辗转相除法

$m = q_1 n + r_1$ ①　　$r_1 = m - q_1 n$

$n = q_2 r_1 + r_2$ ②　　$r_2 = n - q_2 r_1$

...　　...　　...

$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ ⑫　　$r_{k-1} = r_{k-3} - q_{k-1} r_{k-2}$

$r_{k-2} = q_k r_{k-1}$ ⑬

求证 $r_{k-1} = \gcd(m,n)$?

将①代入② $r_2 = n - q_2(m - q_1 n) = (1 + q_1 q_2)n - q_2 m$ ②'

将②'①代入③ $r_3 = q_2 r_1 - q_3 r_2 = (m - q_1 n) - q_3(1 + q_1 q_2)n + q_3 q_2 m = (1 + q_2 q_3)m - (q_1 + q_3 + q_1 q_2 q_3)n$ ③'

...

∴ 将①, ②', ③', ... ⑫'代入⑬有 $r_{k-1} = t_1 m + t_2 n$

验证 $\exists k \in \{0, 1, \cdots n-1\}$. 使 $km \equiv_n r_{k-1}$ 令 t_1 加减某整数倍的 n. 总可以使 $t_1 + k'n \in \{0, 1, \cdots n-1\}$ ($k' = k$)

∴ $r_{k-1} = (k - k'n)m + t_2 n$ ∴ $km \equiv_n r_{k-1}$.

这个问题的本质? ①对于两个互素的 a, b. 有 $\{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\} = \mathbb{Z}$ why?

举例. 10和7　10 − 7 = 3. 不是10的因子. 不是7的因子, (对于 a, b 也一样 $a \bmod b$ 不是 a 的因子. 不是 b 的因子). ∴ 对于7个元素 1, 2, 3, 4, 5, 6, 7. 3的某些倍数(为 $k \cdot 3$)表示循环数 k 倍. ∵ 3不是7的因子. 所以只有7, 3时才是7的倍数. 其余都不是. 则 $1 \cdot 3, 2 \cdot 3, 3 \cdot 3, \cdots 6 \cdot 3$ 分别对应 1, 2, 3, 4, 5, 6 中的一个数. (否则若 $k_1 \cdot 3 \equiv_7 k_2 \cdot 3$ 则 $(k_1 - k_2) \cdot 3 \equiv_7 0$ 3是7的因子) 定有一个 $k \cdot 3$ 落在1上. 即 $k \cdot 3 \equiv_7 1$ (同理对于 a, b 也成立. 可自证, 思考题) ∵ $3 \equiv_7 10$ ∴ $k \cdot 10 \equiv_7 1$ 这个 $k \in \{1, 2, \cdots 6\}$。对于 $\forall m, n \in \mathbb{Z}$ $\{\alpha m + \beta n \mid \alpha, \beta \in \mathbb{Z}\} = \gcd(m,n) \cdot \mathbb{Z}$

m, n 同时除 $\gcd(m,n)$ 得到两互素的 $m' = \frac{m}{\gcd(m,n)}$, $n' = \frac{n}{\gcd(m,n)}$

$\{\alpha m + \beta n \mid \alpha, \beta \in \mathbb{Z}\} = \gcd(m,n) \cdot \{\alpha m' + \beta n' \mid \alpha, \beta \in \mathbb{Z}\} = \gcd \mathbb{Z}$

② 对于两个数 $a, b \in \mathbb{Z}^+$, $0 < |b| < a$. 若 b 不是 a 的因子. 则 $\{0 \bmod a, b \bmod a, 2b \bmod a, \cdots (a-1)b \bmod a\}$

$= \{0, 1, 2, \cdots (a-1)\}$

③ 映射 $\varphi: \mathbb{Z} \to \{0, 1, 2, \cdots (a-1)\}: b \mapsto b \bmod a$ $(-3 \bmod 5 = 2)$

商空间 $\mathbb{Z}/\varphi = \{\bar{0}, \bar{1}, \bar{2}, \cdots \overline{(a-1)}\}$ 若 $0 \le b \le a-1$, b 不是 a 的因子. 则 $\bar{b}$ 在 $\mathbb{Z}/\varphi$ 中有逆元(乘法). 即 $\exists \bar{k}$. 使 $\bar{k} \cdot \bar{b} = \bar{b} \cdot \bar{k} = \bar{1}$; $\bar{1}$ 是单位元 ($\because \bar{1} \cdot \bar{b} = \bar{b} \cdot \bar{1} = \bar{b}$)

先前证过 $\bar{a} \cdot \bar{b} = \overline{ab}$ (可自证. 思考题).

6. 证明: "⇒" $\vec{v}_1,\cdots\vec{v}_k$ 线性无关 $\vec{v}\in\langle\vec{v}_1,\cdots,\vec{v}_k\rangle$ ∴ $\vec{v}=\sum_{i=1}^{k}a_i\vec{v}_i$ (存在性)

若不唯一, $\vec{v}=\sum_{i=1}^{k}a_i'\vec{v}_i$. a_i' 与 a_i 不全相等 ∴ $0=\sum_{i=1}^{k}(a_i'-a_i)\vec{v}_i$ 由 $\vec{v}_1,\cdots\vec{v}_k$ 线性无关.

只有系数全部为零. 即 $a_1'=a_1$ 且 $a_2'=a_2,\cdots a_k'=a_k$. 矛盾, 故唯一. (唯一性)

"⇐" 设 k_i 使 $\sum_{i=1}^{k}k_i\vec{v}_i=\vec{0}$, 已知 $\vec{v}=\sum_{i=1}^{k}a_i\vec{v}_i=\sum_{i=1}^{k}(a_i+k_i)\vec{v}_i$, ∵ 以用线性表达式唯一

∴ $a_i+k_i=a_i\Rightarrow k_i=0$ $i=1,\cdots k$ ∴ $\vec{v}_1,\cdots\vec{v}_k$ 线性无关.

8.7.(ii)法一: 矩阵乘法秩的不等式: $r(A)+r(B)-S\le r(AB)\le\min(A,B)$

法二: A列满秩 ∴ φ_A 单射. B列满秩. φ_B 单射. ∴ $\varphi_{AB}=\varphi_A\circ\varphi_B$ 单射 ∴ AB列满秩.

(iii). 不能.

8. i) $\dim(U\cap V)=\dim(V_A)\Leftrightarrow\dim(U\cup V)=\operatorname{rank}(A)$

$U=\langle\vec{u}_1,\cdots\vec{u}_k\rangle$. $V=\langle\vec{v}_1,\cdots\vec{v}_l\rangle$ 求 $U\cup V$ 的一组基? 按行排做行变换, 按列排做列变换.

相当于对 A 做列变换, 求A的列空间的极大线性无关组. ∴ $\dim(U\cup V)=\operatorname{rank}(A)$

○ 求齐次方程组的解. 即 V_A. 对A做行变换 $\begin{pmatrix}1&2&2&2&9\\1&0&2&1&7\\-1&-1&-2&-1&-6\end{pmatrix}$ 的解. 即 V_A. 对A做行变换 $\begin{pmatrix}1&2&2&2&9\\0&-2&0&-1&-2\\0&1&0&1&3\end{pmatrix}\to\begin{pmatrix}1&2&2&2&9\\0&-2&0&-1&-2\\0&0&0&\frac{1}{2}&2\end{pmatrix}$

$\to\begin{pmatrix}1&0&2&0&7\\0&-1&0&-\frac{1}{2}&-1\\0&0&0&1&4\end{pmatrix}\to\begin{pmatrix}1&0&2&0&3\\0&-1&0&0&1\\0&0&0&1&4\end{pmatrix}\to\left(\begin{array}{ccccc}1&0&2&0&3\\0&1&0&0&-1\\0&0&0&1&4\\\hline0&0&0&0&0\\0&0&0&0&0\end{array}\right)$ 第三行 第五行

基解 $(2\ 0\ -1\ 0\ 0)=\vec{\alpha}$

$(3\ -1\ 0\ 4\ -1)=\vec{\beta}$

$\begin{pmatrix}1&0&2&0&3\\0&1&0&0&-1\\0&0&0&1&4\\0&0&0&0&0\\0&0&0&0&0\end{pmatrix}$ 让行向量首先为1的位置处于矩阵的对角线位置, 然后让对角线位置为零的地方补或-1, 对角线位置为-1的列向量就是 V_A 的基础解. $V_A=\langle\vec{\alpha},\vec{\beta}\rangle$

对于 $A\vec{x}=\vec{b}$. 如果已知 $\vec{x}_0$. 使 $A\vec{x}_0=\vec{b}$ ∴ 解空间为 ~~$\vec{x}_0+V_A$~~ $\{\vec{x}_0+\vec{v}\mid\vec{v}\in V_A\}$

○ 问题 A是一个矩阵. 已知 V_A. 可以求A的行空间的一组基吗? 若 $V_A=\langle(2,3,4,5)^T,(1,1,1,1)^T\rangle$.

$\begin{pmatrix}2&1\\3&1\\4&1\\5&1\end{pmatrix}$ 列变换 $\to\begin{pmatrix}0&1\\1&1\\2&1\\3&1\end{pmatrix}\to\begin{pmatrix}0&1\\1&0\\2&-1\\3&-2\end{pmatrix}\to\begin{pmatrix}1&0\\0&1\\-1&2\\-2&3\end{pmatrix}$ 补全 $A=\begin{pmatrix}0&0&0&0\\0&0&0&0\\-1&2&-1&0\\-2&3&0&-1\end{pmatrix}$ 就是解空间为 V_A 的齐次方程组的

系数矩阵. A的行空间 ~~与~~ 与 $\begin{pmatrix}-1&2&-1&0\\-2&3&0&-1\end{pmatrix}=A'$ 的行空间相同 $V_A=V_{A'}$ (A.B是矩阵. 且列数相同)

若A.B的行空间相同 $\Leftrightarrow V_A=V_B$

$V_A=\ker(\varphi_A)$

○ 问题二. 对于一个向量 $\vec{u}=(u_1,u_2,\cdots u_n)^T$. $U=\langle\vec{u}\rangle$ 求使U为解空间的方阵V.

$\vec{u}'=(-1,-\frac{u_2}{u_1},\cdots-\frac{u_n}{u_1})^T=\frac{1}{u_1}\vec{u}$

$\begin{pmatrix}-1\\-\frac{u_2}{u_1}\\\vdots\\-\frac{u_n}{u_1}\end{pmatrix}$ 补全V $\longrightarrow$ $\begin{pmatrix}0&0&\cdots&0\\-\frac{u_2}{u_1}&1&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\-\frac{u_n}{u_1}&0&\cdots&1\end{pmatrix}$

或者

$\vec{u}'=(-\frac{u_1}{u_n},-\frac{u_2}{u_n}\cdots,-\frac{u_{n-1}}{u_n},-1)=-\frac{1}{u_n}\vec{u}$

$\begin{pmatrix}-\frac{u_1}{u_n}\\-\frac{u_2}{u_n}\\\vdots\\-\frac{u_{n-1}}{u_n}\\-1\end{pmatrix}$ 补全V $\longrightarrow$ $\begin{pmatrix}1&0&\cdots&0&-\frac{u_1}{u_n}\\0&1&\cdots&0&-\frac{u_2}{u_n}\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&-\frac{u_{n-1}}{u_n}\\0&0&\cdots&0&0\end{pmatrix}$

4. $Im(A)$的一组基就是A的列向量的极大线性无关组. why? $\because \varphi_A(\vec{e}_i)\to A^{(i)}$ $\therefore \varphi_A(\mathbb{R}^n)=\langle A^{(1)},A^{(2)},\cdots A^{(n)}\rangle=Im(\varphi_A)$

~~ker(A)~~ $ker(\varphi_A)=V_A$.

$A=\begin{pmatrix}0&1&\cdots&0\\0&\vdots&\ddots&\vdots\\\vdots&\vdots&&\vdots\\0&0&\cdots&1\\0&0&\cdots&0\end{pmatrix}$ 去掉最后行(因为全是零) $A'=\begin{pmatrix}0&1&\cdots&0\\0&\vdots&\ddots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&1\end{pmatrix}$ $\xrightarrow{\text{补全}}$ $A''=\begin{pmatrix}-1&0&\cdots&0\\0&1&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&1\end{pmatrix}$

对角线为-1的列向量即为V_A的基 $\begin{pmatrix}-1\\0\\\vdots\\0\end{pmatrix}$ $\therefore ker(\varphi_A)=\langle\begin{pmatrix}-1\\0\\\vdots\\0\end{pmatrix}\rangle\Rightarrow Im(\varphi_A)=\langle\vec{e}_1,\cdots\vec{e}_{n-1}\rangle$, $ker(\varphi_A)=\langle\vec{e}_1\rangle$

○ 问题三. U是~~n-1维~~$\mathbb{R}^n$中n-1维子空间. 求V. 使V的解空间为U. ?

对U中n-1个基 $\vec{u}_1,\cdots\vec{u}_{n-1}$ 做列变换使 $(\vec{u}_1,\cdots\vec{u}_{n-1})\to\begin{pmatrix}-1&\cdots&0\\\vdots&\ddots&\vdots\\0&\cdots&-1\\u_{1n}^*&\cdots&u_{n-1,n}^*\end{pmatrix}_{n\times(n-1)}$ or $\begin{pmatrix}u_{11}^*&\cdots&u_{n-1,1}^*\\-1&\cdots&0\\\vdots&\ddots&\vdots\\0&\cdots&-1\end{pmatrix}_{n\times(n-1)}$

补全 $\begin{pmatrix}0&\cdots&0&0\\\vdots&&\vdots&\vdots\\0&\cdots&0&0\\u_{1n}^*&\cdots&u_{n-1,n}^*&1\end{pmatrix}$ or $\begin{pmatrix}1&u_{11}^*&\cdots&u_{n-1,1}^*\\0&0&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&0\end{pmatrix}$ $\therefore$ V只有n行向量.

$\mathbb{R}^n$中

V_0是d维子空间, $\vec{v}_1,\vec{v}_2,\cdots\vec{v}_d$是$V_0$的基. 对于$\vec{v}_i$的解空间是n-1维$\mathbb{R}^n$中的空间$U_i$,

对于V_0的解空间, 即以$\vec{v}_1,\cdots\vec{v}_d$为行向量的矩阵的零空间$V_{V_0}$即所有$\vec{v}_i$的解空间的交

(d个线性齐次方程组的解是每个线性方程的解的交)

$\therefore V_{V_0}=\bigcap_{i=1}^{d}U_i$

而V_{V_0}是n-d维空间. 有问题: 对H n-d维$\mathbb{R}^n$中的空间V_{V_0}存在d个n-1维$\mathbb{R}^n$中的空间, 使$V_{V_0}=\bigcap_{i=1}^{d}U_i$

○ 正交: (两个$\mathbb{R}^n$中向量$\vec{x},\vec{y}$. 若$\vec{x}$与$\vec{y}$的内积为零. 即$\sum_{i=1}^{n}x_iy_i=0$. 称$\vec{x},\vec{y}$正交)

$\therefore$ $A\vec{x}=\vec{0}\Leftrightarrow\begin{pmatrix}\vec{A}_1\\\vec{A}_2\\\vdots\\\vec{A}_n\end{pmatrix}\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}=0\Leftrightarrow$ 解$\vec{A}_1\vec{x}=\vec{A}_2\vec{x}=\cdots=\vec{A}_n\vec{x}=0$. 即$\vec{x}$与所有A的行向量的正交.

(如果向量$\vec{x}$. 与$\mathbb{R}^n$中子空间U中. 每个向量都正交. 则称$\vec{x}$与U正交; 如果V中所有向量都与U正交. 则称V与U正交) $\therefore$ A的零空间V_A与A的行空间正交.

思考：若U的零空间 $V_U = V$ (即列空间) 则 V^T 的零空间是？ 已知d维子空间U，与之正交的n-d维子空间V唯一吗？

~~V_{A+B}~~ $V_{A+B} = V_A \cap V_B$　　$V_{A\cap B} = V_A + V_B$ 求证、思考题.

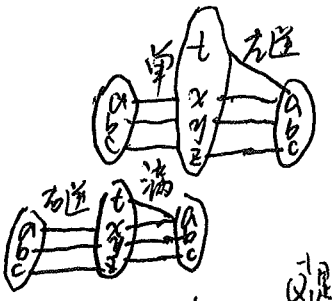
问题 $A_{m\times n}$, $X_{m\times n}$ 求 $AXA=A$ 有解？

设A的秩r. 则 $A=BC$　$B_{m\times r}$, $C_{r\times n}$ 秩都为r. ($\Rightarrow r\le m$, $r\le n$)

$\therefore AXA=A \Leftrightarrow BCXBC=BC$

$\because$ B列满秩、单射 $\therefore CXBC=C \Rightarrow C^T = C^TB^TX^TC^T$

$\because C^T$ 列满秩 单射 $\therefore B^TX^TC^T = E_{r\times r} \Rightarrow CXB = E_{r\times r}$



单射有左逆、满射有右逆

$\therefore \exists B^*.\ B^*B = E_{r\times r}$　$\exists C^*.\ CC^* = E_{r\times r}$

$\therefore$ 令 $X = C^*B^*$ 则 $CXB = CC^*B^*B = E_{r\times r}$

(问题求 C^*, B^*?)　$P_{r\times r}CQ_{m\times n} = (E_r \mid C')$　$C = P^{-1}_{r\times r}(E_r \mid C')\begin{pmatrix} Q^{-1}_{r\times n} \\ Q^{-1}_{2(n-r)\times n}\end{pmatrix}$　Q^{-1}是Q^{-1}的前r行

问题，$AB=BA$. 求证 $r(A+B)+r(AB) \le r(A)+r(B)$

$r(A)+r(B) = r(A+B)+r(A\cap B)$

$\therefore$ 求证 $r(AB) \le r(A\cap B)$

即 ~~$V_{A\cap B}$~~ $\dim(V_{A\cap B}) \le \dim(V_{AB})$

即 $\dim(V_A+V_B) \le \dim(V_{AB})$

若 $V_A+V_B \subseteq V_{AB}$ 可证 (但不是必要条件).

$\forall x+y \in V_A+V_B$　$x\in V_A$　$y\in V_B$ 有 $AB(x+y) = ABx+BAy = BAx+ABy = B\cdot 0 + A\cdot 0 = 0$

$\therefore V_A+V_B \subset V_{AB}$