§5.环

- 环的基本概念
- 环的基本性质
- 无零因子环和含零因子环
- 整环与除环

§5.环

定义1.设〈R, ⊕, ⊗〉是代数系统， ⊕和⊗是R上的两个二元运算，若

(1) 〈R, ⊕〉是交换群；

(2) 〈R, ⊗〉是半群 ；

(3) ⊗对⊕满足分配律：对任何a,b,c∈R，都有

$$a\otimes(b\oplus c)=(a\otimes b)\oplus(a\otimes c)$$

$$(b\oplus c)\otimes a=(b\otimes a)\oplus(c\otimes a)$$ **；**

则称 〈R, ⊕, ⊗〉是环。

注：•环中，〈R, ⊕〉是群，故关于⊕有幺元存在，将关于⊕的幺元记为0，称为环的零元。

•环中，〈R, ⊕〉是群，故R中每个元素有逆元，设a∈R，将a关于⊕的逆元记为-a ，称为a 的负元，且将a ⊕(-b)简记为 a-b。

•环中，对于⊗运算，若有幺元，则记为1或e 。

•环中，设a∈R ，若a关于⊗有逆元，则记为 a^{-1}。

•以后谈到环，只讨论|R|≥2的情况，即不讨论一个元素的环。

•环的定义中，不要求⊕对⊗满足分配律，只要求 ⊗对⊕满足分配律。

例1.〈I,+,×〉是环。 称此环为整数环。I是整数集合，+和×是整数的普通加法运算和普通乘法运算。由前两节知：

(1)〈I,+〉 是交换群；

(2)〈I, ×〉是半群；

(3)×对+满足分配律：由算术知识知整数乘法对整数加法满足分配律。即 $\forall a,b,c \in I$ 有

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

由×的交换律知×对+满足分配律；

由环的定义知〈I,+, ×〉是环。

例2. 〈$M_{n\times n}$,+，×〉是环。 称此环为矩阵环。$M_{n\times n}$是全体n×n阶实矩阵，＋与×是矩阵的加法运算和乘法运算……

例3. 〈N_m,$+_m$,$\times_m$〉是环。

称此环为整数模环。$N_m=\{[0]_m,[1]_m,\ldots,[m-1]_m\}$，$+_m$和$\times_m$是$N_m$上的模加运算和模乘运算……

例4.〈2^X,⊕,∩〉是环。 称此环为X的子集环。X是一个非空集合， 2^X 是X的幂集，⊕是集合的对称差运算, ∩是集合的交运算……

例5. 〈P[x],+, ×〉是环。 称此环为多项式环。

这里：P[x] 是实系数多项式的全体，+和×是多项式的加法运算和乘法运算，由前两节知

(1)〈P[x],+〉是交换群；

(2)〈P[x],×〉是半群；

……

……

(3)×对+满足分配律：由于实数乘法对实数加法满足分配律，故多项式乘法对多项式加法满足分配律。

即$\forall h(x),p(x),q(x)\in P[x]$, 有

$h(x)\times(p(x)+q(x)) = (h(x)\times p(x))+(h(x)\times q(x))$

由×的交换律知×对+满足分配律；

由环的定义知〈$P[x],+,\times$〉是环。

例6. 〈$Z_m[x],+_m,\times_m$〉是环。 称此环为模数多项式环。

这里：$Z_m=\{0,1,2,\ldots,m-1\}$，$Z_m[x]$是系数在Z_m上的多项式的全体，$+_m$和$\times_m$是多项式的模加法运算和模乘法运算。

即$\forall p(x),q(x)\in Z_m[x]$, 有 $p(x)+_m q(x)=(p(x)+q(x)) \bmod m$

$p(x)\times_m q(x)=(p(x)\times q(x)) \bmod m$

(以上取模均是针对系数取模)

于是， 有 (1)〈$Z_m[x],+_m$〉是交换群；

①封闭性：$\forall p(x),q(x)\in Z_m[x]$, 有$p(x)+q(x)\in P[x]$,

从而$(p(x)+q(x)) \bmod m\in Z_m[x]$，因而$p(x)+_m q(x)\in Z_m[x]$；

②结合律：$\forall\ h(x),p(x),q(x)\in Z_m[x]$, 有

$$h(x)+_m(p(x)+_m q(x))= h(x)+_m((p(x)+q(x)) \bmod m)$$

$$= (h(x)+(p(x)+q(x)) \bmod m) \bmod m$$

$$= (h(x)+(p(x)+q(x))) \bmod m$$

$$= ((h(x)+p(x))+q(x)) \bmod m$$

(普通多项式加法的结合律)

$$= ((h(x)+p(x)) \bmod m +q(x)) \bmod m$$

$$= (h(x)+p(x)) \bmod m+mq(x)$$

$$= (h(x)+_m p(x))+_m q(x) \quad ;$$

③有幺元：存在着 $0(x)=0\in Z_m[x]$，使得

$\forall p(x)\in Z_m[x]$，都有 $0(x)+_m p(x)=p(x)+_m 0(x)=p(x)$ ；

④有逆元：$\forall p(x)\in Z_m[x]$，可设

$p(x)=a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ $\quad a_k\in Z_m\ (0\le k\le n)$

令：$b_k=m-a_k\in Z_m\ (0\le k\le n)$

则有 $p^{-1}(x)=b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0\in Z_m[x]$，

使得 $p^{-1}(x)+_m p(x)=p(x)+_m p^{-1}(x)=0(x)$

⑤交换律： $\forall p(x),q(x)\in Z_m[x]$, 有

$$p(x)+_m q(x)=(p(x)+q(x)) \bmod m$$

$$=(q(x)+p(x)) \bmod m \qquad \text{(普通多项式加法的交换律)}$$

$$=q(x)+_m p(x) \ ;$$

(2)〈$Z_m[x],\times_m$〉是(交换含幺)半群;

①封闭性：$\forall p(x),q(x)\in Z_m[x]$, 有$p(x)\times q(x)\in P[x]$，从而

$(p(x)\times q(x)) \bmod m\in Z_m[x]$，因而$p(x)\times_m q(x)\in Z_m[x]$;

②结合律：$\forall\ h(x),p(x),q(x)\in Z_m[x]$，有

$$h(x)\times_m(p(x)\times_m q(x))= h(x)\times_m((p(x)\times q(x)) \bmod m)$$

$$= (h(x)\times(p(x)\times q(x)) \bmod m) \bmod m$$

$$= (h(x)\times(p(x)\times q(x))) \bmod m$$

$$= ((h(x)\times p(x))\times q(x)) \bmod m$$ (普通多项式乘法的结合律)

$$= ((h(x)\times p(x)) \bmod m\times q(x)) \bmod m$$

$$= (h(x)\times p(x)) \bmod m\times_m q(x)$$

$$= (h(x)\times_m p(x))\times_m q(x)\ ;$$

③有幺元：存在着 $1(x)=1\in Z_m[x]$，使得$\forall p(x)\in Z_m[x]$, 都有

$1(x)\times_m p(x)=p(x)\times_m 1(x)=p(x)$ ；

④交换律：$\forall p(x),q(x)\in Z_m[x]$, 有

$p(x)\times_m q(x)=(p(x)\times q(x)) \bmod m$

$=(q(x)\times p(x)) \bmod m$ (普通多项式乘法的交换律)

$=q(x)\times_m p(x)$ ；

(3)$\times_m$对$+_m$满足分配律：即 $\forall\ h(x),p(x),q(x)\in Z_m[x]$, 有

$h(x)\times_m(p(x)+_m q(x))$

$= h(x)\times_m(p(x)+q(x)) \bmod m$

$= (h(x)\times(p(x)+q(x)) \bmod m) \bmod m$

$= (h(x)\times(p(x)+q(x))) \bmod m$

$= ((h(x)\times p(x))+ (h(x)\times q(x))) \bmod m$ (普通多项式乘法对加法的分配律)

$= ((h(x)\times p(x)) \bmod m + (h(x)\times q(x)) \bmod m) \bmod m$

$= ((h(x)\times_m p(x))+(h(x)\times_m q(x))) \bmod m$

$= (h(x)\times_m p(x))+_m(h(x)\times_m q(x))$

由$\times_m$的交换律知$\times_m$对$+_m$满足分配律；

由环的定义知〈$Z_m[x],+_m, \times_m$〉是(交换含幺)环。

例7. 〈$Z_p[x{:}n],+_f,\times_f$〉是环。 称此环为多项式模环。

这里： p是素数，$Z_p=\{0,1,2,\ldots,p-1\}$；$Z_p[x{:}n]$是系数在Z_p上的次数不超过n-1的多项式全体；$f\in Z_p[x]$是一n次首1多项式，$+_f$和$\times_f$是多项式的模f加法运算和模f乘法运算。即$\forall p(x),q(x)\in Z_p[x{:}n]$，有

$$p(x)+_f q(x)=(p(x)+_p q(x)) \bmod f$$

$$p(x)\times_f q(x)=(p(x)\times_p q(x)) \bmod f$$

……

于是， 有

(1)〈$Z_p[x:n],+f$〉是交换群；

①封闭性：$\forall p(x),q(x)\in Z_p[x:n]$, 有$p(x)+_p q(x)\in Z_p[x]$ ，

从而$(p(x)+_p q(x)) \bmod f\in Z_p[x:n]$ ， 因而$p(x)+_f q(x)\in Z_p[x:n]$ ；

②结合律：$\forall\ h(x),p(x),q(x)\in Z_p[x:n]$，有

$$h(x)+_f(p(x)+_f q(x))= h(x)+_f((p(x)+_p q(x)) \bmod f)$$

$$= (h(x)+_p(p(x)+_p q(x)) \bmod f) \bmod f$$

$$= (h(x)+_p(p(x)+_p q(x))) \bmod f$$

$$= ((h(x)+_p p(x))+_p q(x)) \bmod f$$ (模数多项式加法的结合律)

$$= ((h(x)+_p p(x)) \bmod f+_p q(x)) \bmod f$$

$$= (h(x)+_p p(x)) \bmod f +_f q(x)$$

$$= (h(x)+_f p(x))+_f q(x)\ ;$$

③有幺元：存在着$0(x)=0\in Z_p[x:n]$，使得$\forall p(x)\in Z_p[x:n]$ 都有

$$0(x)+_f p(x)=p(x)+_f 0(x)=p(x)\ ;$$

④有逆元：$\forall p(x)\in Z_p[x:n]$, 可设

$$p(x)=a_s x^s + a_{s-1} x^{s-1} + \ldots + a_1 x + a_0 \qquad a_k\in Z_p\ (0\le k\le s)$$

令：$b_k=p-a_k\in Z_p\ (0\le k\le s)$

则有 $p^{-1}(x)=b_s x^s + b_{s-1} x^{s-1} + \ldots + b_1 x + b_0\in Z_p[x:n]$,

使得 $p^{-1}(x)+_f p(x)=p(x)+_f p^{-1}(x)=0(x)$;

……

⑤交换律： $\forall p(x),q(x)\in Z_p[x:n]$, 有

$$p(x)+_f q(x)=(p(x)+_p q(x)) \bmod f$$

$$=(q(x)+_p p(x)) \bmod f \qquad \text{(模数多项式加法的交换律)}$$

$$=q(x)+_f p(x) \ ;$$

(2)〈$Z_p[x:n],\times_f$〉是(交换含幺)半群；

①封闭性：$\forall p(x),q(x)\in Z_p[x:n]$, 有$p(x)\times_p q(x)\in Z_p[x]$，

从而$(p(x)\times_p q(x)) \bmod f \in Z_p[x:n]$，因而$p(x)\times_f q(x)\in Z_p[x:n]$；

②结合律：$\forall\ h(x),p(x),q(x)\in Z_p[x:n]$, 有

$$h(x)\times_f(p(x)\times_f q(x))= h(x)\times_f((p(x)\times_p q(x)) \bmod f)$$

$$= (h(x)\times_p(p(x)\times_p q(x)) \bmod f) \bmod f$$

$$= (h(x)\times_p(p(x)\times_p q(x))) \bmod f$$

$$= ((h(x)\times_p p(x))\times_p q(x)) \bmod f$$ (模数多项式乘法的结合律)

$$= ((h(x)\times_p p(x)) \bmod f \times_p q(x)) \bmod f$$

$$= (h(x)\times_p p(x)) \bmod f \times_f q(x)$$

$$= (h(x)\times_f p(x))\times_f q(x)\ ;$$

③有幺元：存在着$1(x)=1\in Z_p[x:n]$，使得$\forall p(x)\in Z_p[x:n]$ 都有

$$1(x)\times_f p(x)=p(x)\times_f 1(x)=p(x)\ ;$$

④交换律：$\forall p(x),q(x)\in Z_p[x:n]$, 有

$$p(x)\times_f q(x)=(p(x)\times_p q(x)) \bmod f$$

$$=(q(x)\times_p p(x)) \bmod f$$

(模数多项式乘法的交换律)

$$=q(x)\times_f p(x)\ ;$$

……

(3) $\times_f$对$+_f$满足分配律：即 $\forall\ h(x),p(x),q(x)\in Z_p[x:n]$ ，有

$$
\begin{aligned}
&h(x)\times_f(p(x)+_f q(x))\\
&= h(x)\times_f(p(x)+_p q(x)) \bmod f\\
&= (h(x)\times_p(p(x)+_p q(x)) \bmod f) \bmod f\\
&= (h(x)\times_p(p(x)+_p q(x))) \bmod f\\
&= ((h(x)\times_p p(x))+_p(h(x)\times_p q(x))) \bmod f \qquad \text{(模数多项式乘法对模数多项式加法的分配律)}\\
&= ((h(x)\times_p p(x)) \bmod f +_p(h(x)\times_p q(x)) \bmod f) \bmod f\\
&= ((h(x)\times_f p(x))+_p(h(x)\times_f q(x))) \bmod f\\
&= (h(x)\times_f p(x))+_f(h(x)\times_f q(x))
\end{aligned}
$$

由$\times_f$的交换律知$\times_f$对$+_f$满足分配律；

由环的定义知〈$Z_p[x:n],+_f,\times_f$〉是(交换含幺)环。

定义2.交换环 含幺环 交换含幺环

设〈R,⊕,⊗〉是环。

(1)若⊗运算满足交换律，则 称〈R,⊕,⊗〉是交换环。

(2)若关于⊗运算有幺元，则 称〈R,⊕,⊗〉是含幺环。

(3)若⊗运算满足交换律又关于⊗运算有幺元，则 称〈R,⊕,⊗〉是交换含幺环。

例8. (1)整数环〈I,+,×〉是交换含幺环吗？关于×运算的幺元是什么？

(2)矩阵环〈$M_{n\times n}$,,+,×〉是交换含幺环吗？关于×运算的幺元是什么？

(3)整数模环〈N_m,$+_m$,$\times_m$〉是交换含幺环吗？关于$\times_m$运算的幺元是什么？

(4)X的子集环〈2^X,⊕,∩〉是交换含幺环吗？关于∩运算的幺元是什么？

……

(5)多项式环〈P[x],+,×〉是交换含幺环吗？关于×运算的幺元是什么？

(6)模数多项式环〈Z_m[x],$+_m$,$\times_m$〉是交换含幺环吗？关于$\times_m$运算的幺元是？

(7)多项式模环〈Z_p[x:n],$+_f$,$\times_f$〉是交换含幺环吗？关于$\times_f$ 运算的幺元是？

定理1.环的基本性质

设〈R,⊕, ⊗〉是环。则∀a,b,c∈R,有

(1) 0⊗a = a⊗0 = 0　　(加法幺元是乘法的零元)

(2) a⊗(-b) = (-a)⊗b = -(a⊗b)；

(3) (-a)⊗(-b) = a⊗b；

(4)(-1)⊗a = -a　　(-1是乘法幺元1的负元)

(5)(-1)⊗(-1)=1　　(-1的乘法逆元是其本身，即$(-1)^{-1}=-1$)

(6)左分配律：a⊗(b-c)=(a⊗b)-(a⊗c)　　(乘法对减法的)

右分配律：(b–c)⊗a=(b⊗a)–(c⊗a)　　(乘法对减法的)

[证].(1)$a\otimes 0 = (a\otimes 0)\oplus 0$

$= (a\otimes 0)\oplus((a\otimes 0)-(a\otimes 0))$

$= (a\otimes 0)\oplus((a\otimes 0)\oplus(-(a\otimes 0)))$

$= ((a\otimes 0)\oplus(a\otimes 0))\oplus(-(a\otimes 0))$ (结合律)

$= (a\otimes(0\oplus 0))\oplus(-(a\otimes 0))$ (分配律)

$= (a\otimes 0)\oplus(-(a\otimes 0))$ ($0\oplus 0 = 0$)

$= (a\otimes 0)-(a\otimes 0)$

$= 0$;

(2)只证a⊗(-b)= -(a⊗b)

a⊗(-b)= (a⊗(-b))⊕0

= (a⊗(-b))⊕((a⊗b)-(a⊗b))

= (a⊗(-b))⊕((a⊗b)⊕(-(a⊗b)))

= ((a⊗(-b))⊕(a⊗b))⊕(-(a⊗b)) (结合律)

= (a⊗((-b)⊕b))⊕(-(a⊗b)) (分配律)

= (a⊗0)⊕(-(a⊗b)) ((-b)⊕b= 0)

= 0⊕(-(a⊗b)) (根据(1) a⊗0 = 0)

= -(a⊗b) ;

(3)(-a)⊗(-b) =-(a⊗(-b))　(根据(2))

=-(-(a⊗b))　(根据(2))

=a⊗b　　(反身律)；

(4)(-1)⊗a =-(1⊗a)　　(根据(2))

=-a；

(5)(−1)⊗(−1)=1⊗1　(根据(3))

=1 ；

(6)只证a⊗(b−c) = (a⊗b)−(a⊗c)

a⊗(b−c)= a⊗(b⊕(−c))

= (a⊗b)⊕ (a⊗(−c)) (分配律)

= (a⊗b)⊕ (−(a⊗c)) (根据(2))

= (a⊗b)−(a⊗c) 。

定义3.含零因子环 无零因子环

设〈R, ⊕, ⊗〉是环。若在环〈R, ⊕, ⊗〉中

(1)$(\exists a\in R)(\exists b\in R)(a\neq 0\wedge b\neq 0\wedge a\otimes b=0)$，则称环(R, ⊕, ⊗)是含零因子环；称a是环中的左零因子，称b是环中的右零因子；

(2)$(\forall a\in R)(\forall b\in R)(a\neq 0\wedge b\neq 0\Rightarrow a\otimes b\neq 0)$，即环中无零因子(no nil-factor)，则称环〈R, ⊕, ⊗〉是无零因子环。

例9.整数环〈I,+, ×〉是无零因子环

已知〈I,+, ×〉是环，由于任意两个不为零的整数相乘,其积不为零，故由定义3知〈I,+, ×〉是无零因子环。

例10.矩阵环〈$M_{n\times n}$,+, ×〉是含零因子环

已知〈$M_{n\times n}$,+, ×〉是环(n≥2)。不妨设n=2，于是有

$$\text{因为存在着}\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\neq\begin{pmatrix}0&0\\0&0\end{pmatrix},\text{但}\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

即两个不为零的矩阵相乘其积为零矩阵，　由定义3知是〈$M_{n\times n}$,+, ×〉含零因子环。

例11.整数模环〈$N_m,+_m,\times_m$〉，

当m为素数时，是无零因子环；

当m不是素数时，是含零因子环……

例12.X的子集环〈$2^X,\oplus,\cap$〉是含零因子环……

例13.多项式环〈$P[x],+,\times$〉是无零因子环……

例14.模数多项式环〈$Z_m[x],+_m,\times_m$〉，

当m为素数时，是无零因子环；

当m不是素数时，是含零因子环。

已知〈$Z_m[x],+_m,\times_m$〉是环。

……

(1)当m为素数时，对任意的 $p(x),q(x)\in Z_m[x]$， $p(x)\neq 0$， (其首项系数$a_r\neq 0$，即$0<a_r<m$),且$q(x)\neq 0$(其首项系数$b_s\neq 0$，即$0<b_s<m$),从而必有$p(x)\times_m q(x)\neq 0$ (否则， 若$p(x)\times_m q(x)=0$，则其首项系数$c_{r+s}=a_r\times_m b_s=0$，因此$a_r\times b_s=km$，由m是素数，则必有$m\mid a_r$或$m\mid b_s$，于是有$a_r=pm$或$b_s=qm$，这与已知$0<a_r<m$且$0<b_s<m$矛盾) 。

即两个非零多项式经过$\times_m$运算后仍为非零多项式。

由定义3知〈$Z_m[x],+_m,\times_m$〉是无零因子环。

(2)当m不是素数时，必存在着$p(x),q(x)\in Z_m[x]$，

$p(x)=a_r x^r$，$0<a_r<m$(即其首项系数$ar\neq 0$)，故 $p(x)\neq 0$，

且 $q(x)=b_s x^s$， $0<b_s<m$ (即其首项系数$bs\neq 0$)，故 $q(x)\neq 0$，使得 $m = a_r \times b_s$

即有 $p(x)\times_m q(x)= (p(x)\times q(x)) \bmod m$

$= (a_r x^r \times b_s x^s) \bmod m$

$= (a_r \times b_s)x^{r+s} \bmod m$

$= mx^{r+s} \bmod m$

$=0 \bmod m$

$=0$

即$p(x)$，$q(x)$是$Z_m[x]$中的零因子， 由定义3知〈$Z_m[x],+_m,\times_m$〉是含零因子环。

例15． 多项式模环〈$Z_p[x:n],+_f,\times_f$〉

当f为素多项式时，是无零因子环；

当f不是素多项式时，是含零因子环。

注：•**素多项式**，也称为**既约多项式**，是$Z_p[x]$中首1，且在Z_p中不能分解因式的多项式。

已知〈$Z_p[x:n],+_f,\times_f$〉是环。

(1)当f为素多项式时，对任意的 $p(x),q(x)\in Z_p[x:n]$，

$p(x)\neq 0$，（即$p(x)\neq k_1(x)f(x)$),且$q(x)\neq 0$(即$q(x)\neq k_2(x)f(x)$),

从而必有$p(x)\times_f q(x)\neq 0$（否则，若$p(x)\times_f q(x)=0$，则必有$p(x)\times_p q(x)=k(x)f(x)$，由$f(x)$是素多项式，则必有$f(x)\mid p(x)$或 $f(x)\mid q(x)$，于是应有$p(x)=k_1(x)f(x)$)或$q(x)=k_2(x)f(x)$，矛盾)。

即两个非零多项式经过$\times_f$运算后仍为非零多项式。由定义3知〈$Z_p[x:n],+_f,\times_f$〉是无零因子环。

(2)当f不是素多项式时，必存在着$p(x),q(x)\in Z_p[x:n]$，　$p(x)\neq 0$，且 $q(x)\neq 0$，使得 $f(x)=p(x)\times_p q(x)$，从而

$$p(x)\times_f q(x)=(p(x)\times_p q(x)) \bmod f$$

$$=f(x) \bmod f$$

$$=0$$

即$p(x)$，$q(x)$是$Z_p[x:n]$中的零因子。

由定义3知〈$Z_p[x:n],+_f,\times_f$〉是含零因子环。

定义4.整环(integral domain)

交换含幺的无零因子环称为整环。

注：●整环又称为整区。

定义4.除环(division ring)

每个非零元都有(乘法)逆元的含幺环称为除环。即，若含幺环〈R, ⊕, ⊗〉满足：

$$(\forall a \in R)(a \neq 0 \Rightarrow a^{-1} \in R)$$

则称其为除环。

例16. (1)整数环〈I,+,×〉是整环：因为整数环〈I,+,×〉是交换含幺环(例8(1))，又是无零因子环(例9)。

但整数环〈I,+,×〉不是除环：因为在整数环〈I,+,×〉中，除幺元1及其负元-1外，其它非零整数$a \in I(a \neq 0)$都没有(乘法)逆元($a^{-1} = 1/a \notin I$)。

(2)矩阵环〈$M_{n\times n}$,,+,×〉不是整环：因为矩阵环〈$M_{n\times n}$,,+,×〉不是交换环,矩阵的乘法没有交换律(例8(2))，而且还是含零因子环(例10)。

矩阵环〈$M_{n\times n}$,+,×〉也不是除环：因为矩阵环〈$M_{n\times n}$,,+,×〉中一些非零矩阵(行列式是零)关于矩阵乘法没有逆元(逆矩阵)。

(3)整数模环〈N_m,$+_m$,$\times_m$〉当m是素数时是整环：因为整数模环〈N_m,$+_m$,$\times_m$〉是交换含幺环(例8(3))，并且当m为素数时，又是无零因子环(例11)；并且也是除环(见下面注)。

整数模环〈N_m,$+_m$,$\times_m$〉当m不是素数时不是整环：因为整数模环〈N_m,$+_m$,$\times_m$〉当m不是素数时是含零因子环(例11)；并且也不是除环(见下面注)。

(4)X的子集环〈2^X,⊕,∩〉不是整环：因为X的子集环〈2^X,⊕,∩〉是含零因子环(例12)；并且也不是除环(见下面注)……

(5)多项式环〈P[x],+,×〉是整环：因为多项式环〈P[x],+,×〉是交换含幺环(例8(5))，又是无零因子环(例13)。

但多项式环〈P[x],+,×〉不是除环：因为有非零多项式ax∈P[x] (a≠0)，关于多项式乘法没有逆元(否则，若ax×q(x)=1，则用比较系数法，可得 q(x)= 0，于是又有ax×q(x)=0，矛盾)。

(6)模数多项式环〈$Z_m[x],+_m,\times_m$〉当m为素数时是整环：因为模数多项式环〈$Z_m[x],+_m,\times_m$〉是交换含幺环(例8(6))，并且当m为素数时，又是无零因子环(例14)。

模数多项式环〈$Z_m[x],+_m,\times_m$〉当m不是素数时不是整环：因为模数多项式环〈$Z_m[x],+_m,\times_m$〉当m不是素数时，是含零因子环(例14) 。

模数多项式环〈$Z_m[x],+_m,\times_m$〉无论如何不是除环：因为有非零多项式$a^x \in Z_m[x](0<a<m)$，关于模数多项式乘法没有逆元(否则，若$a^x \times_m q(x)=1$，则用比较系数法，可得$a^x \times_m q(x)=0$，矛盾) 。

(7)多项式模环〈$Z_p[x:n],+_f,\times_f$〉当f为素多项式时是整环：因为多项式模环〈$Z_p[x:n],+_f,\times_f$〉是交换含幺环(例8(7))，并且当f为素多项式时，是无零因子环(例15)；并且也是除环(见下面注)。

多项式模环〈$Z_p[x:n],+_f,\times_f$〉当f不是素多项式时不是整环：因为多项式模环〈$Z_p[x:n],+_f,\times_f$〉当f不是素多项式时，是含零因子环(例15)；并且也不是除环(见下面注)。

注：●在下面定理4中，将可证：在有限含幺环中

无零因子⇔(非零元)有逆元 ；

●而整数模环〈$N_m,+_m,\times_m$〉，多项式模环〈$Z_p[x:n],+_f,\times_f$〉都是有限含幺环。

定理2. 在环〈R,⊕,⊗〉中，无零因子⇔消去律，即∀a,b,c∈R且a≠0，都有

$a\otimes b= a\otimes c\Rightarrow b=c$ ；

$b\otimes a= c\otimes a\Rightarrow b=c$ 。

[证]. 先证⇒)： ∀a,b,c∈R且a≠0，

$a\otimes b= a\otimes c$

$\Rightarrow (a\otimes b)-(a\otimes c)=0$ (两边同时⊕上-(a⊗c))

$\Rightarrow a\otimes(b-c)=0$ (分配律)

$\Rightarrow b-c=0$ (a≠0及无零因子)

$\Rightarrow b=c$

次证⇐)：用反证法。假设环中有零因子，因此，

必有一对元素$a,b\in R$，$a\neq 0$且$b\neq 0$，使得$a\otimes b=0$。但是 $a\otimes 0=0$，

于是 有$a\otimes b= a\otimes 0$，由$a\neq 0$及消去律可得 $b= 0$，这与已知$b\neq 0$ 矛盾。

这个矛盾说明假设错误，环中无零因子。

定理3. 除环是含幺的无零因子环。

注：●因此，除环未必是整环，整环也未必是除环;

●除环要成为整环，差乘法交换律；整环要成为除环，差(非零元)有乘法逆元 ；

[证].除环是含幺环，因此只须证环无零因子 即可。

$\forall a,b,c \in R$且$a \neq 0$，

$a \otimes b = a \otimes c$

$\Rightarrow b=c$ (两边同时乘上a^{-1} (因$a \neq 0$))

$\Rightarrow$无零因子 (定理2) 。

定理4.在有限含幺环中，无零因子⇔(非零元)有逆元。

[证]. 先证⇒)：因环无零因子，故⊗运算对R\{0}是封闭的, 因此〈R\{0},⊗〉是代数系统。于是。　在代数系统〈R\{0},⊗〉中，因R有限, 故对任何$r\in R\setminus\{0\}$ ，

有$i, j\in N, j>i\geq 1 (j-i\geq 1)$,使得　$r^i=r^j$

$\Rightarrow r^j=r^i$

$\Rightarrow r^{j-i}\otimes r^i=e\otimes r^i$　(指数律、环含幺)

$\Rightarrow r^{j-i}=e$　(消去律)

$\Rightarrow r^{-1}=r^{j-i-1}\vee r=e$　$(j-i>1\vee j-i=1)$

即，非零元有逆元。

次证⇐)：非零元有逆元

⇒ 消去律　（两边同时乘上a^{-1}（因$a\neq 0$））。

⇒无零因子　（定理2）。

注：•关于消去律、无零因子、非零元有逆元之间的关系，见下图：

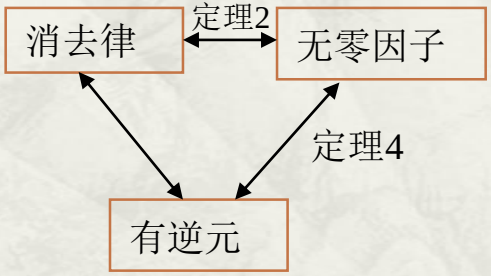


图1

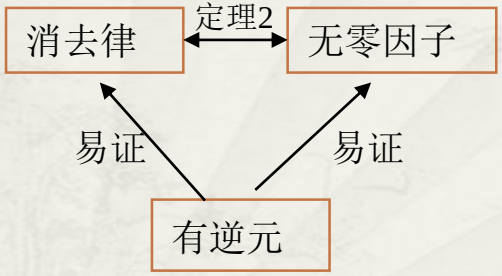


图2

§6.域

定义1.域(field)

设〈F, ⊕, ⊗〉是代数系统， ⊕和⊗是R上的两个二元运算，若

(1) 〈F, ⊕〉是交换群；

(2) 〈F\{0}, ⊗〉是交换群 ；

(3) ⊗对⊕满足分配律：对任何a,b,c∈F，都有

a⊗(b⊕c)=(a⊗b)⊕(a⊗c) ；

则称 〈F, ⊕, ⊗〉是域。

例1.〈Q,+,×〉是域。 称为有理数域。

这里：Q是有理数集，+,×分别是普通的有理数的加法运算和乘法运算，则〈Q,+,×〉是域……

例2.〈R,+,×〉是域。 称为实数域。

这里： R是实数集，+,×分别是普通的实数的加法运算和乘法运算，则〈R,+,×〉是域……

例3.〈C,+,×〉是域。 称为复数域。

这里： C是复数集，+,×分别是普通的复数的加法运算和乘法运算，则〈C,+,×〉是域……

例4.〈X_1,+,×〉是域。称为算术分类域。

这里：$X_1=\{a+b\sqrt{2}:a,b\in Q\}$，+,×分别是普通数的加法运算和乘法运算。

包含性：$X_1\subseteq R$，$X_1\setminus\{0\}\subseteq R$；

非空性：$X_1\neq\varnothing$(因$0=0+0\sqrt{2}\in X_1$)

$X_1\setminus\{0\}\neq\varnothing$(因$1=1+0\sqrt{2}\in X_1\setminus\{0\}$)

(1)〈X_1,+〉是交换群；

①封闭性：$\forall a+b\sqrt{2}$，$c+d\sqrt{2} \in X_1$

$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2} \in X_1$；

②有逆元：$\forall a+b\sqrt{2} \in X_1$，

有$-(a+b\sqrt{2})=(-a)+(-b)\sqrt{2} \in X_1$，

使$(a+b\sqrt{2})+((-a)+(-b)\sqrt{2})=0$；

故根据§6定理14可知〈X_1,+〉是交换群〈R,+〉的子群。因此，〈X_1,+〉是交换群；

(2)〈$X_1\backslash\{0\}$,×〉是交换群；须证它是交换群〈R\{0},×〉的子群。

①封闭性：$\forall a+b\sqrt{2},\ c+d\sqrt{2}\in X_1\backslash\{0\}$，于是a,b至少有一不为零，c,d至少有一不为零，从而

$(a+b\sqrt{2})\times(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in X_1\backslash\{0\}$

否则 ac+2bd =0, ad+bc =0,由a,b至少有一不为零可反解出c=0,d=0

(因为齐次线性方程组

$$\begin{cases} ac+2bd=0 \\ bc+ad=0 \end{cases}$$ 的系数行列式 $$\begin{vmatrix} a & 2b \\ b & a \end{vmatrix}=a^2-2b^2\neq 0$$

(否则a,b全为零与a,b至少有一不为零矛盾，或者全不为零且 $\frac{a}{b}$ ＝a/b是有理数，与其是无理数矛盾))2 而这与c,d至少有一不为零矛盾。

②有逆元：$\forall a+b\sqrt{2}\in X_1\setminus\{0\}$ ，有

$$(a+b\sqrt{2})^{-1}=(a-b\sqrt{2})/(a^2-2b^2)\in X_1\setminus\{0\}$$

使 $(a+b\sqrt{2})\times(a-b\sqrt{2})/(a^2-2b^2)=1$ ；

故根据§6定理14可知〈$X_1\setminus\{0\}$,×〉是交换群〈$R\setminus\{0\}$,×〉的子群。因此，〈$X_1\setminus\{0\}$,×〉是交换群；

(3)×对+满足分配律：由老代数〈R,+,×〉遗传；

所以按定义1知则〈X_1,+,×〉是域。

注：●实际上易证〈X_k,+,×〉都是域。这里$X_k=\{a+b\sqrt{p_k}:a,b\in Q\}$，其中$p_k$是第k个素数 。这正是 为什么称此类域为算术分类域。

定理1. 可交换的除环是域。

[证].除环是每个非零元都有(乘法)逆元的含幺环，它与域概念仅差(乘法)交换律。现在正好补齐，所以，可交换的除环是域。

定理2. 有限整环是域。

[证].整环是交换含幺的无零因子环，它与域概念仅差每个非零元都有(乘法)逆元。但在有限环的情况下，上节定理4已经证明：

无零因子⇔每个非零元都有(乘法)逆元

因此，有限整环是域。

例5. (1)整数环〈I,+,×〉不是域：因为整数环〈I,+,×〉虽是整环，但不是有限环。实际上，它的非零整数$a\in I(a\neq 0)$，除幺元1及其负元-1外，都没有(乘法)逆元($a^{-1}=1/a\notin I$)；

(2)矩阵环〈$M_{n\times n}$,,+,×〉不是域：因为它是含零因子环，它的一些非零矩阵(行列式是零)关于矩阵乘法没有逆元(逆矩阵)；

(3)整数模环〈$N_m,+_m,\times_m$〉当m是素数时是域：因为当m为素数时它是整环，并且又是有限的(|Nm|＝m)；

整数模环〈 $N_m,+_m,\times_m$ 〉当m不是素数时不是域：因为当m不是素数时，它是含零因子环，因而并非每个非零元都有(乘法)逆元；

(4)X的子集环〈2^X,⊕,∩〉不是域：因为它是含零因子环，因而并非每个非零元都有(乘法)逆元；

(5)多项式环〈P[x],+,×〉不是域：因为有非零多项式关于多项式乘法没有逆元；

(6)模数多项式环〈$Z_m[x]$,$+_m$,$\times_m$〉不是域：因为有非零多项式关于模数多项式乘法没有逆元；

(7)多项式模环〈$Z_p[x:n],+_f,\times_f$〉当f为素多项式时是域：因为它是整环，并且又是有限的；

实际上，对任何多项式$p(x)\in Z_p[x:n]$，可设

$$p(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\ldots+a_1x+a_0 \qquad a_k\in Z_p\ (0\le k\le n-1)$$

因为$Z_p=\{0,1,2,\ldots,p-1\}$，因而每个系数都有p种选择，故按乘法原理，可组成p^n个$Z_p[x:n]$中的多项式，因此$|Z_p[x:n]|=p^n$，所以$Z_p[x:n]$是有限的；

多项式模环〈$Z_p[x:n],+_f,\times_f$〉当f不是素多项式时不是域：因为当f不是素多项式时，是含零因子环，因而并非每个非零元都有(乘法)逆元。

投票

最多可选1项

设置

设$<N_m, +_m, \times_m>$是环，当m=15时，$<N_m, +_m, \times_m>$是域。

A 此命题成立

B 此命题不成立

提交

环	$(I,+,\times)$	$(M_{n\times n},+,\times)$	$(N_m,+_m,\times_m)$		$(2^X,\oplus,\cap)$	$(P[x],+,\times)$	$(Z_m[x],+_m,\times_m)$		$(Z_p[x{:}n],+_f,\times_f)$	
运算	×	×	$\times_m$		∩	×	$\times_m$		$\times_f$	
交换律	有	无	有		有	有	有		有	
幺元	1	E	$[1]_m$		X	1	1		1	
零因子	无	有	m是素数	m是合数	有	无	m是素数	m是合数	*f*是素多项式	*f*非素多项式
			无	有			无	有	无	有
整环	是	不是	是	不是	不是	是	是	不是	是	不是
除环	不是	不是	是	不是	不是	不是	不是	不是	是	不是
域	不是	不是	是	不是	不是	不是	不是	不是	是	不是

表3

§7.同余关系(*)

- 同余关系
- 商代数
- 积代数
- 同态图

§7.同余关系

定义1.同余关系(congruence relation)

设(X,*,E)是代数系统，*是X上的二元运算，E是X上的等价关系。若E关于*具有替换性，即

$$(\forall x_1,x_2\in X)(\forall y_1,y_2\in X)(x_1Ex_2\wedge y_1Ey_2\Rightarrow x_1*y_1Ex_2*y_2)$$

则称E是代数系统(X,*)上的同余关系。

例1.$(I,+),(I,\times)$都是代数系统，模m数同余关系为

$\forall a,b\in I, a\equiv b \pmod m \Leftrightarrow (\exists k\in I)(a-b=km)$

是I上的等价关系，即$\forall a,b,c\in I$

$a\equiv a \pmod m$，　　$a\equiv b \pmod m \Rightarrow b\equiv a \pmod m$

$a\equiv b \pmod m \wedge b\equiv c \pmod m \Rightarrow a\equiv c \pmod m$

关于+和×运算都具有替换性，即$\forall a,b,c,d\in I$

$a\equiv b \pmod m \wedge c\equiv d \pmod m \Rightarrow a+c\equiv b+d \pmod m$

$a\equiv b \pmod m \wedge c\equiv d \pmod m \Rightarrow a\times c\equiv b\times d \pmod m$

所以模m数同余关系是代数系统$(I,+)$和$(I,\times)$上的同余关系。

注：●模m数同余关系是同余关系概念的一个具体实例；

●同余关系概念正是模m数同余关系概念的抽象和推广；

定义2.商代数(quotient algebras)

设(X,*,E)是代数系统，*是X上的二元运算，E是X上的同余关系，X/E={$[x]_E$: $x\in X$}是X上E的商集, 其中 $[x]_E=\{y: y\in X \wedge yEx\}$。定义X/E上的二元运算⊗如下：

$$\otimes : X/E \times X/E \to X/E$$

$$\forall x, y\in X, [x]_E \otimes [y]_E = [x*y]_E$$

则(X/E, ⊗)是代数系统， 称(X/E, ⊗)为由(X,*)上同余关系E诱导出的商代数。

注：●要证明⊗是X/E上的二元运算，应证明如下两点：

(1)后者唯一：　$\forall x_1,x_2\in X, \forall y_1,y_2\in X$

$[x_1]_E=[x_2]_E \wedge [y_1]_E=[y_2]_E$

$\Rightarrow x_1 E x_2 \wedge y_1 E y_2$　　（第四章§5定理1(2)）

$\Rightarrow x_1*y_1 E x_2*y_2$　　（E是同余关系,具有替换性）

$\Rightarrow [x_1*y_1]_E=[x_2*y_2]_E$　（第四章§5定理1(2)）

$\Rightarrow [x_1]_E\otimes[y_1]_E=[x_2]_E\otimes[y_2]_E$　；

(2)封闭性: $\forall [x]_E, [y]_E$

$[x]_E, [y]_E \in X/E$

$\Rightarrow x, y \in X$

$\Rightarrow x^* y \in X$ (因(X, *)是代数系统, *运算具有封闭性)

$\Rightarrow [x^* y]_E \in X/E$

$\Rightarrow [x]_E \otimes [y]_E \in X/E$ (因$[x]_E \otimes [y]_E = [x^* y]_E$);

- ⊗具有封闭性已经证明了(X/E, ⊗)是代数系统。

例2. $(N_m, +_m)$是$(I, +)$上模m数同余关系诱导出的商代数。

$N_m = I/\equiv_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-2]_m, [m-1]_m\}$

$\forall [i]_m, [j]_m \in N_m$

$[i]_m +_m [j]_m = [(i+j) \bmod m]_m$ 。

例3. $(N_m, \times_m)$是$(I, \times)$上模m数同余关系诱导出的商代数。

$N_m = I/\equiv_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-2]_m, [m-1]_m\}$

$\forall [i]_m, [j]_m \in N_m$

$[i]_m \times_m [j]_m = [(i \times j) \bmod m]_m$ 。

定理1. 代数系统(X,*)满同态于由其上的同余关系E诱导出的商代数(X/E, ⊗) 。

[证].建立自然映射(典范映射 canonical mapping)：

$$h: X \to X/E$$

$$\forall x \in X,\ h(x)=[x]_E$$

于是有

(1)后者唯一： $\forall x\in X$, 若$\exists [y_1]_E, [y_2]_E\in X/E$, 使得

$h(x)= [y_1]_E \wedge h(x) =[y_2]_E$

$\Rightarrow y_1 E x \wedge y_2 E x$ （定义）

$\Rightarrow y_1 E x \wedge x E y_2$ （E是等价关系,具有对称性）

$\Rightarrow y_1 E y_2$ （E是等价关系,具有传递性）

$\Rightarrow [y_1]_E= [y_2]_E$ （第二章§5定理1 (2)）

(2)同态公式： $\forall x, y\in X$, $h(x*y)=[x*y]_E=[x]_E\otimes[y]_E=h(x)\otimes h(y)$

(3)满射： $\forall [x]_E\in X/E, \exists x\in X$,使得 $h(x)=[x]_E$。

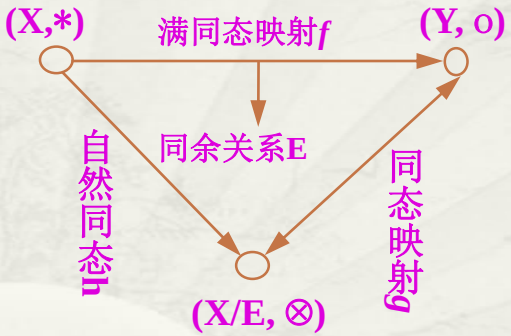
注：●由此而得的同态函数h称为自然同态(natural homomorphism)。

定理2. 设代数系统$(X,*)$满同态于代数系统$(Y,\circ)$。即有同态函数 $f: X\to Y$，且$\Re(f)=Y$。现在由f在X上建立等价关系E：$\forall x, y\in X$

$$xEy \Leftrightarrow f(x)=f(y)$$

则(1) E是X上的同余关系；

(2) $(Y,\circ)$同构于商代数$(X/E,\otimes)$ 。



[证].只证(2)　建立映射 $g:X/E\to Y$

$\forall [x]_E \in X/E$，$g([x]_E)= f(x)$

则有(1) 双射：

(a)后者唯一：$\forall [x]_E, [y]_E \in X/E$，

$[x]_E = [y]_E$

$\Rightarrow xEy$　　（第四章§5定理1 (2)）

$\Rightarrow f(x)= f(y)$

$\Rightarrow g([x]_E)= g([y]_E)$

(b)单射：$\forall [x]_E, [y]_E \in X/E$，

$g([x]_E) = g([y]_E)$

$\Rightarrow f(x) = f(y)$

$\Rightarrow xEy$　　(第四章§5定理1(2))

$\Rightarrow [x]_E = [y]_E$；

(c)满射：对于任何$y \in Y$，由于f是满射，故知

存在着$x \in X$，使$f(x)=y$，从而有$[x]_E \in X/E$，

使　　$g([x]_E) = f(x)=y$；

(2)同态公式：$\forall [x]_E, [y]_E \in X/E$，

$g([x]_E \otimes [y]_E) = g([x*y]_E)$

$= f(x*y)$

$= f(x) \circ f(y)$　　(f是同态函数)

$= g([x]_E) \circ g([y]_E)$ 。

定义3.积代数(product algebras)

两个代数系统(X,*)和(Y, O)的积代数定义为如下的代数系统：

$$(X,*)\times(Y,O)=(X\times Y,\otimes)$$

使得 $\forall(x1,y1),(x2,y2)\in X\times Y,$

$$(x1,y1)\otimes(x2,y2)=(x1*x2,\ y1\ O\ y2)$$ 。

注：•积代数⊗运算的封闭性由两个代数系统的* ， O运算的封闭性来保证;

因此积代数(X×Y, ⊗)显然是代数系统。

例2. $(N_2, +_2, [0]_2)$和 $(N_3, +_3, [0]_3)$的积代数 $(N_2 \times N_3, \oplus, ([0]_2, [0]_3))$,

其中

$$N_2 \times N_3 = \{([0]_2,[0]_3),([1]_2,[1]_3), ([0]_2,[2]_3), ([1]_2,[0]_3), ([0]_2,[1]_3), ([1]_2,[2]_3)\}$$

$$\forall ([a]_2,[b]_3), ([c]_2,[d]_3) \in N_2 \times N_3$$

$$([a]_2,[b]_3) \oplus ([c]_2,[d]_3)$$

$$= ([(a+c) \bmod 2]_2, [(b+d) \bmod 3]_3) \text{ 。}$$