



代数结构

Algebra Structures



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

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

5、环与域

概念：

环，交换环，含么环，整环，域

环 (Ring)

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（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 \mathbb{Z} ，有理数环 \mathbb{Q} ，实数环 \mathbb{R} 和复数环 \mathbb{C} 。
- (2) $n(n \geq 2)$ 阶实矩阵的集合 $M_n(\mathbb{R})$ 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 $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ ， \oplus 和 \otimes 分别表示模 n 的加法和乘法，则 $\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ 构成环，称为模 n 的整数环。

环的运算性质

设 $\langle R, +, \cdot \rangle$ 是环, 则

$$(1) \quad \forall a \in R, \quad a0 = 0a = 0$$

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

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

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

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

例：在环中计算 $(a+b)^3, (a-b)^2$ 。

$$\begin{aligned}\text{解：} \quad (a+b)^3 &= (a+b)(a+b)(a+b) \\ &= (a^2+ba+ab+b^2)(a+b) \\ &= a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3 \\ (a-b)^2 &= (a-b)(a-b) = a^2-ba-ab+b^2\end{aligned}$$

特殊的环

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

例:

- (1) 整数环 \mathbb{Z} 交换环, 含幺环, 无零因子环。
- (2) 令 $2\mathbb{Z}=\{2z \mid z \in \mathbb{Z}\}$, 则 $\langle 2\mathbb{Z}, +, \cdot \rangle$ 构成交换环和无零因子环, 但不是含幺环。

整环(Integrel Domain)

设 $\langle R, +, \bullet \rangle$ 是一个代数系统，若满足：

- (1) $\langle R, + \rangle$ 是阿贝尔群；
- (2) $\langle R, \bullet \rangle$ 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 \bullet 对 $+$ 是可分配的，

则称 $\langle R, +, \bullet \rangle$ 是整环。

注：（1）既是交换环、含么环、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 $\langle R, +, \bullet \rangle$ 是一个代数系统，若满足：

- (1) $\langle R, + \rangle$ 是阿贝尔群；
- (2) $\langle R - \{0\}, \bullet \rangle$ 是阿贝尔群；
- (3) 运算 \bullet 对 $+$ 是可分配的，

则称 $\langle R, +, \bullet \rangle$ 是域。

例：整数环 \mathbb{Z} 整环，但不是域；实数环 \mathbb{R} 既是整环又是域。

性质：

- (1) 域一定是整环。
- (2) 有限整环必是域。