9.3 几个典型的代数系统

- 半群、独异点与群（重点讲）
- 环与域（略讲）
- 格与布尔代数（有所选择讲）

半群与独异点

定义　设$V=<S,\circ>$是代数系统，$\circ$为二元运算.

(1) 如果$\circ$是可结合的，则称$V=<S,\circ>$为半群.

(2) 如果半群$V=<S,\circ>$中的二元运算含有幺元，则称V为含幺半群，也可叫作独异点. 为了强调幺元e的存在，有时将独异点记为$<S,\circ,e>$.

(3) 如果半群$V=<S,\circ>$ (独异点$V=<S,\circ,e>$) 中的二元运算$\circ$是可交换的，则称V为可交换半群 (可交换独异点).

半群与独异点的实例

实例

(1) $<Z^+,+>$,$<N,+>$,$<Z,+>$,$<Q,+>$,$<R,+>$都是可交换半群，除了$<Z^+,+>$外都是可交换独异点，+是普通加法.

(2) 设 n 是大于1的正整数，$<M_n(R),\cdot>$是半群与独异点，其中 · 表示矩阵乘法.

(3) $<\Sigma^*,\circ>$是半群和独异点，其中Σ是有穷字母表，∘ 表示连接运算，幺元是空串λ.

(4) $<P(B),\oplus>$为半群与独异点，其中⊕为集合的对称差运算.

(5) $<Z_n,\oplus>$为半群与独异点，其中 $Z_n=\{0,1,\ldots,n-1\}$，⊕为模 n 加法.

元素的幂运算

设$V=\langle S, \circ\rangle$为半群，对任意 $x\in S$，规定：

$$x^1 = x$$

$$x^{n+1} = x^n \circ x \qquad\qquad n\in Z^+$$

在独异点$V=\langle S,\circ ,e\rangle$中，对任意 $x\in S$ ，规定:

$$x^0=e,$$

$$x^{n+1}=x^n\circ x \qquad\qquad n\in N$$

幂运算规则：

$$x^n \circ x^m = x^{n+m}$$

$$(x^n)^m= x^{nm} \qquad\qquad m, n\in Z^+$$

证明方法：数学归纳法

群的定义与实例

定义 设$<G,\circ>$是代数系统，$\circ$为二元运算. 如果$\circ$运算是可结合的，存在单位元 $e\in G$，并且对 G 中的任何元素 x 都有 $x^{-1}\in G$，则称 G 为 群.

群的实例

(1) $<\mathrm{Z},+>$,$<\mathrm{Q},+>$,$<\mathrm{R},+>$是群；$<\mathrm{Z}^+,+>$,$<\mathrm{N},+>$不是群.

(2) $<M_n(\mathrm{R}),+>$是群，而$<M_n(\mathrm{R}),\cdot>$不是群.

(3) $<P(B),\oplus>$是群，$\oplus$为对称差运算.

(4) $<\mathrm{Z}_n,\oplus>$，是群. $\mathrm{Z}_n=\{0,1,\ldots,n-1\}$，$\oplus$为模 n 加.

Klein四元群

设$G = \{ e, a, b, c \}$， G上的运算由下表给出，

称为 **Klein四元群**

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

运算表特征：

- 对称性---运算可交换
- 主对角线元素都是幺元
  ---每个元素是自己的逆元
- a, b, c 中任两个元素运算都等于第三个元素.

群的术语

- 若群G中的二元运算是可交换的，则称G为交换群或 阿贝尔(Abel)群
- 若群 G 是有穷集，则称 G 是有限群，否则称为无限群
- 群 G 的基数称为群G的 阶，有限群 G 的阶记作$|G|$

<Z,+> 和 <R,+>是无限群，<Z_n,⊕>是有限群，也是 n 阶群，Klein四元群 $G = \{e, a, b, c\}$是 4 阶群上述群都是交换群， n 阶 ($n\geq 2$) 实可逆矩阵集合关于矩阵乘法构成的群是非交换群.

群的术语（续）

定义 设G是群，$x\in G$，$n\in Z$，则 x 的 n 次幂 x^n 定义为

$$x^n=\begin{cases} e & n=0 \\ x^{n-1}x & n>0 \\ (x^{-1})^m & m=-n, n<0 \end{cases} \qquad n\in \mathbb{Z}$$

实例

在$<Z_3,\oplus>$中有 $2^{-3}=(2^{-1})^3=1^3=1\oplus 1\oplus 1=0$

在 $<Z,+>$ 中有 $(-2)^{-3}=2^3=2+2+2=6$

群的术语（续）

设G是群，$x \in G$，使得等式 $x^k = e$ 成立的最小正整数 k 称为 x 的阶（或周期），记作 $|x| = k$，称 x为 k 阶元. 若不存在这样的正整数 k，则称 x 为无限阶元.

在<Z_6,⊕>中，2 和 4 是 3 阶元，3 是 2 阶元，1 和 5 是 6 阶元，0 是 1 阶元

在<Z,+>中，0 是 1 阶元，其它整数的阶都不存在.

群的性质---幂运算规则

定理1 设 G 为群，则 G 中的幂运算满足：

(1) $\forall x \in G$，$(x^{-1})^{-1} = x$.

(2) $\forall x, y \in G$，$(xy)^{-1} = y^{-1}x^{-1}$.

(3) $\forall x \in G$，$x^n x^m = x^{n+m}$，$n, m \in Z$.

(4) $\forall x \in G$，$(x^n)^m = x^{nm}$，$n, m \in Z$.

注意

$(xy)^n = (xy)(xy)\ldots(xy)$, 是 n 个xy 运算，G为交换群，才有 $(xy)^n = x^n y^n$.

$$(x_1 x_2 \ldots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \ldots x_2^{-1} x_1^{-1}$$

群的性质---群方程存在唯一解

定理2 G为群，$\forall a,b\in G$，方程 $ax=b$ 和 $ya=b$ 在G中有解且仅有惟一解.

$a^{-1}b$ 是 $ax=b$的解. ba^{-1} 是 $ya=b$ 的唯一解.

例 设 $G=\langle P(\{a,b\}),\oplus\rangle$，其中$\oplus$为对称差. 群方程

$$\{a\}\oplus X=\varnothing,\qquad Y\oplus\{a,b\}=\{b\}$$

的解 $X=\{a\}^{-1}\oplus\varnothing=\{a\}\oplus\varnothing=\{a\}$,

$$Y=\{b\}\oplus\{a,b\}^{-1}=\{b\}\oplus\{a,b\}=\{a\}$$

群的性质---消去律

定理3 G 为群，则G适合消去律，即$\forall a,b,c \in G$ 有

(1) 若 $ab = ac$，则 $b = c$.

(2) 若 $ba = ca$，则 $b = c$.

例 设 $G = \{a_1, a_2, \ldots, a_n\}$ 是 n 阶群，令

$$a_iG = \{ a_i a_j \mid j = 1,2, \ldots , n \}$$

证明 $a_iG = G$.

证 由群中运算的封闭性有 $a_iG \subseteq G$. 假设$a_iG \subset G$，即 $|a_iG| < n$. 必有$a_j, a_k \in G$使得

$$a_i a_j = a_i a_k \quad (j \neq k)$$

由消去律得 $a_j = a_k$, 与 $|G| = n$ 矛盾.

群的性质---运算表排列规则

定理4 设 G 为有限群，则 G 的运算表中每行每列都是 G 中元素的一个置换，且不同的行（或列）的置换都不相同.

注意：是必要条件，用于判断一个运算表不是群.

	a	b	c	d
a	b	c	d	a
b	b	a	c	d
c	c	d	b	a
d	d	b	a	c

	a	b	c	d
a	a	b	c	d
b	c	d	a	b
c	b	c	d	a
d	d	a	b	c

子群

定义　设 G 是群，H 是 G 的非空子集，如果 H 关于 G 中的运算构成群，则称 H 是 G 的子群, 记作 $H\leq G$. 若 H 是 G 的子群，且 $H\subset G$，则称 H 是 G 的真子群，记作 $H<G$.

实例　nZ（n是自然数）是整数加群 $\langle Z,+\rangle$ 的子群. 当 $n\neq 1$ 时, nZ 是 Z 的真子群.

对任何群 G 都存在子群. G 和 $\{e\}$ 都是 G 的子群，称为 G 的平凡子群.

子群判定

判定定理

设 G 为群，H 是 G 的非空子集. H 是 G 的子群当且仅当 $\forall x, y \in H$ 有 $xy^{-1} \in H$.

设 G 为群，$a \in G$，令 $H = \{ a^k \mid k \in Z \}$，则 H 是 G 的子群，称为**由 a 生成的子群，记作 $<a>$.**

证 首先由 $a \in <a>$ 知道 $<a> \neq \varnothing$. 任取 $a^m, a^l \in <a>$,

$$a^m (a^l)^{-1} = a^m a^{-l} = a^{m-l} \in <a>$$

根据判定定理可知 $<a> \leq G$.

实例

整数加群$<Z,+>$，

由 2 生成的子群是 $<2> = \{ 2k \mid k\in Z \} = 2Z$

模 6 加群 $<Z_6,\oplus >$中

由 2 生成的子群 $<2> = \{ 0, 2, 4 \}$

Klein四元群 $G = \{ e, a, b, c \}$ 的所有生成子群是：

$<e> = \{ e \}$,

$<a> = \{ e, a \}$, $<b> = \{ e, b \}$, $<c> = \{ e, c \}$.

实例

设 G 为群, 令 $C = \{ a \mid a\in G \wedge \forall x\in G(ax=xa)\}$，则 C 是 G 的子群，称为 G 的中心.

证 $e\in C$. C是 G 的非空子集.

任取 $a, b\in C$，证明 ab^{-1}与 G 中所有的元素都可交换. $\forall x\in G$，有

$$(ab^{-1})x = ab^{-1}x = ab^{-1}(x^{-1})^{-1} = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1}$$
$$= a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$$

由判定定理可知 $C\le G$.

循环群

定义 设 G 是群，若存在 $a \in G$ 使得

$$G = \{ a^k \mid k \in Z \}$$

称 G 是循环群，记作 $G=\langle a\rangle$，称 a 为 G 的生成元.

实例： 整数加群 $G = \langle Z,+\rangle = \langle 1\rangle = \langle -1\rangle$

模 6 加群 $G = \langle Z_6,\oplus\rangle = \langle 1\rangle = \langle 5\rangle$

设 $G = \langle a\rangle$，若a 是 n 阶元，则G为 n 阶循环群，即

$$G = \{ a^0=e, a^1, a^2, \ldots , a^{n-1} \}$$

若 a 是无限阶元，则 G 为无限循环群，即

$$G = \{ a^{\pm 0}=e, a^{\pm 1}, a^{\pm 2}, \ldots \}$$

循环群的生成元

定理

设 $G = \langle a \rangle$ 是循环群.

(1) 若G是无限循环群，则 G 只有 a 和 a^{-1} 两个生成元.

(2) 若 G 是 n 阶循环群，则 a^r 是 G 的生成元当且仅当 r 是小于等于 n 且与 n 互质的正整数.

生成元的实例

(1) 设$G=\{e, a, \ldots, a^{11}\}$是12阶循环群，则小于或等于12且与12互素的数是 1, 5, 7, 11, 由定理可知 a，a^5, a^7和 a^{11}是 G 的生成元.

(2) 设$G=\langle Z_9,\oplus\rangle$是模9的整数加群，则小于或等于 9 且与 9 互素的数是 1, 2, 4, 5, 7, 8. 根据定理，G的生成元是 1, 2, 4, 5, 7 和 8.

(3) 设 $G=3Z=\{3z \mid z\in Z\}$, G上的运算是普通加法. 那么G只有两个生成元：3 和 –3.

循环群的子群

定理

设$G=\langle a\rangle$是循环群.

(1) 设$G=\langle a\rangle$是循环群，则 G 的子群仍是循环群.

(2) 若$G=\langle a\rangle$是无限循环群，则 G 的子群除$\{e\}$以外都是无限循环群.

(3) 若$G=\langle a\rangle$是 n 阶循环群，则对 n 的每个正因子 d，G 恰好含有一个d 阶子群.

子群的实例

(1) G=<Z,+>是1无限循环群，对于自然数$m\in$N，1的 m 次幂是 m，m 生成的子群是 mZ，$m\in$N. 即

$$\langle 0\rangle = \{ 0 \} = 0\mathrm{Z}$$

$$\langle m\rangle = \{ mz \mid z\in \mathrm{Z} \} = m\mathrm{Z},\quad m>0$$

(2) $G=\mathrm{Z}_{12}$是12阶循环群. 12的正因子是1, 2, 3, 4, 6 和 12，因此G 的子群是：

1 阶子群 <12>=<0>={0}，2 阶子群 <6> = {0,6}
3 阶子群 <4>={0,4,8}，4 阶子群 <3> = {0,3,6,9}
6 阶子群<2>={0,2,4,6,8,10}，12 阶子群<1> = Z_{12}

n元置换的定义

定义 设 $S = \{1, 2, \dots, n\}$, S上的双射函数 $\sigma: S \to S$ 称为 S上的 n元置换. 一般将 n 元置换σ记为

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

例如 $S = \{1, 2, 3, 4, 5\}$, 则

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

都是 5元置换.

k 阶轮换与对换

定义 设σ是 $S = \{1, 2, \ldots, n\}$上的 n 元置换. 若

$$\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ \ldots,\ \sigma(i_{k-1})=i_k,\ \sigma(i_k)=i_1$$

且保持 S 中的其他元素不变，则称σ为 S上的 k 次轮换，记作 $(i_1 i_2 \ldots i_k)$. 若 $k=2$，称σ为S上的对换.

例如 5元置换

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

分别是 4 阶和 2 阶轮换$\sigma=(1\ 2\ 3\ 4)$,$\tau=(1\ 3)$, 其中 τ 也叫做对换

n元置换分解为轮换之积

例 设 $S = \{ 1, 2, \dots , 8 \}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 2 & 6 & 7 & 5 & 3 \end{pmatrix}$$

从σ中分解出来的第一个轮换式 (1 5 2 3 6)；第二个轮换为(4)；第三个轮换为 (7 8). σ的轮换表示式

$$\sigma=(1\ 5\ 2\ 3\ 6)\ (4)\ (7\ 8)=(1\ 5\ 2\ 3\ 6)\ (7\ 8)$$

用同样的方法可以得到τ的分解式

$$\tau=(1\ 8\ 3\ 4\ 2)\ (5\ 6\ 7)$$

注意：在轮换分解式中，1 阶轮换可以省略.

n元置换的乘法与求逆

两个 n 元置换的乘法就是函数的复合运算
n 元置换的求逆就是求反函数.

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

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

$$\sigma^{-1}=\begin{pmatrix}5&3&2&1&4\\1&2&3&4&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&3&2&5&1\end{pmatrix}$$

使用轮换表示是:

$\sigma\tau = (1\ 5\ 4)\ (2\ 3)\ (1\ 4\ 2\ 3) = (1\ 5\ 2)$

$\tau\sigma = (\ 1\ 4\ 2\ 3)\ (1\ 5\ 4)\ (2\ 3) = (3\ 5\ 4)$

$\sigma^{-1}= (1\ 5\ 4)^{-1}\ (2\ 3)^{-1} = (4\ 5\ 1)\ (2\ 3) = (1\ 4\ 5)\ (2\ 3)$

n元置换群及其实例

考虑所有的 n 元置换构成的集合 S_n

S_n关于置换的乘法是封闭的．置换的乘法满足结合律. 恒等置换(1)是 S_n 中的单位元. 对于任何 n元置换 $\sigma \in S_n$，逆置换σ^{-1}是σ 的逆元．这就证明了S_n关于置换的乘法构成一个群，称为 **n元对称群**. n元对称群的子群称为 **n元置换群**.

例 设 $S = \{1, 2, 3\}$，3元对称群

$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

S_3 的运算表

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

S_3的子群

$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$,

$A_3 = \langle(1\ 2\ 3)\rangle = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$,

$\langle(1)\rangle = \{(1)\}$

$\langle(1\ 2)\rangle = \{(1), (1\ 2)\}$,

$\langle(1\ 3)\rangle = \{(1), (1\ 3)\}$,

$\langle(2\ 3)\rangle = \{(1), (2\ 3)\}$

环的定义

定义 设<R,+,·>是代数系统，+和·是二元运算.如果满足以下条件:

(1) <R,+>构成交换群

(2) <R,·>构成半群

(3) ·运算关于+运算适合分配律

则称<R,+,·>是一个环.

通常称+运算为环中的加法，· 运算为环中的乘法.
环中加法单位元记作 0, 乘法单位元(若存在)记作 1.
对任何元素 x，称 x 的加法逆元为负元，记作$-x$.
乘法逆元(若存在)称为逆元，记作 x^{-1}.

环的实例

(1) 整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为整数环Z，有理数环Q，实数环R 和 复数环C.

(2) $n(n\geq 2)$阶实矩阵的集合$M_n(\mathrm{R})$关于矩阵的加法和乘法构成环，称为n阶实矩阵环.

(3) 集合的幂集$P(B)$关于集合的对称差运算和交运算构成环.

(4) 设$\mathrm{Z}_n=\{0,1,\ldots,n-1\}$，$\oplus$和$\otimes$分别表示模$n$的加法和乘法，则$<\mathrm{Z}_n,\oplus,\otimes>$构成环，称为模$n$的整数环.

环中的零因子

设$<R,+,\cdot>$是环，若存在 $ab=0$, 且 $a\neq 0$, $b\neq 0$, 称 a 为左零因子，b为右零因子.

实例

$<Z_6,\oplus,\otimes>$，其中 $2\otimes 3=0$，2 和 3 都是零因子.

无零因子的条件：$ab = 0 \rightarrow a=0 \vee b=0$

可证明无零因子的充要条件是：乘法满足消去律

特殊的环

定义 设<R,+,·>是环，

(1) 若环中乘法·适合交换律，则称 R是交换环.

(2) 若环中乘法·存在单位元，则称 R是含幺环.

(3) 若$\forall a, b \in R$，$a\,b=0 \Rightarrow a=0 \vee b=0$，则称$R$是无零因子环.

(4) 若 R 既是交换环、含幺环，也是无零因子环，则称 R 是整环.

(5) 若 R为整环，$|R|>1$, 且$\forall a \in R^*=R-\{0\}$，$a^{-1} \in R$, 则称 R 为域.

特殊环的实例

(1)整数环Z、有理数环Q、实数环R、复数环C都是交换环、含幺环、无零因子环和整环. 其中除Z之外都是域

(2)令$2Z=\{ 2z \mid z\in Z \}$，则$<2Z,+,\cdot>$构成交换环和无零因子环. 但不是含幺环和整环.

(3)设$n\in Z$, $n\geq 2$, 则 n 阶实矩阵的集合 $M_n(R)$关于矩阵加法和乘法构成环，它是含幺环，但不是交换环和无零因子环，也不是整环.

(4)$<Z_6,\oplus,\otimes>$构成环，它是交换环、含幺环，但不是无零因子环和整环.

注意：对于一般的 n, Z_n是整环且是域 $\Leftrightarrow$ n是素数.

例题

判断下列集合和给定运算是否构成环、整环和域.

(1) $A=\{a+bi \mid a,b\in\mathbb{Q}\}$, $i^2=-1$, 运算为复数加法和乘法.

(2) $A=\{2z+1 \mid z\in\mathbb{Z}\}$, 运算为普通加法和乘法

(3) $A=\{2z \mid z\in\mathbb{Z}\}$, 运算为普通加法和乘法

(4) $A=\{x \mid x\geq 0 \wedge x\in\mathbb{Z}\}$, 运算为普通加法和乘法.

(5) $A=\{a+b\sqrt[4]{5} \mid a,b\in\mathbb{Q}\}$, 运算为普通加法和乘法

解 (2), (4), (5) 不是环. 为什么?

(1) 是环, 是整环, 也是域.

(3) 是环, 不是整环和域.

环的性质

定理 设 $<R,+,\cdot>$ 是环，则

(1) $\forall a \in R$， $a\cdot 0 = 0\cdot a = 0$

(2) $\forall a,b \in R$， $(-a)b = a(-b) = -ab$

(3) $\forall a,b \in R$， $(-a)(-b) = ab$

(4) $\forall a,b,c \in R$， $a(b-c) = ab-ac$， $(b-c)a = ba-ca$

例 在环中计算 $(a+b)^3, (a-b)^2$

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

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

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

格的定义

定义 设$<S,\preccurlyeq>$是偏序集，如果$\forall x,y\in S$，$\{x,y\}$都有最小上界和最大下界，则称S关于偏序$\preccurlyeq$作成格.

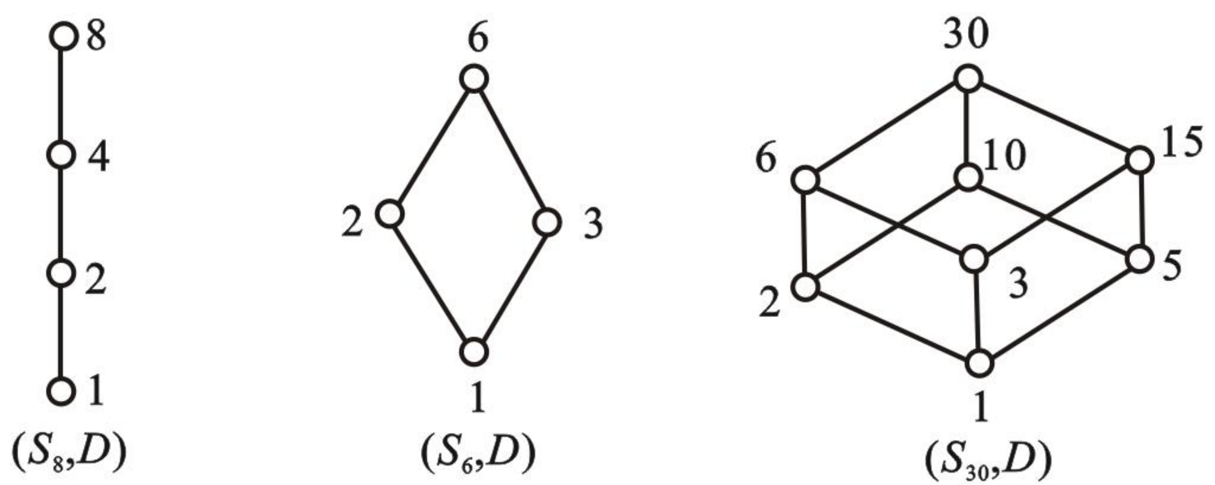
由于最小上界和最大下界的唯一性，可以把求$\{x,y\}$的最小上界和最大下界看成x与y的二元运算$\vee$和$\wedge$，即$x\vee y$和$x\wedge y$分别表示x与y的最小上界和最大下界.

注意：这里出现的$\vee$和$\wedge$符号只代表格中的运算，而不再有其他的含义.

格的实例

例 设n是正整数，S_n是n的正因子的集合. D为整除关系，则偏序集$<S_n,D>$构成格.$\forall x,y\in S_n$，$x\vee y$ 是 lcm(x,y)，即 x 与 y 的最小公倍数. $x\wedge y$ 是 gcd(x,y)，即 x 与 y 的最大公约数.

下图给出了格$<S_8,D>$，$<S_6,D>$和$<S_{30},D>$.



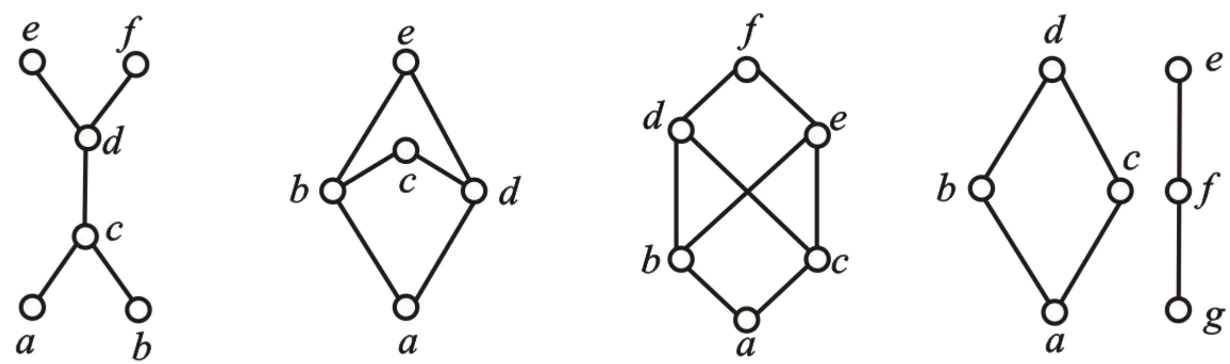
格的实例（续）

例 判断下列偏序集是否构成格，并说明理由.

(1) $<P(B),\subseteq>$，其中$P(B)$是集合B的幂集.

(2) $<Z,\leq>$，其中Z是整数集，$\leq$为小于等于关系.

(3) 偏序集的哈斯图分别在下图给出.



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

解 (1) 是格. 称$<P(B),\subseteq>$为B的幂集格.

(2) 是格.

(3) 都不是格.

格的性质：对偶原理

定义 设 f 是含有格中元素以及符号=,≼ ,≽ ,∨和∧的命题. 令 f^*是将 f 中的≼ 替换成≽ ,≽ 替换成≼ ,∨替换成∧,∧替换成∨所得到的命题. 称 f^* 为 f 的对偶命题.

例如, 在格中： f 是 $(a\vee b)\wedge c \preccurlyeq c$, f^* 是 $(a\wedge b)\vee c \succcurlyeq c$.

格的对偶原理：设 f 是含格中元素以及符号=,≼ ,≽ ,∨和∧等的命题. 若 f 对一切格为真, 则 f 的对偶命题 f^*也对一切格为真.

例如, 若对一切格L都有 $\forall a,b\in L$, $a\wedge b\preccurlyeq a$，那么对一切格L都有 $\forall a,b\in L$, $a\vee b\succcurlyeq a$

格的性质：算律

定理 设$<L, \preccurlyeq>$是格,则运算$\vee$和$\wedge$适合交换律、结合律、幂等律和吸收律,即

(1) $\forall a,b\in L$ 有

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

(2) $\forall a,b,c\in L$ 有

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

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

(3) $\forall a\in L$ 有

$$a\vee a=a,\qquad a\wedge a=a$$

(4) $\forall a,b\in L$ 有

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

算律的证明

证　(1) 交换律.

$a \vee b$ 是 $\{a,b\}$ 的最小上界

$b \vee a$ 是 $\{b,a\}$的最小上界

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

$\Rightarrow a \vee b = b \vee a.$

由对偶原理, $a \wedge b = b \wedge a$ 得证.

算律的证明（续）

(2) 结合律. 由最小上界的定义有

$$(a\vee b)\vee c \geqslant a\vee b \geqslant a \qquad \text{(I)}$$

$$(a\vee b)\vee c \geqslant a\vee b \geqslant b \qquad \text{(II)}$$

$$(a\vee b)\vee c \geqslant c \qquad \text{(III)}$$

由式 (II) 和 (III) 有

$$(a\vee b)\vee c \geqslant b\vee c \qquad \text{(IV)}$$

由式 (I) 和 (IV) 有 $(a\vee b)\vee c \geqslant a\vee(b\vee c)$. 同理可证 $(a\vee b)\vee c \leqslant a\vee(b\vee c)$. 根据偏序的反对称性得到 $(a\vee b)\vee c = a\vee(b\vee c)$. 由对偶原理，$(a\wedge b)\wedge c = a\wedge(b\wedge c)$ 得证.

算律的证明（续）

(3) 幂等律. 显然 $a \leqslant a \vee a$, 又由 $a \leqslant a$ 得 $a \vee a \leqslant a$.

由反对称性 $a \vee a = a$. 用对偶原理, $a \wedge a = a$ 得证.

(4) 吸收律. 显然有

$$a \vee (a \wedge b) \geqslant a \qquad \text{(V)}$$

由 $a \leqslant a$, $a \wedge b \leqslant a$ 可得

$$a \vee (a \wedge b) \leqslant a \qquad \text{(VI)}$$

由式 (V) 和 (VI) 可得 $a \vee (a \wedge b) = a$

根据对偶原理, $a \wedge (a \vee b) = a$ 得证.

格作为代数系统的定义

定理 设 $<S,*,\circ>$ 是具有两个二元运算的代数系统,若对于 $*$ 和 $\circ$ 运算适合交换律、结合律、吸收律,则可以适当定义 S 中的偏序 $\preccurlyeq$,使得 $<S,\preccurlyeq>$ 构成格,且 $\forall a,b\in S$ 有 $a\wedge b = a*b$, $a\vee b = a\circ b$.

根据定理,可以给出格的另一个等价定义.

定义 设 $<S,*,\circ>$ 是代数系统, $*$ 和 $\circ$ 是二元运算,如果 $*$ 和 $\circ$ 运算满足交换律、结合律和吸收律,则 $<S,*,\circ>$ 构成格.

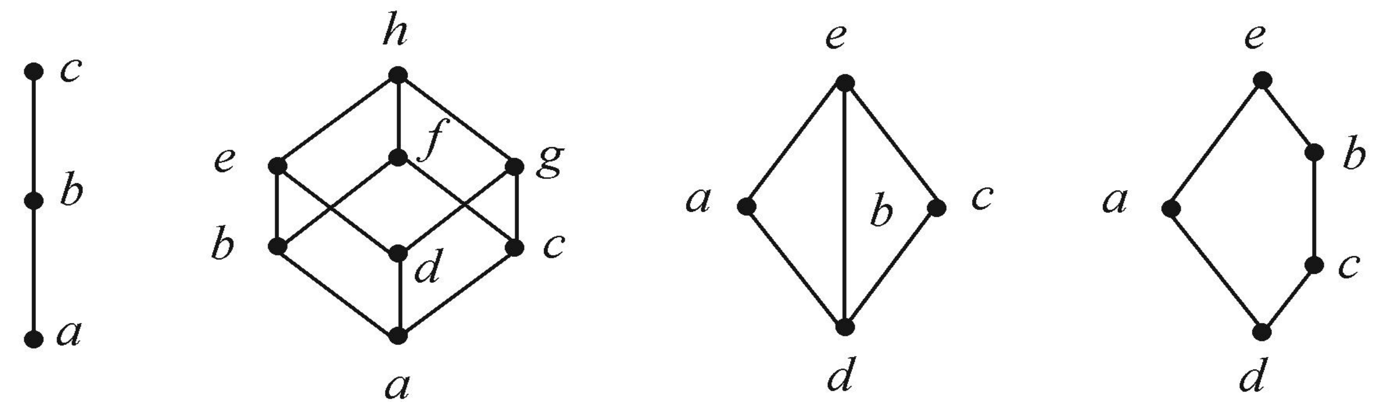
分配格定义

定义 设$<L,\wedge,\vee>$是格, 若$\forall a, b, c \in L$, 有

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

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

则称 L 为分配格.



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

(a)和(b)是分配格，(c)和(d)不是分配格.

全上界与全下界

定义 设L是格，若存在 $a\in L$ 使得 $\forall x\in L$ 有 $a\preccurlyeq x$, 则称 a 为 L 的全下界；若存在 $b\in L$ 使得 $\forall x\in L$ 有 $x\preccurlyeq b$, 则称 b 为 L 的全上界.

说明： 格 L 若存在全下界或全上界,一定是唯一的.
一般将格 L 的全下界记为 0, 全上界记为 1.

定义 设 L是格,若 L存在全下界和全上界, 则称 L为有界格, 有界格 L 记为 $<L,\wedge,\vee,0,1>$.

注意：有限格 $L=\{a_1,a_2,\ldots,a_n\}$是有界格，求对偶命题时, 必须将0与1互换.

补元的定义

定义

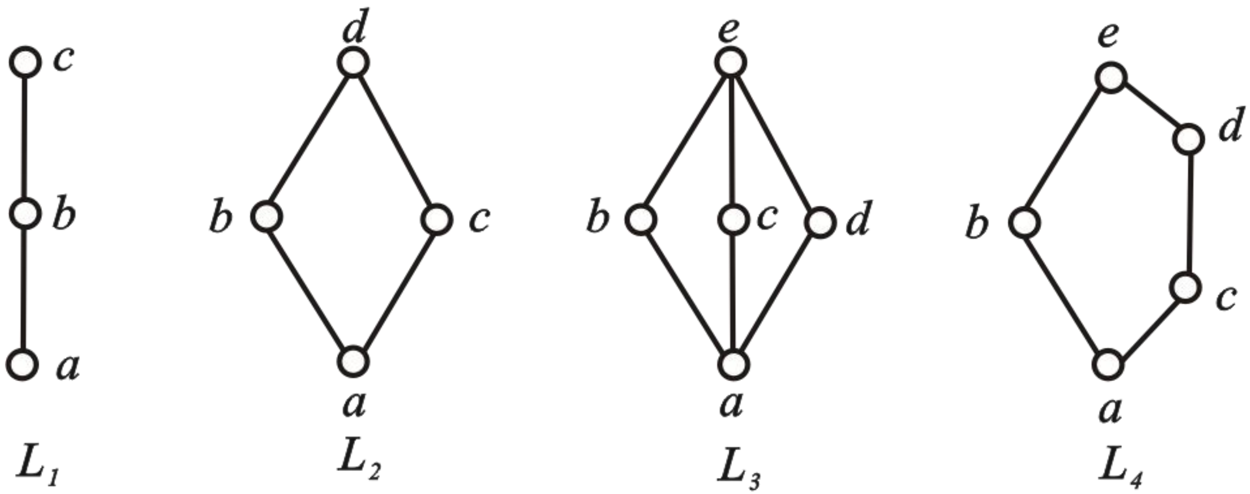
设$<L,\wedge,\vee,0,1>$是有界格, $a\in L$, 若存在 $b\in L$ 使得 $a\wedge b = 0$ 和 $a\vee b =1$ 成立, 则称 b 是 a 的补元.

注意:

若 b 是 a 的补元, 则 a 也是 b 的补元. a 和 b互为补元.

设$<L,\wedge,\vee,0,1>$是有界分配格. 若L中元素 a 存在补元, 则存在惟一的补元.

实例: 求补元



解：L_1中 a, c互补, b没补元.

L_2中 a, d互补, b, c 互补.

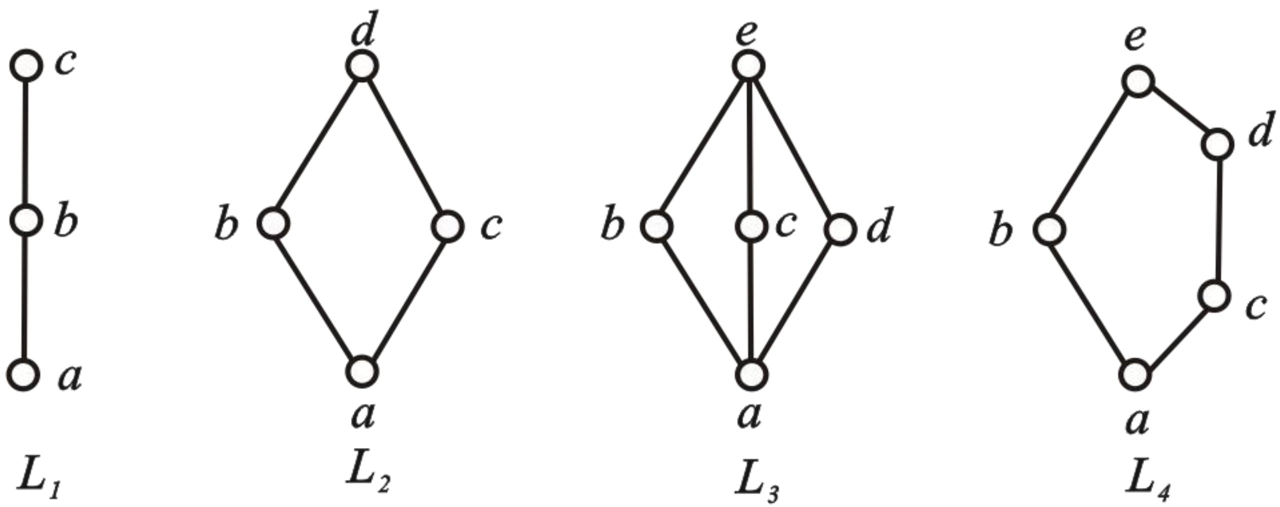
L_3中 a,e互补, b 的补元是 c和d, c 的补元是 b和d, d 的补元是b和c.

L_4中的 a,e互补, b 的补元是 c和d, c 的补元是b, d 的补元是 b.

有补格的定义

定义 设$<L,\wedge,\vee,0,1>$是有界格, 若 L 中所有元素都有补元存在, 则称 L 为有补格.

例如, 下图中的 L_2, L_3和 L_4是有补格, L_1不是有补格.



布尔代数的定义

定义 有补分配格, 称为布尔格或布尔代数.

求补元的运算看作是布尔代数中的一元运算.布尔代数标记为$<B,\wedge,\vee,',0,1>$, 其中’为求补运算

例 设 $S_{110}=\{1, 2, 5, 10, 11, 22, 55, 110\}$ 是110的正因子集合.

gcd 表示求最大公约数的运算

lcm表示求最小公倍数的运算.

则 $<S_{110}$, gcd, lcm$>$是否构成布尔代数?

布尔代数的性质

定理 设$<B, \wedge, \vee, ', 0, 1>$是布尔代数,则

(1) $\forall a \in B, (a')' = a$.

(2) $\forall a, b \in B,$

(3) $(a \wedge b)' = a' \vee b', (a \vee b)' = a' \wedge b'$ （德摩根律）

注意：德摩根律对有限个元素也是正确的.

证明

证 (1) $(a')'$是 a'的补元. A 是 a' 的补元. 由补元惟一性得 $(a')'=a$.

(2) 对任意 $a, b\in B$有

$$(a\wedge b)\vee(a'\vee b') = (a\vee a'\vee b')\wedge(b\vee a'\vee b')$$
$$= (1\vee b')\wedge(a'\vee 1) = 1\wedge 1 = 1,$$
$$(a\wedge b)\wedge(a'\vee b') = (a\wedge b\wedge a')\vee(a\wedge b\wedge b')$$
$$= (0\wedge b)\vee(a\wedge 0) = 0\vee 0 = 0.$$

所以 $a'\vee b'$是 $a\wedge b$ 的补元, 根据补元惟一性可得

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

同理可证 $(a\vee b)' = a'\wedge b'$.

有限布尔代数的表示定理

定理 设 L 是有限布尔代数，则 L 含有 2^n 个元素 $(n\in N)$，且 L 与 $<P(S),\cap,\cup,\sim,\varnothing,S>$ 同构，其中 S 是一个 n 元集合.

结论：含有 2^n 个元素的布尔代数在同构意义下只有一个.