## §3. 环 (Ring)

### §3.1. 环的定义

回忆: $(R, +, 0, \cdot, 1)$

(i) $(R, +, 0)$ 是交换群

(ii) $(R, \cdot, 1)$ 是含么半群

(iii) $\forall\, a, b, c \in R$

$a(b+c) = ab + ac$ (左分配律)

$(b+c)a = ba + ca$ (右分配律)

注: 书中环的定义(ii)只要求 $(R, \cdot)$ 是半群. 为简单起见, 我们只讲带有乘法单位元1的环.

注: $(R, \cdot, 1)$ 如果是交换的含么半群, 则称 $R$ 是交换环, 否则称 $R$ 是非交换环.

例: $(\mathbb{Z}, +, 0, \cdot, 1)$ 交换环 ①

$(\mathbb{R}, +, 0, \cdot, 1)$ 〃

$(\mathbb{Z}_n, +, \bar{0}, \cdot, \bar{1})$ 交换环

$(\mathbb{Z}, \cdot, \bar{1})$ $\bar{a}(\bar{b}\bar{c}) = \bar{a}\,\overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab}\cdot\bar{c}$ 结合律

$\bar{a}\cdot\bar{1} = \overline{a\cdot 1} = \bar{a}\cdot\bar{1}$ $\overline{a(b+c)} = \overline{a(b+c)\cdot 1} = \bar{a}\bar{b} + \bar{a}\bar{c}$

例: $(M_n, +, O_{n\times n}, \cdot, E_n)$ 非交换环.

例: 设 $R$ 是环.

(i) $\forall\, r \in R$ $r\cdot 0 = 0\cdot r = 0$

$r\cdot 0 = r(0+0) = r\cdot 0 + r\cdot 0$

($0$ 是加法单位) (分配律)

$r\cdot 0 = 0$ (加法群的消去律)

(ii) 设 $-1$ 是 $1$ 的加法逆元

则 $(-1)\cdot r$ 是 $r$ 的加法逆元

$1 + (-1) = 0$

$[1 + (-1)]\, r = 0\cdot r = 0$

$r + (-1)\, r = 0$

$\Rightarrow$ $(-1)r$ 是 $r$ 的加法逆元

记为 $(-1)r = -r$

同理 $r(-1) = -r$

即 $\forall r \in R$. $(-1)r = (-1)r = -r$.

特别地 $(-1)(-1)$ 是 $(-1)$ 的逆元

于是 $(-1)(-1) = 1$ [负负得正]

(iii) $a, b \in R$ 我们有 $ab = (-a)(-b)$

$(-a)(-b) = (-1)a(-1)b = (-1)(-1)ab$

$= 1 \cdot ab = ab$.

定理3.1. 广义分配已律.

设 R 是环, $a_1, \cdots a_m, b_1, \cdots b_n \in R$

则 $(a_1 + \cdots + a_m)(b_1 + \cdots + b_n)$

$= \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j = \sum_{j=1}^{m} \sum_{i=1}^{m} a_i b_j$

证: 我们证:

$(a_1 + \cdots + a_m)(b_1 + \cdots + b_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j$

对 n 归纳.



$n=1$

$(a_1 + \cdots + a_m) b_1$

$= (a_1 + (a_2 + \cdots + a_m)) b_1$

$= a_1 b_1 + (a_2 + \cdots + a_m) b_1$. 对 m 归纳得

$= a_1 b_1 + \cdots + a_m b_m = \sum_{i=1}^{m} a_i b_1$

$= \sum_{i=1}^{m} \sum_{j=1}^{1} a_i b_1$

设 $n-1$ 时定理成立.

$(a_1 + \cdots + a_m)(b_1 + \cdots + b_n)$

$= (a_1 + \cdots + a_m)((b_1 + \cdots + b_{n-1}) + b_n)$

$= (a_1 + \cdots + a_m)(b_1 + \cdots + b_{n-1}) + (a_1 + \cdots + a_m) b_n$

$= \sum_{i=1}^{m} \sum_{j=1}^{n-1} a_i b_j + \sum_{i=1}^{m} a_i b_n$

(归纳假设 $(n=1)$

$= \sum_{i=1}^{m} \left[ \left( \sum_{j=1}^{n-1} a_i b_j \right) + a_i b_n \right] = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j$

图

注: $ma = \underbrace{a + \cdots + a}_{m} = \underbrace{(1 + \cdots + 1)}_{m} a$

方幂 仍有 $(ma)(nb) = (mn)(ab)$

注 如果R是交换环. 则

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

$$(a+b)(a-b) = a^2 - b^2 \quad \cdots$$

## §3.2 零因子和可逆元

定义: 设R是环. 如果 $l, r \in R\setminus\{0\}$

如果 $lr = 0$. 则称

$l$ 是R中的左零因子 (非零)

$r$ 是R中的右零因子 (非零)

如果 R交换. 则左、右零因子统称为零因子

注 0 称为平凡的零因子.

例: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ 中没有非平凡零因子

例 $\mathbb{Z}_{12}$ 中 $\bar{3}\cdot\bar{4} = \bar{12}$.

$\bar{3}, \bar{4}$ 是非平凡零因子.

例: 在 $M_n$ 中任何非满秩矩阵 (3)

都是 $M_n$ 中的左零因子, 也是右零因子

设 $A \in M_n$ $\operatorname{rank}(A) < n$.

则 $AX = \vec{0}_n$ 有非平凡解 $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$

设 $B = \begin{pmatrix} \alpha_1 & \cdots & 0 \\ \vdots & & \vdots \\ \alpha_n & \cdots & 0 \end{pmatrix}_{n\times n}$.

则 $AB = 0 \Rightarrow$ $A$ 是左零因子

$B^tA^t = 0 \Rightarrow$ $A^t$ 是右零因子.

定义: 设R是环. $a, b \in R$

如果 存在 $b \in R$ 使得

$$ab = ba = 1$$

则称 $a$ 是可逆元. $b$ 是 $a$ 的逆

由于群中逆的唯一性可知

$b$ 可记作 $a^{-1}$.

例：$(\mathbb{Z}, +, 0, \cdot)$ $\mathbb{Z}$中可逆元是$\pm 1$

$\mathbb{R}$中可逆元是所有非零实数

$M_n$中可逆元是可逆矩阵

命题3.1. 设 $n>1$，在 $\mathbb{Z}_n$ 中，$\bar{m} \in \mathbb{Z}_n$，$\bar{m} \neq \bar{0}$

(i) $\bar{m}$是零因子 $\Leftrightarrow$ $\gcd(m,n)>1$

(ii) $\bar{m}$是可逆元 $\Leftrightarrow$ $\gcd(m,n)=1$

证：设 $g=\gcd(m,n)$，则 $\exists u,v \in \mathbb{Z}$（$s,t$）

(*) $um+vn=g$ 且 (**) $m=sg$，$n=tg$

(i) "$\Rightarrow$" 若$\bar{m}$是零因子，则 $\exists w \in \{0,1,\cdots m-1\}$

使得 $\bar{m}\bar{w}=\bar{0}$

由 (*) $uwm+vwn=wg$

$\Rightarrow$ $\bar{u}\bar{w}\bar{m}+\bar{v}\bar{w}\bar{n}=\bar{w}\bar{g}$

$\Rightarrow$ $\bar{w}\bar{g}=\bar{0}$

$\because \bar{m} \neq \bar{0} \Rightarrow \bar{g} \neq \bar{0}$

$\Rightarrow m \mid wg$

$\because 0<w<n \quad \therefore g>1$



"$\Leftarrow$" $g>1 \Rightarrow t \in \{0,1,\cdots m-1\} \Rightarrow \bar{t} \neq \bar{0}$

$\bar{t}\bar{g}=\bar{0}$

$\bar{t}\bar{m}=\bar{t}\bar{s}\bar{g}=\bar{s}\bar{t}\bar{g}=\bar{0}$.

$\Rightarrow \bar{m}$是零因子

(ii). 设 $\bar{m}$可逆：

$\exists w \in \mathbb{Z}$ 使得

$\bar{m}\bar{w}=\bar{1}$

若 $\gcd(m,n)>1$，则 $\exists x \in \mathbb{Z}$，$\bar{x} \neq \bar{0}$

使得 $\bar{m}\cdot\bar{x}=\bar{0}$

$\bar{w}\cdot\bar{m}\cdot\bar{x}=\bar{w}\cdot\bar{0}=\bar{0}$

$\bar{x}=\bar{0}$ $\rightarrow\leftarrow$

设 $\gcd(m,n)=1$，则

由 (*) $um+vn=1$

$\bar{u}\bar{m}+\bar{v}\bar{n}=\bar{1}$

$\bar{u}\bar{m}=\bar{1}$ ∎

推论3.1 设 $p$ 是素数. 则环 $\mathbb{Z}_p$ 中任何非零元都可逆.

定理3.1 设 $R$ 是环. $U$ 是 $R$ 中所有可逆元的集合. 则 $(U,\cdot,1)$ 是群.

证: 设 $a,b\in U$

$(ab)(b^{-1}a^{-1})=(b^{-1}a^{-1})(ab)=1$

$\Rightarrow ab\in U$

$1\in U$. $\forall a\in U$, $a^{-1}\in U$.

($\because a^{-1}$ 的逆是 $a$) 于是 $U$ 是群.

定义: 设 $R$ 是环且 $R$ 中既无左零因子, 又无右零因子. 则称 $R$ 是整环.

定理3.2. 设 $R$ 是整环. $a,b,c\in R$ 且 $a\neq 0$. 如果 $ab=ac$ 或 $ba=ca$ 则 $b=c$.

证: 设 $ba=ca$

$ba-ca=0$

$(b-c)a=0$

$\because a$ 不是左零因子. $\therefore b-c=0$

同理可证右消去律.

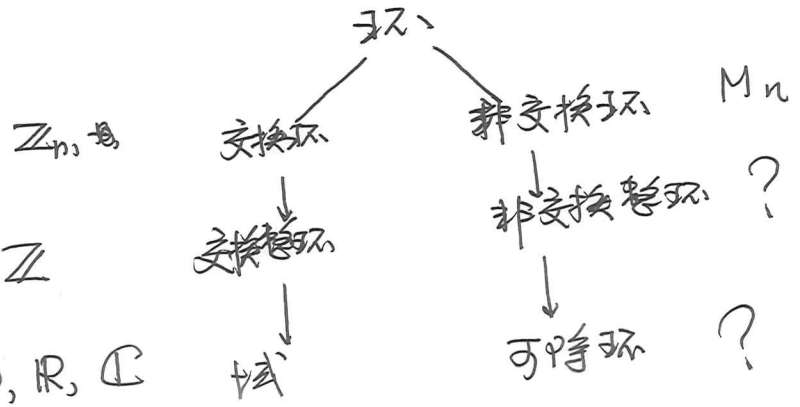
定义: 设 $R$ 是环. 如果 $R$ 中任何非零元素都可逆. 则称 $R$ 是可除环.

交换的可除环称之为域.

例: $\mathbb{Z}$ 是整环

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ 是域.

可除环. (非交换) Hamilton 四元素环.



## §3.3. 环同态：

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

$\forall a,b\in R$

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

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

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

则称 $\varphi$ 是从 $R$ 到 $S$ 的同态

如果 $\varphi$ 是单的，则称 $\varphi$ 是单同态

…… 满的 …… $\varphi$ 是满的……

…… 双射 …… $\varphi$ 是同构。

例：$\pi: \mathbb{Z}\to\mathbb{Z}_n$ 是环同态

$\forall m,n\in\mathbb{Z}$

$$\pi(m+n)=\overline{m+n}=\bar{m}+\bar{n}$$

$$\pi(mn)=\overline{mn}=\bar{m}\cdot\bar{n}$$

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

□

命题3.1

证：设 $\varphi: R\to S$ 是环同态

则 $\varphi$ 是单的 $\Leftrightarrow \forall r\in R$，$\varphi(r)=0_S\Rightarrow r=0_R$

"$\Rightarrow$"：∵ $\varphi$ 是 $(R,+,0_R)$ 到 $(S,+,0_S)$ 的群同态，∴ $\varphi(0_R)=\varphi(0_S)$

∵ $\varphi$ 是单的，∴ $\varphi(r)=0_S\Rightarrow r=0_R$

"$\Leftarrow$"：设 $a,b\in R$，$\varphi(a)=\varphi(b)$

$\Rightarrow \varphi(a)-\varphi(b)=0_S\Rightarrow \varphi(a-b)=0_S$

$\Rightarrow a-b=0_R\Rightarrow a=b.$ □

例：设 $\varphi: R\to S$ 是环同态。

设 $m_1,\dots,m_k\in\mathbb{Z}^+\setminus\{1\}$，两两互素

$\pi_{m_i}$ 是由 $\mathbb{Z}$ 到 $\mathbb{Z}_{m_i}$ 的自然投射

记 $\bar{a}_i\in\mathbb{Z}_{m_i}$，$i=1,\dots,k$

$\exists\, a\in\mathbb{Z}$ 使得

$$\pi_{m_i}(a)=\bar{a}_i,\quad i=1,\dots,k.$$

## §4 域

回忆：$F$ 是域 如果它是交换环且任何非零元可逆

注：域必是整环，（见定理3.1）

例：$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$. （见推论3.1）

例：设 $d \in \mathbb{Q}^+$ 且 $\sqrt{d}$ 是无理数

令 $\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} \mid a, b \in \mathbb{Q}\}$

则 $\mathbb{Q}(\sqrt{d})$ 是域

第一步验证：$(\mathbb{Q}(\sqrt{d}), +, 0)$ 是交换群

设 $x = a+b\sqrt{d}$, $y = u+v\sqrt{d}$, 其 $a, b, u, v \in \mathbb{Q}$

$x - y = (a-u) + (b-v)\sqrt{d} \in \mathbb{Q}(\sqrt{d})$

$\Rightarrow (\mathbb{Q}(\sqrt{d}); +, 0)$ 是 $(\mathbb{R}, +, 0)$ 的子群

$\Rightarrow (\mathbb{Q}\sqrt{d}, +, 0)$ 是交换群

第二步验证：$(\mathbb{Q}(\sqrt{d}), \cdot, 1)$ 是交换幺半群.

只要验证"$\cdot$"封闭性

$$xy = (a+b\sqrt{d})(u+v\sqrt{d}) = (au+bvd) + (av+bu)\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

第三步. 分配律显然.

于是 $\mathbb{Q}(\sqrt{d})$ 是交换环.

第四步 设 $x = a+b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ 且 $x \neq 0$,

只要证：$x$ 可逆.

~~$x \neq 0 \Rightarrow a, b$ 不全~~ 令 $y = \dfrac{a-b\sqrt{d}}{a^2-b^2d}$

（注意到 $\because \sqrt{d}$ 是无理数 $\therefore a^2-b^2d \neq 0$

$$xy = \frac{a^2-b^2d}{a^2-b^2d} = 1.$$

于是 $\mathbb{Q}(\sqrt{d})$ 是域

### §4.1. 域的特征

引理4.1 设 $F$ 是域. 如果在 $(F, +, 0)$ 中 1 的阶有限. 则

$\mathrm{ord}(1)$ 是素数

证：设 $k = \mathrm{ord}(1)$ 则 $k > 1$.

假设 $k$ 不是素数. 则 $\exists\, l, m \in \mathbb{Z}^+ \setminus \{1\}$

使得 $k = lm$

于是 $1 < l < k$. $1 < m < k$

$k\cdot 1 = \underbrace{1+\cdots+1}_{k} = 0 \Rightarrow k\cdot 1 = 0$

$\Rightarrow ml\cdot 1 = 0 \Rightarrow (ml)(1\cdot 1) = 0$

$\Rightarrow (m\cdot 1)(l\cdot 1) = 0 \Rightarrow m\cdot 1 = 0$ 或 $l\cdot 1 = 0$

成立规律

$\underbrace{1+\cdots+1}_{m} = 0$ 或 $\underbrace{1+\cdots+1}_{l} = 0$

$\Rightarrow \operatorname{ord}(1) < k$ →←

定义：设 $F$ 是域，如果 $1$ 在群 $(F,+,0)$ 的阶是无穷，则称 $F$ 是零特征域。

如果 $1$ 在该群中的阶数阶是 $P$ 则称 $F$ 的特征是 $P$。记 $F$ 的特征为 $\operatorname{char}(F)$。

引理 4.2 设 $F$ 是域，如果存在 $m\in\mathbb{Z}^+$ 使得 $\underbrace{1+\cdots+1}_{m} = 0$

则 $m$ 必为素数。

证明：

例：$\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = 0$，$\operatorname{char}(\mathbb{Z}_p) = p$ ($p$ 为素数)



引理 4.2 设域 $F$ 的特征为 $p>0$.

则 $\underbrace{1+1+\cdots+1}_{m} = 0 \Leftrightarrow p\mid m$.

证：设 $m = sp+r$，$r\in\{0,1,\cdots p-1\}$

$\underbrace{1+\cdots+1}_{m} = 0 \Leftrightarrow m\cdot 1 = 0$

$\Leftrightarrow (sp+r)\cdot 1 = 0$

$\Leftrightarrow sp\cdot 1 + r\cdot 1 = 0$

$\Leftrightarrow \underbrace{p\cdot 1+\cdots+p\cdot 1}_{s} + r\cdot 1 = 0$

$\Leftrightarrow r\cdot 0 = 0 \Leftrightarrow r = 0$

($\because p\cdot 1 = 0$). ∎

注：若 $p\mid m$，则 $\forall a\in F$ $ma = 0$

命题 4.1 (Frenshmen's dream)

设域 $F$ 的特征是 $P$

则 $(a+b)^P = a^P + b^P$.

证：$(a+b)^P = a^P + \underbrace{\cdots}_{P-1} + b^P = \sum_{i=0}^{P}\binom{P}{i}a^{P-i}b^i$

当 $i\in\{1,2,\cdots P-1\}$

$\binom{P}{i} = \frac{P!}{i!(P-i)!}\in\mathbb{Z}$ gcd

$\because \gcd(p,k)=1, \quad k=1,2,\cdots p-1$

$\therefore \gcd(p,i!)=1, \ \gcd(p,(p-i)!)=1, \quad i=1,2,\cdots p-1$

$\therefore \quad p \mid \binom{p}{i}$

由引理4.2 $\binom{p}{i}a^{p-i}b^i = (1+\cdots+1)\underbrace{\binom{p}{i}}a^{p-i}b^i$

$=0$

$\Rightarrow (a+b)^p = a^p+b^p$. ☐

例: $a+b \in \mathbb{Z}_2$

$(a+b)^2 = a^2+2ab+b^2$

$= a^2+\bar{2}ab+b^2$

$= a^2+b^2$

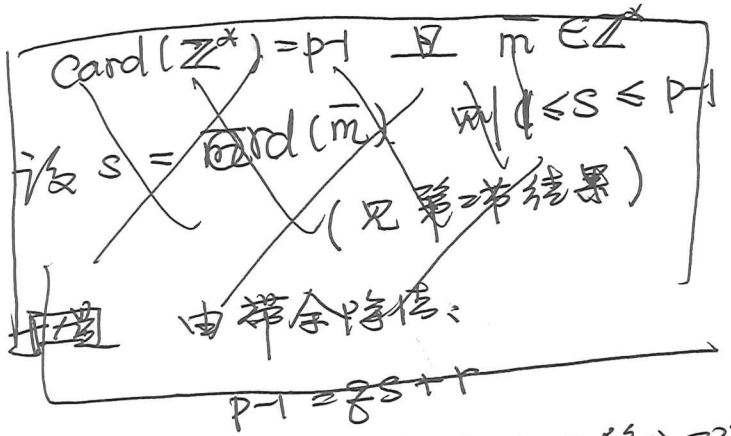
命题4.2 (Format Little Theorem)

设 $m\in\mathbb{Z}^+$, 则 $m^{p-1}\equiv 1 \mod p$

($p$是素数且$p\nmid m$)

证: 在 $\mathbb{Z}_p^*$ 中 $(\mathbb{Z}_p^*\cdots\bar{1})$是群

(定理3.1) 且 $\bar{m}\in\mathbb{Z}_p^*$




于是 $\mathbb{Z}_p^* = \bar{m}\mathbb{Z}_p^*$ (左平移为双射)

即 $\{\bar{1},\bar{2},\cdots\overline{p-1}\} = \{\bar{m},\bar{2}\bar{m},\cdots\overline{p-1}\,\bar{m}\}$

$\bar{1}\cdot\bar{2}\cdots\overline{p-1} = \bar{m}(\bar{2}\bar{m})\cdots(\overline{p-1})\bar{m}$

$= \bar{m}^{p-1}(\bar{1}\cdot\bar{2}\cdots\overline{p-1})$

$\bar{m}^{p-1} = \bar{1}$ in $\mathbb{Z}_p$

则 $m^{p-1}\equiv 1 \mod p$ ☐

## §4.2. 域同态

定义: 设 $E$, $F$ 是域, $\varphi: E\to F$ 是环同态

则称 $\varphi$ 是域同态

命题4.3 设 $E, F$ 是域，$\varphi: E \to F$ 是域同态，则 $\varphi$ 是单射。

证：由命题3.1，只需证明

$\forall a \in E$ $\varphi(a) = 0_F \Rightarrow a \in 0_E$

若 $a \neq 0$ $\varphi(a)\varphi(a^{-1}) = 0_F$

$\varphi(a \cdot a^{-1}) = \varphi(1_E) = 1_F$

$\Rightarrow 0_F = 1_F$ $\to\leftarrow$

$\Rightarrow a = 0$ □

例：设域 $E, F$ 的特征不同，则 $E, F$ 之间没有域同态。

证：设 $\mathrm{char}(E) = p$，$\mathrm{char}(F) = q$，$p \neq q$。假设 $\varphi: E \to F$ 是域同态

$$0_F = \varphi(0_E) = \varphi(\underbrace{1_E + \cdots + 1_E}_{p})$$

$$= \underbrace{\varphi(1_E) + \cdots + \varphi(1_E)}_{p}$$

$$= \underbrace{1_F + \cdots + 1_F}_{p}$$

由引理4.2 $q \mid p$

同为素，$p$ 是素数 $q = p$ $\to\leftarrow$ 易



## §5 域上的线性代数

断言1 第二章，第三章中所有结论对任何域都成立。$p$ 多了那些以 $2 \neq 0$ 而

用了 $2 \neq 0$ 而。

设 $F$ 是域，$M_n(F)$ 代表域 $F$ 上的 $n$ 阶矩阵。设 $A \in M_n$

$n$ 是 $A$ 中有两行或两列相同

则 $\det(A) = 0$

以前的证明（两列相同的情形）换 $\vec{A}^{(i)} = \vec{A}^{(j)}$ $(i \neq j)$

$$\det(A) = \det(\vec{A}^{(1)}, \cdots \vec{A}^{(i)} \cdots \vec{A}^{(j)} \cdots \vec{A}^{(n)})$$

$$= -\det(\vec{A}^{(1)}, \cdots \vec{A}^{(j)}, \cdots \vec{A}^{(i)} \cdots \vec{A}^{(n)})$$

$$= -\det(A)$$

$\Rightarrow \det(A) + \det(A) = 0$

[ 在 $\mathbb{Z}_2$ 中 $\det(A) + \det(A) = 0$ $\Rightarrow \det(A) = 0$ ]

$\det\begin{pmatrix}\bar{1}&\bar{0}\\ \bar{0}&\bar{1}\end{pmatrix}=\bar{1}$ $\det(\vec{A})+\det(A)=\bar{1}+\bar{1}=\bar{0}$

$A$ 模 $\det(A)=\bar{1}$.

新的矩阵：设

$A=(a_{ij})_{n\times n}$. $a_{ij}\in F$

$$\det(A)=\sum_{\sigma\in S_n}\varepsilon_\sigma a_{\sigma(1),1}\cdots a_{\sigma(n),n}$$

设 $t_\sigma=\varepsilon_\sigma a_{\sigma(1),1}\cdots a_{\sigma(i),i}\cdots a_{\sigma(j),j}\cdots a_{\sigma(n),n}$

$\tau=(ij)$

$t_{\sigma\tau}=\varepsilon_{\sigma\tau}a_{\sigma\tau(1),1}\cdots a_{\sigma\tau(i),i}\cdots a_{\sigma\tau(j),j}\cdots a_{\sigma\tau(n),n}$

$=-\varepsilon_\sigma a_{\sigma(1),1}\cdots a_{\sigma(j),i}\cdots a_{\sigma(i),j}\cdots a_{\sigma(n),n}$

$=-\varepsilon_\sigma a_{\sigma(1),1}\cdots a_{\sigma(j),j}\cdots a_{\sigma(i),i}\cdots a_{\sigma(n),n}$

(∵ $\vec{A}^{(i)}=\vec{A}^{(j)}$)

$=-t_\sigma$

$S_n=A_n\cup\tau A_n$ 且 $A_n\cap\tau A_n=\emptyset$

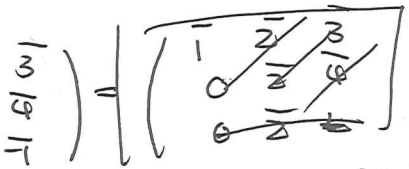
$$\det(A)=\sum_{\sigma\in A_n}t_\sigma+\sum_{\sigma\in A_n}t_{\sigma\tau}=\sum_{\sigma\in A_n}(t_\sigma-t_\sigma)=0$$

□

例：设 $A=\begin{pmatrix}\bar{1}&\bar{2}&\bar{3}\\ \bar{0}&\bar{2}&\bar{4}\\ \bar{1}&\bar{4}&\bar{2}\end{pmatrix}$ 是 $\mathbb{Z}_5$ 上的矩阵 (11)

计算 $A\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=\begin{pmatrix}\bar{0}\\\bar{0}\\\bar{0}\end{pmatrix}$ 的解空间 $V_A$

的一组基.

$A\xrightarrow{\text{行变换}}\begin{pmatrix}\bar{1}&\bar{2}&\bar{3}\\ \bar{0}&\bar{2}&\bar{4}\\ \bar{0}&\bar{2}&\bar{1}\end{pmatrix}$ 

$\xrightarrow{\text{行变换}}\begin{pmatrix}\bar{1}&\bar{2}&\bar{3}\\ \bar{0}&\bar{2}&\bar{4}\\ \bar{0}&\bar{0}&\bar{0}\end{pmatrix}$

$\xrightarrow{\text{行变换}}\begin{pmatrix}\bar{1}&\bar{2}&\bar{3}\\ \bar{0}&\bar{2}&\bar{4}\\ 0&0&\bar{5}\end{pmatrix}=\begin{pmatrix}\bar{1}&\bar{2}&\bar{3}\\ \bar{0}&\bar{2}&\bar{4}\\ \bar{0}&\bar{0}&\bar{0}\end{pmatrix}$

$\longrightarrow\begin{pmatrix}\bar{1}&\bar{2}&\bar{3}\\ \bar{0}&\bar{1}&\bar{2}\\ \bar{0}&\bar{0}&\bar{0}\end{pmatrix}$ $\operatorname{rank}(A)=2$

$\dim V_A=1$

$x_2+\bar{2}x_3=0\Rightarrow x_2=\bar{-2}x_3=\bar{3}x_3$

$\Rightarrow x_1+\bar{2}(\bar{3}x_3)+\bar{3}x_3=0$

$\Rightarrow x_1=x_3$

于是 $\begin{pmatrix}\bar{1}\\\bar{3}\\\bar{1}\end{pmatrix}\neq A\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=\begin{pmatrix}\bar{0}\\\bar{0}\\\bar{0}\end{pmatrix}$ 非零解

即 $V_A=\left\langle\begin{pmatrix}\bar{1}\\\bar{3}\\\bar{1}\end{pmatrix}\right\rangle$.

注 $\operatorname{card}(V_A)=5$ 但 $\dim V_A=1$

# 第五章 多项式与复数

## §2. 一元多项式

$x-1$, $x^2+2x+1$, $3x^7-3x+1$

以什么数作为 $x$ 是什么?

### §2.1 一元多项式的定义

$$p(x)=p_d x^d+p_{d-1}x^{d-1}+\cdots+p_0, \quad p_i\in\mathbb{R}$$

设 $R$ 是交换环. 令

$$\widetilde{R}=\{(a_0,a_1,\cdots,a_k,\cdots) \mid a_k\in R,\ k=0,1,\cdots \text{ 且这些项中只有有限项非零}\}$$

设 $a=(a_0,a_1,\cdots,a_k,\cdots)$

$N\in\mathbb{N}$, 使得 $a_{N+1}=a_{N+2}=\cdots=0$

"$a=a_0+a_1x+\cdots+a_Nx^N$"

同理 "$b=b_0+b_1x+\cdots+b_Nx^N$"

"$a+b=a_0+b_0+(a_1+b_1)x+\cdots+(a_N+b_N)x^N+\cdots$"

设 $b=(b_0,b_1,\cdots b_k,\cdots)\in\widetilde{R}$

定义: $a+b=(a_0+b_0,\ a_1+b_1,\cdots a_k+b_k,\cdots)$ (12)

则 $a+b\in\widetilde{R}$

显然 $+:\widetilde{R}\times\widetilde{R}\to\widetilde{R}$ 是二元运算

令 $0=(0,0,\cdots,\cdots)$

则 $(\widetilde{R},+,0)$ 是加法交换群.

"$a=a_0+a_1x+\cdots+a_Nx^N$"

"$b=b_0+b_1x+\cdots+b_Nx^N$"

$a-b$ 中 $x^k$ 的系数为

$$\sum_{i=0}^{k}a_ib_{k-i}=\sum_{\substack{i+j=k\\ i,j\in\mathbb{N}}}a_ib_j$$

设定义: 设 $a=(a_0,a_1,\cdots)$

$b=(b_0,b_1,\cdots)$

$a*b=(c_0,c_1,\cdots,c_k,\cdots)$

$$c_k=\sum_{i+j=k}a_ib_j.$$

注 对 $c_k$ 存在 $N\in\mathbb{N}$. 使得 $a_{N+1}=a_{N+2}=\cdots=0$

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

于是 当 $l > 2N$ 时

$$c_l = \sum_{i+j=l} a_i b_j = 0$$

即: $c = (c_0, c_1, \cdots c_k \cdots) \in \widetilde{R}$

可直接验证: $(\widetilde{R}, +, \cdot, \mathbb{1})$ 是含幺交换环.

其 $\mathbb{1} = (1, 0, 0 \cdots)$

同样分配律成立. 于是

$(\widetilde{R}, +, \mathbb{0}, \cdot, \mathbb{1})$ 是子交换环.

记 $x = (0, 1, 0 \cdots)$

则 $x^2 = (0, 1, 0 \cdots)(0, 1, 0 \cdots)$

$= (0, 0, 1, 0 \cdots)$

归纳 $\forall i \in \mathbb{N}$

$x^i = (0 \cdots 0\ 1\ 0 \cdots)$

$\uparrow$ 第 $i+1$ 位 (从零开始记数)

此 $i=0$ ✓

设 $i-1$ 时归纳成立

则 $x \cdot x^{i-1} = (0, 1, 0 \cdots)(0 \cdots 0\ 1\ 0 \cdots)$

$\uparrow$ 第 $i$ 位 (从零开始)

$= (0 \cdots 0\ 1\ 0 \cdots) = x^i$ 归



记号约定.

设 $a = (a_0, a_1, \cdots a_N, 0, 0 \cdots) \in \widetilde{R}$

记 $a = a_0 + a_1 x + \cdots + a_N x^N$

$\mathbb{1}$ 记为 1. $\mathbb{0}$ 记为 0

从而记 $\widetilde{R}$ 为 $R[x]$

于是 $R[x] = \left\{ \sum_{i=0}^{N} a_i x^i \;\middle|\; a_i \in R \right\} = \widetilde{R}$

定理 2.1 $(R[x], +, 0, \cdot, 1)$ 是交换环.

称 $x$ 是未定元 (indeterminate), $R[x]$ 为 $R$ 上的一元多项式环。

~~命题 2.1~~ 设 $f = f_d x^d + f_{d-1} x^{d-1} + \cdots f_0 \in R[x]$

~~命题 2.1~~ 设 $f = 0$, 则 $f_d = f_{d-1} = \cdots = f_0 = 0$

证: $f = (f_0, f_1 \cdots f_d \cdots 0 \cdots) = (0, 0 \cdots 0 \cdots)$

$\Rightarrow f_0 = f_1 = \cdots f_d = \cdots = 0$