

§ 7.3 几个典型的代数系统

一、半群的概念

半群：设 $V = \langle S, \circ \rangle$ 是代数系统， $\circ$ 是二元运算。

如果 $\circ$ 在 S 上是可结合的，则称 V 为半群。

即对 $\forall x, y, z \in S$ ，有 $(x \circ y) \circ z = x \circ (y \circ z)$ 。

如： $\langle \mathbb{Z}^+, + \rangle$, $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R}, \times \rangle$, $\langle M_n(\mathbb{R}), \bullet \rangle$,
 $\langle P(S), \cup \rangle$, $\langle P(S), \cap \rangle$, $\langle P(S), \oplus \rangle$, $\langle \mathbb{Z}_n, \oplus \rangle$ 都是半群，
但 $\langle \mathbb{Z}, - \rangle$ 不是半群。



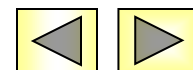
§ 7.3 几个典型的代数系统

含幺半群（独异点）：如果半群 $V = \langle S, \circ \rangle$ 的二元运算 $\circ$ 含有幺元，则称 V 为含幺半群(独异点)。

即 $\exists e \in S$ ，使得对 $\forall x \in S$ 都有 $e \circ x = x \circ e = x$ 。

独异点亦可记为 $\langle S, \circ, e \rangle$ 。

如： $\langle \mathbb{N}, +, 0 \rangle$, $\langle \mathbb{Z}, +, 0 \rangle$, $\langle \mathbb{R}, \times, 1 \rangle$, $\langle M_n(\mathbb{R}), \cdot, E \rangle$,
 $\langle P(S), \cup, \emptyset \rangle$, $\langle P(S), \cap, S \rangle$, $\langle P(S), \oplus, \emptyset \rangle$, $\langle \mathbb{Z}_n, \oplus, 0 \rangle$
都是独异点，但 $\langle \mathbb{Z}^+, + \rangle$ 不是独异点。

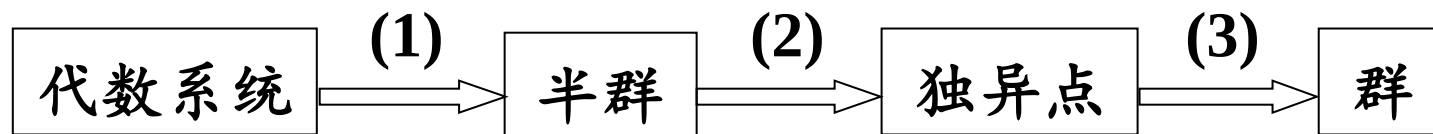


§ 7.3 几个典型的代数系统

二、群的概念

群： 设 $V = \langle G, \circ \rangle$ 是代数系统， $\circ$ 是二元运算。
如果 $\circ$ 在 G 上是可结合的，存在幺元 $e \in G$ ，
并且 G 中的任意元素 x 都有 $x^{-1} \in G$ ，
则称 $V = \langle G, \circ \rangle$ 为群。

如： $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R} - \{0\}, \times \rangle$, $\langle P(S), \oplus \rangle$, $\langle \mathbb{Z}_n, \oplus \rangle$ 是群，
但 $\langle \mathbb{N}, + \rangle$, $\langle M_n(\mathbb{R}), \cdot \rangle$ 不是。





§ 7.3 几个典型的代数系统

有限群： G 为有限集的群 $\langle G, \circ \rangle$ 称为有限群，
否则称为无限群。

$|G|$ 为 **有限群的阶**。

如： $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R} - \{0\}, \times \rangle$ 为无限群， $\langle \mathbb{Z}_n, \oplus \rangle$ 为有限群。

交换群： 若群 $\langle G, \circ \rangle$ 中的二元运算 $\circ$ 是可交换的，
则称群 $\langle G, \circ \rangle$ 为交换群，也称**阿贝尔群**。

如： $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R} - \{0\}, \times \rangle$, $\langle P(S), \oplus \rangle$, $\langle \mathbb{Z}_n, \oplus \rangle$ 都是
阿贝尔群。



§ 7.3 几个典型的代数系统

例8：设 $G = \{e, a, b, c\}$, $\circ$ 为 G 上的二元运算，运算表如下：

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

集合 G 对运算 $\circ$ 封闭

运算 $\circ$ 满足结合律

e 为幺元

每个元素的逆元为自身

称群 $\langle G, \circ \rangle$ 为 **Klein四元群**。



§ 7.3 几个典型的代数系统

证明结合律:对 $\forall x, y, z \in G$ 都有 $(x \circ y) \circ z = x \circ (y \circ z)$

1)若上式 x, y, z 中有一元素为 e , $(e \circ y) \circ z = y \circ z = e \circ (y \circ z),$

$$(x \circ e) \circ z = x \circ z = x \circ (e \circ z), \quad (x \circ y) \circ e = x \circ y = x \circ (y \circ e)$$

2)若上式 x, y, z 中无元素 e , 但三个元素都相等。

$$(x \circ x) \circ x = x \circ (x \circ x)$$

3)若上式 x, y, z 中无元素 e , 但存在某两个元素相等。

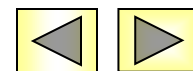
$$\text{当 } x = y, \quad (x \circ x) \circ z = e \circ z = z, \quad x \circ (x \circ z) = x \circ t = z$$

$$\text{当 } x = z, \quad (x \circ y) \circ x = t \circ x = y, \quad x \circ (y \circ x) = x \circ t = y$$

$$\text{当 } y = z, \quad (x \circ y) \circ y = t \circ y = x, \quad x \circ (y \circ y) = x \circ e = x$$

4)若上式 x, y, z 中无元素 e , 且任意两个元素都不相等。

$$(x \circ y) \circ z = z \circ z = e, \quad x \circ (y \circ z) = x \circ x = e$$



§ 7.3 几个典型的代数系统

群中的幂：设群 $\langle G, \circ \rangle$ ，则对 $\forall x \in G$ ，

$$x^0 = e, \quad x^{n+1} = x^n \circ x, \quad (n \text{ 为非负整数})$$

$$x^{-n} = (x^{-1})^n, \quad (n \text{ 为正整数})$$

幂运算的性质：

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

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

$$(3) \quad \forall x \in G, \quad x^m \circ x^n = x^{m+n}, \quad m, n \text{ 为整数}$$

$$(4) \quad \forall x \in G, \quad (x^m)^n = x^{mn}, \quad m, n \text{ 为整数}$$



§ 7.3 几个典型的代数系统

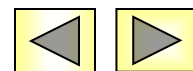
三、子群的概念

子群： 设 $\langle G, \circ \rangle$ 为群， H 是 G 的非空子集，如果 H 关于 G 中的运算 $\circ$ 构成群，则称 $\langle H, \circ \rangle$ 为 $\langle G, \circ \rangle$ 的子群。记作 $H \leq G$

如： $\langle n\mathbb{Z}, + \rangle$ 是 $\langle \mathbb{Z}, + \rangle$ 的子群，其中 $\langle \{0\}, + \rangle$ 和 $\langle \mathbb{Z}, + \rangle$ 是 $\langle \mathbb{Z}, + \rangle$ 的平凡子群；

又如： *Klein* 四元群 $\langle \{e, a, b, c\}, \circ \rangle$ ，有5个子群：

$\langle \{e\}, \circ \rangle$ 、 $\langle \{e, a\}, \circ \rangle$ 、 $\langle \{e, b\}, \circ \rangle$ 、 $\langle \{e, c\}, \circ \rangle$ 和 $\langle \{e, a, b, c\}, \circ \rangle$ ，其中 $\langle \{e\}, \circ \rangle$ 和 $\langle \{e, a, b, c\}, \circ \rangle$ 是 $\langle \{e, a, b, c\}, \circ \rangle$ 的平凡子群。



§ 7.3 几个典型的代数系统

子群的判定定理

设 $\langle G, \circ \rangle$ 为群, H 是 G 的非空子集, 如果对 $\forall x, y \in H, x \circ y^{-1} \in H$, 则 $\langle H, \circ \rangle$ 是 $\langle G, \circ \rangle$ 的子群。

例9: $\langle G, \circ \rangle$ 为群, 对 $\forall x \in G$, 令 $H = \{ x^k \mid k \in \mathbb{Z} \}$, 则 $\langle H, \circ \rangle$ 是 $\langle G, \circ \rangle$ 的子群。

称为由元素 x 生成的子群, 记作 $H = \langle x \rangle$ 。

如: 群 $\langle \mathbb{Z}_6, \oplus \rangle$, $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6$, $\langle 2 \rangle = \{0, 2, 4\}$, $\langle 3 \rangle = \{0, 3\}$, $\langle 4 \rangle = \langle 2 \rangle$, $\langle 5 \rangle = \langle 1 \rangle$ 。





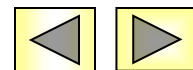
§ 7.3 几个典型的代数系统

四、两种常用的群

1、循环群：

元素的阶(周期)： 设群 $\langle G, \circ \rangle$, $a \in G$, 使 $a^k = e$ 成立的最小正整数 k 称为 a 的阶(周期)。

如：任何群的幺元 e 的阶都为1, *Klein*四元群中 a, b, c 的阶都是2, 群 $\langle \mathbb{Z}_6, \oplus \rangle$ 中2和4的阶是3, 3的阶是2, 1和5的阶是6。



§ 7.3 几个典型的代数系统

循环群： 设群 $\langle G, \circ \rangle$ ，如果 $\exists a \in G$ ，使得

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

则称为循环群，记 $G = \langle a \rangle$ ，

称 a 为循环群 $\langle G, \circ \rangle$ 的生成元。

如：群 $\langle \mathbb{Z}, + \rangle$ 是循环群，其生成元是1或-1，

群 $\langle \mathbb{Z}_6, \oplus \rangle$ 是循环群，其生成元是1或5。

性质： 循环群一定是阿贝尔群，但阿贝尔群不一定是循环群。





§ 7.3 几个典型的代数系统

无限阶循环群 $G = \langle a \rangle$ 的生成元就是 a 和 a^{-1} ,
 n 阶循环群 $G = \langle a \rangle$ 的生成元是 a^t (其中 t 与 n 互质)。

循环群的子群仍是循环群。

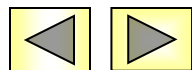
n 阶循环群 $G = \langle a \rangle$ 的子群的阶都是 n 的因子。

对于 n 的每个正因子 d , $a^{n/d}$ 是 G 的 d 阶子群的生成元。

如: 群 $\langle \mathbb{Z}_6, \oplus \rangle$ 中, $\mathbb{Z}_6 = \langle 1 \rangle$, 6 的正因子是 1, 2, 3, 6,

子群有 $\langle 1^6 \rangle = \langle 0 \rangle = \{0\}$, $\langle 1^3 \rangle = \langle 3 \rangle = \{0, 3\}$,

$\langle 1^2 \rangle = \langle 2 \rangle = \{0, 2, 4\}$, $\langle 1^1 \rangle = \langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$ 。



§ 7.3 几个典型的代数系统

2、置换群：

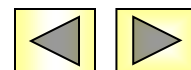
n 元置换： 设 $S = \{1, 2, \dots, n\}$, S 上的任何双射函数

$\sigma: S \rightarrow S$ 构成了 S 上 n 个元素的置换,

称为 n 元置换。记作：
$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

如： $S = \{1, 2, 3\}$, 令 $\sigma: S \rightarrow S$ 且 $\sigma(1) = 2$, $\sigma(2) = 3$,

$\sigma(3) = 1$, 则有一个置换：
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$



§ 7.3 几个典型的代数系统

任何 n 元置换都可以用不交的轮换之积来表示。

如：置换 $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 4 & 1 \end{pmatrix}$ ，

则可表示为 $\sigma_1 = (1\ 3\ 2\ 5\ 4\ 6)$

又如：置换 $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$ ，

则可表示为 $\sigma_2 = (1\ 3\ 2\ 5)(4\ 6)$

又如：置换 $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$ ，

则可表示为 $\sigma_3 = (1\ 3\ 2)(4)(5\ 6) = (1\ 3\ 2)(5\ 6)$



§ 7.3 几个典型的代数系统

例10: 将置换 σ_1 和 σ_2 表成不交的轮换之积,
并求 $\sigma_1 \circ \sigma_2$ 和 $\sigma_2 \circ \sigma_1$,

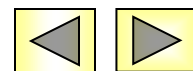
$$\text{其中 } \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}.$$

$$\text{解: } \sigma_1 = (1\ 4\ 5\ 2\ 3), \quad \sigma_2 = (1\ 3\ 2)(4\ 5),$$

$$\sigma_1 \circ \sigma_2 = (1)(2\ 4)(3)(5), \quad \sigma_2 \circ \sigma_1 = (1\ 5)(2)(3)(4),$$

恒等置换: 称 $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ 为恒等置换。记作: I_s

当 $|S| = n$ 时, S 上共有 $n!$ 种不同的 n 元置换, 将这些置换构成的集合记作 S_n 。



§ 7.3 几个典型的代数系统

对于代数系统 $\langle S_n, \circ \rangle$, $\circ$ 是函数的合成运算, 则:

(1) 集合 S_n 对运算 $\circ$ 封闭, 且 $\circ$ 是可结合的。

(2) I_s 是集合 S_n 关于 $\circ$ 运算的么元。

(3) 任何置换 $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ 的逆置换

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix} \text{ 就是 } \sigma \text{ 的逆元。}$$

因此, $\langle S_n, \circ \rangle$ 构成一个群, 称为对称群。

$\langle S_n, \circ \rangle$ 的任何子群则称为置换群。





§ 7.3 几个典型的代数系统

五、格的基本概念和性质

格： 设 $\langle S, \leq \rangle$ 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 $\langle S, \leq \rangle$ 是一个格。

通常记： $\{x, y\}$ 的最小上界为 $x \vee y$

$\{x, y\}$ 的最大下界为 $x \wedge y$





§ 7.3 几个典型的代数系统

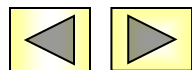
例11: 设 n 为正整数, S_n 是 n 的正因子的集合, R 为整除关系, 验证 $\langle S_n, R \rangle$ 是格, 并举例说明。

解: 因为 $\langle S_n, R \rangle$ 是自反的, 反对称的, 传递的, 从而是偏序集;

对于 $\forall x, y \in S_n$, x 与 y 的最小公倍数 $[x, y]$ 属于 S_n ,
 x 与 y 的最大公约数 (x, y) 属于 S_n ,

且 $x \vee y = [x, y]$, $x \wedge y = (x, y)$ 。

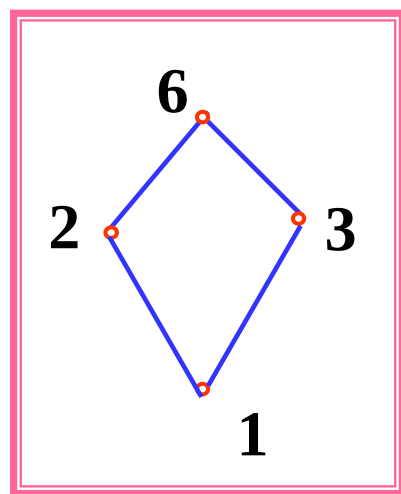
因此, $\langle S_n, R \rangle$ 是一个格。



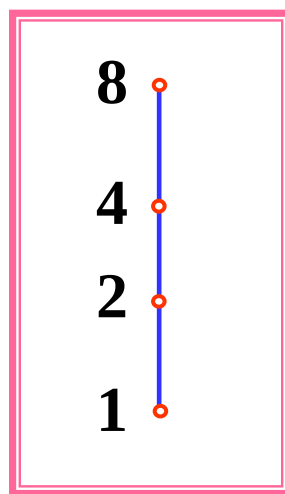
§ 7.3 几个典型的代数系统

例11: 设 n 为正整数, S_n 是 n 的正因子的集合, R 为整除关系, 验证 $\langle S_n, R \rangle$ 是格, 并举例说明。

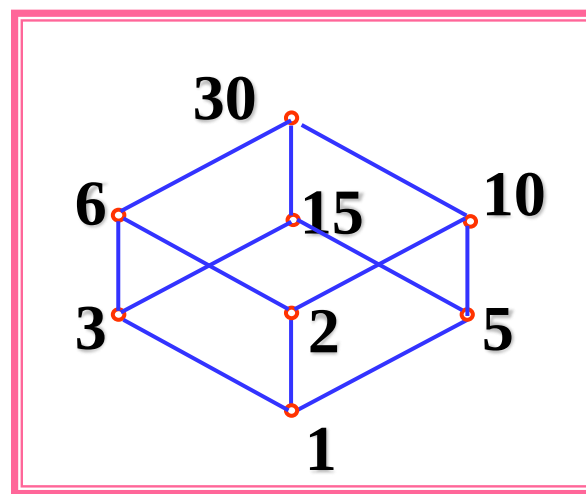
解: 如当 $n = 6, 8, 30$ 时, 分别有下图:



$\langle S_6, R \rangle$



$\langle S_8, R \rangle$

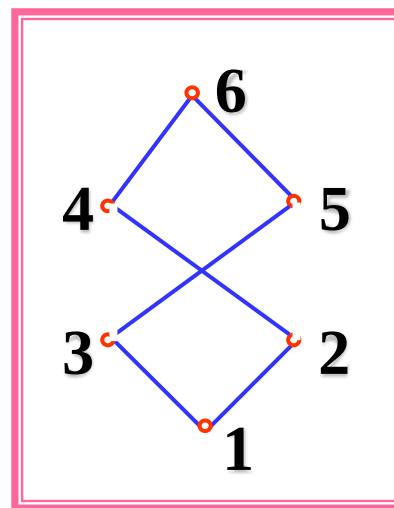
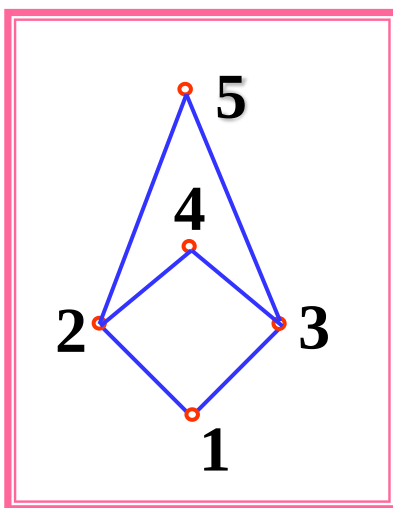
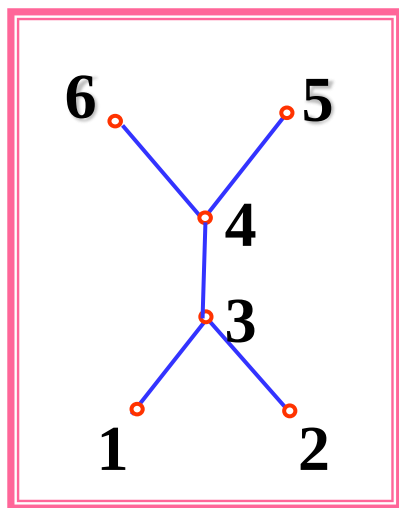


$\langle S_{30}, R \rangle$



§ 7.3 几个典型的代数系统

例12：判断下列偏序集是否构成格，说明原因。

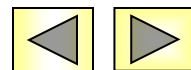


§ 7.3 几个典型的代数系统

格的另一个等价定义：

格： 设 $\langle L, \wedge, \vee \rangle$ 是代数系统， $\wedge$ 和 $\vee$ 是二元运算，若 $\wedge$ 和 $\vee$ 运算满足交换律，结合律和吸收律，则称 $\langle L, \wedge, \vee \rangle$ 是一个格。

子格： 设 $\langle L, \wedge, \vee \rangle$ 是格， S 是 L 的非空子集，若 S 关于运算 $\wedge$ 和 $\vee$ 是封闭的，则称 $\langle S, \wedge, \vee \rangle$ 是格 $\langle L, \wedge, \vee \rangle$ 的子格。

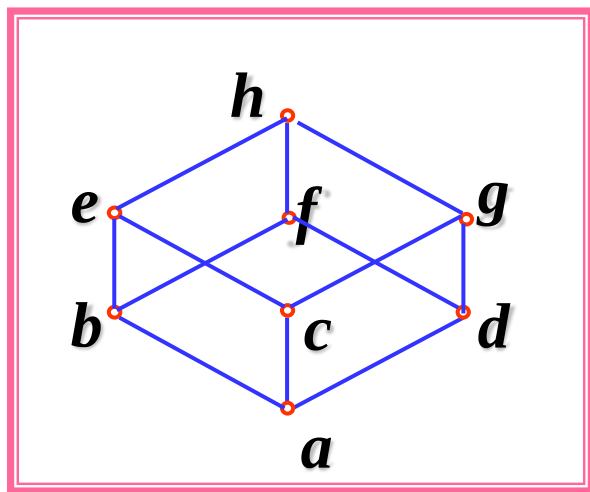


§ 7.3 几个典型的代数系统

例13: 格 $\langle L, \wedge, \vee \rangle$ 如图, $\langle S_i, \wedge, \vee \rangle$ 是否构成其子格。

其中 $S_1 = \{a, e, g, h\}$, $S_2 = \{a, c, e, h\}$,

$S_3 = \{a, b, d, f, h\}$



$\langle S_1, \wedge, \vee \rangle$ 不是子格,

$\langle S_2, \wedge, \vee \rangle$ 是子格,

$\langle S_3, \wedge, \vee \rangle$ 是子格,

§ 7.3 几个典型的代数系统

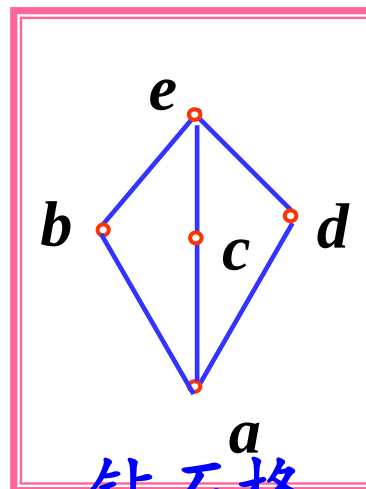
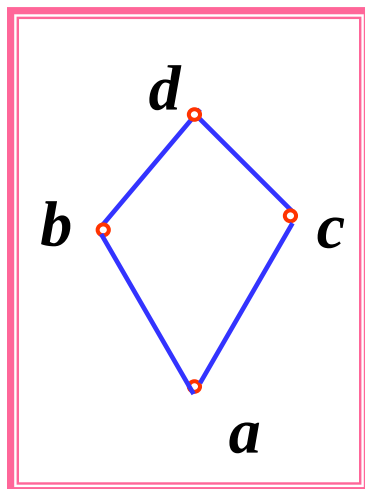
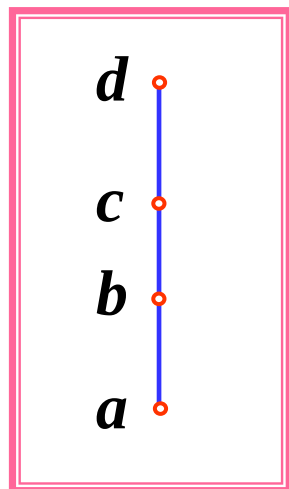
六、特殊的格

1、**分配格**：设 $\langle L, \wedge, \vee \rangle$ 是格，若对 $\forall a, b, c \in L$ 有

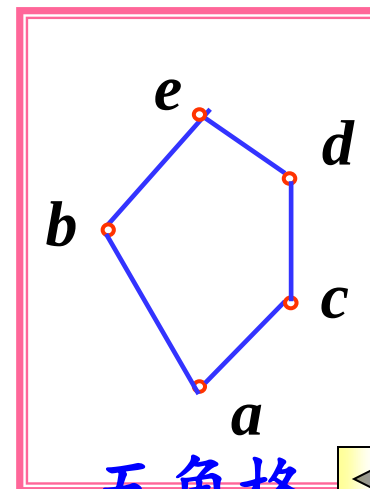
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

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

成立，则称 $\langle L, \wedge, \vee \rangle$ 为分配格。



钻石格



五角格

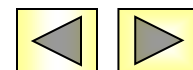
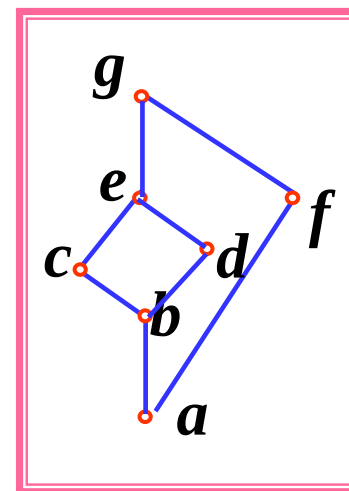
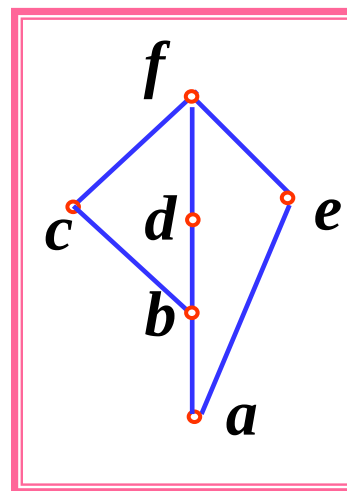
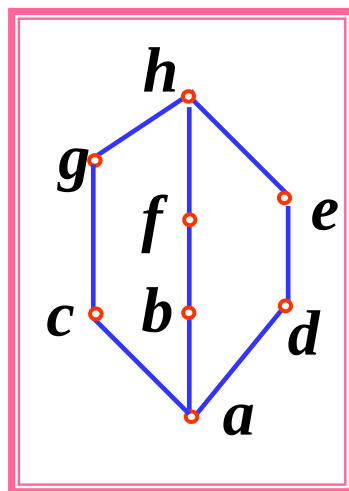
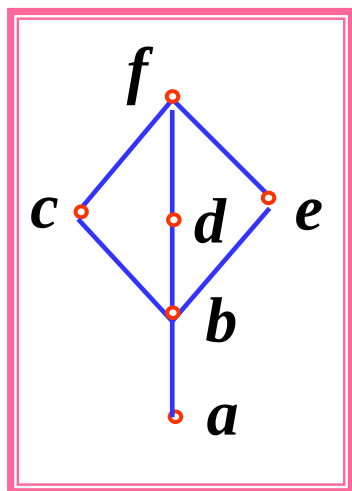


§ 7.3 几个典型的代数系统

分配格的判定定理

格 $\langle L, \wedge, \vee \rangle$ 是分配格当且仅当它不含有与五角格或钻石格同构的子格。

例14：判断下列格是否为分配格。



§ 7.3 几个典型的代数系统

2、有界格:

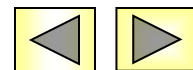
全下界(或全上界): 设 $\langle L, \wedge, \vee \rangle$ 为格,
若存在 $a \in L$, 对 $\forall b \in L$ 有 $a \leq b$ (或 $a \geq b$),
则称 a 为格 $\langle L, \wedge, \vee \rangle$ 的全下界(全上界)。

记全下界为0, 全上界为1。

有界格: 具有全上界和全下界的格。

记作 $\langle L, \wedge, \vee, 0, 1 \rangle$ 。

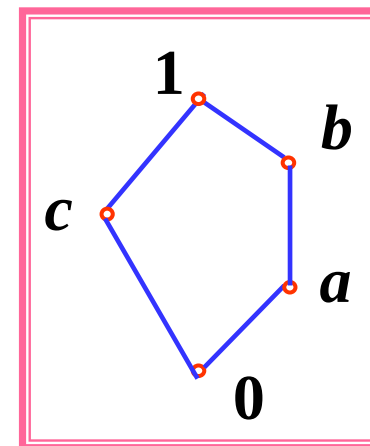
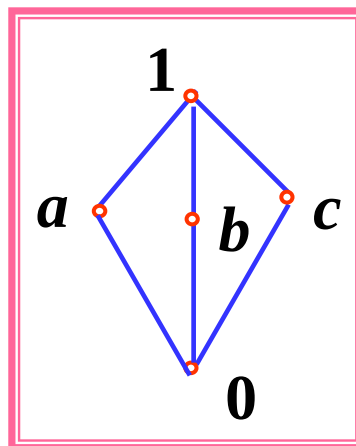
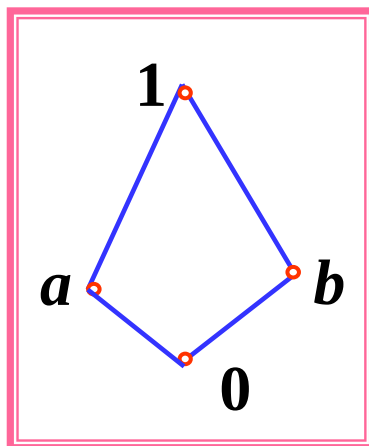
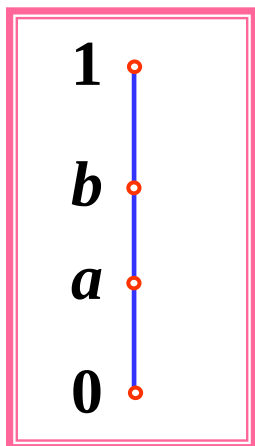
所有的有限元的格都是有界格。



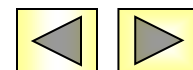
§ 7.3 几个典型的代数系统

3、有补格:

补元: 设 $\langle L, \wedge, \vee, 0, 1 \rangle$ 是有界格, $a \in L$, 若 $\exists b \in L$, 使得 $a \wedge b = 0$, $a \vee b = 1$, 则称 b 为 a 的补元。



补元可能存在或不存在, 存在亦可能不唯一。

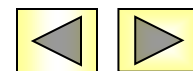


§ 7.3 几个典型的代数系统

有补格： 设 $\langle L, \wedge, \vee, 0, 1 \rangle$ 是有界格，
若对 $\forall a \in L$ ，在 L 中都存在 a 的补元，
则称 $\langle L, \wedge, \vee, 0, 1 \rangle$ 是有补格。

定理 设 $\langle L, \wedge, \vee, 0, 1 \rangle$ 是分配格，若 $a \in L$ 存在补元，
则 a 的补元是唯一的。记为 a'

证明：设 a 有两个补元 b 和 c ，即 $a \wedge b = 0, a \vee b = 1$ ，
 $a \wedge c = 0, a \vee c = 1$ ，于是 $b = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c)$
 $= b \wedge c$ ，则 $b \leq c$ ，又 $b = b \vee (a \wedge c) = (b \vee a) \wedge (b \vee c)$
 $= b \vee c$ ，则 $b \geq c$ ，因此 $b = c$ 。



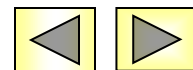


§ 7.3 几个典型的代数系统

4、**布尔格**：如果格 $\langle L, \wedge, \vee, 0, 1 \rangle$ 是有补分配格，
则称 $\langle L, \wedge, \vee, 0, 1 \rangle$ 为布尔格，
也叫做布尔代数。

布尔代数也可记为 $\langle L, \wedge, \vee, ', 0, 1 \rangle$ ，'表示求补运算。

如：集合的幂集格 $\langle P(S), \cap, \cup, \sim, \emptyset, S \rangle$ 是布尔代数，
逻辑代数 $\langle \{0, 1\}, \wedge, \vee, \neg, 0, 1 \rangle$ 是布尔代数。



§ 7.3 几个典型的代数系统

布尔代数的性质：

设 $\langle L, \wedge, \vee, ', 0, 1 \rangle$ 是布尔代数，则有

$$(1) \quad \forall a \in L, (a')' = a,$$

$$(2) \quad \forall a, b \in L, (a \wedge b)' = a' \vee b', (a \vee b)' = a' \wedge b'.$$

定理

设 $\langle L, \wedge, \vee, ', 0, 1 \rangle$ 是有限布尔代数，
则 L 含有 2^n 个元($n \in \mathbb{N}$)，且 $\langle L, \wedge, \vee, ', 0, 1 \rangle$
与 $\langle P(S), \cap, \cup, \sim, \emptyset, S \rangle$ 同构，
其中 S 是一个 n 元集合。

