回忆：设$(R,+,0,\cdot,1)$是环，如果R中既无左零因子，右无右零因子，则称R的无零因子环。如果R是交换环又无零因子，则称R是整环

定理3.2 [整无零因子环中的消去律]

设R是无零因子环，$a,b,c\in R$且$a\neq 0$

$$ab=ac \Rightarrow b=c \quad (\text{左消去})$$
$$ba=ca \Rightarrow b=c \quad (\text{右消去})$$

证：$ab=ac \Rightarrow ab-ac=0$

$\Rightarrow a(b-c)=0$

$\because a$不是左零因子 $\therefore b-c=0$

即 $b=c$.

同样可以证明右消去律.

注：在整环中，左，右消去律同时成立

简称为消去律.

例：$(\mathbb{Z},+,0,\cdot,1)$是整环 ①

注：在环R中什么时候，$a,b,c\in R$

$$ab=ac \Rightarrow b=c$$

特形1 R是无零因子环

特形2 a是可逆元 [$a^{-1}ab=a^{-1}ac$

$\Rightarrow 1b=1c \Rightarrow b=c$]

例：在$\mathbb{Z}_{10}$中 $\bar{2}\cdot\bar{5}=\bar{2}\cdot\bar{0}$ 但 $\bar{5}\neq\bar{0}$

定义：设$(R,+,0,\cdot,1)$是环.

$S\subset R$, $0,1\in S$. 如果$(S,+,0,\cdot,1)$也是环，则称S是R的子环

例：$(\mathbb{Z},+,0,\cdot,1)$是$(\mathbb{Q},+,0,\cdot,1)$的子环.

例：设$A\in M_n(\mathbb{R})$ 记

$\mathbb{R}[A]$是由$A^0, A, A^2, \cdots$在$\mathbb{R}$上所有

$$\mathbb{R}[A]=\{a_mA^m+a_{m-1}A^{m-1}+\cdots+a_0A^0 \mid m\in\mathbb{N},\ a_i\in\mathbb{R}\}$$

则 $\mathbb{R}[A]$ 是 $M_n(\mathbb{R})$ 的子环. 且 $\mathbb{R}[A]$ 是交换环.

验证: $O_{n\times n}\in\mathbb{R}[A]$ (取 $a_m=a_{m-1}=\cdots=a_0=0$)

$E_n\in\mathbb{R}[A]$ (取 $m=0$, $a_0=1$)

设 $P=p_kA^k+p_{k-1}A^{k-1}+\cdots+p_0E_n$ $p_i\in\mathbb{R}$

$Q=q_lA^l+q_{l-1}A^{l-1}+\cdots+q_0E_n$ $q_j\in\mathbb{R}$

不妨设 $k\geq l$, 令 $q_k=\cdots=q_{l+1}=0$ 则

$$Q=q_kA^k+\cdots+q_{l+1}A^{l+1}+q_lA^l+\cdots+q_1E_n$$

$$P-Q=\sum_{i=0}^{k}(p_i-q_i)A^i\in\mathbb{R}[A]$$

$\Rightarrow$ $(\mathbb{R}[A],+,O_{n\times n})$ 是 $(M_n(\mathbb{R}),+,O_{n\times n})$ 的(交换)子环

注意: $p_iA^iq_jA^j=p_iq_jA^{i+j}$

$$PQ=\left(\sum_{i=0}^{k}p_iA^i\right)\left(\sum_{j=0}^{l}q_jA^j\right)$$

$\neq\sum_{i=0}^{k}p_iA^i\sum_{i=0}^{k}q_iA^i$

$$=\sum_{i=0}^{k}\sum_{j=0}^{l}(p_iA^i)(q_jA^j)\quad[\text{分配律}]$$

$$=\sum_{i=0}^{k}\sum_{j=0}^{l}p_iq_jA^{i+j}$$

$$\boxed{PQ=\sum_{i=0}^{k}\sum_{j=0}^{l}p_iq_jA^{i+j}}\quad(*)$$

对(*)的右侧, 关于 A 的幂次合并同类项得 $PQ\in\mathbb{R}[A]$. 于是 $\mathbb{R}[A]$ 关于 $M_n(\mathbb{R})$ 中乘法封闭. $(\mathbb{R}[A],\cdot,E_n)$ 是含幺半群, 分配律自然成立.

由(*)可知 $QP=\sum_{j=0}^{l}\sum_{i=0}^{k}q_jp_iA^{i+j}$

因为 $p_iq_j=q_jp_i$ 所以 $QP=PQ$

$\mathbb{R}[A]$ 是交换环.

定义：设 $(R,+,0_R,\cdot,1_R)$ 和 $(S,+,0_S,\cdot,1_S)$ 是两个环，$\varphi: R \to S$ 是环同态

如果 $\forall\ a,b \in R$

(i) $\varphi(a+b) = \varphi(a)+\varphi(b)$

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$

(iii) $\varphi(1_R) = 1_S$.

注：由(i)可知，φ 是从 $(R,+,0_R)$ 到 $(S,+,0_S)$ 的群同态，于是 $\varphi(0_R)=0_S$

例：商映射 $\pi: \mathbb{Z} \to \mathbb{Z}_n$，$a \mapsto \bar{a}$ 是环同态

验证：设 $a,b \in \mathbb{Z}$

$\pi(a+b) = \overline{a+b} = \bar{a}+\bar{b} = \pi(a)+\pi(b)$

$\pi(ab) = \overline{ab} = \bar{a}\bar{b} = \pi(a)\pi(b)$

$\pi(1) = \bar{1}$.

π 是环同态.

定理2.1 设 R 是环，$U_R = \{r \in R \mid r$ 可逆$\}$

则 $(U_R,\cdot,1)$ 是群.

证：验证乘法封闭. 设 $a,b \in U_R$

则 $a^{-1}, b^{-1} \in R$. $ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$

$= a1a^{-1} = aa^{-1} = 1$ 同理

$(b^{-1}a^{-1})(ab) = 1$. 于是 $ab \in U_R$

$1\cdot 1 = 1 \Rightarrow 1 \in U_R$

a 可逆 $\Rightarrow a^{-1}$ 也可逆 $\Rightarrow a^{-1} \in U_R$

于是 U_R 是群 ☒

例：$U_{M_n(\mathbb{R})} = GL_n(\mathbb{R})$

例：设 p 为素数，证明 $U_{\mathbb{Z}_p} = \mathbb{Z}_p \setminus \{\bar{0}\}$

证：设 $\bar{m} \in \mathbb{Z}_p \setminus \{\bar{0}\}$，则 $p \nmid m$.

~~于是 gcd~~ $\because p$ 为素数 $\therefore \gcd(p,m)=1$

由(第二个)命题1.1. $\bar{m}$ 在 $\mathbb{Z}_p$ 中可逆

$\Rightarrow \bar{m} \in U_{\mathbb{Z}_p}$. 显然 $\bar{0} \notin U_{\mathbb{Z}_p} \Rightarrow U_{\mathbb{Z}_p} = \mathbb{Z}_p \setminus \{\bar{0}\}$

§4. 域 (field)

定义：设 $(F, +, 0, \cdot, 1)$ 是交换环，

如果 F 中任何非零元都可逆

则称 F 是域.

换言之 F 是域当且仅当 F 交换且

$U_F = F \setminus \{0\}$.

注：域是整环. 设 $a \in F \setminus \{0\}$, $b \in F$

$ab = 0 \Rightarrow a^{-1}ab = 0 \Rightarrow 1 \cdot b = 0$

$\Rightarrow b = 0 \Rightarrow a$ 不是零因子.

例：$(\mathbb{Q}, +, 0, \cdot, 1)$, $(\mathbb{R}, +, 0, \cdot, 1)$

是域, $(\mathbb{Z}_p, +, \bar{0}, \cdot, \bar{1})$ 是域. 其中

p 是素数 (见§3节最后的例子)

例. (分式域) 设 D 是整环

$D^* = D \setminus \{0\}$. 在 $D \times D^*$ 上定义

如下等价关系

设 $(a, b), (c, d) \in D \times D^*$

$(a, b) \sim (c, d)$ 如果 $ad = bc$

验证 "$\sim$" 是等价关系

自反 $ab = ba \Rightarrow (a, b) \sim (a, b)$

对称 设 $(a, b) \sim (c, d)$ 则

$ad = bc \Rightarrow cb = da \Rightarrow (c, d) \sim (a, b)$

传递. 设 $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in D \times D^*$

$(a_1, b_1) \sim (a_2, b_2)$, $(a_2, b_2) \sim (a_3, b_3)$

则 $a_1 b_2 = b_1 a_2$, $a_2 b_3 = b_2 a_3$

$\Rightarrow a_1 b_2 a_2 b_3 = b_1 a_2 b_2 a_3$

$\Rightarrow a_1 b_3 = b_1 a_3$ (消去律)

$\Rightarrow (a_1, b_1) \sim (a_3, b_3)$.

设 $F = (D \times D^*)/\sim$ 则 (a, b) 的等价

类为 $\frac{a}{b}$

设 $\frac{a}{b}, \frac{c}{d} \in F$. 定义

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

验证："+" 在 F 上是良定义的

设 $\frac{a}{b}=\frac{a'}{b'}$, $\frac{c}{d}=\frac{c'}{d'}$

即: $(a,b)\sim(a',b')$, $(c,d)\sim(c',d')$

换言之 $\boxed{ab'=ba',\ cd'=dc'\quad (*)}$

要验证 $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$

即 $\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$

即 $(ad+bc,\ bd)=(a'd'+b'c',\ b'd')$

也就是 $\underbrace{(ad+bc)b'd'}_{l}=\underbrace{(a'd'+b'c')bd}_{r}$

$l-r=adb'd'+bcb'd'-a'd'bd-b'c'bd$

$=ba'dd'+c'dbb'-a'bd'd-b'dbb$

$=0$

"+" 是良定义 ✓

结合律 $\left(\frac{a_1}{b_1}+\frac{a_2}{b_2}\right)+\frac{a_3}{b_3}$

$=\frac{a_1b_2+a_2b_1}{b_1b_2}+\frac{a_3}{b_3}=\frac{a_1b_2b_3+a_2b_1b_3+a_3b_1b_2}{b_1b_2b_3}$

$=\frac{a_1}{b_1}+\left(\frac{a_2}{b_2}+\frac{a_3}{b_3}\right)$

记 $\frac{0}{1}=\{(0,b)\mid b\in D^*\}$ (**) ⑤

验证: $(0,1)\sim(0,b)$ 可直接得到

设 $(0,1)\sim(a,b)$ 则 $a=0\cdot b=0$

(**)可记

$\frac{a}{b}+\frac{0}{1}=\frac{a\cdot1+0\cdot b}{b\cdot1}=\frac{a}{b}$

同样 $\frac{0}{1}+\frac{a}{b}=\frac{a}{b}$

$\frac{a}{b}+\frac{-a}{b}=\frac{ab-ba}{b^2}=\frac{0}{b^2}=\frac{0}{1}$ (**)

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

$\Rightarrow (F,+,\frac{0}{1})$ 是交换群

定义: $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$

良定义: $\frac{a}{b}=\frac{a'}{b'}$ $\frac{c}{d}=\frac{c'}{d'}$

要验证: $\frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}$

即 $\frac{ac}{bd}=\frac{a'c'}{b'd'}$

即 $\underbrace{(ac,b'd')}_{l}=\underbrace{(bd)a'c'}_{r}$

$$l - r = acb'd' - bda'c'$$
$$= a'bc'd - bda'c' \quad (\because (*1))$$
$$= 0$$

· 良定义

结合律: $\left(\frac{a_1}{b_1}\cdot\frac{a_2}{b_2}\right)\cdot\frac{a_3}{b_3} = \left(\frac{a_1a_2}{b_1b_2}\right)\cdot\frac{a_3}{b_3}$

$$= \frac{(a_1a_2)a_3}{(b_1b_2)(b_3)} = \frac{a_1(a_2a_3)}{b_1(b_2b_3)} = \frac{a_1}{b_1}\left(\frac{a_2}{b_2}\cdot\frac{a_3}{b_3}\right)$$

注: $\frac{1}{1} = \{(b,b) \mid b \in D^*\}$. (***)

验证: $\frac{1}{1} = \frac{a}{b} \iff (1,1) \sim (a,b)$

$\iff a\cdot 1 = 1\cdot b \iff a = b.$

$$\frac{a}{b}\cdot\frac{1}{1} = \frac{a\cdot 1}{b\cdot 1} = \frac{a}{b}$$

~~$\frac{b}{a}\cdot\frac{1}{1}$~~ $\neq$ ~~$\frac{a}{b}$~~

$$\frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd} = \frac{c}{d}\cdot\frac{a}{b}$$

$(F, \cdot, \frac{1}{1})$ 是交换幺含幺半群.

分配律:

$$\frac{a_1}{b_1}\left(\frac{a_2}{b_2}+\frac{a_3}{b_3}\right) = \frac{a_1}{b_1}\left(\frac{a_2b_3+a_3b_2}{b_2b_2}\right)$$

$$= \frac{a_1a_2b_3 + a_1a_3b_2}{b_1b_2b_3} \quad \text{—①}$$

$$\frac{a_1}{b_1}\frac{a_2}{b_2} + \frac{a_1}{b_1}\frac{a_3}{b_3} = \frac{a_1a_2}{b_1b_2} + \frac{a_1a_3}{b_1b_3}$$

$$= \frac{a_1a_2b_1b_3 + a_1a_3b_1b_2}{b_1^2b_2b_3} \quad \text{—②}$$

注. 约分: 设 $u \in D^*$ $\frac{a}{b} = \frac{ua}{ub}$

验证: $aub - bua = u(ab-ab) = 0$ ✓

由①,②和约分, 分配律成立

于是 $(F, +, \frac{0}{1}, \cdot, \frac{1}{1})$ 是交换环

对 设 $\frac{a}{b} \in F$ $\frac{a}{b} \neq \frac{0}{1}$. 则 $a \in D^*$ [见(***)]

$$\frac{a}{b}\cdot\frac{b}{a} = \frac{ab}{ab} = \frac{1}{1} \quad (\text{约分})$$

于是 F 是域

注 (the abuse of notation). $\forall a \in D$

把 $\frac{a}{1}$ 简记为 a. 于是

$$\frac{0}{1} = 0, \quad \frac{1}{1} = 1$$

则 $(F, +, 0, \cdot, 1)$ 是域, 且

D 是 F 的子集. 称 F 是 D 的分式域

定理4.1 设 D 是整环. 则 D 有分式域 F 且 $D \subset F$. (D 是 F 的子环)

例: $\mathbb{Q}$ 是 $\mathbb{Z}$ 的分式域

例: 设 F 是域. 证明 F 的分式域是 F 本身.

证: 设 $F^* = F \setminus \{0\}$. $(a,b) \in F \times F^*$

则 $b \neq 0$. $\Rightarrow b^{-1} \in F \Rightarrow (ab^{-1}, 1) \in F \times F^*$)

$\because$ ~~$a \cdot b^{-1}$~~ $a \cdot 1 = b a b^{-1} =$

$\therefore (a,b) \sim (ab^{-1}, 1)$

$\Rightarrow \frac{a}{b} = \frac{ab^{-1}}{1} = ab^{-1} \in F$. 图

引理 4.1 设 $(F, +, 0, \cdot, 1)$ 是域, 如果在加法群 $(F, +, 0)$ 中 1 的阶有限

则 该阶是素数

证: 设 $k = \operatorname{ord}(1)$. 则 $k > 1$. 设 $m, n \in \mathbb{Z}^+$

使得 $k = mn$ 由

$0 = k \cdot 1 = mn1 = mn(1 \cdot 1) = (m1)(n1)$ [域中]

$\Rightarrow m1 = 0$ 或 $n1 = 0$

同为 $1 \le m \le k$, $1 \le n \le k$, 所以

$m = k$ 或 $n = k$ (阶的定义) ⑦

$\Rightarrow k$ 是素数 图

定义: 设 $(F, +, 0, \cdot, 1)$ 是域. 如果 1 在 $(F, +, 0)$ 中阶是 ∞. 则称 F 的特征为 0

如果 1 的阶是素数 p, 则称 F 的特征为 p

域的特征记为 $\operatorname{char}(F)$.

命题 4.1 (Freshmen's dream)

设 F 是特征为 p 的域, $a, b \in F$

则 $(a+b)^p = a^p + b^p$

证: $\because F$ 是交换环 $\therefore$ 二项式定理

成立. 于是

$$(a+b)^p = a^p + \left[\sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k \right] + b^p$$

下证, $\binom{p}{k} a^{p-k} b^k = 0$

由 第一章 §8 最后的例子

(讲义五 第一页) $\exists l \in \mathbb{Z}^+$ $\binom{p}{k} = pl$.

回忆：Freshmen's dream

设 F 是特征为 p 的域，其中 p 是素数

则 $\forall\ a, b \in F$

$$(a+b)^p = a^p + b^p$$

例：设 $r \in F$，域 F 的特征为 $p>0$

则：$p \mid k \Rightarrow kr = 0$

证：设 $k = pl$.

$$kr = (pl)r = (pl)(r\cdot 1)$$
$$= (lp)(p\cdot 1) = 0$$

再证：Freshmen's dream

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$$

（二项式定理）

当 $k \in \{1, 2, \cdots p-1\}$

$$p \mid \binom{p}{k} \Rightarrow \binom{p}{1}a^{p-k}b^k = 0$$
$$\Rightarrow (a+b)^p = a^p + b^p$$

定义：设 $\varphi: E \to F$ 是两个域

$\varphi: E \to F$ 是环同态

则称 φ 是 E 到 F 域同态.

命题 4.2 设 $\varphi: E \to F$ 是域同态，则

φ 是单射.

证：设 $a, b \in E$. $\varphi(a) = \varphi(b)$

则 $\varphi(a-b) \neq 0_F$

假设 $a \neq b$.

$a - b \neq 0$ 于是 $\exists\, c \in F$，使得 $c(a-b) = 1_E$

且 $\varphi(a-b) = 0_F$

$$1_F = \varphi(c(a-b)) = \varphi(c)\varphi(a-b) = \varphi(c)\cdot 0_F = 0_F$$

$\to\leftarrow$

例：设 F 是特征为 p 的域. 证明

$\varphi: F \to F$ 是域同态

$a \mapsto a^p$

$$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = (ab)^p = a^p b^p$$
$$\varphi(1_F) = 1^p = 1$$

□

命题4.3 (Fermat little theorem)

设 p 是素数，$m \in \mathbb{Z}$ 且 $p \nmid m$

则 $m^{p-1} \equiv 1 \mod p$

证：$\because \mathbb{Z}_p$ 是域 $\therefore \mathbb{Z}_p \setminus \{0\}$ 是 $p-1$

p 个等价类. $\because p \nmid m \therefore \overline{m}$ 在 $\mathbb{Z}_p$ 中

非零. 由此可知 $\overline{m} \in \mathbb{Z}_p \setminus \{0\}$

由 Lagrange 定理 $\overline{m}^{p-1} = \overline{1} \mod p$

$\Rightarrow$ 即 $m^{p-1} \equiv 1 \mod p$ 得证

例：设 p 是素数. $m \in \mathbb{Z}$. 则

$$m^p \equiv m \mod p$$

证：若 $p \nmid m$. 则 即 $m^{p-1} \equiv 1 \mod p$

$\Rightarrow m^{p-1} - 1 = kp$，其中 $k \in \mathbb{Z}$

$\Rightarrow m^p - m = mkp$

$\Rightarrow m^p \equiv m \mod p$.

若 $p \mid m$. 则

$m = kp \Rightarrow m \equiv 0 \mod p$ 且

$m^p \equiv 0 \mod p \Rightarrow m^p \equiv m \mod p$. 得证

§5 域上的线性代数

注：在第二，三章中，用到若干例子

使用 $2 \neq 0$ 的条件，若 $a_1^2 + \cdots + a_k^2 = 0 \Rightarrow a_1 = \cdots = a_k = 0$

所有的定义，定理，等结论对任

何域都成立.

这是因为，在证明过程中，我

们只用到 $+, \cdot$ 和求逆.

记号：设 F 是任意域

$$M_n(F) = \{ A = (a_{ij})_{n \times n} \mid a_{ij} \in F, i,j \in \{1 \sim n\} \}$$

例: $A=\begin{pmatrix}\bar1 & \bar2 & \bar3\\ \bar0 & \bar2 & \bar4\\ \bar1 & \bar4 & \bar2\end{pmatrix}\in M_3(\mathbb{Z}_5)$

计算 V_A 的维数和一组基

$$A\to\begin{pmatrix}\bar1 & \bar2 & \bar3\\ \bar0 & \bar2 & \bar4\\ 0 & \bar2 & -\bar1\end{pmatrix}\to\begin{pmatrix}\bar1 & \bar2 & \bar3\\ \bar0 & \bar2 & \bar4\\ \bar0 & \bar2 & \bar4\end{pmatrix}\to\begin{pmatrix}\bar1 & \bar2 & \bar3\\ \bar0 & \bar2 & \bar4\\ 0 & 0 & 0\end{pmatrix}$$

$\text{rank}(A)=2 \Rightarrow \dim V_A=3-2=1$

$$\begin{cases}x_1+\bar2x_2+\bar3x_3=\bar0\\ \bar2x_2+\bar4x_3=0\end{cases}$$

$\bar2x_2=-\bar4x_3 \Rightarrow x_2=-\overline{12}x_3 \Rightarrow x_2=\bar3x_3$

$x_1+\bar9x_3 \Rightarrow x_1=\overline{-9}x_3=\bar1x_3$

令 $x_3=\bar1$. V_A 的一组基 $\vec v=\begin{pmatrix}\bar1\\ \bar3\\ \bar1\end{pmatrix}$

$V_A=\{\lambda\vec v\mid\lambda\in\mathbb{Z}_5\}$ 共有五个不同的元素

例: 证明 $\left(\mathbb{Z}_2^3,+,\begin{pmatrix}\bar0\\ \bar0\\ \bar0\end{pmatrix}\right)$ 不可能有两个元素生成。设 $\mathbb{Z}_2^3$ 被两个元素 $\vec v_1,\vec v_2\in\mathbb{Z}_2^3$ 生成

则 $\mathbb{Z}_2^3$ 做为 $\mathbb{Z}_2$ 上线性空间也可由 $\vec v_1,\vec v_2$ 张成 于是 $\dim\mathbb{Z}_2^3\le2$ →←

例3. 回忆: $A\in M_n(F)$ 是斜对称的 即 $A^t=-A$. 证明奇数阶斜对称方阵行列式为零

证: $\det(A)=\det(A^t)=\det(-A)=(-1)^n\det(A)$

$(1+(-1)^n)\det(A)=0$ $(1+1)\det(A)=0$

当 $2\neq0$ 时 $\det(A)=0$

在 $\mathbb{Z}_2$ 中 $A=\begin{pmatrix}\bar0 & \bar1\\ \bar1 & \bar0\end{pmatrix}$ $A^t=\begin{pmatrix}\bar0 & \bar1\\ \bar1 & \bar0\end{pmatrix}=\begin{pmatrix}\bar0 & -\bar1\\ -\bar1 & \bar0\end{pmatrix}=-A$

但 $\det(A)\neq0$.

第5章 复数域和多项式

§2 一元多项式

$f(x)=2x^2-3x+1$

本节中 $(R,+,0,\cdot1)$ 为交换环.

§2.1 一元多项式环的构造

设 $\tilde{R}=\{(a_0,a_1,a_2,\cdots)\mid a_0,a_1,a_2\cdots\in R,\text{有限个非零}\}$

记号 设 $\tilde{a}\in\tilde{R}$. 记 $\tilde{a}_k$ 为 $\tilde{a}$ 中第 $k+1$ 个坐标

其中 $k=0,1,2\cdots$

特别地 $\tilde{0}=(0,0\cdots\cdots)$ 即 $\tilde{0}_k=0,\ k\in\mathbb{N}$

$\tilde{1}=(1,0\cdots\cdots)$ 即 $\tilde{1}_0=1,\ \tilde{1}_k=0\ k\in\mathbb{Z}^+$

于是 $\tilde{R}$ 中含有两个不同元素 $\tilde{0},\tilde{1}$

注: $\forall\ \tilde{a}\in\tilde{R},\ \exists\ l\in\mathbb{N}$ 使得

$$\tilde{a}_{l+1}=\tilde{a}_{l+2}=\cdots=0$$

$$+:\ \begin{aligned}\tilde{R}\times\tilde{R}&\longrightarrow\tilde{R}\\(\tilde{a},\tilde{b})&\longmapsto\tilde{c}\end{aligned}$$

其中 $\tilde{c}_k=\tilde{a}_k+\tilde{b}_k\quad k\in\mathbb{N}$. 记

$\tilde{c}=\tilde{a}+\tilde{b}$

良定义: 设 $N\in\mathbb{N}$ 使得

$$\tilde{a}_{N+1}=\tilde{a}_{N+2}=\cdots=0$$

$$\tilde{b}_{N+1}=\tilde{b}_{N+2}=\cdots=0$$

于是 $\tilde{c}_k=0\quad\forall\ k>N$

$\Rightarrow\ \tilde{c}\in\tilde{R}$

同为 $(R,+,0)$ 为交换群, 可以 $(\tilde{R},+,\tilde{0})$ 为交换群.

定义: $\cdot:\ \begin{aligned}\tilde{R}\times\tilde{R}&\longrightarrow\tilde{R}\\(\tilde{a},\tilde{b})&\longmapsto\tilde{c}\end{aligned}$

其中 $\tilde{c}_k=\sum_{i+j=k}\tilde{a}_i\tilde{b}_j\qquad i,j\in\mathbb{N}$

良定义: 设 N 如上. 设 $k>2N$

$$\tilde{c}_k=\sum_{i+j=k}\tilde{a}_i\tilde{b}_j$$

则 $i>N$ 或 $j>N\ \Rightarrow\ \tilde{a}_i\tilde{b}_j=0$

$\Rightarrow\ \tilde{c}_k=0\ \Rightarrow\ \tilde{c}\in\tilde{R}$

记 $\tilde{c}=\tilde{a}\tilde{b}$

结合律 设 $\tilde{a},\tilde{b},\tilde{c}\in\tilde{R}$

$\tilde{p}=\tilde{a}\tilde{b}$, $\tilde{q}=(\tilde{a}\tilde{b})\tilde{c}$

$\tilde{u}=\tilde{b}\tilde{c}$, $\tilde{v}=\tilde{a}(\tilde{b}\tilde{c})$

$$\tilde{q}_k = \sum_{i+j=k} \tilde{p}_i \tilde{c}_j = \sum_{i+j=k} \left(\sum_{s+t=i} \tilde{a}_s \tilde{b}_t \right) \tilde{c}_j$$

$$= \sum_{i+j=k} \sum_{s+t=i} \tilde{a}_s \tilde{b}_t \tilde{c}_j$$

$$= \sum_{s+t+j=k} \tilde{a}_s \tilde{b}_t \tilde{c}_j$$

$$\tilde{v}_k = \sum_{i+j=k} \tilde{a}_i \tilde{u}_j = \sum_{i+j=k} \tilde{a}_i \sum_{s+t=j} \tilde{b}_s \tilde{c}_t$$

$$= \sum_{i+j=k} \sum_{s+t=j} \tilde{a}_i \tilde{b}_s \tilde{c}_t = \sum_{i+s+t=k} \tilde{a}_i \tilde{b}_s \tilde{c}_t$$

$$\Rightarrow \tilde{q}_k = \tilde{v}_k \Rightarrow \tilde{a}(\tilde{b}\tilde{c}) = (\tilde{a}\tilde{b})\tilde{c}$$

交换律 $\tilde{a}\tilde{b} = \tilde{b}\tilde{a}$

设 $\tilde{p} = \tilde{a}\tilde{b}$, $\tilde{q} = \tilde{b}\tilde{a}$

$$\tilde{p}_k = \sum_{i+j=k} \tilde{a}_i \tilde{b}_j \qquad \tilde{q}_k = \sum_{i+j=k} \tilde{b}_i \tilde{a}_j$$

$$\Rightarrow \tilde{a}\tilde{b} = \tilde{b}\tilde{a}$$

验证 $\tilde{1}$ 是乘法单位

设 $\tilde{b} = \tilde{a}\tilde{1}$

$$\tilde{b}_k = \sum_{i+j=k} \tilde{a}_i \tilde{1}_j = \tilde{a}_k \Rightarrow \tilde{b} = \tilde{a}$$

$(\tilde{R}, \cdots, \tilde{1})$ 是交换幺含幺单环.

分配律

设 $\tilde{p} = \tilde{a}(\tilde{b} + \tilde{c})$, $\tilde{q} = \tilde{a}\tilde{b} + \tilde{a}\tilde{c}$.

$$\tilde{p}_k = \sum_{i+j=k} \tilde{a}_i (\tilde{b}_j + \tilde{c}_j) = \sum_{i+j=k} \tilde{a}_i \tilde{b}_j + \sum_{i+j=k} \tilde{a}_i \tilde{c}_j$$

$$= \tilde{q}_k.$$

由此得到

引理 2.1 $(\tilde{R}, +, \tilde{0}, \cdots \tilde{1})$ 是交换环.

引理 2.2. 在 $\tilde{R}$ 中含

$$x = (0, \overset{1}{\overset{\vee}{1}}, 0, 0 \cdots 0)$$

则 (i) $\forall n \in \mathbb{N}^+$ $x^n = (0, \cdots 0, \overset{n}{\overset{\vee}{1}}, 0 \cdots)$

(ii) $\forall r \in R$ $\tilde{r} \cdot x = (0 \cdots 0, \overset{n}{\overset{\vee}{r}}, 0 \cdots 0)$

其中 $\tilde{r} = (r, 0, 0 \cdots 0)$

证：(i) 对n归纳. $n=1$ ✓

设 $n-1$ 时结论成立. 当 n 时

$$x^n = x\,x^{n-1}$$

$$(x^n)_k = \sum_{i+j=k} (x)_i\,(x^{n-1})_j = \begin{cases} 0 & k\neq n \\ 1 & k=n \end{cases}$$

$$x^n = (0, 0\cdots0, \underset{\uparrow}{1}, 0\,0\cdots)$$
$$\qquad\qquad\quad n$$

(ii) $$(\tilde{r}\,x^n)_k = \sum_{i+j=k} \tilde{r}_i (x^n)_j = \begin{cases} 0, & k\neq n \\ r, & k=n \end{cases}$$

注：避免等号 $\forall r\in R$

记 $(r, 0\cdots0\cdots)$ 为 r

则 $$r\,x^n = (0\cdots0, \underset{\vdots}{r}, 0\cdots0)$$
$$\qquad\qquad\quad n$$

设

$$\tilde{a} = (a_0, a_1, \cdots a_k\cdots) \in \tilde{R} \text{ 且}$$

$$a_{N+1} = a_{N+2} = \cdots = 0$$

$$\tilde{a} = a_0 + a_1 x + \cdots + a_N x^N$$

于是 $$\tilde{R} = \left\{ a_0 + a_1 x + \cdots + a_N x^N \;\middle|\; N\in\mathbb{N}^+ \right\}$$
$$a_0, a_1 \cdots a_N \in R\}$$

且 R 可以看成 $\tilde{R}$ 的子集. 记 $x^0 = 1$

记 $\tilde{R} = R[x]$ 称之为 R 上的一元多项式环

引理2.2：设 $p\in R[x]$ 且 $p\neq 0$.

则 $\exists!\ p_0, p_1 \cdots p_d \in R$, $p_d \neq 0$ 使得

$$p = p_d x^d + p_{d-1} x^{d-1} + \cdots + p_0 \qquad (*)$$

证：设 $p = (p_0, p_1, \cdots)$

$\because p\neq 0 \quad \therefore \exists d\in\mathbb{N}$. 使得 $p_d \neq 0$. 但

$$p_{d+1} = p_{d+2} = \cdots = 0$$

于是 $$p = (p_0, p_1, \cdots p_d, 0, 0\cdots0)$$

$$= p_d x^d + p_{d-1} x^{d-1} + \cdots + p_0$$

因为 $R[x]$ 中两个元素相等当且仅当对应坐标都相等. 所以 $p_0, p_1 \cdots p_d$ 唯一

记号 称 x 是未定元. p 是关于 x 的多项式

p_i 是 p 中关于 x^i 的系数.

p_d 是 p 的首项系数, d 是 p 的次数

记 $p_d = lc(p)$, $d = \deg(p)$.

特别地 $\deg(0) = -\infty$.

命题 2.1 设 $f, g \in R[x]$

(i) $\deg(f+g) \leq \max(\deg(f), \deg(g))$

(ii) $\deg(fg) \leq \deg(f) + \deg(g)$.

证: 当 f 或 g 等于零时. 命题显然

设 f, g 都不为零

$$f = f_m x^m + f_{m-1} x^{m-1} + \cdots + f_0$$

$$g = g_n x^n + g_{n-1} x^{n-1} + \cdots + g_0.$$

其中 $f_i, g_j \in R$. $f_m \neq 0$. $g_n \neq 0$

不妨设 $m \geq n$.

(i) $g = g_m x^m + \cdots + g_{n+1} x^{n+1} + g_n x^n + \cdots + g_0$

其中 $g_m = \cdots = g_{n+1} = 0$

$$f+g = \sum_{k=0}^{m} (f_k + g_k) x^k \Rightarrow \deg(f+g) \leq m$$

(ii) $fg = g_n f x^n + \cdots + g_1 f x + g_0 f$

$$= g_n (f_m x^{m+n} + f_{m-1} x^{m+n-1} + \cdots + f_0 x^n)$$
$$+ g_{n-1} (f_m x^{m+n-1} + \cdots + f_0 x^{n-1})$$
$$+ g_0 (f_m x^m + \cdots + f_0)$$

$$= g_n f_m x^{m+n} + (g_n f_{m-1} + g_{n-1} f_m) x^{m+n-1} + \cdots + f_0 g_0$$

$\deg(fg) \leq m+n$ □

注: 由公式

(*): $fg = g_n f_m x^{m+n}$ + 次数比 x^{m+n} 低次项

可得: 当 $f_m g_n \neq 0$ 时

$$\deg(fg) = \deg(f) + \deg(g)$$

命题 2.2. 设 $f, g \in R[x]$. $f \neq 0$. $g \neq 0$

如果 $lc(f)\, lc(g)$ 中有一个是非零因子

则 $\deg(fg) = \deg(f) + \deg(g)$.

例: 设 $f = \bar{2}x^2 - \bar{2}$, $g = \bar{2}x^2 + \bar{2}$,

$h = \bar{3}x$. 是 $\mathbb{Z}_4[x]$ 中的多项式

求 fg fh

解 $fg = \bar{2}(x^2-\bar{1})\,\bar{2}(x^2+\bar{1}) = \bar{4}(x^2-\bar{1})(x^2+\bar{1}) = \bar{0}$

$fh = \bar{2}(x^2-\bar{1})\,\bar{3}x = \bar{6}(x^3-x) = \bar{2}x^3 - \bar{2}x$