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 $R$, $\sigma$ is an element in $\text{End}_R M$, and the matrix of $\sigma$ diagonalizable. Our purpose is to investigate the relationship between the characteristic polynomial $\chi_{\sigma}$ of $\sigma$ and the minimal polynomial $p_{\sigma}$ of $\sigma$. If $R$ is an integral domain, then we shall show that $p_{\sigma}$ is uniquely determined as a monic polynomial dividing $\chi_{\sigma}$. Also, the difference between the two sets of zeros of $p_{\sigma}$ and $\chi_{\sigma}$, respectively, is only the multiplicity of their roots. If $R$ is not an integral domain, then we shall construct $\sigma$ such that $p_{\sigma}$ is not necessarily monic nor divides $\chi_{\sigma}$.

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 $\sigma$ 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 \( \sigma \) and \( p_\sigma(t) \in F[t] \) the minimal polynomial of \( \sigma \). 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 \( \chi_\sigma \) and \( p_\sigma \), 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 \( \sigma \) is diagonalizable. Above observation about linear endomorphism \( \sigma \) 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 \( \sigma \) in \( \text{End}_F V \) to \( \sigma \) 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. Schneisser [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 \( X = \{x_1, x_2, ..., x_n\} \) a basis for \( M \), and \( \text{End}_R M \) is the endomorphism ring of \( M \) over \( R \). For an element \( \sigma \) in \( \text{End}_R M \), we write

\[
\sigma = A \quad \text{on} \quad X
\]

if \( A \) in \( M_n(R) \) is the matrix of \( \sigma \) relative to \( X \), where \( M_n(R) \) denotes the ring of matrices of \( n \times n \) over \( R \). We define the characteristic polynomial \( \chi_\sigma(t) \), \( \chi_\sigma \) or \( \chi(t) \) of \( A \) (or \( \sigma \)) 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 \( \sigma \). An element \( a \) in \( R \) is called an eigenvalue or a characteristic root of \( \sigma \) in \( R \) if it is a root of \( \chi_\sigma \), i.e., \( \chi_\sigma(a) = 0 \). For \( \sigma \) in \( \text{End}_RM \), we have a canonical ring homomorphism

\[
\pi : R[t] \to \text{End}_RM
\]

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:

\[
K_0 = \text{The set of non-zero polynomials in } \ker \pi \text{ of which degree is the lowest in } \ker \pi.
\]

\[
K_1 = \text{The set of non-zero polynomials in } P \cap \ker \pi \text{ of which degree is the lowest in } P \cap \ker \pi.
\]

Clearly, \( K_0 \neq \emptyset \) and \( K_1 \neq \emptyset \), for \( \ker \pi \) contains a monic polynomial \( \chi_\sigma \). We call any polynomial in \( K_0 \) a minimal polynomial of \( \sigma \) and denote it by \( p_\sigma(t) \), also any one in \( K_1 \) a small polynomial of \( \sigma \) 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, \( p_\sigma \) and \( q_\sigma \) are not necessarily unique for \( \sigma \). Indeed, if \( p_\sigma \) is a minimal polynomial, so is \( cp_\sigma \) for any \( c \) in \( R \) with \( cp_\sigma \neq 0 \). Also, if \( q_\sigma \) 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 \( \sigma \), and we have

\[
\deg p_\sigma \leq \deg q_\sigma.
\]
Lemma 2.2. (a) The following conditions (a\(_1\)) and (a\(_2\)) are equivalent:

(a\(_1\)) \(\deg p_\sigma = \deg q_\sigma\) for any (or some) \(p_\sigma \in K_0\) and any (or some) \(q_\sigma \in K_1\) and

(a\(_2\)) there is a monic minimal polynomial \(p_\sigma\).

(b) In case of (a), \(p_\sigma\) is a unique for \(\sigma\).

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 \(\sigma\) be in \(\text{End}_R M\). For \(\chi_\sigma, p_\sigma\) and \(q_\sigma\) in \(R[t]\), where \(p_\sigma\) and \(q_\sigma\) are arbitrary chosen in \(K_0\) and \(K_1\), respectively, we define three subsets of \(R\) as

\[
S_{\chi_\sigma} = \text{the set of roots of } \chi_\sigma,
\]
\[
S_{p_\sigma} = \text{the set of roots of } p_\sigma
\]
and

\[
S_{q_\sigma} = \text{the set of roots of } q_\sigma.
\]

In Theorem A, we shall show that if \(R\) is an integral domain and \(\sigma\) is diagonalizable, then \(S_{\chi_\sigma}\) and \(S_{p_\sigma}\) 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 \(p_\sigma\),

(b) \(p_\sigma\) divides \(\chi_\sigma\),

(c) \(S_{\chi_\sigma} = S_{p_\sigma}\), that is, the difference between roots of \(\chi_\sigma\) and \(p_\sigma\) is only the multiplicity of each root, and
(d) if $\chi_\sigma$ 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 $\sigma$ 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 $\sigma$ and has no multiple roots, and is decomposed in two ways into a product of linear factors.

(b) $p_\sigma$ with $\deg p_\sigma = 1$ is unique for $\sigma$, 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) $p_\sigma$ does not divide $\chi_\sigma$.

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

(a) $p_\sigma$ is unique for $\sigma$ but not monic, whereas $q_\sigma$ is not unique for $\sigma$.

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

(c) $\chi_\sigma$ has two 2-pf roots and four simple roots, whereas $p_\sigma$ and $q_\sigma$ 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 $\chi_\sigma$, $p_\sigma$ and $q_\sigma$.

### 4. Proof for Theorems A, B and C

#### 4.1. Proof for Theorem A

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

$$\sigma \equiv A = \text{diag}(a_1, a_2, \ldots, a_n),$$

for some basis $X = \{x_1, x_2, \ldots, x_n\}$ for $M$. Therefore, by the definition of
characteristic polynomial of $\sigma$, we have
\[
\chi_\sigma(t) = |I - A| = (t - a_1)(t - a_2)\cdots(t - a_n) \tag{1}
\]
with $a_1, a_2, \ldots, a_n$ 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 $\sigma'$ be the prolongation of $\sigma$ on $M'$.

Define the canonical ring homomorphism
\[
\varphi : K[t] \to \text{End}_K(M')
\]
by $\varphi(f(t)) = f(\sigma')$ for $f(t)$ in $K[t]$. Then, $\ker \varphi$ is an ideal of $K[t]$. Since $K[t]$ is a PID, $\ker \varphi$ is generated by an element $f(t)$ in $K(t)$, that is, we have
\[
\ker \varphi = (f(t)) \text{ for some } f(t) \text{ in } K[t], \tag{2}
\]
where we may assume that $f(t)$ is monic, since $K$ is a field. Consequently, $f(t)$ is unique for $\sigma$. On the other hand, since $\chi_\sigma(\sigma) = 0$ by Lemma 2.1, $\chi_\sigma(t)$ belongs to $R[t] \cap \ker \varphi$. 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 $a_1, a_2, \ldots, a_n$ in $R$.

Decomposing $f$ and $g$ as products of prime elements in $K[t]$, respectively, say, $f = f_1f_2\cdots f_r$ and $g = g_1g_2\cdots g_s$, (4) implies that
\[
f_1f_2\cdots f_r \cdot g_1g_2\cdots g_s = (t - a_1)(t - a_2)\cdots(t - a_n).
\]

Since $K[t]$ is UFD, comparing the both sides of the above equation, we find a subset $\{a_{i_1}, a_{i_2}, \ldots, a_{i_r}\}$ of $\{a_1, a_2, \ldots, a_n\}$ in $R$, and a subset $\{c_1, c_2, \ldots, c_r\}$ in
$K - \{0\}$ such that

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

for $j = 1, 2, ..., r$, which yields that

$$f(t) = c_1c_2 \cdots c_r(t - a_{i_1})(t - a_{i_2})\cdots(t - a_{i_r}), \quad a_{ij} \in R$$

for $j = 1, 2, ..., r$. However, since $f(t)$ is monic, we obtain $c_1c_2 \cdots c_r = 1$ and thus

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

for $j = 1, 2, ..., r$, 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, $p_\sigma$ is monic, divides $\chi_\sigma$ 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 $\sigma'$ is the prolongation of $\sigma$ to $M'$ we understand that $\sigma' = \sigma$ on $X$. Hence, for any $i = 1, 2, ..., n$,

$$0 = p_\sigma(t)x_i$$

$$= f(t)x_i$$

$$= (\sigma - a_{i_1})(\sigma - a_{i_2})\cdots(\sigma - a_{i_r})x_i$$

$$= (a_{i} - a_{i_1})(a_{i} - a_{i_2})\cdots(a_{i} - a_{i_r})x_i,$$

which implies that for any $i$ in $\{1, 2, ..., n\}$, we have $a_i = a_{ij}$, for some $j$ in $\{1, 2, ..., r\}$, 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 $\chi_\sigma$ is that of $p_\sigma$. Consequently, two sets of zeros of $\chi_\sigma$ and $p_\sigma$, respectively, coincides with each other. This shows that the difference between the roots of $\chi_\sigma$ and $p_\sigma$ is only the multiplicity, which is (c). (d) is clear by (c).
4.2. Proof for Theorem B

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

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

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

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

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 $\overline{8}t$ is in $\ker \pi$, since $\overline{8}\sigma = 0$. Our claim is that this is the unique minimal polynomial. Suppose that $f(t) = \overline{a}t + \overline{b} \neq 0$ belongs to $\ker \pi$ for $\overline{a}, \overline{b}$ in $\mathbb{Z}_{16}$. Then we have

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

and

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

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

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

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

Moreover, $p_\sigma(t) = \overline{8}t$ gives us $S_{p_\sigma} = \{\overline{0}, \overline{2}, ..., \overline{14}\}$, i.e., $\overline{2}\mathbb{Z}_{16}$. 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 \( R = \mathbb{Z}_6 = \{ \overline{0}, \overline{1}, ..., \overline{5} \} \), \( M = Rx_1 \oplus Rx_2 \oplus Rx_3 \oplus Rx_4 \) with \( X = \{ x_1, x_2, x_3, x_4 \} \) a basis for \( M \) over \( R \), and
\[
\sigma \overset{\sim}{=} A = \text{diag}(\overline{1}, \overline{2}, \overline{3}, \overline{4})
\]
satisfies all necessary conditions of the theorem. Recall that we have the canonical ring homomorphism
\[
\pi : R[t] \to \text{End}_R M
\]
defined by \( \pi(f(t)) = f(\sigma) \) for \( f(t) \in R[t] \) and \( \sigma \in \text{End}_R M \). Also, we have
\[
(1) \quad \chi(h) = (t - \overline{1})(t - \overline{2})(t - \overline{3})(t - \overline{4}).
\]
First, we show that for \( f(t) = (t - \overline{1})(t - \overline{2})(t - \overline{3}) \) and \( g(t) = \overline{3}t(t - \overline{1}) \), we have
\[
(2) \quad f, g \text{ are contained in } \ker \pi, \text{ i.e.,}
\]
\[
f(A) = g(A) = 0.
\]
Indeed, for the identity matrix \( I = \text{diag}(\overline{1}, \overline{1}, \overline{1}, \overline{1}) \),
\[
f(A) = (A - \overline{1} \cdot I)(A - \overline{2} \cdot I)(A - \overline{3} \cdot I)
\]
\[
= \text{diag}(\overline{0}, \overline{1}, \overline{2}, \overline{3}) \cdot \text{diag}(\overline{1}, \overline{2}, \overline{3}) \cdot \text{diag}(\overline{2}, \overline{3}, \overline{4}) \cdot \text{diag}(\overline{0}, \overline{1}, \overline{2})
\]
\[
= \overline{0} \cdot I
\]
and
\[
g(A) = \overline{3} \text{diag}(\overline{1}, \overline{2}, \overline{3}, \overline{4}) \cdot \text{diag}(\overline{0}, \overline{1}, \overline{2}, \overline{3}) = \overline{0} \cdot I,
\]
which verify (2). Further,
\[
(3) \text{ for } 0 \neq h(t) \in \ker \pi, \text{ we have } \deg h > 1.
\]
To show this, let \( 0 \neq h(t) = \overline{a}t + \overline{b} \in \ker \pi \) for \( \overline{a}, \overline{b} \in R \). Then,
\[
0 = \overline{a}A + \overline{b}I = \text{diag}(\overline{a} + \overline{b}, 2\overline{a} + \overline{b}, 3\overline{a} + \overline{b}, 4\overline{a} + \overline{b}),
\]
which implies that \( \overline{a} = \overline{b} = \overline{0} \), a contradiction. Thus, \( \deg h > 1 \) and we have (3).
By (2) and (3), we find that \( g(t) = \overline{3}(t - \overline{1}) \) is a polynomial of the lowest degree in \( \ker \pi \). Therefore, we may write \( p_\sigma(t) = \overline{3}(t - 1) \). Our next purpose is to show the uniqueness of \( p_\sigma(t) \) for \( \sigma \). Namely, we prove that

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

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

\[
0 = \overline{a} \cdot \text{diag}(\overline{1}, \overline{4}, \overline{3}, \overline{4}) + \overline{b} \cdot \text{diag}(\overline{1}, \overline{2}, \overline{3}, \overline{4}) + \overline{c} \cdot (\overline{1}, \overline{1}, \overline{1}, \overline{1}),
\]

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

\[
(5) \text{ } p_\sigma \text{ is unique for } \sigma, \text{ but not } q_\sigma.
\]

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 \( \chi_\sigma(t) = t(t - \overline{1})^2(t - \overline{2}) = (t - \overline{3})(t - \overline{4})^2 \cdot (t - \overline{5}) \), \( \overline{1} \) and \( \overline{4} \) are multiple roots. On the other hand, \( (t - \overline{1})^2(t - \overline{2}) \) does not have \( \overline{0} \) as zero, and \( t(t - 1)^2 \) not \( \overline{2} \). Therefore, \( \overline{0} \) and \( \overline{2} \) are simple roots of \( \chi_\sigma(t) \). Similarly, substituting \( \overline{3} \) and \( \overline{5} \) for \( t \) in \( (t - \overline{4})^2(t - \overline{5}) \) and \( (t - \overline{3})^2(t - \overline{4})^2 \), respectively, we have no zeros and also find that both \( \overline{3} \) and \( \overline{5} \) 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 $\alpha$ in $R$ for $t$ in each of $\chi_{\sigma}$, $q_{\sigma}$ and $p_{\sigma}$, respectively, we get zero. Further, we see that $p_{\sigma}$ and $q_{\sigma}$ have no multiple roots. So, we have

(8) $\chi_{\sigma}$, $p_{\sigma}$, $q_{\sigma}$ have the same root set $R$, and $p_{\sigma}$ and $q_{\sigma}$ have only simple roots, and

(9) for any $\alpha$ in $R$, $t - \alpha$ divides each of $\chi_{\sigma}$, $p_{\sigma}$ and $q_{\sigma}$,

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

(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


