A Galoisian proof of Ritt theorem on the differential transcendence of Poincaré functions

Lucia Di Vizio[*] & Gwladys Fernandes[†]

March 17, 2021

Abstract

Using Galois theory of functional equations, we give a new proof of the main result of the paper "Transcendental transcendency of certain functions of Poincaré" by J.F. Ritt, on the differential transcendence of the solutions of the functional equation $R(y(t)) = y(qt)$, where $R(t) \in \mathbb{C}(t)$ verifies $R(0) = 0$, $R'(0) = q \in \mathbb{C}$, with $|q| > 1$. We also give a partial result in the case of an algebraic function R.

2010 Mathematics Subject Classification: 30D05, 34M15, 39B12.

1 Introduction

We fix a rational function R, with complex coefficients, such that $R(0) = 0$, $R'(0) = q \in \mathbb{C}$, with $|q| > 1$. To linearize the rational map R at 0, one has to solve the functional equation

$$(1.1) \qquad\qquad R(\sigma(t)) = \sigma(qt).$$

It means that, up to a conjugation by σ, the rational function R acts linearly in the neighborhood of 0. H. Poincaré noticed that such an equation admits a formal solution $\sigma \in t\mathbb{C}[[t]]$, called a Poincaré function, which is actually the expansion at zero of a uniform function, i.e. a meromorphic function over the whole $\mathbb{C}$. See [Poi90, page 318]. The functional equation (1.1) plays a key role in rational dynamics and for this reason has been studied by many authors, in particular relaxing the assumption on the absolute value of q.

In [Rit26], J.F. Ritt addresses the question of the differential algebraicity of σ over the field of rational functions $\mathbb{C}(t)$, i.e., the fact that σ is solution of an algebraic differential equation with coefficients in $\mathbb{C}(t)$. This means that there exists a non-negative integer n and a non-zero polynomial $P \in \mathbb{C}[t, X_0, X_1, \ldots, X_n]$ such that $P(t, \sigma, \sigma', \ldots, \sigma^{(n)}) = 0$. We say that σ is differentially transcendental over $\mathbb{C}(t)$ if it is not differentially algebraic. Ritt's paper is at the origin of a large literature on differential transcendence of solutions of functional equations linked to dynamical systems, which is surveyed in [Fer21].

Theorem 1.1 ([Rit26]). *Let σ be a solution of a functional equation of the form (1.1), where $R(t) \in \mathbb{C}(t)$ is not a homography and $R(0) = 0$, $R'(0) = q \in \mathbb{C}$, with $|q| > 1$. If σ satisfies an algebraic differential equation then it is the composition of a homography with a periodic function belonging to the following list: $\exp(\alpha t^p)$, $\cos(\alpha t^p + \beta)$, $\wp(\alpha t^p + \beta)$, $\wp^2(\alpha t^p + \beta)$, $\wp^3(\alpha t^p + \beta)$ or $\wp'(\alpha t^p + \beta)$, where $\wp$ is the Weierstrass function and for a convenient choice of $p \in \mathbb{Q}$, of $\alpha \in \mathbb{C}$ and of a fraction $\beta \in \mathbb{C}$ of the period.*

The list above appears in [Rit22], where Ritt classifies periodic Poincaré functions. For more comments and explanations on such a list we refer to [Fer21, §3.1]. Notice that σ is rational if and only if $R(t)$ is a homography (see Lemma 2.1 below).

The original proof of the theorem above is organised in the following way:

1. Ritt supposes that σ is solution of a general algebraic differential equation. Replacing t by qt and using (1.1), he derives a new differential equation that allows him to perform an Euclidean division in order to lower what he calls the *rank* of the differential equation. He iterates this operation several times, choosing carefully the terms to eliminate in the process: this part of the proof (namely from §4 to §11 in *loc.cit.*) is really a *tour de force*. He narrows the investigation to three possible differential equations satisfied by σ, that are called (A), (B) and (C) (see §11 in *loc.cit.*), and he notices that the solutions of (A) and (B) are actually solutions of a differential equation of type (C), so that he is left with this last case.

---

[*]Lucia Di Vizio, CNRS, Université Paris-Saclay, UVSQ, Laboratoire de mathématiques de Versailles, 78000, Versailles, France. lucia.di.vizio@math.cnrs.fr, https://divizio.perso.math.cnrs.fr

[†]Gwladys Fernandes, Université Paris-Saclay, UVSQ, CNRS, Laboratoire de mathématiques de Versailles, 78000, Versailles, France. gwladys.fernandes@uvsq.fr, https://fernandes.perso.math.cnrs.fr

2. He shows that the Poincaré functions that are also solutions of (C), are obtained by composing a periodic Poincaré function with a rational power of t.

3. He uses his results in [Rit22] on the classification of periodic Poincaré functions to make the list explicit and concludes a posterori that actually only the differential equation, that he calls (A), can occur:

$$(A) \qquad\qquad (y')^r = t^j A(y), \text{ where } r, j \in \mathbb{Z} \text{ and } A(t) \in \mathbb{C}(t).$$

Ritt's proof of Theorem 1.1 is extremely technical and it may be difficult to understand how the differential equation (A) is singled out at the very last line of the paper. We think that the Galoisian proof presented below, which is much shorter modulo the Galois theory, may give a different insight on the existence of the differential equation (A). The price to pay for a theoretical understanding of the existence of the equation (A) is the algorithmic nature of Ritt's proof. Another proof of Ritt theorem can be found in [Cas06, Cas15], where the same three differential equations as in Ritt's paper appear.

The purpose of this paper is to give a Galoisian proof of the following theorem, from whom one can deduce Ritt's theorem (see §2 below):

Theorem 1.2. *Let $\sigma \in \mathbb{C}[[t]]$ be a formal solution of a functional equation of the form (1.1), for some $R(t) \in \mathbb{C}(t)$ not a homography, such that $R(0) = 0$, $R'(0) = q \neq 0$ not a root of unity. The function σ is differentially algebraic over $\mathbb{C}(t)$ if and only if it is solution of a differential equation "of Ritt type (A)", with $r \neq 0$.*

We close the paper by proving a generalisation of the last statement to the case of a series $R(t) \in \mathbb{C}[[t]]$ algebraic over $\mathbb{C}(t)$, such that $R(0) = 0$ and $R'(0) = q$, with $q \in \mathbb{C}$, $q \neq 0$ not a root of unity.

The paper is organized as follows. In §2 we show how to deduce Theorem 1.1 from Theorem 1.2. In §3 we recall some basic facts of difference Galois theory, that are used in §4 to prove Theorem 1.2. Finally, in §5, we generalize Theorem 1.2 to the case of an algebraic function R.

2 How to deduce Theorem 1.1 from Theorem 1.2

The proof below follows the main ideas of Ritt (see [Rit26, §12]), but it is easier than the original proof, since we are left from the beginning with the simplest differential equation among the three found by Ritt. For the reader convenience we give all the details, even the proofs of the lemmas below that are already in the original reference, and are quite classical.

Let $R(t) \in \mathbb{C}(t)$ be such that $R(0) = 0$ and $R'(0) = q \in \mathbb{C}$, with $|q| > 1$. We consider the only solution $\sigma \in t + t^2\mathbb{C}[[t]]$ of the functional equation (1.1), namely:

$$\sigma(qt) = R(\sigma(t)).$$

As we have already pointed out in the introduction, σ is the expansion at zero of a uniform meromorphic function over the whole $\mathbb{C}$.

Lemma 2.1 ([Rit26, §1]). *The following assertions are equivalent:*

1. *The Poincaré function σ is rational.*

2. *σ is a homography.*

3. *$R(t)$ is a homography.*

Proof. If $R(t)$ is a homography, it must have the form $R(t) = \frac{qt}{at+1}$, for some $a \in \mathbb{C}$. Then $\sigma(t) = \frac{(q-1)t}{at+(q-1)}$. We conclude proving by contradiction that, if σ is rational, then $R(t)$ is a homography. First, notice that Equation (1.1) implies that:

$$(2.1) \qquad\qquad \sigma(q^2 t) = R(R(\sigma(t))).$$

We suppose that $\sigma \in \mathbb{C}(t)$ and assume that the degree of the numerator of R, after eliminating any common factor with the denominator, is at least 2. In this case, $R(t)$ has at least two finite zeros, namely 0, which is

simple zero by assumption, and $a_1 \neq 0$. The rationality of R implies that there exists a_2 such that $R(a_2) = a_1$. Note that $a_2 \notin \{0, a_1\}$ and $R(R(a_2)) = 0$. The rationality of σ implies that there exists b_i such that $\sigma(b_i) = a_i$, for $i \in \{1, 2\}$. Since $b_1 \neq b_2$, b_1 and b_2 cannot be both equal to ∞. If b_1 is finite, we deduce from (1.1) that $\sigma(qb_1) = R(\sigma(b_1)) = 0$. Recursively we obtain that $\sigma(q^n b_1) = 0$ for any positive integer n, and hence that σ has an infinite number of zeros, which contradicts its rationality. If b_2 is finite, we use (2.1) to conclude that $\sigma(q^{2n} b_2) = 0$ for any positive integer n, and hence that σ has an infinite number of zeros, which contradicts its rationality. Therefore the numerator of R cannot have degree greater than 1, and it is equal to qt. If the denominator of $R(t)$ is a polynomial of degree at least 2, then the numerator of $R(R(t))$ has degree at least 2. Applying the previous reasoning to $R \circ R$ and Equation (2.1), we obtain a contradiction. So both the numerator and the denominator of R have degree at most 1, which means that R is a homography. $\square$

Corollary 2.2 ([Rit26, §1 to §3]). *If $R(t)$ is not a homography, then:*

1. *σ has an infinite set of zeros and an essential singularity at ∞.*

2. *σ is transcendental.*

Proof. Let us suppose that the numerator and the denominator of $R(t)$ do not have common factors. If R is not a homography, then either the numerator or the denominator of R has degree at least 2. As in the proof of the previous lemma, we conclude that σ has an infinite set of zeros, that accumulate at ∞. Since σ is not identically zero, it must have an essential singularity at ∞. This also implies that σ is transcendental. $\square$

Proof of Theorem 1.1. By Theorem 1.2, we have $(\sigma')^r = t^j A(\sigma)$, for some $r, j \in \mathbb{Z}$, with $r \neq 0$, and $A(t) \in \mathbb{C}(t)$, and hence:
$$0 = \mathrm{ord}_{t=0}(\sigma')^r = j + \mathrm{ord}_{t=0}A(t)\,\mathrm{ord}_{t=0}\sigma(t).$$

We conclude that $\mathrm{ord}_{t=0}A(t) = -j$. We know from the previous corollary that σ has a finite zero $b \neq 0$. Let $p := \mathrm{ord}_{t=b}\sigma(t) \geq 1$. We observe that:
$$r\,\mathrm{ord}_{t=b}\sigma'(t) = \mathrm{ord}_{t=0}A(t)\,\mathrm{ord}_{t=b}\sigma(t) = -jp,$$

hence $r(p-1) + jp = 0$. We consider the change of variable $t = u^p$ and we set $z(u) := \sigma(u^p)$. A direct calculation shows that:

$$(2.2) \qquad\qquad z(q^{1/p}u) = R(z(u)) \text{ and } z'(u)^r = p^r A(z(u)).$$

Notice that for any non-zero constant $\widetilde{u}$, the function $z(u + \widetilde{u})$ is also a solution of the differential equation above. Since σ has an essential singularity at ∞, then σ takes all the values in $\mathbb{C}$, with at most one exception. The same holds for $z(u)$. Therefore the unique solution of the differential equation $y'(u)^r = p^r A(y(u))$ with initial condition $y(u_0) = c$, with $u_0, c \in \mathbb{C}$, is constructed in the following way: we find u_c such that $z(u_c) = c$ and we chose the solution $z(u - u_0 + u_c)$ of the differential equation above. Given the freedom in the choice of both u_0 and c, one avoids the missing value of $z(u)$ and concludes that all solutions of $y'(u)^r = p^r A(y(u))$ are obtained composing $z(u)$ with a translation.

By construction, the solution $z(u)$ has a non-trivial monodromy. Let $\widetilde{z}(u)$ be another branch of $z(u)$. We observe that $\widetilde{z}(u)$ is solution of the system (2.2), therefore $\widetilde{z}(u) = z(u + \widetilde{u})$, for some non-zero $\widetilde{u} \in \mathbb{C}$. The uniqueness of the analytic continuation implies that $\widetilde{z}(q^{1/p}u) = R(\widetilde{z}(u))$ and hence that:
$$z(q^{1/p}u + \widetilde{u}) = \widetilde{z}(q^{1/p}u) = R(\widetilde{z}(u)) = R(z(u + \widetilde{u})) = z(q^{1/p}(u + \widetilde{u})).$$

We deduce that z is periodic of period $(q^{1/p} - 1)\widetilde{u}$. We conclude as Ritt does, using his result [Rit22] on the classification of periodic Poincaré functions. $\square$

3 Elements of Galois theory of difference equations

For an introduction to the Galois theory of difference equations, we refer the reader to [vdPS97], or to [OW15, §2], where the authors make very general assumptions. The setting considered here (as well as the notation) matches the approach developed in [DV19, §2 to §5], so we are going to refer to it. The only difference with [DV19] is that our field of constants C is algebraically closed. For this reason we can naively identify the Galois groups with their C-points, which makes things slightly easier. We remind below the notions that are essential to the understanding of the proof in the next section.

Let $\mathbb{F}/\mathbb{K}$ be a field extension, such that $\mathbb{F}$ comes equipped with an endomorphism $\Phi : \mathbb{F} \to \mathbb{F}$, which induces a non-periodic endomorphism of $\mathbb{K}$. It means that there exists $x \in \mathbb{K}$ such that $\Phi^n(x) \neq x$, for any non-zero

integer n. We suppose that the field C of elements of $\mathbb{F}$ that are left invariant by Φ is algebraically closed and that $C \subset \mathbb{K}$. We consider the linear system of the form

$$(3.1) \qquad \Phi \vec{y} = \begin{pmatrix} a_1 & b \\ 0 & a_2 \end{pmatrix} \vec{y},$$

where $a_1, a_2, b \in \mathbb{K}$, with $a_1 a_2 \neq 0$, and we suppose that there exists an invertible matrix $\begin{pmatrix} z_1 & w \\ 0 & z_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F})$ that satisfies (3.1).

Definition 3.1 (see [DV19, Def. 3.5]). We call Picard-Vessiot ring of (3.1) over $\mathbb{K}$ the ring $\mathcal{R} = \mathbb{K}[z_1^{\pm 1}, z_2^{\pm 1}, w] \subset \mathbb{F}$. We define the Galois group of (3.1) to be:

$$(3.2) \qquad G := \{\varphi : \mathcal{R} \to \mathcal{R}, \text{ automorphism of } \mathbb{K}\text{-algebras, such that } \varphi \circ \Phi = \Phi \circ \varphi\}.$$

The elements of G extend to automorphisms of the field of fractions $\mathcal{L}$ of $\mathcal{R}$.

The system (3.1) boils down to the equations $\Phi(z_i) = a_i z_i$, for $i = 1, 2$, and $\Phi(w) = a_1 w + b z_2$. Any $\varphi \in G$, being a ring automorphism, must leave globally invariant the space of solutions of (3.1). Therefore there exists non-zero $c_i \in C$ such that $\varphi(z_i) = c_i z_i$, for $i = 1, 2$. As far as $\varphi(w)$ is concerned, it must be a solution of $\Phi(y) = a_1 y + b\varphi(z_2) = a_1 y + b c_2 z_2$, hence there exists $d \in C$ such that $\varphi(w) = d z_1 + c_2 w$. We conclude that

$$\varphi \begin{pmatrix} z_1 & w \\ 0 & z_2 \end{pmatrix} = \begin{pmatrix} z_1 & w \\ 0 & z_2 \end{pmatrix} \begin{pmatrix} c_1 & d \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} c_1 z_1 & d z_1 + c_2 w \\ 0 & c_2 z_2 \end{pmatrix},$$

for some $\begin{pmatrix} c_1 & d \\ 0 & c_2 \end{pmatrix} \in \mathrm{GL}_2(C)$.

We now state the main properties of the Galois group of a functional equation:

Theorem 3.2 ([DV19, Thm. 4.9 and 5.3]). *1. The Galois group G is an algebraic subgroup of $\mathrm{GL}_2(C)$, and its dimension as an algebraic variety over C is equal to the transcendence degree of $\mathcal{L}/\mathbb{K}$.*

2. $\mathbb{K} = \{f \in \mathcal{L} : \varphi(f) = f \ \forall \varphi \in G\}$.

Example 3.3. Let us consider a special case of the system (3.1), with $b = 0$ and, therefore, $w = 0$. In this case the Picard-Vessiot ring coincides with $\mathcal{R} := \mathbb{K}[z_1^{\pm 1}, z_2^{\pm 1}]$ and its Galois group G is a subgroup of the group of the invertible diagonal matrices of rank 2, that we can naively identify with $(C^*)^2$. It means that for any automorphism $\varphi \in G$ there exist two non-zero constants $c_1, c_2 \in C$ such that $\varphi(z_i) = c_i z_i$, for $i = 1, 2$.

The solutions z_1, z_2 are algebraically dependent over $\mathbb{K}$ if and only if G has dimensions 0 or 1, or equivalently if it is a proper algebraic subgroup of $(C^*)^2$. We know that the proper algebraic subgroups of $(C^*)^2$ are defined by equations of the form $X_1^{\alpha_1} X_2^{\alpha_2} = 1$, for some $\alpha_1, \alpha_2 \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$. It means that $c_1^{\alpha_1} c_2^{\alpha_2} = 1$. We conclude from the theorem above that $z_1^{\alpha_1} z_2^{\alpha_2} \in \mathbb{F}$ is invariant under any automorphism of the Galois group G and hence that $z_1^{\alpha_1} z_2^{\alpha_2} \in \mathbb{K}$.

Example 3.4. If in (3.1) we set $a_1 = a_2 = 1$, then we can take $z_1 = z_2 = 1$. The Picard-Vessiot ring boils down to $\mathcal{R} = \mathbb{K}[w]$ and the Galois group G is a subgroup of the group of matrices $\left\{ \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}, d \in C \right\}$, that we can identify to $(C, +)$. It means that for every $\varphi \in G$, there exists a constant $d \in C$ such that $\varphi(w) = w + d$.

The solution w is algebraically dependent over $\mathbb{K}$ if and only if G is a proper algebraic subgroup of $(C, +)$, but the only proper algebraic subgroup of $(C, +)$ is the trivial group 0. Hence, if w is algebraic over $\mathbb{K}$, then $d = 0$ and w is tautologically left fixed by all morphisms of G. We conclude that $w \in \mathbb{K}$.

4 Proof of Theorem 1.2

Let C be an algebraically closed field and $\mathbb{F} := C((x))$. We fix a formal power series $R \in \mathbb{F}$ such that R is not a homography, $R(0) = 0$, $R'(0) = q \neq 0$ is not a root of unity, so that we can define the morphism:

$$\Phi_R : \begin{array}{ccc} \mathbb{F} & \to & \mathbb{F}, \\ f & \mapsto & f(R(x)). \end{array}$$

Notice that Φ_R is an automorphism of $\mathbb{F}$. Moreover, Φ_R is not periodic.

Lemma 4.1. *The field of constants $\mathbb{F}^{\Phi_R} := \{f \in \mathbb{F} : \Phi_R(f) = f\}$ of $\mathbb{F}$ with respect to Φ_R coincides with C.*

Proof. Let $f \in \mathbb{F} \smallsetminus C$ be such that $f(R(x)) = f(x)$. Replacing f with $f - f(0)$, we can suppose that f has no constant term and, replacing f with its inverse for the Cauchy product, we can suppose that $f = \sum_{n \geq N} f_n x^n$, for some positive integer N that we chose so that $f_N \neq 0$. The coefficient of x^N in $f(R(x))$ is $f_N q^N$. We deduce from $f(R(x)) = f(x)$ that $f_N q^N = f_N$, with $q^N \neq 0, 1$, and hence that $f_N = 0$, against our assumption. We conclude that, if f has no constant term, then $f = 0$. This means exactly that $\mathbb{F}^{\Phi_R} = C$. $\qquad\square$

Let $\mathbb{K} := \mathbb{C}(x)$ be the field of rational functions. We assume that R is (the expansion of) a rational function. In this case Φ_R an endomorphism of $\mathbb{K}$ and we consider the functional equation:

$$(4.1) \qquad\qquad \Phi_R(y_0(x)) = q y_0(x).$$

We use the notation y_0 for the unknown function for reasons that will be clearer in a few lines. The equation above has a formal solution $\tau \in \mathbb{F}$. It satisfies necessarily $\tau(0) = 0$. Notice that τ is determined up to a multiplicative constant. We have:

Theorem 4.2. *Let $\tau \in \mathbb{F}$ be a formal solution of (4.1). The following assertions are equivalent:*

1. *τ is differentially algebraic over $C(x)$.*

2. *τ satisfies a differential equation with coefficients in $C(x)$ of order 1.*

3. *τ is solution of the differential equation $(y')^r = A(x) y^j$, for some $(r, j) \in \mathbb{Z}^2$, with $r \neq 0$, and $A(x) \in C(x)$.*

Proof. Notice that the implications $3 \Rightarrow 2 \Rightarrow 1$ are tautological. Proving that $1 \Rightarrow 3$ would end both the proof of this theorem and of Theorem 1.2: to achieve this purpose we will rather prove that $1 \Rightarrow 2 \Rightarrow 3$.

We start proving that $2 \Rightarrow 3$. We consider the system of functional equations

$$(4.2) \qquad\qquad \begin{cases} \Phi_R(y_0) = q y_0, \\ \Phi_R(y_1) = \dfrac{q}{R'} y_1. \end{cases}$$

We are in the case of Example 3.3. The fact that τ is solution of a differential equation of order 1 means that the system above has a basis of solutions, namely τ, τ', which are algebraically dependent over $\mathbb{K}$. Following the example, we conclude that $\tau^{\alpha_1}(\tau')^{\alpha_2} \in \mathbb{K}$, for some integers α_1, α_2, which cannot be simultaneously zero. If $\alpha_2 \neq 0$, it is enough to rephrase the latter statement in Ritt's notation: There exist $r, j \in \mathbb{Z}$, with $r \neq 0$, and $A(x) \in \mathbb{K}$ such that τ is solution of the differential equation $(y')^r = A(x) y^j$, as claimed. On the other hand, if $\alpha_2 = 0$, then $\tau^{\alpha_1} \in \mathbb{K}$, and we can conclude by taking the logarithmic derivative.

We now prove that $1 \Rightarrow 2$. Notice that deriving $\Phi_R(y_0) = q y_0$, calling y_k the k-th derivative of y and using the Faà di Bruno's formula we obtain:

$$(\Phi_R(y_0))^{(n)} = \sum_{k=1}^{n} B_{n,k}(R', \ldots, R^{(n-k+1)}) \Phi_R(y_k) = q y_n,$$

where $B_{n,k}(x_1, \ldots, x_{n-k+1})$ are the Bell polynomials defined by the multivariate identity: $\exp\left(\sum_{j=1}^{\infty} x_j \frac{t^j}{j!}\right) = \sum_{n \geq k \geq 0} B_{n,k}(x_1, \ldots, x_{n-k+1}) \frac{t^n}{n!}$. As $B_{n,n}(x_1) = x_1^n$, replacing the $\Phi_R(y_k)$'s recursively up to y_{n-1}, we obtain an expression of the form:

$$(4.3) \qquad\qquad \Phi_R(y_n) = \frac{q}{(R')^n} y_n + \sum_{k=1}^{n-1} A_{n,k}(x) y_k,$$

where $A_{n,k}(x) \in C(x)$ is a rational function, which is actually a rational expression in the derivatives of R.

Now let us suppose that τ is solution of an algebraic differential equation of order n. Notice that if τ is algebraic, i.e., if $n = 0$, then we get an algebraic differential equation of order 1 by derivation. If $n = 1$ there is nothing to prove, therefore we assume now that $n \geq 2$.

We set $\mathbb{K}_n := \mathbb{K}(\tau, \tau', \ldots, \tau^{(n-1)})$, and $\mathbb{L}_n := \mathbb{K}(y_0, y_1, \ldots, y_{n-1})$, where the y_i are algebraically independent variables over $\mathbb{K}$. By assumption, τ is algebraic over $\mathbb{K}_n$: We are going to prove that in fact $\tau^{(n)} \in \mathbb{K}_n$. To this purpose, we set $b := \sum_{k=1}^{n-1} A_{n,k}(x) \tau^{(k)} \in \mathbb{K}_n$ and $z = (\tau')^n \tau^{1-n} \in \mathbb{K}_2 \subset \mathbb{K}_n$, to simplify the notation. We deduce from the functional equation above that $\omega_n := \frac{\tau^{(n)}}{z}$ verifies the functional equation

$$(4.4) \qquad\qquad \Phi_R(\omega_n) = \omega_n + \frac{b(R')^n}{qz}.$$

We are in the situation of Example 3.4. Since ω_n is algebraic over $\mathbb{K}_n$, we conclude that $\omega_n \in \mathbb{K}_n$. Since $z \in \mathbb{K}_n$, we conclude that also $\tau^{(n)} \in \mathbb{K}_n$, as announced.

We claim that $\tau^{(n)} \in \mathbb{K}_n$ implies the existence of a differential equation satisfied by τ and of order strictly smaller than n. Therefore iterating the reasoning a finite number of times we must get a differential equation of order 0 or 1, which ends the proof. Notice that Formula (4.3) allows to extend Φ_R from $\mathbb{K}$ to $\mathbb{L}_n$, for any n, setting $\Phi_R(y_i) := \frac{q}{(R')^i} y_i + \sum_{k=1}^{i-1} A_{i,k}(x) y_k$. Since $\tau^{(n)} \in \mathbb{K}_n$, there exist two coprime polynomials $U, V \in \mathbb{K}[y_0, \ldots, y_{n-1}]$, such that the equation $U y_n + V = 0$ has $(\tau, \tau', \ldots, \tau^{(n)})$ as solution. Let $S = U y_n + V \in \mathbb{L}_n[y_n]$ and $T = \phi_R(S) \in \mathbb{L}_n[y_n]$. Both polynomials are annihilated by $(\tau, \tau', \ldots, \tau^{(n)})$, since the evaluation at $(\tau, \tau', \ldots, \tau^{(n)})$ commutes to the action of Φ_R. Moreover we can suppose without loss of generality that the coefficients of S do not have a pole at zero and that at least one of them does not have a zero at 0. Let $R \in \mathbb{L}_n$ be the resultant of S, T with respect to y_n. By property of the resultant, there exists $A, B \in \mathbb{L}_n[y_n]$ such that $AS + BT = R$, therefore τ is a solution of $R = 0$, seen as a differential equation as we have done so far. If $R \neq 0$, this is a differential equation of order at most $n - 1$ for τ, and we have proved our claim. We need to consider the case $R = 0$, which implies that S and T have a non-constant common factor over $\mathbb{L}_n[y_n]$. Notice that S is irreducible over $\mathbb{L}_n$, because it is of degree 1 in y_n and the coefficients U, V are coprime over $\mathbb{K}$. Hence, S divides T in $\mathbb{L}_n[y_n]$. As S, T have same degree in y_n there exists $W \in \mathbb{L}_n$ such that $T = WS$. The polynomials S, T also have same total degree, hence $W \in \mathbb{K}$. This means that, if $u y^{\alpha_0} y_1^{\alpha_1} \ldots y_n^{\alpha_n}$, with $u \in \mathbb{K}$, is the greatest monomial of S (for the lexicographical order, with y_n the greatest variable), then the greatest monomial of T is $\phi_R(u) q^{d_0} \left(\frac{1}{R'}\right)^d y^{\alpha_0} y_1^{\alpha_1} \ldots y_n^{\alpha_n}$, where $d_0 = \sum_{i=0}^n \alpha_i$ and $d = \sum_{i=1}^n i \alpha_i$. Moreover $\alpha_n = 1$ and therefore $d \neq 0$. We get $W = \frac{T}{S} = \frac{\phi_R(u)}{u} \frac{q^{d_0}}{(R')^d}$. For any $P(x) \in \mathbb{C}[x]$, we denote by S_P and T_P the evaluation of S and T, respectively, at P and its derivatives. We obtain $\phi_R(S_P) = T_P = W S_P$, hence $\phi_R(S_P) = \frac{\phi_R(u)}{u} \frac{q^{d_0}}{(R')^d} S_P$ and finally:

$$(4.5) \qquad \phi_R\left(\frac{S_P}{u}\right) = \frac{q^{d_0}}{(R')^d} \frac{S_P}{u}.$$

The general solution to (4.5) is $c \frac{(\tau')^d}{\tau^{d-d_0}}$, where $c \in \mathbb{C}$. We deduce that there exists $c \in \mathbb{C}$ such that:

$$\frac{S_P}{u} = c \frac{(\tau')^d}{\tau^{d-d_0}}.$$

It follows from our choice of S that there exists $(z_0, \ldots, z_n) \in \mathbb{C}^{n+1}$ such that $S(0, z_0, \ldots, z_n) \neq 0$. For any $P \in \mathbb{C}[z]$, such that $(P(0), \ldots, P^{(n)}(0)) = (z_0, \ldots, z_n)$, we have $S_P \neq 0$. For such a P, the constant c in the identity above must be non zero. If we set $A = \frac{S_P}{uc} \in \mathbb{K}$, $r = d \neq 0$, and $j = d - d_0$, we prove that τ satisfies the differential equation $(\tau')^r = A \tau^j$, that not only has order 1 but it is already of "type (A)". $\qquad \square$

We deduce theorem Theorem 1.2 from the statement above.

Proof of Theorem 1.2. Let σ be the inverse of τ for the composition. First of all, let us notice that σ is differentially algebraic over $C(t)$ if and only if τ is differentially algebraic over $C(x)$ (see [BR86, page 344] or [Moo96, page 55, (n)]). We consider the local change of variable $t = \tau(x)$ in (1.1), or equivalently $x = \sigma(t)$, which transforms (4.1) and $(\tau')^r = A(x)\tau^j$ into (1.1) and $(\sigma')^{-r} = t^j A(\sigma)$, respectively. $\qquad \square$

5 The algebraic case

We change a little bit the notation with respect to the previous section. Let us consider the relative closure $\mathbb{K}$ of $C(x)$ inside $\mathbb{F} := C((x))$ and $R(x) \in \mathbb{K}$, such that R is not a homography, $R(0) = 0$, $R'(0) = q \neq 0$ is not a root of unity. Then the functional equation

$$\tau(R(x)) = q\tau(x)$$

has a formal solution at 0.

We can define the automorphism Φ_R of $\mathbb{F}$ as in the previous section. Then Φ_R induces an automorphism of $\mathbb{K}$ and the field of constants is C, as in Lemma 4.1. Reasoning word by word as in the previous section one can prove:

Theorem 5.1. *Let $\tau(x)$ be a formal solution of $\tau(R(x)) = q\tau(x)$ in $C[[x]]$. If $\tau(x)$ is differentially algebraic over $\mathbb{K}$, then it satisfies a differential equation of the form $(y')^r = y^j A(x)$, where r, j are integers, with $r \neq 0$, and $A(x) \in \mathbb{K}$.*

Remark 5.2. The fact that $\mathbb{K}/C(x)$ is algebraic implies that being differentially algebraic over $\mathbb{K}$ is equivalent to being differentially algebraic over $C(x)$. Since $A(x) \in \mathbb{K}$, there exists $P(x, T) \in C[x, T]$ such that $P(x, A(x)) = 0$. Then $P(x, (y')^r y^{-j}) = 0$ provides a differential equation for τ over $C(x)$.

References

[BR86]   Michael Boshernitzan and Lee A. Rubel, *Coherent families of polynomials*, Analysis **6** (1986), no. 4, 339–389.

[Cas06]   Guy Casale, *Enveloppe galoisienne d'une application rationnelle de* $\mathbb{P}^1$, Publ. Mat. **50** (2006), no. 1, 191–202.

[Cas15]   ———, *El grupoide de galois de una transformacin racional*, 2015, VIII Escuela Doctoral interconti-nental de Matematicas PUCP-UVa.

[DV19]   Lucia Di Vizio, *Difference Galois theory for the applied mathematician*, In "Arithmetic and geometry over local fields", LNM, Springer   (2019), 20 pages, to appear.

[Fer21]   Gwladys Fernandes, *A survey on the hypertranscendence of the solutions of the Schröder's, Böttcher's and Abel's equations*, Proceedings of the conference "Transient Transcendence in Transylvania". Pro-ceedings in Mathematics & Statistics, Springer. (2021), 31 pages.

[Moo96]   Eliakim Hastings Moore, *Concerning transcendentally transcendental functions*, Mathematische An-nalen **48** (1896), no. 1-2, 49–74.

[OW15]   Alexey Ovchinnikov and Michael Wibmer, σ-*Galois theory of linear difference equations*, Int. Math. Res. Not. IMRN (2015), no. 12, 3962–4018.

[Poi90]   Henri Poincaré, *Sur une classe nouvelle de transcendantes uniformes*, Journal de Mathématiques pures et appliquées **6** (1890), 313–365.

[Rit22]   Joseph F. Ritt, *Periodic functions with a multiplication theorem*, Trans. Amer. Math. Soc. **23** (1922), no. 1, 16–25.

[Rit26]   ———, *Transcendental transcendency of certain functions of Poincaré*, Mathematische Annalen **95** (1926), no. 1, 671–682.

[vdPS97]   Marius van der Put and Michael F. Singer, *Galois theory of difference equations*, Springer-Verlag, Berlin, 1997.