



MINIMAL POLYNOMIALS AND CHARACTERISTIC POLYNOMIALS OVER RINGS

HIROYUKI ISHIBASHI

Department of Mathematics

Josai University

Sakado, Saitama 350-02, Japan

e-mail: hishi@math.josai.ac.jp

Abstract

Let R be a commutative ring with 1, and M be a free module of a finite rank over R . $\text{End}_R M$ is the endomorphism ring of M over R , σ is an element in $\text{End}_R M$, and the matrix of σ diagonalizable. Our purpose is to investigate the relationship between the characteristic polynomial χ_σ of σ and the minimal polynomial p_σ of σ . If R is an integral domain, then we shall show that p_σ is uniquely determined as a monic polynomial dividing χ_σ . Also, the difference between the two sets of zeros of p_σ and χ_σ , respectively, is only the multiplicity of their roots. If R is not an integral domain, then we shall construct σ such that p_σ is not necessarily monic nor divides χ_σ .

1. Introduction

Let F be a field and V be a finite dimensional vector space over F . Let $\text{End}_F V$ be the endomorphism ring of V over F , and let σ be in $\text{End}_F V$. Also let $F[t]$ be the polynomial ring in t over F . Then, it is well known the relationship between

2010 Mathematics Subject Classification: 15A04, 15A23, 15A33.

Keywords and phrases: minimal polynomial, characteristic polynomial, endomorphisms ring of modules, classical groups.

Received October 22, 2010

$\chi_\sigma(t) \in F[t]$ the characteristic polynomial of σ and $p_\sigma(t) \in F[t]$ the minimal polynomial of σ . For instance, $\chi_\sigma(a) = 0$ for a in F if and only if $p_\sigma(a) = 0$, that is, the difference between the two sets of roots of χ_σ and p_σ , respectively, is only the multiplicity of their roots.

Further, if F is sufficiently large, say, an algebraically closed field, then $\chi_\sigma(t)$ is a product of linear equations. Moreover, if these roots of $\chi_\sigma(t)$ are different each other, then σ is diagonalizable. Above observation about linear endomorphism σ of a vector space V over a field F pose us a question what will occur if we replace F the field to R a commutative ring, V the vector space to M a free module over R , and σ in $\text{End}_F V$ to σ in $\text{End}_R M$ of which matrix is diagonalizable. The purpose of this note is to answer partially to the question.

Estes and Guralnick [2] investigated what the possible minimal polynomials are for integral symmetric matrices. Augot and Camion [1] presented algorithms connected with computation of the minimal polynomial of an $n \times n$ matrix over a field K . Fiedler [3] showed that for a given polynomial, we can construct a symmetric matrix whose characteristic polynomial is the given polynomial. Schmeisser [5] proved that for a given polynomial $f(x)$ with only real zeros, we can construct a real symmetric tridiagonal matrix whose characteristic polynomial is $(-1)^n f(x)$ with $n = \deg f$. We will refer Lang [4] as a standard text book in algebra, in which the reader will find necessary concepts and materials.

2. Preliminaries

Throughout in the paper, R is a commutative ring with the identity 1, $R[t]$ is the polynomial ring in t over R , M is a free module over R of rank n with $X = \{x_1, x_2, \dots, x_n\}$ a basis for M , and $\text{End}_R M$ is the endomorphism ring of M over R . For an element σ in $\text{End}_R M$, we write

$$\sigma \underset{X}{\simeq} A$$

if A in $M_n(R)$ is the matrix of σ relative to X , where $M_n(R)$ denotes the ring of matrices of $n \times n$ over R . We define the characteristic polynomial $\chi_\sigma(t)$, χ_σ or $\chi(t)$ of A (or σ) to be the determinant

$$|t \cdot I - A|$$

in $R[t]$. By definition, it is independent to the choice of the basis X for M . Also, it is monic and unique for σ . An element a in R is called an *eigenvalue* or a *characteristic root* of σ in R if it is a root of χ_σ , i.e., $\chi_\sigma(a) = 0$. For σ in $\text{End}_R M$, we have a canonical ring homomorphism

$$\pi : R[t] \rightarrow \text{End}_R M$$

defined by $\pi(f(t)) = f(\sigma)$ for $f(t)$ in $R[t]$. Therefore, M may be viewed as an $R[t]$ -module, defining the operation of $R[t]$ on M by letting $f(t)x = f(\sigma)x$ for $f(t)$ in $R[t]$ and x in M .

Lemma 2.1. $\chi_\sigma(\sigma) = 0$.

Proof. See Theorem 3.1 (Caley-Hamilton) in Lang [4, p. 561].

We note that $\ker \pi \neq \{0\}$, for it contains at least $\chi_\sigma \neq 0$ by Lemma 2.1. Let P be the set of monic polynomials in $R[t]$, for which we define K_0 and K_1 , two subsets of $\ker \pi$ as follows:

K_0 = The set of non-zero polynomials in $\ker \pi$ of which degree is the lowest in $\ker \pi$.

K_1 = The set of non-zero polynomials in $P \cap \ker \pi$ of which degree is the lowest in $P \cap \ker \pi$.

Clearly, $K_0 \neq \emptyset$ and $K_1 \neq \emptyset$, for $\ker \pi$ contains a monic polynomial χ_σ . We call any polynomial in K_0 a *minimal polynomial* of σ and denote it by $p_\sigma(t)$, also any one in K_1 a *small polynomial* of σ and write it as $q_\sigma(t)$. As we know if R is a field, then there exists always a unique minimal polynomial which is monic. In particular, in such a case we may take $p_\sigma(t) = q_\sigma(t)$. As a matter of course, in general, p_σ and q_σ are not necessarily unique for σ . Indeed, if p_σ is a minimal polynomial, so is cp_σ for any c in R with $cp_\sigma \neq 0$. Also, if q_σ is a small polynomial with $\deg p_\sigma < \deg q_\sigma$, so is $p_\sigma + q_\sigma$. On the other hand, it is clear that both $\deg p_\sigma$ and $\deg q_\sigma$ are unique for σ , and we have

$$\deg p_\sigma \leq \deg q_\sigma.$$

Lemma 2.2. (a) *The following conditions (a₁) and (a₂) are equivalent:*

(a₁) $\deg p_\sigma = \deg q_\sigma$ for any (or some) $p_\sigma \in K_0$ and any (or some) $q_\sigma \in K_1$

and

(a₂) *there is a monic minimal polynomial p_σ .*

(b) *In case of (a), p_σ is a unique for σ .*

Proof. Since (a) is clear, we prove (b). Let u and v be both monic minimal polynomials. Then since $\deg u = \deg v$ and they are monic, we have $\deg(u - v) < \deg u$. On the other hand, since u, v , are in $\ker \pi$, so is $u - v$. Hence $u - v = 0$ by the minimality of u . Thus $u = v$ and we have proved (b).

3. Statements of Theorems A, B and C

Let σ be in $\text{End}_R M$. For χ_σ, p_σ and q_σ in $R[t]$, where p_σ and q_σ are arbitrary chosen in K_0 and K_1 , respectively, we define three subsets of R as

S_{χ_σ} = the set of roots of χ_σ ,

S_{p_σ} = the set of roots of p_σ

and

S_{q_σ} = the set of roots of q_σ .

In Theorem A, we shall show that if R is an integral domain and σ is diagonalizable, then S_{χ_σ} and S_{p_σ} coincide with each other, hence the difference between them is only the multiplicity of the roots.

Theorem A. *Let R be an integral domain and the matrix of $\sigma \in \text{End}_R M$ be diagonalizable. Then, we have the following:*

(a) *there is a unique monic minimal polynomial p_σ ,*

(b) p_σ divides χ_σ ,

(c) $S_{\chi_\sigma} = S_{p_\sigma}$, *that is, the difference between roots of χ_σ and p_σ is only the multiplicity of each root, and*

(d) if χ_σ has n distinct roots in R , we have $\chi_\sigma = p_\sigma$.

Theorems B and C show that if R is not an integral domain, then Theorem A is not necessarily valid.

Theorem B. *There is a finite commutative ring R , a module M over R , and an endomorphism σ in $\text{End}_R M$ of which matrix is diagonal and for which we have*

(a) $\chi_\sigma = q_\sigma$ with $\deg \chi_\sigma = 2$ is unique for σ and has no multiple roots, and is decomposed in two ways into a product of linear factors.

(b) p_σ with $\deg p_\sigma = 1$ is unique for σ , but not monic, and has no multiple roots.

(c) $S_{\chi_\sigma} \subseteq S_{p_\sigma}$ with $|S_{\chi_\sigma}| = 4$ and $|S_{p_\sigma}| = 8$.

(d) p_σ does not divide χ_σ .

Theorem C. *There is a finite commutative ring R , a module M over R , and σ in $\text{End}_R M$ of which matrix is diagonal and for which we have*

(a) p_σ is unique for σ but not monic, whereas q_σ is not unique for σ .

(b) $\deg p_\sigma = 2 < \deg q_\sigma = 3 < \deg \chi_\sigma = 4 = \text{rank } M < |R| = 6$.

(c) χ_σ has two 2-ple roots and four simple roots, whereas p_σ and q_σ have all simple roots, and

$$S_{\chi_\sigma} = S_{p_\sigma} = S_{q_\sigma} = R,$$

that is, for any a in R , $t - a$ divides each of χ_σ , p_σ and q_σ .

4. Proof for Theorems A, B and C

4.1. Proof for Theorem A

Since σ is diagonalizable, we have a matrix A in $M_n(R)$ such that

$$\sigma \underset{X}{\simeq} A = \text{diag}(a_1, a_2, \dots, a_n),$$

for some basis $X = \{x_1, x_2, \dots, x_n\}$ for M . Therefore, by the definition of

characteristic polynomial of σ , we have

$$\begin{aligned}\chi_\sigma(t) &= |tI - A| \\ &= (t - a_1)(t - a_2) \cdots (t - a_n)\end{aligned}\tag{1}$$

with a_1, a_2, \dots, a_n in R .

First, we prove (a) and (b) of the theorem. Let K be the quotient field of R , $M' = K \otimes_R M$ be the coefficient extension of M , and σ' be the prolongation of σ on M' .

Define the canonical ring homomorphism

$$\phi : K[t] \rightarrow \text{End}_K(M')$$

by $\phi(f(t)) = f(\sigma')$ for $f(t)$ in $K[t]$. Then, $\ker \phi$ is an ideal of $K[t]$. Since $K[t]$ is a PID, $\ker \phi$ is generated by an element $f(t)$ in $K(t)$, that is, we have

$$\ker \phi = (f(t)) \text{ for some } f(t) \text{ in } K[t],\tag{2}$$

where we may assume that $f(t)$ is monic, since K is a field. Consequently, $f(t)$ is unique for σ . On the other hand, since $\chi_\sigma(\sigma) = 0$ by Lemma 2.1, $\chi_\sigma(t)$ belongs to $R[t] \cap \ker \phi$. Hence, by (2), we have

$$\chi_\sigma(t) = f(t)g(t) \text{ for some } g(t) \in K[t].\tag{3}$$

Therefore, (1) yields that

$$f(t)g(t) = (t - a_1)(t - a_2) \cdots (t - a_n),\tag{4}$$

for some a_1, a_2, \dots, a_m in R .

Decomposing f and g as products of prime elements in $K[t]$, respectively, say, $f = f_1 f_2 \cdots f_r$ and $g = g_1 g_2 \cdots g_s$, (4) implies that

$$f_1 f_2 \cdots f_r \cdot g_1 g_2 \cdots g_s = (t - a_1)(t - a_2) \cdots (t - a_n).$$

Since $K[t]$ is UFD, comparing the both sides of the above equation, we find a subset $\{a_{i_1}, a_{i_2}, \dots, a_{i_r}\}$ of $\{a_1, a_2, \dots, a_n\}$ in R , and a subset $\{c_1, c_2, \dots, c_r\}$ in

$K - \{0\}$ such that

$$f_j = c_j(t - a_{i_j}), \quad c_j \in K, \quad a_{i_j} \in R$$

for $j = 1, 2, \dots, r$, which yields that

$$f(t) = c_1 c_2 \cdots c_r (t - a_{i_1})(t - a_{i_2}) \cdots (t - a_{i_r}), \quad a_{i_j} \in R$$

for $j = 1, 2, \dots, r$. However, since $f(t)$ is monic, we obtain $c_1 c_2 \cdots c_r = 1$ and thus

$$f(t) = (t - a_{i_1})(t - a_{i_2}) \cdots (t - a_{i_r}), \quad a_{i_j} \in R \quad (5)$$

for $j = 1, 2, \dots, r$, which guarantees that $f(t)$ is contained in $R[t]$. Thus, we may choose $f(t)$ as $p_\sigma(t)$ by Lemma 2.2 and $\chi_\sigma(t) = p_\sigma(t)g(t)$. Consequently, p_σ is monic, divides χ_σ and any zero of $p_\sigma(t)$ is that of $\chi_\sigma(t)$, which proves (a) and (b) of the theorem. By (b) any root of $p_\sigma(t)$ is that of $\chi_\sigma(t)$. To show (c) we have to prove the converse of this fact.

Clearly, X the basis for M over R is also that of M' over K . Further, since σ' is the prolongation of σ to M' we understand that $\sigma' = \sigma$ on X . Hence, for any $i = 1, 2, \dots, n$,

$$\begin{aligned} 0 &= p_\sigma(t)x_i \\ &= f(t)x_i \\ &= (\sigma - a_{i_1})(\sigma - a_{i_2}) \cdots (\sigma - a_{i_r})x_i \\ &= (a_i - a_{i_1})(a_i - a_{i_2}) \cdots (a_i - a_{i_r})x_i, \end{aligned}$$

which implies that for any i in $\{1, 2, \dots, n\}$, we have $a_i = a_{i_j}$, for some j in $\{1, 2, \dots, r\}$, since R is an integral domain and X is a basis for M' over K . Thus, we have shown the converse, namely, a zero of χ_σ is that of p_σ . Consequently, two sets of zeros of χ_σ and p_σ , respectively, coincides with each other. This shows that the difference between the roots of χ_σ and p_σ is only the multiplicity, which is (c). (d) is clear by (c).

4.2. Proof for Theorem B

Let $R = \mathbb{Z}_{16} = \{\bar{0}, \bar{1}, \dots, \bar{15}\}$ with $\bar{a} = a + 16\mathbb{Z}$ for $a = 0, 1, \dots, 15$, $M = Rx_1 \oplus Rx_2$ with a basis $X = \{x_1, x_2\}$ over R , and

$$\sigma \underset{X}{\cong} A = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{4} \end{pmatrix}.$$

To show (a), first, we will treat to factorize χ_σ and get its roots. By the definition of the characteristic polynomial, we have the unique monic polynomial $\chi_\sigma(t) = (t - \bar{2})(t - \bar{4})$. Substituting each element in \mathbb{Z}_{16} for t in $\chi_\sigma(t)$, we have $S_{\chi_\sigma} = \{\bar{2}, \bar{4}, \bar{10}, \bar{12}\}$. Therefore, we have exactly two factorizations

$$\chi_\sigma(t) = (t - \bar{2})(t - \bar{4}) = (t - \bar{10})(t - \bar{12}),$$

which also shows that $\chi_\sigma(t)$ has no multiple roots. The rest of (a), $\chi_\sigma(t) = q_\sigma(t)$ will be treated later. Next, we deal with $p_\sigma(t)$ and $q_\sigma(t)$. It is obvious to see that $\bar{8}t$ is in $\ker \pi$, since $\bar{8}\sigma = 0$. Our claim is that this is the unique minimal polynomial. Suppose that $f(t) = \bar{a}t + \bar{b} \neq 0$ belongs to $\ker \pi$ for \bar{a}, \bar{b} in \mathbb{Z}_{16} . Then we have

$$0 = f(\sigma)x_1 = (\bar{2}\bar{a} + \bar{b})x_1$$

and

$$0 = f(\sigma)x_2 = (\bar{4}\bar{a} + \bar{b})x_2,$$

which implies that $\bar{a} = \bar{8}$ and $\bar{b} = \bar{0}$, hence $f(t) = \bar{8}t$. Thus we have shown that $p_\sigma(t) = \bar{8}t$ is the unique minimal polynomial of σ .

Further, this shows that there are no monic polynomial of degree one in $\ker \pi$, and so we have

$$\chi_\sigma = q_\sigma.$$

Moreover, $p_\sigma(t) = \bar{8}t$ gives us $S_{p_\sigma} = \{\bar{0}, \bar{2}, \dots, \bar{14}\}$, i.e., $\bar{2}\mathbb{Z}_{16}$. The rest of the proof is straightforward and we have completed the proof of the theorem.

4.3. Proof for Theorem C

We claim that $R = \mathbb{Z}_6 = \{\bar{0}, \bar{1}, \dots, \bar{5}\}$, $M = Rx_1 \oplus Rx_2 \oplus Rx_3 \oplus Rx_4$ with $X = \{x_1, x_2, x_3, x_4\}$ a basis for M over R , and

$$\sigma \underset{X}{\simeq} A = \text{diag}(\bar{1}, \bar{2}, \bar{3}, \bar{4})$$

satisfies all necessary conditions of the theorem. Recall that we have the canonical ring homomorphism

$$\pi : R[t] \rightarrow \text{End}_R M$$

defined by $\pi(f(t)) = f(\sigma)$ for $f(t) \in R[t]$ and $\sigma \in \text{End}_R M$. Also, we have

$$(1) \chi_\sigma(t) = (t - \bar{1})(t - \bar{2})(t - \bar{3})(t - \bar{4}).$$

First, we show that for $f(t) = (t - \bar{1})(t - \bar{2})(t - \bar{3})$ and $g(t) = \bar{3}t(t - \bar{1})$, we have

$$(2) f, g \text{ are contained in } \ker \pi, \text{ i.e.,}$$

$$f(A) = g(A) = 0.$$

Indeed, for the identity matrix $I = \text{diag}(\bar{1}, \bar{1}, \bar{1}, \bar{1})$,

$$\begin{aligned} f(A) &= (A - \bar{1} \cdot I)(A - \bar{2} \cdot I)(A - \bar{3} \cdot I) \\ &= \text{diag}(\bar{0}, \bar{1}, \bar{2}, \bar{3}) \cdot \text{diag}(-\bar{1}, \bar{0}, \bar{1}, \bar{2}) \cdot \text{diag}(-\bar{2}, -\bar{1}, \bar{0}, \bar{1}) \\ &= \bar{0} \cdot I \end{aligned}$$

and

$$g(A) = \bar{3} \text{diag}(\bar{1}, \bar{2}, \bar{3}, \bar{4}) \cdot \text{diag}(\bar{0}, \bar{1}, \bar{2}, \bar{3}) = \bar{0} \cdot I,$$

which verify (2). Further,

$$(3) \text{ for } 0 \neq h(t) \in \ker \pi, \text{ we have } \deg h > 1.$$

To show this, let $0 \neq h(t) = \bar{a}t + \bar{b} \in \ker \pi$ for $\bar{a}, \bar{b} \in R$. Then,

$$0 = \bar{a}A + \bar{b}I = \text{diag}(\bar{a} + \bar{b}, 2\bar{a} + \bar{b}, 3\bar{a} + \bar{b}, 4\bar{a} + \bar{b}),$$

which implies that $\bar{a} = \bar{b} = \bar{0}$, a contradiction. Thus, $\deg h > 1$ and we have (3).

By (2) and (3), we find that $g(t) = \bar{3}t(t - \bar{1})$ is a polynomial of the lowest degree in $\ker \pi$. Therefore, we may write $p_\sigma(t) = \bar{3}t(t - 1)$. Our next purpose is to show the uniqueness of $p_\sigma(t)$ for σ . Namely, we prove that

(4) if $0 \neq k(t) = \bar{a}t^2 + \bar{b}t + \bar{c}$ belongs to $\ker \pi$, then we have $\bar{a} = \bar{b} = \bar{3}$ and $\bar{c} = 0$.

Since $k(t)$ is in $\ker \pi$, $0 = k(A) = \bar{a}A^2 + \bar{b}A + \bar{c} \cdot I$. Substituting $A = \text{diag}(\bar{1}, \bar{2}, \bar{3}, \bar{4})$ and $A^2 = \text{diag}(\bar{1}, 4, \bar{3}, \bar{4})$ in the above equation, we get

$$0 = \bar{a} \cdot \text{diag}(\bar{1}, 4, \bar{3}, \bar{4}) + \bar{b} \cdot \text{diag}(\bar{1}, \bar{2}, \bar{3}, \bar{4}) + \bar{c}(\bar{1}, \bar{1}, \bar{1}, \bar{1}),$$

which implies that $\bar{a} = \bar{b} = \bar{3}$ and $\bar{c} = \bar{0}$ as was to be shown. Thus we have proved that $p_\sigma(t) = \bar{3}t(t + \bar{1})$ is unique for σ . Also, (4) shows that $\ker \pi$ does not contain a monic polynomial of degree two. This together with $f(A) = 0$ for $f(t) = (t - \bar{1})(t - \bar{2})(t - \bar{3})$ allows us to write $q_\sigma(t) = (t - 1)(t - 2)(t - 3)$. However, since $p_\sigma + q_\sigma$ is in $\ker \pi$, $q_\sigma(t) = (t - 1)(t - 2)(t - 3)$ is not unique for σ . Thus, we have proved

(5) p_σ is unique for σ , but not q_σ .

Since $\deg p_\sigma = 2$, $\deg q_\sigma = 3$, $\deg \chi_\sigma = \text{rank } M = 4$ and $|R| = 6$, we have proved that

(6) $\deg q_\sigma < \deg p_\sigma < \deg \chi_\sigma = \text{rank } M < |R|$.

By (5) and (6), we have proved (a) and (b) of the theorem. Now, we show (c) and (d).

Since we have another factorization $\chi_\sigma(t) = t(t - \bar{1})^2(t - \bar{2}) = (t - \bar{3})(t - \bar{4})^2 \cdot (t - \bar{5})$, $\bar{1}$ and $\bar{4}$ are multiple roots. On the other hand, $(t - \bar{1})^2(t - \bar{2})$ does not have $\bar{0}$ as zero, and $t(t - 1)^2$ not $\bar{2}$. Therefore, $\bar{0}$ and $\bar{2}$ are simple roots of $\chi_\sigma(t)$. Similarly, substituting $\bar{3}$ and $\bar{5}$ for t in $(t - \bar{4})^2(t - \bar{5})$ and $(t - \bar{3})^2(t - \bar{4})^2$, respectively, we have no zeros and also find that both $\bar{3}$ and $\bar{5}$ are simple roots of $\chi_\sigma(t)$. Thus, we have proved

(7) $\chi_\sigma(t)$ has two 2-ple roots and four simple roots.

Finally, substituting any element α in R for t in each of χ_σ , q_σ and p_σ , respectively, we get zero. Further, we see that p_σ and q_σ have no multiple roots. So, we have

(8) χ_σ , p_σ , q_σ have the same root set R , and p_σ and q_σ have only simple roots, and

(9) for any α in R , $t - \alpha$ divides each of χ_σ , p_σ and q_σ ,

which gives us (c) and (d) of the theorem. Thus we have completed the proof for Theorem (C).

Proposition. *Let R be a ring and E be a left module over R . Then, the following (a) and (b) hold:*

(a) *If two elements a, b in R satisfy*

(i) $abE = baE = 0$ and (ii) $aR + bR = R$,

then we have

$$(1) E = E_a + E_b$$

for $E_a = \{x \in E \mid ax = 0\}$ and $E_b = \{y \in E \mid by = 0\}$.

(b) *Further, if an additional condition*

(iii) a, b *are central elements of R*

is satisfied, then we have

$$(2) E = E_a \oplus E_b.$$

References

- [1] D. Augot and P. Camion, On the computation of minimal polynomials, cyclic vectors, and Frobenius forms, *Linear Algebra Appl.* 260(15) (1997), 615-694.
- [2] D. R. Estes and R. M. Guralnick, Minimal polynomials of integral symmetric matrices, *Linear Algebra Appl.* 192 (1993), 88-99.

- [3] M. Fiedler, Expressing a polynomial as the characteristics polynomial of a symmetric matrix, *Linear Algebra Appl.* 141 (1990), 265-270.
- [4] S. Lang, *Algebra*, 3rd ed., Addison-Wesley, Tokyo, 1993.
- [5] G. Schmeisser, A real symmetric tridiagonal matrix with a given characteristic polynomial, *Linear Algebra Appl.* 93(1) (1993), 11-18.