Available online at www.sciencedirect.com
SCIENCE DIRECT
Journal of Algebra 275 (2004) 77–105
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Absolute reducibility of differential operators and Galois groups

É. Compoint [a] and J.A. Weil [b,1,*]

[a] *Département de Mathématiques, Université de Lille I, 59655 Villeneuve d'Ascq cedex, France*
[b] *LACO, Département de Mathématiques, Faculté des Sciences, 123 avenue Albert Thomas, 87060 Limoges cedex, France*

Received 26 July 2002

Communicated by Eva Bayer-Fluckiger

Abstract

A differential operator $L \in \mathbb{C}(x)[d/dx]$ is called *absolutely reducible* if it admits a factorization over an algebraic extension of $\mathbb{C}(x)$. In this paper, we give sharp bounds on the degree of the extension that is needed in order to compute an absolute factorization. Algorithms to characterize and compute absolute factorizations are then elaborated. The ingredients are differential Galois theory, a group-theoretic study of absolute factorization, and a descent technique for differential operators with coefficients in $\overline{\mathbb{C}(x)}$.

Introduction

Let $\mathbb{C}$ denote the field of complex numbers and $\mathcal{D} = \mathbb{C}(x)[\partial]$ the ring of differential operators ($\partial = d/dx$) with coefficients in the field $k = \mathbb{C}(x)$ of rational functions with coefficients in $\mathbb{C}$ (see [31] for an exhaustive presentation of these objects).

Consider the differential operator

$$L = \partial^4 - \frac{1}{x}\partial^3 + \frac{3}{4x^2}\partial^2 - x.$$

* Corresponding author.
E-mail addresses: compoint@agat.univ-lille1.fr (É. Compoint), weil@unilim.fr (J.A. Weil).
[1] During the preparation of this paper, the author was on leave at INRIA, Projet CAFÉ, Sophia Antipolis, France.

0021-8693/$ – see front matter © 2004 Published by Elsevier Inc.
doi:10.1016/j.jalgebra.2003.11.010

One can show that the operator L is irreducible as an element of the ring $\mathcal{D}$. However, if we view L as an element of the ring $\mathcal{D} \otimes k(\sqrt{x}\,) = k(\sqrt{x}\,)[\partial]$, then we obtain

$$L = \tilde{L}_1 L_1 = \left(\partial^2 - \frac{1}{x}\partial + \frac{3}{4x^2} + \sqrt{x}\right)\left(\partial^2 - \sqrt{x}\,\right). \qquad (*)$$

So the operator L, irreducible over k, becomes reducible over $\bar{k}$ (i.e., over $\mathcal{D} \otimes_k \bar{k}$). Such an operator is called *absolutely reducible*[2] (see below for a precise definition). One can check that the above factorization is an *absolute factorization* in the sense that the operators $\tilde{L}_1$ and L_1 are absolutely irreducible.

The topic of this paper is the study of absolute factorization: How can one characterize/compute an absolute factorization of such an operator L?

This question is the first step when one wants to compute the differential Galois group G of a differential operator L. In the known strategies for computing G, the first step consists in finding an absolute factorization (see [12,24]).

We should first note that, from a theoretical point of view, the question of absolute factorization is solved in [12]. The method of [12] is complete (and theoretically operational). However, it is based on the (delicate) search of algebraic solutions of some big linear differential system constructed from the operator. We rather propose to reduce the question to the (much easier) problem of finding solutions with algebraic logarithmic derivatives to ancillary operator of lower order than in [12]. To achieve this, we will study carefully the structural consequences of absolute factorization on the differential Galois group and give a more efficient approach to absolute factorization.

As a test case, we may think of the case when an irreducible $L \in \mathbb{C}(x)[\partial]$ admits a factor of order one: $L = M \circ (\partial - u)$ with $\partial = d/dx$, $M \in \overline{\mathbb{C}(x)}[\partial]$, and u algebraic over $\mathbb{C}(x)$. Such factors have long been studied; there actually exist algorithms [13,22,40] that decide if u exists and, if so, compute the minimum polynomial of u.

These algorithms are based on the remarkable fact that one can provide *a priori* a finite list $\mathcal{L}_n$ of integers (which depends only on the order n of the operator L) such that: if L factors as $L = \widetilde{M} \circ (\partial - \tilde{u})$ with $\tilde{u}$ algebraic, then it must factor as $L = M \circ (\partial - u)$ with $d := \deg(u) \in \mathcal{L}_n$. For example (see Appendix B for more), for $n = 2$ one has $d \in \{2, 4, 6, 12\}$, for $n = 3$ one has $d \in \{3, 6, 9, 21, 36\}$, etc.

In this article, we generalize this method. We show that an irreducible $L \in \mathcal{D}$ has a factor of order r over $\bar{k}$ only if it has such a factor over an extension of degree belonging to $\mathcal{L}_{n/r}$ (Proposition 3) and then give an algorithm (Section 3.2) to obtain a *decomposition* of L into absolutely irreducible factors.

To achieve this, our main tool is differential Galois theory. We translate the (absolute) reducibility properties of L in terms of representation of its differential Galois group. A standard theorem of Clifford leads (as in the works of Singer and Ulmer on first order factors) to a dichotomy between *primitive* and *imprimitive* representations of the differential Galois group (see definitions in page 80). To handle the primitive case (the imprimitive case then being an easy induction), we develop on work of Katz to study

[2] Also sometimes called *Lie-reducible* in the literature.

a "Galoisian descent" process for (suitable) differential operators with coefficients in an algebraic extension of $\mathbb{C}(x)$. We reprove Theorem 2 (from [24]) that, in this case, one can write $L \simeq M \otimes N$ where $M, N \in \mathcal{D}$, M is absolutely reducible, and N has a basis of algebraic solutions. We then explore what this decomposition implies on the Galois group and how to actually deduce absolute factorizations (in particular the degree lists). How to effectively achieve the descent and compute M will appear in subsequent work.

This article is structured as follows. In the first part, we characterize absolute reducibility in terms of representations of the group G. We particularly develop the primitive case and the descent process. In the second part, we study the impact of absolute factorization on the differential Galois group. In the third part, we deduce from this a list of possible degrees and use representation theory to elaborate an effective method for computing absolutely irreducible factors of L.

To conclude this introduction, let us mention cases where absolute factorization is handled in the literature. First consider a linear differential equation $Ly = 0$ with only two singularities 0 being a regular one and ∞ being an irregular one. Under these hypotheses, Beukers, Brownawell and Heckman [5, Corollary 3.3], give conditions for the operator L to be absolutely ("Lie" in their language) irreducible. This condition is easily read on the monodromy at 0 and uses the fact that the (global) monodromy group is generated by the local monodromy at 0 in this case. Beukers, Brownawell and Heckman apply this criterion to confluent hypergeometric operators that enter this frame (Katz and Gabber [24] independently obtain analogous results for this family). Also, works that compute Galois groups of differential operators of given order contain lots of material about absolute reducibility for example [38] (operators of order 2 and 3) and [18] for operators of order 4, now followed by [13,17].

1. Group-theoretic characterizations of absolute reducibility

Throughout this paper, we assume that the reader has a working knowledge of differential Galois theory. The main reference for this is now [31]. Alternative introductions are for example [3,6,27,28,30,37]. Notions on factorization and Liouvillian solutions are recalled in the appendices, mainly to fix notations as we use these notions a lot.

1.1. Notations and conventions

Let k be an ordinary differential field of characteristic zero, and call C its field of constants. Let $L \in \mathcal{D} = k[\partial]$ be a differential operator of order n:

$$L = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0 \in \mathcal{D}.$$

Throughout the paper, the following convention will be used: when a capital letter comes subscripted, it means that the subscript refers to a differential operator it is attached to. For example, K_L will denote the Picard–Vessiot extension of k associated to L (a minimal differential field extension of k generated by solutions of L); V_L will denote the solution space of L in K_L, and G_L will denote the differential Galois group of K_L over k

(the group of k-automorphisms of K that commute with the derivation). The action of G_L on V_L induces a matrix representation of G_L in $GL(n, \mathbb{C})$ that we fix once for all; often, the group will be identified with this representation in $GL(V_L)$. From now on, we assume that L is irreducible in $\mathcal{D}$ (i.e., there are no proper G_L-invariant subspaces of V_L).

Definition 1. Let $L \in \mathcal{D} = k[\partial]$ be an irreducible differential operator of order n.

We say that L is *absolutely reducible* if it factors over an algebraic extension of k. We say that $L_1 \in \bar{k}[\partial]$ is an *absolute factor* of L if L_1 is a factor of L over an algebraic extension of L and L_1 is absolutely irreducible. We say that (the action of) its differential Galois group G_L is *absolutely reducible* if there is a normal subgroup H of finite index such that H acts reducibly on V_L (equivalently: if the connected component of the identity G° acts reducibly on V_L). The representation V_L of G_L is called *imprimitive* if it is irreducible and if there exist an integer $t > 1$ and subspaces $W_1, \ldots, W_t$ of V_L such that $V_L = W_1 \oplus \cdots \oplus W_t$ and G_L acts transitively on the set $\{W_1, \ldots, W_t\}$. The set $\{W_1, \ldots, W_t\}$ is called a *system of imprimitivity* for G. The representation is called *primitive* if it is irreducible and not imprimitive.

In the sequel, we adopt the convention that "system of imprimitivity" will always refer to a system of imprimitivity where the blocks W_i have minimal dimension with respect to this property. If $\dim(W_i) = 1$ then (the representation of) the group is called *monomial*. We will see (Lemma 1) that L is absolutely reducible if and only if G is.

Throughout this section, L is assumed to be *irreducible over* k but *reducible over* k_1, where k_1 denotes an algebraic extension of k. Let $L_1 \in k_1[\partial]$ denote a factor of L over k_1. The following lemma is a trivial exercise in differential Galois theory. We include a proof mainly to set notations.

Lemma 1. *The operator L is reducible over a Galoisian algebraic extension k_1 of k if and only if there exists a normal subgroup $H \lhd G$ of finite index such that H acts reducibly on V_L.*

Proof. Assume such an H exists. Let $V_1 \subset V_L$ be a non-trivial H-invariant subspace of minimal dimension and let k_1 denote the fixed field of H. Because H is of finite index, k_1 is a (Galoisian) algebraic extension of k. By [36, Lemma 1], V_1 is then the solution space of an operator L_1 with coefficients in k_1. Now, as $V_1 \subset V_L$, L_1 is a factor of L.

Conversely, let $L_1 \in k_1[\partial]$ denote a factor of L over k_1. We call Γ_1 the Galois group of k_1 over k. Then Γ_1 acts on the coefficients of L_1. Let L_i, for $i = 1, \ldots, m$, denote the conjugates of L_1 under this action. Obviously, they are again factors of L hence their solution spaces V_i are subspaces of V. Let $H := \bigcap_{i=1,\ldots,m} \mathrm{Stab}_G(V_i)$. The group G has a permutation action on the set $\{V_1, \ldots, V_m\}$; H is the kernel of this permutation representation, and hence a normal subgroup of finite index. □

Remark 1. Note that the index of H in G gives the degree of k_1 but not the degree of a factor in general. To see this, let u_1 denote an element algebraic of degree 3 over k such that its minimum polynomial has Galois group S_3. Let L denote the Least Common Left Multiple (LCLM, see [31]) of $L_1 := \partial - u_1$ and its conjugates $\partial - u_2$ and $\partial - u_3$. Obviously,

L_1 is defined over an algebraic extension of degree 3 whereas (in the above notations), the permutation representation is S_3 and hence $[G : H] = 6$ and $k_1 = k(u_1, u_2, u_3)$.

The above construction on H is the first step towards the following well-known theorem of Clifford:

Theorem 1 (Clifford [9]). *Let $G \in GL_n(C)$ be a linear algebraic group acting irreducibly on $V = C^n$. Assume that G has a normal subgroup H of finite index acting reducibly on V. Then*

(1) *One can decompose V as $V = W_1 \oplus \cdots \oplus W_t$ with the W_i being H-modules all having the same dimensions* (*hence* $\dim(W_i)$ *divides* n) *and such that G permutes the W_i transitively.*
(2) *For each i, one can decompose the W_i as $W_i = \bigoplus_j V_{i,j}$ where the $V_{i,j}$ are irreducible and isomorphic H-modules.*

The W_i are called the homogeneous components of V viewed as an H-module (see Definition 49.5 in [14]). If $t > 1$ then the representation V_L of G is imprimitive. If $t = 1$, then the representation can be imprimitive or primitive but it is *H-isotypical*, i.e., all irreducible H-modules in V are isomorphic. Note that under the hypotheses of Clifford's theorem all the irreducible H-modules have the same dimensions.

We will say that a differential operator L is primitive (respectively imprimitive) if the representation of its differential Galois group G_L on its solution space V_L is primitive (respectively imprimitive). The above theorem shows how L can be written as a Least Common Left Multiple of an absolute factor and its conjugates.

Remark 2. If G is primitive and if $\widetilde{H}$ is *any* normal subgroup of finite index, then the representation is $\widetilde{H}$-isotypical.

Remark 3. If n is prime, then the above results close the problem of absolute factorization as the only possible factors will be of order 1. Factors of order 1 over algebraic extensions have long been studied; lists of possible degrees and algorithms to compute such factors are known (see Appendix B).

Because the imprimitive case can be viewed as a block of primitive cases, we will first start analyzing the primitive case and then will use it for an induction in the imprimitive case. The descent process described in Section 1.3 will rule the primitive case and some imprimitive cases, the other ones then appearing as induction cases.

1.2. The absolute stabilizer $\widetilde{H}$

Let L_1 denote an absolute factor of L, and V_1 its solution space in K_L. For $i = 1, \ldots, m$, let L_i denote the conjugates of L_1, i.e., its images under Galois action on the coefficients of L_1. We let $H := \bigcap_{i=1}^{m} \mathrm{Stab}_G(V_i)$ as above. The fixed field k_1 of H in K_L is a *splitting field* for L, in the sense that L is an LCLM of absolutely irreducible operators over k_1 (see

[12] for more on splitting fields for differential operators.)[3] One may wonder whether H and k_1 depend on the initial choice of V_1. If the group is primitive, we will see that it does not. However, if the group is imprimitive, then H may depend on the choice of V_1. We now introduce a subgroup which canonically describes the absolute factorization. Some of the V_i may be isomorphic G°-modules. In this case, we denote $\phi_{i,j}$ a G°-isomorphism between V_i and V_j.

Definition 2. The group

$$\widetilde{H} = \{ g \in G \mid g(V_i) = V_i \text{ and } g \circ \phi_{i,j} = \phi_{i,j} \circ g \}$$

is called the *absolute stabilizer* in G (with respect to the representation on V).

Note that, in the primitive case, the representation V is H-isotypical so $H = \widetilde{H}$. The fact that this group $\widetilde{H}$ does not depend on its construction (i.e., it is canonical) follows from the following lemma:

Lemma 2. *Any G°-module in V_L is an $\widetilde{H}$-module. Moreover, isomorphic G°-modules are isomorphic $\widetilde{H}$-modules.*

Proof. Let us choose, among the conjugates of V_1, some G°-modules $V_{1,1}, \ldots, V_{1,s}, \ldots, V_{t,1}, \ldots, V_{t,s}$ such that V is the direct sum of those $V_{i,j}$ and, for all j, k, we have $V_{i,j}$ and $V_{i,k}$ are isomorphic as G°-module (and also as $\widetilde{H}$-module by definition). Let W be any G°-irreducible module. Then W is G°-isomorphic to one of the $V_{i,j}$, say $V_{1,1}$ up to renumbering. Goursat's lemma (e.g., Lemma 2.2 in [11]) then implies that there exist constants $c_2, \ldots, c_s$ such that

$$W = \{ y + c_2\phi_{1,2}(y) + \cdots + c_s\phi_{1,s}(y) \mid y \in V_{1,1} \}$$

as a G°-module. Now, as the $\phi_{1,j}$ commute with $\widetilde{H}$, we see that W is an $\widetilde{H}$-module. Moreover, the projection $y + c_2\phi_{1,2}(y) + \cdots + c_s\phi_{1,s}(y) \mapsto y$ is an $\widetilde{H}$-isomorphism from W to $V_{1,1}$. It follows that any two isomorphic G°-modules are also isomorphic $\widetilde{H}$-modules—independently of the initial choice of V_1 and of the $\phi_{i,j}$. $\square$

Remark 4. As pointed out to us by M.F. Singer, if we let $\mathcal{K} = \mathrm{End}_{G^\circ}(V_L)$, then $\mathrm{End}_{\mathcal{K}}(V_L) = C[G^\circ]$ (Jacobson's theorem [26, Chapter XVII, Section 3]) and we obtain that $\widetilde{H} = C[G^\circ] \cap G$. For example, if G is a finite group, this shows that $\widetilde{H}$ is a central cyclic subgroup.

[3] The *splitting* fields are called *decomposition* fields in [12].

Example. To understand better why this group $\widetilde{H}$ has to be introduced, consider the representation in SL_2 of the quaternion group. This is a group of order 8 generated by the matrices

$$M_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

If y_1, y_2 denote the basis of V on which these matrices are expressed, we see that the lines V_i generated by the y_i are permuted by the group. Their stabilizer H is the group of four elements generated by M_1. However, the action of M_1 on V_1 is multiplication by i and the action on V_2 is multiplication by $-i$ so V_1 and V_2 are non-isomorphic H-modules. Because the group is finite, $G^\circ = \{\mathrm{Id}\}$ so of course any line is a G°-module but it is not, in general, an H-module. The group $\widetilde{H}$, in this example, is easily seen to be $\widetilde{H} = \{\mathrm{Id}, -\mathrm{Id}\}$ and, of course, any line is indeed an $\widetilde{H}$-module.

1.3. Descent and absolute factorization

In the paper [9], Clifford shows that, in the case of a primitive absolutely reducible group, each matrix in the group can be written as a tensor products of two matrices. This yields a representation of the group as a tensor product of two *projective* representations (and *not* subrepresentations).

A different approach, and the heart of our analysis, will be to establish (and develop on) the forthcoming theorem of Katz [24, trichotomy page 45], on absolute factorization in the case of isomorphic absolute factors. We will give a complete proof of this result, the interest being that we will recast its two main steps in a setting that will be used for extending and clarifying some of its consequences.

The object of the next subsection will be a descent theory for differential operators over $\mathbb{C}(x)$. The fact that our base field is $\mathbb{C}(x)$ (or an algebraic extension of it, see Corollary 2) plays an essential role there as we will use the fact that certain 2-cocycles will be trivial. We follow closely the argument of Katz in this first part. We will then prove Katz's theorem, giving a proof that seems more elementary to us and that sheds more light on the underlying group-theoretic consequences of the result; it will help establish some corollaries, like Proposition 3.

1.3.1. Descent theory for differential operators

Let $k = \mathbb{C}(x)$ denote the (cohomologically trivial) base field. Recall [31,36] that two operators L_1 and L_2 in $k_1[\partial]$ are called *isomorphic* (or equivalent) over a field $\widetilde{k_1}$ if $\mathrm{ord}(L_1) = \mathrm{ord}(L_2)$ and there exist $R, S \in \widetilde{k_1}[\partial]$ of order less than $\mathrm{ord}(L_2)$ such that $L_1 R = SL_2$ (or, equivalently, if the associated differential modules are isomorphic). The operator R can then be seen as a representant of the isomorphism from L_2 to L_1. We say that L_1 and L_2 are *projectively equivalent* if there exists $r \in k$ such that L_1 is equivalent to $L_2 \otimes (\partial - r)$.

Definition 3. Let k_1 be a Galois extension of $k = \mathbb{C}(x)$ and let $L_1 \in k_1[\partial]$. We say that L_1 *descends to* k over a field k_0 if k_0 is a Galois extension of k containing k_1 and if there exists an operator $M \in k[\partial]$ such that L_1 is isomorphic *over* k_0 to M.

Let k_1 be a Galois extension of $k = \mathbb{C}(x)$ and let $L_1 \in k_1[\partial]$ be an absolutely irreducible operator. Assume that L_1 is isomorphic (over a Galois extension $\widetilde{k_1}$ of k containing k_1) to all its conjugates. Denote by Γ the Galois group of $\widetilde{k_1}$ over k. For each h in Γ, we denote by L_h the conjugate of L_1 under the action of h on coefficients of L_1. By hypotheses, for each $h \in \Gamma$, there exists an isomorphism ϕ_h of ∂-modules

$$\phi_h:\ L_1 \xrightarrow{\phi_h} L_h.$$

Note that ϕ_h is only defined up to multiplication by a constant. Now, if g is another element in Γ (g acts on ϕ_h by action on the coefficients), we may let g act on the above relation, pushing it to a morphism between L_g and $L_{gh} = g(L_h)$, which leads us to the following diagram

$$\begin{tikzcd} L_1 \arrow[r, "\phi_h"] \arrow[d, "\phi_g"'] \arrow[dr, dashed, "\phi_{gh}"] & L_h \\ L_g \arrow[r, "g(\phi_h)"'] & L_{gh} \end{tikzcd}$$

We see that $g(\phi_h) \circ \phi_g$ and ϕ_{gh} are two isomorphisms between L_1 and L_{gh}. As the L_h operators are assumed to be irreducible, Schur's lemma implies that there exists a non-zero constant $a(h,g)$ such that

$$\phi_{gh} = a(h,g)g(\phi_h) \circ \phi_g. \tag{1}$$

Definition 4. We say that the collection of morphisms $\{\phi_h\}_{h\in\Gamma}$ forms a *descent data* if the constant $a(h,g)$ is always equal to 1, i.e., $\phi_{gh} = g(\phi_h) \circ \phi_g$ for all $g, h \in \Gamma$.

If L_1 descends to an $M \in k[\partial]$ over some field k_0, then existence of a descent data (relatively to $\Gamma_0 = \mathrm{Gal}(k_0/k)$) is clear: letting ϕ denote an isomorphism from L_1 to M over k_0, we may set $\phi_h := h(\phi)^{-1} \circ \phi$ for $h \in \Gamma_0$ and it is easily checked that the $\{\phi_h\}_{h\in\Gamma_0}$ form a descent data (because M is defined over k)

$$\begin{tikzcd} L_1 \arrow[rr, "h(\phi)^{-1}\circ\phi"] \arrow[dr, "\phi"'] & & L_h \arrow[dl, "h(\phi)"] \\ & M & \end{tikzcd}$$

The converse is a bit more sophisticated. In [45] for varieties and [15,16] in the general case (see also Chapter III of [33] for explanations on this topic), it is shown that the existence of a descent data guarantees the existence of the descent. Indeed[4] assume we have descent

[4] We are grateful to Michael F. Singer for showing us this (classical) proof, see also [21].

data $\{\phi_h\}_{h\in\Gamma_0}$. The descent conditions show that the map $c : h \mapsto \phi_h$ induces a 1-cocycle in $H^1(\Gamma_0, GL_n(k_0))$. The latter is known to be trivial (e.g., [41, Chapter 11]) so there exists $\phi \in GL_n(k_0)$ such that $c(h) = h(\phi^{-1})\phi$. It is easily verified that the image of L_1 under ϕ is invariant under Γ_0 and hence has coefficients in k (i.e., it is a descent of L_1).

Lemma 3 [24, 2.7.3]. *Let k_1 be an algebraic Galois extension of $\mathbb{C}(x)$ and let $L_1 \in k_1[\partial]$ irreducible and isomorphic (over a Galois extension $\widetilde{k_1}$ of $\mathbb{C}(x)$ containing k_1) to all its conjugates. Assume that L_1 is absolutely irreducible. Then, there exists a Galois extension k_0 of $\mathbb{C}(x)$ containing $\widetilde{k_1}$ and an operator $M \in \mathbb{C}(x)[\partial]$ such that L_1 is isomorphic over k_0 to M.*

Proof. As explained above, the proof will consist in the construction of a descent data.

The set of constants $a(h, g)$ from relation (1) is easily seen to induce a 2-cocycle $a : \Gamma \times \Gamma \to \mathbb{C}^*$, $(h, g) \mapsto a(h, g)$. If a is trivial (i.e., if we can find a 1-cocycle $b \in H^1(\Gamma, \mathbb{C}^*)$ such that $a(h, g) = b(h)b(g)/b(gh)$) then we can construct descent data $\widetilde{\phi_h} := b(h)\phi_h$ and our problem is solved. We will show that, at the cost of considering L_1 over a Galois extension k_0 of $\mathbb{C}(x)$ containing $\widetilde{k_1}$, the 2-cocycle a can be made trivial, hence the conclusion of the lemma.

As Γ is finite of some order m, the 2-cocycle a^m is trivial (see [23, Proposition 7.3, page 61]) so, up to multiplying the ϕ_h by a suitable constant, we may assume that a has values in the group μ_m of mth roots of unity, i.e., $a \in H^2(\Gamma, \mu_m)$.

Let $\mathcal{G} := \mathrm{Gal}(\overline{\mathbb{C}(x)}/\mathbb{C}(x))$ denote the absolute Galois group of $\mathbb{C}(x)$, i.e., the projective limit of Galois groups of algebraic extensions of $\mathbb{C}(x)$. The group $H^2(\mathbb{C}(x), \mu_m) := H^2(\mathcal{G}, \mu_m)$ is an Abelian torsion group, hence it is a direct product of its p-primary components. The p-primary component of $H^2(\mathbb{C}(x), \mu_m)$ identifies to $H^2(\mathbb{C}(x), (\mu_m)_p)$, where $(\mu_m)_p$ is the p-primary component of μ_m [33, proof of Proposition 11 in §I.3]. Now, Tsen's theorem shows that $\mathbb{C}(x)$ (and more generally any field of transcendence degree 1 over $\mathbb{C}$) has cohomological dimension $\leqslant 1$ (see [33, Example 3.3, page II.10]). Proposition 11(ii) of §I.3 in Serre shows that $H^2(\mathbb{C}(x), (\mu_m)_p) = 0$ for all prime p, hence we have $H^2(\mathbb{C}(x), \mu_m) = 0$.[5] But

$$H^2(\mathcal{G}, \mu_m) = \varinjlim H^2(\mathcal{F}, \mu_m)$$

where the inductive limit is taken on the Galois groups $\mathcal{F}$ of finite extensions of $\mathbb{C}(x)$. Viewed as an element of the trivial group $H^2(\mathbb{C}(x), \mu_m)$, the 2-cocycle a must be trivial. So, by definition (of the inductive limit), there exists a Galois extension k_0 of $\mathbb{C}(x)$ with Galois group Γ_0 such that a is trivial *as an element of* $H^2(\Gamma_0, \mathbb{C}^*)$. We then can construct a descent data *over* k_0 and L_1 is isomorphic over k_0 to an operator M with coefficients in $\mathbb{C}(x)$. $\square$

Remark 5. Note that the isomorphisms between L_1 and its conjugates are defined over $\widetilde{k_1}$ and hence the isomorphisms involved in the descent data are defined over $\widetilde{k_1}$. However,

[5] This remains true if we replace $\mathbb{C}(x)$ by an algebraic extension of $\mathbb{C}(x)$, see Corollary 2 below.

if Γ is "not big enough," there may not be "enough" isomorphisms to have the descent conditions realized. Indeed, introducing the overfield k_0 means that we take a bigger Galois group, hence more isomorphisms and more freedom to obtain descent conditions. As we will see in Section 2, this introduction of k_0 is not artificial and is sometimes really needed to achieve the descent. We will indeed show how to control the descent field (the one over which the descent conditions are satisfied, see Corollary 3).

1.3.2. Absolute factorization and tensor products

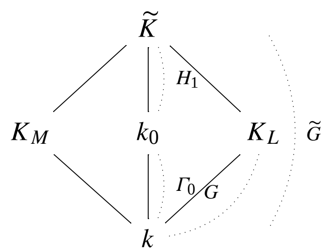
Building on this descent lemma, Katz shows in [24] the following variant on Clifford's second theorem [9]. If M, N are differential operators, we call $M \otimes N$ the differential operator whose solution space is spanned by the products $y_i f_j$ of solutions y_i of M and f_j of N, respectively. If $\mathcal{M}$, $\mathcal{N}$ are the differential modules associated to M and N, then $M \otimes N$ is an operator associated to $\mathcal{M} \otimes \mathcal{N}$ [31].

Theorem 2 [24]. *Let $L \in \mathbb{C}(x)[\partial]$ be an irreducible operator. We assume that L admits factors $L_1, \ldots, L_s$ with coefficients in an algebraic extension k_1 of $\mathbb{C}(x)$ such that*:

(1) *The L_i are all the conjugates of L_1 (and are also absolutely irreducible).*
(2) *The L_i are pairwise isomorphic over $\overline{\mathbb{C}(x)}$.*

Then there exists operators M and N in $\mathbb{C}(x)[\partial]$ such that M is absolutely irreducible and isomorphic over $\overline{\mathbb{C}(x)}$ to L_1, N has a finite Galois group, and L is isomorphic over $\mathbb{C}(x)$ to the tensor product $M \otimes N$.

Proof. The first step in the proof of this theorem is the descent Lemma 3. Under the hypotheses of the theorem, the operator L_1 is isomorphic to all its conjugates. By Lemma 3, there exists an operator $M \in \mathbb{C}(x)[\partial]$ and a Galois extension k_0 of $\mathbb{C}(x)$ such that M is isomorphic to L_1 over k_0. As L_1 is absolutely irreducible, so is M. Let $F_1 \in \mathbb{C}(x)[\partial]$ be a differential operator admitting k_0 as a Picard–Vessiot extension (see, e.g., [32] for a construction of such a differential operator). Let $\tilde{L}$ denote the LCLM of operators F_1 and M. We have $\tilde{L} \in \mathbb{C}(x)[\partial]$ and the Picard–Vessiot extension $\widetilde{K}$ of $\mathbb{C}(x)$ associated with $\tilde{L}$ contains the Picard–Vessiot extensions k_0 and K_M. A direct consequence is that $\widetilde{K}$ also contains $K_{L_1}, \ldots, K_{L_s}$ and thus contains K_L. This can be sketched as



We let H_1 denote the differential Galois group of $\widetilde{K}$ over k_0. As M and L_1 are isomorphic over k_0, the solution spaces V_M and V_{L_1} in $\widetilde{K}$ of the equations $My = 0$ and

$L_1 y = 0$ are isomorphic H_1-modules. As H_1 is normal in $\widetilde{G}$, the set $\mathrm{Hom}_{H_1}(V_M, V_L)$ of H_1-module homomorphisms from V_M to V_L is a $\widetilde{G}$-module (the action being defined by $\tilde{g}.\phi = \tilde{g}\phi\tilde{g}^{-1}$). Now, one easily checks that the application

$$\psi : V_M \otimes \mathrm{Hom}_{H_1}(V_M, V_L) \to V_L, \quad v \otimes \phi \mapsto \phi(v)$$

is a morphism of $\widetilde{G}$-modules. Moreover, it is surjective: $\mathrm{Im}(\psi) = V_L$ because V_L is an irreducible $\widetilde{G}$-module and $\psi \neq 0$. Let us compare dimensions of these two $\widetilde{G}$-modules. We have $V_L = V_{L_1} \oplus \cdots \oplus V_{L_s}$, with $\dim(V_{L_1}) = \cdots = \dim(V_{L_s}) = r$. For all $i \in \{1, \ldots, s\}$, V_M and V_{L_i} are isomorphic and irreducible H_1-modules, hence $\dim \mathrm{Hom}_{H_1}(V_M, V_L) = s$. It follows that $\dim(V_M \otimes \mathrm{Hom}_{H_1}(V_M, V_L)) = \dim V_L$, thus ψ is an isomorphism of $\widetilde{G}$-modules.

Let now $N \in \mathbb{C}(x)[\partial]$ be a differential operator whose solution space in $\widetilde{K}$ is ($\widetilde{G}$-isomorphic to) $\mathrm{Hom}_{H_1}(V_M, V_L)$. By definition all solutions of $Ny = 0$ in $\widetilde{K}$ are fixed by H_1, and thus are algebraic over k. So N must have a finite Galois group. Moreover, as the three operators M, N and L have their Picard–Vessiot extension in $\widetilde{K}$, the isomorphism ψ imposes that L is isomorphic over k to the tensor product $M \otimes N$. □

Remark 6. The operators M and N in Katz's theorem are far from unique: they are defined up to tensoring by an order 1 operator of the form $\partial - f$. Lemma 3 ensures the existence of a descent but gives no indication, like degrees, on the descent morphism (or how to compute such descent). These questions are addressed in Section 2 of this paper.

Remark 7. Under hypothesis of Theorem 2, the order of the operator $M \otimes N$ is $\mathrm{order}(M).\mathrm{order}(N)$. In other words, there is no non-trivial linear relation with coefficients in $\mathbb{C}$ between $\{m_i.n_j\}$ where $\{m_i\}$ and $\{n_j\}$ are bases of solutions of M and N. Indeed M is absolutely irreducible so the $\{m_i\}$ are linearly independent over any algebraic extension of $\mathbb{C}(x)$ [10,11].

From the structure of our proof, we see that we may establish a number of corollaries.

Corollary 1. *If a differential operator $L \in \mathbb{C}(x)[\partial]$ has a primitive absolutely reducible differential Galois group, then the hypotheses (and conclusion) of Katz's theorem hold.*

Proof. Because the group is primitive, the representation V_L is G_0-isotypical and even H-isotypical (with the construction from Section 1.2) and hence the hypotheses of Katz's theorem are satisfied: the L_i are defined and isomorphic over k_1 (because k_1 is the fixed field of H and the representation is H-isotypical). We thus see that $L \simeq M \otimes N$. □

For the study of the imprimitive case, we will need the following easy corollary.

Corollary 2. *Katz's theorem also holds if the base field k is a finite extension of $\mathbb{C}(x)$.*

Proof. The key step for Katz's theorem (the descent) holds if $H^2(k, \mathbb{C}^*)$ is trivial, where k is the base field. A finite extension of a field of cohomological dimension $\leqslant 1$ is a field of cohomological dimension $\leqslant 1$ (Tsen's theorem [33, ex. 3.3, page II.10]). If we replace $\mathbb{C}(x)$ with a finite extension k, then $H^2(k, \mathbb{C}^*)$ is still trivial and the 2-cocycles can be trivialized as in the proof of the descent Lemma 3. □

We now turn to the question of the (non)-unicity of the descent. Obviously, if $M \in k[\partial]$ is a solution to the descent problem, then any operator equivalent over k to M is also a solution; note also that the result $L \simeq M \otimes N$ defines M only up to projective equivalence, even though M itself is defined up to equivalence in the descent process.

The next lemma investigates the number of solutions to the descent problem. This type of result is standard in descent theory.

Proposition 1. *Same hypotheses and notations as in Katz's descent Lemma* 3. *Let k_0 denote the descent field and $\Gamma_0 = \mathrm{Gal}(k_0/k)$. Then*

(1) *To any descent data $\{\phi_h\}_{h \in \Gamma_0}$ corresponds a unique* (*up to k-equivalence*) *operator M equivalent over k_0 to L_1.*
(2) *The number of descent data over k_0* (*and hence of equivalence classes of solutions M to the descent problem*) *is the order of the group* $\mathrm{Hom}(\Gamma_0, \mathbb{C}^*)$ *of the homomorphisms from Γ_0 to $\mathbb{C}^*$.*

Proof. Part (1) is simple and well known. Let $\{\phi_h\}_{h \in \Gamma_0}$ denote descent data and let M and $\widetilde{M}$ denote two descents of L_1 associated with $\{\phi_h\}_{h \in \Gamma_0}$: this means that there are morphisms f from L_1 to M (respectively $\tilde{f}$ from L_1 to $\widetilde{M}$) such that $\phi_h = h(f).f^{-1} = h(\tilde{f}).\tilde{f}^{-1}$. It follows that $h(f.\tilde{f}^{-1}) = f.\tilde{f}^{-1}$ for all $h \in \Gamma_0$ and hence the isomorphism $f.\tilde{f}^{-1}$ between M and $\widetilde{M}$ is defined over k. In our setting, we consider $H^1(\Gamma_0, \mathbb{C}^*)$ with a trivial action of Γ_0 on $\mathbb{C}^*$, so $H^1(\Gamma_0, \mathbb{C}^*) = \mathrm{Hom}(\Gamma_0, \mathbb{C}^*)$ and the result follows from the introduction to Chapter III of [33]. □

We will come back to the descent problem and its impact on the Galois group in Section 2.

1.4. Imprimitive differential operators

We now study the structure of an *imprimitive* differential operator $L \in k[\partial]$ with $k \subset \overline{\mathbb{C}(x)}$. Again, let K_L denote the Picard–Vessiot extension of k associated to L, V_L the solution space in K_L, and G_L the differential Galois group. Let $(W_1, \ldots, W_t)$ denote a system of imprimitivity for G_L (precisely: for the representation of G_L on V_L):

$$V_L = W_1 \oplus \cdots \oplus W_t$$

and G_L permutes the W_i transitively. Let S denote the stabilizer in G of the family $\{W_1, \ldots, W_t\}$: $S := \bigcap \mathrm{Stab}_G(W_i)$. Then S is a normal subgroup of finite index in G_L which acts reducibly on V_L so we see immediately that L already factors over an extension of degree t of the base field k.

Each W_i is a primitive S-module (by minimality of the dimensions of the W_i). For $i \in \{1, \dots, t\}$, we let L_i denote the monic differential operator with coefficients in $K_L^S \subset \bar{k}$ whose solution space is W_i. Note that, though K_L^S is an extension of degree at most $(t!)$ of k, each L_i has its coefficients in a subextension of degree t of k. Our L is the LCLM of the operators $L_1, \dots, L_t$ and each L_i is primitive.

Now assume that $k = \mathbb{C}(x)$ (or a finite extension of it so that the results of the previous section apply). By Theorem 2 and Corollary 2, either L_i is absolutely irreducible or it admits a factorization as a tensor product $L_i = M_i \otimes N_i$ where M_i and N_i have coefficients in the coefficient field k_i of L_i, M_i is absolutely irreducible, and N_i has a finite primitive Galois group.

2. Structure of the Galois group in the descent case

In this section, we place ourselves in the notations and descent hypotheses from Theorem 2 and investigate the consequences of the descent on the Galois group. We also show how to measure the degree of the descent morphism and of the morphisms between the conjugate differential operators L_i.

We first investigate, as a test case, the (easy) case of first order operators.

2.1. *The descent for first order operators*

In the case of a first order operator $\partial - u$ with u algebraic, then the descent process can be explained in a more explicit way. Let $L_1 = \partial - u_1$ be a first order differential operator with coefficients in an algebraic extension of $\mathbb{C}(x)$. Assume that L_1 descends to an operator $M = \partial - f \in \mathbb{C}(x)[\partial]$, i.e., there exists a non-zero element ϕ_1 algebraic over $\mathbb{C}(x)$ such that $(\partial - u_1).\phi_1 = \phi_1.M$. Then a simple computation shows that we must have $u_1 = f + \phi_1'/\phi_1$ with ϕ_1 algebraic. This in turn implies that ϕ_1 is radical over $k(u_1)$, i.e., there exists $d \in N$ such that $\phi_1^d \in k(u_1)$. Equivalently, there exists $\psi_1 \in k(u_1)$ such that $u_1 = f + \psi_1'/d\psi_1$. Using the integration algorithm on algebraic curves [1,4,7,12,42], one can decide if this is the case and compute f, d, ψ_1. Conversely, if $u_1 = f + \phi_1'/\phi_1$ with $f \in k$ and ϕ_1 algebraic over k, then L_1 obviously descends to $\partial - f$ over $k(\phi_1)$.

Example. Let u denote a root of $u^3 - u - x = 0$ and let

$$L_1 = \partial - \frac{4u^2 - 6ux + 5x^2 + 27x^4 - 4}{x(-4 + 27x^2)}.$$

The integration algorithm shows that

$$\frac{4u^2 - 6ux + 5x^2 + 27x^4 - 4}{(-4 + 27x^2)x} = x + \frac{\psi_1'}{3\psi_1} \quad \text{with } \psi_1 = u + x.$$

We see that $L_1.\phi_1 = \phi_1.(\partial - x)$ with ϕ_1 given by $\phi_1^3 = u + x$.

Let M^* denote the dual (or adjoint) of M. Now ϕ_1 is an algebraic solution of $L_1 \otimes M^*$ and the latter descends to ∂. So, we see that, a first order operator admits descent if and only if, up to tensoring over k by a first order operator, it admits descent to ∂. The descent morphism is then multiplication by a solution ϕ_1, whose degree over $k(u_1, u_2, \ldots)$ can again be measured using the integration algorithm; and the isomorphisms between $\partial - u_i$ and $\partial - u_j$ are multiplication by ϕ_i/ϕ_j (which obviously satisfy the descent conditions).

We may remark now, that, because ϕ_1 is an algebraic solution of an equation $y' = u_1 y$, we have $\phi_1^d \in k(u_1)$ for some number d (measured by the integration algorithm). Moreover, there exists a (smaller) number $\bar{d}$ such that $\phi_1^{\bar{d}} \in k_1 = k(u_1, u_2, \ldots)$. A method for measuring this degree $\bar{d}$ is given in [12, Proposition 2.4].

2.2. *Degree for the descent and for the algebraic equivalence*

Throughout this section, we assume that $L \simeq_k M \otimes N$ with L irreducible, M absolutely irreducible of order r, N of order $s = n/r$ with a finite Galois group. Recall (see Appendix B) that we then have $N = \mathrm{LCLM}(\partial - u_1, \ldots, \partial - u_m)$ with the u_i algebraic and conjugate, whose degree m can be picked from a precomputed list $\mathcal{L}_s$ (i.e., m depends uniformly on s). Moreover there exist algebraic functions f_i satisfying $f_i' = u_i f_i$. Note that we may, without loss of generality, assume that N is unimodular. Indeed, write $N = \partial^s + a_{s-1}\partial^{s-1} + \cdots$ and let ω denote the Wronskian of N. As G_N is finite, ω is algebraic over k and hence $N \otimes (\partial - (a_{s-1})/s)$ has a finite unimodular Galois group. Evidently, $M \otimes N \simeq_k (M \otimes (\partial + (a_{s-1})/s)) \otimes (N \otimes (\partial - (a_{s-1})/s))$ so, in the sequel, we assume that G_N is unimodular.

We now will show the link between this structure of N and the degrees for an absolute factor L_1 of L, for the associated descent morphism, and for the equivalence isomorphisms between the L_i.

Lemma 4. *Let $L \in k[\partial]$. Let L_f denote the image of L under the map $\partial \mapsto \partial - f$ in $k[\partial]$. Then $L_f = L \otimes (\partial - f)$.*

Proof. The solutions of $L \otimes (\partial - f)$ are $y.\exp(\int f)$. Now

$$\left(y.\exp\left(\int f\right)\right)' = \exp\left(\int f\right)(\partial + f)(y)$$

Noting that both L_f and $L \otimes (\partial - f)$ are monic and have the same order, this yields the result. □

Theorem 3. *Assume that $L \simeq_k M \otimes N$ with L irreducible, M absolutely irreducible of order r, N of order $s = n/r$ with a finite unimodular*[6] *Galois group. Let u_i be conjugated algebraic functions such that $N = \mathrm{LCLM}(\partial - u_1, \ldots, \partial - u_m)$. Let f_i be non-trivial algebraic functions such that $f_i' = u_i f_i$.*

[6] We saw above that we can impose this without losing generality.

Then L admits a factor $L_1 \in k(u_1)[\partial]$ such that the descent morphism is (in operator form) $R_1 := f_1\widetilde{R_1}$ with $\widetilde{R_1} \in k(u_1)[\partial]$ and the isomorphism between two conjugates L_i and L_j of L_1 is of the form $\phi_{i,j} = (f_i/f_j)\Phi_{i,j}$ with $\Phi_{i,j} \in k(u_i, u_j)[\partial]$.

Proof. By assumption, there exists operators $R, S \in k[\partial]$ such that R has order less than $M \otimes N$ and $L.R = S.(M \otimes N)$. Recall that $N = \mathrm{LCLM}(\partial - u_i,\ i = 1, \dots, m)$. Let m denote the degree of the u_i, chosen minimal.

Let f_i denote a non zero solution of $y' = u_i y$. By construction, there exists measurable integers d and $\bar{d}$ such that $f_i^d \in k(u_i)$ and $f_i^{\bar{d}} \in k_1 = k(u_1, \dots, u_m)$, respectively. Now R maps $V_{M\otimes(\partial-u_1)}$ to a subspace of V_L. Hence, if we let $\overline{R}_1$ denote the remainder of the right division of R by $M \otimes (\partial - u_1)$, then $\overline{R}_1$ maps $V_{M\otimes(\partial-u_1)}$ to a subspace of V_L so there exists a factor $L_1 \in k(u_1)$ of L such that $L_1.\overline{R}_1 = \overline{S}_1.(M \otimes (\partial - u_1))$. The solutions of $M \otimes (\partial - u_1)$ are of the form $z.f_1$ with $M(z) = 0$. Now, we have $(zf_1)' = f_1.(\partial + u_1)(z)$. Hence, by Lemma 4, we see that

$$R(z.f_1) = f_1\big(\overline{R}_1 \otimes (\partial + u_1)\big)(z).$$

Letting $R_1 := f_1(\overline{R}_1 \otimes (\partial + u_1))$, we see that R_1 maps V_M to V_{L_1}. So, we conclude that there exists $S_1 \in k(u_1)(f_1)$ such that $L_1.R_1 = S_1.M$. Moreover, by the irreducibility of V_M and Schur's lemma, any morphism from M to L_1 will be of the form $c.R_1$.

Similarly, $R_2 := f_2(\overline{R}_2 \otimes (\partial + u_2))$. To obtain the inverse of R_2, we write an operator r_2 of order $r - 1$ with indeterminate coefficients. The condition for r_2 to be the inverse of R_2 (viewed as a morphism from V_M to V_{L_2}) is that the remainder of the right division of $r_2.R_2$ by M should be 1. The latter gives linear (non-differential) conditions on the coefficients of r_2 (for which a unique solution exists by construction). In fact, the latter can also be written as

$$f_2\big(r_2 \otimes (\partial + u_2)\big)\big(\overline{R}_2 \otimes (\partial + u_2)\big) = 1 \bmod M,$$

which shows that $R_2^{-1} \in (1/f_2)k(u_2)$. As a consequence, we see that the isomorphism $\phi_{1,2} := R_1.R_2^{-1} \bmod L_2$ has coefficients in $(f_1/f_2).k(u_1, u_2)$ and satisfies $L_1.\phi_{1,2} = \psi_{1,2}.L_2$. □

Remark 8. The result on the $\phi_{i,j}$ can also be seen the following way.

Let k_1 be a Galois extension of k and $\widetilde{k_1}$ a Galois extension of k containing k_1. Let $L_1, L_2 \in k_1[\partial]$ be differential operators, irreducible over $\widetilde{k_1}$ and isomorphic over $\widetilde{k_1}$. Let ϕ denote the isomorphism. For all $g \in \mathrm{Gal}(\widetilde{k_1}/k_1)$, $g(\phi)$ is again an isomorphism between L_1 and L_2 so Schur's lemma implies that there exists a constant c_g such that $g(\phi) = c_g\phi$. It follows that there exist $f \in \widetilde{k_1}$, satisfying $g(f) = c_g f$ for all $g \in \mathrm{Gal}(\widetilde{k_1}/k_1)$, and $\Phi \in k_1[\partial]$ such that $\phi = f.\Phi$. Because $g(f) = c_g f$ for all $g \in \mathrm{Gal}(\widetilde{k_1}/k_1)$, we see that there exists $d \in \mathbb{N}$ such that $f^d \in k_1$.

The disadvantage of this proof is that it gives no information on the possible degrees for f. An analogous remark appears as "rigidity lemma" on page 45 of [24].

Remark 9. Theorem 2, in fact, shows that the hypotheses of the theorem are equivalent to: V_L is G_L-irreducible, G_L°-reducible, and G_L°-isotypical.

So far, $\widetilde{k_1}$ denoted an extension of k_1 over which the operator was isomorphic to its conjugates. It is now natural to study the smallest such field. In the sequel, $\widetilde{k_1}$ is the field generated over k_1 by the coefficients of the morphisms between the L_1 constructed in the above proof and its conjugates. We will show that this does not depend on the choice of L_1.

Corollary 3. *Same hypotheses and notations as in Theorem* 3.

(1) *The coefficient field* $\widetilde{k_1}$ *of the isomorphisms between the* L_j *is in* K_L (*precisely*: $\widetilde{k_1} = K_L^{\widetilde{H}}$).
(2) *The field* $k_0 := K_N = \widetilde{k_1}(f_1)$ *is a descent field. In particular,* K_N *is a cyclic extension of* $\widetilde{k_1}$ *whose degree* (*over* $\widetilde{k_1}$) *divides the order* $s = n/r$ *of* N.

Proof. (1) The coefficients of the L_i are differential functions on their solutions hence $k_1 \in K_L$. Similarly, the morphisms between L_i and L_j are (differential) functions on their solutions so $\widetilde{k_1} \subset K_L$. The Galois correspondence then allows one to check that $\widetilde{k_1}$ is, in fact, the fixed field $K_L^{\widetilde{H}}$ of the absolute stabilizer $\widetilde{H}$ in K_L. The field $\widetilde{k_1}$ hence only depends on the equivalence class of L and not on the choice of absolutely irreducible factors L_i (Lemma 2). We may thus choose $L = M \otimes N$ and $L_i = M \otimes (\partial - u_i)$ without loss of generality.

(2) The above theorem now shows that $k_1 = k(u_1, \ldots, u_m)$, $\widetilde{k_1} = k_1(f_i/f_j)_{i \neq j}$ and immediately $k_0 := \widetilde{k_1}(f_1)$ is a descent field as L_1 and M are (by construction) isomorphic over this k_0. This also shows that $K_N = k_0 = \widetilde{k_1}(f_1)$. Let $g \in \mathrm{Gal}(K_N/\widetilde{k_1})$. As $u_i \in \widetilde{k_1}$, $g(u_i) = u_i$ and so there exists $c_i \in C$ such that $g(f_i) = c_i f_i$. Now, as $g(f_i/f_j) = f_i/f_j$, we have $c_i = c_j$ for all i, j. It follows that g is scalar and hence in the center of G_N. Now, because G_N is unimodular, we must have $g^s = 1$, where $s = n/r$ is the order of N, and thus K_N is a cyclic extension of $\widetilde{k_1}$ whose degree divides s. $\square$

Example. This example was supplied to us by Mark van Hoeij. Let

$$L := \partial^4 + 2\frac{(x-1)\partial^3}{x(x-2)} - \frac{1}{4}\frac{(16x^5 - 80x^4 + 128x^3 - 63x^2 - 2x + 4)\partial^2}{x^2(x-2)^2} - \frac{1}{4}\frac{(32x^4 - 128x^3 + 144x^2 + 1 - 33x)\partial}{x^2(x-2)^2} + \frac{(x-1)(4x^5 - 20x^4 + 32x^3 - 21x^2 + 10x + 2)}{x^2(x-2)^2}.$$

Computation shows that it is irreducible over $\mathbb{C}(x)$ and that it admits the following algebraic factor

$$l_1 := \partial^2 - \frac{1}{2}\frac{\partial}{x-2} - \frac{4x - \sqrt{x} + 2x^3 - 6x^2}{x(x-2)}.$$

It can be shown that the above is absolutely irreducible (for example, by letting $x = t^2$ and checking that the corresponding operator in $\mathbb{C}(t)[d/dt]$ has Galois group G satisfying $G^\circ = SL(2, \mathbb{C})$ with the Kovacic algorithm [25]). Now l_1 and its conjugate l_2 lie in $k_1[\partial]$ where $k_1 := \mathbb{C}(x)(\sqrt{x})[\partial]$ and are isomorphic over $\widetilde{k_1}[\partial]$ where $\widetilde{k_1} := \mathbb{C}(x)(\sqrt{x}, \sqrt{x-2}) = k_1[\sqrt{x-2}]$. Indeed, we have $l_1.r_{1,2} = s_{1,2}.l_2$ with

$$r_{1,2} = \frac{\sqrt{x-2}}{x-2}\big(\partial + \sqrt{x}\big).$$

By the descent theorem, $L \simeq M \otimes N$ with G_N finite. In fact, because the l_i are permuted transitively, we see that G_N is an imprimitive group. We note that we have other factors of order 2, e.g.,

$$\partial^2 - \frac{1}{2}\frac{\partial}{x} - \frac{4\sqrt{x-2} + 1 + 2(x-2)^{5/2} + 6(x-2)^{3/2}}{\sqrt{x-2}x} \quad \text{or}$$
$$\partial^2 - \frac{1}{2}\frac{(x^2 - 2x - \sqrt{(2-x)x})}{x(2 + x^2 - 3x)}\partial - 2x + 2.$$

This implies that G_N has three semi-invariants of degree 2 and hence it is the quaternion group from the example on page 83.

2.3. *About the structure of the differential Galois group*

In Katz's theorem, we obtain L as a tensor product $L \simeq M \otimes N$. Can we then infer that $G_L \simeq G_M \otimes G_N$? This depends on whether the Picard–Vessiot extensions for M and N are included in K_L or, equivalently, if the descent field $k_0 = K_N$ is included in K_L. We may recall the construction from our proof of Theorem 2:

$$\begin{tikzcd}
& \widetilde{K} \arrow[dl, dash] \arrow[dr, dash] \arrow[dr, dotted, bend left, "\text{cyclic}"] & \\
k_0 = K_N = \widetilde{k_1}(f_1) \arrow[dr, dash] \arrow[dr, dotted, bend right, "\text{cyclic}"'] & & K_L \arrow[dl, dash] \arrow[ddl, dotted, bend left, "G_L"] \\
& k_0 \cap K_L \arrow[d, dash] & \\
& k &
\end{tikzcd}$$

Let $\rho_L : \widetilde{G} \to GL(V_L)$ denote the representation of $\widetilde{G}$ on the $\widetilde{G}$-module V_L (similarly define $\rho_M(\widetilde{G})$ and $\rho_N(\widetilde{G})$). Then, as both K_M and K_N lie in $\widetilde{K}$, we have:

Proposition 2. *Same notations and assumptions as in Theorem* 3. *Then*

(1) $\rho_L(G_L) = \rho_L(\widetilde{G}) \simeq \rho_M(\widetilde{G}) \otimes \rho_N(\widetilde{G})$.
(2) G_L *is a quotient of* $\widetilde{G}$ *by a finite cyclic central subgroup whose order divides the order* s *of* N.

Proof. Part (1) follows from the preceding discussion. For part (2), the above diagram shows that G_L is a quotient of $\widetilde{G}$ by $\mathrm{Gal}(\widetilde{K}/K_L)$ and that $\mathrm{Gal}(\widetilde{K}/K_L) \simeq \mathrm{Gal}(K_N/(K_L \cap K_N))$. Corollary 3 shows that the latter is cyclic of order dividing s and central in G_N and hence in $\widetilde{G}$. □

Remark 10. In the primitive case, the L_i are isomorphic over k_1. Hence, Theorem 3 shows that the quotients f_i/f_j lie in k_1. We thus obtain that $K_N = k_0 = k_1(f_1)$, f_1 is radical over k_1 and its order divides s.

Remark 11. A result similar to Proposition 2, though stated with different tools, appears in [9] and [46]. In fact, G_L and $\widetilde{G}$ are projectively equal. If $\overline{\rho_L}$ denotes the projective representation associated with ρ_L, then $\overline{\rho_L}(G)$ is the tensor product $\overline{\rho_M}(G) \otimes \overline{\rho_N}(G)$. If furthermore $K_N \subset K_L$, then $G = \widetilde{G}$ and we obtain a *linear* representation $\rho_L(G) \simeq \rho_M(G) \otimes \rho_N(G)$.

In the isotypical case, we have $G_L \simeq \rho_M(\widetilde{G}) \otimes \rho_N(\widetilde{G})$; it can then be checked that $\widetilde{H} = H = \{\rho_M(g) \otimes \rho_N(g) \mid g \in \rho_N^{-1}(Z(G_N))\}$, where $Z(G_N)$ is the center of $G_N = \rho_N(\widetilde{G})$. Letting $C_G(\widetilde{H})$ denote the centralizer of $\widetilde{H}$ in G, we may also note that $C_G(\widetilde{H}) = C_G(G^\circ)$.

3. Degrees and an algorithm for absolute factorization

In this section, we investigate the degrees over which one may compute an absolute factorization of L. Note that one must here distinguish between the degree of the coefficient field of *one* factor and the field extension of k generated by the coefficients of the set of operators L_i such that $L = \mathrm{LCLM}(L_1, \ldots, L_s)$.

3.1. Degrees for absolute factorization

As in Appendix B, the notation $\mathcal{P}_s$ stands for the (computable) list of possible minimal degrees for an algebraic logarithmic derivative of a solution in the case of a primitive unimodular group of order s (Definition 5, page 102), and the notation $\mathcal{L}_s$ stands for a (precomputable) list of integers such that, if an operator of order s has a first order factor over an algebraic extension, then it has one defined over an extension of degree $m \in \mathcal{L}_s$.

We first start with the possible degrees in the primitive case.

Lemma 5. *Let* L *denote a primitive differential operator of order* n *with coefficients in* $k \subset \overline{\mathbb{C}(x)}$. *Then* L *is absolutely reducible if and only if it admits an* (*absolutely irreducible*) *right-hand factor of order r (where $r \mid n$) over an extension of k whose degree belongs to $\mathcal{P}_{n/r}$.*

Proof. Because L is primitive, Theorem 2 shows that it admits an absolute factorization if and only if we have $L \simeq M \otimes N$ with N primitive finite and M absolutely irreducible. Let r denote the order of M and $s = n/r$. Then N admits a factor $\partial - u$ where u is algebraic of degree $m \in \mathcal{P}_s$. Let Φ denote the map (over k) transforming $M \otimes N$ into L. Because Φ is defined over k, the image of $M \otimes (\partial - u)$ is a factor L_1 of L which is defined over $k(u)$ (see Theorem 3). □

Now the degrees in the imprimitive case.

Lemma 6. *Let L denote an imprimitive differential operator of order n with coefficients in $k \subset \overline{\mathbb{C}(x)}$. Then L is absolutely reducible, and it admits an absolutely irreducible factor defined over an extension of k whose degree belongs to $\bigcup_{t|n,\, t>1} t(\bigcup_{r|(n/t)} \mathcal{P}_{n/(rt)})$ and r is the order of the factor.*

Proof. If t is the cardinal of a (maximal) system of imprimitivity, then Section 1.4 shows that there exists a divisor r of t such that an absolutely irreducible factor has order r and is defined over an extension of degree $m \in t.\mathcal{P}_{n/(rt)}$. □

Summarizing Lemmas 5 and 6, we obtain:

Proposition 3. *Let L denote an irreducible differential operator of order n with coefficients in $k \subset \overline{\mathbb{C}(x)}$. The operator L admits a factor over an algebraic extension of k if and only if L admits a factor whose order r is a divisor of n, and which is defined over an extension of k whose degree belongs to $\mathcal{L}_{n/r}$.*

Proof. The operator L is primitive or imprimitive, and the result follows from the two preceding lemmas and the fact that $\mathcal{L}_{n/r} = \bigcup_{t|(n/r)} t\mathcal{P}_{n/(rt)}$. □

Remark 12. The bounds are sharp in the sense that there actually are absolute factors of these degrees. However, in the imprimitive case, the example constructed at the end of [13] shows that there may, in some cases, exist factors of even lower degrees: this follows from the fact that the lists $\mathcal{L}_r$ given above are sharp but not always minimal. In the primitive case the list $\mathcal{P}_s$ contains exactly the possible minimal degrees.

Example. We give illustrations of this proposition and Lemmas 5 and 6 to compute complete degree lists for $n = 4, 6, \ldots$ (the lists for prime n follow from the works on Liouvillian solutions).

Let $n = 4$. If the group is primitive, we see that the possible degrees for absolute factors are in $\mathcal{P}_4 = [5, 8, 12, 16, 20, 24, 40, 48, 60, 72, 120]$ for factors of order 1 and $\mathcal{P}_2 = [4, 6, 12]$ for factors of order 2. For the imprimitive case, we obtain 2 for absolute factors of order 2 and $4\mathcal{P}_1 \cup 2\mathcal{P}_2 = [4] \cup [8, 12, 24] = [4, 8, 12, 24]$ for factors of order 1. Summarizing, we see that the possible degrees for an order 1 factor at order 4 are

$[4, 5, 8, 12, 16, 20, 24, 40, 48, 60, 72, 120]$ and, for a factor of order 2, the degrees are in $[2, 4, 6, 12]$.

Let us now turn to order 6 and factors of order 2 and 3. For an absolute factor of order 2, the possibilities are $\mathcal{P}_3 = [6, 9, 21, 36]$ (primitive case) and 3 (imprimitive case). For an absolute factor of order 3, the possibilities are $\mathcal{P}_2 = [4, 6, 12]$ (primitive case) and 2 (imprimitive case).

At order 8, we see a new phenomenon occur for factors of order 2. For an absolute factor of order 2, the possibilities are $\mathcal{P}_4 = [5, 8, 12, 16, 20, 24, 40, 48, 60, 72, 120]$ (primitive case) and $4.\mathcal{P}_1 \cup 2.\mathcal{P}_2 = [4] \cup [8, 12, 24] = [4, 8, 12, 24]$ (imprimitive case), thus resulting in the list $[4, 5, 8, 12, 16, 20, 24, 40, 48, 60, 72, 120]$. For an absolute factor of order 4, the possibilities are $\mathcal{P}_2 = [4, 6, 12]$ (primitive case) and 2 (imprimitive case), thus resulting in the list $[2, 4, 6, 12]$.

3.2. Algorithm for computing an absolute factorization

In this section, we give a procedure which, given an irreducible operator L, decides if L is reducible over $\bar{k}$ and, if so, computes an algebraic extension $k(u)$ and an absolute factor $L_1 \in k(u)[\partial]$ of L.

In addition to the degree considerations, we will first show auxiliary results about the representations of G_L on $\Lambda^r(V_L)$ to obtain a more natural algorithm.

A first general observation is the following lemma (which follows from the factorization method exposed in Appendix A).

Lemma 7. *L has a factor of order r over an algebraic extension of degree m if and only if there is a line in the exterior power $\Lambda^r(V)$ generated by a pure tensor and whose orbit under the Galois group is finite of length m.*

Proof. The implication follows from Lemma 10.

Conversely, let $w = v_1 \wedge \cdots \wedge v_r$ denote a pure tensor and assume that the line $C.w$ has an orbit of length m. Let V_1 be the r-dimensional vector space spanned by the v_i. For g in G, let V_g be the vector space spanned by the $g(v_j)$. Now, denote by H the intersection of the stabilizers of all the V_g. We have $\Lambda^r(V_g) = g(w)$ so, because w has finite orbit, there are exactly m $V_g := \{V_1, \ldots, V_m\}$. Then H is a normal subgroup in G of index $\leqslant m!$. Let k_1 be the fixed field of H in K_L. V_1 is the solution space of an operator L_1 with coefficients in k_1. Now the Galois group G acts on the coefficients of L_1 and sends it to some L_g. The solution space of this is one of the V_j so there are exactly m operator L_j. This shows that the coefficient field of L_1 is algebraic of degree m as claimed. And, because $V_1 \subset V_L$, our L_1 is a factor of L. □

Let us first distinguish between the primitive and imprimitive cases.

In the primitive case, Theorem 2 tells us that $L = M \otimes N$. Write $V_N = \mathbb{C}.f_1 \oplus \cdots \oplus \mathbb{C}.f_s$. Then

$$V_L \simeq_{\widetilde{G}} (V_M \otimes \mathbb{C}.f_1) \oplus \cdots \oplus (V_M \otimes \mathbb{C}.f_s).$$

Lemma 8. *Notations as in the proof of Theorem* 2. *Assume that* $L \simeq_k M \otimes N$ *with* $\mathrm{ord}(M) = r$. *Then* $\Lambda^r(V_L)$ *admits a* $\widetilde{G}$*-submodule isomorphic to* $\Lambda^r(V_M) \otimes \mathrm{Sym}^r(V_N)$.

Proof. A simple computation shows that $\Lambda^r(V_M \otimes V_N)$ contains a $\widetilde{G}$-submodule generated by elements of the form $\Lambda^r(V_M) \otimes \mathbb{C}.f^r$ with $N(f) = 0$, hence this module is (isomorphic to) $\Lambda^r(V_M) \otimes \mathrm{Sym}^r(V_N)$. □

Note that this lemma also gives another proof for the degrees measured in Proposition 3.

We now turn to the imprimitive case.

Lemma 9. *Assume that* G_L *is imprimitive, let* $\{W_1, \ldots, W_t\}$ *denote a system of imprimitivity. Then, there exists a monomial submodule of dimension* t *in* $\Lambda^{n/t}(V_L)$.

Proof. Follows from the fact that the t lines $\Lambda^{n/t}(W_i)$ are permuted transitively by the Galois group and, hence, their direct sum is a G_L-submodule in $\Lambda^{n/t}(V_L)$. □

The absolute factorization procedure, thanks to the above lemmas, follows the following path: decompose (over k) the successive exterior powers $\Lambda^r(L)$ (where $r \mid n$), identify the relevant factors via representation theory and dimension analysis, and search for pure tensor first order factors over algebraic extensions of degrees found in the lists.

To explain the absolute factorization process, we show how to proceed for an operator L of order $n = 6$ (the process is similar at any order). The steps below have to be performed successively. We proceed by increasing the order of the sought factors. Success at any step provides an absolute factorization (because we study increasing orders) and the algorithm then stops. If none succeeds, then the operator is absolutely irreducible.

order 1: Search for Liouvillian solutions of L ([22,40], and Appendix B), i.e., first order factors over $\bar{k}$.

order 2: Compute an LCLM decomposition $\Lambda^2(L) = l_1 \oplus l_2 \oplus \cdots$ [36].

(a) For all sums l of l_i of total order 3 (potential imprimitive case with factor of order 2): find if there are Liouvillian solutions of degree 3 of l ([22,40], and Appendix B) and apply the Plücker test (see Appendix A) to those to recover the putative corresponding factor.

(b) For all sums l of l_i of total dimension 6.
If $l = l_1 \oplus l_2$ with $\dim(l_1) = 1$ and $\dim(l_2) = 5$, then search for a Liouvillian solution of degree 6 in l_2.
If $l = l_1 \oplus l_2$ with $\dim(l_i) = 3$, then search for a Liouvillian solution of degree 9 of each of the l_i.
Else l should be irreducible of dimension 6; if so, search for a Liouvillian solution of degrees $9, 21, 36$. For each such Liouvillian solution, apply the Plücker test to recover the putative corresponding factor (Appendix A).

order 3: Compute an LCLM decomposition $\Lambda^3(L) = l_1 \oplus l_2 \oplus \cdots$.

(a) For all sums l of l_i of total order 2 (potential imprimitive case with factor of order 2): find Liouvillian solutions of degree 2 of l and apply the Plücker test to those to those to recover the putative corresponding factor.

(b) For all sums l of l_i of total order 4:

(i) Test [35] if l is projectively isomorphic to the symmetric cube of a second order operator.

(ii) If $l = l_1 \oplus l_2$, then search for a Liouvillian solution of degree 4 for each l_i. Else, l should be irreducible of dimension 4; if so search for Liouvillian solutions of degrees 6, 12.

For each such Liouvillian solution, apply the Plücker test to recover the putative corresponding factor.

Proof. Part (b) at order 2 is the primitive case. In this case, N is (projectively equivalent to) one of the finite primitive subgroups of SL_3. The decompositions of characters for these groups on the second symmetric power (Table 1, page 8 in [38]) gives the desired decomposition (that a solution will exist in some l follows from the unicity up to isomorphism of the LCLM factorization).

Similarly, part (a) at order 3 is the imprimitive case, and part (b) follows as above from the character decompositions given in Table 2, page 8 of [38]. □

4. Conclusion

The method presented relies on the fine analysis of the primitive case, for which we have a factorization of the operator L as a tensor product $L \simeq M \otimes N$. This factorization has given us the degrees (and a characterization) of the extensions over which L may potentially factor. These degrees are sharp (and optimal in the primitive case).

We saw that the factorization of L as a tensor product comes from a phenomenon of Galoisian descent, which leads us to the following two topics:

(1) How one actually realizes the descent. More precisely, given an operator L_1 with algebraic coefficients satisfying the descent conditions, how one computes the set of its descents (up to rational isomorphisms).
(2) How to effectively obtain the factorization of L as a tensor product $M \otimes N$ in the isotypical case.

These two questions will be answered in subsequent work.

Last, in [21], van Hoeij and van der Put also study descent problems for differential operators in a slightly different context, as their concern is operators with coefficients in $C(x)$, with C a non-algebraically closed subfield of $\overline{\mathbb{Q}}$ and questions of definition fields for those. There again, the descent machinery is the source of inspiring results.

Acknowledgments

The authors warmly thank Michael F. Singer and Daniel Bertrand for inspiring conversations, suggestions and comments on this work; M. van Hoeij for enthusiastic comments and examples; Pierre Debes and Jean-Claude Douai for their comments on the "Galoisian descent" classical machinery.

Appendix A. Factorization of differential operators and systems

The general reference for this appendix and the next is [31]. The results thereafter are "well-known" to specialists and recalled here mainly for convenience and notational conventions.

Let $\mathcal{D} = k[\partial]$ denote the ring of differential operators (see [31]). We say that a differential operator L is reducible if there exists non-trivial L_1 and L_2 in $\mathcal{D}$ such that $L = L_1 L_2$. We say that a differential module $\mathcal{M}$ is reducible if it admits a (non-trivial) ∂-submodule. We say that a system (S): $Y' = AY$ is reducible if it is equivalent (over k) to a block-triangular system of the form

$$Y' = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix} Y.$$

It is easily verified that these three properties are equivalent. This section is concerned with algorithms for detecting and computing factorizations of differential operators. The approach given here stems from [8,43], who built on an old work of Beke (1884).

The present presentation came out of discussions of the authors with M. van der Put. Its advantage, besides its natural simplicity, is that it generalizes straightforwardly to factorization of differential systems.

Another approach to factoring differential operators/systems, using ∂-endomorphisms of $\mathcal{M}$, is given in [36] (see [2,19] for its algorithmic developments); yet another approach to factorization (probably the most efficient) was developed by van Hoeij in [20] and will not be used here.

A.1. Exterior powers of differential systems

Let $e_1, \ldots, e_n$ denote a basis of the differential module $\mathcal{M}$. By taking the standard alternating products $e_{i_1} \wedge \cdots \wedge e_{i_r}$ as a basis for the exterior power $\Lambda^r(\mathcal{M})$, we naturally endow it with a structure of ∂-module.

Example. If $\partial(e_i) = -\sum_{i=1}^{n} A_{j,i} e_j$, then the action of ∂ on $\Lambda^2(\mathcal{M})$ is given by $\partial(e_i \wedge e_j) = \partial(e_i) \wedge e_j + e_i \wedge \partial(e_j) = -\sum_{k=1}^{n} A_{k,i} e_k \wedge e_j - \sum_{k=1}^{n} A_{k,j} e_i \wedge e_k$ and the usual antisymmetric rules on the $e_i \wedge e_j$ complete the expression of $\partial(e_i \wedge e_j)$.

From this construction, we see that, to a differential system $Y' = AY$, we can naturally associate an *rth exterior power system* denoted by $Y' = \Lambda_r(A)Y$, "attached" to the ∂-module $\Lambda^r(\mathcal{M})$.

We say that an element $Z \in \Lambda^r(\mathcal{M})$ is a *pure tensor* in $\Lambda^r(\mathcal{M})$ if there exists $f_1, \ldots, f_r \in \mathcal{M}$ such that $Z = f_1 \wedge \cdots \wedge f_r$.

Lemma 10. *The differential module $\mathcal{M}$ admits a ∂-submodule N of dimension r if and only if $\Lambda^r(\mathcal{M})$ admits a* 1*-dimensional submodule generated by a pure-tensor.*

Proof. ($\Rightarrow$) If $f_1, \ldots, f_r$ is a basis of $\mathcal{N}$, then $f_1 \wedge \cdots \wedge f_r$ generates the 1-dimensional ∂-submodule $\Lambda^r(\mathcal{N})$: it is a ∂-module because $\partial(\mathcal{N}) \subset \mathcal{N}$.

($\Leftarrow$) Let $Z := f_1 \wedge \cdots \wedge f_r$ be the pure tensor generating a 1-dimensional submodule in $\Lambda^r(\mathcal{M})$. We thus have $\partial(Z) = aZ$ with $a \in k$. Consider the application

$$\Psi : \mathcal{M} \to \Lambda^{r+1}(\mathcal{M}), \quad Y \mapsto Z \wedge Y.$$

The kernel of Ψ is obviously the k-vector space generated by $f_1, \ldots, f_r$. Let $Y \in \ker(\Psi)$. Then

$$0 = \partial\big(\Psi(Y)\big) = (\partial Z) \wedge Y + Z \wedge (\partial Y) = a\Psi(Y) + Z \wedge (\partial Y) = Z \wedge (\partial Y)$$

and hence $\partial Y \in \ker(\Psi)$, thus turning $\ker(\Psi)$ into the desired r-dimensional submodule. $\square$

To compute the 1-dimensional submodules of $\Lambda^r(\mathcal{M})$, we may apply the algorithm of [29] to the system $Y' = \Lambda_r(A)Y$. The result is a finite set of (finite dimensional) $\mathbb{C}$-vector spaces $\mathcal{N}_i$ such that any element in $\mathcal{N}_i$ generates a 1-dimensional ∂-module (i.e., the $\mathcal{N}_i$ are generated (as $\mathbb{C}$ vector spaces) by elements $v_{i,j}$ such that $\partial(v_{i,j}) = a_i v_{i,j}$ with $a_i \in k$). Let $Z_i = \sum c_i v_{i,j}$ where the c_i are unknown constant parameters.

A.2. The Plücker relations

The Plücker relations characterize elements in an exterior power that are pure tensors. They were introduced in the context of the factorization of differential operators by Tsarëv in [43]. To recover those in an effective way in our context, we use the proof of Lemma 10. For each i, let

$$\Psi_i : \mathcal{M} \to \Lambda^{r+1}(\mathcal{M}), \quad Y \mapsto Z_i \wedge Y.$$

Identifying pure tensors is now just a rank computation, i.e., identify the constants c_j such that Ψ_i has rank $n - r$. The latter can be performed by standard algebraic operations. For those values of the c_j, all that remains to be done is to compute a basis of $\ker(\Psi_i)$: the generators of $\ker(\Psi_i)$ then span a ∂-submodule of $\mathcal{M}$. In particular, if we started from a differential operator L, we may choose a cyclic basis of $\ker(\Psi_i)$, thus obtaining a factor of L. Note that, in [8], Bronstein gives (in a slightly different language) explicit formulas for this reconstruction (i.e., the coefficients of a factor can be read off from a pure-tensor solution of $Y' = \Lambda_r(A)Y$).

Example. Let's continue with order 4 and search for a factor of order 2. Let $\widetilde{Z} = \sum_{i=0}^{2} \sum_{j=i+1}^{3} z_{i,j} e_i \wedge e_j$ denote a (possibly) parameterized generator for a 1-dimensional submodule in $\Lambda^2(\mathcal{M})$. Then $\Psi(e_0) = z_{1,2} e_0 \wedge e_1 \wedge e_2 + z_{1,3} e_0 \wedge e_1 \wedge e_3 + z_{2,3} e_0 \wedge e_2 \wedge e_3$. Continuing like this, we find the matrix of Ψ to be

$$M_\Psi = \begin{pmatrix} z_{12} & -z_{02} & z_{01} & 0 \\ z_{13} & -z_{03} & 0 & z_{01} \\ z_{23} & 0 & -z_{03} & z_{02} \\ 0 & z_{23} & -z_{13} & z_{12} \end{pmatrix}.$$

Computing the determinant gives us the well-known Plücker condition for this matrix to not have full rank: $z_{03}z_{12} - z_{02}z_{13} + z_{23}z_{01} = 0$. This condition can be shown to be equivalent to M_Ψ having rank two. Note that the matrix is not square in general.

Now, assume M_Ψ has a kernel and let Y_1, Y_2 denote a basis for that kernel (if we want to make it cyclic, then we choose a basis of the form $Y_1, \partial(Y_1)$). Complete with vectors Y_3, Y_4 to form a basis of $\mathcal{M}$ and let P denote the matrix whose columns are the Y_i. Then, the Gauge transformation $PAP^{-1} + P'P^{-1}$ has the form

$$PAP^{-1} + P'P^{-1} = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix}$$

which provides the desired factorization over k.

If we had initially started with a differential operator (a companion system), then the second order factor associated to the above pure tensor would be $\partial^2 - (z_{0,2}/z_{0,1})\partial + z_{1,2}/z_{0,1}$.

Appendix B. First order factors over algebraic extensions

As we saw that computing first order factors was the building block for factoring, we now turn to the question of computing first order factors over algebraic extensions. This subject has a long history (Liouvillian solutions, see [37] for abundant details and references). Methods for performing this task were studied in the nineteenth century by Picard, Vessiot, Marotte, and others; the algorithmic approach to the subject was spectacularly revived by Kovacic in 1979 [25] for second order operators and Singer [34] for arbitrary order. Precise bounds for the degree of the algebraic extensions were given in [44] and [39]; the best known algorithms stem from [40] and [22] (see also [13]) and are quickly summarized below.

Suppose $\mathcal{M}$ admits a 1-dimensional submodule over an algebraic extension of k. This means that there exists u_1 algebraic over k and $Y_1 \in \mathcal{M} \otimes k[u_1]$ such that $\partial Y_1 = u_1 Y_1$. Let $u_2, \ldots, u_m$ (respectively $Y_2, \ldots, Y_m$) denote the conjugates of u_1 (respectively Y_1). Then $Y_1 Y_2 \ldots Y_m$ has coefficients in k and generates a 1-dimensional submodule in $\mathrm{Sym}^m(\mathcal{M})$. In [40], the converse is shown (in a different language): $\mathcal{M}$ admits a first order factor over an algebraic extension of k if and only if there exists a 1-dimensional submodule in $\mathrm{Sym}^m(\mathcal{M})$ which factors (over $\bar{k}$) as a product of elements of $\mathcal{M} \otimes \bar{k}$. Note the striking similarity of this criterion (find a 1-dimensional submodule generated by a pure tensor in $\mathrm{Sym}^m(\mathcal{M})$) with the factorization criterion of Lemma 10.

We now turn to the question of the degree of u. Singer showed in [34] that, for an operator of order n, the degree of u was uniformly bounded by a function $\mathcal{F}(n)$. He gave estimates for $\mathcal{F}(n)$, which were refined in [44]. In the latter (and with Singer in [39]), Ulmer further showed how one could actually compute an accurate *list* $\mathcal{L}_n$ of possible degrees[7] for extensions over which $\mathcal{M}$ may factor.

The construction of those lists is achieved the following way. First, separate between primitive finite and imprimitive unimodular groups. There is a finite list of primitive finite unimodular groups for which a list $\mathcal{P}_n$ of corresponding degrees can be computed.

Definition 5. We denote by $\mathcal{P}_n$ the list of minimal possible degrees for a right-hand factor $\partial - u$ of an irreducible operator $L \in k[\partial]$ of order n with finite primitive unimodular differential Galois group.

We denote by $\mathcal{L}_n$ the list of possible degrees for a right-hand factor $\partial - u$ of an irreducible operator $L \in k[\partial]$ or order n.

We recall those lists for use in our paper:

$$\mathcal{P}_2 = [4, 6, 12] \quad \bigl(\text{see [25]}\bigr),$$
$$\mathcal{P}_3 = [6, 9, 21, 36] \quad \bigl(\text{see [39,44]}\bigr),$$
$$\mathcal{P}_4 = [5, 8, 12, 16, 20, 24, 40, 48, 60, 72, 120],$$
$$\mathcal{P}_5 = [6, 10, 15, 30, 40, 55] \quad \bigl(\text{see [13]}\bigr);$$

we adopt the convention that $\mathcal{P}_1 = [1]$. For higher values of n, a bound on the highest element of $\mathcal{P}_n$ is given in [34] and refined in [39,44].

In [39,44], it is shown[8] that the complete list of degrees for factors of order one of an operator of order n is $\mathcal{L}_n = \bigcup_{r|n}(n/r).\mathcal{P}_r$ where $(n/r).\mathcal{P}_r$ is the list of elements of the form $(n/r)\nu$ for $\nu \in \mathcal{P}_r$. For the record, we recall those complete lists:

$$\mathcal{L}_2 = [2, 4, 6, 12],$$
$$\mathcal{L}_3 = [3, 6, 9, 21, 36],$$
$$\mathcal{L}_4 = [4, 5, 8, 12, 16, 20, 24, 40, 48, 60, 72, 120],$$
$$\mathcal{L}_5 = [5, 6, 10, 15, 30, 40, 55].$$

[7] This computation is systematic but by no means easy. Complete lists are known only up to $n = 5$ [13], although the directions towards making such lists, in particular uniform bounds, are known for arbitrary values of n.

[8] In fact, in [39,44], the authors give the (too pessimistic) bound $(n/r)!.\mathcal{P}_r$ but our correction (which has been long known to the authors of [39,44]) follows easily from Clifford's Theorem 1 and the reasoning in Section 3 of this paper.

Those lists are used to construct analogous lists for higher order factors in Section 3 of this paper.

References

[1] F. Baldassarri, B. Dwork, On second order linear differential equations with algebraic solutions, Amer. J. Math. 101 (1) (1979) 42–76.

[2] M. Barkatou, E. Pflügel, On the equivalence problem of linear differential systems and its application for factoring completely reducible systems, in: Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (Rostock), ACM, New York, 1998, pp. 268–275 (electronic).

[3] D. Bertrand, Théorie de Galois différentielle, in: R. Lardon (Ed.), Cours de DEA, Université de Paris VI, 1986.

[4] L. Bertrand, Computing a hyperelliptic integral using arithmetic in the Jacobian of the curve, Appl. Algebra Engrg. Comm. Comput. 6 (4–5) (1995) 275–298.

[5] F. Beukers, W.D. Brownawell, G. Heckman, Siegel normality, Ann. of Math. (2) 127 (2) (1988) 279–308.

[6] F. Beukers, Differential Galois theory, in: From Number Theory to Physics (Les Houches, 1989), Springer, Berlin, 1992, pp. 413–439.

[7] M. Bronstein, Integration of elementary functions, J. Symbolic Comput. 9 (2) (1990) 117–173.

[8] M. Bronstein, An improved algorithm for factoring linear ordinary differential operators, in: Proceedings of the International Symposium on Symbolic and Algebraic Computation ISSAC'94, July 20–22, Oxford, England, 1994, pp. 336–340.

[9] J. Clifford, Representations induced in an invariant subgroup, Ann. of Math. 38 (3) (1937) 533.

[10] É. Compoint, Généralisation d'un Théorème de Fano et Singer, C. R. Acad. Sci. I 318 (1994) 885–887.

[11] É. Compoint, M.F. Singer, Relations linéaires entre solutions d'une équation différentielle, Ann. Fac. Sci. Toulouse Math. (6) 7 (4) (1998) 659–670.

[12] É. Compoint, M.F. Singer, Computing Galois groups of completely reducible differential equations, Differential Algebra and Differential Equations, J. Symbolic Comput. 28 (4–5) (1999) 473–494.

[13] O. Cormier, On Liouvillian solutions of linear differential equations of order 4 and 5, in: Proceedings of International Symposium on Symbolic and Algebraic Computation ISSAC'2001, ACM Press, London, Ontario, 2001.

[14] C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley–Interscience, New York, 1966.

[15] A. Grothendieck, Technique de descente et théorèmes d'existence en géometrie algébrique. I. Généralités. Descente par morphismes fidèlement plats, in: Séminaire Bourbaki, vol. 5, exp. 190, Soc. Math. France, Paris, 1995, pp. 299–327.

[16] A. Grothendieck, Technique de descente et théorèmes d'existence en géométrie algébrique. II. Le théorème d'existence en théorie formelle des modules, in: Séminaire Bourbaki, vol. 5, exp. 195, Soc. Math. France, Paris, 1995, pp. 369–390.

[17] J. Hartmann, Invariants and differential Galois groups in degree four, in: Differential Galois Theory (Bedlewo, 2001), in: Banach Center Publ., vol. 58, Polish Acad. Sci., Warsaw, 2002, pp. 79–87.

[18] S.A. Hessinger, Computing the Galois group of a linear differential equation of order four, Appl. Algebra Engrg. Comm. Comput. 11 (6) (2001) 489–536.

[19] M. van Hoeij, Rational solutions of the mixed differential equation and its application to factorization of differential operators, in: Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation ISSAC'96, ACM Press, New York, 1996, pp. 219–225 (electronic).

[20] M. van Hoeij, Factorization of differential operators with rational functions coefficients, J. Symbolic Comput. 24 (5) (1997) 537–561.

[21] M. van Hoeij, M. van der Put, Descent for differential modules and skew-fields, Preprint, 2002.

[22] M. van Hoeij, J.-F. Ragot, F. Ulmer, J.A. Weil, Liouvillian solutions of linear differential equations of order three and higher, Differential Algebra and Differential Equations, J. Symbolic Comput. 28 (4–5) (1999) 589–609.

[23] G. Karpilovsky, Clifford Theory for Group Representations, in: North-Holland Math. Stud., vol. 156, North-Holland, Amsterdam, 1989.
[24] N.M. Katz, Exponential Sums and Differential Equations, in: Ann. of Math. Stud., vol. 124, Princeton University Press, Princeton, NJ, 1990.
[25] J. Kovacic, An algorithm for solving second order linear homogeneous differential equations, J. Symbolic Comput. 2 (1986) 3–43.
[26] S. Lang, Algebra, third ed., Addison–Wesley, 1992.
[27] A.R. Magid, Lectures on Differential Galois Theory, in: Univ. Lecture Ser., vol. 7, American Mathematical Society, Providence, RI, 1994.
[28] J.-P. Ramis, J. Martinet, Théorie de Galois différentielle et resommation, in: E. Tournier (Ed.), Computer Algebra and Differential Equations, in: Comput. Math. Appl., Academic Press, London, 1990, pp. 117–214.
[29] E. Pflügel, An algorithm for computing exponential solutions of first order linear differential systems, in: Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI), ACM, New York, 1997, pp. 164–171 (electronic).
[30] M. van der Put, Galois theory of differential equations, algebraic groups and Lie algebras, Differential Algebra and Differential Equations, J. Symbolic Comput. 28 (4–5) (1999) 441–472.
[31] M. van der Put, M.F. Singer, Galois Theory of Linear Differential Equations, in: Grundlehren Math. Wiss., vol. 328, Springer-Verlag, Berlin, 2003.
[32] M. van der Put, F. Ulmer, Differential equations and finite groups, J. Algebra 226 (2) (2000) 920–966.
[33] J.-P. Serre, Galois Cohomology, Springer-Verlag, Berlin, 1997.
[34] M.F. Singer, Liouvillian Solutions of nth order linear differential equations, Amer. J. Math. 103 (1981) 661–682.
[35] M.F. Singer, Solving homogeneous linear differential equations in terms of second order linear differential equations, Amer. J. Math. 107 (3) (1985) 663–696.
[36] M.F. Singer, Testing reducibility of linear differential operators: a group-theoretic perspective, Appl. Algebra Engrg. Comm. Comput. 7 (2) (1996) 77–104.
[37] Singer M.F., Direct and inverse problems in differential Galois theory, in: H. Bass, A. Buium, P. Cassidy (Eds.), Selected Works of Ellis Kolchin with Commentary, American Mathematical Society, Providence, RI, 1999.
[38] M.F. Singer, F. Ulmer, Galois groups of second and third order linear differential equations, J. Symbolic Comput. 16 (1) (1993) 9–36.
[39] M.F. Singer, F. Ulmer, Liouvillian and algebraic solutions of second and third order linear differential equations, J. Symbolic Comput. 16 (1) (1993) 37–73.
[40] M.F. Singer, F. Ulmer, Linear differential equations and products of linear forms, in: Algorithms for Algebra (Eindhoven, 1996), in: J. Pure Appl. Algebra, vols. 117/118, 1997, pp. 549–563.
[41] T.A. Springer, Linear Algebraic Groups, second ed., in: Progr. Math., vol. 9, Birkhäuser, 1998.
[42] B. Trager, Integration of algebraic functions, PhD thesis, Department of EECS, MIT, 1984.
[43] S.P. Tsarëv, Some problems that arise in the factorization of linear ordinary differential operators, Programmirovanie 1 (1994) 45–48 (in Russian), translation in Programm. Comput. Softw. 20 (1) (1994) 2–27.
[44] F. Ulmer, On Liouvillian solutions of linear differential equations, Appl. Algebra Engrg. Comm. Comput. 2 (3) (1992) 171–193.
[45] A. Weil, The field of definition of a variety, Amer. J. Math. 78 (1956) 509–524.
[46] B.A.F. Wehrfritz, Infinite Linear Groups. An Account of the Group-Theoretic Properties of Infinite Groups of Matrices, in: Ergeb. Mat. Grenzgeb., vol. 76, Springer-Verlag, New York–Heidelberg, 1973.

Further reading

[1] D. Bertrand, Minimal heights and polarizations on group varieties, Duke Math. J. 80 (1) (1995) 223–250.
[2] K.S. Brown, Cohomology of Groups, in: Grad. Texts in Math., vol. 87, Springer-Verlag, New York–Berlin, 1982.

[3] M. van Hoeij, J.A. Weil, An algorithm for computing invariants of differential Galois groups, in: Algorithms for Algebra (Eindhoven, 1996), in: J. Pure Appl. Algebra, vols. 117/118, 1997, pp. 353–379.
[4] M. van der Put, Recent work on differential Galois theory, in: Séminaire Bourbaki, vol. 1997/98, exp. 849, 5, in: Astérisque, vol. 252, 1998, pp. 341–367.
[5] J.-P. Serre, Corps Locaux, deuxième édition, in: Publications de l'Université de Nancago, vol. VIII, Hermann, Paris, 1968.
[6] M.F. Singer, Moduli of linear differential equations on the Riemann sphere with fixed Galois groups, Pacific J. Math. 160 (2) (1993) 343–395.
[7] S.P. Tsarëv, An algorithm for complete enumeration of all factorizations of a linear ordinary differential operator, in: Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation ISSAC'96, ACM Press, New York, 1996, pp. 226–231 (electronic).
[8] A.E. Zalesskij, Linear groups, in: Algebra IV, in: Encyclopedia Math. Sci., vol. 37, Springer, Berlin, 1993, pp. 97–196.