J. Symbolic Computation (2002) **34**, 355–398
doi:10.1006/jsco.2002.0564
Available online at http://www.idealibrary.com on IDEAL®

Linear Differential Operators for Polynomial Equations*

OLIVIER CORMIER[†¶§§], MICHAEL F. SINGER[‡‖¶¶],
BARRY M. TRAGER[§**] AND FELIX ULMER[††]

[†]*IRMAR, Université de Rennes 1, F-35042 Rennes Cedex, France*
[‡]*Department of Mathematics, Box 8205, NC State University, Raleigh, NC 27695-8205, U.S.A.*
[§]*IBM TJ Watson Research Ctr., PO Box 218, Yorktown Heights, NY 10598, U.S.A.*

Given a squarefree polynomial $P \in k_0[x, y]$, k_0 a number field, we construct a linear differential operator that allows one to calculate the genus of the complex curve defined by $P = 0$ (when P is absolutely irreducible), the absolute factorization of P over the algebraic closure of k_0, and calculate information concerning the Galois group of P over $\overline{k_0}(x)$ as well as over $k_0(x)$.

1. Introduction

The results of this paper spring from the elementary fact that an algebraic function satisfies a linear differential equation.

Let k_0 be a number field and $\overline{k_0}$ be its algebraic closure. Let $P \in k_0(x)[y]$ be a squarefree polynomial of degree n in y. The derivation $\delta = \frac{d}{dx}$ extends uniquely to the algebraic closure $\overline{k_0(x)}$ of $k_0(x)$. We define the *minimal operator associated with* P to be the monic differential operator $L_P = \delta^t + a_{t-1}\delta^{t-1} + \cdots + a_0$ with $a_i \in k_0(x)$ of smallest positive order such that $L_P(y) = 0$ for all roots of P in $\overline{k_0(x)}$. In Section 2, we give algorithms to calculate this operator. In Section 3, we assume that P is absolutely irreducible, that is, irreducible over $\overline{k_0}(x)$. We show that information derived from the singular points of the minimal operator allows one to give a simple formula (and direct method) to calculate the genus of $P = 0$. In Section 4 we give two methods to factor a polynomial $P \in k_0(x)[y]$ over $\overline{k_0}(x)$. Together with the algorithm in Section 3, this yields a new polynomial time algorithm for this task. In Section 5, we discuss how the minimal operator allows us to find properties of the Galois groups of P over $k_0(x)$ and over $\overline{k_0}(x)$. In the appendix we

*Some of these results were presented in a preliminary form at the Computational Aspects of Commutative Algebra and Algebraic Geometry Conference in Dagstuhl (1997), at the International Symposium on Symbolic and Algebraic Computation (ISSAC 2000) in St Andrews, Scotland (Cormier *et al.*, 2000) and at the Differential Galois Theory Workshop in Bedlewo, Poland (2001).

[¶]E-mail: ocormier@maths.univ-rennes1.fr
[‖]E-mail: singer@math.ncsu.edu
[**]E-mail: bmt@us.ibm.com
[††]E-mail: ulmer@univ-rennes1.fr
[§§]Moved to MuPAD Gruppe, Universität Paderborn
[¶¶]Corresponding author. E-mail: singer@msri.org

0747–7171/02/050355 + 44 $35.00/0

present some conjectures related to a problem that is solved in Section 2, that is, the problem of finding a simple Tschirnhaus transformation that will ensure that the roots of a polynomial over $k_0(x)$ become linearly independent over k_0.

Although other methods are known to perform these tasks, our goal is to show that one can approach all of these via differential operators. We note that differential operators have been used to derive power and Puiseux series expansions of algebraic functions in Comtet (1964) and Chudnovsky and Chudnovsky (1986, 1987) and, in a way different from that described here, absolute factorization in Gao (2001). For simplicity, we have assumed k_0 to be a number field but all results are valid for a computable field of characteristic zero over which one has an algorithm to factor polynomials.

2. From Polynomials to Linear Differential Equations

In this section we shall assume that $P \in k_0(x)[y]$ is a squarefree polynomial of degree n and discuss methods to calculate the minimal operator L_P associated with P.

We begin by describing the well known naive algorithm to do this. This algorithm is motivated by the fact that if $\tilde{y}$ is a root of P in some differential extension of $k_0(x)$, then $\delta(\tilde{y}) = -\frac{P_x(\tilde{y})}{P_y(\tilde{y})}$ (where P_x and P_y are the partial derivatives of P with respect to x and y) and this latter expression can be rewritten as a polynomial in $\tilde{y}$. Since P and P_y are relatively prime, the Euclidean algorithm can be used to find polynomials R and S of degrees at most $n-1$ such that $RP + SP_y = -P_x$. We now generate a sequence of polynomials $S_i \in k_0(x)[y]$ of degree at most $n-1$ such that for any root $\tilde{y}$ of P, $\delta^i(\tilde{y}) = S_i(\tilde{y})$. We define $S_0 = y$, $S_1 = S$, and, for $i > 1$, S_{i+1} to be $(S_i)_x + (S_i)yS_1 \bmod P$. At each stage, one checks to see if the polynomials $S_0, \ldots, S_i$ are linearly dependent over $k_0(x)$. If so, then a relation $\sum_{j=0}^{i} a_j S_j = 0$, $a_i = 1$ yields an operator $L = \sum_{j=0}^{i} a_j \delta^j$. If not, one continues. This process must stop after at most n steps, since $n+1$ polynomials of degree at most $n-1$ must be linearly dependent. It remains to justify that this process does yield an operator of minimal order that annihilates the roots of P.

Formally, the process above produces a linear differential operator L of smallest order that annihilates the image $\overline{y}$ of y in the differential ring $k_0(x)[y]/(P)$ where the derivation is defined by $\overline{y}' = -P_x(\overline{y})/P_y(\overline{y})$. Furthermore, if $P = P_1 \cdot \ldots \cdot P_r$ is the factorization of P into irreducible factors over $k_0(x)$, then the map

$$k_0(x)[y]/(P) \to k_0(x)[y]/(P_1) \oplus \cdots \oplus k_0(x)[y]/(P_r) \tag{1}$$

given by $\overline{y} \to (y \bmod P_1, \ldots, y \bmod P_r)$ is not only an isomorphism but a differential isomorphism as well.

To show that L as constructed above is the minimal operator associated with P, we will show that the solution space of L is spanned by the roots of P. The roots of P span a vector space V that is precisely the solution space of a monic operator L_P with coefficients in $k_0(x)$. To see this, let $y_1, \ldots, y_t$ be a basis of V. The Galois group of P acts as $t \times t$ matrices on V and leaves the coefficients of

$$L_P(y) = \frac{\det(Wr(Y, y_1, \ldots, y_t))}{\det(Wr(y_1, \ldots, y_t))}$$

fixed ($Wr(\cdots)$ is the Wronskian matrix). We need to show $L_P = L$. First of all, since all roots of P satisfy $L(y) = 0$, we have that L_P divides L on the right (see Lemma 2.1 of Singer (1996)). Since L_P annihilates each of the $y \bmod P_i$ in (1), the isomorphism in (1) allow us to conclude that L_P annihilates $\overline{y}$. This implies that L divides L_P on

the right. Therefore $L = L_P$. We note that we have also shown that the solution space of the minimal operator is spanned by the roots of P.

The above procedure involves "only" linear algebra but one can encounter problems of expression-swell when trying to carry this out. We will present an alternative algorithm that first bounds the degrees of the numerators and denominators of the coefficients of the minimal operator and then calculates these directly using Padé approximation. This method will work well when the roots of P are linearly independent over $\overline{k_0}$. For this reason and later use, we begin by discussing this condition.

2.1. LINEAR INDEPENDENCE OF ROOTS

In this section, we present a method for transforming a polynomial $P(y) \in k_0(x)[y]$ into a new polynomial whose roots are linearly independent over the constants. In the appendix, we will discuss other possible methods to perform this task.

There are well known efficient algorithms to give a squarefree decomposition of an arbitrary polynomial so questions of factoring and calculating Galois groups can be reduced to considering squarefree polynomials. Furthermore, given a polynomial $P(y)$, it is easy to write it as a product $P(y) = P_1(y)P_2(y)$ where $P_1(y) \in k_0[y]$ and $P_2(y) \in k_0(x)[y]$ with no root of P_2 in $\bar{k}_0$. To do this, multiply by a polynomial $b(x) \in k_0[x]$ to clear denominators so $P_0 = b(x)P \in k_0[x, y]$. Rewrite P_0 as a polynomial in x with coefficients in $k_0[y]$ and let $P_1(y)$ be the greatest common divisor of the coefficients of powers of x. Dividing again by $b(x)$, we have that $P = P_1P_2$ for some $P_2 \in k_0(x)[y]$ having no roots in $\bar{k}_0$. These two observations allow us to reduce questions of factorization, computing genera and computing Galois groups to squarefree polynomials, none of whose roots are constants. For these polynomials, we have the following result (due to Bjorn Poonen).

PROPOSITION 2.1. *Let $P \in k_0(x)[y]$ be a squarefree polynomial none of whose roots $\{y_1, \ldots, y_n\} \subset \overline{k_0(x)}$ lie in $\bar{k}_0$. Except for a set of at most n^2 values of $a \in k_0$, the elements*

$$\frac{1}{y_1 - a}, \ldots, \frac{1}{y_n - a}$$

are linearly independent over $\bar{k}_0$.

PROOF. Let $K = \bar{k}_0(x, y_1, \ldots, y_n) \subset \overline{k_0(x)}$ and let c be an indeterminate. The derivation $\frac{d}{dx}$ on $k_0(x)$ extends naturally to $\overline{k_0(x)}$ and the constant subfield of this latter field is $\bar{k}_0$. For an indeterminate c, the field $\bar{k}_0(x, c)$ can be given the structure of a differential field with $\frac{dc}{dx} = 0$. The constant subfield to this latter field is then $\bar{k}_0(c)$. We shall show that the elements

$$\frac{1}{y_1 - c}, \ldots, \frac{1}{y_n - c} \tag{2}$$

are linearly independent over $\bar{k}_0(c)$. Assume that there are $q_1(c), \ldots, q_n(c) \in \bar{k}_0(c)$ such that

$$\frac{q_1(c)}{y_1 - c} + \cdots + \frac{q_n(c)}{y_n - c} = 0.$$

If we consider the left-hand side of this equality as an element of $K(c)$, we can expand this in partial fractions with respect to the indeterminate c. The coefficient of the term $\frac{1}{y_i - c}$ will then be $q_i(y_i)$, which, by assumption, cannot be zero unless q_i is identically zero. Therefore, the elements in (2) are linearly independent over $\bar{k}_0(c)$.

From the above, we can conclude that the Wronskian of the elements of (2) is nonzero. Considering this as an element of $K(c)$, we may assume that the denominator is $\prod_i (y_i - c)^n$ and that the numerator is a nonzero polynomial of degree at most n^2 in c. Therefore there are at most n^2 values of $a \in k_0$ such that the elements

$$\frac{1}{y_1 - a}, \ldots, \frac{1}{y_n - a}$$

are linearly independent over k_0 and therefore over $\bar{k}_0$. □

We note that the proof gives us a polynomial $W(c) \in K[c]$ whose zeros include the exceptional set of values of c. From the point of view of efficiency this is not very helpful. Instead we shall give a test to determine directly if the roots of a squarefree polynomial are linearly independent over the constants. Having such a test, one selects a value of a and constructs a polynomial for which the $\frac{1}{y_i + a}$ are roots (just multiply $P(\frac{1}{y} - a)$ by sufficiently high power of y). One then applies the test and the proposition guarantees success after at most $n^2 + 1$ choices.

The idea behind the test to determine linear dependence of roots of a polynomial $P \in k_0(x)[y]$ is the following: there is a number M, depending on P, such that if a $\bar{k}_0$-linear combination of roots of P vanishes to order M, then this linear combination must be identically zero. Therefore, to test if the roots of P are linearly dependent, we need only expand the roots as Taylor series at a point $x_0 \in k_0$ where the discriminant is nonzero and test if the first $M + 1$ terms are linearly dependent. Doing this naively will involve working in an algebraic extension of k_0 but we shall also show how this blemish may be removed to allow us to work directly in k_0.

To show that the bound M exists and to show how one may calculate it, we will need some well known concepts and facts concerning linear operators over $\overline{k_0}(x)$ (see Poole, 1960, Chapter 5). We begin by reviewing these.

Let $L = b_n\delta^n + b_{n-1}\delta^{n-1} + \cdots + b_0$ be a linear differential operator with $\delta = \frac{d}{dx}$ and the $b_i \in \overline{k_0}[x]$ and GCD $(b_0, \ldots, b_n) = 1$. At any point $c \in \overline{k_0}$ one can search for solutions of $y = 0$ of the form $y = t^\rho \sum_{j \geq 0} c_j t^j$ where $\rho \in \overline{k_0}$ and $t = x - c$. If we let $b_i = \sum_{j > m} b_{i,j} c^j$, $\delta_{i,m_j} \neq 0$ and substitute the expression for y into Ly we get $Ly = I(\rho) x^{\rho+N} (\sum_{j \geq 0} d_j t^j)$ where $N = \min_i(m_i - i)$, $d_0 \neq 0$ and $I(\rho) = \sum_{\{i | m_i - i = N\}} b_i, m_i \rho^{\underline{i}}$ (we use the notation $\rho^{\underline{i}} = 1$ if $i = 0$ and $\rho^{\underline{i}} = \rho(\rho - 1) \cdots (\rho - i + 1)$ otherwise). The equation $I(\rho) = 0$ is called the *indicial equation* at c and its roots are called the *exponents at c*. A calculation also shows that if $y = \sum_{i=0}^{\infty} c_i t^{\rho_i}$ with $\rho_0 < \rho_1 < \cdots$ real numbers and $c_0 \neq 0$ then ρ_0 is also an exponent. If c is not a root of b_n, we say that c is an *ordinary point* and the values of c such that $b_n(c) = 0$ are called the (finite) *singular points*. We also need to classify the point at infinity. To do this we make the transformation $x = \frac{1}{t}$, $\frac{d}{dx} = -t^2 \frac{d}{dt}$ and say that ∞ is ordinary or singular according to whether 0 is an ordinary or singular point of the transformed equation. The indicial equation at ∞ is defined to be the indicial equation of the transformed equation at 0. If L has coefficients in $k_0(x)$, then the indicial equations at points of $\overline{k_0}$ that are conjugate over k_0 are the same and one can calculate this equation using p-adic expansions where p is the minimal polynomial of the conjugate singular points over k_0. These can be found from a factorization of b_n. We say a singular point is *regular* if its indicial equation has degree n and is *irregular* if its indicial equation has degree less than n. Therefore a singular point c is regular if and only if the order of b_{n-i}/b_n at c is at least $-i$. We say L is *Fuchsian* if all of its singular points are

regular singular points. Let L be a Fuchsian operator, let $p_1, \ldots, p_m$ be the singular points (possibly including infinity) and for each i, let $\{\rho_{i,j}\}_{j=0}^{n-1}$ be the exponents at p_i. Fuchs's relation states that

$$\sum_{i=1}^{m} \sum_{j=0}^{n-1} \rho_{i,j} = \frac{1}{2}(m-2)n(n-1). \tag{3}$$

This equation is proved in Poole (1960, p. 77). Finally, we say that a singularity c is an *apparent singularity* if the equation $Ly = 0$ has n independent solutions that are analytic at $x = c$.

We shall need the following facts about exponents.

LEMMA 2.2. *Let L be as above and $p \in \overline{k}_0 \cup \{\infty\}$.*

1. *If p is an ordinary point, then the exponents at p are $\{0, \ldots, n-1\}$.*
2. *If all solutions of $Ly = 0$ at p can be expressed as Puiseux series, then there are n distinct exponents at p.*
3. *If p is an apparent singularity then there are n distinct integer exponents $0 \leq \rho_1 < \cdots < \rho_n$ at p with $\rho_n \geq n$.*

PROOF.

1. This claim follows from the existence theorem for differential equations.
2. For simplicity, let us assume that $p = 0$. Let $\{y_1, \ldots, y_n\}$ be a basis of the solution space at p and assume we have ordered this set so that $\mathrm{ord}_p y_1 \leq \cdots \leq \mathrm{ord}_p y_n$, where $\mathrm{ord}_p y$ is the exponent of the smallest power of x appearing in y. Since each of these numbers must be an exponent, there are only a finite number of n-tuples $(\mathrm{ord}_p y_1, \ldots, \mathrm{ord}_p y_n)$ that can be generated in this way. Order these lexicographically and select the largest such n-tuple. We claim that the entries are all distinct. If not, say $\mathrm{ord}_p y_i = \mathrm{ord}_p y_{i+1}$. For some $c \in \overline{k}_0$, $\overline{y}_{i+1} = y_i - c y_{i+1}$ has order larger than $\mathrm{ord}_p y_{i+1}$. Replacing y_{i+1} with $\overline{y}_{i+1}$ we get a new basis with a larger associated n-tuple of orders, a contradiction.
3. Again, assume that $p = 0$. From part 2 and the definition of an apparent singular point, there will be n distinct positive integer exponents. We must show that the set of exponents is not $\{0, 1, \ldots, n-1\}$. Assume that this latter set is the set of exponents and let $\{y_1, \ldots, y_n\}$ be a set of solutions of $Ly = 0$ with $\mathrm{ord}_0 y_i = i$. If $w(x) = Wr(y_1, \ldots, y_n)$ is the Wronskian matrix $(y_i^{(j)}(x))$ then one sees that $w(0)$ is a lower triangular matrix none of whose diagonal entries is zero. In particular, $\det(w(x))$ is nonzero at $x = 0$ and the y_i are linearly independent over the constants. The equation
$$\tilde{L}(y) = \frac{\det(Wr(y, y_1, \ldots, y_n))}{\det(Wr(y_1, \ldots, y_n))}$$
has rational coefficients that do not vanish at p. Clearing denominators gives us L and shows that p is not a singular point, yielding a contradiction. □

We now consider the minimal operator L_P of order $q \leq n$ of a squarefree $P(y) \in k[y]$, $k = k_0(x)$ of degree n. At any point, the solutions of $P(y) = 0$ can be expressed as Puiseux series and so the minimal operator will have a basis of solutions of this form. Therefore, Lemma 2.2 applies to this operator.

Using these concepts, we wish to prove the following proposition.

PROPOSITION 2.3. *Let $P \in k_0[x,y]$ be a squarefree polynomial of degree n in y and let $y_1, \ldots, y_n$ be the roots of $P = 0$ in $\overline{k_0(x)}$. Let L_P be the minimal operator of P and let its order be q, $1 \leq q \leq n$. Let*

$$M = q + q\left(\frac{1}{2}(N-2)(q-1) - Nl\right)$$

where

1. *N is the number of points x_0 (possibly including infinity) where either the degree of $P(x_0, y)$ is less than n or $P(x_0, y) = 0$ has a multiple root,*
2. *$l \leq 0$ is a lower bound on the slopes of the sides of the Newton polygon of P at any point on the projective line.*

Then M is an upper bound on the exponents of L_P at any point on the projective line. Furthermore, the number of apparent singularities is bounded by $q\left(\frac{1}{2}(N-2)(q-1) - Nl\right)$.

PROOF. Let $p_1, \ldots, p_m$ be the singular points of L_P (possibly including infinity) and let $p_1, \ldots, p_N$ be the points where $P(p_i, y) = 0$ has a repeated root or the degree drops. Note that $p_{N+1}, \ldots, p_m$ are apparent singularities of L_P.

At each p_i, $1 \leq i \leq N$, the exponents are of the form $\rho_{i,j} = l + n_{i,j}$ where $n_{i,j}$ is a non-negative rational number. This is because at these points the Puiseux expansions of the solutions $\{y_j\}$ have leading terms whose exponents are given by the slopes of the Newton polygon.

At each p_i, $N+1 \leq i \leq m$, the exponents are distinct non-negative integers with the largest one bigger than $q-1$. Therefore, we may assume that they are of the form $\rho_{i,j} = j + n_{i,j}$ with each $n_{i,j}$ a non-negative integer and at least one $n_{i,j}$ positive.

From Fuchs's relation (equation (3)) we have

$$\begin{aligned}
\frac{1}{2}(m-2)q(q-1) &= \sum_{i=1}^{N}\sum_{j=0}^{q-1}\rho_{i,j} + \sum_{i=N+1}^{m}\sum_{j=0}^{q-1}\rho_{i,j} \\
&= \sum_{i=1}^{N}\sum_{j=0}^{q-1}(l + n_{i,j}) + \sum_{i=N+1}^{m}\sum_{j=0}^{q-1}(j + n_{i,j}) \\
&= Nql + \left(\sum_{i=1}^{N}\sum_{j=0}^{q-1} n_{i,j}\right) + \frac{m-N}{2}q(q-1) + \sum_{i=N+1}^{m}\sum_{j=0}^{q-1} n_{i,j}.
\end{aligned}$$

Rewriting this, we have that

$$\frac{1}{2}(N-2)q(q-1) - Nql = \sum_{i=1}^{N}\sum_{j=0}^{q-1} n_{i,j} + \sum_{i=N+1}^{m}\sum_{j=0}^{q-1} n_{i,j}. \tag{4}$$

Note that $\sum_{i=N+1}^{m}\sum_{j=0}^{q-1} n_{i,j}$ is larger than the number of apparent singularities since for each j some $n_{i,j}$ is positive. Therefore the number of apparent singularities is at most $\frac{1}{2}(N-2)q(q-1) - Nql$.

We also have that each $n_{i,j} \leq \frac{1}{2}(N-2)q(q-1) - Nql$. Since $l \leq 0$, $\rho_{i,j} \leq \frac{1}{2}(N-2)q(q-1) - Nql$ at each true singularity and $\rho_{i,j} \leq q + \frac{1}{2}(N-2)q(q-1) - Nql$ at each apparent singularity. Note that at an ordinary point we have that the exponents are less than q and so also satisfy this bound. □

We note that if at some point on the projective line, the Newton polygon has n distinct slopes then these slopes are precisely the exponents of L_P and L_P will have order n, i.e. the roots of P will be linearly independent over constants. If there are fewer than n slopes then the exponents can be larger than the slopes due to cancellation among the roots of P. Furthermore, if we know the exponents at the true singular points, then we can give a better bound on the number of apparent singular points than the one given in the above proposition. Using the notation of the proof of Proposition 2.3, we have

$$\frac{1}{2}(N-2)q(q-1) - \sum_{i=1}^{N}\sum_{j=0}^{q-1}\rho_{i,j} = \sum_{i=N+1}^{m}\sum_{j=0}^{q-1}n_{i,j} \geq m - N. \tag{5}$$

We note that both l and N can be bounded in terms of the total degree d of P in x and y and that this bound is a polynomial in d.

To decide linear dependence of the roots we will use the following corollary.

Corollary 2.4. *Let $P \in k_0[x,y]$ be a squarefree polynomial of degree n in y and let $y_1, \ldots, y_n$ be the roots of $P = 0$ in $\overline{k_0(x)}$. Let*

$$M' = \max_{1 \leq q \leq n}\left\{q + q\left(\frac{1}{2}(N-2)(q-1) - Nl\right)\right\}.$$

Let $t = x - a$ for $a \in \overline{k}_0$ or $t = \frac{1}{x}$, let $c_1, \ldots, c_n \in \overline{k}_0$ and let

$$\sum_{\rho_0 < \rho_1 < \cdots} a_i t^{\rho_i}$$

be the expansion of $c_1y_1 + \cdots + c_ny_n$ in fractional powers of t. If $\rho_0 > M'$, then $c_1y_1 + \cdots + c_ny_n = 0$.

Proof. Note that the number M' bounds the exponents at any point of the minimal operator of P. Any linear combination as above must be a solution of this operator. If it vanishes to an order larger than any exponent then it must be identically zero. □

To apply the above corollary, we will want to expand the roots of P at a point $x = c$ and compare the first few terms. To minimize working over an algebraic extension of k_0, we shall introduce the following series.

Let $x = c$ be a point where the discriminant of P, $\text{Resultant}_y(P, \frac{dP}{dy})$, is not zero. For simplicity, we shall assume that $c = 0$. Let $S = k_0[y]/(P(0,y))$ and let α be the image of y in S. Since $P(0,y)$ is squarefree, $\frac{dP}{dy}(0,\alpha)$ is invertible in S. One can apply Newton's Method (see Lemma 9.2.1 of von zur Gathen and Gerhard, 1999, p. 253) and conclude that there exist $s_i \in k_0[[x]]$ such that $y(x) = s_1 + \alpha s_2 + \cdots + \alpha^{n-1}s_n$ is a solution of $P(x,y) = 0$ in $S[[x]]$. Note that Newton's Method allows one to calculate the s_i to any prescribed power of x. Furthermore, specializing α to any root α_i of $P(0,y)$ in the algebraic closure $\overline{k}_0$ of k_0 yields a solution $y_i(x) = s_1 + \alpha_i s_2 + \cdots + \alpha_i^{n-1}s_n$ of $P(x,y)$ in $\overline{k}_0[[x]]$. Note that $\{y_1, \ldots, y_n\}$ are linearly independent over constants if and only if the

same is true for $\{s_1, \ldots, s_n\}$ since the transformation matrix from one set to the other is a Vandermonde matrix.

DEFINITION 2.5. We shall refer to the s_i constructed as above as an *adapted spanning set* of the solution space of $L_P y = 0$ at $x = c$. If they are linearly independent over the constants then we shall refer to this set as an *adapted basis* of the solution space of $L_P y = 0$ at $x = c$.

Using an adapted spanning set at a point where the discriminant of P is nonzero, we can give a procedure to decide if the roots of $P = 0$ are linearly independent over the constants. Let M' be the number defined in Corollary 2.4. Calculate polynomials $S_i(x)$ such that $s_i(x) = S_i(x) + O(x^{M''+1})$ where M'' is the first integer at least as large as M'. Corollary 2.4 implies that the s_i are linearly independent over constants if and only if the S_i are and this can be decided using linear algebra over k_0. We note that the method presented here for finding an element $c \in k_0$ such that $P\big(c + \frac{1}{y}\big) = 0$ has $\overline{k}_0$-linearly independent roots has complexity given by a polynomial in the total degree of P and the size of the numbers appearing in P (bit size if $k_0 = \mathbf{Q}$ and a similar measure for algebraic numbers).

We illustrate the method with the following example.

EXAMPLE 2.6. Consider the polynomial $P(x, y) = y^2(y^2 + 3)^2 + 4x$ (from Malle and Matzat, 1999, p. 404, $f_{6,3}$). In order to find a transformation such that the roots of the new polynomial are independent over $\overline{\mathbf{Q}}$ we proceed in the following way:

- Consider $P_0 = y^6 P(x, \frac{1}{y})$. Since the coefficient of y^5 is zero, the roots must be linearly dependent. In order to prove the linear dependence using the above we would proceed as follows. Using the notation of Corollary 2.4, we get $N = 3$ (corresponding to $x = 0, 1, \infty$). We choose to work at the regular point $c = 2$ and consider the polynomial
$$\tilde{P}_0 = P_0(x - 2, y) = 1 + 6y^2 + 9y^4 + 4(x - 2)y^6.$$
By computing the Newton polygon of $\tilde{P}_0$ we get $l = -\frac{1}{6}$ and so $M' = 24$. Computing an adapted spanning set up to order $M'+1$ we get that the S_i are linearly dependent over $\mathbf{Q}$ and thus by Corollary 2.4 we get that the roots are linearly dependent over $\overline{\mathbf{Q}}$.
- Now we consider the polynomial $P_1 = y^6 P(x, \frac{1}{y} + 1)$. Following the notation of Corollary 2.4, we get $N = 4$ (corresponding to $x = 0, 1, -4, \infty$). We choose to work at the regular point $c = 2$ and consider the polynomial
$$\tilde{P}_1 = P_1(x - 2, y) = 4(2 + x)y^6 + 48y^5 + 60y^4 + 44y^3 + 21y^2 + 6y + 1.$$
By computing the Newton polygon of $\tilde{P}_1$ we get $l = -\frac{1}{6}$ and so $M' = 40$, which means that in order to guarantee a possible linear dependence of the coefficients S_i of a spanning set we have to compute until order 41. Note that in this case an adapted spanning set computed up to order 6 is
$$\left(-\frac{1}{486}x^3 - \frac{35}{46656}x^4 - \frac{1069}{1679616}x^5 + O(x^6)\right)\alpha^5$$
$$+\left(\frac{1}{9}x + \frac{5}{216}x^2 - \frac{25}{23328}x^3 - \frac{295}{124416}x^4 - \frac{81289}{40310784}x^5 + O(x^6)\right)\alpha^4$$

$$+\left(\frac{5}{9}x+\frac{5}{36}x^2-\frac{817}{23328}x^3+\frac{5525}{559872}x^4+\frac{102061}{40310784}x^5+O(x^6)\right)\alpha^3$$
$$+\left(\frac{7}{18}x+\frac{19}{216}x^2+\frac{977}{46656}x^3+\frac{229}{41472}x^4+\frac{106337}{80621568}x^5+O(x^6)\right)\alpha^2$$
$$+\left(1+\frac{7}{36}x+\frac{37}{864}x^2+\frac{1007}{93312}x^3+\frac{13753}{4478976}x^4+\frac{141923}{161243136}x^5+O(x^6)\right)\alpha$$
$$+\left(\frac{1}{36}x+\frac{5}{864}x^2+\frac{125}{93312}x^3+\frac{515}{1492992}x^4+\frac{13313}{161243136}x^5+O(x^6)\right)$$

where $\tilde{P}_1(0,\alpha)=0$. Since the corresponding S_i are linear independent over $\mathbf{Q}$, the roots of $\tilde{P}_1$ are independent over $\overline{\mathbf{Q}}$. This ensures that $L_{\tilde{P}_1}$ (and thus L_{P_1}) has maximal order 6 (see Example 2.7 for its computation). □

2.2. CALCULATING THE MINIMAL OPERATOR

We now turn to the problem of finding the minimal operator associated with a polynomial $P(y)$ whose roots are linearly independent over $\overline{k_0}$. The previous paragraphs have shown how one can ensure that this happens. Clearing denominators, we shall furthermore assume that $P(x,y)\in k_0[x,y]$ and for simplicity that P is monic as a polynomial in y (this can always be achieved by making a linear transformation of the variables). Since the minimal differential operator is Fuchsian, it will be of the form

$$L_P=\delta^n+\frac{a_{n-1}(x)}{A(x)}\delta^{n-1}+\cdots+\frac{a_0(x)}{A(x)^n}$$

where $A(x)$ is a squarefree polynomial (Poole, 1960, Chapter V.20). We can write $A(x)=A_1(x)A_2(x)$ where the zeros of $A_1(x)$ are the finite "true" singular points and the zeros of $A_2(x)$ are the apparent singular points. We can let $A_1(x)$ be the product of the irreducible factors of the discriminant since outside the zeros of this polynomial we have n analytic solutions of $P=0$. Proposition 2.3 allows us to bound the degree of $A_2(x)$. Since ∞ is at worst a regular singular point we have that $\deg(a_{n-i})\le\deg(A^i)-i$ (Poole, 1960, Chapter V.20). Therefore, once one has a bound on the degree of $A(x)$, one can bound the degree of the a_i. To determine the a_{n-i}/A^i, we proceed as follows.

Let $x=c$ be a point that is not the zero of the discriminant of P and let $\{s_i\}$ be an adapted basis of L_P at $x=c$. We note that

$$L_P(y)=\frac{\det(Wr(y,s_1,\ldots,s_n))}{\det(Wr(s_1,\ldots,s_n))}$$

where Wr is Wronskian matrix. Therefore, each coefficient a_{n-i}/A^i is the ratio of power series that we can compute. Since $N_i=i\deg(A)$ is a bound on the degrees of the numerator and denominator of a_{n-i}/A^i, we can determine this rational function from the first $2N_i+1$ coefficients of the corresponding ratio of power series.

The following example shows that one can sometimes do better than using the rough bounds of Proposition 2.3. In this example there are n distinct slopes at some of the singular points and so we know that the Puiseux series must be linearly independent over the constants. Furthermore, these slopes must be the exponents. We are therefore able to use Fuchs's relation (equation (3)) and its consequence (equation (5)) directly to bound the number of apparent singularities.

Example 2.7. (Example 2.6 Continued) We will compute the differential operator (which is of maximal order) associated to the polynomial $\tilde{P}_1$ of Example 2.6 using the above method.

The singularities of $\tilde{P}_1$ are -2, 2, 3 and ∞. We can give lower bounds on the exponents of $L_{\tilde{P}_1}$ at these points by looking at the Puiseux series of $\tilde{P}_1$. For instance, at $x = 3$ using the command "puiseux" in Maple with the option "minimal" we obtain the following representation using a formal parameter T after translating 3 to 0:

$$\{[x = -1/12T^2, y = -\beta/12T + \cdots], [x = T, y = \alpha + \cdots]\}$$

where $5\alpha^2 + 2\alpha + 1 = 0$ and $2\beta^2 + 2\beta + 1 = 0$. Therefore, since the exponents are all distinct, the sum of exponents at $x = 3$ is at least $0 + \frac{1}{2} + 1 + \frac{3}{2} + 2 + \frac{5}{2} = \frac{15}{2}$. Doing the same with the other singularities, we obtain respectively the lower bounds $\frac{15}{2}$ at $x = 2, 9$ at $x = -4$ and $\frac{7}{2}$ at $x = \infty$. The sum of the exponents at the singularities is therefore at least $\frac{55}{2}$ and equation (5) implies that

$$m - N \leq \frac{1}{2}(4-2)6(5-1) - \frac{55}{2} = \frac{5}{2}$$

and so $L_{\tilde{P}_1}$ admits at most two apparent singularities.

Writing $A(x) = (x-2)(x-3)(x+2)(x^2+ax+b)$, $L_{\tilde{P}_1}$ is of the form

$$L_{\tilde{P}_1} = y^{(6)} + \sum_{i=1}^{6} \frac{a_{6-i}(x)}{A(x)^i}$$

where a_{6-i} is a polynomial of degree at most $4i$. Using the adapted basis at $x = 0$ we have already computed in Example 2.6 and the previous expression of $L_{\tilde{P}_1}$ as a quotient of Wronskian determinants, this leads, when expanding the coefficient $\frac{a_5(x)}{A(x)}$, to a system in the coefficients of a_5 and the variables a and b whose solution gives

$$\frac{a_5(x)}{A(x)} = \frac{444x^4 - 105939x^3 - 325750x^2 + 1112451x + 987286}{2(x-3)(12x^2 - 2697x - 12467)(x^2-4)}$$

so $L_{\tilde{P}_1}$ admits exactly two apparent singularities that are conjugate over $\mathbf{Q}$ (and we can also deduce directly from Fuchs's relation that the exponents at these points are $\{0, 1, 2, 3, 4, 6\}$). The other coefficients can be computed in the same way but we don't reproduce the equation $L_{\tilde{P}_1}$ because of rather huge expressions. □

Note that the algorithm for computing L_P is again of complexity bounded by a polynomial in the total degree of P and the size of the coefficients.

3. A Formula for the Genus of $P = 0$

In this section we will give a formula that gives the genus of an algebraic curve in terms of the exponents of the associated minimal differential operator. Throughout the section $P \in k_0[x, y]$ will denote an absolutely irreducible polynomial of degree n in y. Furthermore, we shall assume that the roots of P in the algebraic closure of $k_0(x)$ are linearly independent over $\overline{k_0}$. If this is not the case, we have shown in Section 2 that we can transform P into a polynomial having this property. It is easy to see that the transformed polynomial is absolutely irreducible if and only if the original one is.

Although there are many ways to define the genus g of the curve $P = 0$ (e.g. the topological genus of the nonsingular model), for the purposes of this paper it will suffice

to define this number to be the integer that satisfies the *Hurwitz formula* given below. In order to state this formula we need to give some well known definitions and facts (see Walker, 1962).

Let K be the quotient field of $\overline{k_0}[x,y]/(P)$ where (P) is the ideal generated in $\overline{k_0}[x,y]$ by P. For each $c \in k_0$, let $t = x - c$ and let $\overline{k_0}((t))$ be the quotient field of the ring of formal power series in t. Expanding any $f \in \overline{k_0}(x\delta)$ as a Laurent series in t gives an embedding of $\overline{k_0}(x) \to \overline{k_0}((t))$. Therefore, we can consider $\overline{k_0}(x)$ as a subfield of $\overline{k_0}((t))$ and there exist n roots $y_1, \ldots, y_n$ of $P = 0$ in the algebraic closure $\overline{k_0((t))}$ of $\overline{k_0}((t))$. It is known that the field $\overline{k_0((t))}$ is the union of all fields of the form $\overline{k_0}((t^{1/m}))$, $m \geq 1$ (Walker, 1962, Chapter IV, Section 3). For each y_i there is a smallest positive integer e such that $y_i \in \overline{k_0}((t^{1/e}))$ which we refer to as the *ramification index* of y_i. The Galois group of $\overline{k_0}((t^{1/e}))$ over $\overline{k_0}((t))$ is cyclic of order e and is generated by $t^{1/e} \longmapsto \zeta t^{1/e}$ where ζ is a primitive eth root of unity. We say two solutions of $P = 0$ are *equivalent* if they have the same ramification e and are conjugate under the Galois group of $\overline{k_0}((t^{1/e}))$ over $\overline{k_0}((t))$. If y_i has ramification e then it is equivalent to e solutions of $P = 0$. Each equivalence class is called a *place*. The elements of each place have a common ramification which we refer to as the *ramification index* of the place. Therefore, to each element $c \in \overline{k_0}$ we can associate the list of ramification indices of the places $e_{1,c}, \ldots, e_{h,c}$. We note that $\sum_i e_{i,c} = n$ and that an integer can appear more than once in this list. Letting $t = \frac{1}{x}$, one can embed $\overline{k_0}(x)$ into $\overline{k_0}((t))$ and define the ramification indices $e_{1,\infty}, \ldots, e_{l,\infty}$ in a similar way. Let $S = \overline{k_0} \cup \{\infty\}$. It is known that there is a smallest finite set $\mathcal{R} \subset S$ such that for $c \notin \mathcal{R}$ all ramification indices at c are 1. We have the *Hurwitz formula*:

$$g = 1 - n + \sum_{\alpha \in S} \sum_i \frac{e_{i,\alpha} - 1}{2}$$

where g is the genus and the sum $\sum_i \frac{e_{i,\alpha}-1}{2}$ is over all ramification indices at α.

We now switch our attention to the minimal operator of P. At each point $\alpha \in S$ there exist n exponents $\rho_{i,\alpha}, \ldots, \rho_{n,\alpha}$. We note that the $\rho_{i,\alpha}$ are distinct rational numbers. For each i let $r_{i,\alpha} \in k_0$ satisfy: $0 \leq r_{i,\alpha} < 1$ and $\rho_{i,\alpha} - r_{i,\alpha}$ is an integer. We shall refer to $r_{i,\alpha}$ as the *fractional part of the exponent* $\rho_{i,\alpha}$. We then have the following proposition.

Proposition 3.1. *Using the above notation*

$$g = 1 - n + \sum_{\alpha \in S} \sum_{j=1}^{n} r_{j,\alpha}.$$

Proof. Let $\alpha \in S$ and $y \in \overline{k_0((t))}$ be a solution of $P = 0$ of ramification e, where t is a local parameter. We may write $y = p_0(t) + t^{\frac{1}{e}} p_1(t) + \cdots + t^{\frac{e-1}{e}} p_{e-1}(t)$ where the $p_i(t)$ are in $\overline{k_0}((t))$. Therefore the place containing y consists of $y_0, \ldots, y_{e-1}$ where $y_i = p_0(t) + \zeta^i t^{\frac{1}{e}} p_1(t) + \cdots + \zeta^{i(e-1)} t^{\frac{e-1}{e}} p_{e-1}(t)$ and ζ is a primitive eth root of unity. We may therefore write

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{e-1} \end{pmatrix} = M \begin{pmatrix} w_{0,e} \\ w_{1,e} \\ \vdots \\ w_{e-1,e} \end{pmatrix}$$

where M is the Vandermonde matrix of 1, ζ, $\zeta^2, \ldots, \zeta^{e-1}$ and $w_{i,e} = t^{\frac{i}{e}} p_i$. Since M is

invertible and, by assumption, the y_i are linearly independent, we see that the $\overline{k_0}$-span of each place of $P = 0$ has a basis of the form $\{w_{i,e}\}$. This implies that there are exponents of the form $n_0, n_1 + \frac{1}{e}, \ldots, n_{e-1} + \frac{e-1}{e}$ where the n_i are integers. The sum of the fractional parts of these exponents is $\sum_{i=0}^{e-1} \frac{i}{e} = \frac{e-1}{2}$.

Let $P_1, \ldots, P_m$ be the places at α and let $e_1, \ldots, e_m$ be the corresponding ramification indices. We have just shown that for each $j = 1, \ldots, m$ there are linearly independent elements $w_{i,e_j} = t^{\frac{i}{e_j}} p_{i,j}$ as above. Let $\rho_{i,j} \in \mathbf{Q}$ be the lowest power of t that appears in w_{i,e_j}. Each $\rho_{i,j}$ is an exponent of α. If all the $\rho_{i,j}$ are distinct then we have *all* the exponents at α and from the above we get that

$$\sum_{j=1}^{n} r_{j,\alpha} = \sum_{i} \frac{e_{i,\alpha} - 1}{2}$$

and the formula of this proposition follows now from the Hurwitz formula.

We therefore must consider the situation when two $\rho_{i,j}$ are equal. Consider all linearly independent families of solutions $\{w_{i,e_j}\}$ of L_P where $w_{i,e_j} = t^{\frac{i}{e_j}} p_{i,j}$ and associate to such a family the vector of lowest powers $(\rho_{i,j})$. Since there are only a finite number of possibilities for the $\rho_{i,j}$ there exists a maximal vector (using the lexicographical order) with associated family $\{w_{i,e_j}\}$. If two $\rho_{i,j}$ are equal we can replace one of the w_{i,e_j} with a combination of two of these and ensure that we get a family having a larger associated vector $(\rho_{i,j})$. Therefore, the powers appearing in the lowest-order terms must all be distinct and the previous argument applies. □

One can use the Hurwitz formula to calculate the genus of a curve but in order to do so one must calculate the ramification indices. Newton polygon methods allow one to do this but it can happen that one must generate many terms of the Puiseux expansions before one sees the ramification index appear in the denominator of an exponent of t. The formula of Proposition 3.1 just requires one to calculate the indicial equation at singularities of the minimal operator. One does not need to calculate the exponents at the apparent singularities (since these will be integers) so one only needs to look at those α such that $x - \alpha$ divides the discriminant of the polynomial (and possibly infinity). Furthermore, assuming that P is monic as a polynomial in y (which can be guaranteed by a Tschirnhaus transform) we do not need to calculate the exponents for all such α. If α has the property that all points (α, β) above α on the curve are nonsingular points, we have that $\sum_i (e_{i,\alpha} - 1)$ is precisely the multiplicity of $x - \alpha$ dividing the discriminant: see the Dedekind Discriminant Theorem (Eichler, 1966, p. 77).

To see this, recall that the discriminant is the product of the differences of the roots. Let $t = x - \alpha$ and assume that $y = \beta + d_1 t^{1/e} + \cdots$ is a root of P belonging to a place with ramification index $e > 1$. In particular, $x - \alpha$ has order e and so $y - \beta$ must have order 1 since the local ring corresponding to this place is nonsingular. Therefore $d_1 \neq 0$. The product of the $e(e-1)$ differences of elements in this place is therefore $d_1^{e(e-1)} d(w) t^{e(e-1)/e} + \cdots$ where $d(w)$ is the discriminant of the polynomial $z^e - 1$, (a nonzero constant). Thus, we get a series of the form constant $(x - \alpha)^{e-1}$+ higher-order terms. Each place contributes a factor of this form. A difference of roots from distinct places does not vanish, so we have our claim concerning the multiplicity n_α of $x - \alpha$ dividing the discriminant. Therefore, we may replace the term $\sum_i \frac{e_{i,\alpha}-1}{2}$ in the Hurwitz formula (or the term $\sum_{j=1}^{n} r_{j,\alpha}$ in the formula of Proposition 3.1) with $\frac{n_\alpha}{2}$.

EXAMPLE 3.2. Let $P(x, y)$ be the polynomial

$$y^2 - 2yx - 4yx^2 + x^2 + 4x^3 + 4x^4 - x^7 + x^5.$$

Its minimal operator is

$$L_P = \delta^2 - \frac{1}{2}\frac{(35x^4 - 54x^2 + 15 + 54x^5 - 76x^3 + 14x)}{x(x^2-1)(5x^2 - 3 + 6x^3 - 2x)}\delta + \frac{1}{2}\frac{84x^5 - 120x^3 + 20x + 35x^4 - 54x^2 + 15}{x^2(x^2-1)(5x^2 - 3 + 6x^3 - 2x)}.$$

The only true singular points are 0, 1, -1, ∞. The discriminant is $4x^5(x-1)(x+1)$. We note that the curve is nonsingular above the points 1 and -1 and the order of the discriminant at these values is 1. The exponents of L_P at 0 are $\{1, \frac{5}{2}\}$ and at ∞ are $\{-2, -\frac{7}{2}\}$. Therefore, the genus is $1 - 2 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} = 1$.

Note that the roots of P can be written as $x + 2x^2 + x^{5/2}\sqrt{x^2-1}$ and $x + 2x^2 - x^{5/2}\sqrt{x^2-1}$ so the ramification does not appear until the third term in the Puiseux series at 0. □

REMARK. An implementation of a method to calculate the genus of a curve based on the formula of Proposition 3.1 and using first-order systems of differential equations is described in Dottax (2001). We also note that there are efficient methods to calculate the genus of a curve based on calculating an integral basis of the associated function field (see Trager, 1984; van Hoeij, 1994). In addition there are geometric methods based on the resolution of singularities (see Henry and Merle, 1989; Teitelbaum, 1990).

4. Absolute Factorization

Let $P \in k_0(x)[y]$ be a squarefree polynomial of degree n. We will give two algorithms that use differential equations to determine the absolutely irreducible factors of P in $\overline{k_0}(x)[y]$; the first relies on properties of the linear representation of the Galois group arising from the associated minimal operator and the second is a modification of the algorithm of Duval (1991). There are several polynomial time algorithms that find the absolutely irreducible factors of a polynomial and we refer the reader to Gao (2001), Kaltofen (1995) and Ragot (1997) for a history of this problem. Other approaches to absolute factorization are given in Bajaj *et al.* (1993), Corless *et al.* (2002) and Galligo and Watt (1997).

4.1. ALGORITHM 1

For the first algorithm, we will assume that the roots of P in the algebraic closure of $k_0(x)[y]$ are linearly independent over $\overline{k_0}$. With this assumption, the algorithm presented here has running time that is a polynomial function of the degrees of x and y and the bit size of the numbers appearing in P (i.e. the bit size if $k_0 = \mathbf{Q}$ or a similar measure for algebraic numbers). Combining this with the algorithms of Section 2 yields a polynomial time algorithm for finding the absolute factorization of any P. Most recently, Gao (2001) has presented a deterministic algorithm that uses systems of partial differential equations to find absolutely irreducible factors in polynomial time (this algorithm also works over fields of sufficiently large prime characteristic). We note that the underlying ideas of Gao's algorithm and ours are different.

We begin by showing how one can determine the *number* of irreducible factors of P in $\overline{k_0}(x)[y]$. Let K be the splitting field of P over $\overline{k_0}(x)[y]$. The Galois group G of K over $\overline{k_0}(x)$ has a natural representation as a permutation group on the n roots $y_1, \ldots, y_n$ of P. The key fact that we use is that each orbit of the action of G on $y_1, \ldots, y_n$ is the set of roots of a monic absolutely irreducible factor of P. The field K is a differential field with a unique derivation extending $\frac{d}{dx}$. The elements of the Galois group commute with this derivation and so form the group of differential automorphisms of K over $\overline{k_0}(x)$ as well. Since K is generated by a fundamental set of solutions of the minimal operator L_P associated with P and has no new constants, it is the Picard–Vessiot extension of this operator (Kaplansky, 1976 or van der Put and Singer, 2001). Since the roots of P are linearly independent over $\overline{k_0}$, they form a basis of the solution space V of the minimal operator L_P. The Galois group of K therefore acts as linear transformations on V and has a representation as a group of $n \times n$ permutation matrices. We refer to this as the *permutation representation of* G. The key to counting the number of factors of P in $\overline{k_0}(x)[y]$ is the following lemma and proposition.

Lemma 4.1. (see Huppert, 1967, V. Satz 20.2a) *Let $G \subset \mathrm{GL}(V)$ be a permutation representation and $V_0 = \{v \in V \mid \sigma(v) = v \text{ for all } \sigma \in G\}$. The number of orbits of G acting on $\{y_1, \ldots, y_n\}$ equals the dimension of V_0.*

Proof. Let $\mathcal{O}_1, \ldots, \mathcal{O}_t$ be the orbits of G in $\{y_1, \ldots, y_n\}$. If $v = \sum c_i y_i \in V_0$, then any two y_i in the same orbit must have the same coefficient c_i. Therefore we may write

$$v = \sum_{i=1}^{t} c_i \left(\sum_{y_j \in \mathcal{O}_i} y_j \right).$$

Since the elements $w_i = \sum_{y_j \in \mathcal{O}_i} y_j$ lie in V_0 and are linearly independent, we have the conclusion of the lemma. □

Proposition 4.2. *Let P and L_P be as above. The number of irreducible factors of P over $\overline{k_0}(x)$ is precisely $\dim_{k_0}\{y \in k_0(x) \mid L_P(y) = 0\}$. In particular, $f \in \overline{k_0}(x)[y]$ is irreducible if and only if the space of rational solutions of $L_P(y) = 0$ is of dimension one and generated by the coefficient of y^{n-1} in P.*

Proof. Let K and G be as above, and let V be the solution space of L_P in K. Let $V_0 = \{v \in V \mid \sigma(v) = v \text{ for all } \sigma \in G\}$. Lemma 4.1 implies that the number of irreducible factors of P over $\overline{k_0}(x)$ equals $\dim_{\overline{k_0}} V_0$. The Galois theory implies that $V_0 = \{y \in \overline{k_0}(x) \mid L_P(y) = 0\}$. It is well known (see Theorem 9.1 of Bronstein, 1992 or Proposition 4.3 of van der Put and Singer, 2001) that, since L_P has coefficient in $k_0(x)$, this later vector space has a basis *in* $k_0(x)$. Therefore $\dim_{\overline{k_0}}\{y \in \overline{k_0}(x) \mid L_P(y) = 0\} = \dim_{k_0}\{y \in k_0(x) \mid L_P(y) = 0\}$. □

Proposition 4.2 allows one to determine the number of factors by determining the size of a k_0-basis of $\{y \in k_0(x) \mid L_P(y) = 0\}$. To do this one can use one of the standard algorithms to find rational solutions of a linear differential equation (see Bronstein, 1992 or van der Put and Singer, 2001). Since we have the polynomial P as well as L_P, we can proceed more directly. One can multiply P by a suitable polynomial in x and produce a squarefree polynomial in $k_0[x, y]$. If $q(x)$ is the coefficient of y^n in this polynomial, then

the (multivalued) functions $qy_1, \ldots, qy_n$ have no poles in the finite plane because the qy_i satisfy a polynomial in $k_0[x, y]$ that is monic in y. Therefore, any linear combination of these that is rational must be a polynomial. This implies that any rational solution of $L_P(y) = 0$ is of the form $\frac{p}{q}$ for some polynomial p. The number $\deg_x(p) - \deg_x(q)$ is bounded by the possible order of a pole of any y_i at infinity and these can be bounded in terms of the slopes of the Newton polygon of P at infinity (or one can determine the possible values of $\deg_x(q) - \deg_x(p)$ from the indicial polynomial of L_P at infinity). Therefore, from the slopes of the Newton polygons of P we can find an upper bound N for the possible degree of p. If we let $y = \frac{c_N x^N + \cdots + c_0}{q}$ where the c_i are indeterminates, substitute this expression in $L_P(y) = 0$, clear denominators, compare powers of x and determine a system of linear equations whose solution space has dimension equal to the space $\{y \in k_0(x) \mid L_P(y) = 0\}$. Note that we can also determine a basis of this latter space.

We now turn to the problem of finding the irreducible factors of P in $\overline{k_0}(x)[y]$. If P is irreducible over $k_0(x)$ then these factors are conjugate under the action of the Galois group $Gal(\overline{k_0}/k_0)$ of $\overline{k_0}$ over k_0. Therefore, once we have found an extension k of k_0 such that $k(x)$ contains the coefficients of such a factor and have found this factor, we have "found" all factors. In the case where P is just assumed to be squarefree, the set of absolutely irreducible factors is the union of $Gal(\overline{k_0}/k_0)$ orbits, one orbit for each irreducible factor of P in $k_0(x)[y]$. We will present an algorithm that produces a $\gamma \in \overline{k_0}$ and an absolutely irreducible $P \in k_0(\gamma, x)[y]$ that is a factor of P. To find all absolutely irreducible factors one can proceed in several ways. The first is to factor P over $k_0(x)$ and apply the algorithm to each irreducible factor. One will then produce an absolutely irreducible factor in each $Gal(\overline{k_0}/k_0)$ orbit. A second approach is to find an absolutely irreducible factor P_1 of P, replace P by P/P_1 and apply the algorithm again. This will yield a list of all absolutely irreducible factors. A third approach is to apply the algorithm and produce an absolutely irreducible factor $P_1 \in k_0(\gamma, x)[y]$. One then calculates the norm $N(P_1) = \prod_\sigma P_1^\sigma$ where the product is over all embeddings of $k_0(\alpha)$ into $\overline{k_0}$. The coefficients of $N(P_1)$ can be calculated from the coefficients of the minimal polynomial of γ (see Winkler, 1996, p. 141). Furthermore, $N(P_1)$ is the power of an irreducible factor of P in $\bar{k}_0(x)[y]$. One then replaces P by $P/GCD(P, N(P_1))$ and repeats the process. This will give a list of absolutely irreducible factors, one from each $Gal(\overline{k_0}/k_0)$ orbit.

We now show that to calculate a factor of P it is enough to calculate the term of second highest degree in this factor. Recall, from the introduction to Section 2, that we have defined a sequence of polynomials S_i of degrees at most $n-1$ in y such that $\delta^i(y) = S_i(y)$ for any root y of P. The assumption that the roots of P are linearly independent over $\overline{k_0}$ implies that 0 is not a root of P. Therefore we can use $P = 0$ to write 1 as a linear combination of $y, \ldots, y^n$ and so write $\delta^i(y) = \overline{S}_i(y)$ where each $\overline{S}_i$ is a $k_0(x)$-linear combination of $y, \ldots, y^n$. We conclude that there is matrix $M \in \mathrm{GL}_n(k_0(x))$ such that $(y, \delta(y), \ldots, \delta^{n-1}(y))^T = M(y, \ldots, y^n)^T$ for any root y of P; the ith row of this matrix is the vector of coefficients of $\overline{S}_i$. We therefore have that $(y, \ldots, y^n)^T = A(y, \delta(y), \ldots, \delta^{n-1}(y))^T$ where $A = M^{-1}$. This implies that for any integer s, and roots $y_1, \ldots, y_s$ of P, we have

$$\begin{pmatrix} y_1 + \cdots + y_s \\ y_1^2 + \cdots + y_s^2 \\ \vdots \\ y_1^n + \cdots + y_s^n \end{pmatrix} = A \begin{pmatrix} y_1 + \cdots + y_s \\ \delta(y_1 + \cdots + y_s) \\ \vdots \\ \delta^{n-1}(y_1 + \cdots + y_s) \end{pmatrix}.$$

Using this equality and the Newton identities, we can write the first s elementary symmetric functions of $y_1, \ldots, y_s$ as differential polynomials in $y_1 + \cdots + y_s$ and its derivatives up to order $n-1$. In particular, if $y_1, \ldots, y_s$ are the roots of an irreducible factor $y^s + b_{s-1}y^{s-1} + \cdots + b_0$ of P, then we can determine $b_{s-2}, \ldots, b_0$ once we have found b_{s-1}. We shall show below how to determine this coefficient. To do this we will need the following lemma that gives the structure of the inverse of the Vandermonde matrix. Although it is known (Zippel, 1993, Chapter 13.1) that the inverse of the Vandermonde matrix has a special form, we thank Hoon Hong for the explicit formulae given in this lemma as well as a proof of their correctness.

LEMMA 4.3. *Let K be a field $x, y, x_1, \ldots, x_n$ indeterminates and let*

$$\begin{aligned} h(y) &= \prod_{i=1}^{n}(y - x_i) \\ q(x,y) &= \frac{h(y) - h(x)}{y - x} = \sum_{j=1}^{n} y^{j-1} q_j(x) \\ r(x) &= \frac{q(x,x) D_y(q(x,y))}{D_y(h(y))} \\ p_j(x) &= q_j(x) r(x) \end{aligned}$$

where $D_y(f(y))$ denotes the discriminant $Res_y(f(y), f_y(y))$. Then the matrix

$$M = \begin{pmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ \vdots & & \vdots & \\ 1 & x_n & \ldots & x_n^{n-1} \end{pmatrix} \begin{pmatrix} p_1(x_1) & p_1(x_2) & \ldots & p_1(x_n) \\ \vdots & & \vdots & \\ p_n(x_1) & p_n(x_2) & \ldots & p_n(x_n) \end{pmatrix}$$

is the identity matrix.

PROOF. Note

$$\begin{aligned} M_{ij} &= \sum_{k=1}^{n} x_i^{k-1} p_k(x_j) = \sum_{k=1}^{n} x_i^{k-1} q_k(x_j) r(x_j) = r(x_j) \sum_{k=1}^{n} x_i^{k-1} q_k(x_j) \\ &= r(x_j) q(x_j, x_i). \end{aligned}$$

Case $i \neq j$:

$$M_{ij} = r(x_j) \frac{h(x_i) - h(x_j)}{x_i - x_j} = r(x_j) \frac{0 - 0}{x_i - x_j} = 0.$$

Case $i = j$:

$$M_{ij} = \frac{q(x_j, x_j) D_y(q(x_j, y))}{D_y(h(y))} q(x_j, x_j) = \frac{q(x_j, x_j)^2 D_y(q(x_j, y))}{D_y(h(y))}.$$

Note that

$$q(x_j, y) = \frac{h(y) - h(x_j)}{y - x_j} = \frac{h(y)}{y - x_j} = \prod_{i \neq j}(y - x_i).$$

Thus

$$q(x_j,x_j)^2 D_y(q(x_j,y)) = \left(\prod_{i\neq j}(x_j-x_i)\prod_{\substack{\mu>\nu\\ \mu\neq j,\nu\neq j}}(x_\mu-x_\nu)\right)^2 = \left(\prod_{\mu>\nu}(x_\mu-x_\nu)\right)^2$$
$$= D_y(h(y)).$$

Hence

$$M_{ij} = 1.$$

Thus M is an identify matrix. □

If $H(y) \in F[y]$ is a squarefree polynomial with coefficients in a field F and $\gamma_1,\ldots,\gamma_n$ are its roots in the algebraic closure of F, then we can specialize $x_i \longmapsto \gamma_i$ in the above result. We denote by $p_i^H(y)$ the result of specializing the x_i in the polynomial $p_i(y)$. Note that the coefficients of p_i are rational symmetric functions in the x_i with denominators that do not vanish under this specialization. Therefore $p_i^H(y) \in F[y]$ and the coefficients of these polynomials can be easily calculated from the coefficients of H.

Algorithm 1.

Input: A squarefree polynomial $P \in k_0(x)[y]$ whose roots are linearly independent over $\overline{k_0}$.
Output: An element $\gamma \in \overline{k_0}$ (given by its minimal polynomial) and an absolutely irreducible factor $\overline{P} \in k_0(\gamma,x)[y]$.
Step 1: Calculate the minimal operator L_P associated with P and find a basis $w_1,\ldots,w_t \in k_0(x)$ of $\{w \in k_0(x) \mid L_P(w) = 0\}$. If $t = 1$ the polynomial is absolutely irreducible and we can stop.
Step 2: Let $\beta \in k_0$ be an ordinary point of L_P and calculate the first $n+1$ terms of an adapted basis $\{s_1,\ldots,s_n\} \subset k_0[[x-\beta]]$ at $x = \beta$ (see Definition 2.5).†
Step 3: Calculate the $t \times n$ matrix B with entries in k_0 such that $(w_1,\ldots,w_t)^T = B(s_1,\ldots,s_n)^T$. This can be achieved by expanding the w_i at $x = \beta$ and solving the resulting linear system determined by equating the coefficients of the first n powers of $x-\beta$.
Step 4: Let $H(y) = P(\beta,y) \in k_0[y]$ and define polynomials $r_i \in k_0[y]$ by the equation $(r_1,\ldots,r_t)^T = B(p_1^H,\ldots,p_n^H)^T$, where the p_i^H are as defined following Lemma 4.3.
Step 5: Let $\gamma \in \overline{k_0}$ be a root of $H(y)$ (determined by some irreducible factor of H). Calculate the greatest common divisor $g(y)$ of the polynomials $H(y), r_1(y) - r_1(\gamma),\ldots,r_t(y) - r_t(\gamma)$ in $k_0(\gamma)[y]$. Calculate (using the Newton identities and the coefficients of $g(y)$) the elements $C_i = \sum c^{i-1} \in k_0(\gamma)$ where the sum is over the roots of g.
Step 6: Find $d_i \in k_0(\gamma)$ such that $(d_1,\ldots,d_t)B = (C_1,\ldots,C_n)$. Let $s = \deg_y g$ and let $b_{s-1} = d_1w_1 + \cdots + d_tw_t$.
Step 7: Calculate $b_{s-2},\ldots,b_0$ as in the paragraph preceding Lemma 4.3. The polynomial $y^3 + b_{s-1}y^{s-1} + \cdots + b_0 \in k_0(\gamma,x)[y]$ is an absolutely irreducible factor of P.

†This may have already been computed in Step 1 depending on the method used to compute L_P.

Before we show that this algorithm is correct, we will make some comments concerning several of the steps. In Step 3, the matrix B is uniquely determined since the s_i form a basis of the solution space of L_P. Since β is an ordinary point of L_P any solution is determined by the first n terms of its Taylor series at this point. Therefore B can be calculated as described. Note that B will have rank t since the w_i are linearly independent. Because of this, once we have shown that the linear system in Step 5 can be solved, the solution will be unique. We now turn to showing that the algorithm is correct.

Since $x = \beta$ is an ordinary point of L_P it will be a nonsingular point of P. The equation $P(\beta, y) = 0$ has n distinct solutions $\gamma_1, \ldots, \gamma_n$ and for each γ_i we have a root y_i of P such that $y_i(\beta) = \gamma_i$. By definition, the s_i satisfy $(y_1, \ldots, y_n)^T = V(s_1, \ldots, s_n)^T$ where V is the Vandermonde matrix of $\gamma_1, \ldots, \gamma_n$. We therefore have $(w_1, \ldots, w_t)^T = BV^{-1}(y_1, \ldots, y_n)^T$. Lemma 4.3 implies that $BV^{-1} = R$ where $R = (r_i(\gamma_j))$ is the $t \times n$ matrix whose ith row is $(r_i(\gamma_1), \ldots, r_i(\gamma_n))$ where the r_i are defined as in Step 4. Notice that the matrix R is uniquely determined by the equation $(w_1, \ldots, w_t)^T = R(y_1, \ldots, y_n)^T$. Let G be the Galois group of the splitting field of P over $\overline{k_0}(x)$. We think of G as a group of permutations on the y_i. The orbits of G correspond to the irreducible factors of P over $\overline{k_0}(x)$ and we know that there are precisely t of these. For any $\sigma \in G$ we have $(w_1, \ldots, w_t)^T = (\sigma(w_1), \ldots, \sigma(w_t))^T = (r_i(\gamma_j))(y_{\sigma(1)}, \ldots, y_{\sigma(n)})^T = (r_i(\gamma_{\sigma(j)}))(y_1, \ldots, y_n)^T$. The last equality is due to the fact that permuting the rows of $(y_1, \ldots, y_n)^T$ is the same as permuting the columns of $(r_i(\alpha_j))$ in the product. By uniqueness, we have that $(r_i(\gamma_j)) = (r_i(\gamma_{\sigma(j)}))$. Fix some value of i and for simplicity we will let $i = 1$. The set of j such that y_j is in the G-orbit of y_1 is therefore the set of j such that $(r_1(\gamma_1), \ldots, r_t(\gamma_1)) = (r_1(\gamma_j), \ldots, r_t(\gamma_j))$. Letting $\gamma = \gamma_1$ in Step 4, we see that the roots c of the polynomial $g(y)$ are precisely the set of γ_i such that $y_j = \sum_{j=1}^{n} \gamma_i^{j-1} s_j$ is in the orbit $\mathcal{O}$ of y_1. The sum

$$w = \sum_{i \in \mathcal{O}} y_i = \sum_{i=1}^{n} \left(\sum_{\{c \mid g(c)=0\}} c^{i-1} \right) s_i = \sum_{i=1}^{n} C_i s_i$$

is therefore in $\overline{k_0}(x)$ and is the coefficient of y^{s-1} in the absolutely irreducible factor corresponding to this orbit (N.B. $s = \deg_y g$). We furthermore have that w is a rational solution of L_P and so there exist $d_1, \ldots, d_t$ such that $d_1 w_1 + \cdots + d_t w_t = C_1 s_1 + \cdots + C_n s_n$. Since $(w_1, \ldots, w_t)^T = B(s_1, \ldots, s_n)^T$ and the s_i are linearly independent over $\overline{k_0}$, we have that $(d_1, \ldots, d_t)B = (C_1, \ldots, C_n)$. Therefore Step 6 can be completed and the claim of Step 7 is true.

Note that the γ we find may generate a field that is larger than necessary.

Example 4.4. We illustrate the above algorithm with $k_0 = \mathbf{Q}$ and the polynomial

$$P = y^4 - 4y^3 + (6x^2 + 6)y^2 + (-4 - 8x^2 - 4x^4)y + 1 + 3x^4 + 3x^2 + x^6.$$

We compute that $P(2, y) = (y^2 - 4y + 5)(y^2 + 25)$. In order to compute series at $x = 0$ later, we consider the transformed polynomial $\tilde{P} = P(x + 2, y)$ and find a factor for $\tilde{P}$.

Step 1: The minimal operator associated to $\tilde{P}$ is

$$L_{\tilde{P}} = \delta^4 + \frac{3}{x+2}\delta^3 + \frac{3}{4(x+2)^2}\delta^2$$

and a basis of rational solutions is $\{w_1 = 1, w_2 = x\}$. This shows that $\tilde{P}$ (and thus P) is reducible and factors into two irreducible factors over $\overline{\boldsymbol{Q}}(x)$.

Step 2: The first five terms of an adapted basis of $L_{\tilde{P}} = 0$ at $x = 0$ are

$$\begin{aligned}
s_1 &= -\frac{1}{64}x^3 + \frac{3}{512}x^4 - \frac{9}{4096}x^5 \\
s_2 &= 1 + \frac{11}{20}x + \frac{3}{32}x^2 - \frac{1}{640}x^3 - \frac{9}{10240}x^4 + \frac{21}{40960}x^5 \\
s_3 &= \frac{1}{20}x + \frac{7}{800}x^2 - \frac{1}{640}x^3 - \frac{23}{51200}x^4 + \frac{31}{204800}x^5 \\
s_4 &= \frac{1}{400}x^2 - \frac{1}{25600}x^4 + \frac{1}{51200}x^5.
\end{aligned}$$

Step 3: The 2×4 matrix B such that $(w_1, w_2)^T = B(s_1, s_2, s_3, s_4)^T$ is

$$B = \begin{pmatrix} 1 & 1 & -11 & 1 \\ -2 & 0 & 20 & -70 \end{pmatrix}.$$

Step 4: Let $H(y) = \tilde{P}(0, y) = (y^2 - 4y + 5)(y^2 + 25)$. The polynomials r_i are $r_1 = -\frac{1}{4000000}(10825 - 4590y + 1383y^2 - 332y^3 + 63y^4 - 6y^5 + y^6)(y^3 - 3y^2 + 15y - 25)^2$ and $r_2 = \frac{1}{2000000}(10825 - 4590y + 1383y^2 - 332y^3 + 63y^4 - 6y^5 + y^6)(y^3 - 4y^2 + 20y - 25)(y^3 - 3y^2 + 15y - 25)$.

Step 5: Let γ be a root of $y^2 + 25 = 0$. Then the greatest common divisor of $H(y), r_1(y) - r_1(\gamma)$ and $r_2(y) - r_2(\gamma)$ is

$$g(y) = y^2 - (2 + 4/5\gamma)y + 5 + 2\gamma.$$

And we have $C_1 = 2$, $C_2 = 2 + 4/5\gamma$, $C_3 = -4/5\gamma - 22$ and $C_4 = -136/5\gamma + 2$.

Step 6: For $d_1 = 2 + 4/5\gamma$ and $d_2 = 2/5\gamma$ we have $(d_1, d_2)B = (C_1, C_2, C_3, C_4)$. Then $-b_1 = -(d_1 w_1 + d_2 w_2) = -(d_1 + d_2 x)$ is the coefficient of degree 1 of an absolutely irreducible factor of degree 2 of $\tilde{P}$.

Step 7: An absolutely irreducible factor of $\tilde{P}$ is therefore

$$y^2 - (2/5\gamma x + 2 + 4/5\gamma)y + 1/5\gamma x^3 + (6/5\gamma + 1)x^2 + (13/5\gamma + 4)x + 2\gamma + 5$$

and so an absolutely irreducible factor of P is

$$y^2 + (-2/5\gamma x - 2)y + 1/5\gamma x^3 + x^2 + 1/5\gamma x + 1$$

where $\gamma^2 = -25$.

4.2. ALGORITHM 2

In this section we no longer assume that the roots of P are linearly independent over $\overline{k_0}$ and we show how one can modify the algorithm of Duval (1991) (see also Ragot, 1997) using differential equations. This idea already appears in Rybowicz (1990) but we shall recapitulate this approach and give the precise needed bounds and a more detailed discussion.

Duval's algorithm is based on the fact that the number of absolutely irreducible factors of P over $\overline{k_0}(x)$ is the k_0-dimension of the subring B of $A = k_0(x)[y]/(P)$ consisting of elements of A that are algebraic over k_0. In particular, this dimension is 1 if and only if the polynomial is absolutely irreducible. The subring B is, in geometric terms, the vector space of functions on the curve having no poles on the curve. One can calculate a basis for B using techniques similar to those used to calculate the integral closure of $k_0[x]$ in

A. As Duval notes, given an element $c \in B \setminus k_0$, if we write $c = a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}$ then the GCD of $P(y)$ and $c - (a_0 + a_1 y + \cdots + a_{n-1} y^{n-1})$ gives a non-trivial factor P_1 of P having coefficients in an algebraic extension k_1 of k_0. One then can proceed by induction to find an absolutely irreducible factor of P.

Our modification is based on the observation that the ring B is precisely the ring of constants of the extension of $\frac{d}{dx}$ from $k_0(x)$ to A. To see this note that since P is squarefree, there exist R, $S \in k_0(x)[y]$ such that $RP + SP_y = -P_x$ as in Section 2 and that the equation $\delta(y) = S$ defines a derivation on $k_0(x)[y]$ that induces a derivation on A. Any element of $a \in A$ is the root of a monic polynomial $p_a(y)$ of minimal degree with coefficients in $k_0(x)$. If a is a constant, then one sees that $\frac{dp_a}{dx}(a) = 0$. This would imply that a satisfies a monic polynomial of smaller degree unless $\frac{dp_a}{dx} \equiv 0$. Therefore a is algebraic over k_0. A similar calculation shows that if a is algebraic over k_0 then a is a constant.

We now show how differential equations can be used to find a k_0-basis for the ring B (the remaining steps in Duval's algorithm remain unchanged). We wish to find a k_0-basis for $V = \{(a_0, \ldots, a_{n-1}) \in k_0(x)^n \mid \delta(a_0 + a_1 y + \cdots + a_{n-1} y^{n-1}) = 0\}$. Expanding the expression $\delta(a_0 + a_1 y + \cdots + a_{n-1} y^{n-1})$, replacing $\delta(y)$ with $S(y)$ and reducing $\bmod P$, we get an expression $b_0 + b_1 y + \cdots + b_{n-1} y^{n-1}$ where the b_i are of the form $\delta(a_i) +$ a $k_0(x)$-linear combination of the a_j. Therefore, there exists an $n \times n$ matrix M such that $(a_0, \ldots, a_{n-1}) \in V$ if and only if $\delta((a_0, \ldots, a_{n-1})^T) = M(a_0, \ldots, a_{n-1})^T$. We therefore need to calculate a basis of the solutions *in* $k_0(x)^n$ of $\delta(Y) = MY$. Although there are standard algorithms to find such a basis (see Barkatou, 1999), one can again take advantage of the special origin of this system. The elements of V are trivially integral over $k_0[x]$. Therefore, we can assume that the a_i are of the form c_i/d where d is the largest squared factor of the discriminant. The degrees of the c_i can furthermore be bounded from a calculation at infinity and once this is done the problem is reduced to solving a system of linear equations for the coefficients of the numerator polynomials.

To bound the degrees of the c_i, replace x by $1/z$ in P and study the local behaviour at 0. We first (using the Newton polygon) determine a minimum power of z such that $z^s y$ is integral above $z = 0$. Now compute the minimal polynomial of $w = z^s y$ and its discriminant. If we let m be the power of z dividing this discriminant, then any locally integral element can be expressed using powers of w with z^k as a common denominator where k is the largest integer less than $m/2$. Sending 0 back to infinity we have now bounded the degrees of our polynomial coefficients.

One can give a more efficient version of the previous construction which avoids computing the polynomial for w and its discriminant. If we let n be the degree of P in y, then the power of z dividing the discriminant can be computed in the following way.

We have found s such that $w = y/x^s$ is integral at all places over infinity. We also have $P(y, x)$ the minimal polynomial for y, which we assume to be monic in y; then the minimal polynomial for w is simply $P(wx^s, x)$. If we let $x = 1/z$ and normalize to be monic, we get that the monic minimal polynomial for w is $Q(w, z) = z^{ns} P(w/z^s, 1/z)$ where $n = \deg_y P(y, x)$. By assumption, w is integral at 0, so its monic minimal polynomial does not contain negative powers of z, i.e. $Q(w, z)$ is a polynomial in w and in z. We need to compute the discriminant of Q. Here we need two discriminant identities which can easily be derived from the basic definition of discriminants, i.e. $\operatorname{disc}(cP(y)) = c^{2n-2} \operatorname{disc}(P(y))$ and $\operatorname{disc}(P(cy)) = c^{n(n-1)} \operatorname{disc}(P(y))$. If we let $\operatorname{disc} P(x)$ be the discriminant of P with

respect to y, we have that $\mathrm{dis}Q(z) = z^{n(n-1)s}\mathrm{disc}P(1/z)$. So if we let m be the exact power of z dividing $\mathrm{disc}Q(z)$ we have that $m = n(n-1)s - \deg_x \mathrm{disc}P(x)$.

To finish the degree bounding job, we are assuming that coefficients of our constant function are of the form c_i/d, our degree constraint at infinity is that $\mathrm{ord}_\infty(x^{is}c_i/d) \geq -m/2$. Since the order at infinity of a rational function is the degree of the denominator minus the degree of the numerator, this implies that $\deg c_i \leq m/2 + \deg d - is$. We shall illustrate these bounds in the following example.

EXAMPLE 4.5. If we let $k_0 = \mathbf{Q}$ and $P_1 = y^2 - 2x^2$ then the element y/x is the constant $\sqrt{2}$. If we make the substitution $y \to y + x^2$ we produce a new polynomial $P = y^2 + 2x^2y + x^4 - 2x^2$ and $\sqrt{2} = (x^2 + y)/x$. We shall calculate the bounds as above with respect to P. The discriminant of P is $8x^2$ so the basic denominator is $d = x$, that is, we may write any constant as $c_0/x + (c_1/x)y$ where the c_i are polynomials in x. If we follow through the degree analysis above, we see that $s = 2$ so y/x^2 is integral at infinity. Substituting we find that $m = 2$ and so $\deg_x c_0 \leq 2$ and $\deg_x c_1 \leq 0$, precisely the minimal degrees that will work. □

EXAMPLE 4.6. We illustrate Algorithm 2 with the same example as used in Algorithm 1:

$$P = y^4 - 4y^3 + (6x^2 + 6)y^2 + (-4 - 8x^2 - 4x^4)y + 1 + 3x^4 + 3x^2 + x^6.$$

The associated matrix M is

$$M = \begin{pmatrix} 0 & 0 & 0 & \frac{3(x^2+1)^2}{2x} \\ 0 & \frac{1-3x^2}{2x(x^2+1)} & 0 & \frac{-6(x^2+1)}{x} \\ 0 & \frac{-1}{2x(x^2+1)} & \frac{1-3x^2}{x(x^2+1)} & \frac{9}{x} \\ 0 & 0 & \frac{-1}{x(x^2+1)} & -\frac{9}{2x} \end{pmatrix}$$

and we find that a basis of rational solutions of the system $\delta(Y) = MY$ is spanned by $w_1 = (1, 0, 0, 0)$ and

$$w_2 = \left(-\frac{3}{x}, \frac{8}{x(x^2+1)}, \frac{x^2-7}{x(x^2+1)^2}, \frac{2}{x(x^2+1)^2}\right).$$

Let γ be a root of $x^2 + 25 = 0$. By evaluating at $x = 2$ (a nonsingular point), one finds that the number $a = w_2(1) + w_2(2)y + w_2(3)y^2 + w_2(4)y^3$, where y is a root of P, is equal to $-1/5\gamma$. Computing the greatest common divisor of P and $-1/5\gamma - (w_2(1) + w_2(2)y + w_2(3)y^2 + w_2(4)y^3)$, one gets a nontrivial factor of P:

$$y^2 + (-2/5\gamma x - 2)y + 1/5\gamma x^3 + x^2 + 1/5\gamma x + 1. \square$$

In the previous example, we avoided the calculation of Puiseux series by evaluating at a point. Another way to avoid the calculation of the Puiseux expansion is the following. Once we have found a constant element in our function field, $c = g(x, y)$, we can determine the minimal polynomial of c by computing an irreducible factor of the resultant, with respect to y, of $c - g(x, y)$ and $P(x, y)$ (if P is irreducible, then the primitive part of this resultant will be a power of the minimal polynomial of c). Working over the field $k_0(c)$, one then takes the GCD of $c - g(x, y)$ and P to get a nontrivial factor of P.

5. Galois Groups

In this section we will show how differential equations can be used to help calculate the Galois groups of a polynomial $P \in k_0(x)[y]$ over $k_0(x)$ and $\overline{k_0}(x)$.

5.1. Galois groups over $\overline{k_0}(x)$

It is well known that the computation of the Galois group of a polynomial can be reduced to the factorization of polynomials (see Matzat *et al.*, 2000; van der Waerden, 1953†). A weaker but similar result holds for differential equations (Singer and Ulmer, 1993). In the following we want to consider differential operators

$$L = \sum_{i=0}^{n} a_i \delta^i$$

(corresponding to differential equations $Ly = \sum_{i=0}^{n} a_i y^{(i)}$) as a polynomial in δ over $\overline{k_0}(x)$. The set $\mathcal{D}$ of differential operators over the field $\overline{k_0}(x)$ forms a non-commutative ring where addition is the usual addition of polynomials and multiplication is the composition of operators defined by the rule $\forall a \in \overline{k_0}(x)$, $\delta a = a\delta + a'$. A differential operator L is *reducible* over $\overline{k_0}(x)$ if and only if $L = L_1 L_2$ in $\mathcal{D}$ where the L_i have positive order (i.e. positive degree in δ). We say that an equation $L(y) = 0$ is reducible if the associated operator L is reducible. We refer to Singer (1996) 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 factorization domain, but if $L = L_1 L_2 \cdots L_s$ and $L = \tilde{L}_1 \tilde{L}_2 \cdots \tilde{L}_t$ are two decompositions of an operator $L \in \mathcal{D}$ into irreducible factors, then $s = t$ and there is a permutation $\sigma \in S_t$ such that $\mathcal{D}/\mathcal{D}L_i \cong \mathcal{D}/\mathcal{D}\tilde{L}_{\sigma(i)}$. In particular, the representations of the differential Galois group G on the solution space of $L_i(y) = 0$ and $\tilde{L}_{\sigma(i)}(y) = 0$ are isomorphic G-modules. In classical Galois theory a polynomial is reducible if and only if its Galois group is intransitive. The differential analogue is the following theorem.

Theorem 5.1. (Singer, 1996) *Let L be a linear differential operator over $\overline{k_0}(x)$ and let V be its solution space in a Picard–Vessiot extension. The operator L factors over $\overline{k_0}(x)$ if and only if its differential Galois group G leaves a proper, nonzero subspace $\{0\} \subset W \subset V$ invariant, i.e. $G \subset \mathrm{GL}_n(\overline{k_0})$ is a reducible linear group.*

The factorization of differential operators is, in general, a difficult task but if the group is reductive, there are special techniques that make the task simpler. We recall that a group is *reductive* if, for any representation of G as a group of linear transformations on a vector space V and any G-invariant subspace $W \subset V$ there exists a G-invariant subspace $W_0 \subset V$ such that $V = W \oplus W_0$. The groups considered here are all finite and so are reductive (Maschke's Theorem; Lang, 1993, Theorem 1.2, Chapter XVIII, Section 1). When the group is reductive a factorization can be found using the *Eigenring* (Singer, 1996; van Hoeij, 1997). This object is defined as

$$\mathcal{E}(L) = \{R \in \mathcal{D} | ord(R) < ord(L) \text{ and } LR \text{ is divisible on the right by } L\}.$$

An element $R \in \mathcal{E}(L)$ of order greater or equal to 1 gives a nontrivial factor of L. Indeed for z in the solution space V of L we have that $L(R)(z)) = 0$ which shows that $z \longmapsto R(z)$

†An implementation of Deconinck and van Hoeij, which is part of the algcurves package in Maple 7, computes the monodromy of P by analytic continuation methods (see Matzat *et al.*, 2000).

is a $\overline{k_0}$-linear map of V to itself. If $c \in \overline{k_0}$ is an eigenvalue of this linear map, then $R - c$ and L will have a nontrivial common factor which can be found by computing a right gcd. The coefficients of $R \in \mathcal{E}(L)$ are rational solutions of a linear differential operator, they can be found using linear algebra. Furthermore, for reductive groups the character of the representation of 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.

We now turn to operators that arise as the minimal operator of a polynomial. Given a permutation group G on n letters, there is a natural linear representation of order n, the permutation representation, associated with G. This is obtained by letting G act on a vector space of dimension n by permuting the basis elements. Let L_P be the minimal operator of the polynomial $P \in \overline{k_0}(x)[y]$ and let G be its Galois group over $\overline{k_0}(x)$ (note that the usual Galois group and the differential Galois group coincide). If L_P is of maximal order then the representation of G on the solution space of L_P is the permutation representation. If L_P has smaller order then the solution space will be a quotient of the permutation representation (and so can be identified with a subrepresentation). The factorization of L_P gives information about G (we do not assume here that the minimal operator L_P is of maximal order).

PROPOSITION 5.2. *Let $P \in \overline{k_0}(x)[y]$ be of degree n.*

1. *The group G is Abelian if and only if L_P is a product of operators of order one.*
2. *The group $G \subset S_n$ is doubly transitive if and only if L_P has an irreducible factor of order $n - 1$.*
3. *The group G is trivial if and only if all solutions of L_P are in $\overline{k_0}(x)$ (which can be computed using linear algebra* (Abramov, 1989; Bronstein, 1992; van der Put and Singer, 2001))

PROOF. The first result follows from the fact that a finite group is Abelian if and only if all its irreducible representations are of degree 1. Let χ_P denote the character of the permutation representation of G associated with the action of G on the roots of P and let χ_{L_P} denote the character of the representation of G acting on the solution space of L_P. If the action of G on the roots of P is doubly transitive, then $\chi_P = \mathbf{1} + \phi$, where ϕ is an irreducible character of G (Huppert, 1967, V Satz 20.2). We have that χ_{L_P} can be identified with a summand of χ_P. Therefore if χ_{L_P} does not have a summand corresponding to an irreducible representation of degree $n - 1$, then $\chi_{L_P} = \mathbf{1}$. This implies that G is trivial and so cannot be doubly transitive. Therefore, the solution space of $L(y) = 0$ has summand that is an irreducible G-module of dimension $n - 1$ and so Assertion 2 follows. The last assertion follows from the Galois correspondence in differential Galois theory. □

As noted, the last statement of this proposition can be checked using linear algebra. To test if the Galois group is doubly transitive, one can proceed as follows. Let $P(y) = y^n + a_{n-1}y^{n-1} + \ldots$. We make a Tschirnhaus transformation $T(y) = y - \frac{1}{n}a_{n-1}$ of the polynomial P and get a new polynomial $\overline{P}$ having a sum of roots that is zero (note that if we decide to do this we cannot use the algorithm of Section 2 to calculate $L_{\overline{P}}$). The minimal operator of this new polynomial $\overline{P}$ will then be irreducible of order $n - 1$ if and only if the Galois group is doubly transitive. Note that this operator is irreducible if and only if the Eigenring has dimension 1 and this can be checked by searching for rational

solutions of an appropriate system. The fact that G is Abelian can also be checked using the Eigenring. This follows from the next two lemmas. We begin with a simple group theoretic fact (see Huppert, 1967, I. Satz 5.3).

LEMMA 5.3. *Let $G \subset S_n$ be a transitive permutation group and let V be the n-dimensional vector space on which G acts via the permutation representation. The group G is Abelian if and only if $V = V_1 \oplus \cdots \oplus V_n$ where the V_i are non-isomorphic one-dimensional G-modules.*

PROOF. If V has the decomposition of the lemma, then $G \subset \mathrm{GL}(V)$ is diagonalizable and so is Abelian. Conversely, if G is Abelian, then we can write $V = V_1 \oplus \cdots \oplus V_n$ where the V_i are one-dimensional G-modules. We must show that they are pairwise non-isomorphic.

Let $\{e_1, \ldots, e_n\}$ be the set on which G acts transitively and consider these as basis elements of V. Since G acts transitively on this set, the span of the orbit of e_1 has dimension n. Now assume that two of the V_i are isomorphic as G-modules. We can then write $e_1 = \sum_{i=1}^{t} w_i$ where $t < n$ and for any i there is a character χ_i of G such that $g(w_i) = \chi_i(g)w_i$ for all $g \in G$. This implies that the orbit of e_1 lies in the span of $\{w_i, \ldots, w_t\}$. Since this span has dimension less than n, we have a contradiction. □

PROPOSITION 5.4. *Suppose that $P \in \overline{k_0}(x)[y]$ is irreducible of degree n and let the order of L_P be $m \leq n$. The Galois group G of P over $\overline{k_0}(x)$ is Abelian if and only if*

1. $\dim(\mathcal{E}(L_P)) = m$, *and*
2. *there exists a basis $R_1, \ldots, R_m$ of $\mathcal{E}(L_P)$, each of order $m-1$ such that $L_P = S_i R_i$ for $i \in \{1, \ldots, m\}$ for some $S_i \in \mathcal{D}$.*

PROOF. Let V be the solution space of L_P. Note that we can identify V with a direct summand of the vector space on which G acts via the permutation representation. We then have that G is Abelian if and only if $V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$ as a G-module, where $\dim(V_i) = 1$ for all $i \in \{1, \ldots, m\}$. We shall use the fact that $\mathcal{E}(L_P)$ is naturally isomorphic to $\mathrm{End}_G(V) = \mathrm{Hom}_G(V, V)$ where we consider V as a G-module (Singer, 1996).

Assume that G is Abelian. From the previous lemma, we have that the permutation representation is a direct sum of pairwise non-isomorphic one-dimensional G-modules. Therefore we may write $V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$, with the V_i pairwise non-isomorphic. Thus $\mathrm{End}_G(V) = \oplus_{i=1}^{m} \mathrm{End}_G(V_i)$. Since each $\mathrm{End}_G(V_i)$ is one-dimensional, we have that the maps $\pi_i : V \to V_i$ form a basis of $\mathrm{End}_G(V)$. Let $R_i \in \mathcal{E}(L_P)$ correspond to π_i. Since R_i has an $m-1$ dimensional kernel, the order or R_i is $m-1$. Since $\ker R_i \subset \ker(L_P)$, the operator R_i must divide L_P on the right, i.e. $L_P = S_i R_i$.

We now prove the converse. Let W be the sum of the one-dimensional subspaces $\mathrm{im}(R_i) \subset V$. If $W \neq V$, then $V = W \oplus \tilde{W}$. Consider the projection $\pi : V \to \tilde{W}$ and $R \in \mathcal{E}(L_P)$ be corresponding operator. Since the R_i form a basis of $\mathcal{E}(L_P)$ we have $R = \sum_{i=1}^{m} c_i R_i$, showing that $\mathrm{im}(R) = \tilde{W} \subset W$. Thus W is a direct sum of the one-dimensional subspaces $\mathrm{im}(R_i)$, showing that G is diagonalizable and thus Abelian. □

Although the above result can be made effective, it is not apparent that this approach leads to a polynomial time algorithm to decide if the Galois group is Abelian. Such an algorithm is known using other techniques (Lenstra, 1992, Corollary 3.3).

To compute the differential Galois group in our situation, we proceed using the idea of Singer and Ulmer (1993) and we use the fact that a finite group G is determined by its action on "constructions": symmetric and alternating products of the solution space, which are also 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 $\wedge^s(V)$).
2. The corresponding characters of G are denoted $\chi_L^{\circledS s}$ and $\chi_L^{\wedge s}$ and can be computed directly from χ_L.
3. Factorization 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 $\chi_L^{\wedge s}$. Computing exponential solutions allows us to find the order of the one-dimensional characters that appear in these decompositions.
4. Comparing the result with the tables below allows us to determine the group.

Tables 1–4 give the decomposition into irreducible characters of $\chi_P - \mathbf{1}$, where χ_P is the permutation character, for all the transitive permutation groups of degree 3 to 11 given in Conway *et al.* (1998). Similar tables can be constructed for every degree.

Some notation: 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 ith 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 $\chi_P - \mathbf{1}$. This approach will work for any degree: using a theorem due to Chevalley, for any finite subgroup H of $\mathrm{GL}_n(C)$, C an algebraically closed field, there is a faithful representation $\Phi : \mathrm{GL}_n(C) \to \mathrm{GL}_m(C)$ for some m such that $\Phi(H)$ is uniquely determined by its set of invariant subspaces in 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 Singer and Ulmer, 1993). Given a polynomial P irreducible over $\overline{k_0}(x)$, we first compute the differential equation $L_P = 0$ associated to it and determine the degrees of the irreducible factors of L_P. If the order of L_P is too small, we may not directly determine the Galois group of P using above tables, but after a transformation of the type described in Section 2, the order will become maximal.

Example 5.5. Consider the polynomial $P = y^4(y^4 - 8y^2 + 18) + 81x^2$ (from Malle and Matzat, 1999, p. 405, $f_{8,32}$) which is irreducible over $\overline{\mathbf{Q}}(x)$. Although the corresponding differential equation could have order 8, a calculation shows that it is

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

Table 1. Degree 3 to 6.

Degree 3

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

Degree 4

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

Degree 5

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

Degree 6

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

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

Table 2. Degree 7 and 8.

Degree 7

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

Degree 8

G	$C(8)$	$4[x]2$	$E(8)$	$D_8(8)$	$Q_8(8)$
$\mathcal{X}_P-\mathbf{1}$	$1_2,1_{4a},1_{4b},1_{8a},1_{8b},1_{8c},1_{8d}$	$1_{2a},1_{2b},1_{2c},1_{4a},1_{4b},1_{4c},1_{4d}$	$1_{2a},\dots,1_{2a}$	$1_{2a},1_{2b},1_{2c},2,2$	$1_{2a},1_{2b},1_{2c},2,2$
$2^{\wedge 2}$				1_2	$\mathbf{1}$

G	$E(8):2$	$Q_8:2$	$1/2[2^3]4$	$[2^2]4$
$\mathcal{X}_P-\mathbf{1}$	$1_{2a},1_{2b},1_{2c},2_a,2_b$	$1_{2a},1_{2b},1_{2c},2_a,2_b$	$1_2,1_{4a},1_{4b},2_a,2_b$	$1_2,1_{4a},1_{4b},2_a,2_b$
$2^{\wedge 2}$	1_2	1_2	1_4	1_2
$2^{\circledS 2}$	$\mathbf{1},1_{2a},1_{2b}$	$1_{2a},1_{2b},1_{2c}$	$1_{4a},1_{4b},1_{4c}$	$\mathbf{1},1_{2a},1_{2b}$

G	$D(8)$	$2D_8(8)$	$[4^2]^2$	$E(8):E_4$
$\mathcal{X}_P-\mathbf{1}$	$1_2,2_a,2_b,2_c$	$1_2,2_a,2_b,2_c$	$1_2,2_a,2_b,2_c$	$1_2,2_a,2_b,2_c$
$2_a^{\circledS 2},2_b^{\circledS 2}$	$\mathbf{1},2$	$1_2,2$	$1_4,2$	$\mathbf{1},1_{2a},1_{2b}$
$2_c^{\circledS 2}$	$\mathbf{1},1_{2a},1_{2b}$	$\mathbf{1},1_{2a},1_{2b}$	$\mathbf{1},1_{2a},1_{2b}$	$\mathbf{1},1_{2a},1_{2b}$

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

G	$[1/4\cdot cD(4)^2]2$	$E(8):4$	$1/2[2^4]eD(4)$	$1/2[2^4]dD(4)$	$E(8):D_8$	$1/2[2^4]cD(4)$	$[2^4]D(4)$
$\mathcal{X}_P-\mathbf{1}$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$	$1_2,2,4$
$4^{\wedge 4}$	$\mathbf{1}$	1_2	$\mathbf{1}$	1_2	1_2	1_2	1_2
$4^{\wedge 2}$	$1_{2a},1_{2b},1_{2c},1_{2d},2$	$1_{4a},1_{4b},2_a,2_b$	$1_{2a},1_{2b},2_a,2_b$	$2,4$	$2_1,2_b,2_c$	$1_{4a},1_{4b},4$	$2,4$
$4^{\circledS 2}$				$\mathbf{1},1_2,1_{4a},1_{4b},2,4$			$\mathbf{1},1_2,2_a,2_b,4$

Table 2. Continued.

G	$1/2[2^4]4$	$[2^3]4$	$1/2[2^4]E(4)$	$E(8):D_4$	$[2^4]4$	$[2^4]E(4)$
$\mathcal{X}_P-\mathbf{1}$	$1_2, 1_{4a}, 1_{4b}, 4$	$1_2, 1_{4a}, 1_{4b}, 4$	$1_{2a}, 1_{2b}, 1_{2c}, 4$	$1_{2a}, 1_{2b}, 1_{2c}, 4$	$1_2, 1_{4a}, 1_{4b}, 4$	$1_{2a}, 1_{2b}, 1_{2c}, 4$
$4^{\wedge 4}$	$\mathbf{1}$	1_2	1_2	$\mathbf{1}$	1_2	1_2
$4^{\wedge 2}$	$1_{2a}, 1_{2b}, 2_a, 2_b$	$1_{4a}, 1_{4b}, 2_a, 2_b$	$1_{4a}, 1_{4b}, 2, 2$	$1_{2a}, \ldots, 1_{2f}$	$2, 4$	$2_a, 2_b, 2_c$

G	$GL(2,3)$	$[2^3]A(4)$	$[2^4]A(4)$	$[2^3]S(4)$	$1/2[2^4]S(4)$	$[2^4]S(4)$
$\mathcal{X}_P-\mathbf{1}$	$3, 4$	$3, 4$	$3, 4$	$3, 4$	$3, 4$	$3, 4$
$4^{\wedge 4}$	$\mathbf{1}$	$\mathbf{1}$	1_2	1_2	$\mathbf{1}$	1_2
$3^{\wedge 3}$	1_2	$\mathbf{1}$	$\mathbf{1}$	1_2	1_2	1_2
$4^{\wedge 2}$	$1_2, 2, 3$	$3_a, 3_b$	6	6	$3_a, 3_b$	6
$4^{\circledS 2}$			$\mathbf{1}, 3, 6$	$\mathbf{1}, 3_a, 3_b, 3_c$		$\mathbf{1}, 3, 6$

G	$E(8):A_4$	$E(4)^2:D_6$	$E(8):S_4$	$[A(4)^2]2$	$[1/2\cdot S(4)^2]2$	$1/2[S(4)^2]2$	$[S(4)^2]2$
$\mathcal{X}_P-\mathbf{1}$	$1_2, 6$	$1_2, 6$	$1_2, 6$	$1_2, 6$	$1_2, 6$	$1_2, 6$	$1_2, 6$
$6^{\wedge 2}$	$3, 6_a, 6_b$	$3_a, 3_b, 3_c, 6$	$3, 6_a, 6_b$	$6, 9$	$6, 9$	$6, 9$	$6, 9$
$3^{\circledS 2}$	$\mathbf{1}, 1_{3a}, 1_{3b}, 3$		$\mathbf{1}, 2, 3$				
$6^{\circledS 2}$				$\mathbf{1}, 1_2, 2_a, 2_b, 6, 9$	$\mathbf{1}, 1_2, 4, 6, 9$	$\mathbf{1}, 1_2, 4, 6, 9$	$\mathbf{1}, 1_2, 4, 6, 9$
$4^{\wedge 2}$					$1_{2a}, 1_{2b}, 2_a, 2b$	$1_{4a}, 1_{4b}, 4$	$2, 4$

G	$E(8):7=F_{56}(8)$	$E(8):F_{21}$	$PSL(2,7)$	$PGL(2,7)$	$E(8):L_7=AL(8)$	$A(8)$	$S(8)$
$\mathcal{X}_P-\mathbf{1}$	7	7	7	7	7	7	7
$7^{\wedge 7}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	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	
$7^{\circledS 2}$					$\mathbf{1}, 6, 7, 14$	$\mathbf{1}, 7, 20$	

Table 3. Degree 9.

G	$C(9)$	$E(9)$	$S(3)[x]3$	$D(9)$	$S(3)[1/2]S(3)$
$\mathcal{X}_P - \mathbf{1}$	$1_{3a}, 1_{3b}, 1_{9a}, \ldots, 1_{9f}$	$1_{3a}, \ldots, 1_{3h}$	$1_{3a}, 1_{3b}, 2_a, 2_b, 2_c$	$2_a, 2_b, 2_c, 2_d$	$2_a, 2_b, 2_c, 2_d$
$2_a^{\circledS 3}$				$\mathbf{1}, 1_2, 2$	$\mathbf{1}, 1_2, 2$
$2_b^{\circledS 3}$				$2_a, 2_b$	$\mathbf{1}, 1_2, 2$

G	$1/3[3^3]3$	$E(9):3$	$[3^3]3$	$S(3)[x]S(3)$	$E(9):4$	$E(9):D_8$
$\mathcal{X}_P - \mathbf{1}$	$1_{3a}, 1_{3b}, 3_a, 3_b$	$1_{3a}, 1_{3b}, 3_a, 3_b$	$1_{3a}, 1_{3b}, 3_a, 3_b$	$2_a, 2_b, 4$	$4_a, 4_b$	$4_a, 4_b$
$3^{\wedge 3}$	1_3	$\mathbf{1}$	1_3			
$3^{\circledS 2}$	$3, 3$		$3_a, 3_b$			
$4^{\wedge 2}$					$1_{2a}, 1_{2b}, 4$	$2, 4$

G	$[3^2]S(3)$	$[3^3]S(3)$	$E(9):D_6$	$[3^3:2]3$	$[1/2\cdot S(3)^3]3$	$[S(3)^3]3$
$\mathcal{X}_P - \mathbf{1}$	$2, 3_a, 3_b$	$2, 3_a, 3_b$	$1_{3a}, 1_{3b}, 6$	$1_{3a}, 1_{3b}, 6$	$1_{3a}, 1_{3b}, 6$	$1_{3a}, 1_{3b}, 6$
$3^{\wedge 3}$	1_2	1_6				
$6^{\wedge 6}$			1_2	1_2	$\mathbf{1}$	1_2
$6^{\wedge 2}$			$1_2, 1_{6a}, 1_{6b}, 2_a, 2_b, 2_c, 6$	$1_2, 1_{6a}, 1_{6b}, 6_a, 6_b$		$3, 12$

G	$[3^2]S(3)_6$	$E(9):6$	$E(9):D_{12}$	$1/2\cdot[3^3:2]S(3)$
$\mathcal{X}_P - \mathbf{1}$	$2, 6$	$2, 6$	$2, 6$	$2, 6$
$6^{\wedge 2}$	$1_2, 1_{6a}, 1_{6b}, 2_a, 2_b, 2_c, 6$	$1_2, 1_{6a}, 1_{6b}, 2_a, 2_b, 2_c, 6$	$1_2, 2_a, 2_b, 4, 6$	$1_2, 2, 3_a, 3_b, 6$
$6^{\wedge 3}$	$2, 6^3$	$\mathbf{1}, 1_2, 6^3$		

G	$[3^3:2]S(3)$	$[1/2\cdot S(3)^3]S(3)$	$1/2[S(3)^3]S(3)$	$[S(3)^3]S(3)$
$\mathcal{X}_P - \mathbf{1}$	$2, 6$	$2, 6$	$2, 6$	$2, 6$
$6^{\wedge 2}$	$1_2, 2, 6, 6$	$3, 12$	$3, 12$	$3, 12$
$6^{\wedge 6}$		$\mathbf{1}$	1_2	1_2
$3^{\wedge 3}$			$\mathbf{1}$	1_2

G	$M(9)$	$E(9):8$	$E(9):2D_8$	$E(9):2A_4$	$E(9):2S_4$	$L(9)$
$\mathcal{X}_P - \mathbf{1}$	8	8	8	8	8	8
$8^{\wedge 8}$	$\mathbf{1}$	1_2	1_2	$\mathbf{1}$	1_2	$\mathbf{1}$
$8^{\wedge 2}$	$2, 2, 8, 8, 8$	$1_{8a}, 1_{8b}, 1_{8c}, 1_{8d}, 8^3$	$2_a, 2_b, 8_a, 8_b^2$	$2_a, 2_b, 8_a, 8_b, 8c$	$4, 8, 16$	$7_a, 7_b, 7_c, 7_d$

G	$L(9):3$	$A(9)$	$S(9)$
$\mathcal{X}_P - \mathbf{1}$	8	8	8
$8^{\wedge 8}$	$\mathbf{1}$	$\mathbf{1}$	1_2
$8^{\wedge 2}$	$7, 21$	28	28

Using the eigenring, we can show that it is irreducible. Therefore the permutation representation has an irreducible summand of dimension 4. According to Table 2, the Galois group G of P over $\overline{\mathbf{Q}}(x)$ belongs to a family of 19 groups (from $[1/4\cdot cD(4)^2]2$ to $[2^4]S(4)$). The fourth exterior power of L_P 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 seven possible groups. The second exterior power of L_P is of order 6 and factors as a product of two irreducible differential equations of order 3, where one is

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

Therefore, the Galois group G of P over $\overline{\mathbf{Q}}(x)$ is either $[2^3]A(4)$ or $1/2[2^4]S(4)$. The third exterior power of L_3 has $\frac{(5x^2-1)}{x^2(1+3x^2)^4}$ as a rational solution, so G is $[2^3]A(4)$. □

Table 4. Degree 10 and 11.

G	$C(10)$	$D(10)$	$D_{10}(10)$	$[5^2]2$
$\mathcal{X}_P - \mathbf{1}$	$1_2, 1_{5a}, 1_{5b}, 1_{5c}, 1_{5d}, 1_{10a}, 1_{10b}, 1_{10c}, 1_{10d}$	$1_2, 2_a^2, 2_b^2$	$1_2, 2_a, 2_b, 2_c, 2_d$	$1_2, 2_a, 2_b, 2_c, 2_d$
$2^{\mathbb{S}2}$			$\mathbf{1}, 2$	$1_5, 2$

G	$1/2[F(5)]2$	$[2^4]5$	$[2^5]5$	$[2^4]D(5)$	$1/2[2^5]D(5)$	$[2^5]D(5)$
$\mathcal{X}_P - \mathbf{1}$	$1_2, 4^2$	$1_{5a}, 1_{5b}, 1_{5c}, 1_{5d}, 5$	$1_{5a}, 1_{5b}, 1_{5c}, 1_{5d}, 5$	$2_a, 2_b, 5$	$2_a, 2_b, 5$	$2_a, 2_b, 5$
$5^{\wedge 5}$		$\mathbf{1}$	1_2	$\mathbf{1}$	1_2	1_2
$5^{\wedge 3}$					$5_a, 5_b$	$5_a, 5_b$
$5_a^{\wedge 5}, 5_b^{\wedge 5}$					$\mathbf{1}$	1_2

G	$F(5)[x]2$	$[1/2 \cdot D(5)^2]2$	$1/2[D(5)^2]2$	$A(5)[x]2$	$1/2[S(5)]2$	$[D(5)^2]2$	$S(5)[x]2$
$\mathcal{X}_P - \mathbf{1}$	$1_2, 4_a, 4_b$	$1_2, 4_a, 4_b$	$1_2, 4_a, 4_b$	$1_2, 4_a, 4_b$	$1_2, 4_a, 4_b$	$1_2, 4_a, 4_b$	$1_2, 4_a, 4_b$
$4^{\wedge 4}$	1_2	$\mathbf{1}$	1_2	$\mathbf{1}$	1_2	1_2	1_2
$4^{\wedge 2}$	$1_{4a}, 1_{4b}, 4$	$1_{2a}, 1_{2b}, 2_a, 2b$	$1_{4a}, 1_{4b}, 4$	$3_a, 3_b$	6	$2, 4$	6
$4^{\mathbb{S}2}$	$\mathbf{1}, 1_2, 4^2$		$\mathbf{1}, 1_2, 4_a, 4_b$				
$6^{\wedge 2}$					$4_a, 5, 6$		$4_c, 5, 6$

G	$A_5(10)$	$S_5(10d)$	$[2^4]F(5)$	$1/2[2^5]F(5)$	$[2^5]F(5)$
$\mathcal{X}_P - \mathbf{1}$	$4, 5$	$4, 5$	$4, 5$	$4, 5$	$4, 5$
$4^{\wedge 4}$	$\mathbf{1}$	1_2	1_2	1_2	1_2
$5^{\wedge 5}$	$\mathbf{1}$	$\mathbf{1}$	1_2	$\mathbf{1}$	1_2
$4^{\wedge 2}$	$3_a, 3_b$	6	$1_{4a}, 1_{4b}, 4$	$1_{4a}, 1_{4b}, 4$	$1_{4a}, 1_{4b}, 4$
$5^{\wedge 2}$	$3_a, 3_b, 4$	$4, 6$			
$5^{\mathbb{S}5}$			$\mathbf{1}, 5^{15}, 10^5$		$1_2, 5^{15}, 10^5$

G	$[2^4]A(5)$	$[2^5]A(5)$	$[2^4]S(5)$	$1/2[2^5]S(5)$	$[2^5]S(5)$
$\mathcal{X}_P - \mathbf{1}$	$4, 5$	$4, 5$	$4, 5$	$4, 5$	$4, 5$
$4^{\wedge 4}$	$\mathbf{1}$	$\mathbf{1}$	1_2	1_2	1_2
$5^{\wedge 5}$	$\mathbf{1}$	1_2	1_2	$\mathbf{1}$	1_2
$4^{\wedge 2}$	$3_a, 3_b$		6	6	6
$5^{\wedge 2}$	10			10	
$5^{\mathbb{S}2}$			$\mathbf{1}, 5^4, 10^4, 15^3, 20$		$1_2, 5^4, 10^4, 15^3, 20$

G	$[5^2:4]^2$	$[5^2:4]2_2$	$[5^2:4_2]2$	$[5^2:4_2]2_2$
$\mathcal{X}_P - \mathbf{1}$	$1_2, 8$	$1_2, 8$	$1_2, 8$	$1_2, 8$
$8^{\wedge 8}$	$\mathbf{1}$	1_2	$\mathbf{1}$	$\mathbf{1}$
$8^{\wedge 2}$	$1_{4a}, 1_{4b}, 1_{4c}, 1_{4d}, 4_a, 4_b, 8_a, 8_b$	$1_{8a}, 1_{8b}, 1_{8c}, 1_{8d}, 8_a, 8_b, 8_c$	$2^2, 4_a, 4_b, 4_c, 4_d, 8$	$2^2, 8_a, 8_b, 8_c$

G	$[1/2 \cdot F(5)^2]2$	$1/2[F(5)^2]2$	$[F(5)^2]2$	$[A(5)^2]2$	$[1/2 \cdot S(5)^2]2$	$1/2[S(5)^2]2$	$[S(5)^2]2$
$\mathcal{X}_P - \mathbf{1}$	$1_2, 8$	$1_2, 8$	$1_2, 8$	$1_2, 8$	$1_2, 8$	$1_2, 8$	$1_2, 8$
$8^{\wedge 8}$	$\mathbf{1}$	1_2	1_2	$\mathbf{1}$	$\mathbf{1}$	1_2	1_2
$8^{\wedge 2}$	$2_a, 2_b, 8_a, 8_b, 8_c$	$2_a, 2_b, 8, 16$	$2_a, 2_b, 8, 16$	$6_a, 6_b, 16$	$12, 16$	$12, 16$	$12, 16$
$2^{\mathbb{S}2}$		$1_{4a}, 1_{4b}, 1_{4c}$	$1_4, 2$				
$8^{\wedge 4}$						$1_4^2, 16^2, 36$	$2, 32, 36$

G	$L(10)$	$L(10):2$	$M(10)$	$S_6(10)$	$L(10) \cdot 2^2$	$A(10)$	$S(10)$
$\mathcal{X}_P - \mathbf{1}$	9	9	9	9	9	9	9
$9^{\wedge 9}$	$\mathbf{1}$	1_2	$\mathbf{1}$	1_2	1_2	$\mathbf{1}$	1_2
$9^{\wedge 2}$	$10^2, 8_a, 8_b$	$8_a, 8_b, 10_a, 10_b$	$10_a, 10_b, 16$	$10_a, 10_b, 16$	$16, 20$	36	36

Degree 11

G	$C(11)$	$D(11)$	$F_{55}(11)$	$F_{110}(11)$	$L(11)$	$M(11)$	$A(11)$	$S(11)$
$\mathcal{X}_P - \mathbf{1}$	$1_{11a}, \ldots, 1_{11j}$	$2_a, \ldots, 2_e$	$5_a, 5_b$	10	10	10	10	10
$10^{\wedge 10}$				1_2	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	1_2
$10^{\wedge 2}$				$1_2, 1_{10}^4, 10^4$	$10, 11, 12^2$	45	45	45
$10^{\wedge 3}$						$10^2, 45, 55$	120	

If in the degree 6 case, one obtains a decomposition of the permutation character of $D_6(6)$ or $D(6)$ (assuming L_P is of order 4, i.e. contains no linear characters), this means that in the latter case L_P is the product of two irreducible isomorphic equations of order 2 and in the former case L_P is the product of two irreducible non-isomorphic equations of order 2. We can distinguish the two cases using the eigenring: 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 Singer (1996)) 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 5.6. (Example 2.6 continued) We wish to find the Galois group of the polynomial $P(x, y) = y^2(y^2 + 3)^2 + 4x$, which is irreducible over $\overline{Q}(x)$. In Example 2.6 we have considered the transformed polynomial $\tilde{P}_1 = y^6 P(x - 2, \frac{1}{y} + 1)$ whose roots are linearly independent over $\overline{Q}$ and whose linear associated differential equation $L_{\tilde{P}_1}$ has been computed in Example 2.7. The latter one is of order 6 and factors into two equations of order 1 and two irreducible equations L_1 and L_2 of order 2. Hence, G is equal to $D_6(6)$, $D(6)$ or $F_{18}(6)$. We have

$$L_1(y) = y'' + \frac{-69x^2 + 150x - 128 + 12x^3}{2(3x^4 - 13x^3 + 52x - 48)} y' + \frac{6x^2 + 28x - 103}{9(3x^4 - 13x^3 + 52x - 48)} y$$

$$L_2(y) = \frac{108x^5 - 1677x^4 + 10869x^3 - 21188x^2 - 2084x + 21824}{2(x-2)(3x-4)(x+2)(x-3)(3x^2 - 33x + 142)} y'$$
$$+ \frac{-19384056x^2 + 15839360x^3 + 10963312x + 5967x^7 - 136744x^6 + 1372731x^5 - 6551430x^4 - 2195328}{36(x-2)^2(3x-4)^2(x+2)(x-3)^2(3x^2 - 33x + 142)} y$$

The LCLM of L_1 and L_2 is of degree 4 and its eigenring is of dimension 2, so G is equal to $D(6)$ or $F_{18}(6)$. The second symmetric power of L_1 has a rational solution $\frac{3x-10}{3(x+2)^2}$ so $G_{\overline{Q}(x)} = D(6)$. □

5.2. Galois group over $k_0(x)$

As mentioned before, our approach computes the geometric Galois group G of P over $\overline{k_0}(x)$. This is due to the fact that in order to apply the differential Galois theory, one must assume that the field of constants is algebraically closed. Of course, the Galois group over $k_0(x)$ may be larger than the Galois group over $\overline{k_0}(x)$. We will refer to the former group as $G_{k_0(x)}$ (the arithmetic Galois group) and the latter group as $G_{\overline{k_0}(x)}$. We always have $G_{\overline{k_0}(x)} \subset G_{k_0(x)}$. Note that the resolvent method (see Matzat *et al.*, 2000) also gives a method to compute the arithmetic Galois group of P over $k_0(x)$ (see Mattman and McKay, 0000).

Example 5.7. Consider $P(y) = y^3 - x \in \mathbf{Q}(x)[y]$. The roots of $P(y) = 0$ 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. One checks that $G_{\mathbf{Q}(x)} = S(3)$ and that $G_{\overline{\mathbf{Q}}(x)} = A(3)$. Note that the splitting field $\mathbf{Q}(x)(z_1, z_2, z_3)$ contains the new constant $\xi = z_2/z_1$ and $2 = [\mathbf{Q}(\xi) : \mathbf{Q}] = |S(3) : A(3)|$. □

The previous example illustrates the fact that the groups $G_{k_0(x)}$ and $G_{\overline{k_0}(x)}$ are distinct precisely when the splitting field of P over $k_0(x)$ contains new constants. This observation will be the basis of the technique we will use to calculate $G_{k_0(x)}$ (and is very similar to

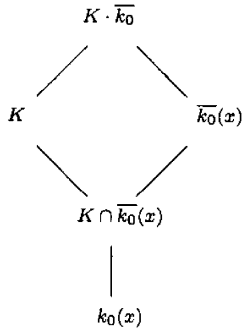
the idea behind Duval's algorithm to find an absolutely irreducible factor, as well as our modification). The key result is the following lemma.

LEMMA 5.8. *Let K be an algebraic extension of $k_0(x)$ and $\overline{k_0}$ be the algebraic closure of k_0. We then have that*

$$[K : k_0(x)] = [K \cdot \overline{k_0} : \overline{k_0}(x)][K \cap \overline{k_0} : k_0]$$

where $K \cdot \overline{k_0}$ is the compositum of K and $\overline{k_0}$ in the algebraic closure of K.

PROOF. Consider the following diagram:



Since $[K : k_0(x)] = [K : K \cap \overline{k_0}(x)][K \cap \overline{k_0}(x) : k_0(x)]$, it is enough to show that $[K \cap \overline{k_0}(x) : k_0(x)] = [K \cap \overline{k_0} : k_0]$ and $[K : K \cap \overline{k_0}(x)] = [K \cdot \overline{k_0} : \overline{k_0}(x)]$.

To prove the first equality, let $\{\alpha_i\}$ be k_0-basis of $K \cap \overline{k_0}$. To show that this set spans the $k_0(x)$ vector space $K \cap \overline{k_0}(x)$, it is enough to show that any polynomial $p \in K \cap \overline{k_0}(x)$ must lie in $(K \cap \overline{k_0})[x]$. We proceed to show this by induction on the degree of P. Differentiating with respect to x we see that all the coefficients of the nonzero powers of x must lie in $K \cap \overline{k_0}$ and so the constant coefficient must also lie in this field. To see that the set $\{\alpha_i\}$ is linearly independent over $k_0(x)$, let $\sum_i f_i(x)\alpha_i = 0$, with $f_i \in k_0(x)$. We then have $f_i(a) = 0$ for all elements $a \in k_0$ that are not poles of the f_i. Since this is an infinite set, we have that all the $f_i = 0$ and so $\{\alpha_i\}$ is a $k_0(x)$-basis of $K \cap \overline{k_0}(x)$.

We now prove the second equality. Note that since $K \cap \overline{k_0}$ is algebraically closed in K, we have that any elements of K, linearly independent over $K \cap \overline{k_0}$ remain linearly independent over $\overline{k_0}$ (see Lang, 1993, Chapter VIII. 4). Let $\{e_i\}_{i=0}^{\infty}, e_0 = 1$, be a $K \cap \overline{k_0}$-basis of $K \cap \overline{k_0}(x)$, and $\{f_i\}_{i=0}^{m}$, $f_0 = 1$, be a $K \cap \overline{k_0}(x)$-basis of K. Since $\{e_i f_j\}$ is a $K \cap \overline{k_0}$-basis of K and $\{e_i\}_{i=0}^{\infty}, e_0 = 1$, is a $\overline{k_0}$-basis of $\overline{k_0}(x)$, we have that $\{f_i\}_{i=0}^{m}$ is a $\overline{k_0}(x)$-basis of $K\overline{k_0}$. □

COROLLARY 5.9. *Let K be the splitting field of a polynomial $P \in k_0(x)[y]$ over $k_0(x)$. Then $|G_{k_0(x)}| = |G_{\overline{k_0}(x)}|[K \cap \overline{k_0} : k_0]$.*

We note that the above lemma is also partly a consequence of Theorem 1.12 of Lang (1993, Chapter VI, Section 1) and can also be used to justify the key fact behind Duval's algorithm.

For the rest of this section, we assume that $P \in k_0[x, y]$ and is absolutely irreducible. Note that in this case $G_{\overline{k_0}(x)}$ is a transitive normal subgroup of the transitive group $G_{k_0(x)}$. From Table 5 we see that, in most cases, there are only very few possibilities of

Table 5. Transitive groups G and their 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		$C(2)$	$C(3)$	$C(6)$	$C(3)$	$C(2)$			$C(2)$

$G_{k_0(x)}$ once $G_{\overline{k_0}(x)}$ is known. Table 5 illustrates 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.

Suppose that we have computed $G_{\overline{k_0}(x)}$ via the previous section. We now fix a possible group G for $G_{k_0(x)}$ having $G_{\overline{k_0}(x)}$ as proper normal subgroup and want to decide, using differential Galois theory, if $G = G_{k_0(x)}$. By Corollary 5.9 we know that if $G = G_{k_0(x)} \neq G_{\overline{k_0}(x)}$ then the extension $k_0(x)(y_1, \ldots, y_n)$ of $k_0(x)$ contains new constants. The method we propose is not an algorithm but does give results in many cases.

We consider a tentative $k_0(x)$-basis $\mathcal{B} = \{b_1 = 1, b_2, \ldots, b_{|G|}\}$ (which we suppose given) of $|G|$ elements of $k_0(x)(y_1, \ldots, y_n)$ over $k_0(x)$ and write $z = \sum_{i=1}^{|G|} u_i b_i$ with $u_i \in k_0(x)$. 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 $k_0(x)$, which can be decided using Barkatou (1999) and Bronstein (1992).[†] There are three possible outcomes:

- The system $\mathcal{S}$ has no non-trivial rational solution. In this case, $G_{k_0(x)} \neq G$. If G is the only candidate, different from $G_{\overline{k_0}(x)}$ for $G_{k_0(x)}$, then we have $G_{k_0(x)} = G_{\overline{k_0}(x)}$.
- The system has a nontrivial rational solution and we have determined that this does not correspond to a new constant. We can then conclude that the putative basis $\mathcal{B}$ is not a basis and thus $G_{k_0(x)} \neq G$. Again, if G is the only candidate different from $G_{\overline{k_0}(x)}$ for $G_{k_0(x)}$ then $G_{k_0(x)} = G_{\overline{k_0}(x)}$ (see Example 5.14).
- The system $\mathcal{S}$ has a nontrivial rational solution and we have determined that this corresponds to a new constant $\gamma \in \overline{k_0} \setminus k_0$ (we discuss methods for this below). We then conclude that $G_{k_0(x)} \neq G_{\overline{k_0}(x)}$ and the index of $G_{\overline{k_0}(x)}$ in $G_{k_0(x)}$ is bounded from below by the degree of γ. In some cases this is enough to determine $G_{k_0(x)}$ (see Example 5.15).

[†]It is important to note that those algorithms work over $k_0(x)$.

This approach raises the questions of finding a tentative $k_0(x)$-basis in an efficient way and of determining if a rational solution of the resulting differential system corresponds to a new constant. The first task can be done for the symmetric groups S_m and the alternating groups A_m, due to the fact that those groups are respectively $m-1$ and $m-2$ transitive groups of degree m. The multiple transitivity allows us in both cases to set up a basis by choosing arbitrary roots y_i of P (see the proof of the next lemma). This can be done for a larger class of groups. Recall that a *Frobenius group* is a transitive subgroup of some symmetric group such that the only group element leaving two elements fixed is the identity.

LEMMA 5.10. *If the Galois group $G_{k_0(x)} \in S_m$ over $k_0(x)$ is an s-transitive group and if the identity is the only element of $G_{k_0(x)}$ that leaves $s+1$ elements fixed, then by choosing arbitrary roots $y_1, \ldots, y_{s+1}$ of P, we get a $k_0(x)$-basis of the splitting field of P by multiplying all elements in the basis*

$$\{1, y_1, \ldots, y_1^{m-1}, y_2, y_2y_1, \ldots, y_2y_1^{m-1}, \ldots, y_s^{m-s} \ldots y_2^{m-2}y_1^{m-1}\}$$

of $k_0(x)(y_1, \ldots, y_s)/k_0(x)$ and the basis $\{1, y_{s+1}, \ldots, y_{s+1}^{\lambda-1}\}$ of $k_0(x)(y_1, \ldots, y_s)(y_s+1)$ over $k_0(x)(y_1, \ldots, y_s)$ where $\lambda \in \mathbf{N}$ is such that $\lambda \cdot m(m-1)\cdots(m-s+1)$ is the order of $G_{k_0(x)}$.

In particular, for $s=1$ this includes the case where $G_{k_0(x)}$ is a Frobenius group, for $s=2$ this includes the Zassenhaus groups (Gorenstein, 1968) and for $s=m-1$ and $s=m-2$ this includes the symmetric group S_m and the alternating group A_m.

PROOF. We proceed by induction. Let $s=1$. Since $G_{k_0(x)}$ is transitive a basis of $k_0(x)(y_1)/k_0(x)$ is $\{1, y_1, \ldots, y_1^{m-1}\}$. Let $y_2 \neq y_1$ be a second root of P and denote K the splitting field of P over $k_0(x)$. The Galois group of $K/k_0(x)(y_1, y_2)$ is a subgroup of $G_{k_0(x)}$ whose elements leave y_1 and y_2 fixed. This group must be trivial by assumption and thus $K = k_0(x)(y_1, y_2)$. The degree of $k_0(x)(y_1, y_2)/k_0(x)(y_1)$ is $\lambda = |G_{k_0(x)}|/m$ showing that a $k_0(x)(y_1)$-basis of K is $\{1, y_2, \ldots, y_2^{\lambda-1}\}$. Putting both bases together as above yields a $k_0(x)$-basis of K and gives the result.

Assume that the result holds until $s=n-1$ and consider $s=n>1$. Since $G_{k_0(x)}$ is transitive the basis of $k_0(x)(y_1)/k_0(x)$ is $\{1, y_1, \ldots, y_1^{m-1}\}$. The Galois group of $K/k_0(x)(y_1)$ is the stabilizer G_{y_1} of y_1. Since $s=n>1$ $G_{k_0(x)}$ is 2-transitive and the polynomial $P_{y_1} = P/(Y-y_1)$ is absolutely irreducible over $k_0(x)(y_1)$. Its Galois group G_{y_1} operates on the roots of P_{y_1} as a permutation group of the $m-1$ remaining roots. Since G_{y_1} is $(s-1)$-transitive and the identity is the only element of G_{y_1} that leaves s elements fixed, we get a $k_0(x)(y_1)$-basis of K by induction. Putting both bases together to get a $k_0(x)$-basis gives the result.

The Frobenius groups satisfy the above conditions for $s=1$ and the symmetric S_m and the alternating groups A_m, due to the fact that those groups are respectively $m-1$ and $m-2$ transitive groups of degree m, also satisfy the above conditions for $s=m-1$ and $s=m-2$. □

If the group G is of the above type (s-transitive and the identity is the only element that leaves $s+1$ elements fixed), then if the group is of order $m\cdot(m-1)\cdots(m-(s-1))$ it is also easy not only to set up a basis but also a multiplication table for the splitting field (for larger groups this would involve some choices of elements).

EXAMPLE 5.11. Suppose that the Galois group $G_{\mathbf{Q}(x)}$ of $g = y^5 + \sum_{i=1}^{4} a_i y_1 \in \mathbf{Q}(x)[y]$ is the Frobenius group $F(5)$ of order $20 = 5 \cdot 4$. Since the assumptions of the above lemma are verified for $s = 2$, a $\mathbf{Q}(x)$-basis of the splitting field is $\mathcal{B} = \{1, y_2, y_2^2, y_2^3, y_1, y_1y_2, y_1y_2^2, y_1y_2^3, y_1^2, y_1^2y_2, y_1^2y_2^2, y_1^2y_2^3, y_1^3, y_1^3y_2, y_1^3y_2^2, y_1^3y_2^3, y_1^4, y_1^4y_2, y_1^4y_2^2, y_1^4y_2^3\}$ where y_1, y_2 are distinct roots of g. In order to multiply elements in the splitting field we use g, the minimal polynomial of y_1 over $\mathbf{Q}(x)$, and

$$g_1(y) = y^4 + (y_1 + a_4)y^3 + (y_1^2 + y_1a_4 + a_3)y^2 + (y_1^3 + y_1^2a_4 + y_1a_3 + a_2)y + (y_1^4 + y_1^3a_4 + y_1^2a_3 + y_1a_2 + a_1)$$

the minimal polynomial of y_2 over $\mathbf{Q}(x)(y_1)$. □

We now turn to the second task. Since we are only dealing with a *putative* basis, once we have a nontrivial rational solution of the associated system, we need to determine if it actually corresponds to a new constant. We can do this, *in theory*, using the following lemma.

LEMMA 5.12. *Let $y_1, \ldots, y_n$ be solutions of $L_P(y) = 0$, $s \in \mathbf{N}$ and $u_1, \ldots, u_{|G|} \in k_0(x)$. One can determine a point $\alpha \in k_0$ and a bound $M \in \mathbf{N}$, depending on $\alpha, s, u_1, \ldots, u_{|G|}$ and $y_1, \ldots, y_n$, such that $z = \sum_{i=1}^{|G|} u_i b_i \in \overline{k_0}$ (where the b_i are monomials in y_j) if and only if the coefficients of $x - \alpha, (x - \alpha)^2, \ldots, (x - \alpha)^M$ 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 $L_1(y) = 0$ satisfied by z (Singer, 1979). Now 1 (and thus any element of $\overline{k_0}$) and z are both solutions of the LCLM $L_3(y)$ 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 $L_3(y)$. 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. □

To apply the preceding lemma, one needs to construct the differential operator L_3, a process which is likely to be expensive. An alternative approach is to use Fuchs's relation to obtain upper bounds for the exponents at possible "true" and apparent singularities and then select a point α and use Taylor series expansions at this point. This can be done since we know (from the Newton polygon of P) lower bounds on the exponents that can occur in power products of roots of P and we will have a basis of the solutions space of $\mathcal{S}$. We will not describe this process in detail but rather work out a specific example (see Example 5.15).

EXAMPLE 5.13. Consider the equation $P(y) = y^3 - x$ over $\overline{\mathbf{Q}}(x)$. We will prove that its Galois group over $\overline{\mathbf{Q}}(x)$ is $A(3)$ and over $\mathbf{Q}(x)$ is $S(3)$.

First, we consider the transformed polynomial $P_1 = y^3P(1/y + 1) = (1 - x)y^3 + 3y^2 + 3y + 1$. The differential equation associated to P_1 is

$$L_{P_1}(y) = y''' + \frac{5x - 2}{x(x - 1)}y'' + \frac{2(19x - 1)}{9x^2(x - 1)}y' + \frac{2}{9x^2(x - 1)}y = 0.$$

As L_{P_1} is the product of the three linear operators $\delta + \frac{1}{x-1}$, $\delta + \frac{5x-2}{3x(x-1)}$ and $\delta + \frac{7x-4}{3x(x-1)}$, the Galois group of P_1 over $\overline{\mathbf{Q}}(x)$ is $A(3)$.

Let y_1, y_2 and y_3 denote the roots of P_1 and suppose that $\{1, y_1, y_2, y_1y_2, y_1^2, y_2y_1^2\}$ is a basis of $\mathbf{Q}(x)(y_1, y_2, y_3)$. 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 $\mathcal{S}_1$:

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

Using the algorithm presented in Barkatou (1999), we find that the differential system $\mathcal{S}_1$ admits the rational solutions: $u_0 = \lambda_1 + \frac{1}{x}\lambda_0$, $u_1 = \frac{x+2}{x}\lambda_0$, $u_2 = \frac{1-x}{x}\lambda_0$, $u_3 = 2u_2$, $u_4 = u_2$ and $u_5 = \frac{(x-1)^2}{x}\lambda_0$, where λ_0 and λ_1 are constants. Computing the Puiseux expansions of P_1 at $x = 0$, we take $y_1 = \frac{1}{x-1}(1 + x^{1/3} + x^{2/3})$ and $y_2 = \frac{1}{2(x-1)}(2 + (-1 - I\sqrt{3})x^{1/3} + (-1 + I\sqrt{3})x^{2/3})$. Since we have explicit expressions for y_1 and y_2 we find that (for $\lambda_0 = 1, \lambda_1 = 0$) $z = \frac{1}{x} + \frac{x+2}{x}y_1 + \frac{1-x}{x}y_2 + \frac{2(1-x)}{x}y_1y_2 + \frac{1-x}{x}y_1^2 + \frac{(x-1)^2}{x}y_2y_1^2$ is $\frac{1}{2}(-1 + I\sqrt{3})$. This new constant has degree 2 over $\mathbf{Q}$ so $G_{\mathbf{Q}(x)} = S(3)$. □

Example 5.14. Consider the polynomial

$$P = y^3 - (1 + 3x^2)(3y - 2)$$

(from Malle and Matzat, 1999, p. 404, $f_{3,1}$) which is irreducible over $\overline{\mathbf{Q}}(x)$. The differential equation associated to P is

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

and L_P 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 P over $\overline{\boldsymbol{Q}}(x)$ is $N = A(3)$.

Suppose that Galois group of P over $\mathbf{Q}(x)$ is $G = S(3)$. Thus, if y_1, y_2, y_3 are the roots of P, a basis for $\mathbf{Q}(x)(y_1, y_2, y_3)$ 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 $\mathcal{S}_2$:

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

This 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 the roots of P at $x = 1$ up to order 5 are

$$y = Z + \left(-\frac{2}{3} + \frac{5}{6}Z + \frac{1}{12}Z^2\right)(x - 1) + \frac{1}{12}Z(x - 1)^2$$

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

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 $z=-3-\frac{5}{32}(x-1)^5+O(x-1)^6$. This contradicts the fact that $\mathcal{B}$ is a basis over $\mathbf{Q}(x)$; so the Galois group of P over $\mathbf{Q}(x)$ is $N=A(3)$. □

Example 5.15. We consider the polynomial $P=y^5-5xy^4+50y^3-50xy^2+125y-25x$ (Malle, private communication). The differential equation associated to P is

$$L_P(y)=y^{(5)}+\frac{5(3x^2+1)}{x(x^2-5)}y^{(4)}+\frac{12(-1+5x^2)}{(x^2-5)^2}y^{(3)}+\frac{12(5x^4-8x^2-5)}{x(x^2-5)^3}y''$$
$$+\frac{384}{25(x^2-5)^4}y'-\frac{384}{25x(x^2-5)^4}y=0.$$

This equation admits a one-dimensional subspace of rational solutions (spanned by x), so P is absolutely irreducible. Since L_P factors completely into linear factors, we get from Table 1 that the Galois group of P over $\overline{\mathbf{Q}}(x)$ is the cyclic group $C(5)$. According to Table 5 its Galois group over $\mathbf{Q}(x)$ is either $C(5)$, $D(5)$ or $F(5)$.

Suppose it is $F(5)$. Since $F(5)$ is Frobenius of order $20=5\cdot 4$, a tentative $\mathbf{Q}(x)$-basis should be $\mathcal{B}=\{1,y_2,y_2^2,y_2^3,y_1,y_1y_2,y_1y_2^2,y_1y_2^3,y_1^2,y_1^2y_2,y_1^2y_2^2,y_1^2y_2^3,y_1^3,y_1^3y_2,y_1^3y_2^2,y_1^3y_2^3,y_1^4,y_1^4y_2,y_1^4y_2^2,y_1^4y_2^3\}$ where y_1 is any root of P and y_2 is another root of P whose minimal polynomial over $\mathbf{Q}(x)(y_1)$ is (see Example 5.11)

$$P_1(y)=y^4+(y_1-5x)y^3+(y_1^2-5xy_1+50)y^2+(y_1^3-5xy_1^2+50y_1-50x)y$$
$$+y_1^4-5xy_1^3+50y_1^2-50xy_1+125.$$

We can thus express any power y_2^n for $n\geq 4$ using y_1 and lower powers of y_2. Suppose that $z=\sum_{b_i\in\mathcal{B}}u_ib_i$ is a constant. Constructing the linear differential system $U'=\frac{1}{5}\mathcal{M}U$ associated to $z'=0$ (see the matrix $\mathcal{M}$ in Table 6), and computing the rational solutions, we obtain

$$u_0=\lambda_0+\frac{(60x\lambda_1+30x\lambda_2+25\lambda_3)}{x^2-5},\qquad u_1=\frac{(40x^2-300)\lambda_1+(15x^2-130)\lambda_2-13x\lambda_3}{x^2-5},$$
$$u_2=\frac{12x\lambda_1+7x\lambda_2+(3x^2-4)\lambda_3}{x^2-5},\qquad u_3=-\frac{20\lambda_1+10\lambda_2+3x\lambda_3}{5(x^2-5)},$$
$$u_4=-\frac{(95x^2-300)\lambda_1+(45x^2-130)\lambda_2+13x\lambda_3}{x^3-5},\qquad u_5=-\frac{-43x\lambda_1-30x\lambda_2+(8x^2-73)\lambda_3}{x^2-5},$$
$$u_6=-\frac{(25x^2-60)\lambda_1+(20x^2-25)\lambda_2+27x\lambda_3}{5(x^2-5)},\qquad u_7=\frac{5x\lambda_1+4x\lambda_2+7\lambda_3}{5(x^2-5)},$$
$$u_8=\frac{39x\lambda_1+23x\lambda_2+(3x^2-4)\lambda_3}{(x^2-5)},\qquad u_9=\frac{-135\lambda_1+(5x^2-175)\lambda_2-27x\lambda_3}{5(x^2-5)},$$
$$u_{10}=\frac{-15x\lambda_1+9x\lambda_2+(5x^2-4)\lambda_3}{5(x^2-5)},\qquad u_{11}=-\frac{-3\lambda_1+2\lambda_2+x\lambda_3}{5(x^2-5)},$$
$$u_{12}=-\frac{(25x^2-20)\lambda_1+(15x^2-10)\lambda_2+3x\lambda_3}{5(x^2-5)},\qquad u_{13}=\frac{5x\lambda_1+14x\lambda_2+7\lambda_3}{5(x^2-5)},$$

$$u_{14} = \frac{(5x^2-4)\lambda_1 - \lambda_2 - x\lambda_3}{5(x^2-5)}, \qquad u_{15} = -\frac{5x\lambda_1 - \lambda_3}{25(x^2-5)},$$
$$u_{16} = \frac{x(5\lambda_1 + 3\lambda_2)}{5(x^2-5)}, \qquad u_{17} = -\frac{\lambda_1 + 3\lambda_2}{5(x^2-5)},$$
$$u_{18} = -\frac{x\lambda_1}{5(x^2-5)}, \qquad u_{19} = \frac{\lambda_1}{25(x^2-5)}$$

where the λ_i are constants.

Computing the Puiseux expansions of the solutions of P at $x = 0$, we take for y_1 the series which has the value 0 at $x = 0$ and for y_2 another series (its value at $x = 0$ is a solution of $Z^4 + 50Z^2 + 125 = 0$). We wish to determine whether z is actually a constant. We find that

$$z = \lambda_0 - 5\lambda_3 - (60\lambda_1 + 26\lambda_2)Z + \frac{4}{5}\lambda_3 Z^2 - \frac{2}{5}(2\lambda_1 + \lambda_2)Z^3 + O(x^2)$$

where Z satisfies $Z^4 + 50Z^2 + 125 = 0$.

Letting $\lambda_0 = \lambda_3 = 0$ and $2\lambda_1 + \lambda_2 = 0$, $60\lambda_1 + 26\lambda_2 = 1$, we find an element $\tilde{z} = \sum_{b_i \in \mathcal{B}} \tilde{u}_i b_i = Z + O(x^2)$. We now compute a bound M which will ensure that $\tilde{z}$ is a constant. Note that the orbit of $\tilde{z}$ under all possible permutations of the y_i has at most 20 elements (which is the maximal order of the arithmetic Galois group). Therefore, $\tilde{z}$ and the element 1 satisfy a linear differential equation of order at most 21. The point 0 is an apparent singularity of L_P, and the exponents of L_P at $\pm\sqrt{5}$ are $\{0, 1/5, 2/5, 3/5, 4/5\}$ and at ∞ are $\{-1, 0, 1, 2, 3\}$. From the explicit form of the u_i we get that the elements of the orbit of $\tilde{z}$ under the Galois group have poles at $\{\sqrt{5}, -\sqrt{5}\}$ of order at most 1 and at ∞ of order at most 1. All other points are, at worst, apparent singularities. We now use equation (4) of Section 2.2 that we deduced from Fuchs's relation. The left-hand side of equation (4) in this situation is at most $\frac{1}{2}(3-2)(21)(20) + 3 = 213$. Therefore, the exponent at any apparent singularity is at most $19 + 213 = 232$. Calculating the Taylor series of y_1 and y_2 to sufficiently high powers, we see that $\tilde{z}$ agrees with a constant up to order 233. Therefore it must be a constant. This implies that $\tilde{z} = Z$, is an element of degree 4 over $\mathbf{Q}$. Corollary 5.9 implies that $C(5) = G_{\overline{k_0}(x)}$ has index at least 4 in $G_{k_0(x)}$ and so this latter group must be $F(5)$. □

6. Final Comments

In this paper we show that several geometric and algebraic properties of a polynomial in two variables can be determined from the associated minimal annihilating operator. One can ask, how can this be generalized to polynomials of more variables? Given a squarefree polynomial $P(x_1, \ldots, x_n, y) \in k_0(x_1, \ldots, x_n)[y]$, one considers the left ideal I of all operators in $k_0(x_1, \ldots, x_n)[\partial_1, \ldots, \partial_n]$ that annihilate the roots of P. One can show that the common solution space of these operators is a finite-dimensional vector space over $\overline{k_0}$ and that the dimension of this vector space is equal to the dimension of the k_0-span of the collection of roots of P. In a manner completely analogous to that of Section 4.1, one can show that the number of irreducible factors of P over $\bar{k}_0(x)$ is the dimension of the space of rational common solutions of the elements of I. Algorithms are known to determine this space (see Oaku *et al.*, 2001) and one can generalize the algorithm presented in Section 4.1 to determine these irreducible factors as well. The question remains as to how one can generalize the techniques of Section 3 to polynomials of several variables, that is, what topological information concerning the hypersurface

Table 6. Matrix $\mathcal{M}$.

$$
\begin{bmatrix}
0 & \frac{5}{x^2-5} & 0 & \frac{375}{x^2-5} & \frac{5}{x^2-5} & 0 & 0 & \frac{75x}{x^2-5} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{-100x}{x^2-5} & 0 & 0 & 0 \\
0 & 0 & \frac{10}{x^2-5} & \frac{-150x}{x^2-5} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{-100x}{x^2-5} & 0 & 0 & 0 & 0 \\
0 & \frac{-1}{x^2-5} & 0 & \frac{165}{x^2-5} & 0 & \frac{5}{x^2-5} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{75}{x^2-5} & 0 & 0 & \frac{-100x}{x^2-5} & 0 & 0 \\
0 & 0 & \frac{-2}{x^2-5} & \frac{-15x}{x^2-5} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{-25x}{x^2-5} \\
0 & 0 & 0 & \frac{-150x}{x^2-5} & 0 & \frac{5}{x^2-5} & 0 & 0 & \frac{75x}{x^2-5} & 0 & 0 & 0 & \frac{75x}{x^2-5} & \frac{-375}{x^2-5} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{150}{x^2-5} & 0 & 0 & \frac{10}{x^2-5} & 0 & \frac{-375}{x^2-5} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{75x}{x^2-5} \\
0 & 0 & 0 & \frac{-15x}{x^2-5} & 0 & \frac{-1}{x^2-5} & 0 & 0 & 0 & \frac{10}{x^2-5} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{75}{x^2-5} & 0 \\
0 & 0 & 0 & \frac{3}{x^2-5} & 0 & 0 & \frac{-2}{x^2-5} & 0 & 0 & 0 & \frac{15}{x^2-5} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{150}{x^2-5} & \frac{-1}{x^2-5} & 0 & 0 & \frac{5}{x^2-5} & 0 & 0 & 0 & \frac{15}{x^2-5} & 0 & 0 & 0 & 0 & 0 & \frac{75x}{x^2-5} \\
0 & 0 & 0 & \frac{-15x}{x^2-5} & 0 & \frac{-1}{x^2-5} & 0 & 0 & \frac{10}{x^2-5} & 0 & 0 & 0 & \frac{75x}{x^2-5} & \frac{-375}{x^2-5} & 0 & 0 & 0 & \frac{75x}{x^2-5} \\
0 & 0 & 0 & \frac{3}{x^2-5} & 0 & 0 & \frac{-1}{x^2-5} & 0 & 0 & 0 & 0 & \frac{15}{x^2-5} & 0 & \frac{150x}{x^2-5} & 0 & 0 & \frac{-200x}{x^2-5} & \frac{-375}{x^2-5} \\
0 & 0 & 0 & \frac{3}{x^2-5} & 0 & 0 & 0 & \frac{2}{x^2-5} & 0 & \frac{-2}{x^2-5} & 0 & 0 & \frac{15}{x^2-5} & \frac{-15x}{x^2-5} & 0 & 0 & 0 & \frac{-50x}{x^2-5} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{-2}{x^2-5} & 0 & 0 & 0 & 0 & \frac{5}{x^2-5} & 0 & 0 & 0 & \frac{75x}{x^2-5} \\
0 & 0 & 0 & \frac{-15x}{x^2-5} & 0 & 0 & 0 & 0 & 0 & \frac{-2}{x^2-5} & 0 & 0 & 0 & 0 & \frac{220}{x^2-5} & 0 & 0 & \frac{-375}{x^2-5} \\
0 & 0 & 0 & \frac{3}{x^2-5} & 0 & 0 & 0 & \frac{-15x}{x^2-5} & 0 & 0 & \frac{-2}{x^2-5} & 0 & \frac{10}{x^2-5} & 0 & 0 & \frac{-220}{x^2-5} & 0 & \frac{150x}{x^2-5} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{3}{x^2-5} & 0 & \frac{-15x}{x^2-5} & 0 & \frac{-1}{x^2-5} & 0 & \frac{15}{x^2-5} & 0 & 0 & \frac{220}{x^2-5} & \frac{70}{x^2-5} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{x^2-5} & 0 & 0 & \frac{-2}{x^2-5} & \frac{-15x}{x^2-5} & 0 & 0 & 0 & \frac{-75}{x^2-5} \\
0 & 0 & 0 & \frac{3}{x^2-5} & 0 & 0 & 0 & 0 & 0 & 0 & \frac{-3}{x^2-5} & 0 & 0 & 0 & \frac{-20x}{x^2-5} & \frac{5}{x^2-5} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{3}{x^2-5} & 0 & 0 & 0 & \frac{-3}{x^2-5} & 0 & 0 & 0 & \frac{-20x}{x^2-5} & \frac{10}{x^2-5} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{3}{x^2-5} & 0 & 0 & 0 & 0 & \frac{-1}{x^2-5} & \frac{-20x}{x^2-5} & \frac{15}{x^2-5} & \frac{-20x}{x^2-5} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{-2}{x^2-5} & \frac{-2}{x^2-5} & \frac{-2}{x^2-5}
\end{bmatrix}
$$

$P = 0$ can be determined from the singular locus of the associated holonomic system (Saito *et al.*, 2000).

Acknowledgements

We wish to thank Erich Kaltofen for stimulating and useful conversations concerning absolute factorizations, Hoon Hong for deriving the explicit formulae of Lemma 4.3, Bjorn Poonen for Proposition 2.1 and the referees for many helpful comments. OC was partially supported by Deutsche Forschunsggemeinschaft (DFG). MFS was partially supported by NSF Grants CCR-9731507 and CCR-009688842.

References

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

Bajaj, C., Canny, J., Garrity, T., Warren, J. (1993). Factoring rational polynomials over the complex numbers. *SIAM J. Comput.*, **22**, 318–331.

Barkatou, M. (1999). On rational solutions of systems of linear differential equations. *J. Symb. Comput.*, **28**, 547–568.

Bronstein, M. (1992). Solutions of linear differential equations in their coefficient field. *J. Symb. Comput.*, **13**, 413–439.

Chudnovsky, D. V., Chudnovsky, G. V. (1986). On expansion of algebraic functions in power and Puiseux series. I. *J. Complexity*, **2**, 271–294.

Chudnovsky, D. V., Chudnovsky, G. V. (1987). On expansion of algebraic functions in power and Puiseux series. II. *J. Complexity*, **3**, 1–25.

Comtet, L. (1964). Calcul pratique des coefficients de Taylor d'une fonction algébrique. *Enseignement Math.*, **2**, 267–270.

Conway, J. H., Hulpke, A., McKay, J. (1998). On transitive permutation groups. *LMS J. Comput. Math.*, **1**, 1–8. (electronic).

Corless, R. M., Galligo, A., Kotsireas, I. S., Watt, S. M. (2002). A symbolic geometric algorithm for factoring multivariate polynomials. In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*. Lille, France, ACM Press.

Cormier, O., Singer, M. F., Ulmer, F. (2000). Computing the Galois group of a polynomial using linear differential equations. In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*, pp. 78–85. St. Andrews, ACM Press.

Dottax, E. (2001). Calcul du Genre d'une Courbe Algébrique, Preprint, INRIA Sophia Antipolis (`http://www.inria.fr/cafe/stages/rapports/dottax.ps.gz`).

Duval, D. (1991). Absolute factorization of polynomials: a geometric approach. *SIAM J. Comput.*, **20**, 1–21.

Eichler, M. (1966). *Introduction to the Theory of Algebraic Numbers and Functions*. New York, Academic Press.

Galligo, A., Watt, S. M. (1977). A numerical absolute primality test for bivariate polynomials. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, pp. 217–224. ACM Press.

Gao, S. (2001). Factoring multivariable polynomials via partial differential equations, Preprint, Clemson University.

Gorenstein, D. (1968). *Finite Groups*. New York, London, Harper & Row.

Henry, J. P. G., Merle, M. (1989). Complexity of computation of embedded resolution of algebraic curves. In *EUROCAL'87 (Leipzig, 1987),* LNCS **378**, pp. 381–390. Berlin, Springer.

Huppert, B. (1967). *Endliche Gruppen I*. Berlin, New York, Springer.

Kaltofen, E. (1995). Effective Noether irreducibility forms and applications, Symposium on the Theory of Computing (New Orleans, LA, 1991). *J. Comput. Syst. Sci.*, **50**, 274–295.

Kaplansky, I. (1976). *An Introduction to Differential Algebra*, 2nd edn. Paris, Herman.

Lang, S. (1993). *Algebra*, 3rd edn. New York, Addison Wesley Inc.

Lenstra, H. W. (1992). Algorithms in algebraic number theory. *Bull. Am. Math. Soc.*, **26**, 211–244.

Mattman, T., McKay, J. (0000). Computation of Galois groups over function fields. *Math. Comput.*, **66**, 823–831.

Malle, G., Matzat, H. (1999). *Inverse Galois Theory, Springer Monographs in Mathematics*. Berlin, Springer.

Matzat, H., McKay, J., Yokoyama, K. (2000). Special issue on algorithmic methods in Galois theory, foreword of the guest editors. *J. Symb. Comput.*, **30**, 631–633.
Oaku, T., Takayama, N., Tsai, H. (2001). Polynomial and rational solutions of holonomic systems, Effective methods in algebraic geometry (Bath, 2000). *J. Pure Appl. Algebr.*, **164**, 199–220.
Poole, E. G. C. (1960). *Introduction to the Theory of Linear Differential Equations*. New York, Dover Publications Inc.
Ragot, J.-F. (1997). Sur la factorisation absolue des polynômes, Thèse. Université de Limoges.
Ritt, J. F. (1966). *Differential Algebra*. New York, Dover Publications Inc.
Rybowicz, M. (1990). Sur le calcul des places et des anneaux d'entiers d'un corps de fonctions algébriques, Thèse. Université de Limoges.
Saito, M., Sturmfels, B., Takayama, N. (2000). *Gröbner Deformations of Hypergeometric Differential Equations*, Volume 6 of *Algorithms and Computation in Mathematics*. Berlin, Springer.
Singer, M. F. (1979). Algebraic solutions of n-th order linear differential equations. In *Proceedings of the 1979 Queens Conference on Number Theory,* pp. 379–420*, Queen's Papers in Pure and Appl. Math.* **54**.
Singer, M. F. (1996). Testing reducibility of linear differential operators: a group theoretic perspective. *Appl. Algebr. Eng. Commun. Comput.*, **7**, 77–104.
Singer, M. F., Ulmer, F. (1993). Galois groups for second and third order linear differential equations. *J. Symb. Comput.*, **16**, 1–36.
Teitelbaum, J. (1990). The computational complexity of the resolution of plane curve singularities. *Math. Comput.*, **54**, 797–837.
Trager, B. M. (1984). Integration of algebraic functions. Ph.D. Thesis, MIT.
van der Put, M., Singer, M. F. (2001). Differential Galois theory, preprint.
van der Waerden, B. L. (1953). *Modern Algebra*, 2nd edn. New York, Frederick Ungar Publishing Co.
van Hoeij, M. (1994). An algorithm for computing an integral basis in an algebraic function field. *J. Symb. Comput.*, **18**, 353–363.
van Hoeij, M. (1997). Factorization of differential operators with rational functions coefficients. *J. Symb. Comput.*, **24**, 53–561.
von zur Gathen, J., Gerhard, J. (1999). *Modern Computer Algebra*. Cambridge, Cambridge University Press.
Walker, R. J. (1962). *Algebraic Curves*. New York, Dover Publications Inc.
Winkler, F. (1996). *Polynomial Algorithms in Computer Algebra, Texts and Monographs in Symbolic Computation*. Vienna, Springer.
Zippel, R. (1993). *Efficient Polynomial Computation*. Boston, Kluwer Academic Publishers.

Appendix: Tschirnhaus Transformations

In Section 2 we gave a method to transform certain polynomials into polynomials whose roots are linearly independent over the constants. In this section we discuss other possible methods that lead to (and depend on) several conjectures of independent interest. We begin with the following definition.

Definition 6.1. Let K be a field and $P(y)$, $T(y) \in K[y]$ be polynomials. We define the Tschirnhaus transform of P with respect to T to be the polynomial $P_T(y) = \mathrm{Res}_z(P(z), y - T(z))$, where Res_z denotes the resultant with respect to z.

One sees that $P_T(y)$ has the same degree as $P(y)$ and that its roots in an algebraic closure $\bar{K}$ of K are $\{T(\alpha) \mid \alpha \text{ is a root of } P\}$. For future use, we wish to ensure that the factorization properties of $P(y)$ are preserved by the Tschirnhaus transformation. The relevant facts are given in the following lemma.

Lemma 6.2. *Let K be a field, $P(y) \in K[y]$ a squarefree polynomial and E the splitting field of $P(y)$ over K. Let $T(y) \in K[y]$ satisfy the property that $T(\alpha) \neq T(\beta)$ for distinct roots of $P(y)$ in E and let $Q(y) = P_T(y)$.*

If $P = cP_1 \cdots P_t$ and $Q = dQ_1 \cdots Q_s$ where c, $d \in K$ and the P_i and Q_i are monic, irreducible polynomials in $K[y]$ then $t = s$. Furthermore, after a possible renumbering $Q_i(y) = \mathrm{Res}_z(P_i(z), y - T(z))$ and $P_i(y) = GCD(Q_i(T(y)), P(y))$.

PROOF. Let G be the Galois group of E over K. The map $\alpha \longmapsto T(\alpha)$ maps the roots of $P(y)$ bijectively onto the roots of $Q(y)$. Furthermore, for any $\alpha \in E$, $\sigma \in G$ we have that $\sigma(T(\alpha)) = T(\sigma(\alpha))$. Therefore, T maps G-orbits of roots of $P(y)$ to G-orbits of roots of $Q(y)$. Identifying an irreducible monic factor of $P(y)$ with its set of roots gives a bijective correspondence between these factors and G-orbits of roots of P. Therefore, after a possible renumbering T maps the roots of $P_i(y)$ bijectively to the roots of $Q_i(y)$. The final statement of the lemma reflects this fact. □

We now turn to the question of transforming a polynomial into a polynomial whose roots are linearly independent.

PROPOSITION 6.3. *Let $k = k_0(x)$ and let $P \in k[y]$ be a squarefree polynomial of degree n. There exist integers $a_{i,j}$, $0 \le a_{i,j} < n$ such that the roots of $P_T(y) = 0$ in $\overline{k}$ are linearly independent over $\overline{k_0}$, where $T(y) = a_0 + a_1 y + \cdots + a_{n-1}y^{n-1}$ and $a_i = \sum_{j=0}^{n-1} a_{i,j}x^j$.*

PROOF. Let $U_0, \ldots, U_{n-1}$ be differential indeterminates and $y_1, \ldots, y_n$ be the roots of P. The field of constants of $K = k < U_0, \ldots, U_{n-1} >$ is once again k_0. The elements $V_i = \sum_{j=0}^{n-1} U_j y_i^j$ are linearly independent over $\overline{k_0}$. To see this, note that $(V_1, \ldots, V_n) = (U_0, \ldots, U_{n-1})V$ where V is the Vandermonde 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 $(U_0, \ldots, U_{n-1})V(c_1, \ldots, c_n)^T = 0$ 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 U_i. This differential polynomial has order $n-1$ in the U_i and so by a result of Ritt (1966, p. 35), van der Put and Singer (2001, Lemma 2.20) there exist polynomials a_i as specified such that the substitution $U_i \longmapsto a_i$ keeps W nonzero. Thus the elements $\tilde{y}_i = \sum_{j=0}^{n-1} a_j y_i^j$ are linearly independent over $\overline{k_0}$ and the polynomial $T(y) = \sum_{i=0}^{n-1} a_i y^i$ satisfies the conclusion of the proposition. □

The set of possible coefficient vectors $(a_{i,j})$ has cardinality $(n+1)^{n^2}$. To decide if a choice yields a desired Tschirnhaus transformation one can formally differentiate $Y = a_0 + a_1 y + \cdots + a_{n-1}y^{n-1}$ as in the algorithm described in the beginning of Section 2. At each stage one replaces y' with a linear combination of powers of y using $P_x + y'P_y = 0$. For some choice within the described bounds one will produce a linear operator of order n. In particular, for almost all choices of $a_{i,j} \in k_0$, we will produce a Tschirnhaus transformation that yields linearly independent roots.

We would like to be able to select *constants* $a_i \neq 0$ such that for $T(y) = \sum_{i=0}^{n-1} a_i y^i$, the roots of $P_T(y)$ are linearly independent over $\overline{k_0}$. Obviously, this cannot be done if the roots of P lie in $\overline{k_0}$ but one could ask if such a Tschirnhaus transform exists assuming that P has no roots in $\overline{k_0}$. This would follow from the following conjecture.

CONJECTURE I. *Let K be a differential field of characteristic zero with field of constants C and $y_1, \ldots, y_n$ distinct, nonconstant elements of K. There exists a polynomial $T(Y)$ in $C[Y]$ of degree at most $n-1$ such that the elements $\tilde{y}_j = T(y_j)$, $j = 1, \ldots, n-1$ are linearly independent over C.*

The conjecture implies that the Wronskian determinant W in the proof of Proposition 6.3 will be nonzero when we replace the U_i with constants. Therefore W is nonzero when we replace all derivatives of the U_i with zero. The resulting polynomial will have degree at most n in the U_i and so there will be a choice of $a_i \in k_0$ within the desired

bounds that are not a zero of this polynomial. This would still not necessarily yield a deterministic method for finding these a_i in polynomial time but would yield a probabilistic argument that almost all choices of a_i yield the desired linear independence.

In Proposition 6.6 we will show that the conjecture is true if we only demand that T be a polynomial of degree at most $n(n-1)/2$ but at present we cannot prove the conjecture in general or even for roots of a general squarefree polynomial having no factors independent of x. We can show that Conjecture I, as stated, is true for roots of an absolutely irreducible polynomial. This will follow from the following lemma.

LEMMA 6.4. *Let $F_0 \subset F_1 \subset F_2$ be fields and assume that F_2 is a finite Galois extension of F_0 with Galois group G. Let $H \subset G$ be the Galois group of F_2 over F_1 and let $\tau_1 H, \ldots, \tau_n H$ be the cosets of H in G. Then there exist $\sigma_1, \ldots, \sigma_n \in G$ such that the set $S = \{v \in F_1 \mid \det(\sigma_i \tau_j(v)) \neq 0\}$ is not empty. Furthermore, any $v \in S$ has the property that its conjugates are linearly independent over F_0.*

PROOF. Let $\sigma_1, \ldots, \sigma_m$ be the elements of G. The usual proof of the Normal Basis Theorem (see Lang, 1993, Chapter VI, Section 13) shows that the set $S' = \{w \in F_2 \mid \det(\sigma_i \sigma_j(w)) \neq 0\}$ is not empty. Fix some $w \in S'$ and let $v = \sum_{\sigma \in H} \sigma(w)$. We then have that $v \in F_1$. Let N be the $m \times n$ matrix $(\sigma_i \tau_j(v))$. The columns of this matrix are the sums of disjoint sets of m/n columns of the $m \times m$ matrix $(\sigma_i \sigma_j(w))$. Therefore, the columns of N are linearly independent. Therefore, after a possible renumbering, we may assume that the matrix $(\sigma_i, \tau_j(v))_{i=1,\ldots,n}^{j=1,\ldots,n}$ is nonsingular. This establishes the first claim of the lemma.

For any $v \in F_1$ the conjugates of v over F_0 are among the elements $\tau_1(v), \ldots, \tau_n(v)$. Let $v \in S$ and let $a_1\tau_1(v) + \cdots + a_n\tau_n(v) = 0$ for some $a_i \in F_0$. For any $\sigma \in G$ we have $\sigma(a_1\tau_1(v) + \cdots + a_n\tau_n(v)) = a_1\sigma\tau_1(v) + \cdots + a_n\sigma\tau(v) = 0$. Since $\det(\sigma_i\tau_j(v)) \neq 0$ we have that each $a_i = 0$. This proves the final conclusion of the lemma. □

We now show the following proposition.

PROPOSITION 6.5. *Let $P(y)$ be an absolutely irreducible polynomial in $k_0(x)[y]$ of degree n. There exist integers a_i, $0 \leq a_i \leq n-1$ such that the roots of $P_T(y)$ in $\overline{k_0(x)}$ are linearly independent over $\overline{k_0}$, where $T(y) = a_0 + a_1 y + \cdots + a_{n-1}y^{n-1}$.*

PROOF. Let $F_0 = \overline{k_0}(x)$ and let F_2 be the splitting field of $P(y)$ over F_0. Let $\alpha \in F_2$ be a root of $P(y)$ and $F_1 = F_0(\alpha)$. The hypothesis implies that $[F_1 : F_0] = n$. Any element of F_1 is of the form $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ for some $a_i \in F_0$. Let $\sigma_1, \ldots, \sigma_n$, $\tau_1, \ldots, \tau_n$ be as in Lemma 6.4 and let $Y_0, \ldots, Y_{n-1}$ be indeterminates. The conclusion of Lemma 6.4 implies that the polynomial $A(Y_0, \ldots, Y_{n-1}) = \det(Y_0 + Y_1\sigma_i\tau_j(\alpha) + \cdots + Y_{n-1}\sigma_i\tau_j(\alpha^{n-1}))_{i=1,\ldots,n}^{j=1,\ldots,n}$ is a *nonzero* homogeneous polynomial of degree n with coefficients in F_2. Therefore, there exist integers a_i, $0 \leq a_i \leq n$ such that $A(a_0, \ldots, a_{n-1}) \neq 0$ and so the conjugates of $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ are linearly independent over $\overline{k_0}(x)$. This implies that the roots of $P_T(y)$ are linearly independent over $\overline{k_0}(x)$ where $T(y) = a_0 + a_1 y + \cdots + a_{n-1}y^{n-1}$. □

We now will show that for distinct nonconstant elements $y_1, \ldots, y_n$ in a differential field K of characteristic zero with field of constants C, there exists a polynomial $T \in C[Y]$, of degree at most $n(n-1)/2$, such that the elements $\tilde{y}_i = T(y_i)$ are linearly independent over C. We note that the usual properties of Wronskians imply that these elements will be linearly independent over the algebraic closure $\overline{C}$ of C (see Kaplansky, 1976).

We begin by noting that, under the above assumptions, there exist n homomorphisms $\phi_i\colon \overline{C}[y_1,\ldots,y_n] \to \overline{C}$ such that the entries of the matrix $(\phi_i(y_j))$ are all distinct. To construct ϕ_1 note that, by assumption, the element $\prod_{i\neq j}(y_i - y_j)$ is nonzero in K and therefore invertible. Theorem 11 of Lang (1993, Chapter IX, Section 1) implies that there exists a homomorphism $\phi_1\colon \overline{C}[y_1,\ldots,y_n,(\prod_{i\neq j}(y_i - y_j))^{-1}] \to \overline{C}$. Clearly, the elements $\phi_1(y_i)$ are distinct. Now assume that we have constructed $\phi_1,\ldots,\phi_t$ such that the entries of the $t \times n$ matrix $(\phi_i(y_j))$ are distinct. The assumptions imply that the elements $\prod_{i\neq j}(y_i - y_j)$ and $\prod_{h,i,j}(y_h - \phi_i(y_j))$ are nonzero. Therefore there exists a homomorphism $\phi_{t+1}\colon \overline{C}[y_1,\ldots,y_n,(\prod_{i\neq j}(y_i - y_j))^{-1},\prod_{h,i,j}(y_h - \phi_i(y_j))^{-1}] \to \overline{C}$. Continuing until $t = n$ yields the desired homomorphisms.

PROPOSITION 6.6. *Let K be a differential field of characteristic zero with field of constants C and $y_1,\ldots,y_n$ distinct, nonconstant elements of K. There exists a polynomial $T(Y)$ in $C[Y]$ of degree at most $n(n-1)/2$ such that the elements $\tilde{y}_j = T(y_j)$, $j = 1,\ldots,n-1$ are linearly independent over C.*

PROOF. We will construct a polynomial $T_1(Y) \in \overline{C}[Y]$ of degree at most $n(n-1)/2$ such that the elements $\tilde{y}_j = T_1(y_j)$, $j = 1,\ldots,n-1$ are linearly independent over $\overline{C}$. Let $\phi_1,\ldots,\phi_n$ be the homomorphisms described above and let $(\phi_i(y_j))$ be the resulting matrix with distinct entries. There exists a polynomial $T_1(Y) \in \overline{C}[Y]$ of degree $n(n-1)/2$ such that $T_1(\phi_i(y_j)) = 0$ for all $i > j$, that is T_1 is zero for each entry below the diagonal. Since T_1 can have no further zeros, the diagonal elements of $(T_1(\phi_i(y_j))$ are nonzero and so the determinant of this matrix is nonzero. Let $c_j \in C$ be elements such that $\sum_{j=1}^{n} c_j T_1(y_j) = 0$. Applying the ϕ_i, we have that $\sum_{j=1}^{n} c_j \phi_i(T_1(y_j)) = 0$. The invertibility of $(T_1(\phi_i(y_j))$ implies that the c_i are zero and so the elements $\{T_1(y_j)\}$ are linearly independent over $\overline{C}$. Note that this implies that the Wronskian of the elements $\{T_1(y_j)\}$ is nonzero.

Let $\overline{T}(Y)$ be a polynomial of degree $n(n-1)/2$ with indeterminate constant coefficients $\{d_0,\ldots,d_{n(n-1)/2}\}$. The Wronskian $W(\overline{T}(y_1,\ldots,\overline{T}(y_n))$ is a polynomial in the d_i with coefficients in K that is furthermore nonzero since the above shows that we can specialize the d_i and obtain a nonzero result. Since C is an infinite field, we can specialize the d_i to elements c_i in C and obtain a polynomial $T(Y)$ satisfying the conclusion of the proposition. □

From the proof of Proposition 6.6, one sees that Conjecture I would follow from the following conjecture.

CONJECTURE II. *Let C be a field of characteristic zero and $(a_{i,j})$ a matrix with distinct entries. There exists a polynomial $T(Y)$ in $C[Y]$ of degree at most $n-1$ such that the matrix $(T(a_{i,j}))$ is invertible.*

We finally note that the set of coefficients of polynomials P_T that satisfy the conclusions in Proposition 6.5 lie in a Zariski open set. This yields a probabilistic argument that almost all such transformations will have the desired effect. In a similar way, almost all polynomials of degree $n(n-1)/2$ will satisfy the conclusion of Proposition 6.6.

Received 14 September 2001
Accepted 17 July 2002