第十五次作业解答

习题 1. 设 $f = \overline{2}x^3 - x + \overline{2}$ 和 $g = \overline{2}x^2 + \overline{2}x$ 是 $\mathbb{Z}_4[x]$ 中的多项式。计算 fg , $\deg(fg)$ 和 $g(\overline{i})$, $i = \overline{0}, \overline{1}, \overline{2}, \overline{3}$ 。

解. 计算乘积 fg:

$$\begin{aligned} fg =& (\overline{2}x^3 - x + \overline{2})(\overline{2}x^2 + \overline{2}x) \\ =& \overline{2}x^3 \cdot \overline{2}x^2 + \overline{2}x^3 \cdot \overline{2}x + (-x) \cdot \overline{2}x^2 + (-x) \cdot \overline{2}x + \overline{2} \cdot \overline{2}x^2 + \overline{2} \cdot \overline{2}x. \\ =& \overline{2}x^3 + \overline{2}x^2 \end{aligned}$$

最高次项为 $\overline{2}x^3$，系数非零，故 $\deg(fg) = 3$。
计算 $g(\overline{i})$:

$$\begin{aligned} g(\overline{0}) &= \overline{2} \cdot \overline{0}^2 + \overline{2} \cdot \overline{0} = \overline{0}, \\ g(\overline{1}) &= \overline{2} \cdot \overline{1}^2 + \overline{2} \cdot \overline{1} = \overline{2} + \overline{2} = \overline{0}, \\ g(\overline{2}) &= \overline{2} \cdot \overline{2}^2 + \overline{2} \cdot \overline{2} = \overline{2} \cdot \overline{0} + \overline{0} = \overline{0}, \\ g(\overline{3}) &= \overline{2} \cdot \overline{3}^2 + \overline{2} \cdot \overline{3} = \overline{2} \cdot \overline{1} + \overline{2} \cdot \overline{3} = \overline{2} + \overline{6} = \overline{2} + \overline{2} = \overline{0}. \end{aligned}$$

所以 $g(\overline{i}) = \overline{0}$ 对所有 $i = \overline{0}, \overline{1}, \overline{2}, \overline{3}$。 □

习题 2. 设 $f = x^3 - x + \overline{2}$ 和 $g = \overline{2}x^2 + x$ 在 $\mathbb{Z}_5[x]$ 中。计算 $\mathrm{quo}(f, g, x)$ 和 $\mathrm{rem}(f, g, x)$。

解. 在 $\mathbb{Z}_5$ 上进行多项式除法。设商为 $q = ax + b$，余数为 $r = cx + d$，满足 $f = qg + r$。展开得

$x^3 - x + \overline{2} = (ax + b)(\overline{2}x^2 + x) + (cx + d) = \overline{2}ax^3 + (a + \overline{2}b)x^2 + (b + c)x + d.$

比较系数:

$$\begin{aligned} \overline{2}a &= \overline{1}, \\ a + \overline{2}b &= \overline{0}, \\ b + c &= -\overline{1} = \overline{4}, \\ d &= \overline{2}. \end{aligned}$$

由 $\overline{2}a = \overline{1}$ 得 $a = \overline{3}$(因为 $\overline{2}{\cdot}\overline{3} = \overline{1}$)。代入第二式:$\overline{3}{+}\overline{2}b = \overline{0} \Rightarrow \overline{2}b = \overline{2} \Rightarrow b = \overline{1}$。由第三式：$\overline{1} + c = \overline{4} \Rightarrow c = \overline{3}$。第四式：$d = \overline{2}$。故

$$\mathrm{quo}(f, g, x) = \overline{3}x + \overline{1}, \quad \mathrm{rem}(f, g, x) = \overline{3}x + \overline{2}.$$

□

习题 3. 设 $f(x) = x^2 + 2x - 3 \in \mathbb{Z}_7[x]$。计算 $f(\overline{5})$ 和 $f(A)$，其中 $A = \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} \end{pmatrix} \in \mathrm{M}_3(\mathbb{Z}_7)$。

解. 计算 $f(\overline{5})$：

$$f(\overline{5}) = \overline{5}^2 + 2 \cdot \overline{5} - 3 = \overline{25} + \overline{10} - \overline{3} = \overline{4} + \overline{3} - \overline{3} = \overline{4}.$$

计算 $f(A) = A^2 + 2A - 3I$（系数在 $\mathbb{Z}_7$ 中运算）：先计算

$$A^2 = \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} \end{pmatrix}^2 = \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{2} & \overline{1} & \overline{0} \\ \overline{1} & \overline{2} & \overline{1} \end{pmatrix}, \quad 2A = \begin{pmatrix} \overline{2} & \overline{0} & \overline{0} \\ \overline{2} & \overline{2} & \overline{0} \\ \overline{0} & \overline{2} & \overline{2} \end{pmatrix},$$

$$-3I = \overline{4}I = \begin{pmatrix} \overline{4} & \overline{0} & \overline{0} \\ \overline{0} & \overline{4} & \overline{0} \\ \overline{0} & \overline{0} & \overline{4} \end{pmatrix}.$$

相加得

$$f(A) = \begin{pmatrix} \overline{1}+\overline{2}+\overline{4} & \overline{0}+\overline{0}+\overline{0} & \overline{0}+\overline{0}+\overline{0} \\ \overline{2}+\overline{2}+\overline{0} & \overline{1}+\overline{2}+\overline{4} & \overline{0}+\overline{0}+\overline{0} \\ \overline{1}+\overline{0}+\overline{0} & \overline{2}+\overline{2}+\overline{0} & \overline{1}+\overline{2}+\overline{4} \end{pmatrix} = \begin{pmatrix} \overline{7} & \overline{0} & \overline{0} \\ \overline{4} & \overline{7} & \overline{0} \\ \overline{1} & \overline{4} & \overline{7} \end{pmatrix} = \begin{pmatrix} \overline{0} & \overline{0} & \overline{0} \\ \overline{4} & \overline{0} & \overline{0} \\ \overline{1} & \overline{4} & \overline{0} \end{pmatrix}.$$

□

习题 4. 设 $f = 236x^3 - 125x + 54$ 和 $g = 5000x^7 - 21x + 3367$ 是整系数多项式，$h = fg$。计算 $h(\overline{3})$，其中 $\overline{3} \in \mathbb{Z}_5$。

解. 利用多项式求值同态：$h(\overline{3}) = f(\overline{3})g(\overline{3})$。分别计算：

$$\begin{aligned} f(\overline{3}) &= \overline{236} \cdot \overline{3}^3 - \overline{125} \cdot \overline{3} + \overline{54} \\ &= \overline{1} \cdot \overline{2} - \overline{0} \cdot \overline{3} + \overline{4} = \overline{2} + \overline{4} = \overline{1}, \\ g(\overline{3}) &= \overline{5000} \cdot \overline{3}^7 - \overline{21} \cdot \overline{3} + \overline{3367} \\ &= \overline{0} \cdot \overline{2} - \overline{1} \cdot \overline{3} + \overline{2} = -\overline{3} + \overline{2} = \overline{2} + \overline{2} = \overline{4}. \end{aligned}$$

所以 $h(\overline{3}) = \overline{1} \cdot \overline{4} = \overline{4}$。 □

习题 5. 设 $A=(a_{i,j})\in \mathrm{M}_n(\mathbb{R})$, 其中 $a_{i,j}\in\mathbb{Z}$, $i,j\in\{1,2,\ldots,n\}$。再设 p 是素数，$\bar{a}_{i,j}$ 是 $a_{i,j}$ 在 $\mathbb{Z}_p$ 中关于同余关系的等价类。令 $\bar{A}=(\bar{a}_{i,j})\in\mathrm{M}_n(\mathbb{Z}_p)$。证明：如果 $\det(\bar{A})\neq 0$，则 $\det(A)\neq 0$。

证明. 考虑行列式函数 $\det:\mathrm{M}_n(\mathbb{Z})\to\mathbb{Z}$。对于矩阵 $A=(a_{ij})$，其行列式 $\det(A)$ 是矩阵元素的整系数多项式：

$$\det(A)=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{i=1}^{n}a_{i,\sigma(i)}.$$

设 $\varphi:\mathbb{Z}\to\mathbb{Z}_p$ 是模 p 同态，$\varphi(a)=\bar{a}=a+p\mathbb{Z}$。由于 φ 是环同态，它诱导出矩阵环的同态 $\Phi:\mathrm{M}_n(\mathbb{Z})\to\mathrm{M}_n(\mathbb{Z}_p)$，其中 $\Phi(A)=(\varphi(a_{ij}))=\bar{A}$。

对于行列式这个多项式函数，环同态与行列式计算可交换，即：

$$\varphi(\det(A))=\det(\Phi(A)).$$

这是因为行列式的计算只涉及加法、减法和乘法运算，而环同态保持这些运算。

已知 $\det(\bar{A})=\det(\Phi(A))\neq 0$ 在 $\mathbb{Z}_p$ 中，即 $\varphi(\det(A))\neq 0$。这意味着 $\det(A)$ 模 p 不为零，特别地，$\det(A)\neq 0$ (若 $\det(A)=0$，则 $\varphi(\det(A))=0$，矛盾)。因此，$\det(A)\neq 0$。 □

习题 6. (矩阵求逆的多项式) 设 F 是域，$A\in\mathrm{M}_n(F)$ 且 $A\neq O$。设

$$f(x)=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_1x+f_0\in F[x],\quad f_i\in F,$$

$f_n\neq 0$ 且 $f(A)=O$。

(i) 证明：如果 $f_0\neq 0$，则 A 可逆且

$$A^{-1}=-f_0^{-1}(f_nA^{n-1}+f_{n-1}A^{n-2}+\cdots+f_2A+f_1I).$$

(ii) 证明：如果 $f_0=0$，且对于任意 $F[x]$ 中次数小于 n 的非零多项式 $g(x)$，都有 $g(A)\neq O$，则 A 不可逆。

(iii) 设 $A^3-2A+12I=O$。证明：当 F 的特征不等于 2 和 3 时，A 可逆并求 A^{-1}。

证明. (i) 由 $f(A)=O$ 得

$$f_nA^n+f_{n-1}A^{n-1}+\cdots+f_1A+f_0I=O.$$

因为 $f_0 \neq 0$，可改写为

$$A(f_nA^{n-1} + f_{n-1}A^{n-2} + \cdots + f_1I) = -f_0I.$$

记 $B = f_nA^{n-1} + f_{n-1}A^{n-2} + \cdots + f_1I$，则 $AB = -f_0I$。由于 $-f_0I$ 可逆，且 A 与 B 可交换（均为 A 的多项式），故 A 可逆，且 $A^{-1} = -f_0^{-1}B$，即

$$A^{-1} = -f_0^{-1}(f_nA^{n-1} + f_{n-1}A^{n-2} + \cdots + f_2A + f_1I).$$

(ii) 反证法。假设 A 可逆。由 $f(A) = O$ 且 $f_0 = 0$ 得

$$f_nA^n + f_{n-1}A^{n-1} + \cdots + f_1A = O.$$

左乘 A^{-1} 得

$$f_nA^{n-1} + f_{n-1}A^{n-2} + \cdots + f_1I = O.$$

令 $g(x) = f_nx^{n-1} + f_{n-1}x^{n-2} + \cdots + f_1$，则 $g(A) = O$。若 $g(x)$ 非零，则与条件矛盾（因为 $\deg g < n$）。故 $g(x)$ 必为零多项式，即所有系数 $f_n, f_{n-1}, \ldots, f_1$ 均为零。但 $f_n \neq 0$，矛盾。因此 A 不可逆。

(iii) 给定 $A^3 - 2A + 12I = O$，即 $f(A) = O$，其中 $f(x) = x^3 - 2x + 12$。常数项 $f_0 = 12$。当 F 的特征不等于 2 和 3 时，$12 \neq 0$ 且可逆。由 (i) 知 A 可逆，且

$$A^{-1} = -12^{-1}(1 \cdot A^2 + 0 \cdot A + (-2)I) = -12^{-1}(A^2 - 2I) = \frac{1}{12}(2I - A^2).$$

□

进阶练习

进阶习题 1. 证明：域 K 上的 n 阶矩阵 A 是幂等矩阵当且仅当

$$\mathrm{rank}(A) + \mathrm{rank}(I - A) = n$$

分块矩阵方法. 我们对分块矩阵 $\begin{pmatrix} A & 0 \\ 0 & I-A \end{pmatrix}$ 依次做如下变换（表现为左乘或右乘可逆矩阵）：

$$\begin{pmatrix} I & 0 \\ I & I \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & I-A \end{pmatrix} = \begin{pmatrix} A & 0 \\ A & I-A \end{pmatrix}$$

$$\begin{pmatrix} A & 0 \\ A & I-A \end{pmatrix} \begin{pmatrix} I & I \\ 0 & I \end{pmatrix} = \begin{pmatrix} A & A \\ A & I \end{pmatrix}$$

$$\begin{pmatrix} I & -A \\ 0 & I \end{pmatrix}\begin{pmatrix} A & A \\ A & I \end{pmatrix} = \begin{pmatrix} A-A^2 & 0 \\ A & I \end{pmatrix}$$

$$\begin{pmatrix} A-A^2 & 0 \\ A & I \end{pmatrix}\begin{pmatrix} I & 0 \\ -A & I \end{pmatrix} = \begin{pmatrix} A-A^2 & 0 \\ 0 & I \end{pmatrix}$$

故

$$\operatorname{rank}\begin{pmatrix} A & 0 \\ 0 & I-A \end{pmatrix} = \operatorname{rank}\begin{pmatrix} A-A^2 & 0 \\ 0 & I \end{pmatrix}$$

即 $\operatorname{rank}(A)+\operatorname{rank}(I-A)=\operatorname{rank}(A-A^2)+n$。故 A 幂等等价于 $A=A^2$，等价于 $\operatorname{rank}(A-A^2)=0$，等价于 $\operatorname{rank}(A)+\operatorname{rank}(I-A)=n$。 □

解空间直和方法. 首先注意到 $\ker(A)\cap\ker(I-A)=\{0\}$，这是因为若 $x\in\ker(A)\cap\ker(I-A)$，则 $x=Ax=0$。

其次，对任意 $x\in\ker(A(I-A))$，$x=(I-A)x+Ax$，其中 $x_1=(I-A)x\in\ker(A)$，$x_2=Ax\in\ker(I-A)$。故

$$\ker(A(I-A))=\ker(A)\oplus\ker(I-A)$$

这意味着 $\operatorname{rank}(A)+\operatorname{rank}(I-A)=n$ 当且仅当 $\ker(A(I-A))=K^n$，当且仅当 $A(I-A)=0$，也即 A 是幂等矩阵。 □

进阶习题 2. 设 A 是域 K 上 $s\times n$ 矩阵，证明：$\operatorname{rank}(A)=r$ 当且仅当存在 $s\times r$ 列满秩矩阵 B 和 $r\times n$ 行满秩矩阵 C，使得 $A=BC$。

证明. **必要性：** 若 $\operatorname{rank}(A)=r$，由打洞引理，存在可逆矩阵 $P\in K^{s\times s}$ 和 $Q\in K^{n\times n}$，使得

$$A=P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}Q,$$

其中 I_r 为 r 阶单位矩阵。令 B 为 P 的前 r 列构成的 $s\times r$ 矩阵，C 为 Q 的前 r 行构成的 $r\times n$ 矩阵，则 $A=BC$。由于 P 可逆，B 列满秩；由于 Q 可逆，C 行满秩。

充分性： 若 $A=BC$，其中 B 列满秩，C 行满秩，则 $\operatorname{rank}(A)\leqslant\operatorname{rank}(B)=r$。再由 Sylvester 不等式，$\operatorname{rank}(A)\geqslant\operatorname{rank}(B)+\operatorname{rank}(C)-r=r$，故 $\operatorname{rank}(A)=r$。 □

进阶习题 3. 计算下述 n 阶行列式：

$$\begin{vmatrix} 0 & 2 & 3 & \cdots & n \\ 1 & 0 & 3 & \cdots & n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & 3 & \cdots & 0 \end{vmatrix}$$

解. 将行列式的第 j 列（$j=1,2,\ldots,n$）提取公因子 j，得

$$D_n = n! \cdot \begin{vmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{vmatrix}.$$

记上述行列式为 Δ_n。将 Δ_n 的所有行加到第一行，得

$$\Delta_n = \begin{vmatrix} n-1 & n-1 & n-1 & \cdots & n-1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{vmatrix} = (n-1) \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{vmatrix}.$$

再将第一行的 -1 倍分别加到第 $2,3,\ldots,n$ 行，得

$$\Delta_n = (n-1) \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{vmatrix} = (n-1)\cdot 1 \cdot (-1)^{n-1} = (n-1)(-1)^{n-1}.$$

因此，

$$D_n = n! \cdot \Delta_n = (-1)^{n-1}(n-1)n!.$$

□

加边法. 首先，从各列提取公因子：第 j 列可提取因子 j（$j=1,2,\ldots,n$），

得

$$D_n = n! \cdot \begin{vmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{vmatrix}.$$

记右边行列式为 Δ_n。构造 $n+1$ 阶行列式（加边法）

$$\Delta_{n+1} = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & 1 & \cdots & 0 \end{vmatrix},$$

按第一列展开知 $\Delta_{n+1} = \Delta_n$。对 Δ_{n+1} 作行变换：将第一行乘以 -1 加到第 2 至第 $n+1$ 行，得

$$\Delta_{n+1} = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ -1 & -1 & 0 & \cdots & 0 \\ -1 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \cdots & -1 \end{vmatrix}.$$

再作列变换：将第 2 列至第 $n+1$ 列都乘以 -1 加到第一列，得

$$\Delta_{n+1} = \begin{vmatrix} 1-n & 1 & 1 & \cdots & 1 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{vmatrix}.$$

这是一个上三角矩阵，其行列式为对角元的乘积：

$$\Delta_{n+1} = (1-n) \cdot (-1)^n = (-1)^{n-1}(n-1).$$

因此，

$$D_n = n! \cdot \Delta_n = n! \cdot \Delta_{n+1} = (-1)^{n-1}(n-1)n!.$$

□