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“。”，且满足：

1）（S，＋）是一个Abel群；

2）（S，。）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，＋，。）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，（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，＋，。）关于乘法满足交换律，即对 $\forall a, b \in S$ ，有

a 。b＝b 。a

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

例2 设Mn为一切n×n实矩阵之集，则（Mn，＋，.）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，＋，。）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Zn关于“$\oplus$”为Abel群，其中单位元为[0]；

Zn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，＋，。）称为零环，其中S＝{0},“＋”与“ 。”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$\forall a, b, c \in S, m, n \in Z$ 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) $a+c=b \Longleftrightarrow a=b-c$

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，+，。）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，＋，。）中两部分群：加法群（F，＋）与

乘法群（F\{0}，。）

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	*Abel*群	*Abel*群
↑	↑ 继承	↑ 升级
体	*Abel*群	群
↑	↑ 继承	↑ 升级
环	*Abel*群	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 $\left(Z_p, \oplus, \bullet\right)$ 是一个有限域。

注： 域 $(F,+,\circ)$ 中引入除法的概念：

1）$\dfrac{b}{a}$：表示b被a除的商，

且 $\dfrac{b}{a}=a^{-1}b(ba^{-1})$

其中 $a\neq 0$

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

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

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

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

其中 $c \neq 0$

定义10 子环：环（S，＋，。）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，＋，。）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) $|E| \geqslant 2$

2) $\forall a, b \in E, a-b \in E$

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