A note on the arithmetic of differential equations

José Felipe Voloch

In this note we give a method for computing the differential Galois group of some linear second-order ordinary differential equations using arithmetic information, namely the p-curvatures.

1. Introduction

Let K be a number field and consider a finite extension $F/K(x)$, where x is an indeterminate, with derivation $D = d/dx$. To a linear differential equation $Ly = \sum_{i=0}^{n} c_i D^i y = 0, c_i \in F$, one associates its differential Galois group G, which is a linear algebraic subgroup of GL_n defined over F and isomorphic over $\bar{F}$ to a group defined over K.

A conjecture of Katz [K3], which generalizes a conjecture of Grothendieck, predicts that the Lie algebra of G is the smallest F-Lie subalgebra of of the Lie algebra of GL_n, whose reduction modulo primes p contains the p-curvature of L, for all sufficiently large p. The p-curvature of L is the $n \times n$ matrix $A_p (\mathrm{mod}\, p)$ where $(D^p y, D^{p+1} y, \ldots, D^{p+n-1} y)^t = A_p (y, Dy, \ldots, D^{n-1} y)^t$. Katz has shown ([K3]) that the p-curvatures of L all belong to the Lie algebra of G. We will show, in some cases where we have an a priori restriction on G, that the fact that its Lie algebra contains the p-curvatures is enough to determine G. This gives an affirmative answer, in these cases, to the question posed at the end of the introduction of [K4].

From now on, assume that $n = 2$, that is L is a second-order linear differential operator. We will also assume that c_1/c_2 is the logarithmic derivative of an element of F. As is well-known, this is equivalent to the Galois group G of L be a subgroup of SL_2. Let us write

$$A_p = \begin{pmatrix} a_p & b_p \\ a_{p+1} & b_{p+1} \end{pmatrix}$$

From the fact that c_1/c_2 is a logarithmic derivative, it follows that the p-curvature of the determinant of $Ly = 0$ is always zero, which means that the trace of the p-curvature

of $Ly = 0$ is zero, that is $b_{p+1} = -a_p$.

For an example that will be useful in the sequel, take the equation $D^2y = ay$, where a has expansion $\alpha x^k + \cdots$, with $k > 0$ at a place P of F/K above $x = \infty$, so a has a pole there. Then $D^n y = a_n y + b_n Dy$, where $a_2 = a, b_2 = 0$ and, for $n > 2$, $a_{n+1} = Da_n + ab_n, b_{n+1} = Db_n + a_n$. It follows by induction that the a_n, b_n have the following expansion at P:

$$a_{2n} = \alpha^n x^{kn} + \cdots, b_{2n} = kn(n-1)\alpha^{n-1}x^{k(n-1)-1} + \cdots,$$
$$a_{2n+1} = kn^2\alpha^n x^{kn-1} + \cdots, b_{2n+1} = \alpha^n x^{kn} + \cdots.$$

it follows that, for a prime $p = 2n + 1$,

$$A_p = \begin{pmatrix} kn^2\alpha^n x^{kn-1} + \cdots & \alpha^n x^{kn} + \cdots \\ \alpha^{n+1}x^{k(n+1)} + \cdots & kn(n+1)\alpha^n x^{kn-1} + \cdots \end{pmatrix}. \qquad (*)$$

Another result that will be useful in the sequel is the following lemma.

Lemma. *Let p be a prime sufficiently large and consider the equation $Ly = 0$ modulo p and assume it has a solution $y \neq 0$ with $u = Dy/y$ separable algebraic over $\mathbf{F}_p(x)$ and that A_p has trace zero. Then u satisfies $b_p u^2 + 2a_p u - a_{p+1} = 0$.*

Proof: Since u is separable algebraic over $\mathbf{F}_p(x)$, we have $D^p u = 0$. Since D^p is a derivation we get $D^{p+1}y = D^p(uy) = uD^p y$. On the other hand, by definition of A_p, $D^p y = a_p y + b_p Dy = y(a_p + b_p u), D^{p+1}y = a_{p+1}y + b_{p+1}Dy = y(a_{p+1} + b_{p+1}u)$. Thus, $a_{p+1} + b_{p+1}u = u(a_p + b_p u)$ and using that $b_{p+1} = -a_p$, we get the equation stated in the lemma.

2. Proper subgroups of SL_2

The list of proper algebraic subgroups of SL_2, up to conjugation, is well-known and we will go through the list pointing out facts relevant to our purposes. Our arguments in this section are based on the work of van der Put [P].

2.1 G finite

In this case all the solutions to the equation $Ly = 0$ are algebraic. This leads to infinitely many Dy/y which are also algebraic and the equation of the lemma therefore has infinitely many solutions, which proves that the p-curvature is zero.

2.2 $G \cong \mathbf{G}_m$

In this case G is conjugate to the group of diagonal matrices with determinant 1. The action of G on the space of solutions of $Ly = 0$ has two invariant lines, generated by y_1, y_2, say. Since the lines are invariant, the logarithmic derivatives $u_i = Dy_i/y_i$ are invariant under G, which means that the u_i are in F but are not logarithmic derivatives, for otherwise we would be in the case G finite.

We then obtain from the Lemma the following two relations among the entries of the p-curvature $b_p u_i^2 + 2a_p u_i - a_{p+1} = 0, i = 1, 2$. Recall that we also have $b_{p+1} = -a_p$, since the p-curvature has trace zero. These relations are easily seen to be independent.

2.3 G extension of $\mathbf{Z}/2$ by $\mathbf{G}_m$

In this case G is conjugate to the group of diagonal and antidiagonal matrices with determinant 1. This case is similar to the previous case, except that now the u_i are in a quadratic extension E/F and are conjugate over F, since the $\mathbf{Z}/2$ must permute the lines invariant under the subgroup of G isomorphic to $\mathbf{G}_m$.

2.4 G extension of $\mathbf{G}_m$ by $\mathbf{G}_a$

In this case G is conjugate to the group of triangular matrices with determinant 1. In this case there is an unique invariant line under G in the solution space of $Ly = 0$, generated by y_1, say. As before, the logarithmic derivative $u_1 = Dy_1/y_1$ is in F and we get a relation $b_p u_1^2 + 2a_p u_1 - a_{p+1} = 0$ as well as $b_{p+1} = -a_p$.

2.5 $G \cong \mathbf{G}_a$

In this case G is conjugate to the group of triangular matrices with both diagonal entries equal to 1. In this case G acts trivially on the invariant line so there is a solution

of $Ly = 0$, say y_1, in F. As before, $u_1 = Dy_1/y_1$ is also in F and this gives a relation $b_p u_1^2 + 2a_p u_1 - a_{p+1} = 0$. But we do not get all relations among the entries of A_p this way. In order to get all relations we use that y_1 is in F to get $D^p y_1 = D^{p+1} y_1 = 0$. This gives two relations $a_p y_1 + b_p D y_1 = a_{p+1} y_1 + b_{p+1} D y_1 = 0$ and, again as before, we have $b_{p+1} = -a_p$.

As an application of the above, we expand an argument of van der Put [P] for the Airy equation (and correct a small error there) in order to reprove a theorem of Katz.

Theorem 1. *The equation $D^2 y = ay$, where a is a polynomial of odd degree, has Galois group SL_2.*

Proof: Suppose G is not SL_2. Notice that, from (*) above, we get in particular that the p-curvature is not zero so G is not finite. In all other cases, $Ly = 0$ has a solution for which $u = Dy/y$ is algebraic. So from the lemma we get the relation $b_p u^2 + 2a_p u - a_{p+1} = 0$, which is a quadratic equation for u. Again from (*), we get the top terms of the a_p, b_p, a_{p+1} and this gives that the discriminant of the quadratic for u, $4(a_p^2 + b_p a_{p+1})$ is a polynomial of degree kp, which is odd for p odd. Therefore the quadratic equation cannot have a rational function as root, since the discriminant is not a square. So the Galois group can only be conjugate to (2.4). To rule out (2.4), we proceed as in [P]. From [P] 4.1 (our b_p is f there), b_p satisfies a third order equation with polynomial coefficients $D^3 b_p - 4aDb_p - 2Dab_p = 0$. If the Galois group is assumed to be (2.4), u satisfies a quadratic equation over $K(x)$ and since it also satisfies $b_p u^2 + 2a_p u - a_{p+1} = 0$, we get that $2a_p/b_p = -Db_p/b_p$ is independent of p. However, b_p has degree $(p-1)/2$ (from (*))and, because of the differential equation it satisfies, b_p cannot have any triple zeros ([P] erroneously asserts the zeros are simple but gives counterexamples a paragraph earlier!). Thus $-Db_p/b_p$ has at least $[(p-1)/4]$ poles and thus cannot be independent of p. This contradiction completes the proof.

3. Globally nilpotent equations

As before we consider a second-order equation $Ly = 0$ with Galois group G contained in SL_2. We will assume that $Ly = 0$ is globally nilpotent, that is, its p-curvatures are

nilpotent for all sufficiently large p. Katz [K3] has shown that factors of the Gauss-Manin connection on the cohomology of families of algebraic varieties are globally nilpotent. In particular, the Gauss hypergeometric equation $x(x-1)D^2y+((a+b+1)x-c)Dy+aby=0$ is globally nilpotent, a result which is also proved directly in [M]. Dwork [D] conjectured that the only second-order equations over $K(x)$ which are globally nilpotent are obtained from Gauss hypergeometric equation by a change of variable or have a rational solution.

In this section we will compute the Galois group of some second order globally nilpotent equations using the p-curvatures. We note that, for the Gauss hypergeometric equation, our result follows from [BH]. Katz [K3] has shown that globally nilpotent equations have regular singular points and rational exponents. The p-curvature of the determinant of $Ly=0$ is the trace of the p-curvature of $Ly=0$ which is zero, by nilpotence. So the determinant of of $Ly=0$ has all its p-curvatures equal to zero, hence finite Galois group if the one-dimensional case of the Grothendieck conjecture holds. Thus, passing to a finite extension of F we may assume that G is a subgroup of SL_2.

As shown by Honda [H], the nilpotence of A_p implies that $Ly=0$ has a non-zero solution y_1 in the reduction of F modulo p. Then, as before, $u_1=Dy_1/y_1$ satisfies the quadratic equation $b_pu^2+2a_pu-a_{p+1}=0$, as does any other algebraic Dy/y with $Ly=0$, by the Lemma. However, the discriminant of the quadratic equation is $4(a_p^2+b_pa_{p+1})=-4\det A_p=0$, by the nilpotence of A_p. So this quadratic equation has only one solution if it is not identically zero, i.e. if $A_p\neq 0$. Hence the only possibilities, if $A_p\neq 0$, for the Galois group are SL_2,(2.4) and (2.5). In both cases (2.4) and (2.5), there a unique $u\in F$, of the form $Dy/y, Ly=0$. and so, from the above $u_1=u$.

Suppose that $Ly=0$ has m singularities and denote by $\rho_1',\rho_1'',\ldots,\rho_m',\rho_m''$ their respective exponents. We say that $Ly=0$ satisfies the *exponent restriction* if for all choices of ρ_i from $\rho_i',\rho_i'', i=1,\ldots,m$, we have that $\sum\rho_i$ is not a nonpositive integer. Suppose that $Ly=0$ satisfies this exponent restriction. Now, the valuation of y_1 is congruent modulo p to 0 or 1 at the regular points. Let k be the number of regular points where the valuation of y_1 is congruent to 1 modulo p. The valuation of y_1 is congruent modulo p

to either ρ_i' or ρ_i'' at the i-th singular point and therefore, by the residue theorem applied to dy_1/y_1, $\sum \rho_i + k$ is divisible by p. If $u_1 dx = dy_1/y_1$ has a bounded number of poles, then k is bounded and therefore $\sum \rho_i$ is congruent modulo p to a bounded nonpositive integer (viz. $-k$) for the choice of ρ_i corresponding to the valuations of y_1. From the exponent restriction and the fact that the ρ_i's are rational numbers, it follows that this cannot happen for infinitely many primes. Therefore u_1 cannot have a bounded number of poles and therefore cannot be congruent to some $u \in K(x)$ independently of p. From the above discussion this implies that the Galois group is SL_2. This argument proves the following theorem.

Theorem 2. *Let $Ly = 0$ be a globally nilpotent, second order differential equation whose p-curvatures do not vanish for all sufficiently large p and which satisfies the above exponent restriction. Then the differential Galois group of $Ly = 0$ is SL_2.*

Acknowledgements: The author would like to thank N. Katz for helpful comments and the NSA for financial support.

References.

[BH] F. Beukers and G. Heckman, *Monodromy for the hypergeometric function ${}_nF_{n-1}$*, Invent. math. 95 (1989) 325-354.

[D] B. Dwork, *Differential operators with nilpotent p-curvature*, Amer. J. Math. 112 (1990), 749–786.

[H] T. Honda, *Algebraic differential equations*, Symposia Math. XXIV (1979) 169-204.

[K1] N. Katz, *Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin*, Publ. Math. IHES 39, (1970), 175–232.

[K2] N. Katz, *Algebraic solutions of differential equations (p-curvature and the Hodge filtration)*, Invent. Math. 18 (1972), 1–118.

[K3] N. Katz, *A conjecture in the arithmetic of differential equations*, Bull. Soc. Math. France 110 (1982) 203-239. Corrections, ibid. 347-348.

[K4] N. Katz, *On the calculation of some differential galois groups*, Invent. math. 87 (1987) 13-61.

[P] M. van der Put, *Reduction modulo p of differential equations*, Indag. Math. 7 (1996) 367–387.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu