ON THE COMPUTATION OF THE DIFFERENCE GALOIS GROUPS OF ORDER THREE EQUATIONS

by Thomas Dreyfus & Marina Poulet

Abstract. — In this paper we consider the problem of computing the difference Galois groups of order three equations for a large class of difference operators including the shift operator (Case S), the q-difference operator (Case Q), the Mahler operator (Case M) and the elliptic case (Case E). We show that the general problem can be reduced to several ancillary problems. We prove criteria to detect the irreducible and imprimitive Galois groups. Finally, we give a sufficient condition of differential transcendence of solutions of order three difference equations. We also compute the difference Galois group of an equation suggested by Wadim Zudilin.

Résumé (*Sur le calcul des groupes de Galois aux différences d'équations d'ordre trois*)
    Dans cet article, nous considérons le problème du calcul des groupes de Galois aux différences des équations d'ordre trois pour une large classe d'opérateurs aux différences incluant l'opérateur de différence finie (Cas S), l'opérateur aux q-différences (Cas Q), l'opérateur de Mahler (Cas M) et le cas elliptique (Cas E). Nous montrons que ce problème général peut se réduire à l'étude de plusieurs problèmes auxiliaires. Nous prouvons un critère pour reconnaître les groupes de Galois irréductibles et imprimitifs. Pour terminer, nous donnons une condition suffisante qui garantit la transcendance différentielle des solutions d'équations aux différences d'ordre trois. Nous calculons aussi le groupe de Galois aux différences d'une équation suggérée par Wadim Zudilin.

Thomas Dreyfus, Thomas Dreyfus, Institut de Mathématiques de Bourgogne, UMR 5584 CNRS, Université de Bourgogne, F-21000, Dijon, France
E-mail : thomas.dreyfus@cnrs.fr
Marina Poulet, Institut de Mathématiques de Marseille, CNRS UMR 7373, Aix-Marseille Université, 3 place Victor Hugo Case 19, 13331 Marseille Cedex 3, France
E-mail : marina.poulet@univ-amu.fr

1. Introduction

Difference Galois theory is the subject of many recent papers because, for instance, of its application to (differential) transcendence of solutions of difference equations. More precisely, consider a field $\mathbf{k}$ equipped with an automorphism ϕ. Let $C \subset \mathbb{C}$ be an algebraically closed field of characteristic 0. Typical examples we are going to consider in this paper are

- (Case S, shift) $\mathbf{k} = C(z)$ and $\phi Y(z) = Y(z + h)$ with $h \in C^*$;
- (Case Q, q-difference) $\mathbf{k} = C\left(z^{1/*}\right) := \cup_{\ell=1}^{\infty} C(z^{1/\ell})$ and $\phi Y(z) = Y(qz)$ with $q \in C^*$ that is not a root of unity;
- (Case M, Mahler) $\mathbf{k} = C\left(z^{1/*}\right)$ and $\phi Y(z) = Y(z^p)$ with $p \geq 2$ an integer;
- (Case E, elliptic) Let Λ be a lattice of $\mathbb{C}$. Without loss of generality, we assume that $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ with $\mathrm{Im}(\tau) > 0$. Let $\wp(z)$ be the corresponding Weierstrass function. In this example, $\mathbf{k} = \mathcal{M}er(\Lambda^{\infty}) := \cup_{\ell=1}^{\infty} C(\wp(z/\ell), \partial_z \wp(z/\ell))$ and $\phi Y(z) = Y(z + h)$ with $h \in \mathbb{C}^*$ such that $h\mathbb{Z} \cap \Lambda = \{0\}$.

Then, consider the difference system

$$\phi Y = AY, \quad A \in \mathrm{GL}_n(\mathbf{k}).$$

The algebraic relations between functions which are entries of matrix solutions of the difference system are reflected by a difference Galois group, which is an algebraic group attached to a difference equation (see for example [vdPS97, Phi15]). Roughly speaking, if the difference Galois group is sufficiently big then there are no algebraic relations between these functions. Moreover, thanks to a differential Galois theory for difference equations (see [HS08]), one can attach a differential algebraic group to a difference equation, which is Zariski-dense in the difference Galois group. Under conditions on the difference Galois groups, this theory may also prove that some solutions of linear difference equations do not satisfy algebraic differential equations (see [HS08, AS17, DHR18, ADHW24, ADH21, ADR21, DHR21]) and has been recently used to prove that, in some cases, the generating series of walks in the quarter plane are differentially transcendental, see for instance [DHRS18]. There are many other applications of difference Galois theory that motivate the computation of the difference Galois groups. We could also mention the computation of the difference Galois groups of q-hypergeometric equations, see [Roq11] and density theorems [RS07, Pou21] but the present introduction does not pretend to be exhaustive.

Toward the proof of differential transcendence, we often need to prove that the difference Galois group is sufficiently big, making it important to be able to compute the latter. However, the computation of difference Galois groups is in general a difficult task. In the literature one can find many algorithms for the computation of Galois groups. The most developed area is the one of differential equations: many algorithms are given to compute differential Galois groups (which are algebraic groups attached to a linear differential system), see for

example [Kov86, SU93, CS99, BCWDV16, DW22]. There is a general algorithm for the computation of the Galois groups of linear differential equations of an arbitrary order but it is not effective (see for example the algorithm of Hrushovski in [Hru02] and some improvements [Fen15, AMP22]). In contrast, the case of difference equations is less developed. Algorithms have been given for the computation of difference equations of order 1 and 2 in these four famous cases: the shift (see [vdPS97, Hen98]), the q-difference (see [Hen97]), the Mahler (see [Roq18]) and the elliptic cases (see [DR15]). For the shift case, an analogue of Hrushovski's algorithm has been developed in [Fen18]. It computes the Galois groups for equations of arbitrary order whose coefficients are rational functions but is still inefficient. However, in general, for the Galois groups of difference equations of order 3 or more, only few things are known. The aim of this article is to explain how one can compute Galois groups of difference equations of order 3 under mild assumptions on the difference field to which the coefficients of the difference equations belong. In particular, it takes into account the four previous difference equations. We also recall general strategies for computing the Galois groups of difference equations of order 1 and 2. We highlight that we are mainly concerned by the theoretical aspects of the algorithm and no study of complexity will be made. Throughout this paper, we explain what we need to be able to do for using it in practice. In fact, one of the key point to apply it concretely is to be able to find rational (resp. hyperexponential) solutions to certain difference equations.

The starting point of this paper was an example suggested by Wadim Zudilin. This example is running as a common thread throughout this paper. The following double sum is related to the Rogers-Ramanujan identities

$$U(z,t) = \sum_{m,n=0}^{\infty} \frac{q^{m^2+3mn+3n^2} z^m t^n}{(q;q)_m (q^3;q^3)_n}, \quad \text{with } (\star;q)_n = (1-\star) \times \cdots \times (1-\star q^{n-1}).$$

For each fixed value of t, $z \mapsto U(z,t)$ satisfies a q-difference equation:

$$(1) \qquad ty(q^3 z) - (t + qt + q^4 z^2) y(q^2 z) + q(t - q^2 z) y(qz) + q^3 z y(z) = 0.$$

One of the questions asked by Zudilin was the computation of the Galois groups for the values $t = 1$ and $t = q^2$. We are going to compute the difference Galois groups over $\mathbb{C}(z^{1/*})$ for every value of $t \neq 0$ and see that it does not depend on the parameter t. Note that when $t = 0$, (1) is a q-difference equation of order 2 and the computation could be made using [Hen98].

THEOREM (Theorem 6.13). — *For all $t \in \mathbb{C}^*$, the difference Galois group of* (1) *is* $\mathrm{GL}_3(\mathbb{C})$.

Using [DHR21, Corollary 3.1] and Theorem 6.13, we may prove that for all $t \in \mathbb{C}^*$, there are no nontrivial algebraic differential relations between $U(z,t)$, $U(qz,t)$ and $U(q^2 z,t)$ over $\mathbb{C}(z^{1/*})$.

Now, we describe more precisely the content of this paper. After some reminders about the Galois theory of difference equations in Section 2.1, we recall a criterion in Section 2.2 to know if the Galois group G of a difference equation is reducible or not. In Section 2.3, we explain what we need, as a framework, in order to compute G in practice. In Section 3 we prove general results about Galois groups of difference systems of arbitrary order. We explain the strategy for computing G if G is reducible in Section 3.1. If G is not reducible we distinguish two cases: the imprimitive case and the primitive case. For the imprimitive case, we give information (the connected component of the identity and its index in G) on the possible Galois groups which occur when the order of the difference system is a prime number in Section 3.2. Moreover, we know which information correspond to G thanks to the knowledge of the determinant of G (which is the Galois group of an equation of order 1). After these general results, we recall the strategies for computing the Galois groups of the difference equations of order 1 and the diagonal systems in Section 4 and the strategies for the difference equations of order 2 in Section 5. Section 6 is devoted to the order three case. We give an application to the differential transcendence in Section 7.

Notations and conventions. — In what follows, all rings are commutative with identity and contain the field of rational numbers. In particular, all fields are of characteristic zero.

If G is an algebraic group, we denote by G^0 the connected component of the identity of G. Let $(\mathbf{k}, \phi)$ be a difference field, that is, a field equipped with an automorphism and let $[A]_\phi$ be the difference system $\phi(Y) = AY$ where $A \in \mathrm{GL}_n(\mathbf{k})$. To lighten notations, we denote it $[A]$ when there is no ambiguity.

2. Difference algebra

2.1. Galois groups. — In this section, we make a short overview of the Galois theory of linear difference equations. For more details on what follows, we refer to [vdPS97, Chapter 1]. A difference ring is a commutative ring $\mathbf{R}$ equipped with an automorphism $\phi : \mathbf{R} \to \mathbf{R}$. We denote by $C_{\mathbf{R}} := \{c \in \mathbf{R} | \phi(c) = c\}$, the constants of the difference ring $(\mathbf{R}, \phi)$. A difference ideal I of a difference ring $(\mathbf{R}, \phi)$ is an ideal such that $\phi(I) \subset I$. If $\mathbf{R}$ is a field, we call $(\mathbf{R}, \phi)$ a difference field. In this case, $C_{\mathbf{R}}$ is a field, the field of constants. With an abuse of notations, we will often denote by $\mathbf{R}$ the difference ring $(\mathbf{R}, \phi)$.

Throughout this paper, we assume that $(\mathbf{k}, \phi)$ is a difference field such that its field of constants $C_{\mathbf{k}}$ is algebraically closed.

If we consider a difference system

$$(2) \qquad\qquad \phi(Y) = AY, \quad with \quad A \in \mathrm{GL}_n(\mathbf{k}),$$

according to [vdPS97, Section 1.1], there exists a difference ring extension $(\mathbf{L}, \phi)$ of $(\mathbf{k}, \phi)$ such that:

- there exists a fundamental matrix of solutions of (2) with entries in $\mathbf{L}$, that is, a matrix $U \in \mathrm{GL}_n(\mathbf{L})$ such that $\phi(U) = AU$;
- $\mathbf{L}$ is generated as a $\mathbf{k}$-algebra by the entries of U and $\det(U)^{-1}$;
- the only difference ideals of $\mathbf{L}$ are $\{0\}$ and $\mathbf{L}$.

A difference ring $\mathbf{L}$ which satisfies these conditions is called a Picard-Vessiot ring for the system (2) over $\mathbf{k}$. It is unique up to isomorphisms of difference rings over $\mathbf{k}$. We have the following property: $C_{\mathbf{L}} = C_{\mathbf{k}}$.

The difference Galois group G of (2) over $\mathbf{k}$ is the group of $\mathbf{k}$-linear automorphisms of $\mathbf{L}$ commuting with ϕ, that is,

$$G := \{\sigma \in \mathrm{Aut}(\mathbf{L}/\mathbf{k}) \mid \sigma \circ \phi = \phi \circ \sigma\}.$$

For any fundamental matrix $U \in \mathrm{GL}_n(\mathbf{L})$, an easy computation shows that $U^{-1}\sigma(U) \in \mathrm{GL}_n(C_{\mathbf{L}}) = \mathrm{GL}_n(C_{\mathbf{k}})$ for all $\sigma \in G$. By [vdPS97, Theorem 1.13], the faithful representation

$$\begin{aligned} \rho : G &\to \mathrm{GL}_n(C_{\mathbf{k}}) \\ \sigma &\mapsto U^{-1}\sigma(U) \end{aligned}$$

identifies G with a linear algebraic subgroup $G \subset \mathrm{GL}_n(C_{\mathbf{k}})$. If we take another fundamental matrix of solutions V, we find an algebraic group that is conjugated to the first one. In this paper, by "computation of the difference Galois group G", we mean "computation of an algebraic subgroup of $\mathrm{GL}_n(C_{\mathbf{k}})$ conjugated to $\rho(G)$", thus we work up to conjugations. Abusing notations, we will still denote by G the image of the difference Galois group under the above representation.

We denote by $\mathbf{k}\left\langle \phi, \phi^{-1} \right\rangle$ the Öre algebra of noncommutative Laurent polynomials with coefficients in $\mathbf{k}$ such that $\phi f = \phi(f)\phi$ for all $f \in \mathbf{k}$. We consider the difference equation

$$(3) \qquad Ly = 0, \quad \text{where} \quad L := \sum_{i=0}^{n} a_i \phi^i \in \mathbf{k}\langle \phi \rangle \text{ with } a_0 a_n \neq 0,$$

that is, $a_0 y + \cdots + a_n \phi^n(y) = 0$ with $a_i \in \mathbf{k}$ and $a_0 a_n \neq 0$. We transform the difference equation (3) into the difference system

$$\phi(Y) = A_L Y, \quad \text{where} \quad A_L = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ -a_0/a_n & \ldots & & -a_{n-1}/a_n \end{pmatrix}$$

is the companion matrix associated with L. By definition, the difference Galois group of (3) is the difference Galois group of the system $[A_L]$.

The change of variables $Z := TY$, $T \in \mathrm{GL}_n(\mathbf{k})$, transforms the system $\phi Y = AY$ with $A \in \mathrm{GL}_n(\mathbf{k})$ into $\phi Z = BZ$ where $B := \phi(T)AT^{-1} \in \mathrm{GL}_n(\mathbf{k})$. Let $A, B \in \mathrm{GL}_n(\mathbf{k})$. We will say that $[A]$ and $[B]$ are equivalent over $\mathbf{k}$ if there exists $T \in \mathrm{GL}_n(\mathbf{k})$ such that $B = \phi(T)AT^{-1}$.

In what follows, we assume moreover that the field $\mathbf{k}$ satisfies:

- $\mathbf{k}$ is a $\mathcal{C}^1$-field, that is every non-constant homogeneous polynomial P over $\mathbf{k}$ has a nontrivial zero provided that the number of its variables is more than its degree;
- $\mathbf{k}$ is the only finite algebraic difference field extension of $\mathbf{k}$.

All the above mentioned examples (S,Q,M,E) satisfy these two conditions, see [Hen97, Hen98, DR15, Roq18]. Note that in the q-difference case, the field $(C(z), \phi)$ is a difference field but there are nontrivial finite algebraic difference field extensions. For instance $C(z^{1/2})|C(z)$ is of degree two and we may extend ϕ on it with $\phi(z^{1/2}) = q^{1/2}z^{1/2}$. This is the reason why we consider $C(z^{1/*})$ instead of $C(z)$ in that setting. Similar considerations occur in the elliptic case.

We recall that $C := C_{\mathbf{k}}$ is by hypothesis algebraically closed and the characteristic of $\mathbf{k}$ is zero. The following statement will be crucial in what follows. See [vdPS97, Propositions 1.20 and 1.21], see also [DR15, Theorem 2.4].

THEOREM 2.1. — *Let $G \subset \mathrm{GL}_n(C)$ be the difference Galois group over $(\mathbf{k}, \phi)$ of* (2). *Then, the following properties hold:*

- G/G^0 *is finite and cyclic, where G^0 is the identity component of G;*
- *there exists $B \in G(\mathbf{k})$ such that* (2) *is equivalent to $\phi Y = BY$ over $\mathbf{k}$.*

Let $\widetilde{G}$ be an algebraic subgroup of $\mathrm{GL}_n(C)$ such that $A \in \widetilde{G}(\mathbf{k})$. The following properties hold:

- G *is conjugate to a subgroup of $\widetilde{G}$;*
- *any minimal element in the set of algebraic subgroups $\widetilde{H}$ of $\widetilde{G}$ for which there exists $T \in \mathrm{GL}_n(\mathbf{k})$ such that $\phi(T)AT^{-1} \in \widetilde{H}(\mathbf{k})$ is conjugate to G;*
- G *is conjugate to $\widetilde{G}$ if and only if, for any $T \in \widetilde{G}(\mathbf{k})$ and for any proper algebraic subgroup $\widetilde{H}$ of $\widetilde{G}$, one has that $\phi(T)AT^{-1} \notin \widetilde{H}(\mathbf{k})$.*

In practice, to compute the difference Galois group, we are going to compute a gauge transformation such that the transformed system lies in $G(\mathbf{k})$. This leads to the following definition.

DEFINITION 2.2. — *Let $G \subset \mathrm{GL}_n(C)$ be the difference Galois group over $(\mathbf{k}, \phi)$ of the system* (2). *We say that the system* (2) *is* in reduced form *(or* reduced*) when $A \in G(\mathbf{k})$.*

Given a difference system $\phi(Y) = AY$ and an integer $\ell \geqslant 1$, we can iterate it:

$$(4) \qquad \phi^\ell(Y) = A_{[\ell]}Y, \quad \text{where} \quad A_{[\ell]} = \phi^{\ell-1}(A) \times \cdots \times A.$$

Let $G_{[\ell]}$ be the difference Galois group of the system (4). The following lemma may be deduced from the proof [DHR21, Proposition 4.6] in the particular case where the parametric operator is the identity, and is proved in [ADH21, Proposition 4.10]. It compares the Galois groups $G_{[\ell]}$, $\ell \geqslant 1$.

LEMMA 2.3. — *For all $\ell \geqslant 1$, $G_{[\ell]}$ has the same connected component of the identity as G. Furthermore, there exists $\ell_0 \geqslant 1$, such that $G_{[\ell_0]}$ is the connected component of the identity of G.*

2.2. Factorisations of difference operators. — In this subsection, we focus on the reducible difference operators and make the relation with the reducible Galois groups and the Riccati equation. Let G be an algebraic subgroup of $\mathrm{GL}_n(C)$. We say that G is reducible if there exists a non trivial vector subspace V of C^n such that for all $\sigma \in G$, $\sigma(V) \subset V$. We say that G is irreducible otherwise.

The following lemma relates the irreducibility of the difference Galois group with the factorisation of the difference operator, see [ADH21, Lemma 4.4].

LEMMA 2.4. — *Let $G \subset \mathrm{GL}_n(C)$ be the difference Galois group of (2). Then, G is reducible with a nontrivial invariant space of dimension $0 < m < n$, if and only if there exists $T \in \mathrm{GL}_n(\mathbf{k})$, $A_1 \in \mathrm{GL}_m(\mathbf{k})$, and A_2, A_3 matrices of convenient size, such that*

$$\phi(T)AT^{-1} = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix}.$$

If we consider the difference system $[A_L]$ attached to (3), then its difference Galois group is reducible with $A_1 \in \mathrm{GL}_m(\mathbf{k})$ if and only if L admits a nontrivial right factor of order m.

Thus, to determine whether G is irreducible or not, we have to determine whether the difference operator L defined in (3) admits a nontrivial right factor or not. For right factors of order one, we have the following criterion.

LEMMA 2.5 (Lemma 2 in [ABPS21]). — *Let L be the difference operator defined in (3). The operator of order one $\phi - \alpha$ is a right factor of L if and only if*

$$\sum_{i=0}^{n} a_i \prod_{j=0}^{i-1} \phi^j(\alpha) = 0.$$

Although the above equation, called the Riccati equation, is nonlinear it might be solved in some situations we are going to describe later.

When L has order two, it admits a nontrivial factor if and only if it admits a nontrivial right factor of order one.

When L has order three, it admits a nontrivial factor if and only if it admits a nontrivial factor of order one. The latter may be either a right or a left factor.

Let us see how we can pass from left factor to right factor. We define the dual $M^\vee$ of an operator $M = \sum_{i=m}^{n} a_i \phi^i \in \mathbf{k} \left\langle \phi, \phi^{-1} \right\rangle$ by

$$M^\vee := \sum_{i=m}^{n} \phi^{-i}(a_i) \phi^{-i}.$$

By linearity, if $M_1, M_2 \in \mathbf{k} \left\langle \phi, \phi^{-1} \right\rangle$, we can check that

$$(M_1 M_2)^\vee = M_2^\vee M_1^\vee.$$

Hence, an operator has a left factor of order one if and only if its dual has a right factor of order one. So we will focus on right factors of order one.

REMARK 2.6. — *Assume $n > 1$ and that L admits a right factor of order one so let us write L as $\widetilde{L}(\phi - \alpha)$ where $\alpha \in \mathbf{k}$ and $\widetilde{L} \in \mathbf{k} \left\langle \phi, \phi^{-1} \right\rangle$ has order $n-1$. Let y_1 be a solution of $Ly = 0$ such that $\phi(y_1) \neq \alpha y_1$ and let $y_2 := \phi(y_1) - \alpha y_1$. By construction $y_2 \neq 0$ is a solution of $\widetilde{L}y = 0$. If $Y := \left(y_1, y_2, \ldots, \phi^{n-2}(y_2) \right)^t$ then $\phi(Y) = \widetilde{A}Y$ where*

$$\widetilde{A} := \begin{pmatrix} \alpha & 1 \, 0 \, \cdots \, 0 \\ \hline 0 & \\ \vdots & A_{\widetilde{L}} \\ 0 & \end{pmatrix}.$$

Thus, the companion system associated with $Ly = 0$ is equivalent to the system $[\widetilde{A}]$. Furthermore, $A_{\widetilde{L}}$ is a companion matrix associated with $\widetilde{L}$.

2.3. From theory to practice. — We recall that the aim of this paper is to explain how one can compute theoretically the Galois group of a difference equation of order 3. In practice we may also need to make more assumptions on the difference field $(\mathbf{k}, \phi)$ in order to compute effectively the difference Galois groups:

- Assume that $\mathbf{k}$ is an effective field, i.e. that one can compute representatives of the four operations $+, -, \times, /$ and one can effectively test whether two elements of $\mathbf{k}$ are equal.
- Assume that, given a homogeneous linear difference system $[A]$ with $A \in \mathrm{GL}_n(\mathbf{k})$, we can effectively find a basis of its rational solutions, i.e. its solutions $Y \in \mathbf{k}^n$.
- Assume that given a difference operator L, if L admits at least one right factor of order one, then we are able to compute effectively one of such right factors.
- Given $\alpha_1, \ldots, \alpha_n \in \mathbf{k}^*$, find the set of $f_1, \ldots, f_n \in \mathbf{k}^*$, $m_1, \ldots, m_n \in \mathbb{Z}$, satisfying

$$(5) \qquad \left(\frac{\phi(f_1)}{f_1} \alpha_1 \right)^{m_1} \times \ldots \times \left(\frac{\phi(f_n)}{f_n} \alpha_n \right)^{m_n} = 1.$$

When $C = \overline{\mathbb{Q}}$, for the cases (S, Q, M), the two first points are satisfied (note that in the case (Q), the authors consider $\mathbf{k} = C(x)$). One can find some references for the second point in this table:

cases	(S)	(Q)	(M)	(E)
ref.	[Abr95, AB98, vH98, AB01]	[Abr95, AB01, Abr02]	[CDDM18]	[DR15, Com22]

Note that in the elliptic case the second point is not satisfied, unless considering the case $n = 2$, see [DR15] (note that the latter is concerned by the more general problem of solving Riccati equations), or when the framework is modified, see for instance [Com22]. Thus, in that case, our algorithm may not lead to a systematic computation of the difference Galois group. It will reduce the computation to the determination of rational solutions of certain linear difference equations that may be complicated to solve concretely. Throughout this paper, we will emphasize which kind of equations we have to be able to solve.

We saw in Section 2.2 that the study of the irreducibility of the Galois groups is closely related to the factorisation of the difference operator. From Lemma 2.5, when we look at a right factor of order one, we have to solve a Riccati equation of the form

$$\sum_{i=0}^{n} a_i \prod_{j=0}^{i-1} \phi^j(\alpha) = 0.$$

When $C = \overline{\mathbb{Q}}$, we are able to compute right-factors of order 1 in the cases (S,Q,E) but we want to emphasis that the complexity is exponential, in the order of the equation, contrary to the search of rational solutions, whose complexity is polynomial. Here-below, one can find some references for these computations:

cases	(S)	(Q)	(E)	(M)
ref.	[Pet92, CvH06, ABPS21]	[APP98, CvH06, ABPS21]	[DR15, Com22]	[CDDM24]

EXAMPLE 2.7. — *Let us now present the strategy of* [ABPS21] *to show that the difference Galois group of* (1) *over* $\mathbb{C}(z^{1/*})$ *is irreducible, which is equivalent to show that the corresponding operator has no factor of order* 1. *We point out the fact that* $\mathbb{C}(z^{1/*})$ *is not an effective field but the strategy still work in that case. Assume that* $t \neq 0$. *Let us begin by proving that there is no right factor of order one. Let*

$$L = a_0 + a_1\phi + a_2\phi^2 + a_3\phi^3$$

be the q-difference operator corresponding to (1), *and let* $L^\vee$ *be its dual. By* [ABPS21, *Lemma* 3], *for any* $\alpha \in \mathbf{k}^\times$ *there exist* $\lambda \in \mathbb{C}^\times$, $\ell \in \mathbb{N}^*$ *and unitary*

$b, c, r \in \mathbb{C}[z^{1/\ell}] \setminus \{0\}$ *such that*

$$\alpha = \lambda \, \frac{b}{c} \, \frac{\phi(r)}{r}$$

and

  – $\gcd(b, \phi^k(c)) = 1$ *for all* $k \in \{0, 1, 2\}$;
  – $\gcd(b, r) = 1$;
  – $\gcd(c, \phi(r)) = 1$.

Using this, one can deduce by [ABPS21, Lemma 3] *that if* $\phi - \alpha$ *is a right factor of order* 1 *of* L *for some* $\alpha \in \mathbf{k}^\times$, *then, in the above decomposition for* α, *we have* $b|a_0$, $c|\phi^{-2}(a_3)$, *and*

$$(6) \quad \lambda^3 a_3 b \phi(b) \phi^2(b) \phi^3(r) + \lambda^2 a_2 b \phi(b) \phi^2(c) \phi^2(r)$$
$$+ \lambda a_1 b \phi(c) \phi^2(c) \phi(r) + a_0 c \phi(c) \phi^2(c) r = 0.$$

The strategy to decide whether L has a right factor of order one is the following. For every unitary pair $(b, c) \in \left(\mathbb{C}[z^{1/\ell}] \setminus \{0\} \right)^2$ such that $b|a_0$, $c|\phi^{-2}(a_3)$, we decide whether there exist $\lambda \in \mathbb{C}^\times$ and $r \in \mathbb{C}[z^{1/\ell}] \setminus \{0\}$ such that (6) holds. If we find a solution then we have a right factor of order one, otherwise there is no right factor of order one. Here, since $a_0 = q^3 z$, $a_3 = t$ are monomials in z (recall that $t \neq 0$) the choices are very limited. The only possibilities for the pair (b, c) are $(z^d, 1)$, with $0 \leqslant d \leqslant 1$. Recall that $\deg(a_3) = 0$, $\deg(a_2) = 2$, $\deg(a_1) = \deg(a_0) = 1$. The degrees of the terms in (6) are respectively given by

$$3d + \deg r(z), \quad 2 + 2d + \deg r(z), \quad 1 + d + \deg r(z), \quad 1 + \deg r(z)$$

and a direct calculation shows that, for $0 \leqslant d \leqslant 1$, $2 + 2d + \deg r(z)$ is greater than the remaining ones, whence there is no solution. We proceed similarly with the dual for the left factor of length one.

$$L^\vee = a_3(q^{-3}z)\sigma_q^{-3} + a_2(q^{-2}z)\sigma_q^{-2} + a_1(q^{-1}z)\sigma_q^{-1} + a_0(z)$$
$$= \sigma_q^{-3}\Big(a_3(z) + a_2(qz)\sigma_q + a_1(q^2 z)\sigma_q^2 + a_0(q^3 z)\sigma_q^3\Big)$$

Here the possible pairs for (b, c) are $(1, z^d)$, with $0 \leqslant d \leqslant 1$. The degrees of the terms of the equation corresponding to (6) are

$$1 + \deg r(z), \quad 1 + d + \deg r(z), \quad 2 + 2d + \deg r(z), \quad 3d + \deg r(z).$$

Again, for $0 \leqslant d \leqslant 1$, $2 + 2d + \deg r(z)$ is greater than the remaining ones.

Then, we will see in Section 4.2 that (5) is closely related to the computation of the difference Galois group of diagonal systems. In [vdPS97, Section 2.2], an algorithm is given to perform this task in the case (S) and when the α_i belong to $\mathbb{Q}(x)$. References to solve this problem when $n = 1$ is given in Remark 4.2. In the other situations, although that in practice we may solve this problem for

many examples, there are no general algorithm to perform the computation of the f_i, n_i.

3. Galois groups of difference systems

Consider the difference system (2) and let $G \subset \mathrm{GL}_n(C)$ be its Galois group. In order to compute G, we follow the strategy of the seminal paper [Hen98], that is, computing a gauge transformation $T \in \mathrm{GL}_n(\mathbf{k})$ such that $[\phi(T)AT^{-1}]$ is in reduced form. We will study the following cases (definitions of reducible and imprimitive groups are given in the corresponding section):

- G is reducible;
- G is irreducible and imprimitive;
- G is irreducible and primitive.

Before considering the particular case of difference equations of order 2 and 3, the aim of this section is to prove some general results for the Galois groups G of systems of the form (2), with $n \geqslant 2$.

3.1. The reducible case. — Let us treat the case where the Galois group G is reducible. By Lemma 2.4, G is reducible if and only if there exist $T \in \mathrm{GL}_n(\mathbf{k})$, $A_1 \in \mathrm{GL}_m(\mathbf{k})$, $m < n$, and A_2, A_3 matrices of convenient size, such that

$$\phi(T)AT^{-1} = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix}.$$

The strategy of reduction will follow the one given in the differential setting in [DW22, Section 5]. Let us assume that the bloc diagonal system $[D]$, where $D := \begin{pmatrix} A_1 & 0 \\ 0 & A_3 \end{pmatrix}$, is in reduced form and let us see how to reduce $[A]$. In general, $[D]$ is not in reduced form and we have to reduce the bloc diagonal system with a bloc diagonal gauge transformation. For small orders, we will see how to do this in practice but we want to emphasize the fact that reducing the bloc diagonal system is a hard task in general. We denote by $G_{\mathcal{D}}$ the Galois group of $[D]$.

LEMMA 3.1. — *Let B be a matrix of the form $\begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix}$ where $D := \begin{pmatrix} A_1 & 0 \\ 0 & A_3 \end{pmatrix}$ is such that the system $[D]$ is in reduced form. A matrix $T \in \mathrm{GL}_n(\mathbf{k})$ such that $\left[\phi(T)BT^{-1}\right]$ is reduced can be found of the form $T = \begin{pmatrix} \mathrm{Id}_m & \star \\ 0 & \mathrm{Id}_{n-m} \end{pmatrix}$.*

Proof. — It is the same kind of results as [DW22, Theorem 2.4] adapted to this difference context. We denote by G (respectively by $G_{\mathcal{D}}$) the Galois group of $[B]$ (respectively of $[D]$). Let H be the smallest algebraic group of upper bloc triangular matrices such that $B \in H(\mathbf{k})$. It is an algebraic group whose elements are

of the form $\begin{pmatrix} \mathscr{H}_1 & \mathscr{H}_2 \\ 0 & \mathscr{H}_3 \end{pmatrix}$. We denote by $H_{\mathcal{D}}$ the group whose matrices are of the form $\begin{pmatrix} \mathscr{H}_1 & 0 \\ 0 & \mathscr{H}_3 \end{pmatrix}$ where $\begin{pmatrix} \mathscr{H}_1 & \mathscr{H}_2 \\ 0 & \mathscr{H}_3 \end{pmatrix} \in H$ for a matrix $\mathscr{H}_2$, it is a block diagonal algebraic group. Let $H_{\mathcal{U}}$ (respectively $G_{\mathcal{U}}$) be the subgroup of H (respectively G) whose elements are of the form $\begin{pmatrix} \mathrm{Id}_m & \star \\ 0 & \mathrm{Id}_{n-m} \end{pmatrix}$. We have $H_{\mathcal{D}} \sim H/H_{\mathcal{U}}$. Let us prove that the group $H_{\mathcal{D}}$ is the smallest algebraic group such that $D \in H_{\mathcal{D}}(\mathbf{k})$. Indeed, considering the projection morphism $\pi : H \to H_{\mathcal{D}}$, where we identify $H/H_{\mathcal{U}}$ and $H_{\mathcal{D}}$, if there exists an algebraic group $\widetilde{H_{\mathcal{D}}} \subsetneq H_{\mathcal{D}}$ such that $D \in \widetilde{H_{\mathcal{D}}}(\mathbf{k})$, then the algebraic group $\widetilde{H} := \pi^{-1}(\widetilde{H_{\mathcal{D}}}) \subsetneq H$ is such that $B \in \widetilde{H}(\mathbf{k})$, which contradicts the minimality of H. Since $[D]$ is in reduced form, we have $G_{\mathcal{D}} = H_{\mathcal{D}}$. Let $R = \begin{pmatrix} R_1 & R_2 \\ 0 & R_3 \end{pmatrix} \in H(\mathbf{k})$ be such that the system $\left[\phi(R)BR^{-1}\right]$ is in reduced form. Let $R_{\mathcal{D}} := \begin{pmatrix} R_1 & 0 \\ 0 & R_3 \end{pmatrix} \in H_{\mathcal{D}}(\mathbf{k}) = G_{\mathcal{D}}(\mathbf{k})$.

Since $G_{\mathcal{D}} \sim G/G_{\mathcal{U}}$, there exists Q_2, such that $Q := \begin{pmatrix} R_1 & Q_2 \\ 0 & R_3 \end{pmatrix} \in G(\mathbf{k})$. Therefore $Q^{-1} = \begin{pmatrix} R_1^{-1} & \star \\ 0 & R_3^{-1} \end{pmatrix} \in G(\mathbf{k})$. A gauge transformation of $\phi(R)BR^{-1} \in G(\mathbf{k})$ by the matrix $Q^{-1} \in G(\mathbf{k})$ gives an element of $G(\mathbf{k})$. Hence $\left[\phi(T)BT^{-1}\right]$ is in reduced form where $T := Q^{-1}R = \begin{pmatrix} \mathrm{Id}_m & \star \\ 0 & \mathrm{Id}_{n-m} \end{pmatrix}$. $\qquad\square$

REMARK 3.2. — *As in* [DW22, *Section 5*]*, we may also consider the case where the system has more than two blocs. More precisely, consider a bloc triangular system* $[A]$*, where*

$$A = \begin{pmatrix} A_1 & A_{1,2} & \dots & \\ & A_2 & A_{2,3} & \\ & & \ddots & \\ 0 & & & A_k \end{pmatrix}.$$

Let us assume that the bloc diagonal system $[D]$*, with* $D = \mathrm{Diag}(A_1, \dots, A_k)$*, is in reduced form. Then, the proof of Lemma 3.1 may be adapted in that context and we find a gauge transformation* $T = \begin{pmatrix} \mathrm{Id} & \star & \dots & \star \\ 0 & \mathrm{Id} & \ddots & \vdots \\ & & \ddots & \star \\ & & & \mathrm{Id} \end{pmatrix} \in \mathrm{GL}_n(\mathbf{k})$ *such that*

$[\phi(T)AT^{-1}]$ *is in reduced form.*

3.2. The imprimitive case. — Let G be an algebraic subgroup of $\mathrm{GL}_n(C)$. We say that G is imprimitive if there exists a nontrivial decomposition into C-vector

spaces $C^n = V_1 \oplus \cdots \oplus V_k$, such that any element of G induces a permutation between the V_i. We say that G is primitive otherwise.

Consider G, an imprimitive group and let us write a decomposition $C^n = V_1 \oplus \cdots \oplus V_k$. The image of V_1 under an element of G is of the form V_j, where V_j and V_1 have the same dimension. If we further assume that G is irreducible, for all $1 \leqslant j \leqslant k$, there exists $\sigma \in G$, such that $\sigma(V_1) = V_j$, proving that each V_j has the same dimension and thus is a divisor of the order n of the equation (2). Therefore, when n is prime and G is irreducible, the situation is simplified since every space has dimension one. In what follows, we give information on the irreducible imprimitive groups that may occur as difference Galois groups when the order n of the system (2) is prime (see Theorem 3.5). Moreover, $\det(G)$ indicates which one of this information correspond to the Galois group G (see Proposition 3.7). More precisely, Theorem 3.5 and Proposition 3.7 imply the following result.

THEOREM 3.3. — *Assume that n is a prime number. Let $G \subset \mathrm{GL}_n(C)$ be an imprimitive irreducible group such that G/G^0 is finite and cyclic.*

1. If $\det(G) = C^*$ then $G^0 \sim (C^*)^n$ and $G/G^0 \sim \mathbb{Z}/n\mathbb{Z}$.
2. If $\det(G) = \mathbb{Z}/\nu\mathbb{Z}$ then $G^0 \sim (C^*)^{n-1}$ and $G/G^0 \sim \mathbb{Z}/ns\mathbb{Z}$ where

$$s = \begin{cases} \nu/n & \textit{if } \nu \in n\mathbb{N}^* \\ \nu & \textit{otherwise.} \end{cases}$$

At the end of this section, we explain how to compute a reduced form and a gauge transformation which gives this reduced form (see Proposition 3.10).

3.2.1. *Imprimitive groups that may occur.* — Let us now describe the possible irreducible imprimitive groups that may occur as difference Galois groups when n is prime. Let us begin by an elementary lemma that will be used several times. Note that the assumption n prime is not required for this lemma.

LEMMA 3.4. — *Let $G \subset \mathrm{GL}_n(C)$ be an irreducible group and let $H \triangleleft G$ be such that G/H is finite and cyclic. Then, H is not composed only of scalar matrices.*

Proof. — By contradiction, assume that H is composed only of scalar matrices. Since G/H is finite and cyclic, there exist a matrix $\mathscr{F}$ and some positive integer m such that $G = H \cup H\mathscr{F} \cup \cdots \cup H\mathscr{F}^{m-1}$. The matrix $\mathscr{F}$ is triangularisable and since H is formed by scalar matrices, it implies that there is a common basis of triangularisation of every elements of G, which contradicts the fact that G is irreducible. $\qquad\square$

For $(\alpha_1, \ldots, \alpha_n) \in (C^*)^n$, let

$$E_n(\alpha_1, \ldots, \alpha_n) := \begin{pmatrix} \alpha_1 & & & \\ & \ddots & & \\ & & & \alpha_{n-1} \\ \alpha_n & & & \end{pmatrix} = \text{Diag}(\alpha_1, \ldots, \alpha_n)E_n,$$

where $E_n = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ 1 & & \end{pmatrix}$ is the companion matrix with last row $(1, 0, \ldots, 0)$.

To lighten the notations, we will denote it E. For $(\alpha_1, \ldots, \alpha_n) \in (C^*)^n$, let $\bar{\alpha} := (\alpha_1, \ldots, \alpha_n)$ and let $\Pi\bar{\alpha} := \prod_{i=1}^{n} \alpha_i$. Note that $(E_n(\alpha_1, \ldots, \alpha_n))^n = (\Pi\bar{\alpha})\text{Id}_n$. Let $\mathcal{M}_\ell$ be the set of invertible matrices of the form $\text{Diag}(\alpha_1, \ldots, \alpha_n)E^\ell$. Note that $\mathcal{M}_0$ is composed of diagonal matrices. The following theorem gives information on the possible groups that may occur as Galois groups.

THEOREM 3.5. — *Assume that n is a prime number. Let $G \subset \text{GL}_n(C)$ be an imprimitive irreducible group such that G/G^0 is finite and cyclic. Then, up to a conjugation, one of the following holds:*

1. *$G = \bigcup_{\ell=0}^{n-1} \mathcal{M}_\ell$. In that case $G^0 \sim (C^*)^n$, $G/G^0 \sim \mathbb{Z}/n\mathbb{Z}$ and $\det(G) = C^*$.*
2. *There exists a positive integer s such that*

$$G \cap \mathcal{M}_0 = \{\text{Diag}(\alpha_1, \ldots, \alpha_n) \mid (\Pi\bar{\alpha})^s = 1\}$$

   and there exists $\mathcal{M}$ of the form $E_n(\beta_1, \ldots, \beta_n)$, where $\Pi\bar{\beta} = e^{2i\pi k/(ns)}$ with $\gcd(k, s) = 1$, such that G/G^0 is generated by $\mathcal{M}$. In that case, we find that $G^0 = \{\text{Diag}(\alpha_1, \ldots, \alpha_n) \mid \Pi\bar{\alpha} = 1\} \sim (C^*)^{n-1}$, $G/G^0 \sim \mathbb{Z}/ns\mathbb{Z}$ and

   (a) *if $n = 2$ then $\det(G) = \mathbb{Z}/(2s/\gcd(k+s, 2))\mathbb{Z}$;*
   (b) *if $n > 2$ then $\det(G) = \mathbb{Z}/(ns/\gcd(k, n))\mathbb{Z}$.*

Proof. — Up to a conjugation, G is a subgroup of $\bigcup_{\ell=1}^{n} \mathcal{M}_\ell$. Since G is irreducible, it contains a nondiagonal element thus there exists $0 < \ell < n$ such that G contains an element of $\mathcal{M}_\ell$. Using that G is a group, G contains an element of $\mathcal{M}_{k\ell}$ for all $k \in \mathbb{Z}$. Since n is prime, for all $0 \leqslant k' < n$, there exists an integer k such that $k\ell = k'$ mod n. This shows that G contains an element of $\mathcal{M}_{k'}$, for all $0 \leqslant k' < n$. Let $\mathcal{D}$ be the diagonal elements of G. It induces an algebraic subgroup of n copies of the multiplicative group.

Assume first that $\mathcal{D}$ is equal to the group of invertible diagonal matrices. Since the latter is connected, $G^0 = \mathcal{D}$. Thus, G contains all the invertible

diagonal elements. Since G contains an element of $\mathcal{M}_{k'}$ for all $0 \leqslant k' < n$ and contains $\mathcal{M}_0$ it follows that $G = \bigcup_{\ell=0}^{n-1} \mathcal{M}_\ell$. This is the first case.

Assume now that $\mathcal{D}$ is strictly included in the group of invertible diagonal matrices. Since $G \subset \bigcup_{\ell=1}^{n} \mathcal{M}_\ell$, we have $G^0 \subset \mathcal{D}$. There exists $(s_1, \ldots s_n) \in \mathbb{Z}^n$, where the s_i are not all zero, such that the diagonal matrices $\mathrm{Diag}(\alpha_1, \ldots, \alpha_n)$ in G satisfy $\prod_{j=1}^{n} \alpha_j^{s_j} = 1$. We recall that C is a subfield of $\mathbb{C}$, so that the modulus on C is well defined. We have $\sum_{j=1}^{n} s_j \ln(|\alpha_j|) = 0$.

Consider a matrix $P := E_n(\beta_1, \ldots, \beta_n) \in \mathcal{M}_1 \cap G$. We have

$$P \cdot \mathrm{Diag}(\alpha_n, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}) = \mathrm{Diag}(\alpha_1, \alpha_2, \ldots, \alpha_n) \cdot P.$$

Therefore, if $\mathrm{Diag}(\alpha_1, \alpha_2, \ldots, \alpha_n) \in G$ then $\mathrm{Diag}(\alpha_n, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}) \in G$. Iterating this computation, we obtain that the nonzero vector $\mathfrak{X} = (\ln(|\alpha_1|), \ldots, \ln(|\alpha_n|))^t$ is a solution of

$$B\mathfrak{X} = 0, \quad \text{where} \quad B = \begin{pmatrix} s_1 & s_2 & \cdots & s_n \\ s_n & s_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & s_2 \\ s_2 & \cdots & s_n & s_1 \end{pmatrix}.$$

Note that $B = \sum_{\ell=0}^{n-1} s_{\ell+1} E^\ell$ is a circulant matrix. Since E^n is the identity, E is diagonalisable with eigenvectors $\mathfrak{X}_k = (1, e^{2ik\pi/n}, \ldots, e^{2ik(n-1)\pi/n})^t$, $0 \leqslant k \leqslant n-1$, and its eigenvalues are the nth roots of unity:

$$E\mathfrak{X}_k = e^{2ik\pi/n} \mathfrak{X}_k.$$

These eigenvectors are also eigenvectors for every polynomial in E, in particular they are eigenvectors of B. Since E is diagonalisable, there exists $P \in \mathrm{GL}_n(C)$ such that $E = PD_0P^{-1}$, where $D_0 = \mathrm{Diag}(1, e^{2i\pi/n}, \ldots, e^{2i(n-1)\pi/n})$ is a diagonal matrix. Since $B\mathfrak{X} = 0$ and $P^{-1}BP = \sum_{\ell=0}^{n-1} s_{\ell+1} D_0^\ell$, the diagonal matrix $\sum_{\ell=0}^{n-1} s_{\ell+1} D_0^\ell$ has a nontrivial kernel, that is, one of its diagonal entries is zero: there exists $0 \leqslant k_0 \leqslant n-1$ such that $\sum_{\ell=0}^{n-1} s_{\ell+1} e^{2i\ell k_0\pi/n} = 0$. The nth roots of unity satisfy $z^n = 1$ and we have $z^n - 1 = (z-1)\Phi_n(z)$ where $\Phi_n(z) := 1 + z + \cdots + z^{n-1}$. Because n is prime, the cyclotomic polynomial Φ_n is irreducible on $\mathbb{Z}$. If $k_0 > 0$, then we must have $s := s_1 = \cdots = s_n \neq 0$. Let us prove by contradiction that we work in the case $k_0 \neq 0$.

By contradiction, assume that $k_0 = 0$. Then, $\sum_{\ell=0}^{n-1} s_{\ell+1} = 0$. Recall that the s_i are not all zero. In particular, we cannot be in the situation where $s_1 = \cdots = s_n$. From what precedes, this implies that for all $k \neq 0$ we have

$\mathfrak{X}_k \notin \ker(B)$. Thus, $\ker(B) = \operatorname{span}(\mathfrak{X}_0)$ and in particular $\mathfrak{X} \in \operatorname{span}(\mathfrak{X}_0)$, that is $\ln(|\alpha_1|) = \cdots = \ln(|\alpha_n|)$. We obtain

$$(7) \qquad\qquad |\alpha_1| = \ldots = |\alpha_n|.$$

Let $g := \gcd(s_1, \ldots, s_n)$, $s_i' := \frac{s_i}{g}$ and $\beta_i := \alpha_i^g$ for $i \in \{1, \ldots, n\}$. Since $\prod_{j=1}^n \alpha_j^{s_j} = 1$, we have $\prod_{j=1}^n \beta_j^{s_j'} = 1$. Thus, there exists $\ell_0 \in \mathbb{Z}$ such that $\sum_{j=1}^n s_j' \arg(\beta_j) = 2\pi\ell_0$. Moreover, since $\gcd(s_1', \ldots, s_n') = 1$, by the Bézout's identity, there exist $u_1, \ldots, u_n \in \mathbb{Z}$ such that $\sum_{j=1}^n u_j s_j' = 1$. We can replace $\arg(\beta_j)$ with $\arg(\beta_j) - 2\pi u_j \ell_0$ (new choices for the determinations of arguments), also called $\arg(\beta_j)$ to lighten notations. With these new choices, $\sum_{j=1}^n s_j' \arg(\beta_j) = 0$. Thus $\mathfrak{Y} := (\arg(\beta_1), \ldots, \arg(\beta_n))^t$ satisfies $B\mathfrak{Y} = 0$. As before (with $\mathfrak{Y}$ instead of $\mathfrak{X}$), we obtain

$$(8) \qquad\qquad \arg(\beta_1) = \ldots = \arg(\beta_n).$$

From (7) and (8), we have $\alpha_1^g = \ldots = \alpha_n^g$. Thus, in that case, there exists $g \in \mathbb{N}^*$ such that $\mathcal{D} \subset \{\operatorname{Diag}(\alpha_1, \ldots, \alpha_n) \in \operatorname{GL}_n(C) \mid \alpha_1^g = \ldots = \alpha_n^g\}$. Let us prove that the connected component of the identity of $\mathcal{D}$ is composed by scalar matrices. Indeed, with the equality $\alpha_1^g - \alpha_j^g = (\alpha_1 - \alpha_j)(\alpha_1^{g-1} + \alpha_1^{g-2}\alpha_j + \ldots + \alpha_1\alpha_j^{g-2} + \alpha_j^{g-1}) = 0$, we find that $\{\operatorname{Diag}(\alpha_1, \ldots, \alpha_n) \in \operatorname{GL}_n(C) \mid \alpha_1^g = \ldots = \alpha_n^g\}$ contains the closed set $\alpha_1 = \ldots = \alpha_n$. The latter is composed by scalar matrices and contains the connected component of the identity. This implies that the elements of G^0 are scalar matrices, which is a contradiction because of Lemma 3.4 (with $H := G^0$ in this lemma). Therefore, $k_0 > 0$ so we must have $s := s_1 = \cdots = s_n \neq 0$.

We proved that $\mathcal{D} \subset \mathcal{D}_s := \{\operatorname{Diag}(\alpha_1, \ldots, \alpha_n) \mid (\Pi\overline{\alpha})^s = 1\}$ and, since $\mathcal{D}_s = \mathcal{D}_{-s}$, we can assume that s is positive. If $\mathcal{D}$ is a strict subgroup of $\mathcal{D}_s$, the same reasoning implies that $\mathcal{D} \subset \mathcal{D}_{s'}$ for some s' that divides s. So, up to taking a smaller positive integer s, we may assume that $\mathcal{D} = \mathcal{D}_s$. In this case, $G^0 = \mathcal{D}_1$.

Let $\mathscr{F} := \operatorname{Diag}(\alpha_1, \ldots, \alpha_n)E^\ell \in \mathcal{M}_\ell \cap G$ be a non diagonal element of G which generates the finite group G/G^0 (we can choose in particular $0 < \ell < n$). Since n is prime, n is the smallest integer such that $\mathscr{F}^n$ is diagonal. We have $\mathscr{F}^n = \operatorname{Diag}(\Pi\overline{\alpha}, \ldots, \Pi\overline{\alpha})$ thus it satisfies $(\Pi\overline{\alpha})^{sn} = 1$. We have $\Pi\overline{\alpha} = e^{2\mathbf{i}\pi k/sn}$ for some integer $0 \leqslant k < sn$ and $\mathscr{F}^n$ has to generate the diagonal elements of G. This shows that $(\Pi\overline{\alpha})^n$ has to be a primitive sth root of unity, that is, k has to be coprime with s. Since G is defined up to an isomorphism and since $\mathscr{F}$ is conjugate to $\operatorname{Diag}(\alpha_{\mu(1)}, \ldots, \alpha_{\mu(n)})E$ where $\mu \in \mathfrak{S}_n$ is a permutation, we can assume (up to renumbering the α_i's, which can be done since we just have conditions on $\Pi\overline{\alpha}$) that $\mathscr{F} = \operatorname{Diag}(\alpha_1, \ldots, \alpha_n)E = E_n(\alpha_1, \ldots, \alpha_n)$.

The determinant of the diagonal elements is a power of $e^{2i\pi/s}$. When $n > 2$, n is odd and the determinant of $\mathscr{F}$ is $e^{2i\pi k/sn}$. When $n = 2$ the determinant of $\mathscr{F}$ is $-e^{2i\pi k/2s} = e^{2i\pi(k+s)/2s}$. The results on the determinant follow. $\square$

REMARK 3.6. — *When $n = 2$, we recover* [Hen98, Lemma 4.8].

Let us now see how $\det(G)$ helps us to distinguish the cases in Theorem 3.5 and compute s. We will explain how to compute $\det(G)$ in Section 4.1.

PROPOSITION 3.7. — *Assume that n is prime. Let $G \subset \mathrm{GL}_n(C)$ be an imprimitive irreducible group such that G/G^0 is finite and cyclic. The following statements holds.*

  – $\det(G) = C^*$ *if and only if G is the group in the case 1 of Theorem 3.5.*
  – *If $\det(G) = \mathbb{Z}/\nu\mathbb{Z}$, with $\nu \in n\mathbb{N}^*$, then $s = \nu/n$ where s is defined in Theorem 3.5.*
  – *Otherwise, $s = \nu$.*

Proof. — If $\det(G) = C^*$ we are clearly in the case case 1 of Theorem 3.5. The converse is also true.

Assume that $n \neq 2$, thus by Theorem 3.5, $\det(G) = \mathbb{Z}/(sn/\gcd(k,n))\mathbb{Z}$. We know the integers n, $\nu := (sn/\gcd(k,n))$ and we want to compute s. Note that, since n is prime, $\nu = sn/\gcd(k,n)$ is either sn or s. Let us prove that $\nu = s$ if and only if $\gcd(\nu, n) = 1$. If $\nu = s$ then $\gcd(k,n) = n$ and, since k is coprime with s, this implies $\gcd(n,s) = 1$, that is $\gcd(\nu,n) = 1$. Obviously, if $\nu = sn$ then $\gcd(\nu, n) = n$. Therefore, either $\gcd(\nu, n) = 1$ and $s = \nu$ or $\gcd(\nu, n) = n$ and $s = \nu/n$.

In the case $n = 2$, k is replaced by $k + s$. Note that $k + s$ is coprime with s and the same conclusion holds. $\square$

3.2.2. *How to compute a reduced form?* — First, we prove a result which is useful in what follows.

PROPOSITION 3.8. — *Let n be a prime number and let $H \subset \mathrm{GL}_n(C)$ be an irreducible group. Assume that K is not composed only of scalar matrices and $K \lhd H$. If H is a primitive group, then K is an irreducible group.*

Proof. — Let us prove by contradiction the irreducibility of K. If K is not irreducible, there exists a vector space $V \subsetneq C^n$ of minimal dimension $\nu > 0$ such that $K(V) = V$. We denote by $V_1, \ldots, V_k$ vector subspaces of C^n in direct sum such that $\nu = \dim(V_j)$ and $K(V_j) = V_j$. We then have $V_1 \oplus \cdots \oplus V_k \subset C^n$. Therefore $\nu k < n$ and k is bounded. Then, without loss of generalities we may assume that k is maximal, meaning that for all $V' \subset C^n$, with $\dim(V') = \nu$ and $K(V') = V'$, V' is not in direct sum with $V_1 \oplus \cdots \oplus V_k$.

We claim that $V_1 \oplus \cdots \oplus V_k = C^n$. To the contrary, assume that $V_1 \oplus \cdots \oplus V_k \subsetneq C^n$. By irreducibility of H, there exist $\mathscr{H} \in H$ and $\ell \in \{1, \ldots, k\}$ such that

$Y := \mathscr{H}(V_\ell)$, whose dimension is ν, is not included in $V_1 \oplus \cdots \oplus V_k$. Since K is a normal subgroup of H, $K\mathscr{H} = \mathscr{H}K$. In particular, $K(Y) = Y$ so Y is stable under K. Since $Y \cap (V_1 \oplus \cdots \oplus V_k)$ is stable under K, by minimality of the dimension ν, it follows that the dimension of $Y \cap (V_1 \oplus \cdots \oplus V_k)$ is either 0 or ν. In the first case, this proves that Y is in direct sum with $V_1 \oplus \cdots \oplus V_k$ and, in the second case, this proves that $Y \subset V_1 \oplus \cdots \oplus V_k$. In both situations this is a contradiction thus $V_1 \oplus \cdots \oplus V_k = C^n$. Hence $\nu k = n$ and, since n is prime, we have $k = n$ and $\nu = 1$. At this stage, we know that $V_1 \oplus \cdots \oplus V_n = C^n$ with $\dim(V_j) = 1$ and $K(V_j) = V_j$ for all $j \in \{1, \ldots, n\}$. This implies that K is composed of diagonal matrices in a basis $\mathcal{B}$ induced by $V_1, \ldots, V_n$.

Let us prove by contradiction that the common eigenspaces of the matrices in K must have the same dimension. Indeed, if it is not the case and if $W_1, \ldots, W_\ell$ are the eigenspaces of K of maximal dimension, then we have $W := W_1 \oplus \ldots \oplus W_\ell \subsetneq C^n$ (it is not C^n because we assume that there exists at least an eigenspace which has an another dimension). Since $K(W_i) = W_i$ for all $i \in \{1, \ldots, n\}$ and $K\mathscr{H} = \mathscr{H}K$ for all $\mathscr{H} \in H$, we have $K(\mathscr{H}(W_i)) = \mathscr{H}(W_i)$. Thus, by maximality of $\dim(W_i) = \dim(\mathscr{H}(W_i))$, $\mathscr{H}(W_i)$ is a common eigenspace of the matrices in K, that is $\mathscr{H}(W_i) = W_j$ for a certain j. Hence $\mathscr{H}(W_i) \subset W$, which proves that $H(W) \subset W$ (and taking the dimension, we have $H(W) = W$), in contradiction with the irreducibility of H.

We proved that the matrices in K are diagonal and we see that the common eigenspaces of the matrices in K have the same dimension. Since, the direct sum of these eigenspaces is C^n, this dimension must divides n, which is a prime number. Thus, this dimension is 1 or n. In the second case, it means that the matrices in K are scalar matrices, a contradiction with a hypothesis on K. In the first case, the eigenspaces are $V_1, \ldots, V_n$. As before, if $\mathscr{H} \in H$, for all $i \in \{1, \ldots, n\}$, we have $K(\mathscr{H}(V_i)) = \mathscr{H}(V_i)$. Thus, $\mathscr{H}(V_i)$, whose dimension is 1, is included in an eigenspace of K so $\mathscr{H}(V_i) = V_j$ for a $j \in \{1, \ldots, n\}$. We obtain in this case that any element of H induces a permutation between the V_i, which contradicts the fact that H is primitive. In both situations, we obtain a contradiction. Finally, K is irreducible. $\qquad\square$

The rest of the subsection is devoted to the computation of the reduced form. We recall that $A_{[\ell]} := \phi^{\ell-1}(A) \ldots A$ and $G_{[\ell]}$ is the difference Galois group of the system $\phi^\ell(Y) = A_{[\ell]}Y$. Let us first give a criterion of imprimitivity.

PROPOSITION 3.9. — *Assume that G is irreducible and n prime. It is imprimitive if and only if $G_{[n]}$ is diagonal.*

Furthermore, when G is imprimitive, the Riccati equation corresponding to $\phi^n(Y) = A_{[n]}Y$ admits a solution $d \in \mathbf{k}^*$ and we may assume that the $(1,1)$ entry of $A_{[n]}$ is d.

Proof. — If G is imprimitive but irreducible, there exists a gauge transformation T such that $B := \phi(T)AT^{-1}$ is an invertible matrix of the form
$$\begin{pmatrix} b_1 & & & \\ & \ddots & & \\ & & b_{n-1} & \\ b_n & & & \end{pmatrix}, \text{ where } b_i \in \mathbf{k}^*, \text{ and such that } [B] \text{ is in reduced form. Then,}$$
$\phi^n(T)A_{[n]}T^{-1} = \phi^{n-1}(B)\dots\phi(B)B =: B_{[n]}$ is diagonal. By Theorem 2.1, this proves that the Galois group of $\phi^n(Y) = A_{[n]}Y$ is diagonal.

Let us prove the converse. Assume that the Galois group of $\phi^n(Y) = A_{[n]}Y$ is diagonal, and G is irreducible. Consider a basis of C^n such that the matrices of $G_{[n]}$ are diagonal. Then, from Lemma 2.3, $G^0 = G^0_{[n]}$ thus G^0 is diagonal. Let us prove that G is imprimitive. From Lemma 3.4 (where $H := G^0$), the group G^0 is not composed only of scalar matrices. Thus, by Proposition 3.8 (applied to $H := G$ and $K := G^0$), if G is a primitive group then G^0 is irreducible, which contradicts the fact that G^0 is diagonal. Thus, G is imprimitive.

The statement on the Riccati equation is a consequence of Remark 2.6. □

Assume that G is irreducible, imprimitive and n is prime. By Proposition 3.9, the Riccati equation corresponding to $\phi^n(Y) = A_{[n]}Y$ admits a solution $d \in \mathbf{k}^*$. Assume that we are able to compute a reduced form of $\phi(y) = dy$, that is compute $f \in \mathbf{k}^*$ such that $\phi(y) = d\frac{\phi(f)}{f}y$ is reduced (see Section 4.1 for the case of order 1). The goal of what follows is to prove the following result.

PROPOSITION 3.10. — *Assume that G is irreducible, imprimitive and n prime. The system $\phi(Y) = AY$ is equivalent to $\phi(Y) = E_n(1,\dots,1,d)Y$. The system $\phi(Y) = E_n(1,\dots,1,f^{-1},\phi(f)d)Y$ is a reduced form of $\phi(Y) = E_n(1,\dots,1,d)Y$ with reduction matrix $\mathrm{Diag}(1,\dots,1,f)$.*

Let us begin by proving a technical lemma.

LEMMA 3.11. — *Assume that G is irreducible, imprimitive and n prime. Then, there exist $T \in \mathrm{GL}_n(\mathbf{k})$ and $u \in \mathbf{k}^*$ such that $\phi(T)AT^{-1} = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ u & & & \end{pmatrix}$, that is, $\phi(T)AT^{-1} = E_n(1,\dots,1,u)$.*

Proof. — This is inspired by [Hen98, Section 4.2]. By Theorem 2.1, there exist $T \in \mathrm{GL}_n(\mathbf{k})$ and $u_1,\dots,u_n \in \mathbf{k}^*$ such that $\phi(T)AT^{-1} = E_n(u_2,\dots,u_n,u_1)$. Let $D := \mathrm{Diag}(a_1,\dots,a_n)$. We have the following equality

$$\phi(D)E_n(u_2,\dots,u_n,u_1)D^{-1} = E_n\left(\frac{\phi(a_1)u_2}{a_2},\dots,\frac{\phi(a_{n-1})u_n}{a_n},\frac{\phi(a_n)u_1}{a_1}\right).$$

If we perform the gauge transformation $D := \mathrm{Diag}(1, u_2, 1, \ldots, 1)$, we may reduce to the case $u_2 = 1$. Then, if $n > 2$, performing the gauge transformation $D := \mathrm{Diag}(1, 1, \phi(u_2)u_3, 1, \ldots, 1)$, we may reduce to the case $u_3 = 1$. Iterating this process allows at the end to reduce to the case $u_2 = \cdots = u_n = 1$ and we change u_1 to $u := u_1\phi(u_n)\phi^2(u_{n-1})\ldots\phi^{n-1}(u_2)$. $\qquad\square$

Let us continue the proof of Proposition 3.10. By the previous lemma, we have that $[A]$ is equivalent to $E_n(1, \ldots, 1, u)$, therefore $\phi^n(Y) = A_{[n]}Y$ is equivalent to $\phi^n(Y) = \mathrm{Diag}(u, \phi(u), \ldots, \phi^{n-1}u)Y$. Unfortunately, we are not yet able to compute u. By Proposition 3.9, there exists a diagonal system $\phi^n(Y) = DY$, that is equivalent to $\phi^n(Y) = A_{[n]}Y$ with $(1,1)$ entry d. We write

$$D := \mathrm{Diag}(d_1, d_2, d_3, \ldots, d_n)$$

where we set $d_1 := d$. Let us now see that we may reduce to the case where $d_i = \phi^{i-1-i_1}(d)$ for an integer $i_1 \in \{1, \ldots, n\}$.

LEMMA 3.12. — *There exists a gauge transformation X and an integer $i_1 \in \{1, \ldots, n\}$ such that*

$$(9) \qquad \phi^n(X)DX^{-1} = \mathrm{Diag}(\phi^{-i_1}(d), \ldots, \phi^{n-1-i_1}(d)).$$

Proof. — Note that there exists an invertible matrix Z such that $\phi^n(Z)DZ^{-1} = \mathrm{Diag}(u, \phi(u), \ldots, \phi^{n-1}u)$. Let $Z_{i,j}$ be the entries of Z. Since Z is invertible, for all j there exists $i_j \in \{1, \ldots, n\}$ such that $Z_{i_j,j} \neq 0$. We can moreover assume that the i_j are distinct. Taking the (i_j, j)-coefficient in $\phi^n(Z)D = \mathrm{Diag}(u, \phi(u), \ldots, \phi^{n-1}(u))Z$ yields $\phi^n(Z_{i_j,j})d_j = \phi^{i_j-1}(u)Z_{i_j,j}$. Thus, for all $j \in \{1, \ldots, n\}$, there exist $i_j \in \{1, \ldots, n\}$ and $f_j \in \mathbf{k}^*$ such that

$$(10) \qquad\qquad \phi^n(f_j)d_j = \phi^{i_j-1}(u)f_j.$$

For $j = 1$ in (10), we have $\phi^{i_1-1}(u) = \frac{\phi^n(f_1)d_1}{f_1}$ thus $\phi^{i_j-1}(u) = \frac{\phi^n(\phi^{i_j-i_1}(f_1))\phi^{i_j-i_1}(d_1)}{\phi^{i_j-i_1}(f_1)}$. Therefore, from (10), setting $g_j := \frac{f_j}{\phi^{i_j-i_1}(f_1)}$, we obtain

$$\phi^n(g_j)d_j = \frac{\phi^n(f_j)d_j}{\phi^n(\phi^{i_j-i_1}(f_1))} = \frac{\phi^{i_j-1}(u)f_j}{\phi^n(\phi^{i_j-i_1}(f_1))} = \phi^{i_j-i_1}(d_1)g_j.$$

Applying ϕ^{i_1} to this equality, we proved that there exists an invertible diagonal matrix Z_0 and distinct integers $i_1, \ldots, i_n \in \{1, \ldots, n\}$ such that

$$\phi^n(Z_0)\phi^{i_1}(D)Z_0^{-1} = \mathrm{Diag}(\phi^{i_1}(d_1), \ldots, \phi^{i_n}(d_1)).$$

Thus there exists a permutation matrix Z_1 such that

$$\phi^n(Y)\phi^{i_1}(D)Y^{-1} = \mathrm{Diag}(d, \ldots, \phi^{n-1}(d)) \quad \text{with } Y := Z_1Z_0.$$

Thus,

$$\phi^n(X)DX^{-1} = \mathrm{Diag}(\phi^{-i_1}(d), \ldots, \phi^{n-1-i_1}(d)) \quad \text{where } X := \phi^{-i_1}(Y).$$

□

Thus, at this stage, we know the existence of $i_1 \in \{1, \ldots, n\}$ such that $\phi^n(Y) = A_{[n]}Y$ is equivalent to

$$\phi^n(Y) = \mathrm{Diag}(\phi^{-i_1}(d), \phi^{1-i_1}(d), \ldots, \phi^{n-1-i_1}(d))Y.$$

Since the system $\phi^n(Y) = \mathrm{Diag}(\phi^{-i_1}(d), \phi^{1-i_1}(d), \ldots, \phi^{n-1-i_1}(d))Y$ is diagonal, we may assume that we have a diagonal fundamental matrix of solutions U. This matrix can be taken of the form $U = \mathrm{Diag}(y, \phi(y), \ldots, \phi^{n-1}(y))$. Then,

$$\phi(U) = FU, \quad \text{where} \quad F := \begin{pmatrix} & & 1 & \\ & & & \ddots & \\ & & & & 1 \\ \phi^{-i_1}(d) & & & \end{pmatrix} = E_n(1, \ldots, 1, \phi^{-i_1}(d)).$$

By construction, $F_{[n]} = \mathrm{Diag}(\phi^{-i_1}(d), \phi^{1-i_1}(d), \ldots, \phi^{n-1-i_1}(d))$. We thus have two ϕ^n- systems $\phi^n(Y) = A_{[n]}Y$ and $\phi^n(Y) = F_{[n]}Y$, that are equivalent and we want to prove that they are equivalent as ϕ-system. This is the goal of the next lemma.

LEMMA 3.13. — *Let $F \in \mathrm{GL}_n(\mathbf{k})$ be such that the systems $\phi^n(Y) = F_{[n]}Y$ and $\phi^n(Y) = A_{[n]}Y$ are equivalent. Then, the systems $[A]$ and $[F]$ are equivalent.*

Proof. — Let us consider $\phi(Y) = \mathrm{Diag}(A, F)Y$. It admits a fundamental solution of the form $\mathrm{Diag}(\mathcal{Y}, \mathcal{Z})$ where $\mathcal{Y}$ and $\mathcal{Z}$ are fundamental matrices of solutions of $\phi(Y) = AY$ and $\phi(Y) = FY$ respectively. Without loss of generalities, we may assume that $\mathrm{Diag}(\mathcal{Y}, \mathcal{Z}) \in \mathrm{GL}_{2n}(\mathbf{L})$, where $\mathbf{L}$ is a Picard-Vessiot extension for $\phi(Y) = \mathrm{Diag}(A, F)Y$ over $\mathbf{k}$. We have $\phi^n(\mathcal{Y}) = A_{[n]}\mathcal{Y}$ and $\phi^n(\mathcal{Z}) = F_{[n]}\mathcal{Z}$. By hypothesis, there exists $T \in \mathrm{GL}_n(\mathbf{k})$ such that $\mathcal{X} := T\mathcal{Y}$ is a solution of $\phi^n(Y) = F_{[n]}Y$. This implies that $P := \mathcal{X}^{-1}\mathcal{Z} \in \mathrm{GL}_n(\mathbf{L})$ is a ϕ^n-constant matrix. Recall that $C_{\mathbf{L}} = C$. By [DH21, Lemma C.1], with $K = C, L = \mathbf{L}$ the entries of P are algebraic over C. Since C is algebraically closed, the entries belong to C so we have

$$A = \phi(\mathcal{Y})\mathcal{Y}^{-1} = \phi(T^{-1})\phi(\mathcal{X})\mathcal{X}^{-1}T = \phi(T^{-1})\phi(\mathcal{Z})\mathcal{Z}^{-1}T = \phi(T)^{-1}FT.$$

□

Let us finish the proof of Proposition 3.10. From what precedes, $[A]$ is equivalent to $[F]$ where $F = E_n(1, \ldots, 1, \phi^{-i_1}(d))$. Using the following lemma and the fact that $\phi(1) = 1$, we obtain that this system is equivalent to $[J]$, where $J := E_n(1, \ldots, 1, d)$.

LEMMA 3.14. — *Let $J \in \mathrm{GL}_n(\mathbf{k})$ and $\ell \in \mathbb{N}$. The systems $[\phi^\ell(J)]$ and $[\phi^{\ell+1}(J)]$ are equivalent.*

Proof. — It follows from the fact that $\phi^{\ell+1}(J) = \phi(X)\phi^\ell(J)X^{-1}$ with $X := \phi^\ell(J)$. $\qquad\square$

Thus, we have that $[A]$ and $[J]$ are equivalent systems. Now, we perform the gauge transformation $S = \mathrm{Diag}(1, \ldots, 1, f)$ to find that $[A]$ is equivalent to $\phi(Y) = E_n(1, \ldots, 1, f^{-1}, d\phi(f))Y$. It remains to check that this system is in a reduced form.

By Theorem 2.1, there exists a reduction matrix of the form $T := \mathrm{Diag}(f_1, \ldots, f_n)E^k$. Note that T may be the identity. We are going to apply Theorem 3.5 and look at the product of the nonzero entries of $B := \phi(T)E_n(1, \ldots, 1, f^{-1}, d\phi(f))T^{-1}$. The latter is $\frac{\phi(f_1 \times \cdots \times f_n)}{f_1 \times \cdots \times f_n}\frac{\phi(f)}{f}d$. Since $\phi y = \frac{\phi(f)}{f}dy$ is in reduced form, the algebraic group generated by $\frac{\phi(f_1 \times \cdots \times f_n)}{f_1 \times \cdots \times f_n}\frac{\phi(f)}{f}d$ is bigger than the algebraic group generated by $\frac{\phi(f)}{f}d$. Since $[B]$ is reduced, by Theorem 2.1, it is also smaller, proving that the algebraic group generated by $\frac{\phi(f_1 \times \cdots \times f_n)}{f_1 \times \cdots \times f_n}\frac{\phi(f)}{f}d$ is the algebraic group generated by $\frac{\phi(f)}{f}d$. By Theorem 2.1 again, this shows that $\phi(Y) = E_n(1, \ldots, 1, f^{-1}, d\phi(f))Y$ is already reduced.

EXAMPLE 3.15. — *Let us go back to the example* (1) *and recall, see Example 2.7, that the difference Galois group G is irreducible. Assume that $t \neq 0$. Instead of applying the criterion of Proposition 3.9 to show that G is imprimitive, let us use a shortcut. We refer to* [RSZ13, Section 2.2] *for more details on what follows. We define the Newton polygon of a q-difference operator $L = \sum_i a_i\phi^k$ as the convex hull in $\mathbb{R}^2$ of*

$$\{(i,j) \mid i,j \in \mathbb{Z},\ j \geqslant \mathrm{val}(a_i(z))\} \subset \mathbb{R}^2$$

where $\mathrm{val} : \mathbb{C}((z)) \to \mathbb{Q} \cup \{+\infty\}$ *denotes the z-adic valuation. The Newton polygon is invariant by an analytic change of variables. By Lemma 3.11, when n is prime, if the difference Galois group of an equation is irreducible and imprimitive, then the lower bound of the Newton polygon is delimited by the segment from $(0, \mathrm{val}(u))$ to $(n, 0)$. In Example (1), the lower part is composed of the segment delimited by $(0,1)$ and $(1,0)$ and the segment delimited by $(1,0)$ and $(3,0)$, see Figure 1. Since G is irreducible, see Example 2.7, we find that G is primitive.*
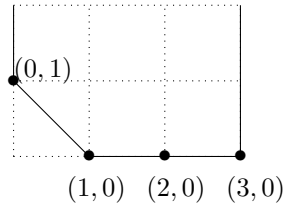

FIGURE 1. The Newton polygon of the operator associated with $U(z,t)$.

3.3. The primitive case. — In this section, we assume that G is irreducible, primitive, and n is prime. We want to prove that the same holds for G^0 and $D(G^0)$ where $D(G^0)$ denotes the derived group of G^0. Note that G^0 is a connected normal subgroup of G and $D(G^0)$ is a connected normal subgroup of G^0.

First, we recall the following result given in [ADH21, Lemma 4.2].

LEMMA 3.16. — *If $K \subset \mathrm{GL}_n(C)$ is a connected and irreducible algebraic group, then K is also primitive.*

LEMMA 3.17. — *Let n be a prime number. If $H \subset \mathrm{GL}_n(C)$ is an irreducible and primitive group, then the derived subgroup of H, denoted by $D(H)$, is not composed only of scalar matrices.*

Proof. — By contradiction, assume that $D(H)$ is composed only of scalar matrices. In this case, for all $\mathscr{G}, \mathscr{H} \in H$, there exists $\alpha \in C^*$ such that $\mathscr{G}\mathscr{H}\mathscr{G}^{-1}\mathscr{H}^{-1} = \alpha\mathrm{Id}_n$, that is $\mathscr{G}\mathscr{H} = \alpha\mathscr{H}\mathscr{G}$. The group H is irreducible so there exists $\mathscr{H}_0 \in H$ having an eigenspace W of maximal dimension $\nu < n$, otherwise H would be composed of scalar matrices, contradicting its irreducibility. Let V be the direct sum of the eigenspaces of $\mathscr{H}_0$ of dimension ν. From the previous equality and the fact that $\mathscr{H}_0(W) = W$, we obtain that

$$(11) \qquad \forall \mathscr{G} \in H, \;\; \mathscr{H}_0(\mathscr{G}(W)) = \mathscr{G}(W).$$

Thus, $\mathscr{G}(W)$ is also an eigenspace of $\mathscr{H}_0$ of dimension ν for all $\mathscr{G} \in H$ so $H(W) \subset V$. Therefore, $H(V) \subset V$ (in fact, taking the dimension, it is an equality of vector spaces) which implies that $V = C^n$ by irreducibility of H. Hence ν divides n. Since n is a prime number and $\nu < n$, we have $\nu = 1$. This means that $\mathscr{H}_0$ is a diagonal matrix with distinct eigenvalues and we denote by $V_1, \ldots, V_n$ its eigenspaces. However, from (11) with $W := V_1$, we obtain that every $\mathscr{G} \in H$ induces a permutation between the V_i, which contradicts the fact that H is primitive. $\qquad\square$

PROPOSITION 3.18. — *Assume that n is prime and $G \subset \mathrm{GL}_n(C)$ is an irreducible and primitive group. Then, the same holds for G^0 and $D(G^0)$ and we may write $G^0 = Z(G^0).D(G^0)$ where $Z(G^0)$ denotes the center of G^0.*

Proof. — We recall that G^0 is a connected normal subgroup of G and $D(G^0)$ is a connected normal subgroup of G^0.

From Lemma 3.4 (with $H := G^0$), G^0 is not composed only of scalar matrices. Thus, by Proposition 3.8 (with $H := G$ and $K := G^0$), G^0 is irreducible. Using Lemma 3.16, G^0 is also primitive. Then, the irreducibility of $D(G^0)$ follows from Lemma 3.17 (with $H := G^0$) and Proposition 3.8 (with $H := G^0$ and $K := D(G^0)$). Thanks to Lemma 3.16, $D(G^0)$ is also primitive.

By [Spr98, Corollary 8.1.6], any connected algebraic group H satisfies $H \sim Z(H).D(H)$, which proves that $G^0 = Z(G^0).D(G^0)$. $\qquad\square$

4. Galois groups of equations of order one and diagonal systems

4.1. Galois groups of equations of order one. — We consider the equation of order one

$$(12) \qquad \qquad \phi(y) = \alpha y \quad \alpha \in \mathbf{k}^*.$$

Let us now see how to compute the Galois group G and a reduced form of this difference equation. Recall that since $G \subset \mathrm{GL}_1(C)$ is an algebraic group, either G is C^*, or it is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ for some $\ell \in \mathbb{N}^*$.

PROPOSITION 4.1. — *We have $G \sim \mathbb{Z}/\ell\mathbb{Z}$ if and only if there exists ζ, a primitive ℓth root of unity and a nonzero solution $f \in \mathbf{k}^*$ of $\phi(y) = (\zeta/\alpha)y$. In that situation, $\zeta = \alpha \frac{\phi(f)}{f}$, and $[\zeta]$ is a reduced form of $[\alpha]$ with a gauge transformation (f).*

Proof. — Since the Galois group G of (12) is an algebraic subgroup of $C^\star$, it is a finite cyclic group or the multiplicative group $C^\star$. Any equivalent equation of (12) is of the form $\phi(y) = \alpha \frac{\phi(f)}{f} y$ with $f \in \mathbf{k}^\star$. Therefore, from Theorem 2.1, if G is a finite cyclic group of order $\ell \in \mathbb{N}^*$ then there exist $f \in \mathbf{k}^\star$ and ζ, a primitive ℓth root of unity, such that $\zeta = \alpha \frac{\phi(f)}{f}$.

Conversely, assume that there exist $f \in \mathbf{k}^\star$ and ζ, a primitive ℓth root of unity, such that $\zeta = \alpha \frac{\phi(f)}{f}$. From Theorem 2.1, G is contained in $\mathbb{Z}/\ell\mathbb{Z}$. Then, $G \sim \mathbb{Z}/\ell_1\mathbb{Z}$ where ℓ_1 divides ℓ. Then, there exist $g \in \mathbf{k}^\star$ and ζ_1, a primitive ℓ_1th root of unity, such that $\zeta_1 = \alpha \frac{\phi(g)}{g}$. This implies $\alpha^{\ell_1} = g^{\ell_1}/\phi(g^{\ell_1})$. Let $h := (f/g)^\ell$. Thus, $\phi(h) = h$ so $h \in C^*$. Since C is algebraically closed, there exists $c \in C^*$ such that $f = cg$ (with $c^\ell = h$). Using this equality, we obtain $\zeta = \zeta_1$ and since ζ is a primitive ℓth root of unity, $\ell = \ell_1$. $\qquad\square$

REMARK 4.2. — *Then, given $\alpha \in \mathbf{k}^*$, we have to determine whether there exist $\ell \in \mathbb{N}^*$ and $f \in \mathbf{k}^*$ such that $\phi(f) = (\zeta/\alpha)f$, where ζ is a primitive ℓth root of unity. This is essentially (5) in the case $n = 1$. Contrary to the case of an arbitrary n, there are many situations where algorithms exist to solve this problem. Let us describe them briefly.*

Consider the case (S). If such f exists, $\phi(f)/f$ tends to 1 as z goes to ∞. Hence, α tends to ζ as z goes to ∞. So the algorithm to find (f,ζ) is the following. Consider the limit of α when z goes to ∞. If this limit is not a root of unity, then the difference Galois group of (12) is C^*. Otherwise, the limit is ζ a primitive ℓth root of unity, for some $\ell \in \mathbb{N}^*$. Then, the difference Galois group is $\mathbb{Z}/\ell\mathbb{Z}$ if and only if the difference equation $\phi(y) = (\zeta/\alpha)y$ has a solution in $\mathbf{k}^*$. Otherwise it is C^*. Recall that we assumed, see Section 2.3, that we are able to find all the solution in $\mathbf{k}^*$ of linear difference equations.

Consider the case (Q). If such f exists, $\phi(f)/f$ tends to q^n as z goes to ∞, where n is the degree of f. Consider the limit of α when z goes to ∞. If this

limit is not of the form ζq^n (see the footnote [1]), where ζ is a root of unity and $n \in \mathbb{Q}$, then the difference Galois group of (12) is C^*. Otherwise, let $\ell \in \mathbb{N}^*$ be the order of the primitive root. Then, the difference Galois group is $\mathbb{Z}/\ell\mathbb{Z}$ if and only if the difference equation $\phi(y) = (\zeta/\alpha)y$ has a solution in $\mathbf{k}^*$. Otherwise it is C^*.

Consider the case (M). If such f exists, $\phi(f)/f$ is equivalent to $z^{(p-1)n}$ as z goes to ∞, where n is the degree of f. If α is not equivalent to ζz^m for some rational number m, and ζ a root of unity, then the difference Galois group of (12) is C^*. Otherwise, let ℓ be the order of the primitive root. Then, the difference Galois group is $\mathbb{Z}/\ell\mathbb{Z}$ if and only if the difference equation $\phi(y) = (\zeta/\alpha)y$ has a solution in $\mathbf{k}^*$. Otherwise it is C^*.

For the case (E), there is no algorithm to perform this task in full generality.

REMARK 4.3. — *Since $\det(G)$ is the Galois group of $\phi(y) = \det(A)y$, an equation of order 1, we may now compute $\det(G)$ if we are able to reduce the difference equations of order 1.*

EXAMPLE 4.4. — *Consider the difference equation (1) and let G be its difference Galois group over $\mathbb{C}(z^{1/*})$. Assume that $t \neq 0$. We want to compute $\det(G)$. We have to compute the difference Galois group of $\phi(y) = \frac{-q^3 z}{t}y = \alpha y$ over $\mathbf{k} = \mathbb{C}(z^{1/*})$. By Proposition 4.1, $\det(G)$ is finite if and only if there exists ζ, a primitive ℓth root of unity, and a nonzero solution $f \in \mathbf{k}^*$ of $\phi(y) = (\zeta/\alpha)y$. But the valuation of α at $z = 0$ is 1, proving that ζ/α must have valuation -1. Since for $f \in \mathbf{k}^*$, f and $\phi(f)$ have the same valuation, the equation $\phi(f) = (\zeta/\alpha)f$ with $f \in \mathbf{k}^*$, and ζ a root of unity, has no solutions. Therefore, $\det(G) = \mathbb{C}^*$.*

4.2. Galois groups of diagonal systems. — For more details on what follows, we refer to [vdPS97, Section 2.2]. Let us consider a diagonal system

$$(13) \qquad \phi(Y) = \mathrm{Diag}\,(\alpha_1, \ldots, \alpha_n)\,Y$$

where $\mathrm{Diag}\,(\alpha_1, \ldots, \alpha_n) \in \mathrm{GL}_n\,(\mathbf{k})$ is the diagonal matrix whose nonzero entry at the line i is α_i. By Theorem 2.1, the Galois group is an algebraic subgroup of the n-dimensional torus T. The matrices of G are of the form $\mathrm{Diag}(c_1, \ldots, c_n)$. We recall that a character on T is a morphism $\chi : T \to C^\star$. It is of the form $\chi_{\mathbf{m}}(z_1, \ldots, z_n) = z_1^{m_1} \ldots z_n^{m_n}$ with $\mathbf{m} := (m_1, \ldots, m_n) \in \mathbb{Z}^n$. Since an algebraic subgroup of T is the intersection of the kernels of some characters on T, we have to find the $\mathbf{m} \in \mathbb{Z}^n$ such that $c_1^{m_1} \ldots c_n^{m_n} = 1$ for all $\mathrm{Diag}(c_1, \ldots, c_n) \in G$.

---

[1]A complex number η is of this form if and only if $n := \ln(|\eta|)/\ln(|q|)$ is a rational number and $\zeta := \eta/q^n$ is a root of unity. Let $\eta = \lim_{z \to +\infty} \alpha(z)$ and assume that $\eta \in C^\star$ (if this limit is not finite or if $\eta = 0$ then η is not of the form ζq^n). By construction, η is a quotient of two coefficients of α (a data). If we look at an equation with rational coefficients and with $q \in \mathbb{Q}$ then $\eta \in \mathbb{Q}$, $\zeta = \pm 1$ and one can check the existence of $n \in \mathbb{Q}$ looking at the prime factor decompositions of q and η.

By Theorem 2.1, a gauge transformation which reduces the system will be diagonal, denoted by $\mathrm{Diag}(f_1, \ldots, f_n)$. Thus, the difference Galois group of (13) is the intersection of the kernels of the $\chi_{\mathbf{m}}$ for all $\mathbf{m} \in \mathbb{Z}^n$ such that there exist $f_1, \ldots, f_n \in \mathbf{k}^*$ satisfying

$$(14) \qquad \left(\frac{\phi(f_1)}{f_1} \alpha_1 \right)^{m_1} \times \ldots \times \left(\frac{\phi(f_n)}{f_n} \alpha_n \right)^{m_n} = 1.$$

The question of how to solve (14) depends on the examples (see one example in [vdPS97, Section 2.2]). There is no algorithm to perform this task in full generality.

5. Galois groups of equations of order two

Consider a difference equation of order 2

$$\phi^2(y) + a_1 \phi(y) + a_0 y = 0, \quad \text{where} \quad a_i \in \mathbf{k} \quad \text{and} \quad a_0 \neq 0.$$

Let

$$L := \phi^2 + a_1 \phi + a_0 \in \mathbf{k} \left\langle \phi, \phi^{-1} \right\rangle$$

be the corresponding difference operator and let $G \subset \mathrm{GL}_2(C)$ be its Galois group. We want to compute G. An algorithm in the cases (Q), (S), (E), (M) is presented in [Hen97, Hen98, DR15, Roq18] respectively.

Reducible case. — We first decide whether L has a right factor of order one. This is the case if and only if G is reducible. Recall, see Lemma 2.5, that it is equivalent to the existence of a solution α of the Riccati equation $\phi(y)y + a_1 y + a_0 = 0$.

Assume first that L is reducible and let us write $L = (\phi - \beta)(\phi - \alpha)$. Then, α is a solution of the Riccati equation $\phi(y)y + a_1 y + a_0 = 0$, and β is determined by $\alpha\beta = a_0$. The difference equation is equivalent to $\phi(Y) = AY$ where $A = \begin{pmatrix} \alpha & 1 \\ 0 & \beta \end{pmatrix}$. We now follow the strategy of Section 3.1. As in the diagonal case, we reduce the diagonal system $\phi(Y) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} Y$ with a diagonal matrix D. Let $B := \phi(D)AD^{-1}$, with $B = \begin{pmatrix} \alpha' & \gamma' \\ 0 & \beta' \end{pmatrix}$. By [Hen98, Lemma 4.4], either $[B]$ is already reduced, or a reduced form is $\begin{pmatrix} \alpha' & 0 \\ 0 & \beta' \end{pmatrix}$. We now have to decide if there exists $t \in \mathbf{k}$ such that $T = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ satisfies $\phi(T)B = \begin{pmatrix} \alpha' & 0 \\ 0 & \beta' \end{pmatrix} T$. Note that this is equivalent to

$$\gamma' + \phi(t)\beta' = \alpha' t.$$

So we just have to decide if an equation of order 1 has a solution t in $\mathbf{k}$ or not. If such a t exists, then the reduction matrix is given by TD, and a reduced

form is $\begin{pmatrix} \alpha' & 0 \\ 0 & \beta' \end{pmatrix}$. Otherwise, the reduction matrix is given by D and a reduced form is $\begin{pmatrix} \alpha' & \gamma' \\ 0 & \beta' \end{pmatrix}$.

Imprimitive case. — Assume now that G is irreducible. It is imprimitive if and only if the difference Galois group of $\phi^2(Y) = A_{[2]}Y$ is diagonal. We use the reducible case (with ϕ replaced by ϕ^2) to check this property. In that case we are able to compute $d \in \mathbf{k}^*$, solution of the Riccati equation corresponding to $\phi^2(Y) = A_{[2]}Y$. We now follow Proposition 3.10. The system $[A]$ is equivalent to $\phi(Y) = \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix}Y$. Let us compute a reduced form of $\phi(y) = dy$, that is compute $f \in \mathbf{k}^*$ such that $\phi(y) = d\frac{\phi(f)}{f}y$ is reduced. Then, a reduced form is given by $\begin{pmatrix} 0 & f^{-1} \\ \phi(f)d & 0 \end{pmatrix}$ and a reduction matrix is given by $\mathrm{Diag}(1, f)$.

Primitive case. — Assume that G is irreducible and primitive. By [Hen98, Section 4.4], either $G = \mathrm{GL}_2(C)$, or there exists an integer k such that

$$G = \{M \in \mathrm{GL}_2(\mathbb{C}) \mid \det(M)^k = 1\}.$$

Recall that $a_0 = \det(A)$ and the algebraic group $\det(G)$ is the difference Galois group of $\phi(y) = a_0 y$, a system of order 1. Let $f \in \mathbf{k}^*$ be such that $\phi(y) = a_0\frac{\phi(f)}{f}y$ is reduced with Galois group $\det(G)$. Then, we perform, as in [Hen98, Section 4.4], the gauge transformation $T = \mathrm{Diag}(f, 1)$ to obtain a system $[B]$. Since $\det(B) = a_0\frac{\phi(f)}{f}$, and $\phi(y) = a_0\frac{\phi(f)}{f}y$ is reduced with Galois group $\det(G)$, we find that $B \in G(\mathbf{k})$. Then, B is a reduced form and T is the reduction matrix.

6. Galois groups of equations of order three

Consider a linear difference equation of order 3

$$\phi^3(y) + a_2\phi^2(y) + a_1\phi(y) + a_0 y = 0, \quad \text{where} \quad a_i \in \mathbf{k} \quad \text{and} \quad a_0 \neq 0.$$

Let

$$L := \phi^3 + a_2\phi^2 + a_1\phi + a_0 \in \mathbf{k}\left\langle \phi, \phi^{-1} \right\rangle$$

be the corresponding difference operator and let $G \subset \mathrm{GL}_3(C)$ be its Galois group. We want to compute G.

6.1. Reducible case. — We follow the strategy explained in Section 3.1 to treat the case where G is reducible. By [ADH21, Lemma 4.4], G is reducible if and only if the operator L admits a right factor. The right factor can have order one or two. So G is reducible if and only if the operator admits a right or left

factor of order one. Recall that up to consider the dual, we may reduce to the case where there is a right factor of order 1.

Recall, see Lemma 2.5, that the existence of a right factor of order one is equivalent to the existence of a solution $\alpha \in \mathbf{k}$ of the Riccati equation $\phi^2(y)\phi(y)y + a_2\phi(y)y + a_1 y + a_0 = 0$. Assume that L admits a right factor of order one. Let us write L as $\widetilde{L}(\phi - \alpha)$ where $\widetilde{L} := \phi^2 - \beta\phi - \gamma$. Then, the system $[A_L]$ is equivalent to the system

$$\phi(Y) = \left(\begin{array}{c|cc} \alpha & 1 & 0 \\ \hline 0 & & A_2 \end{array}\right) Y,$$

where the matrix A_2 corresponds to the equation of order two $\widetilde{L}y = 0$ (that is $A_2 = A_{\widetilde{L}}$). From the order one and order two cases, we know how to compute $T_1 \in \mathrm{GL}_1(\mathbf{k})$ and $T_2 \in \mathrm{GL}_2(\mathbf{k})$ such that the systems whose matrices are $\phi(T_1)\alpha T_1^{-1}$ and $\phi(T_2)A_2 T_2^{-1}$ are in reduced form. Let us consider

$$A := \begin{pmatrix} \phi(T_1) & 0 \\ 0 & \phi(T_2) \end{pmatrix} \left(\begin{array}{c|cc} \alpha & 1 & 0 \\ \hline 0 & & A_2 \end{array}\right) \begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix}^{-1}.$$

This matrix A is of the form $\begin{pmatrix} \phi(T_1)\alpha T_1^{-1} & \star \\ 0 & \phi(T_2)A_2 T_2^{-1} \end{pmatrix}$. The first step consists in reducing the bloc diagonal system $[D]$ where $D := \begin{pmatrix} \phi(T_1)\alpha T_1^{-1} & 0 \\ 0 & \phi(T_2)A_2 T_2^{-1} \end{pmatrix}$. Let $G_{\mathcal{D}}$ be the Galois group of this system, let G_1 be the Galois group of $[\phi(T_1)\alpha T_1^{-1}]$ and let G_2 be the Galois group of $[\phi(T_2)A_2 T_2^{-1}]$. The algebraic group $G_{\mathcal{D}}$ is an algebraic subgroup of $G_1 \times G_2$. We explain the reduction on a case-by-case approach with respect to G_2. We will see that in each situation, reducing $[D]$ is equivalent to reducing a diagonal system whose reduction is explained in Section 4.2. Theorem 6.1 summarize the results we are going to prove for this first step.

THEOREM 6.1. — • *Assume that G_2 is composed of diagonal matrices. We can assume that D is diagonal. Then, we have to reduce a diagonal system and the reduction is explained in Section 4.2.*
• *Assume that G_2 is reducible and the first case does not hold. We can assume that D is upper triangular. Then, the reduction matrix is the diagonal matrix T that reduces the diagonal system $[\mathrm{Diag}(a, b, d)]$, where a, b, d are the diagonal entries of D.*
• *Assume that G_2 is imprimitive and irreducible. We can assume that $\phi(T_2)A_2 T_2^{-1}$ is an anti-diagonal matrix. Then $D_{[2]}$ is diagonal. The reduction matrix that reduces $[D]$ is the matrix T that reduces the diagonal ϕ^2-system $\phi^2(Y) = D_{[2]}Y$.*
• *Assume that G_2 is primitive and irreducible. The reduction matrix is given by*

$T := \mathrm{Diag}(r_1, r_2, 1)$, *where* $\mathrm{Diag}(r_1, r_2)$ *is the reduction matrix of the diagonal system* $\phi(Y) = \begin{pmatrix} \phi(T_1)\alpha T_1^{-1} & 0 \\ 0 & \det(\phi(T_2)A_2 T_2^{-1}) \end{pmatrix} Y$.

Let us now prove the theorem.

Proof. — • Assume that G_2 is formed by diagonal matrices. Then, D is diagonal, $G_{\mathcal{D}}$ is an algebraic group of diagonal matrices and the reduction is explained in Section 4.2.

• Assume that G_2 is reducible but not formed by diagonal matrices. Up to a conjugation, we may assume that G_2 is formed by upper triangular matrices. By the classification of such nondiagonal reducible algebraic groups that can be found in [Hen98, Lemma 4.4], the upper triangular entry can be any element of C^*. We can assume that the matrix D is of the form $\begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & 0 & d \end{pmatrix}$ with $c \neq 0$.

Let us first reduce the diagonal system $[\mathrm{Diag}(a, b, d)]$. This will change the elements a, b, c, d but, simplifying notations, let us denote by a, b, c, d the new ones. With Remark 3.2 and Theorem 2.1, we are looking for a reduction matrix of the form $T := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}$. We denote by $[D']$ a reduced system, $D' = \begin{pmatrix} a & 0 & 0 \\ 0 & b & c' \\ 0 & 0 & d \end{pmatrix}$ for a $c' \in \mathbf{k}$. The only non-trivial equality in $\phi(T)D = D'T$ is on the $(2, 3)$ entry:

$$c + d\phi(t) = bt + c'.$$

We have $c' \neq 0$, otherwise the gauge transformation $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ would transform $[\phi(T_2)A_2 T_2^{-1}]$ into a diagonal system, a contradiction. By [NAvdPT08], for all $c' \neq 0$, the algebraic group generated by $\begin{pmatrix} b & c \\ 0 & d \end{pmatrix}$ and $\begin{pmatrix} b & c' \\ 0 & d \end{pmatrix}$ are the same. Since the $(1, 1)$ entry of the algebraic group generated by $\begin{pmatrix} \star & 0 & 0 \\ 0 & \star & \star \\ 0 & 0 & \star \end{pmatrix}$ does not affect the $(2, 3)$ entry, we deduce that the algebraic group generated by $\begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & 0 & d \end{pmatrix}$ and $\begin{pmatrix} a & 0 & 0 \\ 0 & b & c' \\ 0 & 0 & d \end{pmatrix}$ are the same so we may take $t = 0$ and $c' = c$ and the system is already reduced.

• When G_2 is irreducible and imprimitive, up to a conjugation, it is of the form $G_2 = G_{2,\mathcal{D}} \cup G_{2,\mathcal{A}}$, where $G_{2,\mathcal{D}}$ is formed by diagonal matrices and $G_{2,\mathcal{A}}$ by

anti-diagonal matrices. We then have that $G_{\mathcal{D}}$ is a union of diagonal matrices and matrices of the form $\begin{pmatrix} \star & 0 & 0 \\ 0 & 0 & \star \\ 0 & \star & 0 \end{pmatrix}$. We can assume that the matrix D is of the form $\begin{pmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & c & 0 \end{pmatrix}$ since otherwise G_2 would be reducible.

REMARK 6.2. — *Note that $D_{[2]}$ is a diagonal matrix. By Lemma 2.3, the connected components of the identity of the difference Galois groups of $[D]$ and $[D_{[2]}]$ are the same. So if we are only interested in computing the connected component of G we may just reduce the diagonal system $[D_{[2]}]$, see Section 4.2 for more details.*

Assuming we know how to compute the Galois group of a diagonal system, we are able to compute a reduction matrix $P \in \mathrm{GL}_3(\mathbf{k})$ such that the system $\phi^2(Y) = \phi^2(P)D_{[2]}P^{-1}Y$ is reduced. Consider $B := \phi(P)DP^{-1}$, we have $B_{[2]} = \phi^2(P)D_{[2]}P^{-1}$ thus $[B_{[2]}]$ is reduced. Let us prove that the system $[B]$ is already reduced. Let H be the smallest algebraic group such that $B \in H(\mathbf{k})$. We have $G_{\mathcal{D}} \subset H$ (property of Galois groups, see Theorem 2.1). By Lemma 2.3, the Galois group of the ϕ^2-system $[B_{[2]}]$ and the Galois group of the ϕ-system $[B]$ have the same connected component. Since $[D_{[2]}]$ and $[B_{[2]}]$ have the same Galois group, and $[B_{[2]}]$ is reduced we find $H^0 = G_{\mathcal{D}}^0$. We recall that H is the smallest algebraic group such that $B \in H(\mathbf{k})$. Then, $H/H^0 = H/G_{\mathcal{D}}^0$ is generated by a single element, so it is cyclic (and finite since it is an algebraic group, see [HSS16, Lemma 3.5]). Since $G_{\mathcal{D}}/G_{\mathcal{D}}^0$ is finite cyclic,

$$G_{\mathcal{D}}/G_{\mathcal{D}}^0 \sim \mathbb{Z}/m'\mathbb{Z}, \quad H/G_{\mathcal{D}}^0 \sim \mathbb{Z}/n'\mathbb{Z},$$

for integers m', n'. With Theorem 2.1 and Lemma 2.3, there exists k such that $B_{[k]} \in G_{\mathcal{D}}^0(\mathbf{k})$.

Since, $G_{\mathcal{D}} \subset H$, we have $m' \leqslant n'$. By Theorem 2.1, there exists $P_1 \in H(\mathbf{k})$ such that $B_{red} = \phi(P_1)BP_1^{-1} \in G_{\mathcal{D}}(\mathbf{k})$ is reduced. Since H is an algebraic group defined over C, the equation over C between the entries of B and $\phi^k(B)$, $k \in \mathbb{Z}$, are the same. Then, the class of $\phi^k(B)$ in $H/G_{\mathcal{D}}^0$ is independent of k.

Then, the integer m' (resp. n') is the smallest such that we have the inclusion $B_{red,[m']} = \phi^{m'-1}(B_{red}) \times \cdots \times B_{red} \in G_{\mathcal{D}}^0(\mathbf{k})$ (resp. $B_{[n']} \in G_{\mathcal{D}}^0(\mathbf{k})$). Since $G_{\mathcal{D}}^0$ is composed of diagonal matrices and B, B_{red} are not diagonal (otherwise G_2 would be reducible), we find that $m' = 2m$, $n' = 2n$ for some integers m, n. We have $B_{red,[2m]} = \phi^{2m}(P_1)B_{[2m]}P_1^{-1} \in G_{\mathcal{D}}^0(\mathbf{k})$. Since $G_{\mathcal{D}}^0$ is the smallest algebraic group such that $B_{[2n]} \in G_{\mathcal{D}}^0(\mathbf{k})$ and since $[B_{[2]}]$ is reduced as a ϕ^2-system, we have $n \leqslant m$, proving that $m' = n'$. Then $G_{\mathcal{D}} = H$ and $[B]$ is already reduced.

• When G_2 is irreducible and primitive, by [Hen98, Section 4.4], either $G_2 = \mathrm{GL}_2(C)$, or there exists an integer k such that

$$G_2 = \{M \in \mathrm{GL}_2(\mathbb{C}) \mid \det(M)^k = 1\}.$$

We recall that $\det(G_2)$ is the difference Galois group of $\phi(Y) = dY$ with $d := \det\left(\phi(T_2)A_2T_2^{-1}\right)$. Let $R := \mathrm{Diag}(r_1, r_2)$ be a reduction matrix of the bloc diagonal system $\phi(Y) = BY$ where $B := \begin{pmatrix} \phi(T_1)\alpha T_1^{-1} & 0 \\ 0 & d \end{pmatrix}$. Then,

$$\phi(R)BR^{-1} = \mathrm{Diag}(\underbrace{\phi(r_1 T_1)\alpha(T_1 r_1)^{-1}}_{:=B_1}, \underbrace{\phi(r_2)dr_2^{-1}}_{:=B_2}).$$

Let us prove that $T := \mathrm{Diag}(r_1, r_2, 1)$ is a reduction matrix of $[D]$. Let H be the minimal algebraic group such that $B_{red} := \phi(T)DT^{-1} \in H(\mathbf{k})$. We set $B_{red} = \begin{pmatrix} B_{red,1} & 0 \\ 0 & B_{red,2} \end{pmatrix}$, with $B_{red,\star}$ of convenient size. By construction, we have $B_{red,1} = B_1$ and $\det(B_{red,2}) = B_2$. Note that $G_{\mathcal{D}}$ is a subgroup of $G_1 \times \det(G_2).\mathrm{SL}_2(C)$, where the identification $G_2 \sim \det(G_2).\mathrm{SL}_2(C)$ is made via the map $\mathcal{M} = \mathrm{Diag}(\det(\mathcal{M}), 1)\mathcal{M}'$, with $\det(\mathrm{Diag}(\det(\mathcal{M}), 1)) = \det(\mathcal{M})$, and $\mathcal{M}' \in \mathrm{SL}_2(C)$. Furthermore, since G_2 is irreducible and primitive, $G_{\mathcal{D}}$ contains $\{1\} \times \mathrm{SL}_2(C)$. Consider the map

$$\xi : G_1(\mathbf{k}) \times \det(G_2).\mathrm{SL}_2(\mathbf{k}) \to (\mathbf{k}^*)^2$$
$$(A, B) \qquad\qquad \mapsto (A, \det(B)).$$

Let $\{1\} \times \mathrm{SL}_2 \subset H_1 \subsetneq H_2 \subset G_1 \times G_2$ be two algebraic groups. Since the kernel of ξ is $\{1\} \times \mathrm{SL}_2(\mathbf{k})$, we have $\xi(H_1(\mathbf{k})) \subsetneq \xi(H_2(\mathbf{k}))$. Furthermore, ξ is injective on the set of algebraic subgroups of $(G_1 \times G_2)(\mathbf{k})$ containing $\{1\} \times \mathrm{SL}_2(\mathbf{k})$.

By Theorem 2.1, we find that $G_{\mathcal{D}} \subset H$ so that we have $\xi(G_{\mathcal{D}}(\mathbf{k})) \subset \xi(H(\mathbf{k}))$. Since $R := \mathrm{Diag}(r_1, r_2)$ is a reduction matrix of the bloc diagonal system $\phi(Y) = BY$, we have $\xi(H(\mathbf{k})) \subset \xi(G_{\mathcal{D}}(\mathbf{k}))$, and then $\xi(G_{\mathcal{D}}(\mathbf{k})) = \xi(H(\mathbf{k}))$. From the above injectivity property, $G_{\mathcal{D}}(\mathbf{k}) = H(\mathbf{k})$. Then $T := \mathrm{Diag}(r_1, r_2, 1)$ is a reduction matrix of $[D]$. □

Thus, in all cases, we should be able to reduce the block diagonal system $[D]$ and find an associated reduction matrix, denoted by T'.

The next step consists in reducing the system $[A]$. We will see that finding the reduction matrix is equivalent to finding vector solutions in $\mathbf{k}$ of ϕ-linear systems with coefficients in $\mathbf{k}$ that we will explicit. We summarize these results in Theorem 6.5. We consider

$$B := \phi(T')AT'^{-1}.$$

The matrix B is of the form $\begin{pmatrix} D_1 & \widetilde{A} \\ 0 & D_2 \end{pmatrix}$. By construction, the difference Galois group of $[B]$ is G, so let us compute the latter. We write $B_\mathcal{D} := \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix}$. Recall that $G_\mathcal{D}$ is the Galois group of $[B_\mathcal{D}]$, which is a reduced system thanks to the first step. The Galois group G is conjugated to a subgroup of

$$\left\{ \begin{pmatrix} \mathscr{C}_1 & c_1 & c_2 \\ 0 & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_\mathcal{D}, c_1, c_2 \in C \right\} = G_\mathcal{D} \ltimes U,$$

where $U = \left\{ \begin{pmatrix} 1 & c_1 & c_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| c_1, c_2 \in C \right\}$ is isomorphic to two copies of the additive group.

By Lemma 3.1, there exists $T := \begin{pmatrix} 1 & X \\ 0 & \mathrm{Id}_2 \end{pmatrix} \in \mathrm{GL}_3(\mathbf{k})$ such that $[\phi(T)BT^{-1}]$ is reduced. Let $F := \phi(T)BT^{-1}$. We have $F = \begin{pmatrix} D_1 & A' \\ 0 & D_2 \end{pmatrix}$ where $A' = -XD_1 + \widetilde{A} + \phi(X)D_2$, that is,

$$\widetilde{A} + \phi(X)D_2 = XD_1 + A'.$$

Let $G_\mathcal{U} = G \cap U$. It is an algebraic subgroup of U so it is of dimension 0, 1 or 2.

LEMMA 6.3. — *The dimension of the algebraic group $G_\mathcal{U}$ is 0 if and only if there exists $X \in \mathbf{k}^2$ such that*

$$(15) \qquad\qquad \widetilde{A} + \phi(X)D_2 = XD_1.$$

In this case $[F] = [B_\mathcal{D}]$ is a reduced system equivalent to $[B]$ with the gauge transformation $T := \begin{pmatrix} 1 & X \\ 0 & \mathrm{Id}_2 \end{pmatrix}$ and the Galois group G is $G_\mathcal{D}$.

Proof. — From Theorem 2.1, the dimension of $G_\mathcal{U}$ is 0 if and only if $A' = (0 \quad 0)$. $\qquad\square$

LEMMA 6.4. — *Assume that the dimension of $G_\mathcal{U}$ is not 0. If the dimension of $G_\mathcal{U}$ is 1 then D_2 is a triangular matrix (lower or upper triangular, including the diagonal matrices). If it is the case, we can assume that D_2 is a lower triangular matrix and three cases occur:*
  - *Case where D_2 is lower triangular but not diagonal. In this case*

$$G = \left\{ \begin{pmatrix} \mathscr{C}_1 & c & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_\mathcal{D}, c \in C \right\}.$$

- *Case where D_2 is diagonal but not a scalar matrix. In this case, G is the same group as before or $\left\{ \begin{pmatrix} \mathscr{C}_1 & 0\,c \\ 0 & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_{\mathcal{D}}, c \in C \right\}$, depending if there is a solution in $\mathbf{k}$ of some linear equations with coefficients in $\mathbf{k}$ (see equations (17) or (18)).*
- *Case where D_2 is a scalar matrix. In this case,*

$$G = \left\{ \begin{pmatrix} \mathscr{C}_1 & \lambda c\ \mu c \\ 0 & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_{\mathcal{D}}, c \in C \right\}.$$

where $(\lambda, \mu) \in C^2 \setminus \{(0,0)\}$ can be explicitised, see (19).

In each case, the proof gives an explicit gauge transformation and a reduced system.

Proof. — Let $\mathscr{Y}$ be such that $h = \begin{pmatrix} 1 & \mathscr{Y} \\ 0 & \mathrm{Id}_2 \end{pmatrix} \in G_{\mathcal{U}}$. For $g = \begin{pmatrix} a_g & \mathscr{C}_g \\ 0 & \mathscr{B}_g \end{pmatrix} \in G$, let us compute $ghg^{-1} \in G_{\mathcal{U}}$. We write $ghg^{-1} = \begin{pmatrix} 1 & \mathscr{Z} \\ 0 & \mathrm{Id}_2 \end{pmatrix}$, so that we have $\begin{pmatrix} a_g & \mathscr{C}_g \\ 0 & \mathscr{B}_g \end{pmatrix} \begin{pmatrix} 1 & \mathscr{Y} \\ 0 & \mathrm{Id}_2 \end{pmatrix} = \begin{pmatrix} 1 & \mathscr{Z} \\ 0 & \mathrm{Id}_2 \end{pmatrix} \begin{pmatrix} a_g & \mathscr{C}_g \\ 0 & \mathscr{B}_g \end{pmatrix}$. Then, $a_g \mathscr{Y} + \mathscr{C}_g = \mathscr{C}_g + \mathscr{Z} \mathscr{B}_g$ proving that $ghg^{-1} = \begin{pmatrix} 1 & a_g \mathscr{Y} \mathscr{B}_g^{-1} \\ 0 & \mathrm{Id}_2 \end{pmatrix} \in G_{\mathcal{U}}$. If the dimension of $G_{\mathcal{U}}$ is 1 then $a_g \mathscr{Y} \mathscr{B}_g^{-1} = c\mathscr{Y}$ for some $c \in C^*$. Taking the transposition, we find $(\mathscr{B}_g^{-1})^t \mathscr{Y}^t = c' \mathscr{Y}^t$ for some $c' \in C^*$. So $\mathscr{Y}^t$ is an eigenvector of any elements $(\mathscr{B}_g^{-1})^t$. This means that the elements $\mathscr{B}_g$ are all conjugated to lower triangular matrices (or upper triangular matrices) and $\mathscr{Y}^t$ is necessarily a common eigenvector. Since $[F]$ is a reduced system, D_2 is also a triangular matrix. Thus, if $G_{\mathcal{U}}$ has dimension 1 then D_2 is a triangular matrix.

Let us assume that $G_{\mathcal{U}}$ has dimension 1 thus D_2 is a triangular matrix and, up to conjugation, we can assume that D_2 is lower triangular. In what follows, we denote by $\widetilde{A}_1$ and $\widetilde{A}_2$ the entries of $\widetilde{A}$. We distinguish three cases:

- Case where D_2 is lower triangular but not diagonal. We set $D_2 = \begin{pmatrix} d_1 & 0 \\ d_3 & d_4 \end{pmatrix}$. In this case, the common eigenvectors of the elements $(\mathscr{B}_g^{-1})^t$ for $g \in G$ are $\mathscr{Y}^t$ with $\mathscr{Y} := (f\ 0)$ where $f \in C$, thus the system $[B]$ is equivalent to the system $[F]$ where F is of the form $\begin{pmatrix} D_1 & f & 0 \\ 0 & D_2 \end{pmatrix}$, for a certain $f \in \mathbf{k}^*$, thanks to a gauge transformation $T := \begin{pmatrix} 1 & x_1 & x_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Recall that $\widetilde{A} + \phi(X)D_2 = XD_1 + A'$. Since

the second entry of A' has to be 0, we obtain

$$(16) \qquad \widetilde{A}_2 + \phi(x_2)d_4 = D_1 x_2.$$

From Theorem 2.1, this implies that

$$G \subset \left\{ \begin{pmatrix} \mathscr{C}_1 & c & 0 \\ 0 & & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_{\mathcal{D}}, c \in C \right\}.$$

Since $G = G_{\mathcal{D}} \ltimes G_{\mathcal{U}}$, we obtain that the previous inclusion is an equality.

• Case where D_2 is diagonal but not a scalar matrix. We set $D_2 = \mathrm{Diag}(d_1, d_4)$. Up to a conjugation, we have $G_{\mathcal{U}} = \left\{ \begin{pmatrix} 1 & c & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, c \in C \right\}$ or

$G_{\mathcal{U}} = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, c \in C \right\}$. Using the same notations as before, we obtain that $G_{\mathcal{U}}$ is the first one, resp. the second one, if there exists a solution $y \in \mathbf{k}$ of the equation

$$(17) \qquad \widetilde{A}_2 + \phi(y)d_4 = D_1 y,$$

resp. of the equation

$$(18) \qquad \widetilde{A}_1 + \phi(y)d_1 = D_1 y.$$

Not that only one of these two equations has a solution in $\mathbf{k}$ because if it is not the case, the solutions x_1, x_2 are such that $X := (x_1 \quad x_2) \in \mathbf{k}^2$ is a solution of (15), a contradiction since the dimension of $G_{\mathcal{U}}$ is not 0. With the same reasoning as before, we obtain that the Galois group G is

$$\left\{ \begin{pmatrix} \mathscr{C}_1 & c & 0 \\ 0 & & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_{\mathcal{D}}, c \in C \right\} \text{ or } \left\{ \begin{pmatrix} \mathscr{C}_1 & 0 & c \\ 0 & & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_{\mathcal{D}}, c \in C \right\},$$

if $G_{\mathcal{U}}$ is respectively the first or the second algebraic group.

• Case where D_2 is a scalar matrix. We set $D_2 = d\mathrm{Id}_2$ with $d \in \mathbf{k}^*$. Let $\lambda, \mu \in C$ not all zero such that $G_{\mathcal{U}} = \left\{ \begin{pmatrix} 1 & \lambda c & \mu c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, c \in C \right\}$. From Lemma 3.1, since $G = G_{\mathcal{D}} \ltimes G_{\mathcal{U}}$, there exists $T := \begin{pmatrix} 1 & X \\ 0 & \mathrm{Id}_2 \end{pmatrix}$ such that $\phi(T)B = FT$, where $[F]$ is reduced with $F = \begin{pmatrix} D_1 & \lambda f & \mu f \\ 0 & & D_2 \end{pmatrix}$, $f \in \mathbf{k}^*$. This is equivalent to

$$\widetilde{A} + \phi(X)D_2 = D_1 X + \left(\lambda f \quad \mu f \right),$$

that is,

$$\begin{cases} d\phi(x_1) = D_1 x_1 - \widetilde{A}_1 + \lambda f \\ d\phi(x_2) = D_1 x_2 - \widetilde{A}_2 + \mu f \end{cases}$$

where x_1, x_2 are the coordinates of X. Taking μ times the first line minus λ times the second, we find that $x = \mu x_1 - \lambda x_2$ is solution of $d\phi(x) = D_1 x - \mu \widetilde{A}_1 + \lambda \widetilde{A}_2$. We then find that this is equivalent to the fact that the vector $Y := \begin{pmatrix} \lambda \\ \mu \\ x \end{pmatrix}$ is solution of

$$(19) \qquad \phi(Y) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \widetilde{A}_2 d^{-1} & -\widetilde{A}_1 d^{-1} & D_1 d^{-1} \end{pmatrix} Y.$$

Conversely, any nonzero solution of the latter system in $\mathbf{k}^3$ will give a reduction matrix, and a reduced form. $\qquad\square$

Let us summarize the results proved in Lemma 6.3 and Lemma 6.4.

THEOREM 6.5. — *If the equation* (15) *has a solution then the Galois group G is $G_{\mathcal{D}}$. If this equation has no solution then we have the following cases :*

- *if D_2 is a triangular matrix but not diagonal, up to a conjugation we assume that it is lower triangular, and if the equation* (16) *has a solution then*

$$G = \left\{ \begin{pmatrix} \mathscr{C}_1 & c & 0 \\ 0 & & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_{\mathcal{D}}, c \in C \right\}.$$

- *if D_2 is a diagonal matrix but not a scalar matrix and if* (17) *(the same equation as* (16)*) or* (18) *has a solution then G is the previous group or respectively*

$$\left\{ \begin{pmatrix} \mathscr{C}_1 & 0 & c \\ 0 & & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_{\mathcal{D}}, c \in C \right\}.$$

- *if D_2 is a scalar matrix and* (19) *has a solution then*

$$G = \left\{ \begin{pmatrix} \mathscr{C}_1 & \lambda c & \mu c \\ 0 & & \mathscr{C}_2 \end{pmatrix} \middle| \begin{pmatrix} \mathscr{C}_1 & 0 \\ 0 & \mathscr{C}_2 \end{pmatrix} \in G_{\mathcal{D}}, c \in C \right\}$$

where $\lambda, \mu \in C$ not all zero are given by a solution of (19).
- *if none of these three cases occur then $G = G_{\mathcal{D}} \ltimes U$ (in this case, the dimension of $G_{\mathcal{U}}$ is 2).*

6.2. Imprimitive case. — Assume now that G is irreducible and treat the case where G is imprimitive. This case is solved in Section 3.2. It is imprimitive if and only if the difference Galois group of $\phi^3 Y = A_{[3]} Y$ is diagonal. We use the reducible case (with ϕ replaced by ϕ^3) to check this property. In that case we are able to compute $d \in \mathbf{k}^*$, solution of the Riccati equation corresponding to $\phi^3 Y = A_{[3]} Y$. We now follow Proposition 3.10. Let us compute a reduced form of $\phi(y) = dy$, that is compute $f \in \mathbf{k}^*$ such that $\phi(y) = d\frac{\phi(f)}{f} y$ is reduced. Then, a reduced form is given by $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & f^{-1} \\ \phi(f)d & 0 & 0 \end{pmatrix}$ with reduction matrix $\mathrm{Diag}(1, 1, f)$.

We have listed the potential algebraic groups that may appear as Galois groups in Theorem 3.5 and we have shown in Proposition 3.7 that the later groups are characterized by their group of determinants. The computation of the determinant is then explained in Remark 4.3. Note that we do not claim to be able to compute the generating matrix $\mathcal{M}$ of Theorem 3.5.

6.3. Primitive case. — Assume now that G is irreducible and primitive. Let $D(G^0)$ be the derived subgroup of G^0 that is irreducible and primitive by Proposition 3.18. By definition, $D(G^0) \subset \mathrm{SL}_3(C)$. By [SU93, Section 2.2], either $D(G^0)$ is $\mathrm{SL}_3(C)$, or it is isomorphic to $\mathrm{PSL}_2(C)$. Since $\mathrm{SO}_3(C)$ is also a primitive subgroup of $\mathrm{SL}_3(C)$, it is isomorphic to $\mathrm{PSL}_2(C)$. The matrices commuting with $\mathrm{SL}_3(C)$ (resp. $\mathrm{SO}_3(C)$) are scalar matrices and we find that $Z(G^0)$, the center of G^0, is isomorphic to an algebraic subgroup of C^*. Since it is connected, it is then C^* or $\{1\}$. By Proposition 3.18, $G^0 = Z(G^0).D(G^0)$.

When $D(G^0) = \mathrm{SL}_3(C)$ we find that either $G^0 = \mathrm{GL}_3(C)$, or $G^0 = \mathrm{SL}_3(C)$. Since G/G^0 is cyclic, we deduce that either $G = \mathrm{GL}_3(C)$, or there exists an integer k, which is the order of the group G/G^0, such that $G = \{M \in \mathrm{GL}_3(C) \mid \det(M)^k = 1\}$. Then $G = Z(G).D(G)$, where $Z(G)$ is composed by scalar matrices and $D(G) = \mathrm{SL}_3(C)$.

Assume now that $D(G^0) = \mathrm{SO}_3(C)$. Then either $G^0 \sim C^*.\mathrm{SO}_3(C)$, or $G^0 = \mathrm{SO}_3(C)$. Moreover, since G/G^0 is cyclic, it is abelian and since the derived group $D(G)$ is the smallest subgroup H of G such that G/H is abelian, we have $D(G) \subset G^0$. Then $\mathrm{SO}_3(C) = D(G^0) \subset D(G) \subset G^0 \subset C^*.\mathrm{SO}_3(C)$. The normalizer of $\mathrm{SO}_3(C)$ in $\mathrm{GL}_3(C)$ is $C^*.\mathrm{SO}_3(C)$ and the same holds for $C^*.\mathrm{SO}_3(C)$. Since the normalizer of $D(G)$ in G, which is G, is included in the normalizer of $D(G)$ in $\mathrm{GL}_3(C)$, we find that $G \subset C^*.\mathrm{SO}_3(C)$. Thus, $\mathrm{SO}_3(C) \subset G \subset C^*.\mathrm{SO}_3(C)$. Then, either $G \sim C^*.\mathrm{SO}_3(C)$, or there exists $k \in \mathbb{N}^*$, such that $G \sim U_k.\mathrm{SO}_3(C)$, where U_k denote the group of all kth roots of unity. Hence $G = Z(G).D(G)$, where $Z(G)$ is composed by scalar matrices and $D(G) = \mathrm{SO}_3(C)$. To summary, we have proved the following result:

PROPOSITION 6.6. — *Assume that G is irreducible and primitive. Then, $G = Z(G).D(G)$, where $Z(G)$ is included in the group of scalar matrices and $D(G)$ is either $\mathrm{SL}_3(C)$ or $\mathrm{SO}_3(C)$.*

REMARK 6.7. — *If $D(G) = \mathrm{SL}_3(C)$, then $Z(G) = \{\lambda \mathrm{Id}_3 \text{ where } \lambda^3 \in \det(G)\}$. Recall that $\det(G)$ is the Galois group of an equation of order one $\phi(y) = \det(A)y$.*

Assume now $D(G) = \mathrm{SO}_3(C)$. If $\det(G) = C^*$, then $Z(G) = C^*$. If $\det(G) = U_n$, the group of nth roots of unity, with $\gcd(n,3) \neq 1$, then $Z(G) = U_{3n}$. In the case $\det(G) = U_n$ with $\gcd(n,3) = 1$, we have $Z(G) = U_{3n}$ or U_n.

We want to give a criterion to decide whether $D(G) = \mathrm{SO}_3(C)$ or not. Let us prove the following lemma.

LEMMA 6.8. — *Assume that G is irreducible and primitive. Let $\overline{\mathbf{k}}$ be the algebraic closure of $\mathbf{k}$. We may extend ϕ on the latter. The following facts are equivalent.*

*   *$D(G) = \mathrm{SO}_3(C)$.*
*   *there exist $T \in \mathrm{GL}_3(\mathbf{k})$, $\lambda \in \mathbf{k}^*$ and $B \in \mathrm{SO}_3(\mathbf{k})$ such that*

$$\phi(T)AT^{-1} = \lambda B. \tag{20}$$

*   *there exist $T \in \mathrm{GL}_3(\overline{\mathbf{k}})$, $\lambda \in \overline{\mathbf{k}}^*$ and $B \in \mathrm{SO}_3(\overline{\mathbf{k}})$ such that (20) holds.*

Proof. — Recall that $G \sim Z(G).D(G)$, where $D(G) \in \{\mathrm{SO}_3(C), \mathrm{SL}_3(C)\}$ and $Z(G)$ is composed by scalar matrices. By Theorem 2.1, $D(G) = \mathrm{SO}_3(C)$ if and only if there exist $T \in \mathrm{GL}_3(\mathbf{k})$, $\lambda \in \mathbf{k}^*$ and $B \in \mathrm{SO}_3(\mathbf{k})$ such that (20) holds. So the first two items are equivalent. If the second item holds, then the third item holds. Conversely assume that the third item holds. Consider $\overline{G}$, the Galois group over $\overline{\mathbf{k}}$. By Theorem 2.1, $\overline{G} \subset C^*.\mathrm{SO}_3(C)$. By Galois correspondence, see [vdPS97, Chapter 1], $\overline{G}$ is a subgroup of G and $G/\overline{G}$ is finite. Since $G \sim Z(G).D(G)$, where $D(G) \in \{\mathrm{SO}_3(C), \mathrm{SL}_3(C)\}$, this shows that $D(G)$ cannot be $\mathrm{SL}_3(C)$. Then $D(G) = \mathrm{SO}_3(C)$. $\qquad\square$

The equation (20) is non linear and may be complicated to solve. Let us see how we may reduce to a linear equation over $\overline{\mathbf{k}}$. Let us first recall this well-known result, which can be deduced for instance from [Lan05, Chapter XV, section 3].

LEMMA 6.9. — *Let K be a field of characteristic zero. Let $X \in \mathrm{GL}_n(K)$ be a symmetric matrix. Then, there exist $F, D \in \mathrm{GL}_n(K)$ with D diagonal such that $X = FDF^t$.*

Toward an efficient way to check that (20) holds, let us prove the following.

LEMMA 6.10. — *The following facts are equivalent.*

*   *There exist $T \in \mathrm{GL}_3(\overline{\mathbf{k}})$, $\lambda \in \overline{\mathbf{k}}^*$ and $B \in \mathrm{SO}_3(\overline{\mathbf{k}})$ such that (20) holds.*

– *There exist* $\lambda \in \overline{\mathbf{k}}^*$, $X \in \mathrm{GL}_3(\overline{\mathbf{k}})$ *such that* $X = X^t$, *and* $AXA^t = \lambda^2 \phi(X)$.

Proof. — Let us prove that the first point implies the second. Let us assume the existence of $T \in \mathrm{GL}_3(\overline{\mathbf{k}})$, $\lambda \in \overline{\mathbf{k}}^*$, and $B \in \mathrm{SO}_3(\overline{\mathbf{k}})$ such that (20) holds. Let us set $P := T^{-1}$ and note that P^t is the inverse of T^t. Using $BB^t = \mathrm{Id}_3$ we find that (20) implies

$$\phi(T)APP^tA^t\phi(T^t) = \lambda^2\mathrm{Id}_3.$$

The latter is equivalent to

$$APP^tA^t = \lambda^2\phi(PP^t).$$

We obtain the result if we set $X = PP^t$.

Conversely, assume that the second item holds. By Lemma 6.9, let us write $X = FDF^t$ with matrices whose coefficients are in $\overline{\mathbf{k}}$. Since $\overline{\mathbf{k}}$ is algebraically closed, $F\sqrt{D}$ has coefficients in $\overline{\mathbf{k}}$ and we may write $X = F\sqrt{D}(\sqrt{D})^tF^t$, where $\sqrt{D}$ is any diagonal matrix whose square is D. Let us perform $\phi(T)AT^{-1}$ where $T \in \mathrm{GL}_3(\overline{\mathbf{k}})$ is the inverse of $F\sqrt{D}$. Note that $X = T^{-1}(T^{-1})^t$. It suffices to prove that $B = \phi(T)AT^{-1}\lambda^{-1} \in \mathrm{SO}_3(\overline{\mathbf{k}})$. Then,

$$BB^t = \lambda^{-2}\phi(T)AT^{-1}(T^{-1})^tA^t\phi(T^t) = \lambda^{-2}\phi(T)AXA^t\phi(T^t).$$

We now use $AXA^t = \lambda^2\phi(X)$ to deduce that the latter equals $\phi(T)\phi(X)\phi(T^t)$. With $X = T^{-1}(T^{-1})^t$, we deduce that $\phi(T)\phi(X)\phi(T^t)$ is the identity, that is $B \in \mathrm{SO}_3(\overline{\mathbf{k}})$. $\qquad\square$

If we replace X by $X' := X\det(X)^{-1/3} \in \mathrm{SL}_3(\overline{\mathbf{k}})$, we find $AX'A^t = \det(A)^{2/3}\phi(X')$. Indeed, the equality $AXA^t = \lambda^2\phi(X)$ is equivalent to

(21) $$AX'A^t = \lambda^2\det(X)^{-1/3}\det(\phi(X))^{1/3}\phi(X').$$

Taking the determinant in (21) and using that $\det(X') = 1$, we have $\det(A)^2 = \lambda^6\det(X)^{-1}\det(\phi(X))$. We obtain the desired result thanks to (21) and this last equality. With Lemma 6.8, and Lemma 6.9, we have proved the following result.

PROPOSITION 6.11. — *Assume that G is irreducible and primitive. Then, $D(G) = \mathrm{SO}_3(C)$ if and only if there exists $X \in \mathrm{SL}_3(\overline{\mathbf{k}})$ such that $X = X^t$ and $AXA^t = \det(A)^{2/3}\phi(X)$.*

Proposition 6.11 then reduces the criterion on $D(G)$ to look at solutions in $\overline{\mathbf{k}}$ of linear ϕ-difference systems with coefficients in $\overline{\mathbf{k}}$. More precisely the condition $X = X^t$ drops the number of unknowns from 9 to 6. Solving a linear system in $\overline{\mathbf{k}}$ is in general a complicated task. Let us see how to bypass this problem. Let us see the 6 unknowns of X in a vector column $\widetilde{X}$. Then, we have to solve a system of the form $\phi(\widetilde{X}) = \widetilde{A}\widetilde{X}$, with $\widetilde{A} \in \mathrm{GL}_6(\overline{\mathbf{k}})$. The non-rational part in $\widetilde{A}$ comes from the term $\det(A)^{2/3}$. Then, $\phi(\widetilde{X}^{\otimes_3}) = \widetilde{A}^{\otimes_3}\widetilde{X}^{\otimes_3}$,

where $\widetilde{A}^{\otimes_3}$ has coefficients in $\mathbf{k}$ and $\otimes_3$ denotes the symmetric product of order 3. The column vector $\widetilde{X}^{\otimes_3}$ has coefficients in $\overline{\mathbf{k}}$. Since, by assumption, there is no finite difference field extension of $\mathbf{k}$, $\widetilde{X}^{\otimes_3}$ has coefficients in $\mathbf{k}$. We assumed that we know how to solve in $\mathbf{k}$ the linear difference equations with coefficients in $\mathbf{k}$ (see Section 2.3). So if $D(G) = \mathrm{SO}_3(C)$, then we find $\widetilde{X}^{\otimes_3}$ with coefficients in $\mathbf{k}$ such that $\phi(\widetilde{X}^{\otimes_3}) = \widetilde{A}^{\otimes_3}\widetilde{X}^{\otimes_3}$. Conversely, if we find such $\widetilde{X}^{\otimes_3}$, we compute a third root and find the corresponding symmetric matrix X solution of $AXA^t = \det(A)^{2/3}\phi(X)$. If it is invertible, then $D(G) = \mathrm{SO}_3(C)$. So we might be able to distinguish between the cases $D(G) = \mathrm{SO}_3(C)$ and $D(G) = \mathrm{SL}_3(C)$.

Let us now see how to compute the reduced form. First, assume that $D(G) = \mathrm{SL}_3(C)$. We compute $\det(G)$ as the difference Galois group of an order one system $\phi(y) = a_0 y$ with reduction matrix $f \in \mathbf{k}^*$, that is $\phi(y) = a_0 \frac{\phi(f)}{f} y$ is reduced with Galois group $\det(G)$. Then, we perform, as in [Hen98, Section 4.4], the gauge transformation $T = \mathrm{Diag}(f, 1, 1)$ to obtain a system $[B]$. Since $\det(B) = a_0 \frac{\phi(f)}{f}$, and $\phi(y) = a_0 \frac{\phi(f)}{f} y$ is reduced with Galois group $\det(G)$, we find that $B \in G(\mathbf{k})$. Then, B is a reduced form and T is the reduction matrix.

Now consider the case where $D(G) = \mathrm{SO}_3(C)$. By Lemma 6.8, we know that there exist $T \in \mathrm{GL}_3(\mathbf{k})$, $\lambda \in \mathbf{k}^*$ and $B \in \mathrm{SO}_3(\mathbf{k})$ such that (20) holds. As above, let us set $X' = T^{-1}(T^{-1})^t \det(T)^{2/3} \in \mathrm{SL}_3(\overline{\mathbf{k}})$. Then, X' satisfies $X' = (X')^t$ and $AX'A^t = \det(A)^{2/3}\phi(X')$. Let us write $X' = FDF^t$ as in Lemma 6.9. Note that F and D may be effectively computed. Let us perform the gauge transformation $\phi(\alpha(F\sqrt{D})^{-1})A(\alpha(F\sqrt{D})^{-1})^{-1}$ where $(F\sqrt{D})^{-1} \in \mathrm{GL}_3(\overline{\mathbf{k}})$ and $\alpha \in \overline{\mathbf{k}}^*$. From what precedes, all reduction matrices with coefficients in $\overline{\mathbf{k}}$ are of this form. Since there is a reduction matrix with coefficients in $\mathbf{k}$, there is a choice of X' and α such that the corresponding $\alpha(F\sqrt{D})^{-1}$ has entries in $\mathbf{k}$. The following process is a priori purely theoretical and there is not an effective method to perform this procedure. So if $\alpha(F\sqrt{D})^{-1}$ does not have entries in $\mathbf{k}$ for all $\alpha \in \overline{\mathbf{k}}^*$, we take another solutions X' with a corresponding $\alpha(F\sqrt{D})^{-1} \in \mathrm{GL}_3(\mathbf{k})$. At this stage, we have $\phi(\alpha(F\sqrt{D})^{-1})A(\alpha(F\sqrt{D})^{-1})^{-1} = \beta A_0$, with $\beta \in \mathbf{k}^*$ and $A_0 \in \mathrm{SO}_3(\mathbf{k})$. By Theorem 2.1 and Proposition 6.6, we find that a reduction matrix is of the form $\alpha_1 \alpha(F\sqrt{D})^{-1}$, $\alpha_1 \in \mathbf{k}^*$. We may compute α_1 by reducing the system $\phi(y) = \beta y$. Hence the reduced form is $\frac{\phi(\alpha_1)}{\alpha_1}\beta A_0$.

EXAMPLE 6.12. — *Consider G the difference Galois group of (1) over $\mathbb{C}(z^{1/*})$. Assume that $t \neq 0$. Assume by contradiction that $D(G) = \mathrm{SO}_3(\mathbb{C})$. The eigenvalues of matrices of $\mathrm{SO}_3(\mathbb{C})$ are of the form $(1, a^{\pm 1})$, $a \in \mathbb{C}^*$. Then, the eigenvalues of elements of G are for the form $(c, ca^{\pm 1})$, $c, a \in \mathbb{C}^*$. By [RS09, Section 2.4], combined with the computation of the Newton polygon in Example 3.15, G contains the so-called theta torus, elements of the form $\mathrm{Diag}(1, 1, d)$,*

$d \in \mathbb{C}^*$. *If the triple* $\mathrm{Diag}(1,1,d)$ *is of the form* $(c, ca^{\pm 1})$, *then either* $a = 1 = c = d$, *or* $a = c = -1$ *and* $d = -1$. *Then,* $\mathrm{Diag}(1,1,2)$ *can never be of the form* $(c, ca^{\pm 1})$, *showing that* $D(G) \neq \mathrm{SO}_3(\mathbb{C})$. *Then* $D(G) = \mathrm{SL}_3(\mathbb{C})$.

6.4. Summary. — Let

$$L := \phi^3 + a_2 \phi^2 + a_1 \phi + a_0 \in \mathbf{k} \left\langle \phi, \phi^{-1} \right\rangle$$

and let $G \subset \mathrm{GL}_3(C)$ be the Galois group of $Ly = 0$.

If the Riccati equation attached to L or the similar equation attached to $L^\vee$ has a solution then G is reducible. Otherwise, it is irreducible.

When it is the reducible case, L or $L^\vee$ has a right factor of order 1 denoted by $\phi - \alpha$. Consider the case where L has a right factor of order 1, the other situation is similar. Therefore, up to an isomorphism, the Galois group G is the one of the system

$$\phi(Y) = \left(\begin{array}{c|cc} \alpha & 1 & 0 \\ \hline 0 & & A_2 \end{array} \right) Y.$$

We already know how to reduce the systems $[\alpha]$ and $[A_2]$ (order 1 and 2) and we denote respectively by $[\beta]$ and $[B_2]$ these reduced systems. We consider the system $[A]$ which is equivalent to this previous system with A of the form $\begin{pmatrix} \beta & \star \\ 0 & B_2 \end{pmatrix}$. To reduce the system $[A]$ and compute its Galois group, which is G up to an isomorphism, we proceed in two steps:

1. With Theorem 6.1, we reduce the bloc diagonal system $[D]$ where $D = \begin{pmatrix} \beta & 0 \\ 0 & B_2 \end{pmatrix}$ and we find an associated reduction matrix denoted by T'.
2. We reduce the system $[B]$ where $B := \phi(T')AT'^{-1}$. Doing this, we introduce some linear equations and we know which is the group G if we know that there exists a solution or not of these equations (see equations (15), (17), (18), (19))

When it is not the reducible case, we have to distinguish between the imprimitive case and the primitive case. Let $A := A_L$. We know that it is imprimitive if and only if the difference Galois group of $\phi^3 Y = A_{[3]} Y$ is diagonal. We use the reducible case (with ϕ replaced by ϕ^3) to check this property.

Finally, when it is irreducible and primitive, we have to distinguish between $D(G) = \mathrm{SO}_3(C)$ and $D(G) = \mathrm{SL}_3(C)$. We have $D(G) = \mathrm{SO}_3(C)$, if and only if there is a symmetric solution over $\overline{\mathbf{k}}^*$ of the linear difference equation $AXA^t = \det(A)^{2/3}\phi(X)$. We proved how this reduces to compute a nonzero vector solution in $\mathbf{k}$ of a certain linear difference equation with coefficients in $\mathbf{k}$. Unfortunately, when $D(G) = \mathrm{SO}_3(C)$ we do not present an effective way to compute the reduction matrix.

Combining the facts proved in Examples 2.7, 3.15, 4.4, and 6.12, we then find the Galois group of (1) over $\mathbb{C}(z^{1/*})$:

THEOREM 6.13. — *For all $t \neq 0$, the difference Galois group of* (1) *over* $\mathbb{C}(z^{1/*})$ *is* $\mathrm{GL}_3(\mathbb{C})$.

7. Application to the differential transcendence

Let $\mathbf{k}$ be a field of characteristic zero and $(\mathbf{k}, \phi, \partial)$ be a $\mathcal{C}^1$-field with no proper finite difference field extension, equipped with an automorphism ϕ, and a derivation ∂, that is an additive morphism satisfying the Leibniz rule $\partial(fg) = \partial(f)g + f\partial(g)$. Let us assume that ϕ and ∂ commute. In our examples, we may take $\partial = \partial_z$ (case S and E), and $\partial = z\partial_z$ (case Q). In the Mahler case, we could adapt as in [DHR18] the framework with the derivation $\partial = z\partial_z \log(z)$ but this will complicate the exposition of a general criterion, so let us drop the Mahler case in what follows.

Let us consider R, a ring extension of $\mathbf{k}$ such that ϕ and ∂ extend on R. We say that $f \in R$ is ∂-algebraic over $\mathbf{k}$ if there exists $n \in \mathbb{N}$ and a nonzero $P \in \mathbf{k}[X_0, \ldots, X_n]$ such that $P(f, \ldots, \partial^n f) = 0$. We say that f is ∂-transcendent over $\mathbf{k}$ otherwise. In our examples, f is ∂-algebraic over $\mathbf{k}$ if and only if it is ∂_z-algebraic over $\mathbf{k}$. Many proof of ∂-transcendence of solutions of ϕ-equation are based on the difference Galois theory. Roughly speaking, this kind of theorem says that if the difference Galois group is sufficiently big, then the nonzero solutions of the linear equation are ∂-transcendent. Let $f \in R^*$ be a solution of

$$a_3\phi^3(y) + a_2\phi^2(y) + a_1\phi(y) + a_0 y = 0, \quad \text{where} \quad a_i \in \mathbf{k} \quad \text{and} \quad a_0 a_3 \neq 0.$$

Consider the dual $\sum_{i=0}^3 \phi^{-i}(a_i)\phi^{-i}$ that is equivalent to

$$\phi^3(a_0)\phi^3(y) + \phi^2(a_1)\phi^2(y) + \phi(a_2)\phi(y) + a_3 y = 0, \quad \text{where} \quad a_i \in \mathbf{k}.$$

THEOREM 7.1. — *Let us assume that*

 – *there is no $u \in \mathbf{k}$ such that*

$$a_3 u\phi(u)\phi^2(u) + a_2 u\phi(u) + a_1 u + a_0 = 0.$$

 – *there is no $u \in \mathbf{k}$ such that*

$$\phi^3(a_0)u\phi(u)\phi^2(u) + \phi^2(a_1)u\phi(u) + \phi(a_2)u + a_3 = 0.$$

 – *there is no $g \in \mathbf{k}$ and nonzero linear differential operator $L \in C[\partial]$, such that*

$$L(\partial(a_0/a_3)/(a_0/a_3)) = \phi(g) - g.$$

Then, f is ∂-transcendent over $\mathbf{k}$.

Proof. — Let G be the difference Galois group of the equation of order three satisfied by f. The first assumption ensures that the operator has no right factor of order one and the second assumption ensures that the operator has no left factor of order one. So the operator is irreducible and then the difference Galois group is irreducible. When G is imprimitive, this is the same reasoning as [ADR21, Theorem 3.5]. When G is primitive, it contains $SO_3(C)$ and we now follow the proof of [ADR21, Theorem 3.5]. $\square$

8. Acknowledgments

BIBLIOGRAPHY

[AB98] S. A. ABRAMOV & M. A. BARKATOU – "Rational solutions of first order linear difference systems", in *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (Rostock)*, ACM, New York, 1998, p. 124–131.

[AB01] S. A. ABRAMOV & M. BRONSTEIN – "On solutions of linear functional systems", in *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, ACM, New York, 2001, p. 1–6.

[ABPS21] S. A. ABRAMOV, M. BRONSTEIN, M. PETKOVŠEK & C. SCHNEIDER – "On rational and hypergeometric solutions of linear ordinary difference equations in $\Pi\Sigma^*$-field extensions", *Journal of Symbolic Computation* **107** (2021), p. 23–66.

[Abr95] S. A. ABRAMOV – "Rational solutions of linear difference and q-difference equations with polynomial coefficients", *Programming and Computer Software* **21** (1995), no. 6, p. 273–278.

[Abr02] _____, "A direct algorithm to compute rational solutions of first order linear q-difference systems", *Discrete Mathematics* **246** (2002), p. 3–12.

[ADH21] B. ADAMCZEWSKI, T. DREYFUS & C. HARDOUIN – "Hypertranscendence and linear difference equations", *Journal of the American Mathematical Society* **34** (2021), no. 2, p. 475–503.

[ADHW24] B. ADAMCZEWSKI, T. DREYFUS, C. HARDOUIN & M. WIBMER – "Algebraic independence and linear difference equations", *Journal of the European Mathematical Society* **26** (2024), no. 5, p. 1899–1932.

[ADR21]   C. E. Arreche, T. Dreyfus & J. Roques – "Differential transcendence criteria for second-order linear difference equations and elliptic hypergeometric functions", *Journal de l'École polytechnique—Mathématiques* **8** (2021), p. 147–168.

[AMP22]   E. Amzallag, A. Minchenko & G. Pogudin – "Degree bound for toric envelope of a linear algebraic group", *Mathematics of Computation* **91** (2022), no. 335, p. 1501–1519.

[APP98]   S. A. Abramov, P. Paule & M. Petkovšek – "q-hypergeometric solutions of q-difference equations", in *Proceedings of the 7th Conference on Formal Power Series and Algebraic Combinatorics (Noisy-le-Grand, 1995)*, vol. 180, 1998, p. 3–22.

[AS17]   C. E. Arreche & M. F. Singer – "Galois groups for integrable and projectively integrable linear difference equations", *Journal of Algebra* **480** (2017), p. 423–449.

[BCWDV16]   M. A. Barkatou, T. Cluzeau, J.-A. Weil & L. Di Vizio – "Computing the Lie algebra of the differential Galois group of a linear differential system", in *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, 2016, p. 63–70.

[CDDM18]   F. Chyzak, T. Dreyfus, P. Dumas & M. Mezzarobba – "Computing solutions of linear Mahler equations", *Mathematics of Computation* **87** (2018), p. 2977–3021.

[CDDM24]   ———, "First-order factors of linear mahler operators", *preprint, arXiv:2403.11545* (2024).

[Com22]   T. Combot – "Hyperexponential solutions of elliptic difference equations", *preprint, arXiv:2205.00041* (2022).

[CS99]   E. Compoint & M. F. Singer – "Computing galois groups of completely reducible differential equations", *Journal of Symbolic Computation* **28** (1999), no. 4, p. 473–494.

[CvH06]   T. Cluzeau & M. van Hoeij – "Computing hypergeometric solutions of linear recurrence equations", *Applicable Algebra in Engineering, Communication and Computing* **17** (2006), no. 2, p. 83–115.

[DH21]   T. Dreyfus & C. Hardouin – "Length derivative of the generating function of walks confined in the quarter plane", *Confluentes Mathematici* **13** (2021), no. 2, p. 39–92.

[DHR18]   T. Dreyfus, C. Hardouin & J. Roques – "Hypertranscendence of solutions of mahler equations", *Journal of the European Mathematical Society* **20** (2018), no. 9, p. 2209–2238.

[DHR21]   ———, "Functional relations for solutions of q-difference equations", *Mathematische Zeitschrift* (2021), p. 1–41.

[DHRS18]   T. DREYFUS, C. HARDOUIN, J. ROQUES & M. F. SINGER –
           "On the nature of the generating series of walks in the quarter
           plane", *Inventiones mathematicae* **213** (2018), no. 1, p. 139–203.

[DR15]   T. DREYFUS & J. ROQUES – "Galois groups of difference equa-
           tions of order two on elliptic curves", *SIGMA. Symmetry, In-
           tegrability and Geometry: Methods and Applications* **11** (2015),
           p. 003.

[DW22]   T. DREYFUS & J.-A. WEIL – "Computing the lie algebra of the
           differential galois group: the reducible case", *Journal of Symbolic
           Computation* **112** (2022), p. 122–163.

[Fen15]   R. FENG – "Hrushovski's algorithm for computing the galois
           group of a linear differential equation", *Advances in Applied
           Mathematics* **65** (2015), p. 1–37.

[Fen18]   ———, "On the computation of the Galois group of linear differ-
           ence equations", *Mathematics of Computation* **87** (2018), no. 310,
           p. 941–965.

[Hen97]   P. A. HENDRIKS – "An algorithm for computing a standard form
           for second-order linear q-difference equations", *Journal of pure
           and applied algebra* **117** (1997), p. 331–352.

[Hen98]   P. A. HENDRIKS – "An algorithm determining the difference ga-
           lois group of second order linear difference equations", *Journal of
           Symbolic Computation* **26** (1998), no. 4, p. 445–462.

[Hru02]   E. HRUSHOVSKI – "Computing the galois group of a linear dif-
           ferential equation", *Banach Center Publications* **58** (2002), no. 1,
           p. 97–138.

[HS08]   C. HARDOUIN & M. F. SINGER – "Differential Galois theory of
           linear difference equations", *Mathematische Annalen* **342** (2008),
           no. 2, p. 333–377.

[HSS16]   C. HARDOUIN, J. SAULOY & M. F. SINGER – *Galois theories of
           linear difference equations: an introduction*, vol. 211, American
           Mathematical Society, 2016.

[Kov86]   J. J. KOVACIC – "An algorithm for solving second order linear
           homogeneous differential equations", *Journal of Symbolic Com-
           putation* **2** (1986), no. 1, p. 3–43.

[Lan05]   S. LANG – *Algebra*, Graduate Texts in Mathematics, Springer
           New York, 2005.

[NAvdPT08] K. NGUYEN-AN, M. VAN DER PUT & J. TOP – "Algebraic sub-
           groups of $GL_2(\mathbb{C})$", *Indagationes Mathematicae-New series* **19**
           (2008), no. 2, p. 287–297.

[Pet92]   M. PETKOVŠEK – "Hypergeometric solutions of linear recurrences
           with polynomial coefficients", *Journal of Symbolic Computation*
           14 (1992), no. 2-3, p. 243–264.

[Phi15]   P. PHILIPPON – "Groupes de Galois et nombres automatiques", *Journal of the London Mathematical Society. Second Series* **92** (2015), no. 3, p. 596–614.

[Pou21]   M. POULET – "A density theorem for the difference galois groups of regular singular mahler equations", *International Mathematics Research Notices* **2023** (2021), no. 1, p. 536–587.

[Roq11]   J. ROQUES – "Generalized basic hypergeometric equations", *Inventiones mathematicae* **184** (2011), no. 3, p. 499–528.

[Roq18]   _____, "On the algebraic relations between mahler functions", *Transactions of the American Mathematical Society* **370** (2018), no. 1, p. 321–355.

[RS07]   J.-P. RAMIS & J. SAULOY – "The q-analogue of the wild fundamental group (i)", *RIMS Kôkyûroku Bessatsu* **B2** (2007), p. 167–193.

[RS09]   _____, "The *q*-analogue of the wild fundamental group (II)", *Astérisque* **323** (2009), p. 301–324.

[RSZ13]   J.-P. RAMIS, J. SAULOY & C. ZHANG – *Local analytic classification of q-difference equations*, Astérisque, no. 355, Société mathématique de France, 2013.

[Spr98]   T. A. SPRINGER – *Linear algebraic groups*, Progress in mathematics, vol. 9, Springer, 1998.

[SU93]   M. F. SINGER & F. ULMER – "Galois groups of second and third order linear differential equations", *Journal of Symbolic Computation* **16** (1993), no. 1, p. 9–36.

[vdPS97]   M. VAN DER PUT & M. F. SINGER – *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666, Springer-Verlag, Berlin, 1997.

[vH98]   M. VAN HOEIJ – "Rational solutions of linear difference equations", in *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (Rostock)*, ACM, New York, 1998, p. 120–123.