

# On a Third Order Differential Equation whose Differential Galois Group is the Simple Group of 168 Elements

Michael F. Singer\* and Felix Ulmer\*\*

North Carolina State University  
Department of Mathematics  
Box 8205  
Raleigh, N.C. 27695-8205

**Abstract.** In this paper we compute the differential Galois group of a third order linear differential equation whose existence was predicted by F. Klein [9] and whose construction is due to A. Hurwitz [7]. The aim of this paper is to apply the results of [15] in order to prove, starting only with the equation, that the simple group of 168 elements is the the differential Galois group of this equation.

## 0 Introduction

Let  $L(y) = 0$  be a (homogeneous) linear differential equation of degree  $n$  whose coefficients belong to a differential field  $k$  whose field of constants  $\mathcal{C}$  is algebraically closed of characteristic 0 (see e.g. [8, 14, 16] for those notions). Similar to the case of algebraic equations, there is a notion of a “splitting field” for this equation. More specifically, there is a field  $K = k \langle y_1, \dots, y_n \rangle$ , generated (in the differential sense) by a fundamental set of solutions  $\{y_1, \dots, y_n\}$  of  $L(y) = 0$  such that  $K$  and  $k$  have the same set of constants.  $K$  is called the *Picard-Vessiot extension of  $k$  corresponding to  $L(y)=0$*  and is unique up to a differential  $k$ -isomorphism. The set of differential automorphisms of the field extension  $K/k$  (i.e., the field automorphisms of the field extension  $K/k$  which commute with the derivation of  $K$ ) that leave  $k$  elementwise fixed is called the *differential Galois group  $\mathcal{G}(L)$  of  $L(y) = 0$* . Since the solution space of  $L(y) = 0$  is an  $n$ -dimensional vector space over  $\mathcal{C}$  and since the group  $\mathcal{G}(L)$  sends a solution of  $L(y) = 0$  into another solution of  $L(y) = 0$ , we get a faithful representation of  $\mathcal{G}(L)$  as a subgroup of  $GL(n, \mathcal{C})$ . In fact,  $\mathcal{G}(L)$  can be shown to be a linear algebraic group. Many properties of the differential equation are mirrored in the group structure of  $\mathcal{G}(L)$ . For example, irreducibility of the equation is equivalent to irreducibility of the group and solvability in terms of exponentials, integrals

---

\* 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.

and algebraic functions (the liouvillian functions) is equivalent to the connected component of the identity of  $\mathcal{G}(L)$  being solvable. It is therefore an important problem to be able to calculate the Galois group or at least determine various properties of this group. We note that despite much recent work in determining the Galois group of a differential equation, there is, at present, no general algorithm that will calculate the defining polynomial equations of this group or even determine its dimension (see [15] for references to recent work).

In [15], we use the representation theory of groups to give simple necessary and sufficient conditions regarding the structure of the Galois groups of second and third order linear differential equations. These allow us to give simple necessary and sufficient conditions for a second order linear differential equation to have liouvillian solutions and for a third order linear differential equation to have liouvillian solutions or be solvable in terms of second order equations. In this note we show how these results can be applied to calculate the Galois group of the following equation due to Hurwitz<sup>3</sup> (see [7]):

$$H(y) = x^2(x-1)^2y''' + (7x-4)x(x-1)y'' + \left(\frac{72}{7}(x^2-x) - \frac{20}{9}(x-1) + \frac{3}{4}x\right)y' + \left(\frac{792}{7^3}(x-1) + \frac{5}{8} + \frac{2}{63}\right)y$$

In the first section we review the relevant results of [15], in the second section we show how these can be used to calculate the example and in the final section we make some concluding remarks.

## 1 Symmetric powers and Galois groups

In [15] we show how by factoring differential operators, one can decide if the differential Galois group  $\mathcal{G}(L)$  is reducible, imprimitive or primitive and, if the  $\mathcal{G}(L) \subseteq SL(n, \mathbb{C})$  is a primitive linear group, how to compute this group. The method uses the construction of the differential equation

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

called the *symmetric power* of order  $m$  of  $L(y) = 0$ . The equation  $L^{\otimes m}(y) = 0$  is characterized by the property that it is the monic linear differential operator of smallest order whose solution space is spanned by all products of length  $m$  of solutions of  $L(y) = 0$ . In [13, 15] an algorithm to construct the above equation is given. The differential equation  $L^{\otimes m}(y)$  is of order at most  $\binom{n+m-1}{n-1}$ , where  $n$  is the degree of  $L(y)$ . For example, the second symmetric power  $H^{\otimes 2}(y)$  of

<sup>3</sup> This equation is related to an equation previously produced by Halphen in a letter to F. Klein (cf. [6])

$H(y)$  is:

$$\begin{aligned}
& y^{(6)} + \frac{31x - 18}{x(x-1)} y^{(5)} + \frac{\frac{2320}{7}x^2 - \frac{97135}{252}x + \frac{880}{9}}{x^2(x-1)^2} y^{(4)} \\
& + \frac{\frac{73760}{49}x^3 - \frac{9282095}{3528}x^2 + \frac{526415}{392}x - \frac{1640}{9}}{x^3(x-1)^3} y^{(3)} \\
& + \frac{\frac{141840}{49}x^3 - \frac{4548685}{1176}x^2 + \frac{21381505}{15876}x - \frac{7840}{81}}{x^4(x-1)^3} y'' \\
& + \frac{\frac{4898160}{2401}x^3 - \frac{54698425}{28812}x^2 + \frac{5780305}{15876}x - \frac{560}{81}}{x^5(x-1)^3} y' \\
& + \frac{\frac{40930560}{117649}x^2 - \frac{87839125}{470596}x + \frac{40805}{3969}}{x^5(x-1)^3} y
\end{aligned}$$

In [15] it is shown how the orders of irreducible factors of  $L^{\otimes m}(y)$  are related to the decomposition of the character of the symmetric power of the representation of  $\mathcal{G} \subseteq SL(n, \mathbb{C})$ . This can be used to determine properties of  $\mathcal{G}(L)$ . For example, we are able to give necessary and sufficient conditions for these linear differential equations to have liouvillian solutions. In particular, we show:

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

Factorization properties can also be used to determine Galois groups in many cases. For example (note that the Tetrahedral group is the finite subgroup of  $SL_2$  having a center of order two such that its quotient by this center is isomorphic to the alternating group on 4 letters):

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

For third order equations we proved similar results that we now state in more detail. We first recall that a subgroup  $G$  of  $GL(V)$  is said to *act irreducibly* if the only  $G$ -invariant subspaces of  $V$  are  $\{0\}$  and  $V$ , otherwise it is said to *act reducibly*. Let  $G$  be a subgroup of  $GL(V)$  acting irreducibly.  $G$  is called *imprimitive* if, for  $k > 1$ , there exist non-trivial subspaces  $V_1, \dots, V_k$  such that  $V = V_1 \oplus \dots \oplus V_k$  and, for each  $g \in G$ , the mapping  $V_i \rightarrow g(V_i)$  is a permutation of the set  $\mathcal{S} = \{V_1, \dots, V_k\}$ . An irreducible group  $G \subseteq GL(n, \mathbb{C})$  which is not imprimitive is called *primitive*. One knows the finite primitive subgroups of  $PGL(3, \mathbb{C})$  (c.f., [1]). From this list, one can derive the primitive subgroups of  $SL(3, \mathbb{C})$  (c.f., [1]). Any finite primitive group of  $SL(3, \mathbb{C})$  is isomorphic to one of the following groups:

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

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

$$(1,3)(2,6)(4,5)(7,12)(8,9)(10,13),$$

$$(1,4)(3,8)(5,9)(6,11)(10,14)(12,15),$$

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

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

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

2. The simple group  $G_{168}$  of order 168 defined by:

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

3.  $G_{168} \times C_3$ , the direct product of  $G_{168}$  with the cyclic group  $C_3$  of order 3.
4.  $A_5$ , the alternating group of five letters.
5.  $A_5 \times C_3$ , the direct product of  $A_5$  with a cyclic group  $C_3$  of order 3.
6. The group  $H_{216}^{SL_3}$  of order 648 defined by:

$$\{U, V, S, T | U^9 = V^4 = T^3 = S^3 = (UV)^3 = id, VS = TV,$$

$$VT = S^2 V, [U^6, V] = [U^6, T] = [U, S] = id, [U, V^2] = S\}.$$

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

7. The group  $H_{72}^{SL_3}$  of order 216 generated by the elements  $S, T, V$  and  $UVU^{-1}$  of  $H_{216}^{SL_3}$ .
8. The group  $F_{36}^{SL_3}$  of order 108 generated by the elements  $S, T$  and  $V$  of  $H_{216}^{SL_3}$ .

For each finite primitive subgroup of  $SL(3, \mathbb{C})$ , using its character table (computed using the group theory system Cayley [2]) and the orthogonality relations of characters, we can decompose the characters of the symmetric product (computed using the computer algebra system AXIOM). The result is summarized in the following table, where the numbers  $4, 3^2$  in the column  $A_5$  and row 3 of Figure 1 means that the  $3^{rd}$  symmetric product of the character of any faithful irreducible representation of  $A_5$  in  $SL(3, \mathbb{C})$  has an irreducible summand of degree 4 and two irreducible summands of degree 3.

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

Figure 1

The next two results are proved in [15]:

**Theorem 1.** *Let  $L(y) = 0$  be a third order linear differential equation with coefficients in a differential field  $k$  with algebraically closed field of constants whose differential Galois  $\mathcal{G}(L)$  group is unimodular.*

1.  $L(y) = 0$  is reducible if and only if  $L(y) = 0$  has a solution  $y \neq 0$  such that  $y'/y \in k$  or  $L^*(y) = 0$ , the adjoint of  $L(y) = 0$ , has a solution  $y \neq 0$  such that  $y'/y \in k$  (if  $L(y) = \sum_{i=0}^n a_i y^{(i)}$ , then  $L^*(y) = \sum_{i=0}^n (-1)^i (a_i y)^{(i)}$ ).
2. Assume  $L(y)$  is irreducible. Then  $\mathcal{G}(L)$  is imprimitive if and only if  $L^{\otimes 3}(y) = 0$  has a solution  $y \neq 0$  such that  $y^2 \in k$ . In this case  $\mathcal{G}(L)$  is isomorphic to a subgroup of  $C^* \rtimes S_3$ , where  $S_3$  is the symmetric group on three letters. If  $\mathcal{G}(L)$  is isomorphic to a subgroup of  $C^* \rtimes A_3$ , where  $A_3$  is the alternating group on three letters, then the above solution  $y$  is already in  $k$ .
3. Assume  $L(y)$  is irreducible and 2. does not hold, then  $\mathcal{G}(L)$  is a primitive group.

**Theorem 2.** *Let  $L(y) = 0$  be a third order linear differential equation with coefficients in a differential field  $k$  with algebraically closed field of constants, whose differential Galois group  $\mathcal{G}(L)$  is unimodular. Assume that  $\mathcal{G}(L)$  is primitive.*

1. If  $L^{\otimes 2}(y)$  has order 5 or factors then  $\mathcal{G}(L)$  is isomorphic to  $PSL_2$ ,  $PSL_2 \times C_3$ ,  $A_5$ ,  $A_5 \times C_3$  or  $F_{36}^{SL_3}$ . In this case one of the following holds
  - $\mathcal{G}(L) \cong F_{36}^{SL_3}$  if and only if  $L^{\otimes 2}(y)$  has a factor of order 3, or
  - $\mathcal{G}(L) \cong A_5$  or  $A_5 \times C_3$  if and only if  $L^{\otimes 3}(y)$  has a factor of order 3 and a factor of order 4, or
  - $\mathcal{G}(L) \cong PSL_2$  or  $\mathcal{G}(L) \cong PSL_2 \times C_3$  if and only if the previous two cases do not hold.
2. If  $L^{\otimes 2}(y)$  has order 6 and is irreducible, then one of the following holds
  - $\mathcal{G}(L) \cong G_{168}$  or  $G_{168} \times C_3$  if and only if  $L^{\otimes 3}(y)$  has a factor of order 3.
  - $\mathcal{G}(L) \cong A_6^{SL_3}$  if and only if  $L^{\otimes 4}(y)$  is reducible and  $L^{\otimes 3}(y)$  is irreducible.
  - $\mathcal{G}(L) \cong H_{72}^{SL_3}$  if and only if  $L^{\otimes 5}(y)$  has more than 2 factors of order 3.
  - $\mathcal{G}(L) \cong H_{216}^{SL_3}$  if and only if  $L^{\otimes 5}(y)$  has exactly 2 factors of order 3 and  $L^{\otimes 2}(y)$  has a factor of degree 2.
  - The Galois group is  $SL(3, \mathbb{C})$  if and only if none of the above happen.

Algorithms for factoring linear differential operators are well known, [11, 12, 5]. Therefore the above results will *in theory* allow one to determine the Galois group of  $H(y) = 0$ . Nonetheless, we show how simpler calculations allow us to determine these factorization properties.

## 2 The Galois group of Hurwitz's equation

We start our computations by first showing that  $\mathcal{G}(H)$  is unimodular (i.e. a subgroup of  $SL(n, \mathbb{C})$ ). According to [8] p. 41, this follows from the fact that for the rational function  $w = x^4(x-1)^3$  we have

$$\frac{w'}{w} = \frac{4}{x} + \frac{3}{x-1} = \frac{7x-4}{x(x-1)}$$

## 2.1 Reducibility

We must show that  $H(y)$  is irreducible. Theorem 1 says that we just need to check if  $H(y) = 0$  or  $H^*(y) = 0$  have a solution  $y \neq 0$  such that  $y'/y \in \mathbb{C}(x)$ . There is an algorithm to decide this (cf. [16], section 3.2) which has been implemented in the AXIOM system by M. Bronstein. We used this implementation to show that  $H(y) = 0$  and  $H^*(y) = 0$  have no such solution. Therefore  $H(y)$  is irreducible.

## 2.2 Imprimitivity

Now one must check to see if  $\mathcal{G}(H)$  is an imprimitive linear group. Theorem 1 says that we need to check if  $H^{\otimes 3}(y) = 0$  has a solution  $y \neq 0$  such that  $y^2 \in \mathbb{C}(x)$ . One can calculate  $H^{\otimes 3}(y) = 0$  and use AXIOM to decide this question, but there is an easier way using exponents (c.f., [10] for a definition of exponents and their elementary properties). One can calculate the exponents of  $H(y) = 0$  at the singular points 0, 1 and  $\infty$  (which are all regular singular points) and one gets:

- $\{\frac{11}{7}, \frac{9}{7}, \frac{8}{7}\}$  at  $\infty$
- $\{0, -\frac{1}{3}, -\frac{2}{3}\}$  at  $x = 0$
- $\{\frac{1}{2}, 0, -\frac{1}{2}\}$  at  $x = 1$

Since the exponents at infinity and 0 do not differ by integers, there exist solutions of the form  $x^\rho \sum_{i=0}^{\infty} x^{-i}$  for each exponent  $\rho$  at infinity and  $x^\rho \sum_{i=0}^{\infty} x^i$  for each exponent  $\rho$  at 0. Calculating further, one can show that despite the fact that the exponents differ by an integer at 1 there exist similar solutions at  $x = 1$ , i.e., no logarithmic terms. A basis for the solution space of  $H^{\otimes 3}(y) = 0$  will be gotten by taking three such solutions (allowing repetitions) and forming their products. Using this fact one sees that the exponents at infinity are  $\frac{33}{7}, \frac{31}{7}, \frac{30}{7}, \frac{29}{7}, \frac{28}{7} = 4, \frac{27}{7}, \frac{27}{7} + n$  for some non-negative integer  $n$ ,  $\frac{26}{7}, \frac{25}{7}, \frac{24}{7}$ . Similar lists can be made at 0 and 1. Note that for 0 any such exponent is at worst a fraction with denominator 3 and is  $\geq -2$  and at 1 they are at worst a fraction with denominator 2 and is  $\geq -\frac{3}{2}$ .

A solution  $y$  of  $H^{\otimes 3}(y) = 0$  with  $y^2 \in \mathbb{C}(x)$  must be of the form (because everything is fuchsian)  $y = p(x)x^a(x-1)^b$  where  $p(x)$  is a polynomial and  $a$  resp.  $b$  are exponents of  $H^{\otimes 3}(y) = 0$  at 0 resp. 1. We also have that  $-a - b - \deg(p)$  will be an exponent at infinity. by comparing denominators, we see that the only possibility is that  $-a - b - \deg(p) = 4$ . Since  $a \geq -2$  and  $b \geq -\frac{3}{2}$ , we have  $-a - b - \deg(p) \leq \frac{7}{2} < 4$ . Therefore,  $H^{\otimes 3}(y) = 0$  does not have a solution of the required form and so  $\mathcal{G}(H)$  is not an imprimitive linear group.

## 2.3 Primitivity

We now know that the Galois group is a primitive group subgroup of  $SL(3, \mathbb{C})$ . It therefore must be one of the groups listed above. The computation of  $H^{\otimes 4}(y)$  shows that this equation has order 14. This already gives us some information.

If we start with a vector space  $V$  of dimension 3 and form its fourth symmetric power  $\mathcal{S}^4(V)$ , we will get a vector space of dimension 15. If we let  $V$  be the solution space of  $H(y) = 0$ , then there is a  $\mathcal{G}(H)$  morphism of  $\mathcal{S}^4(V)$  onto the solution space of  $H^{\otimes 4}(y) = 0$  (cf. [15], Section 3.2.2). This means that the kernel of this morphism is a  $\mathcal{G}(H)$  invariant subspace of  $\mathcal{S}^4(V)$ , i.e.,  $\mathcal{S}^4(V)$  will have a one dimensional invariant subspace. Looking at Figure 1, we see that this can only happen for groups corresponding to the first, second and fourth columns. Thus  $\mathcal{G}(H)$  must be one of the groups  $PSL_2$ ,  $A_5$ ,  $G_{168}$  or the direct product of one of those groups with  $C_3$ .

We now show that the groups corresponding to the first two columns cannot occur. Since  $H^{\otimes 2}(y)$  is of order 6, we get from Figure 1 that if  $\mathcal{G}(H)$  is one of the groups  $PSL_2$ ,  $A_5$ ,  $PSL_2 \times C_3$  or  $A_5 \times C_3$ , then  $H^{\otimes 2}(y)$  must have a factor of order 1. Since the singularities are fuchsian and the exponents are rational, this implies that  $H^{\otimes 2}(y) = 0$  would have a solution  $y$  such that  $y^i \in \mathbb{C}(x)$  for some  $i$ . If  $\sigma \in \mathcal{G}(H)$  then  $\sigma(y) = \chi(\sigma)y$  where  $\chi$  is a character of  $\mathcal{G}(H)$ .  $PSL_2$  and  $A_5$  are simple groups and so have no nontrivial characters while if  $\chi$  is a character of  $PSL_2 \times C_3$  or  $A_5 \times C_3$  then  $\chi^3 = 1$ . In all these cases we therefore must have that  $y^3$  is left fixed by the Galois group and so  $y^3 \in \mathbb{C}(x)$ . Looking at the exponents  $\frac{16}{7}, \frac{17}{7}, \frac{18}{7}, \frac{19}{7}, \frac{22}{7}$  at infinity we see that this is impossible. Therefore the Galois group must be one of the groups corresponding to column 4, i.e.,  $G_{168}$  or  $G_{168} \times C_3$ . We must now distinguish between  $G_{168}$  and  $G_{168} \times C_3$ .

To do this, we shall use the monodromy group of the above equation. Consider a linear differential equation with coefficients in  $\mathbb{C}(x)$ . For these equations we can use analytic considerations to define a group called the *monodromy group* that is a subgroup of the Galois group. Let  $c_1, \dots, c_n$  be the singular points of  $L(y) = 0$  (including infinity if it is a singular point) and let  $c_0$  be an ordinary point of the equation. We consider these points as lying on the Riemann Sphere  $S^2$ . Let  $\{y_1, \dots, y_n\}$  be a fundamental set of solutions of  $L(y) = 0$  analytic at  $c_0$  and let  $\gamma$  be a closed path in  $S^2 - \{c_1, \dots, c_n\}$  that begins and ends at  $c_0$ . One can analytically continue  $\{y_1, \dots, y_n\}$  along  $\gamma$  and get new fundamental solutions  $\{\bar{y}_1, \dots, \bar{y}_n\}$  analytic at  $c_0$ . These two sets must be related via  $(\bar{y}_1, \dots, \bar{y}_n)^T = M_\gamma(y_1, \dots, y_n)^T$  where  $M_\gamma \in GL(n, \mathbb{C})$ . One can show that  $M_\gamma$  depends only on the homotopy class of  $\gamma$  and that the map  $\gamma \mapsto M_\gamma$  defines a group homomorphism from  $\pi_1(S^2 - \{c_1, \dots, c_n\})$  to  $\mathcal{G}(L)$ . The image of this map depends on the choice of  $c_0$  and  $\{y_1, \dots, y_n\}$  but is unique up to conjugacy and is called the *monodromy group of  $L(y)$* . In general the image of this group will be a proper subgroup of  $\mathcal{G}(L)$  but when  $L(y)$  is fuchsian, the Zariski closure of this group will be the full Galois group  $\mathcal{G}(L)$  (c.f., [17]). In particular if  $\mathcal{G}(L)$  is finite (i.e., all solutions of  $L(y) = 0$  are algebraic) then the map is surjective and the monodromy and Galois groups coincide.

We now return to  $H(y) = 0$ . At each singular point  $\alpha$ , we have linearly independent solutions  $y_i = (x - \alpha)^{\rho_i} \sum a_{ij}(x - \alpha)^j$ ,  $i = 1, 2, 3$  where the  $\rho_i$  are the distinct exponents at  $\alpha$ . Each  $\rho_i$  is a rational number, say  $\rho_i = \frac{r_i}{s_i}$ ,  $(r_i, s_i) = 1$ . If we analytically continue each  $y_i$  around  $\alpha$ , we get a new solution  $y_i = \zeta_i y_i$  where  $\zeta_i = \exp(\frac{2\pi i r_i}{s_i})$ . Therefore the local monodromy group of  $H(y) = 0$  around

each singular point  $\alpha$  is a cyclic subgroup generated by one element  $g_\alpha$  whose order is the least common multiple of the denominator of the exponents at  $\alpha$ . Thus  $g_\infty$  is of order 7,  $g_0$  is of order 3 and  $g_1$  is of order 2. The product  $g_\infty g_0 g_1$  corresponds to the zero path and thus must be the identity. Since  $g_0$ ,  $g_1$  and  $g_\infty$  generate the monodromy group and  $g_0 g_1 = g_\infty^{-1}$ , we get that the group  $\mathcal{G}(H)$  is generated by an element of order 2 and an element of order 3 whose product is an element of order 7. Using the group theory system CAYLEY (see [2]) one can see that  $G_{168}$  has such a set of generators, while  $G_{168} \times C_3$  does not have such a set of generators. The group  $G_{168}$  is generated by  $S$  and  $T$ , where  $S^7 = (S^4 T)^4 = (ST)^3 = T^2 = 1$ . A set of generators of the above form is given by the element  $T$  of order 2 and  $TS^{-1}$  of order 3 whose product is of order 7.

This shows that  $\mathcal{G}(H) \cong G_{168}$ .

### 3 Final comments

The techniques of [16] give another way to distinguish between these two groups  $G_{168}$  and  $G_{168} \times C_3$ . In [16], we show (among other things) that when the Galois group of a linear differential equation is a finite primitive group one can use invariant theory to construct the minimal polynomial of a solution of the linear differential equation (this is an idea going back to L. Fuchs [3]). In particular if  $\mathcal{G}(H) \cong G_{168}$ , then  $H(y) = 0$  has an algebraic solution whose minimal polynomial is of degree 42, while if  $\mathcal{G}(H) \cong G_{168} \times C_3$ , then any solution of  $H(y) = 0$  has minimal polynomial of degree at least 126 (cf. [16], Theorem 4.2). Techniques are given in [16] to compute these polynomials and one can use these to distinguish between  $G_{168}$  and  $G_{168} \times C_3$ .

We finally mention the source of  $H(y) = 0$ . In [9], Klein studied the Riemann surface  $\mathcal{S}$  defined by  $x^3 y + y^3 z + z^3 x = 0$  in  $\mathbf{CP}^2$ . This surface has genus 3 and its automorphism group  $Aut(\mathcal{S})$  is the group  $G_{168}$ . The quotient of  $\mathcal{S}$  under the action of  $Aut(\mathcal{S})$  is just the Riemann sphere  $\mathbf{CP}^1$ . Let  $\omega_1 = f_1 dt, \omega_2 = f_2 dt, \omega_3 = f_3 dt$  be a basis for the holomorphic 1-forms on  $\mathcal{S}$ , where  $t$  is a  $Aut(\mathcal{S})$  invariant function. The map  $\kappa(p) \mapsto (f_1(p), f_2(p), f_3(p))$  defines the canonical embedding of the curve into  $\mathbf{CP}^2$ . One can show that (after an automorphism of  $\mathbf{CP}^2$ , if necessary),  $\kappa(\mathcal{S}) = \mathcal{S}$ .  $Aut(\mathcal{S})$  acts linearly on the space of holomorphic 1-forms and leaves  $\mathcal{S}$  invariant. Therefore  $\{f_1, f_2, f_3\}$  span an  $Aut(\mathcal{S})$  invariant vector space of dimension 3. This implies that  $\{f_1, f_2, f_3\}$  span the solution space of a linear differential equation  $H(y) = Wr(y, f_1, f_2, f_3)/Wr(f_1, f_2, f_3) = 0$  having coefficients that are rational functions. This equation has Galois group  $G_{168}$  and it has solutions parameterizing the Riemann surface  $\mathcal{S}$ . Referring to this curve, Klein says in footnote 21 of [9]: “*Sie muss sich auch durch eine lineare Differentialgleichung dritter Ordnung lösen lassen; wie hat man dieselbe aufzustellen?*”. Hurwitz [7] used the above reasoning to find this equation (c.f., [4], p. 232, 390).



## References

1. Blichfeld, H. F., *Finite collineation groups*, University of Chicago Press, 1917
2. Cannon, J. J., *An introduction to the group theory language Cayley*. In *Computational Group Theory*, Atkinson, M.D. (ed), New York: Academic Press 1984
3. Fuchs, L., *Ueber die linearen Differentialgleichungen zweiter Ordnung, welche algebraische Integrale besitzen, zweite Abhandlung*, J. für Math., **85** (1878)
4. Gray, J., *Linear differential equations and group theory from Riemann to Poincaré*, Boston, Basel, Stuttgart: Birkhäuser 1986
5. Grigor'ev, D. Yu., *Complexity of factoring and calculating the GCD of linear ordinary differential operators*, J. Symb. Comp., **10** (1990)
6. Halphen, G., *Sur une équation différentielle linéaire du troisième ordre*, Math. Ann., **24** (1884)
7. Hurwitz, A., *Ueber eine besondere homogene lineare Differentialgleichungen*, Math. Ann., **26** (1886)
8. Kaplansky, I., *Introduction to differential algebra*, Paris: Hermann 1957
9. Klein, F., *Über die Transformation siebenter Ordnung der elliptischen Funktionen* Math. Ann, **14**, (1878/79)
10. Poole, E. G. C., *Introduction to the Theory of Linear Differential Equations*, Dover Publications. New York, 1960
11. Schlesinger, L., *Handbuch der Theorie der linearen Differentialgleichungen*, Leipzig: Teubner 1895
12. Schwarz, F., *A Factorization algorithm for linear ordinary differential equations*, Proceedings of the 1989 Symposium on Symbolic and Algebraic Computation, ACM 1989
13. Singer, M. F., *Liouvillian solutions of  $n^{\text{th}}$  order linear differential equations*, Amer. J. Math., **103** (1981)
14. Singer, M. F., *An outline of differential Galois theory*, in *Computer Algebra and Differential Equations*, Ed. E. Tournier, New York: Academic Press 1990
15. Singer, M. F., Ulmer, F., *Galois group of second and third order Linear differential equations*, Preprint, North Carolina State University (1992)
16. Singer, M. F., Ulmer, F., *Liouvillian and algebraic solutions of second and third order Linear differential equations*, Preprint, North Carolina State University (1992)
17. Tretkoff, C., Tretkoff, M., *Solution of the inverse problem of differential Galois theory in the classical case*, Amer. J. Math., **101** (1979)