Testing Reducibility of Linear Differential Operators: A Group Theoretic Perspective

Michael F. Singer*

North Carolina State University

Department of Mathematics

Box 8205

Raleigh, N.C. 27695-8205

e-mail: singer@math.ncsu.edu

January 4, 1995

1 Introduction

Let k be an ordinary differential field of characteristic zero and let $\mathcal{D} = k[D]$ be the ring of linear differential operators over k, that is, the noncommutative polynomial ring in the variable D, where $D \cdot a - a \cdot D = a'$ for all $a \in k$. An element $L \in \mathcal{D}$ is said to be *reducible* if $L = L_1 \cdot L_2$ for some $L_1, L_2 \in \mathcal{D}, L_1, L_2 \notin k$. In this case, L_1 and L_2 are called *factors* of L. This paper was motivated by the desire to answer the following question:

> *Can one decide if a linear differential operator is reducible* WITHOUT *having to find a factor?*

This question is in turn motivated by the following theorem (and its generalizations, [43]): *Let k be a differential field with algebraic closed field of constants and let $L \in \mathcal{D}$ be a second order operator. The equation $L(y) = 0$ has non-zero liouvillian solutions over k if and only if $L^{\circledS 6}$ is reducible in $\mathcal{D}$.* Here, the operator $L^{\circledS 6}$ is the operator of order 7 whose solution space (in the Picard-Vessiot extension of k corresponding to L) is spanned by all 6^{th} powers of solutions of L. The techniques and results of [43] show how one can reduce many

*Partially supported by NSF Grant 90-24624

questions concerning the Galois group of a differential equation to questions of factorizations of auxillary operators.

Each element of $\mathcal{D}$ can be expressed as a product of irreducible factors and, when $k = \overline{\mathbb{Q}}(x)$, $x' = 1$, $\overline{\mathbb{Q}}$ the algebraic closure of the rational numbers, there exist algorithms to carry out such a factorization ([13], [38], [39]). Furthermore, in [14], Grigoriev gives a method (and complexity analysis) for testing reducibility of a system of linear operators but this method is equivalent to finding factors (in the case of a single operator). We present a method based on different ideas. In previous methods the question of deciding if a linear operator L factors is reduced to:

1. Constructing auxillary linear operators $\tilde{L}$ whose associated Riccati equations have among their solutions all possible coefficients $a_i(x)$ of factors $L_1 = D^m + a_{m-1}(x)D^{m-1} + \ldots + a_0(x)$ of L. From $\tilde{L}$ one can bound the degrees of the numerators and denominators of these coefficients (in fact, more information can be extracted from these auxillary operators, [8])

2. Explicitly finding the coefficients of a factor of L. This involves, in general, solving large systems of polynomial equations for the coefficients of the $a_i(x)$ (or at least deciding if such a system has a solution).

Techniques for solving 1. have been implemented by Bronstein in *Axiom*, [8]. Schwarz has implemented the full algorithm for equations of small order. Our aim is to give a method that avoids the need to actually find the coefficients of a factor. Our method will also yield two other benefits. First of all, it gives a method to decide if the Galois group is a reductive group (see section 3.3.1). Secondly, if one knows in advance that the group is reductive (for example, if one knows that the group is finite, as happens in situations discussed in [43]) one can take advantage of this fact to simplify further the reducibility test.

To understand our approach, let us first consider the question of factorization in other contexts. First, consider the *commutative* ring of polynomials $\mathbb{F}_q[x]$ of polynomials over the field $\mathbb{F}_q$ with q elements and let $f \in \mathbb{F}_q[x]$. The approach of the Berlekamp algorithm for factorization is to form the ideal $\mathbb{F}_q[x]{\cdot}f$ and relate factorization properties of f to the structure of the quotient ring $A = \mathbb{F}_q[x]/\mathbb{F}_q[x]{\cdot}f$ (c.f., [32], pp. 247-259). In particular, if $f = f_1 \cdot \cdots \cdot f_m$ where the f_i are pairwise relatively prime irreducible polynomials of degree d_i, then A will be a direct sum of fields, $A = \mathbb{F}_{q^{d_1}} \oplus \cdots \oplus \mathbb{F}_{q^{d_m}}$. If Φ is the map $\Phi : x \mapsto x^q - x$, one has that $dim_{\mathbb{F}_q}(Ker\ \Phi) = m$. Therefore, computing the kernel of the map Φ gives a quick way of determining the number of factors of f and, in particular, of determining if f is irreducible.

When one tries to generalize this idea to noncommutative polynomial rings one runs into various problems. For example, let K be a field and σ a nontrivial automorphism of K and consider the ring $K[x;\sigma]$ of polynomials in x over K with the usual addition and multiplication defined by $x \cdot a = \sigma(a) \cdot x$ for all $a \in K$. These rings were studied by Ore [34], Jacobson [18, 19], Macdonald [31] and Cohn [9]. Most recently, Giesbrecht [12] has given factorization algorithms when K is a finite field. One can begin to proceed as in the commutative case. Let $f \in K[x;\sigma]$ and consider the *left ideal* $K[x;\sigma] \cdot f$. The quotient $M = K[x;\sigma]/K[x;\sigma] \cdot f$ no longer has a canonical ring structure but is only a left $K[x;\sigma]-$module. The key idea is to consider the *ring* $\mathcal{E}(M)$ of $K[x;\sigma]-$endomorphisms of M (also called the *eigenring* of $K[x;\sigma] \cdot f$) instead of the module M. Building on [19], Giesbrecht shows that f is irreducible if and only if $\mathcal{E}(M)$ has no zero divisors (and so can be shown to be a field). Furthermore Giesbrecht shows how one can determine zero divisors of this ring. He is then able to give algorithms for finding the number of irreducible factors and finally for factorization. The key property that is used is that $K[x;\sigma]$ has a rich supply of *two sided* ideals (see [12] for details).

When one considers the ring $\mathcal{D}$ one can begin to proceed as with the ring $K[x;\sigma]$ (in fact, in [18], [19], [34] many results are developed in a context that includes both these rings). In contrast to $K[x;\sigma]$, the ring $\mathcal{D}$ will in general have a very poor supply of two sided ideals (for example, if $k = \overline{\mathbb{Q}}(x)$, $\mathcal{D}$ has no non-trivial two sided ideals ([6], p. 27)). Furthermore, it is easy to construct (see Example 2.8) operators $L_1,\ L_2 \in \mathcal{D}$ such that L_1 is reducible and L_2 is irreducible, and $End_{\mathcal{D}}(\mathcal{D}/\mathcal{D} \cdot L_1)$ and $End_{\mathcal{D}}(\mathcal{D}/\mathcal{D} \cdot L_2)$ are isomorphic. Therefore, one cannot completely rely on these rings to determine irreducibility. We therefore look beyond purely ring theoretic properties to find criteria for irreducibility. For us the key fact will be that to each linear operator $L \in \mathcal{D}$ one can associate a linear algebraic group G, its Galois group, and that the factorization properties of the operator are intimately connected to the structure and representation theory of G. The key is to distinguish the two cases: (1) G a reductive group, and (2) G a non-reductive group. When G is a reductive group, properties of $End_{\mathcal{D}}(\mathcal{D}/\mathcal{D} \cdot L)$ (already known to Ore) determine if L is reducible. When G is not reductive, L must already be reducible. Our main contribution is to give a procedure to test if G is reductive.

The rest of the paper is organized as follows. In section 2, we will describe properties of the ring $\mathcal{D}$ and its modules and relate these properties to Galois groups of differential operators. The section ends with Corollary 2.19 which gives a criterion for the Galois group to be reductive, and Corollary 2.21 which gives us a criterion for irreducibility. Section 3 concerns itself with making this criterion effective, and giving examples and applications to determining Galois groups of linear differential equations.

We would like to thank A. Fauntelroy and F. Ulmer for stimulating conversations concerning the contents of this paper.

2 Factorization in the Ring $\mathcal{D}$

Let k be a differential field of charactersitic 0 with algebraically closed field of constants $\mathcal{C}$. We shall assume that the reader is familliar with the basic facts of the Picard-Vessiot theory (see [21]). Most of the material in Sections 2.1, and 2.2 is either classical or follows from simple considerations concerning $\mathcal{D}-$modules (see the remarks at the end of the section). Nonetheless we have included this material to offer the reader an elementary bridge between the old and the new, to bring out their group theoretic nature and to put these facts in a context suitable for use in the quest for algorithms.

2.1 Generalities

For any $L = a_nD^n + \ldots + a_0 \in \mathcal{D}$ with $a_n \neq 0$, we define the *order* of L, $ord(L)$ to be the integer n and we define $ord(0) = -\infty$. The ring $\mathcal{D}$ is both a left and right euclidean ring, that is, for any $L_1 \neq 0, L_2 \in \mathcal{D}$ there exist unique $Q_r,\ R_r,\ Q_l,\ R_l \in \mathcal{D}$ with $ord(R_r), ord(R_l) < ord(L_1)$ such that $L_2 = Q_rL_1 + R_r$ and $L_2 = L_1Q_l + R_l$. For $k \subset K$, we denote by $Soln_K(L)$ the space of solutions of $L(y) = 0$ in K.

Lemma 2.1 *Let $L_1,\ L_2 \in \mathcal{D}$ and assume that $ord(L_1) = m,\ ord(L_2) = n$. Let K be a differential extension of k having the same constants $\mathcal{C}$.*

1. *$dim_{\mathcal{C}} Soln_K(L_1) \leq m$*
2. *If $dim_{\mathcal{C}} Soln_K(L_1) = m$ and any solution in K of $L_1(y) = 0$ is a solution of $L_2(y) = 0$, then L_1 divides L_2 on the right in $\mathcal{D}$.*
3. *If $dim_{\mathcal{C}} Soln_K(L_1) = m$ and L_2 divides L_1 on the right, then $dim_{\mathcal{C}} Soln_K(L_2) = n$ and $Soln_K(L_2) \subset Soln_K(L_1)$.*

Proof: The first claim follows from a standard wronskian argument ([21], p. 21). To prove the second claim, write $L_2 = QL_1 + R$. Applying both sides of this expression to solutions of $L_1(y) = 0$, we see that $R(y) = 0$ has a solution space of dimension at least m. Since its order is at most $m - 1$, we have that $R = 0$. To prove the final claim note that L_2 can be applied to any element of $Soln_K(L_1)$ and in this way maps this space to $Soln_K(Q)$ where $L_1 = QL_2$. The dimension of the image Im of this map is at most $ord(Q)$ and the dimension of the kernel Ker is at most $ord(L_2)$. Since $ord(L_1) = dim_{\mathcal{C}} Soln_K(L_1) = dim_{\mathcal{C}} Im + dim_{\mathcal{C}} Ker \leq ord(Q) + ord(L_2) = ord(L_1)$, we have that $dim_{\mathcal{C}} Soln_K(L_2) = ord(L_2)$ and $Soln_K(L_2) \subset Soln_K(L_1)$. ∎

When $dim_{\mathcal{C}} Soln_K(L) = ord(L)$, we say that K *contains a full set of solutions of* L. The main fact connecting the Galois group of a linear operator to factorization properties of that operator is the following:

Lemma 2.2 *Let K be a Picard-Vessiot extension of k with Galois group G and let $V \subset K$ be a finite dimensional $\mathcal{C}$ vector space. V is the solution space of some homogeneous linear differential equation $L(y) = 0$ with coefficients in k if and only if V is left invariant by G.*

Proof: If V is the solution space of $L(y) = 0$, then V is left invariant by G because the elements of G take solutions of this equation to other solutions of this equation. Conversely, assume V is $G-$invariant and let $y_1, \ldots, y_m$ be a $\mathcal{C}-$basis. Let

$$L(y) = det(Wr(y, y_1, \ldots, y_m))/det(Wr(y_1, \ldots, y_m)),$$

where Wr is the wronskian matrix. Note that if $\sigma \in G$, then $\sigma(det(Wr(y, y_1, \ldots, y_m))) = det(Wr(y, y_1, \ldots, y_m)det(A_\sigma)$ and $\sigma(det(Wr(y_1, \ldots, y_m))) = det(Wr(y_1, \ldots, y_m)det(A_\sigma)$, where A_σ is the matrix of σ with respect to the given basis. We then have that the coefficients of $L(y)$ are left fixed by all elements of G. Therefore $L \in \mathcal{D}$. ∎

We define an element $L \in \mathcal{D}$ of positive order to be *reducible* if $L = L_1L_2$ for operators $L_1, L_2 \in \mathcal{D}$ of positive order. If L is not reducible, we say it is *irreducible.*

Corollary 2.3 *Let $L \in \mathcal{D}$. The following are equivalent:*

1. *L is irreducible.*
2. *The Galois group of L acts irreducibly on the solution space of L in the Picard-Vessiot extension of k corresponding to $L(y) = 0$.*
3. *If K is any Picard-Vessiot extension of k containing the Picard-Vessiot extension of k corresponding to $L(y) = 0$, then the Galois group of K acts irreducibly on the solution space of $L(y) = 0$ in K.*

Proof: This follows easily from Lemma 2.1 and Lemma 2.2. ∎

We say two operators $L_1, L_2 \in \mathcal{D}$ are *relatively prime* if there is no operator of positive order dividing both on the right.

Corollary 2.4 *Let $L_1, L_2 \in \mathcal{D}$. The following are equivalent:*

1. *L_1 and L_2 are relatively prime.*
2. *There exist $R, S \in \mathcal{D}$ such that $RL_1 + SL_2 = 1$.*
3. *L_1 and L_2 have no common nonzero solution in any extension of k.*

Proof: The equivalence of 1. and 2. follows from the existence of a euclidean algorithm. If L_1 and L_2 are not relatively prime then they have a common nonzero solution in the Picard-Vessiot extension corresponding to the common factor. Conversely, if there exist $R, S \in \mathcal{D}$ such that $RL_1 + SL_2 = 1$, then any common solution v of L_1 and L_2 satisfies $0 = RL_1(v) + SL_2(v) = v$. ∎

As we have already noted, the module $\mathcal{D}/\mathcal{D} \cdot L$ is not a ring and one cannot apply Berlekamp techniques directly to this module. A substitute for this module is the ring $End_{\mathcal{D}}(\mathcal{D}/\mathcal{D} \cdot L)$. We shall show that this ring arises in several settings.

Let $L_1, L_2 \in \mathcal{D}$ and denote by $\overline{R}$ the equivalence class of R in $\mathcal{D}/\mathcal{D} \cdot L_2$ and define

$$\mathcal{E}_{\mathcal{D}}(L_1, L_2) = \{\overline{R} \in \mathcal{D}/\mathcal{D} \cdot L_2 \mid L_1 R \text{ is divisible on the right by } L_2\}$$

One easily checks that this condition depends only on the equivalence class and not on the choice of representative. Note that $\mathcal{E}_{\mathcal{D}}(L_1, L_2)$ is closed under addition and multiplication by elements in $\mathcal{C}$. If $L_1 = L_2 = L$, one can define a multiplication on this vector space and the resulting ring is called the *(left) eigenring of* L and is denoted by $\mathcal{E}_{\mathcal{D}}(L)$. The multiplication on $\mathcal{E}_{\mathcal{D}}(L)$ is defined in the following way: for $\overline{R_1}, \overline{R_2} \in \mathcal{E}_{\mathcal{D}}$, let $\overline{R_1} \cdot \overline{R_2} = \overline{R_1 R_2}$. To see that this is well defined, let $S_1 = R_1 + Q_1 L$ and $S_2 = R_2 + Q_2 L$. $S_1 S_2 = R_1 R_2 + R_1 Q_2 L + Q_1 L R_2 + Q_1 L Q_2 L$. Since $\overline{R_2} \in \mathcal{E}_{\mathcal{D}}(L)$, we have that LR_2 is divisible on the right by L. Therefore $\overline{S_1 S_2} = \overline{R_1 R_2}$. This shows that $\mathcal{E}_{\mathcal{D}}(L)$ is a $\mathcal{C}-$algebra.

Lemma 2.5 *Let $L_1, L_2 \in \mathcal{D}$, let K be a Picard-Vessiot extension containing a full set of solutions of L_1 and L_2, and let G be its Galois group.*

1. *The following three $\mathcal{C}-$spaces are isomorphic:*
   - $\mathcal{E}_{\mathcal{D}}(L_1, L_2)$
   - $Hom_{\mathcal{D}}(\mathcal{D}/\mathcal{D} \cdot L_1, \mathcal{D}/\mathcal{D} \cdot L_2)$
   - $Hom_G(V_2, V_1)$, *where V_i is the solution space of $L_i(y) = 0$ in K for $i = 1, 2$.*

   Furthermore, if $L_1 = L_2$, then these rings are isomorphic as $\mathcal{C}-$algebras.

2. *Assuming L_1 and L_2 have the same order, the isomorphisms of these rings may be chosen in such a way as to induce bijections among the following sets:*
   - $\mathcal{E}_{\mathcal{D}}(L_1, L_2)^* = \{\overline{R} \in \mathcal{E}_{\mathcal{D}}(L_1, L_2) \mid R \text{ and } L_2 \text{ have no common factors}\}$
   - $Isom_{\mathcal{D}}(\mathcal{D}/\mathcal{D}\cdot L_1, \mathcal{D}/\mathcal{D}\cdot L_2) = \{\phi \in Hom_{\mathcal{D}}(\mathcal{D}/\mathcal{D}\cdot L_1, \mathcal{D}/\mathcal{D}\cdot L_2) \mid \phi \text{ is an isomorphism}\}$
   - $Isom_G(V_2, V_1) = \{\psi \in Hom_G(V_2, V_1) \mid \psi \text{ is an isomorphism}\}$

Proof: We will first show that there is an isomorphism between $\mathcal{E}_{\mathcal{D}}(L_1, L_2)$ and $Hom_{\mathcal{D}}(\mathcal{D}/\mathcal{D}\cdot L_1, \mathcal{D}/\mathcal{D}\cdot L_2)$. Let $\overline{R} \in \mathcal{E}_{\mathcal{D}}(L_1, L_2)$. We define an element $\phi_R \in Hom_{\mathcal{D}}(\mathcal{D}/\mathcal{D}\cdot L_1, \mathcal{D}/\mathcal{D}\cdot L_2)$ by $\phi_R(1 + \mathcal{D}/\mathcal{D}\cdot L_1) = \overline{R}$. One easily checks that this map is well defined and is a $\mathcal{D}-$homomorphism. The map $\Phi : \overline{R} \mapsto \phi_R$ is clearly a $\mathcal{C}-$homomorphism. If $\phi_R = 0$, then $R \in \mathcal{D}\cdot L_2$ so $\overline{R} = 0$. Therefore Φ is injective. If $\phi \in Hom_{\mathcal{D}}(\mathcal{D}/\mathcal{D}\cdot L_1, \mathcal{D}/\mathcal{D}\cdot L_2)$, let $\overline{R} = \phi(1 + \mathcal{D}/\mathcal{D}\cdot L_1)$. Since $0 = \phi(L_1(1 + \mathcal{D}/\mathcal{D}\cdot L_1)) = \overline{L_1 R}$, we have that $L_1 R$ is divisible on the right by L_2. Therefore, $\overline{R} \in \mathcal{E}_{\mathcal{D}}(L_1, L_2)$ and $\phi = \phi_R$, so Φ is surjective.

We now show that Φ is a bijection on the corresponding sets mentioned in 2. The Euclidean algorithm shows that R and L_2 are relatively prime if and only if there exist $P, Q \in \mathcal{D}$ such that $PR + QL_2 = 1$. Let $\overline{R} \in \mathcal{E}_{\mathcal{D}}(L_1, L_2)$ with R relatively prime to L_2. Then for any $S \in \mathcal{D}$, $SPR + SQL_2 = S$. Therefore $\phi_R(SP + \mathcal{D}\cdot L_1) = \overline{S}$, so ϕ_R is surjective. Since $\mathcal{D}/\mathcal{D}\cdot L_1$ and $\mathcal{D}/\mathcal{D}\cdot L_2$ have the same dimension as vector spaces, this map must be an isomorphism. Conversely, assume that ϕ_R is an isomorphism. Then for some $P \in \mathcal{D}$ we have $\phi_R(P + \mathcal{D}\cdot L_1) = \overline{1}$. Therefore, there is a $Q \in \mathcal{D}$ such that $PR = 1 + QL_2$, so R and L_2 are relatively prime.

Now we show that there is an isomorphism between $\mathcal{E}_{\mathcal{D}}(L_1, L_2)$ and $Hom_G(V_2, V_1)$. Let $\overline{R} \in \mathcal{E}_{\mathcal{D}}(L_1, L_2)$ and let $v \in V_2$. We may apply R to v. Since $L_1 R$ is divisible on the right by L_2 we have that $R(v) \in V_1$. Therefore the map $\psi_R : v \mapsto R(v)$ is a linear map of V_2 to V_1 and this map depends only on the equivalence class of R. One easily checks that, since the coefficients of R lie in k, one has $\psi_R \in Hom_G(V_2, V_1)$. Therefore the map $\Psi : \overline{R} \mapsto \psi_R$ is well defined and can be seen to be a $\mathcal{C}-$homomorphism. If $\psi_R = 0$ then $R(v) = 0$ for all $v \in V_2$, so (by Lemma 2.1) L_2 divides R on the right. Therefore $\overline{R} = 0$ and so Ψ is injective. Let $\psi \in Hom_G(V_2, V_1)$ and let $v_1, \ldots, v_n$ be a basis of V_2. One sees that the entries of the matrix $A = Wr(\psi(v_1), \ldots, \psi(v_n)) \cdot Wr(v_1, \ldots, v_n)^{-1}$ are left invariant by G and so lie in k. If $(a_0, \ldots, a_{n-1})$ is the first row of A, let $R = a_{n-1}D^{n-1} + \ldots + a_0$. One then checks that $\psi = \psi_R$. Therefore Ψ is surjective.

We now show that Ψ is a bijection between the corresponding sets mentioned in 2. Let $\overline{R} \in \mathcal{E}_{\mathcal{D}}(L_1, L_2)$ with R relatively prime to L_2 (c.f., Lemma 2.1). If $v \in V_2$ satisfies $\psi_R(v) = 0$, then $R(y) = 0$ and $L_2(y) = 0$ have a common solution v contradicting the fact that these two operators are relatively prime. Therefore ψ_R is injective and so must be an isomorphism. Conversely, assume that R and L_2 have a common factor L_3. We may write $R = PL_3$ and $L_2 = QL_3$. By Lemma 2.1.3, L_3 has a full set of solutions in K so the map $v \mapsto L_3(v)$ has a nontrivial kernel. Therefore the map $\psi_R : v \mapsto R(v)$ has a nontrivial kernel, so ψ_R is not an isomorphism.

We leave the statement concerning the case when $L_1 = L_2 = L$ to the reader. ∎

From part 2. of the above (and its proof), we conclude:

Corollary 2.6 *Let L_1, L_2 be monic operators in $\mathcal{D}$, both of order n. The following are equivalent:*

1. *If K is a Picard-Vessiot extension of k containing the Picard-Vessiot extensions of k corresponding to L_1 and L_2, then the solution spaces of $L_1(y) = 0$ and $L_2(y) = 0$ are isomorphic G-modules, where G is the Galois group of K.*

2. *There exist $u_0, \ldots, u_{n-1} \in k$ such that for any Picard-Vessiot extension K of k containing the Picard-Vessiot extension of k corresponding to L_1, the map $y \mapsto \sum u_j y^{(j)}$ is a vector space isomorphism of the solution space of L_1 onto the solution space of L_2.*

3. *There exists an operator L_3, with coefficients in k, relatively prime to L_1 such that $L_2 \circ L_3 = L_4 \circ L_1$ for some operator L_4 with coefficients in k.*

4. *$\mathcal{D}/(\mathcal{D} \cdot L_1) \simeq \mathcal{D}/(\mathcal{D} \cdot L_2)$ as $\mathcal{D}$-modules.*

Classically, two operators of the same order are said to be *of the same type* if conditions 2. or 3. hold.

Corollary 2.7 *Let $L_1, L_2 \in \mathcal{D}$. If L_1 and L_2 are irreducible then $\mathcal{E}_{\mathcal{D}}(L_1, L_2)$ has dimension 1 or 0, depending on whether L_1 and L_2 are of the same type or not. In particular, if L is irreducible then $\mathcal{E}_{\mathcal{D}}(L)$ is isomorphic to $\mathcal{C}$.*

Proof: Let K be a Picard-Vessiot extension of k containing the Picard-Vessiot extensions of L_1 and L_2, let G be the Galois group of L and let V_i be the solution space of $L_i(y) = 0$ in K, for $i = 1, 2$. Since each L_i is irreducible, Corollary 2.3 implies that V_i is an irreducible $G-$module. Schur's Lemma implies that $Hom_G(V_2, V_1)$ has dimension 1 or 0 depending on whether V_1 and V_2 are isomorphic or not. Note that for any $L \in \mathcal{D}, \mathcal{C} \subset \mathcal{E}_{\mathcal{D}}(L)$ so $dim \mathcal{E}_{\mathcal{D}}(L) \geq 1$. Therefore when L is irreducible, we conclude from the first part that $\mathcal{E}_{\mathcal{D}}(L) \simeq \mathcal{C}$ ∎

Example 2.8 The converse of the last statement of the above corollary is not true. To see this, let $k = \mathbb{C}(x)$ and $L = D^2 + \frac{1}{x}D - (1 + \frac{1}{x}) = (D + (1 + \frac{1}{x}))(D - 1)$. This has a fundamental set of solutions $y_1 = e^x$, $y_2 = e^x \int \frac{e^{-2x}}{x}$. The corresponding Picard-Vessiot extension is $K = k(e^x, \int(e^{-2x}/x))$ and the Galois group is $G = \{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{C}^*,\ b \in \mathbb{C}\}$. The only matrices that commute with each of the matrices in this group are the constant matrices. Since we can identify $Hom_G(V, V)$, $V = Soln_K(L)$, with $\mathcal{E}_{\mathcal{D}}(L)$, we see that $\mathcal{E}_{\mathcal{D}}(L)$ is isomorphic to $\mathcal{C}$, while L is reducible.

Let L_1 have order m and L_2 have order n. Note that each element of $\mathcal{E}_{\mathcal{D}}(L_1, L_2)$ has a unique representative in $\mathcal{D}$ of order at most $n - 1$. Therefore, one may identify $\mathcal{E}_{\mathcal{D}}(L_1, L_2)$

with a $\mathcal{C}-$subspace W of k^n via the map $R = a_{n-1}D^{n-1} + \ldots + a_0 \mapsto (a_{n-1}, \ldots, a_0)$. Since $dim_{\mathcal{C}}(Hom_G(V_2, V_1)) \leq nm$, we have that $dim_{\mathcal{C}} W \leq nm$. Let R be a linear operator with differential indeterminates $\overline{a}_{n-1}, \ldots, \overline{a}_0$ for coefficients. If we divide $L_1 R$ on the right by L_2 we will get a remainder $\tilde{R}$ where the coefficient $\tilde{a}_i$ of each D^i, $0 \leq i \leq n-1$, is a linear expression (with coefficients in k) in the $\overline{a}_j$ and their derivatives. Therefore, there is an $n \times n$ matrix $\mathcal{A}_{L_1,L_2}$ with entries in $\mathcal{D}$ such that $\mathcal{A}_{L_1,L_2} \cdot (\overline{a}_{n-1}, \ldots, \overline{a}_0)^T = (\tilde{a}_{n-1}, \ldots, \tilde{a}_0)^T$. This implies that $R = a_{n-1}D^{n-1} + \ldots + a_0 \in \mathcal{D}$, of order at most n, represents an element of $\mathcal{E}_{\mathcal{D}}(L_1, L_2)$ if and only if $\mathcal{A}_{L_1,L_2} \cdot (a_{n-1}, \ldots, a_0)^T = 0$. If F is a differential field containing k with the same constants as K, we denote by $Soln_F(\mathcal{A}_{L_1,L_2})$ the $\mathcal{C}-$space of solutions of $\mathcal{A}_{L_1,L_2} \cdot \overline{a} = 0$ with $\overline{a} \in F^n$. We then have:

Corollary 2.9 *Let F be a differential extension field of k with the same constants. Then the vector spaces $\mathcal{E}_{F[D]}(L_1, L_2)$ and $Soln_F(\mathcal{A}_{L_1,L_2})$ are isomorphic. In particular, if $L = L_1 = L_2$ is irreducible in $F[D]$, then $Soln_F(\mathcal{A}_L)$ has dimension one.*

Example 2.10 Let $k = \mathcal{C}(x)$ and $L = D^4$. $\mathcal{E}_{\mathcal{D}}(L) = \{R \in \mathcal{D} \mid ord(R) < 4$ and $D^4 R$ is divisible on the right by $D^4\}$. If we let $R = \overline{a}_3 D^3 + \overline{a}_2 D^2 + \overline{a}_1 D + \overline{a}_0$, the condition that $\overline{R} \in \mathcal{E}_{\mathcal{D}}(L)$ is that the coefficients of D^3, D^2, D^1, and D^0 in $D^4 R$ are all zero. This yields the following system $\mathcal{A}_L$):

$$\begin{aligned} \overline{a}_0^{(iv)} &= 0 \\ 4\overline{a}_0^{(iii)} + \overline{a}_1^{(iv)} &= 0 \\ 6\overline{a}_0^{(ii)} + 4\overline{a}_1^{(iii)} + \overline{a}_2^{(iv)} &= 0 \\ 4\overline{a}_0' + 6\overline{a}_1^{(ii)} + 4\overline{a}_2^{(iii)} + \overline{a}_3^{(iv)} &= 0 \end{aligned}$$

By inspection, one sees that all solutions $(\overline{a}_3, \overline{a}_2, \overline{a}_1, \overline{a}_0)$ have polynomial entries and that the space of such solutions has dimension 16. Therefore, $dim_{\mathcal{C}}\mathcal{E}_{\mathcal{D}}(L) = 16$. One can verify this by noting that the Galois group of L is trivial, so $End_G(V)$ is the ring of all 4×4 matrices.

In Section 3.1, we will discuss how one determines, in general, the dimension of $Soln_F(\mathcal{A}_L)$ and show how this result gives an effective sufficient condition for reducibility.

We close this subsection by stating the theorem of unique factorization for linear operators. One cannot hope to claim that the operators appearing in a factorization into irreducible operators are unique. For example, $D^2 = D \cdot D = (D + \frac{1}{x})(D - \frac{1}{x})$.

Proposition 2.11 *For any $L \in \mathcal{D}$ of positive order, we may write $L = rL_1 \cdots L_m$ where $r \in k$ and each $L_i \in \mathcal{D}$ is monic and irreducible. If $L = \tilde{r}\tilde{L}_1 \cdots \tilde{L}_{\tilde{m}}$ is another such factorization, then $r = \tilde{r}, m = \tilde{m}$, and there exists a permutation π such that L_i and $\tilde{L}_{\pi(i)}$ are of the same type.*

Proof: Let G be the Galois group of L. A factorization of $L = rL_1 \cdots L_m$ corresponds to a normal series in the solution space $V = V_1 \supseteq \ldots V_m \supseteq \{0\}$ where each V_i is the solution space of $L_iL_{i-1} \cdots L_m(y) = 0$. Note that each V_i/V_{i-1} is G-isomorphic to the solution space of $L_i(y) = 0$ and so is an irreducible G-module. The Jordan-Hölder Theorem ([17], Ch. VII.1; [44], Sec. 46) implies that any two such normal series are equivalent, that is, there is a permutation such that V_i/V_{i-1} and $\tilde{V}_i/\tilde{V}_{i-1}$ are $G-$isomorphic. Lemma 2.6 implies that the coresponding operators would be of the same type. ∎

We note that a proof could also proceed by applying the Jordan-Hölder Theorem directly to the $\mathcal{D}$-module $\mathcal{D}/\mathcal{D} \cdot L$.

2.2 Reducibility of Completely Reducible Operators

We have seen above that the structure of $\mathcal{E}_{\mathcal{D}}(L)$ does not determine, in general, whether or not L is reducible. In this section we describe a class of operators where the structure of this ring does determine the factorization properties of L.

Given two operators $L_1, L_2 \in \mathcal{D}$ one can define the *least commmon left multiple of* L_1 *and* L_2, $[L_1, L_2]_l$ to be the monic nonzero operator of smallest order such that both L_1 and L_2 divide this operator on the right. To see that this definition uniquely defines $[L_1, L_2]_l$, note that if S and T are two such operators, then they must be of the same order. Writing $S = QT + R$ with $ord(R) < ord(T)$, one sees that L_1 and L_2 divide R on the right. Therefore, $R = 0$ and so comparing orders and leading coefficients, one has $S = T$. One can clearly define the least common left multiple $[L_1, \ldots, L_m]_l$ of any finite set of operators $\{L_1, \ldots, L_m\}$. We say that a linear operator is *completely reducible* if it is a k-left multiple of the least common left multiple of a set of irreducible operators. In Lemma 2.13, we shall give a group theoretic characterization of this notion.

Lemma 2.12 *Let $L, L_1, \ldots, L_m \in \mathcal{D}$ and let K be a Picard-Vessiot extension of k containing a full set of solutions of each of $L(y) = 0, L_1(y) = 0, \ldots, L_m(y) = 0$. $L = a[L_1, \ldots, L_m]_l$, for some $a \in k$ if and only if the solution spaces V_i of $L_i(y) = 0$ generate the solution space V of $L(y) = 0$.*

Proof: Let W be the vector space spanned by the V_i and let G be the Galois group of K. Clearly W is G-invariant, so it is the solution space of some monic $\overline{L} \in \mathcal{D}$. Since $V_i \subset W$, L_i divides $\overline{L}$ on the right. If $\tilde{L} \in \mathcal{D}$ and for each i, L_i divides $\tilde{L}$, then $\tilde{L}$ vanishes on W, so $\overline{L}$ divides $\tilde{L}$ on the right. Therefore $\overline{L} = [L_1, \ldots, L_m]_l$ and so $L = a\overline{L}$ if and only if $V = W$. ∎

Let G be a linear algebraic group. Given a $G-$module W and a submodule W_1, we say W_1 has a *complementary submodule* if there is a submodule W_2 of W such that $W = W_1 \oplus W_2$. A finite dimensional $G-$module V is said to be *completely reducible* if every submodule has a complementary invariant submodule. This is equivalent to V being the direct sum of irreducible submodules. Recall that the unipotent radical G_u of a group is the largest normal unipotent subgroup (see [16] for a definition of these and related notions). Note that G_u coincides with the unipotent radical of the connected component of the identity. The group G is said to be *reductive* if its unipotent radical is trivial. When the field is algebraically closed and of characteristic zero, it is well known that G is reductive if and only if it has a *faithful* completely reducible $G-$module. In this case, all G-modules will be completely reducible [7].

Lemma 2.13 *Let $L \in \mathcal{D}$. Let K be a Picard-Vessiot extension of k corresponding to $L(y) = 0$, and let G be the Galois group of K. The following are equivalent:*

1. *L is completely reducible.*
2. *The solution space of $L(y) = 0$ in K is a completely reducible $G-$submodule.*
3. *The Galois group of L is a reductive group.*

Proof: Assume 1. is true and let $L = [L_1, \ldots, L_m]_l$ be a minimal representation of L as a least common left multiple of irreducible operators. By minimality, we have that L_i does not divide $[L_1, \ldots, \hat{L}_i, \ldots, L_m]_l$. For each i, we may write $L = \tilde{L}_i L_i$. By Lemma 2.1, L_i has a full set of solutions in K. Furthermore, since each L_i is irreducible, each V_i is an irreducible $G-$module. From the condition that L_i does not divide $[L_1, \ldots, \hat{L}_i, \ldots, L_m]_l$ on the right, we have that $V_i \cap V_1 + \ldots + \hat{V}_i + \ldots + V_m = \{0\}$. Lemma 2.12 implies that V is the direct sum of the V_i. Therefore V is a completely reducible $G-$module.

Assume 2. is true and write $V = V_1 \oplus \ldots \oplus V_m$ where the V_i are irreducible $G-$modules. By Lemma 2.2, each V_i is the solution space of an irreducible operator L_i and by Lemma 2.12, we have that 1. is true.

The equivalence of 2. and 3. follows from the discussion preceding the lemma. ∎

One can easily describe $\mathcal{E}_{\mathcal{D}}(L)$ when L is completely reducible. Given any ring $\mathcal{R}$, any completely reducible $\mathcal{R}-$module $\mathcal{M}$ may be written in the form $\mathcal{M} = \mathcal{M}_1^{(n_1)} \oplus \cdots \oplus \mathcal{M}_1^{(n_r)}$ where the $\mathcal{M}_i$ are non-isomorphic irreducible $\mathcal{M}-$modules, each repeated n_i-times in the direct sum. It is a well known extension of Schur's Lemma (c.f., [23], Chapter XVII, Section 1, Proposition 1.2) that $End_{\mathcal{R}}(\mathcal{M})$ is isomorphic to $Mat_{n_1}(End_{\mathcal{R}}(\mathcal{M}_1)) \oplus \ldots \oplus Mat_{n_r}(End_{\mathcal{R}}(\mathcal{M}_r))$, where $Mat_{n_i}(End_{\mathcal{R}}(\mathcal{M}_i))$ is the ring of $n_i \times n_i$ matrices with entries in $End_{\mathcal{R}}(\mathcal{M}_i)$. If L is a completely reducible operator, we can apply this result to the $\mathcal{C}[G]$-module V, where V is the solution space of L in the associated Picard-Vessiot extension of k and $\mathcal{C}[G]$ is the group algebra of G. Note that since $\mathcal{C}$ is algebraically closed we have (by Schur's Lemma) that any $End_{\mathcal{C}[G]}(V_i)$ is isomorphic to $\mathcal{C}$. Therefore, using the isomorphisms of Lemma 2.5, we have the following:

Lemma 2.14 *If L be a completely reducible linear operator, then $\mathcal{E}_{\mathcal{D}}(L)$ is isomorphic to $Mat_{n_1}(\mathcal{C}) \oplus \ldots \oplus Mat_{n_r}(\mathcal{C})$ for some integers n_i. In this case, L is irreducible if and only if $\mathcal{E}_{\mathcal{D}}(L)$ is isomorphic to $\mathcal{C}$.*

Recalling the notation of the previous section, we have:

Corollary 2.15 *A completely reducible operator L is reducible if and only if $dim_{\mathcal{C}} Soln_k(\mathcal{A}_L) > 1$. This happens if and only if $\mathcal{A}_L \cdot \overline{a}^T = 0$ for some $\overline{a} = (a_{n-1}, \ldots, a_0) \in k^n$ with either $a_i \neq 0$ for some $i > 0$ or $a_0 \notin \mathcal{C}$.*

Proof: The first part of the corollary follows from the fact that $\mathcal{E}_{\mathcal{D}}(L)$ is isomorphic to $Soln_k(\mathcal{A}_L)$ as $\mathcal{C}-$vector spaces. Recall that $End_G(V)$ always contains the endomorphisms induced by constant multiplication. Such an endomorphism corresponds to an element $\overline{R} = 0D^{n-1} + \ldots 0D + a \in \mathcal{E}_{\mathcal{D}}(L)$, $a \in \mathcal{C}$ and so is given by $(0, \ldots, 0, a) \in Soln_k(\mathcal{A}_L)$. Therefore $dim_{\mathcal{C}} Soln_k(\mathcal{A}_L) > 1$ if and only if this space contains elements not of this form. ∎

2.3 Reducibility of General Operators

In this section we give a criterion for a linear operator to be completely reducible. If L is an operator that is not completely reducible, then it cannot be irreducible. Therefore, this criterion together with the results of the previous section will yield a criterion for an operator to be reducible.

An operator is not completely reducible if and only if its Galois group G is a non-reductive group. This happens if and only if the solution space (in the associated Picard-Vessiot extension) is not a completely reducible G-module. We begin by considering a modification of the notion of completely reducible. We say that W is *1-reductive* if every 1-dimensional G-submodule has a complementary submodule.

Lemma 2.16 *Let G be a linear algebraic group over an algebraically closed field, V a G-module and W_1 be the sum of all one dimensional submodules of V. The following are equivalent:*

1. *V is 1-reductive.*
2. *W_1 has a complementary submodule in V.*
3. *If W is a submodule of W_1, then W has a complementary submodule in V.*

Proof: Assume 2. holds. Since W_1 is the sum of irreducible modules it is completely reducible. Therefore, for any submodule $W \subset W_1$, W has a complementary submodule in W_1. Since W_1 has a complementary submodule in V, W will have a complementary submodule in V. Therefore 3. holds.

Assume 3. holds. Any 1-dimensional submodule V_1 of V is a submodule of W_1, so V_1 has a complementary submodule in V. Therefore 1. holds.

Assume 1. holds. Let W_0 be a submodule of W_1, maximal with respect to the property of having a complementary submodule in V and write $V = W_0 \oplus \tilde{W}_0$. If $W_0 \neq W_1$, then there is a one dimensional submodule $V_1 \subset W_1, V_1 \not\subset W_0$. Using 1., we may write $V = V_1 \oplus \tilde{V}_1$. Let π be the projection of V onto $\tilde{W}_0$ with kernel W_0. Since V_1 is one dimensional and $V_1 \cap W_0 = (0)$, we have that $\pi(V_1) \neq (0)$. Writing $\tilde{W}_0 = \pi(V_1) \oplus \pi(\tilde{V}_1)$, we have that $(W_0 \oplus \pi(V_1)) \oplus \pi(\tilde{V}_1) = V$. Therefore $W_0 \oplus \pi(V_1)$ is strictly larger than W_0 and has a complementary submodule in V, contradicting the maximality of W_0. Therefore, $W_0 = W_1$ and 2. holds. ∎

For a non-reductive group G, we have that the unipotent radical $G_u \neq (0)$ so we begin by studying unipotent groups. The following contains the facts we will need concerning unipotent groups.

Lemma 2.17 *Let U be a nontrivial unipotent group defined over an algebraically closed field $\mathcal{C}$ and let V be a faithful $U-$module of dimension n.*

1. *$V_0 = \{v \in V \mid \sigma(v) = v \text{ for all } \sigma \in U\}$ is a nonzero invariant $U-$submodule of V of dimension at most $n-1$.*
2. *If dim $V_0 = i$ then $\bigwedge^i V_0$ is a one-dimensional submodule of $\bigwedge^i V$ that has no complementary submodule and so $\bigwedge^i V$ is not 1-reductive.*

Proof: V_0 is nonzero by ([16], Thm 17.5). If its dimension is n, then the group would be trivial, since the module is a faithful module.

To prove 2., note that $\bigwedge^i V_0$ is clearly one-dimensional and $U-$invariant. Applying 1. to the module V/V_0, we see that there is an element $w \in V, w \notin V_0$ such that for any $\sigma \in U$, there exists a $w_\sigma \in V_0$ such that $\sigma(w) = w + w_\sigma$. Furthermore, for some $\sigma \in U$, we must have $w_\sigma \neq 0$, otherwise w would lie in V_0. Fix such a σ. Now assume that $\bigwedge^i V_0$ has a complementary submodule W and write $\bigwedge^i V = \bigwedge^i V_0 \oplus W$. Let $v_1 = w_\sigma, \ldots, v_i$ be a basis of V_0, so $v_1 \wedge v_2 \wedge \cdots \wedge v_i$ is a basis of $\bigwedge^i V_0$. Therefore $\sigma(w) = w + v_1$. We may write $w \wedge v_2 \wedge \cdots \wedge v_i = w_0 + bv_1 \wedge v_2 \wedge \cdots \wedge v_i$, for some $w_0 \in W$. Therefore we have

$$\sigma(w \wedge v_2 \wedge \cdots \wedge v_i) = w \wedge v_2 \wedge \cdots \wedge v_i + v_1 \wedge v_2 \wedge \cdots \wedge v_i = w_0 + (1+b)v_1 \wedge v_2 \wedge \cdots \wedge v_i$$

and

$$\sigma(w \wedge v_2 \wedge \cdots \wedge v_i) = \sigma(w_0 + bv_1 \wedge v_2 \wedge \cdots \wedge v_i) = \sigma(w_0) + bv_1 \wedge v_2 \wedge \cdots \wedge v_i$$

Comparing the final expressions in these two formulas we see

$$w_0 - \sigma(w_0) = v_1 \wedge v_2 \wedge \cdots \wedge v_i$$

Since $w_0 - \sigma(w_0)$ is in W and W and $\bigwedge^i V_0$ are complementary, we must have $v_1 \wedge v_2 \wedge \cdots \wedge v_i = 0$ a contradiction ∎

Proposition 2.18 *Let G be a linear algebraic group defined over an algebraically closed field $\mathcal{C}$ and let V be a faithful $G-$module of dimension n. Then G is reductive if and only if for every i, $1 \leq i \leq n-1$, $\bigwedge^i V$ is 1-reductive.*

Proof: If G is reductive then any submodule of a module has a complementary submodule. Now assume that G is not reductive and so $G_u \neq (0)$. In the notations of Lemma 2.17.1, $V_0 \neq (0)$. Since G_u is normal in G and the elements of V_0 are the only elements of V left fixed by G_u, V_0 is a $G-$invariant subspace of V. $\bigwedge^i V_0$ is therefore a one dimensional $G-$submodule of $\bigwedge^i V$ and by Lemma 2.17.2, it does not have a G_u-complement, so it cannot have a $G-$complement. ∎

Let $L_0 \in \mathcal{D}$ and let K_0 be the Picard-Vessiot extension of k asociated to L_0 with Galois group G_0. We say that L_0 is *1-reductive* if the solution space of L_0 is 1-reductive as a G_0 module. If K is any Picard-Vessiot extension of k, with Galois group G having a full set of solutions of $L_0(y) = 0$, then we can embedd K_0 into K. The action of G on K_0 factors through the action of G_0 on K_0. Therefore L_0 is 1-reductive if and only if *for any* Picard-Vessiot extension of k with Galois group G, having a full set of solutions of $L_0(y) = 0$, the solution space of $L_0(y) = 0$ in K is 1-reductive as a G module. Also note that L_0 is 1-reductive if and only if for each first order right factor $L_1 \in \mathcal{D}$ of L_0, there exists an $\tilde{L}_1 \in \mathcal{D}$, relatively prime to L_1 such that $L_0 = [L_1, \tilde{L}_1]_l$. We shall show in the next section how the following gives an effective method to test if a linear operator is completely reducible.

Corollary 2.19 *Let $L \in \mathcal{D}$ and let K be the associated Picard-Vessiot extension with Galois group G. Let $L^{\wedge i}$ be an operator whose solution space is $G-$isomorphic to $\bigwedge^i V$, where V is the solution space of L in K. L is a completely reducible operator if and only if $L^{\wedge i}$ is $1-$reductive for each $i = 1, \ldots, n-1$.*

Proof: This follows from the previous lemma by noting that L is completely reducible if and only if its Galois group is reductive. ∎

Proposition 2.20 *Let G be a linear algebraic group defined over an algebraically closed field $\mathcal{C}$ and let V be a faithful $G-$module of dimension n. Then V is an irreducible $G-$module if and only if:*

1. *For each* $i, 1 \leq i \leq n-1$, $\bigwedge^i V$, *is* 1-*reductive, and*

2. $End_G(V) = \mathcal{C}$

Proof: If V is irreducible then the second condition holds by Schur's Lemma. Furthermore, in this case G is reductive, so any submodule of a module will have a complement.

If V is not irreducible and G is reductive then $End_G(V) \neq \mathcal{C}$ by the discussion preceeding Lemma 2.14. Assume V is not irreducible and G is not reductive. Then Proposition 2.18 implies that the first condition cannot hold. ∎

Corollary 2.21 *Let* $L \in \mathcal{D}$ *and let* K *be the associated Picard-Vessiot extension with Galois group* G. *Let* $L^{\wedge i}$ *be an operator whose solution space is* $G-$*isomorphic to* $\bigwedge^i V$, *where* V *is the solution space of* L *in* K. L *is irreducible if and only if all of the following hold:*

1. *For each* $i, 1 \leq i \leq n-1$, $L^{\wedge i}$ *is* $1-$*reductive.*

2. $dim_{\mathcal{C}} Soln_k(\mathcal{A}_L) = 1$

Proof: This is just a restatement of Proposition 2.20. ∎

Corollary 2.21 is the basis of our reducibility tests. Condition 2. can be restated in several ways using Lemma 2.5 and we will show in section 3.1 how each of these equivalent statements can be used to develop algorithms to test reducibility. Condition 1. appears to require that one check a possibly infinite number of possibilities. We shall show in section 3.2 that this is not the case and give an algorithm that decides if condition 1. holds.

2.4 Remarks

A good guide to the nineteenth century literature concerning linear differential equations is [15]. We will give a brief indication of the sources of the results in sections 2.1 and 2.2. Lemma 2.1.2 already occurs in [11]. In this paper, Frobenius also determines necessary and sufficient conditions for a Fuchsian equation with three singular points to be reducible. The connection between reduciblity of the equation and reducibility of the group was made by Jordan in [20] for Fuchsian equations and by Beke in [4] for general equations. In Beke's paper, one can also find a decision procedure for determining if a linear differential equation with rational coefficients is reducible or not (a related procedure is described in [38]). Unique factorization of linear differential operators is discussed in [22]. In this paper, Landau proves the uniqueness of the number of irreducible factors and their sets of orders. At the end of the paper, Landau notes the similarity of his techniques with those used by Jordan to prove his theorem concerning composition series for finite groups. In [24], Loewy gives the complete factorization theorem (although the notion of linear equations of the same type goes back to (at least) Poincaré [36]). In a subsequent series of papers [25, 26, 27, 28], Loewy examined the notion of completely reducible operators, factorization into completely reducible operators, and what properties carry over to operators of the same type. In [29, 30] Loewy considers systems of linear differential equations and proves results analogous to the results in the above papers. These results follow easilly from either the group theoretic or $\mathcal{D}-$module approach. In [33], Ore considers the ring of linear differential operators from a ring theoretic perspective. In the second part of this sequence, he defines the eigenring of an operator and shows that it is a finite dimensional algebra corresponding to solutions of a certain system of differential equations (our $\mathcal{A}_L$). He also discusses various kinds of factorizations. In [34], Ore generalizes many of these results to skew polynomial rings $F[T]$ where for some derivation D of F and automorphism σ of F we have $T \cdot v = \sigma(v)T + Dv$, for all $v \in F$. Jacobson [18] (see also [19]) develops a theory of finite dimensional modules over such a ring. This theory applies to the situation when V is a finite dimension $\mathcal{D}-$module (let $\sigma=$ identity, so $F[T]$ is isomorphic to $F[D]$). In the general situation, Jacobson shows that such a vector space can be decomposed into cyclic subspaces. Furthermore he shows that when V is completely reducible, the eigenring is a sum of matrix rings (with entries in a division algebra). For the special case of $\mathcal{D}-$modules, Jacobson shows that all finite dimensional $\mathcal{D}-$modules are cyclic (see [3] for references to other proofs and effective methods). Jacobson ends his paper by noting that when T is irreducible, the eigenring is a division algebra over $\mathcal{C}$ (here we do not assume that $\mathcal{C}$ is algebraically closed) and that this observation may be used to construct interesting division algebras. Amitsur further develops this idea in [1]. He recapitulates the results of Ore and Jacobson in more modern language and then uses these ideas to classify all central division algebras over a field $\mathcal{C}$ that are split by k where k is a transcendental extension of $\mathcal{C}$. Some of the results of Ore, Jacobson and Amitsur are contained in Chapter 0 of [9].

The results of section 2.3 seem new.

Finally we note that the classical factorization algorithms can be considered in this light. Given $L \in \mathcal{D}$ let $V = Soln_k(L)$ and let W be a $G-$invariant subspace of V, where G is the Galois group of L. If W is nontrivial, it will be the solution space of some factor L_1 of L. We can think of L_1 as a surjective element of $Hom_G(V, V/W)$. Therefore, to decide if L is reducible, we only need to decide if there exists a surjective $G-$morphism of V onto a nontrivial $G-$module of smaller dimension. This is the philosophy behind the algorithm in [14], where the question of reducibility of systems is examined. This approach seems to be equivalent to factoring.

3 Algorithmic Considerations

Let $L \in \mathcal{D}$, K the associated Picard-Vessiot extension of k with Galois group G and V the space of solutions of $L(y) = 0$ in K. Proposition 2.20 states that to test if L is irreducible in $\mathcal{D}$ it is necessary and sufficient to:

1. Show that $End_G(V) = \mathcal{C}$, and
2. Show that for each $i, 1 \leq i \leq n-1$, $\bigwedge^i V$ is $1-$reductive, i.e., each one-dimensional submodule V_i of $\bigwedge^i V$, has a complementary submodule.

In the next two subsections we will describe techniques for performing these tasks. In the third subsection we will describe an applications to computing Galois groups and some directions for further investigations.

Since the goal of this paper is to describe reducibility tests for linear differential equations (scalar equations) and not systems, we tailor our strategies to handle single n^{th} order equations (although some of these strategies can be clearly modified to handle systems). Regretably, some of the strategies require one to convert to systems. We review this process now. Recall that the companion matrix of a scalar equation $L(y) = y^{(n)} - a_{n-1}y^{(n-1)} - \ldots - a_0$ is

$$A = \begin{pmatrix} 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ a_{n-1} & a_{n-2} & a_{n-3} & \ldots & a_0 \end{pmatrix}$$

The system $Y' = AY$ is equivalent to the equation $L(y) = 0$. This means one of the following equivalent statements:

- The $\mathcal{D}$ modules $\mathcal{D}/\mathcal{D} \cdot L$ and k^n (where the action is defined by $D \cdot (v_1, \ldots, v_n)^T = (v_1', \ldots, v_n')^T + A(v_1, \ldots, v_n)^T$ for $v \in k^n$) are $\mathcal{D}-$isomorphic,
- The solution spaces of $L(y) = 0$ and $Y' = AY$ (in the Picard-Vessiot extension of L) are G-isomorphic.

Using the second characterization, one sees that the space of solutions of $L(y) = 0$ *in* k and the space of solutions of $Y' = AY$ *in* k^n are isomorphic since these are just the $G-$fixed points of the solution spaces of these respective equations.

We shall also need the notion of the adjoint of a differential equation (see [35]). If L is as above, the *adjoint* L^* of L is defined to be the equation $L^*(y) = (-1)^n y^{(n)} - (-1)^{n-1}(a_{n-1}y)^{(n-1)} - \ldots - a_0 y$. One can show that

- The $\mathcal{D}$ modules $\mathcal{D}/\mathcal{D}\cdot L^*$, $Hom_k(\mathcal{D}/\mathcal{D}\cdot L, k)$ and k^n (where the action is defined by $D\cdot(v_1,\ldots,v_n)^T = (v_1',\ldots,v_n')^T - A^T(v_1,\ldots,v_n)^T$ for $v\in k^n$) are $\mathcal{D}-$isomorphic,
- The solution spaces of $L^*(y)=0$ and $Y' = -A^TY$ (in the Picard-Vessiot extension of L) are G-isomorphic.

3.1 Calculating $dim_{\mathcal{C}}End_G(V)$

Let L be a linear differential operator with coefficients in $\mathcal{C}(x)$, K the associated Picar-Vessiot extension, G the Galois group and V the space of solutions of $L(y)=0$ in K. In this subsection, we shall present three algorithms for calculating $dim_{\mathcal{C}}End_G(V)$ and discuss their relative merits.

Algorithm 1: We shall use the fact that $End_G(V)$ is isomorphic to $\mathcal{E}_{\mathcal{D}}(L)$. In the discussion preceding Corollary 2.9, we noted that this space is precisely the set of solutions in k of a system of linear differential equations $\mathcal{A}_L(Y)=0$ and we described how, using the division algorithm, one could effectively calculate this system (an alternate method is described in [33] II, p. 237). One then is confronted with calculating the dimension of the space of solutions in k^n. Occasionally, one is lucky and one can easily read off this dimension (see the example below). At present, the only general technique we know is to convert this system to a single scalar equation (of order n^2) using a cyclic vector computation (see the bibliography of [3]) or to an equivalent system in companion block diagonal form as in [3]. This reduces the problem to finding solutions (in k) of one or several scalar equations. When $k=\mathcal{C}(x)$, this latter problem was solved in the nineteenth century. For recent algorithms, that also consider other fields k, see [8, 41]. An open problem is the problem of finding the dimension of the space of solutions in k^n of this system without having to convert to scalar equations.

We also note that if one has found an element $\overline{R}\in\mathcal{E}_{\mathcal{D}}(L)$, R of order greater than or equal to 1, then one can produce a non-trivial factor of L. To do this, let $R\in\mathcal{E}_{\mathcal{D}}(L), ord(R)\geq 1$. We then have that LR is divisible on the right by L. Therefore, if z is a solution of $L(y)=0$, we have that $R(z)$ is again a solution of $L(y)=0$. This implies that $z\mapsto R(z)$ is a linear map of the solution space of $L(y)=0$ into itself. If c is an eigenvalue of this map, then $(R-c)(y)=0$ and $L(y)=0$ have a common solution. Since $0<ord(R-c)<n$, $GCRD(R-c,L)$ will be a non-trivial factor of L. Therefore given $\overline{R}\in\mathcal{E}_{\mathcal{D}}(L)$, the condition $GCRD(R-c,L)\neq 1$, defines a nonempty set of at most n constants and for each of these $GCRD(R-c,L)$ will be a non-trivial factor of L.

Example 3.1 In Example 2.10 we determined $\mathcal{A}_L$ using the above method. One can also find factors as described above. For example, $\overline{a}_0=-4, \overline{a}_1=x, \overline{a}_2=0, \overline{a}_3=0$ is a solution of the system, so $R=xD-4\in\mathcal{E}(D^4)$. We then have that $GCRD(D^4, xD-4-c)\neq 1$ if and only if $c=-1,-2,-3,-4$. One can see this by perfoming the euclidean algorithm or more simply (in this case) by noting that $GCRD(D^4, xD - 4 - c) \neq 1$ if and only if $xD - 4 - c$ divides D^4 which happens if and only if $y = x^{4+c}$ is a solution of $D^4(y) = 0$. ∎

Algorithm 2: This strategy is based on the fact that $End_G(V)$ is G-isomorphic to $(V^* \otimes V)^G$, the $G-$invariant elements of the tensor product of V and its dual V^*. We shall construct an operator whose solution space is G-isomorphic to this latter G-module. Let A be the companion matrix of L and let $B = -A^T \otimes I + I \otimes A$, where I is the $n \times n$ identity matrix. It is known ([10], Sec. 1.2.7) that the solution space of $Y' = BY$ is $(V^* \otimes V)^G$. We are now again confronted with finding the dimension of the space of rational solutions of a system of differential equations. The advantage of this approach over the previous one is that the system $Y' = BY$ is easy to compute and that it is a first order system. On the other hand, one has lost whatever special properties the system $Y' = \mathcal{A}_L Y$ possesses. Again, one can occassionally be lucky and avoid a cyclic vector computation. (Note that the system $Y' = BY$ can be rerwritten in a more classical way using matrix notation. If we represent an element of $End_{\mathcal{D}}(\mathcal{D}/caldL)$ as a map $X \mapsto ZX$, Z an $n \times n$ matrix, for which $X' = AX$ and $(ZX)' = A(ZX)$, then Z will satisfy $Z' = AZ - ZA$.)

Example 3.2 Let $k = \mathcal{C}(x)$ and $L = D^4$. The associated companion matrix is the 4×4 zero matrix, so the matrix $B = -A^T \otimes I + I \otimes A$ is the 16×16 zero matrix. Clearly the space of solutions of $Y' = BY$ in k^{16} has dimension 16. ∎

Algorithm 3: The disadvantage of the previous two strategies is that they convert a question about a scalar equation to a question about a system of equations and that to answer the latter question one must (at present) convert back to scalar equations. We will give two algorithms that avoid this and discuss nondeterministic versions of these as well. Given a linear operator L we wish to construct, as directly as possible an operator $\hat{L}$ whose solution space is $G-$isomorphic to $V \otimes V^*$. It is not hard to find an equation whose solution space is V^* - this is just the adjoint. The question is therefore: given two operators L_1 and L_2 with solution spaces V_1 and V_2, construct an equation whose solution space is $V_1 \otimes V_2$. We shall do this below. The basic philosophy motivating this algorithm is that *tensor products of generic cyclic vectors are again cyclic.*

Given two operators $L_1, L_2 \in \mathcal{D}$ there exists an operator $L_1 \circledS L_2 \in \mathcal{D}$ having the following property: If K is a differential extension of k containing a full set of solutions $\{u_1, \ldots, u_{n_1}\}$ of $L_1(y) = 0$ and $\{v_1, \ldots, v_{n_2}\}$ of $L_2(y) = 0$, then K contains a full set of solutions of $L_1 \circledS L_2(y) = 0$ and the solution space of this latter equation is spanned by $\{u_1 v_1, \ldots, u_{n_1} v_1, \ldots, u_{n_1} v_{n_2}\}$. (see [40, 43] where a method is given to compute this operator). When $L_1 = L_2$ we write $L^{\circledS 2}$ for $L \circledS L$. Note that the solution space of $L_1 \circledS L_2(y) = 0$ is a homomorphic image of $V_1 \otimes V_2$ where V_i is the solution space of $L_i(y) = 0$.

Example 3.3 Let $L = D^4$ and $k = \mathcal{C}(x)$. The solution space V of $L(y) = 0$ is the set of polynomials of degree at most 3. Therefore the solution space of $L^{\circledS 2}(y) = 0$ is the set of polynomials of degree at most 6, so $L^{ⓢ 2} = D^7$. This latter space has dimension 7 while $V \otimes V$ has dimension 16. ∎

Despite this example, we will want to use the construction of $L_1 ⓢ L_2(y) = 0$ to find an operator whose solution space is isomorphic to $V_1 \otimes V_2$. To do this we will have to replace L_2 by an operator of the same type. The following lemma gives two ways that this can be done. Before we state this lemma, we describe an ancillary construction. Given $L \in \mathcal{D}, ord(L) = n$ and $(b_0, \ldots, b_{n-1}) \in k^n$, we denote by $L^{(b_0,\ldots,b_{n-1})}$ the monic operator whose solution space is $\{z \mid z = b_0 y + b_1 y' + \ldots + b_{n-1} y^{(n-1)}$ for y satisfying $L(y) = 0\}$. One can effectively construct $L^{(b_0,\ldots,b_{n-1})}$ from L by letting z and y be indeterminates and differentiating $z = b_0 y + b_1 y' + \ldots + b_{n-1} y^{(n-1)}$ n times. Using $L(y) = 0$ to replace all $y^{(i)}, i \geq n$ by k-linear combinations of $y^{(i)}, i < n$, we are left with $n+1$ k-linear equations in the n quantities $y, \ldots, y^{(n-1)}$. Therefore, there will be a relation $c_n z^{(n)} + \ldots + c_0 z = 0$. Such a relation of smallest order will give $L^{(b_0,\ldots,b_{n-1})}$. Note that $L^{(b_0,\ldots,b_{n-1})}$ will have order n if and only if $L(y) = 0$ and $R(y) = b_0 y + \ldots + b_{n-1} y^{(n-1)} = 0$ have no common solutions. In this case, L and $L^{(b_0,\ldots,b_{n-1})}$ will be of the same type.

Lemma 3.4 *Let $k = \mathcal{C}(x)$ and let $L_1, L_2 \in \mathcal{D}, ord(L_1) = n, ord(L_2) = m$.*

1. *For all but a finite number of $c \in \mathcal{C}$, $ord(L_1 ⓢ L_2^{(1,(x-c)^{mn},(x-c)^{2mn},\ldots,(x-c)^{(n-1)mn})}) = mn$.*
2. *There exist polynomials $b_0, \ldots, b_{m-1}$ with constant coefficients and of degree at most $mn-1$ such that $ord(L_1 ⓢ L_2^{(b_0,\ldots,b_{n-1})}) = mn$.*

Proof: To prove 1., first consider the operators $L_1 ⓢ L_2, L_1 ⓢ L_2^{(0,1,0,\ldots,0)}, \ldots, L_1 ⓢ L_2^{(0,0,0,\ldots,1)}$. Each has order at most mn and only a finite number of singular points. Let c be a regular point of all of these operators. The standard existence and uniqueness theorem implies that if y is any solution of one of these such that y and all of its derivatives up to order mn vanish at c, then y is identically zero. Let $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_m\}$ be fundamental sets of solutions of $L_1(y) = 0$ and $L_2(y) = 0$ respectively and let $z_i = v_i + (x-c)^{mn} v_i' + (x-c)^{2mn} v_i'' + \ldots + (x-c)^{mn(mn-1)} v_i^{(m-1)}$ for $1 \leq i \leq m$. We claim that the elements $\{u_i v_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ are linearly independent. This suffices to prove 1. To prove the claim, assume that for some $c_{ij} \in \mathcal{C}, 0 = \sum_{i,j} c_{ij} u_i z_j$. We then have that

$$0 = \sum_{i,j} c_{ij} u_i z_j = \sum_{t=0}^{m-1} (\sum_{i,j} c_{i,j} u_i v_j^{(t)})(x-c)^{tmn}$$

Each $\sum_{i,j} c_{i,j} u_i v_j^{(t)}$ is either zero or vanishes to order at most $mn-1$ at c. Comparing powers of $x-c$ in the above expression we can therefore conclude that for each t, $\sum_{i,j} c_{i,j} u_i v_j^{(t)} = 0$.

Since the matrix $(v_j^{(k)})$ is invertible, we have that for each j, $\sum_{i,j} c_{i,j} u_i = 0$. Since the u_i are linearly independent, we have $c_{i,j} = 0$ for all i, j.

To prove 2., let $B_0, \ldots, B_{m-1}$ be differential indeterminates, let $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_m\}$ be as above and let $z_i = B_0 v_i + B_1 v_i' + \ldots + B_{m-1} v_i^{(m-1)}$. Consider the differential polynomial $R(B_0, \ldots, B_{m-1}) = det(Wr(u_1 z_1, \ldots, u_1 z_m, \ldots, u_n z_m))$. This polynomial is not identically zero (this follows from 1.) and has order at most $mn - 1$ in each variable B_i. Therefore, a result of Ritt ([37], p.35) implies that there exist polynomials $b_0, \ldots, b_{m-1}$ of degree at most $mn - 1$ such that $R(b_0, \ldots, b_{m-1}) \neq 0$. These polynomials satisfy the conclusion of 2. ∎

Example 3.5 This illustrates statement 1. of the above lemma. Let $L = D^4$. We then have that $L^{(1, x^{16}, x^{32}, x^{48})} =$

$$D^4 - \frac{480\, x^{14} \left(364\, x^{15} + 577536\, x^{45} + 8336640\, x^{60} + 3 + 37748736\, x^{75} + 21387\, x^{30}\right)}{228128\, x^{45} + 5824\, x^{30} + 96\, x^{15} + 4620288\, x^{60} + 53354496\, x^{75} + 201326592\, x^{90} + 1} D^3$$
$$+ \frac{480\, x^{13} \left(-1339\, x^{15} + 6983424\, x^{45} + 164465664\, x^{60} - 28 + 1063256064\, x^{75} + 79696\, x^{30}\right)}{228128\, x^{45} + 5824\, x^{30} + 96\, x^{15} + 4620288\, x^{60} + 53354496\, x^{75} + 201326592\, x^{90} + 1} D^2$$
$$- \frac{\left(4399992668160\, x^{75} + 214477701120\, x^{60} - 8726446080\, x^{45} - 413806080\, x^{30} - 4569600\, x^{15} + 43680\right) x^{12}}{228128\, x^{45} + 5824\, x^{30} + 96\, x^{15} + 4620288\, x^{60} + 53354496\, x^{75} + 201326592\, x^{90} + 1} D$$

If one calculates $L \circledS L^{(1, x^{16}, x^{32}, x^{48})}$ one gets an operator of order 16 with enormous coefficients. For example the coefficient of D^8 is a quotient of polynomials of degree 150 with 48 digit coefficients. ∎

Example 3.6 This illustrates statement 2. of the above lemma. We again let $L = D^4$. We then have that $L^{(x^{12}, x^8, x^4, 1)} =$

$$D^4 - \frac{884736 + 48\, x^{30} - 1032\, x^{25} + 14592\, x^{20} - 131736\, x^{15} + 559104\, x^{10} - 1333632\, x^5}{x\left(-24\, x^{25} + 384\, x^{20} - 3992\, x^{15} + 19968\, x^{10} - 57984\, x^5 + 49152 + x^{30}\right)} D^3$$
$$+ \frac{936\, x^{30} - 17664\, x^{25} + 213624\, x^{20} - 1617792\, x^{15} + 5643648\, x^{10} - 10520064\, x^5 + 5455872}{x^2\left(-24\, x^{25} + 384\, x^{20} - 3992\, x^{15} + 19968\, x^{10} - 57984\, x^5 + 49152 + x^{30}\right)} D^2$$
$$- \frac{8736\, x^{30} - 141144\, x^{25} + 1383264\, x^{20} - 7997952\, x^{15} + 21523968\, x^{10} - 26855424\, x^5 + 11354112}{\left(-24\, x^{25} + 384\, x^{20} - 3992\, x^{15} + 19968\, x^{10} - 57984\, x^5 + 49152 + x^{30}\right) x^3} D$$
$$+ \frac{360\, x \left(39232\, x^5 - 14336 - 24704\, x^{10} + 8612\, x^{15} + 91\, x^{25} - 1220\, x^{20}\right)}{-24\, x^{25} + 384\, x^{20} - 3992\, x^{15} + 19968\, x^{10} - 57984\, x^5 + 49152 + x^{30}}$$

Note that the degrees of the numerators and denominators of the coefficients are considerably smaller than in the previous example. If one calculates $L \circledS L^{(x^{12}, x^8, x^4, 1)}$ one again gets an operator of order 16 but with better coefficients. For example the coefficient of D^8 is a quotient of polynomials of degree 35 with 13 digit coefficients. ∎

We now give two procedures to calculate the dimension of $End_G(V)$.

Algorithm 3A: This uses Lemma 3.4.1. Select $c \in \mathcal{C}$ and form $L^* \circledS L^{(1, (x-c)^{n^2}, (x-c)^{2n^2}, \ldots, (x-c)^{(n-1)n^2})}$. If $ord(L^* \circledS L^{(1, (x-c)^{n^2}, (x-c)^{2n^2}, \ldots, (x-c)^{(n-1)n^2})}) = n^2$, then we have found an operator whose solution space is G-isomorphic to $V^* \otimes V$. One then proceeds as in the other algorithms to find the dimension of the space of rational solutions of this operator.

If $ord(L^* \circledS L^{(1,(x-c)^{n^2},(x-c)^{2n^2},\ldots,(x-c)^{(n-1)n^2})}) < n^2$, select another value for c and recalculate. Since there are only a finite number of bad values for c, we will eventually find one that works. In Example 3.5, this strategy was used. The proof of Lemma 3.4 gives a way of finding a value of c that works. An alternative approach is to form $L^* \circledS L^{(1,(x-c)^{n^2},(x-c)^{2n^2},\ldots,(x-c)^{n^2(n^2-1)})}$ for an indeterminate c with $c' = 0$. The condition that this operator have order n^2 will be equivalent to $p(c) \neq 0$ for some polynomial p that will be found in the process of forming the operator. We also note that the size of the set of "bad points" can be bounded in terms of the coefficients of L using the generalization of Fuchs' relation ([5, 42]).

Algorithm 3B: This is based on Lemma 3.4.2 and was used in Example 3.6. Let $B_0, \ldots, B_{n-1}$ be polynomials of degree n^2-1 with indeterminate coefficients. The condition that $L^* \circledS L^{(B_0,\ldots,B_{n-1})}$ is of order $n^2 - 1$ gives a non-empty (by Lemma 3.4.2) Zariski open set of coefficients in $\mathcal{C}$. The defining equations can be constructed and a element of this set can be found. One then proceeds as above to find the dimension of the space of rational solutions.

In practice (and in Example 3.6) one should select arbitrary polynomials $b_0, \ldots, b_{n-1}$ with constant coefficients and of degree at most $n^2 - 1$ and form $L^* \circledS L^{(b_0,\ldots,b_{n-1})}$. If this operator has order n^2, proceed as above to find the dimension of the space of rational solutions. If the order is less than n^2, select another choice of $b_0, \ldots, b_{n-1}$. We know from Lemma 3.4 that some choice will work. It would be of interest to understand the probabilistic aspects of this approach.

3.2 Deciding if $\wedge^i V$ is 1-reductive

To decide if, for $1 \leq i \leq n-1$, $\wedge^i V$ is 1-reductive, we proceed in two steps. Firstly, we shall show how to find an operator $L^{\wedge i}$ whose solution space is G-isomorphic to $\wedge^i V$. Secondly, we shall produce an algorithm that, given a linear operator, decides if this operator is 1$-$reductive.

3.2.1 An operator whose solution space is $\wedge^i V$

We shall present two algorithms.

Algorithm 4: Let A be the $n \times n$ companion matrix of L. One can construct an $\binom{n}{i} \times \binom{n}{i}$ first order system whose solution space is $G-$isomorphic to $\wedge^i V$. This is done in [14] in the following way. Let $y_1, \ldots, y_n$ be indeterminates and let $Y = (y_1, \ldots, y_n)^T$. Let $\mathcal{S}_i$ be the set of all $i-$tuples $J = (j_1, \ldots, j_i), 1 \leq j_1 < \ldots < j_i \leq n$. For each $J \in \mathcal{S}_i$, let

$z_J = y_{j_1} \wedge \ldots \wedge y_{j_i}$. Formally differentiating, we have $z'_J = y'_{j_1} \wedge \ldots \wedge y_{j_i} + \ldots + y_{j_1} \wedge \ldots \wedge y'_{j_i}$. Using $Y' = AY$, we may rewrite each y'_j as a linear combination of the $y_i, \ldots, y_n$ and so have $z'_J = \sum_{H \in \mathcal{S}_i} c_{J,H} z_H$ for some constants $c_{J,H}$. Ordering the $i-$tuples in $\mathcal{S}_i$ in some manner, we have $Z' = A^{\wedge i} Z$ where $Z = (z_1, \ldots, z_{j_t}), t = \begin{pmatrix} n \\ i \end{pmatrix}$, and $A^{\wedge i} = (c_{J,H})$. We refer the reader to [14] for a proof that the solution space of this system is $G-$isomorphic to $\wedge^i V$. Construction of a cyclic vector (for the dual system) will yield an operator $L^{\wedge i}$ of order $\begin{pmatrix} n \\ i \end{pmatrix}$ whose solution space is $G-$isomorphic to $\wedge^i V$.

Algorithm 5: We now give an algorithm that avoids the conversion from scalar equation to matrix system and back. This relies on the following definitions and lemmas.

We first define the i^{th} *Associated Operator* L. Let K be the Picard-Vessiot extension of k associated to $L(y) = 0$ and let $y_1, \ldots, y_n$ be a fundamental set of solutions of $L(y) = 0$ in K. We define $L^{det(i)}$ to be the monic operator of smallest order whose solution set is spanned by $\{detWr(y_{j_1}, \ldots, y_{j_i}) \mid (j_1, \ldots, j_i) \in \mathcal{S}_i\}$. One sees that the vector space $V^{det(i)}$ spanned by these elements is left invariant under the action of the Galois group G and so this operator has coefficients in k. If V is the solution space of $L(y) = 0$, one sees that the map sending $y_{j_1} \wedge \ldots \wedge y_{j_i}$ to $detWr(y_{j_1}, \ldots, y_{j_i})$ is a G-homomorphism of $\wedge^i V$ onto $V^{det(i)}$. Therefore, the solution space of $L^{det(i)}$ is a homomorphic image of $\wedge^i V$ and is an isomorphic image if and only if the order of $L^{det(i)}$ is $\begin{pmatrix} n \\ i \end{pmatrix}$[1].

One can calculate $L^{det(i)}$ directly from L by setting $w = detWr(y_1, \ldots, y_i)$ differentiating this $\nu = \begin{pmatrix} n \\ i \end{pmatrix}$ times, using the relation $L(y_j) = 0$ to eliminate derivatives of y_j of order larger than $n-1$, and then finding a linear dependence among the resulting $\nu + 1$ expressions for $z, z', \ldots, z^{\nu}$. If there is more than one such dependence, one takes one where the maximum $z^{(j)}$ is as small as possible.

Example 3.7 Let $L = D^4$ and $i = 2$. If we use $y_i = x^i, i = 0, 1, 2, 3$ as a basis for the solution space, the set $\{detWr(y_{j_1}, \ldots, y_{j_i}) \mid (j_1, \ldots, j_i) \in \mathcal{S}_i\}$ is $\{1, 2x, 3x^2, x^2, 2x^3, x^4\}$. Therefore, $L^{det(2)} = D^5$, so the solution space of $L^{det(2)}$ is not $\wedge^2 V$, which has dimension 6.∎

[1] In [38], Section 167, Schlesinger also defines an associated operator. Schlesinger only defines this operator when the space $V^{det(i)}$ has dimension $\begin{pmatrix} n \\ i \end{pmatrix}$. In this case, our i^{th} associated operator would be called the $(n-i)^{te}$ associirte Differentialgleichung in his terminology.

Example 3.8 Let $L = D^4 - 4xD - (x^4+2)$. Calculating[2] one finds that

$$L^{det(2)} = D^6 - \frac{1}{x}D^5 + 4x^4D^2 + 20x^3D$$

Therefore in this case the solution space of $L^{det(2)}$ is $\wedge^2 V$. ∎

Since we want an operator whose solution space is $G-$isomorphic to $\wedge^i V$, we wish to guarantee that $L^{det(i)}$ has the correct order. This will be done with the aid of the following two lemmas. Again, we shall follow the philosophy that the tensor product of generic cyclic vectors is cyclic.

Let K be a differential field with constants $\mathcal{C}$ and $y_1, \ldots, y_n \in K$, linearly independent over $\mathcal{C}$. Let $B_0, \ldots, B_{n-1}$ be differential indeterminates and, for $i = 1, \ldots, n$, let $z_i = B_0 y_i + B_1 y_i' + \ldots + B_{n-1} y_i^{(n-1)}$. Note that the differential field $K < B_0, \ldots, B_{n-1} >$ has the same constants as K. For each $J = (j_1, \ldots, j_i) \in \mathcal{S}_i$ let $W_J = detWr(z_{j_1}, \ldots, z_{j_i}) \in K < B_0, \ldots, B_{n-1} >$.

Lemma 3.9 *For each $i, 1 \leq i \leq n$, $\{W_J \mid J \in \mathcal{S}_i\}$ forms a linear independent set over $\mathcal{C}$.*

Proof: The proof proceeds by induction on i. For $i = 1$ this is just a restatement of the fact that $y_1, \ldots, y_n$ are linearly independent over $\mathcal{C}$. Now assume that the statement is true for $i-1$. For each $J = (j_1, \ldots, j_i) \in \mathcal{S}_i$, we have that $W_J = \sum_{r=1}^{i} (-1)^{r+1} z_{j_r}^{(i-1)} W_{(j_1,\ldots,\widehat{j_r},\ldots,j_i)}$ (expand by minors using the last row). Note that the order of each $B_t, 0 \leq t \leq n-1$ in $W_{(j_1,\ldots,\widehat{j_r},\ldots,j_i)}$ is at most $i-2$. Furthermore, note that $z_{j_r}^{(i-1)} = B_0^{(i-1)} y_{j_r} + \ldots + B_{n-1}^{(i-1)} y_{j_r}^{(n-1)} + R(B_0, \ldots, B_{n-1}, y_{j_r})$ where R is a differential polynomial with rational coefficients and of order at most $i-2$ in each B_j. Therefore

$$W_J = \sum_{r=1}^{i} (-1)^{i-1} \sum_{t=0}^{n-1} B_t^{(i-1)} y_{j_r}^{(t)} W_{(j_1,\ldots,\widehat{j_r},\ldots,j_i)} + R_J$$

where R_J has order at most $i-2$ in each B_t. Now assume that $\sum_{J \in \mathcal{S}_i} c_J W_J = 0$ for some $C_J \in \mathcal{C}$. If we write $\sum_{J \in \mathcal{S}_i} c_J W_J$ as a polynomial in the $B_t^{(i-1)}, t = 0, \ldots, n-1$ we see that for each t the coefficient of $B_t^{(i-1)}$ is

$$\sum_{J=(j_1,\ldots,j_i) \in \mathcal{S}_i} c_J \sum_{r=1}^{i} (-1)^{i-1} y_{j_r}^{(t)} W_{(j_1,\ldots,\widehat{j_r},\ldots,j_i)}$$

and that this must equal 0. Rewriting this last expression, we get, for $t = 0, \ldots, n-1$

$$\sum_{j=1}^{n} y_j^{(t)} \sum_{J \in \mathcal{S}_i^j} \pm c_J W_{J|j} = 0$$

[2]In [2], Appell works out most of the relations for $L^{det(2)}$, when L is a fourth order operator

where $\mathcal{S}_i^j = \{J \in \mathcal{S}_i \mid i \text{ appears in } J\}$ and $J \mid j$ is the $(i-1)-$tuple obtained from J by deleting j. Since the matrix $(y_j^{(t)})_{j=1,\ldots,n}^{t=0,\ldots,n-1}$ is invertible, we have for each j, that

$$\sum_{J \in \mathcal{S}_i^j} \pm c_J W_{J|j} = 0$$

By induction, $\{W_{J|j} \mid J \in \mathcal{S}_i^j\}$ is a linearly independent set, so all $c_J = 0$. ∎.

Lemma 3.10 *Let $k = \mathcal{C}(x)$ and $L \in \mathcal{D}$. For each $i, 1 \leq i \leq n-1$, there exist polynomials $p_0, \ldots, p_{n-1}$ of degree at most $i + \begin{pmatrix} n \\ i \end{pmatrix} - 2$ such that the i^{th} associated operator of $L^{(p_0,\ldots,p_{n-1})}$ has order $\begin{pmatrix} n \\ i \end{pmatrix}$. Furthermore, one can select $p_0, \ldots, p_{n-1}$ of degree at most $max_{0 \leq i \leq n-1}\{i + \begin{pmatrix} n \\ i \end{pmatrix} - 2\}$ such that for all $i = 1, \ldots, n-1$, the order of the i^{th} associated operator of $L^{(p_0,\ldots,p_{n-1})}$ is $\begin{pmatrix} n \\ i \end{pmatrix}$.*

Proof: Fix i and let $\mathcal{W}_i$ be the determinant of the wronskian matrix of the $\{W_J \mid J \in \mathcal{S}_i\}$. By the previous lemma, we know that $\mathcal{W}_i$ is non-zero. This differential polynomial has order at most $i - 1 + \begin{pmatrix} n \\ i \end{pmatrix} - 1 = i + \begin{pmatrix} n \\ i \end{pmatrix} - 2$ in the variables $P_0, \ldots, P_{n-1}$. Therefore, the result of Ritt ([37], p.35) implies that there exist polynomials $p_0, \ldots, p_{n-1}$ of degree at most $i + \begin{pmatrix} n \\ i \end{pmatrix} - 2$ such that $\mathcal{W}_i(p_0, \ldots, p_{n-1}) \neq 0$. This guarantees that the order of $L^{det(i)}$ is $\begin{pmatrix} n \\ i \end{pmatrix}$. Setting $\mathcal{W} = \prod_{i=1}^{n-1} \mathcal{W}_i$, the result of Ritt implies that there are polynomials $p_0, \ldots, p_{n-1}$ of degree at most $max_{2 \leq i \leq n-1}\{i + \begin{pmatrix} n \\ i \end{pmatrix} - 2\}$ such that $\mathcal{W}(p_0, \ldots, p_{n-1}) \neq 0$. This gives the final result. ∎

We can now state the algorithm. Let $\tilde{P}_0, \ldots, \tilde{P}_{n-1}$ be polynomials of degree $i + \begin{pmatrix} n \\ i \end{pmatrix} - 2$ with indeterminates for coefficients. The condition that $(L^{(\tilde{P}_0,\ldots,\tilde{P}_{n-1})})^i$ have order $\begin{pmatrix} n \\ i \end{pmatrix}$ defines a non-empty Zariski open set of constants whose defining equations can be found. Furthermore one can find a point in this set. Using this as coefficients in the $\tilde{P}_0, \ldots, \tilde{P}_{n-1}$, we can get polynomials $p_0, \ldots, p_{n-1}$ such that $(L^{(p_0,\ldots,p_{n-1})})^{det(i)}$ has order $\begin{pmatrix} n \\ i \end{pmatrix}$.

In practice, we keep selecting arbitrary $p_0, \ldots, p_{n-1}$ and form $(L^{(p_0,\ldots,p_{n-1})})^{det(i)}$ until we find one of the prescribed order.

Example 3.11 Let $L = D^4$. We have seen that $L^{det(2)}$ has order 5. When we consider $L^{(1,x^2,0,0)}$ we get $L^{(1,x^2,0,0)} =$

$$D^4 - \frac{(72\,x^2 + 12 + 72\,x)}{36\,x^2 + 24\,x^3 + 1 + 12\,x} D^3 + \frac{(72 + 144\,x)}{36\,x^2 + 24\,x^3 + 1 + 12\,x} D^2 - \frac{144}{36\,x^2 + 24\,x^3 + 1 + 12\,x} D$$

and that $(L^{(1,x^2,0,0)})^{det(2)} =$

$$D^6 + \frac{\left(145152\,x^8 + 580608\,x^7 + 852768\,x^6 + 544752\,x^5 + 125064\,x^4 - 13392\,x^3 - 10332\,x^2 - 1440\,x - 54\right)}{12096\,x^9 + 54432\,x^8 + 94176\,x^7 + 77544\,x^6 + 30024\,x^5 + 3852\,x^4 - 756\,x^3 - 288\,x^2 - 30\,x - 1} D^5$$

$$+ \frac{\left(6967296\,x^{10} + 34836480\,x^9 + 68117760\,x^8 + 64696320\,x^7 + 28615680\,x^6 + 1990656\,x^5 - 3363120\,x^4 - 1438560\,x^3 - 252720\,x^2 - 19800\,x - 504\right)}{290304\,x^{12} + 1741824\,x^{11} + 4364928\,x^{10} + 5916672\,x^9 + 4696704\,x^8 + 2198016\,x^7 + 558360\,x^6 + 42120\,x^5 - 16308\,x^4 - 5316\,x^3 - 684\,x^2 - 42\,x - 1} D^4$$

$$- \frac{\left(15178752\,x^5 + 6967296\,x^9 - 1052352\,x^3 + 53747712\,x^7 + 684288\,x^4 + 43047936\,x^6 - 28512\,x + 31352832\,x^8 - 792 - 292896\,x^2\right)}{290304\,x^{12} + 1741824\,x^{11} + 4364928\,x^{10} + 5916672\,x^9 + 4696704\,x^8 + 2198016\,x^7 + 558360\,x^6 + 42120\,x^5 - 16308\,x^4 - 5316\,x^3 - 684\,x^2 - 42\,x - 1} D^3$$

$$+ \frac{\left(15552\,x^2 + 2592 + 15552\,x\right)\left(336\,x^4 + 672\,x^3 + 288\,x^2 + 32\,x + 1\right)}{290304\,x^{12} + 1741824\,x^{11} + 4364928\,x^{10} + 5916672\,x^9 + 4696704\,x^8 + 2198016\,x^7 + 558360\,x^6 + 42120\,x^5 - 16308\,x^4 - 5316\,x^3 - 684\,x^2 - 42\,x - 1} D^2$$

$$- \frac{(15552 + 31104\,x)\left(336\,x^4 + 672\,x^3 + 288\,x^2 + 32\,x + 1\right)}{290304\,x^{12} + 1741824\,x^{11} + 4364928\,x^{10} + 5916672\,x^9 + 4696704\,x^8 + 2198016\,x^7 + 558360\,x^6 + 42120\,x^5 - 16308\,x^4 - 5316\,x^3 - 684\,x^2 - 42\,x - 1} D$$

$$+ \frac{10450944\,x^4 + 20901888\,x^3 + 8957952\,x^2 + 995328\,x + 31104}{290304\,x^{12} + 1741824\,x^{11} + 4364928\,x^{10} + 5916672\,x^9 + 4696704\,x^8 + 2198016\,x^7 + 558360\,x^6 + 42120\,x^5 - 16308\,x^4 - 5316\,x^3 - 684\,x^2 - 42\,x - 1}$$

∎

3.2.2 Deciding if an operator is 1-reductive

We will show that the algorithm **1-reductive**, below, decides if an operator L is $1-$reductive. We shall asume that our differential field k (with algebraically closed constants) comes equiped with two ancillary algorithms. The first is an algorithm to decide if, given a differential operator $L \in \mathcal{D}, L(y) = 0$ has a nonzero solution in k and, if so, produces such a solution. The second is an algorithm to decide if, given a differential operator $L \in \mathcal{D}, L(y) = 0$ has a solution y such that $y'/y = u \in k$, and, if such a solution exists, produces such an element $u \in k$. This is equivalent to deciding if the associated Riccati equation has a solution u in k and is also equivalent to deciding if L has a first order right factor of the form $D - u$ for some $u \in k$. As we have already noted, such algorithms exist for $\overline{\mathbb{Q}}(x)$, as well as for any finite purely transcendental liouvillian extension of $\overline{\mathbb{Q}}(x)$ or for any elementary extension of $\overline{\mathbb{Q}}(x)$. In the following, if $L_1, L_2 \in \mathcal{D}$, $Quotient(L_1, L_2)$ will denote the unique operator $A \in \mathcal{D}$ such that $L_1 = AL_2 + B$ for some $B \in \mathcal{D}$ with $ord(R) < ord(L_1)$ and L_1^* will denote the adjoint of L_1.

Recall that an operator R is $1-$reductive if, for any first order right factor S of R there exists an $\tilde{S}$, relatively prime to S, such that $R = [S, \tilde{S}]_l$. We first will present an effective criterion (Lemma 3.12) to decide if, given such an S, whether or not an $\tilde{S}$ as above exisits. We will then show that one does not need to check this *for all* right factors S (a possibly infinite set) and that it is enought to check this for a suitably defined sequence of pairs of operators (R_i, S_i), where S_i has order 1 and is a right divisor of R_i. In the following lemma, we have occasion to take an operator L and an element $h \in k$ and form the new operator $e^{\int h} \circ L \circ e^{-\int h}$. Note that is nothing more that the operator gotten from L by replacing D by $D - h$.

Lemma 3.12 *Let $S, R \in \mathcal{D}$, $S = D - h, R \neq 0$ and assume that S is a right divisor of R. The following are equivalent:*

1. *There exists an $\tilde{S} \in \mathcal{D}$, relatively prime to S, such that $R = [S, \tilde{S}]_l$.*
2. *There exists an $\overline{R}_0 \in \mathcal{E}_{\mathcal{D}}(S, R) \neq 0$ such that S does not divide R_0 on the right.*
3. *For $T := e^{\int h} \circ R^* \circ e^{-\int h}$, $T(y) = 0$ has a nonzero solution $g \in k$, such that for $R_0 =$ (Quotient$(R^*, -g^{-1}D + g^{-2}g' - g^{-1}h))^*$, S does not divide R_0 on the right.*

Proof: Let K be the Picard-Vessiot extension of k corresponding to R and let G be its Galois group. Assume that 1. is true. We then have that $Soln_K(R) = Soln_K(S) \oplus Soln_K(\tilde{S})$ as $G-$modules. Let ϕ be the projection of $Soln_K(R)$ onto $Soln_K(S)$. Using the correspondence given in Lemma 2.5, this implies that there exists an $\overline{R}_0 \in \mathcal{E}_{\mathcal{D}}(S, R)$ such that $R_0(y) = y$ for all $y \in Soln_K(S) \subset Soln_K(R)$. In particular S does not divide R_0 on the right, so 2. holds.

Now assume, that 2. holds. Using the correspondence given in Lemma 2.5, $\overline{R}_0$ corresponds to a homomorphism $\phi \in Hom_G(Soln_K(R), Soln_K(S))$. Since S does not divide R_0 on the right, ϕ induces an isomorphism on $Soln_K(S)$. Therefore, we may write $Soln_K(R) = Soln_K(S) \oplus Ker(\phi)$. Since $Ker(\phi)$ is a $G-$submodule of $Soln_K(R)$, there exists an operator $\tilde{S}$ such that $Soln_K(\tilde{S}) = Ker(\phi)$. Therefore, 1. holds.

Assume that 2. is true and let $\overline{R}_0 \in \mathcal{E}_{\mathcal{D}}(S, R)$ with $R_0 \neq 0$ and $ord(R_0) < ord(R)$. We then have that $SR_0 = AR$ for some $A \in \mathcal{D}$. Comparing orders, we see that $ord(A) = 0$ so $A = g \in k, g \neq 0$. Taking adjoints of both sides of the equation $R = g^{-1}SR_0$ we have

$$\begin{aligned} R^* &= R_0^* S^* g^{-1} \\ &= R_0^*(-D - h)g^{-1} \\ &= R_0^*(-g^{-1}D + g^{-2}g' - g^{-1}h) \\ &= R_0^*(-g^{-1})(D - g^{-1}g' + h) \end{aligned}$$

Therefore $y = ge^{-\int h}$ is a solution of $R^*(y) = 0$ and so g is a solution of T. Furthermore, $R_0^* = Quotient(R^*, -g^{-1}D + g^{-2}g' - g^{-1}h)$ so $R_0 = (Quotient(R^*, -g^{-1}D + g^{-2}g' - g^{-1}h))^*$ and 3. holds.

Now assume that T has a non-zero solution $g \in k$. This implies that $y = ge^{-\int h}$ is a solution of $R^*(y) = 0$. Therefore, for some $\tilde{R} \in \mathcal{D}$, we have

$$\begin{aligned} R^* &= \tilde{R}(D - g^{-1}g' + h) \\ &= \tilde{R}(-g)(-g^{-1}D + g^{-2}g' - g^{-1}h) \\ &= R_0^*(-g^{-1}D + g^{-2}g' - g^{-1}h) \end{aligned}$$

where $R_0 = (\tilde{R}(-g))^*$. Therefore, $R = (-g^{-1}D + g^{-2}g' - g^{-1}h)^* R_0 = g^{-1}(D - h)R_0$. Rewritting this as $gR = (D - h)R_0$, we see $R_0 \in \mathcal{E}_{\mathcal{D}}(S, R)$. Therefore, 3. holds. ∎

We now show that the problem of deciding if an operator is $1-$ reductive can be reduced to applying the above criterion to a suitably defined sequence of pairs of operators. We will need the following definition. Let $L \in \mathcal{D}$ and $m > 1$. A *test set $\mathcal{T}_m$ of length m for L* is a set of two sequences $\{(R_1, \ldots, R_m), (S_1, \ldots, S_{m-1})\}$ of nonzero operators $R_i, S_i \in \mathcal{D}$ such that

1. $R_1 = L$,
2. $ord(S_i) = 1$ and S_i divides R_i on the right for $i = 1, \ldots, m-1$.
3. $ord(R_{i+1}) < ord(R_i)$, $\overline{R}_{i+1} \in \mathcal{E}_{\mathcal{D}}(S_i, R_i)$ and S_i does not divide R_{i+1} on the right for $i = 1, \ldots, m-1$.

The only test set of length 1 for L is the set $\{R_1 = L\}$. Note that the conditions $R_1 = L$ and $ord(R_{i+1}) < ord(R_i)$ imply that any test set for L has length at most $ord(L)$. We say that a test set $\mathcal{T}_{\tilde{m}} = \{(\tilde{R}_1, \ldots, \tilde{R}_{\tilde{m}}), (\tilde{S}_1, \ldots, \tilde{S}_{\tilde{m}-1})\}$ *extends* a test set $\mathcal{T}_m = \{(R_1, \ldots, R_m), (S_1, \ldots, S_{m-1})\}$ if $\tilde{m} \geq m$, $\tilde{R}_i = R_i$ for $i = 1, \ldots, m$ and $\tilde{S}_i = S_i$ for $i = 1, \ldots, m-1$.

Lemma 3.13 *Let $L \in \mathcal{D}$ and let K be the Picard-Vessiot extension of k corresponding to $L(y) = 0$. Let $\mathcal{T}_m$ be a test set of length m for L. Then for $i = 2, \ldots, m$, $R_i(y) = 0$ and $S_i(y) = 0$ have complete sets of solutions in K and*

$$Soln_K(L) = Soln_K(R_i) \oplus Soln_K(S_{i-1}) \oplus \ldots \oplus Soln_K(S_1)$$

Proof: Note that $Soln_K(L) = Soln_K(R_1)$ so to prove the lemma it is enough to show that $Soln_K(R_i) = Soln_K(R_{i+1}) \oplus Soln_K(S_i)$ (Lemma 2.1 will yield the statement concerning complete sets of solutions). Since $\overline{R}_{i+1} \in \mathcal{E}_{\mathcal{D}}(S_i, R_i)$ we have $S_i R_{i+1} = T R_i$ for some $T \in \mathcal{D}$. Comparing orders, we see that $ord(T) = 0$. Therefore R_{i+1} maps solutions of R_i onto the solution space of S_i. The solution space of R_{i+1} is the kernel of this map. Furthermore, the condition that S_i does not divide R_{i+1} on the right insures that $Soln_K(R_{i+1}) \cap Soln_K(S_i) = (0)$ so $Soln_K(R_i) = Soln_K(R_{i+1}) \oplus Soln_K(S_i)$. ∎

Lemma 3.14 *Let $L \in \mathcal{D}$. The following are equivalent:*

1. *L is $1-$reductive.*

2. *For any m, if $\mathcal{T}_m = \{(R_1, \ldots, R_m), (S_1, \ldots, S_{m-1})\}$ is a test set for L of length m then either*

   (a) *for any first order right factor S_m of R_m there exists an $R_{m+1} \in \mathcal{D}$ such that $\mathcal{T}_{m+1} = \{(R_1, \ldots, R_m, R_{m+1}), (S_1, \ldots, S_{m-1}, S_m)\}$ is a test set, or*

   (b) *R_m has no first order right factor in $\mathcal{D}$*

3. *For some $m \leq n$, there is a test set $\mathcal{T}_m$ for L of length m such that R_m has no first order right factor in $\mathcal{D}$.*

Proof: Let G be the Galois group of L. Assuming 1. holds we wish to show that 2. holds. Let $\mathcal{T}_m$ be a test set for L of length m. If R_m has no first order right factor, we are done. Let S_m be a first order right factor. Lemma 3.13, R_m has a full set of solutions in K and $Soln_K(R_m) \subset Soln_K(L)$. By Lemma 2.1.3, S_m will also have a full set of solutions in K and $Soln_K(S_m) \subset Soln_K(R_m) \subset Soln_K(L)$. Since L is $1-$reductive, we may write $Soln_K(L) = Soln_K(S_m) \oplus W$ for some G-module W. We then have $Soln_K(R_m) = Soln_K(S_m) \oplus (W \cap Soln_K(R_m))$. Let π be the projection of $Soln_K(R_m)$ onto $Soln_K(S_m)$ with kernel $(W \cap Soln_K(R_m))$. We have that π is a nonzero element of $Hom_G(Soln_K(R_m), Soln_K(S_m))$ and so, by Lemma 2.5, corresponds to a nonzero element $\overline{R}_{m+1}$ of $\mathcal{E}_{\mathcal{D}}(S_m, R_m)$. We can select R_{m+1} so that $ord(R_{m+1}) < ord(R_m)$ and any such R_{m+1} has no solutions in common with S_m, (otherwise it would not induce a projection onto this solution space). Therefore we have that S_m does not divide R_{m+1} on the right and this gives an extension of $\mathcal{T}$ to a larger test set. Therefore 2. holds.

Assume that 2. holds. By convention $\{L\}$ is a test set. Let $\mathcal{T}_m$ be a maximal test set (with respect to extension). By 2. we have that R_m has no first order right factor. Therefore 3. holds.

Assume that 3. holds. Lemma 3.13 allows us to write $Soln_K(L) = Soln_K(R_m) \oplus Soln_K(S_{m-1}) \oplus \ldots \oplus Soln_K(S_1)$. Since R_m has no first order right factor, $Soln_K(R_m)$ has no one dimensional $G-$submodules. Therefore any one dimensional $G-$submodule of $Soln_K(L)$ lies in $Soln_K(S_{m-1}) \oplus \ldots \oplus Soln_K(S_1)$. This implies that this latter space is the sum of all one dimensional $G-$submodules of $Soln_K(L)$. Since it clearly has a complementary submodule, Lemma 2.16 implies that L is $1-$reductive so 1. holds. ∎

Algorithm $1-$reductive uses Lemma 3.12 to generate a test set and decide if condition 3. of the above lemma holds. We shall state this algorithm, give three examples and then prove its correctness.

Algorithm 1-reductive

Input: A non-zero $L \in \mathcal{D}$
Output: *'true'* if L is $1-$reductive; *'false'* if L is not $1-$reductive

Status:= true;
$R := L$;
While R has a first order right factor and *Status*= $1-$reductive **do**
  h:= a solution in k of the Riccati equation associated to R;
  T:= $e^{\int h} \circ R^* \circ e^{\int -h}$;
    If $T(y) = 0$ has a non-zero solution in k **then**
      $g_1, \ldots, g_t :=$ a basis of the space of solutions in k of $T(y) = 0$;
      $g := c_1 g_1 + \ldots + c_t g_t$ for new variables $c_1, \ldots, c_t$;
      $\tilde{R}(c_1, \ldots, c_t)$:= $(Quotient(R^*, -g^{-1}D + g^{-2}g' - hg^{-1}))^*$;
        If there exist constants $d_1, \ldots, d_t$ such that
          $D - h$ does not divide $\tilde{R}(d_1, \ldots, d_t)$ on the right **then**
          $R := \tilde{R}(d_1, \ldots, d_t)$;
        else *Status*:= false;
    else *Status*:= false;
od;
return(*Status*);
end;

In the above algorithm, the phrase $Quotient(R^*, -g^{-1}D + g^{-2}g' - hg^{-1})$ denotes the right quotient in the ring $k(c_1, \ldots, c_t)[D]$ where each $c_i' = 0$. Also note that if $L \in \mathcal{D}$ where $L = p(D)$ for some polynomial $p(D) \in k[D]$, then $e^{\int h} \circ L \circ e^{\int -h} = p(D - h)$. This implies that the operator T defined in the algorithm has coefficients in k and also gives an efficient way of calculating T. We finally note that the algorithm could be modified so that the **While** loop is exited when the order of R is at most 1. To see this note that if $R = D - h$ (the case where R is not monic is similar, but notationally more complex and is left to the reader), then $T := D, g := c_1$, and $\tilde{R} := c_1$. Therefore c_1 can always be chosen so that $D - h$ does not divide $\tilde{R}(d_1, \ldots, d_t)$ on the right and one updates $R := 1$. Therefore the algorithm will end with *Status* = *true*.

Example 3.15 Let $k = \mathbb{C}$ and $L = D^2$. We begin by setting $R = D^2$. Clearly R has a right factor D, so we set $h := 0$ and $T := R^* = D^2$. The equation $T(y) = 0$ has a nonzero solution $y = 1$ in k and this forms a basis for all solutions in k. We set $g := c_1$ and $\tilde{R}(c_1) = Quotient(D^2, -c_1^{-1}D) = c_1 D$. For all values d_1 of c_1 we have that D divides

($\tilde{R}(d_1) = d_1 D$ so the above equation is not 1−reductive. Note that the Galois group of L is $G = \{\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbb{C}\}$. ∎

Example 3.16 Let $k = \mathbb{C}(x)$ and again let $L = D^2$. We again have that $R := D^2$ has a right factor D. Let $h := 0$ and $T := R^* = D^2$. The equation $T(y) = 0$ is now satisfied by 1 and x and these two elements form a basis for the solution space of $T(y) = 0$ in k. Let $g = c_1 \cdot 1 + c_2 \cdot x$ and let $c_1 = 0, c_2 = 1$. We then have that $(Quotient(D^2, -\frac{1}{x}D + \frac{1}{x}))^* = xD - 1$ and D does not divide $xD - 1$ on the right. Therefore we update $R := xD - 1$. This has a first order factor and we set $h := \frac{1}{x}$. We then have $T := xD + 1$ and $\frac{-1}{x}$ forms a basis for the solution space of $T(y) = 0$ in k. Setting $g := c_1 \frac{-1}{x}$ we get $\tilde{R} := c_1$, so setting $c_1 = 1$ allows us to update $R := 1$. Since this has no first order right factor, we exit the algorithm and conclude that the original operator is 1−reductive. As we have already noted, we could have concluded this when we reached the stage that R had order 1. Also note that the Galois group is trivial. ∎

Example 3.17 Let $k = \mathbb{C}(x)$. The equation $L^{det(2)} = D^6 - \frac{1}{x}D^5 + 4x^4D^2 + 20x^3D$ was constructed in Example 3.8. We shall consider the equation gotten by clearing denominators. We begin by setting $R = xL^{det(2)} = xD^6 - D^5 + 4x^5D^2 + 20x^4D = (xD^5 - D^4 + 4x^5D + 20x^4)D$ so R clearly has a right first order factor D. We set $h := 0$ and $T := R^* = xD^6 + 7D^5 + 4x^5D^2 + 20x^4D$. The equation $T(y) = 0$ has a nonzero solution $y = 1$ in k, and this is a basis of the space of all solutions in k. Set $g := c_1$ and redefine $\tilde{R}(c_1) :=$ Quotient$(xD^6 + 7D^5 + 4x^5D^2 + 20x^4D, -c_1^{-1}D)^* = c_1(-xD^5 - 7D^4 - 4x^5D - 20x^4)^* = c_1(xD^5 - 2D^4 + 4x^5D)$. For all values d_1 of c_1 we have that D divides $\tilde{R}(d_1)$ on the right.Therefore *Status* changes to 'false'.

This furthermore, implies that $L^{det(2)}$ is not 1−reductive. As we have noted, $L^{det(2)}$ is an operator whose solution space is $\wedge^2 V$ where V is the solution space of $L = D^4 - 4xD - (x^4 + 2)$. Therefore, Corollary 2.21 implies that this latter operator is not completely reducible and, in particular, factors. One can easily show that it has no first or third order right factors (for the latter look at the adjoint), so this operator factors as the product of two second order operators. ∎

Proof of correctness of Algorithm 1−Reductive: We shall show that the algorithm generates a maximal test set $\mathcal{T}_m$ and terminates with 'true' if R_m has no first order right factor or 'false' if R_m has a first order right factor. Lemma 3.14 implies that the algorithm is correct.

Initially the algorithm sets $R := L$. Assume, inductively, that at the beginning of the i^{th} pass through the **While** statement, we have generated a test set $\mathcal{T}_i = \{(R_1, \ldots, R_i), (S_1, \ldots, S_{i-1})\}$ with $R := R_i$. We shall show that the algorithm either extends this test set or concludes that it is maximal, in which case it halts with the correct output. Since there is an upper bound on the length of test sets, this will also show that the algorithm terminates.

If R has no first order right factor then the test set is maximal and the algorithm will terminate with *Status* = true, which is the correct output by Lemma 3.14.3. Assume that R has a first order right factor. The algorithm will find a $h \in k$ such that $S_i = D - h$ is a right factor of R. The algorithm then determines if $T(y) = 0$ has a nonzero solution in k. If it does, Lemma 3.12.3 implies that the algorithm finds a nonzero R_{i+1} with $\overline{R}_{i+1} \in \mathcal{E}_{\mathcal{D}}(S, R)$ and updates the value of $R := R_{i+1}$. The algorithm therefore has generated a test set $\mathcal{T}_{i+1} = \{(R_1, \ldots, R_i, R_{i+1}), (S_1, \ldots, S_{i-1}, S_i)\}$ extending $\mathcal{T}_i$ and does not change *Status*. If the only solution of $T(y) = 0$ in k is $y = 0$, then Lemma 3.12.3 implies that $\mathcal{E}_{\mathcal{D}}(S_i, R_i) = (0)$. Therefore, R_i has a first order right factor but $\mathcal{T}_i$ cannot be extended. Lemma 3.14 implies that L is not $1-$reductive. In this case the algorithm changes *Status*:= 'false' and halts with the correct output. ∎

3.3 Remarks

1. In [43], the authors show how various properties of the Galois group of a linear differential equation $L(y) = 0$ can be determined by determining factorization properties of auxillary operators. The above methods can be used to do this. In many instances, one does not need to apply the full irreducibility test, but in fact can just use the criterion for completely reducible operators (Corollary 2.15).

Let us consider the result mentioned in the introduction: *Let k be a differential field with algebraic closed field of constants and let $L \in \mathcal{D}$ be a second order operator. The equation $L(y) = 0$ has non-zero liouvillian solutions over k if and only if $L^{\circledS 6}$ is reducible in $\mathcal{D}$.* If one knows that L is irreducible, then the Galois group G must be a reductive group. The solution space of $L^{\circledS 6}$ is a $G-$module and so will be completely reducible. Therefore, $L^{\circledS 6}$ will be a completely reducible operator (Lemma 2.13). Furthermore, it is reducible if and only if $\dim_{\mathcal{C}} \mathcal{E}_{\mathcal{D}}(L^{\circledS 6}) > 1$. Let L_1 be an operator (of order 49) whose solution space is $G-$isomorphic to $Hom_G(Soln_K(L^{\circledS 6}), Soln_K(L^{\circledS 6}))$, where K is the Picard-Vessiot extension corresponding to L. We can therefore restate the above theorem as:

Theorem 3.18 *Let $k, L,$ and L_1 be as above. The equation $L(y) = 0$ has non-zero liouvillian solutions over k if and only if*

- *The equation $L(y) = 0$ has a solution $y \neq 0$ such that $y'/y \in k$, or*
- *The equation $L_1(y) = 0$ has two solutions in k linearly independent over the constants.*

Proof: The operator L is reducible if and only if the equation $L(y) = 0$ has a solution $y \neq 0$ such that $y'/y \in k$, in which case, $L(y) = 0$ has a liouvillian solution. If the operator L is irreducible, then the discussion preceeding this Theorem shows that the equation $L(y) = 0$ has non-zero liouvillian solutions over k if and only if $L_1(y) = 0$ has two solutions in k linearly independent over the constants. ∎

Simillar results can be stated for third order operators using the results of [43]. In general, once one knows that an operator L is irreducible (or, at worst, completely reducible), any operator that one constructs from L will be completely reducible and so special methods for testing reduciblity can be used.

2. One of the goals of this paper was to develop reducibility tests that, starting with a linear differential operator, do not resort to systems and cyclic vector techniques to make a determination. To do this, we replaced the original operator L with an operator of the form $L^{(b_0,\ldots,b_{n-1})}$ before constructing $L^* \circledS L$. In reality, this construction allows one to go directly from a cyclic vector for L to a cyclic vector for the system $\mathcal{A}_L(Y)$ in section 3.1. Algorithms $1, 2$ and 4 require one to construct a cyclic vector for a system. The reason for having to find a cyclic vector (or companion block diagonal form) in Algorithms 1, 2, and 4 is that we know of no direct method of finding the dimension of the space of solutions of a system $Y' = AY$ in k^n, even when $k = \mathcal{C}(x)$. Is there a direct method for determining the dimension of this space of solutions? Given a single linear differential equation, is there a method to find the dimension of the space of solutions in k *without* having to find the solutions?

References

[1] Amitsur, A. S., *Differential polynomials and division algebras*, Ann. of Math., **59**, (1954), 245-278.

[2] Appell, P., *Mémoire sur les Équations Différentielles Linéaires*, Ann. Scient. Éc. Norm. Sup., Ser. 2, **10**, (1881), 391-424.

[3] Barkatou, M.A., *An algorithm for computing a companion diagonal form for a system of linear differential equations*, AAECC, **4**, (1993), 185-195.

[4] Beke, E., *Die Irreducibilität der homogenen linearen Differentialgleichungen*, Math. Ann., **45**, (1894), 278-294.

[5] Bertrand, D., Beukers, F., *Équations Différentielles Linéaires et Majorations de Multiplicités*, Ann. Scient. Éc. Norm. Sup., **18**, (1985), 181-192.

[6] Björk, J.-E., **Rings of Differential Operators**, North Holland, New York, 1979.

[7] Borel, A., *Linear algebraic groups* In Proc. Symp. Pure Math., **9**, 3-19. Amer. Math. Soc., Providence, 1966.

[8] Bronstein, M., *On solutions of linear ordinary differential equations in their coefficient field*, J. Symb. Comp., **13**, (1992), 413-439.

[9] Cohn, P., **Free Rings and their Relations**, Academic Press, London, 1985.

[10] Deligne, P., **Equations Différentielles à Points Singuliers Réguliers**, Lecture Notes in Mathematics, **163** Springer-Verlag, New York, 1970.

[11] Frobenius, G. *Über den Begriff der Irreducibilität in der Theorie der linearen Differentialgleichungen*, J. für Math., **76** 236-271, 1873.

[12] Giesbrecht, M., *Factoring in skew-polynomial rings*, Department of Computer Science, University of Toronto, preprint, 1992.

[13] Grigoriev, D. Yu., *Complexity of factoring and calculating the GCD of linear ordinary differential operators*, J. Symbolic Computation (1990), **10**, 7-37.

[14] Grigoriev, D. Yu., *Complexity of irreducibility testing for a system of linear ordinary differential equations*, Proc. Int. Symp. on Symb. Alg. Comp., ACM Press (1990) 225-230.

[15] Hilb, E., *Lineare Differentialgleichungen im Komplexen Gebiet*, in **Encyklopedie der mathematischen Wissenschaften**, IIBb, , Teubner, Leipzig, 1915.

[16] Humphreys, J., **Linear Algebraic Groups**, Graduate Texts in Mathematics, **21**, Springer-Verlag, 1975.

[17] Hungerford, T., **Algebra**, Graduate Texts in Mathematics, **73**, Springer-Verlag, New York, 1974.

[18] Jacobson, N., *Pseudo-linear transformations*, Ann. of Math., **38**, (1937), 484-507.

[19] Jacobson, N., **Structure of Rings**, American Mathematical Society Colloquium Publications, XXXVII, Second Edition, Providence, 1964

[20] Jordan, C., *Sur une application de la théorie des substitutions à l'étude des équations différentielles linéaires*, Bull. Soc. Math. France II, **100**, 1875.

[21] Kaplansky, I., **Introduction to Differential Algebra**, Paris: Hermann 1957.

[22] Landau, E., *Ein Satz über die Zerlegung homogener linearer Differentialausdrücke in irreducible Factoren*, J. Für Math., **24**, (1902), 115-120.

[23] Lang, S., **Algebra**, Second Edition, Addison-Wesley, 1984.

[24] Loewy, A., *Über reduzible lineare homogene Differentialgleichungen*, Math. Ann., **56**, (1903), 549 -584.

[25] Loewy, A., *Über vollständig reduzible lineare homogene Differentialgleichungen*, Math. Ann., **62**, (1906), 89-117.

[26] Loewy, A., *Über lineare homogene Differentialgleichungen derselben Art*, Math. Ann., **70**, (1911), 551-560.

[27] Loewy, A., *Zur Theorie der linearen homogenen Differentialausdrücke*, Math. Ann., **72**, (1912), 203-210.

[28] Loewy, A., *Über die Zerlegungen eines linearen homogenen Differentialausdruckes in grösste volständig reduzible Faktoren*, Sitz. der Heidelberger Akad. der Wiss., **8**, (1917), 1-20.

[29] Loewy, A., *Über Matrizen- und Differentailkomplexe*, Math Ann., **78**, (1917), I: 1-51; II: 343-358; III: 359-368.

[30] Loewy, A., *Begleitmatrizen und lineare homogene Differentialausdrücke*, Math. Zeit., **7**, (1920), 58-125.

[31] MacDonald, B., **Finite Rings with Identity**, Marcel Dekker, New York, 1974.

[32] Mignotte, M., **Mathematics for Computer Algebra**, Springer-Verlag, New York, 1992

[33] Ore,O., *Formale Theorie der linearen Differentialgleichungen*, J. für Math., **167**, (1932), 221-234, II, *ibid.*, **168**, (1932), 233-252.

[34] Ore, O, *Theory of non-commutative polynomial rings*, Ann. of Math., **34**, (1933), 480-508.

[35] Poole, E.G.C., **Introducion to the Theory of Linear Differential Equations**, Dover Publications, New York, 1960.

[36] Poincaré, H., *Mémoire sur les fonctions Zétafuchsiennes*, Acta Math., **5**, (1884), 209-278.

[37] Ritt, J.F., **Differential Algebra**, Dover Publications, New York, 1966.

[38] Schlesinger, L., **Handbuch für Theorie der linearen Differentialgleichungen II**, Leipzig: Teubner, (1887).

[39] Schwarz, F., *A factorization algorithm for linear ordinary differential equations*, Proc. of the ACM-SIGSAM 1989 ISSAC, ACM Press, (1989), 17-25.

[40] Singer, M.F., *Algebraic solutions of n^{th} order linear differential equations*, Proceedings of the 1979 Queens Conference on Number Theory, Queens Papers in Pure and Applied Mathematics **54**, (1980).

[41] Singer, M.F., *Liouvillian solutions of linear differential equations with liouvillian coefficients*, J. Symb. Comp., **11**, (1991), 251-273.

[42] Singer, M.F., *Moduli of linear differential equations on the Riemann Sphere with fixed Galois groups*, Pacific Journal of Math., **160**, No. 2, (1993), 343-395.

[43] Singer, M.F., Ulmer, F., *Galois groups of second and third order linear differential equations*, J. Symb. Comp., **16**, July 1993, 9 - 36.

[44] van der Waerden, B.L., **Modern Algebra**, Vol. I, Second Edition, Frederick Ungar, New York, 1953.