Difference Galois theory for the "applied" mathematician

Lucia Di Vizio

October 9, 2020

Abstract

The lecture notes below correspond to the course given by the author in occasion of the VIASM school on Number Theory (18-24 June 2018, Hanoi). We have chosen to omit the proofs that are already presented in details in many references in the literature, although they were explained during the lectures, and we have devoted more space to statements useful in the applications. The applications concern many different mathematical settings, where linear difference equations naturally arise. We cite in particular the case of Drinfeld modules, which is considered in [Pel] and [TR].

Contents

1 Introduction

The initial data of classical Galois theory are a field K, let's say of characteristic 0, and an irreducible polynomial $P \in K[x]$, with coefficients in K. Then *the* minimal field extension L of K containing a *full set* of roots of P is constructed and one defines the Galois group G of L/K, namely the group of the field automorphisms of L that fix the elements of K. The group G is finite and acts on L by shuffling the roots of P. The idea behind this construction is that the structure of the group G should reveal hidden algebraic relations among the roots of P, other than the evident relations given by P itself.

The same kind of philosophy applied to functional equations has been the starting point of differential Galois theory, first, and difference Galois theory, later. The references are numerous and it is almost impossible to list them all. We refer to [vdPS03], for the differential case, and to [vdPS97] and [HSS16], for the difference case.

Let K be a base field and τ be an endomorphism of K. We consider a linear difference equation $\tau(Y) = AY$, where A is a square invertible matrix with coefficients in K and Y is a square matrix of unknowns. The usual approach in Galois theory of difference equations is to construct an abstract K-algebra L/K containing the entries of a fundamental (i.e., invertible) matrix of solutions, under the assumption that the characteristic of K is zero, that the field of constants k is algebraically closed and that τ is surjective. The idea is that, in order to study the properties of the solutions a difference equation, it is not "important" to solve it, but only to understand the structure of its Galois group. However, in applications, it usually happens that a set of solutions is given in some specific K-algebra: When that's the case, it is not always easy to understand which properties transfer from the abstract solutions to the ones that we have found.

In this paper we suppose that we have a fundamental solution is some field L/K, equipped with an extension of τ. The divergence between the classical approach and the apparently more pedestrian approach that we are considering here, starts immediately: Indeed in general we cannot assume that the field L exists and only the existence of a pseudo field is ensured (see Remark 3.6 below). In [CHS08], the authors reconcile these two points of view and the point of view of model theory: They construct a group using given solutions in a specific algebra and compare it with the group constructed in [vdPS97], but they assume that τ is an automorphism and the statements on the comparison of the Galois groups are not easy to apply in other settings.

More recently, a very general abstract approach has been considered by A. Ovchinnikov and M. Wibmer in [OW15, §2.2], where, in contrast with the more classical references, the authors do not make any assumption on the characteristic of the field, they do not require that the endomorphism is surjective, and they do not assume that the constants are algebraically closed. They do not even assume that K is a field, but only that K is a pseudo field.

M. Papanikolas in [Pap08, §4] chooses a framework which is in between the two examples above: He works on a field K equipped with an automorphisms τ, but the characteristic can be positive and the field of constants is not necessarily algebraically closed. Moreover he supposes that he already has a fundamental solution in a field extension of K. We will consider the same setting as Papanikolas, apart from the fact that we only ask that τ is an endomorphism. This seems to be a reasonable framework for many applications. For the proofs, we usually refer to [OW15], which is the reference with more general assumptions. Notice that Papanikolas has a more geometric approach while Ovchinnikov and Wibmer prefer algebraic arguments.

Finally we point out that we assume that the characteristic is zero in §6.2 and §7 and that τ is an automorphism in §8.

Remarks on the content and the organization of the text below. The text below is meant to be a guide to the existing literature. From this perspective, I will give references for the proofs, rather than writing a self-contained exposition. I'm addressing with particular attention readers that need to apply Galois theory of difference equations, therefore a large space is devoted to statements that may be useful in applications.

The exposition is divided in three parts. The first part quickly explains the fundamentals results and ideas of difference Galois theory. In order to be precise and correct I have been obliged to use some more sophisticated tools. The second part, devoted to applications, is more accessible and applies the statements of the first part as black boxes. We conclude with a last paragraph on the role of normal subgroups in the Galois correspondence.

Acknowledgements I'm indebted to the organizers of the VIASM school on Number Theory, in particular to Bruno Anglès and Tuan Ngo Dac for their invitation both to give the course and to write the this paper. I'd like to thank the participants of the *Groupe de travail autour des marches dans le quart de plan*, who have endured several talks on this topic, that have influenced the text below. In particular, I'm grateful to Alin Bostan, Frédéric Chyzac and Marni Mishna for their remarks and their attentive reading of various drafts of this survey and to the anonymous referees for the many useful and constructive comments.

2 Glossary of difference algebra

We give here a short glossary of terminology in difference algebra. Classical references are [Coh65] and [Lev08].

We consider a field F equipped with an endomorphism τ. We will call the pair (F, τ) a τ-field or a difference field, when the reference to τ is clear from the context. The set $k = \{f \in F : \tau(f) = f\}$, also denoted F^τ, is naturally a field and is called the field of constants of F. All along this exposition, we will assume that τ is non-periodic on F (i.e. there exists $f \in F$ such that for any $n \in \mathbb{Z}$ we have $\tau^n f \neq f$) and we won't assume that k is algebraically closed. The example below will be our playground until the end of the paper.

Example 2.1. We consider $k = \mathbb{C}$, $F = k(x)$ and τ a non-periodic homography acting on x, so that $\tau(f(x)) = f(\tau(x))$. Supposing that τ has one or two fixed points, we can assume without loss of generality that $\tau(x) = x+1$ or that $\tau(x) = qx$, for some $q \in \mathbb{C} \setminus \{0, 1\}$, not a root of unity.

We will add the prefix τ to the usual terminology in commutative algebra, to signify the invariance with respect to τ. For instance:

- A τ-subfield K of a τ-field F is a subfield of F such that τ induces an endomorphism of K, i.e., such that $\tau(K) \subset K$.
- A τ-K-algebra is a K-algebra equipped with an endomorphism extending τ (which we still call τ for simplicity).

- An ideal I of a τ-K-algebra R is a τ-ideal if $\tau(I) \subset I$.
- A τ-K-algebra R is τ-simple if its only τ-ideals are R and 0.

Example 2.2. For any $x \in F$ transcendental over k, such that $\tau(x) \in k(x)$ and that for any $n \in \mathbb{Z}$ we have $\tau^n(x) \neq x$, we can consider the field $K := k(x)$, on which τ induces a non-periodic endomorphism. Since we don't ask τ to be surjective, the situation is a little bit more general than Example 2.1. For instance τ can be the Mahler operator $\tau(x) = x^\kappa$, where $\kappa \geq 2$ is an integer.

For any positive integer n, we can consider $k_n = F^{\tau^n}$ and the difference fields $(K_n := k_n(x), \tau)$ and $(K_n := k_n(x), \tau^n)$.

Sometimes it is useful to consider (k, id), where id stands for the identity map, as a difference field, therefore we will call it a trivial τ-field. In general we will say that a k-algebra is equipped with a trivial action of τ, when τ acts on it as the identity. For further reference we state the following lemma:

Lemma 2.3. *Let B be a k-algebra endowed with a trivial action of τ, K a τ-subfield of F such that $K^\tau = k$ and let $R \subset F$ be a τ-K-algebra. Then $R \otimes_k B$ has a natural structure of τ-K-algebra defined by*

$$\tau(r \otimes b) = \tau(r) \otimes b, \text{ for any } r \in R \text{ and } b \in B. \tag{2.1}$$

Moreover $R \otimes_k B \hookrightarrow F \otimes_k B$ and $(R \otimes_k B)^\tau = k \otimes_k B \cong B$.

Remark 2.4. We have chosen to detail the proof, even if the lemma above is included in many references and could partially be proved invoking the flatness of F over k. The argument is indeed an instance of a classical way of reasoning in difference algebra and is useful in many situations.

Proof. Clearly Eq. (2.1) defines a ring endomorphism, that is the tensor product of τ and the identity in the category of rings. Since $R \subset F$, we have a natural map of τ-K-algebras $R \otimes_k B \to F \otimes_k B$. We want to prove that this map is injective. By absurdum, we suppose that the kernel is non-trivial and therefore we choose a non-zero element $\sum_{i=1}^n r_i \otimes b_i \in R \otimes_k B$ in the kernel such that n is minimal, i.e., we suppose that there exists no element of $R \otimes_k B$ in the kernel, that can be written as a sum of less than n elements of the form $r \otimes b \in R \otimes_k B$. This implies in particular that the r_i's are linearly independent over k and that all the r_i's and b_i's are non-zero. Since F is a field, in $F \otimes_k B$ we can multiply by $r_n^{-1} \otimes 1$, hence we have: $1 \otimes b_n + \sum_{i=1}^{n-1} r_i r_n^{-1} \otimes b_i = 0$ in $F \otimes_k B$. We conclude that the image of

$$\sum_{i=1}^{n-1} \left(\tau(r_i r_n^{-1}) - r_i r_n^{-1}\right) \otimes b_i \in R \otimes_k B$$

in $F \otimes_k B$ is zero. The minimality of n, together with the fact that $b_i \neq 0$, implies that $\tau(r_i r_n^{-1}) - r_i r_n^{-1} = 0$ and hence that $r_i r_n^{-1} \in k$ for any $i = 1, \ldots, n-1$. The linear independence of the r_i's over k implies that $n = 1$ and hence that $r_1 \otimes b_1 = 0$ in $F \otimes_k B$, with $r_1 \neq 0$. Since F is a field, $r_1^{-1} \otimes 1 \in F \otimes_k B$ and hence:

$$1 \otimes b_1 = (r_1^{-1} \otimes 1) \cdot (r_1 \otimes b_1) = 0$$

in $F \otimes_k B$, and we obtain the contradiction $b_1 = 0$. This proves the injectivity.

To conclude it is enough to prove that $(R \otimes_k B)^\tau = k \otimes_k B$. First of all, notice that if $r \otimes b \in (R \otimes_k B)^\tau$, with $r \neq 0 \neq b$, then $r \in k$. By absurdum, let us suppose that there exists $\sum_{i=1}^n r_i \otimes b_i \in (R \otimes_k B)^\tau \setminus k \otimes_k B$, such that no r_i belongs to k and n is minimal. Once again, the minimality of n implies that the r_i's and the b_i's are linearly independent over k. Moreover we know that necessarily $n \geq 2$. We conclude that

$$\sum_{i=1}^n (\tau(r_i) - r_i) \otimes b_i = \tau\left(\sum_{i=1}^n r_i \otimes b_i\right) - \left(\sum_{i=1}^n r_i \otimes b_i\right) = 0.$$

There are two possibility: either the $(\tau(r_i) - r_i)$'s are linearly dependent over k or they are not. If they are linearly dependent over k, we can find $\lambda_1, \ldots, \lambda_n \in k$, not all zero, such that $\sum_{i=1}^n \lambda_i(\tau(r_i) - r_i) = 0$. We can suppose without loss of generality that $\lambda_n \neq 0$. It implies that

$$\sum_{i=1}^n \lambda_i r_i = \sum_{i=1}^n \lambda_i \tau(r_i) = \tau\left(\sum_{i=1}^n \lambda_i r_i\right),$$

and hence that $c := \sum_{i=1}^n \lambda_i r_i \in k$. Since the r_i's are linearly independent over k, c is not zero. The k-linearity of the tensor product implies:

$$\begin{aligned} \textstyle\sum_{i=1}^n r_i \otimes b_i &= \textstyle\sum_{i=1}^{n-1} r_i \otimes b_i + \lambda_n^{-1}\left(c - \sum_{i=1}^{n-1} \lambda_i r_i\right) \otimes b_n \\ &= \textstyle\sum_{i=1}^{n-1} r_i \otimes (b_i - \lambda_n^{-1}\lambda_i b_n) + \lambda_n^{-1} c \otimes b_n \in (R \otimes_k B)^\tau. \end{aligned}$$

Because $\lambda_n^{-1}c \otimes b_n \in k \otimes_k B \subset (R \otimes_k B)^\tau$, we conclude that $\sum_{i=1}^{n-1} r_i \otimes (b_i - \lambda_n^{-1}\lambda_i b_n) \in (R \otimes_k B)^\tau$. The minimality of n implies that $b_i = \lambda_n^{-1}\lambda_i b_n$, for any $i = 1, \dots, n-1$. Finally we obtain:

$$\sum_{i=1}^{n} r_i \otimes b_i = \left(\sum_{i=1}^{n} \lambda_n^{-1}\lambda_i r_i \right) \otimes b_n \in (R \otimes_k B)^\tau,$$

and therefore that $\sum_{i=1}^{n} r_i \otimes b_i \in k \otimes_k B$, in contradiction with our choice of $\sum_{i=1}^{n} r_i \otimes b_i$. We still have to consider the case in which $(\tau(r_i) - r_i)$'s are linearly independent over k, with $\sum_{i=1}^{n} (\tau(r_i) - r_i) \otimes b_i = 0$ in $F \otimes_k B$, but we have seen in the first part of the proof that this cannot happen, unless $\tau(r_i) = r_i$, which is against our assumptions. This ends the proof of the whole lemma. □

3 Picard-Vessiot rings

We now consider a field F with an endomorphism $\tau : F \to F$. Our base field will be a τ-subfield K of F, containing $k := F^\tau$, which implies that $K^\tau = k$. We do assume neither that k is algebraically closed, nor that τ induces an automorphism of K, but we assume that τ is non-periodic over K. Moreover we assume that F/k is a separable extension.

Remark 3.1. In the classical theory, one usually assumes that k is algebraically closed, which simplifies a little the theory, although not in a fundamental way. The main difference comes from the fact that the Galois group, that we will define in the following section, is an algebraic group over the field k. Therefore if k is algebraically closed one can avoid a more sophisticated geometric point of view and simply identify the Galois group to a group of invertible matrices with coefficients in k. This remark will become clearer in what follows. We will comment again on the consequences of the fact that k is not algebraically closed.

We also point out that the assumption $F^\tau = K^\tau = k$ is crucial, othewise we may end up introducing new meaningless solutions in the theory. For more details, see Example 3.7 and the proof of Proposition 6.1 below.

We consider a linear difference system

$$\tau(Y) = AY, \text{ where } A \in \mathrm{GL}_d(K), \tag{3.1}$$

and we suppose that *there exists a fundamental solution matrix* $U \in \mathrm{GL}_d(F)$ *of* (3.1). Then the field $L := K(U) \subset F$ is obviously stable by τ. We have made an abuse of notation that we will repeat frequently: By $K(U)$ we mean the field generated over K by the entries of U.

There are two main situations that the readers, according to their background, could keep in mind as a guideline through the text below:

Example 3.2. One can consider the following two classical situations:

1. F is the field of meromorphic functions over $\mathbb{C}$ in the variable x and $\tau : f(x) \mapsto f(x+1)$. Then k is the field of meromorphic 1-periodic functions over $\mathbb{C}$.

2. F is the field of meromorphic functions over $\mathbb{C}^*$ in the variable x and $\tau : f(x) \mapsto f(qx)$, for a fixed complex number $q \in \mathbb{C} \setminus \{0, 1, \text{ roots of unity}\}$. Here k is the field of meromorphic q-elliptic functions over $\mathbb{C}^*$.

In both cases, we can chose K to be any τ-subfield of F, containing k. A typical choice for K is $k(x)$, which is the point of view taken in [CHS08], as far as q-difference equations is concerned.

Let as consider a linear system $\tau(\vec{y}) = A\vec{y}$ with coefficients in K, of the form (3.1). In the settings above, plus the assumption $|q| \neq 1$ in the q-difference case, Praagman proves that $\tau(\vec{y}) = A\vec{y}$ has a fundamental matrix of solutions with coefficients in F. See [Pra86, Theorem 1 and Theorem 3]. This does not mean that all possible solutions are meromorphic. Indeed it is enough to multiply a solution matrix by a matrix whose entries are functions with some essential singularities and that are constant with respect to τ.

Example 3.3. In [Pap08, §4.1] the triple (k, K, F) is called a τ-admissible triple. He is specifically interested in the study of t-motifs and, hence, of the associated triple $(\mathbb{F}_q(t), \mathbb{K}, \mathbb{L})$, defined as follows [Pap08, §2.1]:

- $\mathbb{F}_q(t)$ is the field of rational functions in the variable t and with coefficients in the field $\mathbb{F}_q$ with q elements, where q is an integer power of a prime p;

- $\mathbb{K}$ is the smallest algebraically closed and complete extension of a field of rational functions $\mathbb{F}_q(\theta)$, with respect to the θ^{-1}-adic valuation.

- $\mathbb{L}$ is the field of fractions of the ring of all power series in $\mathbb{K}[[t]]$ convergent on the closed unit disk for the θ^{-1}-adic valuation.

The automorphism τ is the inverse of the Frobenius morphism on the algebraic closure of $\mathbb{F}_q$, sends θ to $\theta^{1/q}$, and is defined on $\mathbb{K}[[t]]$ as

$$\tau\left(\sum_{n\geq 0} a_n t^n\right) = \sum_{n\geq 0} a_n^{1/q} t^n.$$

Finally, it extends to $\mathbb{L}$ by multiplicativity. Then $\mathbb{L}^\tau = \mathbb{K}^\tau = \mathbb{F}_q(t)$, as proved in Lemma 3.3.2 in *loc.cit.*.

We start mentioning a technical but fundamental property of the τ-K-algebra generated by the entries of the solution matrices of (3.1), which allows to reconnect our point of view with the more classical approach of the Picard-Vessiot theory.

Proposition 3.4. *In the notation above, let $U \in \mathrm{GL}_d(F)$ verify $\tau(U) = AU$. Then $R = K\left[U, \det U^{-1}\right] \subset F$ is τ-simple.*

Proof. The statement is a special case of [OW15, Proposition 2.14], as one can see from Definitions 2.2 and 2.4 in *loc. cit.* □

At this point, the reader should pay attention to the terminology in the literature. The ring R in the proposition above and its field of fractions L are a *weak* Picard-Vessiot ring and a *weak* Picard-Vessiot field, respectively, according to [CHS08, Definition 2.1]. Indeed it follows immediately from their definition that $R^\tau = L^\tau = k$. Proposition 3.4 shows that R and L are respectively a Picard-Vessiot ring and a Picard-Vessiot field, following also the definition [OW15, Defintion 2.12]. For the purpose of this paper, we will use a terminology in between [CHS08] and [OW15], knowing that R and L satisfy the definitions in both the cited references, and that, therefore, the results in both references apply here.

Definition 3.5. *A τ-simple τ-K-algebra R is called a Picard-Vessiot ring (for (3.1)) if there exists $V \in \mathrm{GL}_d(R)$ such that $\tau(V) = AV$ and $R = K\left[V, \det V^{-1}\right]$.*

A difference field L is called a Picard-Vessiot field over K (for (3.1)) if $L^\tau = k$ and $L = K(V)$ for a $V \in \mathrm{GL}_d(L)$ such that $\tau(V) = AV$. We will call L/K a Picard-Vessiot extension.

Remark 3.6. If we do not have a field where to find enough solutions of our equation, we have to construct an abstract Picard-Vessiot extension. To do so, one considers the ring of polynomials in the d^2 variables $X = (x_{i,j})$ with coefficients in K. Inverting $\det X$ and setting $\tau(X) = AX$, we obtain a ring $K[X, \det X^{-1}]$ with an endomorphism τ. Any of its quotients by a maximal τ-invariant ideal is a Picard-Vessiot ring of $\tau(\vec{y}) = A\vec{y}$ over K. It is important to notice that the ring R does not need to be a domain. It can be written has a direct sum $R_1 \oplus \cdots \oplus R_r$, such that: $R_i = e_i R$, for some $e_i \in R$ such that $e_i^2 = e_i$; R_i is a domain; there exists a permutation σ of $\{1, \ldots, r\}$ such that $\tau(R_i) \subset R_{\sigma(i)}$. See [vdPS97, Cor. 1.16]. Its total field of fractions is a pseudo field, that is the tensor product of the fraction field of each R_i. For a precise definition of pseudo field, see for instance [OW15, Definition 2.2].

The following example shows the importance of the assumption $L^\tau = k$ in the definition of Picard-Vessiot field.

Example 3.7. Let us consider the equation $\tau(y) = -y$, with k, K and F as above. We suppose that there exists a 2-dimensional k-vector space of solutions of $\tau(y) = -y$ in F, which coincides with $k_2 := F^{\tau^2}$. The Picard-Vessiot field (contained in F) of $\tau(y) = -y$ over K is $L := K(k_2)$.

We could also have considered a field of rational function $F(T)$ with coefficients in F and in the variable T. Since T is transcendental, we can set $\tau(T) = -T$ and obtain an endomorphism of $F(T)$. If we do not assume that the Picard-Vessiot field has the same field of constants than the base field K, we see that $K(k_2)(T)$ is a Picard-Vessiot field for $\tau(y) = -y$, whose field of constants is $k_2(T^2)$. Of course, the solution T is somehow artificial and the extension $K(k_2)(T)/K$ is much bigger (i.e. has many more automorphisms, see next section) than $K(k_2)/K$.

The expected relations between Picard-Vessiot rings and Picard-Vessiot fields are verified. If $R, L \subset F$, the proof is actually straightforward.

Corollary 3.8. [OW15, Proposition 2.15]

1. Let R be domain which is a Picard-Vessiot ring. Then its field of fractions is a Picard-Vessiot field.

2. Let L be a Picard-Vessiot field for (3.1) and let $U \in \mathrm{GL}_d(L)$ be a solution of (3.1). Then $K[U, \det U^{-1}]$ is a Picard-Vessiot ring.

Notice that one can always compare two different Picard-Vessiot rings, up to an algebraic extension of the field of constants:

Proposition 3.9. *Picard-Vessiot rings have the following uniqueness properties:*

1. *Let R_1 and R_2 be two Picard-Vessiot rings for (3.1), both contained in F. Then $R_1 = R_2$.*
2. *Let $R \subset F$ and R' be two Picard-Vessiot rings for (3.1). (Notice that we do not suppose that $R' \subset F$!) Then there exists an algebraic field extension $\widetilde{k}$ of k, containing a copy of $k' := (R')^\tau$, such that $R \otimes_k \widetilde{k}$ is isomorphic to $R' \otimes_{k'} \widetilde{k}$ as a $K \otimes_k \widetilde{k}$-$\tau$-algebra.*

Proof. The first assertion follows from the fact that any pair of fundamental solutions $U, V \in \mathrm{GL}_d(F)$ verifies $\tau(U^{-1}V) = U^{-1}V$, i.e., $U^{-1}V \in \mathrm{GL}_d(k)$. In fact, this implies that $K[U, \det U^{-1}] = K[V, \det V^{-1}] \subset F$. For the second assertion, see [OW15, Theorem 2.16]. Notice that the key-point of its proof is Lemma 2.13 in *loc.cit.*, which ensure that k'/k must be an algebraic extension. □

We give an explicit example to explain the necessity of extending the constants to $\widetilde{k}$ in the statement above.

Example 3.10. Let k be the field of 1-periodic meromorphic functions over $\mathbb{C}$ and let $K = k(x)$. The Picard-Vessiot ring of the equation $\tau(y) = xy$ over K, contained in F, is $R := K[\Gamma(x), \Gamma(x)^{-1}]$, where $\Gamma(x)$ is the Euler Gamma function.

Now let $f(x)$ be a 2-periodic function, algebraic over k, but not meromorphic over $\mathbb{C}$. It means that $f(x)$ lives on an analytic 2-fold covering of $\mathbb{C}$ and has some branching points. The function $c(x) := f(2x)$ is 1-periodic but does not belong to F, and hence not to k. The K-algebra $R' := K[\widetilde{\Gamma}(x), \widetilde{\Gamma}(x)^{-1}]$, where $\widetilde{\Gamma}(x) := c(x)\Gamma(x)$, is a Picard-Vessiot ring for $\tau(y) = xy$. In the notation of the proposition above, we have $k' = k$ and $\widetilde{k} := k(c(x))$. Indeed, $\Gamma(x) \mapsto c(x)\Gamma(x)$ defines an automorphism from $R \otimes_k \widetilde{k}$ to $R' \otimes_k \widetilde{k}$ as $K \otimes_k \widetilde{k}$-algebras.

We close the section with a couple of easy, yet crucial, examples:

Example 3.11. Let a be a non-zero element of K and let us consider the rank-one equation $\tau(y) = ay$. By assumption there exists a solution $z \in F$ verifying $\tau(z) = az$. Hence $K[z, z^{-1}]$ is a Picard-Vessiot ring for $\tau(y) = ay$ and $K(z)$ is a Picard-Vessiot field. Generically, z is transcendental over K, but not always. For instance, if F is the field of meromorphic functions over $\mathbb{C}$ in the variable x, $\tau(f(x)) = f(x+1)$ for any $f \in F$, $K = k(x)$ and $a = -1$, we can take $z = \exp(\pi i x) \in F$. In this case $K(z)$ is a finite extension of degree 2, since $\exp(\pi i x)^2 = \exp(2\pi i x)$ is a 1-periodic function, belonging to k.

Example 3.12. Let $f \in K$ and let us consider the inhomogeneous equation $\tau(y) = y + f$. Such an equation is equivalent to the matrix system

$$\tau(Y) = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} Y,$$

whose fundamental solution is given by $Y = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$, where $z \in F$ verifies $\tau(z) = z + f$. Since $Y^{-1} = \begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix}$, the Picard-Vessiot ring of $\tau(y) = y + f$ is $K[z]$ and the Picard-Vessiot field is $K(z)$.

4 The Galois group

The Galois group of a difference system of the form (3.1) is a linear algebraic group defined over the field of constants k. As we have already pointed out, since we have chosen not to assume that k is algebraically closed, we cannot stick to a naive approach to linear algebraic groups as sets of matrices with entries in the base field, but we have to use the point of view of group schemes. For the reader's convenience we recall informally a minimal amount of definitions that are necessary in what follows. They are contained in any classical reference on group schemes, for instance [Wat79].

4.1 A short digression on group schemes

A group scheme G over the field k is a covariant functor from the category of k-algebras to the category of groups:

$$\begin{array}{rccc} G: & k\text{-algebras} & \to & \text{Groups} \\ & B & \mapsto & G(B) \end{array}.$$

An affine group scheme is a group scheme which is representable, i.e., there exists a k-algebra $k[G]$ such that the functor G and $\mathrm{Hom}_k(k[G], -)$ are naturally isomorphic. This implies, in particular, that $G(B)$ and $\mathrm{Hom}_k(k[G], B)$ are isomorphic as groups, for any k-algebra B.

Example 4.1. For $k = \mathbb{Q}$, we can look at GL_n as an affine group scheme over $\mathbb{Q}$ in the following way:

$$\begin{array}{rccc} \mathrm{GL}_{n,\mathbb{Q}}: & \mathbb{Q}\text{-algebras} & \to & \text{Groups} \\ & B & \mapsto & \mathrm{GL}_n(B) \end{array}.$$

We recall that, for a general $\mathbb{Q}$-algebra B, $GL_n(B)$ is the group of square matrices with coefficients in B, whose determinant is an invertible element of B. We have:

$$\mathbb{Q}[\mathrm{GL}_{n,\mathbb{Q}}] = \frac{\mathbb{Q}[t, x_{i,j},\, i,j = 1,\ldots,n]}{(t\det(x_{i,j}) - 1)}.$$

Of course an analogue definition holds for the affine group scheme $\mathrm{GL}_{n,k}$, define over a generic field k. For $n = 1$, we obtain the multiplicative affine group scheme, for whom we will use the notation $\mathbb{G}_{m,k}$ rather then $\mathrm{GL}_{1,k}$. The additive affine group scheme $\mathbb{G}_{a,k}$ is defined as follows:

$$\begin{array}{rccc} \mathbb{G}_{a,k}: & k\text{-algebras} & \to & \text{Groups} \\ & B & \mapsto & \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in B \right\}. \end{array}.$$

We have:

$$k[\mathbb{G}_{a,k}] = \frac{k[\mathrm{GL}_{2,k}]}{(x_{1,1} - 1, x_{2,2} - 1, x_{2,1})}.$$

It follows that $k[\mathbb{G}_{a,k}]$ can be naturally identified with the algebra $k[x]$ of polynomial in the variable x and coefficients in k. One can define in an analogous way the affine group scheme $\mathrm{SL}_{n,k}$ over k, whose algebra is $k[\mathrm{SL}_{n,k}] = \frac{k[x_{i,j},\, i,j=1,\ldots,n]}{(\det(x_{i,j})-1)}$.

The Yoneda Lemma ensures that $k[G]$ is unique up to isomorphism. An important property (that we won't use, because we are not getting into the details of the proofs) of $k[G]$ is that it has a natural structure of Hopf algebra.

The affine group scheme G is said to be an algebraic group if $k[G]$ is a finitely generated k-algebra. This means that $k[G]$ can be identified with a quotient $k[x_1, \ldots, x_n]/I$ of a ring of polynomials by a convenient (Hopf) ideal I. It allows to identify $G(B)$ with the set of zeros of I in B^n, for any k-algebra B. In other words, G can be identified with an affine variety defined over k. All the affine group schemes in Example 4.1, as well as all the affine group schemes appearing in this paper, are algebraic groups.

If G is an algebraic group and G' is another affine group scheme defined over k, we say that G' is an affine subgroup scheme of G if there exists a surjective morphism of Hopf algebras $k[G] \to k[G']$. This implies that $G'(B)$ can be identified naturally to a subgroup of $G(B)$, for any k-algebra B. We say that G' is a normal algebraic subgroup of G, if $G'(B)$ is a normal subgroup of $G(B)$, for any k-algebra B.

Example 4.2. In the notation of Example 4.1, we have:

1. The additive affine group scheme $\mathbb{G}_{a,k}$ is an algebraic subgroup of $\mathrm{GL}_{2,k}$.

2. We have a surjective morphism from $k[\mathrm{GL}_{n,k}]$ to $k[\mathrm{SL}_{n,k}]$ defined by $t \mapsto 1$, therefore $\mathrm{SL}_{n,k}$ is naturally an algebraic subgroup of $\mathrm{GL}_{n,k}$.

For further reference, we describe the algebraic subgroups of $\mathbb{G}_{m,k}$. As we have already pointed out, we have $k[\mathbb{G}_{m,k}] = \frac{k[x,t]}{(xt-1)}$, therefore we can write for short $k[\mathbb{G}_{m,k}] = k\left[x, \frac{1}{x}\right]$. The algebraic subgroups of $\mathbb{G}_{m,k}$ are the defined by equations of the form $x^n - 1$, for any non-negative integer n. They are represented by the quotients $\frac{k\left[x, \frac{1}{x}\right]}{(x^n-1)}$. If G is one of those subgroups, with $n \geq 1$, and B is a k-algebra, then $G(B)$ is nothing more that the group of n-th roots of unity contained in B. For $n = 1$, we obtain the trivial algebraic subgroup $\{1\}$ of $\mathbb{G}_{m,k}$, while for $n = 0$ we obtain the whole $\mathbb{G}_{m,k}$.

Let us consider the algebraic group $G^n_{m,k}$, for some positive integer n. We have $k[G^n_{m,k}] = k\left[x_1, \frac{1}{x_1}, \ldots, x_n, \frac{1}{x_n}\right]$. The algebraic subgroups of $G^n_{m,k}$ are defined by polynomials of the form $x_1^{\alpha_1} \ldots x_n^{\alpha_n} - 1$, where $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$.

We will also need the description of the algebraic subgroups of $\mathbb{G}^n_{a,k}$, where n is a positive integer. For any k-algebra B, $\mathbb{G}^n_{a,k}(B)$ can be naturally identified to B^n. Therefore, an algebraic subgroup G of $\mathbb{G}^n_{a,k}$ is defined by an ideal generated by at most n independent linear equations with coefficients in k. In particular, we will use the fact that a proper algebraic subgroup of $\mathbb{G}^n_{a,k}$ is always an algebraic subgroup of the group represented by the algebra $\frac{k[x_1,\ldots,x_n]}{(\alpha_1 x_1 + \cdots + \alpha_n x_n)}$, for some $\alpha_1, \ldots, \alpha_n \in k$, not all zero. Notice that, for $n = 1$, the algebraic group $G_{a,k}$ does not have any proper algebraic subgroup.

4.2 The Galois group of a linear difference system

Let $K \subset F$ be our base field, with $k = K^\tau = F^\tau$, and let us consider a system of the form (3.1). From now on we will assume *implicitly* that all Picard-Vessiot rings and all Picard-Vessiot fields are contained in F. So let R ($\subset F$) be a Picard-Vessiot ring for (3.1) and let L be its field of fractions.

For more details on what follows, see [OW15, §2.7].[1]

Definition 4.3. [OW15, 2.50] *We call the (difference) Galois group of* (3.1) *the following group scheme:*

$$\begin{array}{rccc} \mathrm{Gal}(L/K): & k\text{-Algebras} & \to & \text{Groups} \\ & B & \mapsto & \mathrm{Aut}^\tau(R \otimes_k B / K \otimes_k B), \end{array}$$

where:

1. *the k-algebra B is endowed with a structure of trivial τ-k-algebra, so that $\tau(f \otimes b) = \tau(f) \otimes b$, for any $f \in R$ and any $b \in B$;*
2. *$\mathrm{Aut}^\tau(R \otimes_k B / K \otimes_k B)$ is the group of the ring automorphisms of $R \otimes_k B$, that fix $K \otimes_k B$ and commute with τ.*

The functor $\mathrm{Gal}(L/K)$ *acts on morphisms by extension of constants, namely, each morphism of k-algebras $\alpha : B_1 \to B_2$ defines a structure of B_1-algebra over B_2 and the definition of* $\mathrm{Gal}(L/K)(\alpha) : \mathrm{Aut}^\tau(R \otimes_k B_1 / K \otimes_k B_1) \to \mathrm{Aut}^\tau(R \otimes_k B_2 / K \otimes_k B_2)$ *relies on the fact that $R \otimes_k B_2 \cong R \otimes_k B_1 \otimes_{B_1,\alpha} B_2$.*

For any choice of a fundamental solution matrix $U \in \mathrm{GL}_d(R)$ of (3.1), for any k-algebra B and any $\varphi \in \mathrm{Gal}(L/K)(B)$ we have that

$$\tau(U^{-1}\varphi(U)) = U^{-1}A^{-1}\varphi(A)\varphi(U) = U^{-1}\varphi(U) \in \mathrm{GL}_d(B),$$

where we have identified U and $U \otimes 1$ in $R \otimes_k B$, making an abuse of notation that we will repeat frequently. (Notice that we have used the fact that $(R \otimes_k B)^\tau = B$. See Lemma 2.3.) The maps $\varphi \mapsto U^{-1}\varphi(U)$ represents $\mathrm{Gal}(L/K)(B)$ as a subgroup of $\mathrm{GL}_d(B)$. The linearity of the difference system (3.1) immediately implies that another choice of the fundamental solution matrix leads to a conjugated representation, so that most of the times we can identify $\mathrm{Gal}(L/K)(B)$ with a subgroup scheme of $\mathrm{GL}_{d,k}(B)$, forgetting to mention the matrix U. The following proposition says that such a representation is functorial in B, in the sense that $\mathrm{Gal}(L/K)$ is an algebraic subgroup of $\mathrm{GL}_{d,k}$, as in the next example.

Example 4.4. Let us consider the rank-one difference equation $\tau(y) = ay$, where $a \in K$, as in Example 3.11. By assumption, there exists $z \in F$ such that $\tau(z) = az$ and $R = K[z, z^{-1}]$ is its Picard-Vessiot ring. For any k-algebra B and any $\varphi \in \mathrm{Gal}(L/K)(B)$, the element $\varphi(z \otimes 1)$ of $R \otimes_k B$ must be a solution of $\tau(y) = ay$, and hence there exists $c_\varphi \in B^*$ such that $\varphi(z \otimes 1) = c_\varphi(z \otimes 1)$. This means that $\mathrm{Gal}(L/K)$ can be identified with a subgroup of the multiplicative group $\mathbb{G}_{m,k}$ defined over k, therefore it coincides either with $\mathbb{G}_{m,k}$ or with a cyclic group. If for instance $a = -1$, then we must have $z^2 \in k$, and therefore $c_\varphi^2 = 1$.

Proposition 4.5. [OW15, Lemma 2.51] *The Galois group* $\mathrm{Gal}(L/K)$ *is an algebraic group defined over k, represented by the k-algebra $(R \otimes_K R)^\tau$.*

Remark 4.6. We remind that the statement above means that $(R \otimes_K R)^\tau$ is a finitely generated k-algebra and that the functors $\mathrm{Gal}(L/K)$ and $\mathrm{Hom}_{k\text{-Algebra}}((R \otimes_K R)^\tau, -)$ are naturally isomorphic. In particular for any k-algebra B, we have can identify $\mathrm{Gal}(L/K)(B)$ with $\mathrm{Hom}_{k\text{-Algebra}}((R \otimes_K R)^\tau, B)$.

[1] In the notation of [OW15], one has to take $\Phi = \tau$ and σ to be the identity.

The proposition above says that there exists an ideal I of the ring of polynomials $k[X, \det X^{-1}]$, with $X = (x_{i,j})_{i,j=1,\dots,d}$, such that for any k-algebra B the image of the group morphism defined above

$$\begin{array}{ccc} \mathrm{Gal}(L/K)(B) & \to & \mathrm{GL}_d(B) \\ \varphi & \mapsto & [\varphi]_U := U^{-1}\tau(U) \end{array}$$

is exactly the set of zeros of I in $\mathrm{GL}_d(B)$. The idea of the proof is to consider the k-algebra $k[Z, \det Z^{-1}] \hookrightarrow (R \otimes_k R)^\tau$, where $Z := (U^{-1} \otimes 1)(1 \otimes U)$. Then one can prove that we have the series of isomorphisms:

$$R \otimes_K R \cong R.k[Z, \det Z^{-1}] \cong R \otimes_k (R \otimes_K R)^\tau .$$

This allows to prove a series of group isomorphisms showing that for any k-algebra B we have:

$$\mathrm{Hom}_{\tau\text{-}(K \otimes_k B)\text{-alg}}(R \otimes_k B, R \otimes_k B) \cong \mathrm{Hom}_{k\text{-alg}}((R \otimes_K R)^\tau, B).$$

See [OW15] for details.

Example 4.7. Let F be the field of meromorphic functions over $\mathbb{C}^*$ and let τ be defined by $\tau : f(x) \mapsto f(qx)$, for $q \in \mathbb{C}$, such that $|q| > 1$. The field of constants k is the field of meromorphic functions over the torus $\mathbb{C}^*/q^{\mathbb{Z}}$ and we set $K = k(x)$. The Jacobi Theta function

$$\Theta(x) = \sum_{x \in \mathbb{Z}} q^{-n(n+1)/2} x^n \in F$$

is solution of the difference equation $\tau(y) = xy$. Its differential Galois group G is the multiplicative group. Indeed for any k-algebra B and for any $\varphi \in G(B)$, φ multiplies $\Theta(x)$ by an invertible element of B. On the other hand, since $\Theta(x)$ is a transcendental function, any invertible constant of B defines an automorphism of $K[\Theta(x), \Theta(x)^{-1}] \otimes_k B$.

Now let us consider an integer $r \geq 2$ and choose a r-th root $q^{1/r}$ of q. The meromorphic function $z(x) := \Theta(q^{1/r}x)/\Theta(x) \in F$ is a solution of the finite difference equation $\tau(y) = q^{1/r}y$ and its difference Galois group is the cyclic subgroup of $G_{m,k}$ of order r. To prove the last claim it is enough to notice that $z(qx)^r = qz(x)^r$, hence $z(x)^r$ is a meromorphic function of the form $xg(x)$, with $g(x) \in k \subset K$.

Example 4.8. Let us consider an element $f \in K$ and the inhomogeneous difference equation $\tau(y) = y + f$. By assumption, there exists a solution $z \in F$ and we have already noticed that $R = k[z]$. See Example 3.12. For any k-algebra B and any $\varphi \in \mathrm{Gal}(L/K)$, the element $\varphi(z)$ of $R \otimes_k B$ must be another solution of $\tau(y) = y + f$, hence there exists $c_\varphi \in B$ such that $\varphi(z) = z + c_\varphi$ (here we have identified z and $z \otimes 1$). It follows that $\mathrm{Gal}(L/K)$ is a algebraic subgroup of the additive group $\mathbb{G}_{a,k}$. This means that either $\mathrm{Gal}(L/K) = \{1\}$ or $\mathrm{Gal}(L/K) = \mathbb{G}_{a,k}$.

4.3 Transcendence degree of the Picard-Vessiot extension

We can now state the first important result from the point of view of applications to number theory and more specifically to transcendence. It compares the dimension of G over k as an algebraic variety and the transcendence degree of R over K and its proof is based on Proposition 4.5.

Theorem 4.9. [OW15, Lemma 2.53] *Let R, L and G be as above. Then the dimension of G as an algebraic variety over k is equal to the transcendence degree of R (or of L) over K:*

$$\dim_k G = \mathrm{trdeg}_K R = \mathrm{trdeg}_K L.$$

Example 4.10. Let us consider the case of finite difference equations, i.e, let F be the field of meromorphic functions over $\mathbb{C}$ equipped with the operator $\tau : f(x) \mapsto f(x+1)$. Then k is the field of 1-periodic functions and we set $K = k(x)$. We consider the difference equations $\tau(y) = xy$, which is satisfied by the Euler Gamma function $\Gamma(x)$. Its Picard-Vessiot ring is $K[\Gamma(x), \Gamma(x)^{-1}]$, as discussed in Example 3.11. As in Example 4.4, its Galois group G is a subgroup of $\mathbb{G}_{m,k}$. For any k-algebra B and any $\varphi \in G(B)$, there exists an invertible element c_φ of B such that $\varphi(\Gamma) = c_\varphi \Gamma$. As already explained, the proper subgroups of $\mathbb{G}_{m,k}$ are the finite cyclic groups. If G was a the cyclic group, $\Gamma(x)$ would be an algebraic function, by the previous theorem. Proving that the functional equations of the Gamma function implies that it is not algebraic over $k(x)$ is an exercise that we leave to the reader. Therefore the difference Galois group G is the whole $\mathbb{G}_{m,k}$.

Example 4.11. Let us consider the system

$$\tau(Y) = \begin{pmatrix} x & 1 & 0 \\ 0 & x & 1 \\ 0 & 0 & x \end{pmatrix} Y.$$

We denote by $(\cdot)'$ the derivation $\frac{d}{dx}$, with respect to x. Since τ and $\frac{d}{dx}$ commute, we have:

$$\tau\Big(\Gamma'(x)\Big) = \frac{d}{dx}\Big(x\Gamma(x)\Big) = x\Gamma'(x) + \Gamma(x)$$

and

$$\tau\left(\frac{\Gamma''(x)}{2}\right) = \frac{1}{2}\frac{d}{dx}\Big(x\Gamma'(x) + \Gamma(x)\Big) = x\frac{\Gamma''(x)}{2} + \Gamma'(x).$$

Therefore a solution matrix is given by

$$Y = \begin{pmatrix} \Gamma(x) & \Gamma'(x) & \Gamma''(x)/2 \\ 0 & \Gamma(x) & \Gamma'(x) \\ 0 & 0 & \Gamma(x) \end{pmatrix},$$

so that the associated Picard-Vessiot ring is $R = K\big[\Gamma(x), \Gamma'(x), \Gamma''(x), \Gamma(x)^{-1}\big]$. Let G be its difference Galois group and let B be a k-algebra. For any $\varphi \in G(B)$, φ commutes to the action of τ over $R \otimes_k B$, therefore it must send any element of R, which is solution of a τ-difference equation, into a solution of the same equation. We know that Γ is solution of a homogenous order 1 equation, while $\frac{\Gamma'(x)}{\Gamma(x)}$ and $\frac{d}{dx}\left(\frac{\Gamma'(x)}{\Gamma(x)}\right)$ are solutions inhomogeneous order 1 equations. Therefore, as in Examples 4.4 and 4.8, there must exist $c_\varphi \in \mathbb{G}_{m,k}(B)$ and $(d_{1,\varphi}, d_{2,\varphi}) \in \mathbb{G}_{a,k}(B)^2$ such that

$$\begin{cases} \varphi\big(\Gamma(x)\big) = c_\varphi \Gamma(x), \\ \varphi\left(\dfrac{\Gamma'(x)}{\Gamma(x)}\right) = \dfrac{\Gamma'(x)}{\Gamma(x)} + d_{1,\varphi}, \\ \varphi\left(\dfrac{d}{dx}\left(\dfrac{\Gamma'(x)}{\Gamma(x)}\right)\right) = \dfrac{d}{dx}\left(\dfrac{\Gamma'(x)}{\Gamma(x)}\right) + d_{2,\varphi} = \dfrac{\Gamma''(x)}{\Gamma(x)} - \dfrac{\Gamma'(x)}{\Gamma^2(x)} + d_{2,\varphi}. \end{cases}$$

So we have represented G as a subgroup of $\mathbb{G}_{m,k} \times \mathbb{G}_{a,k}^2$. Since $\Gamma(x), \Gamma'(x), \Gamma''(x)$ are algebraically independent by Hölder theorem [Höl87] (see Proposition 7.3 below for a proof), it is actually an isomorphism, thanks to Theorem 4.9. The construction above can be easily generalized to system associated to a Jordan block of eigenvalue x and order higher than 3, using higher order derivatives of Γ.

Now let us consider the finite difference equation $(\tau - x)^n(y) = 0$, for some positive integer n. Such an equation occurs in generalized Carlitz modules studied in [HR97] and more extensively in [Pel13]. We have seen that Γ is a solution for $n = 1$. One can verify recursively that, for $n > 1$, a basis of solution over k is given by the higher order derivatives of Γ with respect to x, namely the set $\Gamma(x), \Gamma'(x), \ldots, \Gamma^{(n-1)}(x)$. It follows that the Picard-Vessiot ring is the same as the one of the system above, namely $R = \big[\Gamma(x), \Gamma'(x), \ldots, \Gamma^{(n-1)}(x), \Gamma(x)^{-1}\big]$. We conclude that the Galois group is $\mathbb{G}_{m,k} \times \mathbb{G}_{a,k}^{n-1}$.

Before being able to prove the most common results used in the applications, we need to state the Galois correspondence and its properties.

5 The Galois correspondence (first part)

We consider $R, L \subset F$ and $G := \mathrm{Gal}(L/K)$ as above.

Definition 5.1. *Let $\frac{r}{s} \in L$, with $r, s \in R$ and $s \neq 0$, and let $\varphi \in G(B)$, for a k-algebra B. We say that $\frac{r}{s}$ is invariant under the action of φ if in $R \otimes_k B$ we have:*

$$\varphi(r \otimes 1)(s \otimes 1) = (r \otimes 1)\varphi(s \otimes 1).$$

If H is an algebraic subgroup of G defined over k, then $\frac{r}{s}$ is invariant under the action of H if $\frac{r}{s}$ is invariant under the action of φ, for all k-algebras B and all $\varphi \in H(B)$.

We denote by L^H the set of elements of L invariant under the action of H.

Remark 5.2. Notice that if $\varphi \in G(k)$, then the condition above simply means that $\frac{\varphi(r)}{\varphi(s)} = \frac{r}{s}$ in L.

If M is an intermediate field of L/K, stable by τ, then we can consider (3.1) as a system defined over M. Indeed if L is a Picard-Vessiot field over K, it must be a Picard-Vessiot field over M and we can define $\mathrm{Gal}(L/M)$.

Theorem 5.3. [OW15, 2.52] *There exists a one-to-one correspondence between the algebraic subgroup of G defined over k and the intermediate fields of L/K stable by τ. In the notation above we have two maps that are one the inverse of the other and are defined by:*

$$H \mapsto L^H, \ M \mapsto \mathrm{Gal}(L/M).$$

Moreover if H is an algebraic subgroup of G, then $H = G$ if and only if $L^H = K$.

As usual in Galois theories, the last statement is the key-point of the Galois correspondence.

6 Application to transcendence and differential transcendence

6.1 General statements

From the theorems above we deduce a first result on transcendency that is very useful in many settings. The criteria of transcendence below are contained in [HS08, §3], up to some reformulations. They are the key-point of several applications, for instance in [DHR18], [DHR16], [DHRS18], [DHRS20], [DH19].

In the proposition below the assumption $k = F^\tau = K^\tau$ is crucial as well as in all the subsequent results in this section.

Proposition 6.1. *Let $f_1, \dots, f_d \in K^*$ and let $z_1, \dots, z_d \in F$ be a solution of the following inhomogeneous difference system:*

$$\left\{ \tau(z_i) = z_i + f_i, \text{ for } i = 1, \dots, d. \right. \tag{6.1}$$

The following assertions are equivalent:

1. *There exist $\lambda_1, \dots, \lambda_d \in k$, not all zero, and $g \in K$ such that $\lambda_1 f_1 + \cdots + \lambda_d f_d = \tau(g) - g$.*
2. *There exist $\lambda_1, \dots, \lambda_d \in k$, not all zero, such that $\lambda_1 z_1 + \cdots + \lambda_d z_d \in K$.*
3. *There exist $\lambda_1, \dots, \lambda_d \in K$, not all zero, such that $\lambda_1 z_1 + \cdots + \lambda_d z_d \in K$.*
4. *$z_1, \dots, z_d$ are algebraically dependent over K.*

Remark 6.2. Notice that the first statement above is about the f_i's, while the others are about the z_i's.

Proof. Let us assume that we are in the situation of the first assertion. We have:

$$\tau\left(\sum_{i=1}^d \lambda_i z_i - g\right) = \sum_{i=1}^d \lambda_i z_i - \tau(g) + \sum_{i=1}^d \lambda_i f_i = \sum_{i=1}^d \lambda_i z_i - g,$$

hence $\sum_{i=1}^d \lambda_i z_i - g \in k$, which proves 2. Moreover, the implications $2 \Rightarrow 3 \Rightarrow 4$ are tautological.

We conclude by proving that $4 \Rightarrow 1$. As in Example 4.8, the system (6.1) is equivalent to the following linear system of order $2d$:

$$\tau(Y) = \begin{pmatrix} \boxed{\begin{matrix} 1 & f_1 \\ 0 & 1 \end{matrix}} & 0 & \cdots & 0 \\ 0 & \boxed{\begin{matrix} 1 & f_2 \\ 0 & 1 \end{matrix}} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \boxed{\begin{matrix} 1 & f_d \\ 0 & 1 \end{matrix}} \end{pmatrix} Y,$$

so that its Picard-Vessiot ring is $R = k[z_1, \dots, z_d]$. It follows that $\mathrm{Gal}(L/K)$ is an algebraic subgroup of $\mathbb{G}_{a,k}^d$, defined over k, and that for any k-algebra B and any $\varphi \in \mathrm{Gal}(L/K)(B)$ there exists $c_{\varphi,1}, \dots, c_{\varphi,d} \in B$ such that $\varphi(z_i) = z_i + c_{\varphi,i}$.

Since $z_1, \dots, z_d$ are algebraically dependent over K, Theorem 4.9 implies that the dimension of $\mathrm{Gal}(L/K)$ is strictly smaller than d and hence $\mathrm{Gal}(L/K)$ is a proper subgroup scheme of $\mathbb{G}_{a,k}^d$. All the proper algebraic subgroup of $\mathbb{G}_{a,k}^d$ are contained in a hyperplane and $\mathrm{Gal}(L/K)$ is defined over k, therefore there exist $\lambda_1, \dots, \lambda_d \in$

k, not all zero, such that for any k-algebra B and any $\varphi \in \mathrm{Gal}(L/K)(B)$, we have $\sum_{i=1}^{d} \lambda_i c_{\varphi,i} = 0$. We conclude that $g := \sum_{i=1}^{d} \lambda_i z_i$ verifies

$$\varphi(g) = \sum_{i=1}^{d} \lambda_i z_i + \sum_{i=1}^{d} \lambda_i c_{\varphi,i} = \sum_{i=1}^{d} \lambda_i z_i = g,$$

and hence that $g \in K$, by the Galois correspondence. Finally we have:

$$\tau(g) - g = \tau\left(\sum_{i=1}^{d} \lambda_i z_i\right) - \sum_{i=1}^{d} \lambda_i z_i = \sum_{i=1}^{d} \lambda_i f_i. \qquad \square$$

In an analogous way, taking into account that the algebraic subgroup of $\mathbb{G}_{m,k}^{d}$ are defined by equations of the form $x_1^{\alpha_1} \cdots x_d^{\alpha_d} = 1$, for some $\alpha_1, \ldots \alpha_d \in \mathbb{Z}$, it is possible to prove the following proposition:

Proposition 6.3. *Let $a_1, \ldots a_d \in K^*$ and let $z_1, \ldots, z_d \in F^*$ be a solution of the following difference system:*

$$\left\{ \tau(z_i) = a_i z_i, \text{ for } i = 1, \ldots, d. \right. \tag{6.2}$$

The following assertions are equivalent:

1. *There exist $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}$, not all zero, and $g \in K$ such that $a_1^{\lambda_1} \cdots a_d^{\lambda_d} = \tau(g)/g$.*
2. *There exist $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}$, not all zero, such that $z_1^{\lambda_1} \cdots z_d^{\lambda_d} \in K$.*
3. *$z_1, \ldots, z_d$ are algebraically dependent over K.*

Remark 6.4. Notice that Proposition 6.3 has one more characterization of the algebraic dependency of the solutions. Here we only have 3 assertions because of the multiplicative form of the algebraic subgroups of $\mathbb{G}_{m,k}^{d}$.

6.2 Differential algebraicity and D-finiteness

We now switch our attention to the characterization of differential algebraicity, hence in this subsection we assume that we are in characteristic zero. We assume that the field F comes equipped with a derivation ∂ that commutes with the endomorphism τ. This implies in particular that ∂ induces a derivation on both k and K.

Example 6.5. In the notation of Example 2.1, we can take $\partial = \frac{d}{dx}$ for $\tau : f(x) \mapsto f(x+1)$ and and $\partial = x\frac{d}{dx}$ for $\tau : f(x) \mapsto f(qx)$.

We recall the following definition:

Definition 6.6. *We say that $f \in F$ is differentially algebraic (with respect to ∂) over K, if there exists an integer $n \geq 0$ such that $f, \partial(f), \ldots, \partial^n(f)$ are algebraically dependent over K, or, equivalently, if f is solution of an algebraic differential equation over K. We say that f is differentially transcendental over K if it is not differentially algebraic over K and that it is D-finite over K if it is differentially algebraic and, moreover, it is the solution of a linear differential equation with coefficients in K.*

We say that F is differentially algebraic over K is all elements of F are differentially algebraic over k.

Once again, the assumption $F^\tau = K^\tau$ is crucial in the following corollaries:

Corollary 6.7. *Let $f \in K^*$ and $z \in F$ be a solution of $\tau(y) = y + f$. The following statements are equivalent:*

1. *There exist $n \geq 0$, $\lambda_0, \ldots, \lambda_n \in k$, not all zero, and $g \in K$ such that $\lambda_0 f + \lambda_1 \partial(f) + \cdots + \lambda_n \partial^n(f) = \tau(g) - g$.*
2. *There exist $n \geq 0$, $\lambda_0, \ldots, \lambda_n \in k$, not all zero, such that $\lambda_0 z + \lambda_1 \partial(z) + \cdots + \lambda_n \partial^n(z) \in K$.*
3. *z is D-finite over K.*
4. *z is differentially algebraic over K.*

In particular, the corollary above says that:

Corollary 6.8. *In the notation of Corollary 6.7, if z is not D-finite over K then z is differentially transcendental over K.*

Proof of Corollary 6.7. The assumption on the commutativity of ∂ and τ implies that z satisfies all the following difference equations:

$$\tau\left(\partial^i(z)\right) = \partial^i(z) + \partial^i(f), \text{ for all } i = 0, 1, 2, \dots.$$

The statement follows from Proposition 6.1. □

Corollary 6.9. *Let $a \in K^*$ and $z \in F^*$ be a solution of $\tau(y) = ay$. The following statement are equivalent:*

1. *There exist $n \geq 0$, $\lambda_0, \dots, \lambda_n \in k$, not all zero, and $g \in K$ such that $\lambda_0 \frac{\partial(a)}{a} + \lambda_1 \partial\left(\frac{\partial(a)}{a}\right) + \cdots + \lambda_n \partial^n\left(\frac{\partial(a)}{a}\right) = \tau(g) - g$.*
2. *There exist $n \geq 0$, $\lambda_0, \dots, \lambda_n \in k$, not all zero, such that $\lambda_0 \frac{\partial(z)}{z} + \lambda_1 \partial\left(\frac{\partial(z)}{z}\right) + \cdots + \lambda_n \partial^n\left(\frac{\partial(z)}{z}\right) \in K$.*
3. *$\frac{\partial(z)}{z}$ is D-finite over K.*
4. *z is differentially algebraic over K.*

Proof. Notice that z is differentially algebraic over K if and only if $\partial(z)/z$ is differentially algebraic over K. In fact, $\partial^n\left(\frac{\partial(z)}{z}\right) \in \frac{1}{z^n} K[z, \partial(z), \dots, \partial^n(x)]$, therefore an elementary algebraic manipulation allows to transform an algebraic differential equation satisfied by z into an algebraic differential equation satisfied by $\partial(z)/z$ and *vice versa*. Taking the logarithmic derivative of $\tau(z) = az$, we obtain:

$$\tau\left(\frac{\partial(z)}{z}\right) = \frac{\partial(z)}{z} + \frac{\partial(a)}{a}.$$

The statement follows from the Corollary 6.7. □

Remark 6.10. The generalization of the last two corollaries to systems of order 1 equations and to an arbitrary set of commuting derivations is straightforward. For the generalization to the case of equation of the form $\tau(y) = ay + f$, we refer to [HS08, Propositions 3.8, 3.9, and 3.10].

7 Applications to special cases

In this section we suppose that F has characteristic zero. The results in §7.1 and §7.3 have been originally proven in [HS08, §3].

7.1 Finite difference equations and Hölder theorem

We are in the situation of Example 4.10, i.e., let F be the field of meromorphic functions over $\mathbb{C}$ equipped with the operator $\tau : f(x) \mapsto f(x+1)$. Then k is the field of meromorphic 1-periodic functions and we set $K = k(x)$. We set $\partial = \frac{d}{dx}$, which commutes with τ.

Corollary 7.1. *In the notation above, let $f \in K^*$ and $z \in F$ be such that $\tau(z) = z + f$. The following assertions are equivalent:*

1. *z is differentially algebraic over K.*
2. *z is D-finite over K.*
3. *There exist a positive integer n, $\lambda_0, \dots, \lambda_n \in k$ and $g \in K$ such that*

$$\lambda_0 f + \lambda_1 \partial(f) + \cdots + \lambda_n \partial^n(f) = g(x+1) - g(x).$$

If $f \in \mathbb{C}(x)$ (resp. $f \in \overline{\mathbb{Q}}(x)$), then they are also equivalent to:

4. *There exist a positive integer n, $\lambda_0, \dots, \lambda_n \in \mathbb{C}$ (resp. $\in \overline{\mathbb{Q}}$) and $g \in \mathbb{C}(x)$ (resp. $\in \overline{\mathbb{Q}}(x)$) such that*

$$\lambda_0 f + \lambda_1 \partial(f) + \cdots + \lambda_n \partial^n(f) = g(x+1) - g(x).$$

Proof. Notice that $1 \Leftrightarrow 2 \Leftrightarrow 3$ follow from Corollary 6.7. Moreover $4 \Rightarrow 3$ is trivial. Let us prove that $3 \Rightarrow 4$, by a classical descent argument. Let $C = \mathbb{C}$ or $\overline{\mathbb{Q}}$, so that $f \in C(x)$. Let N be the degree of the denominator of g and M the degree of its denominator. We consider a ring of polynomials of the form $C[\Lambda_0, \dots, \Lambda_n, A_0, \dots, A_N, B_0 \dots, B_M]$, so that we can write the equality

$$\Lambda_0 f + \Lambda_1 \partial(f) + \cdots + \Lambda_n \partial^n(f) = \frac{A_0 + A_1(x+1) + \cdots + A_N(x+1)^N}{B_0 + B_1(x+1) + \cdots + B_M(x+1)^M} - \frac{A_0 + A_1 x + \cdots + A_N x^N}{B_0 + B_1 x + \cdots + B_M x^M}. \tag{7.1}$$

Equalizing the coefficients of each integer powers of x in (7.1), we obtain a system of polynomial equations with coefficients in C, that has a solution in k, by assumption. Since C is an algebraically closed field contained in k, it must also have a solution in C. This proves the corollary. □

Although the last assertion of Corollary 7.1 is stated over $\mathbb{C}$ (or over $\overline{\mathbb{Q}}$), we cannot conclude the differential algebraicity of z over $\mathbb{C}(x)$. See Example 7.4 that it is based on the fact that there are meromorphic 1-periodic functions that are differentially transcendental over $\mathbb{C}(x)$. For now, notice that the statement above only implies the following:

Corollary 7.2. *We consider the same notation as in the previous corollary, with $C = \overline{\mathbb{Q}}$ or $\mathbb{C}$ and $f \in C(x)$. Suppose that for any $n \geq 0$, any $\lambda_0, \dots, \lambda_n \in C$ and any $g \in C(x)$, we have: $\lambda_0 f + \lambda_1 \partial(f) + \cdots + \lambda_n \partial^n(f) \neq g(x+1) - g(x)$. Then z is differentially transcendent over K and hence over $C(x)$.*

The Euler Gamma function, that we have already mentioned in some examples, is a meromorphic function over $\mathbb{C}$ satisfying the functional equation $\Gamma(x+1) = x\Gamma(x)$. Hölder theorem [Höl87] says that the Gamma function is differentially transcendental over $\mathbb{C}(x)$ and we are now able to prove it, using a Galoisian argument that has first appeared in [Har08] and [HS08]. Notice that in [BK78] there is a similar proof of the differential transcendency of the Gamma function, which relies on a statement similar to Corollary 7.2 in the specific case of the Gamma function, proven by an elementary argument of complex analysis.

Proposition 7.3. *The Gamma function Γ is differentially transcendental over $\mathbb{C}(x)$.*

Proof. As in the proof of Proposition 6.9, the Gamma function Γ is differentially transcendental over $\mathbb{C}(x)$ if and only if the function $\psi(x) := \partial(\Gamma)(x)/\Gamma(x)$, that verifies the functional equation

$$\tau(\psi(x)) = \psi(x) + \frac{1}{x},$$

is differentially transcendental over $\mathbb{C}(x)$. Suppose that there exist a positive integer n, $\lambda_0, \dots, \lambda_n \in \mathbb{C}$ and $g \in \mathbb{C}(x)$ such that

$$\lambda_0 \frac{1}{x} + \lambda_1 \partial\left(\frac{1}{x}\right) + \cdots + \lambda_n \partial^n\left(\frac{1}{x}\right) = g(x+1) - g(x).$$

Since the left-hand side has all its poles at 0, while the right-hand side must have at least a non-zero pole, we find a contradiction, by Corollary 7.2. □

The following is a counterexample, based on Hölder theorem, for the fact that we cannot conclude the differential algebraicity over $\mathbb{C}(x)$ in Corollary 7.1.

Example 7.4. The meromorphic function $\Gamma(\exp(2i\pi x))$ is 1-periodic, hence belongs to $k \subset K$, but is not differentially algebraic over $\mathbb{C}(x)$, since it is the composition of a differentially algebraic function and a differentially transcendental function. In other words, K itself is differentially transcendental over $\mathbb{C}(x)$.

Corollary 7.5. [HS08, Corollary 3.4] *Let $a(x) \in \mathbb{C}(x)^*$ and let z be a meromorphic function over $\mathbb{C}$ solution of $z(x+1) = a(x)z(x)$. Then $z(x)$ is differentially algebraic over $k(x)$ if and only if $a(x) = c\frac{g(x+1)}{g(x)}$, for some $g(x) \in \mathbb{C}(x)$ and $c \in \mathbb{C}$.*

Proof. First of all, replacing $z(x)$ with $z(x)g(x)^{-1}$, for a convenient $g(x) \in \mathbb{C}(x)$, and $a(x)$ with $a(x)\frac{g(x)}{g(x+1)}$, we can suppose that two distinguished poles of $a(x)$ do not differ by an integer.

It follows from Corollary 7.1, that $z(x)$ is differentially algebraic over $k(x)$ if and only if there exist a positive integer n, $\lambda_0, \dots, \lambda_n \in \mathbb{C}$ and $g \in \mathbb{C}(x)$ such that

$$\lambda_0 \frac{\partial(a)}{a} + \lambda_1 \partial\left(\frac{\partial(a)}{a}\right) + \cdots + \lambda_n \partial^n\left(\frac{\partial(a)}{a}\right) = g(x+1) - g(x).$$

In the differential relation above, the right hand side must have at least two pole in any τ-orbit where it has a pole. while the left hand side has at worst one pole per τ-orbit. We conclude that $a(x)$ is constant.

On the other hand, if $a(x) = c\frac{g(x+1)}{g(x)}$ and we choose a logarithm $\log c$ of c, a general solution of $y(x+1) = a(x)y(x)$ has the form $z(x) = p(x)\exp(x \log c)$, with $p(x) \in k$. The latter is differentially algebraic over $k(x)$. □

7.2 Linear inhomogeneous q-difference equations of the first order

We consider the setting of q-difference equations, i.e., F is the field of meromorphic functions over $\mathbb{C}^*$, q is a fixed complex number such that $|q| > 1$, $\tau : f(x) \mapsto f(qx)$, $K = k(x)$, with $k = F^\tau$. We consider the derivation $\partial = x\frac{d}{dx}$, that commutes with τ.

With respect to differential algebraicity, the case of q-difference equations deeply differs from the case of finite difference equation because of the following property (see Example 7.4):

Lemma 7.6. *The field of elliptic functions k is differentially algebraic over $\mathbb{C}$.*

To prove Lemma 7.6, it suffices to write the torus $\mathbb{C}^*/q^{\mathbb{Z}}$ in the form $\mathbb{C}/\mathbb{Z} + i\tau\mathbb{Z}$, where $q = \exp(2i\pi\tau)$, using the exponential function, and remember that the Weierstrass function $\wp$ is differentially algebraic over $\mathbb{C}(x)$, which is itself differentially algebraic over $\mathbb{C}$.

For further reference, we state the following corollary which is a consequence of the fact that, if we have a tower of differentially algebraic extensions $\widetilde{k}/k'$ and k'/k, then $\widetilde{k}/k$ is also differentially algebraic:

Corollary 7.7. *For a meromorphic function $f \in F$, it is equivalent to be differentially algebraic over the following fields: $k(x)$, k, $\mathbb{C}(x)$, $\mathbb{C}$.*

Taking into account the previous lemma, the proof of the corollary below follows word by word the proof of Corollary 7.1:

Corollary 7.8. *In the notation above, let $f \in K^*$ and $z \in F$ be such that $\tau(z) = z + f$. The following assertions are equivalent:*

1. *f is differentially algebraic over K.*
2. *f is differentially algebraic over $\mathbb{C}(x)$.*
3. *f is D-finite over K.*
4. *There exist a positive integer n, $\lambda_0, \dots, \lambda_n \in k$ and $g \in K$ such that*

$$\lambda_0 f + \lambda_1 \partial(f) + \cdots + \lambda_n \partial^n(f) = g(qx) - g(x).$$

Moreover, if $f \in \overline{\mathbb{Q}}(x)$ (resp. $\mathbb{C}(x)$), they are also equivalent to:

1. *There exist a positive integer n, $\lambda_0, \dots, \lambda_n \in \overline{\mathbb{Q}}$ (resp. $\mathbb{C}$) and $g \in \overline{\mathbb{Q}}(x)$ (resp. $\mathbb{C}(x)$) such that*

$$\lambda_0 f + \lambda_1 \partial(f) + \cdots + \lambda_n \partial^n(f) = g(qx) - g(x).$$

We finally conclude by proving a result for homogenous order 1 q-difference equations:

Corollary 7.9. [HS08, Corollary 3.4] *Let $a(x) \in \mathbb{C}(x)^*$ and let z be a meromorphic function over $\mathbb{C}^*$ (resp. $\mathbb{C}$) be a solution of $z(qx) = a(x)z(x)$. The $z(x)$ is differentially algebraic over $\mathbb{C}(x)$ (or equivalently over $k(x)$) if and only if $a(x) = cx^n \frac{g(qx)}{g(x)}$, for some $g(x) \in \mathbb{C}(x)$, $n \in \mathbb{Z}$ and $c \in \mathbb{C}$ (resp. $n = 0$ and $c \in q^{\mathbb{Z}}$).*

Proof. If $a(x) = cx^n \frac{g(qx)}{g(x)}$, then a meromorphic solution in F is given by $z(x) = p(x)\frac{\Theta(cx)}{\Theta(x)}\Theta(x)^n g(x)$, where $p(x) \in k$ and $\Theta(x) = \sum_{n\in\mathbb{Z}} q^{-n(n+1)/2}x^n \in F$ is the Jacobi Theta function, which verifies the functional equation $\Theta(qx) = x\Theta(x)$. Notice that $\partial\left(\frac{\partial(\Theta(x))}{\Theta(x)}\right) \in k$, therefore z is differentially algebraic over $\mathbb{C}(x)$. In particular, if $n = 0$, and c is an integer power of q, the solution is also meromorphic at zero.

Let us prove the inverse. We assume that z is meromorphic over $\mathbb{C}^*$. First of all, replacing $z(x)$ with $z(x)g(x)^{-1}$, for a convenient $g(x) \in \mathbb{C}(x)$, and $a(x)$ with $a(x)\frac{g(x)}{g(qx)}$, we can suppose that two distinguished poles of $a(x)$ do not differ by an integer power of q.

It follows from Corollary 7.8, that $z(x)$ is differentially algebraic over $\mathbb{C}(x)$ if and only if there exist a positive integer n, $\lambda_0, \dots, \lambda_n \in \mathbb{C}$ and $g \in \mathbb{C}(x)$ such that

$$\lambda_0 \frac{\partial(a)}{a} + \lambda_1 \partial\left(\frac{\partial(a)}{a}\right) + \cdots + \lambda_n \partial^n\left(\frac{\partial(a)}{a}\right) = g(qx) - g(x).$$

The differential relation above shows that $a(x)$ must have at least two poles in any non-zero τ-orbit, which is in contradiction with our assumptions, therefore we conclude that $a(x) = cx^n$, for some $c \in \mathbb{C}$ and $n \in \mathbb{Z}$.

If moreover z is has a pole at zero, rather than an essential singularity, we can take the expansion of z in $\mathbb{C}((x))$. Plugging it into the equation $z(qx) = cx^n z(x)$, we see that $n = 0$ and hence that c must be an integer power of q. □

7.3 A particular case of the Ishizaki-Ogawara's theorem

In the case of q-difference equations we give a Galoisian proof of the following statement, which is a particular case of Ogawara's theorem [Oga14, Theorem 2]. As already noted by Ogawara, Ishizaki's theorem [Ish98, Theorem 1.2] can be deduced from his formal result. The latter is proved using elementary complex analysis and it is a crucial ingredient of [DHRS20]. Both Ishizaki's and Ogawara's results are based on the idea that q-difference equations "do not have many solutions which are meromorphic in a neighborhood of 0". In this subsection we only need to assume that $q \neq 0$ is not a root of unity, hence we allow q to have norm equal to 1.

Proposition 7.10. [Oga14, Theorem 2] *Let $q \in \mathbb{C} \setminus \{0, \text{roots of unity}\}$, $f \in \mathbb{C}(x)$, $f \neq 0$ and let $z \in \mathbb{C}((x))$ be a formal power series solution of $\tau(z) = z + f$. The following assertions are equivalent:*

1. *$z \in \mathbb{C}(x)$.*
2. *z is algebraic over $\mathbb{C}(x)$.*
3. *z is D-finite over $\mathbb{C}(x)$.*
4. *z is differentially algebraic over $\mathbb{C}(x)$.*

Proof. The implications $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4$ are trivial. We prove that $4 \Rightarrow 1$. We decompose $f(x)$ into elementary fractions and we take care of each part of the decomposition separately. We consider a pole $\alpha \in \mathbb{C}^*$ of $f(x)$ such that all the other poles of $f(x)$ in $\alpha q^{\mathbb{Z}}$ are of the form $q^{-n}\alpha$, with $n \geq 0$. Let N_α the largest integer such that $q^{-N_\alpha}\alpha$ is a pole of $f(x)$ and $\sum_i \frac{a_i}{(x-q^{-N_\alpha}\alpha)^i}$ be the polar part of $f(x)$ at $q^{-N_\alpha}\alpha$. We set $h_1(x) = \sum_i \frac{q^i a_i}{(x-q^{-N_\alpha}\alpha)^i}$. Replacing $z(x)$ with $z_1(x) = z(x) + h_1(x)$, we are reduced to consider a new functional equation $y(qx) = y(x) + f_1(x)$, with $f_1(x) = f(x) - h_1(qx) + h_1(x)$, which has a smaller N_α. Iterating the argument we obtain a q-difference equation with an inhomogeneous term $f(x)$ having at most a single pole in each q-orbit $\alpha q^{\mathbb{Z}}$. Corollary 6.7 (for $F = \mathbb{C}((x))$ and $K = \mathbb{C}(x)$) implies that there exist $n \geq 0$, $\lambda_0, \dots, \lambda_n \in \mathbb{C}$, not all zero, and $g \in \mathbb{C}(x)$ such that $\lambda_0 f + \lambda_1 \partial(f) + \cdots + \lambda_n \partial^n(f) = \tau(g) - g$. Since $\tau(g) - g$ cannot have a single pole in $q^{\mathbb{Z}}\alpha$, for $\alpha \neq 0$, we conclude that the rational function $f(x)$ must have no pole at all in $q^{\mathbb{Z}}\alpha$. We are reduced to prove the claim in the case $f \in \mathbb{C}[x, x^{-1}]$, but this assumption obliges $z(x) \in \mathbb{C}((x))$ to be an element of $\mathbb{C}[x, x^{-1}]$, as one can see directly from the equation $f(x) = z(qx) - z(x)$, identifying the coefficients of x^n, for every integer n. This ends the proof. □

The expansion at zero defines an injective morphism from the field of meromorphic functions over $\mathbb{C}$ to $\mathbb{C}((x))$, which commutes to the action of ∂, therefore we obtain:

Corollary 7.11. [Ish98, Theorem 1.2] *Let $f \in \mathbb{C}(x)$, $f \neq 0$ and let $z \in F$ be a meromorphic function over $\mathbb{C}$, solution of $\tau(z) = z + f$. Then the assertions of Proposition 7.10 are equivalent for z.*

Remark 7.12. The reader can find a Galoisian proof of the Ishizaki theorem in whole generality in [HS08, Proposition 3.5], i.e., for equations of the form $\tau(y) = ay + f$. The general statement can be proven using the parameterized Galois theory of difference equations.

Remark 7.13. We make some comments on the relation between convergent and meromorphic solutions, under the assumption that $|q| \neq 1$:

1. An important property of q-difference equations is the following:

   > *For a solution of a linear q-difference equation with meromorphic coefficients over $\mathbb{C}^*$, it is equivalent to be meromorphic in a neighborhood of zero and to be meromorphic over $\mathbb{C}$.*

   The proof is quite easy and relies on the fact that we have supposed that $|q| \neq 1$. In fact, this allows to consider a meromorphic continuation of the solution thanks to the fact that any point can be "brought next to zero" with a repeated application of τ or of τ^{-1}. It seems that this remark is originally due to H. Poincaré [Poi90, page 318].

2. Let us suppose that z is a meromorphic function over $\mathbb{C}$ and algebraic over $\mathbb{C}(x)$. Then z is a meromorphic function over $\mathbb{C}$, which has at worst a pole at ∞, hence it is rational. This proves that $2 \Rightarrow 1$ in Proposition 7.10 is true for all linear q-difference equations with rational coefficients, as soon as the solution is meromorphic at 0.

8 The Galois correspondence (second part)

In this section we are going to focus on the role of normal subgroups in the Galois correspondence, under the following assumption.

Assumption 8.1. We suppose that τ is an automorphism of F and induces an automorphism of K. In difference algebra, when τ is an automorphism, i.e. admits an inverse, is usually called inversive.

The assumption above immediately implies that τ is also an automorphism of any Picard-Vessiot ring and any Picard-Vessiot field contained in F. In fact, if U is a fundamental solution of a system $\tau(Y) = AY$ as in (3.1), we also have $\tau^{-1}(U) = \tau^{-1}(A^{-1})U$. Notice that we continue to work under the assumption of §3 and in particular that F contains a fundamental solution of the linear system $\tau(Y) = AY$ with coefficients in K, and hence, that all our Picard-Vessiot ring and extensions are contained in F.

The main result of this section is the following:

Theorem 8.2. *In the notation of Theorem 5.3 above, let H be an algebraic subgroup of G defined over k and let $M = L^H$. The following assertions are equivalent:*

1. *H is a normal subgroup of G;*
2. *M is a Picard-Vessiot field over K (for a convenient linear difference equation).*

Assuming the equivalent conditions above, the algebraic group $\mathrm{Gal}(M/K)$ *is naturally isomorphic to G/H.*

In order to complete the proof of the Galois correspondence, we need to prove a quite classical proposition on the action of the Galois group on the elements of the Picard-Vessiot extension. The proof is not difficult and indeed it is quite similar to the differential case [vdPS03, Corollary 1.38], but, to the best of my knowledge, it is not detailed anywhere in the literature. Notice that the hypothesis that τ is inversive is a central ingredient.

Proposition 8.3. *Let $R \subset F$ be the Picard-Vessiot ring for a linear difference system of the form* (3.1) *over K and f an element of the field of fractions of R. The following statements are equivalent:*

1. *$f \in R$;*
2. *the K-vector space spanned by $\{\tau^n(f), n \geq 0\}$ has finite dimension.*

Proof. Let us prove that (1) $\Rightarrow$ (2). We remind that there exists a fundamental solution matrix U of a difference system of the form (3.1), such that $R = K[U, \det U^{-1}]$. Let us denote by $t_1, \ldots, t_{d^2+1}$ the elements of the matrix U, plus $\det U^{-1}$. Since $\tau(U) = AU$ and $\tau(\det U^{-1}) = \det A^{-1} \cdot \det U^{-1}$, for any integer $r \geq 1$, the K-vector space generated by the monomials of degree r in the t_i's and their τ-iterated has finite dimension over K. This proves the statement, because any $f \in R$ can be written as a polynomial in the t_i's and hence the K-vector space spanned by $\{\tau^n(f), n \geq 0\}$ is contained in a finite dimensional K-vector space.

We now show that (2) $\Rightarrow$ (1). Let W be the K-vector space generated by $\{\tau^n(f), n \geq 0\}$. We consider the ideal of R defined by $I := \{a \in R | aW \subset R\}$. Since $f \in L$ and L is the field of fractions of R, the ideal I is non-zero. Moreover τ is inversive, hence $W \subset \tau^{-1}W$. Since W and $\tau^{-1}(W)$ are vector spaces of the same dimension, this implies that $\tau^{-1}(W) = W$. We conclude that $\tau(a)W \subset \tau(aW) \subset R$ for any $a \in I$ and therefore that I is τ-invariant. Finally, $1 \in I$, because R is τ-simple, and $f \in W \subset R$. □

Corollary 8.4. *Let L/K be a Picard-Vessiot extension and R be the Picard-Vessiot ring of L.*

1. *Let M be an intermediate field which is itself a Picard-Vessiot field over K. Moreover let R_M be its Picard-Vessiot ring. Then $R_M = M \cap R$.*
2. *We fix $f \in R$ and a linear difference equation $\mathcal{L}(y) = 0$ with coefficients in K such that $\mathcal{L}(f) = 0$. Furthermore, we suppose that the operator associated with the equation $\mathcal{L}(y) = 0$ has minimal order m in τ. Then the solutions of $\mathcal{L}(y) = 0$ in R form a k-vector space of solutions of maximal dimension m.*

Proof. 1. The statement follows from the previous proposition, since $f \in M \cap R$ if and only if $f \in M$ and f is a solution of a linear difference equation with coefficients in K.
2. Let W be the space of solution of $\mathcal{L}(y) = 0$ in R. Since $f \in W$, we know that $W \neq 0$ and we can consider a k-basis $w_1, \ldots, w_r$ of W. The following formula

$$\det \begin{pmatrix} w_1 & w_2 & \cdots & w_r & y \\ \tau(w_1) & \tau(w_2) & \cdots & \tau(w_r) & \tau(y) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \tau^r(w_1) & \tau^r(w_2) & \cdots & \tau^r(w_r) & \tau^r(y) \end{pmatrix} = 0$$

gives a τ-difference equation $\widetilde{\mathcal{L}}(y) = 0$ with coefficients in L having W as space of solutions. By definition of the Galois group, $\varphi(W \otimes_k B) = W \otimes_k B$, for any $\varphi \in G(B)$ and any k-algebra B. The Galois correspondence and the invariance by the action of the Galois group show that the coefficients of $\widetilde{\mathcal{L}}(y) = 0$ are actually in K. Because of the minimality of the order of the operator associated with $\mathcal{L}(y) = 0$, we conclude that $\mathcal{L}$ and $\widetilde{\mathcal{L}}$ coincide up to the multiplication of a non-zero element of K. This implies that $W \subset R$ has maximal dimension m over k. □

Remark 8.5. Notice that in the proof of the second statement above, we could replace R by any τ-K-algebra $\widetilde{R} \subset R$, such that for any k-algebra B and any $\psi \in G(B)$, we have $\psi(\widetilde{R} \otimes B) \subset (\widetilde{R} \otimes B)$.

Proof of Theorem 8.2. Let M be a Picard-Vessiot field. Then $R_M := R \cap M$ is a Picard-Vessiot ring, which is generated by the entries of a matrix U solution of a difference linear system with coefficients in K, and its inverse. By definition of the difference Galois group, for any k-algebra B and any $\psi \in G(B)$ we have $\psi(R_M \otimes B) \subset R_M \otimes B$. It implies that we have a natural group morphism $G(B) \to \mathrm{Gal}(M/K)(B)$, given by the restriction of the morphisms. The kernel coincides with $H(B)$, hence H is a normal subgroup of G.

Let us suppose that H is a normal subgroup of G. We set $M = L^H$ and $R_M = R \cap M$, so that any $\varphi \in H(B)$ induces the identity over $R_M \otimes B$. Because of the normality of $H(B)$ in $G(B)$, any $\psi \in G(B)$ verifies $\psi(R_M \otimes B) \subset R_M \otimes B$. Finally Remark 8.5 shows that R_M is generated by the solution of a linear difference equations, and hence that it is a Picard-Vessiot ring. We deduce that M is the field of fraction of R_M because they both coincide with L^H. □

Remark 8.6. In the notation of the proof, for any k-algebra B, we have a functorial isomorphism

$$(G/H)(B) \cong \mathrm{Aut}^\tau(R_M \otimes_k B/K \otimes_k B),$$

which is actually an isomorphism of algebraic group.

We remind that $k_n = K^{\tau^n}$. See Example 2.2.

Corollary 8.7. *Let L and G be as above and let G° be the connected component of the identity of G. Then, L^{G° is the relative algebraic closure of K in L (and, hence in our framework coincides with $K(k_n)$, for a convenient positive integer n).*

Proof. Since G° is a normal subgroup of G, the finite quotient G/G° is isomorphic to $\mathrm{Gal}(L^{G^\circ}/K)$. Theorem 4.9 implies that L^{G°/K is an algebraic extensions, which is also finitely generated.

Let $\widetilde{L}$ be the relative algebraic closure of K in L. Then $L^{G^\circ} \subset \widetilde{L}$. Since any algebraic element of L over K is solution of a differential equation over K, $\widetilde{L}$ is also a Picard-Vessiot field, that therefore correspond to an algebraic subgroup H of G, in the sense that $\widetilde{L} = L^H$. The inclusion $L^{G^\circ} \subset \widetilde{L}$ implies that $H \subset G^\circ$. Moreover G/H is a finite group, because it must have dimension 0, after Theorem 4.9. Since G° is the smallest group such that the quotient G/G° is finite, we deduce that $H = G^\circ$ and therefore, from the Galois correspondence, that $\widetilde{L} = L^{G^\circ}$. □

A Behavior of the Galois group with respect to the iteration of τ

Let us consider the system (3.1) and its n-th iteration:

$$\tau^n y = A_n y, \text{ where } A_n := \tau^{n-1}(A) \cdots \tau(A) A. \tag{A.1}$$

We want to compare the Galois group of (3.1) with the Galois group of (A.1).

It follows from the Definition 3.5 of Picard-Vessiot ring and field that, if R (resp. L) is a Picard-Vessiot ring (resp. field) for (3.1) over K, $R(k_n)$ (resp. $L(k_n)$) is also a Picard-Vessiot ring (resp. field) for (A.1) over $K(k_n)$. Let $G_n := \mathrm{Gal}^{\tau^n}(L(k_n)/K(k_n))$, where we have add the superscript τ^n to the notation with the obvious meaning, to avoid any confusion.

Let G_1° be the identity component of G_1. By Corollary 8.7, there exists r, such that $k_r \subset L$ and that $\mathrm{Gal}^\tau(L/K(k_r)) = G_1^\circ$.

Lemma A.1. *In the notation above, we have* $\mathrm{Gal}^{\tau^r}(L/K(k_r)) = G_1^\circ \otimes_k k_r$.

Proof. By definition, for any k_r- algebra B, we have an injective morphisms from $G_1^\circ(B) \to \mathrm{Gal}^{\tau^r}(L/K(k_r))(B)$, indeed if a morphisms commutes with τ, it commutes also with τ^n. The equality follows from the fact that the groups are connected and that they have the same dimension, by Theorem 4.9. □

Proposition A.2. *In the notation introduced above, for any $n \geq r$, the Galois group of* (3.1) *over $K(k_n)$ is isomorphic to the Galois group of* (A.1) *over $K(k_n)$.*

Proof. The Galois group of (3.1) over $K(k_n)$ is $\mathrm{Gal}^{\tau}(L(k_n)/K(k_n)) \cong G_1^{\circ} \otimes_k k_n$. It can be naturally seen as a subgroup of $\mathrm{Gal}^{\tau^n}(L(k_n)/K(k_n))$. Equality follows from Theorem 4.9 and the connectedness of the groups, as in the proof of the previous lemma. □

References

[BK78] S.B. Bank and R.P. Kaufman, *A note on Hölder's theorem concerning the gamma function*, Mathematische Annalen **232** (1978), no. 2, 115–120.

[CHS08] Zoé Chatzidakis, Charlotte Hardouin, and Michael F. Singer, *On the definitions of difference Galois groups*, Model theory with applications to algebra and analysis. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 349, Cambridge Univ. Press, Cambridge, 2008, pp. 73–109.

[Coh65] Richard M. Cohn, *Difference algebra*, Interscience Publishers John Wiley & Sons, New York-London-Sydeny, 1965.

[DH19] Thomas Dreyfus and Charlotte Hardouin, *Length derivative of the generating series of walks confined in the quarter plane*, arXiv:1902.10558, 2019.

[DHR16] Thomas Dreyfus, Charlotte Hardouin, and Julien Roques, *Functional relations of solutions of q-difference equations*, arXiv:1603.06771, 2016.

[DHR18] ———, *Hypertranscendence of solutions of Mahler equations*, J. Eur. Math. Soc. (JEMS) **20** (2018), no. 9, 2209–2238.

[DHRS18] Thomas Dreyfus, Charlotte Hardouin, Julien Roques, and Michael F. Singer, *On the nature of the generating series of walks in the quarter plane*, Invent. Math. **213** (2018), no. 1, 139–203.

[DHRS20] ———, *Walks in the quarter plane: genus zero case*, J. Combin. Theory Ser. A **174** (2020), 105251, 25.

[Har08] Charlotte Hardouin, *Hypertranscendance des systèmes aux différences diagonaux*, Compositio Mathematica **144** (2008), no. 3, 565–581.

[Höl87] Otto Hölder, *Ueber die Eigenschaft der Gammafunction keiner algebraischen Differentialgleichung zu genügen*, Math. Ann. **28** (1887), 1–13.

[HR97] Yves Hellegouarch and François Recher, *Generalized t-modules*, J. Algebra **187** (1997), no. 2, 323–372.

[HS08] Charlotte Hardouin and Michael F. Singer, *Differential Galois theory of linear difference equations*, Math. Ann. **342** (2008), no. 2, 333–377. MR MR2425146 (2009j:39001)

[HSS16] Charlotte Hardouin, Jacques Sauloy, and Michael F. Singer, *Galois theories of linear difference equations: an introduction*, Mathematical Surveys and Monographs, vol. 211, American Mathematical Society, Providence, RI, 2016, Papers from the courses held at the CIMPA Research School in Santa Marta, July 23–August 1, 2012.

[Ish98] Katsuya Ishizaki, *Hypertranscendency of meromorphic solutions of a linear functional equation*, Aequationes Math. **56** (1998), no. 3, 271–283.

[Lev08] Alexander Levin, *Difference algebra*, Algebra and Applications, vol. 8, Springer, New York, 2008.

[Oga14] Hiroshi Ogawara, *Differential transcendency of a formal Laurent series satisfying a rational linear q-difference equation*, Funkcial. Ekvac. **57** (2014), no. 3, 477–488.

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

[Pap08] Matthew A. Papanikolas, *Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms*, Invent. Math. **171** (2008), no. 1, 123–174.

[Pel] Federico Pellarin, *From the carlitz exponential to drinfeld modular forms.*

[Pel13] ———, *On the generalized Carlitz module*, J. Number Theory **133** (2013), no. 5, 1663–1692.

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

[Pra86] C. Praagman, *Fundamental solutions for meromorphic linear difference equations in the complex plane, and related problems*, J. Reine Angew. Math. **369** (1986), 101–109. MR 850630 (88b:39004)

[TR] Floric Tavares Ribeiro, *On the stark units of drinfeld modules.*

[vdPS97] Marius van der Put and Michael F. Singer, *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666, Springer-Verlag, Berlin, 1997.

[vdPS03] ———, *Galois theory of linear differential equations*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 328, Springer-Verlag, Berlin, 2003.

[Wat79] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979.