b)$ 就行了。

设 $a\vee b=c$，则 $a\leqslant c$ 且 $b\leqslant c$，从而 $f(a)\subseteq f(c)$，且 $f(b)\subseteq f(c)$。再由定理 17.5 第⑥条知道 $f(a)\oplus f(b)\subseteq f(c)$，这说明 $f(c)$ 是 $f(a)$ 和 $f(b)$ 的一个上界。剩下的任务要证明

$f(c)$是 $f(a)$ 和 $f(b)$ 的最小上界。设 $f(d)$ 是 $f(a)$ 和 $f(b)$ 的任意一个上界，即 $f(a)\subseteq f(d)$且 $f(b)\subseteq f(d)$。由题设条件可以得到 $a\leqslant d$ 且 $b\leqslant d$，从而 $a\vee b\leqslant d$，即 $c\leqslant d$，于是 $f(c)\subseteq f(d)$。

由此，就证明了 $f(c)=f(a\vee b)=f(a)\oplus f(b)$。

同理可证 $f(a\wedge b)=f(a)\otimes f(b)$。因此，双射 f 是格同构。 ■

17.3 分配格与有补格

定义 17.7 设 $\langle L,\ \vee,\ \wedge\rangle$ 是格，如果对任意 $a,\ b,\ c,\ d\in L$ 都使

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

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

则称 $\langle L,\ \vee,\ \wedge\rangle$ 为**分配格**。

根据对偶原理，定义中关于分配格的两个等式，只要其中之一成立，另一个必然成立。因此，在判别一个格的可分配性时，只要其中一个式子成立就行。

【例 17.7】 由集合并运算和交运算的性质知道，幂集格 $\langle 2^S,\ \cup,\ \cap\rangle$ 满足分配格的定义，因而是分配格。 ■

【例 17.8】 由正整数 n 决定的因子格 $\langle D_n,\ |\rangle$ 满足分配格的定义，其证明如下：

因子格上的两个运算时 lcm 和 gcd，要证明分配性，只需证明对任何 $a,\ b,\ c\in D_n$ 有

$$\operatorname{lcm}(a,\gcd(b,c))=\gcd(\operatorname{lcm}(a,b),\operatorname{lcm}(a,c))$$

令 $q=\operatorname{lcm}(a,\gcd(b,c))$，于是 $a|q$，$\gcd(b,c)|q$，从而 $q|\operatorname{lcm}(a,b)$ 且 $q|\operatorname{lcm}(a,c)$，即

$$\operatorname{lcm}(a,\gcd(b,c))\mid\gcd(\operatorname{lcm}(a,b),\operatorname{lcm}(a,c)) \tag{17-3}$$

另一方面，令 $t=\gcd(\operatorname{lcm}(a,b),\operatorname{lcm}(a,c))$，则 $t|\operatorname{lcm}(a,b)$，且 $t|\operatorname{lcm}(a,c)$。同时，$t$ 的因子或是 a 的因子，或是 b 和 c 的公因子，由此可知

$$\gcd(\operatorname{lcm}(a,b),\operatorname{lcm}(a,c))\mid\operatorname{lcm}(a,\gcd(b,c)) \tag{17-4}$$

由式 (17-3) 和式 (17-4) 就导出了结论。 ■

【例 17.9】 如果 $\langle L,\ \leqslant\rangle$ 是一个全序格，则必是分配格，因为此时对任何 $a,\ b\in L$，必有 $a\leqslant b$ 或 $b\leqslant a$ 两种情形之一成立。设格上的运算是 $\vee$ 和 $\wedge$。要证明分配律成立，任取 $a,\ b,\ c\in L$，则可能出现下面两种情况：

1) a 是三者中最大的，于是 $b\leqslant a$ 且 $c\leqslant a$，由定理 17.5⑥式知道 $b\vee c\leqslant a$ 成立，从而$a\wedge(b\vee c)=b\vee c$。

另一方面，$(a\wedge b)\vee(a\wedge c)=b\vee c$，因而

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

2) a 不是三者中最大的，不妨设 $a\leqslant b$，于是

$$\begin{aligned}a\wedge(b\vee c)&=a\\&=a\vee(a\wedge c)\qquad\text{(吸收律)}\\&=(a\wedge b)\vee(a\wedge c)\end{aligned}$$

综上所述，全序格中分配律成立。 ■

然而，并不是每个格都满足分配律，有两个重要的五点格都不满足分配律。

【例 17.10】 证明图 17-3 所示的两个五点格都不是分配格。

【证明】 在图 17-3a 的格中，$b\wedge(c\vee d)=b\wedge a=b$，但是$(b\wedge c)\vee(b\wedge d)=e\vee e=e$，因而 $b\wedge(c\vee d)\neq(b\wedge c)\vee(b\wedge d)$ 不满足分配律条件，故不是分配格。

在图 17-3b 的格中，$c \wedge (b \vee d) = c \wedge a = c$，但是 $(c \wedge d) \vee (c \wedge d) = e \vee d = d$，因而也不满足分配律的条件，故不是分配格。 ■

由此可知，如果一个格含与图 17-3a 或图 17-3b 同构的子格，那么它必定不是分配格。事实上，这个条件是判断一个格是否分配格的充分必要条件。

在分配格中，也存在着类似于群和整环的消去律。

定理 17.9　设 $\langle L, \vee, \wedge \rangle$ 是一个分配格，$a, b, c \in L$。如果 $a \vee b = a \vee c$ 且 $a \wedge b = a \wedge c$，则 $b = c$。

【证明】

$$
\begin{aligned}
b &= b \wedge (a \vee b) && \text{（吸收律）} \\
&= b \wedge (a \vee c) && \text{（已知条件）} \\
&= (b \wedge a) \vee (b \wedge c) && \text{（分配律）} \\
&= (a \wedge c) \vee (b \wedge c) && \text{（已知条件）} \\
&= (a \vee b) \wedge c && \text{（分配律）} \\
&= (a \vee c) \wedge c && \text{（已知条件）} \\
&= c && \blacksquare
\end{aligned}
$$

现在，讨论另一种重要的格——有补格。

定义 17.8　如果格 $\langle L, \vee, \wedge \rangle$ 中存在最大元和最小元，则称 $\langle L, \vee, \wedge \rangle$ 是**有界格**。

【例 17.11】　幂集格 $\langle 2^S, \subseteq \rangle$ 是有界格，其中最大元是 S，最小元是 $\varnothing$。因子格 $\langle D_n, | \rangle$ 也是有界格，其中最大元是 n，最小元是 1。 ■

有限格一定是有界格，但有界格不一定是有限格。例如，格 $\langle [0, 1], \leqslant \rangle$ 是有界格，其中 $[0, 1] = \{x \mid x \in R, 0 \leqslant x \leqslant 1\}$，而 $\leqslant$ 表示数的小于或等于关系，但这个格不是有限格。

一般把最大元记为 1，把最小元记为 0。在有界格 $\langle L, \vee, \wedge \rangle$ 中，根据最大元和最小元的定义，可以得到下面两类式子。$\forall a \in L$，

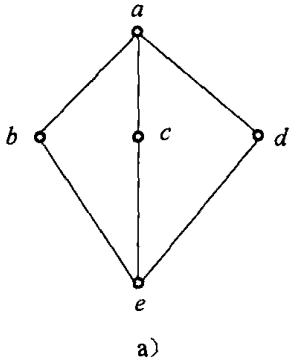
$$a \vee 1 = 1, \quad a \wedge 0 = 0$$

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

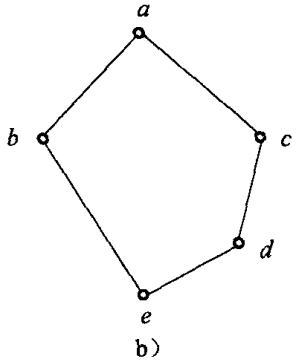
第一行两式说明格中零律成立，第二行两式则说明同一律成立。

定义 17.9　设 $\langle L, \vee, \wedge \rangle$ 是以 1 为最大元、以 0 为最小元的有界格。如果对于 $a \in L$，存在 $b \in L$ 使 $a \vee b = 1$ 且 $a \wedge b = 0$，则称 a 和 b 是**互补的元素**。a 的**补元**可以用 $\bar{a}$ 来表示。

【例 17.12】　在图 17-4 所示格中，b 和 a 是互补的元，因此 $\bar{a} = b$，$\bar{b} = a$。同样，也可以看出 $\bar{a} = e$，$\bar{b} = c$，$\bar{1} = 0$，$\bar{0} = 1$。然而，元素 d 却没有补元。 ■



a)



b)

图　17-3

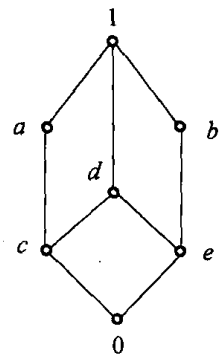


图　17-4

上面的例子说明，在一般有界格中，有的元素可以有多个补元，而某些元素却没有补元。

定义 17.10 每个元素都存在补元的有界格，叫做**有补格**。

注意，即使在有补格中，每个元素的补元也可以不止一个。例如在图 17.3a 的五点格中，每个元均有补元，且 c，d，b 中任何一个都是另一个的补元。

定理 17.10 在有补分配格中每个元的补元是唯一的。

【证明】 设 $\langle L, \vee, \wedge\rangle$ 是有补分配格，a 是 L 中任一元素。如果 a 有两个补元 b 和 c，由补元定义必有

$$a \vee b = 1 = a \vee c$$

$$a \wedge b = 0 = a \wedge c$$

利用分配格中的消去律，立即可得 $b=c$，即 a 的补元唯一。 ■

下面再证明有着广泛应用的 De Morgan 定律。

定理 17.11 在有补分配格 $\langle L, \vee, \wedge\rangle$ 中，有

① $\overline{a \vee b} = \bar{a} \wedge \bar{b}$　　② $\overline{a \wedge b} = \bar{a} \vee \bar{b}$

【证明】 ①因为 $(a \vee b) \vee (\bar{a} \wedge \bar{b}) = (a \vee \bar{a} \vee b) \wedge (a \vee b \vee \bar{b})$　　（分配律）

$$= 1 \wedge 1 = 1$$

$$(a \vee b) \wedge (\bar{a} \wedge \bar{b}) = (a \wedge \bar{a} \wedge \bar{b}) \vee (b \wedge \bar{a} \vee \bar{b})$$

$$= 0 \vee 0 = 0$$

由定义，$\bar{a} \wedge \bar{b}$ 是 $a \vee b$ 的补元，即 $\overline{a \vee b} = \bar{a} \wedge \bar{b}$。

②式可类似地加以证明，留作读者练习。 ■

由此可见，集合论中的 De Morgan 律和命题逻辑中的 De Morgan 律都是有补分配格中 De Morgan 律的特例。

在定义格上的偏序 $\leqslant$ 时，我们采用的办法是

$$a \leqslant b \Leftrightarrow a \wedge b = a$$

在有补格中，偏序还可以用另外的形式表达。

定理 17.12 设 $\langle L, \vee, \wedge\rangle$ 是有补分配格，$a, b \in L$，则 $a \leqslant b$ 当且仅当 $a \wedge \bar{b} = 0$。

【证明】 设 $a \leqslant b$，则 $a \wedge b = a$；两端同时与 $\bar{b}$ 作运算 $\wedge$，得到 $a \wedge \bar{b} = a \wedge b \wedge \bar{b} = 0$。

反过来，设 $a \wedge \bar{b} = 0$，两端同时与 b 作运算 $\vee$，得到

$$b = b \vee (a \wedge \bar{b}) = = (b \vee a) \wedge (b \vee \bar{b}) = a \vee b$$

即有 $a \leqslant b$。 ■

17.4 布尔代数

在一个格上再加上分配、有界、有补的条件，就得到一个布尔格。布尔格也称为布尔代数，它包含了三种运算：$\vee$，$\wedge$ 和 $^-$，并且有特殊元素 1 和 0，因而布尔格 $\langle B, \leqslant\rangle$ 一般又写成 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 的六元组形式以突出其代数特征。

综合前面几节的内容，可以知道，布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 满足下面的运算规律：

定理 17.13 设 a，b，c 是布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 中的任意元素，则

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

② $a \vee (b \vee c) = (a \vee b) \vee c$，$a \wedge (b \wedge c) = (a \wedge b) \wedge c$　　（结合律）

③ $a \vee (b \wedge a) = a$，$a \wedge (a \vee b) = a$　　（吸收律）

④ $a \wedge a = a$，$a \vee a = a$　　（幂等律）

⑤ $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$，$a \wedge (b \vee c) = (a \wedge b) \wedge (a \vee c)$　　（分配律）

⑥如果 $a \vee b = a \vee c$ 且 $a \wedge b = a \wedge c$，则 $b = c$　　（消去律）

⑦$0 \leqslant a \leqslant 1$　　（有界性）

⑧$a \vee 0 = a$，$a \wedge 1 = a$　　（同一律）

⑨$a \vee 1 = 1$，$a \wedge 0 = 0$　　（零律）

⑩$a \vee \bar{a} = 1$，$a \wedge \bar{a} = 0$　　（补元）

⑪$\overline{a \vee b} = \bar{a} \wedge \bar{b}$，$\overline{a \wedge b} = \bar{a} \vee \bar{b}$　　（De Morgan 律）

【证明】 参见前面各节。 ■

【例 17.13】 幂集格 $\langle 2^S, \subseteq \rangle$ 是布尔代数。相应的运算为并、交、补，最大元是 S，最小元是空集，因而可以写成 $\langle 2^S, \cup, \cap, ^-, \varnothing, S \rangle$ 的形式。 ■

【例 17.14】 因子格 $\langle D_{30}, | \rangle$ 是布尔代数，前面已经证明它是分配格，由习题十七第 19 题，$30 = 2 \times 3 \times 5$，所以它又是有补格，因而是布尔格。它对应的运算是 lcm，gcd，补运算用“^”表示 $\hat{n} = 30/n$，最小元是 1，最大元是 30。于是，这个布尔代数可写为 $\langle D_{30}$，lcm，gcd，^，1，30$\rangle$。 ■

通过考察一些具体的格发现，布尔格是很特殊的一类格。例如，从习题十七第 16 题中可以得出结论，元素个数超过 2 的全序格一定不是布尔格。那么，布尔格是否具有一定特征？能不能用一个标准形式来统一呢？下面介绍有关有限布尔代数的表示问题。

定义 17.11　*在布尔格 $\langle B, \leqslant \rangle$ 中，直接盖住最小元 0 的元素称为原子。*

a 是格中的原子，则不能存在元素 b 使得 $0 \leqslant b \leqslant a$。例如在幂集格 $\langle 2^S, \subseteq \rangle$ 中，由 S 中单元素构成的子集都是原子，其余的就不是原子。

在布尔代数中原子有一些特殊性质。下面的定理列出了几个在后面用到的结论。

定理 17.14　*在有限布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1 \rangle$ 中，a，b 是不同原子，x，y 是任意元素，则*

①$a \wedge b = 0$。

②$a \leqslant x$ 和 $a \leqslant \bar{x}$ 两式中有且仅有一式成立。

③$a \leqslant x \vee y$，当且仅当 $a \leqslant x$ 或者 $a \leqslant y$。

【证明】 ①由于 $a \wedge b \leqslant a$ 且 $a \wedge b \leqslant b$，不可能存在 $a \wedge b = a$ 或 $a \wedge b = b$ 得情况。因为它导致 $a \leqslant b$ 或 $b \leqslant a$ 的结果与原子定义矛盾，因此只能 $a \wedge b = 0$。

②两式不可能同时成立，否则 $a \leqslant x \wedge \bar{x} = 0$ 会导致矛盾。其次，由于 $a \wedge x \leqslant a$ 且 a 是原子，必然 $a \wedge x = a$ 或 $a \wedge x = 0$ 之一成立。前者表明 $a \leqslant x$，而后者 $a \wedge x = 0$，又因为 $a \wedge (x \vee \bar{x}) = a$，所以 $(a \wedge x) \vee (a \wedge \bar{x}) = a$，即有 $a \wedge \bar{x} = a$，$a \leqslant \bar{x}$ 成立。

③如果 $a \leqslant x \leqslant \vee y$，那么 $a \wedge (x \vee y) = a$，即 $(a \wedge x) \vee (a \wedge y) = a$。由于 a 是原子，必然 $a \wedge x = a$ 或 $a \wedge y = a$，即 $a \leqslant x$ 或 $a \leqslant y$。

反之，如果 $a \leqslant x$ 或者 $a \leqslant y$，都能导出 $a \leqslant x \vee y$ 的结论。 ■

定理 17.15　*设由有限布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1 \rangle$ 的全体原子构成的集合为*

$$S = \{a_1, a_2, , \cdots, a_n\}$$

则对 B 中任何不是 0 的元素 x，存在 a_{i1}，a_{i2}，…，$a_{im} \in S$ 使得

$$x = a_{i1} \vee a_{i2} \vee \cdots \vee a_{im} \tag{17-5}$$

并且当不计原子在式中出现的顺序时，这种表示是唯一的。

【证明】 显然，每个原子 a_i 都可以用 $a_i = a_i$ 的形式来表示。现在设 B 中不能用式 (17-5) 的形式表示出来的非 0 元素全体构成的集合为 A，那么 A 中不含 0 和任何原子。如果 A 为非空有限集，必有极小元 y，并且根据原子的定义知道，必有原子 $a_j \in S$ 使 $a_j < y$。

然而 y 可以表示成

$$y=(y\wedge\overline{a}_j)\vee a_j$$

由习题十七中的第 17 题（2）知道 $y\wedge\overline{a_j}<y$，这说明 $y\wedge\overline{a_j}\notin A$，因而存在原子 a_{j1}，a_{j2}，…，$a_{jt}\in S$ 使

$$y\wedge\overline{a}_j=a_{j1}\vee a_{j2}\vee\cdots\vee a_{jt}$$

从而

$$y=(y\wedge\overline{a_j})\vee a_j=a_{j1}\vee a_{j2}\vee\cdots\vee a_{jt}$$

与集合 A 的定义相矛盾，因而必然 $A=\varnothing$。这就证明了表示法的存在性。

至于唯一性，可设 x 为

$$x=b_1\vee b_2\vee\cdots\vee b_m$$

的形式，式中每个 b_i 都是 S 中的元素，并且 $b_i\leqslant x$，现在任取一个小于等于 x 的原子 a，即 $a\in S$ 且 $a\leqslant x$，那么

$$0\neq a=a\wedge x=(a\wedge b_1)\vee(a\wedge b_2)\vee\cdots\vee(a\wedge b_m)$$

其中至少有一个 $a\wedge b_t\neq 0$。但是 a 和 b_t 都是原子，根据原子定义，必定有 $a=b_t$。由此可知，x 的表达式中必然包括所有小于等于 x 的原子，因而表示是唯一的。 ■

定理 17.15 说明一个布尔代数完全由它的原子所决定，下面的定理说明具有相同数目原子的两个布尔代数是同构的，从而与幂集代数 $\langle 2^S,\cup,\cap,^-,\varnothing,S\rangle$ 同构。

定理 17.16 *设 A 是以 $S=\{a_1,a_2,\cdots,a_n\}$ 为原子集的布尔代数 $\langle A,\vee,\wedge,^-,0,1\rangle$，$B$ 是以 $V=\{b_1,b_2,\cdots,b_n\}$ 为原子集的布尔代数 $\langle B,\cup,\cap,^\sim,0',1'\rangle$，则必存在双射 $f:A\to B$，使得对 A 中任意元素 x，y，下列式子成立。*

① $f(x\vee y)=f(x)\cup f(y)$

② $f(x\wedge y)=f(x)\cap f(y)$

③ $f(\overline{x})=f(\tilde{x})$

【证明】 由定理 17.15，A 中每个元素 $x\neq 0$ 均可唯一表示为

$$x=a_{i1}\vee a_{i2}\vee\cdots\vee a_{in}\tag{17-6}$$

为此，定义映射 $f:A\to B$，使得

$$f(x)=b_1\cup b_2\cup\cdots\cup b_{ik}\tag{17-7}$$

特别当 x 是原子时，不妨设 $f(a_i)=b_i(1\leqslant i\leqslant n)$。由于表达式（17-6）和式（17-7）的唯一性，容易看出 f 是双射，根据 f 的定义，式（17-6）可以表示为

$$f(x)=\cup\{f(a_i)\mid a_i\in S\text{ 且 }a_i\leqslant x\}$$

也可以表示为

$$f(x)=\cup\{b_i\mid b_i\in V\text{ 且 }b_i\leqslant f(x)\}$$

由 $f(x)$ 表达式的唯一性，可知，对任何 $a\in S$，

$$a\leqslant x\Leftrightarrow f(a)\leqslant f(x)\tag{17-8}$$

在式（17-8）中，以 $x\vee y$ 代 x 得到

$$a\leqslant x\vee y\Leftrightarrow f(a)\leqslant f(x\vee y)$$

由于 a 是 A 中的原子，所以

$$a\leqslant x\vee y\Leftrightarrow a\leqslant x\text{ 或 }a\leqslant y$$

根据式（17-8）又可得到

$$f(a)\leqslant f(x\vee y)\Leftrightarrow f(a)\leqslant f(x)\cup f(y)$$

由于 $f(a)$ 既是 $f(x\vee y)$ 的原子，也是 $f(x)\cup f(y)$ 的原子，而 $f(x\vee y)$ 与 $f(x)\cup f(y)$

都能被小于等于它们的原子唯一表出，因此 $f(x \vee y)=f(x) \cup f(y)$，这就证明了①式。

②式可类似地证明。

至于③式，由①式和②式可得

$$f(x) \cup f(\bar{x}) = f(x \vee \bar{x}) = f(1)$$
$$f(x) \cap f(\bar{x}) = f(x \wedge \bar{x}) = f(0)$$

这表明 $f(\bar{x})=f(\tilde{x})$，③式得到证明。 ■

推论 17.16.1　任何 n 个原子的有限布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 都和 n 元集 S 对应的幂集代数 $\langle 2^S, \cup, \cap, ^-, \varnothing, S\rangle$ 同构，从而具有 n 个原子的布尔代数共有个 2^n 元素。

【证明】　推论的结论直接可由定理 17.16 得出，此略。 ■

17.5　布尔表达式

设 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 是一个布尔代数，现考虑一个从 B^n 到 B 的函数。

【例 17.15】　设 $B=\{0, 1\}$，表 17-1 表示了一个 B^3 从到 B 的函数 f；设 $B=\{0, 1, 2, 3\}$，表 17-2 表示了一个从 B^2 到 B 的函数 g。

表　17-1

	f		f
⟨0, 0, 0⟩	0	⟨1, 0, 0⟩	1
⟨0, 0, 1⟩	0	⟨1, 0, 1⟩	1
⟨0, 1, 0⟩	1	⟨1, 1, 0⟩	0
⟨0, 1, 1⟩	0	⟨1, 1, 1⟩	1

表　17-2

	f		f
⟨0, 0⟩	1	⟨2, 0⟩	2
⟨0, 1⟩	0	⟨2, 1⟩	0
⟨0, 2⟩	0	⟨2, 2⟩	1
⟨0, 3⟩	3	⟨2, 3⟩	1
⟨1, 0⟩	1	⟨3, 0⟩	3
⟨1, 1⟩	1	⟨3, 1⟩	0
⟨1, 2⟩	0	⟨3, 2⟩	2
⟨1, 3⟩	3	⟨3, 3⟩	2

以上这种表示函数的方法通常称为列表法。 ■

下面采用别的方法来描述函数。

定义 17.12　设 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 是一个布尔代数，在此布尔代数上定义布尔表达式：

①B 中任何元素是一个**布尔表达式**。

②任何变元是一个**布尔表达式**。

③如果 e_1 和 e_2 是布尔表达式，则 $\bar{e}_1$，$(e_1 \vee e_2)$，$(e_1 \wedge e_2)$ 都是**布尔表达式**。

只有经过有限次使用②和③得到的符号串才是**布尔表达式**。

【例 17.16】　$\langle\{0, 1, 2, 3\}, \vee, \wedge, ^-, 0, 1\rangle$ 是一个布尔代数，那么 $0 \wedge x_1$，$(1 \vee \bar{x}) \wedge x_2$，$((\overline{2 \vee 3}) \wedge (\bar{x} \vee x_2)) \wedge (\overline{x_1 \wedge x_3})$ 都是布尔表达式，并且分别称为含有单个变元 x_1 的布尔表达式，含有 2 个变元 x_1，x_2 的布尔表达式和含有 3 个变元 x_1，x_2，x_3 的布尔表达式。 ■

定义 17.13　一个含有 n 个相异变元的布尔表达式，称为含有 **n 元的布尔表达式**，记为

$$E(x_1, x_2, \cdots, x_n)$$

其中 x_1，x_2，…，x_n 为**变元**。

定义 17.14 布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 上的一个含有 n 元的布尔表达式

$$E(x_1, x_2, \cdots, x_n)$$

的**值**是指：将 B 中的元素作为变元 x_i（$i=1, 2, \cdots, n$）的值来代替表达式中相应的变元（即对变元赋值），从而计算出表达式的值。

【例 17.17】 设布尔代数 $\langle\{0, 1\}, \vee, \wedge, ^-, 0, 1\rangle$ 上的布尔表达式为

$$E(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (\overline{x}_1 \vee \overline{x}_2) \wedge (\overline{x_2 \vee x_3})$$

如果变元的一组赋值为 $x_1=1$，$x_2=0$，$x_3=1$，那么便可求得

$$E(1,0,1) = (1 \vee 0)(\overline{1} \vee \overline{0}) \wedge (\overline{0 \vee 1}) = 1 \wedge 1 \wedge 0 = 0$$ ■

定义 17.15 设布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 上的两个 n 元的布尔表达式为

$$E_1(x_1, x_2, \cdots, x_n)$$

和

$$E_2(x_1, x_2, \cdots, x_n)$$

如果对于 n 个变元的任意赋值 $x_i=\tilde{x}_i$，$\tilde{x}_i \in B$ 时均有

$$E_1(\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_n) = E_2(\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_n)$$

则称这两个布尔表达式是**等价的**。记作

$$E_1(x_1, x_2, \cdots, x_n) = E_2(x_1, x_2, \cdots, x_n)$$

【例 17.18】 在布尔代数$\langle\{0, 1\}, \vee, \wedge, ^-, 0, 1\rangle$ 上的两个布尔表达式

$$E_1(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge \overline{x}_3)$$

和

$$E_2(x_1, x_2, x_3) = x_1 \wedge (x_2 \vee \overline{x}_3)$$

容易验证它们是等价的，如以下方法。

$$\begin{cases} E_1(0,1,1) = (0 \wedge 1) \vee (0 \wedge 0) = 0 \vee 0 = 0 \\ E_2(0,1,1) = 0 \wedge (1 \vee 0 = 0 \wedge 1 = 0 \end{cases}$$

$$\begin{cases} E_1(1,1,1) = (1 \wedge 1) \vee (1 \wedge 0) = 1 \vee 0 = 1 \\ E_2(1,1,1) = 1 \wedge (1 \vee 0) = 1 \wedge 1 = 1 \end{cases}$$ ■

事实上，由于布尔代数是有补分配格，所以当对布尔表达式赋值以后，表达式中运算 $\vee$ 对于运算 $\wedge$ 是可分配的，运算 $\wedge$ 对于运算 $\vee$ 也是可分配的。因此，如果将布尔表达式中的变元看作是已经赋值的，那么上例中的 E_1 和 E_2 的等价性可以直接写为

$$\begin{aligned} E_2(x_1, x_2, x_3) &= x_1 \wedge (x_2 \vee \overline{x}_3) \\ &= (x_1 \wedge x_2) \vee (x_1 \wedge \overline{x}_3) \\ &= E_1(x_1, x_2, x_3) \end{aligned}$$

对于布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 上的任何一个布尔表达式 $E(x_1, x_2, \cdots, x_n)$。由于运算 $\vee$，$\wedge$，$^-$ 在 B 上的封闭性，所以对于任何一个有序 n 元组 $\langle x_1, x_2, \cdots, x_n\rangle$（$x_i \in B$）可以对应着一个表达式 $E(x_1, x_2, \cdots, x_n)$ 的值，这个值必属于 B。由此可见，可以说布尔表达式 $E(x_1, x_2, \cdots, x_n)$ 确定了一个由 B^n 到 B 的函数。

容易验证，在布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 上的布尔表达式

$$E(x_1, x_2, x_3) = (\overline{x}_1 \wedge x_2 \wedge \overline{x}_3) \vee (x_1 \wedge \overline{x}_2) \vee (x_1 \wedge x_3)$$

定义了表 17-1 中的从 $\{0, 1\}^3$ 到 $\{0, 1\}$ 的函数。

然而，是否任意一个从 A^n 到 A 的函数都一定能列出一个在布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 上的布尔表达式呢？这个问题的回答是否定的。

定义 17.16　设 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 是一个布尔代数，一个由 A^n 到 A 的函数，如果它能够用 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 上的 n 元布尔表达式来表示，那么，这个函数就称为**布尔函数**。

定理 17.17　对于两个元素的布尔代数 $\langle\{0, 1\}, \vee, \wedge, ^-, 0, 1\rangle$，任何一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数都是布尔函数。

【证明】　含有 n 个变元 $x_1, x_2, \cdots, x_n$ 的布尔表达式，如果它有形式 $\tilde{x}_1 \wedge \tilde{x}_2 \wedge \cdots \wedge \tilde{x}_n$（其中 $\tilde{x}_i$ 是 x_i 或 $\overline{x}_i$ 中任意一个），则称这个布尔表达式为**小项**。一个在 $\langle\{0, 1\}, \vee, \wedge, ^-, 0, 1\rangle$ 上的布尔表达式，如果它能表示成小项的并，则称这个布尔表达式为**析取范式**。对于一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数，先用那些使函数值为 1 的有序 n 元组分别构造小项 $\tilde{x}_1 \wedge \tilde{x}_2 \wedge \cdots \wedge \tilde{x}_n$，其中

$$\tilde{x}_i = \begin{cases} x_i & \text{若 } n \text{ 元组中第 } i \text{ 个分量为 } 1 \\ \overline{x}_i & \text{若 } n \text{ 元组中第 } i \text{ 个分量为 } 0 \end{cases}$$

然后，再由这些小项所组成析取范式，它就是原来函数所对应的布尔表达式。

类似地，含有 n 个变元 $x_1, x_2, \cdots, x_n$ 的布尔表达式，如果它有形式 $\tilde{x}_1 \vee \tilde{x}_2 \vee \cdots \vee \tilde{x}_n$（其中 $\tilde{x}_i$ 是 x_i 或 $\overline{x}_i$ 中任意一个），则称这个布尔表达式为**大项**。一个在 $\langle\{0, 1\}, \vee, \wedge, ^-, 0, 1\rangle$ 上的布尔表达式，如果它能表示成大项的交，则称这个布尔表达式为**合取范式**。对于一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数，可以用那些使函数值为 0 的有序 n 元组分别构造大项 $\tilde{x}_1 \vee \tilde{x}_2 \vee \cdots \vee \tilde{x}_n$，其中

$$\tilde{x}_i = \begin{cases} x_i & \text{若 } n \text{ 元组中第 } i \text{ 个分量为 } 0 \\ \overline{x}_i & \text{若 } n \text{ 元组中第 } i \text{ 个分量为 } 1 \end{cases}$$

然后，再由这些大项所组成合取范式，它就是原来函数所对应的布尔表达式。 ■

【例 17.19】　讨论表 17-3 所给出的函数 f 的析取范式和合取范式。

表　17-3

	f		f
$\langle 0, 0, 0\rangle$	1	$\langle 1, 0, 0\rangle$	0
$\langle 0, 0, 1\rangle$	0	$\langle 1, 0, 1\rangle$	0
$\langle 0, 1, 0\rangle$	1	$\langle 1, 1, 0\rangle$	0
$\langle 0, 1, 1\rangle$	0	$\langle 1, 1, 1\rangle$	1

因为函数值为 1 所对应的有序三元组分别为 $\langle 0, 0, 0\rangle$，$\langle 0, 1, 0\rangle$ 和 $\langle 1, 1, 1\rangle$，于是可分别构造小项为 $\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3$，$\overline{x}_1 \wedge x_2 \wedge \overline{x}_3$ 和 $x_1 \wedge x_2 \wedge x_3$。因此，函数 f 所对应的析取范式为

$$(\overline{x}_1 \wedge \overline{x}_2 \wedge \overline{x}_3) \vee (\overline{x}_1 \wedge x_2 \wedge \overline{x}_3) \vee (x_1 \wedge x_2 \wedge x_3)$$

它是一个含有 3 个小项的析取范式的布尔表达式。

因为函数值为 0 所对应的有序三元组分别为 $\langle 0, 0, 1\rangle$，$\langle 0, 1, 1\rangle$，$\langle 1, 0, 0\rangle$，$\langle 1, 0, 1\rangle$ 和 $\langle 1, 1, 0\rangle$，于是可分别构造大项为 $x_1 \vee x_2 \vee \overline{x}_3$，$x_1 \vee \overline{x}_2 \vee \overline{x}_3$，$\overline{x}_1 \vee x_2 \vee x_3$，$\overline{x}_1 \vee x_2 \vee \overline{x}_3$ 和 $\overline{x}_1 \vee \overline{x}_2 \vee x_3$。因此，函数 f 所对应的合取范式为

$$(x_1 \vee x_2 \vee \overline{x}_3) \wedge (x_1 \vee \overline{x}_2 \vee \overline{x}_3) \wedge (\overline{x}_1 \vee x_2 \vee x_3) \wedge (\overline{x}_1 \vee x_2 \vee \overline{x}_3) \wedge (\overline{x}_1 \vee \overline{x}_2 \vee x_3)$$

它是一个含有 5 个大项的合取范式的布尔表达式。 ■

下面，将布尔代数 $\langle\{0, 1\}, \vee, \wedge, ^-, 0, 1\rangle$ 上的布尔表达式的析取范式和合取范式的概念扩充到一般的布尔代数上。假如 $E(x_1, x_2, \cdots, x_n)$ 是布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$

上的一个布尔表达式。如果这个布尔表达式能够表示成形如 $C_{\delta_1\delta_2\cdots\delta_n}\wedge\tilde{x}_1\wedge\tilde{x}_2\wedge\cdots\wedge\tilde{x}_n$ 的并，其中 $C_{\delta_1\delta_2\cdots\delta_n}$ 是 B 中的一个元素，$\tilde{x}_i$ 是 x_i 或 $\overline{x}_i$ 中任意一个，则称这种布尔表达式为**析取范式**。

定理 17.18 设 $E(x_1, x_2, \cdots, x_n)$ 是布尔代数 $\langle B, \vee, \wedge, ^-, 0, 1\rangle$ 上的任意一个布尔表达式，则它一定能写成析取范式。

【证明】 令 $E(x_i=a)=E(x_1, x_2, \cdots, x_{i-1}, a, x_{i+1}, \cdots, x_n)$，$a\in B$。表达式 $E(x_1, x_2, \cdots, x_n)$ 的长度定义为该表达式中出现的 B 的元素个数、变元的个数以及 $\vee$，$\wedge$，$^-$ 的个数的总和（如果重复出现就要重复计数）。记 $E(x_1, x_2, \cdots, x_n)$ 的长度为 $|E|$。

首先证明：对于任何 x_i，必有

$$E(x_1, x_2, \cdots, x_n)=(\overline{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))$$

对 $|E|$ 用归纳证明。

若 $|E|=1$，则 $E=a$ 或 $E=x_j$，如果 $E=a$，则有

$$E(x_i=0)=E(x_i=1)=a$$

所以

$$\begin{aligned}E=a&=(\overline{x}_i\vee x_i)\wedge a\\&=(\overline{x}_i\wedge a)\vee(x_i\wedge a)\\&=(\overline{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))\end{aligned}$$

如果 $j=i$，显然有 $E(x_i=0)=0$，$E(x_i=1)=1$，所以

$$\begin{aligned}E=x_j&=(\overline{x}_i\wedge 0)\vee(x_i\wedge 1)\\&=(\overline{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))\end{aligned}$$

如果 $j\neq i$，显然有 $E(x_i=0)=E(x_i=1)=x_j$，所以

$$\begin{aligned}E=x_j&=(\overline{x}_i\vee x_j)\wedge x_j\\&=(\overline{x}_i\wedge x_j)\vee(x_i\wedge x_j)\\&=(\overline{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))\end{aligned}$$

因此，$|E|=1$ 时，$E=(\overline{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))$ 成立。

设 $|E|\leqslant n$ 时，结论成立。当 $|E|=n+1$ 时，有以下三种情况：

1）如果 $E=E_1\vee E_2$，则必有 $|E_1|\leqslant n$，$|E_2|\leqslant n$，因此由归纳假设，就有

$$E_1=(\overline{x}_i\wedge E_1(x_i=0))\vee(x_i\wedge E_1(x_i=1))$$

$$E_2=(\overline{x}_i\wedge E_2(x_i=0))\vee(x_i\wedge E_2(x_i=1))$$

$$\begin{aligned}E&=E_1\vee E_2\\&=[(\overline{x}_i\wedge E_1(x_i=0))\vee(x_i\wedge E_1(x_i=1))]\vee[(\overline{x}_i\wedge E_2(x_i=0))\vee(x_i\wedge E_2(x_i=1))]\\&=[\overline{x}_i\wedge(E_1(x_i=0)\vee E_2(x_i=0))]\vee[\overline{x}_i\wedge E_1(x_i=1)\vee E_2(x_i=1))]\\&=(\overline{x}_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))\end{aligned}$$

2）如果 $E=E_1\wedge E_2$，则必有 $|E_1|\leqslant n$，$|E_2|\leqslant n$，同样由归纳假设，就有

$$\begin{aligned}E&=E_1\wedge E_2\\&=[(\overline{x}_i\wedge(E_1(x_i=0))\vee(x_i\wedge E_1(x_i=1))]\wedge[(\overline{x}_i\wedge E_2(x_i=0))\vee(x_i\wedge E_2(x_i=1))]\\&=[\overline{x}_i\wedge(E_1(x_i=0)\wedge E_2(x_i=0))]\vee[\overline{x}_i\wedge(E_1(x_i=1)\wedge E_2(x_i=1))]\\&=(x_i\wedge E(x_i=0))\vee(x_i\wedge E(x_i=1))\end{aligned}$$

3）如果 $E=\overline{E}_1$，则必有 $|E_1|=n$，由归纳假设，即有

$$\begin{aligned}E=\overline{E}_1&=\overline{(\overline{x}_1\wedge E_1(x_1=0))\vee(x_1\wedge E_1(x_1=1))}\\&=\overline{(\overline{x}_1\wedge E_1(x_1=0))\wedge(x_1\wedge E_1(x_1=1))}\end{aligned}$$

$$
\begin{aligned}
&=(x_i \vee \overline{E}_1(x_i=0)) \wedge (\overline{x}_i \vee \overline{E}_1(x_i=1))\\
&=[(x_i \vee \overline{E}_1(x_i=0)) \wedge \overline{x}_i] \vee [x_i \vee \overline{E}_1(x_i=0)) \wedge \overline{E}_1(x_i=1)]\\
&=[(x_i \wedge \overline{x}_i) \vee (\overline{E}_1(x_i=0) \wedge \overline{x}_i)] \vee [(x_i \wedge \overline{E}_1(x_i=1)) \vee \overline{E}_1(x_i=0) \wedge \overline{E}_1(x_i=1))]\\
&=(\overline{x}_i \wedge E(x_i=0)) \vee (\overline{x}_i \wedge E(x_i=1)) \vee [(\overline{x}_i \vee x_i) \wedge (E(x_i=0) \wedge E(x_i=1))]\\
&=(\overline{x}_i \wedge \overline{E}(x_i=0)) \vee (\overline{x}_i \wedge E(x_i=1))] \vee (\overline{x}_i \wedge (E(x_i=0) \wedge E(x_i=1)) \vee\\
&\quad (x_i \wedge E(x_i=0) \wedge E(x_i=1))\\
&=[(\overline{x}_i \wedge \overline{E}(x_i=0)) \wedge (1 \vee E(x_i=1))] \vee [(\overline{x}_i \wedge E(x_i=1)) \wedge (1 \vee E(x_i=0))]\\
&=(\overline{x}_i \wedge E(x_i=0)) \vee (x_i \wedge E(x_i=1))
\end{aligned}
$$

由上面证明的结果

$$E(x_1,x_2,\cdots,x_n)=(\overline{x}_i \wedge E(x_i=0)) \vee (x_i \wedge E(x_i=1))$$

可得

$$
\begin{aligned}
&E(x_1,x_2,\cdots,x_n)\\
&=(\overline{x}_1 \wedge E(0,x_2,\cdots,x_n)) \vee (x_1 \wedge E(1,x_2,\cdots,x_n))\\
&=\{\overline{x}_1 \wedge (\overline{x}_2 \wedge E(0,0,x_3,\cdots,x_n)) \vee (x_2 \wedge E(0,1,x_3,\cdots,x_n))\} \vee\\
&\quad \{x_i \wedge (\overline{x}_2 \wedge E(1,0,x_3,\cdots,x_n)) \vee (x_2 \wedge E(1,1,x_3,\cdots,x_n))\}\\
&=[\overline{x}_1 \wedge \overline{x}_2 \wedge E(0,0,x_3,\cdots,x_n)] \vee [\overline{x}_1 \wedge x_2 \wedge E(0,1,x_3,\cdots,x_n)] \vee\\
&\quad [x_1 \wedge \overline{x}_2 \wedge E(1,0,x_3,\cdots,x_n)] \vee [x_1 \wedge x_2 \wedge E(1,1,x_3,\cdots,x_n)]\\
&\qquad \vdots\\
&=[x_1 \wedge \overline{x}_2 \wedge \cdots \wedge \overline{x}_n \wedge E(0,0,\cdots,0)] \vee\\
&\quad [\overline{x}_1 \wedge \overline{x}_2 \wedge \cdots \wedge \overline{x}_{n-1} \wedge \overline{x}_n \wedge E(0,0,\cdots,0,1)] \vee \cdots \vee\\
&\quad [x_1 \wedge x_2 \wedge \cdots \wedge x_{n-1} \wedge \overline{x}_n \wedge E(1,1,\cdots,1,0)] \vee [\overline{x}_1 \wedge \overline{x}_2 \wedge \cdots \wedge \overline{x}_{n-1} \wedge x_n \wedge E(1,1,\cdots,1,1)]
\end{aligned}
$$

其中每一个方括号里的布尔表达式可以写成统一形式 $C_{\delta_1\delta_2\cdots\delta_n} \wedge \tilde{x}_1 \wedge \tilde{x}_2 \wedge \cdots \wedge \tilde{x}_n$，而 $C_{\delta_1\delta_2\cdots\delta_n} \in B$，$\tilde{x}_i$ 是 x_i 或 $\overline{x}_i$ 中的一个。

类似地，可以通过证明以下等式

$$E(x_1,x_2,\cdots,x_n)=(x_i \vee E(x_i=0)) \wedge (\overline{x}_i \vee E(x_i=1))$$

来证明任何布尔表达式能够写成形如 $C_{\delta_1\delta_2\cdots\delta_n} \vee \tilde{x}_1 \vee \tilde{x}_2 \vee \cdots \vee \tilde{x}_n$ 的交，其中 $C_{\delta_1\delta_2\cdots\delta_n} \in B$，$\tilde{x}_i$ 是 x_i 或 $\overline{x}_i$ 中的一个，即表示成合取范式。 ■

【例 17.20】 表 17-2 中所确定的从 B^2 到 B 的函数 g，其中 $B=\{0, 1, 2, 3\}$，证明 g 不是布尔函数。

【证明】 （反证法）如果是布尔函数，那么它的布尔表达式必可以表示成析取范式为：

$$g(x_1,x_2)=(C_{11} \wedge x_1 \wedge x_2) \vee (C_{12} \wedge x_1 \wedge \overline{x}_2) \vee (C_{21} \wedge \overline{x}_1 \wedge x_2) \vee (C_{22} \wedge \overline{x}_1 \wedge \overline{x}_2)$$

由表 17-2 可知

$$
\begin{aligned}
C_{11} &= g(1,1)=1\\
C_{12} &= g(1,0)=1\\
C_{21} &= g(0,1)=0\\
C_{22} &= g(0,0)=1
\end{aligned}
$$

所以

$$g(x_1,x_2)=(x_1 \wedge x_2) \vee (x_1 \wedge \overline{x}_2) \vee (\overline{x}_1 \wedge \overline{x}_2)$$

对于布尔格 $\langle\{0, 1, 2, 3\}, \leqslant\rangle$，可用图 17-5 的 Hasse 图来表示。由图 17-5 可知

$$\begin{aligned} g(3,3) &= (3 \wedge 3) \vee (3 \wedge 2) \vee (2 \wedge 2) \\ &= 3 \vee 0 \vee 2 \\ &= 1 \end{aligned}$$

这就与表 17-2 中的 $g(3, 3)=2$ 相矛盾，所以表 17-2 中的函数不是布尔函数。 ■

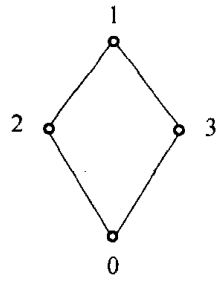


图 17-5

作为布尔代数的直接应用，可以确认：

1）命题逻辑可以用布尔代数$\langle\{F, T\}, \vee, \wedge, ^-, 0, 1\rangle$来描述，一个原子命题就是一个变元，它的取值为 T 或 F，因此，任一复合命题都可以用代数系统 $\langle\{F, T\}, \vee, \wedge, ^-, 0, 1\rangle$ 上的一个布尔函数来表示。

2）开关代数可以用布尔代数$\langle\{$断开，闭合$\}$，并联，串联，反向，0，1$\rangle$来描述，一个开关就是一个变元，它的取值为“断开”或“闭合”，因此，任一开关线路都可以用代数系统 $\langle\{$断开，闭合$\}$，并联，串联，反向，0，1$\rangle$ 上的一个布尔函数来表示。

习题十七

1. 证明：$\langle \mathbf{N}, | \rangle$ 是格，其中的偏序“$|$”为整除。
2. 设 n 为正整数，D_n 为 n 的所有正因子构成的集合。画出 $\langle D_6, | \rangle$，$\langle D_8, | \rangle$，$\langle D_{30}, | \rangle$ 对应的 Hasse 图，并证明它们都是格。
3. 在 $\langle L, \vee, \wedge \rangle$ 上定义偏序“$\leqslant$”为 $a \leqslant b$ 当且仅当 $a \wedge = a$，可使 $\langle L, \leqslant \rangle$ 成为偏序格。证明：这个偏序也可以等价地定义为 $a \leqslant b$，当且仅当 $a \vee b = b$。
4. 设 S 是有限个整数构成的集合，定义二元运算 max 和 min 分别为求二数中的最大数和最小数。证明：$\langle$S, max, min$\rangle$ 是格。对应的偏序格是什么？
5. 证明：在任何格中下述结论成立：
   (1) 如果 $a \wedge b \wedge c = a \vee b \vee c$，则必有 $a=b=c$。
   (2) $a \vee [(a \vee b) \wedge (a \vee c)] = (a \vee b) \wedge (a \vee c)$。
6. 设 f 是集合 A 到 B 的映射，令 $S=\{y \mid y=f(x), x \in 2^A\}$。证明：$\langle S, \subseteq \rangle$ 是 $\langle 2^B, \subseteq \rangle$ 的子格。
7. 设格上的偏序为“$\leqslant$”，$a, b, c \in L$，且 $a \leqslant b \leqslant c$。求证：
   (1) $a \vee b = b \wedge c$
   (2) $(a \wedge b) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
8. 设 $\langle L, \vee, \wedge, \rangle$ 是格，“$\leqslant$”是对应偏序，a, b, c, d 是 L 中任意元素。证明：
   (1) $(a \wedge b) \vee (c \wedge d) \leqslant (a \vee c) \wedge (b \vee d)$
   (2) $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$
9. 设 $\mathbf{E}$ 是正偶数集，$\mathbf{N}^+$ 是正整数集，定义 $\mathbf{N}^+$ 上的偏序为整除，证明：格 $\langle \mathbf{N}^+, | \rangle$ 和 $\langle \mathbf{E}, | \rangle$ 同构。
10. 确定图 17-6 各 Hasse 图对应的格中哪些是分配格，哪些是有补格。

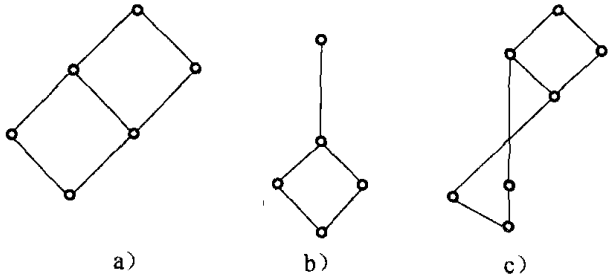


图 17-6

11. 求证：〈**N**，max，min〉是分配格。

12. 设〈L，$\vee$，$\wedge$〉是分配格，$\leqslant$是对应的偏序，$a,b\in L$，且$a\leqslant b$。定义集合

$$S=\{x\mid x\in L\wedge a\leqslant x\leqslant b\}$$

及映射$f:L\to S$为$f(x)=(x\vee a)\wedge b$。证明：f是格同态。

13. 设a，b，c是格中任意3个元素。证明：格是分配格的充要条件是：

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

14. 设〈L，$\vee$，$\wedge$〉是以$\leqslant$为偏序的格。如果对任意$a,b,c\in L$，由$a\leqslant b$能得到$a\vee(b\wedge c)=b\wedge(a\vee c)$，则称〈$L$，$\vee$，$\wedge$〉是一个模格。证明：〈$L$，$\vee$ $\wedge$〉是模格当且仅当对任意a，b，$c\in L$，等式$a\vee(b\wedge(a\vee c))=(a\vee b)\wedge(a\wedge c)$成立。

15. 作一个十元格的 Hasse 图，使其中某些元有多个补元，某些元有一个补元，某些元没有补元。

16. 如果全序格〈L，$\vee$，$\wedge$〉是有补格，求L中的元素个数。

17. 设〈L，$\vee$，$\wedge$〉是有补分配格，x，y，$z\in L$。证明：

(1) 如果$x\leqslant y$且$y\wedge z=0$，则$z\leqslant\overline{x}$。

(2) 如果$x<y$，则$\overline{x}\wedge y<y$。

18. 设〈L，$\vee$，$\wedge$〉是有补分配格，a和b是L中的两个确定元素，求下面方程组的解。

$$\begin{cases}x\vee a=b\\ x\wedge a=0\end{cases}$$

19. 说明因子格〈D_{12}，$|$〉不是有补格。证明：一个因子格〈D_n，$|$〉是有补格的充分必要条件是，n的素因子分解式中每个因子的幂不超过1。

20. 证明：因子格〈D_{210}，$|$〉是布尔代数，并找出它的全部原子，以及所有包含元素1和210的子布尔代数。

21. 设x，y是布尔代数的元素。证明：$x\leqslant y\Leftrightarrow\overline{y}\leqslant\overline{x}$。

22. 设x和y是一个布尔代数的元素，它们都能被布尔代数的原子唯一地表示出来。如果x能被原子a_{i1}，a_{i2}，…，a_{im}表示出来，y能被原子a_{j1}，a_{j2}，…，a_{jn}表示出来，试确定$x\vee y$，$x\wedge y$和$\overline{x}$的表达式。

23. 设〈B，$\vee$，$\wedge$，$^-$，0，1〉是布尔代数，在B上定义新运算“$+$”使得$a+b=(a\wedge\overline{b})\vee(\overline{a}\wedge b)$。证明：〈$B$，$+$〉是交换群。

24. 设〈B，$\vee$，$\wedge$，$^-$，0，1〉是布尔代数，在B上定义新运算“$+$”和“$*$”如下：

$$a+b=(a\wedge\overline{b})\ \vee\ (\overline{a}\wedge b),\quad a*b=a\wedge b$$

证明：〈B，$+$，$*$〉是环。

25. 设S是实数区间[0，1)，集合A是以空集$\varnothing$以及可以表示成S的形如[x，y)的子区间的并的全体构成的集合。在A上定义运算$\cup$，$\cap$，$^-$使得对于元素a，$b\in A$，$a\cup b$为a和b中子区间之并，$a\cap b$为a和b中子区间之交的并，$\overline{a}=$ [0，1)$-a$。例如设

$$a=[0.1,0.2)\cup[0.5,0.6)$$
$$b=[0.15,0.3)\cup[0.4,0.5)$$

那么

$$a\cup b=[0.1,\ 0.3)\ \cup\ [0.4,\ 0.6]$$
$$a\cap b=[0.15,\ 0.2)$$
$$\overline{a}=[0,\ 0.1)\ \cup\ [0.2,\ 0.5)\ \cup\ [0.6,\ 1)$$

证明：〈A，$\cup$，$\cap$，$^-$，$\varnothing$，[0，1)〉是布尔代数，它的原子是什么？

26. 设$E(x_1,x_2,x_3)=(x_1\wedge x_2)\vee(x_2\wedge x_3)\vee(\overline{x}_2\wedge x_3)$

是布尔代数

$$\langle\{0,1\},\vee,\wedge,^{-},0,1\rangle$$

上的一个布尔表达式。试写出 $E(x_1, x_2, x_3)$ 的析取范式和合取范式。

27. 设 $E(x_1, x_2, x_3, x_4)=(x_1\wedge x_2\wedge\overline{x}_3)\vee(x_1\wedge\overline{x}_2\wedge x_4)\vee(x_2\wedge\overline{x}_3\wedge\overline{x}_4)$

是布尔代数

$$\langle\{0,1\},\vee,\wedge,^{-},0,1\rangle$$

上的一个布尔表达式。试写出 $E(x_1, x_2, x_3, x_4)$ 的析取范式和合取范式。

28. 对于表 17-4 中的函数 f，试分别用析取范式和合取范式来表示。

表 17-4

	f
⟨0, 0, 0⟩	1
⟨0, 0, 1⟩	0
⟨0, 1, 0⟩	1
⟨0, 1, 1⟩	0
⟨1, 0, 0⟩	0
⟨1, 0, 1⟩	1
⟨1, 1, 0⟩	0
⟨1, 1, 1⟩	1