The Grothendieck-Katz p-curvature conjecture: an introduction

Julien Roques[*]

October 14, 2024

Abstract

These are lecture notes from a mini-course given at the workshop Algebraicity and Transcendence for Singular Differential Equations held at the Erwin Schrödinger Institute in Vienna from October 7 to 19, 2024 about the Grothendieck-Katz p-curvature conjecture.

Contents

[*] Universite Claude Bernard Lyon 1, CNRS, Ecole Centrale de Lyon, INSA Lyon, Université Jean Monnet, ICJ UMR5208, 69622 Villeurbanne, France. Email: Julien.Roques@univ-lyon1.fr

2020 Mathematics Subject Classification:. Primary: 11-02; Secondary: 12H05, 33C20. 12H25, 34A20, 34A30, 34M15, 05A15, 68W30.

About this document

This text is based on the survey paper [14] written in collaboration with A. Bostan and X. Caruso. Some parts have been expanded or added, while others have been reduced or deleted to meet the objectives and the format of this mini-course. In particular, readers interested in the effective aspects, which are not covered in this text, are invited to consult *loc. cit.*. The solutions of the exercises included in the present document are given in the very last section.

1 Algebraicity and D-finiteness

Let's begin by introducing the main protagonists of these notes: algebraic functions and differentially finite functions.

Let F be a field extension of $\mathbb{Q}(x)$. We recall that $f \in F$ is *algebraic* over $\mathbb{Q}(x)$ (or, simply, *algebraic*) if f satisfies a polynomial equation

$$P(x, f) = 0 \tag{1}$$

for some $P(x, Y) \in \mathbb{Q}(x)[Y] \setminus \{0\}$. Otherwise, f is called *transcendental*. We recall that the set of algebraic elements of F is a subfield of F.

Remark 1.1. A typical case is $F = \mathbb{Q}((x))$. Actually, as far as we are concerned with algebraic extensions of $\mathbb{Q}(x)$, one can always assume that $F = \bigcup_{d \in \mathbb{Z}_{\geq 1}} \overline{\mathbb{Q}}((x^{1/d}))$ is the field of (formal) Puiseux series, as the latter field is an algebraically closed field extension of $\mathbb{Q}(x)$.

Let us now assume that F is not only a field extension but a differential field extension of $\mathbb{Q}(x)$, *i.e.*, that F is equipped with a derivation $F \to F$, $f \mapsto f'$ extending the usual derivation $\mathbb{Q}(x) \to \mathbb{Q}(x)$, $f \mapsto f'$. We say that $f \in F$ is *differentially finite* (in short, *D-finite*) if it satisfies a linear differential equation of some order $r \geq 1$, say

$$a_r f^{(r)} + a_{r-1} f^{(r-1)} + \cdots + a_1 f' + a_0 f = 0, \tag{2}$$

where the a_i belong to $\mathbb{Q}(x)$ with $a_r \neq 0$. The set of D-finite elements of F is a differential subring of F, *i.e.*, a subring of F invariant by the derivation $F \to F$, $f \mapsto f'$.

Remark 1.2. In connection with Remark 1.1, we emphasize that the general D-finite case cannot be reduced to the formal Puiseux series case. For example, $x^{\sqrt{2}}$ or $e^{1/x}$ are D-finite but are not Puiseux series.

Exercise 1 — Prove that $f(x) = \sum_{n \in \mathbb{Z}} f_n x^n \in \mathbb{Q}((x))$ is D-finite if and only if its sequence of coefficients $(f_n)_{n \in \mathbb{Z}}$ is P-recursive, *i.e.*, if and only there exist finitely many polynomials $p_0(X), \ldots, p_d(X) \in \mathbb{Q}[X]$ with $p_d(X) \neq 0$ such that, for all $n \in \mathbb{Z}$,

$$p_d(n) f_{n+d} + p_{d-1}(n) f_{n+d-1} + \cdots + p_0(n) f_n = 0.$$

It is a general fact and an old result, already known by Abel, that algebraicity implies D-finiteness. Precisely, if f satisfies an algebraic equation of the form (1) with P of degree $n \geq 1$ in Y, then f also satisfies a differential equation like (2) of order r bounded from above by n.

This follows easily from the following reasoning. By differentiating $P(x, f) = 0$ and by using the chain rule, we obtain the equality

$$P_X(x, f) + f' P_Y(x, f) = 0$$

where P_X (resp. P_Y) denotes the derivative of P with respect to its first (resp. second) variable. Therefore, if P is assumed to be a polynomial of minimal degree $n \geq 1$ in Y satisfied by f, then $P_Y(x, f)$ is nonzero and, hence, $f' = -P_X(x, f)/P_Y(x, f) \in \mathbb{Q}(x)(f)$. It follows easily that $\mathbb{Q}(x)(f)$ is a differential subfield of F. In particular, the successive derivatives $f, f', f'', \ldots$ of f belong to $\mathbb{Q}(x)(f)$. As $\mathbb{Q}(x)(f)$ is a $\mathbb{Q}(x)$-vector space of dimension $\leq n$, the successive derivatives $f, f', f'', \ldots$ are $\mathbb{Q}(x)$-linearly dependent and this concludes the proof.

The converse of Abel's result is completely false. Most D-finite functions are transcendental, already for solutions of differential equations of order $r = 1$; for instance, the exponential function, that satisfies $y' = y$, is transcendental.

Deciding D-finiteness or algebraicity is a classical and (most of the time) difficult question. In addition to its intrinsic interest, this question has concrete motivations. Here's an illustration in combinatorics.

Example 1.3 (Catalan numbers)**.** By definition, a *Dyck path* is a path drawn in the quarter plane $\mathbb{N}^2$ that starts at $(0, 0)$, consists of steps $\nearrow$ (directed by the vector $(1, 1)$) or $\searrow$ (directed by the vector $(1, -1)$) and finally ends on the x-axis (see Figure 1).

Let C_n be the number of Dyck paths ending at $(2n, 0)$; we say that such paths have semilength n. For instance $C_1 = 1$ since there is a single Dyck path ending at $(2, 0)$, namely $\nearrow$–$\searrow$, while $C_2 = 2$ since there are two Dyck paths ending at $(4, 0)$, namely $\nearrow$–$\nearrow$–$\searrow$–$\searrow$ and $\nearrow$–$\searrow$–$\nearrow$–$\searrow$. We use the convention that $C_0 = 1$. We notice that any Dyck path of semilength $n+1$ can be written uniquely as the concatenation of (1) a step $\nearrow$, (2) a Dyck path of semilength $k-1$ (translated by $(1, 1)$), (3) a step $\searrow$ and (4) a Dyck path of semilength $n-k$. It follows that the sequence $(C_n)_{n\geq 0}$ satisfies the following nonlinear recurrence relation:

$$C_n = \sum_{k=1}^{n} C_{k-1} C_{n-k}, \qquad \text{for all } n \geq 1.$$

If $y(x)$ denotes the generating function of the C_n's, *i.e.*, $y(x) = \sum_{n=0}^{\infty} C_n x^n$, the previous relation translates to the algebraic identity

$$y(x) = 1 + x \cdot y(x)^2 \tag{3}$$

(the summand 1 comes from the fact that $C_0 = 1$), *i.e.*,

$$P(x, y(x)) = 0$$

with $P(x, Y) = xY^2 - Y + 1$. Therefore $y(x)$ is algebraic and one can even solve equation (3) and get the closed formula $y(x) = \frac{1-\sqrt{1-4x}}{2x}$. From this, one get the formula $C_n = \frac{1}{n+1}\binom{2n}{n}$.

Let's continue as if we didn't have the previous formula for $y(x)$, but only the equation (3) and let us derive a linear differential equation satisfied by $y(x)$ using only the equation (3). Specializing the proof of Abel's result to the present case, we first differentiate (3) and we get $y'(x) = y(x)^2 + 2x\, y(x)\, y'(x)$. Therefore:

$$y'(x) = \frac{y(x)^2}{1 - 2x\, y(x)} = \frac{(2x-1)y(x) + 1}{x(1-4x)}$$

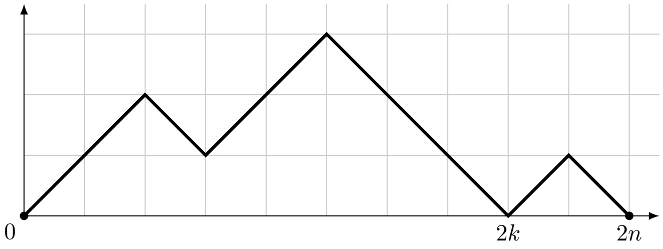

Figure 1: A Dyck path

(for the latter equality, we first compute an inverse of $1-2x\,y(x)$ in $\mathbb{Q}(x)(y(x))$ by computing a Bezout relation between $1-2xY$ and $P(x,Y)=xY^2-Y+1$). One obtains the inhomogeneous differential equation

$$(4x^2-x)y'(x)+(2x-1)y(x)+1=0.$$

From this, we can derive the simpler recurrence relation $C_n=\frac{4n-2}{n+1}\cdot C_{n-1}$ for all $n\geq 1$, from which we further derive the closed formula $C_n=\frac{1}{n+1}\binom{2n}{n}$. Using Stirling's formula, we also deduce the asymptotic estimate $C_n\sim 4^n/\sqrt{\pi n^3}$.

This example shows that being able to write down an equation (either algebraic or differential) for a generating series can help a lot in studying its coefficients (even if obtaining explicit closed formulas as we did for the Catalan numbers will not be possible in general). Besides, in many cases it turns out that the algebraicity of a generating series is the mirror of a (sometimes hidden) "algebraic" structure on the combinatorial side which often takes the form of a recursive tree structure: in the previous example, for instance, a Dyck path can be decomposed as a concatenation of smaller Dyck paths which themselves can be decomposed similarly, *etc.* We refer to [26] for a detailed discussion on this topic (including much more examples).

Let's restrict our attention to the differential field extension $F=\mathbb{Q}((x))$ of $\mathbb{Q}(x)$ (here, $\mathbb{Q}((x))$ is equipped with the usual derivation given by $(\sum_n a_n x^n)'=\sum_n a_n n x^{n-1}$). Here are some properties of the elements of $\mathbb{Q}((x))$ algebraic over $\mathbb{Q}(x)$; they do not characterize algebraicity but they may help to recognize transcendance.

Proposition 1.4. *Consider an algebraic $f(x)=\sum_{n\geq 0}a_n x^n\in\mathbb{Q}[[x]]\setminus\mathbb{Q}[x]$. Then $f(x)$ has a finite nonzero radius of convergence, can be analytically continued along any path in $\mathbb{C}\setminus$ {finitely many points} and admits a convergent Puiseux expansion at any point of $\mathbb{C}$.*

Remark 1.5. None of the properties listed in Proposition 1.4 is satisfied by all D-finite elements of $\mathbb{Q}[[x]]$, except the fact that any D-finite germ of analytic function can be analytically continued along all path avoiding the finitely many singularities of any differential equations it satisfies (we will come back to this later). Here are counter-examples:

- D-finite power series may be divergent; this is the case of

  $$f(x)=\sum_{k\geq 1}(-1)^{k-1}(k-1)!x^k$$

  that satisfies Euler's equation given by

  $$x^2y'(x)+y(x)=x.$$

- Non polynomial D-finite functions may be entire functions; this is the case of e^x.
- D-finite power series may not have a Puiseux series expansion at any point; this is the case of $\ln(1-x)$.

In particular, this shows that $f(x) = \sum_{k\geq 1}(-1)^{k-1}(k-1)!x^k$, e^x and $\ln(1-x)$ are transcendental.

Proposition 1.6 (Theorems A and D in [47]). *Consider an algebraic* $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]] \setminus \mathbb{Q}[x]$. *Then its coefficient sequence* $(a_n)_{n\geq 0}$ *is such that*

$$a_n = \frac{\beta^n n^r}{\Gamma(r+1)} \sum_{i=0}^{m} C_i \omega_i^n + O(\beta^n n^q), \tag{4}$$

where $m \in \mathbb{Z}_{\geq 0}$, $r \in \mathbb{Q} \setminus \mathbb{Z}_{<0}$, $q < r$, $\beta \in \overline{\mathbb{Q}}$, *and* $C_i, \omega_i \in \overline{\mathbb{Q}} \setminus \{0\}$ *with* $|\omega_i| = 1$.

This leads to the following useful transcendence criterion.

Corollary 1.7 ("Flajolet's criterion"). *If* $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]]$ *and* $a_n \sim \gamma\, \beta^n\, n^r$ *with either* $r \notin \mathbb{Q} \setminus \mathbb{Z}_{<0}$, *or* $\beta \notin \overline{\mathbb{Q}}$, *or* $\gamma \cdot \Gamma(r+1) \notin \overline{\mathbb{Q}}$, *then* $f(x)$ *is transcendental.*

Example 1.8. A very simple example of application is $\ln(1-x)$ because we have an asymptotic behavior as in Corollary 1.7 with $r = -1$.

In a more arithmetic vain, we have:

Proposition 1.9 (Eisenstein (1852)). *If* $f(x) = \sum_{k\geq 0} a_k x^k \in \mathbb{Q}[[x]]$ *is algebraic, then there exists* $N \in \mathbb{N} \setminus \{0\}$ *such that* $f(Nx) - f(0) \in \mathbb{Z}[[x]]$. *In particular, only a finite number of prime numbers can divide the denominators of the coefficients* a_k.

Remark 1.10. This property is not satisfied by all D-finite elements of $\mathbb{Q}[[x]]$; counter-examples include $\ln(1-x)$ and e^x.

Consider an algebraic $f(x) = \sum_{k\geq 0} a_k x^k \in \mathbb{Q}[[x]]$. According to Proposition 1.9, only finitely many primes are involved in the denominators of the coefficients of f. Therefore, one can consider the reduction $f_p \in \mathbb{F}_p((x))$ of f modulo almost all prime p. Of course, f_p is algebraic over $\mathbb{F}_p(x)$ for almost all prime p.

Is the converse true ? Precisely, consider an $f \in \mathbb{Q}[[x]]$ that can be reduced modulo p for almost all prime p (*i.e.*, such that only finitely many primes are involved in the denominators of the coefficients of f) and assume that, for almost all prime p, its reduction $f_p \in \mathbb{F}_p((x))$ is algebraic over $\mathbb{F}_p(x)$. Is it true that f is algebraic ? The answer is negative, even if we restrict our attention to D-finite power series. Indeed, we have already seen that the D-finite power series

$$f(x) = \sum_{k\geq 1} (-1)^{k-1}(k-1)!x^k$$

is transcendental but, for all prime p, its reduction is polynomial and, hence, algebraic.

Remark 1.11. You may object that this is not a good example because the sequence of coefficients $((-1)^{k-1}(k-1)!)_{k\geq 1}$ grow too fast. Exercise 2 gives another counter-example with a sequence of coefficients having moderate growth.

However, we will see that the converse is true for solutions of first order equations and that there is a lot to be said for equations of arbitrary order if instead of considering single D-finite series, we consider full bases of solutions. We will see this in details in the next section.

Exercise 2 — Throughout this exercise, $f(x)$ will denote the series

$$f(x) = \sum_{n=0}^{\infty} \binom{2n}{n}^t x^n \in \mathbb{Z}[[x]]$$

for $t \in \mathbb{Z}_{\geq 2}$. The aim of this exercise is to prove that $f(x)$ is transcendental. We follow the proof given in [82].

1. Consider a prime number p. Consider $n, m \in \mathbb{Z}_{\geq 0}$ and $i, j \in \{0, \ldots, p-1\}$. Prove Lucas' congruence:
$$\binom{np+i}{mp+j} \equiv \binom{n}{m}\binom{i}{j} \pmod{p}$$
2. Prove that, for any odd prime p, the reduction $f_p(x) \in \mathbb{F}_p[[x]]$ of $f(x)$ modulo p is algebraic over $\mathbb{F}_p(x)$ and satisfies
$$f_p(x) = \alpha_p f_p(x)^p$$
where $\alpha_p = \sum_{i=0}^{\frac{p-1}{2}} \binom{2i}{i}^t x^i \in \mathbb{F}_p[x]$.
3. Let $p > 2$ be a prime. We set
$$F(X) = X^{p-1} - \alpha_p \in \mathbb{F}_p(x)[X].$$
We let $F(X) = \prod_{i=1}^{k} P_i(X)$ be the irreducible factorization of $F(X)$ in $\mathbb{F}_p(x)[X]$. Let K be the splitting field of $F(X)$ over $\mathbb{F}_p(x)$ and set $r = [K : \mathbb{F}_p(x)]$.
   a) Prove that each $P_i(X)$ has degree r.
   b) Prove that f_p has degree r over $\mathbb{F}_p(x)$.
   c) Prove that $r \neq 1$.
   d) Prove that if $p > 3^{t-1}$ then $r \neq 2$.
   e) Prove that r divides $p-1$.
4. Prove that, for any $A > 0$, there exist infinitely many primes p such that whenever $m \in \mathbb{Z}_{\geq 1}$ divides $p-1$, then $m = 1, 2$ or $m > A$.
5. Conclude.

Exercise 3 — We recall that the Hadamard product of $f(x) = \sum_k f_k x^k \in \mathbb{Q}((x))$ and $g(x) = \sum_k g_k x^k \in \mathbb{Q}((x))$ is given by

$$f \odot g(x) = \sum_k f_k g_k x^k \in \mathbb{Q}((x)).$$

1. Use the result of Exercise 2 to prove that algebraicity is not necessarily preserved by Hadamard product.
2. Prove that D-finiteness is preserved by Hadamard product.

Exercise 4 — Prove that $\bigcup_{d\geq 1}\overline{\mathbb{F}_p}((x^{1/d}))$ is no algebraically closed.

Exercise 5 — (Dieudonné-Dwork Lemma.) Let $f(x)=\sum_{i\geq 0}a_ix^i\in 1+x\mathbb{Q}_p[[x]]$ be a formal power series.

1. The first objective of this exercise is to prove that the following properties are equivalent:

   (i) The coefficients a_i of $f(x)$ are in $\mathbb{Z}_p$.

   (ii) $f(x)^p/f(x^p)\in 1+px\mathbb{Z}_p[[x]]$.

   This result is called Dieudonné-Dwork Lemma. We follow the proof given in [77, p. 409].

   a) Prove (i) $\Rightarrow$ (ii).

   b) We will now prove (ii) $\Rightarrow$ (i). By assumption, we have

   $$f(x)^p=f(x^p)\left(1+p\sum_{j\geq 1}b_jx^j\right) \tag{5}$$

   for some $b_j\in\mathbb{Z}_p$. We will prove that the a_i belongs to $\mathbb{Z}_p$ by induction. We have $a_0=1\in\mathbb{Z}_p$. Consider $n\in\mathbb{Z}_{>0}$ and assume that, for all $i\in\{0,\ldots,n-1\}$, $a_i\in\mathbb{Z}_p$. Let us prove that $a_n\in\mathbb{Z}_p$.

   i – Prove that the coefficient of x^n in the left-hand side of (5) is of the form

   $$a_{n/p}^p+pa_n+\text{terms in }p\mathbb{Z}_p$$

   with $a_{n/p}=0$ when n is not divisible by p.

   ii – Prove that the coefficient of x^n in the right-hand side of (5) is of the form

   $$a_{n/p}+\text{terms in }p\mathbb{Z}_p.$$

   iii – Conclude.

2. Let $g(x)=\sum_{i\geq 1}a_ix^i\in x\mathbb{Q}_p[[x]]$ be a formal power series. One can prove that the following properties are equivalent :

   (i) The coefficients of $e^{g(x)}\in x1+x\mathbb{Q}_p[[x]]$ are in $\mathbb{Z}_p$.

   (ii) $g(x^p)-pg(x)\in p\mathbb{Z}_p[[x]]$.

   a) Prove the implication (ii)$\Rightarrow$(i) using Dieudonné-Dwork Lemma.

   b) Consider

   $$f(x)=\exp(\arctan(x))$$

   which is solution of the following first order differential equation:

   $$y'=\frac{1}{x^2+1}y.$$

   We set

   $$f(x)=\exp(\arctan(x))=\sum_{n=0}^{\infty}c_nx^n$$

   where the c_n's are rational numbers. Determine for which prime $p\neq 2$ (for simplicity) all the c_n are p-adic integers.

2 Grothendieck's conjecture

Grothendieck's conjecture relates the existence of a *full basis of algebraic solutions* of the differential equation (2) to the existence of a *full basis of rational solutions* of its reductions modulo almost all prime numbers p. We first examine in detail the case of first order equations in §2.1 and come to the general case in §2.2.

2.1 The case of equations of order 1: Honda's theorem

Consider a linear differential operator of order 1

$$\mathscr{L} = \partial_x + a(x) \tag{7}$$

with $a(x) \in \mathbb{Q}(x)$ and $\partial_x = d/dx$. It makes sense to consider the reduction $a(x) \bmod p \in \mathbb{F}_p(x)$ of (the coefficients of) $a(x)$ modulo p for almost all prime numbers p (for instance, $a(x) = \frac{1}{2(x-1)}$ can be reduced modulo p for all prime p but $p = 2$). Thus, one can consider the reduction

$$\mathscr{L}_p = \partial_x + a(x) \bmod p \tag{8}$$

of $\mathscr{L}$ modulo p for almost all primes p. This is a linear differential operator of order 1 with coefficients in $\mathbb{F}_p(x)$. Our aim is to relate the existence of a nonzero algebraic solution of (7) to the existence of nonzero rational solutions of the reduced equations (8).

In what follows, we say that an element f of a differential field extension of $\mathbb{Q}(x)$ (resp. $\mathbb{F}_p(x)$) is a solution of $\mathscr{L}$ (resp. of $\mathscr{L}_p$) when it is a solution of the corresponding differential equation, *i.e.*, when $\mathscr{L}(f) = f' + a(x)f = 0$ (resp. $\mathscr{L}_p(f) = f' + a(x)f = 0$).

2.1.1 Rational and algebraic solutions in characteristic 0: a criterion

What makes the case of first order equations tractable is the fact that there is a simple explicit criterion for the existence of a nonzero algebraic (or rational) solution.

Proposition 2.1. *The monic first order differential operator* (7) *has a nonzero rational (resp. algebraic) solution if and only if its constant coefficient $a(x)$ has at most a simple pole with integral (resp. rational) residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞.*

Proof. We first consider the "rational case". Let us first assume that $a(x)$ has at most a simple pole with integral residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞. We thus have

$$-a(x) = \sum_{i=1}^{m} \frac{n_i}{x - a_i} \tag{9}$$

for some $a_i \in \overline{\mathbb{Q}}$ and some $n_i \in \mathbb{Z}$. A straightforward calculation shows that

$$f(x) = \prod_{i=1}^{m} (x - a_i)^{n_i} \tag{10}$$

is a nonzero rational solution of (7).

Conversely, assume that (7) has a nonzero rational solution $f(x)$. This $f(x)$ can be factored as a product of linear factors $f(x) = c\prod_{i=1}^{m}(x-a_i)^{n_i}$ with $c \in \overline{\mathbb{Q}}^{\times}$, $a_i \in \overline{\mathbb{Q}}$ and $n_i \in \mathbb{Z}$. A straightforward calculation yields

$$-a(x) = \frac{f'(x)}{f(x)} = \sum_{i=1}^{m} \frac{n_i}{x-a_i}.$$

This shows that $a(x)$ has at most a simple pole with integral residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞, as expected.

We now consider the "algebraic case". Let us first assume that $a(x)$ has at most a simple pole with rational residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞. Then, we can argue as we did above in the rational case, the only differences being that the n_i involved in (9) are no longer in $\mathbb{Z}$ but in $\mathbb{Q}$ and that (10) is no longer rational but algebraic.

Conversely, assume that (7) has a nonzero algebraic solution $f(x)$. Let $M(Y) = Y^N + \sum_{i=0}^{N-1} m_i(x)Y^i \in \mathbb{Q}(x)[Y]$ be the minimal polynomial of $f(x)$ over $\mathbb{Q}(x)$. By differentiating the equality $M(f) = 0$ with respect to x and by using $f'(x) = -a(x)f(x)$, we get

$$\begin{aligned}0 = M(f)' = Nf^{N-1}f' + \sum_{i=0}^{N-1} m_i'(x)f^i + \sum_{i=0}^{N-1} m_i(x)if^{i-1}f' \\ = -Nf^{N-1}a(x)f + \sum_{i=0}^{N-1} m_i'(x)f^i - \sum_{i=0}^{N-1} m_i(x)if^{i-1}a(x)f \\ = -Na(x)f^N + \sum_{i=0}^{N-1}(m_i'(x) - m_i(x)ia(x))f^i.\end{aligned}$$

Hence, the polynomial $P(Y) = -Na(x)Y^N + \sum_{i=0}^{N-1}(m_i'(x) - m_i(x)ia(x))Y^i$ satisfies $P(f) = 0$. By minimality of $M(Y)$, we get $P(Y) = -Na(x)M(Y)$. Equating the constant terms in this equality, we get that $m_0(x)$ is a nonzero solution in $\mathbb{Q}(x)$ of $y'(x) = -Na(x)y(x)$. Using the "rational case" treated above, we get that $-Na(x)$ has at most a simple pole with integral residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞. Hence, $a(x)$ has at most a simple pole with rational residue at each point of $\overline{\mathbb{Q}}$ and vanishes at ∞, as expected. □

2.1.2 Algebraic solutions: from characteristic 0 to characteristic p

We shall now consider the following question: assuming that (7) has a nonzero algebraic solution, what can be said about the reduced equation (8)? It is natural to expect that the latter has a nonzero algebraic solution as well for almost all primes p. Actually, something even better happens. Let us consider an example.

Example 2.2. Consider the differential equation

$$y' = \frac{1}{2(x-1)}y. \tag{11}$$

It has a nonzero algebraic solution, namely $f(x) = (1-x)^{1/2}$. For any prime $p \neq 2$, one can consider the reduction of (11) modulo p. Any such reduced equation has a nonzero algebraic solution, namely $f_p(x) = (1-x)^{1/2}$. Let us clarify our notations: $f_p(x)$ is a root of the polynomial $Y^2 - (1-x) \in \mathbb{F}_p(x)[Y]$, whereas $f(x)$ is a root of the polynomial $Y^2 - (1-x) \in \mathbb{Q}(x)[Y]$. However, the reduction of (11) modulo p can also be written as $y' = \frac{n_p}{x-1}y$ where $n_p \in \mathbb{Z}$ is such that $n_p \equiv \frac{1}{2} \bmod p$ and, hence $\widetilde{f_p}(x) = (1-x)^{n_p}$ is a nonzero solution of the reduction modulo p of (11). The interesting point is that $\widetilde{f_p}(x)$ is not only algebraic but rational, contrary to $f_p(x)$!

This phenomenon does not happen in characteristic 0: (11) has an algebraic solution $f(x) = (1-x)^{1/2} \in \overline{\mathbb{Q}}((x))$ but no nonzero rational solution because any other solution $g(x) \in \overline{\mathbb{Q}}((x))$ is of the form $g(x) = \lambda f(x)$ for some $\lambda \in \overline{\mathbb{Q}}$. Why is there such a difference difference between zero and positive characteristic? In characteristic p, the reduction modulo p of (11) has an algebraic solution $f_p(x) = (1-x)^{1/2} \in \mathbb{F}_p((x))$ and any other solution $g_p(x) \in \mathbb{F}_p((x))$ is of the form $g_p(x) = \lambda f_p(x)$. So far, everything is quite similar to the characteristic zero case, but there is an important difference: λ is not necessarily in $\mathbb{F}_p$, it rather belongs to a much bigger field, namely to the field of constants of the differential field $\mathbb{F}_p((x))$ given by

$$\{u(x) \in \mathbb{F}_p((x)) \mid u'(x) = 0\} = \mathbb{F}_p((x^p)).$$

The phenomenon observed in Example 2.2 is a general fact as shown by Theorem 2.4 below. Let us first give an analogue in positive characteristic of the “rational case” of Proposition 2.1.

Proposition 2.3. *Consider $b(x) \in \mathbb{F}_p(x)$. The differential equation*

$$y' + b(x)y = 0$$

has a nonzero rational solution if and only if $b(x)$ has at most a simple pole with residue in $\mathbb{F}_p$ at each point of $\overline{\mathbb{F}_p}$ and vanishes at ∞.

Proof. The proof is entirely similar to the proof of the rational case of Proposition 2.1, it is sufficient to replace everywhere $\overline{\mathbb{Q}}$ by $\overline{\mathbb{F}_p}$ and $\mathbb{Z}$ by $\mathbb{F}_p$. □

Exercise 6 — Consider the differential equation

$$y' = \frac{1}{x^2+1}y \tag{12}$$

whose general solution in characteristic zero is $c \cdot \exp(\arctan(x))$ where c is a constant. We are interested in determining whether or not this equation has a rational solution in characteristic $p > 0$. Proposition 2.3 ensures that, for all $b(x) \in \mathbb{F}_p(x)$, the differential equation $y' + b(x)y = 0$ has a nonzero rational solution if and only if $b(x)$ has at most a simple pole with residue in $\mathbb{F}_p$ at each point of $\overline{\mathbb{F}_p}$ and vanishes at ∞. Using this result, prove the following:

1. The reduction modulo $p = 2$ of equation (12) has no nonzero rational solution.
2. The reduction modulo $p > 2$ of equation (12) has a nonzero rational solution if and only if $p \equiv 1 \pmod 4$.

Theorem 2.4. *If (7) has a nonzero algebraic solution, then, for almost all primes p, (8) has a nonzero rational solution.*

Proof. Proposition 2.1 (and its proof) ensures that

$$a(x) = \sum_{i=1}^{m} \frac{e_i}{x - a_i} \tag{13}$$

for some $a_i \in \overline{\mathbb{Q}}$ and some $e_i \in \mathbb{Q}$.

Let us first assume that the a_i's belong to $\mathbb{Q}$. For any prime p, we let $\mathbb{Z}_{(p)}$ be the ring of rational numbers with denominator relatively prime to p. We denote by $\pi_p : \mathbb{Z}_{(p)} \to \mathbb{F}_p$ the "reduction modulo p" map. For almost all primes p, the a_i's and the e_i's belong to $\mathbb{Z}_{(p)}$. For any such p, we have:

$$a(x) \bmod p = \sum_{i=1}^{m} \frac{\pi_p(e_i)}{x - \pi_p(a_i)}$$

and the result follows from Proposition 2.3.

The proof in the general case is similar but requires basic notions from algebraic number theory. Let K be a number field containing the a_i and the e_i. Let $\mathcal{O}_K$ be the ring of integers of K. For any prime $\mathfrak{P}$ of K (which is by definition a prime ideal of $\mathcal{O}_K$), we let $\mathcal{O}_{K,\mathfrak{P}}$ be the valuation ring of K at $\mathfrak{P}$ (this is the localization of $\mathcal{O}_K$ at $\mathfrak{P}$). We denote by $\kappa_{\mathfrak{P}} = \mathcal{O}_{K,\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{K,\mathfrak{P}}$ the corresponding residue field and by $\pi_{\mathfrak{P}} : \mathcal{O}_{K,\mathfrak{P}} \to \kappa_{\mathfrak{P}}$ the quotient map. The residue field $\kappa_{\mathfrak{P}}$ is a finite field of characteristic p such that $\mathfrak{P} \cap \mathbb{Z} = (p)$. We say that $\mathfrak{P}$ is above p. For almost all primes p, for all primes $\mathfrak{P}$ of K above p (there is always at least one and they are finitely many), the a_i's and the e_i's belong to $\mathcal{O}_{K,\mathfrak{P}}$. For such p and $\mathfrak{P}$, we have:

$$a(x) \bmod p = a(x) \bmod \mathfrak{P} = \sum_{i=1}^{m} \frac{\pi_{\mathfrak{P}}(e_i)}{x - \pi_{\mathfrak{P}}(a_i)}.$$

Since e_i is rational, $\pi_{\mathfrak{P}}(e_i)$ belongs to the prime subfield $\mathbb{F}_p$ of $\kappa_{\mathfrak{P}}$. The result follows from Proposition 2.3. □

2.1.3 From characteristic p to characteristic 0

It is now tempting to ask: if (8) has a nonzero rational solution for almost all primes p, does (7) have a nonzero algebraic solution? The (positive) answer is given by the following result.

Theorem 2.5 (Honda [54]). *The converse of Theorem 2.4 holds true, i.e., if, for almost all primes p, (8) has a nonzero rational solution, then (7) has a nonzero algebraic solution.*

Proof. Consider the partial fraction decomposition of $a(x)$:

$$a(x) = P(x) + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\alpha_{i,j}}{(x - a_i)^j}$$

with $P(x) \in \overline{\mathbb{Q}}[x]$, $a_i \in \overline{\mathbb{Q}}$, $\alpha_{i,j} \in \overline{\mathbb{Q}}$ and $r_j \in \mathbb{Z}_{\geq 1}$. According to Proposition 2.1, we have to prove that $P(x)$ and the $\alpha_{i,j}$'s for $j \geq 2$ are 0 and that the $\alpha_{i,1}$'s belong to $\mathbb{Q}$.

Let K be a number field containing the a_i, the $\alpha_{i,j}$'s and the coefficients of $P(x)$. We will use the notation and terminology (prime $\mathfrak{P}$ of K, valuation ring $\mathcal{O}_{K,\mathfrak{P}}$, quotient map $\pi_{\mathfrak{P}}$, *etc.*)

introduced in the proof of Theorem 2.4. For almost all primes p, for all primes $\mathfrak{P}$ of K above p, the a_i's, the $\alpha_{i,j}$'s and the coefficients of $P(x)$ belong to $\mathcal{O}_{K,\mathfrak{P}}$. For such p and $\mathfrak{P}$, we have:

$$a(x) \bmod p = a(x) \bmod \mathfrak{P} = P^{\pi_{\mathfrak{P}}}(x) + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\pi_{\mathfrak{P}}(\alpha_{i,j})}{(x - \pi_{\mathfrak{P}}(a_i))^j},$$

where $P^{\pi_{\mathfrak{P}}}(x)$ denotes the polynomial obtained from $P(x)$ by applying $\pi_{\mathfrak{P}}$ coefficientwise.

Proposition 2.3 ensures that, for almost all primes p, $a(x) \bmod p$ has at most simple poles, so, for almost all primes p, for all primes $\mathfrak{P}$ of K above p, for all $j \in \{2, \ldots, r_i\}$, we have $\pi_{\mathfrak{P}}(\alpha_{i,j}) = 0$, *i.e.*, $\alpha_{i,j} \in \mathfrak{P}$. This implies that, for all $j \in \{2, \ldots, r_i\}$, we have $\alpha_{i,j} = 0$. Similarly, Proposition 2.3 also ensures that, for almost all primes p, $a(x) \bmod p$ vanishes at ∞, so, for almost all primes p, for all primes $\mathfrak{P}$ of K above p, $P^{\pi_{\mathfrak{P}}}(x) = 0$. This implies that $P(x) = 0$. Last, Proposition 2.3 ensures that, for almost all primes p, for all primes $\mathfrak{P}$ above p, we have $\pi_{\mathfrak{P}}(\alpha_{i,1}) \in \mathbb{F}_p$. Using Kronecker's Theorem recalled below, we get that $\alpha_{i,1}$ belongs to $\mathbb{Q}$ and Proposition 2.1 yields the desired result: (7) has a nonzero algebraic solution. □

The Kronecker Theorem mentioned above (which is usually seen as a consequence of Chebotarev's density Theorem) reads as follows

Theorem 2.6 (Kronecker). *An irreducible element $P(x)$ of $\mathbb{Q}[x]$ such that, for almost all primes p, $P(x) \bmod p$ has a zero in $\mathbb{F}_p$ is linear.*

2.1.4 Rational solutions in characteristic p and p-curvature

Consider a differential equation

$$y' + b(x)y = 0 \tag{14}$$

with $b(x) \in \mathbb{F}_p(x)$. We will give an alternative criterion (an alternative to Proposition 2.3) for determining whether (14) has a nonzero rational solution based on the notion of p-curvature that we shall now introduce.

Consider the map

$$\begin{array}{rcl} \Delta : \mathbb{F}_p(x) & \rightarrow & \mathbb{F}_p(x) \\ f & \mapsto & f' + b(x)f. \end{array}$$

It is $\mathbb{F}_p(x^p)$-linear and satisfies

$$\forall f, g \in \mathbb{F}_p(x), \Delta(fg) = f'g + f\Delta(g). \tag{15}$$

The homogeneity follows from the fact that the elements of $\mathbb{F}_p(x^p)$ are constants of the differential field $\mathbb{F}_p(x)$ in the sense that their derivative is 0 (see Exercise 7 below) implying that $\Delta(\alpha g) = \alpha' g + \alpha\Delta(g) = \alpha\Delta(g)$ for all $\alpha \in \mathbb{F}_p(x^p)$ and $f \in \mathbb{F}_p(x)$.

Exercise 7 — Prove that the field of constants of the differential field $\mathbb{F}_p(x)$ is $\mathbb{F}_p(x^p)$, *i.e.*,

$$\mathbb{F}_p(x^p) = \{f(x) \in \mathbb{F}_p(x) \mid f'(x) = 0\}.$$

Definition 2.7. The map

$$\Delta^p : \mathbb{F}_p(x) \to \mathbb{F}_p(x)$$

is called the p-curvature of (14).

A remarkable and fundamental fact is:

Proposition 2.8. *The p-curvature is not only $\mathbb{F}_p(x^p)$-linear but it is also $\mathbb{F}_p(x)$-linear.*

Proof. Indeed, a simple induction along with (15) show that, for all $k \geq 0$, for all $\alpha, f \in \mathbb{F}_p(x)$, we have

$$\Delta^k(\alpha f) = \sum_{i=0}^{k} \binom{k}{i} \alpha^{(i)} \Delta^{k-i}(f).$$

Taking $k = p$ and using the fact that $\binom{p}{i} \equiv 0 \bmod p$ for all $1 < i < p$, we get

$$\Delta^p(\alpha f) = \alpha^{(p)} + \alpha \Delta^p(f),$$

and the $\mathbb{F}_p(x)$-homogeneity follows from the fact that $\alpha^{(p)} = 0$. □

As it is $\mathbb{F}_p(x)$-linear, the p-curvature is entirely determined by its value at 1:

$$\forall f \in \mathbb{F}_p(x),\ \Delta^p(f) = \Delta^p(1) f.$$

For this reason, we often say that the p-curvature of (14) is $\Delta^p(1) \in \mathbb{F}_p(x)$.

Note that we actually have

$$\Delta^p(1) \in \mathbb{F}_p(x^p).$$

Indeed, we have, for all $f \in \mathbb{F}_p(x)$,

$$\Delta(\Delta^p(f)) = \Delta(\Delta^p(1) f).$$

But, on the one hand,

$$\Delta(\Delta^p(f)) = \Delta^p(\Delta(f)) = \Delta^p(1)\Delta(f)$$

and, on the other hand, by (15),

$$\Delta(\Delta^p(1) f) = \Delta^p(1)' f + \Delta^p(1)\Delta(f).$$

Therefore, $\Delta^p(1)' = 0$, so $\Delta(1) \in \mathbb{F}_p(x^p)$.

Remark 2.9. The above properties of the p-curvature can also be seen as a consequence of the fact that $(\partial_x + b(x))^p$ is a central element in $\mathbb{F}_p(x)\langle \partial_x \rangle$. Indeed, a simple induction along with the identity $(\partial_x + b(x)) f = f' + f(\partial_x + b(x))$ shows that, for all $f \in \mathbb{F}_p(x)$,

$$(\partial_x + b(x))^p f = \sum_{i=0}^{p} \binom{p}{i} f^{(i)} (\partial_x + b(x))^{p-i} = f(\partial_x + b(x))^p,$$

so $(\partial_x + b(x))^p$ and f commute. Moreover, the equality $\partial_x = (\partial_x + b(x)) - b(x)$ and the fact that $(\partial_x + b(x))$ and $b(x)$ commute with $(\partial_x + b(x))^p$ imply that ∂_x commute with $(\partial_x + b(x))^p$

as well. This proves our claim that $(\partial_x + b(x))^p$ is a central element in $\mathbb{F}_p(x)\langle\partial_x\rangle$. Now, we have

$$\big(\partial_x + b(x)\big)^p = \partial_x^p + \star\partial_x^{p-1} + \cdots + \star\partial_x + b_p(x) \tag{16}$$

where $\star$ are some unspecified elements of $\mathbb{F}_p(x)$ and Exercise 8 below ensures that all terms in ∂_x^i with $1 \le i < p$ have to vanish, and that $b_p(x)$ belongs to $\mathbb{F}_p(x^p)$. In conclusion, we have the relation

$$\big(\partial_x + b(x)\big)^p = \partial_x^p + b_p(x). \tag{17}$$

This implies that

$$\begin{array}{rcl} \Delta^p : \mathbb{F}_p(x) & \to & \mathbb{F}_p(x) \\ f & \mapsto & \Delta^p(f) = f^{(p)} + b_p(x) f \end{array}$$

is $\mathbb{F}_p(x)$-linear and that $\Delta^p(1) = b_p(x)$ belongs to $\mathbb{F}_p(x^p)$.

Formula (17) also shows the following:

Proposition 2.10. *The p-curvature $\Delta^p(1) = b_p(x)$ is the opposite of the remainder in the right Euclidean division of ∂_x^p by $\mathscr{L} = \partial_x + b(x)$.*

In particular, the p-curvature vanishes if and only if $\mathscr{L}$ divides ∂_x^p in $\mathbb{F}_p(x)\langle\partial_x\rangle$.

Exercise 8 — Prove that the center Z of $\mathbb{F}_p(x)\langle\partial_x\rangle$ is equal to $\mathbb{F}_p(x^p)\langle\partial_x^p\rangle$ (to be compared to the center $\mathbb{Q}$ of $\mathbb{Q}(x)\langle\partial_x\rangle$).

Proposition 2.11. *The differential equation* (14) *has a nonzero rational solution if and only if $\Delta^p = 0$.*

Proof. If (14) has a nonzero rational solution f, then $\Delta(f) = 0$ and, hence, $\Delta^p(f) = 0$. As Δ^p is $\mathbb{F}_p(x)$-linear, we get $\Delta^p = 0$. Conversely, if $\Delta^p = 0$, then Δ has a nonzero kernel and, hence, (14) has a nonzero rational solution. □

We conclude this section by giving inductive and closed formulae for the p-curvature.

For all $k \ge 0$, we denote by $b_k(x) \in \mathbb{F}_p(x)$ the constant term of the differential operator $\big(\partial_x + b(x)\big)^k$, so that

$$\big(\partial_x + b(x)\big)^k = \partial_x^k + \star\partial_x^{k-1} + \cdots + \star\partial_x + b_k(x), \tag{18}$$

where $\star$ are some unspecified elements of $\mathbb{F}_p(x)$. Equating the terms of degree 0 (with respect to ∂_x) in the equality $(\partial_x + b(x))^{k+1} = (\partial_x + b(x)) \cdot (\partial_x + b(x))^k$, we get the following inductive formula for computing the $b_k(x)$'s:

$$\forall k \ge 0,\ \ b_{k+1}(x) = b_k'(x) + b(x) b_k(x). \tag{19}$$

This gives the desired inductive formula for the p-curvature of (14) since

$$\Delta^p(1) = b_p(x).$$

Last, one can deduce from (19) the following remarkable closed formula (that does not extend to higher order equations).

Theorem 2.12. *We have $b_p(x) = b^{(p-1)}(x) + b(x)^p$.*

Proof. This proof is due to Jacobson [56]. For another proof, due to Van der Put, see Exercise 9 below. For a positive integer k, let I_k be the set of all tuples $\underline{\alpha} = (\alpha_1, \ldots, \alpha_k)$ of nonnegative integers such that $\sum_{i=1}^k i\alpha_i = k$. A calculation shows that $b_k(x)$ is explicitly given by

$$b_k(x) = \sum_{\underline{\alpha} \in I_k} \lambda_{\underline{\alpha}} \cdot b(x)^{\alpha_1} \cdot b^{(1)}(x)^{\alpha_2} \cdots b^{(k-1)}(x)^{\alpha_k},$$

where $\lambda_{\underline{\alpha}}$ is a coefficient in $\mathbb{Z}$ determined by the following rule

$$\lambda_{\underline{\alpha}} = \sum_{i=1}^{k} (\alpha_{i-1} + 1) \cdot \lambda_{\tau_i(\underline{\alpha})} \qquad \text{(for } \underline{\alpha} \in I_k\text{)},$$

where τ_i denotes the function from I_k to I_{k-1} defined by

$$\tau_i(\underline{\alpha}) = (\alpha_1,\ \ldots,\ \alpha_{i-2},\ \alpha_{i-1}{-}1,\ \alpha_i{+}1,\ \alpha_{i+1},\ \ldots,\ \alpha_{k-1})$$

and where we agree that $\lambda_{\underline{\beta}} = 0$ if $\underline{\beta}$ has one negative coordinate. From this relation, one can check by induction on k that $\lambda_{\underline{\alpha}}$ (with $\underline{\alpha} = (\alpha_1, \ldots, \alpha_k) \in I_k$) is given by the closed formula:

$$\lambda_{\underline{\alpha}} = \frac{k!}{(\alpha_1)! \cdots (\alpha_k)! \cdot (2!)^{\alpha_2} \cdot (3!)^{\alpha_3} \cdots (k!)^{\alpha_k}}.$$

In particular, when $k = p$, we find that the $\lambda_{\underline{\alpha}}$'s vanish modulo p for all $\underline{\alpha} \in I_p$ (thanks to the numerator $p!$) except when $\underline{\alpha} = (p, 0, \ldots, 0)$ or $\underline{\alpha} = (0, \ldots, 0, 1)$ (because, in those cases, the numerator cancels with a factor $p!$ in the denominator). Besides, in both cases, one finds $\lambda_{\underline{\alpha}} = 1$. This concludes the proof. □

Remark 2.13. If (14) has p-curvature 0, then an explicit rational solution is given by

$$u_0(x) = \sum_{k=0}^{p-1} (-1)^k \frac{x^k}{k!} b_k(x) = \sum_{k=0}^{p-1} (-1)^k \frac{x^k}{k!} \Delta^k(1). \tag{20}$$

Indeed, using (15), we get, for all $k \in \{1, \ldots, p-1\}$,

$$\Delta\left(\frac{x^k}{k!}\Delta^k(1)\right) = \left(\frac{x^k}{k!}\right)' \Delta^k(1) + \frac{x^k}{k!}\Delta\left(\Delta^k(1)\right) = \frac{x^{k-1}}{(k-1)!}\Delta^k(1) + \frac{x^k}{k!}\Delta^{k+1}(1)$$

and, hence,

$$\begin{aligned}\Delta(u_0(x)) = \Delta\left(\sum_{k=0}^{p-1}(-1)^k \frac{x^k}{k!}\Delta^k(1)\right) &= \Delta(1) + \sum_{k=1}^{p-1}(-1)^k\left(\frac{x^{k-1}}{(k-1)!}\Delta^k(1) + \frac{x^k}{k!}\Delta^{k+1}(1)\right) \\ &= (-1)^{p-1}\frac{x^{p-1}}{(p-1)!}\Delta^p(1).\end{aligned}$$

It follows that (20) is a solution of (14) if and only if the latter equation has p-curvature 0, whence our claim. Note that, according to Wilson theorem,

$$(-1)^{p-1}\frac{x^{p-1}}{(p-1)!}\Delta^p(1) = -(-1)^{p-1}x^{p-1}\Delta^p(1)$$

but this will not be used.

But, be careful, (20) may be 0. Indeed, if $b = x^{-1}$ then $\Delta(1) = 1' + x^{-1}1 = x^{-1}$, $\Delta^2(x^{-1}) = -x^{-2} + x^{-1}x^{-1} = 0$ and, hence, for all $k \in \mathbb{Z}_{\geq 2}$, $\Delta^k(1) = 0$. It follows that $u_0(x) = 1 - x\Delta(1) = 0$.

However, if $b(x)$ has no pole at 0, then $u_0(x)$ has no pole at 0 as well and we have $u_0(0) = 1$. So $u_0(x)$ is nonzero rational solution of $y' + b(x)y = 0$.

Note that, more generally, if $a \in \mathbb{F}_p$ is not a pole of $b(x)$, then

$$u_a(x) = \sum_{k=0}^{p-1} (-1)^k \frac{(x-a)^k}{k!} b_k(x)$$

is a nonzero rational solutions of $y' + b(x)y = 0$.

Exercise 9 — In this exercise, we give a second proof of the formula $b_p(x) = b^{(p-1)}(x) + b(x)^p$ for the p-curvature of the rank 1 equation $y' + b(x)y = 0$ with $b(x) \in \mathbb{F}_p(x)$ after M. van der Put in [87].

1. Prove that, for any $b_1(x), b_2(x) \in \mathbb{F}_p(x)$, the p-curvature of $y' + (b_1(x) + b_2(x))y = 0$ is equal to the sum of the p-curvatures of $y' + b_1(x)y = 0$ and $y' + b_2(x)y = 0$.
2. Explain why it is sufficient to prove the desired formula for the p-curvature in the case $b = cx^i$ with $c \in \mathbb{F}_p(x^p)$ and $i \in \{0, \dots, p-1\}$.
3. Prove that the map that associates to an element c of $\mathbb{F}_p(x^p)$ the p-curvature (seen as an element of $\mathbb{F}_p(x^p)$) of $y' + cx^i$ is of the form

   $$c \mapsto c^p x^{ip} + c^{p-1} e_{p-1} + \cdots + c e_1$$

   where the e_j are elements of $\mathbb{F}_p(x)$ not depending on c.
4. Prove that $e_{p-1} = \cdots = e_2 = 0$ and give an explicit expression for e_1.
5. Conclude.

Exercise 10 — Give a second proof of Proposition 2.3 stating that, for all $b(x) \in \mathbb{F}_p(x)$, the differential equation $y' + b(x)y = 0$ has a nonzero rational solution if and only if $b(x)$ has at most a simple pole with residue in $\mathbb{F}_p$ at each point of $\overline{\mathbb{F}_p}$ and vanishes at ∞ using the explicit formula $b_p(x) = b^{(p-1)}(x) + b(x)^p$ for the p-curvature of $y' + b(x)y = 0$ given by Theorem 2.12.

Remark 2.14. There is a link between the p-curvature of first-order linear differential operators and a fairly famous algorithm for factoring polynomials in $\mathbb{F}_p[x]$, designed by Niederreiter in [70]. This connection seems to have been unnoticed until now. To factor a separable polynomial $f = \prod_i g_i$ of $\mathbb{F}_p[x]$, with irreducible g_i, Niederreiter considers the space of rational functions $y = h/f$ solutions of the equation $y^{(p-1)} + y^p = 0$, and shows that as a vector space over $\mathbb{F}_p$ it is generated by the logarithmic derivatives g_i'/g_i. As a result, factoring boils down to a linear algebra problem over $\mathbb{F}_p$. This algorithm created a lot of excitement as a promising alternative to the much more classical one due to Berlekamp [7].

Putting together Theorem 2.4, Theorem 2.5, Proposition 2.11 and Remark 2.9, we obtain the following result.

Theorem 2.15. *Let $\mathscr{L} = \partial_x + a(x)$ as in equation (7) and, for almost all prime numbers p, denote by $\mathscr{L}_p$ its reduction modulo p as in equation (8). The following properties are equivalent:*

(1) $\mathscr{L}$ has a nonzero algebraic solution;

(2) for almost all primes p, $\mathscr{L}_p$ has a nonzero rational solution;

(3) for almost all primes p, the p-curvature of $\mathscr{L}_p$ vanishes;

(4) for almost all primes p, the operator $\mathscr{L}_p$ divides ∂_x^p in $\mathbb{F}_p(x)\langle\partial_x\rangle$.

Grothendieck's p-curvature conjecture is a far reaching conjectural generalization of these equivalences for higher order equations.

2.2 The general case

Let us now consider a linear differential operator of arbitrary order:

$$\mathscr{L} = \partial_x^n + a_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + a_1(x)\cdot\partial_x + a_0(x) \tag{22}$$

with $a_i(x) \in \mathbb{Q}(x)$. As in the order-1 case, one can consider the reduction $\mathscr{L}_p$ of $\mathscr{L}$ modulo p for almost all primes p. This is a differential operator of order n with coefficients in $\mathbb{F}_p(x)$. Grothendieck's conjecture relates the algebraicity of the solutions of $\mathscr{L}$ to the rationality of the solutions of $\mathscr{L}_p$ for almost all primes p.

In view of the case of order one equations studied above, it is tempting to expect that a solution of a linear differential equation is algebraic if and only if almost all its reductions modulo p are algebraic. We have already seen at the end of Section 1 that this expectation is completely false. We can also ask the following question: if for almost all prime p, $\mathscr{L}_p$ admits a non-zero algebraic (or rational) solution, does $\mathscr{L}$ necessarily admit an algebraic solution? The answer is again negative, as the following example shows.

Example 2.16. Consider the inhomogeneous differential equation of order 1, called Euler equation, given by

$$x^2y'(x) + y(x) = x. \tag{23}$$

Note that a formal power series $f(x) = \sum_{k\geq 0} a_kx^k$ satisfies the latter equation if and only if

$$\sum_{k\geq 0} ka_kx^{k+1} + \sum_{k\geq 0} a_kx^k = x$$

if and only if $a_0 = 0$, $a_1 = 1$ and, for all $k \geq 0$, $a_k = -(k-1)a_{k-1}$. Therefore, (23) has a unique formal power series solution given by

$$f(x) = \sum_{k\geq 1}(-1)^{k-1}(k-1)!x^k.$$

The reduction $f_p(x)$ of $f(x)$ modulo any prime p is polynomial but $f(x)$ is not algebraic (as it is divergent). The homogenized equation

$$\left(\frac{x^2y'(x) + y(x)}{x}\right)' = xy''(x) + (1 + \frac{1}{x})y'(x) - \frac{y(x)}{x^2} = 0$$

has no nonzero algebraic solutions because its nonzero formal Puiseux series solutions are scalar multiples of $f(x)$ (exercise) and, hence, are not algebraic. But, for any prime p, its reduction modulo p has a nonzero polynomial solution.

So, the straightforward generalization of Theorem 2.15 cannot be true for higher order differential operators: there are many examples of differential equations that do not admit algebraic solutions and whose reductions modulo p have nonzero rational solutions for almost all p.

The main new insight behind Grothendieck's conjecture is the brilliant idea to replace the existence of a unique nonzero solution by the existence of a *full basis* of solutions.

We recall that the set of solutions of $\mathscr{L}$ in $\overline{\mathbb{Q}(x)}$ is a $\overline{\mathbb{Q}}$-vector space of dimension at most n by the wronskian lemma (see Exercise 11). When this dimension is maximal, that is, equal to n, we say that $\mathscr{L}$ has a full basis of algebraic solutions. Similarly, it is tempting to look at the set of solutions of $\mathscr{L}_p$ in $\mathbb{F}_p(x)$ as an $\mathbb{F}_p$-vector space. However, the example given by the differential equation $y^{(p)} = 0$ shows that this vector space may be infinite dimensional (any element of $\mathbb{F}_p(x)$ is a solution of $y^{(p)} = 0$). The point is that $\overline{\mathbb{Q}}$ is the relevant base field in characteristic 0 because it is the field of differential constants of $\overline{\mathbb{Q}(x)}$. In characteristic p, the field of differential constants of $\mathbb{F}_p(x)$ is not $\mathbb{F}_p$ but $\mathbb{F}_p(x^p)$ (a differential constant may depend on x in characteristic p (!)). Now, the wronskian lemma ensures that the set of solutions of $\mathscr{L}_p$ in $\mathbb{F}_p(x)$ is an $\mathbb{F}_p(x^p)$-vector space of dimension at most n. When this dimension is maximal, that is, equal to n, we say that $\mathscr{L}_p$ has a full basis of rational solutions.

Exercise 11 — (Wronskian Lemma) Let K be a differential field and denote by $C = \{f \in K \mid f' = 0\}$ its field of constants.

1. Consider a differential system $Y' = AY$ with $A \in \mathrm{M}_n(K)$.
   a) Prove that any K-linearly dependent family of solutions of $Y' = AY$ in K^n is actually C-linearly dependent.
   b) Prove that the C-vector space of solutions of $Y' = AY$ in K^n has dimension $\leq n$.
2. Consider a differential equation
$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0 y = 0$$
   with coefficients $a_0, \ldots, a_{n-1} \in K$. Prove that the C-vector space of solutions in K of the latter differential equation has dimension $\leq n$.

We are now ready to state Grothendieck's conjecture.

Conjecture 2.17 (Grothendieck's conjecture)**.** *For a differential operator $\mathscr{L} \in \mathbb{Q}(x)\langle\partial_x\rangle$ as in equation (22), the following properties are equivalent:*

(1) $\mathscr{L}$ has a full basis of algebraic solutions;

(2) for almost all primes p, $\mathscr{L}_p$ has a full basis of rational solutions.

Consider the linear differential operator

$$\mathscr{L} = \partial_x^n + b_{n-1}(x)\cdot\partial_x^{n-1} + \cdots + b_1(x)\cdot\partial_x + b_0(x) \tag{24}$$

with $b_i(x) \in \mathbb{F}_p(x)$. There is no straightforward generalization of Proposition 2.3 for determining whether (24) has a full basis of rational solutions but the criterion given by Proposition 2.11 via the p-curvature does extend to higher order equations. Let us briefly explain this.

Let $Y' + B(x)Y = 0$ be the differential system associated to (24), where

$$B = \begin{pmatrix} 0 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -1 \\ b_0 & b_1 & b_2 & \cdots & b_{n-2} & b_{n-1} \end{pmatrix} \in M_n(\mathbb{F}_p(x)). \tag{25}$$

Mimicking what has been done in Section 2.1.4 in the order-1 case, we consider the map

$$\begin{array}{rcl} \Delta : \mathbb{F}_p(x)^n & \to & \mathbb{F}_p(x)^n \\ F & \mapsto & F' + B(x)F. \end{array}$$

It is $\mathbb{F}_p(x^p)$-linear and satisfies

$$\forall f, g \in \mathbb{F}_p(x), \Delta(fg) = f'g + f\Delta(g).$$

Definition 2.18. The map

$$\Delta^p : \mathbb{F}_p(x)^n \to \mathbb{F}_p(x)^n$$

is called the p-curvature of (24).

As in the first-order case, one can easily prove that the p-curvature is not only $\mathbb{F}_p(x^p)$-linear, but also $\mathbb{F}_p(x)$-linear. Moreover, the inductive formula (19) for computing the p-curvature of equations of order 1 can be extended as follows: the matrix $B_p(x)$ of the p-curvature with respect to the canonical basis is given by the recurrence

$$B_{k+1}(x) = B_k'(x) + B(x)B_k(x) \tag{26}$$

starting with $B_1(x) = B(x)$.

The following fundamental result is a generalization of Proposition 2.11 to higher order differential equations. We recall the fact, already mentioned at the very beginning of Section 2.2, that the set of solutions of a given $\mathscr{L} \in \mathbb{F}_p(x)\langle\partial_x\rangle$ in $\mathbb{F}_p(x)$ of order n is an $\mathbb{F}_p(x^p)$-vector space of dimension at most n and that, when this dimension is maximal, that is, equal to n, we say that $\mathscr{L}$ has a full basis of rational solutions.

Theorem 2.19 (Cartier's lemma)**.** *Let $\mathscr{L} \in \mathbb{F}_p(x)\langle\partial_x\rangle$ be a differential operator as in equation* (24)*. The following properties are equivalent:*

(1) $\mathscr{L}$ has a full basis of rational solutions;

(2) the p-curvature of $\mathscr{L}$ (that is Δ^p) vanishes;

(3) $\mathscr{L}$ divides ∂_x^p in $\mathbb{F}_p(x)\langle\partial_x\rangle$.

Proof. Let us first note that the following properties, relative to the $\mathbb{F}_p(x^p)$-vector space $S := \ker(\Delta)$, are equivalent:

i) the differential equation (24) has a full basis of rational solutions;

ii) the $\mathbb{F}_p(x^p)$-vector space S has dimension n;

iii) the $\mathbb{F}_p(x)$-vector space $\mathbb{F}_p(x)^n$ is spanned by S.

The equivalence between i) and ii) follows immediately from the easily verifiable fact that the map

$$f(x) \mapsto (f(x), f'(x), \ldots, f^{(n-1)}(x))$$

induces an $\mathbb{F}_p(x^p)$-linear isomorphism from the $\mathbb{F}_p(x^p)$-vector space of solutions of $\mathscr{L}$ in $\mathbb{F}_p(x)$ to the $\mathbb{F}_p(x^p)$-vector space S. The equivalence between ii) and iii) follows from the wronskian lemma (see Exercise 11). Indeed, the wronskian lemma ensures that any family of elements of S is linearly dependent over $\mathbb{F}_p(x^p)$ if and only if it is linearly dependent over $\mathbb{F}_p(x)$. Therefore, the dimension of the $\mathbb{F}_p(x^p)$-vector space S and the dimension of the $\mathbb{F}_p(x)$-vector space spanned by S are equal. Considering the case where one or other of these dimensions is n, we obtain the equivalence between ii) and iii).

We are now ready to prove the theorem.

Let us first prove (1)$\Longrightarrow$(2). If $\mathscr{L}$ has a full basis of rational solutions, then the implication i)$\Longrightarrow$iii) ensures that the $\mathbb{F}_p(x)$-vector space $\mathbb{F}_p(x)^n$ is spanned by S. Since Δ^p is $\mathbb{F}_p(x)$-linear and vanishes on S, we have $\Delta^p = 0$.

Let us now prove (2)$\Longrightarrow$(1). We assume that $\Delta^p = 0$. We claim that the $\mathbb{F}_p(x)$-vector space $\mathbb{F}_p(x)^n$ is spanned by S. To prove this, consider the map

$$\begin{array}{rcl} P : \mathbb{F}_p(x)^n & \rightarrow & \mathbb{F}_p(x)^n \\ F & \mapsto & \displaystyle\sum_{k=0}^{p-1} (-1)^k \frac{x^k}{k!} \Delta^k(F). \end{array}$$

We first note that

$$\Delta(P(F)) = (-x)^{p-1} \Delta^p(F) = 0;$$

indeed,

$$\begin{aligned} \Delta(P(F)) &= \sum_{k=0}^{p-1} (-1)^k \left((\frac{x^k}{k!})' \Delta^k(F) + (-1)^k \frac{x^k}{k!} \Delta^{k+1}(F) \right) \\ &= -\sum_{k=1}^{p-1} (-1)^{k-1} \frac{x^{k-1}}{(k-1)!} \Delta^k(F) + \sum_{k=0}^{p-1} (-1)^k \frac{x^k}{k!} \Delta^{k+1}(F) \\ &= (-x)^{p-1} \Delta^p(F) = 0 \end{aligned}$$

This implies that P has values in S. But, another calculation shows that, for all $F \in \mathbb{F}_p(x)^n$, we have

$$F = \sum_{k=0}^{p-1} \frac{x^k}{k!} P(\Delta^k(F));$$

indeed,

$$\begin{aligned}
\sum_{k=0}^{p-1} \frac{x^k}{k!} P(\Delta^k(F)) &= \sum_{k=0}^{p-1} \frac{x^k}{k!} \sum_{l=0}^{p-1} (-1)^l \frac{x^l}{l!} \Delta^{k+l}(F) \\
&= \sum_{k=0}^{p-1} \sum_{l=0}^{p-1} (-1)^l \binom{k+l}{k,l} \frac{1}{(k+l)!} x^{k+l} \Delta^{k+l}(F) \\
&= \sum_{j=0}^{2(p-1)} \left(\sum_{\substack{k,l\in\{0,\dots,p-1\} \\ k+l=j}} (-1)^l \binom{j}{k,l} \right) \frac{1}{j!} x^j \Delta^j(F). \\
&= \sum_{j=0}^{p-1} (1-1)^j \frac{1}{j!} x^j \Delta^j(F) \\
&= F
\end{aligned}$$

where, for the fourth equality, we have used the fact that $\Delta^j = 0$ for all $j \geq p$. This shows that the $\mathbb{F}_p(x)$-vector space $\mathbb{F}_p(x)^n$ is spanned by S as claimed. Now, using the implication iii)$\Longrightarrow$i), we get that $\mathscr{L}$ has a full basis of rational solutions.

It remains to prove that (2)$\Longleftrightarrow$(3). In order to do so, we first notice that, given rational functions $f_0(x), \dots, f_{n-1}(x), g_0(x), \dots, g_{n-1}(x)$, the equality

$$\Delta\big(f_0(x), \dots, f_{n-1}(x)\big) = \big(g_0(x), \dots, g_{n-1}(x)\big)$$

is equivalent to the following congruence in $\mathbb{F}_p(x)\langle\partial_x\rangle$:

$$\big(f_0(x) + \cdots + f_{n-1}(x)\partial_x^{n-1}\big) \cdot \partial_x \equiv g_0(x) + \cdots + g_{n-1}(x)\partial_x^{n-1} \pmod{\mathscr{L}}.$$

It follows from this observation that, writing $E_i = (0, \dots, 0, 1, 0, \dots, 0)$ with the coordinate 1 in i-th position, the coordinates of $\Delta^p(E_i)$ are exactly the coefficients of the remainder in the division of ∂_x^{p+i} by $\mathscr{L}$. Hence $\Delta^p(E_i)$ vanishes if and only if $\mathscr{L}$ divides ∂_x^{p+i}. The equivalence (2)$\Longleftrightarrow$(3) follows immediately. □

Exercise 12 — Prove that a linear differential operator with coefficients in $\mathbb{F}_p(x)$ has a full basis of rational solutions if and only if $\mathscr{L}$ has n solutions in $\mathbb{F}_p[x]$, linearly independent over $\mathbb{F}_p(x^p)$.

Remark 2.20. Actually, under the equivalent assertions (1)–(5), Proposition 1 in [24] shows that there exists a full basis of polynomial solutions in $\mathbb{F}_p[x]$, each of them having degree less than pd, where d is the maximal degree of the numerators/denominators of the coefficients $b_i(x)$ of $\mathscr{L}$ in (24).

Exercise 13 — Consider the map

$$\begin{aligned}
\widehat{\Delta} : \mathbb{F}_p((x))^n &\rightarrow \mathbb{F}_p((x))^n \\
F &\mapsto F' + B(x)F.
\end{aligned}$$

1. State and prove an analogue of Theorem 2.19 involving the solutions in $\mathbb{F}_p((x))^n$ of $\mathscr{L}$ and $\widehat{\Delta}$ instead of the rational solutions of $\mathscr{L}$ and Δ respectively.
2. Deduce from the previous question that $\mathscr{L}$ has a full basis of rational solutions if and only if $\mathscr{L}$ has n solutions in $\mathbb{F}_p((x))$, linearly independent over $\mathbb{F}_p((x^p))$.
3. Prove that $\mathscr{L}$ has n solutions in $\mathbb{F}_p((x))$, linearly independent over $\mathbb{F}_p((x^p))$ if and only if $\mathscr{L}$ has n solutions in $\mathbb{F}_p[[x]]$, linearly independent over $\mathbb{F}_p[[x^p]]$.

Remark 2.21. Assume that $\mathscr{L}$ has p-curvature zero. An easy calculation shows that

$$U_0(x) = \sum_{k=0}^{p-1} (-1)^k \frac{x^k}{k!} B_k(x) \in M_n(\mathbb{F}_p(x))$$

is a solution of $Y' + B(x)Y = 0$. If, moreover, $B(x)$ has no pole at 0, then $U_0(x)$ has no pole at 0 as well and we have $U_0(0) = I_n$, so $U_0(x)$ is a fundamental matrix of rational solutions of $Y' + B(x)Y = 0$. If $B(x)$ has a pole at 0, then $U_0(x)$ is not necessarily invertible (we already saw an example for first order equations).

Note that, more generally, if $a \in \mathbb{F}_p$ is not a pole of $B(x)$, then

$$U_a(x) = \sum_{k=0}^{p-1} (-1)^k \frac{(x-a)^k}{k!} B_k(x)$$

is a fundamental matrix of rational solutions of $Y' + B(x)Y = 0$.

Exercise 14 — (Cartier) The aim of this exercise is to extend the link between the p-curvature and the rational solutions of $\mathscr{L}$ beyond the p-curvature zero case.

1. By inspecting the proof of Theorem 2.19, give a link between the kernel of the p-curvature and the space of rational solutions (*i.e.*, in $\mathbb{F}_p(x)^n$) of $Y' + B(x)Y = 0$.
2. Prove that the dimension of the $\mathbb{F}_p(x^p)$-vector space of rational solutions of $Y' + B(x)Y = 0$ or, equivalently, of (24) is equal to $\dim_{\mathbb{F}_p(x)} \ker \Delta$.

Putting together all that precedes, we obtain a simple algorithm to determine whether (24) has a full basis of rational solutions: compute inductively $B_p(x)$ and, then, check whether $B_p(x)$ vanishes. Note however that no extension of the simple formula of Theorem 2.12 is known for higher order differential equations. Roughly speaking, this is due to the fact that, contrarily to $\mathbb{F}_p(x)$, the ring of $n \times n$ matrices over $\mathbb{F}_p(x)$ is noncommutative as soon as $n \geq 2$. Computing the p-curvature is then much more complicated in this case but rather efficient algorithms for this task are nevertheless available.

Using Theorem 2.19 (Cartier's lemma), we get the following reformulation of Grothendieck's conjecture.

Conjecture 2.22 (Grothendieck's conjecture in terms of p-curvature)**.** *For a differential operator $\mathscr{L}$ as in equation (22), the following properties are equivalent:*

(1) $\mathscr{L}$ has a full basis of algebraic solutions;

(2) for almost all primes p, the p-curvature of $\mathscr{L}_p$ vanishes;

(3) for almost all primes p, $\mathscr{L}_p$ divides ∂_x^p in the ring of differential operators $\mathbb{F}_p(x)\langle\partial_x\rangle$.

Unfortunately, there no simple way to decide whether a given differential operator $\mathscr{L}$ satisfies either of the the last two (equivalent) conditions of Conjecture 2.22. Nonetheless, any differential operator $\mathscr{L}$ satisfying either of these conditions satisfies two easy-to-check properties: they are regular singular with rational exponents. Let's explain this.

3 Vanishing of the p-curvatures, regular singularities and rational exponents: a result of Katz

In this section, we explain the meaning and prove the following statement.

Theorem 3.1 (Katz)**.** *Consider a differential operator $\mathscr{L} \in \mathbb{Q}(x)\langle\partial\rangle$. If, for almost all prime p, the reduction $\mathscr{L}_p$ of $\mathscr{L}$ modulo p has a full basis of solutions in $\mathbb{F}_p(x)$ then $\mathscr{L}$ is regular singular and has rational exponents.*

Remark 3.2. The conclusion of the previous theorem still holds true if, in its hypothesis, we replace "the reduction $\mathscr{L}_p$ of $\mathscr{L}$ modulo p has a full basis of solutions in $\mathbb{F}_p(x)$", which is equivalent to "the reduction $\mathscr{L}_p$ of $\mathscr{L}$ modulo p has p-curvature 0", by "the reduction $\mathscr{L}_p$ of $\mathscr{L}$ modulo p has nilpotent p-curvature". This is what Katz proved.

The fact that "$\mathscr{L}$ is regular singular and has rational exponents" means that $\mathscr{L}$ is regular singular and has rational exponents at any $s \in \mathbb{P}^1(\overline{\mathbb{Q}})$. We will concentrate on the case $s = 0$; the general case reduces to this particular case by a suitable change of variable as we will explain later.

3.1 Regular singular differential equations

In this section, we let C be an algebraically closed field and we consider the differential fields $K = C(z)$ and $\widehat{K} = C((z))$ endowed with the usual derivation $\partial = d/dx$.

We consider a differential operator

$$\mathscr{L} = \sum_{i=0}^{n} a_i(x)\partial^i \in \widehat{K}\langle\partial\rangle$$

of degree n; of course, a differential operator with coefficients in K can be seen as a differential operator with coefficients in $\widehat{K}$.

In what follows, we denote the x-adic valuation by

$$v_x : \widehat{K} \to \mathbb{Z} \cup \{+\infty\}.$$

Definition 3.3. We say that $\mathscr{L}$ is regular singular at 0 if, for all $i \in \{0, \dots, n\}$,

$$v_x(a_i(x)) \geq v_x(a_n(x)) - (n-i).$$

Alternately, expressing the differential operator $\mathscr{L}$ in terms of the derivation $\delta = x\partial$, say

$$\mathscr{L} = \sum_{i=0}^{n} b_i(x)\delta^i,$$

we have :

Proposition 3.4. *The differential operator $\mathscr{L}$ is regular singular at 0 if and only if, for all $i \in \{0, \dots, n\}$,*

$$v_x(b_i(x)) \geq v_x(b_n(x)),$$

the latter condition being equivalent to

$$\frac{b_i(x)}{b_n(x)} \in C[[x]].$$

Exercise 15 — Prove Proposition 3.4. Hint: first prove that, for any $k \in \mathbb{Z}_{\geq 1}$, we have

- $z^k \partial_x^k = \delta(\delta - 1) \cdots (\delta - k + 1)$,
- $\delta^k \in x^k \partial_x^k + \mathrm{Span}_{\mathbb{C}}(x^{k-1}\partial_x^{k-1}, \dots, x\partial_x)$.

Definition 3.5. Assume that $\mathscr{L}$ is regular singular at 0. We define the indicial polynomial of $\mathscr{L}$ at 0 as the monic polynomial of degree n given by

$$\sum_{i=0}^{n} c_i X^i \in C[X]$$

where $c_i = (b_i(x) b_n(x)^{-1})_{|x=0} \in C$. The roots of this polynomial are called the exponents of $\mathscr{L}$ at 0.

We refer to Section 3.4 for a clarification of the interest of this concept.

Exercise 16 — 1. Assume that $\mathscr{L}$ is regular singular at 0 with $a_n = 1$. Let $\widetilde{c}_i = \lim_{z \to 0} z^{n-i} a_i(z)$ for $i \in \{1, \dots, n\}$. Show that the indicial polynomial at 0 of $\mathscr{L}$ is given by

$$X(X-1)\cdots(X-n+1) + \widetilde{c}_{n-1} X(X-1)\cdots(X-n+2) + \cdots + \widetilde{c}_1 X + \widetilde{c}_0.$$

2. Prove that if 0 is an ordinary point of $\mathscr{L}$, then the local exponents at 0 are $0, 1, \dots, n-1$.

Proposition 3.6. *If $\mathscr{L}$ has a full basis of solutions in $\widehat{K}$, then $\mathscr{L}$ is regular singular at 0 and its exponents belong to the prime subring of C.*

Proof. Without loss of generality, we can and will assume that $b_n(x) = 1$.

We claim that

$$\mathscr{L} = (\delta - \delta(f_n) f_n^{-1}) \cdots (\delta - \delta(f_1) f_1^{-1})$$

for certain nonzero $f_1, \dots, f_n \in \widehat{K}$.

Indeed, let us set $\mathscr{L}_1 = \mathscr{L}$. By hypothesis

$$V_1 = \ker(\mathscr{L}_1 : \widehat{K} \to \widehat{K})$$

is a $\widehat{K}^{\partial}$-vector space of dimension n. Let f_1 be a nonzero element of V_1. Then, f_1 is a solution of $\mathscr{L}$ and of $\delta - \delta(f_1) f_1^{-1}$. By euclidean division, there exists $\mathscr{L}_2 \in \widehat{K}\langle \partial \rangle$ of degree $n-1$ such that

$$\mathscr{L} = \mathscr{L}_2(\delta - \delta(f_1) f_1^{-1}).$$

Note that the $\widehat{K}^{\partial}$-vector space

$$V_2 = \ker(\mathscr{L}_2 : \widehat{K} \to \widehat{K}).$$

has at most dimension $n-1$. But, it contains the $\widehat{K}^{\partial}$-vector space $\operatorname{im}(\delta - \delta(f_1)f_1^{-1} : V_1 \to V_1)$ which has dimension $n-1$ by the rank-nullity theorem. So,

$$V_2 = \ker(\mathscr{L}_2 : \widehat{K} \to \widehat{K}) = \operatorname{im}(\delta - \delta(f_1)f_1^{-1} : V_1 \to V_1)$$

is a $\widehat{K}^{\partial}$-vector space of dimension $n-1$. In other words, $\mathscr{L}_2$ has a full basis of solutions in $\widehat{K}$.

Arguing as we did for $\mathscr{L}_1$, we see that

$$\mathscr{L}_2 = \mathscr{L}_3(\delta - \delta(f_2)f_2^{-1})$$

for some $\mathscr{L}_3 \in \widehat{K}\langle\partial\rangle$ of degree $n-2$ having a full basis of solutions in $\widehat{K}$ and some $f_2 \in \widehat{K}^{\times}$.

Our claim clearly follows clearly by iterating this argument.

We are now ready to conclude the proof. Note that, if

$$f_i = c_i x^{\alpha_i} + \text{ higher order terms,}$$

with $c_i \in C^{\times}$ and $\alpha_i \in \mathbb{Z}$, then

$$\delta(f_i)f_i^{-1} \in \alpha_i + xC[[x]].$$

It follows clearly that the $b_i(x)$ belong to $C[[x]]$ and, hence, $\mathscr{L}$ is regular singular at 0 (see Proposition 3.4). Moreover, the indicial polynomial of $\mathscr{L}$ at 0 is $\prod_{i=1}^{n}(X-\alpha_i)$. Indeed, we have

$$\begin{aligned} \mathscr{L} &= (\delta - \delta(f_n)f_n^{-1})\cdots(\delta - \delta(f_1)f_1^{-1}) \\ &= (\delta - \alpha_1 + \star)\cdots(\delta - \alpha_n + \star) \\ &= (\delta - \alpha_1)\cdots(\delta - \alpha_n) + \diamond \end{aligned}$$

where the $\star$ denote elements of $xC[[x]]$ and where $\diamond$ is a sum of terms of the form $p_1 \cdots p_n$ where $p_i \in \{\delta, -\alpha_1, \ldots, -\alpha_n, \star\}$ and at least one of $p_1, \ldots, p_n$ is equal to $\star \in xC[[x]]$. It is easily seen that such a product belongs to $xC[[x]]\langle\delta\rangle$ and the indicial polynomial of $\mathscr{L}$ at 0 is $\prod_{i=1}^{n}(X-\alpha_i)$ as expected. Thus, the exponents of $\mathscr{L}$ at 0 are $\alpha_1, \ldots, \alpha_n$ and, hence, belong to the prime subring of C. □

As an immediate consequence, we have :

Corollary 3.7. *If $\mathscr{L}$ has a full basis of solutions in K, then $\mathscr{L}$ is regular singular at 0 and its exponents belong to the prime subring of C.*

3.2 Regular singular differential equations and reduction modulo p

We consider a differential operator

$$\mathscr{L} = \sum_{i=0}^{n} a_i(x)\partial^i \in \mathbb{Q}(x)\langle\partial\rangle$$

and, for almost all prime p, we denote by

$$\mathscr{L}_p = \sum_{i=0}^{n} a_{i,p}(x)\partial^i \in \mathbb{F}_p(x)\langle\partial\rangle$$

its reduction modulo p.

Proposition 3.8. *The following properties are equivalent :*

- *$\mathscr{L}$ is regular singular at 0;*
- *for almost all prime p, $\mathscr{L}_p$ is regular singular at 0.*

Moreover, in the regular singular case, the following properties are equivalent :

- *the exponents of $\mathscr{L}$ at 0 belong to $\mathbb{Q}$;*
- *for almost all prime p, the exponents of $\mathscr{L}_p$ at 0 belong to the prime subfield $\mathbb{F}_p$.*

Proof. For almost all prime p, we have, for all $i \in \{0, \ldots, n\}$,

$$v_x(a_i(x)) = v_x(a_{i,p}(x)).$$

The following two conditions are thus equivalent :

- for all $i \in \{0, \ldots, n\}$, $v_x(a_i(x)) \geq v_x(a_n(x)) - (n-i)$;
- for almost all prime p, for all $i \in \{0, \ldots, n\}$, $v_x(a_{i,p}(x)) \geq v_x(a_{n,p}(x)) - (n-i)$.

This means that $\mathscr{L}$ is regular singular if and only if, for almost all prime p, $\mathscr{L}_p$ is regular singular.

Let us now assume that $\mathscr{L}$ is regular singular. It is clear that, for almost all prime p, the indicial polynomial of $\mathscr{L}_p$ is equal to the reduction modulo p of the indicial polynomial of $\mathscr{L}$. It is thus sufficient to prove that a monic polynomial $P(X) \in \mathbb{Q}[x]$ of degree n splits completely in $\mathbb{Q}$ if and only if, for almost all prime p, the reduction $P_p(X)$ of $P(X)$ modulo p splits completely in the prime field $\mathbb{F}_p$. But, this latter assertion is true and follows from Kronecker's Theorem 2.6. □

3.3 Proof of Theorem 3.1

Assume that $\mathscr{L}$ has a full basis of solutions in $\mathbb{F}_p(x)$ for almost all prime p. Proposition 3.6 ensures that, for almost all prime p, $\mathscr{L}_p$ is regular singular at 0 and that its exponents belong to $\mathbb{F}_p$. Proposition 3.8 ensures that $\mathscr{L}$ is regular singular at 0 and that its exponents at 0 are rational.

Now, Theorem 3.1 states that $\mathscr{L}$ is regular singular and with rational exponents at any $s \in \mathbb{P}^1(\overline{\mathbb{Q}})$, not only at $s = 0$. Consider the local coordinate $u = x - s$ if $s \in \overline{\mathbb{Q}}$, and $u = 1/x$ if $s = \infty$. We have $\partial_u = \partial$ if $s \in \overline{\mathbb{Q}}$, and $-u^2\partial_u = \partial$ if $s = \infty$. The fact that $\mathscr{L}$ is regular singular at s means that $\mathscr{L}$, seen as an element of $\overline{\mathbb{Q}}(u)\langle\partial_u\rangle$, is regular singular at $u = 0$ in the sense of Definition 3.3.

If $s \in \mathbb{Q} \cup \{\infty\}$, then $\mathscr{L}$ belongs to $\mathbb{Q}(u)\langle\partial_u\rangle$ and it is clear that Theorem 3.1 follows from the case $s = 0$ treated above.

The general case $s \in \overline{\mathbb{Q}} \cup \{\infty\}$ is similar except that the coefficients of $\mathscr{L}$ belong to $\overline{\mathbb{Q}}(u)$ (not necessarily to $\mathbb{Q}(u)$) and we have to extend the case $s = 0$ to this situation; this is not a fundamental problem and all the above could be extended to this situation.

Remark 3.9. Theorem 3.1 leads to satisfactory reformulation of Honda's proof of Grothendieck conjecture for first order equations, *i.e.*, of the fact that, for any first order differential operator $\mathscr{L} = \partial + a(x) \in \mathbb{Q}(x)\langle\partial\rangle$, the following properties are equivalent:

1. $\mathscr{L}$ has a nonzero algebraic solution;
2. for almost all prime p, the reduction $\mathscr{L}_p$ of $\mathscr{L}$ modulo p has a nonzero rational solution.

Indeed, assume that 2 is satisfied. Theorem 3.1 ensures that $\mathscr{L}$ is regular singular on $\mathbb{P}^1(\overline{\mathbb{Q}})$. This implies that $a(x)$ has at most simple poles on $\overline{\mathbb{Q}}$ and that $a(x)$ vanishes at ∞. So :

$$a(x) = \sum_{i=1}^{r} \frac{\alpha_i}{x - x_i}$$

for some $\alpha_i \in \overline{\mathbb{Q}}$ and $x_i \in \overline{\mathbb{Q}}$. The indicial polynomial of $\mathscr{L}$ at x_i is $X + \alpha_i$ and, hence, the exponent of $\mathscr{L}$ at x_i is $-\alpha_i$. Using Theorem 3.1 , we get $-\alpha_i \in \mathbb{Q}$. Now, a nonzero algebraic solution of $\mathscr{L}$ is given by $\prod_{i=1}^{r}(x - x_i)^{-\alpha_i}$, whence 1.

3.4 Regular singular equations in the case $K = \mathbb{C}(\{z\})$

We assume in this section that $K = \mathbb{C}(\{z\})$. We will briefly recall basic facts concerning the analytic theory of regular singular differential equations.

In the case $K = \mathbb{C}(\{z\})$, the fact that $\mathscr{L}$ is regular singular at 0 is equivalent to the fact that its solutions have moderate growth at 0, *i.e.*, to the fact that, for any open sector $S = \{x \in \mathbb{C}^* \mid |x| < \epsilon, \theta_- < \arg(x) < \theta_+\}$ with vertex 0, there exist $C_S > 0$ and $N_S \in \mathbb{Z}$ such that, for any analytic solution $f : S \to \mathbb{C}$ of $\mathscr{L}$, we have, for all $x \in S$,

$$|f(x)| \leq C_S |x|^{N_S}.$$

Also, in the case $K = \mathbb{C}(\{z\})$ we are considering in this section, we can speak of the monodromy of $\mathscr{L}$ at 0 (whether $\mathscr{L}$ is regular singular at 0 or not). Let us briefly recall what it is. Let $D^*(0, \epsilon)$ be a small punctured disc on which the coefficient of $\mathscr{L}$ are analytic and let $x_0 \in D^*(0, \epsilon)$. By Cauchy theorem, the $\mathbb{C}$-vector space V of solutions of $\mathscr{L}$ in $\mathbb{C}\{x - x_0\}$ has dimension n; let $\mathcal{B} = (f_1, \ldots, f_n)$ be a basis of V. One can prove that the f_i can be continued analytically along any loop $\gamma : [0,1] \to D^*(0, \epsilon)$ based at x_0. After analytic continuation, we get a new basis $(\gamma_* f_1, \ldots, \gamma_* f_n)$ of V. So, there exists $M(\gamma) \in \mathrm{GL}_n(\mathbb{C})$ such that

$$(\gamma_* f_1, \ldots, \gamma_* f_n) = (f_1, \ldots, f_n) M(\gamma).$$

This matrix $M(\gamma)$ only depends on the homotopy class of γ in $D^*(0, \epsilon)$ and is called the monodromy matrix of $\mathscr{L}$ along γ. The map

$$\begin{array}{rcl} \rho_{mono} : \pi_1(D^*(0, \epsilon), x_0) & \to & \mathrm{GL}_n(\mathbb{C}) \\ [\gamma] & \mapsto & M([\gamma]) := M(\gamma) \end{array}$$

is a linear representation of $\pi_1(D^*(0,\epsilon),x_0)$ called the monodromy representation of $\mathscr{L}$ (with respect to the basis $\mathcal{B}$). Let $[\gamma_1] \in \pi_1(D^*(0,\epsilon),x_0)$ with winding number 1 around 0. As $[\gamma_1]$ is a generator of $\pi_1(D^*(0,\epsilon),x_0)$, the monodromy representation ρ_{mono} is entirely determined by $\rho_{mono}([\gamma_1]) = M([\gamma_1])$.

Let us now assume that $\mathscr{L}$ is regular singular. Then, the list of eigenvalues (counted with multiplicity) of $M([\gamma_1])$ is given by the $e^{2\pi i\alpha}$ where α varies through the exponents (counted with multiplicity) of $\mathscr{L}$ at 0. The reason is as follows. Let us look for a solution of $\mathscr{L}$ of the form $f(x)x^\alpha$ with $f(x) = 1 + f_1x + f_2x^2 + \cdots \in 1 + x\mathbb{C}[[x]]$ and $\alpha \in \mathbb{C}$. Setting

$$b_i(x) = \sum_j b_{i,j}x^j,$$

it is easily seen that the equations $\mathscr{L}(f(x)x^\alpha) = 0$ is equivalent to

$$\sum_{i=0}^{n}\sum_{j,k\geq 0} b_{i,j}x^j(k+\alpha)^{n-i}f_kx^{k+\alpha} = 0,$$

i.e., to

$$\forall m \geq 0, \quad \sum_{i=0}^{n}\sum_{\substack{j,k\geq 0\\ j+k=m}} b_{i,j}(k+\alpha)^i f_k = 0. \tag{27}$$

For $m = 0$, the latter equation reduces to

$$\sum_{i=0}^{n} b_{i,0}\alpha^i = 0,$$

i.e.,

$$\chi_0(\alpha) = 0$$

where χ_0 is the indicial polynomial of $\mathscr{L}$ at 0; it is satisfied if and only if α is one of the local exponents $\alpha_1,\ldots,\alpha_n$ of $\mathscr{L}$at 0.

To simplify the exposition, let us assume that the local exponents $\alpha_1,\ldots,\alpha_n$ are pairwise distinct modulo $\mathbb{Z}$. Then, for any $\alpha \in \{\alpha_1,\ldots,\alpha_n\}$, there is a unique sequence $(f_n)_{n\geq 0}$ satisfying (27): it can be computed inductively using the following rewriting of (27):

$$\forall m \geq 1, \quad \chi_0(\alpha+m)f_m = -\sum_{i=0}^{n}\sum_{k=0}^{m-1} b_{i,m-k}(k+\alpha)^i f_k.$$

In conclusion, we have shown that $\mathscr{L}$ has n solutions of the form $x^{\alpha_1}f_1,\ldots,x^{\alpha_n}f_n$ with $f_1,\ldots,f_n \in 1 + x\mathbb{C}[[x]]$. These solutions are $\mathbb{C}$-linearly independent. One can prove that actually $f_1,\ldots,f_n \in 1 + x\mathbb{C}\{x\}$. With respect to this basis, the monodromy matrix $M([\gamma_1])$ is given by $\mathrm{diag}(e^{2\pi i\alpha_1},\ldots,e^{2\pi i\alpha_n})$.

If $\alpha_1,\ldots,\alpha_n$ are not distinct modulo $\mathbb{Z}$, then (powers of) $\log(x)$ may come into play creating some unipotent component in $M([\gamma_1])$, but its eigenvalues are still given by $e^{2\pi i\alpha_1},\ldots,e^{2\pi i\alpha_n}$.

The procedure outlined above is known as Frobenius method; see for instance Section 3 of Chapter 1 of [55] for details.

Remark 3.10. For an extension of Frobenius in positive characteristic, we refer to [52] and to the references therein.

4 Grothendieck conjecture for the generalized hypergeometric equations

In this Section, we will focus our attention on differential operators of the form

$$\mathscr{H}\left(P(X),Q(X)\right)=P(\delta)-xQ(\delta) \tag{28}$$

where $\delta=x\partial=x\partial_x$ and $P(X),Q(X)\in\mathbb{Q}[X]\setminus\{0\}$. These are called generalized hypergeometric operators.

Example 4.1. For $P(X)=X(X+\gamma-1)$ and $Q(X)=(X+\alpha)(X+\beta)$, we obtain the classical Gauss hypergeometric operator, that can be written, up to a left multiplicative factor in $\mathbb{Q}(x)^\times$, as follows:

$$x(1-x)\partial^2+\left[\gamma-(\alpha+\beta+1)x\right]\partial-\alpha\beta.$$

Our next objective is to explain how the condition "for almost all prime p, the reduction $\mathscr{H}\left(P(X),Q(X)\right)_p$ of $\mathscr{H}\left(P(X),Q(X)\right)$ modulo p has a full basis of solutions in $\mathbb{F}_p(x)$" can be read on the polynomials $P(X)$ and $Q(X)$.

4.1 Generalized hypergeometric equations with p-curvature 0

Lemma 4.2. *Assume that, for almost all prime p, the reduction $\mathscr{H}\left(P(X),Q(X)\right)_p$ modulo p of the generalized hypergeometric operator $\mathscr{H}\left(P(X),Q(X)\right)$ has a full basis of solutions in $\mathbb{F}_p(x)$, then $P(X)$ and $Q(X)$ have the same degree and they split completely over $\mathbb{Q}$.*

Proof. Theorem 3.1 ensures that $\mathscr{H}\left(P(X),Q(X)\right)$ is regular singular with exponents in $\mathbb{Q}$.

We claim that $\mathscr{H}\left(P(X),Q(X)\right)$ is regular singular if and only if $P(X)$ and $Q(X)$ have the same degree. We set

$$P(X)=\sum_{i=0}^{d}p_ix^i,\quad Q(X)=\sum_{i=0}^{e}q_ix^i$$

where $d=\deg_X P(X)$ and $e=\deg_X Q(X)$.

If $d<e$ then

$$\mathscr{H}\left(P(X),Q(X)\right)=P(\delta)-xQ(\delta)=q_ex\delta^e+\cdots+q_{d+1}x\delta^{d+1}+\sum_{i=0}^{d}(p_i-q_ix)\delta^i$$

The coefficient q_ex of δ^e vanishes at $x=0$ but, as $p_d\neq 0$, the coefficient p_d-q_dx of δ^d does not at $x=0$; this implies that $\mathscr{H}\left(P(X),Q(X)\right)$ is irregular (=non regular singular) at $x=0$ (use Proposition 3.4).

If $d>e$ then, in terms of the variable $u=x^{-1}$ and of the derivatives $\delta_u=ud/du=-\delta$, we have

$$\mathscr{H}\left(P(X),Q(X)\right)=u^{-1}(uP(-\delta_u)-Q(-\delta_u)). \tag{29}$$

It follows from the case $d<e$ treated above that $\mathscr{H}\left(P(X),Q(X)\right)$ is irregular at $u=0$, *i.e.*, at $x=\infty$.

Let us prove that $\mathscr{H}(P(X), Q(X))$ is regular singular if $d = e$. Indeed, in this case, we have

$$\mathscr{H}(P(X), Q(X)) = P(\delta) - xQ(\delta) = \sum_{i=0}^{d}(p_i - q_i x)\delta^i. \tag{30}$$

As $p_d - q_d x$ does not vanish at $x = 0$, we see that $\mathscr{H}(P(X), Q(X))$ is regular singular at $x = 0$ (use Proposition 3.4). Using (29), we see similarly that $\mathscr{H}(P(X), Q(X))$ is regular singular at $x = \infty$. Using the fact that $\delta^k \in x^k(d/dx)^k + \mathrm{Span}_{\mathbb{C}}(x^{k-1}(d/dx)^{k-1}, \dots, x(d/dx))$ (see Exercise 15), we see that the coefficient of $(d/dz)^d$ in $\mathscr{H}(P(X), Q(X))$ is $z^d(p_d - q_d x)$ (and all the other coefficients are polynomials). So, except 0 and ∞, p_d/q_d is the only other possible singular point and it follows clearly from the definition that this is at most a regular singularity.

Until the end of the proof, we assume that $\mathscr{H}(P(X), Q(X))$ is regular singular, *i.e.*, that $d = e$.

Note that the indicial polynomial of $\mathscr{H}(P(X), Q(X))$ at 0 (resp. at ∞) is, up to a multiplicative constant, $P(X)$ (resp. $Q(-X)$); this follows immediately from formulas (30) and (29). So, as $\mathscr{H}(P(X), Q(X))$ has exponents in $\mathbb{Q}$, the polynomials $P(X)$ and $Q(X)$ split completely over $\mathbb{Q}$. □

Therefore, as far as we are interested in operators $\mathscr{H}(P(X), Q(X))$ such that, for almost all prime p, $\mathscr{H}(P(X), Q(X))_p$ has a full basis of solutions in $\mathbb{F}_p(x)$, we can assume that

$$P(X) = \prod_{i=1}^{n}(X - \alpha_i) \text{ and } Q(X) = \prod_{i=1}^{n}(X - \beta_i)$$

for some $n \in \mathbb{Z}_{\geq 1}$, $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{Q}^n$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n) \in \mathbb{Q}^n$ (one can assume that $P(X)$ and $Q(X)$ are monic after a change of variable $x \leftarrow \lambda x$ for some $\lambda \in \mathbb{Q}^\times$). We will use the following notation:

$$\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \mathscr{H}\left(\prod_{i=1}^{n}(X - \alpha_i), \prod_{i=1}^{n}(X - \beta_i)\right) = \prod_{i=1}^{n}(\delta - \alpha_i) - x\prod_{i=1}^{n}(\delta - \beta_i).$$

This operator is regular singular, its set of singularities is included in $\{0, 1, \infty\}$, its exponents at 0 are $\alpha_1, \dots, \alpha_n$, its exponents at ∞ are $\beta_1, \dots, \beta_n$ (see Lemma 4.2 and its proof).

Exercise 17 — Show that the exponents at 1 of $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ are:

$$0, 1, \dots, n-2, -1 + n + \sum_{i=1}^{n}\alpha_i - \sum_{i=1}^{n}\beta_i.$$

The fact that the reduction $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})_p$ of $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ modulo p has or doesn't have a full basis of solutions can be read on the parameters $\boldsymbol{\alpha}, \boldsymbol{\beta}$. [59, SubLemma 5.5.2.1]

Proposition 4.3 (Katz [59, SubLemma 5.5.2.1])**.** *Consider $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in (\mathbb{Q} \cap [0, 1[)^n$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n) \in (\mathbb{Q} \cap [0, 1[)^n$ such that*[1]*, for all $i, j \in \{1, \dots, n\}$, $\alpha_i \neq \beta_j$. Let N be a common*

[1] For $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{C}^n$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n) \in \mathbb{C}^n$, the hypergeometric operator $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is irreducible if and only if, for all $i, j \in \{1, \dots, n\}$, $\alpha_i - \beta_j \notin \mathbb{Z}$. Moreover, if it is irreducible, $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ with $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{C}^n$ is isomorphic to $\mathscr{H}(\boldsymbol{\alpha}', \boldsymbol{\beta}')$ with $\boldsymbol{\alpha}', \boldsymbol{\beta}' \in \mathbb{C}^n$ if and only if, up to permuting the entries of $\boldsymbol{\alpha}'$ and $\boldsymbol{\beta}'$, we have $\boldsymbol{\alpha}' - \boldsymbol{\alpha} \in \mathbb{Z}^n$ and $\boldsymbol{\beta}' - \boldsymbol{\beta} \in \mathbb{Z}^n$.

denominator to the α_i and of the β_j. Then, for any prime $p > N \max\{|\alpha_i - \beta_j| \mid i, j \in \{1, \ldots, n\}\}$, the reduction $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})_p$ of $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ modulo p has a full basis of solutions in $\mathbb{F}_p(x)$ if and only if the following conditions are statisfied :

1. *the α_i and the β_j have $2n$ distinct reductions modulo p in $\mathbb{F}_p$;*
2. *the reductions modulo p of the α_i are intertwined with those of the β_j in the sense that as we walk through $\mathbb{F}_p$ in the standard order $0, 1, \ldots$ we alternately encounter α_is and β_js.*

Proof. We will only give the proof in the case $n = 2$; the general case is similar, but requires more notations.

Let $b_2 \in \mathbb{Z}$ be such that

$$\beta_2 = b_2 \operatorname{mod} p$$

and let $b_1 \in \{b_2 - p + 1, \ldots, b_2\}$ be such that

$$\beta_1 = b_1 \operatorname{mod} p.$$

We have to prove that the kernel of the $\mathbb{F}_p(x^p)$-linear map $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})_p : \mathbb{F}_p(x) \to \mathbb{F}_p(x)$ has dimension 2 if and only if conditions (1) and (2) are satisfied. The key observation is that $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})_p$ acts in a very simple way on x^i :

$$\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})_p (x^i) = P(i)x^i - Q(i)x^{i+1}.$$

This observation suggests that we consider the matrix of the $\mathbb{F}_p(x^p)$-linear map $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})_p : \mathbb{F}_p(x) \to \mathbb{F}_p(x)$ with respect to the basis

$$\mathcal{B} = (x^{b_2-p+1}, \ldots, x^{b_2})$$

of the $\mathbb{F}_p(x^p)$-vector space $\mathbb{F}_p(x)$.

Let us first assume that $b_1 = b_2 =: b$. Using the fact that $Q(b) = 0 \operatorname{mod} p$, we see that the matrix of the $\mathbb{F}_p(x^p)$-linear map $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})_p : \mathbb{F}_p(x) \to \mathbb{F}_p(x)$ with respect to the basis $\mathcal{B} = (x^{b-p+1}, \ldots, x^b)$ is given by

$$A = \begin{pmatrix} P(b-p+1)) & 0 & & & 0 \\ -Q(b-p+1) & P(b-p+2) & & & \\ 0 & -Q(b-p+2) & \ddots & & \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & -Q(b-1) & P(b) \end{pmatrix} \operatorname{mod} p.$$

Since the subdiagonal terms of this matrix are nonzero, the rank of A is at least $n-1$ (its first $n-1$ columns are $\mathbb{F}_p(x^p)$-linearly independent), so the kernel of A has dimension at most 1 and, in particular, is not equal to 2.

Let us now assume that $b_1 \neq b_2$. Using the fact that $Q(b_1) = Q(b_2) = 0 \operatorname{mod} p$, we see that the matrix of the $\mathbb{F}_p(x^p)$-linear map $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})_p : \mathbb{F}_p(x) \to \mathbb{F}_p(x)$ with respect to the basis $\mathcal{B} = (x^{b_2-p+1}, \ldots, x^{b_1}, x^{b_1+1}, \ldots, x^{b_2})$ is given by

$$A = \begin{pmatrix} A_0 & 0 \\ 0 & A_1 \end{pmatrix}$$

where

$$A_0 = \begin{pmatrix} P(b_2 - p + 1)) & 0 & & & 0 \\ -Q(b_2 - p + 1) & P(b_2 - p + 2) & & & \\ 0 & \ddots & \ddots & & \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & -Q(b_1 - 1) & P(b_1) \end{pmatrix} \bmod p$$

and

$$A_1 = \begin{pmatrix} P(b_1 + 1) & 0 & & & 0 \\ -Q(b_1 + 1) & P(b_1 + 2) & & & \\ 0 & \ddots & \ddots & & \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & -Q(b_2 - 1) & P(b_2) \end{pmatrix} \bmod p.$$

As above, since the subdiagonal terms of these matrices are nonzero, their kernels have dimension at most 1. Therefore, $\ker A = \ker A_0 \oplus \ker A_1$ has dimension 2 if and only if $\ker A_0$ and $\ker A_1$ both have dimension ≥ 1. This is equivalent to the fact that at least one of the diagonal terms of A_0 and at least one of the diagonal terms of A_1 is zero, that is, equivalent to the fact that there exist $a_1 \in \{b_2 - p + 1, \dots, b_1\}$ and $a_2 \in \{b_1 + 1, \dots, b_2\}$ such that $P(a_1) = P(a_2) = 0 \bmod p$.

In order to conclude, it remains to note that $b_1 \neq a_1$ and $b_2 \neq a_2$. Indeed, if $b_i = a_i$ then $\beta_i = \alpha_i \bmod p$ so $N(\beta_i - \alpha_i) = 0 \bmod p$, but $N(\beta_i - \alpha_i) \in \mathbb{Z}$ and $p > N \max\{|\alpha_i - \beta_j| \mid i, j \in \{1, \dots, n\}\}$, so $\alpha_i = \beta_i$, whence a contradiction. □

Using [59, SubLemma 5.5.2.2], Katz deduces the following result from Proposition 4.3.

Theorem 4.4. *Consider $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in (\mathbb{Q} \cap [0, 1[)^n$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n) \in (\mathbb{Q} \cap [0, 1[)^n$ such that, for all $i, j \in \{1, \dots, n\}$, $\alpha_i \neq \beta_j$. Let N be a common denominator to the α_i and the β_j. Then, the reduction modulo p of $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ has a full basis of solutions in $\mathbb{F}_p(x)$ for almost all prime p if and only if the following conditions are satisfied :*

1. *$e^{2\pi i r\alpha_1}, \dots, e^{2\pi i r\alpha_n}, e^{2\pi i r\beta_1}, \dots, e^{2\pi i r\beta_n}$ are pairwise distinct;*
2. *for any integer $r \in \{1, \dots, N-1\}$ coprime with N, $e^{2\pi i r\alpha_1}, \dots, e^{2\pi i r\alpha_n}$ and $e^{2\pi i r\beta_1}, \dots, e^{2\pi i r\beta_n}$ are intertwined on the unit circle.*

In this way, Katz recovered the famous intertwining condition that appeared in the famous paper [10] by Beukers and Heckman, where it is proven that they are equivalent to the fact that $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ has a full basis of algebraic solutions. In the next section, we give a brief overview of their proof of this equivalence.

Remark 4.5. Katz gives a a second proof of this equivalence in [59]; see Section 5.

4.2 Generalized hypergeometric equations with a full basis of algerbaic solutions

The equivalence between conditions 2 and 3 of the following result is a result due Beukers and Heckman in [10], of which Katz later gave another proof in [59]. The equivalence between conditions 1 and 2 is due to Katz in [59].

Theorem 4.6. *Consider $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in (\mathbb{Q} \cap [0,1[)^n$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n) \in (\mathbb{Q} \cap [0,1[)^n$ such that, for all $i, j \in \{1, \dots, n\}$, $\alpha_i \neq \beta_j$. Let N be a common denominator to the α_i and of the β_j. The following conditions are equivalent :*

1. *for almost all prime p, the reduction modulo p of $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ has a full basis of rational solutions;*

2. *$e^{2\pi i r \alpha_1}, \dots, e^{2\pi i r \alpha_n}, e^{2\pi i r \beta_1}, \dots, e^{2\pi i r \beta_n}$ are pairwise distinct and, for any integer $r \in \{1, \dots, N-1\}$ coprime with N, $e^{2\pi i r \alpha_1}, \dots, e^{2\pi i r \alpha_n}$ and $e^{2\pi i r \beta_1}, \dots, e^{2\pi i r \beta_n}$ are intertwined on the unit circle;*

3. *$\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ has a full basis of algebraic solutions.*

Let us outline the proof of the equivalence between conditions 2 and 3 following Beukers and Heckman in [10]. The starting point is the following fact:

Proposition 4.7. *A linear differential equation $\mathscr{L}(y) = 0$ with coefficients in $\mathbb{Q}(x)$ has a full basis of algebraic solutions if and only the following conditions are satisfied:*

- *$\mathscr{L}$ is regular singular;*

- *the monodromy group of $\mathscr{L}$ is finite.*

Before proving this result, we recall that the concept of regular singular operator has already been introduced in Section 3.1: it was defined by an algebraic condition (on the valuations of the coefficients of $\mathscr{L}$) but, as mentioned in Section 3.4, it is equivalent to an analytic condition of moderate growth of the solutions of $\mathscr{L}$ at its singularities. Moreover, the construction of the (global) monodromy representation and of the (global) monodromy group attached to $\mathscr{L}$ follows the same lines as the construction of the (local) monodromy representation attached to a differential equation with coefficients on $\mathbb{C}(\{z\})$ given in Section 3.4, we only have to replace the punctured disk $D^*(0,\epsilon)$ by $\mathbb{P}^1(\mathbb{C}) \setminus S$ where S is the set of singularities in $\mathbb{P}^1(\mathbb{C})$ of $\mathscr{L}$. Precisely, let $x_0 \in \mathbb{P}^1(\mathbb{C}) \setminus S$ and let $\mathcal{B} = (f_1, \dots, f_n)$ be a basis of analytic solutions at x_0 of $\mathscr{L}$. The f_i can be continued analytically along any loop $\gamma : [0,1] \to \mathbb{P}^1(\mathbb{C}) \setminus S$ based at x_0 and, after analytic continuation, we get a new basis $(\gamma_* f_1, \dots, \gamma_* f_n)$ of solutions of $\mathscr{L}$. So, there exists $M(\gamma) \in \mathrm{GL}_n(\mathbb{C})$ such that

$$(\gamma_* f_1, \dots, \gamma_* f_n) = (f_1, \dots, f_n) M(\gamma).$$

This matrix $M(\gamma)$ only depends on the homotopy class of γ in $\mathbb{P}^1(\mathbb{C}) \setminus S$. The monodromy representation is nothing but

$$\begin{array}{rcl} \rho_{mono} : \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S, x_0) & \to & \mathrm{GL}_n(\mathbb{C}) \\ [\gamma] & \mapsto & M([\gamma]) := M(\gamma). \end{array}$$

The corresponding monodromy group is the image of ρ_{mono}.

The fundamental group $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S, z_0)$ is a free group with $m-1$ generators where $m = \sharp S$. Set $S = \{s_1, \dots, s_m\}$. For any $i \in \{1, \dots, m\}$, let $\gamma_{s_i} : [0,1] \to \mathbb{P}^1(\mathbb{C}) \setminus S$ be the loop represented in Figure 2 and set

$$M_{s_i} = \rho_{mono}([\gamma_{s_i}]) \in G_{mono}.$$

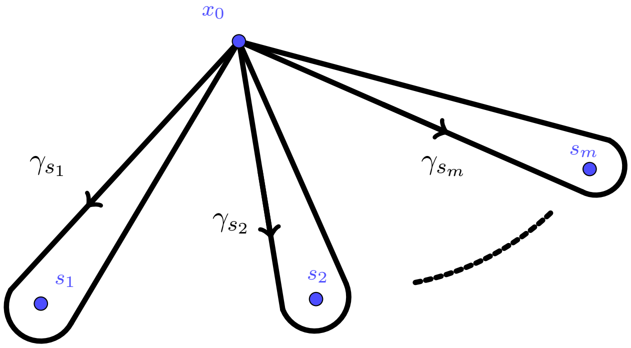

Figure 2: The loops $\gamma_{s_1}, \ldots, \gamma_{s_m}$.

Then, $([\gamma_{s_1}], \ldots, [\gamma_{s_{m-1}}])$ is a basis of $\pi_1(\mathbb{P}^1(\mathbb{C})\backslash S, z_0)$ and G_{mono} is generated by $M_{s_1}, \ldots, M_{s_{m-1}}$:

$$G_{mono} = \langle M_{s_1}, \ldots, M_{s_{m-1}} \rangle.$$

Moreover, we have $[\gamma_{s_1}] \cdots [\gamma_{s_m}] = 1$ and, hence,

$$M_{s_1} \cdots M_{s_m} = I_n. \tag{32}$$

The eigenvalues (listed with multiplicities) of M_{s_i} are the $e^{2\pi i \alpha}$ where α varies through the roots (counted with multiplicities) of the indicial polynomial of $\mathscr{L}$ at s_i. So far, we have defined the monodromy by fixing a basis, but it can of course be define without choosing a basis, by replacing $\mathrm{GL}_n(\mathbb{C})$ by $\mathrm{GL}(V)$ where V is the $\mathbb{C}$-vector space of dimension n of analytic solutions at x_0 of $\mathscr{L}$.

Proof of Proposition 4.7. Assume that $\mathscr{L}$ has a full basis of algebraic solutions. Then, with the notations introduced in the discussion preceding this proof, $f_1, \ldots, f_n$ are algebraic. Let $P_i(X) \in \mathbb{Q}[X] \setminus \{0\}$ be such that $P_i(f_i) = 0$. Then, for any $[\gamma] \in \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S, x_0)$, $P_i(\gamma_*(f_i)) = \gamma_*(P_i(f_i)) = 0$, so $\gamma_*(f_i)$ is a root of P_i. In particular, there are only finitely many possibilities for $\gamma_*(f_i)$ when $[\gamma]$ varies in $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S, x_0)$. This clearly implies that G_{mono} is finite (it can be identified with a subgroup of the group of permutations of $f_1, \ldots, f_n$).

Conversely, let us assume that G_{mono} is finite (we see G_{mono} as a subgroup of $\mathrm{GL}(V)$ where V is the $\mathbb{C}$-vector space of dimension n of germs of analytic solutions at x_0 of $\mathscr{L}$). Let f be a solution of $\mathscr{L}$ analytic near x_0. Consider the polynomial $P(X) = \prod_{\sigma \in G_{mono}} (X - \sigma(f))$. A priori, its coefficients are germs of analytic functions at x_0 that can be analytically continued along any path in $\mathbb{P}^1(\mathbb{C}) \setminus S$ (*i.e.*, analytic functions on the universal covering of $\mathbb{P}^1(\mathbb{C}) \setminus S$). But, these coefficients are invariant under the action of $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S, x_0)$, so they are meromorphic over $\mathbb{P}^1(\mathbb{C}) \setminus S$. Moreover, the fact that $\mathscr{L}$ is regular singular ensures that they have moderate growth at any $s \in S$. Therefore, they are meromorphic on $\mathbb{P}^1(\mathbb{C})$, *i.e.*, rational. Since $P(f) = 0$, we get that f is algebraic. □

A key result in Beukers and Heckman's proof is the following result due to Levelt giving an explicit formula for generators of the monodromy group of $\mathscr{H}(\boldsymbol{\alpha},\boldsymbol{\beta})$ (with respect to a suitable basis of solutions) provided that[2], for all $i,j \in \{1,\ldots,n\}$, $\alpha_i \not\equiv \beta_j \bmod \mathbb{Z}$.

Theorem 4.8 (Levelt)**.** *We assume that, for all $i,j \in \{1,\ldots,n\}$, $\alpha_i \not\equiv \beta_j \bmod \mathbb{Z}$. With respect to a suitable basis of solutions, the monodromy matrices M_0 and M_∞ of $\mathscr{H}(\boldsymbol{\alpha},\boldsymbol{\beta})$ are given by*

$$M_0 = \begin{bmatrix} 0 & 0 & \ldots & 0 & -A_n \\ 1 & 0 & \ldots & 0 & -A_{n-1} \\ 0 & 1 & \ldots & 0 & -A_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -A_1 \end{bmatrix}$$

and

$$M_\infty = \begin{bmatrix} 0 & 0 & \ldots & 0 & -B_n \\ 1 & 0 & \ldots & 0 & -B_{n-1} \\ 0 & 1 & \ldots & 0 & -B_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -B_1 \end{bmatrix}^{-1}$$

where the A_i and the B_j are given by:

$$\prod_{k=1}^{n}(X - e^{2\pi i\alpha_k}) = X^n + A_1X^{n-1} + \cdots + A_n$$

and

$$\prod_{k=1}^{n}(X - e^{2\pi i\beta_k}) = X^n + B_1X^{n-1} + \cdots + B_n.$$

Therefore, with respect to a suitable basis of solutions, the monodromy group $H(\boldsymbol{\alpha},\boldsymbol{\beta})$ of $\mathscr{H}(\boldsymbol{\alpha},\boldsymbol{\beta})$ is generated by M_0 and M_∞:

$$H(\boldsymbol{\alpha},\boldsymbol{\beta}) = \langle M_0, M_\infty\rangle.$$

Remark 4.9. We emphasize that Theorem 4.8 gives no information about the basis of solutions for which the monodromy matrices at 0 and ∞ are given by the formulae above.

Remark 4.10. We point out that it is generally very difficult to calculate generators of the monodromy group of an arbitrary differential equation; what makes the hypergeometric case tractable is the fact that the (irreducible) generalized hypergeometric operators $\mathscr{H}(\boldsymbol{\alpha},\boldsymbol{\beta})$ are rigid.

The following exercise gives a proof of Theorem 4.8 in the case $n = 2$.

Exercise 18 — The aim of this exercise is to prove Theorem 4.8 for Gauss hypergeometric equation, *i.e.*, for $\alpha_1 = 0$, $\alpha_2 = \gamma - 1$, $\beta_1 = \alpha$, $\beta_2 = \beta$ assuming that $\alpha, \beta, \alpha-\gamma, \beta-\gamma \notin \mathbb{Z}$.

[2] We recall that, for $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n) \in \mathbb{C}^n$ and $\boldsymbol{\beta} = (\beta_1,\ldots,\beta_n) \in \mathbb{C}^n$, the hypergeometric operator $\mathscr{H}(\boldsymbol{\alpha},\boldsymbol{\beta})$ is irreducible if and only if, for all $i,j \in \{1,\ldots,n\}$, $\alpha_i - \beta_j \notin \mathbb{Z}$.

Here are some useful facts that we already know. The monodromy group G is generated by the local monodromy matrices M_0, M_1 and M_∞ along the loops γ_0, γ_1 and γ_∞ respectively represented in Figure 3 with respect to an arbitrary fundamental matrix of solutions. We have

$$M_0 M_1 M_\infty = I_2.$$

This relation implies that G is generated by any two of M_0, M_1 and M_∞, and in particular by M_0 and M_∞. The eigenvalues of M_0, M_1 and M_∞ are given by $(1, e^{-2\pi i\gamma})$, $(1, e^{2\pi i(\gamma-\alpha-\beta)})$ and $(e^{2\pi i\alpha}, e^{2\pi i\beta})$ respectively.
We have to prove that there exists $P \in \mathrm{GL}_n(\mathbb{C})$ such that

$$M_0 = P \begin{pmatrix} 0 & -p_0 \\ 1 & -p_1 \end{pmatrix} P^{-1},$$

$$M_\infty^{-1} = P \begin{pmatrix} 0 & -q_0 \\ 1 & -q_1 \end{pmatrix} P^{-1},$$

$$M_1 = P M_0^{-1} M_\infty^{-1} P^{-1}$$

where $p_0, p_1, q_0 q_1 \in \mathbb{C}$ are determined by the equalities $X^2 + p_1 X + p_0 = (X-1)(X - e^{-2\pi i\gamma})$ and $X^2 + q_1 X + q_0 = (X - e^{-2\pi i\alpha})(X - e^{-2\pi i\beta})$.
The monodromy group G it is generated by the local monodromy matrices M_0, M_1 and M_∞ along the loops represented in Figure 3. We have seen that

$$M_0 M_1 M_\infty = I_2$$

and that the eigenvalues of M_0, M_1 and M_∞ are given by $(1, e^{-2\pi i\gamma})$, $(1, e^{2\pi i(\gamma-\alpha-\beta)})$ and $(e^{2\pi i\alpha}, e^{2\pi i\beta})$ respectively.

1. Prove that the monodromy representation (*i.e.*, the standard representation of G) is irreducible.
2. Prove that $W = \ker(M_0^{-1} - M_\infty)$ has dimension 1.
3. Prove that $\mathbb{C}^2 = W \oplus M_0^{-1} W$.
4. Conclude the proof.

We are now in a position to outline the proof of Theorem 4.6.

Outline of the proof of Theorem 4.6. As $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is regular singular, it has a full basis of algebraic solutions if and only if its monodromy group is finite in virtue of Proposition 4.7.

We denote by $H(\boldsymbol{\alpha}, \boldsymbol{\beta})$ the group generated by the matrices M_0 and M_∞ given in Theorem 4.8; this is the monodromy group of $\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ with respect to a suitable basis of solutions.

Using these explicit generators of $H(\boldsymbol{\alpha}, \boldsymbol{\beta})$, Beukers and Heckman's prove the following facts which are the main ingredients of their proof of Theorem 4.6:

1. the monodromy group $H(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is contained in $\mathbb{Z}[\zeta]$ with $\zeta = e^{\frac{2\pi i}{N}}$ where $N \in \mathbb{Z}_{\geq 1}$ is a common denominator of the α_i and of the β_j;

2. the monodromy group $H(\boldsymbol{\alpha}, \boldsymbol{\beta})$ leaves invariant a non-degenerate hermitian form $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ with signature (p, q) satisfying

$$|p - q| = |\sum_{j=1}^{n} (-1)^{j+m_j}|$$

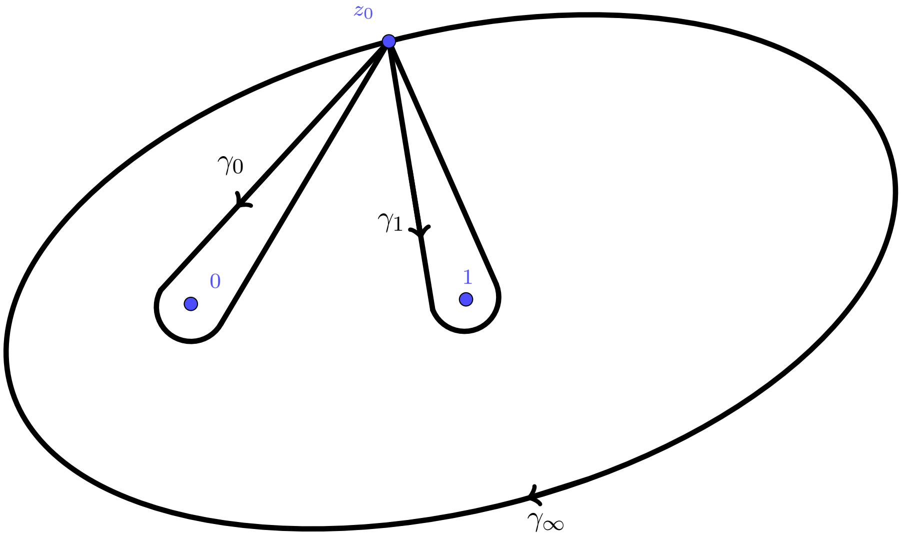

Figure 3: The loops $\gamma_0, \gamma_1, \gamma_\infty$.

where the m_j are defined as follows: denote by $\prec$ the total ordering on the unit circle corresponding to increasing argument, set $a_j = e^{2\pi i \alpha_j}$ and $b_j = e^{2\pi i \beta_j}$ and assume that $a_1 \preceq \cdots \preceq a_n$ and $b_1 \preceq \cdots \preceq b_n$ (always possible up to renumbering), set $m_j = \sharp\{k \in \{1, \ldots, n\} \mid b_k \prec a_j\}$, then $m_j = \sharp\{k \in \{1, \ldots, n\} \mid b_k \prec a_j\}$. In particular, we see that $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ is definite if and only if $a_1, \ldots, a_n, b_1, \ldots, b_n$ are pairwise distinct and $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are intertwined on the unit circle (indeed, it is definite if and only if $|p - q| = n$ if and only if all the $(-1)^{j+m_j}$ have the same value if and only if either m_1 is odd, m_2 is even, m_3 is odd, m_4 is even, *etc*, or m_1 is even, m_2 is odd, m_3 is even, m_4 is odd, *etc*; as $m_1, \ldots, m_n$ is a nondecreasing sequence of elements of $\{0, \ldots, n\}$, the latter condition holds true if and only if either, for all $j \in \{1, \ldots, n\}$, $m_j = j$ or, for all $j \in \{1, \ldots, n\}$, $m_j = j - 1$; these conditions are equivalent to the fact that $a_1, \ldots, a_n, b_1, \ldots, b_n$ are pairwise distinct and that $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are intertwined on the unit circle).

The first point is clear as the matrices $M_0^{\pm 1}$ and $M_0^{\pm 1}$ have entries in $\mathbb{Z}[\zeta]$. The second point needs more work and will not be detailed here.

Assume that condition 2 of Theorem 4.6 is satisfied and let us prove that $H(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is finite. This condition 2 guaranties that $F_{r\boldsymbol{\alpha},r\boldsymbol{\beta}}$ is definite for any $r \in \{1, \ldots, N-1\}$ coprime with N. Since $\sigma_r(H(\boldsymbol{\alpha}, \boldsymbol{\beta})) = H(r\boldsymbol{\alpha}, r\boldsymbol{\beta})$ where $\sigma_r \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is defined by $\sigma_r(\zeta) = \zeta^r$, we have that $\sigma_r(H(\boldsymbol{\alpha}, \boldsymbol{\beta}))$ leaves invariant the definite hermitian form $F_{r\boldsymbol{\alpha},r\boldsymbol{\beta}}$. So, we obtain that, for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $\sigma(H(\boldsymbol{\alpha},\boldsymbol{\beta}))$ leaves invariant a definite hermitian form. Now, the desired result follows from the general fact that, given a family of definite hermitian forms $(F_\sigma)_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})}$ on $\mathbb{C}^n$, there are finitely many $n\times n$ square matrices M with coefficients in $\mathbb{Z}[\zeta]$ such that, for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $\sigma(M)$ leaves invariant F_σ.

Conversely, assume that $H(\boldsymbol{\alpha},\boldsymbol{\beta})$ is finite. Then, $H(\boldsymbol{\alpha},\boldsymbol{\beta})$ leaves invariant the definite hermitian form $\frac{1}{|H(\boldsymbol{\alpha},\boldsymbol{\beta})|}\sum_{M\in H(\boldsymbol{\alpha},\boldsymbol{\beta})}\langle Mx, My\rangle$ where $\langle,\rangle$ is an arbitrary definite hermitian form on $\mathbb{C}^n$. But, by irreducibility of $H(\boldsymbol{\alpha},\boldsymbol{\beta})$, any $H(\boldsymbol{\alpha},\boldsymbol{\beta})$-invariant hermitian form on $\mathbb{C}^n$ is a multiple by a nonzero scalar of that one. It follows that $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ is definite and, hence, that $e^{2\pi i\alpha_1},\dots,e^{2\pi i\alpha_n},e^{2\pi i\beta_1},\dots,e^{2\pi i\beta_n}$ are pairwise distinct and that $e^{2\pi i\alpha_1},\dots,e^{2\pi i\alpha_n}$ and $e^{2\pi i\beta_1},\dots,e^{2\pi i\beta_n}$ are intertwined on the unit circle. Applying the same argument to $\sigma(H(\boldsymbol{\alpha},\boldsymbol{\beta}))=H(r\boldsymbol{\alpha},r\boldsymbol{\beta})$ for $\sigma=\sigma_r\in\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $r\in\{1,\dots,N-1\}$ coprime with N, we get that $e^{2\pi i r\alpha_1},\dots,e^{2\pi i r\alpha_n}$ and $e^{2\pi i r\beta_1},\dots,e^{2\pi i r\beta_n}$ are intertwined on the unit circle. □

Assuming that $\alpha_n=0$, a solution of $\mathscr{H}(\boldsymbol{\alpha},\boldsymbol{\beta})$ is given by

$$ {}_nF_{n-1}([-\beta_1,\dots,-\beta_n],[1-\alpha_1,\dots,1-\alpha_{n-1}];x)=\sum_{k\geq 0}\frac{(-\beta_1)_k\cdots(-\beta_n)_k}{(1-\alpha_1)_k\cdots(1-\alpha_{n-1})_k k!}x^k \tag{33}$$

where $(x)_k=x(x+1)\cdots(x+k-1)$ is the usual Pochhammer symbol. Under the condition that none of the $\alpha_i-\beta_j$ belong to $\mathbb{Z}$, the series (33) is algebraic if and only if $\mathscr{H}(\boldsymbol{\alpha},\boldsymbol{\beta})$ has a full basis of algebraic solutions. Hence, the algebraicity/transcendence of (33) can be decided by using the Beukers-Heckman criterion.

Remark 4.11. Deciding the algebraicity of the solutions of Gauss hypergeometric equations is an old problem, solved by Schwarz [78] using geometric tools (Riemann mappings, Schwarzian derivatives and sphere tilings by spherical triangles) and by Landau [66, 67] and Errera [43] using arithmetic tools (Eisenstein's criterion for algebraic power series, and Dirichlet's theorem on prime numbers in arithmetic progressions).

Remark 4.12. For the case when $\alpha_i-\beta_j\in\mathbb{Z}$ for some $i,j\in\{1,\dots,n\}^2$ (*i.e.*, the case when $\mathscr{H}(\boldsymbol{\alpha},\boldsymbol{\beta})$ is reducible), we refer to Fürnsinn and Yurkevich paper [53].

Exercise 19 — Let F be a differential field extension of $\mathbb{Q}(x)$. Let f be an element of F algebraic over $\mathbb{Q}(x)$. Prove that f is solution of a nonzero $\mathscr{L}\in\mathbb{Q}(x)\langle\partial\rangle$ having a full basis of algebraic solutions.

5 Progresses toward Grothendieck's conjecture

Besides for order-1 equations (Honda, see Section 2.1) and for generalized hypergeometric equations (Beukers and Heckman, see Section 4), Grothendieck's conjecture has been proved in several particular cases.

On the one hand, for Picard-Fuchs differential equations (satisfied by periods of a family of smooth algebraic varieties), and more generally for certain direct factors, Grothendieck's conjecture was established by Katz [57]. As an application, Katz gave in [59, Theorem 5.5.3] a new proof of the aforementioned results of Beukers and Heckman [10] about the generalized hypergeometric equations. Katz [57, §1], and later André [5, §III], related the p-curvatures to the reduction modulo p of the *Kodaira-Spencer map*. (See also Foucault [49] and Foucault and Toffin [50] for explicit computations for families of curves of genus 2 and 3.) As explained in [5, p. 108], this approach has a potential of delivering effective versions of Grothendieck's conjecture, similar to effective versions of Chebotarev's density theorem [65, 79]: the hope is to obtain, for instance for any Picard-Fuchs operator $\mathscr{L}$, an integer $N(\mathscr{L})$ such that the fact that $\mathscr{L}$ has a full basis of algebraic solutions can be read on the p-curvatures of $\mathscr{L}$ for the primes $p < N(\mathscr{L})$.

On the other hand, an arithmetic approach to Grothendieck's conjecture was introduced by the Chudnovsky brothers [36] who proved Grothendieck's conjecture for any rank one linear homogeneous differential equation over an algebraic curve [36, Theorem 8.1] (the case of first order equations over $\mathbb{P}^1$ had been proved by Honda in [54, §1], see Theorem 2.5). The arithmetic approach was extended by André to the case when the differential Galois group has a solvable neutral component [5] (see also [3], [4, Chap. VIII], [12, Thm. 2.9] and [30, Thm. 3.5]).

Katz [58] proposed a conjectural description of the differential Galois group in terms of p-curvatures and he proved that his conjecture is equivalent to the initial conjecture by Grothendieck.

Using the language of schemes and sheaves, Grothendieck's conjecture can be formulated more generally for differential equations over any algebraic smooth curve defined over a number field. In [5, Remark 7.1.4], André noticed that, using Belyi maps, one can reduce the general case to that of the curve $X = \mathbb{P}^1 \backslash \{0, 1, \infty\}$. In our setting, this means that one can safely assume that the differential operator $\mathscr{L}$ has only singularities at 0, 1 and ∞. Under this additional assumption, Tang [86] proves that if *all*[3] the p-curvatures of $\mathscr{L}$ vanish, then $\mathscr{L}$ has a full basis of *rational* solutions. Although this latter result differs from Grothendieck's in the hypotheses (which are stronger) and the conclusion (which is also stronger), it is closely related.

We also point out the work of Bost in [12] giving an algebraicity criterion for leaves of algebraic foliations defined over number fields. For additional details, we refer to [30]. We mention the work of van der Put in [89] concerned with inhomogeneous equations of order 1. Other special cases of the conjecture have been proven recently, see [45, 81, 73]. Last but not least, an analogue of Grothendieck's conjecture for q-difference equations was conjectured by Bézivin [11, §5] and proved by Di Vizio in [38].

6 A formal parallel with Kronecker's theorem

It is instructive to observe that Grothendieck's conjecture appears to be, in some sense, a differential version of Kronecker's theorem we have already encountered earlier (see Theorem 2.6). Indeed, Kronecker's theorem can be reformulated as follows.

Theorem 6.1. *For a separable polynomial $L \in \mathbb{Q}[x]$, the following conditions are equivalent:*

(1) all the roots of L are in $\mathbb{Q}$;

(2) for almost all primes p, all the roots of L mod p are in $\mathbb{F}_p$;

[3] When $\mathscr{L}$ does not reduce properly at a prime p, the p-curvature of $\mathscr{L}_p$ is *a priori* not defined; however Tang gives an alternative definition of the vanishing of the p-curvature, see [86, Definition 2.1.7].

(3) for almost all primes p, we have $X^p \equiv X \pmod{L, p}$.

It is striking that the three conditions of Theorem 6.1 are formal analogues of the conditions of Conjecture 2.17, at least if we admit that algebraic solutions in the differential case correspond to rational solutions in the algebraic case. Besides, the fact that the condition $X^p \equiv X \pmod{L, p}$ translates to $\partial_x^p \equiv 0 \pmod{\mathscr{L}, p}$, *i.e.*, that the right-hand side shifts from X to 0, is explained by the fact that the classical Frobenius map behaves "multiplicatively" (it belongs naturally to some Galois group) while the p-curvature behaves "additively" (it belongs naturally to some Lie algebra).

In the classical setting, Kronecker's theorem is obtained as a corollary of Chebotarev's density theorem, which is itself proved by means of Artin's L-functions. Unfortunately, similar tools do not seem to be available so far in the differential context; developing them might then sound as an exciting project.

As mentioned above, Honda proved that the Grothendieck conjecture for first order differential equations is equivalent to Kronecker's theorem. In [36, §4], the Chudnovsky brothers gave an elementary (although "extravagant") proof of these equivalent statements; their approach is based on Hermite's explicit Hermite-Padé approximants to binomial functions. More precisely, they proved that if $y'(x) = \frac{x}{\alpha} y(x)$ has zero p-curvature for almost all primes p, then for all primes ideals $\mathfrak{P}$ of $\mathbb{Q}(\alpha)$ all the binomial coefficients $\binom{\alpha}{n}$ are $\mathfrak{P}$-integral for all n. From there, it is shown that Hermite-Padé approximants to $1, x^\alpha, \ldots, x^{(m-1)\alpha}$ at $x = 1$ with weights $(N, \ldots, N)$ are trivial for large m and N. This in turn implies that $1, x^\alpha, \ldots, x^{(m-1)\alpha}$ are linearly dependent over $\mathbb{Q}(x)$, that is x^α is an algebraic function, which is equivalent to $\alpha \in \mathbb{Q}$.

7 Solutions

Solution to Exercise 1 — Assume that $f(x)$ is D-finite. Then, it satisfies a linear differential equation of the form

$$\sum_{i=0}^{r} a_i(x) \delta^i(f(x)) = 0$$

where the $a_i(x) = \sum_{j=0}^{d} a_{ij} x^j$ are polynomials and where $\delta = xd/dx$. We have

$$\delta^i(f(x)) = \sum_{n \in \mathbb{Z}} n^i f_n x^n$$

so

$$x^j \delta^i(f(x)) = \sum_{n \in \mathbb{Z}} (n-j)^i f_{n-j} x^n$$

and, hence,

$$\sum_{i=0}^{r} a_i(x) \delta^i(f(x)) = \sum_{n \in \mathbb{Z}} \left(\sum_{i=0}^{r} \sum_{j=0}^{d} a_{ij} (n-j)^i f_{n-j} \right) x^n$$

It follows that

$$\forall n \in \mathbb{Z}, \sum_{i=0}^{r} \sum_{j=0}^{d} a_{ij}(n-j)^i f_{n-j} = 0,$$

i.e.,

$$\forall n \in \mathbb{Z}, \sum_{j=0}^{d} \left(\sum_{i=0}^{r} a_{ij}(n-j)^i \right) f_{n-j} = 0.$$

So, $(f_n)_{n\in\mathbb{Z}}$ is P-recursive.

Conversely, assume that $(f_n)_{n\in\mathbb{Z}}$ is P-recursive, then there exist finitely many polynomials $p_0(X), \ldots, p_d(X) \in \mathbb{Q}[X]$ with $p_d(X) \neq 0$ such that,

$$\forall n \in \mathbb{Z}, \sum_{j=0}^{d} p_j(n) f_{n-j} = 0.$$

We decompose the $p_j(X)$ in the basis $((X-j)^i)_{i\geq 0}$ of $\mathbb{Q}[X]$:

$$p_j(X) = \sum_{i=0}^{r} a_{ij}(X-j)^i.$$

The above recurrence relation becomes

$$\forall n \in \mathbb{Z}, \sum_{j=0}^{d} \left(\sum_{i=1}^{r} a_{ij}(n-j)^i \right) f_{n-j} = 0.$$

By going back up the chain of reasoning of the first part of this proof, we obtain that $f(x)$ is D-finite.

Solution to Exercise 2 —

1. We have

$$\sum_{k=0}^{\infty} \binom{np+i}{k} x^k = (1+x)^{np+i}(1+x)^{np+i} = ((1+x)^p)^n \, (1+x)^i$$
$$= (1+x^p)^n (1+x)^i = \sum_{m=0}^{\infty} \sum_{j=0}^{\infty} \binom{n}{m}\binom{i}{j} x^{mp+j}.$$

   Since any integer $k \in \mathbb{Z}_{\geq 0}$ has a unique decomposition of the form $k = mp + j$ with $m \in \mathbb{Z}_{\geq 0}$ and $j \in \{0, \ldots, p-1\}$, we get the desired result by equating the coefficients in the above equality.

2. Applying Lucas' Theorem, we get

$$\begin{aligned} f_p(x) &= \sum_{n=0}^{\infty} \binom{2n}{n}^t x^n = \sum_{i=0}^{p-1} \sum_{n=0}^{\infty} \binom{2np+2i}{np+i}^t x^{np+i} \\ &= \sum_{i=0}^{\frac{p-1}{2}} \sum_{n=0}^{\infty} \binom{2np+2i}{np+i}^t x^{np+i} + \sum_{i=\frac{p+1}{2}}^{p-1} \sum_{n=0}^{\infty} \binom{(2n+1)p+(2i-p)}{np+i}^t x^{np+i} \\ &= \sum_{i=0}^{\frac{p-1}{2}} \sum_{n=0}^{\infty} \binom{2n}{n}^t \binom{2i}{i}^t x^{np+i} + \sum_{i=\frac{p+1}{2}}^{p-1} \sum_{n=0}^{\infty} \binom{2n+1}{n}^t \binom{2i-p}{i}^t x^{np+i}. \end{aligned}$$

As $2i - p < i$, the very last term in the previous equality is equal to 0 and, hence,

$$f_p(x) = \sum_{i=0}^{\frac{p-1}{2}} \sum_{n=0}^{\infty} \binom{2n}{n}^t \binom{2i}{i}^t x^{np+i} = \left(\sum_{i=0}^{\frac{p-1}{2}} \binom{2i}{i}^t x^i \right) \left(\sum_{n=0}^{\infty} \binom{2n}{n}^t x^{np} \right) = \alpha_p f_p(x)^p.$$

3. a) Let ω be a root of $P_1(X)$. The set of roots of $F(X)$ is $\mathbb{F}_p^{\times}\omega$. In particular, $K = \mathbb{F}_p(x)(\omega)$ and we have $r = [K : \mathbb{F}_p(x)] = [\mathbb{F}_p(x)(\omega) : \mathbb{F}_p(x)] = \deg P_1(X)$. Moreover, for any $\zeta \in \mathbb{F}_p^{\times}$, the minimal polynomial of $\zeta\omega$ over $\mathbb{F}_p(x)$ is $P_1(\zeta^{-1}X)$; therefore any $P_i(X)$ is, up to a muliplicative constant in $\mathbb{F}_p^{\times}$, of the form $P_1(\zeta_i^{-1}X)$ for some $\zeta_i \in \mathbb{F}_p^{\times}$. In particular, any $P_i(X)$ has degree r.

   b) Since f_p^{-1} is a root of $F(X)$, it follows from the previous question that f_p^{-1} and, hence, f_p have degree r over $\mathbb{F}_p(x)$.

   c) To prove that $r \neq 1$, we argue by contradiction, assuming $r = 1$. Then $f_p \in \mathbb{F}_p(x)$. Consider $b, c \in \mathbb{F}_p[x]$ such that $c \neq 0$ and $f = \frac{b}{c}$. We have seen that $f_p(x) = \alpha_p f_p(x)^p$. Thus, $c^{p-1} = \alpha_p b^{p-1}$. Hence, $p-1$ divides the degree of α_p, this is a contradiction because the degree of α_p is equal to $(p-1)/2$.

   d) To prove that $r \neq 2$, we argue by contradiction, assuming $r = 2$. Then the degree of each $P_j(X)$ is 2. So

   $$P_j(X) = (X - \zeta_j\omega)(X - \xi_j\omega)$$

   where ω is a root of $F(X)$ in K and $\zeta_j \neq \xi_j \in \mathbb{F}_p^{\times}$. Equating the terms of degree 0 in the equality $P_j(X) = (X - \zeta_j\omega)(X - \xi_j\omega)$, we get $\omega^2 \in \mathbb{F}_p(x)$. Equating the coefficients of degree 0 in the equality $F(X) = \prod_{i=1}^{k} P_i(X)$, we get $\alpha_p = \omega^{p-1}$ (we have $\prod_{i=1}^{k} \zeta_j\xi_j = \prod_{\zeta\in\mathbb{F}_p^{\times}} \zeta = -1$). Therefore, $\alpha_p = (\omega^2)^{\frac{p-1}{2}} \in \mathbb{F}_p(x)^{\frac{p-1}{2}}$. It follows that $\alpha_p = (bx+a)^{\frac{p-1}{2}}$ for some $a, b \in \mathbb{F}_p$. Equating the coefficients of 1, x, and x^2, we get $1 = a^{(p-1)/2}$, $2^t = \frac{p-1}{2}a^{(p-1)/2-1}b$, $6^t = \frac{(p-1)(p-3)}{8}a^{(p-1)/2-2}b^2$. So, $b/a = -2^{t+1}$ and $(b/a)^2 = 2^3 6^t 3^{-1}$ so $2^{2t+2} = 2^3 6^t 3^{-1}$, *i.e.*, $3^{t-1} = 2^{t-1}$ in $\mathbb{F}_p$. Since $p > 3^{t-1}$, this is a contradiction.

   e) Follows from the fact that $p - 1 = \deg F(X) = \sum_{i=1}^{k} \deg P_i(X) = rk$.

4. Let $p_1, p_2, \ldots, p_t$ be the distinct odd primes which are not greater than A. By the Chinese Remainder Theorem, there exists $x \in \mathbb{Z}$ such that

$$x \equiv 2 \pmod{p_1 p_2 \ldots p_t}$$

$$x \equiv 3 \pmod 4.$$

Any element of $x + 4p_1p_2 \dots p_t\mathbb{Z}$ satisfies the same congruences. But, by Dirichlet's Theorem on primes in arithmetic progression, we can find infinitely many primes p in $x + \mathbb{Z}4p_1p_2 \dots p_t$. For any such prime, we have $p - 1 \equiv 1 \pmod{p_1p_2 \dots p_t}$, so none of $p_1, \dots, p_t$ is a divisor of $p - 1$, and we have $p - 1 \equiv 2 \pmod 4$, so 4 does not divide $p - 1$. Therefore, if $m \in \mathbb{Z}_{\geq 1}$ divides $p - 1$, then $m = 1, 2$ or $m > A$.

Solution to Exercise 3 —

1. The series
$$f(x) = \sum_{n=0}^{\infty} \binom{2n}{n} x^n = (1 - 4x)^{-1/2} \in \mathbb{Z}[[x]]$$
is algebraic but $f \odot f$ is transcendental by Exercise 2.
2. According to Exercise 1, it is sufficient to prove that the set of P-recursive sequence is stable by product.

Solution to Exercise 4 — Consider the Artin–Schreier equation $Y^p - Y = x^{-1}$ in $\mathbb{F}_p(x)[Y]$. Assume that it has a solution $f(x) \in \bigcup_{d \geq 1} \overline{\mathbb{F}_p}((x^{1/d}))$. Taking valuations in the equality $f(x)^p - f(x) = x^{-1}$, we see that the valuation of $f(x)$ is $-1/p$ and that its term of lower valuation is $x^{-1/p}$. Set $f(x) = x^{-1/p} + f_2(x)$. Then, $f_2(x)$ is solution of $Y^p - Y = x^{-1/p}$. Taking valuations in $f_2(x)^p - f_1(x) = x^{-1/p}$, we see that the valuation of $f_2(x)$ is $-1/p^2$ and that its term of lower valuation is x^{-1/p^2}. Iterating this argument, we see that that arbitrary high power of p appear in the denominators of the elements of the support of $f(x)$, whence a contradiction.

Solution to Exercise 5 —

1. If $f(x) \in 1 + x\mathbb{Z}_p[[x]]$, then $f(x)^p \equiv f(x^p) \pmod p$. Both series belong to $1 + x\mathbb{Z}_p[[x]]$, and $f(x^p) \in 1 + x\mathbb{Z}_p[[x]]$ is invertible, whence (ii).
2. a) The coefficient of x^n in the left-hand side is the same as in
$$\left(\sum_{i \leq n} a_i x^i\right)^p.$$
But, we have
$$\begin{aligned}\left(\sum_{i \leq n} a_i x^i\right)^p &= \sum_{k=0}^{p} \binom{p}{k} \left(\sum_{i \leq n-1} a_i x^i\right)^k (a_n x^n)^{p-k} \\ &= \left(\sum_{i \leq n-1} a_i x^i\right)^p + p \left(\sum_{i \leq n-1} a_i x^i\right) a_n x^n + \text{terms of degree} > n \\ &= \sum_{i \leq n} a_i^p x^{ip} + p a_n x^n + \text{terms with coefficients in } p\mathbb{Z}_p + \text{terms of degree} > n.\end{aligned}$$

Hence, the coefficient of x^n in the left-hand side of (5) is

$$a_{n/p}^p + pa_n + \text{terms in } p\mathbb{Z}_p$$

with $a_{n/p} = 0$ when n is not divisible by p.

b) The coefficient of x^n in the right-hand side of (5) is the same as in

$$\left(\sum_{i \le n/p} a_i x^{pi}\right)\left(1 + p\sum_{j \le n} b_j x^j\right),$$

and, hence, is equal to

$$a_{n/p} + \text{terms in } p\mathbb{Z}_p.$$

c) Since $n/p < n$, we have $a_{n/p} \in \mathbb{Z}_p$ by induction and, hence, $a_{n/p}^p \equiv a_{n/p} \pmod{p\mathbb{Z}_p}$. Comparing the above two formulas for the coefficient of x^n in (5), we get $pa_n \in p\mathbb{Z}_p$ and, hence, $a_n \in \mathbb{Z}_p$.

3. a) Direct application of Dieudonné-Dwork Lemma.

b) According to Dieudonné-Dwork Lemma, the denominators all the c_n are p-adic integers if and only if

$$\arctan(x^p) - p \cdot \arctan(x) \in p\mathbb{Z}_p[[x]].$$

We have:

$$\arctan(x^p) - p \cdot \arctan(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} x^{(2n+1)p} - p \cdot \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} x^{(2n+1)}. \qquad (6)$$

Clearly, when $2n+1$ is coprime with p, the coefficient $p \cdot \frac{(-1)^n}{2n+1}$ is divisible by p. Therefore, we can only retain in the second sum of equation (6) the terms for which $2n \equiv -1 \pmod p$, *i.e.*, $2n = p - 1 + 2\ell p$ with $\ell \in \mathbb{Z}_{\ge 0}$. We thus get:

$$\begin{aligned}\arctan(x^p) - p \cdot \arctan(x) &\equiv \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} x^{(2n+1)p} - \sum_{\ell=0}^{\infty} \frac{(-1)^{\ell - \frac{p-1}{2}}}{2\ell+1} x^{(2\ell+1)p} \\ &= \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} \cdot \left(1 - (-1)^{\frac{p-1}{2}}\right) \cdot x^{(2n+1)p} \pmod{p\mathbb{Z}_p[[x]]},\end{aligned}$$

hence $\arctan(x^p) - p \cdot \arctan(x)$ is divisible by p when $p \equiv 1 \bmod 4$ and is not otherwise. In conclusion, the denominators of the c_n's are all p-adic integers if and only if $p \equiv 1 \bmod 4$.

Solution to Exercise 6 —

1. Modulo $p = 2$, the rational function $b(x) = 1/(x^2+1)$ writes $1/(x+1)^2$; thus it has a pole of order 2 and hence the differential equation (12) has no nonzero rational solutions by Proposition 2.3.

2. For $p \neq 2$, the partial fraction decomposition of $b(x)$ reads

$$b(x) = \frac{i}{2} \cdot \left(\frac{1}{x+i} - \frac{1}{x-i} \right)$$

where i denotes a square root of -1 in $\overline{\mathbb{F}_p}$. We now need to distinguish between two cases depending on the congruence class of p modulo 4. Indeed, we recall that $a \in \mathbb{Z}$ is a quadratic residue modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$; applying this to $a = -1$, we get that -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$. So, when $p \equiv 1 \pmod 4$, we have $i \in \mathbb{F}_p$ and so the residues belong to $\mathbb{F}_p$ as well. In this case, the equation (12) has then a nonzero rational solution, namely

$$y(x) = \left(\frac{x+i}{x-i} \right)^{i/2},$$

where the exponent $i/2$ is a lift in $\mathbb{Z}$ of $i/2 \in \mathbb{F}_p$. On the contrary, when $p \equiv 3 \pmod 4$, we have that -1 is not a square in $\mathbb{F}_p$, showing that the residues are not in $\mathbb{F}_p$ either. Therefore, in this case, the equation (12) has no nonzero rational solution.

Solution to Exercise 7 — It is clear that $\mathbb{F}_p(x^p)$ is included in the field of differential constants of $\mathbb{F}_p(x)$. It remains to prove the converse inclusion. We recall that $\mathbb{F}_p(x)$ is an $\mathbb{F}_p(x^p)$-vector space of dimension p, a basis being given by $1, x, x^2, \ldots, x^{p-1}$. Consider an element f of the field of differential constants of $\mathbb{F}_p(x)$. There exist $\lambda_0, \cdots, \lambda_{p-1} \in \mathbb{F}_p(x^p)$ such that $f = \sum_{i=0}^{p-1} \lambda_i x^i$. We have $0 = f' = \sum_{i=0}^{p-1} \lambda_i i x^{i-1}$ so $\lambda_1 = \cdots = \lambda_{p-1} = 0$ and, hence, f belongs to $\mathbb{F}_p(x^p)$.

Solution to Exercise 8 — We have, for all $j \in \mathbb{Z}_{\geq 0}$, $\partial_x^j x = x\partial_x^j + j\partial_x^{j-1}$. For $j = p$, we get $\partial_x^p x = x\partial_x^p$, so ∂_x^p commutes with x. It follows that $\partial_x^p \in Z$. We also have $\partial_x x^p = x^p \partial_x + p x^{p-1} = x^p \partial_x$, so x^p commutes with ∂_x. It follows that $x^p \in Z$. So, $\mathbb{F}_p(x^p)\langle \partial_x^p \rangle \subset Z$.

Conversely, consider $\mathscr{M} \in Z$. It has a unique decomposition of the form

$$\mathscr{M} = \sum_{0 \leq i,j \leq p-1} m_{i,j} x^i \partial_x^j$$

with $m_{i,j} \in \mathbb{F}_p(x^p)\langle \partial_x^p \rangle$. We have

$$0 = \mathscr{M}x - x\mathscr{M} = \sum_{0 \leq i,j \leq p-1} m_{i,j} x^i j \partial_x^{j-1}$$

so $m_{i,j} = 0$ for all $j \neq 0$ and, hence, $\mathscr{M} = \sum_{0 \leq i \leq p-1} m_{i,0} x^i$. Moreover, we have

$$0 = \mathscr{M}\partial_x - \partial_x \mathscr{M} = \sum_{0 \leq i,j \leq p-1} m_{i,0} i x^{i-1},$$

so $m_{i,0} = 0$ for $i \neq 0$ and, hence, $\mathscr{M} = m_{0,0} \in \mathbb{F}_p(x^p)\langle \partial_x^p \rangle$.

Solution to Exercise 9 —

1. Let us first note that, for any $f_1, f_2 \in \mathbb{F}_p(x)$,

$$\Delta(f_1 f_2) = \Delta_1(f_1) f_2 + f_1 \Delta_2(f_2)$$

where

$$\begin{array}{rcl} \Delta : \mathbb{F}_p(x) & \to & \mathbb{F}_p(x) \\ f & \mapsto & f' + (b_1(x) + b_2(x)) f \end{array}$$

and, for $i \in \{1, 2\}$,

$$\begin{array}{rcl} \Delta_i : \mathbb{F}_p(x) & \to & \mathbb{F}_p(x) \\ f & \mapsto & f' + b_i(x) f. \end{array}$$

Iterating this equation, we get, for all $k \in \mathbb{Z}_{\geq 0}$,

$$\Delta^k(f_1 f_2) = \sum_{i=0}^{k} \binom{k}{i} \Delta_1^i(f_1) \Delta_2^{k-i}(f_2).$$

For $k = p$, we get

$$\Delta^p(f_1 f_2) = \Delta_1^p(f_1) f_2 + f_1 \Delta_2^p(f_2).$$

Specializing this equality to $f_1 = f_2 = 1$, we get

$$\Delta^p = \Delta_1^p + \Delta_2^p,$$

and this proves our claim.

2. Using the previous question, we see that it is sufficient to prove the expected formula for the p-curvature in the case $b = cx^i$ with $c \in \mathbb{F}_p(x^p)$ and $i \in \{0, \dots, p-1\}$ because any element of $\mathbb{F}_p(x)$ is a sum of terms of this form.

3. We have

$$\left(\partial_x + cx^i\right)^p = c^p x^{ip} + c^{p-1} E_{p-1} + \cdots + cE_1 + \partial_x^p$$

where the $E_j \in \mathbb{F}_p(x)\langle \partial_x \rangle$ are differential operators not depending on c; in particular, $E_1 = \sum_{k=0}^{p-1} \partial_x^{p-1-k} x^i \partial_x^k$. Therefore, denoting by $\Delta_{cx^i}^p$ the p-curvature of $y' + cx^i$, we have

$$\Delta_{cx^i}^p(1) = c^p x^{ip} + c^{p-1} e_{p-1} + \cdots + ce_1$$

where the $e_j = E_j(1)$ are elements of $\mathbb{F}_p(x)$ not depending on c.

4. As the map $c \mapsto \Delta_{cx^i}^p(1)$ is additive, we have $e_{p-1} = \cdots = e_2 = 0$. Moreover, $e_1 = E_1(1) = \partial_x^{p-1}(x^i) = 0$ if $i < p-1$, $(p-1)! = -1$ (by Wilson theorem) if $i = p-1$.

5. In conclusion,

$$\Delta_{cx^i}^p(1) = c^p x^{ip} + \partial_x^{p-1}(cx^i) = \begin{cases} c^p x^{ip} & \text{if } i \in \{0, \dots, p-2\} \\ c^p x^{ip} - c & \text{if } i = p-1 \end{cases}$$

Solution to Exercise 10 — Consider a rational function $b(x) \in \mathbb{F}_p(x)$ and write its partial fraction decomposition

$$b(x) = P(x) + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\beta_{i,j}}{(x-b_i)^j}$$

where $P(x)$ is a polynomial, the b_i's are pairwise distinct elements of $\overline{\mathbb{F}_p}$ and $\beta_{i,j} \in \overline{\mathbb{F}_p}$ with $\beta_{i,r_i} \neq 0$. Each b_i is a pole of $b(x)$ of multiplicity r_i and residue $\beta_{i,1}$. Moreover, $b(x)$ has an extra pole at infinity when the degree of $P(x)$ is positive. A direct computation now gives:

$$\begin{aligned} b_p(x) &= P^{(p-1)}(x) + P(x)^p \\ &\quad + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{(-j)(-j-1)\cdots(-j-(p-2))\beta_{i,j}}{(x-b_i)^{j+p-1}} + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\beta_{i,j}^p}{(x-b_i)^{pj}} \\ &= P^{(p-1)}(x) + P(x)^p - \sum_{i=1}^{m} \sum_{\substack{1 \leq j \leq r_i \\ j \equiv 1 \bmod p}} \frac{\beta_{i,j}}{(x-b_i)^{j+p-1}} + \sum_{i=1}^{m} \sum_{j=1}^{r_i} \frac{\beta_{i,j}^p}{(x-b_i)^{pj}} \end{aligned} \tag{21}$$

and we see that the latter is zero if and only if $P(x)$ vanishes and, for all $i \in \{1, \ldots, m\}$, we have $r_i = 1$ and $\beta_{i,1}^p = \beta_{i,1}$, *i.e.*, $\beta_{i,1} \in \mathbb{F}_p$. After Proposition 2.11, we then recover by different means the result of Proposition 2.3.

Solution to Exercise 11 —

1. a) Let $\mathcal{F}$ be a K-linearly dependent family of elements of $Y' = AY$. Consider $F_1, \ldots, F_r \in \mathcal{F}$ such that $(F_1, \ldots, F_r)$ is K-linearly dependent but any strict subfamily is K-linearly independent (i.e., a family of K-linearly dependent elements of $\mathcal{F}$ with minimal cardinality with respect to this property). Then there is a (unique) relation $F_1 = \sum_{i=2}^{r} a_i F_i$ with all $a_i \in K$. Now

   $$0 = F_1' - AF_1 = \sum_{i=2}^{r} a_i' F_i + \sum_{i=2}^{r} a_i (F_i' - AF_i) = \sum_{i=2}^{r} a_i' F_i.$$

   Thus all $a_i' = 0$ and so all $a_i \in C$.

   b) Immediate consequence of the previous question.
2. Apply the previous question to the differential system $Y' = AY$ associated to the differential equation and use the fact that the map

   $$f(x) \mapsto (f(x), f'(x), \ldots, f^{(n-1)}(x))$$

   induces an C-linear isomorphism from the C-vector space of solutions of the differential equation (see formula (25)) in K to the C-vector space of solutions of $Y' = AY$ in K^n.

Solution to Exercise 12 — Let us first note that, for any $u \in \mathbb{F}_p(x)$, there exist $a \in \mathbb{F}_p[x]$ and $b \in \mathbb{F}_p[x^p] \setminus \{0\}$ such that $u = a/b$. Indeed, there exist $v \in \mathbb{F}_p[x]$ and $w \in \mathbb{F}_p[x] \setminus \{0\}$ such that $u = v/w$ and we have $u = a/b$ with $a = vw^{p-1} \in \mathbb{F}_p[x]$ and $b = w^p \in \mathbb{F}_p[x^p] \setminus \{0\}$.

As the elements of $\mathbb{F}_p[x^p]$ are differential constants, we see that if $u \in \mathbb{F}_p(x)$ is a solution of $\mathscr{M} \in \mathbb{F}_p(x)\langle\partial_x\rangle$, then there exists $b \in \mathbb{F}_p[x^p] \setminus \{0\}$ such that $bu \in \mathbb{F}_p[x]$ is again a solution of $\mathscr{M}$. This implies immediately that if $\mathscr{M}$ has a full basis of rational solutions then it has a full basis of polynomial solutions. The converse implication is trivial.

Solution to Exercise 13 —

Solution to Exercise 14 —

1. An easy modification of the proof of Theorem 2.19 shows that the kernel of the p-curvature coincides with the $\mathbb{F}_p(x)$-vector space generated by the rational solutions (*i.e.*, in $\mathbb{F}_p(x)^n$) of $Y' + B(x)Y = 0$.
2. As the solutions of the latter system in $\mathbb{F}_p(x)^n$ are linearly independent over $\mathbb{F}_p(x)$ if and only if they are linearly independent over $\mathbb{F}_p(x^p)$ (Wronskian Lemma, Exercise 11), this implies that the dimension of the $\mathbb{F}_p(x^p)$-vector space of rational solutions of $Y' + B(x)Y = 0$ or, equivalently, of (24) is equal to $\dim_{\mathbb{F}_p(x)} \ker \Delta$.

Solution to Exercise 15 — To prove the formula $x^k\partial_x^k = \delta(\delta-1)\cdots(\delta-k+1)$, we argue by induction on $k \in \mathbb{Z}_{\geq 1}$. The case $k = 1$ is obvious. Assume that the formula is true for some $k \in \mathbb{Z}_{\geq 1}$. Note that we have

$$\delta\partial_x = \partial_x\delta - \partial_x = \partial_x(\delta - 1)$$

so, for all $j \in \mathbb{Z}_{\geq 1}$,

$$(\delta - j)\partial_x = \partial_x(\delta - j - 1).$$

It follows that

$$\begin{aligned} x^{k+1}\partial_x^{k+1} &= x(x^k\partial_x^k)\partial_x = x\delta(\delta-1)\cdots(\delta-k+1)\partial_x \\ &\qquad\qquad = x\partial_x(\delta-1)(\delta-2)\cdots(\delta-k) = \delta(\delta-1)(\delta-2)\cdots(\delta-(k+1)+1) \end{aligned}$$

and this concludes the induction.

The formula we have just proved is of the form:

$$\forall k \in \mathbb{Z}_{\geq 1},\quad x^k\partial_x^k \in \delta^k + \mathrm{Span}_{\mathbb{C}}(\delta^{k-1},\dots,\delta),$$

therefore:

$$\forall k \in \mathbb{Z}_{\geq 1},\quad \delta^k \in x^k\partial_x^k + \mathrm{Span}_{\mathbb{C}}(x^{k-1}\partial_x^{k-1},\dots,x\partial_x).$$

Assume that $\mathscr{L}$ is regular singular. Without loss of generality, we can assume that $a_n = 1$. Set $\widetilde{a}_i = x^{n-i}a_i$. Then,

$$a_i\partial_x^i = x^{-n}\widetilde{a}_i x^i\partial_x^i = x^{-n}\widetilde{a}_i\delta(\delta-1)\cdots(\delta-i+1).$$

As $\mathscr{L}$ is regular singular, the $\widetilde{a}_i$ belong to $C[[x]]$ and it follows clearly that $\mathscr{L} = x^{-n}\sum_{i=0}^n b_i(x)\delta^i$, for some $b_i \in C[[x]]$, whence the direct implication in Proposition 3.4. We leave the converse implication to the reader.

Solution to Exercise 16 —

1. With the notations of the solution of Exercise 15, we have $\mathscr{L} = \sum_{i=1}^{n} \widetilde{a}_i \delta(\delta-1)\cdots(\delta - i+1)$, so the indicial polynomial at 0 of $\mathscr{L}$ is given by

   $$X(X-1)\cdots(X-n+1) + \widetilde{a}_1(0)X(X-1)\cdots(X-n+2) + \cdots + \widetilde{a}_{n-1}(0)X + \widetilde{a}_n(0),$$

   which is exactly the expected formula.
2. Direct consequence of the previous question as $\widetilde{c}_{n-1} = \cdots = \widetilde{c}_0 = 0$ in this case.

Solution to Exercise 17 — We have

$$\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (1-x)\delta^n + (-\sum_{i=1}^{n} \alpha_i + x \sum_{i=1}^{n} \beta_i)\delta^{n-1} + \star\delta^{n-2} + \cdots + \star\delta + \star$$

where the symbols $\star$ stand for unspecified polynomials. Using the fact that $\delta^k \in x^k \partial_x^k + \mathrm{Span}_{\mathbb{C}}(x^{k-1}\partial_x^{k-1}, \ldots, x\partial_x)$ (see Exercise 15), we see that

$$\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = (1-x)x^n\partial_x^n + (1-x)\lambda x^{n-1}\partial_x^{n-1} + (-\sum_{i=1}^{n} \alpha_i + x\sum_{i=1}^{n} \beta_i)x^{n-1}\partial_x^{n-1} \\ + \diamond\partial_x^{n-2} + \cdots + \diamond\partial_x + \diamond$$

for some $\lambda \in \mathbb{Q}$ and where the symbols $\diamond$ stand for unspecified polynomials. Therefore

$$\begin{aligned} \frac{1}{(1-x)x^n}\mathscr{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{i=0}^{n} a_i \partial_x^i \\ &= \partial_x^n + \frac{\lambda}{x}\partial_x^{n-1} + \frac{(-\sum_{i=1}^{n}\alpha_i + x\sum_{i=1}^{n}\beta_i)}{(1-x)x}\partial_x^{n-1} \\ &\quad + \frac{\diamond}{(1-x)x^n}\partial_x^{n-2} + \cdots + \frac{\diamond}{(1-x)x^n}\partial_x + \frac{\diamond}{(1-x)x^n}. \end{aligned}$$

Now, using Exercise 16, we see that the indicial polynomial at 1 is

$$X(X-1)\cdots(X-n+1) + \widetilde{c}_{n-1}X(X-1)\cdots(X-n+2) + \cdots + \widetilde{c}_1 X + \widetilde{c}_0. \tag{31}$$

where $\widetilde{c}_i = \lim_{z\to 0}(z-1)^{n-i}a_i(z)$ for $i \in \{1, \ldots, n\}$. We have $\widetilde{c}_n = 1$, $\widetilde{c}_{n-1} = -\sum_{i=1}^{n}\alpha_i + \sum_{i=1}^{n}\beta_i - n$ and $\widetilde{c}_{n-2} = \cdots = \widetilde{c}_0 = 0$. So, (31) reduces to

$$X(X-1)\cdots(X-n+1) + \left(-\sum_{i=1}^{n}\alpha_i + \sum_{i=1}^{n}\beta_i\right)X(X-1)\cdots(X-n+2),$$

i.e., to

$$X(X-1)\cdots(X-n+2)\left(X-n+1-\sum_{i=1}^{n}\alpha_i + \sum_{i=1}^{n}\beta_i\right).$$

Solution to Exercise 18 —

1. Assume on the contrary that G is reducible. Then, it leaves a line V invariant. This line is generated by a common eigenvector of M_0, M_1 and M_∞. Let λ_0, λ_1 and λ_∞ be the respective eigenvalues. Since $M_0 M_1 M_\infty = I_2$, we have $\lambda_0\lambda_1\lambda_\infty = 1$. But, using the facts that $\lambda_0 \in \{1, e^{-2\pi i\gamma}\}$, $\lambda_1 \in \{1, e^{2\pi i(\gamma-\alpha-\beta)}\}$ and $\lambda_\infty \in \{e^{2\pi i\alpha}, e^{2\pi i\beta}\}$ and the hypotheses relative to α, β, γ, it easily seen that $\lambda_0\lambda_1\lambda_\infty \neq 1$, whence a contradiction. Note that this implies in particular that $M_1 \neq I_2$ because otherwise G would be generated by M_0 and, hence, would be reducible.
2. The $\mathbb{C}$-vector space $W = \ker(M_0^{-1} - M_\infty)$ has dimension 1 because $M_0^{-1} - M_\infty = (M_1 - I_n)M_\infty$ so $\dim_{\mathbb{C}} W = \dim_{\mathbb{C}}(M_1 - I_n)$ which is equal to 1 because 1 is an eigenvalue of M_1 and $M_1 \neq I_2$.
3. The $\mathbb{C}$-vector spaces W and $M_0^{-1}W$ are in direct sum because otherwise these lines would be equal, so W would be left invariant by M_0 and, hence, by M_∞ because M_∞ acts as M_0^{-1} on W; since G is generated by M_0 and M_∞, this would contradict the irreducibility of G.
4. Let e be nonzero element of W, then $(e, M_0 e = M_\infty^{-1} e)$ is a basis of $\mathrm{M}_{2,1}(\mathbb{C})$ and the matrices of M_0 and M_∞^{-1} seen as $\mathbb{C}$-linear automorphisms of $\mathrm{M}_{2,1}(\mathbb{C})$ with respect to this basis are given by the companion matrices mentioned in the statement of the exercise.

Solution to Exercise 19 — Hint. Use a determinant.

References

[1] B. Adamczewski and T. Rivoal. Exceptional values of E-functions at algebraic points. *Bull. Lond. Math. Soc.*, 50(4):697–708, 2018.

[2] G. Almkvist and D. Zeilberger. The method of differentiating under the integral sign. *J. Symbolic Comput.*, 10(6):571–591, 1990.

[3] Y. André. Quatre descriptions des groupes de Galois différentiels. In *Séminaire d'algèbre Paul Dubreil et Marie-Paule Malliavin (Paris, 1986)*, volume 1296 of *Lecture Notes in Math.*, pages 28–41. Springer, Berlin, 1987.

[4] Y. André. *G-functions and geometry*. Aspects of Mathematics, E13. Friedr. Vieweg & Sohn, Braunschweig, 1989.

[5] Y. André. Sur la conjecture des p-courbures de Grothendieck-Katz et un problème de Dwork. In *Geometric aspects of Dwork theory. Vol. I, II*, pages 55–112. Walter de Gruyter, Berlin, 2004.

[6] V. G. Berkovich. *Spectral theory and analytic geometry over non-Archimedean fields*, volume 33 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1990.

[7] E. R. Berlekamp. Factoring polynomials over finite fields. *Bell System Tech. J.*, 46:1853–1859, 1967.

[8] O. Bernardi, M. Bousquet-Mélou, and K. Raschel. Counting quadrant walks via Tutte's invariant method. *Comb. Theory*, 1:Paper No. 3, 77, 2021.

[9] M. Bertola, B. Dubrovin, and D. Yang. Simple Lie algebras and topological ODEs. *Int. Math. Res. Not. IMRN*, (5):1368–1410, 2018.

[10] F. Beukers and G. Heckman. Monodromy for the hypergeometric function ${}_nF_{n-1}$. *Invent. Math.*, 95(2):325–354, 1989.

[11] J.-P. Bézivin. Les suites q-récurrentes linéaires. *Compositio Math.*, 80(3):285–307, 1991.

[12] J.-B. Bost. Algebraic leaves of algebraic foliations over number fields. *Publ. Math. Inst. Hautes Études Sci.*, (93):161–221, 2001.

[13] A. Bostan. Computer algebra in the service of enumerative combinatorics. In *ISSAC '21—Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation*, pages 1–8. ACM, New York, [2021] ©2021.

[14] A. Bostan, X. Caruso, and J. Roques. Algebraic solutions of linear differential equations: an arithmetic approach. To appear in *Bulletin of the AMS*, 2024. arXiv:2304.05061.

[15] A. Bostan, X. Caruso, and E. Schost. A fast algorithm for computing the characteristic polynomial of the p-curvature. In *ISSAC'14—Proceedings of the 2014 ACM International Symposium on Symbolic and Algebraic Computation*, pages 59–66. ACM, New York, 2014.

[16] A. Bostan, X. Caruso, and E. Schost. A fast algorithm for computing the p-curvature. In *ISSAC'15—Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation*, pages 69–76. ACM, New York, 2015.

[17] A. Bostan, X. Caruso, and E. Schost. Computation of the similarity class of the p-curvature. In *ISSAC'16—Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, pages 111–118. ACM, New York, 2016.

[18] A. Bostan, F. Chyzak, F. Ollivier, B. Salvy, E. Schost, and A. Sedoglavic. Fast computation of power series solutions of systems of differential equations. In *18th ACM-SIAM Symposium on Discrete Algorithms*, pages 1012–1021. ACM, New Orleans, 2007.

[19] A. Bostan, F. Chyzak, M. van Hoeij, M. Kauers, and L. Pech. Hypergeometric expressions for generating functions of walks with small steps in the quarter plane. *European J. Combin.*, 61:242–275, 2017.

[20] A. Bostan and M. Kauers. The complete generating function for Gessel walks is algebraic. *Proc. Amer. Math. Soc.*, 138(9):3063–3078, 2010. With an appendix by Mark van Hoeij.

[21] A. Bostan, I. Kurkova, and K. Raschel. A human proof of Gessel's lattice path conjecture. *Trans. Amer. Math. Soc.*, 369(2):1365–1393, 2017.

[22] A. Bostan, T. Rivoal, and B. Salvy. Minimization of differential equations and algebraic values of E-functions. *Math. Comp.*, 93(347):1427–1472, 2024.

[23] A. Bostan, B. Salvy, and M. Singer. On deciding transcendence of power series. In preparation, 2023.

[24] A. Bostan and E. Schost. Fast algorithms for differential equations in positive characteristic. In *ISSAC 2009—Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, pages 47–54. ACM, New York, 2009.

[25] A. Bostan and S. Yurkevich. On a class of hypergeometric diagonals. *Proc. Amer. Math. Soc.*, 150(3):1071–1087, 2022.

[26] M. Bousquet-Mélou. Rational and algebraic series in combinatorial enumeration. In *International Congress of Mathematicians. Vol. III*, pages 789–826. Eur. Math. Soc., Zürich, 2006.

[27] M. Bousquet-Mélou. An elementary solution of Gessel's walks in the quadrant. *Adv. Math.*, 303:1171–1189, 2016.

[28] M. Bousquet-Mélou and M. Mishna. Walks with small steps in the quarter plane. In *Algorithmic probability and combinatorics*, volume 520 of *Contemp. Math.*, pages 1–39. Amer. Math. Soc., Providence, RI, 2010.

[29] T. Budd. Winding of simple walks on the square lattice. *J. Combin. Theory Ser. A*, 172:105191, 59, 2020.

[30] A. Chambert-Loir. Théorèmes d'algébricité en géométrie diophantienne (d'après J.-B. Bost, Y. André, D. & G. Chudnovsky). Number 282, Exp. No. 886, viii, pages 175–209. 2002. Séminaire Bourbaki, Vol. 2000/2001.

[31] G. Christol. Solutions algébriques des équations différentielles p-adiques. In *Seminar on number theory, Paris 1981–82 (Paris, 1981/1982)*, volume 38 of *Progr. Math.*, pages 51–58. Birkhäuser Boston, Boston, MA, 1983.

[32] G. Christol. Fonctions hypergéométriques bornées. *Groupe de travail d'analyse ultramétrique*, 14, 1986-1987. Talk:8.

[33] G. Christol. Diagonales de fractions rationnelles. In *Séminaire de Théorie des Nombres, Paris 1986–87*, volume 75 of *Progr. Math.*, pages 65–90. Birkhäuser Boston, Boston, MA, 1988.

[34] G. Christol. Globally bounded solutions of differential equations. In *Analytic number theory (Tokyo, 1988)*, volume 1434 of *Lecture Notes in Math.*, pages 45–64. Springer, Berlin, 1990.

[35] G. Christol and B. Dwork. Modules différentiels sur des couronnes. *Ann. Inst. Fourier (Grenoble)*, 44(3):663–701, 1994.

[36] D. V. Chudnovsky and G. V. Chudnovsky. Applications of Padé approximations to the Grothendieck conjecture on linear differential equations. In *Number theory (New York, 1983–84)*, volume 1135 of *Lecture Notes in Math.*, pages 52–100. Springer, Berlin, 1985.

[37] O. Cormier, M. F. Singer, B. M. Trager, and F. Ulmer. Linear differential operators for polynomial equations. *J. Symbolic Comput.*, 34(5):355–398, 2002.

[38] L. Di Vizio. Arithmetic theory of q-difference equations: the q-analogue of Grothendieck-Katz's conjecture on p-curvatures. *Invent. Math.*, 150(3), 2002.

[39] T. Dreyfus, C. Hardouin, J. Roques, and M. F. Singer. On the nature of the generating series of walks in the quarter plane. *Invent. Math.*, 213(1):139–203, 2018.

[40] R. Duan, H. Wu, and R. Zhou. Faster matrix multiplication via asymmetric hashing. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 2129–2138, Los Alamitos, CA, USA, nov 2023. IEEE Computer Society.

[41] B. Dubrovin, D. Yang, and D. Zagier. Geometry and arithmetic of integrable hierarchies of KdV type. I. Integrality. *Adv. Math.*, 433:Paper No. 109311, 73, 2023.

[42] B. Dwork. Differential operators with nilpotent p-curvature. *Amer. J. Math.*, 112(5):749–786, 1990.

[43] A. Errera. Zahlentheoretische Lösung einer functionentheoretischen Frage. *Rend. Circ. Mat. Palermo*, 35:107–144, 1913.

[44] L. Euler. Specimen de constructione aequationum differentialium sine indeterminatarum separatione. *Commentarii academiae scientiarum Petropolitanae*, 6:168–174, 1733.

[45] B. Farb and M. Kisin. Rigidity, locally symmetric varieties, and the Grothendieck-Katz conjecture. *Int. Math. Res. Not. IMRN*, (22):4159–4167, 2009.

[46] G. Fayolle, R. Iasnogorodski, and V. Malyshev. *Random walks in the quarter-plane*, volume 40 of *Applications of Mathematics (New York)*. Springer-Verlag, Berlin, 1999. Algebraic methods, boundary value problems and applications.

[47] P. Flajolet. Analytic models and ambiguity of context-free languages. *Theoret. Comput. Sci.*, 49(2-3):283–309, 1987. Twelfth international colloquium on automata, languages and programming (Nafplion, 1985).

[48] P. Flajolet and R. Sedgewick. *Analytic combinatorics*. Cambridge University Press, Cambridge, 2009.

[49] F. Foucault. Équations de Picard-Fuchs et invariants des courbes de genre 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 314(8):617–619, 1992.

[50] F. Foucault and P. Toffin. Courbes hyperelliptiques de genre trois et application de Kodaira-Spencer. *C. R. Math. Acad. Sci. Paris*, 345(12):685–687, 2007.

[51] H. Furstenberg. Algebraic functions over finite fields. *J. Algebra*, 7:271–277, 1967.

[52] F. Fürnsinn and H. Hauser. Fuchs' theorem on linear differential equations in arbitrary characteristic, 2023. 40 pages, arXiv: 2307.01712.

[53] F. Fürnsinn and S. Yurkevich. Algebraicity of hypergeometric functions with arbitrary parameters. *Bull. Lond. Math. Soc.*, 2024. 23 pages, in print, https://doi.org/10.1112/blms.13103.

[54] T. Honda. Algebraic differential equations. In *Symposia Mathematica, Vol. XXIV (Sympos., INDAM, Rome, 1979)*, pages 169–204. Academic Press, London-New York, 1981.

[55] K. Iwasaki, H. Kimura and S. Shimomura and M. Yoshida. From Gauss to Painlevé. Aspects of Mathematics, E16. Friedr. Vieweg & Sohn, Braunschweig, 1991.

[56] N. Jacobson. Abstract derivation and Lie algebras. *Trans. Amer. Math. Soc.*, 42:206–224, 1937.

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

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

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

[60] M. Kauers, C. Koutschan, and D. Zeilberger. Proof of Ira Gessel's lattice path conjecture. *Proc. Natl. Acad. Sci. USA*, 106(28):11502–11505, 2009.

[61] K. S. Kedlaya. Local monodromy of p-adic differential equations: an overview. *Int. J. Number Theory*, 1(1):109–154, 2005.

[62] K. S. Kedlaya. *p-adic differential equations*, volume 125 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2010.

[63] R. Kelisky. The numbers generated by $\exp(\arctan x)$. *Duke Math. J.*, 26:569–581, 1959.

[64] J. J. Kovacic. An algorithm for solving second order linear homogeneous differential equations. *J. Symbolic Comput.*, 2(1):3–43, 1986.

[65] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464, 1977.

[66] E. Landau. Eine Anwendung des Eisensteinschen Satzes auf die Theorie der Gaussschen Differentialgleichung. *J. Reine Angew. Math.*, 127:92–102, 1904.

[67] E. Landau. Über einen zahlentheoretischen Satz und seine Anwendung auf die hypergeometrische Reihe. *Sitzungsber. Heidelb. Akad. Wiss. Math.-Natur. Kl.*, 18:3–38, 1911.

[68] L. Lipshitz. The diagonal of a D-finite power series is D-finite. *J. Algebra*, 113(2):373–378, 1988.

[69] S. Melczer. *Algorithmic and symbolic combinatorics—an invitation to analytic combinatorics in several variables*. Texts and Monographs in Symbolic Computation. Springer, Cham, [2021] ©2021. With a foreword by Robin Pemantle and Mark Wilson.

[70] H. Niederreiter. A new efficient factorization algorithm for polynomials over small finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 4(2):81–87, 1993.

[71] A. Ogus. Hodge cycles and crystalline cohomology. In *Hodge cycles, motives, and Shimura varieties, LNM 900*, pages 357–414. Springer-Verlag, 1982.

[72] R. Pagès. Computing characteristic polynomials of p-curvatures in average polynomial time. In *ISSAC'21—Proceedings of the 2021 ACM International Symposium on Symbolic and Algebraic Computation*. ACM, New York, 2021.

[73] A. Patel, A. N. Shankar, and J. P. Whang. The rank two p-curvature conjecture on generic curves. *Adv. Math.*, 386:Paper No. 107800, 33, 2021.

[74] J. Poineau. La droite de Berkovich sur $\mathbb{Z}$. In *Astérisque*, volume 333. Soc. Math. France, 2010.

[75] G. Pólya. Sur les séries entières, dont la somme est une fonction algébrique. *Enseign. Math.*, 22:38–47, 1921/1922.

[76] E. G. C. Poole. *Introduction to the theory of linear differential equations*. Dover Publications, Inc., New York, 1960.

[77] A. M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[78] H. A. Schwarz. Ueber diejenigen Fälle, in welchen die Gaussische hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt. *J. Reine Angew. Math.*, 75:292–335, 1873.

[79] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[80] J.-P. Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440, 2003.

[81] A. N. Shankar. The p-curvature conjecture and monodromy around simple closed loops. *Duke Math. J.*, 167(10):1951–1980, 2018.

[82] C. F. Woodcock and H. Sharif. On the transcendence of certain series. *J. Algebra* , 121, 1989, no. 2, 364–369.

[83] M. F. Singer. Algebraic solutions of nth order linear differential equations. In *Proceedings of the Queen's Number Theory Conference, 1979 (Kingston, Ont., 1979)*, volume 54 of *Queen's Papers in Pure and Appl. Math.*, pages 379–420. Queen's Univ., Kingston, ON, 1980.

[84] V. Strassen. Gaussian elimination is not optimal. *Numerische mathematik*, 13:354–356, 1969.

[85] E. Stridsberg. Sur le théorème d'Eisenstein et l'équation différentielle de Gauss. *Ark. Mat. Astron. Fys.*, 6(35):1–17, 1911.

[86] Y. Tang. Algebraic solutions of differential equations over $\mathbb{P}^1 - \{0, 1, \infty\}$. *Int. J. Number Theory*, 14(5):1427–1457, 2018.

[87] M. van der Put. Differential equations in characteristic p. *Compositio Math.* **97** (1995), no. 1-2, 227–251; MR1355126

[88] M. van der Put. Reduction modulo p of differential equations. *Indag. Math. (N.S.)*, 7(3):367–387, 1996.

[89] M. van der Put. Grothendieck's conjecture for the Risch equation $y' = ay + b$. *Indag. Math. (N.S.)*, 12(1):113–124, 2001.

[90] M. van der Put and M. F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.

[91] D. Vargas-Montoya. Algébricité modulo p, séries hypergéométriques et structures de Frobenius fortes. *Bull. Soc. Math. France*, 149(3):439–477, 2021.

[92] S. Yurkevich. The art of algorithmic guessing in gfun. *Maple Trans.*, 2(1):14421:1–14421:19, 2022.

[93] D. Zagier. The arithmetic and topology of differential equations. In *European Congress of Mathematics*, pages 717–776. Eur. Math. Soc., Zürich, 2018.