

第3章 环和域

环和域是具有两个二元代数运算的代数系。

基本内容：

- 1) 环和域的定义及其基本性质
- 2) 无零因子环的特征数
- 3) 环的同态



§ 3.1 基本定义及简单性质

定义1 环： 设 S 为非空集合， S 中有两个二元代数运算，分别称为加法“ $+$ ”与乘法“ \cdot ”，且满足：

- 1) $(S, +)$ 是一个Abel群；
- 2) (S, \cdot) 是一个半群；
- 3) 乘法对加法满足左右分配律

即对 $\forall a, b, c \in S$ 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 $(S, +, \circ)$ 为环。



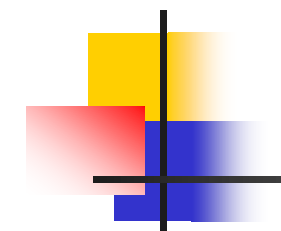
注：

加法的单位元用“0”表示，称为S的零元素；

加法的逆元素记为 $-a$ ，称为a的负元（素）；

加法的逆运算称为减法，用“ $-$ ”表示，其定义为：对 $\forall a, b \in S$ 有：

$$a - b = a + (-b);$$



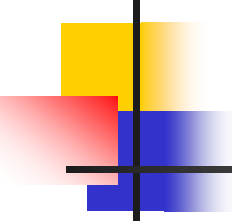
a 对加法的 m 次幂记为 ma ,

当 $m > 0$ 时, ma 定义为 m 个 a 相加, 即:

$$1a = a, \quad (m+1)a = ma + a;$$

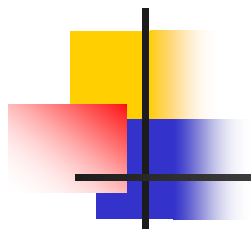
当 $m < 0$ 时, ma 定义为 $(-m)$ 个 $(-a)$

当 $m = 0$ 时, $0a = 0$, 其中左边的 0 是数零, 右边的 0 是 S 的零元素。



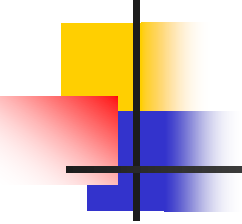
定义2 交换环：环 $(S, +, \cdot)$ 关于乘法满足交换律，即对 $\forall a, b \in S$ ，有

$$a \cdot b = b \cdot a$$



例1 $(\mathbb{R}, +, *)$ 、 $(\mathbb{Z}, +, *)$ 、 $(\mathbb{Q}, +, *)$
对通常的加法和乘法均构成交换环。

例2 设 M_n 为一切 $n \times n$ 实矩阵之集，则
 $(M_n, +, \cdot)$ 对矩阵的加法和乘法构成一个非交换环，称为 n 阶矩阵环。



定义3 有限环：环 $(S, +, \cdot)$
称为有限环，若 R 是有限
非空的集合。

例3 同余类环: (Z_n, \oplus, \bullet)

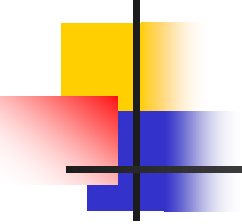
$$\forall [i], [j] \in Z_n, [i] \oplus [j] = [i + j]$$

$$[i] \bullet [j] = [i * j]$$

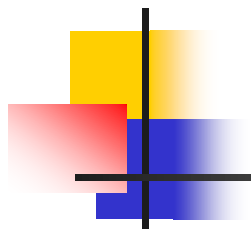
显然 Z_n 关于“ \oplus ”为Abel群，其中单位元为 $[0]$ ；

Z_n 关于“ \bullet ”为交换半群。

注：对任何自然数 n 必有恰好含有 n 个元素的交换环。



定义4 零环： $(S, +, \cdot)$ 称为零环，其中 $S = \{0\}$ ，“+”与“ \cdot ”为通常的加法和乘法。



环的简单性质： 首先由于环关于加法为Abel群，故有Abel群的一切性质。
设 $\forall a, b, c \in S, m, n \in \mathbb{Z}$ 则有：

1) $0+a=a+0=a$

2) $a+b=b+a$

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

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

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

$$6) a+c=b \iff a=b-c$$

$$7) -(-a)=a$$

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

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

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

$$11) m(a+b)=ma+mb$$

$$12) n(a-b)=na-nb$$

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

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

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

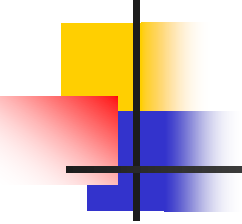
$$15) \forall a \in S, 0 \circ a = a \circ 0 = 0$$

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

$$a \circ (-b) = -(a \circ b)$$

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

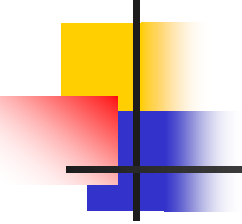
$$18) a(b - c) = ab - ac$$



19)

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

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



21) 若 $ab=ba$ ，则二项式定理成立，
即当 $n>0$ 时有：

$$(a+b)^n = \sum_{i=0}^n C_n^i a^i b^{n-i}$$

定义5 设 $(S, +, \cdot)$ 为环,

若 $\exists b \in S, b \neq 0$ 使 $ab = 0, a \in S$,
则称 a 为 S 的一个左零因子。

右零因子: 若 $\exists c \in S, c \neq 0$
使 $ca = 0, a \in S$, 则称 a 为 S 的
一个右零因子。

零因子: a 同时为 S 的左右零因子。

- 注：** 1) 显然 S 的零元素为零因子；
- 2) 若无特殊声明，上述定义均为非零的；
- 3) 由2) 知，若 a 为 S 的左零因子，则 $a \neq 0$ ，从而 S 必有右零因子（ $\because \exists b \in S, b \neq 0$ 使得 $ab=0$ ）
- 如在模6同余类中：
- $$[2] \bullet [3] = [6] = [0]$$
- 4) 若 b 为 S 的零因子，则必为左右零因子；

例4 在例2中令 $M_n = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a, b \in R \right\}$

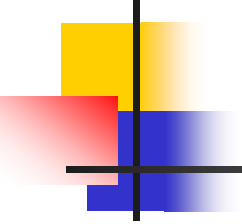
$$\begin{pmatrix} 1 & 0 \\ d & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

由此可见左零因子不一定为右零因子。

另在例2中：

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

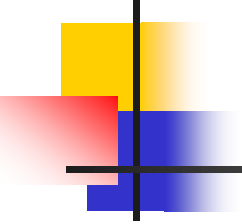
$$\begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$



定义6 无零因子环：无非零的左零因子，也没有非零的右零因子的环。

即对 $\forall a, b \in S$ 若 $ab=0$ ，
则必有 $a=0$ 或 $b=0$ 。

整环：可换无零因子环。



定理1 环 S 是无零因子环的充要条件是在 S 中乘法满足消去律，即：

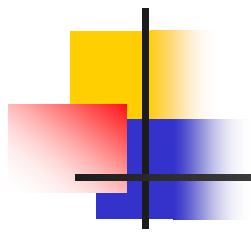
若 $a \neq 0$, $ab = ac$, 则 $b=c$

若 $a \neq 0$, $ba = ca$, 则 $b=c$



定义7 体：若环 S 满足：

- 1) 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。



- 注： 1) 体 $(F, +, \cdot)$ 中两部分
群：加法群 $(F, +)$ 与
乘法群 $(F \setminus \{0\}, \cdot)$
2) 群中无零元素。



定义8 域：可换体称为域。

注：体和域中没有零因子
(因为关于乘法满足消去律)

例：有理数环、实数环均为体，
同时也为域。

代数系

加法运算

乘法运算

域



体



环

Abel 群



继承

Abel 群



继承

Abel 群

Abel 群



升级

群



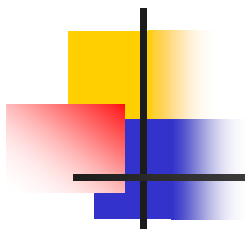
升级

半群



定义9 仅有有限个元素的体（域）
称为有限体（域）。

定理2 至少有一个非零元素的无零
因子有限环是体



例 设 p 是一个素数，则模 p 同余类环 $(\mathbb{Z}_p, \oplus, \bullet)$ 是一个有限域。

注：域 $(F, +, \circ)$ 中引入除法的概念：

1) $\frac{b}{a}$: 表示 b 被 a 除的商,

且 $\frac{b}{a} = a^{-1}b(ba^{-1})$

其中 $a \neq 0$

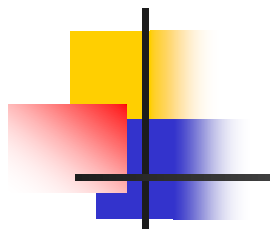
$$2) \quad \forall a, b, c, d \in F, b \neq 0, d \neq 0$$

$$\text{则: } ad = bc \Leftrightarrow \frac{a}{b} = \frac{c}{d}$$

$$\frac{a}{b} \circ \frac{c}{d} = \frac{ac}{bd}, \quad \frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$$

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$$

其中 $c \neq 0$



定义10 子环：环 $(S, +, \cdot)$ 的非空子集 T 若对其中的加法和乘法也形成环，则称 T 为 S 的子环。

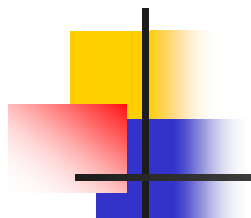
定义11 子体（域）：设 $(F, +, \cdot)$ 为体（域），若 F 的非空子集 E 对 F 的加法和乘法也构成一个体（域），则称 E 为 F 的一个子体（域）。



定理3 环 S 的非空子集 T 是 S 的子环的充要条件是：

1) $\forall a, b \in T$, 有 $ab \in T$

2) $\forall a, b \in T$, 有 $a - b \in T$



体F的非空子集E是F的一个子体的充要条件是以下三个条件同时成立：

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