

离散数学

代数结构

9.3 几个典型的代数系统

9.3 几个典型的代数系统

- 半群、独异点与群
- 环与域
- 格与布尔代数

半群与独异点

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

- (1) 如果 \circ 是可结合的，则称 $V=\langle S, \circ \rangle$ 为**半群**。
- (2) 如果半群 $V=\langle S, \circ \rangle$ 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 $\langle S, \circ, e \rangle$ 。
- (3) 如果半群 $V=\langle S, \circ \rangle$ (独异点 $V=\langle S, \circ, e \rangle$) 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) $\langle \mathbb{Z}^+, + \rangle, \langle \mathbb{N}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}, + \rangle, \langle \mathbb{R}, + \rangle$ 都是可交换半群，除了 $\langle \mathbb{Z}^+, + \rangle$ 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， $\langle M_n(\mathbb{R}), \cdot \rangle$ 是半群与独异点，其中 \cdot 表示矩阵乘法。
- (3) $\langle \Sigma^*, \circ \rangle$ 是半群和独异点，其中 Σ 是有穷字母表， \circ 表示连接运算，幺元是空串 λ 。
- (4) $\langle P(B), \oplus \rangle$ 为半群与独异点，其中 \oplus 为集合的对称差运算。
- (5) $\langle \mathbb{Z}_n, \oplus \rangle$ 为半群与独异点，其中 $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ ， \oplus 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:

$$x^1 = x$$

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

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

$$x^0 = e,$$

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

- 幂运算规则:

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

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

证明方法: 数学归纳法

群的定义与实例

- **定义** 设 $\langle G, \circ \rangle$ 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) $\langle \mathbf{Z}, + \rangle, \langle \mathbf{Q}, + \rangle, \langle \mathbf{R}, + \rangle$ 是群； $\langle \mathbf{Z}^+, + \rangle, \langle \mathbf{N}, + \rangle$ 不是群。
- (2) $\langle M_n(\mathbf{R}), + \rangle$ 是群，而 $\langle M_n(\mathbf{R}), \cdot \rangle$ 不是群。
- (3) $\langle P(B), \oplus \rangle$ 是群， \oplus 为对称差运算。
- (4) $\langle \mathbf{Z}_n, \oplus \rangle$ 是群。 $\mathbf{Z}_n = \{ 0, 1, \dots, n-1 \}$ ， \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, 为 **Klein四元群**

- 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。

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

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 $|G|$
- $\langle \mathbb{Z}, + \rangle$ 和 $\langle \mathbb{R}, + \rangle$ 是无限群， $\langle \mathbb{Z}_n, \oplus \rangle$ 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, $x \in G$, $n \in \mathbb{Z}$, 则 x 的 n 次幂 x^n 定义为

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

- **实例**

- 在 $\langle \mathbb{Z}_3, \oplus \rangle$ 中有 $2^{-3} = (2^{-1})^3 = 1^3 = 1 \oplus 1 \oplus 1 = 0$
- 在 $\langle \mathbb{Z}, + \rangle$ 中有 $(-2)^{-3} = ((-2)^{-1})^3 = 2^3 = 2 + 2 + 2 = 6$

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 $\langle \mathbb{Z}_6, \oplus \rangle$ 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 $\langle \mathbb{Z}, + \rangle$ 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

半群, 独异

• **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) $\forall x \in G, x^n x^m = x^{n+m}, n, m \in \mathbb{Z}$ 。

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

> 群

> 半群, 独异

• 注意

• $(xy)^n = \underbrace{(xy)(xy)\dots(xy)}_{n \text{ 个 } xy \text{ 运算}}, G \text{ 为交换群, 才有 } (xy)^n = \underbrace{x^n y^n}_{x^n y^n}。$

$$\underbrace{(x_1 x_2 \dots x_n)^{-1}}_{(x_1 x_2 \dots x_n)^{-1}} = x_n^{-1} x_{n-1}^{-1} \dots x_2^{-1} x_1^{-1}$$

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 $ax=b$ 的唯一解。 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。求以下群方程的解
$$\{a\} \oplus X = \emptyset, \quad Y \oplus \{a,b\} = \{b\}$$
- 解:
- $X = \{a\}^{-1} \oplus \emptyset = \{a\} \oplus \emptyset = \{a\}, \quad Y = \{b\} \oplus \{a,b\}^{-1} = \{b\} \oplus \{a,b\} = \{a\}$

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 $G = \{a_1, a_2, \dots, a_n\}$ 是 n 阶群, 令 $a_i G = \{a_i a_j \mid j=1,2,\dots,n\}$ 证明 $a_i G = G$ 。
- 证 由群中运算的封闭性有 $a_i G \subseteq G$ 。假设 $a_i G \subset G$, 即 $|a_i G| < n$ 。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。

↓ X 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

4元 群

	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** $n\mathbb{Z}$ (n 是自然数) 是整数加群 $\langle \mathbb{Z}, + \rangle$ 的子群。当 $n \neq 1$ 时, $n\mathbb{Z}$ 是 \mathbb{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 $xy^{-1} \in H$ 。

例: 设 G 为群, $a \in G$, 令 $H = \{ a^k \mid k \in \mathbb{Z} \}$, 则 H 是 G 的子群, 称为由 a 生成的子群, 记作 $\langle a \rangle$ 。

证: 首先由 $a \in \langle a \rangle$ 知道 $\langle a \rangle \neq \emptyset$ 。 任取 $a^m, a^l \in \langle a \rangle$,

$$a^m (a^l)^{-1} = a^m a^{-l} = a^{m-l} \in \langle a \rangle$$

根据判定定理可知 $\langle a \rangle \leq G$ 。

实例

整数加群 $\langle \mathbb{Z}, + \rangle$,

由 2 生成的子群是 $\langle 2 \rangle = \{ 2k \mid k \in \mathbb{Z} \} = 2\mathbb{Z}$

模 6 加群 $\langle \mathbb{Z}_6, \oplus \rangle$ 中

由 2 生成的子群 $\langle 2 \rangle = \{ 0, 2, 4 \}$

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

$$\langle e \rangle = \{ e \},$$

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

实例

$$\forall x, y \in H \quad xy^{-1} \in H \quad G \text{ 为群}$$

$$\forall a, b \in C \quad \underbrace{ab^{-1} \in C} \Rightarrow C \leq G \text{ 为群}$$

• 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**。 $e \in C$ 。

• 证 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

$$\begin{aligned} (ab^{-1})x &= ab^{-1}x = ab^{-1}(x^{-1})^{-1} = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} \\ &= a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}) \end{aligned}$$

由判定定理可知 $C \leq G$ 。

循环群

- **定义** 设 G 是群, 若存在 $a \in G$ 使得
$$G = \{ a^k \mid k \in \mathbb{Z} \}$$

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 $G = \langle \mathbb{Z}, + \rangle = \langle \underline{1} \rangle = \langle \underline{-1} \rangle$

模 6 加群 $G = \langle \mathbb{Z}_6, \oplus \rangle = \langle \underline{1} \rangle = \langle \underline{5} \rangle$

- 设 $G = \langle a \rangle$, 若 a 是 n 阶元, 则 G 为 n 阶**循环群**, 即
$$G = \{ a^0 = e, a^1, a^2, \dots, a^{n-1} \}$$

- 若 a 是无限阶元, 则 G 为**无限循环群**, 即
$$G = \{ a^{\pm 0} = e, a^{\pm 1}, a^{\pm 2}, \dots \}$$

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。

$\{ \mathbb{Z}, \oplus \}$

1 5
1, 5, 2, 3, 4

生成元的实例

$a^r \leq 12$ 1, 5, 7, 11

(1) 设 $G = \{e, a, \dots, a^{11}\}$ 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 $G = \langle \mathbb{Z}_9, \oplus \rangle$ 是模 9 的整数加群, 1, 2, 4, 5, 7, 8

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 $G = 3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\}$, 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) $G=\langle \mathbb{Z}, + \rangle$ 是无限循环群，对于自然数 $m \in \mathbb{N}$ ，1 的 m 次幂是 m ， m 生成的子群是 $m\mathbb{Z}$ ， $m \in \mathbb{N}$ 。即

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

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

(2) $G=\mathbb{Z}_{12}$ 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 $\langle 12 \rangle = \langle 0 \rangle = \{0\}$ ，2 阶子群 $\langle 6 \rangle = \{0, 6\}$

3 阶子群 $\langle 4 \rangle = \{0, 4, 8\}$ ，4 阶子群 $\langle 3 \rangle = \{0, 3, 6, 9\}$

6 阶子群 $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$ ，12 阶子群 $\langle 1 \rangle = \mathbb{Z}_{12}$

n 元置换的定义

- **定义** 设 $S = \{ 1, 2, \dots, n \}$, S 上的双射函数 $\sigma: S \rightarrow S$ 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 $S = \{ 1, 2, 3, 4, 5 \}$, 则以下都是 5元置换

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

k 阶轮换与对换

- **定义** 设 σ 是 $S = \{1, 2, \dots, n\}$ 上的 n 元置换。若 $\sigma(i_1)=i_2$, $\sigma(i_2)=i_3, \dots, \sigma(i_{k-1})=i_k, \sigma(i_k)=i_1$ 且保持 S 中的其他元素不变, 则称 σ 为 S 上的 **k 阶轮换**, 记作 $(i_1 i_2 \dots i_k)$ 。若 $k=2$, 称 σ 为 S 上的**对换**。

- **例如 5元置换**

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

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

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

- 使用轮换表示是：

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

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

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

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

S_3 的子群

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

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

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

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

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

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

环的定义

- **定义** 设 $\langle R, +, \cdot \rangle$ 是代数系统， $+$ 和 \cdot 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) \cdot 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**， \cdot 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 \mathbf{Z}** ，**有理数环 \mathbf{Q}** ，**实数环 \mathbf{R}** 和**复数环 \mathbf{C}** 。
- (2) $n(n \geq 2)$ 阶实矩阵的集合 $M_n(\mathbf{R})$ 关于矩阵的加法和乘法构成环，称为 **n 阶实矩阵环**。
- (3) 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 $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ ， \oplus 和 \otimes 分别表示模 n 的加法和乘法，则 $\langle \mathbf{Z}_n, \oplus, \otimes \rangle$ 构成环，称为**模 n 的整数环**。

环中的零因子

- 设 $\langle R, +, \cdot \rangle$ 是环，若存在 $a \cdot b = 0$ ，且 $a \neq 0, b \neq 0$ ，称 a 为左零因子， b 为右零因子。
- 实例
 - $\langle \mathbb{Z}_6, \oplus, \otimes \rangle$ ，其中 $2 \otimes 3 = 0$ ，2和3都是零因子。
- 无零因子的条件： $a \cdot b = 0 \rightarrow a=0 \vee b=0$
- 可证明无零因子的充要条件是：对于非零元，乘法满足消去律

特殊的环

定义 设 $\langle R, +, \cdot \rangle$ 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 $\forall a, b \in R, a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$, 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 \mathbf{Z} 、有理数环 \mathbf{Q} 、实数环 \mathbf{R} 、复数环 \mathbf{C} 都是交换环、含幺环、无零因子环和整环。其中除 \mathbf{Z} 之外都是域
- (2) 令 $2\mathbf{Z}=\{ 2z \mid z \in \mathbf{Z} \}$ ，则 $\langle 2\mathbf{Z}, +, \cdot \rangle$ 构成交换环和无零因子环。但不是含幺环和整环。
- (3) 设 $n \in \mathbf{Z}, n \geq 2$ ，则 n 阶实矩阵的集合 $M_n(\mathbf{R})$ 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) $\langle \mathbf{Z}_6, \oplus, \otimes \rangle$ 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 ， \mathbf{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) $A = \{a + bi \mid a, b \in \mathbf{Q}\}$, $i^2 = -1$, 运算为复数加法和乘法。

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

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

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

(5) $A = \{a + b\sqrt[4]{5} \mid a, b \in \mathbf{Q}\}$, 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 $\langle R, +, \cdot \rangle$ 是环, 则

(1) $\forall a \in R, \quad a \cdot 0 = 0 \cdot a = 0$ --- 加法的幺元是乘法的零元

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

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

(4) $\forall a, b, c \in R, \quad a \cdot (b - c) = a \cdot b - a \cdot c, \quad (b - c) \cdot a = b \cdot a - c \cdot a$

例 在环中计算 $(a+b)^3, (a-b)^2$

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

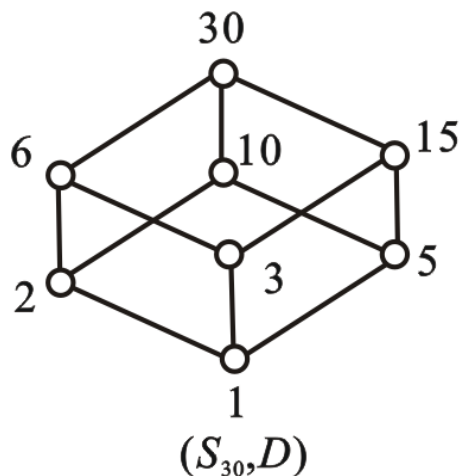
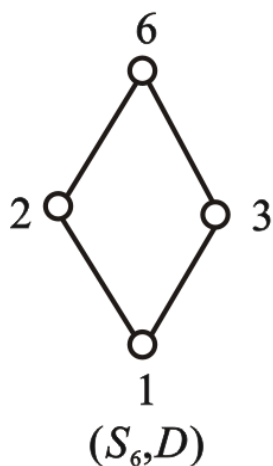
$(a-b)^2 = (a-b)(a-b) = a^2-ba-ab+b^2$

格的定义

- **定义** 设 $\langle S, \leq \rangle$ 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 S 关于偏序 \leq 构成**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

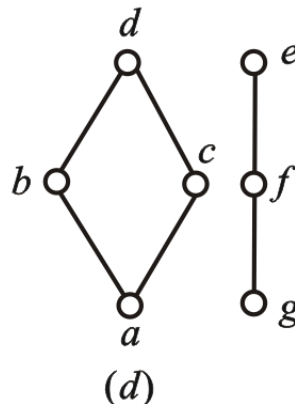
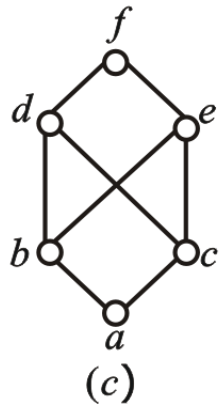
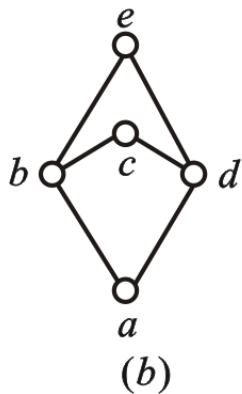
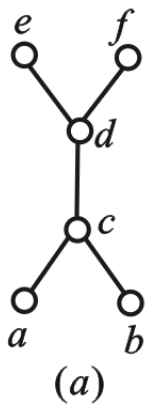
- 例 设 n 是正整数， S_n 是 n 的正因子的集合。 D 为整除关系，则偏序集 $\langle S_n, D \rangle$ 构成格。 $\forall x, y \in S_n$,
- $x \vee y$ 是 $\text{lcm}(x, y)$ ，即 x 与 y 的最小公倍数。 $x \wedge y$ 是 $\text{gcd}(x, y)$ ，即 x 与 y 的最大公约数。
- 下图给出了格 $\langle S_8, D \rangle$ ， $\langle S_6, D \rangle$ 和 $\langle S_{30}, D \rangle$ 。



格的实例（续）

例 判断下列偏序集是否构成格，并说明理由。

- (1) $\langle P(B), \subseteq \rangle$ ，其中 $P(B)$ 是集合 B 的幂集。
- (2) $\langle \mathbb{Z}, \leq \rangle$ ，其中 \mathbb{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。



解 (1) 是格。称 $\langle P(B), \subseteq \rangle$ 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 $=, \leq, \geq, \vee$ 和 \wedge 的命题。令 f^* 是将 f 中的 \leq 替换成 \geq , \geq 替换成 \leq , \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**。
- 例如, 在格中: f 是 $(a \vee b) \wedge c \leq c$, f^* 是 $(a \wedge b) \vee c \geq c$ 。
- **格的对偶原理**: 设 f 是含格中元素以及符号 $=, \leq, \geq, \vee$ 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。
- 例如, 若对一切格 L 都有 $\forall a, b \in L, a \wedge b \leq a$, 那么对一切格 L 都有 $\forall a, b \in L, a \vee b \geq a$

格的性质：算律

- **定理** 设 $\langle L, \leq \rangle$ 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

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

(3) $\forall a \in L$ 有

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

(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

$$(a \vee b) \vee c \geq a \vee b \geq a \quad (\text{I})$$

$$(a \vee b) \vee c \geq a \vee b \geq b \quad (\text{II})$$

$$(a \vee b) \vee c \geq c \quad (\text{III})$$

由式 (II) 和 (III) 有 $(a \vee b) \vee c \geq b \vee c \quad (\text{IV})$

由式 (I) 和 (IV) 有 $(a \vee b) \vee c \geq a \vee (b \vee c)$ 。

同理可证 $(a \vee b) \vee c \leq a \vee (b \vee c)$ 。

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 $a \leq a \vee a$, 又由 $a \leq a$ 得 $a \vee a \leq a$ 。

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

$$a \vee (a \wedge b) \geq a \quad (\text{V})$$

由 $a \leq a, a \wedge b \leq a$ 可得

$$a \vee (a \wedge b) \leq a \quad (\text{VI})$$

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 $\langle S, *, \circ \rangle$ 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 \leq , 使得 $\langle S, \leq \rangle$ 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 $\langle S, *, \circ \rangle$ 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 $\langle S, *, \circ \rangle$ 构成格。

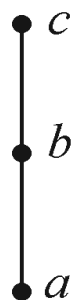
分配格定义

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

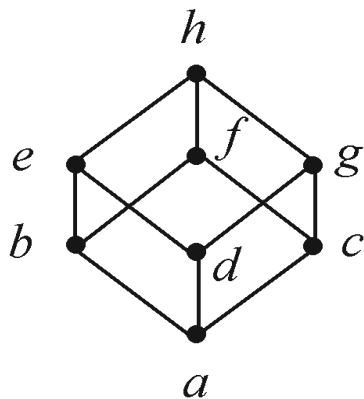
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

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

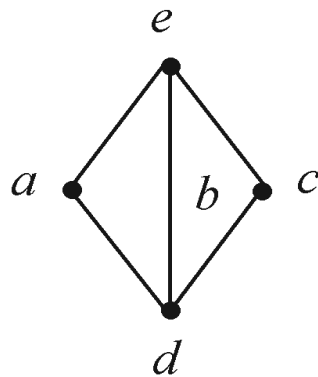
则称 L 为**分配格**。



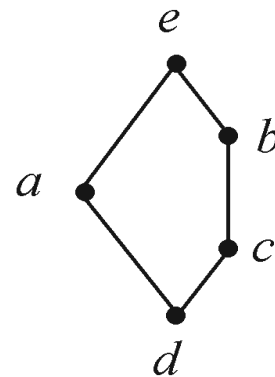
(a)



(b)



(c)



(d)

(a)和(b)是分配格,
(c)和(d)不是分配格。

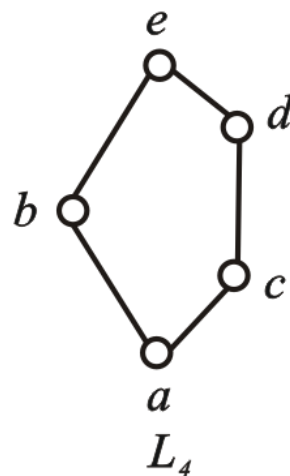
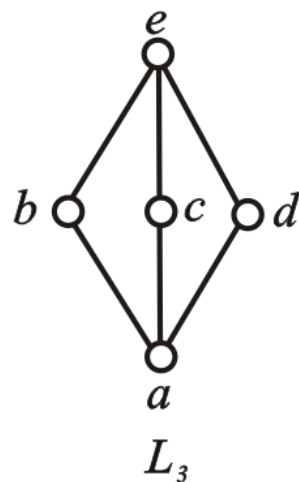
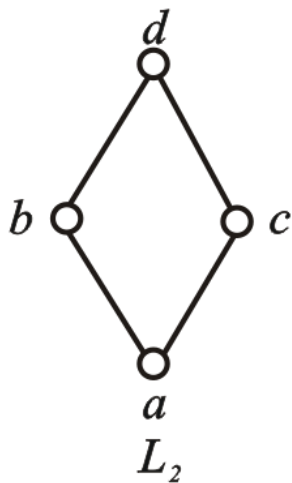
全上界与全下界

- **定义** 设 L 是格, 若存在 $a \in L$ 使得 $\forall x \in L$ 有 $a \leq x$, 则称 a 为 L 的**全下界**; 若存在 $b \in L$ 使得 $\forall x \in L$ 有 $x \leq b$, 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 $\langle L, \wedge, \vee, 0, 1 \rangle$ 。
- 注意: 有限格 $L = \{a_1, a_2, \dots, a_n\}$ 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 $\langle L, \wedge, \vee, 0, 1 \rangle$ 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 $\langle L, \wedge, \vee, 0, 1 \rangle$ 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。

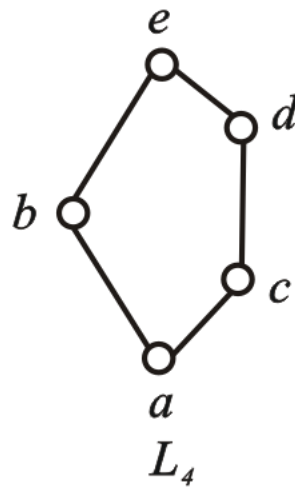
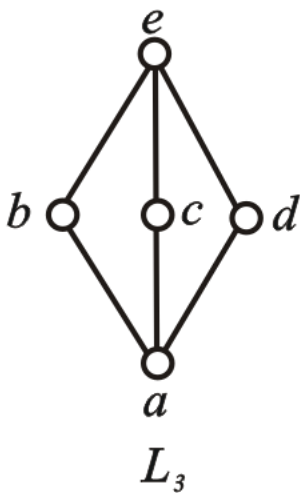
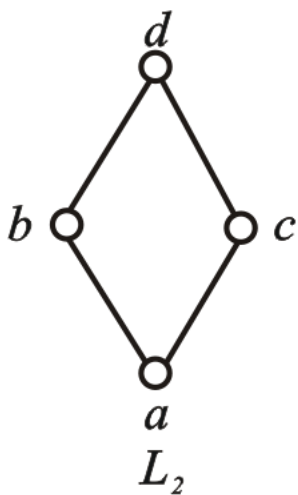
L_3 中 a, e 互补, b 的补元是 c 和 d , c 的补元是 b 和 d , d 的补元是 b 和 c 。

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 $\langle L, \wedge, \vee, 0, 1 \rangle$ 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 $\langle B, \wedge, \vee, ', 0, 1 \rangle$, 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 $\langle S_{110}, \text{gcd}, \text{lcm} \rangle$ 是否构成布尔代数?

布尔代数的性质

定理 设 $\langle B, \wedge, \vee, ', 0, 1 \rangle$ 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)

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

$$\begin{aligned}(a \wedge b) \vee (a' \vee b') &= (a \vee a' \vee b') \wedge (b \vee a' \vee b') \\ &= (1 \vee b') \wedge (a' \vee 1) = 1 \wedge 1 = 1, \\ (a \wedge b) \wedge (a' \vee b') &= (a \wedge b \wedge a') \vee (a \wedge b \wedge b') \\ &= (0 \wedge b) \vee (a \wedge 0) = 0 \vee 0 = 0.\end{aligned}$$

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($n \in \mathbb{N}$)，且 L 与 $\langle P(S), \cap, \cup, \sim, \emptyset, S \rangle$ 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。

作业

- P227
- 9.20
- 9.22
- 9.24

问题？

