

在介绍环的定义之前，我们有必要回顾一下交换群的概念和简单性质，运算满足交换律的群称为交换群，交换群的运算称为加法运算，并用加号表示交换群的单位元称为零元，用 0 表示，每个元素 a 的逆元称为负元，用 $-a$ 表示在交换群中，我们可以定义减法运算: $a-b=a+(-b)$ ，它是加法的逆运算，若规定 $0a=0$ (第一个 0 是数零，第二个 0 是零元)，并对正整数 n 规定

$$na = \underbrace{a+a+\cdots+a}_{n \text{ 个 } a}, \quad -na = \underbrace{(-a)+(-a)+\cdots+(-a)}_{n \text{ 个 } (-a)}$$

则对任意整数 m, n 以及群中的元素 a, b ，我们有下列运算性质：

- (1) $m(a+b)=ma+mb$;
- (2) $(m+n)a=ma+na$;
- (3) $m(na)=(mn)a=n(ma)$,

定义 1.1 如果代数系统 $\{R; +, \cdot\}$ 满足以下条件:

- (1) $\{R; +\}$ 是交换群;
 - (2) $\{R; \cdot\}$ 是半群;
 - (3) 运算“ $\cdot$ ”对“ $+$ ”满足分配律，即 $a \cdot (b+c)=a \cdot b+a \cdot c$, $(b+c) \cdot a=b \cdot a+c \cdot a$,
- 则称代数系统 $\{R; +, \cdot\}$ 是环，简称 R 是环，

今后，我们称环 $\{R; +, \cdot\}$ 中的运算“+”为加法运算，“ $\cdot$ ”为乘法运算，
并将加法群 $\{R; +\}$ 的单位元素称为 R 的零元，用 0 表示，
将 a 关于加法运算的逆元称为 a 的负元，用 $-a$ 表示，
特别地，如果环 R 的乘法运算还满足交换律，即 $a \cdot b = b \cdot a$ ，
其中任意 a, b 属于 R ，那么称 R 为交换环，否则，称 R 是非交换环，
如果环 R 中存在元素 e ，使得对属于 R 的任意 a ，有 $e \cdot a = a \cdot e = a$ ，
则称 e 是 R 的单位元，并称环 R 是有单位元的环，
若 R 是有单位元的环，则易知 R 的单位元是唯一的，
我们也时常常用 1 表示环 R 中的单位元，并将有单位元的环称为有 1 的环，
设 R 是有 1 的环，对属于 R 的任意 a ，若存在属于 R 的 b ，使得 $b \cdot a = a \cdot b = 1$ ，
则称 a 是可逆元， b 是 a 的逆元，若 a 是可逆元，则 a 的逆元是唯一的
事实上，若 b, c 均为 a 的逆元，则 $b = b \cdot 1 = b \cdot (a \cdot c) = (b \cdot a) \cdot c = 1 \cdot c = c$
一般地，我们用 a^{-1} 表示 a 的逆元，

环的运算性质，除了在本节开始介绍的三个关于加法运算的性质，
还有下列关于乘法运算的性质，

命题 1.1 设 $\{R; +, \cdot\}$ 是环，则对属于 R 的任意 a, b ，和属于 Z 的 n ，有

(1) $0 \cdot a = 0 = a \cdot 0$;

(2) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$;

(3) $(na) \cdot b = n(a \cdot b) = a \cdot (nb)$;

(4) 若环 R 是有 1 的环，则 $(-1) \cdot a = -a$ ，

证: (1) 由零元的定义及分配律可知， $0 + 0 \cdot a = 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$ ，

再根据加法群的消去律，得到 $0 = 0 \cdot a$ ，类似地，可证 $0 = a \cdot 0$

(2) 由分配律和性质(1)可知， $(-a) \cdot b + (a \cdot b) = (-a + a) \cdot b = 0 \cdot b = 0$ ，

即 $(-a) \cdot b = -(a \cdot b)$ ，类似地，可证 $-(a \cdot b) = a \cdot (-b)$ ，

(3) 当 n 是非负整数时，易知 $(na) \cdot b = n(a \cdot b) = a \cdot (nb)$ ，

若 n 是负整数，则由分配律和(2)得

$$(na) \cdot b = ((-n)(-1)a) \cdot b = ((-n)(-a)) \cdot b = (-n)(-ab) = (-n)(-(a \cdot b)) = n(a \cdot b),$$

类似地，可证 $a \cdot (nb) = n(a \cdot b)$ ，

(4) 由单位元的定义及分配律有 $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a$ ，

再由 $0 \cdot a = 0$ 得证，

下面给出具有环结构的一些代数系统的例子

例 1.1 整数集关于数的加法和乘法运算 $(\mathbb{Z}; +, \cdot)$ 是有单位元的交换环，称为整数环，

整数环 $\{\mathbb{Z}; +, \cdot\}$ 中的零元是数 0，单位元是数 1， n 的负元是 $-n$ ，可逆元是 ± 1 ，

有理数集 $\mathbb{Q}$ 、实数集 $\mathbb{R}$ 及复数集 $\mathbb{C}$ 关于数的加法和乘法运算也都是交换环，分别称为有理数域、实数域和复数域，

数域 F 上 n 阶方阵集合 $M_n(F)$ 关于矩阵的加法和乘法运算

构成有单位元的非交换环，称为数域 F 上的矩阵环，

矩阵环 $\{M_n(F); +, \cdot\}$ 中的零元是 n 阶零矩阵，单位元是 n 阶单位矩阵，

$M_n(F)$ 中元素 A 的负元是 $-A$ ，而 $M_n(F)$ 中的可逆元是可逆矩阵，

数域 F 上一元多项式集合 $F[x]$ 关于多项式的加法和乘法运算

构成有单位元的交换环，称为数域 F 上的一元多项式环，

$F[x]$ 中的零元是数 0，单位元是数 1，

$F[x]$ 中多项式 $f(x)$ 的负元是 $-f(x)$ ， $F[x]$ 中的可逆元是零次多项式，

$\{\mathbb{Z}_n; +, \cdot\}$ 是有单位元的交换环，称为模 n 的剩余类环，

$\mathbb{Z}_n$ 中的零元是 0，单位元是 1，元素 a 的负元是 $\overline{n-a}$ ，

$\mathbb{Z}_n$ 中的元素 a 是可逆元的充分必要条件是 a 与 n 互素，

例 1.2 证明 $\mathbb{Z}[i] = \{a+bi \mid a, b \text{ 都属于 } \mathbb{Z}\}$ 是有单位元的交换环(高斯整环)，

其中 i 是虚数单位

证: 对属于 $\mathbb{Z}$ 的任意 a_1, a_2, b_1, b_2 ，

有 $(a_1+b_1i)+(a_2+b_2i)=(a_1+a_2)+(b_1+b_2)i$ 属于 $\mathbb{Z}[i]$ ，

$(a_1+b_1i)(a_2+b_2i)=(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i$ 属于 $\mathbb{Z}[i]$ ，

即复数域的加法运算和乘法运算也是 $\mathbb{Z}[i]$ 的加法和乘法运算，

又因 $\mathbb{Z}[i]$ 是复数域的子集，

所以在 $\mathbb{Z}[i]$ 上的加法运算和乘法运算都满足结合律和交换律，

且乘法运算对加法运算满足分配律，

易知， $\mathbb{Z}[i]$ 的零元是数 0，单位元是数 1，元素 $a+bi$ 的负元是 $-a-bi$ ，

因此根据环的定义可知， $\mathbb{Z}[i]$ 是有单位元的交换环

例 1.3 求高斯整环 $Z[i]$ 的可逆元，

解: 若令属于 $Z[i]$ 的 $\alpha=a+bi$ ，并且我们用 $N(\alpha)$ 表示 α 的范数，即 $N(\alpha)=a^2+b^2$ ，

则对任意属于 $Z[i]$ 的 α, β ，有 $N(\alpha\beta)=N(\alpha)N(\beta)$ ，

若 $\alpha=a+bi$ 是 $Z[i]$ 的可逆元，

则存在属于 $Z[i]$ 的 β ，使得 $\alpha\beta=1$ ，故 $1=N(\alpha\beta)=N(\alpha)N(\beta)$ ，

所以 $N(\alpha)=1$ ， $\alpha=\pm 1, \pm i$ ，因此， $Z[i]$ 的可逆元有 $\pm 1, \pm i$ ，

命题 1.2 设 R 是有 1 的环，若 $U(R)$ 表示 R 中所有可逆元构成的集合，

则 $U(R)$ 关于 R 的乘法运算构成群，我们称其为环 R 的单位群，

证: 显然，1 属于 $U(R)$ ，即 $U(R)$ 是非空集合，

又因可逆元的乘积还是可逆元 $((ab)^{-1}=b^{-1}a^{-1})$ ，

所以 R 的乘法运算也是 $U(R)$ 的乘法运算，

而环 R 的乘法运算满足结合律，

故在 R 的子集合 $U(R)$ 上的乘法运算也满足结合律，

再若 a 属于 $U(R)$ ，则 a^{-1} 属于 $U(R)$ ，所以 $U(R)$ 关于 R 的乘法运算构成群，

易知， $U(Z)=\{\pm 1\}$ ，

$U(Q)=Q-\{0\}$ ，

$U(M_n(R))=GL_n(R)$ ，

$U(Z_3)=\{\bar{1}, \bar{2}\}$ ，

$U(Z_4)=\{\bar{1}, \bar{3}\}$ ，

$U(Z[i])=\{1, -1, i, -i\}$ ，

定义 1.2 设 $\{R; +, \cdot\}$ 是一个环， S 是 R 的非空子集，

若 S 关于 R 的加法运算和乘法运算也构成一个环，

则称 $\{S; +, \cdot\}$ 是 $\{R; +, \cdot\}$ 的子环，简称 S 是 R 的子环，也称 R 是 S 的扩环，

显然， $\{0\}$ 和 R 都是 R 的子环，称为平凡子环，

注意，在环 $\{0\}$ 中的零元和单位元相等，称 $\{0\}$ 为零环，其他环称为非零环，

定理 1.1 设 S 是环 R 的非空子集，则 S 是 R 的子环的充分必要条件是，
 对属于 S 的任意 a, b ，有 $a-b$ 属于 S ， ab 属于 S ，
证： 必要性是显然的，下面证明充分性，
 由 $a-b$ 属于 S 可知， S 关于环 R 的加法运算是群，
 又由 ab 属于 S 可知，环 R 的乘法运算也是 S 的乘法运算，并且满足结合律，
 再由 S 是环 R 的非空子集可知， R 的分配律在 S 上也成立，
 因此， S 是 R 的子环，

例 1.4 因为子环关于环的加法运算是子群，
 因此，我们可以通过环的加法子群找其所有子环，
 我们已经知道 $\{Z; +\}$ 的所有子群为 $\{\langle n \rangle | n \text{ 是非负整数}\}$ ，其中 $\langle n \rangle = \{rn | r \in Z\}$ ，
 对于每个子群 $\langle n \rangle$ ，根据定理 1.1 可知， $\langle n \rangle$ 是整数环 Z 的子环，
 因此， Z 的所有子环为 $\{\langle n \rangle | n \text{ 是非负整数}\}$ ，
 特别地，当 n 不等于 1 时，子环 $\langle n \rangle$ 是没有单位元的交换环，

例 1.5 我们已经知道剩余类加法群 Z_n 的全部子群为 $\{\langle s\bar{1} \rangle = \langle \bar{s} \rangle | s \text{ 是 } n \text{ 的正因数}\}$
 而对于每个子群 $\langle \bar{s} \rangle = \{r\bar{s} | r \in Z\}$ ，根据定理 1.1 可知， $\langle \bar{s} \rangle$ 是剩余类环 Z_n 的子环
 因此， Z_n 的所有子环为 $\{\langle s\bar{1} \rangle | s \text{ 是 } n \text{ 的正因数}\}$ ，

例 1.6 设 R 是环，试证明 $C(R) = \{a \in R | ab = ba, \forall b \in R\}$ 是 R 的子环，
 称其为环 R 的中心，

证： 显然 0 属于 $C(R)$ ，即 $C(R)$ 是 R 的非空子集，
 又因对属于 $C(R)$ 的任意 a, b ，和属于 R 的任意 c ，有

$$(a-b)c = ac - bc = ca - cb = c(a-b),$$

$$(ab)c = a(bc) = a(cb) = (ac)b = (ca)b = c(ab),$$
 即 $a-b$ 属于 $C(R)$ ， ab 属于 $C(R)$ ，
 所以，根据定理 1.1 可知， $C(R)$ 是环 R 的子环，