On the Definitions of Difference Galois Groups

Zoé Chatzidakis[†]
CNRS - Université Paris 7

Charlotte Hardouin
Universität Heidelberg IWR INF 368

Michael F. Singer[‡]
University of North Carolina

Summary

We compare several definitions of the Galois group of a linear difference equation that have arisen in algebra, analysis and model theory and show, that these groups are isomorphic over suitable fields. In addition, we study properties of Picard-Vessiot extensions over fields with not necessarily algebraically closed subfields of constants.

1 Introduction

In the modern Galois theory of polynomials of degree n with coefficients in a field k[1], one associates to a polynomial $p(x)$ a splitting field K, that is a field K that is generated over k by the roots of $p(x)$. All such fields are k-isomorphic and this allows one to define the Galois group of $p(x)$ to be the group of k-automorphisms of such a K. If k is a differential field and $Y' = AY, A$ an $n \times n$ matrix with entries in k, one may be tempted to naively define a "splitting field" for this equation to be a differential field K containing k and generated (as a differential field) by the entries of a fundamental solution matrix Z of the differential equation[2]. Regrettably, such a field is not unique in general. For example,

† The author thanks the Isaac Newton Institute for Mathematical Sciences for its hospitality and financial support during spring 2005.
‡ The preparation of this paper was supported by NSF Grant CCR- 0096842 and by funds from the Isaac Newton Institute for Mathematical Sciences during a visit in May 2005.

1 All fields in this paper are assumed to be of characteristic zero.
2 that is, an invertible $n \times n$ matrix Z such that $Z' = AZ$. Note that the columns of Z form a basis of the solution space.

for the equation $y' = \frac{1}{2x}y$ over $k = \mathbb{C}(x), x' = 1$, the fields $k(x^{1/2})$ and $k(z), z$ transcendental over k and $z' = \frac{1}{2x}z$ are not k-isomorphic. If one insists that the constants $C_k = \{c \in k \mid c' = 0\}$ are algebraically closed and that K has no new constants, then Kolchin [16] showed that such a K exists (and is called the *Picard-Vessiot* associated with the equation) and is unique up to k-differential isomorphism. Kolchin [15] defined the Galois group of such a field to be the group of k-differential automorphisms of K and developed an appropriate Galois theory[3].

When one turns to difference fields k with automorphism σ and difference equations $\sigma Y = AY$, $A \in \mathrm{GL}_n(k)$, the situation becomes more complicated. One can consider difference fields K such that K is generated as a difference field by the entries of a fundamental solution matrix. If the field of constants $C_k = \{c \in k \mid \sigma(c) = c\}$ is algebraically closed and K has no new constants, then such a K is indeed unique and is again called a Picard-Vessiot extension ([23], Proposition 1.23 and Proposition 1.9). Unlike the differential case, there are equations for which such a field does not exist. In fact there are difference equations that do not have any nonzero solution in a difference field with algebraically closed constants. For example, let K be a difference field containing an element $z \neq 0$ such that $\sigma(z) = -z$. One then has that z^2 is a constant. If, in addition, the constants C_K of K are algebraically closed, then $z \in C_K$ so $\sigma(z) = z$, a contradiction. This example means that either one must consider "splitting fields" with subfields of constants that are not necessarily algebraically closed or consider "splitting rings" that are not necessarily domains. Both paths have been explored and the aim of this paper is to show that they lead, in essence, to the same Galois groups.

The field theoretic approach was developed by Franke[4] in [10] and succeeding papers. He showed that for Picard-Vessiot extension fields the Galois group is a linear algebraic group defined over the constants and that there is the usual correspondence between closed subgroups and intermediate difference fields. Franke notes that Picard-Vessiot extension fields do not always exist but does discuss situations when they do exist and results that can be used when adjoining solutions of a linear difference equation forces one to have new constants.

3 It is interesting to note that the Galois theory was developed before it was known if such K always exist. See the footnote on p.29 of [15].

4 Bialynicki-Birula [2] developed a general Galois theory for fields with operators but with restrictions that forced his Galois groups to be connected.

Another field theoretic approach is contained in the work of Chatzidakis and Hrushovski [4]. Starting from a difference field k, they form a certain large difference extension $\mathcal{U}$ having the properties (among others) that for any element in $\mathcal{U}$ but not in k, there is an automorphism of $\mathcal{U}$ that moves this element and that any set of difference equations (not necessarily linear) that have a solution in some extension of $\mathcal{U}$ already have a solution in $\mathcal{U}$. The subfield of constants $C_{\mathcal{U}}$ is not an algebraically closed field. Given a linear difference equation with coefficients in k, there exists a fundamental solution matrix with entries in $\mathcal{U}$. Adjoining the entries of these to $k(C_{\mathcal{U}})$ yields a difference field K. A natural candidate for a Galois group is the group of difference automorphisms of K over $k(C_{\mathcal{U}})$ and these do indeed correspond to points in a linear algebraic group. Equality of this automorphism group with the Galois group coming from Picard-Vessiot rings is shown in 4.15 under certain conditions (which are always verified when C_k is algebraically closed). Proofs are very algebraic in nature, and along the way produce some new algebraic results on Picard-Vessiot rings: we find numerical invariants of Picard-Vessiot rings of the equation $\sigma(X) = AX$, and show how to compute them (see 4.9 and 4.11). Furthermore, we show how to compute the number of primitive idempotents of a Picard-Vessiot ring when the field C_k is algebraically closed (4.13). This situation will be further discussed in Section 4.

The field theoretic approach also seems most natural in the analytic situation. For example, let $\mathcal{M}(\mathbb{C})$ be the field of functions $f(x)$ meromorphic on the complex plain endowed with the automorphism defined by the shift $\sigma(x) = x + 1$. Note that the constants $C_{\mathcal{M}(\mathbb{C})}$ are the periodic meromorphic functions. A theorem of Praagman [21] states that a difference equation with coefficients in $\mathcal{M}(\mathbb{C})$ will have a fundamental solution matrix with entries in $\mathcal{M}(\mathbb{C})$. If k is the smallest difference field containing the coefficients of the equation and $C_{\mathcal{M}(\mathbb{C})}$ and K is the smallest difference field containing k and the entries of fundamental solution matrix, then, in this context, the natural Galois group is the set of difference automorphisms of K over k. For example, the difference equation $\sigma(y) = -y$ has the solution $y = e^{\pi i x}$. This function is algebraic of degree 2 over the periodic functions $k = C_{\mathcal{M}(\mathbb{C})}$. Therefore, in this context the Galois group of $K = k(e^{\pi i x})$ over k is $\mathbb{Z}/2\mathbb{Z}$.

One can also consider the field $\mathcal{M}(\mathbb{C}^*)$ of meromorphic functions on the punctured plane $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ with $q-$automorphism $\sigma_q(x) = qx,\ |q| \neq 1$.

Difference equations in this context are q-difference equations and Praagman proved a global existence theorem in this context as well. The constants $C_{\mathcal{M}(\mathbb{C}^*)}$ naturally correspond to meromorphic functions on the elliptic curve $\mathbb{C}^*/q^{\mathbb{Z}}$ and one can proceed as in the case of the shift. One can also define local versions (at infinity in the case of the shift and at zero or infinity in the case of q-difference equations). In the local case and for certain restricted equations one does not necessarily need constants beyond those in $\mathbb{C}$ (see [9], [22], [23] as well as connections between the local and global cases. Another approach to q-difference equations is given by Sauloy in [26] and Ramis and Sauloy in [25] where a Galois group is produced using a combination of analytic and tannakian tools. The Galois groups discussed in these papers do not appear to act on rings or fields and, at present, it is not apparent how the techniques presented here can be used to compare these groups to other putative Galois groups.)

An approach to the Galois theory of difference equations with coefficients in difference fields based on rings that are not necessarily integral was presented in [23] (and generalized by André in [1] to include differential and difference equations with coefficients in fairly general rings as well). One defines a *Picard-Vessiot ring* associated with a difference equation $\sigma Y = AY$ with coefficients in a difference field k to be a simple difference ring (i.e., no σ-invariant ideals) R of the form $R = k[z_{i,j}, 1/\det(Z)]$ where $Z = (z_{i,j})$ is a fundamental solution matrix of $\sigma Y = AY$. Assuming that C_k is algebraically closed, it is shown in [23] that such a ring *always* exists and is unique up to k-difference isomorphism. A similar definition for differential equations yields a ring that is an integral domain and leads (by taking the field of quotients) to the usual theory of Picard-Vessiot extensions (see [24]). In the difference case, Picard-Vessiot rings need not be domains. For example, for the field $k = \mathbb{C}$ with the trivial automorphism, the Picard-Vessiot ring corresponding to $\sigma y = -y$ is $\mathbb{C}[Y]/(Y^2 - 1), \sigma(Y) = -Y$. Nonetheless, one defines the *difference Galois group of* $\sigma Y = AY$ to be the k-difference automorphisms of R and one can shows that this is a linear algebraic group defined over C_k. In the example above, the Galois group is easily seen to be $\mathbb{Z}/2\mathbb{Z}$. Furthermore, in general there is a Galois correspondence between certain subrings of the total quotient ring and closed subgroups of the Galois group.

The natural question arises: *How do these various groups relate to each*

other? The example of $\sigma(y) = -y$ suggests that the groups may be the same. Our main result, Theorem 2.9, states that all these groups are isomorphic as algebraic groups over a suitable extension of the constants. This result has interesting ramifications for the analytic theory of difference equations. In [11], the second author gave criteria to insure that solutions, meromorphic in $\mathbb{C}^*$, of a first order q-difference equation over $\mathbb{C}(x)$ satisfy no algebraic differential relation over $C_{\mathcal{M}(\mathbb{C}^*)}(x)$, where $C_{\mathcal{M}(\mathbb{C}^*)}$ is the field of meromorphic functions on the elliptic curve $\mathbb{C}^*/q^{\mathbb{Z}}$. The proof of this result presented in [11] depended on knowing the dimension of Galois groups in the analytic (i.e., field-theoretic) setting. These groups could be calculated in the ring theoretic setting of [23] and the results of the present paper allow one to transfer this information to the analytic setting. Although we will not go into more detail concerning the results of [11], we will give an example of how one can deduce transcendence results in the analytic setting from their counterparts in the formal setting.

The rest of the paper is organized as follows. In Section 2, we show how results of [23] and [24] can be modified to prove the correspondence of various Galois groups. In Section 3 we prove this result again in the special case of q-difference equations over $\mathbb{C}(x)$ using tannakian tools in the spirit of Proposition 1.3.2 of [14]. In Section 4, we discuss the model-theoretic approach in more detail and, from this point of view, show the correspondence of the Galois groups. In addition, we consider some additional properties of Picard-Vessiot rings over fields with constant subfields that are not necessarily algebraically closed. The different approaches and proofs have points of contacts (in particular, Proposition 2.4) and we hope comparisons of these techniques are enlightening.

The authors would like to thank Daniel Bertrand for suggesting the approach of Section 3 and his many other useful comments concerning this paper.

2 A Ring-Theoretic Point of View

In this section we shall consider groups of difference automorphisms of rings and fields generated by solutions of linear difference equations and show that these groups are isomorphic, over the algebraic closure of the constants to the Galois groups defined in [24]. We begin by defining the rings and fields we will study.

Definition 2.1 Let K be a difference field with automorphism σ and let $A \in \mathrm{GL}_n(K)$.

a. We say that a difference ring extension R of K is a *weak Picard-Vessiot ring* for the equation $\sigma X = AX$ if

(i) $R = K[Z, \frac{1}{\det(Z)}]$ where $Z \in \mathrm{GL}_n(R)$ and $\sigma Z = AZ$ and
(ii) $C_R = C_K$.

b. We say that a difference field extension L of K is a *weak Picard-Vessiot field* for $\sigma X = AX$ if $C_L = C_K$ and L is the quotient field of a weak Picard-Vessiot ring of $\sigma X = AX$.

In [23], the authors define a *Picard-Vessiot ring* for the equation $\sigma Y = AY$ to be a difference ring R such that (i) holds and in addition R is simple as a difference ring, that is, there are no σ-invariant ideals except (0) and R. When C_K is algebraically closed, Picard-Vessiot rings exist, are unique up to K-difference isomorphisms and have the same constants as K ([23], Section 1.1). Therefore in this case, the Picard-Vessiot ring will be a weak Picard-Vessiot ring.

In general, even when the field of constants is algebraically closed, Example 1.25 of [23] shows that there will be weak Picard-Vessiot rings that are not Picard-Vessiot rings. Furthermore this example shows that the quotient field of a weak Picard-Vessiot integral domain R need not necessarily have the same constants as R so the requirement that $C_L = C_K$ is not superfluous.

The Galois theory of Picard-Vessiot rings is developed in [23] for Picard-Vessiot rings R over difference fields K with algebraically closed constants C_K. In particular, it is shown ([23], Theorem 1.13) that the groups of difference K-automorphisms of R over K corresponds to the set of C_K-points of a linear algebraic group defined over C_K. A similar result for differential equations is proven in ([24], Theorem 1.27). It has been observed by many authors beginning with Kolchin ([17], Ch. VI.3 and VI.6; others include [1], [7], [6], [14], [18] in a certain characteristic p setting for difference equations) that one does not need C_k to be algebraically closed to achieve this latter result. Recently, Dyckerhoff [8] showed how the proof of Theorem 1.27 of [24] can be adapted in the differential case to fields with constants that are not necessarily

algebraically closed. We shall give a similar adaption in the difference case.

Proposition 2.2 *Let K be a difference field of characteristic zero and let $\sigma Y = AY, A \in \mathrm{GL}_n(K)$ be a difference equation over K. Let R be a weak Picard-Vessiot ring for this equation over K. The group of difference K-automorphisms of R can be identified with the C_K-points of a linear algebraic group G_R defined over C_K.*

Proof. We will define the group G_R by producing a representable functor from the category of commutative C_K-algebras to the category of groups (c.f., [27]).

First, we may write $R = K[Y_{i,j}, \frac{1}{\det(Y)}]/q$ as the quotient of a difference ring $K[Y_{i,j}, \frac{1}{\det(Y)}]$, where $Y = \{Y_{i,j}\}$ is an $n \times n$ matrix of indeterminates with $\sigma Y = AY$, by a σ-ideal q. Let $C = C_K$. For any C-algebra B, one defines the difference rings $K \otimes_C B$ and $R \otimes_C B$ with automorphism $\sigma(f \otimes b) = \sigma(f) \otimes b$ for $f \in K$ or R. In both cases, the ring of constants is B. We define the functor $\mathcal{G}_R$ as follows: the group $\mathcal{G}_R(B)$ is the group of $K \otimes_C B$-linear automorphisms of $R \otimes_C B$ that commute with σ. One can show that $\mathcal{G}_R(B)$ can be identified with the group of matrices $M \in \mathrm{GL}_n(B)$ such that the difference automorphism ϕ_M of $R \otimes_C B$, given by $(\phi_M Y_{i,j}) = (Y_{i,j})M$, has the property that $\phi_M(q) \subset (q)$ where (q) is the ideal of $K[Y_{i,j}, \frac{1}{\det(Y_{i,j})}] \otimes_C B$ generated by q.

We will now show that $\mathcal{G}_R$ is representable. Let $X_{s,t}$ be new indeterminates and let $M_0 = (X_{s,t})$. Let $q = (q_1, \ldots, q_r)$ and write $\sigma_{M_0}(q_i)$ mod $(q) \in R \otimes_C C[X_{s,t}, \frac{1}{\det(X_{s,t})}]$ as a finite sum

$$\sum_i C(M_0, i, j) e_i \text{ with all } C(M_0, i, j) \in C[X_{s,t}, \frac{1}{\det(X_{s,t})}] \ ,$$

where $\{e_i\}_{i \in I}$ is a C-basis of R. Let I be the the ideal in $C[X_{s,t}, \frac{1}{\det(X_{s,t})}]$ generated by all the $C(M_0, i, j)$. We will show that

$$U := C[X_{s,t}, \frac{1}{\det(X_{s,t})}]/I$$

represents $\mathcal{G}_R$.

Let B be a C-algebra and $\phi \in \mathcal{G}_R(B)$ identified with ϕ_M for some

$M \in \mathrm{GL}_n(B)$. One defines the C-algebra homomorphism

$$\Phi : C[X_{s,t}, \frac{1}{\det(X_{s,t})}] \to B, \qquad (X_{s,t}) \mapsto M.$$

The condition on M implies that the kernel of Φ contains I. This then gives a unique C-algebra homomorphism

$$\Psi : U \to B, \qquad \Psi(M_0 \mod I) \mapsto M.$$

The Yoneda Lemma can now be used to show that $G_R = \mathrm{Spec}(U)$ is a linear algebraic group (see Appendix B, p. 382 of [24] to see how this is accomplished or Section 1.4 of [27]). □

We will refer to G_R as the *Galois group* of R. When R is a Picard-Vessiot extension of K, we have the usual situation. We are going to compare the groups associated with a Picard-Vessiot extension and weak Picard-Vessiot field extensions for the same equation over different base fields. We will first show that extending a Picard-Vessiot ring by constants yields a Picard-Vessiot ring whose associated group is isomorphic to the original group over the new constants. In the differential case and when the new constants are algebraic over the original constants this appears in Dyckerhoff's work ([8], Proposition 1.18 and Theorem 1.26). Our proof is in the same spirit but without appealing to descent techniques. We will use Lemma 1.11 of [23], which we state here for the convenience of the reader:

Lemma 2.3 *Let R be a Picard-Vessiot ring over a field k with $C_R = C_k$[5] and A be a commutative algebra over C_k. The action of σ on A is supposed to be the identity. Let N be an ideal of $R \otimes_{C_k} A$ that is invariant under σ. Then N is generated by the ideal $N \cap A$ of A.*

Proposition 2.4 *Let $k \subset K$ be difference fields of characteristic zero and $K = k(C_K)$. Let R be a Picard-Vessiot ring over k with $C_R = C_k$ for the equation $\sigma X = AX, A \in \mathrm{GL}_n(k)$. If $R = k[Y, \frac{1}{\det(Y)}]/q$ where Y is an $n \times n$ matrix of indeterminates, $\sigma Y = AY$ and q is a maximal σ-ideal, then $S = K[Y, \frac{1}{\det(Y)}]/qK$ is a Picard-Vessiot extension of K for the same equation. Furthermore, $C_S = C_K$.*

5 The hypothesis $C_R = C_k$ is not explicitly stated in the statement of this result in [23] but is assumed in the proof.

Proof. First note that the ideal $qK \neq K[Y, \frac{1}{\det(Y)}]$. Secondly, Lemma 2.3 states that for R as above and A a commutative C_k algebra with identity, any σ-ideal N of $R \otimes_{C_k} A$ (where the action of σ on A is trivial) is generated by $N \cap A$. This implies that the difference ring $R \otimes_{C_k} C_K$ is simple. Therefore the map $\psi : R \otimes_{C_k} C_K \to S = K[Y, \frac{1}{\det(Y)}]/(q)K$ where $\psi(a \otimes b) = ab$ is injective. Let R' be the image of ψ. One sees that any element of S is of the form $\frac{a}{b}$ for some $a \in R', b \in k[C_k] \subset R'$. Therefore any ideal I in S is generated by $I \cap R'$ and so S is simple.

For any constant $c \in S$, the set $J = \{a \in R' \mid ac \in R'\} \subset R'$ is a nonzero σ-ideal so $c \in R'$. Since the constants of R' are C_K, this completes the proof. □

Corollary 2.5 *Let R and S be as in Proposition 2.4. If G_R and G_S are the Galois groups associated with these rings as in Proposition 2.2, then G_R and G_S are isomorphic over C_K.*

Proof. We are considering G_R as the functor from C_k algebras A to groups defined by $G_R(A) := Aut(R \otimes_{C_k} A)$ where $Aut(..)$ is the group of difference $k \otimes A$-automorphisms. Let T_R be the finitely generated C_k-algebra representing G_R (i.e., the coordinate ring of the group). Similarly, let T_S be the C_K-algebra representing G_S. We define a new functor F from C_K-algebras to groups as $F(B) := Aut((R \otimes_{C_k} C_K) \otimes_{C_K} B)$. One checks that F is also a representable functor represented by $T_R \otimes_{C_k} C_K$. Using the embedding ψ of the previous proof, one sees that $F(B) = Aut(S \otimes_{C_K} B) = G_R(B)$ for any C_K-algebra B. The Yoneda Lemma implies that $T_R \otimes_{C_k} C_K \simeq T_S$. □

In Proposition 2.7 we will compare Picard-Vessiot rings with weak Picard-Vessiot fields for the same difference equation. To do this we need the following lemma. A version of this in the differential case appears as Lemma 1.23 in [24].

Lemma 2.6 *Let L be a difference field. Let $Y = (Y_{i,j})$ be and $n \times n$ matrix of indeterminates and extend σ to $L[Y_{i.j}, \frac{1}{\det(Y)}]$ by setting $\sigma(Y_{i,j}) = Y_{i,j}$. The map $I \mapsto (I) = I \cdot L[Y_{i.j}, \frac{1}{\det(Y)}]$ from the set of ideals in $C_L[Y_{i.j}, \frac{1}{\det(Y)}]$ to the set of ideals of $L[Y_{i.j}, \frac{1}{\det(Y)}]$ is a bijection.*

Proof. One easily checks that $(I) \cap C_L[Y_{i.j}, \frac{1}{\det(Y)}] = I$. Now, let J be an ideal of $L[Y_{i.j}, \frac{1}{\det(Y)}]$ and let $I = J \cap C_L[Y_{i.j}, \frac{1}{\det(Y)}]$. Let $\{e_i\}$ be a

basis of $C_L[Y_{i.j}, \frac{1}{\det(Y)}]$ over C_L. Given $f \in L[Y_{i.j}, \frac{1}{\det(Y)}]$, we may write f uniquely as $f = \sum f_i e_i,\ f_i \in L$. Let $\ell(f)$ be the number of i such that $f_i \neq 0$. We will show, by induction on $\ell(f)$, that for any $f \in J$, we have $f \in (I)$. If $\ell(f) = 0, 1$ this is trivial. Assume $\ell(f) > 1$. Since L is a field, we can assume that there exists an i_1 such that $f_{i_1} = 1$. Furthermore, we may assume that there is an $i_2 \neq i_1$ such that $f_{i_2} \in L \backslash C_L$. We have $\ell(f - \sigma(f)) < \ell(f)$ so $\sigma(f) - f \in (I)$. Similarly, $\sigma(f_{i_2}^{-1} f) - f_{i_2}^{-1} f \in (I)$. Therefore, $(\sigma(f_{i_2}^{-1}) - f_{i_2}^{-1}) f = \sigma(f_{i_2}^{-1})(f - \sigma(f)) + (\sigma(f_{i_2}^{-1} f) - f_{i_2}^{-1} f) \in (I)$. This implies that $f \in (I)$. □

The following is a version of Proposition 1.22 of [24] modified for difference fields taking into account the possibility that the constants are not algebraically closed.

Proposition 2.7 *Let K be a difference field with constants C and let $A \in \mathrm{GL}_n(K)$. Let $S = K[U, \frac{1}{\det(U)}],\ U \in \mathrm{GL}_n(S),\ \sigma(U) = AU$ be a Picard-Vessiot extension of K with $C_S = C_k$ and let $L = K(V),\ V \in GL_n(L),\ \sigma(V) = AV$ be a weak Picard-Vessiot field extension of K. Then there exists a K-difference embedding $\rho : S \to L \otimes_C \overline{C}$ where $\overline{C}$ is the algebraic closure of C and σ acts on $L \otimes_C \overline{C}$ as $\sigma(v \otimes c) = \sigma(v) \otimes c$.*

Proof. Let $X = (X_{i,j})$ be an $n \times n$ matrix of indeterminates over L and let $S_0 := K[X_{i,j}, \frac{1}{\det(X)}] \subset L[X_{i,j}, \frac{1}{\det(X)}]$. We define a difference ring structure on $L[X_{i,j}, \frac{1}{\det(X)}]$ by setting $\sigma(X) = AX$ and this gives a difference ring structure on S_0. Abusing notation slightly, we may write $S = S_0/p$ where p is a maximal σ-ideal of S_0. Define elements $Y_{i,j} \in L[X_{i,j}, \frac{1}{\det(X)}]$ via the formula $(Y_{i,j}) = V^{-1}(X_{i,j})$. Note that $\sigma Y_{i,j} = Y_{i,.j}$ for all i, j and that $L[X_{i,j}, \frac{1}{\det(X)}] = L[Y_{i,j}, \frac{1}{\det(Y)}]$. Define $S_1 := C[Y_{i,j}, \frac{1}{\det(Y)}]$. The ideal $p \subset S_0 \subset L[Y_{i,j}, \frac{1}{\det(Y)}]$ generates an ideal (p) in $L[Y_{i,j}, \frac{1}{\det(Y)}]$. We define $\tilde{p} = (p) \cap S_1$. Let m be a maximal ideal in S_1 such that $\tilde{p} \subset m$. We then have a homomorphism

$$S_1 \to S_1/m \to \overline{C}.$$

We can extend this to a homomorphism

$$\psi : L[Y_{i,j}, \frac{1}{\det(Y)}] = L \otimes_C S_1 \to L \otimes_C \overline{C}.$$

Restricting ψ to S_0, we have a difference homomorphism

$$\psi : S_0 \to L \otimes_C \overline{C}$$

whose kernel contains p. Since p is a maximal σ-ideal we have that this kernel is p. Therefore ψ yields an embedding

$$\rho : S = S_0/p \to L \otimes_C \overline{C}.$$

□

Corollary 2.8 *Let $K, C, \overline{C}, S, L$, ρ be as above and let $T = K[V, \frac{1}{\det(V)}]$. Then ρ maps $S \otimes_C \overline{C}$ isomorphically onto $T \otimes_C \overline{C}$. Therefore the Galois group G_S is isomorphic to G_T over $\overline{C}$.*

Proof. In Proposition 2.7, we have that $\rho(U) = V(c_{i,j})$ for some $(c_{i,j}) \in \mathrm{GL}_n(\overline{C})$. Therefore ρ is an isomorphism. The isomorphism of G_S and G_T over $\overline{C}$ now follows in the same manner as the conclusion of Corollary 2.5. □

We can now prove the following result.

Theorem 2.9 *Let*

1. *k be a difference field with algebraically closed field of constants C,*
2. *$\sigma Y = AY$ be a difference equation with $A \in \mathrm{GL}_n(k)$ and let R be the Picard-Vessiot ring for this equation over k,*
3. *K a difference field extension of k such that $K = k(C_K)$*
4. *L a weak Picard-Vessiot field for the equation $\sigma(Y) = AY$ over K.*

Then

a. *If we write $L = K(V)$ where $V \in \mathrm{GL}_n(L)$ and $\sigma V = AV$ then $R \otimes_C \overline{C}_K \simeq K[V, \frac{1}{\det(V)}] \otimes_{C_K} \overline{C}_K$ where $\overline{C}_K$ is the algebraic closure of C_K. Therefore $K[V, \frac{1}{\det(V)}]$ is also a Picard-Vessiot extension of K.*
b. *The Galois groups of R and $K[V, \frac{1}{\det(V)}]$ are isomorphic over $\overline{C}_K$.*

Proof. Let $Y = (Y_{i,j})$ be an $n \times n$ matrix of indeterminates and write $R = k[Y_{i,j}, \frac{1}{\det(Y)}]/(p)$, where (p) is a maximal σ-ideal. Assumptions 1. and 2. imply that $C_R = C_k$ ([23],Lemma 1.8) so Propostion 2.4 implies that $S = K[Y_{i,j}, \frac{1}{\det(Y)}]/(p)K$ is a Picard-Vessiot ring with constants C_K. Corollary 2.5 implies that its Galois group G_R is isomorphic over C to G_S. Corolary 2.8 finishes the proof. □

3 A Tannakian Point of View

In this section we shall give another proof of Theorem 2.9 for q-difference equations in the analytic situation. Let $\mathcal{M}(\mathbb{C}^*)$ be the field of functions $f(x)$ meromorphic on $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ with the automorphism $\sigma(f(x)) = f(qx)$ where $q \in \mathbb{C}^*$ is a fixed complex number with $|q| \neq 1$. As noted before, the constants $C_{\mathcal{M}(\mathbb{C}^*)}$ in this situation correspond to meromorphic functions $\mathcal{M}(E)$ on the elliptic curve $E = \mathbb{C}^*/q^{\mathbb{Z}}$. We shall show how the theory of tannakian categories also yields a proof of Theorem 2.9 when $k = \mathbb{C}(x)$ and $K = k(C_{\mathcal{M}(\mathbb{C}^*)})$.

We shall assume that the reader is familiar with some basic facts concerning difference modules ([23], Ch. 1.4) and tannakian categories ([7],[6]; see [24], Appendix B or [3] for an overview). We will denote by $\mathcal{D}_k = k[\sigma, \sigma^{-1}]$ (resp. $\mathcal{D}_K = K[\sigma, \sigma^{-1}]$) the rings of difference operators over k (resp. K). Following ([23], Ch. 1.4), we will denote by $\mathit{Diff}(k, \sigma)$ (resp. by $\mathit{Diff}(K, \sigma)$) the category of difference-modules over k (resp. K). The ring of endomorphisms of the unit object is equal to $\mathbb{C}$ (resp. $C_K = C_{\mathcal{M}(\mathbb{C}^*)} = \mathcal{M}(E)$) the field of constants of k (resp. K).

Let M be a $\mathcal{D}_k$-module of finite type over k. We will denote by $M_K = M \otimes_k K$ the $\mathcal{D}_K$-module constructed by extending the field k to K. We will let $\{\{M\}\}$ (resp. $\{\{M_K\}\}$) denote the full abelian tensor subcategory of $\mathit{Diff}(k, \sigma)$ (resp. $\mathit{Diff}(K, \sigma)$) generated by M (resp. M_K) and its dual M^* (resp. ${M_K}^*$).

Theorem 1.32 of [23] gives a fiber functor ω_M over $\mathbb{C}$ for $\{\{M\}\}$. In [21], Praagman gave an existence theorem (see Section 1) for q-difference equations which can be used to construct a fiber functor ω_{M_K} for $\{\{M_K\}\}$ over C_K (described in detail in Proposition 3.9 below). In particular, $\{\{M\}\}$ and $\{\{M_K\}\}$ are neutral tannakian categories over $\mathbb{C}$ and C_K respectively. The main task of this section is to compare the Galois groups associated to the fiber functors ω_M and ω_{M_K}. We will prove the following theorem:

Theorem 3.1 *Let $M \in \mathit{Diff}(k, \sigma)$ be a $\mathcal{D}_k$-module of finite type over k. Then*

$$\mathit{Aut}^{\otimes}(\omega_M) \otimes_{\mathbb{C}} \overline{C_K} \simeq \mathit{Aut}^{\otimes}(\omega_{M_K}) \otimes_{C_K} \overline{C_K}.$$

The proof is divided in two parts. In the first part, we will construct a fiber functor $\tilde{\omega}_M$ from $\{\{M_K\}\}$ to $Vect_{C_K}$, which *extends* ω_M and we will

compare its Galois group to that associated to ω_M. In the second part, we will compare the Galois group associated to ω_{M_K} and the Galois group associated to $\tilde{\omega}_M$, and finally relate these groups to the Galois groups considered in Theorem 2.9.b).

3.1 The action of $\mathrm{Aut}(C_K/\mathbb{C})$ *on* $\{\{M_K\}\}$

A module $M_K = M \otimes_k K$ is constructed from the module M essentially by extending the scalars from $\mathbb{C}$ to C_K. In order to compare the subcategories $\{\{M\}\}$ and $\{\{M_K\}\}$ they generate, it seems natural therefore to consider an action of the automorphism group $\mathrm{Aut}(C_K/\mathbb{C})$ on M_K as well as on $\{\{M_K\}\}$. Before we define this action we state some preliminary facts.

Lemma 3.2 *We have:*

1. *The fixed field* $C_K^{\mathrm{Aut}(C_K/\mathbb{C})}$ *is* $\mathbb{C}$.
2. $K \simeq C_K(X)$ *where* $C_K(X)$ *denotes the field of rational functions with coefficients in* C_K. *This isomorphism maps* $\mathbb{C}(X)$ *isomorphically onto* k.

Proof. 1. For all $c \in \mathbb{C}^*$, the restriction to C_K of the map σ_c which associates to $f(x) \in C_K$ the function $\sigma_c(f)(x) = f(cx)$ defines an element of $\mathrm{Aut}(C_K/\mathbb{C})$. Let $\phi \in C_K^{\mathrm{Aut}(C_K/\mathbb{C})}$, the fixed field of $\mathrm{Aut}(C_K/\mathbb{C})$. Because $\sigma_c(\phi) = \phi$ for any $c \in \mathbb{C}^*$, ϕ must be constant.

2. For any $f(X) \in C_K[X]$, put $\phi(f) = f(z)$, viewed as a meromorphic function of the variable $z \in \mathbb{C}^*$. Then, ϕ is a morphism from $C_E[X]$ to K_E. We claim that ϕ is injective. Indeed, let us consider a dependence relation:

$$\sum c_i(z)k_i(z) = 0, \forall z \in \mathbb{C} \tag{1}$$

where $c_i \in C_E$ and $k_i \in K$. Using Lemma II of ([5], p. 271) or the Lemma of ([9], p. 5) the relation (1) implies that

$$\sum c_i(z)k_i(X) = 0, \forall z \in \mathbb{C}. \tag{2}$$

So ϕ extends to the function field $C_K(X)$, whose image is the full K. Notice that, by definition of ϕ, $\mathbb{C}(X)$ maps isomorphically on k. □

Since $\mathrm{Aut}(C_K/\mathbb{C})$ acts on $C_K(X)$ (via its action on coefficients), we can consider its action on K.

Lemma 3.3 *1. The action of* $\mathrm{Aut}(C_K/\mathbb{C})$ *on* K *extends the natural action of* $\mathrm{Aut}(C_K/\mathbb{C})$ *on* C_K*. Moreover the action of* $\mathrm{Aut}(C_K/\mathbb{C})$ *on* K *is trivial on* k*.*

2. $K^{\mathrm{Aut}(C_K/\mathbb{C})} = k$*.*

3. The action of $\mathrm{Aut}(C_K/\mathbb{C})$ *on* K *commutes with the action of* σ_q*.*

Proof. 1. This comes from the definition of the action of $\mathrm{Aut}(C_K/\mathbb{C})$ on K. Because $\mathrm{Aut}(C_K/\mathbb{C})$ acts trivially on $\mathbb{C}(X)$, its action on k is also trivial.

2. Because of Lemma 3.2, $C_K^{\mathrm{Aut}(C_K/\mathbb{C})} = \mathbb{C}$. Thus, by construction $K^{\mathrm{Aut}(C_K/\mathbb{C})} = k$.

3. Let i be a natural integer and $f(X) = cX^i$ where $c \in C_K$. Then

$$\tau(\sigma_q(f)) = \tau(cq^iX^i) = \tau(c)q^iX^i = \sigma_q(\tau(f))$$

with $\tau \in \mathrm{Aut}(C_K/\mathbb{C})$. Thus, the action of $\mathrm{Aut}(C_K/\mathbb{C})$ commutes with σ_q on $C_K[X]$. It therefore commutes on $C_K(X) = K$. □

Before we finally define the action of $\mathrm{Aut}(C_K/\mathbb{C})$ on $\{\{M_K\}\}$, we need one more definition.

Definition 3.4 Let F be a field of caracteristic zero and V be a F-vector space of finite dimension over F. We denote by $Constr_F(V)$ any *construction of linear algebra* applied to V inside $Vect_F$, that is to say any vector space over F obtained by tensor products over F, direct sums, symetric and antisymetric products on V and its dual $V^* := Hom_{F-lin}(V, F)$.

Lemma 3.5 *Let* V *be a vector space of finite dimension over* k *(respectively over* $\mathbb{C}$*). Then,* $Constr_k(V) \otimes_k K = Constr_K(V \otimes K)$ *(respectively* $Constr_{\mathbb{C}}(V) \otimes C_K = Constr_{C_K}(V \otimes C_K)$*). In other words, the constructions of linear algebra commute with the scalar extension.*

Proof. Consider for instance $Constr_k(V) = Hom_{k-lin}(V, k)$. Because V is of finite dimension over k, we have

$$Hom_{k-lin}(V, k) \otimes_k K = Hom_{K-lin}(V \otimes_k K, K).$$

□

To define the action of $\mathrm{Aut}(C_K/\mathbb{C})$ on $\{\{M_K\}\}$ we note that for any object N of $\{\{M_K\}\}$, there exists, by definition, a construction $M' = Constr_k(M)$ such that $N \subset M' \otimes_k K$. Let now $M' = Constr_k(M)$ be a construction of linear algebra applied to M. The Galois group $\mathrm{Aut}(C_K/\mathbb{C})$ acts on $M'_K = M' \otimes_k K$ via the semi-linear action $(\tau \to id \otimes \tau)$. It therefore permutes the objects of $\{\{M_K\}\}$. It remains to prove that this permutation is well defined and is independent of the choice of the construction in which these objects lie. If there exist M_1 and M_2 two objects of $Constr_k(M)$ such that $N \subset M_1 \otimes_k K$ and $N \subset M_2 \otimes_k K$. Then, by a diagonal embedding $N \subset (M_1 \oplus M_2) \otimes_k K$. The action of $\mathrm{Aut}(C_K/\mathbb{C})$ on $(M_1 \oplus M_2) \otimes_k K$ is the direct sum of the action of $\mathrm{Aut}(C_K/\mathbb{C})$ on $M_1 \otimes_k K$ with the action of $\mathrm{Aut}(C_K/\mathbb{C})$ on $M_2 \otimes_k K$.This shows that the restriction of the action of $\mathrm{Aut}(C_K/\mathbb{C})$ on $M_1 \otimes_k K$ to N is the same as the restriction of the action of $\mathrm{Aut}(C_K/\mathbb{C})$ on $M_2 \otimes_k K$ to N. Thus, the permutation is independent of the choice of the construction in which these objects lie.

3.2 Another fiber functor $\tilde{\omega}_M$ for $\{\{M_K\}\}$

We now extend ω_M to a fiber functor $\tilde{\omega}_M$ on the category $\{\{M_K\}\}$. For this purpose, we appeal to Proposition 2.4 to conclude that *if R be a Picard-Vessiot ring for M over k and $\sigma X = AX, A \in \mathrm{GL}_n(k)$ be an equation of M over k. If $R = K[Y, \frac{1}{det(Y)}]/I$ where Y is an $n \times n$ matrix of indeterminates, $\sigma Y = AY$ and I is a maximal σ-ideal, then $R_K = R \otimes_k K$ is a weak Picard-Vessiot ring for M_K over K.*

We then have the following proposition-definition:

Proposition 3.6 *For any object N of $\{\{M_K\}\}$ let*

$$\tilde{\omega}_M(N) = \mathrm{Ker}(\sigma - Id, R_K \otimes_K N).$$

Then $\tilde{\omega}_M : \{\{M_K\}\} \to Vect_{C_K}$ is a faithful exact, C_K-linear tensor functor. Moreover, $\tilde{\omega}_M(N \otimes K) = \omega_M(N) \otimes C_K$ for every $N \in \{\{M\}\}$.

Proof. Because of the existence of a fundamental matrix with coefficients in R_K, $\tilde{\omega}_M(M_K)$ satisfies $R_K \otimes_{K_K} M_K = R_K \otimes_{C_K} \tilde{\omega}_M(M_K)$. Let $\sigma X = AX, A \in \mathrm{GL}_n(k)$ be an equation of M over k and $R = k[Y, \frac{1}{det(Y)}]/I$ be its corresponding Picard-Vessiot ring over k. Let M' be a construction of linear algebra applied to M over k. Then R_K contains a fundamental

matrix of $M' \otimes K$. This comes from the fact that an equation of M' is obtained from the same construction of linear algebra applied to A. Moreover, if $N \in \{\{M_K\}\}$, then R contains also a fundamental matrix for N. Indeed, there exists M', a construction of linear algebra applied to M over k, such that $N \subset M' \otimes K$. Now, R_K contains the entries of a fundamental solution matrix of N and this matrix is invertible because its determinant divides the determinant of a fundamental matrix of solutions of $M' \otimes K$. Thus, $R_K \otimes_K N = R_K \otimes_{C_K} \tilde{\omega}_M(N)$. We deduce from this fact, that $\tilde{\omega}_M$ is a faithful, exact, C_K-linear tensor functor.

For every $N \in \{\{M\}\}$, we have a natural inclusion of C_K-vector spaces of solutions $\omega_M(N) \otimes C_K \subset \tilde{\omega}_M(N \otimes K)$. Since their dimensions over C_K are both equal to the dimension of N over k, they must coincide. □

3.3 Comparison of the Galois groups

Let $M' = Constr_K(M)$ be a construction of linear algebra applied to M. The group $\mathrm{Aut}(C_K/\mathbb{C})$ acts on $\tilde{\omega}_M(M'_K) = \omega_M(M') \otimes_{\mathbb{C}} C_K$ via the semi-linear action $(\tau \to id \otimes \tau)$. It therefore permutes the objects of the tannakian category generated by $\omega_M(M) \otimes_{\mathbb{C}} C_K$ inside $Vect_{C_K}$.

Lemma 3.7 *Let N be an object of $\{\{M_K\}\}$ and τ be an element of $\mathrm{Aut}(C_K/\mathbb{C})$. Then, for the actions of $\mathrm{Aut}(C_K/\mathbb{C})$ defined as above and in Section 3.1, we have:*

$$\tau(\tilde{\omega}_M(N)) = \tilde{\omega}_M(\tau(N))$$

(equality inside $\omega_M(M') \otimes_{\mathbb{C}} C_K$ for any $M' = Constr_k(M)$ such that $N \subset M' \otimes K$.)

Proof. Let $M' = Constr_K M$ be such that $N \subset M' \otimes_k K$ and consider the action of $\mathrm{Aut}(C_K/\mathbb{C})$ on $R \otimes_k (M' \otimes_k K)$ defined by $id \otimes id \otimes \tau$.

This allows us to consider the action of $\mathrm{Aut}(C_K/\mathbb{C})$ on $R_K \otimes_K N = R \otimes_k N$. By definition, we have

$$\tau(R_K \otimes_K N) = R \otimes_k (\tau(N)) = R_K \otimes_K \tau(N)$$

for all $\tau \in \mathrm{Aut}(C_K/\mathbb{C})$. Moreover inside $R \otimes_k (M' \otimes K)$, the action of $\mathrm{Aut}(C_K/\mathbb{C})$ commutes with the action of σ_q (see Lemma 3.3). Therefore

$$\tau(\mathrm{Ker}(\sigma_q - Id, R_K \otimes_K N)) = \mathrm{Ker}(\sigma_q - Id, R_K \otimes_K \tau(N)).$$

□

The next proposition is Corollary 2.5, but we shall now give a tannakian proof of it, following the proof of ([14], Lemma 1.3.2).

Proposition 3.8 $Aut^{\otimes}(\omega_M) \otimes C_K = Aut^{\otimes}(\tilde{\omega}_M)$.

Proof. By definition, $Aut^{\otimes}(\tilde{\omega}_M) = Stab(\tilde{\omega}_M(W),\ W \in \{\{M_K\}\})$ is the stabilizer inside $\mathcal{G}l(\tilde{\omega}_M(M_K)) = \mathcal{G}l(\omega_M(M)) \otimes C_K$ of the fibers of all the sub-equations W of M_K. Similarly, $Aut^{\otimes}(\omega_M) = Stab(\omega_M(W)),\ W \in \{\{M\}\})$, so that the following inclusion holds:

$$Aut^{\otimes}(\tilde{\omega}_M) \subset Aut^{\otimes}(\omega_M) \otimes C_K.$$

The semi-linear action of $\mathrm{Aut}(C_K/\mathbb{C})$ permutes the sub-$\mathcal{D}_K$-modules W of $\{\{M_K\}\}$ and the fixed field of C_K of Γ_E is $\mathbb{C}$ (see Lemma 3.2.1). Therefore $Aut^{\otimes}(\tilde{\omega}_M)$ *is defined* over $\mathbb{C}$, i.e., it is of the form $G \otimes C_K$ for a unique subgroup $G \subset Aut^{\otimes}(\omega_M)$. By Chevalley's theorem, G is defined as the stabilizer of one $\mathbb{C}$-subspace V of $\omega_M(M')$ for some construction $M' = Constr_k(M)$.

We must show that V is stable under $Aut^{\otimes}(\omega_M)$, i.e., we must show that V is of the form $\omega_M(N)$ for $N \in \{\{M\}\}$. Because $G \otimes C_K = Aut^{\otimes}(\tilde{\omega}_M)$ leaves $V \otimes C_K$ stable, we know that there exists $N \in \{\{M_K\}\}$ with $\tilde{\omega}_M(N) = V \otimes C_K$. For any $\tau \in \mathrm{Aut}(C_K/\mathbb{C})$,

$$\tilde{\omega}_M(N) = V \otimes C_K = \tau(V \otimes C_K) = \tau(\tilde{\omega}_M(N)) = \tilde{\omega}_M(\tau(N)),$$

in view of Lemma 3.7. We therefore deduce from Proposition 3.6 that $\tau(N) = N$ for any $\tau \in \mathrm{Aut}(C_K/\mathbb{C})$. Consequently, N is *defined over* K (see Lemma 3.3.3)), i.e., it is of the form $N \otimes K$, where $N \in \{\{M\}\}$. □

We need to define one more functor before we finish the proof of Theorem 3.1.

Proposition 3.9 *Let*

$$\sigma_q Y = AY \tag{3}$$

be an equation of M with $A \in \mathrm{GL}_n(K)$. There exists a fundamental matrix of solutions U of (3) with coefficients in the field $\mathcal{M}(\mathbb{C}^*)$ of functions meromorphic on $\mathbb{C}^*$. Moreover, if V is another fundamental matrix of solutions of (3), there exists $P \in \mathrm{GL}_n(C_K)$ such that $U = PV$.

Let L be the subfield of $\mathcal{M}(\mathbb{C}^*)$ generated over K by the entries of U. For any object N of $\{\{M_K\}\}$ let

$$\omega_{M_K}(N) = \mathrm{Ker}(\sigma - Id, L \otimes N).$$

Then $\omega_{M_K} : \{\{M_K\}\} \to Vect_{C_K}$ is a faithful exact, C_K-linear tensor functor.

Proof. For the existence of U see [21] Theorem 3. Since the field of constants of L is C_K, L is a *weak Picard Vessiot* field for M_K, and the proof that ω_{M_K} is a fiber functor on $\{\{M_K\}\}$ is the same as that of Proposition 3.6. □

We now turn to the

Proof of Theorem 3.1. By Propositions 3.6 on the one hand and 3.9 on the other hand, there exists two fiber functors $\tilde{\omega}_M$ and ω_{M_K} on $\{\{M_K\}\}$ which is a neutral tannakian category over C_E. A fundamental theorem of Deligne ([7], Theorem 3.2) asserts that for any field C of caracteristic zero, two fiber functors of a neutral tannakian category over C become isomorphic over the algebraic closure of C. Taking $C = C_K$ and combining this with Proposition 3.8, we therefore have

$$Aut^{\otimes}(\omega_M) \otimes \overline{C_K} \simeq Aut^{\otimes}(\omega_{M_K}) \otimes \overline{C_K}.$$

□

To show the connection between Theorem 3.1 and Theorem 2.9 we must show that the group of difference k (rep. K)-automorphisms of R (resp. F) can be identified with the $\mathbb{C}$ (resp. C_K)-points of $Aut^{\otimes}(\omega_M)$ (resp. $Aut^{\otimes}(\omega_{M_K})$). In the first case, this has been shown in Theorem 1.32.3 of [23]; the second case can be established in a similar manner. This enables us to deduce, in our special case, Theorem 2.9 from Theorem 3.1.

We conclude with an example to show that these considerations can be used to show the algebraic independence of certain classical functions.

Example 3.10 Consider the q-difference equation

$$\sigma_q(y) = y + 1. \tag{4}$$

In ([23], Section 12.1) the authors denote by l the formal solution of 4, i.e. the formal q-logarithm. It is easily seen that the Galois group, in the

sense of [23], of (4) is equal to $(\mathbb{C}, +)$ and therefore that the dimension of the Galois group $G_{R/\mathbb{C}}$ is equal to 1. We deduce from Theorem 2.9 that the dimension of the Galois group G_{S/C_K} is also equal to 1. In particular, the field generated over K by the meromorphic solutions of (4) has transcendence degree 1 over K.

The classical Weiestrass ζ function associated to the elliptic curve $E = \mathbb{C}^*/q^{\mathbb{Z}}$ satisfies the equation (4). Therefore, if $\wp$ is the Weierstrass function of E, we obtain that $\zeta(z)$ is transcendental over the field $\mathbb{C}(z, \wp(z))$.

4 A Model-Theoretic Point of View

4.1 Preliminary model-theoretic definitions and results

Definition 4.1 Let K be a difference field with automorphism σ.

1. K is *generic* iff
   $(*)$ every **finite** system of difference equations with coefficients in K and which has a solution in a difference field containing K, already has a solution in K.
2. A *finite σ-stable extension* M of K is a finite separably algebraic extension of K such that $\sigma(M) = M$.
3. The *core of L over K*, denoted by $\mathrm{Core}(L/K)$, is the union of all finite σ-stable extensions of K which are contained in L.

One of the difficulties with difference fields, is that there are usually several non-isomorphic ways of extending the automorphism to the algebraic closure of the field. An important result of Babbitt (see [5]) says that once we know the behaviour of σ on $\mathrm{Core}(\overline{K}/K)$, then we know how σ behaves on the algebraic closure $\overline{K}$ of K.

Fix an infinite cardinal κ which is larger than all the cardinals of structures considered (e.g., in our case, we may take $\kappa = |\mathbb{C}|^+ = (2^{\aleph_0})^+$). In what follows we will work in a generic difference field $\mathcal{U}$, which we will assume *sufficiently saturated*, i.e., which has the following properties:

(i) $(*)$ *above holds for every system of difference equations* **of size** $< \kappa$ *(in infinitely many variables).*

(ii) *(1.5 in [4]) If f is an isomorphism between two algebraically closed difference subfields of $\mathcal{U}$ which are of cardinality $< \kappa$, then f extends to an automorphism of $\mathcal{U}$.*

(iii) *Let $K \subset L$ be difference fields of cardinality $< \kappa$, and assume that $K \subset \mathcal{U}$. If every finite σ-stable extension of K which is contained in L K-embeds in $\mathcal{U}$, then there is a K-embedding of L in $\mathcal{U}$.*

Note that the hypotheses of (iii) are always verified if K is an algebraically closed subfield of $\mathcal{U}$. If K is a difference field containing the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, then K will embed into $\mathcal{U}$, if and only if the difference subfield $\overline{\mathbb{Q}}$ of K and the difference subfield $\overline{\mathbb{Q}}$ of $\mathcal{U}$ are isomorphic. This might not always be the case. However, every difference field embeds into some sufficiently saturated generic difference field.

Let us also recall the following result (1.12 in [4]): Let n be a positive integer, and consider the field $\mathcal{U}$ with the automorphism σ^n. Then $(\mathcal{U}, \sigma^n)$ is a generic difference field, and satisfies the saturation properties required of $(\mathcal{U}, \sigma)$.

Notation. We use the following notation. Let R be a difference ring. Then, as in the previous sections, C_R denotes the field of "constants" of R, i.e., $C_R = \{a \in R \mid \sigma(a) = a\}$. We let $D_R = \{a \in R \mid \sigma^m(a) = a \text{ for some } m \neq 0\}$. Then D_R is a difference subring of R, and if R is a field, D_R is the relative algebraic closure of C_R in R. We let D'_R denote the difference ring with same underlying ring as D_R and on which σ acts trivially. Thus $C_{\mathcal{U}}$ is a pseudo-finite field (see 1.2 in [4]), and $D_{\mathcal{U}}$ is its algebraic closure (with the action of σ), $D'_{\mathcal{U}}$ the algebraic closure of $C_{\mathcal{U}}$ on which σ acts trivially.

Later we will work with powers of σ, and will write $Fix(\sigma^n)(R)$ for $\{a \in R \mid \sigma^n(a) = a\}$ so that no confusion arises. If $R = \mathcal{U}$, we will simply write $Fix(\sigma^n)$. Here are some additional properties of $\mathcal{U}$ that we will use.

Let $K \subset M$ be difference subfields of $\mathcal{U}$, with M algebraically closed, and let a be a tuple of $\mathcal{U}$. By 1.7 in [4]:

(iv) *If the orbit of a under $\mathrm{Aut}(\mathcal{U}/K)$ is finite, then $a \in \overline{K}$ (the algebraic closure of K).*

We already know that every element of $\mathrm{Aut}(M/KC_M)$ extends to an automorphism of $\mathcal{U}$. More is true: using 1.4, 1.11 and Lemma 1 in the appendix of [4]:

(v) *every element of* $\mathrm{Aut}(M/KC_M)$ *can be extended to an element of* $\mathrm{Aut}(\mathcal{U}/KC_{\mathcal{U}})$.

Recall that a definable subset S of $\mathcal{U}^n$ is *stably embedded* if whenever $R \subset \mathcal{U}^{nm}$ is definable with parameters from $\mathcal{U}$, then $R \cap S^m$ is definable using parameters from S. An important result ([4] 1.11)) shows that $C_{\mathcal{U}}$ is stably embedded. Let $d \geq 1$. Then, adding parameters from $Fix(\sigma^d)$, there is a definable isomorphism between $Fix(\sigma^d)$ and $C_{\mathcal{U}}^d$. Hence,

(vi) *for every* $d > 0$, $Fix(\sigma^d)$ *is stably embedded, and*
(vii) *if* θ *defines an automorphism of* $D_{\mathcal{U}}$ *which is the identity on* D_M, *then* θ *extends to an automorphism of* $\mathcal{U}$ *which is the identity on* M.

We also need the following lemma. The proof is rather model-theoretic and we refer to the Appendix of [4] for the definitions and results. Recall that if K is a difference subfield of $\mathcal{U}$, then its definable closure, $\mathrm{dcl}(K)$, is the subfield of $\mathcal{U}$ fixed by $\mathrm{Aut}(\mathcal{U}/K)$. It is an algebraic extension of K, and is the subfield of the algebraic closure $\overline{K}$ of K which is fixed by the subgroup $\{\tau \in \mathcal{G}al(\overline{K}/K) \mid \sigma^{-1}\tau\sigma = \tau\}$.

Lemma 4.2 *Let* K *be a difference field, and* M *be a finite* σ*-stable extension of* $KC_{\mathcal{U}}$. *Then* $M \subset \overline{K}D_{\mathcal{U}}$, *i.e., there is some finite* σ*-stable extension* M_0 *of* K *such that* $M \subset M_0 D_{\mathcal{U}}$.

Proof. Fix an integer $d \geq 1$. Then, in the difference field $(\mathcal{U}, \sigma^d)$, $Fix(\sigma^d)$ is stably embedded, $\mathrm{dcl}(\overline{K}) = \overline{K}$ and $\mathrm{dcl}(Fix(\sigma^d)) = Fix(\sigma^d)$. Denoting types in $(\mathcal{U}, \sigma^d)$ by tp_d, this implies

$$(\sharp) \qquad tp_d(\overline{K}/\overline{K} \cap Fix(\sigma^d)) \vdash tp_d(\overline{K}/Fix(\sigma^d)).$$

Assume by way of contradiction that $KC_{\mathcal{U}}$ has a finite σ-stable extension M which is not contained in $\overline{K}D_{\mathcal{U}}$. We may assume that M is Galois over $\overline{K}C_{\mathcal{U}}$ (see Thm 7.16.V in [5]), with Galois group G. Choose d large enough so that σ^d commutes with all elements of G, and

$M = M_0 D_{\mathcal{U}}$, where M_0 is Galois over $\overline{K}Fix(\sigma^d)$. Then there are several non-isomorphic ways of extending σ^d to M. As $tp_d(\overline{K}/Fix(\sigma^d))$ describes in particular the $\overline{K}Fix(\sigma^d)$-isomorphism type of the σ^d-difference field M, this contradicts ($\sharp$) (see Lemmas 2.6 and 2.9 in [4]). □

4.2 The Galois group

From now on, we assume that all fields are of characteristic 0. Most of the statements below can be easily adapted to the positive characteristic case. Let K be a difference subfield of $\mathcal{U}$, $A \in \mathrm{GL}_n(K)$, and consider the set $\mathcal{S} = \mathcal{S}(\mathcal{U})$ of solutions of the equation

$$\sigma(X) = AX,\ \det(X) \neq 0.$$

Consider $H = \mathrm{Aut}(K(\mathcal{S})/KC_{\mathcal{U}})$. We will call H the *Galois group of* $\sigma(X) = AX$ *over* $KC_{\mathcal{U}}$[6].

Then H is the set of $C_{\mathcal{U}}$-points of some algebraic group $\mathbb{H}$ defined over $KC_{\mathcal{U}}$. To see this, we consider the ring $R = K[Y, \det(Y)^{-1}]$ (where $Y = (Y_{i,j})$ is an $n \times n$ matrix of indeterminates), extend σ to R by setting $\sigma(Y) = AY$, and let L be the field of fractions of R. Then L is a regular extension of K, and there is a K-embedding φ of L in $\mathcal{U}$, which sends C_L to a subfield of $C_{\mathcal{U}}$, and D_L to a subfield of $D_{\mathcal{U}}$. We let $T = \varphi(Y)$. Then every element $g \in H$ is completely determined by the matrix $M_g = T^{-1}g(T) \in \mathrm{GL}_n(C_{\mathcal{U}})$, since if $B \in \mathcal{S}$, then $B^{-1}T \in \mathrm{GL}_n(C_{\mathcal{U}})$. Moreover, since $KC_{\varphi(L)}(T)$ and $KC_{\mathcal{U}}$ are linearly disjoint over $KC_{\varphi(L)}$, the algebraic locus W of T over $KC_{\mathcal{U}}$ (an algebraic subset of GL_n) is defined over $KC_{\varphi(L)}$, and H is the set of elements of $\mathrm{GL}_n(C_{\mathcal{U}})$ which leave W invariant. It is therefore the set of $C_{\mathcal{U}}$-points of an algebraic group $\mathbb{H}$, defined over $KC_{\varphi(L)}$. We let $\mathbb{H}'$ denote the Zariski closure of $\mathbb{H}(C_{\mathcal{U}})$. Then $\mathbb{H}'$ is defined over $C_{\mathcal{U}}$, and it is also clearly defined over $\overline{K\varphi(C_L)}$, so that it is defined over $C_{\mathcal{U}} \cap \overline{K\varphi(C_L)} = C_{\mathcal{U}} \cap \overline{\varphi(C_L)}$.

Proposition 4.3 *Let $\mathbb{H}^0$ denote the connected component of $\mathbb{H}$, and let M_0 be the relative algebraic closure of $K\varphi(C_L)$ in $\varphi(L)$, M its Galois closure over $K\varphi(C_L)$.*

1. $\dim(\mathbb{H}) = \mathrm{tr.deg}(L/KC_L)$.

6 Warning: This is not the usual Galois group defined by model theorists, please see the discussion in subsection 4.4.

2. *M_0 is a finite σ-stable extension of $K\varphi(C_L)$ and $[\mathbb{H} : \mathbb{H}^0]$ divides $[M : K\varphi(C_L)]$*
3. *$[\mathbb{H}' : \mathbb{H}^0] = [\mathbb{H}(C_\mathcal{U}) : \mathbb{H}^0(C_\mathcal{U})]$ equals the number of left cosets of $\mathcal{G}al(M/M_0)$ in $\mathcal{G}al(M/K\varphi(C_L))$ which are invariant under the action of σ by conjugation.*
4. *If the algebraic closure of C_K is contained in $C_\mathcal{U}$, then the element $\sigma \in \mathcal{G}al(D_L/C_L)$ lifts to an element of $\mathrm{Aut}(KC_\mathcal{U}(T)/KC_\mathcal{U})$.*

Proof. 1. Choose another K-embedding φ' of L into $\mathcal{U}$ which extends φ on the relative algebraic closure of KC_L in L, and is such that $\varphi'(L)$ and $\varphi(L)$ are linearly disjoint over M_0. Then $B = \varphi'(Y)^{-1}T \in \mathbb{H}(C_\mathcal{U})$, and $\mathrm{tr.deg}(\varphi(KC_L)(B))/\varphi(KC_L)) = \mathrm{tr.deg}(L/KC_L)$. Thus $\dim(\mathbb{H}) = \mathrm{tr.deg}(L/KC_L)$.

2. As $M_0 \subset K\varphi(L)$, we obtain that $[M_0 : K\varphi(C_L)]$ is finite and $\sigma(M_0) = M_0$. Furthermore, $\sigma(M) = M$ (see Thm 7.16.V in [5]). The algebraic group $\mathbb{H}$ is defined as the set of matrices of GL_n which leaves the algebraic set W (the algebraic locus of T over $K\varphi(C_L)$) invariant.

Hence $\mathbb{H}^0$ is the subgroup of $\mathbb{H}$ which leaves all absolutely irreducible components of W invariant. Its index in $\mathbb{H}$ therefore must divide $[M : K\varphi(C_L)]$.

3. The first equality follows from the fact that $\mathbb{H}^0(C_\mathcal{U})$ and $\mathbb{H}'(C_\mathcal{U})$ are Zariski dense in $\mathbb{H}^0$ and $\mathbb{H}'$ respectively. Some of the (absolutely irreducible) components of W intersect $\mathcal{S}$ in the empty set. Indeed, let W_0 be the component of W containing T, let W_1 be another component of W and $\tau \in \mathcal{G}al(M/K\varphi(C_L))$ such that $W_1 = W_0^\tau$. Then W_1 is defined over $\tau(M_0)$. If τ defines a (difference-field) isomorphism between M_0 and $\tau(M_0)$, then τ extends to an isomorphism between $K\varphi(L)$ and a regular extension of $K\varphi(C_L)\tau(M_0)$, and therefore $W_1 \cap \mathcal{S} \neq \emptyset$. Conversely, if $B \in W_1 \cap \mathcal{S}$, then $B^{-1}T \in \mathbb{H}(C_\mathcal{U})$, so that B is a generic of W_1. The difference fields $K\varphi(C_L)(B)$ and $K\varphi(L)$ are therefore isomorphic (over $K\varphi(C_L)$), and $\tau(M_0) \subset K\varphi(C_L)(B)$. Hence the difference subfields M_0 and $\tau(M_0)$ of M are $K\varphi(C_L)$-isomorphic. One verifies that M_0 and $\tau(M_0)$ are isomorphic over $K\varphi(C_L)$ if and only if $\sigma^{-1}\tau^{-1}\sigma\tau \in \mathcal{G}al(M/M_0)$, if and only if the coset $\tau\mathcal{G}al(M/M_0)$ is invariant under the action of σ by conjugation.

4. We know that the algebraic closure $\overline{K}$ of K and $D_\mathcal{U}$ are linearly disjoint over $C_{\overline{K}} = \overline{C_K}$. Let $a \in \varphi(D_L)$ generates $\varphi(D_L)$ over $\varphi(C_L)$.

By 4.1(vi), $tp(a/\overline{K}C_{\mathcal{U}}) = tp(\sigma(a)/\overline{K}C_{\mathcal{U}})$, and therefore there is θ in $\mathrm{Aut}(\mathcal{U}/\overline{K}C_{\mathcal{U}})$ such that $\theta(a) = \sigma(a)$. Thus $T^{-1}\theta(T) \in H$. □

Remarks 4.4 1. Even when the algebraic closure of C_K is contained in $C_{\mathcal{U}}$, we still cannot in general conclude that $\mathbb{H}' = \mathbb{H}$.

2. The isomorphism type of the algebraic group $\mathbb{H}$ only depends on the isomorphism type of the difference field K (and on the matrix A). The isomorphism type of the algebraic group $\mathbb{H}'$ does however depend on the embedding of K in $\mathcal{U}$, that is, on the isomorphism type of the difference field $\mathrm{Core}(\overline{K}/K)$. Indeed, while we know the isomorphism type of the difference field M_0 over $K\varphi(C_L)$, we do not know the isomorphism type of the difference field M over $K\varphi(C_L)$, and in view of 4.3.3, if $\mathcal{G}al(M/K\varphi(C_L))$ is not abelian, it may happen that non-isomorphic extensions of σ to M yield different Galois groups.

3. Assume that σ acts trivially on $\mathcal{G}al(\mathrm{Core}(\overline{K}/K)/K)$, and that $\mathcal{G}al(\mathrm{Core}(\overline{K}/K)/K)$ is abelian. Then

$$\mathbb{H} = \mathbb{H}' \quad \text{and} \quad [\mathbb{H} : \mathbb{H}^0] = [M_0 : K\varphi(C_L)].$$

Indeed, by Lemma 4.2, M_0 is Galois over $K\varphi(C_L)$ with abelian Galois group G and σ acts trivially on G. The result follows by 4.3.3. Thus we obtain equality of $\mathbb{H}$ and $\mathbb{H}'$ in two important classical cases:

   a. $K = \mathbb{C}(t)$, $C_K = \mathbb{C}$ and $\sigma(t) = t + 1$.
   b. $K = \mathbb{C}(t)$, $C_K = \mathbb{C}$ and $\sigma(t) = qt$ for some $0 \neq q \in \mathbb{C}$, q not a root of unity.

4. If $B \in \mathcal{S}$, then the above construction can be repeated, using B instead of T. We then obtain an algebraic group $\mathbb{H}_1$, with $\mathbb{H}_1(C_{\mathcal{U}}) \simeq \mathrm{Aut}(KC_{\mathcal{U}}(\mathcal{S})/KC_{\mathcal{U}})$. Since $KC_{\mathcal{U}}(B) = KC_{\mathcal{U}}(T)$, the algebraic groups $\mathbb{H}_1$ and $\mathbb{H}$ are isomorphic (via $B^{-1}T$).

5. In the next subsection, we will show that the algebraic group $\mathbb{H}$ and the algebraic group $G_{R'}$ introduced in section 2 are isomorphic when $C_{R'} = C_K = D_K$.

4.3 More on Picard-Vessiot rings

Throughout the rest of this section, we fix a difference ring K, some $A \in \mathrm{GL}_n(K)$, $R = K[Y, \det(Y)^{-1}]$ as above, with $\sigma(Y) = AY$, and $R' = R/q$ a Picard-Vessiot ring for $\sigma(X) = AX$ over K. We denote the image of Y in R' by y. We keep the notation introduced in the previous subsections.

If q is not a prime ideal, then there exists ℓ and a prime σ^ℓ-ideal p of R which is a maximal σ^ℓ-ideal of R, such that $q = \bigcap_{i=0}^{\ell-1} \sigma^i(p)$, and $R' \simeq \oplus_{i=0}^{\ell-1} R_i$, where $R_i = R/\sigma^i(p)$ (see Corollary 1.16 of [23]. One verifies that the second proof does not use the fact that C_K is algebraically closed). Thus the σ^ℓ-difference ring R_0 is a Picard-Vessiot ring for the difference equation $\sigma^\ell(X) = \sigma^{\ell-1}(A) \cdots \sigma(A)AX$ over K. We denote $\sigma^{\ell-1}(A) \cdots \sigma(A)A$ by A_ℓ.

We will identify R' with $\oplus_{i=0}^{\ell-1} R_i$, and denote by e_i the primitive idempotent of R' such that $e_i R' = R_i$. Then $e_i = \sigma^i(e_0)$. We will denote by R^* the ring of quotients of R', i.e., $R^* = \oplus_{i=0}^{\ell-1} R_i^*$, where R_i^* is the field of fractions of R_i. The difference ring R^* is also called the *total Picard-Vessiot ring of* $\sigma(X) = AX$ *over* K. There are two numerical invariants associated to R': the number $\ell = \ell(R')$, and the number $m(R')$ which is the product of $\ell(R')$ with $[D_{R_0^*} : D_K C_{R_0^*}]$. We call $m(R')$ the *m-invariant of* R'. We will be considering other Picard-Vessiot rings for $\sigma(X) = AX$, and will use this notation for them as well.

Recall that the *Krull dimension* of a ring S is the maximal integer n (if it exists) such that there is a (strict) chain of prime ideals of S of length n. We denote it by $\mathrm{Kr.dim}(S)$. If S is a domain, and is finitely generated over some subfield k, then $\mathrm{Kr.dim}(S)$ equals the transcendence degree over k of its field of fractions. Observe that if S is a domain of finite Krull dimension, and $0 \neq I$ is an ideal of S, then $\mathrm{Kr.dim}(S) > \mathrm{Kr.dim}(S/I)$. Also, if $S = \oplus_i S_i$, then $\mathrm{Kr.dim}(S) = \sup\{\mathrm{Kr.dim}(S_i)\}$.

Lemma 4.5 *1. $C_{R'}$ is a finite algebraic extension of C_K, and is linearly disjoint from K over C_K (inside R').*

2. If $C_{R'} \otimes_{C_K} D_K$ is a domain, then R' is a Picard-Vessiot ring for $\sigma(X) = AX$ over $KC_{R'}$.

Proof. 1. We know by Lemma 1.7 of [23] that $C_{R'}$ is a field. Assume by way of contradiction that $C_{R'}$ and K are not linearly disjoint over

C_K, and choose n minimal such that there are $a_1, \ldots, a_n \in C_{R'}$ which are C_K-linearly independent, but not K-linearly independent. Let $0 \neq c_1, \ldots, c_n \in K$ be such that $\sum_{i=1}^n a_i c_i = 0$. Multiplying by c_1^{-1}, we may assume $c_1 = 1$. Then $\sigma(\sum_{i=1}^n a_i c_i) = \sum_{i=1}^n a_i \sigma(c_i) = 0$, and therefore $\sum_{i=2}^n a_i(\sigma(c_i) - c_i) = 0$. By minimality of n, all $(\sigma(c_i) - c_i)$ are 0, i.e., all $c_i \in C_K$, which gives us a contradiction.

Observe that $e_0 C_{R'} \subset Fix(\sigma^\ell)(R_0)$, and we may therefore replace R' by the domain R_0. Since R_0 is a finitely generated K-algebra, we know that its Krull dimension equals the transcendence degree over K of its field of fractions. Thus R_0 cannot contain a subfield which is transcendental over K, i.e., the elements of $Fix(\sigma^\ell)(R_0)$ are algebraic over K. his furthermore implies that $Fix(\sigma^\ell)(R_0)$ is an algebraic extension of $Fix(\sigma^\ell)(K)$. Since the latter field is an algebraic extension of C_K, we have the conclusion.

2. Our hypothesis implies that $K[C_{R'}]$ is a field. Hence R' is a simple difference ring containing $KC_{R'}$, and is therefore a Picard-Vessiot ring for $\sigma(X) = AX$ over $KC_{R'}$. □

Lemma 4.6 *1.* $C_{R'} = C_{R^*}$.

2. $Fix(\sigma^\ell)(e_0 R^*) = e_0 C_{R'}$.

3. $D_{R^*} = \oplus_{i=0}^{\ell-1} D_{e_i R^*}$.

Proof. 1. If $c \in C_{R^*}$, then c can be represented by some ℓ-tuple $(\frac{a_0}{b_0}, \ldots, \frac{a_{\ell-1}}{b_{\ell-1}})$, where $a_i, b_i \in R_i$, and $b_i \neq 0$. Thus the ideal $I = \{d \in R' \mid dc \in R'\}$ is a σ-ideal of R' and contains the element $b = (b_0, \ldots, b_{\ell-1}) \neq 0$. Since R' is simple, $1 \in I$, i.e., $c \in R'$.

2. Assume $a \in e_0 R^*$ satisfies $\sigma^\ell(a) = a$. Then $a = e_0 a$, $\sum_{i=0}^{\ell-1} \sigma^i(e_0 a)$ is fixed by σ, and therefore belongs to $C_{R'}$. Hence $a \in e_0 C_{R'}$.

3. If $a \in R^*$ satisfies $\sigma^m(a) = a$ for some m, then $\sigma^{m\ell}(e_i a) = e_i a$. □

Remark 4.7 Observe that ℓ and the isomorphism type of the K-σ^ℓ-difference algebra R_0 completely determine the isomorphism type of the difference algebra R'. Indeed, for each $i = 1, \ldots, \ell - 1$, one chooses a copy R_i of the domain R_0, together with an isomorphism $f_i : R_0 \to R_i$ which extends σ^i on K. This f_i then induces an automorphism σ^ℓ of R_i. One then defines σ on $\oplus_{i=0}^{\ell-1} R_i$ by setting $\sigma(a_0, \ldots, a_{\ell-1}) = (f_1(a_0), f_2 f_1^{-1}(a_1), \ldots, \sigma^\ell f_{\ell-1}^{-1}(a_{\ell-1}))$.

Proposition 4.8 *Let $K \subset K_1$ be difference fields of characteristic 0 where $K_1 = K(C_{K_1})$, and assume that $C_K = D_K$. Then $R' \otimes_K K_1 = \oplus_{i=1}^d R'_i$, where each R'_i is a Picard-Vessiot ring for $\sigma(X) = AX$ over K_1, and $d \leq [C_{R'} : C_K]$. Moreover, each R'_i has the same Krull-dimension and m-invariant as R'.*

Proof. Our assumption implies that $K \otimes_{C_K} C_{K_1}$ is a domain. Let C be the relative algebraic closure of C_K in C_{K_1}. Then $K(C) = K[C]$, and $R' \otimes_K K(C) \simeq R' \otimes_{C_K} C$.

Let $a \in C_{R'}$ be such that $C_{R'} = C_K(a)$ and let $f(X) \in C_K[X]$ be its minimal polynomial over C_K. Let $g_1(X), \ldots, g_d(X)$ be the irreducible factors of $f(X)$ over C. Then $f(X) = \prod_{i=1}^d g_i(X)$, and $C'_R \otimes_{C_K} C \simeq \oplus_{i=1}^d C_i$, where C_i is generated over C by a root of $g_i(X) = 0$. Indeed, identifying C with $1 \otimes C$, every prime ideal of $C_{R'} \otimes_{C_K} C$ must contain some $g_i(a \otimes 1)$; on the other hand, each $g_i(a \otimes 1)$ generates a maximal ideal of $C_{R'} \otimes_{C_K} C$. Thus

$$R' \otimes_{C_K} C \simeq R' \otimes_{C_{R'}} (C_{R'} \otimes_{C_K} C) \simeq \oplus_{i=1}^d R' \otimes_{C_{R'}} C_i.$$

By Lemmas 2.3 and 4.5, each $R' \otimes_{C_{R'}} C_i = R'_i$ is a simple difference ring, with field of constants C_i. Hence R'_i is a Picard-Vessiot ring for $\sigma(X) = AX$ over KC (and also over KC_i). Note that $d \leq \deg(f) = [C_{R'} : C_K]$, and that $\mathrm{Kr.dim}(R'_i) = \mathrm{Kr.dim}(R')$ (because KC is algebraic over K, and R'_i is finitely generated over K).

By Proposition 2.4, $R'_i \otimes_{KC_i} K_1C_i$ is a Picard-Vessiot ring. Because C_i and K_1 are linearly disjoint over C, and C_i is algebraic over C, $KC_i \otimes_{KC} K_1 \simeq K_1C_i$, and therefore

$$R'_i \otimes_{KC} K_1 \simeq R'_i \otimes_{KC_i} K_1C_i.$$

This shows that $R' \otimes_K K_1$ is the direct sum of Picard-Vessiot rings over K_1.

Identifying $C_{R'}$ with $e_jC_{R'} = C_{R_j}$, we obtain

$$R'_i = (\oplus_{j=0}^{\ell-1} R_j) \otimes_{C_{R'}} C_i \simeq \oplus_{j=0}^{\ell-1} R_j \otimes_{C_{R'}} C_i.$$

Each R_j being a Picard-Vessiot ring for $\sigma^\ell(X) = A_\ell X$, we know by Proposition 2.4 that $R_j \otimes_{C_{R'}} C_i$ is also a Picard-Vessiot ring for $\sigma^\ell(X) = A_\ell X$. Thus $R_0 \otimes_{C_{R'}} C_i = \sum_{j=0}^{s-1} S_j$, where each S_j is a simple $\sigma^{\ell s}$-difference ring, and a domain. Because all rings R_j are isomorphic over $C_{R'}$, and all S_j are isomorphic over $C_{R'}$, $m(R'_i)$ is the product of ℓs with $m(S_0) = [D_{S_0^*} : C_{S_0^*}]$, where S_0^* is the field of fractions of S_0. To show

that $m(R_i') = m(R')$, it therefore suffices to show that $sm(S_0) = m(R_0)$. By Lemma 4.5.2,

$$Fix(\sigma^{\ell s})(S_0^*) = Fix(\sigma^\ell)(R_0^* \otimes_{C_{R'}} C_i) = Fix(\sigma)(R' \otimes_{C_{R'}} C_i) = C_i.$$

We know that $D_{R_0^*}$ is a (cyclic) Galois extension of $C_{R'} = Fix(\sigma^\ell)(R_0^*)$, and is therefore linearly disjoint from C_i over $D_{R_0^*} \cap C_i = C_i'$. Write $C_i' = C_{R'}(\alpha)$, and let $a, b \in R_0$, $b \neq 0$, be such that (inside R_0^*), $C_{R'}(a/b) = C_i'$. The minimal prime ideals of $R_0 \otimes_{C_{R'}} C_i$ are the ideals $Q_0, \ldots, Q_{r-1}$, where $r = [C_i' : C_{R'}]$ and Q_k is generated by $\sigma^{k\ell}(a) \otimes 1 - \sigma^{k\ell}(b) \otimes \alpha$. This shows that $r = s$, since s is also the number of minimal prime ideals of $R_0 \otimes_{C_{R'}} C_i$.
Let e be a primitive idempotent of $R_0 \otimes_{C_{R'}} C_i$ such that $S_0 = e(R_0 \otimes_{C_{R'}} C_i)$. Then $eC_iD_{R_0^*}$ is a subfield of S_0^*, contained in $D_{S_0^*}$, and its degree over $eC_i = Fix(\sigma^{\ell s})(S_0^*)$ is the quotient of $[D_{R_0^*} : C_{R'}]$ by $[C_i' : C_{R'}]$, i.e., equals $m(R_0)/s$. To finish the proof, it therefore suffices to show that $D_{S_0^*} = eC_iD_{R_0}^*$.

Assume that $c \in R_0^* \otimes_{C_{R'}} C_i$ satisfies $\sigma^m(c) = c$ for some $m \neq 0$. Write $c = \sum_k a_k \otimes c_k$, where the a_k are in R_0^*, and the c_k are in C_i and are linearly independent over $C_{R'}$. Then $\sigma^m(c) = c = \sum_k \sigma^m(a_k)c_k$, which implies $\sigma^m(a_k) = a_k$ for all k, and all a_k's are in $D_{R_0^*}$. As every element of $D_{S_0^*}$ is of the form ec for such a c (Lemma 4.6.3), this shows that $D_{S_0^*} = eC_iD_{R_0}^*$. This finishes the proof that $m(R_i') = m(R')$.

Consider now $R' \otimes_{KC} K_1$. It is the direct sum of ℓs $\sigma^{\ell s}$-difference rings, each one being isomorphic to $S_0 \otimes_{KC} K_1$. Because K_1 is a regular extension of KC, $S_0 \otimes_{KC} K_1$ is a domain, of Krull dimension equal to $\mathrm{Kr.dim}(S_0) = \mathrm{Kr.dim}(R')$. Inside its field of fractions (a $\sigma^{\ell s}$-difference field) K_1 and S_0^* are linearly disjoint over KC, which implies that $C_{K_1}C_i$ is the field of constants of $S_0 \otimes_{KC} K_1$, $C_{K_1}D_{S_0^*}$ is the field of elements fixed by some power of σ, and $[C_{K_1}D_{S_0^*} : C_{K_1}C_i] = [D_{S_0}^* : C_i] = m(S_0)$. This shows that $m(R_i' \otimes_{KC} K_1) = m(R')$ and finishes the proof. □

Proposition 4.9 *Assume that $C_K = D_K$. Then all Picard-Vessiot rings for $\sigma(X) = AX$ over K have the same Krull dimension and the same m-invariant.*

Proof. Let C be the algebraic closure of C_K, and let R'' be a Picard-Vessiot ring for $\sigma(X) = AX$ over K. By Proposition 4.8, $R' \otimes_K KC$ is the direct sum of finitely many Picard-Vessiot rings for $\sigma(X) = AX$ over KC, and each of these rings has the same Krull dimension and

m-invariant as R'. The same statement holds for R''. On the other hand, by Proposition 1.9 of [23], all Picard-Vessiot rings over KC are isomorphic. □

Corollary 4.10 *Assume $D_K = C_K$. Let $R'' = K[V, \det(V)^{-1}]$, where $\sigma(V) = AV$, and assume that* $\mathrm{Kr.dim}(R'') = \mathrm{Kr.dim}(R')$ *and that R'' has no nilpotent elements. Then R'' is a finite direct sum of Picard-Vessiot rings for $\sigma(X) = AX$.*

Proof. Because R'' has no nilpotent elements and is Noetherian, (0) is the intersection of the finitely many prime minimal ideals of R''. Let $\mathcal{P}$ be the set of minimal prime ideals of R''. Then the intersection of any proper subset of $\mathcal{P}$ is not (0), i.e., no element of $\mathcal{P}$ contains the intersection of the other elements of $\mathcal{P}$. Also, if $P \in \mathcal{P}$, then $\sigma(P) \in \mathcal{P}$, and there exists $m > 0$ such that $\sigma^m(P) = P$. Then $I_P = \bigcap_{i=0}^{m-1} \sigma^i(P)$ is a σ-ideal, which is proper if the orbit of P under σ is not all of $\mathcal{P}$. Observe that for each $P \in \mathcal{P}$, $\mathrm{Kr.dim}(R''/P) \leq \mathrm{Kr.dim}(R''/I_P) \leq \mathrm{Kr.dim}(R'') = \mathrm{Kr.dim}(R')$, and that for some P we have equality.

If I is a maximal σ-ideal of R'', then $\mathrm{Kr.dim}(R''/I) = \mathrm{Kr.dim}(R') = \mathrm{Kr.dim}(R'')$ by Proposition 4.8, and this implies that I is contained in some $P \in \mathcal{P}$. Hence $I = I_P$ and R''/I_P is a Picard-Vessiot ring. If $I = (0)$, then we are finished. Otherwise, $\mathcal{P}$ contains some element P_1 not in the orbit of P under σ. Observe that I_{P_1} is contained in some maximal σ-ideal of R'', and is therefore maximal, by the same reasoning. Since the intersection of any proper subset of $\mathcal{P}$ is non-trivial, $I_P + I_{P_1}$ is a σ-ideal of R'' which contains properly I_P, and therefore equals 1. If $P_1, \ldots, P_r$ are representatives from the σ-orbits in $\mathcal{P}$, the Chinese Remainder Theorem then yields $R'' \simeq \oplus_{i=1}^{r} R''/I_{P_i}$. □

Proposition 4.11 *Assume $C_K = D_K$. Then $KC_L[R]$ is a Picard-Vessiot ring for $\sigma(X) = AX$ over KC_L,*

$$\mathrm{Kr.dim}(R') = \mathrm{tr.deg}(L/KC_L), \quad \textit{and } [D_L : C_L] = m(R').$$

Proof. Let us first assume that R' is a domain. There is some generic difference field $\mathcal{U}$ containing R' and its field of fractions R^*, and which is sufficiently saturated. Because L is a regular extension of K, there is some K-embedding φ of L into $\mathcal{U}$, and we will denote by T the image of Y in $\mathcal{U}$, and by y the image of Y in R'. Then $\varphi(C_L) \subset C_{\mathcal{U}}$, and there

is some $B \in \mathrm{GL}_n(C_{\mathcal{U}})$ such that $T = yB$. Hence

$$KC_{\mathcal{U}}[T, \det(T)^{-1}] = KC_{\mathcal{U}}[y, \det(y)^{-1}].$$

By Proposition 4.8, $R' \otimes_K KC_{\mathcal{U}}$ is a direct sum of Picard-Vessiot rings of $\sigma(X) = AX$ over $KC_{\mathcal{U}}$, and clearly one of those is the domain $KC_{\mathcal{U}}[y, \det(y)^{-1}]$. Thus

$$\begin{gathered}\mathrm{Kr.dim}(R') = \mathrm{tr.deg}(R^*/K) = \mathrm{tr.deg}(L/KC_L),\\ D_{R^*}C_{\mathcal{U}} = \varphi(D_L)C_{\mathcal{U}}, \text{ and } m(R') = [D_L : C_L].\end{gathered}$$

This implies also that $K\varphi(C_L)[T, \det(T)^{-1}]$ is a simple difference ring, and therefore a Picard-Vessiot ring for $\sigma(X) = AX$ over $K\varphi(C_L)$. Hence $KC_L[R]$ is a Picard-Vessiot extension for $\sigma(X) = AX$ over KC_L.

In the general case, we replace R' by R_0, σ by σ^ℓ, find some generic sufficiently saturated σ^ℓ-difference field $\mathcal{U}$ containing R_0, and a K-embedding φ of the σ^ℓ-difference domain L into $\mathcal{U}$, and conclude as above that $KFix(\sigma^\ell)[R_0] = KFix(\sigma^\ell)[\varphi(R)]$, that the Krull dimension of R' equals $\mathrm{tr.deg}(L/KC_L)$, and that $m(R_0) = [Fix(\sigma^\ell)(\varphi(D_L)) : Fix(\sigma^\ell)]$.

Because K and D_L are linearly disjoint over C_K, $[KD_L : KC_L] = [D_L : C_L]$, whence $D_{KC_L} = KC_L$, and by Corollary 4.10, the difference domain $KC_L[R]$ is a simple difference ring, i.e., a Picard-Vessiot ring for $\sigma(X) = AX$ over KC_L. By Proposition 4.8 $m(R') = [D_L : C_L]$.

We have $m(R') = \ell m(R_0)$, and $m(R_0)$ is the quotient of $[D_L : C_L]$ by the greatest common divisor of $[D_L : C_L]$ and ℓ. □

Corollary 4.12 *Assume that $C_K = D_K$. Let $R'' = K[V, \det(V)^{-1}]$ be a difference domain, where $\sigma(V) = AV$, with field of fractions L_1, and assume that C_{L_1} is a finite algebraic extension of C_K. Then R'' is a Picard-Vessiot ring for $\sigma(X) = AX$ over K.*

Proof. Let $\mathcal{U}$ be a sufficiently saturated generic difference field containing R'', and let φ be a K-embedding of L into $\mathcal{U}$. Then $KC_{\mathcal{U}}[\varphi(R)] = KC_{\mathcal{U}}[R'']$. Hence $\mathrm{Kr.dim}(R'') = \mathrm{Kr.dim}(R')$ and R'' is a Picard-Vessiot ring by Corollary 4.10. □

Corollary 4.13 *Assume that C_K is algebraically closed. Then $\ell(R') = [D_L : C_L]$.*

Proof. Immediate from Proposition 4.11 and the fact that $D_{R^*} = C_{R'} = C_K$. □

Corollary 4.14 *The difference ring $KC_L[R]$ is a Picard-Vessiot ring for $\sigma(X) = AX$ over KC_L. All Picard-Vessiot rings for $\sigma(X) = AX$ over K have the same Krull dimension, which equals* $\mathrm{tr.deg}(L/KC_L)$.

Proof. Let $m = [D_K : C_K]$. Note that replacing σ by some power of σ does not change the fields D_K or D_L, and that $Fix(\sigma^m)(K) = D_K$. Therefore we can apply the previous results to the equation $\sigma^m(X) = A_m X$ over K. By Corollary 4.12 and because $KC_L[R]$ is a domain, $KC_L[R]$ is a Picard-Vessiot ring for $\sigma^m(X) = A_m X$ over KC_L, and therefore a simple σ^m-difference ring, whence a simple σ-difference ring, and finally a Picard-Vessiot ring for $\sigma(X) = AX$ over K.

Let $R' = R/q$ be a Picard-Vessiot ring for $\sigma(X) = AX$ over K. Assume first that R' is a domain, and let $\mathcal{U}$ be a generic difference field containing it. Because L is a regular extension of K, there is a K-embedding φ of L into $\mathcal{U}$, and from $KC_{\mathcal{U}}[\varphi(R)] = KC_{\mathcal{U}}[R']$ and Lemma 4.5.1, we obtain the result. If R' is not a domain, then we reason in the same fashion, replacing R' by R_0 and σ by σ^ℓ, to obtain the result. □

Proposition 4.15 *Assume that $C_{R'} = C_K = D_K$ and $K \subset \mathcal{U}$. Then $G_{R'}$ and $\mathbb{H}$ are isomorphic.*

Proof. By Proposition 2.4, we may replace R' by $R' \otimes_K KD'_{\mathcal{U}}$, and consider the ring $K\varphi(C_L)[T, \det(T)^{-1}] \otimes_{K\varphi(C_L)} KD'_{\mathcal{U}}$, which is a Picard-Vessiot ring by Proposition 4.11 and Corollary 4.10. We identify $1 \otimes KD'_{\mathcal{U}}$ with $KD'_{\mathcal{U}}$. These two rings are isomorphic over $KD'_{\mathcal{U}}$ by Proposition 1.9 of [23], and it therefore suffices to show that

$$\mathrm{Aut}(\varphi(L) \otimes_{K\varphi(C_L)} KD'_{\mathcal{U}}/KD'_{\mathcal{U}}) = \mathbb{H}(D'_{\mathcal{U}}).$$

Inside $\varphi(L) \otimes_{K\varphi(C_L)} KD'_{\mathcal{U}}$, $\varphi(L) \otimes 1$ and $KD'_{\mathcal{U}}$ are linearly disjoint over $K\varphi(C_L)$. Hence, the algebraic loci of $(T, \det(T)^{-1})$ over $K\varphi(C_L)$ and over $KD'_{\mathcal{U}}$ coincide. As $\mathbb{H}$ was described as the subgroup of GL_n which leaves this algebraic set invariant, we get the result. □

4.4 Concluding remarks

4.16 Model-theoretic Galois groups: definition and a bit of history. Model-theoretic Galois groups first appeared in a paper by Zilber [28] in the context of $\aleph_1$-categorical theories, and under the name of

binding groups. Grosso modo, the general situation is as follows: in a saturated model M we have definable sets D and C such that, for some finite tuple b in M, $D \subset \mathrm{dcl}(C, b)$ (one then says that D is C-internal). The group $\mathrm{Aut}(M/C)$ induces a group of (elementary) permutations of D, and it is this group which one calls the *Galois group of D over C*. In Zilber's context, this group and its action on D are definable in M. One issue is therefore to find the correct assumptions so that these Galois groups and their action are definable, or at least, an intersection of definable groups. Hrushovski shows in his PhD thesis ([12]) that this is the case when the ambient theory is stable.

Poizat, in [20], recognized the importance of elimination of imaginaries in establishing the Galois correspondence for these Galois groups. He also noticed that if M is a differentially closed field of characteristic 0 and D is the set of solutions of some linear differential equation over some differential subfield K of M, and C is the field of constants of M, then the model-theoretic Galois group coincides with the differential Galois group introduced by Kolchin [15]. This connection was further explored by Pillay in a series of papers, see [19]. Note that because the theory of differentially closed fields of characteristic 0 eliminates quantifiers, this Galois group does coincide with the group of KC-automorphisms of the differential field $KC(D)$.

Since then, many authors studied or used Galois groups, under various assumptions on the ambient theory, and in various contexts, either purely model-theoretic (e.g., simple theories) or more algebraic (e.g. fields with Hasse derivations). In the context of generic difference fields, (model-theoretic) Galois groups were investigated in (5.11) of [4] (a slight modification in the proof then gives the Galois group described in section 4.1 of this paper). In positive characteristic p, the results generalize easily to twisted difference equations of the form $\sigma(X) = AX^{p^m}$, the field $Fix(\sigma)$ being then replaced by $Fix(\tau)$, where $\tau : x \mapsto \sigma(x)^{p^{-m}}$.

Recent work of Kamensky ([13]) isolates the common ingredients underlying all the definability results on Galois groups, and in particular *very much weakens the assumptions* on the ambient theory (it is not even assumed to be complete). With the correct definition of C-internality of the definable set D, he is able to show that a certain group of permutations of D is definable in M. These are just permutations, do not a priori preserve any relations of the language other than equality. From this group, he is then able to show that subgroups which preserve a (fixed) finite set of relations are also definable, and that the complexity

of the defining formula does not increase, or not too much. For details, see section 3 of [13].

This approach of course applies to the set D of solutions of a linear system of difference equations (over a difference field K), and Kamensky also obtains the result that $\mathrm{Aut}(KFix(\sigma)(D)/KFix(\sigma))$ is definable (see section 5 in [13]).

4.17 A question arises in view of the proof of the general case of Proposition 4.11. When R' is not a domain, we found an embedding of the σ^ℓ-difference ring R_0 into a generic σ^ℓ-difference field $\mathcal{U}$. It may however happen that K is not relatively algebraically closed in R_0^*, even when $D_{R_0} = C_K$. Thus one can wonder: can one always find a generic difference field $\mathcal{U}$ containing K, and such that there is a K-embedding of the σ^ℓ-difference ring R_0 into $(\mathcal{U}, \sigma^\ell)$? Or are there Picard-Vessiot rings for which this is impossible?

4.18 Issues of definability. It is fairly clear that the algebraic group $\mathbb{H}$ is defined over $\varphi(KC_L)$. On the other hand, using the saturation of $\mathcal{U}$ and the fact that L is a regular extension of K, we may choose another K-embedding φ_1 of L in $\mathcal{U}$, and will obtain an algebraic group $\mathbb{H}_1$, which will be isomorphic to $\mathbb{H}$ (via some matrix $C \in \mathrm{GL}_n(C_\mathcal{U})$). It follows that $\mathbb{H}$ is K-isomorphic to an algebraic group $\mathbb{H}_0$ defined over the intersections of all possible $\varphi(KC_L)$, i.e., over K.

Observe that the isomorphism between $\mathbb{H}$ and $\mathbb{H}_1$ yields an isomorphism between $\mathbb{H}(C_\mathcal{U})$ and $\mathbb{H}_1(C_\mathcal{U})$, so that we will also have an isomorphism between $\mathbb{H}_0(C_\mathcal{U})$ and $\mathbb{H}(C_\mathcal{U})$, i.e., $\mathbb{H}'$ is K-isomorphic to an algebraic subgroup of $\mathbb{H}_0$ which is defined over $\overline{C_K} \cap C_\mathcal{U}$. Thus when C_K is algebraically closed, it will be defined over C_K.

The Galois duality works as well for subgroups of $\mathbb{H}(C_\mathcal{U})$ defined by equations (i.e., corresponding to algebraic subgroups of $\mathbb{H}'$, whose irreducible components are defined over $C_\mathcal{U}$). It works less well for arbitrary definable subgroups of $\mathbb{H}(C_\mathcal{U})$. In order for it to work, we need to replace $K(\mathcal{S})$ by its definable closure $\mathrm{dcl}(K\mathcal{S})$, i.e., the subfield of $\mathcal{U}$ which is fixed by all elements of $\mathrm{Aut}_{el}(\mathcal{U}/K\mathcal{S})$. Because the theory of $\mathcal{U}$ eliminates imaginaries (1.10 in [4]), any orbit of an element of $\mathcal{S}$ under the action of a definable subgroup of $\mathbb{H}(C_\mathcal{U})$ has a "code" inside $\mathrm{dcl}(K\mathcal{S})$.

4.19 Problems with the algebraic closure. Assume that $\mathcal{U}$ is a generic difference field containing K, and sufficiently saturated. Then if

K is not relatively algebraically closed in the field of fractions of R_0, we may not be able to find a K-embedding of R_0 into the σ^ℓ-difference field $\mathcal{U}$. Thus in particular, a priori not all Picard-Vessiot domains K-embed into $\mathcal{U}$. This problem of course does not arise if we assume that K is algebraically closed, or, more precisely, if we assume that
All extensions of the automorphism σ to the algebraic closure of K define K-isomorphic difference fields.

This is the case if K has no finite (proper) σ-stable extension, for instance when $K = \mathbb{C}(t)$, with $\sigma(t) = t + 1$ and σ the identity on $\mathbb{C}$.
However, in another classical case, this problem does arise: let $q \in \mathbb{C}$ be non-zero and not a root of unity, and let $K = \mathbb{C}(t)$, where σ is the identity on $\mathbb{C}$ and $\sigma(t) = qt$. Then K has non-trivial finite σ-stable extensions, and they are obtained by adding n-th roots of t.
Let us assume that, inside $\mathcal{U}$, we have $\sigma(\sqrt{t}) = \sqrt{q}\sqrt{t}$. Let us consider the system

$$\sigma(Y) = -\sqrt{q}Y, \quad Y \neq 0$$

over K. Then the Picard-Vessiot ring is $R' = K(y)$, where $y^2 = t$ and $\sigma(y) = -\sqrt{q}y$. Clearly R' does not embed in $\mathcal{U}$. If instead we had considered this system over $K(\sqrt{t})$, then the new Picard-Vessiot ring R'' is not a domain anymore, because it will contain a non-zero solution of $\sigma(X)+X = 0$ (namely, $y/\sqrt{t}$). In both cases however the Galois group is $\mathbb{Z}/2\mathbb{Z}$. And because R' embeds in R'', it also embeds in $K(T)\otimes_{\varphi(C_L)} D'_{\mathcal{U}}$.

This suggests that, when $C_K = D_K$, if one takes $\mathcal{M}$ to be the subfield of $\mathcal{U}$ generated over $KC_{\mathcal{U}}$ by all tuples of $\mathcal{U}$ satisfying some linear difference equation over K, then $\mathcal{M}\otimes_{C_{\mathcal{U}}} D'_{\mathcal{U}}$ is a universal (full) Picard-Vessiot ring of $KD'_{\mathcal{U}}$. This ring is not so difficult to describe in terms of $\mathcal{M}$. Observe that $\mathcal{M}$ contains $D_{\mathcal{U}}$. Thus $\mathcal{M}\otimes_{C_{\mathcal{U}}} D'_{\mathcal{U}}$ is isomorphic to $\mathcal{M}\otimes_{D_{\mathcal{U}}}(D_{\mathcal{U}}\otimes_{C_{\mathcal{U}}} D'_{\mathcal{U}})$. It is a regular ring, with prime spectrum the Cantor space $\mathcal{C}$ (i.e., the prime spectrum of $D_{\mathcal{U}} \otimes_{C_{\mathcal{U}}} D'_{\mathcal{U}}$), and σ acting on $\mathcal{C}$. As a ring, it is isomorphic to the ring of locally constant functions from $\mathcal{C}$ to $\mathcal{M}$.

It would be interesting to relate this ring to the universal Picard-Vessiot rings defined in [23].

4.20 Saturation hypotheses. The saturation hypothesis on $\mathcal{U}$ is not really needed to define the model-theoretic Galois group, since we only need $\mathcal{U}$ to contain a copy of L to define it. We also used it in the proof of Proposition 4.11, when we needed a K-embedding of L into $\mathcal{U}$. Thus, to define the model-theoretic Galois group, we only need $\mathcal{U}$ to be a generic

difference field containing K. Its field of constants will however usually be larger than C_K. Indeed, the field $C_{\mathcal{U}}$ is always a pseudo-finite field (that is, a perfect, pseudo-algebraically closed field, with Galois group isomorphic to $\hat{\mathbb{Z}}$). However, one can show that if F is a pseudo-finite field of characteristic 0, then there is a generic difference field $\mathcal{U}$ containing F and such that $C_{\mathcal{U}} = F$. Thus, the field of constants of $\mathcal{U}$ does not need to be much larger than C_K. In the general case, a general non-sense construction allows one to find a pseudo-finite field F containing C_K and of transcendence degree at most 1 over C_K.

4.21 A partial description of the maximal σ^ℓ-ideal p of R. We keep the notation of the previous subsections, and will first assume that the Picard-Vessiot ring $R' = R/q$ is a domain contained in $\mathcal{U}$.

We will describe some of the elements of q. Write $C_L = C_K(\alpha_1, \ldots, \alpha_m)$, and $\alpha_i = f_i(Y)/g_i(Y)$, where $f_i(Y), g_i(Y) \in K[Y]$ are relatively prime. Then $\sigma(f_i)(AY)$ and $\sigma(g_i)(AY)$ are also relatively prime. Looking at the divisors defined by these polynomials, we obtain that there is some $k_i \in K$ such that $\sigma(f_i)(AY) = k_i f_i(Y)$ and $\sigma(g_i)(AY) = k_i g_i(Y)$. Then $(q, f_i(Y))$ and $(q, g_i(Y))$ are σ-ideals. By the maximality of q, this implies that either $f_i(Y)$ and $g_i(Y)$ are both in q, or else, say if $f_i(Y) \notin q$, that there is some $c_i \in C_{R'}$ such that $g_i(y) = c_i f_i(y)$, because $f_i(y)$ is invertible in R'. If $P_i(Z)$ is the minimal monic polynomial of c_i over C_K and is of degree r, then $g_i(Y)^r P_i(g_i(Y)/f_i(Y)) \in q$. In case $C_{R'} = C_K$ (this is the case for instance if C_K is algebraically closed), then $c_i \in C_K$, and $g_i(Y) - c_i f_i(Y)$ will belong to q. (Note also that if $k_i = k_j$, then also for some $d_j \in C_K$ we will have $f_j(Y) - d_j f_i(Y) \in q$, and $g_j(Y) - c_j d_j f_i(Y) \in q$). The σ-ideal I generated by all these polynomials in R could all of q. In any case one shows easily that q is a minimal prime ideal containing it (because $KC_L[Y, \det(Y)^{-1}]$ and R/I have the same Krull dimension, which is also the Krull dimension of R').

A better result is obtained by Kamensky in [13] Proposition 33: if $C_{R'} = C_K$, and instead of looking at a generating set of C_L over C_K one applies the same procedure to all elements of C_L, one obtains a generating set of the ideal q.

In case R' is not a domain, we reason in the same fashion to get a partial description of the σ^ℓ-ideal p.

References

[1] Y. André, Différentielles non commutatives et théorie de Galois différentielle ou aux différences, *Ann. Sci. École Norm. Sup. (4)*, 34 (2001), no. 5, 685–739.

[2] A. Bialynicki-Birula, On Galois theory of fields with operators, *Amer. J. Math.*, 84 (1962), 89–109.

[3] L. Breen, Tannakian categories, In U. Jannsen and et al, editors, *Motives*, volume 55 of *Proceedings of Symposia in Pure Mathematics*, American Mathematical Society, 1994, 337–376.

[4] Z. Chatzidakis and E. Hrushovski, Model theory of difference fields, *Trans. Amer. Math. Soc.*, 351(1999) no. 8, 2997–3071, .

[5] R. Cohn, *Difference Algebra*, Tracts In Mathematics, Number 17, Interscience Press, New York, 1965.

[6] P. Deligne, Catégories tannakiennes, In P. Cartier et al., *The Grothendieck Festschrift, Vol. 2*, pages 111–195, Progress in Mathematics, Vol. 87, Birkhäuser, Boston, MA, 1990.

[7] P. Deligne and J. Milne, Tannakian categories, In P. Deligne et al., *Hodge cycles, motives and Shimura varieties*, pages 101–228, Lecture Notes in Mathematics, Vol. 900, Springer-Verlag, Berlin-New York, 1982.

[8] T. Dyckerhoff, Picard-Vessiot extensions over number fields, Diplomarbeit, Fakultät für Mathematik und Informatik der Universität Heidelberg, 2005.

[9] P. I. Etingof, Galois groups and connection matrices of q-difference equations, *Electron. Res. Announc. Amer. Math. Soc.*, 1(1995) no.1, 1–9 (electronic).

[10] C. H. Franke, Picard-Vessiot theory of linear homogeneous difference equations, *Transactions of the AMS*, 108 (1963), 491–515.

[11] C. Hardouin, *Structure galoisienne des extensions itérées de modules différentiels*, Ph.D. thesis, Paris 6, 2005, available at `http://www.institut.math.jussieu.fr/theses/2005/hardouin/`.

[12] E. Hrushovski, *Contributions to stable model theory*, Ph.D. thesis, Berkeley, 1986.

[13] M. Kamensky, Definable groups of partial automorphisms, Preprint available at `http://arxiv.org/abs/math.LO/0607718`, 2006.

[14] N. Katz, On the calculation of some differential Galois groups, *Inventiones Mathematicae*, 87 (1987), 13–61.

[15] E. R. Kolchin, Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations, *Annals of Mathematics*, 49 (1948), 1–42.

[16] E. R. Kolchin, Existence theorems connected with the Picard-Vessiot theory of homogeneous linear ordinary differential equations, *Bull. Amer. Math. Soc.*, 54 (1948), 927–932.

[17] E. R. Kolchin, *Differential algebra and algebraic groups*, Academic Press, New York, 1976.

[18] M. A. Papanikolas, Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms, Preprint, Texas A&M University, 2005, available at `http://arxiv.org/abs/math.NT/0506078`.

[19] A. Pillay, Differential Galois theory I, *Illinois J. Math.* 42 (1998), 678–699.

[20] B. Poizat, Une théorie de Galois imaginaire, *J. of Symb. Logic*, 48 (1983), 1151–1170.

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

[22] M. van der Put and M. Reversat, Galois theory of q-difference equations, Preprint 2005, available at `http://arxiv.org/abs/math.QA/0507098`.

[23] M. van der Put and M. F. Singer, *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*, Springer-Verlag, Heidelberg, 1997.

[24] M. van der Put and M. F. Singer, *Galois theory of linear differential equations*, volume 328 of *Grundlehren der mathematischen Wissenshaften*. Springer, Heidelberg, 2003.

[25] J.-P. Ramis and J. Sauloy, The q-analogue of the wild fundamental group (I), in *Algebraic, analytic and geometric aspects of complex differential equations and their deformations. Painlevé hierarchies*, 167–193, RIMS Kôkyûroku Bessatsu, B2, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007. Preprint available at `http://arxiv.org/abs/math.QA/0611521`, 2006.

[26] J. Sauloy, Galois theory of Fuchsian q-difference equations, *Ann. Sci. École Norm. Sup. (4)*, 36 (2003) no.6, 925–968.

[27] W. C. Waterhouse, *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1979.

[28] B. I. Zi'lber, Totally categorical theories; structural properties and the non-finite axiomatizability. in L. Pacholski et al. editors, *Model theory of algebra and arithmetic (Proc. Conf., Karpacz, 1979)*, pages 381–410, Lecture Notes in Mathematics volume 834, Springer Verlag, Berlin Heidelberg 1980.