Scientific Research Publishing

Advances in Linear Algebra & Matrix Theory, 2019, 9, 83-88
https://www.scirp.org/journal/alamt
ISSN Online: 2165-3348
ISSN Print: 2165-333X

A Minimality of the Rational Canonical Form

Heguo Liu[1], Honglian Zhang[2]

[1]School of Mathematics and Statistics, Hubei University, Wuhan, China
[2]Department of Mathematics, Shanghai University, Shanghai, China
Email: ghliu@hubu.edu.cn, hlzhangmath@shu.edu.cn

How to cite this paper: Liu, H.G. and Zhang, H.L. (2019) A Minimality of the Rational Canonical Form. *Advances in Linear Algebra & Matrix Theory*, **9**, 83-88.

https://doi.org/10.4236/alamt.2019.94006

Received: September 4, 2019
Accepted: November 12, 2019
Published: November 15, 2019

Abstract

The rational canonical form theorem is very essential basic result of matrix theory, which has been proved by different methods in the literature. In this note, we provide an efficient direct proof, from which the minimality for the decomposition of the rational canonical form can be found.

Keywords

Minimal Polynomial, Rational Canonical Form, Cyclic Subspace

1. Introduction

The rational canonical form, also called the Frobenius normal form, is one of the most useful and substantial canonical forms, which plays an essential role in many aspects of linear algebra. The rational canonical form of a matrix A is obtained by expressing it on a basis adapted to a decomposition into cyclic subspaces whose associated minimal polynomials are the invariant factors of A. Two matrices are similar if and only if they have the same rational canonical form. In the literature, there were a lot of approaches to understand and prove the rational canonical form theorem from different points of view ([1–3] etc.). For example, the author presented a pure matrix proof of the rational canonical form theorem in [4]. In this note, we will provide a brief alternative and self-contained proof of the well-known rational canonical theorem. The proof reflects a minimality for the decompositions of the vector space into cyclic subspaces since there is only one decomposition which can be reached from a given matrix. In particular, this ideal can also be generalized to others structural theorem in abstract algebra.

2. Main Results

Throughout this note, let F be a field and $F[\lambda]$ be the polynomial ring over F. Suppose that $\partial(f(\lambda))$ be the degree of the polynomial $f(\lambda)$ and V be the n-dimensional vector space over F. Here let A be

a fixed $n \times n$-matrix over F. For arbitrary nonzero vector $\alpha \in V$, denote by $m_\alpha(\lambda)$ the minimal polynomial of α associated to A, *i.e.*, the monic polynomial of the least degree among all polynomials in $\{f(\lambda)|f(A)\alpha = 0\}$. Let us begin with the following two lemmas which will be used in the sequel.

Lemma 2.1. *If $f_1(\lambda), f_2(\lambda), \cdots, f_n(\lambda)$ are coprime polynomials in $F[\lambda]$, that is $(f_1(\lambda), f_2(\lambda), \cdots f_n(\lambda)) = 1$, then there exists a $n \times n$-matrix M in $F[\lambda]$,*

$$M = \begin{bmatrix} f_1(\lambda) & f_2(\lambda) & & \cdots & f_n(\lambda) \\ & & & & \\ & & W & & \end{bmatrix}$$

such that $detM = 1$.

Proof. Here we use induction on n. Firstly, if $n = 2$, there exist two polynomials $u(\lambda), v(\lambda) \in F[\lambda]$, such that $u(\lambda)f_1(\lambda) + v(\lambda)f_2(\lambda) = 1$. Therefore we obtain

$$M = \begin{bmatrix} f_1(\lambda) & f_2(\lambda) \\ -v(\lambda) & u(\lambda) \end{bmatrix},$$

which satifies $detM = 1$.

In general case, let us denote $d(\lambda) = (f_1(\lambda), f_2(\lambda), \cdots, f_{n-1}(\lambda))$ and set $f_i(\lambda) = d(\lambda)g_i(\lambda)$ for $1 \leq i \leq n-1$. Immediately, it is easy to see that

$$(g_1(\lambda), g_2(\lambda), \cdots, g_{n-1}(\lambda)) = 1. \tag{1}$$

By inductive hypothesis, there exists a $(n-1) \times (n-1)$-matrix N in $F[\lambda]$ such that $\det N = 1$. Suppose

$$N = \begin{bmatrix} g_1(\lambda) & g_2(\lambda) & \cdots & g_{n-1}(\lambda) \\ & & & \\ & & W_1 & \end{bmatrix}.$$

On the other hand, thanks to $(d(\lambda), f_n(\lambda)) = 1$, there exist $p(\lambda), q(\lambda) \in F[\lambda]$ such that

$$p(\lambda)d(\lambda) + q(\lambda)f_n(\lambda) = 1. \tag{2}$$

Consequently, we get the $n \times n$-matix M that we want as follows:

$$M = \begin{bmatrix} f_1(\lambda) & f_2(\lambda) & \cdots & f_{n-1}(\lambda) & f_n(\lambda) \\ & & & & \\ & & W_1 & & 0 \\ & & & & \\ -q(\lambda)g_1(\lambda) & -q(\lambda)g_2(\lambda) & \cdots & -q(\lambda)g_{n-1}(\lambda) & p(\lambda) \end{bmatrix},$$

It is clear that $detM = 1$. □

The following lemma will be used in the proof of the uniqueness.

Lemma 2.2. *If there exist two decompositions for the vector space V over F associated to A,*

$$V = F[A]\alpha_1 \oplus F[A]\alpha_2 \oplus \cdots \oplus F[A]\alpha_r \tag{3}$$
$$nonumber = F[A]\beta_1 \oplus F[A]\beta_2 \oplus \cdots \oplus F[A]\beta_s, \tag{4}$$

where α_i, β_j are the nonzero vectors in V such that

$$\begin{aligned} m_{\alpha_1}(\lambda) \mid m_{\alpha_2}(\lambda) \mid \cdots \mid m_{\alpha_r}(\lambda), \\ m_{\beta_1}(\lambda) \mid m_{\beta_2}(\lambda) \mid \cdots \mid m_{\beta_s}(\lambda). \end{aligned} \tag{5}$$

Then $r = s$.

Proof. Let $p(\lambda)$ be an irreducible factor of $m_{\alpha_1}(\lambda)$. First, we have

$$V = F[A]\alpha_1 \oplus \cdots \oplus F[A]\alpha_r,$$

Then we get,

$$p(A)V = F[A]\big(p(A)\alpha_1\big) \oplus \cdots \oplus F[A]\big(p(A)\alpha_r\big).$$

It is clear that,

$$\dim\big(p(A)V\big) = \dim V - r\partial\big(p(\lambda)\big).$$

On the other hand, we have,

$$\begin{aligned}
&\dim\big(p(A)V\big)\\
&= \sum_{j=1}^{s}\Big(F[A]\big(p(A)\beta_j\big)\dim\Big)\\
&= \sum_{j=1}^{s}\Big(\partial\big(m_{\beta_j}(\lambda)\big) - \partial\big((p(\lambda), m_{\beta_j}(\lambda))\big)\Big)\\
&= \dim V - \sum_{j=1}^{s}\partial\big((p(\lambda), m_{\beta_j}(\lambda))\big).
\end{aligned}$$

It follows immediately that,

$$r\partial\big(p(\lambda)\big) = \sum_{j=1}^{s}\partial\big((p(\lambda), m_{\beta_j}(\lambda))\big)\Big), \tag{6}$$

which implies that $r \le s$.

Similarly, we can also get that $s \le r$, therefore we have $r = s$. □

Now we turn to state the rational canonical form theorem and give a direct efficient proof, from which we can display the minimality of the rational canonical form.

Theorem 2.3. *There exits a decomposition*

$$V = F[A]\alpha_1 \oplus F[A]\alpha_2 \oplus \cdots \oplus F[A]\alpha_r, \tag{7}$$

where $\alpha_1, \alpha_2, \cdots, \alpha_r$ are the nonzero vectors of V, and $m_{\alpha_1}(\lambda) \mid m_{\alpha_2}(\lambda) \mid \cdots \mid m_{\alpha_r}(\lambda)$.

If there exits another decomposition

$$V = F[A]\beta_1 \oplus F[A]\beta_2 \oplus \cdots \oplus F[A]\beta_s, \tag{8}$$

where $\beta_1, \beta_2, \cdots, \beta_s$ are the nonzero vectors of V, and $m_{\beta_1}(\lambda) \mid m_{\beta_2}(\lambda) \mid \cdots \mid m_{\beta_s}(\lambda)$, then $r = s$, and $m_{\alpha_i}(\lambda) = m_{\beta_i}(\lambda)$ for every $1 \le i \le r$.

Proof. Firstly, for any decomposition

$$V = F[A]v_1 + F[A]v_2 + \cdots + F[A]v_t,$$

such that $1 \le m_{v_1}(\lambda) \le m_{v_2}(\lambda) \le \cdots \le m_{v_t}(\lambda)$, we define a $(t+1)$-tuple vector associated to this decomposition,

$$\Big(t, \partial\big(m_{v_1}(\lambda)\big), \partial\big(m_{v_2}(\lambda)\big), \cdots, \partial\big(m_{v_t}(\lambda)\big)\Big). \tag{9}$$

Let S be the set of all these vectors. Clearly S is a totally ordered set on the lexicographical order from small to large. Then there exists a minimal element of S denoted by

$$\Big(r, \partial\big(m_{\alpha_1}(\lambda)\big), \partial\big(m_{\alpha_2}(\lambda)\big), \cdots, \partial\big(m_{\alpha_r}(\lambda)\big)\Big). \tag{10}$$

The corresponding decomposition is written as

$$V = F[A]\alpha_1 + F[A]\alpha_2 + \cdots + F[A]\alpha_r, \tag{11}$$

which will be verified to be the rational canonical form we expected.

For the decomposition $V = F[A]\alpha_1 + F[A]\alpha_2 + \cdots + F[A]\alpha_r$, we first need to verify $m_{\alpha_i}(\lambda) \mid m_{\alpha_{i+1}}(\lambda)$ for $i = 1, 2, \cdots r-1$.

By contradiction, if not, then for some i, we have $\big(m_{\alpha_i}(\lambda), m_{\alpha_{i+1}}(\lambda)\big) = d(\lambda)$ such that $\partial\big(d(\lambda)\big) < \partial\big(m_{\alpha_i}(\lambda)\big)$. There exist $u(\lambda), v(\lambda) \in F[\lambda]$ such that

$$u(\lambda)\frac{m_{\alpha_i}(\lambda)}{d(\lambda)} + v(\lambda)\frac{m_{\alpha_{i+1}}(\lambda)}{d(\lambda)} = 1. \tag{12}$$

Denote $\gamma_i = \frac{m_{\alpha_i}(A)}{d(A)}\alpha_i + \frac{m_{\alpha_{i+1}}(A)}{d(A)}\alpha_{i+1}$, and $\gamma_{i+1} = -v(A)\alpha_i + u(A)\alpha_{i+1}$. It is obvious that,

$$F[A]\alpha_i + F[A]\alpha_{i+1} = F[A]\gamma_i + F[A]\gamma_{i+1},$$

such that $m_{\gamma_i}(\lambda) | d(\lambda)$. Therefore we have immediately,

$$\begin{aligned} V &= F[A]\alpha_1 + F[A]\alpha_2 + \cdots + F[A]\alpha_i + F[A]\alpha_{i+1} + \cdots + F[A]\alpha_r \\ &= F[A]\alpha_1 + F[A]\alpha_2 + \cdots + F[A]\gamma_i + F[A]\gamma_{i+1} + \cdots + F[A]\alpha_r, \end{aligned} \tag{13}$$

which contradicts with the minimality of $\Big(r, \partial\big(m_{\alpha_1}(\lambda)\big), \partial\big(m_{\alpha_2}(\lambda)\big), \cdots, \partial\big(m_{\alpha_r}(\lambda)\big)\Big)$.

Next, we focus on checking

$$V = F[A]\alpha_1 \oplus F[A]\alpha_2 \oplus \cdots \oplus F[A]\alpha_r.$$

If not, let $f_j(A)\alpha_j + f_{j+1}(A)\alpha_{j+1} + \cdots + f_r(A)\alpha_r = 0$, where $f_j(A)\alpha_j \neq 0$, and $\partial\big(f_j(\lambda)\big) < \partial\big(m_j(\lambda)\big)$. Denote that

$$e(\lambda) = \big(f_j(\lambda), f_{j+1}(\lambda), \cdots f_r(\lambda)\big) \tag{14}$$

and

$$\delta_j = \frac{f_j(A)}{e(A)}\alpha_j + \frac{f_{j+1}(A)}{e(A)}\alpha_{j+1} + \cdots + \frac{f_r(A)}{e(A)}\alpha_r. \tag{15}$$

It is clear that $e(A)\delta_j = 0$, and $m_{\delta_j}(\lambda) | e(\lambda)$.

On the other hand, it holds that

$$\partial\big(m_{\delta_j}(\lambda)\big) \leq \partial\big(e(\lambda)\big) \leq \partial\big(f_j(\lambda)\big) < \partial\big(m_{\alpha_j}(\lambda)\big). \tag{16}$$

By Lemma 2.1, there exits a matrix M in $F[\lambda]$ with $detM = 1$ as follows.

$$M = \begin{bmatrix} \frac{f_j(\lambda)}{e(\lambda)} & \frac{f_{j+1}(\lambda)}{e(\lambda)} & \cdots & \frac{f_r(\lambda)}{e(\lambda)} \\ f_{j+1,j}(\lambda) & f_{j+1,j+1}(\lambda) & \cdots & f_{j+1,r}(\lambda) \\ \cdots & \cdots & \cdots & \cdots \\ f_{r,j}(\lambda) & f_{r,j+1}(\lambda) & \cdots & f_{r,r}(\lambda) \end{bmatrix}.$$

Using the above matrix, we further define that

$$\begin{cases} \delta_j = \frac{f_j(\lambda)}{e(\lambda)}\alpha_j + \frac{f_{j+1}(\lambda)}{e(\lambda)}\alpha_{j+1} + \cdots + \frac{f_r(\lambda)}{e(\lambda)}\alpha_r \\ \delta_{j+1} = f_{j+1,j}(A)\alpha_j + f_{j+1,j+1}(A)\alpha_{j+1} + \cdots + f_{j+1,r}(A)\alpha_r \\ \cdots\cdots \\ \delta_r = f_{r,j}(A)\alpha_j + f_{r,j+1}(A)\alpha_{j+1} + \cdots + f_{r,r}(A)\alpha_r \end{cases}$$

It follows directly that

$$\begin{aligned} & F[A]\alpha_j \oplus F[A]\alpha_{j+1} \oplus \cdots \oplus F[A]\alpha_r \\ = \; & F[A]\delta_j \oplus F[A]\delta_{j+1} \oplus \cdots \oplus F[A]\delta_r, \end{aligned}$$

which implies that

$$V = F[A]\alpha_1 \oplus F[A]\alpha_2 \oplus \cdots \oplus F[A]\alpha_{j-1} + F[A]\delta_j + \cdots + F[A]\delta_r.$$

Thanks to the minimality of

$$\Big(r, \partial\big(m_{\alpha_1}(\lambda)\big), \partial\big(m_{\alpha_2}(\lambda)\big), \cdots, \partial\big(m_{\alpha_r}(\lambda)\big)\Big),$$

we get a contradiction.

So far, we have checked the existence, it suffices to verify the uniqueness. Suppose that there exists another decomposition of V

$$V = F[A]\beta_1 \oplus F[A]\beta_2 \oplus \cdots \oplus F[A]\beta_s,$$

where $\beta_1, \beta_2, \cdots, \beta_s$ are the nonzero vectors of V such that

$$m_{\beta_1}(\lambda) \;\mid\; m_{\beta_2}(\lambda) \;\mid\; \cdots \;\mid\; m_{\beta_s}(\lambda).$$

It is clear that $r = s$ by Lemma 2.2. Furthermore, it follows easily that,

$$\begin{aligned} m_{\alpha_1}(A)V &= F[A]\big(m_{\alpha_1}(A)\alpha_1\big) \oplus F[A]\big(m_{\alpha_1}(A)\alpha_2\big) \cdots \oplus F[A]\big(m_{\alpha_1}(A)\alpha_r\big) \\ &= F[A]\big(m_{\alpha_1}(A)\beta_1\big) \oplus F[A]\big(m_{\alpha_1}(A)\beta_2\big) \cdots \oplus F[A]\big(m_{\alpha_1}(A)\beta_s\big) \end{aligned}$$

Note that $m_{\alpha_1}(A)\alpha_1 = 0$. Meanwhile, it follows from Lemma 2.2 easily that

$$m_{\alpha_1}(A)\beta_1 = 0, \quad m_{\beta_1}(\lambda) | m_{\alpha_1}(\lambda).$$

Similarly, one has $m_{\alpha_1}(\lambda) | m_{\beta_1}(\lambda)$. That means $m_{\alpha_1}(\lambda) = m_{\beta_1}(\lambda)$.

Repeating the above steps, it is easy to get that for $i = 2, 3, \cdots r$

$$m_{\alpha_i}(\lambda) = m_{\beta_i}(\lambda).$$

In other words, there exists only one decomposition corresponding to the unique minimal element of S. We have completed the proof. □

3. Conclusion

For a vector space V, the decomposition of V associated to the rational canonical form is exact the unique minimal element in our sense, which reveals the minimality of the rational canonical form on the lexicographical order.

Acknowledgements

We thank the Editor and the referee for their comments. Research of H. Liu is funded the National Natural Science Foundation of China grant No.11771129. Research of H. Zhang is funded the National Natural Science Foundation of China Grant No.11871325.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Halmos, P. (1974) Finite-Dimensional Vector Spaces. Springer-Verlag, New York. https://doi.org/10.1007/978-1-4612-6387-6

[2] Horn, R.A. and Johnson, C.R. (1985) Matrix Analysis. Cambridge University Press, Cambridge.

[3] Jacobson, N. (1953) Lectures in Abstract Algebras II Linear Algebra. Springer-Verlag, New York. https://doi.org/10.1007/978-1-4684-7053-6

[4] Hartwig, R.E. (1996) Roth's Removal Rule and the Rational Canonical Form. *The American Mathematical Monthly*, **103**, 332-335. https://doi.org/10.1080/00029890.1996.12004746