

# 第五部分 代数结构

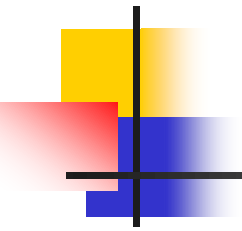
## 第16章 环与域

---

计算机（软件）学院

林 兰

[linlan@scu.edu.cn](mailto:linlan@scu.edu.cn)



前面讨论了具有一个二元运算的代数系统——半群、含么半群、群、子群。

下面讨论具有两个二元运算的代数系统。给定两个代数系统 $\langle A, + \rangle$ ,  $\langle A, * \rangle$ 可将它们组合成一个具有两个二元运算的代数系统 $\langle A, +, * \rangle$ , 而这两个二元运算符 $+$ 和 $*$ 之间是有联系的。

环在计算机科学的很多领域, 诸如编码理论的研究中起着重要作用; 而域, 特别是有限域是纠错码理论的基础。



# 主要内容

---

- 1. 环的定义与基本性质
- 2. 特殊环
- 3. 域



# 1. 环的定义与性质

## 定义(环)

一个代数系统 $\langle R, +, * \rangle$ , 如果满足:

- (1)  $\langle R, + \rangle$ 是阿贝尔群;
- (2)  $\langle R, * \rangle$ 是半群;
- (3) 运算 $*$ 在运算 $+$ 上可分配。即对任意 $a, b, c \in R$

有

$$a * (b + c) = (a * b) + (a * c)$$

$$(b + c) * a = (b * a) + (c * a)$$

则称 $\langle R, +, * \rangle$ 是一个环。

联系两个二元运算，  
否则就不是一个系统  
而是两个系统



# 1. 环的定义与性质

---

例1 在加法和乘法运算下，整数、实数、有理数、偶数和复数都能构成环。

$$\langle \mathbb{Z}, +, \times \rangle$$

$$\langle \mathbb{R}, +, \times \rangle$$

$$\langle \mathbb{Q}, +, \times \rangle$$

$$\langle \mathbb{E}, +, \times \rangle$$

$$\langle \mathbb{C}, +, \times \rangle$$

0是“+”的幺元， $x$ 的逆为 $-x$ ；“+”可以交换，

“+， $\times$ ”可结合，“ $\times$ ”对“+”可分配。



# 1. 环的定义与性质

例2 设 $Z_k$ 表示整数集 $Z$ 上的模 $k$ 剩余类集合,

即  $Z_k = \{[0], [1], [2], \dots, [k-1]\}$

$\langle Z_k, \oplus \rangle$ 是群（**剩余类加群**），

$\langle Z_k, \otimes \rangle$ 是半群（**剩余类乘半群**），

$\because$  对 $\forall [i], [j], [k] \in Z_k$

有 $[i] \otimes ([j] \oplus [k]) = [i(j+k)] = [ij+ik]$

$$= [ij] \oplus [ik]$$

$$= ([i] \otimes [j]) \oplus ([i] \otimes [k])$$

$\therefore \langle Z_k, \oplus, \otimes \rangle$ 是环，称为（**模 $k$** ）**剩余类环**。

➤ 特别，  $k=2$ 时，称为**布尔环**。



# 1. 环的定义与性质

---

书写约定：环中加法么元记为 $\theta$ ，元素 $a$ 的加法逆元记为 $-a$ ，且 $b + (-a) = b - a$ 。

## 定理1 (移项法则)

设 $\langle R, +, * \rangle$ 是一个环， $\theta$ 是加法么元，对任意 $a, b, c \in R$ ，则

$$a + b = c \Leftrightarrow a + b - c = \theta$$



# 1. 环的定义与性质

---

## 定理2

设 $\langle R, +, * \rangle$ 是一个环,  $\theta$  是加法幺元, 对任意 $a, b, c \in R$ 有

①  $a * \theta = \theta * a = \theta$  (加法幺元是乘法零元)

②  $a * (-b) = (-a) * b = -(a * b)$

③  $(-a) * (-b) = a * b$

④  $(b - c) * a = b * a - c * a$

⑤  $a * (b - c) = a * b - a * c$





# 1. 环的定义与性质

证明①、②两式：

$$\textcircled{1} \quad a * \theta = \theta * a = \theta$$

证明：  $a * \theta = a * (\theta + \theta)$

由分配律：  $a * \theta = (a * \theta) + (a * \theta)$

再由移项法则：  $a * \theta = \theta$ 。

同理，可证  $\theta * a = \theta$ 。

$$\textcircled{2} \quad a * (-b) = (-a) * b = -(a * b)$$

证明：考虑  $a * (-b) + (a * b)$

由分配律：  $a * (-b) + (a * b) = a * (-b + b) = a * \theta = \theta$

所以，  $-(a * b) = a * (-b)$

同理，可证  $-(a * b) = (-a) * b$



# 主要内容

---

- 1. 环的定义与基本性质
- 2. 特殊环
- 3. 域



## 2. 特殊环

**定义** 设 $\langle R, +, * \rangle$ 是一个环,

- ① 如果 $\langle R, * \rangle$ 是可交换的, 称 $\langle R, +, * \rangle$ 是**交换环**;
- ② 如果 $\langle R, * \rangle$ 是含么半群, 称 $\langle R, +, * \rangle$ 是**含么环**;
- ③ 如果存在元素 $a, b \in R, a \neq \theta, b \neq \theta$ , 但 $a*b = \theta$ , 则称 $a$ 为 $R$ 中的左零因子,  $b$ 为 $R$ 中的右零因子。

如果环 $\langle R, +, * \rangle$ 中不含零因子, 则称 $R$ 是**无零因子环**。

- ④ 如果 $\langle R, +, * \rangle$ 是**可交换的, 含么, 无零因子**, 则称它是**整环**。



## 2. 特殊环

**例3** 证明（模 $k$ ）剩余类环 $\langle \mathbb{Z}_k, \oplus, \otimes \rangle$ 无零因子当且仅当 $k$ 是素数。

证明：

$\because$  当 $k$ 是合数时， $\exists a \geq 2, b \geq 2$ ，使得 $k=ab$   
而 $[a] \otimes [b] = [k] = [0]$ ，即 $[a]$ 、 $[b]$ 都是零因子，  
又  $\because$  当 $k$ 是素数时，不 $\exists a \geq 2, b \geq 2$ ，使得 $k=ab$   
因而无零因子  $\therefore$  结论成立。

例如 $\langle \mathbb{Z}_6, \oplus, \otimes \rangle$ 中，

$$[2] \otimes [3] = [0]$$

$$[4] \otimes [3] = [0]$$



# 主要内容

---

- 1. 环的定义与基本性质
- 2. 特殊环
- 3. 域



### 3. 域

---

给环施加进一步的限制，从而得到另一个代数系统——域。

#### 定义（域）

设 $\langle R, +, * \rangle$ 是一个环，如果 $\langle R, + \rangle$ 和 $\langle R - \{ 0 \}, * \rangle$ 都是交换群，则称 $\langle R, +, * \rangle$ 是域。

域是在整环的基础上增加了除0之外每元都有乘法逆元的条件；一般情况下，整环不是域，但当环的元素个数有限时，有以下结论：

#### 定理5

有限整环 $\langle R, +, * \rangle$ 必是域。



### 3. 域

---

#### 例4

(1) 实数环 $\langle \mathbb{R}, +, \times \rangle$ 、有理数环 $\langle \mathbb{Q}, +, \times \rangle$ 、剩余类环 $\langle \mathbb{Z}_p, \oplus, \otimes \rangle$  ( $p$ 是素数) 都是域。

(2) 整数环 $\langle \mathbb{Z}, +, \times \rangle$ 、剩余类环 $\langle \mathbb{Z}_m, \oplus, \otimes \rangle$   
( $m$ 是合数) 都不是域。

因为 $\langle \mathbb{Z} - \{0\}, \times \rangle$ 、 $\langle \mathbb{Z}_m - \{[0]\}, \otimes \rangle$ 都不是群。