1. 设

$$A=\begin{pmatrix}\bar 1 & \bar 2 & \bar 0\\ \bar 0 & \bar 1 & \bar 1\\ \bar 1 & \bar 1 & \bar 2\end{pmatrix}\in \underline{M_3(\mathbb{Z}_3)} \qquad \mathbb{Z}_p$$

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 中有非零向量的个数.

解：通过高斯消元法可得

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

$$\Rightarrow \begin{cases}\bar 1\cdot x_1+\bar 2\cdot x_2=\bar 0\\ \bar 1\cdot x_2+\bar 1\cdot x_3=\bar 0\end{cases}$$

$\mathrm{rank}(A)=2 \Rightarrow \dim V_A = 1$. $\qquad \mathrm{Card}(V_A)=3^{\dim V_A}$

取 $x_3=\bar 1$，则 $x_2=\bar 2$，$x_1=\bar 2$，V_A 的一组基为 $(\bar 2,\bar 2,\bar 1)^t$.

非零向量的个数为 $\underset{\sim}{3}-1=2$.

$AX=\begin{pmatrix}\bar 1\\ \bar 0\\ \bar 1\end{pmatrix}$

$$(A\mid \begin{smallmatrix}\bar 1\\ \bar 0\\ \bar 1\end{smallmatrix})=\left(\begin{array}{ccc|c}\bar 1 & \bar 2 & \bar 0 & \bar 1\\ \bar 0 & \bar 1 & \bar 1 & \bar 0\\ \bar 1 & \bar 1 & \bar 2 & \bar 1\end{array}\right)\to\left(\begin{array}{ccc|c}\bar 1 & \bar 2 & \bar 0 & \bar 1\\ \bar 0 & \bar 1 & \bar 1 & \bar 0\\ \bar 0 & \bar 2 & \bar 2 & \bar 0\end{array}\right)\to\left(\begin{array}{ccc|c}\bar 1 & \bar 2 & \bar 0 & \bar 1\\ \bar 0 & \bar 1 & \bar 1 & \bar 0\\ \bar 0 & \bar 0 & \bar 0 & \bar 0\end{array}\right)$$

$\underbrace{\qquad}_{A}\ \underbrace{\qquad}_{\tilde A}$

$\mathrm{rank}(A)=\mathrm{rank}(\tilde A)=2.$

一个特解 $(\bar 1,\bar 0,\bar 0)^t$，

对应齐次线性方程组的解空间为 $\left\langle\begin{pmatrix}\bar 2\\ \bar 2\\ \bar 1\end{pmatrix}\right\rangle$

$\Rightarrow$ 全部解为 $\left\{\begin{pmatrix}\bar 1\\ \bar 0\\ \bar 0\end{pmatrix}+\lambda\begin{pmatrix}\bar 2\\ \bar 2\\ \bar 1\end{pmatrix}\ \middle|\ \lambda\in\mathbb{Z}_3\right\}$.

解的个数 3 个.

2. 设 ϕ 是域 F 到域 K 的环同态，证明 ϕ 为单射.

$\Updownarrow$

$\ker(\phi)=\{0_F\}$.

解：设 $a,b\in F$，$\phi(a)=\phi(b)$

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

若 $a-b\neq 0$，由域上所有非零元素均可逆，则

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

$$\Rightarrow \phi(1_F)=0 \quad \to \Leftarrow$$

由环同态，$\phi(1_F)=1_K$.

$$\Rightarrow a-b=0$$

$$\Rightarrow a=b$$

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

(a) $f(2)\in\mathbb{Z}$

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

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

pf: (a) $f(2)=2^2+2-2=4$.

(b) $f(\bar{5})=\bar{5}^2+\bar{5}-\bar{2}=\overline{28}=\bar{0}$

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

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 $quo(f,g,x)$, $rem(f,g,x)$; 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:

$$
\begin{array}{r}
x^3+2x^2-2x+4\\
x^2+x+1\,\big)\,\overline{x^5+3x^4+x^3+4x^2-3x-1}\\
\underline{x^5+x^4+x^3}\\
2x^4+4x^2-3x-1\\
\underline{2x^4+2x^3+2x^2}\\
-2x^3+2x^2-3x-1\\
\underline{-2x^3-2x^2-2x}\\
4x^2-x-1\\
\underline{4x^2+4x+4}\\
-5x-5
\end{array}
$$

$\mathbb{Z}[x]$

在 $\mathbb{Z}[x]$ 中,

$quo(f,g,x)=x^3+2x^2-2x+4$

$rem(f,g,x)=-5x-5$

$0+5$

在 $\mathbb{Z}_5[x]$ 中.

$quo(f,g,x)=x^3+\bar{2}x^2+\bar{3}x-\bar{1}$.

$rem(f,g,x)=\bar{0}$.

$g\mid f$.

在 $\mathbb{Z}[x]$ 中, 若 $g\mid f$, 那么在 $\mathbb{Z}_5[x]$ 中, $g\mid f$ 吗?

定义映射: $\pi_5:\mathbb{Z}[x]\to\mathbb{Z}_5[x]$

$x^n+\overline{a_{n-1}}x^{n-1}+\cdots+\overline{a_1}x+\overline{a_0}$.

$x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$

若 $g|f$，则 $\exists\ h\in\mathbb{Z}[x]$，$f=gh$。

$\pi_5(f)=\pi_5(g)\pi_5(h)$

f,g 都是首一（首项系数为1）

$\pi_5(f),\pi_5(g)\neq0$，从而 $\pi_5(h)\neq0$

$\Rightarrow \pi_5(g)\mid\pi_5(f)$ 在 $\mathbb{Z}_5[x]$

5. 设 F 是域

(a) 设 $a,b\in F$ 且 $a\neq0$。证明：映射 $x\mapsto ax+b$

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

$a(mx+n)+b=x$

$\Rightarrow am=1$ $\Rightarrow m=a^{-1}$

$an+b=0$ $n=-a^{-1}b$

是从 $F[x]$ 到 $F[x]$ 的环同构

(b) 设 $\sigma:F[x]\to F[x]$ 是环同构且 $\sigma|_F=id_F$。证明：$\exists\ a,b\in F$ 且 $a\neq0$ 使得 $\sigma=\phi_{a,b}$。

Pf: (1) 法一：环同构 = 环同态 + 双射

$\forall f,g\in F[x]$

$\phi_{a,b}(f+g)=\phi_{a,b}(f)+\phi_{a,b}(g)$

$\phi_{a,b}(fg)=\phi_{a,b}(f)\phi_{a,b}(g)$

$\phi_{a,b}(1_{F[x]})=1_{F[x]}$

双射可以通过构造逆映射：$\phi_{a^{-1},-a^{-1}b}$ 已经验证

$\boxed{\phi_{a^{-1},-a^{-1}b}(x)=a^{-1}x-a^{-1}b,\ a\neq0}$

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

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

$\Rightarrow \forall f\in F[x]$

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

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

$\Rightarrow \phi_{a,b}$ 是双射

法二：由赋值同态定理可知，$\exists!$ 环同态 $\phi_{a,b}:F[x]\to F[x]$ 满足 $\phi_{a,b}|_F=id_F$，

$\phi_{a,b}(x)=ax+b$，$a\neq0$

(2) 令 $f(x)=\sigma(x)\in F[x]$，则 $f(x)\notin F$，否则 σ 不是满射，从而 $\deg f(x)\geq1$

设 σ' 是 σ 的逆映射，且 $g(x)=\sigma'(x)$，$\deg(g(x))\geq1$

设 $\sigma(x)=f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_0,\quad a_n\neq 0,\ n\geq 1$

$\sigma^{-1}(x)=g(x)=b_m x^m+b_{m-1}x^{m-1}+\cdots+b_0,\quad b_m\neq 0,\ m\geq 1$

$$
\begin{aligned}
x=\sigma^{-1}(\sigma(x)) &= \sigma^{-1}(a_n x^n+a_{n-1}x^{n-1}+\cdots+a_0)\\
&= a_n(\sigma^{-1}(x))^n+a_{n-1}(\sigma^{-1}(x))^{n-1}+\cdots+a_0\\
&= \underbrace{a_n(b_m x^m+\cdots+b_0)^n+\cdots+a_0}_{h}
\end{aligned}
$$

$\deg(h)=mn$

$\Rightarrow mn=1 \quad /m,n\in\mathbb{N}_+ \quad \Rightarrow m=n=1,\quad a_n,b_m\neq 0$

$\Rightarrow \sigma(x)=ax+b,\quad a\neq 0.$

期末复习

1. 解有限域上的线性方程组

例 $A=\begin{pmatrix}\bar{1}&\bar{2}&\bar{3}\\ \bar{0}&\bar{2}&\bar{4}\\ \bar{1}&\bar{4}&\bar{2}\end{pmatrix}\in M_n(\mathbb{Z}_5)$，$V_A=\mathrm{sol}(A\vec{x}=\vec{0})=\left\{\alpha\begin{pmatrix}\bar{1}\\ \bar{3}\\ \bar{1}\end{pmatrix}\,\middle|\,\alpha\in\mathbb{Z}_5\right\}$

2. 矩阵求逆

下述 $A\in M_n(F)$，求 A^{-1}:

① $(A\,|\,E)\xrightarrow{\text{初等行变换}}(E\,|\,A^{-1})$

② 设 k 是最小正整数 s.t. $\alpha_k A^k+\cdots+\alpha_1 A+\alpha_0 E=O$，$\alpha_i\in F$，$\alpha_k\neq 0,\alpha_0\neq 0$ → 对应多项式 f.

$\boxed{A^{-1}=-\alpha_0^{-1}(\alpha_1 E+\cdots+\alpha_k A^{k-1})}$ → 注：A 可逆 $\Leftrightarrow f(0)\neq 0$

用多项式

f 是满足 $f(A)=0$ 的最小次数的首1多项式

③ $AA^{\vee}=A^{\vee}A=|A|E \Rightarrow A^{-1}=\dfrac{A^{\vee}}{|A|}$

3. 伴随矩阵

$A\in M_n(F)$，$A^{\vee}=\begin{pmatrix}A_{11}&A_{21}&\cdots&A_{n1}\\ A_{12}&A_{22}&\cdots&A_{n2}\\ \vdots&\vdots&&\vdots\\ A_{1n}&A_{2n}&\cdots&A_{nn}\end{pmatrix}$，$A_{ij}$ 是代数余子式

$$\mathrm{rank}(A^{\vee})=\begin{cases}n, & \mathrm{rank}(A)=n\\ 1, & \mathrm{rank}(A)=n-1\\ 0, & \mathrm{rank}(A)<n-1\end{cases}$$

4. 行列式计算

(cut off line) …上三角或者下三角

①初等变换将行列式化成上三角或下三角

(注：做初等变换时，I：交换行的位置 $(-1)^{\square}$

II：行列式不变

III：行列式前乘以某个非零数.)

② 按行或列展开

③ 利用分块矩阵

④ 有递推关系 (适用n阶行列式)

注：以上方法可以混合使用. n阶行列式看不出规律，先以n=2, 3, 4找找规律，再回到n阶 (用数学归纳法证明)

5. 判断矩阵可逆

$A\in M_n(F)$, F是一个域

A可逆 $\Leftrightarrow |A|\neq 0 \Leftrightarrow$ A满秩 $\Leftrightarrow Ax=\vec{0}$ 只有零解.

$A=(a_{ij})\in F^{m\times n}$. A的k阶子式记为

$$M_A\begin{pmatrix} i_1 & i_2 & \cdots & i_k \\ j_1 & j_2 & \cdots & j_k \end{pmatrix}=\begin{vmatrix} a_{i_1,j_1} & a_{i_1,j_2} & \cdots & a_{i_1,j_k} \\ a_{i_2,j_1} & a_{i_2,j_2} & \cdots & a_{i_2,j_k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i_k,j_1} & a_{i_k,j_2} & \cdots & a_{i_k,j_k} \end{vmatrix}$$

命题 $A\in F^{m\times n}$、以下命题等价

① $\mathrm{rank}(A)=r$

② A中所有大于r阶的子式都等于0且存在一个r阶子式非0.

③ A中所有r+1阶的子式都等于0且存在一个r阶子式非0

6. 群

Def G集合 $\cdot : G\times G\to G$

① (封闭性) $\forall a,b\in G,\ ab\in G$ 半群 含幺半群 群

② (结合律)：$\forall a,b,c\in G,\ (ab)\cdot c=a\cdot(bc)$

③ 单位元：$\exists e\in G$, s.t. $\forall a\in G$, $ae=ea=a$

④ 逆元：$\forall a\in G$, $\exists b\in G$, s.t. $ab=ba=e$

子群: $H \le G \iff \forall a,b \in H,\ ab^{-1} \in H$

群同态: $\varphi: (G,\cdot,e) \longrightarrow (H,*,\varepsilon)$. $\forall a,b \in G$. $\varphi(ab)=\varphi(a)*\varphi(b)$

群同构 = 群同态 + 双射

阶 $(G,\cdot,e)$ 群. $g \in G$

若 $\exists n \in \mathbb{Z}^+$, s.t. $g^n = e$ (*) 称 g 是有限阶. 满足(*)最小正整数称为 g 的阶, 记为 $ord(g)$

否则称为无限阶.

$$\boxed{\text{若 } ord(a)=k,\quad ord(a^m)=\frac{k}{\gcd(m,k)}}$$

循环群 分类

设 $(G,\cdot,e)$ 是循环群, $|G|>1$

① 若 $|G|=\infty$, 则 $G \cong (\mathbb{Z},+,0)$

② 若 $|G|=n$, 则 $G \cong (\mathbb{Z}_n,+,\bar{0})$

$\mathbb{Z}=\langle 1\rangle$, $\mathbb{Z}_n = \langle \bar{1}\rangle = \langle \bar{k}\rangle$, $\gcd(k,n)=1$

环

Def $(R,+,0,\cdot,1)$, $0,1 \in R$, $0 \ne 1$, $+,\cdot$ 是 R 上二元运算

① $(R,+,0)$ 是交换群

② $(R,\cdot,1)$ 是含幺半群

③ 分配律 $\forall x,y,z \in R$, $x(y+z)=xy+xz$. $(x+y)z=xz+yz$

子环 验证 S 是 R 的子环, 只需验证

① S 对 $-$ 封闭

② S 对 $\cdot$ 封闭

③ $1_R \in S$

或者 $\begin{cases} S \text{ 对 } + \text{ 封闭} \\ S \text{ 对 } \cdot \text{ 封闭} \\ \pm 1_R \in S \end{cases}$

环同态: $\varphi (R,+,0_R,\cdot,1_R) \mapsto (S,+,0,\cdot,1_S)$

$\forall x,y \in R$, $\varphi(x+y)=\varphi(x)+\varphi(y)$, $\varphi(xy)=\varphi(x)\varphi(y)$. $\varphi(1_R)=1_S$

环同构 = 环同态 + 双射

整环 = 交换 + 无零因子

若 $a \in R$, $ab=0$ 则称 b 为 a 的右零因子

环 R 有特征, $char(R)=\begin{cases} 0, & \text{例 } \mathbb{Q}, \mathbb{R}. \\ p, & p \text{ 是个素数} \quad \text{例: } \mathbb{Z}_p \end{cases}$

$a\neq 0, b\neq 0,$

域：

域 = 交换环 + 非零元都可逆

一元多项式环

设 F 是域，则 $F[x]$ 是整环

$F[x]$ 中有带余除法，$\forall f, g \in F[x]$，$\exists!\ q, r \in F[x]$ s.t. $f = qg + r$，$\deg(r) < \deg(g)$

应用：

设 $f \in F[x]$，$A \in M_n(F)$，计算 $f(A)$