A polynomial-time algorithm for the Jacobson form for matrices of differential operators

Johannes Middeke

Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Linz, Austria.

Abstract

We consider a ring $R = K[\partial; \mathrm{id}, \vartheta]$ of differential operators over a differential field (K, ϑ). This is a (left and right) principal ideal domain. Hence, if R is simple, then for every matrix $M \in {}^nR^n$ there exist unimodular matrices S and $T \in {}^nR^n$ and $f \in R$ such that $SMT = \mathrm{diag}(1, \ldots, 1, f, 0, \ldots, 0)$. The proof of the existence goes back to Jacobson, Nakayama and Teichmüller. Therefore, this strong diagonal form is known as Jacobson form in Zerz (2007, Theorem 3.2) or Teichmüller-Nakayama normal form in Ilchmann and Mehrmann (2005, Theorem 2.1).

In this paper, we present a polynomial time algorithm for computing a strong diagonal form (which we will later call Jacobson form) in the case where M has R-linearly independent rows. The method exploits the well-known existence of cyclic vectors for the module R^n/R^nM, and is applicable for all fields with "enough" constants and a "sufficiently" high degree over their constant field. We will achieve the form $\mathrm{diag}(1, \ldots, 1, f)$ even for non-simple R.

Key words: Jacobson form, Strong diagonal form, Differential operators, Skew polynomials, Differential module
1991 MSC: Primary 16S36, 15A21, secondary 15A33

1. Introduction

The existence of strong diagonal forms (which will later be called Jacobson form) for matrices over rings goes back to Henry John Steven Smith who studied it for the integers. Therefore, over the integers the Jacobson form usually bears his name, the *Smith form*.

⋆ This work was supported by the Austrian Science Foundation (FWF) under the project DIFFOP (P20 336–N18).

Email address: jmiddeke@risc.uni-linz.ac.at (Johannes Middeke).

Later on, generalisations for other kinds of rings were explored by Nathan Jacobson and Oswald Teichmüller. A statement about the uniqueness (up to similarity) was given by Tadashi Nakayama. For further historical remarks we refer the reader to Cohn (1985, Notes and comments for chapter 8).

The first use of the the two-sided diagonal normal form over a skew polynomial ring in the context of control theory appeared already 1984 in Ilchmann et al. (1984, Prop. 2.13). The use in control theory is one of the important motivations for the development of algorithms for skew polynomial matrix normal forms, see, e. g., Zerz (2007) and Ilchmann and Mehrmann (2005). There, for example, the Jacobson form may be used to prove the existence of full row rank representations of systems and and for their computation (see, e. g., Zerz (2006, Section 5.1)).

Other applications are solving systems of differential equations. See, e. g., Culianez and Quadrat (2005) for various worked out examples.

While other (one-sided) normal forms over certain skew-polynomial rings can in the meanwhile be computed with the help of implementations in computer algebra packages, it seems that an efficient implementation for the Jacobson form does not yet exist. The implementations known to the author are based on the classical algorithm (see section 4 for the algorithm and, e. g., Culianez and Quadrat (2005) for an implementation).

In this paper we will thus consider the following task: Let R be a ring of differential operators (see section 2). Given $M \in {}^nR^n$ with R-linearly independent rows, our goal is to compute in polynomial time unimodular matrices $S, T \in ({}^nR^n)^*$, i. e., matrices possessing a both-sided inverse, such that

$$SMT = \operatorname{diag}(1, \ldots, 1, f)$$

for some non-zero $f \in R$.

This is a special case of the Jacobson form which may also be defined for non-square matrices and matrices without independent rows. It is interesting, however, that—in contrast to the general definition of the Jacobson form—for the matrices considered in this paper the form $\operatorname{diag}(1, \ldots, 1, f)$ may be reached even if R is not simple.

2. Preliminaries

Let (K, ϑ) be a differential field. I. e., K is a (commutative) field and ϑ is a *derivative* on K, that is, an additive map that additionally satisfies the Leibniz rule $\vartheta(ab) = \vartheta(a)b + a\vartheta(b)$. In this paper we will assume that ϑ is not the zero map. Following the notation of Cohn (1985) we define the *ring of differential operators* over K in ϑ as $R = K[\partial; \mathrm{id}, \vartheta]$. [1] That means, as a set R consists of all polynomial expression in the variable ∂ with coefficients in K, where we write the powers of ∂ on the right. Addition is just like for the usual polynomials, but multiplication is given by the *commutation rule* $\partial a = a\partial + \vartheta(a)$ for all $a \in K$. Expanding this rule by associativity and distributivity R becomes a non-commutative ring. For details of the construction and a proof of the existence we refer to Cohn (1985, Chapter 0.10).

[1] In Cohn (1985) a more general case is considered where instead of the identity function id any endomorphism is allowed (imposing restrictions on ϑ, though).

Rings of the type of R are also known as *skew polynomial ring* or *Ore polynomial rings* (after Øystein Ore who did the first studies on such domains). A prominent example is the ring $\mathbb{Q}(x)[\partial; \mathrm{id}, d/dx]$ where the coefficient field are the rational functions $\mathbb{Q}(x)$ in x and the derivative is just the standard derivative w. r. t. x. Note, however, that in this paper we do not restrict ourselves to fields of characteristic zero.

For $f = a_n\partial^n + \ldots + a_1\partial + a_0 \in R \setminus \{0\}$ we define the *order* of f to be $\operatorname{ord} f = n$ unless $a_n = 0$. For $f = 0$ we use the convention $\operatorname{ord} 0 = -\infty$. The order has the properties of the usual (commutative) polynomial degree, i. e., we have $\operatorname{ord}(f+g) \leq \max\{\operatorname{ord} f, \operatorname{ord} g\}$ and $\operatorname{ord}(fg) = \operatorname{ord} f + \operatorname{ord} g$ for all $f, g \in R$. It is well-known (see, e. g., Bronstein and Petkovšek (1996, Chapter 3)) that with this degree function R becomes a left and right Euclidean domain.

As in the commutative case, we may also define the leading coefficient of a differential operator $f = a_n\partial^n + \ldots + a_1\partial + a_0 \in R \setminus \{0\}$ to be $\operatorname{lcoeff}(f) = a_n$ if $a_n \neq 0$. Again we have the familiar rule $\operatorname{lcoeff}(fg) = \operatorname{lcoeff}(f) \cdot \operatorname{lcoeff}(g)$ for all $f, g \in R \setminus \{0\}$ as can be seen easily from the commutation rule.

We write ${}^mR^n$ for the set of $m \times n$ matrices with entries in R, R^n for row vectors of length n and ${}^mR$ for column vectors of length m.

Our subject will be square matrices with entries in R. Let $n \geq 1$ and $M \in {}^nR^n$. If we multiply M by row vectors $v \in R^n$ from the left, the set of all these multiples will form a left R-submodule of the left R-module of all row vectors. We will consider the factor module $\mathfrak{M} = R^n/R^nM$. This is again a left R-module and hence a K-vector space. Our algorithm deals with the case that $\dim_K \mathfrak{M} = m < \infty$. It is not hard to show that this condition is equivalent to the R-linearly independence of the rows of M: Since R is left and right Euclidean we may use elementary row and column operations to convert M into a diagonal matrix $D = \operatorname{diag}(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in R$. Since $\mathfrak{M} \cong R^n/R^nD \cong \bigoplus_{j=1}^n R/Ra_j$, we see that $\mathfrak{M}$ has finite K-dimension if and only if $a_j \neq 0$ for $j = 1, \ldots, n$, if and only if the rows of M are R-linearly independent.

3. The structure of $\mathfrak{M}$

The most important tool for our algorithm will be cyclic vectors. An element $v \in \mathfrak{M}$ is called *cyclic* if its (left) R-multiples generate $\mathfrak{M}$, i. e., if $Rv = \mathfrak{M}$. This is equivalent to saying that $v, \partial v, \partial^2 v, \ldots, \partial^{m-1} v$ is a K-basis of $\mathfrak{M}$. A nice proof of the existence and a short historical overview may be found in Churchill and Kovacic (2002). In fact, their proof is constructive and allows us to derive an algorithm for computing cyclic vectors of a special form, that will be needed in order to compute the Jacobson form. The restrictions on the field for our algorithm comes solely from the restrictions on this algorithm for computing cyclic vectors.

The algorithm is based on the following theorem which we adapt slightly to our notation. With $\operatorname{Const}(K) = \{a \in K \mid \vartheta(a) = 0\}$ we denote the subfield of constants.

Theorem 1 (Churchill and Kovacic (2002, Theorem 3.8))**.** *Suppose* $[K : \operatorname{Const}(K)] \geq m = \dim_K \mathfrak{M}$ *and* $|\operatorname{Const}(K)| \geq m + 1$. *Choose* $S \subseteq K$ *and* $S_0 \subseteq \operatorname{Const}(K) \setminus \{0\}$ *such that* $|S| = m = |S_0|$ *and the elements of* S *are linearly independent over* $\operatorname{Const}(K)$. *Let* $v \in \mathfrak{M}$. *If there exists* $u \in \mathfrak{M} \setminus Rv$, *then there exist* $\lambda \in S$ *and* $\lambda_0 \in S_0$ *such that*

$$\dim_K Rv < \dim_K R(v + \lambda\lambda_0 u).$$

We remark, that the choices of S and S_0 in the theorem are independent of $\mathfrak{M}$. That means fixed sets S and S_0 might be used for any $M \in {}^nR^n$.

From theorem 1 one derives easily an algorithm for the computation of cyclic vectors. We state a condensed version and refer the reader to Churchill and Kovacic (2002, Algorithm 4.1) for a more detailed one.

Algorithm 1 (Churchill and Kovacic (2002))**.** Let (K, ϑ) be as in theorem 1, and choose S and S_0 accordingly.
Input A matrix $M \in {}^nR^n$ with R-linear independent rows and $\dim_K R^n/R^nM = m$.
Output A cyclic vector v for $\mathfrak{M} = R^n/R^nM$.

Step 1 Choose $v \in \mathfrak{M}$ at random.
Step 2 If $\dim_K Rv = m$ then return v.
Step 3 Else choose any $u \in \mathfrak{M} \setminus Rv$ and find $\lambda \in S$ and $\lambda_0 \in S_0$ such that $\dim_K Rv < \dim_K R(v + \lambda\lambda_0 u)$.
This can be done by just trying all (finitely many) elements in S and S_0.
Step 4 Set $v \leftarrow v + \lambda\lambda_0 u$ and go to step Step 2.

The algorithm terminates since the dimension of subspace spanned by v is strictly increasing in every iteration. In Churchill and Kovacic (2002, Section 4) an analysis of the (more detailed) algorithm shows that it uses at most $\mathscr{O}(n^5)$ multiplications and divisions in K.

For the application of the algorithm in this paper the statement that u in the theorem can be chosen arbitrarily in $\mathfrak{M} \setminus Rv$ is important. For the computation of the Jacobson form we will need cyclic vectors that have representatives in K^n. These can be computed by starting with the residue class of the first unit vector $\overline{\mathfrak{e}_1} \in R^n$ modulo R^nM, by which we mean that vector in R^n with 1 in the first position and 0 in all other positions. Especially, we have $v = \mathfrak{e}_1 \in K^n \subseteq R^n$. If it is not cyclic, we choose as u the class of another unit vector. Since $S, S_0 \subseteq K$ also the class of $v + \lambda\lambda_0 u$ has a representative in K^n for any choice of $\lambda \in S$ and $\lambda_0 \in S_0$.

It remains to discuss whether we are always able to find a class of a unit vector in $\mathfrak{M} \setminus Rv$. Suppose the classes of all unit vectors are already included in Rv, i. e., for $j = 1, \ldots, n$ there exists $g_j \in R$ such that $\overline{\mathfrak{e}_j} = g_j v$. Let $w = [b_1, \ldots, b_n] \in R^n$ be arbitrary. We have for the class $\overline{w}$ of w

$$\overline{w} = \sum_{j=1}^{n} b_j \overline{\mathfrak{e}_j} = \Big(\sum_{j=1}^{n} b_j g_j \Big)\, v,$$

and hence $Rv = \mathfrak{M}$. By contraposition we get that for $Rv \neq \mathfrak{M}$ there must exists $1 \leq k \leq n$ s. t. $\overline{\mathfrak{e}_k} \notin \mathfrak{M}$.

We state this observation as a lemma:

Lemma 2. *In the situation of theorem 1 we can always compute a cyclic vector that has a representative in $K^n \subseteq R^n$.*

An important tool to make the computations of the cyclic vector algorithm easier are so called defining matrices which we will discuss now. They allow us to tread the

computations entirely in $K^m \cong \mathfrak{M}$. Again, this results are well-known and may for example also be found in Churchill and Kovacic (2002). We repeat them here just for convenience of the reader and in order to introduce some notation.

For $m = \dim_K \mathfrak{M}$ we have $\mathfrak{M} \cong K^m$ as K-vector spaces. We want to carry over the R-module structure to the right hand side. Choose a basis $\mathfrak{F} = (u_1, \ldots, u_m)$ in $\mathfrak{M}$. Using the ∂-action on the basis elements we get

$$\partial u_i = \sum a_{ij} u_j$$

for some $a_{ij} \in K$ where $i, j = 1, \ldots, m$. For $w \in \mathfrak{M}$, we now denote the coordinate vector w. r. t. $\mathfrak{F}$ as $w_{\mathfrak{F}}$. If we define the matrix $A = (a_{ij})_{i,j=1}^m$ an easy computation using the commutation rule verifies that for arbitrary $w \in \mathfrak{M}$

$$(\partial w)_{\mathfrak{F}} = \vartheta(w_{\mathfrak{F}}) + w_{\mathfrak{F}} A$$

where ϑ is applied to $w_{\mathfrak{F}}$ entry-wise.

Now, if we define the ∂-action on K^m to be $w \mapsto \vartheta(w) + wA$ the vector space K^m becomes an R-module, and the coordinate map $w \mapsto w_{\mathfrak{F}}$ becomes an R-isomorphism. The matrix A is called the *defining* $\mathfrak{F}$*-matrix*. Once a basis is chosen and the defining matrix is computed, we may thus execute all operations in $\mathfrak{M}$ by using usual linear algebra.

It is interesting to consider, how defining matrices behave during a change of bases. Let $\mathfrak{F}$ and $\mathfrak{G}$ be two bases, P be the matrix of change from $\mathfrak{G}$ to $\mathfrak{F}$, A be the defining $\mathfrak{F}$-matrix and B the defining $\mathfrak{G}$-matrix. A short computation shows

$$B = \left(\vartheta(P) + PA\right) P^{-1},$$

where application of ϑ is again componentwise. This kind of transformation is called a *gauge transformation* in Churchill and Kovacic (2002).

Thus, even change of basis does not require us to go back to $\mathfrak{M}$ for the computation of the new defining matrix.

4. The Jacobson form

As usual we call two matrices $M, N \in {}^nR^n$ *equivalent* if there exists two unimodular matrices $S, T \in ({}^nR^n)^*$ such that $SMT = N$. Our goal is it to compute for every matrix a special representative or *normal form* w. r. t. equivalence, the so called Jacobson form.

We give the definition of the Jacobson form only for simple rings. The definition for general rings is more complicated. But interestingly enough, we will for matrices with R-linearly independent rows always be able to compute this simpler form below.

Definition 3 (Jacobson form for simple rings)**.** A matrix $M \in {}^nR^n$ where R is simple is said to be in *Jacobson form*, if

$$M = \operatorname{diag}(1, \ldots, 1, f, 0, \ldots, 0)$$

where $f \in R$.

It is well-known that this is indeed a normal form w. r. t. equivalence. A proof (and some historical remarks as well as statements about the uniqueness) may be found in Cohn (1985, Chapter 8). There, elementary row and column operations are used to

reduce a given matrix M first to a matrix of the form $\operatorname{diag}(a_1, \tilde{M})$ where $a_1 \in R$ and $\tilde{M} \in {}^{n-1}R^{n-1}$. Then induction is used to get a (weak) diagonal form $\operatorname{diag}(a_1, \ldots, a_n)$ with $a_1, \ldots, a_n \in R$. This is completely constructive, although the complexity appears to be exponential w. r. t. operations in the ground field K, since the reduction of one position may blow up the orders of the entries in other positions.

The problem is that the column (row) operation on the first column (row) also effect the other entries. Their shape is not known and therefore might every column (row) operation increase the orders. The calculation here runs as follows: One can show, that applying the Euclidean algorithm to a vector of size n with maximal entry order k produces a transformation matrix with maximal entry order less or equal to k^2.

In the diagonalisation procedure we apply Euclid to the first row and column until the order stabilises. Since we may reorder the matrix, this normalisation is needed at most ℓ times where ℓ is the minimal entry order in M. But since an element of maximal order might appear in the first row, the transformation matrices from the Euclidean algorithm have—in the worst case—the orders

$$k^2, (\ell - 1)^2, (\ell - 2)^2, \ldots, 0.$$

That means by application of the transformation matrices to M in the remaining entries the order can grow to $k + k^2 + (\ell - 1)^2 + \ldots + 0 = \mathscr{O}(\ell^4 + k^2)$. In the worst case, all entries are of the order k and hence they may grow to order $\mathscr{O}(k^4)$. In the next iteration the order is bounded by $\mathscr{O}((k^4)^4)$ and in the n^{th} iteration this becomes $\mathscr{O}(k^{4^n})$.

Now this considerations are really worst case and very pessimistic, but still it shows, that the classial algorithm might not be very efficient.

When the matrix is in (weak) diagonal form, one has to apply further computations on each consecutive pair of diagonal entries to get the desired Jacobson form. Let w. l. o. g. $M = \operatorname{diag}(a_1, a_2)$ where $a_1, a_2 \in R \setminus \{0\}$. Cohn's approach (as given in the proof of Cohn (1985, Theorem 8.1.1)) for further reduction is to transform

$$\begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} = \begin{bmatrix} a_1 & da_2 \\ 0 & a_2 \end{bmatrix}$$

where $d \in R$ is chosen in a way that a_1 is not a left factor of a_2. Then, we can again reduce the result to a (weak) diagonal form where the order of a_1 strictly decreases. If no such d may be found, then one can argue—at least in the case where R is simple—, that a_1 is already a unit.

A problem remains to find such a d or to prove the non existence. The latter is easy since—in the simple case—this happens precisely when a_1 is a unit. The first problem is harder, but for ground fields of characteristic zero, one may use a result by Adjamagbo in order to determine a suitable d.

Lemma 4 (Adjamagbo (1988, Lemme 6))**.** *Let $f, g \in R \setminus K$ and let $c \in K$ such that $pc - cp \neq 0$ for all $p \in R \setminus K$. Then there exists $0 \leq k \leq \max\{\operatorname{ord} g - \operatorname{ord} f + 1, 0\}$ such that f is not a right divisor of $c^{-k} g c^k$. An analogous statement holds for left division.*

If $\operatorname{char} K = 0$, then any c with $\vartheta(c) \neq 0$ will fulfil the condition $pc - cp \neq 0$ for all $p \in R \setminus K$.

Proof. We prove only the case of right division. It is an immediate consequence of the commutation rule that $\operatorname{ord}(gc - cg) \leq \operatorname{ord} g - 1$. We use this fact to do an induction over the difference of the orders of f and g. If $\operatorname{ord} f > \operatorname{ord} g$ then the statement holds for $k = 0$. Let $\operatorname{ord} g - \operatorname{ord} f = n \geq 0$ and suppose the claim holds for $gc - cg \neq 0$, i. e., suppose for $0 \leq k \leq \operatorname{ord}(gc - cg) - \operatorname{ord} f + 1$ or for $k = 0$ that f is not a right divisor of $c^{-k}(gc - cg)c^k$. Now, if $c^{-k}gc^k = af$ and $c^{-k-1}gc^{k+1} = bf$ for $a, b \in R$ then

$$c^{1-k}gc^k = caf \qquad \text{and} \qquad c^{-k}gc^{k+1} = cbf$$

which implies

$$c^{-k}(gc - cg)c^k = c^{-k}gc^{k+1} - c^{1-k}gc^k = c(b - a)f$$

contradicting our assumption. Since $\operatorname{ord}(gc - cg) < \operatorname{ord} g$ we also have $k, k + 1 \leq \operatorname{ord} g - \operatorname{ord} f + 1$.

If $\operatorname{char} K = 0$ and $\vartheta(c) \neq 0$, we may consider the K-linear map $\alpha = h \mapsto c^{-1}hc$. We have for all $k \geq 0$

$$\alpha(\partial^k) = c^{-1}\partial^k c = \partial^k + kc^{-1}\vartheta(c)\partial^{k-1} + \text{lower order terms.}$$

Hence, if we restrict α to $R_{\leq n} = \{h \in R \mid \operatorname{ord} h \leq n\}$ where $n \geq \operatorname{ord} g$ then letting $y = c^{-1}\vartheta(c) \neq 0$, the matrix for $\alpha|R_{\leq n}$ w. r. t. the K-basis $\partial^n, \ldots, \partial, 1$ is

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ ny & 1 & \ddots & \vdots \\ * & (n-1)y & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \cdots & * & y & 1 \end{bmatrix}$$

which has only 1 as eigenvalue and $K \cdot 1$ as only eigenspace, since $kc^{-1}\vartheta(c) \neq 0$ for all $k \geq 1$. Hence for non constant $p \in R$ we will always have $pc - cp \neq 0$. □

The bound on k in the lemma is not found in Adjamagbo's original paper. But it is important here in order to make the computation finite: In the above problem, we just need to test divide the elements $a_2, c^{-1}a_2c^1, \ldots c^{-\ell}a_2c^\ell$ for $\ell = \operatorname{ord} a_2 - \operatorname{ord} a_1 + 1$ by a_1; and by the lemma must find a non divisible element in that way.

We remark, that this lemma does not hold for arbitrary characteristic. Consider for example the differential field $(\mathbb{F}_2(x), d/dx)$ where d/dx is the usual derivative w. r. t. x. Let $f = g = \partial^2 + 1 \in R = \mathbb{F}_2(x)[\partial; \mathrm{id}, d/dx]$. We have $(d/dx)x = 1 \neq 0$, but

$$gx = (\partial^2 + 1) \cdot x = x\partial^2 + 2\partial + x \equiv x\partial^2 + x = xg \pmod 2.$$

Thus, obviously, f is a right divisor of $x^{-k}gx^k$ for every $k \geq 0$. In fact, for all $p \in \mathbb{F}_2(x)$ we have always $gp = p\partial^2 + 2(dp/dx)\partial + (d^2p/dx^2) + p \equiv pg \pmod 2$). [2] This additionally proves that $\mathbb{F}_2(x)[\partial; \mathrm{id}, d/dx]$ is not simple, since g commutes with ∂, too.

On the other hand, the additional statement of the lemma that for $\operatorname{char} K = 0$ every $c \notin \operatorname{Const}(K)$ will satisfy $pc - cp \neq 0$ and $\operatorname{ord}(pc - cp) < \operatorname{ord} p$ for all $p \in R \setminus K$, can be used to prove that for $\operatorname{char} K = 0$ and $\vartheta \neq 0$ the ring R must be simple.

[2] If we derive a polynomial $p \in \mathbb{F}_2[x]$ once then all even powers of x vanish and all odd powers become even. So d^2p/dx^2 becomes 0. Using the quotient rule this expands to $\mathbb{F}_2(x)$ as well.

5. Main result

We now state the main result whose proof will take the remainder of this section.

Theorem 5. *Let (K,ϑ) be a differential field. Let $R = K[\partial;\mathrm{id},\vartheta]$ and let $M \in {}^nR^n$ where $n \geq 1$ such that $\dim_K(R^n/R^nM) = m < \infty$. Assume $[K : \mathrm{Const}(K)] \geq m$ and $|\mathrm{Const}(K)| \geq m+1$. Then we can compute unimodular matrices $S,T \in ({}^nR^n)^*$ such that*

$$SMT = \mathrm{diag}(1,\ldots,1,f)$$

for some $f \in R$ using at most $\mathcal{O}(n^3m^6k^3)$ operations in K where k is the maximum order of all entries in M.

Note, that the conditions already imply $\vartheta \neq 0$, if $m > 0$. The case $m = 0$ (and also the case $n = 1$) is trivial. Therefore, we will below consider only $m \geq 1$.

Letting again $\mathfrak{M} = R^n/R^nM$ we first choose a K-basis $\mathfrak{F} = (u_1,\ldots,u_m)$ and compute the defining $\mathfrak{F}$-matrix A. Let $\varkappa$ be the coordinate map from $\mathfrak{M}$ to K^m w. r. t. $\mathfrak{F}$. Let v be a cyclic vector of K^m which has a representative in K^n, say $v = \varkappa(\overline{[v_1,\ldots,v_n]})$ where $v_1,\ldots,v_n \in K$. The computation of such a v has been discussed in section 3. Let $\mathfrak{G} = (v,\partial v,\ldots,\partial^{m-1}v)$ be the cyclic basis, and let P be the matrix of change from $\mathfrak{G}$ to $\mathfrak{F}$.

Since $\partial\cdot\partial^k v = \partial^{k+1}v$ for $k \leq m-2$ the defining $\mathfrak{G}$-matrix must have the shape

$$B = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \\ p_0 & \cdots & \cdots & \cdots & p_{m-1} \end{bmatrix}$$

for some $p_0,\ldots,p_{m-1} \in K$. Remember, that B may be computed from A and P by the formula $B = (\vartheta(P)+PA)P^{-1}$. We now set $f = \partial^m - \sum_{j=0}^{m-1} p_j\partial^j \in R$. Then an R-isomorphism ψ between K^m (using the basis $\mathfrak{G}$ and the defining matrix B) to R/Rf is given by mapping $\partial^k v$ to the residue class of ∂^k modulo f: Since $\overline{1},\overline{\partial},\ldots,\overline{\partial^{m-1}}$ is a K-basis of R/Rf—which holds because the orders are lower than the order of f—this is certainly a K-isomorphism. Further, for $k \leq m-2$ we have

$$\partial\cdot\partial^k v = \partial^{k+1}v \quad \mapsto \quad \overline{\partial^{k+1}} = \partial\cdot\overline{\partial^k}$$

and

$$\partial\cdot\partial^{m-1}v = \sum_{j=0}^{m-1} p_j\partial^j v \quad \mapsto \quad \overline{\textstyle\sum_{j=0}^{m-1} p_j\partial^j} = \overline{\partial^m} = \partial\cdot\overline{\partial^{m-1}}.$$

This f will already be the one from the theorem. It remains to construct the matrices S and $T \in ({}^nR^n)^*$ in order to show that $N = \mathrm{diag}(1,\ldots,1,f) \in {}^nR^n$ is really equivalent to M.

If we combine ψ with the map ω of change from $\mathfrak{F}$ to $\mathfrak{G}$ and the coordinate map $\varkappa$ from $\mathfrak{M}$ to K^m w. r. t. $\mathfrak{F}$ we obtain an R-isomorphism φ from $\mathfrak{M}$ to R/Rf making the

following diagram commutative:

$$\begin{array}{ccc} \mathfrak{M} = \frac{R^n}{R^n M} & \xrightarrow{\quad\varphi\quad} & \frac{R}{Rf} \\ \downarrow{\scriptstyle \varkappa} & & \uparrow{\scriptstyle \psi} \\ K^m & \xrightarrow{\quad\omega\quad} & K^m \end{array} .$$

Of course, ω is given simply by $w \mapsto wP^{-1}$.

We now study φ in more detail. Let $\mathfrak{e}_j \in R^n$ for $j = 1, \ldots, n$ be again the j^{th} unit vector, and let $g_j \in R$ be such that $\varphi(\overline{\mathfrak{e}_j}) = \overline{g_j}$. Let $w = [w_1, \ldots, w_n] \in R^n$ be arbitrary. Then

$$\varphi(\overline{w}) = \sum_{j=1}^{n} w_j \varphi(\mathfrak{e}_j) = \sum_{j=1}^{n} w_j \overline{g_j} = \overline{\textstyle\sum_{j=1}^{n} w_j g_j} = \overline{wg},$$

where $g = [g_1, \ldots, g_n]^t \in {}^nR$.[3]

We may assume w. l. o. g. that $\operatorname{ord} g_j < m = \operatorname{ord} f$ for $j = 1, \ldots, n$. (In fact, φ will already provide such g_j as can be seen from the definition of ψ). We claim that in this case the elements $g_1, \ldots, g_n$ will be relatively right coprime. The proof of this is simply the application of φ to the (preimage of the) cyclic vector v: We have

$$\varphi(\overline{[v_1, \ldots, v_n]}) = \psi(\omega(v)) = \psi(e_1) = \overline{1},$$

where e_1 is the first unit vector in K^m, and

$$\varphi(\overline{[v_1, \ldots, v_n]}) = \overline{\textstyle\sum_{j=1}^{n} v_j g_j}.$$

This implies that

$$1 - \sum_{j=1}^{n} v_j g_j = pf$$

for some $p \in R$. But since the orders of $g_1, \ldots, g_n$ are strictly smaller that the order of f and $v_1, \ldots, v_n \in K$ have order 0, comparing the order of both sides reveals $p = 0$ and hence

$$1 = \sum_{j=1}^{n} v_j g_j$$

in R, which proves the right coprimeness we claimed.

Since the entries of g are relatively right coprime, using the Euclidean algorithm we can compute an unimodular matrix $T = [D \mid g] \in ({}^nR^n)^*$ having g as its last column. This will play the rôle of the T from the theorem, leaving us with the need to provide a suitable S.

But first we need to convince ourselves that $Mg \in {}^nR$: Application of φ to the residue class of the j^{th} row $M_{j\bullet}$ of M yields

$$\overline{M_{j\bullet} g} = \varphi(\overline{M_{j\bullet}}) = \varphi(\overline{0}) = \overline{0}.$$

Because of that fact we see that $MT = M[D \mid g] = [MD \mid qf]$ for some $q \in {}^nR$. Let $\lambda f = \operatorname{gcrd}(qf)$, by which we mean the greatest common right divisor of the entries

[3] For $C \in {}^kR^\ell$, with C^t we denote the (formal) transpose of the matrix C. Note, however, that because of the non-commutativity of our rings the transpose is not R-linear.

of qf. Again using Euclid there exists an unimodular matrix $Q \in {}^nR^n)^*$ such that $Q \cdot qf = \lambda f \cdot \mathfrak{e}_n^t$. Thus,

$$QMT = \left[\begin{array}{c|c} QMD & \begin{array}{c} 0 \\ \vdots \\ 0 \\ \lambda f \end{array} \end{array}\right].$$

Our next goal is to show that λ must be a unit.

Since Q and T are unimodular the homomorphism theorem for modules yields

$$\mathfrak{M} = \frac{R^n}{R^n M} \cong \frac{R^n}{R^n(QMT)}.$$

The K-dimension of the left hand side is m and hence also $\dim_K R^n/R^n(QMT) = m$. We consider now the subspace $R\overline{\mathfrak{e}_n} \subseteq R^n/R^n(QMT)$. For any $h \in R$ the equation $h\overline{\mathfrak{e}_n} = \overline{h\mathfrak{e}_n} = 0$ implies $h\mathfrak{e}_n = w(QMT)$ for some $w \in R^n$. Comparing the last entries, we see that $h = w_n \lambda f$. Hence $h\overline{\mathfrak{e}_n} = 0$ implies $h \in R\,\lambda f$.

Since as a subspace $R\overline{\mathfrak{e}_n}$ has at most K-dimension m, there must exist a $h \in R \setminus \{0\}$ with $\operatorname{ord} h \leq m$ and $h\overline{\mathfrak{e}_n} = 0$. That means, that there exists such an h in $R\lambda f$. But since $\operatorname{ord} f = m$ this is only possible, if $\operatorname{ord} \lambda = 0$, i. e., if λ is a unit.

We will now w. l. o. g. assume that $\lambda = 1$. Since all elements of $Rf \setminus \{0\}$ have at least order m we see that $\dim_K R\overline{\mathfrak{e}_n}$ must be exactly m and hence already

$$R\overline{\mathfrak{e}_n} = \frac{R^n}{R^n(QMT)}.$$

But that means that for $j = 1, \ldots, m-1$ also the classes $\overline{\mathfrak{e}_j}$ must be members of $R\overline{\mathfrak{e}_n}$. Thus we get $\mathfrak{e}_j - p\mathfrak{e}_n = w(QMT)$ for suitable $p \in R$ with $\operatorname{ord} p \leq m-1$ and $w \in R^n$.

Again comparing the last entries (and their orders) we find that p and hence also w_n must be zero. Hence $\mathfrak{e}_j$ for $j = 1, \ldots, m-1$ is already in the span of the first $m-1$ rows of QMT. Let $U \in {}^{n-1}R^{n-1}$ be the matrix consisting of all entries of QMT except for the last column and the last row. Since linear combinations of the rows of U yield the unit vectors (in R^{n-1}), there exists a matrix $Z \in {}^{n-1}R^{n-1}$ such that $ZU = \mathrm{E}_{n-1}$ where E_{n-1} is the $(n-1) \times (n-1)$ identity matrix. Since Z has an right inverse and R is Euclidean, Z is already unimodular. The proof is as follows: There exists $t_1, \ldots, t_n \in R^{n-1}$ s. t. $Zt_j = \mathfrak{e}_j$ for $j = 1, \ldots, n$. Hence the entries of the first row of Z are relatively left coprime and via Euclid one computes a matrix C such that

$$ZC = \left[\begin{array}{c} \mathfrak{e}_1 \\ \hline \hat{Z} \end{array}\right].$$

(Note that C as given by the Euclidean algorithm is a product of elementary matrices). Using elementary operations D we arrive at $DZC = \operatorname{diag}(1, \tilde{Z})$. From here, we use induction on $\tilde{Z}$ which is possible, since for all j

$$(DZC)\,(C^{-1} \sum_{k=1}^{n} t_k (D^{-1})_{kj}) = \mathfrak{e}_j.$$

This computation shows $\mathrm{E}_n = FZG$ for elementary matrices F and G and hence $Z = F^{-1}G^{-1}$ is a product of elementary matrices, too.

The fact that Z is unimodular means that the transformation

$$\operatorname{diag}(Z,1)(QMT) = \left[\begin{array}{c|c} \mathrm{E}_{n-1} & \begin{matrix}0\\ \vdots\\ 0\end{matrix} \\ \hline * \cdots * & f \end{array}\right]$$

is admissible where $\operatorname{diag}(Z,1)$ is unimodular, too. Hence, using elementary row operations Y, we finally have

$$\underbrace{Y\operatorname{diag}(Z,1)Q}_{=S}\ M\ T = \operatorname{diag}(1,\ldots,1,f) = N,$$

where S is a product of unimodular matrices and thus itself unimodular.

By now we have proved the existence claim of theorem 5. The complexity will be discussed in the next section, after we stated the entire algorithm.

6. The algorithm and its complexity

In the proof S is computed in a slightly complicated way, but that may be done easier:[4] Since N is not a zero divisor in ${}^nR^n$ by cancellation applied to $MT = S^{-1}N$ we get

$$S = (MT/N)^{-1}.$$

Inversion of a matrix can be done quite fast using a technique similar to minimal basis computation for usual polynomials (cf. G. David Forney (1975)). For $k = 1,\ldots,n$ and $Q = (q_{ij})_{i,j=1}^n \in {}^nR^n$ we define the k^{th} *index* of Q as $\operatorname{ind}_k Q = \max\{\operatorname{ord} q_{kj} \mid 1 \le j \le n\}$ and the *leading coefficient matrix* of Q as

$$\mathrm{LC}(Q) = \Big(\ \operatorname{coeff}_{\operatorname{ind}_i Q}(q_{ij})\ \Big)_{i,j=1}^n \in {}^nK^n,$$

where $\operatorname{coeff}_j(p)$ selects the coefficient of ∂^j from $p \in R$. Following G. David Forney (1975), we call a matrix *row-reduced* if $\mathrm{LC}(Q)$ has full rank. (This concept is also named *row-proper*, see, e. g., Zerz (2007, Section 2.2)).

If Q is not row-reduced then we can find $\alpha \in K^n \setminus \{0\}$ such that $\alpha\,\mathrm{LC}(Q) = 0$. Let now, w. l. o. g., $\alpha_1 \neq 0$ and $\operatorname{ind}_1 Q = \nu$ be maximal within all $\operatorname{ind}_j Q$ where $\alpha_j \neq 0$. Set $\nu_j = \max\{\nu - \operatorname{ind}_j Q, 0\}$ for $j = 2,\ldots,n$ and let $\hat\alpha = [\alpha_1, \alpha_2\partial^{\nu_2}, \ldots, \alpha_n\partial^{\nu_n}]$. Then $\hat\alpha Q$ has entries with order at most $\operatorname{ind}_1 Q - 1$. Since $\hat\alpha_1 = \alpha_1 \neq 0$ the matrix

$$A = \left[\begin{array}{c|c} \hat\alpha & \\ \hline \begin{matrix}0\\ \vdots\\ 0\end{matrix} & \mathrm{E}_{n-1} \end{array}\right]$$

is invertible and $\sum_{j=1}^n \operatorname{ind}_j AQ$ is strictly lower than $\sum_{j=1}^n \operatorname{ind}_j Q$. Of course, if Q is unimodular, so is AQ.

If we can prove that a unimodular matrix is never row-reduced unless it is in ${}^nK^n$, then the above reduction yields an algorithm for computing inverses: Reduce the sum of

[4] Although the complexity stays pretty much the same.

the indices (in G. David Forney (1975) also known as the *order* of Q—but that conflicts with our notation here) using matrices like above until one obtains a matrix in ${}^nK^n$ which can then be inverted using linear algebra.

The statement that a unimodular $Q \in {}^nR^n \setminus {}^nK^n$ cannot possess a full rank leading coefficient matrix follows from the contraposition of the so called *predictable degree property* which appears in G. David Forney (1975) for the usual (commutative) polynomial case.

Lemma 6 (Predictable degree property)**.** *Let $Q \in {}^nR^n$ be such that* $\mathrm{LC}(Q)$ *has full rank. Then for any $x, y \in R^n$ the equation $y = xQ$ implies*

$$\max\{\operatorname{ord} y_j \mid 1 \le j \le n\} \;=\; \max\{\operatorname{ord} x_j + \operatorname{ind}_j Q \mid 1 \le j \le n\}.$$

Proof. The proof follows G. David Forney (1975) closely and runs as follows: We have $y = xQ = \sum_{j=1}^{n} x_j Q_{j\bullet}$ where $Q_{j\bullet}$ is the j^{th} row of Q. In this proof we use the abbreviation $\operatorname{ord} U = \max\{\operatorname{ord} u_{ij} \mid 1 \le i \le \ell, 1 \le j \le k\}$ for any matrix $U = (u_{ij})_{\substack{i=1,\dots,\ell \\ j=1,\dots,k}} \in {}^{\ell}R^k$. Then

$$\operatorname{ord}(x_j Q_{j\bullet}) = \operatorname{ord} x_j + \operatorname{ord} Q_{j\bullet} = \operatorname{ord} x_j + \operatorname{ind}_j Q$$

and hence $\operatorname{ord} y \le d = \max\{\operatorname{ord} x_j + \operatorname{ind}_j Q \mid 1 \le j \le n\}$.

We consider now the vector $\tilde{x} \in K^n$ which has as j^{th} entry, $j = 1, \dots, n$, the coefficient of order $d - \operatorname{ind}_j G$ of x_j. Since $\operatorname{ord} x_j \le d - \operatorname{ind}_j Q$ for all j, the entry $\tilde{x}_j$ is $\operatorname{lcoeff}(x_j)$ if $\operatorname{ord} x_j = d - \operatorname{ind}_j Q$ and 0 otherwise. By the definition of d the former case must occur at least once, meaning that $\tilde{x} \neq 0$. Since $\mathrm{LC}(Q)$ has full rank we have $\tilde{x}\,\mathrm{LC}(Q) \neq 0$ and hence the linear combination via x of those rows where $\operatorname{ord}(x_j Q_{j\bullet}) = d$ has order d meaning $\operatorname{ord} y = \operatorname{ord}(xQ) = d$. □

It remains to argue, why exactly the contraposition does help us here. Suppose, w. l. o. g., $\operatorname{ind}_1 Q \ge 1$. If Q is invertible then $y^{(j)}Q = \mathfrak{e}_j$ for some non-zero $y^{(j)} \in R^n$ and for all $j = 1, \dots, n$. If $y_1^{(j)} = 0$ for all j then $\tilde{Q} \in {}^nR^n$ consisting of all rows of Q but with the first one set to zero has a left inverse $Y \in {}^nR^n$ and hence also a right inverse. But from $\tilde{Q}Y = \mathrm{E}_n$ we get a contradiction since the first row must be zero here.

Hence there is one j with $y_1^{(j)} \neq 0$ and thus $0 = \operatorname{ord} \mathfrak{e}_j = \operatorname{ord} y^{(j)}Q < 1 \le \operatorname{ind}_1 Q + \operatorname{ord} y^{(j)} \le \max\{\operatorname{ord} y^{(k)} + \operatorname{ind}_k Q \mid 1 \le k \le n\}$ implying that $\mathrm{LC}(Q)$ does not have full rank.

Computing the inverse in that way, has the following complexity: The final step will be to invert a matrix in ${}^nK^n$ which needs at most $\mathcal{O}(n^3)$ field operations. Until we reach such a matrix we have to reduce the matrix according to the reduction step described above. This means, we have to solve the system $x \cdot \mathrm{LC}(Q) = 0$ which also needs $\mathcal{O}(n^3)$ operations in K. Next, we have to carry out the multiplication AQ. But since only one row of AQ differs from Q, this may be done in $\mathcal{O}(n^2 \cdot k^2)$ field operations where k is the maximal order occurring among the entries of Q.

In total, since the sum of the indices is reduced in each step, we need at most $\sum_{j=1}^{n} \operatorname{ind}_j Q \le n \cdot k$ steps. Hence the reduction takes $\mathcal{O}(nk \cdot n^2k^2) = \mathcal{O}(n^3k^3)$ operations in K.

Next, we have to more closely inspect, how to actually compute φ from the proof of theorem 5. There we defined φ as $\varphi = \psi \circ \omega \circ \varkappa$. We have to apply φ only to the residue

classes of the unit vectors $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$. Let us assume we already now $\varkappa(\overline{\mathfrak{e}_1}), \ldots, \varkappa(\overline{\mathfrak{e}_n})$ and $\varkappa(\overline{v})$. Using the defining matrix v will be computed within K^m anyways, i. e., we would directly compute $\varkappa(v)$, and the classes of the unit vectors are the first candidates for basis vectors, justifying the assumption. The matrix of change from the cyclic basis $\mathfrak{G}$ to the chosen basis $\mathfrak{F}$ from the proof will then be nothing else but

$$P = \begin{bmatrix} \varkappa(v) \\ \varkappa(\partial v) \\ \vdots \\ \varkappa(\partial^{m-1} v) \end{bmatrix}.$$

where $\varkappa(\partial^j v) = \partial^j \varkappa(v)$, $j = 1, \ldots, m-1$, can be computed using the defining matrix. Since the map ω is given by $w \mapsto wP^{-1}$, ψ can be computed using the matrix product $w \mapsto \overline{w \cdot [1, \partial, \ldots, \partial^{m-1}]}^t$. Hence

$$\varphi(\overline{w}) = \overline{\varkappa(\overline{w}) \cdot P^{-1} \cdot [1, \partial, \ldots, \partial^{m-1}]^t}$$

for all $w \in R^n$.

Using this we can state the complete algorithm:

Algorithm 2 (Main algorithm)**.**
Input A matrix $M \in {}^nR^n$ as in theorem 5.
Output Unimodular matrices $S, T \in ({}^nR^n)^*$ and a monic $f \in R \setminus \{0\}$ such that $SMT = \operatorname{diag}(1, \ldots, 1, f)$.
Step 1 Choose a basis $\mathfrak{F}$ of $\mathfrak{M} = R^n/R^nM$ and compute the defining $\mathfrak{F}$-matrix A. Let $\dim_K \mathfrak{M} = m$ and the coordinate map to $\mathfrak{F}$ be $\varkappa$.
Step 2 Use algorithm 1 to compute a cyclic vector v of $\mathfrak{M}$ with representative in K^n.
Step 3 Compute the matrix $P = [\varkappa(v)^t \mid \partial\varkappa(v)^t \mid \ldots \mid \partial^{m-1}\varkappa(v)^t]^t$ and set $B = (b_{ij})_{ij,=1}^m = (\vartheta(P) - PA)P^{-1}$.
Step 4 Set $f = \partial^m - \sum_{j=0}^{m-1} b_{m,j-1}\partial^j$.
Step 5 Compute $g_j = \varkappa(\overline{\mathfrak{e}_j}) \cdot P^{-1} \cdot [1, \partial, \ldots, \partial^{m-1}]^t$ for $j = 1, \ldots, n$.
Step 6 Use the Euclidean algorithm to compute a unimodular matrix $T \in ({}^nR^n)^*$ with last column $[g_1, \ldots, g_n]^t$.
Step 7 Compute MT and replace the entries in the last column of MT with their remainders upon right division by f yielding a matrix $\hat{S}$.
Step 8 Compute $S = \hat{S}^{-1}$.
Step 9 Return S, T and f.

We will discuss the first step in more detail below. As we have seen in section 3 the second step takes $\mathscr{O}(m^5)$ operations (multiplications and divisions) in K. The third, forth and fifth step need no more than $\mathscr{O}(m^3)$ operations. The Euclidean algorithm in the sixth step needs at most $\mathscr{O}(nm^2(nm+m^2)) = \mathscr{O}(n^2m^4)$ operations in K and produces a matrix T where the order of the entries is bounded by m^2.

Computation of MT needs at most $n^3 \cdot k(m^2+k) = \mathscr{O}(n^3m^2k^2)$ operations in K where k is the maximal order among the entries of M. The order of the entries of MT will be

at most km^2. Also division of the last row can be done in $\mathscr{O}(n \cdot (km^2 - m) \cdot km^2 \cdot m) = \mathscr{O}(nk^2m^5)$ field operations. The maximal entry order of MT/N stays km^2.

Finally $(MT/N)^{-1}$ can be computed using

$$\mathscr{O}(n^3(km^2)^3) = \mathscr{O}(n^3k^3m^6)$$

operations in K. This is the most expensive step of the algorithm and thus also the total complexity.

The first step of the algorithm is not yet detailed. It is a strait forward but tedious calculation to prove that

$${}^nR^n = {}^n(K[\partial; \mathrm{id}, \vartheta])^n \;\cong\; ({}^nK^n)[\hat{\partial}; \mathrm{id}, \hat{\vartheta}] \qquad \text{as rings,}$$

where $\hat{\partial}$ is a new variable and $\hat{\vartheta}(Q) = (\vartheta(q_{ij}))_{i,j=1}^n$ for every $Q = (q_{ij})_{i,j=1}^n \in {}^nK^n$ is a derivative. In the following, we will not distinguish between symbols with hat and those without. Although $({}^nK^n)[\partial; \mathrm{id}, \vartheta]$ is not an Euclidean domain, one can still do left and right long division as long as the leading coefficient of the divisor is an invertible matrix. Since matrix multiplication from the left works row-wise we may as dividend also take non-square matrices by using the following trick: Suppose $G \in {}^nR^n$ has an invertible leading coefficient. Let $v \in R^n$. We now can carry out the long division

$$\left[\begin{array}{c} v \\ \hline {}_{n-1}0_n \end{array}\right] = QG + Y$$

where $Q, Y \in {}^nR^n$ with $\operatorname{ord} Y < \operatorname{ord} G$ and where ${}_{n-1}0_n$ is the $n-1 \times n$ zero matrix. Now, if we just consider the first rows of Q and Y we get the following lemma:

Lemma 7 (Bézout)**.** *For all $G \in {}^nR^n$ and all $v \in R^n$ there exist $q, r \in R^n$ with $\max\{\operatorname{ord} r_i \mid 1 \le i \le n\} < \operatorname{ord} G$ such that $v = qG + r$. The remainder r is uniquely determined.*

The statement about the uniqueness comes from the fact that the remainder Y in the above computation is unique, which holds in every skew polynomial ring.

The lemma makes it easy to compute a basis for the case where the leading coefficient of M is invertible. We assume, w. l. o. g., that

$$M = \mathrm{E}_n\partial^\ell - \sum_{j=1}^{\ell-1} M^{(j)}\partial^j$$

where $M^{(j)} = (m_{ik}^{(j)})_{i,k=1}^n \in {}^nK^n$. Using Bézout's lemma we see that

$$\mathfrak{E} = (\overline{\mathfrak{e}_1}, \overline{\partial\mathfrak{e}_1}, \ldots, \overline{\partial^{\ell-1}\mathfrak{e}_1},\ \overline{\mathfrak{e}_2}, \overline{\partial\mathfrak{e}_2}, \ldots, \overline{\partial^{\ell-1}\mathfrak{e}_2},\ \ldots,\ \overline{\mathfrak{e}_n}, \overline{\partial\mathfrak{e}_n}, \ldots, \overline{\partial^{\ell-1}\mathfrak{e}_n},\ )$$

is a basis of R^n/R^nM. Furthermore, since for $i = 1, \ldots, n$ and $j = 1, \ldots, \ell-2$ we have $\partial \cdot \overline{\partial^j\mathfrak{e}_i} = \overline{\partial^{j+1}\mathfrak{e}_i}$ and

$$\partial \cdot \overline{\partial^{\ell-1}\mathfrak{e}_i} = \overline{\partial^\ell\mathfrak{e}_i} = \sum_{j=1}^{\ell-1}\sum_{k=1}^{n} m_{i,k}^{(j)}\overline{\partial^j\mathfrak{e}_k},$$

we see that the defining $\mathfrak{E}$-matrix has the shape $A = (A_{i,k})_{i,k=1}^{n\cdot\ell}$ where

$$A_{i,k} = \begin{bmatrix} 0 & \cdots & \delta_{ik} & 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & & \delta_{ik} \\ \\ m_{i,k}^{(0)} & \cdots & \cdots & \cdots & \cdots & \cdots & m_{i,k}^{(\ell-1)} \end{bmatrix} \in {}^{\ell}K^{\ell}.$$

(Here, δ_{ik} means the Kronecker symbol).

This computations shows, that in the case of M with an invertible leading coefficient the defining $\mathfrak{E}$-matrix can be "computed" by just copying the coefficients of the entries of M into the right places.

7. Example

Let $(K, \vartheta) = (\mathbb{F}_2(x, y), d/dx)$ where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and d/dx is the usual derivative with respect to x. Hence $d/dx(\mathbb{F}_2(y)) = 0$ meaning that we have infinitely many constants.

Let $R = K[\partial; \mathrm{id}, \vartheta]$ and

$$M = \underbrace{\begin{bmatrix} y^2 & 0 \\ 0 & x^2 \end{bmatrix}}_{=M^{(2)}} \partial^2 + \underbrace{\begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}}_{=M^{(1)}} \partial + \underbrace{\begin{bmatrix} 1 & 1 \\ 0 & y \end{bmatrix}}_{=M^{(0)}} \in {}^2R^2$$

Since $M^{(2)}$ is invertible, $\mathfrak{M} = R^2/R^2M$ has K-dimension 4. We convert the system to

$$\hat{M} = (M^{(2)})^{-1}M = \begin{bmatrix} \partial^2 + (1/y^2)\partial + (1/y^2) & 1/y^2 \\ (1/x)\partial & \partial^2 + (1/x^2)\partial + (y/x^2) \end{bmatrix}.$$

Now, we can read of the defining matrix for the basis $\mathfrak{E} = (\overline{\mathfrak{e}_1}, \overline{\partial\mathfrak{e}_1}, \overline{\mathfrak{e}_2}, \overline{\partial\mathfrak{e}_1}) = (e_1, e_2, e_3, e_4)$ of $R^2/R^2\hat{M}$:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1/y^2 & 1/y^2 & 1/y^2 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1/x & y/x^2 & 1/x^2 \end{bmatrix}.$$

We let $v = e_1$ (i. e., $v = \overline{\mathfrak{e}_1}$) and compute

$$P = \begin{bmatrix} v \\ \partial v \\ \partial^2 v \\ \partial^3 v \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1/y^2 & 1/y^2 & 1/y^2 & 0 \\ 1/y^4 & 1/y^2 + 1/y^4 & 1/y^4 & 1/y^2 \end{bmatrix}.$$

Since $\det P = 1/y^4$, we see that v is cyclic. The inverse of P is

$$Q = P^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & y^2 & 0 \\ 0 & 1 & 1 & y^2 \end{bmatrix},$$

and hence we have

$$B = \left(\frac{dP}{dx} + PA\right) Q = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \frac{1}{yx^2} & \frac{x+y+1}{x^2y^2} & \frac{x^2+y^3+1}{x^2y^2} & \frac{x^2+y^2}{x^2y^2} \end{bmatrix}.$$

That means, a Jacobson form of $\hat{M}$ (and also of M) is $N = \operatorname{diag}(1, 1, 1, f)$ where

$$f = \partial^4 + \frac{x^2+y^2}{x^2y^2}\partial^3 + \frac{x^2+y^3+1}{x^2y^2}\partial^2 + \frac{x+y+1}{x^2y^2}\partial + \frac{1}{yx^2}.$$

It remains to compute T and S. Since $\varkappa(\overline{\mathfrak{e}_1}) = e_1$ and $\varkappa(\overline{\mathfrak{e}_2}) = e_3$ we have

$$g = \begin{bmatrix} 1 \\ y^2\partial^2 + \partial + 1 \end{bmatrix}$$

which is right coprime. Using Euclid we get

$$T = \begin{bmatrix} 0 & 1 \\ 1 & y^2\partial^2 + \partial + 1 \end{bmatrix} \quad \text{and} \quad T^{-1} = \begin{bmatrix} y^2\partial^2 + \partial + 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Furthermore, we have

$$MT = \begin{bmatrix} 1/y^2 & 0 \\ \partial^2 + (1/x^2)\partial + y/x^2 & y^2 \cdot f \end{bmatrix} \quad \text{and thus} \quad MT/N = \begin{bmatrix} 1/y^2 & 0 \\ \partial^2 + (1/x^2)\partial + y/x^2 & y^2 \end{bmatrix}$$

Inverting MT/N yields

$$(MT/N)^{-1} = \begin{bmatrix} y^2 & 0 \\ \partial^2 + (1/x^2)\partial + y/x^2 & 1/y^2 \end{bmatrix}.$$

From that we finally get

$$S = (MT/N)^{-1}(M^{(2)})^{-1} = \begin{bmatrix} 1 & 0 \\ (1/y^2)\partial^2 + (1/x^2y^2)\partial + 1/(yx^2) & 1/(x^2y^2) \end{bmatrix}.$$

And indeed $SMT = N$.

Acknowledgements

I would like to thank my Diploma thesis advisor Prof. Schmale, Carl von Ossietzky University, Oldenburg, Germany, for leading me to this subject. The idea to compute via cyclic vectors is also his as well as several methodological hints.

References

Adjamagbo, K., 1988. Sur l'effectivité du lemme du vecteur cyclique. C. R. Acad. Sci. Paris Sér I Math. 306 (13), 543–546.

Bronstein, M., Petkovšek, M., 1996. An introduction to pseudo-linear algebra. Theoretical Computer Science 157, 3-33 157, 3–33.

Churchill, R. C., Kovacic, J. J., 2002. Cyclic vectors. In: Guo, L., Cassidy, P. J., Keigher, W. F., Sit, W. Y. (Eds.), Differential algebra and related topics. World Scientific Publishing Co. Pte. Ltd., pp. 191–218.

Cohn, P. M., 1985. Free rings and their relations, 2nd Edition. Academic press inc. (London) Ltd.

Culianez, G., Quadrat, A., 2005. Formes de hermite et de jacobson: implémentations et applications. Tech. rep., INRIA Sophia Antipolis.

G. David Forney, j., May 1975. Minimal bases of rational vector spaces with applications to multivariable linear systems. SIAM J. Control 13, 493 – 520.

Ilchmann, A., Mehrmann, V., 2005. A behavioral approach to time-varying linear systems. part 1: general theory. SIAM J. Control Optim. 44 (5), 1725–1747.

Ilchmann, A., Nürnberger, I., Schmale, W., 1984. Time-varying polynomial matrix systems. Int. J. Control 40 (2), 329–362.

Jacobson, N., 1978. The theory of rings. American Mathematical Society, Providence, R.I.

Zerz, E., 2006. An algebraic analysis approach to linear time-varying systems. IMA Journal of Mathematical Control and Information 23, 113–126.

Zerz, E., 2007. State representation of time-varying linear systems. In: Gröbner Bases in Control Theory and Signal Processing. No. 3 in Radon Series on Computational and Applied Mathematics. pp. 235–251.