A note on p-curvatures

Julien Roques

Abstract. *In this note, we give an arithmetic criterion for the Lie-irreducibility of linear differential equations based on p-curvatures.*

Contents

1 Introduction - Statement of the main result

A. Grothendieck conjectured that a linear differential equation with coefficients in $\mathbb{Q}(x)$ has a full set of algebraic solutions if and only if its p-curvatures are zero for almost all prime p. This conjecture was reformulated by N. Katz in [1] (Grothendieck-Katz' conjecture).

In contrast with the original Grothendieck's conjecture, this note is concerned with the non vanishing of the p-curvatures. Our main result is :

Theorem 1. *Let L be a linear differential operator with coefficients in $\mathbb{Q}(x)$, irreducible over $\overline{\mathbb{Q}}(x)$. Assume that the order n of L is a prime and that, for infinitely many prime p, the reduction of L mod. p is nilpotent and has non zero p-curvature. Then L is Lie-irreducible.*

We recall that an operator L as above is Lie-irreducible if the neutral component of its differential Galois group over $\overline{\mathbb{Q}}(x)$ acts irreducibly (on the solutions).

This note is inspired by J. F. Voloch's paper [5] which is concerned with second order operators. Indeed, it is easily seen that, in the case that $n = 2$, Theorem 1 can be paraphrased as follows : *Let L be a linear differential operator of order 2 with coefficients in $\mathbb{Q}(x)$, irreducible over $\overline{\mathbb{Q}}(x)$. Assume that, for infinitely many prime p, the reduction of L mod. p is nilpotent and has non zero p-curvature. Then the Galois group of L over $\overline{\mathbb{Q}}(x)$ contains $SL_2(\overline{\mathbb{Q}})$.* This result is proved in [5]. The starting point of this work was a question raised by N. Katz in the introduction of [2]. It is interesting to note the similarity of Theorem 1 with N. Katz' Proposition 2.7.2 in [3].

Acknowledgments. Je remercie L. Di Vizio et D. Bertrand.

2 Differential equations, differential systems and p-curvatures

We will denote by $\mathbb{Q}(x)\langle\partial\rangle$ be the usual non commutative algebra of differential operators with coefficients in $\mathbb{Q}(x)$ (i.e. the non commutative algebra of non commutative polynomials with coefficients in $\mathbb{Q}(x)$ satisfying to the relation $\partial x = x\partial + 1$).

Let us consider $L = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0 \in \mathbb{Q}(x)\langle\partial\rangle$. The corresponding linear homogeneous differential equation is

$$\partial^n y + a_{n-1}\partial^{n-1} y + \cdots + a_0 y = 0. \tag{1}$$

Setting $Y = (y, \partial y, ..., \partial^{n-1} y)^t$, this differential equation is equivalent to the differential system

$$\partial Y = AY; \quad A = \begin{pmatrix} 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \\ -a_0 & -a_1 & \cdots & -a_{n-1} \end{pmatrix} \in M_n(\mathbb{Q}(x)). \tag{2}$$

We define a sequence $(A_k)_{k\in\mathbb{N}^*}$ of elements of $M_n(\mathbb{Q}(x))$ by $A_1 = A$ and, for all $k \in \mathbb{N}^*$, $A_{k+1} = \partial A_k + A_k A$ (in other terms, for all $k \in \mathbb{N}^*$, $\partial^k Y = A_k Y$). For all $k \in \mathbb{N}$, we will set :

$$A_k = (a_{k;i,j})_{1\leq i,j\leq n}.$$

For almost all prime p, we define the p-curvature of L as A_p mod. p. Note if the first line of the p-curvature is zero then the p-curvature itself is zero (immediate from the formula $\partial^p Y = A_p Y$).

3 Proof of Theorem 1

We start with some preliminary results.

Lemma 1. *Let L be an irreducible element of $\mathbb{Q}(x)\langle\partial\rangle$ of order $m \in \mathbb{N}$. Let y be a non zero element of some differential field extension of $(\mathbb{Q}(x), \partial)$ such that $Ly = 0$. Then $y, \partial y, \partial^2 y, ..., \partial^{m-1} y$ are linearly independent over $\mathbb{Q}(x)$.*

Proof. This lemma means that if $L' \in \mathbb{Q}(x)\langle\partial\rangle$ is a differential operator of order $< m$ such that $L'y = 0$ then $L' = 0$. This is a direct consequence of the fact that the left ideal $\{L' \in \mathbb{Q}(x)\langle\partial\rangle \mid L'y = 0\}$ of $\mathbb{Q}(x)\langle\partial\rangle$ is generated by L (by the usual Euclidean division argument). □

Lemma 2. *Let n be a prime. Let $G \subset GL_n(\overline{\mathbb{Q}})$ be a linear algebraic group which acts irreducibly on $\overline{\mathbb{Q}}^n$. Then either G^0 acts irreducibly on $\overline{\mathbb{Q}}^n$ or there exists a line in $\overline{\mathbb{Q}}^n$ invariant by the action of G^0.*

Proof. Assume that G^0 acts reducibly on $\overline{\mathbb{Q}}^n$. Let $V \neq \{0\}, \overline{\mathbb{Q}}^n$ be a non trivial subspace of $\overline{\mathbb{Q}}^n$ invariant for the action of G^0 and minimal for this property. For all $g \in G$, gV is invariant under the action of G^0 because G^0 is normalized by G. So, since G acts irreducibly on $\overline{\mathbb{Q}}^n$, $\overline{\mathbb{Q}}^n = \sum_{g\in G} gV$. Let E be a finite subset of G such that $\overline{\mathbb{Q}}^n = \sum_{g\in E} gV$ and minimal for this property. For any $h \in E$, $(\sum_{g\in E\setminus\{h\}} gV) \cap hV$ is an invariant subspace for G^0 so, by the minimality property of the (dimension of) V, either $(\sum_{g\in E\setminus\{h\}} gV)\cap hV=\{0\}$ or $(\sum_{g\in E\setminus\{h\}} gV)\cap hV=hV$. The case that $(\sum_{g\in E\setminus\{h\}} gV)\cap hV=hV$ is excluded by the minimality property of E. Therefore $\overline{\mathbb{Q}}^n=\bigoplus_{g\in E} gV$. In particular, since n is prime, we get $\dim V=1$. □

Notations. In what follows, we will use the Picard-Vessiot approach for differential Galois theory ([4]). For any $L\in\mathbb{Q}(x)\langle\partial\rangle$, we will denote by K_L some Picard-Vessiot extension for L over $\overline{\mathbb{Q}}(x)$ and by $S_L=\{y\in K_L \mid Ly=0\}$ the corresponding $\overline{\mathbb{Q}}$-vector space of solutions (whose dimension is the order of L).

Proposition 1. *Let n be a prime. Let L be an element of $\mathbb{Q}(x)\langle\partial\rangle$ of order n, irreducible over $\overline{\mathbb{Q}}(x)$. Then either L is Lie-irreducible or there exists $y\neq 0$ in S_L such that, for all $k\in\mathbb{N}$, $\frac{\partial^k y}{y}$ is algebraic over $\mathbb{Q}(x)$.*

Proof. Let $G\subset GL(S_L)$ be the differential Galois group of L over $\overline{\mathbb{Q}}(x)$. Since L is irreducible over $\overline{\mathbb{Q}}(x)$, G acts irreducibly on S_L. Assume that L is Lie-reducible. Lemma 2 ensures that there exists $y\in S_L$ which spans a $\overline{\mathbb{Q}}$-line invariant by the action of G^0; in particular, for any $k\in\mathbb{N}$, $g\frac{\partial^k y}{y}=\frac{\partial^k(gy)}{gy}$ does not depend on $g\in G^0$. So, we can set (without ambiguity), for any $\overline{g}\in G/G^0$, $\overline{g}\frac{\partial^k y}{y}=g\frac{\partial^k y}{y}$. It is clear that any symmetric polynomial with coefficients in $\overline{\mathbb{Q}}(x)$ in $(\overline{g}\frac{\partial^k y}{y}\mid \overline{g}\in G/G^0)$ is fixed by the action of G and hence belongs to $\overline{\mathbb{Q}}(x)$. Therefore, $\frac{\partial^k y}{y}$ is algebraic over $\overline{\mathbb{Q}}(x)$ of degree at most $[G:G^0]$. □

We now prove our main result.

Proof of Theorem 1. Assume that L is Lie-reducible. Proposition 1 ensures that there exists $y\neq 0$ in S_L such that, for all $k\in\mathbb{N}$, $\frac{\partial^k y}{y}$ is algebraic over $\mathbb{Q}(x)$. For the sake of conciseness, we set, for all $k\in\mathbb{N}$, $u_k=\frac{\partial^k y}{y}$ and $K=\mathbb{Q}(x)(u_1,...,u_{n-1})\subset K_L$. Then K is a finite differential extension of $\mathbb{Q}(x)$.

Let T be an indeterminate over $\mathbb{Q}(x)$ and let $F(T)=\sum_{k=0}^n f_k T^k$ be a unitary irreducible element of $\mathbb{Q}(x)[T]$ such that K can be identified with $\mathbb{Q}(x)[T]/(F(T))$; we denote by t the class of T in $\mathbb{Q}(x)[T]/(F(T))$. With this identification ∂ is given by $\partial t=-(\sum_{k=0}^n \partial(f_k)t^k)(\frac{d}{dT}F(t))^{-1}$.

Let $r\in\mathbb{Z}[x]$ be some multiple of denominators of the coefficients of $F(T)$ and of L such that the image R of $\mathbb{Z}[x][r^{-1}][T]$ in $K=\mathbb{Q}(x)[T]/(F(T))$ contains $(\frac{d}{dT}F(t))^{-1}$ and $u_1,...,u_{n-1}$. It is clear that R is a subring of K stable by ∂. Moreover, for all $k\in\mathbb{N}$, $u_k\in R$ as it is easily seen from the relation $Ly=0$.

In what follows by "mod. p" we will mean "in R/pR".

Let us consider $k\in[\![0,n-1]\!]$. Using Leibniz formula, we get $u_{p+k}=\frac{\partial^{p+k}y}{y}=\frac{\partial^p\partial^k y}{y}=\frac{\partial^p(u_k y)}{y}=\sum_{j=0}^p\binom{j}{p}\partial^j(u_k)u_{p-j}=u_k u_p+\partial^p u_k$ mod. p, for almost all prime p. But, since u_k is algebraic over $\mathbb{Q}(x)$, $\partial^p u_k=0$ mod. p, for almost all prime p. Thus, we are lead to the fact that, for almost all prime p, $u_{p+k}=u_k u_p$ mod. p i.e. $\frac{\partial^{p+k}y}{y}=u_k\frac{\partial^p y}{y}$ mod. p and hence $a_{p;k+1,1}+a_{p;k+1,2}u_1+\cdots+a_{p;k+1,n}u_{n-1}=u_k(a_{p;1,1}+a_{p;1,2}u_1+\cdots+a_{p;1,n}u_{n-1})$ mod. p (we use the notations of section 2 for the p-curvatures).

Therefore, for almost all prime p, the vector $(1,u_1,...,u_{n-1})^t$ mod. p is an eigenvector with coefficients in R/pR for the p-curvature A_p mod. p associated to the eigenvalue $a_{p;1,1}+$

$a_{p;1,2}u_1 + \cdots + a_{p;1,n}u_{n-1}$ mod. p. Since A_p mod. p is nilpotent and non zero for infinitely many prime p and since the first coordinate of the above eigenvector is equal to 1, we get that $a_{p;1,1} + a_{p;1,2}u_1 + \cdots + a_{p;1,n}u_{n-1}$ mod. p is a nilpotent element of R/pR for infinitely many prime p (the fact that the first coordinate is equal to 1 is used because R/pR need not be entire). Since R/pR is a reduced ring for almost all prime p, we get a non trivial linear relation $a_{p;1,1} + a_{p;1,2}u_1 + \cdots + a_{p;1,n}u_{n-1} = 0$ mod. p for infinitely many prime p in the $\mathbb{Z}[x][r^{-1}]/p\mathbb{Z}[x][r^{-1}]$-module R/pR..

So 1 mod. p, u_1 mod. p,..., u_{n-1} mod. p are linearly dependent in the $\mathbb{Z}[x][r^{-1}]/p\mathbb{Z}[x][r^{-1}]$-module R/pR, for infinitely many prime p. Using the fact that R is a free $\mathbb{Z}[x][r^{-1}]$-module of finite type, we get that $1, u_1, ..., u_{n-1}$ are linearly dependent over $\mathbb{Q}(x)$: this is a contradiction in virtue of Lemma 1. □

References

[1] N. M. Katz. A conjecture in the arithmetic theory of differential equations. *Bull. Soc. Math. France*, 110(2):203–239, 1982.

[2] N. M. Katz. On the calculation of some differential Galois groups. *Invent. Math.*, 87(1):13–61, 1987.

[3] N. M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 1990.

[4] M. Van der Put and M. F. Singer. *Galois Theory of Linear Differential Equations*, volume 328 of *Grundlehren der mathematischen Wissenschaften.* Springer-Verlag, Berlin, 2003.

[5] J. P. Voloch. A note on the arithmetic of differential equations. *Indag. Math.*, 11(4):617–621, 2000.

Julien Roques
Université Grenoble 1 - CNRS UMR 5582
Institut Fourier
100 rue des Maths
BP 74
38402 St Martin d'Hères cedex (France)
E-mail : Julien.Roques@ujf-grenoble.fr