第十五次习题课

- **域**：设 F 为交换环，若 F 中任何非零元都可逆，则称 F 为域

  整环 + 每个非零元都可逆 $\Leftrightarrow$ 域.

  例：若 p 是素数 则 $\mathbb{Z}_p$ 是域.

  $\mathbb{Q}$ 是 $\mathbb{R}$ 的子域.

- **特征**：设 F 是一个域，若 1 的加法阶有限，则定义 $\mathrm{char}(F)=\mathrm{ord}(1)$

  否则，定义 $\mathrm{char}(F)=0$.

  ① 一个域的特征是 0 或一个素数

  ② 设 $\mathrm{char}(F)=p>0$，则 $\forall x\in F$ 和 $m\in\mathbb{Z}$，$(mp)x=0$

  ③ 设 $\mathrm{char}(F)=p>0$，则 $\forall x,y\in F$，$(x+y)^p=x^p+y^p$

  （Freshmen's dream）

  ④ $\mathrm{char}(\mathbb{Q})=\mathrm{char}(\mathbb{R})=0$，$\mathrm{char}(\mathbb{Z}_p)=p$ if p prime.

- **性质**：① 域之间的环同态都是单射.

  ② 域具有加.减.乘.除的运算封闭性.

  除了奇数阶斜对称行列式为 0 以外.（特征不等于2时）.

  其他所有实数域上线性代数的结论对一般域的成立.

- **Fermat 小定理**：设 p 是素数，$m\in\mathbb{Z}\setminus\{0\}$ 且 $p\nmid m$，则 $m^{p-1}\equiv 1 \bmod p$.

  推论：设 p 是素数，$\overline{k}\in\mathbb{Z}_p$，则 $\overline{k}^p=\overline{k}$.

- **分式域**：设 D 是整环，$D^*=D\setminus\{0\}$　$Fr(D)=\left\{\frac{a}{b}\mid a\in D, b\in D^*\right\}$

  其中 $\frac{a}{b}=(a,b)$ 关于 $\sim$ 的等价类的代表元. $(a,b)\sim(c,d)\Leftrightarrow ad=bc$

  $(Fr(D),+,0/1,\cdot,1/1)$

  性质：设 D 是整环，则 $\phi: D\longrightarrow Fr(D)$，$x\longmapsto \frac{x}{1}$ 是环的单同态.

  $D\cong \mathrm{im}(\phi)=\left\{\frac{x}{1}\mid x\in D\right\}$　　$D\subseteq Fr(D)$.（子集）

• 多项式环：设 R 是交换环，$\widetilde{R}=\{(r_0,r_1,\cdots,r_n,\cdots)\mid r_i\in R\}$

$(\widetilde{R},+,0,\cdot,1)$ ⇒交换环．$0=(0,\cdots)$ $1=(1,0,\cdots)$

$R\cong\{(r,0,\cdots)\mid r\in R\}$ $R[x]=\{\sum_{i=0}^{n} r_i x^i \mid r_i\in R, n\in\mathbb{N}\}$

$\forall f(x)=\sum_{i=0}^{n} a_i x^i$ $g(x)=\sum_{i=0}^{m} b_i x^i$ $(n\geq m)$

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

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

⇒ $(R[x],+,0,\cdot,1)$ 构成多项式环．

• 首项系数与次数：$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$

$\deg(f)=n$ $lc(f)=a_n$

若 $f(x)=0$ ⇒ $\deg(f)=-\infty$，$lc(f)=0$

• 性质：$p,q\in R[x]$，$\deg(p+q)\leq\max\{\deg(p),\deg(q)\}$

$\deg(p\cdot q)\leq\deg(p)+\deg(q)$

当 $lc(p)lc(q)\neq 0$ 时等号成立 且 $lc(p\cdot q)=lc(p)\cdot lc(q)$．

• 定理：设 D 是整环．则 $D[x]$ 是整环．特别地，当于是域时，$F[x]$ 是整环．
(无零因子)

• 赋值定理：

定理 1.9 设 S 是交换环，$\phi:R\longrightarrow S$ 是环同态，且 $s\in S$.
则存在唯一的环同态 $\phi_s:R[x]\longrightarrow S$ 满足

$$\phi_s|_R=\phi \quad 和 \quad \phi_s(x)=s.$$

$\phi_s:R[x]\longrightarrow S$

$\sum_{i=0}^{n} r_i x^i\longmapsto\sum_{i=0}^{n}\phi(r_i)s^i$

ϕ_s 为 ϕ 在 s 处的赋值同态

• $S=R$ 且 $\phi=id_R$ 时 $\phi_s:f(x)\longmapsto f(s)$．

• $\phi=\pi_n:\mathbb{Z}\longrightarrow\mathbb{Z}_n$，$\forall\bar{k}\in\mathbb{Z}_n$，$\phi_{\bar{k}}:\mathbb{Z}[x]\longrightarrow\mathbb{Z}_n$ $f(x)\longmapsto f(\bar{k})$

1. 设

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

(1) 求线性方程组 $A\mathbf{x} = \mathbf{0}$ 的解空间;

(2) 求 A 的列空间中所含向量的个数.

1. (1) 设线性方程组 $A\vec{x}=\vec{0}$ 解空间为 V_A 设 $\vec{x}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$

利用行初等变换.

$$A \longrightarrow \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} \\ \bar{0} & \bar{0} & \bar{2} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix} \qquad \mathrm{rank}(A)=2 \Rightarrow \dim(V_A)=1$$

$$\begin{cases} \bar{1}x_1+\bar{2}x_2=\bar{0} \\ \bar{2}x_3=\bar{0} \end{cases} \Rightarrow \begin{cases} x_1=x_2 \\ x_3=\bar{0} \end{cases} \quad \therefore V_A \text{一组基为} \begin{pmatrix} \bar{1} \\ \bar{1} \\ \bar{0} \end{pmatrix}$$

$$V_A = \left\langle \begin{pmatrix} \bar{1} \\ \bar{1} \\ \bar{0} \end{pmatrix} \right\rangle$$

(2) $\dim(V_C(A)) = \mathrm{rank}(A) = 2$

设 $\{\vec{u}, \vec{v}\}$ 为 $V_C(A)$ 一组基 则 $V_C(A)=\{\alpha\vec{u}+\beta\vec{v} \mid \alpha,\beta\in\mathbb{Z}_3\}$

由 $\vec{u},\vec{v}$ 线性无关 $\Rightarrow$ 其线性表示 $\alpha\vec{u}+\beta\vec{v}$ 唯一.

由 (α,β) 可能取值 9 种 $\Rightarrow$ $V_C(A)$ 包含向量 9 个.

2. 设 $\phi : \mathbb{Z}_5^4 \to \mathbb{Z}_5^2$ 的由

$$\phi(\mathbf{e}_1) = \boldsymbol{\epsilon}_1 + \bar{2}\boldsymbol{\epsilon}_2,\ \phi(\mathbf{e}_2) = -\boldsymbol{\epsilon}_2,\ \phi(\mathbf{e}_3) = \bar{3}\boldsymbol{\epsilon}_1,\ \phi(\mathbf{e}_4) = \bar{3}\boldsymbol{\epsilon}_1 + \bar{2}\boldsymbol{\epsilon}_2$$

确定的线性映射, 其中 $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4$ 是 $\mathbb{Z}_5^4$ 的标准基, $\boldsymbol{\epsilon}_1, \boldsymbol{\epsilon}_2$ 是 $\mathbb{Z}_5^2$ 的标准基. 计算: (i) ϕ 在上述标准基下的矩阵, (ii) $\dim(\mathrm{im}(\phi))$ 和 $\dim(\ker(\phi))$, (iii) $\phi(\mathbf{v})$, 其中 $\mathbf{v} = (\bar{1}, -\bar{1}, \bar{0}, \bar{2})^t$

2. (1) $\phi(\vec{e}_1,\vec{e}_2,\vec{e}_3,\vec{e}_4)=(\vec{\varepsilon}_1,\vec{\varepsilon}_2)=\begin{pmatrix} \bar{1} & \bar{0} & \bar{3} & \bar{3} \\ \bar{2} & -\bar{1} & \bar{0} & \bar{2} \end{pmatrix}$

$$\Rightarrow A_\phi = \begin{pmatrix} \bar{1} & \bar{0} & \bar{3} & \bar{3} \\ \bar{2} & -\bar{1} & \bar{0} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} & \bar{3} & \bar{3} \\ \bar{2} & \bar{4} & \bar{0} & \bar{2} \end{pmatrix}$$

$\mathbb{Z}_n$: $\bar{i}+\bar{j}=\bar{0}$ if $i+j=n$. $(i,j\le n-1)$

(2) $A_\phi \longrightarrow \begin{pmatrix} \bar{1} & \bar{0} & \bar{3} & \bar{3} \\ \bar{0} & \bar{4} & \bar{4} & \bar{1} \end{pmatrix}$ $\operatorname{rank}(A_\phi) = 2$

$\Rightarrow \dim(\operatorname{im}(\phi)) = 2$ 根据对偶定理 $\dim(\ker(\phi)) = 4-2 = 2$

(3) $\phi(\vec{v}) = \phi\begin{pmatrix} \bar{1} \\ \bar{4} \\ \bar{0} \\ \bar{2} \end{pmatrix} = A_\phi \vec{v} = \begin{pmatrix} \bar{1} & \bar{0} & \bar{3} & \bar{3} \\ \bar{2} & \bar{4} & \bar{0} & \bar{2} \end{pmatrix}\begin{pmatrix} \bar{1} \\ \bar{4} \\ \bar{0} \\ \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{2} \\ \bar{2} \end{pmatrix}$

3. 计算 $11^{1752} \mod 71$ (提示：利用 Fermat 小定理).

3. 71 素数 Fermat 小定理：$\forall m \Rightarrow m^{p-1} \equiv 1 \pmod{p}$

$11^{1752} = 11^{70\times 25+2} \equiv 1^{25}\cdot 11^2 \equiv 11^2 \equiv 50 \pmod{71}$

4. 设 $f(x) = x^2 + 2x - 3 \in \mathbb{Z}[x]$ 分别求

(a) $f(3) \in \mathbb{Z}$;

(b) $f(\bar{5})$, 其中 $\bar{5} \in \mathbb{Z}_7$;

(c) $f(A)$, 其中 $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

4. $f(x) = (x-1)(x+3)$

(a) $f(3) = (3-1)(3+3) = 12$

(b) $f(\bar{5}) = (\bar{5}-\bar{1})(\bar{5}+\bar{3}) = \bar{4}\cdot\bar{1} = \bar{4}$

(c) $f(A) = (A-E)(A+3E)$

$= \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 4 & 0 & 0 \\ 1 & 4 & 0 \\ 0 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 4 & 0 & 0 \\ 1 & 4 & 0 \end{pmatrix}$

5. 设 $\mathbb{F}$ 是域

(a) 设 $a, b \in \mathbb{F}$ 且 $a \neq 0$. 证明: 映射

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

是从 $\mathbb{F}[x]$ 到 $\mathbb{F}[x]$ 的环同构.

(b) 设 $\sigma : \mathbb{F}[x] \to \mathbb{F}[x]$ 是环同构且 $\sigma|_{\mathbb{F}} = id_{\mathbb{F}}$. 证明: 存在 $a, b \in \mathbb{F}$ 且 $a \neq 0$ 使得 $\sigma = \phi_{a,b}$.

5. (1) 环同构: 环同态 + 双射.

环同态: $\forall\ p_1(x), p_2(x) \in \mathbb{F}[x]$

① $\phi_{a,b}(p_1(x)+p_2(x)) = \phi_{a,b}(p_1(x)) + \phi_{a,b}(p_2(x))$

② $\phi_{a,b}(p_1(x)\cdot p_2(x)) = \phi_{a,b}(p_1(x)) \cdot \phi_{a,b}(p_2(x))$

③ $\phi_{a,b}(1) = 1$

双射: 构造逆映射 $\psi : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]$

$p(x) \longmapsto p(\frac{1}{a}x - \frac{b}{a})$

$\psi(\phi_{a,b}(p(x))) = \psi(p(ax+b)) = p(\frac{1}{a}(ax+b) - \frac{b}{a})$

$= p(x)$

$\phi_{a,b}(\psi(p(x))) = \phi_{a,b}(p(\frac{x}{a} - \frac{b}{a})) = p(a(\frac{x}{a} - \frac{b}{a}) + b)$

$= p(x)$

$\Rightarrow$ ψ 是 $\phi_{a,b}$ 逆映射 即 $\phi_{a,b}$ 是双射.

(2) 设 $\sigma : \mathbb{F}[x] \to \mathbb{F}[x]$ 是环同构 且 $\sigma|_{\mathbb{F}} = id_{\mathbb{F}}$

不妨设 $\sigma(x) = \sum_{i=0}^{n} a_i x^i$

由 σ 是同构, $\exists$ 逆映射 $g(x) = \sum_{i=0}^{m} c_i x^i \in \mathbb{F}[x]$ s.t. $\sigma(g(x)) = x$.

由于 $\sigma|_{\mathbb{F}} = id_{\mathbb{F}}$, $\Rightarrow \sigma(g(x)) = g(\sigma(x)) = \sum_{i=0}^{m} c_i (\sigma(x))^i = x$

(即 $\sigma(c) = c$ if $c \in \mathbb{F}$.) $\Rightarrow n=1$, $a_1 \neq 0$ 即 $\sigma(x) = a_1 x + a_0$

又由 $\sigma(p(x)) = p(a_1 x + a_0)$ $\Rightarrow \sigma = \phi_{a_1,b}$.