10.4 环和域

前面的内容如半群，群，他们都是具有一个运算的代数系统。这对于研究简单的整数和实数系统来说都是不够的。因此，我们必须研究具有两个运算的代数系统——环和域。

① 环

定义 1： 设<**R**, +, •>是代数系统, +和•是二元运算。如果满足以下条件：

(1) < **R**, +>构成交换群。

(2) < **R**, •>构成半群。

(3) •运算关于+运算适合分配律。

则称< $\mathbb{R}$, +, •>是一个环。

- 通常称+运算为环中的加法，•运算为环中的乘法。

环的实例：

(1) 整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为整数环$\mathbb{Z}$，有理数环$\mathbb{Q}$，实数环$\mathbb{R}$和复数环$\mathbb{C}$。

(2) n (n≥2) 阶实矩阵的集合$M_n(\mathbb{R})$关于矩阵的加法和乘法构成环，称为 n 阶实矩阵环。

(3) 设 $\mathbf{Z}_n$＝$\{0,1,2,\ldots,n-1\}$，⊕和⊗分别表示模 n 的加法和乘法，即

$$x \oplus y = (x+y) \bmod n, x \otimes y = (x\, y) \bmod n$$

则<$\mathbf{Z}_n$，⊕，⊗>构成环, 称为模 n 的整数环。

环的运算约定:

- 加法的单位元记作 0。
- 乘法的单位元记作 1(对于某些环中的乘法不存在单位元)。
- 对任何环中的元素 x，称 x 的加法逆元为负元，记作$-x$。
- 若 x 存在乘法逆元的话，则将它称为逆元，记作x^{-1}。
- 针对环中的加法,
  - $x-y$表示$x+(-y)$。
  - nx 表示 $x+x+\cdots+x$ (n 个 x 相加)，即 x 的 n 次加法幂。
  - $-xy$表示 xy 的负元。

注 1: 运算的顺序是先计算乘法，再计算加法。

定理 1: 设<$\mathbf{R}$, +, ·>是环，则

(1) $\forall a\in\mathbf{R}$，$a0=0a=0$。

(2) $\forall a, b\in\mathbf{R}$，$(-a)b=a(-b)=-ab$。

(3) $\forall a, b\in\mathbf{R}$，$(-a)(-b)=ab$。

(4) $\forall a, b, c\in\mathbf{R}$，$a(b-c)=ab-ac$，$(b-c)a=ba-ca$。

(5) 如果乘法的单位元存在，则$(-1)a=-a$。

(6) 如果乘法的单位元存在，则$(-1)(-1)=1$。

常常又因为环中的乘法半群满足于不同的乘法的各种性质，将环冠于

不同的名称。

定义 2： 设$\langle \mathbf{R}, +, \cdot \rangle$是环。

(1) 若环中乘法$\cdot$适合交换律，则称$\mathbf{R}$是交换环。

(2) 若环中乘法$\cdot$存在单位元，则称$\mathbf{R}$是含幺环。

(3) $\forall a, b \in \mathbf{R}$，若 $ab=0$，则必有 $a=0$ 或 $b=0$，则称$\mathbf{R}$是无零因子环。

(4) 若 $\mathbf{R}$ 即是交换环，含幺环，也是无零因子环，则称 $\mathbf{R}$ 是整环。

(5) 设 $\mathbf{R}$ 是整环，且其中至少含有两个元素。若$\forall a \in \mathbf{R}^* = \mathbf{R} - \{0\}$，都有$a^{-1} \in \mathbf{R}$，则称 $\mathbf{R}$ 是域。

例如：

(1) 全体整数，有理数，实数和复数按普通加法和普通乘法构成无零因子的环，所以是整环。除了整数环以外，都是域。

(2) 令 $2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$，则 $2\mathbb{Z}$关于普通的加法和乘法构成交换环和无零因子环。但不是含幺环和整环，因为 $1 \notin 2\mathbb{Z}$。

(3) 设 n 是大于或等于 2 的正整数，则 n 阶实矩阵的集合$M_n(\mathbb{R})$关于矩阵加法和乘法构成环，它是含幺环，但不是交换环和无零因子环，也不是整环。

(4) $\mathbf{Z}_6$ 关于模 6 加法和乘法构成环，它是交换环、含幺环，但不是无零因子环和整环。

注 2： 有限整环必为域。

例 1： 设 $S=\{e, a, b, c\}$, $<S, *>$ 构成 Klein 四元群。

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

如果再定义 S 上的二元运算 • 如下，

•	e	a	b	c
e	e	e	e	e
a	e	a	e	a
b	e	b	e	b
c	e	c	e	c

则$<S, *, \bullet>$是个环。

例 2： 设 R 是环，R 是无零因子环当且仅当 R 中的乘法适合消去律，即$\forall a, b, c \in R$，$a \neq 0$，有

$$ab=ac \Rightarrow b=c \quad 和 \quad ba=ca \Rightarrow b=c。$$

例 3：判断下述集合关于给定的运算是否构成环、整环和域。如果不能构成，请说明理由。

(1) $A=\{a+b\sqrt{2}\mid a, b\in\mathbb{Z}\}$，关于数的加法和乘法。

(2) $A=\{a+b\sqrt[3]{2}\mid a, b\in\mathbb{Z}\}$，关于数的加法和乘法。

(3) $A=\{a+b\mathrm{i}\mid a, b\in\mathbb{Z}\wedge \mathrm{i}^2=-1\}$，关于复数的加法和乘法。

(4) $A=\{\begin{pmatrix} a & b \\ b & a \end{pmatrix}\mid a, b\in\mathbb{Z}\}$，关于矩阵的加法和乘法。