离 散 数 学

代数结构 **Algebra Structures**

任课教师：杨海
yanghai@ecust.edu.cn

勤 奋 求 实
励 志 明 德

内容提要

1. 运算及其性质
2. 代数系统
3. 群与子群
4. 阿贝尔群和循环群
5. 环与域
6. 格与布尔代数

1、运算及其性质

概念：

运算， 封闭的，可交换的，可结合的，可分配的，吸收律，幂等的， 幺元，零元，逆元，消去律

运算 对于集合 A，f 是从A^n到 A 的函数，称 f 为集合A上的一个n元运算。

注：函数f：$A^n \to B$，若$B \subseteq A$，称函数f在集合A上是**封闭的**。

运算实例:

(1) 加法和乘法是N上的二元运算，但减法和除法不是.

(2) 加法、减法和乘法都是Z上的二元运算，而除法不是.

(3) 乘法和除法都是R*上的二元运算，而加法和减法不是.

(4) 设M_n(R)表示所有n 阶(n≥2)实矩阵的集合，即

$$M_n(R)=\left\{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \middle|\, a_{ij}\in R,\ i,j=1,2,\ldots,n\right\}$$

则矩阵加法和乘法都是M_n(R)上的二元运算.

(5) S为任意集合，则∪、∩、−、⊕ 为$P(S)$上二元运算.

运算的表示

1．算符

可以用$\circ$, $*$, $\cdot$, $\oplus$, $\otimes$,Δ 等符号表示二元或一元运算，称为算符.

2. 运算表：表示有穷集上的一元和二元运算

$\circ$	a_1	a_2	…	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	…	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	…	$a_2 \circ a_n$
.		…		
.		…		
.		…		
a_n	$a_n \circ a_1$	$a_n \circ a_2$	…	$a_n \circ a_n$

二元运算的运算表

	$\circ a_i$
a_1	$\circ a_1$
a_2	$\circ a_2$
.	.
.	.
.	.
a_n	$\circ a_n$

一元运算的运算表

运算表的实例

例 设 $S=P(\{a,b\})$，S上的⊕和 ~运算的运算表如下

$\oplus$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\varnothing$	$\{a.b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\varnothing$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\varnothing$

x	$\sim x$
$\varnothing$	$\{a,b\}$
$\{a\}$	$\{a\}$
$\{b\}$	$\{b\}$
$\{a,b\}$	$\varnothing$

运算的性质

交换律 (Commutative)

已知<A，*>，若∀x，y∈A，有x*y=y*x，称*在A上是**可交换的**。

例:判断相应的运算是否满足交换律。

(1) （Z，+）、（Z，-） （Z，×）

(2) 设<R，*>,*定义如下：a*b=a+b-ab

结合律(Associative)

已知⟨A，*⟩，若∀x，y，z∈A，有

$$x*(y*z)=(x*y)*z,$$

称*在A上是可结合的。

例:判断相应的运算是否满足结合律。

(1) (Z，+)、(Z，-) (Z，×)

(2) <A，*>，若∀a，b∈A，有a*b=b

幂等律(Idempotent)

已知〈A，*〉，若∀x∈A，x*x=x 则称满足幂等律 。

例：已知集合s，〈 ℘（s），∪，∩〉，则∪，∩满足幂等律。

分配律(Distributive)

设<A，*，△>，若∀x，y，z∈A有：

$x*(y\triangle z)=(x*y)\triangle(x*z)$ ；

$(y\triangle z)*x=(y*x)\triangle(z*x)$

称运算*对△是可分配的。

*	α	β
α	α	β
β	β	α

△	α	β
α	α	α
β	α	β

例：设A={α，β}，二元运算*，△定义如左：

问分配律成立否？

① 运算△对*是可分配的。

即： $x\triangle(y*z)=(x\triangle y)*(x\triangle z)$ 成立

证： 当 $x=\alpha$： $x\triangle(y*z)=\alpha$

*	α	β
α	α	β
β	β	α

$(x\triangle y)*(x\triangle z)=\alpha$

当 $x=\beta$： $x\triangle(y*z)=y*z$

$(x\triangle y)*(x\triangle z)=y*z$

△	α	β
α	α	α
β	α	β

②、运算*对运算△不可分配

证： $\because \beta*(\alpha\triangle\beta)=\beta*\alpha=\beta$

$(\beta*\alpha)\triangle(\beta*\alpha)=\beta\triangle\alpha=\alpha$

吸收律(Absorbtive)

设$*$, Δ是定义在集合A上的两个可交换二元运算，若对

$\forall x, y \in A$, 都有:

$$x*(x\Delta\ y) = x$$

$$x\Delta(x*\ y) = x$$

则称运算$*$和Δ满足吸收律.

例：幂集P(S)上的运算$\cup$和$\cap$满足吸收律。

单位元（幺元）(Identity)

设*是A上二元运算， $e_l, e_r, e \in A$

若$\forall x \in A$，有$e_l * x = x$，称e_l为运算*的**左幺元**；

若$\forall x \in A$，有$x * e_r = x$，称e_r为运算*的**右幺元**

若e既是左幺元又是右幺元，称e为运算*的**幺元**

- $\forall x \in A$，有$e * x = x$，$x * e = x$

定理：设*是A上的二元运算，具有左幺元e_l，右幺元e_r，则$e_l=e_r=e$

证明：　$e_r = e_l * e_r = e_l$

推论：二元运算的幺元若存在则唯一

证明：反证法：设有二个幺元e，e’；

则$e=e*e'=e'$

零元 (Zero)

设*是A上二元运算， θ_l， θ_r， $\theta \in A$

若$\forall x \in A$，有$\theta_l * x = \theta_l$ ，称θ_l为运算*的左零元；

若$\forall x \in A$，有$x * \theta_r = \theta_r$，称θ_r为运算*的右零元；

若θ既是左零元又是右零元，称θ为运算*的零元。

- $\forall x \in A$，有$\theta * x = x * \theta = \theta$

例：

a）$\langle Z, \times \rangle$，Z为整数集

则幺元为1，零元为0

b）$\langle \wp(A), \cup, \cap \rangle$

对运算$\cup$，$\varnothing$是幺元，A是零元

对运算$\cap$，A是幺元，$\varnothing$是零元。

c）$\langle N, + \rangle$

有幺元0，无零元。

例：代数A=〈{a，b，c，d}，*〉用下表定义：

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

左幺元　无

右幺元　a

左零元　a, b

右零元　无

定理：设*是A上的二元运算，具有左零元θ_l，右零元θ_r，则$\theta_l = \theta_r = \theta$

推论：二元运算的零元若存在则唯一。

逆元 (Inverse)

设*是A上的二元运算，e是运算*的幺元

若x*y=e那对于运算*，x是y的左逆元，y是x的右逆元

若x*y=e，y*x=e，则称x是y的逆元。记为y^{-1}

- 存在逆元(左逆元，右逆元）的元素称为可逆的（左可逆的，右可逆的）

例：

a)、代数〈N，+〉仅有幺元0，有逆元0，

b)、A=〈{a，b，c}，*〉由下表定义：

*	a	b	c
a	a	a	b
b	a	b	c
c	a	c	c

b是幺元，

a的右逆元为c，无左逆元，

b的逆元为b，

C无右逆元，左逆元为a

定理：对于可结合运算 o ，如果元素x有 左逆元 l ，右逆元r，则 $l=r=x^{-1}$

证：$l = l \circ e = l \circ (x \circ r)$

$= (l \circ x) \circ r = e \circ r = r$

∴逆元存在为r

推论：逆元若存在，则唯一

证：若存在X的另一个逆元r^1； 则：

$r^1 = r^1 \circ e = r^1 \circ (x \circ r)$

$= (r^1 \circ x) \circ r = e \circ r = r$

消去律 (Cancellation Law)

已知<A，*>，若∀x，y，z∈A，有

(1) 若 $x*y = x*z$ 且 $x \neq \theta$, 则 $y=z$；

(2) 若 $y*x = z*x$ 且 $x \neq \theta$, 则 $y=z$；

那么称*满足消去律。

例: **(1) 整数集上的加法和乘法都满足消去律；**

(2) S ={1,2,3}, P(S)的交、并运算不满足消去律。

2、代数系统及同态

概念：

代数系统，子代数，积代数，同态，同构。

代数系统 设**A**为非空集合，**Ω**为**A**上运算的集合,称**<A,Ω >**为一个代数系统.

- 当Ω $=\{f_1,\ldots,f_n\}$是有限时,代数系统常记为$\langle A,f_1,\ldots,f_n\rangle$;
- 当A有限时,称<A,Ω>是有限代数系统。

例：

(1) $\langle \mathbf{N},+\rangle,\langle \mathbf{Z},+,\cdot\rangle,\langle \mathbf{R},+,\cdot\rangle$是代数系统，+和·分别表示普通加法和乘法。

(2) $\langle P(S),\cup,\cap,\sim\rangle$是代数系统，∪和∩为并和交，~为绝对补。

构成代数系统的成分：

- 集合（也叫载体，规定了参与运算的元素）
- 运算（这里只讨论有限个二元和一元运算）
- 代数常数（通常是与运算相关的特异元素：如单位元等）

例如：代数系统$<\mathbf{Z},+,0>$：集合**Z**, 运算+, 代数常数**0**

代数系统$<P(S),\cup,\cap>$：集合$P(S)$, 运算$\cup$和$\cap$，无代数常数

如果两个代数系统中运算的个数相同，对应运算的元数相同，且代数常数的个数也相同，则称它们是同类型的代数系统.

例：

$V_1=<\mathbf{R}, +, \cdot, 0, 1>$

$V_2=<M_n(\mathbf{R}), +, \cdot, \theta, E>$, θ为 n 阶全0矩阵，E为 n 阶单位矩阵

$V_3=<P(B), \cup, \cap, \varnothing, B>$

- V_1, V_2, V_3是同类型的代数系统，它们都含有2个二元运算, 2个代数常数.

设$V=<S, f_1, f_2, \ldots, f_k>$是代数系统，$B$是$S$的非空子集，如果$B$对$f_1, f_2, \ldots, f_k$都是封闭的，且$B$和$S$含有相同的代数常数，则称$<B, f_1, f_2, \ldots, f_k>$是$V$的子代数系统，简称子代数。

注：有时将子代数系统简记为B.

实例

N是<Z,＋>的子代数，N也是<Z,＋,0>的子代数

N−{0}是<Z,＋>的子代数，但不是<Z,＋,0>的子代数

几个术语

(1) 最大的子代数：就是V本身

(2) 最小的子代数：如果令V中所有代数常数构成的集合是B，且B对V中所有的运算都是封闭的，则B就构成了V的最小的子代数

(3) 最大和最小的子代数称为V的平凡的子代数

(4) 若B是S的真子集，则B构成的子代数称为V的真子代数.

例 设$V=\langle Z,+,0\rangle$,令 $nZ=\{nz \mid z\in Z\}$,n为自然数，则nZ是V的子代数

当$n=1$和0时，nZ是V的平凡的子代数，其他的都是V的非平凡的真子代数.

设$V_1=<A,\circ>$和$V_2=<B,*>$是同类型的代数系统，$\circ$和$*$为二元运算，在集合$A\times B$上如下定义二元运算▪，

$\forall <a_1,b_1>,<a_2,b_2>\in A\times B$，有

$$<a_1,b_1>\blacksquare<a_2,b_2>=<a_1\circ a_2,\ b_1*b_2>$$

称$V=<A\times B,\blacksquare>$为$V_1$与$V_2$的积代数，记作$V_1\times V_2$. 这时也称$V_1$和$V_2$为$V$的因子代数.

定理 设$V_1=<A,\circ>$和$V_2=<B,*>$是同类型的代数系统，$V_1\times V_2=<A\times B,\blacksquare>$是它们的积代数.

(1) 如果$\circ$和$*$运算是可交换（可结合、幂等）的，那么▪运算也是可交换（可结合、幂等）的

(2) 如果e_1和e_2（θ_1和θ_2）分别为$\circ$和$*$运算的单位元（零元），那么$<e_1,e_2>$（$<\theta_1,\theta_2>$）也是▪运算的单位元（零元）

(3) 如果x和y分别为$\circ$和$*$运算的可逆元素，那么$<x,y>$也是▪运算的可逆元素，其逆元就是$<x^{-1},y^{-1}>$

设$V_1=<A,\circ>$和$V_2=<B,*>$是同类型的代数系统，$f:A\to B$，

对$\forall x, y\in A$ 有 $f(x\circ y) = f(x)*f(y)$,

则称 f 是V_1到V_2的同态映射，简称同态 (Homomorphism) 。

特殊的同态

(1) f 如果是单射，则称为单同态(Monomorphism)。

(2) 如果是满射，则称为满同态 (Epimorphism)，这时称V_2是V_1的同态像， 记作$V_1\sim V_2$。

(3) 如果是双射，则称为同构 (Isomorphism)，也称代数系统V_1同构于V_2， 记作$V_1\cong V_2$ 。

(4) 如果$V_1=V_2$，则称作自同态(Endomorphism)。

实例

(1) 设V_1=<Z,+>, V_2=<Z_n,⊕>．其中Z为整数集，+为普通加法；Z_n={0,1,…,n−1}，⊕为模n加. 令

$$f: Z\to Z_n，f(x)=(x)\bmod n$$

那么 f 是V_1到V_2的满同态.

(2) 设V_1=<R,+>, V_2=<R*,·>，其中R和R*分别为实数集与非零实数集，+ 和 · 分别表示普通加法与乘法．令

$$f: R\to R^*，f(x)= e^x$$

则 f 是V_1到V_2的单同态.

(3) 设V=<Z,+>，其中Z为整数集，+为普通加法. ∀a∈Z，令

$$f_a: Z\to Z，f_a(x)=ax，$$

那么 f_a 是V的自同态；当a=±1时，称 f_a 为自同构；除此之外其他的 f_a 都是单自同态.

3、群与子群

概念：

半群, 子半群, 元素的幂，独异点，群，群的阶数，子群，平凡子群，陪集，拉格朗日（Lagrange）定理

半群（Semigroup）

设V=<S, ∘ >是代数系统，∘为二元运算，如果∘运算是可结合的，则称V为半群。

独异点(Monoid).

设V=<S,∘>是半群，若$e \in S$是关于∘运算的单位元，则称V是含幺半群，也叫做独异点。 有时也将独异点V 记作V=<S,∘,e>.

实例

(1) $<Z^+,+>$,$<N,+>$,$<Z,+>$,$<R,+>$都是半群，+是普通加 法. 这些半群中除$<Z^+,+>$外都是独异点

(2) $<P(B),\oplus>$为半群，也是独异点，其中$\oplus$为集合对称差运算

(3) $<R^*,\circ>$为半群，但不是独异点，其中R^*为非零实数集合，$\circ$运算定义如下：$\forall x, y \in R^*, x \circ y = y$

群(Group)

设V=<G,∘>是独异点，$e \in$ G关于∘运算的单位元，若 $\forall a \in G$，$a^{-1} \in G$，则称V是群(Group). 通常将群记作G.

群的另一种定义（基本形式）

设<G, ∘ >是代数系统，∘为二元运算。

(1) ∘ 对**G**是封闭的；

(2) ∘ 是可结合的；

(3) 存在幺元 **e**；

(4) 对于每一个元素 $x \in G$，都存在它的逆元$x^{-1} \in G$

则称<G, ∘ >是一个群.

实例

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

特征:

1. 满足交换律
2. 每个元素都是自己的逆元
3. a, b, c中任何两个元素运算结果都等于剩下的第三个元素

群的阶数

设<G,∗>是一个群,如果G是有限集，那么称<G,∗>为有限群，并且|G| 为该有限群的阶数；如果G是无限集，则称<G,∗>为无限群。

注：阶数为1（即只含单位元）的群称为平凡群.

例：<Z,+>和<R,+>是无限群；

$<Z_n,\oplus>$是有限群，也是 n 阶群；

Klein四元群是4阶群；

<{0},+>是平凡群。

n阶($n\geq2$)实可逆矩阵集合关于矩阵乘法构成的群是非交换群.

群的性质

设<G,∗>是一个群。

（1）非平凡群中不可能有零元.

（2）对于$\forall a,b \in G$, 必存在唯一的$x \in G$,使得$a * x = b$.

（3）对于$\forall \{a,b,c\} \in G$若:

$$a*b = a*c \text{或}$$

$$b*a = c*a$$

则必有$b=c$ (消去律)。

（4）运算表中的每一行或每一列都是一个置换。

（5）除幺元e外,不可能有任何别的幂等元。

元素的幂

设G是群，$a\in G$，$n\in Z$，则a 的 n次幂.

$$a^n = \begin{cases} e & n = 0 \\ a^{n-1}a & n > 0 \\ (a^{-1})^m & n < 0,\ n = -m \end{cases}$$

注：群中元素可以定义负整数次幂.

在$<Z_3,\oplus>$中有

$$2^{-3} = (2^{-1})^3 = 1^3 = 1\oplus 1\oplus 1 = 0$$

在$<Z,+>$中有

$$(-2)^{-3} = 2^3 = 2+2+2 = 6$$

幂运算性质

设G 为群，则G中的幂运算满足：

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

(2) $\forall a,b\in G$，$(ab)^{-1}=b^{-1}a^{-1}$

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

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

(5) 若G为交换群，则 $(ab)^n = a^n b^n$.

元素的阶

设G是群，$a \in G$，使得等式 $a^k=e$ 成立的最小正整数k 称为元素a 的阶，记作$|a|=k$，称 a 为 k 阶元。若不存在这样的正整数 k，则称 a 为无限阶元。

例：(1) 在$<Z_6,\oplus>$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 。

(2) 在$<Z,+>$中，0是1阶元，其它整数的阶均为无限。

元素的阶的性质

G为群，$a \in G$且 $|a| = r$. 设k是整数，则

(1) $a^k = e$当且仅当$r \mid k$

(2) $|a^{-1}| = |a|$

子群（Subgroup）

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$H \leqslant G$。

① 若H是G 的子群，且$H \subset G$，则称H是G的真子群，记作$H < G$.

② 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.

例： nZ (n是自然数) 是整数加群<Z,+> 的子群. 当$n \neq 1$时，nZ是Z的真子群.

子群判定定理1

设G为群，H是G的非空子集，则H是G的子群当且仅当

(1) $\forall a,b\in H$有$ab\in H$；

(2) $\forall a\in H$有$a^{-1}\in H$。

证 必要性是显然的. 为证明充分性，只需证明$e\in H$.
因为H非空，存在$a\in H$. 由条件(2) 知$a^{-1}\in H$，根据条件(1)
$aa^{-1}\in H$，即$e\in H$.

子群判定定理2

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

证　必要性显然. 只证充分性.

因为H非空，必存在$a\in H$.

根据给定条件得$aa^{-1}\in H$，即$e\in H$.

任取$a\in H$, 由$e,a\in H$ 得 $ea^{-1}\in H$，即$a^{-1}\in H$.

任取$a,b\in H$，知$b^{-1}\in H$. 再利用给定条件得$a(b^{-1})^{-1}\in H$，即$ab\in H$.

综合上述，可知H是G的子群.

子群判定定理3

设G为群，H是G的非空有穷子集，则H是G的子群当且仅当

$\forall a,b \in H$有$ab \in H$.

证 必要性显然. 为证充分性，只需证明 $a \in H$有$a^{-1} \in H$.

任取$a \in H$, 若$a = e$, 则$a^{-1} = e \in H$.

若$a \neq e$，令$S=\{a,a^2,\ldots\}$，则$S \subseteq H$.

由于H是有穷集，必有$a^i = a^j$（$i<j$）.

根据G中的消去律得 $a^{j-i} = e$，由$a \neq e$可知 $j-i>1$，由此得

$$a^{j-i-1}a = e \text{ 和 } a\,a^{j-i-1} = e$$

从而证明了$a^{-1} = a^{j-i-1} \in H$.

生成子群

设G为群，$a\in G$，令$H=\{a^k | k\in Z\}$，则H是G的子群，称为由a 生成的子群，记作$\langle a\rangle$.

例：

（1）整数加群，由2生成的子群是 $<2>=\{2^k | k\in Z\}=2Z$

（2）$<Z_6,\oplus>$中，由2生成的子群$<2>=\{0,2,4\}$

（3）Klein四元群 $G=\{e,a,b,c\}$的所有生成子群是：

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

$\langle G,*\rangle$是一个群, $A,B\in P(G)$,且$A\neq\varnothing,B\neq\varnothing$, 定义:

$AB = \{a*b \mid a\in A$且$b\in B\}$

$A^{-1}=\{a^{-1} \mid a\in A\}$

称AB为A,B的积，A^{-1}为A的逆 。

陪集

设$\langle H,*\rangle$是群$\langle G,*\rangle$的一个子群,$a\in G$则:

左陪集: $aH ::= \{a\}H$，由a所确定的H在G中的左陪集.

右陪集: $Ha::=H\{a\}$

陪集是左陪集与右陪集的统称.

例： 设$G=\{e,a,b,c\}$是Klein四元群，$H=\langle a\rangle$是G的子群.

H所有的右陪集是：

$He=\{e,a\}=H$，$Ha=\{a,e\}=H$，$Hb=\{b,c\}$，$Hc=\{c,b\}$

不同的右陪集只有两个，即H和$\{b,c\}$.

陪集性质

设H是群G的子群，则

① $He = H$

② $\forall a \in G$ 有$a \in Ha$

③ $\forall a,b \in G$有：$a \in Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha=Hb$

④ 在G上定义二元关系R：

$$\forall a,b \in G, <a,b> \in R \Leftrightarrow ab^{-1} \in H$$

则 R是G上的等价关系，且$[a]_R = Ha$.

⑤ $|Ha|=|H|$

Lagrange定理

设G是有限群，H是G的子群，则

$$|G| = |H|\cdot[G:H]$$

其中$[G:H]$ 是H在G中的不同右陪集(或左陪集) 数，称为H在G 中的**指数**.

$$|G| = |H| \cdot [G:H]$$

证 设$[G:H]=r$，$a_1,a_2,\cdots,a_r$分别是H的r个右陪集的代表元素. 根据定理10.9的推论有

$$G=Ha_1\cup Ha_2\cup\cdots\cup Ha_r$$

由于这r个右陪集是两两不交的，所以有

$$|G|=|Ha_1|+|Ha_2|+\cdots+|Ha_r|$$

因为$|Ha_i|=|H|$，$i=1,2,\cdots,r$. 将这些等式代入上式得

$$|G|=|H|\cdot r=|H|\cdot[G:H]$$

推论：

（1） 设G是n阶群，则$\forall a \in G$，$|a|$是n的因子，且$a^n = e$.

（2） 对阶为素数的群G，必存在$a \in G$使得$G = \langle a \rangle$.

证 任取 $a \in G$,则$\langle a \rangle$是 G 的子群. 由拉格朗日定理知$\langle a \rangle$的阶是 n 的因子. 另一方面,$\langle a \rangle$是由 a 生成的子群,若$|a| = r$,则

$$\langle a \rangle = \{ a^0 = e, a^1, a^2, \cdots, a^{r-1} \}$$

这说明$\langle a \rangle$的阶与$|a|$相等,所以$|a|$是 n 的因子. 根据定理 10.3(1)必有 $a^n = e$.

证 设$|G| = p$,p 是素数. 由 $p \geq 2$ 知 G 中必存在非单位元. 任取 $a \in G$,$a \neq e$,则$\langle a \rangle$是 G 的子群. 根据拉格朗日定理,$\langle a \rangle$的阶是 p 的因子,即$\langle a \rangle$的阶是 p 或 1. 显然$\langle a \rangle$的阶不等于 1. 这就推出 $G = \langle a \rangle$.

4、阿贝尔群和循环群

概念：

阿贝尔群(交换群)，循环群, 生成元

阿贝尔 (Abel) 群

若群G中的运算是可交换的，则称G为交换群或阿贝尔 群。

例：（1）$<Z,+>$和$<R,+>$，$<Z_n,\oplus>$、Klein四元群均是阿贝尔群。

（2）n阶($n\geq 2$)实可逆矩阵集合关于矩阵乘法构成的群不是阿贝尔群。

循环群（Cyclic group）

设G是群，若存在$a \in G$使得

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

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

循环群的分类

(1) n 阶循环群：设$G=\langle a\rangle$是循环群，若a是n 阶元，则

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

(2)无限循环群：若a 是无限阶元，则

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

循环群的生成元

设G=<a>是循环群。

(1) 若G是无限循环群，则G只有两个生成元，即a和a^{-1}.

(2) 若G是 n 阶循环群，则G含有$\phi(n)$个生成元. 对于任何小于n且与 n 互质的数$r\in\{0,1,\ldots,n\text{-}1\}$, a^r是G的生成元.

实例

(1) 设$G=\{e, a, \ldots, a^{11}\}$是12阶循环群，则$\phi(12)=4$. 小于12且与12互素的数是1, 5, 7, 11, 由定理10.13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$\phi(9)=6$. 小于9且与9互素的数是 1, 2, 4, 5, 7, 8. 根据定理10.13，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

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。

实例

(1) G=<Z,+>是无限循环群，其生成元为1和−1．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

$$<0> = \{0\} = 0Z$$

$$<m> = \{mz \mid z\in Z\}= mZ,\quad m>0$$

(2) $G=Z_{12}$是12阶循环群. 12正因子是1,2,3,4,6和12，G 的子群:

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 $<1>=Z_{12}$

5、环与域

概念：

环，交换环，含幺环，整环，域

环（Ring）

设$\langle R,+,\cdot\rangle$是代数系统，+和·是二元运算. 如果满足以下条件:

(1) $\langle R,+\rangle$构成交换群;

(2) $\langle R,\cdot\rangle$构成半群;

(3) · 运算关于+运算适合分配律,

则称$\langle R,+,\cdot\rangle$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（如果存在）记作1.

对任何元素 x，称 x 的加法逆元为负元，记作$-x$.

若 x 存在乘法逆元的话，则称之为逆元，记作x^{-1}.

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，称为子集环.

(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.

环的运算性质

设$<R,+,\cdot>$是环，则

(1) $\forall a \in R$，$a0 = 0a = 0$

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

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

(4) $\forall a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_m \in R$ $(n,m \geq 2)$

$$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

例：在环中计算$(a+b)^3$, $(a-b)^2$

解： $(a+b)^3 = (a+b)(a+b)(a+b)$

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

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

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

特殊的环

设$<R,+,\cdot>$是环

(1) 若环中乘法 $\cdot$ 适合交换律，则称R是交换环；

(2) 若环中乘法 $\cdot$ 存在单位元，则称R是含幺环；

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

例：

(1) 整数环Z交换 环，含幺环，无零因子环。

(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。

整环(Integrel Domain)

设<R,+,•>是一个代数系统,若满足:

(1) <R,+>是阿贝尔群;

(2) <R,•>是可交换独异点，且无零因子，即对$\forall a,b \in R$, $a \neq 0, b \neq 0$ 则$a \bullet b \neq 0$;

(3) 运算•对+是可分配的,

则称<R,+,•>是整环。

注:（1）既是交换环、含幺环、无零因子环 的代数系统是整环。

（2）整环中的无零因子条件等价于乘法消去律，即对于$c \neq 0$ 和$c \bullet a = c \bullet b$,有$a = b$.

域 (Field)

设<R,+,•>是一个代数系统,若满足:

(1) <R,+>是阿贝尔群;

(2) <R-{0},•>是阿贝尔群;

(3) 运算•对+是可分配的,

则称<R,+,•>是域。

例: 整数环Z整环，但不是域；实数环R既是是域。

两点结论:

(1) 域一定是整环。

(2) 有限整环必是域。

6、格与布尔代数

概念：

格，对偶原理，子格，分配格，有界格，有补格

布尔代数，有限布尔代数的表示定理

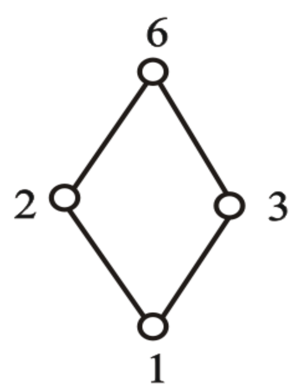
格（Lattice）

设<S, ≼>是偏序集，如果∀$x,y\in S$，$\{x,y\}$都有最小上界和最大下界，则称S关于偏序≼作成一个格。

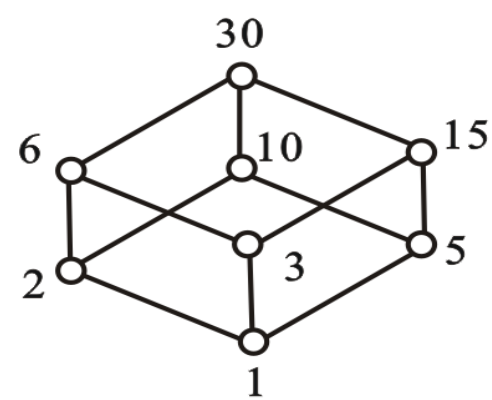
注：求$\{x,y\}$ 最小上界和最大下界看成 x 与 y 的二元运算∨和∧.

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<Sn,D>构成格. ∀$x,y\in S_n$，$x\vee y$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.

(S_8,D)



(S_6,D)



(S_{30},D)

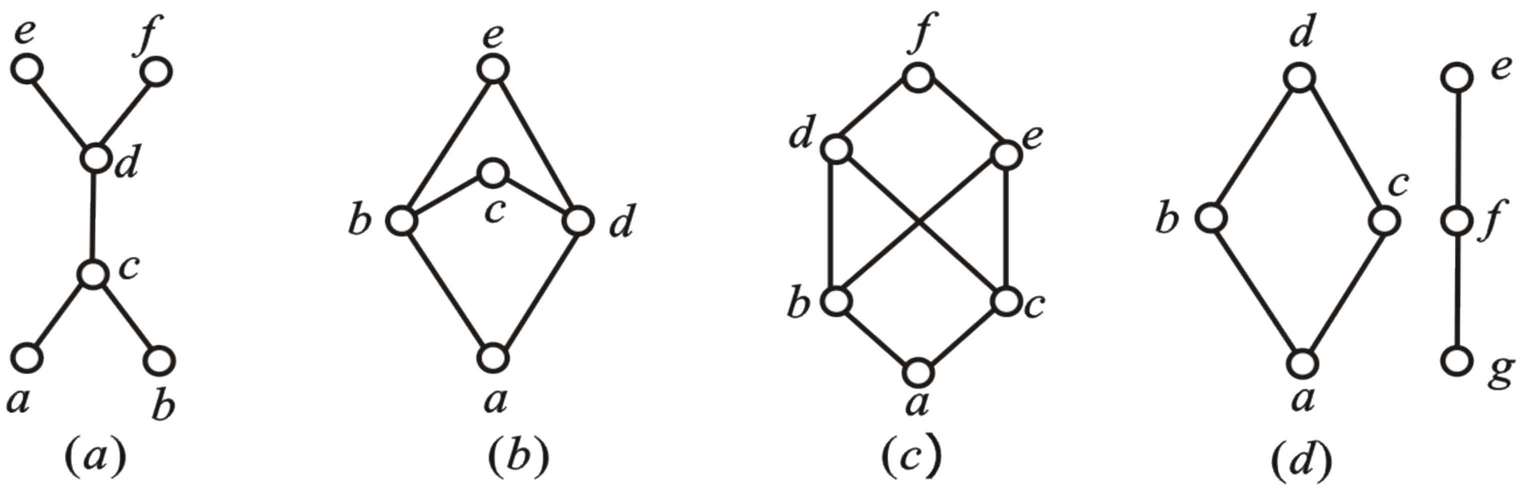
实例

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) $<\mathrm{Z}, \leq>$，其中Z是整数集，≤为小于或等于关系.

(3) 偏序集的哈斯图分别在下图给出.



(1) 幂集格. $\forall x,y\in P(B)$，$x\vee y$就是$x\cup y$，$x\wedge y$就是$x\cap y$.

(2) 是格. $\forall x,y\in Z$，$x\vee y = \max(x,y)$，$x\wedge y = \min(x,y)$，

(3) 都不是格. 可以找到两个结点缺少最大下界或最小上界

设 f 是含有格中元素以及符号 $=, \preccurlyeq, \succcurlyeq, \vee$ 和 $\wedge$ 的命题.

令 f^* 是将 f 中的 $\preccurlyeq$ 替换成 $\succcurlyeq$, $\succcurlyeq$ 替换成 $\preccurlyeq$, $\vee$ 替换成 $\wedge$, $\wedge$ 替换成 $\vee$ 所得到的命题. 称 f^* 为 f 的对偶命题.

例: 在格中令 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 是含有格中元素以及符号 $=, \preccurlyeq, \succcurlyeq, \vee$ 和 $\wedge$ 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.

格的性质

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

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

(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

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

(4) $\forall a,b \in L$ 有

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

格的性质：序与运算

设L是格, 则$\forall a,b\in L$有

$$a \preccurlyeq b \Leftrightarrow a\wedge b = a \Leftrightarrow a\vee b = b$$

证 (1) 先证 $a \preccurlyeq b \Rightarrow a\wedge b = a$

由 $a \preccurlyeq a$ 和 $a \preccurlyeq b$ 可知 a 是$\{a,b\}$的下界, 故 $a \preccurlyeq a\wedge b$.

显然有$a\wedge b \preccurlyeq a$. 由反对称性得 $a\wedge b = a$.

(2) 再证 $a\wedge b = a \Rightarrow a\vee b = b$

根据吸收律有 $b = b\vee(b\wedge a)$

由 $a\wedge b = a$ 和上面的等式得 $b = b\vee a$, 即 $a\vee b = b$.

(3) 最后证 $a\vee b = b \Rightarrow a\preccurlyeq b$

由 $a \preccurlyeq a\vee b$ 得 $a \preccurlyeq a\vee b = b$

格的性质：保序

设L是格, $\forall a,b,c,d \in L$，若$a \preccurlyeq b$ 且 $c \preccurlyeq d$, 则

$$a \wedge c \preccurlyeq b \wedge d, \quad a \vee c \preccurlyeq b \vee d$$

证 $\qquad a \wedge c \preccurlyeq a \preccurlyeq b,\ a \wedge c \preccurlyeq c \preccurlyeq d$

因此 $a \wedge c \preccurlyeq b \wedge d$. 同理可证 $a \vee c \preccurlyeq b \vee d$

格的代数系统定义

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

注：S中的偏序关系 $\preccurlyeq$定义为： 对$\forall a,b \in S$ 有

$$a \preccurlyeq b \Leftrightarrow a \circ b = b .$$

子格（Sub-lattice）

设$<L,\wedge,\vee>$是格, S是L的非空子集, 若S关于L中的运算$\wedge$和$\vee$仍构成格, 则称S是L的子格.

例：设格L如图所示. 令

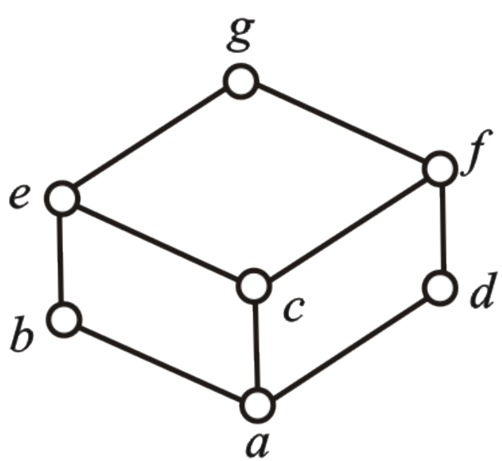
$S_1=\{a, e, f, g\}$,

$S_2=\{a, b, e, g\}$

S_1不是L的子格, 因为$e, f\in S_1$ 但

$e\wedge f = c\notin S_1$.

S_2是L的子格.



注： 对于格$<L, \preccurlyeq >$, S是L的非空子集, $<S, \preccurlyeq >$必定是偏序集，但未必是格；而且即使$<S, \preccurlyeq >$是格，也未必是$<L, \preccurlyeq >$的子格。

分配格（Distributive lattice）

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

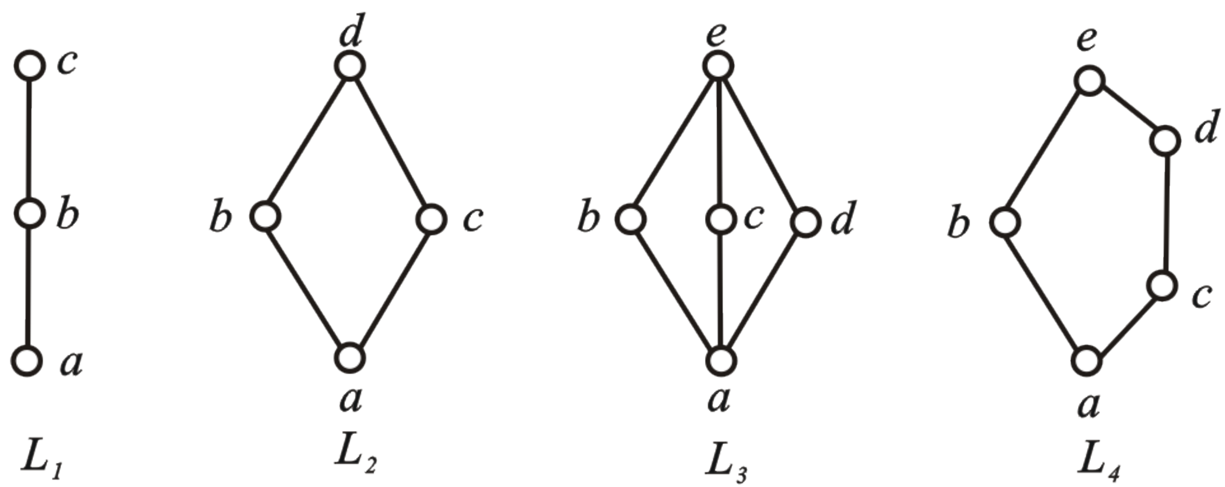
$$a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)$$

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

则称L为分配格.

- 注意：可以证明以上两个条件是等价的。

例



L_1 和 L_2 是分配格, L_3 和 L_4不是分配格.
称 L_3为钻石格, L_4为五角格.

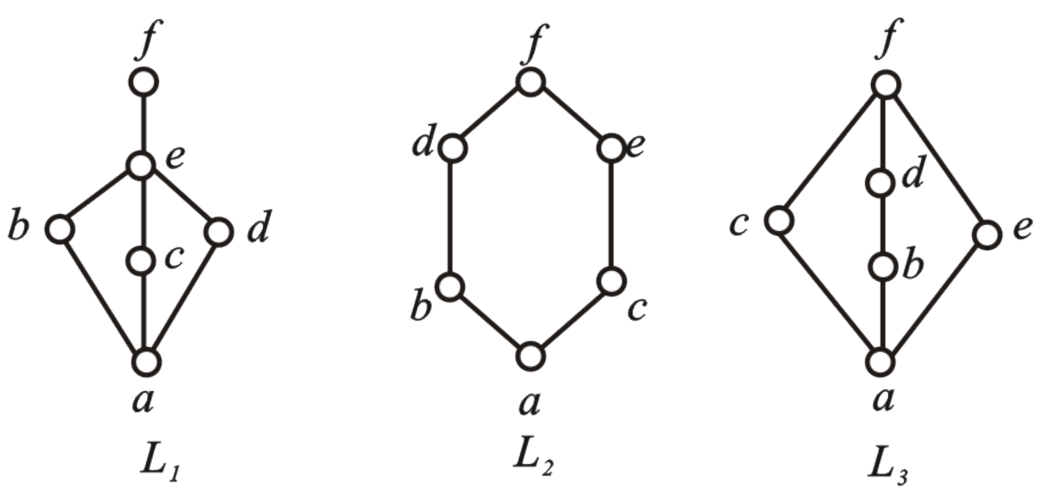
分配格的判别

定理： 设L是格, 则L是分配格当且仅当L不含有与钻石格或五角格同构的子格.

推论 (1) 小于五元的格都是分配格.

(2) 任何一条链都是分配格.

例： 说明图中的格是否为分配格, 为什么？



解 都不是分配格.

$\{a,b,c,d,e\}$是L_1的子格, 同构于钻石格

$\{a,b,c,e,f\}$是L_2的子格, 同构于五角格;

$\{a,c,b,e,f\}$ 是L_3的子格同构于钻石格.

设L是格,

(1) 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;

(2) 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, 一定是惟一的.
- 一般将格L的全下界记为0, 全上界记为1.

有界格 （Bounded lattice）

设L是格，若L存在全下界和全上界, 则称L 为有界格，一般将有界格L记为$<L,\wedge,\vee,0,1>$.

有界格的性质

定理： 设$<L,\wedge,\vee,0,1>$是有界格, 则$\forall a\in L$有

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

注意：

- 有限格$L=\{a_1,a_2,\ldots,a_n\}$是有界格, $a_1\wedge a_2\wedge\ldots\wedge a_n$是$L$的全下界, $a_1\vee a_2\vee\ldots\vee a_n$是$L$的全上界.
- 0是关于$\wedge$运算的零元,$\vee$运算的单位元；1是关于$\vee$运算的零元,$\wedge$运算的单位元.
- 对于涉及到有界格的命题, 如果其中含有全下界0或全上界1, 在求该命题的对偶命题时, 必须将0替换成1, 而将1替换成0.

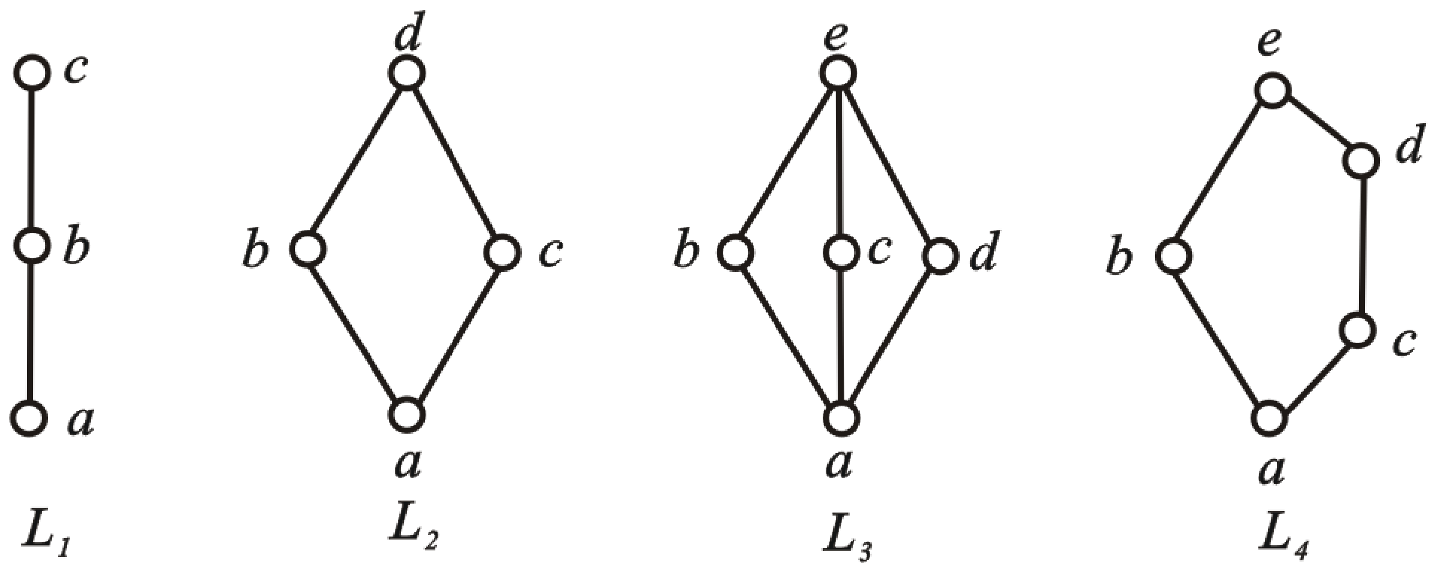
设$<L,\wedge,\vee,0,1>$是有界格, $a\in L$, 若存在$b\in L$ 使得

$$a\wedge b = 0 \text{ 和 } a\vee b = 1$$

成立, 则称b是a的补元.

- 注意：若b是a的补元, 那么a也是b的补元. a和b互为补元.

例： 考虑下图中的格. 针对不同的元素，求出所有的补元.



解答

(1) L_1中 a 与 c 互为补元, 其中 a 为全下界, c为全上界, b 没有补元.

(2) L_2中 a 与 d 互为补元, 其中 a 为全下界, d 为全上界, b与 c 也互为补元.

(3) L_3中a 与 e 互为补元, 其中 a 为全下界, e 为全上界, b 的补元是 c 和 d； c 的补元是 b 和 d ; d 的补元是 b 和 c； b, c, d 每个元素都有两个补元.

(4) L_4中 a 与 e 互为补元, 其中 a 为全下界, e 为全上界, b 的补元是 c 和 d； c 的补元是 b； d 的补元是 b .

有界分配格的补元惟一性

定理： 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.

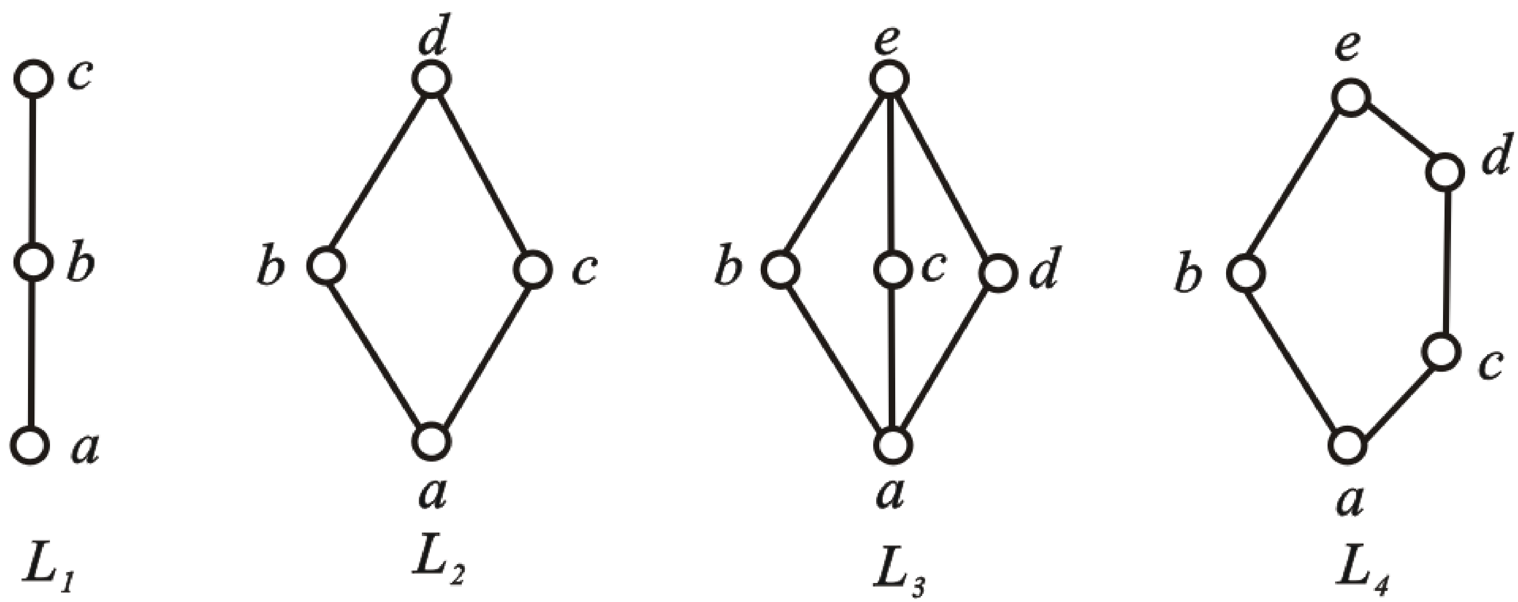
注意：

- 在任何有界格中, 全下界0与全上界1互补.
- 对于一般元素, 可能存在补元, 也可能不存在补元. 如果存在补元, 可能是惟一的, 也可能是多个补元. 对于有界分配格, 如果元素存在补元, 一定是惟一的.

有补格 (Complemented lattice)

设<L,∧,∨,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：图中的L_2, L_3和L_4是有补格, L_1不是有补格.



布尔格 (Boolean lattice)

如果一个格是有补分配格, 则称它为**布尔格**或**布尔代数**. 布尔代数标记为$<B, \wedge, \vee, ', 0, 1>$, $'$为求补运算.

例:

（1）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$<S_{110}, \mathrm{gcd}, \mathrm{lcm}>$构成布尔代数。

（2）设B为任意集合, 证明B的幂集格$<P(B), \cap, \cup, \sim, \varnothing, B>$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) $\forall a,b\in B$, $(a\wedge b)'=a'\vee b'$, $(a\vee b)'=a'\wedge b'$ （德摩根律）

布尔代数的代数系统定义

设$<B, *, \circ>$是代数系统, $*$和$\circ$是二元运算. 若$*$和$\circ$运算满足:

(1) 交换律, 即$\forall a,b \in B$有 $a*b = b*a$, $a\circ b = b\circ a$

(2) 分配律, 即$\forall a,b,c \in B$有

$$a*(b\circ c) = (a*b)\circ(a*c),\ \ a\circ(b*c) = (a\circ b)*(a\circ c)$$

(3) 同一律, 即存在$0,1 \in B$, 使得$\forall a \in B$有$a*1 = a$, $a\circ 0 = a$

(4) 补元律, 即$\forall a \in B$, 存在 $a' \in B$ 使得 $a*a' = 0$, $a\circ a' = 1$

则称 $<B,*,\circ>$是一个布尔代数.

有限布尔代数的结构

设 L 是格, $0\in L$, $a\in L$若$\forall b\in L$有 $0 \prec b \preccurlyeq a \Leftrightarrow b = a$, 则称 a 是 L 中的原子.

注：原子是盖住全下界0的元素。

有限布尔代数的表示定理

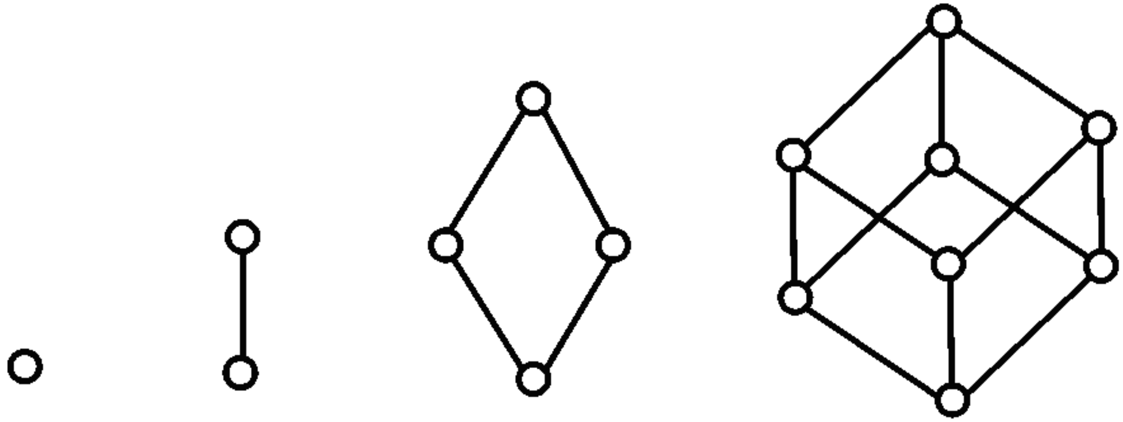
设B是有限布尔代数, A是B的全体原子构成的集合，则B同构于A的幂集代数$P(A)$.

推论1　任何有限布尔代数的基数为2^n, $n\in \mathbf{N}$.

推论2　任何等势的有限布尔代数都是同构的.

实例

下图给出了 1 元, 2 元, 4 元和 8 元的布尔代数.



总结

1. 运算及其性质：运算，封闭的, 可交换的, 可结合的, 可分配的, 吸收律，幂等的，幺元, 零元, 逆元
2. 代数系统：代数系统，子代数，积代数，同态，同构。
3. 群与子群：半群, 子半群, 元素的幂，独异点，群，群的阶数，子群, 平凡子群，陪集，拉格朗日（**Lagrange**）定理
4. 阿贝尔群和循环群：阿贝尔群(交换群)，循环群, 生成元
5. 环与域：环，交换环，含幺环，整环，域
6. 格与布尔代数：格，对偶原理，子格，分配格，有界格，有补格，布尔代数，有限布尔代数的表示定理