J. Symbolic Computation (1993) **16**, 9–36

Galois Groups of Second and Third Order Linear Differential Equations

MICHAEL F. SINGER[†] and FELIX ULMER[‡]

North Carolina State University, Department of Mathematics, Box 8205

Raleigh, N.C. 27695-8205

(Received 29 April 1992)

Using the representation theory of groups, we are able to give simple necessary and sufficient conditions regarding the structure of the Galois groups of second and third order linear differential equations. These allow us to give simple necessary and sufficient conditions for a second order linear differential equation to have liouvillian solutions and for a third order linear differential equation to have liouvillian solutions or be solvable in terms of second order equations. In many cases these conditions also allow us to determine the group.

1. Introduction

Let k be a differential field[††] with algebraically closed field of constants C and $L(y) = 0$ a linear differential equation[‡‡] with coefficients in this field. One can form the m^{th} symmetric power $L^{\circledS m}(y)$ of $L(y)$ which is the smallest order nonzero linear differential equation satisfied by the m^{th} power of any solution of $L(y) = 0$. In this paper we show how factorization properties of these symmetric powers can be used to determine structural properties of the Galois groups of second and third order linear differential equation. This in turn will allow us to give necessary and sufficient conditions for these linear differential equations to have liouvillian solutions. For example we show (Corollary 4.4):

Let $L(y) = y'' + ry = 0$ be a second order linear differential equation with $r \in k$. $L(y) = 0$ has liouvillian solutions if and only if $L^{\circledS 6}(y)$ is reducible.

For third order equations we have similar conditions and are also able to characterize those equations that are solvable in terms of lower order equations (Corollary 4.8):

† Partially supported by NSF Grant 90-24624

‡ Partially supported by Deutsche Forschungsgemeinschaft, while on leave from Universität Karlsruhe. The second author would like to thank North Carolina State University for its hospitality and partial support during the preparation of this paper.

†† of characteristic zero as are all the fields in this paper.

‡‡ All linear differential equations in this paper are homogeneous

0747–7171/93/070009 + 28 $08.00/0

Let $L(y) = y''' + ry' + sy = 0$ be a third order linear differential equation with $r, s \in k$. $L(y) = 0$ is solvable in terms of lower order linear differential equations if and only if $L^{\circledast 4}(y)$ has order less than 15 or is reducible.

Factorization properties can also be used to determine Galois groups in many cases. For example (see Section 2.2 for the definition of the Tetrahedral Group and Theorem 4.3):

Let $L(y) = y'' + ry = 0$ be a second order linear differential equation with $r \in k$. The Galois group of $L(y) = 0$ is the Tetrahedral Group $A_4^{SL_2}$ if and only if $L^{\circledast 2}(y)$ is irreducible and $L^{\circledast 3}(y)$ is reducible.

Our results show that one can reduce many questions concerning the Galois groups of linear differential equations to factoring associated differential equations. This underscores the importance of finding efficient factorization algorithms, (c.f., Grigor'ev (1990), Schwarz (1989)).

The main tool of this paper is representation theory and the results spring from the following facts. The first fact (due to Chevalley) is that if one is given an algebraic subgroup H of $GL(n, C)$ then there is a faithful representation $\Phi : GL(n, C) \to GL(m, C)$ for some m such that $\Phi(H)$ is uniquely determined by its set of invariant subspaces in C^m (c.f., Theorem 11.2 of Humphreys (1981)). The second fact is that given a faithful representation of an algebraic group, any other representation can be constructed from this representation using the tools of linear algebra, i.e., tensor product, duals, direct sums and subspaces. Furthermore, if the group is the Galois group of a linear differential equation and the representation is the representation on the solution space of the linear differential equation, then one can mimic this construction at the level of the equation to produce an equation whose solution space corresponds to the other representation (c.f., Beukers, Brownawell and Heckman (1988), Deligne (1990), Katz (1982), Katz (1990) and Singer (1991)). The final fact that we use is that the solution space of a linear differential equation has a subspace of dimension m invariant under the action of the Galois group if and only if the equation has a factor of order m, Kolchin (1948). Combining these facts one sees that one should be able to determine the Galois group of a linear differential equation by considering the factorization properties of certain associated operators. This philosophy has been successfully used in Beukers, Brownawell and Heckman (1988), Deligne (1990), Katz (1982), Katz (1990) and Singer (1991). In this paper, we apply this philosophy to the study of second and third order linear differential equations. Except for the last fact we do not use the full theoretical power of the above facts, but rather calculate directly for the groups involved. In particular we show that in this case it is enough to consider just symmetric powers of small order.

The paper is organized in the following manner. Section 2 contains a description of the groups that can appear as Galois groups of second and third order linear differential equations as well as facts about their representation theory. Section 3 reviews facts from the formal theory of linear differential equations and Galois theory. In section 4, we present the main results. Section 5 is devoted to examples.

We wish to thank John Cannon for making available to us a copy of *Cayley* and the the Institute für Algorithmen und Kognitive Systeme of the University of Karlsruhe for allowing us to use their computer algebra systems.

2. Group Theory

To any homogeneous linear differential equation $L(y) = 0$ of order n with coefficients in a differential field k (with algebraically closed field of constants C), one can associate a group of $n \times n$ matrices $\mathcal{G}(L) \subseteq GL(n, C)$ called the differential Galois group of $L(y) = 0$ (see Kaplansky (1957) or Singer (1990) for an exposition of this theory; for concreteness, one may let $k = \overline{\mathbb{Q}}(x)$ and $C = \overline{\mathbb{Q}}$) . Differential and algebraic properties of the equation are mirrored by group theoretic properties of this group. This section is devoted to studying properties of subgroups of $SL(n, C)$. The reader interested only in the form of the algorithms and willing to accept certain group theoretic facts, may proceed to the next section.

Let V denote a finite dimensional vector space of dimension n over an algebraically closed field C.

DEFINITION 2.1. A subgroup G of $GL(V)$ is said to act *irreducibly* if the only G-invariant subspaces of V are $\{0\}$ and V. The group G is *completely reducible* if there are minimal G-invariant subspaces $V_1, \cdots, V_k$ such that $V = V_1 \oplus \cdots \oplus V_k$.

According to Maschke's theorem, every finite subgroup of $GL(V)$ is completely reducible. We shall see (in sections 3 and 4) that $L(y) = 0$ has a Galois group that acts reducibly if and only if $L(y)$ is reducible and that one can test directly if this occurs (A differential equation $L(y)$ with coefficients in k is called *reducible* if $L(y)$ can be written as $L_1(L_2(y))$, where $L_1(y)$ and $L_2(y)$ are differential equations with coefficients in k of order > 0. $L(y) = 0$ is *irreducible* if it is not reducible). We shall need finer group theoretic information when the equation (and therefore the Galois group) is irreducible. The following definitions are crucial to studying this situation.

DEFINITION 2.2. Let G be a subgroup of $GL(n, C)$ acting irreducibly, i.e. G is a linear group acting irreducibly on the vector space V of dimension n over C. Then G is called *imprimitive* if, for $k > 1$, there exist subspaces $V_1, \cdots, V_k$ such that $V = V_1 \oplus \cdots \oplus V_k$ and, for each $g \in G$, the mapping $V_i \rightarrow g(V_i)$ is a permutation of the set $\mathcal{S} = \{V_1, \ldots, V_k\}$. The set $\mathcal{S}$ is called a *system of imprimitivity* of G. If all the subspaces V_i are one dimensional, then G is called *monomial*. An irreducible group $G \subseteq GL(n, C)$ which is not imprimitive is called *primitive*.

We note that since an imprimitive group G is assumed to act irreducibly on V, we have that G acts transitively on the V_i. In particular, all the V_i have the same dimension.

DEFINITION 2.3. A group $G \subseteq GL(n, C)$ whose elements have a common eigenvector is called 1-*reducible*.

In Ulmer (1992) it is proven that, if an irreducible differential equation $L(y) = 0$ has a liouvillian solution, then $\mathcal{G}(L) \subseteq GL(n, C)$ has a 1-reducible subgroup H of finite index and that there is a solution z of $L(y) = 0$ such that the algebraic degree of $u = z'/z$ over k is $\leq [\mathcal{G}(L) : H]$.

In this section we will analyse imprimitive and primitive subgroups of $G \subseteq GL(n, C)$ and also see what consequences we can draw from assuming that such a group has a 1-reducible subgroup of finite index.

2.1. Imprimitive Groups

When n is prime any system of imprimitivity for an imprimitive subgroup $G \subseteq GL(n, \mathcal{C})$ contains only subspaces of dimension one (and therefore G must be a monomial group). The subgroup leaving one of these subspaces fixed will be a 1-reducible subgroup of index n. We therefore have the following:

Proposition 2.1. (Ulmer (1992)) *Let n be a prime number and let $G \subseteq GL(n, \mathcal{C})$ be an imprimitive group. Then G is a monomial group and contains a 1-reducible subgroup of index n.*

2.2. Primitive Groups

The differential Galois group $\mathcal{G}(L)$ of a linear differential equation is a linear algebraic group which, after a suitable change of variables (cf. Theorem 3.3), can be assumed to be unimodular, i.e. $\mathcal{G}(L) \subseteq SL(n, \mathcal{C})$. We thus restrict ourselves to linear algebraic subgroups of $SL(n, \mathcal{C})$ (see Humphreys (1981), Kaplansky (1957) or Singer (1990) for the appropriate definitions). We have the following general result:

Lemma 2.2. *Let $G \subseteq GL(n, \mathcal{C})$ be a primitive group. If H is a normal 1-reducible subgroup of G, then H is a subgroup of the group of scalar matrices.*

Proof. We say a subspace $W \subseteq \mathcal{C}^n$ is a maximal eigenspace of H if each element of H acts by scalar multiplication on W and W is maximal with respect to this property. Let $\mathcal{W}$ be the set of maximal eigenspaces of H. By hypothesis, this set is non-empty. If $W_1, \ldots, W_{m+1}$ are elements of $\mathcal{W}$ such that $W_{m+1} \cap (W_1 + \ldots + W_m) \neq \{0\}$, then one can easily show that $m = 1$ and $W_1 = W_2$. This implies that $\mathcal{W}$ is finite and that the sum V' of the elements of $\mathcal{W}$ is a direct sum. Note that H is normal in G so G permutes the elements of $\mathcal{W}$ and so leaves V' invariant. Since G is irreducible, we have $V' = \mathcal{C}^n$ and so $\mathcal{W}$ is a system of imprimitivity of G, unless $\mathcal{W}$ contains just one element. Therefore, we can conclude that the elements of H are all scalar matrices. □

Proposition 2.3. *Let $G \subseteq SL(n, \mathcal{C})$ be a primitive linear algebraic group. Then:*

(i) either G is finite or G°, the connected component of the identity of G, is a semisimple subgroup of $GL(n, \mathcal{C})$,
(ii) if G also contains a 1-reducible subgroup of finite index, G must be finite,
(iii) if $n = 2$ or 3, and G° is semisimple, then G° acts irreducibly on $\mathcal{C}^n$.

Proof. (c.f., Beukers, Brownawell and Heckman (1988) p. 301 for a similar result) Assume that G is primitive and not finite. Let $R(G^\circ)$ be the radical of G°. Note that $R(G^\circ)$ is normal in G. Since $R(G^\circ)$ is connected and soivable, the Lie-Kolchin Theorem (Humphreys (1981), p. 113) implies that the elements of $R(G^\circ)$ have a common eigenvector, i.e. $R(G^\circ)$ is 1-reducible. Therefore, we can conclude from Lemma 2.2 that the elements of $R(G^\circ)$ are all scalar matrices. Since there are only a finite number of such matrices in $SL(n, \mathcal{C})$, we must have that $R(G^\circ)$ is trivial and so G° is semisimple. This proves (i).

If G also contains a 1-reducible subgroup of finite index, then it contains a 1-reducible

normal subgroup of finite index. Lemma 2.2 implies that this latter group consists only of scalar matrices and, since $G \subseteq SL(n,C)$, must be finite. Therefore, G is finite. This proves (*ii*).

If G° is semisimple, then any invariant subspace has a complementary invariant subspace. If $n = 2$ or 3, and G° has a non-trivial invariant subspace, then G° must have an invariant subspace of dimension 1. This means that G° is 1-reducible and so by (*ii*), G is finite, a contradiction. Therefore G° acts irreducibly. □

Proposition 2.3 reduces the question of finding the primitive subgroups of $SL(n,C)$ to the question of finding the finite primitive subgroups and the semisimple subgroups. We begin with the latter. A connected semisimple group is a quotient (by a finite group) of a direct product of simple groups (Humphreys (1981), p. 167). The simple algebraic groups and their representations are well understood. In particular, by comparing dimensions one can see that the only semisimple subgroup of $SL(2,C)$ is $SL(2,C)$. Therefore any primitive proper subgroup of $SL(2,C)$ is finite. For $n = 3$, it is shown in (Singer (1985), p. 674) that the only connected proper semisimple subgroup of $SL(3,C)$ that acts irreducibly on C^3 is conjugate to the representation of $SL(2,C)$ given by

$$\rho_3\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{bmatrix}$$

This is just the irreducible three dimensional representation of $SL(2,C)$ (see Proposition 2.4 and the discussion after it). $\rho_3(SL(2,C)) \cong SL(2,C)/\{\pm 1\}$ and we shall refer to this group as PSL_2. The normalizer of PSL_2 in $SL(3,C)$ is $PSL_2 \times C_3$ where C_3 is the three element subgroup of scalar matrices (Singer (1985), p. 674). Therefore any non-finite proper primitive subgroup of $SL(3,C)$ is conjugate to either PSL_2 or $PSL_2 \times C_3$.

We now turn to the finite primitive subgroups of $SL(2,C)$ and $SL(3,C)$.

One knows the finite primitive subgroups of $PGL(3,C)$ (c.f., Blichfeld (1917)). From this list, one can derive the primitive subgroups of $SL(3,C)$ (c.f., Blichfeld (1917)). Any finite primitive group of $SL(3,C)$ is isomorphic to one of the following groups:

(i) The Valentiner Group $A_6^{SL_3}$ of order 1080 generated as a transitive permutation group of 18 letters by:

$$(1,2,4)(3,8,13)(5,7,9)(6,10,12)(11,15,14),$$
$$(1,3)(2,6)(4,5)(7,12)(8,9)(10,13),$$
$$(1,4)(3,8)(5,9)(6,11)(10,14)(12,15),$$
$$(1,4,8,3,5,9)(2,7,13)(6,12,10)(11,16,14,17,15,18),$$
$$(1,5,8)(2,7,13)(3,4,9)(6,12,10)(11,15,14)(16,18,17).$$

We have $A_6^{SL_3}/Z(A_6^{SL_3}) \cong A_6$.

(ii) The simple group G_{168} of order 168 defined by:

$$\{X,Y \mid X^7=(X^4Y)^4=(XY)^3=Y^2=id\}.$$

(iii) $G_{168} \times C_3$, the direct product of G_{168} with the cyclic group C_3 of order 3.

(*iv*) A_5, the alternating group of five letters.

(v) $A_5 \times C_3$, the direct product of A_5 with a cyclic group C_3 of order 3.

(vi) The group $H_{216}^{SL_3}$ of order 648 defined by:

$$\{U,V,S,T \mid U^9=V^4=T^3=S^3=(UV)^3=id, VS=TV$$
$$VT=S^2V, [U^6,V]=[U^6,T]=[U,S]=id, [U,V^2]=S\}.$$

Note that the group $H_{216}^{SL_3}/Z(H_{216}^{SL_3})$ is the *hessian group* of order 216.

(vii) The group $H_{72}^{SL_3}$ of order 216 generated by the elements S, T, V and UVU^{-1} of $H_{216}^{SL_3}$.

(viii) The group $F_{36}^{SL_3}$ of order 108 generated by the elements S, T and V of $H_{216}^{SL_3}$.

If $G/Z(G)$ is a simple group, then G also is a perfect group (i.e. equals its commutator group). In this case any representation of G belongs to $SL(n,C)$. But for the groups $H_{72}^{SL_3}$ and $F_{36}^{SL_3}$ there exist irreducible representations in $GL(3,C)$ which do not belong to $SL(3,C)$. Note that if $g \in SL(3,C)$ has order 2, then the trace of g is -1, and if g has order 4, then the trace cannot be I, $-I$ or -1. Considering the character tables of these groups, one sees that this restriction implies that there are only two irreducible characters of degree 3 left for $H_{72}^{SL_3}$ and $F_{36}^{SL_3}$. For the computations in the rest of the paper we will only have to consider these characters.

The finite primitive subgroups of $SL(2,C)$ are isomorphic to one of the following groups (c.f., Blichfeld (1917), Kovacic (1986)):

(i) The icosahedral group $A_5^{SL_2}$ of order 120 generated as a transitive permutation group of 24 letters by:

(1,4,2)(3,20,5)(6,13,14)(7,22,8)(9,24,10)(11,21,12)(15,23,16)(17,19,18),

(1,6,5,3,15,2)(4,12,21,20,22,7)(8,19,18,11,10,9)(13,17,16,23,24,14),

(1,3)(2,5)(4,20)(6,15)(7,21)(8,11)(9,18)(10,19)(12,22)(13,23)(14,16)(17,24),

(1,3)(2,5)(4,20)(6,15)(7,21)(8,11)(9,18)(10,19)(12,22)(13,23)(14,16)(17,24).

(ii) The octahedral $S_4^{SL_2}$ of order 48 given by:

$$\{X,Y \mid X^3=Y^8=id, YX^2=XY^3\}.$$

(iii) The tetrahedral group $A_4^{SL_2}$ of order 24 generated by X and Y^2.

We note that, the tetrahedral group has two faithfull irreducible representations in $GL(2,C)$ which do not belong to $SL(2,C)$.

2.3. The characters of symmetric products

The main idea of this paper is that for $n = 2$ or 3, one can distinguish between the various primitive groups by decomposing small symmetric powers of the original representation. We do this calculation in this section.

The first step is to calculate the characters χ_m of the m^{th} symmetric powers. We follow the presentation in (Weyl (1946), p. 181). Let z be a variable and define the functions on $GL(n,C)$, $q_0,\ldots,q_n$, via the formula:

$$det(I - zg) = q_0 - q_1 z + q_2 z^2 - \ldots \pm q_n z^n$$

for $g \in G$. Note that $q_0 = 1$ and $q_n = det(g)$. The characters χ_m of the symmetric power

$S^m(\mathcal{C}^n)$, then satisfy the following recursion:

$$\begin{aligned} \chi_0 &= 1 \\ \chi_l - q_1\chi_{l-1} + q_2\chi_{l-2} - \ldots \pm q_n\chi_{l-n} &= 0 \end{aligned}$$

for $l = 1, 2, \ldots$ and $\chi_{-1}, \chi_{-2}, \ldots$ are set equal to zero. If $G \subseteq SL(2, C)$ we have that $q_0 = q_2 = 1$ and $q_1 = \chi$, the character of the representation of G on $\mathcal{C}^2$. We get the following:

$$\begin{aligned} \chi_2 &= \chi^2 - 1 \\ \chi_3 &= \chi^3 - 2\chi \\ \chi_4 &= \chi^4 - 3\chi^2 + 1 \\ \chi_5 &= \chi^5 - 4\chi^3 + 3\chi \\ \chi_6 &= \chi^6 - 5\chi^4 + 6\chi^2 - 1 \end{aligned}$$

For $G \subseteq SL(3, C)$, we have that $q_0 = q_3 = 1$, $q_1 = \chi$, the character of the representation of G on $\mathcal{C}^3$ and $q_2 = \bar{\chi}$, where $\bar{\chi}(g) = \chi(g^{-1})$. We get the following:

$$\begin{aligned} \chi_2 &= \chi^2 - \bar{\chi} \\ \chi_3 &= \chi^3 - 2\chi\bar{\chi} + 1 \\ \chi_4 &= \chi^4 - 3\bar{\chi}\chi^2 + 2\chi + \bar{\chi}^2 \\ \chi_5 &= \chi^5 - 4\bar{\chi}\chi^3 + 3\chi^2 + 3\bar{\chi}^2\chi - 2\bar{\chi} \end{aligned}$$

For higher dimensional representations of G the *power maps* (cf. Neubüser, Pahlings and Plesken (1984)) are needed in the formula for χ_i (see e.g. Neubüser, Pahlings and Plesken (1984) for details and further references).

PROPOSITION 2.4. (See Fulton and Harris (1991), pages 150, 180) *$SL(n, \mathcal{C})$ acts irreducibly on $\mathcal{C}^n$ and on all symmetric powers $S^m(\mathcal{C}^n)$ of $\mathcal{C}^n$.*

In fact, any irreducible representation of $SL(2, \mathcal{C})$ is of the form $S^m(\mathcal{C}^2)$ for $n = 0, 1, 2, \ldots$ ($S^0(\mathcal{C}^2)$ is the trivial one dimensional representation). Note that PSL_2 is just the image of $SL(2, \mathcal{C})$ in $SL(S^2(\mathcal{C}^2)) \cong SL(3, \mathcal{C})$. For m odd, these representations are faithful representations of $SL(2, \mathcal{C})$ and for m even, these have kernel $\{\pm 1\}$ (and so factor through PSL_2). Therefore the irreducible representations of PSL_2 are $S^m(\mathcal{C}^2), m = 0, 2, 4, \ldots$. A character of a representation of $SL(2, \mathcal{C})$ is determined by its behavior on the diagonalizable elements of $SL(2, \mathcal{C})$, since these are Zariski dense in this group. If ϕ_m is the character associated with $S^m(\mathcal{C}^2)$ and $g = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ is a diagonal element, then $\phi_m(g) = a^m + a^{m-2} + \ldots + a^{-m}$. We use this notation in the following:

PROPOSITION 2.5. *Let χ be the character of the irreducible representation of PSL_2 on $\mathcal{C}^3$ and χ_m the character of the representation on $S^m(\mathcal{C}^2)$. We then have the following decompositions:*

(i) $\chi_2 = \phi_4 + \phi_0$
(ii) $\chi_3 = \phi_6 + \phi_2$
(iii) $\chi_4 = \phi_8 + \phi_4 + \phi_0$
(iv) $\chi_5 = \phi_{10} + \phi_6 + \phi_2$

PROOF. To verify these formulas, it is enough to evaluate the χ_m on the diagonal elements of PSL_2. Such a diagonal element is of the form $\begin{pmatrix} a^2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a^{-2} \end{pmatrix}$. Therefore, $\chi(g) = a^2 + 1 + a^{-2} = \bar{\chi}(g)$. Using the formulas $\chi_2 = \chi^2 - \bar{\chi}, \chi_3 = \chi^3 - 2\chi\bar{\chi} + 1$, etc., we are able to verify the above formulas. □

For each finite primitive subgroup of $SL(2,C)$ and $SL(3,C)$, using its character table (computed using the group theory system Cayley, cf. Cannon (1984)) and the orthogonality relations of characters, we can decompose the characters of the symmetric product (computed using the computer algebra system AXIOM, cf. Jenks and Sutor (1992)). The result is summarised in the following two tables, where the numbers $4, 3^2$ in the column A_5 and the row 3 of Table 2 means that the 3-th symmetric product of the character of any faithfull irreducible representation of A_5 in $SL(3,\mathbb{C})$ has an irreducible summand of degree 4 and two irreducible summands of degree 3.

	$A_5^{SL_2}$	$S_4^{SL_2}$	$A_4^{SL_2}$
2	3	3	3
3	4	4	2^2
4	5	3, 2	$3, 1^2$
5	6	4, 2	2^3
6	4, 3	$3^2, 1$	$3^2, 1$

Table 1

	PSL_2 $PSL_2 \times C_3$	A_5 $A_5 \times C_3$	$F_{36}^{SL_3}$	G_{168} $G_{168} \times C_3$	$A_6^{SL_3}$	$H_{72}^{SL_3}$	$H_{216}^{SL_3}$
2	5, 1	5, 1	3, 3	6	6	6	6
3	7, 3	$4, 3^2$	$1^2, 4^2$	7, 3	10	8, 2	8, 2
4	9, 5, 1	$5^2, 4, 1$	3^5	8, 6, 1	9, 6	$6^2, 3$	$6^2, 3$
5	11, 7, 3	$5, 4, 3^4$	3^7	$8, 7, 3^2$	$15, 3^2$	$6, 3^5$	$9, 6, 3^2$

Table 2

For later use we note that in the decomposition of the third symmetric product of $F_{36}^{SL_3}$, the two one dimensional characters ψ_i are of order 4, i.e. $\psi_i^4 = 1$ but $\psi_i^2 \neq 1$.

3. Differential Equations

3.1. Galois Theory

In this section we first briefly review some facts about differential algebra and the existing algorithms for computing liouvillian solutions of linear differential equations. For a more complete exposition we refer to Kaplansky (1957), Kovacic (1986), Singer (1981) and Singer (1990).

A *differential field* $(k\ \delta)$ is a field k together with a derivation δ on k. A *differential field extension* of (k, δ) is a differential field (K, Δ) such that K is a field extension of k and Δ is an extension of the derivation δ to a derivation on K. In this paper we always assume that k is a field of characteristic 0 and that the field $C = \ker_k(\delta)$ of constants of δ in k is algebraically closed (e.g. $(\overline{\mathbb{Q}}(x), \frac{d}{dx})$).

We also write $y^{(n)}$ instead of $\delta^n(y)$ and $y', y'', \ldots$ for $\delta(y), \delta^2(y), \ldots$. *Unless otherwise* stated, a differential equation $L(y) = 0$ over k always means an ordinary homogeneous linear differential equation

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0 \qquad (a_i \in k).$$

Definition 3.1. A differential field extension (K, Δ) of (k, δ) is a *liouvillian extension* if there is a tower of fields

$$k = K_0 \subset K_1 \subset \cdots \subset K_m = K,$$

where K_{i+1} is a simple field extension $K_i(\eta_i)$ of K_i, such that one of the following holds:

(i) η_i is algebraic over K_i, or
(ii) $\delta(\eta_i) \in K_i$ (extension by an integral), or
(iii) $\delta(\eta_i)/\eta_i \in K_i$ (extension by the exponential of an integral).

A function contained in a liouvillian extension of k is called a *liouvillian function* over k.

In Kovacic (1986) J. Kovacic gives an algorithm to find a basis of the liouvillian solutions of a second order linear differential equation with coefficients in $k_0(x)$, where k_0 is a finite algebraic extension of $\mathbb{Q}$. In Singer (1981) the first author gives a procedure to find a basis of the liouvillian solutions of a linear differential equation $L(y) = 0$ of arbitrary degree n with coefficients belonging to a finite algebraic extension of $\mathbb{Q}(x)$.

Definition 3.2. Let K_1 and K_2 be two differential extensions of k. A *differential k-isomorphism* between K_1 and K_2 is a field isomorphism that leaves k fixed and commutes with δ. The *differential Galois group* $\mathcal{G}(K/k)$ of a differential field extension K of k is the set of all differential k-automorphisms of K.

Definition 3.3. Let $L(y) = 0$ be a homogeneous linear differential equation of degree n with coefficients in a differential field k. A differential field extension K of k is called a *Picard-Vessiot extension (PVE)* of k for $L(y) = 0$ if the following holds:

(i) $K = k < y_1, y_2, \ldots, y_n >$, the differential field generated by k and $y_1, y_2, \ldots, y_n$, where $\{y_1, y_2, \ldots, y_n\}$ is a fundamental set of solutions of $L(y) = 0$.

(ii) K and k have the same field of constants.

We denote $\mathcal{G}(L)$ the differential Galois group of a PVE associated to $L(y) = 0$.

A PVE of k associated with $L(y) = 0$ is well defined and unique up to differential k-isomorphisms if $\ker_k(\delta)$ is an algebraically closed field of characteristic 0. It may be viewed as the splitting field for the equation $L(y) = 0$. The differential Galois group $\mathcal{G}(L)$ of $L(y) = 0$ is a linear algebraic group, and there is a Galois correspondence between differential subfields of K/k and linear algebraic subgroups of $\mathcal{G}(L)$ (see, e.g. Kaplansky (1957), Singer (1990)). If we choose a fundamental set of solutions $\{y_1, y_2, \ldots, y_n\}$ of the equation $L(y) = 0$, then for each $\sigma \in \mathcal{G}(L)$ we get $\sigma(y_i) = \sum_{j=1}^{n} c_{ij} y_j$, where $c_{ij} \in C$. This gives a faithful representation of $\mathcal{G}(L)$ as a subgroup of $GL(n, C)$. Different choices of basis $\{y_1, y_2, \ldots, y_n\}$ give equivalent representations. This equivalence class of representations is fundamental to our approach. In the sequel we always consider this representation as *the* representation of $\mathcal{G}(L)$.

The following known results show that many properties of the equation $L(y) = 0$ and of its solutions are related to the structure of the group $\mathcal{G}(L)$:

THEOREM 3.1. *(*see e.g. Kolchin (1948), §22, Singer (1990), §33*) The differential equation $L(y) = 0$ of degree n over k factors as a differential operator over k if and only if $\mathcal{G}(L) \in GL(n, C)$ is a reducible linear group. Let V be the solution space of $L(y) = 0$. $\mathcal{G}(L)$ leaves an m dimensional subspace of V invariant if and only if $L(y) = L_{n-m}(L_m(y))$ where $L_{n-m}(y)$ and $L_m(y)$ have coefficients in k and are of order $m - n$ and m.*

THEOREM 3.2. (see e.g. Kolchin (1948)) *A differential equation $L(y) = 0$ with coefficients in k has*

(i) only solutions which are algebraic over k if and only if $\mathcal{G}(L)$ is a finite group,
(ii) only liouvillian solutions over k if and only if the component of the identity $\mathcal{G}(L)^\circ$ of $\mathcal{G}(L)$ in the Zariski topology is solvable. In this case $L(y) = 0$ has a solution whose logarithmic derivative is algebraic over k.

The following theorem will enable us to always assume that the differential Galois group $\mathcal{G}(L) \subseteq GL(n, C)$ of a differential equation $L(y) = 0$ of degree n is unimodular.

THEOREM 3.3. (Kaplansky (1957), p. 41) *The differential Galois group of an differential equation of the form*

$$L(y) = y^{(n)} + a_{n-2}y^{(n-2)} + \cdots + a_1 y' + a_0 y = 0 \qquad (a_i \in k) \tag{3.1}$$

is a unimodular group (i.e. $\mathcal{G}(L) \subseteq SL(n, C)$).

Using the variable transformation $y = z \cdot \exp\left(-\frac{\int a_{n-1}}{n}\right)$ it is always possible to transform a given differential equation $L(y)$ into an equation $L_{SL}(y)$ of the form (3.1). For $L(y) = y''' + a_2 y'' + a_1 y' + a_0 y$ we get:

$$L_{SL}(y) = y''' + \left(a_1 - \frac{{a_2}^2}{3} - a_2'\right) y' + \left(a_0 - \frac{a_1 a_2}{3} - \frac{a_2''}{3} + \frac{2{a_2}^3}{27}\right) y.$$

The above form is a sufficient but not necessary condition for $\mathcal{G}(L)$ to be unimodular.

3.2. Linear Operators

We first collect some basic facts on linear differential operators. Linear differential operators can be seen as skew polynomials which can be manipulated almost in the same way as ordinary polynomials.

3.2.1. Factorization of linear differential equations

Let k be a field and δ be a derivation on k. In order to define the notions of irreducibility and factorization for a linear differential equation

$$L(y) = a_n\delta^n(y) + a_{n-1}\delta^{(n-1)}(y) + \cdots + a_0 y = 0$$

of degree n and coefficients in k we look at the associated differential operator:

$$p(\delta) \quad = \quad a_n\delta^n + a_{n-1}\delta^{(n-1)} + \cdots + a_0$$

We now replace δ^n by D^n in $p(\delta)$ and consider

$$p(D) \quad = \quad a_n D^n + a_{n-1}D^{(n-1)} + \cdots + a_0$$

as a *skew polynomial* in D. From $\delta(ay) = \delta(a)y + a\delta(y)$ one gets the rule $Da = aD + a^\delta$. We denote $k[D,\delta]$ the set of all such skew polynomials. This is an example of what is called an Ore ring in the litterature.

In Ore (1933) an algebraic theory of $k[D,\delta]$ is given. It is shown there that the usual polynomial addition and a multiplication defined by $Da = aD + a^\delta$ and distributivity makes $k[D,\delta]$ into a (non commutative) ring which has a left and right euclidean algorithm. The degree of $p(D)$ is defined to be the usual polynomial degree of $p(D)$ in D. Since k is a field, the degree of a product is the sum of the degrees.

Definition 3.4. *A linear differential operator $p(D) \in k[D,\delta]$ is* reducible, *if $\exists q_1(D)$, $q_2(D) \in k[D,\delta]$ of degrees > 0 such that $p(D) = q_1(D)\, q_2(D)$. If $p(D)$ is not reducible, then $p(D)$ is called irreducible. A linear differential equation is called reducible (resp. irreducible) if the associated differential operator is reducible (resp. irreducible).*

If $L(y)$ is reducible, then $L(y)$ can be writen as $L_1(L_2(y))$, where $L_1(y)$ and $L_2(y)$ are differential equations of degree > 0. We point out that a factorization of differential equation is usually not unique:

Example. We give two irreducible decompositions of a third order differential operator:

$$\begin{aligned}
&\frac{d^3}{dx^3} - \frac{8x^2-2x-3}{2x(4x+1)}\frac{d^2}{dx^2} - \frac{12x+11}{4x(4x+1)}\frac{d}{dx} + \frac{4x+5}{4x(4x+1)} \\
&= \left(\frac{d^2}{dx^2} + \frac{4x+3}{2x(4x+1)}\frac{d}{dx} - \frac{4x+5}{4x(4x+1)}\right)\left(\frac{d}{dx} - 1\right) \\
&= \left(\frac{d}{dx} - \frac{4x^2+x-1}{x(4x+1)}\right)\left(\frac{d^2}{dx^2} + \frac{1}{2x}\frac{d}{dx} - \frac{1}{4x}\right)
\end{aligned}$$

This shows that different irreducible decompositions, where the degrees are permuted, are possible. □

In general, although the irreducible factors are not unique, their degrees are unique

(up to permutation) (see Loewy (1903)). By Theorem 3.1, any irreducible subspace of the solution space of $L(y) = 0$ corresponds to a right factor of $L(y)$. Therefore for a completely reducible Galois group (for example, a finite differential Galois group) the irreducible factors correspond to irreducible invariant subspaces. In this case, any permutation of the degrees gives a (possibly different) factorization. Further properties of factorizations and an algorithm computing a factorization of a reducible differential equation $L(y)$ with coefficients in $\mathbf{C}(x)$ can be found in Grigor'ev (1990), Schlesinger (1895), Schwarz (1989).

An Eisenstein criterion for linear differential equation is given in Kovacic (1972). Another condition for irreducibility is given in Beukers, Brownawell and Heckman (1988), p. 293.

3.2.2. Symmetric power of a differential equation

In this section we show how, given some linear differential equations, one can construct the following equations:

THEOREM 3.4. (cf. Singer (1980)) *Let $L_1(y) = 0$ and $L_2(y) = 0$ be linear differential equations of degree respectively n_1 and n_2 and fundamental system respectively $S_1 = \{u_1, \cdots, u_{n_1}\}$ and $S_2 = \{v_1, \cdots, v_{n_2}\}$. Then one can construct a differential equation:*

(i) $L(y) = L_1(y) \circledcirc L_2(y) = 0$ of degree $n_3 \leq n_1 n_2$, whose solution space is spanned by $S = \{u_1 v_1, \cdots, u_{n_1} v_1, \cdots, u_{n_1} v_{n_2}\}$.

(ii) $L^{(1)}(y) = 0$ of degree $n \leq n_1$, whose solution space is spanned by the set $S^{(1)} = \{\delta(u_1), \cdots, \delta(u_{n_1})\}$.

PROOF. In order to construct $L_1(y) \circledcirc L_2(y) = 0$ we take two "arbitrary" solutions u and v of $L_1(y) = 0$ resp. $L_2(y) = 0$ and differentiate their product:

$$\begin{aligned} Y &= uv \\ \delta(Y) &= \delta(u)v + u\delta(v) \\ &\cdots \\ \delta^m(Y) &= \sum_{j=0}^{m} \binom{m}{j} \delta^j(u)\delta^{m-j}(v). \end{aligned}$$

On the right side we can always replace terms $\delta^{n_1}(u)$ and $\delta^{n_2}(v)$ by derivatives of lower order using $L_1(u) = 0$ and $L_2(v) = 0$. On the right side there are then at most $n_1 n_2$ different terms $\delta^i(u)\delta^j(v)$ where $i < n_1$ and $j < n_2$. This shows that for some $m \leq n_1 n_2$ the set $\{Y, \delta(Y), \cdots, \delta^m(Y)\}$ is linear dependent over k, which gives a differential equation for $Y = uv$.

For $L_1 = \sum_{i}^{n_1} a_i \delta^i(y)$ the differential equation $L^{(1)}(y)$ is given by:

(i) If $a_0 = 0$, then $L^{(1)}(y) = \sum_{i=1}^{n_1} a_i \delta^{i-1}(y)$.

(ii) If $a_0 \neq 0$ then

$$L^{(1)}(y) = a_n \delta^n(y) + \sum_{i=0}^{n-1} (\delta(a_{i+1}) + a_i)\delta^i(y) - \frac{\delta(a_0)}{a_0} \left(\sum_{i=1}^{n} a_i \delta^{i-1}(y) \right).$$

In Singer (1980) it is shown that S (resp. $S^{(1)}$) spans the solution space of $L_1(y) \circledS L_2(y) = 0$ (resp. $L^{(1)}(y) = 0$). □

An important special case of the above construction is:

DEFINITION 3.5. *The linear differential equation*

$$L^{\circledS m}(y) = \overbrace{L(y) \circledS \cdots \circledS L(y)}^{m} = 0$$

is called symmetric power of order m of $L(y) = 0$.

In order to compute $L^{\circledS m}(y)$, one can also differentiate u^m, where u is an "arbitrary" solution of $L(y) = 0$. It can be shown that the differential equation of lowest degree for u^m is just $L^{\circledS m}(y)$ (note that u^m has to be a solution of $L^{\circledS m}(y)$). The order of $L^{\circledS m}$ is at most $\binom{n+m-1}{n-1}$, where n is the degree of $L(y)$ (cf. Singer (1985)).

EXAMPLE. For the the Airy equation $L(y) = \dfrac{d^2y}{dx^2} - xy = 0$ we get

$$\begin{aligned} L^{\circledS 2}(y) &= \frac{d^3y}{dx^3} - 4x\frac{dy}{dx} - 2y \\ L^{\circledS 6}(y) &= \frac{d^7y}{dx^7} - 56x\frac{d^5y}{dx^5} - 140\frac{d^4y}{dx^4} + 784x^2\frac{d^3y}{dx^3} + 2352x\frac{d^2y}{dx^2} \\ &\quad -4(576x^3 - 295)\frac{dy}{dx} - 3456x^2y. \end{aligned}$$

Note that $\left(L^{\circledS 2}\right)^{\circledS 3} = L^{\circledS 6}(y)$. □

Let $L(y)$ have order n and let $L(y) = 0$ have solution space V in some Picard-Vessiot K extension of k. There is a natural map Φ_m of the m^{th} symmetric power $S^m(V)$ (c.f., Lang (1984), p. 586) into K given by sending $z_1 \circledS \ldots \circledS z_m$ to $z_1 \cdot \ldots \cdot z_m$. The image of this map is the solution space of $L^{\circledS m}(y) = 0$. The following lemma summarizes the properties of Φ_m needed later:

LEMMA 3.5. *(i)* Φ_m *is a* $\mathcal{G}(L)$ *morphism of* $\mathcal{G}(L)$ *modules.*

(ii) If all representations of $\mathcal{G}(L)$ *are completely reducible, then the solution space of* $L^{\circledS m}(y) = 0$ *is* $\mathcal{G}(L)$*-isomorphic to a direct summand of* $S^m(V)$.

(iii) If $n = 2$, *then* Φ_m *is a bijection for all* m. *In particular,* $L^{\circledS m}(y) = 0$ *has order* $m + 1$.

(iv) If $n = 3$ *and* Φ_i *is a bijection for* $i < m$, *then the dimension of the kernel of* Φ_m *is at most* 1. *In this case, the order of* $L^{\circledS m}(y) = 0$ *is either* $\frac{1}{2}(m+2)(m+1)$ *or* $\frac{1}{2}(m+2)(m+1) - 1$.

(v) If $n = 3$ *and* Φ_i *is a bijection for* $i < m-1$, *then the dimension of the kernel of* Φ_m *is at most* 3. *In this case, the order of* $L^{\circledS m}(y) = 0$ *is at least* $\frac{1}{2}(m+2)(m+1) - 3$.

PROOF. (i) is obvious and (ii) follows from (i) and complete reducibility. Now assume $n = 2$. If Φ_m is not injective, then there is a homogeneous polynomial F of degree m with coefficients in C such that $F(y_1, y_2) = 0$ for some linearly independent solutions y_1

and y_2 of $L(y) = 0$. Since C is algebraically closed, F may be written as a product of linear polynomials, so $F(y_1, y_2) = 0$ would imply that y_1 and y_2 are linearly dependent, a contradiction. This proves (*iii*).

Assume $n = 3$ and assume Φ_i is a bijection for $i < m$. Let $\{y_1, y_2, y_3\}$ be a basis of V. We then have that if $P \neq 0$ is a homogeneous polynomial of degree $i, i < m$, then $P(y_1, y_2, y_3) \neq 0$. Let $W = \{F \mid F$ is a homogeneous polynomial of degree m with coefficients in C such that $F(y_1, y_2, y_3) = 0\}$. Each non-zero F in W must be irreducible, since otherwise we would have $P(y_1, y_2, y_3) = 0$ for some homogeneous P of degree less than m. If the kernel of Φ_m has dimension at least 2, then there would be two relatively prime irreducible homogeneous polynomials F_1 and F_2 such that $F_1(y_1, y_2, y_3) = F_2(y_1, y_2, y_3) = 0$. The resultant $Res_{y_3}(F_1, F_2)$, of F_1 and F_2 with respect to y_3, is an homogeneous polynomial $F(y_1, y_2)$ of degree m^2 in y_1 and y_2 which must be zero. As in the previous case, a factorization of $F(y_1, y_2)$ yields a contradiction. This proves (*iv*).

Again assume $n = 3$ and assume Φ_i is a bijection for $i < m - 1$. Let $\{y_1, y_2, y_3\}$ be a basis of V. If Φ_{m-1} is a bijection then by what we have just shown, the kernel of Φ_m has dimension at most 1. Assume Φ_{m-1} is not a bijection. This means that the kernel of Φ_{m-1} has dimension 1. Identifying the symmetric powers with spaces of homogeneous polynomials, we let P be a homogeneous polynomial of degree $m - 1$ that spans this kernel. We see, as above, that P must be irreducible. Let $W = \{F \mid F$ is a homogeneous polynomial of degree m with coefficients in C such that $F(y_1, y_2, y_3) = 0\}$. If $F \in W$ and P does not divide F, then arguing with resultants as in the previous case, we would have a contradiction. Therefore, P divides all the elements of W. This means that W is a subspace of the space of homogeneous polynomials of degree m spanned by Y_1P, Y_2P and Y_3P. Therefore the dimension of W is at most 3. □

The following will give us a criterium to test if the Galois group is monomial. As we have noted at the beginning of section 2.1, if n is prime, then a subgroup of $GL(n, \mathbb{C})$ is imprimitive if and only if it is monomial. If n is not prime, there are always non-monomial imprimitive subgroups of $GL(n, \mathbb{C})$.

PROPOSITION 3.6. *If an irreducible linear differential equation $L(y) = 0$ of order n with coefficients in k has a monomial differential Galois group $\mathcal{G}(L) \subseteq SL(n, C)$, then the n-th symmetric power $L^{\circledS n}(y) = 0$ of $L(y) = 0$ has a solution which is the square root of an element of k.*

PROOF. If $\mathcal{G}(L) \subseteq SL(n, C)$ is a monomial group, then there is a basis $\{y_1, \cdots, y_n\}$ of the solution space of $L(y) = 0$ such that all matrices $\sigma \in \mathcal{G}(L)$ contain only one non zero element in any row and any column. Such a matrix σ has n non zero entries $a_1, \cdots, a_n$, and since it is an element of a unimodular group, its determinant $\pm a_1 a_2 \cdots a_n$ is 1. For any $\sigma \in \mathcal{G}(L)$ we get

$$\begin{aligned} \sigma(y_1 y_2 \cdots y_n) &= (a_1 a_2 \cdots a_n)(y_1 y_2 \cdots y_n) = \pm det(\sigma) \cdot (y_1 y_2 \cdots y_n) \\ &= \pm y_1 y_2 \cdots y_n. \end{aligned}$$

This shows that $(y_1 y_2 \cdots y_n)^2$ is invariant under $\mathcal{G}(L)$ and thus belongs to k. Since $y_1 y_2 \cdots y_n$ is a solution of $L^{\circledS n}(y) = 0$, we get that $L^{\circledS n}(y) = 0$ has a solution which is the square root of an element of k. □

4. Main results

4.1. Galois groups and symmetric powers

In this section we describe the behavior of the Galois group in terms of properties of various symmetric powers of the differential equation. This will give necessary and sufficient conditions for a second or third order linear differential equation to have a liouvillian solution. We start with second order equations. In what follows k will always be a differential field with algebraically closed field of constants C.

THEOREM 4.1. *Let $L(y) = 0$ be a second order homogeneous linear differential equation with coefficients in k and unimodular differential Galois group.*

(i) $L(y)$ is reducible if and only if $L(y) = 0$ has a solution $y \neq 0$ such that $y'/y \in k$. In this case $G(L) \subseteq SL(2, C)$ is reducible.
(ii) Assume $L(y)$ is irreducible. Then $G(L)$ is imprimitive if and only if $L^{\circledS 2}(y) = 0$ is reducible. In this case $L^{\circledS 2}(y) = 0$ has a solution $y \neq 0$ such that $y^2 \in k$. and $G(L) \cong C^* \rtimes \mathbb{Z}/2\mathbb{Z}$ or the dihedral group D_{2n}.
(iii) Assume $G(L)$ is primitive. Then $L^{\circledS 6}(y) = 0$ is reducible if and only if $G(L)$ is a finite group.
(iv) $G(L) \cong SL(2, C)$ if none of the above hold.

PROOF. Theorem 3.1 handles case (i) Therefore assume that $L(y)$ is irreducible. In this case the Galois group is either primitive or imprimitive. As we noted in the discussion following Proposition 2.3, the only primitive subgroups of $SL(2, C)$ are either finite or all of $SL(2, C)$.

Assume that $L(y)$ is irreducible and that $L^{\circledS 2}(y)$ is reducible. Lemma 3.5 implies that the solution space of $L^{\circledS 2}(y)$ is $G(L)$-isomorphic to the second symmetric power of the solution space of $L(y) = 0$. Therefore this symmetric power must be reducible. Table 1 shows that $G(L)$ cannot be a finite primitive group. Proposition 2.4 shows that $G(L)$ cannot be $SL(2, C)$. Therefore $G(L)$ must be imprimitive. Proposition 3.6 implies that $L^{\circledS 2}(y)$ has a solution $y \neq 0$ such that $y^2 \in k$. Furthermore $G(L)$ must be a monomial group which in this case means that it is a subgroup of $C^* \rtimes \mathbb{Z}/2\mathbb{Z}$. Either it is the full group or it must be a proper subgroup, in which case it is finite and must be a dihedral group. Conversely, if $G(L)$ is imprimitive, Proposition 3.6 implies that $L^{\circledS 2}(y)$ is reducible.

Now assume that $G(L)$ is primitive. We then have that $G(L)$ is one of the finite primitive groups or all of $SL(2, C)$. Table 1 implies that $L^{\circledS 6}(y)$ is reducible. Conversely, Proposition 2.4 implies that $L^{\circledS 6}(y)$ is irreducible if $G(L) \cong SL(2, C)$.

Finally, any proper subgroup of $SL(2, C)$ is either reducible, imprimitive or a finite primitive group so the final statement above is true. □

In cases (i), (iii) and (iv) of the above, one can give simple criteria to determine the Galois group. We do this in the next three propositions. Case (ii) is more problematic and we discuss this following these three results.

PROPOSITION 4.2. *Let $L(y) = 0$ be a second order homogeneous linear differential equation with coefficients in k and unimodular differential Galois group. Assume $L(y)$ is reducible (and so has a solution $y \neq 0$ such that $y'/y \in k$).*

(i) If $L(y) = 0$ has a unique (up to constant multiple) solution $y \neq 0$ such that $y'/y \in k$, then $\mathcal{G}(L)$ is conjugate to a subgroup of

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a, b \in C, a \neq 0 \right\}$$

Furthermore, $\mathcal{G}(L)$ is a proper subgroup of T if and only if $y^m \in k$ for some positive integer m. In this case, $\mathcal{G}(L)$ is conjugate to

$$T_m = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a, b \in C, a^m = 1 \right\}$$

where m is the smallest positive integer such that $y^m = 1$.

(ii) If $L(y) = 0$ has two linearly independent solutions y_1 and y_2 such that $y_i'/y_i \in k, i = 1, 2$, then $\mathcal{G}(L)$ is conjugate to a subgroup of

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in C, a \neq 0 \right\}$$

In this case, $y_1 y_2 \in k$. Furthermore, $\mathcal{G}(L)$ is conjugate to a proper subgroup of D if and only if $y_1^m \in k$ for some positive integer m. In this case $\mathcal{G}(L)$ is a cyclic group of order m where m is the smallest positive integer such that $y_1^m \in k$.

PROOF. If $L(y) = 0$ has a solution $y \neq 0$ such that $y'/y \in k$ then y is an eigenvector for all the elements of $\mathcal{G}(L)$ so $\mathcal{G}(L)$ is conjugate to a subgroup of T. If $L(y) = 0$ has two linearly independent solutions $y \neq 0$ such that $y'/y \in k$ then the elements of $\mathcal{G}(L)$ have two independent common eigenvectors so $\mathcal{G}(L)$ is conjugate to a subgroup of D.

Assume case (i) holds and select a basis of the solution space such that $\mathcal{G}(L) \subseteq T$. The map sending $\sigma = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ to a is an isomorphism of $\mathcal{G}(L)$ to C^*. If the image of $\mathcal{G}(L)$ is a proper subgroup of C^*, then this image is a finite cyclic group. Therefore, $\mathcal{G}(L) = T_m$. Let y be a common eigenvector of $\mathcal{G}(L)$. We then have $\sigma(y^m) = (ay)^m = y^m$ for any $\sigma \in \mathcal{G}(L)$ since a is an m^{th} root of 1. Clearly, m is the smallest positive integer such that $y^m \in k$. This proves (i).

Assume $L(y) = 0$ has two linearly independent solutions y_1 and y_2 such that $y_i'/y_i \in k, i = 1, 2$. With respect to y_1 and y_2 $\mathcal{G}(L)$ may be identified with a subgroup of D. D is isomorphic to C^* so any proper subgroup is a finite cyclic group. Furthermore, for any $\sigma \in \mathcal{G}(L), \sigma(y_1 y_2) = a y_1 a^{-1} y_2 = y_1 y_2$ so $y_1 y_2 \in k$. The remaining claim follows as above. □

When $k = \mathbb{C}(x), x' = 1$, one has algorithms to decide this question (see the factorization algorithms mentioned above and also Kovacic (1986), Duval and Loday-Richaud (1992)). Duval and Loday-Richaud (1992) also mentions the idea of seeing how many solutions one has of a specified form to determine the Galois group.

PROPOSITION 4.3. *Let $L(y) = 0$ be a second order homogeneous linear differential equation with coefficients in k and unimodular differential Galois group. Assume $\mathcal{G}(L)$ is primitive.*

(i) $L^{\circledS 3}(y)$ factors over k if and only if $\mathcal{G}(L) \cong A_4^{SL_2}$. In this case, $L^{\circledS 3}(y) = L_1(L_2(y))$ where $L_1(y)$ and $L_2(y)$ have order 2.

(ii) Assuming $L^{\circledS 3}(y)$ *irreducible, then* $L^{\circledS 4}(y)$ *factors over* k *if and only if* $\mathcal{G}(L) \cong S_4^{SL_2}$. *In this case,* $L^{\circledS 4}(y) = L_1(L_2(y))$ *where* $L_1(y)$ *and* $L_2(y)$ *have orders* 3 *and* 2.

(iii) Assuming $L^{\circledS 4}(y)$ *irreducible, then* $L^{\circledS 6}(y)$ *factors over* k *if and only if* $\mathcal{G}(L) \cong A_5^{SL_2}$. *In this case,* $L^{\circledS 6}(y) = L_1(L_2(y))$ *where* $L_1(y)$ *and* $L_2(y)$ *have orders* 4 *and* 3.

(iv) $\mathcal{G}(L) \cong SL(2,C)$ *if and only if* $L^{\circledS 6}(y)$ *is irreducible over* k.

PROOF. Lemma 3.5 states that the solution space of $L^{\circledS m}(y) = 0$ is isomorphic to the m^{th} symmetric power of V, the solution space of $L(y) = 0$. Table 1 gives the decompositions of these spaces for small m and Proposition 3.1 gives the first three results. Proposition 2.4 gives the final result. □

PROPOSITION 4.4. *Let* $L(y) = 0$ *be a second order homogeneous linear differential equation with coefficients in* k *and unimodular differential Galois group.* $\mathcal{G}(L) \cong SL(2,C)$ *if and only if* $L^{\circledS 6}(y)$ *is irreducible over* k. *Therefore,* $L(y) = 0$ *has liouvillian solutions if and only if* $L^{\circledS 6}(y)$ *is reducible.*

PROOF. If $\mathcal{G}(L) \cong SL(2,C)$, then Proposition 2.4 implies $L^{\circledS 6}(y)$ is irreducible over k. Conversely, if $\mathcal{G}(L)$ is a proper subgroup of $SL(2,C)$, then Theorem 4.1 implies that $L(y), L^{\circledS 2}(y)$, or $L^{\circledS 6}(y)$ are reducible. If $L(y)$ is reducible then the solution space V of $L(y) = 0$ has a $\mathcal{G}(L)$ invariant subspace W. $S^6(W)$ will be a $\mathcal{G}(L)$ invariant subspace of $S^6(V)$, so $L^{\circledS 6}(y)$ will be reducible. Similarly, if W is a proper $\mathcal{G}(L)$ invariant subspace of $S^2(V)$, then $S^3(W)$ will be a proper $\mathcal{G}(L)$ invariant subspace of $S^6(V)$. The final statement follows from the fact that any proper subgroup of $SL(2,C)$ has a component of the identity that has dimension less than 3 and so is solvable. □

Proposition 4.4 can be improved if one knows a priori that $L(y) = 0$ has no algebraic solutions (for example, if $k = \mathbb{C}(x)$ and $L(y) = 0$ is not fuchsian). In this case, the proof shows that $\mathcal{G}(L) \cong SL(2,C)$ if and only if $L^{\circledS 2}(y)$ is irreducible over k (in fact, if and only if $L^{\circledS 2}(y) = 0$ has a solution $y \neq 0$ such that $y'/y \in k$). This fact is the basis of the necessary conditions for liouvillian solutions developed by Kaplansky (1957). The above shows that they are also sufficient in this case.

We note that it is not so simple to distinguish between the cases of a finite and an infinite group when $\mathcal{G}(L)$ is imprimitive. This question is discussed in Baldassarri and Dwork (1979) and depends on being able to decide : given an element u algebraic over k, determine if there is a non-zero integer n such that $y'/y = nu$ has a solution y algebraic over k. This question is decidable when $k = \mathbb{C}(x), x' = 1$.

We now discuss the relationship between our ideas and Kovacic's algorithm and we assume the reader is familliar with Kovacic (1986). Kovacic's algorithm deals with four cases. His first case corresponds to the case when the equation (and therefore also the group) is reducible. The second case corresponds to the Galois group being an imprimitive group. Kovacic shows that in this case the linear differential equation $L(y) = 0$ has a solution $y \neq 0$ such that $u = y'/y$ satisfies an irreducible polynomial equations $u^2 + a_1 u + a_0 = 0$. Kovacic's algorithm attempts to find this equation. The coefficient a_1 is of the form $a_1 = \frac{y_1'}{y_1} + \frac{y_2'}{y_2} = \frac{(y_1 y_2)'}{y_1 y_2}$ for some solutions y_1, y_2 of $L(y) = 0$. In particular, this implies that $L^{\circledS 2}(z) = 0$ has a nonzero solution z such that z'/z is rational. By considering the structure of the Galois group, Kovacic can in fact show that z^2 is rational.

Kovacic further shows that the coefficient a_0 is completely determined once a_1 is known. Therefore, a careful reading of Kovacic's proof shows that he has proven parts (i) and (ii) of Theorem 4.1. Case 3 of Kovacic's algorithm corresponds to the Galois group being a primitive proper subgroup of $SL(2,C)$ and therefore being finite. Kovacic shows that in this case, $L(y) = 0$ has a solution $y \neq 0$ such that $u = y'/y$ satisfies an irreducible polynomial equation $u^m + a_{m-1}u^{m-1} + \ldots + a_0 = 0$ for $m = 4, 6$, or 12. The form of a_{m-1} shows that for $m = 4, 6$, or 12 $L^{\circledS m}(z) = 0$ has a nonzero solution z such that z'/z is rational. In particular, $L^{\circledS m}(z) = 0$ will have a factor of order 1 in one of these cases. Kovacic again shows that the other coefficients a_i are completely determined by a_{n-1} and so, he shows that (assuming cases 1 and 2 do not hold) a necessary and sufficient condition that $L(y) = 0$ has an algebraic solution is that for $m = 4, 6$, or 12 the equation $L^{\circledS m}(z) = 0$ has a nonzero solution z such that z'/z is rational. Kovacic shows this using the internal structure (e.g., existence of "large" abelian subgroups) of the finite primitive subgroups of $SL(2,C)$. This could also be shown just from the representation theory in the spirit of Theorem 4.1. When one uses the representation theory as we did, one is naturally led to consider higher order factors of the symmetric powers. One can then find necessary and sufficient conditions in terms of the factorization of symmetric powers of relatively small order. This leads to our distinction of the cases of the algorithm in Kovacic (1986) using $L^{\circledS m}(z) = 0$ for $m \in \{2, 3, 4, 6\}$ instead of $m \in \{2, 4, 6, 12\}$ (see Kovacic (1986): p. 5 and p. 32):

COROLLARY 4.5. *Let $L(y) = 0$ be a second order homogeneous linear differential equation with coefficients in k and unimodular differential Galois group. Then one of the following holds:*

(i) The equation $L(y) = 0$ has a solution of the form $e^{\int \omega}$ where $\omega \in k$ if and only if $L(y) = 0$ is reducible.

(ii) Assume that the above does not hold. The equation $L(y) = 0$ has a solution of the form $e^{\int \omega}$ where ω is algebraic over k of degree 2 if and only if $L^{\circledS 2}(y) = 0$ is reducible. In this case $\mathcal{G}(L)$ is an imprimitive subgroup of $SL(2,C)$.

(iii) Assume that the above does not hold, then

(a) The equation $L(y) = 0$ has an algebraic solution of the form $e^{\int \omega}$ where ω is algebraic over k of degree 4 if and only if $L^{\circledS 3}(y) = 0$ is reducible. In this case $\mathcal{G}(L) \cong A_4^{SL_2}$.

(b) The equation $L(y) = 0$ has an algebraic solution of the form $e^{\int \omega}$ where ω is algebraic over k of degree 6 if and only if $L^{\circledS 4}(y) = 0$ is reducible and $L^{\circledS 3}(y) = 0$ is irreducible. In this case $\mathcal{G}(L) \cong S_4^{SL_2}$

(c) The equation $L(y) = 0$ has an algebraic solution of the form $e^{\int \omega}$ where ω is algebraic over k of degree 12 if and only if $L^{\circledS 6}(y) = 0$ is reducible and $L^{\circledS 4}(y) = 0$ is irreducible. In this case $\mathcal{G}(L) \cong A_5^{SL_2}$.

(iv) The differential equation has no liouvillian solutions. In this case $\mathcal{G}(L) \cong SL(2,C)$.

PROOF. The first case is trivial, so assume $\mathcal{G}(L)$ acts irreducibly.

If $\mathcal{G}(L) \subseteq SL(2,C)$ is an irreducible algebraic group which is not imprimitive and not finite, then the last case holds.

If $\mathcal{G}(L) \subseteq SL(2,C)$ is a finite primitive group, then $\mathcal{G}(L) \cong A_4^{SL_2}$, $S_4^{SL_2}$ or $A_5^{SL_2}$. Table 1 proves the facts about the decomposition of the symmetric powers. That the algebraic degree 4, 6, 12 for ω is best possible follows from Kovacic (1986) p. 32 (or Singer and Ulmer (1991), Ulmer (1992)).

Since $\mathcal{G}(L)$ acts irreducibly (i.e. case (i) does not hold), we get from Theorem 4.1 and Table 1 that $\mathcal{G}(L)$ is imprimitive if and only if $L^{\circledS 2}(y) = 0$ is reducible. The fact that the algebraic degree 2 for ω is best possible follows from Kovacic (1986) p. 32 (or Singer and Ulmer (1991), Ulmer (1992)). □

We do not make any claims that the above conditions yield, at present, an algorithm that is better than Kovacic's. Kovacic analyses the situation much further and gives more information than we do above (see Duval and Loday-Richaud (1992) for improvements of Kovacic's algorithm and applications and Singer and Ulmer (1991) for generalizations to higher order equations of some of Kovacic's other ideas and necessary conditions). We do claim that our results show the importance of factorization algorithms and the need for finding more efficient ways to factor linear operators. They are also readily generalized to higher order equations and can be used over any differential field in which there exists an algorithm to factor differential operators.

We now turn to third order equations. We state our results first for groups that are not primitive and then for primitive groups.

THEOREM 4.6. *Let $L(y) = 0$ be a third order linear differential equation with coefficients in a differential field k with algebraically closed field of constants whose differential Galois $\mathcal{G}(L)$ group is unimodular.*

(i) $L(y) = 0$ is reducible if and only if $L(y) = 0$ has a solution $y \neq 0$ such that $y'/y \in k$ or $L^*(y) = 0$, the adjoint of $L(y) = 0$, has a solution $y \neq 0$ such that $y'/y \in k$ (if $L(y) = y''' + py' + qy = 0$, then $L^*(y) = y''' + py' - (q - p')y = 0$).

(ii) Assume $L(y)$ is irreducible. Then $\mathcal{G}(L)$ is imprimitive if and only if $L^{\circledS 3}(y) = 0$ has a solution $y \neq 0$ such that $y^2 \in k$. In this case $\mathcal{G}(L)$ is isomorphic to a subgroup of $C^* \rtimes S_3$, where S_3 is the symmetric group on three letters. If $\mathcal{G}(L)$ is isomorphic to a subgroup of $C^* \rtimes A_3$, where A_3 is the alternating group on three letters, then the above solution y is already in k.

(iii) Assume $L(y)$ is irreducible and (ii) does not hold, then $\mathcal{G}(L)$ is a primitive group.

PROOF. $L(y) = 0$ is reducible if and only if $L(y) = L_2(L_1(y))$ or $L(y) = L_1(L_2(y))$ where $L_1(y)$ and $L_2(y)$ are of order 1 and 2 respectively with coefficients in k. If $L(y) = L_1(L_2(y))$ then taking adjoints, we have $L^*(y) = L_2^*(L_1^*(y))$. Therefore (i) holds.

Now assume that $\mathcal{G}(L)$ is irreducible. If $\mathcal{G}(L)$ is imprimitive, then Proposition 2.1 implies that $L^{\circledS 3}(y) = 0$ has a solution $y \neq 0$ such that $y^2 \in k$. Now assume the conditions of (ii) hold. Table 2 implies that these conditions cannot hold if $\mathcal{G}(L)$ is primitive, unless $\mathcal{G}(L) \cong F_{36}^{SL_3}$. Since $y^2 \in k$, we must have that $\chi^2 = 1$ where χ is the associated character of the one dimensional invariant subspace generated by y of the third symmetric power of the solution space S of $L(y) = 0$. If $\mathcal{G}(L) \cong F_{36}^{SL_3}$, then all one dimensional characters in the decomposition of the third symmetric power of S have degree 4, i.e. $\chi^2 \neq 1, \chi^4 = 1$ (see remark after Table 2). We cannot be in this case. □

THEOREM 4.7. *Let $L(y) = 0$ be a third order linear differential equation with coefficients in a differential field k with algebraically closed field of constants, whose differential Galois group $\mathcal{G}(L)$ is unimodular. Assume that $\mathcal{G}(L)$ is primitive.*

(i) If $L^{\circledS 2}(y)$ has order 5 or factors then $\mathcal{G}(L)$ is isomorphic to PSL_2, $PSL_2 \times C_3$, A_5, $A_5 \times C_3$ or $F_{36}^{SL_3}$. In this case one of the following holds

(a) $\mathcal{G}(L) \cong F_{36}^{SL_3}$ if and only if $L^{\circledS 2}(y)$ has a factor of order 3, or

(b) $\mathcal{G}(L) \cong A_5$ or $A_5 \times C_3$ if and only if $L^{\circledS 3}(y)$ has a factor of order 3 and a factor of order 4, or

(c) $\mathcal{G}(L) \cong PSL_2$ or $\mathcal{G}(L) \cong PSL_2 \times C_3$ if and only if the previous two cases do not hold.

(ii) If $L^{\circledS 2}(y)$ has order 6 and is irreducible, then one of the following holds

(a) $\mathcal{G}(L) \cong G_{168}$ or $G_{168} \times C_3$ if and only if $L^{\circledS 3}(y)$ has a factor of order 3.

(b) $\mathcal{G}(L) \cong A_6^{SL_3}$ if and only if $L^{\circledS 4}(y)$ is reducible and $L^{\circledS 3}(y)$ is irreducible.

(c) $\mathcal{G}(L) \cong H_{72}^{SL_3}$ if and only if $L^{\circledS 5}(y)$ has more than 2 factors of order 3.

(d) $\mathcal{G}(L) \cong H_{216}^{SL_3}$ if and only if $L^{\circledS 5}(y)$ has exactly 2 factors of order 3 and $L^{\circledS 2}(y)$ has a factor of degree 2.

(iii) The Galois group is $SL(3, C)$ if and only if none of the above happen.

PROOF. The proof proceeds by examining Table 2. Let V be the solution space of $L(y) = 0$. If $L^{\circledS 2}(y)$ has order 5 or factors, then $S^2(V)$ must have an invariant subspace. This can only happen if $\mathcal{G}(L)$ is one of the groups mentioned. Lemma 3.5 (iii) implies that the order of $L^{\circledS 2}(y)$ is at least 5, so $\mathcal{G}(L) \cong F_{36}^{SL_3}$ if and only if $L^{\circledS 2}(y)$,has a factor of order 3. Lemma 3.5 (iv) implies that $L^{\circledS 3}(y)$ has order at least 7. Therefore if $\mathcal{G}(L) \cong A_5$ or $A_5 \times C_3$ then $L^{\circledS 3}(y)$ has a factor of order 3. This does not happen in the other cases considered, therefore (i) holds.

Assume $L^{\circledS 2}(y)$ has order 6 and is irreducible. Table 2 implies that $\mathcal{G}(L) \cong G_{168}$ or $G_{168} \times C_3$ or $A_6^{SL_3}$ or $H_{72}^{SL_3}$ or $H_{216}^{SL_3}$ or $SL(3, C)$. From Table 2 we get that $\mathcal{G}(L) \cong G_{168}$ or $G_{168} \times C_3$ if and only if $L^{\circledS 3}(y)$ has a factor of order 3. If $\mathcal{G}(L) \ncong G_{168}$ or $G_{168} \times C_3$, then none of the m^{th} symmetric powers, $m = 2, 3, 4, 5$ of V have a 1 dimensional invariant subspace for these groups, so the m^{th} symmetric powers of $L(y)$ have order exactly $\frac{1}{2}(m+2)(m+1)$. Table 2 describes how these symmetric powers factor and (ii) summarizes the distinguishing cases.

If the Galois group is $SL(3, C)$ then all symmetric powers are irreducible, so the theorem follows. □

One can use Table 2 to state other necessary and sufficient conditions for the primitive groups. For example, if $L^{\circledS 2}(y)$ has order 6 and is irreducible then $\mathcal{G}(L) \cong A_6^{SL_3}$ if and only if $L^{\circledS 3}(y)$ is irreducible and $L^{\circledS 4}(y)$ factors. Since it is not clear which criteria will be most usefull, we have just stated one set of criteria to give a taste of what can be done. The above theorems allow us to give criteria for a third order linear differential

equation to be solvable in terms of lower order linear differential equations (c.f., Singer (1988), for third order equations this concept coincides with the concept of "solving in terms of second order equations" or "eulerian" Singer (1985), Singer (1990)).

COROLLARY 4.8. *A third order linear differential equation $L(y) = 0$ with coefficients in a differential field k with algebraically closed field of constants and whose differential Galois group $G(L)$ is unimodular, is solvable in terms of lower order linear differential equations if and only if $L^{\circledS 4}(y)$ has order less than 15 or factors.*

PROOF. We first note that $L(y) = 0$ is solvable in terms of lower order linear differential equations if and only if $G(L)$ is a proper subgroup of $SL(3, C)$. To see this we use the criterion of Singer (1988), Theorem 1 (c.f., Singer (1990) Theorem 5.1, p. 48): $L(y) = 0$ cannot be solved in terms of lower order linear differential equations if and only if $G(L)$ has a lie algebra $\mathfrak{g}$ that is simple and such that if $\rho : \mathfrak{g} \to \mathfrak{gl}(m, C)$ with $m < n$, then $\rho \equiv 0$. The simple lie subalgebras of `sl(3,C)` are `sl(3,C)` and `sl(2,C)` (c.f., Singer (1988)). Since `sl(2,C)` has a representation of smaller degree, the only simple lie algebra having no nontrivial representations of lower order is `sl(3,C)`. Therefore $L(y) = 0$ cannot be solved in terms of lower order linear differential equations if and only if $G(L) = SL(3, C)$. Therefore if $L^{\circledS 4}(y)$ has order less than 15 or factors, then $G(L) \neq SL(3, C)$, so $L(y) = 0$ is solvable in terms of lower order linear differential equations.

Now we note that $G(L)$ is a proper subgroup of $SL(3, C)$ if and only if $G(L)$ acts reducibly or is imprimitive or is a primitive proper subgroup of $SL(3, C)$. If $G(L)$ acts reducibly, then the solution space V of $L(y) = 0$ has an invariant one or two dimensional subspace W. $S^4(W)$ will be a proper invariant subspace of $S^4(V)$, so $L^{\circledS 4}(y)$ has order less than 15 or factors. If $G(L)$ is imprimitive, then Theorem 4.6 implies that $L^{\circledS 3}(y)$ has a factor of order 1. Therefore the solution space Z of $L^{\circledS 3}(y) = 0$ has a one dimensional invariant subspace. Let p span this space and y_1, y_2, y_3 be a basis of V. Then $y_1 p, y_2 p, y_3 p$ spans an invariant subspace of the solution space of $L^{\circledS 4}(y) = 0$ and so $L^{\circledS 4}(y)$ must factor or have order at most 3. Finally, if $G(L)$ is a primitive proper subgroup of $SL(3, C)$, then Table 2 shows that $L^{\circledS 4}(y)$ has order less than 15 or factors. □

One also can give necessary and sufficient conditions for the existence of liouvillian solutions:

COROLLARY 4.9. *Let $L(y) = 0$ be an irreducible third order linear differential equation with coefficients in a differential field k with algebraically closed field of constants whose differential Galois $G(L)$ group is unimodular. $L(y) = 0$ has a liouvillian solution if and only if*

(i) $L^{\circledS 4}(y)$ has order less than 15 or factors, and
(ii) one of the following holds:

(a) $L^{\circledS 2}(y)$ has order 6 and is irreducible, or
(b) $L^{\circledS 3}(y)$ has a factor of order 4.

PROOF. $L(y) = 0$ has a liouvillian solution if and only if it is solvable in terms of lower order linear differential equations and its Galois group is not PSL_2 or $PSL_2 \times C_3$. The result now follows from Theorem 4.6 and Table 2. □

We now show how our approach can be used to distinguish the different cases for the algebraic degree of the logarithmic derivative of a liouvillian solution in the algorithm given in Singer (1981) using the bounds given in Ulmer (1992) Theorem 5.2 and the improvement of this bounds given in Singer and Ulmer (1991).

COROLLARY 4.10. *Let $L(y) = 0$ be an irreducible third order linear differential equation with coefficients in a differential field k with algebraically closed field of constants whose differential Galois $\mathcal{G}(L)$ group is unimodular.*

(i) $L(y)$ has a solution whose logarithmic derivative is algebraic of degree 3 if and only if $L^{\circledS 3}(y)$ has a solution $y \neq 0$ such that $y^2 \in k$. In this case $\mathcal{G}(L)$ is an imprimitive subgroup of $SL(3,C)$.

(ii) If the above does not hold, then

(a) $L(y)$ has an algebraic solution whose logarithmic derivative is algebraic of degree 6 if and only if $L^{\circledS 3}(y)$ has an irreducible factor of order 4. In this case $\mathcal{G}(L) \cong A_5$, $A_5 \times C_3$ or $F_{36}^{SL_3}$.

(b) $L(y)$ has an algebraic solution whose logarithmic derivative is algebraic of degree 9 if and only if $L^{\circledS 3}(y)$ has an irreducible factor of order 2. In this case $\mathcal{G}(L) \cong H_{216}^{SL_3}$ or $H_{72}^{SL_3}$.

(c) $L(y)$ has an algebraic solution whose logarithmic derivative is algebraic of degree 21 if and only if $L^{\circledS 3}(y)$ has an irreducible factor of order 3 and $L^{\circledS 2}(y)$ is irreducible of degree 6. In this case $\mathcal{G}(L) \cong G_{168}$ or $G_{168} \times C_3$.

(d) $L(y)$ has an algebraic solution whose logarithmic derivative is algebraic of degree 36 if and only if $L^{\circledS 3}(y)$ is irreducible of degree 10 and $L^{\circledS 4}(y)$ is reducible. In this case $\mathcal{G}(L) \cong A_6^{SL_3}$.

(iii) If none of the above holds, then $L(y) = 0$ has no liouvillian solutions.

PROOF. If $L^{\circledS 3}(y)$ has a solution $y \neq 0$ such that $y^2 \in k$, then $\mathcal{G}(L)$ is an imprimitive subgroup of $SL(3,C)$ (Theorem 4.6). In this case $L(y) = 0$ has a solution whose logarithmic derivative is algebraic of degree 3 (Theorem 5.2 of Ulmer (1992)) The only if part follows from the fact that the finite primitive group the bounds given in the Theorem are best possible (cf. Singer and Ulmer (1991), Theorem 4.4).

If the first case does not hold, then $\mathcal{G}(L)$ is a primitive subgroup of $SL(3,C)$. If $L^{\circledS 3}(y)$ has a factor of order 4, or $L^{\circledS 2}(y)$ is irreducible of degree 6 or $L^{\circledS 3}(y)$ is irreducible of degree 10, then $\mathcal{G}(L) \not\cong PSL_2$ or $PSL_2 \times C_3$. If $L^{\circledS 3}(y)$ or $L^{\circledS 4}(y)$ is reducible, then $\mathcal{G}(L) \not\cong SL(3,C)$ (cf. Proposition 2.4). Thus $\mathcal{G}(L)$ is a finite primitive subgroup of $SL(3,C)$. The conditions of the symmetric powers of $L(y) = 0$ now follow from Table 2 and the algebraic degree of the logarithmic derivative from Theorem 4.4 of Singer and Ulmer (1991). This proves *(ii)*.

If $\mathcal{G}(L)$ is not an imprimitive group and not a finite primitive subgroup of $SL(3,C)$, then the irreducible equation $L(y) = 0$ has no liouvillian solutions (cf. Singer and Ulmer (1991), Corollary 3.7). □

The above result shows that with the necessary and sufficient conditions given in this paper, one has to look for at most one possible degree of logarithmic derivative of the solution of $L(y) = 0$. This gives a substantial simplification of the algorithm given in Singer (1981) for third order differential equations.

5. Examples

Using our results, we want to decide if the differential equation

$$L(y) = \frac{d^3y}{dx^3} + \frac{32x^2 - 27x + 27}{36x^2(x-1)^2}\frac{dy}{dx} - \frac{64x^3 - 81x^2 + 135x - 54}{72x^3(x-1)^3}y = 0$$

has a liouvillian solution.

The equation $L(y) = 0$ is reducible if and only if $L(y) = 0$ or its adjoint $L^*(y) = 0$ has a right factor of order 1. This is equivalent to saying that either $L(y) = 0$ or $L^*(y) = 0$ has a solution whose logarithmic derivative is rational (cf. Singer (1985)). Since no such solution exists (this could be computed for example using an algorithm implemented by Manuel Bronstein in the computer algebra system AXIOM, cf. Jenks and Sutor (1992)), we get that $L(y) = 0$ is irreducible.

We now test if the differential Galois group is an imprimitive subgroup of $SL(3, C)$. This is the case (cf. Theorem 4.6) if and only if $L^{\circledS 3}(y) =$

$$\frac{d^7y}{dx^7} + \frac{224x^2 - 189x + 189}{18x^2(x-1)^2}\frac{d^5y}{dx^5} + \frac{-2240x^3 + 2835x^2 - 4725x + 1890}{36x^3(x-1)^3}\frac{d^4y}{dx^4}$$

$$+\frac{340480x^4 - 574560x^3 + 1263465x^2 - 969570x + 280665}{1296x^4(x-1)^4}\frac{d^3y}{dx^3}$$

$$+\frac{-358400x^5 + 756000x^4 - 2036475x^3 + 2275560x^2 - 1284255x + 289170}{432x^5(x-1)^5}\frac{d^2y}{dx^2}$$

$$+\left(\frac{1003520x^6 - 2540160x^5 + 8042895x^4 - 11711070x^3}{576x^6(x-1)^6}\right.$$

$$\left.+\frac{9723735x^2 - 4309200x + 793800}{576x^6(x-1)^6}\right)\frac{dy}{dx}$$

$$+\left(\frac{-1576960x^7 + 4656960x^6 - 16875810x^5 + 30150225x^4}{864x^7(x-1)^7}\right.$$

$$\left.+\frac{-32863320x^3 + 21565845x^2 - 7858620x + 1224720}{864x^7(x-1)^7}\right)y$$

has a solution y such that $y^2 \in \overline{\mathbb{Q}}(x)$.

Since $x^2(x-1)^2$ is a solution of $L^{\circledS 3}(y) = 0$, we get that $\mathcal{G}(L)$ is an imprimitive subgroup of $SL(3, C)$. Thus $L(y) = 0$ has a solution whose logarithmic derivative is algebraic of degree 3 (cf., Corollary 4.10).

We note that our approach does not determine the group $\mathcal{G}(L)$ in the imprimitive case. But since in this example $L(y) = 0$ is the second symmetric power of the equation

$$\frac{d^2y}{dx^2} + \left(\frac{3}{16x^2} + \frac{2}{9(x-1)^2} - \frac{3}{16x(x-1)}\right)y = 0$$

whose differential Galois group is $A_4^{SL_2}$ (Kovacic (1986), p. 23), we get by construction that $\mathcal{G}(L) \cong A_4$ (from Table 1 it now also follow that $L(y) = 0$ is irreducible).

For third order differential equations very few examples can be found in the literature†. We shall show how one can construct such examples for the primitive groups. Assume, we are given a finite group G and a differential equation of arbitrary order with G as its Galois group. Let us also assume we know that G has an irreducible representation of degree n. We shall show how to construct a differential equation of order n having the image of G in $GL(n)$ as its Galois group. The idea behind this construction is that such a differential equation will occur as a factor of some other equation that we can construct. This will also allow us to construct a differential equation for a group G from the knowledge of an irreducible polynomial $P(Y) \in \overline{\mathbf{Q}}(x)[Y]$ whose Galois group is G.

The validity of our construction depends on the following result of Burnside which shows that if V is a faithful G-module, then any irreducible G-module is a G-summand of $V^{\otimes n} = \underbrace{V \otimes \ldots \otimes V}_{n \text{ times}}$ for some $n \geq 1$:

THEOREM 5.1. (Burnside (1911), Fulton and Harris (1991) p. 25) *Let V be a finite dimensional vector space and $G \subset GL(V)$ a finite group. If W is a finite dimensional vector space on which G acts irreducibly, then for some $n \geq 1$, W appears as a direct summand of $V^{\otimes n}$.*

We shall also need the following result which shows that one can construct a linear differential equation whose solution space is isomorphic to the tensor product of the solution spaces of two given linear differential equations.

PROPOSITION 5.2. *Let $L_1(y) = 0$ and $L_2(y) = 0$ be linear differential equations with coefficients in $\overline{\mathbf{Q}}(x)$ of orders n and m respectively. One can effectively construct a linear differential equation $L_1 \otimes L_2(y) = 0$ with coefficients in $\overline{\mathbf{Q}}(x)$ having the following property: if K is a Picard-Vessiot extension of $\overline{\mathbf{Q}}(x)$ such that $L_1(y) = 0$ (resp. $L_2(y) = 0$) has n (resp. m) linearly independent solutions in K, then the solution space of $L_1 \otimes L_2(y) = 0$ in K is $\mathcal{G}(K/\overline{\mathbf{Q}}(x))$ isomorphic to $V_1 \otimes V_2$ where V_1 (resp. V_2) is the solution space of $L_1(y) = 0$ (resp. $L_2(y) = 0$) in K.*

PROOF. Let $L_2^{(i)}(y) = 0$ be the differential equation whose solution space is $\{y^{(i)} \mid y \in V_2\}$ and let α be a nonsingular point of $L_1 \circledast L_2^{(i)}(y)$ for $i = 0, \ldots, m-1$. Such a point exists and can be effectively found since each $L_2^{(i)}(y) = 0$ and so, each $L_1 \circledast L_2^{(i)}(y)$ can be effectively constructed. For notational convenience, we assume $\alpha = 0$. Let t be any integer greater than or equal to the orders of the $L_1 \circledast L_2^{(i)}(y)$. Note that if z is a solution of $L_1 \circledast L_2^{(i)}(y) = 0$ and $z(0) = z'(0) = \ldots = z^{(t)}(0) = 0$, then $z = 0$.

Let K be a Picard-Vessiot extension of $\overline{\mathbf{Q}}(x)$ and let $w_1, \ldots, w_m$ be a basis of the solution space V_2 of $L_2(y) = 0$ in K. Let $u_i = \sum_{j=1}^{m-1} x^{j \cdot t} w_i^{(j)}$. One can show that the u_i are linearly independent (since $det(w_i^{(j)}) \neq 0$) and that they form a basis of a $\mathcal{G}(K/\overline{\mathbf{Q}}(x))$ module isomorphic to V_2. Let $y_1, \ldots, y_n$ be a basis of V_1 in K and consider the elements $\{y_i u_j\}$ in K. We claim that these are linearly independent over the constants. To see this,

† *Added in Proof:* The authors have recently become aware of an example (Hurwitz (1886)) of a third order linear differential equation whose Galois group is G_{168}. See Singer and Ulmer (1993) for further references to the classical literature and an exposition of how our techniques apply to this equation.

let $\sum_{i,j} c_{ij} y_i u_j = 0$ for some constants c_{ij}. This implies that $\sum_{k=0}^{m-1} x^{k \cdot t} \sum_{i,j} c_{ij} y_i w_j^{(k)} = 0$. Note that each $z_k = \sum_{i,j} c_{ij} y_i w_j^{(k)}$ is a solution of $L_1 \circledast L_2^{(k)}(y) = 0$ and so has a zero of order at most $t-1$ at $x = 0$ if $z_k \neq 0$. Therefore each term $x^{k \cdot t} \sum_{i,j} c_{ij} y_i w_j^{(k)}$ is either zero or has a zero of order between $k \cdot t$ and $k \cdot t + t - 1$. Since these terms sum to zero, each of them must equal zero. Therefore, for each $k, 0 \leq k \leq m-1, \sum_{i,j} c_{ij} y_i w_j^{(k)} = 0$. Since $det(w_j^{(k)}) \neq 0$, we have for each $j, 1 \leq j \leq m, \sum_{i=1}^{n} c_{ij} y_i = 0$. Since the y_i are linearly independent, we have all $c_{ij} = 0$. Therefore the elements $\{y_i u_j\}$ are linearly independent over the constants. One now sees that they form the basis of a $\mathcal{G}(K/\overline{\mathbb{Q}}(x))$ module isomorphic to $V_1 \otimes V_2$. Proceeding as in Theorem 3.4, one sees that these form the basis of the solution space of a linear differential equation $L_1 \otimes L_2(y) = 0$ with coefficients in $\overline{\mathbb{Q}}(x)$ and that this operator can be constructed just knowing $L_1(y), L_2(y)$ and the integer t. □

COROLLARY 5.3. *Let $L(y) = 0$ be a linear differential equation of order n with coefficients in $\overline{\mathbb{Q}}(x)$. For any m, one can effectively construct a linear differential equation $L_1^{\otimes m}(y) = 0$ with coefficients in $\overline{\mathbb{Q}}(x)$ having the following property: if K is a Picard-Vessiot extension of $\overline{\mathbb{Q}}(x)$ such that $L_1(y) = 0$ has n linearly independent solutions in K, then the solution space of $L_1^{\otimes m}(y) = 0$ in K is $\mathcal{G}(K/\overline{\mathbb{Q}}(x))$ isomorphic to $V^{\otimes m}$ where V is the solution space of $L(y) = 0$.*

Combining Theorem 5.1 and Corollary 5.3, we see that the desired differential equation will eventually occur as a factor of some $L^{\otimes m}(y) = 0$. The orders of these equations grow very quickly. Sometimes one can find the desired differential equation by looking at only symmetric powers:

EXAMPLE. The differential equation

$$\frac{d^2y}{dx^2} + \frac{21}{100} \frac{x^2 - x + 1}{x^2(x-1)^2} y = 0$$

is irreducible and $\mathcal{G}(L) \cong A_5^{SL_2}$ (see Pépin (1881), p. 342). According to Table 1, the third symmetric power of this differential equation

$$L(y) = \frac{d^3y}{dx^3} + \frac{21(x^2 - x + 1)}{25x^2(x-1)^2} \frac{d^2y}{dx^2} + \frac{21(-2x^3 + 3x^2 - 5x + 2)}{50x^3(x-1)^3} y$$

is irreducible and has Galois group A_5. In order to prove that $\mathcal{G}(L) \cong A_5$ using factorization of differential operators over over $\overline{\mathbb{Q}}(x)$, it is enough (cf., Theorem 4.6 and 4.7) to show that:

(i) $L(y)$ is irreducible.
(ii) $L^{\circledS 3}$ has no solution y such that $y^2 \in \overline{\mathbb{Q}}(x)$.
(iii) $L^{\circledS 2}$ has order 5 or factors.
(iv) $L^{\circledS 3}$ has a factor of order 3.

We note that, since $L^{\circledS 2}$ is the fourth symmetric power of the above second order equation, $L^{\circledS 2}$ will be of order 5 in this case (cf., Lemma 3.5). In this case, the fact that $L^{\circledS 3}$

has no solution y such that $y^2 \in \overline{\mathbb{Q}}(x)$ will follow from a factorization of $L^{\circledS 3}$, which (if $\mathcal{G}(L) \cong A_5$) will have no factor of order 1. □

Assume we are given an irreducible polynomial $P(Y) \in \overline{\mathbb{Q}}(x)$ such that the Galois group of $P(Y) = 0$ is G and an irreducible representation of $G \in GL(V)$. Assume $P(Y)$ has degree n. Differentiating $P(Y) = 0$, and successively solving for the derivatives of Y and reducing mod $P(Y)$. we get for $i = 0, \ldots, n$ expressions of the form $Y^{(i)} = a_{i,0} + a_{i,1}Y + \ldots + a_{i,n-1}Y^{n-1}$, with the $a_{i,j} \in \overline{\mathbb{Q}}(x)$. These $n+1$ expressions in the n terms Y^j must be linearly dependent over $\overline{\mathbb{Q}}(x)$, so we can find a linear differential equation $L(y) = y^{(n')} + \ldots + a_0 y = 0$ with $n' \leq n$ and coefficients in $\overline{\mathbb{Q}}(x)$ whose solution space is spanned by the roots of $P(Y) = 0$. Note that $\mathcal{G}(L)$ is G. For some value of m, $L^{\otimes m}(y) = 0$ has a solution space having a subspace $\mathcal{G}(L)$ isomorphic to W. Therefore some factor of $L^{\otimes m}(y) = 0$ will have a solution space $\mathcal{G}(L)$ isomorphic to W.

There are two problems in using the above method. The first is that one needs to determine the representation (or at least its character) of $\mathcal{G}(L)$ on the solution space of $L(y) = 0$ in order to be able to predict for which value of m $L^{\otimes m}(y) = 0$ has a solution space having a subspace isomorphic to W. The second problem is that $L^{\otimes m}(y) = 0$ may have many factors of the same order whose solution spaces are different G-modules. One is faced with the problem of determining which factor gives the desired representation. Nonetheless, the above argument shows that such an operator always exists. We now give an example, where some of these problems can be avoided.

EXAMPLE. We will show how a third order differential equation with differential Galois group G_{168} can be constructed using the polynomial

$$Z^7 - 56Z^6 + 609Z^5 + 1190Z^4 + 6356Z^3 + 4536Z^2 - 6804Z - xZ^3(Z+1) - 5832,$$

which is irreducible over $\overline{\mathbb{Q}}(x)$ and has Galois group $G_{168} \cong PSL_2(7)$ (se e.g. Matzat (1980), p. 188).

Using the variable transformation $Z = Y + 8$ we get the irreducible polynomial

$$Y^7 - 735\,Y^5 - (x + 10290)\,Y^4 - (33x - 4116)\,Y^3 - (408x - 979608)\,Y^2 - (2240x - 7020524)\,Y - (4608x - 15731352),$$

which we denote $P(Y)$, whose Galois group over $\overline{\mathbb{Q}}(x)$ is also G_{168}. We denote $y_1, \ldots, y_7$ the solutions of $P(Y) = 0$ and K the splitting field of $P(Y) = 0$ over $\overline{\mathbb{Q}}(x)$. The functions $y_1, \ldots, y_7$, whose derivatives all belong to K, will satisfy a differential equation $L(y) = 0$ of order at most 7 with coefficients in $\overline{\mathbb{Q}}(x)$. If $L(y) = 0$ is of degree 7, then $\mathcal{G}(L)$ is equivalent to a permutation representation of degree 7 of G_{168}. Such a permutation representation has an invariant subspace generated by $y_1 + \ldots + y_7$. Since $y_1 + \ldots + y_7 = 0$ by construction, the functions $y_1, \ldots, y_7$ must satisfy a differential equation $L(y) = 0$ of degree at most 6, and computation shows that $L(y) = 0$ is in fact of degree 6. This differential equation is not of the form given in Theorem 3.3, but since G_{168} is a perfect group, the corresponding differential Galois group will be unimodular. The group G_{168} has 6 irreducible characters: the trivial charcater χ_1, two characters $\chi_{3,1}$ and $\chi_{3,2}$ of degree 3 and the characters χ_6, χ_7, χ_8 of degree 6, 7 and 8. According to these characters, if $L(y) = 0$ is reducible, then it either has an irreducible factor of order 3 or only irreducible factors of order 1. The last case clearly can not happen. Thus, if a factorization of $L(y) = 0$ does not produce an irreducible third order equation (one can show that this is not possible), then $L(y) = 0$ is an irreducible equation of order 6 with $\mathcal{G}(L) \cong G_{168}$. Using the above Corrolary 5.3 we can construct an equation $L^{\otimes m}(y) = 0$ whose solution

space is isomorphic to $V^{\otimes m}$ where V is the solution space of $L(y) = 0$. From Theorem 5.1 we get that for some m the character of $\mathcal{G}(L^{\otimes m})$ contains a character of degree 3 of G_{168}. Decomposing powers of χ_6 we get:

$$\begin{aligned}(\chi_6)^2 &= \chi_1 + 2\chi_6 + \chi_7 + 2\chi_8 \\ (\chi_6)^3 &= 2\chi_1 + 3\chi_{3,1} + 3\chi_{3,2} + 10\chi_6 + 8\chi_7 + 10\chi_8\end{aligned}$$

Thus by factoring $L^{\otimes 3}(y) = 0$ one will get an irreducible third order differential equation with Galois group G_{168}. □

The above example shows that working with tensor products instead of symmetric products leads to differential equations of very large order containing a large amount of redundancy. This is the reason why we have stated our main results using symmetric powers instead of tensor powers.

References

Baldassarri, F., Dwork, B. (1979). On second Order Linear Differential Equations with Algebraic Solutions. *Amer. J. of Math.* **101**.

Beukers, F., Brownawell, W.D., Heckman (1988). Siegel Normality. *Annals of Math.* **127**.

Blichfeld, H.F. (1917). *Finite collineation groups*. University of Chicago Press.

Burnside, W. (1911). *Theory of Groups of Finite Order*. Second Edition, Cambridge: Cambridge University Press.

Cannon, J.J. (1984). An introduction to the group theory language Cayley. In *Computational Group Theory*, Atkinson, M.D. (ed), New York: Academic Press.

Deligne, P. (1990). *Catégories Tannakiennes*. Birkaüser Progr. Math., Grothendieck Festschrift II.

Duval, A., Loday-Richaud, M. (1992). Kovacic's algorithm and its application to some families of special functions. *J. of Appl. Alg. in Eng. Comm. and Comp.* **3**.

Fulton, W., Harris, J. (1991). *Representation Theory*. Springer Verlag.

Grigor'ev, D.Yu. (1990). Complexity of factoring and calculating the GCD of linear ordinary differential operators. *J. Symb. Comp.* **10**.

Humphreys, J. E. (1981). *Linear Algebraic Groups*. Second Edition, New York: Springer-Verlag.

Hurwitz, A. (1886). Ueber einige besondere homogene lineare Differentialgleichungen. *Math. Ann.* **26**.

Jenks, R.D, Sutor, R.S. (1992). *Axiom, the scientific computation system*. New York: Springer-Verlag.

Kaplansky, I. (1957). *Introduction to differential algebra*. Paris: Hermann.

Katz, N. (1982). A Conjecture in the Arithmetic Theory of Differential Equations. *Bull. Soc. math. France* **110**.

Katz, N. (1990). Exponential Sums and Differential Equations. *Annals of Mathematics Studies* **124**.

Kolchin, E. R. (1948). Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations. *Annals of Math.* **49**.

Kovacic, J. (1972). An Eisenstein criterium for noncommutative polynomials. *Proc. Amer. Math. Soc.* **34**.

Kovacic, J. (1986). An algorithm for solving second order linear homogeneous differential equations. *J. Symb. Comp.* **2**.

Lang, S. (1984). *Algebra*. Second Edition, New York: Addison Wesley Publishing Company.

Loewy, A. (1903). Über reduzible lineare homogene Differentialgleichungen. *Math. Ann.* **56**.

Matzat, B. H. (1980). *Konstruktive Galoistheorie*. Springer Lecture Notes in Mathematics 1284, Berlin: Springer.

Neubüser, J., Pahlings, H., Plesken, W, (1984). CAS; Design and Use of a System for the Handling of Characters of Finite Groups. In *Computational Group Theory*, Atkinson, M.D. (ed), New York: Academic Press.

Ore, O. (1933). Theory of non-commutative polynomials. *Ann. of Math.* **34**.

Pépin, P. Th. (1881). Méthode pour obtenir les intégrales algébriques des équations différentielles linéaires du second ordre. *Atti dell' Accad. Pont. de Nuovi Lincei, XXXIV, p. 243-388.*

Schlesinger, L. (1895). *Handbuch der Theorie der linearen Differentialgleichungen*. Leipzig: Teubner.

Schwarz, F. (1989). A Factorization algorithm for linear ordinary differential equations. *Proceedings of the 1989 Symposium on Symbolic and Algebraic Computation. ACM.*

Singer, M. F. (1980). 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**.

Singer, M. F. (1981). Liouvillian solutions of n^{th} order linear differential equations. *Amer. J. Math.* **103**.

Singer, M. F. (1985). Solving homogeneous linear differential equations in terms of second order linear differential equations. *Amer. J. of Math.* **107**.

Singer, M. F. (1988). Algebraic relations among solutions of linear differential equations: Fano's Theorem. *Am. J. of Math.* **110**.

Singer, M. F. (1990). An outline of differential Galois theory. In *Computer Algebra and Differential Equations*, Ed. E. Tournier, New York: Academic Press.

Singer, M. F. (1991). Moduli of Linear Differential Equations on the Riemann Sphere with Fixed Galois Groups. To appear in the Pacific Journal of Mathematics.

Singer, M. F., Ulmer, F. (1991). Bounds and Necessary Conditions for Liouvillian Solutions of (Third Order) Linear Differential Equations. Preprint.

Singer, M. F., Ulmer, F. (1993). On a Third Order Differential Equation whose Differential Galois Group is the Simple Group of 168 Elements. To appear in *Proceedings of AAECC-10*, LNCS, Springer-Verlag.

Ulmer, F. (1992). On liouvillian solutions of differential equations. *J. of Appl. Alg. in Eng. Comm. and Comp.* **2**.

Weyl, H. (1946). *The Classical Groups*, Princeton University Press.