第二周习题课

——作业讲解与知识扩展

一. 作业讲解

习题1 设 $p=(x-y)(x-z)+3x^2y^2z^2-x^3-2\in\mathbb{Z}[x,y,z]$

(i) 计算 p 的齐次分解.

(ii) 计算 $\deg_x(p)$, $\deg_y(p)$, $\deg_z(p)$ 和 $\deg(p)$.

解. (i) (第一学期第十七周讲义例2.12)

$p=h_6+h_5+h_4+h_3+h_2+h_1+h_0$. 其中

$h_6=3x^2y^2z^2$, $h_5=0$, $h_4=0$, $h_3=-x^3$, $h_2=x^2-xz-xy+yz$,

$h_1=0$, $h_0=-2$.

(ii) $\deg_x(p)=3$, $\deg_y(p)=2$, $\deg_z(p)=2$, $\deg(p)=6$

习题2. 后面讲

习题3. 设 $A=\begin{pmatrix}1 & 1 & \cdots & 1\\ \varepsilon_0 & \varepsilon_1 & \cdots & \varepsilon_{n-1}\\ \vdots & \vdots & \ddots & \vdots\\ \varepsilon_0^{n-1} & \varepsilon_1^{n-1} & \cdots & \varepsilon_{n-1}^{n-1}\end{pmatrix}$, 其中 $\varepsilon_1=e^{\frac{2\pi\sqrt{-1}}{n}}$, $\varepsilon_i=\varepsilon_1^i$, $i=0,\cdots,n-1$

验证 $A^{-1}=\frac{1}{n}\begin{pmatrix}1 & 1 & \cdots & 1\\ \varepsilon_0^{-1} & \varepsilon_1^{-1} & \cdots & \varepsilon_{n-1}^{-1}\\ \vdots & \vdots & \ddots & \vdots\\ \varepsilon_0^{-(n-1)} & \varepsilon_1^{-(n-1)} & \cdots & \varepsilon_{n-1}^{-(n-1)}\end{pmatrix}\doteq B$

证明. 设 $C=\begin{pmatrix}1 & 1 & \cdots & 1\\ \varepsilon_0 & \varepsilon_1 & \cdots & \varepsilon_{n-1}\\ \vdots & \vdots & \ddots & \vdots\\ \varepsilon_0^{n-1} & \varepsilon_1^{n-1} & \cdots & \varepsilon_{n-1}^{n-1}\end{pmatrix}\begin{pmatrix}1 & 1 & \cdots & 1\\ \varepsilon_0^{-1} & \varepsilon_1^{-1} & \cdots & \varepsilon_{n-1}^{-1}\\ \vdots & \vdots & \ddots & \vdots\\ \varepsilon_0^{-(n-1)} & \varepsilon_1^{-(n-1)} & \cdots & \varepsilon_{n-1}^{-(n-1)}\end{pmatrix}=AB$

计算 C 的 (i,j) 位置元素：

$$C_{ij}=\sum_{k=0}^{n-1}\varepsilon_k^{i-1}\varepsilon_{j-1}^{-k}=\sum_{k=0}^{n-1}\varepsilon_1^{(i-1)k}\varepsilon_1^{-(j-1)k}=\sum_{k=0}^{n-1}\varepsilon_1^{k(i-j)}$$

$$=\begin{cases}\sum_{k=0}^{n-1}1=n, & i=j\\ \frac{1-\varepsilon_1^{(i-j)n}}{1-\varepsilon_1^{i-j}}=0, & i\neq j\end{cases}$$

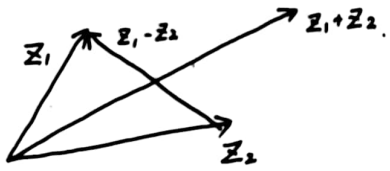
所以 $AB=nE_n$，即 $A(\frac{1}{n}B)=E_n$.

□

习题4. 设 $z_1,z_2\in\mathbb{C}$，证明：$|z_1+z_2|^2+|z_1-z_2|^2=2(|z_1|^2+|z_2|^2)$.
并说明其几何意义.

证明. 直接设 $z_1=a_1+b_1i$，$z_2=a_2+b_2i$，验证上式.

几何意义.



平行四边形四条边的平方和
等于两对角线长度的平方和.

习题5 设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbb{Z}[x]$，若 $\alpha=\frac{a}{b}$ 为其根，其中 $a,b\in\mathbb{Z}$，且 $\gcd(a,b)=1$. 证明：$a\mid a_0$，$b\mid a_n$.

证明. 因为 $f(\frac{a}{b})=0$，所以

$$a_n\left(\frac{a}{b}\right)^n+a_{n-1}\left(\frac{a}{b}\right)^{n-1}+\cdots+a_1\left(\frac{a}{b}\right)+a_0=0$$

则 $a_na^n+a_{n-1}a^{n-1}b+\cdots+a_1ab^{n-1}+a_0b^n=0$. 所以

$$a_na^n=-(a_{n-1}a^{n-1}b+\cdots+a_0b^n)=-b(a_{n-1}a^{n-1}+\cdots+a_0b^{n-1}).$$

则 $b\mid a_na^n$，因为 $\gcd(a,b)=1$，所以 $\gcd(a^n,b)=1$，则 $b\mid a_n$.
同理 $a\mid a_0$.

□

补充. 条件如上，证明：$f(x)=(bx-a)q(x)$，且 $q(x)\in\mathbb{Z}[x]$.

证明. 因为 $\frac{a}{b}$ 为 $f(x)$ 的根，所以存在 $g(x)\in\mathbb{Q}[x]$. 使得

$$f(x)=(x-\frac{a}{b})g(x).$$

即 $f(x)=(bx-a)\cdot(\frac{1}{b}g(x))$. 把 $g(x)$ 写为 $g(x)=\frac{t}{s}p(x)$，$p(x)$ 为本原多项式. 则 $f(x)=\frac{t}{bs}(bx-a)p(x)$. 由高斯引理可知 $(bx-a)p(x)$ 为本原多项式. 设 $\frac{t}{bs}=\frac{c_1}{c_2}$，$\gcd(c_1,c_2)=1$，则

$$f(x)=\frac{c_1}{c_2}[(bx-a)p(x)],$$

因为 $f(x)$ 为整系数多项式，$(bx-a)p(x)$ 为本原多项式，所以 $c_2=\pm1$，则 $\frac{c_1}{c_2}p(x)\in\mathbb{Z}[x]$，所以 $f(x)=(bx-a)q(x)$，其中 $q(x)=\frac{c_1}{c_2}p(x)\in\mathbb{Z}[x]$. □

推论. 设 $q(x)=b_{n-1}x^{n-1}+\cdots+b_1x+b_0$，则

$$(bx-a)(b_{n-1}x^{n-1}+\cdots+b_1x+b_0)=a_nx^n+\cdots+a_1x+a_0,$$

比较系数，$bb_{n-1}=a_n$，$-ab_0=a_0$，则 $b\mid a_n$，$a\mid a_0$. □

习题6. 和例4.19一样，用核按分解和维数公式.

二. 拉格朗日插值.

习题2. 求 $\mathbb{Q}[x]$ 中次数小于3的多项式，使得 $f(0)=2$，$f(1)=1$，$f(3)=0$.

解. 待定系数法：设 $f(x)=a_0+a_1x+a_2x^2$，代入条件可得

$$\begin{cases} a_0 = 2 \\ a_0+a_1\cdot1+a_2\cdot1^2=1 \\ a_0+a_1\cdot3+a_2\cdot3^2=0 \end{cases},$$

解得 $a_0=2$，$a_1=-\frac{7}{6}$，$a_2=\frac{1}{6}$，所以 $f(x)=\frac{1}{6}x^2-\frac{7}{6}x+2$.

□

问题：给定 n 个点 $(x_1,y_1),\cdots,(x_n,y_n)$，$x_i\neq x_j$，是否存在多项式 $f(x)$，使得 $f(x_i)=y_i$，$i=1,\cdots,n$？

定理　设有 n 个点 $(x_1,y_1),\cdots,(x_n,y_n)\in\mathbb{R}^2$，$x_i\neq x_j$，则存在 $f(x)\in\mathbb{R}[x]$ 满足 $f(x_i)=y_i$，$i=1,\cdots,n$，且 $\deg f<n$，而且满足该条件的多项式 $f(x)$ 是唯一的.

证明. 设 $f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$，代入 n 个点可得 n 个方程：

$$\begin{cases} a_0+a_1x_1+\cdots+a_{n-1}x_1^{n-1}=y_1\\ a_0+a_1x_2+\cdots+a_{n-1}x_2^{n-1}=y_2\\ \vdots\\ a_0+a_1x_n+\cdots+a_{n-1}x_n^{n-1}=y_n \end{cases}$$

即 $\begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1}\\ 1 & x_2 & \cdots & x_2^{n-1}\\ & \vdots & & \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix}\begin{pmatrix} a_0\\ a_1\\ \vdots\\ a_n \end{pmatrix}=\begin{pmatrix} y_1\\ y_2\\ \vdots\\ y_n \end{pmatrix}$，因为 A 为范德蒙矩阵，

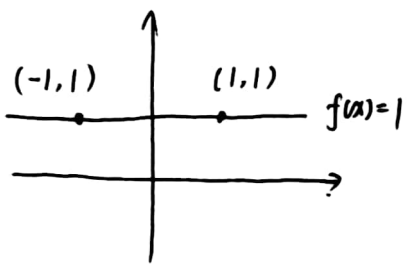
A

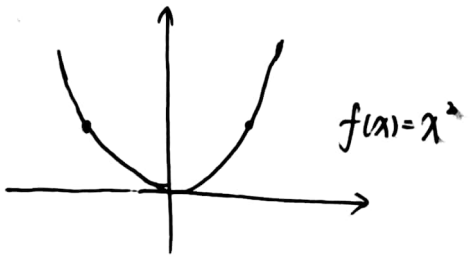
所以 A 可逆，则方程存在唯一解 $\begin{pmatrix} a_0\\ a_1\\ \vdots\\ a_n \end{pmatrix}=A^{-1}\begin{pmatrix} y_1\\ y_2\\ \vdots\\ y_n \end{pmatrix}$.

则 $f(x)$ 存在且唯一. □

注. 如果对 $f(x)$ 的次数没有限制，则 $f(x)$ 不一定唯一.

比如





拉格朗日插值公式：设 $(x_1, y_1), \cdots, (x_n, y_n) \in \mathbb{R}^n$，$x_i \neq x_j$，$i \neq j$.

构造

$$f_1(x) = \frac{(x-x_2)(x-x_3)\cdots(x-x_n)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)}$$

$$f_2(x) = \frac{(x-x_1)(x-x_3)\cdots(x-x_n)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_n)}$$

$$\vdots$$

$$f_n(x) = \frac{(x-x_1)(x-x_2)\cdots(x-x_{n-1})}{(x_n-x_1)(x_n-x_2)\cdots(x_n-x_{n-1})}$$

令 $f(x) = y_1 f_1(x) + \cdots + y_n f_n(x)$，则 $f(x_i) = y_i$，$i = 1, \cdots, n$.

证明. 可以验证对于 $i = 1, \cdots, n$，有

$$f_i(x_j) = \begin{cases} 1 & j = i \\ 0 & j \neq i \end{cases}.$$

所以 $f(x_i) = y_i \cdot f_i(x_i) = y_i$，$i = 1, 2, \cdots, n$.

例（习题2） $f(0) = 2$，$f(1) = 1$，$f(3) = 0$.

解. 构造：

$$f_1(x) = \frac{(x-1)(x-3)}{(0-1)(0-3)} = \frac{x^2-4x+3}{3}$$

$$f_2(x) = \frac{(x-0)(x-3)}{(1-0)(1-3)} = \frac{x^2-3x}{-2}$$

$$f_3(x) = \frac{(x-0)(x-1)}{(3-0)(3-1)} = \frac{x^2-x}{6}$$

则 $f(x) = 2 \cdot f_1(x) + 1 \cdot f_2(x) + 0 \cdot f_3(x)$.

$$= \frac{x^2-7x+12}{6}.$$

□

三. 中国剩余定理

问题 求整数 y，满足

$$\begin{cases} y \equiv 2 \mod 3 \\ y \equiv 3 \mod 5 \\ y \equiv 2 \mod 7 \end{cases}$$

实际上，满足此条件整数集合为

$$\{23 + 105k \mid k \in \mathbb{Z}\}$$

定理（中国剩余定理）设 $m_1, \cdots, m_s \in \mathbb{Z}^+ \setminus \{1\}$ 两两互素，对于任意 $a_1, a_2, \cdots, a_s \in \mathbb{Z}$，都存在 $y \in \mathbb{Z}$，使得

$$\begin{cases} y \equiv a_1 \mod m_1 \\ y \equiv a_2 \mod m_2 \\ \vdots \\ y \equiv a_k \mod m_s \end{cases}$$

而且满足该条件的整数集合可以写为

（证明类似拉格朗日插值公式） $\{y + (m_1 \cdots m_s) \cdot k \mid k \in \mathbb{Z}\}$

证明. 对于 $i = 1, \cdots, s$，构造 $y_i \in \mathbb{Z}$，满足

$$\begin{cases} y_i \equiv 1 \mod m_i \\ y_i \equiv 0 \mod m_j, \ j \neq i \end{cases}$$

构造方法如下：设 $m = m_1 \cdots m_s$，$\hat{m}_i = \frac{m}{m_i} \in \mathbb{Z}$，因为 $m_1, \cdots, m_k$ 两两互素，所以 $\gcd(m_i, \hat{m}_i) = 1$，$i = 1, \cdots, s$，所以存在 $u_i, v_i \in \mathbb{Z}$，使得

$$\hat{m}_i u_i + m_i v_i = 1,$$

令 $y_i = \hat{m}_i u_i$，则 $y_i \equiv 1 \mod m_i$，而且当 $j \neq i$ 时，$m_j \mid \hat{m}_i$，所以

$$y_i \equiv 0 \mod m_j, \ j \neq i.$$

令 $y = a_1 y_1 + \cdots + a_k y_k$，则 $y \equiv a_i \mod m_i$，$i = 1, \cdots, s$.

下证 $\{y+(m_1\cdots m_s)k \mid k\in\mathbb{Z}\}$ 为所有满足条件的整数：首先，y 满足 $y\equiv a_i \mod m_i$ 可以推出

$$y+(m_1\cdots m_s)k \equiv a_i \mod m_i \quad i=1,\cdots,n$$

所以整数 $y+(m_1\cdots m_s)k$ ($k\in\mathbb{Z}$) 也满足条件. 反之，假设 y' 满足

$$y'\equiv a_i \mod m_i$$

则 $y\equiv y' \mod m_i$，所以 $m_i \mid (y'-y)$，$i=1,\cdots,s$，因为 $m_1,\cdots,m_s$ 两两互素，所以 $m_1m_2\cdots m_s \mid (y'-y)$，所以存在 $k\in\mathbb{Z}$，使得

$$y'-y=(m_1\cdots m_s)k,$$

即 $y'=y+(m_1\cdots m_s)k\in\{y+(m_1\cdots m_s)k \mid k\in\mathbb{Z}\}$. 于是

$$\{y+(m_1\cdots m_s)k \mid k\in\mathbb{Z}\}$$

是所有满足条件的集合. □