Jordan 标准型 (部分习题解答)

Problem 1 (零空间的增长) 记 $A \in \mathbb{F}^{n\times n}$ 是任意域上的方阵. 约定 $A^0 = I$ 是单位矩阵, 以及 $A^{k+1} = A \cdot A^k$.

1. 证明有子空间的包含列

$$0 = N(A^0) \subset N(A^1) \subset N(A^2) \subset \cdots$$

特别地, 若 $N(A^N) = N(A^{N+1})$, 则 $N(A^{N+1}) = N(A^{N+2}) = \cdots$.

> 假定 $N(A^N) = N(A^{N+1})$. 对所有形如 Ax 的向量 y, 依定义, $A^N y = 0$ 当且仅当 $A^{N+1}y = 0$. 这说明 $N(A^{N+1}) = N(A^{N+2})$.

2. 假定存在**最小的**正整数 N 使得 $N(A^N) = N(A^{N+1})$. 证明 $N \le n$.

> 若 $N > n$, 则 $n > N(A) > N(A^2) > \cdots > N(A^n) > N(A^{n+1}) \ge 0$. 矛盾.

3. (Slightly challenging?) 证明: $\dim N(A^{N+2}) - \dim N(A^{N+1}) \le \dim N(A^{N+1}) - \dim N(A^N)$. 换言之, 散点图 $\left\{(k, \dim N(A^k))\right\}_{k\in\mathbb{N}}$ 是上凸函数.

> 将 $N(A^{N+1})$ 扩张成 $N(A^{N+2})$, 等价于添加一些基 $\{v_i\}_{i=1}^s$, 使得 $\{A^{N+1}v_i\}_{i=1}^s$ 是 $C(A^{N+1}) \cap N(A)$ 的一组基, 因此左式是 $\dim(C(A^{N+1}) \cap N(A))$. 相应地, 右式是 $\dim(C(A^N) \cap N(A))$.

Problem 2 (幂零矩阵的标准型) 仍假定 $A \in \mathbb{F}^{n\times n}$ 是**任意域上**的幂零方阵.

1. 证明: 存在正整数 $N \le n$ 使得 $A^N = O$.

2. (若觉得简单, 可以跳过) 假定 $n = 3$, $A^2 \ne O$, 但 $A^3 = O$. 证明: 存在向量 $\{x, y, z\}$ 使得 $Ax = y$, $Ay = z$, 但 $Az = \mathbf{0}$. 换言之, 存在链

$$\boxed{x \xrightarrow{A} y \xrightarrow{A} z \xrightarrow{A} \mathbf{0}}.$$

同时, 仿照 **Problem 0** 说明 A 相似于 $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

3. (若觉得简单, 可以跳过) 假定 $n = 3$, $A \ne O$, 但 $A^2 = O$. 证明: 存在向量 $\{x, y, z\}$ 使得 $Ax = y$, $Ay = Az = \mathbf{0}$. 换言之, 存在链

$$\boxed{x \xrightarrow{A} y \xrightarrow{A} \mathbf{0}}, \quad \boxed{z \xrightarrow{A} \mathbf{0}}.$$

同时, 仿照 **Problem 0** 说明 A 相似于 $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

4. (Slightly challenging) 使用归纳法证明: 存在若干条链

$$\left[\boxed{x_i^1 \xrightarrow{A} x_i^2 \xrightarrow{A} x_i^3 \xrightarrow{A} \cdots x_i^{n_i} \xrightarrow{A} \mathbf{0}}\right]_{i=1}^s.$$

且 $\bigcup_{i=1}^s \{x_i^j\}_{1\le j\le n_i}$ 是 $\mathbb{F}^n$ 的一组基. 作为推论, $\sum_{i=1}^s n_i = n$.

5. 不妨设 $n_1 \ge n_2 \ge \cdots \ge n_s$. 证明 $\dim N(A) = s$, 也就是 $\{x_i^1 \mid i \ge 1\}$ 的大小.

6. 证明: 对给定的正整数 k, 集合 $\{x_i^k \mid i \ge 1\}$ 的大小是 $\dim N(A^{k-1}) - \dim N(A^k)$.

7. 证明: A 相似于分块对角矩阵 $\mathrm{diag}(J_{n_1}(0), \ldots, J_{n_s}(0))$. 此处, $J_k(0)$ 是大小为 k, 特征值为 0 的 Jordan 块.

8. 假定 $\lambda \in \mathbb{F}$, 方阵 A 能被形如 $(x-\lambda)^l$ 的多项式零化. 证明: A 相似于分块对角矩阵 $\mathrm{diag}(J_{n_1}(\lambda), \ldots, J_{n_s}(\lambda))$.

Problem 3 假定 A 与 B 是**一般域**上的方阵, 下研究矩阵乘法式 $AX-XB$.

1. 假定 $\mathbb{F}\subset\mathbb{K}$ 是两个包含的域, 例如 $\mathbb{Q}\subset\mathbb{Q}[\sqrt[3]{2}]$, 或是 $\mathbb{R}\subset\mathbb{C}$). 任取 $\mathbb{F}$ 上的矩阵 M, 记 m 是 $\mathbb{F}$-线性空间 $\{x\in\mathbb{F}^N \mid Mx=0\}$ 的维数; 由于 A 也是 $\mathbb{K}$ 上的矩阵, 记 n 是 $\mathbb{K}$-线性空间 $\{x\in\mathbb{K}^N \mid Mx=0\}$ 的维数. 证明 $m=n$.

> 零空间维数即标准阶梯形中的全零行数. 这一结果和域的选取无关.

2. 假定 $\varphi: V\to V$ 是有限维线性空间到自身的线性映射. 证明: φ 是单射, 当且仅当 φ 是满射, 亦当且仅当 φ 是双射.

> 将 φ 写成矩阵形式, 即方阵 A. 此时
>
> 1. φ 是双射当且仅当存在线性映射 ψ, 使得 $\varphi\psi=\psi\varphi=\mathrm{id}_V$, 等价地看, A 可逆;
> 2. φ 是单射当且仅当 $\varphi(u_\bullet P)=\varphi(u_\bullet)P=0 \iff P=0$, 等价地看, $AP=O \iff P=O$, 即 $N(A)=0$;
> 3. φ 是满射当且仅当 $V=C(\varphi(u_\bullet))=C(u_\bullet\cdot A)$. 换言之, $N(A^T)=0$.
>
> 因此以上三者等价.

3. 证明: $AX-XB=O$ 只有零解, 当且仅当 A 与 B 的特征多项式互素. 提示: 可以使用 Hamilton-Cayley 定理.

> 假定 A 与 B 的特征多项式互素, 此时存在多项式 g 与 f 使得 $\chi_A f+\chi_B g=1$. 此时 $\chi_A(B)\cdot g(B)=I$, 以及 $\chi_B(A)\cdot f(A)=I$. 归纳得 $A^kX=XB^k$, 从而
>
> $$O=\chi_A(A)X=X\cdot\underbrace{\chi_A(B)}_{\text{可逆}}.$$
>
> 这说明 $X=O$.
>
> 反之, 假定 χ_A 与 χ_B 有公共因子 $d(x)$, 再不妨设 d 是不可约多项式. 下给出方程的非零解.
>
> 对 A, 由不变子空间得分块上三角矩阵
>
> $$P^{-1}AP=\begin{pmatrix}A_1 & A_2\\ O & A_4\end{pmatrix},\quad \det(xI-A_1)=d(x).$$
>
> 对 A, 由不变子空间得分块下三角矩阵
>
> $$Q^{-1}BQ=\begin{pmatrix}B_1 & O\\ B_3 & B_4\end{pmatrix},\quad \det(xI-B_1)=d(x).$$
>
> 此时 $A_1\sim B_1$. 由于分块相似变换不改变上 (下) 三角矩阵, 故不妨设 $A_1=B_1=T$. 考虑相抵换元, 可以直接写出非零解 $X=P^{-1}\begin{pmatrix}T & O\\ O & O\end{pmatrix}Q$.
>
> - 注: 此题也可以使用有限扩域, 使得 χ_A 与 χ_B 可以分解作一次因子的乘积, 从而取 A 的上三角矩阵化与 B 的下三角化. 这一解法本质上与上述方法相同, 但关于扩域的论述是比较麻烦的.

4. 给定矩阵 $A\in\mathbb{F}^{n\times n}$ 和 $B\in\mathbb{F}^{m\times m}$. 证明以下是等价的 (建议灵活使用先前作业中的结论).

   1. 对未知量 $X\in\mathbb{F}^{n\times m}$, 方程 $AX-XB=O$ 只有零解.
   2. 任意给定矩阵 $C\in\mathbb{F}^{n\times m}$, 对未知量 $X\in\mathbb{F}^{n\times m}$, 方程 $AX-XB=C$ 总有解.
   3. 任意给定矩阵 $C\in\mathbb{F}^{n\times m}$, 对未知量 $X\in\mathbb{F}^{n\times m}$, 方程 $AX-XB=C$ 有且仅有唯一的解.
   4. 对任意矩阵 C, 总有相似矩阵

   $$\begin{pmatrix}A & C\\ O & B\end{pmatrix}\sim\begin{pmatrix}A & O\\ O & B\end{pmatrix}.$$

   5. A 与 B 的特征多项式互素.

> 一处重要概念辨析.

1. $\operatorname{rank}\begin{pmatrix} A & C \\ O & B \end{pmatrix} = \operatorname{rank}(A) + \operatorname{rank}(B)$ 的充要条件: 存在 X 与 Y 使得 $AX + YB = C$.
2. $\begin{pmatrix} A & C \\ O & B \end{pmatrix} \sim \begin{pmatrix} A & O \\ O & B \end{pmatrix}$ 的充要条件: 存在 X 使得 $AX - XB = C$.

Problem 4 以下是求解 Jordan 标准型的一般步骤.

1. 证明: A 相似于一个分块上三角矩阵,

$$\begin{pmatrix} A_1 & * & \cdots & * \\ O & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ O & \cdots & O & A_s \end{pmatrix},$$

其中, A_i 配有一个不可分解的多项式 f_i, 使得 $f_i(A_i)$ 是幂零矩阵.

> 以下是一种可行的解法: 假定 A 是一般域 $\mathbb{F}$ 上的 n-阶方阵, 则 A 的特征多项式可以分解作 $\mathbb{F}[x]$ 中不可分解多项式的乘积, 记作 $\chi_A(x) = \prod_{i=1}^{s} f_i(x)^{n_i}$. 对多项式 f_i, 定义
>
> $$V_i := \{v \mid \text{存在 } N \geq 1, \text{使得 } (f_i(A))^N \cdot v = \mathbf{0}\}.$$
>
> 此时有直和分解 $\mathbb{F}^n = V_1 \oplus V_2 \oplus \cdots \oplus V_s$. 对于任意 $1 \leq t \leq s$, 子空间 $V_1 \oplus V_2 \oplus \cdots \oplus V_t$ 是关于左乘 $(A\cdot)$ 这一线性映射的不变子空间.

2. 使用 **Problem 3** 说明上一小问的分块上三角矩阵可以取作分块对角矩阵. 换言之, 证明存在相似矩阵

$$\begin{pmatrix} A_1 & * & \cdots & * \\ O & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ O & \cdots & O & A_s \end{pmatrix} \sim \begin{pmatrix} A_1 & O & \cdots & O \\ O & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \cdots & O & A_s \end{pmatrix}.$$

3. 这是惟一的需要使用复数域的地方! 如果所有 $f_i(x) = (x - \lambda_i)$ 都是一次多项式, 则所有 $(A_i - \lambda_i I)$ 都是幂零矩阵, 因此相似于 **Problem 2** 中所得的标准型.

4. 假若 f_i 不是一次多项式, 请自行学习有理标准型相关知识.

Problem 4+ 在许多情境下, 不便对实方阵使用有理标准型. 以下给出实方阵的一种标准型.

1. 假定 A 与 B 是实方阵. 若存在可逆复方阵 C 使得 $C^{-1}AC = B$, 则存在可逆实方阵 R 使得 $R^{-1}AR = B$.

   > 这对一般域也成立: 两个矩阵相似, 当且仅当它们在某一扩域上相似. 此处的证明类似 Problem 3.1, 只需将初等因子组写作形如 $Fx = \mathbf{0}$ 的式子即可.

2. 若 A 是实方阵, 其 (视作复方阵) Jordan 形是 $\operatorname{diag}(J_1, \ldots, J_s)$. 证明: 若存在 $z \in \mathbb{C} \setminus \mathbb{R}$ 使得 $J_d(z)$ 是 A 的 Jordan 块, 则 $J_d(\overline{z})$ 也是 A 的 Jordan 块.

   > 提示: $(A - zI)$ 与 $(A - \overline{z}I)$ 有相同的零空间增长序列 (Problem 1.1), 从而共轭的 Jordan 块成对出现.

3. 证明并推广以下相似矩阵的结论:

$$\begin{pmatrix} e^{i\theta} & 1 & & \\ & e^{i\theta} & & \\ & & e^{-i\theta} & 1 \\ & & & e^{-i\theta} \end{pmatrix} \sim \begin{pmatrix} \cos\theta & \sin\theta & & \\ -\sin\theta & \cos\theta & 1 & \\ & & \cos\theta & \sin\theta \\ & & -\sin\theta & \cos\theta \end{pmatrix}.$$

   由此描述实方阵的标准型.

4. 证明: 任意两个实方阵都是两个**实对称**方阵的乘积.

   > 先前作业 (对称矩阵相关) 出现过类似的构造.

复矩阵特征根的重要工具: Gershgorin 圆盘

Definition 给定 $A \in \mathbb{C}^{n\times n}$. 对 $1 \le k \le n$, 定义复平面 $\mathbb{C} = \mathbb{R}^2$ 上的第 i 个闭圆盘如下:

- 圆盘的中心是 $a_{i,i} \in \mathbb{C}$,
- 圆盘的半径是 $\sum_{1\le j\le n,\ 且\ j\ne i} |a_{i,j}|$.

以上定义了第 i 个 Gershgorin 圆盘, 记作

$$D_i = \left\{ z : |z - a_{i,i}| \le \sum_{1\le j\le n,\ 且\ j\ne i} |a_{i,j}| \right\}.$$

Problem 5 (Gershgorin 圆盘定理) 对上述复方阵 A, 任取特征值 λ 和相应特征向量 v, 满足 $Av = \lambda v$.

1. 假定 v 中第 i 个分量模长最大, 证明 $\lambda \in D_i$.

> 直接计算得 $\lambda v_i = \sum_{1\le j\le n} a_{i,j} v_j$. 由于向量 Av 的第 i 个分量模长最大 (因此 $v_i \ne 0$), 计算得
>
> $$|\lambda - a_{i,i}| = \frac{|\sum_{1\le j\le n} a_{i,j} v_j|}{|v_i|} \le \sum_{1\le j\le n} |a_{i,j}| \cdot \frac{|v_i|}{v_i} \le \sum_{1\le j\le n} |a_{i,j}|.$$

2. 作为推论, $\bigcup_{i=1}^n D_i$ 中包含了 A 的所有特征值.

3. 记复矩阵 $A := \begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & -1 \\ 1 & 0 & -2 \end{pmatrix}$. 尝试求出 A 的所有特征根, 并画出所有的 Gershgorin 圆盘. 对 A^T 作类似的操作.

4. 假定 A 与 B 是可对角化的 n-阶复方阵. 证明: 对 $t \in [0,1]$, 存在复平面上连续的道路 $\{\lambda_i : [0,1] \to \mathbb{C}\}_{i=1}^n$, 满足

   1. $\{\lambda_i(0)\}_{i=1}^n$ 恰是 A 的所有特征值;
   2. $\{\lambda_i(1)\}_{i=1}^n$ 恰是 B 的所有特征值;
   3. $\{\lambda_i(t)\}_{i=1}^n$ 是 $(1-t)A + tB$ 的特征值.

   思考: 对某些 $t \in (0,1)$, 矩阵 $(1-t)A + tB$ 未必可对角化. 此时的特征道路应作何种调整?

> 依照 ε-δ 语言的论证, 这是可去间断点. 所以不用做任何调整.

5. 假定 A 可对角化, 且 $\bigcup_{i=1}^n D_i$ 有两个连通分支 $\bigcup_{i=1}^k D_i$ 与 $\bigcup_{i=k+1}^n D_i$. 证明: 则第一个连通分支恰包含 k 个特征值, 第二个连通分支包含 $n-k$ 个特征值.

> 记 Λ 是 A 的对角部分, $N := A - \Lambda$ 是对角线全零的矩阵. 定义 $A^{(t)} = \Lambda + tN$, 记第 i 个圆盘为 $D_i^{(t)}$. 对任意 $t \in [0,1]$ 总有
>
> $$\underbrace{\left(\bigcup_{i=1}^k D_i^{(t)}\right)}_{记作集合\ M^{(t)}} \cap \underbrace{\left(\bigcup_{i=k+1}^n D_i^{(t)}\right)}_{记作集合\ N^{(t)}} = \emptyset.$$
>
> $M^{(0)}$ 中包含 k 个特征值, 依照连续性, $M^{(t)}$ 中恰好包含 k 个特征值. $N^{(t)}$ 亦然.

6. 假定 A 的 n 个圆盘两两不交, 则 A 一定可对角化, 且每一圆盘中恰好包含一个特征值.

> 同上, 将 n 个离散的点连续变换作 n 个两两不交的闭圆盘.

Problem 6 以下研究复矩阵的幂方问题.

1. 找出所有 2×2 的复矩阵 A, 使得不存在 $B^2 = A$. 使用 Jordan 标准型, 将这个结论推广至 $n\times n$ 阶的复矩阵.

> 论断: 2×2 复矩阵存在平方根, 当且仅当矩阵不相似于 $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
>
> 1. 一方面, 矩阵 $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ 不存在平方根. 若此类矩阵有平方根 Q, 则 Q 幂零且非零. 从而 $Q \sim \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. 这与 $Q^2 \neq O$ 矛盾.
> 2. 另一方面, 所有可对角化矩阵存在平方根, 所有相似于 $J_2(\lambda)$ $(\lambda \neq 0)$ 的矩阵存在平方根.
>
> - n-维情形: 仅需关注幂零部分. 若幂零矩阵 N 存在平方根, 当且仅当 N 是幂零矩阵的平方, 亦当且仅当 $J_1(0)$ 的数量不小于所有 $J_{\geq 2}(0)$ 的数量.
>
> 提供一个计算矩阵级数的一般方法:
>
> $$f(J_n(\lambda)) = \begin{pmatrix} f(\lambda) & f'(\lambda) & \frac{f''(\lambda)}{2} & \cdots & \frac{f^{(n-1)}(\lambda)}{(n-1)!} \\ 0 & f(\lambda) & f'(\lambda) & \cdots & \frac{f^{(n-2)}(\lambda)}{(n-2)!} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & f(\lambda) & f'(\lambda) \\ 0 & 0 & 0 & 0 & f(\lambda) \end{pmatrix}.$$
>
> 假定 A 是 n 阶矩阵, f 是解析函数 (依照收敛的形式幂级数定义的函数). 那么 $f(A)$ 仅与 f 的前 $(n-1)$ 阶导数相关.

2. 假定 $A \in \mathbb{R}^{n\times n}$. 若对一切 $1 \leq i \leq n$ 都有

$$2|a_{i,i}| > \sum_{i=1}^{n} |a_{i,j}|,$$

则 A 是可逆矩阵.

> 依照圆盘定理, 0 不属于任何一个圆盘, 从而矩阵可逆.

3. 假定 $A \in \mathbb{R}^{n\times n}$. 称 A 是有趣的, 当且仅当对一切 $1 \leq i \leq n$, 都有

$$2a_{i,i} > \sum_{i=1}^{n} |a_{i,j}|.$$

试用圆盘定理证明以下是单射:

$$n\text{-阶有趣矩阵} \to \mathbb{R}^{n\times n}, \quad A \mapsto A^2.$$

> 依照圆盘定理, $\sigma(A) \subset \{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$. 由于
>
> $$\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\} \to \mathbb{C}, \quad z \mapsto z^2$$
>
> 是单射, 故以上对应的逆映射可以直接写出.

4. 假定 $A \in \mathbb{R}^{n\times n}$. 称 A 是奇妙的, 当且仅当对一切 $1 \leq i \leq n$, 都有

$$3|a_{i,i}| > \sum_{i=1}^{n} |a_{i,j}|.$$

试用圆盘定理证明以下是单射:

$$n\text{-阶奇妙矩阵} \to \mathbb{R}^{n\times n}, \quad A \mapsto A^3.$$

> 类似地, $\sigma(A)$ 中特征向量的辐角属于 $(-30^\circ, 30^\circ) \cup (\pi - 30^\circ, \pi + 30^\circ)$, 以这一开区域为定义域的立方函数 $z \mapsto z^3$ 是单射.

5. 称一个复方阵 A 是本质正的，若 A 的所有特征根都是正实数. 试证明: 若 A 与 B 都是本质正的矩阵，且 $A^2 = B^2$，则 $A = B$.

> 考虑 $A(A-B) = (A-B)(-B)$. 由于 $\sigma(A) \cap \sigma(-B) = \emptyset$，因此 $AX = X(-B)$ 只有零解. 这说明 $A = B$.

6. 若 A 与 B 是本质正的，且 $A^3 = B^3$，则 $A = B$.

> 提示: 记 $\omega_{1,2} = \frac{-1 \pm \sqrt{3}}{2}$ 是三次单位根，考虑方程组
>
> $$\begin{cases} A(A^2 + \omega_1 AB + \omega_1^2 B^2) = (A^2 + \omega_1 AB + \omega_1^2 B^2)(\omega B); \\ A(A^2 + \omega_2 AB + \omega_2^2 B^2) = (A^2 + \omega_2 AB + \omega_2^2 B^2)(\omega B). \end{cases}$$
>
> 特别地，可以对本质正的条件做一些弱化，例如本题第 4 小问.

7. 证明: 本质正的矩阵有唯一的本质正的 n-次方根.

> 先考虑 $n = p$ 是素数. 记 w 是 p-次单位根，则对一切 $1 \le k \le p-1$，
>
> $$\begin{aligned} & A(A^{p-1} + w^k A^{p-2}B + w^{2k}A^{p-3}B^2 + \cdots + w^{(p-1)k}B^{p-1}) \\ = \ & (A^{p-1} + w^k A^{p-2}B + w^{2k}A^{p-3}B^2 + \cdots + w^{(p-1)k}B^{p-1})(w^k B). \end{aligned}$$
>
> 因此，$A^{p-1} + w^k A^{p-2}B + w^{2k}A^{p-3}B^2 + \cdots + w^{(p-1)k}B^{p-1} = O$. 写作线性方程组，得
>
> $$(w^{i\cdot(j-1)})_{1\le i\le(p-1),\,1\le j\le p} \cdot \begin{pmatrix} A^{p-1} \\ A^{p-1}B \\ \vdots \\ B^{p-1} \end{pmatrix}_p = \begin{pmatrix} O \\ O \\ \vdots \\ O \end{pmatrix}_{p-1}.$$
>
> 此处，$\{A^l B^{p-1-l}\}_{0\le l\le p-1}$ 是 p 个未知量. 左侧矩阵 $W_{(p-1)\times p} = (w^{i\cdot(j-1)})$ 形如增广矩阵 $(\mathbf{1} \ \ V)$，V 是 p-阶 Vandermonde 方阵 (可逆). 因此，存在行初等变换，使得
>
> $$W = (\mathbf{1} \ \ V) \xrightarrow{\text{行初等变换}} (\mathbf{v} \ \ I) \quad (\text{存在唯一的 } \mathbf{v} \in \mathbb{C}^{p-1}).$$
>
> 由于行变换不改变列线性关系，结合 $\mathbf{1} \in N(W)$ 知 $\mathbf{v} = -\mathbf{1}$. 此时，方阵组的最后一个等式是 $A^{p-1} - B^{p-1} = O$.
>
> (关键结论) 我们证明了对任意素数 p，若本质正矩阵满足 $A^p = B^p$，则 $A^{p-1} = B^{p-1}$.
>
> 记 $S(p)$ 是命题: 本质正的矩阵有唯一的本质正的 n-次方根. 那么
>
> $$S(a) \text{ 真, 且 } S(b) \text{ 真} \implies S(a\cdot b) \text{ 真}.$$
>
> 上一条引理说明
>
> $$S(p-1) \text{ 真} \implies S(p) \text{ 真} \quad (\forall p \in \text{ 素数}).$$
>
> 从而对所有 $n \ge 2$，$S(n)$ 真.