Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

ON THE COMPUTATION OF THE DIFFERENCE GALOIS GROUPS OF ORDER 3 EQUATIONS

Thomas Dreyfus & Marina Poulet

Tome 153
Fascicule 1

2025

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 143-186

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 1, tome 153, mars 2025

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
`commandes@smf.emath.fr`

AMS
P.O. Box 6248
Providence RI 02940
USA
`www.ams.org`

Tarifs

Vente au numéro : 50 € ($ 75)
Abonnement électronique : 165 € ($ 247),
avec supplément papier : Europe 251 €, hors Europe 289 € ($ 433)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Bulletin de la SMF

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 1 44 27 67 99 • Fax : (33) 1 40 46 90 96
`bulletin@smf.emath.fr` • `smf.emath.fr`

ISSN 0037-9484 (print) 2102-622X (electronic)

Directrice de la publication : Isabelle GALLAGHER

Bull. Soc. Math. France
153 (1), 2025, p. 143-186

ON THE COMPUTATION OF THE DIFFERENCE GALOIS GROUPS OF ORDER 3 EQUATIONS

BY THOMAS DREYFUS & MARINA POULET

ABSTRACT. — In this paper we consider the problem of computing the difference Galois groups of order 3 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 3 difference equations. We also compute the difference Galois group of an equation suggested by Wadim Zudilin.

Texte reçu le 4 juillet 2023, modifié le 28 août 2024, accepté le 9 octobre 2024.

THOMAS DREYFUS, Université Bourgogne Europe, CNRS, IMB UMR 5584, 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

Mathematical subject classification (2010). — 39A06, 12H05.

Key words and phrases. — Difference Galois theory, algorithm, differential transcendence.

This project has received funding from the ANR De rerum natura project (ANR-19-CE40-0018) and ANR Resyst (ANR-22-CE40-0002). The IMB receives support from the EIPHI Graduate School (contract ANR-17-EURE-0002).

 0037-9484/2025/143/$ 5.00
 doi:10.24033/bsmf.2898

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.

1. Introduction

Difference Galois theory has been 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 that 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) $\mathbf{k} = C\left(z^{1/*}\right) := \bigcup_{\ell=1}^{\infty} C(z^{1/\ell})$ 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, $\mathbf{k} = \mathcal{M}er(\Lambda^\infty) := \bigcup_{\ell=1}^{\infty} C(\wp(z/\ell), \partial_z \wp(z/\ell))$ 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 that 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, [36, 38]). 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 [27]), 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 [7, 8, 10, 11, 19, 20, 27]) 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, [21]. 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 [42] and density theorems [37, 39], 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, [12, 17, 23, 32, 44]. 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 [31] and some improvements [9, 24]). 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 [29, 38]), the q-difference (see [28]), the Mahler (see [43]) and the elliptic cases (see [22]). For the shift case, an analogue of Hrushovski's algorithm was developed in [25]. 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 a 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 with 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 to use it in practice. In fact, one of the key points 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 runs as a common thread throughout this paper. The following double sum is related to the Rogers–Ramanujan identities

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

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

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

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 [29].

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

Using [20, 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 $U(q^2z,t)$ over $\mathbb{C}(z^{1/*})$.

Now, we describe the content of this paper more precisely. After some reminders about the Galois theory of difference equations in Section 2.1, we recall a criterion in Section 2.2 to determine whether or not the Galois group G of a difference equation is reducible. 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 that occur when the order of the difference system is a prime number in Section 3.2. Moreover, we know what information corresponds 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 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 3 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 by $[A]$ when there is no ambiguity.

2. Difference algebra

2.1. Galois groups. — In this section, we give a short overview of the Galois theory of linear difference equations. For more details on what follows, we refer the reader to [38, 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

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

according to [38, 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 $\mathbf{L}$ that 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 [38, 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 $\rho(G)$", and, 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.