

近世代数 环和域

任世军

Email: ren_shijun@163.com

哈尔滨工业大学 计算机学院

2008 年 5 月 28 日

目录

- ① 环和域
- ② 无零因子环的特征数
- ③ 同态和理想子环
- ④ 极大理想和费尔玛定理

- 1 环和域
- 2 无零因子环的特征数
- 3 同态和理想子环
- 4 极大理想和费尔玛定理

环的定义

定义13.1.1

设 R 是一个非空集合， R 上有两个代数运算，一个称为加法，用“+”来表示，另一个称为乘法，用“ \circ ”表示。如果下面三个条件成立：

环的定义

定义13.1.1

设 R 是一个非空集合， R 上有两个代数运算，一个称为加法，用“+”来表示，另一个称为乘法，用“ \circ ”表示。如果下面三个条件成立：

- ① $(R, +)$ 是一个Abel群。

环的定义

定义13.1.1

设 R 是一个非空集合， R 上有两个代数运算，一个称为加法，用“+”来表示，另一个称为乘法，用“ \circ ”表示。如果下面三个条件成立：

- ① $(R, +)$ 是一个Abel群。
- ② (R, \circ) 是一个半群。

环的定义

定义13.1.1

设 R 是一个非空集合， R 上有两个代数运算，一个称为加法，用“+”来表示，另一个称为乘法，用“ \circ ”表示。如果下面三个条件成立：

- ① $(R, +)$ 是一个Abel群。
- ② (R, \circ) 是一个半群。
- ③ 乘法对加法满足左右分配律：对 $\forall a, b, c \in R$ 有

$$a \circ (b + c) = a \circ b + a \circ c$$

$$(b + c) \circ a = b \circ a + c \circ a$$

环的定义

定义13.1.1

设 R 是一个非空集合, R 上有两个代数运算, 一个称为加法, 用“+”来表示, 另一个称为乘法, 用“ \circ ”表示。如果下面三个条件成立:

- ① $(R, +)$ 是一个Abel群。
- ② (R, \circ) 是一个半群。
- ③ 乘法对加法满足左右分配律: 对 $\forall a, b, c \in R$ 有

$$a \circ (b + c) = a \circ b + a \circ c$$

$$(b + c) \circ a = b \circ a + c \circ a$$

则称代数系统 $(R, +, \circ)$ 是一个环。

环的一些例子

定义13.1.2

如果环 $(R, +, \circ)$ 的乘法满足交换律, 即对 $\forall a, b \in R$ 有 $a \circ b = b \circ a$, 则称 $(R, +, \circ)$ 是一个交换环或可换环。

环的一些例子

定义13.1.2

如果环 $(R, +, \circ)$ 的乘法满足交换律, 即对 $\forall a, b \in R$ 有 $a \circ b = b \circ a$, 则称 $(R, +, \circ)$ 是一个交换环或可换环。

例13.1.1

整数集合 \mathbb{Z} 对通常的加法和乘法构成一个环 $(\mathbb{Z}, +, \cdot)$, 这个环是一个交换环。

环的一些例子

定义13.1.2

如果环 $(R, +, \circ)$ 的乘法满足交换律, 即对 $\forall a, b \in R$ 有 $a \circ b = b \circ a$, 则称 $(R, +, \circ)$ 是一个交换环或可换环。

例13.1.1

整数集合 \mathbb{Z} 对通常的加法和乘法构成一个环 $(\mathbb{Z}, +, \cdot)$, 这个环是一个交换环。

例13.1.2

有理数集 \mathbb{Q} 、实数集 \mathbb{R} 和复数集 \mathbb{C} 对通常的加法和乘法分别构成交换环 $(\mathbb{Q}, +, \cdot)$ 、 $(\mathbb{R}, +, \cdot)$ 和 $(\mathbb{C}, +, \cdot)$ 。

环的一些例子

定义13.1.2

如果环 $(R, +, \circ)$ 的乘法满足交换律, 即对 $\forall a, b \in R$ 有 $a \circ b = b \circ a$, 则称 $(R, +, \circ)$ 是一个交换环或可换环。

例13.1.1

整数集合 Z 对通常的加法和乘法构成一个环 $(Z, +, \cdot)$, 这个环是一个交换环。

例13.1.2

有理数集 Q 、实数集 R 和复数集 C 对通常的加法和乘法分别构成交换环 $(Q, +, \cdot)$ 、 $(R, +, \cdot)$ 和 $(C, +, \cdot)$ 。

例13.1.3

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

环的一些例子

定义13.1.3

环 $(R, +, \circ)$ 称为有限环, 如果 R 是有限非空集合, 即 $|R| < +\infty$ 。

环的一些例子

定义13.1.3

环 $(R, +, \circ)$ 称为有限环, 如果 R 是有限非空集合, 即 $|R| < +\infty$ 。

例13.1.4

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交换环。

环的一些例子

定义13.1.3

环 $(R, +, \circ)$ 称为有限环, 如果 R 是有限非空集合, 即 $|R| < +\infty$ 。

例13.1.4

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交换环。

例13.1.5 (最小的环)

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。

环的一些例子

定义13.1.3

环 $(R, +, \circ)$ 称为有限环, 如果 R 是有限非空集合, 即 $|R| < +\infty$ 。

例13.1.4

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交换环。

例13.1.5 (最小的环)

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13.1.6

有限环的一类重要例子是模 n 同余类环 $(Z_n, +, \cdot)$, 其中 Z_n 是全体整数集 Z 对模 n 的同余类之集

$$Z_n = \{[0], [1], \dots, [n-1]\}$$

环中的特定术语

- 在环 $(R, +, \cdot)$ 中, 加法的单位元用 0 表示, 并称为 R 的零元 (素)。

环中的特定术语

- 在环 $(R, +, \cdot)$ 中, 加法的单位元用 0 表示, 并称为 R 的零元 (素)。
- 对 $\forall a \in R$, a 对加法的逆元素记为 $-a$, 并称为 a 的负元素。

环中的特定术语

- 在环 $(R, +, \cdot)$ 中, 加法的单位元用 0 表示, 并称为 R 的零元 (素)。
- 对 $\forall a \in R$, a 对加法的逆元素记为 $-a$, 并称为 a 的负元素。
- R 中加法的逆运算称为减法, 并用“-”表示, 对 $\forall a, b \in R$, $a - b$ 定义为 $a + (-b)$ 。

环中的特定术语

- 在环 $(R, +, \cdot)$ 中, 加法的单位元用 0 表示, 并称为 R 的零元 (素)。
- 对 $\forall a \in R$, a 对加法的逆元素记为 $-a$, 并称为 a 的负元素。
- R 中加法的逆运算称为减法, 并用“-”表示, 对 $\forall a, b \in R$, $a - b$ 定义为 $a + (-b)$ 。
- a 对加法的 m 次幂记为 ma , 即如果 $m > 0$ 则 $1a = a, (m + 1)a = ma + a$
$$ma = \underbrace{a + a + \cdots + a}_m$$

如果 $m < 0$ 则 $ma = (-m)(-a)$
如果 $m = 0$ 则 $0a = 0$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

2. $a + b = b + a$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

2. $a + b = b + a$

3. $(a + b) + c = a + (b + c)$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

2. $a + b = b + a$

3. $(a + b) + c = a + (b + c)$

4. $-a + a = a + (-a) = 0$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

2. $a + b = b + a$

3. $(a + b) + c = a + (b + c)$

4. $-a + a = a + (-a) = 0$

5. $-(a + b) = -a - b$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

2. $a + b = b + a$

3. $(a + b) + c = a + (b + c)$

4. $-a + a = a + (-a) = 0$

5. $-(a + b) = -a - b$

6. $a + c = b \Leftrightarrow a = b - c$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

2. $a + b = b + a$

3. $(a + b) + c = a + (b + c)$

4. $-a + a = a + (-a) = 0$

5. $-(a + b) = -a - b$

6. $a + c = b \Leftrightarrow a = b - c$

7. $-(-a) = a$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

2. $a + b = b + a$

3. $(a + b) + c = a + (b + c)$

4. $-a + a = a + (-a) = 0$

5. $-(a + b) = -a - b$

6. $a + c = b \Leftrightarrow a = b - c$

7. $-(-a) = a$

8. $-(a - b) = -a + b$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

2. $a + b = b + a$

3. $(a + b) + c = a + (b + c)$

4. $-a + a = a + (-a) = 0$

5. $-(a + b) = -a - b$

6. $a + c = b \Leftrightarrow a = b - c$

7. $-(-a) = a$

8. $-(a - b) = -a + b$

9. $ma + na = (m + n)a$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$

2. $a + b = b + a$

3. $(a + b) + c = a + (b + c)$

4. $-a + a = a + (-a) = 0$

5. $-(a + b) = -a - b$

6. $a + c = b \Leftrightarrow a = b - c$

7. $-(-a) = a$

8. $-(a - b) = -a + b$

9. $ma + na = (m + n)a$

10. $m(na) = (mn)a$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$
2. $a + b = b + a$
3. $(a + b) + c = a + (b + c)$
4. $-a + a = a + (-a) = 0$
5. $-(a + b) = -a - b$
6. $a + c = b \Leftrightarrow a = b - c$
7. $-(-a) = a$
8. $-(a - b) = -a + b$
9. $ma + na = (m + n)a$
10. $m(na) = (mn)a$
11. $m(a + b) = ma + mb$

环的性质

设 $(R, +, \cdot)$ 是一个环, 对 $\forall a, b, c \in R, m, n \in \mathbb{Z}$, 我们有:

1. $0 + a = a + 0 = a$
2. $a + b = b + a$
3. $(a + b) + c = a + (b + c)$
4. $-a + a = a + (-a) = 0$
5. $-(a + b) = -a - b$
6. $a + c = b \Leftrightarrow a = b - c$
7. $-(-a) = a$
8. $-(a - b) = -a + b$
9. $ma + na = (m + n)a$
10. $m(na) = (mn)a$
11. $m(a + b) = ma + mb$
12. $n(a - b) = na - nb$

环的性质(续)

$$13. (a \circ b) \circ c = a \circ (b \circ c)$$

环的性质(续)

$$13. (a \circ b) \circ c = a \circ (b \circ c)$$

$$14. a \circ (b + c) = a \circ b + a \circ c \quad (b + c) \circ a = b \circ a + c \circ a$$

环的性质(续)

$$13. (a \circ b) \circ c = a \circ (b \circ c)$$

$$14. a \circ (b + c) = a \circ b + a \circ c \quad (b + c) \circ a = b \circ a + c \circ a$$

$$15. 0 \circ a = a \circ 0 = 0$$

环的性质(续)

$$13. (a \circ b) \circ c = a \circ (b \circ c)$$

$$14. a \circ (b + c) = a \circ b + a \circ c \quad (b + c) \circ a = b \circ a + c \circ a$$

$$15. 0 \circ a = a \circ 0 = 0$$

$$16. (-a) \circ b = -(a \circ b), a \circ (-b) = -(a \circ b)$$

环的性质(续)

$$13. (a \circ b) \circ c = a \circ (b \circ c)$$

$$14. a \circ (b + c) = a \circ b + a \circ c \quad (b + c) \circ a = b \circ a + c \circ a$$

$$15. 0 \circ a = a \circ 0 = 0$$

$$16. (-a) \circ b = -(a \circ b), a \circ (-b) = -(a \circ b)$$

$$17. (-a)(-b) = ab$$

环的性质(续)

$$13. (a \circ b) \circ c = a \circ (b \circ c)$$

$$14. a \circ (b + c) = a \circ b + a \circ c \quad (b + c) \circ a = b \circ a + c \circ a$$

$$15. 0 \circ a = a \circ 0 = 0$$

$$16. (-a) \circ b = -(a \circ b), a \circ (-b) = -(a \circ b)$$

$$17. (-a)(-b) = ab$$

$$18. a(b - c) = ab - ac$$

环的性质(续)

$$13. (a \circ b) \circ c = a \circ (b \circ c)$$

$$14. a \circ (b + c) = a \circ b + a \circ c \quad (b + c) \circ a = b \circ a + c \circ a$$

$$15. 0 \circ a = a \circ 0 = 0$$

$$16. (-a) \circ b = -(a \circ b), a \circ (-b) = -(a \circ b)$$

$$17. (-a)(-b) = ab$$

$$18. a(b - c) = ab - ac$$

$$19. (\sum_{i=1}^n a_i)(\sum_{j=1}^m b_j) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$$

环的性质(续)

$$13. (a \circ b) \circ c = a \circ (b \circ c)$$

$$14. a \circ (b + c) = a \circ b + a \circ c \quad (b + c) \circ a = b \circ a + c \circ a$$

$$15. 0 \circ a = a \circ 0 = 0$$

$$16. (-a) \circ b = -(a \circ b), a \circ (-b) = -(a \circ b)$$

$$17. (-a)(-b) = ab$$

$$18. a(b - c) = ab - ac$$

$$19. (\sum_{i=1}^n a_i)(\sum_{j=1}^m b_j) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$$

$$20. (na)b = a(nb) = n(ab)$$

环的性质(续)

$$13. (a \circ b) \circ c = a \circ (b \circ c)$$

$$14. a \circ (b + c) = a \circ b + a \circ c \quad (b + c) \circ a = b \circ a + c \circ a$$

$$15. 0 \circ a = a \circ 0 = 0$$

$$16. (-a) \circ b = -(a \circ b), a \circ (-b) = -(a \circ b)$$

$$17. (-a)(-b) = ab$$

$$18. a(b - c) = ab - ac$$

$$19. (\sum_{i=1}^n a_i)(\sum_{j=1}^m b_j) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$$

$$20. (na)b = a(nb) = n(ab)$$

$$21. \text{如果 } ab = ba, \text{ 那么 } (a + b)^n = \sum_{i=0}^n C_n^i a^i b^{n-i}$$

环的例子（零因子）

例子12.1.7. 令 $C_{[-1,1]}$ 为区间 $[-1,1]$ 上的一切实值连续函数的集合。
在 $C_{[-1,1]}$ 上定义加法和乘法如下： $\forall f, g \in C_{[-1,1]}, x \in [-1, 1]$,

$$(f + g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x)g(x)$$

容易验证 $(C_{[-1,1]}, +, \cdot)$ 是一个环。

考察函数 $f(x), g(x)$, 满足:

$$f(x) = x \quad \text{if} \quad 0 \leq x \leq 1$$

$$f(x) = 0 \quad \text{else}$$

$$g(x) = 0 \quad \text{if} \quad 0 \leq x \leq 1$$

$$g(x) = x \quad \text{else}$$

零因子

定义13.1.4 (零因子的定义)

设 $(R, +, \circ)$ 是一个环, $a \in R$ 。如果存在一个元素 $b \in R$, $b \neq 0$, 使得 $ab = 0$, 则称 a 是 R 的一个左零因子。如果存在一个元素 $c \in R$, 使得 $c \neq 0$, $ca = 0$, 则称 a 为 R 的一个右零因子。如果 a 既是 R 的左零因子, 又是 R 的右零因子, 则称 a 为 R 的零因子。

0是一个零因子。

零因子

定义13.1.4 (零因子的定义)

设 $(R, +, \circ)$ 是一个环, $a \in R$ 。如果存在一个元素 $b \in R$, $b \neq 0$, 使得 $ab = 0$, 则称 a 是 R 的一个左零因子。如果存在一个元素 $c \in R$, 使得 $c \neq 0$, $ca = 0$, 则称 a 为 R 的一个右零因子。如果 a 既是 R 的左零因子, 又是 R 的右零因子, 则称 a 为 R 的零因子。

0是一个零因子。

定义13.1.5 (无零因子环)

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。可换无零因子环称为整环。

无零因子环和体

定理13.1.1

环 R 是无零因子环的充分必要条件是在 R 中乘法满足消去律, 即:

如果 $a \neq 0$, $ab = ac$, 则 $b = c$ 。

如果 $a \neq 0$, $ba = ca$, 则 $b = c$ 。

无零因子环和体

定理13.1.1

环 R 是无零因子环的充分必要条件是在 R 中乘法满足消去律, 即:

如果 $a \neq 0$, $ab = ac$, 则 $b = c$ 。

如果 $a \neq 0$, $ba = ca$, 则 $b = c$ 。

定义13.1.6

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。

无零因子环和体

定理13.1.1

环 R 是无零因子环的充分必要条件是在 R 中乘法满足消去律, 即:

如果 $a \neq 0$, $ab = ac$, 则 $b = c$ 。

如果 $a \neq 0$, $ba = ca$, 则 $b = c$ 。

定义13.1.6

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13.1.7

可换体称为域。

体和域

例13.1.8

有理数环 \mathbb{Q} 、实数环 \mathbb{R} 和复数环 \mathbb{C} 均是体，并且也是域。

体和域

例13.1.8

有理数环 \mathbb{Q} 、实数环 \mathbb{R} 和复数环 \mathbb{C} 均是体，并且也是域。

定理13.1.2

至少有一个非零元素的无零因子有限环是体。

体和域

例13.1.8

有理数环 \mathbb{Q} 、实数环 \mathbb{R} 和复数环 \mathbb{C} 均是体，并且也是域。

定理13.1.2

至少有一个非零元素的无零因子有限环是体。

定义13.1.8

仅有有限个元素的体（域）称为有限体（域）。

体和域

例13.1.8

有理数环 \mathbb{Q} 、实数环 \mathbb{R} 和复数环 \mathbb{C} 均是体，并且也是域。

定理13.1.2

至少有一个非零元素的无零因子有限环是体。

定义13.1.8

仅有有限个元素的体（域）称为有限体（域）。

定理13.1.3

环 $(R, +, \cdot)$ 是体当且仅当 $R \setminus \{0\} \neq \emptyset \ \forall a, b \in R \setminus \{0\}$, 方程 $ax = b (xa = b)$ 在 R 中有解。

体和域

例13.1.8

有理数环 \mathbb{Q} 、实数环 \mathbb{R} 和复数环 \mathbb{C} 均是体，并且也是域。

定理13.1.2

至少有一个非零元素的无零因子有限环是体。

定义13.1.8

仅有有限个元素的体（域）称为有限体（域）。

定理13.1.3

环 $(R, +, \cdot)$ 是体当且仅当 $R \setminus \{0\} \neq \emptyset \ \forall a, b \in R \setminus \{0\}$, 方程 $ax = b (xa = b)$ 在 R 中有解。

定义13.1.9

设 p 是一个素数，则 $(\mathbb{Z}_p, +, \cdot)$ 是一个有限域。

子环、子体（域）

定义13.1.9

环 $(R, +, \cdot)$ 的非空子集 S 若对其中的加法和乘法也形成一个环, 则 S 称为 R 的子环。

子环、子体（域）

定义13.1.9

环 $(R, +, \cdot)$ 的非空子集 S 若对其中的加法和乘法也形成一个环, 则 S 称为 R 的子环。

定义13.1.10

设 $(F, +, \cdot)$ 是体（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（域）。

子环、子体（域）

定理13.1.4

环 R 的非空子集 S 是 R 的子环的充分必要条件是

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

体 F 的非空子集 E 是 F 的一个子体, 当且仅当以下三个条件同时成立:

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

- ① 环和域
- ② 无零因子环的特征数
- ③ 同态和理想子环
- ④ 极大理想和费尔玛定理

例子

在初等代数中, 如果 $a \neq 0$, 那么 $na = a + a + \cdots + a \neq 0$ 是对的。
在环中未必成立。

例子

在初等代数中, 如果 $a \neq 0$, 那么 $na = a + a + \cdots + a \neq 0$ 是对的。
在环中未必成立。

例13.2.1

设 p 是一个素数, 则模 p 剩余类环 Z_p 是一个域。在 Z_p 中同余类 $[1] \neq [0]$,
但 $p[1] = [0]$

例子

在初等代数中, 如果 $a \neq 0$, 那么 $na = a + a + \cdots + a \neq 0$ 是对的。
在环中未必成立。

例13.2.1

设 p 是一个素数, 则模 p 剩余类环 Z_p 是一个域。在 Z_p 中同余类 $[1] \neq [0]$,
但 $p[1] = [0]$

例13.2.2

令 $G_1 = \langle b \rangle, G_2 = \langle c \rangle$ 是两个循环群, b 的阶是无穷, c 的阶是 n , 如果用 $+$ 表示其中的代数运算, 那么 $G_1 = \{mb | m \in Z\}, G_2 = \{0, c, 2c, \cdots, (n-1)c\}$ 。
令 $R = G_1 \times G_2 = \{(mb, kc) | mb \in G_1, kc \in G_2\}$, 在 R 中定义加法和乘法如下:
对 $\forall (m_1b, k_1c), (m_2b, k_2c) \in R, (m_1b, k_1c) + (m_2b, k_2c) = ((m_1 + m_2)b, (k_1 + k_2)c), (m_1b, k_1c) \circ (m_2b, k_2c) = ((m_1m_2)b, (k_1k_2)c)$, 可以证明 R 是一个环。 $(0, 0)$ 为 R 的零元素。 $(b, 0), (0, c)$ 对加法的阶分别为 ∞, n

无零因子环——定理、推论

定理13.2.1

在一个无零因子环中，每个非零元素对加法的阶均相同。

无零因子环——定理、推论

定理13.2.1

在一个无零因子环中，每个非零元素对加法的阶均相同。

推论13.2.1

体和域中每个非零元素对加法的阶均相同。

无零因子环——定理、推论

定理13.2.1

在一个无零因子环中，每个非零元素对加法的阶均相同。

推论13.2.1

体和域中每个非零元素对加法的阶均相同。

定义13.2.1

无零因环中非零元素对加法的阶称为该环的特征数，简称为特征。域（体）中非零元素对加法的阶称为域（体）的特征数，简称为特征。

无零因子环——定理、推论

定理13.2.1

在一个无零因子环中，每个非零元素对加法的阶均相同。

推论13.2.1

体和域中每个非零元素对加法的阶均相同。

定义13.2.1

无零因环中非零元素对加法的阶称为该环的特征数，简称为特征。域（体）中非零元素对加法的阶称为域（体）的特征数，简称为特征。

定理13.2.2

若无零因子环 R 的特征数为正整数 p ，则 p 是素数。

无零因子环——定理、推论

推论13.2.2

整环、体、域的特征数或是无穷大，或是是个素数。

无零因子环——定理、推论

推论13.2.2

整环、体、域的特征数或是无穷大，或是是个素数。

定理13.2.3

在特征为 p 的域里： $(a + b)^p = a^p + b^p$, $(a - b)^p = a^p - b^p$

- ① 环和域
- ② 无零因子环的特征数
- ③ 同态和理想子环**
- ④ 极大理想和费尔玛定理

同构的定义、定理

定义13.3.1

设 $(R, +, \circ)$ 与 $(\bar{R}, \bar{+}, \bar{\circ})$ 是两个环（体、域），如果存在一个一一对应 $\phi: R \rightarrow \bar{R}$ ，使得 $\forall a, b \in R$ 有 $\phi(a + b) = \phi(a) \bar{+} \phi(b)$, $\phi(a \circ b) = \phi(a) \bar{\circ} \phi(b)$ ，则称 R 与 \bar{R} 同构。记为 $R \cong \bar{R}$ ， ϕ 称为称 R 到 \bar{R} 的一个同构映射。

同构的定义、定理

定义13.3.1

设 $(R, +, \circ)$ 与 $(\bar{R}, \bar{+}, \bar{\circ})$ 是两个环（体、域），如果存在一个一一对应 $\phi: R \rightarrow \bar{R}$ ，使得 $\forall a, b \in R$ 有 $\phi(a + b) = \phi(a) \bar{+} \phi(b)$, $\phi(a \circ b) = \phi(a) \bar{\circ} \phi(b)$ ，则称 R 与 \bar{R} 同构。记为 $R \cong \bar{R}$ ， ϕ 称为称 R 到 \bar{R} 的一个同构映射。

定理13.3.1

设 $(R, +, \circ)$ 是一个环（体、域），与 $(\bar{R}, \bar{+}, \bar{\circ})$ 是一个具有两个代数运算的代数系，如果存在一个一一对应 $\phi: R \rightarrow \bar{R}$ ，使得上面的条件（满足运算）成立。则 \bar{R} 是一个环（体、域）。

同态的定义、定理

定义13.3.2

设 $(R, +, \circ)$ 与 $(\bar{R}, \bar{+}, \bar{\circ})$ 是两个环(体、域), 如果存在一个映射 $\phi: R \rightarrow \bar{R}$, 使得 $\forall a, b \in R$ 有 $\phi(a + b) = \phi(a) \bar{+} \phi(b)$, $\phi(a \circ b) = \phi(a) \bar{\circ} \phi(b)$, 则称 R 与 \bar{R} 同态, ϕ 称为称 R 到 \bar{R} 的一个同态映射。如果 ϕ 是满射, 则称 ϕ 为满同态, 记为 $R \sim \bar{R}$ 。

同态的定义、定理

定义13.3.2

设 $(R, +, \circ)$ 与 $(\bar{R}, \bar{+}, \bar{\circ})$ 是两个环（体、域），如果存在一个映射 $\phi: R \rightarrow \bar{R}$ ，使得 $\forall a, b \in R$ 有 $\phi(a + b) = \phi(a) \bar{+} \phi(b)$, $\phi(a \circ b) = \phi(a) \bar{\circ} \phi(b)$ ，则称 R 与 \bar{R} 同态， ϕ 称为称 R 到 \bar{R} 的一个同态映射。如果 ϕ 是满射，则称 ϕ 为满同态，记为 $R \sim \bar{R}$ 。

定理13.3.2

设 ϕ 是一个从环 R 到环 \bar{R} 的同态，则：

- (1) $\phi(0) = \bar{0}$
- (2) 如果环 R 和环 \bar{R} 分别有单位元 e, \bar{e} ，则 $\phi(e) = \bar{e}$
- (3) $\forall a \in R, \phi(-a) = -\phi(a)$
- (4) 如果 $a \in R$ ， a 有逆元素 a^{-1} ，则 $\phi(a^{-1}) = (\phi(a))^{-1}$
- (5) 如果 S 是 R 的一个子环，则 $\phi(S)$ 是 \bar{R} 的一个子环。
- (6) 如果 \bar{S} 是 \bar{R} 的一个子环，则 $\phi^{-1}(\bar{S})$ 是 R 的一个子环。

理想的定义、例子

定义13.3.3

环 R 的子环 N 称为 R 的左(右)理想(子环), 如果对 $\forall r \in R, rN \subseteq N (Nr \subseteq N)$ 。如果 N 既是 R 的左理想, 又是 R 的右理想, 则称 N 是 R 的理想。

理想的判定条

件: (1) $\forall n_1, n_2 \in N, (n_1 - n_2) \in N$ (2) $\forall r \in R, n \in N, rn \in N, nr \in N$

理想的定义、例子

定义13.3.3

环 R 的子环 N 称为 R 的左(右)理想(子环), 如果对 $\forall r \in R, rN \subseteq N (Nr \subseteq N)$ 。如果 N 既是 R 的左理想, 又是 R 的右理想, 则称 N 是 R 的理想。

理想的判定条

件: (1) $\forall n_1, n_2 \in N, (n_1 - n_2) \in N$ (2) $\forall r \in R, n \in N, rn \in N, nr \in N$

例13.3.1

设 $N = \{2n | n \in \mathbb{Z}\}$, 则 N 是 \mathbb{Z} 的一个子环, 并且还是理想。

理想的定义、例子

定义13.3.3

环 R 的子环 N 称为 R 的左(右)理想(子环), 如果对 $\forall r \in R, rN \subseteq N (Nr \subseteq N)$ 。如果 N 既是 R 的左理想, 又是 R 的右理想, 则称 N 是 R 的理想。

理想的判定条

件: (1) $\forall n_1, n_2 \in N, (n_1 - n_2) \in N$ (2) $\forall r \in R, n \in N, rn \in N, nr \in N$

例13.3.1

设 $N = \{2n | n \in \mathbb{Z}\}$, 则 N 是 \mathbb{Z} 的一个子环, 并且还是理想。

例13.3.2

设 a 是可换环 R 的一个元素, 则 R 中一切形如 $ra + na (r \in R, n \in \mathbb{N})$ 的元素构成的集合是 R 的一个理想子环。

理想的定理

定理13.3.2

设 $\{H_l\}_{l \in I}$ 是环 R 的理想构成的集族, 则 $\bigcap_{l \in I} H_l$ 是 R 的理想。

理想的定理

定理13.3.2

设 $\{H_l\}_{l \in I}$ 是环 R 的理想构成的集族, 则 $\bigcap_{l \in I} H_l$ 是 R 的理想。

推论13.3.1

设 A 是环 R 的一个非空子集, 则 R 中包含 A 的所有理想的交还是 R 理想。

理想的定理

定理13.3.2

设 $\{H_l\}_{l \in I}$ 是环 R 的理想构成的集族, 则 $\bigcap_{l \in I} H_l$ 是 R 的理想。

推论13.3.1

设 A 是环 R 的一个非空子集, 则 R 中包含 A 的所有理想的交还是 R 理想。

定义13.3.4

设 A 是环 R 的一个非空子集, 则 R 中包含 A 的所有理想的交称为由 A 生成的理想, 记为 (A) 。若 $A = \{a\}$, 则记 $(A) = (a)$ 。若 $A = \{a_1, a_2, \dots, a_n\}$, 则 $(A) = (a_1, a_2, \dots, a_n)$ 。由一个元素 a 生成的理想 (a) 称为 R 的主理想。

理想的定理

定理13.3.2

设 $\{H_l\}_{l \in I}$ 是环 R 的理想构成的集族, 则 $\bigcap_{l \in I} H_l$ 是 R 的理想。

推论13.3.1

设 A 是环 R 的一个非空子集, 则 R 中包含 A 的所有理想的交还是 R 理想。

定义13.3.4

设 A 是环 R 的一个非空子集, 则 R 中包含 A 的所有理想的交称为由 A 生成的理想, 记为 (A) 。若 $A = \{a\}$, 则记 $(A) = (a)$ 。若 $A = \{a_1, a_2, \dots, a_n\}$, 则 $(A) = (a_1, a_2, \dots, a_n)$ 。由一个元素 a 生成的理想 (a) 称为 R 的主理想。

定理13.3.3

体(域)中只有两个理想, 它们是 $\{0\}$ 和体(域)自身。

- 1 环和域
- 2 无零因子环的特征数
- 3 同态和理想子环
- 4 极大理想和费尔玛定理**

极大理想和费尔玛定理

定义13.5.1

环 R 的理想子环 H 称为 R 的极大理想子环,如果 H 是 R 的真理想并且 R 不存在真理想 N 使得 $H \subset N$ 。

极大理想和费尔玛定理

定义13.5.1

环 R 的理想子环 H 称为 R 的极大理想子环,如果 H 是 R 的真理想并且 R 不存在真理想 N 使得 $H \subset N$ 。

例13.5.1

设 p 是一个素数,则由 p 生成的主理想 (p) 是整数环 \mathbb{Z} 的极大理想子环。

极大理想和费尔玛定理

定义13.5.1

环 R 的理想子环 H 称为 R 的极大理想子环,如果 H 是 R 的真理想并且 R 不存在真理想 N 使得 $H \subset N$ 。

例13.5.1

设 p 是一个素数,则由 p 生成的主理想 (p) 是整数环 Z 的极大理想子环。

证: 设 N 是 Z 的一个理想, 并且 $(p) \subset N$, 于是有一个元素 $a \in N$, 但是 $a \notin (p)$, 所以 p 不整除 a , 从而 $(a, p) = 1$, 所以存在两个整数 $r_1, r_2 \in Z$, 使得 $r_1 a + r_2 p = 1$, 由于 N 是理想并且 $a \in N, p \in (p) \subset N$, 故 $1 = r_1 a + r_2 p \in N$, 这样就有 $N = Z$ 。所以 (p) 是极大理想。

这个例子的逆也成立。

极大理想和费尔玛定理(续)

定理13.5.1

设 R 是一个有单位元 e 的可换环, H 是 R 的理想。 R/H 是域当且仅当 H 是 R 的极大理想子环。

极大理想和费尔玛定理(续)

定理13.5.1

设 R 是一个有单位元 e 的可换环, H 是 R 的理想。 R/H 是域当且仅当 H 是 R 的极大理想子环。

证: \Rightarrow)

R/H 是域, $H \subset N$, N 是 R 的理想, 有 $a \in N, a \notin H, a + H \neq H$,
有 $x \in R$ 使得 $(a + H)(x + H) = e + H$, 故有 $h \in H$ 使得 $e = ax + h \in N$,
故 $N = R$

极大理想和费尔玛定理(续)

定理13.5.1

设 R 是一个有单位元 e 的可换环, H 是 R 的理想。 R/H 是域当且仅当 H 是 R 的极大理想子环。

证: \Rightarrow)

R/H 是域, $H \subset N$, N 是 R 的理想, 有 $a \in N, a \notin H, a + H \neq H$, 有 $x \in R$ 使得 $(a + H)(x + H) = e + H$, 故有 $h \in H$ 使得 $e = ax + h \in N$, 故 $N = R$

\Leftarrow)

H 为 R/H 的零元素, $e + H$ 是 R/H 的单位元素, 只须证明对 $\forall a + H \in R/H, a \notin H, a + H$ 可逆就可以了。即 $\exists x \in R$, 使得 $(a + H)(x + H) = e + H$, 即 $ax - e \in H$, 令 $N = h + ax | h \in H, x \in R$, 显然 N 为 R 的理想并且 $H \subset N$, 所以有 $N = R$, 从而有 $x \in R, h \in H$ 使得 $h + ax = e$, 这样有 $(a + H)(x + H) = e + H$ 。故 R/H 是域。

极大理想和费尔玛定理(续)

定理13.5.2(费尔玛)

设 $p > 2$ 是一个整数。如果存在正整数 $x, 1 < x < p$ 使得

(1) $x^{p-1} \equiv 1 \pmod{p}$ 并且

(2) $x^i \not\equiv 1 \pmod{p}, i = 1, 2, \dots, p-1$

则 p 是一个素数。

又若 p 是一个素数, 则对任何正整数 a 有: $a^p \equiv a \pmod{p}$ 。