Indag. Mathem., N.S., 7 (3), 367–387 September 30, 1996

Reduction modulo p of differential equations

by Marius van der Put

Department of Mathematics, University of Groningen, P.O. Box 800, 9700 AV Groningen, the Netherlands

Communicated by Prof. T.A. Springer at the meeting of September 25, 1995

1. INTRODUCTION

The theme of this note is to use the classification of differential equations in positive characteristic and the conjectures of A. Grothendieck and N. Katz for finding symbolic solutions or factorizations of differential operators over $\boldsymbol{Q}(z)$. The paper of N. Katz [K1] lies at the origin of this note. The main tool is the p-curvature for differential equations in characteristic p.

For an $n \times n$-matrix A with coefficients in $\boldsymbol{Q}(z)$ we consider the linear homogeneous differential equation $y' + Ay = 0$.

For almost all primes p (i.e. with finitely many exceptions) one can reduce A modulo p, the resulting matrix $\bar{A}$ has coefficients in the field $\boldsymbol{F}_p(z)$. This leads to the linear homogeneous differential equation $y' + \bar{A}y = 0$ over $\boldsymbol{F}_p(z)$. The *p-curvature* of this equation is the $\boldsymbol{F}_p(z)$-linear map

$$\psi_p := \left(\frac{d}{dz} + \bar{A}\right)^p : \boldsymbol{F}_p(z)^n \to \boldsymbol{F}_p(z)^n.$$

There is an obvious algorithm for the p-curvature, namely:
Define the sequence of matrices $A(k)$ by

$$A(1) := A \quad \text{and} \quad A(k+1) = \frac{d}{dz}(A(k)) + A.A(k), \quad \text{then}$$
$$\psi_p = A(p) \text{ modulo } p.$$

The p-curvature of the order one equation $y' = ry$ can be seen to be $\psi_p = r^{(p-1)} + r^p$ modulo p.

The importance of the p-curvature is given by the following lemma.

Lemma 1.1. *$\psi_p = 0$ if and only if $y' + \bar{A}y = 0$ has a fundamental matrix with coefficients in $\boldsymbol{F}_p(z)$.*

A finer result on the p-curvature is the following. For the differential equation $y' + \bar{A}y = 0$ one can define a differential Galois group. This is an abelian group scheme of height one over the field $\boldsymbol{F}_p(z^p)$. The Lie-algebra of this group scheme is the commutative p-Lie algebra over $\boldsymbol{F}_p(z^p)$ generated by ψ_p. See [A1, A 2] and [P].

We will state the two conjectures above in a simplified form.

Grothendieck's conjecture asserts that the following statements are equivalent.

(1) *$y' + Ay = 0$ has a fundamental matrix with as coefficients algebraic functions.*

(2) *For almost all primes p the p-curvature is* 0.

The implication (1) $\Rightarrow$ (2) in Grothendieck's conjecture is easily proved.

Katz' conjecture concerns the differential Galois group G of the equation $y' + Ay = 0$ and its Lie-algebra Lie(G). The statement is: Lie(G) is the smallest algebraic Lie-algebra in $M(n \times n, \bar{\boldsymbol{Q}})$ such that Lie(G) 'contains' ψ_p for almost all primes p.

N. Katz has proved Grothendieck's conjecture in many cases and has shown that this conjecture is equivalent to the one of Grothendieck.

The difficulty in trying to use the p-curvature for finding symbolic solutions (or the differential Galois group) of the equation $y' + Ay = 0$ is the expression 'almost all primes p'. For order one equations we will show how one can specify 'almost all' by using a method of Rothstein and Trager. (See [L]).

For a differential field k with a derivation written as $'$ we denote by $k[\partial]$ the skew ring of differential operators. Its structure is given by the formula $\partial a = a\partial + a'$ with $a \in k$. The ultimate goal is to factorize a given differential operator L over the field $\boldsymbol{Q}(z)$ by computing the factorizations of the reduction $\bar{L} \in \boldsymbol{F}_p(z)[\partial]$. We propose here some methods for factoring $\bar{L}$ and L. A complete algorithm seems not within reach at the moment. For order two operators L however, a fairly complete procedure for factoring L is given.

Order two differential equations in positive characteristic have also been studied in [J, Ks]. An algorithm for order two differential equations in positive characteristic is developed in [Ho].

I would like to thank Frits Beukers for his helpful comments.

In this section we give some proofs and statements which will be used in the sequel. The differential field k is supposed to have characteristic $p > 0$. We suppose that $[k : k^p] = p$ and we fix a $z \in k$ such that $k = k^p(z)$. The differentiation $'$ of k is defined by $z' = 1$. A differential module M over k will be a finite dimensional vector space over k equiped with a k^p-linear map $\partial : M \to M$ satisfying $\partial(fm) = f'm + f\partial m$ (with $m \in M$ and $f \in k$). The p-curvature ψ_p is simply the k-linear map ∂^p on M.

Lemma 2.1. *The p-curvature of a differential module M is 0 if and only if M is trivial, i.e. there is a basis $e_1, \ldots, e_m$ of M over k with $\partial(e_i) = 0$ for all i.*

Proof. If M is the trivial module then obviously the p-curvature is 0. On the other hand, suppose that ∂^p is 0 on M. Then ∂ is a nilpotent k^p-linear operator on M and has an element $e_1 \neq 0$ in its kernel. By induction the module M/ke_1 has a basis $\bar{e}_2, \ldots, \bar{e}_m$ with $\partial(\bar{e}_i) = 0$. Let e_i (for $i > 1$) denote a lift of $\bar{e}_i$ to M. Then $\partial e_i = a_i e_1$ for some $a_i \in k$. Then $\partial^p(e_i) = a_i^{(p-1)} e_1$ and so $a_i^{(p-1)} = 0$. It follows from $a_i^{(p-1)} = 0$ that there exists $b_i \in k$ with $b_i' = a_i$. The elements $e_1, e_2 - b_2 e_1, \ldots, e_m - b_m e_1$ form a basis of M on which ∂ is 0. □

Lemma 2.2. (1) *For the one-dimensional module k with $\partial e = re$ one has $\partial^p(e) = (r^{(p-1)} + r^p)e$. Further $r^{(p-1)} + r^p \in k^p$.*

(2) *For $r \in k$ one has $r^{(p-1)} + r^p = 0$ if and only if $r = f'/f$ for some $f \in k^*$.*

Proof. (1) Define the map $\tau : k \to k$ as follows:

If $\partial e = re$ then $\partial^p e = \tau(r)e$. As we have seen in the introduction $-\tau(r)$ is the constant term in the expression $((d/dz) - r)^p$. A calculation shows that $\tau(r) = r^{(p-1)} + r^p$. (See [P], Lemma 1.4.2.) The derivative of $\tau(r)$ is seen to be 0 and so $\tau(r) \in k^p$.

(2) According to 2.1, the p-curvature is 0 if and only if there exists an $f \in k^*$ with $\partial(fe) = 0$. The last condition is equivalent to $r = -(f'/f)$. □

2.1. Classification of differential modules over k

We summarize here results from [P]. We will use the notation $t = \partial^p$. The center Z of $k[\partial]$ turns out to be the polynomial ring $k^p[t]$. For every monic irreducible polynomial $F \in k^p[t]$ and every $m \geq 1$ one can define an indecomposable differential module $I(F^m)$. If $k[\partial]/(F)$ happens to be a skew field then $I(F^m)$ is equal to $k[\partial]/(F^m)$. If $k[\partial]/(F)$ is not a skew field then $k[\partial]/(F)$ is isomorphic to $M(p \times p, Z/(F))$ (i.e. the ring of $p \times p$ matrices over the field $Z/(F)$). In this case $k[\partial]/(F^m) \cong M(p \times p, Z/(F^m))$. The module $I(F^m)$ is equal to $(Z/(F^m))^p$ with the obvious action of $M(p \times p, Z/(F^m))$ and therefore equipped with a left action of $k[\partial]$.

The set $\{I(F^m)\}$ is the set of all indecomposable differential modules over k. Further any differential module N is a direct sum $\sum_{F,m} I(F^m)^{e(F,m)}$. The

numbers $e(F,m)$ are uniquely determined by N. They can be found by calculating the dimensions of the k-vector spaces $\ker(F^m(\psi_p), N)$.

Let N be a differential module over k of dimension n. In order to find the decomposition of N into indecomposable modules one views the operator $\partial : N \to N$ as a k^p-linear map. Let $F(T)$ denote the characteristic polynomial of ∂ on N. This polynomial in $k^p[T]$ has degree pn. The characteristic polynomial of ∂^p on N (still considered as a k^p-linear map) is easily seen to be $F(T^{1/p})^p$. The characteristic polynomial $G(T)$ of ∂^p, considered as a k-linear map on N, is then $F(T^{1/p})$. We note that $G(T)$ lies in $k^p[T]$.

Let $G = F_1^{m_1} \cdots F_s^{m_s}$ denote the factorization of G in $k^p[T]$ with monic distinct and irreducible F_i. The module N has a unique direct sum decomposition $N = \bigoplus_i N_i$ where the differential module N_i has $F_i^{m_i}$ as characteristic polynomial for its p-curvature.

The further decomposition of N_i has the form $\bigoplus_{1 \le m \le m_i} I(F_i^m)^{e(F_i,m)}$, where the numbers $e(F_i,m)$ can be found by calculating the dimensions of the kernels of the action of $F_i^m(\psi_p)$ acting on N_i (or N).

We note that the case where $k[\partial]/(F)$ (for some monic irreducible $F \in k^p[t]$) is a skew field is rather exceptional. This exceptional case will not concern us in this paper.

3. EQUATIONS OF ORDER ONE

3.1. Order one homogeneous equations

One considers the equation $y' = ry$ with $r \in \boldsymbol{Q}(z)^*$. Grothendieck's conjecture is known to be true in this case. So we know that:

There is an algebraic solution $\neq 0$ if and only if for almost all primes p the p-curvature is zero.

We study a possible proof of this statement and specify the term 'almost all primes'. First we have to see how reduction modulo a prime p works for operators.

A polynomial $P \in \boldsymbol{Z}[z]$ is called *primitive* if the g.c.d. of the coefficients of P is 1. The ring R denotes the localization of $\boldsymbol{Z}[z]$ at the set of unit polynomials. The proper ideals of R are the nR with $n > 1$. For any prime p the ring R/pR is equal to $\boldsymbol{F}_p(z)$. The ring R is invariant under the differentiation of $\boldsymbol{Q}(z)$. For every non zero $r \in \boldsymbol{Q}(z)$ there are unique positive integers t, n with g.c.d. one such that $r = (t/n)f$ with $f \in R^*$. We will call t and n the numerator and the denominator of r. For a prime p which does not divide the denominator of r we write r_p, or r mod p, for the image of r in $\boldsymbol{F}_p(z)$.

We will call an operator $L := \sum_i a_i \partial^i \in R[\partial]$ a *primitive operator* if the ideal in R generated by the coefficients a_i is the unit ideal of R. The product of two primitive operators is again a primitive operator. Indeed, for every prime p the skew ring $R[\partial]/(p)$ is equal to the ring $\boldsymbol{F}_p(z)[\partial]$. The latter ring has no zero divisors.

Consider a monic operator L with coefficients in $R[1/m]$, for some positive integer m. Let a factorization $L = L_1 L_2$ with monic operators L_i by given. From the observations above it follows that L_1 and L_2 have their coefficients in $R[1/m]$. In particular, for any prime p which does not divide m one finds a factorization $\bar{L} = \bar{L}_1 \bar{L}_2$ in the ring $\boldsymbol{F}_p(z)[\partial]$ by reduction modulo p. The classification of differential equations in characteristic p will be used to provide the possible factorizations of $\bar{L}$. An ultimate goal is to find factorizations of L by combining factorizations $\bar{L}$ for suitable primes p.

We return now to the first order equation. There is a rational number λ with $\lambda r R = R$. We normalize r by requiring that $r \in R^*$. This does not change the problem.

Write $r = a/b$ with $a, b \in \boldsymbol{Z}[z]$ primitive polynomials with g.c.d.$(a, b) = 1$. Necessary conditions for the equation to have algebraic solutions are: b has no multiple roots and that the degree of a is less than the degree of b.

We will assume that $r = a/b$ satisfies these conditions.

By assumption the resultant $\text{resultant}_z(b, b')$ is not zero. Let the integer M denote the absolute value of this resultant. We note that the highest coefficient of b divides M. Let K denote the splitting field of b. Then the ramified primes in K are divisors of M.

We apply a method of Rothstein and Trager to the equation $y' = ry$. This consists of considering the resultant $R(x) := \text{resultant}_z(a - xb', b) \in \boldsymbol{Z}[x]$. Let $\Omega \supset \boldsymbol{Q}$ denote the splitting field of $R(x)$. Let α be a zero of $R(x)$. Then the g.c.d. $(a - \alpha b', b)$ is not trivial and hence is divisible by $z - \beta$ where β is a zero of b. It follows that $\alpha = a(\beta)/b'(\beta)$. Therefore Ω is a subfield of K. Any prime p not dividing M is therefore unramified in Ω. We note further that for any zero β of b, the zero $a(\beta)/b'(\beta)$ of $R(x)$ is the *local exponent* of the equation $y' = ry$ at β. In particular, zeroes of $R(x)$ are the local exponents of the equation.

If the equation $y' = ry$ has an algebraic solution its differential Galois group over $\bar{\boldsymbol{Q}}$ is finite cyclic of order m. Then there is a non trivial solution $f \in \bar{\boldsymbol{Q}}(z)$ of $f' = mrf$. For any element σ in the Galois group of $\bar{\boldsymbol{Q}}/\boldsymbol{Q}$ the element $\sigma(f)$ is also a solution of the equation and so $\sigma(f) = c(\sigma)f$ for some $c(\sigma) \in \bar{\boldsymbol{Q}}^*$. The map $\sigma \mapsto c(\sigma)$ is a 1-cocycle. By Hilbert 90, the group $H^1(\text{Gal}_{\boldsymbol{Q}}, \bar{\boldsymbol{Q}}^*)$ is trivial. Hence there is also a solution $f \in \boldsymbol{Q}(z)^*$ of $f' = mrf$.

Lemma 3.1. *$y' = ry$ has a non trivial algebraic solution if and only if $\Omega = \boldsymbol{Q}$.*

Proof. Suppose that an algebraic solution $\neq 0$ exists. Let $m \geq 1$ be minimal such that there exists a $f \in \boldsymbol{Q}(z)^*$ with $f' = mrf$. Normalize f such that $f \in R^*$. Write $f = f_1^{n_1} \cdots f_s^{n_s}$ where $f_1, \ldots, f_s$ are distinct irreducible unit polynomials in $\boldsymbol{Z}[z]$ and where the $n_1, \ldots, n_s \in \boldsymbol{Z} \setminus \{0\}$. The minimality of m implies that the g.c.d. of $\{n_1, \ldots, n_s\}$ is 1.

As a consequence $mr = \sum (n_i f_i'/f_i)$ and $b = \pm f_1 \cdots f_s$. We may suppose that $b = f_1 \cdots f_s$. Then

$$a - xb' = \frac{1}{mb}\left(\sum \frac{n_i f_i'}{f_i} - \sum \frac{mx f_i'}{f_i}\right) = \sum_{i=1}^{s} \left(\frac{n_i}{m} - x\right) f_i' f_1 \cdots \hat{f}_i \cdots f_s.$$

Further $R(\alpha) = 0$ if and only if the g.c.d.$(a - \alpha b', b)$ is not 1. The last statement is equivalent to $\alpha = n_i/m$ for some i. Therefore all the zeroes of R are rational.

Suppose that all the zeroes of $R(x)$ are rational. Write $\lambda_1, \ldots, \lambda_s$ for the distinct zeroes. We note that $R(0) \neq 0$. Let $f_i := \text{g.c.d.}(a - \lambda_i b', b)$ be normalized such that f_i is a primitive polynomial. For $i \neq j$ one has g.c.d.$(f_i, f_j) = 1$ since g.c.d.$(b', b) = 1$. Hence $f_1 \cdots f_s \mid b$. In order to see the equality (up to a sign) it suffices to show that any zero $\beta \in \boldsymbol{K}$ of b is also a zero of $f_1 \cdots f_s$. By assumption $b'(\beta) \neq 0$. Then $a - (a(\beta)/b'(\beta))$ and b have the common zero β. It follows that $a(\beta)/b'(\beta) = \lambda_i$ for some i and that β is a zero of f_i.

Hence $f_1 \cdots f_s = b$. It is easy to see now that $r = \sum_i \lambda_i (f_i'/f_i)$. One finds the algebraic solution $y = \prod_i f_i^{\lambda_i}$ of $y' = ry$. □

Proposition 3.2. *Suppose that $\Omega = \boldsymbol{Q}$. Then*

(1) *The minimal $m \geq 1$ such that $f' = mrf$ has a solution $f \in \boldsymbol{Q}(z)^*$ is a divisor of $M := |\text{resultant}_z(b', b)|$.*

(2) *For $p \nmid M$ the p-curvature, i.e. $r^{(p-1)} + r^p \bmod p$, is zero.*

Proof. (1) The highest coefficient of $R(x) \in \boldsymbol{Z}[x]$ is equal to $\pm \text{resultant}_z(b', b)$. Let $\lambda_1, \ldots, \lambda_s$ denote the zeroes of $R(x)$. Then all $M\lambda_i \in \boldsymbol{Z}$. Using the proof of the last lemma one sees that there is a solution $f \in \boldsymbol{Q}(z)^*$ of $f' = Mrf$. This proves (1).

(2) Let $f \in \boldsymbol{Q}(z)^*$ with $f' = Mrf$ be normalized such that $f \in R^*$. Then

$$(Mr)^{(p-1)} + (Mr)^p \equiv M(r^{(p-1)} + r^p) \equiv \left(\frac{f'}{f}\right)^{(p-1)} + \left(\frac{f'}{f}\right)^p$$

$$\equiv 0 \bmod p. \qquad \square$$

Proposition 3.3. *Suppose that $\Omega \neq \boldsymbol{Q}$. Suppose that the prime p does not divide $M := |\text{resultant}_z(b', b)|$. Then p is totally split in Ω if and only if the p-curvature of the equation $y' = ry$ is 0.*

Proof. We write $\bar{a}$ and $\bar{b}$ for the reductions of a and b modulo p. Since p does not divide the resultant of b and b', the degree of $\bar{b}$ is the same as the degree of b and g.c.d.$(\bar{b}', \bar{b}) = 1$. Let $F(x) := \text{resultant}_z(\bar{a} - x\bar{b}', \bar{b})$. Then $F(x)$ is the reduction of $R(x)$ modulo p. Let $\mu_1, \ldots, \mu_r \in \bar{\boldsymbol{F}}_p$ be the set of zeroes of $F(x)$. Put $v_i := \text{g.c.d.}(\bar{a} - \mu_i \bar{b}', \bar{b})$. Then we claim that $\bar{a}/\bar{b} = \sum_i \mu_i (v_i'/v_i)$.

Indeed, every v_i divides $\bar{b}$. Further g.c.d.$(v_i, v_j) = 1$ if $i \neq j$ because g.c.d.$(\bar{b}', \bar{b}) = 1$. Hence $v_1 \cdots v_s$ divides $\bar{b}$. Let $\beta \in \bar{\boldsymbol{F}}_p$ be a zero of $\bar{b}$. Then $\bar{a}(\beta)/\bar{b}'(\beta)$ is a zero of $F(x)$ and so equal to some μ_i. Then β is a zero of v_i. This shows that $\bar{b} = v_1 \cdots v_s$. Further every v_i and hence $\bar{b}$ divides $\bar{a} - \sum_i \mu_i (v_i'/v_i)\bar{b}$. The degree of the last expression is less than the degree of $\bar{b}$. Therefore the expression is 0 and $\bar{a}/\bar{b} = \sum_i \mu_i (v_i'/v_i)$. The p-curvature is equal to

$$\left(\frac{\bar{a}}{\bar{b}}\right)^{(p-1)} + \left(\frac{\bar{a}}{\bar{b}}\right)^p = \sum_i (\mu_i^p - \mu_i)\left(\frac{v_i'}{v_i}\right)^p.$$

It follows that the p-curvature is zero if and only if all $\mu_i \in \boldsymbol{F}_p$. Since $F(x)$ is the reduction of $R(x)$ modulo p, the condition that all the roots of $F(x)$ are in $\boldsymbol{F}_p$ is equivalent to p is totally split in the field Ω. □

3.1.1. Examples

(1) $r = z/(z^2+1)$. The resultant of b and b' is 4. The 2-curvature $r' + r^2 \bmod 2$ is equal to $1/(z^2+1)^2 \not\equiv 0 \bmod 2$. The minimal m such that $f' = mf$ has a solution in $\boldsymbol{Q}(z)^*$ is $m = 2$. The p-curvature is 0 for all $p \neq 2$.

(2) $r = 1/(z^2-2)$. Then $R(x) = -8x^2 + 1$ and $\Omega = \boldsymbol{Q}(\sqrt{2})$. Then p is split if $p \equiv \pm 1 \bmod 8$. The equation $y' = \bar{r}y$ over $\boldsymbol{F}_p(z)$ has a solution $\neq 0$ since $\bar{r} = (a_1/(z-b_1)) + (a_2/(z-b_2))$ with $a_1, a_2, b_1, b_2 \in \boldsymbol{F}_p$. Hence the p-curvature is 0.

If p is inert, i.e. $p \equiv \pm 3 \bmod 8$, then $\bar{r} = (a_1/(z-b_1)) + (a_2/(z-b_2))$ with a_1, $a_2, b_1, b_2 \in \boldsymbol{F}_{p^2}$. The p-curvature is then easily seen to be $((a_1^p - a_1)/(z-b_1)^p) + ((a_2^p - a_2)/(z-b_2)^p)$. However a_1 and a_2 are not in $\boldsymbol{F}_p$ and so the p-curvature is not zero.

3.2. Symbolic integration

For $r \in \boldsymbol{Q}(z)$ one wants to know whether $y' = r$ has a solution in $\boldsymbol{Q}(z)$. Write $r = (a/b) + c$, where $a, b, c \in \boldsymbol{Q}[z]$ satisfy g.c.d.$(a, b) = 1$, the degree of a is less than the degree of b and b is a primitive polynomial in $\boldsymbol{Z}[z]$. After multiplying r with an integer we may assume that $a, c \in \boldsymbol{Z}[z]$. The degree m of c and the highest multiplicity n of the zeroes of b play both a role. Put $s = \max(2+m, n)$. The square-free decomposition of b has the form $b = b_1 b_2^2 \cdots b_s^s$ with all b_i primitive polynomials in $\boldsymbol{Z}[z]$ and $\tilde{b} := b_1 b_2 \cdots b_s$ square-free. Let M denote the absolute value of the resultant of $\tilde{b}$ and $\tilde{b}'$.

In order to find an expression for the p-curvature we consider the differential module over $\boldsymbol{Q}(z)$ with basis e_1, e_2 and $\partial e_1 = re_2$; $\partial e_2 = 0$. The element e_1 is a cyclic element with minimal polynomial $\partial^2 - (r'/r)\partial$. The corresponding equation $y'' - (r'/r)y' = 0$ is the homogeneous equation associated with $y' = r$. Then $\partial^p(e_1) = r^{(p-1)}e_2$ and $\partial^p e_2 = 0$. Hence the p-curvature is 0 if and only if $r^{(p-1)} \equiv 0$ modulo p. Our problem is to find the relation between solvability of the equation and p-curvature.

Proposition 3.4. (1) *Let $y' = r$ have a solution in $\boldsymbol{Q}(z)$. Then for every prime p with $p \nmid M$ and $p \geq s$ the p-curvature is* 0.

(2) *Let $y' = r$ have no solution in $\boldsymbol{Q}(z)$. There are only finitely many primes p for which the p-curvature is* 0.

Proof. Let T denote $\boldsymbol{Z}[1/M(s-1)!]$. Then $r - c = (a/b) = (a/(b_1 b_2^2 \cdots b_s^s)) = (A/(b_1 \cdots b_{s-1}^{s-1})) - (B/b_s^s)$ holds with certain $A, B \in T[z]$. Write $B = Cb_s' + Db_s$ with $C, D \in T[z]$. Then

$$\frac{B}{b_s^s} = \left(\frac{C(1-s)^{-1}}{b_s^{s-1}}\right)' + \frac{C'(1-s)^{-1} + D}{b_s^{s-1}}.$$

In particular we have written $r = (E/(b_1 b_2^2 \cdots (b_{s-1} b_s)^{s-1})) + (F/n_s^{s-1})'$ with $E, F \in T[z]$. After finitely many steps of this type one finds a formula

$$r = c + \frac{G}{b_1 b_2 \cdots b_s} + \left(\frac{H}{b_1 b_2^2 \cdots b_s^s}\right)'$$

with $G, H \in T[z]$. Further c has a primitive in $T[z]$.

In case (1) the term G is zero and so for all primes p of T we have that the p-curvature is 0.

In case (2) the term G is not 0. For a prime p of T which does not divide G (i.e. G is not zero modulo p), the reduction modulo p of the term $G/(b_1 b_2 \cdots b_s)$ is not zero and has a simple pole. Therefore $r^{(p-1)}$ is not zero modulo p and the p-curvature is not 0. □

Remark 3.5. In the second case of the proposition it seems difficult to give an a priori estimate of the exceptional primes in T, since we do not know G beforehand.

3.3. The Risch equation

This is the equation $y' = ry + s$ with $r, s \in \boldsymbol{Q}(z)$. We suppose that $rs \neq 0$ and we are interested in algebraic solutions of the equation. Suppose that there exists a solution y_0 which is algebraic but does not lie in $\boldsymbol{Q}(z)$. Let K be a finite Galois extension of $\boldsymbol{Q}(z)$ which contains y_0 and let the Galois group of this extension be G. Let $|G|$ denote the order of G. Then $y_1 := (1/|G|) \sum_{\sigma \in G} \sigma(y_0)$ lies in $\boldsymbol{Q}(z)$ and is still a solution of the equation. Hence we may as well ask for a solution $y \in \boldsymbol{Q}(z)$.

Let M be the differential module over $\boldsymbol{Q}(z)$ generated by e_1, e_2 and satisfying $\partial e_1 = re_1 + se_2$; $\partial e_2 = 0$. Then there is an exact sequence of differential modules

$$0 \to \boldsymbol{Q}(z)e_2 \to M \to N \to 0,$$

where $N = \boldsymbol{Q}(z)e_3$ with $\partial e_3 = re_3$. The existence of a solution in $\boldsymbol{Q}(z)$ of $y' = ry + s$ is equivalent to the splitting of this exact sequence.

Let us for convenience suppose that $r, s \in R$, then the modules have an obvious structure of differential modules over R. In particular one can reduce the exact sequence modulo any prime p. The images of r and s in $\boldsymbol{F}_p(z)$ are denoted by r_p and s_p. The existence of a solution in $\boldsymbol{F}_p(z)$ of $y' = r_p y + s_p$ is again equivalent to the splitting of the exact sequence of the reduced modules.

If the module $\boldsymbol{F}_p(z)e_3$ with $\partial e_3 = r_p e_3$ is not the trivial module, or equivalently if the p-curvature $r_p^{(p-1)} + r^p \neq 0$, then the classification of differential modules over $\boldsymbol{F}_p(z)$ asserts that the sequence splits. Hence there is a solution $y_p \in \boldsymbol{F}_p(z)$.

If the p-curvature $r_p^{(p-1)} + r^p = 0$ then a solution $y_p \in \boldsymbol{F}_p(z)$ exists if and only if the p-curvature of M is 0.

Using this knowledge one can make examples where $y' = ry + s$ has no solution in $\boldsymbol{Q}(z)$ and where there is a solution of $y' = r_p y + s_p$ for every prime p.

Suppose that a solution $y \in \boldsymbol{Q}(z)$ exists. Then for a prime which does not divide the denominator of y one can reduce y to a solution in $y_p \in \boldsymbol{F}_p(z)$. If p divides the denominator then for some $m \geq 1$ the reduction of f of $p^m y$ modulo p exists and is not 0. Then f satisfies the equation $f' = r_p f$. This means that the p-curvature $r_p^{(p-1)} + r_p^p$ of $\boldsymbol{Q}(z)e_3$ is 0. As we will see any such prime can be a denominator of y.

The conclusion seems to be that the relation between the Risch equation and its reductions modulo primes is not obvious at all. This is illustrated by the following examples.

3.3.1. Examples

(1) The equation $y' = (1/z^2)y + 1$ has no solution in $\boldsymbol{Q}(z)$. Indeed, a possible solution y is easily seen to be of the form z^2F where F is a polynomial. The equation becomes $z^2F' + (2z-1)F = 1$. Over the field $\boldsymbol{Q}$ one sees that the degree of $z^2F' + (2z-1)F$ is one higher than the degree of F. Hence there is no solution.

Moreover the p-curvature of $\boldsymbol{Q}(z)e_3$ is easily seen to be z^{-2p} modulo p for every prime p. Hence there is a solution $y_p \in \boldsymbol{F}_p(z)$ for every p.

One can make this example more explicit by the substitution of $y = z^2F$ where F denotes a polynomial over $\boldsymbol{F}_p$. One considers the vector space V of the polynomials of degree $\leq p-2$. The map $F \mapsto z^2F' + (2z-1)F$ is injective because the homogeneous equation has no solution $\neq 0$ in $\boldsymbol{F}_p(z)$. Thus there is an $F_p \in V$, in fact of degree $p-2$, with $z^2F_p' + (2z-1)F_p = 1$.

It is interesting to compare this with the unique formal power series solution $y_\infty =: -z^2 \sum_{n \geq 0} (n+1)!z^n$ of the equation. This divergent power series has as reduction modulo p the unique solution $y_p = z^2F_p$. It seems that the reductions modulo p have some relation with the Stokes theory of this example.

Another translation of the example above is the following:

The associated second order homogeneous equation is $y'' - (1/z^2)y' + (2/z^3)y = 0$. This equation has only the trivial solution in $\boldsymbol{Q}(z)$. For every p there is a non trivial solution in $\boldsymbol{F}_p(z)$.

(2) The equation $y' = (1/(z^2-2))y - ((z^2-3)/(z^2-2)(z-3)^2)$ has as solution $(z+3)/7(z-3)$ with 7 in the denominator! In a similar way one can make for any prime p with $p \equiv \pm 1$ modulo 8, an example of a rational solution y of an equation $y' = (1/(z^2-2))y + s$ with $s \in R$ and p in the denominator of y.

3.3.2. More examples

In connection with the first example of 3.3.1, F. Beukers has raised the following question:

Let $y' = ay + b$ be a differential equation over $\bar{\boldsymbol{Q}}(z)$ such that every singular point of the equation $y' = ay$ is regular singular. Suppose that the equation has for almost all primes p a solution modulo p. Does the equation have a solution in $\bar{\boldsymbol{Q}}(z)$?

One can give the assumption in the question a precise meaning as follows. The equation is defined over some field $K(z)$ where K is a number field. The assumption is that for almost every maximal ideal $\boldsymbol{q}$ of the ring of integers of K the reduction modulo $\boldsymbol{q}$ exists and has a solution $\boldsymbol{F}_{\boldsymbol{q}}(z)$, where $\boldsymbol{F}_{\boldsymbol{q}}$ denotes the residue field of $\boldsymbol{q}$.

A test-case

One considers the equation

$$y' = \left(\frac{a+1}{z} + \frac{b+1}{z-1}\right) y + 1 \quad \text{with } a, b \in \bar{\boldsymbol{Q}} \backslash \boldsymbol{Z}.$$

A solution $y \in \bar{\boldsymbol{Q}}(z)$ of this equation must have the form $(z^2 - z)F$ where F is a polynomial with coefficients in $\bar{\boldsymbol{Q}}$. The term

$$L(F) := y' - \left(\frac{a+1}{z} + \frac{b+1}{z-1}\right) y$$

is equal to $(z^2 - z)F' + ((-a-b)z + a)F$. In particular $L(z^k) = (k - a - b)z^{k+1} + (-k + a)z^k$. It follows that the linear map $L : \bar{\boldsymbol{Q}}[z] \to \bar{\boldsymbol{Q}}[z]$ has 1 in its image if and only if $a + b$ is an integer ≥ 0.

Let $K = \boldsymbol{Q}(a, b)$. For a maximal ideal $\boldsymbol{q}$ of the ring of integers of K, lying above the rational prime p, we calculate now whether the equation has a solution 'modulo p'. We consider only the $\boldsymbol{q}$ such that the equation has a reduction modulo $\boldsymbol{q}$.

If the homogeneous equation $y' = (((a+1)/z) + (b+1)/(z-1))\, y$ has only the trivial solution modulo $\boldsymbol{q}$ then one knows (as before) that the inhomogeneous equation does have a solution modulo p. A direct proof is the following:

The map $y \mapsto y' - (((a+1)/z) + (b+1)/(z-1))\, y$ from $\bar{\boldsymbol{F}}_p(z)$ into itself is linear over $\bar{\boldsymbol{F}}_p(z^p)$ and has kernel 0. Hence the map is bijective.

The homogeneous equation $y' = (((a+1)/z) + (b+1)/(z-1))y$ does have a solution modulo $\boldsymbol{q}$ if and only if the reductions of a and b modulo $\boldsymbol{q}$ exist and lie in $\boldsymbol{F}_p$, where $\boldsymbol{q}$ lies above the rational prime p. We suppose now that the homogeneous equation has a solution modulo $\boldsymbol{q}$.

Let $N_0 = N_0(\boldsymbol{q})$, $N_1 = N_1(\boldsymbol{q})$, with $0 \leq N_i < p$ denote the representatives of a and $b \bmod \boldsymbol{q}$. A solution of the homogeneous equation is then $y_0 = z^{N_0+1}(z-1)^{N_1+1}$. By variation of constants (i.e. $y = y_0 f$) one transforms the inhomogeneous equation into $f' = z^{-N_0-1}(z-1)^{-N_1-1}$ or $z^p(z-1)^p f' = z^{p-N_0-1}(z-1)^{p-N_1-1}$. This is solvable if and only if this polynomial has no term z^{p-1}. This condition is equivalent to

$$N_0 + N_1 \geq p.$$

The question of F. Beukers for this special equation translates into:

Suppose that for almost all maximal ideals $\boldsymbol{q}$ of the ring of integers of $K = \boldsymbol{Q}(a, b)$ with residue field the prime field $\boldsymbol{F}_p$, one has that $N_0(\boldsymbol{q}) + N_1(\boldsymbol{q}) \geq p$. Is $a + b$ a non-negative integer?

Example $a = \frac{1}{2}$ *and* $b = \frac{1}{3}$

For $p \neq 2, 3$ one has $N_0(p) = (p+1)/2$ and $N_1(p) = (\varepsilon p + 1)/3$ with $\varepsilon = 1, 2$. Thus $N_0(p) + N_1(p) = ((3 + 2\varepsilon)p + 5)/6$. According to Dirichlet theorem on primes in an arithmetic progression, there are infinitely many primes p with $p \equiv -1 \bmod 3$. For this infinite set of primes $\varepsilon = 1$ and $N_0(p) + N_1(p) < p$.

The case where a, b *are rational*

Put $a = t_0/n_0$; $b = t_1/n_1$ with $1 < n_0 \leq n_1$ and g.c.d.(t_0, n_0) = g.c.d.$(t_1, n_1) = 1$. By Dirichlet's theorem we can choose infinitely many N_1's such that $n_1 N_1 - t_1 = p$ with p prime. Then $N_1 = N_1(p)$ and $N_0(p) = (\varepsilon p + t_0)/n_0$ with $1 \leq \varepsilon \leq n_0 - 1$. Clearly $N_0(p) + N_1(p) = ((n_0 + n_1\varepsilon)p + n_1 t_0 + n_0 t_1)/n_0 n_1$. Let Σ be the set of primes such that $n_1 N_1(p) - t_1 = p$ and $N_0 + N_1 \geq p$. By assumption Σ is infinite. This implies that $(n_0 + n_1(n_0 - 1))/n_0 n_1 \geq 1$ and so $n_0 = n_1$. Further for almost all $p \in \Sigma$ we have $\varepsilon = n_0 - 1$ and therefore $(n_1 t_0 + n_0 t_1)/n_0 n_1$ is an integer and ≥ 0. This proves that $a + b$ is a nonnegative integer. The conclusion is that Dirichlet's theorem implies the statement for $a, b \in \boldsymbol{Q} \setminus \boldsymbol{Z}$. One can show that Dirichlet's theorem on primes in an arithmetic progression is equivalent to the positive answer of the statement for $a, b \in \boldsymbol{Q} \setminus \boldsymbol{Z}$.

The case where a *or* b *is not rational*

We have not found an example where the question has a negative answer. To illustrate the question we take $a = \frac{1}{4}$ and $b = i$. The primes that we are interested in are the p with $p \equiv 1 \bmod 4$. For such a prime one has $N_0(p) = (3p + 1)/4$. Suppose that the question has a positive answer. Then there are infinitely primes p, with $p \equiv 1 \bmod 4$ such that the number N_1 defined by $0 < N_1 < (p/2)$ and $N_1^2 \equiv -1 \bmod p$ satisfies $N_1 < (p/4)$.

It seems to be unknown whether the last statement is true. The statement is rather close to the open question, raised by Hardy and Littlewood, whether there are infinitely many integers x for which $x^2 + 1$ is a prime number.

4. HOMOGENEOUS EQUATIONS OF ORDER TWO

We will assume that the differential field has characteristic $\neq 2$. Any operator $\partial^2 + a\partial + b$ can be transformed into $\partial^2 - r$ by applying the shift $\partial \mapsto \partial - (a/2)$. Hence it suffices to study $\partial^2 - r$ and the equation $y'' = ry$.

4.1. The p-curvature of the equation $y'' = ry$

As in Section 2 we suppose that k is a field of characteristic p such that $[k : k^p] = p$. One fixes a $z \in k$ such that $k = k^p(z)$. The differentiation $'$ of k is given by $z' = 1$. The differential module N corresponding to $\partial^2 - r$ (or to $y'' = ry$) has basis $e, \partial e$ and satisfies $\partial^2 e = re$. Euclidean division in $k[\partial]$ implies that $\partial^p = A(\partial^2 - r) + f\partial + g$ for certain $f, g \in k$. Then $\partial^{p+1} = (\partial A + f)(\partial^2 - r) + (f' + g)\partial + (fr + g')$. Hence $\partial^p e = ge + f\partial e$ and $\partial^p(\partial e) = (fr + g')e + (f' + g)\partial e$. The form of the operator $\partial^2 - r$ implies that the sec-

ond exterior power $\Lambda^2 N$ of N has a trivial ∂-action and trivial p-curvature. It follows that the matrix of the p-curvature of N has trace 0. Therefore $g = -\frac{1}{2}f'$. The matrix of $\partial^p = \psi_p$ on the basis $e, \partial e$ of N reads

$$\begin{pmatrix} -\frac{1}{2}f' & fr - \frac{1}{2}f'' \\ f & \frac{1}{2}f' \end{pmatrix}.$$

The determinant of ψ_p is $-\frac{1}{4}(f')^2 - f^2 r + \frac{1}{2}ff''$. According to 2.1 this term lies in k^p and its derivative is therefore 0. This leads to the differential equations $f^{(3)} - 4f^{(1)}r - 2fr^{(1)} = 0$ for f. We note that this differential equation is the second symmetric power of the equation $y^{(2)} = ry$.

In general, the term f is some formula in r and its derivatives, depending on the prime p. The formula can be found by Euclidean division in $k[\partial]$. For $p = 3, 5, 7, 11, 13$ one finds the formulas for f:

$$\begin{aligned} & r; \quad r^2 + 3r_2; \quad r^3 + 10r_1^2 + 13rr_2 + 5r_4; \\ & r^5 + 160r^2r_1^2 + 70r^3r_2 + 792r_1^2r_2 + 531rr_2^2 + 818rr_1r_3 + 336r_3^2 \\ & \quad + 166r^2r_4 + 558r_2r_4 + 306r_1r_5 + 91rr_6 + 9r_8; \\ & r^6 + 380r^3r_1 + 880r_1 + 125r^4r_2 + 7172rr_1^2r_2 + 2401r^2r_2 + 3465r_2^3 \\ & \quad + 3678r^2r_1r_3 + 16390r_1r_2r_3 + 4296rr_3^2 + 496r^3r_4 + 5280r_1r_4 \\ & \quad + 7048rr_2r_4 + 1650r_4^2 + 3760rr_1r_5 + 2838r_3 + r_5 + 553r^2r_6 \\ & \quad + 1771r_2r_6 + 748r_1r_7 + 174rr_8 + 11r_{10}. \end{aligned}$$

The notation r_i is used here to denote the i-th derivative $r^{(i)}$ of r.

In some cases the third order differential equation satisfied by f leads to a more or less explicit expression for f valid for every p.

4.2. Factoring $\partial^2 - r$ in characteristic p

A factorization of $\partial^2 - r$ in monic order 1 operators always has the form $\partial^2 - r = (\partial + u)(\partial - u)$. In the following we allow u to be separable algebraic over k.

It is clear that any u satisfies the Riccati equation $u' + u^2 = r$. Moreover the element $m := (\partial - u)e$ satisfies $\partial m = -um$. Hence $\partial^p(m) = -(u^{(p-1)} + u^p)m$ and therefore m is an eigenvector of ψ_p.

The eigenvalues of the ψ_p are $\pm(\frac{1}{4}(f')^2 + f^2 r - \frac{1}{2}ff'')^{1/2}$.
If the determinant of the ψ_p is not zero then the two solutions for u are

$$u = \frac{1}{2}\frac{f'}{f} \pm \left(-\frac{1}{4}\left(\frac{f'}{f}\right)^2 - \frac{1}{2}\left(\frac{f'}{f}\right) + r\right)^{1/2}.$$

If $f \neq 0$ and the determinant is 0 then there is only one solution $u = \frac{1}{2}(f'/f)$. Moreover $f^{1/2}$ satisfies $y^{(2)} = ry$.

If $f = 0$ then the formula does not make sense. But of course $\partial^2 - r$ still factors, since the equation $y'' = ry$ has a full set of solutions in k. There are infinitely many solutions for u in k.

We conclude that $\partial^2 - r$ always factors as $(\partial + u)(\partial - u)$ over k or over a quadratic extension of k.
If $f \neq 0$ then the elements u with this property satisfy

$$u^2 - \frac{f'}{f} u - r + \frac{1}{2}\left(\frac{f'}{f}\right)^2 + \frac{1}{2}\left(\frac{f'}{f}\right)' = 0.$$

We note that for any solution $h \neq 0$ of the differential equation $h^{(3)} - 4h^{(1)}r - 2hr^{(1)} = 0$ the elements v defined by

$$v = \frac{1}{2}\frac{h'}{h} \pm \left(-\frac{1}{4}\left(\frac{h'}{h}\right)^2 - \frac{1}{2}\left(\frac{h'}{h}\right)' + r\right)^{1/2}$$

satisfies $\partial^2 - r = (\partial + v)(\partial - v)$. In some cases one finds in this way a factorization of $\partial^2 - r$ without knowing f.

4.3. The equation $y^{(2)} = ry$ over $\boldsymbol{Q}(z)$

4.3.1. Differential Galois theory and the Riccati equation

In the following we summarize some results on the differential Galois group and Riccati equation for the equation $y^{(2)} = ry$.

The Picard–Vessiot theory is well defined over an algebraically closed base field. For the equation above we will work over the algebraic closure $\bar{\boldsymbol{Q}}$ of $\boldsymbol{Q}$. There is a Picard–Vessiot field $K \supset \bar{\boldsymbol{Q}}(z)$ for the equation $y^{(2)} = ry$. The set $V := \{ y \in K \mid y^{(2)} = ry \}$ is a vector space over $\bar{\boldsymbol{Q}}$ of dimension 2. The field K is generated over $\bar{\boldsymbol{Q}}(z)$ by V. The group G of the $\bar{\boldsymbol{Q}}(z)$-linear automorphisms of K, commuting with the differentiation, acts faithfully on V. In fact G is an algebraic subgroup of $Sl(V) = Sl(2, \bar{\boldsymbol{Q}})$. The component of the neutral element of G is denoted by G^0. For any $y \in V$ with $y \neq 0$ the element $u = y'/y$ satisfies the Riccati equation $u' + u^2 = r$ and $\partial^2 - r = (\partial + u)(\partial - u)$ holds. Further any solution of the Riccati equation has the form y'/y with $y \in V$ and $y \neq 0$. Transcendental solutions u of the Riccati equation are of no interest in this theory. A solution u of the Riccati equation is algebraic if and only if u is invariant under G^0. The last condition is equivalent to: the line $\bar{\boldsymbol{Q}}y$ in V is invariant under G^0. One has the following possibilities for algebraic solutions u of the Riccati equation:

1. If $G = Sl(2, \bar{\boldsymbol{Q}})$ then there is no algebraic solution u of the Riccati equation.

2. If G is reducible and contains the additive group $\boldsymbol{G}_a$ as algebraic subgroup then there is precisely one algebraic solution u of the Riccati equation. Moreover this u lies in $\boldsymbol{Q}(z)$.

3. If G is the multiplicative group $\boldsymbol{G}_m$ then there are two algebraic solutions u_1, u_2 of the Riccati equation. They lie in $L(z)$ where L is an extension of $\boldsymbol{Q}$ of degree 1 or 2. The polynomial $X^2 - (u_1 + u_2)X + u_1u_2 = X^2 - aX + b$ has coefficients in $\boldsymbol{Q}(z)$.

4. If G is the infinite dihedral group D_∞ then there are two algebraic solu-

tions u_1, u_2 of the Riccati equation. They lie in a quadratic extension of $\boldsymbol{Q}(z)$. The polynomial $X^2 - (u_1 + u_2)X + u_1u_2 = X^2 - aX + b$ has coefficients in $\boldsymbol{Q}(z)$.

5. If G is a finite group then there are infinitely many algebraic solutions of the Riccati equation.

Most of the statements above are well known from the Kovacic algorithm ([Ko]). The rationality statements about the algebraic solutions of the Riccati equation are proved in [HP].

4.3.2. Some observations

We will need more information about the $u, a, b \in \boldsymbol{Q}(z)$. For any prime p one introduces a discrete valuation ord_p on $\boldsymbol{Q}(z)$ which extends to usual p-adic discrete valuation ord_p on $\boldsymbol{Q}$. For elements in $\boldsymbol{Z}[z]$ one defines $\mathrm{ord}_p(a_0 + a_1z + \cdots a_sz^s) = \mathrm{ord}_p(\mathrm{g.c.d.}(a_0, \ldots, a_s))$. For arbitrary $(a/b) \in \boldsymbol{Q}(z)$ one defines $\mathrm{ord}_p(a/b) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$. We note that the subring R of $\boldsymbol{Q}(z)$ consists of the elements f with $\mathrm{ord}_p(f) \geq 0$ for all primes p. For $f \in \boldsymbol{Q}(z)$; $f \neq 0$ one defines $\mathrm{den}(f)$ to be the smallest integer $m \geq 1$ with $mf \in R$.

In connection with case 2 of 4.3.1 we consider a solution $u \in \boldsymbol{Q}(z)$ of the Riccati equation $u' + u^2 = r$. Let p be a prime with $\mathrm{ord}_p(u) < 0$. Then the equation implies that $\mathrm{ord}_p(u) = \frac{1}{2}\mathrm{ord}_p(r)$. This shows that $\mathrm{den}(r)$ is a square, say n^2, and that $\mathrm{den}(u) = n$. Moreover, the equation $n(nu)' + (nu)^2 = n^2r$ proves that the residue of n^2r in R/nR is a square of an element in R/nR. The two conditions above are new necessary conditions (in addition to the ones in [Ko]) on r for the existence of a solution $u \in \boldsymbol{Q}(z)$ of the Riccati equation.

In connection with the cases 3 and 4 of 4.3.1 we recall from [Ko] that the polynomial $X^2 - aX + b$ is determined by the properties: $b = \frac{1}{2}a' + \frac{1}{2}a^2 - r$ and a is a solution of the Riccati equation

$$w^{(2)} + 3ww^{(1)} + w^3 - 4wr - 2r^{(1)} = 0,$$

associated to the second symmetric power

$$h^{(3)} - 4h^{(1)}r - 2hr^{(1)} = 0 \quad \text{of the equation} \quad y^{(2)} - ry = 0.$$

From $a^{(2)} + 3aa^{(1)} + a^3 - 4ar - 2r^{(1)} = 0$ one can easily derive an estimate for $\mathrm{den}(a)$. If the prime $p > 2$ satisfies $\mathrm{ord}_p(a) < 0$ then $\mathrm{ord}_p(a) = \frac{1}{2}\mathrm{ord}_p(r)$. If $\mathrm{ord}_2(a) \leq -2$ then $\mathrm{ord}_2(a) = \frac{1}{2}\mathrm{ord}_2(r)$. If $\mathrm{ord}_2(a) = -1$ then $\mathrm{ord}_2(r) \leq -4$.

The connection between $X^2 - aX + b$ and this second Riccati equation holds in a more general context. Let $p > 2$ and $e \geq 1$ an integer. On the ring $R/(p^e)[X]$ one defines a differentiation $'$ by: on R/p^eR this is the differentiation induced by $'$ on R and $X' = r - X^2 \bmod p^e$. The ideal $(X^2 - aX + b) \subset R/(p^e)[X]$ is invariant under differentiation if and only if $b \equiv \frac{1}{2}a' + \frac{1}{2}a^2 - r \bmod p^e$ and $a^{(2)} + 3aa^{(1)} + a^3 - 4ar - 2r^{(1)} \equiv 0 \bmod p^e$.

As in the Kovacic algorithm one tries to solve $y^{(2)} = ry$ by producing algebraic solutions of the Riccati equation. Unlike the Kovacic algorithm we do this by trying to lift solutions modulo primes to characteristic 0. This method will only produce algebraic solutions of the Riccati equation of degree 1 or 2

over $\boldsymbol{Q}(z)$ since the solutions that we find of the reduced equation $u' + u^2 = r \bmod p$ are of degree 1 or 2 over $\boldsymbol{F}_p(z)$.

On the other hand a solution $u \in \boldsymbol{Q}(z)$ of the Riccati equation satisfies $\operatorname{ord}_p(u) \geq 0$ if $\operatorname{ord}_p(r) \geq 0$. Hence $u \bmod p^e$ is a solution of $u' + u^2 = r \bmod p^e$. In the case of algebraic solutions of degree 2 over $\boldsymbol{Q}(z)$, the ideal $(X^2 - aX + b)$ considered above reduces modulo p^e (where $p > 2$ and $\operatorname{ord}_p(r) \geq 0$) to an ideal of $R/(p^e)[X]$ which is invariant under differentiation. The two solutions of $X^2 - aX + b \equiv 0$ in R/p^e or in a quadratic extension of R/p^e are solutions modulo p^e of the Riccati equation $u' + u^2 \equiv r \bmod p^e$.

4.3.3. Procedure

(1) One tries to find a small prime p with $p > 2$ and $\operatorname{ord}_p(r) \geq 0$ such that p-curvature of the reduced equation is not zero. This can be done by a direct calculation of the term f of 4.1. Another way is to consider the $\boldsymbol{F}_p(z^p)$ linear operator $L_p : \boldsymbol{F}_p(z) \to \boldsymbol{F}_p(z)$, given by $L_p(y) = y^{(2)} - ry \bmod p$. The p-curvature is 0 if and only if the dimension of the kernel of L_p is two.

If this is not successful then one conjectures that the differential Galois group G is finite. Another algorithm, along the lines of [BD], should be developed to deal with $y^{(2)} = ry$ under the assumption that the differential Galois group is finite.

(2) Suppose that a prime p is found with non-zero p-curvature. Let M denote the differential module over $\boldsymbol{F}_p(z)$ corresponding to the reduced equation. By construction, the second exterieur power $\Lambda^2 M$ is a trivial differential module. This leads to the following possibilities for the classification of M.

1. $M \cong I(t^2)$ and the dimension of $\ker(L_p)$ is 1.
2. $M \cong I(t - \alpha) \oplus I(t + \alpha)$ with $\alpha \in \boldsymbol{F}_p(z^p)^*$. In this case $\ker(L_p) = 0$.
3. $M \cong I(t^2 - \beta)$ with $\beta \in \boldsymbol{F}_p(z^p)$ and β not a square. Again $\ker(L_p) = 0$.

(3) If $M \cong I(t^2)$ then one makes the guess that the differential Galois G is reducible and contains $\boldsymbol{G}_a$. First one verifies the necessary conditions for the existence of a solution $u \in \boldsymbol{Q}(z)$ of the Riccati equation. Let $\operatorname{den}(r) = n^2$ then $nu \in R$ has the form $nu = A/B$ where $A, B \in \boldsymbol{Z}[z]$; B primitive and $\text{g.c.d.}(A, B) = 1$. Let $f \in \boldsymbol{F}_p(z)$ be a non zero solution of $y^{(2)} \equiv ry \bmod p$. Then f'/f is the only solution of the Riccati equation $\bmod p$. We want to lift $n(f'/f) = (a/b) \in R/pR$, with $a, b \in \boldsymbol{F}_p[z]$; b monic and $\text{g.c.d.}(a, b) = 1$, to a suitable element $(A/B) \in R$. One can calculate the finitely many possibilities for $A, B \in \boldsymbol{Z}[z]$ such that:

- The coefficients of A and B are in $\{-(p-1)/2, \ldots, (p-1)/2\}$.
- B is primitive.
- $A \equiv ca$ and $B \equiv cb \bmod p$ for some $c \in \boldsymbol{F}_p^*$.

If for some $v_0 = A/B$ the element v_0/n satisfies the Riccati equation then we are done. If not then we try to refine v_0. The refinement $v_0 + pw$ should satisfy $n(v_0 + pw)' + (v_0 + pw)^2 \equiv n^2 r \bmod p^2$. This leads to the equation $nw' + 2v_0 w \equiv (n^2 r - nv_0' - v_0^2)/p \bmod p$. The $\boldsymbol{F}_p(z^p)$-linear map $w \mapsto nw' + 2v_0 w$ on the vector space $\boldsymbol{F}_p(z)$ has a kernel of dimension 1. Hence the equation may not have a solution w. In that case we conclude that $u' + u^2 = r$ has no solution in $\boldsymbol{Q}(z)$.

If there is a solution w then we choose one and find a lift $v_1 \in R$ (similarly to the construction as above) which gives a candidate $v_1/n \in \boldsymbol{Q}(z)$ for the Riccati equation. One can continue this process.

(4) We suppose now that $\ker L_p = 0$. The second symmetric power of the module M is isomorphic to $N \oplus I(t)$ where N is either $I(t-2\alpha) \oplus I(t+2\alpha)$ or $I(t^2-4\beta)$. Let f be a non zero solution of the operator $\mathrm{Sym}^2 L_p = \partial^3 - 4r\partial - 2r^{(1)}$ acting on $\boldsymbol{F}_p(z)$. Since f is unique up to multiplication by an element in $\boldsymbol{F}_p(z^p)^*$ one finds a unique solution $a_0 := f'/f$ on the second Riccati equation $a^{(2)} + 3aa^{(1)} + a^3 - 4ar - 2r^{(1)} \equiv 0 \bmod p$. We will show now that a_0 has a unique lift $a_e \in R/p^e R$ which satisfies $a^{(2)} + 3aa^{(1)} + a^3 - 4ar - 2r^{(1)} \equiv 0 \bmod p^e$. Let the existence and uniqueness of a_e already be shown. Let $\tilde{a}_e$ denote any lift of a_e to $R/p^{e+1}R$. Then $a_{e+1} = \tilde{a}_e + p^e w$ for some $w \in R/pR$. The condition that a_{e+1} satisfies the second Riccati equation mod p^{e+1} leads to the following differential equation for w:

$$w^{(2)} + 3a_0 w' + (3a_0' + 3a_0^2 - 4r)w = \frac{-(\tilde{a}_e^{(2)} + 3\tilde{a}_e\tilde{a}_e' + \tilde{a}_e^3 - 4\tilde{a}_e r - 2r')}{p^e}.$$

The homogeneous differential equation $w^{(2)} + 3a_0 w' + (3a_0' + 3a_0^2 - 4r)w = 0$ is the differential equation corresponding to the module N defined above. The kernel of ∂ on N is 0 and one concludes that the $\boldsymbol{F}_p(z^p)$-linear operator

$$\partial^2 + 3a_0\partial + (3a_0' + 3a_0^2 - 4r) : \boldsymbol{F}_p(z) \to \boldsymbol{F}_p(z)$$

is bijective. This proves the existence and uniqueness of a_{e+1}.

Suppose that a_e is calculated. Let m be an estimate for $\mathrm{den}(a)$. Then $ma_e \in R/p^e R$ can be lifted to R by the method described in (3) or with LLL-reduction. This may lead to a solution $a \in R$ of the second Riccati equation.

(5) If the prime p of (1) does not lead to a solution of the Riccati equation then one can try to find another prime q with non zero q-curvature. For q one proceeds as before and one combines the results for p and q to obtain solutions modulo $p^n q^m$ of the Riccati equation.

Remarks. There are two main difficulties that can occur in the search above. The first one would be that for the considered primes the p-curvature 0. In that case one expects that the differential equation $y^{(2)} = ry$ has only algebraic solutions (or equivalently G is finite).

A theoretical complication is that Grothendieck's conjecture for order two equations is not completely proved. The missing case is to show that for an equation with differential Galois group $Sl(2)$ there are infinitely many primes p with non zero curvature.

The other difficulty would be that a fair number of different primes p with $\psi_p \neq 0$ do not lead to a solution u of $u' + u^2 = r$. This could mean either that u does not exist (and so $G = Sl(2)$) or that u exists but is a rather complicated expression in terms of degrees and height of the coefficients occurring in u.

5.1. $y^{(2)} = (c/z^4)y$

Here c denotes a non zero rational number. For a prime p which does not divide the denominator and the numerator of c one can explicitly calculate ψ_p. With the notations of 4.1 one can see that f is a polynomial in z^{-1} with highest term $c^{(p-1)/2}z^{-2p+2}$. Using that f also satisfies the differential equation $f^{(3)} - 4f^{(1)}r - 2fr^{(1)} = 0$ one finds that $f = c^{(p-1)/2}z^{-2p+2}$. Then $f'/f = 2/z$ is a modulo p solution of the second Riccati equation. One verifies that $2/z$ is an actual solution. The polynomial $X^2 - aX + b$ is then known, $a = 2/z$ and $b = \frac{1}{2}a' + \frac{1}{2}a^2 - r = z^{-2} - cz^{-4}$. The two solutions of the Riccati equation $u' + u^2 = r$ are therefore $z^{-1} \pm \sqrt{c}z^{-2}$.

The differential Galois group of the equation must be $\boldsymbol{G}_m$ since a finite cyclic differential Galois group would imply that almost all p-curvatures are 0.

5.2. $y^{(2)} = (\frac{5}{16}z^{-2} + z)y$

For the prime $p = 3$ one finds by 4.1 that $f = r = -z^{-2} + z$ and $f'/f = z^{-1}$ is a solution modulo 3 of the second Riccati equation. One can refine this to the solution $z^{-1} + 3z^{-1} = 4z^{-1}$ modulo 9 of the second Riccati equation.

A possible solution $a \in \boldsymbol{Q}(z)$ of the second Riccati equation has $\mathrm{ord}_2(a) \geq -2$ and $\mathrm{ord}_p(a) \geq 0$ for all $p > 2$. Hence $4a \in R$. Now $4a \equiv 16z^{-1} \equiv -2z^{-1}$ mod 9, leads to the choice $a = -\frac{1}{2}z^{-1}$. This is an actual solution of the second Riccati equation. The term $b = \frac{1}{2}a' + \frac{1}{2}a^2 - r = 1/16z^2 - z$ and the two solutions of $u' + u^2 = r$ are $-\frac{1}{4}z^{-1} \pm z^{1/2}$. The differential Galois group is D_∞. We note that the equation is in fact one of the rare examples of an equation with two singular points and differential Galois group D_∞.

5.3. $y^{(2)} = (24/(z^2 - 1)^2)y$

Clearly ψ_2 and ψ_3 are 0. For the prime $p = 5$ the corresponding f is equal to $-(z^2 - 1)^{-4}$ and the determinant of the matrix of ψ_5 is 0. This leads to a unique solution $u_5 = z/(z^2 - 1)$. The lift of u_5 to $\boldsymbol{Q}(z)$ has the same form and does not satisfy the equation. However $z/(z^2 - 1)$ satisfies the Riccati equation modulo 5^2. A refinement of this solution to a solution modulo 5^3 of the form $z/(z^2 - 1) + 25w$ does not work! Let us try nevertheless $z/(z^2 - 1) + 5w$ as a solution modulo 5^3. This leads to the equation

$$w' + \frac{2z}{z^2 - 1}w + 5w \equiv \frac{5}{(z^2 - 1)^2} \text{ modulo } 5^2.$$

Then $w + (2z/(z^2 - 1))w \equiv 0$ modulo 5. This implies that $w = c/(z^2 - 1)$ where c is a 'constant'. One finds at once that $c = 1$. This modulo 5^3-solution $(z + 5)/(z^2 - 1)$ for the Riccati equation turns out to be a solution in $\boldsymbol{Q}(z)$. We have thus found a factorization $\partial^2 - 24/(z^2 - 1)^2 = (\partial + u)(\partial - u)$ with $u = (z + 5)/(z^2 - 1)$. A further inspection learns that $y' = uy$ has the solution $y_1 := (z^2 - 1)^{-2}(z - 1)^5$. Finally by variation of constants one finds a second solution

in $y_2 := (z^2-1)^{-2}(5z^4+10z^2+1) \in \boldsymbol{Q}(z)$ of $y^{(2)} = 24/(z^2-1)^2$. This means that the equation is trivial. For any prime $p \neq 5$ the reductions of y_1 and y_2 mod p are linearly independent over $\boldsymbol{F}_p(z^p)$. Hence $\psi_p = 0$ for $p \neq 5$. The reductions of y_1 and y_2 mod 5 are linearly dependent over $\boldsymbol{F}_5(z^5)$. This explains why $\psi_5 \neq 0$.

5.4. The Airy equation

This is the equation $y^{(2)} = zy$. It is well known that the differential Galois group G of this equation is $Sl(2)$. We want to show that this can be found by using the information from the p-curvature for every $p > 2$. With the notation of 4.1, one sees that f is a polynomial with highest term $z^{(p-1)/2}$. Using that f is a solution of the differential equation

$$f^{(3)} - 4f^{(1)}r - 2fr^{(1)} = 0,$$

one obtains the following expression for f:

$$z^{(p-1)/2} + a_1 z^{(p-1)/2-3} + a_2 z^{(p-1)/2-6} + a_3 z^{(p-1)/2-9} + \cdots,$$

where the a_i can be found by linear algebra. For $p = 3, 5, 7, 11, 13, 17, 19$ one finds that f is equal to:

$$z; z^2; z^5 + 6z^2; z^6 + 3z^3 - 4; z^8 + 6z^5 + 2z^2; z^9 - 4z^6 + z^3 + 3.$$

The first conclusion is that G cannot be a finite group. The determinant of ψ_p is a polynomial of degree p with highest term $-z^p$. This is not a square in $\boldsymbol{F}_{p^2}(z)$ and the equation $u' + u^2 \equiv r \bmod p$ has no solutions in $\boldsymbol{F}_{p^2}(z)$. Therefore G cannot be reducible group containing $\boldsymbol{G}_a$ nor can it be $\boldsymbol{G}_m$. The only possibilities for G are now $Sl(2)$ and the infinite imprimitive subgroup D_∞. We still have to exclude the latter possibility.

If $G = D_\infty$ then algebraic solution u of the Riccati equation are the zeroes of a certain polynomial $X^2 - aX + b$. The element a lies in R and for every $p > 2$ the reduction mod p of a is equal to f'/f. From the differential equation for f one sees that f and f' have no common factor. The degree of f is $(p-1)/2$. This shows that a does not exist. We conclude that the differential Galois group of the Airy equation is $Sl(2)$.

6. HIGHER ORDER EQUATIONS

6.1. Factoring in characteristic $p > 0$

Suppose that the field k has the property $[k : k^p] = p$. Let $z \in k$ satisfy $k = k^p[z]$ and let the differentiation $'$ be given by $z' = 1$. The fields $\boldsymbol{F}(z)$ and $\boldsymbol{F}((z))$, where $\boldsymbol{F}$ is a finite field or the algebraic closure of $\boldsymbol{F}_p$, will be called *special fields*. For those fields one can write algorithms.

The differential operator L, that we want to factor, is supposed to be monic and to have degree n. The operator L induces a differential module $N := k[\partial]/k[\partial]L$ of dimension n over k. Let e denote the image of $1 \in k[\partial]$ in N. Then $e, \partial e, \ldots, \partial^{n-1} e$ is a basis of N.

The monic left hand factors of degree d of L are in a one-to-one correspondence with the submodules M of dimension d over k of N. Indeed, for a submodule M there is a minimal monic operator L_2 of degree $n-d$ such that $L_2 e \in M$. Then $L = L_1 L_2$ holds for some monic L_1 of degree d. On the other hand, a factorization $L = L_1 L_2$ with L_1, L_2 monic of degrees d and $n-d$ gives rise to the submodule M with basis $L_2 e, \partial L_2 e, \ldots, \partial^{d-1} L_2 e$.

The classification (see 2.1) applied to N gives in principle the possible submodules M of N and all the factorizations of L. We have to see how this can be done in an algorithmic way.

6.1.1. *Calculation of ψ_p and its characteristic polynomial $G(T)$*

The matrix of the k-linear operator ψ_p with respect to the basis $e, \partial e, \ldots, \partial^{n-1} e$ can be calculated as follows. Using the Euclidean division in $k[\partial]$ one finds expressions $\partial^{p+i} = A_i L + B_i$ for $i = 0, \ldots, n-1$ with $\text{degree}(B_i) < n$. The $B_0 e, \ldots, B_{n-1} e$ are the columns of the matrix of ψ_p. Indeed, $\psi_p \partial^i e = \partial^{p+i} e = (A_i L + B_i) e = B_i e$. In principle the characteristic polynomial $G(T)$ of ψ_p is computable.

An alternative way would be to calculate the characteristic polynomial $F(T)$ of ∂ seen as a k^p-linear map on N. Using $G(T) = F(T^{1/p})$ one finds $G(T)$. This shows moreover that $F(T) \in k^p[T^p]$ and we have to compute only $n+1$ coefficients in k^p.

6.1.2. *Factoring $G(T)$*

If the factorization $G(T) = F_1^{m_1} \cdots F_s^{m_s}$ is known then one can explicitly find the decomposition $N = \bigoplus_{i=1}^{s} N_i$. A certain factorization of L is a consequence of this.

For *special fields* k it seems possible to factor polynomials over k. If $k = \boldsymbol{F}(z)$ then we have to consider in fact factorizations of polynomials over $\boldsymbol{F}[z]$. This is done by factorizations over $\boldsymbol{F}[z]/\boldsymbol{m}$ for various maximal ideals $\boldsymbol{m}$.

If $k = \boldsymbol{F}((z))$ then one uses Newton polygons and Newton approximation to find a factorization over $\boldsymbol{F}((z))$.

The special case where one wants to find *linear factors* (or zeroes in k^p) of $G(T)$ is rather easy. For $k = \boldsymbol{F}(z)$ one writes $G(T)$ as

$$a_n^{-1}(a_n T^n + \cdots + a_1 T + a_0),$$

where $a_0, \ldots, a_n \in \boldsymbol{F}[z^p]$ have g.c.d. 1. The zeroes of $G(T)$ in k^p have the form a/b where a is a divisor of a_0 and where b is a monic divisor of a_n.

For $k = \boldsymbol{F}((z))$ the Newton polygon of $G(T)$ determines the valuations of the possible zeroes of $G(T)$ in k^p. By Newton approximation one can calculate a zero in k^p up to any order.

6.1.3. *Left hand factors of degree 1*

We are looking for the possible factorizations

$$L = (\partial + u)(\partial^{n-1} + a_{n-2}\partial^{n-2} + \cdots + a_0).$$

The vector $m := a_0 e + a_1 \partial e + \cdots + a_{n-2} + \partial^{n-1} e \in N$ has the property $\partial m = -um$. From $\partial m = -um$ one can deduce that $\psi_p m = -(u^{(p-1)} + u^p)m$. The element $-(u^{(p-1)} + u^p)$ lies in k^p. Therefore m is an eigenvector of ψ_p corresponding to an eigenvalue of ψ_p belonging to k^p.

On the other hand suppose that we have found an eigenvector $m = a_0 e + a_1 \partial e + \cdots + a_{n-2} + \partial^{n-1} e$ of ψ_p corresponding to an eigenvalue $\lambda \in k^p$ of ψ_p. Since ψ_p and ∂ commute and $\lambda' = 0$ one finds that $\psi_p(\partial m) = \lambda \partial m$. If the kernel M of $\psi_p - \lambda$ on N has dimension one over k then $\partial m = um$ for some $u \in k$ and we found a left hand factor of degree 1.

If the kernel M of $\psi_p - \lambda$ has dimension greater than 1 then according to the classification N contains at least a direct sum $I(F^a) \oplus I(F^b)$ where $F = \partial^p - \lambda$. It follows that N contains infinitely many copies of $I(F)$ and so L has infinitely many left hand factors of degree 1. In this case it seems not useful to calculate one of those left hand factors.

6.2. Left hand factors of degree one over $\boldsymbol{Q}(z)$

The operator $L \in \boldsymbol{Q}(z)[\partial]$ is supposed to be monic of degree n. The *denominator of* L is defined to be the smallest positive integer m such that $mL \in R[\partial]$. Suppose that there is a decomposition

$$L = (\partial + u)(\partial^{n-1} + a_{n-2}\partial^{n-2} + \cdots + a_0),$$

with $u, a_{n-2}, \ldots, a_0 \in \boldsymbol{Q}(z)$. Let p be a prime not dividing m then we know that p does not divide the denominators of the two terms. Therefore one finds a decomposition of $L \bmod p$. In particular, $\partial + u \bmod p$ is a left hand factor of $L \bmod p$. In the sequel we will suppose for convenience that $m = 1$.

If one is in the lucky situation that for every zero λ in k^p of the characteristic polynomial of the ψ_p there is only one eigenvector then the number of possibilities for $u \bmod p$ is $\leq n$. Each possible $u \bmod p$ can be lifted to an element of $R \subset \boldsymbol{Q}(z)$ in the way described in 4.3. One finds then a number of guesses $u_1, \ldots, u_s$ with $s \leq n$ for u. Division of L by the $\partial + u_i$ may lead to a factorization of L.

If no factorization is found then one has several possibilities to continue the search for u. The first one tries to solve $L \equiv (\partial + u)(\partial^{n-1} + \cdots) \bmod p^2$ (or modulo higher powers of p). This can be done as follows:

Let v_0 denote one of the u_i. Write $L = (\partial + v_0)A + pf$ (division of L by $(\partial + v_0)$) where $f \in R$. Let $v_1 \in \boldsymbol{F}_p(z)$ and $B \in \boldsymbol{F}_p(z)[\partial]$ of degree less than $n - 1$. Then we want to solve

$$L \equiv (\partial + v_0 + pv_1)(A + Bp) \bmod p^2.$$

This amounts to the equation $v_1 A + (\partial + v_0)B \equiv f \bmod p$. In making this explicit one finds an inhomogeneous differential equation $K(v_1) = f$ of order $n - 1$ for v_1. The assumption that $\lambda \in k^p$ is a simple zero of $G(T)$ implies that

$K(w) = 0$ has no solutions $w \neq 0$ in k. It follows that the k^p-linear operator $K : k \to k$ is invertible. Linear algebra over k^p yields the unique v_1.

A second possibility is to take another prime q and use the information of L mod q. This can give a finite number of guesses for u modulo pq.

It is not clear at the moment how efficient the method above will be.

REFERENCES

[A1] André, Y. – Quatre descriptions des groupes de Galois différentielles. Séminaire d'algèbre de Paris 86/87, Lect. Notes in Math. **1296** (1987).

[A2] André, Y. – Notes sur la théorie de Galois différentielle. IHES/M/89/49. Preprint (1989).

[BD] Baldassarri, F. and B. Dwork – Differential equations with algebraic solutions. Amer. J. Math. **101** (1), 42–76 (1979).

[Ho] Hoeppner, S. – Lineare Differentialgleichungen zweiter Ordnung in positive Charakteristik. Inst. f. Exper. Math. Essen. Preprint (1995).

[HP] Hendriks, P.A. and M. van der Put – Galois actions on the solutions of a differential equation. To appear in Journal of Symbolic Computation.

[J] Jaeger, A. – Gewöhnliche Differentialgleichungen in Körpern von Primzahlcharakteristik. Monatsheft für Math. **56** (1952).

[K1] Katz, N. – A conjecture in the arithmetic theory of differential equations. Bull. Soc. Math. France **110**, 203–239 (1982).

[K2] Katz, N. – On the calculations of some differential Galois groups. Invent. Math. **87**, 13–61 (1987).

[Ko] Kovacic, J. – An algorithm for solving second order linear homogeneous differential equations. J. of Symbolic Computation, 3–43 (1986).

[Ks] Kasch, F. – Über die Riccatische Differentialgleichung in Körper der Charakteristik p. Arch. der Math. **4**, 17–22 (1953).

[L] Levelt, A.H.M. – Lectures on symbolic integration. University of Nijmegen (1992).

[P] Put, M. van der – Differential equations in characteristic p. To appear in Compositio Math. (1995).