





# 近世代数

计算机科学与技术学院  
唐琳琳



# 内容

- 第一章 基本概念
- 第二章 群
- 第三章 正规子群和群的同态与同构
- 第四章 环与域
- 第五章 因子分解
- 第六章 域的扩张

# 第四章 环与域

- 环的定义
- 环的零因子和特征
- 除环和域
- 模 $n$ 剩余类环
- 环与域上的多项式环
- 理想
- 商环与环同态基本定理
- 素理想和极大理想
- 非交换环

# 环的零因子和特征

- **定义1:** 设  $a \neq 0$  是环  $R$  的一个元素。如果在  $R$  中存在元素  $b \neq 0$  使  $ab = 0$ ，称  $a$  为环  $R$  的一个左零因子。

同样可以定义环  $R$  的一个右零因子。

左、右零因子统称为零因子，只在有必要区分时才加左右。

- **例1:** 设  $R$  为由一切形如 
$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \quad (x, y \in Q)$$

的方阵关于方阵的普通加法和乘法做成的环，则  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$  是  $R$  的一个左零因子，  
因为

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

但  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$  不是  $R$  的右零因子，因为，若

$$\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

则只有  $x = y = 0$ 。

# 环的零因子和特征

- **例2:** 数域F上二阶全阵环中,  $\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}$  既是左零因子又是右零因子, 因为

$$\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad .$$

- **注:**

- 1) 数环以及数域上的多项式环, 都无零因子。
- 2) 在无零因子的环中, 关于乘法的消去律成立。

- **定理1:** 在环R中, 若  $a$  不是左零因子, 则

$$ab = ac, a \neq 0 \Rightarrow b = c \quad ; \quad (1)$$

若  $a$  不是右零因子, 则

$$ba = ca, a \neq 0 \Rightarrow b = c \quad . \quad (2)$$

证明: 由  $ab = ac$ , 得

$$a(b - c) = 0$$

由于  $a \neq 0$  且  $a$  不是左零因子, 故  $b - c = 0$ ,  $b = c$ 。同理可证另一结论。

# 环的零因子和特征

- 若对环 $R$ 中任意元素  $a \neq 0, b, c$  , (1)成立, 则称环 $R$ 满足左消去律; 若(2)成立, 则称环 $R$ 满足右消去律。
- **推论:** 若环 $R$ 无左(或右)零因子, 则消去律成立; 反之, 若 $R$ 中有一个消去律成立, 则 $R$ 无左及右零因子, 且另一个消去律也成立。

证明:  $R$ 无左零因子时,  $R$ 也无右零因子。即

$$\text{无左零因子} \Leftrightarrow \text{无右零因子}$$

故由定理1即得消去律成立。

反之, 设在环 $R$ 中左消去律成立, 且

$$a \neq 0, ab = 0 \quad , \quad \text{即} \quad ab = a0$$

则  $b = 0$  , 即 $R$ 无左零因子, 从而 $R$ 也无右零因子, 于是 $R$ 也满足右消去律。

# 环的零因子和特征

- **定义2**：阶大于1、有单位元且无零因子的交换环称为**整环**。
- **例**：整数环和数域上的多项式环都是整环。例1，例2中的方阵环都不是整环。
- **定义3**：若环R的元素（对加法）有最大阶n，则称n为环**R的特征**（或**特征数**）。
- **注**：
  - 1) 若环R的元素（对加法）无最大阶，则称R的**特征是无限（或零）**。
  - 2) 用**char R**表示环R的特征。
  - 3) 有限环的特征必有限；无限环特征未必无限。
  - 4) 只含有零元素的环，其特征是1；在数环中除了 $\{0\}$ 外，其他环的特征均无限。
  - 5) 通常环中各元素的阶（对加法）是不相等的。但对于无零因子环，情况特殊。

以下关于环的说法正确的是（）

- ☒ A 环是有两个代数运算的代数系统
- ☐ B 环与其子环的单位元相同
- ☒ C 素数阶环必为循环环
- ☒ D 环中有左零因子就有右零因子

提交



# 环的零因子和特征

• **定理2:** 设 $R$ 是一个无零因子环, 且 $|R| > 1$ 。则

1)  $R$ 中所有非零元素 (对加法) 的阶均相同。

2) 若 $R$ 的特征有限, 则必为素数。

证明: 1) 若所有非零元素的阶均无限, 从无限的角度上讲, 各个元素的阶相同成立。

若 $R$ 中有某个元素 $a \neq 0$ , 它的阶为 $n$ , 则在环 $R$ 中任取一个元素 $b \neq 0$ , 有

$$a(nb) = (na)b = 0b = 0$$

但 $a \neq 0$ , 又是无零因子环, 故有 $nb = 0, |b| \leq n$ 。

若设 $|b| = m$ , 则 $(ma)b = a(mb) = a0 = 0$ , 由于 $b \neq 0$ , 且 $R$ 为无零因子环, 故 $ma = 0$ , 于是有 $n|m$ , 从而 $n \leq m = |b|$ , 故 $|b| = n$ 。

因此, 原结论, 所有非零元素 (对加法) 的阶均相同。

# 环的零因子和特征

2) 设  $\text{char } R = n > 1$ , 且

$$n = n_1 n_2, \quad 1 < n_i < n$$

则在  $R$  中任取  $a \neq 0$ , 由于  $R$  中每个非零元的阶都为  $n$ , 故

$$n_1 a \neq 0, \quad n_2 a \neq 0$$

而

$$(n_1 a)(n_2 a) = (n_1 n_2) a^2 = n a^2 = 0$$

这与  $R$  是一个无零因子环矛盾, 故假设不成立, 即  $\text{char } R = n$ ,  $n$  必为素数。

- 注: 任何阶大于1的有限无零因子环, 特征都是素数。
- 若无零因子环  $R$  的特征是素数  $p$ , 且  $R$  为一交换环, 则对  $R$  中任意元素  $a_1, a_2, \dots, a_n$  必有

$$(a_1 + a_2 + \cdots + a_n)^p = a_1^p + a_2^p + \cdots + a_n^p$$

# 环的零因子和特征

• **定理3**：若环 $R$ 有单位元，则单位元在加群 $(R, +)$ 中的阶就是 $R$ 的特征。

证明：若单位元 $1$ 在 $(R, +)$ 中阶无限，则 $R$ 的特征无限；若 $1$ 的阶是正整数 $n$ ，则在 $R$ 中任取  $a \neq 0$ ，有

$$na = (n \cdot 1)a = 0a = 0$$

即 $n$ 是 $R$ 中非零元素的最大阶，亦即

$$\text{char} R = n$$

# 除环和域

- **定义1**：设 $R$ 是一个环。如果 $|R| > 1$ ，又 $R$ 有单位元且每个非零元都有逆元，则称 $R$ 是一个除环（或体）。
- 可换除环称为域。

• 注：

1) 数域都是域；

2) 整数环是有单位元且无零因子的交换环，即整环，但不是域。

- **定理1**：除环和域没有零因子。

证明:设 $R$ 是一个除环， $a \in R$ 。如果

$$a \neq 0, \quad ab = 0$$

则  $b = a^{-1}(ab) = 0$ ，从而可知 $R$ 无零因子。

- 注：除环和域的特征只能是素数或无限。

# 除环和域

• 例1：令

$$D = \{a \cdot 1 + bi + cj + dk \mid a, b, c, d \in R\}$$

并称D中元素为四元数。另规定系数为零的项可以略去不写，且

$$a1 = a, \quad 1i = i, \quad 1j = j, \quad 1k = k$$

于是

$$G = \{1, i, j, k, -1, -i, -j, -k\} \subseteq D$$

依据G（四元数群）的乘法定义D上的相等、加法、乘法：

相等：对应系数相等

加法：对应系数相加

乘法：四元数群上的乘法

可以验证在此加法和乘法下，D作成环，1是单位元。又因为

$$(a - bi - cj - dk)(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$$

# 除环和域

故当  $a + bi + cj + dk \neq 0$  (即a, b, c, d不全为0) 时有逆元, 且

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$

因此, D作成一個除环, 通常称为四元数除环。

由于  $ij \neq ji$ , 故四元数除环是一个无限非可换除环。

- 注: 有限除环必为域。----魏德邦定理。
- 定理2: 阶数大于1的有限环若有非零非零因子元素, 则其有单位元; 且每个非零非零因子元素都是可逆元。

证明: 设  $a \neq 0$  是有限环中任一非零因子元素, 则  $a, a^2, a^3, \dots$  中必有相等的, 不妨设  $a^m = a^n$ ,  $1 \leq m < n$ , 于是有  $a^{m-1}(a - a^{n-m+1}) = 0$ , 但  $a \neq 0$ , 且a不是零因子, 故  $a = a^{n-m+1}$ 。对任意  $x \in R$  有

$$ax = a^{n-m+1}x, \quad a(x - a^{n-m}x) = 0, \quad x = a^{n-m}x$$

同理  $xa^{n-m} = x$ , 即得  $a^{n-m}$  为环R单位元。

# 除环和域

由  $a \cdot a^{n-m-1} = a^{n-m-1} \cdot a = a^{n-m}$  可知,  $a$  是  $R$  的可逆元。

- **推论:** 阶大于1的有限环  $R$  若无零因子, 则必为除环。
- 根据魏德邦定理可知这样的环还是一个域。
- **定理3:** 设  $R$  是环且  $|R| > 1$ 。则  $R$  是除环当且仅当对  $R$  中任意元素  $a \neq 0, b$ , 方程

$$ax = b \quad (\text{或 } ya = b)$$

在  $R$  中有解。

证明: 必要性显然。

充分性:

1) 对  $\forall a \neq 0, b \neq 0$ , 因方程  $ax = b$  在  $R$  中有解, 可设为  $c$ , 即有

$$ac = b$$

同样设  $bx = c$  的解为  $d$ , 则有  $bd = c$ , 于是

$$abd = ac = b \neq 0$$

故  $ab \neq 0$ , 即  $R$  无零因子。

# 除环和域

2) 证明R有单位元。在R中任取  $a \neq 0$  。因方程  $ax = a$  在R中有解，设为e，即

$$ae = a$$

从而有

$$ae^2 = ae$$

由于  $a \neq 0$ ，R中无零因子，故有  $e^2 = e \neq 0$  。

对任意的  $b \in R$ ，有

$$(be - b)e = 0, \quad e(eb - b) = 0$$

但  $e \neq 0$ ，R无零因子，故有

$$be = eb = b$$

即e为R的单位元。

3) 证明非零元都有逆元。在R中任取  $a \neq 0$  。因方程  $ax = e$  在R中有解，设为  $a'$  即有  $aa' = e$  。下证  $a'a = e$  。实际上，

$$(a'a - e)a' = a'(aa') - a' = a'e - a' = 0$$



# 除环和域

但  $a' \neq 0$ ,  $R$  无零因子, 必有

$$a'a - e = 0, \quad a'a = e$$

即  $a$  在  $R$  中有逆元。

故  $R$  为一个除环。

- 环中----“加、减、乘”

- 除环（或域）中----“加、减、乘、除”（除环不一定可换故  $a^{-1}b (a \neq 0)$ 、 $ba^{-1}$  虽然有意义, 但不一定相等)

- 当上两式相等即  $a^{-1}b = ba^{-1}$  时, 可统一的记为  $\frac{b}{a}$ , 即  $\frac{b}{a} = a^{-1}b = ba^{-1} \quad (a \neq 0)$ 。

由此得“除法”的运算法则:

$$1) \frac{b}{a} = \frac{d}{c} \Leftrightarrow ad = bc \qquad 2) \frac{b}{a} + \frac{d}{c} = \frac{bc + ad}{ac}$$

$$3) \frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac} \qquad 4) \frac{\frac{b}{a}}{\frac{d}{c}} = \frac{bc}{ad}$$

这其中,  $a \neq 0, c \neq 0$

# 除环和域

- 子除环、子域：

$$a, b \in F_1 \Rightarrow a - b \in F_1$$

$$0 \neq a, b \in F_1 \Rightarrow a^{-1}b \in F_1$$

域F中的子集  $F_1$ ，成子除环、子域的充分必要条件。

- 每个有理数都是二整数之商，且有理数域是包含整数环的最小数域。由此引出一般的整环和域之间的关系推广：

- **定义2：** 设R是一个整环，K是包含R为其子环的一个域。则

$$F = \left\{ \frac{b}{a} = a^{-1}b \mid 0 \neq a, b \in R \right\}$$

作成K的一个包含R为其子环的子域（而且是包含R的最小域）。称F为整环R的**分式域**或**商域**。

- 分式域是存在的，而且对环的加法与乘法来说，**同构整环的分式域必同构**。

# 除环和域

- **定义3**：设 $R$ 是一个有单位元的环，则 $R$ 的可逆元也称为 $R$ 的**单位**； $R$ 的全体可逆元（单位）作成的群，称为 $R$ 的**乘群**或**单位群**，并用 $R^*$ 或 $U(R)$ 表示。

- 例如：整数环 $\mathbb{Z}$ 和12阶循环环  $R_{12} = \{0, e, 2e, \dots, 11e\} (e^2 = e)$  的单位群分别为

$$\mathbb{Z}^* = \{1, -1\}, \quad R_{12}^* = \{e, 5e, 7e, 11e\}$$

其中 $R_{12}^*$  的单位元是 $e$ ，且每个元素的逆元为自身。

- 数域 $F$ 上的 $n$ 阶全阵环的单位群是全体 $n$ 阶满秩方阵对乘法作成的群，即 $F$ 上的 $n$ 阶线性群  $GL_n(F)$ 。

# 除环和域

• 例2：证明：

$$Z[i] = \{a + bi \mid a, b \in Z\}$$

作成一个整环（这个环称为Gauss整环），并且其单位群是  $\{\pm 1, \pm i\}$ 。

证明： $Z[i]$  作成整环显然。又显然  $\pm 1, \pm i$  均为其单位。下证  $Z[i]$  没有别的单位。

设  $\varepsilon = a + bi$  是  $Z[i]$  的任一单位，则有  $\eta \in Z[i]$  使

$$\varepsilon\eta = 1, \quad |\varepsilon|^2 |\eta|^2 = 1 \quad .$$

这里只有  $|\varepsilon|^2 = a^2 + b^2 = 1$ ，从而只有

$$a = \pm 1, b = 0 \text{ 或 } a = 0, b = \pm 1$$

即  $\varepsilon$  只能是  $\pm 1$  及  $\pm i$ 。

因此， $\pm 1$  和  $\pm i$  是环  $Z[i]$  的全部单位。故

$$U(Z[i]) = \{\pm 1, \pm i\}$$

# 除环和域

• 考虑：

$$(a+bi)(a-bi)=a^2+b^2\Rightarrow (a+bi)^{-1}=\frac{a-bi}{a^2+b^2}$$

从而有  $a^2+b^2=1$ ，故只能有  $a=\pm 1, b=0$  或  $a=0, b=\pm 1$ 。即得证。

# 作业：

- P141. 2、证明：数域上 $n$ 阶全阵环的元素  $A \neq 0$  若不是零因子，就是可逆元（即可逆方阵）。

- 3、设 $P(M)$ 为集合 $M$ 的幂集。

- 1) 证明 $P(M)$ 对运算

$$A + B = A \cup B - A \cap B, \quad AB = A \cap B \quad (\forall A, B \subseteq M)$$

作成有一个单位元的交换环（此环成为 $M$ 的幂集环）

- 2)  $P(M)$  的零因子为何？其特征又为何？