第十七周习题课: 域上的线性代数, 一元多项式环

郑晓鹏

中国科学院数学与系统科学研究院

目录

实数域 $\mathbb{R}$ 上有但一般域不一定有的性质:

(1) 任意非零整数 n, 有 $n \neq 0$. 所以, 在实数域中, $A = -2A$ 可以推出 $A = 0$, 但特征 3 的域不可以.

$3 \neq 0$ $\quad 2 \neq 0$

$A = -A$, $\mathrm{char} \neq 2$ $\Rightarrow A = 0$

n $\quad n \neq 0$

$A = -2A$

$\Rightarrow 3A = 0 \Rightarrow A = 0$

$A = -2A$

$3A = 0$ $\quad \mathrm{char} = 3$

$\not\Rightarrow A = 0$

$\mathrm{char} = 3$

$3 = 3 \cdot 1_F$

$= 0$

实数域 $\mathbb{R}$ 上有但一般域不一定有的性质:

(1) 任意非零整数 n, 有 $n \neq 0$. 所以, 在实数域中, $A = -2A$ 可以推出 $A = 0$, 但特征 3 的域不可以.

(2) $a^2 + b^2 = 0$ 可以推出 $a = b = 0$. 其他域不一定, 比如复数域 $\mathbb{C}$ 中, $1^2 + i^2 = 0$.

实数域 $\mathbb{R}$ 上有但一般域不一定有的性质:

(1) 任意非零整数 n, 有 $n \neq 0$. 所以, 在实数域中, $A = -2A$ 可以推出 $A = 0$, 但特征 3 的域不可以.

(2) $a^2 + b^2 = 0$ 可以推出 $a = b = 0$. 其他域不一定, 比如复数域 $\mathbb{C}$ 中, $1^2 + i^2 = 0$.

(3) 实数中任意两个数可以比较大小, 实数域可以考虑连续性, 其他域中不一定. (一般域上摄动法的证明和实数域不一样(李老师课上讲过))

实数域 $\mathbb{R}$ 上有但一般域不一定有的性质:

(1) 任意非零整数 n, 有 $n \neq 0$. 所以, 在实数域中, $A = -2A$ 可以推出 $A = 0$, 但特征 3 的域不可以.

(2) $a^2 + b^2 = 0$ 可以推出 $a = b = 0$. 其他域不一定, 比如复数域 $\mathbb{C}$ 中, $1^2 + i^2 = 0$.

(3) 实数中任意两个数可以比较大小, 实数域可以考虑连续性, 其他域中不一定. (一般域上摄动法的证明和实数域不一样(李老师课上讲过))

除了奇数阶斜对称矩阵行列式等于零以外, 关于线性方程组、矩阵、线性空间、向量、线性映射和行列式的所有结果适用于所有的域上的任何方阵.

解一般域上的线性方程组

$$V_A = \left\{ \lambda \begin{pmatrix} \bar{2} \\ \bar{2} \\ \bar{1} \end{pmatrix} : \lambda \in \mathbb{Z}_3 \right\}$$

$\mathrm{card}(V_A) = 3$

习题1. 设

$$A = \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{1} & \bar{1} & \bar{2} \end{pmatrix} \in \mathrm{M}_3(\mathbb{Z}_3).$$

计算以 A 为系数矩阵的齐次线性方程组的解空间 V_A 的一组基, 并计算 V_A 中的非零向量的个数.

解: $A = \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{1} & \bar{1} & \bar{2} \end{pmatrix} \longrightarrow \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{0} & \bar{2} & \bar{2} \end{pmatrix} \longrightarrow \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix}$

$-\bar{1} = \bar{2}$

所以原方程等价于

$$\begin{cases} x_1 + \bar{2}x_2 = \bar{0} \\ x_2 + x_3 = \bar{0}. \end{cases}$$

因为 $\mathrm{rank}(A) = 2$, 所以

$\dim(V_A) = 3 - 2 = 1$.

所以令 $x_3 = \bar{1}$, 解得 $x_2 = \bar{2}$, $x_1 = \bar{2}$

所以 V_A 的一组基为 $\left\{ \begin{pmatrix} \bar{2} \\ \bar{2} \\ \bar{1} \end{pmatrix} \right\}$.

所以 V_A 中非0向量的个数为2. □

例. 设有限域 $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. 计算非齐次线性方程组.

$$\begin{cases} x_1 + \bar{2}x_2 = \bar{1} \\ x_2 + x_3 = \bar{2} \\ x_1 + x_2 + \bar{2}x_3 = \bar{2} \end{cases}$$

$$A = \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{1} & \bar{1} & \bar{2} \end{pmatrix}$$

在 $\mathbb{Z}_3^3$ 中所有解的个数.

解: $\begin{pmatrix} \bar{1} & \bar{2} & \bar{0} & \bar{1} \\ \bar{0} & \bar{1} & \bar{1} & \bar{2} \\ \bar{1} & \bar{1} & \bar{2} & \bar{2} \end{pmatrix} \to \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} & \bar{1} \\ \bar{0} & \bar{1} & \bar{1} & \bar{2} \\ \bar{0} & \bar{2} & \bar{2} & \bar{1} \end{pmatrix} \to \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} & \bar{1} \\ \bar{0} & \bar{1} & \bar{1} & \bar{2} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} \end{pmatrix}$

解流形的维数为 $3 - \mathrm{rank}(A) = 1$

所以...所有解的个数为 $3^1 = 3$.

因为增广矩阵的秩等于系数矩阵的秩, 所以原方程有解. 设 H 是该方程对应的齐次线性方程组的解空间, 则对偶定理可得 $\dim(H) = 3 - \mathrm{rank}(A) = 1$. 所以设原非齐次线性方程组为 L, 则 $\mathrm{sol}(L) = \{v + w \mid w \in H\}$. 其中 $v = \begin{pmatrix} \bar{2} \\ \bar{1} \\ \bar{1} \end{pmatrix}$

目录

原方程等价于

$$x_1 + \bar{2}x_2 = \bar{1}$$

$$x_2 + x_3 = \bar{2}$$

所以 $v = \begin{pmatrix} \bar{2} \\ \bar{1} \\ \bar{1} \end{pmatrix}$ 是该方程的一个特解.

所以 $card(sol(L)) = 3$.

因为 $card(H) = 3^{dim(H)}$

3^2

$\{\alpha(\ ) + \beta(\ ), \alpha, \beta \in \mathbb{Z}_3\}$

环同态

设 $(R,+,0_R,\cdot,1_R)$ 和 $(S,+,0_S,\cdot,1_S)$ 是两个环. 如果映射 $\phi: R \longrightarrow S$ 满足对任意 $x,y \in R$,

$$\phi(x+y)=\phi(x)+\phi(y), \phi(xy)=\phi(x)\phi(y), \text{ 和 } \phi(1_R)=1_S,$$

则称 ϕ 是环同态. 如果环同态 ϕ 是单射, 则称 ϕ 是环嵌入; 如果是双射, 则称环同构.

$$\pi: \mathbb{Z} \longrightarrow \mathbb{Z}_3$$
$$m \longmapsto \overline{m}$$

$$1 \longmapsto \overline{1}$$
$$4 \longmapsto \overline{4}=\overline{1}$$

"$\phi(a)=\tilde{0}_K \Rightarrow a=\tilde{0}_F$" $\Rightarrow$ ϕ 是单射.

习题2. 设 ϕ 是域 F 到域 K 的环同态, 证明: ϕ 为单射.

证: 设 $a,b\in F$, 且 $\phi(a)=\phi(b)$. 则

$$\phi(a-b)=0_K \quad (1)$$

反证, 若 $a-b\neq 0$, 则 $a-b$ 在 F 可逆. 在 (1) 两边同时乘以 $\phi((a-b)^{-1})$, 得

$$\phi(a-b)\phi((a-b)^{-1})=0_K$$

$$\Rightarrow \phi((a-b)(a-b)^{-1})=0_K$$

$$\Rightarrow \phi(1_F)=0_K$$

矛盾

$\|$

1_K

于是 $a-b=0$, 即 $a=b$. □

习题2. 设 ϕ 是域 F 到域 K 的环同态, 证明: ϕ 为单射.

常见错误:

$\phi(a)=\phi(b)$

$\Rightarrow \phi(ab^{-1})=1_K$

$\not\Rightarrow ab^{-1}=1_F$

$\phi(1_F)=1_K$

习题2. 设 ϕ 是域 F 到域 K 的环同态, 证明: ϕ 为单射.

常见错误:

证明: 设 $a, b \in F$, $\phi(a) = \phi(b)$. 则 $\phi(a-b) = 0$. 若 $a - b \neq 0$, 则 $a - b$ 可逆, 两边同时乘以 $\phi((a-b)^{-1})$, 得 $\phi(1) = 0$, 矛盾. 所以 $a - b = 0$. 即 $a = b$.

目录

多项式环

设 R 是一个交换环, 设 $R[x] = \{\sum_{k=0}^{n} r_k x^k \mid n \in \mathbb{N}, r_k \in R\}$, 定义加法和乘法: 设 $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i, n \geq m$.

$$f + g = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i.$$

$$f \cdot g = \sum_{k=0}^{n+m} ((\sum_{i+j=k} a_i b_j) x^k).$$

则 $(R[x], +, 0, \cdot, 1)$ 构成一个多项式环, 简写为 $R[x]$.

多项式环上的运算和赋值

$(\bar{5}-\bar{1})(\bar{5}+\bar{2}) = \bar{4}\cdot\bar{7} = \bar{4}\cdot\bar{0} = \bar{0}$

设 $f(x) = x^2 + x - 2 = (x-1)(x+2) \in \mathbb{Z}[X]$, 分别求

1. $f(2) \in \mathbb{Z}$;
2. $f(\bar{5})$, 其中 $\bar{5} \in \mathbb{Z}_7$;
3. $f(A), A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

$2 \to 2\cdot\bar{1} = \bar{2}$

$2 \to \begin{pmatrix} 2 & & \\ & 2 & \\ & & 2 \end{pmatrix}$

解: (1) $f(2) = (2-1)(2+2) = 4$

(2) $f(\bar{5}) = \bar{1}\cdot(\bar{5})^2 + \bar{1}\cdot\bar{5} - \bar{2}\cdot = \bar{0} \in \mathbb{Z}_7$

(3) $f(A) = A^2 + A - 2\cdot E_3$

$= \begin{pmatrix} 0 & 3 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$

$(A-E)(A+2E)$

$= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 3 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$

多项式环上的运算和赋值

设 $f(x)=x^2+x-2=(x-1)(x+2)\in\mathbb{Z}[X]$, 分别求

1. $f(2)\in\mathbb{Z}$;
2. $f(\bar{5})$, 其中 $\bar{5}\in\mathbb{Z}_7$;
3. $f(A), A=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$.

解: (1) $f(2)=4$; (2) $\bar{5}^2+\bar{5}-\bar{2}=\bar{0}$;
(3)

$$f(A)=(A-E)(A+2E)=\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}3&1&0\\0&3&1\\0&0&3\end{pmatrix}=\begin{pmatrix}0&3&1\\0&0&3\\0&0&0\end{pmatrix}$$

多项式除法

引理 1.17. 设 $f, g \in R[x]$ 且 $g \neq 0$. 再设 $\mathrm{lc}(g)$ 可逆. 则存在唯一的多项式 $q, r \in R[x]$ 满足

$$f = qg + r \quad \text{和} \quad \deg(r) < \deg(g).$$

习题 4. 多项式 $f(X)=X^5+3X^4+X^3+4X^2-3X-1, g(X)=X^2+X+1$ 可以看作环 $\mathbb{Z}[X]$ 中的多项式或者 $\mathbb{Z}_5[X]$ 中的多项式. 用带余除法, 证明在第一种情况下 $f(X)$ 不被 $g(X)$ 整除, 并计算 $quo(f,g,X), \mathrm{rem}(f,g,X)$; 而在第二种情况下, $f(X)$ 可以被 $g(X)$ 整除. 与此相反的情况可能出现吗?

$\pi(f)$ $\pi(g)$

解: 计算可得, $\mathrm{quo}(f,g,X)=X^3+2X^2-2X+4\in\mathbb{Z}[X]$,
$\mathrm{rem}(f,g,X)=-5X-5\in\mathbb{Z}[X]$.

整除: $f,g\in R[X]$,
$g\mid f \Leftrightarrow \exists h\in R[X]$, s.t. $f=gh$.

$$X^2+X+\bar{1}\ \overline{)\ X^5+\bar{3}X^4+X^3+\bar{4}X^2-\bar{3}X-\bar{1}}$$

若 $f,g\in\mathbb{Z}_5[X]$, 则

$quo(f,g,X)=X^3+\bar{2}X^2-\bar{2}X+\bar{4}\in\mathbb{Z}_5[X]$

$rem(f,g,X)=-\bar{5}X-\bar{5}=\bar{0}\in\mathbb{Z}[X]$

$f=g(X^3+2X^2-2X+4)+(-5X-5)$ 唯一

习题 4. 多项式 $f(X)=X^5+3X^4+X^3+4X^2-3X-1, g(X)=X^2+X+1$ 可以看作环 $\mathbb{Z}[X]$ 中的多项式或者 $\mathbb{Z}_5[X]$ 中的多项式. 用带余除法, 证明在第一种情况下 $f(X)$ 不被 $g(X)$ 整除, 并计算 $quo(f,g,X), \mathrm{rem}(f,g,X)$; 而在第二种情况下, $f(X)$ 可以被 $g(X)$ 整除. 与此相反的情况可能出现吗?

解: 计算可得, $\mathrm{quo}(f,g,X)=X^3+2X^2-2X+4\in\mathbb{Z}[X]$, $\mathrm{rem}(f,g,X)=-5X-5\in\mathbb{Z}[X]$. 定义映射:

$$\pi:\mathbb{Z}[X]\to\mathbb{Z}_5[X],,$$

$$a_nx^n+\cdots+a_1x+a_0\mapsto\overline{a_n}x^n+\cdots+\overline{a_1}x+\overline{a_0}.$$

{ 任意 $f,g\in\mathbb{Z}[X]$, $g|f$ 在 $\mathbb{Z}[X]$,
问有没有可能 $\pi(g)\nmid\pi(f)$ 在 $\mathbb{Z}_p[X]$. $p\in\mathbb{Z}$..

习题 4. 多项式 $f(X)=X^5+3X^4+X^3+4X^2-3X-1, g(X)=X^2+X+1$ 可以看作环 $\mathbb{Z}[X]$ 中的多项式或者 $\mathbb{Z}_5[X]$ 中的多项式. 用带余除法, 证明在第一种情况下 $f(X)$ 不被 $g(X)$ 整除, 并计算 $quo(f,g,X), \mathrm{rem}(f,g,X)$; 而在第二种情况下, $f(X)$ 可以被 $g(X)$ 整除. 与此相反的情况可能出现吗?

解: 计算可得, $\mathrm{quo}(f,g,X)=X^3+2X^2-2X+4\in\mathbb{Z}[X]$, $\mathrm{rem}(f,g,X)=-5X-5\in\mathbb{Z}[X]$. 定义映射:

$$\pi:\mathbb{Z}[X]\to\mathbb{Z}_5[X],,$$

$$a_nx^n+\cdots+a_1x+a_0\mapsto\overline{a_n}x^n+\cdots+\overline{a_1}x+\overline{a_0}.$$

可以证明 π 是同态. 设 $f,g\in\mathbb{Z}[X]$, 而且 $g\mid f$. 即存在 $h\in\mathbb{Z}[X]$, 使得 $f=gh$. 两边用 π 作用; 得

$\pi(f)=\pi(g)\pi(h)$. $\pi(f)=\pi(g)h'\Rightarrow\pi(g)\mid\pi(f)$.

则 $\pi(g)\mid\pi(f)$. 在 $\mathbb{Z}_5[X]$.

$\Rightarrow\pi(g)\mid\pi(f)$ 在 $\mathbb{Z}_5[X]$ 中.

习题 4. 多项式 $f(X)=X^5+3X^4+X^3+4X^2-3X-1, g(X)=X^2+X+1$ 可以看作环 $\mathbb{Z}[X]$ 中的多项式或者 $\mathbb{Z}_5[X]$ 中的多项式. 用带余除法, 证明在第一种情况下 $f(X)$ 不被 $g(X)$ 整除, 并计算 $quo(f,g,X), \mathrm{rem}(f,g,X)$; 而在第二种情况下, $f(X)$ 可以被 $g(X)$ 整除. 与此相反的情况可能出现吗?

解: 计算可得, $\mathrm{quo}(f,g,X)=X^3+2X^2-2X+4\in\mathbb{Z}[X]$, $\mathrm{rem}(f,g,X)=-5X-5\in\mathbb{Z}[X]$. 定义映射:

$$\pi:\mathbb{Z}[X]\to\mathbb{Z}_5[X],,$$

$$a_nx^n+\cdots+a_1x+a_0\mapsto\overline{a_n}x^n+\cdots+\overline{a_1}x+\overline{a_0}.$$

可以证明 π 是同态.

$$(X^5+\bar{3}X^4+X^3+\bar{4}X^2-\bar{3}X-\bar{1})=(X^2+X+\bar{1})(X^3+\bar{2}X^2-\bar{2}X+\bar{4}).$$

所以 f 在 $\mathbb{Z}_5[X]$ 中被 g 整除.

设 f 在 $\mathbb{Z}[X]$ 中可以被 g 整除, 则 $\pi(f)$ 在 $\mathbb{Z}_5[X]$ 中一定可以被 $\pi(g)$ 整除. 这是因为, 如果 f 在 $\mathbb{Z}[X]$ 中可以被 g 整除, 则存在 $h\in\mathbb{Z}[X]$, 使得 $f=gh$. 所以 $\pi(f)=\pi(g)\pi(h)$. 所以 $\pi(g)$ 整除 $\pi(f)$.

习题5. 设 F 是域

1. 设 $a, b \in F$ 且 $a \neq 0$. 证明: 映射

$$\begin{aligned} \phi_{a,b} : F[x] &\longrightarrow F[x] \\ p(x) &\longmapsto p(ax+b) \end{aligned}$$

是从 $F[x]$ 到 $F[x]$ 的环同构.

2. 设 $\sigma : F[x] \longrightarrow F[x]$ 是环同构且 $\sigma|_F = id_F$. 证明: 存在 $a, b \in F$ 且 $a \neq 0$ 使得 $\sigma = \phi_{a,b}$.

证明: (1). ① $\forall p_1(x), p_2(x) \in F[x]$,

$\phi_{a,b}(p_1(x)+p_2(x)) = \phi_{a,b}(p_1(x)) + \phi_{a,b}(p_2(x))$

$\phi_{ab}(p_1(x)p_2(x)) = \phi_{a,b}(p_1(x))\phi_{a,b}(p_2(x))$

$\phi_{ab}(1) = 1$

双射

$\phi_{a,b}(p_1(x)+p_2(x)) = p_1(ax+b)+p_2(ax+b) = \phi_{a,b}(p_1(x)) + \phi_{ab}(p_2(x))$

习题5. 设 F 是域

1. 设 $a, b \in F$ 且 $a \neq 0$. 证明: 映射

$$\begin{aligned} \phi_{a,b} : F[x] &\longrightarrow F[x] \\ p(x) &\longmapsto p(ax+b) \end{aligned}$$

是从 $F[x]$ 到 $F[x]$ 的环同构.

2. 设 $\sigma : F[x] \longrightarrow F[x]$ 是环同构且 $\sigma|_F = id_F$. 证明: 存在 $a, b \in F$ 且 $a \neq 0$ 使得 $\sigma = \phi_{a,b}$.

证明: (1) 直接验证即可. 双射证明可以构造逆映射 $\phi_{a^{-1},-a^{-1}b}(x) = a^{-1}x - a^{-1}b$, 则

$$\phi_{a,b}(\phi_{a^{-1},-a^{-1}b}(x)) = a(a^{-1}x - a^{-1}b) + b = x,$$

$$\phi_{a^{-1},-a^{-1}b}(\phi_{a,b}(x)) = a^{-1}(ax - b) + a^{-1}b = x.$$

(2) 设 $\sigma(x) \in F[x]$，设

$$\sigma(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 .$$

$\sigma : F[x] \to F[x]$

$f_0(x) \mapsto x$

因为 σ 为环同构，所以 $\exists f_0 \in F[x]$，使得

$$\sigma(f_0(x)) = x$$

设 $f_0(x) = c_m x^m + \cdots + c_1 x^1 + c_0 \in F[x]$.

$$\sigma(f_0(x)) = \sigma(c_m)(\sigma(x))^m + \cdots + \sigma(c_1)\sigma(x) + \sigma(c_0) .$$

因为 $\sigma|_F = id_F$，所以 $(c_i \in F)$

$$\sigma(f_0(x)) = c_m(\sigma(x))^m + \cdots + c_1\sigma(x) + c_0$$

$$= c_m(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^m + \cdots +$$

$$c_1(a_n x^n + \cdots + a_1 x + a_0) + c_0 = x$$

若 $m > 1$ 或 $n > 1$，则 $\deg(\sigma(f_0(x))) > 1$

$\Downarrow$

$\Rightarrow m = n = 1$，$a_1 \neq 0$

$\Rightarrow \sigma(x) = a_1 x + a_0$.

则 $\forall f \in F[x]$，$\sigma(f) = f(\sigma(x)) = f(a_1 x + a_0)$. 于是

$\sigma = \phi_{a_1, a_0}$.

□

(2) 假设 $\sigma(x) = a_n x^n + \ldots + a_1 x + a_0$, 因为 σ 为同构, 所以存在 $f_0(x) = c_m x^m + \cdots + c_1 x + c_0 \in F[x]$, 使得 $\sigma(f_0(x)) = x$. 由于 $\sigma|_F = id_F$, 所以根据同构的性质, 有 $\sigma(f_0(x)) = f_0(\sigma(x)) = c_m(a_n x^n + \ldots + a_1 x + a_0)^m + \cdots + c_1(a_n x^n + \ldots + a_1 x + a_0) + c_0$. 于是有

$$c_m(a_n x^n + \ldots + a_1 x + a_0)^m + \cdots + c_1(a_n x^n + \ldots + a_1 x + a_0) + c_0 = x$$

所以 $n = 1$, $a_1 \neq 0$, 即 $\sigma(x) = a_1 x + a_0$. 而且任意 $f \in F[x]$, 有

$$\sigma(f(x)) = f(a_1 x + a_0).$$

即$\sigma = \phi_{a,b}$, $a = a_1$, $b = a_0$.

谢谢!