第十三周习题课

李文桥

2023 年 12 月 15 日

1 伴随矩阵、 Cramer 法则与矩阵的秩

回忆: 设 $A \in \mathrm{M}_n(\mathbb{R})$, $B \in \mathbb{R}^{m\times n}$.

1. A 的伴随矩阵 $A^\vee$ 定义为: $(A_{j,i})_{n\times n}$, 其中 $A_{i,j}$ 为 A 的第 i 行第 j 列的代数余子式.
2. $AA^\vee = |A|E_n$.
3. 设 $\boldsymbol{b} \in \mathbb{R}^n$, $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)^t$, 则线性方程组 $A\boldsymbol{x} = \boldsymbol{b}$ 的充要条件为 $|A| \neq 0$, 即 A 可逆. 此时 $x_i = \det(\overrightarrow{A_1}, \cdots, \overrightarrow{A_{i-1}}, \boldsymbol{b}, \overrightarrow{A_{i+1}}, \cdots, \overrightarrow{A_n})/\det(A)$.
4. 设 $B \neq O$, 则以下命题等价:

   (1) $\mathrm{rank}(B) = r$;

   (2) B 的所有大于 r 阶的子式为零且存在至少一个 r 阶子式非零;

   (3) B 的所有 $r+1$ 阶子式为零且存在至少一个 r 阶子式非零.

   所以 r 就是 A 的最大非零子式的阶数.

习题 1: (a) $(\lambda A)^\vee = ((\lambda A)_{j,i})_{n\times n} = (\lambda^{n-1}A_{j,i})_{n\times n} = \lambda^{n-1}(A_{j,i})_{n\times n} = \lambda^{n-1}A^\vee$;

$AA^\vee = |A|E_n$, 从而 $|A||A^\vee| = |A|^n$. 若 $|A| \neq 0$, 则 $|A^\vee| = |A|^{n-1}$, 若 $|A| = 0$, 则 A 不可逆, 从而 $A^\vee$ 不可逆, 即 $|A|^\vee = 0 = |A|$.

(b) 当 A 满秩时, $A^\vee$ 可逆, 从而 $\mathrm{rank}(A^\vee) = n$. 当 $\mathrm{rank}(A) < n-1$ 时, A 的所有 $n-1$ 阶子式均为零, 从而 $A^\vee = O$, 即 $\mathrm{rank}(A^\vee) = 0$. 当 $\mathrm{rank}(A) = n-1$ 时:

法一: 由于 A 至少含有一个 $n-1$ 阶非零子式, 所以 $A^\vee \neq O$, 从而 $\mathrm{rank}(A^\vee) \geq 1$. 另一方面, $|A| = 0$, 所以 $AA^\vee = O$. 由 *Sylvester* 不等式知:

$$\mathrm{rank}(A) + \mathrm{rank}(A^\vee) \leq n + \mathrm{rank}(AA^\vee) = n.$$

从而 $\mathrm{rank}(A^\vee) \leq 1$. 故 $\mathrm{rank}(A^\vee) = 1$.

法二: 同法一, $\mathrm{rank}(A^\vee) \geq 1$. 由于 $AA^\vee = O$, 故 $A^\vee$ 的每一列都是齐次线性方程组 $A\boldsymbol{x} = \mathbf{0}$ 的解. 而由对偶定理, 该方程组的解空间维数为 $n - \mathrm{rank}(A) = 1$, 所以 $A^\vee$ 的列空间维数不超过 1, 即 $\mathrm{rank}(A^\vee) \leq 1$. 故 $\mathrm{rank}(A^\vee) = 1$.

习题 2: 当 A 可逆时, $|A| \neq 0$, $A^\vee = |A|A^{-1}$. 则 $A^\vee$ 可逆, $(A^\vee)^\vee = |A^\vee|(A^\vee)^{-1}$. 结合习题1, 我们有:

$$(A^\vee)^\vee = |A|^{n-1}(|A|A^{-1})^{-1} = |A|^{n-2}A.$$

当 A 不可逆时, $|A| = 0$. 若 $n > 2$, 则由习题 1, $\mathrm{rank}(A^\vee) \leq 1 < n-1$, 从而 $\mathrm{rank}((A^\vee)^\vee) = 0$, 故 $(A^\vee)^\vee = O = |A|^{n-2}A$. 若 $n = 2$, 则设 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 直接计算:

$$A^\vee = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},\ (A^\vee)^\vee = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A.$$

习题 3: (a) 设 $x_1, x_2, y_1, y_2 \in \mathbb{R}$ 使得 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, 则

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

用 $Cramer$ 法则解出

$$x_1 = \frac{d}{ad-bc},\ x_2 = -\frac{c}{ad-bc},\ y_1 = \frac{b}{ad-bc},\ y_2 = \frac{a}{ad-bc}.$$

(b) 用待定系数法, 设 $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, 其中 $a_0, \cdots, a_{n-1}$ 待定. 则

$$a_0 + a_1x_i + \cdots + a_{n-1}x_i^{n-1} = y_i,\ i = 1, \cdots, n$$

此为关于 $a_0, \cdots, a_{n-1}$ 的线性方程组, 系数矩阵为 $A = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix}$. $|A|$ 是 $Vandermode$ 行列式, 由于 x_i 互不相同, $|A| \neq 0$, 从而该方程组有唯一解. 这说明满足条件的多项式是存在唯一的.

回忆: 设 $A \in \mathbb{R}^{(n-1)\times n}$ 满秩, 则齐次线性方程组 $A\boldsymbol{x} = \mathbf{0}$ 的一个非零解为: $(|A_1|, (-1)|A_2|, \cdots, (-1)^{n-1}|A_n|)^t$, 其中 $|A_i|$ 为 A 去掉第 i 列后的矩阵.

证明: 设 $A=(a_{i,j})_{(n-1)\times n}=\begin{pmatrix}\boldsymbol{\alpha}_1\\ \vdots\\ \boldsymbol{\alpha}_{n-1}\end{pmatrix}$, 其中 $\boldsymbol{\alpha}_i$ 为 A 的第 i 行. 令 $B_i=\begin{pmatrix}\boldsymbol{\alpha}_i\\ \boldsymbol{\alpha}_1\\ \vdots\\ \boldsymbol{\alpha}_{n-1}\end{pmatrix}\in\mathbb{R}^{n\times n}$, 则 $|B_i|=0$. 另一方面, 若将 $|B_i|$ 按第一行展开, 我们有:

$$0=|B_i|=|A_1|a_{i,1}+(-1)|A_2|a_{i,2}+\cdots+(-1)^{n-1}|A_n|a_{i,n}.$$

注意到上式对任意的 $i=1,2,\cdots n-1$ 成立, 这就说明 $(|A_1|,(-1)|A_2|,\cdots,(-1)^{n-1}|A_n|)^t$ 为方程组的一个解. 由 $\mathrm{rank}(A)=n-1$ 知此为非零解.

习题 4: 注意到该题目与上述回忆的条件基本一致, 我们只需要证明 $\mathrm{rank}(A)=n-1$ 即可. 但很容易找到 A 的一个 $n-1$ 阶子式非零. 所以所求方程组的一个非零解为:

$$(\,|A_1|,(-1)|A_2|,\cdots,(-1)^{n-1}|A_n|\,)^t=(-1)^{n-1}\prod_{1\le i<j\le n}(\alpha_j-\alpha_i)(\,\frac{1}{\prod\limits_{k\neq 1}(\alpha_1-\alpha_k)},\frac{1}{\prod\limits_{k\neq 2}(\alpha_2-\alpha_k)},\cdots,\frac{1}{\prod\limits_{k\neq n}(\alpha_n-\alpha_k)}\,)^t$$

所以该方程组的解空间的一个基底为 $(\,\frac{1}{\prod\limits_{k\neq 1}(\alpha_1-\alpha_k)},\frac{1}{\prod\limits_{k\neq 2}(\alpha_2-\alpha_k)},\cdots,\frac{1}{\prod\limits_{k\neq n}(\alpha_n-\alpha_k)}\,)^t$.

补充: 一个 n 次的非零多项式至多有 n 个根. 从而两个次数不超过 n 的多项式在 $n+1$ 个取值处相同, 就说明这两个多项式相等.

补充(重要): (摄动法) 我们尝试证明下面一个结论:

命题 1.1 设 $A,B\in\mathrm{M}_n(\mathbb{R})$, 则 $(AB)^\vee=B^\vee A^\vee$.

证明: 若 A,B 均可逆, 则 $(AB)^\vee=|AB|(AB)^{-1}=(|B|B^{-1})(|A|A^{-1})=B^\vee A^\vee$.

到这里会发现, 不可逆的情形是有些困难的. 我们希望能用可逆的情形“逼近”不可逆的情形.

一般地, 设 $A'(\lambda)=\lambda E_n+A$, $B'(\lambda)=\lambda E_n+B$, $\lambda\in\mathbb{R}$. 则 $\det(A'),\det(B')$ 均为 λ 的多项式, 故只有有限个 λ 的取值使得 $A'(\lambda),B'(\lambda)$ 的行列式为 0, 即不可逆. 也就是说, $(A'B')^\vee=B'^\vee A'^\vee$ 对无穷多个 λ 成立. 而该等式的每个分量都是关于 λ 的多项式的等式, 这说明 $(A'B')^\vee=B'^\vee A'^\vee$ 对任意的 λ 恒成立. 特别地, $(AB)^\vee=B^\vee A^\vee$.

该问题解决的一个关键点是对不可逆情形的扰动, 将其转化为可逆情形. 将 n 阶方阵 $X=(x_{i,j})_{n\times n}$ 视为 $\mathbb{R}^{n^2}$ 中的一个点, 那么全体不可逆 n 阶方阵由方程 $\det(X)=0$ 给出. 直观理解, 这是一个 $\mathbb{R}^{n^2}$ 空间中的超曲面, 维数为 $n-1$. 所以所有可逆矩阵在整个矩阵空间中所占的“体积”为0, 它们是十分稀少的, 于是我们可以用空间中大量的、稠密的可逆矩阵去“逼近”这些不可逆矩阵, 也就是用曲面外的点逼近曲面上的点. 在上题中, 我们只是选取了一条特殊的道路 λE_n+A 去逼近 A, 这是一条经过 A 的直线, 直

线上只有有限个点落在曲面上, 其余的均落在曲面外. 实际上, 由 $\det(X)=0$ 决定的曲面是 $\mathbb{R}^{n^2}$ 中一个正则子流形, 它局部形状的是十分光滑平坦的.

例 1.2 设 $A\in \mathrm{M}_n(\mathbb{R})$, $\boldsymbol{\beta},\boldsymbol{\gamma}\in\mathbb{R}^{n\times 1}$, 求 $\det\begin{pmatrix}0 & \boldsymbol{\beta}^t\\ \boldsymbol{\gamma} & A\end{pmatrix}$.

解: 我们证明 $\det\begin{pmatrix}0 & \boldsymbol{\beta}^t\\ \boldsymbol{\gamma} & A\end{pmatrix}=-\boldsymbol{\beta}^tA^\vee\boldsymbol{\gamma}$. 若 A 可逆, 则:

$$\begin{pmatrix}1 & \boldsymbol{\beta}^tA^{-1}\\ \mathbf{0} & A\end{pmatrix}\begin{pmatrix}0 & \boldsymbol{\beta}^t\\ \boldsymbol{\gamma} & A\end{pmatrix}=\begin{pmatrix}-\boldsymbol{\beta}^tA^{-1}\gamma & \mathbf{0}^t\\ \boldsymbol{\gamma}^t & A\end{pmatrix}$$

对上式取行列式, 得: $\det\begin{pmatrix}0 & \boldsymbol{\beta}^t\\ \boldsymbol{\gamma} & A\end{pmatrix}=-\boldsymbol{\beta}^tA^\vee\boldsymbol{\gamma}$.

若 A 不可逆, 则对其对角线进行扰动, 转化为可逆情形即可.

2 群

回忆: 1. 二元运算,(封闭性) 同余运算.

2. 半群的定义, 群的定义.

3. 群结构的对称性: 左平移映射, Cayley 定理.

(1) 设 G 为一个有限群, $|G|=n$. 定义: $L_g:\ G\to G,\ x\mapsto gx$. 则 L_g 为双射, 从而 $L_g\in T_G$;

(2) $\phi:\ G\to T_G,\ g\mapsto L_g$ 是一个单的群同态, 而 T_G 同构于 S_n, 从而 G 可以被嵌入到 S_n 中.

习题 4: 直接计算即可. 只要与 22 互素均可逆.

习题 5: 按半群定义验证即可. 注意验证二元运算的封闭性.

补充: 群的例子.

课上我们已经知道, 一般线性群 $\mathrm{GL}_n(\mathbb{R})$ 是一个群. 若将其视为 $\mathbb{R}^{n^2}$ 的子集, 则它实际上是 $\mathbb{R}^{n^2}$ 的正则子流形. 也就是说, $\mathrm{GL}_n(\mathbb{R})$ 既有几何结构, 也有群的结构. 这时, 群的对称性就会起作用, 因为左平移 L_g 成为一个微分同胚, 这使得所有 $g\in\mathrm{GL}_n(\mathbb{R})$ 附近的特性与单位元 E_n 附近的特性完全一致. 于是只需关注 E_n 附近的拓扑结构, 我们就能研究清楚 $\mathrm{GL}_n(\mathbb{R})$. 实际上, $\mathrm{GL}_n(\mathbb{R})$ 被称为李群 (*Lie group*), 几何结构上的群结构使得李群有很多优美的性质.

另一个经典例子是椭圆曲线. 如图所示, 任取曲线上两点 A,B, 其连线与曲线的第三个交点关于 x 轴的对

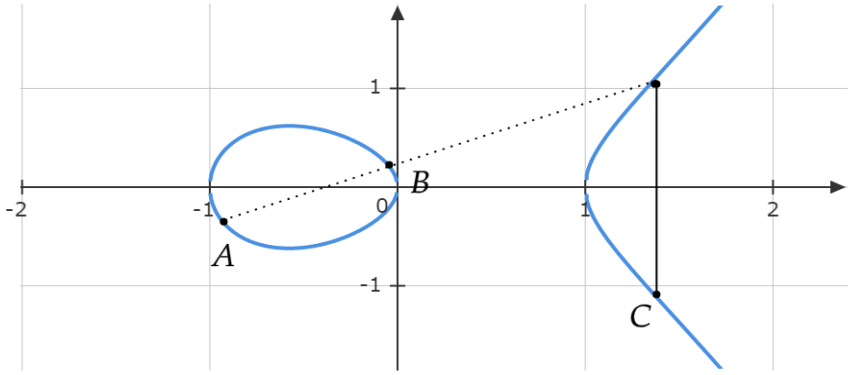

图 1: $y^2 = x^3 - x$

称点 C 定义为 $A + B$. 显然 $A + B = B + A$. 我们规定无穷远点为单位元, 与 x 轴对称的两点互为逆元, 那么这条曲线上的点关于“$+$” 构成一个群(结合律是可以验证的).

椭圆曲线上的群结构可以用来设计密码.在曲线上取一个基点 g, 同时取定 $a \in \mathbb{N}^+$, 记 $\alpha = a \cdot g$. 只要曲线和数域选取适当, 在已知 g, α 的情况下计算 a 往往是一个很困难的问题, 这类问题被称为离散对数问题. 设需要秘密传输的信息为 x, 这里 x 已转化为曲线上的一点, 公钥(公开的信息)为 g, α , 秘钥(保密的信息)为 a. 发送信息者随机选取一个正整数 k(保密), 将信息对 (y, t) 发送给接收者, 其中 $y = x + k \cdot \alpha$, $t = k \cdot g$. 接收者想要得到 x, 只需要计算 $y - a \cdot t$ 即可. 因为:

$$y - a \cdot t = x + k \cdot \alpha - ak \cdot g = x + ak \cdot g - ak \cdot g = x.$$

而攻击者想要窃取信息 x, 需要拦截传输的信息对 (y, t), 从中计算 x. 但由于攻击者不知道秘钥 a, 其需要从 t 和公开信息 g 计算出 k, 进而计算 $x = y - k \cdot \alpha$. 但这是一个困难问题, 往往需要耗费数月, 那时信息已经失去时效性.