第九章 环与域

- 9.1 环：两个二元运算的代数结构
- 1. 环的概念
- 定义9.1：<R, +, ·>是代数系统，+， ·是二元运算，若满足：

(1):<R，+>是阿贝尔群；(2):<R，·>是半群；

(3):·对+可分配；则称<R, +, ·>为环(Ring)，+称为加法，·称为乘法(未必是数加和数乘)；同时加法幺元记为0，加法逆元-x，n次幂为nx，若存在的话，乘法幺元记为1，逆元为 x^{-1} n次幂为 x^{n}

9.1 环

- **例9-1：（1）:<Z, +, ·>, <Q, +, ·>, <R, +, ·>, <C, +, ·>均为环；（2）:实数分量的n×n方阵集合** $M_n(R)$ **，构成环：** $<M_n(R),+,\bullet>$ **；（3）:** $<P(A),\oplus,\cap>$

$(4): <Z_k,+_k,\times_k>$ 为环。

证：$<Z_k,+_k>$ 为加群，$<Z_k,\times_k>$ 为半群；

$\forall a,b\in Z_k$，有 $a+_k b=(a+b)\bmod k,\ a\times_k b=(a\times b)\bmod k$

$\therefore a\times_k(b+_k c)=a\times_k((b+c)\bmod k)=(a\bullet(b+c)\bmod k)\bmod k$

$=(a\bullet(b+c))\bmod k=(a\bullet b+a\bullet c)\bmod k$

$=(a\bullet b)\bmod k+_k(a\bullet c)\bmod k=a\times_k b+_k a\times_k c$

同理:$(b+_k c)\times_k a=b\times_k a+_k c\times_k a$ $\quad\therefore$ 为环。

（5）:<{0}, +, ·>(0为加法幺元，乘法零元)为环，称为零环；（6）:<{0, 1}, +, ·>(1为乘法幺元)为环

9.1 环

- **2. 环的性质**
- **定理9.1：** 设<R, +, ·>是环，则对任意的a, b, c有：

(1)：加法幺元必为乘法零元；(2)：(−a)·b=a·(−b)=−(a·b)；(3)：a·(b−c)=a·b−a·c，(b−c)·a=b·a−c·a；(4)：$\forall a_i, b_j \in R, \sum a_i \bullet \sum b_j = \sum a_i \bullet b_j$

证:$(1) a \bullet 0 = a \bullet (0+0) = a \bullet 0 + a \bullet 0, < R,+ >$ 是阿贝尔群,

$\therefore$ 满足消去律, $\therefore a \bullet 0 = 0$, 同理 $0 \bullet a = 0$;

$(2) (-a) \bullet b + a \bullet b = (-a+a) \bullet b = 0 \bullet b = 0, < R,+ >$ 是阿贝尔群,

$\therefore$ 逆元唯一, $\therefore (-a) \bullet b = -a \bullet b$;

$(3) a \bullet (b-c) = a \bullet (b+(-c)) = a \bullet b + a \bullet (-c) = a \bullet b + (-a \bullet c)$

$= a \bullet b - a \bullet c$, 同理 $(b-c) \bullet a = b \bullet a - c \bullet a$

(4)略(书上)

9.1 环

- <R, +, ·>中·不一定满足交换律，也不一定有幺元，但一定有零元。

- **3. 子环与环同态**
- 定义9.2：子环：环<R, +, ·>，若 $S\subseteq R, <S,+,\bullet>$ 构成环，则为R的子环。

子环判定： $\begin{cases} +:\text{阿贝尔群} \\ \bullet:\text{半群} \\ \text{分配律} \end{cases} \Rightarrow \begin{cases} +:\text{群} \\ \bullet:\text{封闭} \end{cases} \Rightarrow \begin{cases} +:\text{子群判定定理} \\ \bullet:\text{封闭} \end{cases}$

- 定义9.3：环同态：

$$R_1 \to R_2 : \begin{cases} + \quad \varphi(x+y)=\varphi(x)+\varphi(y) \\ \bullet \quad \varphi(x\bullet y)=\varphi(x)\bullet\varphi(y) \end{cases}$$

9.2 整环和域

- **定义9.4：** 设<R, +, ·>是环：

(1). 若·满足交换律，则称R是交换环；

(2). 若·运算含有幺元，则称R是含幺环；

(3). 若有非零元素a, b满足a·b=0，则称a, b为R的零因子(a为左零因子，b为右零因子)，此时称R为含零因子环，否则称R为无零因子环；

(4). 若R是交换环，含幺环，也是无零因子环，则称R是整环。

- **例9-2：** (1):Z, Q, R, C都是交换环，含幺环，无零因子环，整环；

9.2 整环和域

(2)：$<Z_8,+_8,\times_8>$中，[0]是零元，[2],[4]是零因子，$([2]\times_8[4]=[0])$

$<M_2(R),+,\bullet>$中有零因子：$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$和$\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$

- **定理9. 2：设R是环，则R中无零因子当且仅当R中乘法运算满足消去律，即：**$\forall a,b,c\in R, a\neq 0$ **有：**

$ab=ac\Rightarrow b=c, ba=ca\Rightarrow b=c$($R$中非零元可约)

证：$(\Leftarrow)$任取$a,b\in R$，$a\neq 0$，若$ab=0=a0$，则$b=0$，$\therefore R$无零因子

$(\Rightarrow)$任取$a,b,c\in R$，且$a\neq 0$，$ab=ac$，则$ab-ac=0$，

即$a(b-c)=0$，由于R无零因子，$a\neq 0,\therefore b-c=0$，即$b=c$

$$整环：\begin{cases}+：封闭，可结合，含幺，逆元，可交换\\ \bullet：封闭，可结合，含幺，无零因子，可交换\\ \bullet对+可分配\end{cases}$$

9.2 整环和域

- 定义9.5：R是环，令 $R^* = R - \{0\}$ ，若 $< R^*, \bullet >$ 为阿贝尔群，则称<R,+,·>为域(field)。

由于 R^* 为群，满足消去律，无零因子，∴域必定是整环；域也可定义为：非零元素都有乘法逆元的整环。

- 例9-2：(1):<Q, +, ·>, <R,+, ·>, <C,+, ·>均为域， <Z,+, ·>不是域，无乘法逆元；

  $(2):< Z_7, +_7, \times_7 >$ 是域，2,4， 3,5互为逆元，1的逆元为1，6的逆元为6

  $< Z_8, +_8, \times_8 >$ 不是域，不是整环，有零因子，2,4无乘法逆元

9.2 整环和域

- **定理9.3：有限整环都是域。**

证：设$<R,+,\bullet>$是有限整环，$R=\{r_0,r_1,\cdots,r_n\}$，不妨设$r_0=0$，$r_1=1$，考虑$R-\{0\}=\{r_1,r_2,\cdots,r_n\}$，则只需证$\forall r_i\in R-\{0\}$有逆元，$\forall r_i\in\{r_1,r_2,\cdots,r_n\}$，则$\{r_i\bullet r_0,r_i\bullet r_1,\cdots,r_i\bullet r_n\}\subseteq R$，

由整环中的消去律，$l\neq k$时，$r_i\bullet r_k\neq r_i\bullet r_l$，即

$\{r_i\bullet r_0,r_i\bullet r_1,\cdots,r_i\bullet r_n\}$的元素互异，故$\{r_i\bullet r_0,r_i\bullet r_1,\cdots,r_i\bullet r_n\}=R$，

于是存在r_j，使得$r_i\bullet r_j=1$，即r_j是r_i的逆元。

- **定理9.4：**Z_p(指$<Z_p,+_p,\times_p>$) **为域的充要条件是p是素数。**

9.2 整环和域

证:(⇐) p是素数 $\Rightarrow Z_p$为有限整环 $\Rightarrow Z_p$为域,

易知 $<Z_p,+_p,\times_p>$ 为含幺1交换环,任取$i,j\in Z_p, i\neq 0$

若$[i]\times_p[j]=[0]$,则$p\mid i\times j$,而$i\neq 0$,即$p\nmid i$, $\therefore p\mid j$, $\therefore j=0$

即Z_p中无零因子,为整环,有限, $\therefore$为域;

(⇒)若p不是素数,则$p=a\times b$, $0<a<p$, $0<b<p$,则

$[a]\times_p[b]=[0]$, a,b为零因子,而Z_p为域$\Rightarrow Z_p$为整环,矛盾

$\therefore p$是素数。

- **定理9.5:** **设<F, +, ·>为域,则F中非零元素在<F, +>中有相同的阶。**

9.2 整环和域

证：当$<F,+>$中每个元素都是无限阶时，命题成立；

当$<F,+>$中有非零元素a具有有限阶n时，

则$<F,+>$中任一非零元素b的阶也是n。

$(nb)\bullet a = b\bullet(na) = 0$，而$F$无零因子，且$a \neq 0$，故$nb = 0$

$\therefore b$的阶不超过n，即$|b| \leq |a|$设b的阶为m，即$|b| = m$，

由$(ma)\bullet b = a\bullet(mb) = 0$可知，$ma = 0$，$\therefore a$的阶不超过$m$，

即$|a| \leq |b|$　$\therefore |b| = |a|$

- **定义9.6：设<F, +, ·>为域，<S, +, ·>为F的子环，且<S, +, ·>为域，则称S为F的子域。**

9.2 整环和域

- **定理9.6：设<F,+,·>为域，$F' \subseteq F$，且F'中至少有2个元素，那么$<F',+,\bullet>$为<F,+,·>的子域当且仅当F'满足：**

  (1).$\forall a,b \in F', a \neq b$，有$a-b \in F'$($<F',+>$为$<F,+>$的子群)

  (2).$\forall a,b \in F', a \neq b$，有$ab^{-1} \in F'$($<F'-\{0\},\bullet>$为$<F-\{0\},\bullet>$的子群)

例：<Q,+,·>是<R,+,·>和<C,+,·>的子域。