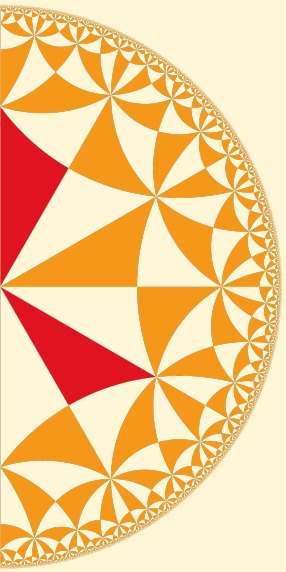
Université Grenoble Alpes



ANNALES DE
L'INSTITUT FOURIER

Ehud de Shalit

Algebraic independence and difference equations over elliptic function fields

Tome 75, n° 4 (2025), p. 1509-1554.

https://doi.org/10.5802/aif.3694

Les *Annales de l'Institut Fourier* sont membres du Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org e-ISSN : 1777-5310

Ann. Inst. Fourier, Grenoble
75, 4 (2025) 1509-1554

ALGEBRAIC INDEPENDENCE AND DIFFERENCE EQUATIONS OVER ELLIPTIC FUNCTION FIELDS

by Ehud DE SHALIT

ABSTRACT. — For a lattice Λ in the complex plane, let K_Λ be the field of Λ-elliptic functions. For two relatively prime integers p (respectively q) greater than 1, consider the endomorphisms ψ (resp. ϕ) of K_Λ given by multiplication by p (resp. q) on the elliptic curve $\mathbb{C}/\Lambda$. We prove that if f (resp. g) are complex Laurent power series that satisfy linear difference equations over K_Λ with respect to ϕ (resp. ψ) then there is a dichotomy. *Either*, for some sublattice Λ' of Λ, one of f or g belongs to the ring $K_{\Lambda'}[z, z^{-1}, \zeta(z, \Lambda')]$, where $\zeta(z, \Lambda')$ is the Weierstrass zeta function, *or* f and g are algebraically independent over K_Λ. This is an elliptic analogue of a recent theorem of Adamczewski, Dreyfus, Hardouin and Wibmer (over the field of rational functions).

RÉSUMÉ. — Pour un reseau Λ dans le plan complexe, soit K_Λ le corps des fonctions Λ-elliptiques. Pour deux entiers p (respectivement q), premiers entre eux, considérons les endomorphismes ψ (resp. ϕ) de K_Λ donnés par multiplication par p (resp. q) sur la courbe elliptique $\mathbb{C}/\Lambda$. Nous prouvons que si f (resp. g) sont des séries de Laurent complexes qui satisfont les équations aux différences linéaires sur K_Λ par rapport à ϕ (resp. ψ), alors il y a une dichotomie. Soit, pour un sous-réseau Λ' de Λ, l'un de f ou g appartient à l'anneau $K_{\Lambda'}[z, z^{-1}, \zeta(z, \Lambda')]$, où $\zeta(z, \Lambda')$ est la fonction zeta de Weierstrass, ou f et g sont algébriquement indépendents sur K_Λ. C'est un analogue elliptique d'un théorème récent d'Adamczewski, Dreyfus, Hardouin et Wibmer (sur le corps des fonctions rationelles).

1. Introduction

1.1. Background, over fields of rational functions

A ϕ-field is a field K equipped with an endomorphism ϕ. The fixed field $C = K^\phi$ of ϕ is called *the field of constants* of K. Throughout this paper we shall only consider ground fields which are *inversive:* ϕ is an automorphism of K, but for a general extension of K we do not impose this condition. Let

Keywords: Difference equations, elliptic functions, algebraic independence.
2020 *Mathematics Subject Classification:* 12H10, 14H52, 39A10.

$(K,\phi) \subset (F,\phi)$ be an extension of ϕ-fields (written from now on $K \subset F$), which is also inversive, and with the same field of constants:

$$C = K^{\phi} = F^{\phi}.$$

Denote by $S_{\phi}(F/K)$ the collection of all $u \in F$ which satisfy a linear homogenous ϕ-difference equation

$$a_0\phi^n(u) + a_1\phi^{n-1}(u) + \cdots + a_n u = 0, \tag{1.1}$$

with coefficients $a_i \in K$. The set $S_{\phi}(F/K)$ is a K-subalgebra of F.

Suppose now that K and F are endowed with a second automorphism ψ, commuting with ϕ, and that tr.deg.$(K/C) \leqslant 1$. Various results obtained in recent years support the philosophy that *if ϕ and ψ are sufficiently independent, the K-algebras $S_{\phi}(F/K)$ and $S_{\psi}(F/K)$ are also "independent" in an appropriate sense.*

Here are some classical examples. Let C be an algebraically closed field of characteristic 0. We consider three classes of examples where

(2S) $K = C(x)$, $F = C((x^{-1}))$, $\phi f(x) = f(x+h)$, $\psi f(x) = f(x+k)$, $(h,k \in C)$,

(2Q) $K = C(x)$, $F = C((x))$, $\phi f(x) = f(qx)$, $\psi f(x) = f(px)$ $(p,q \in C^{\times})$,

(2M) $K = \bigcup_{s=1}^{\infty} C(x^{1/s})$, $F = \bigcup_{s=1}^{\infty} C((x^{1/s}))$ (the field of Puiseux series), $\phi f(x) = f(x^q)$, $\psi f(x) = f(x^p)$ $(p,q \in \mathbb{N})$.

Note that ϕ and ψ are indeed *auto*morphisms. In all three examples, the assumption that ϕ and ψ are "sufficiently independent" is that the group

$$\Gamma = \langle \phi, \psi \rangle \subset \mathrm{Aut}(K)$$

is free abelian of rank 2. The letters S,Q and M stand for "shifts", "q-difference operators" and "Mahler operators" respectively, and the independence assumption gets translated into the additive independence of h and k in the case (2S), and the multiplicative independence[(1)] of p and q in the cases (2Q) and (2M). Schäfke and Singer proved in [14] the following theorem, confirming the above philosophy.

THEOREM 1.1. — *Assume that Γ is free abelian of rank 2. Then in any of the three cases* (2S), (2Q) *or* (2M)

$$S_{\phi}(F/K) \cap S_{\psi}(F/K) = K.$$

(1) p and q are called multiplicatively independent if $p^n q^m = 1$ if and only if $n = m = 0$.

Some instances of this theorem were known before. The case (2Q) dates back to the work of Bézivin and Boutabaa [5], and the case (2M), originally a conjecture of Loxton and van der Poorten [12], was proved by Adamczewski and Bell in [1]. The earlier proofs, however, used a variety of ad-hoc techniques, and only [14] gave a unified treatment, revealing the common principles behind these theorems. This new approach enabled the authors to prove a few more theorems of the same nature, dealing with power series satisfying simultaneously a ϕ-difference equation and a linear ordinary differential equation. See, also, the exposition in [18], where we removed some unnecessary restrictions on the characteristic of the field C and on $|p|$ and $|q|$, in the case (2Q). In addition, this last paper deals for the first time with a case, denoted there (1M1Q), in which ϕ is a q-difference operator and ψ a p-Mahler operator, and the resulting group Γ is generalized dihedral rather than abelian. The formulation of the analogous result has to be cast now in the language of *difference modules*, the classical language of equations being inadequate when Γ is non-abelian. Modulo this remark, however, the main result *and* its proof are very similar, if not identical, to the above three cases.

The next breakthrough occured in a recent paper by Adamczewski, Hardouin, Dreyfus and Wibmer [3]. Building on an earlier work [2] dealing with difference-differential systems, these authors obtained a far-reaching strengthening of the above theorem.

THEOREM 1.2. — *Consider any of the three cases* (2S), (2Q) *or* (2M). *Let* $f \in S_\phi(F/K)$ *and* $g \in S_\psi(F/K)$. *If* $f, g \notin K$ *then* f *and* g *are algebraically independent over* K.

Letting $f = g$ one recovers Theorem 1.1. The key new tool which allows to upgrade Theorem 1.1 to Theorem 1.2 is the "parametrized" Picard-Vessiot theory, as developed in [10, 11]. We shall elaborate on this theory and summarize its main ingredients in § 3.

1.2. Background, over fields of elliptic functions

1.2.1. The case (2Ell)

In [16, 17] we initiated the study of the same theme over fields of elliptic functions. For a lattice $\Lambda \subset \mathbb{C}$ let E_Λ stand for the elliptic curve whose associated Riemann surface is $\mathbb{C}/\Lambda$ and

$$K_\Lambda = \mathbb{C}\left(\wp(z,\Lambda), \wp'(z,\Lambda)\right)$$

its function field, the field of Λ-periodic meromorphic functions on $\mathbb{C}$. Here

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

is the Weierstrass $\wp$-function of the lattice Λ. Fix Λ_0 and let

$$K = \bigcup_{\Lambda \subset \Lambda_0} K_\Lambda.$$

This is the function field of the universal cover of E_{Λ_0}, and should be compared to the field K in the case (2M), which is the function field of the universal cover of $\mathbb{G}_m$. Let $p, q \in \mathbb{N}$. Multiplication by p or q induces an endomorphism of E_Λ for each Λ, and *automorphisms* of the field K given by

$$\phi f(z) = f(qz), \ \psi f(z) = f(pz).$$

For F we take the field of Laurent series $\mathbb{C}((z))$ with the same ϕ and ψ. Via the Taylor–Maclaurin expansion at 0, $K \subset F$. We label this choice of (K, F, ϕ, ψ) by (2Ell).

1.2.2. The ring S

To formulate our results we need to introduce a ring slightly larger than K, namely the ring

$$S = K\left[z, z^{-1}, \zeta(z,\Lambda)\right] \subset F$$

generated over K by z, z^{-1} and the Weierstrass zeta function $\zeta(z,\Lambda)$. Recall that the latter is a primitive of $-\wp(z,\Lambda)$ and satisfies, for $\omega \in \Lambda$,

$$\zeta(z+\omega,\Lambda) - \zeta(z,\Lambda) = \eta(\omega,\Lambda),$$

where the additive homomorphism $\eta(\cdot,\Lambda) : \Lambda \to \mathbb{C}$ is Legendre's eta function. Explicitly,

$$\zeta(z,\Lambda) = \frac{1}{z} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right),$$

and

$$\eta(\omega,\Lambda) = -\int_{z_0}^{z_0+\omega} \wp(z,\Lambda) dz.$$

It is easy to see that the ring S does not depend on which $\Lambda \subset \Lambda_0$ we use: once we adjoin one $\zeta(z,\Lambda)$, they are all in S. See the discussion at the end of Section 2.1. It is also easy to see that ϕ and ψ induce automorphisms of S.

1.2.3. Previous results in the case (2Ell)

In [17], the following analogue of Theorem 1.1 was proved:

THEOREM 1.3. — *Assume that* $2 \leqslant p, q$ *and* $(p, q) = 1$. *Then in the case (2Ell) we have*

$$S_\phi(F/K) \cap S_\psi(F/K) = S.$$

Remark.

(i) The reader should note the assumption on p and q being relatively prime integers $\geqslant 2$. This is stronger than assuming p and q to be only multiplicatively independent. This stronger assumption was needed in only one lemma of [17], but so far could not be avoided.

(ii) The case (2Ell) brings up two completely new issues, absent from the rational cases discussed so far. One is the issue of *periodicity*. The method of [14] starts with a formal analysis of the solutions to our ϕ- and ψ-difference equations at common fixed points of ϕ and ψ. Using estimates on coefficients in Taylor expansions one shows that certain formal power series converge in some open disks around these fixed points. Using the difference equations one writes down a functional equation for these functions, that allows to continue them meromorphically all the way up to a "natural boundary". While each of the three cases (2S), (2Q) and (2M) has its own peculiarities, and is technically different, the upshot in all three cases is that a certain matrix with meromorphic entries is proved to be *globally* meromorphic on $\mathbb{P}^1(\mathbb{C})$, hence a matrix with entries in $K = \mathbb{C}(x)$. This matrix is used to descend a certain difference module attached to our system of equations from K to $\mathbb{C}$, and this leads to a proof of Theorem 1.1.

In the case (2Ell) the analysis of the situation starts along the same lines. However, the matrix of globally meromorphic functions on $\mathbb{C}$ thus produced bears, a priori, no relation to the lattices Λ. It starts its life as a matrix of formal power series, convergent in some disk $|z| < \varepsilon$, and is then continued meromorphically using a functional equation with respect to $z \mapsto qz$, losing the connection to the lattices. In fact, examples show that this matrix *need not be* a matrix of elliptic functions.

The Periodicity Theorem of [16], and its vast generalization in [17], show that just enough of the periodicity can be salvaged to push this approach to an end. A certain generalization of the "baby case" of

this theorem, considered in [16], will be instrumental in the present work, when we deal with equations of the first order.

(iii) The second new issue in the case (2Ell) has to do with the emergence of certain *vector bundles* over the elliptic curve E_Λ, that we associate to our system of difference equations. Luckily, vector bundles over elliptic curves have been fully analyzed in Atiyah's work [4]. Their classification allows us to understand the (ϕ,ψ)-difference modules associated to an $f \in S_\phi(F/K) \cap S_\psi(F/K)$. The ensuing structure theorem for elliptic (ϕ,ψ)-difference modules is the main theorem of [17], and Theorem 1.3 is a corollary of it. The need to include $\zeta(z,\Lambda)$ in S reflects the non-triviality of these vector bundles. Over the field $\mathbb{C}(z)$ none of this shows up, essentially because every vector bundle over $\mathbb{G}_a$ or $\mathbb{G}_m$ is trivial.

1.3. The main results

Our main result is an elliptic analogue of Theorem 1.2 ([3, Theorem 1.3]). In fact, both our result and Theorem 1.2 admit a mild generalization. Let $AS_\psi(F/K)$ be the collection of all $u \in F$ for which there exists an $n \geqslant 0$ such that

$$\psi^n(u) \in K\left(u, \psi(u), \dots, \psi^{n-1}(u)\right).$$

Clearly $S_\psi(F/K) \subset AS_\psi(F/K)$.

THEOREM 1.4. — *Let (K,F,ϕ,ψ) be as in case (2Ell) and assume that $2 \leqslant p,q$ and $(p,q)=1$. Let $f \in S_\phi(F/K)$ and $g \in AS_\psi(F/K)$. If $f \notin S$ and $g \notin K$, then f and g are algebraically independent over K.*

Theorem 1.4 will be deduced from the following analogue of [3, Theorem 4.1], which concerns a *single* power series $f \in F$.

THEOREM 1.5. — *Let (K,F,ϕ,ψ) be as in case (2Ell) and assume that $2 \leqslant p,q$ and $(p,q)=1$. Let $f \in S_\phi(F/K)$ and assume that $f \notin S$. Then $\{f, \psi(f), \psi^2(f), \dots\}$ are algebraically independent over K.*

The two automorphisms ϕ and ψ do not show up in the last Theorem symmetrically. While f is assumed to satisfy a *linear* ϕ-difference equation, the conclusion is that, unless $f \in S$, it does not satisfy any *algebraic* ψ-difference equation. The roles of ϕ and ψ can be, of course, interchanged.

1.4. Survey of the proof and comparison to [3]

Although the proof of the two main theorems follows the general strategy of the rational case, treated in [3] (and, in a difference-differential context, in [2]), the elliptic case requires new ideas, and new phenomena arise. At the suggestion of the referee, we survey the strategy, and highlight the differences. Two of them have already been pointed out in the remark following Theorem 1.3.

To go further, we have to formally introduce the notion of a difference module, to which we already alluded several times. A *ϕ-difference module* (M, Φ) over K (called, in short, a ϕ-module) is a finite dimensional K-vector space M equipped with a ϕ-linear bijective endomorphism Φ. Its *rank* $\mathrm{rk}(M)$ is the dimension of M as a K-vector space. The set of Φ-fixed points M^Φ is a C-subspace of dimension $\leqslant \mathrm{rk}(M)$.

Since ψ commutes with ϕ, the module

$$M^{(\psi)} = (K \otimes_{\psi,K} M, \phi \otimes \Phi)$$

is another ϕ-module. Our M is called *ψ-isomonodromic* (or ψ-integrable) if $M \simeq M^{(\psi)}$.

To any ϕ-difference equation (1.1) one can attach a ϕ-module M of rank n whose fixed points M^Φ correspond to the solutions of the equation in K. This is classical, and explained in § 2.2 below. For this reason we shall refer to M^Φ also as the space of "solutions" of M.

To any ϕ-module M of rank n over K one can associate a *difference Galois group* $\mathcal{G}$, which is a Zariski closed subgroup of $GL_{n,\mathbb{C}}$, uniquely determined up to conjugation (and reviewed in § 2.5 below). This linear algebraic group measures the algebraic relations that exist between the solutions of M, not over K itself (where there might be none, or too few solutions), but after we have base-changed to a suitable universal extension (the Picard–Vessiot extension) in which a full set of solutions can be found. The larger $\mathcal{G}$ is, the fewer such relations exist. The analogy with classical Galois theory, in which the Galois group measures the algebraic relations between the roots of a polynomial in a splitting field, is obvious. It should be noted, however, that contrary to ordinary Galois theory, or to differential Galois theory, where splitting fields or Picard–Vessiot extensions are *fields*, in difference Galois theory one has to admit zero-divisors in the Picard–Vessiot extensions.

The input, deduced from the main theorem of [17], needed in the proof of Theorem 1.5, is the following. We continue to assume that $2 \leqslant p, q$ and $(p, q) = 1$.

THEOREM 1.6. — *Assume that M is ψ-isomonodromic. Then its difference Galois group $\mathcal{G}$ is solvable.*

This theorem, which does not show up in the rational case, is crucial for the "Galois theoretic" approach in the elliptic case, as eventually one uses an induction on the rank, and it is this solvability which allows us to carry out the induction.

We prove Theorem 1.6 in Section 4.1 below. It requires the full force of the classification theorem of elliptic (p, q)-difference modules from [17], and gives an affirmative answer to a question which was left open in that paper.

Both the rational case treated in [3] and the elliptic case treated here require, first of all, a reslution of the rank 1 case of the theorem. While this is fairly easy in the rational case, once the focus shifts to elliptic coefficients, issues of periodicity arise, just as they showed up in our our previous work [17]. It turns out that a suitable generalization of the "baby" Periodicity Theorem of [16], given in § 4.2, settles the rank 1 case of the theorem, and allows one to start the induction.

The rest of the proof of Theorems 1.4 and 1.5 imitates the Galois theoretic approach of [3]. As this depends on results scattered through many references [2, 3, 8, 6, 7, 11], we shall make an effort to collect all the prerequisites in a way that facilitates the reading.

1.5. Outline of the paper

Section 2 will be devoted to generalities on difference equations, difference modules, Picard–Vessiot extensions and the difference Galois group. The standard reference here is [13], although our language will sometimes be different.

Section 3 will be devoted to the more recent theory of *parametrized* Picard–Vessiot theory and the *parametrized* difference Galois group, to be found in the references cited above.

In Section 4 we shall prove the two results that we need as input in the proof of Theorem 1.5, relying on [16, 17].

Section 5 will start by explaining how to deduce Theorem 1.4 from Theorem 1.5. We shall then carry out the proof of Theorem 1.5, following the program of [3].

2. Review of classical Picard–Vessiot theory

2.1. The ground field

Let K be defined as in § 1.2, in the case (2Ell). We shall need the following facts about it. Recall that if G is a linear algebraic group over K, a *G-torsor* is a K-variety X, equipped with a simply transitive action of G. In other words, the morphism

$$G \times X \to X \times X, \quad (g, x) \mapsto (gx, x)$$

is an isomorphism. A G-torsor is *trivial* if it admits a K-point, i.e. if $X(K) \neq \emptyset$. A choice of $x_0 \in X(K)$ then gives an isomorphism $G \simeq X$, $g \mapsto gx_0$, compatible with the action of G on the left.

Proposition 2.1.

(i) *K is a C^1 field (any homogenous polynomial of degree d in $n > d$ variables has a nontrivial zero in K).*
(ii) *If G is a connected linear algebraic group over K then any G-torsor over K is trivial.*
(iii) *K does not have any non-trivial finite extension L/K to which ϕ (or ψ) extends as an automorphism.*

Proof. — (i) It is enough to prove the claim for every K_Λ, where this is Tsen's theorem: the function field of any curve over an algebraically closed field of characteristic 0 is a C^1-field.

(ii) This is Springer's theorem: a C^1-field of characteristic 0 is of cohomological dimension $\leqslant 1$. By Steinberg's theorem this implies that every torsor of a connected linear algebraic group over K is trivial. See [15, Chapter III.2].

(iii) (Compare [9, Proposition 6]). Suppose L is a finite extension of K to which ϕ extends as an automorphism. Then, for Λ small enough, $L = L_\Lambda K$ where L_Λ is an extension of K_Λ, $[L : K] = [L_\Lambda : K_\Lambda]$. Let $\Lambda' \subset \Lambda$ and $L_{\Lambda'} = L_\Lambda K_{\Lambda'}$. Then for Λ' sufficiently small $\psi(L_\Lambda) \subset L_{\Lambda'}$. Replacing Λ by Λ' we may therefore assume that $\psi(L_\Lambda) \subset L_\Lambda$. Thus ψ extends to an endomorphism of L_Λ. Let $\pi : Y \to E_\Lambda$ be the covering of complete nonsingular curves corresponding to $L_\Lambda \supset K_\Lambda$ and $\alpha : Y \to Y$ the morphism inducing ψ on L_Λ. Since $\pi \circ \alpha = [q] \circ \pi$ we get that $\deg(\alpha) = q^2$. By the Riemann–Hurwitz formula

$$2g_Y - 2 = (2g_Y - 2)q^2 + \sum_{x \in Ram(\alpha)} (e_x - 1)$$

where $g_Y \geqslant 1$ is the genus of Y and $Ram(\alpha)$ the ramification locus of α, e_x being the ramification index. This equation can only hold if $g_Y = 1$ (and α is everywhere unramified). In particular, π is an isogeny of elliptic curves, hence $L_\Lambda \subset K$ and $L = K$. □

Define

$$S = K\left[z, z^{-1}, \zeta(z,\Lambda)\right] \subset F.$$

If $\Lambda' \subset \Lambda$ is another lattice then

$$h(z) = \wp(z,\Lambda) - \sum_{\omega \in \Lambda/\Lambda'} \wp(z+\omega,\Lambda')$$

is a meromorphic Λ-periodic function. The poles of $\wp(z+\omega,\Lambda')$ are at the coset $-\omega + \Lambda'$. These cosets are disjoint and their union is just Λ, the set of poles of $\wp(z,\Lambda)$. Thus the poles of $h(z)$ are contained in Λ. But h is Λ-periodic and at 0 the poles of $\wp(z,\Lambda)$ and $\wp(z,\Lambda')$ cancel each other, as both start with z^{-2} + (holomorphic), while the other terms $\wp(z+\omega,\Lambda')$ ($\omega \notin \Lambda'$) are holomorphic. It follows that $h(z)$ has no poles at all, hence is a constant, $h(z) = a$. Integrating, we find that

$$\zeta(z,\Lambda) - \sum_{\omega \in \Lambda/\Lambda'} \zeta(z+\omega,\Lambda') = az + b$$

for some $a, b \in \mathbb{C}$. On the other hand $\zeta(z+\omega,\Lambda') - \zeta(z,\Lambda') \in K_{\Lambda'} \subset K$. It follows that

$$\zeta(z,\Lambda) - [\Lambda : \Lambda']\zeta(z,\Lambda') \in K\left[z, z^{-1}\right].$$

This shows that the definition of S does not depend on which $\Lambda \subset \Lambda_0$ we use. Since for any rational number $r = m/n$ $\zeta(rz,\Lambda) - r\zeta(z,\Lambda) \in K_{n\Lambda} \subset K$, ϕ and ψ induce automorphisms of S.

Problem. — Does the field of fractions of S satisfy Proposition 2.1?

We have not figured out the answer to this problem. It will not be needed in the sequel, and we mention it just for curiosity.

2.2. Difference equations, difference systems and difference modules

In this subsection and the next ones, the ϕ-field (K,ϕ) can be arbitrary. The standard reference is [13]. As usual, to the difference equation (1.1) we

associate the companion matrix

$$A = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & & \\ & & & 0 & 1 \\ -a_n/a_0 & & \cdots & & -a_1/a_0 \end{pmatrix},$$

and the first order linear system of equations

$$\phi(Y) = AY \tag{2.1}$$

for which we seek solutions $Y = {}^t(u_1, \ldots, u_n)$ in ϕ-ring extensions L of K. Notice that if u is a solution of (1.1) then ${}^t(u, \phi(u), \ldots, \phi^{n-1}(u))$ is a solution of (2.1).

From now on we concentrate on first order systems of equations of the form (2.1) with $A \in GL_n(K)$ *arbitrarily given*.

With the system (2.1) we associate the ϕ-difference module $M = (K^n, \Phi)$ where

$$\Phi(v) = A^{-1}\phi(v).$$

Notice that a solution $v \in K^n$ to (2.1) is nothing but an element of M^Φ, the fixed points of Φ in M. This is a $C = K^\phi$-subspace, and the well-known Wronskian Lemma shows that

$$\dim_C M^\Phi \leqslant \mathrm{rk}M.$$

By abuse of language, we shall refer to M^Φ also as the space of "solutions" of M.

An equality $\dim_C M^\Phi = \mathrm{rk}M$ holds if and only if a full set of solutions of (2.1) exists in K, if and only if M is isomorphic to the trivial module (K^n, ϕ). In such a case a matrix $U \in GL_n(K)$ satisfying

$$\phi(U) = AU$$

is called a *fundamental matrix*for (2.1). Its columns form a basis of M^Φ over C.

Given any ϕ-module, a choice of a basis of M over K shows that it is of the above form. A choice of another basis results in a *gauge transformation*, replacing A with

$$A' = \phi(P)^{-1}AP$$

for some $P \in GL_n(K)$. Conversely, the systems of equations defined by A and by A' are equivalent if and only if A and A' are gauge equivalent. The transition from a system of equations to a ϕ-module can therefore be reversed. Thanks to Birkhoff's cyclicity lemma, the transition from a single

linear equation of order n to a system of equations of order one can also be reversed. The three notions are therefore equivalent, and which language one chooses to work with is very much a matter of taste.

2.3. Isomonodromy and (Φ, Ψ)-difference modules

Assume now that the ϕ-field K is endowed with a second automorphism ψ, *commuting* with ϕ. If (M, Φ) is a ϕ-module over K, then

$$M^{(\psi)} = (K \otimes_{\psi, K} M, \phi \otimes \Phi)$$

is another ϕ-module, called the ψ-*transform* of M. For $a, b \in K$ and $m \in M$ we have $a \otimes bm = a\psi(b) \otimes m$, and $\lambda \in K$ acts on $M^{(\psi)}$ by multiplication by $\lambda \otimes 1$. If $M = (K^n, \Phi)$ with $\Phi(v) = A^{-1}\phi(v)$ then $M^{(\psi)}$ is likewise given by the matrix $\psi(A)$.

The notion of a (ϕ, ψ)-difference module is naturally defined. It is a finite dimensional vector space M over K equipped with bijective ϕ-linear (resp. ψ-linear) endomorphisms Φ (resp. Ψ) commuting with each other: $\Phi \circ \Psi = \Psi \circ \Phi$.

LEMMA 2.2. — *For a ϕ-module M over K of rank n, the following are equivalent:*

(i) *$M^{(\psi)} \simeq M$ as a ϕ-module.*
(ii) *M admits a structure of a (ϕ, ψ)-module extending the given ϕ-module structure.*
(iii) *If $A = A_\phi$ is the matrix associated to M in some basis, there exists a matrix $A_\psi \in GL_n(K)$ satisfying the compatibility condition*

$$\phi(A_\psi)A_\phi = \psi(A_\phi)A_\psi.$$

The proof is left as an easy exercise. A ϕ-module satisfying the above conditions is called ψ-*isomonodromic* (or ψ-integrable). Property (iii) shows that the definition is symmetric: If (M, Φ) is ψ-isomonodromic and Ψ is the ψ-linear operator as in (ii), then (M, Ψ) is ϕ-isomonodromic as a ψ-module. The terminology is derived from the differential set-up, of which the theory of difference equations is a discrete analogue.

2.4. Picard–Vessiot theory

A general reference for the topics reviewed in this section is [13, Chapter 1]. [11, Section 2.2] is another good survey.

2.4.1. Picard–Vessiot rings and extensions

It is natural to look for an extension of K in which (2.1) attains a full set of solutions, or, equivalently, over which the associated module M is trivialized, after base change. Easy examples show that such an extension might have to have zero divisors. The best we can do is encapsulated in the following definition.

DEFINITION 2.3.

(i) *A* ϕ-ring *is a commutative unital ring* R *equipped with an* endomorphism ϕ. *It is called* ϕ-simple *if it does not have any non-zero ideals* I *invariant under* ϕ, *i.e. satisfying* $\phi(I) \subset I$.

(ii) *A* Picard–Vessiot (PV) ring *for the* ϕ*-module* M *(associated to* $A \in GL_n(K)$ *as above) is a simple* ϕ*-ring extension* (R, ϕ) *of* (K, ϕ) *over which* $M_R = (R \otimes_K M, \phi \otimes \Phi)$ *is trivialized (i.e. becomes isomorphic to* (R^n, ϕ)*), and such that* $R = K[u_{ij}, \det(U)^{-1}]$ *if* $U = (u_{ij}) \in GL_n(R)$ *is a fundamental matrix of* (2.1).

Here are the main properties of PV rings.

- PV rings exist, are noetherian and (like any ϕ-simple ring) reduced. Furthermore, a PV ring R is a finite product $R_1 \times \cdots \times R_t$ of integral domains, permuted cyclically by ϕ.
- Since ϕ was assumed to be an automorphism of K and A is invertible, a PV ring R happens to be *inversive:* ϕ is an automorphism of R.
- The field of constants $C_R = R^\phi$ is an algebraic extension of $C = K^\phi$. If C is algebraically closed, $C = C_R$.
- The fundamental matrix $U \in GL_n(R)$ is unique up to $U \mapsto UV$ with $V \in GL_n(C_R)$.
- If C is algebraically closed, any two PV rings for M are (noncanonically) isomorphic.
- Let $L = Quot(R)$ be the total ring of fractions of R (the localization of R in the ϕ-invariant multiplicative set of non-zero divisors of R). Thus $L = L_1 \times \cdots \times L_t$ is a finite product of fields, which are permuted cyclically by ϕ. We have $L^\phi = C_R$. A ϕ-ring L of this type is a called a ϕ*-pseudofield*.

Assume from now on that C is algebraically closed.

LEMMA 2.4 ([11, Corollary 2.15]). — *Let* L *be a* ϕ*-pseudofield extension of* K *which trivializes* M *and is generated over* K *(as a pseudofield) by the entries* u_{ij} *of a fundamental matrix* U. *Suppose that* $L^\phi = C$. *Then*

$R = K[u_{ij}, \det(U)^{-1}] \subset L$ is ϕ-simple, hence it is a PV ring for M, and L is its total ring of fractions.

The last lemma is of great practical value, because it is often much easier to check that $L^{\phi} = C$ then to verify directly that R is ϕ-simple. The ϕ-pseudofield L is called the PV *extension* associated with M.

- Notation as above, L_1 is a ϕ^t-PV extension for (M, Φ^t) over (K, ϕ^t). Indeed, it is a ϕ^t-field, generated over K by the entries of U, and $L_1^{\phi^t} = C$. Note that the matrix associated to (M, Φ^t) is

$$A_{[t]} = \phi^{t-1}(A) \cdots \phi(A)A.$$

  Thus, at the expense of replacing ϕ by a suitable power, we may assume that L is a field and R a domain. In the current paper, this will turn out to be always possible.

A PV ring R for (2.1) is constructed as follows. Let $X = (X_{ij})$ be an $n \times n$ matrix of indeterminates. Let ϕ act on the ring $\widetilde{R} = K[X_{ij}, \det(X)^{-1}]$ via its given action on K and the formula

$$\phi(X) = AX,$$

i.e. $\phi(X_{ij}) = \sum_{\nu=1}^{n} a_{i\nu} X_{\nu j}$. Let I be a maximal ϕ-invariant ideal in $\widetilde{R}$. Then

$$R = \widetilde{R}/I$$

is a PV ring for (2.1), and $U = X \mod I$ is a fundamental matrix in $GL_n(R)$. We remark that since $\widetilde{R}$ is noetherian, any ϕ-invariant ideal I satisfies $\phi(I) = I$. A maximal ϕ-invariant I is radical, and R is therefore reduced.

The reduced K-scheme $W = Spec(R)$ is called the PV *scheme* associated with R. Since the choice of a fundamental matrix U amounts to a presentation $R = \widetilde{R}/I$ as above, the choice of U determines a closed embedding

$$W \hookrightarrow GL_{n,K}.$$

In general, the K-scheme W might not have any K-points. We shall see soon (Proposition 2.5) that if K satisfies the conclusions of Proposition 2.1, $W(K) \neq \emptyset$. This will be an important observation in our context.

2.4.2. The map τ

If $h \in GL_n(K) = \mathrm{Hom}_K(K[X_{ij}, \det(X)^{-1}], K)$ we let

$$\tau(h) = \phi \circ h \circ \phi^{-1} \in GL_n(K).$$

If $X_h = h(X)$ is the matrix in $GL_n(K)$ representing the K-point h, then since $\phi^{-1}(X) = \phi^{-1}(A)^{-1}X$ we have

$$X_{\tau(h)} = \tau(h)(X) = A^{-1}\phi(X_h).$$

If $h \in W(K)$, i.e. h factors through I, then since $\phi^{-1}(I) = I$, so does $\tau(h)$. Regarded as a subset of $GL_n(K)$, if $P \in W(K)$ then

$$\tau(P) = A^{-1}\phi(P) \in W(K).$$

The set of K-points of the Picard–Vessiot scheme is therefore, if not empty, invariant under τ.

2.5. The difference Galois group of (M, Φ)

We continue to assume that $C = K^\phi$ is algebraically closed. Let (M, Φ) be a ϕ-module, A the matrix associated to it in some basis, R a PV ring and $L = Quot(R)$ the associated PV extension.

Let B be a C-algebra, with a trivial ϕ-action. Writing $-_B = B \otimes_C -$ we let

$$\mathcal{G}(B) = \mathrm{Aut}_\phi(R_B/K_B)$$

be the group of automorphisms of R_B that fix K_B pointwise and commute with ϕ. An element $\sigma \in \mathcal{G}(B)$ induces an action on the total fraction ring $Quot(R_B)$, which contains L_B. While this action need not preserve L_B, it makes sense to say that an element of L_B is invariant under the action of a subgroup $\mathcal{H}$ of $\mathcal{G}(B)$, and the set $L_B^{\mathcal{H}}$ of $\mathcal{H}$-invariant elements is a subring of L_B containing K_B.

The assignment $B \mapsto \mathcal{G}(B)$ yields a functor

$$\mathcal{G} : \mathrm{Alg}_C \rightsquigarrow \mathrm{Groups}.$$

Then:

- $\mathcal{G}$ is representable by a closed subgroup scheme of $GL_{n,C}$. We write $\mathcal{G}$, or $Gal(L/K)$, for the affine group scheme representing the functor. If $\sigma \in \mathcal{G}(B)$

  $$\sigma(U) = U \cdot V(\sigma)$$

  with $V(\sigma) \in GL_n(B)$ and $\sigma \mapsto V(\sigma)$ embeds $\mathcal{G}$ in $GL_{n,C}$. If $char(C) = 0$ then $\mathcal{G}$ is reduced, but in positive characteristic we must include the possibility of non-reduced $\mathcal{G}$.

- If A is replaced by $\phi(P)^{-1}AP$ (change of basis of M, $P \in GL_n(K)$) and U is replaced by $P^{-1}U$ then, since $\sigma(P) = P$, we get *the same embedding* $\mathcal{G} \hookrightarrow GL_{n,C}$. If U is replaced by another fundamental matrix for (2.1), necessarily of the form UT with $T \in GL_n(C)$, then $V(\sigma)$ is replaced by $T^{-1}V(\sigma)T$. Thus $\mathcal{G}$ *is uniquely determined up to conjugation by an element of* $GL_n(C)$.
- The coordinate ring of $\mathcal{G}$ is given by $C[\mathcal{G}] = (R \otimes_K R)^{\phi}$. Let
$$Z = \left(U^{-1} \otimes 1\right) \cdot (1 \otimes U) \in GL_n(R \otimes_K R),$$
i.e. $Z_{ij} = \sum_{\nu=1}^{n} (U^{-1})_{i\nu} \otimes U_{\nu j}$. Then
$$\phi(Z) = \left(U^{-1} \otimes 1\right) \cdot \left(A^{-1} \otimes 1\right) \cdot (1 \otimes A) \cdot (1 \otimes U) = Z$$
so $Z_{ij} \in C[\mathcal{G}]$. In fact, $C[\mathcal{G}] = C[Z_{ij}, \det Z^{-1}]$. We have
$$\sigma \in \mathcal{G}(B) = \mathrm{Hom}(C[\mathcal{G}], B) \leftrightsquigarrow (Z \mapsto V(\sigma))$$
and $\mathcal{G} \hookrightarrow GL_{n,C}$ implies the comultiplication
$$m^*(Z) = Z \otimes Z,$$
i.e. $m^*(Z_{ij}) = \sum_{\nu=1}^{n} Z_{i\nu} \otimes Z_{\nu j}$.
- Inside $R \otimes_K R$ we have the canonical isomorphism
$$R \otimes_K K[\mathcal{G}] = R \otimes_C C[\mathcal{G}] \simeq R \otimes_K R$$
(since $(U \otimes 1) \cdot Z = 1 \otimes U$), which means that $W = Spec(R)$ is a *torsor* of $\mathcal{G}_K$. We conclude that $W(K) \neq \emptyset$ is a necessary and sufficient condition for W to be the trivial torsor, i.e. to be (noncanonically) isomorphic to $\mathcal{G}_K$.
- If L is a field, $\mathrm{tr.deg.}L/K = \dim \mathcal{G}$.

PROPOSITION 2.5. — *Assume that* $char(C) = 0$ *and that* K *satisfies the conclusions of Proposition 2.1 for every power of* ϕ. *Then* $W(K) \neq \emptyset$.

Proof. — If $\mathcal{G}$ is connected, this follows from part (ii) of Proposition 2.1. Following [13, Proposition 1.20] we explain how part (iii) of the same Proposition allows us to get rid of the assumption that $\mathcal{G}$ is connected. Let
$$R = R_1 \times \cdots \times R_t$$
be the decomposition of R into a product of integral domains, permuted cyclically by ϕ. Since K does not have any finite extension to which ϕ^t extends, it is algebraically closed in the field $L_i = Quot(R_i)$. This means that $W_i = Spec(R_i)$ remains irreducible over the algebraic closure $\overline{K}$ of K. It follows that one of the W_i, say W_1, is a torsor of $\mathcal{G}_K^0$. Since $\mathcal{G}_K^0$ is connected, $W_1(K) \neq \emptyset$, hence $W(K) \neq \emptyset$. □

We continue to assume, as in the Proposition, that C is algebraically closed of characteristic 0.

THEOREM 2.6 ([13] Theorem I.1.21).

(i) *Let $H \subset GL_{n,C}$ be a closed subgroup. If in some basis $A \in H(K)$, then we can choose $U \in H(R)$ and $\mathcal{G} \subset H$. For a general fundamental matrix $U \in GL_n(R)$, some conjugate of $\mathcal{G}$ by an element of $GL_n(C)$ will be contained in H.*

(ii) *Assume that the conclusions of Proposition 2.1 hold. Then conversely, there exists a basis of M with respect to which $A \in \mathcal{G}(K)$. Equivalently, for the original A there exists a $P \in GL_n(K)$ such that $\phi(P)^{-1}AP \in \mathcal{G}(K)$.*

(iii) *Under the assumptions of (ii) $\mathcal{G}$ is characterized (up to conjugation by $GL_n(C)$) as a* minimal *element of the set*

$$\mathscr{H} = \left\{ H \subset GL_{n,C} \,\middle|\, H \text{ closed}, \ \exists\, P \in GL_n(K) \text{ s.t.} \quad \phi(P)^{-1}AP \in H(K) \right\}.$$

Every other element of $\mathscr{H}$ therefore contains a conjugate of $\mathcal{G}$.

(iv) *$\mathcal{G}/\mathcal{G}^0$ is cyclic.*

Proof. — (i) Assume $A \in H(K)$, and H is given explicitly as

$$Spec\left(C\left[X_{ij}, \det(X)^{-1}\right]/N\right)$$

where N is a Hopf ideal. Let ϕ act on $K[X_{ij}, \det(X)^{-1}]$ via the given action on K and via $\phi(X) = AX$. Then N_K is a ϕ-ideal because if $f \in N$ then

$$\phi(f) = (\alpha \times 1) \circ m^*(f)$$

where m^* is the comultiplication and α the homomorphism $C[X_{ij}, \det(X)^{-1}] \to K$ substituting A for X. But

$$m^*(f) \in N \otimes_C C\left[X_{ij}, \det(X)^{-1}\right] + C\left[X_{ij}, \det(X)^{-1}\right] \otimes_C N$$

and $\alpha(N) = 0$ since $A \in H(K)$. Thus $\phi(f) \in K \otimes_C N = N_K$.

Let I be a maximal ϕ-ideal in $K[X_{ij}, \det(X)^{-1}]$ *containing* N_K and $U = X \mod I$. Then

$$W = Spec(R) = Spec\left(K\left[X_{ij}, \det(X)^{-1}\right]/I\right) \subset H_K$$

is the PV scheme, and $U \in H(R)$ (corresponding to the canonical homomorphism $C[X_{ij}, \det(X)^{-1}]/N \to K[X_{ij}, \det(X)^{-1}]/I$.) It follows that for $\sigma \in \mathrm{Aut}_\phi(R_B/K_B)$ we have $\sigma(U) \in H(R_B)$, hence

$$V(\sigma) = U^{-1}\sigma(U) \in H(R_B)^\phi = H(B).$$

Any other fundamental matrix is of the form UT with $T \in GL_n(C)$, so $T\mathcal{G}T^{-1} \subset H$.

(ii) Under our assumptions, $W(K)$ is non-empty. Any $P \in W(K) \subset GL_n(K)$ satisfies

$$W = P\mathcal{G}_K.$$

Since $\tau(P) \in W(K)$ as well (see 2.4.2), $\tau(P)^{-1}P = \phi(P)^{-1}AP \in \mathcal{G}(K)$ and there exists a basis of M for which $A \in \mathcal{G}(K)$.

(iii) By (i) every member of $\mathscr{H}$ contains $\mathcal{G}$ up to conjugacy. By (ii) every $\mathcal{G}$ (uniquely determined up to conjugacy) belongs to $\mathscr{H}$. Thus $\mathcal{G}$ is the unique minimal member of $\mathscr{H}$, up to conjugacy. Note that it is not a-priori clear that all the minimal members of $\mathscr{H}$ are conjugate, but this follows from the proof.

(iv) See [13]. □

2.6. The Galois correspondence

Let R be a PV ring for M and L its total ring of fractions. Let $\mathcal{G}$ be the difference Galois group of M.

We quote the following basic theorem. We say that $a \in L$ is fixed by $\mathcal{G}$ and write $a \in L^{\mathcal{G}}$ if for every $B \in \mathrm{Alg}_C$ the element $1 \otimes a \in L_B$ is fixed[(2)] by $\mathcal{G}(B)$. The set $L^{\mathcal{G}}$ is a ϕ-sub-pseudofield of L. The same definition applies if we replace $\mathcal{G}$ by a Zariski closed subgroup $\mathcal{G}'$.

THEOREM 2.7.

(i) *For any closed subgroup $\mathcal{G}' \subset \mathcal{G}$ let*

$$\mathscr{F}(\mathcal{G}') = K' = L^{\mathcal{G}'},$$

a ϕ-sub-pseudofield of L containing K. For any ϕ-pseudofield $K \subset K' \subset L$ let $\mathscr{G}(K') = \mathcal{G}'$ be the closed subgroup of $\mathcal{G}$ whose B-points, for $B \in \mathrm{Alg}_C$, are

$$\mathscr{G}(K')(B) = \mathcal{G}'(B) = \mathrm{Aut}_\phi(R_B/K'_B \cap R_B).$$

Then $\mathcal{G}' \mapsto K' = \mathscr{F}(\mathcal{G}')$ and $K' \mapsto \mathcal{G}' = \mathscr{G}(K')$ is a 1-1 correspondence between closed subgroups of $\mathcal{G}$ and ϕ-sub-pseudofields of L containing K. In particular $L^{\mathcal{G}} = K$.

(ii) *$\mathcal{G}'$ is normal in $\mathcal{G}$ if and only if K' is a PV extension of some difference ϕ-module M'. In this case the difference Galois group of K'/K is $\mathcal{G}/\mathcal{G}'$.*

(2) By the remark at the beginning of § 2.5 this phrase is meaningful.

(iii) *$\mathcal{G}^0$ corresponds to the algebraic closure of K in L. If we assume (replacing ϕ by some ϕ^r) that L is a field, then since L is a finitely generated field extension of K, the algebraic closure of K in L is a finite extension. Under Proposition 2.1*(iii) *we conclude that K must be algebraically closed in L, hence $\mathcal{G}$ must be connected.*

2.7. An example

Let K and ϕ be as in case (Ell). Let $A \in GL_2(K)$ be the matrix

$$A = \begin{pmatrix} q & g_q(z,\Lambda) \\ 0 & 1 \end{pmatrix}$$

where $g_q(z,\Lambda) = \zeta(qz,\Lambda) - q\zeta(z,\Lambda) \in K$. The matrix

$$U = \begin{pmatrix} z & \zeta(z,\Lambda) \\ 0 & 1 \end{pmatrix}$$

is a fundamental matrix for the system $\phi(Y) = AY$. The field

$$E = K(z, \zeta(z,\Lambda))$$

is therefore a PV extension for that system, since (i) ϕ induces an automorphism of E, (ii) E is generated by the entries of U, and (iii) its field of constants is $\mathbb{C}$.

The difference Galois group is

$$\mathcal{G} = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \middle| \, \alpha, \beta \in \mathbb{C} \right\}.$$

The automorphism $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & 1 \end{smallmatrix}\right)$ acts on E via

$$\sigma(z) = \alpha z, \quad \sigma\zeta(z,\Lambda) = \zeta(z,\Lambda) + \beta z.$$

The unipotent subgroup ($\alpha = 1$) is normal, and corresponds, in the Galois correspondence, to $K(z)$. The field $K(\zeta(z,\Lambda))$ is also a ϕ-subfield corresponding to the torus ($\beta = 0$), but is not a normal extension of K. Note that this field, unlike E, depends on the lattice Λ.

2.8. Filtrations and descent

As before, let K be a ϕ-field with an algebraically closed field of constants $C = K^\phi$ of characteristic 0, (M,Φ) a ϕ-difference module over K of

rank n, and $R \subset L$ the associated PV ring and extension (unique up to isomorphism). Let $\mathcal{G} = Gal(L/K)$ be the difference Galois group of M.

For simplicity, assume that L is a field.

Let $M_L = L \otimes_K M$ and

$$\mathcal{V} = \mathcal{V}_L(M) = (L \otimes_K M)^{\Phi_L},$$

where $\Phi_L = \phi \otimes \Phi$. Then $\mathcal{V}$, the space of solutions of M_L, is n-dimensional over C. If

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of ϕ-modules, and $\mathrm{rk}(M') = m$, then the sequence

$$0 \to \mathcal{V}_L(M') \to \mathcal{V}_L(M) \to \mathcal{V}_L(M'') \to 0$$

is left exact. Since $\dim_C \mathcal{V}_L(M') \leqslant m$ and $\dim_C \mathcal{V}_L(M'') \leqslant n - m$, while $\dim_C \mathcal{V}_L(M) = n$, we conclude

(a) that the above sequence is exact also on the right,
(b) that M' and M'' attain a full set of solutions over L (i.e. the above inequalities are equalities).

Note that L will, in general, be larger than a PV extension for M' or M''.

The homomorphism

$$L \otimes_C \mathcal{V} \xrightarrow{\sim} L \otimes_K M, \;\; a \otimes v \mapsto a \cdot v,$$

is an isomorphism. The proof that it is injective is standard: if $0 \neq \sum_{i=1}^{r} a_i \otimes v_i$ maps to 0, where the a_i are linearly independent over C, we may assume that r is minimal and that $a_1 = 1$. Applying $\Phi_L - 1$ we arrive at a shorter element in the kernel, so that element must vanish, and we must have $\phi(a_i) = a_i$ for all i. This forces $a_i \in C$, a contradiction. Once injectivity has been established, a dimension count shows that the homomorphism is bijective.

Applying Φ_L, one recovers $\mathcal{V}$ from $L \otimes_C \mathcal{V}$ as its fixed part. We can also recover M as the fixed part under $\mathcal{G}$ (in the sense of § 2.6). Since C is algebraically closed of characteristic 0, we may identify the algebraic group $\mathcal{G}$ with the group of its C-points $\mathcal{G}(C)$. Note that the latter acts on $L = Quot(R)$, and not only on R. Letting $\mathcal{G}$ act trivially on M we get an action of $\mathcal{G}$ on $\mathcal{V} = (L \otimes_K M)^{\Phi_L}$, well defined by the fact that any $\sigma \in \mathcal{G}$ commutes with ϕ and fixes K. In the language of matrices, if $M = K^n$ with $\Phi(v) = A^{-1}\phi(v)$ as before, and U is a fundamental matrix with entries in L, then

$$\mathcal{V} = UC^n \subset L^n = M_L,$$

and the embedding $\sigma \mapsto V(\sigma) \in GL_n(C)$ yields the matrix representation of $\mathcal{G}$ on $\mathcal{V}$ in the basis given by the columns of U. Thus

$$M = (L \otimes_K M)^{\mathcal{G}} \simeq (L \otimes_C \mathcal{V})^{\mathcal{G}}$$

where $\sigma \in \mathcal{G}$ acts on $L \otimes_C \mathcal{V}$ diagonally.

Suppose now that

$$0 \to \mathcal{V}' \to \mathcal{V} \to \mathcal{V}'' \to 0$$

is a short exact sequence of C-vector spaces. Then letting $\Phi' = \phi \otimes 1$ on $N' = L \otimes_C \mathcal{V}'$ and similarly Φ'' on $N'' = L \otimes_C \mathcal{V}''$, we get a short exact sequence

$$0 \to N' \to M_L \to N'' \to 0 \tag{2.2}$$

of trivial ϕ-modules over L. We say that this short exact sequence (or filtration of M_L) *descends* to K if there exists a short exact sequence $0 \to M' \to M \to M'' \to 0$ of ϕ-modules over K, with $N' = M'_L$ and $N'' = M''_L$.

PROPOSITION 2.8. — *A necessary and sufficient condition for* (2.2) *to descend to K is that $\mathcal{V}'$ be invariant under $\mathcal{G}$.*

Proof. — If $\mathcal{V}'$ is $\mathcal{G}$-invariant we can define a ϕ-module $M' = (L \otimes_C \mathcal{V}')^{\mathcal{G}}$ over K. The map $L \otimes_K M' \to L \otimes_C \mathcal{V}'$ is shown to be injective by the same "trick" as above, using the action of $\mathcal{G}$ instead of the action of Φ_L. It follows that $\mathrm{rk}(M') \leqslant \dim_C \mathcal{V}'$. Similarly define M'' and infer $\mathrm{rk}(M'') \leqslant \dim_C \mathcal{V}''$. As above we conclude from the equality $\mathrm{rk}(M) = \dim_C \mathcal{V}$ that

$$0 \to M' \to M \to M'' \to 0$$

is not only left exact, but exact, and that $\mathrm{rk}(M') = \dim_C \mathcal{V}'$, $\mathrm{rk}(M'') = \dim_C \mathcal{V}''$. It follows that $M'_L = N'$ and $M''_L = N''$.

Conversely, if M' exists then $\mathcal{V}' = (L \otimes_K M')^{\Phi'}$ is clearly $\mathcal{G}$-invariant. □

3. Review of parametrized Picard-Vessiot theory

3.1. ψ-linear algebraic groups

3.1.1. Generalities

In this section C will be an algebraically closed field of characteristic 0, equipped with an automorphism ψ (denoted σ in most of the references). For example, if K is a (ϕ, ψ)-field and $C = K^{\phi}$ then C inherits an action

of ψ, although this action might well be trivial, as it is in the case (2Ell). We let Alg_C^{ψ} denote the category of C-ψ-algebras[(3)]. All our schemes and ψ-schemes will be affine. If $R \in \mathrm{Alg}_C^{\psi}$ we denote by $Spec^{\psi}(R)$ the functor

$$Spec^{\psi}(R) : \mathrm{Alg}_C^{\psi} \to \mathrm{Sets}$$

defined by $Spec^{\psi}(R)(S) = \mathrm{Hom}_C^{\psi}(R, S)$ (homomorphisms of C-ψ-algebras). Note that if $h \in Spec^{\psi}(R)(S)$ then $\psi(h) = \psi \circ h = h \circ \psi \in Spec^{\psi}(R)(S)$ as well, so the functor factors through the category of ψ-sets.

Let L be a ψ-field extension of C. A subset $\{a_1, \ldots, a_n\}$ of L is called *ψ-algebraically independent* over C if the collection $\{\psi^i a_j | \, 0 \leqslant i, \ 1 \leqslant j \leqslant n\}$ is algebraically independent over C. The ψ-transcendence degree of L over C, denoted $\psi\mathrm{tr.deg.}(L/C)$, is the cardinality of a maximal ψ-algebraically independent set in L. This notion is well defined (any two such maximal sets have the same cardinality).

We refer to [6, Appendix A] for an introduction to ψ-schemes and ψ-group schemes. A *ψ-algebraic group* G over C is a ψ-group scheme that is *ψ-algebraic* over C. This means that its coordinate ring $C\{G\}$ is finitely ψ-generated over C : it contains a finite set $\{u_1, \ldots, u_n\}$ such that $\psi^i(u_j)$ for $0 \leqslant i$ and $1 \leqslant j \leqslant n$ generate $C\{G\}$ as a C-algebra. It is called *ψ-reduced* if ψ is injective on $C\{G\}$, *perfectly ψ-reduced* if the equation $u^{e_0}\psi(u)^{e_1} \cdots \psi^m(u)^{e_m} = 0$ ($e_i \geqslant 0$) forces $u = 0$ in $C\{G\}$, and *ψ-integral* if $C\{G\}$ is an integral domain and ψ is injective.

If G is a ψ-algebraic group over C its ψ-dimension is a non-negative integer, defined in [6, Definition A.25]. If G is ψ-integral then

$$\psi\dim(G) = \psi\mathrm{tr.deg.}(Quot(C\{G\})/C).$$

If $\mathcal{G}$ is a (classical) algebraic group over C then the functor $B \mapsto \mathcal{G}(B^{\flat})$ from Alg_C^{ψ} to Groups, where $B^{\flat}$ is the C-algebra B with the ψ-structure forgotten, is representable by a ψ-algebraic group that we denote $[\psi]\mathcal{G}$. Suppose $\mathcal{G}$ is exhibited as a closed subgroup of $GL_{n,C}$, so that

$$\mathcal{G} = Spec\left(C\left[X_{ij}, \det(X)^{-1}\right]/I\right) \tag{3.1}$$

where $1 \leqslant i, j \leqslant n$ and I is a Hopf ideal. Then $G = [\psi]\mathcal{G} = Spec^{\psi}C\{G\}$ where $C\{G\} = C[\psi^k X_{ij}, \det \psi^k(X)^{-1}]/I_{\psi}$, $0 \leqslant k < \infty$, the $\psi^k X_{ij}$ are symbols treated as independent variables, the ψ-action is the obvious one,

(3) *It is important, when developing the general formalism, to abandon the requirement that ψ be invertible on a general C-ψ-algebra. Thus while we maintain the assumption that ψ is an automorphism of C, hence (C, ψ) is "inversive", we must allow rings in which ψ is only an endomorphism, perhaps not even injective, in the category* Alg_C^{ψ}.

and I_ψ is the Hopf ψ-ideal generated by all $\psi^k(h)$ for $h \in I$. As might be expected,

$$\psi \dim([\psi]\mathcal{G}) = \dim(\mathcal{G}).$$

As a non-trivial example of a ψ-algebraic group, consider the ψ-closed subgroup of $[\psi]\mathbb{G}_m$ given by the equation

$$X^{e_0}\psi(X)^{e_1}\cdots\psi^m(X)^{e_m} = 1 \tag{3.2}$$

for some $e_i \in \mathbb{Z}$ (here $\mathbb{G}_m = Spec(C[X, X^{-1}])$.

By [6, Lemma A.40] any closed ψ-subgroup of $[\psi]\mathbb{G}_m$ is defined by a (possibly infinite) collection of ψ-monomials of the form (3.2). All that we shall need is the following weaker result.

LEMMA 3.1. — *If $G \subsetneq [\psi]\mathbb{G}_m$ is a proper closed ψ-subgroup of the multiplicative group, then there exists a non-trivial ψ-monomial of the form* (3.2) *satisfied by G, and $\psi \dim(G) = 0$.*

3.1.2. (Classical) Zariski closure

Let $\mathcal{G}$ be a (classical) linear algebraic group over C and $G \subseteq [\psi]\mathcal{G}$ a ψ-closed subgroup. We say that G is *Zariski dense* in $\mathcal{G}$ if for any proper subvariety (or subgroup, since G is a group functor, this will turn out to be the same) $\mathcal{H} \subset \mathcal{G}$, $G \nsubseteq [\psi]\mathcal{H}$. If $\mathcal{G}$ is a subgroup of $GL_{n,C}$ given by the Hopf algebra (3.1), and

$$G = Spec^\psi\left(C\left[\psi^k X_{ij}, \det \psi^k(X)^{-1}\right]/J\right)$$

for a Hopf ψ-ideal J, a necessary and sufficient condition for G to be Zariski dense in $\mathcal{G}$ is that $J \cap C[X_{ij}, \det(X)^{-1}] = I$, i.e. the "ordinary" equations, not involving ψ, in the ideal defining G, are just those defining $\mathcal{G}$. In such a case $I_\psi \subset J$, because J is a ψ-ideal and I_ψ is the smallest ψ-ideal containing I, but this inclusion might be strict if $G \subsetneq [\psi]\mathcal{G}$.

Conversely, starting with a ψ-algebraic group G presented in the above form, and defining

$$J \cap C\left[X_{ij}, \det(X)^{-1}\right] =: I$$

one sees that I is Hopf ideal in $C[X_{ij}, \det(X)^{-1}]$ and the algebraic group $\mathcal{G}$ that it defines is the (classical) *Zariski closure* of G.

3.1.3. The structure of ψ-linear algebraic groups whose Zariski closure is simple

We shall need the following result, which, for simplicity, we only state in the case: $C = \mathbb{C}$ and ψ is the identity. It shows that if $\mathcal{G}$ is *simple*, proper ψ-subgroups of $[\psi]\mathcal{G}$, which are nevertheless Zariski dense in it, are (under a mild technical condition of ψ-reducedness) of a very special form. Alternatively, one may start with an arbitrary ψ-reduced ψ-linear group G and ask (i) that it be *properly contained* in its (classical) Zariski closure, i.e. G "is not classical", and (ii) that this Zariski closure be simple[(4)].

PROPOSITION 3.2 ([7, Proposition A.19 and Theorem A.20]). — *Let $\mathcal{G}$ be a* simple *linear algebraic group over $\mathbb{C}$ and $G \subsetneq [\psi]\mathcal{G}$ a* proper, *ψ-closed, ψ-reduced subgroup of $[\psi]\mathcal{G}$. Assume that G is Zariski dense in $\mathcal{G}$. Then there exists an automorphism $\alpha \in \mathrm{Aut}(\mathcal{G})$ and an integer $m \geqslant 1$ such that*

$$G(B) = \{g \in \mathcal{G}(B) \,|\, \psi^m(g) = \alpha(g)\}$$

for every $B \in \mathrm{Alg}_{\mathbb{C}}^{\psi}$. Furthermore, replacing m by a multiple of it we find that there exists an $h \in \mathcal{G}(\mathbb{C})$ such that

$$G(B) \subset \left\{g \in \mathcal{G}(B) \,\middle|\, \psi^m(g) = hgh^{-1}\right\}.$$

3.2. Parametrized Picard–Vessiot extensions

Let (K, ϕ) be an inversive ϕ-field, and assume that it is endowed with another automorphism ψ, commuting with ϕ. Assume that the field of ϕ-constants $C = K^{\phi}$ is algebraically closed of characteristic 0, and note that it inherits a structure of a ψ-field. Let (M,Φ) be a ϕ-module of rank n over K, and let $A \in GL_n(K)$ be the matrix associated with it in some basis.

DEFINITION 3.3. — *-A ψ-*Picard–Vessiot extension, *called also a* parametrized Picard–Vessiot (PPV) extension *for (M, Φ) (or the system $\phi(Y) = AY$), is a ϕ-pseudofield L_ψ containing K which:*

(i) *carries, in addition, a structure of a (not necessarily inversive) ψ-field, commuting with ϕ,*

(ii) *trivializes M after base-change, and if $U \in GL_n(L_\psi)$ is a fundamental matrix for $\phi(Y) = AY$,*

$$L_\psi = K(u_{ij})_\psi = K\left(\psi^k(u_{ij})\right)$$

(4) In fact, allowing $m = 0$ and $\alpha = 1$ in the Proposition, one may drop (i) and assume only that the Zariski closure of G is simple.

is generated as a total ring (a ring in which every non-zero divisor is invertible) by the elements $\psi^k(u_{ij})$ *for* $1 \leqslant i, j \leqslant n$ *and* $0 \leqslant k < \infty$. *We shall express this property by saying that* L_ψ *is the* ψ-hull *(as a total ring) of* $K(u_{ij})$.

(iii) $L_\psi^\phi = K^\phi = C$.

Here are the main facts about PPV extensions.

- A PPV extension L_ψ as above exists ([11, Theorem 2.28 and Corollary 2.29]). This is tricky! One is inclined to construct inductively (classical) PV extensions for the ϕ-modules
$$M_d = M \oplus M^{(\psi)} \oplus \cdots \oplus M^{(\psi^d)}$$
and go to the limit when $d \to \infty$. The difficulty is in showing that we can get L_ψ to be a *finite* product of fields. One should keep track of the number of connected components in this inductive procedure, and prove that it stays bounded.
- Let
$$R_\psi = K\left[u_{ij}, \det(U)^{-1}\right]_\psi = K\left[\psi^k(u_{ij}), \psi^k(\det U)^{-1}\right]$$
be the *ring* ψ*-hull* of $K[u_{ij}, \det(U)^{-1}]$ inside L_ψ. Then R_ψ is ϕ-simple and L_ψ is its total ring of fractions. One calls R_ψ the PPV *ring* of M. Since U is uniquely determined up to right multiplication by $V \in GL_n(C)$, R_ψ is uniquly determined as a subring of L_ψ.
- Let $L = K(u_{ij})$ and $R = K[u_{ij}, \det(U)^{-1}]$ (inside L_ψ). Then L is a (classical) PV extension and R a PV ring for M.

3.3. The parametrized difference Galois group

3.3.1. General facts and definitions

Assumptions and notation as above, fix a PPV extension L_ψ and the PPV ring $R_\psi \subset L_\psi$. Consider the functor $G : \mathrm{Alg}_C^\psi \rightsquigarrow$ Groups given by
$$G(B) = \mathrm{Aut}_{\phi,\psi}\left((R_\psi)_B / K_B\right),$$
the automorphisms of $(R_\psi)_B = B \otimes_C R_\psi$ that fix $B \otimes_C K$ pointwise and commute with both ϕ and ψ. Here B is given the trivial ϕ-action. If $\sigma \in G(B)$ then
$$\sigma(U) = UV(\sigma)$$

with $V(\sigma) \in GL_n(B)$. Moreover, since σ commutes with ψ, we have for every $i \geqslant 0$

$$\sigma\left(\psi^i(U)\right) = \psi^i(U)\psi^i(V(\sigma)). \tag{3.3}$$

Thus the choice of U determines an embedding $G \hookrightarrow [\psi]GL_{n,C}$.

The main facts about G, mirroring the facts listed for the classical difference Galois group $\mathcal{G}$, are the following (see [11, § 2.7]).

- G is representable by a ψ-linear algebraic group. We denote it by the same letter G or by $Gal^{\psi}(L_{\psi}/K)$.
- The Hopf ψ-algebra $C\{G\}$ of G is $(R_{\psi} \otimes_K R_{\psi})^{\phi}$.
- The natural map

  $$R_{\psi} \otimes_C C\{G\} = R_{\psi} \otimes_K K\{G\} \simeq R_{\psi} \otimes_K R_{\psi}$$

  sending $r \otimes h$ ($r \in R_{\psi},\ h \in C\{G\}$) to $r \otimes 1 \cdot h$ is an isomorphism of K-(ϕ, ψ)-algebras. This means that $W_{\psi} = Spec^{\psi}(R_{\psi})$ is a ψ-G_K-torsor.
- If L_{ψ} is a field, $\psi\dim(G) = \psi\text{tr.deg.}(L_{\psi}/K)$.
- The fixed field of a PPV extension under the parametrized Galois group being defined in the same way as the fixed field of a PV extension under the classical Galois group, we have

  $$L_{\psi}^{G} = K.$$

- More generally, there is a 1-1 correspondence between ψ-algebraic subgroups of G and intermediate ϕ-pseudofields of L_{ψ} stable under ψ. Normal ψ-subgroups correspond to PPV extensions (of some other ϕ-modules M').

3.3.2. Relation between G and $\mathcal{G}$

Let $L = K(u_{ij}) \subset L_{\psi}$ be the classical PV extension inside the PPV extension, and $R \subset R_{\psi}$ the PV ring. Let $\mathcal{G}$ be the classical Galois group. The realization of $\sigma \in G(B)$ as $V(\sigma) \in GL_n(B)$ via its action on U, namely

$$\sigma : U \mapsto UV(\sigma)$$

shows that σ restricts to a ϕ-automorphism of R_B over K_B, hence a map of functors

$$G \hookrightarrow [\psi]\mathcal{G},$$

which is evidently injective. In general, it need not be an isomorphism, as $\sigma \in [\psi]\mathcal{G}(B) = \mathcal{G}(B^{\flat})$ "does not know" about the extra automorphism

ψ, and may not extend to R_ψ so that the extra compatibilities (3.3) are satisfied. However, since

$$C[\mathcal{G}] = (R \otimes_K R)^\phi \hookrightarrow (R_\psi \otimes_K R_\psi)^\phi = C\{G\}$$

is injective, any function from $C[\mathcal{G}]$ that vanishes on G is 0. It follows that there does not exist a proper (classical) subgroup $\mathcal{H} \subset \mathcal{G}$ with $G \subset [\psi]\mathcal{H}$, hence

- G is Zariski dense in $\mathcal{G}$ ([3, Proposition 2.12]).

3.3.3. A Galoisian criterion for being ψ-isomonodromic

The ψ-Galois group G of a difference ϕ-module M enables us to state a criterion for M to be ψ-isomonodromic, i.e. for $M \simeq M^{(\psi)}$.

PROPOSITION 3.4 ([11, Theorem 2.55]). — *The ϕ-module M is ψ-isomonodromic if and only if there exists an $h \in GL_n(C)$ such that*

$$\psi(X) = hXh^{-1}$$

holds in G (i.e. for any $B \in \mathrm{Alg}_C^\psi$ and any $\sigma \in G(B) \subset \mathcal{G}(B) \subset GL_n(B)$, $\psi(\sigma) = h\sigma h^{-1}$).

Proof. — Assume that M is ψ-isomonodromic. Then there exists a matrix $A_\psi \in GL_n(K)$, such that with $A_\phi = A$, we have the compatibility relation

$$\phi(A_\psi)A_\phi = \psi(A_\phi)A_\psi.$$

Using this relation and the relation $1 = \phi(U)^{-1}A_\phi U$ we see that

$$h = \psi(U)^{-1}A_\psi U$$

is fixed under ϕ, hence belongs to $GL_n(L_\psi^\phi) = GL_n(C)$. Let $\sigma \in G(B)$ and compute $\sigma(\psi(U))$ in two ways. On the one hand

$$\sigma(\psi(U)) = \sigma\left(A_\psi U h^{-1}\right) = A_\psi U V(\sigma) h^{-1}.$$

On the other hand

$$\sigma(\psi(U)) = \psi(\sigma(U)) = \psi(UV(\sigma)) = A_\psi U h^{-1}\psi(V(\sigma)).$$

Comparing the two expressions we get $\psi(V(\sigma)) = hV(\sigma)h^{-1}$. This string of identities can be reversed. Starting with h as above and defining $A_\psi = \psi(U)hU^{-1}$, we see that A_ψ is fixed by every σ in the Galois group, hence lies in $GL_n(K)$, and we get the desired compatibility relation between A_ψ and A_ϕ. □

Remark 3.5. — The last proof can be given a matrix-free version. If $h : M \simeq M^{(\psi)}$ is an isomorphism of ϕ-modules, then h can be base-changed to L_ψ and then, since it commutes with Φ, induces an isomorphism between the modules of solutions. If $\sigma \in G$ (and not only in $\mathcal{G}$) then σ induces a commutative diagram

$$\begin{array}{ccc} M_{L_\psi}^{\Phi} & \xrightarrow{h} & \left(M_{L_\psi}^{(\psi)}\right)^{\Phi} \\ \Big\downarrow{\scriptstyle \sigma} & & \Big\downarrow{\scriptstyle \psi(\sigma)} \\ M_{L_\psi}^{\Phi} & \xrightarrow{h} & \left(M_{L_\psi}^{(\psi)}\right)^{\Phi} \end{array}$$

yielding the relation $\psi(\sigma) = h\sigma h^{-1}$. If we identify, as usual, the spaces of solutions $M_{L_\psi}^{\Phi}$ and $(M_{L_\psi}^{(\psi)})^{\Phi}$ with C^n, in the bases given by the columns of U and $\psi(U)$, then h becomes a matrix in $GL_n(C)$ as in the Proposition. Conversely, a descent argument shows that given such a diagram relating the spaces of solutions (*after* base change to L_ψ) yields an isomorphism $M \simeq M^{(\psi)}$ (*before* the base-change). In fact, this "conceptual proof" is not any different than the "matrix proof" by Ovchinnikov and Wibmer. Unwinding the arguments, one sees that the two proofs are one and the same.

3.4. Example 2.7 continued

Suppose we add, in Example 2.7, a second difference operator $\psi f(z) = f(pz)$, as in the case (2Ell). Then the ϕ-module corresponding to the system $\phi(Y) = AY$ is ψ-isomonodromic, and the corresponding system $\psi(Y) = BY$ is given by

$$B = \begin{pmatrix} p & g_p(z,\Lambda) \\ 0 & 1 \end{pmatrix}.$$

The compatability relation

$$\phi(B)A = \psi(A)B$$

is satisfied. The field E is also a PPV extension, being ψ-stable. The ψ-Galois group G is "classical", i.e.

$$G = [\psi]\mathcal{G}.$$

3.5. Filtrations and descent, continued

Let the notation be as in § 2.8. We assume that $C = K^{\phi}$ is not only algebraically closed, but also of characteristic 0. Assume that K is endowed, in addition, with a second automorphism ψ, commuting with ϕ. The field C inherits the structure of an inversive ψ-field. Let L_ψ be a PPV extension for (M, Φ) and *assume that it is a field*. Realize the PV extension L as a subfield of L_ψ. Let $G = Gal^{\psi}(L_\psi/K)$ be the parametrized Galois group.

Let L_ψ^a be the subfield of L_ψ consisting of the elements which are ψ-algebraic over K, i.e.

$$L_\psi^a = \{x \in L_\psi \,|\, \text{tr.deg.}(K(x)_\psi/K) < \infty\}\,.$$

If $x, y \in L_\psi^a$ then $\text{tr.deg.}(K(x)_\psi/K) < \infty$ and $\text{tr.deg.}(K(x,y)_\psi/K(x)_\psi) < \infty$, so $\text{tr.deg.}(K(x,y)_\psi/K) < \infty$. This shows that the sum and product of two ψ-algebraic elements is ψ-algebraic, so L_ψ^a is indeed a subfield. It is clearly invariant under ψ, and since ϕ and ψ commute it is invariant under ϕ as well. For the same reason, it is also evident that L_ψ^a is invariant under $G(C)$. We need, however, the stronger invariance under G in the sense of § 2.6. This is a non-trivial technical point. We circumvent it by quoting the following result, where one substitutes the PPV ring R_ψ for L_ψ.

LEMMA 3.6 ([3, Corollary A.17]). — *Let*

$$R_\psi = K\left[\psi^k(u_{ij}), \psi^k \det(U)^{-1} \,\middle|\, 1 \leqslant i, j \leqslant n,\ \ 0 \leqslant k\right] \subset L_\psi$$

be the PPV ring. Then $R_\psi^a = R_\psi \cap L_\psi^a$, the subring of ψ-algebraic elements in R_ψ, is invariant under ϕ and ψ, and is also G-stable, i.e. for any $B \in \text{Alg}_C^{\psi}$ and any $\sigma \in G(B) = \text{Aut}_{\phi,\psi}(B \otimes_C R_\psi/B \otimes_C K)$,

$$\sigma\left(B \otimes_C R_\psi^a\right) = B \otimes_C R_\psi^a.$$

Inside $\mathcal{V} = (L_\psi \otimes_K M)^{\Phi_{L_\psi}}$ $(= \mathcal{V}_L(M) = (L \otimes_K M)^{\Phi_L})$ we consider the C-subspace

$$\mathcal{V}^a = \mathcal{V} \cap \left(L_\psi^a \otimes_K M\right) = \left(L_\psi^a \otimes_K M\right)^{\Phi_{L_\psi}}.$$

Let $m = \dim_C \mathcal{V}^a$. If $M = K^n$ with $\Phi(v) = A^{-1}\phi(v)$, and $U \in GL_n(L)$ is a fundamental matrix, then we may assume that the first m columns of U span $\mathcal{V}^a$. This means that all their entries are ψ-algebraic over K, and any solution of $\phi(Y) = AY$ all of whose coordinates are ψ-algebraic over K is a C-linear combination of the first m columns of U. Observe that since the entries of U lie in R_ψ, we have

$$\mathcal{V}^a = \mathcal{V} \cap \left(R_\psi^a \otimes_K M\right) = \left(R_\psi^a \otimes_K M\right)^{\Phi_{L_\psi}}.$$

By the last Lemma, $\mathcal{V}^a$ is invariant under G, in the following strong sense: for any $B \in \mathrm{Alg}_C^{\psi}$, $B \otimes_C \mathcal{V}^a \subset B \otimes_C \mathcal{V}$ is invariant under $G(B) \subset \mathcal{G}(B)$, under the natural action of $\mathcal{G}(B)$ on $B \otimes_C \mathcal{V}$.

Consider the exact sequence

$$0 \to \mathcal{V}^a \to \mathcal{V} \to \mathcal{V}_a \to 0$$

of C-vector spaces, where $\mathcal{V}_a := \mathcal{V}/\mathcal{V}^a$. Since $\mathcal{V}^a$ is G-invariant, and G is Zariski dense in $\mathcal{G}$, $\mathcal{V}^a$ is also $\mathcal{G}$-invariant. From Proposition 2.8 we deduce the following.

PROPOSITION 3.7. — *There exists an exact sequence of ϕ-modules*

$$0 \to M^a \to M \to M_a \to 0$$

over K such that

$$\mathcal{V}^a = \mathcal{V}_L\left(M^a\right) = \left(L \otimes_K M^a\right)^{\Phi_L}.$$

Intuitively, M^a is the largest submodule of M all of whose "periods" in L are ψ-algebraic (when viewed in L_ψ).

4. Some preliminary results

4.1. Isomonodromy and solvability

Let (K, F, ϕ, ψ) be as in the case (2Ell) and assume that $2 \leqslant p, q$ and $(p, q) = 1$. This condition is more restrictive than assuming p and q to be multiplicatively independent, but is needed in [17], specifically in Theorem 6 there.

Let M be a ϕ-module over K, A the associated matrix (in a fixed basis), R a PV ring for M, $L = Quot(R)$ the corresponding PV extension, $U \in GL_n(R)$ a fundamental matrix, and $\mathcal{G} \subset GL_{n,\mathbb{C}}$ the difference Galois group, its embedding in $GL_{n,\mathbb{C}}$ determined by the choice of U. The following theorem will be used in the proof of Theorem 1.5, but has independent interest.

THEOREM (Theorem 1.6). — *Assume that M is ψ-isomonodromic. Then $\mathcal{G}$ is solvable.*

Proof. — By Theorem 2.6(i), it is enough to show that with respect to a suitable basis of M the matrix A is upper triangular. Indeed, if this is the case, take H to be the Borel subgroup of upper triangular matrices. Since (a conjugate of) $\mathcal{G} \subset H$ and H is solvable, $\mathcal{G}$ is solvable too.

Endow $M = (M, \Phi, \Psi)$ with a (ϕ, ψ)-module structure. Call M solvable if there exists a sequence

$$0 \subset M_1 \subset \cdots \subset M_n = M$$

of (ϕ, ψ)-submodules M_i, $\mathrm{rk}(M_i) = i$. This would clearly imply that $A = A_\phi$ is gauge-equivalent to a matrix in upper triangular form.

We show that M is solvable. It is enough to show that M contains a rank-one (ϕ, ψ)-submodule M_1. Letting $\overline{M} = M/M_1$, one can then use induction on the rank to find a chain

$$0 \subset \overline{M}_2 \subset \cdots \subset \overline{M}_n = \overline{M}$$

of (ϕ, ψ)-submodules with $\mathrm{rk}(\overline{M}_i) = i - 1$. Their pre-images in M, together with M_1, would give the desired chain in M.

We apply [17, Theorem 35]. Using the notation there, let $(r_1, \ldots, r_k)$ be the *type* of M, $r_1 \leqslant r_2 \leqslant \cdots \leqslant r_k$, $\sum_{i=1}^k r_i = n$. Let $e_1, \ldots, e_n$ be the basis of M in which A has the canonical form prescribed by that theorem.

Let us recall this special canonical form. Let $N_r = (n_{ij})$ be the nilpotent $r \times r$ matrix with $n_{i,i+1} = 1$, $n_{ij} = 0$ if $j \neq i+1$. Let $U_r(z)$ be the unipotent upper-triangular matrix

$$U_r(z) = \exp(\zeta(pqz, \Lambda) N_r) = \sum_{j=0}^{r-1} \frac{\zeta(pqz, \Lambda)^j}{j!} N_r^j.$$

Write $A = (A_{ij})$ in block-form, $A_{ij} \in M_{r_i \times r_j}(K)$. Then

$$A_{ij}(z) = U_{r_i}(z/p) T_{ij} U_{r_j}(z)^{-1}. \tag{4.1}$$

Here

$$T_{ij} = \begin{pmatrix} 0 & T_{ij}^* \\ 0 & 0 \end{pmatrix}$$

where T_{ij}^* is a square upper-triangular $s \times s$ matrix for $s \leqslant \min(r_i, r_j)$, with *constant* (i.e. $\mathbb{C}$-valued) entries.

An analogous description, with a constant matrix S replacing T, gives the matrix B, associated with Ψ in the same basis.

Let

$$i_1 = 1,\ i_2 = r_1 + 1, \ldots, i_k = r_1 + \cdots + r_{k-1} + 1$$

be the first indices in each of the k blocks. Let $M' = Span_K\{e_{i_1}, \ldots, e_{i_k}\}$. Then (a) M' is a rank k (ϕ, ψ)-submodule of M, and moreover, (b) $\Phi|_{M'}$ and $\Psi|_{M'}$ are given in this basis by *constant* matrices. To see these two points note that by (4.1) and the fact that T_{ij} is a *constant* matrix, each block A_{ij} is upper-triangular with *constants* along the diagonal. Write

$$M = \oplus_{j=1}^k M_j$$

as a direct sum of k vector spaces, where $M_j = Span\{e_{i_j}, e_{i_j+1}, \ldots, e_{i_{j+1}-1}\}$ has dimension r_j. If we let

$$\iota_j : M_j \hookrightarrow M, \quad , \pi_j : M \twoheadrightarrow M_j$$

be the inclusion and projection of the j^{th} factor in the direct sum decomposition, then (up to replacing A by A^{-1}), $A_{\ell j}$ is the matrix of $\pi_\ell \circ \Phi \circ \iota_j$. Since it is upper-triangular with constants along the diagonal, this matrix takes e_{i_j} (the first basis vector of M_j) to a *constant* multiple of e_{i_ℓ} (the first basis vector of M_ℓ). Summing over $\ell = 1, \ldots, k$ gives that $\Phi(e_{i_j}) = \Phi \circ \iota_j(e_{i_j})$ is a linear combination of the e_{i_ℓ}'s with constant coefficients. The analysis of the matrix B corresponding to the endomorphism Ψ is similar. This shows both points (a) and (b).

In other words, we have shown that M' is a (ϕ, ψ)-submodule of M which *descends to* $\mathbb{C}$. Thus $M' = M'_0 \otimes_{\mathbb{C}} K$, where M'_0 is a $\mathbb{C}$-representation of $\Gamma = \langle \phi, \psi \rangle \simeq \mathbb{Z}^2$, and Φ and Ψ are extended semilinearly from M'_0 to M'. Since any two commuting endomorphisms of a $\mathbb{C}$-vector space have a common eigenvector, M' has a rank-one (ϕ, ψ)-submodule $M_1 \subset M' \subset M$, which concludes the proof of Theorem 1.6. □

Incidentally, note that we have given an affirmative answer to [17, Problem 36], where we conjectured that every *simple* elliptic (p, q)-difference module is 1-dimensional.

4.2. A periodicity theorem

In this subsection we generalize [16, Theorem 1.1]. Let $\mathscr{D}$ be the $\mathbb{Q}$-vector space of discretely supported functions $f : \mathbb{C} \to \mathbb{Q}$, i.e. functions for which $\mathrm{supp}(f) = \{z | \, f(z) \neq 0\}$ has no accumulation point in $\mathbb{C}$. For any lattice $\Lambda \subset \mathbb{C}$ let $\mathscr{D}_\Lambda$ be the subspace of $f \in \mathscr{D}$ which are Λ-periodic. We may identify

$$\mathscr{D}_\Lambda = \mathrm{Div}(E_\Lambda)_{\mathbb{Q}}$$

with the group of $\mathbb{Q}$-divisors on the elliptic curve E_Λ.

Given two functions $f, \widetilde{f} \in \mathscr{D}$ we say that $\widetilde{f}$ is a *modification at 0* of f if $\widetilde{f}(z) = f(z)$ for every $z \neq 0$.

Let $2 \leqslant p, q \in \mathbb{N}$ be relatively prime integers: $(p, q) = 1$. Consider the operators

$$\phi f(z) = f(qz), \quad \psi f(z) = f(pz) \tag{4.2}$$

on $\mathscr{D}$. These operators preserve every $\mathscr{D}_\Lambda$, because if f is Λ-periodic and $\omega \in \Lambda$ then

$$\phi f(z + \omega) = f(qz + q\omega) = f(qz) = \phi f(z),$$

and similarly for ψ.

PROPOSITION 4.1. — *Let $f \in \mathscr{D}$. Assume that for some Λ-periodic $f_p, f_q \in \mathscr{D}_\Lambda$ the relations*

$$f_q(z) = f(qz) - f(z)$$
$$f_p(z) = \sum_{i=0}^{m} e_{m-i} f\left(p^{1-i} z\right)$$

($e_i \in \mathbb{Q}$, $e_m = 1$, $e_0 \neq 0$) hold for all $z \neq 0$. Then, after replacing Λ by a sublattice, a suitable modification $\widetilde{f}$ of f at 0 is Λ-periodic.

[16, Theorem 1.1] concerned the case $f_p(z) = f(pz) - f(z)$. In this case, or more generally if $\sum_{i=0}^{m} e_{m-i} = 0$, we may modify $f$at 0 without affecting f_p and f_q. Thus f itself need not be periodic, and we can not forgo the need to modify f at 0.

We shall now show how to modify the proof to treat the more general case given here.

Observe first that for some $r_\nu \in \mathbb{Q}$, $r_1 = 1$, we have for every $z \neq 0$

$$f(z) = \sum_{\nu=1}^{\infty} f_q\left(\frac{z}{q^\nu}\right) = \sum_{\nu=1}^{\infty} r_\nu f_p\left(\frac{z}{p^\nu}\right). \tag{4.3}$$

Formally, this is clear for the first sum, and in the second sum one solves recursively for the r_ν. Since all our functions are discretely supported, for any given z the infinite sums are actually finite, and the formal identity becomes an equality.

Let $S_p \subset \mathbb{C}/\Lambda$ and $S_q \subset \mathbb{C}/\Lambda$ be the supports of f_p and f_q (modulo Λ). Let $\pi_\Lambda : \mathbb{C} \to \mathbb{C}/\Lambda$ be the projection and $\widetilde{S}_p = \pi_\Lambda^{-1}(S_p)$, $\widetilde{S}_q = \pi_\Lambda^{-1}(S_q)$. Let $\widetilde{S}$ be the support of f, and $S = \pi_\Lambda(\widetilde{S})$. By (4.3) we have

$$\widetilde{S} - \{0\} \subset \bigcup_{\nu=1}^{\infty} p^\nu \widetilde{S}_p \cap \bigcup_{\nu=1}^{\infty} q^\nu \widetilde{S}_q. \tag{4.4}$$

LEMMA 4.2. — *The set S is finite.*

Proof. — See [16, Lemma 2.3]. It is enough to assume here that p and q are multiplicatively independent. □

LEMMA 4.3. — *Let $z \in \widetilde{S}_q$, $z \notin \mathbb{Q}\Lambda$, and let $n_q(z)$ be the largest $n \geqslant 0$ such that $q^n z \in \widetilde{S}_q$ (it exists since S_q is finite and the points $q^n z$ have distinct images modulo Λ). Note that $n_q(z) = n_q(z + \lambda)$ for $\lambda \in \Lambda$ so that*

$$n_q = 1 + \max_{z \in \widetilde{S}_q,\, z \notin \mathbb{Q}\Lambda} n_q(z)$$

exists. Then

$$f\left(z+q^{2n_q}\lambda\right)=f(z)$$

for every $z\notin\mathbb{Q}\Lambda$ *and* $\lambda\in\Lambda$.

Proof. — The proof preceding [16, Proposition 2.4] holds, word for word, except that the P there is our q here. Thus, away from torsion points of the lattice, f is $q^{2n_q}\Lambda$-periodic. The proof of this Lemma, which relies on the previous one, still assumes only the multiplicative independence of p and q. □

We now treat torsion points $z\in\mathbb{Q}\Lambda$, for which we have to assume $(p,q)=1$. We may assume, without loss of generality, that f, hence f_p and f_q, are supported on $\mathbb{Q}\Lambda$, because away from $\mathbb{Q}\Lambda$ we have already proved periodicity, so we may subtract the part of f supported on non-torsion points from the original f without affecting the hypotheses.

Since S is finite we may rescale Λ and assume that f is supported on $pq\Lambda$. Then f_p is supported on $q\Lambda$ and f_q on $p\Lambda$, as becomes evident from (4.3).

LEMMA 4.4. — *If both* f_p *and* f_q *are* $N\Lambda$*-periodic, then so is a suitable modification of* f *at 0.*

Proof. — The proof of [16, Proposition 2.2] works the same, substituting the relations (4.3) for the relations used there. □

The two Lemmas prove that a suitable modificiation of f at 0 is Λ-periodic, for a sufficiently small lattice Λ, on non-torsion points and on torsion points separately. This concludes the proof of Proposition 4.1.

5. Proof of the main theorems

5.1. Deduction of Theorem 1.4 from Theorem 1.5

From now on we let (K,F,ϕ,ψ) be as in the case (2Ell), assuming that $2\leqslant p,q,\ (p,q)=1$. Recall that $S_\phi(F/K)$ is the collection of all $u\in F$ satisfying a linear homogeneous ϕ-difference equation, and $AS_\psi(F/K)$ is the collection of all $u\in F$ for which there exists an $n\geqslant 0$ such that

$$\psi^n(u)\in K\left(u,\psi(u),\ldots,\psi^{n-1}(u)\right).$$

Clearly $S_\psi(F/K)\subset AS_\psi(F/K)$. We have also denoted by

$$S=K\left[z,z^{-1},\zeta(z,\Lambda)\right]$$

the ring generated over K by $z^{\pm 1}$ and the Weierstrass ζ-function. Let us recall the statements of the two main theorems.

THEOREM (Theorem 1.4). — *Let (K, F, ϕ, ψ) be as in case (2Ell) and assume that $2 \leqslant p, q$ and $(p, q) = 1$. Let $f \in S_\phi(F/K)$ and $g \in AS_\psi(F/K)$. If $f \notin S$ and $g \notin K$, then f and g are algebraically independent over K.*

THEOREM (Theorem 1.5). — *Let (K, F, ϕ, ψ) be as in case (2Ell) and assume that $2 \leqslant p, q$ and $(p, q) = 1$. Let $f \in S_\phi(F/K)$ and assume that $f \notin S$. Then $\{f, \psi(f), \psi^2(f), \dots\}$ are algebraically independent over K.*

The deudction of Theorem 1.4 from Theorem 1.5 is short, and follows the exact same lines as in [3]. For completeness, we include it here. Assume that Theorem 1.5 is proven, and let f and g be as in Theorem 1.4. Let n be the first integer such that

$$\psi^n(g) \in K\left(g, \psi(g), \dots, \psi^{n-1}(g)\right).$$

Clearly all the $\psi^i(g)$, $i \geqslant n$, also belong there.

If g were algebraic over K, so would be all the $\psi^i(g)$, and the field

$$K(g)_\psi = K\left(g, \psi(g), \dots, \psi^{n-1}(g)\right)$$

would be a finite extension of K to which ψ extends as an endomorphism. In fact, since ψ is an automorphism of K and $[K(g)_\psi : K] < \infty$, it would be an *automorphism* of $K(g)_\psi$. By Proposition 2.1 (iii) this is impossible. Hence g is transcendental over K.

Suppose f and g were algebraically dependent over K. Then this dependence must involve f, hence f is algebraic over $K(g)_\psi$, and so would be all the $\psi^i(f)$. It follows that

$$\text{tr.deg.}(K(f, g)_\psi/K) = \text{tr.deg.}(K(g)_\psi/K) \leqslant n < \infty.$$

A fortiori,

$$\text{tr.deg.}\,(K(f)_\psi/K) < \infty,$$

contradicting the conclusion of Theorem 1.5.

5.2. First order equations

Consider the difference equation

$$\phi(y) = ay \tag{5.1}$$

with $a \in K^\times$. The associated ϕ-module is $M = Ke$ with $\Phi(e) = a^{-1}e$. Let L_ψ be a PPV extension for M, and $u \in L_\psi$ a solution: $\phi(u) = au$. Replacing ϕ and ψ by some powers ϕ^r and ψ^s we may assume that L_ψ is a field. Indeed, let

$$L_\psi = L_1 \times \cdots \times L_r$$

be the decomposition of the ϕ-pseudofield L_ψ into a product of fields. Then ϕ^r is an endomorphism of L_1, and some power ψ^s of ψ must also preserve it, and induces an endomorphism of L_1. The subfield of L_1 generated by (the projection of) u and all its ψ^s-transforms is a PPV extension for M as a ϕ^r-module, which is stable by ψ^s.

Assume therefore that L_ψ is a field.

PROPOSITION 5.1. — *The following are equivalent:*

(i) *u is ψ-algebraic over K, i.e.* $\mathrm{tr.deg.}(L_\psi/K) < \infty$.
(ii) *u satisfies an equation $\psi(u) = \widetilde{a}u$ for some $\widetilde{a} \in K^\times$.*
(iii) *The ϕ-module M descends to $\mathbb{C}$: there exist $b \in K^\times$ and $c \in \mathbb{C}^\times$ such that*

$$a = c\frac{\phi(b)}{b}.$$

COROLLARY 5.2. — *If $ord_0(a) \neq 0$ then u is ψ-transcendental over K.*

Proof. — In this case, (iii) can not hold, so (i) can not hold either. □

In [16] we proved⇒ (iii), but we shall not need this step here. Clearly (ii) ⇒ (i), and (iii)⇒(ii) because if (iii) holds we may assume, replacing u by u/b, that $a = c \in \mathbb{C}^\times$. Then

$$\left(u^{\psi-1}\right)^{\phi-1} = \left(u^{\phi-1}\right)^{\psi-1} = a^{\psi-1} = 1,$$

so $\widetilde{a} = u^{\psi-1} \in L_\psi^\phi = \mathbb{C}$, and (ii) holds. (If we did not assume $a \in \mathbb{C}^\times$ we would only get $\widetilde{a} \in K^\times$.) We shall now prove (i) ⇒(iii). We remark that while, formally, Proposition 5.1 resembles the analogons statement in the rational case, the proof of (i)⇒(iii) is much more involved in the elliptic case. It relies on the Periodicity Theorem 4.1, as well as on standard results on elliptic functions.

Proof. — Let G be the ψ-Galois group of (5.1). It is a ψ-closed subgroup of $[\psi]\mathbb{G}_m$. If $R_\psi = K[u, u^{-1}]_\psi \subset L_\psi$ is the PPV ring then for any $B \in \mathrm{Alg}_{\mathbb{C}}^\psi$ and $\sigma \in G(B)$ we embed $\sigma \mapsto v_\sigma \in B^\times$ where $\sigma(u) = uv_\sigma$.

Assume that u is ψ-algebraic. Then

$$\psi\dim(G) = \psi\mathrm{tr.deg.}(L_\psi/K) = 0 < 1 = \psi\dim([\psi]\mathbb{G}_m),$$

so G is a proper closed ψ-subgroup of $[\psi]\mathbb{G}_m$. It follows from Lemma 3.1 that there is a ψ-monomial relation

$$\mu(v_\sigma) = v_\sigma^{e_0}\psi(v_\sigma)^{e_1}\cdots\psi^m(v_\sigma)^{e_m} = 1$$

($e_i \in \mathbb{Z}$, $e_m \neq 0$) that holds for all $\sigma \in G$.

Let $B \in \mathrm{Alg}_{\mathbb{C}}^\psi$ and $\sigma \in G(B)$. Then

$$\sigma(\mu(u)) = \mu(\sigma(u)) = \mu(uv_\sigma) = \mu(u)$$

so by the ψ-Galois correspondence $b' = \mu(u) \in L_\psi^G = K$. We conclude that

$$\mu(a) = \mu(u^{\phi-1}) = \mu(u)^{\phi-1} = \phi(b')/b'. \tag{5.2}$$

Let $\alpha(z) = ord_z(a)$ and $\beta(z) = ord_z(b')$, so that $\alpha = \mathrm{div}(a)$ and $\beta = \mathrm{div}(b')$. These are the divisors of the elliptic functions a and b', so for some $\Lambda \subset \Lambda_0$ we have $\alpha, \beta \in \mathscr{D}_\Lambda$. The action of ϕ and ψ on $\mathscr{D}_\Lambda$ has been defined in (4.2) and

$$\psi(\mathrm{div}(a)) = \mathrm{div}(\psi(a)), \;\; \phi(\mathrm{div}(b')) = \mathrm{div}(\phi(b'))$$

hold true. Therefore, taking the divisor of the relation (5.2) gives

$$\sum_{i=0}^{m} e_i \psi^i(\alpha) = \phi(\beta) - \beta.$$

Define

$$\delta(z) = \sum_{\nu=1}^{\infty} \alpha(\frac{z}{q^\nu}) \;\; (z \neq 0); \;\; \delta(0) = 0.$$

Then $\delta \in \mathscr{D}$ and for $z \neq 0$

$$\begin{cases} \alpha(z) = \delta(qz) - \delta(z) \\ \beta(z) = \sum_{i=0}^{m} e_i \delta(p^i z). \end{cases}$$

Applying the Periodicity Theorem 4.1 to $f_p(z) = \beta(pz)$, $f_q(z) = \alpha(p^m z)$ and $f(z) = \delta(p^m z)$ we conclude:

- After replacing Λ by a sublattice, a suitable modification $\widetilde{\delta}$ of δ at 0 is Λ-periodic.
- We must have $\alpha(0) = 0$.

The first assertion is the Periodicity Theorem. For the second, if $z \neq 0$ we have

$$\alpha(z) = \delta(qz) - \delta(z) = \widetilde{\delta}(qz) - \widetilde{\delta}(z).$$

Let Λ be a periodicity lattice for both α and $\widetilde{\delta}$. Take $0 \neq \lambda \in \Lambda$. Then $\alpha(\lambda) = \widetilde{\delta}(q\lambda) - \widetilde{\delta}(\lambda) = 0$, hence $\alpha(0) = 0$.

We may therefore assume that $\delta(z)$ is already periodic and $\alpha(z) = \delta(qz) - \delta(z)$ holds everywhere, including at 0. Observe, however, that in the process of modifying δ at 0, we might no longer have $\delta(0) = 0$.

Let Π be a fundamental parllelopiped for $\mathbb{C}/\Lambda$ where Λ is a periodicity lattice for α, β and δ. Observe that

$$\sum_{z \in \Pi} \delta(qz) = \sum_{z \in q\Pi} \delta(z) = \sum_{\omega \in \Lambda/q\Lambda} \sum_{z \in \Pi + \omega} \delta(z) = q^2 \sum_{z \in \Pi} \delta(z).$$

In addition, for $\omega \in \Lambda$,

$$\sum_{z \in \Pi+\omega} z\delta(z) = \sum_{z \in \Pi} z\delta(z)$$

because δ is Λ-periodic and $\sum_{z \in \Pi} \delta(z) = 0$. Thus we also have

$$\sum_{z \in q\Pi} z\delta(z) = q^2 \sum_{z \in \Pi} z\delta(z).$$

We conclude that

$$0 = \sum_{z \in \Pi} \alpha(z) = \sum_{z \in \Pi} \delta(qz) - \sum_{z \in \Pi} \delta(z) = \left(q^2 - 1\right) \sum_{z \in \Pi} \delta(z),$$

so $\delta \in \mathrm{Div}^0(\mathbb{C}/\Lambda)$. We also have

$$\begin{aligned} \sum_{z \in \Pi} z\alpha(z) &= q^{-1} \sum_{z \in \Pi} qz\delta(qz) - \sum_{z \in \Pi} z\delta(z) \\ &= q^{-1} \sum_{z \in q\Pi} z\delta(z) - \sum_{z \in \Pi} z\delta(z) = (q-1) \sum_{z \in \Pi} z\delta(z). \end{aligned}$$

Let $\Lambda' = (q-1)\Lambda$. Let Π' be a fundamental parallelopiped for Λ'. Then by the same argument as above

$$\sum_{z \in \Pi'} z\delta(z) = (q-1)^2 \sum_{z \in \Pi} z\delta(z) = (q-1) \sum_{z \in \Pi} z\alpha(z) \in \Lambda'$$

because by Abel–Jacobi and the fact that α is Λ-elliptic, $\sum_{z \in \Pi} z\alpha(z) \in \Lambda$. We recall that the Abel–Jacobi theorem asserts that a divisor $\sum n_i[\zeta_i]$, where $\zeta_i \in \mathbb{C}/\Lambda$, is the divisor of a Λ-elliptic function if and only if $\sum n_i = 0$ and $\sum n_i\zeta_i = 0$.

Replacing Λ by Λ' we conclude, again by Abel–Jacobi, that δ is the divisor of some $b \in K_\Lambda$. Let $c = a/(\phi(b)/b)$. Then c is Λ-elliptic and its divisor is

$$\alpha - (\phi(\delta) - \delta) = 0.$$

Thus c is constant, and the proof of Proposition 5.1 is complete. □

Corollary 5.3 (First order case of Theorem 1.5). — *Let $f \in F$ satisfy the first order, linear homogenous equation*

$$\phi(f) = af$$

with $a \in K^\times$. Then either $f \in S$ or $\{f, \psi(f), \psi^2(f), \dots\}$ are algebraically independent over K.

Proof. — We may embed $K(f)_\psi$ in the PPV extension L_ψ. If $\{f, \psi(f), \psi^2(f), \dots\}$ are not algebraically independent over K then, according to the last Proposition f satisfies also a linear homogenous ψ-difference equation over K. By Theorem 1.3 we must have $f \in S$. □

Remark. — According to [16], in the order one case, if f is ψ-algebraic over K, we can even infer that for some $m \in \mathbb{Z}$, $z^m f \in K$.

Generalizing from first order homogenous equations to first order inhomogenous equations is done exactly as in [3, Proposition 4.5]. We do not repeat the proof, as it can be duplicated word for word, and will not be needed in the sequel, see the remark below. The only difference is that at the last step in [3], assuming f was ψ-algebraic over K, Theorem 1.1 of that paper was invoked to deduce that $f \in K$. Here we should invoke Theorem 1.3 instead, so we can only deduce $f \in S$. We arrive at the following Proposition.

PROPOSITION 5.4. — *Let $f \in F$ satisfy the inhomogenous difference equation*

$$\phi(f) = af + b$$

with $a, b \in K$. Then either $f \in S$ or $\{f, \psi(f), \psi^2(f), \dots\}$ are algebraically independent over K.

Remark. — We shall not need this Proposition. In the last stage of our proof of Theorem 1.5 we shall deal with the same type of inhomogenous equation, but where $b \in S$. We shall give full details there.

5.3. The case of a simple $\mathcal{G}$

5.3.1. Recall of notation and assumptions

Let

$$M = (K^n, \Phi)\,,\ \Phi(v) = A^{-1}\phi(v)$$

be the rank-n ϕ-module over K associated with the system $\phi(Y) = AY$.

Let $L \subset L_\psi$ be PV and PPV extensions for M, $\mathcal{G}$ the (classical) difference Galois group and G the (parametrized) ψ-Galois group.

Fixing a fundamental matrix U with entries in L we get embeddings

$$G \subset [\psi]\mathcal{G} \subset [\psi]GL_{n,\mathbb{C}}.$$

When we base change M to L we get the full, n-dimensional, complex vector space of "solutions"

$$\mathcal{V} = M_L^{\Phi} = U\mathbb{C}^n \subset M_L = L^n. \tag{5.3}$$

If instead of L we use the even larger PPV extension L_ψ we get the same complex vector space $\mathcal{V}$, as all the solutions already lie in L^n. However, over L_ψ we get also the solution spaces $\psi^i(\mathcal{V})$ of all the ψ-transforms $M^{(\psi^i)}$, $i \geqslant 0$.

The difference Galois group $\mathcal{G}$ acts on $\mathcal{V}$. If $\sigma \in \mathcal{G}(\mathbb{C})$ then for $v \in \mathbb{C}^n$

$$\sigma(Uv) = UV(\sigma)v,$$

so $\sigma \mapsto V(\sigma)$ is the matrix representation of $\mathcal{G}$ on $\mathcal{V}$ in the basis consisting of the columns of U.

5.3.2. The simple case

LEMMA 5.5 ([3, Lemma 3.9]). — *Assume that L_ψ is a field. Then $\mathcal{G}$ is connected and G is ψ-integral, hence in particular ψ-reduced.*

The proof relies on Proposition 2.1. Recall that being ψ-integral means that the coordinate ring $\mathbb{C}\{G\}$ is a domain and ψ is injective on it.

PROPOSITION 5.6 ([3, Proposition 4.11]). — *Assume that L_ψ is a field. If $\mathcal{G}$ is simple, then $G = [\psi]\mathcal{G}$. In particular,*

$$\psi\mathrm{tr.deg.}(L_\psi/K) = \psi\dim(G) = \dim(\mathcal{G}) > 0.$$

Proof. — We repeat the arguments of [3]. Note first that G is Zariski dense in $\mathcal{G}$ (always true) and ψ-reduced (by the previous lemma). By Proposition 3.2, if $G \subsetneq [\psi]\mathcal{G}$, there exists an $h \in GL_n(\mathbb{C})$ and an $m \geqslant 1$ such that

$$\psi^m(X) = hXh^{-1}$$

holds in G.

By Proposition 3.4 M is then ψ^m-isomonodromic.

By Theorem 1.6, $\mathcal{G}$ must be solvable, contradicting the assumption that it was simple. This contradiction shows that we must have had $G = [\psi]\mathcal{G}$. □

PROPOSITION 5.7 ([3, Proposition 4.12]). — *Assume that L_ψ is a field. Then either $\mathcal{G}$ is connected and solvable or $\psi\mathrm{tr.deg.}(L_\psi/K) > 0$.*

Proof. — Same as in [3]. Connectendness follows from Lemma 5.5. If $\mathcal{G}$ is not solvable then it has a simple quotient $\mathcal{G}/\mathcal{N}$. The Galois correspondence theorem is used to obtain a PV extension $L' = L^{\mathcal{N}}$ for a ϕ-module M',

whose difference Galois group is $\mathcal{G}/\mathcal{N}$. The PPV extension of the same M' is a subfield $L'_\psi \subset L_\psi$, and by the previous Proposition $\psi\text{tr.deg.}(L'_\psi/K) > 0$. A fortiori, $\psi\text{tr.deg.}(L_\psi/K) > 0$. □

5.4. Conclusion of the proof: Galois acrobatics

We prove the following claim, which clearly implies Theorem 1.5, by induction on n. The assumptions on p and q are maintained.

CLAIM 5.8. — *Let $n \geqslant 1$, $A \in GL_n(K)$ and $u = {}^t(u_1, \ldots, u_n) \in F^n$ a solution of $\phi(Y) = AY$. Assume that all the coordinates u_i are ψ-algebraic, i.e.* $\text{tr.deg.}(K(u)_\psi/K) < \infty$ *where $K(u)_\psi$ is the field ψ-hull of $K(u)$ in F. Then $u \in S^n$.*

The case $n = 1$ follows from Corollary 5.3. The following Lemma will be used to reduce the general case to certain inhomogenous first order equations, albeit with coefficients outside K.

LEMMA 5.9. — *Without loss of generality, we may assume:*

(1) *The PPV extension L_ψ is a field, and all its elements are ψ-algebraic over K. Equivalently, $\psi\dim(G) = 0$.*
(2) *$\mathcal{G}$ is solvable, and the matrices A and U are upper triangular.*
(3) *The diagonal elements of A are in $\mathbb{C}^\times$.*
(4) *$K(u)_\psi \subset L_\psi$ and the vector u is the last column of U.*

Proof. — Let M be the ϕ-difference module over K associated with the system $\phi(Y) = AY$. Thus $M = K^n$ and $\Phi(v) = A^{-1}\phi(v)$. As before, replacing ϕ and ψ by some powers ϕ^r and ψ^s, and A by $A_{[r]}$, we may assume, *not changing u,* that the PPV extension L_ψ of M is a field, $K(u)_\psi$ (a priori a subfield of F) is embedded as a (ϕ, ψ)-subfield of L_ψ, and that the (classical) difference Galois group $\mathcal{G}$ is connected. Let U be a fundamental matrix, with entries in L_ψ. The given vector u is some linear combination of its columns.

Let L^a_ψ be the subfield of L_ψ consisting of elements that are ψ-algebraic. It is stable under ϕ and ψ, and as we have mentioned in § 3.5, at least the ring $R^a_\psi = R_\psi \cap L^a_\psi$ is also invariant under G.

Let $\mathcal{V} = M^\Phi_{L_\psi} = U\mathbb{C}^n \subset L^n_\psi$ be the space of solutions, and $\mathcal{V}^a = \mathcal{V} \cap (L^a_\psi)^n$, so that $u \in \mathcal{V}^a$. Proposition 3.7 implies that M has a ϕ-submodule M^a such that $\mathcal{V}_L(M^a) = \mathcal{V}^a$. Choose a new basis $e_1, \ldots, e_n$ of M over K, so that the first m vectors $e_1, \ldots, e_m$ span M^a. If $P \in GL_n(K)$ is the change-of-basis matrix, then A is replaced by $\phi(P)AP^{-1}$, and u by

Pu. Since to prove the claim it is enough to show that $Pu \in S^n$, we may assume that the first m vectors of the original basis formed a basis of M^a.

In such a basis

$$A = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix}$$

in block form (where A_{11} is of size $m \times m$). We may further assume that the $\mathbb{C}$-basis of the solution space $\mathcal{V}$ (namely, the columns of U) has been chosen in such a way that the first m vectors form a basis of $\mathcal{V}^a = \mathcal{V}_L(M^a)$ over $\mathbb{C}$. Then

$$U = \begin{pmatrix} U_{11} & U_{12} \\ 0 & U_{22} \end{pmatrix}$$

has the same shape as A. The vector u, which we have to show lies in S^n, is a $\mathbb{C}$-linear combination of the columns of U_{11}.

Let $\mathcal{P} \subset GL_{n,\mathbb{C}}$ be the maximal parabolic subgroup stabilizing $Span\{e_1, \ldots, e_m\}$, i.e. the subgroup of matrices whose lower-left $(n-m) \times m$ block is 0. Then $\mathcal{G} \subset \mathcal{P}$ because if $\sigma \in \mathcal{G}$ then the associated matrix is $V(\sigma) = U^{-1}\sigma(U)$. Since our task is to prove that u has entries in S, and u depends only on U_{11}, we may replace our system of equations by the system $\phi(Y) = A_{11}Y$ and the fundamental matrix U by U_{11}. Assume, therefore, that $n = m$, $A = A_{11}$, $\mathcal{V} = \mathcal{V}^a$ etc., hence $L_\psi = L_\psi^a$. This proves (1). Assume for the rest of the proof of the Lemma that this is the case, so that $\psi\text{tr.deg.}(L_\psi/K) = 0$.

By Proposition 5.7 the Galois group $\mathcal{G}$ is solvable. By the Lie-Kolchin theorem we may assume that $\mathcal{G}$ is contained in the upper-triangular Borel subgroup of $GL_{n,\mathbb{C}}$. By Theorem 2.6 (ii) we may assume that so is A, hence by Theorem 2.6 (i) an appropriate choice of U is also upper triangular. This proves (2).

Recall that the vector u is a linear combination of the columns of U. If the last non-zero entry of u is u_r then we can assume, by a further change of coordinates, not affecting the upper triangular form, that u is the rth column of U. Replacing the system of equations by the one corresponding to the upper-left $r \times r$ block we may assume that $r = n$, and u is the last column of U. This is (4).

By induction, we may assume that (3) had been proved for all the diagonal elements of A, but the first one. Since u_{11} is a solution of $\phi(y) = a_{11}y$, and is ψ-algebraic, Proposition 5.1 shows that there exists a $b \in K^\times$ such that $a_{11}/(\phi(b)/b) \in \mathbb{C}^\times$. Replacing A by the gauge-equivalent $\phi(P)^{-1}AP$, where $P = \text{diag.}[b, 1, \ldots, 1]$, we do not spoil all our assumptions so far, and in addition we get (3). □

From now on the proof can be concluded either by the methods of [17], or by the Galois theoretic "acrobatics" adapted from [3]. We chose to use the second approach.

Assume therefore that we are in the situation of the Lemma. In particular $u_i = u_{in}$ is the ith entry in the last column of the fundamental matrix U. The u_i lie in F, but also in L_ψ, by our assumption (4) that $K(u)_\psi \subset L_\psi$.

We may also assume that $E = Quot(S)$ is contained in L_ψ. If this is not the case, augment the matrix A by adding to it along the diagonal a 2×2 block as in example 2.7. The fundamental matrix gets augmented by the block

$$\begin{pmatrix} z & \zeta(z,\Lambda) \\ 0 & 1 \end{pmatrix},$$

hence the PPV extension for the augmented system contains E. If we prove the main theorem for the augmented system, we clearly have proved it also for the original one.

By induction we may assume that $u_2, \ldots, u_n \in S$. We have to show that $u' = u_1 \in S$.

This $u' \in F$ satisfies the equation

$$\phi(u') = au' + b$$

where $a = a_{11} \in \mathbb{C}^\times$, and $b = a_{12}u_{2n} + \cdots + a_{1n}u_{nn} \in S$ (by our induction hypothesis). Let $v = u_{11}$, so that $\phi(v) = av$.

Since $(\phi - a)(u') \in S \subset S_\phi(F/K)$ clearly $u' \in S_\phi(F/K)$. To conclude the proof we shall show, following the ideas of the proof of [3, Proposition 4.5] that

$$u' \in S_\psi(F/K)$$

as well. Theorem 1.3 will show then that $u' \in S$, as desired. The discrepancy between K and S makes the arguments here somewhat more complicated than in [3]. It will force us to consider difference equations over $E = Quot(S)$, rather than over K alone.

Consider the matrix

$$U' = \begin{pmatrix} v & u' \\ 0 & 1 \end{pmatrix} \in GL_2(L_\psi).$$

This is a fundamental matrix for the system

$$\phi(Y) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} Y,$$

regarded as a system of difference equations over E. The field

$$L'_\psi = E(v, u')_\psi \subset L_\psi$$

is its PPV extension. Furthermore, the ψ-Galois group of the last system is

$$G' = Gal^{\psi}(L'_{\psi}/E) \subset \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \in GL_2 \right\}$$

and its intersection with the unipotent radical (where $\alpha = 1$), denoted G'_u, corresponds via the Galois correspondence to $E(v)_{\psi}$:

$$G'_u = Gal^{\psi}\left(L'_{\psi}/E(v)_{\psi}\right).$$

This is a ψ-subgroup of $[\psi]\mathbb{G}_a$. By our assumption that u' is ψ-algebraic over K, hence clearly over E,

$$\psi \dim G'_u = \psi\text{tr.deg.}\left(L'_{\psi}/E(v)_{\psi}\right) = 0.$$

It follows from [6, Corollary A.3] that there exists an $0 \neq \mathcal{L}_1 \in \mathbb{C}[\psi]$ such that for any $B \in \mathrm{Alg}^{\psi}_{\mathbb{C}}$ we have

$$G'_u(B) \subset \left\{ \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \in GL_2(B) \;\middle|\; \mathcal{L}_1(\beta) = 0 \right\}.$$

Observe that

$$\phi(\frac{u'}{v}) = \frac{u'}{v} + \frac{b}{av},$$

and $b/av \in E(v)_{\psi}$, so $L'_{\psi}/E(v)_{\psi}$ is a PPV extension for $\phi(y) = y + (b/av)$, equivalently for the system

$$\phi(Y) = \begin{pmatrix} 1 & b/av \\ & 1 \end{pmatrix} Y$$

over $E(v)_{\psi}$. The action of $\tau \in G'_u(B)$ is given by

$$\tau\left(\frac{u'}{v}\right) = \frac{u'}{v} + \beta_{\tau}$$

where $\beta_{\tau} \in B$ corresponds to the above realization of τ as a unipotent 2×2 matrix. Indeed, if

$$\tau(U') = U' \begin{pmatrix} 1 & \beta_{\tau} \\ 0 & 1 \end{pmatrix}$$

then $\tau(u') = v\beta_{\tau} + u'$ and $\tau(v) = v$.

It follows that for any $\tau \in G'_u(B)$

$$\tau\left(\mathcal{L}_1\left(\frac{u'}{v}\right) \otimes 1\right) = \mathcal{L}_1\left(\tau\left(\frac{u'}{v}\right)\right) \otimes 1 = \mathcal{L}_1\left(\frac{u'}{v} + \beta_{\tau}\right) \otimes 1 = \mathcal{L}_1\left(\frac{u'}{v}\right) \otimes 1,$$

hence $\mathcal{L}_1(u'/v) \in E(v)_{\psi}$. But

$$\left(v^{\psi-1}\right)^{\phi-1} = \left(v^{\phi-1}\right)^{\psi-1} = a^{\psi-1} = 1,$$

so $d = v^{\psi-1} \in \mathbb{C}$ and $\psi(v) = dv$, $E(v)_\psi = E(v)$. It follows that there exists a second operator $\mathcal{L}_2 \in \mathbb{C}[\psi]$, easily derived from $\mathcal{L}_1$, such that

$$\mathcal{L}_2(u') \in E(v).$$

This $\mathcal{L}_2(u')$ satisfies the equation

$$\phi(y) = ay + \mathcal{L}_2(b)$$

where we have used the fact that a was constant, and where $\mathcal{L}_2(b) \in S$. By [3, Lemma 4.7], with E serving as the base field *and* the intermediate field, there exists a $g \in E$ with

$$\phi(g) = ag + \mathcal{L}_2(b).$$

We are indebted to Charlotte Hardouin for pointing out the following lemma.

LEMMA 5.10. — *In fact, $g \in S$.*

Proof. — Let $I = \{s \in S | \, sg \in S\}$ be the ideal of denominators of g. If $s \in I$ then $\phi(s) \in I$ because

$$\phi(s)g = a^{-1}(\phi(sg) - \phi(s)\mathcal{L}_2(b)) \in S.$$

Since S is a simple ϕ-ring (it is the localization at z of the PV ring $K[z, \zeta(z, \Lambda)]$ associated to the system considered in Example 2.7), we must have $1 \in I$, so $g \in S$. □

It follows that $\phi(\mathcal{L}_2(u') - g) = a(\mathcal{L}_2(u') - g)$. Since also $\phi(v) = av$, the element $d' = (\mathcal{L}_2(u') - g)/v$ is fixed by ϕ, hence lies in $\mathbb{C}$, and

$$\mathcal{L}_2(u') = d'v + g.$$

Since $(\psi - d)d'v = d'(\psi - d)v = 0$ by the definition of d,

$$(\psi - d) \circ \mathcal{L}_2(u') = (\psi - d)(g) \in S.$$

As $(\psi - d) \circ \mathcal{L}_2 \in \mathbb{C}[\psi]$ and any element of S is annihilated by a non-trivial operator from $K[\psi]$, we deduce that $u' \in S_\psi(F/K)$, and the proof is complete.

Acknowledgements

The author would like to thank Charlotte Hardouin and Thomas Dreyfus for fruitful discussions regarding this work. He would also like to thank Zev Rosengarten and the participants of the Kazhdan Seminar at the Hebrew University for carefully and critically attending his lectures on the subject.

BIBLIOGRAPHY

[1] B. Adamczewski & J. P. Bell, "A problem about Mahler functions", *Ann. Sc. Norm. Super. Pisa, Cl. Sci. (5)* **17** (2017), p. 1301-1355.

[2] B. Adamczewski, T. Dreyfus & C. Hardouin, "Hypertranscendence and linear difference equations", *J. Am. Math. Soc.* **34** (2021), p. 475-503.

[3] B. Adamczewski, T. Dreyfus, C. Hardouin & M. Wibmer, "Algebraic independence and linear difference equations", *J. Eur. Math. Soc.* (2022).

[4] M. F. Atiyah, "Vector bundles over an elliptic curve", *Proc. Lond. Math. Soc. (3)* **7** (1957), p. 414-452.

[5] J.-P. Bézivin & A. Boutabaa, "Sur les équations fonctionelles p-adiques aux q-différences", *Collect. Math.* **43** (1992), p. 125-140.

[6] L. Di Vizio, C. Hardouin & M. Wibmer, "Difference Galois theory of linear differential equations", *Adv. Math.* **260** (2014), p. 1-58.

[7] ———, "Difference algebraic relations among solutions of linear differential equations", *J. Inst. Math. Jussieu* **16** (2017), no. 1, p. 59-119.

[8] T. Dreyfus, C. Hardouin & J. Roques, "Functional relations for solutions of q-differential equations", *Math. Z.* **298** (2021), no. 3-4, p. 1751-1791.

[9] T. Dreyfus & J. Roques, "Galois groups of difference equations of order two on elliptic curves", *SIGMA, Symmetry Integrability Geom. Methods Appl.* **11** (2015), article no. 003 (23 pages).

[10] C. Hardouin & M. F. Singer, "Differential Galois theory of linear difference equations", *Math. Ann.* **342** (2008), no. 2, p. 333-377.

[11] A. Ovchinnikov & M. Wibmer, "σ-Galois theory of linear difference equations", *Int. Math. Res. Not.* **12** (2015), p. 3962-4018.

[12] A. J. van der Poorten, "Remarks on automata, functional equations and transcendence", *Séminaire de Théorie des Nombres de Bordeaux* **1986-1987** (1986), article no. 27 (11 pages).

[13] M. van der Put & M. F. Singer, *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666, Springer, 1997.

[14] R. Schäfke & M. F. Singer, "Consistent systems of linear differential and difference equations", *J. Eur. Math. Soc.* **21** (2019), p. 2751-2792.

[15] J.-P. Serre, *Cohomologie Galoisienne. Cours au College de France, 1962-1963*, 4e ed., Lecture Notes in Mathematics, vol. 5, Springer, 1973.

[16] E. de Shalit, "Criteria for periodicity and an application to elliptic functions", *Can. Math. Bull.* **64** (2021), p. 530-540.

[17] ———, "Elliptic (p, q)-difference modules", *Algebra Number Theory* **15** (2021), p. 1303-1342.

[18] E. de Shalit & J. Gutiérrez, "On the structure of certain Γ-difference modules", *Enseign. Math. (2)* **68** (2022), no. 3-4, p. 341-377.

Manuscrit reçu le 15 novembre 2022,
révisé le 4 juillet 2023,
accepté le 2 octobre 2023.

Ehud DE SHALIT
Einstein Institute
of Mathematics,
The Hebrew University
of Jerusalem (Israel)
ehud.deshalit@mail.huji.ac.il