J. Symbolic Computation (1998) **11**, 1–22

Computing Galois Groups of Completely Reducible Differential Equations

ELIE COMPOINT[§†] AND MICHAEL F. SINGER[*‡]

[§] *Mathématiques, Université de Paris VI, T. 46, Case 247, 4, Place Jussieu, 75 230 Paris Cédex 05*
[*] *Department of Mathematics, North Carolina State University, Raleigh, NC 27695-8205*

(Received April 25, 1997)

We give an algorithm to calculate a presentation of the Picard-Vessiot extension associated to a completely reducible linear differential equation (i.e., an equation whose Galois group is reductive). Using this, we show how to compute the Galois group of such an equation as well as properties of the Galois groups of general equations.

1. Introduction

At present we do not know a general algorithm that will compute the Galois group of a linear differential equation with coefficients in a differential field k, even when $k = \bar{\mathbb{Q}}(x)$, where $\bar{\mathbb{Q}}$ is the algebraic closure of the rational numbers. In contrast, algorithms for calculating the Galois group of a polynomial with coefficients in $\mathbb{Q}$ or $\bar{\mathbb{Q}}(x)$ have been known for a long time (Cohen, 1993; van der Waerden, 1953; Pohst and Zassenhaus, 1989). The key idea behind these methods is to represent the splitting field of a polynomial in terms of generators and relations. The Galois group is then the set of permutations of the generators that preserve the relations. In the differential case, the analogue of the splitting field is called the Picard-Vessiot extension and the Galois group is defined as the group of differential automorphisms leaving elements of the base field fixed. The obstruction to mimicking the ideas from the Galois theory of polynomials is that, at present, we do not know how to effectively present a general Picard-Vessiot extension in terms of generators and relations. In this paper, we will show that for differential equations whose Galois group is reductive, one can effectively present the corresponding Picard-Vessiot extension and from this presentation compute the Galois group.

In (Compoint, 1996a; Compoint, 1996b), the first author showed that if a Picard-Vessiot extension has a reductive unimodular Galois group then the relations defining this extension come from the invariants of the Galois group. To be more specific, let k be a differential field of characteristic zero with algebraically closed field C of constants and let $Y' = AY$ be a differential equation where A is an $n \times n$ matrix with entries in k. Let $G \subset SL(n)$ be the Galois group and let its action on the polynomial ring $C[Y_{1,1}, \ldots, Y_{n,n}]$

[†] E-mail: `compoint@riemann.math.jussieu.fr`
[‡] E-mail: `singer@math.ncsu.edu` . Research partially supported by NSF Grant CCR-93222422

0747–7171/90/000000 + 00 $03.00/0

be defined by letting each element of G act on the $n \times n$ matrix $[Y_{i,j}]$ by multiplication on the left. Since G is reductive, the ring $C[Y_{1,1}, \ldots, Y_{n,n}]^G$ of invariants is finitely generated. Compoint showed that if this ring is generated by polynomials of degree at most m, then the Picard-Vessiot extension is the quotient field of the ring $k[Y_{1,1}, \ldots, Y_{n,n}]/I$, where I is an ideal generated by polynomials of degree at most m as well. It is known that given m, one can calculate these generators directly from the equation $Y' = AY$, without a priori knowledge of the Galois group (van Hoeij and Weil, 1996). Therefore the question of determining the Galois group of an equation $Y' = AY$ with reductive unimodular group is reduced to the question of finding a bound on the degrees of the generators of the ring of invariants. The main result of this paper is that there is an effective method to find such a bound.

The rest of the paper is organized as follows. In Section 2 we review some material concerning the relationship between connections, differential equations and $\mathcal{D}$-modules, discuss the concept of completely reducible operators in these settings and prove some ancillary results concerning exponential extentions of differential fields. In Section 3, we show how to bound the degree of generators of the invariants of the Galois group of a completely reducible operator. In Section 4 we show how one can use these bounds together with the results of (Compoint, 1996a; Compoint, 1996b) to give an effective presentation of the Picard-Vessiot extension of an algebraic extension of $C(x)$ associated to a completely reducible differential operator and show how this can be used to compute the Galois group of this extension. We also show how to apply this result to *arbitrary* operators to deduce properties (e.g. , connectedness) of their Galois groups. We have included an appendix where we give algorithms to factor linear operators over algebraic extensions of $C(x)$ as well as algorithms to decide if operators over these fields are completely reducible.

We would like to thank Dimitri Chmelkine for Lemma 3.1 in Section 3.2.

All fields in this paper will be assumed to be of characteristic zero. We shall use the term *computable field* to denote a field in which the field operations are recursive functions and over which we can factor polynomials. We shall also assume that the reader is familiar with the basics of the Picard-Vessiot theory, (Kaplansky, 1976; Kolchin, 1976; Magid, 1994).

2. Connections, Equations and $\mathcal{D}$-Modules

In this section we start by giving a quick review of the definitions and basic facts concerning these topics. We then characterize linear differential equations whose Galois groups are reductive groups and give procedures to determine if an equation has a reductive Galois group as well as constructions that will be used later in this paper. Throughout this section k is a differential field with algebraically closed field of constants C.

2.1. Connections

A *connection* is a finite dimensional k-space $\mathcal{M}$ with an operator $\nabla : \mathcal{M} \to \mathcal{M}$ satisfying

$$\begin{aligned} \nabla(u+v) &= \nabla(u) + \nabla(v) \\ \nabla(fu) &= f'u + f\nabla(u) \end{aligned}$$

for all $u, v \in \mathcal{M}$ and $f \in k$ (c.f., (Haefliger, 1987)). We shall refer to the k-dimension of $\mathcal{M}$ as the dimension of the connection. If $e_1, \ldots, e_n$ is a k-basis of $\mathcal{M}$, we may write

$$\nabla e_i \quad = \quad -\sum_j a_{j,i} e_j \tag{2.1}$$

where $A = (a_{i,j}) \in HOM_k(\mathcal{M}, \mathcal{M})$. If $u = \sum_i u_i e_i$, then $\nabla(u) = \sum_i (u_i' - \sum_j a_{i,j} u_j) e_i$. Therefore, once a basis of $\mathcal{M}$ has been selected and the identification $\mathcal{M} \simeq k^n$ has been made, we have that $u \in k^n$ satisfies $u' = Au$ if and only if $\nabla u = 0$. Conversely, given a system $Y' = AY$, $A \in HOM(k^n, k^n)$ one can use equation 2.1 to define a connection ∇_A on k^n. A connection $(\mathcal{N}, \nabla_N)$ is a subconnection of $(\mathcal{M}, \nabla)$ if $\mathcal{N} \subset \mathcal{M}$ and $\nabla_N = \nabla|_N$. Given a connection and a subconnection one can define a quotient connection and if $(\mathcal{M}_1, \nabla_1)$ and $(\mathcal{M}_2, \nabla_2)$ are two connections one can form the direct sum $(\mathcal{M}_1 \oplus \mathcal{M}_2, \nabla_1 \oplus \nabla_2)$ and the tensor product $(\mathcal{M}_1 \otimes \mathcal{M}_2, \nabla_1 \otimes 1 + 1 \otimes \nabla_2)$ in the obvious ways. A morphism $\phi : (\mathcal{M}_1, \nabla_1) \to (\mathcal{M}_2, \nabla_2)$ is a k-linear map $\phi : \mathcal{M}_1 \to \mathcal{M}_2$ such that $\phi \circ \nabla_1 = \nabla_2 \circ \phi$. If $\{e_1, \ldots, e_n\}$ is a basis of $\mathcal{M}_1$ (resp. $\{f_1, \ldots, f_m\}$ is a basis of $\mathcal{M}_2$) and $Y' = A_1 Y$ (resp. $Y' = A_2 Y$) is the equation associated with $(\mathcal{M}_1, \nabla_1)$ (resp. $(\mathcal{M}_2, \nabla_2)$) then $U \in HOM_k(\mathcal{M}_1, \mathcal{M}_2)$ defines a morphism if and only if $U' = A_2 U - U A_1$. One can define a connection $(HOM_k(\mathcal{M}_1, \mathcal{M}_2), \nabla_{HOM})$ by the equation $\nabla_{HOM}\phi(u) = \nabla_2(\phi(u)) - \phi(\nabla_1 u)$. One sees that $\phi \in HOM_k(\mathcal{M}_1, \mathcal{M}_2)$ defines a morphism if and only if $\nabla_{HOM}\phi = 0$. When $\mathcal{M}_2 = k$ and ∇_2 is the trivial connection, then we say that $(HOM_k(\mathcal{M}_1, \mathcal{M}_2), \nabla_{HOM})$ is the dual connection $(\mathcal{M}_1^*, \nabla_1^*)$. The differential equation associated with $(\mathcal{M}_1^*, \nabla_1^*)$ is $Y' = -A^T Y$. If $\mathcal{M}_1 = \mathcal{M}_2$ and U defines an isomorphism, we then have

$$A_2 \quad = \quad U'U^{-1} + UA_1U^{-1} \tag{2.2}$$

We therefore define the systems $Y' = A_1 Y$ and $Y' = A_2 Y$ to be *equivalent* if there exists a matrix $U \in GL(n, k)$ such that equation 2.2 holds.

Let K be a Picard-Vessiot extension of k containing the full solution spaces V_1 and V_2 of $Y' = A_1 Y$ and $Y' = A_2 Y$ and let $G = Gal(K/k)$ be the Galois group of K over k. The spaces V_1 and V_2 are G-modules. If they are isomorphic as G-modules, then there exist fundamental solution matrices† Z_1 and Z_2 of $Y' = A_1 Y$ and $Y' = A_2 Y$ respectively such that for each $g \in G$, there is a matrix $[g] \in GL(n, C)$ such that $g(Z_1) = Z_1[g]$ and $g(Z_2) = Z_2[g]$. Therefore the matrix $U = Z_1 Z_2^{-1}$ is left fixed by G and so must lie in $GL(n, k)$. The matrix U then defines an isomorphism between (k^n, ∇_{A_1}) and (k^n, ∇_{A_2}). Conversely, if the two systems $Y' = A_1 Y$ and $Y' = A_2 Y$ are equivalent one sees that the map $Z_1 = UZ_2$ defines a G-isomorphism between the two solution spaces V_1 and V_2. In fact, this argument shows that if $Y' = A_1 Y$ and $Y' = A_2 Y$ are equivalent differential systems and K is a Picard-Vessiot extension containing the full solution space of $Y' = A_1 Y$, then it will contain the full solution space of $Y' = A_2 Y$.

2.2. D-modules

Linear differential equations are frequently given by n^{th} order scalar equations $L(y) = y^{(n)} + a_{n-1} y^{(n-1)} + \ldots a_0 y = 0$, $a_i \in k$. It is useful to associate with such an equation the operator $L = D^n + a_{n-1} D^{n-1} + \ldots + a_0$ in the ring $\mathcal{D} = k[D]$ of linear differential operators (c.f., Singer (1996)). This ring is the ring of noncommutative polynomials in

† A fundamental solution matrix is a matrix whose columns form a basis of the solution space

D where D satisfies $Df = fD + f'$ for all $f \in k$. The ring $\mathcal{D}$ has a right and left division algorithm and one can calculate right and left least common multiples. A $\mathcal{D}$-module is a finite dimensional k-space $\mathcal{M}$ on which $\mathcal{D}$ acts on the left. A connection $(\mathcal{M}, \nabla)$ can be considered a $\mathcal{D}$-module by defining $Du = \nabla u$ for $u \in \mathcal{M}$. Conversely, to any $\mathcal{D}$-module $\mathcal{M}$ one can associate the connection $(\mathcal{M}, \nabla)$ where $\nabla u = Du$. Given an operator $L = D^n + a_{n-1}D^{n-1} + \ldots + a_0 \in \mathcal{D}$ one can associate to it the system $Y' = A_L Y$ where

$$A_L = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -a_0 & -a_1 & \ldots & \ldots & -a_{n-1} \end{pmatrix} \tag{2.3}$$

We denote the associated connection (k^n, ∇_L). One can easily check that this $\mathcal{D}$-module is isomorphic to $(\mathcal{D}/\mathcal{D}\cdot L)^*$. It is well known (Katz, 1987) that if k contains a non-constant element then any connection $(\mathcal{M}, \nabla)$ is cyclic, that is, there exists an element $u \in \mathcal{M}$ such that the elements $u, \nabla u, \nabla^2 u, \ldots, \nabla^{n-1}u$ form a k-basis of $\mathcal{M}$. Applying this fact to the dual $(\mathcal{M}^*, \nabla^*)$, we see that with respect to a basis of the form $v, \nabla^* v, \ldots, (\nabla^*)^{n-1}v$, the connection will have a matrix of the form

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & -a_0 \\ 1 & 0 & 0 & \ldots & -a_1 \\ 0 & 1 & 0 & \ldots & -a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

Therefore $(\mathcal{M}^{**}, \nabla^{**}) \simeq (\mathcal{M}, \nabla)$ is associated with the equation $Y' = -B^T Y$ where $-B^T = A_L$ for the operator $L = D^n + a_{n-1}D^{n-1} + \ldots + a_0$. Let $Y' = AY$ be a differential equation and (k^n, ∇_A) the associated connection. We shall refer to an operator L so that $(k^n, \nabla_A) \simeq (k^n, \nabla_L)$ as an operator *equivalent to the system* $Y' = AY$ or *equivalent to the connection* ∇_A.

2.3. Completely Reducible Operators

An operator $L \in \mathcal{D}$ is said to be *reducible over* k if it can be written as the product $L = L_1 L_2$ of operators of smaller order. The following gives several equivalent properties. We will call an equation $Y' = AY$ (or its connection) *reducible over* k or simply *reducible*, if k is clear from the context, if any of these equivalent conditions holds. An equation that is not reducible is said to be *irreducible*. Recall that a module is reducible if it has a proper, nonzero submodule.

Proposition 2.1. *Let $Y' = AY$ be a linear differential equation with coefficients in k and let K be its Picard-Vessiot extension with Galois group G. Let L be an operator equivalent to this system. The following are equivalent:*

1. *The connection (k^n, ∇_A) contains a proper nonzero subconnection.*
2. *The $\mathcal{D}$-module $\mathcal{M}_A$ is reducible.*
3. *$Y' = AY$ is equivalent to a system $Y' = BY$ where B has the form*

$$B = \begin{pmatrix} B_1 & 0 \\ B_2 & B_3 \end{pmatrix}$$

4 The $\mathcal{D}$-module $\mathcal{D}/\mathcal{D}L$ is reducible.
5 L is a reducible over k.
6 The solution space V of $Y' = AY$ in K is a reducible G-module.

Proof. Since K contains the full solution space of $Y' = AY$, it will contain the full solution space of any equivalent operator. Furthermore, these spaces will be G−isomorphic. The equivalence of 5. and 6. is given by Corollary 2.3 of (Singer, 1996). The equivalence of 3. and 6. is given in (Grigoriev, 1990). Since $\mathcal{D}/\mathcal{D}L$ is the dual of $\mathcal{M}_A$, the equivalence of 2. and 4. is clear. The equivalence of 1., 2. and 3 is by definition. □

An operator L is said to be *completely reducible* if it is the least common left multiple of irreducible operators. A module is *completely reducible* if it is the direct sum of irreducible modules. Finally, a linear algebraic group G is *reductive* if its unipotent radical is trivial (see (Humphreys, 1975) for the definition of this and related notions). The following proposition relates these notions.

Proposition 2.2. *Let $Y' = AY$ be a linear differential equation with coefficients in k and let K be its Picard-Vessiot extension with Galois group G. Let L be an operator equivalent to this system. The following are equivalent:*

1 The connection (k^n, ∇_A) is the direct sum of irreducible subconnections.
2 The $\mathcal{D}$-module $\mathcal{M}_A$ is completely reducible.
3 $Y' = AY$ is equivalent to a system $Y' = BY$ where B has the form

$$B = \begin{pmatrix} B_1 & 0 & \dots & 0 \\ 0 & B_2 & \dots & 0 \\ 0 & 0 & \dots & B_t \end{pmatrix}$$

and where each equation $Y' = B_iY$ is irreducible over k.
4 The $\mathcal{D}$-module $\mathcal{D}/\mathcal{D}L$ is completely reducible.
5 L is a completely reducible over k.
6 The solution space V of $Y' = AY$ in K is a completely reducible G-module.
7 G is a reductive group.

Proof. The equivalence of 5., 6. and 7. is given by Lemma 2.13 of (Singer, 1996). The equivalence of 1., 2. and 3. is by definition. A module is completely reducible if and only if its dual is and so 2. is equivalent to 4. We now show that 4. is equivalent to 5.

Assume 4. holds and write $\mathcal{D}/\mathcal{D}L = \mathcal{M}_1 \oplus \ldots \oplus \mathcal{M}_t$ where each $\mathcal{M}_i$ is irreducible. Let $\bar{1}$ be the coset of $1 \in \mathcal{D}$. We may write $\bar{1} = v_1 + \ldots + v_t$ where each $v_i \in \mathcal{M}_i$. Let $L_i \in \mathcal{D}$ be the monic operator of smallest degree such that $L_i(v_i) = 0$. Since each $\mathcal{M}_i$ is irreducible, each L_i is irreducible. Furthermore, $0 = L(\bar{1}) = L(v_1) + \ldots + L(v_t)$ so each $L(v_i) = 0$. Therefore each L_i divides L on the right. If each L_i divides an operator L_0 on the right, then $L_0(\bar{1}) = L_0(v_1) + \ldots + L_0(v_t) = 0 + \ldots + 0 = 0$. Therefore, L divides L_0 on the right and so L is the least common left multiple of th L_i.

Assume 5. holds and let L be the least common multiple of the distinct monic irreducible operators $L_1, \ldots, L_t$. One easily sees that this implies that the map $\phi : \mathcal{D} \to \mathcal{D}/\mathcal{D}L_1 \oplus \ldots \oplus \mathcal{D}/\mathcal{D}L_t$ taking $L \in \mathcal{D}$ to the sum of cosets has kernel $\mathcal{D}L$. Since the L_i are distinct, the sum of their orders equals the order of L. Therefore the k-dimensions of $\mathcal{D}/\mathcal{D}L$ and $\mathcal{D}/\mathcal{D}L_1 \oplus \ldots \oplus \mathcal{D}/\mathcal{D}L_t$ are the same and so these modules are isomorphic. □

In (Singer, 1996), an algorithm is described that decides if a given operator $L \in k[D]$ is completely reducible when $k = C(x)$, C a computable algebraically closed field. This algorithm is extended in Section 5.2 to fields k that are algebraic extensions of $C(x)$.

Finally, let k_2 be an algebraic extension of k_1 both fields having the same algebraically closed field of constants and let $L \in k_1[D]$. We then have that L_1 is completely reducible over k_1 if and only if it is completely reducible over k_2. This is because the Galois groups of L over k_1 and k_2 share a common connected component and a group is reductive if and only if its identity component is reductive.

2.4. Decomposition Fields

Let k be a differential field with algebraically closed field of constants C. A connection $(\mathcal{M}, \nabla)$ defined over k is said to be *absolutely irreducible over* k if for any algebraic extension K of k, the connection $(\mathcal{M} \otimes K, \nabla)$ is irreducible over K. Let $\mathcal{M}$ be a completely reducible $k[D]$-module. We say that $k_1 \supset k$ is a *decomposition field* for $\mathcal{M}$ if

1 k_1 is an algebraic extension of k, and
2 $\mathcal{M} \otimes k_1 = \mathcal{M}_1 \oplus \ldots \oplus \mathcal{M}_t$ where each $\mathcal{M}_i$ is an absolutely irreducible $k_1[D]$-module.

In terms of equations, we can state this as follows. An algebraic extension k_1 of k is a decomposition field of $Y' = AY$ if this equation is equivalent (over k_1) to an equation in block diagonal form where the equation corresponding to each block remains irreducible over any algebraic extension of k_1. Clearly, the algebraic closure of k is a decomposition field for any completely reducible equation.

Now assume that for any equation $Y' = AY$ over k one can effectively find an algebraic extension k_1 of k and elements $Y_1, \ldots, Y_r \in k_1^n$ such that any solution of $Y' = AY$ algebraic over k is a C-linear combination of the Y_i. Examples of such fields are $C(x)$, where C is a computable algebraically closed field, any finitely generated algebraic or elementary extension of $C(x)$, and certain liouvillian extensions of $C(x)$ (Singer, 1979; Singer, 1991). The following result shows that for such fields one can compute a decomposition field.

Proposition 2.3. *Let $(\mathcal{M}, \nabla)$ be a completely reducible connection defined over the field k and let $\bar{k}$ be the algebraic closure of k. Let $(HOM_k(\mathcal{M}, \mathcal{M}), \nabla_{HOM})$ be the connection associated with the endomorphisms of $\mathcal{M}$.*

1 Let $k_1 \subset \bar{k}$ be a computable differential field containing k. If we can effectively find a C-basis of all elements U of $HOM_{k_1}(\mathcal{M} \otimes k_1, \mathcal{M} \otimes k_1)$ such that $\nabla_{HOM}(U) = 0$, then we can effectively decompose $(\mathcal{M} \otimes k_1, \nabla)$ as a sum of irreducible connections over k_1. If k_1 is furthermore a decomposition field of $(\mathcal{M}, \nabla)$, then we can effectively decompose $(\mathcal{M} \otimes k_1, \nabla)$ as a sum of absolutely irreducible connections.
2 Let k_1 be an algebraic extension of k such that any $U \in HOM_k(\mathcal{M}, \mathcal{M}) \otimes \bar{k}$ with $\nabla_{HOM}(U) = 0$ is already in $HOM_k(\mathcal{M}, \mathcal{M}) \otimes k_1$, then k_1 is a decomposition field of $(\mathcal{M}, \nabla)$.

In more pedestrian terms, Proposition 2.3 says the following. If $Y' = AY$ is the equation associated with the connection and if we can find all solutions in k_1 of $U' = AU - UA$, then 1. says that we can find an equation equivalent to $Y' = AY$ whose matrix is in block diagonal form where the blocks along the diagonal correspond to irreducible equations. Furthermore, if k_1 is a decomposition field, we can do this in such a way that the equations corresponding to the blocks are absolutely irreducible. Part 2. says that if k_1 is an algebraic extension of k such that k_1 contains the entries of any matrix $U \in HOM(\bar{k}^n, \bar{k}^n)$ satisfying $U' = AU - UA$, then k_1 is a decomposition field for $Y' = AY$. Therefore to construct a decomposition field, we need only find a field containing the entries of all algebraic solutions of $U' = AU - UA$.

Proof. 1. As we have already noted at the end of the last section, $(\mathcal{M} \otimes k_1, \nabla)$ remains completely reducible over k_1. Select a k_1-basis of $(\mathcal{M} \otimes k_1, \nabla)$ and let $Y' = AY$ be the associated equation with respect to this basis. Let $U_1, \dots, U_t$ be a basis of the solution space of $\nabla_{HOM}(U) = U' - (AU - UA) = 0$. Note that the solution space of this latter equation forms a matrix algebra that contains the identity. Fix an integer s. Let $\{a_{i,j}\}_{1 \le i \le s}^{1 \le j \le t}$ be a set of indeterminates and let $P_i = \sum_j a_{i,j} U_j$ for $i = 1, \dots, s$. Consider the following conditions:

1 For all pairs $i \neq l$, $1 \le i, l \le s$, $P_i P_l = P_l P_i = 0$.
2 For all i, $P_i^2 = P_i$.
3 For all i, $P_i \neq 0$.

Expanding these equalities and inequalities in terms of a C-basis of k_1 we see that there is a C-constructible set $\mathcal{T}_s \subset C^{ts}$ such that $(a_{i,j}) \in \mathcal{T}_s$ if and only if the above conditions hold. These conditions are equivalent to the statement that the P_i are disjoint projections in the category of connections. Note that when $s = 1$, the identity matrix $P_1 = I$ satisfies the above conditions. Therefore $\mathcal{T}_1$ is not empty. Since $\mathcal{M}$ is finite dimensional we have that for large s, the $\mathcal{T}_s$ are empty. Let m be the smallest integer such that $\mathcal{T}_{m+1}$ is empty. Then for $(a_{i,j}) \in \mathcal{T}_m$, the projections P_i form a maximal set of disjoint nonzero projections. Therefore the image of each of these must be an irreducible subconnection. Again by maximality, the sum of these images must be the entire space $\mathcal{M}$. If we therefore take a maximal linearly independent set of columns from the P_i, we will have a basis of $\mathcal{M}$ with respect to which the connection is block diagonal with irreducible blocks.

If k_1 is furthermore a decomposition field, then there will be no further projections P_i in an algebraic extension of k_1. Therefore, the images of the P_i will be absolutely irreducible.

2. For k_1 as described, the above procedure will produce a decomposition into irreducible subconnections. If one of these subconnections is not absolutely irreducible, then the associated projection could be written as a sum of projections in some algebraic extension k_2. By assumption, these new projections must already be defined over k_1, contradicting the irreducibility of the subconnection. □

2.5. Exponential Extension Fields

Let $k \subset E$ be differential fields and $0 \neq u \in E$. We say that u is *exponential over* k if $u'/u \in k$. We say that a differential field E is an *exponential extension* of a differential field k if they have a common field of constants and $E = k(u_1, \dots, u_m)$ where each u_i is exponential over k. If the constants are algebraically closed, then one sees that E is a Picard-Vessiot extension of k whose Galois group is a finite extension of a torus. We shall show that, given an algebraic extension k of $C(x)$, C algebraically closed, and elements

$v_1, \ldots, v_m \in k$, one can explicitly describe the structure of the exponential extension E that is the Picard-Vessiot extension for the equation $Y' = diag(v_1, \ldots, v_m)Y$. We recall the following weak version of the Kolchin-Ostrowski Theorem (Kolchin, 1968): *Let $k \subset E$ be differential fields with the same constants and let $u_1, \ldots, u_n$ be elements of E exponential over k. If $u_1, \ldots, u_n$ are algebraically dependent over k then there exist integers, $e_1, \ldots, e_n$, not all zero, such that $\prod u_i^{e_i} \in k$.*

PROPOSITION 2.4. *Let $E = k(u_1, \ldots, u_m)$ be an exponential extension of k, a finitely generated algebraic extension of $C(x)$. Assume that one is given elements $v_1, \ldots, v_m \in k$ such that $u_i'/u_i = v_i$. Then one can effectively find a (possibly empty) set of elements $S = \{u_{i_1}, \ldots, u_{i_r}\} \subset \{u_1, \ldots, u_m\}$ and an integer M such that*

1 $\{u_{i_1}, \ldots, u_{i_r}\}$ is a transcendence basis of E over k.
2 If k_1 is the algebraic closure of k in E, then $[k_1 : k] \leq M$.

Furthermore, for each $j \in \{1, \ldots, m\}$ one can effectively find an element $f_j \in k$ and integers n_j, $n_{i,j}$, $n_j \neq 0$ such that

$$u_j^{n_j} = f_j \prod_{t=1}^{r} u_{i_t}^{n_{t,j}} \tag{2.4}$$

if S is nonempty, or $u_j^{n_j} = f_j$ if S is empty.

PROOF. We shall proceed by induction on m. We may assume that $u_1, \ldots, u_s$ form a transcendence basis of $K = k(u_1, \ldots, u_{m-1})$ over k. Given $v \in k$ and $u \in E$ with $u' = vu$ we will first show how to decide if u is algebraic over K and if it is find integers $n, n_j,\ n \neq 0$ and an element $f \in k$ such that

$$u^n = f \prod_{j=1}^{s} u_j^{n_j}\ .$$

The Kolchin-Ostrowski Theorem implies that such integers will exist if and only if u is algebraic over K. This is furthermore equivalent to deciding if there exist integers $n, n_j,\ n \neq 0$ such that

$$n\frac{u'}{u} - \sum_{j=1}^{s} n_j \frac{u_j'}{u_j} \quad = \quad nv - \sum_{j=1}^{s} n_j v_j \tag{2.5}$$

is the logarithmic derivative of an element of k. Let $\mathcal{C}$ be the curve associated with the function field k and define the following divisors:

$$\begin{aligned} D &= \sum_{P \in \mathcal{C}} res_P(vdx)\ P \\ D_i &= \sum_{P \in \mathcal{C}} res_P(v_i dx)\ P \end{aligned}$$

One sees that if 2.5 is the logarithmic derivative of a function $f \in k$ then $nD + \sum n_i D_i$ is the divisor of a function in k.

Conversely, the set of $(n, n_1, \ldots, n_s) \in \mathbb{Z}^{s+1}$ such that $nD + \sum n_i D_i$ is the divisor of an element of k forms a $\mathbb{Z}$-module $\mathcal{T}$. In (Bertrand, 1995; Masser, 1988) techniques are given to find a set of generators of $\mathcal{T}$ and therefore we can find a basis $\{(e_i, e_{i,1}, \ldots, e_{i,s})\}_{i=1}^{l}$ of this free module. Furthermore, for each i one can find an element $f_i \in k$ such that $e_i D + \sum e_{i,j} D_j$ is the divisor of f_i, (Baldassarri and Dwork, 1979; Coates, 1970; Trager, 1984). Each of the differential forms

$$\omega_i \quad = \quad (\frac{f_i'}{f_i} - e_i v - \sum_j e_{i,j} v_j) dx$$

is a holomorphic 1-form. We claim that 2.5 is the logarithmic derivative of an element in k for some choice of $n, n_i,\ n \neq 0$ if and only if the ω_i are linearly dependent over $\mathbb{Z}$ (this can also be decided using methods of (Coates, 1970; Trager, 1984)). If $\sum_j N_j \omega_j = 0$, then

$$\frac{(\prod f_j^{N_j})'}{\prod f_j^{N_j}} = (\sum_j N_j e_j) v + \sum_i (\sum_j N_j e_{i,j}) v_i$$

Note that if $\sum_j N_j e_j = 0$, then for each i, $\sum_j N_j e_{i,j} = 0$ or else the $u_1, \ldots, u_s$ would be algebraically dependent. Therefore $\sum_j N_j e_j \neq 0$, since the $(e_i, e_{i,1}, \ldots, e_{i,s})$ are independent.

Now assume that

$$\frac{f'}{f} = nv + \sum_{j=1}^{s} n_j v_j$$

Then $(n, n_1, \ldots, n_s) \in \mathcal{T}$ so there exist $N_i \in \mathbb{Z}$ such that

$$(n, n_1, \ldots, n_s) = \sum_i N_i (e_i, e_{i,1}, \ldots, e_{i,s}) \ .$$

This implies that

$$\begin{aligned} \sum_i N_i \omega_i \quad &= \quad \sum_i N_i \omega_i + (\frac{f'}{f} - (nv + \sum_{j=1}^{s} n_j v_j) dx \\ &= \quad ((\sum_i N_i \frac{f_i'}{f_i}) + \frac{f'}{f}) dx \\ &= \quad \frac{d(f \prod_i f_i^{N_i})}{f \prod_i f_i^{N_i}} \end{aligned}$$

If $d(f \prod_i f_i^{N_i}) \neq 0$ this last expression is a differential with simple poles. Since $\sum_i N_i \omega_i$ is holomorphic, we must have $d(f \prod_i f_i^{N_i}) = \sum_i N_i \omega_i = 0$.

Therefore we can decide if u and the u_i are algebraically dependent and if so find integers $n, n_j,\ n \neq 0$ and an element $f \in k$ such that

$$u^n = f \prod_{t=1}^{s} u_j^{n_j} \ .$$

If the degree of the algebraic closure of k in $k(u_1, \ldots, u_{m-1})$ is bounded by M_1, the degree of the algebraic closure k_1 of k in E is bounded by $M = nM_1$ $\square$

PROPOSITION 2.5. *Using the notation of Proposition 2.4, the map*

$$\eta : (t_1, \ldots, t_r) \quad \mapsto \quad (\prod_{l=1}^{r} t_l^{\frac{Nn_{l,1}}{n_1}}, \prod_{l=1}^{r} t_l^{\frac{Nn_{l,2}}{n_2}}, \ldots, \prod_{l=1}^{r} t_l^{\frac{Nn_{l,m}}{n_m}}) \tag{2.6}$$

where $N = LCM(n_1, \ldots, n_m)$ is a surjective homomorphism of $(C^*)^r$ onto the connected component $Gal(E/k)^o$ of the Galois group of E over k. This homomorphism has finite kernel.

PROOF. We first note that for $j \in \{i_1, \ldots, i_r\}$ the relation 2.4 is precisely $u_j^{n_j} = u_j^{n_j}$ since the u_j with $j \in \{i_1, \ldots, i_r\}$ are algebraically independent. Therefore for $i_s \in \{i_1, \ldots, i_r\}$, the i_s^{th} entry on the right hand side of 2.6 is just $t_{i_s}^N$. We identify the Galois group G of E over k with a closed subgroup of the group of diagonal matrices $diag(a_1, \ldots a_m)$ in $GL(m, C)$. Since the u_i satisfy the relations 2.4, we have that an element $(a_1, \ldots, a_m) \in Gal(E/k)$ satisfies

$$a_j^{n_j} \quad = \quad \prod_{t=1}^{r} a_{i_t}^{n_{t,j}}$$

These equations define a subgroup H of the diagonal group and using the observation at the beginning of this proof we see that this group has dimension r. Since E has transcendence degree r over k the connected component of the Galois group has dimension r. Therefore $Gal(E/k)^o = H^o$. The map 2.6 defines a homomorphism of $(C^*)^r$ into H as well and again, by dimension considerations, we see that the image of 2.6 must be H^o.

Comparing dimensions we see that the kernel has finite dimension. □

3. Invariant Theory

In the Introduction, we stated that to solve the problem of finding a presentation of the Picard-Vessiot extension of a linear differential equation $Y' = AY$ with reductive Galois group G, it is sufficient to find a bound for the degree of generators for the ring of polynomial invariants corresponding to the action of G on the n-fold sum of the solution space of $Y' = AY$. In this section we will show how this bound may be calculated directly from $Y' = AY$ without *a priori* knowledge of G.

We begin by reviewing some facts from the constructive invariant theory of reductive groups, (Kempf, 1987). Let G be a reductive group defined over an algebraically closed field C acting faithfully on a finite dimensional vector space V. The group G then acts on the coordinate ring $C[V]$. Its ring of invariants $C[V]^G$ is finitely generated and we denote by $N_{G,V}$ a bound on the degree of a set of generators of this ring. Such a bound has been calculated in several cases:

1 If G is a finite group then E. Noether showed (Noether, 1916; Sturmfels, 1993) that, independent of V, $N_{G,V} = |G|$.
2 If G is a torus, several authors (Kempf, 1987; Sturmfels, 1991; Wehlau, 1993) have given expressions for $N_{G,V}$. We may identify G with an r-fold product $(C^*)^r$. Let χ be a weight of G acting on V. Then $\chi(t_1, \ldots, t_r) = \prod_{i=1}^{r} t_i^{m_i}$ for some integers m_i. We define $||\chi|| = \max |m_i|$, and let $t = \max ||\chi||$ where the χ run through all weights of G on V. Wehlau, for example, showed that $N_{G,V} = (2t)^{2r-1}$ as well as $N_{G,V} = (n - r - 1)r!\mathrm{vol}(\mathcal{C})$, where n is the dimension of V and $\mathrm{vol}(\mathcal{C})$ is the volume of the convex hull of the exponents of the weights of G on V.

3 If G is a connected semisimple group, Popov showed in (Popov, 1981) that

$$N_{G,V} = nC(\frac{2^{r+s}n^{s+1}(n-1)^{s-r}t^r(s+1)!}{3^s((\frac{s-r}{2})!)^2})$$

where $C(M)$ denotes the least common multiple of all positive integers less than or equal to M, $n = dim(V)$, $s = dim(G)$, $r = rank(G)$ and t is defined as above for a maximal torus T_{max} of G.

Hiss (Hiss, 1996) has given expressions for $N_{G,V}$ for any connected reductive group but for our purposes it will be easier to deal with semisimple groups and tori separately.

To deal with reductive groups we will need to glue these results together. We will use the following result of Kempf (Kempf, 1987). Let $G_2 \lhd G_1$ be a normal subgroup of the reductive group G_1 and let V be a G_1-module. Since G_2 is normal in G_1 we have that G_1 acts on the ring $k[V]^{G_2}$. Let $W = k[V]^{G_2} \cap k[V]_{1 \le i \le N_{G_2,V}}$ where $k[V]_{1 \le i \le N_{G_2,V}}$ denotes the sum of homogeneous terms of degree between 1 and $N_{G_2,V}$. Kempf shows that

$$N_{G_1,V} = N_{G_1/G_2,W} \cdot N_{G_2,V} \ .$$

An arbitary reductive group G has a tower of normal subroups $(e) \lhd T \lhd G^o \lhd G$ where G^o is the component of the identity in G and T is the component of the identity of the center of G^o. It is known that T is furthermore a torus and that G^o/T is semisimple. Therefore to find $N_{G,V}$ it will be sufficient to

1 Calculate T together with its weights on V.
2 Bound $N_{G^o/T,W}$, where $W = k[V]^T \cap k[V]_{1 \le i \le N_{T,V}}$
3 Bound the order of G/G^o.

We will deal with each of these problems separately in the next three subsections. In what follows we will assume that k is a finitely generated algebraic extension of $C(x)$ where C is a computable algebraically closed field.

3.1. T

Let $Y' = AY$ be a completely reducible differential equation with coefficients in k and let k_0 be a decomposition field for $Y' = AY$. Proposition 2.3 says that we can effectively construct such a field. Let K be the Picard-Vessiot extension of k_0 corresponding to $Y' = AY$ and let $G = Gal(K/k_0)$ be the Galois group of K over k_0. Since k_0 is an algebraic extension of k the component of the identity of G is the same as the component of the identity of the Galois group of $Y' = AY$ over k. Over k_0, $Y' = AY$ is equivalent to a block diagonal equation $Y' = diag(A_1, \ldots, A_m)$ where each equation $Y' = A_iY$ is absolutely irreducible. In particular, each $Y' = A_iY$ is irreducible over the fixed field of G^o. Therefore Schur's Lemma implies that the center of G^o acts via scalar multiplication on the solution space of each $Y' = A_iY$.

PROPOSITION 3.1. *Let k_0 be a differential field with algebraically closed field of constants and let $Y' = diag(A_1, \ldots, A_m)Y$ be a block diagonal differential equation with $A_i \in HOM(k_0^{d_i}, k_0^{d_i})$ where the equations $Y' = A_iY$ are absolutely irreducible. Let K be the Picard-Vessiot extension of k_0 corresponding to $Y' = AY$ and let $G = Gal(K/k_0)$ be* *its Galois group. Let $E = k_0(u_1, \ldots, u_m)$ be the exponential extension of k_0 where $u_i' = tr(A_i)u_i$ for $i = 1, \ldots, m$ and assume that $Gal(E/k_0)$ has dimension r. If*

$$\eta : (t_1, \ldots, t_r) \quad \mapsto \quad (\chi_1(t_1, \ldots, t_r), \ldots, \chi_m(t_1, \ldots, t_r))$$

is a homomorphism of $(C^*)^r$ onto the component of the identity of $Gal(E/k_0)$, then

$$\phi : (t_1, \ldots, t_r) \quad \mapsto \quad diag(\overbrace{\chi_1^{\frac{N}{d_1}}, \ldots, \chi_1^{\frac{N}{d_1}}}^{d_1}, \ldots, \overbrace{\chi_m^{\frac{N}{d_m}}, \ldots, \chi_m^{\frac{N}{d_m}}}^{d_m})$$

where $N = lcm(d_1, \ldots, d_m)$, is a homomorphism of $(C^*)^r$ onto T, the component of the identity of the center of G^o.

Proof. The remarks preceeding this proposition imply that T is a subgroup of

$$H = \{diag(\overbrace{a_1, \ldots, a_1}^{d_1}, \ldots, \overbrace{a_m, \ldots, a_m}^{d_m}) \mid a_i \in C^*\}$$

Since E is a Picard-Vessiot extension of k contained in K, the component G^o of the identity of the Galois group G leaves E invariant. This induces a surjective homomorphism ψ of G^o onto $Gal(E/k_0)^o$. Explicitly, this map is given by

$$\psi(diag(g_1, \ldots, g_m)) = (det(g_1), \ldots, det(g_m)) \ .$$

Writing $G^o = (G^o, G^o) \cdot Z(G^o)$ where $Z(G^o)$ is the center of G^o (Humphreys (1975), page 168) we see that (G^o, G^o) lies in the kernel of ψ. Therefore, ψ maps T onto the component of the identity of $Gal(E/k_o)$. One sees that the kernel of ψ in T is finite so T has dimension r. Note that

$$\psi(diag(a_1, \ldots, a_1, \ldots, a_m, \ldots, a_m)) = (a_1^{d_1}, \ldots, a_m^{d_m})$$

so we have $\psi \circ \phi = \eta^N$. Therefore, the image of ϕ is a connected group of dimension r that is mapped by ψ onto $Gal(E/k_0)^o$. Therefore this image must coincide with T. □

We are now able to show how to calculate the action of T on the solution space of $Y' = AY$. First calculate a decomposition field k_0 as in Proposition 2.3. We then calculate the map η as in Proposition 2.5. Finally, Proposition 3.1 gives us the characters of the action of T on the solution space of $Y' = AY$. As noted in the introduction to this section, this allows us to bound the degrees of generators for the invariants.

3.2. G^o/T

We shall use Popov's formula to bound $N_{G^o/T,W}$. In practice, once the dimension of W is known we know that there are at most a finite number of semisimple groups having faithful representations of that dimension. For each of these groups we can calculate these representations and bound t as well as calculating the dimension and ranks of these groups.

Another approach is to give *a priori* bounds for the elements appearing in Popov's formula. Let $n = dim\ W$. The dimension of the semisimple group G^o/T is then at most $n^2 - 1$ and its rank is at most $n - 1$. The following lemma gives a bound for t.

Lemma 3.1. *Let H be a connected semisimple group with maximal torus T_{max} and W*

an H-module of dimension n. We can fix an isomorphism $T_{max} \simeq (C^*)^r$ such that for any weight $\chi(t_1, \ldots, t_r) = \prod_i t_i^{n_i}$ of T_{max} on W, we have that each $|n_i| \leq n$.

PROOF. (c.f., Onishchik and Vinberg (1990), Ch. 4.6) Let $\mathfrak{h}$ be the Lie algebra of H and let $\mathfrak{h} = \mathfrak{t} \oplus \bigoplus \mathfrak{g}_\alpha$ be the root decomposition of $\mathfrak{h}$. For each positive root α we may select $e_\alpha \in \mathfrak{g}_\alpha$, $e_{-\alpha} \in \mathfrak{g}_{-\alpha}$ such that $h_\alpha = [e_\alpha, e_{-\alpha}]$, e_α, $e_{-\alpha}$ span a Lie subalgebra $\mathfrak{g}^{(\alpha)}$ isomorphic to $\mathfrak{sl}(2)$. Since $SL(2)$ is simply connected, there exists a homomorphism $\phi_\alpha : SL(2) \rightarrow H$ such that $d\phi_\alpha$ maps the Lie algebra of $SL(2)$ isomorphically onto $\mathfrak{g}^{(\alpha)}$. Let $T_\alpha \simeq C^*$ be the maximal torus of $\phi_\alpha(SL(2))$. If $\{h_{\alpha_1}, \ldots, h_{\alpha_r}\}$ are a basis of $\mathfrak{t}$. then $T_{\alpha_1} \times \ldots \times T_{\alpha_r} = T_{max}$. We shall use the isomorphism $\phi_{\alpha_1} \times \ldots \times \phi_{\alpha_r}$ as our fixed isomorphism of $(C^*)^r$ onto T_{max}. If we restrict χ to $T_{\alpha_i} \subset \phi_{\alpha_i}(SL(2))$, we get the weight $t_i^{n_i}$ of the action of the maximal torus $T_{\alpha_i} \subset \phi_{\alpha_i}(SL(2))$ on W. As an $SL(2)$-module, W is the direct sum of irreducible $SL(2)$-modules. The weights t^m of an irreducible $SL(2)$-module of dimension d satisfy $|m| \leq d$. Therefore we have that each $|n_i| \leq n$.□

3.3. G/G^o

We shall show how one can bound the order of G/G^o. We begin with a group theoretic lemma.

LEMMA 3.2. *Let G be a connected reductive linear algebraic group defined over an algebraically closed field C. Let V be an irreducible G-module of dimension n and H a subgroup of $SL(V)$ such that H normalizes G. Then $|H/H \cap G| < n \cdot n!$.*

PROOF. Let us first assume that G is semisimple. We shall show that $|H \cdot G/G| = |H/H \cap G| < n \cdot n!$. The action of $H \cdot G$ on G by conjugation induces a homomorphism $\Phi : H \cdot G/G \rightarrow Aut(G)/Inn(G)$ where $Aut(G)$ is the group of automorphisms of G and $Inn(G)$ is the subgroup of inner automorphisms. The kernel $Ker(\Phi)$ of Φ consists of those cosets $h \cdot G$ where, for some $g \in G$, hg commutes with all elements of G. Since V is irreducible, Schur's Lemma implies that hg is a constant matrix. Since $H \subset SL(V)$ and $G = (G, G) \subset SL(V)$, we have that the coset $h \cdot G$ has a representative that is a constant matrix in $SL(V)$. Therefore $|Ker(\Phi)| \leq n$. Since G is semisimple, $Aut(G)$ is the product of $Inn(G)$ and the automorphism group of its Dynkin diagram ((Humphreys, 1975), p. 166). The automorphism group of the Dynkin diagram forms a subgroup of the symmetric group on r objects where r is the rank of G. Therefore $|Aut(G)/Inn(G)| \leq r! < n!$ and so $|H \cdot G/G| = |H/H \cap G| < n \cdot n!$.

Now assume that G is an arbitrary connected reductive group. In this case we can write $G = G' \cdot Z(G)$ where $G' = (G, G)$. Since V is irreducible, $Z(G)$ consists of constant matrices. Therefore V is an irreducible G'-module. Furthermore H normalizes G'. Since $|H/H \cap G| \leq |H/H \cap G'|$, the conclusion of the lemma follows from the result of the previous paragraph. □

Before continuing, we note that an equation $Y' = AY$ with coefficents in k has a Galois group over k that is conjugate to a unimodular group if and only if there exists a non-zero element $u \in k$ such that $u' = tr(A)u$. This follows from the facts that $Y' = AY$ has such a group if and only if it has a fundamental solution matrix Z with $det(Z) \in k$ and that $det(Z)$ satisfies $det(Z)' = tr(A)det(Z)$.

Let $Y' = AY$, $A \in HOM_k(k^n, k^n)$ be a completely reducible equation and let k_0 be a decomposition field for this equation. Proposition 2.3 implies that we can find such a field when k is algebraic over $C(x)$. Over k_0 we may assume that $A = diag(A_1, \ldots A_m)$ where each A_i corresponds to an absolutely irreducible equation. For $i = 1, \ldots, m$ let $u_i' = tr(A_i)u_i$ and let $E = k_0(u_1, \ldots, u_m)$. Proposition 2.4 implies that one can explicitly bound $[k_1 : k_0]$, where k_1 is the algebraic closure of k_0 in E and so bound $[k_1 : k]$.

PROPOSITION 3.2. *Let $Y' = AY$, k_0, E, and k_1 as above. If G is the Galois group of $Y' = AY$ over k, then*

$$|G/G^o| < [k_1 : k]n^n \cdot n!$$

PROOF. Let K be the Picard-Vessiot extension of $Y' = AY$ over k_0 and let $\tilde{G}$ be the Galois group of K over k_0. We shall first show that

$$|\tilde{G}/\tilde{G}^o| < [k_1 : k_0]n^n \cdot n!$$

Since K will contain a full set of solutions of each $Y' = A_iY$, it will contain the determinant of a fundamental solution matrix of each of these equations. We can therefore assume that $E \subset K$. Note that

$$|\tilde{G}/\tilde{G}^o| \leq |Gal(E/k_0)/Gal(E/k_0)^o| \cdot |Gal(K/E)/Gal(K/E)^o| \ .$$

This follows from the fact that the index of the component of the identity in a Galois group equals the degree of the maximal algebraic extension of the ground field. By definition, $|Gal(E/k_0)/Gal(E/k_0)^o| = [k_1 : k_0]$, so it remains to prove that

$$|Gal(K/E)/Gal(K/E)^o| < n^n \cdot n! \ .$$

To do this we will describe the group $Gal(K/E)^o$ and its action on the solution space of $Y' = AY$ in greater detail.

Let $V = V_1 \oplus \ldots \oplus V_m$ be the solution space of $Y' = AY$ where each V_i corresponds to the solution space of $Y' = A_iY$. Let n_i be the dimension of V_i. Each V_i is an irreducible $\tilde{G}^0$-module. The group $\tilde{G}^0$ can be written as $(\tilde{G}^o, \tilde{G}^o) \cdot Z$ where Z is the center of $\tilde{G}^o$. Schur's Lemma implies that on each V_i, Z acts as scalar multiplication. Therefore each V_i is an irreducible $(\tilde{G}^o, \tilde{G}^o)$-module. Note that u_i is the determinant of a fundamental solution matrix of $Y' = A_iY$. Since $(\tilde{G}^o, \tilde{G}^o)$ must be unimodular on each V_i, we have that $(\tilde{G}^o, \tilde{G}^o)$ leaves each u_i fixed and so is a subset of $Gal(K/E)$. Therefore, each V_i is an irreducible $Gal(K/E)$-module. Furthermore $Gal(K/E)|_{V_i}$ is unimodular since $Gal(K/E)$ leaves each u_i fixed. We may write $Gal(K/E) = Gal(K/E)^o \cdot H$ where H is a finite group (Wehrfritz (1973), page 142). Note that $|Gal(K/E)/Gal(K/E)^o| = |H/H \cap Gal(K/E)^o|$. Let $G_i = Gal(K/E)|_{V_i}$ and $H_i = H|_{V_i}$. Note that $Gal(K/E)^o|_{V_i} = (Gal(K/E)|_{V_i})^o$. Lemma 3.2 implies that for each i, $|H_i/H_i \cap Gal(K/E)_i^o| < n_i \cdot (n_i)!$. Therefore $|H/H \cap Gal(K/E)^o| \leq \prod |H_i/H_i \cap G_i^o| < n^n n!$.

To complete the proof of the proposition, let F be the Picard-Vessiot extension of $Y' = AY$ over k. We then have that $F \cdot k_0$ is the Picard-Vessiot extension of k_0 for this equation and so can be identified with K. Proposition 6.6 of (Magid, 1994) implies that $\tilde{G} = Gal(K/k_0) = Gal(F \cdot k_0/k_0)$ may be identified with $Gal(F/F \cap k_0)$. This implies that $\tilde{G}$ and G share a common component of the identity. Since the index of $Gal(F/F \cap k_0)$ in G is at most $[k_0 : k]$ we have that $|G/G^o| \leq |\tilde{G}/\tilde{G}^o| \cdot [k_0 : k] < [k_1 : k_0]n^n \cdot n![k_0 : k] = [k_1 : k]n^n \cdot n!$ □

Note that no attempt was made to optimize the bound in this proposition. Once a decomposition of $Y' = AY$ is known, a better bound can be achieved.

4. Algorithms

4.1. Completely Reducible Equations

Let $Y' = AY$ be a differential equation with A an $n \times n$ matrix with coefficients in $k = C(x), x' = 1, C$ an computable algebraically closed field of characteristic zero. In this section we shall show how to compute the basis for a prime ideal $I \subset k[Y_{11}, \ldots Y_{nn}]$ such that the quotient field of $k[Y_{11}, \ldots Y_{nn}]/I$ is the Picard-Vessiot extension of k corresponding to $Y' = AY$. Compoint (Compoint, 1996a; Compoint, 1996b) showed that such an ideal is generated by elements of the form $Q(Y_{i,j}) - c$ where Q is a homogeneous invariant of the Galois group and f is a constant. In what follows, we shall show that the string of coefficients of the polynomial Q can be identified with a solution of an auxillary differential equation and that the element c can be determined from Q by evaluating Q at a power series solution (at a regular point) of $Y' = AY$.

In order to define and calculate the auxillary operator mentioned above, we continue the discussion started in Section 2 concerning connections. We have defined subconnections, quotients, direct sums, tensor products and duals. Using these operations one can construct symmetric powers of connections. More concretely, let $(\mathcal{M}, \nabla)$ be a connection of dimension N and let $e_1, \ldots, e_N$ be a basis of $\mathcal{M}$. Let $Y' = BY$ be the associated equation with respect to this basis. The d^{th} symmetric power of this connection is defined on the space $Sym^d(\mathcal{M})$. If we use the basis $\{e_1^{i_1} e_2^{i_2} \cdots e_N^{i_N} \mid i_1 + i_2 + \ldots + i_N = d\}$, the connection $Sym^d(\nabla)$ is defined by the equation $Z' = Sym^d(B)Z$ where $Sym^d(B)$ is the $\begin{pmatrix} N+d-1 \\ d-1 \end{pmatrix} \times \begin{pmatrix} N+d-1 \\ d-1 \end{pmatrix}$ matrix whose entries are defined by expanding the equations

$$\begin{aligned}
(e_1^{i_1} e_2^{i_2} \cdots e_N^{i_N})' &= i_1 e_1^{i_1-1} e_1' e_2^{i_2} \cdots e_N^{i_N} + i_2 e_1^{i_1} e_2^{i_2-1} e_2' \cdots e_N^{i_N} + \ldots + i_N e_1^{i_1} e_2^{i_2} \cdots e_N^{i_N-1} e_N' \\
&= i_1 e_1^{i_1-1}(Be_1) e_2^{i_2} \cdots e_N i_N + i_2 e_1^{i_1} e_2^{i_2-1}(Be_2) \cdots e_N^{i_N} + \ldots \\
&\quad + i_N e_1^{i_1} e_2^{i_2} \cdots e_N^{i_N-1}(Be_N)
\end{aligned}$$

The dual $(Sym^d(\mathcal{M})^*, Sym^d(\nabla)^*)$ of this connection corresponds to homogeneous polynomials of degree d on $\mathcal{M}$ with coefficients in k. To be explicit, let us order the basis $s_{i_i i_2 \ldots i_N} = e_1^{i_1} e_2^{i_2} \cdots e_N^{i_N}$ of $Sym^d(\mathcal{M})$ in some way. If $\Phi = (\ldots, f_{i_1 i_2 \ldots i_N}, \ldots)$ is a solution of $Sym^d(\nabla)^*(\Phi) = 0$, then we consider the associated polynomial

$$Q_\Phi = \sum \frac{d!}{i_1! \ldots i_N!} f_{i_1 i_2 \ldots i_N} Y_1^{i_1} \ldots Y_N^{i_N}$$

with $i_1 + \ldots + i_N = d$, and we have $Q_\Phi(y_1, \ldots, y_N) = \Phi(S^d v)$, with $v = y_1 e_1 + \ldots + y_N e_N$.

Let K be the Picard-Vessiot extension of k corresponding to $Y' = BY$, let G be its Galois group and V be the solution space of this equation in K with basis $v_1, \ldots, v_N$. One can consider the symmetric power $Sym^d(V)$, with basis $\{v_1^{i_1} v_2^{i_2} \cdots v_N^{i_N}\}$, and its dual $(Sym^d(V))^* \simeq Sym^d(V^*)$. One can show (Compoint, 1996a) that the two spaces $Sym^d(\mathcal{M})^* \otimes K$ and $Sym^d(V) \otimes K$ are isomorphic as K-spaces. Note that if $Sym^d(\nabla)^*(\Phi) = 0$, then, for $v = y_1 v_1 + \ldots + y_N v_N$,

$$(Q_\Phi(y_1, \ldots, y_N))' = \Phi(S^d(v)))'$$

$$\begin{aligned} &= \Phi(Sym^d(\nabla)(S^d(v))) \\ &= \Phi(0) \\ &= 0\ . \end{aligned}$$

Therefore the polynomial Q_Φ will take on constant values on solutions of $Y' = BY$. Furthermore, the solutions of $Sym^d(\nabla)^*(Z) = 0$ in $Sym^d(\mathcal{M})^*$, that is the solutions of $Sym^d(\nabla)^*(Z) = 0$ in $Sym^d(\mathcal{M}^*)\otimes K$ with coefficients in k, correspond to the G-invariant elements of $(Sym^d(V))^* \otimes K$. A consequence of this is that a G-invariant homogeneous polynomial ϕ with constant coefficients (considered as an element of $Sym^d(V^*)$) corresponds to a vector Φ that is a solution of $\Phi' = (Sym^d(B))^*\Phi$ with entries in k.Therefore, for ϕ as above we have a polynomial $Q_\phi - \phi(S^d v)$ of degree d with coefficients in k that vanishes when evaluated at $(y_1, ..., y_N)$. Let $\{y_{ij}\}$ be a fundamental system of solutions of $Y' = BY$, and consider the system $Y^{'} = diag(B, ..., B)Y$. The vector v whose coordinates are ${}^t(y_{11}, y_{21}, ..., y_{nn})$ is a solution of this system. If ϕ is an element of $Sym^d(V \oplus ... \oplus V)$ wich is G-invariant, then we obtain the polynomial $P_\phi = Q_\phi - \phi(S^d v)$. This polynomial clearly is in the ideal of polynomial relations among the $\{y_{ij}\}$. The main result of (Compoint, 1996a) is the following.

Proposition 4.1. *Let k be a differential field with algebraically closed constants C and let $Y' = AY$ be a differential equation with A an $n \times n$ matrix with entries in k . Let $(y_{i,j})$ be a fundamental solution matrix of this equation in a Picard-Vessiot extension of k. Assume that the Galois group of this equation is reductive and unimodular and let $\{\phi_1, \ldots, \phi_t\}$ be homogeneous generators of the ring of invariants $C[Y_{i,j}]^G$. Then $k[y_{i,j}] \simeq k[Y_{i,j}]/I$ where $I = (P_{\phi_1}, \ldots, P_{\phi_t})$.*

We can now state and prove the main result of this paper.

Theorem 4.1. *Let k be an algebraic extension of $C(x)$, C a computable algebraic closed field and let $\{Y_{i,j}\}$, $\{X_{i,j}\}$ be two sets of n^2 variables. Let $Y' = AY$ be a differential equation, with A an $n \times n$ matrix with entries in k, whose Galois group is reductive. Then one can compute in a finite number of steps a basis for a prime ideal $I \subset k[Y_{i,j}]$ such that the quotient field K of $k[Y_{i,j}]$ is a Picard-Vessiot extension of k corresponding to $Y' = AY$. Furthermore, one can compute a basis for an ideal $J \subset k[X_{i,j}]$ such that the Galois group of $Y' = AY$ is the set of zeroes of J in $GL(n, C)$.*

Proof. We will use Proposition 4.1 so our first task is to show that we may assume that the Galois group is unimodular. Consider the differential equation $Y' = \tilde{A}Y$ where

$$\tilde{A} = \begin{pmatrix} A & 0 \\ 0 & -tr(A) \end{pmatrix}$$

If Z is a fundamental solution matrix of $Y' = AY$, then

$$\begin{pmatrix} Z & 0 \\ 0 & (det(Z))^{-1} \end{pmatrix}$$

is a fundamental solution matrix of $Y' = \tilde{A}Y$. The Picard-Vessiot extensions of these two equations are the same and so they have the same Galois groups. If $g \in GL(n, C)$ is an element of the Galois group of $Y' = AY$, then the map

$$g \quad \mapsto \quad \begin{pmatrix} g & 0 \\ 0 & (det(g))^{-1} \end{pmatrix}$$

is an isomorphism between the Galois group of $Y' = AY$ and that of $Y' = \tilde{A}Y$. Clearly the image of this map is unimodular. If we calculate the defining ideal I of a Picard-Vessiot extension for $Y' = \tilde{A}Y$ then using Gröbner bases techniques, we can find the defining ideal of the solutions of $Y' = AY$. We therefore will assume that the Galois group of $Y' = AY$ is unimodular.

In Section 3, we showed how one can calculate a bound for the degrees of a set of homogeneous generators of the invariants of a Galois group. We apply this to the equation $Y' = BY$ where $B = diag(A, A, \ldots, A)$. Assume that N is such a bound. Since k is an algebraic extension of $C(x)$, Propositions 3.1 and 3.2 of (Singer, 1991) imply that we can, for each $d \leq N$, calculate a C-basis $\mathcal{B}_d$ for the solutions Φ *in* k of $Y' = Sym^d(B)Y$ (see also (van Hoeij and Weil, 1996)). The entries of the Φ are in k and so can be considered functions on an algebraic curve. Let z_0 be a C-point of this curve at which none of these functions have a pole. If we evaluate each of the coefficients of the polynomials $Q_\phi(Y_{1,1}, \ldots, Y_{n,n})$ at z_0 and let $Y_{i,j} = \delta_{i,j}$, we get a constant c_Φ. From the discussion preceeding Proposition 4.1, we see that $P_\Phi = Q_\Phi - c_\Phi$ vanishes on the solution $\{y_{i,j}\}$ of $Y' = AY$ corresponding to the initial conditions $y_{i,j}(z_0) = \delta_{i,j}$. Therefore we have found generators of the ideal I defining the Picard-Vessiot extension $k(\{y_{i,j}\})$.

We now turn to calculating the Galois group. The Galois group of $K = k(y_{i,j})$ is the subgroup of $GL(n, C)$ leaving the ideal I invariant. This is equivalent to leaving each polynomial P_ϕ invariant, $\phi \in \mathcal{B}_d$, $0 \leq d \leq N$. Expanding each P_Φ in a C-basis of k, we see that this is equivalent to a system of polynomial equations with constant coefficients. These give the defining equations of the Galois group. □

Note that in the process of proving this result we have obtained polynomials that characterize the Galois group: The Galois group is precisely the set of matrices that fix the polynomials P_Φ. This gives an illustration of the theorem of Chevalley.

4.2. General Equations

In this section we shall show how Theorem 4.1 can be used to calculate properties of the Galois group of an *arbitrary* differential equation. The key to this is the following Proposition.

Proposition 4.2. *Let k be a differential field with algebraically closed field of constants and let $L \in k[D]$ be a differential operator. Let $L = L_m L_{m-1} \cdots L_1$ where each L_i is an irreducible operator and let $\tilde{L} = LCLM\{L_m, \ldots, L_1\}$ where $LCLM\{\ldots\}$ denotes the least common left multiple. If G is the Galois group of $L(y) = 0$, then G/R_u is the Galois group of $\tilde{L}$, where R_u is the unipotent radical of G.*

Proof. For simplicity we shall assume that $m = 2$; the general case can be proven in a similar manner. Let K be the Picard-Vessiot extension of k corresponding to $L(y) = 0$ and let n be the order of L and n_i be the order of L_i. Since L_1 maps the solution space V of $L(y) = 0$ onto the solution space of $L_2(y) = 0$ there exists a basis $\{y_1, \ldots, y_n\}$ such that $\{y_1, \ldots, y_{n_1}\}$ is a basis of the solution space of $L_1(y) = 0$ and $\{L_1(y_j)\}_{j=n_1+1}^{n}$ is a basis of the solution space of $L_2(y) = 0$. Therefore $\{y_1, \ldots, y_{n_1}, L_1(y_{n_1+1}), \ldots, L_1(y_n)\}$ spans the solution space of LCLM$\{L_1, L_2\}$ (note that these elements need not be linearly independent). Let $K_0 \subset K$ be the Picard-Vessiot extension generated by $\{y_1, \ldots, y_{n_1}, L_1(y_{n_1+1}), \ldots, L_1(y_n)\}$ and their derivatives, that is, the Picard-Vessiot extension corresponding to the equation LCLM$\{L_1, L_2\}$. We shall show that the subgroup H of G leaving K_0 fixed is precisely R_u. First note that with respect to the basis $\{y_1, \ldots, y_n\}$ any element $g \in G$ is in block diagonal form

$$g = \begin{pmatrix} g_1 & * \\ 0 & g_2 \end{pmatrix}$$

where $g_i \in GL(n_i, C)$. Therefore, if g leaves the elements of K_0 fixed, it must be of the form is in block diagonal form

$$g = \begin{pmatrix} I_1 & * \\ 0 & I_2 \end{pmatrix}$$

where I_i is the $n_i \times n_i$ identity matrix. Therefore H consists of unipotent matrices. Furthermore, H is the kernel of the map $G \to Gal(K_0/k)$ given by restriction. Since $Gal(K_0/k)$ is the Galois group of a completely reducible operator, it is a reductive group. Therefore H is not properly contained in any normal unipotent subgroup and so it must be the radical of G. □

THEOREM 4.2. *Let k be an algebraic extension of $C(x)$ and let $L \in k[D]$. Let G be the Galois group of $L(y) = 0$. Then one can*

1. *calculate G/R_u where R_u is the unipotent radical of G,*
2. *calculate G/G^o, and*
3. *decide if G^o is solvable and therefore decide if $L(y) = 0$ is solvable in terms of liouvillian functions.*

PROOF. One begins by factoring L into a product $L_1 L_2 \cdots L_m$ of irreducible factors (see Section 5.1) and then forming the operator $\tilde{L} = LCLM\{L_m, \ldots, L_1\}$. Proposition 4.2 implies that $\tilde{L}$ has Galois group isomorphic to G/R_u where G is the Galois group of L and R_u is its unipotent radical. If $\tilde{L}$ has order r then Theorem 4.1 implies that we can find polynomials $\{f_i\}$ in r^2 variables whose zero set in $GL(r, C)$ is the Galois group $\tilde{G}$ of $\tilde{L}$. This proves 1.

The map $G \to G/G^o$ induces an isomorphism of G/G^o onto $(G/R_u)/(G/R_u)^o$. Therefore to prove 2., we shall show how to compute $(G/R_u)/(G/R_u)^o$. Compute G/R_u as in 1. Standard arguments (Gianni *et al.*, 1988; Eisenbud *et al.*, 1992) allow one to decompose the variety defined by $\{f_i = 0\}$ into irreducible components. The number of these components will be $|(G/R_u)/G/R_u)^o|$. Selecting a distinct set of representatives $\{g_j\}$ from these components and deciding to which component each $g_i g_j$ belongs allows us to write down a multiplication table for $(G/R_u)/G/R_u)^o$. This proves 2.

Note that G^o is solvable if and only if $G^o/R_u = (G/R_u)^o$ is solvable. Using the decomposition of G/R_u into irreducible components, we can select the component of the identity of this latter group. Since $(G/R_u)^o$ is reductive, it is solvable if and only if it is conjugate to a subgroup of the diagonal group D. Using Gröbner bases techniques, one can decide if the set of $h \in GL(r, C)$ such that $h(G/R_u)^o h^{-1} \subset D$ is nonempty and so decide if $(G/R_u)^o$ is semisimple. This proves 3. We note that decisions procedures for 3. also appear in (Singer, 1981; Singer, 1991; Singer and Ulmer, 1996). □

5. Appendix

Let C be an algebraically closed field and let k be an algebraic extension of $C(x)$. In this section we shall show that there are algorithms to factor operators over k or decide if operators are completely reducible over k. Although it may be apparent to the experts that many of the algorithms to do these tasks over $C(x)$ can be modified to work over k (see (van Hoeij, 1996; van Hoeij, 1997; Singer, 1996) for references to the known algorithms), this has not been explicitly presented in print. We do not claim that the algorithms we present here are the most efficient but rather are ones that are simple to describe.

5.1. Factoring

We begin by recalling some known procedures. Let K be a differential field. We say that we can *effectively solve homogeneous linear differential equations over K* if for any operator $L \in K[D]$ we can effectively find a basis for the vector space of all $y \in K$ such that $L(y) = 0$ (c.f., (Singer, 1991)). We say that we can *effectively find all exponential solutions of homogeneous linear differential equations over K* if for any operator $L \in K[D]$ we can effectively find $u_1, \ldots, u_m \in K$ such that if $L(e^{\int u}) = 0$ for some $u \in K$, then for some i, $e^{\int u}/e^{\int u_i} \in K$. It is clear that we can perform both of these tasks if $K = C$. Propositions 2.1 and 3.1 of (Singer, 1991) imply that we can then perform both of these tasks over k where k is an algebraic extension of $C(x)$. Lemma 2.4 of (Singer, 1991) implies that we can refine the second task in the following way:

> Given $L \in k[D]$, one can effectively find u_i and $v_{i,j}$, $1 \leq i \leq m$, $1 \leq j \leq n_i$ in k such that if $u \in k$ and $L(e^{\int u}) = 0$ then there exists an i and constants $c_{i,j}$ such that $e^{\int u} = (\sum_{j=1}^{n_j} c_{i,j} v_{i,j}) e^{\int u_i}$.

Using the methods of Proposition 2.4 we can decide if $e^{\int u_i}/e^{\int u_j} = f_{i,j} \in k$ for each pair $i > j$. If this is the case, we can replace $v_{i,1}, \ldots, v_{i,n_i}$ with $v_{i,1}, \ldots, v_{i,n_i}$, $f_{i,j}v_{j,1}, \ldots, f_{i,j}v_{j,n_j}$, delete u_j and assume that the new set of u_i's satisfies $e^{\int u_i}/e^{\int u_j} \notin k$ for $i \neq j$.

To factor operators over k we proceed as follows. Let $L = L_1 L_2$ where L_1 has order $n - r$ and L_2 has order r. Since the solutions of $L_2(y) = 0$ are also solutions of $L(y) = 0$, we can write

$$L_2(y) = y^{(r)} + b_{r-1} y^{(r-1)} + \ldots + b_0 y \tag{5.1}$$

$$= \frac{det \begin{pmatrix} Y & y_1 & \ldots & y_r \\ Y' & y_1' & \ldots & y_r' \\ \ldots & \ldots & \ldots & \ldots \\ Y^{(r)} & y_1^{(r)} & \ldots & y_r^{(r)} \end{pmatrix}}{det \begin{pmatrix} y_1 & \ldots & y_r \\ y_1' & \ldots & y_r' \\ \ldots & \ldots & \ldots \\ y_1^{(r-1)} & \ldots & y_r^{(r-1)} \end{pmatrix}} \tag{5.2}$$

where $y_1, \ldots, y_r$ are solutions of $L(y) = 0$.

Note that the denominator of the right hand side of 5.2 is the wronskian of a fundamental set of solutions of L_2. Therefore it is exponential over k. Furthermore the coefficients of L_2 are quotients of determinants of $r \times r$ submatrices of

$$\begin{pmatrix} y_1 & \dots & y_r \\ y_1' & \dots & y_r' \\ \dots & \dots & \dots \\ y_1^{(r)} & \dots & y_r^{(r)} \end{pmatrix} \tag{5.3}$$

and this wronskian. Since the coefficients of L_2 are in k, each determinant of an $r \times r$ submatrix of 5.3 is exponential over k.

One can calculate a differential equation $L^{\wedge r}$ whose solution space is spanned by all such determinants as $y_1, \dots, y_r$ varies over all subsets of r solutions of $L(y) = 0$ (c.f., Schlesinger (1887), Section 167 - 168). We use the algorithm alluded to in the displayed paragraph above to calculate $u_i, v_{i,j}$ as described for the equation $L^{\wedge r}$. Since we are assuming that for distinct i, j, $e^{\int u_i}/e^{\int u_j} \notin k$, we see that for each coefficient b_l of L_2 there is an index i and constants $c_{i,j}, d_{i,j}$ such that

$$b_l = \frac{\sum_{j=0}^{n_j} c_{i,j} v_{i,j}}{\sum_{j=0}^{n_j} d_{i,j} v_{i,j}} \tag{5.4}$$

Therefore to decide if L has a factor of order r one selects a $j \in \{1, \dots, m\}$ for each l, forms the expression 5.4 with indeterminate $c_{i,j}, d_{i,j}$ for each possible coefficient b_l and formally divides the resulting operator into L. Setting the remainder equal to zero gives polynomial conditions on the $c_{i,j}, d_{i,j}$ and one then decides if there are constants satisfying these conditions. If no factor is found in this way then L is irreducible. Otherwise one factors L and proceeds by induction until an irreducible factorization is found.

We note that this procedure can be modified to find an algebraic extension k_1 of k and a factorization of L over k_1 such that each factor is absolutely irreducible. To do this one can modify the algorithm displayed above to find a set of elements u_i and $v_{i,j}$, $1 \leq i \leq m$, $1 \leq j \leq n_j$ *algebraic* over k such that if u is *algebraic* over k and $L(e^{\int u}) = 0$ then there exists an i and constants $c_{i,j}$ such that $e^{\int u} = (\sum_{j=1}^{n_j} c_{i,j} v_{i,j}) e^{\int u_i}$. One then proceeds to factor over $k_1 = k(\{u_i\}, \{v_{i,j}\})$ and continue this process until no further factorization is possible.

5.2. Testing Complete Reducibility

In (Singer, 1996), a test is given to decide if an element $L \in C(x)[D]$ is completely reducible. One can extend this to a test for elements of $k[D]$, k an algebraic extension of $C(x)$ in the following way. We may assume that k is a Galois extension of $C(x)$. Let G be its Galois group and let L^σ denote the operator gotten from L by applying $\sigma \in G$ to all the coefficients of L. Let M be the least common left multiple of all the elements of $\{L^\sigma \mid \sigma \in G\}$. Since L divides M on the right, the Galois group of L will be a quotient of the Galois group of M. Proposition 2.2.6 implies that if M is completely reducible, then L is completely reducible. Conversely, if L is completely reducible then each L^σ is completely reducible and so M is completely reducible. Therefore to decide if L is completely reducible over k it suffices to decide if M is completely reducible over k. Note that the coefficients of M are invariant under the Galois group and so must lie in $C(x)$.

As noted at the end of Section 2.3 M is completely reducible over k if and only if it is completely reducible over $C(x)$. Therefore we can use the results of (Singer, 1996) to decide if M (and therefore L) is completely reducible.

The results of (Singer, 1996) allow one to decide if an equation is completely reducible without having to find a factorization. If a factorization is given, then one can proceed in a different manner. Let $Y' = AY$ be a differential equation with

$$A = \begin{pmatrix} A_1 & 0 & 0 & \dots & 0 \\ * & A_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ * & * & \dots & * & A_r \end{pmatrix} \tag{5.5}$$

where each equation $Y' = A_iY$ is irreducible and let $(\mathcal{M}, \nabla)$ be the associated connection. One sees that this connection has a filtration $(\mathcal{M}, \nabla) = (\mathcal{M}_1, \nabla_1) \supset (\mathcal{M}_2, \nabla_2) \supset \ldots \supset (\mathcal{M}_r, \nabla_r)$ where the quotient of the i and $i+1$ elements is a connection having equation $Y' = A_iY$. From general properties of completely reducible modules, we see that $(\mathcal{M}, \nabla)$ is isomorphic to $\oplus_{i=1}^r(\mathcal{M}_i/\mathcal{M}_{i+1}, \nabla_{\mathcal{M}_i/\mathcal{M}_{i+1}})$. This latter connection has equation $Y' = \tilde{A}Y$ where

$$\tilde{A} = \begin{pmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & A_r \end{pmatrix} \tag{5.6}$$

Conversely, since each $Y' = A_iY$ is irreducible, we see that if A and $\tilde{A}$ are equivalent then $Y' = AY$ is completely reducible. Therefore to decide if $Y' = AY$ is completely reducible we must decide if there exists a $U \in GL(n, k)$ such that $U' = AU - U\tilde{A}$. To do this we find a basis $U_1, \ldots U_s$ of the solution space of $U' = UA - \tilde{A}U$ with entries in k and decide if there are constants c_i such that $det(\sum c_iU_i) \neq 0$.

References

Baldassarri, F., Dwork, B. (1979). On second order linear differential equations with algebraic solutions. *American Journal of Mathematics*, **101**:42–76.

Bertrand, D. (1995). Minimal heights and polarizations on group varieties. *Duke Mathematics Journal*, **80:1**:223–250.

Coates, J. (1970). Constructions of rational functions on a curve. *Proceedings of the Cambridge Philosophical Society*, **68**:105–123.

Cohen, H. (1993). *A Course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics. Springer-Verlag, New York.

Compoint, E. (1996a). Differential Equations and Algebraic Relations. Technical report, Université de Paris VI.

Compoint, E. (1996b). *Équations Différentielles, Relations Algébriques et Invariants.* PhD thesis, Université de Paris VI.

Eisenbud, D., Huneke, C., Vasconcelos, W. (1992). Direct methods for primary decomposition. *Inventiones Mathematicae*, **110**:207–236.

Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, **6**:149–167.

Grigoriev, D. Y. (1990). Complexity of irreducibility testing for a system of linear ordinary differential equations. In *Proceedings of the 1990 International Symposium on Symbolic and Algebraic Computation*, pages 225–230. ACM Press.

Haefliger, A. (1987). Local theory of meromorphic connections in dimension one (Fuchs theory). In *Algebraic D-Modules,* Borel et al, chapter III., pages 129–149. Academic Press.

Hiss, K. (1996). Constructive invariant theory for reductive groups. Technical report, Brandeis University.

Humphreys, J. (1975). *Linear Algebraic Groups.* Graduate Texts in Mathematics. Springer-Verlag, New York.

Kaplansky, I. (1976). *An Introduction to Differential Algebra.* Hermann, Paris, second edition.
Katz, N. (1987). A simple algorithm for cyclic vectors. *American Journal of Mathematics*, **109**:65–70.
Kempf, G. (1987). Computing invariants. In Koh, S. S., editor, *Invariant Theory*, Lecture Notes in Mathematics, **1278**, pages 81–94. Springer-Verlag, Berlin, Heidelberg, New York.
Kolchin, E. (1968). Algebraic groups and algebraic dependence. *American Journal of Mathematics*, **90**:1151–1164.
Kolchin, E. (1976). *Differential Algebra and Algebraic Groups.* Academic Press, New York.
Magid, A. (1994). *Lectures on Differential Galois Theory.* University Lecture Series. American Mathematical Society.
Masser, D. (1988). Linear relations on algebraic groups. In Baker, A., editor, *New Advances in Transcendence Theory*, pages 248–262. Cambride University Press, Cambridge.
Noether, E. (1916). Der Endlichkeitsatz der Invarianten endlicher Gruppen. *Mathematische Annalen*, **77**:89–92.
Onishchik, A. L., Vinberg, E. B. (1990). *Lie Groups and Algebraic Groups.* Springer-Verlag, Berlin.
Pohst, M., Zassenhaus, H. (1989). *Algorithmic Algebraic Number Theory.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge.
Popov, V. L. (1981). Constructive invariant theory. *Astérisque*, **87/88**:303–334.
Schlesinger, L. (1887). *Handbuch der Theorie der Linearen Differentialgleichungen.* Teubner, Leipzig.
Singer, M. F. (1979). Algebraic solutions of n^{th} order linear differential equations. In *Proceedings of the 1979 Queen's Conference on Number Theory*, pages 379–420. Queen's Papers in Pure and Applied Mathematics, **59**.
Singer, M. F. (1981). Liouvillian solutions of n^{th} order homogeneous linear differential equations. *American Journal of Mathematics*, **103**:661–681.
Singer, M. F. (1991). Liouvillian solutions of linear differential equations with liouvillian coefficients. *Journal of Symbolic Computation*, **11**:251–273.
Singer, M. F. (1996). Testing reducibility of linear differential operators: a group theoretic perspective. *Applicable Algebra in Engineering, Communication and Computing*, **7**:77–104.
Singer, M. F., Ulmer, F. (1996). Linear differential equations and products of linear forms. *Journal of Pure and Applied Algebra.* to appear.
Sturmfels, B. (1991). Gröbner bases for toric varieties. *Tôhoku Mathematics Journal*, **43**:249–261.
Sturmfels, B. (1993). *Algorithms in Invariant Theory.* Springer-Verlag, Vienna.
Trager, B. (1984). *Integration of Algebraic Functions.* PhD thesis, MIT.
van der Waerden, B. L. (1953). *Modern Algebra.* Frederick Ungar Publishing Co., New York, second edition.
van Hoeij, M. (1996). Rational solutions of the mixed differential equation and its applications to factorization of differential operators. In *Proceedings of the 1996 ISSAC Conference*, pages 219 – 225. ACM Press.
van Hoeij, M. (1997). Factorization of differential operators with rational function coefficients. *to appear in the Journal of Symbolic Computation.*
van Hoeij, M., Weil, J.-A. (1996). An Algorithm for Computing Invariants of Differential Galois Groups. Technical report, University of Groningen.
Wehlau, D. (1993). Constructive invariant theory for tori. *Annales de l'Institut Fourier, Grenoble*, **43**:1055–1066.
Wehrfritz, B. A. F. (1973). *Infinite Linear Groups.* Ergebnisse der Mathematik. Springer-Verlag, Berlin.