ELSEVIER

Journal of Pure and Applied Algebra 139 (1999) 3–23

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Calculating the Galois group of $L_1(L_2(y)) = 0$, L_1, L_2 completely reducible operators ☆

P.H. Berman, M.F. Singer *

Department of Mathematics, Box 8205, North Carolina State University, Raleigh, NC 27695-8205, USA

Received 15 February 1998

Abstract

In *Calculating Galois groups of completely reducible linear operators*, Compoint and Singer describe a decision procedure that computes the Galois group of a completely reducible linear differential operator with rational or algebraic function coefficients (i.e., a linear differential operator that is the least common left multiple of irreducible operators or, equivalently, one whose Galois group is a reductive group). At present, it is unknown how to calculate the Galois group of a general operator. In this paper, we push beyond the completely reducible case by showing how to compute the Galois group of an operator of the form $L_1 \circ L_2$ where L_1 and L_2 are completely reducible and have rational function coefficients.

We begin by showing how to compute the Galois group of an equation of the form $L(y) = b$ with L completely reducible. This corresponds to the case of $L_1 \circ L_2$ where $L_1 = D - b'/b$. We then show how one can reduce the general case to the above case and give several examples.

MSC: 12H05; 68Q40

1. Introduction

In [3] a decision procedure is described that computes the Galois group of a completely reducible linear differential operator with rational or algebraic function coefficients (i.e., a linear differential operator that is the least common left multiple of irreducible operators or, equivalently, one whose Galois group is a reductive group). At present, it is unknown how to calculate the Galois group of a general operator. In this paper, we push beyond the completely reducible case by showing how

☆ The preparation was partially supported by NSF Grant CCR-93222422.

* Corresponding author.

E-mail address: phberman@eos.ncsu.edu; singer@math.ncsu.edu; http://www.math.ncsu.edu/ ~singer.

0022-4049/99/$ – see front matter
PII: S0022-4049(99)00003-1

to compute the Galois group (and Picard–Vessiot extension) of an operator of the form $L_1 \circ L_2$ where L_1 and L_2 are completely reducible and have rational function coefficients.

The paper is organized as follows. In Section 2 we show how to compute the Galois group and Picard–Vessiot extension of an equation of the form $L(y)=b$ with L completely reducible. This corresponds to the case of $L_1 \circ L_2$ where $L_1 = D - b'/b$. In Section 3, we show how one can reduce the general case to the above case and give several examples.

2. Calculating the Galois group of $L(y) = b$, L completely reducible

Let k be a differential field of characteristic zero with algebraically closed field of constants $\mathscr{C}$ and let $\mathscr{D} = k[D]$ be the ring of differential operators with coefficients in k. For any $L \in \mathscr{D}$ and $b \in k$, we shall use the phrase *the Picard–Vessiot extension of* $L(y)=b$ to denote the Picard–Vessiot extension of k corresponding to $(D - b'/b)L$, that is, the smallest Picard–Vessiot extension of k containing a full set of solutions of $L(y)=0$ as well as a specific solution of $L(y)=b$. We shall call the Galois group of this Picard–Vessiot extension the *Galois group of* $L(y)=b$. We will combine the techniques of [1,2] with those of [3] to show how, given $L \in k[D]$, L completely reducible, and $b \in k$, one can calculate the Galois group and Picard–Vessiot extension of $L(y)=b$. Note that an operator is said to be *completely reducible* if it is the least common left multiple of irreducible operators. An equivalent condition is that the Galois group G be reductive ([7], p. 125), that is, the largest normal subgroup of G consisting of unipotent elements is trivial (for equivalent conditions see Lemma 2.13 of [13] and Proposition 2.2 of [3]). The key is the following proposition, which is a slight modification of Théorème 1 of [2]. We say that an algebraic group is a *vector group* if it is isomorphic to $(\mathscr{C}^n, +)$ for some n.

Proposition 2.1. *Let k, b and L be as above. The Galois group of $L(y)=b$ is isomorphic to the semidirect product $W \rtimes G_L$, of the Galois group G_L of $L(y)=0$ and a vector group W. Furthermore, if $L_1 \in k[D]$ is a monic operator of maximal order satisfying*

1. *$L_1(y)=b$ has a solution $f_1 \in k$, and*
2. *$L = L_1 L_0$ for some $L_0 \in k[D]$*

then W is G-isomorphic to the solution space of L_0. In addition such an L_1 is unique.

Proof. We first note that the operator $L_1 = 1$ satisfies conditions 1. and 2. with $L_0 = L$. Therefore there will exist an operator L_1 of maximal order satisfying these conditions.

Let K be the Picard–Vessiot extension of k corresponding to $(D - b'/b)L$ and $K_L \subset K$ be the Picard–Vessiot extension corresponding to L. If $L = L_1 L_0$, then K_L will contain

fundamental sets of solutions of both $L_0(y)=0$ and $L_1(y)=0$ and so it makes sense to speak of the action of G_L on the solution spaces of these two equations.

Let $f\in K$ be a solution of $L(y)=b$. For any $\sigma\in G=Gal(K/k)$, $\sigma(f)-f$ is in the solution space V_L of $L(y)=0$. Let $\Phi: G\to V_L$ be the map sending σ to $\sigma(f)-f$. Let H be the normal subgroup of G leaving K_L fixed.

Since $K=K_L\langle f\rangle$, we see that Φ is injective on H. For any $\sigma\in G, \tau\in H$, we have that

$$\begin{aligned}\Phi(\sigma\tau\sigma^{-1}) &= \sigma\tau\sigma^{-1}(f)-f\\ &= \sigma[\tau(\sigma^{-1}(f)-f)+\tau(f)]-f\\ &= \sigma[\sigma^{-1}(f)-f]+\sigma\tau(f)-f \text{ since } \tau \text{ fixes the elements of } V_L\subset K_L\\ &= \sigma[\tau(f)-f]\\ &= \sigma\Phi(\tau).\end{aligned}$$

This calculation (from the proof of Théorèm 1 of [2]) shows that Φ is a G-morphism, where the action of G on H is given by conjugation. Therefore, Φ identifies H with a G-invariant subspace W of V_L. Since G/H is isomorphic to the reductive group G_L and H is unipotent, H is the unipotent radical of G. Any linear algebraic group may be written as a semidirect product $G=H\rtimes P$ where H is the unipotent radical of G and P is a reductive group (called a *Levi subgroup of* G, [11]). Clearly, P is isomorphic to G_L.

Let $\tilde{L}_0$ be the monic operator in $k[D]$ whose solution space is W and let $L=\tilde{L}_1\tilde{L}_0$. Since $\sigma(f)-f\in W$ for all $\sigma\in H$, we have that $\tilde{L}_0(\sigma(f))=\tilde{L}_0(f)$ for all $\sigma\in H$. Therefore, $\tilde{L}_0(f)\in K_L$. Let W_1 be the solution space of $\tilde{L}_1$ in K_L and let $W_{\tilde{L}_0(f)}$ be the space spanned by W_1 and $\tilde{L}_0(f)$. For any $\sigma\in G_L$, $\sigma(\tilde{L}_0(f))$ is again a solution of $\tilde{L}_1(y)=b$ and so the space $W_{\tilde{L}_0(f)}$ is left invariant by G_L. Furthermore, $W_{\tilde{L}_0(f)}/W_1$ is a trivial one-dimensional G_L-module. Since G_L is a reductive group, W_1 has a G_L-complement in $W_{\tilde{L}_0(f)}$. This implies that there is an element $f_0\in K_L$ such that $f_0\equiv\tilde{L}_0(f) \bmod W_1$ and f_0 is left fixed by G_L. We conclude from this that $f_0\in k$ and $\tilde{L}_1(f_0)=b$.

Now let L_1 satisfy 1. and 2. above. Since $L_1(L_0(f))=b$, we have that $L_0(f)-f_1\in W_1$, where W_1 is the solution space of L_1. In particular, $L_0(f)\in K_L$. Therefore, for any $\sigma\in H$, $L_0(\sigma(f)-f)=0$. This implies that the image of Φ lies in the solution space of L_0. Therefore, $\tilde{L}_0$ divides L_0 on the right and so the order of L_1 is at most the order of $\tilde{L}_1$. If these two orders are the same and L_1 is monic, then $\tilde{L}_0=L_0$ and so we must then have that $L_1=\tilde{L}_1$. □

The following example illustrates this proposition:

Example 2.2. Let $k=\mathbb{C}(x)$ and $L=D^2-4xD+(4x^2-2)=(D-2x)\circ(D-2x)$. A basis for the solution space of equation $L(y)=0$ is $\{e^{x^2}, xe^{x^2}\}$ so the Galois group of this homogeneous equation over k is $\mathbb{C}^*$.

For any $(c,d)\in\mathscr{C}^2$, $(c,d)\neq(0,0)$, we have that $(c+dx)e^{x^2}$ is a solution of $L(y)=0$ and so L has a right factor of the form $D-(2x+\frac{d}{c+dx})$. Furthermore, all right factors of order one are of this form. Therefore the formula

$$L=\left(D-\left(2x-\frac{d}{c+dx}\right)\right)\circ\left(D-\left(2x+\frac{d}{c+dx}\right)\right)$$

with $(c,d)\neq(0,0)$ yields a parameterization of all irreducible factorizations of L.

We shall now compute the Galois groups of $L(y)=b$ where $b=4x^2-2,1$ and $\frac{1}{x}$.

1. $b=4x^2-2$. In this case the equation $L(y)=b$ has the rational solution $y=1$. This implies that the W of Proposition 2.1 is trivial and so the Galois group of $L(y)=b$ is $\mathscr{C}^*$.

2. $b=1$. A partial fraction computation shows that $L(y)=1$ has no rational solutions. Now let us search for first order left factors L_1 of L such that $L_1(y)=1$ has a rational solution. A calculation shows that the equation

$$y'-\left(2x-\frac{d}{c+dx}\right)y=1 \tag{1}$$

has a rational solution $y=f$ if and only if $z=(c+dx)f$ is a rational solution of

$$z'-2xz=c+dx \tag{2}$$

(cf., Lemma 2.4). The rational solutions of (2) must be polynomials and one sees that this has a polynomial solution if and only if $c=0$. Therefore the space W of Proposition 2.1 is the solution space of $y'-(2x+\frac{1}{x})y=0$, that is, the space spanned by xe^{x^2} in the solution space of $L(y)=0$. Therefore the Galois group of $L(y)=1$ is $\mathscr{C}\rtimes\mathscr{C}^*$.

3. $b=\frac{1}{x}$. We shall show that for any $(c,d)\neq(0,0)$, the equation

$$y'-\left(2x-\frac{d}{c+dx}\right)y=\frac{1}{x} \tag{3}$$

has no rational solution. This implies that $L(y)=\frac{1}{x}$ also has no rational solution and so the W of Proposition 2.1 is the solution space of $L(y)=0$. Therefore the Galois group of $L(y)=\frac{1}{x}$ is $\mathscr{C}^2\rtimes\mathscr{C}^*$.

Eq. (3) has a rational solution $y=f$ if and only if $z=(c+dx)f$ is a rational solution of

$$z'-2xz=\frac{c+dx}{x}. \tag{4}$$

If $c\neq 0$ then any rational solution of (4) must have a pole at $x=0$. Comparing orders of the left and right-hand side of this equation yields a contradiction. Therefore $c=0$. Similar considerations show that $z'-2xz=d$ can never have a rational solution if $d\neq 0$. □

Proposition 2.1 allows us to give a detailed description of the Picard–Vessiot extension of k corresponding to $L(y)=b$.

Corollary 2.3. *Let k, b, L be as above and let K_L be the Picard–Vessiot extension of k corresponding to $L(y)=0$. Let $L_1 \in k[D]$ be the unique monic operator of maximal order satisfying*

1. *$L_1(y)=b$ has a solution $f_1 \in k$, and*
2. *$L = L_1 L_0$ for some $L_0 = D^t - b_{t-1}D^{t-1} - \cdots - b_0 \in k[D]$.*

Then the Picard–Vessiot extension K of k corresponding to $L(y)=b$ is the field $K_L(z_0, z_1, \ldots, z_{t-1})$ where $z_0, z_1, \ldots, z_{t-1}$ are algebraically independent, $z_i' = z_{i+1}$ for $i = 0, \ldots, t-2$ and $z_{t-1}' = f_1 + b_0 z_0 + \cdots + b_{t-1} z_{t-1}$.

Proof. Let V be the solution space of $(D - b'/b)L$ in K. The linear operator L_0 maps V onto the solution space of $(D - b'/b)L_1$. Therefore, there exists a $z \in V$ such that $L_0(z) = f_1$. Since $L(z) = b$, we have that $K = K_L\langle z \rangle$. Since the Galois group of K over K_L is a vector group of dimension t, we have that K is a purely transcendental extension of K_L of transcendence degree t. Therefore $K = K_L(z, z', \ldots, z^{(t-1)})$. The elements $z_i = z^{(i)}$ satisfy the conclusion of the Corollary. □

Proposition 2.1 also implies that in order to find the Galois group of $L(y)=b$ we must

1. Calculate the Galois group G_L of L, and
2. Find the monic operator L_1 of maximal order satisfying 1. and 2. of Proposition 2.1 and identify the action of G on the solution space of L_0.

The first task was dealt with in [3]. In this paper it is shown (Theorem 4.1 [1] and its proof) how for all points $z_0 \in \mathbb{C}$ outside some finite set (depending on L), one can calculate a matrix representation for the Galois group of L in the basis $\{y_0, \ldots, y_{n-1}\}$ of the solution space given by $y_i^{(j)}(z_0) = \delta_{i,j}$.

Dealing with the second task will occupy the remainder of this section. We begin by recalling some basic definitions and facts concerning linear differential equations.

Two operators L_2 and L_1 are said to be equivalent if the $\mathscr{D}$-modules $\mathscr{D}/\mathscr{D}L_2$ and $\mathscr{D}/\mathscr{D}L_1$ are $\mathscr{D}$-isomorphic (see [13]). This is equivalent to the statement that the two operators have the same order m and that there exist operators R, S of orders at most $m-1$ with $\mathrm{GCRD}(R, L_1) = 1$ such that

$$L_2 R = S L_1. \tag{5}$$

Note that such an operator R can be used to define a map $1 \mapsto R$ which gives the isomorphism from $\mathscr{D}/\mathscr{D}L_2$ to $\mathscr{D}/\mathscr{D}L_1$. We note that the ring $\mathscr{D}$ is a left and right euclidean domain. In particular given operators $U, V \in \mathscr{D}$ an extended euclidean algorithm yields operators $A, B \in \mathscr{D}$, $\mathrm{ord}\, A < \mathrm{ord}\, V, \mathrm{ord}\, B < \mathrm{ord}\, U$, such that $AU + BV = \mathrm{GCRD}(U, V)$.

Lemma 2.4. *Let $L_1, L_2 \in \mathscr{D}$ be equivalent operators and $S \in \mathscr{D}$ as in Eq. (5). The equation $L_1(y) = b$, $b \in k$ has a solution in k if and only if the equation $L_2(y) = S(b)$ has a solution in k.*

[1] This theorem is stated in terms of matrix systems $Y' = AY$ but the translation to scalar equations $L(y)=0$ is immediate.

Proof. The extended euclidean algorithm yields $\tilde{R}$ and $\tilde{L}_1$ in $\mathscr{D}$ such that $\tilde{R}R+\tilde{L}_1L_1=1$ and ord $\tilde{R}<$ ord L_1. The map $v\mapsto R(v)$ is an isomorphism of V_{L_1} (the solution space of L_1) onto V_{L_2} and the map $w\mapsto \tilde{R}(w)$ is the inverse of this isomorphism [13]. Since $L_1\tilde{R}$ and $R\tilde{R}-1$ vanish on V_{L_2}, we have that L_2 divides both of these operators. Therefore there exist $\tilde{S}$ and $\tilde{L}_2\in\mathscr{D}$ such that $L_1\tilde{R}=\tilde{S}L_2$ and $R\tilde{R}+\tilde{L}_2L_2=1$.

We now claim that $\tilde{S}S+L_1\tilde{L}_1=1$. We have that

$$\begin{aligned}(\tilde{S}S+L_1\tilde{L}_1)L_1 &= \tilde{S}SL_1+L_1\tilde{L}_1L_1\\ &= \tilde{S}L_2R+L_1(1-\tilde{R}R)\\ &= \tilde{S}L_2R+L_1-L_1\tilde{R}R\\ &= \tilde{S}L_2R+L_1-\tilde{S}L_2R\\ &= L_1,\end{aligned}$$

and the equation follows after cancelling L_1 on the right.

To prove one direction of the lemma, suppose $L_1(f)=b$ for some $f\in k$. If $h=R(f)\in k$, then $L_2(h)=SL_1(f)=S(b)$ as desired. To prove the other direction, suppose $L_2(h)=S(b)$ for some $h\in k$. Let $f=\tilde{R}(h)+\tilde{L}_1(b)\in k$. Then

$$\begin{aligned}L_1(f) &= L_1\tilde{R}(h)+L_1\tilde{L}_1(b)\\ &= \tilde{S}L_2(h)+(1-\tilde{S}S)(b)\\ &= \tilde{S}S(b)+b-\tilde{S}S(b)\\ &= b,\end{aligned}$$

completing the proof. □

Any operator can be written as a product of irreducible operators and for any other factorization, one has the same number of irreducible factors. Moreover, after a possible renumbering, the irreducible factors are equivalent. By definition any completely reducible operator L can be written as the least common left multiple of a finite set of irreducible operators. Any left or right factor will therefore be equivalent to the least common left multiple of some subset of these operators. When k is a finite algebraic extension of $\mathscr{C}(x)$, where $\mathscr{C}$ is a computable algebraically closed field of characteristic zero, one can effectively factor any differential operator into a product of irreducible differential operators, determine if an operator is completely reducible and, if so, effectively write it as a least common left multiple of irreducible operators [3].

We shall attack the second task above in the following way. We start by writing L as the least common left multiple of a set of irreducible operators $\mathscr{T}=\{T_1,\ldots,T_s\}$. Any monic operator L_1 dividing L on the left is equivalent to a least common left multiple of elements from $\mathscr{T}$. We fix a subset of $\mathscr{T}$ and let L_2 be the least common left multiple of elements of this subset. We will show below that one can parameterize all pairs of elements (L_1,S), ord $S<$ ord $L_1=$ ord L_2, where S and L_2 are as in Eq. (5) and L_1 divides L on the left. We furthermore will show that one can decide if there are values of the parameters so that $L_1(y)=b$ has a solution in k. Performing these tasks over all subsets of $\mathscr{T}$, we will eventually find an operator L_1 of maximal

order satisfying conditions 1. and 2. of Proposition 2.1. We will then show how to describe the action of G_L on the solution space of L_0 where $L = L_1 L_0$.

The following three lemmas are used to describe the set of pairs (L_1, S) mentioned above. The fourth lemma will be used to decide if there are values of the parameters so that $L_1(y) = b$ has a solution in k.

Let $k = \mathscr{C}(x)$. For $a = \frac{p}{q} \in k$, $p, q \in \mathscr{C}[x]$, $(p, q) = 1$, we define $\deg a = \max(\deg p, \deg q)$. For $L = a_n D^n + a_{n-1} D^{n-1} + \cdots + a_0 \in k[D]$, we define $\deg L = \max_{1 \le i \le n}(\deg a_i)$ and $\operatorname{ord} L = n$. Given operators L and L_2, we will want to parameterize all pairs of operators (L_1, S) satisfying:

1. L_1 is a monic operator equivalent to L_2 that divides L on the left, and
2. $\operatorname{ord} S \le \operatorname{ord} L_2 - 1$ and $L_2 R = S L_1$ for some $R \in \mathscr{D}$, $\operatorname{GCRD}(L_1, R) = 1$.

Lemma 2.5. *Let T_1 and T_2 be operators with coefficients in $\mathscr{C}(x)$ of orders n and m and degrees N and M respectively. If T_3 is an operator with coefficients in $\mathscr{C}(x)$ such that $T_3 T_2 = T_1$, then* $\deg T_3 \le (n - m + 1)^2 M + N$.

Proof. Let $T_1 = \sum_{i=0}^{n} a_i D^i$, $T_2 = \sum_{i=0}^{m} b_i D^i$ and $T_3 = \sum_{i=0}^{n-m} c_i D^i$. The equation $T_3 T_2 = T_1$ yields a system of (algebraic) linear equations

$$\begin{pmatrix} a_n \\ a_{n-1} \\ \vdots \\ a_0 \end{pmatrix} = B \begin{pmatrix} c_{n-m} \\ c_{n-m-1} \\ \vdots \\ c_0 \end{pmatrix},$$

where B is a matrix whose entries are sums of terms of the form $D^j(b_i), 0 \le j \le n-m$. Therefore $\deg B \le (n-m+1)M$. A solution of this system will be unique so the matrix B has rank $n - m$. Therefore there is an $(n - m) \times (n - m)$ invertible submatrix $\tilde{B}$ of B. For convenience of notation we shall assume this is formed by the first $n - m$ rows of B. We then have

$$\begin{pmatrix} c_{n-m} \\ c_{n-m-1} \\ \vdots \\ c_0 \end{pmatrix} = \tilde{B}^{-1} \begin{pmatrix} a_n \\ a_{n-1} \\ \vdots \\ a_{m+1} \end{pmatrix}.$$

Since $\deg \tilde{B}^{-1} \le (n - m + 1) \deg \tilde{B} \le (n - m + 1)^2 M$, we have that

$$\deg \begin{pmatrix} c_{n-m} \\ c_{n-m-1} \\ \vdots \\ c_0 \end{pmatrix} = \left(\tilde{B}^{-1} \begin{pmatrix} a_n \\ a_{n-1} \\ \vdots \\ a_{m+1} \end{pmatrix} \right) \le (n - m + 1)^2 M + N. \qquad \square$$

Lemma 2.6. *Let $k=\mathscr{C}(x)$ and L, L_2 be monic operators in $\mathscr{D}$ of orders n and m, respectively.*

1. *For any i, $0 \leq i \leq \operatorname{ord} L$ one can effectively find an integer n_i such that if $L=L_1L_0$ with monic $L_1, L_0 \in \mathscr{D}$ and $\operatorname{ord} L_1 = i$ then $\deg L_0 \leq n_i$.*

2. *One can effectively find an integer N such that if $L_2\tilde{R}=\tilde{S}L$ for some $\tilde{R},\tilde{S}\in\mathscr{D}$ with $\operatorname{ord}\tilde{R} < \operatorname{ord} L$ and $\operatorname{ord}\tilde{S} < \operatorname{ord} L_2$, then $\deg\tilde{S} \leq N$.*

3. *One can effectively find an integer M such that if L_1 is a monic operator equivalent to L_2, dividing L on the left, then there exist R and S in $\mathscr{D}$ such that $L_2R=SL_1$, $\operatorname{ord} R < \operatorname{ord} L_1$, $\operatorname{ord} S < \operatorname{ord} L_2$ and $\deg R, \deg S \leq M$.*

Proof. 1. This fact is well known (cf., Section 5.1 of [3] and also [5]; the latter paper also contains explicit bounds) and so we only outline the proof. Let $L=L_1L_0$ and $\operatorname{ord} L_1 = n-i$ and let $\{y_1,\ldots,y_{n-i}\}$ be a fundamental set of solutions of $L_1(y)=0$. The coefficients of L_1 are quotients a/w where w is the wronskian determinant of $\{y_1,\ldots,y_{n-i}\}$ and a is the determinant of some $(n-i)\times(n-i)$ submatrix of $W=(y_l^{(j)})_{l=1,\ldots,n-i}^{j=0,\ldots,n-i}$ (note that w is also the determinant of such a matrix). Since the logarithmic derivative of w is in k, we have that the logarithmic derivative of a is also in k. Furthermore, the determinants of $(n-i)\times(n-i)$ submatrices of W satisfy an equation $L^{\wedge i}(y)=0$ where $L^{\wedge i}$ is an operator that can be effectively constructed from L. Therefore the coefficients of L_0 are quotients of two solutions of $L^{\wedge i}(y)=0$, each of which has logarithmic derivative in k. One can effectively find sets of rational functions $\{g_r\}$, $\{f_{rs}\}$ such that the elements $e^{\int g_r}$ are algebraically independent over k and if y satisfies $L^{\wedge i}(y)=0$, $y'/y\in k$, then for some r there are constants $\{c_s\}$ such that $y=(\sum c_s f_{rs})e^{\int g_r}$. If a quotient of two such elements lies in k it will be of the form $\sum d_s f_{rs}/\sum c_s f_{rs}$ for some constants c_s, d_s, and so $\deg L_0$ can be bounded in terms of the degrees of the f_{rs}.

2. We will consider the dual equation $\tilde{R}^*L_2^* = L^*\tilde{S}^*$ formed by taking adjoints (the *adjoint* of an operator $L=\sum_{i=0}^n a_iD^i$ is the operator $L^*=\sum_{i=0}^n(-1)^iD^ia_i$, [12], Ch. 10). Ore showed (see [13] for a modern presentation and references) that there exists an $(m\times m)$ matrix $\mathscr{A}$ whose entries lie in $\mathscr{D}$ and can be calculated from the coefficients of L and L_2 such that $\tilde{S}^* = s_0 + s_1D + \cdots + s_{m-1}D^{m-1}$ satisfies such an equation if and only if $\mathscr{A}(s_0,\ldots,s_{m-1})=0$. Using row and column operations one can find a set of linear scalar equations equivalent to the system $\mathscr{A}(s_0,\ldots,s_{m-1})=0$ (see [4]). Using standard algorithms to find rational solutions of scalar linear differential equations one can therefore find a bound on $\deg\tilde{S}^*$ and therefore on $\deg\tilde{S}=\deg\tilde{S}^{**}$.

3. Let $L=L_1L_0$. From 1., one can effectively calculate an integer n_i such that $\deg L_0 \leq n_i$. Lemma 2.5 then allows us to calculate an integer m_i such that $\deg L_1 \leq m_i$. If $L_2R=SL_1$ with $\operatorname{ord} R < \operatorname{ord} L_1$ and $\operatorname{ord} S < L_2$ then $L_2(RL_0)=SL_1L_0=SL$. From 2., we have that there is a computable integer N such that $\deg S \leq N$. Let $i=\operatorname{ord} L_2=\operatorname{ord} L_1$. Taking adjoints in the equation $L_2R=SL_1$ we have that $R^*L_2^*=L_1^*S^*$. One can bound $\deg L_1^*S^*$ in terms of $\deg L_1^*$ and $\deg S^*$. Applying Lemma 2.5 to the equation $R^*L_2^*=L_1^*S^*$ allows us to bound $\deg R^*$ and therefore $\deg R$. □

Before stating the next lemma, we introduce the following notion. Let $L=\sum_{i=0}^{n} a_i D^i \in \mathscr{C}(x)[D]$ be an operator of order n and degree at most m where each

$$a_i = \frac{\sum_{j=0}^{m} b_{i,j} x^j}{\sum_{j=0}^{m} c_{i,j} x^j}$$

with $b_{i,j}, c_{i,j} \in \mathscr{C}$. We may identify the operator L with the vector $(b_{0,0}, b_{0,1}, \ldots, c_{n-1,m}) \in \mathscr{C}^{2(n+1)(m+1)}$. We say that a set of operators $\mathscr{L}$ is *constructible* if, under this identification, they form a constructible subset of $\mathscr{C}^{2(n+1)(m+1)}$.

Lemma 2.7. *Let k, L and L_2 be as in the hypotheses of Lemma* 2.6.

1. *The set of pairs of monic operators (L_1, L_0), $\operatorname{ord} L_1 = m$, $\operatorname{ord} L_0 = n - m$ such that $L = L_1 L_0$ forms a constructible set whose defining equations can be explicitly computed.*
2. *Let n_m be as in Lemma* 2.6.1 *and M be as in Lemma* 2.6.3. *The set $\mathscr{P}_{L_2}$ of triples of operators (L_1, R, S) where*
   2.1. $\operatorname{ord} L_1 = m; \deg L_1 \le n_m$; $\operatorname{ord} R, S \le m - 1$; $\deg R, S \le M$,
   2.2. *L_1 divides L on the the left,*
   2.3. *$GCRD(L_1, R) = 1$,*
   2.4. *$L_2 R = S L_1$ (and so L_1 is equivalent to L_2)*
   is constructible. Furthermore, one can effectively calculate the defining equations of $\mathscr{P}_{L_2}$.
3. *The set $\mathscr{M}_{L_2}$ of pairs (L_1, S) such that for some $R \in \mathscr{D}$, $(L_1, R, S) \in \mathscr{P}_{L_2}$ is a constructible set. Furthermore, one can effectively calculate the defining equations of $\mathscr{M}_{L_2}$.*

Proof. 1. By Lemmas 2.5 and 2.6.1, we can effectively bound the degrees of L_1 and L_0. Comparing the coefficients of D^i in the equation $L = L_1 L_0$ yields defining conditions for the constructible set.

2. Projecting the set defined in 1. yields the set $\mathscr{L}_1$ of L_1 that divide L on the left. Therefore this is a constructible set. Lemma 2.6.3 yields a bound on the degrees of R and S. Therefore, the set of (L_1, R, S) such that $L_2 R = S L_1$, $L_1 \in \mathscr{L}_1$ is a constructible set. Imposing the condition that $\mathrm{GCRD}(L_1, R) = 1$ yields a constructible subset.

3. This follows from the fact that the projection of a constructible set is constructible. □

Let $L = y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_0 y \in \mathscr{C}(x)[D]$, let $\alpha \in \mathscr{C}$ and let $m_\alpha = \min_{0 \le i \le n}\{m_i - i\}$ where m_i is the order of a_i at α. Let S_L be the set of pairs (m, α) where m is a negative integer, $\alpha \in \mathscr{C}$ and $L((x-\alpha)^m)$ has order at α strictly larger than $m + m_\alpha$. If $(m, \alpha) \in S_L$, then α must be a finite singular point of L. Furthermore, for any finite singular point α, there is a nonzero polynomial equation (the *indicial equation at* α) such that the set of m with $(m, \alpha) \in S_L$ is precisely the set of roots of this equation. This equation can be effectively determined from the $(x-\alpha)$-adic expansion of the a_i.

In particular, the set S_L is a finite set that can be effectively determined. Similar calculations can be done at infinity (i.e., at 0 for the equation obtained after replacing x by $1/t$ and d/dx by $-t^2 d/dt$) to determine a finite set S_L^∞ of positive integers m having the property that $L(x^m)$ has order at infinity strictly larger than $-m+m_\infty$. Here $m_\infty = \min_{0\le i\le n}\{\tilde{m}_i + i\}$ where $\tilde{m}_i$ is the order of a_i at infinity.

Lemma 2.8. *Let $k=\mathscr{C}(x)$, N an integer and $L=y^{(n)}+\cdots+a_0 y\in\mathscr{D}$. The set $\mathscr{V}$ of $(c_0,\ldots,c_N,d_0,\ldots,d_N)\in\mathscr{C}^{2N+2}$ such that*

$$L(y)=\frac{c_N x^N+\cdots+c_0}{d_N x^N+\cdots+d_0} \tag{6}$$

has a solution in k, is constructible. Furthermore, one can effectively find the defining equations of $\mathscr{V}$.

Proof. Although this result can be deduced from the results of [5], we present a direct proof here. We shall show that there is an a priori bound on the degrees of the denominator and numerator of such a solution. Let $f=\frac{p}{q}\in k$, $(p,q)=1$ be a solution of (6) for some fixed $(c_0,\ldots,c_N,d_0,\ldots,d_N)\in\mathscr{C}^{2N+2}$. We first claim that q divides

$$Q=\prod_{(n,\alpha)\in S_L}(x-\alpha)^{-n_\alpha}\cdot(d_N x^N+\cdots+d_0).$$

Let

$$q=\prod(x-\alpha)^{n_\alpha}$$

be the factorization of q. If $(-n_\alpha,\alpha)\in S_L$, then $(x-\alpha)^{n_\alpha}$ divides Q. If $(-n_\alpha,\alpha)\notin S_L$ then $L(f)$ has a pole of order $n_\alpha+n$ at α. Therefore $(x-\alpha)^{n_\alpha+n}$ divides $d_N x^N+\cdots+d_0$ and so our first claim is proved. In particular, we have a bound for the degree of the denominator of f. To bound the degree of the numerator, we expand at infinity. We have that $f=x^{\deg p-\deg q}+$ smaller powers of x. If $\deg p-\deg q>\deg(c_N x^N+\cdots+c_0)-\deg(d_N x^N+\cdots+d_0)$, then $(\deg p-\deg q)\in S_L^\infty$. Therefore, $\deg p-\deg q<\max_{m\in S_L^\infty}\{m,N\}$, so we can bound the degree of p.

Let M be a bound for the degree of the denominators and numerators of possible f. The set of $(h_M,\ldots h_0,k_M,\ldots,k_0,c_N,\ldots,c_0,d_N,\ldots d_0)\in\mathscr{C}^{2M+2N+4}$ such that

$$L\left(\frac{h_M x^M+\cdots+h_0}{k_M x^M+\cdots+k_0}\right)=\frac{c_N x^N+\cdots+c_0}{d_N x^N+\cdots+d_0}$$

is clearly a constructible set. Projection yields the set $\mathscr{V}$. □

We note that the previous lemma is true when k is replaced by an algebraic extension of $\mathscr{C}(x)$ and the parameterized rational function is replaced by a parameterized set of elements from k, but for simplicity we have only stated and proved it in the more restricted context. The fact that the set of factorizations of a linear differential operator constitutes a constructible set is well known (cf., [5] and [14]). Since we need more information, we have presented our method above.

We are now in a position to deal with the second of the above tasks and present the complete algorithm to calculate the Galois group of $L(y)=b$.

Algorithm 1

Input: A completely reducible nth order operator $L\in\mathscr{C}(x)[D]$ and an element $b\in\mathscr{C}(x)$.

Output: A set of equations in n^2 variables defining the Galois group G_L of $L(y)=0$, an integer t and a rational homomorphism $\Phi: G_L \to \mathrm{GL}_t(\mathscr{C})$ such that the Galois group of $L(y)=b$ is $\mathscr{C}^t \rtimes G_L$ where the action of G_L on $\mathscr{C}^t$ by conjugation is given by Φ.

1. Write L as a least common left multiple of a set $\mathscr{T}=\{T_1,\dots,T_s\}$ of irreducible operators (using, for example, the algorithms in the Appendix of [3]).
2. If $L=L_1L_0$ then complete reducibility implies that L_1 is equivalent to the least common left multiple of some subset of $\mathscr{T}$. Fix some subset of $\mathscr{T}$ and let L_2 be the least common left multiple of its elements. For this operator, apply Lemma 2.7.3 to construct the set $\mathscr{M}_{L_2}$.
3. Let $(L_1,S)\in\mathscr{M}_{L_2}$. Lemma 2.4 implies that $L_1(y)=b$ has a solution in $\mathscr{C}(x)$ if and only if the equation
$$L_2(y)=S(b) \tag{7}$$
has a solution $y\in\mathscr{C}(x)$. Apply Lemma 2.8 to Eq. (7) to determine the set of (L_1,S) for which this equation has a rational solution.
4. Repeat steps 2. and 3. until one finds an L_2 of maximal order so that the set $\mathscr{R}_{L_2}$ of $(L_1,S)\in\mathscr{M}_{L_2}$ for which the Eq. (7) has a rational solution is nonempty. In this case, Proposition 2.1 implies that there exists a unique L_1 such that $(L_1,S)\in\mathscr{R}_{L_2}$ for some S.
5. We write $L=L_1L_0$ and let t be the order of L_0. Find defining equations of the Galois group G_L of L with respect to a basis of the solution space that contains a basis of the solution space of $L_0(y)=0$ (the results of [3] allow one to do this). In this basis the Galois group will be in block triangular form. Restriction to the space $W\simeq\mathscr{C}^t$ (i.e., selecting an appropriate block) yields the desired rational map $\Phi: G_L\to\mathrm{GL}_t(\mathscr{C})$ that gives the action of G_L on $\mathscr{C}^t$ in $\mathscr{C}^t\rtimes G_L$. □

Remarks. 1. One can easily interpret the calculations in Example 2.2 in terms of the method given above. From the factorization $L=(D-2x)\circ(D-2x)$ one sees that all factors of L are equivalent to $D-2x$. All left first order factors are given parametrically by $D-(2x-\frac{d}{c+dx})$, $(c,d)\neq(0,0)$. Therefore to decide if L has a first order left factor L_1 such that $L_1(y)=b$ has a rational solution, we must decide if there exists $(c,d)\neq(0,0)$ such that $y'-(2x-\frac{d}{c+dx})y=b$ has a rational solution. A calculation using Lemma 2.4 implies that this is equivalent to deciding if $y'-2xy=(c+dx)\cdot b$ has a rational solution. Lemma 2.8 gives a method to find all (c,d) such that this latter equation has a rational solution.

2. The results of [3] allow one to construct a presentation of the Picard–Vessiot extension associated to $L(y)=0$. These can be combined with Corollary 2.3 to give a presentation of the Picard–Vessiot extension associated with $L(y)=b$.

3. Calculating the Galois group of $L_1(L_2(y))=0$, L_1, L_2 completely reducible

We shall show how to reduce this question to the question dealt with in the previous section. This reduction was made by D. Bertrand in [1] in the context of $\mathscr{D}$-modules and this section is devoted to making Bertrand's reduction explicit and effective.

Despite the title of this section, we will find it useful to deal with first order systems $Y'+AY=0$. We begin by recalling certain facts concerning such systems (cf., [3,6]). Let k be a differential field and let $A_1, A_2 \in M_n(k)$, the ring of $n\times n$ matrices over k. We say that the systems $Y'+A_1Y=0$ and $Y'+A_2Y=0$ are equivalent if there exists a matrix $B\in \mathrm{GL}(n,k)$ such that $A_2=-B'B^{-1}+BA_1B^{-1}$. Let K be a Picard–Vessiot extension of k with Galois group G and assume that $Y'+A_1Y=0$, $Y'+A_2Y=0$ both have fundamental sets of solutions in K^n. One can show that these two systems are equivalent if and only if their solution spaces in K^n are isomorphic as G-modules (in fact, if Y_1 is a fundamental solution matrix of $Y'+A_1Y=0$ then $Y_2=BY_1$ is a fundamental solution matrix of $Y'+A_2Y=0$). To each scalar equation $L(y)=y^{(n)}+a_{n-1}y^{(n-1)}+\cdots+a_0y_0=0$ one can associate a matrix equation $Y'+A_LY=0$ where

$$A_L=\begin{pmatrix} 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_0 & \dots & \dots & \dots & a_{n-1} \end{pmatrix}.$$

The equation $L(y)=b$ can then be written as $Y'+A_LY=B$ where $B=(0,0,\dots,b)^{\mathrm{T}}$. Conversely if k contains non-constants then any system is equivalent to one of the form $Y'+A_LY=0$ [9]. Finally, it can be shown that if $L=L_1L_2$ where L_1 and L_2 are completely reducible operators, then $Y'+A_LY=0$ is equivalent to a system of the form

$$Y'+\begin{pmatrix} A_2 & C \\ 0 & A_1 \end{pmatrix} Y=0, \tag{8}$$

where the $Y'+A_1Y=0$ and $Y'+A_2Y=0$ are completely reducible (cf., [3], Section 2.3). In fact, A_1 may be taken to be A_{L_1}, A_2 may be taken to be A_{L_2}, and C may be taken to be the $m\times n$ matrix with entry -1 in the m, 1 position and 0's everywhere else, where n is the order of L_1 and m is the order of L_2. The following result is a concrete realization of Lemma 1 and the discussion in Section 2 of [1].

Lemma 3.1. *If Y_1 and Y_2 are fundamental solution matrices of $Y'+A_1Y=0$ and $Y'+A_2Y=0$ respectively then*

$$Y=\begin{pmatrix} Y_2 & UY_1 \\ 0 & Y_1 \end{pmatrix} \tag{9}$$

is a fundamental solution matrix of Eq. (8) if and only if U satisfies $U'+(A_2U-UA_1)=-C$.

Proof. Substitute and calculate. □

We note that the equation $V' + (A_2V - VA_1) = 0$ arises naturally when studying systems of linear differential equations. If $Y' + A_1Y = 0$ and $Y' + A_2Y = 0$ are two such systems then the map $Y \mapsto VY$ with V an $m \times n$ matrix with entries in k maps solutions of $Y' + A_1Y = 0$ to solutions of $Y' + A_2Y = 0$ if and only if $V' + (A_2V - VA_1) = 0$. This allows one to identify solutions of this latter equation with elements of $HOM(W_1, W_2)$ where each W_i is the solutions space of $Y' + A_iY = 0$. One can furthermore identify $HOM(W_1, W_2)$ with $W_1^* \otimes W_2$ and rewrite the differential equation $V' + (A_2V - VA_1) = 0$ in terms of this identification. We shall now make this explicit.[2]

Let V be an $m \times n$ matrix and let v_i be the ith column of V. Let $\tilde{V}$ be the column vector $(v_1^{\mathrm{T}}, \ldots, v_n^{\mathrm{T}})^{\mathrm{T}}$. A calculation shows that V satisfies $V' + A_2V - VA_1 = 0$ if and only if $\tilde{V}$ satisfies $\tilde{V}' + (-A_1^{\mathrm{T}} \otimes I_m + I_n \otimes A_2)\tilde{V} = 0$. Furthermore, if Y_1 and Y_2 are fundamental solution matrices of $Y' + A_1Y = 0$ and $Y' + A_2Y = 0$, respectively, then a calculation shows that $(Y_1^{-1})^{\mathrm{T}} \otimes Y_2$ is a fundamental solution matrix of $\tilde{V}' + (-A_1^{\mathrm{T}} \otimes I_m + I_n \otimes A_2)\tilde{V} = 0$. Denoting the columns of C by c_i we will let $\tilde{C}$ be the column vector $(c_1^{\mathrm{T}}, \ldots, c_n^{\mathrm{T}})^{\mathrm{T}}$.

Lemma 3.2. *Assume that k contains a nonconstant. Let $Y' + A_1Y = 0$ and $Y' + A_2Y = 0$ be completely reducible equations and let K be the Picard–Vessiot extension of k corresponding to Eq. (8). Let $F \subset K$ be the Picard–Vessiot extension corresponding to*

$$Y' + \begin{pmatrix} A_2 & 0 \\ 0 & A_1 \end{pmatrix} Y = 0. \tag{10}$$

Then

1. *F contains the Picard–Vessiot extension E corresponding to*

$$\tilde{V}' + (-A_1^{\mathrm{T}} \otimes I_m + I_n \otimes A_2)\tilde{V} = 0 \tag{11}$$

and so the Galois group $G(E/k)$ is a quotient of $G(F/k)$.

2. *$K = F(\tilde{V})$ where $\tilde{V}$ is a solution of*

$$\tilde{V}' + (-A_1^{\mathrm{T}} \otimes I_m + I_n \otimes A_2)\tilde{V} = -\tilde{C}. \tag{12}$$

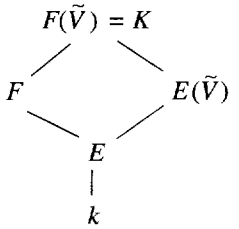
3. *The Galois group $G(E(\tilde{V})/k)$ is the semidirect product $W \rtimes G(E/k)$ of the Galois group $G(E/k)$ and a vector group W. Furthermore, the Galois group $G(K/k)$ is the semidirect product $W \rtimes G(F/k)$ where the action of $G(F/k)$ on W is given by composing the quotient map $G(F/k) \to G(E/k)$ and the action of $G(E/k)$ on W.*

Proof. The first two statements follow from the discussion preceding the lemma.

[2] One can formulate this in terms of $\mathscr{D}$-modules (although we shall not need this). Let $\mathscr{M}_1$ and $\mathscr{M}_2$ be the $\mathscr{D}$-modules associated to $Y' + A_1Y = 0$ and $Y' + A_2Y = 0$ (see [3]). One can put a natural $\mathscr{D}$-module structure on $HOM_k(\mathscr{M}_1, \mathscr{M}_2)$ such that $V \in HOM_k(\mathscr{M}_1, \mathscr{M}_2)$ defines a $\mathscr{D}$-module isomorphism if and only if $V' + (A_2V - VA_1) = 0$. The $\mathscr{D}$-modules $HOM_k(\mathscr{M}_1, \mathscr{M}_2)$ and $\mathscr{M}_1^* \otimes \mathscr{M}_2$ are isomorphic $\mathscr{D}$-modules and the above identification of the two equations $V' + (A_2V - VA_1) = 0$ and $\tilde{V}' + (-A_1^{\mathrm{T}} \otimes I_m + I_n \otimes A_2)\tilde{V} = 0$ makes explicit what we need from this identification.

To prove the third statement we note that since $Y' + A_1 Y = 0$ and $Y' + A_2 Y = 0$ are completely reducible equations, the Galois group $G(F/k)$ is a reductive group. Since the Galois group $G(E/k)$ is a quotient of $G(F/k)$ it is also reductive. If $\hat{L}$ is a scalar equation such that $Y' + A_{\hat{L}} Y = 0$ is equivalent to Eq. (11), then Eq. (12) is equivalent to $\hat{L}(y) = \hat{b}$ for some $\hat{b} \in k$. Since $G(E/k)$ is reductive, $\hat{L}$ is a completely reducible operator and we can apply Proposition 2.1 to conclude the first part of the third statement.

To prove the second part, we consider the following diagram:



We will first show that $G(F(\tilde{V})/F) \simeq G(E(\tilde{V})/E)$. To do this it suffices to show that $F \cap E(\tilde{V}) = E$ (cf., Lemma 5.10 of [8]). Since $G(E(\tilde{V})/E)$ is abelian (it is the vector group W), $F \cap E(\tilde{V})$ is a Picard–Vessiot extension of k. The Galois group $G(F \cap E(\tilde{V})/E)$ is a quotient of W and so is unipotent. Since $G(F \cap E(\tilde{V})/E)$ is also a quotient of the reductive group $G(F/k)$ it is also reductive and therefore must be trivial. Therefore $F \cap E(\tilde{V}) = E$.

Let us denote by $\tilde{W}$ the Galois group $G(K/F)$. As we have just shown this is isomorphic to W, the Galois group $G(E(\tilde{V})/E$. Since $G(K/F)/\tilde{W} \simeq G(F/k)$ is reductive, we have that $\tilde{W}$ is the unipotent radical of $G(K/k)$. Therefore $G(K/k)$ is isomorphic to $\tilde{W} \rtimes P$ where P is a Levi factor isomorphic to $G(F/k)$ (via the map that takes a $\sigma \in G(K/k)$ and restricts to F) and $\tilde{W}$ is isomorphic to W (via the map that takes $\sigma \in G(K/k)$ and restricts to $E(\tilde{V})$). We now consider the action of P on $\tilde{W}$ by conjugation. Let P_E be the subgroup of P that leaves E elementwise fixed. This is a normal subgroup of P and so is reductive. If $\sigma \in P_E$, then σ leaves $E(\tilde{V})$ invariant and so restriction gives a homomorphism of P_E to $G(E(\tilde{V})/E)$. Since this latter group is unipotent, the homomorphism must be trivial. Therefore any element of P_E leaves $\tilde{V}$ fixed and so must commute with any element of $\tilde{W}$. Therefore, the action of P on $\tilde{W}$ factors through the action of P/P_E on $\tilde{W}$, and this is the same as the action of $G(E/k)$ on W. □

This last result and its proof tell us how to compute the Galois group of Eq. (8) when $k = \mathscr{C}(x)$.

Algorithm II

Input: A system of linear differential equations (8) where $Y' + A_1 Y = 0$ and $Y' + A_2 Y = 0$ are completely reducible with $A_1 \in \mathrm{M}_n(\mathscr{C}(x)), A_2 \in \mathrm{M}_m(\mathscr{C}(x))$.

Output: A system of equations in $m + n$ variables defining the Galois group $G(F/k) \subset \mathrm{GL}_{n+m}(\mathscr{C})$ of the Picard–Vessiot extension corresponding to the system (10),

an integer t and a rational homomorphism $\Phi: G(F/k) \to \mathrm{GL}_t(\mathscr{C})$ such that the Galois group of (8) is $\mathscr{C}^t \rtimes G(F/k)$ where the action of $G(F/k)$ on $\mathscr{C}^t$ by conjugation is given by Φ.

1. One first calculates the Galois group $G(F/k)$ of Eq. (10) using the results of [3]. This Galois group will be represented as matrices acting on $\mathrm{diag}(Y_1, Y_2)$ where Y_1 is a fundamental solution matrix of $Y' + A_1 Y = 0$ and Y_2 is a fundamental solution matrix of $Y' + A_2 Y = 0$. One can easily calculate the action of $G(F/k)$ on $(Y_1^{-1})^{\mathrm{T}} \otimes Y_2$ and so calculate the Galois group $G(E/k)$ of equation (11) as well as the map $G(F/k) \to G(E/k)$.
2. Find a scalar equation $\hat{L}(y) = 0$ equivalent to the Eq. (11) as well as an element $\hat{b} \in k$ so that Eq. (12) is equivalent to $\hat{L}(y) = \hat{b}$ (an algorithm to do this is presented in [9]; in the examples below *ad hoc* methods are used). Using the transformation of $Y' + A_L Y = 0$ to $\tilde{V}' + (-A_1^{\mathrm{T}} \otimes I_n + I_m \otimes A_2)\tilde{V} = 0$ allows us to calculate the action of $G(E/k)$ on the solution space of $\hat{L}(y) = 0$.
3. Proposition 2.1 allows us to calculate a vector group W so that the Galois group of $\hat{L}(y) = \hat{b}$ (and so of Eq. (12)) is $W \rtimes G(E/k)$.
4. Lemma 3.2 now tells us that the Galois group of Eq. (8) is the group $W \rtimes G(F/k)$ where the action of $G(F/k)$ on W (i.e., the homomorphism Φ) can be calculated from the information we have. □

Remark. As in the case of the equation $L(y) = b$, the algorithms of [3] can be combined with the above to give a presentation of the Picard–Vessiot extension corresponding to $L_1(L_2(y)) = 0$.

We will now give three examples of this method. In these examples we will start with an equation of the form $L_1(L_2(y)) = 0$ with coefficients in $k = \mathscr{C}(x)$. The Galois group $G(F/k)$ that is the Galois group of equation (10) in Lemma 3.2, is the same as the Galois group of $\mathrm{LCLM}(L_1, L_2)$. In the examples we shall apply *ad hoc* methods to calculate this Galois group. We will then calculate a scalar equation equivalent to the system (11) as well as the matrix B defining this equivalence. This will allow us to find a scalar equation $\hat{L}(y) = \hat{b}$ equivalent to the system (12). We then apply the methods of Section 2 to calculate the vector space W.

Example 3.3. Consider the equation $L(y) = 0$, where $L = L_1 \circ L_2$, $L_1 = D^2 - x$, $L_2 = D^2 + \frac{1}{x}D + 1$.

The Galois group of this equation is an extension of the Galois group $G_{\tilde{L}}$ of $\tilde{L} = \mathrm{LCLM}(L_1, L_2)$. Since L_1 and L_2 are both known to have Galois group isomorphic to $\mathrm{SL}_2(\mathscr{C})$ (L_1 is a form of Airy's equation and L_2 is a Bessel equation), $G_{\tilde{L}}$ is a subgroup of $\mathrm{SL}_2(\mathscr{C}) \times \mathrm{SL}_2(\mathscr{C})$.

According to ([10], p. 1158), if $G_{\tilde{L}}$ is a *proper* subgroup of $\mathrm{SL}_2(\mathscr{C}) \times \mathrm{SL}_2(\mathscr{C})$, then there exist a scalar matrix $R = \mathrm{diag}(\alpha, \alpha)$ with entries in a quadratic extension of $\mathscr{C}(x)$ and a matrix $S \in \mathrm{GL}_2(\mathscr{C}(x))$ such that

$$\mathrm{Wr}(y_1, y_2) = R \cdot S \cdot \mathrm{Wr}(z_1, z_2),$$

where $\{y_1, y_2\}$ (resp., $\{z_1, z_2\}$) is a basis for a fundamental solution space of L_1 (resp., L_2). Assuming this is the case, one can then show that

$$\mathrm{Wr}(y_1^2, y_1y_2, y_2^2) = \hat{R} \cdot \mathrm{Wr}(z_1^2, z_1z_2, z_2^2)$$

for some matrix $\hat{R} \in \mathrm{GL}_2(\mathscr{C}(x))$. Since $\{y_1^2, y_1y_2, y_2^2\}$ (resp., $\{z_1^2, z_1z_2, z_2^2\}$) is a basis for the fundamental solution space of L_1^2 (resp., L_2^2), we see that such an equation holds if and only if L_1^2 and L_2^2 are equivalent over $\mathscr{C}(x)$.

In our case, we claim that L_1^2 and L_2^2 are *in*equivalent (and therefore that $G_{\tilde{L}} = \mathrm{SL}_2(\mathscr{C}) \times \mathrm{SL}_2(\mathscr{C})$). The expanded version of *DEtools* developed by Mark van Hoeij for MapleV.5 allows one to calculate symmetric powers, LCLM's and a basis of the ring of $\mathscr{D}$-module endomorphisms of $\mathscr{D}/\mathscr{D}L$ for an operator $L \in \mathscr{D} = \mathscr{C}(x)[D]$. Using this we proceed as follows. A calculation shows that

$$M = \mathrm{LCLM}(L_1^2, L_2^2)$$

is of order 4. If L_1^2 and L_2^2 were equivalent then $\mathscr{D}/\mathscr{D}M$ would be the direct sum of two isomorphic $\mathscr{D}$-modules. The endomorphism ring of $\mathscr{D}/\mathscr{D}M$ would therefore have dimension 4. Using the `eigenring` command in *DEtools* one sees that this ring has dimension 2 and the desired result follows.

We now consider the equation

$$\tilde{V}' + H\tilde{V} = -\tilde{C},$$

where

$$H = -A_1^{\mathrm{T}} \otimes I_2 + I_2 \otimes A_2,$$

$$A_1 = \begin{bmatrix} 0 & -1 \\ -x & 0 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0 & -1 \\ 1 & \dfrac{1}{x} \end{bmatrix},$$

$$\tilde{C} = (0, -1, 0, 0)^{\mathrm{T}}.$$

A cyclic-vector computation shows that the system $\tilde{V}' + H\tilde{V} = 0$ is equivalent to $Z' + KZ = 0$, where

$$K = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ g_1 & g_2 & g_3 & g_4 \end{bmatrix},$$

$$g_1 = \frac{x^6 + 3x^5 + 3x^4 + 5x^3 + 6x^2 + 3x - 3}{x(x^3 + x^2 + 1)},$$

$$g_2 = -\frac{x^6 + 5x^5 + 3x^3 - 7x^2 - 1}{x^3(x^3 + x^2 + 1)},$$

$$g_3 = -\frac{2x^3 - 2x^2 + 1}{x^2},$$

$$g_4 = -\frac{x^3 - 2}{x(x^3 + x^2 + 1)}.$$

The equivalence is given by the equation $Z = B\tilde{V}$, where

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -x & 0 \\ -1 + x & -\frac{1}{x} & -1 & -2x \\ 2 + \frac{1}{x} & \frac{3x^3 - x^2 + 2}{x^2} & 3x - x^2 & 0 \end{bmatrix}.$$

Therefore, the equation $\tilde{V}' + H\tilde{V} = -\tilde{C}$ is equivalent to

$$Z' + KZ = -B\tilde{C}. \tag{13}$$

(The reader can verify that $K = -B'B^{-1} + BHB^{-1}$.) Since K is in companion-matrix form, it is easy to convert (13) into the inhomogeneous scalar equation $\hat{L}(y) = \hat{b}$, where

$$\hat{L} = D^4 + g_4D^3 + g_3D^2 + g_2D + g_1 \quad (g_i \text{ as above}),$$

$$\hat{b} = \frac{x^4 + 2x^3 + x^2 + 4x + 3}{x^3 + x^2 + 1}.$$

Computations using the `DFactor` and `ratsols` commands in *DEtools* show that $\hat{L}$ is irreducible over $\mathscr{C}(x)$ and that this equation admits no rational solutions. Thus, the vector space W referred to in Lemma 3.2(3) is all of $\mathscr{C}^4$. We conclude that the Galois group G_L is $\mathscr{C}^4 \rtimes (\mathrm{SL}_2(\mathscr{C}) \times \mathrm{SL}_2(\mathscr{C}))$.

Example 3.4. Consider the equation $L(y) = 0$, where $L = L_1 \circ L_2$, $L_1 = D^2 + \frac{1}{x}D + 1$, $L_2 = D^2 - D$.

The Galois group G_L of L is once again an extension of $G_{\tilde{L}}$, the group of $\tilde{L} = \mathrm{LCLM}(L_1, L_2)$. To calculate $G_{\tilde{L}}$ note that the Galois group G_{L_1} of L_1 is SL_2 and the Galois group G_{L_2} of L_2 is the multiplicative group $\mathscr{C}^*$. The group $G_{\tilde{L}}$ is a subgroup of $G_{L_1} \times G_{L_2}$ that projects surjectively onto each factor. The Theorem of [10] implies that, in this case, $G_{\tilde{L}} = G_{L_1} \times G_{L_2}$.

We now consider the equation

$$\tilde{V}' + H\tilde{V} = -\tilde{C},$$

where

$$H = -A_1^{\mathrm{T}} \otimes I_2 + I_2 \otimes A_2,$$

$$A_1 = \begin{bmatrix} 0 & -1 \\ 1 & \frac{1}{x} \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0 & -1 \\ 0 & -1 \end{bmatrix},$$

$$\tilde{C} = (0, -1, 0, 0)^{\mathrm{T}}.$$

A cyclic-vector computation shows that the system $\tilde{V}' + H\tilde{V} = 0$ is equivalent to $Z' + KZ = 0$, where

$$K = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ g_1 & g_2 & g_3 & g_4 \end{bmatrix},$$

$$g_1 = \frac{10x^4 + 5x^3 - 6x^2 + 6x + 3}{x^2(5x^2 - 3)},$$

$$g_2 = -\frac{10x^3 + 15x^2 + 9x + 12}{x(5x^2 - 3)},$$

$$g_3 = 3\frac{5x^2 + 5x + 2}{5x^2 - 3},$$

$$g_4 = -2\frac{5x^2 + 5x - 3}{5x^2 - 3}.$$

The equivalence is given by the equation $Z = B\tilde{V}$, where

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 1 & \frac{1}{x} & 2 \\ -\frac{1}{x} & -2 & -1 & 3 + \frac{3}{x} \end{bmatrix}.$$

Therefore, the system $\tilde{V}' + H\tilde{V} = -\tilde{C}$ is equivalent to

$$Z' + KZ = -B\tilde{C}.$$

(The reader can again verify that $K = -B'B^{-1} + BHB^{-1}$.) Conversion to an inhomogeneous scalar equation yields $\hat{L}(y) = \hat{b}$, where

$$\hat{L} = D^4 + g_4D^3 + g_3D^2 + g_2D + g_1 \quad (g_i \text{ as above}),$$

$$\hat{b} = -2 + \frac{5x^2 + 5x + 12}{5x^2 - 3}.$$

Using the `eigenring` command of *DEtools*, one sees that the dimension of the endomorphism ring of $\mathscr{D}/\mathscr{D}\hat{L}$ is two. Since $\hat{L}$ is completely reducible, this implies that $\mathscr{D}/\mathscr{D}\hat{L}$ is the direct sum of two nonisomorphic irreducible $\mathscr{D}$-modules. This furthermore implies that $\hat{L}$ has exactly two nontrivial irreducible right (resp., left) factors. A computation using the command `endomorphism_charpoly` yields two different right factors. From these one calculates the unique left factors and then one can show that for neither of

these left factors $\bar{L}$ does the equation $\bar{L}(y)=\hat{b}$ have a rational solution. Since $\hat{L}(y)=\hat{b}$ also has no rational solutions, we conclude that G_L is $\mathscr{C}^4 \rtimes (\mathrm{SL}_2(\mathscr{C}) \times \mathscr{C}^*)$.

Example 3.5. Consider the equation $L(y)=0$, where $L=L_1 \circ L_2$, $L_1=\mathrm{LCLM}(D-2x, D)$, $L_2=D^2$.

Here it is clear that $G_{\tilde{L}}$, the group of $\tilde{L}=\mathrm{LCLM}(L_1, L_2)$, is $\mathscr{C}^*$.

We now consider the equation

$$\tilde{V}' + H\tilde{V} = -\tilde{C},$$

where

$$H = -A_1^{\mathrm{T}} \otimes I_2 + I_2 \otimes A_2,$$

$$A_1 = \begin{bmatrix} 0 & -1 \\ 0 & -2x - \dfrac{1}{x} \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix},$$

$$\tilde{C} = (0, -1, 0, 0)^{\mathrm{T}}.$$

A cyclic-vector computation shows that the system $\tilde{V}' + H\tilde{V} = 0$ is equivalent to $Z' + KZ = 0$, where

$$K = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & h_1 & h_2 \end{bmatrix},$$

$$h_1 = 2\frac{8x^6 - 12x^4 + 18x^2 + 9}{4x^4 + 3},$$

$$h_2 = 4\frac{x(4x^4 - 4x^2 + 3)}{4x^4 + 3}.$$

The equivalence is given by the equation $Z = B\tilde{V}$, where

$$B = \begin{bmatrix} 0 & -x & -x & 0 \\ x & -1 & 2x^2 & -x \\ -2x^2 + 1 & 2x & -2x(2x^2 - 1) & 4x^2 \\ 2x(2x^2 - 3) & -6x^2 + 3 & 4x^2(2x^2 - 3) & -6x(2x^2 - 1) \end{bmatrix}.$$

Therefore, the equation $\tilde{V}' + H\tilde{V} = -\tilde{C}$ is equivalent to

$$Z' + KZ = -B\tilde{C}.$$

(The reader can once again verify that $K = -B'B^{-1} + BHB^{-1}$.) In this example, the equivalent inhomogeneous scalar equation is $\hat{L}(y) = \hat{b}$, where

$$\hat{L} = D^4 + h_2 D^3 + h_1 D^2,$$

$$\hat{b} = 3 - 6x^2 + 6\frac{4x^4 - 8x^2 - 5}{4x^4 + 3}.$$

The `eigenring` command shows that the corresponding endomorphism ring has dimension 10 and yields a basis of this ring. Applying the `endomorphism_charpoly` to each of these will yield a list of right factors and a simple calculation yields their corresponding left factors. Despite the fact that in this case there is an infinite set of left factors, there is a third order operator

$$L_0 = D^3 + \frac{8x^6 - 12x^4 + 6x^2 + 3}{x(4x^4 + 3)}D^2 - 2\frac{8x^6 + 3}{x^2(4x^4 + 3)}D + 2\frac{8x^6 + 12x^4 - 6x^2 + 3}{x^3(4x^4 + 3)}$$

on this list of left factors such that $L_0(y) = \hat{b}$ admits the rational solution $y = -\frac{1}{4}x(6x^2 + 5)$. Meanwhile, another computation shows $\hat{L}(y) = \hat{b}$ admits no rational solutions. We are therefore able to avoid a calculation involving parameterized operators. Thus, we have

$$G_L = \mathscr{C} \rtimes \mathscr{C}^*.$$

Acknowledgements

We would like to thank Mark van Hoeij for making available to us his wonderful improvements to the *DEtools* package in *Maple*.

References

[1] D. Bertrand, Extensions de D-modules et groupes de Galois différentiels, in: F.B. et al. (Eds.), P-adic analysis (Trento, 1989), Lecture Notes in Mathematics, vol. 1454, Springer, Berlin, 1990, pp. 125–141.
[2] D. Bertrand, Un analogue différentiel de la théorie de Kummer, in: P. Philippon (Ed.), Approximations Diophantiennes et Nombres Transcendents, Luminy 1990, Walter de Gruyter, Berlin, 1992, pp. 39–49.
[3] E. Compoint, M.F. Singer, Calculating Galois groups of completely reducible linear operators, J. Symbol. Comput., in press; a preprint is available at `http://www.math.ncsu.edu/~singer`.
[4] J. Davenport, M.F. Singer, Elementary and liouvillian solutions of linear differential equations, J. Symbol. Comput. 2 (3) (1986) 237–260.
[5] D.Y. Grigoriev, Complexity of factoring and calculating the gcd of linear ordinary differential operators, J. Symbol. Comput. 10 (1) (1990) 7–38.
[6] A. Haefliger, Local theory of meromorphic connections in dimension one (Fuchs theory), in: Borel et al. (Eds.), Algebraic D-Modules, Academic Press, 1987, ch. III., pp. 129–149.
[7] J. Humphreys, Linear Algebraic Groups, Graduate Texts in Mathematics, Springer, New York, 1975.
[8] I. Kaplansky, An Introduction to Differential Algebra, 2nd ed., Hermann, Paris, 1976.
[9] N. Katz, A simple algorithm for cyclic vectors, Amer. J. Math. 109 (1987) 65–70.
[10] E. Kolchin, Algebraic groups and algebraic dependence, Amer. J. Math. 90 (1968) 1151–1164.
[11] G.D. Mostow, Fully reducible subgroups of algebraic groups, Amer. J. Math. 78 (1956) 211–264.

[12] E.G.C. Poole, Introduction to the Theory of Linear Differential Equations, Dover, New York, 1960.
[13] M.F. Singer, Testing reducibility of linear differential operators: a group theoretic perspective, Appl. Algebra Eng. Commun. Comput. 7 (1996) 77–104.
[14] S.P. Tsarev, An algorithm for complete enumeration of all factorizations of a linear ordinary differential operator, in: L.Y.N. (Ed.), Proc. 1996 Internat. Symp. on Symbolic and Algebraic Computation, ACM Press, New York, 1996, pp. 226–231.