

第十讲环的定义及简单性质

陈建文

November 9, 2022

定义1. 设 R 为一个非空集合, R 中有两个代数运算, 一个叫做加法并用“ $+$ ”表示, 另一个叫做乘法并用“ \circ ”表示, 如果

- (1) $(R, +)$ 为一个Abel群;
- (2) (R, \circ) 为一个半群;
- (3) 乘法对加法满足左、右分配律: $\forall a, b, c \in R$

$$\begin{aligned}a \circ (b + c) &= (a \circ b) + (a \circ c) \\(b + c) \circ a &= (b \circ a) + (c \circ a)\end{aligned}$$

则称代数系 $(R, \circ, +)$ 为一个环 (ring)。

以下 $a \circ b$ 简写为 ab 。

例. 整数集合 Z 对通常数的加法和乘法构成一个环 $(R, +, \cdot)$, 称为整数环。

例. 文字 x 的整系数多项式之集 $Z[x]$ 对多项式的加法和乘法构成一个环。

定义2. 环 $(R, +, \circ)$ 称为交换环或可换环, 如果其中的乘法满足交换律, 即 $\forall a, b \in R, ab = ba$ 。

例. 设 M_n 为一切 $n \times n$ 实矩阵之集, 则 M_n 对矩阵的加法和乘法构成一个非交换环 $(M_n, +, \cdot)$, 称为 n 阶矩阵环。

定义3. 环 $(R, +, \circ)$ 称为有限环, 如果 R 为有限非空的集合。

例. 令 $S = \{0\}$, 则 S 对数的通常加法和乘法构成一个环, 称为零环, 它仅有一个元素。

例. 全体整数集 Z 对模 n 同余类之集 $Z_n = \{[0], [1], \dots, [n-1]\}$ (n 为正整数), 对其上定义的同余类加法和同余类乘法构成一个环。同余类加法定义为

$$[i] + [j] = [i + j]$$

同余类乘法定义为

$$[i] \cdot [j] = [i \cdot j]$$

定义4. 设 $(R, +, \circ)$ 为一个环, $\forall a, b \in R, a - b$ 定义为 $a + (-b)$ 。

定理1. 设 $(R, +, \circ)$ 为一个环, $\forall a, b, c \in R$,

1. $-(a + b) = -a - b$
2. $0 \circ a = a \circ 0 = 0$
3. $(-a)b = -(ab), a(-b) = -(ab)$
4. $(-a)(-b) = ab$
5. $a(b - c) = ab - ac$

定义5. 在环 $(R, +, \circ)$ 中, $\forall a \in R$, 定义 $0a = 0, (n + 1)a = na + a(n \geq 0), (-n)a = n(-a)(n \geq 1)$ 。

定理2. 设 $(R, +, \circ)$ 为一个环, $\forall a, b \in R, m, n \in Z$,

1. $(m + n)a = ma + na$
2. $m(na) = (mn)a$
3. $m(a + b) = ma + mb$
4. $n(a - b) = na - nb$
5. $(na)b = a(nb) = n(ab)$

定义6. 在环 $(R, +, \circ)$ 中, $\forall a \in R$, 定义 $a^1 = a, a^{m+1} = a^m \circ a(m \geq 1)$ 。

定理3. 设 $(R, +, \circ)$ 为一个环, $\forall a, b \in R, m, n \in Z^+$,

1. $a^{m+n} = a^m \circ a^n$
2. $(a^m)^n = a^{mn}$
3. 如果 $ab = ba$, 则二项式定理成立, 即当 $n > 0$ 时

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$$

例. 在环 $(M_2, +, \cdot)$ 中, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ 和 $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ 是 M_2 中的两个非零元素, 但是

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

定义7. 设 $(R, +, \circ)$ 为一个环, $a \in R$, 如果存在一个元素 $b \in R, b \neq 0$, 使得 $ab = 0$, 则称 a 为 R 的一个左零因子; 如果存在一个元素 $c \in R, c \neq 0$, 使得 $ca = 0$, 则称 a 为 R 的一个右零因子; R 的左零因子和右零因子统称为零因子。

定义8. 没有非零的左零因子, 也没有非零的右零因子的环称为无零因子环。可换的无零因子环称为整环。

定理4. 环 R 为无零因子环的充分必要条件是 $\forall a, b \in R$, 如果 $a \neq 0$ 并且 $b \neq 0$, 则 $ab \neq 0$ 。

定理5. 环 R 为无零因子环的充分必要条件是在 R 中乘法满足左消去律或右消去律, 即

- $\forall a, b, c \in R$, 如果 $a \neq 0, ab = ac$, 则 $b = c$;
或者
 $\forall a, b, c \in R$, 如果 $a \neq 0, ba = ca$, 则 $b = c$ 。

定义9. 一个环称为一个体，如果它满足以下两个条件：

- (1) 它至少含有一个非零元素；
- (2) 非零元素的全体对乘法构成一个群。

定义10. 如果一个体中的乘法满足交换律，则称之为域。

定义11. 有理数集 Q 、实数集 R 、复数集 C 对通常的乘法和加法都构成域。

定理6. 至少有一个非零元素的无零因子有限环是体。

定义12. 仅有有限个元素的体（域）称为有限体（域）。

例. 设 p 为一个素数，则模 p 同余类环 $(Z_p, +, \circ)$ 为一个有限域。

定义13. 设 $(F, +, \circ)$ 为一个域， $\forall a, b \in F$ ， b 除以 a 的商 $\frac{b}{a}$ 定义为 $a^{-1}b$ 。

定理7. 在域 F 中，商有以下性质：

- (1) $\forall a, b, c, d \in F, b \neq 0, d \neq 0, ad = bc \Leftrightarrow \frac{a}{b} = \frac{c}{d}$;
- (2) $\forall a, b, c, d \in F, b \neq 0, d \neq 0, \frac{a}{b} \circ \frac{c}{d} = \frac{ac}{bd}, \frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$;
- (3) $\forall a, b, c, d \in F, b \neq 0, d \neq 0, c \neq 0, \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$ 。

定义14. 设 $(R, +, \circ)$ 为一个环， $S \subseteq R$ ，如果 S 对 R 的加法和乘法也构成一个环，则称 S 为 R 的一个子环。

定义15. 设 $(F, +, \circ)$ 为一个体（域）， $E \subseteq F$ ，如果 E 对 F 的加法和乘法也构成一个体（域），则称 E 为 F 的一个子体（子域）。

定理8. 环 R 的非空子集 S 为 R 的一个子环的充分必要条件是：

- (1) $\forall a, b \in S, a - b \in S$;
- (2) $\forall a, b \in S, ab \in S$ 。

体（域） F 的非空子集 E 为 F 的一个子体（子域）的充分必要条件是：

- (1) $|E| \geq 2$;
- (2) $\forall a, b \in E, a - b \in E$;
- (3) $\forall a, b \in E, a \neq 0, b \neq 0, ab^{-1} \in E$ 。

课后作业题：

练习1. 设 $Z(\sqrt{2}) = \{m + n\sqrt{2} | m, n \in Z\}$ ，其中 Z 为全体整数之集合。试证： $Z(\sqrt{2})$ 对数的通常加法和乘法构成一个环。

练习2. 设 $Q(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} | a, b \in Q\}$ ，其中 Q 为全体有理数之集合。试证： $Q(\sqrt[3]{2})$ 对数的通常加法和乘法不构成一个环。

练习3. 设 e 为环 R 的唯一左单位元，试证 e 为 R 的单位元。

练习4. 设 $(R, +, \circ)$ 为一个有单位元1的环，如果 R 中的元素 a, b 及 $ab - 1$ 均有逆元素，试证 $a - b^{-1}$ 及 $(a - b^{-1})^{-1} - a^{-1}$ 也有逆元素，并且

$$((a - b^{-1})^{-1} - a^{-1})^{-1} = aba - a$$

练习5. 有单位元素的环 R 中零因子没有逆元素。

练习6. 在交换环中二项式定理

$$(a + b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$$

成立。