Computing the Galois group of a polynomial using linear differential equations

Olivier Cormier
IRMAR
Université de Rennes I
Campus de Beaulieu
F-35042 Rennes Cedex
ocormier@maths.univ-rennes1.fr

Michael F. Singer*
Dept. of Math.
Box 8205
NC State University
Raleigh, NC 27695-8205
singer@math.ncsu.edu

Felix Ulmer
IRMAR
Université de Rennes I
Campus de Beaulieu
F-35042 Rennes Cedex
ulmer@maths.univ-rennes1.fr

ABSTRACT

In this paper we show how to compute the Galois group G of a polynomial $f \in \overline{\mathbb{Q}}(x)[Y]$ by factoring the associated linear differential equation $L_f(Y) = 0$ (and constructions of it) of minimal order satisfied by the roots of f. We use that the differential Galois group of $L_f(Y)$ is a faithful linear representation of G whose character is a summand of the permutation character of G acting on the roots of f. Our approach is motivated by the fact that the orders of the involved differential equations are much lower than the degrees of the Lagrange resolvants of f. In the final section we show how, if $f \in \mathbb{Q}(x)[Y]$, our approach via differential Galois theory helps one to also compute the Galois group of f over $\mathbb{Q}(x)$.

1. FROM POLYNOMIALS TO LINEAR DIFFERENTIAL EQUATIONS

In the following we will consider the field $\mathbb{Q}$, but the results remain valid for any field of characteristic 0. Let

$$f = Y^m + \sum_{i=0}^{m-2} b_i(x)Y^i \in \overline{\mathbb{Q}}(x)[Y]$$

be a polynomial of degree m where the coefficient of Y^{m-1} is assumed to be zero[1]. We assume that f is an irreducible element of $\overline{\mathbb{Q}}(x)[Y]$ (i.e. that f is absolutely irreducible) and denote K the splitting field of f over $\overline{\mathbb{Q}}(x)$ and $z_1, \ldots, z_m$ the roots of $f(Y) = 0$ in K.

We now describe the well known construction of a linear differential equation with coefficients in $\overline{\mathbb{Q}}(x)$ whose solution space is spanned, as $\overline{\mathbb{Q}}$-vector space, by the zeros z_i of f. On the rational function field $\overline{\mathbb{Q}}(x)$ we consider the usual derivation δ given by $\delta(\mathbb{Q}) = 0$ (resp. $\delta(\overline{\mathbb{Q}}) = 0$) and $\delta(x) = 1$. There is a unique extension of δ to the field K given by

$$\delta(z_j) = -\frac{\sum_{i=0}^{m-2} b_i(x)' z_j^i}{m z_j^{m-1} + \sum_{i=1}^{m-2} i b_i(x) z_j^{i-1}}$$

obtained by differentiating $f(z_j) = 0$. Let z_i be a zero of f, then by the above formula all derivatives of z_i also belong to $\overline{\mathbb{Q}}(x)(z_i)$. Thus, with this derivation, K is a differential field extension of $\overline{\mathbb{Q}}(x)$. In the following we denote $\delta(t)$ by t' and $\delta^i(t)$ simply $t^{(i)}$. Since $\overline{\mathbb{Q}}(x)(z_i)$ is a $\overline{\mathbb{Q}}(x)$-vector space of dimension m, we get that the $m+1$ elements $z_i, z_i', \ldots, z_i^{(m)}$ must be linearly dependent over $\overline{\mathbb{Q}}(x)$, i.e. z_i must satisfy a linear differential equation of order at most m over $\overline{\mathbb{Q}}(x)$. Let $L_f(Y)$ be the linear differential equation corresponding to the linear dependent set $z_i, z_i', \ldots, z_i^{(n)}$ having the property that n is minimal. Since the computations involve only division by f, all roots of f will be solutions of L_f which thus is the linear differential equation of lowest order over $\overline{\mathbb{Q}}(x)$ satisfied by all z_i. The construction of $L_f(Y)$ can be done using linear algebra. In particular, if $f \in \mathbb{Q}(x)[Y]$, then the coefficients of L_f are in $\mathbb{Q}(x)$.

We refer to [6, 11] for an introduction to differential field extensions, Picard-Vessiot extensions and differential Galois groups. Let k be a differential field and $f \in k[Y]$. A Picard-Vessiot extension F of k for L_f is the differential analogous of a splitting field and has the following properties:

1. F is the smallest differential field extension obtained by adjoining a fundamental solution set $\{y_1, \ldots, y_n\}$ of $L_f(y) = 0$ to k.

2. The constants of F and k are the same.

So F is an extension of k with no new constants. If the field of constants of the ground field is algebraically closed, then F always exists. This is the reason for considering f in $k[Y] = \overline{\mathbb{Q}}(x)[Y]$ and explains why our approach produces the Galois group of f over $\overline{\mathbb{Q}}(x)$. The differential Galois

*Partially supported by NSF Grant CCR-9731507.

[1]This is not necessary for the results to hold, but avoids a trivial character in the character decompositions later

group of L_f (over $\overline{\mathbb{Q}}(x)$) is the subgroup of the Galois group of $F/\overline{\mathbb{Q}}(x)$ whose elements σ commute with δ, i.e. $\sigma\delta = \delta\sigma$.

PROPOSITION 1. *Let K be the splitting field of f over $\overline{\mathbb{Q}}(x)$, G the galois group of $K/\overline{\mathbb{Q}}(x)$, F a Picard-Vessiot extension of $\overline{\mathbb{Q}}(x)$ for $L_f(Y) = 0$ and $\mathcal{G}$ the differential Galois group of $F/\overline{\mathbb{Q}}(x)$. Then $K = F$ and $G = \mathcal{G}$.*

PROOF. Since any root of f is a solution of $L_f(Y) = 0$, we have that $K \subset F$. Since elements of $\mathcal{G}$ are automorphisms they must send a root of f into another root. Thus the $\overline{\mathbb{Q}}$-vector subspace V of the solution space of $L_f(Y) = 0$ generated by $\{z_1, \ldots, z_m\}$ is $\mathcal{G}$-invariant. We denote n the dimension and $y_1, \ldots, y_n$ a basis of V over $\overline{\mathbb{Q}}$. According to [11] Proposition 3.5 the linear differential equation $\tilde{L}(Y)$ obtained by expanding

$$\frac{1}{|Wr(y_1, \ldots, y_n)|}\begin{vmatrix} y_1 & \ldots & y_n & Y \\ y_1' & \ldots & y_n' & Y' \\ \vdots & \vdots & \vdots & \vdots \\ y_1^{(n)} & \ldots & y_n^{(n)} & Y^{(n)} \end{vmatrix} = 0$$

along the last column is a linear differential equation over $\overline{\mathbb{Q}}(x)$ having V as solution space. Since V is a subspace of the solution space of $L_f(Y) = 0$, we have that $\tilde{L}(Y)$ is a right divisor of $L_f(Y)$ (cf. [11] Proposition 3.5). Since $L_f(Y)$ is a differential equation of minimal order with respect of having all z_i as solutions, we have that, up to multiple in $\overline{\mathbb{Q}}(x)$, $\tilde{L}(Y) = L_f(Y)$. Thus $F \subset K$ showing that $F = K$. Since for a finite algebraic extension the classical and the differential Galois group coincide (cf. [14]), we have that G and $\mathcal{G}$ are the same groups acting on $K = F$. ☐

EXAMPLE 1. *We consider the polynomial $f = Y^3 - x \in \mathbb{Q}(x)[Y]$. Here the derivative of a root z of f is given by $z' = \frac{1}{3x}\, z$ and the linear differential equation $L_f(y)$ is $y' - \frac{1}{3x}\, y$. Note that the roots of f are $z_1 = x^{1/3}$, $z_2 = \xi \cdot x^{1/3}$ and $z_3 = \xi^2 \cdot x^{1/3}$ where ξ is a primitive cube root of unity. Thus the $\overline{\mathbb{Q}}$-vector space generated by the roots is of dimension one. Our approach will show that the Galois group of f over $\overline{\mathbb{Q}}(x)$ is cyclic. Thus we do not in general get the Galois group over $\mathbb{Q}(x)$ which in this case would be S_3.* ◇

The Galois group of f acts by permutation of the roots which gives a faithful permutation representation of G whose permutation character is denoted χ_P. Since G is also the differential Galois group of $L_f(y)$, the action of G on the solution space V gives a faithful character χ_L of G. The trivial character of G is denoted by $\mathbb{1}$.

PROPOSITION 2. *(see [9]) The character χ_L of G is a summand of $\chi_P - \mathbb{1}$.*

PROOF. Denote z_i the roots of f in the Picard-Vessiot extension F and V the solution space of $L_f(Y) = 0$. We consider the application $\varphi\colon \oplus_{i=1}^m z_i\overline{\mathbb{Q}} \to V$ given by $\varphi(z_i) = z_i$. Both spaces are G-modules of characters respectively χ_P and χ_L. It is clear that φ is a surjective G-morphism. The image V of φ is a summand of $\oplus_{i=1}^m z_i\overline{\mathbb{Q}}$. Since G is a finite group, by Maschke's theorem this summand must be a direct summand and its character a summand of χ_P. In $\oplus_{i=1}^m z_i\overline{\mathbb{Q}}$ the character of G on the one dimensional subspace generated by $z_1 + \cdots + z_m$ is trivial. Since in V one has $\sum_{i=1}^m z_i = 0$, we see that χ_L is a summand of $\chi_P - \mathbb{1}$. ☐

2. FACTORISATION OF LINEAR DIFFERENTIAL EQUATIONS

It is well known that the computation of the Galois group of a polynomial can be reduced to the factorisation of polynomials. A weaker but similar result holds for differential equations [13]. In the following we want to consider a linear differential equation:

$$L(y) = \sum_{i=0}^{n} a_i y^{(i)} = \left(\sum_{i=0}^{n} a_i \delta^i\right)(y) = (p(\delta))\,(y)$$

as a polynomial in δ (i.e. as a differential operator) over $\overline{\mathbb{Q}}(x)$. The set $\mathcal{D}$ of differential operators over the field $\overline{\mathbb{Q}}(x)$ forms a non-commutative ring where addition is the usual addition of polynomials and multiplication is the composition of operators defined by the rule $\forall a \in \overline{\mathbb{Q}}(x)$, $\delta a = a\delta + a'$. A differential equation $L(y) = 0$ is reducible over $\overline{\mathbb{Q}}(x)$ if and only if $L(y) = L_1(L_2(y))$, i.e. if the differential operator factors in products of degree > 0. We refer to [12] for the properties of $\mathcal{D}$. In particular the non-commutative ring $\mathcal{D}$ is a left and right euclidean ring. The ring $\mathcal{D}$ is not a unique factorisation domain, but if $p = p_1 p_2 \cdots p_s$ and $p = \tilde{p}_1 \tilde{p}_2 \cdots \tilde{p}_t$ are two decompositions of an operator $p \in \mathcal{D}$ into irreducible factors, then $s = t$ and there is a permutation $\sigma \in S_t$ such that $\mathcal{D}/\mathcal{D}p_i \cong \mathcal{D}/\mathcal{D}\tilde{p}_{\sigma(i)}$. In particular the representations of $\mathcal{G}$ on the solution space of $p_i(y) = 0$ and $\tilde{p}_{\sigma(i)}(y) = 0$ are isomorphic $\mathcal{G}$-modules. In classical Galois theory a polynomial is reducible if and only if its Galois group is intransitive. The differential analogous is:

THEOREM 1. *(see for example [11]) A linear differential equation $L(y) = 0$ over $\overline{\mathbb{Q}}(x)$ factors if and only if its differential Galois group $\mathcal{G}$ is a reducible linear group over $\overline{\mathbb{Q}}$.*

The factorisation of differential operators is a difficult task. But if the group is reductive (which is always the case in our situation since the groups are subgroups of S_m and thus finite) a factorisation can be found using the Eigenring [12, 15], i.e. using rational solutions of some associated differential equation and thus using linear algebra. Furthermore for reductive groups the character of the representation of $\mathcal{G}$ on the solution space of $L(y) = 0$ will be the sum of the characters on the solution space of the irreducible factors of $L(y)$. The factorisation of L_f gives informations about $\mathcal{G}$:

PROPOSITION 3. *1. The group $\mathcal{G}$ is abelian if and only if L_f is a product of operators of order one.*

2. *The group $G \subset S_m$ is doubly transitive if and only if L_f is irreducible of order $m - 1$.*
3. *The group $\mathcal{G}$ is trivial if and only if all solutions of L_f are in $\overline{\mathbb{Q}}(x)$ (which can be computed using linear algebra [3, 1]).*

PROOF. The first result follows from the fact that a group is abelian if and only if all its irreducible representations are of degree 1. If the action of G on the roots of f is doubly transitive, then $\chi_P = \mathbb{1}+\phi$, where ϕ is an irreducible character of G ([5], Satz 20.2). Since χ_L is a summand of $\chi_P - \mathbb{1} = \phi$ we get that $\chi_L = \phi$ and thus L_f is irreducible. The last assertion follows from the Galois correspondence in differential Galois theory. $\square$

To compute the differential Galois group in our situation, we proceed using the idea of [13] and we use the fact that a finite group $\mathcal{G}$ is determined by its action on "constructions": symmetric and alternating products of the solution space, which are also $\mathcal{G}$-modules.

1. One can construct a differential equation $L^{\circledS s} = 0$ (resp. $L^{\wedge s} = 0$) whose solution space corresponds to the symmetric product $\mathrm{Sym}^s(V)$ (resp. the alternating product $\bigwedge^s(V)$).
2. The corresponding characters of $\mathcal{G}$ are denoted $\chi_L^{\circledS s}$ and $\chi_L^{\wedge s}$ and can be computed directly from χ_L.
3. Factorisation of $L^{\circledS s}$ (resp. $L^{\wedge s}$) gives us the degrees of the irreducible characters of χ_L that appear in the decompositions of $\chi_L^{\circledS s}$ and $\chi_L^{\wedge s}$.
4. Comparing the result with the tables below allows us to determine the group.

Tables 1 and 2 give the decomposition into irreducible characters of $\chi_P - \mathbb{1}$, where χ_P is the permutation character, for all the transitive permutation groups of degree 3 to 8 given in [4]. Similar tables can be constructed for every degree.

Some notations: A linear character of order i is denoted by 1_i and a character of degree n simply by n. In order to distinguish non-equivalent irreducible characters of the same degree n, we use the notation $n_a, n_b, \ldots$ and if the decompositions of the i^{th} symmetric (resp. alternating) product of n_a and n_b are the same we simply write $n^{\circledS i}$ (resp. $n^{\wedge i}$). For example, the second exterior power of the irreducible character 6 (of degree 6) appearing in the decomposition of the permutation character of $F_{42}(7)$ is the sum of a linear character of order 2, two non-equivalent linear characters of order 6 and two copies of (the character) 6.

We see that we can distinguish each of the transitive groups from the decomposition of their permutation character χ_P and from decompositions of symmetric or alternating powers of irreducible characters appearing in $\chi_P - \mathbb{1}$. This approach will work for any degree: Using a theorem due to Chevalley, for any finite subgroup H of $GL(n, \mathcal{C})$ there is a faithful representation $\Phi : GL(n, \mathcal{C}) \rightarrow GL(m, \mathcal{C})$ for some m such that $\Phi(H)$ is uniquely determined by its set of invariant subspaces in $\mathcal{C}^m$ and any representation can be constructed from a given faithful representation using the tools of linear algebra, i.e., tensor product, duals, direct sums and subspaces (see [13]). Given a polynomial f irreducible over $\overline{\mathbb{Q}}(x)$, we first compute the differential equation $L_f = 0$ associated to it and determine the degrees of the irreducible factors of L_f. If the order of L_f is too small, we may not directly determine the Galois group of f using the tables above, but after Tschirnhaus transformation $Y \mapsto \sum_{j=0}^{m-1} u_j Y^j$ where $u_i \in \mathbb{Q}(x)$ the degree will become maximal.

LEMMA 1. *Let k be a differential field of characteristic zero with field of constants C. Assume that there is an element $x \in k$ with $x' = 1$. If $y_1, \ldots, y_m \in k$ are distinct elements, then there exist polynomials $u_i \in C[x]$ of degree at most m such that the elements $\tilde{y}_i = \sum_{j=0}^{m-1} u_j y_i^j$ are linearly independent over C. In particular, if $y_1, \ldots, y_m$ are solutions of a polynomial f of degree m over $\mathbb{Q}(x)$ (resp. $\overline{\mathbb{Q}}(x)$), then $\tilde{y}_1, \ldots, \tilde{y}_m$ are also solutions of a polynomial $\tilde{f}$ of degree m over $\mathbb{Q}(x)$ (resp. $\overline{\mathbb{Q}}(x)$), the Galois groups of f and $\tilde{f}$ are the same and the equation $L_{\tilde{f}}$ will be of maximal order m.*

PROOF. Let $U_1, \ldots, U_m$ be differential indeterminates. The field of constants of $K = k < U_1, \ldots, U_m >$ is once again C. The elements $V_i = \sum_{j=0}^{m-1} U_{j+1} y_i^j$ are linearly independent over C. To see this, note that $(V_1, \ldots, V_m) = (U_1, \ldots, U_m)V$ where V is the van der Monde matrix of $y_1, \ldots, y_n$. Let $c_1, \ldots, c_n$ be constants such that $\sum c_i V_i = 0$. We then have that $(U_1, \ldots, U_n)V(c_1, \ldots, c_n)^T = 0$ and so $V(c_1, \ldots, c_n)^T = 0$. Since V is nonsingular, we must have that $(c_1, \ldots, c_n)^T = 0$. We can therefore conclude that the wronskian determinant W of the V_i is a nonzero differential polynomial in the Y_i. This polynomial has order $n-1$ in the U_i and so by a result of [8] p.35, there exist polynomials u_i of degree at most n such that the substitution $U_i \mapsto u_i$ keeps W nonzero. Thus the elements $\tilde{y}_i = \sum_{j=0}^{m-1} u_j y_i^j$ are linearly independent over C.
If $y_1, \ldots, y_m$ are zeros of a polynomial f over $\mathbb{Q}(x)$, then the permutation action of the Galois group G of f on the y_i coincides with the permutation action of G on the $\tilde{y}_i$. Thus $\tilde{y}_1, \ldots, \tilde{y}_m$ are also solutions of a polynomial $\tilde{f}$ of degree m over $\mathbb{Q}(x)$, and the Galois group of f and $\tilde{f}$ coincide. Being solutions of a polynomial of degree m over $\mathbb{Q}(x)$, $\tilde{y}_1, \ldots, \tilde{y}_m$ are solutions of a linear differential equation $L_{\tilde{f}}$ of degree at most m over $\mathbb{Q}(x)$. Since $\tilde{y}_1, \ldots, \tilde{y}_m$ are linearly independent over the field of constants $\mathbb{Q}$, the equation $L_{\tilde{f}}$ is of degree m. The same result holds for $\overline{\mathbb{Q}}(x)$. $\square$

EXAMPLE 2. *Consider the polynomial $f = Y^4(Y^4 - 8Y^2 + 18) + 81x^2$ (from [7], p. 405, $f_{8,32}$) which is irreducible over $\overline{\mathbb{Q}}(x)$. The corresponding differential equation is:*

$$L_f(y) = y^{(4)} + \frac{2(12x^4-15x^2-1)}{x(x^2-1)(3x^2+1)} y^{(3)} + \frac{2997x^6-4600x^4-995x^2+6}{24x^2(x^2-1)(3x^2+1)^2} y'' + \frac{810x^6-1863x^4-97x^2-6}{24x^3(x^2-1)(3x^2+1)^2} y' - \frac{27(5x^2-21)}{256(x^2-1)(3x^2+1)^2} y = 0$$

Using the Eigenring, we show that it is irreducible. According to the tables, the Galois group $G_{\overline{\mathbb{Q}}(x)}$ of f belongs to a family of 19 groups (from $[1/4.cD(4)^2]2$ to $[2^4]S(4)$). The 4th exterior power of L_f is $y' + \frac{2(12x^4-15x^2-1)}{x(x^2-1)(3x^2+1)} y = 0$ and has the rational solution $\frac{(x^2-1)}{x^2(1+3x^2)^4}$. So there remain 7 possible groups. The 2nd exterior power of L_f is of order 6 and factors as a product of two irreducible differential equations of order 3, which one is:

Table 1: Degree 3 to 6

Degree 3

G	$C(3)=A(3)$	$S(3)$
$\chi_P-\mathbb{1}$	$1_{3a},1_{3b}$	2

Degree 4

G	$C(4)$	$E(4)$	$D(4)$	$A(4)$	$S(4)$
$\chi_P-\mathbb{1}$	$1_2,1_{4a},1_{4b}$	$1_{2a},1_{2b},1_{2c}$	$1_2,2$	3	3
$3^{\wedge 3}$				$\mathbb{1}$	1_2

Degree 5

G	$C(5)$	$D(5)$	$F(5)$	$A(5)$	$S(5)$
$\chi_P-\mathbb{1}$	$1_{5a},1_{5b},1_{5c},1_{5d}$	$2_a,2_b$	4	4	4
$4^{\wedge 4}$			1_2	$\mathbb{1}$	1_2
$4^{\wedge 2}$			$1_{4a},1_{4b},4$		6

Degree 6

G	$C(6)$	$D_6(6)$	$D(6)$	$F_{18}(6)$	$S_4(6d)$	$S_4(6c)$	$2S_4(6)$	$A_4(6)$	$2A_4(6)$
$\chi_P-\mathbb{1}$	$1_2,1_{3a},1_{3b},1_{6a},1_{6b}$	$1_2,2,2$	$1_2,2_a,2_b$	$1_2,2_a,2_b$	$2,3$	$2,3$	$2,3$	$1_{3a},1_{3b},3$	$1_{3a},1_{3b},3$
$2^{\circledS 2}$			$\mathbb{1},2$	$1_3,2$					
$3^{\wedge 3}$					1_2	$\mathbb{1}$	1_2	$\mathbb{1}$	1_2
$3^{\circledS 2}$					$\mathbb{1},2,3$	$\mathbb{1},2,3$	$\mathbb{1},2,3$	$\mathbb{1},1_{3a},1_{3b},3$	$\mathbb{1},1_{3a},1_{3b},3$
$3^{\circledS 3}$					$\mathbb{1},3_a,3_a,3_b$		$1_2,3_a,3_a,3_b$		

G	$F_{18}(6):2$	$F_{36}(6)$	$F_{36}(6):2$	$A_5(6)$	$S_5(6)$	$A(6)$	$S(6)$
$\chi_P-\mathbb{1}$	$1_2,4$	$1_2,4$	$1_2,4$	5	5	5	5
$4^{\wedge 4}$	$\mathbb{1}$	1_2	1_2				
$4^{\wedge 2}$		$1_{4a},1_{4b},4$	$2,4$				
$5^{\wedge 5}$				$\mathbb{1}$	1_2	$\mathbb{1}$	1_2
$5^{\wedge 2}$				$3_a,3_b,4$	$4,6$	10	10

$$L_3(y)=y^{(3)}+\frac{2(60x^4-15x^2-1)}{x(5x^2-1)(1+3x^2)}y''+\frac{7425x^6-1951x^4-613x^2+3}{12x^2(1+3x^2)^2(5x^2-1)}y' + \frac{2025x^6-1269x^4-17x^2-3}{12x^3(5x^2-1)(1+3x^2)^2}y=0$$

Therefore, $G_{\overline{\mathbb{Q}}(x)}$ is either $[2^3]A(4)$ or $1/2[2^4]S(4)$. The 3rd exterior power of L_3 has $\frac{(5x^2-1)}{x^2(1+3x^2)^4}$ as a rational solution, so $G_{\overline{\mathbb{Q}}(x)}$ is $[2^3]A(4)$. $\diamond$

If one obtains decomposition of L_f like the decomposition of the permutation character of $D_6(6)$ or $D(6)$ (let's forget the linear characters), this means that in the latter case L_f is the product of two irreducible isomorphic equations of order 2 and in the former case L_f is the product of two irreducible non-isomorphic equations of order 2. We can distinguish the two cases using the Eigenring: Let's consider L_c the Least Common Left Multiple (LCLM) of the two irreducible equations L_1 and L_2 of order 2. A simple consideration (see for instance Section 2.2 in [12]) yields that in the first case the Eigenring of L_c, $\mathcal{E}_{\mathcal{D}}(L_c)$, is of dimension 1 or 4 (depending on whether L_1 and L_2 are equal or not) whereas in the second case $\mathcal{E}_{\mathcal{D}}(L_c)$ is of dimension 2.

Example 3. *Consider the polynomial $f=Y^2(Y^2+3)^2+4x$ (from [7], p. 404, $f_{6,3}$) which is irreducible over $\overline{\mathbb{Q}}(x)$. By the transformation $Y\mapsto(Y+1)/(Y-1)$, f is changed in $\tilde{f}=(x+4)Y^6-6xY^5+15xY^4+(8-20x)Y^3+15xY^2-6xY+x+4$. The differential equation $L_{\tilde{f}}=0$ is of order 6 (note that here the character is χ_P because the coefficient of Y^5 is not 0) and factors into two equations of order 1 and two irreducible equations L_1 and L_2 of order 2. Hence, $G_{\overline{\mathbb{Q}}(x)}$ is equal to $D_6(6)$, $D(6)$ or $F_{18}(6)$. We have :*

$$L_1(y)=y''+\frac{-5x-4+4x^2}{2x(x+4)(x-1)}y'+\frac{5x+2}{36x(x+4)(x-1)}y=0$$

$$L_2(y)=y''+\frac{36x^4-213x^3+703x^2+3684x-1760}{2x(x+4)(x-1)(3x^2-21x+88)}y' + \frac{336x^5-3342x^4+16147x^3+21381x^2-28240x+3168}{18(x+4)x^2(x-1)^2(3x^2-21x+88)}y=0$$

The LCLM of L_1 and L_2 is of degree 4 and it's Eigenring is of dimension 2, so $G_{\overline{\mathbb{Q}}(x)}$ is equal to $D(6)$ or $F_{18}(6)$. The 2nd symmetric power of L_1 has a rational solution $\frac{5x+4}{(x+4)^2}$ so $G_{\overline{\mathbb{Q}}(x)}=D(6)$. $\diamond$

3. GALOIS GROUP OVER $\mathbb{Q}(X)$

As mentioned before, our approach computes the Galois group $G_{\overline{\mathbb{Q}}(x)}$ of f over $\overline{\mathbb{Q}}(x)$. This is due to the fact that the Picard-Vessiot extension is a no new constants extension. To illustrate this we look at the following example:

Example 4. *We consider $f=Y^3-x\in\mathbb{Q}(x)[Y]$. The roots of $f(Y)=0$ are $z_1=x^{1/3}$, $z_2=\xi\cdot x^{1/3}$ and $z_3=\xi^2\cdot x^{1/3}$ where ξ is a primitive cube root of unity. If we consider the splitting field $\mathbb{Q}(x)(z_1,z_2,z_3)$, we see that it contains the new constant $\xi=z_2/z_1$. This explains why the differential Galois group that we compute using differential equations turns out to be $A(3)$, which is the Galois group over $\overline{\mathbb{Q}}(x)$.* $\diamond$

Table 2: Degree 7 to 8

Degree 7

G	$C(7)$	$D(7)$	$F_{21}(7)$	$F_{42}(7)$	$L(7)=L(3,2)$	$A(7)$	$S(7)$
$\chi_p-\mathbb{1}$	$1_{7a},\cdots,1_{7f}$	$2_a,2_b,2_c$	$3_a,3_b$	6	6	6	6
$6^{\wedge 6}$				1_2	$\mathbb{1}$	$\mathbb{1}$	1_2
$6^{\wedge 2}$				$1_2,1_{6a},1_{6b},6,6$	$7,8$	15	15

Degree 8

G	$C(8)$	$4[x]2$	$E(8)$	$D_8(8)$	$Q_8(8)$
$\chi_p-\mathbb{1}$	$1_2,1_{4a},1_{4b},1_{8a},1_{8b},1_{8c},1_{8d}$	$1_{2a},1_{2b},1_{2c},1_{4a},1_{4b},1_{4c},1_{4d}$	$1_{2a},\cdots,1_{2g}$	$1_{2a},1_{2b},1_{2c},2,2$	$1_{2a},1_{2b},1_{2c},2,2$
$2^{\wedge 2}$				1_2	$\mathbb{1}$

G	$E(8):2$	$Q_8:2$	$1/2[2^3]4$	$[2^2]4$
$\chi_p-\mathbb{1}$	$1_{2a},1_{2b},1_{2c},2_a,2_b$	$1_{2a},1_{2b},1_{2c},2_a,2_b$	$1_2,1_{4a},1_{4b},2_a,2_b$	$1_2,1_{4a},1_{4b},2_a,2_b$
$2^{\wedge 2}$	1_2	1_2	1_4	1_2
$2^{\odot 2}$	$\mathbb{1},1_{2a},1_{2b}$	$1_{2a},1_{2b},1_{2c}$	$1_{4a},1_{4b},1_{4c}$	$\mathbb{1},1_{2a},1_{2b}$

G	$D(8)$	$2D_8(8)$	$[4^2]2$	$E(8):E_4$
$\chi_p-\mathbb{1}$	$1_2,2_a,2_b,2_c$	$1_2,2_a,2_b,2_c$	$1_2,2_a,2_b,2_c$	$1_2,2_a,2_b,2_c$
$2_a^{\odot 2}$, $2_b^{\odot 2}$	$\mathbb{1},2$	$1_2,2$	$1_4,2$	$\mathbb{1},1_{2a},1_{2b}$
$2_c^{\odot 2}$	$\mathbb{1},1_{2a},1_{2b}$	$\mathbb{1},1_{2a},1_{2b}$	$\mathbb{1},1_{2a},1_{2b}$	$\mathbb{1},1_{2a},1_{2b}$

G	$E(8):3$	$S(4)[1/2]2$	$E(8):D_6$	$2A_4(8)=SL(2,3)$
$\chi_p-\mathbb{1}$	$1_2,3_a,3_b$	$1_2,3_a,3_b$	$1_2,3_a,3_b$	$2_a,2_b,3$
$3^{\odot 2}$	$\mathbb{1},1_{3a},1_{3b},3$	$\mathbb{1},2,3$	$\mathbb{1},2,3$	
$3_a^{\wedge 3}$		$\mathbb{1}$	1_2	
$3_b^{\wedge 3}$		1_2	1_2	

G	$[1/4.cD(4)^2]2$	$E(8):4$	$1/2[2^4]eD(4)$	$1/2[2^4]dD(4)$	$E(8):D_8$	$1/2[2^4]cD(4)$	$[2^4]D(4)$
$\chi_p-\mathbb{1}$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$
$4^{\wedge 4}$	$\mathbb{1}$	1_2	$\mathbb{1}$	1_2	1_2	1_2	1_2
$4^{\wedge 2}$	$1_{2a},1_{2b},1_{2c},1_{2d},2$	$1_{4a},1_{4b},2_a,2_b$	$1_{2a},1_{2b},2_a,2_b$	$2,4$	$2_a,2_b,2_c$	$1_{4a},1_{4b},4$	$2,4$
$4^{\odot 2}$				$\mathbb{1},1_2,1_{4a},1_{4b},2,4$			$\mathbb{1},1_2,2_a,2_b,4$

G	$1/2[2^4]4$	$[2^3]4$	$1/2[2^4]E(4)$	$E(8):D_4$	$[2^4]4$	$[2^4]E(4)$
$\chi_p-\mathbb{1}$	$1_2,1_{4a},1_{4b},4$	$1_2,1_{4a},1_{4b},4$	$1_{2a},1_{2b},1_{2c},4$	$1_{2a},1_{2b},1_{2c},4$	$1_2,1_{4a},1_{4b},4$	$1_{2a},1_{2b},1_{2c},4$
$4^{\wedge 4}$	$\mathbb{1}$	1_2	1_2	$\mathbb{1}$	1_2	1_2
$4^{\wedge 2}$	$1_{2a},1_{2b},2_a,2_b$	$1_{4a},1_{4b},2_a,2_b$	$1_{4a},1_{4b},2,2$	$1_{2a},\cdots,1_{2f}$	$2,4$	$2_a,2_b,2_c$

G	$GL(2,3)$	$[2^3]A(4)$	$[2^4]A(4)$	$[2^3]S(4)$	$1/2[2^4]S(4)$	$[2^4]S(4)$
$\chi_p-\mathbb{1}$	$3,4$	$3,4$	$3,4$	$3,4$	$3,4$	$3,4$
$4^{\wedge 4}$	$\mathbb{1}$	$\mathbb{1}$	1_2	1_2	$\mathbb{1}$	1_2
$3^{\wedge 3}$	1_2	$\mathbb{1}$	$\mathbb{1}$	1_2	1_2	1_2
$4^{\wedge 2}$	$1_2,2,3$	$3_a,3_b$	6	6	$3_a,3_b$	6
$4^{\odot 2}$			$\mathbb{1},3,6$	$\mathbb{1},3_a,3_b,3_c$		$\mathbb{1},3,6$

G	$E(8):A_4$	$E(4)^2:D_6$	$E(8):S_4$	$[A(4)^2]2$	$[1/2.S(4)^2]2$	$1/2[S(4)^2]2$	$[S(4)^2]2$
$\chi_p-\mathbb{1}$	$1_2,6$	$1_2,6$	$1_2,6$	$1_2,6$	$1_2,6$	$1_2,6$	$1_2,6$
$6^{\wedge 2}$	$3,6_a,6_b$	$3_a,3_b,3_c,6$	$3,6_a,6_b$	$6,9$	$6,9$	$6,9$	$6,9$
$3^{\odot 2}$	$\mathbb{1},1_{3a},1_{3b},3$		$\mathbb{1},2,3$				
$6^{\odot 2}$				$\mathbb{1},1_2,2_a,2_b,6,9$	$\mathbb{1},1_2,4,6,9$	$\mathbb{1},1_2,4,6,9$	$\mathbb{1},1_2,4,6,9$
$4^{\wedge 2}$					$1_{2a},1_{2b},2_a,2_b$	$1_{4a},1_{4b},4$	$2,4$

G	$E(8):7=F_{56}(8)$	$E(8):F_{21}$	$PSL(2,7)$	$PGL(2,7)$	$E(8):L_7=AL(8)$	$A(8)$	$S(8)$
$\chi_p-\mathbb{1}$	7	7	7	7	7	7	7
$7^{\wedge 7}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$	1_2
$7^{\wedge 2}$	$7,7,7$	$7_a,7_b,7_c$	$3_a,3_b,7,8$	$6,7,8$	21	21	
$7^{\odot 2}$					$\mathbb{1},6,7,14$	$\mathbb{1},7,20$	

However there is a connection between the differential Galois group $G_{\mathbb{Q}(x)}$ of f over $\mathbb{Q}(x)$ and $G_{\overline{\mathbb{Q}}(x)}$. We consider the following diagram:

$$\begin{tikzcd}
& \overline{\mathbb{Q}}(x)(y_1,\dots,y_n) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(x)(y_1,\dots,y_n) \arrow[dr, dash] & & \overline{\mathbb{Q}}(x) \arrow[dl, dash] \\
& \mathbb{Q}(x)(y_1,\dots,y_n)\cap\overline{\mathbb{Q}}(x) \arrow[d, dash] & \\
& \mathbb{Q}(x) &
\end{tikzcd}$$

Thus $G_{\overline{\mathbb{Q}}(x)}$, which is isomorphic to the Galois group of $\mathbb{Q}(x)(y_1,\dots,y_n)$ over $\mathbb{Q}(x)(y_1,\dots,y_n)\cap\overline{\mathbb{Q}}(x)$, is a normal subgroup of $G_{\mathbb{Q}(x)}$. The next corollary shows that the groups are distinct if and only if new constants appear.

LEMMA 2. *Let k_0 be a field of characteristic 0 with algebraic closure $\overline{k_0}$. Let F be a field with $k_0(x)\subset F\subset \overline{k_0}(x)$. If $k_0(x)\neq F$, then there exists a $c\in F\cap\overline{k_0}$. Furthermore $F=k(x)$ for some $k_0\subset k\subset\overline{k_0}$.*

PROOF. F is algebraic over $k_0(x)$. We begin by assuming that $[F:k_0(x)]<\infty$. The primitive element theorem implies that $F=k_0(x)(z)$ for some $z\in\overline{k_0}(x)$. Since $z\in\overline{k_0}(x)$, we may write $z=\frac{\sum_i a_i x^i}{\sum_j b_j x^j}$ with $a_i,b_i\in\overline{k_0}$. Therefore $F\subset k_0(x)(\{a_i\},\{b_j\})$ and, again by the primitive element theorem, this latter field may be written as $k_0(x)(\alpha)$ with $\alpha\in\overline{k_0}$. We now extend the zero derivation on k_0 via $x'=1$ to a derivation of $\overline{k_0}(x)$. In particular the set of constants is $\overline{k_0}$ and so $\alpha'=0$. An element $w\in F$ can be written uniquely as $w=\sum_{i=0}^{s}\omega_i\alpha^i$ with $\omega_i\in k_0(x)$ and $s<[k_0(\alpha):k_0]$. Consider now some $w\in F$ which is not in $k_0(x)$ and having the property that s is minimal. For this w we may assume $\omega_s=1$. Differentiating we get $w'=\sum_{i=0}^{s-1}\omega_i'\alpha^i$ and, by the minimality of s, $w'\in k_0(x)$. We therefore have that $\omega_i'=0$ for $i\in\{1,\dots,s-1\}$ and $\omega_0'=g\in k_0(x)$. Therefore $(w-\omega_0)'=0$ and $w-\omega_0\notin k_0(x)$. This proves the first claim under the assumption that $[F:k_0(x)]<\infty$. One removes this assumption by noting that any F as described in the lemma is a direct limit of fields finitely generated over $k_0(x)$. To prove the second claim, let $k=F\cap k_0(x)$. If $F\neq k(x)$, then the first part implies that there exists an element $c\in F\cap\overline{k_0}$ such that $c\notin k$, a contradiction. $\square$

COROLLARY 1. *If $G_{\overline{\mathbb{Q}}(x)}\neq G_{\mathbb{Q}(x)}$, then the field extension $\mathbb{Q}(x)(y_1,\dots,y_n)\cap\overline{\mathbb{Q}}(x)$ of $\mathbb{Q}(x)$ is generated by constants (i.e. is obtained by adjoining new constants to $\mathbb{Q}(x)$).*

Note that $G_{\overline{\mathbb{Q}}(x)}$ is a (transitive) normal subgroup of the (transitive) group $G_{\mathbb{Q}(x)}$. From the table below we see that, in most cases, there are only very few possibilities for $G_{\mathbb{Q}(x)}$ once $G_{\overline{\mathbb{Q}}(x)}$ is known.

Table 3 illustrate this fact: Given a transitive group G on n letters, we list, for $n=3,4,5,6$ and 7, all the proper normal transitive subgroups N of G.

Thus once the group $G_{\overline{\mathbb{Q}}(x)}$ is known, there are only few possibilities left for $G_{\mathbb{Q}(x)}$. We now fix a possible group G for $G_{\mathbb{Q}(x)}$ having $G_{\overline{\mathbb{Q}}(x)}$ as proper normal subgroup and want to decide, using differential Galois theory, if $G=G_{\mathbb{Q}(x)}$. By Corollary 1 we know that if $G=G_{\mathbb{Q}(x)}\neq G_{\overline{\mathbb{Q}}(x)}$ then the extension $\mathbb{Q}(x)(y_1,\dots,y_n)$ of $\mathbb{Q}(x)$ contains new constants. We consider a tentative $\mathbb{Q}(x)$-basis $\mathcal{B}=\{b_1=1,b_2,\dots,b_{|G|}\}$ (which we suppose given) of $|G|$ elements of $\mathbb{Q}(x)(y_1,\dots,y_n)$ over $\mathbb{Q}(x)$ and write $z=\sum_{i=1}^{|G|}u_ib_i$ with $u_i\in\mathbb{Q}(x)$. The condition $z'=0$ is therefore equivalent to a certain differential system $\mathcal{S}$ of order one, in the variables u_i, having solutions in $\mathbb{Q}(x)$, which can be decided using [2, 3][2]. We assume that we know how to compute the system $\mathcal{S}$. A new constant corresponds to a "non trivial solution ", i.e. for which $\exists i>1,\ u_i\neq 0$. We now want to decide if a non trivial solution

$$z=\sum_{i=1}^{|G|}u_ib_i$$

where the b_i are monomials in y_j is indeed a new constant. For this we will use Taylor series at a point $\alpha\in\mathbb{Q}$.

LEMMA 3. *Let $y_1,\dots,y_n$ be solutions of $L_f(y)=0$, $s\in\mathbb{N}$ and $u_1,\dots,u_n\in\mathbb{Q}(x)$. There exist a point $\alpha\in\mathbb{Q}$ and a bound $M\in\mathbb{N}$, depending on α, s, $u_1,\dots,u_n$ and $y_1,\dots,y_n$, such that: $z=\sum_{i=1}^{|G|}u_ib_i\in\overline{\mathbb{Q}}$ (where the b_i are monomials in y_j) if and only if the coefficients of $x-\alpha,(x-\alpha)^2,\dots,(x-\alpha)^M$ in the Taylor series expansion of z at α are 0.*

PROOF. Since the u_i and the y_i all satisfy some linear differential equations, one can construct a differential equation $L_1(y)$ satisfied by z ([10]). Now 1 (and thus any element of $\overline{\mathbb{Q}}$) and z are both solutions of the Least Common Left Multiple $L_3(y)$ of $L_1(y)$ and $L_2(y)=y'$. We take for α a regular point of $L_3(y)$ and for M the order of $L_3(y)$ at α. If at α the Taylor series of two solutions agree on terms of order less than M, then the solutions coincide. The result now follows. $\square$

We use the notation of the Lemma. Note that $\gamma\in\overline{\mathbb{Q}}\cap\mathbb{Q}(y_1,\dots,y_n)$ is uniquely determined by its Taylor series $\gamma+O((x-\alpha)^{M+1})$. We now have the following cases:

- if $\mathcal{S}$ has no non-trivial rational solution then we must have $G_{\mathbb{Q}(x)}\neq G$. If G is the only candidate different from $G_{\overline{\mathbb{Q}}(x)}$ for $G_{\mathbb{Q}(x)}$, then $G_{\mathbb{Q}(x)}=G_{\overline{\mathbb{Q}}(x)}$.
- if $\mathcal{S}$ has a non-trivial rational solution whose Taylor series evaluates to $\gamma+O((x-\alpha)^{M+1})$ with $\gamma\notin\mathbb{Q}$,

[2]It is important to note that those algorithms work over $\mathbb{Q}(x)$

Table 3: Transitive groups G and its normal transitive subgroups N

G	$A(3)$	$S(3)$
N		$A(3)$
G/N		$C(2)$

G	$C(4)$	$E(4)$	$D(4)$		$A(4)$	$S(4)$	
N			$C(4)$	$E(4)$	$E(4)$	$E(4)$	$A(4)$
G/N			$C(2)$	$C(2)$	$C(3)$	$S(3)$	$C(2)$

G	$C(5)$	$D(5)$	$F(5)$		$A(5)$	$S(5)$
N		$C(5)$	$C(5)$	$D(5)$		$A(5)$
G/N		$C(2)$	$C(4)$	$C(2)$		$C(2)$

G	$C(6)$	$D_6(6)$	$D(6)$		$A_4(6)$	$F_{18}(6)$	$2A_4(6)$	$S_4(6d)$	$S_4(6c)$	$F_{18}(6):2$	
N			$C(6)$	$D_6(6)$		$D_6(6)$	$A_4(6)$	$A_4(6)$	$A_4(6)$	$D_6(6)$	$F_{18}(6)$
G/N			$C(2)$	$C(2)$		$C(3)$	$C(2)$	$C(2)$	$C(2)$	$S(3)$	$C(2)$

G	$F_{36}(6)$	$2S_4(6)$				$PSL(2,5)$	$F_{36}(6):2$		$PGL(2,5)$	$A(6)$	$S(6)$
N		$A_4(6)$	$S_4(6d)$	$S_4(6c)$	$2A_4(6)$		$F_{18}(6):2$	$F_{36}(6)$	$PSL(2,5)$		$A(6)$
G/N		$E(4)$	$C(2)$	$C(2)$	$C(2)$		$C(2)$	$C(2)$	$C(2)$		$C(2)$

G	$C(7)$	$D(7)$	$F_{21}(7)$	$F_{42}(7)$			$L(3,2)$	$A(7)$	$S(7)$
N		$C(7)$	$C(7)$	$C(7)$	$D(7)$	$F_{21}(7)$			$A(7)$
G/N		$C(2)$	$C(3)$	$C(6)$	$C(3)$	$C(2)$			$C(2)$

then $z = \gamma$ and we found a new constant in $\overline{\mathbb{Q}} - \mathbb{Q}$. We then conclude that $G_{\mathbb{Q}(x)} \neq G_{\overline{\mathbb{Q}}(x)}$.

- if $\mathcal{S}$ has a non-trivial rational solution which is not of the form $\gamma + O((x-\alpha)^{M+1})$ with $\gamma \notin \mathbb{Q}$, then we get a contradiction, because according to Corollary 1 any new constant must be of this form. We then conclude that our tentative $\mathbb{Q}(x)$-basis $\mathcal{B}$ was not a basis and thus that $G_{\mathbb{Q}(x)} \neq G$. If G is the only candidate different from $G_{\overline{\mathbb{Q}}(x)}$ for $G_{\mathbb{Q}(x)}$, then $G_{\mathbb{Q}(x)} = G_{\overline{\mathbb{Q}}(x)}$.

EXAMPLE 5. *We have already seen that the Galois group of $f = Y^3 - x$ over $\overline{\mathbb{Q}}(x)$ is $N = A(3)$. We will prove that its Galois group over $\mathbb{Q}(x)$ is $G = S(3)$.*
First, by performing the Tschirnaus transformation $Y \mapsto \frac{Y+1}{Y-1}$ on f and eliminating the term in Y^2, we obtain the following polynomial $\tilde{f} = Y^3 - \frac{12x}{(x-1)^2}Y - \frac{8x(x+1)}{(x-1)^3}$. The differential equation associated to $\tilde{f}$ is :

$$L_{\tilde{f}}(y) = y'' + \frac{2}{x-1}y' + \frac{2}{9x^2}y = 0$$

As $L_{\tilde{f}}$ is the product of the two linear operators $\delta + \frac{4x-1}{3x(x-1)}$ and $\delta + \frac{2x+1}{3x(x-1)}$, the Galois group of $\tilde{f}$ over $\overline{\mathbb{Q}}(x)$ is $A(3)$.
Let y_1, y_2 and y_3 denote the roots of $\tilde{f}$ and suppose that $\{1, y_1, y_2, y_1y_2, y_1^2, y_2y_1^2\}$ is a basis of $\mathbb{Q}(x)(y_1, y_2, y_3)$. Suppose that $z = u_0 + u_1y_1 + u_2y_2 + u_3y_1y_2 + u_4y_1^2 + u_5y_2y_1^2$ is a constant. The condition $z' = 0$ leads to the system $\mathcal{S}_1$.

Using the algorithm presented in [2], we find that the above differential system admits the rational solutions : $u_0 = \lambda_1 + \frac{8}{x-1}\lambda_0$, $u_1 = 4\lambda_0$, $u_2 = -4\lambda_0$, $u_3 = u_4 = 0$ and $u_5 = \frac{(x-1)^2}{x}\lambda_0$, where λ_0 and λ_1 are constants. Computing the Puiseux expansions of $\tilde{f}$ at $x = 0$, we take $y_1 = \frac{2}{x-1}(x^{1/3} + x^{2/3})$ and $y_2 = \frac{1}{x-1}((-1 + I\sqrt{3})x^{1/3} + (-1 - I\sqrt{3})x^{2/3})$. We find therefore that (for $\lambda_0 = 1$) $z = \frac{8}{x-1} + 4y_1 - 4y_2 + \frac{(x-1)^2}{x}y_2y_1^2$ evaluates to $-4(1 + I\sqrt{3})$ which is a multiple of the cube root of unity ξ. We have found a new non-rational constant so $G_{\mathbb{Q}(x)} = S(3)$. ◇

EXAMPLE 6. *Consider the polynomial $f = Y^3 - (1 + 3x^2)(3Y - 2)$ (from [7], p. 404, $f_{3,1}$) which is irreducible over $\overline{\mathbb{Q}}(X)$. The differential equation associated to f is :*

$$L_f(y) = y'' - \frac{8}{3(1+3x^2)^2}y = 0$$

and L_f is the product of the linear operators $\delta + \frac{3\sqrt{3}x+I}{\sqrt{3}(1+3x^2)}$ and $\delta - \frac{3\sqrt{3}x+I}{\sqrt{3}(1+3x^2)}$, thus the Galois group of f over $\overline{\mathbb{Q}}(x)$ is $N = A(3)$.
Suppose that the Galois group of f over $\mathbb{Q}(x)$ is $G = S(3)$. Thus, if y_1, y_2, y_3 are the roots of f, a basis for $\mathbb{Q}(x)(y_1, y_2, y_3)$ is $\mathcal{B} = \{1, y_1, y_2, y_1y_2, y_1^2, y_2y_1^2\}$. If $z = u_0 + u_1y_1 + u_2y_2 + u_3y_1y_2 + u_4y_1^2 + u_5y_2y_1^2$ is a constant then we have the differential system $\mathcal{S}_2$.

It admits the rational solutions $u_0 = \lambda_1 + \frac{1}{x}\lambda_0$, $u_1 = -\frac{1}{x}\lambda_0$, $u_2 = \frac{1}{x}\lambda_0$, $u_3 = u_4 = 0$ and $u_5 = -\frac{1}{x(1+3x^2)}\lambda_0$. The Puiseux expansions for f at $x = 1$ at the order 5 are:

$$Z + \left(-\tfrac{2}{3} + \tfrac{5}{6}Z + \tfrac{1}{12}Z^2\right)(x-1) + \tfrac{1}{12}Z(x-1)^2 + \tfrac{1}{54}\left(-1 - \tfrac{13}{4}Z + \tfrac{1}{8}Z^2\right)(x-1)^3 + \tfrac{1}{36}\left(1 + \tfrac{17}{12}Z - \tfrac{1}{8}Z^2\right)(x-1)^4 + \left(-\tfrac{19}{648} - \tfrac{29}{1296}Z^2 + \tfrac{19}{5184}Z\right)(x-1)^5$$

where Z satisfies $Z^3 - 12Z + 8 = 0$. We take two Puiseux expansions y_1 and y_2 corresponding to different solutions Z_1 and Z_2 of $Z^3 - 12Z + 8 = 0$ and by expanding (for $\lambda_0 = 1$) the constant $z = \frac{1}{x} - \frac{1}{x}y_1 + \frac{1}{x}y_2 - \frac{1}{x+3x^3}y_2y_1^2$ at $x = 1$, we find that $z = -3 - \frac{5}{32}(x-1)^5 + O(x-1)^5$. This contradicts the fact that $\mathcal{B}$ is a basis over $\mathbb{Q}(x)$; so the Galois group of f over $\mathbb{Q}(x)$ is $N = A(3)$. ◇

4. CONCLUSION

?????????????

$$
\mathcal{S}_1 \ : \ \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{bmatrix}' = \begin{pmatrix} 0 & \frac{-4}{3(x-1)^2} & \frac{2}{3(x-1)^2} & \frac{-4(x+1)}{3(x-1)^3} & \frac{8(x+1)}{3(x-1)^3} & 0 \\ 0 & \frac{x+1}{3x(x-1)} & 0 & \frac{-4}{3(x-1)^2} & \frac{4}{3(x-1)^2} & \frac{-4(x+1)}{3(x-1)^3} \\ 0 & 0 & \frac{x+1}{3x(x-1)} & \frac{-4}{3(x-1)^2} & 0 & \frac{4(x+1)}{3(x-1)^3} \\ 0 & 0 & \frac{-1}{6x} & \frac{2(x+1)}{3x(x-1)} & 0 & \frac{-2}{3(x-1)^2} \\ 0 & \frac{1}{6x} & \frac{-1}{6x} & 0 & \frac{2(x+1)}{3x(x-1)} & \frac{-4}{3(x-1)^2} \\ 0 & 0 & 0 & 0 & 0 & \frac{x+1}{x(x-1)} \end{pmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{bmatrix}
$$

$$
\mathcal{S}_2 \ : \ \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{bmatrix}' = \begin{pmatrix} 0 & \frac{2}{3x} & -\frac{1}{3x} & -\frac{2}{3x} & \frac{4}{3x} & 0 \\ 0 & -\frac{1+9x^2}{3x(1+3x^2)} & 0 & \frac{2}{3x} & -\frac{2}{3x} & -\frac{2}{3x} \\ 0 & 0 & -\frac{1+9x^2}{3x(1+3x^2)} & \frac{2}{3x} & 0 & \frac{2}{3x} \\ 0 & 0 & \frac{1}{3x(1+3x^2)} & -\frac{2(1+9x^2)}{3x(1+3x^2)} & 0 & \frac{1}{3x} \\ 0 & -\frac{1}{3x(1+3x^2)} & \frac{1}{3x(1+3x^2)} & 0 & -\frac{2(1+9x^2)}{3x(1+3x^2)} & \frac{2}{3x} \\ 0 & 0 & 0 & 0 & 0 & -\frac{1+9x^2}{3x(1+3x^2)} \end{pmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{bmatrix}
$$

5. ACKNOWLEDGMENTS

We thank Frédéric Lehobey for fruitful conversations during the preparation of this paper. Most computations were realized with the computer algebra systems Gap, Magma, or Maple and using the packages ISOLDE and BERNINA[3] on the machines of the French CNRS-UMS Medicis.

6. REFERENCES

[1] S. A. Abramov. Rational solutions of linear differential and difference equations with polynomial coefficients. *USSR Comput. Math. and Math. Phys.*, 29(11):1611–1620, 1989.

[2] M. Barkatou. On rational solutions of systems of linear differential equations. *J. Symb. Comp.*, 28(4-5):547–567, 1999.

[3] M. Bronstein. Solutions of linear differential equations in their coefficient field. *J. Symb. Comp.*, 13(4):413–439, 1992.

[4] G. Butler and J. McKay. The transitive groups of degree up to 11. *Comm. Algebra*, 11(8):863–911, 1983.

[5] B. Huppert. *Endliche Gruppen I.* Springer-Verlag, Berlin-New York, 1967.

[6] A. Magid. *Lectures on Differential Galois Theory.* University Lecture Series, 7 - American Mathematical Society, 1994.

[7] G. Malle and H. Matzat. *Inverse Galois Theory.* Springer Monographs in Mathematics, Berlin, 1999.

[8] J. F. Ritt. *Differential algebra.* Dover Publications, Inc., New York, 1966.

[9] L. Schmiedt-Thieme. Lineare differentialoperatoren mit endlicher galoisgruppe. *IZWR preprint*, 99-25, Universität Heidelberg, 1999.

[10] M. F. Singer. Algebraic solutions of n-th order linear differential equations. In *Proceedings of the 1979 Queens Conference on Number Theory*, pages 379–420. Queen's Papers in Pure and Appl. Math., 54, 1979.

[3] http://www-sop.inria.fr/safir/WHOSWHO/Manuel.Bronstein

[11] M. F. Singer. An outline of differential galois theory. In *Computer Algebra and Differential Equations*, pages 3–57. Edited by E. Tournier, Academic Press, London-New York, 1990.

[12] M. F. Singer. Testing reducibility of linear differential operators: a group theoretic perspective. *Appl. Alg. in Eng. Comm. and Comp.*, 7(2):77–104, 1996.

[13] M. F. Singer and F. Ulmer. Galois groups for second and third order linear differential equations. *J. Symb. Comp.*, 16(1):1–36, 1993.

[14] F. Ulmer. On liouvillian solutions of linear differential equations. *Appl. Alg. in Eng. Comm. and Comp.*, 2(3):171–193, 1992.

[15] M. van Hoeij. Factorization of differential operators with rational functions coefficients. *J. Symb. Comp.*, 24(5):537–561, 1997.