ON THE REDUCTION MODULO p OF MAHLER EQUATIONS

JULIEN ROQUES

Abstract. The guiding thread of the present work is the following result, in the vain of Grothendieck's conjecture for differential equations : if the reduction modulo almost all prime p of a given linear Mahler equation with coefficients in $\mathbb{Q}(z)$ has a full set of algebraic solutions, then this equation has a full set of rational solutions. The proof of this result, given at the very end of the paper, relies on intermediate results of independent interest about Mahler equations in characteristic zero as well as in positive characteristic.

Contents

1. Introduction 1
2. Notations 3
3. 1st Step - Algebraic vs rational solutions in characteristic $p > 0$ 3
4. 2nd Step - Factorization of Mahler operators 6
5. 3rd Step - Formal triviality : from characteristic $p > 0$ to characteristic 0 8
6. Conclusion - Proof of Theorem 1 10
References 10

1. Introduction

Fix $\ell \in \mathbb{Z}_{\geq 2}$ and $n \in \mathbb{Z}_{\geq 1}$. This short paper is concerned with functional equations of the form

$$a_n(z)f(z^{\ell^n}) + a_{n-1}(z)f(z^{\ell^{n-1}}) + \cdots + a_0(z)f(z) = 0 \tag{1}$$

with coefficients $a_0(z), \ldots, a_n(z) \in \mathbb{Q}(z)$ such that $a_0(z)a_n(z) \neq 0$. These equations and the corresponding solutions are called Mahler equations and functions, in reference to the work of Mahler [6, 7, 8] who investigated the algebraic relations over $\overline{\mathbb{Q}}$ between special values of Mahler functions. See K. Nishioka's book [9] for further informations and developments. Note that Mahler equations appear naturally in the context of automatic sequences : the generating series of any automatic sequence satisfies some Mahler equation.

Date: May 20, 2015.

2010 *Mathematics Subject Classification.* Primary 39A06; Secondary 12H10; 65Q20.

Key words and phrases. Mahler equations.

For almost all[1] prime numbers p, we can reduce the coefficients of equation (1) modulo p, and we obtain the equation

$$a_{n,p}(z)f(z^{\ell^n}) + a_{n-1,p}(z)f(z^{\ell^{n-1}}) + \cdots + a_{0,p}(z)f(z) = 0 \tag{2}$$

with coefficients $a_{0,p}(z), \ldots, a_{n,p}(z) \in \mathbb{F}_p(z)$, where $\mathbb{F}_p$ is the field with p elements.

In the present paper, we give some results about Mahler equations in characteristic zero, such as (1), as well as Mahler equations in positive characteristic, such as (2), and about their interplay. These results will allow us to prove the following theorem, in the spirit of Grothendieck's conjecture for differential equations.

Theorem 1. *Assume that, for almost all prime p, equation (2) has n $\mathbb{F}_p$-linearly independent solutions in $\mathbb{F}_p((z))$ algebraic over $\mathbb{F}_p(z)$. Then, equation (1) has n $\overline{\mathbb{Q}}$-linearly independent solutions in $\overline{\mathbb{Q}}(z)$.*

We shall now give the structure of the proof of this theorem, which, as mentioned above, relies on intermediate results of independent interest.

1st Step. The first step consists in proving that any solution in $\mathbb{F}_p((z))$ algebraic over $\mathbb{F}_p(z)$ of equation (2) is actually rational. This is Theorem 2 in Section 3. This result extends to positive characteristic the rational-transcendental dichotomy for Mahler functions over fields of characteristic 0; see [9, 2].

Let $\overline{\mathbb{Q}}((z))_b$ be the field made of the formal series $f(z) \in \overline{\mathbb{Q}}((z))$ whose coefficients belong to some finitely generated $\mathbb{Z}$-subalgebra of $\overline{\mathbb{Q}}$.

Assume temporarily that equation (1) has n $\overline{\mathbb{Q}}$-linearly independent solutions $f_1(z), \ldots, f_n(z)$ in $\overline{\mathbb{Q}}((z))_b$. Let K be a number field containing the coefficients of $f_1(z), \ldots, f_n(z)$. For almost all prime $\mathfrak{p}$ of K, whose residual characteristic is denoted by p, the reduction modulo $\mathfrak{p}$ of $f_1(z), \ldots, f_n(z)$ are solutions of equation (2), and hence are rational according to the 1st step. Adamczewski and Bell's [1, Lemma 5.3] implies that $f_1(z), \ldots, f_n(z)$ themselves are rational.

So, in order to conclude the proof, it is sufficient to prove that $f_1(z), \ldots, f_n(z)$ exist. By the light of the arithmetic theory of differential or q-difference equations (see [5, 3]), it would have been natural to prove the existence of $f_1(z), \ldots, f_n(z) \in \overline{\mathbb{Q}}((z))$ via some formal classification at 0 of Mahler equations (*i.e.* some analogue of Levelt-Turrittin theorem). Unfortunately, such a classification seems unknown (and, anyway, even if such a classification was known, we would also need an avatar of the notion of p-curvature). However, we show that Mahler operators have nice factorization properties at 0. This leads us to the second step of the proof.

For any integer $d \geq 1$, we set $z_d = z^{1/d}$ and we denote by $\overline{\mathbb{Q}}((z_d))_b$ the field made of the formal series $f(z_d) \in \overline{\mathbb{Q}}((z_d))$ whose coefficients belong to some finitely generated $\mathbb{Z}$-subalgebra of $\overline{\mathbb{Q}}$. Let ϕ_ℓ be the operator acting on $f(z_d)$ by $\phi_\ell(f(z_d)) = f(z_d^\ell)$. Equation (1) can be rewritten as

$$L(f(z)) = 0 \text{ with } L = a_n(z)\phi_\ell^n + a_{n-1}(z)\phi_\ell^{n-1} + \cdots + a_0(z).$$

[1] As usually, "for almost all" means "for all but finitely many".

2nd Step. The second step consists in proving that there exist an integer $d \geq 1$ and $g_1, \dots, g_n \in \overline{\mathbb{Q}}((z_d))_b$ such that

$$L = a_n(\phi_\ell - g_n) \cdots (\phi_\ell - g_1).$$

This is achieved in Theorem 6 of Section 4. Note that such a decomposition is valid for an arbitrary L, without any assumption on its reductions modulo p.

3rd Step. The third step consists in proving the existence of $f_1(z), \dots, f_n(z)$: we prove that if, for almost all prime p, equation (2) has n $\mathbb{F}_p$-linearly independent solutions in $\mathbb{F}_p((z))$ then equation (1) has n $\overline{\mathbb{Q}}$-linearly independent solutions $f_1(z), \dots, f_n(z)$ in $\overline{\mathbb{Q}}((z_d))_b$. The basic idea is to reduce the problem to non homogeneous Mahler equations of order 1 with coefficients in $\overline{\mathbb{Q}}((z_d))_b$ by using the 2nd step. We refer to Proposition 10 in Section 5 for details.

I thank B. Adamczewski for bringing [1, Lemma 5.3] to my attention, and for discussions on the present paper.

2. Notations

In the whole paper, $\ell \in \mathbb{Z}_{\geq 2}$ and $n \in \mathbb{Z}_{\geq 1}$ are fixed.

The algebraic closure of $\mathbb{Q}$ will be denoted by $\overline{\mathbb{Q}}$.

The letter p will denote some prime number, $\mathbb{F}_p$ will be the field with p elements and $\overline{\mathbb{F}_p}$ its algebraic closure.

The linear equation

$$a_n(z)f(z^{\ell^n}) + a_{n-1}(z)f(z^{\ell^{n-1}}) + \cdots + a_0(z)f(z) = 0 \tag{3}$$

with coefficients $a_0, \dots, a_n \in \mathbb{Q}(z)$ can be rewritten as

$$L(f) = 0$$

where $L = a_n(z)\phi_\ell^n + a_{n-1}(z)\phi_\ell^{n-1} + \cdots + a_0(z)$ and where ϕ_ℓ acts on $f(z)$ by $\phi_\ell(f(z)) = f(z^\ell)$. Such an operator L has to be understood as an element of the Öre algebra $\mathbb{Q}(z)\langle\phi_\ell\rangle$ of non commutative polynomials with coefficients in $\mathbb{Q}(z)$ such that $\phi_\ell a = \phi_\ell(a)\phi_\ell$ for all $a \in \mathbb{Q}(z)$. This can be extended to various fields instead of $\mathbb{Q}(z)$, e.g. $K(z)$, $K((z))$, etc, where K is a given field.

3. 1st Step - Algebraic vs rational solutions in characteristic $p > 0$

Theorem 2. *Let $f(z) \in \mathbb{F}_p((z))$ be such that*

$$a_n(z)f(z^{\ell^n}) + a_{n-1}(z)f(z^{\ell^{n-1}}) + \cdots + a_0(z)f(z) = 0$$

with $a_0(z), \dots, a_n(z) \in \mathbb{F}_p(z)$ such that $a_0(z)a_n(z) \neq 0$. Assume that $\gcd(\ell, p) = 1$. *If $f(z)$ is algebraic over $\mathbb{F}_p(z)$ then it actually belongs to $\mathbb{F}_p(z)$.*

The proof of this theorem will be given at the end of this section, as a consequence of a more general statement (Proposition 4 below) concerning the finite extensions of $\overline{\mathbb{F}_p}(z)$ endowed with an extension of $\phi_\ell : a(z) \in \overline{\mathbb{F}_p}(z) \mapsto a(z^\ell) \in \overline{\mathbb{F}_p}(z)$.

We start with a basic geometric result.

Proposition 3. *Let X be of smooth projective curve over $\overline{\mathbb{F}_p}$ with genus $g \geq 2$. Then, any non constant separable endomorphism of X is an automorphism and X has finitely many such endomorphisms.*

Proof. Let $\varphi : X \to X$ be a non constant separable endomorphism of X. Hurwitz's formula (see [4, Corollary 2.4]) ensures that

$$-2(N-1)(g-1) = \sum_P \ell_P$$

where

- $N \geq 1$ is the degree of φ;
- the sum is taken over the ramification points P of φ;
- ℓ_P is an integer $\geq e_P - 1$, where $e_P \geq 1$ is the ramification index of φ at P.

The fact that the right hand side of the above equality is ≥ 0 implies that $N = 1$ that is that φ has degree 1 and hence is an automorphism.

The fact that the group of automorphisms of X is finite is due to Schmid [10]. □

Proposition 4. *Let L be a finite extension of $\overline{\mathbb{F}_p}(z)$. Assume that* $\gcd(\ell, p) = 1$ *and that the endomorphism ϕ_ℓ of $\overline{\mathbb{F}_p}(z)$ defined by $\phi_\ell(f(z)) = f(z^\ell)$ extends to a field endomorphism of L. Then, there exists $N \in \mathbb{Z}_{\geq 1}$ and $z_N \in L$ such that :*

(i) $z_N^N = z$;

(ii) L is a purely inseparable extension of $\overline{\mathbb{F}_p}(z_N)$.

Proof. The extension of ϕ_ℓ to L is still denoted by ϕ_ℓ.

Let E be the separable closure of $\overline{\mathbb{F}_p}(z)$ in L. This is the unique subextension of $L/\overline{\mathbb{F}_p}(z)$ such that $E/\overline{\mathbb{F}_p}(z)$ is separable and L/E is purely inseparable. We have to prove that $E = \overline{\mathbb{F}_p}(z)$.

We claim that ϕ_ℓ induces a field endomorphism of E. Indeed, if $x \in E$ then $P(x) = 0$ for some non zero separable polynomial $P = \sum a_i(z)X^i \in \overline{\mathbb{F}_p}(z)[X]$. Then $P^{\phi_\ell}(\phi_\ell(x)) = 0$ with $P^{\phi_\ell} = \sum \phi_\ell(a_i(z))X^i \in \overline{\mathbb{F}_p}(z)[X]$ and P^{ϕ_ℓ} is separable (because the discriminant of P^{ϕ_ℓ} is the image by ϕ_ℓ of the discriminant of P and hence is non zero). So $\phi_\ell(x)$ is separable over $\overline{\mathbb{F}_p}(z)$ and hence belongs to E.

Now, consider a morphism of smooth projective curves $\varphi : X \to \mathbb{P}^1(\overline{\mathbb{F}_p})$ whose induced morphism of function fields is the inclusion $\overline{\mathbb{F}_p}(z) \subset E$. What precedes shows that ϕ_ℓ induces an endomorphism f of X such that the following diagram is commutative :

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\varphi"'] & X \arrow[d, "\varphi"] \\ \mathbb{P}^1(\overline{\mathbb{F}_p}) \arrow[r, "z \mapsto z^\ell"'] & \mathbb{P}^1(\overline{\mathbb{F}_p}) \end{tikzcd} .$$

Observe that

- f is a separable morphism. Indeed, this is equivalent to the fact that $E/\phi_\ell(E)$ is separable. It is therefore sufficient to prove that $E/\phi_\ell(\overline{\mathbb{F}_p}(z))$ is separable and this property holds true because $E/\overline{\mathbb{F}_p}(z)$

and $\overline{\mathbb{F}_p}(z)/\phi_\ell(\overline{\mathbb{F}_p}(z))$ are separable (the latter is separable because $\gcd(\ell,p)=1$).
- X has genus $g \in \{0,1\}$ (follows from Proposition 3 since f has infinite order).
- f has degree ℓ (take degrees in the above commutative diagram).
- $f^{-1}(\varphi^{-1}(0)) = \varphi^{-1}(0)$, $f^{-1}(\varphi^{-1}(\infty)) = \varphi^{-1}(\infty)$, and f is totally ramified above any point of $Z = \varphi^{-1}(0) \cup \varphi^{-1}(\infty)$. Indeed, the inclusion $f^{-1}(\varphi^{-1}(0)) \subset \varphi^{-1}(0)$ follows immediately from the above commutative diagram. Since f is not constant, it is surjective. Now, for cardinality reasons, this implies that the inclusion $f^{-1}(\varphi^{-1}(0)) \subset \varphi^{-1}(0)$ is an equality and that the fiber of f above any element of $\varphi^{-1}(0)$ has exactly one element. The arguments for $\varphi^{-1}(\infty)$ are similar.

Assume that $g=0$, so that we can replace X by $\mathbb{P}^1(\overline{\mathbb{F}_p})$. Hurwitz's formula for the separable morphism f (cf. [4, Corollary 2.4]) ensures that

$$2(\ell-1) = \sum_P \ell_P$$

where
- the sum is taken over the ramification points P of f;
- ℓ_P is an integer $\geq e_P - 1$, where $e_P \geq 1$ is the ramification index of f at P.

Note that $\sum_{P\in Z} \ell_P \geq \sum_{P \in Z}(e_P-1) = \sharp Z(\ell-1)$. Since $\sharp Z \geq 2$, we deduce that $\sharp Z = 2$ i.e. that $\sharp\varphi^{-1}(0) = \sharp\varphi^{-1}(\infty) = 1$ and that f is unramified outside Z.

Let c be an automorphism of $\mathbb{P}^1(\overline{\mathbb{F}_p})$ such that $c(\varphi^{-1}(0)) = 0$ and $c(\varphi^{-1}(\infty)) = \infty$. Then, cfc^{-1} is totally ramified at 0 and ∞, unramified elsewhere, of degree p, and fixes 0 and ∞, so $cfc^{-1}(z) = z^\ell$. It follows from the commutative diagram

$$\begin{tikzcd}
\mathbb{P}^1(\overline{\mathbb{F}_p}) \arrow[r, "cfc^{-1}"] \arrow[d, "\varphi c^{-1}"'] & \mathbb{P}^1(\overline{\mathbb{F}_p}) \arrow[d, "\varphi c^{-1}"] \\
\mathbb{P}^1(\overline{\mathbb{F}_p}) \arrow[r, "z\mapsto z^\ell"'] & \mathbb{P}^1(\overline{\mathbb{F}_p})
\end{tikzcd}$$

that $\varphi c^{-1}(z) = z^N$ for some $N \in \mathbb{Z}_{\geq 1}$. That is $\varphi = c^N$ and $f(z) = c^{-1}(c(z)^\ell)$. Therefore, there exists $z_N \in E$ such that $z_N^N = z$ and $E = \overline{\mathbb{F}_p}(z_N)$, as expected.

Assume that $g=1$. Then f is unramified (immediate from Hurwitz's formula) of degree ℓ. Considering cardinals in the inclusion $f^{-1}(\varphi^{-1}(0)) \subset \varphi^{-1}(0)$, we get that the degree of f is equal to 1, so $\ell = 1$, which is excluded. □

We have the following immediate consequence of Proposition 4.

Corollary 5. *Let L be a finite extension of $\overline{\mathbb{F}_p}(z)$ in $\overline{\mathbb{F}_p}((z))$. Assume that $\gcd(\ell,p)=1$ and that the endomorphism ϕ_ℓ of $\overline{\mathbb{F}_p}((z))$ defined by $\phi_\ell(f(z)) = f(z^\ell)$ induces an endomorphism of L. Then L is a purely inseparable extension of $\overline{\mathbb{F}_p}(z)$.*

We are now in position to prove Theorem 2.

Proof of Theorem 2. Let L be the finite extension of $\mathbb{F}_p(z)$ generated by $f(z), f(z^\ell), \ldots, f(z^{\ell^{n-1}})$. The Mahler equation satisfied by $f(z)$ ensures that ϕ_ℓ induces a field endomorphism of L. Corollary 5 implies that L is a purely inseparable extension of $\overline{\mathbb{F}_p}(z)$. So $f(z)^{p^m}$ belongs to $\overline{\mathbb{F}_p}(z)$ for some $m \in \mathbb{Z}_{\geq 0}$. We deduce from this and from the equality $f(z)^{p^m} = f(z^{p^m})$ that $f(z)$ itself belongs to $\overline{\mathbb{F}_p}(z)$. □

4. 2nd Step - Factorization of Mahler operators

We denote by $\overline{\mathbb{Q}}((z))_b$ the field made of the formal series $f(z) = \sum_{k\in\mathbb{Z}} f_k z^k \in \overline{\mathbb{Q}}((z))$ whose coefficients belong to some finitely generated $\mathbb{Z}$-subalgebra of $\overline{\mathbb{Q}}$. We set $\overline{\mathbb{Q}}[[z]]_b = \overline{\mathbb{Q}}((z))_b \cap \overline{\mathbb{Q}}[[z]]$.

More generally, consider the field of Puiseux series $\cup_{d\geq 1}\overline{\mathbb{Q}}((z_d))$ where $z_d^d = z$. We denote by $\overline{\mathbb{Q}}((z_d))_b$ the field made of the formal series $f(z_d) = \sum_{k\in\mathbb{Z}} f_k z_d^k \in \overline{\mathbb{Q}}((z_d))$ whose coefficients belong to some finitely generated $\mathbb{Z}$-subalgebra of $\overline{\mathbb{Q}}$. We set $\overline{\mathbb{Q}}[[z_d]]_b = \overline{\mathbb{Q}}((z_d))_b \cap \overline{\mathbb{Q}}[[z_d]]$.

In this section, we denote by

$$L = a_n(z)\phi_\ell^n + a_{n-1}(z)\phi_\ell^{n-1} + \cdots + a_0(z)$$

the operator associated to the equation

$$a_n(z)f(z^{\ell^n}) + a_{n-1}(z)f(z^{\ell^{n-1}}) + \cdots + a_0(z)f(z) = 0$$

with $a_0(z), \ldots, a_n(z) \in \overline{\mathbb{Q}}((z))_b$ and $a_0(z)a_n(z) \neq 0$ (see Section 2). In order to simplify the notations, we will assume that $a_n(z) = 1$.

The aim of this section is to prove the following result.

Theorem 6. *The operator L admits a factorization of the form*

$$L = (\phi_\ell - g_n)\cdots(\phi_\ell - g_1)$$

with $g_1, \ldots, g_n \in \overline{\mathbb{Q}}((z_d))_b$ for some integer $d \geq 1$.

This result will be proved at the very end of this section, after some lemmas. We first introduce some notations and terminologies.

Let a, r, with $r \neq 0$, be elements of some difference field extension of $(\overline{\mathbb{Q}}((z)), \phi_\ell)$ such that $\phi_\ell(r) = ar$. We will denote by $L^{[r]}$ the operator defined by

$$L^{[r]} := r^{-1}Lr = \sum_{i=0}^{n} a\phi_\ell(a)\cdots\phi_\ell^{i-1}(a)a_i\phi_\ell^i,$$

so that $L^{[r]}(f) = 0$ if and only if $L(rf) = 0$. For instance :

– for any $\mu \in \mathbb{Q}$, we consider $\theta_\mu = z^{\frac{\mu}{\ell-1}}$ so that $\phi_\ell(\theta_\mu) = z^\mu\theta_\mu$ and

$$L^{[\theta_\mu]} = \sum_{i=0}^{n} z^{(1+\ell+\cdots+\ell^{i-1})\mu}a_i\phi_\ell^i;$$

– for any $c \in \mathbb{C}^\times$, we consider e_c such that $\phi_\ell(e_c) = ce_c$ so that

$$L^{[e_c]} = \sum_{i=0}^{n} c^i a_i \phi_\ell^i.$$

We define the Newton polygon $\mathcal{N}(L)$ of L as the convex hull in $\mathbb{R}^2$ of

$$\{(i,j) \in \mathbb{Z} \times \mathbb{R} \mid j \geq v_z(a_{n-i})\}$$

where $v_z : \cup_{d \geq 1} \overline{\mathbb{Q}}((z_d)) \to \mathbb{Q} \cup \{+\infty\}$ denotes the z-adic valuation. This polygon is made of two vertical half lines and of k vectors $(r_1, d_1), \dots, (r_k, d_k) \in \mathbb{N}^* \times \mathbb{Q}$ having pairwise distinct slopes, called the Newton-slopes of L.

Lemma 7. *There exists an unique $\mu_1 \in \mathbb{Q}$ such that the greatest Newton-slope of $L^{[\theta_{\mu_1}]}$ is* 0*.*

Proof. The fact that the greatest Newton-slope of $L^{[\theta_{\mu_1}]}$ is 0 means that, for all $i \in \{1, \dots, n\}$,

$$v_z(a_i) + (1 + \ell + \cdots + \ell^{i-1})\mu_1 \geq v_z(a_0)$$

and that this inequality is an equality for some $i \in \{1, \dots, n\}$. It is easily seen that there exists an unique $\mu_1 \in \mathbb{Q}$ with these properties. □

Set $L^{[\theta_{\mu_1}]} = \sum_{i=0}^{n} b_i \phi_\ell^i$ with $b_0, \dots, b_n \in \overline{\mathbb{Q}}((z_d))_b$. Let $c_1 \in \overline{\mathbb{Q}}^\times$ be a root of the polynomial $\sum_{i=0}^{n} \left(b_i z^{-v_z(b_0)}\right)_{|z=0} X^i \in \overline{\mathbb{Q}}[X]$ (which has degree ≥ 1 and non zero constant coefficient). Let $d_1 \in \mathbb{Z}_{\geq 1}$ be a denominator of μ_1.

Lemma 8. *There exists $f_1 \in 1 + z_{d_1}\overline{\mathbb{Q}}[[z_{d_1}]]_b$ such that $L(\theta_{\mu_1} e_{c_1} f_1) = 0$.*

Proof. We set $\mu = \mu_1$, $c = c_1$, $d = d_1$ and $L^{[\theta_\mu]} = \sum_{i=0}^{n} b_i \phi_\ell^i$ with $b_i = \sum_j b_{i,j} z_d^j \in \overline{\mathbb{Q}}((z_d))_b$. Using the fact that the greatest Newton-slope of L is 0, we see that, up to left multiplication of L by some element of $\overline{\mathbb{Q}}((z_d))_b^\times$, we can assume that $b_0, \dots, b_n \in \overline{\mathbb{Q}}[[z_d]]_b$ and $b_{0,0} \neq 0$. For $f = \sum_{k \geq 0} f_k z_d^k \in 1 + z_d\overline{\mathbb{Q}}[[z_d]]$, we have

$$L(\theta_\mu e_c f) = \theta_\mu e_c \sum_{i,j,k \geq 0} b_{i,j} c^i f_k z_d^{j + k\ell^i} = 0$$

if and only if, for all $m \in \mathbb{Z}_{\geq 0}$,

$$\sum_{\substack{i,j,k \geq 0 \\ j + k\ell^i = m}} b_{i,j} c^i f_k = 0. \tag{4}$$

This equation is automatically satisfied for $m = 0$ because

$$\sum_{\substack{i,j,k \geq 0 \\ j + k\ell^i = 0}} b_{i,j} c^i f_k = \left(\sum_i b_{i,0} c^i \right) f_0$$

and $\sum_i b_{i,0} c^i = 0$ by definition of c. For $m > 0$, equation (4) can be rewritten as follows

$$\sum_{\substack{i,j,k \geq 0 \\ k < m,\ j + k\ell^i = m}} b_{i,j} c^i f_k = -b_{0,0} f_m$$

so that the coefficients of f are (uniquely) recursively determined, and belong to the finitely generated $\mathbb{Z}$-algebra $R[c, b_{0,0}^{-1}]$ where R is a finitely generated $\mathbb{Z}$-algebra containing the $b_{i,j}$. □

Lemma 9. *We have*

$$L = L_2(\phi_\ell - g_1)$$

for some $g_1 \in \overline{\mathbb{Q}}((z_{d_1}))_b$ *and some operator* $L_2 \in \overline{\mathbb{Q}}((z_{d_1}))_b\langle\phi_\ell\rangle$.

Proof. The operators L and $\phi_\ell(f_1)(\phi_\ell - z^{\mu_1}c_1)f_1^{-1} = \phi_\ell - z^{\mu_1}c_1\phi_\ell(f_1)f_1^{-1}$ annihilate $\theta_{\mu_1}e_{c_1}f_1$. The result follows by euclidean division of the former by the later. □

Proof of Theorem 6. Follows from a repeated application of the previous lemma. □

5. 3rd Step - Formal triviality : from characteristic $p > 0$ to characteristic 0

In this section, we denote by

$$L = a_n(z)\phi_\ell^n + a_{n-1}(z)\phi_\ell^{n-1} + \cdots + a_0(z)$$

the operator associated to the equation

$$a_n(z)f(z^{\ell^n}) + a_{n-1}(z)f(z^{\ell^{n-1}}) + \cdots + a_0(z)f(z) = 0 \tag{5}$$

with $a_0(z), \ldots, a_n(z) \in \mathbb{Q}(z)$ and $a_0(z)a_n(z) \neq 0$ (see Section 2).

We can reduce the coefficients $a_0, \ldots, a_n$ modulo almost all prime numbers p. These reductions, denoted $a_{0,p}, \ldots, a_{n,p}$, belong to $\mathbb{F}_p(z)$. We denote by L_p the reduction of L modulo p :

$$L_p = a_{n,p}(z)\phi_\ell^n + a_{n-1,p}(z)\phi_\ell^{n-1} + \cdots + a_{0,p}(z),$$

which is associated to the equation

$$a_{n,p}(z)f(z^{\ell^n}) + a_{n-1,p}(z)f(z^{\ell^{n-1}}) + \cdots + a_{0,p}(z)f(z) = 0. \tag{6}$$

Proposition 10. *Assume that, for almost all prime p, the equation (6) has n linearly independent solutions in $\cup_{d\geq 1}\mathbb{F}_p((z_d))$. Then, equation (5) has n linearly independent solutions in $\cup_{d\geq 1}\overline{\mathbb{Q}}((z_d))_b$.*

Proof. We can assume that $a_n(z) = 1$. We know from Theorem 6 that $L = (\phi_\ell - f_n)\cdots(\phi_\ell - f_1)$ with $f_1, \ldots, f_n \in \cup_{d\geq 1}\overline{\mathbb{Q}}((z_d))_b^\times$. Let K be a number field and R be a finitely generated $\mathbb{Z}$-subalgebra of K such that $f_1, \ldots, f_n \in \cup_{d\geq 1}R[[z_d]][z_d^{-1}]$. For almost all prime $\mathfrak{p}$ of K, R is contained in the valuation subring of K at $\mathfrak{p}$, and hence we can reduce the coefficients of $f_1, \ldots, f_n$ modulo $\mathfrak{p}$. These reductions, denoted $f_{1,\mathfrak{p}}, \ldots, f_{n,\mathfrak{p}}$, belong to $\cup_{d\geq 1}\kappa_\mathfrak{p}((z_d))$ where $\kappa_\mathfrak{p}$ is the residue field of K at $\mathfrak{p}$, which is a finite extension of the prime field $\mathbb{F}_p$ of $\kappa_\mathfrak{p}$.

We will denote by $L_\mathfrak{p}$ the reduction of L modulo $\mathfrak{p}$ i.e. $L_\mathfrak{p} = L_p$.

By hypothesis, for almost all prime $\mathfrak{p}$ of K, the equation $L_\mathfrak{p}y = 0$ has n $\mathbb{F}_p$−linearly independent solutions in $\cup_{d\geq 1}\mathbb{F}_p((z_d))$ and hence in $\cup_{d\geq 1}\kappa_\mathfrak{p}((z_d))$, so

($1_\mathfrak{p}$) $(\phi_\ell - f_{n,\mathfrak{p}})y = 0$ has a solution $y_{1,1} \in \cup_{d\geq 1}\kappa_\mathfrak{p}((z_d))^\times$;

($2_\mathfrak{p}$) $y_{1,1} = (\phi_\ell - f_{n-1,\mathfrak{p}})y$ has a solution $y_{2,1} \in \cup_{d\geq 1}\kappa_\mathfrak{p}((z_d))$ and $(\phi_\ell - f_{n-1,\mathfrak{p}})y = 0$ has a solution $y_{2,2} \in \cup_{d\geq 1}\kappa_\mathfrak{p}((z_d))^\times$;

$\cdots \quad \cdots \quad \cdots$

($n_\mathfrak{p}$) for all $i \in \{1, \ldots, n-1\}$, $y_{i,n-1} = (\phi_\ell - f_{1,\mathfrak{p}})y$ has a solution $y_{i,n} \in \cup_{d\geq 1}\kappa_\mathfrak{p}((z_d))$ and $(\phi_\ell - f_{1,\mathfrak{p}})y = 0$ has a solution $y_{1,n} \in \cup_{d\geq 1}\kappa_\mathfrak{p}((z_d))^\times$.

In order to prove that $Ly=0$ has n $\overline{\mathbb{Q}}$-linearly independent solutions in $\cup_{d\geq 1}\overline{\mathbb{Q}}((z_d))$, we have to prove that L satisfies the properties similar to $(1_{\mathfrak{p}})$–$(n_{\mathfrak{p}})$ above obtained by replacing $L_{\mathfrak{p}}$ by L and $\kappa_{\mathfrak{p}}((z_d))$ by $\overline{\mathbb{Q}}((z_d))_b$. This follows clearly from the following lemmas. In what follows, we denote by $\mathrm{cld}(f)$ the coefficient of the term of the lowest degree of $f\in\cup_{d\geq 1}\overline{\mathbb{Q}}((z_d))^{\times}$, so that $f=\mathrm{cld}(f)z^{v_z(f)}\widetilde{f}$ where $\widetilde{f}\in\cup_{d\geq 1}(1+z_d\overline{\mathbb{Q}}[[z_d]])$ and where $v_z(f)$ is the z-adic valuation of f. We use a similar notation for the elements of $\cup_{d\geq 1}\kappa_{\mathfrak{p}}((z_d))$.

Lemma 11. *We have* $\mathrm{cld}(f_1)=\cdots=\mathrm{cld}(f_n)=1$.

Proof. According to properties $(1_{\mathfrak{p}})$–$(n_{\mathfrak{p}})$, for almost all prime $\mathfrak{p}$ of K, we have $(\phi_\ell - f_{i,\mathfrak{p}})y_{i,\mathfrak{p}}=0$ for some $y_{i,\mathfrak{p}}\in\cup_{d\geq 1}\kappa_{\mathfrak{p}}((z_d))^{\times}$. So $f_{i,\mathfrak{p}}=\phi_\ell(y_{i,\mathfrak{p}})/y_{i,\mathfrak{p}}$ and hence $\mathrm{cld}(f_{i,\mathfrak{p}})=\frac{\mathrm{cld}(\phi_\ell(y_{i,\mathfrak{p}}))}{\mathrm{cld}(y_{i,\mathfrak{p}})}=1$. But, for almost all prime $\mathfrak{p}$ of K, $\mathrm{cld}(f_{i,\mathfrak{p}})$ is equal to the reduction of $\mathrm{cld}(f_i)$ modulo $\mathfrak{p}$. Hence $\mathrm{cld}(f_i)=1$. □

Lemma 12. *Consider* $f\in\cup_{d\geq 1}R[[z_d]][z_d^{-1}]$ *with* $f\neq 0$ *and* $\mathrm{cld}(f)=1$. *Then, the equation* $0=(\phi_\ell - f)y$ *has a non zero solution in* $\cup_{d\geq 1}R[[z_d]][z_d^{-1}]$.

Proof. Let $\nu=v_z(f)$ so that $f=z^{\nu}\widetilde{f}$ with $\widetilde{f}\in\cup_{d\geq 1}(1+z_dR[[z_d]])$. Then $r=z^{\frac{\nu}{\ell-1}}\prod_{j\geq 0}\phi_\ell^j(\widetilde{f})^{-1}\in z^{\mathbb{Q}}\cup_{d\geq 1}(1+z_dR[[z_d]])$ is such that $\phi_\ell(r)=fr$. □

Lemma 13. *Consider* $f,g\in\cup_{d\geq 1}R[[z_d]][z_d^{-1}]$ *with* $f\neq 0$ *and* $\mathrm{cld}(f)=1$. *For almost all prime* $\mathfrak{p}$ *of* K, *we denote by* $f_{\mathfrak{p}}$ *and* $g_{\mathfrak{p}}$ *the reductions of* f *and* g *modulo* $\mathfrak{p}$. *Assume that, for almost all prime* $\mathfrak{p}$ *of* K, *the equation* $g_{\mathfrak{p}}=(\phi_\ell - f_{\mathfrak{p}})y$ *has a solution in* $\cup_{d\geq 1}\kappa_{\mathfrak{p}}((z_d))$. *Then, the equation* $g=(\phi_\ell - f)y$ *has a solution in* $\cup_{d\geq 1}R[[z_d]][z_d^{-1}]$.

Proof. Let $\nu=v_z(f)$ so that $f=z^{\nu}\widetilde{f}$ with $\widetilde{f}\in\cup_{d\geq 1}(1+z_dR[[z_d]])$. Then $r=z^{\frac{\nu}{\ell-1}}\prod_{j\geq 0}\phi_\ell^j(\widetilde{f})^{-1}\in z^{\mathbb{Q}}\cup_{d\geq 1}(1+z_dR[[z_d]])$ is such that $\phi_\ell(r)=fr$.

Using the change of unknown function $r\widetilde{y}=y$, we see that

- $g=(\phi_\ell - f)y$ has solution $y\in\cup_{d\geq 1}R[[z_d]][z_d^{-1}]$ if and only if $\widetilde{g}=(\phi_\ell - 1)\widetilde{y}$ has solution in $\cup_{d\geq 1}R[[z_d]][z_d^{-1}]$, where $\widetilde{g}=g/(rf)$;
- for almost all prime $\mathfrak{p}$ of K, $g_{\mathfrak{p}}=(\phi_\ell - f_{\mathfrak{p}})y$ has a solution $y\in\cup_{d\geq 1}\kappa_{\mathfrak{p}}((z_d))$ if and only if $\widetilde{g}_{\mathfrak{p}}=(\phi_\ell - 1)y$ has a solution $\widetilde{y}\in\cup_{d\geq 1}\kappa_{\mathfrak{p}}((z_d))$, where $\widetilde{g}_{\mathfrak{p}}$ is the reduction modulo $\mathfrak{p}$ of $\widetilde{g}=g/(rf)$.

Therefore, we can assume that $f=1$.

So, we suppose that, for almost all prime $\mathfrak{p}$ of K, $g_{\mathfrak{p}}=(\phi_\ell - 1)y$ has a solution in $\cup_{d\geq 1}\kappa_{\mathfrak{p}}((z_d))$. It follows that $g_{\mathfrak{p}}$ has no constant term and that $\sum_{j\geq 0}\phi_\ell^j(g_{\mathfrak{p}})$, which is a priori an element of $\cup_{d\geq 1}\kappa_{\mathfrak{p}}[[z_d,z_d^{-1}]]$, belongs to $\cup_{d\geq 1}\kappa_{\mathfrak{p}}[[z_d]][z_d^{-1}]=\cup_{d\geq 1}\kappa_{\mathfrak{p}}((z_d))$. What precedes implies that g has no constant term. Moreover, the set $\{a_i\mid i\in\mathbb{Z}_{<0}\}$ of coefficients of the terms of negative degree of $\sum_{j\geq 0}\phi_\ell^j(g)=:\sum_{i\in\mathbb{Z}}a_iz_{d'}^i$ (for some $d'\in\mathbb{Z}_{>0}$) is easily seen to be finite. But, as noticed above, for almost all prime $\mathfrak{p}$ of K, $a_j=0$ modulo $\mathfrak{p}$ provided that $j<<0$. Therefore, $a_j=0$ for $j<<0$ and hence $\sum_{j\geq 0}\phi_\ell^j(g)$ belongs to $R[[z_{d'}]][z_{d'}^{-1}]$. We conclude by noticing that $\sum_{j\geq 0}\phi_\ell^j(g)$ is a solution of $g=(\phi_\ell - 1)y$. □

□

6. Conclusion - Proof of Theorem 1

According to Proposition 10, equation (1) has n $\overline{\mathbb{Q}}$-linearly independent solutions $y_1,\ldots,y_n \in \cup_{d\geq 1}\overline{\mathbb{Q}}((z_d))_b$. Let K be a number field and R be a finitely generated $\mathbb{Z}$-subalgebra of K such that $y_1,\ldots,y_n \in \cup_{d\geq 1}R[[z_d]][z_d^{-1}]$. For almost all prime $\mathfrak{p}$ of K, we can reduce the coefficients of $y_1,\ldots,y_n$ modulo $\mathfrak{p}$. These reductions, denoted $y_{1,\mathfrak{p}},\ldots,y_{n,\mathfrak{p}}$, belong to $\cup_{d\geq 1}\kappa_{\mathfrak{p}}((z_d))$ where $\kappa_{\mathfrak{p}}$ is the residue field of K at $\mathfrak{p}$ and are n $\mathbb{F}_p$-linearly independent solutions of equation (2), for almost all prime $\mathfrak{p}$ of K.

On the other hand, by hypothesis, for almost all prime p, equation (2) has n $\mathbb{F}_p$-linearly independent solutions in $\mathbb{F}_p((z))$ algebraic over $\mathbb{F}_p(z)$. Theorem 2 ensures that, for almost all prime p, equation (2) has n $\mathbb{F}_p$-linearly independent solutions in $\mathbb{F}_p(z)$.

Therefore, for almost all prime $\mathfrak{p}$ of K, $y_{1,\mathfrak{p}},\ldots,y_{n,\mathfrak{p}}$ belong to $\overline{\mathbb{F}_p}(z)$. Now, Adamczewski and Bell's [1, Lemma 5.3] ensures that $y_1,\ldots,y_n \in \overline{\mathbb{Q}}(z)$. This concludes the proof.

References

[1] B. Adamczewski and J. P. Bell, A problem around Mahler functions. 2013.

[2] J. P. Bell, M. Coons and E. Rowland, The rational-transcendental dichotomy of Mahler functions. J. Integer Seq. 16 (2013), no. 2, Article 13.2.10, 11 pp.

[3] L. Di Vizio, Arithmetic theory of q-difference equations: the q-analogue of Grothendieck-Katz's conjecture on p-curvatures. Invent. Math. 150 (2002), no. 3, 517–578.

[4] R. Hartshorne, Algebraic geometry. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[5] N. M. Katz, Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin. Inst. Hautes Études Sci. Publ. Math. No. 39 (1970), 175–232.

[6] K. Mahler, Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen. Math. Ann. 103 (1930), no. 1, 532.

[7] K. Mahler, Arithmetische Eigenschaften einer Klasse transzendental-transzendente funktionen. Math. Z. 32 (1930), no. 1, 545–585.

[8] K. Mahler, Über das Verschwinden von Potenzreihen mehrerer Veränderlichen in speziellen Punktfolgen. Math. Ann. 103 (1930), no. 1, 573–587.

[9] K. Nishioka, Mahler functions and transcendence, volume 1631 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1996.

[10] H. L. Schmid, Über die automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik. J. Reine Angew. Math. 179 (1938), 5–15.

Institut Fourier, Université Grenoble 1, CNRS UMR 5582, 100 rue des Maths, BP 74, 38402 St Martin d'Hères

E-mail address: Julien.Roques@ujf-grenoble.fr