A study memo on jordan normal form of matricies

Proposition 1. *Let*

(S1) $m \in \mathbb{N} \cup [2, \infty)$

(S2) $f_1, ..., f_m \in \mathbb{C}[X] \setminus 0$.

(A1) $f_1, ..., f_m$ *don't have common divisor.*

then there are $h_1, ..., h_m \in \mathbb{C}[X]$ *such that*

$$\Sigma_{i=1}^{m} h_i f_i = 1 \tag{1}$$

Case when $m = 2$. When $\Sigma_{i=1}^{m} deg(f_i) = 0$, $deg(f_1) = deg(f_2) = 1$. In this case, the the claim in this Proposition holds. We assume the claim in this Proposition holds when $\Sigma_{i=1}^{m} deg(f_i) < K$. We can assume $deg(f_1) > 0$ There is $q, r \in \mathbb{C}[X]$ such that $f_1 = qf_2 + r$ and $deg(r) < deg(f_1)$ By the assumption of our mathematical induction, there are $h_1, h_2 \in \mathbb{C}[X]$ such that $h_1 r + h_2 f_2 = 1$. Because $r = qf_2 - f_1$, $-h_1 f_1 + (q + h_2) f_2 = 1$. □

Case when $m > 2$. We assume the claim in this Proposition holds when $m = K$. Let us set q is a maximum diviser of $f_1, ..., f_K$ and $g_i := \dfrac{f_i}{q_i}$ $(i = 1, 2, ..., K)$. Clearly, $g_1, ..., g_m$ don't have common divisor and f_{K+1} and q don't have common divisor. By the assumption of mathematical induction,
there are $h_1, ..., h_K, h_{K+1}, s \in \mathbb{C}[X]$ such that

$$\Sigma_{i=1}^{K} h_i g_i = 1 \tag{2}$$

and

$$sq + h_{K+1} f_{K+1} = 1 \tag{3}$$

Then $\Sigma_{i=1}^{K} h_i f_i = q$. Consequently,

$$\Sigma_{i=1}^{K} s h_i f_i + h_{K+1} f_{K+1} = 1 \tag{4}$$

□

Theorem 1. *Let*

(S1) $A \in M(n, \mathbb{C})$

then the followings hold.

(i) *There is $P \in GL(n, \mathbb{C})$ and $\alpha_1, ..., \alpha_K \in \mathbb{C}$ such that*

$$P^{-1}AP = \begin{pmatrix} J(\alpha_1) & O & ... & O \\ O & J(\alpha_2) & ... & O \\ ... & ... & ... & ... \\ O & & ... & J(\alpha_K) \end{pmatrix}$$

Here, for each i, there are $j_1, ..., j_{n_i}$ such that

$$J(\alpha_i) = \begin{pmatrix} J_1(\alpha_i) & O & ... & O \\ O & J_2(\alpha_i) & ... & O \\ ... & ... & ... & ... \\ O & & ... & J_{n_i}(\alpha_i) \end{pmatrix}$$

and $J_k(\alpha_i)$ is a j_k-th square matrix

$$J_k(\alpha_i) = \begin{pmatrix} \alpha_i & 1 & & & O \\ O & \alpha_i & 1 & & O \\ ... & ... & ... & ... & ... \\ O & & & \alpha_i & 1 \\ O & & & & \alpha_i \end{pmatrix}$$

We call $J_k(\alpha_i)$ is a Jordan block.

(ii) *If $\alpha_i \neq \alpha_j$ (for any $i \neq j$), A is diagonalizable.*

(iii) *For any W_1 and W_2 such that W_1 and W_2 are $J_k(\alpha_i)$-invariant subspaces and $\mathbb{C}^\nu = W_1 \oplus W_2$, $W_1 = \mathbb{C}^\nu$ or $W_2 = \mathbb{C}^\nu$.*

STEP1. Existence of the minimal polynomial of A. Because $E, A, A^2, ..., A^{n^2}$ are linearly dependent, there are $a_0, a_2, ..., a_n$ such that

$$\Sigma_{i=0}^{n^2} a_i A^i = 0 \tag{5}$$

So there is a $\varphi_A \in \mathbb{C}[X]$ such that

$$deg(\varphi_A) = min\{deg(\varphi) | \varphi \in \mathbb{C}[X] \text{ and } \varphi(A) = 0\} \tag{6}$$

□

STEP2. Decomposition of $\mathbb{C}^n$ into generalized eigenspaces. By fundamental theorem of algebra, there are distinct $\alpha_1, ..., \alpha_K \in \mathbb{C}$

$$\varphi_A(x) = \Pi_{i=1}^K (x - \alpha_i)^{m_i} \tag{7}$$

We set $f_i \in \mathbb{C}[X]$ by $f_i(x) := \dfrac{\varphi_A(x)}{(x - \alpha_i)^{m_i}}$ $(i = 1, 2, ..., K)$. By Proposition(), then there are $h_1, ..., h_m \in \mathbb{C}[X]$ such that

$$\Sigma_{i=1}^K h_i(A) f_i(A) = E \tag{8}$$

We set $W_{i,j} := \{x \in \mathbb{C}^n | (A - \alpha_i E)^j x = 0\}$ and $W_i := W_{i,m_i}$ $(j = 1, 2, ..., m_i)$ For any $x \in \mathbb{C}^n$, $x = \Sigma_{i=1}^K h_i(A) f_i(A) x$. For each i, $h_i(A) f_i(A) x \in W_i$. So

$$\mathbb{C}^n = \Sigma_{i=1}^K W_i \tag{9}$$

□

STEP3. Showing $W_{i,k} \cap W_{j,l} = \{0\}$ $(i \neq j)$. We assume $k = l = 1$. Let us fix arbitary $x \in W_{i,1} \cap W_{j,1}$. Because $0 = Ax - Ax = \alpha_i x - \alpha_j x = (\alpha_i - \alpha_j) x$, $x = 0$. So $W_{i,1} \cap W_{j,1} = \{0\}$ $(i \neq j)$. Nextly we assume if $k + l \leq K$ then $W_{i,k} \cap W_{j,l} = \{0\}$ $(i \neq j)$. Let us fix arbitary i, j, k, l such that $i \neq j$. Let us fix arbitary $x_0 \in W_{i,k} \cap W_{j,l}$. We set $s : \mathbb{C}^n \ni x \mapsto [x] \in \mathbb{C}^n / W_{1,1}$. Because $AW_{1,1} \subset W_{1,1}$, $\tilde{A} : \mathbb{C}^n / W_{1,1} \ni [x] \mapsto [Ax] \in \mathbb{C}^n / W_{1,1}$ is well-definied and linear. We set $\tilde{W_{i,k}} := \tilde{A} s(W_{i,k})$ and $\tilde{W_{i,l}} := \tilde{A} s(W_{i,l})$ We can assume $k > 1$. Clearly $\tilde{W_{i,k}} \subset \{[x] \in \tilde{W_{i,k}} | (\tilde{A} - \alpha_i)^{k-1} [x] = 0\}$. So by the assumption of mathematical induction, $\tilde{W_{i,k}} \cap \tilde{W_{j,l}} = \{0\}$. This implies that $W_{i,k} \cap W_{j,l} \subset W_{i,1}$. Similarly, $W_{i,k} \cap W_{j,l} \subset W_{j,1}$. So $W_{i,k} \cap W_{j,l} \subset W_{i,1} \cap W_{j,1} = \{0\}$. □

STEP4. Showing $\Sigma_{i=1}^K W_i = \oplus_{i=1}^K W_i$. By STEP3, $\Sigma_{i=1}^2 W_i = \oplus_{i=1}^2 W_i$. We assume if $K \leq K_0$ then $\Sigma_{i=1}^K W_i = \oplus_{i=1}^K W_i$. We will show if $K = K_0 + 1$ then $\Sigma_{i=1}^K W_i = \oplus_{i=1}^K W_i$. By the assumption of mathematicalinduction,

$$\Sigma_{i=1}^{K_0} W_i / W_{K_0+1} = \oplus_{i=1}^K W_i / W_{K_0+1} \tag{10}$$

Let us fix arbitary $w_i \in W_i$ $(i = 1, 2, ..., K_0 + 1)$ such that $\Sigma_{i=1}^{K_0+1} w_i = 0$. By (10), $w_i \in W_i \cap W_{K_0+1}$ $(i = 1, ..., K_0)$. By STEP3, $w_i = 0$ $(i = 1, ..., K_0)$. So $w_K = 0$. □

STEP5. Constructing a basis of W_i. Let us fix i. There is $\nu \leq m_i$ such that

$$W_{i,\nu-1} \subsetneq W_{i,\nu} = W_i$$

If $\nu = 1$, then we take a basis of $W_{i,1} = W_i$. If $\nu > 1$, there are $w_1, ..., w_{r_\nu}$ such that $\{w_j + W_{i,v-1}\}_{j=1}^{r_\nu}$ is a basis of $W_{i,\nu} / W_{i,v-1}$. Clearly $A_i w_1, ..., A_i w_{r_\nu}$ are containd in $W_{i,\nu-1}$. Here,

$$A_i := A - \alpha_i E$$

We will show $\{A_i^j w_k\}_{k=1,...,r_\nu,\ j=0,...,\nu-1}$ are linear independent. Let us fix any $\{a_i^j w_k\}_{k=1,...,r_\nu,\ j=0,...,\nu-1} \subset \mathbb{C}$ such that

$$\sum_{k=1}^{r_\nu} \sum_{j=0}^{\nu-1} a_{k,j} A_i^j w_k = 0$$

Then

$$\sum_{k=1}^{r_\nu} a_{k,0} w_k = -\sum_{k=1}^{r_\nu} \sum_{j=1}^{\nu-1} a_{k,j} A_i^j w_k$$

Because the right side is contained in $W_{i,\nu-1}$ and $\{w_j + W_{i,v-1}\}_{j=1}^{r_\nu}$ are linear independent,

$$a_{k,0} = 0 \ (\forall k)$$

So,

$$\sum_{k=1}^{r_\nu} \sum_{j=0}^{\nu-1} a_{k,j+1} A_i^{j+1} w_k = 0$$

This implies that

$$\sum_{k=1}^{r_\nu} a_{k,1} w_k + \sum_{k=1}^{r_\nu} \sum_{j=1}^{\nu-1} a_{k,j+1} A_i^j w_k = \sum_{k=1}^{r_\nu} \sum_{j=0}^{\nu-1} a_{k,j+1} A_i^j w_k \in W_{i,\nu-1}$$

Because $\sum_{k=1}^{r_\nu} \sum_{j=1}^{\nu-1} a_{k,j+1} A_i^j w_k$ is contained in $W_{i,\nu-1}$,

$$\sum_{k=1}^{r_\nu} a_{k,1} w_k \in W_{i,\nu-1}$$

Because $\{w_j + W_{i,v-1}\}_{j=1}^{r_\nu}$ are linear independent,

$$a_{k,1} = 0 \ (\forall k)$$

Hereafter, by repeating this discussion,

$$a_{k,j} = 0 \ (\forall k, j)$$

We set

$$U_{i,k} := \left\langle \{A_i^j w_k\}_{j=0,\ldots,\nu-1} \right\rangle$$

Clearly $U_{i,k}$ is A-invariant and the representation matrix of A respects to $\{A_i^j w_k\}_{j=0,\ldots,\nu-1}$ is the Jordan block whose order is ν.

We set

$$V_i := \sum_{k=1}^{r_\nu} U_{i,k}$$

Because V_i is A-invariant,

$$\tilde{A} : W_i/V_i \ni w + V_i \mapsto Aw + V_i \in W_i/V_i$$

is well-defined and linear. Because $\{w_j + W_{i,\nu-1}\}_{j=1}^{r_\nu}$ is a spanning set of $W_{i,\nu}/W_{i,\nu-1}$, for any $w \in W_{i,\nu}$,

$$w + W_{i,\nu-1} \in V_i + W_{i,\nu-1}$$

So,

$$A_i^{\nu-1} w \in V_i$$

This implies

$$(\tilde{A}_i - \alpha_i E)^{\nu-1} = 0$$

By applying the above argument to $\tilde{A}_i$, $\tilde{A}_i$ is broken into Jordan blocks whose order is less than ν with respect to some basis. □

STEP6. Showing (ii). (i) implies (ii). □

STEP7. Showing (iii). We set $M := j_k$ and $J := J_k(\alpha_i)$ and $\alpha := \alpha_i$ and $J_\alpha := J - \alpha E$. There are $w_{1,1} \in W_1$ and $w_{1,2} \in W_2$ sucht that

$$e_1 = w_{1,1} + w_{1,2}$$

Because

$$J_\alpha e_1 = 0$$

and W_1 is J_α-invariant and W_2 is J_α-invariant,

$$J_\alpha w_{1,1} = J_\alpha w_{1,2} = 0$$

and the kernel of J_α is $\mathbb{C}e_1$, there are a_1 and a_2 such that

$$w_{1,1} = a_1 e_1, w_{1,2} = a_2 e_1$$

If $a_1 = 0$, then $a_2 = 1$ and $\mathbb{C}e_1 \subset W_2$. If $a_1 \neq 0$, then $\mathbb{C}e_1 \subset W_1$. By replacing W_1 by W_2, we can assume $\mathbb{C}e_1 \subset W_1$. There are $w_{2,1} \in W_1$ and $w_{2,2} \in W_2$ sucht that

$$e_2 = w_{2,1} + w_{2,2}$$

Because $J_\alpha e_2 = e_1$,

$$e_1 = J_\alpha w_{2,1} + J_\alpha w_{2,2}$$

Because $\mathbb{C}e_1 \subset W_1$,

$$J_\alpha w_{2,2} = 0$$

So,

$$w_{2,2} \in W_2 \cap \mathbb{C}e_1 = \{0\}$$

This implies $e_2 \in W_1$. By repeating this argument, $e_1, e_2, ..., e_M \subset W_1$. □

Proposition 2. *We succeed notations in Theorem1. Let us assume*

$$f_A(x) = \Pi_{i=1}^{K}(x - \alpha_i)^{n_i}$$

Then

$$dimW_i = n_i$$

Proof. By the proof of Theorem1, the order of $J(\alpha_i)$ is $dimW_i$. So,

$$f_A = \Pi_{i=1}^{K} f_{J(\alpha_i)} = \Pi_{i=1}^{K}(x - \alpha_i)^{\dim W_i}$$

So,

$$\dim W_i = n_i$$

□

By Theorem1, it is easy to show the following famous theorem.

Theorem 2 (Cayley-Hamilton theorem)**.** *Let*

(S1) $A \in M(n, \mathbb{C})$.

(S2) f_A *is the characteristic polynomial.*

then

$$f_A(A) = O \tag{11}$$

Proof. We will show this theorem by mathematical induction. If $n = 1$, then this theorem holds. Because $f_{P^{-1}AP} = f_A$ for any $P \in GL(n, \mathbb{C})$, by Theorem1, we can assume A is an upper triangle matrix.

$$\begin{aligned} & f_A(A) \\ = & \Pi_{i=1}^{n}(A - \alpha_i E) \\ = & (A - \alpha_1 E)\Pi_{i=2}^{n}(A - \alpha_i E) \\ = & \begin{pmatrix} 0 & x \\ 0 & X \end{pmatrix} \Pi_{i=2}^{n}(A - \alpha_i E) \end{aligned}$$

For any a_1, a_2, A and b_1, b_2, B there is c_1, c_2 such that

$$\begin{pmatrix} a_1 & a_2 \\ 0 & A \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ 0 & B \end{pmatrix} = \begin{pmatrix} c_1 & c_2 \\ 0 & AB \end{pmatrix}$$

So, there are d_1, d_2 such that

$$\Pi_{i=2}^{n}(A - \alpha_i E) = \begin{pmatrix} d_1 & d_2 \\ 0 & O \end{pmatrix}$$

This implies

$$f_A(A) = \begin{pmatrix} 0 & x \\ 0 & X \end{pmatrix} \begin{pmatrix} d_1 & d_2 \\ 0 & O \end{pmatrix} = O$$

□

References

[1] Ichiro Satake, LINEAR ALGEBRA, ISBN-0 8247-1596-9.