离散数学

第六章: 几个典型的代数系统

卢杨

厦门大学信息学院计算机科学系

luyang@xmu.edu.cn

6.1 群, 环与域

半群, 独异点与群

定义 6.1&6.2

设$V = \langle S,\circ\rangle$是代数系统, $\circ$为二元运算的.

(1) 如果$\circ$是可结合的, 则称$V = \langle S,\circ\rangle$为半群;

(2) 如果半群V具有单位元e, 则称$V = \langle S,\circ,e\rangle$为独异点.

(3) 如果G是独异点, 并且S中任何元素x都有逆元, 则称$G = \langle S,\circ,e\rangle$为群.

由上述定义有:

$$\{\text{群}\} \subset \{\text{独异点}\} \subset \{\text{半群}\} \subset \{\text{代数系统 (广群)}\}$$

- 验证一个代数系统是群, 只需四点: 封闭性, 结合律, 单位元, 逆元.
- 方便起见, 在不引起混淆的时候也用V表示V中的集合S. 因此, 可以说群G中的某个元素.

半群, 独异点与群

例 6.1 (1) $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}$关于普通加法和乘法都可以构成半群和独异点；$\mathbf{Z}^+$关于普通乘法可以构成半群和独异点$\langle \mathbf{Z}^+, \times \rangle$，而关于普通加法只能构成半群$\langle \mathbf{Z}^+, + \rangle$ (单位元0没了).

对于普通加法，只有$\langle \mathbf{Z}, + \rangle$, $\langle \mathbf{Q}, + \rangle$, $\langle \mathbf{R}, + \rangle$是群，$\langle \mathbf{N}, + \rangle$不是群，因为$\mathbf{N}$中不是所有元素都有逆元.

对于普通乘法，只有$\langle \mathbf{Q}^+, \times \rangle$，$\langle \mathbf{R}^+, \times \rangle$是群，因为它们没有0，0关于普通乘法没有逆元.

(2) $n(n \geq 2)$阶实矩阵$M_n(\mathbf{R})$关于矩阵加法或矩阵乘法都能构成半群和独异点. 它不是群，因为不是所有的实矩阵都存在逆矩阵.

(3) 有穷字母表Σ上所有有限长度的字符串的集合Σ^*，关于串的连接运算$\circ$能构成半群和独异点. 其中，空串是单位元. 它不是群，因为除了空串外其他的串都没有逆元.

半群, 独异点与群

(4) 幂集$P(B)$关于集合的并，交和对称差运算都可以构成半群和独异点. 其中只有关于对称差的代数系统是群，因为对于任何$A \in P(B)$, A的逆元就是自身, 即$A \oplus A = \emptyset$.

(5) $\mathbf{Z}_n = \{0,1,\ldots,n-1\}$关于模$n$加法$\oplus$能构成半群和独异点. 它是群, 若$x = 0$, 则$x$的逆元就是$x$; 若$x \neq 0$, 则$n - x$就是$x$的逆元.

(6) $\langle \mathbf{R}^*, \circ \rangle$为半群, $\forall x, y \in \mathbf{R}^*$, $x \circ y = y$. 因为$\circ$是可结合的, 但是该半群没有单位元.

(7) A上所有关系的集合S关于关系的右复合运算$\circ$能构成半群和独异点. 其中, 恒等关系是单位元. 它不是群.

(8) S为任意非空集合, a为S中某个指定的元素, 且$\forall x, y \in S$, $x * y = a$, $\langle S, * \rangle$为半群.

半群, 独异点与群

例 6.2

- 令$G=\{e,a,b,c\}$, $\cdot$ 是G上的二元运算, 由上表给出.
- 在a,b,c中, 任两个元素运算结果等于第三个元素.
- 容易验证 $\cdot$ 运算是可结合的, e是G中的单位元, $\forall x\in G$, $x^{-1}=x$, G关于 $\cdot$ 运算构成一个群.
- 称这个群为Klein四元群.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

半群, 独异点与群

例 6.3

考虑模n加群$\langle \mathbf{Z}_n, \oplus \rangle$, 其中

$$\mathbf{Z}_n = \{0, 1, 2, \cdots, n-1\}, \forall x, y \in \mathbf{Z}_n,$$
$$x \oplus y = (x + y) \bmod n.$$

- 例如模6加群$\mathbf{Z}_6$, 其运算表如该表所示.
- 该表中, 上一行循环左移得下一行.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

半群, 独异点与群

例 6.6

设$N = \{1, 2, 3\}$, 如下定义N上的6个函数:

$$f_1 = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \{3, 3\rangle\}, \qquad f_2 = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 3, 3\rangle\},$$

$$f_3 = \{\langle 1, 3\rangle, \langle 2, 2\rangle, \langle 3, 1\rangle\}, \qquad f_4 = \{\langle 1, 1\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle\},$$

$$f_5 = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle\}, \qquad f_6 = \{\langle 1, 3\rangle, \langle 2, 1\rangle, \langle 3, 2\rangle\},$$

$$S = \{f_1, f_2, f_3, f_4, f_5, f_6\},$$

则S关于函数的右复合运算是否构成群?

解 构成群. 其单位元是恒等函数f_1;

f_1, f_2, f_3, f_4的逆元都是自身, f_5与f_6互为反函数, 即互为逆元.

群

定义

(1) 若群G为有穷集, 则称G为有限群, 否则称为无限群. 有限群G的元素数记作$|G|$, 称为G的阶.

(2) 若群G中只含有一个元素, 则称G为平凡群.

(3) 若群G中的二元运算是可交换的, 则称G为交换群或Abel群.

例

- $\langle \mathbf{Z}, +\rangle$, $\langle \mathbf{Q}, +\rangle$, $\langle \mathbf{R}, +\rangle$都是无限群, Klein四元群是4阶群.
- $\{0\}$关于普通加法构成平凡群, $\{1\}$关于普通乘法构成平凡群.
- Klein四元群和模n加群都是Abel群, 但是上例中的函数右复合群不是Abel群, 因为右复合不满足交换律.

群中元素的次幂

定义

对于任意整数n，群中元素x的n次幂x^n定义如下：

$$x^0 = e,$$
$$x^{n+1} = x^n x, n \in \mathbf{N},$$
$$x^{-n} = (x^{-1})^n.$$

注意此处n是自然数的条件. $n < 0$时没定义.

例 6.5 (1) $G = \langle \mathbf{Z}, + \rangle$，则

$$1^{-3} = (1^{-1})^3 = (-1)^3 = (-1) + (-1) + (-1) = -3,$$

$$(-4)^{-2} = \left((-4)^{-1}\right)^2 = 4^2 = 4 + 4 = 8.$$

(2) $G = \langle \mathbf{Z}_6, \oplus \rangle$，则

$$2^3 = 2 \oplus 2 \oplus 2 = 0,$$
$$2^{-4} = (2^{-1})^4 = 4^4 = 4 \oplus 4 \oplus 4 \oplus 4 = 4.$$

群中元素的阶

定义

G是群,设x是群的元素,使得$x^k=e$成立的**最小正整数k**,称为x的阶. 如果x的阶存在,则记作$|x|$. 如果不存在,则称x是无穷阶的.

- 在有限群G中,元素的阶一定存在,且是群G的阶的因子.
- **注意和群的阶进行区分.**
- 单位元e自身是1阶元,因为$e^1=e^0e=e$. 因此一个群里总是存在1阶元.

例 (1) 整数加群$\langle \mathbf{Z},+\rangle$中只有$|0|=1$,其他元素的阶都不存在.

(2) 模6加群$\langle \mathbf{Z}_6,\oplus\rangle$中,$|0|=1$, $|1|=|5|=6$, $|2|=|4|=3$, $|3|=2$.

(3) Klein四元群$G=\{e,a,b,c\}$中,e是1阶元,a,b和c都是2阶元,因为$\forall x\in G, x^2=e$.

群的基本性质

- 下面讨论群的性质，在一般情况下，可以省略二元运算符。

定理 6.1

设G为群，$m, n \in \mathbf{Z}$，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) $\forall a \in G, a^n a^m = a^{n+m}$,

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

证明

(1) $(a^{-1})^{-1}$是a^{-1}的逆元，a也是a^{-1}的逆元. 根据逆元的唯一性，命题得证.

群的基本性质

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

证明 只需证明$b^{-1}a^{-1}$是ab的逆元即可.

根据群的定义，以及逆元的定义有，

$$(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)b=b^{-1}eb=b^{-1}b=e,$$
$$(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aea^{-1}=aa^{-1}=e.$$

由此可见，$b^{-1}a^{-1}$是ab的逆元，命题得证.

- 通过归纳可推广:

$$(a_1a_2,\ldots,a_n)^{-1}=a_n^{-1}\ldots a_2^{-1}a_1^{-1}.$$

群的基本性质

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

证明

- 先考虑n和m都是自然数的情况. 任意给定n, 对m进行归纳.

  对于$m = 0$, 有

$$a^n a^0 = a^n e = a^n = a^{n+0}.$$

  假设$a^n a^m = a^{n+m}$成立, 考虑$m + 1$的情况, 则

$$a^n a^{m+1} = a^n(a^m a) = (a^n a^m)a = a^{n+m} a = a^{n+m+1}.$$

- 然后考虑n或m中存在负数的情况. 假设$n < 0, m \geq 0$, 令$n = -t, t \in \mathbf{Z}^+$, 则

$$a^n a^m = a^{-t} a^m = (a^{-1})^t a^m = \begin{cases} (a^{-1})^{t-m}(a^{-1})^m a^m = a^{m-t} = a^{n+m}, & t \geq m; \\ (a^{-1})^t a^t a^{m-t} = a^{(m-t)} = a^{n+m}, & t < m. \end{cases}$$

对于$n < 0, m < 0$或$n \geq 0, m < 0$的情况类似可证. 同理可证(4).

厦门大学信息学院 SCHOOL OF INFORMATICS XIAMEN UNIVERSITY 厦门大学计算机科学系 Computer Science Department of Xiamen University

群的基本性质

定理 6.2

G为群, $\forall a,b\in G$, 方程$ax=b$和$ya=b$在G中有解, 且有惟一解.

证明 $\forall a,b\in G$有

$$a(a^{-1}b)=(aa^{-1})b=b,$$

所以$a^{-1}b$是方程$ax=b$的一个解.

然后证明唯一性. 假设c是方程$ax=b$的任一解, 则

$$c=ec=(a^{-1}a)c=a^{-1}(ac)=a^{-1}b.$$

$ya=b$也可通过类似方法证明.

群的基本性质

例 6.6 $G=\langle P(S),\oplus\rangle$, 其中$S=\{1,2,3\}$, $\oplus$为集合的对称差运算. 求方程$\{1,2\}\oplus x=\{1,3\}$和方程$y\oplus\{1\}=\{2\}$的解.

解

$$x=\{1,2\}^{-1}\oplus\{1,3\}=\{1,2\}\oplus\{1,3\}=\{2,3\};$$
$$y=\{2\}\oplus\{1\}^{-1}=\{2\}\oplus\{1\}=\{1,2\}.$$

群的基本性质

定理 6.3

群中运算满足消去律, 即

$$ab = ac \Rightarrow b = c \text{ (左消去律)},$$

$$ba = ca \Rightarrow b = c \text{ (右消去律)}.$$

证明 $\forall a, b, c \in G$,

$$\begin{aligned} & ab = ac, \\ \Rightarrow\ & a^{-1}(ab) = a^{-1}(ac), \\ \Rightarrow\ & (a^{-1}a)b = (a^{-1}a)c, \\ \Rightarrow\ & b = c. \end{aligned}$$

同理可证右消去律.

群的基本性质

定理 6.4 (1)

G是群, $a \in G$, $k \in \mathbf{Z}$, 且$|a| = r$, 则$a^k = e$当且仅当$r|k$.

证明

- 必要性. 根据除法可构造$p, q \in \mathbf{Z}$, $0 \le q \le r-1$, 使得$k = pr + q$. 因为$a^k = e$, 所以有

$$e = a^k = a^{pr+q} = (a^r)^p a^q \ = a^q.$$

a的阶是r, 且$q < r$, 根据阶的定义可得$q = 0$, 这就证明了$r|k$.

- 充分性. 已知$r|k$, 即存在整数s, 使得$k = rs$. 所以有

$$a^k = a^{rs} = (a^r)^s = e^s = \ e.$$

群的基本性质

定理 6.4 (2)

G是群，$a \in G$且$|a| = r$，则$|a| = |a^{-1}|$.

证明

- 由$(a^{-1})^r = a^{-r} = (a^r)^{-1} = e$，可知$a^{-1}$的阶存在. 令$|a^{-1}| = t$，由(1)可得$t|r$.
- 另一方面，$a^t = \left((a^{-1})^t\right)^{-1} = e^{-1} = e$，由(1)可得$r|t$.
- 这就证明了$r = t$，即$|a| = |a^{-1}|$.

子群

定义6.3

(1) 设G是群, H是G的非空子集, 若H关于G中的运算构成群, 则称H为G的子群, 记作$H \le G$.

(2) 如果子群H是G的真子集, 则称H为G的真子群, 记作$H < G$.

(3) 若$H = \{e\}$或$H = G$, 则称H是G的平凡子群.

例 $\langle \mathbf{Z}, +\rangle$是$\langle \mathbf{Q}, +\rangle$, $\langle \mathbf{R}, +\rangle$的真子群, $\langle \mathbf{Q}, +\rangle$是$\langle \mathbf{R}, +\rangle$的真子群.
$\langle \{0\}, +\rangle$和$\langle \mathbf{R}, +\rangle$都是$\langle \mathbf{R}, +\rangle$的平凡子群.

子群判定定理

定理 6.5 (子群判定定理)

G是群，H是G的非空子集，则$H \leq G$当且仅当$\forall a, b \in H$有$ab^{-1} \in H$.

证明 必要性. 由子群的每一元素存在逆元和二元运算的封闭性得证.

充分性.

- 由H非空必存在$x \in H$. 根据充分条件, 则有$xx^{-1} \in H$, 即$e \in H$ (有单位元).
- 任取$a \in H$, 由$e, a \in H$, 再根据充分条件得$ea^{-1} = a^{-1} \in H$ (有逆元).
- 任取$a, b \in H$, 根据上面的证明有$b^{-1} \in H$. 再根据充分条件有$a(b^{-1})^{-1} \in H$, 即$ab \in H$ (二元运算结果封闭).

由于H显然满足结合律, 所以H是G的子群.

子群

例 6.9 G是群, $a \in G$, 令

k是整数, 可以为负

$$\langle a \rangle = \{a^k \mid k \in \mathbf{Z}\},$$

则$\langle a \rangle$是G的子群, 称为由a生成的子群.

证明 $a \in \langle a \rangle$, 所以$\langle a \rangle$是G的非空子集.

任取$a^i, a^j \in \langle a \rangle$, $i, j \in \mathbf{Z}$, 有

$$a^i \left(a^j\right)^{-1} = a^i\, a^{-j} = a^{i-j} \in \langle a \rangle.$$

由子群判定定理得$\langle a \rangle \leq G$.

厦门大学信息学院 SCHOOL OF INFORMATICS XIAMEN UNIVERSITY 厦门大学计算机科学系 Computer Science Department of Xiamen University

子群

例

- $G=\langle \mathbf{Z},+\rangle$由2生成的子群$\langle 2\rangle$包含2的所有的倍数, 即

$$\langle 2\rangle = 2\mathbf{Z} = \{2k \mid k \in \mathbf{Z}\}.$$

- $G=\langle \mathbf{Z}_6,\oplus\rangle$, 则

$$\langle 1\rangle = \langle 5\rangle = \mathbf{Z}_6 = \{0,1,2,3,4,5\},$$
$$\langle 2\rangle = \langle 4\rangle = \{0,2,4\},$$
$$\langle 3\rangle = \{0,3\},$$
$$\langle 0\rangle = \{0\}.$$

- Klein四元群$G=\{e,a,b,c\}$, 它的元素生成的子群为:

$$\langle e\rangle = \{e\},\qquad \langle a\rangle = \{e,a\},\qquad \langle b\rangle = \{e,b\},\qquad \langle c\rangle = \{e,c\}.$$

子群

例 6.10 设G是群, 令C是与G中所有元素都可交换的元素构成的集合, 即

$$C = \{a \mid a \in G \text{ 且 } \forall x \in G, xa = ax\},$$

则C是G的子群, 叫做G的中心.

证明 $\forall x \in G, ex = xe$, 显然$e \in C$, 且C非空.

$\forall a, b \in C$, 为了使用判定定理证明$C \leq G$, 只需证明$\forall x \in G, ab^{-1}$与x可交换.

$$(ab^{-1})x = ab^{-1}(x^{-1})^{-1}$$

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

$$= (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}).$$

所以$ab^{-1} \in C$. 由判定定理有$C \leq G$.

- 群G的中心有大小, 有的群的中心只含有一个单位元e, 而有的群的中心就是群G, 如Abel群.

子群

例 6.11 (1) G是群, H和K是G的子群, 则$H \cap K \ \le \ G$.

证明 因为H和K都是G的子群, 所以$e \in H \cap K$, 且$H \cap K$非空.

任取$a, b \in H \cap K$, 则$a, b \in H$, $a, b \in K$.

又由于H和K是G的子群, 所以$b^{-1} \in H$, $b^{-1} \in K$.

这就得到$ab^{-1} \in H$和$ab^{-1} \in K$, 即$ab^{-1} \in H \cap K$.

由判定定理有$H \cap K \le G$.

子群

例 6.13 (2) G是群, H和K是G的子群, 则$H \cup K \leq G$当且仅当$H \subseteq K$或$K \subseteq H$.

证明 充分性显然, 充分条件成立时, $H \cup K = H$或$H \cup K = K$.

必要性通过反证法, 假设$H \nsubseteq K$且$K \nsubseteq H$,

则存在$h \in H$且$h \notin K$, 同时存在$k \in K$且$k \notin H$.

可得$hk \notin H$, 否则$k = h^{-1}(hk) \in H$, 产生矛盾. 同理$hk \notin K$.

因此$hk \notin H \cup K$, 但是$h, k \in H \cup K$, 与$H \cup K \leq G$矛盾.

子群

- 由上例可知，子群的并集不一定是子群.
- 对于子群H和K，为了得到包含H和K的最小的子群，往往需要在$H \cup K$中添加一些G中的其他元素，以使得$H \cup K$对于G中的运算封闭.
- 类似的例子是满足传递性的关系的并集.

例 Klein四元群G有子群$\langle a \rangle$和$\langle b \rangle$，那么$\langle a \rangle \cup \langle b \rangle = \{a, b, e\}$，这不是$G$的子群，因为$ab = c$，$c$不在这个集合中.

为了满足封闭性，必须把c加进去，因此包含$\langle a \rangle$和$\langle b \rangle$的最小的子群就是G自身.

子群格

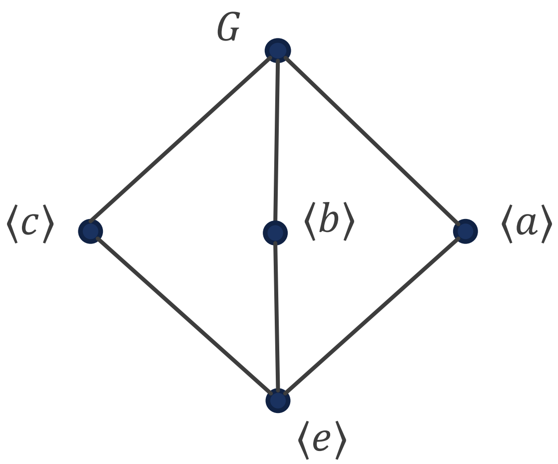
定义

设G是群, 令$S = \{H | H \le G\}$, 在S上定义偏序关系,

$$\forall A, B \in S, A \preccurlyeq B \Leftrightarrow A\text{是}B\text{的子群}.$$

那么$(S, \preccurlyeq)$构成偏序集, 称为群G的子群格.

例 $G = \{e, a, b, c\}$是Klein四元群, G的子群是$\langle e \rangle = \{e\}, \langle a \rangle = \{e, a\}, \langle b \rangle = \{e, b\}$, $\langle c \rangle = \{e, c\}$和$G$. 子格群如图所示.



子群格

例 $G=\langle \mathbf{Z}_{12},\oplus\rangle$为模12加群, G有6个子群:

$H_1=\{0\}=\langle 0\rangle$,

$H_2=\{0,6\}=\langle 6\rangle$,

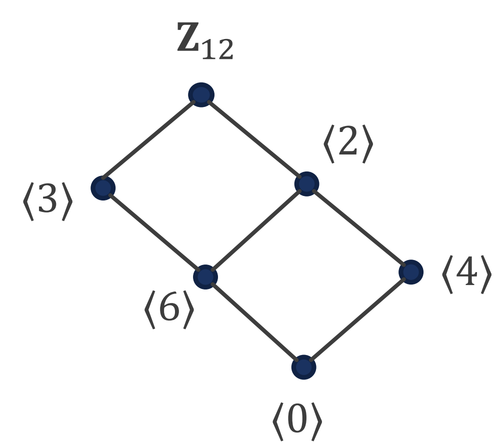
$H_3=\{0,4,8\}=\langle 4\rangle=\langle 8\rangle$,

$H_4=\{0,3,6,9\}=\langle 3\rangle=\langle 9\rangle$,

$H_5=\{0,2,4,6,8,10\}=\langle 2\rangle=\langle 10\rangle$,

$G=\mathbf{Z}_{12}=\{0,1,2,3,4,5,6,7,8,9,10,11\}$

$\quad=\langle 1\rangle=\langle 5\rangle=\langle 7\rangle=\langle 11\rangle$.



- G的子群格如图所示.
- a和逆元$12-a$必在同一子群, $\langle a\rangle=\langle 12-a\rangle$.

循环群

定义 6.4

(1) 设G是群, 若存在$a \in G$使得G和它由a的生成子群相等, 即$G = \langle a \rangle$, 则称G为循环群, 称a是G的生成元.

(2) 在循环群$\langle a \rangle$中, 若$|a| = n$, 且$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$中都是不等的元素, 叫做有限循环群或$n$阶循环群.

(3) 若$|a|$不存在, 则$\langle a \rangle = \{e, a, a^2, \ldots\}$是无限的, 则称为无限循环群.

- 判断a是否是G的生成元就是判断a^k是否涵盖所有G里的元素.

例 整数加群$\langle \mathbf{Z}, + \rangle$是无限阶循环群, 1是它的一个生成元;

模n加群$\langle \mathbf{Z}_n, \oplus \rangle$是$n$阶循环群, 1也是它的一个生成元.

循环群

- 对于循环群，一个重要问题是**它有几个生成元**? **有哪些生成元**?

定义

设n是正整数，欧拉函数$\varphi(n)$是小于等于n且与n互质的正整数的个数.

例 $\varphi(1)=1, \varphi(2)=1, \varphi(3)=2, \varphi(4)=2, \varphi(5)=4, \varphi(6)=2$.

例 $n=12$, 小于等于12且与12互质的正整数是1, 5, 7和11, 因此 $\varphi(12)=4$.

- 若p是素数，则$\varphi(p)=p-1$.

循环群的生成元

定理 6.6

设$G=\langle a\rangle$是循环群,

(1) 若G是无限阶循环群, 则G只有两个生成元a和a^{-1}.

(2) 若G是n阶循环群, 则G有$\varphi(n)$个生成元, 对于每个小于等于n且与n互质的正整数r, a^r都是G的生成元.

例 6.13 (1) $G=\langle a^2\rangle$是无限循环群, 其生成元为a^2, a^{-2}.

(2) 模20加群$G=\langle \mathbf{Z}_{20},\oplus\rangle$是有限循环群, 小于20且与20互质的正整数为1, 3, 7, 9, 11, 13, 17, 19, 根据定理, 这些都是生成元.

循环群的子群

定理 6.7 设$G = \langle a \rangle$是循环群, 那么

(1) G的子群也是循环群;

(2) 若G是无限循环群, 则G的子群除$\{e\}$外都是无限阶的;

(3) 若G是n阶循环群, 那么对于n的每个正因子d, G有一个d阶循环子群.

- 定理6.7(3)说明对于n的每个正因子d, n阶循环群G有且仅有一个d阶子群, 但是没有说明G是否还有其他阶的子群.
- Lagrange定理回答了这个问题, 对于n阶群G, **G的子群的阶和G中元素的阶都是n的因子**.
- 因此, 对于n阶循环群G, 只要找出n的所有正因子, 就可以求出G的所有子群.

循环群生成元和子群的个数

- 对于无限阶循环群G:
  - 生成元的个数 = 2.
  - 子群的个数 = 无限.
- 对于n阶循环群G:
  - 生成元的个数 = $\varphi(n)$, 小于等于n且与n互质的正整数的个数.
  - 子群的个数 = 正因子的个数.

循环群

例 6.14 (1) 求无限循环群$G = \langle a \rangle$的所有的子群.

解 G有无数个子群, 分别为:

$$\langle e \rangle = \{e\},$$
$$\langle a \rangle = \langle a^{-1} \rangle = \langle a^k | k \in \mathbf{Z} \rangle = G,$$
$$\langle a^2 \rangle = \langle a^{-2} \rangle = \{e, a^{\pm 2}, a^{\pm 4}, a^{\pm 6}, \dots\}$$
$$\langle a^3 \rangle = \langle a^{-3} \rangle = \{e, a^{\pm 3}, a^{\pm 4}, a^{\pm 6}, \dots\}$$

循环群

例 6.14 (2) 求12阶循环群$G = \langle a \rangle$的所有生成元和子群.

解 $\varphi(12) = 4$, 因此G有4个生成元, 分别是$\{a, a^5, a^7, a^9\}$. 12的正因子为1, 2, 3, 4, 6, 12, 因此G有6个子群:

$$\langle e \rangle = \{e\},$$
$$\langle a \rangle = \langle a^k | k \in \mathbf{Z} \rangle = G,$$
$$\langle a^2 \rangle = \{e, a^2, a^4, a^6, a^8, a^{10}\},$$
$$\langle a^3 \rangle = \{e, a^3, a^6, a^9\},$$
$$\langle a^4 \rangle = \{e, a^4, a^8\},$$
$$\langle a^6 \rangle = \{e, a^6\}.$$

- 那么负次幂元素生成的子群, 例如$\langle a^{-2} \rangle$, 以及非正因子生成的子群, 例如$\langle a^{10} \rangle$是什么呢?

循环群

- 由于$G=\langle a\rangle$是12阶有限循环群, $a^{12}=e$.

$$\langle a^{-2}\rangle=\langle a^{-2}e\rangle=\langle a^{-2}a^{12}\rangle=\langle a^{10}\rangle.$$

- 根据生成的子群的定义:

$$\langle a^{10}\rangle=\{a^{20}=a^{8},a^{18}=a^{6},a^{16}=a^{4},a^{14}=a^{2},a^{12}=e,a^{10}\}$$
$$=\{e,a^{2},a^{4},a^{6},a^{8},a^{10}\}=\langle a^{2}\rangle.$$

- 以此类推可得$\langle a^{10}\rangle=\langle a^{2}\rangle,\langle a^{9}\rangle=\langle a^{3}\rangle,\langle a^{8}\rangle=\langle a^{4}\rangle,\langle a\rangle=\langle a^{11}\rangle$.

- 那么剩下的$\langle a^{5}\rangle$和$\langle a^{7}\rangle$呢?

课堂练习

求模15加群$G = \langle \mathbf{Z}_{15}, \oplus \rangle$的所有生成元和子群, 并画出$G$的子群格.

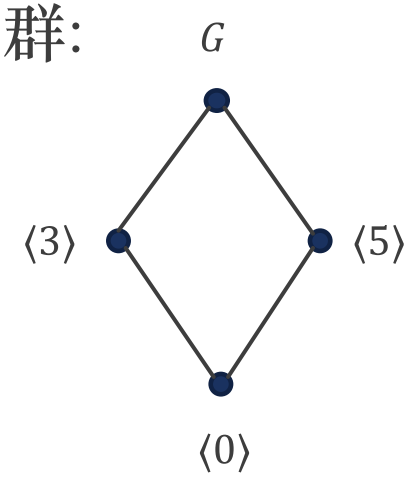
课堂练习

求模15加群$G=\langle \mathbf{Z}_{15},\oplus\rangle$的所有生成元和子群, 并画出$G$的子群格.

解 与15互质的正整数为1, 2, 4, 7, 8, 11, 13, 14, 这些都是生成元.

G是阶是15, 正因子为1, 3, 5, 15. 所以G有4个子群:

$$\langle 0\rangle=\{0\},$$
$$\langle 1\rangle=G,$$
$$\langle 3\rangle=\{0,3,6,9,12\},$$
$$\langle 5\rangle=\{0,5,10\}.$$



置换

定义 6.5

设$N=\{1,2,\dots,n\}$, 如果$\sigma\colon N\to N$是双射函数, 则称σ为N上的n元置换. n元置换通常采用置换符号表示, 即

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

- 易见$\sigma(1),\sigma(2),\dots,\sigma(n)$恰为$\{1,2,\dots,n\}$的一个排列, 其本质是一个双射函数:

$$\{\langle 1,\sigma(1)\rangle,\langle 2,\sigma(2)\rangle,\dots,\langle n,\sigma(n)\rangle\}.$$

- N上的所有置换和N的所有排列之间存在着一一对应.
- 当$|N|=n$时, n元集有$n!$个排列, 所以有$n!$个n元置换.
- 所有这些置换的集合记作S_n.

置换

例 $S_3=\{\sigma_1,\sigma_2,\dots,\sigma_6\}$, 其中

$$\sigma_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \sigma_2=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \sigma_3=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},$$

$$\sigma_4=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \sigma_5=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \sigma_6=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}.$$

轮换

- n元置换还可以用轮换来表示，这种表示方法更为简洁.

定义 6.6

设σ是n元置换，如果

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

并且保持N中的其它元素不变，则称σ是k阶轮换，记作

$$\sigma=(i_1 i_2 \ldots i_k).$$

- 由定义：在上述轮换中，不论用哪个文字作为起始文字，只要文字的顺序不变，它们都代表同一个轮换.

$$(1\ 3\ 6\ 4\ 2)=(3\ 6\ 4\ 2\ 1)=(6\ 4\ 2\ 1\ 3)=(4\ 2\ 1\ 3\ 6)=(2\ 1\ 3\ 6\ 4)$$

轮换

例 S_3的6个置换如果采用轮换表示, 则有

$$\sigma_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=(1)(2)(3),\quad \sigma_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(2\ 3)(1),$$

$$\sigma_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(1\ 2)(3),\quad \sigma_4=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(1\ 3)(2),$$

$$\sigma_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(1\ 2\ 3),\quad \sigma_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(1\ 3\ 2).$$

1阶轮换在表示时可以省略, 但是如果分解式中全都是1阶轮换, 则需要保留一个.

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

轮换

定义

设$\sigma_1 = (i_1 i_2 \dots i_k)$和$\sigma_2 = (j_1 j_2 \dots j_s)$是两个轮换. 若$\{i_1 i_2 \dots i_k\} \cap \{j_1 j_2 \dots j_s\} = \emptyset$, 则称$\sigma_1$与$\sigma_2$是不相交的.

例 6.15 设σ, τ是8元置换, 且

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

写出σ和τ的不相交轮换表示.

解 先从σ中取出1, $\sigma(1) = 5, \sigma(5) = 7, \sigma(7) = 2, \sigma(2) = 6, \sigma(6) = 3, \sigma(3) = 1$, 这就得到第一个轮换$(1\ 5\ 7\ 2\ 6\ 3)$.

然后从剩下的元素中取出4, $\sigma(4) = 4$, 再取出8, $\sigma(8) = 8$.

由于$\sigma(4) = 4$和$\sigma(8) = 8$都是在σ作用下保持不变的文字, 即1阶轮换, 可以省略, 因此可写成$\sigma = (1\ 5\ 7\ 2\ 6\ 3)$.

同理可得$\tau = (1\ 2\ 3\ 7\ 8)(4\ 5\ 6)$.

轮换

- (1 2 3 7 8)(4 5 6)称为轮换之积, 是两个轮换经过右复合运算后得到的结果.
- 任何n元置换在分解成不交的轮换之积时, 分解式是唯一的.

定理

设$\sigma, \tau \in S_n$, 若σ与τ是不相交的, 则$\sigma\tau = \tau\sigma$.

例 在S_5中, $\sigma = (134)$, $\tau = (25)$是不相交的.

例 在S_5中,

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

(5 2 3)(1 4)和(1 4)(5 2 3)都是同一个轮换.

课堂练习

用轮换表示写出S_4的所有元素.

课堂练习

用轮换表示写出S_4的所有元素.

解 S_4的元素个数为$4! = 24$:

1234	(1)	2134	(1 2)	3124	(1 3 2)	4123	(1 4 3 2)
1243	(3 4)	2143	(1 2)(3 4)	3142	(1 3 4 2)	4132	(1 4 2)
1324	(2 3)	2314	(1 2 3)	3214	(1 3)	4213	(1 4 3)
1342	(2 3 4)	2341	(1 2 3 4)	3241	(1 3 4)	4231	(1 4)
1423	(2 4 3)	2413	(1 2 4 3)	3412	(1 3)(2 4)	4312	(1 4 2 3)
1432	(2 4)	2431	(1 2 4)	3421	(1 3 2 4)	4321	(1 4)(2 3)

置换群

定义

设σ与τ是n元置换，由于n元运算是从N到N的双射函数，经过右复合运算后所得结果仍是N到N的双射函数，称这个右复合运算为置换乘法，所得结果为σ,τ之积，记作$\sigma\tau$.

- N上的恒等置换(1)是置换乘法运算的单位元.
- 每个n元置换的逆都存在，因为双射函数有反函数，其依然是N上的双射函数.
- n元置换的乘法在S_n上是封闭的，并且满足交换律，即$\sigma\tau = \tau\sigma$.
- 封闭的，满足结合律，有单位元，每个元素都有逆元，因此S_n关于置换的乘法构成一个群，称为n元对称群. S_n的子群称为n元置换群.

置换群

例 6.17 $S_3 = \{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$, 那么3元对称群的运算表如下:

置换乘法	(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)

置换群

- 因此, S_3的6个子群列出如下:
  - 1阶子群: $\{(1)\}$,
  - 2阶子群: $\{(1), (1\ 2)\}, \{(1), (1\ 3)\}, \{(1), (2\ 3)\}$,
  - 3阶子群: $\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$,
  - 6阶子群: S_3.
- 它们都是3元置换群.

对称群有生成元吗?

课堂练习

设σ,τ是8元置换，且

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

(1) 给出σ,τ的轮换表示.

(2) 求σ与τ之积$\sigma\tau$.

课堂练习

设σ,τ是8元置换，且

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

(1) 给出σ,τ的轮换表示.

(2) 求σ与τ之积$\sigma\tau$.

解

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

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

环

- 半群, 独异点和群是只有一个二元运算的代数系统.
- 环和域是具有两个二元运算的代数系统.

定义 6.7

设$\langle R, +, \cdot \rangle$是具有两个二元运算的代数系统, 如果:

(1) $\langle R, + \rangle$构成Abel群,

(2) $\langle R, \cdot \rangle$构成半群,

(3) $\cdot$ 对$+$满足分配律,

则称$\langle R, +, \cdot \rangle$是环, 并称$+$和 $\cdot$ 分别为R中的加法和乘法.

- 环只对$+$是群, 对 $\cdot$ 不是群.
- 分配律把两个二元运算联系在一起.
- 乘法运算符 $\cdot$ 通常可省略, 例如$a \cdot b$可写作ab.

环

例6.18 (1) **Z**, **Q**, **R**, **C**关于普通数的加法+和乘法×都构成环, 分别称为整数环, 有理数环, 实数环, 复数环.

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

(3) $\langle \mathbf{Z}_n, \oplus, \otimes \rangle$构成一个环, 称为模$n$整数环, 其中$\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$, $\oplus$和$\otimes$分别表示模n加法和模n乘法:

$$x \oplus y = (x + y) \bmod n,$$

$$x \otimes y = (xy) \bmod n.$$

(4) $\langle P(B), \oplus, \cap \rangle$构成一个环, 其中$\oplus$是集合的对称差运算. 但是$\langle P(B), \oplus, \cup \rangle$不构成一个环, 因为$\cup$运算对$\oplus$运算不分配.

环

为了叙述方便, 作出以下定义.

- 环中加法的单位元记作0, 元素x关于加法的逆元称为x的负元, 记作$-x$.
- 如果环中乘法有单位元, 记作1. 如果x关于乘法存在逆元, 记作x^{-1}.
- 类似地, 可以用$x-y$表示$x+(-y)$.

域

定义

考虑环中两个元素a和b, $a \neq 0$, $b \neq 0$, 但是$ab = 0$, 则称a和b分别为环中的左零因子和右零因子.

定义 6.8

设$\langle R, +, \cdot \rangle$是环,

(1) 若R中乘法适合交换律, 则称R是交换环.

(2) 若R中存在乘法的单位元, 则称R是含幺环.

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

- (3)的等价定义为：设R是一个是环，如果R中任意非0元素a和b，都有$ab \neq 0$，则称$\langle R, +, \cdot \rangle$是无零因子环.

例 在模6的整数环$\langle \mathbf{Z}_6, \oplus, \otimes \rangle$中，$2 \otimes 3 = 0$，但是2和3都不是0，因此它们是零因子. 这个环含有零因子, 不是无零因子环.

域

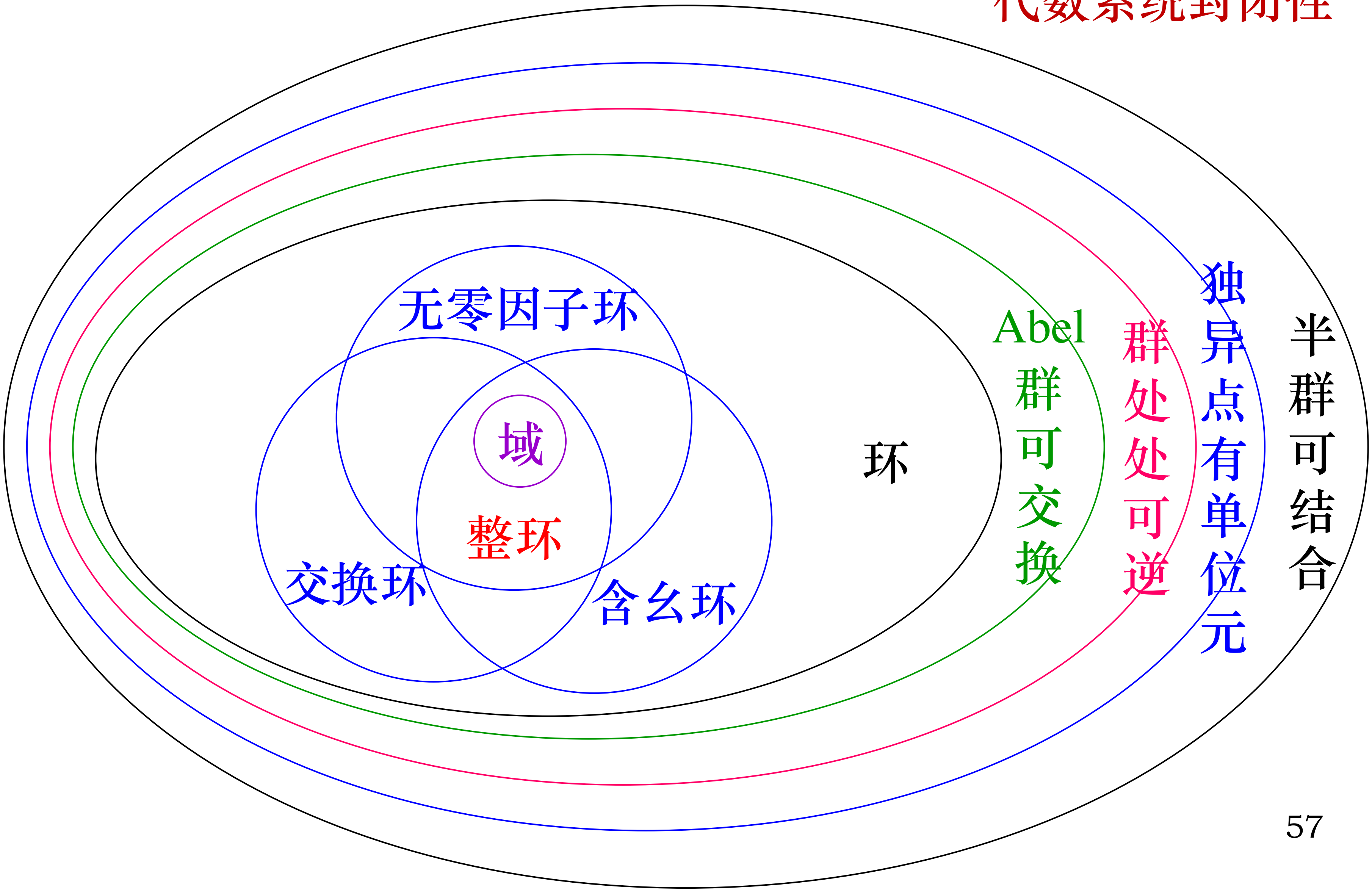
定义 6.8

设$\langle R, +, \cdot \rangle$是环,

(4) 若R是交换的含幺的无零因子环, 则称R是整环;

(5) 若R是整环, R至少含有两个元素, 且$\forall a \in R^* = R - \{0\}$, 都有$a^{-1} \in R$, 则称$R$是域.

代数系统封闭性



域

例 6.19 (1) 整数环, 有理数环, 实数环中的乘法适合交换律, 含有单位元1, 不含零因子, 因此它们都是交换环, 含幺环, 无零因子环和整环.

其中有理数环, 实数环也是域, 因为$a(a \neq 0)$存在乘法逆元, 就是它的倒数$1/a$.

但是整数环不是域, 因为很多整数的倒数不再是整数.

(2) 模n整数环$\langle \mathbf{Z}_n, \oplus, \otimes \rangle$是交换环, 含幺环. 当$n$为素数时可以证明$\mathbf{Z}_n$构成域; 当$n$为合数时不构成整环和域.

例如合数$n = pq$, p和q是大于1的整数, 那么$p \otimes q = 0$, p和q是零因子.

域

例6.24 (3) 设$n \geq 2$, n阶实矩阵环$\langle M_n(\mathbf{R}), +, \cdot \rangle$不是交换环, 因为矩阵乘法不可交换.

但它是含幺环, 单位矩阵是乘法的单位元.

它不是无零因子环, 因为存在两个非零矩阵相乘为零矩阵的情况, 这样的非零矩阵分别为左零因子和右零因子. 因此它也不是整环和域.

域

例 6.29 判断下述集合关于数的加法和乘法是否构成环, 整环和域.

(1) $A=\{a+b\sqrt{2} \mid a,b\in\mathbf{Z}\}$;

(2) $A=\{a+b\sqrt{3} \mid a,b\in\mathbf{Q}\}$;

(3) $A=\{a+b\sqrt[3]{2} \mid a,b\in\mathbf{Z}\}$;

(4) $A=\{a+bi \mid a,b\in\mathbf{Z}, i^2=-1\}$.

解 (1) 是环和整环, 但不是域, 因为$\sqrt{2}$对于乘法没有逆元.

(2) 是环, 整环和域.

(3) 不是环, 因为A关于乘法不封闭.

(4) 是环和整环, 但不是域, 因为$2i$对于乘法没有逆元. (但是i有逆元)

域

- 域是一类重要的代数系统, 一般常把域表示为$\langle F, +, \cdot \rangle$.
- 域中的运算有着非常良好的性质. 其中$\langle F, + \rangle$构成Abel群, $+$有交换律, 结合律, 单位元, 每个元素都有负元;
- $\langle F, \cdot \rangle$也构成Abel群, $\cdot$也有交换律, 结合律, 单位元, 除了零以外, 每个元素都有逆元.
- 此外, 乘法对加法还有分配律. 正由于这些良好的性质, 域有着广泛的应用. 特别是伽罗华域$GF(p)$在密码学中是很重要的基础.

6.2 格与布尔代数

格

- 格和布尔代数是具有两个二元运算的代数系统，布尔代数是格的特例.
- 与前面讨论的代数系统之间存在着一个重要区别：格与布尔代数的载体都是偏序集.

上界与下界

定义4.26

设$\langle A, \preccurlyeq \rangle$为偏序集, $B \subseteq A$, $y \in A$.

(1) 若$\forall x(x \in B \rightarrow x \preccurlyeq y\}$成立, 则称$y$为$B$的上界.

(2) 若$\forall x(x \in B \rightarrow y \preccurlyeq x\}$成立, 则称$y$为$B$的下界.

(3) 令$C = \{y |\ y$是B的上界$\}$, 则称C的最小元为B的最小上界或上确界.

(4) 令$C = \{y |\ y$是B的下界$\}$, 则称C的最大元为B的最大下界或下确界.

- 当B中仅含一个元素时, $x \preccurlyeq y$也可以直接看做y是x的上界, 或者x是y的下界.

格

定义 6.9

设$\langle S, \preccurlyeq \rangle$是偏序集, 若对于$\forall x, y \in S$, $\{x, y\}$都有最小上界和最大下界, 则称S关于偏序$\preccurlyeq$作成一个格.

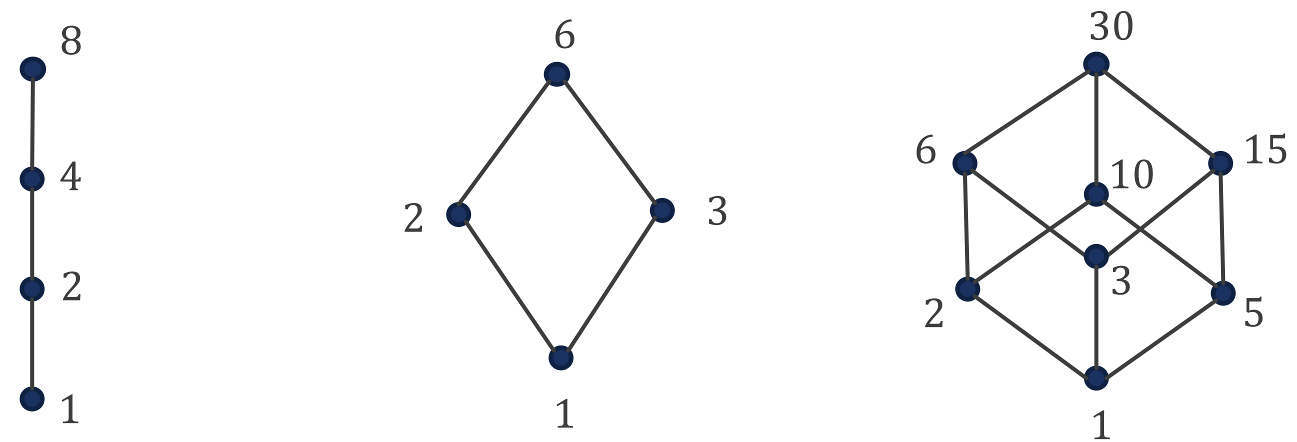
设x, y是格中任意两个元素, 由于$\{x, y\}$的最大下界和最小上界是惟一存在的, 将$\{x, y\}$的最大下界记作$x \wedge y$, 最小上界记作$x \vee y$.

- 偏序$\preccurlyeq$是一个二元关系, 不是二元运算. 格是特殊的偏序集.
- 本章中的$\wedge$和$\vee$符号只代表格中求最大下界 (读作取小) 和最小上界 (读作取大) 的运算, 不再具有逻辑上的析取或合取的含义.
- 对给定的偏序集, 可以先画出哈斯图, 直接由哈斯图来判断它是否构成格, 即考虑任何两个元素是否有最小上界和最大下界同时存在.

格

例 6.20 设$n \in \mathbf{Z}^+$, S_n是n的正因子的集合, $|$为整除关系, 则$\langle S_n, D\rangle$构成格.

$\forall x, y \in S_n$, $x \vee y$是x与y的最小公倍数, $x \wedge y$是x与y的最大公约数. 下图给出了格$\langle S_8, |\rangle$, $\langle S_6, |\rangle$和$\langle S_{30}, |\rangle$.

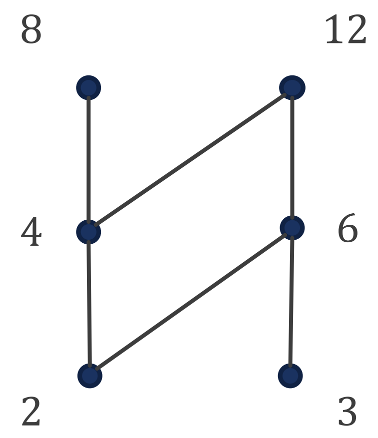


$\langle S_8, |\rangle$ $\langle S_6, |\rangle$ $\langle S_{30}, |\rangle$

格

例 $A=\{2,3,4,6,8,12\}$, $\preccurlyeq$是整除关系，A不是格.

因为2和3没有最大下界, 8和12没有最小上界.



格

例 6.26 (1) $P(B)$是集合B的幂集, $\langle P(B), \subseteq\rangle$构成一个格, 称为幂集格.

因为$\forall x, y \in P(B)$, 设$x \vee y = x \cup y, x \wedge y = x \cap y$. 由于$\cup$和$\cap$运算在$P(B)$上是封闭的, 所以$x \cup y, x \cap y \in P(B)$.

(2) $\leq$为小于等于关系, 则$\langle \mathbf{Z}, \leq\rangle$是格.

因为$\forall x, y \in \mathbf{Z}$, 设$x \vee y = \max\{x, y\}, x \wedge y = \min\{x, y\}$, 它们都是整数.

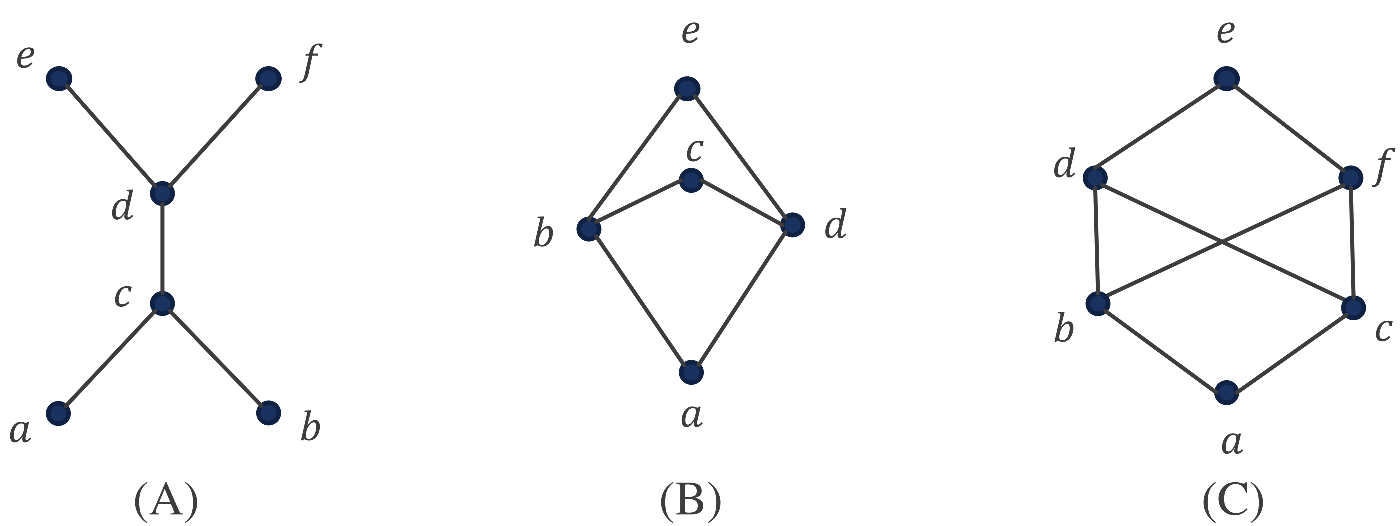
格

例 6.26 (3) 图中给出的偏序集都不是格.

(A) 中的$\{e, f\}$没有最小上界, $\{a, b\}$没有最大下界.

(B) 中的$\{b, d\}$有上界c和e, 但没有最小上界.

(C) 中的$\{b, c\}$有三个上界d, e和f, 但没有最小上界.



格

定义

设$\langle S,\preccurlyeq\rangle$是格，$f$是由格中元素及$\preccurlyeq$，$=$，$\succcurlyeq$，$\wedge$，$\vee$等符号所表示的公式，如果将$f$中的$\preccurlyeq$和$\succcurlyeq$相互替换，$\wedge$和$\vee$相互替换后得到的公式为$f^*$. 称为$f$的对偶式，简称对偶. 根据格的对偶原理，若$f$对一切格为真，则$f^*$也对一切格为真.

例 若f是$a\wedge b\preccurlyeq a$，那么f 的对偶式f^*是$a\vee b\succcurlyeq a$.

若f是$a\wedge(a\vee b)=a$，那么f的对偶式f^*是$a\vee(a\wedge b)=a$.

格中运算的性质

定理 6.8 (1)

设$\langle L, \preccurlyeq\rangle$为格，则运算$\vee$和$\wedge$适合交换律，即$\forall a, b \in L$有

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

证明 $a \vee b$是$\{a, b\}$的最小上界，$b \vee a$是$\{b, a\}$的最小上界，由于$\{a, b\} = \{b, a\}$，且最小上界是唯一的，所以$a \vee b = b \vee a$. 同理可证$a \wedge b = b \wedge a$.

格中运算的性质

定理 6.8 (3)

设$\langle L, \preccurlyeq \rangle$为格，则运算$\vee$和$\wedge$适合幂等律，$\forall a \in L$有

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

证明

可以通过偏序关系的反对称性进行证明$a \vee a = a$，即

$$a \preccurlyeq a \vee a \text{且} a \vee a \preccurlyeq a \Rightarrow a \vee a = a.$$

- 首先证明$a \preccurlyeq a \vee a$. 因为$\forall x \in L$, $a \vee x$是a的最小上界，也是a的上界，因此$a \preccurlyeq a \vee x$.
- 再证明$a \vee a \preccurlyeq a$. 由偏序关系的自反性$a \preccurlyeq a$，即a是自身的上界之一. $a \vee a$是所有a的上界中最小的，所以可得$a \vee a \preccurlyeq a$.
- 根据偏序关系的反对称性可证$a \vee a = a$.

同理可证$a \wedge a = a$.

格中运算的性质

定理 6.8 (2)

设$\langle L,\preccurlyeq\rangle$为格，则运算$\vee$和$\wedge$适合结合律，即$\forall a,b,c\in L$有

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

证明 由最小上界的定义有

$$(a\vee b)\vee c\succcurlyeq a\vee b\succcurlyeq a, \qquad ①$$

$$(a\vee b)\vee c\succcurlyeq a\vee b\succcurlyeq b, \qquad ②$$

$$(a\vee b)\vee c\succcurlyeq c. \qquad ③$$

由②和③可得，$(a\vee b)\vee c$是$\{b,c\}$的上界，$\{b,c\}$的最小上界$b\vee c$是所有上界中的最小元，所以

$$(a\vee b)\vee c\succcurlyeq b\vee c.$$

同理，再根据①可得，$(a\vee b)\vee c$是$\{b\vee c,a\}$的上界，所以$(a\vee b)\vee c\succcurlyeq(b\vee c)\vee a$.

同理可证，$(a\vee b)\vee c\preccurlyeq(b\vee c)\vee a$，根据反对称性可得

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

再次同理可证$(a\wedge b)\wedge c=a\wedge(b\wedge c)$.

格中运算的性质

定理 6.8 (4)

设$\langle L, \preccurlyeq\rangle$为格，则运算$\vee$和$\wedge$适合吸收律，即$\forall a, b \in L$有

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

证明 由$\forall x \in L, a \preccurlyeq a \vee x$，可得

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

同理，由$\forall x \in L, a \wedge x \preccurlyeq a$，可得

$$a \wedge b \preccurlyeq a.$$

又由$a \preccurlyeq a$和$a \wedge b \preccurlyeq a$，可得$a$是$\{a, a \wedge b\}$的上界，最小上界是上界中的最小元，所以

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

根据反对称性可得$a \vee (a \wedge b) = a$，同理可证$a \wedge (a \vee b) = a$.

格与代数系统

- 很明显，格L与运算$\wedge$和$\vee$构成代数系统$\langle L, \wedge, \vee\rangle$. 定理6.8说明格中的运算$\wedge$和$\vee$遵从交换律，结合律，幂等律和吸收律.
  - 这个代数系统是先确定了偏序关系，再定义二元运算的.
- 考虑一个相反的问题，能不能像群和环一样，通过规定集合，集合上的运算及运算所遵从的算律来给出格作为代数系统的定义呢?
  - 也就是说，有没有一个代数系统，满足一些性质，就成为了格?
- 回答是肯定的. 但是这样定义的格中的偏序关系是什么? 而这个通过偏序集定义的格所导出的代数系统和原来的代数系统有什么关系呢?

格与代数系统

定理6.9

设$\langle S,*,\circ\rangle$是具有两个二元运算的代数系统．若$*$和$\circ$运算适合交换律，结合律和吸收律，则可以适当定义S上的偏序关系$\preccurlyeq$，使得$\langle S,\preccurlyeq\rangle$构成一个格，且$\langle S,\preccurlyeq\rangle$导出的代数系统$\langle S,\wedge,\vee\rangle$就是$\langle S,*,\circ\rangle$.

- 也就是说，适合交换律，结合律和吸收律的代数系统$\langle S,*,\circ\rangle$可以**构造出**偏序关系$\preccurlyeq$和一个格$\langle S,\preccurlyeq\rangle$．$*$运算和$\circ$运算分别对应$\wedge$运算和$\vee$运算.

格与代数系统

证明

要证明$\langle S,*,\circ\rangle$可以通过某种构造的方式称为格，需要三步：

1. 通过定义二元运算$*$或$\circ$构造出一个二元关系$\preccurlyeq$.

2. 证明该二元关系$\preccurlyeq$是偏序关系（自反，反对称，传递）.

3. 证明$\langle S,\preccurlyeq\rangle$构成格，即该定义下的二元运算$*$和$\circ$就是最大下界和最小上界.

证明

(1) 首先通过定义$\circ$运算来定义二元关系$\preccurlyeq$, $\forall a, b \in S$:

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

下面依次通过自反性, 反对称性和传递性证明$\preccurlyeq$是偏序关系.

格与代数系统

(2)证明该二元关系$\preccurlyeq$是偏序关系(自反,反对称,传递).

- 首先证明$\preccurlyeq$在S上的自反性,即$a \preccurlyeq a$. 通过定义可得等价证明$a \circ a = a$,即$\circ$适合幂等律.

$\forall a \in S$,通过吸收律$a = a * (a \circ b)$,可得:

$$a = a * (a \circ a)$$

把a看做b, $*$对$\circ$吸收

两边同时进行$\circ$运算后,再次使用吸收律:

$$a \circ a = a \circ \big(a * (a \circ a)\big) = a.$$

把$a \circ a$看做b, $\circ$对$*$吸收

即$\preccurlyeq$在S上是自反的. 同理可证$a * a = a$.

格与代数系统

- 证明$\preccurlyeq$在S上的反对称性. $\forall a, b \in S$, 有

$$
\begin{aligned}
& a \preccurlyeq b \text{且} b \preccurlyeq a \\
\Leftrightarrow\ & a \circ b = b \text{且} b \circ a = a && (\preccurlyeq\text{的定义}) \\
\Leftrightarrow\ & b = a \circ b = b \circ a = a && (\text{交换律})
\end{aligned}
$$

通过反对称的定义, 可知$\preccurlyeq$在S上是反对称的.

- 证明$\preccurlyeq$在S上的传递性. $\forall a, b, c \in S$, 有

$$
\begin{aligned}
& a \preccurlyeq b \text{且} b \preccurlyeq c \\
\Leftrightarrow\ & a \circ b = b \text{且} b \circ c = c && (\preccurlyeq\text{的定义}) \\
\Leftrightarrow\ & a \circ c = a \circ (b \circ c) = (a \circ b) \circ c = b \circ c = c && (\text{结合律})
\end{aligned}
$$

可得$a \preccurlyeq c$, 因此可知$\preccurlyeq$在S上是传递的. 综上所述, $\preccurlyeq$为S的偏序关系.

格与代数系统

(3) 最后一步, 证明⟨S,≼⟩构成格, 即$x \circ y$和$x * y$运算分别对应最小上界和最大下界.

- 首先证明$a \circ b$是$\{a, b\}$的上界, 即$a, b \preccurlyeq a \circ b$.

  $\forall a, b \in S$, 根据≼的定义$a \preccurlyeq b \Leftrightarrow a \circ b = b$, 有

  $$a \circ (a \circ b) = (a \circ a) \circ b = a \circ b \Rightarrow a \preccurlyeq a \circ b \quad (\preccurlyeq\text{的定义})$$

  $$b \circ (a \circ b) = a \circ (b \circ b) = a \circ b \Rightarrow b \preccurlyeq a \circ b \quad (\preccurlyeq\text{的定义})$$

  所以$a \circ b$是$\{a, b\}$的上界.

厦门大学信息学院 SCHOOL OF INFORMATICS XIAMEN UNIVERSITY 厦门大学计算机科学系 Computer Science Department of Xiamen University

格与代数系统

- 然后证明$a \circ b$是$\{a, b\}$的最小上界, 即$a \circ b \preccurlyeq \{a, b\}$的任意其他上界.

  假设c为$\{a, b\}$的任一上界, 则有$a \preccurlyeq c$且$b \preccurlyeq c$, 可得

  $$(a \circ b) \circ c = a \circ (b \circ c) = a \circ c = c \Rightarrow a \circ b \preccurlyeq c \quad (\preccurlyeq\text{的定义})$$

  所以$a \circ b$是$\{a, b\}$的最小上界, 即$a \circ b = a \vee b$.

- 然后证明$a * b$是$\{a, b\}$的最大下界. 由$a \circ b = b$可知

  $$a * b = a * (a \circ b) = a \qquad (\text{吸收律})$$

  通过$a * b = a$重复之前的步骤同理可证$a * b$是$\{a, b\}$的最大下界, 即$a * b = a \wedge b$.

格与代数系统

- 根据定理6.12, 我们可以从代数系统的角度给出格的另一个等价定义.

定义 6.10

设$\langle S,*,\circ\rangle$是代数系统, $*$和$\circ$是二元运算. 若$*$和$\circ$满足交换律, 结合律和吸收律, 则称$\langle S,*,\circ\rangle$构成一个格.

- 由定理, 偏序构成的格和代数系统构成的格是等价的.
- 格中的运算需要满足四条算律, 但是定义6.10中没有幂等律, 这是因为幂等律可以由吸收律推出, 所以只需满足三条算律即可.

子格

- 子格就是格的子代数.

定义 6.11

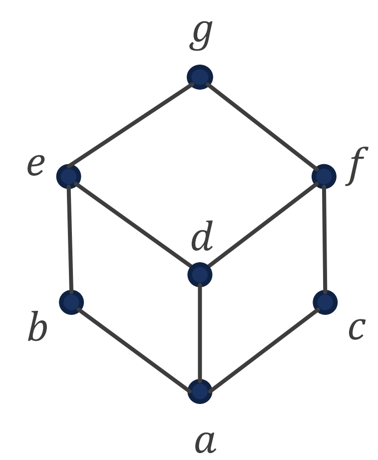
设L为格, S是L的非空子集. 若S关于L中的$\wedge$和$\vee$运算是封闭的, 即$\forall a, b \in S, a \wedge b \in S, a \vee b \in S$, 则称$S$是$L$的子格.

- 设$\langle L, \wedge, \vee \rangle$是格, $\forall a \in L$, $\langle \{a\}, \wedge, \vee \rangle$为格$L$的子格.
- 在格L的哈斯图中，经传递边构成的两个元素的集合是格L的子格.

子格

例 6.22 考虑图中的7元格L.

- 1元子格有7个: $\{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{f\}, \{g\}$.
- 2元子格有14个: $\{a,b\}, \{a,c\}, \{a,d\}, \{a,f\}, \{a,g\}, \{b,e\}, \{b,g\}, \{c,f\}, \{c,g\}, \{d,e\}, \{d,f\}, \{d,g\}, \{e,g\}, \{f,g\}$.
- 3元子格有13个: $\{a,b,e\}, \{a,b,g\}, \{a,d,e\}, \{a,d,f\}, \{a,d,g\}, \{a,c,f\}, \{a,c,g\}, \{a,e,g\}, \{a,f,g\}, \{b,e,g\}, \{c,f,g\}, \{d,e,g\}, \{d,f,g\}$.
- 4元子格有9个: $\{a,b,e,g\}, \{a,d,e,g\}, \{a,d,f,g\}, \{a,c,f,g\}, \{a,b,d,e\}, \{a,c,d,f\}, \{d,e,f,g\}, \{a,b,f,g\}, \{a,c,e,g\}$.
- 5元子格有5个: $\{a,b,d,e,g\}, \{a,c,d,f,g\}, \{a,d,e,f,g\}, \{a,b,c,f,g\}, \{a,b,c,e,g\}$.
- 6元子格有2个: $\{a,c,d,e,f,g\}, \{a,b,d,e,f,g\}$.
- 7元子格只有1个, 就是L本身. 其它非空子集都非子格.



$\{a,e,f,g\}$是格, 但不是L的子格, 因为$e \wedge f = d$, 但是$d \notin \{a,e,f,g\}$

课堂练习

$S_{30}=\{1,2,3,5,6,10,15,30\}$, $\langle S_{30},|\rangle$是格吗?

$S=\{1,2,5,6,10,15,30\}$,$\langle S,|\rangle$是格吗?

$\langle S,|\rangle$是$\langle S_{30},|\rangle$的子格吗?

画出S_{30}和S的哈斯图.

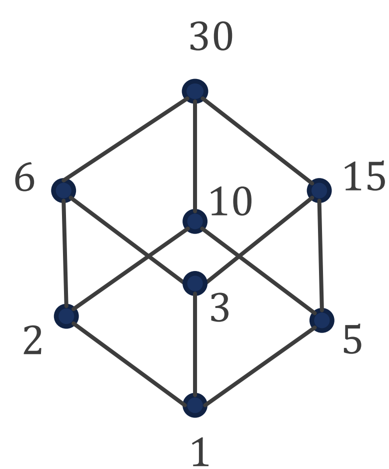
课堂练习

$S_{30}=\{1,2,3,5,6,10,15,30\}$, $\langle S_{30},|\rangle$是格吗?

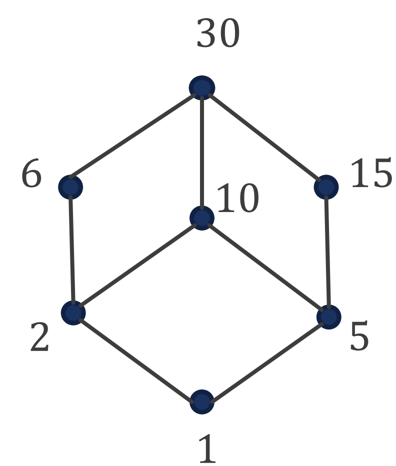
$S=\{1,2,5,6,10,15,30\}$,$\langle S,|\rangle$是格吗?

$\langle S,|\rangle$是$\langle S_{30},|\rangle$的子格吗?

解 S_{30}和$\langle S,|\rangle$都是格,但$\langle S,|\rangle$不是$\langle S_{30},|\rangle$的子格, 因为$6\wedge 15=3\notin S$.



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



$\langle S,|\rangle$

同构

定义 6.12

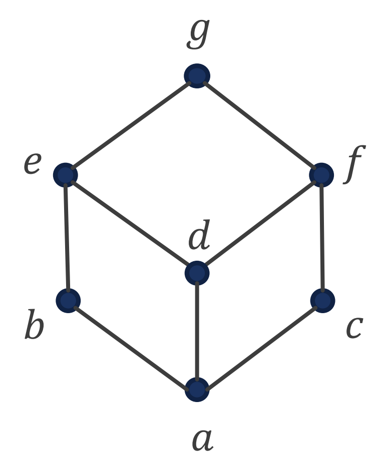
设L_1, L_2是格, f: $L_1 \to L_2$. 若$\forall x, y \in L_2$有

$$f(x \wedge y) = f(x) \wedge f(y),$$

$$f(x \vee y) = f(x) \vee f(y),$$

则称f是格L_1到L_2的同态映射, 简称同态. 若f是双射, 则称f是同构.

- 同构的格的哈斯图一定相同.
- 在该图中尽管L的4元子格有9个, 在同构意义上只有2个.
- 在该图中尽管L的5元子格有5个, 在同构意义上只有3个.



分配格

定义 6.13

设$\langle L,\wedge,\vee\rangle$是格, 若$\wedge$运算对$\vee$运算可分配, 或$\vee$运算对$\wedge$运算可分配, 即$\forall a,b,c\in L$有

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

$$\text{或}\ a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c),$$

成立, 则称L是**分配格**.

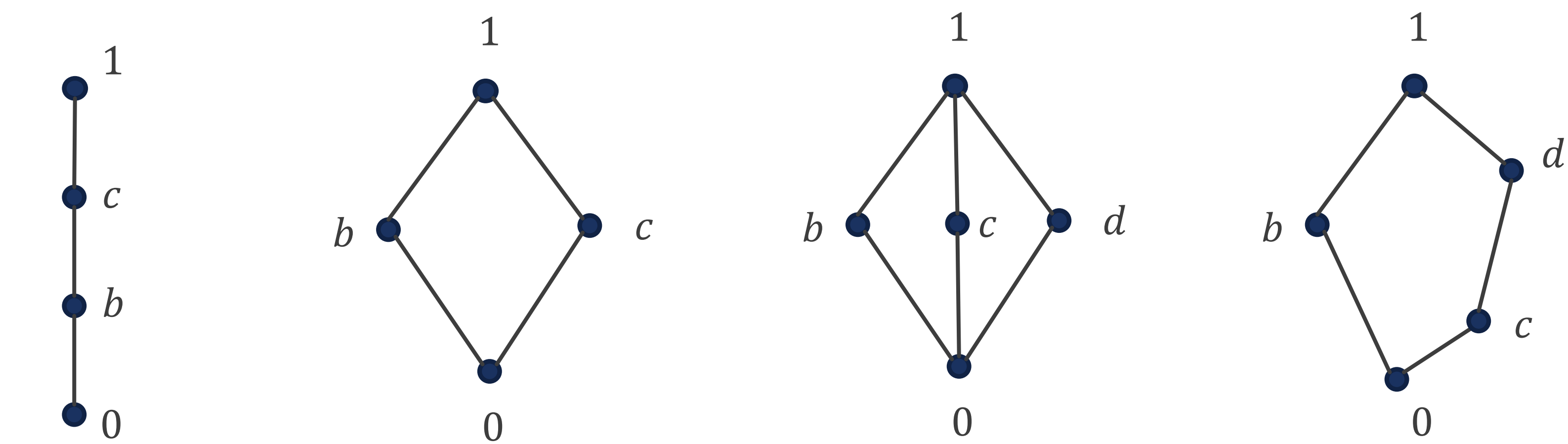
分配格

例 6.23 图中链格(1)和菱形格(2)是分配格, 钻石格(3)和五角格(4)不是分配格. 因为钻石格中有

$$d \wedge (b \vee c) = d \wedge 1 = d, \qquad (d \wedge b) \vee (d \wedge c) = 0 \vee 0 = 0,$$

五角格中有

$$d \wedge (b \vee c) = d \wedge 1 = d, \qquad (d \wedge b) \vee (d \wedge c) = 0 \vee c = c.$$



(1) 链格　(2) 菱形格　(3) 钻石格　(4) 五角格

分配格

定理 在分配格的定义中

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

证明 必要性. 设$\langle L,\vee,\wedge\rangle$是格, $\forall a, b, c \in L$, 若左式成立, 现证明右式

$$\begin{aligned}
& a \vee (b \wedge c) \\
&= \big(a \vee (a \wedge c)\big) \vee (b \wedge c) && \text{(吸收律)} \\
&= a \vee \big((a \wedge c) \vee (b \wedge c)\big) && \text{(结合律)} \\
&= a \vee \big((a \vee b) \wedge c\big) && (\wedge \text{对} \vee \text{分配律}) \\
&= \big((a \vee b) \wedge a\big) \vee \big((a \vee b) \wedge c\big) && \text{(吸收律)} \\
&= (a \vee b) \wedge (a \vee c) && (\wedge \text{对} \vee \text{分配律})
\end{aligned}$$

充分性同理可证.

分配格

定理 6.10

(1) L是分配格当且仅当L不含有与钻石格和五角格同构的子格.

(2) L是分配格当且仅当$\forall a,b,c\in L$有

$$a\wedge c=b\wedge c \text{ 且 } a\vee c=b\vee c\Rightarrow a=b.$$

推论

(1) 所有的链都是分配格.

(2) 元数小于5的格都是分配格.

- 在验证格是否为分配格时,最常用的方法就是找出其所有的五元子格.

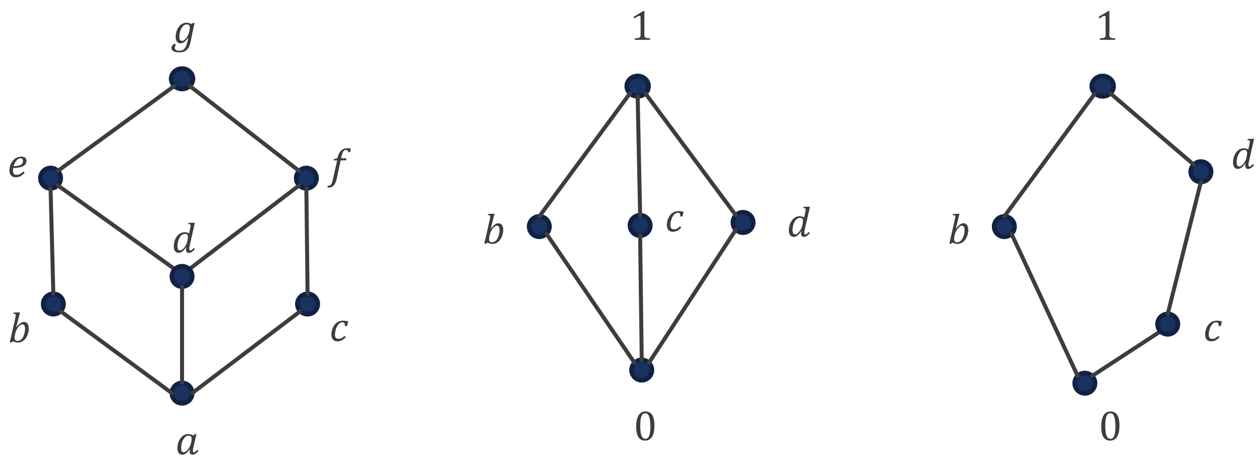
分配格

例 (1)含有子格$\{a, b, c, f, g\}$与五角格同构. (2)和(3)中均有

$$b \wedge c = b \wedge d \text{且} b \vee c = b \vee d$$

但是$c \neq d$, 不满足定理6.10(2).

因此它们都不是分配格.



(1) (2) (3)

有界格

定义 6.14

设L是格,

(1) 若存在元素$a \in L$, 使得$\forall b \in L$都有$a \preccurlyeq b$, 则称a是L的全下界,记为0;

(2) 若存在元素$c \in L$, 使得$\forall b \in L$都有$b \preccurlyeq c$,则称b是L的全上界,记为1;

(3) 如果L存在全上界和全下界, 则称L为有界格. 通常将有界格记作$\langle L, \wedge, \vee, 0, 1 \rangle$.

- 格L的全下界实际上就是偏序集L的最小元, 而全上界则是偏序集L的最大元.
- 而最小元和最大元如果存在, 则是惟一的. 所以有界格存在着惟一的全上界和全下界.

有界格

例 6.24 (1) 设$L = \{a_1, a_2, \dots, a_n\}$是$n$元格, 则

$$a_1 \wedge a_2 \wedge \cdots \wedge a_n 是L的全下界,$$

$$a_1 \vee a_2 \vee \cdots \vee a_n 是L的全上界.$$

因此有限格都是有界格.

(2) $\langle [0,1], \preccurlyeq \rangle$是有界格, 但不是有限格, 所以有界格不一定是有限格.

(2) 集合B的幂集格$P(B)$是有界格, 其中全下界是$\emptyset$, 全上界是B.

(3) 群G的子群格$L(G)$是有界格, 其中全下界是平凡子群$\{e\}$, 全上界是平凡子群G.

(4) $\langle \mathbf{Z}, \leq \rangle$不是有界格, 因为既没有最大的整数, 也没有最小的整数.

有补格

定义 6.15

设$\langle L,\wedge,\vee,0,1\rangle$是有界格，$a\in L$，如果存在$b\in L$使得$a\wedge b=0$，$a\vee b=1$，则称$b$是$a$的补元. 如果$L$中的每个元素都存在补元，则称$L$是有补格.

- 补元是相互的，即b是a的补元，那么a也是b的补元.

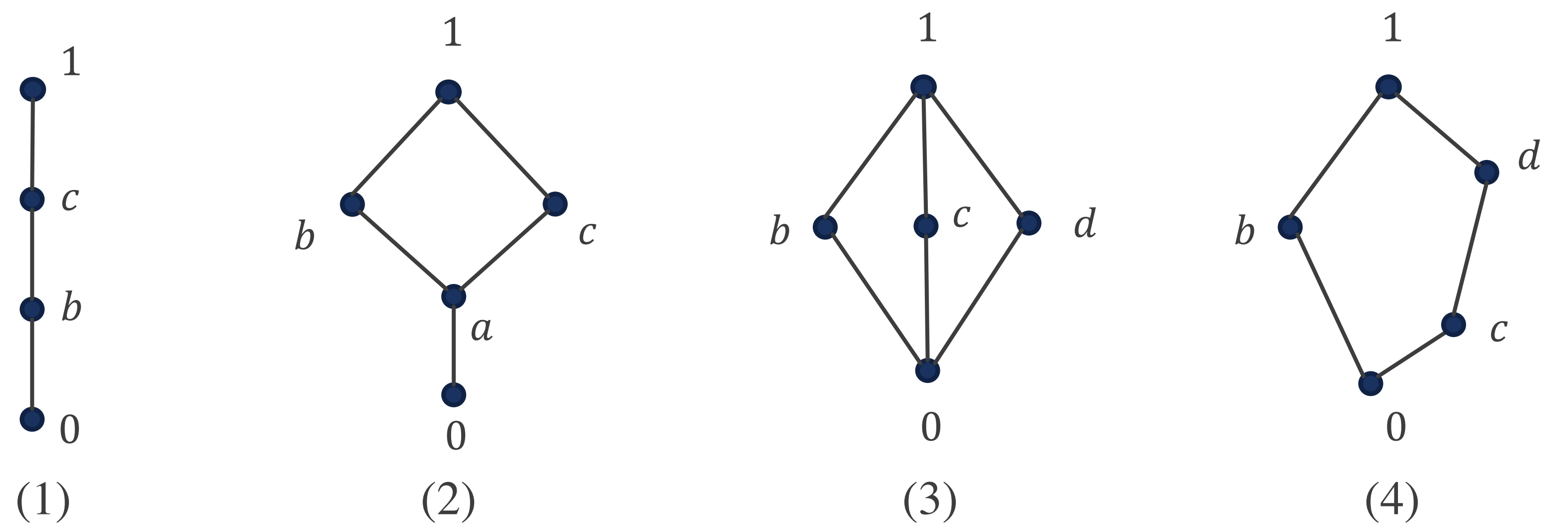
有补格

例 6.25 (1)中0与1互为补元, b和c无补元; 不是有补格.

(2)中0与1互为补元, a,b,c无补元; 不是有补格.

(3)中0与1互为补元, b的补元是c和d, c的补元是b和d, d的补元是b和c. 是有补格.

(3)中0与1互为补元, b的补元是c和d, c的补元是b, d的补元是b. 是有补格.



有补格

- L是有界格, 对任何元素$a \in L$, a的补元可能不存在, 如果存在也可能不是唯一的.

例 6.26 证明在分配格L中, $a \in L$, 若a存在补元, 一定是唯一的.

证明 设L是分配格, 假设b和c都是a的补元, 则有

$$a \vee b = a \vee c = 1, \qquad a \wedge b = a \wedge c = 0.$$

从而有$a \vee b = a \vee c$和$a \wedge b = a \wedge c$,

根据定理6.10(2)分配格有$b = c$, 所以a的补元是唯一的.

厦门大学信息学院 SCHOOL OF INFORMATICS XIAMEN UNIVERSITY 厦门大学计算机科学系 Computer Science Department of Xiamen University

布尔代数

定义 6.16

有补分配格称为布尔格, 也叫作布尔代数.

- 布尔格中的每个元素都有补元存在, 并且是唯一的, 因此可以把求补运算看作是布尔格中的一元运算.
- 通常将a的补元记作a', 并将布尔格B记作$\langle B,\wedge,\vee,',0,1\rangle$.

例 (1) 集合B的幂集格$\langle P(B),\cap,\cup,\sim,\emptyset,B\rangle$是布尔代数, 称集合代数, 其中$\cap$和$\cup$分别为集合的交和并运算, $\sim$是绝对补运算 (全集是B).

(2) 命题代数$\langle S,\wedge,\vee,\neg,0,1\rangle$是布尔代数, S为命题公式集合.

(3) 钻石格和五角格不是分配格, 长度大于2的链格不是有补格, 因此它们都不是布尔格.

布尔代数

- 从代数系统的角度可以把布尔代数看作是具有两个二元运算, 一个一元运算和两个零元的代数系统, 其中二元运算满足交换律, 结合律, 吸收律, 幂等律和分配律, 而一元运算为求补运算.
- 反过来, 也可以通过规定集合上的运算和算律来定义一个布尔代数.

布尔代数

定义 6.17

设$\langle B,*,\circ,\ ',0,1\rangle$是代数系统，$*$和$\circ$是二元运算，$'$是一元运算，$0,1 \in B$是代数常数，满足：

(1) 交换律，即$\forall a,b \in B$有

$$a*b=b*a, \qquad a\circ b=b\circ a,$$

(2) 分配律，即$\forall a,b,c \in B$有

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

(3) 同一律，1是$*$的单位元和$\circ$的零元，0是$\circ$的单位元和$*$的零元即$\forall a \in B$有，

$$a*1=a, \qquad a\circ 0=a, \qquad a*0=0, \qquad a\circ 1=1,$$

(4) 补元律，即$\forall a \in B$有

$$a*a'=0, \qquad a\circ a'=1,$$

则称$\langle B,*,\circ,',0,1\rangle$是一个布尔代数.

布尔代数

- 为了证明通过该定义的布尔代数也是格, 只需证明$*$和$\circ$运算满足结合律和吸收律即可.

证明 吸收律. $\forall a, b \in B$, 有

$$a \circ (a * b) = (a * 1) \circ (a * b) = a * (1 \circ b) = a * 1 = a.$$

同理可证$a * (a \circ b) = a$.

布尔代数

证明 结合律. 首先证明以下命题, $\forall a, b, c \in B$,

$$a \circ b = a \circ c \text{且} a' \circ b = a' \circ c \Rightarrow b = c.$$

两边同时加上$*$运算可得

$$\begin{aligned} & (a \circ b) * (a' \circ b) = (a \circ c) * (a' \circ c) \\ \Rightarrow\ & (a * a') \circ b = (a * a') \circ c \\ \Rightarrow\ & 0 \circ b = 0 \circ c \\ \Rightarrow\ & b = c. \end{aligned}$$

由该结论, 为了证明结合律$a * (b * c) = (a * b) * c$, 只需证明以下两个等式即可:

$$a \circ \big(a * (b * c)\big) = a \circ \big((a * b) * c\big),$$
$$a' \circ \big(a * (b * c)\big) = a' \circ \big((a * b) * c\big).$$

布尔代数

对于a, 由吸收律和分配律有

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

所以$a\circ\big(a*(b*c)\big)=a\circ\big((a*b)*c\big)$.

对于a',由吸收律和分配律有

$$\begin{aligned}a'\circ\big(a*(b*c)\big)&=(a'\circ a)*\big(a'\circ(b*c)\big)\\&=1*\big(a'\circ(b*c)\big)=a'\circ(b*c),\end{aligned}$$

$$\begin{aligned}a'\circ\big((a*b)*c\big)&=\big(a'\circ(a*b)\big)*(a'\circ c)\\&=\big((a'\circ a)*(a'\circ b)\big)*(a'\circ c)\\&=\big(1*(a'\circ b)\big)*(a'\circ c)\\&=(a'\circ b)*(a'\circ c)=a'\circ(b*c),\end{aligned}$$

所以$a'\circ\big(a*(b*c)\big)=a'\circ\big((a*b)*c\big)$.

布尔代数

不难证明布尔代数$\langle B, \wedge, \vee, ', 0, 1\rangle$有以下性质:

(1) $\forall a \in B$，补元a'是惟一的;

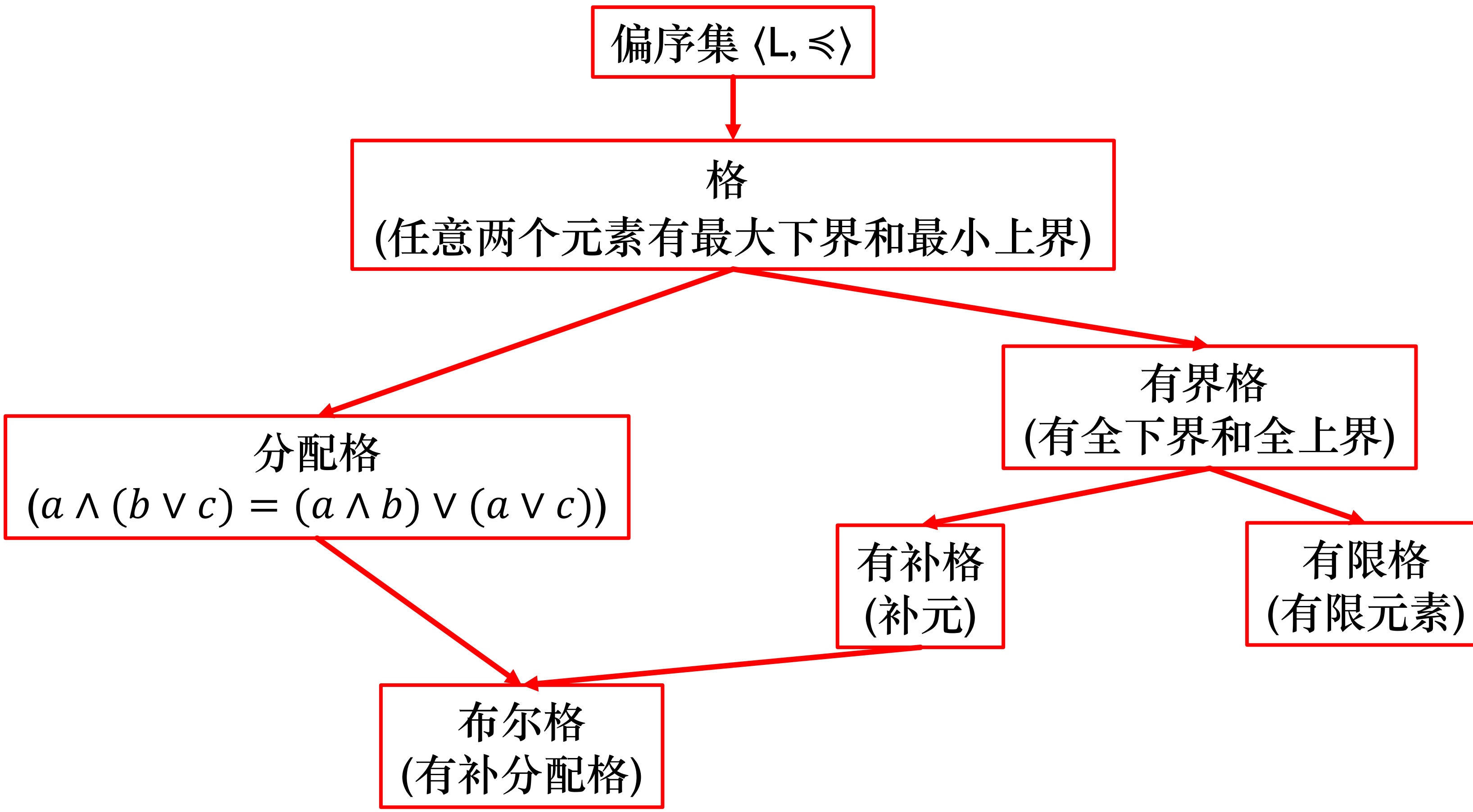
(2) 双重否定律: $\forall a \in B, (a')' = a$;

(3) 德 · 摩根律:

$$\forall a, b \in B,\ (a \wedge b)' = a' \vee b', (a \vee b)' = a' \wedge b'$$

(4) $\forall a, b \in B, a \preccurlyeq b \Leftrightarrow b' \preccurlyeq a'$.

格



偏序集 ⟨L, ≼⟩
格
(任意两个元素有最大下界和最小上界)
分配格
$(a \wedge (b \vee c) = (a \wedge b) \vee (a \vee c))$
有界格
(有全下界和全上界)
有补格
(补元)
有限格
(有限元素)
布尔格
(有补分配格)

作业

P142

1 (1)(4)(5)

5

6

7

11

12

15

16 (1)(3)

18

谢谢

有问题欢迎随时跟我讨论

厦门大学信息学院
SCHOOL OF INFORMATICS XIAMEN UNIVERSITY
厦门大学计算机科学系
Computer Science Department of Xiamen University