

本节我们将依据环结构中乘法运算的性质，对环作简单的分类，并对一些具有重要性质的环作简单介绍，

首先，可以根据环中是否存在单位元，将其分为两类：有 1 的环和没有 1 的环，例如，整数环 $\mathbb{Z}$ 是有 1 的环，而 $2\mathbb{Z}$ (偶数构成的环)就是一个没有 1 的环，

其次，可以根据环的乘法运算是否具有交换律，将环分为两类：交换环($ab=ba$, 任意 a, b)和非交换环($ab \neq ba$, 存在 a, b)，

例如，整数环 $\mathbb{Z}$ 为交换环，实数域 $\mathbb{R}$ 上的矩阵环 $M_n(\mathbb{R})$ 为非交换环，

再次，可以根据环中元素的个数，将环分为两类：有限环($|R| < \infty$)和无限环($|R| = \infty$)，

另外，若仔细考察实数域 $\mathbb{R}$ 上的矩阵环 $M_2(\mathbb{R})$ ，

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

也就是说两个不为 0 的元素乘积是 0，

这与我们通常遇到的整数、有理数、实数和复数的运算性质是完全不同的，

事实上，具有这种性质的环还有很多，

例如，模 6 的剩余类环 $\mathbb{Z}_6(\bar{2}, \bar{3} \neq 0, \bar{2}\bar{3}=0)$ 就是其中的一个，

因此，我们完全可以依据环的乘法运算是否具有非零元素的乘积是零的性质，将环分为两类：“有这种性质”的环和“没有这种性质”的环，

定义 2.1 设 R 是一个环，如果对于 R 的非零元素 a, b ，有 $ab=0$ ，

则称 a 是环 R 的左零因子， b 是环 R 的右零因子，

特别地，若 R 的一个元素既是左零因子，又是右零因子，则称它是 R 的零因子

注意，环的可逆元一定不是(左、右)零因子，

(左、右)零因子也一定不是可逆元，

现在，我们可以依据环是否具有零因子，

将环分为两类：有零因子环和无零因子环，

例 2.1 整数环是无零因子环，而实数域 R 上的矩阵环 $M_2(R)$ 是有零因子环
事实上，在 $M_2(R)$ 中，有

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

即 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ 是 $M_2(R)$ 的零因子，

命题 2.1 当且仅当环 R 的乘法运算具有左(或右)消去律时，
环 R 无左(或右)零因子

即若 $ax=ay$ 且 $a \neq 0$ ，则 $x=y$ (或若 $xa=ya$ 且 $a \neq 0$ ，则 $x=y$)，

证: ($\Rightarrow$) 若 $ax=ay$ ，则 $a(x-y)=0$ ，

因为环 R 无左(或右)零因子，所以当 $a \neq 0$ 时，必有 $x-y=0$ ，即 $x=y$ ，

因此，环 R 的乘法运算具有左消去律，

若 $xa=ya$ ，则 $(x-y)a=0$ ，

因为环 R 无左(或右)零因子，所以当 $a \neq 0$ 时，必有 $x-y=0$ ，即 $x=y$ ，

因此，环 R 的乘法运算具有右消去律，

($\Leftarrow$) 反证，假设 R 有左零因子 a ，则在 R 中存在非零元 b ，使得 $ab=0$ ，

另外，由 R 的乘法运算具有左(或右)消去律及 $ab=0$ (或 $ab=0b$)

可推得 $b=0$ (或 $a=0$)，矛盾，所以 R 中无左零因子，

类似地，若 R 的乘法运算具有左(或右)消去律，则 R 中无右零因子，

无零因子环中有三类重要的环：整环、域和除环，

下面我们分别介绍这几种环的概念和简单性质，

一、整环

定义 2.2 称非零的、有 1 的、交换的无零因子环为整环，

由整环的定义可知，整环至少含有两个元素 0 和 1，并且 $0 \neq 1$ ，

例 2.2 整数环 Z ，有理数域 Q ，实数域 R ，复数域 C ，

以及其上的一元多项式环 $Z[x]$ ， $Q[x]$ ， $R[x]$ ， $C[x]$ 都是整环，

而矩阵环 $M_n(R)$ ($n > 1$) 不是整环，

另外，剩余类环 Z_p (p 是素数) 是整环，但 Z_n (n 不是素数) 不是整环，

例 2.3 设自然数 $n > 1$ ，试证明当且仅当 n 是素数时， $\{Z_n; +, \cdot\}$ 是整环，

证: $(\Rightarrow)$ 反证，假设 n 不是素数，则存在属于 Z 的 a, b ，使得 $n = ab, 1 < a, b < n$ ，

从而 $\bar{0} = \bar{n} = \bar{a}\bar{b}$ ， $\bar{a} \neq \bar{0}$ ， $\bar{b} \neq \bar{0}$ ，

这就是说， Z_n 中有零因子，即 Z_n 不是整环，矛盾，因此， n 是素数，

$(\Leftarrow)$ 反证，假设 $\{Z_n; +, \cdot\}$ 不是整环，则 Z_n 有零因子，

令 $\bar{a}$ 是 Z_n 的一个零因子，则存在不为 $\bar{0}$ 的 $\bar{b}$ ，使得 $\bar{a}\bar{b} = \bar{0}$ ，从而 $n | ab$ ，

又因为 n 是素数，所以 $n | a$ 或者 $n | b$ ，从而 $\bar{a} = \bar{0}$ 或者 $\bar{b} = \bar{0}$ ，矛盾，

因此， $\{Z_n; +, \cdot\}$ 是整环，

例 2.4 设 R 是有单位元的交换环， R_0 是 R 的子环，且与 R 有相同的单位元，

对属于 R 的 α ，我们定义 $R_0[\alpha] = \{a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_0 \mid a_0, a_1, \cdots, a_n \in R, n \in N\}$ ，

则可知 $R_0[\alpha]$ 是 R 的子环，且是有单位元的交换环，

若 R 是整环，则 R 具有左消去律，

当然子环 $R_0[\alpha]$ 也具有左消去律，从而 $R_0[\alpha]$ 也是整环，

我们知道整数环是复数域的子环，

因此， $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$ ， $Z[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in Z\}$ ，

$Z[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in Z\}$ 和 $Z[i] = \{a + bi \mid a, b \in Z\}$ 都是整环，

整环的元素具有一个非常好的性质：

任意两个非零元素在加法群中的阶都相等，

命题 2.2 若 $\{R; +, \cdot\}$ 是整环，

则在加法群 $\{R; +\}$ 中，任意两个非零元素的阶都相等，

证: 因为对属于 R 的任意 $a, b, a \neq 0, b \neq 0, n$ 属于 Z^+ (正整数集合)，

从 $(na)b = a(nb)$ 可知 $na = 0 \Leftrightarrow nb = 0$ ，

所以， $\{R; +\}$ 中的任意两个非零元素的阶都相等

命题 2.3 令 $\{R; +, \cdot\}$ 是整环，若 p 是 $\{R; +\}$ 中非零元素的阶，则 p 是素数，

证：反证，若 p 不是素数，则可以令 $p=mn, 1 < m, n < p$,

那么对属于 R 的任意 $a, a \neq 0$ ，有 $0=pa=m(na)$ ，

若 $na \neq 0$ ，则 na 的阶是 $p, p|m$ ，这与 $m < p$ 矛盾，

若 $na=0$ ，则 $p|n$ ，这与 $n < p$ 矛盾，

因此 p 一定是素数，

定义 2.3 设 $\{R; +, \cdot\}$ 是整环，

若存在最小的正整数 n ，使得对属于 R 的任意 a ，有 $na=0$ ，

则称 n 为环 R 的特征，记其为 $\text{Char } R=n$;

否则称 R 的特征是 0 ，并记其为 $\text{Char } R=0$ ，

因为在整环中非零元素的阶都相等，

所以在求整环的特征时，只需要考虑单位元的阶就可以了，

例如，数环 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 的特征均为 0 ，

类似地，易知数域 F 上的一元多项式环 $F[x]$ ，高斯整环 $\mathbb{Z}[i]$ 的特征都是 0 ，

但是，剩余类环 $\mathbb{Z}_p$ (p 是素数) 的特征是 p ，

另外，整环的特征是素数或是 0 ，

若整环 R 是有限环，则 R 的特征一定是素数，且是 $|R|$ 的因数，

二、域

定义 2.4 设 F 是非零的、有 1 的交换环，
若 F 的每个非零元都可逆，则称 F 是域，

定义 2.4' 令 $\{F; +, \cdot\}$ 是至少含有两个元素的代数系统，若它具有下列性质：

- (1) $\{F; +\}$ 是交换群；
 - (2) $\{F^*; \cdot\}$ 是交换群 ($F^* = F - \{0\}$)；
 - (3) 运算“ $\cdot$ ”对“ $+$ ”具有分配律，
- 则称 F 是域，

显然，域是整环，但整环却不一定是域，
例如，我们熟知的 Q, R, C 等都是域，但 Z 是整环，却不是域，
因为其中的 2 没有逆元，
同样地，在高斯整环 $Z[i]$ 中，
由于 $1+i$ 没有逆元，因此 $Z[i]$ 是整环，却不是域，
因为域也是整环，所以，域有特征，域的特征为素数或 0 ，

命题 2.4 有限整环是域

证： 设 R 是有限整环，则 R 是非零的、有 1 的交换环，
令 $R^* = R - \{0\}$ ，为证 R 是域，我们仅需证明 $\{R^*; \cdot\}$ 是群，
因为整环无零因子，因此， $\{R^*; \cdot\}$ 是有限半群，
另外，由命题 2.1 可知，在 $\{R^*; \cdot\}$ 中消去律成立，
因而，根据第二章定理 1.1 可知， $\{R^*; \cdot\}$ 是群，进而 R 是域，

定义 2.5 设 S 是环 R 的非空子集，
若 S 在 R 的运算下构成域，则称 S 是 R 的子域，
若环 R 也是域，则称 R 是 S 的扩域

定理 2.1 域 F 的至少含有两个元素的子集合 S 是 F 的子域的充分必要条件是以下两个条件成立:

(1)对属于 S 的任意 a, b , 有 $a-b$ 属于 S ;

(2)对属于 S 的任意 $a, b, b \neq 0$, 有 ab^{-1} 属于 S ,

证: 必要性是显然的,

下面证充分性,

由(1)知 $\{S; +\}$ 是群, 由(2)知 $\{S-\{0\}; \cdot\}$ 是群,

因为 F 是域, F 的加法运算、乘法运算都具有交换律,

且乘法对加法运算具有分配律,

所以在 F 的子集合 S 上这些运算规律也同样成立, 因此, S 是域,

例 2.5 试证明当且仅当 n 是素数时, $\{Z_n; +, \cdot\}$ 是域

证: 若 $\{Z_n; +, \cdot\}$ 是域, 则 $\{Z_n; +, \cdot\}$ 是整环, 从而, n 是素数,

反之, 若 n 是素数, 则 $\{Z_n; +, \cdot\}$ 是有限整环, 从而是域

例 2.6 证明 $Q[i] = \{a+bi | a, b \in Q\}$ (i 是虚数单位) 是域

证: 因为 $Q[i]$ 是复数域的子集合, 所以我们仅需要指出 $Q[i]$ 是复数域的子域,

对属于 $Q[i]$ 的任意 $a+bi, c+di$, 总有 $(a+bi)-(c+di)=(a-c)+(b-d)i \in Q[i]$,

当 $c+di \neq 0$ 时, $(a+bi)(c+di)^{-1} = (a+bi) \frac{c-di}{c^2+d^2} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} \in Q[i]$

于是, 根据定理 2.1 可知 $Q[i]$ 是复数域的子域, 从而 $Q[i]$ 是域,

例 2.7 若有限域 F 的阶为 n ($|F|=n$), 则对属于 F 的任意的 a , 有 $a^n=a$,

证: 由于 $F-\{0\}$ 是 $n-1$ 阶乘法群, 因此对不等于 0 的任意的 a , 有 $a^{n-1}=1$,

从而 $a^n=a$, 自然, 当 $a=0$ 时, 也有 $a^n=a$,

三、除环

定义 2.6 设 R 是非零的、有 1 的环，

若 R 的每个非零元都可逆，则称 R 是除环(或体)，

显然，交换的除环是域，域是除环，

注意，在除环的定义中，并没有要求交换性，那么非交换的除环是否存在呢？

下面的例子就是一个除环，但它不是域，

例 2.8 设 $H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$ ($\bar{\alpha}$ 表示 α 的共轭)，试证明 H 是除环但不是域，

证：首先，对属于 $\mathbb{C}$ 的任意 $\alpha_1, \alpha_2, \beta_1, \beta_2$ ，有

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta}_1 & \bar{\alpha}_1 \end{pmatrix} - \begin{pmatrix} \alpha_2 & \beta_2 \\ -\bar{\beta}_2 & \bar{\alpha}_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 - \alpha_2 & \beta_1 - \beta_2 \\ \bar{\beta}_2 - \bar{\beta}_1 & \bar{\alpha}_1 - \bar{\alpha}_2 \end{pmatrix} \in H$$

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta}_1 & \bar{\alpha}_1 \end{pmatrix} \begin{pmatrix} \alpha_2 & \beta_2 \\ -\bar{\beta}_2 & \bar{\alpha}_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \alpha_2 - \beta_1 \bar{\beta}_2 & \alpha_1 \beta_2 + \beta_1 \bar{\alpha}_2 \\ \alpha_1 \bar{\beta}_2 - \bar{\beta}_1 \alpha_2 & \alpha_1 \bar{\alpha}_2 - \beta_1 \bar{\beta}_2 \end{pmatrix} \in H$$

所以 H 是 $M_2(\mathbb{C})$ 的子环，

其次， H 有单位元 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ，并且当 $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \neq 0$ 时，

有 $\det \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = \alpha \bar{\alpha} + \beta \bar{\beta} \neq 0$ ，即 $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ 是可逆矩阵，

而且其逆为 $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}^{-1} = \frac{1}{\alpha \bar{\alpha} + \beta \bar{\beta}} \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix} \in H$

即 H 的每个非零元都可逆，因此 H 是除环，

最后，因 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ 与 $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ 不相等，

即 H 的乘法运算不具有交换律，

综上， H 确是除环，但它不是域，

实际上，这个除环就是哈密顿四元数体，

下面我们说明这个除环 H 为何被称为四元数体，

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

因此，若令 $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

则当 $\alpha = a+bi$, $\beta = c+di$ 时，就有 $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = ae+bi+cj+dk$ ，这里 a, b, c, d 属于 R

这就是说， H 的结构是由四个元素 e, i, j, k 及实数所确定的，

$$H = \{ae+bi+cj+dk \mid a, b, c, d \in R\},$$