Factoring Partial Differential Systems in Positive Characteristic

M. A. Barkatou, T. Cluzeau, J.-A. Weil

with an appendix by M. van der Put:
Classification of Partial Differential Modules in Positive Characteristic

Abstract. An algorithm for factoring differential systems in characteristic p has been given by Cluzeau in [Cl03]. It is based on both the reduction of a matrix called p-curvature and eigenring techniques. In this paper, we generalize this algorithm to factor partial differential systems in characteristic p. We show that this factorization problem reduces effectively to the problem of simultaneous reduction of commuting matrices.
In the appendix, van der Put shows how to extend his classification of differential modules, used in the work of Cluzeau, to partial differential systems in positive characteristic.

Mathematics Subject Classification (2000). 68W30; 16S32; 15A21; 16S50; 35G05.

Keywords. Computer Algebra, Linear Differential Equations, Partial Differential Equations, D-Finite Systems, Modular Algorithms, p-Curvature, Factorization, Simultaneous Reduction of Commuting Matrices.

Introduction

The problem of factoring D-finite partial differential systems in characteristic zero has been recently studied by Li, Schwarz and Tsarëv in [LST02, LST03] (see also [Wu05]). In these articles, the authors show how to adapt Beke's algorithm (which factors ordinary differential systems, see [CH04] or [PS03, 4.2.1] and references therein) to the partial differential case. The topic of the present paper is an algorithm that factors D-finite partial differential systems in characteristic p. Aside from its theoretical value, the interest of such an algorithm is its potential use as a first step in the construction of a modular factorization algorithm; in addition, it provides useful modular filters, *e.g.*, for detecting the irreducibility of partial differential systems.

T.Cluzeau initiated this work while being a member of Laboratoire stix, École polytechnique, 91128 Palaiseau Cedex, France.

Concerning the ordinary differential case in characteristic p, factorization algorithms have been given by van der Put in [Pu95, Pu97] (see also [PS03, Ch.13]), Giesbrecht and Zhang in [GZ03] and Cluzeau in [Cl03, Cl04]. In this paper, we study the generalization of the one given in [Cl03]. Cluzeau's method combines the use of van der Put's classification of differential modules in characteristic p based on the p-curvature (see [Pu95] or [PS03, Ch.13]) and the approach of the eigenring factorization method (see [Si96, Ba01, PS03]) as set by Barkatou in [Ba01].

In the partial differential case, we also have notions of p-curvatures and eigenrings at our disposal, but van der Put's initial classification of differential modules in characteristic p cannot be applied directly, so we propose an alternative algorithmic approach. To develop a factorization algorithm (and a partial generalization of van der Put's classification) of D-finite partial differential systems, we rebuild the elementary parts from [Cl03, Cl04] (where most proofs are algorithmic and independent of the classification) and generalize them to the partial differential context.
In the appendix, van der Put develops a classification of "partial" differential modules in positive characteristic which sheds light on our developments, and comes as a good complement to the algorithmic material elaborated in this paper.

We follow the approach of [Cl03], that is, we first compute a maximal decomposition of our system before reducing the indecomposable blocks. The decomposition phase is separated into two distinct parts: we first use the p-curvature to compute a *simultaneous decomposition* (using a kind of "isotypical decomposition" method), and then, we propose several methods to refine this decomposition into a maximal one.

The generalization to the partial differential case amounts to applying simultaneously the ordinary differential techniques to several differential systems. Consequently, since in the ordinary differential case we are almost always reduced to performing linear algebra on the p-curvature matrix, our generalization of the algorithm of [Cl03] relies on a way to reduce simultaneously commuting matrices (the p-curvatures).

A solution to the latter problem has been sketched in [Cl04]; similar ideas can be found in papers dealing with numerical solutions of zero-dimensional polynomial systems such as [CGT97]. The essential results are recalled (and proved) here for self-containedness.

The paper is organized as follows. In the first part, we recall some definitions about (partial) differential systems and their factorizations. We then show how to generalize to the partial differential case some useful results concerning p-curvatures, factorizations and rational solutions of the system: we generalize the proofs given in [Cl03, Cl04]. After a section on simultaneous reduction of commuting matrices, the fourth part contains the factorization algorithms. Finally, in Section 5, we show how the algorithm in [Cl03] can be directly generalized (with fewer efforts than for the partial differential case) to other situations: the case of "local" differential systems and that of difference systems.

1. Preliminaries

In this section, we recall some classical definitions concerning differential systems in several derivations. When there is only one derivation ($m = 1$ in what follows), we recover the ordinary definitions of differential field, ring of differential operators,$\cdots$. We refer to [PS03, Ch.2 and Ap.D] for more details on all these notions.

1.1. D-Finite Partial Differential Systems

Let $m \in \mathbb{N}^*$ and let $\mathscr{F} = k(x_1, \ldots, x_m)$ be the field of rational functions in the m variables $x_1, \ldots, x_m$ with coefficients in a field k.
For i in $\{1, \ldots, m\}$, let $\partial_i := \frac{d}{dx_i}$ be the operator "derivation with respect to the i-th variable" and let $\Theta := \{\partial_1, \ldots, \partial_m\}$ be the commutative monoïd generated by the ∂_i. Following the terminology of [PS03, Ap.D], we say that $(\mathscr{F}, \Theta)$ is a *partial differential field* or Θ*-field*. The *field of constants* of $(\mathscr{F}, \Theta)$ is $\mathscr{C} := \{f \in \mathscr{F} \,;\, \forall\, \delta \in \Theta,\, \delta(f) = 0\}$.

Definition 1. *Let $(\mathscr{F}, \Theta)$ be a partial differential field. The* ring of partial differential operators *with coefficients in $\mathscr{F}$ denoted $\mathscr{F}[\Theta]$ is the non-commutative polynomial ring over $\mathscr{F}$ in the variables ∂_i, where the ∂_i satisfy $\partial_i\,\partial_j = \partial_j\,\partial_i$, for all i, j and $\partial_i\, f = f\,\partial_i + \partial_i(f)$, for all $f \in \mathscr{F}$.*

Definition 2. *A* system of partial (linear) differential equations *or* (linear) partial differential system *is given by a finite set of elements of the ring $\mathscr{F}[\Theta]$. To every partial differential system S, we associate the (left) ideal (S) generated by the elements of S.*

Definition 3. *A partial differential system S is said to be* D-finite *if the $\mathscr{F}$-vector space $\mathscr{F}[\Theta]/(S)$ has finite dimension.*

D-finite partial differential systems correspond with $\mathscr{F}[\Theta]$-modules, *i.e.*, with vector spaces of finite dimension over $\mathscr{F}$ that are left modules for the ring $\mathscr{F}[\Theta]$ (see [PS03, Ap.D], and the next section in positive characteristic). In other words, a D-finite partial differential system is a partial differential system whose solutions only depend on a finite number of constants.

Throughout this paper, the partial differential systems that we consider are D-finite partial differential systems written in the form

$$\left\{\begin{array}{lll} \Delta_1(y) = 0 & \text{with} & \Delta_1 := \partial_1 - A_1, \\ \quad\vdots & & \\ \Delta_m(y) = 0 & \text{with} & \Delta_m := \partial_m - A_m, \end{array}\right. \tag{1}$$

where the $A_i \in \mathbb{M}_n(\mathscr{F})$ are square matrices of size $n \in \mathbb{N}^*$ with coefficients in $\mathscr{F}$ and the Δ_i commute. This implies the following relations, called *integrability conditions*, on the matrices A_i (see [PS03, Ap.D] for example):

$$\partial_i(A_j) - \partial_j(A_i) - A_i\,A_j + A_j\,A_i = 0, \text{ for all } i,\, j. \tag{2}$$

The (D-finite) partial differential system given by (1) will sometimes be noted $[A_1, \ldots, A_m]$; this is convenient when one wants to refer to the matrices A_i or to the operators Δ_i.

There exist algorithms to test whether a given partial differential system S is D-finite and if so, to write it into the form (1). For example, this can be achieved by computing a *Janet basis* (also called *involutive basis* in the literature) of S (see [Ja20, Ja29, HS02, BCGPR03]). These bases can be viewed as some kind of (non-reduced) Groebner bases. A Janet basis of the system yields a basis of the quotient $\mathscr{F}[\Theta]/(S)$. And, the fact that this basis is finite is then equivalent to the fact that the system is D-finite. The matrices A_i can be obtained by computing the action of the ∂_i on the basis of the quotient.

Let $\mathscr{M}$ be a $\mathscr{F}[\Theta]$-module of dimension n over $\mathscr{F}$. Let $(e_1, \ldots, e_n)$ and $(f_1, \ldots, f_n)$ be two bases of $\mathscr{M}$ related by

$$(f_1, \ldots, f_n) = (e_1, \ldots, e_n)\, P$$

where $P \in \mathrm{GL}_n(\mathscr{F})$ is an invertible element of $\mathbb{M}_n(\mathscr{F})$. If $[A_1, \ldots, A_m]$ and $[B_1, \ldots, B_m]$ are respectively the partial differential systems associated with $\mathscr{M}$ with respect to the bases $(e_1, \ldots, e_n)$ and $(f_1, \ldots, f_n)$, then, for all $i \in \{1, \ldots, m\}$, $B_i = P^{-1}\,(A_i\, P - \partial_i(P))$.

In the sequel, to simplify the notations, we will note $P[A_i] := P^{-1}\,(A_i\, P - \partial_i(P))$.

1.2. Factorization and Eigenrings

In this subsection, we define some notions about factorization of partial differential systems that are used in the sequel. We have seen in the last subsection, that a partial differential system over $(\mathscr{F}, \Theta)$ can be thought of as a left module over $\mathscr{F}[\Theta]$. This classical approach has the advantage of enabling one to apply directly the general theorems on modules [Ja80] (like the Jordan-Hölder theorem, Schur's lemma, the Krull-Schmidt theorem) to partial differential systems. This allows a better understanding of the problems arising in the study of partial differential systems.

Let $(\mathscr{F}, \Theta)$ be a partial differential field. Two partial differential systems $S_1 = [A_1, \ldots, A_m]$ and $S_2 = [B_1, \ldots, B_m]$ over $(\mathscr{F}, \Theta)$ are called *equivalent differential systems* (or *similar*) if the associated $\mathscr{F}[\Theta]$-modules are isomorphic. A simple computation shows that S_1 and S_2 are equivalent if, and only if, there exists a matrix $P \in \mathrm{GL}_n(\mathscr{F})$ such that, $B_i = P[A_i]$, for all i.

Let $S = [A_1, \ldots, A_m]$ be a partial differential system over $(\mathscr{F}, \Theta)$ and denote by $\mathscr{M}$ the associated $\mathscr{F}[\Theta]$-module. A subspace $\mathscr{W} \subset \mathscr{M}$ is called *invariant* if $\Delta_i\, \mathscr{W} \subset \mathscr{W}$, for all i. One can see easily that $\mathscr{W} \subset \mathscr{M}$ is invariant if, and only if,

$\mathscr{W}$ is a submodule of $\mathscr{M}$.

The partial differential system S is called a *reducible partial differential system* if the $\mathscr{F}[\Theta]$-module $\mathscr{M}$ is reducible, *i.e.*, if there exists a submodule $\mathscr{W}$ of $\mathscr{M}$ such that $0 \neq \mathscr{W} \neq \mathscr{M}$. Otherwise, S is called *irreducible*.

The partial differential system S is called a *decomposable partial differential system* if $\mathscr{M}$ is decomposable, *i.e.*, if $\mathscr{M} = \mathscr{W}_1 \oplus \mathscr{W}_2$ where $\mathscr{W}_i \neq 0$. Otherwise, S is called *indecomposable*.

The partial differential system S is called a *completely reducible partial differential system* if $\mathscr{M}$ is completely reducible, *i.e.*, if it is a direct sum of irreducible submodules.

In matrix terms, S is reducible (resp. decomposable) if there exists a system $[B_1, \ldots, B_m]$ equivalent to S over $\mathscr{F}$ such that, for all i, B_i has the following *reduced form*

$$B_i = \begin{pmatrix} B_{1,1} & B_{1,2} & \ldots & B_{1,r} \\ 0 & B_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & B_{r-1,r} \\ 0 & \ldots & 0 & B_{r,r} \end{pmatrix},$$

resp. *decomposed form*

$$B_i = \begin{pmatrix} B_{1,1} & & 0 \\ & \ddots & \\ 0 & & B_{r,r} \end{pmatrix}.$$

Definition 4. *Let $S = [A_1, \ldots, A_m]$ be a partial differential system.* Factoring S *means deciding whether it is reducible or irreducible, decomposable or indecomposable, and, in the reducible (resp. decomposable) case, find an invertible matrix P such that $P[A_i]$ has a reduced (resp. decomposed) form, for all i.*

Thus, factoring a partial differential system means factoring *simultaneously* the systems $\partial_i(Y) = A_i Y$. Particularly, we already see that if one of these systems is irreducible over $\mathscr{F}$, then the system $[A_1, \ldots, A_m]$ is irreducible over $\mathscr{F}$ as well.

In the ordinary differential case, when one wants to factor a reducible differential system, a very useful object is the eigenring associated with the differential system; indeed, non-trivial elements of this ring provide factorizations of the differential system (see [Si96, Ba01, PS03] for example).

Definition 5. *The* eigenring $\mathscr{E}(S)$ *of a partial differential system* $S = [A_1, \ldots, A_m]$ *is the set of all* $P \in \mathbb{M}_n(\mathscr{F})$ *satisfying:* $\partial_i(P) = P\,A_i - A_i\,P$*, for all* i*.*

The eigenring of a partial differential system S is isomorphic to the ring of endomorphisms $\mathrm{End}(S)$ of the associated $\mathscr{F}[\Theta]$-module $\mathscr{M}$. Indeed, it is not difficult to see that a map $u : \mathscr{M} \longrightarrow \mathscr{M}$ belongs to $\mathscr{E}(S)$ if, and only if, u is an $\mathscr{F}$-linear map satisfying $u \circ \Delta_i = \Delta_i \circ u$, for all i.

In the sequel, we will also use the *partial eigenrings* $\mathscr{E}_i(S)$ consisting of all $P \in \mathbb{M}_n(\mathscr{F})$ satisfying $P\,\Delta_i = \Delta_i\,P$. We clearly have $\mathscr{E}(S) = \bigcap_{i=1}^m \mathscr{E}_i(S)$.

Remark 1. *The following facts are standard (*e.g.*,* [Ba01, PS03]*) for usual differential equations and generalize easily to the case of D-finite partial differential equations.*
$\mathscr{E}(S)$ is a finite dimensional $\mathscr{C}$-subalgebra of $\mathbb{M}_n(\mathscr{F})$ which contains $\mathscr{C}\,I_n$. As a consequence, any element of $\mathscr{E}(S)$ has a minimal (and characteristic) polynomial with coefficients in $\mathscr{C}$.
The eigenrings of two equivalent partial differential systems are isomorphic as $\mathscr{C}$-algebras.
If $\mathscr{E}(S)$ is a division ring, then S is indecomposable.
If S is irreducible, then $\mathscr{E}(S)$ is a division ring (Schur's lemma). The converse is false. However, if S is completely reducible and if $\mathscr{E}(S)$ is a division ring, then S is irreducible.

2. Partial Differential Systems in Positive Characteristic

Let p be a prime number and $r \in \mathbb{N}^*$. Consider the partial differential field $(\mathbb{K}, \Theta)$ where $\mathbb{K} := k(x_1, \ldots, x_m)$ with $k = \mathbb{F}_q$ for $q = p^r$. The *partial constant field* of $\mathbb{K}$ with respect to, say, ∂_1 is $\mathscr{C}_1 := \ker_{\mathbb{K}}(\partial_1) = k(x_1^p, x_2, \ldots, x_m)$. The constant field of $(\mathbb{K}, \Theta)$ is $\mathscr{C} := \bigcap_{i=1}^m \mathscr{C}_i = k(x_1^p, x_2^p, \ldots, x_m^p)$. Note that $\mathbb{K}$ is a $\mathscr{C}$-vector space of dimension p^m and a $\mathscr{C}_i$-vector space of dimension p.

In the following, we consider partial differential systems $[A_1, \ldots, A_m]$ with coefficients in $(\mathbb{K}, \Theta)$ and, to avoid pathologies, we assume that the prime number p is strictly greater than the size n of the A_i.

Following the theory of differential equations in characteristic p, we now introduce *partial p-curvatures*:

Definition 6. *Let* $[A_1, \ldots, A_m]$ *be a partial differential system over* $(\mathbb{K}, \Theta)$*. The* partial p-curvatures of $[A_1, \ldots, A_m]$ *are the* $\mathbb{K}$*-linear operators* $\Delta_i^p = (\partial_i - A_i)^p$*, for* $i \in \{1, \ldots, m\}$*, acting on* $\mathbb{K}^n$*.*

The proof of the following lemma is then immediate:

Lemma 1. *Let $S = [A_1, \ldots, A_m]$ be a partial differential system over $(\mathbb{K}, \Theta)$. All the partial p-curvatures Δ_i^p commute and belong to the eigenring $\mathscr{E}(S)$. In particular, the minimal (and characteristic) polynomial of each Δ_i^p has its coefficients in $\mathscr{C} = k(x_1^p, \ldots, x_m^p)$.*

Note that in [Ka70, 5, p.189] (see also [Ka82, VII, p.222]), Katz defines a notion of p-curvature in the case of several derivations and remarks the links between this p-curvature and the eigenring of the system (refined in Lemma 1). In [Ka82], he gives a method for computing the partial p-curvatures (see also [PS03, Ch.13] or [Cl03]). For all i in $\{1, \ldots, m\}$, it consists in computing the index p element in the Lie sequence $(A_{i,(j)})_{j\in\mathbb{N}}$ associated with $[A_i]$ which is defined by:

$$A_{i,(0)} := I_n \text{ and } \forall j \geq 0,\ A_{i,(j+1)} := \Delta_i(A_{i,(j)}) = \partial_i(A_{i,(j)}) - A_i\, A_{i,(j)}.$$

In [Pu95] (see also [PS03, Ch.13]), van der Put gives a classification of differential modules in characteristic p. A consequence of this classification for the factorization problem is that the Jordan form of the p-curvature leads to all the factorizations of the system. In [Cl03] (see also [Pu97, Cl04]), this is made algorithmic and combining this to the approach of the eigenring factorization method proposed by Barkatou in [Ba01], the author develops an algorithm for factoring differential systems in characteristic p and provides elementary effective proofs of the key results (that can also be viewed from van der Put's classification).

In the sequel, we build upon the approach of [Cl03] to generalize the main steps of the van der Put classification that are needed for the algorithm ; in the appendix, van der Put shows how to completely generalize his classification to partial differential modules.

2.1. Rational Solutions

Let $S = [A_1, \ldots, A_m]$ be a partial differential system over $(\mathbb{K}, \Theta)$. The space of rational solutions (or solutions in $\mathbb{K}^n$) of the system S is the set $\mathrm{Sol}_{\mathbb{K}}(S) = \{Y \in \mathbb{K}^n;\ \forall\, i,\ \Delta_i(Y) = 0\}$. One can show that $\mathrm{Sol}_{\mathbb{K}}(S)$ is a vector space over the field of constants $\mathscr{C}$ of dimension $\leq n$.

The first algorithmic use of the p-curvature stems from Cartier's lemma ([Ka70, Theorem 5.1]).

Lemma 2 (Cartier). *Let $S = [A_1, \ldots, A_m]$ be a partial differential system over $(\mathbb{K}, \Theta)$. The partial p-curvatures Δ_i^p are all zero if, and only if, S admits a basis of rational solutions, i.e solutions in $\mathbb{K}^n$*

Note that S admits a basis of rational solutions if, and only if, S has a fundamental matrix of rational solutions, *i.e.*, a matrix $P \in \mathrm{GL}_n(\mathbb{K})$ satisfying $\Delta_i(P) = \partial_i(P) - A_i\, P = 0$, for all i. In other words, S admits a basis of rational solutions if, and only if, there exists $P \in \mathrm{GL}_n(\mathbb{K})$ such that $P[A_i] = 0$, for all i.

Although a proof of the above lemma can be found in [Ka70, Theorem 5.1], we propose a new constructive proof for further algorithmic use.

Proof. The implication "$\Leftarrow$" is trivial so we only need to prove "$\Rightarrow$". Consider first the differential field $(k(x_2,\dots,x_m)(x_1),\partial_1)$ which has $\mathscr{C}_1$ as constant field, and view Δ_1 as a differential operator acting on $k(x_2,\dots,x_m)(x_1)^n$; as it satisfies $\Delta_1^p = 0$, Cartier's lemma in the ordinary differential case (*e.g.*, [Cl03, Lemma 3.3]) implies the existence of some $P_1 \in \mathrm{GL}_n(k(x_2,\dots,x_m)(x_1))$ such that $P_1^{-1}\,\Delta_1\,P_1 = \partial_1$. For all i in $\{1,\dots,m\}$, let $\tilde{\Delta}_i = P_1^{-1}\,\Delta_i\,P_1 := \partial_i - B_i$ for some matrices B_i having coefficients in $k(x_1,\dots,x_m)$. The integrability conditions imply that $\partial_1(B_i) = 0$ so that the B_i have their coefficients in $\mathscr{C}_1$, for all i. Now, we use the hypothesis $\tilde{\Delta}_2^p = 0$ and we apply Cartier's lemma in the ordinary differential case to $\tilde{\Delta}_2$: there exists $P_2 \in \mathrm{GL}_n(\mathscr{C}_1)$ such that $P_2^{-1}\,\tilde{\Delta}_2\,P_2 = \partial_2$. Moreover $P_2 \in \mathrm{GL}_n(\mathscr{C}_1)$ implies that ∂_1 commutes with P_2 and thus $P_2^{-1}\,P_1^{-1}\,\Delta_1\,P_1\,P_2 = P_2^{-1}\,\tilde{\Delta}_1\,P_2 = P_2^{-1}\,\partial_1\,P_2 = \partial_1$. Applying this process recursively, we finally find an invertible matrix $P = P_1\cdots P_m$ with coefficients in $k(x_1,\dots,x_m)$ such that $P^{-1}\,\Delta_i\,P = \partial_i$, for all i; the result follows. □

This proof exhibits an algorithm to compute a fundamental matrix of rational solutions of a partial differential system whose partial p-curvatures vanish.

Algorithm SimRatSols
Input: a partial differential system $S = [A_1,\dots,A_m]$
with the $A_i \in \mathbb{M}_n(\mathbb{K})$ and whose partial p-curvatures vanish.
Output: a fundamental matrix of rational solutions of $[A_1,\dots,A_m]$.
1- For i from 1 to m, set $A_i^{[1]} := A_i$.
2- For i from 1 to m do:
  2*a*- Compute a fundamental matrix P_i of rational solutions of
the differential system (viewed as a system in one variable) $\partial_i(Y) = A_i^{[i]}\,Y$
  2*b*- For j from 1 to m, compute $A_j^{[i+1]} := P_i^{-1}\,(A_j^{[i]}\,P_i - \partial_j(P_i))$.
3- Return $P_1\cdots P_m$.

Remark 2. *When only one of the partial p-curvatures is zero, then, after a change of basis, the system (1) can be written*

$$\begin{cases} \Delta_1(y) = 0 \quad \textit{with} \quad \Delta_1 := \partial_1, \\ \quad\vdots \\ \Delta_m(y) = 0 \quad \textit{with} \quad \Delta_m := \partial_m - A_m, \end{cases} \tag{3}$$

so that the integrability conditions (2) imply $\partial_1(A_j) = 0$ for all $j \in \{2,\dots,m\}$. We can thus deduce that the partial differential system no longer depends on the variable x_1 but rather on x_1^p.

An alternative to Algorithm SimRatSols is to use the "Katz' projector formula"; this will be studied (and used) at the end of next subsection.

In general (when the partial p-curvatures do not vanish), in characteristic p, computing rational solutions is an ordinary linear algebra problem which can be set (and solved) in two ways:

- An iterative method: since for all i, $\mathbb{K} \cong \bigoplus_{j=0}^{p-1} \mathscr{C}_i\, x_i^j$, any element Y of $\mathbb{K}^n$ can be written $Y = \sum_{i=0}^{p-1} C_i\, x_1^i$ with $C_i \in \mathscr{C}_1^n$. The equation $\Delta_1(Y) = 0$ is then seen as an $np \times np$ linear system for the entries of the C_i. Let $Y_{1,1}, \ldots, Y_{1,r_1}$ denote a basis (over $\mathscr{C}_1$) of solutions in $\mathbb{K}^n$ of $\Delta_1(Y) = 0$ obtained from this linear system. As the Δ_i commute, the space generated over $\mathscr{C}_1 \cap \mathscr{C}_2$ by this basis is stable under Δ_2. Set $Y_2 := \sum_{i=1}^{r_1} \sum_{j=0}^{p-1} c_{i,j}\, Y_{1,i}\, x_2^j$. The equation $\Delta_2(Y_2) = 0$ translates into an $r_1 p \times r_1 p$ linear system for the $c_{i,j} \in \mathscr{C}_1 \cap \mathscr{C}_2$. Solving this system yields a basis $Y_{2,1}, \ldots, Y_{2,r_2}$ (over $\mathscr{C}_1 \cap \mathscr{C}_2$) of solutions in $\mathbb{K}^n$ of $\{\Delta_1(Y) = 0, \Delta_2(Y) = 0\}$. Iterating this process, we finally find a basis over $\mathscr{C}$ of rational solutions of $[A_1, \ldots, A_m]$.
- A direct (less interesting) method proceeds as follows: as $\mathbb{K}$ is a $\mathscr{C}$ vector space (of dimension p^m over $\mathscr{C}$), the system $\{\Delta_1(Y) = 0, \ldots, \Delta_m(Y) = 0\}$ translates into m linear systems of size np^m over $\mathscr{C}$, from which a basis (over $\mathscr{C}$) of rational solutions is obtained.

As observed in [Cl03, 3.2.1] (see also [Cl04]), this leads to an immediate algorithm for computing the eigenring (by computing rational solutions of a partial differential system of dimension n^2).

2.2. Scalar Partial p-Curvatures

We consider the case when all the partial p-curvatures Δ_i^p are scalar, that is, for all i, $\Delta_i^p = \lambda_i\, I_n$ with $\lambda_i \in \mathscr{C} = k(x_1^p, \ldots, x_m^p)$ (see Lemma 1).

First consider individually the system $\partial_1(Y) = A_1\, Y$ (also noted $[A_1]$) with coefficients in the differential field $\mathbb{K} = k(x_2, \ldots, x_m)(x_1)$ endowed with the derivation ∂_1 and having $\mathscr{C}_1$ as constant field. In [Cl04] (see also [Pu97, PS03]), partial fraction decomposition shows that if $\Delta_1^p = \lambda_1\, I_n$ with $\lambda_1 \in \mathscr{C}_1$, then there exists $\nu_1 \in \overline{k(x_2, \ldots, x_m)}(x_1)$ such that $[A_1]$ is equivalent (over $\overline{k(x_2, \ldots, x_m)}(x_1)$) to $[\nu_1 I_n]$. Now Theorem 3.7 of [Cl03] applies and its proof shows that in fact $\mu_1 = \mathrm{Tr}(A_1)/n \in \mathbb{K}$ satisfies $\partial_1^{p-1}(\mu_1) + \mu_1^p = \lambda_1$ and the system $[A_1]$ is thus equivalent over $\mathbb{K}$ to $[\mu_1\, I_n]$.

Proposition 1. *Let $S = [A_1, \ldots, A_m]$ be a partial differential system over $(\mathbb{K}, \Theta)$. All the partial p-curvatures Δ_i^p are scalar if, and only if, the system S is equivalent over $\mathbb{K}$ to a "diagonal system". In other words, for all i, $\Delta_i^p = \lambda_i\, I_n$ with $\lambda_i \in \mathscr{C}$ if, and only if, there exists $P \in \mathrm{GL}_n(\mathbb{K})$ such that $P[A_i] = \mu_i\, I_n$ with $\mu_i \in \mathbb{K}$, for all i.*

Proof. Suppose, without loss of generality, that $m = 2$. Consider a partial differential system $[A_1, A_2]$ satisfying $\Delta_1^p = \lambda_1 I_n$ and $\Delta_2^p = \lambda_2 I_n$ with $\lambda_1, \lambda_2 \in \mathscr{C} = k(x_1^p, x_2^p)$. Set $(\mu_1, \mu_2) = (\mathrm{Tr}(\mathrm{A}_1)/n, \mathrm{Tr}(\mathrm{A}_2)/n)$ and consider the partial differential system $[A_1 - \mu_1 I_n, A_2 - \mu_2 I_n]$. By construction, its partial p-curvatures vanish. Moreover the integrability condition for this new partial differential system is satisfied: indeed, after some simplifications, this condition can be written $\partial_1(\mu_2) = \partial_2(\mu_1)$ which is equivalent to $\mathrm{Tr}(\partial_1(A_2)) = \mathrm{Tr}(\partial_2(A_1))$ and, from (2), to $\mathrm{Tr}(A_2\, A_1) = \mathrm{Tr}(A_1\, A_2)$. Then, Lemma 2 shows the existence of an invertible matrix P with coefficients in $\mathbb{K}$ such that $P[A_1 - \mu_1 I_n] = P[A_2 - \mu_2 I_n] = 0$, that is, $P^{-1}\,(\,(A_1 - \mu_1 I_n)\,P - \partial_1(P)) = P^{-1}\,(\,(A_2 - \mu_2 I_n)\,P - \partial_2(P)) = 0$ and the result follows. □

The proof of the next lemma, from [Ka70], exhibits a "Katz' formula" (see [Ka70], Formulas 5.1.2 and 5.1.7, p.191) to compute a fundamental matrix of rational solutions when all the partial p-curvatures are zero.

Let $S = [A_1, \ldots, A_m]$ be a partial differential system over $(\mathbb{K}, \Theta)$. It is clear that the space of rational solutions $\mathrm{Sol}_{\mathbb{K}}(S)$ of S is included in $\bigcap_{i=1}^m \ker(\Delta_i^p)$ (the common kernel of the partial p-curvatures Δ_i^p).

Lemma 3 (Katz). *Let $S = [A_1, \ldots, A_m]$ be a partial differential system over $(\mathbb{K}, \Theta)$. Then*

$$\bigcap_{i=1}^m \ker(\Delta_i^p) = \mathrm{Sol}_{\mathbb{K}}(S) \otimes_{\mathscr{C}} \mathbb{K}.$$

Proof. (Adapted from [Ka70]) Assume, for simplicity, that the denominators of A_i do not vanish at $x_i = 0$. For all $i \in \{1, \ldots, m\}$, we define

$$\mathrm{Pr}_i : \ \mathbb{K}^n \to \mathbb{K}^n,\ v \mapsto \sum_{k=0}^{p-1} \frac{(-x_i)^k}{k!}\, \Delta_i^k(v),$$

and we verify that:

- for all $v \in \mathbb{K}^n$, $\Delta_i(\mathrm{Pr}_i(v)) = -\,(-x_i)^{p-1}\, \Delta_i^p(v)$ so that Pr_i sends $\ker(\Delta_i^p)$ into $\ker(\Delta_i)$,
- for all $i, j \in \{1, \ldots, m\}$ such that $i \neq j$, $\Delta_j(\mathrm{Pr}_i(v)) = \mathrm{Pr}_i(\Delta_j(v))$ so that the Pr_i commute.

Now set $\mathrm{Pr} := \prod_{i=1}^m \mathrm{Pr}_i$. This operator from $\mathbb{K}^n$ to $\mathbb{K}^n$ satisfies the following property: for all $i \in \{1, \ldots, m\}$, if $\Delta_i^p(v) = 0$, then $\Delta_i(\mathrm{Pr}(v)) = 0$. From [Ka70, Formula 5.1.2, p.191], the formula for $\mathrm{Pr}(v)$ can be expanded to obtain

$$\mathrm{Pr}(v) = \sum_{\omega} \prod_{i=1}^m \frac{(-x_i)^{\omega_i}}{\omega_i!} \prod_{i=1}^m \Delta_i^{\omega_i}(v),$$

where the sum is taken over all r-uples $\omega = (\omega_1, \ldots, \omega_r)$ of integers such that $0 \leq \omega_i \leq p - 1$. This projector sends $\bigcap_{i=1}^m \ker(\Delta_i^p)$ to $\mathrm{Sol}_{\mathbb{K}}(S)$ and the (Taylor)

formula [Ka70, Formula 5.1.7, p.191] induces the identity on $\bigcap_{i=1}^{m} \ker(\Delta_i^p)$ and proves the lemma (compare to the proof of [Cl03, Theorem 3.8]). □

This thus yields an explicit formula for the calculation of a fundamental matrix of rational solutions of a partial differential system whose partial p-curvatures vanish and which satisfies further that $(0, \ldots, 0)$ does not cancel the denominator of the A_i.

From this, we obtain the following algorithm that diagonalizes partial differential systems having scalar partial p-curvatures.

Algorithm ScalpCurv
Input: a partial differential system $S = [A_1, \ldots, A_m]$
satisfying $\Delta_i^p = \lambda_i I_n$, for all i.
Output: a matrix P and the $P[A_i] = \mu_i I_n$.
1- For all i, compute $\mu_i := \mathrm{Tr}(A_i)/n$.
2- For all i, set $B_i := A_i - \mu_i I_n$ and compute the Lie sequences $B_{i,(j)}$.
3 Let $P := \prod_{i=1}^{m} \sum_{j=0}^{p-1} \frac{(-x_i)^j}{j!} B_{i,(j)}$
4- Return P and the $P[A_i] = \mu_i I_n$.

The correctness of this algorithm follows directly from Proposition 1, Lemma 3 and their proofs. In Step 3, to apply "Katz' formula", we have to make sure that $(0, \ldots, 0)$ does not vanish the denominator of the B_i; if it is the case, then we shift with respect to the corresponding variable. The calculation in Step 2, can be accelerated using [Cl03, Lemma 3.4] and the fact that the Lie sequences of the $[A_i]$ have already been computed to obtain the Δ_i^p.

2.3. Nilpotent Partial p-Curvatures

In the sequel, the characteristic (resp. minimal) polynomial of a matrix M will be noted $\chi(M)$ (resp. $\chi_{\min}(M)$).

We now treat the case when all the partial p-curvatures are nilpotent. Here, we use a method adapted from [Pu97, PS03] to handle the partial differential case.

Assume that all partial p-curvatures are nilpotent so, for all $i \in \{1, \ldots, m\}$, $\chi_{\min}(\Delta_i^p) = X^{d_i}$ with $d_i \in \mathbb{N}^*$. The case $d_i = 1$ for all i has already been addressed in Subsection 2.1, so we assume that there exists i such that $d_i > 1$.

The reasoning is the same as in the iterative method for computing rational solutions given at the end of Subsection 2.1. We have $\chi_{\min}(\Delta_1^p) = X^{d_1}$ so, as shown in [Pu97, PS03], one can find a basis of solutions of $\Delta_1(Y) = 0$ in $\mathbb{K}^n + \mathbb{K}^n\, l_1 + \cdots + \mathbb{K}^n\, l_1^{d_1-1}$ where l_1 satisfies $\partial_1(l_1) = 1/x_1$ (note: a general natural algorithm to perform this task - in characteristic zero - is given in [BP99] and is

easily adapted to our setting). So, the solutions of $\Delta_1(Y) = 0$ are of the form $Y_{1,i} = \sum_{j=0}^{d_i-1} Y_{1,i,j}\, l_1^j$ with $Y_{1,i,j} \in \mathbb{K}^n$. We now search for solutions of $\Delta_2(Y) = 0$ of the form $\sum_i c_i\, Y_{1,i}$ where the c_i are constant with respect to ∂_1. Viewing the c_i as functions in the variable x_2, the relation $\Delta_2\left(\sum_i c_i(x_2)\, Y_{1,i}\right) = 0$ yields a linear differential system (S_{Δ_2}) for the $c_i(x_2)$. Now $\chi_{\min}(\Delta_2^p) = X^{d_2}$, so we know that we can find a basis of solutions of (S_{Δ_2}) in $\mathbb{K}^n + \mathbb{K}^n\, l_2 + \cdots + \mathbb{K}^n\, l_2^{d_2-1}$ with $\partial_2(l_2) = 1/x_2$ (using again a method like in [BP99]). Iterating this process yields a basis of solutions in $\mathbb{K}^n[l_1, \ldots, l_m]$. Let P denote the invertible matrix whose columns are (generated by) the components in $\mathbb{K}^n$ of these solutions; then, for all i, $P[A_i]$ has a reduced form with zeros as diagonal blocks.

The case when, for all i, $\chi_{\min}(\Delta_i^p) = (X - a_i)^{d_i}$ with $a_i \in \mathbb{K}$ can then be handled since it reduces to the nilpotent case by using the tools from the previous subsection: indeed, letting $\mu_i := \mathrm{Tr}(A_i)/n$ and $B_i := A_i - \mu_i\, I_n$, we factor the partial differential system $[B_1, \ldots, B_m]$ having nilpotent partial p-curvatures, and then we shift back to deduce the factorization of $[A_1, \ldots, A_m]$. Note that this particular case appears naturally when we want to adapt van der Put's method for the computation of the maximal decomposition of a partial differential system $[A_1, \ldots, A_m]$ satisfying $\chi(\Delta_i^p) = F_i^{m_i}$, for all i (see Subsection 4.2, [Pu97, PS03] or [Cl03, Cl04]).

We now have the building blocks for factoring at our disposal. The key will be to reduce the problem to the simultaneous reduction of the (commuting) partial p-curvature matrices, so we address this problem first before proceeding to factorization.

3. Simultaneous Reduction of Commuting Matrices

Let K be a field and V be a vector space of finite dimension n over K. Let $\mathscr{L} = \{\phi_1, \ldots, \phi_s\}$ be a set of s commuting linear endomorphisms of V; V can be viewed as a left $K[X_1, \ldots, X_s]$-module by defining $X_j.v = \phi_j(v)$ for all $v \in V$, $j \in \{1, \ldots, s\}$. We shall denote this module $(V, \mathscr{L})$.

We say that $\mathscr{L}$ is *reducible*, *decomposable* or *completely reducible* over K if the $K[X_1, \ldots, X_s]$-module $(V, \mathscr{L})$ is reducible, decomposable or completely reducible.

In all of this section, $M_1, \ldots, M_s$ are s square matrices of size n with coefficients in K. We further assume that the M_i commute, *i.e.*, $\forall\, i,\, j,\, [M_i, M_j] := M_i\, M_j - M_j\, M_i = 0$. We set $\Omega := \{M_1, \ldots, M_s\}$. Viewing the M_i as commuting linear transformations written in the standard basis of K^n, we naturally define the terms Ω reducible, decomposable and completely reducible.

3.1. Simultaneous Decomposition

Recall first (see [Ja53, Ch.4,9]) that if Ω is indecomposable, then the minimal polynomial of any $N \in \Omega$ is a power of an irreducible polynomial over K.

Suppose now that Ω is decomposable and let $\mathscr{M} = (K^n, \Omega)$ be the corresponding $K[X_1, \ldots, X_s]$-module. We decompose $\mathscr{M}$ as

$$\mathscr{M} = \mathscr{W}_1 \oplus \cdots \oplus \mathscr{W}_d,$$

where the $\mathscr{W}_i$ are indecomposable. Now from [Ja53, Ch.4,9], we know that with respect to a basis of K^n adapted with this decomposition, each element of Ω has a decomposed form. Moreover, the minimal polynomial of each diagonal block is a power of an irreducible polynomial. In other words, there exists $P \in \mathrm{GL}_n(K)$ such that for all N in Ω, $P^{-1} N P$ has the form

$$P^{-1} N P = \begin{pmatrix} N_1 & & 0 \\ & \ddots & \\ 0 & & N_d \end{pmatrix}, \tag{4}$$

where, for all j, $\chi_{\min}(N_j) = F_j^{m_j}$ with F_j irreducible over K.

Definition 7. *A* simultaneous decomposition of Ω *is the given of* $P \in \mathrm{GL}_n(K)$ *such that, for all* $N \in \Omega$, $P^{-1} N P$ *has the form (4).*

In the following, we shall show how to compute a simultaneous decomposition of Ω. The key to this computation is the (obvious) lemma:

Lemma 4. *Assume that there exists* N *in* Ω *such that* $\chi(N) = F_1 \cdots F_h$ *with* $h \geq 2$ *and the* F_j *pairwise coprime. Then, we can compute* $P \in \mathrm{GL}_n(K)$ *such that, for all* N' *in* Ω, $P^{-1} N' P$ *has a decomposed form.*

Proof. We know from the kernel decomposition theorem that if $\chi(N) = F_1 \cdots F_h$ with the F_j pairwise coprime, then $K^n = \bigoplus_{j=1}^{h} \ker(F_j(N))$. Now, as the matrices N and N' commute, $\ker(F_j(N))$ is stable under N' and the result follows. □

Following this lemma, one can easily construct a recursive rational algorithm to compute a simultaneous decomposition of Ω (see [Cl04]).

We now propose to use another approach to compute a simultaneous decomposition. The idea underlying this method can be found in [CGT97 , Cl04].

Consider the matrix

$$M := t_1 M_1 + \cdots + t_s M_s, \tag{5}$$

with coefficients in $K[t_1, \ldots, t_s]$. Here $t_1, \ldots, t_s$ are indeterminates over K. Note that, in practice (see [CGT97 , Cl04]), the calculations are performed after having specialized the t_i to random values.

For all $i \in \{1, \ldots, s\}$, there exists a unique couple of matrices (S_i, N_i) with S_i semi-simple (that is diagonalizable over $\overline{K}$) and N_i nilpotent such that $M_i = S_i + N_i$ and $[S_i, N_i] = 0$. Such a decomposition $M_i = S_i + N_i$ is called the SN *decomposition of* M_i.

Remark 3. *The eigenvalues of M_i in $\overline{K}$ coincide with the eigenvalues of S_i in $\overline{K}$. In other words, M_i and S_i have the same characteristic polynomial.*

Lemma 5. *With the above notations, let $S = t_1 S_1 + \cdots + t_s S_s$ and $N = t_1 N_1 + \cdots + t_s N_s$. Then $M = S + N$ is the* SN *decomposition of the matrix $M = \sum_{i=1}^{s} t_i M_i$.*

Proof. We have to show that S is semi-simple, N is nilpotent and $[S, N] = 0$. We know (see [CO68, Théorème 19.6, p.294] or [Le94]) that for all i, S_i and N_i are polynomials in M_i. Consequently, as the M_i are pairwise commuting matrices, we have $[S_i, S_j] = [N_i, N_j] = [N_i, S_j] = 0$, for all i, j. The matrices $S_1, \ldots, S_s$ are thus pairwise commuting and semi-simple matrices. Thus they are simultaneously diagonalizable over $\overline{K}$, that is, there exists an invertible P with coefficients in $\overline{K}$ such that, $P^{-1} S_i P$ is diagonal, for all i. The fact that S is semi-simple follows immediately. If we note u_i the nilpotence index of N_i: $N_i^{u_i} = 0$ and $N_i^l \neq 0$ for all $l < u_i$. Then, a direct calculation shows that N is nilpotent with nilpotence index at most $u_1 + \cdots + u_s$. Finally, the equality $[S, N] = 0$ is clear since $[S_i, N_j] = 0$ for all i, j. □

Corollary 1. *With the previous notations, let $(v_1, \ldots, v_n) \in \overline{K}^n$ be a basis of common eigenvectors of $S_1, \ldots, S_s$. Let $\lambda_{i,j}$ be the eigenvalue of S_i associated with v_j,* i.e., *$S_i v_j = \lambda_{i,j} v_j$. Then $S v_j = (\sum_{i=1}^{s} t_i \lambda_{i,j}) v_j$ and, in particular, S has all its eigenvalues in $\sum_{i=1}^{s} t_i \overline{K} \subset \overline{K}[t_1, \ldots, t_s]$.*

An interesting consequence of this corollary is that the eigenvalues of M can be computed without having computing first those of the M_i. To proceed, it suffices to factor into products of linear forms over $\overline{K}[t_1, \ldots, t_s]$ the determinant of M (for example, we can use the algorithm given in [HRUW98, Ap.]). Indeed, we know that $\det(M)$ equals $(-1)^n$ times the product of the eigenvalues of M. Now, from Corollary 1, these eigenvalues are linear forms in the t_i with coefficients in $\overline{K}$ thus $\det(M)$ necessarily factors into linear forms over $\overline{K}[t_1, \ldots, t_s]$.

We obtain the following algorithm that computes a simultaneous decomposition of $\{M_1, \ldots, M_s\}$ ([CGT97 , Cl04]).

Algorithm SimDec (Simultaneous Decomposition)
Input: $\Omega = \{M_1, \ldots, M_s\}$ (with $M_i \in \mathbb{M}_n(K)$ pairwise commuting matrices).
Output: $P \in \mathbb{M}_n(K)$ giving a simultaneous decomposition of Ω.
1- Let $M := t_1\, M_1 + \cdots + t_s\, M_s$.
2- Compute $\chi(M)$ and factor it over $K(t_1, \ldots, t_s)$: let $\chi(M) = F_1^{m_1} \cdots F_d^{m_d}$ with F_i coprime irreducibles over $K(t_1, \ldots, t_s)$
3- For $i \in \{1, \ldots, d\}$, do:
 3a- Compute a basis $e_i = (e_{i,1}, \ldots, e_{i,n_i})$ of $\ker(F_i^{m_i}(M))$.
(choose the $e_{i,j}$ independent of the t_i)
4- Return the invertible P having the e_{ij} as columns.

Remark 4. *This algorithm does not necessarily provide a maximal decomposition of* Ω. *However, if the associated module* $\mathscr{M}$ *is semi-simple, then the result of this algorithm corresponds to the* isotypical decomposition *of* $\mathscr{M}$.

Note that the fact that factoring a partial differential system leads to reducing a linear combination with indeterminate coefficients of matrices already appears in a natural way when we consider integrable systems with constant coefficients. Indeed, let $M_1, \ldots, M_s$ be s commuting matrices with coefficients in $\mathbb{C}$. The D-finite partial differential system $\frac{d}{dt_i} Y = M_i\, Y$, $1 \leq i \leq s$ admits $\exp(M_1\, t_1 + \ldots + M_s\, t_s)$ as a fundamental matrix of solutions. Thus, if we want to calculate this exponential of matrix, we have first to reduce the matrix $M_1\, t_1 + \ldots + M_s\, t_s$ to a diagonal form (when possible) or a triangular form.

3.2. Reduction of Indecomposable Blocks

Suppose now that Ω is indecomposable. This implies (see [Ja53, Ch.4, 9]) that there exists $P \in \mathrm{GL}_n(K)$ such that for all $N \in \Omega$, the matrix $P^{-1}\, N\, P$ has the reduced form:

$$P^{-1}\, N\, P = \begin{pmatrix} N_{1,1} & N_{1,2} & \ldots & N_{1,r} \\ 0 & N_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & N_{r-1,r} \\ 0 & \ldots & 0 & N_{r,r} \end{pmatrix}, \tag{6}$$

where, for all j, $\chi_{\min}(N_{j,j}) = F$ with F is irreducible over K.

Definition 8. *Assume that* Ω *is indecomposable. A* (maximal) simultaneous reduction of Ω *is the given of* $P \in \mathrm{GL}_n(K)$ *such that, for all* $N \in \Omega$, $P^{-1}\, N\, P$ *has the form (*6*).*

To compute a simultaneous reduction of Ω, we can once again use the matrix

$$M = t_1\, M_1 + \cdots + t_s\, M_s.$$

We know that $\chi_{\min}(M) = F^m$ with F irreducible over $K(t_1, \ldots, t_s)$. Reducing this single matrix M over $K(t_1, \ldots, t_s)$, we obtain a simultaneous reduction of Ω (for

details, see [Cl04]). This leads to the following algorithm:

Algorithm SimRed (Simultaneous Reduction)
Input: $\Omega = \{M_1, \ldots, M_s\}$ (with $M_i \in \mathbb{M}_n(K)$) indecomposable.
Output: $P \in \mathbb{M}_n(K)$ giving a simultaneous reduction of Ω.
1- Let $M := t_1 M_1 + \cdots + t_s M_s$.
2- Compute the polynomial $\chi_{\min}(M) = F^m$.
3- For $i \in \{1, \ldots, m\}$, set $\mu_i := F^i(M)$ and $E_i := \ker(\mu_i)$.
4- Compute a basis of V adapted with the flag $(E_i)_i$
(choose one that does not depend on the t_i, see proof below).
5- Return the matrix P having the elements of this basis as columns.

Proposition 2. *The algorithm* SimRed *above computes a simultaneous reduction of* Ω.

Proof. Let $\mu := F(M)$. We have $\mu^m = 0$ and $\mu^i \neq 0$, for $i \in \{1, \ldots, m-1\}$. Let $E_i := \ker(\mu^i)$. It is clear that $E_m = K^n$ and $E_i \subset E_{i+1}$ such that $(E_i)_i$ is a flag of K^n. Let $\mathscr{B}$ be a basis of K^n adapted with this flag (*i.e.*, a basis computed from a basis of E_1 extended into a basis of E_2, ...) and that does not depend on the t_i; this is always possible because simultaneous reduction exists. The matrix of μ with respect to $\mathscr{B}$ has a reduced form with zeros as diagonal blocks and the matrix of M with respect to $\mathscr{B}$ has a reduced form. Calling P the matrix formed by the vectors of $\mathscr{B}$, the reduced forms of the M_i can be retrieved by conjugating by P (or by specializing $(t_1, \ldots, t_s)$ respectively into $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$ in the reduced form of M). □

4. Factoring Partial Differential Systems in Positive Characteristic

Let $[A_1, \ldots, A_m]$ be a partial differential system with coefficients in $(\mathbb{K}, \Theta)$ with $\mathbb{K} = k(x_1, \ldots, x_m)$ and $k = \mathbb{F}_q$ for $q = p^r$. We already know that factoring individually the system $\partial_i(Y) = A_i Y$ can be done by applying the algorithm developed in [Cl03]. To achieve this, we use the partial p-curvature Δ_i^p as well as the partial eigenring $\mathscr{E}_i(S)$. This can be done since during the algorithm of [Cl03], we are always reduced to performing linear algebra either on the p-curvature or on an element of the eigenring. Now, if we want to factor the system $[A_1, \ldots, A_m]$, then we have to factor simultaneously the systems $\partial_i(Y) = A_i Y$; we are thus naturally lead to reduce simultaneously the partial p-curvatures Δ_i^p which commute from Lemma 1.

As in the ordinary differential case, we first give a method to decompose the system and then, we show how to reduce indecomposable blocks.

4.1. Simultaneous Decomposition

The first step to decompose a partial differential system consists in computing a *simultaneous decomposition* of the system.

Definition 9. *Let* $[A_1, \ldots, A_m]$ *be a partial differential system with coefficients in* $(\mathbb{K}, \Theta)$. *A* simultaneous decomposition of $[A_1, \ldots, A_m]$ *is given by* $P \in \mathrm{GL}_n(\mathbb{K})$ *such that:*

1. *for all* i, $P[A_i] = \begin{pmatrix} B_i^{[1]} & & 0 \\ & \ddots & \\ 0 & & B_i^{[d]} \end{pmatrix}$,
2. *for all* i, *the partial* p*-curvature of each system* $\partial_i(Y) = B_i^{[j]} Y$ *has a characteristic polynomial of the form* $F_{i,j}^{m_{i,j}}$ *with* $F_{i,j}$ *irreducible.*

Proposition 3. *Let* $[A_1, \ldots, A_m]$ *be a partial differential system with coefficients in* $(\mathbb{K}, \Theta)$. *The matrix* $P \in \mathrm{GL}_n(\mathbb{K})$ *obtained by applying Algorithm* SimDec *to* $\{\Delta_1^p, \ldots, \Delta_m^p\}$ *provides a simultaneous decomposition of* $[A_1, \ldots, A_m]$.

Proof. For any polynomial Q, the spaces $\ker(Q(\Delta_i^p))$ are stable under the Δ_j since for all i, j, $[\Delta_i^p, \Delta_j^p] = 0$. So P obviously achieves Conditions (i) and (ii) of Definition 9. □

This induces an algorithm for computing a simultaneous decomposition of a partial differential system $[A_1, \ldots, A_m]$:

- Compute the partial p-curvatures Δ_i^p of $[A_1, \ldots, A_m]$,
- Return $P := \mathrm{SimDec}(\{\Delta_1^p, \ldots, \Delta_m^p\})$.

Example 1. *Let* $\mathbb{K} := \mathbb{F}_p(x_1, x_2)$ *with* $p = 3$ *and consider the D-finite partial differential system* $[A_1, A_2]$ *where* A_1 *and* A_2 *are the following matrices:*

$$A_1 = \begin{pmatrix} 1 & x_1 x_2 \\ 0 & 1 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} a_{1,1}^{(2)} & \frac{1}{2} f_2(x_2) x_2 x_1^4 + \frac{1}{2} f_3(x_2) x_1^2 + f_4(x_2) \\ -\frac{2 f_2(x_2)}{x_2} & f_1(x_2) + f_2(x_2) x_1^2 \end{pmatrix},$$

where $a_{1,1}^{(2)} = \frac{x_1 - 2x_1^3 x_2 f_2(x_2) - f_3(x_2) x_1 + x_1 x_2 (f_1(x_2) + f_2(x_2) x_1^2)}{x_1 x_2}$ *and* f_1, f_2, f_3 *and* f_4 *are functions in the variable* x_2.

Case 1: *first have a look at the case*

$$\{f_1(x_2) = x_2^4,\ f_2(x_2) = x_2,\ f_3(x_2) = x_2^6,\ f_4(x_2) = 2\,x_2^6 + 2\,x_2^4\}.$$

Following the algorithm given above, we compute the partial p*-curvatures* Δ_1^p *and* Δ_2^p, *and then, we apply* SimDec *to* $\{\Delta_1^p, \Delta_2^p\}$*: to proceed with the second step,*

we form the matrix $M = t_1\,\Delta_1^p + t_2\,\Delta_2^p$ *and we compute and factor its characteristic polynomial* $\chi(M)$*. We find:*

- $\chi(M)(X) = 2\,t_2\,x_2^{15}\,X + 2\,t_1\,t_2\,x_2^{12} + 2\,X\,t_2\,x_2^{12} + X\,t_2\,x_2^3 + 2\,t_2\,x_2^{15}t_1 + t_1\,t_2\,x_2^3 + X^2 + 2\,X\,t_1 + {t_1}^2 + {t_2}^2\,x_2^{18} + {t_2}^2x_2^{15} + {t_2}^2x_2^{24} + 2\,{t_2}^2x_2^{27}$.

The fact that $\chi(M)$ *is irreducible over* $\mathbb{K}(t_1, t_2)$ *implies that the partial p-curvatures can not be simultaneously reduced (nor decomposed) and consequently, the partial differential system* $[A_1, A_2]$ *is irreducible over* $\mathbb{K}$*.*

Case 2: *now, if*

$$\{f_1(x_2) = 2\,x_2,\ f_2(x_2) = 0,\ f_3(x_2) = 2x_2^6 + x_2,\ f_4(x_2) = x_2 + x_2^2\}.$$

then, applying the same process, we find:

- $\chi(M)(X) = (X + t_1 + 2\,t_2 + t_2\,x_2^3 + t_2\,x_2^{15})\ (X + t_1 + 2\,t_2\,x_2^3)$,

  so that the system is decomposable.

Applying the method of Algorithm SimDec*, we find*

$$P := \begin{pmatrix} 1 & 2\,\frac{x_2\left(x_2+{x_2}^4+{x_2}^{10}+2\,{x_2}^3{x_1}^2+{x_2}^{11}+{x_2}^6+2\,{x_1}^2+{x_1}^2{x_2}^{15}\right)}{2\,{x_2}^3+2+{x_2}^{15}} \\ 0 & 1 \end{pmatrix}$$

We can then verify that this matrix decomposes simultaneously the differential systems $[A_1]$ *and* $[A_2]$ *(and thus the partial differential system):*

$$P[A_1] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$P[A_2] = \begin{pmatrix} \frac{{x_2}^6 + 2\,{x_2}^2 + 2\,x_2 + 1}{x_2} & 0 \\ 0 & 2\,x_2 \end{pmatrix}.$$

More generally, we can see that the factorization of the system is the following:

- *If* $f_2(x_2) \neq 0$*, then the system is irreducible,*
- *If* $f_2(x_2) = 0$*, then the system is decomposable.*

4.2. Maximal Decomposition

Once a simultaneous decomposition has been computed, we may restrict the study to each block separately. We are now confronted to the case when the partial differential system $[A_1, \ldots, A_m]$ has partial p-curvatures satisfying $\chi(\Delta_i^p) = F_i^{m_i}$ with F_i irreducible and $m_i \geq 1$. If some $m_i = 1$, then $[A_1, \ldots, A_m]$ is irreducible and the factorization stops.

Let $\mathscr{M}$ denote the (partial) differential module associated with the system $[A_1, \ldots, A_m]$. We want to find a *maximal decomposition* of $\mathscr{M}$, *i*.e., a decomposition

$$\mathscr{M} = \mathscr{W}_1 \oplus \cdots \oplus \mathscr{W}_d,$$

where the $\mathscr{W}_i$ are indecomposable. As a result, we will write the differential system $[A_1, \ldots, A_m]$ in block diagonal form where the modules corresponding to the diagonal blocks are indecomposable. Here, the techniques from the previous section do not apply because a matrix $P \in \mathrm{GL}_n(\mathbb{K})$ that decomposes simultaneously the Δ_i^p does not necessarily decompose the differential systems $\partial_i(Y) = A_i\, Y$.

To handle this case, we can use the eigenring. In [Cl03, Proposition 4.7], it is shown that there exists a "separating" element in the eigenring. This is a matrix T with characteristic polynomial $\chi(T) = F_1 \cdots F_d$ such that $\gcd(F_i, F_j) = 1$ and $\chi(T_{\lfloor \mathscr{W}_i}) = F_i$. Applying a classical result of the eigenring factorization method (see [Ba01, Theorem 2] or [Cl04, Proposition 6]) to this element T yields a maximal decomposition of $\mathscr{M}$.

In practice, such a separating element can be found by taking random elements in the eigenring. In case of failure, one can use the idempotent decomposition of the eigenring from [GZ03] to obtain a maximal decomposition.

As noted in [Cl03], one can also adapt here the method proposed by van der Put in [Pu97, PS03]. Let a_i denote a root of F_i, *i*.e., the image of X in $\mathbb{K}[X]/(F)$. Let $\mathbb{K}^+ := \mathbb{K}(a_1, \ldots, a_m)$. Applying the algorithm of Subsection 4.1 over $\mathbb{K}^+$, we are reduced to studying a differential module $\mathscr{M}^+$ over $\mathbb{K}^+$ having p-curvatures with characteristic polynomial of the form $(X - a_i)^{m_i}$. The latter can be reduced (over $\mathbb{K}^+$) using Subsection 2.3 and, thus, we obtain a differential module $\mathscr{M}^+$ (over $\mathbb{K}^+$) with a maximal decomposition (and a complete reduction of the indecomposable blocks). Now, $\mathbb{K}^+$ has a structure of differential module over $\mathbb{K}$ and we have $\mathscr{M} = \mathscr{M}^+ \otimes_{\mathbb{K}} \mathbb{K}^+$: from this, we recover a basis of $\mathscr{M}$ over $\mathbb{K}$ and, then, a maximal decomposition of $\mathscr{M}$ (and the indecomposable blocks are fully reduced).

This last method can turn out to be costly because it may require to work in an unnecessary algebraic extension. In the next section, we give a simple rational alternative to handle the reduction of indecomposable partial differential systems.

4.3. Reducing Indecomposable Blocks

Definition 10. *Let* $[A_1, \ldots, A_m]$ *be an indecomposable partial differential system with coefficients in* $(\mathbb{K}, \Theta)$. *A* (maximal) simultaneous reduction *of* $[A_1, \ldots, A_m]$ *is given by an invertible matrix* P *such that:*

1. *for all* i, $P[A_i] = \begin{pmatrix} B_i^{[1]} & * & \dots & * \\ 0 & B_i^{[2]} & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & B_i^{[r]} \end{pmatrix}$,
2. *for all* i, *the partial* p*-curvature of each system* $\partial_i(Y) = B_i^{[j]} Y$ *has a minimal polynomial of the form* F_i *with* F_i *irreducible.*

Proposition 4. *Let* $S = [A_1, \dots, A_m]$ *be an indecomposable partial differential system with coefficients in* $(\mathbb{K}, \Theta)$. *The matrix* $P \in \mathrm{GL}_n(\mathbb{K})$ *obtained by applying Algorithm* SimRed *to* $\{\Delta_1^p, \dots, \Delta_m^p\}$ *provides a simultaneous reduction of* $[A_1, \dots, A_m]$.

Proof. In the proof of Proposition 2, we have constructed an element μ and an invertible matrix P such that $P^{-1}\,\mu\,P = S$ where S is block triangular with zeros as diagonal blocks. Now, we remark that, after turning $(t_1, \dots, t_s)$ into some $(0, \dots, 0, 1, 0, \dots, 0)$ (the 1 is in the i-th position) the element $\mu^{[i]}$ obtained is a non-zero and non-invertible element in the partial eigenring $\mathscr{E}_i(S)$. Then, for the same reasons as in the proof of [Ba01, Theorem 1], a direct calculation shows that, $B_i := P[A_i]$ has a reduced form (compare to the proof of [Cl03, Proposition 5.1]). □

We obtain thus the following method to compute a simultaneous reduction of indecomposable partial differential systems.

- Compute the partial p-curvatures Δ_i^p of $[A_1, \dots, A_m]$,
- Return $P := \mathrm{SimRed}(\{\Delta_1^p, \dots, \Delta_m^p\})$.

5. Two Other Generalizations

We have shown in the previous sections 3 and 4 how to generalize the algorithm of [Cl03] to factor partial differential systems in characteristic p. We will now see that this algorithm can be directly adapted to other situations as well. We will sketch the algorithms corresponding to [Cl03] in the case of one variable but, following the approach of Sections 3 and 4 to generalize [Cl03] to the multivariate case, one would obtain algorithms for factoring (integrable) partial local systems and (integrable) partial difference systems.

5.1. "Local" Factorizations

In this subsection, we give the elements needed to generalize the algorithm factoring differential systems with coefficients in $\mathbb{K} = k(x)$ with $k = \mathbb{F}_q$ for some $q = p^r$ to the case where the coefficients belong to $\mathbb{K}((x))$.

Let $[A]$ be a differential system with $A \in \mathbb{M}_n(\mathbb{K}((x)))$. The notions of p-curvature and eigenring can be defined as in the ordinary differential case. Noting that $\mathbb{K}((x))$ is a C_1-field ([Ja80, Definition 11.5, p.649]), we deduce that the classification of differential modules in characteristic p given by van der Put in [Pu95]

(see also [PS03, Ch.13]) can be applied in this case. Consequently, to construct an algorithm as the one given in [Cl03] when $A \in \mathbb{M}_n(\mathbb{K}(x))$, it only remains to specify how to factor a polynomial with coefficients in $\mathbb{F}_q((x))$ where $q = p^r$: this can be done using the standard Newton/Puiseux theorem (see [Abh90, Lecture 12] for example):

Lemma 6. *Let $F(Y) = Y^n + a_{n-1}(x)\,Y^{n-1} + \cdots + a_0(x)$ be a monic polynomial with coefficients in $k((x))$ with $k = \overline{\mathbb{F}}_p$ and $p > n$. There exists $r \in \mathbb{N}^*$ such that p does not divide r, and $F(Y) = \prod_{i=1}^{n}(Y - \nu_i)$ with $\nu_i \in k((x^{1/r}))$.*

All the ingredients needed have thus been given and by applying this theorem to the characteristic polynomial of the p-curvature, we obtain an immediate generalization of the algorithm given in [Cl03] to the case where the system has coefficients in $\mathbb{K}((x))$.

Remark 5. *In Lemma 6, if F denotes the characteristic polynomial of the p-curvature, then the ν_i are related to what we call the* exponential parts *of the system. More precisely, we can define a notion of exponential parts in characteristic p in the same way as in characteristic zero and show that they are exactly the reduction modulo p of the exponential parts in characteristic zero: this is detailed in* [CH04] *(see also* [Cl04, Ch.2]*).*

5.2. Factorizations of Difference Systems

The algorithm developed to factor differential systems $Y(x)' = A(x)\,Y(x)$ in characteristic p can be generalized to the case of difference systems $Y(x+1) = A(x)\,Y(x)$. The differential field $(k(x),')$ where $k = \mathbb{F}_q$ with $q = p^r$ is replaced by the difference field $(k(x),\sigma)$ where σ is defined by $\sigma(x) = x + 1$ and $\sigma(f) = f$ for all $f \in k$. The constant field $\{a \in k\,;\,\sigma(a) = a\}$ is then $k(x^p - x)$ (see [PS97, Ch.5] or [GZ03, Theorem 3.1]).

As in the differential case, there exists a natural notion of p-curvature:

Definition 11. *Let $\sigma(Y) = A\,Y$ with $A \in \mathrm{GL}_n(k(x))$ ($k = \mathbb{F}_q$, $q = p^r$) be a difference system. Its* p-curvature *is the product of matrices $A(x+p-1)\cdots A(x+1)\,A(x)$.*

A classification of difference modules in characteristic p (similar to that of [Pu95] or [PS03, Ch.13] in the differential case) is given in [PS97, Ch.5]. It implies that the Jordan form of the p-curvature gives all the factorizations of the difference system. The equation $y^{(p-1)} + y^p = \lambda$ with $\lambda \in k(x^p)$ is replaced by $u(x+p-1)\cdots u(x+1)\,u(x) = \lambda$ with $\lambda \in k(x^p - x)$. When the p-curvature is scalar, then the method used to improve [Cl03, Lemma 3.6] and to obtain [Cl03, Theorem 3.7] can not be imitated; indeed, if we suppose $p > n$ and try to adapt the proof, the solution $\mathrm{Tr}(A)/n$ of $y^{(p-1)} + y^p = \lambda$ is replaced by the solution $\det(A)^{1/n}$ of $u(x+p-1)\cdots u(x+1)\,u(x) = \lambda$ and we lose the rationality of this solution.

One can define an eigenring as well (see for example [Ba01, GZ03]): let $\sigma(Y) = AY$ be a difference system with $A \in \mathbb{M}_n(k(x))$. *The eigenring* $\mathcal{E}(A)$ *of* $[A]$ is the set defined by

$$\mathcal{E}(A) \quad = \quad \{P \in \mathbb{M}_n(k(x)) \,|\, \sigma(P)\, A = A\, P\}.$$

All the elements needed to develop an algorithm similar to that of [Cl03] are collected and the algorithm follows naturally. Note further that:

- The results of [Ba01] stay true in the difference case ([Ba01] is written in the general setting of pseudo-linear equations),
- The algorithm of Giesbrecht and Zhang ([GZ03]) can be used to factor Ore polynomials thus, in particular, difference operators.

Acknowledgments: the authors would like to thank Alban Quadrat for helpful explanations and references concerning D-finite partial differential systems and Janet bases, and Marius van der Put for his comments and the appendix that follows.

References

[Abh90] S. S. Abhyankar. *Algebraic geometry for scientists and engineers.* Mathematical Surveys and monographs, number **35**. Published by the A.M.S., 1990.

[Ba01] M. A. Barkatou. On the reduction of matrix pseudo-linear equations. Technical Report RR 1040, Rapport de Recherche de l'institut IMAG, 2001.

[BP99] M. A. Barkatou and E. Pflügel. An algorithm computing the regular singular formal solutions of a linear differential system. In *Journal of Symbolic Computation* **28(4-5)**, 1999.

[BCGPR03] Y. A. Blinkov, C. F. Cid, V. T. Gerdt, W. Plesken and D. Robertz. The Maple package "Janet": II. Polynomial Systems. In Proceedings of *Computer Algebra and Scientific Computing (CASC)*, Passau, 2003. `http://wwwmayr.informatik.tu-muenchen.de/CASC2003/`

[CO68] L. Chambadal and J. L. Ovaert. *Algèbre linéaire et algèbre tensorielle.* Dunot Université, Paris, 1968.

[Ch01] A. Chambert-Loir. Théorèmes d'algébricité en géométrie diophantienne. *Séminaire Bourbaki*, exposé No. **886**, Mars 2001.

[Cl03] T. Cluzeau. Factorization of differential systems in characteristic p. In *Proceedings of ISSAC'03*, ACM Press, 58-65, 2003.

[Cl04] T. Cluzeau. Algorithmique modulaire des équations différentielles linéaires. Thèse de l'université de Limoges, Septembre 2004.

[CH04] T. Cluzeau and M. van Hoeij. A modular algorithm for computing the exponential solutions of a linear differential operator. In *Journal of Symbolic Computation*, **38(3)**: 1043-1076, 2004.

[CGT97] R. Corless,P. Gianni, B. Trager. A reordered Schur factorization method for zero-dimensional polynomial systems with multiple roots. In *Proceedings of*

the 1997 International Symposium on Symbolic and Algebraic Computation, 133-140 ACM, New York, 1997.

[GZ03] M. Giesbrecht and Y. Zhang. Factoring and decomposing Ore polynomials over $\mathbb{F}_p(t)$. In *Proceedings of ISSAC'03*, ACM Press, 127-134, 2003.

[HS02] M. Hausdorf and M. Seiler. Involutives basis in MuPAD-Part I: involutive divisions. In *MathPad*, **11/1**: 51-56, 2002.

[HRUW98] M. van Hoeij, J.-F. Ragot, F. Ulmer and J.-A. Weil. Liouvillian solutions of linear differential equations of order three and higher. In *Journal of Symbolic Computation*, **11**: 1-17, 1998.

[Ja53] N. Jacobson. *Lectures in abstract algebra. II. Linear algebra.* Graduate Texts in Mathematics **31**, Springer-Verlag, 1953.

[Ja80] N. Jacobson. *Basic algebra II.* W.H. Freeman and Compagny, San Francisco, 1980.

[Ja20] M. Janet. Sur les systèmes aux dérivées partielles. In *Journal de Math.*, 8-ème série, III, 65-151, 1924.

[Ja29] M. Janet. *Leçons sur les systèmes d'équations aux dérivées partielles.* Cahiers Scientifiques, **IV**, Gauthiers-Villars, 1929.

[Ka70] N. Katz. Nilpotent connections and the monodromy theorem: applications of a result of Turritin. *Publ. Math. I. H. E. S.*, **39**: 355-412, 1970.

[Ka82] N. Katz. A conjecture in the arithmetic theory of differential equations. *Bull. Soc. Math. France*, **110**: 203-239, 1982.

[Le94] A. H. M. Levelt. The semi-simple part of a matrix. In *Algorithmen in de Algebra*, 85-88, 1994. `http://www.math.ru.nl/medewerkers/ahml/other.htm`

[LST02] Z. Li, F. Schwarz and S. P. Tsarev. Factoring zero-dimensional ideals of linear partial differential operators. In *Proceedings of ISSAC'02*, ACM Press, 168-175, 2002.

[LST03] Z. Li, F. Schwarz and S. P. Tsarev. Factoring systems of linear PDEs with finite-dimensional solution spaces. *Journal of Symbolic Computation*, **36(3-4)**: 443-471, 2003.

[Pu95] M. van der Put. Differential equations in characteristic p. *Compositio Math.*, **97**: 227-251, 1995.

[Pu97] M. van der Put. Modular methods for factoring differential operators. Manuscript, 1997.

[PS97] M. van der Put and M. F. Singer. *Galois theory of difference equations.* Lectures Notes in Mathematics, vol. **1666**, Springer (Berlin), 1997.

[PS03] M. van der Put and M. F. Singer. *Galois Theory of Linear Differential Equations* Grundlehren der mathematischen Wissenschaften, vol. **328**, Springer, 2003.

[Si96] M. F. Singer. Testing reducibility of linear differential operators: a group theoretic perspective. *Journal of Appl. Alg. in Eng. Comm. and Comp.*, **7(2)**: 77-104, 1996.

[Wu05] M. Wu. Factoring Finite-Dimensional Differential Modules. This volume.

Appendix: Classification of Partial Differential Modules in Positive Characteristic.

By Marius van der Put,
University of Groningen, Department of Mathematics
P.O. Box 800, 9700 AV Groningen, The Netherlands
M.van.der.Put@math.rug.nl

(1) *Introduction.* In [Pu95, PS03] a classification of differential (resp. difference in [PS97]) modules over a differential field K of characteristic $p > 0$ with $[K : K^p] = p$ is given. The differential modules in question can be seen as ordinary matrix differential equations. Here we show how to extend this to, say, the case $[K : K^p] = p^m$ with $m > 1$ (compare [1], 6.6 Remarks (1)). The (partial) differential modules are the partial differential equations considered in this paper. In order to simplify the situation, we will, as in the paper, avoid the skew field that may arise in the classification. The algorithmic results of the paper are made more transparent from the classification that we will work out.

(2) *Assumptions and notation.* Let K be a field of characteristic $p > 0$ and let K_0 be a subfield such that the universal differential module Ω_{K/K_0} has dimension $m \geq 1$ over K. There are elements $x_1, \ldots, x_m \in K$ such that $\{dx_1, \ldots, dx_m\}$ is a basis of Ω_{K/K_0}. Then $x_1, \ldots, x_m$ form a p-basis of K/K_0 which means that the set of monomials $\{x_1^{a_1} \cdots x_m^{a_m} \ | 0 \leq a_i < p \text{ for all } i\}$ is a basis of K over K^pK_0. We will write $C := K^pK_0$. For $i \in \{1, \ldots, m\}$, the derivation ∂_i of K/K_0 is given by $\partial_i x_j = \delta_{i,j}$. Clearly, the $\{\partial_i\}$ is a set of commuting operators. Put $\mathcal{D} := K[\partial_1, \ldots, \partial_m]$. This is a ring of differential operators and the partial differential equations that one considers (in the paper and here) are left $\mathcal{D}$-modules M of finite dimension over K. We note that M is a cyclic module (and thus $M \cong \mathcal{D}/J$ for some left ideal J of finite codimension) if $\dim_K M \leq p$. If $\dim_K M > p$, then in general M is not cyclic (compare [2], Exercise 13.3, p. 319). For notational convenience we will write $\mathcal{D}$-module for left $\mathcal{D}$-module of finite dimension over K.

(3) *Classification of the irreducible $\mathcal{D}$-modules.*
Similarly to [Pu95], one can prove the following statements. The center Z of $\mathcal{D}$ is $C[t_1, \ldots, t_m]$. The latter is a (free) polynomial ring in the variables $\{t_i := \partial_i^p\}_{i=1}^m$. Consider any maximal ideal $\underline{m} \subset Z$ and put $L = Z/\underline{m}$. Then $L \otimes_Z \mathcal{D}$ is a central simple algebra over L of dimension p^{2m}. The well known classification implies that this algebra is isomorphic to a matrix algebra $\mathrm{Matr}(p^{m_1}, D)$ where D is a (skew) field having dimension p^{2m_2} over its center L. Clearly $m_1 + m_2 = m$. The unique simple left module M of this algebra is $D^{p^{m_1}}$ and has dimension $p^{-m}[L : C]p^{m_1+2m_2} = p^{m_2}[L : C]$ over K. In particular, if the dimension of M over K is $< p$, then $L \otimes_Z \mathcal{D}$ is isomorphic to $\mathrm{Matr}(p^m, L)$.

Let M be an irreducible $\mathcal{D}$-module. Then M is also a Z-module of finite dimension over C. The irreducibility of M implies that $\underline{m}M = 0$ for some maximal ideal $\underline{m}$ of Z (write again $L = Z/\underline{m}$). Hence M is a simple left module over $L \otimes_Z \mathcal{D}$. If one knows the structure of the algebras $L \otimes_Z \mathcal{D}$, then the classification of irreducible $\mathcal{D}$-modules is complete.

(4) *Isotypical decomposition.*
Let M be any $\mathcal{D}$-module. Put $I := \{a \in Z \mid aM = 0\}$, the annulator of M. Then $I \subset Z$ is an ideal of finite codimension. Thus M is also an Z/I-module of finite dimension. Let $\{\underline{m}_1, \ldots, \underline{m}_s\}$ denote the set of maximal ideals containing I. This is the support of M. Then the Artin ring Z/I is the direct product of the local Artin rings $Z_{\underline{m}_i}/(I)$. One writes $1 = e_1 + \cdots + e_m$, where e_i is the unit element of the ring $Z_{\underline{m}_i}/(I)$. Then $M = \oplus M_i$, with $M_i = e_i M$. This is a module over $Z_{\underline{m}_i}/(I)$. Since Z is the center of $\mathcal{D}$ each M_i is again a $\mathcal{D}$-module. Moreover, the annulator of M_i is an ideal with radical $\underline{m}_i$. The above decomposition will be called the isotypical decomposition of M. The classification of $\mathcal{D}$-modules is in this way reduced to the classification of $\mathcal{D}$-modules with are annihilated by a power of some maximal ideal $\underline{m}$ of Z. The latter depends on the structure of $Z/\underline{m} \otimes_Z \mathcal{D}$.

(5) *Restricting the class of $\mathcal{D}$-modules.*
Let S denote the set of maximal ideals $s = \underline{m}$ in Z such that the algebra $Z/\underline{m} \otimes_Z \mathcal{D}$ is isomorphic to $\mathrm{Matr}(p^m, Z/\underline{m})$. In the sequel we will only consider $\mathcal{D}$-modules with support in S. The differential modules M, considered in this paper, satisfy $\dim_K M < p$. According to (3), their support is in S. We note that S depends on the fields $K_0 \subset K$. There are examples where S is the set of all maximal ideals of Z.

(6) *Classification of the $\mathcal{D}$-modules with support in $\{s\}$, where $s \in S$.*
We fix a maximal ideal $s = \underline{m} \in S$. The above Tannakian category will be denoted by $(\mathcal{D}, s)$. We note that the tensor product $M_1 \otimes M_2$ of two object in this category is defined as $M_1 \otimes_K M_2$, provided with the action of ∂_i (for $i = 1, \ldots, m$) given by $\partial_i(m_1 \otimes m_2) = (\partial_i m_1) \otimes m_2 + m_1 \otimes (\partial_i m_2)$.

Consider the category (Z, s) of the finitely generated Z-modules N, with support in $\{s\}$. The Tannakian structure of this category is determined by the definition of a tensor product. The tensor product of two modules N_1, N_2 in (Z, s) is $N_1 \otimes_C N_2$ equipped with the operations t_i given by $t_i(n_1 \otimes n_2) = (t_i n_1) \otimes n_2 + n_1 \otimes (t_i n_2)$.

The aim is to produce an equivalence $\mathcal{F}_s : (Z, s) \to (\mathcal{D}, s)$ of Tannakian categories. Once this is established, the required classification is reduced to classifying the objects of (Z, s). The functor $\mathcal{F}_s$ is defined as $\mathcal{F}_s(N) = M := K \otimes_C N$. The right hand side is clearly a (left) $K[t_1, \ldots, t_m]$-module. It suffices to extend this to a left $\mathcal{D}$-module by defining the operation of the ∂_i on M.

Let $\widehat{Z}_s$ denote the completion of the local ring $Z_{\underline{m}}$. Let $(\widehat{Z}_s, s)$ denote the category of the $\widehat{Z}_s$-modules of finite dimension over C. The categories (Z, s) and $(\widehat{Z}_s, s)$ are clearly the 'same'. Put $\widehat{\mathcal{D}}_s = \widehat{Z}_s \otimes_Z \mathcal{D}$ and let $(\widehat{\mathcal{D}}_s, s)$ denote the category of the left $\widehat{\mathcal{D}}_s$-modules which have finite dimension over K. Then the categories $(\mathcal{D}, s)$ and $(\widehat{\mathcal{D}}_s, s)$ are the 'same'. Therefore it suffices to construct an equivalence $\mathcal{F}_s : (\widehat{Z}, s) \to (\widehat{\mathcal{D}}_s, s)$.

For this purpose we need a free, rank one, $\widehat{Z}_s \otimes_C K$-module $\mathcal{Q}_s = \widehat{Z}_s \otimes_C Ke$, such that its structure of $\widehat{Z}_s \otimes_C K$-module extends to that of a left $\widehat{\mathcal{D}}_s$-module. Given $\mathcal{Q}_s$, the functor $\mathcal{F}_s$ is defined by $N \mapsto M := N \otimes_{\widehat{Z}_s} \mathcal{Q}_s$. Then M is a left $\widehat{\mathcal{D}}_s$-module by $\lambda(n \otimes \mu e) = n \otimes (\lambda\mu)e$. It is easily verified that $\mathcal{F}_s$ is indeed an equivalence of Tannakian categories. We note that M is equal to $N \otimes_C K$ as $\widehat{Z}_s \otimes_C K$-module, and our construction extends this to a left $\widehat{\mathcal{D}}_s$-module structure.

(7) *The construction of $\mathcal{Q}_s$.*
By assumption $A_0 := Z/\underline{m} \otimes_Z \mathcal{D}$ is isomorphic to $\mathrm{Matr}(p^m, Z/\underline{m})$. Let I be the (unique) simple left module of A_0. Then the morphism $A_0 \to \mathrm{End}_{Z/\underline{m}}(I)$ is a bijection. In particular, the commutative subalgebra $Z/\underline{m} \otimes_C K$ of A_0 acts faithfully on I. By counting dimensions over C, one sees that I is in fact a free $Z/\underline{m} \otimes_C K$-module with generator, say, e. Thus we have found a left A_0-module structure on $Z/\underline{m} \otimes_C Ke$. Now $\mathcal{Q}_s$ is constructed by lifting this structure, step by step, to a left $\widehat{\mathcal{D}}_s$-module structure on $\widehat{Z}_s \otimes_C Ke$. This is in fact equivalent to lifting a given isomorphism $A_0 \to \mathrm{Matr}(p^m, Z/\underline{m})$ to an isomorphism $\widehat{\mathcal{Q}}_s \to \mathrm{Matr}(p^m, \widehat{Z}_s)$. The method of [1] for the case $m = 1$, can be extended here. For notational convenience we present here a proof for the case $p = 2$ and $m = 2$.

We note that $\widehat{Z}_s \otimes_C K = \widehat{Z}_s[x_1, x_2]$ has a free basis $\{1, x_1, x_2, x_1x_2\}$ over $\widehat{Z}_s$. Consider the free module $\widehat{Z}_s[x_1, x_2]e$. We have to construct operators ∂_1 and ∂_2 on this module such that $\partial_1\partial_2 - \partial_2\partial_1 = 0$ and $\partial_i^2 = t_i$ for $i = 1, 2$. Put $\partial_i e = \ell_i e$ for $i = 1, 2$. Then the conditions are $\partial_i(\ell_i) + \ell_i^2 - t_i = 0$ for $i = 1, 2$ and $\partial_1(\ell_2) - \partial_2(\ell_1) = 0$. Suppose that we have found ℓ_1, ℓ_2 such that these equalities hold modulo $\underline{m}^s$. Then we want to change the ℓ_i in $\ell_i + r_i$ with $r_1, r_2 = 0 \bmod (\underline{m}^s)$ such that the required equalities hold module $\underline{m}^{s+1}$. This step suffices for the proof of the statement. It amounts to solving

$$\partial_i(r_i) = -\partial(\ell_i) - \ell_i^2 + t_i \bmod \underline{m}^{s+1} \text{ and}$$

$$\partial_1(r_2) - \partial_2(r_1) = \partial_2(\ell_1) - \partial_1(\ell_2) \bmod \underline{m}^{s+1}.$$

The right hand sides of the equalities are already 0 mod $\underline{m}^s$. Write $r_1 = r_1(0,0) + r_1(1,0)x_1 + r_1(0,1)x_2 + r_1(1,1)x_1x_2$ and similarly for r_2. The right hand side of the first equation with $i = 1$, is killed by the operator ∂_1 and therefore contains only the terms $1, x_2$. This leads to a unique determination of $r_1(1,0)$ and $r_1(1,1)$ and the $r_1(0,0), r_1(0,1)$ can be chosen freely. Similarly, the terms $r_2(0,1), r_2(1,1)$

are determined and the terms $r_2(0,0), r_2(1,0)$ can be chosen freely. The second equation reads

$$r_2(1,0) - r_1(0,1) + r_2(1,1)x_2 - r_1(1,1)x_1 = \partial_2(\ell_1) - \partial_1(\ell_2) \bmod \underline{m}^{s+1}.$$

The right hand side R uses only the terms $1, x_1, x_2$. Moreover, $\partial_1(R) = \partial_1\partial_2(\ell_1) = \partial_2\partial_1(\ell_1)$ and this is equal to $\partial_2(\partial_1(\ell_1) + \ell_1^2 - t_1)$. Hence the coefficients of x_1 of the two sides are equal. The same holds for the coefficients of x_2. The coefficient of 1 on the two sides can be made equal for a suitable choice of $r_1(0,1)$ and/or $r_2(1,0)$.

(8) *Final remarks.*
Let (Z, S) denote the Tannakian category of the Z-modules, having finite dimension over C and with support in S. Let $(\mathcal{D}, S)$ denote the category of the left $\mathcal{D}$-modules having finite dimension over K and with support in S (as Z-module). One can 'add' the equivalences $\mathcal{F}_s$ in an obvious way to an equivalence $\mathcal{F} : (Z, S) \to (\mathcal{D}, S)$. For an object M of $(\mathcal{D}, S)$, there is an object N of (Z, S) such that $\mathcal{F}(N) = M$. Then M, as module over $K[t_1, \ldots, t_m]$, describes in fact the p-curvature of M. Since $N \otimes_C K \cong M$, one can say that N represents already the p-curvature of M. In particular, the characteristic (and minimal) polynomials for the t_i have their coefficients in $C = K_0K^p$.

As observed before, classifying the left $\mathcal{D}$-modules of finite dimension over K and with support in S is equivalent to classifying the Z-modules of finite dimension over C and with support in S. The latter is done by decomposing an object into isotypical components. Hence we may restrict our attention to a single maximal ideal $s = \underline{m} \in S$. The modules N that we want to classify are in fact the finitely generated modules over the complete regular local ring $\widehat{Z}_s \cong L[[d_1, \ldots, d_m]]$ which are annihilated by a power of the maximal ideal $\underline{m}$. Unlike the case $m = 1$, no reasonable classification (or moduli spaces) seems possible. One observation can still be made. The module N has a sequence of submodules $0 = N_0 \subset N_1 \subset \cdots \subset N_t = N$ such that each quotient N_{i+1}/N_i is isomorphic to the module $L = Z/\underline{m}$. In other words, N is a multiple extension of the module L.

M. A. Barkatou, T. Cluzeau, J.-A. Weil
LACO, Université de Limoges
123 avenue Albert Thomas
87060 Limoges, France
e-mail: {moulay.barkatou,thomas.cluzeau,jacques-arthur.weil}@unilim.fr