域的引入

2022年12月12日 7:01

回忆：第1,2,3章中线性代数内容

对一般域都成立，除非域的

特征②，即 $1+1=0$，等价 $1=-1$.

例：在 $\mathbb{Z}_5$ 上求解齐次线性方程组

$$\underbrace{\begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{2} & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix}}_{A} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{0} \end{pmatrix}$$

解 $A \longrightarrow \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{2} & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix}$

$\operatorname{rank}(A)=2 \Longrightarrow$ 解空间 V_A 的维数为1

↳ 对任意域

求得 $V_A = \left\langle \begin{pmatrix} \bar{1} \\ \bar{3} \\ \bar{1} \end{pmatrix} \right\rangle = \left\{ \lambda \begin{pmatrix} \bar{1} \\ \bar{3} \\ \bar{1} \end{pmatrix} \middle| \lambda \in \mathbb{Z}_5 \right\}$

$\operatorname{Card}(V_A) = 5$ $(\dim(V_A)=1)$

命题：设 $A \in M_n(F)$，其中 F 是特征为2的域. 设 A 有两行（或两列）相同. 则 $\det(A)=0$

证：设 $A=(a_{ij})_{n\times n}$

$$\det(A)=\sum_{\sigma\in S_n}\varepsilon_\sigma a_{1,\sigma(1)}a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}$$

$\because$ $char(F)=2$ $\therefore$ $1_F=-1_F$

于是 $\det(A)=\sum_{\sigma\in S_n}a_{1,\sigma(1)}a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}$

不妨设 $\vec{A_1}=\vec{A_2}$

$$\det(A)=\sum_{\substack{\sigma\in S_n\\ \sigma(1)<\sigma(2)}}\underline{(a_{1,\sigma(1)}a_{2,\sigma(2)}+a_{1,\sigma(2)}a_{2,\sigma(1)})\,a_{3,\sigma(3)}\cdots a_{n\sigma(n)}}$$

因为 $\vec{A_1}=\vec{A_2}$ 所以

$a_{1,\sigma(1)}=a_{2,\sigma(1)}$ $a_{2,\sigma(2)}=a_{1,\sigma(2)}$

于是 $a_{1,\sigma(1)}a_{2\sigma(2)}=a_{1\sigma(2)}a_{2\sigma(1)}$

$$\det A=\sum_{\substack{\sigma\in S_n\\ \sigma(1)<\sigma(2)}}\underline{2a_{1,\sigma(1)}a_{2,\sigma(2)}a_{3\sigma(3)}\cdots a_{n\sigma(n)}}$$

$=0$ $[char(F)=2]$ 证

例 $\mathbb{R}^3$，任意域 F，F^3

考虑 $\mathbb{Z}_2^3$ 是域 $\mathbb{Z}_2$ 上的 3 维

坐标空间，则

$(\mathbb{Z}_2^3,+,\vec{0})$ 是 Abel 群

$(\mathbb{Z}_2^3, +, \vec{0})$ 是加法群

$\left(\vec{0} = \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{0} \end{pmatrix} \right)$

验证 该加法群不能有两个元素生成

假设 $\mathbb{Z}_2^3$ 作为加法群由 $\vec{u}, \vec{v}$ 生成

于是 $\mathbb{Z}_2^3$ 是由标准基 $\vec{e}_1 = \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{0} \end{pmatrix}, \vec{e}_2 = \begin{pmatrix} \bar{0} \\ \bar{1} \\ \bar{0} \end{pmatrix}$

$\vec{e}_3 = \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{1} \end{pmatrix}$ 在 $\vec{u}, \vec{v}$ 所生成的子空间中

$$\Rightarrow \quad \dim(\mathbb{Z}_2^3) \leq 2 \quad \rightarrow\leftarrow$$

注: $\mathrm{card}(\mathbb{Z}_2^3) = 8$

$$\underline{(\mathbb{Z}_2^3, +, \vec{0})} \hookrightarrow S_8$$

$$S_8 = \langle (12), (12\cdots 8) \rangle$$

S_8 中有子群不可能由两个元素生成

例. 设 $A \in \mathbb{R}^{m\times n}$ 证明

$$\mathrm{rank}(A) = \mathrm{rank}(A^t A)$$

$$A^t A \in M_n(\mathbb{R})$$

证: 令 V_A 是 $A\vec{x} = \vec{0}_m$

记 $B = A^t A$ ... 的解空间

的解空间. V_B是 $B\vec{x}=0_n$ 的解空间,

$$\boxed{\text{断言}\quad V_A=V_B}$$

断言的证明　设 $\vec{u}\in V_A$

$$A\vec{u}=\vec{0}_m$$

$$B\vec{u}=A^t(A\vec{u})=A^t\vec{0}_m=\vec{0}_n$$

$$\Rightarrow \vec{u}\in V_B \Rightarrow V_A\subset V_B$$

设 $\vec{v}\in V_B$.　设 $\vec{w}=A\vec{v}=\begin{pmatrix}w_1\\ \vdots\\ w_m\end{pmatrix}$

$$\underbrace{A^tA}_{B}\vec{v}=\vec{0}_n$$

$$\vec{v}^{\,t}A^tA\vec{v}=\vec{v}^{\,t}\vec{0}_n=0$$

$$(A\vec{v})^tA\vec{v}=0$$

$$(w_1,\cdots w_m)\begin{pmatrix}w_1\\ \vdots\\ w_m\end{pmatrix}=0$$

$$w_1^2+\cdots+w_m^2=0$$

因为 $w_1,\cdots w_m\in\mathbb{R}$. 所以 $w_1=\cdots=w_m=0$

故 $\vec{w}=\vec{0}_m \Rightarrow \vec{v}\in V_A$

$$\Rightarrow V_A=V_B$$

由对偶定理　$\mathrm{rank}(A)=\mathrm{rank}(B)$ ☐

---

e例的结论对一般域不对

后例的结论对一般域不对

$$A = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{2} \end{pmatrix} \in M_2(\mathbb{Z}_5)$$

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

$$= \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \overline{1+4} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}.$$

$\operatorname{rank}(A) = 1$. 而 $\operatorname{rank}(A^t A) = 0$

注. 第十一周 习题 6 对一般域不成立

$\operatorname{tr}(A^t A) = 0 \Rightarrow A = O$

---

§4.3 域的嵌入

设 F, K 是两个域

$\varphi: F \to K$ 是环同态

已知 φ 是单射

$F \cong \varphi(F) \subset K$

$\underbrace{\qquad\qquad}$ 环同构 (域同构)

例 设 $(F, +, 0_F, \cdot, 1_F)$

是域. 如果 $\operatorname{char}(F) = 0$

则 $\mathbb{Q} \hookrightarrow F$

1.1 域嵌入

证：$\varphi: \mathbb{Q} \longrightarrow F$

$$\frac{m}{n} \longmapsto (m1_F)(n1_F)^{-1}$$

说明 φ 是良定义

设 $\frac{m}{n} = \frac{k}{l}$，$m, n, k, l \in \mathbb{Z}$，$n \neq 0, l \neq 0$

则 $ml = nk$

要证 $(m1_F)(n1_F)^{-1} = (k1_F)(l1_F)^{-1}$

等价于

$$(m1_F)(l1_F) = (k1_F)(n1_F)$$

由这分配律，上式等价于

$$(ml)1_F = (kn)1_F$$

$\because ml = kn$ $\therefore$ 上式成立 故 φ 是良定义的

$$\boxed{\varphi: \mathbb{Q} \longrightarrow F, \quad \frac{m}{n} \longmapsto (m1_F)(n1_F)^{-1}}$$

$$\varphi\left(\frac{m}{n} + \frac{k}{l}\right) = \varphi\left(\frac{ml+nk}{nl}\right)$$

$$= \left[(ml+nk)1_F\right](nl1_F)^{-1}$$

$$\varphi\left(\frac{m}{n}\right) + \varphi\left(\frac{k}{l}\right) = (m1_F)(n1_F)^{-1} + (k1_F)(l1_F)^{-1}$$

$= [(m\ell \cdots)]$

$\varphi\left(\frac{m}{n}\right)+\varphi\left(\frac{k}{\ell}\right)=(m1_F)(n1_F)^{-1}+(k1_F)(\ell 1_F)^{-1}$

要证 φ 保持加法，只要证

$$((m\ell+nk)1_F)\underline{(n\ell 1_F)}^{-1}=(m1_F)(n1_F)^{-1}+(k1_F)(\ell 1_F)^{-1}$$

即要证

$$(m\ell+nk)\cdot 1_F=(m1_F)(\ell 1_F)+(k1_F)\overset{(n1_F)}{}$$

$$=(m\ell+kn)1_F \checkmark$$

φ 保持乘法类似

$$\varphi(1)=\varphi\left(\frac{1}{1}\right)=1_F 1_F^{-1}=1_F$$

保持乘法单位

φ 是单同态. $\square$

注 $\mathbb{Q}$ 被看成 F 中"子集"

" $(\mathbb{Q}\hookrightarrow F)$

例 设 $\operatorname{char}(F)=p>0$

则 $\mathbb{Z}_p\hookrightarrow F$

证：
$$\varphi:\ \mathbb{Z}_p\longrightarrow F$$
$$\overline{m}\longmapsto m1_F$$

验证良定义. 设 $\overline{m}=\overline{n}$

$n=m+kp$

验证良定义. 设 $\bar{m} = \bar{n}$

则 $\exists k \in \mathbb{Z}$ $\quad n = m + kp$

$$\varphi(\bar{n}) = (m+kp)1_F$$

$$= m1_F + k\underbrace{(p1_F)}$$

$$= m1_F \qquad \left(p1_F = 0_F \quad \because char(F) = p \right)$$

$$= \varphi(\bar{m})$$

验证保持乘法

$$\varphi(\bar{m}\,\bar{n}) = \varphi(\overline{mn})$$

$$= mn1_F = (m1_F)(n1_F) \quad \text{广义分配律}$$

$$= \varphi(\bar{m})\,\varphi(\bar{n}).$$

保持加法自己验证

$$\varphi(\bar{1}) = 1 \cdot 1_F = 1_F \ ✓$$

$\because$ $\mathbb{Z}_p$ 是域 $\therefore$ φ 是单射 $\square$

$\mathbb{Q} \subset F$ 如果 $char(F) = 0$

$\mathbb{Z}_p \subset F$ 如果 $char(F) = p$

$\boxed{\text{abuse of notation}}$

$(1 = \frac{1}{1})$ $\qquad \mathbb{Q} = \left\{ \frac{m}{n} \;\middle|\; m, n \in \mathbb{Z},\ n \neq 0 \right.$

$(1 = \frac{1}{1})$ $\mathbb{Q} = \{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \}$

m "=" $\frac{m}{1}$

分式（数）是怎么来的？

设 D 是一个整环，令

$D^* = D \setminus \{0\}$

在 $D \times D^*$ 上引入二元关系 $\sim$

"$\frac{a}{b} \times \frac{c}{d}$" $(a, b) \sim (c, d)$ 如果 $ad = bc$

验证 $\sim$ 是等价关系

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

对称 $(a, b) = (c, d) \Rightarrow ad = bc \Rightarrow bc = ad$

$\Rightarrow (c, d) \sim (a, b)$

传递. 设 $(a, b) \sim (c, d)$, $(c, d) \sim (e, f)$

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

$(c, d) \sim (e, f) \Rightarrow cf = de$

$\Rightarrow adcf = bcde$

$\because d \neq 0 \quad \therefore acf = bce$ [消去律]

情形1. $c \neq 0$ $af = be$ [消去律]

$\Rightarrow (a, b) \sim (e, f)$

情形2 $c = 0$, $ad = 0 \Rightarrow a = 0$ ($d \neq 0$)

$de = 0 \Rightarrow e = 0$ ($d \neq 0$)

$(0, f)$

特别地 $c=0$, $de=0 \Rightarrow e=0$ $(d\neq 0)$

$\Rightarrow af=be=0 \Rightarrow (a,b)\sim(e,f)$.

传递律成立

"$\sim$" 是等价关系

$\overline{(1,2)}=\frac{1}{2}$

$\overline{(2,4)}=\frac{2}{4}=\frac{1}{2}$ 把 $(D\times D^*)/\sim$ 记为 $Fr(D)$.

(fraction)

$$\overline{(a,b)}=\frac{a}{b}$$

$$Fr(D)=\left\{\frac{a}{b}\,\middle|\, a\in D,\ b\in D^*\right\}$$

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

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

$\frac{0}{1}$ 是加法单位

$\frac{1}{1}$ 是乘法单位

则 $(Fr(D),\ +,\ \frac{0}{1},\ \cdot,\ \frac{1}{1})$

是域

验证: $+$ 是良定义的

$$\boxed{\begin{gathered}\frac{a}{b}=\frac{a'}{b'}\quad \frac{c}{d}=\frac{c'}{d'}\\ \Rightarrow \frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}\end{gathered}}$$

$ab' = ba' \quad cd' = dc'$

$\Rightarrow (ad+bc)b'd' = (a'd'+b'c')bd$

良定义

$$\boxed{\frac{a}{b}\cdot\frac{c}{d} = \frac{a'}{b'}\cdot\frac{c'}{d'}}$$

$(ac)(b'd') = (a'c')(bd)$

所有的规律

可逆性 $\frac{a}{b} \neq \frac{0}{1}$ 如果 $a \neq 0$

$(a\neq 0) \quad \frac{a}{b}\cdot\frac{b}{a} = \frac{1}{1}$

$\left(Fr(D), +, \frac{0}{1}, \frac{1}{1}\right)$ 是域

称为 D 的分式域

命题: $\underline{D} \hookrightarrow Fr(D)$

证: $\varphi: D \longrightarrow Fr(D)$

$a \longmapsto \frac{a}{1}$

$\varphi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$

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

$\varphi(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1}$

$\varphi(1) = \frac{1}{1}$

命题: 设 F 是域. D 是整环

命题：设 F 是域. D

如果 D 是 F 的子环，

则 $Fr(D) \hookrightarrow F$

证：$\varphi: Fr(D) \hookrightarrow F$

$$\frac{a}{b} \mapsto ab^{-1}$$

$\mathbb{Q} \hookrightarrow F \quad (\mathrm{char}(F)=0)$

$\mathbb{Z}_p \hookrightarrow F \quad (\mathrm{char}(F)=p)$

如果 $D \subset F$ 则

$\underline{Fr(D)} \hookrightarrow F$

$D \subset Fr(D) \subset F$

R 环

交换 ／ 非交换

$\mathbb{Z}, \mathbb{Z}_n, \mathbb{R}[A]$ ↓ 整环 $\mathbb{Z}$, ↓ 域 $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (p 是素数)

$M_n(\mathbb{R})$ ↓ ? ↓ $\boxed{\text{四元数集}}$ 有的斜域

$\underline{\text{Hamilton 十年}}$

域的嵌入"不考"

重点是域上的线性代数

数量域上的线性代数

第5章 复数域和多项式环

§1 一元多项式

$f(x) = x^2 + 2x - 5$

$x^2 + 2x - 5 = 0$ 求解

x 变元　　未知数

§1.1 一元多项式环的构造

本节中 $(R, +, 0, \cdot, 1)$ 是交换环

目的：构造以 R 中元素为系数的一元多项式.

$r_0 + r_1 x + \cdots + r_n x^n$

$r_0 \quad r_1 \quad \cdots \quad r_n$

$r_0 \quad r_1 \quad \cdots \quad r_n \quad \cdots \quad r_{n+k}$

令 $\tilde{R} = \{(r_0, r_1, r_2, \cdots) \mid r_i \in R$ 有限个非零$\}$

$+: \tilde{R} \times \tilde{R} \longrightarrow \tilde{R}$

$(\cdots r_n \cdots), (\cdots s_n \cdots) \longmapsto (\cdots r_n + s_n, \cdots)$

由 $(R, +, 0)$ 是交换群可直接得

$(\tilde{R}, +, \tilde{0})$ 是交换群

由 $(R, +, 0)$ …

$(\tilde{R}, +, \tilde{0})$ 是交换群

$\tilde{0} = (0, 0, \cdots)$

$(a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0)(b_n x^n + \cdots + b_1 x + b_0)$

x^i 的系数 $\sum_{j=0}^{i} a_j b_{i-j}$

$$\tilde{R} \times \tilde{R} \longrightarrow \tilde{R}$$

$$(\cdots r_n \cdots), (\cdots s_n \cdots) \longmapsto (\cdots \sum_{i=0}^{n} r_i s_{n-i} \cdots)$$

设当 $n > M$, $r_n = 0$

当 $n > N$ $s_n = 0$

当 $n > M+N+1$ 时 $\sum_{i=0}^{n} r_i s_{n-i} = 0$

于是 "·" 是二元运算

$\tilde{1} := (1, 0, 0, \cdots)$

则 $\tilde{r} \cdot \tilde{1} = \tilde{1} \cdot \tilde{r} = \tilde{r}$

验证：$(\tilde{R}, \cdot, \tilde{1})$ 是交换的幺半群

验证乘法结合律

设 $\tilde{a} = (a_0, a_1, \cdots)$ $\in \tilde{R}$

$\tilde{b} = (b_0, b_1, \cdots)$

$\tilde{c} = (c_0, c_1, \cdots)$

$\tilde{c} = (c_0, c_1, \ldots)$

要验证 $\tilde{a}(\tilde{b}\tilde{c}) = (\tilde{a}\tilde{b})\tilde{c}$

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

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

要验证: $\tilde{p}\tilde{q} = \tilde{u}\tilde{v}$

$\tilde{p} = (p_0, p_1, \ldots)$, $\tilde{q}, \tilde{u}, \tilde{v} \ldots$

$$q_n = \sum_{i+j=n} \underline{p_i} c_j = \sum_{i+j=n} \left(\sum_{k+l=i} a_k b_l \right) c_j$$

$$= \sum_{j+k+l=n} \underline{a_k b_l c_j}$$ [R中结合, 交换, 分配

$$v_n = \sum_{k+i=n} a_k u_i = \sum_{k+i=n} a_k \sum_{l+j=i} b_l c_j$$

$$= \sum_{k+l+j=n} \underline{a_k b_j c_j}$$

$\Rightarrow q_n = v_n \quad \forall n \in \mathbb{N}$

$\Rightarrow q = v$. 结合律

命题: 设 $(R, +, 0, \cdot, 1)$ 是交换环

则 $(\tilde{R}, +, \tilde{0}, \cdot, \underline{\tilde{1}})$ 也是交换环 $\tilde{1} = (1, 0, 0, \ldots 0)$

且 $\varphi: R \longrightarrow \tilde{R}$

$r \longmapsto (r, 0, 0, \ldots)$

是 单的 环同态

是单的环同态

证明 $\varphi(r+s) = (r+s, 0, 0 \cdots 0 \cdots)$

$= (r, 0, 0 \cdots) + (s, 0, 0, \cdots)$

$= \varphi(r) + \varphi(s)$

$\varphi(rs) = (rs, 0, 0 \cdots 0)$

$\varphi(r)\varphi(s) = \underbrace{(r, 0, 0 \cdots 0)(s, 0, 0 \cdots)}_{\tilde{t}}$

$\tilde{t}$ 中第 n 项 $t_n = \sum_{i+j=n} r_i s_j$

$\Rightarrow t_0 = rs, \quad t_k = 0, \quad k > 0$

$\varphi(r)\varphi(s) = (rs, 0, 0 \cdots 0 \cdots)$

$= \varphi(rs)$

$\varphi(1) = (1, 0, 0 \cdots) = \tilde{1}$.

设 $\varphi(r) = \tilde{0} \Rightarrow (r, 0 \cdots 0 \cdots) = (0, 0, \cdots 0 \cdots)$

$\Rightarrow \varphi$ 是单的环同态 □

设 $x = (0, 1, 0, 0, \cdots)$

网断了，下课