GALOIS THEORY OF DIFFERENCE EQUATIONS WITH PERIODIC PARAMETERS*

Benjamin Antieau, Alexey Ovchinnikov, and Dmitry Trushin

Department of Mathematics, University of California at Los Angeles, Los Angeles, California, USA

Department of Mathematics, CUNY Queens College, Queens, New York, USA
Department of Mathematics, CUNY Graduate Center, New York, New York, USA

Einstein Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel

We develop a Galois theory for systems of linear difference equations with periodic parameters, for which we also introduce linear difference algebraic groups. We apply this to constructively test if solutions of linear q-difference equations, with $q \in \mathbb{C}^*$ and q not a root of unity, satisfy any polynomial ζ-difference equations with $\zeta^t = 1$, $t \geqslant 1$.

Key Words: Difference Galois theory; q-Difference equations; Difference pseudofields.

2010 Mathematics Subject Classification: Primary 12H10; Secondary 13N99, 20H25, 39A13.

1 INTRODUCTION

In this paper, we give a new Galois theory of systems of linear difference equations with periodic (of finite order) difference parameters. This appears to be the first time that equations with difference parameters have been treated in the literature. In this theory, the Galois groups are linear difference algebraic groups, and they measure difference algebraic dependence of solutions of difference equations. Our Galois theory and Galois correspondence works over fields of any characteristic. In characteristic p, our Galois correspondence is presented here for separable extensions of difference pseudofields[1]. Among numerous potential applications of our approach, we show how this can be applied to studying properties of solutions of q-difference equations.

For the purposes of this introduction, we briefly describe the setup and motivation in the following simple case. Let $q \in \mathbb{C}\setminus\{0\}$. A q-difference equation of order n is an equation in f of the form

$$f(q^n z) + a_{n-1}(z)\cdot f\left(q^{n-1}z\right) + \ldots + a_0(z)\cdot f(z) = 0, \tag{1}$$

*Address correspondence to Prof. Alexey Ovchinnikov, Department of Mathematics, CUNY Queens College, 65-30 Kissena Blvd., Queens, NY 11367, USA; E-mail: aovchinnikov@qc.cuny.edu

[1]Our proofs apply to the non-separable case by using non-reduced Hopf algebras, as pointed out to us by Michael Wibmer.

where $a_0(z),\dots,a_{n-1}(z)\in\mathbb{C}(z)$ are given. Over $\mathbb{C}(z)$, a solution to such an equation will not exist in general. However, there is a ring extension of $\mathbb{C}(z)$, called the Picard–Vessiot ring for the equation that is universal for the property of having a full set of solutions to the equation. Let $f(z)$ be the solution in the Picard–Vessiot ring. When, in addition, we fix a primitive tth root of unity, ζ, and we let $\mathbb{Z}/(t)$ act on $\mathbb{C}(z)$ by $f(z)\mapsto f(\zeta t)$, we show in this paper that we can construct a Picard–Vessiot extension and an action of $\mathbb{Z}/(t)$ on the ring extending the action of ζ on $\mathbb{C}(z)$. The motivation for developing a Galois theory of difference equations with periodic parameters is to study the algebraic relations satisfied by

$$f(z),f(\zeta z),\dots,f\left(\zeta^{t-1}z\right).$$

In particular, as an application of the method of our difference Galois groups with parameters, Theorem 4.9 gives an explicit, complete description of all first-order q-difference equations

$$f(qz)=a(z)f(z) \tag{2}$$

with rational coefficients whose solutions are ζ-difference algebraically independent over the rational functions in variable z with coefficients belonging to the field $\Bbbk$ of q-invariant meromorphic functions on $\mathbb{C}\setminus\{0\}$. This description is easy to use: the inputs are simple functions in the multiplicities of the zeros and poles of $a(z)$. Our proof requires a similar approach to that of [21, Section 3], but it is substantially modified to take into account difference algebraic independence and make the result as explicit as possible. As an example of our methods, we include a deduction of some algebraic independence properties of theta functions (see Theorem 4.5).

The approach of this paper resembles the Galois theory of difference equations with differential parameters studied in [20, 21, 22, 14, 15, 16, 17, 13, 12], where algebraic methods have been developed to test whether solutions of difference equations satisfy polynomial differential equations (see also [23] for a general Tannakian approach). In particular, these methods can be used to prove Hölder's theorem which says that the Γ-function, which satisfies the difference equation $\Gamma(x+1)=x\cdot\Gamma(x)$, satisfies no non-trivial differential equation over $\mathbb{C}(x)$. However, when treating difference equations with differential parameters, one may use fields as the rings of constants. This is not available when using difference parameters, as Example 2.3 and [29, Proposition 7.3] show. The constants in our theory are rings that have zero-divisors, and this fact requires numerous additional subtleties into our approach. The key idea is to find a suitable notion of a difference closed ring. We use the difference-closed pseudofields of [30], which we review in Section 2. Another approach to the question of difference algebraic closure is in [24], where difference versions of valuation rings are given. However, since we require zero-divisors, Lando's approach is insufficient.

Picard–Vessiot extensions with zero divisors for systems of linear difference equation have been considered in [32, 10, 27] with a non-linear generalization considered in [19]. Also, Galois theories of linear difference equations, without parameters, when the ground ring has zero divisors have been studied in [4, 3, 1, 2, 34], where including zero divisors into the ground ring is needed and provides a much more transparent Galois correspondence. In all the mentioned cases, the ground ring must be a finite product of fields (called Noetherian difference pseudofields).

Our approach allows us not only to treat parameters, but also prepares a foundation for studying the non-Noetherian case as we base our methods on a natural geometric approach to difference varieties developed in [30], which has been further generalized to the non-Noetherian case in [31]. However, to extend the theory to infinite parameter groups, it is necessary to treat the non-Noetherian case, as the same construction results in a non-Noetherian ring. This generalization has been carried out in [28] using the methods of [34, 35] and the present paper (see also [18] for the Galois theory of linear differential equations with difference parameters).

Some of our results can be treated in another way, via the method of faithfully flat descent from algebraic geometry [26]. However, our theory gives a more flexible theory than that obtained via descent, as explained in Section 3.6.

The paper is organized as follows. We give basic definitions in Section 2.1. The main properties of difference pseudofields are detailed in Sections 2.2 and 2.3. Section 3 contains the development of our main technique, difference Galois theory (also called difference Picard–Vessiot theory) with periodic parameters. Difference algebraic groups are introduced and studied in Section 3.3. We finish by showing in Section 4 how to use our theory to study periodic difference algebraic dependencies among solutions of difference equations. In particular, we apply these results to study Jacobi's theta-function in Section 4.3 and to give a complete characterization to all first-order q-difference equations with ζ-difference algebraically independent solutions over rational functions in variable z with coefficients belonging to the field of q-invariant meromorphic functions on $\mathbb{C}\setminus\{0\}$ in Section 4.4.

2 BASIC DEFINITIONS

2.1 Difference rings

Most of the basic notions on difference algebra can be found in [11, 25]. Below, we will introduce those that we use here. Let

$$\Sigma_0=\mathbb{Z},\quad \Sigma_1=\mathbb{Z}/t_1\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}/t_s\mathbb{Z},\quad \text{and}\quad \Sigma=\Sigma_0\oplus\Sigma_1,$$

where each $t_i\geqslant 2$. Let σ be a generator of Σ_0 and ρ_i, $1\leqslant i\leqslant s$, generate each component of Σ_1.

A ring R equipped with an action of a fixed subgroup $\Sigma'\subset\Sigma$ by automorphisms is called a Σ'-ring.

Example 2.1. Let $R=\mathbb{C}(x)$ and $\sigma(x)=px$, $\rho(x)=qx$ with $p,q\in\mathbb{C}^*$, $|p|\neq 1$ and q a primitive m-th root of unity for some $m\geqslant 2$. Then $\Sigma_0=\{\sigma^n\mid n\in\mathbb{Z}\}$ and $\Sigma_1=\left\{\mathrm{id},\rho,\ldots,\rho^{m-1}\right\}$.

Let R be a Σ'-ring and let $R[\Sigma'] = \left\{\sum r_\tau \tau \,\middle|\, r_\tau \in R,\ \tau \in \Sigma'\right\}$ denote the ring of difference operators on R. The multiplication on $R[\Sigma']$ is given by $\tau \cdot r = \tau(r)\tau$. For a set Y, let

$$R\{Y\}_{\Sigma'} = R\left[\ldots, \tau y, \ldots \mid \tau \in \Sigma',\ y \in Y\right]$$

denote the ring of Σ'-polynomials over R with Y as the set of Σ'-indeterminates.

Example 2.2. For example, if $\Sigma' = \Sigma_1 = \mathbb{Z}/2\mathbb{Z}$ and ρ is a generator of Σ_1, then $R\{y\}_{\Sigma'} = R[y, \rho y]$ with the action of ρ given by $\rho(y) = \rho y$ and $\rho(\rho y) = y$.

An ideal $\mathfrak{a} \subset R$ is called a Σ'-ideal if $\Sigma'(\mathfrak{a}) \subset \mathfrak{a}$, where

$$\Sigma'(\mathfrak{a}) := \left\{\sigma(a) \mid \sigma \in \Sigma', a \in \mathfrak{a}\right\}.$$

The smallest Σ'-ideal containing a set $F \subset R$ is denoted by $[F]_{\Sigma'}$. If $\Sigma' = \Sigma$, then it is also denoted simply by $[F]$. Let R_1 and R_2 be Σ'-rings. A ring homomorphism $f : R_1 \to R_2$ is called a Σ'-homomorphism if $f(\tau(r)) = \tau(f(r))$, for all $\tau \in \Sigma'$, $r \in R_1$.

The following example shows that even if we start with a base field, the constants of the solution space as constructed in Section 3 have zero divisors.

Example 2.3. Let $\Sigma_1 = \mathbb{Z}/4\mathbb{Z}$ with a generator ρ. Consider the equation $\sigma x = -x$. The procedure of constructing a solution space (called Picard–Vessiot extension) of the above equation described in Section 3 first takes $\mathbb{C}\{x, 1/x\}_\rho$, with $\sigma x = -x$, and then quotients by $\left[\rho x - ix, x^4 - 1\right]$, which is a maximal Σ-ideal. Thus, we arrive at the ring $\mathbb{C}[x]/\left(x^4 - 1\right)$, $\sigma x = -x$ and $\rho x = ix$, which is a Σ-pseudofield generated by the solution of the equation. The subring of constants is generated by x^2 and is isomorphic to $\mathbb{C}[t]/\left(t^2 - 1\right)$, which is not a field.

Denote the ring of Σ'-constants of R by $R^{\Sigma'}$. In other words,

$$R^{\Sigma'} = \left\{r \in R \mid \tau(r) = r \text{ for all } \tau \in \Sigma'\right\}.$$

The set of all Σ'-ideals of R will be denoted by $\mathrm{Id}^{\Sigma'}(R)$.

Definition 2.4. A Σ'-ideal $\mathfrak{p}$ of R is called pseudoprime if there exists a multiplicatively closed subset $S \subset R$ such that $\mathfrak{p}$ is a maximal Σ-ideal with $\mathfrak{p} \cap S = \varnothing$.

Lemma 2.5. *Let A and B be Σ-rings and $\varphi : A \to B$ be a Σ-homomorphism. Then for any pseudoprime ideal $\mathfrak{q}$ in B the ideal $\varphi^{-1}(\mathfrak{q})$ is pseudoprime.*

Proof. See [30, Section 2]. □

The set of all pseudoprime ideals of R will be denoted by $\operatorname{PSpec} R$ or $\operatorname{PSpec}^{\Sigma'} R$. For $s \in R$, $(\operatorname{PSpec} R)_s$ denotes the set of pseudoprime ideals of R not containing s. Let R_1 and R_2 be Σ'-rings and $f : R_1 \to R_2$ be a Σ'-homomorphism. Then $f^*(\mathfrak{q}) := f^{-1}(\mathfrak{q})$ defines a map

$$f^* : \operatorname{PSpec} R_2 \to \operatorname{PSpec} R_1$$

by Lemma 2.5. For an ideal $\mathfrak{a} \subset R$ denote by $\mathfrak{a}_{\Sigma'}$ the largest Σ'-ideal of R contained in $\mathfrak{a}$. Note that if $\mathfrak{p}$ is a prime ideal of R, then the ideal $\mathfrak{p}_{\Sigma'}$ is pseudoprime.

Recall that an R-module M with an action of Σ' is called a Σ'-module if for all $\tau \in \Sigma'$, $r \in R$, and $m \in M$, we have $\tau(rm) = \tau(r)\tau(m)$. A Σ'-ring is called simple if it contains no proper Σ'-ideals except for (0).

Definition 2.6. A ring R is called absolutely flat if every R-module is flat. An absolutely flat simple Σ'-ring $\mathbf{k}$ is called a Σ'-pseudofield (see [30]).

For every subset $E \subset R\{y_1,\ldots,y_n\}_{\Sigma'}$, let $\mathbb{V}(E) \subset R^n$ be the set of common zeroes of E in R^n. Conversely, for every subset $X \subset R^n$, let

$$\mathbb{I}(X) \subset R\{y_1,\ldots,y_n\}_{\Sigma'}$$

be the Σ'-ideal of all polynomials in $R\{y_1,\ldots,y_n\}_{\Sigma'}$ vanishing on X. One sees that, for any reduced R and Σ'-ideal $I \subset R\{y_1,\ldots,y_n\}_{\Sigma'}$, we have $\sqrt{I} \subset \mathbb{I}(\mathbb{V}(I))$.

Definition 2.7. [30, Section 4.3] A Σ'-pseudofield R is called *difference closed* if, for every Σ'-ideal $I \subset R\{y_1,\ldots,y_n\}_{\Sigma'}$, we have $\sqrt{I} = \mathbb{I}(\mathbb{V}(I))$.

2.2 Properties of pseudofields

Proposition 2.8. *Let L be Σ'-simple ring and $K \subset L$ be an absolutely flat Σ'-subring. Then, K is a Σ'-pseudofield.*

Proof. Let $0 \neq a \in K$. We will show that the Σ'-ideal of K generated by a contains 1. Since K is absolutely flat, we may assume that $a^2 = a$, since every principal ideal is generated by an idempotent [5, Exercise II.27]. Since the Σ'-ideal generated by a in L contains 1, there exist $h_i \in L$, $0 \leqslant i \leqslant r$, such that

$$1 = h_0 a + h_1\sigma_1(a) + \ldots + h_r\sigma_r(a) \tag{3}$$

for some $\sigma_k \in \Sigma'$. Set $\sigma_0 = \mathrm{id}$ for notation. We will show by induction on $k \leqslant r$ that the h_i's can be selected so that $h_i \in K$, $0 \leqslant i \leqslant k$. The base $k = 0$ is done in the same way as the inductive step. Assume the statement for $k-1 \geq 0$. We will show it for k. Multiplying (3) by $1-\sigma_k(a)$ and using $a^2 = a$, we have:

$$1-\sigma_k(a) = (1-\sigma_k(a))(h_0\cdot a + \ldots + h_{k-1}\cdot\sigma_{k-1}(a) + h_{k+1}\cdot\sigma_{k+1}(a) + \ldots + h_r\cdot\sigma_r(a)).$$

Hence,

$$\begin{aligned} 1 =& (1-\sigma_k(a))h_0\cdot a + \ldots + (1-\sigma_k(a))h_{k-1}\cdot\sigma_{k-1}(a) + \\ &+ \sigma_k(a) + (1-\sigma_k(a))h_{k+1}\cdot\sigma_{k+1}(a) + \ldots + (1-\sigma_k(a))h_r\cdot\sigma_r(a) \end{aligned}$$

with $(1-\sigma_k(a))h_0,\ldots,(1-\sigma_k(a))h_{k-1}, 1 \in K$, which finishes the proof. □

Proposition 2.9. *Let L be an absolutely flat ring and $H \subset \mathrm{Aut}(L)$. Then the ring L^H is absolutely flat.*

Proof. Let $0 \neq a \in L^H$. Then by [5, Exercise II.27] there exist unique an idempotent e and a' in L such that

$$e = aa', \quad a = ea, \quad \text{and} \quad a' = ea'. \tag{4}$$

To see uniqueness, note that if $(\bar{e}, \bar{a}')$ is another such pair, then $e\bar{e} = ea\bar{a}' = a\bar{a}' = \bar{e}$ and, similarly, $e\bar{e} = e$. So, the element e is unique. Now, $a' = ea' = \bar{e}a' = a\bar{a}'a'$ and, in the same manner, $\bar{a}' = \bar{e}\bar{a}' = e\bar{a}' = aa'\bar{a}'$.

We will show now that e and a' are H-invariant. For $\sigma \in H$ we have

$$a = \sigma(a) = \sigma(ae) = a\sigma(e).$$

Multiplying by a', we obtain $e = e\sigma(e)$. Similarly, we obtain $e = e\sigma^{-1}(e)$, which implies that $\sigma(e) = e\sigma(e)$. Hence, $\sigma(e) = e$. We, therefore, have

$$e = a\sigma(a'), \quad a = ea, \quad \text{and} \quad \sigma(a') = e\sigma(a'). \tag{5}$$

Since the pair (e, a') is unique, (4) and (5) imply that $\sigma(a') = a'$. Applying [5, Exercise II.27] again, we conclude that L^H is absolutely flat. □

Proposition 2.10. *Let A be a Σ_1-closed pseudofield. Then the ring $R = A[\Sigma_1]$ is completely reducible: $R \cong A \oplus \ldots \oplus A$ as Σ_1-modules over A. In other words, every Σ_1-module over A has a basis of Σ_1-invariant elements. Moreover, $A[\Sigma_1] \cong \mathbf{M}_n(C)$ as rings, where $C = A^{\Sigma_1}$.*

Proof. Follows [30, Proposition 26 and Remark 27]. □

Proposition 2.11. *Let R be a Σ-simple ring and $A := R^\sigma$ be a Σ_1-difference closed pseudofield. Let B be any Σ-A-algebra with σ acting as the identity. Then the Σ-homomorphism $B \to R \otimes_A B$, with $b \mapsto 1 \otimes b$, $b \in B$, induces a bijection*

$$\mathrm{Id}^{\Sigma_1}(B) \longleftrightarrow \mathrm{Id}^{\Sigma}(R \otimes_A B)$$

via $\mathfrak{a} \subset B \longrightarrow \mathfrak{a}^e := R \otimes_A \mathfrak{a}$, $\mathfrak{b}^c := \mathfrak{b} \cap B \longleftarrow \mathfrak{b} \subset R \otimes_A B$.

Proof. Let I be a Σ-ideal of the ring $R \otimes_A B$ and let $I^c = J$. We will show that $I = J^e$. In other words, by passing to $R \otimes_A (B/J)$, we will show that if $I^c = (0)$, then $I = (0)$. By Proposition 2.10, there exists a basis $\{b_i\}_{i \in I}$ of B over A consisting of Σ_1-invariant elements. Then, every element of $R \otimes_A B$ is of the form

$$a_1 \otimes b_{i_1} + \ldots + a_n \otimes b_{i_n}$$

for some $a_i \in R$, $1 \leqslant i \leqslant n$. Let $0 \neq u \in I$ have the shortest expression of the form $u = a_1 \otimes b_{j_1} + \ldots + a_k \otimes b_{j_k}$,

$$M = \left\{ a \in R \mid \exists c_2, \ldots, c_k \in R, i_1, \ldots, i_k \in I : a \otimes b_{i_1} + c_2 \otimes b_{i_2} + \ldots + c_k \otimes b_{i_k} \in I \right\}.$$

As $0 \neq a_1 \in M$, and since $\Sigma(b_i) = b_i$, $1 \leqslant i \leqslant n$, the set M is a non-zero Σ-ideal of R. Hence, $1 \in M$. Therefore, there exists u with $a_1 = 1$. Since

$$u - \sigma(u) = (a_2 - \sigma(a_2)) \otimes b_{i_2} + \ldots + (a_k - \sigma(a_k)) \otimes b_{i_k} \in I \tag{6}$$

and has a shorter expression than u, we have

$$u - \sigma(u) = 0. \tag{7}$$

Since $\{b_i\}_{i \in I}$ is a basis of B over A, $\{1 \otimes b_i\}_{i \in I}$ is a basis of $R \otimes_A B$ over R. Therefore, (6) and (7) imply that $\sigma(a_2) = a_2, \ldots, \sigma(a_k) = a_k$, that is, $a_2, \ldots, a_k \in A$. Thus,

$$u = 1 \otimes \left(b_{i_1} + a_2 b_{i_2} + \ldots + a_k b_{i_k}\right).$$

Hence,

$$0 \neq b_{i_1} + a_2 b_{i_2} + \ldots + a_k b_{i_k} \in I^c,$$

contradicting $I^c = (0)$. Therefore, we have shown that $(I^c)^e = I$. On the other hand, since R is a free A-module, the B-module $R \otimes_A B$ is also free and, therefore, faithfully flat. Thus, by [5, Exercise III.16] for every ideal $J \subset B$ we have $(J^e)^c = J$, which finishes the proof. □

Corollary 2.12. *Let B be a Σ-ring containing a Σ-pseudofield L with $C_L := L^\sigma$ being a Σ_1-closed pseudofield. Let $C \subset B^\sigma$ be a Σ_1-subring such that $C_L \subset C$. Then $L \cdot C = L \otimes_{C_L} C$.*

Proof. The kernel I of the Σ-homomorphism

$$L \otimes_{C_L} C \to L \cdot C \subset B, \quad l \otimes c \mapsto l \cdot c,$$

is a Σ-ideal with $I^c = (0) \subset C$. By Proposition 2.11, we conclude that $I = 0$. □

2.3 Noetherian pseudofields

Lemma 2.13. *Let $A \subset B$ be Σ-rings such that for some $s \in A$ the map $\operatorname{Spec} B_s \to \operatorname{Spec} A_s$ is surjective. Then the map $\varphi : (\operatorname{PSpec} B)_s \to (\operatorname{PSpec} A)_s$ is surjective as well.*

Proof. Let $\mathfrak{q} \subset A$ be a pseudoprime ideal with $s \notin \mathfrak{q}$. Then, since the maximal ideal not intersecting a multiplicative subset is prime, by definition, there exists a prime ideal $\mathfrak{p} \supset \mathfrak{q}$ such that

$$\mathfrak{q} = \bigcap\nolimits_{\tau \in \Sigma} \tau(\mathfrak{p})$$

with $\mathfrak{q}$ being a maximal Σ-ideal contained in $\tau(\mathfrak{p})$, $\tau \in \Sigma$. Since $s \notin \mathfrak{q}$, there exists $\tau \in \Sigma$ such that $s \notin \tau(\mathfrak{p})$. By our assumption, there exists a prime ideal $\mathfrak{p}' \subset B$ with $\mathfrak{p}' \cap A = \mathfrak{p}^\tau$. Then the ideal $\mathfrak{p}'_\Sigma$ is the pseudoprime ideal in B that is mapped to $\mathfrak{p}$ by φ. □

Lemma 2.14. *Let $A \subset B$ be Σ-rings such that A is Noetherian and reduced and B is a finitely generated A-algebra. Then there exists $0 \neq s \in A$ such that the map $(\operatorname{PSpec} B)_s \to (\operatorname{PSpec} A)_s$ is surjective.*

Proof. There exists $s \in A$ such that A_s is an integral domain. For instance, suppose that $(0) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t$ is the representation of (0) as the intersection of the finitely many minimal prime ideals in the Noetherian ring A. Let $s \in \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_t$ be such that $t \notin \mathfrak{p}_1$. Then, A_s is a reduced ring with a single minimal prime ideal. Thus, it is integral. By [30, Lemma 30], there exists $t \in A$ such that the map $\operatorname{Spec} B_{st} \to \operatorname{Spec} A_{st}$ is surjective. The statement now follows from Lemma 2.13. □

Theorem 2.15. *Let L be a Noetherian Σ-pseudofield with $C := L^\sigma$ being a Σ_1-closed pseudofield. Let R be a Σ_1-finitely generated Σ-simple ring over L. Then $R^\sigma = C$.*

Proof. Let $b \in R^\sigma$. Since $|\Sigma_1| < \infty$, the ring R is finitely generated over L. Since R is Σ-simple, it is reduced. Therefore, the Σ-subring of R generated by L and b, denoted by $L\{b\}$, is reduced as well. Hence, by Lemma 2.14, there exists a non-nilpotent element $s \in L\{b\}$ such that the map

$$(\operatorname{PSpec} R)_s \to (\operatorname{PSpec} L\{b\})_s$$

is surjective. Therefore, since $\operatorname{PSpec} R = \{(0)\}$, every non-zero pseudoprime ideal in $L\{b\}$ contains s. By Corollary 2.12, we have $L\{b\} = L \otimes_C C\{b\}$. By Proposition 2.10, L is a free C-module. Let $\{l_i\}_{i \in I}$ be a Σ_1-invariant basis over C. Then there exist $r_1, \ldots, r_k \in C\{b\}$ such that

$$s = l_1 \otimes r_1 + \ldots + l_k \otimes r_k.$$

Since the ring $L\{b\}$ is reduced, r_1 is not nilpotent. Therefore, by [30, Proposition 34], there exists a maximal Σ-ideal $\mathfrak{m}$ in $C\{b\}$ such that $C\{b\}/\mathfrak{m} = C$ and $r_1 \notin \mathfrak{m}$. Let

$$\varphi : L\{b\} = L \otimes_C C\{b\} \to L \otimes_C C\{b\}/\mathfrak{m} = L \otimes_C C = L.$$

Then,

$$\varphi(s) = l_1 \bar{r}_1 + \ldots + l_k \bar{r}_k,$$

where $\bar{r}_i$ are the images of r_i modulo $\mathfrak{m}$, $1 \leqslant i \leqslant k$. Since $\{l_1, \ldots, l_k\}$ are linearly independent over C and $\bar{r}_1 \neq 0$, the ideal $L \otimes_C \mathfrak{m}$ does not contain s. Since φ is a Σ-homomorphism, $L \otimes_C \mathfrak{m} = \varphi^{-1}((0))$, and (0) is a pseudoprime ideal in L, the ideal $L \otimes_C \mathfrak{m}$ is pseudoprime by Lemma 2.5. Therefore, $L \otimes_C \mathfrak{m} = (0)$ by the above. Thus, we see that $b \in C$ by taking σ-invariants as φ is an injective Σ-homomorphism. □

Recall that an idempotent that is not a sum of several distinct orthogonal idempotents is called indecomposable.

Proposition 2.16. *Let L be a Noetherian Σ-pseudofield and let $F = L/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal ideal in L. Then, $L \cong F \times \ldots \times F$. Moreover, Σ acts transitively on the set of indecomposable idempotents of L.*

Proof. Since the ring L is Noetherian and $\dim L = 0$, by [5, Theorem 8.5], the ring L is Artinian. Therefore, by [5, Theorem VII.7], it is a finite product of local Artinian rings. Since L is reduced, by [5, Proposition VIII.1],

$$L = F_1 \times \ldots \times F_n, \tag{8}$$

where F_i is a field, $1 \leqslant i \leqslant n$. Since L is Σ-simple, the group Σ acts transitively on $\operatorname{Spec} L$. Therefore, $F_i \cong F_1$, $1 \leqslant i \leqslant n$, as residue fields. Let e be an indecomposable idempotent in L. Let $\operatorname{Orb}_\Sigma(e) = \{e_1, \ldots, e_k\}$. Then, the idempotent

$$E := e_1 + \ldots + e_k$$

is Σ-invariant. Since L is Σ-simple, we have $E = 1$. Decomposition (8) implies that L has n indecomposable idempotents, each one is of the form

$$(0, \ldots, 0, 1, 0, \ldots, 0)$$

and, thus, $k = n$ and Σ acts transitively on the set of indecomposable idempotents of L. □

Let B be a Σ_0-ring and let

$$F_{\Sigma_1}(B) = \prod_{\mu \in \Sigma_1} B = \{f : \Sigma_1 \to B\}, \tag{9}$$

which is a Σ_0-ring with the component-wise action of Σ_0. Define

$$(\mu f)(\tau) = f\left(\mu^{-1}\tau\right), \quad f \in F_{\Sigma_1}(B), \ \mu, \tau \in \Sigma_1.$$

The above makes $F_{\Sigma_1}(B)$ a Σ-ring. For every $\mu \in \Sigma_1$ define a Σ_0-homomorphism

$$\gamma_\mu : F_{\Sigma_1}(B) \to B, \quad f \mapsto f(\mu). \tag{10}$$

Moreover, we have

$$\gamma_\tau(\mu f) = (\mu f)(\tau) = f\left(\mu^{-1}\tau\right) = \gamma_{\mu^{-1}\tau}(f).$$

Proposition 2.17. *Let A be a Σ-ring, B be a Σ_0-ring, and $\varphi : A \to B$ be a Σ_0-homomorphism. Then for every $\mu \in \Sigma$ there exists unique Σ-homomorphism $\Phi_\mu : A \to F_{\Sigma_1}(B)$ such that the following diagram*

$$\begin{tikzcd} & F_{\Sigma_1}(B) \arrow[d, "\gamma_\mu"] \\ A \arrow[ur, "\Phi_\mu"] \arrow[r, "\varphi"] & B \end{tikzcd}$$

is commutative.

Proof. Since

$$\Phi_\mu(a)\left(\tau^{-1}\mu\right) = (\tau\Phi_\mu(a))(\mu) = \varphi(\tau a),$$

where $a \in A$ and $\tau \in \Sigma$, the homomorphism Φ_μ is unique if it exists. Define

$$\Phi_\mu(a)(\tau) = \varphi\left(\mu\tau^{-1}a\right).$$

For every $\alpha \in \Sigma_1$ we have

$$\Phi_\mu(\alpha a)(\tau) = \varphi\left(\mu\tau^{-1}\alpha a\right) = \varphi\left(\mu\left(\alpha^{-1}\tau\right)^{-1}a\right) = \Phi_\mu(a)\left(\alpha^{-1}\tau\right) = (\alpha\Phi_\mu(a))(\tau)$$
$$\Phi_\mu(\nu a)(\tau) = \varphi\left(\mu\tau^{-1}\nu a\right) = \nu\left(\varphi\left(\mu\tau^{-1}a\right)\right) = \nu(\Phi_\mu(a)(\tau)) = \nu(\Phi_\mu(a))(\tau)$$

for all $\alpha, \tau \in \Sigma_1$, $\nu \in \Sigma_0$, and $a \in A$. Thus, Φ_μ is a Σ-homomorphism. □

Proposition 2.18. *Let L be a Noetherian Σ-pseudofield such that L^σ is a Σ_1-closed pseudofield. Then, there exists a Noetherian Σ_0-pseudofield B such that $L \cong F_{\Sigma_1}(B)$.*

Proof. By [30, Theorem 17(4)], there exists an algebraically closed field K such that

$$L^\sigma = F_{\Sigma_1}(K).$$

Let $\delta_\tau \in F_{\Sigma_1}(K)$ be the indicator of the point $\tau \in \Sigma_1$ and $e = \delta_{\mathrm{id}}$. Let also $B = eL$, which is a Noetherian absolutely flat ring as a quotient of a Noetherian Σ-pseudofield. By Proposition 2.17, the homomorphism $L \to B$, with $a \mapsto e \cdot a$, lifts to a unique Σ-homomorphism

$$\phi : L \longrightarrow F_{\Sigma_1}(B).$$

Since L is Σ-simple, ϕ is injective. To show that ϕ is surjective, we will prove that $\phi(L)$ contains all indecomposable idempotents of $F_{\Sigma_1}(B)$. Every indecomposable idempotent of the ring $F_{\Sigma_1}(B)$ is of the form $\delta_\tau \cdot f$, f is an indecomposable idempotent of B. Let $f = eh$, where $h \in L$. Since

$$\phi(\tau(e)h)(\nu) = (e\tau(e)h)(\nu) = (\tau(e)f)(\nu) = e\left(\tau^{-1}\nu\right)f = \delta_\tau(\nu)f,$$

we are done. Finally, B is Σ_0-simple. Indeed, let $\mathfrak{b} \subset B$ be a Σ_0-ideal. Let $I \subset F_{\Sigma_1}(B)$ consist of all functions f with image contained in $\mathfrak{b}$. Since I is an ideal and Σ_1 is acting on the domain, I is invariant under the Σ_1-action. Since $\mathfrak{b}$ is a Σ_0 ideal, then I is a Σ_0-ideal as well. Therefore, I is a Σ-ideal, which contradicts to L being a pseudofield. □

Proposition 2.19. *Let L be a Noetherian Σ-pseudofield such that L^σ is a Σ_1-closed pseudofield. Then,*

$$L \cong \prod_{i=1}^{n} F_{\Sigma_1}(F)$$

as Σ_1-rings, where F is a field.

Proof. By Proposition 2.18, $L = F_{\Sigma_1}(B)$, where B is a Noetherian Σ_0-pseudofield. Let $f_1,\ldots,f_n$ be all indecomposable idempotents of B. Then

$$L = f_1L\times\ldots\times f_nL.$$

On the other hand,

$$f_iF_{\Sigma_1}(B) = F_{\Sigma_1}(f_iB) = F_{\Sigma_1}(F_i),$$

where $F_i = f_iB$ and $F_1 \cong F_i$, $1 \leqslant i \leqslant n$. □

Proposition 2.20. *Let L be a Noetherian Σ-pseudofield and $K \subset L$ be a Σ-pseudofield as well. Then K is Noetherian.*

Proof. Note that a pseudofield is Noetherian if and only if it contains a finite set of indecomposable idempotents $e_1,\ldots,e_n$ with

$$e_1+\ldots+e_n = 1. \tag{11}$$

Necessity has been discussed above. To show sufficiency, note that if e is an indecomposable idempotent of an absolutely flat ring R, then eR is a field. Indeed, eR is an absolutely flat ring without nontrivial idempotents [5, Exercise II.27]. Moreover, for every element $x \in R$ we have $x = ax^2$. Therefore, ax is an idempotent. So, either $ax = 0$ and, thus, $x = ax^2 = 0$, or $ax = 1$. Hence, equality (11) implies that R is finite product of fields and, therefore, is Noetherian.

Thus, since every idempotent of K is an idempotent of L, which is Noetherian, the ring K has finitely many indecomposable idempotents $f_1,\ldots,f_k$. Since $f_1+\ldots+f_k$ is left fixed by Σ, we have $f_1+\ldots+f_k = 1$. Again, by the above, the ring K is Noetherian. □

Proposition 2.21. *Let L be a Σ-field such that the subfield $C := L^\sigma$ is algebraically closed. Then there exists a Σ-pseudofield A and a Σ-embedding $\varphi : L \to A$ such that A^σ is the Σ_1-closure of the Σ_1-field $\varphi(C)$.*

Proof. Set $A = F_{\Sigma_1}(L)$ and and let φ be the Taylor homomorphism for $\mathrm{id} : L \to L$ by Proposition 2.17. Then, $A^\sigma = F_{\Sigma_1}(C)$ is the Σ_1-closure of C [30, discussions preceding Proposition 19]. □

3 PICARD–VESSIOT THEORY

3.1 Picard–Vessiot ring

Let K be a Noetherian Σ-pseudofield and let $C = K^\sigma$ be a Σ_1-closed pseudofield. Let $A \in \mathrm{GL}_n(K)$. Consider the following difference equation

$$\sigma Y = AY. \tag{12}$$

Let R be a Σ-ring containing K.

Definition 3.1. A matrix $F \in \mathrm{GL}_n(R)$ is called a fundamental matrix of equation (12) if $\sigma F = AF$.

Let F_1 and F_2 be two fundamental matrices of (12). Then for $M := F_1^{-1}F_2$ we have

$$\sigma(M) = \sigma(F_1)^{-1}\sigma(F_2) = F_1^{-1}A^{-1}AF_2 = F_1^{-1}F_2 = M,$$

that is, $M \in \mathrm{GL}_n(R^\sigma)$.

Definition 3.2. A Σ-ring R is called a Picard–Vessiot ring for equation (12) if

1. there exists a fundamental matrix $F \in \mathrm{GL}_n(R)$ for (12),
2. R is a Σ-simple ring, and
3. R is Σ-generated over K be the matrix entries F_{ij} and $1/\det F$.

Proposition 3.3. *Let K be a Noetherian Σ-pseudofield, K^σ be a Σ_1-closed pseudofield, and R be a Picard–Vessiot ring for equation* (12)*. Then, $R^\sigma = K^\sigma$.*

Proof. Since R is a Σ_1-finitely generated algebra over K and $|\Sigma_1| < \infty$, R is finitely generated over K. Then the result follows from Theorem 2.15. ☐

Proposition 3.4. *Let K be a Noetherian Σ-pseudofield with K^σ being a Σ_1-closed pseudofield. Then there exists a unique Picard–Vessiot ring for equation* (12)*.*

Proof. For existence, define the action of σ on the Σ_1-ring

$$R := K\{F_{ij}, 1/\det F\}_{\Sigma_1}$$

by $\sigma F = AF$. Let $\mathfrak{m}$ be any maximal Σ-ideal in R. Then $R/\mathfrak{m}$ is the Picard–Vessiot ring for equation (12). For uniqueness, let R_1 and R_2 be two Picard–Vessiot rings of equations (12). Let

$$R = (R_1 \otimes_K R_2)/\mathfrak{m},$$

where $\mathfrak{m}$ is a maximal Σ-ideal. Since R_1 and R_2 are Σ-simple, the Σ-homomorphisms

$$\varphi_1 : R_1 \to R,\ r \mapsto r \otimes 1, \quad \varphi_2 : R_2 \to R,\ r \mapsto 1 \otimes r,$$

are injective. Let F_1 and F_2 be fundamental matrices of R_1 and R_2, respectively. Then there exists $M \in \mathrm{GL}_n(R^\sigma)$ such that $\varphi_1(F_1) = \varphi_2(F_2)M$. Proposition 3.3 implies that $R^\sigma = K^\sigma$. Therefore, $\varphi_1(F_1) \subset \varphi_2(R_2)$. Similarly, $\varphi_2(F_2) \subset \varphi_1(R_1)$. Hence, $\varphi_1(R_1) = \varphi_2(R_2)$ and, thus, $R_1 \cong R_2 \cong R$. ☐

Proposition 3.5. *Let K be a Noetherian Σ-pseudofield with K^σ being a Σ_1-closed pseudofield and R be a Picard–Vessiot ring of equation* (12)*. Then the complete quotient ring $L := \mathrm{Qt}(R)$ is a Noetherian Σ-pseudofield with $L^\sigma = K^\sigma$.*

Proof. We will first show that L is Σ-simple. Let $\mathfrak{a}$ be a non-zero Σ-ideal of L. Then $\mathfrak{a}\cap R \neq (0)$ and, therefore, $1 \in \mathfrak{a}$.

We will now show that L is a finite product of fields. Since the ring K is Noetherian and R is finitely generated over K, the ring R is Noetherian as well by the Hilbert basis theorem. Hence, there exists a smallest set of prime ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$ in R such that $(0) = \mathfrak{p}_1\cap\ldots\cap\mathfrak{p}_n$. The set of non-zero divisors in R coincides with $R\setminus\bigcup_{i=1}^n \mathfrak{p}_i$. In $\mathrm{Qt}(R)$, all prime ideals correspond to the $\mathfrak{p}_i$'s, that is, they are all maximal and their intersection is (0). Therefore, by [5, Proposition 1.10]

$$\mathrm{Qt}(R) \cong \mathrm{Qt}(R/\mathfrak{p}_1)\times\ldots\times\mathrm{Qt}(R/\mathfrak{p}_n),$$

which is absolutely flat and Noetherian.

Let $c = \frac{a}{b} \in L^\sigma$. Using Theorem 2.15, it suffices to show that $R\{c\}_{\Sigma_1}$ is a Σ-simple Σ-ring, since this would imply that $c \in K^\sigma$. For this, we will show that every Σ-subring $D \subset L$ containing K is Σ-simple. Indeed, for every $0 \neq d \in L$ there exists $a \in R$ such that $0 \neq ad \in R$, which is true because L is the localization with respect to the set of non-zero divisors. Therefore, for every nonzero ideal $\mathfrak{a}$ of D we have $\mathfrak{a}\cap R \neq \{0\}$. Since R is Σ-simple, $1 \in \mathfrak{a}$. □

3.2 Picard–Vessiot pseudofield

Let K be a Noetherian Σ-pseudofield with K^σ being Σ_1-closed.

Definition 3.6. A Noetherian Σ-pseudofield L is called a Picard–Vessiot pseudofield for equation (12) if

1. there is a fundamental matrix F of equation (12) with coefficients in L,
2. $L^\sigma = K^\sigma$,
3. L is Σ_1-generated over K by the entries of F.

It follows from Proposition 3.5 that every equation (12) has a Picard–Vessiot pseudofield. We will show that all Picard–Vessiot pseudofields are of this form.

Proposition 3.7. *Let K be a Noetherian Σ-pseudofield, with $C := K^\sigma$ being a Σ_1-closed pseudofield, and L be a Picard–Vessiot pseudofield for equation* (12)*. Then, $L \cong \mathrm{Qt}(R)$, where R is the corresponding Picard–Vessiot ring.*

Proof. Let σ act on the Σ_1-ring $R := L\{X_{ij}, 1/\det X\}_{\Sigma_1}$ by $\sigma X = AX$. Let F be a fundamental matrix of (12) with coefficients in L. Define $Y = F^{-1}X$. Then $R = L\{Y_{ij}, 1/\det Y\}_{\Sigma_1}$ and $\sigma Y = Y$. Therefore,

$$R^\sigma = C\{Y_{ij}, 1/\det Y\}_{\Sigma_1}.$$

Moreover, we have a Σ-isomorphism

$$L\otimes_K K\{X_{ij}, 1/\det X\}_{\Sigma_1} \cong L\otimes_C C\{Y_{ij}, 1/\det Y\}_{\Sigma_1}. \tag{13}$$

Recall that the Picard–Vessiot ring is given by $R = K\{X_{ij}, 1/\det X\}_{\Sigma_1}/I$, where I is a maximal Σ-ideal. By Proposition 2.11 and isomorphism (13), the ideal $L\otimes_K I$ corresponds to a Σ-ideal of the form $L\otimes_C J$, where J is a Σ_1-ideal of $C\{Y_{ij}, 1/\det Y\}_{\Sigma_1}$. This induces a Σ-isomorphism

$$\phi : L\otimes_K R \to L\otimes_C B,$$

where $B = C\{Y_{ij}, 1/\det C\}_{\Sigma_1}/J$ consists of σ-constants. Let $\mathfrak{m}$ be a maximal Σ-ideal in B. By [30, Proposition 14], we have

$$\gamma : B \to B/\mathfrak{m} \cong C,$$

since C is a Σ_1-closed pseudofield. Let φ be the Σ-homomorphism defined by

$$R \xrightarrow{r\mapsto 1\otimes r} L\otimes_K R \xrightarrow{\phi} L\otimes_C B \xrightarrow{\mathrm{id}_L\otimes\gamma} L\otimes_C C \xrightarrow{l\otimes c\mapsto l\cdot c} L.$$

Since R is Σ-simple, the homomorphism φ is injective. By the universal property, φ extends to a Σ-embedding $\overline{\varphi}$ of $\mathrm{Qt}(R)$ into L. Since L is generated by the entries of its fundamental matrix F, we finally conclude that $\overline{\varphi}(\mathrm{Qt}(R)) = L$. □

3.3 Difference algebraic groups

3.3.1 Definitions

In analogy with differential algebraic groups [8, 9], we make the following definitions. Throughout, C will denote a Σ_1-closed pseudofield. Recall that for $E \subseteq C\{y_1,\ldots,y_n\}_{\Sigma_1}$, the set $\mathbb{V}(E)$ is the set of all common zeroes for elements of E in C^n. The sets of the form $\mathbb{V}(E)$, for some E, are called C-Σ_1-algebraic varieties (also called pseudovarieties in [30]).

Also recall that, for an arbitrary C-Σ_1-algebraic variety X, the set of all difference polynomials vanishing on X will be denoted by $\mathbb{I}(X)$. Every difference polynomial defines a polynomial function on X. The ring of all polynomial functions, thus, coincides with $C\{y_1,\ldots,y_n\}_{\Sigma_1}/\mathbb{I}(X)$.

Definition 3.8. A regular map $f\colon X \to Y$ of C-Σ_1-algebraic varieties is a map given by difference polynomials in coordinates (for a general definition see [30, Section 4.6], in particular, Theorem 40 there).

Definition 3.9. A C-Σ_1-algebraic group is a group supplied with a structure of a C-Σ_1-algebraic variety such that the multiplication and inverse maps are regular.

Definition 3.10. A C-Σ_1-Hopf algebra is a C-Σ_1-algebra H supplied with comultiplication, counit, and antipode morphisms that are all C-Σ_1-algebra morphisms.

Note that the ring of polynomial functions of a C-Σ_1-algebraic variety is a reduced Hopf algebra such that the comultiplication, antipod, and counit are homomorphisms of C-Σ_1-algebras.

An example of a C-Σ_1-algebraic group is the group $\mathrm{GL}_{m,\Sigma_1}(C)$, that is the set of all $m\times m$ matrices with coefficients in C and having invertible determinant. The corresponding ring of regular functions is

$$H_m = C\{x_{11},\ldots,x_{mm},1/\det X\}_{\Sigma_1}.$$

The C-Σ_1-algebra H_m has a Hopf algebra structure defined on the Σ_1-generators in the usual way and is extended by commuting to the Σ_1-monomials in the generators.

Example 3.11. Let us describe the structure of $\mathrm{GL}_{1,\Sigma_1}(C)$ explicitly. Let

$$\Sigma_1 = \left\{\mathrm{id},\rho,\rho^2,\ldots,\rho^{t-1}\right\}$$

and consider

$$H_1 = C\{x,1/x\}_{\Sigma_1} = C\left[x,1/x,\rho(x),1/\rho(x),\ldots,\rho^{t-1}(x),1/\rho^{t-1}(x)\right].$$

Then, the comultiplication is

$$\rho^l(x)\mapsto\rho^l(x)\otimes\rho^l(x),$$

and the antipode map is

$$\rho^l(x)\mapsto 1/\rho^l(x).$$

Since C is Σ_1-closed, it is of the form $F_{\Sigma_1}(K)$ for some algebraically closed field K. Then the group $\mathrm{GL}_{1,\Sigma_1}(C)$ has a natural structure of a K-algebraic group such that

$$\mathrm{GL}_{1,\Sigma_1}(C) = \mathrm{GL}_1(K)^t.$$

Definition 3.12. A linear C-Σ_1-algebraic group is a closed subgroup in $\mathrm{GL}_{m,\Sigma_1}(C)$, that is a subgroup given by difference polynomials.

In particular, this means that the C-Σ_1-Hopf algebra H of a linear C-Σ_1-algebraic group is a quotient of H_m by a radical Σ_1-Hopf-ideal. More explicitly, the above equivalence also follows from the equivalence of the categories of affine pseudovarieties and the category of reduced Σ_1-finitely generated algebras [30, Proposition 42].

3.3.2 Difference algebraic subgroups of $\mathbb{G}_{m,\Sigma_1}$

Example 3.13. In the usual case of varieties over a field $\mathbf{k}$, the algebraic subgroups of $\mathbb{G}_m$ are given by equations $x^l = 1$. The corresponding ideal of $\mathbf{k}\left[x,x^{-1}\right]$ is (x^l-1). In the case of C-Σ_1-groups, where

$$\Sigma_1 = \mathbb{Z}/t_1\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}/t_p\mathbb{Z} =: \{\mathrm{id}=\alpha_1,\ldots,\alpha_t\},\quad t := t_1\cdot\ldots\cdot t_p,$$

there are more Σ_1-algebraic subgroups of $\mathbb{G}_{m,\Sigma_1}$. Let C be an arbitrary Noetherian Σ_1-pseudofield. Let also $\{e_0,\ldots,e_{s-1}\}$ be all indecomposable idempotents of C with $\alpha_i(e_0) = e_{i-1}$, $1\leqslant i\leqslant s$. Then the Σ_1-Hopf algebra of $\mathbb{G}_{m,\Sigma_1}$ is

$$C\{x,1/x\}_{\Sigma_1} = (K\times\ldots\times K)[x_\alpha,1/x_\alpha\,|\,\alpha\in\Sigma_1],$$

where $K = C/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$ of C. We have

$$\begin{aligned} C\{x,1/x\}_{\Sigma_1} &= e_0C\{x,1/x\}_{\Sigma_1} \times \ldots \times e_{s-1}C\{x,1/x\}_{\Sigma_1}, \\ R_i = e_iC\{x,1/x\}_{\Sigma_1} &= K[x_\alpha, 1/x_\alpha \mid \alpha \in \Sigma_1]. \end{aligned}$$

As we can see, each R_i is a Hopf algebra. Let I be the Σ_1-ideal defining our Σ_1-closed subgroup of $\mathbb{G}_{m,\Sigma_1}$. Then,

$$I = e_0I \times \ldots \times e_{s-1}I.$$

For each i, $0 \leqslant i \leqslant s-1$, the ideal $e_iI \subset R_i$ is defined by equations

$$\begin{gathered} x_{\alpha_1}^{k_{i,1,\alpha_1}} \cdot \ldots \cdot x_{\alpha_t}^{k_{i,1,\alpha_t}} = 1, \\ \vdots \\ x_{\alpha_1}^{k_{i,m,\alpha_1}} \cdot \ldots \cdot x_{\alpha_t}^{k_{i,m,\alpha_t}} = 1. \end{gathered}$$

So, if we collect all equations of all ideals e_iI, $0 \leqslant i \leqslant s-1$, we obtain the equations

$$\begin{array}{rcl} e_0x^{k_{0,1,1}}\alpha_2\left(x^{k_{0,1,2}}\right) \cdot \ldots \cdot \alpha_t\left(x^{k_{0,1,t}}\right) & = & e_0, \\ & \vdots & \\ e_{s-1}x^{k_{s-1,m,1}}\alpha_2\left(x^{k_{s-1,m,2}}\right) \cdot \ldots \cdot \alpha_t\left(x^{k_{s-1,m,t}}\right) & = & e_{s-1}. \end{array}$$

Applying α_i^{-1} to the equations with e_i, $0 \leqslant i \leqslant s$, we can rewrite the above system in the form

$$\begin{array}{rcl} e_0x^{k_{1,1}}\alpha_2\left(x^{k_{1,2}}\right) \cdot \ldots \cdot \alpha_t\left(x^{k_{1,t}}\right) & = & e_0, \\ & \vdots & \\ e_0x^{k_{m,1}}\alpha_2\left(x^{k_{m,2}}\right) \cdot \ldots \cdot \alpha_t\left(x^{k_{m,t}}\right) & = & e_0, \end{array} \tag{14}$$

which generate I as a Σ_1-ideal. The latter equations also give generators of the ideal e_0I. So, by [33, Section 2.2] we must have $m \leqslant t$.

Now we claim that there is an equation in I of the form $\varphi(x) - 1 = 0$, where $\varphi(xy) = \varphi(x)\varphi(y)$. Indeed, for this, denote the first equation in (14) by $\psi(x) - e_0$. Then, the equation

$$\sum_{1 \leqslant k \leqslant s} \alpha_k(\psi(x) - e_0) = \sum_{1 \leqslant k \leqslant s} \alpha_k(\psi(x)) - 1.$$

is of the desired form, where the sum $\sum_{1 \leqslant k \leqslant s} \alpha_k(\psi(x))$ is multiplicative because the e_i's are orthogonal.

Now suppose that $s = t$ (this is the case, for example, when C is Σ_1-closed). In this case, we know that the number m of equations does not exceed the number s of our idempotents. Then the following system defines the ideal I.

$$e_0 x^{k_{1,1}} \alpha_2(x^{k_{1,2}}) \cdot \ldots \cdot \alpha_t(x^{k_{1,t}}) = e_0, \tag{1}$$

$$\vdots$$

$$e_0 x^{k_{m,1}} \alpha_2(x^{k_{m,2}}) \cdot \ldots \cdot \alpha_t(x^{k_{m,t}}) = e_0, \tag{m}$$

$$e_0 = e_0, \tag{m+1}$$

$$\vdots$$

$$e_0 = e_0. \tag{t}$$

Applying α_i to the ith equation, $1 \leqslant i \leqslant t$, we obtain

$$e_0 x^{k_{1,1}} \alpha_2(x^{k_{1,2}}) \cdot \ldots \cdot \alpha_t(x^{k_{1,t}}) = e_0, \tag{1}$$

$$\vdots$$

$$e_{m-1}\alpha_m(x^{k_{m,1}})(\alpha_m\alpha_2)(x^{k_{m,2}}) \cdot \ldots \cdot (\alpha_m\alpha_t)(x^{k_{m,t-1}}) = e_{m-1}, \tag{m}$$

$$e_m = e_m, \tag{m+1}$$

$$\vdots$$

$$e_{t-1} = e_{t-1}. \tag{t}$$

By taking the sum of the above equations, we arrive at an equation of the form

$$\varphi(x) = 1. \tag{15}$$

Since the e_i's are orthogonal, the left-hand side is multiplicative. Moreover, this equation defines the same subgroup. Vice versa, every multiplicative $\varphi(x) \in C\{x, 1/x\}_{\Sigma_1}$ defines a Σ_1-subgroup of $\mathbb{G}_{m,\Sigma_1}$ via (15). Note that it might happen that the set of solutions is empty. For example, this is the case for $\varphi = e$, where e is idempotent and not equal to 1.

Example 3.14. Let $C = \mathbb{C} \times \mathbb{C} \times \mathbb{C}$ with $\rho(a_0, a_1, a_2) = (a_2, a_0, a_1)$, $a_i \in \mathbb{C}$. By [30, Proposition 15], (C, ρ) is a Σ_1-closed pseudofield. Let

$$G = \{a \in C \,|\, a \cdot \rho(a) = 1\}, \tag{16}$$

a Σ_1-subgroup of $\mathbb{G}_m$ considered in Example 3.13. A calculation shows that $G = \{(1,1,1), (-1,-1,-1)\}$. This demonstrates a major difference between Σ_1-subgroups and differential algebraic subgroups (see [8, Chapter IV]) of $\mathbb{G}_m$. More precisely, in the differential case the order of the defining equation coincides with the algebraic dimension of the subgroup.

In our case, the order of ρ in (16) is equal to 1, however, the group is finite. Therefore, in order to compute the algebraic dimension of a Σ_1-group one needs to do more calculation than just to look at the ρ-order of the equation.

3.4 Galois group

As before, let K be a Noetherian Σ-pseudofield with $C := K^\sigma$ being Σ_1-closed.

Definition 3.15. Let L be a Picard–Vessiot pseudofield of equation (12). Then the group of Σ-automorphisms of L over K is called the difference Galois group of (12) and denoted by $\mathrm{Aut}_\Sigma(L/K)$.

Let L be a Picard–Vessiot pseudofield of equation (12) and $F \in \mathrm{GL}_n(L)$ be a fundamental matrix. Then for any $\gamma \in \mathrm{Aut}_\Sigma(L/K)$ we have

$$\gamma(F) = FM_\gamma, \tag{17}$$

where $M_\gamma \in \mathrm{GL}_n(C)$, which, as usual, defines an injective group homomorphism from $\mathrm{Aut}_\Sigma(L/K)$ into $\mathrm{GL}_n(C)$. Since L is generated by the entries of F, the action of γ on L is determined by its action on F. This induces an identification of $\mathrm{Aut}_\Sigma(L/K)$ with $\mathrm{Aut}_\Sigma(R/K)$, where R is the Picard–Vessiot ring corresponding to F.

We will now construct a map $\mathrm{Aut}_\Sigma(R/K) \to \mathrm{Max}_\Sigma(R \otimes_K R)$, the maximal Σ-ideals of $R \otimes_K R$. For this, let F be a fundamental matrix of equation (12) with entries in R and $\gamma \in \mathrm{Aut}_\Sigma(R/K)$. As above, $\gamma F = FM_\gamma$, where $M_\gamma \in \mathrm{GL}_n(C)$. We will then map

$$\gamma \mapsto [F \otimes 1 - 1 \otimes FM_\gamma]_\Sigma,$$

the smallest Σ-ideal containing $F \otimes 1 - 1 \otimes FM_\gamma$. Since R is Σ-simple, the kernel of the surjective Σ-homomorphism

$$(\gamma, \mathrm{Id})\colon R \otimes_K R \to R,$$

which is $[F \otimes 1 - 1 \otimes FM_\gamma]_\Sigma$, is a maximal Σ-ideal in $R \otimes_K R$.

To construct a map in the reverse direction, let

$$\phi_1, \phi_2 : R \to R \otimes_K R,$$

with $r \mapsto r \otimes 1$ and $r \mapsto 1 \otimes r$, respectively. Let $\mathfrak{m}$ be a maximal Σ-ideal of $R \otimes_K R$. Then, $(R \otimes_K R)/\mathfrak{m}$ is a Picard–Vessiot ring of equation (12). As in Proposition 3.4, the composition homomorphisms

$$\overline{\phi}_i : R \to R \otimes_K R \to (R \otimes_K R)/\mathfrak{m}$$

are isomorphisms. This induces an automorphism of the ring R defined by

$$\phi_{\mathfrak{m}} := \overline{\phi}_2^{-1} \circ \overline{\phi}_1.$$

Proposition 3.16. *The correspondence* $\mathrm{Aut}_\Sigma(R/K) \to \mathrm{Max}_\Sigma(R \otimes_K R)$ *constructed above is bijective. Moreover, these bijections are inverses of each other.*

Proof. Let $\gamma \in \mathrm{Aut}_\Sigma(R/K)$ and $M \in \mathrm{GL}_n(C)$ be such that $\gamma(F) = FM$. Set $\mathfrak{m} = [F \otimes 1 - 1 \otimes FM]_\Sigma$. Since

$$\overline{\phi}_1(F) = F \otimes 1, \quad F \otimes 1 = 1 \otimes FM \text{ in } (R \otimes_K R)/\mathfrak{m}, \text{ and } \overline{\phi}_2(FM) = 1 \otimes FM,$$

we have $\phi_\mathfrak{m}(F) = FM$.

Conversely, let $\mathfrak{m} \in \mathrm{Max}_\Sigma(R \otimes_K R)$. Then $\phi_\mathfrak{m}(F) = FM$ for some $M \in \mathrm{GL}_n(C)$. Hence,

$$\overline{\phi}_1(F) = \overline{\phi}_2(FM).$$

Thus,

$$[F \otimes 1 - 1 \otimes FM]_\Sigma \subset \mathfrak{m}.$$

Since, as above, the former ideal is Σ-maximal, it coincides with $\mathfrak{m}$. □

Proposition 3.17. *The Galois group G of equation (12) is a closed subgroup of $\mathrm{GL}_n(C)$. Moreover, if the ring $R \otimes_K R$ is reduced, then*

$$R \otimes_K R \cong R \otimes_C C\{G\},$$

where $C\{G\}$ is the ring of regular functions on G and R is a Picard–Vessiot ring of (12).

Proof. As before, define σ on the Σ_1-ring $R\{X_{ij}, 1/\det X\}_{\Sigma_1}$ by $\sigma X = AX$. Let F be a fundamental matrix of (12) with coefficients in R and let, as above, $Y = F^{-1}X$, which implies that $\sigma Y = Y$. We have a Σ-isomorphism

$$R \otimes_K K\{X_{ij}, 1/\det X\}_{\Sigma_1} \cong R \otimes_C C\{Y_{ij}, 1/\det Y\}_{\Sigma_1}.$$

As in the proof of Proposition 3.7, this induces a Σ-isomorphism

$$R \otimes_K R \cong R \otimes_C B, \tag{18}$$

where $B = C\{Y_{ij}, 1/\det Y\}_{\Sigma_1}/J$ and J is a Σ_1-ideal.

By Proposition 3.16, $\mathrm{Aut}_\Sigma(R/K)$ as a set can be identified with $\mathrm{Max}_\Sigma(R \otimes_K R)$. The latter set, by Proposition 2.11 and isomorphism (18), can be identified with $\mathrm{Max}_{\Sigma_1} B$. Since C is Σ_1-closed, by [30, Proposition 14], the set $\mathrm{Max}_{\Sigma_1} B$ can be identified with a closed subset of $\mathrm{GL}_n(C)$. The group structure of G is preserved under this identification due to (17). If the ring $R \otimes_K R$ is reduced, then the ideal J is radical and, therefore, B is the coordinate ring of G. □

3.5 Galois correspondence

Proposition 3.18. *Let L be a Picard–Vessiot pseudofield of equation (12), R be its Picard–Vessiot ring, and G be its Galois group. If the ring $R \otimes_K R$ is reduced, then $L^G = K$.*

Proof. Let
$$a/b \in L \setminus K, \tag{19}$$
where a, $b \in R$ and b is not a zero divisor. Set
$$d = a \otimes b - b \otimes a \in R \otimes_K R.$$
We will show that $d \neq 0$. For this, let $\{e_1, \ldots, e_n\}$ be all indecomposable idempotents of the Noetherian Σ-pseudofield K. Since b is not a zero divisor,
$$e_i \cdot b \neq 0, \quad 1 \leqslant i \leqslant n. \tag{20}$$
Suppose that for each i, $1 \leqslant i \leqslant n$, $e_i \cdot a$ and $e_i \cdot b$ are linearly dependent over e_iK, that is, $\lambda_i \cdot e_i \cdot a = \mu_i \cdot e_i \cdot b$ for all i. Then (20) implies that $\lambda_i \neq 0$, $1 \leqslant i \leqslant n$. Since e_iK is a field, we have $e_i \cdot a = e_i \cdot b \cdot \mu_i/\lambda_i$. Hence,
$$a = \sum_{i=1}^{n} e_i a = \left(\sum_{i=1}^{n} \frac{\mu_i}{\lambda_i} e_i\right) b, \quad \text{that is,} \quad \frac{a}{b} = \sum_{i=1}^{n} \frac{\mu_i}{\lambda_i} e_i \in K,$$
which is a contradiction to (19). Therefore, there exists i, $1 \leqslant i \leqslant n$, such that $e_i \cdot a$ and $e_i \cdot b$ are linearly independent over e_iK. Then,
$$e_i \cdot a \otimes e_i \cdot b - e_i \cdot b \otimes e_i \cdot a \neq 0$$
in $e_iR \otimes_{e_iK} e_iR$. Hence,
$$a \otimes b - b \otimes a \neq 0 \quad \text{in} \quad R \otimes_K R.$$
We will now show that there is a maximal Σ-ideal in $R \otimes_K R$ that does not contain d. Since $R \otimes_K R$ is reduced, then by Proposition 3.17 we have $R \otimes_K R \cong R \otimes_C C\{G\}$. Let $\{l_i\}_{i \in I}$ be a basis of R over K. Then there exist $r_1, \ldots, r_m \in C\{G\}$ such that
$$d = l_1 \otimes r_1 + \ldots l_m \otimes r_m.$$
Since r_1 is not nilpotent, there exists a maximal Σ_1-ideal $\mathfrak{m} \subset C\{G\}$ such that $\overline{r}_1 \neq 0$ in $C\{G\}/\mathfrak{m}$. Then image of d in $R \otimes_C C\{G\}/\mathfrak{m} \cong R$ is
$$\overline{d} = l_1 \overline{r}_1 + \ldots + l_m \overline{r}_m.$$
Since $\overline{r}_1 \neq 0$, we have $\overline{d} \neq 0$. Thus, $d \notin R \otimes_C \mathfrak{m}$. Using the correspondence between maximal Σ-ideals in $R \otimes_K R$ and Σ-automorphisms of R over K, let
$$\phi_{\mathfrak{m}} = \overline{\phi}_2^{-1} \circ \overline{\phi}_1$$
correspond to $\mathfrak{m}$ as in the proof of Proposition 3.16. Then our choice of $\mathfrak{m}$ implies that
$$(R \otimes_K R)/\mathfrak{m} \ni \overline{\phi}_1(a)\overline{\phi}_2(b) - \overline{\phi}_1(b)\overline{\phi}_2(a) \neq 0. \tag{21}$$
Applying $\overline{\phi}_2^{-1}$ to both sides of (21), we obtain that $\phi_{\mathfrak{m}}(a)b - \phi_{\mathfrak{m}}(b)a \neq 0$. Therefore, $\phi_{\mathfrak{m}}\left(\frac{a}{b}\right) \neq \frac{a}{b}$. $\square$

Lemma 3.19. *Let $K \subset L$ be Noetherian Σ-pseudofields. Let $H \subset \mathrm{Aut}_\Sigma(L)$ such that $L^H = K$. Suppose that $K \cong \prod_{i=1}^n F_{\Sigma_1}(F)$ as Σ_1-rings, where F is a field. Let $\{e_i\}$ be the corresponding idempotents. Then for each i the abstract group generated by Σ_1 and H acts transitively on the set of indecomposable idempotents of the ring e_iL.*

Proof. Let $e \in e_iL$ be an idempotent and S be its $\Sigma_1 * H$-orbit. The set S coincides with the set of indecomposable idempotents if and only if $\sum_{f\in S} f = 1$. This sum is H-invariant and, therefore, it belongs to $F_{\Sigma_1}(F)$. Since it is Σ_1-invariant as well, it is equal to 1, because a Σ_1-invariant idempotent of $F_{\Sigma_1}(F)$ generates a Σ_1-ideal. □

Proposition 3.20. *Let L be a Picard–Vessiot pseudofield for equation (12) and H be a closed subgroup of the Galois group G. Then $L^H = K$ implies $H = G$.*

Proof. As before, let F be a fundamental matrix with entries in L and $\sigma X = AX$ define the action of Σ on the Σ_1-ring $D := L\{X_{ij}, 1/\det X\}_{\Sigma_1}$. Let also $Y = F^{-1}X$. Again, as before,

$$L \otimes_K K\{X_{ij}, 1/\det X\}_{\Sigma_1} \cong L \otimes_C C\{Y_{ij}, 1/\det Y\}_{\Sigma_1}.$$

Suppose that $H \subsetneq G$ and let $I \subsetneq J$ be the defining ideals of G and H, respectively. Denote their extensions to $L\{X_{ij}, 1/\det X\}$ by (I) and (J), respectively. By Proposition 2.11, we have $(I) \subsetneq (J)$. Explicitly, we have

$$(I) = \left\{ f(X) \in L\{X_{ij}, 1/\det X\}_{\Sigma_1} \mid f(FM) = 0 \text{ for all } M \in G \right\}$$

and

$$(J) = \left\{ f(X) \in L\{X_{ij}, 1/\det X\}_{\Sigma_1} \mid f(FM) = 0 \text{ for all } M \in H \right\}. \tag{22}$$

Let $T = (J) \setminus (I) \neq \varnothing$. Define the action of H on $L \otimes_K K\{X_{ij}, 1/\det X\}_{\Sigma_1}$ by

$$h(a \otimes b) = h(a) \otimes b, \quad h \in H.$$

Then, equality (22) implies that (J) is stable under this action of H. By Proposition 2.19,

$$K \cong F_{\Sigma_1}(F) \times \ldots \times F_{\Sigma_1}(F)$$

as Σ_1-rings, where F is a field. Let $e_1, \ldots, e_n$ be the idempotents corresponding to the components $F_{\Sigma_1}(F)$ in the above product. By Proposition 2.10, the ring $K\{X_{ij}, 1/\det X\}_{\Sigma_1}$ has a Σ_1-invariant basis $\{Q_\alpha\}$. Then every element of the ring D is of the form

$$Q = q_1 Q_{\alpha_1} + \ldots + q_n Q_{\alpha_n}, \tag{23}$$

where $q_i \in L$, $1 \leqslant i \leqslant n$. Let Q be an element in T with the shortest presentation of the form (23). Since $Q = \sum_i e_i Q$, there exists i such that $e_i Q \in T$. Denote the latter polynomial by Q as well. Now, we have $Q \in e_i D$. Let $\{f_1, \ldots, f_m\}$ be all indecomposable idempotents of the Noetherian ring e_iL. Then,

$$Q = \sum\nolimits_{j=1}^m f_j Q.$$

Hence, there exists j such that $f_jQ \in T$. By Lemma 3.19, there exist $h_t \in \Sigma_1 * H$ such that the coefficients of

$$Q' := \sum_t h_t(Q)$$

are invertible in e_iL. Therefore,

$$Q' = e_iQ_1 + g_2Q_2 + \ldots + g_mQ_m.$$

Since the ideal (J) is stable under the action of $\Sigma_1 * H$, we have $Q' \in T$. Since $e_i \in K$, for every $h \in H$ the polynomial $Q''_h := Q' - h(Q')$ has a shorter presentation than Q and, therefore, $Q''_h \notin T$. That is,

$$Q''_h \in (I) \quad \text{for all} \quad h \in H. \tag{24}$$

We will show now that $Q''_h = 0$ for all $h \in H$. Suppose that $Q''_h \neq 0$ for some $h \in H$. Then (24) implies that there exists j such that $0 \neq f_jQ''_h \in (I)$. Since $\Sigma_1 * H$ acts transitively on the indecomposable idempotents of e_iL, there exist $\phi_t \in \Sigma_1 * H$ such that

$$\overline{Q}_h := \sum_t \phi_t\left(Q''_h\right) = r_2Q_2 + \ldots + r_mQ_m \in (I),$$

where r_2 is invertible in e_iL. Therefore, there exists $r \in e_iL$ such that $g_2 = rr_2$. Then, the polynomial $Q' - r\overline{Q} \in T$ has a shorter presentation than Q', which is a contradiction. We have shown that $h(Q') = Q'$ for all $h \in H$. Hence, all coefficients of Q' are in K and, therefore, are invariant under the action of G as well. Since $0 = Q'(F \cdot \mathrm{id}) = Q'(F)$, we have

$$0 = g(Q'(F)) = g(Q')(FM_g) = Q'(FM_g)$$

for all $g \in G$. Thus, $Q' \in (I)$, which contradicts to $Q' \in T$. $\square$

Lemma 3.21. *Let M be a field,*

$$D := M \times \ldots \times M, \tag{25}$$

$F \subset D$ be a subfield and $H \subset \mathrm{Aut}(D)$ with $D^H = F$. Let $f := (1,0,\ldots,0) \in D$ and $H_1 \subset H$ be the stabilizer of f. Then, $fF = M^{H_1}$, where M is from the first component in (25).

Proof. Since fF is H_1-invariant, we have $fF \subseteq M^{H_1}$. We will show the reverse inclusion. Let $l \in (fD)^{H_1} = M^{H_1}$. We need to show that there is an element $a \in F$ such that $l = fa$. Let the H-orbit of l be $\{l_1,\ldots,l_k\}$, where $l = l_1$. For each i, $1 \leqslant i \leqslant k$, there exists $a_i \in D$ such that $l_i = a_if_i$, where f_i is the idempotent corresponding to the ith factor in D (so we have $f = f_1$), since if $l \neq 0$, then H_1 is the stabilizer of l. Hence, for $d = \sum_{i=1}^k l_i$ we have

$$fd = \sum_{i=1}^k f_1l_i = l_1 = l$$

and H permutes the l_i's. Thus, $d \in D^H = F$ as desired. $\square$

Proposition 3.22. *Let K be a Noetherian Σ-pseudofield, R be a Σ-simple Noetherian algebra over K, and $L = \mathrm{Qt}(R)$. Then for the statements*

1. *the ring $R \otimes_K R$ is reduced,*
2. *the ring $L \otimes_K L$ is reduced,*
3. *there exists a subgroup $H \subset \mathrm{Aut}_\Sigma(L/K)$ such that $L^H = K$,*

we have: (1) is equivalent to (2) and (3) implies (2). Moreover, if R is a Picard–Vessiot ring over K, then the above statements are equivalent.

Proof. The equivalence of (1) and (2) follows from the fact that $R \otimes_K R \subset L \otimes_K L$ and that the latter ring is a localization of the former one. We will show that (3) implies (2). Let $\{e_1,\ldots,e_n\}$ be the indecomposable idempotents of K. Then,

$$L \otimes_K L = \prod_{i=1}^{n} e_i L \otimes_{e_i K} e_i L.$$

It is enough to show that the ring $e_i L \otimes_{e_i K} e_i L$ is reduced. Note that $e_i K$ is a field. Since $e_i \in K$, they are all invariant under H and, moreover, $(e_i L)^H = e_i K$. Let now $\{f_1,\ldots,f_m\}$ be the indecomposable idempotents of the ring $e_i L$ and let H_1 be the stabilizer of f_1. Lemma 3.21 with $D = e_i L$ and $F = e_i K$ implies that

$$(e_i f_1 L)^{H_1} = f_1 e_i K.$$

Since

$$e_i L \otimes_{e_i K} e_i L = \prod_{s,t} e_i f_s L \otimes_{e_i K} e_i f_t L,$$

it remains to show that the ring

$$D := e_i f_s L \otimes_{e_i K} e_i f_t L$$

is reduced. By [6, Corollary 1, §7, no. 2], with $A = e_i f_s L$, $B = e_i f_t L$, $N = B$, and $K = e_i K$, the Jacobson radical of the ring D is zero. In particular, the ring D is reduced.

The last statement follows from Proposition 3.18. □

Definition 3.23. A Picard–Vessiot extension L/K is called separable if one of the three equivalent conditions in Proposition 3.22 is satisfied.

Theorem 3.24. *Let R be a Picard–Vessiot ring of equation (12) and $L = \mathrm{Qt}(R)$ be separable over K. Let $\mathcal{F}$ denote the set of all intermediate Σ-pseudofields F such that L is separable over K and $\mathcal{G}$ denote the set of all Σ_1-closed subgroups H in the Galois group G of L over K. Then the correspondence*

$$\mathcal{F} \longleftrightarrow \mathcal{G}, \quad F \mapsto \mathrm{Aut}_\Sigma(L/F), \quad H \mapsto L^H$$

is bijective and the above maps are inverses of each other. Moreover, H is normal in G if and only if the Σ-pseudofield $F := L^H$ is G-invariant.

Proof. The map $\mathcal{F} \longrightarrow \mathcal{G}$ is well-defined by Proposition 3.17. Propositions 2.8 and 2.9 imply that $L^H \subset L$ is a Σ-pseudofield. By Proposition 2.20, it is Noetherian and, by Proposition 3.22, it is separable.

Let $F \in \mathcal{F}$. Then the extension L over F is separable and is a Picard–Vessiot pseudofield for equation (12) considered over F. Moreover, $F = F^{\mathrm{Aut}_\Sigma(L/F)}$ by Proposition 3.18. Conversely, let H be a Σ_1-closed subgroup of G. Set $F = L^H$. Then L is a Picard–Vessiot pseudofield for equation (12) over F. By Proposition 3.20, we have $H = \mathrm{Aut}_\Sigma(L/F)$. The equality

$$g(F) = \left\{r \in L \,|\, ghg^{-1}r = r \text{ for all } h \in H\right\}$$

implies the statement about normality. □

Remark 3.25. The base pseudofield K is a product of the fields, say $L \times \ldots \times L$. If the field L is perfect, then for every pseudofields F and E containing K the ring $F \otimes_K E$ is reduced. Indeed, let $e_0, \ldots, e_{t-1}$ be all indecomposable idempotents of K, then

$$F \otimes_K E = \prod_{i=0}^{t-1} e_i F \otimes_L e_i E.$$

Since L is perfect and L-algebras e_iF and e_iE are reduced, then $e_iF \otimes_L e_iE$ is reduced as well (see [7, A.V. 119, No. 5, Théorèm 3(d)]). Therefore, if L is perfect, then any Picard–Vessiot extension is separable. If the field L is finite, algebraically closed or of characteristic zero, then L is perfect. In this case, the set $\mathcal{F}$ contains all intermediate Σ-pseudofields.

3.6 Extension to non-faithful action

In the introduction, we alluded to the fact that some of our results could instead be obtained via faithfully flat descent [26]. However, this requires the additional assumption[2] that Σ_1 acts faithfully in the setup for faithfully flat descent. The theory we have developed in this paper works more generally, as we now illustrate. Let L be a field, $\Sigma_1 = \mathbb{Z}/4\mathbb{Z}$, and ρ be a generator. Suppose that Σ_1 acts on L faithfully and $K = L^{\rho^2}$. Then

$$\mathrm{Aut}^\rho(L/K) \cong \mathbb{Z}/2\mathbb{Z} \quad \text{but} \quad \mathrm{Aut}\left(L^{\Sigma_1}/K^{\Sigma_1}\right) = \{1\},$$

where Aut^ρ is the set of ρ-automorphisms (so, we also have to store the order of ρ – not only the field of invariants). Roughly speaking, replacing a difference object by a non-difference one, we cannot recover the group of difference automorphisms. This example (where L is a Picard–Vessiot extension and K is a base field) appears naturally in the Picard–Vessiot theory if, for instance, the initial field contains only ρ-constants. Also note that if we replace L by L^{Σ_1}, then the σ-constants of L^{Σ_1} are not necessarily algebraically closed.

[2] We also assume this in Section 3, but it is only needed to guarantee the uniqueness of a parameterized PV-extension, which we do not use in the applications. It also implies the existence, but is only a sufficient condition, and there are situations when one does not have to make this assumption. The Galois correspondence in its Hopf-algebraic version does not need this as we show below.

Therefore, using descent, extra preparatory steps are required before we are able to apply the standard non-parametric difference Galois theory.

Here is another example in which it is preferable to consider not necessarily faithful actions of Σ_1. Let

$$L=\mathbb{C}(x),\quad \sigma(x)=2\cdot x,\ \rho(x)=-x,\quad K=\mathbb{C}\left(x^2\right),\quad \Sigma_1=\{\mathrm{id},\rho\}$$

and the difference equation be

$$\sigma(y)=2\cdot y. \tag{26}$$

There are no solutions of (26) in K and L is a Picard–Vessiot extension of the equation, on which Σ_1 acts faithfully, while the action of Σ_1 on K is trivial. Of course, the field L considered with the trivial action of ρ is also a Picard–Vessiot extension, but restricting to this would not allow us to consider more interesting and useful cases outlined in this example. We will show how one can generalize our results to include non-faithful actions of Σ_1.

Theorem 3.26 ((Instead of Theorem 3.24))**.** *Let R be a Picard–Vessiot ring over a pseudofield K with the corresponding Σ_1-Hopf-algebra H (which replaces the Galois group – see [3, Section 2]) and $L=\mathrm{Qt}(R)$ be the pseudofield of fractions. Let $\mathcal{F}$ denote the set of all intermediate Σ-pseudofields and $\mathcal{G}$ denote the set of all Σ_1-Hopf-ideals in H. Then the correspondence*

$$\mathcal{G}\to\mathcal{F},\ I\mapsto L^I:=\{x\in L\,|\,1\otimes x-x\otimes 1\in I\cdot(L\otimes_K L)\}$$

is bijective. Moreover, I is normal in H if and only if the Σ-pseudofield L^I is H-invariant. A Σ_1-Hopf-ideal I is radical if and only if L is separable over L^I.

In order to prove this result, one extends the Hopf-algebraic approach given in [2]. The main technical results one uses are [2, Proposition 3.10] and

Proposition 3.27 ((Instead of Proposition 2.11))**.** *Let R be a Picard-Vessiot ring over K and*

$$R\otimes_K R\cong R\otimes_C H$$

be the torsor isomorphism for R, where H is a Σ_1-Hopf-algebra over Σ_1-pseudofield $C=R^\sigma$. Then this isomorphism induces a $1-1$ correspondence between Σ_1-Hopf-ideals of H and Σ-coideals of $R\otimes_K R$. That is, if $I\subseteq R\otimes_K R$ is a Σ-coideal, then $I\cap H$ is a Σ_1-Hopf-ideal; if $\mathfrak{a}$ is a Σ_1-Hopf-ideal, then $R\otimes_C\mathfrak{a}$ is a Σ-coideal.

From the Hopf-algebraic point of view, the Galois correspondence can be derived from Theorem 3.26 above using the following result:

Theorem 3.28. *Let H be a reduced Σ_1-Hopf-algebra over a difference closed pseudofield K. Then H induces a functor F from the category of Σ_1-K-algebras to the category of groups by the rule*

$$F(R)=\hom_{\Sigma_1-K}(H,R).$$

Then H can be recovered from $F(K)$.

3.7 Torsors

Let C be a Σ_1-closed pseudofield and $K \supset C$ be a Noetherian Σ-pseudofield. Let G be a Σ_1-group over C be $C\{G\}$ be its Σ_1-Hopf algebra with comultiplication Δ, antipode S, and counit ε.

Definition 3.29. A Σ_1-finitely generated K-algebra R supplied with a Σ-K-algebra homomorphism

$$\nu^* : R \to R \otimes_C C\{G\}$$

is called a G-torsor over K if the following statements are true:

1. R is a $C\{G\}$-comodule with respect to ν^*,
2. the vertical arrow in the following diagram is an isomorphism:

$$\begin{tikzcd} & R \otimes_K R \arrow[d] & \\ R \arrow[ur, "\mathrm{id}_R \otimes 1"] \arrow[dr, "\nu^*"'] & & R \arrow[ul, "1 \otimes \mathrm{id}_R"'] \arrow[dl, "1 \otimes \mathrm{id}_R"] \\ & C\{G\} \otimes_C R & \end{tikzcd}$$

In the above notation, the rings R and $C\{G\}$ are finitely generated algebras over Artinian rings. Then the Krull dimension is defined for them, which we will denote by $\dim R$ and $\dim C\{G\}$, respectively. The isomorphism in (2) implies that $\dim R = \dim C\{G\}$. Moreover, let e be an indecomposable idempotent in C and $F := eC$ be the corresponding residue field. Then $F \otimes_C C\{G\}$ is a finitely generate F-algebra of dimension equal to $\dim C\{G\}$. Hence, for any minimal prime ideal $\mathfrak{p}$ of the ring $F \otimes_C C\{G\}$,

$$\operatorname{tr.deg.}_F \mathbf{k}(\mathfrak{p}) = \dim C\{G\} = \dim R,$$

where $\mathbf{k}(\mathfrak{p})$ is the residue field of $\mathfrak{p}$.

Proposition 3.30. *Let K be a Noetherian Σ-pseudofield with K^σ being a Σ_1-closed pseudofield. Let R be a Picard–Vessiot ring for equation (12) with $L = \mathrm{Qt}(R)$. Let G be the Galois group of L over K. If R is separable over K, then R is a G-torsor over K.*

Proof. Follows from Proposition 3.17. □

4 APPLICATIONS

We will start by giving a difference dependence statement in the spirit of [21], which we prove using our own methods. We then show how this is related to Jacobi's theta-function in Section 4.3 and demonstrate our applications in Section 4.4, in particular, in Theorem 4.9, which provides a very explicit difference dependence test.

4.1 General approach

For any nonzero complex number a we define an automorphism $\sigma_a : \mathbb{C}(z) \to \mathbb{C}(z)$ by

$$\sigma_a(f)(z) = f(az).$$

Let $\Sigma_1 \subseteq \mathbb{C}^*$ be a finite subgroup. Then Σ_1 is a cyclic group generated by a root of unity ζ of degree t. Let $q \in \mathbb{C}$ be a complex number such that $|q| > 1$. Now we have an action of the group $\Sigma = \mathbb{Z} \oplus \mathbb{Z}/t\mathbb{Z}$ on $\mathbb{C}(z)$, where the first summand is generated by σ_q and the second one is generated by σ_ζ. Throughout this section the ring $\mathbb{C}(z)$ is supplied with this structure of a Σ-ring.

Theorem 4.1. *Let R be a Σ-ring containing the field $\mathbb{C}(z)$ such that $\mathbf{k} := R^{\sigma_q}$ is a field. Suppose additionally that R contains the field $\mathbf{k}(z)$. Let $f \in R$ and $a \in \mathbb{C}(z)$ be such that f is an invertible solution of*

$$\sigma_q(f) = af. \tag{27}$$

Then f is σ_ζ-algebraically dependent over $\mathbf{k}(z)$ if and only if

$$\varphi(a) = \sigma_q(b)/b \tag{28}$$

for some $0 \neq b \in \mathbb{C}(z)$ and $1 \neq \varphi(x) = x^{n_0}\sigma_\zeta(x)^{n_1} \cdot \ldots \cdot \sigma_\zeta^{t-1}(x)^{n_{t-1}}$.

Proof. If (28) holds, then

$$\sigma_q(\varphi(f)/b) = \varphi(\sigma_q(f))/\sigma_q(b) = \varphi(af)/\sigma_q(b) = \varphi(a)\varphi(f)/\sigma_q(b) = \varphi(f)/b.$$

Therefore,

$$\varphi(f)/b = c \in R^{\sigma_q} = \mathbf{k}.$$

Thus, $\varphi(f) = c \cdot b \in \mathbf{k}(z)$, which gives a Σ_1-algebraic dependence for f over $\mathbf{k}(z)$. First, note that z is algebraically independent over $\mathbf{k}$. Indeed, suppose that there is a relation

$$a_n \cdot z^n + a_{n-1} \cdot z^{n-1} + \ldots + a_0 = 0$$

for some $a_i \in \mathbf{k}$. Applying σ_q n times, we obtain the following system of linear equations

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ q^n & q^{n-1} & \ldots & q & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (q^n)^n & (q^{n-1})^n & \ldots & q^n & 1 \end{pmatrix} \begin{pmatrix} a_n \cdot z^n \\ a_{n-1} \cdot z^{n-1} \\ \vdots \\ a_0 \end{pmatrix} = 0$$

Since the matrix is invertible, our relation is of the form $a \cdot z^k = 0$ for some $a \in \mathbf{k}$. Since $\mathbf{k}$ is a field, we have $z^k = 0$. However, $z \in \mathbb{C}(z)$, which is a contradiction.

Assume now that f is Σ_1-algebraically dependent over $\mathbf{k}(z)$. Let C be the Σ_1-closure of $\mathbf{k}$ and K be the total ring of fraction of the polynomial ring $C[z]$, where $\sigma_q(z) = qz$ and

$\sigma_\zeta(z) = \zeta z$. So, the field $\mathbf{k}(z)$ is naturally embedded into K. Let D be the smallest Σ-subring in R generated by $\mathbf{k}(z)$, f, and $1/f$ and let

$$\mathfrak{m} \subseteq K \otimes_{\mathbf{k}(z)} D$$

be a maximal Σ-ideal. Then,

$$L = \left(K \otimes_{\mathbf{k}(z)} D\right) / \mathfrak{m}$$

is a Picard–Vessiot ring over K for equation (27). The image of f in L will be denoted by $\bar{f}$. Since f is Σ_1-algebraically dependent over $\mathbf{k}(z)$, $\bar{f}$ is Σ_1-algebraically dependent over K.

It follows from Section 3.7 that $\bar{f}$ is Σ_1-algebraically dependent over K if and only the Σ-Galois group G of equation (27) is a proper subgroup of $\mathbb{G}_{m,\Sigma_1}$. Then, by Example 3.13, there exists a multiplicative

$$\varphi \in (F_{\Sigma_1}\mathbb{Q})\{x, 1/x\}_{\Sigma_1}$$

(see also (9)) such that G is given by the equation $\varphi(x) = 1$. Therefore, for all ϕ in the Galois group,

$$\phi(\varphi(\bar{f})) = \varphi(\phi(\bar{f})) = \varphi(c_\phi \cdot \bar{f}) = \varphi(c_\phi) \cdot \varphi(\bar{f}) = 1 \cdot \varphi(\bar{f}) = \varphi(\bar{f}).$$

Hence, by Proposition 3.18, we have

$$b := \varphi(\bar{f}) \in K = C(z),$$

as in [22, Proposition 3.1]. Since f is invertible, $\bar{f}$ is also invertible and, since φ is multiplicative, $\varphi(\bar{f})$ is invertible as well. Therefore,

$$\varphi(a) = \varphi\left(\sigma_q(\bar{f})/\bar{f}\right) = \sigma_q\left(\varphi(\bar{f})\right)/\varphi(\bar{f}) = \sigma_q(b)/b. \tag{29}$$

We will show now that b can be chosen from $(F_{\Sigma_1}\mathbb{C})(z)$ satisfying (28) as in [22, Corollary 3.2]. We have the equalities $a = \bar{a}/c$ and $b = \bar{b}/d$, where $\bar{a}, c \in \mathbb{C}[z]$ and $\bar{b}, d \in C[z]$. Consider the coefficients of $\bar{b}$ and d as difference indeterminates. Then, equation (29) can be considered as a system of equations in the coefficients of $\bar{b}$ and d. Indeed, equation (29) is equivalent to

$$\varphi(\bar{a}/c) = \sigma_q\left(\bar{b}/d\right)/\left(\bar{b}/d\right).$$

So, we have

$$\varphi(\bar{a}) \cdot \sigma_q(d) \cdot \bar{b} - \varphi(c) \cdot \sigma_q(\bar{b}) \cdot d = 0 \tag{30}$$

The left-hand side of equation (30) is a polynomial in z. The desired system of equations is given by the equalities for all coefficients. Now note that the condition of $y \in C[z]$ being invertible in $C(z)$ is given by the inequation

$$y \cdot \sigma_\zeta(y) \cdot \ldots \cdot \sigma_\zeta^{t-1}(y) \neq 0.$$

Therefore, the coefficients of the polynomials $\bar{b}$ and d are given by the system of equations and inequalities. Since the pseudofield $F_{\Sigma_1}\mathbb{C}$ is Σ_1-closed, existence of invertible $\bar{b}$ and d with coefficients in C implies existence of invertible $\bar{b}$ and d with coefficients in $F_{\Sigma_1}\mathbb{C}$ (see [30, Proposition 25 (3)]).

We will now show that $b \in \mathbb{C}(z)$ and φ can be found of the desired form. We have proven that

$$\varphi(a) = \sigma_q(b)/b \tag{31}$$

for some $b \in (F_{\Sigma_1}\mathbb{C})(z)$. It follows from Example 3.13 that

$$\begin{aligned}\varphi(x) =& e_0 \cdot x^{n_{0,0}} \cdot \sigma_\zeta(x)^{n_{0,1}} \cdot \ldots \cdot \sigma_\zeta^{t-1}(x)^{n_{0,t-1}} + \ldots + \\ &+ e_{t-1} \cdot x^{n_{t-1,0}} \cdot \sigma_\zeta(x)^{n_{t-1,1}} \cdot \ldots \cdot \sigma_\zeta^{t-1}(x)^{n_{t-1,t-1}}.\end{aligned}$$

Note that if $a \in (F_{\Sigma_1}\mathbb{C})(z)$ belongs to $\mathbb{C}(z)$, then

$$\gamma_e(a) = a \quad \text{and} \quad \gamma_e(\sigma_\zeta^i(a)) = \sigma_\zeta^i(\gamma_e(a)),$$

where the σ_q-homomorphism $\gamma_e\colon (F_{\Sigma_1}\mathbb{C})(z) \to \mathbb{C}(z)$ is defined in (10). Applying this homomorphism to (31), we obtain

$$a^{n_{0,0}} \cdot \sigma_\zeta(a)^{n_{0,1}} \cdot \ldots \cdot \sigma_\zeta^{t-1}(a)^{n_{0,t-1}} = \sigma_q(\gamma_e(b))/\gamma_e(b),$$

which concludes the proof. □

4.2 Setup for meromorphic functions

The ring of all meromorphic functions on $\mathbb{C}^*$ will be denoted by $\mathcal{M}$. For any nonzero complex number a we define an automorphism $\sigma_a : \mathcal{M} \to \mathcal{M}$ by

$$\sigma_a(f)(z) = f(az).$$

Let $\Sigma_1 \subseteq \mathbb{C}^*$ be a finite subgroup. Then Σ_1 is a cyclic group generated by a root of unity ζ of degree t. Let $q \in \mathbb{C}$ be such that $|q| > 1$. Now, we have an action of the group $\Sigma = \mathbb{Z} \oplus \mathbb{Z}/t\mathbb{Z}$, where the first summand is generated by σ_q and the second one is generated by σ_ζ.

The set of all σ_q-invariant meromorphic functions will be denoted by $\Bbbk$. As we can see $\Bbbk$ is a Σ_1-ring. Let C be the Σ_1-closure of the field $\Bbbk$. Supply the polynomial ring $C[z]$ with the following structure of a Σ-ring:

$$\sigma_q(z) = qz \quad \text{and} \quad \sigma_\zeta(z) = \zeta z.$$

Let K be the total ring of fractions of $C[z]$, so, K is a Noetherian Σ-pseudofield with Σ_1-closed subpseudofield of σ_q-constants C. The meromorphic function z is algebraically independent over $\Bbbk$. Hence, the minimal Σ-subfield in $\mathcal{M}$ generated by $\Bbbk$ and z is the ring of rational functions $\Bbbk(z)$. Thus, this field can be naturally embedded into K with z being mapped to z.

4.3 Jacobi's theta-function

We will study Σ_1-relations for Jacobi's theta-function (being a solution of $\theta_q(qz) = -qz\cdot\theta_q(z)$)

$$\theta_q(z) = -\sum_{n\in\mathbb{Z}}(-1)^n q^{\frac{-n(n-1)}{2}} z^n, \quad z\in\mathbb{C}, \tag{32}$$

with coefficients in $\Bbbk(z)$.

4.3.1 Relations for θ_q with q-periodic coefficients

First, we will show that there are many relations of such form:

1. Suppose that $t \geqslant 3$. Then, the function

   $$\lambda = \theta_q(z)\cdot\theta_q^{-2}(\zeta z)\cdot\theta_q(\zeta^2 z)$$

   is σ_q-invariant. Therefore, θ_q vanishes the following nontrivial Σ_1-polynomial:

   $$y\cdot\sigma_{\zeta^2}(y) - \lambda\cdot(\sigma_\zeta(y))^2 \in \Bbbk(z)\{y\}.$$

2. Suppose that $t = m\cdot n$, where m and n are coprime. Then, there exist two numbers $u\neq v$ such that the automorphisms $\sigma_\zeta^u \neq \sigma_\zeta^v$ but $\sigma_\zeta^{un} = \sigma_\zeta^{vn} \neq \mathrm{id}$. Then, the function

   $$\lambda = \theta_q^n(\zeta^u z)\cdot\theta_q^{-n}(\zeta^v z)$$

   is σ_q-invariant. Therefore, θ_q vanishes the following nontrivial Σ_1-polynomial:

   $$(\sigma_{\zeta^u}(y))^n - \lambda\cdot(\sigma_{\zeta^v}(y))^n \in \Bbbk(z)\{y\}.$$

3. For any given ζ, the function

   $$\lambda = \theta_q^t(z)\cdot\theta_q^{-t}(\zeta z)$$

   is σ_q-constant. Therefore, θ_q vanishes the following nontrivial Σ_1-polynomial:

   $$y^t - \lambda\cdot(\sigma_\zeta(y))^t \in \Bbbk(z)\{y\}.$$

4.3.2 Periodic difference-algebraic independence for θ_q with q-periodic coefficients

We will show now that in some sense these relations are the only possible ones.

Lemma 4.2. *Suppose that for some rational function $b\in\Bbbk(z)$ there is a relation*

$$(-qz)^{k_0}(-q\zeta z)^{k_1}\cdot\ldots\cdot\left(-q\zeta^{t-1}z\right)^{k_{t-1}} = \sigma_q(b)/b$$

for some $k_i\in\mathbb{Z}$. Then, $\sum_{i=0}^{t-1} k_i = 0$.

Proof. The function $\sigma_q(b)/b$ is of the following form $\sigma_q(b)/b = h/g$, where h and g have the same degree and the same leading coefficient. The equality follows from the condition on the degree. □

Lemma 4.3. *Suppose that there exist $\lambda \in \Bbbk(z)$ and η, $q \in \mathbb{C}$ such that $\sigma_q(\lambda) = \eta \cdot \lambda$, where $|\eta| = 1$ and $0 \neq q$ is not a root of unity. Then, $\lambda \in \Bbbk$ and $\eta = 1$.*

Proof. Let

$$\lambda = a \cdot z^r \cdot \frac{(z-a_1)\cdot \ldots \cdot (z-a_n)}{(z-b_1)\cdot \ldots \cdot (z-b_m)}$$

be the irreducible representation of λ, where $a_i, b_i \in \overline{\Bbbk}$, the algebraic closure of $\Bbbk$. By the hypothesis, we have

$$q^{r+n-m} \cdot \frac{(z-a_1/q)\cdot \ldots \cdot (z-a_n/q)}{(z-b_1/q)\cdot \ldots \cdot (z-b_m/q)} = \eta \cdot \frac{(z-a_1)\cdot \ldots \cdot (z-a_n)}{(z-b_1)\cdot \ldots \cdot (z-b_m)}.$$

Therefore, $q^{r+n-m} = \eta$. Thus, $r+n-m = 0$ and $\eta = 1$. Moreover, the sets $\{a_1, \ldots, a_n\}$ and $\{a_1/q, \ldots, a_n/q\}$ must coincide. If $\lambda \notin \Bbbk$, then, from $r+n-m = 0$, it follows that either $n > 0$ or $m > 0$. Suppose that the first inequality holds. There exists i such that $a_1 = \frac{a_i}{q}$. If $i = 1$, then we set $i_0 = 1$. Otherwise, $i > 1$ and, rearranging the elements $\{a_j\}$ for $j > 1$ suppose that $i = 2$. Again, $a_2 = \frac{a_i}{q}$. If $i = 1$, we set $i_0 = i$. Otherwise, $i > 2$ and rearranging the elements $\{a_j\}$ for $j > 2$, suppose that $i = 3$, and so on. Since there are only finitely many elements, the process will stop and we obtain a number i_0 with the following system of equations:

$$a_1 = a_2/q,\ a_2 = a_3/q,\ \ldots,\ a_{i_0} = a_1/q$$

Therefore, $q^{i_0} = 1$. Thus, $|q| = 1$, which is a contradiction. □

Proposition 4.4. *Let the pseudofield K be as above. Let R be a Picard–Vessiot ring over K for the equation $\sigma_q(y) = -qz \cdot y$ and L be the corresponding Picard–Vessiot pseudofield. Suppose f is an invertible solution in R. Then $L \otimes_K R$ is a graded ring such that f is of degree 1 and σ_q and σ_ζ preserve the grading.*

Proof. It follows from Proposition 3.17 that $R \otimes_K R = R \otimes_C C\{G\}$, where G is the corresponding Galois group. Multiplying by $L \otimes_R -$, we obtain: $L \otimes_K R = L \otimes_C C\{G\}$. Since group G is a subgroup of $\mathbf{G}_m$,

$$C\{G\} = C\{x, 1/x\}_{\Sigma_1}/J,$$

where the ideal J is generated by difference polynomials of the form

$$e_0 \cdot x^{k_0} \cdot \left(\sigma_\zeta x\right)^{k_1} \cdot \ldots \cdot (\sigma_\zeta^{t-1} x)^{k_{t-1}} - e_0$$

(see Example 3.13 for details). The ring $C\{x,1/x\}_{\Sigma_1}$ is a graded ring such that x is homogeneous of degree 1 and σ_ζ preserves the grading. In the proof of Theorem 4.1, we have obtained that

$$(-qz)^{k_0}\cdot(-q\zeta z)^{k_1}\cdot\ldots\cdot\left(-q\zeta^{t-1}z\right)^{k_{t-1}}=\sigma_q(b)/b$$

for some $b\in\mathbb{C}(z)$. Thus, it follows from Lemma 4.2 that

$$\sum_{i=0}^{t-1}k_i=0.$$

Therefore, the ideal J is homogeneous. Hence, $C\{G\}$ is graded. Thus, $L\otimes_C C\{G\}$ is graded. Since $f=\bar{f}\cdot y$, where $\bar{f}\in L$ is a solution of the equation in L, then f is a homogeneous element of degree 1. Since x is σ_q-constant, σ_q preserves the grading. □

Theorem 4.5. *For every prime number t, every relation of the form*

$$\lambda_0+\sum_{d=1}^{t-1}\left(\lambda_{0d}\cdot\theta_q(z)^d+\lambda_{1d}\cdot\theta_q(\zeta z)^d+\ldots+\lambda_{t-1d}\cdot\theta_q\left(\zeta^{t-1}z\right)^d\right)=0, \tag{33}$$

with $\lambda_0,\lambda_{ij}\in\Bbbk(z)$, implies that $\lambda_0=\lambda_{ij}=0$.

Proof. Let the pseudofield K be as above, R be a Picard–Vessiot ring over K for the equation $\sigma_q(y)=-qz\cdot y$, and L be the corresponding Picard–Vessiot pseudofield for R. It follows from Proposition 4.4 that $D=L\otimes_K R$ is a graded ring such that the image of θ_q in D is homogeneous of degree 1. Suppose now that θ_q satisfies an equation of the form (33). Then, the same equation holds in R and, after embedding R into D, it holds in D. Since D is graded, our equation is homogeneous. Thus, it is of the form

$$\lambda_0\cdot\theta_q(z)^d+\lambda_1\cdot\theta_q(\zeta z)^d+\ldots+\lambda_{t-1}\cdot\theta_q\left(\zeta^{t-1}z\right)^d=0$$

for some d. Consider the shortest equation and rewrite it as follows

$$\theta_q(z)^d+\lambda_r\cdot\theta_q(\zeta^r z)^d+\ldots+\lambda_{t-1}\cdot\theta_q\left(\zeta^{t-1}z\right)^d=0,$$

where $\lambda_r\cdot\theta_q(\zeta^r z)^d$ is the first nonzero summand immediately following $\theta_q(z)^d$. Applying σ_q and dividing by $(-qz)^d$, we obtain

$$\theta_q(z)^d+\sigma_q(\lambda_r)\cdot(\zeta^r)^d\cdot\theta_q\left(\zeta^r z\right)^d+\ldots+\sigma_q(\lambda_{t-1})\cdot\left(\zeta^{t-1}\right)^d\cdot\theta_q\left(\zeta^{t-1}z\right)^d=0$$

Therefore,

$$\sigma_q(\lambda_r)=\zeta^{-rd}\cdot\lambda_r.$$

Now, it follows from Lemma 4.3 that $\zeta^{-rd}=1$, contradiction. Thus, $\theta_q(z)^d=0$ must hold, but Picard–Vessiot pseudofield is reduced, which is a contradiction again. □

4.3.3 Difference-algebraic independence for θ_q over $\mathbb{C}(z)$

We will now show difference-algebraic independence for θ_q over $\mathbb{C}(z)$.

Example 4.6. Consider an equation

$$F(\theta_q) = \sum_{(n_1,\dots,n_p)\in\mathbb{Z}^p} g_{n_1,\dots,n_p}(z)\cdot\theta_q(\alpha_1 z)^{n_1}\cdot\ldots\cdot\theta_q(\alpha_p z)^{n_p} = 0,$$

where $g_{n_1,\dots,n_p}\in\mathbb{C}(z)$ and $1\neq\alpha_i\neq\alpha_j$ in $\mathbb{C}^*/q^{\mathbb{Z}}$. We will show that all $g_{n_1,\dots,n_p}$ are equal to zero. Since the sum is finite, there exists a monomial

$$M(\theta_q) = \theta_q(\alpha_1 z)^{d_1}\cdot\ldots\cdot\theta_q(\alpha_p z)^{d_p}$$

such that $M(\theta_q)\cdot F(\theta_q)$ contains monomials with negative powers. Now, we will calculate the poles of a given monomial with negative powers. The poles of the i-th factor of the monomial

$$M(\theta_q) = \frac{1}{\theta_q(\alpha_1 z)^{n_1}}\cdot\ldots\cdot\frac{1}{\theta_q(\alpha_p z)^{n_p}}.$$

are $\alpha_i^{-1}q^r$ for all $r\in\mathbb{Z}$ and the multiplicity of each of the poles is n_i. The poles of distinct factors are distinct. Indeed, suppose that

$$\alpha_i^{-1}\cdot q^{r_1} = \alpha_j^{-1}\cdot q^{r_2}.$$

Then, $\alpha_j = \alpha_i\cdot q^{r_2-r_1}$. Therefore, $\alpha_i=\alpha_j$ in $\mathbb{C}^*/q^{\mathbb{Z}}$, which is a contradiction. Thus, the set of all poles of the monomial $M(\theta_q)$ is $\alpha_i^{-1}\cdot q^r$ with multiplicity n_i.

Every function $g\in\mathbb{C}(z)$ has only finitely many poles and zeros, so, all of them are inside of a disk $U_d=\{z\in\mathbb{C}\mid |z|<d\}$. So, the set of all poles for $M(\theta_q)$ and $g\cdot M(\theta_q)$ coincides in $\mathbb{C}\setminus U_d$ for some d. There exists a disk U_d such that this property holds for all summands in F. We can rewrite F as follows:

$$\begin{aligned}F(\theta_q) &= \sum_{n_1}\left(\sum_{n_2,\dots,n_p} g_{n_1,\dots,n_p}\cdot\theta_q(\alpha_1 z)^{n_1}\cdot\ldots\cdot\theta_q(\alpha_p z)^{n_p}\right) = \\ &= \sum_{n_1} F_{n_1}(\theta_q) = 0.\end{aligned}$$

The point $\alpha_1^{-1}q^{r_1}$ (where r_1 is large enough positive if $q>1$ and large enough negative if $q<1$) is a pole for all summands F_{n_i} and the multiplicity of this pole is different for different n_i. To annihilate these poles, $F_{n_1}=0$ must hold for all n_1. Repeating the same argument for all n_i, we arrive at

$$g_{n_1,\dots,n_p}(z)\cdot\theta_q(\alpha_1 z)^{n_1}\cdot\ldots\cdot\theta_q(\alpha_p z)^{n_p} = 0$$

for each $n_1,\dots,n_p$. Therefore, $g_{n_1,\dots,n_p}=0$.

It follows from this result that for an arbitrary root of unity ζ the function θ_q is σ_ζ-algebraically independent over $\mathbb{C}(z)$ in the field of meromorphic functions on $\mathbb{C}^*$. However, to generalize this result to finitely many roots of unity, we need to require the following:

$$\text{for all } i \text{ and } j \quad \zeta_i^k=\zeta_j^m \quad \text{implies} \quad \zeta_i^k=\zeta_j^m=1.$$

Otherwise, the result is not true. Indeed, if $\zeta_i^k = \zeta_j^m \neq 1$, then the relation

$$\sigma_{\zeta_i}^k(\theta_q) - \sigma_{\zeta_j}^m(\theta_q) = 0$$

is non-trivial. Indeed, note that the difference indeterminates $\sigma_{\zeta_i}^k x$ and $\sigma_{\zeta_j}^m x$ are distinct even in the difference polynomial ring $\mathbb{Q}\{x\}_{\Sigma_1}$ in spite of the fact that they define the same automorphisms of meromorphic functions.

4.4 General order one q-difference equations

We will start by discussing several examples of σ_ζ-dependence and independence and finish by providing a general criterion in Theorem 4.9.

Example 4.7. For $a(z) = \frac{z+1}{z-1}$, $t = 2$, and $\zeta = -1$, we have

$$\sigma_\zeta(a)(z) \cdot \sigma_\zeta^0(a)(z) = \frac{-z+1}{-z-1} \cdot \frac{z+1}{z-1} = 1 = \sigma_q(1)/1.$$

Let g be a meromorphic function on $\mathbb{C}\setminus\{0\}$ such that $\sigma_q(g) = \frac{z+1}{z-1} \cdot g$. Then, $g(z) \cdot g(-z)$ is σ_q-invariant:

$$\sigma_q(g \cdot \sigma_\zeta(g)) = \frac{z+1}{z-1} \cdot g \cdot \sigma_\zeta\left(\frac{z+1}{z-1} \cdot g\right) = \frac{z+1}{z-1} \cdot \frac{-z+1}{-z-1} \cdot g \cdot \sigma_\zeta(g) = g \cdot \sigma_\zeta(g).$$

So, the function g is σ_ζ-algebraically dependent over $\Bbbk$.

Example 4.8. For $a(z) = 2^z$ and $t = 4$ with $\zeta = i$, we have

$$\sigma_\zeta^2(a)(z) \cdot \sigma_\zeta^0(a)(z) = 2^{-z} \cdot 2^z = 1 = \sigma_q(1)/1.$$

As before, let g be a meromorphic function on $\mathbb{C}\setminus\{0\}$ such that $\sigma_q(g) = 2^z \cdot g$. Then, $g(z) \cdot g(-z)$ is σ_q-invariant. Indeed,

$$\sigma_q(g \cdot \sigma_\zeta^2(g)) = 2^z \cdot g \cdot \sigma_\zeta^2(2^z \cdot g) = 2^z \cdot 2^{-z} \cdot g \cdot \sigma_\zeta^2(g) = g \cdot \sigma_\zeta^2(g).$$

So, the function g is σ_ζ-algebraically dependent over $\Bbbk$.

4.4.1 General characterization of periodic difference-algebraic independence

Let $a \in \mathbb{C}(z)$ and $q, \zeta \in \mathbb{C}^*$ be such that $|q| > 1$ and ζ is a primitive root of unity of order t. Then, a can be represented as follows

$$a = \lambda \cdot z^T \cdot \prod_{k=0}^{t-1} \prod_{d=-N-1}^{N} \prod_{i=1}^{R} \left(z - \zeta^k \cdot q^d \cdot r_i\right)^{s_{k,d,i}},$$

where $\lambda, r_i \in \mathbb{C}^*$ and the r_i's are distinct in $\mathbb{C}^*/\zeta^{\mathbb{Z}} \cdot q^{\mathbb{Z}}$. Let

$$a_{i,k} = \sum_{d=-N-1}^{N} s_{k,d,i}, \; d_{k,i} = \sum_{j=0}^{t-1} \zeta^{k \cdot j} \cdot a_{i,j}, \text{ and } D = \begin{pmatrix} d_{0,1} & d_{0,2} & \dots & d_{0,R} \\ d_{1,1} & d_{1,2} & \dots & d_{1,R} \\ \vdots & \vdots & \ddots & \vdots \\ d_{t-1,1} & d_{t-1,2} & \dots & d_{t-1,R} \end{pmatrix}.$$

The following result combined with Theorem 4.1 provides a complete characterization of all equations (27) whose solutions are σ_ζ-algebraically independent.

Theorem 4.9. *Let $a \in \mathbb{C}(z)$ and D be as above. Then,*

1. *If $T = 0$ and, either $\lambda^{\mathbb{Z}} \cap q^{\mathbb{Z}} \neq 1$ or λ is a root of unity, then there exist $b \in \mathbb{C}(z)$ and a multiplicative function*
$$\varphi(x) = x^{n_0} \cdot \left(\sigma_\zeta x\right)^{n_1} \cdot \ldots \cdot (\sigma_\zeta^{t-1} x)^{n_{t-1}}$$
such that $\varphi(a) = \sigma_q(b)/b$ if and only if the matrix D contains a zero row.
2. *If either $T \neq 0$ or, $\lambda^{\mathbb{Z}} \cap q^{\mathbb{Z}} = 1$ and λ is not a root of unity, then there exist $b \in \mathbb{C}(z)$ and a multiplicative function*
$$\varphi(x) = x^{n_0} \cdot \left(\sigma_\zeta x\right)^{n_1} \cdot \ldots \cdot (\sigma_\zeta^{t-1} x)^{n_{t-1}}$$
such that $\varphi(a) = \sigma_q(b)/b$ if and only if D contains a zero row other than the first one.

Proof. We will write φ and b with undetermined coefficients and exponents. Suppose that

$$b = \mu \cdot z^M \cdot \prod_{k=0}^{t-1} \prod_{d=-N}^{N} \prod_{i=1}^{R} \left(z - \zeta^k \cdot q^d \cdot r_i\right)^{l_{k,d,i}} \text{ and } \varphi(x) = x^{n_0} \cdot \left(\sigma_\zeta x\right)^{n_1} \cdot \ldots \cdot (\sigma_\zeta^{t-1} x)^{n_{t-1}}$$

are such that $\varphi(a) = \sigma_q(b)/b$. Let us calculate the right and left-hand sides of this equality. We see that

$$\sigma_q(b) = \mu \cdot q^{M + \sum_{k,d,i} l_{k,d,i}} \cdot z^M \cdot \prod_{k=0}^{t-1} \prod_{d=-N}^{N} \prod_{i=1}^{R} \left(z - \zeta^k \cdot q^{d-1} \cdot r_i\right)^{l_{k,d,i}}.$$

Hence,

$$\frac{\sigma_q(b)}{b} = q^{M+\sum_{k,d,i} l_{k,d,i}} \cdot \prod_{k=0}^{t-1} \prod_{d=-N-1}^{N-1} \prod_{i=1}^{R} \left(z - \zeta^k \cdot q^d \cdot r_i\right)^{l_{k,d+1,i}} \cdot$$
$$\cdot \prod_{k=0}^{t-1} \prod_{d=-N}^{N} \prod_{i=1}^{R} \left(z - \zeta^k \cdot q^d \cdot r_i\right)^{-l_{k,d,i}} =$$
$$= q^{M+\sum_{k,d,i} l_{k,d,i}} \cdot \prod_{k=0}^{t-1} \prod_{i=1}^{R} \Big[\left(z - \zeta^k \cdot q^{-N-1} \cdot r_i\right)^{l_{k,-N,i}} \cdot$$
$$\cdot \prod_{d=-N}^{N-1} \left(z - \zeta^k \cdot q^d \cdot r_i\right)^{l_{k,d+1,i} - l_{k,d,i}} \left(z - \zeta^k \cdot q^N \cdot r_i\right)^{-l_{k,N,i}} \Big].$$

Now, we calculate the left-hand side. We see that

$$\sigma_\zeta^r a = \lambda \cdot \zeta^{rT + \sum_{k,d,i} r \cdot s_{k,d,i}} \cdot z^T \cdot \prod_{k=0}^{t-1} \prod_{d=-N-1}^{N} \prod_{i=1}^{R} \left(z - \zeta^{k-r} \cdot q^d \cdot r_i\right)^{s_{k,d,i}} =$$
$$= \lambda \cdot \zeta^{rT + \sum_{k,d,i} r \cdot s_{k,d,i}} \cdot z^T \cdot \prod_{k=0}^{t-1} \prod_{d=-N-1}^{N} \prod_{i=1}^{R} \left(z - \zeta^{k} \cdot q^d \cdot r_i\right)^{s_{k+r,d,i}}.$$

Hence,

$$\varphi(a) = \lambda^{\sum_{r=0}^{t-1} n_r} \cdot \zeta^{\left(T + \sum_{k,d,i} s_{k,d,i}\right) \cdot \left(\sum_{r=0}^{t-1} r \cdot n_r\right)} \cdot z^{T \cdot \left(\sum_{k=0}^{t-1} n_r\right)} \cdot$$
$$\cdot \prod_{k=0}^{t-1} \prod_{d=-N-1}^{N} \prod_{i=1}^{R} \left(z - \zeta^k \cdot q^d \cdot r_i\right)^{\sum_{r=0}^{t-1} n_r s_{k+r,d,i}}.$$

Now, the equation $\varphi(a) = \sigma_q(b)/b$ gives the following system of equations

$$\begin{cases} \begin{cases} \sum_{r=0}^{t-1} s_{k+r,-N-1,i} \cdot n_r = l_{k,-N,i} \\ \sum_{r=0}^{t-1} s_{k+r,d,i} \cdot n_r = l_{k,d+1,i} - l_{k,d,i}, \qquad -N \leqslant d \leqslant N-1 \\ \sum_{r=0}^{t-1} s_{k+r,N,i} \cdot n_r = -l_{k,N,i} \end{cases} \\ \lambda^{\sum_{k=0}^{t-1} n_r} \cdot \zeta^{\left(T + \sum_{k,d,i} s_{k,d,i}\right) \cdot \left(\sum_{r=0}^{t-1} r \cdot n_r\right)} = q^{M + \sum_{k,d,i} l_{k,d,i}} \\ T \cdot \sum_{r=0}^{t-1} n_r = 0 \end{cases}$$

In this system, the unknown variables are $l_{k,d,i}$, n_r, and M. If $l_{k,d,i}, n_r, M$ is a solution of the system such that not all n_r's are zeroes, then $t \cdot l_{k,d,i}, t \cdot n_r, t \cdot M$ is a solution with the same property. Therefore, we can replace the second equation with

$$\lambda^{\sum_{k=0}^{t-1} n_r} = q^{M+\sum_{k,d,i} l_{k,d,i}}.$$

The first subsystem can be rewritten as follows:

$$\begin{pmatrix} s_{k,-N-1,i} & s_{k+1,-N-1,i} & \dots & s_{k-1,-N-1,i} \\ s_{k,-N,i} & s_{k+1,-N,i} & \dots & s_{k-1,-N,i} \\ \vdots & \vdots & \ddots & \vdots \\ s_{k,N,i} & s_{k+1,N,i} & \dots & s_{k-1,N,i} \end{pmatrix} \begin{pmatrix} n_0 \\ n_1 \\ \vdots \\ n_{t-1} \end{pmatrix} = \begin{pmatrix} l_{k,-N,i} \\ l_{k,-N+1,i} - l_{k,-N,i} \\ \vdots \\ -l_{k,N,i} \end{pmatrix}.$$

This system has a solution in $l_{k,d,i}$ if and only if the sum of all equations is zero. Thus, we can replace this system with the following:

$$n_0 \cdot \sum_{d=-N-1}^{N} s_{k,d,i} + n_1 \cdot \sum_{d=-N-1}^{N} s_{k+1,d,i} + \ldots + n_{t-1} \cdot \sum_{d=-N-1}^{N} s_{k-1,d,i} = 0.$$

Using the definition of the $a_{i,j}$'s, we obtain the following system:

$$\begin{pmatrix} a_{i,0} & a_{i,1} & \dots & a_{i,t-1} \\ a_{i,1} & a_{i,2} & \dots & a_{i,0} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i,t-1} & a_{i,0} & \dots & a_{i,t-2} \end{pmatrix} \begin{pmatrix} n_0 \\ n_1 \\ \vdots \\ n_{t-1} \end{pmatrix} = 0.$$

Thus, for some integers $\gamma_{k,d,i,j}$, we have:

$$\begin{cases} \begin{pmatrix} a_{i,0} & a_{i,1} & \dots & a_{i,t-1} \\ a_{i,1} & a_{i,2} & \dots & a_{i,0} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i,t-1} & a_{i,0} & \dots & a_{i,t-2} \end{pmatrix} \begin{pmatrix} n_0 \\ n_1 \\ \vdots \\ n_{t-1} \end{pmatrix} = 0 \\ \lambda^{\sum_{k=0}^{t-1} n_r} = q^{M+\sum_{k,d,i} l_{k,d,i}} \\ T \cdot \sum_{r=0}^{t-1} n_r = 0 \\ l_{k,d,i} = \sum_{r=0}^{t-1} \gamma_{k,d,i,r} \cdot n_r \end{cases}$$

Consider the **first case**: $T = 0$ and $\lambda^{\mathbb{Z}} \cap q^{\mathbb{Z}} \neq 1$. Then, for some $u, v \in \mathbb{Z} \setminus \{0\}$ we have $\lambda^u = q^v$. Hence, the second equation is equivalent to

$$v \cdot \sum_{r=0}^{t-1} n_r = u \cdot \left(M + \sum\nolimits_{k,d,i} l_{k,d,i}\right)$$

Suppose that n_r and $l_{k,d,i}$ form a solution of all equations except for the second one, where not all n_r's are zero. Then,

$$u \cdot n_r, \quad u \cdot l_{k,d,i}, \quad M = \sum_{r=0}^{t-1}(v \cdot n_r) - \sum\nolimits_{k,d,i}(u \cdot l_{k,d,i})$$

form a solution of the whole system. Thus, in this case, we may exclude the second equation. Now we will check the case $T = 0$ and $\lambda^w = 1$ for some $w \in \mathbb{Z} \setminus \{0\}$. In this situation, if $n_r, l_{k,d,i}$ is a solution of all equations except for the second one, then

$$w \cdot n_r, \;\; w \cdot l_{k,d,i}, \;\; M = -\sum\nolimits_{k,d,i} w \cdot l_{k,d,i}$$

is a solution of the whole system. Therefore, in this case, the existence of φ and b is equivalent to

$$\begin{pmatrix} a_{i,0} & a_{i,1} & \dots & a_{i,t-1} \\ a_{i,1} & a_{i,2} & \dots & a_{i,0} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i,t-1} & a_{i,0} & \dots & a_{i,t-2} \end{pmatrix} \begin{pmatrix} n_0 \\ n_1 \\ \vdots \\ n_{t-1} \end{pmatrix} = 0 \tag{34}$$

having a nontrivial common solution.

Consider the **second case**: $T \neq 0$ or $\big(\lambda^{\mathbb{Z}} \cap q^{\mathbb{Z}} = 1$ and λ is not a root of unity$\big)$. If $T \neq 0$, then the third equation gives $\sum_{r=0}^{t-1} n_r = 0$, and if $\lambda^{\mathbb{Z}} \cap q^{\mathbb{Z}} = 1$ and λ is not a root of unity, then the second equation gives $\sum_{r=0}^{t-1} n_r = 0$. Therefore, in both cases, the second equation is of the form

$$M + \sum\nolimits_{k,d,i} l_{k,d,i} = 0.$$

Again, if $n_r, \; l_{k,d,i}$ form a solution of all equations except the second one, where not all n_r's are zeroes, then

$$n_r, \;\; l_{k,d,i}, \;\; M = -\sum\nolimits_{k,d,i} l_{k,d,i}$$

form a solution of the whole system with the same property. Thus, in this case, we need to show the existence of a nontrivial solution of the system

$$\begin{cases} \begin{pmatrix} a_{i,0} & a_{i,1} & \dots & a_{i,t-1} \\ a_{i,1} & a_{i,2} & \dots & a_{i,0} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i,t-1} & a_{i,0} & \dots & a_{i,t-2} \end{pmatrix} \begin{pmatrix} n_0 \\ n_1 \\ \vdots \\ n_{t-1} \end{pmatrix} = 0, \\ n_0 + n_1 + \ldots + n_{t-1} = 0. \end{cases} \tag{35}$$

Since all the coefficients in (34) and (35) are integers, there is a nontrivial solution with integral coefficients if and only if there is a nontrivial solution with complex coefficients.

Define

$$E_+ = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \dots & \zeta^{t-1} \\ 1 & \zeta^2 & \zeta^{2\cdot 2} & \dots & \zeta^{2\cdot(t-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{t-1} & \zeta^{(t-1)\cdot 2} & \dots & \zeta^{(t-1)\cdot(t-1)} \end{pmatrix},$$

$$E_- = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta^{-1} & \zeta^{-2} & \dots & \zeta^{-(t-1)} \\ 1 & \zeta^{-2} & \zeta^{-2\cdot 2} & \dots & \zeta^{-2\cdot(t-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{-(t-1)} & \zeta^{-(t-1)\cdot 2} & \dots & \zeta^{-(t-1)\cdot(t-1)} \end{pmatrix},$$

$$A_i = \begin{pmatrix} a_{i,0} & a_{i,1} & \dots & a_{i,t-1} \\ a_{i,1} & a_{i,2} & \dots & a_{i,0} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i,t-1} & a_{i,0} & \dots & a_{i,t-2} \end{pmatrix}, \quad D_i = \begin{pmatrix} d_{0,i} & 0 & \dots & 0 \\ 0 & d_{1,i} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_{t-1,i} \end{pmatrix}.$$

A straightforward calculation shows that $E_+ \cdot A_i = D_i \cdot E_-$. Let n be the vector with the coordinates $n_0, n_1, \dots, n_{t-1}$. Hence, in the **first case**, the systems $E_+ \cdot A_i \cdot n = D_i \cdot E_- \cdot n = 0$ have a nontrivial solution. This is equivalent to the condition that the systems $D_i \cdot m = 0$ have a nontrivial solution, where $m = E_- \cdot n$. Since the D_i's are diagonal, there is a common solution of all systems $D_i \cdot m = 0$ if and only if the matrices D_i have a zero in the same place. In other words, there is an integer i_0 such that for all i we have $d_{i_0,i} = 0$. The latter condition is equivalent to the condition that there is a zero row in the matrix D.

Consider the **second case**. Let $l = (1,1,\dots,1)$ with t coordinates. We must to show that the systems

$$A_i \cdot n = 0, \quad l \cdot n = 0$$

have a nontrivial solution. Multiplying by E_+, we have

$$D_i \cdot E_- \cdot n = 0, \quad l \cdot n = 0.$$

Let $p_1, \dots, p_u$ be the positions of all zero rows in the matrix D. And let $E_1, \dots, E_u$ be the columns in E_-^{-1} with the p_i's as indices. Since the matrices D_i are diagonal, every common solution of the systems $D_i \cdot E_- \cdot n = 0$ is of the form:

$$n = W \cdot \mu, \quad W := (E_1, \dots, E_u), \quad \mu := (\mu_1, \dots, \mu_n)^T.$$

Then, the equation $l \cdot n = 0$ gives $l \cdot W \cdot \mu = 0$ Now, we find a condition when $l \cdot E_i$ is zero. For this, note that $(1,0,\dots,0) \cdot E_- = (1,1,\dots,1)$ and, therefore,

$$(1,1,\dots,1) \cdot E_-^{-1} = (1,0,\dots,0).$$

Hence, only the first column of the matrix E_-^{-1} gives nonzero elements in the vector $l \cdot W$. The system $l \cdot W \cdot \mu = 0$ has only the zero solution if and only if W is just one column and $l \cdot W \neq 0$. Thus, this system has a nontrivial solution if and only if W contains a row of E_-^{-1} other than the first one. In other words, the elements $d_{k,i}$ are zeroes for some $k \neq 0$ and all i, $1 \leqslant i \leqslant R$. This is equivalent to the condition that D contains a zero row other than the first one. □

Corollary 4.10. *In the situation of Theorem 4.1, if the zeros and poles of $a \in \mathbb{C}(z)$ are pairwise distinct modulo the group generated by ζ and q, then any non-zero solution f of the equation $\sigma_q(f) = af$ is σ_ζ-independent over $\Bbbk(z)$.*

Example 4.11. If $0 \neq c \in \mathbb{C}$, then any non-zero solution f of $\sigma_q(f) = (z-c) \cdot f$ is σ_ζ-independent over $\Bbbk(z)$.

ACKNOWLEDGMENTS

We are grateful to Yves André, Henri Gillet, Sergey Gorchinskiy, Charlotte Hardouin, Manuel Kauers, Alexander Levin, Alice Medvedev, Eric Rosen, Jacques Sauloy, Michael Singer, Lucia di Vizio, Michael Wibmer, and the referee for their helpful comments.

FUNDING

B. Antieau was supported by the NSF Grants DMS-0901373 and CCF-0901175. A. Ovchinnikov was supported by the grants: NSF CCF-0901175, 0964875, and 0952591 and PSC-CUNY No. 60001-40 41.

REFERENCES

[1] K. Amano. Liouville extensions of Artinian simple module algebras. *Communications in Algebra*, 34(5):1811–1823, 2006. URL http://dx.doi.org/10.1080/00927870500542796.

[2] K. Amano and A. Masuoka. Picard-Vessiot extensions of Artinian simple module algebras. *Journal of Algebra*, 285(2):743–767, 2005. URL http://dx.doi.org/10.1016/j.jalgebra.2004.12.006.

[3] K. Amano, A. Masuoka, and M. Takeuchi. Hopf algebraic approach to Picard-Vessiot theory. *Handbook of Algebra*, 6:127–171, 2009. URL http://dx.doi.org/10.1016/S1570-7954(08)00204-0.

[4] Y. André. Différentielles non commutatives et théorie de Galois différentielle ou aux différences. *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série*, 34(5):685–739, 2001. URL http://dx.doi.org/10.1016/S0012-9593(01)01074-6.

[5] M. Atiyah and I. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, Reading, MA, 1969.

[6] N. Bourbaki. *Algèbre. Chapitre 8: Modules et anneaux semi-simples*. Hermann, Paris, 1958.

[7] N. Bourbaki. *Algèbre. Chapitres 4–7*. Éléments de Mathématique. Springer, 2007. URL http://dx.doi.org/10.1007/978-3-540-34499-5.

[8] P. Cassidy. Differential algebraic groups. *American Journal of Mathematics*, 94:891–954, 1972. URL http://www.jstor.org/stable/2373764.

[9] P. Cassidy. The differential rational representation algebra on a linear differential algebraic group. *Journal of Algebra*, 37(2):223–238, 1975. URL http://dx.doi.org/10.1016/0021-8693(75)90075-7.

[10] Z. Chatzidakis, C. Hardouin, and M. F. Singer. On the definitions of difference Galois groups. In *Model theory with applications to algebra and analysis. Vol. 1*, volume 349, pages 73–109. 2008. URL http://dx.doi.org/10.1017/CBO9780511735226.006.

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

[12] L. Di Vizio. Approche galoisienne de la transcendance différentielle. Journée annuelle 2012 de la SMF, 2012. URL http://divizio.perso.math.cnrs.fr/PREPRINTS/16-JourneeAnnuelleSMF/difftransc.pdf.

[13] L. Di Vizio and C. Hardouin. Courbures, groupes de Galois génériques et D-groupoïdes de Galois d'un système aux D-différences. *C. R. Math. Acad. Sci. Paris*, 348(17–18):951–954, 2010. URL http://dx.doi.org/10.1016/j.crma.2010.08.001.

[14] L. Di Vizio and C. Hardouin. Galois theories for q-difference equations: comparison theorems. 2011. URL http://arxiv.org/abs/1002.4839.

[15] L. Di Vizio and C. Hardouin. Parameterized generic Galois groups for q-difference equations, followed by the appendix "The Galois D-groupoid of a q-difference system" by Anne Granier. 2011. URL http://arxiv.org/abs/1002.4839.

[16] L. Di Vizio and C. Hardouin. On the Grothendieck conjecture on p-curvatures for q-difference equations. 2011. URL http://arxiv.org/abs/1002.4839.

[17] L. Di Vizio and C. Hardouin. Descent for differential Galois theory of difference equations. Confluence and q-dependency. *Pacific Journal of Mathematics*, 256(1):79–104, 2012. URL http://dx.doi.org/10.2140/pjm.2012.256.79.

[18] L. Di Vizio, C. Hardouin, and M. Wibmer. Difference Galois theory of linear differential equations. *Advances in Mathematics*, 260:1–58, 2014. URL http://dx.doi.org/10.1016/j.aim.2014.04.005.

[19] A. Granier. A Galois D-groupoid for q-difference equations. *Annales de l'Institut Fourier*, 61 (4):1493–1516, 2011. URL http://dx.doi.org/10.5802/aif.2648.

[20] C. Hardouin. Hypertranscendance et groupes de Galois aux différences. 2006. URL http://arxiv.org/abs/math/0609646.

[21] C. Hardouin. Hypertranscendance des systèmes aux différences diagonaux. *Compositio Mathematica*, 144(3):565–581, 2008. URL http://dx.doi.org/10.1112/S0010437X07003430.

[22] C. Hardouin and M. F. Singer. Differential Galois theory of linear difference equations. *Mathematische Annalen*, 342(2):333–377, 2008. URL http://dx.doi.org/10.1007/s00208-008-0238-z.

[23] M. Kamensky. Tannakian formalism over fields with operators. *International Mathematics Research Notices*, 2013(24):5571–5622, 2013. URL http://dx.doi.org/10.1093/imrn/rns190.

[24] B. Lando. Extensions of difference specializations. *Proceedings of the American Mathematical Society*, 79(2):197–202, 1980. URL http://dx.doi.org/10.1090/S0002-9939-1980-0565337-1.

[25] A. Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008. URL http://dx.doi.org/10.1007/978-1-4020-6947-5.

[26] J. Milne. *Étale Cohomology*. Princeton University Press, Princeton, NJ, 1980.

[27] S. Morikawa. On a general difference Galois theory. I. *Annales de l'Institut Fourier*, 59(7): 2709–2732, 2009. URL http://dx.doi.org/10.5802/aif.2505.

[28] A. Ovchinnikov and M. Wibmer. σ-Galois theory of linear difference equations. *International Mathematics Research Notices*, 2015. URL http://dx.doi.org/10.1093/imrn/rnu060.

[29] E. Rosen. A differential Chevalley theorem. 2008. URL http://arxiv.org/abs/0810.5486.

[30] D. Trushin. Difference Nullstellensatz in the case of finite group. 2009. URL http://arxiv.org/abs/0908.3863.

[31] D. Trushin. Difference Nullstellensatz. 2009. URL http://arxiv.org/abs/0908.3865.

[32] M. van der Put and M. F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997. URL http://dx.doi.org/10.1007/BFb0096118.

[33] W. Waterhouse. *Introduction to affine group schemes*. Springer, New York, 1979. URL http://dx.doi.org/10.1007/978-1-4612-6217-6.

[34] M. Wibmer. *Geometric Difference Galois Theory*. PhD thesis, University of Heidelberg, 2010.

[35] M. Wibmer. A Chevalley theorem for difference equations. *Mathematische Annalen*, 354(4): 1369–1396, 2012. URL http://dx.doi.org/10.1007/s00208-011-0770-0.