J. Symbolic Computation (1995) **11**, 1–000

Irreducible Linear Differential Equations of Prime Order

FELIX ULMER†

IRMAR

Université de Rennes I

Campus de Beaulieu

F-35042 Rennes Cedex

Email: ulmer@univ-rennes1.fr

(Received 11 February 1994)

With the exception of a finite set of finite differential Galois groups, if an irreducible linear differential equation $L(y) = 0$ of prime order with unimodular differential Galois group has a Liouvillian solution, then all algebraic solutions of smallest degree of the associated Riccati equation are solutions of a unique minimal polynomial. If the coefficients of $L(y) = 0$ are in $\mathbb{Q}(\alpha)(x) \subset \overline{\mathbb{Q}}(x)$ this unique minimal polynomial is also defined over $\mathbb{Q}(\alpha)(x)$. In the finite number of exceptions all solutions of $L(y) = 0$ are algebraic and in each case one can apriori give an extension $\mathbb{Q}(\beta)(x)$ over which the minimal polynomial of an algebraic *solution* of $L(y) = 0$ can be computed.

1. Introduction

In this paper we consider linear differential equations of the form

$$L(y) = \frac{d^p y}{dx^p} + a_{p-1}\frac{d^{p-1} y}{dx^{p-1}} + \ldots + a_0 y, \qquad a_i \in k \tag{1.1}$$

where p is a prime and k is a differential field whose field of constants is algebraically closed of characteristic 0. We also assume that there exists $b \in k$ such that $b'/b = a_{p-1}$ (i.e. the differential Galois group is unimodular), which can always be achieved by a suitable variable transformation without altering the Liouvillian character of the solutions (cf. Kaplansky (1957), p. 41). We will also only consider irreducible equations $L(y)$ (i.e. whose differential Galois group are irreducible linear groups), leaving the case of a reducible equation as an induction case (cf. Singer and Ulmer (1993b), Section 2). We note that if $L(y) = 0$

† This paper was prepared during the author's visit at the Department of Mathematics at Cornell University during the Fall semester of 1993. This work was supported in part by the David and Lucile Packard Foundation

0747–7171/90/000000 + 00 $03.00/0

is reducible of order > 3, the bounds used in the algorithms (cf. Singer (1981), Singer and Ulmer (1993b), Ulmer (1992)) are not as good as in the irreducible case and that a factorisation should be computed first.

The current algorithms to compute Liouvillian solutions (see e.g. Kovacic (1986), Singer and Ulmer (1993b) or Ulmer (1992) for definitions) of $L(y) = 0$ require to consider the coefficients a_i of $L(y)$ in a differential field whose field of constants is algebraically closed. Thus, even if the coefficients are in $\mathbb{Q}(\alpha)(x) \subset \overline{\mathbb{Q}}(x)$, one has to consider them as being in $\overline{\mathbb{Q}}(x)$. This means that an algebraic extension $\mathbb{Q}(\alpha, \gamma)$ of $\mathbb{Q}(\alpha)$ might be needed in the computations and in the result. It is likely that an appriori knowledge of this extension would simplify the computation, in particular in the cases where one knows beforehand that no such extension is needed.

If $L(y) = 0$ has a Liouvillian solution, then $L(y) = 0$ has a solution z whose logarithmic derivative $w = z'/z$ is algebraic over k (cf. Singer (1981)). The computation of the Liouvillian solutions can thus be reduced to the computation of the minimal polynomial of some algebraic solution of the Riccati equation $R(u) = 0$ associated with $L(y) = 0$. For imprimitive linear groups, this is the only known method. Recently some new results Hendriks and Van der Put (1993) and Zharkov (1993) have been obtained concerning the problem of rationality for this computation. We denote by $\mathcal{P}_R = \{P_1, P_2, \ldots\}$ the set of all minimal polynomials of an algebraic solution of minimal degree of $R(u) = 0$. We have $\mathcal{P}_R \neq \{\}$ if and only if $L(y) = 0$ has a Liouvillian solution (cf. Singer (1981)). If the coefficients of $L(y) = 0$ belong to $\mathbb{Q}(\alpha)(x) \subset \overline{\mathbb{Q}}(x)$, then the degree of the algebraic extension $\mathbb{Q}(\alpha, \gamma)/\mathbb{Q}(\alpha)$ can be bounded by the number of elements of $\mathcal{P}_R$ (cf. Hendriks and Van der Put (1993)). In Hendriks and Van der Put (1993) and Zharkov (1993) the number of elements of $\mathcal{P}_R$ has been bounded for the primes $p = 2$ and $p = 3$. However, the results do not produce the extension $\mathbb{Q}(\gamma)/\mathbb{Q}$ or characterize the linear differential equations, via its coefficients, for which such an extension might be needed.

We show that for an irreducible equation of prime order and unimodular differential Galois group one can always distinguish the two following cases:

1 $\mathcal{P}_R$ contains exactly one element. If the coefficients of $L(y) = 0$ belong to $\mathbb{Q}(\alpha)(x) \subset \overline{\mathbb{Q}}(x)$, then the coefficients of the unique element of $\mathcal{P}_R$ are in $\mathbb{Q}(\alpha)(x)$.
2 The differential Galois group of $L(y) = 0$ belongs to a finite set of finite groups. In this case all solutions of $L(y) = 0$ are algebraic and the minimal polynomial of a solution of $L(y) = 0$ can be constructed according to Singer and Ulmer (1993b). If the coefficients belong to $\mathbb{Q}(\alpha)(x) \subset \overline{\mathbb{Q}}(x)$ one can, for each group, appriori give an algebraic extension $\mathbb{Q}(\alpha, \beta)$ of $\mathbb{Q}(\alpha)$ so that all computations can be done in $\mathbb{Q}(\alpha, \beta)$†.

In particular the algebraic extension needed during the computation is not only of bounded degree but known in advance.

Considering first the finite set of possible finite groups, one can then assume that $\mathcal{P}_R$ contains exactly one element with coefficients in $\mathbb{Q}(\alpha)(x)$. We note that in the existing algorithms (Kovacic (1986), Singer and Ulmer (1993b)) one already has to consider separately a finite set of finite groups (the primitive linear groups). For second order equations only

† The result, i.e. the coefficients, may not be expressible over $\mathbb{Q}(\beta)$, but the final Gröbner basis computation will yield polynomials whose roots generate an extension F of $\mathbb{Q}$ such that the coefficients belong to $F(x)$ (cf. Section 5.2)

the group of quaternions and for third order equations only 2 imprimitive groups of order resp. 27 and 54 must be added to the list of finite primitive groups.

For each prime p the approach also produces examples of an imprimitive subgroup of $SL(p,\mathbb{C})$ for which the number of elements of $\mathcal{P}_R$ is exactly $p+1$.

The paper is organised as follows: In the first section we derive properties of monomial groups. In the second we connect maximal normal subgroups and elements of $\mathcal{P}_R$. We then show that the above case distinction is always possible. In the fourth section we show how a minimal polynomial of a solution can be computed directly for a known finite differential Galois group and apply this method to an example. We also derive necessary conditions in terms of exponents which must be satisfied, if a given finite group is the differential Galois group of a given equation.

2. Abelian normal subgroups of monomial groups

The aim of this section is to determine the structure of a monomial group containing two distinct maximal abelian normal subgroups. We will show in the next section that those subgroups correspond to distinct elements $P_i \in \mathcal{P}_R$, i.e. to cases where $\mathcal{P}_R$ has more than one element.

Definition & Theorem: (see e.g. Dixon (1971), Theorem 4.2B) *Let G be a subgroup of $GL(n,\mathcal{C})$ acting irreducibly, i.e. G is a linear group acting irreducibly on the vector space V of dimension n over $\mathcal{C}$. Then G is called* imprimitive *if, for $k>1$, there exist subspaces $V_1,\cdots,V_k$ such that $V=V_1\oplus\cdots\oplus V_k$ and $\mathcal{S}=\{V_1,\ldots,V_k\}$ is a transitive G-set. This gives a homomorphism ϕ of G onto a transitive subgroup $T_{\mathcal{S}}$ of k elements. All the V_i have the same dimension n/k and the set $\mathcal{S}$ is called a* system of imprimitivity *of G. The stabilizer of V_i is denoted G_i and $\cap_i G_i$ is a normal subgroup of G.*
An irreducible group $G\subseteq GL(n,\mathcal{C})$ which is not imprimitive is called primitive.
If all the subspaces V_i are one-dimensional, then G is called monomial. *In this case $\cap_i G_i$ is a maximal abelian normal subgroup of G. If $\cap_i G_i \subseteq Z(G)$ we say that G is* central-monomial *of degree n. There are only finitely many central-monomial subgroups of $SL(n,\mathbb{C})$, since the order of such a group divides $n\cdot(n!)$. A central-monomial group of degree n is a central extension of a transitive permutation group of degree n. If G is monomial but not central-monomial, then $\cap_i G_i$ is a non-central maximal abelian normal subgroup of G.*

We note that an irreducible representation of degree n of a group G is imprimitive if and only if the representation is induced by a representation of degree m of a subgroup H of index k with $n=k\cdot m$ and $1\le k<n$ (cf. Issacs (1976), pp. 65-66). This gives a constructive method to test if a given representation is imprimitive. If ζ is a character of H, we denote the induced character of G by ζ^G.

Let V be a finite dimensional $\mathcal{C}$-vectorspace, $G\subseteq GL(V)$ and H a subgroup of G. Let W be a minimal H-invariant subspace of V. Then the *homogeneous component* V_W of H associated with W is the H-invariant subspace of V formed as the sum of all H-invariant subspaces W' which are isomorphic with W as H-modules (cf. Dixon (1971), §4.2).

Imprimitivity is closely related to the existence of certain normal subgroups (cf. Dixon (1971), §4.2). In particular, if an irreducible group $G\subseteq GL(n,\mathbb{C})$ has a non-central normal abelian subgroup, then G is imprimitive (see e.g. Dixon (1971), Corollary 4.2A). However, the converse is false, i.e. not any monomial group has a non-central normal abelian subgroup:

Example. - Let G be the alternating group on 5 letters. Then G has a unique irreducible faithful character χ of degree 5. The subgroup H generated by the permutations $(1,3,4)$ and $(1,5,3)$ of index 5 is isomorphic to A_4 and thus has exactly two non-trivial linear characters, say $\zeta_i, i \in \{1,2\}$. Clearly, by Frobenius' reciprocity, the trivial character of G is not a constituent of ζ_i^G. Since G has five irreducible characters the degrees of which are respectively 1, 3, 3, 4 and 5, we get that $\zeta_i^G = \chi$. In particular χ is the character of an imprimitive and central-monomial representation of G. $\diamond$

We note that there are no *central-monomial* subgroups of $SL(2,\mathbb{C})$. The order of such a group must divide 4 and the group would be abelian. Also, there are no *central-monomial* subgroups of $SL(3,\mathbb{C})$. Such a group is a central extension of A_3 or S_3 which both have a trivial *Schur-Multiplicator* (see e.g. Issacs (1976) or Ulmer (1992)). Since neither A_3 nor S_3 have an irreducible representation of degree 3 we get that such a group does not exist. The above example shows that $SL(5,\mathbb{C})$ has a *central-monomial* subgroup.

Example. - For $p = 2$ there exist two non-abelian groups of order $p^3 = 8$, the dihedral group D_4 and the quaternion group Q_8. Since D_4 contains non-central elements of order 2, the group has no faithful irreducible representation in $SL(2,\mathbb{C})$. An irreducible representation of Q_8 in $SL(2,\mathbb{C})$ is given in section 5.1.1.
For a prime $p > 2$ there exist two non-abelian groups of order p^3: The *extra-special* group $E_{p,1}$ of order p^3 and exponent p and the *extra-special* group $E_{p,2}$ of order p^3 of exponent p^2 (cf. Huppert (1983), Ch. 1, Theorem 14.10). Both groups have $p-1$ irreducible representations of degree p (Huppert (1983), Ch. V, Theorem 17.13) which must be monomial since the groups are nilpotent (Huppert (1983), Ch. V, Theorem 18.5). Since we will restrict our attention to unimodular groups we note that:

1 The representations of degree p of $E_{p,1}$ must be unimodular. Consider the subgroup generated by an arbitrary non-central element g and the center. This abelian group is of index p and normal. Since the group is not central all homogeneous components are one-dimensional. In particular all eigenvalues of g are distinct p-th roots of unity and their product, since $p > 2$, is 1.

2 Any representation of degree p of $E_{p,2}$ has a non-central element g of order p^2 with $det(g) \neq 1$. To see this note that $g^p \neq 1$ is a central element of order p and thus g^p is a scalar multiplication by a primitive p-th root of unity ε. Using the same argument as above we get that all eigenvalues of g are distinct p-th roots of $\varepsilon \neq 1$ and that their product is ε. Thus none of the monomial representations of degree p of $E_{p,2}$ is unimodular.

This allows the following

DEFINITION 2.1. *We denote N_p the (up to isomorphism) unique non-abelian subgroup of order p^3 of $SL(p,\mathbb{C})$. For $p = 2$ this is the group of quaternions and for $p \geq 3$ it is the extra-special group of exponent p.*

THEOREM 2.1. *Let p be prime and $G \subseteq SL(p,\mathbb{C})$ be an imprimitive linear group. If G has two distinct maximal normal abelian subgroups, then:*

1 G is isomorphic to a split extension $C \rtimes N_p$ of N_p and a cyclic group C of order dividing $p-1$. In particular the order of G divides $p^3(p-1)$.

2 There are at most $p+1$, for $G \cong N_p$ exactly $p+1$, distinct maximal normal abelian subgroups of G.

PROOF. 1 We denote by A_1 and A_2 the two distinct maximal normal abelian subgroups of G. The groups A_i must both properly contain the center $Z(G)$ of G which, since G is unimodular, is of order 1 or p. Put $N = A_1A_2$ and note that N is a non-abelian normal subgroup of G. In particular, N is not contained in $Z(G)$. If N was reducible, then the dimension of a homogeneous component of N would be 1 or p; in any case N would be abelian, a contradiction. Hence N is irreducible.

For the commutator subgroup N' of N we have $1 \neq N' \subseteq A_1 \cap A_2 \subseteq Z(N)$. By Dixon (1971), Theorem 4.3 the group $N/Z(N)$ must be abelian of order p^2. Since N is non-abelian and acts irreducibly we have $|Z(N)| = p$ which implies $|N| = p^3$ and $|N : A_i| = p$. In particular $N \cong N_p$. The p distinct homogeneous components of A_i form a system of imprimitivity for G. This gives a homomorphism of G/A_i onto a transitive subgroup T_{A_i} of S_p which shows that the order of G/A_i must divide $(p!)$. Since G/A_i divide $(p!)$ and $|A_i| = p^2$, the largest power of p dividing the order of G is at most p^3. Thus N is a p-Sylow subgroup of G. Since N is a normal subgroup of G, it is the unique subgroup of order p^3 of G.

From the above we have that the order of G divides $p^2 \cdot (p!)$ and thus for $p = 2$ the order must be 2^3 and we must have $G = N \cong N_2$, the group of quaternions. We now consider the case $p \geq 3$. Since both A_i and N are normal subgroups of G, the group N/A_i is a normal subgroup of $G/A_i = T_{A_i} \subseteq S_p$, which shows that the transitive permutation group T_{A_i} also has a normal p-Sylow subgroup. Thus T_{A_i} is generated by an element P of order p and an element Q whose order divides $p-1$ (cf. Huppert (1983), Ch. 5, Theorem 21.1).

From Huppert (1983), Ch. 1, Theorem 18.1 we get that $N \cong N_p$ has a complement in G which must be isomporphic to the cyclic group generated by Q. This gives the semi-direct product representation stated in the theorem.

2 Assume that G has a third maximal normal abelian subgroup A_3. Using the above reasoning for, say, A_2 and A_3 we get that A_2A_3 is a non-abelian normal subgroup of G of order p^3. Since N is the only subgroup of G of order p^3, A_2A_3 and thus A_3 must be contained in N. In particular any maximal normal abelian subgroup of G is a subgroup of N of order p^2. The number μ of such subgroups is congruent to 1 mod p (Huppert (1983), Ch. 1, Theorem 7.2). Since there are at least two such groups and $|N| = p^3$, we get that there are exactly $p+1$ maximal abelian normal subgroups of N and thus at most $p+1$ abelian normal subgroups of G. If G is of order p^3, then $G \cong N_p$ has exactly $p+1$ abelian normal subgroups (Huppert (1983), Ch. 3, Theorem 13.7.(f)).

The Theorem shows that there is only a finite number of unimodular monomial groups of prime degree containing more than one maximal abelian normal subgroup and that those groups are all finite. It also shows how those groups can be constructed. One way of constructing the groups is to note that $G = C \rtimes N_p$ is a subgroup of the wreath product $N_p \wr C$ (cf. Huppert (1983), Ch. 1, Theorem 15.12). For $p = 3$ we get that $N_3 \wr (\mathbb{Z}/2\mathbb{Z})$ has up to congugation only one subgroup of order $3^3 \cdot 2$ which we denote by $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$ (cf. Blichfeld (1917) p. 105). An irreducible representation in $SL(3,\mathbb{C})$ of $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$ is given in Section 5.1.2.

For prime degree p a *worst case*, i.e. an unimodular group with a maximal number of non-central maximal abelian normal subgroups, is always given by N_p.

3. Normal abelian subgroups and the Riccati

In this section we connect non-central normal abelian subgroups and algebraic solutions of the Riccati.

We consider $L(y) = 0$ given in (1.1) and associate to $L(y) = 0$ a Picard-Vessiot extension K and a differential Galois group $\mathcal{G}(K/k)$ consisting of all differential field automorphims of K/k (see e.g. Kaplansky (1957), Singer and Ulmer (1993b) or Ulmer (1992) for definitions). We also denote $\mathcal{G}(K/k)$ by $\mathcal{G}(L)$. The action of $\mathcal{G}(L)$ on the solution space of $L(y) = 0$ gives a faithful representation of degree p of $\mathcal{G}(L)$ over the field of constants of k. Unless otherwise mentioned, this will be *the* representation of $\mathcal{G}(L)$ in what follows.

THEOREM 3.1. *Consider an equation (1.1) of prime degree p whose differential Galois group $\mathcal{G}(L)$ is an imprimitive subgroup of $SL(p, \mathbb{C})$. Then*

1. *$\mathcal{P}_R$ is non-empty and consists of polynomials of degree p.*
2. *If $\mathcal{G}(L)$ has no faithful central-monomial representation of degree p, then $\mathcal{P}_R$ contains at most $p+1$ elements and there is a bijection between maximal normal abelian subgroups of $\mathcal{G}(L)$ and elements of $\mathcal{P}_R$.*
3. *If $\mathcal{G}(L)$ has no faithful central-monomial representation of degree p and is not isomorphic to a split extension $C \rtimes N_p$ of N_p and a cyclic group C of order dividing $p-1$ (in particular if the order of $\mathcal{G}(L)$ does not divide $p \cdot (p!)$ or $p^3(p-1)$), then $\mathcal{P}_R$ contains exactly one element.*

PROOF. Since $\mathcal{G}(L)$ is a monomial group, $\mathcal{G}(L)$ has a subgroup H of index p which has a common eigenvector z, i.e. which is 1-reducible (Ulmer (1992), Lemma 4.2). The logarithmic derivative of z is left fixed by H and thus is algebraic of degree p. The group $\mathcal{G}(L) \subseteq SL(p, \mathbb{C})$ cannot have a 1-reducible subgroup H' of index $< p$ whithout being reducible, since the orbit of the eigenvector of H' would generate a non-trivial $\mathcal{G}(L)$-invariant subspace. Thus p is the minimal index of a 1-reducible subgroup of $\mathcal{G}(L)$. This shows that $\mathcal{P}_R$ is non-empty and that all polynomials in $\mathcal{P}_R$ are of degree p (see Singer and Ulmer (1993b), Lemma 3.1).
We now assume that $\mathcal{G}(L)$ has no central-monomial representation of degree p. Let P_i be an element of $\mathcal{P}_R$ of degree p and w a root of P_i which is the logarithmic derivative of a solution z. The one dimensional subspaces V_i generated by the p vectors $\{\sigma(z) | \sigma \in \mathcal{G}(L)\}$ (i.e. the conjugates of z under $\mathcal{G}(L)$) form a system of imprimitivity for $\mathcal{G}(L)$. We set $G_i = \{\sigma \in \mathcal{G}(L) | \sigma(V_i) = V_i\}$. Then $A_i = \cap_i G_i$ is a maximal normal abelian subgroup of $\mathcal{G}(L)$. Since $\mathcal{G}(L)$ has no central-monomial representation, A_i must be a maximal non-central normal abelian subgroup of $\mathcal{G}(L)$. Since A_i is a non-central abelian normal subgroup of $\mathcal{G}(L)$, there are p homogeneous components of A_i and thus up to multiples a unique basis of eigenvectors of A_i whose logarithmic derivatives are the solutions of P_i. Since A_i is a maximal abelian subgroup, we get that, to each P_i corresponds a unique maximal normal abelian subgroup A_i. Conversely, the logarithmic derivatives of a basis of eigenvectors of a maximal (and thus non-central) normal abelian subgroup A_i corresponds to the p solutions of an element P_i of $\mathcal{P}_R$, which gives a bijection between elements of $\mathcal{P}_R$ and maximal normal abelian subgroups of $\mathcal{G}(L)$. From Theorem 2.1 we get that an imprimitive group has at most

$p+1$ maximal normal abelian subgroups.
From Theorem 2.1 we get that if $\mathcal{G}(L)$ is not isomorphic to a split extension $C \rtimes N_p$ of N_p and a cyclic group C of order dividing $p-1$, then the imprimitive group $\mathcal{G}(L)$ has exactly one maximal normal abelian subgroup. Since $\mathcal{G}(L)$ has no faithful central-monomial representation then there is a bijection between maximal normal abelian subgroups of $\mathcal{G}(L)$ and elements of $\mathcal{P}_R$, which shows that $\mathcal{P}_R$ contains exactly one element. □

Let $L(y) = 0$ with coefficients in $\mathbb{Q}(\alpha)(x) \subset \overline{\mathbb{Q}}(x)$. Considering K as a differential field extension of $\mathbb{Q}(\alpha)(x)$ (with new constants) we get the group $\mathcal{G}(K/\mathbb{Q}(\alpha)(x))$ of differential field automorphisms of $K/\mathbb{Q}(\alpha)(x)$. We denote $G(\overline{\mathbb{Q}}/\mathbb{Q}(\alpha))$ the classical Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}(\alpha)$. In Hendriks and Van der Put (1993) it is shown that the following sequence

$$1 \longrightarrow \mathcal{G}(K/\overline{\mathbb{Q}}(x)) \hookrightarrow \mathcal{G}(K/\mathbb{Q}(\alpha)(x)) \longrightarrow G(\overline{\mathbb{Q}}/\mathbb{Q}(\alpha)) \longrightarrow 1$$

is split exact. Choose a point $a \in \mathbb{Q}$ which is a regular point of $L(y) = 0$ and consider K as a subfield of $\overline{\mathbb{Q}}((x-a))$. We denote by s the splitting homomorphism given in Hendriks and Van der Put (1993) and defined by $s\sigma(\sum_{i=k}^{\infty} a_i(x-a)^i) = \sum_{i=k}^{\infty} \sigma(a_i)(x-a)^i$. It has the property that the elements of $\overline{\mathbb{Q}}(x)$ which are left fixed by $s\left(G(\overline{\mathbb{Q}}/\mathbb{Q}(\alpha))\right)$ are in $\mathbb{Q}(\alpha)(x)$. From the splitting one gets, that $\mathcal{G}(K/\mathbb{Q}(\alpha)(x))$ is the semi-direct product of $\mathcal{G}(K/\overline{\mathbb{Q}}(x))$ and $s\left(G(\overline{\mathbb{Q}}/\mathbb{Q}(\alpha))\right)$.

COROLLARY 3.2. *Consider an equation (1.1) of prime degree p with coefficients in $\mathbb{Q}(\alpha)(x) \subset k = \overline{\mathbb{Q}}(x)$ whose differential Galois group $\mathcal{G}(L)$ is an imprimitive subgroup of $SL(p,\mathbb{C})$. If $\mathcal{G}(K/k)$ has no faithful central-monomial representation of degree p and is not isomorphic to a split extension $C \rtimes N_p$ of N_p and a cyclic group C of order dividing $p-1$, then the unique element of $\mathcal{P}_R$ has coefficients in $\mathbb{Q}(\alpha)(x)$.*

PROOF. Theorem 3.1 shows that $\mathcal{P}_R$ contains exactly one element P and that $\mathcal{G}(K/k)$ has exactly one maximal normal abelian subgroup A. The solutions u_i of P are the logarithmic derivatives of a basis of eigenvectors y_i for A. The group $\mathcal{G}(K/\overline{\mathbb{Q}}(x))$ permutes the u_i's and thus leaves the coefficients of P, which are in $\overline{\mathbb{Q}}(x)$, invariant. We denote σ an element of $s\left(G(\overline{\mathbb{Q}}/\mathbb{Q}(\alpha))\right)$. Since y_i is an eigenvector of A, we get that $\sigma(y_i)$ is an eigenvector of $A^\sigma = \sigma A \sigma^{-1}$ which is thus also a non-central abelian normal subgroup of $\mathcal{G}(K/\overline{\mathbb{Q}}(x))$ isomorphic to A. Since A is the unique maximal non-central normal abelian subgroup of $\mathcal{G}(K/\overline{\mathbb{Q}}(x))$ we have $A^\sigma = A$. In particular $\sigma(y_i)$ is a multiple of some y_j and thus $s\left(G(\overline{\mathbb{Q}}/\mathbb{Q}(\alpha))\right)$ also permutes the u_i's and leaves the coefficients of P fixed. The coefficients must belong to $\mathbb{Q}(\alpha)(x)$. □

The number of elements in $\mathcal{P}_R$ is only an upper bound for degree of the algebraic extension needed to represent the elements of $\mathcal{P}_R$. Even if $\mathcal{P}_R$ contains more than one polynomial, all its elements are in some cases defined over the coefficient field of $L(y)$ (cf. Ulmer and Weil (1994), pp. 15-16).

COROLLARY 3.3. *(*cf. Hendriks and Van der Put (1993) and Zharkov (1993)[†]*) Let $L(y) =$*

[†] The corresponding results in Hendriks and Van der Put (1993) and Zharkov (1993) contain a mistake which has been corrected by the authors in later preprints (cf. Hendriks and Van der Put (1993b)). The

0 be a linear differential equation of 2 (resp. 3) with coefficients in $\mathbb{Q}(\alpha)(x)$ and whose differential Galois group $\mathcal{G}(K/\overline{\mathbb{Q}}(x))$ is an imprimitive subgroup of $SL(p,\mathbb{C})$. If $\mathcal{G}(K/\overline{\mathbb{Q}}(x))$ is not isomorphic to $N_2 = Q_8$ (resp. to N_3 or $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$), then $\mathcal{P}_R$ contains exactly one element with coefficients in $\mathbb{Q}(\alpha)(x)$. If $\mathcal{G}(K/\overline{\mathbb{Q}}(x))$ is isomorphic to Q_8 (resp. to N_3 or $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$), then $\mathcal{P}_R$ contains exactly 3 (resp. 4) elements.

PROOF. It only remains to show that $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$ has 4 normal abelian subgroups of order 9. This can be computed directly (e.g. using CAYLEY) or by noting that elements of order 2 of N act invertingly on the quotient $N_3/Z(N_3)$. □

4. The two possible cases

THEOREM 4.1. (Jordan's Theorem. See e.g. Ulmer (1992), Section 3) *There exists a function $f : \mathbb{N} \mapsto \mathbb{N}$ depending only on n, such that any finite subgroup of $GL(n,\mathbb{C})$ has a normal abelian subgroup of index $\leq f(n)$.*

Several bounds for $f(n)$ are known. One has $f(2) = 60$, $f(3) = 360$, $f(4) = 25920$,... (see e.g. Ulmer (1992) Section 3 for further references). From Jordan's Theorem we get that any finite primitive subgroup of $SL(n,\mathbb{C})$ is of order at most $n \cdot f(n)$ and thus that there are at most finitely many such groups.

THEOREM 4.2. *Let $L(y) = 0$ be an irreducible linear differential equation over k of prime order p with differential Galois group $\mathcal{G}(L) \subseteq SL(p,\mathbb{C})$. If $L(y) = 0$ has a Liouvillian solution over k, then one (or both†) of the following holds:*

1. *$\mathcal{P}_R$ contains exactly one element.*
2. *$\mathcal{G}(L)$ belongs to a finite set of finite groups. The group $\mathcal{G}(L)$ is a finite primitive group or a central-monomial group or isomorphic to a split extension $C \rtimes N_p$ of N_p and a cyclic group C of order dividing $p-1$ (in particular the order of $\mathcal{G}(L)$ is either less than $p \cdot f(p)$ or divides $p^3(p-1)$ or divides $p \cdot (p!)$).*

PROOF. The group $\mathcal{G}(L)$ is either imprimitive or primitive. If $\mathcal{G}(L)$ is imprimitive, then the result follows from Theorem 3.1. If $\mathcal{G}(L)$ is primitive, then $L(y) = 0$ has a Liouvillian solution if and only $\mathcal{G}(L) \subseteq SL(p,\mathbb{C})$ is a finite group (cf. Ulmer (1992), Corollary 3.7). The result follows from Jordan's Theorem. □

The fact that there are only a finite set of finite groups where $\mathcal{P}_R$ may contain more than one element, allows to consider those cases separately. If $\mathcal{G}(L)$ is one of those finite groups, then all solutions of $L(y) = 0$ must be algebraic and one can use the method presented in Singer and Ulmer (1993b) to compute the minimal polynomial of a solution of $L(y) = 0$ (instead of the minimal polynomial of an algebraic solution of the Riccati). This will be presented in the next section. If, after having tried the finitely many finite groups

approach via systems of imprimitivity used in this paper allowed M.F. Singer and the author to find the error in Hendriks and Van der Put (1993) for the third order case.

† For some of the finite groups considered, $\mathcal{P}_R$ has only one element

no solution is found, then we can assume that $\mathcal{P}_R$ contains at most one element and, if $k = \overline{\mathbb{Q}}(x)$, that no algebraic extension will be needed to represent the polynomial in $\mathcal{P}_R$.

5. Case of a known finite differential Galois group

In this section we review the method presented in Singer and Ulmer (1993b) to find the minimal polynomial of an algebraic solution of $L(y) = 0$ (instead of the minimal polynopmial of a logarithmic derivative) if $\mathcal{G}(L)$ is a given finite subgroup of $SL(p, \mathbb{C})$. In the following we assume that, for linear differential equations over the field k, algorithms for computing solutions that are in k exists (cf. Bronstein (1992) and the references given in Singer and Ulmer (1993b), Section 1).

In order to apply the method presented in Section 4 of Singer and Ulmer (1993b) we start with a group $\mathcal{G}(L) \subseteq SL(p, \mathbb{C})$ given in terms of matrices over a basis corresponding to unknown solutions which we denote symbolically $\{y_1, y_2, \cdots, y_p\}$ and proceed as follows:

1 Compute a maximal subgroup H_z having the common eigenvector $z = \sum_i \alpha_i y_i$. In practice one can choose z so that H_z is of maximal order.
2 Compute a maximal subgroup $Stab_{\mathcal{G}(L)}(z)$ leaving z invariant (the stabiliser of z in $\mathcal{G}(L)$) and denote by i the index of $Stab_{\mathcal{G}(L)}(z)$ in H_z.
3 Compute a set of left coset representatives $\mathcal{T}$ of H_z in $\mathcal{G}(L)$. The minimal polynomial $P(Y)$ of z is given by:

$$P(Y) = \prod_{\sigma \in H_z} \left(Y^i - \sigma(z)^i\right)$$

whose coefficients will be in k and thus invariant under $\mathcal{G}(L)$.
4 Compute a basis $I_1, \cdots I_I$ of the ring of invariants (cf. Sturmfels (1993)) of the finite group $\mathcal{G}(L) \subseteq SL(p, \mathbb{C})$ and decompose the coefficients of $P(Y)$ in this basis.

The above computations do not depend on the particular equation and needs to be done only once for each finite group in the list. The above decomposition does not depend on the coefficient field of $L(y)$, but only on the choice of the matrix representation of $\mathcal{G}(L)$ and on the choice of the common eigenvector z.

In order to find the minimal polynomial of a solution of a given particular equation $L(y) = 0$ via the above decomposition we use *symmetric powers*:

DEFINITION 5.1. *Let $\{y_1, \ldots, y_n\}$ be a fundamental set of solutions of the linear differential equation $L(y) = 0$. The m^{th} symmetric power $L^{\circledS m}(y)$ of $L(y)$ is the unique differential equation of smallest order whose the solution space is spanned by $\{y_1^m, y_1^{m-1} y_2, \ldots, y_n^m\}$.*

An algorithm to construct the equation $L^{\circledS m}(y)$ is given in Singer (1980) and Singer and Ulmer (1993), Section 3.2.2. Since $L^{\circledS m}(y)$ is obtained by solving a linear sytem over the field of coefficients of $L(y) = 0$, the coefficients of $L^{\circledS m}(y)$ belong also to this field. In the following we use the fact that rational solutions of $L^{\circledS m}(y) = 0$ are homomorphic images of invariants of degree m of $\mathcal{G}(L) \subseteq SL(p, \mathbb{C})$ (cf. Singer and Ulmer (1993b), Lemma 1.6). This allows to connect the above decomposition to a particular given linear differential equation $L(y)$:

1 Collect the invariants $I_1, \cdots I_I$ into set $S_d = \{I_{d_1}, \cdots, I_{d_i}\}$ of equal total degree d. Compute (cf. Bronstein (1992)) a basis $Q_{d,1}, \cdots Q_{d,r}$ of the space of rational solutions (i.e. solutions in k) of d-th symmetric power $L^{\circledS d}(y) = 0$ and set $I_{d_j} = \sum_{t=1}^{r} c_{d,j,t} Q_{d,t}$, where $c_{d,j,t}$ are unknown constants.
2 Substitute I_{d_j} by $\sum_{t=1}^{r} c_{d,j,t} Q_{d,t}$ in the decomposed expression of $P(Y)$ and compute for $s \in \{2, \cdots, p\}$ the corresponding expressions for the derivatives $Y^{(s)}$ of Y in terms of the unknown constants $c_{d,j,t}$.
3 Substitute the values $Y^{(s)}$ depending on the $c_{d,j,t}$ in $L(y) = 0$, which gives a system of polynomial equations for the variables $c_{d,j,t}$.
4 Compute a lexicographical Groebner basis (cf. Sturmfels (1993)) for the above system of polynomial equations.
5 If a value for the $c_{d,j,t}$ can be found for which the polynomial $P(Y)$ is square free, then $P(Y)$ is the minimal polynomial of a solution of $L(y) = 0$.

If the above methode does not produce a square free polynomial $P(Y)$, then the chosen finite subgroup of $SL(p, \mathbb{C})$ is not the differential Galois group of $L(y) = 0$ and another group must eventually be considered. The connection with the rationallity problem is that, for $k = \overline{\mathbb{Q}}(x)$ all computations can be done in an extension of the coefficient field where the above decomposition of the coefficients of $P(Y)$ in terms of invariants is possible.

The correctness of the above method is proven in Singer and Ulmer (1993b) where it is applied to the finite primitive subgroups of $SL(2, \mathbb{C})$ and $SL(3, \mathbb{C})$. In the following we applied the method to the imprimitive subgroups $N_2 = Q_8$, N_3 and $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$ of $SL(2, \mathbb{C})$ and $SL(3, \mathbb{C})$ where $\mathcal{P}_R$ has more than one element. We first compute the above decomposition for those groups and then apply the method to an example. In a final subsection we derive necessary condition which allows to test if a given finite group is the differential Galois group of $L(y) = 0$.

5.1. Precomputations

Theorem 5.1. *Let $L(y)$ be a linear differential equation of prime degree p over k with imprimitive differential Galois group $\mathcal{G}(L) \subset SL(p, \mathbb{C})$. If $\mathcal{P}_R$ has more than one element, then:*

1 *If $p = 2$ then $\mathcal{G}(L) \cong N_2$ and $L(y) = 0$ has a solution which is algebraic over k and whose minimal polynomial is of the form:*

$$P(\mathbf{Y}) \quad = \quad \mathbf{Y}^8 - I_1 \mathbf{Y}^4 + (I_2)^2$$

where I_1 and I_2 are solutions in k of $L^{\circledS 4}(y) = 0$.
2 *If $p = 3$ then $\mathcal{G}(L) \cong N_3$ or $\mathcal{G}(K/k) \cong (\mathbb{Z}/2\mathbb{Z} \rtimes N_3)$.*

(a) *If $\mathcal{G}(K/k) \cong N_3$, then $L(y) = 0$ has an algebraic solution whose minimal polynomial is of the form:*

$$P(\mathbf{Y}) \quad = \quad \mathbf{Y}^9 - I_2 \mathbf{Y}^6 + \frac{1}{2}\left((I_2)^2 - I_3\right)\mathbf{Y}^3 - (I_1)^3$$

where I_1 and I_2 are solutions in k of $L^{\circledS 3}(y) = 0$ and I_3 is a solution in k of $L^{\circledS 6}(y) = 0$.

(b) If $\mathcal{G}(K/k) \cong (\mathbb{Z}/2\mathbb{Z} \rtimes N_3)$, *then* $L(y) = 0$ *has an algebraic solution whose minimal polynomial is of the form:*

$$P(\mathbf{Y}) \quad = \quad \mathbf{Y}^{18} - I_4\mathbf{Y}^{12} + \left(\frac{1}{4}(I_4)^2 - \frac{1}{2}I_2 I_4 - 2I_1 I_3 + \frac{1}{4}(I_2)^2\right)\mathbf{Y}^6 - (I_1)^3$$

where I_1, I_2, I_3 *and* I_4 *are solutions in* k *of* $L^{\circledS 6}(y) = 0$.

The Theorem is proven in the following subsections.

We note that alltrough all decompositions given in the Theorem are over $\mathbb{Q}$, an extension of $\mathbb{Q}$ is sometimes necessary, due to the fact that the invariants of $\mathcal{G}(L)$ are not defined over $\mathbb{Q}$ (the representation of $\mathcal{G}(L)$ is usually not defined over $\mathbb{Q}$) or that the choosen eigenvector does not have coordinates in $\mathbb{Q}$. This occurs for some primitive finite subgroups of $SL(2,\mathbb{C})$ and $SL(3,\mathbb{C})$ (cf. Singer and Ulmer (1993b), Section 4).

5.1.1. Second order equations

From Corollary 3.3 we get that for second order equations the quaternion group $N_2 = Q_8$ is the only imprimitive group where $\mathcal{P}_R$ has more than one element. We now determine the algebraic degree of a solution of $L(y) = 0$ and decompose the coefficients of its minimal polynomial in terms of invariants of $\mathcal{G}(L)$.

An irreducible representation of degree 2 of Q_8 (unique up to equivalence) is generated by:

$$r = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad t = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

We denote by $\{y_1, y_2\}$ the basis of the solution space corresponding to the above representation. The group H_{y_1} generated by r is of order 4 and is a maximal subgroup of Q_8 having a common eigenvector which is y_1. The degree of the extension $[\overline{\mathbb{Q}}(x)(y_1) : \overline{\mathbb{Q}}(x)]$ must divide the order $8 = |Q_8|$. Since Q_8 does not have a faithful transitive representation of degree 4 or 2, we get that the degree of the minimal polynomial $P(Y)$ of y_1 must be 8 and that the stabiliser $Stab_{\mathcal{G}(L)}(y_1)$ of y_1 is trivial. Thus $i = [H_{y_1} : Stab_{\mathcal{G}(L)}(y_1)] = 4$. A transversal of H_{y_1} in Q_8 is given by $\mathcal{T} = \{id, t\}$ which gives the following formula for $P(Y)$:

$$P(\mathbf{Y}) = \prod_{\sigma\in\mathcal{T}} \left(\mathbf{Y}^4 - (\sigma(y))^4\right) = \left(\mathbf{Y}^4 - y_1^4\right)\left(\mathbf{Y}^4 - y_2^4\right) = \mathbf{Y}^8 - (y_1^4 + y_2^4)\mathbf{Y}^4 + (y_1 y_2)^4$$

In order to decompose the above coefficients in terms of the invariants of Q_8 we need to compute a basis[†] of the ring of invariants $\mathbb{C}[y_1, y_2]^{Q_8}$ of Q_8. This can be done using the algorithms described in Sturmfels (1993). The expansion of the Hilbert series $\Phi_G(z)$ of the ring $\mathbb{C}[y_1, y_2]^{Q_8}$ is

$$\Phi_G(z) = \frac{1}{|Q_8|}\sum_{g\in Q_8}\frac{1}{\det(id - zg)} = \frac{z^4 - z^2 + 1}{z^6 - z^4 - z^2 + 1} = 1 + 2z^4 + z^6 + 3z^8 + O(z^9)$$

This shows that there are two fundamental invariants I_1 and I_2 of degree 4 and one fundamental invariant of degree 6. In order to decompose $P(Y)$ we will only need the two

[†] Not all the invariants of Q_8 are needed, only those whose degree is less than the maximal degree of the homogenous forms appearing in the coefficients

fundamental invariants of degree 4 which are $I_1 = (y_1^4 + y_2^4)$ and $I_2 = (y_1 y_2)^2$. Using a Gröbner basis (cf. Sturmfels (1993)) or an Ansatz one can decompose the coefficients of $P(Y)$ in terms of those invariants:

$$P(\mathbf{Y}) \quad = \quad \mathbf{Y}^8 - I_1 \mathbf{Y}^4 + (I_2)^2$$

5.1.2. Third order equations

According to Blichfeld (1917), pp. 105-106 we define

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

where $\omega^3 = 1$ and $\omega \neq 1$. The commutator $S_2 = [S_1, T]$ corresponds to the scalar multiplication by ω. The group N_3 is generated by S_1 and T and the group $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$ is generated by S_1, T and R (cf. Blichfeld (1917), pp. 105-106). According to Corollary 3.3 those are, up to isomorphism, the only two imprimitive subgroups of $SL(3,\mathbb{C})$ for which $\mathcal{P}_R$ has more than one element. To decompose the minimal polynomial of a solution of $L(y) = 0$ we proceed as in the previous section using that:

1 **For** $\mathcal{G}(L) =< S_1, T > \cong N_3$ the group $H_{y_1} =< S_1, S_2 >$ of order 9 has y_1 as a common eigenvector. The stabiliser of y_1 is $< S_1 >$ and $i = [H_{y_1} : Stab_{\mathcal{G}(L)}(y_1)] = 3$. The set $\mathcal{T} = \{id, T, T^2\}$ is a set of left coset representative of H_{y_1} in $\mathcal{G}(L)$. One can decompose the minimal polynomial of y_1 using the invariants

$$I_1 = y_1 y_2 y_3;\ I_2 = y_1^3 + y_2^3 + y_3^3;\ I_3 = y_1^6 + y_2^6 + y_3^6$$

2 **For** $\mathcal{G}(L) =< S_1, T, R > \cong (\mathbb{Z}/2\mathbb{Z} \rtimes N_3)$ the group $H_{y_1} =< S_1, S_2, R >$ of order 18 has y_1 as a common eigenvector. The stabiliser of y_1 is $< S_1 >$ and $i = [H_{y_1} : Stab_{\mathcal{G}(L)}(y_1)] = 6$. The set $\mathcal{T} = \{id, T, T^2\}$ is a set of left coset representative of H_{y_1} in $\mathcal{G}(L)$. One can decompose the minimal polynomial of y_1 using the invariants:

$$I_1 = (y_1 y_2 y_3)^2;\ I_2 = (y_1^3 + y_2^3 + y_3^3)^2;\ I_3 = y_1 y_2 y_3 (y_1^3 + y_2^3 + y_3^3);\ I_4 = y_1^6 + y_2^6 + y_3^6$$

The fact that the faithful representations of N_3 and of $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$ in $SL(3,\mathbb{C})$ are conjugated under the Galois automorphism $\omega \mapsto \omega^2$ shows that the given decompositions, which are invariant under this automorphism, hold for any such representation.

5.2. Application to an example

To illustrate the method we apply it to the following irreducible linear differential equation given in Hendriks and Van der Put (1993b):

$$L(y) \quad = \quad \frac{d^2y}{dx^2} + \frac{27x}{8(x^3-2)^2}\, y = 0$$

The group $\mathcal{G}(L) \subseteq SL(2,\mathbb{C})$ is the quaternion group $N_2 = Q_8$, since the rational solution space (computed using the algorithm described in Bronstein (1992)) of

$$L^{\circledS 4}(y) \quad = \quad \frac{d^5y}{dx^5} + \frac{135x}{2(x^3-2)^2}\frac{d^3y}{dx^3} + \frac{405(5x^3+2)}{4(x^3-2)^3}\frac{d^2y}{dx^2}$$

$$+\frac{3645x^2(x^3+2)}{2(x^3-2)^4}\frac{dy}{dx}-\frac{405x(7x^6+35x^3+10)}{(x^3-2)^5}y$$

is generated by x^3-2 and $x(x^3-2)$ and thus is of dimension 2 (cf. Ulmer and Weil (1994), Lemma 6). This example was constructed in Hendriks and Van der Put (1993b) in order to prove that an algebraic extension of degree 3 of the coefficient field is sometime necessary to construct an element of $\mathcal{P}_R$ if $\mathcal{G}(L)=Q_8$. Using the method presented in Ulmer and Weil (1994) we get the 3 elements $P_\lambda(U)$ of $\mathcal{P}_R$:

$$P_\lambda(U) \quad = \quad U^2-\frac{2x^2+\lambda^2x-\lambda}{x^3-2}U+\frac{8x^4+8\lambda^2x^3-6\lambda x^2-x-4\lambda^2}{8x^6-32x^3+32},$$

where $2\lambda^3+1=0$. Which shows that a cubic extension of the coefficient field $\mathbb{Q}(x)$ is necessary to represent the elements of $\mathcal{P}_R$ in this case.

We now use the method presented in Singer and Ulmer (1993b) to compute the minimal polynomial of a solution of $L(y)=0$. From Theorem 5.1 we get that if $\mathcal{G}(L)=Q_8$, then there is a solution of $L(y)$, whose minimal polynomial is of the form

$$P(\mathbf{Y}) \quad = \quad \mathbf{Y}^8-I_1\mathbf{Y}^4+(I_2)^2$$

where I_1 and I_2 are solutions in k of the 4-th symmetric power $L^{\circledS 4}(y)=0$.
We set

$$-I_1=c_1\left(x^3-2\right)+c_2\left(x^4-2x\right) \qquad I_2=c_3\left(x^3-2\right)+c_4\left(x^4-2x\right)$$

and get

$$P(\mathbf{Y}) \quad = \quad \mathbf{Y}^8+\left(c_1\left(x^3-2\right)+c_2\left(x^4-2x\right)\right)\mathbf{Y}^4+\left(c_3\left(x^3-2\right)+c_4\left(x^4-2x\right)\right)^2$$

This equation is square free if and only if its discriminant

$$\begin{aligned} Disc(P(\mathbf{Y})) \quad = \quad & 65536(x^3-2)^{14}(c_4x+c_3)^6\left((c_2+2c_4)x+(c_1+2c_3)\right)^4 \\ & \left((c_2-2c_4)x+(c_1-2c_3)\right)^4 \end{aligned}$$

is not zero.

Following Singer and Ulmer (1993b) (Section 5) we compute the expression for Y'' which we substitute into $L(y)=0$. This gives a polynomial in Y and x whose coefficients, which are polynomials in $c_1,\ldots,c_4$, must be zero. We get a set of polynomial equations for the constants $c_1,\ldots,c_4$. Computing a lexicographical Gröbner basis (cf. Sturmfels (1993)) for $c_1>c_2>c_3>c_4$ we get that $c_1,\ldots,c_4$ must, among others, satisfy the following polynomials:

$$\begin{aligned} &(c_4^6-\frac{1}{4}c_2^2c_4^4-\frac{1}{4}c_3^6+\frac{1}{16}c_1^2c_3^4) \\ &c_3(c_1c_4^3-\frac{1}{2}c_2c_3c_4^2-\frac{1}{8}c_2^3c_3) \\ &c_4^3(c_1c_4^3-\frac{1}{2}c_2c_3c_4^2-\frac{1}{8}c_2^3c_3) \\ &c_3(c_4-\frac{1}{2}c_2)c_4(c_4+\frac{1}{2}c_2)(c_4^2+\frac{1}{12}c_2^2) \\ &(c_4-\frac{1}{2}c_2)c_4^2(c_4+\frac{1}{2}c_2)(c_4^3+\frac{1}{2}c_3^3) \end{aligned}$$

Form the last equation we get that c_4 equals 0, $\pm\frac{1}{2}c_2$ or $-\frac{1}{\sqrt[3]{2}}c_3$.

1 Let $c_4 = 0$. In this case c_3 must be non zero for $Disc(P(\mathbf{Y}))$ to be non-zero. From the second polynomial we get that c_2 is zero and from the first that $c_3 = \pm\frac{1}{2}c_1$. But then $Disc(P(\mathbf{Y})) = 0$.

2 Let $c_4 = \frac{1}{2}c_2 \neq 0$ (resp. $c_4 = -\frac{1}{2}c_2 \neq 0$). The first polynomial implies that $c_3 = 0$ or $c_3 = \frac{1}{2}c_1$ (resp. $c_3 = -\frac{1}{2}c_1$). If $c_3 = 0$, then the third polynomial implies $c_1 = 0$. In any case $Disc(P(\mathbf{Y})) = 0$.

3 Let $c_3 = -\sqrt[3]{2}c_4 \neq 0$. From the fourth equation we get that $c_2 = 2\sqrt{-3}c_4$ and from the second that $c_1 = 2\sqrt{-3}\sqrt[3]{2}c_4$. Since $Disc(P(\mathbf{Y})) \neq 0$ this always gives a square free polynomial. One verifies that for $c_4 \neq 0$ the point $(2\sqrt{-3}\sqrt[3]{2}c_4, 2\sqrt{-3}c_4, -\sqrt[3]{2}c_4, c_4)$ belongs to the variety defined by the above Gröbner Basis, and thus that

$$\begin{aligned} P(\mathbf{Y}) &= \mathbf{Y}^8 + 2c_4\sqrt{-3}\left(\sqrt[3]{2}\left(x^3-2\right) + \left(x^4-2x\right)\right)\mathbf{Y}^4 \\ &\quad + (c_4)^2\left(-\sqrt[3]{2}\left(x^3-2\right) + \left(x^4-2x\right)\right)^2 \end{aligned}$$

is the minimal polynomial of a solution of $L(y) = 0$.

If the coefficient field of $L(y)$ is a subfield of $\overline{\mathbb{Q}}(x)$, then all computations including the final Gröbner basis in $c_1, \ldots, c_4$ can be done over the field containing the coefficient field and over which the decomposition of $P(Y)$ in terms of invariants can be done. The final Gröbner basis gives equations for the algebraic extension needed to represent $P(Y)$.

The minimal polynomials found above have roots whose logarithmic derivatives, by the choice of y_1 as eigenvector, are roots of an element of $\mathcal{P}_R$. The example shows that a field extension (here $\sqrt{-3}$) is sometime needed to get from the minimal polynomial of a logarithmic derivative u, defined in this case over $\mathbb{Q}(\sqrt[3]{2})(x)$, to the minimal polynomial of the algebraic solution $\exp(\int u)$, defined in this case over $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})(x)$.

5.3. Necessary conditions for finite groups

If the coefficients of (1.1) are in $\mathbb{C}(x)$, we can use Theorem 3.5 of Singer and Ulmer (1994) to derive necessary conditions for $\mathcal{G}(L)$ to be a given finite subgroup of $SL(p, \mathbb{C})$. The goal of those necessary conditions is to exclude, with little computation, a group from the list of possible differential Galois groups of a given equation $L(y)$. Such conditions are given in Singer and Ulmer (1994) for the finite primitive groups and will be extended now to the imprimitive finite groups $N_2 = Q_8$, N_3 and $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$:

Lemma 5.2. *1 Let $L(y)$ be an irreducible second order linear differential equation with coefficients in $\mathbb{C}(x)$ whose differential Galois group is the quaternion group Q_8. Then $L(y) = 0$ must be a differential equation of fuchsian type having at any singularity 2 distinct rational exponents e_1, e_2 such that:*

(a) each e_i is of the form a_i/m_i, with $(a_i, m_i) = 1$, $a_i, m_i \in \mathbb{Z}$ and $lcm(m_1, m_2) \in \{1, 2, 4\}$, and

(b) there exist non-negative integers n_1, n_2, such that $n_1+n_2 = 2$ and $2(n_1e_1+n_2e_2) \in \mathbb{Z}$.

We also have the condition that $L^{\circledS 4}(y) = 0$ has a two dimensional solution space of rational solutions (i.e. solutions in k).

2 *Let $L(y)$ be an irreducible third order linear differential equation with coefficients in $\mathbb{C}(x)$ whose differential Galois group is isomorphic to N_3 or $\mathbb{Z}/2\mathbb{Z} \ltimes N_3$. Then $L(y) = 0$ must be a differential equation of fuchsian type having at any singularity 3 distinct rational exponents e_1, e_2, e_3 such that:*

(a) If $\mathcal{G}(L) \cong N_3$, then

i each e_i is of the form a_i/m_i, with $(a_i, m_i) = 1$, $a_i, m_i \in \mathbb{Z}$ and $lcm(m_1, m_2, m_3) \in \{1, 3\}$ and

ii there exist non-negative integers n_1, n_2, n_3, such that $\sum_{i=1}^{3} n_i = 3$ and such that $\sum_{i=1}^{3} n_i e_i \in \mathbb{Z}$.

(b) If $\mathcal{G}(L) \cong (\mathbb{Z}/2\mathbb{Z} \ltimes N_3)$, then

i each e_i is of the form a_i/m_i, with $(a_i, m_i) = 1$, $a_i, m_i \in \mathbb{Z}$ and $lcm(m_1, m_2, m_3) \in \{1, 2, 3, 6\}$, and

ii there exist non-negative integers n_1, n_2, n_3, such that $\sum_{i=1}^{3} n_i = 2$ and such that $2(\sum_{i=1}^{3} n_i e_i) \in \mathbb{Z}$.

We also have the condition that $L^{\circledS 3}(y) = 0$ has a non-trivial solution in k for $\mathcal{G}(L) \cong N_3$ and no non-trivial solution in k for $\mathcal{G}(L) \cong (\mathbb{Z}/2\mathbb{Z} \ltimes N_3)$.

PROOF. The proof follows from Theorem 3.5 of Singer and Ulmer (1994) and is similar to the proof of the *Necessary Conditions 3* in Singer and Ulmer (1994).

1 The representation of Q_8 is given in Section 5.1.1. To conclude as in Singer and Ulmer (1994) we need that the elements of Q_8 are of order 1, 2 or 4 and that $y_1 y_2$ is a semi-invariant of order 2 (i.e. $(y_1 y_2)^2$ is an invariant). Also the two invariants $(y_1 y_2)^2$ and $y_1^4 + y_2^4$ generate a two dimensional space of solutions in k of $L^{\circledS 4}(y) = 0$ (according to Lemma 3.5 of Singer and Ulmer (1993) the homomorphic image of those invariants is never be 0).

2 We consider the representation of N_3 and $\mathbb{Z}/2\mathbb{Z} \ltimes N_3$ given in Section 5.1.2 (to which the other representations are conjugate under $\omega \mapsto \omega^2$). The first assertion follows from the fact that the order of the elements of N_3 is in $\{1, 3\}$ and that those of $\mathbb{Z}/2\mathbb{Z} \ltimes N_3$ is in $\{1, 2, 3, 6\}$. The second assertion follows from the fact that $y_1 y_2 y_3$ is an invariant of N_3 and a semi-invariant of order 2 of $\mathbb{Z}/2\mathbb{Z} \ltimes N_3$. If $\mathcal{G}(L) \cong N_3$, then $y_1 y_2 y_3$ is a non-zero solution in k of $L^{\circledS 3}(y) = 0$. Since $\mathbb{Z}/2\mathbb{Z} \ltimes N_3$ has no invariant of degree 3, $L^{\circledS 3}(y) = 0$ cannot have a solution in k if $\mathcal{G}(L) \cong \mathbb{Z}/2\mathbb{Z} \ltimes N_3$.

□

Example. - We consider the following differential equation[†]:

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

[†] This equation is the second symmetric power of a second order linear differential equation whose differential Galois group is the tetrahedral group (cf. Singer and Ulmer (1993), Section 5, p. 31). The differential Galois group $\mathcal{G}(K/k)$ of $L(y) = 0$ is thus isomorphic to A_4, the alternating group of 4 elements

and want to use necessary conditions on the exponents to show, with little computation, that the unimodular group $\mathcal{G}(L)$ is an imprimitive group which is not isomorphic to N_3 or $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$ and thus that $\mathcal{P}_R$ has exactly one element whose coefficients belong to $\mathbb{Q}(x)$ (Corollary 3.3)
The equation is of fuchsian type (cf. Singer and Ulmer (1994)) and has 3 regular singular points at $x = 0$, $x = 1$ and $x = \infty$. The exponents at those singularities are: $\{1, \frac{1}{2}, \frac{3}{2}\}$, $\{1, \frac{2}{3}, \frac{4}{3}\}$ and $\{-1, -\frac{2}{3}, -\frac{4}{3}\}$.

1 The equation is irreducible, since it is not possible to find an exponent a_i at each finite singular point such that for some exponent e_∞ at ∞, the sum $(\sum_i a_i) + e_\infty$ is a non-positive integer (cf. Corollary 3.3 of Singer and Ulmer (1994)).
2 The group $\mathcal{G}(K/k)$ is an imprimitive subgroup of $SL(3, \mathbb{C})$, since $x^2(x-1)^2$ is a solution of $L^{\circledS 3}(y) = 0$ (cf. Singer and Ulmer (1993)), Theorem 4.6).
3 We now use Lemma 5.2: $\mathcal{G}(K/k)$ cannot be N_3, since we have exponents, e.g. $\frac{1}{2}$, whose denominators do not divide any element of $\{1, 3\}$. The group $\mathcal{G}(K/k)$ cannot be $\mathbb{Z}/2\mathbb{Z} \rtimes N_3$, since $L^{\circledS 3}(y) = 0$ has a solution in $k = \overline{\mathbb{Q}}(x)$, e.g. $x^2(x-1)^2$.

6. Conclusion

For an irreducible linear differential equation $L(y) = 0$ of prime degree, one can always reduce the computation of a Liouvillian solution to one of the following:

1 The computation of a solution of $L(y) = 0$ where $\mathcal{G}(K/k)$ belongs to a finite set of finite groups.
2 The computation of the unique minimal polynomial $P(Y)$ in $\mathcal{P}_R$ whose coefficients, if the coefficients of $L(y) = 0$ are in $\mathbb{Q}(\alpha)(x) \subset \overline{\mathbb{Q}}(x)$, are also in $\mathbb{Q}(\alpha)(x)$.

It is likely that this result simplifies the computation of $P(Y)$ in the second case, but no result in this direction is curently known to the author.

Acknowledgement: I would like to thank M.F. Singer for many useful comments, B. Sturmfels for his invitation to Cornell and his support during my visit, W. Lempken for pointing out that the complement of N_p in Theorem 2.1 must be cyclic, J.A. Weil for computing the 3 elements of $\mathcal{P}_R$ given in Section 5.2 and the referees for helpful suggestions.

References

Blichfeld, H.F. (1917). *Finite Collineation Groups*. Chicago: The University of Chicago Press.
Bronstein, M. (1992). On solutions of linear differential equation in their coefficient field. *J. Symb. Comp.* **13**.
Dixon, J. D. (1971). *The Structure of Linear Groups*. London: Van Nostrand Reinhold.
Hendriks, P.A., Van der Put, M. (1993). A rationality result for Kovacic's algorithm. *Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation, ACM Press*.
Hendriks, P.A., Van der Put, M. (1993b). Galois action on solutions of a differential equation. *Preprint University Groningen*.
Huppert, B. (1983). *Endliche Gruppen I*. Grundlehren der mathematischen Wissenschaften Band 134, Berlin: Springer-Verlag.
Issacs, M. (1976). *Character Theory of Finite Groups*. New York: Academic Press.
Kaplansky, I. (1957). *Introduction to differential algebra*. Paris: Hermann.

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

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. *Am. J. Math.* **103**.

Singer, M.F., Ulmer, F. (1993). Galois groups of second and third order linear differential equations. *J. Symb. Comp.* **16**.

Singer, M.F., Ulmer, F. (1993b). Liouvillian and algebraic solutions of second and third order linear differential equations. *J. Symb. Comp.* **16**.

Singer, M.F., Ulmer, F. (1994). Necessary Conditions for Liouvillian Solutions of (Third Order) Linear Differential Equations. *J. Appl. Alg. in Eng., Comm. and Comp.* **6**.

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

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

Ulmer, F., Weil, J.A. (1994). Note on Kovacic's algorithm. *Prépublication 94-13, IRMAR, Université de Rennes 1*.

Zharkov, A. (1993). On algebraic solutions of first order Riccati equation. *Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation, ACM Press.*