高等代数期中讲座

王尔卓

2022 年 11 月 4 日

目录

1 例题讲解

1.1 行列式

我们先来看看去年第一次月考的第三道题: 设 $\sum_{i=1}^{n} x_i^2 = 1$，试求矩阵 $(a_{ij})_{n\times n}$ 的行列式，其中 $a_{ij} = \delta_{ij} - x_i x_j, 1 \leq, i, j \leq n$

Proof: 拿到题第一感觉是题的答案是个定值，我们想先去猜测答案: 当 $n = 2$ 时，$\det(a_{ij}) = (1-x_1^2)(1-x_2^2) - (-x_1x_2)(-x_2x_1) = 1 - x_1^2 - x_2^2 = 0$, 因此我们想用归纳法证明对任意正整数 n，该行列式值为零。

假设对所有小于 n 的数该结论成立 $(n \geq 3)$，对于 n 的情况，不难发现如果 x_i 中某个取值为 0，那么该行列式取值会自动退化为某个小于 n 的情况，因此我们不妨设 x_i 全不为 0。

将该矩阵写出来以后，我们发现这个矩阵每一行元素相同的系数比较多，我们将第 i 行的 x_i 提出来后可以简化行列式的计算:

$$\begin{vmatrix} 1-x_1x_1 & -x_1x_2 & \dots & -x_1x_n \\ -x_2x_1 & \ddots & & -x_2x_n \\ \vdots & & \ddots & \vdots \\ -x_nx_1 & \dots & & 1-x_nx_n \end{vmatrix} = x_1x_2\dots x_n \begin{vmatrix} x_1^{-1}-x_1 & -x_2 & \dots & -x_n \\ -x_1 & \ddots & & -x_n \\ \vdots & & \ddots & \vdots \\ -x_1 & \dots & & x_n^{-1}-x_n \end{vmatrix}$$

此时每一行彼此相同的项比较多，我们用第一行去减后面所有的行, 再用后 $n-1$ 行消去第一行的后 $n-1$ 个元素得到:

$$= x_1\dots x_n \begin{vmatrix} x_1^{-1}-x_1 & -x_2 & \dots & -x_n \\ -x_1^{-1} & x_2^{-1} & & 0 \\ \vdots & & \ddots & \\ -x_1^{-1} & 0 & & x_n^{-1} \end{vmatrix} = x_1\dots x_n \begin{vmatrix} \dfrac{1-\sum_{i=1}^n x_i^2}{x_1} & \dots & 0 & 0 \\ -x_1^{-1} & x_2^{-1} & & 0 \\ \vdots & & \ddots & \\ -x_1^{-1} & \dots & & x_n^{-1} \end{vmatrix} = 0$$

证毕!

$\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$

上面一道题是一个比较具有技巧性的习题，下面这个题，我们想推广去年第一次月考第二题，而这正是教材第二章补充题 4 的 (4):

$$D_n = \begin{vmatrix} x & y & y & \dots & y \\ z & x & y & & \vdots \\ z & z & x & & \\ \vdots & & & \ddots & y \\ z & \dots & & z & x \end{vmatrix} = \begin{cases} \dfrac{(x-z)^n y - (x-y)^n z}{y-z} & \text{如果 } y \neq z \\ (x+(n-1)y)(x-y)^{n-1} & \text{如果 } y = z \end{cases} \tag{1}$$

Proof: 我们先讨论 $y = z$ 的情况，注意到此时每一行元素和都相等，我们将后 $n-1$ 列加

到第一列，然后提出来第一列，然后用第一列消去后面的列得到:

$$\begin{vmatrix} x & y & y & \dots & y \\ y & x & y & & \vdots \\ y & y & x & & \\ \vdots & & & \ddots & y \\ y & \dots & & y & x \end{vmatrix} = (x+(n-1)y) \begin{vmatrix} 1 & y & y & \dots & y \\ 1 & x & y & & \vdots \\ 1 & y & x & & \\ \vdots & & & \ddots & y \\ 1 & \dots & & y & x \end{vmatrix}$$

$$= (x+(n-1)y) \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & x-y & 0 & & \vdots \\ 1 & 0 & x-y & & \\ \vdots & & & \ddots & 0 \\ 1 & \dots & & 0 & x-y \end{vmatrix} = (x+(n-1)y)(x-y)^{n-1}$$

对于 $y \neq z$ 的情况，如果 y, z 中有一个为 0, 则结论是显然的，现考虑 y, z 都不为 0 的情况。我们想用递推的方法解决这个问题，因此消项的时候尽量避免触及右下角 $n-1$ 阶的子矩阵，先用第二行去减第一行, 再用第一行展开得到:

$$D_n = \begin{vmatrix} x & y & y & \dots & y \\ z & x & y & & \vdots \\ z & z & x & & \\ \vdots & & & \ddots & y \\ z & \dots & & z & x \end{vmatrix} = \begin{vmatrix} x-z & y-x & 0 & \dots & 0 \\ z & x & y & & \vdots \\ z & z & x & & \\ \vdots & & & \ddots & y \\ z & \dots & & z & x \end{vmatrix} = (x-z)D_{n-1} - (y-x)\det M$$

其中 $n-1$ 阶矩阵 M 形如:

$$M = \begin{bmatrix} z & y & y & \dots & y \\ z & x & y & & \vdots \\ z & z & x & & \\ \vdots & & & \ddots & y \\ z & \dots & & z & x \end{bmatrix}$$

用第一行去减后面 $n-2$ 行以后发现可以直接计算出 $\det M = z(x-y)^{n-2}$, 从而对于 $n \geq 3$ 我们得到了: $D_n = (x-z)D_{n-1} + z(x-y)^{n-1}$, 将 D_n 用其对应矩阵去转置以后的矩阵再如上计算一次得到:$D_n = (x-y)D_{n-1} + y(x-z)^{n-1}$, 将两个方程联立消去 D_n 即可得到:

$$D_{n-1} = \frac{(x-z)^{n-1}y - (x-y)^{n-1}z}{y-z}, \quad \forall n \geq 3$$

将 n 用 $n+1$ 代换即可得到原来的结论。

对于这种比较有规律的矩阵的行列式的计算，值得掌握的还有第二章第 18 题的 (3) 和 (4)，因为他们分别对应了二阶线性递推数列以及切比雪夫多项式。

$\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$

最后对于行列式的运算，我们看一道简单且深刻的习题，考虑一个多项式 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{C}[x]$，我们定义其友矩阵 $C_{f(x)}$ 为：

$$C_{f(x)}=\begin{bmatrix}0&0&0&\dots&-a_0\\1&0&0&&-a_1\\0&1&0&&\vdots\\\vdots&&&\ddots&-a_{n-2}\\0&\dots&&1&-a_{n-1}\end{bmatrix}$$

试证明 $|\lambda E_n-C_{f(x)}|=f(\lambda)$。

事实上友矩阵源自于有理标准型，对于一个域 F 上的 n 维线性空间 V, 其上一个线性变换 $\mathcal{A}$ 会诱导出一个 $F[x]-$ 模，我们通过研究这个 $F[x]-$ 模的结构 (也就是通过主理想整环上的有限生成模结构定理)，最终得到每一个域 F 上的矩阵都能和一个分块对角阵相似，而且分块对角阵的每一块形如某个多项式的友矩阵，从上至下，这些友矩阵对应的多项式有整除的递进关系，即满足 $a_1(x)|a_2(x)|\dots|a_s(x)$。在此题中，我们只想讨论一个友矩阵的特征多项式正好是他自己。

Proof: 对 $n=1,2$ 的情况，不难验证其成立，对 n 归纳，假设对所有小于 n 的数成立，则按第一列展开有, 由归纳假设:

$$|\lambda E_n-C_{f(x)}|=\begin{vmatrix}\lambda&0&0&\dots&a_0\\-1&\lambda&0&&a_1\\0&-1&\lambda&&\vdots\\\vdots&&&\ddots&a_{n-2}\\0&\dots&&-1&\lambda+a_{n-1}\end{vmatrix}=\lambda(a_1+\cdots+a_{n-1}\lambda^{n-2}+\lambda^{n-1})+$$

$$a_0(-1)^{n-2}(-1)^{n-2}=f(\lambda)$$

1.2 矩阵的秩与线性方程组

在此我们讨论一道大一上学期高等代数的期末考试题:

判断 $n\geq 3$ 时线性方程组:

$$\begin{bmatrix}1+\lambda&1&1&\dots&1\\1&1+\lambda&1&&1\\1&1&1+\lambda&&\vdots\\\vdots&&&\ddots&1\\1&\dots&&1&1+\lambda\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\\\vdots\\x_n\end{bmatrix}=\begin{bmatrix}n-1\\n-1\\n-1\\\vdots\\n-1+\lambda\end{bmatrix}$$

何时无解，有唯一解，有无穷多个解，在有无穷多解时求出通解。

Proof: 由 (1) 式，该线性方程组系数矩阵的行列式为:$(\lambda+n)\lambda^{n-1}$，从而在 $\lambda\neq -n,0$ 时，由克莱默法则，该方程有唯一解。

$\lambda=-n$ 时，将后 $n-1$ 行加到第一行得到 $0=n-2$，从而该方程无解。

当 $\lambda = -0$，即求 $x_1 + \cdots + x_n = n - 1$ 的通解，其通解可以写为一个特解 $\alpha = (n-1, 0, \ldots, 0)^T$ 加上其次线性方程组 $x_1 + x_2 \cdots + x_n = 0$ 的基础解系的线性组合，不难找出一个基础解系为 $\alpha_1 = (1, 0, \ldots, 0, -1)^T, \alpha_2 = (0, 1, \ldots, 0, -1)^T, \ldots, \alpha_{n-1} = (0, 0, \ldots, 1, -1)^T$，则通解为:

$$\alpha + k_1\alpha_1 + \cdots + k_{n-1}\alpha_{n-1}$$

$\sim \quad \sim \quad \sim \quad \sim \quad \sim \quad \sim \quad \sim \quad \sim \quad \sim$

其次我们来讨论一道与矩阵的秩有关的问题，考虑一个复数域 $\mathbb{C}$ 上的 n 级矩阵 A, 我们想证明 $rank(A^n) = rank(A^{n+1})$。

Proof: 事实上这个问题如果引入若当标准型后是平凡的，对于一个 n 级矩阵，将其相似为若当标准型后，其特征值非零的分块再累乘后依然满秩，而特征值为 0 的分块在每累乘一次秩会减少 1，经过 n 次累乘后所有特征值为 0 的分块都会变成 0，从而得证。

但是我们目前没有如此犀利的工具，为了解决这个问题，我们需要采用一些技巧，由于满秩是结论显然，下面只考虑非满秩的情况。

考虑矩阵的秩在累乘时逐项递减，即 $0 \leq rank(A^{n+1}) \leq \cdots \leq rank(A^2) \leq rank(A) \leq n-1$, 因此他们彼此之间的不等号不能全都不成立，也就是说如果 $rank(A^{n+1}) < \cdots < rank(A^2) < rank(A)$，则 $rank(A) >= n$，与非满秩矛盾。从而必有 $k \in \mathbb{Z}$ 使得 $rank(A^k) = rank(A^{k+1})$，此时我们只需证如果 $rank(A^m) = rank(A^{m+1})$, 则 $rank(A^{m+1}) = rank(A^{m+2})$, 这样就能归纳得到:$rank(A^n) = rank(A^{n+1})$。

由于 $rank(A^m) = rank(A^{m+1})$，则 $A^m\vec{x} = 0$ 和 $A^{m+1}\vec{x} = 0$ 基础解系的向量个数相同，又因为左边方程组的解包含于右边方程组的解，因此如果如果考虑左边方程组的基础解系，其一定也是右边方程组的基础解系，从而两个向量组有相同的解。

再考虑线性方程组 $A^{m+2}\vec{x} = 0$, 如果 $\vec{x_0}$ 为其解，那么 $A\vec{x_0}$ 是 $A^{m+1}\vec{x} = 0$ 的解，从而 $A\vec{x_0}$ 是 $A^m\vec{x} = 0$ 的解，从而 $\vec{x_0}$ 是 $A^{m+1}\vec{x} = 0$ 的解，则 $A^{m+2}\vec{x} = 0$ 和 $A^{m+1}\vec{x} = 0$ 这两个方程组同解，从而有相同的基础解系，再利用基础解系的向量个数加矩阵的秩等于 n, 得到 $rank(A^{m+1}) = rank(A^{m+2})$，证毕!

$\sim \quad \sim \quad \sim \quad \sim \quad \sim \quad \sim \quad \sim \quad \sim \quad \sim$

下面我们再来看一道有关基础解系的问题，对于 n 级矩阵 A, 考虑线性方程组 $A\vec{x} = 0$ 的基础解系:$\alpha_1, \ldots, \alpha_t$, 如果 l 为奇数，则

$$\beta_1 = \alpha_1 + \alpha_2, \ldots, \beta_{l-1} = \alpha_{l-1} + \alpha_l, \beta_l = \alpha_l + \alpha_1$$

也为该方程组的基础解系。

注意到:

$$[\beta_1, \beta_2, \ldots, \beta_t] = [\alpha_1, \alpha_2 \ldots, \alpha_t] \begin{bmatrix} 1 & 0 & 0 & \ldots & 1 \\ 1 & 1 & 0 & & \\ 0 & 1 & \ddots & & \vdots \\ \vdots & & & 1 & \\ 0 & \ldots & 0 & 1 & 1 \end{bmatrix}$$

我们记右侧矩阵的行列式为 D_t，如果能证明 n 为奇数是非零，即可得到量个向量组等价，进而证明该结论。

我们考虑 D_t 的递推关系，按第一行展开有:

$$D_t = D_{t-1} + (-1)^{t-1}$$

直接计算得到 $D_2 = 0$，通过递推可以得到所有奇数项取值为 1, 从而证明了该结论。

$\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$ $\sim$

我们最后试着举出 $sylvester$ 不等式等号不成立的例子。

我们都知道 $sylvester$ 不等式是指对于 n 级矩阵 A, B, $r(AB) \geq r(A) + r(B) - n$, 这个不等式蕴含着若 $AB = O$, 则 $r(A) + r(B) \leq n$，因此后者等号不成立时自然有前者等号不成立。

而对于 n 级矩阵 A 对应的线性方程组 $A\vec{x} = 0$，其系数矩阵的秩与基础解系向量个数之和为 n，因此只需要取 A 并非构成基础解系的一组向量即可使等号不成立，譬如:

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

1.3 解析几何

我们先来梳理几个解析几何里有关距离的公式，这些距离公式不需要死记，了解证明思路后考场现推也行，不过能熟记最好，能节约一些时间。

1. 点 $P(x_0, y_0, z_0)$ 到平面 $\pi : Ax + By + Cz + D = 0$ 的距离公式:

$$d = \frac{|Ax_0 + By_0 + Cz_0 + D|}{\sqrt{A^2 + B^2 + C^2}}$$

证明思路是找该平面的法向量然后做内积。

2. 点 $P_1(x_1, y_1, z_1)$ 到直线 $\dfrac{x - x_0}{m} = \dfrac{y - y_0}{l} = \dfrac{z - z_0}{n}$ 的距离公式:

$$d = \frac{|\vec{PP_0} \times \vec{v}|}{|\vec{v}|}$$

其中 $P_0 = (x_0, y_0, z_0)$, $\vec{v}$ 为直线的方向向量, 证明思路是由于两向量外积的模长是这两个向量构成的平行四边形的面积，将该直线方向向量模长除去，得到的就是点 P_1 到该直线的距离。

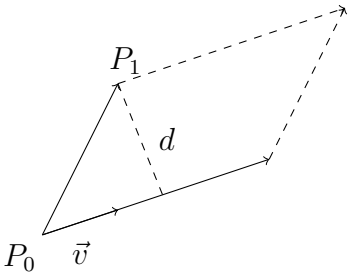

图 1: 点到直线距离公式

3. 两直线间距离公式: 两条直线间的距离通常定义为在这两条直线上分别任取一点, 这两点之间距离的最小值即为两直线之间的距离，而通常解析几何教材中并未证明这一定义 well-defined，即一定能取到两点使其之间距离达到最小，因此这里我不打算重述通常解析几何教材里并不严谨的解决方法，而采用线性代数的手段去作处理。

Proof: 考虑两条直线 $\frac{x-x_0}{m}=\frac{y-y_0}{l}=\frac{z-z_0}{n}$ 和 $\frac{x-x_1}{a}=\frac{y-y_1}{b}=\frac{z-z_1}{c}$, 不妨假设两者不平行，因为平行时可以转化为点到直线的距离公式去计算，将两者用参数方程表示为:

$$\begin{cases} x=x_0+lt \\ y=y_0+mt \\ z=z_0+nt \end{cases} \qquad \begin{cases} x=x_1+as \\ y=y_1+bs \\ z=z_1+cs \end{cases} \qquad s,t\in\mathbb{R}$$

则分别取一点，记 $x_0-x_1=x_2, y_0-y_0=y_2, z_0-z_1=z_2$ 得到两点之间距离的平方为:

$$d^2=(x_2+lt-as)^2+(y_2+mt-bs)^2+(z_2+nt-cs)^2$$

考虑关于变量 s,t 的线性方程组:

$$\begin{cases} as-lt=x_2 \\ bs-mt=y_2 \\ cs-nt=z_2 \end{cases}$$

将该方程左侧系数矩阵记为 A，右侧列向量记为 $\beta=[x_2,y_2,z_2]^T$，记 $\alpha=[s,t]^T$, 由丘维生高等代数上册 4.6 节例 18、19 或者王萼芳高等代数第九章第 7 节 (即线性方程组的最小二乘解)，d 取得最小值当且仅当

$$A^TA\alpha=A^T\beta$$

即为:

$$\begin{bmatrix} a^2+b^2+c^2 & -(al+bm+cn) \\ -(al+bm+cn) & l^2+m^2+n^2 \end{bmatrix}\begin{bmatrix} s \\ t \end{bmatrix}=\begin{bmatrix} ax_2+by_2+cz_2 \\ -(lx_2+my_2+nz_2) \end{bmatrix}$$

解得:

$$s=\frac{(ax_2+by_2+cz_2)(l^2+m^2+n^2)-(al+bm+cn)(lx_2+my_2+nz_2)}{(a^2+b^2+c^2)(l^2+m^2+n^2)-(al+bm+cn)^2}$$

$$t=\frac{-(a^2+b^2+c^2)(lx_2+my_2+nz_2)+(ax_2+by_2+cz_2)(al+bm+cn)}{(a^2+b^2+c^2)(l^2+m^2+n^2)-(al+bm+cn)^2}$$

将 s,t 代入 d^2 表达式中即可得到结论，这个解法的优势在于可以轻易的推广的更高维的情况，而解析几何中的很多论证在更高维时我们没法从几何直观去入手了, 同时这个解法 s,t 代表的两点确定了公垂线，所以我们也一举多得的求出了公垂线的方程，而且由于两直线相交当且仅当他们之间距离为 0，所以我们也得到了两直线是否相交的判定条件。

有关解析几何中各种夹角的计算，应该是高考考查的重点，这里就不赘述了，我们来梳理一下柱面和锥面方程的求解。

4. 考虑一个柱面，其准线为 $\begin{cases} F(x,y,z)=0 \\ G(x,y,z)=0 \end{cases}$，母线方向已知为 $\vec{\alpha}=(m,n,l)$, 设柱面上一点为 (x,y,z), 则这一点要与准线上一点 (x_1,y_1,z_1) 形成母线，从而列出三个方程:

$$\begin{cases} F(x_1,y_1,z_1)=0 \\ G(x_1,y_1,z_1)=0 \\ \dfrac{x-x_1}{m}=\dfrac{y-y_1}{l}=\dfrac{z-z_1}{n} \end{cases}$$

将三者联立消去 (x_1,y_1,z_1) 即可得到柱面方程。

5. 考虑一个锥面，其准线为 $\begin{cases} F(x,y,z)=0 \\ G(x,y,z)=0 \end{cases}$，顶点已知为 (x_0,y_0,z_0), 设锥面上一点为 (x,y,z), 则这存在准线上一点 (x_1,y_1,z_1) 使得该点与顶点的连线与 $(x-x_0,y-y_0,z-z_0)$ 共线，从而列出三个方程:

$$\begin{cases} F(x_1,y_1,z_1)=0 \\ G(x_1,y_1,z_1)=0 \\ \dfrac{x-x_0}{x_1-x_0}=\dfrac{y-y_0}{y_1-y_0}=\dfrac{z-z_0}{z_1-z_0} \end{cases}$$

将三者联立消去 (x_1,y_1,z_1) 即可得到锥面方程。

2 补充材料

对于本次讲座补充材料，感兴趣的同学可以尝试阅读，这些是我在学习过程中所遇到的高等代数的一些应用，意图为同学们展现高等代数不单单是一门需要考试学科，更是一个在不同方向上都很好用的刻画不同数学对象的工具，不过囿于的我个人能力，我只能描绘一些我感兴趣的方向。

2.1 范德蒙行列式与牛顿公式

考虑一个多项式 $f(x)=(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)\in\mathbb{C}[x],\alpha_i\in\mathbb{C}$，定义这个多项式的判别式为:

$$d(f)=\prod_{1\le r<s\le n}(\alpha_r-\alpha_s)^2$$

多项式的判别式是一个很重要的概念，一方面他能判定一个多项式是否有重根，其次，在伽罗瓦理论中，对于有一个 n 次有理系数多项式，其伽罗瓦群是 A_n 的子群当且仅当其判别式是一个有理数的平方，而且通过计算分圆多项式的判别式，我们可以证明代数数论中Kronecker-Weber定理的二次域情况。而本则材料我们想通过范德蒙行列式将多项式的判别式与等幂和建立联系，并通过牛顿公式计算三次有理系数多项式的判别式。

若记 $s_k=\sum_{i=1}^n\alpha_i^k$, 由范德蒙行列式的性质:

$$\begin{aligned}\prod_{1\le r<s\le n}(\alpha_r-\alpha_s)^2&=\begin{vmatrix}1&1&1&\dots&1\\ \alpha_1&\alpha_2&\alpha_3&\dots&\alpha_n\\ \alpha_1^2&\alpha_2^2&\alpha_3^2&\dots&\alpha_n^2\\ \vdots&&&&\vdots\\ \alpha_1^{n-1}&\alpha_2^{n-1}&\alpha_3^{n-1}&\dots&\alpha_n^{n-1}\end{vmatrix}^2\\ &=\begin{vmatrix}1&1&1&\dots&1\\ \alpha_1&\alpha_2&\alpha_3&\dots&\alpha_n\\ \alpha_1^2&\alpha_2^2&\alpha_3^2&\dots&\alpha_n^2\\ \vdots&&&&\vdots\\ \alpha_1^{n-1}&\alpha_2^{n-1}&\alpha_3^{n-1}&\dots&\alpha_n^{n-1}\end{vmatrix}\times\begin{vmatrix}1&\alpha_1&\alpha_1^2&\dots&\alpha_1^{n-1}\\ 1&\alpha_2&\alpha_2^2&\dots&\alpha_2^{n-1}\\ 1&\alpha_3&\alpha_3^2&\dots&\alpha_3^{n-1}\\ \vdots&\vdots&\vdots&\dots&\vdots\\ 1&\alpha_n&\alpha_n^2&\dots&\alpha_n^{n-1}\end{vmatrix}\\ &=\begin{vmatrix}s_0&s_1&s_2&\dots&s_{n-1}\\ s_1&s_2&s_3&\dots&s_n\\ s_2&s_3&s_4&\dots&s_{n+1}\\ \vdots&\vdots&\vdots&\dots&\vdots\\ s_{n-1}&s_n&s_{n+1}&\dots&s_{2n-2}\end{vmatrix}\end{aligned}$$

接下来我们引入牛顿公式:

考虑复数域上的 n 元多项式环 $\mathbb{C}[x_1,x_2,\dots,x_n]$, 记其上多项式

$$s_k=\sum_{i=1}^n x_i^k$$

为 k 次等幂和，记

$$\begin{aligned}\sigma_1 =& \sum_{i=1}^{n} x_i \\ \sigma_2 =& \sum_{1\le i<j\le n} x_i x_j \\ \sigma_3 =& \sum_{1\le i<j<k\le n} x_i x_j x_k \\ &\vdots \\ \sigma_n =& x_1 \dots x_n\end{aligned}$$

为初等对称多项式。牛顿公式是指:

$$\begin{aligned}&s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k k\sigma_k = 0\,, && \forall 1 \le k \le n \\ &s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} + \cdots + (-1)^{n-1}\sigma_{n-1}s_{k-n+1} + (-1)^n \sigma_n s_{k-n} = 0\,, && \forall k > n\end{aligned}$$

证明可以参考丘维声《高等代数》下册第七章多项式部分。

考虑三次有理系数多项式 $x^3 + ax + b$, 我们用上述两个公式计算其判别式，若记其三个根为 x_1, x_2, x_3，则:

$$d(f) = \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}$$

其中:

$$s_k = \sum_{i=1}^{n} x_i^k\,, \quad k = 0, 1, 2, 3, 4$$

, 由韦达定理:

$$\sigma_1 = x_1 + x_2 + x_3 = 0 \quad \sigma_2 = x_1x_2 + x_2x_2 + x_3x_1 = a \quad \sigma_3 = x_1x_2x_3 = -b$$

由牛顿公式:

$$s_0 = 3 \quad s_1 = \sigma_1 = 0 \quad s_2 = \sigma_1 s_1 - 2\sigma_2 = -2a$$

$$s_3 = \sigma_1 s_2 - \sigma_2 s_1 + 3\sigma_3 = -3b \quad s_4 = \sigma_1 s_3 - \sigma_2 s_2 + \sigma_3 s_1 = 2a^2$$

从而:

$$d(f) = \begin{vmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{vmatrix} = -4a^3 - 27b^2$$

通过完全一样的思路，我们可以将该命题推广到 $g(x) = x^n + ax + b$ 的判别式为

$$d(g) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n)$$

有兴趣的同学可以自行尝试。

2.2 矩阵的 Kronecker 积

Kronecker积实际上是张量积的一种特殊情况，我们将 n 级矩阵 $A=(a_{ij})$ 和 m 级矩阵 $B=(b_{ij})$ 矩阵的Kronecker积定义为 mn 级分块矩阵：

$$A\otimes B=\begin{bmatrix} a_{11}B & a_{12}B & a_{13}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & \dots & a_{2n}B \\ a_{31}B & \dots & \dots & \dots & a_{3n}B \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_{n1}B & a_{n2}B & a_{n3}B & \dots & a_{nn}B \end{bmatrix}$$

其在代数学中有重要作用，比如群表示论中两个表示的张量积特征标的计算最终转化为矩阵Kronecker积的迹的计算，代数数论中我们研究代数数域 K 的判别式 $d(K)$ 时，两个代数数域的合成的判别式计算往往能转化为Kronecker积的行列式的计算，本则材料想要证明Kronecker积的两个性质：

$$\mathrm{tr}(A\otimes B)=\mathrm{tr}(A)\mathrm{tr}(B)$$

$$\det(A\otimes B)=(\det A)^m(\det B)^n$$

Proof:

$$\mathrm{tr}(A\otimes B)=\mathrm{tr}(B)(a_{11}+a_{22}+\cdots+a_{nn})=\mathrm{tr}(A)\mathrm{tr}(B)$$

接下来我们将重心放在讨论 $\det(A\otimes B)$，根据矩阵的分块乘法：

$$A\otimes B=(A\otimes I_m)(I_n\otimes B)$$

而直接计算得到 $\det I_n\otimes B=(\det B)^n$，因此只需证明 $\det(A\otimes I_m)=(\det A)^m$。事实上一种比较自然的证明方式是，考虑 n 为线性空间 V_1 以 $e_1,\dots,e_n$ 为基，m 维线性空间 V_2 以 $u_1,\dots,u_m$ 为基，则两个线性空间的张量积是一个以 $e_i\otimes u_j$ 为基的 mn 维线性空间，从而 $A\otimes I_m$ 与 $\mathrm{diag}\{A,\dots,A\}$(共 m 个)，在相似意义下只差一个从基 $e_1\otimes u_1,e_2\otimes u_1,\dots,e_n\otimes u_1,e_1\otimes u_2,e_2\otimes u_2,\dots,e_n\otimes u_2,\dots,e_1\otimes u_m,\dots e_n\otimes u_m$ 到基 $e_1\otimes u_1,e_1\otimes u_2,\dots,e_1\otimes u_m,e_2\otimes u_1,e_2\otimes u_2,\dots,e_2\otimes u_m,\dots,e_n\otimes u_1,\dots e_n\otimes u_m$ 的过渡矩阵，当然，用成对的交换行列也可以将 $A\otimes I_m$ 转化为 $\mathrm{diag}\{A,\dots,A\}$(共 m 个)，从而 $\det(A\otimes I_m)=(\det A)^m$，但是过程比较technical。具体思路是像拼拼图一样，先用行列变换将 $\det(A\otimes I_m)$ 左上角拼出一块 A，然后再用剩下的拼第二块，感兴趣的同学可以用低阶情况进行尝试，再给出一般情况的证明。

2.3 素数阶有限域上可逆矩阵计数

推荐对初等数论中同余类的概念熟悉或抽象代数中域概念熟悉的同学阅读本则材料。

在我们高等代数教材中给出了数域的定义，其为 $\mathbb{C}$ 的子集，关于加减乘除封闭，而域是推广了数域的概念，我们只需要有加减乘除的类似物即可定义出一个域，严格的定义可以参考抽象代数教材。素数阶有限域可以理解为 $\mathbb{F}_p=\{\bar{0},\bar{1},\dots,\bar{p-1}\}$，其中的加减乘是 $\bmod p$ 同余类的加减乘，除法按取逆元理解。

考虑所有有限域 $\mathbb{F}_p$ 上的 n 级可逆矩阵，称作一般线性群 $\mathrm{GL}_n(\mathbb{F}_p)$, 这显然是一个有限集，我们可以用组合数学的思想，分别从第一行开始选取，从而计数。第一行除非全是 0，其余均可选，故共有 p^n-1 种选法，第二行要与第一行线性无关，因此共有 p^n-p 种选法，第三行共有 p^n-p^2 种选法，依次类推到第 n 行共有 p^n-p^{n-1} 种选法，从而一般线性群 $\mathrm{GL}_n(\mathbb{F}_p)$ 中的元素个数为:

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\dots(p^n-p^{n-1})$$

更进一步，如果你对抽象代数的基本内容有所了解的话，我们知道，行列式给出了一个域上可逆矩阵到其这个域乘法群的同态，即为:

$$\det : \mathrm{GL}_n(\mathbb{F}_p) \to \mathbb{F}_p^*$$

其同态核为所有 $\mathrm{GL}_n(\mathbb{F}_p)$ 中行列式为 1 的矩阵，即为特殊线性群 $\mathrm{SL}_n(\mathbb{F}_p)$, 从而

$$\mathrm{GL}_n(\mathbb{F}_p)/\mathrm{SL}_n(\mathbb{F}_p) \simeq \mathbb{F}_p^*$$

从而我们得到了特殊线性群 $\mathrm{SL}_n(\mathbb{F}_p)$ 的元素个数:

$$|\mathrm{SL}_n(\mathbb{F}_p)| = \frac{(p^n-1)(p^n-p)\dots(p^n-p^{n-1})}{p-1}$$

借助有理标准型，Sylow定理，以及本材料提到的有限域上的一般线性群元素个数公式，我们可以得到关于素数阶分圆多项式在 $\mathbb{F}_p$ 上分解出的不可约因子的刻画，感兴趣的同学可以参考 [DF91]，同时，我们在讨论有限Abel群的自同构群计数问题时也会用到该结论 [HR07]。

参考文献

[DF91] David S Dummit and Richard M Foote. *Abstract algebra*, volume 1999, page 489. Prentice Hall Englewood Cliffs, NJ, 1991.

[HR07] Christopher J Hillar and Darren L Rhea. Automorphisms of finite abelian groups. *The American Mathematical Monthly*, 114(10):917–923, 2007.