J. Symbolic Computation (1996) **22**, 179–200

Note on Kovacic's Algorithm†

FELIX ULMER*‡ AND JACQUES-ARTHUR WEIL‡§

*IRMAR, *Université de Rennes 1*
‡GAGE, *École Polytechnique*

(Received 1 February 1995)

Algorithms exist to find Liouvillian solutions of second order homogeneous linear differential equations (Kovacic, 1986, Singer and Ulmer, 1993b). In this paper, we show how, by carefully combining the techniques of those algorithms, one can find the Liouvillian solutions of an irreducible second order linear differential equation by computing only rational solutions of some associated linear differential equations. The result is an easy-to-implement simplified version of the Kovacic algorithm, based as much as possible on the computation of rational solutions of linear differential equations.

1. Differential Galois Theory

The material presented in this section is well known and has been included to make the exposition self contained. We refer to Kaplansky (1976), Kolchin (1948), Singer (1990) for further details about this section.

1.1. INTRODUCTION

A *differential field* (k, δ) is a field k together with a derivation δ on k. We also write $y^{(n)}$ instead of $\delta^n(y)$ and $y', y'', \ldots$ for $\delta(y), \delta^2(y), \ldots$. The field of constants $\{c \in k \mid c' = 0\}$ is denoted $\mathcal{C}$. Unless otherwise stated, a differential equation $L(y) = 0$ over k always means an ordinary homogeneous linear differential equation

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

In the following we will look at solutions of $L(y) = 0$ in a differential field extension of 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 of k to a derivation on K. The differential Galois group $\mathcal{G}(K/k)$ of a differential field extension K of k is the set of k-automorphisms of K which commute with the derivation of K. There is a unique way to extend the derivation of k to an algebraic extension of k making any algebraic extension of k into a differential extension.

† Research supported by the CNRS GDR 1026 (MEDICIS), the GDR-PRC 967 (Math-Info), and the CEC ESPRIT BRA contract 6846 (POSSO).

‡ E-mail: `Felix.Ulmer@univ-rennes1.fr`

§ E-mail: `Jacques-Arthur.Weil@polytechnique.fr`

0747–7171/96/080179 + 22 $25.00/0

DEFINITION 1.1. *A differential field extension* (K, Δ) *of* (k, δ) *is called 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 solution of $L(y) = 0$ which is contained in:

(i) k, the coefficient field, will be called a *rational* solution,
(ii) an algebraic extension of k will be called an *algebraic* solution,
(iii) a Liouvillian extension of k will be called a *Liouvillian* solution

A solution z of $L(y) = 0$ is called *exponential*[†] if z'/z is in the coefficient field k. In the following we will have to compute rational and exponential solutions of $L(y) = 0$. For this reason we always assume that k is a differential field over which such solutions can be computed (e.g. $(\mathbb{C}(x), \frac{d}{dx})$). The computation of an exponential solution is usually much more difficult than the computation of a rational solution.

For $k = \mathbb{C}(x)$ and a differential equation $L(y) = 0$ with coefficients in k, an algorithm to compute

(i) rational solutions is given in Liouville (1833). More recent algorithms for more general coefficient fields are presented in Bronstein (1992), Singer (1991);
(ii) algebraic solutions of a second order equation $L(y) = 0$ is given in Fuchs (1878) and in Pépin (1881). The study of the third order case is started in Jordan (1878), a general algorithm was given by Boulanger and Singer, cf. Singer (1979);
(iii) Liouvillian solution of a second order equation is given in Kovacic (1986). A general procedure for equations of arbitrary order is presented in Singer (1981). The third order case is treated in Singer and Ulmer (1993b).

DEFINITION 1.2. *Let* $L(y) = 0$ *be a homogeneous linear differential equation of order* n *with coefficients in* k*. A differential field extension* K *of* k *is called a* Picard–Vessiot extension (PVE) *of* k *for* $L(y) = 0$ *if*

(i) $K = k\langle y_1, \ldots, y_n\rangle$*, the* differential *field extension of* k *generated by* $y_1, \ldots, y_n$ *where* $\{y_1, \ldots, y_n\}$ *is a fundamental set of solutions of* $L(y) = 0$*.*
(ii) K *and* k *have the same field of constants.*

A PVE extension plays the role of a splitting field for $L(y) = 0$. A PVE exists and is unique up to differential isomorphisms if the field of constants of k is algebraically closed of characteristic 0 (Kaplansky, 1976, p. 21 and Kolchin, 1948). In the sequel we will always assume that the coefficient field is algebraically closed of characteristic 0. By definition the differential Galois group $\mathcal{G}(L)$ of $L(y) = 0$ is the differential Galois group of K/k, where

[†] Note that the exponential solutions of $L(y) = 0$ do not form a ring.

K is a PVE of k for $L(y) = 0$. 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 $c_{ij} \in \mathcal{C}$. This gives a faithful representation of $\mathcal{G}(L)$ as a subgroup of $\mathrm{GL}(n, \mathcal{C})$. Different choices of bases $\{y_1, y_2, \ldots, y_n\}$ give equivalent representations. In the sequel we always consider this equivalence class of representations as *the* representation (module) of $\mathcal{G}(L)$. In fact, $\mathcal{G}(L)$ is a linear algebraic subgroup of $\mathrm{GL}(n, \mathcal{C})$ (Kolchin, 1948; Kovacic, 1986). We can limit our considerations to differential equations with $\mathcal{G}(L) \subseteq \mathrm{SL}(n, \mathcal{C})$:

THEOREM 1.1. (KAPLANSKY, P. 41) *The differential Galois group of a differential equation of the form*

$$L(y) = y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0 \qquad (a_i \in k) \tag{1.1}$$

is a unimodular group (i.e. $\mathcal{G}(L) \subseteq \mathrm{SL}(n, \mathcal{C})$) if and only if $\exists W \in k$, such that $W'/W = a_{n-1}$.

In particular for a differential equation of the form

$$L(y) = y^{(n)} + a_{n-2} y^{(n-2)} + \cdots + a_1 y' + a_0 y = 0 \tag{1.2}$$

we have $\mathcal{G}(L) \subseteq \mathrm{SL}(n, \mathcal{C})$. Using the variable transformation $y = z \cdot e^{\left(-\frac{\int a_{n-1}}{n}\right)}$ it is always possible to transform a given differential equation $L(y)$ into an equation $\widetilde{L}(y)$ of the form (1.2) without altering the Liouvillian character of the solutions. This transformation is always performed in Kovacic (1986). The algorithm presented in this paper works independently of this particular form and avoids unnecessary transformations.

1.2. PROPERTIES OF THE DIFFERENTIAL GALOIS GROUP

Properties of the equation $L(y) = 0$ are reflected by properties of the group $\mathcal{G}(L)$. To the equation (1) we associate a linear differential operator:

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

The set of differential operators forms a ring $k[\delta]$ where multiplication is defined by $\delta a = a\delta + \delta(a)$. The ring $k[\delta]$ is a right and left euclidian ring in which a right (resp. left) least common multiple of differential operators can be computed (Ore, 1933). The factorization of differential operators in $k[\delta]$ is not unique but, as shown in Kolchin (1948), Singer (1990), or Singer (1996), we have:

THEOREM 1.2. *The linear differential equation $L(y)$*

(i) *factors as a linear differential operator, if and only if $\mathcal{G}(L) \subseteq \mathrm{GL}(n, \mathcal{C})$ is a reducible linear group.*
(ii) *is the least common left multiple of irreducible operators if and only if $\mathcal{G}(L) \subseteq \mathrm{GL}(n, \mathcal{C})$ is a completely reducible linear group.*

Another property of $L(y) = 0$ that can be characterized by a property of $\mathcal{G}(L)$ is the solvability in terms of Liouvillian solutions. Note that if a second order equation has a Liouvillian solution, then another Liouvillian solution can be found using the d'Alembert reduction method. Thus a second order equation has either no Liouvillian solutions or only Liouvillian solutions.

THEOREM 1.3. (KOLCHIN, 1948) *A differential equation $L(y) = 0$ with coefficients in k has 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.*

If $\mathcal{G}(L)^\circ$ is solvable, then it can be put simultaneously in triangular form (Lie–Kolchin Theorem, Kolchin, 1948) and thus has a common eigenvector z. In particular z'/z is in the fixed field of $\mathcal{G}(L)^\circ$ and thus, using the Galois correspondence, algebraic over k of degree at most $[\mathcal{G}(L) : \mathcal{G}(L)^\circ] < \infty$. In Singer (1981), it is shown that the algebraic degree of the logarithmic derivative z_1'/z_1 of *a particular* solution z_1 can be bounded independently of the equation $L(y) = 0$ (Singer, 1981; Ulmer, 1992). To compute the coefficients of the minimal polynomial of $u_1 = z_1'/z_1$ one notes that all conjugates u_i of u_1 under $\mathcal{G}(L)$ are also logarithmic derivatives of solutions z_i, the minimal polynomial $P(u)$ of u_1 can be written as

$$P(u) = \prod_{i=1}^{m} \left(u - \frac{\delta(z_i)}{z_i} \right) \tag{1.3}$$

$$= u^m - \frac{\delta\left(\prod_{i=1}^m z_i\right)}{\prod_{i=1}^m z_i} u^{m-1} + \cdots + (-1)^m \prod_{i=1}^{m} \frac{\delta(z_i)}{z_i}. \tag{1.4}$$

In particular, the coefficient of u^{m-1} is the negative logarithmic derivative of a product of m solutions of $L(y) = 0$. It is possible (Singer, 1979) to construct a differential equation whose solutions are the products of length m of solutions of $L(y) = 0$:

DEFINITION 1.3. *Let $L(y) = 0$ be a homogeneous linear differential equation of order n and let $\{y_1, \ldots, y_n\}$ be a fundamental system of solutions. The differential equation $L^{\circledS m}(y)$ whose solution space is generated by the monomials of degree m in $y_1, \cdots, y_n$ is called the* mth symmetric power[†] *of $L(y) = 0$.*

To construct the equation $L^{\circledS m}(y)$ one starts with $Y = \prod_{i=1}^m z_i$, where z_i are arbitrary solutions of $L(y) = 0$. Taking derivatives of Y and replacing derivatives of order $\geq m$ of the z_i on the right-hand side by lower order derivatives using $L(y) = 0$ gives a linear differential equation for Y of order at most $\binom{n+m-1}{n-1}$ (Singer and Ulmer, 1993a). The group $\mathcal{G}(L)$ operates on the solutions space of $L^{\circledS m}(y)$ in a natural way which gives another representation of $\mathcal{G}(L)$.

From (1.4) we get that the coefficient of u^{m-1} in the minimal polynomial $P(u)$ is the negative logarithmic derivative of an exponential solution of $L^{\circledS m}(y)$.

Example. Let $L(y) = y'' + \dfrac{3}{16x^2} y$ and $k = \mathbb{C}(x)$. This equation has a solution whose logarithmic derivative is a solution of

$$P(u) = u^2 - \frac{1}{x} u + \frac{3}{16x^2}.$$

[†] One of the referees proposed the following equivalent definition. The differential equation corresponds to a differential module M together with a cyclic element e such that $Le = 0$ and L has minimal order with respect to this property. Let $\mathcal{S}^m(M)$ denote the mth symmetric power of M (Lang, 1984, p. 586). The minimal equation $L^{\circledS m}(y)$ of the element $e \otimes \cdots \otimes e \in \mathcal{S}^m(M)$ is called the *mth symmetric power* of L. Note that $e \otimes \cdots \otimes e$ is not always cyclic.

The coefficient of u is the negative logarithmic derivative of the solution $y = x$ of

$$L^{\circledS 2}(y) = y''' + \frac{3}{4x^2}y' - \frac{3}{4x^3}y = 0.$$

In this case the exponential solution is even rational. $\diamond$

In general the order of $L^{\circledS m}(y)$ can be less than $\binom{n+m-1}{n-1}$. For second order equations, the order is always $m+1$ (Singer and Ulmer, 1993a, Lemma 3.5) and the solution space of $L^{\circledS m}(y)$ is isomorphic to the mth symmetric power $\mathcal{S}^m(V)$ (Lang, 1984, p. 586) of the solution space V of $L(y) = 0$. In particular the character χ_m of the representation of $\mathcal{G}(L)$ on the solution space of $L^{\circledS m}(y)$ is the symmetrization of the character χ of the representation of $\mathcal{G}(L)$ on the solution space of $L(y) = 0$. For finite groups one can compute χ_m from χ (Singer and Ulmer, 1993a).

Definition 1.4. (see, e.g., Sturmfels, 1993) *Let V be a $\mathcal{C}$-vector space, call $\{y_1, \ldots, y_n\}$ a basis for V, and let $G \subseteq \mathrm{GL}(V)$ be a linear group. Define an action of $g \in G$ on $\mathcal{C}[y_1, \ldots, y_n]$ by $g \cdot (p(y_1, \ldots, y_n)) = p\,(g(y_1), \ldots, g(y_n))$. A polynomial with the property that*

$$\forall g \in G, \quad g\,(p(y_1, \ldots, y_n)) = \psi_p(g) \cdot (p(y_1, \ldots, y_n))\,, \ \textit{with } \psi_p(g) \in \mathcal{C}$$

is called a semi-invariant *of G. If $\forall g \in G$ we have $\psi_p(g) = 1$, then $p(y_1, \ldots, y_n)$ is called an* invariant *of G.*

Clearly, ψ_p must be a character of degree one. In the above definition the $y_1, \ldots y_n$ are independent variables. If we evaluate a polynomial $p(y_1, \ldots, y_n)$ by replacing the variables by the elements of a fundamental set of solutions of $L(y) = 0$, we get a function of the PVE associated to $L(y) = 0$. By differential Galois theory, since an invariant I of degree m of $\mathcal{G}(L)$ is left fixed by $\mathcal{G}(L)$, it must evaluate to a rational solution of $L^{\circledS m}(y) = 0$. In this paper we will identify the invariants with this rational solution and by *computing an invariant* we always mean *computing the corresponding rational solution.* Similarly a semi-invariant of degree m evaluates to an exponential solution of $L^{\circledS m}(y) = 0$ and thus, if it is not 0, to a right factor of order one of $L^{\circledS m}(y)$.

If $L(y) = 0$ is a second order equation, then any semi-invariant S of degree m of $\mathcal{G}(L)$ is a non-trivial exponential solution of $L^{\circledS m}(y) = 0$. To this semi-invariant corresponds a character of degree 1 in the decomposition of χ_m (the character of the representation of $\mathcal{G}(L)$ on the solution space of $L^{\circledS m}(y)$). For finite groups, the existence of a non-trivial semi-invariant of degree m can be deduced from the existence of a character of degree 1 in the decomposition of χ_m into irreducible characters.

Using this terminology, we see from (1.4) that the coefficient of u^{m-1} in $P(u)$ is a semi-invariant of degree m of $\mathcal{G}(L)$. In Section 2, we will show that to any semi-invariant of $\mathcal{G}(L)$ corresponds a unique polynomial $P(u)$ whose irreducible *factors* are all minimal polynomials of logarithmic derivatives of some solutions of $L(y) = 0$.

Example. Let $L(y) = y'' + \frac{3}{16x^2}y$ and $k = \mathbb{C}(x)$. we choose the two exponential solutions

$$y_1 = e^{\int \frac{1}{4x}} = x^{\frac{1}{4}}, \qquad y_2 = e^{\int \frac{3}{4x}} = x^{\frac{3}{4}}$$

as a basis of the solution space of $L(y) = 0$. A PVE of k for $L(y) = 0$ is the algebraic extension $\mathbb{C}(x)(x^{\frac{1}{4}})$ and $\mathcal{G}(L)$ is cyclic of order 4. The group $\mathcal{G}(L)$ is an abelian group and has four characters of degree one: the trivial character $\mathbf{1}$, a character $\psi_{1,1}$ of order 2

(i.e. $(\psi_{1,1})^2 = \mathbf{1}$) and two characters $\psi_{1,2}$ and $\psi_{1,3}$ of order 4. In the basis $\{y_1, y_2\}$, the group $\mathcal{G}(L)$ is generated by:

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

From the above form we get that $\chi = \psi_{1,2} + \psi_{1,3}$ and thus that $\mathcal{G}(L)$ has two linearly independent semi-invariants $S_{1,1} = x^{\frac{1}{4}}$ and $S_{1,2} = x^{\frac{3}{4}}$ of degree one corresponding to the characters $\psi_{1,2}$ and $\psi_{1,3}$. To the logarithmic derivatives of $S_{1,1}$ and $S_{1,2}$ correspond two minimal polynomials $\left(u - \frac{1}{4x}\right)$ and $\left(u - \frac{3}{4x}\right)$ of logarithmic derivatives $u_i = y_i'/y_i$ of solutions of $L(y) = 0$.
A basis of the solution space of $L^{\circledS 2}(y) = 0$ (cf. previous Example) is given by:

$$(y_1)^2 = x^{\frac{1}{2}}, \qquad y_1 y_2 = x, \qquad (y_2)^2 = x \cdot x^{\frac{1}{2}}.$$

In the basis $\{(y_1)^2, y_1 y_2, (y_2)^2\}$, the group $\mathcal{G}\left(L^{\circledS 2}\right)$ is generated by:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

From the above form we get that $\chi_2 = \mathbf{1} + 2\psi_{1,1}$ and thus that $\mathcal{G}(L)$ has an invariant $I_2 = y_1 y_2 = x$ of degree 2 and two linearly independent semi-invariants $S_{2,1} = y_1^2 = x^{\frac{1}{2}}$ and $S_{2,2} = y_2^2 = x \cdot x^{\frac{1}{2}}$ of degree 2 corresponding both to the character $\psi_{1,1}$. To the logarithmic derivative $\frac{1}{x}$ of I_2 corresponds the polynomial $\left(u^2 - \frac{1}{x}u + \frac{3}{16x^2}\right)$. This polynomial is not irreducible, but is the product of the above polynomials of degree one corresponding to $\psi_{1,2}$ and $\psi_{1,3}$. We will show in this paper that this factorization corresponds to the factorization $I_2 = S_{1,1} \cdot S_{1,2}$. $\diamond$

Since exponential solutions (semi-invariants) are usually more difficult to compute than rational solutions (invariants), we want to compute whenever possible the minimal polynomials corresponding to rational solutions (invariants) and, if necessary, factor the corresponding polynomial $P(u)$. In particular we will show that for *irreducible* second order equations this will always be possible.

1.3. SECOND ORDER EQUATION

Let $L(y) = y'' + a_1 y' + a_0 y$ be a second order equation with coefficients in k and unimodular Galois group $\mathcal{G}(L) \subset \mathrm{SL}(2, \mathcal{C})$. The logarithmic derivatives of the solutions are precisely the solutions of the associated Riccati equation $\mathrm{Ri}(u) := u' + a_0 + a_1 u + u^2 = 0$. The possible groups $\mathcal{G}(L)$ are the linear algebraic subgroups of $\mathrm{SL}(2, \mathcal{C})$ which can be classified, up to conjugacy, as follows (Kovacic, 1986):

(i) The reducible but non-reductive groups, where a non-trivial $\mathcal{G}(L)$-invariant subspace has no complementary $\mathcal{G}(L)$-invariant subspace.
(ii) The diagonal linear algebraic subgroups of $\mathrm{SL}(2, \mathcal{C})$.
(iii) The imprimitive subgroups of $\mathrm{SL}(2, \mathcal{C})$ which are up to conjugacy:

(a) The finite groups $D_n^{\mathrm{SL}_2}$ of order $4n$ (central extensions of the dihedral groups D_n) and generated by:

$$\begin{pmatrix} e^{\pi i/n} & 0 \\ 0 & e^{-\pi i/n} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

(b) The infinite group:

$$D_\infty = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix} \right\} \qquad \text{where } a \in \mathcal{C}^*.$$

(iv) The primitive finite subgroups of $\mathrm{SL}(2,\mathcal{C})$ which are isomorphic to either the tetrahedral, the octahedral or the icosahedral group; we denote them respectively $A_4^{\mathrm{SL}_2}$, $S_4^{\mathrm{SL}_2}$ and $A_5^{\mathrm{SL}_2}$. A definition for these groups is given in Kovacic (1986) or Singer and Ulmer (1993b).

(v) The group $\mathrm{SL}(2,\mathcal{C})$.

In order to bound the degree of an algebraic solution of $\mathrm{Ri}(u) = 0$, we compute a maximal subgroup H_z having a common eigenvector z, i.e. a reducible subgroup of $\mathcal{G}(L) \subseteq \mathrm{SL}(2,\mathcal{C})$. The group H_z is the stabilizer of z'/z and thus, if the index $[\mathcal{G}(L) : H_z]$ is finite, the minimal polynomial of z'/z will be of degree $[\mathcal{G}(L) : H_z]$.

LEMMA 1.5. *Let H be a finite reducible subgroup of $\mathrm{SL}(2,\mathcal{C})$ which is not contained in the center $Z(\mathrm{SL}(2,\mathcal{C}))$ of $\mathrm{SL}(2,\mathcal{C})$. Then H is cyclic and there exists up to multiples a unique basis in which H is a diagonal subgroup of $\mathrm{SL}(2,\mathcal{C})$.*

PROOF. Since H is finite, Maschke's theorem shows that any invariant subspace has a complementary invariant subspace. Thus, we can put the elements of H simultaneously in diagonal form. Since $H \subset \mathrm{SL}(2,\mathcal{C})$ the diagonal entries will be given by characters χ and χ^{-1}. Therefore the map $h \in H \mapsto \chi(h)$ is an isomorphism of H onto a finite (and therefore cyclic) subgroup of $\mathcal{C}$. The result now follows from the linear independence of characters (Lang, 1984). □

LEMMA 1.6. *Let $L(y) = 0$ be an irreducible second order equation over k whose differential Galois group $\mathcal{G}(L)$ is a finite unimodular group. Let $Z(\mathcal{G}(L))$ be the center of $\mathcal{G}(L)$. Then, the number of irreducible minimal polynomials of degree $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$ of algebraic solutions of the Riccati equation $\mathrm{Ri}(u) = 0$ is equal to $2/m$ times the number of maximal cyclic subgroups (i.e. not contained in a larger cyclic subgroup) of index m of $\mathcal{G}(L)$. In particular, this number is always finite. All other solutions of the Riccati equation are algebraic of degree $[\mathcal{G}(L) : Z(\mathcal{G}(L))]$.*

PROOF. Let w be an algebraic solution of $\mathrm{Ri}(u)$. The degree m of the minimum polynomial of w equals the index $[\mathcal{G}(L) : H_1]$ of the stabilizer $H_1 = \mathrm{Stab}_{\mathcal{G}(L)}(w)$ of w in $\mathcal{G}(L)$. Note that $\mathrm{Stab}_{\mathcal{G}(L)}(w)$ always contains $Z(\mathcal{G}(L))$. If $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$ then, by the above Lemma, H_1 is a non-central cyclic group having up to multiples a unique basis $\{y_1, y_2\}$ in which it is a diagonal group.

Denote z_1 the solution of $L(y) = 0$ such that $z_1'/z_1 = w$. Then z_1 spans an H_1-invariant subspace, which by Maschke's Theorem has a complementary subspace spanned by some solution z_2. Since H_1 is also diagonal in the basis $\{z_1, z_2\}$, z_1 must be a multiple of y_1 or y_2, say y_1. The cyclic group H_1 cannot be contained in a larger cyclic subgroup of $\mathcal{G}(L)$: from Lemma 1.5 such a group would also be diagonal in the (up to multiples unique) basis $\{y_1, y_2\}$ and thus would be contained in H_1, the stabilizer of $w = y_1'/y_1$. In particular H_1 is also the stabilizer of y_2'/y_2 which must be algebraic of the same degree as y_1'/y_1.

It follows that the stabilizer of any algebraic solution of degree $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$ of $R_i(u) = 0$ is a maximal cyclic subgroup, and each maximal cyclic subgroup of index $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$ is the stabilizer of exactly two algebraic solutions of degree m of $R_i(u) = 0$. If there are N maximal cyclic subgroups of index $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$, there are exactly $2N$ solutions of $R_i(u) = 0$ which are algebraic of degree m, and we must have exactly $2N/m$ minimum polynomials of degree m for these solutions. □

Using for example the group theory system CAYLEY one gets:

COROLLARY 1.7. *Let $L(y) = 0$ be a second order equation over k. For the possible minimal polynomials of the algebraic solutions of the Riccati equation we get:*

- *If $\mathcal{G}(L) \cong D_2^{\mathrm{SL}_2}$ (quaternion group), there are exactly three minimal polynomials of degree 2 and all the others are of degree 4.*
- *If $\mathcal{G}(L) \cong A_4^{\mathrm{SL}_2}$ (tetrahedral group), there are exactly two minimal polynomials of degree 4, one of degree 6, and all the others are of degree 12.*
- *If $\mathcal{G}(L) \cong S_4^{\mathrm{SL}_2}$ (octahedral group), there is exactly one minimal polynomial of degree 6, one of degree 8, one of degree 12, and all the others are of degree 24.*
- *If $\mathcal{G}(L) \cong A_5^{\mathrm{SL}_2}$ (icosahedral group), there is exactly one minimal polynomial of degree 12, one of degree 20, one of degree 30, and all the others are of degree 60.*

This gives a partial proof of the following theorem which is the basis of the Kovacic algorithm:

THEOREM 1.4. (KOVACIC, 1986) *Let $L(y) = 0$ be a second order linear differential equation with $\mathcal{G}(L) \subseteq \mathrm{SL}(2, \mathcal{C})$.*

(i) *$\mathcal{G}(L)$ is a reducible linear group if and only if the differential operator associated to $L(y)$ factors. In this case $L(y) = 0$ has an exponential solution.*
(ii) *If the previous case does not hold, then $\mathcal{G}(L)$ is an imprimitive linear group if and only if $L(y) = 0$ has a solution whose logarithmic derivative is algebraic of degree 2.*
(iii) *If the previous cases do not hold, then $\mathcal{G}(L)$ is a primitive finite linear group if and only if $L(y) = 0$ has a solution whose logarithmic derivative is algebraic of degree 4, 6 or 12.*
(iv) *If the previous cases do not hold, then $\mathcal{G}(L) = \mathrm{SL}(2, \mathcal{C})$ and $L(y) = 0$ has no Liouvillian solution.*

In the above result only the minimal degrees of an algebraic logarithmic derivative is mentioned. In this paper, in order to use invariants instead of semi-invariants, we will consider also other solutions, whose minimal polynomial is of higher degree.

2. Algebraic Solutions of the Riccati and Semi-invariants

Let $L(y) = y'' + a_1 y' + a_0 y$ be a second order equation with coefficients in k, and $\mathrm{Ri}(u) = u' + a_0 + a_1 u + u^2 = 0$ be the associated Riccati equation. We saw in Section 1.2 that, in order to compute a Liouvillian solution of $L(y) = 0$, one can compute the minimal polynomial $P(u) = u^m + b_{m-1}u^{m-1} + \cdots + b_0$ of an algebraic solution of $\mathrm{Ri}(u) = 0$. The main reason for the efficiency of the Kovacic algorithm is the fact that, for $k = \mathbb{C}(x)$ and

$a_1 = 0$, the coefficients of $P(u)$ are given by a linear recurrence from the knowledge of b_{m-1} (Kovacic, 1986; Duval and Loday-Richaud, 1992). In this section we give a proof of this fact without assuming that $\mathcal{G}(L)$ is unimodular or that $k = \mathbb{C}(x)$. The proof also applies to reducible polynomials, which will be fundamental to our approach.

A differential extension $k\{u\}$ of k by a differential variable u is obtained by adjoining to k a variable u and new variables u_i for the ith derivative of u. A derivation Δ on $k\{u\}$ is defined by $\Delta(a) = \delta(a)$ for $a \in k$ and $\Delta(u) = u_1$ which we also denote by u', $\Delta^2(u) = u_2, \ldots$. Note that one can also consider u as a usual variable and that we have $k[u] \subset k\{u\}$ which will result in some abuse of notation in what follows. Also note that Δ is not a derivation on $k[u]$ and that in the following we will consider simultaneously different derivations among which some are derivations on $k[u]$ and some are not.

Definition 2.1. *Let $P \in k[u]$ and D be a derivation on $k[u]$. A polynomial P is called* special *for D if P divides $D(P)$ in $k[u]$.*

The special polynomials exist in wider contexts (Weil, 1994, and references therein).

Lemma 2.2. *If $P_1, P_2 \in k[u]$ are special for a derivation D on $k[u]$, then P_1P_2 is special for D. Conversely, if P is special for D, then all its factors are special for D.*

Proof. If $D(P_1) = Q_1P_1$ and $D(P_2) = Q_2P_2$ with $Q_1, Q_2 \in k[u]$, then $D(P_1P_2) = D(P_1)P_2 + P_1D(P_2) = (Q_1 + Q_2)P_1P_2$.

Conversely, suppose that $D(P) = Q \cdot P$ with $Q \in k[u]$. If $P = P_1^n P_2$ where P_1 is prime and P_1 and P_2 are relatively prime, then $D(P) = QP_1^nP_2 = nP_1^{n-1}D(P_1)P_2 + P_1^nD(P_2)$. Since P_1^n divides both sides and P_1 is prime with P_2, P_1 must divide $D(P_1)$. Similarly P_2 must divides $D(P_2)$. By induction it follows that all irreducible factors of P are special. □

Using the following two derivations on $k[u]$:

$$\partial_k \left(\sum_{i=0}^{m} b_i u^i \right) = \sum_{i=0}^{m} \delta(b_i) u^i$$
$$\frac{\partial}{\partial u} \left(\sum_{i=0}^{m} b_i u^i \right) = \sum_{i=0}^{m} i b_i u^{i-1}.$$

We define a derivation $\mathcal{D}_{L,k}$ on $k[u]$ by:

$$\mathcal{D}_{L,k}\left(P(u)\right) = \partial_k\left(P(u)\right) - (a_0 + a_1u + u^2)\frac{\partial}{\partial u}\left(P(u)\right).$$

The derivative of a polynomial $P(u) = \sum_{i=0}^{m} b_i u^i \in k[u] \subset k\{u\}$ by Δ can now be written:

$$\begin{aligned}\Delta\left(P(u)\right) &= \partial_k\left(P(u)\right) + u'\frac{\partial P}{\partial u}(u) \\ &= \partial_k\left(P(u)\right) - (a_0 + a_1u + u^2)\frac{\partial P}{\partial u}(u) + \left(u' + u^2 + a_0 + a_1u\right)\frac{\partial P}{\partial u}(u) \\ &= \mathcal{D}_{L,k}\left(P(u)\right) + \mathrm{Ri}(u) \cdot \frac{\partial P}{\partial u}(u).\end{aligned}$$

LEMMA 2.3. *If K is a differential field extension of k and $P(u) \in k[u]$ is special for $\mathcal{D}_{L,K}$, then $P(u)$ is special for $\mathcal{D}_{L,k}$*

PROOF. Since $P \in k[u]$ and $\delta(k) \subset k$, we have that $\mathcal{D}_{L,K}(P) = \mathcal{D}_{L,k}(P)$ is in $k[u]$. If P divides $\mathcal{D}_{L,k}(P)$ over $K[u]$, then, by the uniqueness of the euclidian division, P divides $\mathcal{D}_{L,k}(P)$ over $k[u]$. □

LEMMA 2.4. (WEIL, 1994) *All zeroes of $P \in k[u]$ are solutions of the Riccati equation if and only if P is special for $\mathcal{D}_{L,k}$.*

PROOF. Suppose that P is special and pick any irreducible factor P_1 which must again be special (Lemma 2.2). Since P_1 divides $\mathcal{D}_{L,k}(P_1)$, we have that $P_1(v) = 0$ implies $\mathcal{D}_{L,k}(P_1)(v) = 0$. Since P_1 is prime, it can not divide $\frac{\partial}{\partial u}(P_1)$. From

$$\Delta(P_1(u)) = \mathcal{D}_{L,k}(P_1)(u) + \mathrm{Ri}(u) \cdot \left(\frac{\partial}{\partial u} P_1\right)(u), \tag{2.1}$$

we finally get that if $P_1(v) = 0$, then $\mathrm{Ri}(v) = 0$. Since any zero of P is a zero of an irreducible factor, the result follows.

Conversely, suppose that all zeroes of $P(u)$ are zeroes of $\mathrm{Ri}(u)$. Pick an irreducible factor $P_1(u)$ of $P(u)$; then, reasoning as above, we get from (2.1) that, since $\mathrm{Ri}(u) = 0$, all zeroes of P_1 are zeroes of $\mathcal{D}_{L,k}(P_1)$ and thus that P_1 is special. Since all irreducible factors of $P(u)$ are special for $\mathcal{D}_{L,k}$, $P(u)$ is special for $\mathcal{D}_{L,k}$ (Lemma 2.2). □

Remark. This result also follows from Corrollary 1.6 and Lemma 1.10 of Bronstein (1990). ◇

A polynomial $P(u) = u^m + b_{m-1}u^{m-1} + \cdots + b_0$ is special if and only if $\mathcal{D}_{L,k}(P(u))$ is divisible by $P(u)$. Performing the division and setting the remainder equal to 0 gives the following system $(\sharp)_m$ for the coefficients b_i:

$$(\sharp)_m : \quad \begin{cases} b_m = 1 \\ b_{i-1} = \frac{-b_i' + b_{m-1}b_i + a_1(i-m)b_i + a_0(i+1)b_{i+1}}{m-i+1}, & m-1 \geq i \geq 0. \\ b_{-1} = 0 \end{cases}$$

Note that $P(u)$ is special if and only its coefficients b_i satisfy the above system. The last equation $b_{-1} = 0$ plays a central role in Kovacic (1986) but is not used in our proofs. From the form of the system we see that the coefficients b_i are all determined from the knowledge of the coefficient b_{m-1}. A special polynomial is thus uniquely determined by its degree m and by its coefficient b_{m-1}: we may say that such a b_{m-1} solves the system $(\sharp)_m$. Note that, if $P_1 = u^m + b_{m-1}u^{m-1} + \cdots$ and $P_2 = u^n + \beta_{n-1}u^{n-1} + \cdots$ are special, then $P_1P_2 = u^{m+n} + (b_{m-1} + \beta_{n-1})u^{m+n-1} + \cdots$ is also special and so $b_{m-1} + \beta_{n-1}$ solves the system $(\sharp)_{n+m}$. Our next step is to characterize the elements b_{m-1} of k which solve the system $(\sharp)_m$ and thus give a special polynomial of degree m.

THEOREM 2.1. *Let $L(y) = y'' + a_1y' + a_0y$ be a second order equation with $a_i \in k$, then all zeroes of $P(u) = u^m + \sum_{i=0}^{m-1} b_iu^i$ with $b_i \in k$ are solutions of the Riccati equation $\mathrm{Ri}(u) = 0$ if and only if*

(1) *the coefficient b_{m-1} is the negative logarithmic derivative of an exponential solution*

(over k) of $L^{\circledS m}(y) = 0$, i.e. b_{m-1} is the negative logarithmic derivative of a semi-invariant of $\mathcal{G}(L) \subseteq \mathrm{GL}(2, \mathcal{C})$.

(2) *for $i < m-1$ the coefficients b_i of P are determined from b_{m-1} by the system $(\sharp)_m$.*

PROOF. Suppose that $P(u) \in k[u]$ is special. From Lemma 2.4 we get that all zeroes of $P(u) = 0$ are solutions of $\mathrm{Ri}(u) = 0$. From relation (1.4) we get that b_{m-1} is the negative logarithmic derivative of an exponential solution of $L^{\circledS m}(y) = 0$.

We now show that any exponential solution z of a $L^{\circledS m}(y) = 0$ yields a special polynomial of degree m. Consider the polynomial $P(u) = u^m + \sum_{i=0}^{m-1} b_i u^i$, where $b_{m-1} = -z'/z$ and where the other coefficients $b_{m-2}, \ldots, b_0$ are given according to the recurrence $(\sharp)_m$. Since $b_{m-1} \in k$, all b_i will also be in k and thus $P(u) \in k[u]$. Let y_1, y_2 be a fundamental system of solutions of $L(y) = 0$ and (K, Δ) be a PVE of (k, δ) for $L(y) = 0$. Since z is a semi-invariant of degree m of $\mathcal{G}(L)$, it can be written as a homogeneous form $z = F(y_1, y_2)$ of degree m in y_1, y_2 over $\mathcal{C}$. As $\mathcal{C}$ is algebraically closed, $F(y_1, y_2)$ can be factored over K as a product of m linear forms: $F(y_1, y_2) = \prod_{i=1}^{m} (\beta_i y_1 - \alpha_i y_2)$ with $\beta_i, \alpha_i \in \mathcal{C}$. We note that $u_i = \Delta(\beta_i y_1 - \alpha_i y_2)/(\beta_i y_1 - \alpha_i y_2)$ is a solution of $\mathrm{Ri}(u) = 0$. Thus all zeros of the polynomial $Q(u) = \prod_{i=1}^{m} (u - u_i) \in K[u]$ are solutions of $\mathrm{Ri}(u) = 0$. The polynomial $Q(u) = 0$ must be special for $\mathcal{D}_{L,K}$ (Lemma 2.4) and its coefficients must satisfy $(\sharp)_m$. In particular, since $z'/z = -b_{m-1} = \sum_{i=1}^{m} u_i$, the coefficients of $Q(u) = 0$ are in k. Since $P(u)$ and $Q(u)$ are of the same degree and are both constructed from z'/z and $(\sharp)_m$, we have $P(u) = Q(u)$. The polynomial $P(u) = Q(u)$ is special for $\mathcal{D}_{L,K}$ and has coefficients in k. By Lemma 2.3, $P(u)$ is also special for $\mathcal{D}_{L,k}$. From Lemma 2.4 we get that all roots of $P(u) = 0$ are solutions of $\mathrm{Ri}(u) = 0$. □

This gives a bijection between monic polynomials of degree m over k whose roots are solutions of the Riccati equation and exponential solutions of $L^{\circledS m}(y) = 0$, i.e. semi-invariants of degree m of $\mathcal{G}(L)$. In particular, if z_1 and z_2 are two semi-invariants, then the special polynomial associated with the product $z_1 z_2$ is the product of the special polynomials associated with z_1 and z_2 respectively. In the sequel, we will use this remark without further mention.

For higher order linear differential equations, the minimum polynomial of an algebraic solution of the Riccati equation is no longer special, and the bijection does not exist any more.

3. The Algorithm

In this section, we will always assume that $L(y)$ is a second order equation with $\mathcal{G}(L) \subseteq \mathrm{SL}(2, \mathcal{C})$. The previous section shows that there is a bijection between exponential solutions of $L^{\circledS m}(y) = 0$ and polynomials of degree m whose zeroes are solutions of the Riccati. We now propose an algorithm where rational solutions of $L^{\circledS m}(y) = 0$ are used as much as possible instead of exponential solutions.

The proposed algorithm can be outlined as follows:

(i) Test if $L(y)$ has a non-trivial rational (and thus Liouvillian) solution.

(ii) Test if $L^{\circledS 2}$ has a non-trivial rational solution. If it is the case, then $\mathcal{G}(L)$ is a reducible subgroup of $\mathrm{SL}(2, \mathcal{C})$.

  (a) If the space of rational solutions of $L^{\circledS 2}$ is of dimension 3, then $\mathcal{G}(L) = \{id, -id\}$

and any special polynomial $P(u)$ of degree 2 associated to a non-trivial rational solution of $L^{\circledS 2}$ is reducible. A factor of $P(u)$ gives a Liouvillian solution.

(b) If the previous case does not hold, then $\mathcal{G}(L)$ is a completely reducible group if an only if the special polynomial $P(u)$ of degree 2 associated to a non-trivial rational solution of $L^{\circledS 2}$ factors but is not a square. The two factors of $P(u)$ give two exponential solutions.

(c) If the above cases do not hold, then the special polynomial $P(u)$ of degree 2 associated to a non-trivial rational solution of $L^{\circledS 2}$ is either a square or is irreducible. In both cases a Liouvillian solution is found.

(iii) Test if $L(y) = 0$ has a non-trivial exponential (and thus Liouvillian) solution. Such a solution must then be unique and gives a unique right factor of order one of $L(y)$.

(iv) Test if $L^{\circledS 4}$ has non-trivial rational solutions. The special polynomial $P(u)$ associated to an arbitrary non-trivial rational solution of $L^{\circledS 4}$ is either the square of an irreducible special polynomial of order 2 or is irreducible.

(v) Test for increasing $m \in \{6, 8, 12\}$ if $L^{\circledS m}$ has a non-trivial rational solution. The corresponding special polynomial will be irreducible.

(vi) Conclude that $L(y) = 0$ has no Liouvillian solution.

The steps have to be performed in the given order and the algorithm terminates as soon as a solution is found in one of the cases. The third step is the only one where instead of some rational solution one has to compute an exponential solution of $L(y)$ (which is, however, known to be unique in this case). We note that it is not difficult to test if a special polynomial $P(u)$, known to be either irreducible or a square, is a square. This is the case if and only if $Q(u) = \gcd\left(P(u), \frac{d}{du}P(u)\right)$ is not constant in u, in which case, under the given assumption, $(Q(u))^2 = P(u)$.

In the remainder of this section we prove that the proposed algorithm is correct and compute examples in each case.

3.1. THE REDUCIBLE CASE

Proposition 4.2 of Singer and Ulmer (1993a) describes the reducible Galois groups, in particular if L has a rational solution. The next lemma complements this proposition.

LEMMA 3.1. *Let $L(y)$ be a second order equation with $\mathcal{G}(L) \subseteq \mathrm{SL}(2, \mathcal{C})$ having no non-trivial rational solutions. If $L^{\circledS 2}(y) = 0$ has a non-trivial rational solution, then $\mathcal{G}(L)$ is a reducible subgroup of $\mathrm{SL}(2, \mathcal{C})$.*

(i) *If the space of rational solutions of $L^{\circledS 2}$ is of dimension 3, then $\mathcal{G}(L) = \{id, -id\}$ and any special polynomial $P(u)$ associated to a non-trivial rational solution of $L^{\circledS 2}$ factors.*

(ii) *If the previous case does not hold, then $\mathcal{G}(L)$ is a completely reducible group if and only if the special polynomial $P(u)$ associated to a non-trivial rational solution of $L^{\circledS 2}$ factors but is not a square. The two factors of $P(u)$ give two exponential solutions which are linearly independent over $\mathcal{C}$.*

(iii) *If the above cases do not hold, then the special polynomial $P(u)$ associated to a non-trivial rational solution of $L^{\circledS 2}$ is either a square or is irreducible. In both cases a Liouvillian solution is found.*

PROOF. We first note that if $\mathcal{G}(L) \subseteq \mathrm{SL}(2,\mathcal{C})$ is irreducible (i.e. primitive or imprimitive), then $L^{\circledS 2}$ has no non-trivial rational solution because there is no invariant of degree 2 in those cases (cf. proofs of Lemmas 3.2 and 3.3). Thus, if $L^{\circledS 2}(y) = 0$ has a non-trivial rational solution, then $\mathcal{G}(L) \subseteq \mathrm{SL}(2,\mathcal{C})$ is reducible.

Assume that $\mathcal{G}(L)$ is completely reducible. For a basis denoted $\{y_1, y_2\}$ all elements g of $\mathcal{G}(L)$ must be of the form

$$g = \begin{pmatrix} a_g & 0 \\ 0 & a_g^{-1} \end{pmatrix}.$$

In particular y_1 and y_2 are semi-invariants and $y_1 y_2$ is an invariant of $\mathcal{G}(L)$.

(i) If $\mathcal{G}(L)$ has another linearly independent invariant of degree two, say $F(y_1, y_2) = \alpha(y_1)^2 + \beta(y_2)^2$, then, for $g \in \mathcal{G}(L)$, we have $g \cdot F(y_1, y_2) = a_g^2 \alpha(y_1)^2 + a_g^{-2}\beta(y_2)^2$. Thus $\forall g \in \mathcal{G}(L), a_g^2 = 1$ and we get $\mathcal{G}(L) = \{id, -id\}$. In this case any homogeneous form of degree 2 is invariant and $L^{\circledS 2}(y) = 0$ has a rational solution space of dimension 3. Any solution of $L(y) = 0$ is an exponential solution and thus any polynomial $P(u)$ factors into two linear polynomials.

(ii) If $\mathcal{G}(L)$ has no other linearly independent invariant of degree two, then any rational solution of $L^{\circledS 2}(y) = 0$ is a multiple of $y_1 y_2$ and factors. The polynomial $P(u)$ associated to a non-trivial rational solution of $L^{\circledS 2}(y) = 0$ will be the product of the distinct minimal polynomials associated to the semi-invariants y_1 and y_2. In particular, $P(u)$ is not a square.

Suppose that $P(u)$ factors but is not a square, then each factor is a special polynomial of order one corresponding to a different logarithmic derivative z_1'/z_1 and z_2'/z_2. The corresponding solutions z_1 and z_2 must be linearly independent over $\mathcal{C}$. In the basis $\{z_1, z_2\}$, the group $\mathcal{G}(L)$ is diagonal and thus completely reducible.

The only cases left are those where $\mathcal{G}(L) \neq \{id, -id\}$ and $P(u)$ is a square or is irreducible over $k[u]$. By the above, $\mathcal{G}(L)$ is reducible, but cannot be completely reducible. □

Remark. The fact that factorization of differential operators is easier in the completely reducible case was used by Singer (1996). ◇

An example of a completely reducible group is the example given in Section 1.2 which we now summarize:

Example. Let $L(y) = y'' + \frac{3}{16x^2}y$. This equation has no non-trivial rational solution, and the equation $L^{\circledS 2}(y) = 0$ has a one-dimensional space of rational solutions generated by x. Thus $\mathcal{G}(L) \subseteq \mathrm{SL}(2,\mathcal{C})$ is a reducible group and $L(y) = 0$ factors. Since the rational solution space of $L^{\circledS 2}(y) = 0$ is not of dimension 3, we have $\mathcal{G}(L) \neq \{id, -id\}$. The special polynomial obtained from the logarithmic derivative $1/x$ of x is

$$u^2 - \frac{1}{x}u + \frac{3}{16x^2}$$

which factors into $\left(u - \frac{1}{4x}\right)\left(u - \frac{3}{4x}\right)$. Since $P(u)$ is not a square, $\mathcal{G}(L) \subseteq \mathrm{SL}(2,\mathcal{C})$ is a completely reducible group. From the factorization of $P(u)$, we get the following two Liouvillian solutions of $L(y) = 0$:

$$y_1 = e^{\int \frac{1}{4x}}, \qquad y_2 = e^{\int \frac{3}{4x}}.$$

Viewed as an operator, L is the least common left multiple of $\delta - \frac{1}{4x}$ and $\delta - \frac{3}{4x}$. $\diamond$

In the following example, we deal with a reducible but not completely reducible linear group:

Example. Consider $L(y) = y'' + \left(\frac{3}{16x^2} + \frac{1}{4(x-1)^2} - \frac{1}{4x(x-1)}\right)y$. The equation $L^{\circledS 2}(y) = 0$ has no non-trivial rational solution and thus $\mathcal{G}(L) \subseteq \mathrm{SL}(2,\mathcal{C})$ has no invariant of degree 2. In this case the exponential solution $e^{\int \frac{3x-1}{4x(x-1)}}$ is a semi-invariant of degree one, but there exists no other linearly independent semi-invariant of degree one. We thus get a unique polynomial $P(u) = u - \frac{3x-1}{4x(x-1)}$ of degree one. The group $\mathcal{G}(L) \subseteq \mathrm{SL}(2,\mathcal{C})$ is reducible but not completely reducible.
We note that even if no invariant of degree two exists, there could exist other invariants of higher degree. In this example $L^{\circledS 4}$ has a one-dimensional rational solution space generated by $x(x-1)^2$.
The example shows that, even if no invariant of degree 2 exists, the equation $L(y)$ could be reducible, and that in order to proceed in the algorithm, one must look for exponential solutions of $L(y) = 0$ at this stage. $\diamond$

3.2. THE IMPRIMITIVE CASE

In this case we show that the computation of a Liouvillian solution of a second order equation $L(y) = 0$ is reduced to the computation of a rational solution of $L^{\circledS 4}(y) = 0$ and that the special polynomial associated to the logarithmic derivative is either a square or irreducible. In this section we need to assume that $L(y) = 0$ is an irreducible equation.

LEMMA 3.2. *Let $L(y) = 0$ be an irreducible second order equation over K whose Galois group $\mathcal{G}(L)$ is unimodular. Then $\mathcal{G}(L)$ is an imprimitive subgroup of* $\mathrm{SL}(2,\mathcal{C})$ *if and only if $L^{\circledS 4}$ has a rational solution q. The special polynomial obtained from the logarithmic derivative of q is then*

(i) *The square of a unique special polynomial of degree* 2 *if $L^{\circledS 4}$ has a one-dimensional rational solution space.*
(ii) *Either the square of a special polynomial of degree* 2 *or is irreducible if $L^{\circledS 4}$ has a two-dimensional rational solution space, in which case $\mathcal{G}(L) \cong D_2^{\mathrm{SL}_2}$.*

PROOF. Denote $\{y_1, y_2\}$ a basis in which all $g \in \mathcal{G}(L) \subseteq \mathrm{SL}(2,\mathcal{C})$ are simultaneously in the form

$$\begin{pmatrix} a_g & 0 \\ 0 & a_g^{-1} \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} 0 & -a_g \\ a_g^{-1} & 0 \end{pmatrix}$$

(cf. Section 1.3). Since $\forall g \in \mathcal{G}(L)$ we have $g(y_1y_2) = \pm y_1y_2$, we get that y_1y_2 is a semi-invariant of degree 2 and that $y_1^2y_2^2$ is an invariant of degree 4 of $\mathcal{G}(L)$. Since $L^{\circledS 4}(y) = 0$ has no rational solution if $\mathcal{G}(L)$ is a primitive subgroup of $\mathrm{SL}(2,\mathcal{C})$ (cf. character decompositions of the finite primitive groups in the next subsection and Springer, 1973, for $\mathrm{SL}(2,\mathcal{C})$), we get the first assertion (this result is also proven in Singer and Ulmer, 1993a, Theorem 4.1 or Kovacic, 1986, p. 20).

If the space of rational solutions of $L^{\circledS 4}$ is one dimensional then, up to a constant multiple, this rational solution is the square of y_1y_2. Thus, the (unique) special polynomial

corresponding to the (unique) logarithmic derivative of a rational solution $y_1^2 y_2^2$ of $L^{\circledS 4}$ will be the square of the special polynomial associated with the semi-invariant $y_1 y_2$. Note that the special polynomial associated with $y_1 y_2$ must be irreducible, because $\mathcal{G}(L)$ is irreducible and thus has no semi-invariants of degree 1. Since for second order equations there is a bijection between rational solutions and invariants, we now look at the ring of invariants to see if the $\mathcal{C}$-subspace of invariants of degree 4 is of dimension 1. As shown in Springer (1973, p. 95), the ring of invariants of $D_n^{\mathrm{SL}_2}$ is generated by:

$$I_1 = y_1^2 y_2^2, I_2 = y_1^{2n} + (-1)^n y_2^{2n}, I_3 = y_1 y_2 (y_1^{2n} - (-1)^n y_2^{2n}).$$

The group D_∞ has up to scalar multiples only one invariant $y_1^2 y_2^2$ of degree 4. To see this one looks at the diagonal subgroup and, as in the proof of Lemma 3.1, shows that this diagonal subgroup would be of order at most 4 making D_∞ finite, a contradiction. Thus the group $D_2^{\mathrm{SL}_2}$ is the only imprimitive group for which the space of rational solutions of $L^{\circledS 4}$ is of dimension 2 and not 1.

The group $D_2^{\mathrm{SL}_2}$ has 5 irreducible characters, the trivial one denoted $\mathbf{1}$, 3 characters $\zeta_{1,1}$, $\zeta_{1,2}$, $\zeta_{1,3}$ of degree one and one character ζ_2 of degree two. The non-trivial characters of degree one have the property that the product $\zeta_{1,i}\zeta_{1,j}$ is $\mathbf{1}$ for $i = j$ and different from $\mathbf{1}$ otherwise. If a second order equation $L(y) = 0$ has Galois group $\mathcal{G}(L) \cong D_2^{\mathrm{SL}_2}$, then the corresponding character of $\mathcal{G}(L)$ will be ζ_2. The character χ_m of $\mathcal{G}(L^{\circledS m})$ can be computed according to the formula given in Singer and Ulmer (1993a, p. 15):

$$\chi_2 = \zeta_{1,1} + \zeta_{1,2} + \zeta_{1,3}, \qquad \chi_3 = 2\zeta_2, \qquad \chi_4 = 2 \cdot \mathbf{1} + \zeta_{1,1} + \zeta_{1,2} + \zeta_{1,3}$$

this shows that there are three semi-invariants S_i associated to the characters $\zeta_{1,i}$ ($i \in \{1, 2, 3\}$) whose squares are rational. The products $S_1 S_2$, $S_1 S_3$ and $S_2 S_3$ are not invariants (i.e. do not correspond to a rational solution) since the products of the associated characters are not the trivial character. Thus a rational solution of $L^{\circledS 4}$ is either the square of a semi-invariant S_i of order 2 (in which case the associated special polynomial will be a square), or it is not the product of semi-invariants and the associated special polynomial is irreducible. □

Example. Consider the irreducible equation

$$L(y) = y'' - \frac{2}{2x-1} y' + \frac{\left(27x^4 - 54x^3 + 5x^2 + 22x + 27\right)(2x-1)^2}{144x^2(x-1)^2(x^2-x-1)^2} y = 0.$$

It is unimodular because $\frac{2}{2x-1}$ is the logarithmic derivative of $2x - 1$. The equation $L^{\circledS 4}(y) = 0$ has a one-dimensional space of rational solutions generated by $x(x-1)(x^2-x-1)^2$. The special polynomial that is associated with the logarithmic derivative $\frac{(2x-1)(3x^2-3x-1)}{(x^2-x-1)(x-1)x}$ is:

$$\begin{aligned} u^4 &- \frac{(2x-1)(3x^2-3x-1)}{(x^2-x-1)(x-1)x} u^3 \\ &+ \frac{(2x-1)^2(243x^4-486x^3+77x^2+166x+27)}{72x^2(x-1)^2(x^2-x-1)^2} u^2 \\ &- \frac{(81x^4-162x^3+23x^2+58x+9)(2x-1)^3(3x^2-3x-1)}{144x^3(x-1)^3(x^2-x-1)^3} u \end{aligned}$$

$$+\frac{(81x^4-162x^3+23x^2+58x+9)^2(2x-1)^4}{20736x^4(x-1)^4(x^2-x-1)^4}$$

which is the square of:

$$u^2-\frac{(2x-1)\left(3x^2-3x-1\right)}{2x(x-1)(x^2-x-1)}u+\frac{(81x^4-162x^3+23x^2+58x+9)(2x-1)^2}{144x^2(x-1)^2(x^2-x-1)^2}.$$

Since $L^{\circledS 6}$ also has a rational solution $x^2(x-1)^2(x^2-x-1)^2$, we get from the above proof that $\mathcal{G}(L)$ is $D_3^{\mathrm{SL}_2}$ $\diamond$

The next example has a Galois group $\mathcal{G}(L)\cong D_2^{\mathrm{SL}_2}$

Example. Consider the irreducible equation

$$L(y)=y''-\frac{2}{2x-1}y'+\frac{3(2x-1)^2\left(x^4-2x^3+x+1\right)}{16x^2(x-1)^2\left(x^2-x-1\right)^2}y.$$

The fourth symmetric power has a two-dimensional rational solution space generated by $J_0=x(x-1)\left(x^2-x-1\right)$ and $J_1=x(x-1)\left(x^2-x+1\right)\left(x^2-x-1\right)$. Thus, $\mathcal{G}(L)$ is the quaternion group and we get the following two special polynomials:

$$\begin{aligned}&u^4-\frac{(2x-1)(2x^2-2x-1)}{x(x-1)(x^2-x-1)}u^3+\frac{(2x-1)^2(11x^4-22x^3+11x+3)}{8x^2(x-1)^2(x^2-x-1)^2}u^2\\&\quad-\frac{(2x-1)^3(2x^2-2x-1)(3x^4-6x^3+3x+1)}{16x^3(x-1)^3(x^2-x-1)^3}u\\&\quad+\frac{(3x^4-6x^3+3x+1)^2(2x-1)^4}{256x^4(x-1)^4(x^2-x-1)^4}\end{aligned}$$

and

$$\begin{aligned}&u^4-\frac{(2x-1)(3x^4-6x^3+3x^2-1)}{x(x-1)(x^2-x+1)(x^2-x-1)}u^3\\&\quad+\frac{3(2x-1)^2(9x^6-27x^5+19x^4+7x^3-8x^2+1)}{8x^2(x-1)^2(x^2-x-1)^2(x^2-x+1)}u^2\\&\quad-\frac{(2x-1)^3(27x^8-108x^7+117x^6+27x^5-86x^4+x^3+21x^2+x-1)}{16x^3(x-1)^3(x^2-x-1)^3(x^2-x+1)}u\\&\quad+\frac{(2x-1)^4(81x^{10}-405x^9+621x^8-54x^7-572x^6+204x^5+231x^4-55x^3-48x^2-3x+1)}{256x^4(x-1)^4(x^2-x-1)^4(x^2-x+1)}.\end{aligned}$$

From the theorem, we know that each polynomial is either a square or is irreducible. In this example, the first polynomial is a square and the second is irreducible. $\diamond$

3.3. THE PRIMITIVE CASE

The following shows that for the primitive case it is always possible to look only for rational solutions of symmetric powers. However the algebraic solution of the Riccati found this way will not be of lowest algebraic degree for $A_4^{\mathrm{SL}_2}$ and $S_4^{\mathrm{SL}_2}$.

LEMMA 3.3. *Let $L(y)=0$ be a second order equation whose differential Galois group $\mathcal{G}(L)$ is a finite primitive subgroup of* $\mathrm{SL}(2,\mathcal{C})$.

- *If* $\mathcal{G}(L) \cong A_4^{\mathrm{SL}_2}$*, then the unique special polynomial obtained from the logarithmic derivative of a non-trivial rational solution of* $L^{\circledS 6}$ *is irreducible.*
- *If* $\mathcal{G}(L) \cong S_4^{\mathrm{SL}_2}$*, then the unique special polynomial obtained from the logarithmic derivative of a non-trivial rational solution of* $L^{\circledS 8}$ *is irreducible. Also the unique special polynomial obtained from the logarithmic derivative of a non-trivial rational solution of* $L^{\circledS 12}$ *is the square of a unique special polynomial of degree* 6.
- *If* $\mathcal{G}(L) \cong A_5^{\mathrm{SL}_2}$*, then the unique special polynomial obtained from the logarithmic derivative of a non-trivial rational solution of* $L^{\circledS 12}$ *is irreducible.*

In all cases, it is the special polynomial of lowest order that one can construct using rational *solutions of symmetric powers of* $L(y)$.

Proof. The (abstract) group $A_4^{\mathrm{SL}_2}$ has seven irreducible characters, the trivial one denoted $\mathbf{1}$, two characters $\zeta_{1,1}$ and $\zeta_{1,2}$ of degree 1, two characters $\zeta_{2,1}$ and $\zeta_{2,2}$ of degree 2 (where the trace of an element of order 3 is different from one and thus the representation is not in $\mathrm{SL}(2,\mathcal{C})$), another character ζ_2 of degree two (corresponding to a representation in $\mathrm{SL}(2,\mathcal{C})$) and a character ζ_3 of degree 3. If a second order equation $L(y) = 0$ has Galois group $\mathcal{G}(L) \cong A_4^{\mathrm{SL}_2}$, then the corresponding character of $\mathcal{G}(L)$ will be $\chi = \zeta_2$. The character χ_m of $\mathcal{G}(L^{\circledS m})$ can be computed according to the formula given in Singer and Ulmer (1993a, p. 15):

$$\begin{array}{lll} \chi_2 = \zeta_3 & \chi_4 = \zeta_{1,1} + \zeta_{1,2} + \zeta_3 & \chi_6 = \mathbf{1} + 2\zeta_3 \\ \chi_3 = \zeta_{2,1} + \zeta_{2,2} & \chi_5 = \zeta_{2,1} + \zeta_{2,2} + \zeta_2. & \end{array}$$

Since there are no semi-invariants of degree 2 or 3, the unique special polynomial obtained from the logarithmic derivative of a rational solution of $L^{\circledS 6}$ cannot be the product of special polynomials of lower order.

The proof in the other cases are similar and can be deduced from the decompositions that follow:

- The (abstract) group $S_4^{\mathrm{SL}_2}$ has eight irreducible characters, the trivial one $\mathbf{1}$, another character $\zeta_{1,1}$ of degree 1, one character ζ_2 of degree 2 which is not faithful, two (conjugate) characters $\zeta_{2,0}$ and $\zeta_{2,1}$ of degree 2 (corresponding to representations in $\mathrm{SL}(2,\mathcal{C})$), two characters $\zeta_{3,1}$ and $\zeta_{3,2}$ of degree 3 and a character ζ_4 of degree 4. For $\zeta_{2,i}$ we set $j \equiv i+1 \pmod 2$ and get:

  $$\begin{array}{lll} \chi_2 = \zeta_{3,1} & \chi_5 = \zeta_{2,j} + \zeta_4 & \chi_8 = \mathbf{1} + \zeta_2 + \zeta_{3,1} + \zeta_{3,2} \\ \chi_3 = \zeta_4 & \chi_6 = \zeta_{1,1} + \zeta_{3,1} + \zeta_{3,2} & \chi_{12} = \mathbf{1} + \zeta_{1,1} + \zeta_2 + \zeta_{3,1} + 2\zeta_{3,2} \\ \chi_4 = \zeta_2 + \zeta_{3,2} & \chi_7 = \zeta_{2,i} + \zeta_{2,j} + \zeta_4. & \end{array}$$

  In the above case we note that the character χ_{12} as a unique trivial summand and thus that $L^{\circledS 12}(y) = 0$ has a one-dimensional rational solution space and thus that (up to multiples) there is a unique invariant of degree 12. But this invariant must be the square of the semi-invariant of degree 6 since the one-dimensional character $\zeta_{1,1}$ is of order 2. The special polynomial associated to the invariant of degree 12 must be the square of the unique special polynomial of degree 6.
- The (abstract) group $A_5^{\mathrm{SL}_2}$ has nine irreducible characters, the trivial one $\mathbf{1}$, two (conjugate) characters $\zeta_{2,0}$ and $\zeta_{2,1}$ of degree 2 (corresponding to two representations in $\mathrm{SL}(2,\mathcal{C})$), two characters $\zeta_{3,1}$ and $\zeta_{3,2}$ of degree 3, two characters $\zeta_{4,1}$ and $\zeta_{4,2}$ of degree 4, a character ζ_5 of degree 5 and a character ζ_6 of degree 6. For

$\zeta_{2,i}$ we set $j \equiv i+1 \pmod 2$ and get:

$$\begin{array}{lll} \chi_2 = \zeta_{3,i} & \chi_6 = \zeta_{3,j} + \zeta_{4,2} & \chi_{10} = \zeta_{3,1} + \zeta_{3,2} + \zeta_5 \\ \chi_3 = \zeta_{4,1} & \chi_7 = \zeta_{2,j} + \zeta_6 & \chi_{11} = \zeta_{2,i} + \zeta_{4,1} + \zeta_6 \\ \chi_4 = \zeta_5 & \chi_8 = \zeta_{4,2} + \zeta_5 & \chi_{12} = \mathbf{1} + \zeta_{3,i} + \zeta_{4,2} + \zeta_5. \\ \chi_5 = \zeta_6 & \chi_9 = \zeta_{4,1} + \zeta_6. & \end{array}$$

□

Example. Consider the irreducible equation

$$L(y) = y'' - \left(-\frac{3}{16x^2} - \frac{2}{9(x-1)^2} + \frac{3}{16x(x-1)} \right) y.$$

This equation is studied in Kovacic (1986, p. 23), where a minimal polynomial of degree 4 of an algebraic solution of the Riccati equation is given. This minimal polynomial corresponds to an exponential solution of $L^{\circledS 4}$ which is not rational, but which is the cube root of a rational function. The same equation is also studied in Singer and Ulmer (1993b, p. 68) where the minimal polynomial of a solution (not of a logarithmic derivative) is computed.

Using our approach, since $L^{\circledS 4}$ has no rational solution we know that $\mathcal{G}(L)$ is a primitive subgroup of $\mathrm{SL}(2,\mathcal{C})$. Since $L^{\circledS 6}$ has a rational solution $x^2(x-1)^2$, we get that $\mathcal{G}(L)$ is the tetrahedral group and that the special polynomial associated with the logarithmic derivative $\frac{4x-2}{x^2-x}$ will be irreducible. This gives the following minimal polynomial for an algebraic solution of the Riccati:

$$\begin{aligned} & u^6 - 2\frac{(2x-1)}{x(x-1)}u^5 + \frac{5(64x^2-63x+15)}{48x^2(x-1)^2}u^4 \\ & - \frac{5(512x^3-745x^2+351x-54)}{432x^3(x-1)^3}u^3 \\ & + \frac{5(4096x^4-7840x^3+5485x^2-1674x+189)}{6912x^4(x-1)^4}u^2 \\ & - \frac{(3645x-16254x^2+35781x^3-38720x^4+16384x^5-324)}{20736x^5(x-1)}u \\ & + \frac{-29889x+169209x^2-506331x^3+842008x^4+262144x^6-735232x^5+2187}{2985984x^6(x-1)^6}. \end{aligned}$$

◇

4. Rationality Problem

In order to use differential Galois theory and in particular the existence of a PVE for $L(y) = 0$, we needed to assume that the field of constants of the coefficient field is algebraically closed of characteristic 0. This implies that even if the coefficients of $L(y) = 0$ belong to $\mathbb{Q}(x)$, the coefficient of a special polynomial could be in $\overline{\mathbb{Q}}(x)$ but not in $\mathbb{Q}(x)$. The question of which algebraic extension of the constant field is needed to represent a special polynomial is studied in Hendriks and van der Put (1993,1995) and Ulmer (1994). The following result is trivial but useful, since it connects the approach used in this paper to the rationality problem:

LEMMA 4.1. *Let $L(y) = 0$ be a linear differential equations whose coefficients belong to a differential field $k_0 \subseteq \mathbb{C}(x) = k$. If a special polynomial $P(u)$ is obtained from an invariant of degree m corresponding to a solution in k_0 of $L^{\circledS m}(y) = 0$, then the coefficients of $P(u)$ are in k_0, i.e. no algebraic extension is needed to represent the coefficients of this particular special polynomial $P(u)$.*

To see how to use this result we note that:

(i) The coefficient of any symmetric power $L^{\circledS m}(y)$ of $L(y)$ are obtained by solving a linear system over k_0 and thus also belong to k_0.
(ii) An invariant of degree m is a rational solution of $L^{\circledS m}(y) = 0$. By Theorem 9.1 of Bronstein (1992), there exists a basis of the rational solution space of $L^{\circledS m}(y) = 0$ in k_0 which can be computed without extending the constant field[†].
(iii) If the invariant and thus b_{m-1} is in k_0, then all other coefficients of $P(u)$ obtained by the recurrence $(\sharp)_m$ will also be in k_0.

In what follows we assume (e.g. using the algorithm given in Bronstein, 1992, Theorem 9.1) that all computed invariants from now on are in k_0, the smallest field containing the coefficients. Thus, if a special polynomial can be computed using an invariant of some degree (i.e. a rational solution of some symmetric power), then this special polynomial also has coefficients in k_0. Our results imply that this is possible in all cases except for the non-reductive subgroups $\mathcal{G}(L) \subseteq \mathrm{SL}(2, \mathcal{C})$. For reducible non-reductive groups, there is a unique exponential solution, and so the result of Hendriks and van der Put (1995) quoted above shows that no extension of the constant field is needed to express this solution[‡]. Thus, one can always find (at least) *one* special polynomial without increasing the constant field.

4.1. THE REDUCIBLE CASE

If we are in a non-completely reducible case then, as seen just above, there a unique exponential solution and its logarithmic derivative lies in k_0.

In Section 3.1, we showed that the Galois group $\mathcal{G}(L) \neq \{id, -id\}$ is reducible and completely reducible if and only if it has an invariant of degree 2 such that the corresponding special polynomial factors but is not a square. In that case, an algebraic extension of degree 2 of the constant field may be needed to factor the special polynomial, as shown in this example:

Example. Consider $L(y) = y'' + \frac{7}{16x^2}y$ whose coefficients belong to $k_0 = \mathbb{Q}(x) \subset \overline{\mathbb{Q}}(x) = k$. A rational solutions of $L^{\circledS 2}$ is x and we get the special polynomial

$$u^2 - \frac{1}{x}u + \frac{7}{16x^2}.$$

[†] If $L(y) = 0$ has coefficients in $k_0 = \mathcal{C}_0(x)$ and V is the $\mathcal{C}_0$-space of solutions of $L(y) = 0$ in k_0, then $W = \overline{\mathcal{C}_0} \otimes_{\mathcal{C}_0} V$ is the $\overline{\mathcal{C}_0}$-space of solutions of $L(y) = 0$ in $\overline{\mathcal{C}_0}k_0$. In particular, a $\mathcal{C}_0$-basis of V will be a $\overline{\mathcal{C}_0}$-basis of W.

[‡] However, it is not certain yet that an extension of the constant field will not be needed during the computational process that provides this unique exponential solution.

This special polynomial is irreducible over $\mathbb{Q}(x)$, but factors over $\mathbb{Q}(\sqrt{-3})(x)$ into

$$\left(u - \frac{2-\sqrt{-3}}{4x}\right)\left(u - \frac{2+\sqrt{-3}}{4x}\right).$$

We get the following two Liouvillian solutions of $L(y) = 0$:

$$y_1 = e^{\int \left(\frac{2-\sqrt{-3}}{4x}\right)}, \qquad y_2 = e^{\int \left(\frac{2+\sqrt{-3}}{4x}\right)}.$$

$\diamond$

4.2. THE IRREDUCIBLE CASE

For irreducible equations $L(y) = 0$ we showed how to construct an irreducible special polynomial using an invariant. So, in this case, no algebraic extension of the coefficient field is needed to represent a solution. But, for the quaternion and the tetrahedral groups, the special polynomial proposed is not of minimal degree. To construct the special polynomial of minimal degree, an algebraic extension of k_0 is sometimes necessary. In fact, there are exactly two cases when one may need to augment the constant field; we now detail them.

4.3. THE GROUP OF QUATERNIONS

If $\mathcal{G}(L) \cong D_2^{\mathrm{SL}_2}$ (the group of quaternions), we saw that there are three irreducible special polynomials of degree 2 and all the other irreducible ones of degree 4. With our approach, one can also find the polynomials of degree 2. The idea, explained through the following example, is to choose the correct linear combination of invariants in order to guarantee that the corresponding special polynomial is a square.

Example. Consider the equation $y'' + \frac{27x}{8(x^3-2)^2}y = 0$ (from Hendriks and van der Put, 1995). Applying our algorithm, we find that $\mathcal{G}(L)$ has no invariant of degree less than 4 and that $L^{\circledS 4}(y) = 0$ has a basis of rational solutions given by $J_1 = \left(x^3 - 2\right)$ and $J_2 = x(-2 + x^3)$. Thus, $\mathcal{G}(L)$ is the quaternion group and we get the following two special polynomials $P_1(u)$ and $P_2(u)$:

$$u^4 - 3\frac{x^2}{x^3-2}u^3 + \frac{3x(4x^3+1)}{4(x^3-2)^2}u^2 - \frac{8x^6+13x^3-4}{8(x^3-2)^3}u + \frac{27x^2(-1+2x^3)}{64(x^3-2)^4}$$

and

$$u^4 - 2\frac{(-1+2x^3)}{(x^3-2)x}u^3 + \frac{3x(8x^3-7)}{4(x^3-2)^2}u^2 - \frac{16x^6-19x^3+1}{4(x^3-2)^3}u + \frac{(4x^3-3x-2)(16x^6+12x^4-16x^3+9x^2-6x+4)}{64(x^3-2)^4x}.$$

A simple gcd computation shows that none of these is a square, so they both provide Liouvillian solutions. We now wish to compute the special polynomials of minimal degree 2 using a linear combination $J_\lambda = J_0 + \lambda J_1$ and construct the special polynomial $P_\lambda(u)$ associated with J_λ. The results of Section 3.2 show that there are exactly three values of λ such that P_λ is a square (and it is irreducible otherwise). Call R_u the resultant in u of $P_\lambda(u)$ and $\frac{\partial}{\partial u}P_\lambda(u)$; then, we must have $R_u(x, \lambda) = 0$ for all x. So, we

compute the gcd of all coefficients in x and obtain $\left(2\lambda^3+1\right)^2$ (in fact, the resultant was $-115\,964\,116\,992(x^3-2)^{22}(1+2\lambda^3)^2(\lambda x+1)$). Call α a solution of $2\alpha^3+1=0$. Then, P_α is necessarily a square. Actually, we have $P_\alpha = Q_\alpha^2$, where $Q_\alpha(u)$ is:

$$u^2 - \frac{(2x^2+x\alpha^2-\alpha)}{(x^2+2x\alpha^2-2\alpha)(x-2\alpha^2)}u + \frac{(4x^3-3\alpha x-2)(x+\alpha^2)}{4(x^2+2x\alpha^2-2\alpha)^2(x-2\alpha^2)^2}.$$

Note that there are 3 conjugate solutions of $2\alpha^3+1=0$ and thus we have three minimum polynomials of degree 2 given by the above relation. The above process can be applied to any equation with a quaternion Galois group. $\diamond$

4.4. THE TETRAHEDRAL GROUP

In the finite primitive cases, Kovacic (1986) already mentioned that one could get the minimum special polynomials by factoring special polynomials obtained from invariants of degree 12. In the tetrahedral case, there is a 2-dimensional space of invariants. Taking the same notation as in the proof of Lemma 3.3, one can see this from:

$$\chi_{12} = 2\cdot\mathbf{1} + \zeta_{1,1} + \zeta_{1,2} + 3\zeta_3.$$

Among those invariants of degree 12, two must be the cube of the two semi-invariants of degree 4, since the corresponding linear characters $\zeta_{1,1}$ and $\zeta_{1,2}$ are of order 3.

One can proceed like for the group of quaternions and look for the linear combinations of the two invariants of degree 12 whose corresponding special polynomials are the cubes of one of the two special polynomials of degree 4. The linear combination may require a quadratic extension of the field of constants of k_0.

5. Conclusion

We do not claim that the algorithm presented here is always better/faster than the Kovacic algorithm. However we feel that the formulation via rational solutions simplifies the presentation and makes the algorithm easier to implement.

The algorithm presented here is not limited to the case $k=\mathbb{C}(x)$ and holds for any second order equation with unimodular Galois group (i.e. the special form $p(x)y''-q(x)y(x)=0$ used in Kovacic (1986) is not always needed). The fact that we reduce almost everything to the computation of rational solutions of some auxiliary linear differential equations allows us to work with complicated singularities without having to factor polynomials (Bronstein, 1992).

It turns out that an implementation of our approach treats easily examples with several complicated singularities and finite group (see our examples pages 193 and 198) which the known implementations of the Kovacic algorithm could hardly solve; in practice, the only case that remains difficult is the non-reductive case where the Riccati equation has a unique rational solution.

The necessary conditions used in the Kovacic algorithm can also be used in our approach to distinguish between the different case. Similar necessary conditions (even stronger in some cases) to those given in Kovacic (1986) which do not assume the special form $p(x)y''-q(x)y(x)=0$ are given in Singer and Ulmer (1994). Necessary conditions for the group of quaternions are given in Ulmer (1994).

In the case of a finite group, an alternative to our approach is to use the algorithm of

Singer and Ulmer (1993b) to compute the minimum polynomial of an algebraic solution of $L(y) = 0$ instead of its logarithmic derivative.

Acknowledgements

We would like to thank M.F. Singer and the referees for many useful comments.

References

Bronstein, M. (1990). A unification of Liouvillian extensions. *Appl. Alg. in Eng. Comm. and Comp.* **1**, 5–24.

Bronstein, M. (1992). Solutions of linear differential equations in their coefficient field. *J. Symbolic Computation* **13**, 413–439.

Duval, A., Loday-Richaud, M. (1992) Kovacic's algorithm and its application to some families of special functions. *Appl. Alg. in Eng. Comm. and Comp.* **3**, 211–246.

Fuchs, L. (1878). Ueber die linearen Differentialgleichungen zweiter Ordnung, welche algebraische Integrale besitzen, zweite Abhandlung. *J. für Math.* **85**, 1–25.

Hendriks, P., van der Put, M. (1993) A rationality result for Kovacic's algorithm *Proceedings ISSAC'93*, New York: ACM press.

Hendriks, P., van der Put, M. (1995). Galois action on solutions of linear differential equations. *J. Symbolic Computation* **19**, 559–576.

Jordan, C. (1878). Mémoire sur les équations différentielles linéaires à intégrale algébrique. *J. für Math.* **84**, 89–215.

Kaplansky, I. (1976). *An Introduction to Differential Algebra.* Second edition, Paris: Hermann.

Kolchin, E. R. (1948). Algebraic matrix groups and the Picard–Vessiot theory of homogeneous linear ordinary differential equations., *Annals of Math.* **49**, 1–42.

Kovacic, J. (1986). An algorithm for solving second order linear homogeneous differential equations. *J. Symbolic Computation* **2**, 3-43.

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

Liouville, J. (1833). Sur la détermination des intégrales dont la valeur est algébrique. *J. de l'École Polytechnique* **22**, 149–193.

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, 243–388.

Ore, O. (1933). Theory of non-commutative polynomials. *Ann. of Math.* **34**, 480–508.

Singer, M.F. (1979). Algebraic solutions of nth 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 nth order homogeneous linear differential equations. *Amer. J. Math.* **103**, 661–682.

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). Liouvillian solutions of linear differential equations with Liouvillian coefficients. *J. Symbolic Computation* **11**, 251–273.

Singer, M.F. (1996). Testing reducibility of linear differential operators: a group theoretic perspective. *Appl. Alg. in Eng. Comm. and Comp.* **7**, 77–104.

Singer, M.F., Ulmer, F. (1993a). Galois groups of second and third order linear differential equations. *J. Symbolic Computation* **16**, 1–36.

Singer, M.F., Ulmer, F. (1993b). Liouvillian and algebraic solutions of second and third order linear differential equations. *J. Symbolic Computation* **16**, 37–73.

Singer, M.F., Ulmer, F. (1994). Necessary conditions for Liouvillian solutions of (third order) linear differential equations. *Appl. Alg. in Eng. Comm. and Comp.* **6**, 1–22.

Springer, T.A. (1973). *Invariant Theory* Lecture notes in Math. **585**. New York: Springer-Verlag.

Sturmfels, B. (1993). *Algorithms in Invariant Theory*, Texts and Monographs in Symbolic Computation, Wien: Springer-Verlag.

Ulmer, F. (1992). On Liouvillian solutions of differential equations. *Appl. Alg. in Eng. Comm. and Comp.* **2**, 171–193.

Ulmer, F. (1994) Linear differential equations of prime order. *J. Symbolic Computation* **18**, 385–401.

Weil, J.-A. (1994), The use of the Special semi-groups for solving quasi-linear differential equations *Proceedings ISSAC'94*, New York: ACM press.