Advances in Linear Algebra & Matrix Theory, **2012, 2, 48-50**
http://dx.doi.org/10.4236/alamt.2012.24008 Published Online December 2012 (http://www.SciRP.org/journal/alamt)

On the Minimal Polynomial of a Vector

Dabin Zheng, Heguo Liu
Faculty of Mathematics and Computer Science, Hubei University, Wuhan, China
Email: dzheng@hubu.edu.cn, ghliu@hubu.edu.cn

Received October 26, 2012; revised November 30, 2012; accepted December 9, 2012

ABSTRACT

It is well known that the Cayley-Hamilton theorem is an interesting and important theorem in linear algebras, which was first explicitly stated by A. Cayley and W. R. Hamilton about in 1858, but the first general proof was published in 1878 by G. Frobenius, and numerous others have appeared since then, for example see [1,2]. From the structure theorem for finitely generated modules over a principal ideal domain it straightforwardly follows the Cayley-Hamilton theorem and the proposition that there exists a vector *v* in a finite dimensional linear space *V* such that *v* and a linear transformation of *V* have the same minimal polynomial. In this note, we provide alternative proofs of these results by only utilizing the knowledge of linear algebras.

Keywords: Finite Dimensional Linear Space; Linear Transformation; Minimal Polynomial

1. Introduction

Let F be a field, V be a vector space over F with dimension n, and φ be a linear transformation of V. It is known that V becomes a $F[x]$-module according to the following definition:

$$F[x]\times V \to V$$

$$(f(x), v) \mapsto f(\varphi)v.$$

For a fixed linear transformation φ and a vector $v\in V$, the annihilator of v with respective to φ is defined to be

$$ann(v)=\{p(x)\in F[x] \mid p(\varphi)v=0\}.$$

Similarly, the annihilator of V with respective to φ is defined to be

$$ann(V)=\{p(x)\in F[x] \mid p(\varphi)v=0, \forall v\in V\}.$$

Since $F[x]$ is a principal ideal domain the ideals $ann(v)$ and $ann(V)$ can be generated by the unique monic polynomials, denote them by $m_v(x)$ and $m_\varphi(x)$, respectively. Which are called the order ideals of v and V in abstract algebras, respectively. They are also called the minimal polynomials of v and V with respective to φ in linear algebras, respectively. It is clear that the minimal polynomial of zero vector (or zero transformation) is 1. By the structure theorem for finitely generated modules over a principal ideal domain [3,4], the module V can be decomposed into a direct sum of finite cyclic submodules:

$$V = F[x]\alpha_1 + F[x]\alpha_2 + \cdots + F[x]\alpha_s, \tag{1}$$

and $\alpha_1,\alpha_2,\cdots,\alpha_s$ are vectors in V such that

$$ann(\alpha_i)=\langle d_i(x)\rangle, d_i(x)\mid d_{i+1}(x), \tag{2}$$

where $i=1,2,\cdots,s-1$. Let $\Delta_\varphi(x)$ be the characteristic polynomial of φ. By (1) and (2) one has

- $m_\varphi(x)=ann(\alpha_s)=d_s(x)$;
- $\Delta_\varphi(x)=\prod_{i=1}^{s} ann(\alpha_i)=\prod_{i=1}^{s} d_i(x)$.

Furthermore, these results straightforwardly imply the following theorem:

Theorem 1. [3,4] With the notations as above, we have

1) [**Cayley-Hamilton Theorem**]

$$m_\varphi(x)\mid\Delta_\varphi(x), \text{ and so } \Delta_\varphi(\varphi)=0.$$

2) There exists a vector $v\in V$ such that

$$m_v(x)=m_\varphi(x).$$

2. Proofs Based on Linear Algebras

In this section we give an alternative proof of Theorem 1 by only utilization of knowledge of linear algebras. To demonstrate an interesting proof of some proposition in linear algebras and its applications, we present two proofs of (2) in Theorem 1 for infinite fields and arbitrary fields, respectively, and then use the related results to prove the Cayley-Hamilton theorem.

The following lemma provide an interesting proof of an proposition in linear algebras that a vector space over an infinite field can not be an union of a finite number of its proper subspaces by Vandermonde determinants.

Lemma 1. Let F be an infinite field, and V be a vector space over F with dimension n, and V_i be nontrivial subspaces of V for $i=1,2,\cdots,s$. Then there exists infinite many bases of V such that any element of them is not in each V_i for $i=1,2,\cdots,s$. Therefore, if $V=\bigcup_{i=1}^{s}V_i$ then $V=V_i$ for some i.

Proof: Let $\alpha_1,\alpha_2,\cdots,\alpha_n$ be a F-base of V. For any $b\in F$ we set

$$\beta_b=\alpha_1+b\alpha_2+b^2\alpha_3+\cdots+b^{n-1}\alpha_n .$$

Let $b_1,b_2,\cdots,b_n$ distinct elements in F. We have

$$\left(\beta_{b_1},\beta_{b_2},\cdots,\beta_{b_n}\right)=\left(\alpha_1,\alpha_2,\cdots,\alpha_n\right)Van\left(b_1,b_2,\cdots,b_n\right)$$

where $Van\left(b_1,b_2,\cdots,b_n\right)$ is a Vandemonde matrix. So $\beta_{b_1},\beta_{b_2},\cdots,\beta_{b_n}$ is a base of V because the determinant of $Van\left(b_1,b_2,\cdots,b_n\right)$ is nonzero. Let S be the following set with an infinite number of vectors:

$$S=\left\{\beta_b \mid b\in F\right\}.$$

Since V_i with $i=1,2,\cdots,s$ is a nontrivial subspace of V one can verify that $\left|S\cap V_i\right|\le n-1$. And so

$$\left|S\cap\left(\bigcup_{i=1}^{s}V_i\right)\right|=\left|\bigcup_{i=1}^{s}\left(S\cap V_i\right)\right|\le s\left(n-1\right).$$

Therefore, $S\setminus S\cap\left(\bigcup_{i=1}^{s}V_i\right)$ is infinite, and any distinct n vectors in the set constitute a base of V.

Proposition 1. Let F be an infinite field. Let V be a F-vector space with dimension n, and φ be a linear transformation of V. Then there exists a vector $v\in V$ such that $m_v\left(x\right)=m_\varphi\left(x\right)$.

Proof: It is clear that $1,\varphi,\varphi^2,\cdots,\varphi^{n^2}$ are linearly dependent over F. So the degree $\deg\left(m_\varphi\left(x\right)\right)\le n^2$. For any $v\in V$, the minimal polynomial $m_v\left(x\right)$ of v is a monic factor of $m_\varphi\left(x\right)$. So there exist finite number of vectors $v_i, i=1,2,\cdots,s$ such that

$$m_\varphi\left(x\right)=m_{v_1}\left(x\right)m_{v_2}\left(x\right)\cdots m_{v_s}\left(x\right),$$

where $m_{v_i}\left(x\right)'s$ are mutually coprime irreducible polynomials. Set $V_i=\left\{\alpha\in V \middle| m_{v_i}\left(\varphi\right)\alpha=0\right\}$. One can verify that

$$V=V_1\cup V_2\cup\cdots\cup V_s .$$

By Lemma 1, there exists k with $1\le k\le s$ such that $V=V_k$. Which shows that

$$m_{v_k}\left(\varphi\right)\alpha=0,\ \text{for all } \alpha\in V ,$$

and so $m_{v_k}\left(\varphi\right)$ is a zero linear transformation. Hence we have $m_{v_k}\left(x\right)=m_\varphi\left(x\right)$.

In fact, Proposition 1 holds for arbitrary fields from the introduction. To obtain a general proof we first give the following lemma.

Lemma 2. Let F be a field, V be a n-dimensional linear space over F, and φ be a linear transformation of V. For any $0\ne\beta,\gamma\in V$, there exists $\alpha\in V$ such that

$$m_\alpha\left(x\right)=lcm\left(m_\beta\left(x\right),m_\gamma\left(x\right)\right),$$

here lcm and the following gcd stand for the least common multiple and greatest common divisor of two polynomials, respectively.

Proof: By properly arrangement, the minimal polynomials of β,γ with respective to φ have the following irreducible factorization respectively,

$$m_\beta\left(x\right)=\underbrace{p_1^{k_1}\cdots p_r^{k_r}}_{u_1(x)}\ \underbrace{p_{r+1}^{k_{r+1}}\cdots p_s^{k_s}}_{u_2(x)},$$

$$m_\gamma\left(x\right)=\underbrace{p_1^{l_1}\cdots p_r^{l_r}}_{v_1(x)}\ \underbrace{p_{r+1}^{l_{r+1}}\cdots p_s^{l_s}}_{v_2(x)}.$$

Moreover, $k_i\ge l_i$ for $i=1,2,\cdots,r$, and $k_i\le l_i$ for $i=r+1,\cdots,s$. So, we have

$$lcm\left(m_\beta\left(x\right),m_\gamma\left(x\right)\right)=u_1\left(x\right)v_2\left(x\right),$$

$$\gcd\left(u_1\left(x\right),v_2\left(x\right)\right)=1.$$

One can verify that the minimal polynomials of $u_2\left(\varphi\right)\beta$ and $v_1\left(\varphi\right)\gamma$ are

$$m_{u_2(\varphi)\beta}\left(x\right)=u_1\left(x\right),\quad m_{v_1(\varphi)\gamma}\left(x\right)=v_2\left(x\right),$$

respectively. Set $\alpha=u_2\left(\varphi\right)\beta+v_1\left(\beta\right)\gamma$, then

$$u_1\left(\varphi\right)v_2\left(\varphi\right)\alpha=0.$$

Which implies that

$$m_\alpha\left(x\right)\big|u_1\left(x\right)v_2\left(x\right). \tag{3}$$

Conversely, from $u_2\left(\varphi\right)\beta=\alpha-v_1\left(\varphi\right)\gamma$ it follows that

$$m_\alpha\left(\varphi\right)m_{v_1(\varphi)\gamma}\left(\varphi\right)\left(u_2\left(\varphi\right)\beta\right)=0.$$

Which shows that

$$m_{u_2(\varphi)\beta}\left(x\right)\big|m_\alpha\left(x\right)m_{v_1(\varphi)\gamma}\left(x\right),\ i.e.\ u_1\left(x\right)\big|m_\alpha\left(x\right)v_2\left(x\right)$$

So, $u_1\left(x\right)\big|m_\alpha\left(x\right)$ since $\gcd\left(u_1\left(x\right),v_2\left(x\right)\right)=1$ Similarly, $v_2\left(x\right)\big|m_\alpha\left(x\right)$. By $\gcd\left(u_1\left(x\right),v_2\left(x\right)\right)=1$ again, we have

$$u_1\left(x\right)v_2\left(x\right)\big|m_\alpha\left(x\right). \tag{4}$$

Equations (3) and (4) imply that

$$m_\alpha\left(x\right)=u_1\left(x\right)v_2\left(x\right)=lcm\left(m_\beta\left(x\right)m_\gamma\left(x\right)\right).$$

Proposition 2. Let F be a field. Let V be a

F-vector space with dimension n and φ be a linear transform of V. Then there exists a vector $v \in V$ such that

$$m_v(x) = m_\varphi(x).$$

Proof: Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be a F-base of V. One can verify that

$$m_\varphi(x) = lcm\left(m_{\alpha_1}(x), m_{\alpha_2}(x), \cdots, m_{\alpha_n}(x)\right).$$

By repeatedly utilization of Lemma 2, we can find a vector $v \in V$ such that

$$m_\varphi(x) = lcm\left(m_{\alpha_1}(x), m_{\alpha_2}(x), \cdots, m_{\alpha_n}(x)\right) = m_v(x).$$

According to Proposition 2, we can easily deduce the Cayley-Hamilton theorem.

Proof of Cayley-Hamilton Theorem: Let $\Delta_\varphi(x)$ be the characteristic polynomial of φ. We show $m_\varphi(x) | \Delta_\varphi(x)$. By Proposition 2 there exists $v \in V$ such that $m_v(x) = m_\varphi(x)$. Let

$$m_\varphi(x) = m_v(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

So, one can verify that vectors $v, \varphi(v), \cdots, \varphi^{m-1}(v)$ are linearly independent over F. We extend them to a basis of V as follows:

$$v, \varphi(v), \cdots, \varphi^{m-1}(v), \alpha_1, \cdots, \alpha_{n-m}.$$

We have

$$\begin{aligned}&\varphi\left(v, \cdots, \varphi^{m-1}(v), \alpha_1, \cdots, \alpha_{n-m}\right) \\ &= \left(v, \cdots, \varphi^{m-1}(v), \alpha_1, \cdots, \alpha_{n-m}\right)\begin{pmatrix} B & X \\ 0 & C \end{pmatrix}\end{aligned}$$

where the m square matrix B has the form

$$B = \begin{pmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & \cdots & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -b_{m-1} \end{pmatrix}$$

and C is an $n-m$ square matrix, and X is an $m \times (n-m)$ matrix. So the characteristic polynomial of φ is

$$\Delta_\varphi(x) = \left| xI_n - \begin{pmatrix} B & X \\ 0 & C \end{pmatrix} \right| = |xI_m - B||xI_{n-m} - C|,$$

and

$$|xI_m - B| = x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

Hence, $m_\varphi(x) | \Delta_\varphi(x)$, and $\Delta_\varphi(\varphi) = 0$.

Actually, the Cayley-Hamilton theorem can be obtained by only using the minimal polynomial of a vector.

Another Proof of Cayley-Hamilton Theorem: Let $\Delta_\varphi(x)$ be the characteristic polynomial of φ. For any $v \in V$ let $m_v(x)$ be the minimal polynomial of the vector v with respective to φ. To prove the Cayley-Hamilton theorem, it is enough to show that

$$m_v(x) | \Delta_\varphi(x) \text{ for any } v \in V.$$

This statement can be verified by the same arguments as that in above proof.

3. Acknowledgements

The authors would like to thank the anonymous referees for helpful comments. The work of both authors was supported by the Fund of Linear Algebras Quality Course of Hubei Province of China. The work of D. Zheng was supported by the National Natural since Foundation of China (NSFC) under Grant 11101131.

REFERENCES

[1] K. Hoffman and R. Kunze, "Linear Algebra," 2nd Edition, Prentice Hall Inc., Upper Saddle River, 1971.

[2] R. A. Horn and C. R. Johnson, "Matrix Analysis," Cambridge University Press, Cambridge, 1986.

[3] N. Jacobson, "Basic Algebra I," 2nd Edition, W. H. Freeman and Company, New York, 1985.

[4] Th. W. Hungerford, "Algebra, GTM 73," Springer-Verlag, New York, 1980. doi:10.1007/978-1-4612-6101-8