*J. Symbolic Computation* (1997) **11**, 1–000

# Liouvillian and Algebraic Solutions 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 in final form 12 August 1997)*

In this paper we show that the index of a 1-reducible subgroup of the differential Galois group of an ordinary homogeneous linear differential equation $L(y) = 0$ yields the best possible bound for the degree of the minimal polynomial of an algebraic solution of the Riccati equation associated to $L(y) = 0$. For an irreducible third order equation we show that this degree belongs to $\{3, 6, 9, 21, 36\}$. When the Galois group is a finite primitive group, we reformulate and generalize work of L. Fuchs to show how to compute the minimal polynomial of a solution instead of the minimal polynomial of the logarithmic derivative of a solution. These results lead to an effective algorithm to compute Liouvillian solutions of second and third order linear differential equations.

## 0. Introduction

The computation of the algebraic solutions of a linear differential equation $L(y) = 0$ over the field of rational functions was a problem of great interest of the end of last century. P. Pepin, H. Schwarz, L. Fuchs, F. Klein, C. Jordan and others worked on this problem and gave a solution for second order equations (cf. (Baldassarri and Dwork (1979)), the intoduction of Boulanger (1898), and Gray (1986)). Many of the earliest contributions to the representation theory of finite groups have been made in connection with differential equation (e.g. Jordan's Theorem) and it was the starting point for the classification of the finite primitive groups. In this paper we will focus on the ideas of Fuchs. In Fuchs (1878), Fuchs showed how the (then new) tools of invariant theory could be used to construct, in many cases, the minimal polynomial of an algebraic solution of a second order linear differential equation.

The more general question of finding the liouvillian solutions of a linear differential equation, in which case the differential Galois group can be infinite, leads to the theory of linear algebraic groups. But for a primitive unimodular Galois group, all liouvillian solutions are algebraic (cf. Ulmer (1992)) and in this case the approach of Fuchs can

† 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.

0747–7171/90/000000 + 00 $03.00/0 © 1997 Academic Press Limited

be used. This leads to an effective method for computing the minimal polynomial of a solution in this case. This computation is much more *linear* than the computation of the minimal polynomial of the logarithmic derivative of a solution which is performed in the algorithm proposed by Kovacic for second order equations† and in the general algorithm proposed by the first author (cf. Kovacic (1986) and Singer (1981)). In the direct computation of a minimal polynomial of a solution, the knowledge of the finitely many possibilities for the differential Galois group can be used not only to bound the degree of the minimal polynomial, but also to compute the coefficients of this polynomial. In this paper we propose the following method for the computation of liouvillian solutions:

i) **Case 1:** If the differential Galois group is a reducible linear group, then a factorisation of the differential equation is used to reduce the problem to a linear differential equation of lower order. In this paper we show how this can be done for third order equations.
ii) **Case 2:** If the differential Galois group is an imprimitive linear group, then the algorithm proposed in Singer (1981) by the first author is used. For second (resp. third) order equations, this leads to the computation of a solution whose logarithmic derivative is algebraic of degree 2 (resp. 3), in which case this general algorithm is still practicable.
iii) **Case 3:** If the differential Galois group is a primitive finite linear group, then we show how the method of Fuchs can be extended to compute the minimal polynomial of an algebraic solution in a very efficient way.

In our approach, we assume that, over the differential field $k$ of coefficients of $L(y) = 0$, algorithms computing a factorisation, a solution whose logarithmic derivative is in $k$ (for case 2) and a solution which is in $k$ (for case 3) of a of linear differential equation exist (see Section 1 for a discussion and references).

In this paper we discuss explicitely second and third order differential equation, but the extension of the method of Fuchs for case 3 to higher order equations is now straightfoward.

The paper is organized as follow: in the first section we derive some results from differential Galois theory. In the second section we show how, using factorisation, case 1 of a reducible third order linear differential equation can be be reduced to the problem of finding liouvillian solutions of a second order equation. In the next section we derive exact possible algebraic degrees of the logarithmic derivative of a second or third order equation. We then briefly discuss the algorithm given by the first author which is used in case 2, where the Galois group is an imprimitive linear group. In the last and main section we focus on differential equations with primitive differential Galois groups. We first compute a bound for the algebraic degree of a solution and then use the semi-invariants of the Galois group to compute the coefficients of the minimal polynomial of an algebraic solution. We also apply the method to a second and a third order linear differential equation with primitive Galois group and compute the minimal polynomial of a solution in both cases.

† In fact, an algorithm (with some mistakes) to find the minimal polynomial of the logarithmic derivatives of a solution of a second order linear differential equation was first given by Pepin one hundred years before Kovacic (1986) and Singer (1981) (cf. Pépin (1881)). Furthermore, in Pépin (1881), Pépin is able to use his method to verify the Schwarz list of hypergeometric equations with algebraic solutions (cf. Boulanger (1898))

## 1. Differential 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) or Singer (1990). In the following we will use the same notation as in Ulmer (1992) or Singer and Ulmer (1992).

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

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

In the following we will have to compute rational solutions $z$ of $L(y) = 0$ (i.e. $z \in k$), and solutions of $L(y) = 0$ whose logarithmic derivative is rational (i.e. $z'/z \in k$). Algorithms computing such solutions for various coefficient fields are described in Bronstein. (1992), Liouville (1833), Schlesinger (1895) (volume II, §177) and Singer (1991) (cf. Proposition (2.3)). In the following we always assume that $k$ is a differential field over which such solutions can be computed (e.g. $\mathbf{C}(x), \frac{d}{dx}$)). The computation of a solution whose logarithmic derivative is rational is usually much more difficult than the computation of a rational solution.

Definition 1.1. *A differential field extension $(K, \Delta)$ of $(k, \delta)$ 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) $\eta_i$ 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) an algorithm is given 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 $\mathbf{Q}$. 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 $\mathbf{Q}(x)$.

We refer to Kaplansky (1957), Kovacic (1986), Singer (1981), Singer (1990), Ulmer (1992) or Singer and Ulmer (1992) for the definition of a Picard Vessiot extension (PVE) $K$ associated with $L(y) = 0$, which can be viewed as a splitting field of $L(y) = 0$, and of

the differential Galois group $\mathcal{G}(L)$ of $L(y) = 0$, which consists of the automorphisms of a PVE $K$ of $k$ that commute with $\delta$.

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 $GL(n, \mathcal{C})$. Different choices of bases $\{y_1, y_2, \ldots, y_n\}$ 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 $\mathcal{G}(L)$.

Many properties of the equation $L(y) = 0$ and of its solutions are related to the structure of the group $\mathcal{G}(L)$:

THEOREM 1.1. (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 $\mathcal{G}(L) \subseteq GL(n, \mathcal{C})$ of a differential equation $L(y) = 0$ of degree $n$ is unimodular.

THEOREM 1.2. (Kaplansky (1957), 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. $\mathcal{G}(L) \subseteq SL(n, \mathcal{C})$) if and only if $\exists W \in k$, such that $W'/W = a_{n-1}$.*

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:

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

For $L(y) = y''' + a_2 y'' + a_1 y' + a_0 y$ we get:

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

LEMMA 1.3. *Let $k \subset K$ be differential fields of characteristic zero with the same field of constants and $y \in K$ with $y'/y \in k$. If $y$ is algebraic over $k$, then the minimal polynomial of $y$ over $k$ is of the form $y^n - a = 0$ for some $a \in k$,*

PROOF. Let $y'/y = u \in k$ and

$$y^n + a_{n-1} y^{n-1} + \ldots + a_0 \;\; = \;\; 0$$

be the minimal polynomial of $y$ over $k$. Differentiating we have:

$$nuy^n + (a_{n-1}' + (n-1)ua_{n-1}) y^{n-1} + \ldots + a_0' \;\; = \;\; 0.$$

Comparing coefficients we have

$$nua_i = a_i' + iua_i \qquad (i = 1, \ldots, n-1).$$

If for some $i$, $0 < i < n$, $a_i \neq 0$, we have that

$$(n-i)u = \frac{a_i'}{a_i},$$

we then have

$$\frac{(y^{n-i}a_i^{-1})'}{y^{n-i}a_i^{-1}} = 0.$$

Therefore $y^{n-i}a_i^{-1}$ is a constant (in $k$). This further implies that $y$ would satisfy a polynomial of degree less than $n$, a contradiction. Therefore, for each $i$, $0 < i < n$, we have $a_i = 0$. □

COROLLARY 1.4. *Let $k \subset K$ be as above, where the field of constants is algebraically closed.*

*i) If for $y \in K$ algebraic over $k$ we have $y'/y$ algebraic over $k$ of degree $m$, then the minimal polynomial $P(\mathbf{Y}) = 0$ of $y$ over $k$ is of the form*

$$\mathbf{Y}^{i\cdot m} + a_{m-1}\mathbf{Y}^{i\cdot(m-1)} + \ldots + a_1\mathbf{Y}^i + a_0 \quad (a_j \in k,\ m = [k(y'/y)/k])$$

*ii) The extension $k(y)/k(y'/y)$ is a normal extension. If $H$ is the maximal subgroup of the Galois group $G$ of $K/k$ with the property that $\forall h \in H, h(y'/y) = y'/y$, then there is a normal subgroup $N$ of $H$ such that $H/N$ is a cyclic group of order $i$.*

*iii) If $\mathcal{T}$ is a set of left coset representatives of $H$ in $G$, then $P(\mathbf{Y}) = 0$ can be written in the following way:*

$$P(\mathbf{Y}) = \prod_{\sigma \in \mathcal{T}} \left(\mathbf{Y}^i - (\sigma(y))^i\right) \tag{1.3}$$

PROOF. i) By the previous theorem, the minimal polynomial of $y$ over $k(y'/y)$ is of the form $y^i - a = 0$ for some $a \in k(y'/y)$. Let $m = [k(y'/y) : k]$, then $y$ is a solution of a polynomial of the form:

$$a_m\mathbf{Y}^{i\cdot m} + a_{m-1}\mathbf{Y}^{i\cdot(m-1)} + \ldots + a_1\mathbf{Y}^i + a_0 \quad (a_j \in k)$$

Since $[k(y) : k] = [k(y) : k(y'/y)] \cdot [k(y'/y) : k] = i \cdot m$, $y$ cannot be a solution of a polynomial of lower degree over $k$. Thus the above polynomial is the minimal polynomial of $y$ over $k$.

ii) To the tower of fields $k \subseteq k(y'/y) \subseteq k(y) \subseteq K$ corresponds the tower of groups $G \supseteq H \supseteq N \supseteq \{id\}$. Since $k$ contains all the $i$-th roots of unity, the polynomial $y^i - a = 0$ splits over $k(y'/y)$ and thus $k(y)$ is a normal extension of $k(y'/y)$. Thus $N$ is a normal subgroup of $H$ and the Galois group of $k(y)/k(y'/y)$ is isomorphic to $H/N$ and is a cyclic group.

iii) Since $y^i$ is left fixed by the elements of $H$, we can use a set of left coset representatives $\mathcal{T}$ of $H$ in $G$ to write the minimal polynomial of $y^i$ is the following way:

$$\prod_{\sigma \in \mathcal{T}} \left(\mathbf{Y} - \sigma(y^i)\right).$$

This gives the following polynomial for $y$:

$$P(\mathbf{Y}) \quad = \quad \prod_{\sigma \in \mathcal{T}} \left( \mathbf{Y}^i - (\sigma(y))^i \right).$$

Comparing degrees as above, we get that $P(\mathbf{Y})$ is the minimal polynomial of $y$.
□

In the following we will need some differential equations associated to $L(y) = 0$:

THEOREM 1.5. (cf. Singer (1980)) *Let $L_1(y) = 0$ and $L_2(y) = 0$ be linear differential equations of degrees respectively $n_1$ and $n_2$ and fundamental systems 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) $L(y) = L_1(y) \circledS L_2(y) = 0$ 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) $L_\delta(y) = 0$ of degree $n \leq n_1$, whose solution space is spanned by the set $S_\delta = \{\delta(u_1), \cdots, \delta(u_{n_1})\}$.*

In Singer (1980) and Singer and Ulmer (1992) algorithms to construct the above equations are given. The equation

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

is called the symmetric power of order $m$ of $L(y) = 0$ and is of order at most $\binom{n+m-1}{n-1}$.

Let $L(y)$ have order $n$ and let $L(y) = 0$ have solution space $V$ in some Picard-Vessiot extension $K$ of $k$. There is a natural $\mathcal{G}(L)$ morphism $\Phi_m$ of $\mathcal{G}(L)$ modules from the $m^{th}$ symmetric power $\mathcal{S}^m(V)$ (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 $L^{\circledS\, m}(y) = 0$. If all representations of $\mathcal{G}(L)$ are completely reducible (e.g. if $\mathcal{G}(L)$ is finite), then the solution space of $L^{\circledS\, m}(y) = 0$ is $\mathcal{G}(L)$-isomorphic to a direct summand of $\mathcal{S}^m(V)$ (cf. Singer and Ulmer (1992), Lemma 3.5). If $I$ is an (semi-) invariant of degree $m$ of *the* representation of $\mathcal{G}(L)$, then by the *computation* of the (semi-) invariant $I$ we will always mean the computation of the image $\Phi_m(I)$ up to a constant multiple. For an invariant $I$ of degree $m$, $\Phi_m(I)$ is a rational solution of $L^{\circledS\, m}(y) = 0$. If $I$ is a semi-invariant, then there exists a one dimensional character $\chi$ of the group $\mathcal{G}(L)$ such that

$$\forall \sigma \in \mathcal{G}(L),\ \sigma(I) = \chi(\sigma) \cdot I.$$

In particular, if $j$ is the smallest integer $j$ such that $\chi^j$ is the trivial character, then $\Phi_m(I^j)$ is a rational solution of $L^{\circledS\,(m\,j)}(y) = 0$. A bound for $j$ follows from the character table of the group $\mathcal{G}(L)$. The one dimensional characters $\chi$ corresponding to the semi-invariants and the number of linear independent semi-invariants corresponding to a given character of degree one can be found by decomposing the character of the representation of $\mathcal{G}(L)$ on the $m^{th}$ symmetric power $\mathcal{S}^m(V)$ (cf. Singer and Ulmer (1992), section 2.3). For later reference, we summarize those simple facts:

LEMMA 1.6. *Let $L(y) = 0$ be a linear differential equation with coefficients in $k$ whose differential Galois group $\mathcal{G}(L) \subset GL(n, \mathcal{C})$ is finite. If $I$ is a semi-invariant of degree $m$ of $\mathcal{G}(L)$ and $\Phi_m(I) \neq 0$, then $\Phi_m(I)$ is a non trivial rational solution of $L^{\circledS\,(m\,i)}(y) = 0$,*

*where $i$ divides the order of a one dimensional character $\chi$ of $\mathcal{G}(L)$. If $I$ is an invariant, then $i = 1$. The possible characters $\chi$ corresponding to the semi-invariants can be found by decomposing the character of the representation of $\mathcal{G}(L)$ on the $m^{th}$ symmetric power $\mathcal{S}^m(V)$.*

## 2. Case 1: a reducible differential Galois group

The equation $L(y)$ factors as a linear differential operator, if and only if $\mathcal{G}(L)$ is a reducible linear group (see e.g. Kolchin (1948)). The factorisation of a differential operator is not unique (see e.g. Singer and Ulmer (1992), section 3.2.1), but an algorithm for computing a factorisation of a differential operator with coefficients in $\overline{\mathbf{Q}}(x)$ is well known (see e.g. Grigor'ev (1990) and Schlesinger (1895)). For third order equations a factorisation can be found by computing the rational solutions of the Riccati equation of both $L(y) = 0$ and of its adjoint. In this section we show how, for a third order differential equation, one can use only one factorisation of $L(y)$ in order to find all liouvillian solutions of $L(y) = 0$.

We will use the well known reduction method of d'Alembert, which allows one to reduce the order of a linear differential equation $L(y) = \sum_{i=0}^{n} a_i y^{(i)} = 0$ using a non trivial solution $y_1$. The problem of finding further solutions of $L(y) = 0$ reduces to finding the solutions of

$$\tilde{L}(y) \quad = \quad \sum_{i=0}^{n} a_i \left( y_1 \int y \right)^{(i)} = 0,$$

since from a fundamental set of solutions $y_1^*, \cdots, y_{n-1}^*$ of $\tilde{L}(y) = 0$ we get a fundamental system of solutions

$$y_1, y_1 \cdot \int (y_1^*), \cdots, y_1 \cdot \int (y_{n-1}^*)$$

of $L(y) = 0$.

If a second order equation is reducible, then after computing a solution whose logarithmic derivative is rational, one gets a second linearly independent liouvillian solution using the above. Thus, for second order equations, either none or all solutions are liouvillian. This is no longer true for higher order reducible equations:

LEMMA 2.1. *Let $L(y) = y''' + Ay' + By = 0$ be a reducible third order differential equation with $A, B \in \overline{\mathbf{Q}}(x)$.*

*i) If $L(y) = 0$ has a solution $z$ such that $z'/z = u \in \overline{\mathbf{Q}}(x)$, then the reduction method of d'Alembert gives the equation*

$$\tilde{L}(y) \quad = \quad y'' + 3u'y' + \left(3u'' + 3(u')^2 + A\right) y.$$

*If $\tilde{L}(y) = 0$ has no non zero liouvillian solutions, then $z$ is, up to a constant multiple, the only liouvillian solution of $L(y) = 0$. If $\tilde{L}(y) = 0$ has a non zero liouvillian solution, then applying again the method of d'Alembert gives 3 linear independent liouvillian solutions.*

*ii) If $L(y) = 0$ has no solution $z$ such that $z'/z = u \in \overline{\mathbf{Q}}(x)$, then any factorisation algorithm will give a factorisation $L(y) = L_1(L_2(y))$, where $L_2(y)$ is of order 2.*

*Either $L_2(y) = 0$ has only liouvillian solutions, in which case the procedure of d'Alembert will produce a third liouvillian solution of $L(y) = 0$ which is not a solution of $L_2(y) = 0$, or $L(y) = 0$ has no liouvillian solution.*

*Furthermore, one can determine algorithmically which of these cases hold.*

PROOF. If $L(y) = 0$ has a solution $z$ such that $z'/z = u \in \overline{\mathbf{Q}}(x)$, then the reduction method of d'Alembert always gives an equation

$$\tilde{L}(y) \quad = \quad y'' + 3u'y' + \left(3u'' + 3(u')^2 + A\right) y.$$

whose coefficients belong to $\overline{\mathbf{Q}}(x)$. The equation $\tilde{L}(y) = 0$ is a second order equation which can be solved using the Kovacic algorithm or the algorithm presented in this paper. Since a second order linear differential equation has either only liouvillian solution or no liouvillian solutions, we get the result.

If a third order differential equation $L(y) = 0$ has no solution $z$ such that $z'/z = u \in \overline{\mathbf{Q}}(x)$, then any factorisation of $L(y)$ will be of the form $L_1(L_2(y))$, where $L_2(y)$ is a second order linear differential equation. We now apply the Kovacic algorithm to $L_2(y) = 0$. If $L_2(y) = 0$ has a liouvillian solution, then $L_2(y) = 0$ and thus $L(y) = 0$ will have two linear independent liouvillian solutions. Using the reduction method of d'Alembert we will get a third solution of $L(y) = 0$ which is not a solution of $L_2(y) = 0$. If $V$ is the subspace of liouvillian solutions of $L(y) = 0$, then $L_2(y)$ maps $V$ into the solution space of $L_1(y) = 0$. If $L_2(y) = 0$ has no liouvillian solutions, then $L_2(y)$ cannot vanish on $V$. So $V$ has dimension at most 1. Since $V$ is a $\mathcal{G}(L)$ invariant subspace of the solution space of $L(y) = 0$, there is a non zero $z \in V$ so that $z'/z \in \overline{\mathbf{Q}}(x)$. Since we assume that there are no such solutions, $V$ has dimension zero. □

## 3. Optimal bounds for the logarithmic derivative and case 2: an imprimitive differential Galois group

It is well known, that for a differential equation $L(y) = 0$, one can construct a non linear differential equation $R(u) = 0$, called the *Riccati equation* associated to $L(y)$, such that the logarithmic derivative $u = z'/z$ of any solution of $L(y) = 0$ is a solution of $R(u) = 0$. The Riccati equation associated to $L(y) = y''' + a_2y'' + a_1y' + a_0y$ is $R(u) = u'' + 3uu' + a_2u' + u^3 + a_2u^2 + a_1u + a_0$.

The known algorithms computing liouvillian solutions of a linear differential equation $L(y) = 0$ use the fact that if $L(y) = 0$ has a liouvillian solution, then $L(y) = 0$ has a solution $z$ such that $z'/z$ is algebraic of bounded degree. In Ulmer (1992) a sharp bound for the degree of the minimal polynomial of an algebraic solution of $R(u) = 0$ is derived.

In this section we will first derive the exact degrees of the minimal polynomial $P(u)$ of an algebraic solution of $R(u) = 0$ for a third order differential equation and then present the general method given in Singer (1981) to compute the coefficients of $P(u)$. If $L(y) = 0$ has a liouvillian solution, this, of course, allows us to find a liouvillian solution of the form $y = e^{\int u}$. When $\mathcal{G}(L)$ is an imprimitive linear group, we show that the minimal degree of $P(u)$ is 3 and we offer no alternative to the general method of Singer (1981). On the other hand, when $\mathcal{G}(L)$ is a finite primitive linear group (in which case the minimal degree of $P(u)$ is much larger), we shall show in the next section how to determine directly the minimal polynomial of a solution of $L(y) = 0$. Nonetheless, we shall need the information found in this section.

### 3.1. The degree of an algebraic logarithmic derivative of a solution

In this section we assume the reader familiar with the notion of a reducible, imprimitive or primitive linear group and with the notion of a projective representation (see e.g. Huppert (1983), (Curtis and Reiner, I. (1962)), Issacs (1976) or Ulmer (1992)).

Since a normal abelian subgroup of a primitive group $G$ is contained in the center $Z(G)$ of $G$, we get from Jordan's Theorem (see Jordan (1878) and (Curtis and Reiner (1962))) that for a finite primitive group $G$, there are only finitely many possible groups $G/Z(G)$. If a group $\widetilde{G} \subseteq PGL(n, \mathbf{C})$ is the image (under the canonical map) of a primitive subgroup of $GL(n, \mathbf{C})$, we call $\widetilde{G}$ a primitive subgroup of $PGL(n, \mathbf{C})$.

Definition 3.1. A group $G \subseteq GL(n, \mathcal{C})$ whose elements have a common eigenvector is called 1-*reducible*.

In Ulmer (1992) Theorem 3.4 it is proven that, if an irreducible differential equation $L(y) = 0$ has a liouvillian solution, then $\mathcal{G}(L) \subseteq GL(n, \mathcal{C})$ 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 fact the minimal index of a 1-reducible subgroup of $\mathcal{G}(L)$ is the best possible bound for the degree of an algebraic solution of the Riccati equation of $L(y) = 0$:

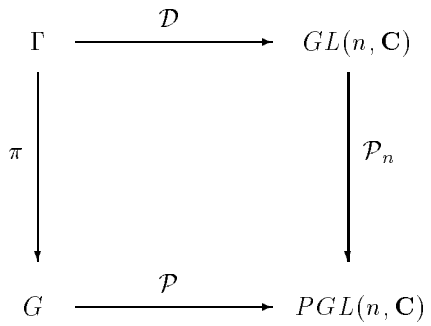
Lemma 3.1. *If a differential equation $L(y) = 0$ of degree $n$ has a solution $z$ such that $u = z'/z$ is algebraic of degree $m$, then $\mathcal{G}(L) \subseteq GL(n, \mathcal{C})$ has a 1-reducible subgroup $H$ of index $m$.*

Proof. Let $H$ be the subgroup of $\mathcal{G}(L)$ which keeps $u = z'/z$ fixed. For any $\sigma \in G$ we have

$$\begin{aligned}
\left(\frac{\sigma(z)}{z}\right)' &= \frac{\sigma(z')z - z'\sigma(z)}{z^2} \\
&= \sigma(z)\frac{\dfrac{\sigma(z')}{\sigma(z)} - \dfrac{z'}{z}}{z} \\
&= \frac{\sigma(z)}{z}\left(\sigma\left(\frac{z'}{z}\right) - \frac{z'}{z}\right) \\
&= 0.
\end{aligned}$$

Thus $\sigma(z)/z = c_\sigma \in \mathcal{C}$ or $\sigma(z) = c_\sigma z$. This shows that $z$ is a common eigenvector of $H$ and that $H$ must be a 1-reducible subgroup of $\mathcal{G}(L)$. Since $H$ is the stabiliser of $u$, the orbit of $u$ under the action of $\mathcal{G}(L)$ is of length $[\mathcal{G}(L) : H]$. Thus $[k(u) : k] = [\mathcal{G}(L) : H]$. □

A Schur representation group $(\Gamma, \pi)$ of a group $G$ (see e.g. Huppert (1983) p. 630) is a central extension of $G$ having the universal property that, if a projective representation $\mathcal{P}$ of $G$ of degree $n$ is given, there exists a representation $\mathcal{D}$ of $\Gamma$ such that the following diagram commutes:




where $\mathcal{P}_n : GL(n, \mathbf{C}) \longmapsto PGL(n, \mathbf{C}) = GL(n, \mathbf{C})/Z(GL(n, \mathbf{C}))$ denotes the canonical homomorphism.

A Schur represention group is usually not uniquely defined, but for our purposes, the knowledge of only one Schur representation group (which by a theorem of I. Schur exists for any finite group $G$) is necessary (see Ulmer (1992)). There is a routine to construct **a** Schur representation group of a finite group in the group theory system CAYLEY, see Cannon (1984). We make the following definition:

DEFINITION 3.2. We denote by $\mathcal{F}$ a function whose value $\mathcal{F}(n)$ gives the minimal value, such that for each finite primitive subgroup $G \subseteq PGL(n, \mathcal{C})$, any primitive representation of degree $n$ of a Schur representation group of $G$ has a 1-reducible subgroup of index $\leq \mathcal{F}(n)$.

In Ulmer (1992) it is shown that the above function $\mathcal{F}(n)$ is well defined. The following result of Ulmer (1992) shows that the bound in the imprimitive case is always small compared to the bound in the primitive case:

THEOREM 3.2. *If an irreducible differential equation $L(y) = 0$ of degree $n$ with coefficients in a differential field $k$, whose field of constants is algebraic closed, has a liouvillian solution over $k$, then $L(y) = 0$ has a solution $z$ such that*

*i) if $\mathcal{G}(L) \subseteq GL(n, \mathcal{C})$ is an imprimitive group, then $u = z'/z$ is algebraic over $k$ of degree at most $\max_{d|n, d>1} \{d! \cdot \mathcal{F}(n/d)\}$.*

*ii) if $\mathcal{G}(L) \subseteq GL(n, \mathcal{C})$ is a primitive group, then $u = z'/z$ is algebraic over $k$ of degree at most $\mathcal{F}(n)$.*

We note that if $n$ is prime, one can get a better bound in the imprimitive case (Ulmer (1992), Lemma 4.2). In this case $u = z'/z$ can be chosen to be algebraic of degree $n$.

In order to compute the bound $\mathcal{F}(n)$ one needs a list of the finite primitive subgroups of $PGL(n, \mathbf{C})$. For $n = 3$ such a list is given for example in Blichfeld (1917):

(i) $A_6$, the alternating permutation group of 6 letters.
(ii) $G_{168}$, the simple group of order 168.
(iii) $A_5$, the alternating permutation group of 5 letters.
(iv) $H_{216}$, the Hessian group of order 216, which is isomorphic to the permutation group of 9 letters generated by the permutations $(4, 5, 6)(7, 9, 8)$ and $(1, 2, 4)(5, 6, 8)(3, 9, 7)$.

(v) $H_{72}$, the normal subgroup of order 72 of the group $H_{216}$.
(vi) $F_{36}$, a normal subgroup of order 36 of the group $H_{72}$ (there are 3 such groups, which are all isomorphic).

From such a (finite) list of the finite primitive subgroups of $PGL(n, \mathbf{C})$ the bound $\mathcal{F}(n)$ can always be computed using the characters of the subgroups of corresponding Schur representation groups. Let $G$ be a finite primitive subgroup of $PGL(n, \mathbf{C})$, $\Gamma_G$ a Schur representation group of $G$ and $\rho(\Gamma_G)$ an irreducible representation of degree $n$ of $\Gamma_G$ with character $\zeta$. The restriction of $\rho(\Gamma_G)$ to a subgroup $H$ is 1-reducible if and only if there is a one dimensional character $\psi$ of $H$ such that the scalar product $(\psi, \zeta|H) \neq 0$, where $\zeta|H$ denotes the restriction of $\zeta$ to $H$ (cf. Curtis and Reiner (1962), §38). Considering the finitely many primitive groups $G$ and the finitely many subgroups $H$ of $\Gamma_G$ will give $\mathcal{F}(n)$.

For $n = 3$ the computation is simplified by the fact that a 1-reducible subgroup $\rho(H)$ of a irreducible finite group $\rho(\Gamma_G) \subseteq GL(3, \mathcal{C})$ is either abelian or $\mathcal{C}^3$ is a direct sum of an irreducible one dimensional representation of $H$ and an irreducible two dimensional represention of $H$. Let $\zeta$ be the character of $\rho(\Gamma_G)$. If $\rho(H)$ is 1-reducible, then either $\zeta|H$ is the sum of 3 characters of degree 1, or $\zeta|H$ is the sum of two characters $\chi_1$ and $\chi_2$ of $H$, where $\chi_1(1) = 1$ and $\chi_2(1) = 2$. We note also that, if a subgroup $H$ of $\Gamma$ has no irreducible character of degree 3, then $\rho(H)$ must be 1-reducible.

We now look at a Schur representation group $\Gamma$ of the above groups, constructed using CAYLEY (for the non simple groups these groups are not all isomorphic, so we will only give the generators and relations of the groups which have been used). Using character tables (also computed in CAYLEY) we performed the following case-by-case study (In the appendix the character tables of the subgroups of index $\leq 6$ of the Schur representation group of $A_5$ are given):

(i) $\Gamma/Z(\Gamma) \cong A_6$. All subgroups of index 36 have no irreducible character of degree 3 and thus are 1-reducible. In order to see that 36 is the smallest index of a 1-reducible subgroup of $\rho(\Gamma)$ we need to look at all subgroups whose index is less than 36 (We note that the kernel of an irreducible representation of degree 3 of $\Gamma$ is always of order 2 and thus elements of order 3 have trace $\neq 3$):
   (a) Any subgroup $H$ of index 30 contains an element $g$ of order 4. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) = -1$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 0$. Thus $\zeta|H$ can not be the sum of 3 character of degree 1 and since $\chi_1(g) + \chi_2(g) = 1$, we have $\chi_1 + \chi_2 \neq \zeta|H$. Thus $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.
   (b) Any subgroup $H$ of index 20 contains an element $g$ of order 3 with the property that for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 2$. But for any irreducible character $\zeta$ of $\Gamma$, we have $\zeta(g) \neq 3$. Since $\zeta|H$ can not be the sum of 3 character of degree 1 and $\chi_1 + \chi_2 \neq \zeta|H$, $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.
   (c) Any subgroup $H$ of index 18 contains an element $g$ of order 4. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) = -1$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 0$. Since $\zeta|H$ can not be the sum

of 3 character of degree 1 and $\chi_1 + \chi_2 \neq \zeta|H$, $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(d) Any subgroup $H$ of index 15 contains an element $g$ of order 4. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) = -1$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 0$ or $\chi_2(g) = 2$. Since $\zeta|H$ can not be the sum of 3 character of degree 1 and $\chi_1 + \chi_2 \neq \zeta|H$, $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(e) Any subgroup $H$ of index 10 has no irreducible character of degree 2. For an element of order 3 of $H$ and any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$ and $\zeta|H$ can not be the sum of 3 character of degree 1. Thus $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(f) Any subgroup $H$ of index 6 contains an element $g$ of order 4. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) = -1$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 0$. Since $\zeta|H$ can not be the sum of 3 character of degree 1 and $\chi_1 + \chi_2 \neq \zeta|H$, $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(ii) $\Gamma/Z(\Gamma) \cong G_{168}$. All subgroups of index 21 of $G$ have no irreducible character of degree 3, and thus are 1-reducible. In order to see that 21 is the smallest index of a 1-reducible subgroup of $\Gamma$ we need to look at all subgroups whose index is less than 21 (We note that the kernel of an irreducible representation of degree 3 of $\Gamma$ is always of order 2 and thus elements of order 7 have trace $\neq 3$):

(a) The subgroups of index 16 are all conjugate and have no representation of degree 2. For an element $g$ of order 7 of $H$ and any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$ and $\zeta|H$ can not be the sum of 3 character of degree 1. Thus no subgroup of index 16 can be a 1-reducible subgroup of $\rho(\Gamma)$.

(b) Any subgroup $H$ of index 14 contains an element $g$ of order 4. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) = -1$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 0$. Since $\zeta|H$ can not be the sum of 3 character of degree 1 and $\chi_1 + \chi_2 \neq \zeta|H$, $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(c) The subgroups of index 8 are all conjugate and have no irreducible character of degree 2. For an element of order 7 of $H$ and any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$ and $\zeta|H$ can not be the sum of 3 character of degree 1. Thus no subgroup of index 8 can be a 1-reducible subgroup of $\rho(\Gamma)$.

(d) Any subgroup $H$ of index 7 contains an element $g$ of order 4 whose conjugacy class contains 6 elements. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) = -1$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 0$ or $\chi_2(g) = 2$. Since $\zeta|H$ can not be the sum of 3 character of degree 1 and $\chi_1 + \chi_2 \neq \zeta|H$, $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(iii) $\Gamma/Z(\Gamma) \cong A_5$. All subgroups of index 6 of $\Gamma$ have no irreducible character of degree 3, and thus are 1-reducible. In order to see that 6 is the smallest index of a 1-reducible subgroup of $\Gamma$ we need to look at all subgroups whose index is less than 6. These non abelian groups are all conjugate and of index 5. A subgroup $H$ of index 5 contains an element $g$ of order 4. If $\zeta$ is an irreducible character of degree 3 of

$\Gamma$, then $\zeta(g) = -1$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 0$. Since $\zeta|H$ can not be the sum of 3 character of degree 1 and $\chi_1 + \chi_2 \neq \zeta|H$, $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(iv) From the presentation $\{a, b \mid a^3 = b^3 = (ab)^4 = [(aba)^2, a] = id\}$ of $H_{216}$, CAYLEY computes the following Schur representation group

$$\begin{aligned}\{a, b, c, d \quad | \quad & a^3c = b^3 = (ab)^4c = a^{-1}b^{-1}a^{-1}(a^{-1}b^{-1})^2(aba)^2bd^{-1} \\ & = [a, c] = [b, c] = [a, d] = [b, d] = [c, d] = id\}.\end{aligned}$$

We will only considere the faithfull representation of degree 3, since the non faithfull represenation of degree 3 of $\Gamma$ has non central elements in its kernel. Any subgroup $H$ of index 9 has an element $g$ of order 4. If $\zeta$ is a faithfull irreducible character of degree 3 of $\Gamma$, then $\zeta(g) = 1$. But for any irreducible character $\chi'$ of degree 3 of $H$ we must have $\chi'(g) = -1$. Thus $\chi' \neq \zeta|H$ and $H$ must be a 1-reducible subgroup of $\Gamma$. In order to see that 9 is the smallest index of a 1-reducible subgroup of $\Gamma$ we need to look at all subgroups whose index is less than 9. Since those groups are all non abelian and the irreducible representation $\rho(\Gamma)$ of degree 3 is assumed faithfull, $\zeta|H$ can not be the sum of 3 character of degree 1.

(a) The subgroups of index 8 are all conjugate and have no irreducible character of degree 2. Thus no subgroup of index 8 can be a 1-reducible subgroup of $\rho(\Gamma)$.

(b) The subgroups of index 6 are all conjugate and have no irreducible character of degree 2. Thus no subgroup of index 6 can be a 1-reducible subgroup of $\rho(\Gamma)$.

(c) Any subgroup $H$ of index 4 contains an element $g$ of order 3 whose conjugacy class in $H$ contains 1 element. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) \neq 3$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 2$. Since $\chi_1 + \chi_2 \neq \zeta|H$, $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(d) Any subgroup $H$ of index 3 contains an element $g$ of order 3 whose conjugacy class in $H$ contains 24 elements. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) \neq 3$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 2$. Since $\chi_1 + \chi_2 \neq \zeta|H$, $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(v) From the presentation $\{a, b, c \mid a^2b^{-2} = aba^{-1}b = c^4 = acb^{-1}c^{-2} = id\}$ of $H_{72}$, CAYLEY computes the following Schur representation group $\Gamma$:

$$\begin{aligned}\{a, b, c, d \quad | \quad & a^2b^{-2} = aba^{-1}b = c^4d = acb^{-1}c^{-2} \\ & = [a, d] = [b, d] = [c, d] = id\}.\end{aligned}$$

All subgroups of index 9 of $\Gamma$ have no irreducible character of degree 3, and thus are 1-reducible. In order to see that 9 is the smallest index of a 1-reducible subgroup of $\Gamma$ we need to look at all subgroups whose index is less than 9. Since those groups are all non abelian and all irreducible representations $\rho(\Gamma)$ of degree 3 are faithfull, $\zeta|H$ can not be the sum of 3 character of degree 1.

(a) The subgroups of index 8 are all conjugate and have no irreducible character of degree 2. Thus no subgroup of index 8 can be a 1-reducible subgroup of $\rho(\Gamma)$.

(b) Any subgroup $H$ of index 4 contains an element $g$ of order 3 whose conjugacy class contains one element. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) \neq 3$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 2$. Thus $\chi_1 + \chi_2 \neq \chi$ and $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

(c) Any subgroup of index 2 has no irreducible character of degree 2. Thus no subgroup of index 2 can be a 1-reducible subgroup of $\rho(\Gamma)$.

(vi) From the presentation $\{a, b \mid a^4 = (ab^{-1})^2 = b^4 = (ab)^3 = id\}$ of $F_{36}$, CAYLEY computes the following Schur representation group $\Gamma$:

$$\{a, b, c, d \quad | \quad a^4c^{-1}d^2 = (ab^{-1})^2d = b^4 = (ab)^3d \\ = [a, c] = [b, c] = [a, d] = [b, d] = [c, d] = id\}.$$

All subgroups of index 6 of $\Gamma$ have no irreducible character of degree 3, and thus are 1-reducible. In order to see that 6 is the smallest index of a 1-reducible subgroup of $\Gamma$ we need to look at all subgroups whose index is less than 9. Since those groups are all non abelian and all irreducible representations $\rho(\Gamma)$ of degree 3 are faithfull, $\zeta|H$ can not be the sum of 3 character of degree 1.

(a) The subgroups of index 4 are all conjugate and have no irreducible character of degree 2. Thus no subgroup of index 4 can be a 1-reducible subgroup of $\rho(\Gamma)$.

(b) Any subgroup $H$ of index 2 contains an element $g$ of order 3 whose conjugacy class in $H$ contains 1 element. If $\zeta$ is an irreducible character of degree 3 of $\Gamma$, then $\zeta(g) \neq 3$. But for any irreducible character $\chi_1$ of degree 1 of $H$ we get $\chi_1(g) = 1$, and for any irreducible character $\chi_2$ of degree 2 of $H$ we get $\chi_2(g) = 2$. Thus $\chi_1 + \chi_2 \neq \zeta|H$ and $\rho(H)$ can not be a 1-reducible subgroup of $\rho(\Gamma)$.

Since, as noted above, any imprimitive subgroup of $GL(3, \mathbf{C})$ has a 1-reducible subgroup of index 3 (Ulmer (1992), Lemma 4.2) we get:

THEOREM 3.3. *If an irreducible third order linear differential equation $L(y) = 0$ with coefficients in $k$ has a liouvillian solution, then $L(y) = 0$ has a solution $z$, such that for the logarithmic derivative $u = z'/z$ of $z$ one of the following holds:*

*i) $u$ is algebraic of degree 36 over $k$ and $\mathcal{G}(L)/Z(\mathcal{G}(L)) \cong A_6$.*
*ii) $u$ is algebraic of degree 21 over $k$ and $\mathcal{G}(L))/Z(\mathcal{G}(L) \cong G_{168}$.*
*iii) $u$ algebraic of degree 9 over $k$ and $\mathcal{G}(L)/Z(\mathcal{G}(L))$ is isomorphic to $H_{72}$ or $H_{216}$.*
*iv) $u$ is algebraic of degree 6 over $k$ and $\mathcal{G}(L)/Z(\mathcal{G}(L))$ is isomorphic to $F_{36}$ or $A_5$.*
*v) $u$ is algebraic of degree 3 over $k$ and $\mathcal{G}(L) \subseteq GL(3, \mathbf{C})$ is an imprimitive group.*

*For each group $\mathcal{G}(L) \subseteq GL(3, \mathcal{C})$ the numbers given above are best possible.*

PROOF. That there exists a solution whose logarithmic derivative is of the given degree follows from Theorem 3.4 of Ulmer (1992) and the previous discussion. From Lemma 3.1 we know that the degree $[k(u) : k]$ is precisely the index of a 1-reducible subgoup of $\mathcal{G}(L)$. Since the above numbers are the minimal index of a 1-reducible subgroup of $\mathcal{G}(L)$, they are best possible. □

A similar calculation can be done to show that for second order equations, the best possible degrees are: 4 if $\mathcal{G}(L)/Z(\mathcal{G}(L)) \cong A_4$, 6 if $\mathcal{G}(L)/Z(\mathcal{G}(L)) \cong S_4$ and 12 if $\mathcal{G}(L)/Z(\mathcal{G}(L)) \cong A_5$ (cf. Ulmer (1992)). This gives an alternative proof of theorem 1 of Kovacic (1986).

We point out that the above result is derived without explicitely determining the possible finite primitive unimodular Galois groups of $L(y) = 0$ but follows just from the knowledge of the list of the finite primitive subgroups of $PGL(3, \mathcal{C})$.

### 3.2. Computing the coefficients of a minimal polynomial of an algebraic solution of known degree of the Riccatti

Since we have just produced the exact minimal degrees of an algebraic solution $u$ of the Riccati equation, we now briefly review the method given in Singer (1981) to computes the coefficients of the minimal polynomial of $u$. This method is the only known method which can be used in the case of an imprimitive differential Galois group of order $n \geq 3$.

We start by describing an algorithm for finding all solutions $y$ of $L(y) = 0$ such that $\delta(y)/y \in \mathbf{C}(x)$. Let $\mathcal{S}$ be the set of singular points of $L(y)$. At each point $c \in \mathcal{S}$ one can determine a finite set $\mathcal{P}_c$ of elements of $\mathbf{C}(x)$ of the form

$$f_c = \frac{\alpha_{1c}}{x-c} + \frac{\alpha_{2c}}{(x-c)^2} + \ldots + \frac{\alpha_{nc}}{(x-c)^n}$$

or $f_c = \alpha_{1c}x + \ldots + \alpha_{nc}x^n$ if $c = \infty$, such that if $y$ is a solution of $L(y) = 0$ such that $y'/y \in \mathbf{C}(x)$ then

$$\begin{aligned} y &= P(x)e^{\left(\int \sum_{c\in\mathcal{S}} f_c\right)} \\ &= P(x)\prod_{c\in\mathcal{S}}(x-c)^{\alpha_{1c}} e^{\left(\frac{\alpha_{2c}}{x-c} + \frac{\alpha_{3c}}{(x-c)^2} + \ldots + \frac{\alpha_{nc}}{(x-c)^n}\right)} \end{aligned}$$

for some choice of $f_c \in \mathcal{P}$ and $P(x) \in \mathbf{C}[x]$. Futhermore, the degree of any possible $P(x)$ can be bounded in terms of the $\alpha_{1c}$. A method for determining the sets $\mathcal{P}_c$ is given in (Schlesinger (1895), Vol. II.1 Section 177). A modern presentation using Newton polygons and emphasizing computational aspects and an implementation in DESIRE is given in Grigor'ev (1990) and Tournier (1987). This reduces the problem of finding such solutions to the problem of determining the coefficients of the possible $P(x)$, a problem in linear algebra. A related method is given in Singer (1991).

Let $L(y) = 0$ be an irreducible differential equation and $P(u)$ the minimal polynomial of an algebraic logarithmic derivative $\delta(y_1)/y_1$ of a solution $y_1$ of $L(y) = 0$. Any solution of $P(u) = 0$ is then a logarithmic derivative of a solution of $L(y) = 0$ and we get:

$$\begin{aligned} P(u) &= u^m + c_{m-1}u^{m-1} + \ldots + c_0 \\ &= (u - \frac{y_1'}{y_1})(u - \frac{y_2'}{y_2})\ldots(u - \frac{y_m'}{y_m}) , \end{aligned}$$

where the $y_i$ are solutions of $L(y) = 0$. The coefficients $c_i \in k$ are homogeneous forms of degree $m - i$ in the $m$ logarithmic derivatives $\{y_1'/y_1, \cdots, y_m'/y_m\}$.

We have

$$\begin{aligned} c_{m-1} &= \frac{y_1'}{y_1} + \frac{y_2'}{y_2} + \cdots + \frac{y_m'}{y_m} \\ &= \frac{(y_1 y_2 \cdots y_m)'}{y_1 y_2 \cdots y_m}. \end{aligned}$$

The product $y_1 y_2 \cdots y_m$ is a solution of $L^{\circledS m}(y) = 0$. Thus $c_{m-1}$ is a rational logarithmic derivative of a solution of $L^{\circledS m}(y) = 0$.

Using $c_{m-1}$ we can now compute the other coefficients $c_i$. The coefficient $c_i$ can be written as:

$$c_i = \sum_{1 \le k_1 < \cdots < k_i \le m} \left( \frac{y_{k_1}'}{y_{k_1}} \cdots \frac{y_{k_i}'}{y_{k_i}} \right).$$

Let

$$\begin{aligned} v_i &= c_i y_1 y_2 \ldots y_n \\ &= \sum_{1 \le k_1 < \cdots < k_i \le m} y_{k_1}' y_{k_2}' \ldots y_{k_i}' \prod_{j \ne k_1, \ldots, k_i} y_j . \end{aligned}$$

Note that $v_i$ is a solution of $(L_\delta)^{\circledS i}(y) \circledS L^{\circledS (m-i)}(y)$, where $L_\delta(y)$ is a differential equation which is satisfied by the derivatives of solutions $L(y) = 0$. We then have:

$$\begin{aligned} \frac{v_i'}{v_i} &= \frac{c_i'}{c_i} + \frac{(y_1 y_2 \ldots y_n)'}{y_1 y_2 \ldots y_n} \\ &= \frac{c_i'}{c_i} + c_{m-1}. \end{aligned}$$

Therefore, $v_i$ is the solution of a linear differential equation (that we can construct) and the logarithmic derivative of $v_i$ is rational. We can describe all such solutions. Simillarly, $y_1 y_2 \ldots y_n$ is also a solution of a linear differential equation and its logarithmic derivative is also rational. Since $c_i = v_i/(y_1 y_2 \ldots y_n)$, we can determine the degrees of the numerator and denominator of $c_i$ using the algorithm described at the beginning of this section to determine the possible candidates for $v_i$ and $(y_1 y_2 \ldots y_n)$.

We therefore are able to determine bounds on the degrees of the numerators and denominators of the coefficients of a minimal polynomial. To determine the actual numbers that can appear as coefficients of these numerators and denominators, one must differentiate $P(u) = 0$ repeatedly, solve for the higher derivatives of $u$, and reduce the Riccati equation $R(u) = 0 \bmod P(u)$. This will give algebraic conditions on the numbers appearing in the coefficients of $P(u)$ (a similar method is used in the last section).

We note that for second order linear differential equations, $R(u)$ has order 1. In this case , it is showed in Kovacic (1986) that for $0 \le i \le n-2$ a simple recursion gives each $c_i$ in terms of the $c_j$ with $j > i$. Therefore in the second order case it suffices to just find the possible $c_{m-1}$. We do not know a similar statement for higher order equations.

## 4. Case 3: a primitive unimodular Galois group

In this section we show that in this case, where the bound for the algebraic degree of an algebraic solution of the Riccati is large compared to the imprimitive case (cf.

Theorem 3.2 and 3.3), the difficult computation of a rational solution of some Riccati can be avoided. We will reduce the problem to the computation of a rational solution of some symmetric power and a Gröbner basis computation. In contrast to the previous section where only a projective representation of $\mathcal{G}(L)$ was used, a list of the possible Galois groups will be needed. We start by giving this list (taken from Blichfeld (1917) and (Miller, Blichfeld and Dickson (1938)) ) for second and third order equations.

## 4.1. The primitive unimodular groups of degree 2 and 3

### 4.1.1. The primitive unimodular groups of degree 2

Up to isomorphism, there are 3 primitive unimodular groups of degree 2. According to Miller, Blichfeld and Dickson (1938) we define the following matrices:

$$T = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad S = \begin{pmatrix} \frac{i-1}{2} & \frac{i-1}{2} \\ \frac{i+1}{2} & \frac{-i-1}{2} \end{pmatrix} \quad U = \begin{pmatrix} \frac{1+i}{\sqrt{2}} & 0 \\ 0 & \frac{1-i}{\sqrt{2}} \end{pmatrix}$$

$$S' = \begin{pmatrix} \xi^3 & 0 \\ 0 & \xi^2 \end{pmatrix} \quad U' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad T' = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix},$$

where $\xi^5 = 1$, $\alpha = \dfrac{\xi^4 - \xi}{\sqrt{5}}$ and $\beta = \dfrac{\xi^2 - \xi^3}{\sqrt{5}}$.

Then the groups are the following:

(i) The icosahedral group $A_5^{SL_2}$ of order 120 is generated by $S'$, $U'$ and $T'$. We have $A_5^{SL_2}/\{\pm 1\}$ is isomorphic to the alternating group $A_5$ of 5 letters.

(ii) The octahedral group $S_4^{SL_2}$ of order 48 is generated by $S$ and $U$. We have $S_4^{SL_2}/\{\pm 1\}$ is isomorphic to the symmetric group $S_4$ of 4 letters.

(iii) The Tetrahedral group of $A_4^{SL_2}$ of order 24 is generated by $S$ and $T$. We have $A_4^{SL_2}/\{\pm 1\}$ is isomorphic to the alternating group $A_4$ of 4 letters.

When one looks at a character table of $A_4^{SL_2}$, one sees 3 irreducible representations of degree 3, but since in $SL(2, \mathbf{C})$ the trace of an element of order 3 is $-1$, only one of these is in $SL(2, \mathbf{C})$. The groups $A_5^{SL_2}$ and $S_4^{SL_2}$ have two non conjugate representation in $SL(2, \mathbf{C})$. But the non equivalent representations can be obtained from each other using the Galois group of $\mathbf{Q}(\sqrt{2}, \xi)$ over $\mathbf{Q}$. This follows from the fact that under the automorphism sending $\sqrt{2}$ to $-\sqrt{2}$ the trace of $U$ will change and that under the automorphism sending $\sqrt{5} \in \mathbf{Q}(\xi)$ to $-\sqrt{5}$ the trace of an element of order 10 will change. This will allow us to work with only one representation and to get the complete result by applying the corresponding automorphism.

### 4.1.2. The primitive unimodular groups of degree 3

Up to isomorphism, there are 8 primitive unimodular groups of degree 3. According to Miller, Blichfeld and Dickson (1938)† we define the following matrices:

$$E_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi^4 & 0 \\ 0 & 0 & \xi \end{pmatrix} \quad E_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \quad E_3 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 & 2 \\ 1 & s & t \\ 1 & t & s \end{pmatrix}$$

$$E_4 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2\lambda_2 & 2\lambda_2 \\ \lambda_1 & s & t \\ \lambda_1 & t & s \end{pmatrix} \quad S = \begin{pmatrix} \beta & 0 & 0 \\ 0 & \beta^2 & 0 \\ 0 & 0 & \beta^4 \end{pmatrix} \quad R = \frac{1}{\sqrt{-7}} \begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}$$

$$S_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \quad T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad U = \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon\omega \end{pmatrix}$$

$$V = \rho \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \qquad Z = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{pmatrix}$$

where $\xi^5 = 1, s = \xi^2+\xi^3, t = \xi+\xi^4, \sqrt{5} = t-s, \varepsilon^6+\varepsilon^3+1 = 0$ $(\varepsilon^9 = 1), \omega = -\varepsilon^3-1$ $(\omega^3 = 1)$, $\beta^7 = 1$, $a = \beta^4 - \beta^3$, $b = \beta^2 - \beta^5$, $c = \beta - \beta^6$, $\dfrac{1}{\sqrt{-7}} = \dfrac{\beta+\beta^2+\beta^4-\beta^6-\beta^5-\beta^3}{7}$, $\lambda_1 = \dfrac{-1 \pm \sqrt{-15}}{4}$, $\lambda_2 = \dfrac{-1 \mp \sqrt{-15}}{4}$ and $\rho = \dfrac{1}{\omega - \omega^2}$.

Then the groups are the following:

(i) The Valentiner group $A_6^{SL_3}$ of order 1080 is generated by $E_1$, $E_2$, $E_3$ and $E_4$. We have $A_6^{SL_3}/ < Z >$ is isomorphic to the alternating group $A_6$ of 6 letters.
(ii) The alternating group $A_5$ of five letters generated by $E_1$, $E_2$ and $E_3$.
(iii) The direct product $A_5 \times C_3$, of $A_5$ and the cyclic group $C_3$ of three elements, generated by $E_1$, $E_2$, $E_3$ and $Z$.
(iv) The simple group $G_{168}$ of order 168 generated by $S$, $T$ and $R$.
(v) The direct product $G_{168} \times C_3$, of $G_{168}$ and the cyclic group $C_3$ of three elements, generated by $S$, $T$, $R$ and $Z$.
(vi) The group $H_{216}^{SL_3}$ of order 648 generated by $S_1$, $T$, $V$ and $U$, whose projective representation is the Hessian group of order 216.
(vii) The group $H_{72}^{SL_3}$ of order 216 generated by $S_1$, $T$, $V$ and $UVU^{-1}$.
(viii) The group $F_{36}^{SL_3}$ of order 108 generated by $S_1$, $T$ and $V$.

As in the previous case, all non equivalent representations of these groups in $SL(3, \mathbf{C})$ can be obtained using the Galois group of the field to which the coefficients of the matrices belong. The group $H_{72}^{SL_3}$ has two faithfull non conjugate representations in $SL(3, \mathcal{C})$ which

† The matrix $T$ used here corresponds to the inverse of the matrix $T$ used in Miller, Blichfeld and Dickson (1938) and the definition of $A_6^{SL_3}$ and $A_5$ correspond to the definitions given in exercise 3 and 4 p. 252 of Miller, Blichfeld and Dickson (1938)

are sent to each other by the automorphism $\sigma : \varepsilon \mapsto \varepsilon^2$ of the Galois group of $\mathbf{Q}(\varepsilon)/\mathbf{Q}$, since the trace of $M = UVU^{-1}VT^{-1}UVU^{-1}$ is $\omega$, while the trace of $\sigma(M)$ is $\omega^2$. The automorphism $\sigma$ also sends the two faithfull non conjugate representations of $F_{36}^{SL_3}$ in $SL(3,\mathcal{C})$ to each other, since the trace of $M = VS^2TST^{-1}$ is $\omega$, while the trace of $\sigma(M)$ is $\omega^2$. This will allow us to work with only one representation and to get the complete result by applying the corresponding automorphism. We also note that for $H_{72}^{SL_3}$ and $F_{36}^{SL_3}$ only the representations where the elements of order 4 all have trace 1 belong to $SL(3,\mathbf{C})$.

We point out that the above groups do not in general correspond to the Schur representation groups used in the previous section. For example, the group $A_6^{SL_3}$ is of order 1080 while the Schur representation group of $A_6$ is of order 2160.

### 4.2. Algebraic degree of a solution

From Theorem 3.3 and Theorem 3.8 of Ulmer (1992) we see that for the computation of an algebraic logarithmic derivative $u = y'/y$ of a solution $y$, the most difficult cases, where the algebraic degree of $u$ is large, are those of a finite primitive unimodular differential Galois group. In this case all solutions will be algebraic and we shall show how to compute the minimal polynomial of such a solution. From Corollary 1.4 we get that the number of coefficients of the minimal polynomials of $y$ and $y'/y$ are the same. In this section we will derive a bound for the algebraic degree of a solution $y$ of $L(y) = 0$. We note that from $k(y'/y) \subseteq k(y)$ the index of a 1 reducible subgroup of $\mathcal{G}(L)$ is a lower bound for the degree of a solution (cf. Lemma 3.1).

For a second order differential equation $L(y) = 0$ an old result of P. Pepin and L. Fuchs (see Fuchs (1875) and the introduction in Boulanger (1898)) shows that the degree of $P(y)$ is always the largest possible degree, which is the order of $\mathcal{G}(L)$. This can be seen in the following way: If $L(y) = y'' - ry$ $(r \in k)$, then the Wronskian $y_1'y_2 - y_1y_2'$ of two solutions $y_1$ and $y_2$ of $L(y) = 0$ is a constant $c$ (see e.g. Kaplansky (1957), p. 40). Thus

$$\frac{y_2}{y_1} \quad = \quad c \int \frac{1}{y_1^2}$$

If $y_1$ and $y_2$ are algebraic over $k$, then the integral on the right hand side must be algebraic and thus a rational function in $y_1$ over $k$. Since any solution can be used as $y_1$, we get that for any solution $y_1$ of $L(y) = 0$ the field $k(y_1)$ is the full Picard-Vessiot extension $K$ associated to $L(y) = 0$ . Thus any solution is a primitive element of $K$ and must be of degree $\mathcal{G}(L)$.

The following Theorem shows that the above result of Pepin and Fuchs no longer holds for third order differential equations:

Theorem 4.1. *Let $L(y)$ be an irreducible third order linear differential equation with Galois group a primitive group $\mathcal{G}(L) \subset SL(3,\mathbf{C})$. If $L(y) = 0$ has a liouvillian solution then all solution are algebraic and there is a solution $z$ whose minimal polynomial $P(\mathbf{Y})$ is of the form*

$$\mathbf{Y}^{d\cdot m} + a_{m-1}\mathbf{Y}^{d\cdot(m-1)} + \ldots + a_1\mathbf{Y}^d + a_0 \quad (a_i \in k)$$

*such that one of the following holds:*

*(i) If $\mathcal{G}(L) \cong A_6^{SL_3}$, $m = 36$ and $d = 6$.*

*(ii)* If $\mathcal{G}(L) \cong A_5$, $m = 6$ and $d = 2$.
*(iii)* If $\mathcal{G}(L) \cong A_5 \times C_3$, $m = 6$ and $d = 6$.
*(iv)* If $\mathcal{G}(L) \cong G_{168}$, , $m = 21$ and $d = 2$.
*(v)* If $\mathcal{G}(L) \cong G_{168} \times C_3$, , $m = 21$ and $d = 6$.
*(vi)* If $\mathcal{G}(L) \cong H_{216}^{SL_3}$, $m = 9$ and $d = 9$.
*(vii)* If $\mathcal{G}(L) \cong H_{72}^{SL_3}$, $m = 9$ and $d = 3$.
*(viii)* If $\mathcal{G}(L) \cong F_{36}^{SL_3}$, $m = 6$ and $d = 6$.

*The above numbers are also the minimal degree of an algebraic solution, except for the group* $F_{36}^{SL_3}$*, where there also exists a solution whose minimal polynomial is of degree* 27 *instead of* 36.

In order to prove the above result we need a result linking the permutation representation of $\mathcal{G}(L)$ on the solutions of $P(Y) = 0$ and the linear representation of $\mathcal{G}(L)$ on the solutions of $L(y) = 0$.

Lemma 4.2. *Let $G$ be a finite group and $V$ a finite irreducible $G$-module over a field of characteristic 0 with character $\chi$. Let $\{v_1, \ldots, v_m\}$ be a $G$-invariant subset of $V$ and $V_m$ be the associated permutation $G$-module. Then $V$ is a direct summand of $V_m$ and*

$$\sum_{g \in G} \chi(g) \cdot fix(g) \quad = \quad t \cdot |G| > 0,$$

*where $fix(g)$ is the number of vectors in $\{v_1, \ldots, v_m\}$ left fixed by $g$ and $t$ is the multiplicity of $V$ in $V_m$.*

Proof. By the definition of $V_m$ we can identify a basis $\{z_1, \ldots, z_m\}$ of $V_m$ with the set $\{v_1, \ldots, v_m\}$ in such a way that the action of $G$ on these two sets are the same. We now define a map $\varphi : V_m \longmapsto V$ by $\varphi(z_i) = v_i$ $(i \in \{1, \ldots m\})$. This clearly defines a $G$-morphism. According to Maschke's Theorem, $V_m$ is completely reducible and thus the direct sum of the image $\varphi(V_m)$ and the kernel of $\varphi$. Since $V$ is an irreducible $G$-module, $\varphi(V_m) = V$. This shows that $V$ is a direct summand of $V_m$.
If we denote $\chi_m$ the character of $V_m$, then the orthogonality relations give us

$$\sum_{g \in G} \chi(g) \cdot \overline{\chi_m(g)} \quad = \quad t \cdot |G| > 0.$$

With respect to the basis $\{z_1, \ldots, z_m\}$, an element $g \in G$ has a 1 in the $(i, i)$ place if $z_i$ is left fixed and a 0 otherwise. Therefore the trace of this matrix is $fix(g)$ and the formula now follows. □

**Proof of Theorem 4.1** For each possible group $\mathcal{G}(L)$ we know the index $m$ of a one reducible subgroup $H$ of smallest index (Theorem 3.3). If $\mathcal{G}(L) \ncong F_{36}^{SL_3}$ and $\mathcal{G}(L) \ncong G_{168} \times C_3$, then using Cayley one can show that all groups $H$ of index $m$ are conjugate so that one can choose any of these groups to perform the computations in the following. If $\mathcal{G}(L) \cong F_{36}^{SL_3}$, then two non conjugate groups $H$ have to be considered. If $\mathcal{G}(L) \cong G_{168} \times C_3$, then $m = 21$, but the groups of index 21 which have an irreducible representation of degree 3 cannot be 1-reducible, since from the character tables we get that in such a representation there is an element of order 2 whose trace is $-1$, but in any 1-dimensional representation of $G_{168} \times C_3$ this element has a trace 1 and in any

2-dimensional representation this element has trace 2. Those subgroups of $G_{168} \times C_3$ of index 21 which are always 1-reducible are all congugate and we can choose any of them.

From Theorem 3.3 we get that $L(y) = 0$ has a solution $y$ such that $[k(y'/y) : k] = m$. From Corollary 1.4 we get that the differential Galois group of $k(y)/k(y'/y)$ is cyclic. If $K$ denotes the PVE of $L(y) = 0$, then the extension $k(y)$ is an intermediate field of $K/k(y'/y)$. The differential Galois group of $K/k(y'/y)$ is isomorphic to $H$ and the Galois group of $k(y)/k(y'/y)$ is a cyclic factor of $H$ (cf. Corollary 1.4). Since we know the possible groups $H$, using CAYLEY we can compute the order $d$ of all possible cyclic factor groups of $H$. We get:

i) If $\mathcal{G}(L) \cong A_6^{SL_3}$, $A_5 \times C_3$, $G_{168} \times C_3$, $H_{72}^{SL_3}$ or $F_{36}^{SL_3}$, then $d$ belongs to $\{1, 2, 3, 6\}$.
ii) If $\mathcal{G}(L) \cong A_5$ or $G_{168}$ then $d$ belongs to $\{1, 2\}$.
iii) If $\mathcal{G}(L) \cong H_{216}^{SL_3}$, then $d$ belongs to $\{1, 3, 9\}$.

From Corollary 1.4 we get that the minimal polynomial of $y$ must be of the form:

$$P(\mathbf{Y}) = \mathbf{Y}^{d \cdot m} + a_{m-1}\mathbf{Y}^{d(m-1)} + \ldots + a_1\mathbf{Y}^d + a_0 \quad (a_j \in k)$$

Since $\mathcal{G}(L) \subseteq SL(3, \mathbf{C})$ is irreducible, the splitting field of $P(\mathbf{Y}) = 0$ is a Picard Vessiot extension for $L(y) = 0$ (cf. Ulmer (1992), Corollary 2.4). Thus $\mathcal{G}(L)$ is the (classical) Galois group of $P(\mathbf{Y}) = 0$ (cf. Ulmer (1992), Lemma 1.1) and must have a faithfull representation as a transitive permutation group of degree $d \cdot m$. Using CAYLEY one can see that for a faithfull transitive representation of

(i) $A_6^{SL_3}$ of degree $36 \leq j \leq (6 \cdot 36)$, $j$ must be 45, 90, 108 135, 180 or 216.
(ii) $A_5$ of degree $6 \leq j \leq (2 \cdot 6)$, $j$ must be 6, 10 or 12.
(iii) $A_5 \times C_3$ of degree $6 \leq j \leq (6 \cdot 6)$, $j$ must be 15, 18, 30 or 36.
(iv) $G_{168}$ of degree $21 \leq j \leq (2 \cdot 21)$, $j$ must be 21, 24, 28 or 42.
(v) $G_{168} \times C_3$ of degree $21 \leq j \leq (6 \cdot 21)$, $j$ must be 21, 24, 42, 63, 72, 84 or 126.
(vi) $H_{216}^{SL_3}$ of degree $9 \leq j \leq (9 \cdot 9)$, $j$ must be 81.
(vii) $H_{72}^{SL_3}$ of degree $9 \leq j \leq (6 \cdot 9)$, $j$ must be 27, 36 or 54.
(viii) $F_{36}^{SL_3}$ of degree $6 \leq j \leq (6 \cdot 6)$, $j$ must be 18, 27 or 36.

For each possible $j$ above, we construct all transitive permutation representations of the corresponding differential Galois group $\mathcal{G}(L)$ (note that it is enougth to let $\mathcal{G}(L)$ act on the cosets of one representant of each set of conjugate subgroups) and compute the corresponding permutation representation $P$ with character $\chi_P$ of degree $j$. If for all irreducible characters $\chi$ of degree 3 of $G$, the scalar product $\chi$ and $\chi_P$ is 0, then from Lemma 4.2 we get that $\mathcal{G}(L)$ cannot permute the $j$ solutions according to $P$. If this is the case for all transitive permutation respresentations of degree $j$, then we can exclude the possibility $j$.

For the groups $A_6^{SL_3}$, $A_5$, $G_{168}$, $G_{168} \times C_3$ and $H_{216}^{SL_3}$ only the numbers $j = d \cdot m$ given in the Theorem are still possible and must thus be minimal.

For the groups $H_{72}^{SL_3}$ the values $3 \cdot 9$ and $6 \cdot 9$ and for $F_{36}^{SL_3}$ the values 27 and $6 \cdot 6$ are still possible. We will show by examining the matrices defining the three dimensional representations that in both cases there is always a solution of degree 27 which will then be the minimal degree.

A representation $G$ in $SL(3, \mathcal{C})$ of the group $H_{72}^{SL_3}$ is generated by the matrices $S_1$, $T$,

$V$ and $UVU^{-1}$ given in section 4.1.2. A 1-reducible subgroup $H$ of index 9 is generated by $S_1TUVU^{-1}$, $S_1TUVU^{-1}V$ and $S_1T^{-1}S_1^{-1}T$. The solution $y=(0,-1,1)$ is left invariant by the first two matrices and sent to $\omega y$ by the last matrix. This shows that $y^3$ is left invariant by $H$ and, since by the above no solution of lower degree is possible, that for this representation of $\mathcal{G}(L)\cong H_{72}^{SL_3}$ the equation $L(y)=0$ has a solution of the form stated. Since we can map this representation of $H_{72}^{SL_3}$ to a non equivalent one by the automorphism $\sigma:\varepsilon\mapsto\varepsilon^2$ of the Galois group of $\mathbf{Q}(\varepsilon)/\mathbf{Q}$ and that the given eigenvector and eigenvalues of the elements of $H$ belong to $\mathbf{Q}(\varepsilon)$, it follows that for the representation $\sigma(G)$ the group $\sigma(H)$ will have the above properties of $H$. This shows that a differential equation whose Galois group is isomorphic to $H_{72}^{SL_3}$ will always have a solution of degree $3\cdot 9$ and of the form stated.

A representation $G$ in $SL(3,\mathcal{C})$ of the group $F_{36}^{SL_3}$ is generated by $S_1$, $T$ and $V$ of section 4.1.2. The cyclic subgroup $F$ generated by $S_1^{-1}T^{-1}S_1V^{-1}$ is of order 4 and index 27. The solution $y=(-\varepsilon^3,1,0)$ is left invariant by $F$. Since from the above we know that no solution of lower degree is possible, the degree of $y$ must be 27. This shows that for this representation of $F_{36}^{SL_3}$, a solution of degree 27 always exists. Since we can map this representation of $H_{72}^{SL_3}$ to a non equivalent one by the automorphism $\sigma:\varepsilon\mapsto\varepsilon^2$ of the Galois group of $\mathbf{Q}(\varepsilon)/\mathbf{Q}$ and that the given eigenvector and eigenvalues of the elements of $H$ belong to $\mathbf{Q}(\varepsilon)$, it follows that for the representation $\sigma(G)$ the group $\sigma(F)$ will have the above properties of $F$. This shows that a differential equation whose Galois group is isomorphic to $F_{36}^{SL_3}$ will always have a solution of degree 27. On the other hand, since $6\cdot 6$ is the only possibility left of the form $6\cdot i$, there will also always exists a solution of degree $6\cdot 6$. This completes the proof of Theorem 4.1.

We also note that the result of Fuchs and Pepin, which states that for second order equations the degree of an algebraic solution always corresponds to the order of the primitive unimodular group $\mathcal{G}(L)$ (i.e. any solution is a primitive element of the PVE) can also be proven using the method above.

### 4.3. Decomposition of the coefficients in terms of (semi-)invariants

In this section as in the previous one we deal with the case of a differential equation $L(y)=0$ whose Galois group $\mathcal{G}(L)$ is a finite primitive unimodular group. We show how the coefficients of the minimal polynomial of a solution of $L(y)=0$ can be computed using a basis of the ring of invariants of $\mathcal{G}(L)$ (see e.g. Cox, Little and O'Shea (1992), Chapter 7). This approach is not new and has been successfully used in Fuchs (1875) for the case of second order differential equation. In this section we will describe this procedure and show how it can be generalized to higher order equations.

Let $L(y)=0$ be a differential equation of degree $n$ with finite primitive differential Galois group $\mathcal{G}(L)\subseteq SL(n,\mathcal{C})$. Let $\{y_1,y_2,\ldots,y_n\}$ be a basis of the solution space of $L(y)=0$ corresponding to the representation $\mathcal{G}(L)$, $H$ a 1-reducible subgroup of $\mathcal{G}(L)$ of minimal index $m$ and $\mathcal{T}$ a set of left coset representatives of $H$ in $\mathcal{G}(L)$. Let $y$ be a common eigenvector of $H$, then by Corollary 1.4 we get that the minimal polynomial of $y$ is the form

$$\begin{aligned} P(\mathbf{Y}) &= \prod_{\sigma\in\mathcal{T}}\left(\mathbf{Y}^d-(\sigma(y))^d\right)\\ &= \mathbf{Y}^{d\cdot m}+\alpha_{d(m-1)}\mathbf{Y}^{d(m-1)}+\ldots+\alpha_d\mathbf{Y}^d+\alpha_0 \quad (m=|\mathcal{G}(L)/H|), \end{aligned}$$

where any coefficient $\alpha_i$ is a polynomial of degree $d \cdot m - i$ in $\{y_1, y_2, \ldots, y_n\}$. By construction these polynomials are invariant under the action of $\mathcal{G}(L)$ and thus can be expressed in terms of the elements of a basis of the ring of invariants (or semi-invariants) of $\mathcal{G}(L)$. This can be done in the following way:

i) Choose a representation $\mathcal{G}(L) \subseteq SL(n, \mathcal{C})$ of the differential Galois group of $L(y) = 0$ (i.e. fix a basis of the solution space) and compute a basis $\{b_1(y_1, \ldots, y_n), \ldots, b_j(y_1, \ldots, y_n)\}$ of the ring of invariants of $\mathcal{G}(L)$.
ii) Compute a 1-reducible subgroup $H$ of minimal index of $\mathcal{G}(L)$ and a common eigenvector $y$ for the matices of $H$.
iii) Compute a set of left coset representatives $\mathcal{T}$ of $H$ in $\mathcal{G}(L)$.
iv) Compute the polynomial

$$\begin{aligned} P(\mathbf{Y}) &= \prod_{\sigma \in \mathcal{T}} (\mathbf{Y}^d - \sigma(z)^d) \\ &= \mathbf{Y}^{d \cdot m} + \gamma_{m-1}(y_1, \ldots, y_n)\mathbf{Y}^{d \cdot (m-1)} + \ldots + \gamma_0(y_1, \ldots, y_n), \end{aligned}$$

where $m = |\mathrm{G(L)}/H|$ and $d$ is the index of a normal subgroup $F$ of $H$ such that $H/F$ is a cyclic group.
v) Using the Gröbner basis algorithm, express $\gamma_i(y_1, \ldots, y_n)$ in terms of polynomials in the invariants $\{b_1(y_1, \ldots, y_n), \ldots b_j(y_1, \ldots, y_n)\}$ (cf. Cox, Little and O'Shea (1992), Chapter 7, §3, Prop. 7. In practice an *Ansatz* turned out to be more effective).

The above computation has to be done once for the finitely many primitive finite subgroups of $SL(n, \mathbf{C})$.

In the following we will use semi-invariants of $\mathcal{G}(L)$ to represent the coefficients of $P(Y)$, since they are usually of lower degree.

### 4.3.1. Second order equations

For second order equations the decomposition of the coefficients $\alpha_i(y_1, \ldots, y_n)$ in terms of $\{b_1(y_1, \ldots, y_n), \ldots b_j(y_1, \ldots, y_n)\}$ has been computed by Fuchs in Fuchs (1875) for $A_4^{SL_2}$ and $S_4^{SL_2}$. In the following we show that the result for second order equations can be obtained by our approach and restate Fuchs' results.

The second order case is simplified by the following facts:

i) According to the result of Pepin and Fuchs, we must have $d \cdot m = |\mathcal{G}(L)|$ (i.e. any solution is a primitive element of the PVE associated to $L(y) = 0$).
ii) Any one reducible subgroup is abelian and (assuming $\mathcal{G}(L)$ unimodular) is a cyclic group, so that a common eigenvector is just an eigenvector of a generator.

We have to deal with each group separetely.

**The tetrahedral group $A_4^{SL_2}$:**

We consider the algebraic extension $\mathbf{Q}(\omega)$ of the rational numbers, where $\omega$ is a root of $\omega^4 - 2\omega^3 + 5\omega^2 - 4\omega + 1$. We have $i = \sqrt{-1} = -2\omega^3 + 3\omega^2 - 9\omega + 4$ and $\sqrt{-3} = 4\omega^3 - 6\omega^2 + 16\omega - 7$. The group $A_4^{SL_2}$ is generated by the matrices $S$ and $T$ of section 4.1.1 which are defined in $\mathbf{Q}(\omega)$.

We denote $\{y_1, y_2\}$ the basis corresponding to the above representation. In this representation, the ring of semi-invariants of $A_4^{SL_2}$ is generated by (see Miller, Blichfeld and Dickson (1938), p. 224):

$$\begin{aligned} I_1 &= y_1^4 + 2\sqrt{-3}y_1^2y_2^2 + y_2^4, \\ I_2 &= y_1y_2(y_1^4 - y_2^4), \\ I_3 &= y_1^4 - 2\sqrt{-3}y_1^2y_2^2 + y_2^4, \end{aligned}$$

together with the relation $12\sqrt{-3}I_2^2 - I_1^3 + I_3^3 = 0$. We will only need $I_1$ and $I_2$ to represent the coefficients of $P(Y)$.

A maximal 1-reducible subgroup of $A_4^{SL_2}$ is the cyclic group of order 6 generated by the matrix $TS^{-1}$ which has an eigenvector $z = (\omega^3 - \omega^2 + 3\omega - 1)y_1 + y_2$. A set of left coset representatives $\mathcal{T}$ of $< TS^{-1} >$ in $A_4^{SL_2}$ is

$$\{id, S, S^{-1}, TS\}$$

and the minimal polynomial of $z$ is given by:

$$P(\mathbf{Y}) = \prod_{\sigma \in \mathcal{T}} (\mathbf{Y}^6 - \sigma(z)^6),$$

which is:

$$\begin{aligned}
&\mathbf{Y}^{24} + 48\omega^3(y_2y_1^5 - y_2^5y_1)\ \mathbf{Y}^{18} \\
&+ \big((-780\omega^2 + 780\omega - 210)y_1^{12} + (-1824\omega^3 + 2736\omega^2 - 1368\omega + 228)y_2^2y_1^{10} \\
&\quad +(25740\omega^2 - 25740\omega + 6930)y_2^4y_1^8 + (3648\omega^3 - 5472\omega^2 + 2736\omega - 456)y_2^6y_1^6 \\
&\quad +(25740\omega^2 - 25740\omega + 6930)y_2^8y_1^4 \\
&\quad +(-1824\omega^3 + 2736\omega^2 - 1368\omega + 228)y_2^{10}y_1^2 + (-780\omega^2 + 780\omega - 210)y_2^{12}\big)\ \mathbf{Y}^{12} \\
&+ \big((6816\omega^3 + 2496\omega^2 - 7488\omega + 2496)y_2y_1^{17} \\
&\quad +(97088\omega^3 - 326784\omega^2 + 255744\omega - 61568)y_2^3y_1^{15} \\
&\quad +(-231744\omega^3 - 84864\omega^2 + 254592\omega - 84864)y_2^5y_1^{13} \\
&\quad +(-291264\omega^3 + 980352\omega^2 - 767232\omega + 184704)y_2^7y_1^{11} \\
&\quad +(291264\omega^3 - 980352\omega^2 + 767232\omega - 184704)y_2^{11}y_1^7 \\
&\quad +(231744\omega^3 + 84864\omega^2 - 254592\omega + 84864)y_2^{13}y_1^5 \\
&\quad +(-97088\omega^3 + 326784\omega^2 - 255744\omega + 61568)y_2^{15}y_1^3 \\
&\quad +(-6816\omega^3 - 2496\omega^2 + 7488\omega - 2496)y_2^{17}y_1\big)\ \mathbf{Y}^6 \\
&+ \big((780\omega^2 - 780\omega + 209)y_1^{24} + (-8688\omega^3 + 13032\omega^2 - 6672\omega + 1164)y_2^2y_1^{22} \\
&\quad +(-135720\omega^2 + 135720\omega - 36366)y_2^4y_1^{20} \\
&\quad +(304080\omega^3 - 456120\omega^2 + 233520\omega - 40740)y_2^6y_1^{18} \\
&\quad +(1134900\omega^2 - 1134900\omega + 304095)y_2^8y_1^{16} \\
&\quad +(-295392\omega^3 + 443088\omega^2 - 226848\omega + 39576)y_2^{10}y_1^{14} \\
&\quad +(1194960\omega^2 - 1194960\omega + 320188)y_2^{12}y_1^{12} \\
&\quad +(-295392\omega^3 + 443088\omega^2 - 226848\omega + 39576)y_2^{14}y_1^{10} \\
&\quad +(1134900\omega^2 - 1134900\omega + 304095)y_2^{16}y_1^8 \\
&\quad +(304080\omega^3 - 456120\omega^2 + 233520\omega - 40740)y_2^{18}y_1^6 \\
&\quad +(-135720\omega^2 + 135720\omega - 36366)y_2^{20}y_1^4 \\
&\quad +(-8688\omega^3 + 13032\omega^2 - 6672\omega + 1164)y_2^{22}y_1^2 \\
&\quad +(780\omega^2 - 780\omega + 209)y_2^{24}\big)
\end{aligned}$$

Using the Gröbner basis algorithm in Axiom (cf. Jenks and Sutor (1992)) we can

represent the coefficients of $P(Y)$ as polynomials in the invariants $I_1$ and $I_2$:

$$\begin{aligned}
&\mathbf{Y}^{24} + \left(48\omega^3 I_2\right)\ \mathbf{Y}^{18} \\
&+ \left((-780\omega^2 + 780\omega - 210)I_1^3 + (-6144\omega^3 + 9216\omega^2 - 4608\omega + 768)I_2^2\right)\ \mathbf{Y}^{12} \\
&+ \big((6816\omega^3 + 2496\omega^2 - 7488\omega + 2496)I_2 I_1^3 \\
&\qquad + (167936\omega^3 - 565248\omega^2 + 442368\omega - 106496)I_2^3\big)\ \mathbf{Y}^6 \\
&+ (780\omega^2 - 780\omega + 209)I_1^6
\end{aligned}$$

The above representation shows that the semi-invariant $I_2$ is a rational function and thus an invariant, and that $I_1$ is the cube root of a rational function. This last fact can also be derived using the one dimensional characters of $A_4^{SL_2}$ (cf. Lemma 1.6), since in the decomposition of the character of the sixth symmetric product of a two dimensional character of $A_4^{SL_2}$ there is exactly 1 one dimensional character $\phi$ which is of order 3 (i.e. $\phi^3 = 1$, $\phi \neq 1$). This also shows that, up to a constant, there is exactly one solution of $L^{\circledS\, 6}(y) = 0$ which is the cube root of a rational function.

We note that there are other minimal polynomials of solutions that can be derived using either another representation of the group, another eigenvector of a cyclic subgroup of order 4 or another cyclic subgroup of order 4. In Fuchs (1878) p. 21 the following decomposition of a polynomial $P(Y)$ is given:

$$\mathbf{Y}^{24} - 3\varphi\,\mathbf{Y}^{18} + (-3\chi_1^3 - 78\chi^3)\,\mathbf{Y}^{12} + (-\chi_1^3\varphi + 10\chi^3\varphi)\,\mathbf{Y}^6 - 27\chi^6,$$

where $\chi$ is an invariant of degree 4 of $A_4^{SL_2}$, $\chi_1$ (the Hessian of $\chi$) is another invariant of degree 4 and $\varphi$ (the jacobian of $\chi_1$ and $\chi$) is an invariant of degree 6.
We note that our invariants differ from those of Fuchs because we select a different basis for our representation.

**The octahedral group $S_4^{SL_2}$:**

We consider the algebraic extension $\mathbf{Q}(i, \sqrt{2})$ of the rational numbers. The group $S_4^{SL_2}$ is generated by the matrices $S$ and $U$ of section 4.1.1.

We denote $\{y_1, y_2\}$ the basis corresponding to the above representation. In this representation, the ring of semi-invariants of $S_4^{SL_2}$ is generated by (see Miller, Blichfeld and Dickson (1938), p. 224):

$$\begin{aligned}
I_1 &= y_1 y_2 (y_1^4 - y_2^4), \\
I_2 &= y_1^8 + 14 y_1^4 y_2^4 + y_2^8, \\
I_3 &= y_1^{12} - 33 y_1^8 y_2^4 - 33 y_1^4 y_2^8 + y_2^{12},
\end{aligned}$$

Together with the relation $108 I_1^4 - I_2^3 + I_3^2 = 0$. We will only need $I_1$ and $I_2$ to represent the coefficients.

A maximal 1-reducible subgroup of $S_4^{SL_2}$ is the cyclic group of order 8 generated by the above matrix $U$ and $y_1$ is an eigenvector of $U$. A set of left coset representatives $\mathcal{T}$ of $< U >$ in $S_4^{SL_2}$ is

$$\left\{id, S, US, U^2S, S^{-1}U, SUS\right\}$$

and the minimal polynomial of $z$ is given by:

$$P(\mathbf{Y}) \quad = \quad \prod_{\sigma \in \mathcal{T}} (\mathbf{Y}^8 - \sigma(z)^8)$$

Using the Gröbner basis algorithm in AXIOM II we can represent the coefficients of $P(Y)$ as polynomials in $I_1$ and $I_2$. We get the following representation for $P(Y)$:

$$\mathbf{Y}^{48} - \frac{5}{4} I_2 \, \mathbf{Y}^{40} + \frac{35}{128} I_2^2 \, \mathbf{Y}^{32} + \left( \frac{1351}{128} I_1^4 - \frac{25}{1024} I_2^3 \right) \mathbf{Y}^{24}$$
$$+ \left( \frac{265}{1024} I_2 I_1^4 + \frac{65}{65536} I_2^4 \right) \mathbf{Y}^{16} + \left( \frac{39}{32768} I_2^2 I_1^4 - \frac{1}{65536} I_2^5 \right) \mathbf{Y}^8 + \frac{1}{65536} I_1^8$$

The above representation shows that $I_2$ is a rational function and that $I_1$ is the fourth root of a rational function. Since in the decomposition of the character of the sixth symmetric product of a faithfull two dimensional character of $S_4^{SL_3}$ there is exactly 1 one dimensional character $\phi$ which is of order 2 (i.e. $\phi^2 = 1$, $\phi \neq 1$), we get that $I_1$ is the square root of a rational function (cf. Lemma 1.6). This is also derived by L. Fuchs (cf. Fuchs (1878) p. 13). The decomposition of the characters also shows that there will be, up to a constant, exactly one rational solution of $L^{\circledS 6}(y) = 0$ and exactly one solution of $L^{\circledS 6}(y) = 0$ which is the square root of a rational function, and thus, up to a constant, exactly one choice for $I_1$ and $I_2$.

The above polynomial was obtained using only one representation of $S_4^{SL_2}$, which has in fact two faithfull non equivalent representations in $SL(2, \mathcal{C})$. Since there is an automorphism $\sigma$ of the Galois group of $\mathbf{Q}(i, \sqrt{2})/\mathbf{Q}$ sending this representation to a non equivalent representation, $\sigma(P(\mathbf{Y}))$ would be the minimal polynomial of a solution for this representation. Since the above decomposition of $P(\mathbf{Y})$ contains only rational coefficients, any representation of $S_4^{SL_2}$ in $SL(2, \mathcal{C})$ will lead to a solution whose minimal polynomial is of the above form.

We again note that there are other minimal polynomials of solutions that can be derived using either another representation of the group, another eigenvector of a cyclic subgroup of order 6 or another cyclic subgroup of order 6. In Fuchs (1878) p. 21 the following decomposition of a polynomial $P(\mathbf{Y})$ is given:

$$\mathbf{Y}^{48} - 20\chi_1 \, \mathbf{Y}^{40} + 70\chi_1^2 \, \mathbf{Y}^{32} + (-100\chi_1^3 - 14 \cdot 3088\chi^4) \, \mathbf{Y}^{24}$$
$$+ (65\chi_1^4 + 40 \cdot 424\chi_1\chi^4) \, \mathbf{Y}^{16} + (-16\chi_1^5 - 1248\chi_1^2\chi^4) \, \mathbf{Y}^8 - 16^2\chi^8,$$

where $\chi$ is an invariant of degree 6 of $S_4^{SL_2}$ and $\chi_1$ (the Hessian of $\chi$) is another invariant of degree 8.

**The icosahedral group $A_5^{SL_2}$:**

We consider the algebraic extension $\mathbf{Q}(\xi)$ of the rational numbers, where $\xi^5 = 1$. The group $A_5^{SL_2}$ is generated by the matrices $S'$, $U'$ and $T'$ of section 4.1.1.

We denote $\{y_1, y_2\}$ the basis corresponding to the above representation. In this representation, the ring of invariants of $S_4^{SL_2}$ is generated by (see Miller, Blichfeld and Dickson (1938), p. 224):

$$\begin{aligned} I_1 &= y_1 y_2 (y_1^{10} + 11 y_1^5 y_2^5 - y_2^{10}), \\ I_2 &= -y_1^{20} - y_2^{20} + 228(y_1^{15} y_2^5 - y_1^5 y_2^{15}) - 494 y_1^{10} y_2^{10}, \\ I_3 &= y_1^{30} + y_2^{30} + 522(y_1^{25} y_2^5 - y_1^5 y_2^{25}) - 10005(y_1^{20} y_2^{10} + y_1^{10} y_2^{20}), \end{aligned}$$

Together with the relation $I_3^2 + I_2^3 - 1728 I_1^5 = 0$.

A maximal 1-reducible subgroup of $A_5^{SL_2}$ is the cyclic group of order 10. Such a group $H$ is generated by the matrix $U^2S$, which has an eigenvector $z = y_1$. A set of left coset representatives $\mathcal{T}$ of $H$ in $A_5^{SL_2}$ is

$$\left\{id, U, T^{-1}, UT^{-1}, ST^{-1}, TST, S^{-2}T, TS^{-2}T, USTS^{-2}, US^{-1}T, S^2T^{-1}, US^{-2}T^{-1}\right\}$$

and the minimal polynomial of $z$ is given by:

$$P(\mathbf{Y}) \quad = \quad \prod_{\sigma \in \mathcal{T}} (\mathbf{Y}^{10} - \sigma(z)^{10})$$

Using an *Ansatz* we can represent the coefficients of $P(Y)$ as polynomials in the invariants $I_1$, $I_2$ and $I_3$ we get the following representation for $P(Y)$:

$$\begin{aligned}
&\mathbf{Y}^{120} + \frac{374}{625} I_2\, \mathbf{Y}^{100} - \frac{1001}{3125} I_3\, \mathbf{Y}^{90} - \frac{142373}{1953125} I_2^2\, \mathbf{Y}^{80} \\
&+ \frac{78254}{9765625} I_2 I_3 \mathbf{Y}^{70} + \left( \frac{832814147}{5273437500000} I_2^3 - \frac{8910209}{42187500000} I_3^2 \right) \mathbf{Y}^{60} \\
&- \frac{81631}{30517578125} I_3 I_2^2\, \mathbf{Y}^{50} + \left( \frac{-39788034}{152587890625} I_1^5 I_2 - \frac{158499}{19073486328125} I_2^4 \right) \mathbf{Y}^{40} \\
&+ \left( \frac{-611864}{762939453125} I_1^5 I_3 + \frac{1254}{95367431640625} I_2^3 I_3 \right) \mathbf{Y}^{30} \\
&+ \left( \frac{103862}{476837158203125} I_1^5 I_2^2 + \frac{3124}{298023223876953125} I_2^5 \right) \mathbf{Y}^{20} \\
&+ \left( \frac{4}{2384185791015625} I_1^5 I_2 I_3 - \frac{1}{298023223876953125} I_2^4 I_3 \right) \mathbf{Y}^{10} \\
&+ \frac{1}{298023223876953125} I_1^{10}
\end{aligned}$$

Since $A_5^{SL_2}$ has only one irreducible character of degree 1, any invariant will be rational and thus not hard to compute. Since there is no polynomial relation between $I_1$, $I_2$ and $I_3$, we get that, up to a constant multiple, there will be one polynomial solution of $L^{\circledS 12}(y) = 0$, $L^{\circledS 20}(y) = 0$ and $L^{\circledS 30}(y) = 0$. This can also be derived from the decomposition of the characters of the 12-th, 20-th and 30-th symmetric product of the irreducible characters of degree 3 of $A_5^{SL_2}$.

As for $S_4^{SL_2}$ there is an element $\sigma$ of the Galois group of $\mathbf{Q}(\xi)/\mathbf{Q}$ sending the above representation in a non equivalent representation. Thus $\sigma(P(\mathbf{Y}))$ would be the minimal polynomial of a solution for this representation. Since the above decomposition of $P(\mathbf{Y})$ contains only rational coefficients, any representation of $A_5^{SL_2}$ in $SL(2, \mathcal{C})$ will lead to a solution whose minimal polynomial is of the above form.

In Fuchs (1878) (cf. p. 16) no explicit decomposition of a polynomial $P(Y)$ is given.

### 4.3.2. Third order equations

For third order equations it is not the case that any solution of $L(y) = 0$ is a primitive element of the PVE extension associated to $L(y) = 0$. For $\mathcal{G}(L) \cong H_{216}^{SL_3}$ the order of the minimal polynomial of a primitive element (which always exists) is 648, while from Corollary 4.1 there is a solution whose monic minimal polynomial is of order 81 where at most 9 non zero coefficients have to be computed.

In this section we present results involving groups, so that only the decomposition of the coefficients in terms of the fundamental invariants remains to be done. To illustrate the procedure for third order differential equations, we perform the decomposition of the minimal polynomial in the case $\mathcal{G}(L) \cong A_5$.

We consider each group separetely:

**The Valentiner group $A_6^{SL_3}$:**

The group $A_6^{SL_3}$ is generated by the matrices $E_1$, $E_2$, $E_3$ and $E_4$ given in section 4.1.2. The 1-reducible subgroups of index 36 are all conjugate. Such a 1-reducible group $H$ is generated by $E_1$, $(E_3E_1^2E_4E_1^{-1})^2$ and $E_2$. If we denote $\{y_1, y_2, y_3\}$ the basis of the solution space corresponding to the above representation, then the solution $z = y_1$ spanns a one dimensional invariant subspace of $H$.
A set of left coset representatives $\mathcal{T}$ of $H$ in $A_6^{SL_3}$ is

$$\begin{aligned}\big\{&id, E_3, E_4, E_3E_4, E_1E_3, E_3E_1E_3, E_1E_4, E_4E_1E_4, E_1^{-2}E_3, E_1^{-2}E_4, E_4E_1^{-1}E_3,\\ &E_1E_4E_1^{-1}E_3, E_1^2E_4E_1^{-1}E_3, E_1^2E_4E_1^{-1}, E_3E_1^2E_4E_1^{-1}, E_1^{-1}E_3E_1^2E_4E_1^{-1},\\ &E_1^{-1}E_3E_4, E_4E_1^{-1}E_3E_4, E_1E_4E_1^{-1}E_3E_4, E_2E_1^2E_4E_1^{-1}E_3, E_1^2E_3, E_1E_4E_3,\\ &E_4E_1E_4E_3, E_1^{-2}E_4E_3, E_4E_1^{-2}E_4E_3, E_2E_1E_4E_1^{-2}E_3, E_4E_1^2E_3E_4E_1^{-1},\\ &E_3E_1^{-2}E_3E_4, E_1E_3E_1^{-2}E_4, E_1^2E_3E_4, E_3E_1^{-1}E_3E_4, E_2E_4E_1^{-1}E_3,\\ &E_1^{-1}E_4E_1E_3, E_3E_1^2E_3E_4E_1^{-1}, E_1E_4E_1^{-1}E_3E_4E_1E_3, E_1E_4E_1^2E_4E_3E_1^{-1}\big\}\end{aligned}$$

and the minimal polynomial of $z$ is given by:

$$P(\mathbf{Y}) = \prod_{\sigma\in\mathcal{T}} (\mathbf{Y}^6 - \sigma(z)^6)$$

**The simple group $A_5$:**

The group $A_5$ is generated by the matrices $E_1$, $E_2$ and $E_3$ given in section 4.1.2. The 1-reducible subgroups of index 6 are all conjugate. Such a 1-reducible group $H$ is generated by $E_1$ and $E_2$. If we denote $\{y_1, y_2, y_3\}$ the basis of the solution space corresponding to the above representation, then the solution $z = y_1$ spanns a one dimensional invariant subspace of $H$.
A set of left coset representatives $\mathcal{T}$ of $H$ in $A_5$ is

$$\big\{id, E_3, E_1E_3, E_3E_1E_3, E_1^{-2}E_3, E_1^2E_3\big\}$$

and the minimal polynomial of $z$ is given by:

$$P(\mathbf{Y}) = \prod_{\sigma\in\mathcal{T}} (\mathbf{Y}^2 - \sigma(z)^2)$$

In the given representation (cf. reference to F. Klein in Miller, Blichfeld and Dickson (1938), p. 254), the ring of invariants of $A_5 \subset SL(3, \mathbf{C})$ is generated by:

$$\begin{aligned} I_1 &= y_1^2 + y_2y_3,\\ I_2 &= 8y_1^4y_2y_3 - 2y_1^2y_2^2y_3^2 + y_2^3y_3^3 - y_1(y_2^5 + y_3^5)\\ I_3 &= 320y_1^6y_2^2y_3^2 - 160y_1^4y_2^3y_3^3 + 20y_1^2y_2^4y_3^4 + 6y_2^5y_3^5\\ &\quad -4y_1(y_2^5 + y_3^5)(32y_1^4 - 20y_1^2y_2y_3 + 5y_2^2y_3^2) + y_2^{10} + y_3^{10}, \end{aligned}$$

and an invariant $I_4$ of degree 15. Using an *Ansatz* we can represent the coefficients of $P(Y)$ as polynomials in the invariants $I_1$, $I_2$ and $I_3$. We get the following representation for $P(Y)$:

$$\mathbf{Y}^{12} - 2I_1\,\mathbf{Y}^{10} + \frac{7}{5}I_1^2\,\mathbf{Y}^8 + \left(-\frac{12}{25}I_1^3 + \frac{2}{25}I_2\right)\mathbf{Y}^6 + \left(\frac{11}{125}I_1^4 - \frac{6}{125}I_1I_2\right)\,\mathbf{Y}^4$$
$$+ \left(-\frac{26}{3125}I_1^5 + \frac{6}{625}I_1^2I_2 - \frac{64}{625\cdot 320}I_3\right)\,\mathbf{Y}^2 + \left(\frac{1}{3125}I_1^6 + \frac{1}{3125}I_2^2 - \frac{2}{3125}I_2I_1^3\right)$$

**The group $A_5 \times C_3$:**

This group is the direct product of the previous group with the center of $SL(3,\mathbf{C})$ generated by $Z$. The 1-reducible subgroups of index 6 are all conjugate. From the previous case we get a 1-reducible group $H \times C_3$ generated by $E_1$, $E_2$ and $Z$ which has the same set of left coset representatives $\mathcal{T}$ in $A_5 \times C_3$ has $H$ in $A_5$. Since $C_3$ consists of scalar multiplications, the common eigenvector $z = y_1$ of $H$ given in the previous case will be a common eigenvector for $H \times C_3$.
The function $z^3$ of the PVE is left invariant by the normal subgroup $C_3$, which shows that $k(z^3)/k$ has Galois group $A_5$. Since $z'/z$ is left fixed by $H$, the same holds for $(z^3)'/z^3$. From Corollary 1.4 and the bound for $d$ computed in Theorem 4.1 we get that the minimal polynomial $P_3(Y)$ of $z^3$ over $k$ is given by:

$$\prod_{\sigma\in\mathcal{T}} (\mathbf{Y}^2 - \sigma(z^3)^2)$$

The following polynomial $P(Y)$ has $z$ as a solution:

$$P(\mathbf{Y}) \quad = \quad \prod_{\sigma\in\mathcal{T}} (\mathbf{Y}^6 - \sigma(z)^6)$$

and comparing degrees (cf. Theorem 4.1), we get that $P(Y)$ is the minimal polynomial of $z$.

**The simple group $G_{168}$:**

The group $G_{168}$ is generated by the matrices $S$, $T$ and $R$ given in section 4.1.2. The 1-reducible subgroups of index 21 are all conjugate. Such a 1-reducible group $H$ is generated by $S^{-2}RS$ and $RS^{-1}RTS$. If we denote $\{y_1, y_2, y_3\}$ the basis of the solution space corresponding to the above representation, then the solution

$$z \quad = \quad \left(\beta^5 + \beta^4 + \beta^2 + 1\right) y_1 + \left(\beta^5 + \beta\right) y_2 + y_3$$

spanns a one dimensional invariant subspace of $H$.
A set of left coset representatives $\mathcal{T}$ of $H$ in $G_{168}$ is

$$\{id, T, T^{-1}, S^{-1}T^{-1}, S^{-2}, S^{-1}, SR, RSR, RS^{-1}RS^{-1}, RS^{-3}, S, TS^{-1}, S^{-1}T,$$
$$SRT, RSRT, RS^{-1}RS^{-1}T, STSR, RSTSR, RTS^2, TS^2, RSRT^{-1}\}$$

and the minimal polynomial of $z$ is given by:

$$P(\mathbf{Y}) \quad = \quad \prod_{\sigma\in\mathcal{T}} (\mathbf{Y}^2 - \sigma(z)^2)$$

**The group $G_{168} \times C_3$:**

This group is the direct product of the previous group with the center of $SL(3, \mathbf{C})$ generated by $Z$. The 1-reducible subgroups of index 21 are **not** all conjugate. From the previous case we get a 1-reducible group $H \times C_3$ generated by $S^{-2}RS$, $RS^{-1}RTS$ and $Z$ which has the same set of left coset representatives $\mathcal{T}$ has $H$ in $G_{168}$. Since $C_3$ consists of scalar multiplications, the common eigenvector $z$ of $H$ given in the previous case will be a common eigenvector for $H \times C_3$.
As in the case $A_5 \times C_3$ we get the following minimal polynomial for $z$ over $k$.

$$P(\mathbf{Y}) \quad = \quad \prod_{\sigma \in \mathcal{T}} (\mathbf{Y}^6 - \sigma(z)^6).$$

**The group $H_{216}^{SL_3}$:**

The group $H_{216}^{SL_3}$ is generated by the matrices $S_1$, $T$, $V$ and $UV$ given in section 4.1.2. The 1-reducible subgroups of index 9 are all conjugate. Such a 1-reducible group $H$ is generated by $U^2V^{-1}S_1$ and $V^{-1}U^2S_1$. If we denote $\{y_1, y_2, y_3\}$ the basis of the solution space corresponding to the above representation, then the solution $-\varepsilon^3 y_1 + y_2$ spanns a one dimensional invariant subspace of $H$.
A set of left coset representatives $\mathcal{T}$ of $H$ in $H_{216}^{SL_3}$ is

$$\left\{id, V, V^2, V^{-1}, T^{-1}, S^{-1}, V^{-1}T^{-1}, VS^{-1}, V^2UT^{-1}S\right\}$$

and the minimal polynomial of $z$ is given by:

$$P(\mathbf{Y}) \quad = \quad \prod_{\sigma \in \mathcal{T}} (\mathbf{Y}^9 - \sigma(z)^9)$$

**The group $H_{72}^{SL_3}$:**

The group $H_{72}^{SL_3}$ is generated by the matrices $S_1$, $T$, $V$ and $UVU^{-1}$ given in section 4.1.2. The 1-reducible subgroups of index 9 are all conjugate. Such a 1-reducible group $H$ is generated by $S_1TUVU^{-1}$, $S_1TUVU^{-1}V$ and $S_1T^{-1}S_1^{-1}T$. If we denote $\{y_1, y_2, y_3\}$ the basis of the solution space corresponding to the above representation, then the solution $z = -y_2 + y_3$ spanns a one dimensional invariant subspace of $H$.
A set of left coset representatives $\mathcal{T}$ of $H$ in $H_{72}^{SL_3}$ is

$$\left\{id, T, T^{-1}, S, S^{-1}, TS, U^{-2}VU^{-1}, STS, U^{-1}V^{-1}U\right\},$$

and the minimal polynomial of $z$ is given by:

$$P(\mathbf{Y}) \quad = \quad \prod_{\sigma \in \mathcal{T}} (\mathbf{Y}^3 - \sigma(z)^3)$$

**The group $F_{36}^{SL_3}$:**

The group $F_{36}^{SL_3}$ is generated by $S_1$, $T$ and $V$ of section 4.1.2. A 1-reducible group $H$ is generated by $S^{-1}T$, $STS$ and $V^2T$. If we denote $\{y_1, y_2, y_3\}$ the basis of the solution space corresponding to the above representation, then the solution $y_1 + y_2 + \omega y_3$ spanns a one dimensional invariant subspace of $H$.
A set of left coset representatives $\mathcal{T}$ of $H$ in $F_{36}^{SL_3}$ is

$$\left\{id, V, V^2, V^{-1}, T^{-1}, V^{-1}T^{-1}\right\},$$

and the minimal polynomial of $z$ is given by:

$$P(\mathbf{Y}) \quad = \quad \prod_{\sigma \in \mathcal{T}} (\mathbf{Y}^6 - \sigma(z)^6)$$

## 5. Computing a solution

Let $L(y) = 0$ be an equation of degree $n$ with coefficients in $k$ and finite primitive Galois group $\mathcal{G}(L) \subset SL(n, \mathbf{C})$. Then the decomposition of the coefficients of the minimal polynomial $P(\mathbf{Y})$ of a solution given in the previous section reduces the computation of the coefficients of $P(\mathbf{Y})$ to the computation of finitely many semi-invariants of $\mathcal{G}(L)$ and of the constants of the semi-invariants, which can be done using a Gröbner basis (for second order equation only gcd computation are needed). In fact, since the coefficients are invariants of $\mathcal{G}(L)$, only powers of the semi-invariants which are rational functions have to be computed. This reduces the computations to the computation of rational solutions of some symmetric power of $L(y) = 0$.

To compute the coefficients of $P(\mathbf{Y})$ one can proceed in the following way:

From the a representation of the minimal polynomial $P(Y)$ of a solution $y$ of $L(y) = 0$ in terms of the semi-invariants of $G$ one can compute the coefficients of $P(Y)$ in the following way:

i) Compute the set $\mathcal{L}$ of $i$-th symmetric powers $L^{\circledS i}(y)$ of $L(y) = 0$, where $i$ belongs to the set of orders of the semi-invariants appearing in the decomposition of the coefficients of $P(Y)$.

ii) for each equation in $\mathcal{L}$, compute a solution $f_i$ such that $f_i^j \in k$, where $j$ belongs to the set of orders of the one dimensional characters of $\mathcal{G}(L)$ (cf. Lemma 1.6). In general the possible $j$'s can be further restricted by looking at the decomposition of $P(Y)$ in terms of the semi-invariants of $\mathcal{G}(L)$ and noting that the coefficients of $P(Y)$ must be rational.

iii) For each possible value $f_i$ (defined up to a constant $c_i$) of the invariants $I_i$ obtained, replace $I_i$ by $c_i \cdot f_i$ in $P(Y) = 0$. This gives a new polynomial $Q(Y) = 0$ whose coefficients are polynomials in the variables $c_i$ over $k$.

iv) For $s \leq n$, using $Q(Y) = 0$, express the derivatives $Y^{(s)}$ of $Y$ as a polynomial in $Y$ and replace $Y^{(s)}$ by this value in $L(y) = 0$. This gives a polynomial $\overline{P}(Y) = 0$ whose coefficients are polynomials in the variables $c_i$ over $k$.

v) compute the rest $R(Y)$ of the division of $\overline{P}(Y)$ by $Q(Y)$ and determine the constants $c_i$ by setting all coefficients of $R(Y)$ equal to 0. For $i \geq 2$ this can be done using a Gröbner basis.

vi) If a non trivial solution set $\{c_i\}$ is found, then replacing $c_i$ by these values in $Q(Y)$ gives the minimal polynomial of a solution of $L(y) = 0$.

The above method is based on the fact that the polynomial $Q(Y)$ is at least square free. If the cases are considered without knowing the group $\mathcal{G}(L)$, then one has to start with the cases where the polynomial to be constructed is of smallest degree (e.g. first the case $A_4^{SL_2}$, then $S_4^{SL_2}$ and then $A_5^{SL_2}$) and test if the resuling polynomial is square free. Another possibility would be to use the method given in Singer and Ulmer (1992) to determine the differential Galois group of $L(y) = 0$ and make sure that the assumption on $\mathcal{G}(L)$ is correct.

EXAMPLE. We now apply the above method to compute the solutions of the differential equation

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

which is also studied in Kovacic (1986), p. 23 and Ulmer (1991), p 452. From the result of Kovacic (1986) we know that $\mathcal{G}(L) \cong A_4^{SL_2}$. This could also be computed using the result of Singer and Ulmer (1992) by showing that $L^{\circledS 2}(y)$ is irreducible and $L^{\circledS 3}(y)$ is reducible.

In Section 4.3.1 we decomposed the coefficients of $P(Y)$ and noted that the only semi-invariants present are $I_1$, a semi-invariant of degree 4, and $I_2$, a semi-invariant of degree 6. Furthermore, one can see from the form of the coefficients of $P(Y)$ (or from the orders of the associated characters) that ${I_1}^3$ and $I_2$ are rational. To compute $I_1$ we compute the 4-th symmetric power of $L(y) = 0$:

$$\begin{aligned} L^{\circledS 4}(y) &= \frac{d^5y}{dx^5} \\ &\quad + \frac{5(32x^2-27x+27)}{36x^2(x-1)^2}\,\frac{d^3y}{dx^3} \\ &\quad - \frac{5(64x^3-81x^2+135x-54)}{24x^3(x-1)^3}\,\frac{d^2y}{dx^2} \\ &\quad + \frac{5(1760x^4-2970x^3+6615x^2-5103x+1458)}{324x^4(x-1)^4}\,\frac{dy}{dx} \\ &\quad - \frac{5(1792x^5-3780x^4+10395x^3-11718x^2+6561x-1458)}{324x^5(x-1)^5}\,y \\ &= 0\,. \end{aligned}$$

We must find a solution $y$ of this equation such that $y^3 \in \mathbf{C}(x)$. Since only ${I_1}^3$ is needed, it is enough to compute the rational solution $y^3$ of $L^{\circledS 12}(y) = 0$ (cf. Lemma 1.6). To compute $y$ one can either use the algorithm described at the begining of Section 3.2 or more simply proceed as follows: Let

$$y = \left(P(x)\prod_i (x-\alpha_i)^{n_i}\right)^{1/3},$$

where $P(x)$ is a polynomial, $\{\alpha_i\}$ are the singular points of $L^{\circledS 4}(y)$ and $n_i$ are non-negative integers. This implies that for each $i$, $n_1/3$ is an exponent at $\alpha_i$ and that the exponent at infinity is $\frac{-1}{3}\,(deg(P) + \sum n_i)$. Checking the possibilities shows that $P(x)$ must be constant and that $I_2$ must be a constant multiple of $x(x-1)^{4/3}$ or $x(x-1)^{5/3}$.

From a similar computation we get the solution $x^2(x-1)^2$ for $L^{\circledS 6}(y) = 0$ (see e.g. Ulmer (1991)).

We set $I_1 = c_1x(x-1)^{4/3}$ and $I_2 = c_2x^2(x-1)^2$ in $P(Y)$ and get a polynomial $Q(Y)$ whose coefficients are polynomials in $c_1$ and $c_2$. Using $Q(Y) = 0$ we write $Y'$ and $Y''$ as a fraction of polynomials in $Y$ and substitute those in $L(y) = 0$. The numerator of the rational function in $Y$ obtained in this way is a polynomial $\overline{P}(Y)$ having a common

solution with $Q(Y) = 0$. The pseudo remainder $R(Y)$ of $\overline{P}(Y)$ and $Q(Y) = 0$ is a polynomial in $Y$ of degree at most 23 which must be zero. Thus all coefficients of $R(Y)$ must be zero, which gives a set of polynomials in $c_1$, $c_2$ and $x$. Equating coefficients of powers of $x$ to zero, gives a set of polynomials in $c_1$ and $c_2$. We now can compute a Gröbner basis to find the constants $c_1$ and $c_2$ and get:

$$[432c_1^2c_2^4 + c_1^4, (-48\omega^3 + 72\omega^2 - 192\omega + 84)c_1^2c_2^4 + c_1^3c_2^2]$$

In order for $Q(Y) = 0$ to be an irreducible polynomial we must have $c_1 \neq 0$ and $c_2 \neq 0$. Setting $c_2 = 1$ we get $c_1 = 48\omega^3 - 72\omega^2 + 192\omega - 84$, which we also write $\sqrt{-432}$. This gives the following minimal polynomial of a solution of $L(y) = 0$:

$$\begin{aligned}
&\mathbf{Y}^{24} + \left(48\omega^3x^2(x-1)^2\right)\ \mathbf{Y}^{18} \\
&+ \Big((-780\omega^2 + 780\omega - 210)\left(\sqrt{-432}\right)^3x^3(x-1)^4 \\
&\qquad +(-6144\omega^3 + 9216\omega^2 - 4608\omega + 768)x^4(x-1)^4\Big)\ \mathbf{Y}^{12} \\
&+ \Big((6816\omega^3 + 2496\omega^2 - 7488\omega + 2496)\left(\sqrt{-432}\right)^3x^5(x-1)^6 \\
&\qquad + (167936\omega^3 - 565248\omega^2 + 442368\omega - 106496)x^6(x-1)^6\Big)\ \mathbf{Y}^6 \\
&+(780\omega^2 - 780\omega + 209)\left(\sqrt{-432}\right)^6x^6(x-1)^8
\end{aligned}$$

□

The above shows that for the Tetrahedral group (as for any second order equation with primitive unimodular Galois group) the computation of the minimal polynomial of a solution is reduced to the computation of two semi-invariants (i.e. solutions of symmetric powers whose power is rational) and two constants. In fact one constant can be choosen arbitrary so that only one constant remains to be computed. This shows that for second order equations the constant can be computed using only gcd computations. In the paper of Fuchs it is shown that using the Hessian $H(I_1)$ and Jacobian $J(I_1, H(I_1))$ of an invariant $I_1$ of lowers degree, one gets the other invariants. For the tetrahedral group $A_4^{SL_2}$ one has (Miller, Blichfeld and Dickson (1938), p. 226)

$$I_3 = \frac{H(I_1)}{48\sqrt{-3}} = \frac{1}{48\sqrt{-3}}\begin{vmatrix} \dfrac{\partial^2 I_1}{\partial y_1 \partial y_1} & \dfrac{\partial^2 I_1}{\partial y_1 \partial y_2} \\ \dfrac{\partial^2 I_1}{\partial y_2 \partial y_1} & \dfrac{\partial^2 I_1}{\partial y_2 \partial y_2} \end{vmatrix}$$

$$I_2 = \frac{J(I_1, I_3)}{-32\sqrt{-3}} = \frac{1}{-32\sqrt{-3}}\begin{vmatrix} \dfrac{\partial I_1}{\partial y_1} & \dfrac{\partial I_1}{\partial y_2} \\ \dfrac{\partial I_3}{\partial y_1} & \dfrac{\partial I_3}{\partial y_2} \end{vmatrix}$$

Fuchs then shows how, as a function in $x$, for a given differential equation $L(y) = y'' - r(x)y = 0$ the Hessian $\chi_1$ and Jacobian $\varphi$ of an invariant $\chi$ of minimal degree can be written as a polynomial in $\chi(x)$ and derivatives of $\chi(x)$. He proves the following relations

(Fuchs (1878), pp. 21-22):

$$\begin{aligned}\chi_1(x) &= c\left[\left(\frac{d\log\,\chi(x)}{dx}\right)^2 + 4\frac{d^2\log\,\chi(x)}{dx^2} - 16r\right]\chi(x)^2\\ \varphi(x) &= \sqrt{-\chi_1(x)^3 + 64\chi(x)^3},\end{aligned}$$

where $c$ is a constant that can be computed (Fuchs (1878), p. 22). If we let $\chi$ be the invariant $I_1$ used in Miller, Blichfeld and Dickson (1938), these formulas also yield expressions for $I_2$ and $I_3$.

This reduces the above to the computation of one semi-invariant of lowest degree and one constant.

We now compute an example of a third order differential equation:

Example. We now apply the above method to compute the solutions of the differential equation

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

which is irreducible and has Galois group $A_5$ (cf. Singer and Ulmer (1992), section 5).

Since the invariants of $A_5 \subset SL(3,\mathbf{C})$ are of order 2, 6 and 10, we have to compute rational solutions of the second, 6-th and 10-th symmetric powers of $L(y) = 0$. The equation $L^{\circledS 2}(y) = 0$ has no non trivial rational solution. The subspaces of rational solutions of $L^{\circledS 6}(y) = 0$ and $L^{\circledS 10}(y) = 0$ each are one dimensional and generated by $x^4(x-1)^4$ and $x^6(x-1)^6(x^2-x+1)$ respectively.

We set $I_1 = 0$, $I_2 = c_2x^4(x-1)^4$ and $I_3 = c_3x^6(x-1)^6(x^2-x+1)$ in $P(Y)$ and get a polynomial $Q(Y)$ whose coefficients are polynomials in $c_2$ and $c_3$. Using $Q(Y) = 0$ we write $Y'$ and $Y''$ as a fraction of polynomials in $Y$ and substitute those in $L(y) = 0$. The numerator of the rational function in $Y$ obtained this way is a polynomial $\overline{P}(Y)$ having a common solution with $Q(Y) = 0$. The pseudo remainder $R(Y)$ of $\overline{P}(Y)$ and $Q(Y) = 0$ is a polynomial in $Y$ of degree at most 11 which must be zero. Thus all coefficients of $R(Y)$ must be zero, which gives a set of polynomials in $c_2$ and $c_3$. We now can compute a Gröbner basis to find the constants $c_2$ and $c_3$ and get:

$$[-\frac{1}{256}c_2^3c_3^3 + c_2^8, -\frac{1}{256}c_2c_3^4 + c_2^6c_3, -\frac{1}{256}c_3^5 + c_2^5c_3^2]$$

Since $I_1 = 0$, we must have $c_2 \neq 0$ and $c_3 \neq 0$ in order for $Q(Y) = 0$ to be an irreducible polynomial with Galois group $A_5$. Setting $c_3 = 1$ we get $c_2^5 = 1/256$. This gives the following minimal polynomial of a solution of $L(y) = 0$:

$$\mathbf{Y}^{12} + \frac{2}{25}\frac{x^4(x-1)^4}{2\sqrt[5]{8}}\mathbf{Y}^6 - \frac{64x^6(x-1)^6(x^2-x+1)}{625\cdot 320}\,\mathbf{Y}^2 + \frac{1}{3125}\left(\frac{x^4(x-1)^4}{2\sqrt[5]{8}}\right)^2$$

□

The above method turned out to be very efficient. The computation of a minimal polynomial (assuming known the decomposition of the minimal polynomial in term of the invariants) could be done in both cases in much less than 1 CPU hour on an IBM RISC 6000 with 64MB of main memory. An attempt to compute the minimal polynomial of

the logarithmic derivative of a solution of the above second order equation (which is used as an example in Kovacic (1986)) using the implementation in MAPLE of the Kovacic algorithm on a SUN 4 with 20MB of main memory did not give any result within 10 CPU hours.

We note, that the above computations can always be done in an algebraic extension $\mathbf{Q}(\alpha)$ of $\mathbf{Q}$ containing the finite singular points of $L(y) = 0$, the entries of the matrices in the transversal $\mathcal{T}$, the coordinates of the common eigenvector of the choosen 1-reducible subgroup $H$ and the coefficients of the invariants of $\mathcal{G}(L)$. Thus no additional algebraic extension is needed at runtime. However, as show in both examples, the coefficients of $P(Y) = 0$ (i.e. the result of the Gröbner basis computation) do not in general belong to $\mathbf{Q}(\alpha)(x)$. Note that the final Gröbner basis computation will yield polynomials whose roots generate an extension $F$ of $\mathbf{Q}(\alpha)$ such that the coefficients belong to $F(x)$.

## A. The character tables of the subgroups of index $\leq 6$ of the Schur representation group of $A_5$

We denote $G$ the Schur representation group of $A_5$ wihch is of order 120. The table of the irreducible characters of degree $\leq 3$ of $G$ produced by CAYLEY is:

| *class* | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| *conj* | 1 | 1 | 20 | 30 | 12 | 12 | 20 | 12 | 12 |
| *order* | 1 | 2 | 3 | 4 | 5 | 5 | 6 | 10 | 10 |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 2 | $-2$ | $-1$ | 0 | $z_1$ | $-1-z_1$ | 1 | $-z_1$ | $1+z_1$ |
| $\chi_3$ | 2 | $-2$ | $-1$ | 0 | $-1-z_1$ | $z_1$ | 1 | $1+z_1$ | $-z_1$ |
| $\chi_4$ | 3 | 3 | 0 | $-1$ | $-z_1$ | $1+z_1$ | 0 | $-z_1$ | $1+z_1$ |
| $\chi_5$ | 3 | 3 | 0 | $-1$ | $1+z_1$ | $-z_1$ | 0 | $1+z_1$ | $-z_1$ |

where $z_1 = -1 - \omega^2 - \omega^3$ and $\omega = e^{2\pi i/5}$.

The subgroups of $G$ of index $\leq 6$ are of index 5 or 6.

The subgroups of index 5 are all congugate and the table of the irreducible characters of degree $\leq 3$ of of such a group produced by CAYLEY is:

| *class* | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| *conj* | 1 | 1 | 4 | 4 | 6 | 4 | 4 |
| *order* | 1 | 2 | 3 | 3 | 4 | 6 | 6 |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | $-1-J$ | $J$ | 1 | $-1-J$ | $J$ |
| $\chi_3$ | 1 | 1 | $J$ | $-1-J$ | 1 | $J$ | $-1-J$ |
| $\chi_4$ | 2 | $-2$ | $-1$ | $-1$ | 0 | 1 | 1 |
| $\chi_5$ | 2 | $-2$ | $-J$ | $1+J$ | 0 | $J$ | $-1-J$ |
| $\chi_6$ | 2 | $-2$ | $1+J$ | $-J$ | 0 | $-1-J$ | $J$ |
| $\chi_7$ | 3 | 3 | 0 | 0 | $-1$ | 0 | 0 |

where $J = e^{2\pi i/3}$.

The subgroups of index 6 are all congugate and the table of the irreducible characters of degree $\leq 3$ of of such a group produced by CAYLEY is:

| $class$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $conj$ | 1 | 1 | 5 | 5 | 2 | 2 | 2 | 2 |
| $order$ | 1 | 2 | 4 | 4 | 5 | 5 | 10 | 10 |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | $-I$ | $I$ | 1 | 1 | $-1$ | $-1$ |
| $\chi_3$ | 1 | 1 | $-1$ | $-1$ | 1 | 1 | 1 | 1 |
| $\chi_4$ | 1 | $-1$ | $I$ | $-I$ | 1 | 1 | $-1$ | $-1$ |
| $\chi_5$ | 2 | $-2$ | 0 | 0 | $z_1$ | $-1-z_1$ | $-z_1$ | $1+z_1$ |
| $\chi_6$ | 2 | $-2$ | 0 | 0 | $-1-z_1$ | $z_1$ | $1+z_1$ | $-z_1$ |
| $\chi_7$ | 2 | 2 | 0 | 0 | $z_1$ | $-1-z_1$ | $z_1$ | $-1-z_1$ |
| $\chi_8$ | 2 | 2 | 0 | 0 | $-1-z_1$ | $z_1$ | $-1-z_1$ | $z_1$ |

where $I = e^{2\pi i/4}$, $z_1 = -1-\omega^2-\omega^3$ and $\omega = e^{2\pi i/5}$.

**Acknowledgment:** We would like to thank J. Cannon for his support regarding the group theory system CAYLEY and M. Bronstein for his help with AXIOM.

## References

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

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

Boulanger, A. (1898). Contribution á l'étude des équation différentielles linéaires homogènes intégrable algébriquement. *J. École Polytechnique*, série 2, **4**.

Bronstein, M. (1992). On solutions of linear differential equation in their coefficient field. *J. Symb. Comp.* **13**

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

Cox, D., Little, J., O'Shea, D. (1992). *Ideals, Varieties and Algorithms.* New York: Springer Verlag.

Curtis, C. W., Reiner, I. (1962). *Representation theory of finite groups and associative algebras.* London: Interscience Publishers

Fuchs, L. (1875). Ueber die linearen Differentialgleichungen zweiter Ordnung, welche algebraische Integrale besitzen, und eine neue Anwendung der Invariantentheorie. *J. für Math.* **81**.

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

Gray, J. (1986). *Linear differential equations and group theory from Riemann to Poincaré.* Boston, Basel, Stuttgart: Birkhäuser.

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

Huppert, B. (1983). *Endliche Gruppen I.* New York: Springer Verlag.

Issacs, M. (1976). *Character theory of finite groups.* Academic Press Inc

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

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

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

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

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.

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

Miller, G.A., Blichfeld, H.F., Dickson, L.E. (1938). *Theory and Applications of Finite Groups.* New York: G. E. Stechert and Co.

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.

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. (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. Symb. Comp.* **11**.

Singer, M. F., Ulmer, F. (1992) Galois group of second and third order Linear differential equations. to appear in the J. of Symb. Comp.

Tournier, E. (1987). *Solutions formelles d'équations différentielles.* Grenoble, IMAG, TIM3: Thèse d'état

Ulmer, F. (1991). *On Algebraic Solutions of Linear Differential Equations with Primitive Unimodular Galois Group.* Proceedings of the 1991 Conference on Algebraic Algorithms and Error Correcting Codes, Springer Lecture Notes in Computer Science, Vol. 539.

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