

INVARIANTS AND DIFFERENTIAL GALOIS GROUPS IN DEGREE FOUR

JULIA HARTMANN

*Interdisziplinäres Zentrum für wissenschaftliches Rechnen, Universität Heidelberg
 Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
 E-mail: Julia.Hartmann@iwr.uni-heidelberg.de*

Abstract. This note extends the algorithm of [Hes2] for computing unimodular Galois groups of irreducible differential equations of order four. The main tool is invariant theory.

1. Introduction. In her thesis [Hes1] and the revised version [Hes2], Hessinger gives a strategy for determining unimodular Galois groups of irreducible linear homogeneous differential equations of order four with the help of representation theory: Similar to what is done in [SU], she uses factorisation of symmetric (and exterior) powers of differential equations into irreducible parts and the fact that these correspond to irreducible constituents of the respective powers of the corresponding representations.

These methods do not yield a complete identification of the groups. The purpose of this note is to fill in some of the remaining gaps (see below for more details) to obtain a decision procedure for determining the Galois groups, especially for equations with non-Liouvillian solutions. The main tool is invariant theory, and the idea is very basic:

Suppose that $L(y) = 0$ is a linear homogeneous differential equation defined over a differential field with algebraically closed field of constants C . The Galois group G of this equation acts linearly on the solution space V . Consequently, after choosing a basis of fundamental solutions y_1, \dots, y_m of V , we may consider G as a subgroup of $\mathrm{GL}_m(C)$. The action of G on the solution space extends to an action on symmetric powers of V , and hence to an action on $C[V] = C[x_1, \dots, x_m]$, the polynomial ring over C in m variables, on which the group acts in the same way as on the y_i . An element of $C[V]$ which remains unchanged under this action is called an invariant.

For a fixed degree, the invariants of the Galois group of some irreducible linear homogeneous differential equation can be computed using an algorithm of van Hoeij and Weil [HW]. The key observation is that the actual Galois group must be contained in the largest group leaving those invariants fixed. We will see that in many cases, this criterion

2000 *Mathematics Subject Classification*: Primary 12H99.

The paper is in final form and no version of it will be published elsewhere.

will be enough to distinguish the groups, once a predecision using representation theory has been made.

For different choices of bases, one obtains conjugate (in $\mathrm{GL}_m(C)$) representations of the differential Galois group. Two such conjugate groups will in general not have the same invariants, but their invariant rings will be isomorphic. In particular, they will have the same number of invariants in each degree. This number is encoded in the so called Poincaré series of the invariant ring.

Most of the groups in degree four (the finite collineation groups) have been listed by Blichfeldt in [Bli] (see also the reference to several papers of Blichfeldt's there).

The imprimitive groups fall into the classes of monomial and nonmonomial groups (note that degree four is the first occurrence of imprimitive nonmonomial groups). Given an imprimitive nonmonomial group G , it is shown in [Hes2], Theorem 2.2.2, that G contains an index two subgroup H which is in block diagonal form and that there is a primitive subgroup T of $\mathrm{GL}_2(C)$ such that $H \subseteq T \times T$ and the projections of H onto the first and last two coordinates, respectively, equal T . Those groups split up further into the ones where T maps to a finite or infinite subgroup of $\mathrm{PGL}_2(C)$ under the canonical projection $\mathrm{GL}_2(C) \xrightarrow{\pi} \mathrm{PGL}_2(C)$. We call such groups projectively finite or projectively infinite, respectively. Finally, the primitive groups can be separated into the finite and infinite ones. Altogether, we obtain the five different classes listed below:

- monomial groups,
- imprimitive nonmonomial groups with T projectively finite,
- imprimitive nonmonomial groups with T projectively infinite,
- finite primitive groups,
- infinite primitive groups.

The algorithm described in [Hes2] decides to which of these classes the Galois group of a given differential equation belongs. In the sequel, we will explain a decision procedure for determining the Galois groups in the last three cases plus some information in the case of an imprimitive nonmonomial group with T projectively finite. It will become apparent that the method works best in the primitive cases, where there are not many similar groups to distinguish. We do not determine the Galois group in the monomial case. Note that this is also a case which the degree three algorithms (see, for example, [SU]) do not handle. We use [Hes2] as a main reference. To keep the two articles compatible, we adhere to the notation used there.

The main advantage of our method is that with the information at hand, it is often only necessary to compute invariants of a few fixed degrees which are known in advance. So for computational purposes, this strategy should be a good addition to the representation-theoretic methods.

This note should be considered as a report on what may be done using invariant theory. In the purely computational cases (Sections 2 and 4), we have therefore not included complete lists of the separating degrees.

The letter I will always denote an identity matrix. Its size should be clear from context. For a representation $\rho : G \hookrightarrow \mathrm{GL}(V)$, we define the k -fold representation $k\rho$ of ρ to be the representation given by simultaneous action of G on k copies of V .

2. The imprimitive nonmonomial groups with T projectively finite. In this case, T has to be projectively equivalent (two groups are called projectively equivalent if their images under the canonical projection $\mathrm{GL} \rightarrow \mathrm{PGL}$ coincide) to one of the primitive subgroups of $\mathrm{SL}_2(C)$, i.e., to $A_4^{\mathrm{SL}_2}$, $A_5^{\mathrm{SL}_2}$ or $S_4^{\mathrm{SL}_2}$ (in the notation of [SU]). Let P_n ($n \in \mathbb{N}$) denote the central extension of a group P by the group of n -th roots of unity (as scalar matrices), and P_∞ the central extension by $\mathrm{diag}(\mathrm{SL}(2, C))$. Let further $K \leq A_4$ denote the Klein four group. The following theorem is taken from [Hes2] (Theorem 2.2.3):

THEOREM 1. *Let G be an imprimitive, nonmonomial subgroup of $\mathrm{SL}_4(C)$ containing a normal subgroup H of index two where $H \leq T \times T$, with T projectively finite. Then there exists a nonnegative integer, n , and a subgroup $F \leq \mathrm{SL}_2(C)$ of T such that G is conjugate to one of the following groups.*

1. $\left\{ \begin{pmatrix} A & 0 \\ 0 & \pm \det(A)^{-1}B \end{pmatrix} : A, B \in P_n, BA^{-1} \in F \right\} \cup \left\{ \begin{pmatrix} 0 & A \\ \pm \det(A)^{-1}B & 0 \end{pmatrix} : A, B \in P_n, BA^{-1} \in F \right\}$ where
 - (a) $P = A_5$ and $\pi(F) \cong \{I\}$ or A_5 .
 - (b) $P = S_4$ and $\pi(F) \cong \{I\}$, K , A_4 , or S_4 .
 - (c) $P = A_4$ and $\pi(F) \cong \{I\}$, K , or A_4 .
2. $\left\{ \begin{pmatrix} A & 0 \\ 0 & \pm \det(A)^{-1}B \end{pmatrix} : A, B \in P_n, BA^{-1} \in F \right\} \cup \left\{ \begin{pmatrix} 0 & A \\ \pm \det(A)^{-1}B & 0 \end{pmatrix} : AO_{S_4}^{-1}, BO_{S_4}^{-1} \in P_n, BA^{-1} \in F \right\}$ where $P = A_4$, $\pi(F) \cong \{I\}$, K , or A_4 and $O_{S_4} = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}$.

We denote a group of the first or second type by $G_1(P, F)_n$ or $G_2(P, F)_n$, respectively.

In [Hes2], the groups with different P and F are distinguished, except for groups of the type $G_1(A_4, I)$, $G_2(A_4, I)$ and $G_1(S_4, I)$ or $G_1(A_4, K)$, $G_2(A_4, K)$ and $G_1(S_4, K)$.

The Poincaré series of the invariant rings of the finite groups may be computed using the computer algebra system MAGMA. For the Poincaré series of the infinite groups, we have used the fact that the central extension defines a normal subgroup N of the whole group G , so the invariants can be computed successively. The invariants under the normal subgroup $N = \{\mathrm{diag}(c, c, c^{-1}, c^{-1}) \mid c \in C^*\}$ are generated as an algebra by the four polynomials $f_1 = x_1x_3$, $f_2 = x_1x_4$, $f_3 = x_2x_3$, $f_4 = x_2x_4$ subject to one relation: $r = f_1f_4 = f_2f_3$, which is an invariant for all groups under consideration. Consequently, we have a surjective homomorphism $C[f_1, f_2, f_3, f_4] \rightarrow C[x_1, x_2, x_3, x_4]^N$ with kernel (r) which yields an exact sequence of graded C -vector spaces

$$0 \rightarrow C[f_1, f_2, f_3, f_4]^{G/N} \cap (r) \rightarrow C[f_1, f_2, f_3, f_4]^{G/N} \rightarrow C[x_1, x_2, x_3, x_4]^G \rightarrow 0$$

since G/N is reductive. Hence the Poincaré series of $C[x_1, x_2, x_3, x_4]^G$ is given as

$$\mathcal{P}(C[x_1, x_2, x_3, x_4]^G, t) = \mathcal{P}(C[f_1, f_2, f_3, f_4]^{G/N}, t^2) - \frac{1}{1 - t^4},$$

where we have substituted t by t^2 on the right hand side since the f_i have degree two. The group G/N is finite, and hence its Poincaré series can be computed in the standard way. This leads to the following.

PROPOSITION 2. *The three types of groups $G_1(A_4, I)_n$, $G_2(A_4, I)_n$ and $G_1(S_4, I)_n$ or $G_1(A_4, K)_n$, $G_2(A_4, K)_n$ and $G_1(S_4, K)_n$, respectively, may be distinguished by computing invariants of degree at most 20 and 24, respectively.*

Proof. The groups $G_1(A_4, I)_1$ and $G_1(S_4, I)_1$ both have an invariant of degree four, which remains invariant under all central extensions we have to consider. The group $G_2(A_4, I)_1$ does not have any invariant in that degree, and therefore none of the extended groups does. Hence in degree four we can separate the groups of type $G_2(A_4, I)_n$ from the other two types. In degree 12, $G_1(A_4, I)_1$ has four invariants which remain invariant under all central extensions under consideration, whereas $G_1(S_4, I)_1$ has only three such invariants. So in this degree we may separate the two types of groups as long as there are no more invariants resulting from small values of n . Clearly, that may only happen for $n \leq 12$. A list of invariants of degree 12 for the groups $G_1(A_4, I)_n$ and $G_1(S_4, I)_n$ for $n \leq 12$ shows that the only ambiguous case is when four invariants in degree 12 are found. Computing Poincaré series of the respective groups, one sees that in the worst case one needs to compute invariants of degree 20 to separate the candidates.

For the other three types of groups, we proceed in a similar manner (with a little more computational effort) to find that computing invariants up to degree 24 is sufficient to distinguish the groups. ■

3. The imprimitive nonmonomial groups with T projectively infinite. Let $(\mathrm{SL}_2)_n := \{A \in \mathrm{GL}_2(C) : \det(A)^n = 1\}$ for $n \in \mathbb{N}$.¹ By [Hes2], Theorem 2.2.2 (Notation of 3.2.2.), H is conjugate (in $\mathrm{GL}_4(C)$) to either of the following groups:

1. $H_n^1 = \left\{ \begin{pmatrix} B & 0 \\ 0 & \det(B)^{-1}B \end{pmatrix} : B \in (\mathrm{SL}_2)_n \right\}.$
2. $H_n^2 = \left\{ \begin{pmatrix} B & 0 \\ 0 & \pm \det(B)^{-1}B \end{pmatrix} : B \in (\mathrm{SL}_2)_n \right\}.$
3. $H_n^3 = \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} : A, B \in (\mathrm{SL}_2)_n, \det(AB) = 1 \right\}.$

Let $\gamma = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$. Then $G_n^i = H_n^i \cup \gamma H_n^i$ ($i = 1, 2, 3$) are all possible Galois groups. Using [Hes2], Case 3 of 3.2.2. (see also Table 2 of the Appendix), one can tell if $H = H_n^3$ for some n .

LEMMA 1. *The types of groups G_n^1 and G_n^2 may be separated by their number of invariants of degree two in the twofold representation.*

Proof. To separate the groups G_n^1 and G_n^2 , we need to work with the degree two invariants of the twofold representation. In this representation and degree, G_n^2 does not have any invariant (for $n > 1$ or $n = 0$), whereas G_n^1 has the invariant $x_1x_8 - x_2x_7 + x_3x_6 - x_4x_5$ (actually, the vector space dimension of the invariant ring of G_n^1 for $n > 1$ or $n = 0$ in degree 2 is 1). For $n = 1$, G_n^1 has two linearly independent invariants in degree two (still in the twofold representation), but G_n^2 has only one. ■

¹Note that this differs from the usage of the subscript n in the previous section!

We continue working with the twofold representation. Once the three types of groups have been separated (the first two are separated using Lemma 1, the third type is detected by the methods of [Hes2] as explained above), n is the smallest positive number such that $(x_1x_6 - x_2x_5)^n + (x_3x_8 - x_4x_7)^n$ is an invariant. That is to say, we have to look for the first occurrence of an "extra invariant" (it is clear that the extra condition $\det A^n = 1$ cannot "cause" any invariants in lower degrees than degree $2n$). This may be done by comparing the number of invariants computed in each degree to the Poincaré series of the groups G_0^1 , G_0^2 and G_0^3 for the three types of Galois groups, respectively.

PROPOSITION 3. *The Poincaré series of the above groups in their twofold representation read:*

$$\begin{aligned}\mathcal{P}(G_1, t) &= \frac{1 + 3t^4}{(1 + t^2)^3(1 - t^2)^4} \\ \mathcal{P}(G_2, t) &= \frac{1 + 3t^4}{(1 + t^2)^4(1 - t^2)^4} \\ \mathcal{P}(G_3, t) &= 1.\end{aligned}$$

Proof. Let us first compute the Poincaré series of the twofold representation of H_0^1 . Since H_0^1 is connected, the Poincaré series can be computed from the roots and weights as follows ([DK], 4.5). A maximal torus of H_0^1 is $T = \{\text{diag}(z_1, z_2, z_2^{-1}, z_1^{-1}) | z_i \in C\}$. The roots are $\alpha_1 = z_1z_2^{-1}$ and $-\alpha_1$. Thus the Poincaré series of the twofold representation is the coefficient of $z_1^0z_2^0$ in the formal expansion of

$$f = \frac{1 - z_1^{-1}z_2}{(1 - z_1t)^2(1 - z_2t)^2(1 - z_1^{-1}t)^2(1 - z_2^{-1}t)^2}.$$

We compute this coefficient using the residue theorem of complex analysis. Assume that $|z_1| = 1$ and $|t| < 1$. The only pole of f as a function of z_2 inside the unit disk is $z_2 = t$. The residue is

$$\text{Res}(z_2^{-1}f, t) = \frac{1 - z_1^{-1}t}{(1 - z_1t)^2(1 - z_1^{-1}t)^2(1 - t^2)^2} = \frac{1}{(1 - z_1t)^2(1 - t^2)^2(1 - z_1^{-1}t)} =: g.$$

The only pole of g as a function of z_1 inside the unit disk (still assume $|t| < 1$) is $z_1 = t$, and the residue is

$$\text{Res}(z_1^{-1}g, t) = \frac{1}{(1 - t^2)^2(1 - t^2)^2} = \frac{1}{(1 - t^2)^4}.$$

This already suggests that the invariant ring might be a free polynomial algebra on four generators of degree two.

We find the following invariants in degree two (labelling the eight variables x_1, \dots, x_8):

$$f_1 = x_3x_2 - x_1x_4, \quad f_2 = x_5x_4 - x_6x_3, \quad f_3 = x_7x_2 - x_8x_1, \quad f_4 = x_7x_6 - x_8x_5.$$

Specialising $x_1 = x_3 = x_6 = x_8 = 1$ gives

$$\tilde{f}_1 = x_2 - x_4, \quad \tilde{f}_2 = x_5x_4 - 1, \quad \tilde{f}_3 = x_2x_7 - 1, \quad \tilde{f}_4 = x_7 - x_5.$$

The Jacobian determinant $J(\tilde{f}_1, \tilde{f}_2, \tilde{f}_3, \tilde{f}_4)$ is given by

$$\det \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & x_5 & x_4 & 0 \\ x_7 & 0 & 0 & x_2 \\ 0 & 0 & -1 & 1 \end{pmatrix} = x_5x_2 - x_7x_4$$

which is nonzero, so the \tilde{f}_i are in fact algebraically independent. Hence the f_i are algebraically independent. Since the subalgebra $S \leq C[V]^{H_0^1}$ they generate has the same Poincaré series as $C[V]^{H_0^1}$, we conclude that $S = C[V]^{H_0^1}$, i.e., that the f_i generate the invariants of H_0^1 as a free polynomial algebra.

Next consider G_0^1 . H_0^1 is normal in G_1 , hence the invariants of G_0^1 can be computed from those of H_0^1 . The action of G_0^1 on the invariants of H_0^1 is given by

$$\gamma f_1 = -f_1, \quad \gamma f_2 = f_3, \quad \gamma f_3 = f_2, \quad \gamma f_4 = -f_4.$$

The Poincaré series of G_0^1 on the invariants of H_0^1 can then be computed with the help of Molien's formula as

$$\begin{aligned} \frac{1}{2} \left(\det \begin{pmatrix} 1+s & & & \\ & 1 & -s & \\ & -s & 1 & \\ & & & 1+s \end{pmatrix}^{-1} + \det \begin{pmatrix} 1-s & & & \\ & 1-s & & \\ & & 1-s & \\ & & & 1-s \end{pmatrix}^{-1} \right) \\ = \frac{1}{2} \left(\frac{1}{(1+s)^2(1-s)^2} + \frac{1}{(1-s)^4} \right) \frac{1+3s^2}{(1+s)^3(1-s)^4} \end{aligned}$$

which gives the desired Poincaré series for G_0^1 after resubstituting $s = t^2$.

H_0^1 is also normal in G_0^2 , and the quotient is generated by the images of $\sigma = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}$ and γ . The action on the invariants of H_0^1 is given by

$$f_1 \xrightarrow{\sigma} -f_1 \xrightarrow{\gamma} f_1, \quad f_2 \xrightarrow{\sigma} -f_2 \xrightarrow{\gamma} -f_3, \quad f_3 \xrightarrow{\sigma} -f_3 \xrightarrow{\gamma} -f_2, \quad f_4 \xrightarrow{\sigma} -f_4 \xrightarrow{\gamma} f_4$$

which is the action of a Klein four group. Again, the Poincaré series is computed using Molien's formula as

$$\begin{aligned} \frac{1}{4} \left(\det \begin{pmatrix} 1-s & & & \\ & 1-s & & \\ & & 1-s & \\ & & & 1-s \end{pmatrix}^{-1} + \det \begin{pmatrix} 1+s & & & \\ & 1 & -s & \\ & -s & 1 & \\ & & & 1+s \end{pmatrix}^{-1} \right. \\ \left. + \det \begin{pmatrix} 1+s & & & \\ & 1+s & & \\ & & 1+s & \\ & & & 1+s \end{pmatrix}^{-1} + \det \begin{pmatrix} 1-s & & & \\ & 1 & s & \\ & s & 1 & \\ & & & 1-s \end{pmatrix}^{-1} \right) \\ = \frac{1}{4} \left(\frac{1}{(1-s)^4} + \frac{1}{(1+s)^2(1-s)^2} + \frac{1}{(1+s)^4} + \frac{1}{(1-s)^2(1-s^2)} \right) = \frac{1+3s^2}{(1-s)^4(1+s)^4}. \end{aligned}$$

Again, we resubstitute $s = t^2$ to obtain the Poincaré series of G_0^2 .

Finally, consider the normal subgroup H_0^3 of G_0^3 of 2×2 -block diagonal matrices in $\text{SL}_4(C)$. A similar calculation as above shows that there are in fact no invariants of H_0^3 in its twofold representation, which implies that G_0^3 does not have any invariants in this representation. ■

4. The finite primitive groups. Up to projective equivalence, the finite primitive subgroups of $\mathrm{SL}_4(C)$ have been listed by Blichfeldt. Matrix generators for these groups can be found in Hessinger's thesis [Hes1]. In [Hes2], it is explained how to distinguish the groups up to projective equivalence except for one case (FP20 and FP21 in the notation of [Hes2]). Two projectively equivalent groups can at most differ by a central extension by a four dimensional scalar representation of the group of fourth roots of unity. Computing the number of invariants of degree at most 18 (but a lot smaller in most cases), one can distinguish between all groups with the following exception: In three cases (namely FP14, FP15, and FP30) there are two index two nonconjugate subgroups with the same Poincaré series.² In these cases it is necessary to use more information about the invariants. The invariant ring is generated by elements of degree at most the group order by Noether's degree bound (see, for example, [DK], Corollary 3.7.4.). On the other hand, the differential Galois group is already determined by its invariants (see [Com]), i.e., in theory, calculating a set of generating invariants is sufficient to distinguish the groups.

5. The infinite primitive groups. Suppose that G is infinite primitive, and denote by G^0 the connected component of the identity of G . We will first deal with the case when G^0 is irreducible.

5.1. G^0 irreducible: According to [Hes2], proof of Theorem 2.1.2, the irreducible linear algebraic subgroups of $\mathrm{SL}_4(C)$ are:

1. $\mathrm{SL}_4(C)$ in its standard representation V or the dual representation V^* .
2. $\mathrm{Sp}_4(C)$ in its standard representation.
3. $\mathrm{SO}_4(C)$ in its standard representation.
4. $\mathrm{SL}_2(C)$ in the third symmetric power of its standard representation.

It is shown in [Hes2] that these different possibilities for the identity component can be distinguished via decomposing symmetric powers of the representations (Table 4 of the Appendix), and which possibilities then remain for the whole group (loc.cit., Theorem 2.1.2).

LEMMA 2. *Let $G \leq \mathrm{SL}_n(C)$ and denote by Z the set of scalar matrices in G . Then every invariant of G has degree divisible by $|Z|$.*

Proof. The group Z is finite cyclic, and $f \in C[x_1, \dots, x_n]$ is invariant under Z if and only if f is a sum of monomials of the form $x_1^{k_1} \cdots x_n^{k_n}$ for $k_i \in \mathbb{N}$ with $k_1 + \dots + k_n \equiv 0 \pmod{|Z|}$. Every invariant of G is in particular an invariant of $Z \leq G$, from which the claim follows. ■

PROPOSITION 4. *Suppose the identity component G^0 of an infinite primitive differential Galois group G is known, and assume that it is irreducible. Then G may be determined by the number of its degree two invariants in the usual representation and in the twofold representation.*

²In the last two cases, the groups are isomorphic as abstract groups.

Proof. We will show that in each of these cases, the bigger possible group will not have any invariants in degree two, whereas the smaller groups do. Obviously, there is nothing to do in the case $G^0 = \mathrm{SL}_4(C)$ since we assumed $G \leq \mathrm{SL}_4(C)$.

Assume $G^0 = \mathrm{Sp}_4(C)$. Then $G \leq \langle \omega I, G^0 \rangle$, where ω denotes a primitive fourth root of unity, but since $\omega^2 = -1$, and $-1I \in G^0$, either $G = G^0$ or $G = G^0 \times_{\mathbb{Z}/2} \mathbb{Z}/4$, the subdirect product of G^0 and $\mathbb{Z}/4$ by $\mathbb{Z}/2$. A separating invariant for these two possible groups in the twofold representation is simply the defining skew-symmetric form of $\mathrm{Sp}_4(C)$, which is of degree two and therefore not invariant under $G^0 \times_{\mathbb{Z}/2} \mathbb{Z}/4$ by Lemma 2.

If $G^0 = \mathrm{SO}_4(C)$, then $G \leq \langle \omega I, J, G^0 \rangle$, where ω is a primitive fourth root of unity and $J = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$. Since $\omega^2 = -1$, and $-1I \in G^0$, and further $J \in G^0$, we find again that $G = G^0$ or $G = G^0 \times_{\mathbb{Z}/2} \mathbb{Z}/4$. Again the invariant separating these two can be found in degree two, namely the defining form of the orthogonal group, $x_1^2 + x_2^2 + x_3^2 + x_4^2$ (which is not invariant under the bigger group by Lemma 2).

If $G^0 = \mathrm{SL}_2(C)$, then $G \leq \langle \omega I, G^0 \rangle$, where ω is a primitive fourth root of unity. Since $\omega^2 = -1$, and $-1I \in G^0$, we see that either $G = G^0$ or $G = G^0 \times_{\mathbb{Z}/2} \mathbb{Z}/4$. Any invariant of the given representation of $\mathrm{SL}_2(C)$ is of degree divisible by four, so any of them will be invariant under $G^0 \times_{\mathbb{Z}/2} \mathbb{Z}/4$ also. What we need is an invariant which is of degree divisible by two, but not by four (Lemma 2). If we use the twofold of the given representation, with basis x_1, \dots, x_8 , we find the invariant $-x_1x_8 + \frac{1}{3}x_2x_7 - \frac{1}{3}x_3x_6 + x_4x_5$ of $\mathrm{SL}_2(C)$, which separates the two groups. ■

5.2. G^0 reducible: By [Hes2], Lemma 2.1.1, G^0 is conjugate to

$$2\mathrm{SL}_2(C) = \left\{ \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} : A \in \mathrm{SL}_2(C) \right\}.$$

Further, if G^0 equals the image of the twofold representation of $\mathrm{SL}_2(C)$ as above, then by [Hes2], Theorem 2.1.1, there exists a finite primitive subgroup \tilde{H} of $(\mathrm{SL}_2)_2 := \{A \in \mathrm{GL}_2(C) : \det(A)^2 = 1\}$ such that $G = H\tilde{H}G^0$ where

$$H = \left\{ \begin{pmatrix} aI & bI \\ cI & dI \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{H} \right\}.$$

Moreover, any such construction yields a primitive subgroup of $\mathrm{SL}_4(C)$.

The finite primitive subgroups of $\mathrm{GL}_2(C)$ are the groups $A_4^{\mathrm{SL}_2}$, $A_5^{\mathrm{SL}_2}$, $S_4^{\mathrm{SL}_2}$ (in the notation of [SU]) and extension of one of these groups by ωI , where ω is a primitive fourth root of unity.

The algorithm in [Hes2] identifies the corresponding finite subgroup of $\mathrm{SL}_2(C)$ ($A_4^{\mathrm{SL}_2}$, $A_5^{\mathrm{SL}_2}$, $S_4^{\mathrm{SL}_2}$), but does not distinguish between those and the respective extensions ([Hes2], Table 4 of the Appendix).

LEMMA 3. *Suppose that G^0 is reducible and that G is known up to a central extension by the group of fourth roots of unity (as scalar matrices). Then G may be determined by its number of degree two invariants.*

Proof. The extended groups do not have invariants of degree two (by Lemma 2), so a separating invariant is $x_1x_4 - x_2x_3$, which can be checked by direct computation. ■

Acknowledgements. I am indebted to Prof. B.H. Matzat for bringing this subject to my attention, as well as for many fruitful discussions. I also thank Gregor Kemper and Jürgen Klüners for helpful comments and suggestions.

References

- [Bli] H. F. Blichfeldt, *Finite Collineation Groups*, University of Chicago Press, 1917.
- [Com] E. Compoint, *Differential equations and algebraic relations*, J. Symbolic Computation 25 (1998), 705–725.
- [DK] H. Derksen and G. Kemper, *Computational Invariant Theory*, Springer-Verlag, Berlin, 2002.
- [Hes1] S. Hessinger, *Galois groups of fourth order linear differential equations*, Ph.D. Thesis, North Carolina State University, 1998.
- [Hes2] S. Hessinger, *Computing the Galois group of a linear differential equation of order four*, Appl. Algebra Eng. Commun. Comput. 11 (2001), 489–536.
- [Hil] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. 36 (1890), 473–534.
- [HW] M. van Hoeij and J.-A. Weil, *An algorithm for computing invariants of differential Galois groups*, J. Pure Applied Algebra 117 & 118 (1997), 353–379.
- [SU] M. F. Singer and F. Ulmer, *Galois groups of second and third order differential equations*, J. Symbolic Computation 16 (1993), 9–36.