Operators and Matrices

With Compliments of the Author

Zagreb, Croatia Volume 12, Number 3, September 2018

Adolfo Ballester-Bolinches, Ramón Esteban-Romeroand Vicente Pérez-Calabuig

A note on the rational canonical form of an endomorphism of a vector space of finite dimension

OaM-12-49 823–836

OPERATORS AND MATRICES

AIMS AND SCOPE

'Operators and Matrices' (OaM), aims towards developing a high standard international journal which will publish top quality research papers in matrix and operator theory and their applications. The journal will publish mainly pure mathematics, but occasionally papers of a more applied nature could be accepted providing they have a nontrivial mathematical content. OaM will also publish expository papers and relevant book reviews.

OaM is published quarterly, in March, June, September and December.

SUBMISSION

Manuscripts should be submitted through OaM page: oam.ele-math.com, by e-mail of Editorial office, or directly to any one of the editors working in a related subject area.

Manuscripts are accepted for refereeing on the understanding that the same work has not been published (except in the form of an abstract), and is not under consideration for publication elsewhere.

Authors are advised to send notification of submission by e-mail to oam@element.hr (author(s), title, number of pages, name of editor to whom paper was sent to).

In order to facilitate refereeing, copies of those papers (whether by the author or someone else) which are essential and referred to in the manuscript but are not conveniently accessible, should be enclosed.

The publisher strongly encourages submission of manuscripts written in TeX or one of its variants LaTeX, AMSTeX or AMSLaTeX. On acceptance of the paper, authors will be asked to send the file by electronic mail. The file must be the one from which the accompanying manuscript (finalized version) was printed out. A poscript or pdf file of this final version must also be enclosed.

TITLE PAGE

The following data should be included on title page: the title of the article, author's name (no degrees) author's affiliation, e-mail addresses, mailing address of the corresponding author, and running head less than 60 characters.

ABSTRACT, KEY WORDS, SUBJECT CLASSIFICATION

The manuscript must be accompanied by a brief abstract, no longer than 100-150 words. It should make minimal use of mathematical symbols and displayed formulas. Mathematics Subject Classification (2010) and a list of 4-5 key words must be given.

FIGURES

Figures should be prepared in a digital form suitable for direct reproduction, at resolution of 300 dpi or higher, and in EPS, TIFF or JPEG format.

REFERENCES

Bibliographic references should be listed alphabetically at the end of the article. The authors should consult Mathematical Reviews for the standard abbreviations of journal names.

PROOFS, PAGE CHARGES, OFFPRINTS

The galley proofs will be sent to corresponding author. Late return of the proofs will delay the article to a later issue.

There are no page charges. Authors will receive PDF file of the printed article free of charge. Additional offprints may be ordered from OaM prior to publication.

FORTHCOMING PAPERS

Papers accepted and prepared for publication will appear in the forthcoming section of Journal Web page. They are identical in form as final printed papers, except volume, issue and page numbers.

OaM is published by Publishing House **ELEMENT**, Zagreb, Croatia.

The publication of this journal is supported by Ministry of science, education and sports, Croatia

All correspondence and subscription orders should be addressed to the Editorial Office:

www.ele-math.com

e-mail: oam@ele-math.com

Operators and Matrices
Editorial Office
Menceticeva 2, 10000 Zagreb, Croatia

Fax: +385 1 6008799

The content of this publication is indexed in Mathematical Reviews (MathSciNet), Zentralblatt für Mathematik, Реферативный журнал – Математика, Current Contents, Science Citation Index Expanded, and Scopus.

Operators
and
Matrices

Volume 12, Number 3 (2018), 823–836

doi:10.7153/oam-2018-12-49

A NOTE ON THE RATIONAL CANONICAL FORM OF AN ENDOMORPHISM OF A VECTOR SPACE OF FINITE DIMENSION

ADOLFO BALLESTER-BOLINCHES, RAMÓN ESTEBAN-ROMERO
AND VICENTE PÉREZ-CALABUIG

(*Communicated by M. Omladič*)

Abstract. In this note, we give an easy algorithm to construct the rational canonical form of a square matrix or an endomorphism h of a finite dimensional vector space which does not depend on either the structure theorem for finitely generated modules over principal ideal domains or matrices over the polynomial ring. The algorithm is based on the construction of an element whose minimum polynomial coincides with the minimum polynomial of the endomorphism and on the fact that the h-invariant subspace generated by such an element admits an h-invariant complement. It is also shown that this element can be easily obtained without the factorisation of a polynomial as a product of irreducible polynomials.

1. Introduction

One of the classical problems in matrix theory has been to identify whether two given $n \times n$ matrices over a field K are similar. Recall that two matrices $\mathsf{A}, \mathsf{B} \in \mathscr{M}_n(K)$ are *similar* if there exists a regular matrix $\mathsf{P} \in \mathscr{M}_n(K)$ such that $\mathsf{B} = \mathsf{P}^{-1}\mathsf{A}\mathsf{P}$. This problem has been solved by finding a suitable representative of the similarity class, namely a *canonical form* or a *normal form*. Since an $n \times n$ matrix over a field K can be regarded as the matrix of an endomorphism of a K-vector space V of dimension n in basis $\mathscr{B}$ and two matrices of the same endomorphism in different bases are similar, our problem is equivalent to proving the existence of a basis $\mathscr{B}'$ in which the matrix is a canonical form; the columns of the regular matrix P are the coordinate vectors of the vectors of the basis $\mathscr{B}'$ in the original basis $\mathscr{B}$. In what follows, K will denote a fixed field, V a K-vector space of finite dimension n, and h a fixed endomorphism of V.

One of the most interesting canonical forms was introduced by Frobenius in [2] and is called the *rational canonical form* or *Frobenius canonical form*. Its main advantage is that it can be obtained just with field operations from the entries of the matrix and so it is invariant under field extensions. This matrix is a diagonal sum of the so-called companion matrices associated to monic polynomials. For a polynomial $p = p(x)$, we will denote its degree by δp.

Mathematics subject classification (2010): 15A21, 12E05, 12Y05.

Keywords and phrases: Similarity of matrices, rational canonical form, minimum polynomial, endomorphism.

DEFINITION 1. Let $p = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + x^m$ be a monic polynomial with coefficients in K of degree $m = \delta p \geqslant 1$. The *companion matrix* of p is the $m \times m$ matrix

$$\mathrm{C}(p) = \begin{bmatrix} 0\ 0\ 0 \ldots 0 & -a_0 \\ 1\ 0\ 0 \ldots 0 & -a_1 \\ 0\ 1\ 0 \ldots 0 & -a_2 \\ \vdots\ \vdots\ \vdots\ \ddots\ \vdots & \vdots \\ 0\ 0\ 0 \ldots 0 & -a_{m-2} \\ 0\ 0\ 0 \ldots 1 & -a_{m-1} \end{bmatrix}.$$

THEOREM 2. *There exists a basis of V in which the coordinate matrix of h is the diagonal sum of matrices $\mathrm{C}(d_1)$, $\mathrm{C}(d_2), \ldots,$ $\mathrm{C}(d_s)$, where d_1, $d_2, \ldots,$ d_s are non-constant monic polynomials with coefficients in K and $d_1 \mid d_2 \mid \ldots \mid d_s$. Moreover, the polynomials d_1, $d_2, \ldots,$ d_s are uniquely determined by h.*

The polynomials d_1, $d_2, \ldots,$ d_s receive the name of *invariant factors* of h.

It follows by Theorem 2 that each square matrix over a field K is similar to a unique rational canonical form. Other canonical matrices which can be taken as standard representatives of the similarity class of a matrix include the *primary rational canonical form*, the *Jordan canonical form* and its generalisations (see, for instance, [3, Chapter 3, Section 10] or [4] for details), and the *Weyr canonical form* [8].

Most of the known proofs of Theorem 2 depend on the structure of finitely generated modules over principal ideal domains (see, for instance, [3, Chapter 3]) or the diagonal Smith form for matrices with polynomial entries (like in [1, Section 12.2]) and do not give efficient algorithms to compute the rational canonical form or the basis associated to this matrix. The PhD thesis of Ozello [6] contains a constructive proof for the calculation of the rational canonical form of a square matrix, by means of similarity transformations in the matrix. These algorithms have also been presented in the book [5].

In this note, we present an improvement of Ozello's algorithm to compute the rational canonical form with the help of elements of the vector space whose minimum polynomial coincides with the minimum polynomial of the endomorphism. The computation of these elements is usually presented with the help of the decomposition of a polynomial as a product of irreducible polynomials (see Remark 8 below) or as a consequence of Theorem 2. However, exact or efficient algorithms for the computation of this decomposition can be unavailable for some fields and some polynomials. It is well known that Euclid's algorithm is an efficient method for the computation of the greatest common divisor and so of the least common multiple of two polynomials. In Section 2 we show that the interesting factors needed to compute the least common multiple of two polynomials can be obtained without determining explicitly the decomposition of the polynomials as products of irreducible polynomials. In Section 3 a method to compute an element whose minimum polynomial coincides with the minimum polynomial of the endomorphism is presented. The results of Section 2 are used in Section 3 to show that this element can be computed without appealing to the factorisation of a polynomial as a product of irreducible polynomials. Section 4 provides a proof of Theorem 2. Finally, Section 5 presents an example of the computation of the rational canonical form of a matrix as an application of the results of this paper.

2. A remark on the least common multiple of two polynomials

Let f, g be two monic polynomials in the polynomial ring $R = K[x]$. We can decompose them as

$$f = rst \quad \text{and} \quad g = jkl, \tag{1}$$

where r, s, t, j, k, and l are monic polynomials such that:

1. r is the product of all powers of irreducible factors in f which appear also in g with exponents more than or equal to the corresponding exponents in f,
2. s is the product of all powers of irreducible factors in f which appear also in g but with exponents strictly less than the corresponding exponents in f,
3. t is the product of all powers of irreducible factors in f which do not appear in g,
4. j is the product of all powers of irreducible factors in g which appear also in f with exponents less than or equal to the corresponding exponents in g,
5. k is the product of all powers of irreducible factors in g which appear also in f but with exponents strictly greater than the corresponding exponents in g,
6. l is the product of all powers of irreducible factors in g which do not appear in f,

where the products are understood to be 1 if no irreducible factors satisfy the corresponding condition. For example, let

$$f = x^2(x-1)^3(x-2)(x-3) \quad \text{and} \quad g = x^2(x-1)^2(x-2)^4(x-4).$$

The corresponding decomposition (1) is $f = rst$ and $g = jkl$, with $r = x^2(x-2)$, $s = (x-1)^3$, $t = x-3$, $j = x^2(x-2)^4$, $k = (x-1)^2$, $l = x-4$.

The purpose of this section is to describe how to effectively compute the factors r, s, t, j, k, and l without finding the factorisations of f and g as a product of irreducible monic polynomials, but using only the sum, the product, the Euclidean division, and the Euclidean algorithm.

It is well known that the decomposition (1) allows us to calculate the greatest common divisor and the least common multiple of two monic polynomials.

LEMMA 3. *Let f, $g \in K[x]$ be two monic polynomials and let $f = rst$, $g = jkl$ as in* (1). *Then* $\gcd\{f,g\} = rk$ *and* $lcm\{f,g\} = stjl$.

Now we state the main result of this section.

LEMMA 4. *The factors r, s, t, j, k, and l of Lemma 3 can be obtained from f and g with polynomial operations (sum, multiplication, Euclidean division, and the Euclidean algorithm to compute the greatest common divisor) without needing to know the decompositions of f and g as products of powers of irreducible polynomials.*

In order to prove Lemma 4, we will use the following lemma.

LEMMA 5. *Assume that f and g are monic polynomials. Decompose $f = pq$ such that p contains all powers of irreducible factors in f appearing in g, and q contains all powers of irrreducible factors in f not appearing in g. Then p and q can be computed as*

$$p = \gcd\{f, g^{\mu}\} \quad \textit{and} \quad q = f/\gcd\{f, g^{\mu}\},$$

where μ is any natural number satisfying $p \mid g^{\mu}$.

Proof. Since q and g are coprime, it follows that q and g^{μ} are coprime. Hence

$$\gcd\{f, g^{\mu}\} = \gcd\{pq, g^{\mu}\} = \gcd\{p, g^{\mu}\} = p. \quad \square$$

Note that since p divides some power of g, we can always take $\mu \geqslant \delta f$ in Lemma 5.

Proof of Lemma 4. Let $f = rst$ and $g = jkl$ as in (1). An application of Lemma 5 to the polynomials $f = rst$ and $d = \gcd\{f, g\} = rk$ allows us to identify $p_1 = rs$ and $q_1 = t$. Similarly, an application of Lemma 5 to g and d allows us to identify $p_2 = jk$ and $q_2 = l$. Note that $s/k = (rs)/(rk) = p_1/d$. Moreover, s, k, and s/k all contain the same irreducible factors by the definition of s and k. Hence, applying Lemma 5 to $p_1 = rs$ and $s/k = p_1/d$ we obtain $p_3 = s$ and $q_3 = r$, and, similarly, applying Lemma 5 to $p_2 = jk$ and $p_3 = s$ we obtain $p_4 = k$ and $q_4 = j$. $\square$

3. The minimum polynomial of an element and an endomorphism

Given a polynomial $f = f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m \in K[x]$, we denote by $fv = f(x)v = f(h)(v) = a_0 v + a_1 h(v) + a_2 h^2(v) + \cdots + a_m h^m(v) \in V$. With this definition, V acquires a structure of module over the polynomial ring $K[x]$.

Given a vector $v \in V$, the set of all polynomials $f \in K[x]$ such that $fv = 0$ is an ideal of $K[x]$. This ideal cannot be zero, because the set $\{v, h(v), h^2(v), \dots, h^m(v)\}$ must be linearly dependent for some m. Since $K[x]$ is a principal ideal domain, this ideal has a unique monic generator $\operatorname{min\,pol} v$, called the *minimum polynomial* or the *order* of v under h. The minimum polynomial of a vector can be easily obtained by computing the elements v, $h(v)$, $h^2(v), \dots$, until we find that these elements are linearly dependent. The dependency relation between these elements will give the minimum polynomial of v.

The ring of endomorphisms of V is a K-vector space of dimension n^2 and so the set $\{\mathrm{id}_V, h, h^2, \dots, h^m\}$ must be K-linearly dependent for some m. If m is the smallest number for which there is a linear dependence relation $a_0 \operatorname{id}_V + a_1 h + a_2 h^2 + \cdots + a_m h^m = 0$ with not all coefficients equal to 0, then the polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$ satisfies that $fv = 0$ for each $v \in V$. Therefore, for every subset S of V, the set of all polynomials $f \in K[x]$ such that $fv = 0$ for all $v \in S$ is again a non-zero ideal of $K[x]$ and its unique monic generator is called the *minimum polynomial* of S under h. When $S = V$, the minimum polynomial of V is simply called the *minimum polynomial* of h and denoted by $\operatorname{min pol} h$.

The following result is elementary.

LEMMA 6. (see [3, Chapter 3, Section 3]) *If* $\{v_1, \ldots, v_n\}$ *is a basis of* V*, then* $\operatorname{min pol} h = \operatorname{lcm}\{\operatorname{min pol} v_i : 1 \leqslant i \leqslant n\}$.

The next result can be used to obtain vectors with given minimum polynomials.

LEMMA 7. (see [3, page 68])

1. *Assume that* f, $g \in K[x]$ *are monic and that* $v \in V$ *satisfies that* $\operatorname{min pol} v = fg$. *Then* $\operatorname{min pol} gv = f$.

2. *Assume that* f, $g \in K[x]$ *are monic,* $\gcd\{f, g\} = 1$ *and that* v, $w \in V$ *are such that* $f = \operatorname{min pol} v$ *and* $g = \operatorname{min pol} w$. *Then* $\operatorname{min pol}(v + w) = fg$.

We say that a subspace W of V is h*-invariant* if $h(W) \subseteq W$. Let $R = K[x]$. Denote by $Ra = \{fa : f \in R\}$. Then Ra is an h-invariant subspace of V. If $p = \operatorname{min pol} a = a_0 + a_1 x + a_2 x^2 + \cdots + a_{m-1} x^{m-1} + x^m$, then $\{a, h(a), h^2(a), \ldots, h^{m-1}(a)\}$ is a basis of Ra and the coordinate matrix of $h|_{Ra}$ in this basis is precisely the companion matrix $\mathrm{C}(p)$.

REMARK 8. It is possible to use Lemma 7 with the help of the decomposition of a polynomial as a product of irreducible polynomials to conclude easily the existence of a vector in V whose minimum polynomial coincides with the minimum polynomial of the endomorphism. For example, let $\{v_1, \ldots, v_n\}$ be a basis of V. Let f_i be the minimum polynomial of v_i and, for a monic irreducible polynomial p dividing the minimum polynomial of h, suppose that $f_i = p^{m_{p,i}} q_{p,i}$ where p does not divide $q_{p,i}$. Choose i_p such that $m_{p,i_p} = \max\{m_{p,i} \mid 1 \leqslant i \leqslant n\}$. Then the minimum polynomial of $w_p = q_{p,i_p} v_{i_p}$ is $p^{m_{p,i_p}}$. The sum of the w_p for all irreducible polynomials p dividing the minimum polynomial of h has as minimum polynomial the minimum polynomial of h by Lemma 6. The drawback of this approach is that the algorithms to compute exactly the irreducible factors of a polynomial can be unavailable or inefficient.

Theorem 2 admits the following alternative statement.

THEOREM 9. *Let* K *be a field, let* V *be a vector space over* K *of finite dimension* n *and let* h *be an endomorphism of* V. *Then there exist elements* a_1, $a_2, \ldots,$ a_s *of* V *such that* $V = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_s$ *and if* $d_j = \operatorname{min pol} a_j$ *for* $1 \leqslant j \leqslant s$*, then* $d_1 \mid d_2 \mid \cdots \mid d_s$. *Moreover, the polynomials* d_1, $d_2, \ldots,$ d_s *are uniquely determined by* h.

The proofs known to us for the existence of an element $v \in V$ such that $\operatorname{minpol} v = \operatorname{minpol} h$ (Theorem 11 below) follow from Theorem 9 or are proved by induction on the dimension of V and rely on the following result, which generalises the second part of Lemma 7.

LEMMA 10. *Given two vectors v, $w \in V$, there exists $c \in V$ such that*

$$\operatorname{minpol} c = \operatorname{lcm}\{\operatorname{minpol} v, \operatorname{minpol} w\}.$$

Proof of Lemma 10. Write $f = \operatorname{minpol} v$ and $g = \operatorname{minpol} w$, and decompose $f = rst$ and $g = jkl$ as in (1). By Lemma 7, we have that $\operatorname{minpol} rv = st$ and $\operatorname{minpol} kw = jl$. Since s, t, j, and l are pairwise coprime, it follows that $\operatorname{minpol}(rv + kw) = (st)(jl) = \operatorname{lcm}\{f, g\}$. □

We must observe that, despite the polynomials r, s, t, j, k, and l can be defined as products of certain irreducible monic factors, they can be obtained without knowing efficient factorisation algorithms, according to Lemma 4.

The last result of this section, which is established with elementary arguments, will play a major role in our approach.

THEOREM 11. *There exists an element $v \in V$ with* $\operatorname{minpol} v = \operatorname{minpol} h$.

Proof. Let $\{v_1, \dots, v_n\}$ be a basis of V. Let $w_1 = v_1$, and for $2 \leqslant i \leqslant n$ we construct an element w_i such that

$$\operatorname{minpol} w_i = \operatorname{lcm}\{\operatorname{minpol} w_{i-1}, \operatorname{minpol} v_i\}$$

with the help of Lemma 10. By Lemma 6, $\operatorname{minpol} w_n = \operatorname{minpol} h$. □

4. The rational canonical form

Ozello's algorithm [6] begins with the computation of a *weak Frobenius form*, in which the associated matrix is a direct sum of companion matrices, but the divisibility property is not ensured. This form can be used to obtain the rational canonical form. However, we observe that Ozello's algorithm would give directly the matrix of Theorem 2 if an element satisfying Theorem 11 were given as an input value.

THEOREM 12. *Let $a \in V$ such that the minimum polynomial of a is the minimum polynomial of h. Then there exists an h-invariant subspace W of V such that $V = W \oplus Ra$.*

It is worth mentioning that other algorithms give the existence of an element $v \in V$ whose minimum polynomial coincides with the minimum polynomial of the endomorphism and such that Rv admits and h-invariant complement in V. Theorem 12 shows that Ra has an h-invariant complement in V for every element $a \in V$ whose minimum polynomial coincides with the minimum polynomial of the endomorphism.

Although Theorem 12 can be obtained from an application of the procedures on [6, pages 29–35] and [6, Théorème 4], we will present here a direct and shorter proof for the reader's interest.

Proof of Theorem 12. Let $p = \min\mathrm{pol}\, h$ and $m = \delta p$. Consider the natural basis

$$\{a, h(a), h^2(a), \ldots, h^{m-1}(a)\}$$

of Ra. Let us complete it to a basis $\mathscr{B} = \{v_1, \ldots, v_n\}$ of V, where $v_{n-m+1+i} = h^i(a)$ for $0 \leqslant i \leqslant m-1$. In this basis, the coordinate matrix of h is

$$\mathsf{A} = (a_{i,j}) = \begin{bmatrix} \mathsf{B} & \mathsf{O} \\ \mathsf{C} & \mathsf{C}(p) \end{bmatrix}.$$

We will obtain the result if we replace the elements $v_1, \ldots,$ v_{n-m} of $\mathscr{B}$ in such a way the block corresponding to C vanishes. Assume that the last k rows of the matrix C are null, with $0 \leqslant k \leqslant m-2$, and let $\alpha = a_{n-k,j} \neq 0$ with $1 \leqslant j \leqslant n-m$. Consider the basis $\bar{\mathscr{B}} = \{\bar{v}_1, \ldots, \bar{v}_n\}$, where $\bar{v}_j = v_j - \alpha v_{n-k-1}$ and $\bar{v}_l = v_l$ for $l \neq j$. The effect of this basis change on the matrix A is to subtract to the j-th column of A its $n-k-1$-th column, so that the element $a_{n-k,j}$ becomes 0, and to add to the $n-k-1$-th row of A its j-th row. Since the m right elements of the j-th row of A are zero, the block corresponding to $\mathsf{C}(p)$ does not change. The k last rows of C do not change. Arguing in this way, we can find a new basis $\widetilde{\mathscr{B}} = \{\tilde{v}_1, \ldots, \tilde{v}_n\}$ of V in such a way the matrix associated to h in $\widetilde{\mathscr{B}}$ has the form

$$\tilde{\mathsf{A}} = (\tilde{a}_{i,j}) = \begin{bmatrix} \mathsf{B} & \mathsf{O} \\ \tilde{\mathsf{C}} & \mathsf{C}(p) \end{bmatrix},$$

where all rows of $\tilde{\mathsf{C}}$ except perhaps the first one are null. Suppose that $\beta = \tilde{a}_{n-m+1,j} \neq 0$ with $1 \leqslant j \leqslant n-m$. Consider the set of vectors $\{\tilde{v}_j, h(\tilde{v}_j), \ldots, h^m(\tilde{v}_j)\}$. The matrix which has as columns the coordinate vectors of these vectors in the basis $\tilde{\mathscr{B}}$ has the form

$$\begin{array}{r|cccccc|}
 & 0 & * & * & \ldots & * & * \\
 & \vdots & \vdots & \vdots & & \vdots & \vdots \\
j \rightarrow & 1 & * & * & \ldots & * & * \\
 & \vdots & \vdots & \vdots & & \vdots & \vdots \\
 & 0 & * & * & \ldots & * & * \\
n-m+1 \rightarrow & 0 & \beta & * & \ldots & * & * \\
 & 0 & 0 & \beta & \ldots & * & * \\
 & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
 & 0 & 0 & 0 & \ldots & \beta & * \\
 & 0 & 0 & 0 & \ldots & 0 & \beta
\end{array},$$

where each symbol "$*$" denotes an unspecified element of K. The rank of this matrix is $m+1$. This implies that the minimum polynomial of $\tilde{v}_j$ has degree greater than m, in contradiction with the fact that the minimum polynomial of h has degree m. Hence

$\tilde{\mathsf{C}} = \mathsf{O}$. In particular, $W = \langle \tilde{v}_1, \ldots, \tilde{v}_{n-m} \rangle$ is an h-invariant subspace and we have the desired decomposition. □

Most of the proofs we know of the unicity of the polynomials d_1, $d_2, \ldots,$ d_s in Theorem 9 are based on the structure theorems for finitely generated modules over principal ideal domains or require the Smith canonical form for matrices over $K[x]$. Our proof of the unicity of Theorem 9 will use the following theorem, which does not require these results and is more general, because the divisibility of the minimum polynomials is not required.

THEOREM 13. *Let $V = Ra_1 \oplus \cdots \oplus Ra_s$ with* $\operatorname{min\,pol} a_i = d_i$, $1 \leqslant i \leqslant s$*. Let p be an irreducible monic polynomial. Let m be a natural number. Then the number of d_i divisible by p^m is*

$$\frac{\dim_K \operatorname{Ker} p(h)^m - \dim_K \operatorname{Ker} p(h)^{m-1}}{\delta p}.$$

Proof. Choose any $m \geqslant 0$ and let $v \in \operatorname{Ker} p(h)^m$. Write $v = f_1 a_1 + \cdots + f_s a_s$ with $f_i \in R$. Then $p^m f_1 a_1 + \cdots + p^m f_s a_s = 0$ and so $p^m f_i a_i = 0$ for each i. Therefore $d_i \mid p^m f_i$. Write $d_i = p^{n_i} q_i$, where $\gcd\{p, q_i\} = 1$. Then $p^{n_i} q_i \mid p^m f_i$ yields $p^{n_i} \mid p^m f_i$ and $q_i \mid f_i$. Substituting $f_i = r_i q_i$, we get $p^{n_i} \mid p^m r_i$. Thus we have

$$\operatorname{Ker} p(h)^m = \left\{ \sum_{i=1}^{s} r_i q_i a_i \;\middle|\; r_i \in R \text{ and } p^{n_i} \mid p^m r_i \text{ for each } i \right\}.$$

For each i we have two possibilities: if $n_i \leqslant m$, then always $p^{n_i} \mid p^m r_i$, and if $n_i > m$, then $p^{n_i} \mid p^m r_i$ forces $r_i \in R p^{n_i - m}$. Thus

$$\operatorname{Ker} p(h)^m = \left(\bigoplus_{\substack{1 \leqslant i \leqslant s \\ n_i \leqslant m}} R q_i a_i \right) \oplus \left(\bigoplus_{\substack{1 \leqslant i \leqslant s \\ n_i > m}} R p^{n_i - m} q_i a_i \right).$$

To compute the dimension of this space, note that by Lemma 7 the minimum polynomial of $q_i a_i$ is p^{n_i} and the minimum polynomial of $p^{n_i - m} q_i a_i$ is p^m if $n_i > m$. Consequently, $\dim_K(R q_i a_i) = (\delta p) \cdot n_i$ and, if $n_i > m$, then $\dim_K(R p^{n_i - m} q_i a_i) = (\delta p) \cdot m$, which yields

$$\dim_K \operatorname{Ker} p(h)^m = (\delta p) \left(\sum_{\substack{1 \leqslant i \leqslant s \\ n_i \leqslant m}} n_i + \sum_{\substack{1 \leqslant i \leqslant s \\ n_i > m}} m \right).$$

Now choosing $m \geqslant 1$ and applying this formula for m and for $m - 1$, we easily see that

$$\dim\bigl(\operatorname{Ker} p(h)^m\bigr) - \dim\bigl(\operatorname{Ker} p(h)^{m-1}\bigr) = (\delta p) \sum_{\substack{1 \leqslant i \leqslant s \\ n_i \geqslant m}} 1,$$

as needed. □

We are now in a position to give a proof of Theorem 9, and so a proof of Theorem 2.

Proof of Theorem 9. In order to prove the existence of the decomposition, we argue by induction on n. If $n=1$, then obviously $V=Ra$ with $a\in V\setminus\{0\}$. Assume that the result is true for vector spaces of dimension $m<n$. By Theorem 11, there exists $a\in V$ such that $\operatorname{min\,pol} h=\operatorname{min\,pol} a$. By Theorem 12, there exists an h-invariant subspace W of V such that $V=W\oplus Ra$. By induction, there exist a_1, $a_2,\dots,$ $a_{s-1}\in W$ such that $W=Ra_1\oplus Ra_2\oplus\cdots\oplus Ra_{s-1}$ and if $d_i=\operatorname{min\,pol} a_i$, $1\leqslant i\leqslant s-1$, then $d_1\mid d_2\mid\cdots\mid d_{s-1}$. Now $\operatorname{min\,pol} h|_W=\operatorname{min\,pol} W$ divides $\operatorname{min\,pol} h$. Let $a_s=a$, then $\operatorname{min\,pol} a_i\mid\operatorname{min\,pol} h=\operatorname{min\,pol} a_s$ for $1\leqslant i\leqslant s-1$ and the existence follows.

The unicity of the d_i follows immediately from Theorem 13. □

5. An example

As an application of the above techniques, we consider the endomorphism h of a vector space V of dimension 7 over the rational field $\mathbb{Q}$ such that the matrix in the basis $\mathscr{B}=\{v_1,\dots,v_7\}$ is

$$\mathsf{A}=\begin{bmatrix}2&0&0&0&0&0&0\\2&4&1&-1&-7&-2&-1\\0&0&1&0&0&0&0\\1&0&0&1&0&0&0\\0&0&0&0&1&0&0\\2&1&1&-1&-5&1&-1\\1&0&1&0&0&0&1\end{bmatrix}.$$

Let us compute its rational canonical form C as well as the transition matrix P such that $\mathsf{P}^{-1}\mathsf{A}\mathsf{P}=\mathsf{C}$. Although the computations can be done by hand, we can make use of a computer algebra system like Scilab [7].

The minimum polynomials of the elements of the basis $\mathscr{B}$ are

$$\begin{aligned}\operatorname{min\,pol} v_1&=x^2-3x+2,\\\operatorname{min\,pol} v_2&=x^2-5x+6,\\\operatorname{min\,pol} v_3&=x^2-2x+1,\\\operatorname{min\,pol} v_4&=x^2-3x+2,\\\operatorname{min\,pol} v_5&=x^3-6x^2+11x-6,\\\operatorname{min\,pol} v_6&=x^2-5x+6,\\\operatorname{min\,pol} v_7&=x^2-3x+2.\end{aligned}$$

We compute a vector whose minimum polynomial coincides with the minimum polynomial of A. In this case, we could easily obtain factorisations of all these polynomials as products of linear polynomials, but we will not use the factorisations to obtain that vector.

Following Theorem 11, we set $w_1 = v_1$. Now we apply Lemma 10 to compute a vector w_2 with minimum polynomial $\operatorname{lcm}\{\operatorname{min\,pol} w_1, \operatorname{min\,pol} v_2\} = \operatorname{lcm}\{x^2-3x+2, x^2-5x+6\} = x^3-6x^2+11x-6$. Let us find the factors of Lemma 3 with Lemma 4; we will use the notation of these lemmas. Let $f = \operatorname{min\,pol} w_1 = x^2-3x+2$ and $g = \operatorname{min\,pol} v_2 = x^2-5x+6$. Since $d = \gcd\{x^2-3x+2, x^2-5x+6\} = x-2$, we can compute $p_1 = rs = \gcd\{x^2-3x+2, (x-2)^2\} = x-2$ and $q_1 = t = x-1$. Then we can identify $p_2 = jk = \gcd\{x^2-5x+6, (x-2)^2\} = x-2$ and $q_2 = l = x-3$. Now with $p_1 = rs = x-2$ and $s/k = p_1/d = (x-2)/(x-2) = 1$ we compute $p_3 = s = \gcd\{x-2, 1\} = 1$ and $q_3 = r = x-2$ and, with $p_2 = jk = x-2$ and $p_3 = s = 1$ we obtain $p_4 = k = \gcd\{x-2, 1\} = 1$ and $q_4 = j = x-2$. By Lemma 10, $w_2 = rw_1 + kv_2 = (x-2)w_1 + v_2 = 3v_2 + v_4 + 2v_6 + v_7$ has minimum polynomial $x^3-6x^2+11x-6$.

We use again Lemma 3 now with the polynomials $f = \operatorname{min\,pol} w_2 = x^3-6x^2+11x-6$ and $g = \operatorname{min\,pol} v_3 = x^2-2x+1$ to obtain a vector w_3 with minimum polynomial $\operatorname{min\,pol} w_3 = \operatorname{lcm}\{f, g\} = x^4-7x^3+17x^2-17x+6$. Note that $d = rk = \gcd\{\operatorname{min\,pol} w_2, \operatorname{min\,pol} v_3\} = x-1$. We can compute $p_1 = \gcd\{x^3-6x^2+11x-6, (x-1)^3\} = x-1 = rs$ and $q_1 = t = x^2-5x+6$. Now with g and d we can identify $p_2 = jk = \gcd\{x^2-2x+1, (x-1)^2\} = x^2-2x+1$ and $l = 1$. Now $s/k = p_1/d = (x-1)/(x-1) = 1$. With $p_1 = rs = x-1$ and $s/k = 1$ we obtain $p_3 = s = \gcd\{rs, (s/k)^1\} = \gcd\{x-1, 1\} = 1$ and $q_3 = r = x-1$, and, from $p_2 = jk = x^2-2x+1$ and $p_3 = s = 1$ we obtain $p_4 = k = \gcd\{x^2-2x+1, 1\} = 1$ and $q_4 = j = x^2-2x+1$. By Lemma 10, $w_3 = rw_2 + kv_3 = (x-1)w_2 + v_3 = 3v_2 + v_3 + v_6$. Note that $\operatorname{min\,pol} w_3 = \operatorname{min\,pol} \mathsf{A}$, and so we can work with this element.

The set $\{w_3, h(w_3), h^2(w_3), h^3(w_3)\}$ is linearly independent and we can complete it with v_1, v_4, v_5 to obtain a new basis

$$\mathscr{B}_1 = \{v_1, v_4, v_5, w_3, h(w_3), h^2(w_3), h^3(w_3)\}$$

of V. The matrix whose columns are the coordinate vectors of $\mathscr{B}_1$ in $\mathscr{B}$ is

$$\mathsf{Q} = \begin{bmatrix} 1&0&0&0&0&0&0 \\ 0&0&0&3&11&34&103 \\ 0&0&0&1&1&1&1 \\ 0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&1&5&16&49 \\ 0&0&0&0&1&2&3 \end{bmatrix}.$$

The matrix of h in $\mathscr{B}_1$ is

$$\mathsf{B} = \mathsf{Q}^{-1}\mathsf{A}\mathsf{Q} = \begin{bmatrix} 2&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ -6&3&19/2&0&0&0&-6 \\ 25/2&-7&-89/4&1&0&0&17 \\ -8&5&16&0&1&0&-17 \\ 3/2&-1&-13/4&0&0&1&7 \end{bmatrix}.$$

Now we will make zeros in the last four rows and the first three columns, starting from the last row, with similarity elementary operations. In order to know the new basis, we can also make the column operations on the matrix Q. We do it by putting Q below B. We add to the first column $-3/2$ times the sixth column, to the second column the sixth column, and to the third column $13/4$ times the sixth column, and we do the inverse operations on files, namely we add to the sixth row $3/2$ times the first row, -1 times the second row, and $-13/4$ times the third row. We obtain the following matrix:

$$\left[\begin{array}{ccccccc}
2 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
-6 & 3 & 19/2 & 0 & 0 & 0 & -6 \\
25/2 & -7 & -89/4 & 1 & 0 & 0 & 17 \\
-6 & 4 & 51/4 & 0 & 1 & 0 & -17 \\
0 & 0 & 0 & 0 & 0 & 1 & 7 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
-51 & 34 & 221/2 & 3 & 11 & 34 & 103 \\
-3/2 & 1 & 13/4 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
-24 & 16 & 52 & 1 & 5 & 16 & 49 \\
-3 & 2 & 13/2 & 0 & 1 & 2 & 3
\end{array}\right].$$

Now we subtract to the first column -6 times the fifth column, to the second column 4 times the fifth column, and to the third column $51/4$ times the fifth column, and we make the inverse operations on rows, that is, we add to the fifth row -6 times the first row, 4 times the second row, and $51/4$ times the third row. We get the following matrix:

$$\left[\begin{array}{ccccccc}
2 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
-6 & 3 & 19/2 & 0 & 0 & 0 & -6 \\
9/2 & -3 & -19/2 & 1 & 0 & 0 & 17 \\
0 & 0 & 0 & 0 & 1 & 0 & -17 \\
0 & 0 & 0 & 0 & 0 & 1 & 7 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
15 & -10 & -119/4 & 3 & 11 & 34 & 103 \\
9/2 & -3 & -19/2 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
6 & -4 & -47/4 & 1 & 5 & 16 & 49 \\
3 & -2 & -25/4 & 0 & 1 & 2 & 3
\end{array}\right].$$

Finally, we subtract to the first column $9/2$ times the fourth one, to the second column -3 times the fourth one, and to the third column $-19/2$ times the fourth one, and we do the corresponding inverse operations on rows, namely we add to the fourth row $9/2$

times the first one, -3 times the second one, and $-19/2$ times the third one. We obtain the following matrix:

$$\left[\begin{array}{ccccccc}
2 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -6 \\
0 & 0 & 0 & 1 & 0 & 0 & 17 \\
0 & 0 & 0 & 0 & 1 & 0 & -17 \\
0 & 0 & 0 & 0 & 0 & 1 & 7 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
3/2 & -1 & -5/4 & 3 & 11 & 34 & 103 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
3/2 & -1 & -9/4 & 1 & 5 & 16 & 49 \\
3 & -2 & -25/4 & 0 & 1 & 2 & 3
\end{array}\right]$$

Let $\bar{v}_1 = v_1 + (3/2)v_2 + (3/2)v_6 + 3v_7$, $\bar{v}_2 = -v_2 + v_4 - v_6 - 2v_7$, $\bar{v}_3 = -(5/4)v_2 + v_5 - (9/4)v_6 - (25/4)v_7$. Then $\mathscr{B}_W = \{\bar{v}_1, \bar{v}_2, \bar{v}_3\}$ is a basis for an h-invariant subspace W and the matrix of $h|_W$ with respect to $\mathscr{B}_W$ is

$$\mathsf{A}_1 = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Now $\operatorname{min\,pol} \bar{v}_1 = x^2 - 3x + 2$ and $\operatorname{min\,pol} \bar{v}_2 = \operatorname{min\,pol} \bar{v}_3 = x - 1$. Hence $\operatorname{min\,pol} \bar{v}_1 = \operatorname{min\,pol} \mathsf{A}_1$. Therefore we can consider the linearly independent set $\{\bar{w}_1, h(\bar{w}_1)\} = \{\bar{v}_1, 2\bar{v}_1 + \bar{v}_2\}$, that we complete to a basis $\bar{\mathscr{B}}_W = \{\bar{v}_3, \bar{v}_1, 2\bar{v}_1 + \bar{v}_2\}$ of W by adjoining the element $\bar{v}_3$, that is, $\bar{\mathscr{B}}_W = \{\tilde{w}_1, \tilde{w}_2, \tilde{w}_3\}$ with $\tilde{w}_1 = (-5/4)v_2 + v_5 - (9/4)v_6 - (25/4)v_7$, $\tilde{w}_2 = v_1 + (3/2)v_2 + (3/2)v_6 + 3v_7$, and $\tilde{w}_3 = 2v_1 + 2v_2 + v_4 + 2v_6 + 4v_7$. Let $\bar{\mathsf{Q}}$ be the matrix whose columns are the coordinate vectors of this basis in the basis $\mathscr{B}_W$, that is,

$$\bar{\mathsf{Q}} = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

The matrix of $h|_W$ in this new basis is

$$\bar{\mathsf{Q}}^{-1} \mathsf{A}_1 \bar{\mathsf{Q}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{bmatrix}.$$

Since the entry $(3,1)$ of this matrix is 0, this matrix is in the block-diagonal form corresponding to the rational canonical form and the algorithm ends here. Then $W = \langle \tilde{w}_1 \rangle \oplus R\tilde{w}_2$ and both summands are h-invariant. Hence the rational canonical form of h is

$$\mathsf{C} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -6 \\ 0 & 0 & 0 & 1 & 0 & 0 & 17 \\ 0 & 0 & 0 & 0 & 1 & 0 & -17 \\ 0 & 0 & 0 & 0 & 0 & 1 & 7 \end{bmatrix}.$$

The transition matrix

$$\mathsf{P} = \begin{bmatrix} 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ -5/4 & 3/2 & 2 & 3 & 11 & 34 & 103 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -9/4 & 3/2 & 2 & 1 & 5 & 16 & 49 \\ -25/4 & 3 & 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

satisfies that $\mathsf{P}^{-1}\mathsf{A}\mathsf{P} = \mathsf{C}$. The invariant factors are $d_1 = x - 1$, $d_2 = x^2 - 3x + 2$, $d_3 = x^4 - 7x^3 + 17x^2 - 17x + 6$.

Acknowledgements. This work has been supported by the grants MTM2014-54707-C3-1-P from the *Ministerio de Economía y Competitividad*, Spain, and FEDER, European Union, and PROMETEO/2017/057 from the *Generalitat* (Valencian Community, Spain). The first author has been also supported by a project from the National Natural Science Foundation of China (NSFC, No. 11271085) and a project of Natural Science Foundation of Guangdong Province, China (No. 2015A030313791). The third author has been also supported by a predoctoral grant from the programme *Atracció del talent* of the Universitat de València.

We thank the anonymous referee for his/her careful review, that has helped us to clarify and simplify the presentation of the paper.

REFERENCES

[1] D. S. DUMMIT AND R. M. FOOTE, *Abstract Algebra*, John Wiley & Sons, Inc., Hoboken, NJ, USA, third edition, 2004.

[2] G. FROBENIUS, *Theorie der linearen Formen mit ganzen Coefficienten*, J. Reine Angew. Math. **86**: 146–208, 1879.

[3] N. JACOBSON, *Basic Algebra I*, Dover Books on Mathematics. Dover Publications, Mineola, NY, USA, second edition, 2012.

[4] K. R. MATTHEWS, *A rational canonical form algorithm*, Math. Bohem. **117** (3): 315–324, 1992.

[5] J. M. OLAZÁBAL, *Procedimientos simbólicos en álgebra lineal*, Servicio de Publicaciones, Universidad de Cantabria, Santander, Spain, 1988.

[6] P. OZELLO, *Calcul exact des formes de Jordan et de Frobenius d'une matrice. Modélisation et simulation*, PhD thesis, Université Joseph-Fourier–Grenoble I, Grenoble, France, 1987.

[7] Scilab Enterprises, *Scilab: Free and Open Source software for numerical computation*, Scilab Enterprises, Orsay, France, 2012.

[8] E. WEYR, *Zur Theorie der bilinearen Formen*, Monatsh. Math. Physik **1**: 163–200, 1890.

(Received December 8, 2016)

Adolfo Ballester-Bolinches
Departament de Matemàtiques
Universitat de València
Dr. Moliner, 50, 46100 Burjassot, València, Spain
e-mail: Adolfo.Ballester@uv.es

Ramón Esteban-Romero
Departament de Matemàtiques
Universitat de València
Dr. Moliner, 50, 46100 Burjassot, València, Spain
e-mail: Ramon.Esteban@uv.es
and
Institut Universitari de Matemàtica Pura i Aplicada
Universitat Politècnica de València
Camí de Vera, s/n, 46022 València, Spain
e-mail: resteban@mat.upv.es

Vicente Pérez-Calabuig
Departament de Matemàtiques
Universitat de València
Dr. Moliner, 50, 46100 Burjassot, València, Spain
e-mail: Vicente.Perez-Calabuig@uv.es