On Primary Decomposition and Polynomial of a Matrix

S. Bouarga

Department of Mathematics
Faculty of Sciences and technology, FST Fez Saiss
Fez, Morocco

M. E. Charkani

Department of Mathematics
Faculty of Sciences, Dhar-Mahraz
P. 0. Box 1796, Atlas-Fez, Morocco

Copyright © 2014 S. Bouarga and M. E. Charkani. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

The goal of this paper is to study some unknown questions on the primary decomposition of matrices over a field $K$ and to give the analogous of some well known results of spectral, algebraic and geometric multiplicity order of an eigenvalue to any $P$-component of the characteristic polynomial $C_A$ of a matrix $A$ over a field $K$. More precisely we compute the dimension of the kernel of a polynomial of a square matrix $A$ over any arbitrary commutative field $K$ in terms of its invariant factors. As an application we determine the value of the $P$-algebraic and $P$-geometric multiplicity order of any $P$-component of the characteristic polynomial $C_A$ of a matrix $A$.

Keywords: Primary decomposition, invariant factors, algebraic multiplicity, geometric multiplicity
1 Introduction

Let $K$ be a field. Let $A \in \mathcal{M}_n(K)$ and $P$ be an irreducible polynomial of $K[X]$. We will say that $A$ is $P$-primary matrix if the characteristic polynomial $C_A$ of $A$ is a power of $P$. The Primary decomposition Theorem states that if $A \in \mathcal{M}_n(K)$ is a non zero matrix and $m_A(X) = \prod_{i=1}^{s} P_{\alpha_i}^{n_i}$ is the prime decomposition of its minimal polynomial $m_A(X)$ then the matrix $A$ is similar to a block diagonal of $P$-primary matrices $\text{diag}(A_1, A_2, \ldots, A_s)$. The dimension of sequence vector spaces $\text{Ker } P^s(A)$ is unknown.

In the first part of this paper, we use some deep results on module theory over a PID to compute the dimension of the kernel of a polynomial of a square matrix $A$ over a commutative field $K$ in terms of its invariant factors.

In the second part, we give the analogous of some well known results of spectral, algebraic and geometric multiplicity order of an eigenvalue, to any $P$-component of the characteristic polynomial $C_A$ of a matrix $A$ over any arbitrary commutative field $K$. Some new results on the $P$-algebraic and $P$-geometric multiplicity order are also established.

2 Preliminary Notes

Let $K$ be a field. Let $M$ be a finite dimension vector space over $K$ and $f$ a $K$-endomorphism of $M$. The vector space $M$ is endowed by a structure of $K[X]$-module via the endomorphism $f$ by $X.m = f(m)$ for any $m \in M$. We will denote by $M_f$ the $K[X]$-module on $M$ induced by $f$. As the ring $K[X]$ is a PID, then by applying the structure theorem of finitely generated torsion modules over a PID, the very useful following theorem is deduced (see [6], §2, p. 556), [8], §14, [1], p. 235] and [3]):

Theorem 2.1 (Rational canonical form) Let $M$ be a finite-dimensional vector space over a field $K$ and $f$ be a $K$-endomorphism of $M$. Let $M_f$ be the $K[X]$-module induced by $f$ then there exists a unique sequence of polynomials $q_1, \ldots, q_r$ such that:

$$M_f \simeq \frac{K[X]}{(q_1)} \oplus \frac{K[X]}{(q_2)} \oplus \cdots \oplus \frac{K[X]}{(q_r)}$$

and

- $q_i \mid q_{i+1}$
- $q_r = m_f(X)$ the minimal polynomial of $f$ and $\prod_{i=1}^{r} q_i = c_f(X)$ the characteristic polynomial of $f$.

The ascending sequence of polynomials $q_1, \ldots, q_r$ are unique and called the invariant factors of $f$. 

If \( q_1, \cdots, q_r \) are the invariant factors of \( f \) then we will write \( IF(f) = (q_1, \cdots, q_r) \).

Let \( A \in \mathcal{M}_n(K) \) be a non zero matrix, and for any linear transformation that has matrix \( A \) relative to some basis, we denote \( M_A \) the \( K[X] \)-module induced by \( A \). Then by theorem 2.1:

\[
M_A \cong \frac{K[X]}{(q_1)} \oplus \frac{K[X]}{(q_2)} \oplus \cdots \oplus \frac{K[X]}{(q_r)}
\]
such that \( q_i | q_{i+1}, q_r = m_A(X) \) the minimal polynomial of \( A \) and \( \prod_{i=1}^{r} q_i = c_A(X) \) the characteristic polynomial of \( A \). The sequence of polynomials \( q_1, \cdots, q_r \) are called the invariant factors of \( A \). The invariant factors of \( A \) are unique up similarity. Indeed if \( q_1, \cdots, q_r \) are the invariant factors of \( A \) then \( A \) is similar to a block diagonal matrix \( \text{diag}(A_1, A_2, ..., A_m) \) where \( A_i = \text{Comp}(q_i) \) is the companion matrix of \( q_i \).

Let \( K \) be a field. Let \( A \in \mathcal{M}_n(K) \) and \( P \) be an irreducible polynomial of \( K[X] \). We will say that \( A \) is \( P \)-primary matrix if the characteristic polynomial \( C_A \) of \( A \) is a power of \( P \).

**Proposition 2.2 (Primary decomposition Theorem)** Let \( A \in \mathcal{M}_n(K) \) be a non zero matrix. Let \( m_A(X) = \prod_{i=1}^{s} P_i^{a_i} \) be the prime decomposition of \( m_A(X) \). Let \( E_i = \text{Ker} P_i^{a_i}(A) \). Then the subspaces \( E_i \) are invariant under \( A \) and \( A \) is similar to a block diagonal of \( P \)-primary matrices \( \text{diag}(A_1, A_2, ..., A_s) \).

**Proof.** See [[7], Theorem 1.5.1,p29].

Throughout this paper, \( E \) is a finite-dimensional vector space over a field \( K \). If \( f \in \text{End}_K(E) \), \( m_f \) and \( C_f \) stand respectively for the minimal and the characteristic polynomial of \( f \).

## 3 Main Results

This is the main result of this paper.

**Theorem 3.1** Let \( K \) be a field. Let \( A \in \mathcal{M}_n(K) \) be a non zero matrix and \( IF(A) = (q_1, \cdots, q_r) \) its invariant factors. Then

\[
\dim_K \text{Ker} P(A) = \sum_{i=1}^{r} \deg (\gcd(P, q_i))
\]

for any \( P \in K[X] \). In particular \( \dim_K \text{Ker} A \) is the number of \( i \) such that \( q_i(0) = 0 \).
To prove this Theorem we need the following lemmas

**Lemma 3.2** Let \( u \) be an endomorphism of a finite dimensional vector space \( E \) over \( K \). Assume that \( E = \bigoplus_{i=1}^{n} E_i \) such that \( E_i \) are \( u \)-invariant subspaces of \( E \). Then \( u = \bigoplus_{i=1}^{n} u_i \) with \( u_i = \text{res}_{E_i} u \) the restriction of \( u \) to \( E_i \) and

1. \( u(x) = \sum_{i=1}^{n} u_i(x_i) \) for all \( x = \sum_{i=1}^{n} x_i \).
2. \( P(u) = \bigoplus_{i=1}^{n} P(u_i) \) for all \( P \in K[X] \)
3. \( \text{Ker}P(u) = \bigoplus_{i=1}^{n} \text{Ker}P(u_i) \)

**Proof.** Easy to prove (see [8], Proposition 1.3.2 and [5]).

**Lemma 3.3** Let \( R \) be a PID and let \( a, b \) be nonzero elements of \( R \). If \( d = (a,b) = \gcd\{a,b\} \), then

\[
\{\overline{c} \in R/bR \mid a\overline{c} = \overline{0}\} \simeq R/dR.
\]

**Proof.** Indeed let \( M_a := \{\overline{c} \in R/bR \mid a\overline{c} = \overline{0}\} \) clearly \( M_a \) is a submodule of the \( R \)-module \( R/bR \). Let \( b' = \frac{b}{d} \). Then

\[
\phi : R \longrightarrow M_a \\
x \longmapsto \overline{b'x}
\]

\( \phi \) is an \( R \)-homomorphism. Notice that \( a\overline{b'x} = \overline{\frac{b}{d} dx} = \overline{0} \). So \( \overline{b'x} \in M_a \).

Furthermore if \( \overline{ax} = \overline{0} \) then \( ax \in bR \) so \( x \in b'R \). Hence \( \phi \) is an onto homomorphism. \( \text{Ker} \phi = \{x \in R \mid b'x \in bR\} = dR \). Hence \( M_a \simeq R/dR \).

**Lemma 3.4** Let \( A \in \mathcal{M}_n(K) \) and let \( M_A \) be the \( K[X] \)-module induced by \( A \). If \( M_A \simeq K[X]/(q) \). Let \( P \in K[X] \), then

\[
\text{Ker}(P(A)) \simeq \text{Ker}(\widetilde{P}(X))
\]

where \( \widetilde{P}(X) : K[X]/(q) \rightarrow K[X]/(q), \overline{T} \mapsto P(X)\overline{T} \)

**Proof.** Let \( \varphi \) denotes the \( K[X] \)-isomorphism between \( M_A \) and \( K[X]/(q) \)
We have \( m \in \text{Ker} P(A) \) if and only if \( P(A)(m) = 0 \) if and only if \( \varphi(P(X).m) = 0 \) if and only if \( \varphi(P(X).\varphi(m)) = 0 \) if and only if \( P(X)(\varphi(m)) = 0 \) if and only if \( \varphi(m) \in \text{Ker} P(X) \), where \( \widetilde{P}(X) : K[X]/(q) \rightarrow K[X]/(q), \overline{T} \mapsto P(X)\overline{T} \) hence \( \text{Ker}(P(A)) \simeq \text{Ker}(P(X)) \).
Lemma 3.5 Let $A \in \mathcal{M}_n(K)$ and let $M_A$ be the $K[X]$-module induced by $A$. If $M_A \simeq K[X]/(q)$ then for all $P \in K[X]$

$$\text{Ker}(P(A)) \simeq \begin{cases} (0) & \text{if } \gcd(P, q) = 1 \\ K[X]/(D) & \text{if } \gcd(P, q) = D \end{cases}$$

Proof. By lemma 3.4 and lemma 3.3 we have $\text{Ker}P(X) \simeq K[X]/(D)$ where $D = \gcd(P, q)$.

Now let’s give the proof of the theorem 3.1

Proof. Let $E$ be a $K$-vector space of finite dimension. Let $f \in \text{End}_K(E)$ and $B$ a basis of $E$ such that $\text{mat}_B(f) = A$. The space $E$ can be viewed as a $K[X]$-module $(K[X] \times E \rightarrow E,(P,x) \mapsto P.x = P(f)(x))$. Then $E = M_f \simeq \bigoplus_{i=1}^r K[X]/(q_i)$ as $K[X]$-modules, where $q_1, q_2, \ldots, q_r$ are the invariant factors of $A$. Hence $E \simeq \bigoplus_{i=1}^r E_i$ where $E_i$’s are $f$-invariant subspaces and $E_i \simeq K[X]/(q_i)$ as $K[X]$-modules. Hence by lemma 3.2 $f = \bigoplus_{i=1}^r f_i$ and $P(f) = \bigoplus_{i=1}^r P(f_i)$ where $f_i = \text{res}_{E_i} f$. So it turns to study the case where $f$ admits one invariant factor ($A$ is companion). By lemma 3.5 $\text{Ker}P(f_i) \simeq K[X]/(D_i)$ where $\gcd(P, q_i) = D_i$. We have by lemma 3.2 $\text{Ker}P(f) = \bigoplus_{i=1}^r \text{Ker}P(f_i) \simeq \bigoplus_{i=1}^r K[X]/(D_i)$. Hence $\dim_K \text{Ker}P(f) = \sum_{i=1}^r \dim_K(K[X]/(D_i)) = \sum_{i=1}^r \deg(D_i) = \sum_{i=1}^r \deg(gcd(P, q_i))$.

4 Generalized algebraic and geometric multiplicity order

Let $K$ be a field. Let $Q$ be a polynomial of $K[X]$ and $P$ be an irreducible polynomial of $K[X]$ which occur in the prime decomposition of $Q$. We will say that the power polynomial $P^s$ is the $P$-component of $Q$ if $Q = P^sQ_1$ where $Q_1$ is a polynomial of $K[X]$ coprime with $P$. The integer $s$ is said the $P$-valuation of $Q$ and will be denoted by $\nu_P(Q)$.

In order to give the analogous of some well known results of spectral, algebraic and geometric multiplicity order of an eigenvalue. We introduce the $P$-algebraic and $P$-geometric multiplicity order relative to any $P$-component of the characteristic polynomial $C_A$ of the matrix $A$.

Definition 4.1 Let $A \in \mathcal{M}_n(K)$. Let $C_A$ be the characteristic polynomial of the matrix $A$. If $P$ is an irreducible monic factor of $C_A$ then

- The $P$-algebraic multiplicity order of the matrix $A$ (or the algebraic multiplicity order of $A$ at the factor $P$) is $\dim_K \text{Ker}P(A)^{\nu_P(C_A)}$. 
• The $P$-geometric multiplicity order of the matrix $A$ (or the geometric multiplicity order of $A$ at the factor $P$) is $\dim_K \ker P(A)$.

Throughout this work we will follow the notations used by the authors of [1]:

1) $\nu_{\text{alg}}(P)$ denote the $P$-algebraic multiplicity order of the matrix $A$.

2) $\nu_{\text{geom}}(P)$ denote the $P$-geometric multiplicity order of the matrix $A$.

**Proposition 4.2** Let $f \in \text{End}_K(E)$ and $IF(f) = (q_1, \ldots, q_r)$ its invariant factors. Let $P \in K[X]$ be an irreducible monic factor of $C_f$. If $s_i = \nu_P(q_i)$. Then for any positive integer $l$

$$\dim_K \ker P^l(f) = \begin{cases} r \times l \times \deg P & \text{if } l \leq s_1 \\ \sum_{i=1}^k s_i + (r-k)l \deg P & \text{if } l \geq s_1 \end{cases}$$

where $k$ is the number of $i$ such that $s_i \leq l$.

**Proof.** Indeed, by theorem 3.1 $\dim_K \ker P^l(f) = \sum_{i=1}^r \deg (\gcd(P^l, q_i)) = \sum_{i=1}^r \inf(l, s_i) \deg P$ so we deduce the result.

**Corollary 4.3** Let $f \in \text{End}_K(E)$ and $P \in K[X]$ be an irreducible monic factor of $C_f$. Let $s = \nu_P(m_f)$. Then

$$\dim_K \ker P^l(f) = \nu_P(C_f) \deg P$$

for any positive integer $l \geq s$.

**Proof.** Indeed, if $t = \nu_P(C_f)$ and $IF(f) = (q_1, \ldots, q_r)$ are the invariant factors of $f$ and $l \geq s = s_r$ then $l \geq s_i$ for all $i = 1, \ldots, r$ so by proposition 4.2 $r=k$ hence $\dim_K \ker P^l(f) = (\sum_{i=1}^r s_i) \deg P = t \deg P$ since $\sum_{i=1}^r s_i = t$.

**Corollary 4.4** Let $A \in \mathcal{M}_n(K)$. Let $C_A$ be the characteristic polynomial of $A$. If $P$ is an irreducible monic factor of $C_A$ then $P$-algebraic multiplicity order of the matrix $A$ is $\nu_P(C_A) \deg P$.

**Proof.** Indeed, let $f$ be the endomorphism canonically associated to $A$. By the corollary 4.3 and since $\nu_P(C_f) \geq \nu_P(m_f)$ we have $\dim_K \ker P^t(f) = t \deg P$ where $t = \nu_P(C_f)$.

Let $f \in \text{End}_K(E)$ and $N_k = \ker f^k$. As $E$ is a finite dimension vector space over $K$, the sequence $N_k$ is stationary. It is well known that if $N_k = N_{k+1}$
then $N_s = N_k$ for any number $s \geq k$. Hence if $k$ is the small number such that $N_k = N_{k+1}$ then the sequence $N_m$ is a strictly increasing sequence in the interval $[0, k]$.

**Corollary 4.5** Let $f \in \text{End}_K(E)$. Let $P \in K[X]$ be an irreducible monic factor of $C_f$. Let $s = \nu_P(m_f)$. Let $N_k = \text{Ker}P^k(f)$. Then the sequence $N_k$ is a strictly increasing sequence in the interval $[0, s]$ and $N_l = N_s$ for any positive integer $l \geq s$.

**Proof.** Indeed, $\text{Ker}P^s(f) \subseteq \text{Ker}P^l(f)$ and by corollary 4.3 if $l \geq s = \nu_P(m_f)$ then $\text{dim}_K \text{Ker}P^l(f) = \text{dim}_K \text{Ker}P^s(f)$ and hence $\text{Ker}P^s(f) = \text{Ker}P^l(f)$ for any positive integer $l \geq s$.

**Corollary 4.6** Let $f \in \text{End}_K(E)$ and $\text{IF}(f) = (q_1, \cdots, q_r)$ its invariant factors. Let $P \in K[X]$ be an irreducible monic factor of $m_f$. If $s_i = \nu_P(q_i)$ then

$$
\nu_{\text{geom}}(P) = \begin{cases} r \text{deg}P & \text{if } s_1 > 1 \\
(\sum_{i=1}^r s_i + (r-k))\text{deg}P & \text{if } s_1 \leq 1
\end{cases}
$$

where $k$ is the number of indices $i$ such that $s_i \leq 1$. In particular if $\nu_P(m_f) = 1$ then $\nu_{\text{geom}}(P) = \nu_P(C_f) \deg P$.

**Proof.** Indeed, if $\nu_P(m_f) = 1$ then by corollary 4.3, we have $\nu_{\text{geom}}(P) = \text{dim}_K \text{Ker}P(f) = t \text{deg} P$.

If the characteristic polynomial $C_f$ of $f$ splits completely (as in the case where $K$ is an algebraically closed field) we refine the classical known results in the following corollary

**Corollary 4.7** Let $f \in \text{End}_K(E)$ factors. Let $P \in K[X]$ be an irreducible factor of $C_f$. Let $s = \nu_P(m_f)$. Then $\text{dim}_K \text{Ker}(f - \lambda I)$ is the number of $i$ such that $q_i(\lambda) = 0$. If further $s = 1$ then the geometric multiplicity order of $\lambda$ is $\nu_P(C_f)$.

**Proof.** If $P = X - \lambda$ then by theorem 3.1 we have $\text{dim}_K \text{Ker}(f - \lambda I) = \sum_{i=1}^r \text{deg}(\gcd(X - \lambda, q_i)) = \text{number of } i \text{ such that } q_i(\lambda) = 0$.
If $s = 1$ we apply the corollary 4.6.

**Proposition 4.8** Let $f \in \text{End}_K(E)$. Let $P \in K[X]$ be an irreducible monic factor of $C_f$. Then $\nu_{\text{alg}}(P) = \nu_{\text{geom}}(P)$ if and only if $\nu_P(m_f) = 1$. 
Proof. Indeed, if \( t = \nu_P(C_f) \) and \( \nu_P(m_f) = 1 \) then by corollary 4.6 \( \nu_{\text{geom}}(P) = t \deg P = \nu_{\text{alg}}(P) \). Conversely if \( \nu_{\text{alg}}(P) = \nu_{\text{geom}}(P) \) then \( (\sum_{i=1}^k s_i + (r-k)) \deg P = t \deg P \) and hence \( \sum_{i=1}^k s_i + (r-k) = t \). If \( k < r \) then \( \sum_{i=k+1}^r s_i = r-k \) and \( 1 < s_i \) for any \( k < i \). But the sum \( \sum_{i=k+1}^r s_i = r-k \) contradicts \( 1 < s_i \) for any \( k < i \). Therefore \( k = r \) and \( s_r \leq 1 \). As \( P \) is a component of the characteristic polynomial \( C_f \) of \( f \) we conclude that \( \nu_P(m_f) = s_r = 1 \).

Proposition 4.9 Let \( f \in \text{End}_K(E) \). Let \( P \in K[X] \) be an irreducible monic factor of \( C_f \). Then \( \nu_{\text{geom}}(P) = \deg P \) if and only if \( \nu_P(m_f) = \nu_P(C_f) \).

Proof. Indeed \( \nu_{\text{geom}}(P) = l \deg P \) where \( l = \sum_{i=1}^k s_i + (r-k) \) and \( k \) is the number of indices \( i \) such that \( s_i \leq 1 \). If \( \nu_{\text{geom}}(P) = \deg P \) then \( l = 1 \) hence if \( k = r \) then \( \sum_{i=1}^r s_i = 1 \) hence \( s_r = 1 \) and \( s_i = 0 \), \( \forall i \leq r-1 \). Hence \( \nu_P(C_f) = \sum_{i=1}^r s_i = s_r = \nu_P(m_f) \).

Conversely if \( \nu_P(m_f) = \nu_P(C_f) \) then \( \sum_{i=1}^{r-1} s_i = 0 \) since \( s_i = 0 \) \( \forall i \leq r-1 \). If \( k < r \) then \( k = r-1 \) and \( s_r \leq 1 \) and \( s_i = 0 \) \( \forall i \leq r-1 \). If \( k = r \) then \( s_r \leq 1 \) since \( P \) is a component of the characteristic polynomial \( C_f \) of \( f \) we conclude that \( s_r = 1 \) and by consequence \( l = 1 \) and \( \nu_{\text{geom}}(P) = \deg P \).

References


Received: December 15, 2013