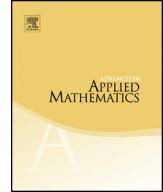




Contents lists available at ScienceDirect

Advances in Applied Mathematics

www.elsevier.com/locate/yaama



Computing differential Galois groups of second-order linear q -difference equations [☆]



Carlos E. Arreche ^a, Yi Zhang ^{b,*}

^a Department of Mathematical Sciences, The University of Texas at Dallas, Richardson, TX 75080, United States of America

^b Department of Foundational Mathematics, School of Science, Xi'an Jiaotong-Liverpool University, Suzhou, 215123, China

ARTICLE INFO

Article history:

Received 15 October 2020

Received in revised form 9 August 2021

Accepted 17 August 2021

Available online xxxx

MSC:

primary 39A06

secondary 12H10, 12H05, 20H20

Keywords:

q -Difference equations

Difference Galois theory

Differential Galois theory

ABSTRACT

We apply the differential Galois theory for difference equations developed by Hardouin and Singer to compute the differential Galois group for a second-order linear q -difference equation with rational function coefficients. This Galois group encodes the possible polynomial differential relations among the solutions of the equation. We apply our results to compute the differential Galois groups of several concrete q -difference equations, including for the colored Jones polynomial of a certain knot.

© 2021 Elsevier Inc. All rights reserved.

[☆] The work of both authors was partially supported by NSF grant CCF-1815108. The work of Y. Zhang was supported by XJTLU Research Development Funding RDF-20-01-12 and the National Nature Science Foundation of China grant NSFC-12101506.

* Corresponding author.

E-mail addresses: arreche@utdallas.edu (C.E. Arreche), Yi.Zhang03@xjtlu.edu.cn (Y. Zhang).

1. Introduction

Consider a second-order homogeneous linear q -dilation equation

$$y(q^2x) + a(x)y(qx) + b(x)y(x) = 0, \quad (1.1)$$

whose coefficients $a(x), b(x) \in \bar{\mathbb{Q}}(x)$ are rational functions in x with $b(x) \neq 0$, and $q \in \bar{\mathbb{Q}}$ is neither zero nor a root of unity. Difference equations such as (1.1) are satisfied by special functions and generating series occurring in combinatorics, number theory, mathematical physics, and many other areas. There has been much recent work devoted to the question of which additional functional equations are satisfied by solutions of difference equations. We develop algorithms that allow one to discover all the polynomial differential equations satisfied by the solutions to (1.1), or to decide that there are none. Our methods and results apply equally well, with small and obvious modifications, to equations (1.1) where q is not necessarily an algebraic number and the coefficients $a, b \in C(x)$ for any computable algebraically closed field C containing $\mathbb{Q}(q)$.

Our strategy here is similar to the one followed in [4], where analogous algorithmic results were developed in the context of shift difference equations. We apply the differential Galois theory for difference equations developed in [13], which studies equations such as (1.1) from a purely algebraic point of view. This theory attaches a geometric object G to (1.1), called the differential Galois group, that encodes all the difference-differential algebraic relations among the solutions to (1.1). We develop an algorithm to compute the differential Galois group G associated to (1.1) by the theory of [13].

The differential Galois theory for difference equations of [13] is a generalization of the q -dilation analogue of the Galois theory for difference equations presented in [26], where the Galois groups that arise encode the algebraic relations among the solutions to a given linear difference equation. An algorithm to compute the Galois group $\tilde{H}$ associated to (1.1) by the theory of [26] is developed in [11]—but for technical reasons this algorithm works only over the larger base field $\bar{\mathbb{Q}}(\{x^{1/n}\}_{n \in \mathbb{N}})$, rather than the field of definition $\bar{\mathbb{Q}}(x)$ of (1.1). In the course of our computation of the differential Galois group G of (1.1), we also extend the algorithm of [11] to compute the Galois group H of (1.1) over the smaller original basefield $\bar{\mathbb{Q}}(x)$.

A priori one knows that the Galois group H is a linear algebraic group, and the differential Galois group G is a linear differential algebraic group (Definition 2.7). The Galois group H serves as a close upper bound for the differential Galois group G : it is shown in [13] that one can consider G as a Zariski-dense subgroup of H (see Proposition 2.10 for a precise statement). In view of this fact, our strategy to compute G is to first apply our extension (developed in the present work) of the algorithm of [11] to compute H , and then compute the additional differential-algebraic equations (if any) that define G as a subgroup of H . The computation of G in general can be much more difficult than that of H because there are many more linear differential algebraic groups than there are linear algebraic groups (more precisely, the latter are instances of the former), so identifying

the correct differential Galois group from among these additional possibilities requires additional work.

This strategy is reminiscent of the one begun in [9], and concluded in [1–3], to compute the parameterized differential Galois group for a second-order linear differential equation with differential parameters, where the results of [15,6] are first applied to compute the classical (non-parameterized) differential Galois group for the differential equation, and one then computes the additional differential-algebraic equations, with respect to the parametric derivations, that define the parameterized differential Galois group inside the classical one. However, the computation of the differential Galois group G for (1.1) presents substantial new complications that do not arise in the parameterized differential setting. Many of these new complications are inherent to the computation of differential Galois groups of difference equations in general, and already arise in the context of shift difference equations (see the introduction to [4] for a summary), but a brand new technical difficulty arises for the first time in the context of q -difference equations, which we describe below. The same difficulties will recur, with a vengeance, in the context of Galois theory for difference equations over elliptic curves; our hope is that the treatment developed here will serve as a useful blueprint for that more technical setting.

It is known (see [11]) that the Galois group $\tilde{H}$ of any q -difference equation over $\bar{\mathbb{Q}}(\{x^{1/n}\}_{n \in \mathbb{N}})$ has a cyclic group of connected components $\tilde{H}/\tilde{H}^\circ$. This fact facilitates the development of the algorithm of [11]. However, the Galois group H of a q -difference equation over $\bar{\mathbb{Q}}(x)$ may admit more generally a bicyclic group of connected components, which requires the development of new techniques to identify the correct Galois group from among this larger set of possibilities.

A theoretical consequence of the results of §6 is Corollary 6.4, which states that the unipotent radical of the differential Galois group may only be trivial, the additive group of differentially constant σ -invariants, or the full additive group of σ -invariants. This result was already known when the whole differential Galois G group was already unipotent [13, Prop. 4.3(2)], but not when the unipotent radical is a proper subgroup of G . In other contexts (see for example [19,20]) the computation of the unipotent radical has turned out to be the main theoretical obstacle in the development of algorithms to compute Galois groups in general. We expect that this contribution to the inverse Galois problem in the present setting will have useful ramifications in the development of future algorithms to compute differential Galois groups for higher-order q -difference equations.

Let us now describe the contents of this work in more detail. In §2, we summarize the differential Galois theory for difference equations of [13], and prove some auxiliary results that will be used in the sequel. In §3, we recall some known results, and prove some new ones, concerning differential relations among solutions to first-order q -difference equations. In §4, we summarize Hendriks' algorithm [12] to compute the Galois group $\tilde{H}$ for (1.1) over $\bar{\mathbb{Q}}(\{x^{1/n}\}_{n \in \mathbb{N}})$, and explain how to extend it to compute the Galois group H for (1.1) over $\bar{\mathbb{Q}}(x)$. In §5, we show how to compute the differential Galois group G for (1.1) when H is diagonalizable in Proposition 5.2. In §6, we show how to compute G when H is assumed to be reducible but non-diagonalizable in Proposition 6.1

and Proposition 6.2—as a consequence, we show in Corollary 6.4 that the unipotent radical of G is always of a very special form. In §7, we compute G in Proposition 7.4, Proposition 7.6, and Proposition 7.7, under the assumption that H is irreducible and imprimitive (which possibility can arise in three different ways, as a consequence of our insistence on computing Galois groups over the basefield $\bar{\mathbb{Q}}(x)$ and not just over $\bar{\mathbb{Q}}(\{x^{1/n}\}_{n \in \mathbb{N}})$). In §8, we apply results from [5] to compute G in Proposition 8.1, under the assumption that H contains SL_2 . We conclude in §9 by applying these results to some concrete examples of q -difference equations; in particular to the one satisfied by the colored Jones polynomial of a certain knot.

2. Preliminaries on differential Galois theory for difference equations

We begin with a summary of the differential Galois theory for difference equations developed in [13]. Every field is assumed to be of characteristic zero, and every ring is assumed to be commutative unless otherwise stated.

Definition 2.1. A $\sigma\delta$ -ring is a commutative ring R with unit, equipped with an automorphism σ and a derivation δ such that $\sigma(\delta(r)) = \delta(\sigma(r))$ for every $r \in R$. A $\sigma\delta$ -field is defined analogously. We write

$$R^\sigma = \{r \in R \mid \sigma(r) = r\}; \quad R^\delta = \{r \in R \mid \delta(r) = 0\}; \quad \text{and} \quad R^{\sigma\delta} = R^\sigma \cap R^\delta,$$

and refer to these as the subrings of σ -constants, δ -constants, and $\sigma\delta$ -constants, respectively.

A $\sigma\delta$ - R -algebra is a $\sigma\delta$ -ring S equipped with a ring homomorphism $R \rightarrow S$ that commutes with both σ and δ . If R and S are fields, we also say that S is a $\sigma\delta$ -field extension of R . The notions of σ - R -algebra, δ - R -algebra, σ -field extension, and δ -field extension are defined analogously. If $z_1, \dots, z_n \in S$, we write $R\{z_1, \dots, z_n\}_\delta$ for the smallest δ - R -subalgebra of S that contains $z_1, \dots, z_n$; as R -algebras, we have

$$R\{z_1, \dots, z_n\}_\delta = R[\{\delta^i(z_1), \dots, \delta^i(z_n) \mid i \in \mathbb{N}\}].$$

If $Z = (z_{ij})$ with $1 \leq i, j \leq n$ is a matrix, we write $R = \{Z\}_\delta$ for

$$R\{z_{11}, \dots, z_{1n}, \dots, z_{n1}, \dots, z_{nn}\}_\delta.$$

An important example of a $\sigma\delta$ -field that will play a prominent role throughout this work is $k = \bar{\mathbb{Q}}(x)$, where σ denotes the $\bar{\mathbb{Q}}$ -linear automorphism defined by $\sigma(x) = qx$ for some fixed $q \in \bar{\mathbb{Q}}$ that is neither zero nor a root of unity, and $\delta = x \frac{d}{dx}$. Note that in this case $k^\sigma = k^\delta = \bar{\mathbb{Q}}$.

Suppose that k is a $\sigma\delta$ -field, and consider the matrix difference equation

$$\sigma(Y) = AY, \quad \text{where } A \in \mathrm{GL}_n(k). \quad (2.1)$$

Definition 2.2. A $\sigma\delta$ -Picard-Vessiot ring (or $\sigma\delta$ -PV ring) over k for (2.1) is a $\sigma\delta$ - k -algebra R such that:

- (i) R is a *simple* $\sigma\delta$ -ring, i.e., R has no ideals, other than 0 and R , that are stable under both σ and δ ;
- (ii) there exists a matrix $Z \in \mathrm{GL}_n(R)$ such that $\sigma(Z) = AZ$; and
- (iii) R is generated as a δ - k -algebra by the entries of Z and $1/\det(Z)$, i.e., $R = k\{Z, 1/\det(Z)\}_\delta$.

The matrix Z is called a *fundamental solution matrix* for (2.1).

Note that when $\delta = 0$, this coincides with the definition of the σ -PV ring over k for (2.1) given in [26, Def. 1.5]. In the usual Galois theory of difference equations presented in [26], the existence and uniqueness of Picard-Vessiot rings up to k - σ -isomorphism is guaranteed by the assumption that k^σ is algebraically closed (see [26, §1.1]). Analogously, in the difference-differential Galois theory developed in [13], one needs to assume that k^σ is δ -closed [14,25].

Definition 2.3. The ring of δ -polynomials in n variables over a δ -field C is

$$C\{Y_1, \dots, Y_n\}_\delta = C[\{\delta^i(Y_1), \dots, \delta^i(Y_n) \mid i \in \mathbb{N}\}],$$

the free C -algebra on the symbols $\delta^i(Y_j)$, on which δ acts as a derivation in the obvious way. We say $\mathcal{L} \in C\{Y_1, \dots, Y_n\}_\delta$ is a *homogeneous linear δ -polynomial* if it belongs to the C -linear span of the symbols $\delta^i(Y_j)$.

If R is a δ - C -algebra, we say that $z_1, \dots, z_n \in R$ are *differentially dependent* over C if there exists a δ -polynomial $0 \neq P \in C\{Y_1, \dots, Y_n\}_\delta$ such that $P(z_1, \dots, z_n) = 0$; otherwise we say that $z_1, \dots, z_n$ are δ -*independent* over C . When a single element $z \in R$ is δ -independent (resp., δ -dependent) over C , we say that z is δ -*transcendental* (resp., δ -*algebraic*) over C .

We say the δ -field C is δ -closed if any system of δ -polynomial equations

$$\{P_1 = 0, \dots, P_m = 0 \mid P_i \in C\{Y_1, \dots, Y_n\}_\delta \text{ for } 1 \leq i \leq m\}$$

that has a solution in $\tilde{C}^n$ for some δ -field extension $\tilde{C} \supseteq C$ already has a solution in C^n .

Theorem 2.4. (Cf. [13, Prop. 2.4]) If $k^\sigma = C$ is δ -closed, there exists a $\sigma\delta$ -PV ring for (2.1), and it is unique up to $\sigma\delta$ - k -isomorphism. Moreover, $R^\sigma = k^\sigma$.

For the rest of this section, unless explicitly stated otherwise, we assume that k is a $\sigma\delta$ -field such that k^σ is δ -closed.

Definition 2.5. The $\sigma\delta$ -Galois group of (2.1) is the group of $\sigma\delta$ - k -automorphisms of the $\sigma\delta$ -PV ring R for (2.1):

$$\mathrm{Gal}_{\sigma\delta}(R/k) = \{\gamma \in \mathrm{Aut}_{k\text{-alg}}(R) \mid \gamma \circ \sigma = \sigma \circ \gamma \text{ and } \gamma \circ \delta = \delta \circ \gamma\}.$$

As in the usual (non-differential) Galois theory of difference equations [26], a choice of fundamental solution $Z = (z_{ij}) \in \mathrm{GL}_n(R)$ defines a faithful representation $\mathrm{Gal}_{\sigma\delta}(R/k) \hookrightarrow \mathrm{GL}_n(k^\sigma) : \gamma \mapsto M_\gamma$, via

$$\gamma(Z) = \begin{pmatrix} \gamma(z_{11}) & \cdots & \gamma(z_{1n}) \\ \vdots & & \vdots \\ \gamma(z_{n1}) & \cdots & \gamma(z_{nn}) \end{pmatrix} = \begin{pmatrix} z_{11} & \cdots & z_{1n} \\ \vdots & & \vdots \\ z_{n1} & \cdots & z_{nn} \end{pmatrix} \cdot M_\gamma.$$

A different choice of fundamental solution matrix $Z' \in \mathrm{GL}_n(R)$ defines a conjugate representation of $\mathrm{Gal}_{\sigma\delta}(R/k)$ in $\mathrm{GL}_n(k^\sigma)$.

Definition 2.6. The systems $\sigma(Y) = AY$ and $\sigma(Y) = BY$ for $A, B \in \mathrm{GL}_n(k)$ are *equivalent* if there exists a matrix $T \in \mathrm{GL}_n(k)$ such that $\sigma(T)AT^{-1} = B$. In this case, if Z is a fundamental solution matrix for $\sigma(Y) = AY$, then TZ is a fundamental solution matrix for $\sigma(Y) = BY$, and therefore the $\sigma\delta$ -PV rings of k for these systems defined by the choice of fundamental solution matrices Z and TZ , and the associated representations of $\sigma\delta$ -Galois groups in $\mathrm{GL}_n(k^\sigma)$, are isomorphic.

Definition 2.7. Suppose that C is a δ -closed field. A *linear differential algebraic group* over C is a subgroup G of $\mathrm{GL}_n(C)$ defined by (finitely many) δ -polynomial equations in the matrix entries.

Theorem 2.8. (Cf. [13, Thm. 2.6]) *The $\sigma\delta$ -PV ring R over k for (2.1) is a reduced ring, and any choice of fundamental solution matrix $Z \in \mathrm{GL}_n(R)$ identifies $\mathrm{Gal}_{\sigma\delta}(R/k)$ with a linear differential algebraic subgroup of $\mathrm{GL}_n(k^\sigma)$.*

As in [13, p. 337], we observe that if R is a $\sigma\delta$ -PV ring over k for (2.1), and K is the total ring of fractions of R , then any $\sigma\delta$ - k -automorphism of K must leave R invariant, whence the group $\mathrm{Gal}_{\sigma\delta}(K/k)$ of such automorphisms coincides with $\mathrm{Gal}_{\sigma\delta}(R/k)$. The consideration of the total ring of fractions of R is necessary to obtain the following Galois correspondence.

Theorem 2.9. (Cf. [13, Thm. 2.7]) *With notation as above, let $\mathcal{F}$ be the set of $\sigma\delta$ -rings F such that $k \subseteq F \subseteq K$ and every non-zero divisor in F is a unit in F , and let $\mathcal{G}$ denote the set of linear differential algebraic subgroups G of $\mathrm{Gal}_{\sigma\delta}(K/k)$. There is a bijective correspondence $\mathcal{F} \leftrightarrow \mathcal{G}$ given by*

$$F \mapsto \mathrm{Gal}_{\sigma\delta}(K/F) = \{\gamma \in \mathrm{Gal}_{\sigma\delta}(K/k) \mid \gamma(r) = r, \forall r \in F\}; \quad \text{and} \\ G \mapsto K^G = \{r \in K \mid \gamma(r) = r, \forall \gamma \in G\}.$$

In particular, an element $r \in K$ is left fixed by all of $\mathrm{Gal}_{\sigma\delta}(K/k)$ if and only if $r \in k$.

The following result relates the $\sigma\delta$ -PV rings and $\sigma\delta$ -Galois groups of [13] to the σ -PV rings and σ -Galois groups considered in [26,12].

Proposition 2.10. (Cf. [13, Prop. 2.8]) Assume k^σ is δ -closed. Let R be a $\sigma\delta$ -PV ring over k for (2.1) with fundamental solution matrix $Z \in \mathrm{GL}_n(R)$, and let $S = k[Z, 1/\det(Z)] \subset R$. Then:

- (i) S is a σ -PV ring over k for (2.1); and
- (ii) $\mathrm{Gal}_{\sigma\delta}(R/k)$ is Zariski-dense in the σ -Galois group $\mathrm{Gal}_\sigma(S/k)$.

3. Differential relations among solutions of first-order q -difference equations

In this section we recall some known results, and prove some new ones, concerning differential relations among solutions of first-order q -difference equations. The following result is proved in [13, Prop. 3.1].

Proposition 3.1. Let R be a $\sigma\delta$ - k -algebra with $R^\sigma = k^\sigma$. Suppose $b_1, \dots, b_m \in k$ and $z_1, \dots, z_m \in R$ satisfy

$$\sigma(z_i) - z_i = b_i; \quad i = 1, \dots, m.$$

Then $z_1, \dots, z_m$ are differentially dependent over k if and only if there exists a nonzero homogeneous linear δ -polynomial $\mathcal{L}(Y_1, \dots, Y_m)$ with coefficients in k^σ and an element $f \in k$ such that

$$\mathcal{L}(b_1, \dots, b_m) = \sigma(f) - f.$$

For the remainder of this section, we restrict our attention to the $\sigma\delta$ -field $k = C(x)$, where $\delta(x) = x$, C is a δ -closed field of characteristic zero, and σ is the C -linear automorphism of k defined by setting $\sigma(x) = qx$ for some $q \in C^\delta$ that is neither zero nor a root of unity.

The following notion of q -discrete residue, defined in [8, Def. 2.7], will be crucial in several proofs in this paper.

Definition 3.2. For any non-zero $\beta \in C$, we call the subset

$$[\beta]_q = \beta q^\mathbb{Z} = \{\beta q^\ell \mid \ell \in \mathbb{Z}\} \subset C$$

the $q^\mathbb{Z}$ -orbit of β in C . Any $f \in k$ can be decomposed into the form

$$f = c + xp_1 + \frac{p_2}{x^s} + \sum_{i=1}^m \sum_{j=1}^{n_i} \sum_{\ell=0}^{d_{i,j}} \frac{\alpha_{i,j,\ell}}{(x - \beta_i q^\ell)^j},$$

where $p_1, p_2 \in C[x]$; $s, m, n_i, d_{i,j} \in \mathbb{N}$; $c, \alpha_{i,j,\ell}, \beta_i \in C$; $\deg(p_2) < s$; and the β_i are non-zero and belong to distinct $q^{\mathbb{Z}}$ -orbits.

The q -discrete residue of f at the $q^{\mathbb{Z}}$ -orbit $[\beta_i]_q$ of multiplicity j (with respect to x) is defined as:

$$q\text{-dres}(f, [\beta_i]_q, j) = \sum_{\ell=0}^{d_{i,j}} q^{-\ell j} \alpha_{i,j,\ell}.$$

In addition, the constant c above is the q -discrete residue of f at infinity, which we denote by $q\text{-dres}(f, \infty)$.

The usefulness of the notion of discrete residue stems from the following result.

Proposition 3.3. (Cf. [8, Prop. 2.10]) *Let $f, g \in C[x]$ be non-zero, relatively prime polynomials. There exists $h \in k$ such that $\sigma(h) - h = f/g$ if and only if $q\text{-dres}(f/g, \infty) = 0$ and $q\text{-dres}(f/g, [\beta]_q, j) = 0$ for every $j \in \mathbb{N}$ and every $0 \neq \beta \in C$ such that $g(\beta) = 0$.*

The following computational lemma will be used to sharpen the conclusion of [13, Cor. 3.3] in the following Corollary 3.5.

Lemma 3.4. *Suppose $0 \neq a \in C^\delta(x)$, $r \in \mathbb{Z}_{\geq 0}$, and $0 \neq \beta \in C^\delta$ is a zero or pole of a . Then*

$$q\text{-dres}\left(\delta^r\left(\frac{\delta(a)}{a}\right), [\beta]_q, r+1\right) = (-1)^r \cdot r! \cdot \beta^r \cdot q\text{-dres}\left(\frac{\delta(a)}{a}, [\beta]_q, 1\right).$$

Proof. We may assume without loss of generality that

$$\frac{\delta(a)}{a} = \sum_{\ell=0}^d \left(e_\ell + \frac{e_\ell q^\ell \beta}{x - \beta q^\ell} \right) \quad (3.1)$$

for some $0 \neq \beta \in C^\delta$, $d \in \mathbb{Z}_{\geq 0}$, and $e_\ell \in \mathbb{Z}$ for $\ell = 0, \dots, d$. Observe that in this case $q\text{-dres}\left(\frac{\delta(a)}{a}, [\beta]_q, 1\right) = \sum_{\ell=0}^d \beta e_\ell$, by Definition 3.2. We claim that

$$\delta^r\left(\frac{\delta(a)}{a}\right) = \sum_{\ell=0}^d \frac{(-1)^r r! q^{\ell(r+1)} \beta^{r+1} e_\ell}{(x - \beta q^\ell)^{r+1}} + (\text{lower-order terms}), \quad (3.2)$$

which would indeed imply that

$$q\text{-dres}\left(\delta^r\left(\frac{\delta(a)}{a}\right), [\beta]_q, r+1\right) = \sum_{\ell=0}^d (-1)^r r! \beta^{r+1} e_\ell$$

and conclude the proof of the Lemma. We prove (3.2) by induction. The case $r = 0$ is just (3.1). Assuming (3.2) for some $r \geq 0$, note that

$$\delta^{r+1} \left(\frac{\delta(a)}{a} \right) = \sum_{\ell=0}^d \frac{(-1)^{r+1} (r+1)! q^{\ell(r+1)} \beta^{r+1} e_{\ell} ((x - \beta q^{\ell}) + \beta q^{\ell})}{(x - \beta q^{\ell})^{r+2}} + (\text{lower-order terms}).$$

This concludes the proof of the claim, and the Lemma. $\square$

The following result sharpens the conclusion of [13, Cor. 3.3].

Corollary 3.5. *Let R be a $\sigma\delta$ - k -algebra with $R^{\sigma} = k^{\sigma} = C$. Let $a_1, \dots, a_m \in C^{\delta}(x)^{\times}$ and $z_1, \dots, z_m \in R^{\times}$ such that*

$$\sigma(z_i) = a_i z_i; \quad i = 1, \dots, m.$$

Then $z_1, \dots, z_m$ are differentially dependent over k if and only if there exist: $n_1, \dots, n_m \in \mathbb{Z}$, not all zero and with $\gcd(n_1, \dots, n_m) = 1$; $c \in \mathbb{Z}$; and an element $f \in k$, such that

$$n_1 \frac{\delta(a_1)}{a_1} + \dots + n_m \frac{\delta(a_m)}{a_m} = \sigma(f) - f + c. \quad (3.3)$$

Proof. First suppose there exist integers $n_1, \dots, n_m, c \in \mathbb{Z}$ as in (3.3). Since for each $i = 1, \dots, m$ we have that $\sigma\left(\frac{\delta(z_i)}{z_i}\right) = \frac{\delta(z_i)}{z_i} + \frac{\delta(a_i)}{a_i}$, it follows that

$$\begin{aligned} \sigma \left[\left(\sum_{i=1}^m n_i \delta \left(\frac{\delta(z_i)}{z_i} \right) \right) - \delta(f) \right] &= \sum_{i=1}^m n_i \delta \left(\frac{\delta(z_i)}{z_i} \right) + \delta \left(\sum_{i=1}^m n_i \frac{\delta(a_i)}{a_i} \right) - \sigma(\delta(f)) = \\ &= \sum_{i=1}^m n_i \delta \left(\frac{\delta(z_i)}{z_i} \right) + \delta(\sigma(f) - f + c) - \sigma(\delta(f)) = \sum_{i=1}^m n_i \delta \left(\frac{\delta(z_i)}{z_i} \right) - \delta(f). \end{aligned}$$

Therefore,

$$\sum_{i=1}^m n_i \delta \left(\frac{\delta(z_i)}{z_i} \right) = \delta(f) + e$$

for some $e \in R^{\sigma} = k^{\sigma}$. This shows that $z_1, \dots, z_m$ are δ -dependent over k , after multiplying by $(z_1 \dots z_m)^2$ on both sides.

Since $\sigma\left(\frac{\delta(z_i)}{z_i}\right) = \frac{\delta(z_i)}{z_i} + \frac{\delta(a_i)}{a_i}$ for each $i = 1, \dots, m$, Proposition 3.1 implies that the z_i are differentially dependent over k if and only if there exists an element $f \in k$ and a nonzero homogeneous linear δ -polynomial

$$\mathcal{L}(Y_1, \dots, Y_m) = \sum_{i=1}^m \sum_{j=0}^{r_i} c_{i,j} \delta^j Y_i, \quad c_{i,j} \in C,$$

such that

$$g = \mathcal{L} \left(\frac{\delta(a_1)}{a_1}, \dots, \frac{\delta(a_m)}{a_m} \right) = \sigma(f) - f. \quad (3.4)$$

Let $r = \max\{r_i \mid c_{i,r_i} \neq 0 \text{ for some } i\}$. For each $0 \neq \beta \in C$, it follows from (3.4), Proposition 3.3, and Lemma 3.4, that

$$q\text{-dres}(g, [\beta]_q, r+1) = (-1)^r \cdot r! \cdot \beta^r \cdot \sum_{i=1}^m c_{i,r} \cdot q\text{-dres}\left(\frac{\delta(a_i)}{a_i}, [\beta]_q, 1\right) = 0. \quad (3.5)$$

On the other hand, it follows from Definition 3.2 that for each $i = 1, \dots, m$ we have that

$$q\text{-dres}\left(\frac{\delta(a_i)}{a_i}, [\beta]_q, 1\right) = \beta \cdot e_i \quad \text{for some} \quad e_i \in \mathbb{Z}. \quad (3.6)$$

Substituting (3.6) into (3.5), we have

$$q\text{-dres}(g, [\beta]_q, r+1) = (-1)^r \cdot r! \cdot \beta^{r+1} \cdot \sum_{i=1}^m c_{i,r} \cdot e_i = 0. \quad (3.7)$$

Since $\beta \neq 0$, the above equation is equivalent to $\sum_{i=1}^m c_{i,r} \cdot e_i = 0$. Since $e_i \in \mathbb{Z}$ for each $i = 1, \dots, m$, we may take the $c_{i,r} = n_i$ to be integers. Set $c = \sum_{i=1}^m n_i \cdot q\text{-dres}\left(\frac{\delta(a_i)}{a_i}, \infty\right)$. Since both n_i and $q\text{-dres}\left(\frac{\delta(a_i)}{a_i}, \infty\right)$ are integers, we see that $c \in \mathbb{Z}$ is divisible by $\gcd(n_1, \dots, n_m)$. Moreover, we have

$$q\text{-dres}\left(n_1 \frac{\delta(a_1)}{a_1} + \dots + n_m \frac{\delta(a_m)}{a_m} - c, \infty\right) = 0. \quad (3.8)$$

By (3.7) and (3.8), the conclusion follows from another application of Proposition 3.3 and dividing both sides by $\gcd(n_1, \dots, n_m)$. $\square$

Remark 3.6. The statement of [13, Cor. 3.3] is equivalent to that of Corollary 3.5, except that each $n_i \in \mathbb{Z}$ is replaced with a homogeneous linear δ -polynomial $\mathcal{L}_i(Y) \in C^\delta\{Y\}_\delta$, the $c \in \mathbb{Z}$ is omitted, and (3.3) is replaced with

$$\mathcal{L}_1\left(\frac{\delta(a_1)}{a_1}\right) + \dots + \mathcal{L}_m\left(\frac{\delta(a_m)}{a_m}\right) = \sigma(f) - f.$$

We emphasize that our proof of Corollary 3.5 initially follows the same strategy of that of [13, Cor. 3.3], and then applies the technology of q -discrete residues of [8], in particular the computational Lemma 3.4, to obtained the sharpened conclusion. Although we find this result is of independent interest, it also plays an important role in the computation of differential Galois groups in the following sections, because it restricts a priori many possible differential algebraic groups from occurring as Galois groups.

4. Hendriks' algorithm

In this section, we summarize the results of [11] that we will need in our algorithm, and explain how to refine them to meet our goals. From now on, we restrict our attention to equations of the form

$$\sigma^2(y) + a\sigma(y) + by = 0, \quad (4.1)$$

where $a, b \in \bar{\mathbb{Q}}(x)$ with $b \neq 0$, and σ is the $\bar{\mathbb{Q}}$ -linear automorphism of $\bar{\mathbb{Q}}(x)$ defined by $\sigma(x) = qx$, where $q \in \bar{\mathbb{Q}}$ is neither zero nor a root of unity. Our discussion here could be generalized to drop the assumption that q is an algebraic number and allowing $a, b \in C_0(x)$, for any computable algebraically closed field C_0 containing $\mathbb{Q}(q)$, as we mentioned in the introduction (see also the introduction to [11]), but at the cost of overburdening the notation.

The matrix equation corresponding to (4.1) is

$$\sigma(Y) = AY, \quad \text{where } A := \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \in \text{GL}_2(k). \quad (4.2)$$

We consider $\bar{\mathbb{Q}}(x)$ as a $\sigma\delta$ -field by setting $\delta = x \frac{d}{dx}$, the Euler derivation. In this section only we will denote $k = \bar{\mathbb{Q}}(x)$, but in future sections we will recycle notation and denote by k the larger $\sigma\delta$ -field $C(x)$, where C is a δ -closure of $\bar{\mathbb{Q}}$, and σ is the C -linear automorphism of $C(x)$ defined by $\sigma(x) = qx$.

The algorithm of [11] computes the σ -Galois group of (4.1) over the larger basefield k_∞ defined as follows. Let $\{q_n \in \bar{\mathbb{Q}} \mid n \in \mathbb{N}\}$ denote a compatible system of n -th roots of $q = q_1$, so that for any factorization $\ell m = n$ we have $q_n^\ell = q_m$, and consider the cyclic σ -field extension $k_n = \bar{\mathbb{Q}}(x_n)$ of $\bar{\mathbb{Q}}(x)$ such that $x_n^n = x_1 = x$ and $x_n^\ell = x_m$ for any factorization $n = \ell m$, with the σ -field structure given by $\sigma(x_n) = q_n x_n$. Then the $\bar{\mathbb{Q}}$ -linear maps $k_m \hookrightarrow k_n$ defined by $x_m \mapsto x_n^\ell$ are embeddings of σ -fields. Let $k_\infty = \varinjlim k_n = \bigcup_{n \geq 1} k_n$. By [11, Lemmas 9 and 10], the σ -field k_∞ has property $\mathcal{P}$:

Definition 4.1. We say a σ -field k has property $\mathcal{P}$ if:

- (1) k is a $\mathcal{C}_1$ (quasi-algebraically closed) field in the sense of [17]; and
- (2) if k' is a finite algebraic extension of k such that σ extends to an automorphism of k' then $k' = k$.

This allows Hendriks to compute the σ -Galois group of (4.1) over k_∞ by finding a gauge transformation $T \in \text{GL}_2(k_\infty)$ that puts (4.2) in the standard form of [11, Definition 8].

Another special consequence of the fact that k_∞ enjoys property $\mathcal{P}$ (Definition 4.1) is that the σ -Galois group H_∞ for (4.1) over k_∞ (and in fact every difference Galois group over k_∞) is such that its quotient H_∞/H_∞° by the connected component of the identity

H_∞° must be a (finite) cyclic group (cf. [11, Thm. 6]). This facilitates the algorithm of [11] by ruling out a priori the consideration of algebraic groups whose group of connected components is not cyclic (cf. [11, Lem. 12]). The situation for σ -Galois groups over k_1 is less restrictive, but we still know by [26, Prop. 12.2(1)] that the σ -Galois group H_1 for (4.1) over k_1 (and in fact every difference Galois group over k_1) has the property that the quotient H_1/H_1° is (finite) bicyclic, i.e., a product of two finite cyclic groups. Thus it is possible for us to realize additional algebraic groups H_1 as σ -Galois groups for (4.1) over k_1 that do not occur in the list [11, Lem. 16 and Lem. 20] of possible σ -Galois groups over k_∞ . In particular, any reducible algebraic subgroup of $\mathrm{GL}_2(\bar{\mathbb{Q}})$ can occur as the σ -Galois group for some difference equation (4.1), and any irreducible imprimitive algebraic subgroup of $\mathrm{GL}_2(\bar{\mathbb{Q}})$ with bicyclic group of connected components can occur as a Galois group over k_1 .

The algorithm developed in [11] to compute H_∞ proceeds as follows. We first decide whether there exists a solution $u \in k_\infty$ to the *Riccati equation*

$$u\sigma(u) + au + b = 0. \quad (4.3)$$

If such a solution u exists, then the σ -Galois group H_∞ of (4.2) over k_∞ is *reducible*, i.e., conjugate to an algebraic subgroup of

$$\mathbb{G}_m(\bar{\mathbb{Q}})^2 \ltimes \mathbb{G}_a(\bar{\mathbb{Q}}) \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \lambda \end{pmatrix} \mid \alpha, \beta, \lambda \in \bar{\mathbb{Q}}, \alpha\lambda \neq 0 \right\}.$$

Moreover, if there exist at least two distinct solutions $u_1, u_2 \in k_\infty$ to (4.3) then H_∞ is *diagonalizable*, i.e., conjugate to an algebraic subgroup of

$$\mathbb{G}_m(\bar{\mathbb{Q}})^2 \simeq \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \lambda \end{pmatrix} \mid \alpha, \lambda \in \bar{\mathbb{Q}}, \alpha\lambda \neq 0 \right\};$$

and if there are at least three distinct solutions in k_∞ to (4.3) then there are infinitely many, and this occurs if and only if H_∞ is an algebraic subgroup of

$$\mathbb{G}_m(\bar{\mathbb{Q}}) \simeq \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \mid \alpha \in \bar{\mathbb{Q}}, \alpha \neq 0 \right\}.$$

If there is no solution $u \in k_\infty$ to the Riccati equation (4.3), then H_∞ is irreducible by [11, Thm. 13]. In this case, the next step is to attempt to find $T \in \mathrm{GL}_2(k_\infty)$ and $r \in k_\infty$ such that

$$\sigma(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1} = \begin{pmatrix} 0 & 1 \\ -r & 0 \end{pmatrix}. \quad (4.4)$$

If $a = 0$ already, then we may take $T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $r = b$. If $a \neq 0$, we then attempt to find a solution $e \in k_\infty$ to the Riccati equation

$$e\sigma^2(e) + \left(\sigma^2\left(\frac{b}{a}\right) - \sigma(a) + \frac{\sigma(b)}{a}\right)e + \frac{\sigma(b)b}{a^2} = 0. \quad (4.5)$$

If there exists such a solution $e \in k_\infty$ to (4.5), then it is proved in [11, Thm. 18] that there exists a matrix $T \in \mathrm{GL}_2(k_\infty)$ such that (4.4) is satisfied with

$$r = -a\sigma(a) + \sigma(b) + a\sigma^2\left(\frac{b}{a}\right) + a\sigma^2(e), \quad (4.6)$$

and H_∞ is *imprimitive*, i.e., conjugate to an algebraic subgroup of

$$\{\pm 1\} \ltimes \mathbb{G}_m(\bar{\mathbb{Q}})^2 \simeq \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \lambda \end{pmatrix} \mid \alpha, \lambda \in \bar{\mathbb{Q}}, \alpha\lambda \neq 0 \right\} \cup \left\{ \begin{pmatrix} 0 & \beta \\ \epsilon & 0 \end{pmatrix} \mid \beta, \epsilon \in \bar{\mathbb{Q}}, \beta\epsilon \neq 0 \right\}. \quad (4.7)$$

Finally, if $a \neq 0$ and neither (4.3) nor (4.5) admits a solution in k_∞ , then $\mathrm{SL}_2(\bar{\mathbb{Q}}) \subseteq H_\infty$, and we compute H_∞ as in [11, §4.4], by determining the image $\det(H_\infty) \subseteq \mathbb{G}_m(\bar{\mathbb{Q}})$ of the determinant homomorphism.

In order to produce an algorithm that computes the σ -Galois group of (4.1) over $k = k_1$, we need to be more careful in keeping track of which algebraic extension k_n the solutions of the Riccati equations (4.3) and (4.5) belong to, and what effect this has on the shape of the Galois group. We begin by introducing some additional notation and stating some ancillary results. Let $\zeta_n \in \bar{\mathbb{Q}}$ for $n \in \mathbb{N}$ denote a compatible system of n -th roots of unity, so that for any factorization $\ell m = n$ we have $\zeta_n^\ell = \zeta_m$. Then k_n is a σ -PV ring over k_m for $\sigma(y) = q_n y$ with fundamental solution (1×1 matrix) $y = x_n$ and cyclic σ -Galois group $\langle \tau_{n,m} \rangle = \mathrm{Gal}_\sigma(k_n/k_m)$ given by $\tau_{n,m}(x_n) = \zeta_\ell x_n$, where $\ell = n/m$. Let S_∞ denote a σ -PV ring over k_∞ for (4.2) with fundamental solution matrix Y . Then $S_n = k_n[Y, 1/\det(Y)]$ is a σ -PV ring over k_n for (4.2). Let us write $H_n = \mathrm{Gal}_\sigma(S_n/k_n)$ for $n \in \mathbb{N} \cup \{\infty\}$. Then we see that S_n is a σ -PV ring over k_1 for the system

$$\sigma(Y_n) = \begin{pmatrix} 0 & 1 & 0 \\ -b & -a & 0 \\ 0 & 0 & q_n \end{pmatrix} Y_n, \quad \text{with fundamental solution matrix}$$

$$Y_n = \begin{pmatrix} y_1 & y_2 & 0 \\ \sigma(y_1) & \sigma(y_2) & 0 \\ 0 & 0 & x_n \end{pmatrix}.$$

The following result is proved formally along the same lines of [2, Lem. 3.1 and Prop. 3.2] and [3, Lem. 12 and Prop. 13], but we include the full argument here for completeness.

Proposition 4.2. *Let $\tilde{H}_n := \mathrm{Gal}_\sigma(S_n/k_1)$ and μ_n denote the cyclic group of n -th roots of unity. Then the intersection $S_1 \cap k_n = k_m$ for some factorization $n = \ell m$, and the map*

$$\varphi : \tilde{H}_n \rightarrow H_1 \times \mu_n$$

$$\gamma \mapsto (\gamma|_{S_1}, \gamma|_{k_n})$$

is an isomorphism onto the fiber product

$$H_1 \times_{\mu_m} \mu_n = \{(\gamma, \zeta) \mid \gamma \in H_1 \text{ and } \zeta \in \mu_n \text{ such that } \gamma(x_m) = \zeta^\ell x_m\}. \quad (4.8)$$

Proof. Note that $S_1 \cap k_n \subset k_n$ is a k_1 -subalgebra of k_n , and therefore equal to k_m for some m dividing n by classical Galois theory. Since the embedding of $\tilde{H}_n \hookrightarrow \mathrm{GL}_3(\mathbb{Q}) : \gamma \mapsto M_\gamma$ is given by $\gamma(Y_n) = Y_n M_\gamma$ and $Y_n = Y \oplus (x_n)$, we see that if $\gamma|_{S_1}$ and $\gamma|_{k_n}$ are both trivial then so is γ , and therefore the group homomorphism $\varphi(\gamma) = (\gamma|_{S_1}, \gamma|_{k_n})$ is injective. That the image of φ is contained in the fiber product (4.8) is clear: $\gamma(x_n) = \zeta x_n$ for some $\zeta \in \mu_n$, and then $\gamma|_{S_1}(x_m) = \gamma(x_m) = \gamma(x_n^\ell) = \zeta^\ell x_m$. It remains to show that φ surjects onto the fiber product (4.8).

Let L_n and L_1 be the total rings of fractions of S_n and S_1 , respectively (we emphasize that neither L_n nor L_1 is necessarily a field). We still have $L_1 \cap k_n = k_m$, and $H_1 = \mathrm{Gal}_\sigma(L_1/k_1)$ and $\tilde{H}_n = \mathrm{Gal}_\sigma(L_n/k_1)$. Let us write $\mathrm{Gal}_\sigma(L_n/L_1) := \{\gamma \in \tilde{H}_n \mid \gamma|_{L_1} = 1\}$ even if L_1 is not a field. By Theorem 2.9, $\mathrm{Gal}_\sigma(L_n/L_1)$ is a closed subgroup of $\mathrm{Gal}_\sigma(L_n/k)$.

We claim that the map

$$\begin{aligned} \psi : \mathrm{Gal}_\sigma(L_n/k_n) &\rightarrow \mathrm{Gal}_\sigma(L_1/k_m) \\ \gamma &\mapsto \gamma|_{L_1} \end{aligned}$$

is an isomorphism. That the image of ψ is contained in the specified group follows from $L_1 \cap k_n = k_m$. To see that ψ is injective, note that if $\gamma \in \mathrm{Gal}_\sigma(L_n/k_n)$ then $\gamma(x_n) = 1$, and if $\gamma|_{L_1} = 1$ then $\gamma(Y) = Y$, and therefore $\gamma(Y_n) = Y_n$, so $\gamma = 1$. To see that ψ is surjective, note that since the projection ψ is an algebraic group homomorphism and $\mathrm{Gal}_\sigma(L_n/k_n)$ is an algebraic subgroup of $\mathrm{Gal}_\sigma(L_n/k)$, the image $\mathrm{im}(\psi)$ is a (closed) algebraic subgroup of $\mathrm{Gal}_\sigma(L_1/k_m)$. But since $L_1^{\mathrm{im}(\psi)} \subseteq L_1 \cap k_n = k_m$, it follows that $\mathrm{im}(\psi) = \mathrm{Gal}_\sigma(L_1/k_m)$ by Theorem 2.9.

Let us now show that φ surjects onto the fiber product (4.8). Let $(\gamma, \zeta) \in H_1 \times_{\mu_m} \mu_n$, so that $\gamma(x_m) = \zeta^\ell x_m$. There exists $\lambda \in \tilde{H}_n$ such that $\lambda(x_n) = \zeta x_n$, for otherwise $\{\gamma|_{k_n} \mid \gamma \in \tilde{H}_n\}$ would be a proper subgroup of $\mathrm{Gal}(k_n/k_1)$, which is impossible by Theorem 2.9. Then we see that $\gamma' := \gamma \circ \lambda|_{L_1}^{-1} \in \mathrm{Gal}_\sigma(L_1/k_m)$ and therefore there exists $\tilde{\gamma} \in \mathrm{Gal}_\sigma(L_n/k_n)$ such that $\psi(\tilde{\gamma}) = \tilde{\gamma}|_{L_1} = \gamma'$. A computation now shows that $\tilde{\gamma} \circ \lambda \in \tilde{H}_n$ satisfies $(\tilde{\gamma} \circ \lambda)|_{L_1} = \gamma$ and $(\tilde{\gamma} \circ \lambda)(x_n) = \zeta x_n$, and therefore $\varphi(\tilde{\gamma} \circ \lambda) = (\gamma, \zeta)$, as we wanted to show. $\square$

We record the following two consequences of Proposition 4.2.

Corollary 4.3. $S_1 \cap k_n = k_1$ if and only if $H_n \simeq H_1$, and $S_1 \cap k_n = k_n$ if and only if H_n is a normal subgroup of H_1 of index n .

Proof. In any case, H_n is identified with the normal subgroup

$$\{(\gamma, \zeta) \in H_1 \times_{\mu_m} \mu_n \mid \zeta = 1\} \leq \tilde{H}_n,$$

which has index n in $\tilde{H}_n$. In particular, $S_1 \cap k_n = k_1$ if and only if $\tilde{H}_n \simeq H_1 \times \mu_n$ and $H_n \simeq H_1 \times \{1\}$. On the other hand, $S_1 \cap k_n = k_n$ if and only if $\tilde{H}_n \simeq H_1 \times_{\mu_n} \mu_n \simeq H_1$, so H_n is as claimed. $\square$

Corollary 4.4. *The intersection in S_∞ given by $k_\infty \cap S_1 = k_m$ for some $m \in \mathbb{N}$, and $H_\infty \simeq H_{\ell m}$ for every $\ell \in \mathbb{N}$. In particular, H_∞ is a normal subgroup of H_1 of index m .*

Proof. Note that $H_\infty \hookrightarrow H_n$ for every $n \in \mathbb{N}$ via their actions on the same fundamental solution matrix $Y \in \mathrm{GL}_2(S_\infty)$. Since $S_1 = k_1[Y, \det(Y)^{-1}]$ is finitely generated over k_1 , there is a largest $m \in \mathbb{N}$ such that S_1 admits k_m as an intermediate σ - k_1 -subalgebra, and we see that $H_\infty \simeq H_{\ell m}$ for every $\ell \in \mathbb{N}$, and H_∞ is a closed normal subgroup of H_1 of index m . $\square$

Having computed the σ -Galois group H_∞ of (4.1) over k_∞ as in [11], we can then compute the σ -Galois group H_1 of (4.1) over k_1 according to the following possibilities. The explicit computation of H_1 is obtained in each case as a by-product of our computation of the corresponding $\sigma\delta$ -Galois group of (4.1) in the following sections.

Proposition 4.5. *Precisely one of the following possibilities occurs.*

- (1) *There are infinitely many solutions to (4.3) in k_1 . In this case, H_1 is a subgroup of $\mathbb{G}_m(\bar{\mathbb{Q}})$ (included in $\mathrm{GL}_2(\bar{\mathbb{Q}})$ as scalar matrices).*
- (2) *There are exactly two solutions $u_1, u_2 \in k_1$ to (4.3). In this case, H_1 is diagonalizable (but not contained in the group of scalar matrices).*
- (3) *There is exactly one solution $u \in k_1$ to (4.3). In this case, H_1 is reducible but not diagonalizable.*
- (4) *There are no solutions to (4.3) in k_1 , but there are exactly two solutions $u_1, u_2 \in k_2 \setminus k_1$ to (4.3), and $u_2 = \bar{u}_1$ is the Galois conjugate of u_1 over k_1 . In this case, H_1 is irreducible and imprimitive.*
- (5) *There are no solutions to (4.3) in k_2 , and either $a = 0$ or there is a solution $e \in k_2$ to (4.5). In this case, H_1 is irreducible and imprimitive.*
- (6) *There are no solutions to (4.3) nor to (4.5) in k_2 and $a \neq 0$. In this case, H_1 is irreducible and primitive, and $\mathrm{SL}_2(\bar{\mathbb{Q}}) \subseteq H_1$.*

Proof. It is clear that the possibilities above are mutually exclusive. It remains to show that these possibilities are exhaustive, and that the σ -Galois group H_1 is as stated in each case.

Let us first show that these possibilities are exhaustive. By [11, Thm. 13], there are either zero, one, two, or infinitely many solutions to (4.3) in k_∞ . By [11, Thm. 15], if there exists a solution $u \in k_\infty$ to the Riccati equation (4.3), then there exists a solution in k_2 . Since the coefficients $a, b \in k = k_1$, for any solution $u \in k_2 \setminus k_1$ to (4.3) the Galois conjugate $\bar{u} := \tau_{2,1}(u)$ must also satisfy (4.3). Hence, if there is exactly one solution

$u \in k_\infty$ to (4.3), then $u \in k_1$, and if there are exactly two solutions $u_1, u_2 \in k_\infty$ to (4.3), then either $u_1, u_2 \in k_1$, or else $u_1, u_2 \in k_2 \setminus k_1$ and $u_2 = \bar{u}_1$ is the Galois conjugate of u_1 over k_1 . In the case where there are infinitely many solutions to (4.3) in k_∞ , the proof of [11, Thm. 15] shows that at least three of these solutions actually belong to k_1 , in which case the proof of [12, Thm. 4.2] shows that there are infinitely many solutions to (4.3) in k_1 . This shows that cases (1)–(4) exhaust the possibilities where there is at least one solution to (4.3) in k_∞ . Supposing now that there are no solutions to (4.3) in k_∞ and $a \neq 0$, by [11, Thm. 15] we again have that if there exists at least one solution in k_∞ to (4.5), then there exists a solution in k_2 . This concludes the proof that the possibilities listed in Proposition 4.5 are exhaustive and mutually exclusive.

The statements corresponding to the form of the σ -Galois group H_1 will be established separately in the following sections according to the possibilities listed above, depending on the existence of solutions to (4.3) or (4.5) in k_1 or k_2 as discussed above. $\square$

In view of Proposition 2.10, in order to compute the $\sigma\delta$ -group G of (4.1), we will first apply the results of [11] to compute the solutions to (4.3) and/or (4.5) in k_2 , which according to the possibilities in Proposition 4.5 (and as we will show in each case in the following sections) results in knowing whether the corresponding σ -Galois group H is: diagonalizable; reducible (but not diagonalizable); irreducible and imprimitive; or irreducible and primitive. We will then compute the additional δ -algebraic equations that define G as a subgroup of H in each case (and obtain the explicit computation of H itself along the way). In order to apply the theory of [13] to study (4.1), we will consider (4.1) as a difference equation over the larger basefield $C(x)$ mentioned at the beginning of this section, where we recall C is a δ -closed field extension of $(\bar{\mathbb{Q}}, \delta)$ such that $C^\delta = \bar{\mathbb{Q}}$ (the existence of such a C is guaranteed by [14,25]), and the $\sigma\delta$ -structure of $C(x)$ extends that of $\bar{\mathbb{Q}}(x)$: σ is the C -linear automorphism of $C(x)$ defined by $\sigma(x) = qx$.

Remark 4.6 (*Descent from $C(x)$ to $\bar{\mathbb{Q}}(x)$*). The application of the results of [11] and Proposition 4.5 to compute the σ -Galois group of (4.1) over $C(x)$, rather than over $\bar{\mathbb{Q}}(x)$, requires some justification. Although it is possible to see from general Tannakian principles that the σ -Galois group of (4.1) over $C(x)$ is obtained by base change from $\bar{\mathbb{Q}}$ to C of the σ -Galois group of (4.1) over $\bar{\mathbb{Q}}(x)$, it is possible to see this directly in the present situation. The point is that the number of solutions to the Riccati equations (4.3) and (4.5) in $C(x_2)$ is the same as the number of solutions in $\bar{\mathbb{Q}}(x_2)$. This follows from an elementary argument: suppose that a given polynomial σ -equation over $\bar{\mathbb{Q}}(x)$ admits a solution $\frac{p}{q} \in C(x)$, where $p = a_n x^n + \cdots + a_1 x + a_0$ and $q = b_m x^m + \cdots + b_1 x + b_0$. This is equivalent to the coefficients a_i and b_j satisfying $b_m \neq 0$ and a system of polynomial equations defined over $\bar{\mathbb{Q}}$, which defines an affine algebraic variety V over $\bar{\mathbb{Q}}$. Since $\bar{\mathbb{Q}}$ is algebraically closed and C is countable, $V(C)$ and $V(\bar{\mathbb{Q}})$ must have the same cardinality.

Moreover, the possible defining equations for the σ -Galois groups of (4.1) over $\bar{\mathbb{Q}}(x)$ and over $C(x)$, whether in the reducible, irreducible and imprimitive, or irreducible and primitive cases, are all witnessed by monomial relations among (the standard form of)

elements in $\bar{\mathbb{Q}}(x)$. Though we will see this explicitly in each situation in the following sections, it is worthwhile to emphasize now that the σ -Galois group of (4.1) over $C(x)$ consists of the C -points of the σ -Galois group over $\bar{\mathbb{Q}}(x)$, i.e., the former is defined as an algebraic subgroup of $\mathrm{GL}_2(C)$ by the same algebraic equations defining the latter as an algebraic subgroup of $\mathrm{GL}_2(\bar{\mathbb{Q}})$.

On the other hand, the $\sigma\delta$ -Galois group G of (4.1) that we compute in the following sections results, in each case, in defining equations for $G \subseteq \mathrm{GL}_2(C)$ with coefficients in $\bar{\mathbb{Q}}$, and not just in C . The existence of a so-called $\bar{\mathbb{Q}}$ -form of G (which is what we in fact end up computing) can be expected on general theoretical grounds, because the differential Tannakian category generated by the difference module corresponding to (4.1) is defined over $\bar{\mathbb{Q}}(x)$; see [22] for more details. We do not address here the interesting question of to what extent this $\bar{\mathbb{Q}}$ -form of G is unique or algorithm-dependent, but rather content ourselves with computing a set of defining δ -equations for G as a subset of $\mathrm{GL}_2(C)$.

5. Diagonalizable groups

We recall the notation introduced in the previous sections: $k = C(x)$, C is a δ -closure of $\bar{\mathbb{Q}}$ with $C^\delta = \bar{\mathbb{Q}}$, σ denotes the C -linear automorphism of k defined by $\sigma(x) = qx$, and $\delta(x) = x$. Let us first suppose that there exist at least two distinct solutions $u_1, u_2 \in \bar{\mathbb{Q}}(x)$ to the Riccati equation (4.3) as in items (1) or (2) of Proposition 4.5. Then (4.2) is equivalent over $\bar{\mathbb{Q}}(x)$ to

$$\sigma(Y) = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix} Y,$$

in view of the following remark.

Remark 5.1. Given two distinct solutions u_1 and u_2 to (4.3), the gauge transformation (which is different from the one specified in the proof of [12, Thm. 4.2])

$$T := \frac{1}{u_1 - u_2} \cdot \begin{pmatrix} u_2 & -1 \\ u_1 & -1 \end{pmatrix}$$

satisfies $\sigma(T)AT^{-1} = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix}$.

In this case, we compute G with the following result.

Proposition 5.2. Assume that $u_1, u_2 \in \bar{\mathbb{Q}}(x)$ are both different from 0, and let R be the $\sigma\delta$ -PV ring over k corresponding to the system

$$\sigma(Y) = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix} Y. \quad (5.1)$$

Then $G = \mathrm{Gal}_{\sigma\delta}(R/k)$ is the subgroup of

$$\mathbb{G}_m(C)^2 = \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C, \alpha_1 \alpha_2 \neq 0 \right\} \quad (5.2)$$

defined by the following conditions on α_1 and α_2 .

- (i) There exist $m_1, m_2 \in \mathbb{Z}$, not both zero, and $f \in \bar{\mathbb{Q}}(x)^\times$ such that $u_1^{m_1} u_2^{m_2} = \frac{\sigma(f)}{f}$ if and only if $\alpha_1^{m_1} \alpha_2^{m_2} = 1$.
- (ii) There exist $m_1, m_2 \in \mathbb{Z}$, not both zero and with $\gcd(m_1, m_2) = 1$; $c \in \mathbb{Z}$; and $f \in \bar{\mathbb{Q}}(x)$ such that $m_1 \frac{\delta(u_1)}{u_1} + m_2 \frac{\delta(u_2)}{u_2} = \sigma(f) - f + c$ if and only if $\delta(m_1 \frac{\delta(\alpha_1)}{\alpha_1} + m_2 \frac{\delta(\alpha_2)}{\alpha_2}) = 0$. Moreover, $c = 0$ if and only if $\delta(\alpha_1^{m_1} \alpha_2^{m_2}) = 0$.
- (iii) If neither of the conditions above is satisfied, then $G = H = \mathbb{G}_m(C)^2$.

Proof. We begin by observing that, if we can find $f \in k$ witnessing the relations in items (i) or (ii), then we may take $f \in \bar{\mathbb{Q}}(x)$, since $u_i \in \bar{\mathbb{Q}}(x)$ (cf. [10, Lem. 2.4, Lem. 2.5] and Remark 4.6). Note that by Theorem 2.4, $R^\sigma = C$. Let $y_1, y_2 \in R$ be non-zero elements such that $\sigma(y_i) = u_i y_i$. Then $\begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix}$ is a fundamental solution matrix for (5.1), so $y_1, y_2 \in R^\times$ and the embedding of G into (5.2) is given by $\gamma(y_i) = \alpha_{\gamma,i} y_i$ for $i = 1, 2$ and $\gamma \in G$.

The proof of item (i) is standard: given $m_1, m_2 \in \mathbb{Z}$ we have that $\alpha_{\gamma,1}^{m_1} \alpha_{\gamma,2}^{m_2} = 1$ for every $\gamma \in G$ if and only if $\gamma(y_1^{m_1} y_2^{m_2}) = y_1^{m_1} y_2^{m_2}$ for every $\gamma \in G$. By Theorem 2.9, this is equivalent to $y_1^{m_1} y_2^{m_2} = f \in k$, which in turn is equivalent to $\frac{\sigma(f)}{f} = u_1^{m_1} u_2^{m_2}$.

Setting $\frac{\delta(y_i)}{y_i} =: g_i \in R$ for $i = 1, 2$, we see that

$$\sigma(g_i) - g_i = \frac{\delta(u_i)}{u_i} \quad \text{and} \quad \gamma(g_i) = g_i + \frac{\delta(\alpha_{\gamma,i})}{\alpha_{\gamma,i}}. \quad (5.3)$$

By Corollary 3.5, y_1 and y_2 are differentially dependent over k if and only if there exist $m_1, m_2 \in \mathbb{Z}$, not both zero and with $\gcd(m_1, m_2) = 1$, $c \in \mathbb{Z}$, and $f \in k$ such that

$$m_1 \frac{\delta(u_1)}{u_1} + m_2 \frac{\delta(u_2)}{u_2} = \sigma(f) - f + c. \quad (5.4)$$

Hence, if there do not exist such $m_1, m_2, c \in \mathbb{Z}$ and $f \in k$, y_1 and y_2 are δ -independent over k , which implies that $G = \mathbb{G}_m(C)^2$ by [13, Prop. 6.26]. This proves item (iii).

Let us establish item (ii). It follows from (5.3) that for any $m_1, m_2 \in \mathbb{Z}$ we have

$$\begin{aligned} \sigma(m_1 g_1 + m_2 g_2) - (m_1 g_1 + m_2 g_2) &= m_1 \frac{\delta(u_1)}{u_1} + m_2 \frac{\delta(u_2)}{u_2}; \quad \text{and} \\ \gamma(m_1 g_1 + m_2 g_2) &= (m_1 g_1 + m_2 g_2) + m_1 \frac{\delta(\alpha_{\gamma,1})}{\alpha_{\gamma,1}} + m_2 \frac{\delta(\alpha_{\gamma,2})}{\alpha_{\gamma,2}}. \end{aligned}$$

Suppose there exists $f \in k$ satisfying (5.4) with $c = 0$ and $\gcd(m_1, m_2) = 1$. Then $m_1 g_1 + m_2 g_2 - f \in k^\sigma$, which implies that $m_1 g_1 + m_2 g_2 \in k$ and therefore $\delta(\alpha_{\gamma,1}^{m_1} \alpha_{\gamma,2}^{m_2}) = 0$

for every $\gamma \in G$. On the other hand, if $\delta(\alpha_{\gamma,1}^{m_1}\alpha_{\gamma,2}^{m_2}) = 0$ for every $\gamma \in G$ with at least one $m_i \neq 0$, then the same relation holds after replacing m_i with $\frac{m_i}{\gcd(m_1, m_2)}$ and we see that $m_1g_1 + m_2g_2 = f \in k$ satisfies (5.4) with $c = 0$.

More generally, suppose there exist $f \in k$ and $c \in \mathbb{Z}$ satisfying (5.4) with $\gcd(m_1, m_2) = 1$. Then we see that $m_1\delta(g_1) + m_2\delta(g_2) - \delta(f) \in k^\sigma$, and therefore $m_1\delta(g_1) + m_2\delta(g_2) \in k$, which implies that

$$\delta\left(m_1\frac{\delta(\alpha_{\gamma,1})}{\alpha_{\gamma,1}} + m_2\frac{\delta(\alpha_{\gamma,2})}{\alpha_{\gamma,2}}\right) = 0 \quad \text{for every } \gamma \in G. \quad (5.5)$$

On the other hand, assuming (5.5) with at least one $m_i \neq 0$, then the same relation holds after replacing m_i with $\frac{m_i}{\gcd(m_1, m_2)}$, and we have that $m_1\delta(g_1) + m_2\delta(g_2) = g \in k$, and therefore

$$m_1\delta\left(\frac{\delta(u_1)}{u_1}\right) + m_2\delta\left(\frac{\delta(u_2)}{u_2}\right) = \sigma(g) - g.$$

By Proposition 3.3, for each $\beta \in \mathbb{Q}^\times$ we have that

$$0 = q\text{-dres}\left(\delta\left(\frac{\delta(u_1^{m_1}u_2^{m_2})}{u_1^{m_1}u_2^{m_2}}\right), [\beta]_q, 2\right) = -\beta \cdot q\text{-dres}\left(\frac{\delta(u_1^{m_1}u_2^{m_2})}{u_1^{m_1}u_2^{m_2}}, [\beta]_q, 1\right),$$

where the second equality follows from Lemma 3.4. Hence, letting

$$c := q\text{-dres}\left(\frac{\delta(u_1^{m_1}u_2^{m_2})}{u_1^{m_1}u_2^{m_2}}, \infty\right) = m_1 \cdot q\text{-dres}\left(\frac{\delta(u_1)}{u_1}, \infty\right) + m_2 \cdot q\text{-dres}\left(\frac{\delta(u_2)}{u_2}, \infty\right), \quad (5.6)$$

we have that $c \in \mathbb{Z}$ and every q -discrete residue of $m_1\frac{\delta(u_1)}{u_1} + m_2\frac{\delta(u_2)}{u_2} - c$ is 0. By another application of Proposition 3.3, there exists $f \in k$ satisfying (5.4) with c as in (5.6). $\square$

Remark 5.3. To compute the difference-differential Galois group G for (4.1) when there exist at least two distinct solutions $u_1, u_2 \in \mathbb{Q}(x)$ to the Riccati equation (4.3), we apply Proposition 5.2 as follows. First, compute the q -discrete residues $r_i([\beta]_q) := q\text{-dres}\left(\frac{\delta(u_i)}{u_i}, [\beta]_q, 1\right)$ at each $q^\mathbb{Z}$ -orbit $[\beta]_q$ for $\beta \in \bar{\mathbb{Q}}^\times$ as in Definition 3.2 (note these will be zero for any β that is neither a zero nor a pole of u_1 or u_2). Then decide whether there exist relatively prime $m_1, m_2 \in \mathbb{Z}$ such that $m_1r_1([\beta]_q) + m_2r_2([\beta]_q) = 0$ for every $q^\mathbb{Z}$ -orbit $[\beta]_q$ simultaneously (in general this will be an overdetermined linear system over $\bar{\mathbb{Q}}$, so the task is to decide whether there exists a non-zero solution in $\bar{\mathbb{Q}}^2$ and then whether such a solution can be taken to be in $\mathbb{Z}^2$). For any such pair $(0, 0) \neq (m_1, m_2) \in \mathbb{Z}^2$, taking $c \in \mathbb{Z}$ as in (5.6) the proof of Proposition 5.2 shows that there exists $f \in \bar{\mathbb{Q}}(x)$ satisfying (5.4); it is not necessary to determine what the certificate f actually is.

The $\mathbb{Z}$ -module M generated by all pairs $(m_1, m_2) \in \mathbb{Z}^2$ as in Proposition 5.2(ii) is free of rank $r \leq 2$. It follows from the proof of Corollary 3.5 that $\mathbb{Z}^2/M$ is torsion-free, and therefore also free of rank $2 - r$, since if $(dm_1, dm_2) \in M$ for any $0 \neq d \in \mathbb{Z}$, then

$(m_1, m_2) \in M$ also. Thus, if the rank of M is $r = 2$ then $M = \mathbb{Z}^2$. It follows that the defining equations for G arising from Proposition 5.2(ii) are given by either: a single pair (m_1, m_2) , unique up to multiplication by ± 1 and with the form of the defining equation determined by whether the corresponding value of c in (5.6) is 0; or else the two relations corresponding to $(1, 0)$ and $(0, 1)$, with an additional relation occurring only in case $c_i := q\text{-dres}(\frac{\delta(u_i)}{u_i}, \infty) \neq 0$ for both $i = 1, 2$, in which case we obtain an additional relation given by $\delta(\alpha_1^{d_1} \alpha_2^{\varepsilon d_2}) = 0$ with

$$d_i := \frac{\text{lcm}(|c_1|, |c_2|)}{c_i} \quad \text{and} \quad \varepsilon = \begin{cases} 1 & \text{if } c_1 c_2 \in \mathbb{Z}_{<0}; \\ -1 & \text{if } c_1 c_2 \in \mathbb{Z}_{>0}. \end{cases} \quad (5.7)$$

Having computed all possible relations arising from Proposition 5.2(ii), let us now show how to find the possible relations arising from Proposition 5.2(i), and thus determine all defining equations for $G \subseteq \mathbb{G}_m(C)^2$. We still denote by $M \subseteq \mathbb{Z}^2$ the $\mathbb{Z}$ -submodule generated by pairs (m_1, m_2) as in Proposition 5.2. If $M = \{(0, 0)\}$ then $G = \mathbb{G}_m(C)^2$ as in Proposition 5.2(iii), so from now on we assume M is not trivial. We saw above that either $M = \mathbb{Z}^2$ or else $M = \mathbb{Z} \cdot (m_1, m_2)$ with $\gcd(m_1, m_2) = 1$.

Suppose $M = \mathbb{Z} \cdot (m_1, m_2)$. If the value of c given in (5.6) is not 0, then G is defined by the single equation $\delta\left(\frac{\delta(\alpha_1^{m_1} \alpha_2^{m_2})}{\alpha_1^{m_1} \alpha_2^{m_2}}\right) = 0$ as in Proposition 5.2(ii). On the other hand, if this $c = 0$, then we must decide whether there exist: a primitive n -th root of unity ζ_n , integers r, s such that $0 \leq r < s$ and $\gcd(r, s) = 1$, and $g \in \mathbb{Q}(x)^\times$ such that $u_1^{m_1} u_2^{m_2} = \zeta_n q_s^r \frac{\sigma(g)}{g}$. If so, then G is defined by the single equation $(\alpha_1^{m_1} \alpha_2^{m_2})^\ell = 1$ as in Proposition 5.2(i), where $\ell := \text{lcm}(n, s)$, the least common multiple of n and s ; otherwise, $\alpha_1^{m_1} \alpha_2^{m_2}$ has infinite order in $\mathbb{G}_m(C^\delta)$ for every $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in G$, and G is defined by the single equation $\delta(\alpha_1^{m_1} \alpha_2^{m_2}) = 0$ as in Proposition 5.2(ii) only.

If $M = \mathbb{Z}^2$, let again $c_i := q\text{-dres}(\frac{\delta(u_i)}{u_i}, \infty)$. If exactly one c_i is 0, say $c_1 = 0 \neq c_2$, then we must decide whether there exist: a primitive n -th root of unity ζ_n , integers r, s such that $0 \leq r < s$ and $\gcd(r, s) = 1$, and $g \in \bar{\mathbb{Q}}(x)^\times$ such that $u_1 = \zeta_n q_s^r \frac{\sigma(g)}{g}$. If so, then G is defined by the equations: $\alpha_1^\ell = 1$ as in Proposition 5.2(i), with $\ell := \text{lcm}(n, s)$, and $\delta\left(\frac{\delta(\alpha_2)}{\alpha_2}\right) = 0$ as in Proposition 5.2(ii); otherwise, G is defined instead by $\delta(\alpha_1) = 0$ and $\delta\left(\frac{\delta(\alpha_2)}{\alpha_2}\right) = 0$. The case where $c_2 = 0 \neq c_1$ is analogous. If $c_1, c_2 \neq 0$, then we must decide whether there exist: a primitive n -th root of unity ζ_n , integers r, s such that $0 \leq r < s$ and $\gcd(r, s) = 1$, and $g \in \bar{\mathbb{Q}}(x)^\times$ such that $u_1^{d_1} u_2^{\varepsilon d_2} = \zeta_n q_s^r \frac{\sigma(g)}{g}$, with d_1, d_2, ε defined as in (5.7). If so, then G is defined by the equations $\delta\left(\frac{\delta(\alpha_i)}{\alpha_i}\right) = 0$ for $i = 1, 2$ as in Proposition 5.2(ii), together with $(\alpha_1^{d_1} \alpha_2^{\varepsilon d_2})^\ell = 1$ as in Proposition 5.2(i), where $\ell := \text{lcm}(n, s)$; otherwise, G is defined by $\delta\left(\frac{\delta(\alpha_i)}{\alpha_i}\right) = 0$ for $i = 1, 2$ only.

The case where $M = \mathbb{Z}^2$ and $c_i := q\text{-dres}(\frac{\delta(u_i)}{u_i}, \infty) = 0$ for both $i = 1, 2$ is similar in principle: we must decide whether there exist $m_1, m_2 \in \mathbb{Z}$, a primitive n -th root of unity ζ_n , integers r, s such that $0 \leq r < s$ and $\gcd(r, s) = 1$, and $g \in \bar{\mathbb{Q}}(x)^\times$ such that $u_1^{m_1} u_2^{m_2} = \zeta_n q_s^r \frac{\sigma(g)}{g}$. If so, then G is defined by $\delta(\alpha_i) = 0$ for $i = 1, 2$ as in

Proposition 5.2(ii), together with $(\alpha_1^{m_1} \alpha_2^{m_2})^\ell = 1$ as in Proposition 5.2(i), where $\ell := \text{lcm}(n, s)$; otherwise, G is defined by $\delta(\alpha_i) = 0$ for $i = 1, 2$ only.

The problem of deciding whether $u := u_1^{m_1} u_2^{m_2} = \zeta_n q_s^r \frac{\sigma(g)}{g}$ as above for a given *single* pair (m_1, m_2) is addressed in [11, §3]: a straightforward modification of the algorithm given there allows us to compute a *reduced form* $\tilde{u} = h x^n \frac{p}{q}$ where: $h \in \bar{\mathbb{Q}}^\times$; $n \in \mathbb{Z}$; $p, q \in \bar{\mathbb{Q}}[x]$ are monic such that $\gcd(p, \sigma^m(q)) = 1$ for every $m \in \mathbb{Z}$; if $h = \zeta q^t$ for some root of unity ζ and $t \in \mathbb{Q}$, then $0 \leq t < 1$; and such that there exists $g \in \bar{\mathbb{Q}}(x)^\times$ with $u = \tilde{u} \frac{\sigma(g)}{g}$ for some $g \in \bar{\mathbb{Q}}(x)^\times$. Thus we only need to check whether $\tilde{u} = \zeta_n q_s^r$.

In the case where $M = \mathbb{Z}^2$ and $c_i := q\text{-dres}(\frac{\delta(u_i)}{u_i}, \infty) = 0$ for both $i = 1, 2$, one can show that the standard form $\tilde{u}_i = h_i$ with $h_i \in \bar{\mathbb{Q}}^\times$, and one needs to decide whether h_1 and h_2 are multiplicatively independent modulo $q^\mathbb{Z}$. We do not know how to produce *a priori* bounds on the possible coefficients (m_1, m_2) such that $h_1^{m_1} h_2^{m_2} \in q^\mathbb{Z}$ in general, so in this case only we offer no improvements on the algorithm in [11, §4.2]. But in the remaining cases, we have reduced the computation of all the possible relations in Proposition 5.2(i) to checking a finite list of possibilities for $(m_1, m_2) \in \mathbb{Z}^2$, although this requires the ability to compute the q -discrete residues of $\frac{\delta(u_i)}{u_i}$ (cf. [26, §2.2]).

6. Reducible non-diagonalizable groups

We recall the notation introduced in the previous sections: $k = C(x)$, where C is a δ -closure of $\bar{\mathbb{Q}}$, σ denotes the C -linear automorphism of k defined by $\sigma(x) = qx$, and $\delta(x) = x$.

We now proceed to define the additional notation that we will use throughout this section. We will assume that there exists exactly one solution $u \in \bar{\mathbb{Q}}(x)$ to the Riccati equation (4.3), so that the σ -Galois group H for (4.1) is reducible but not diagonalizable as in Proposition 4.5(3), and the difference operator implicit in (4.1) factors as

$$\sigma^2 + a\sigma + b = (\sigma - \frac{b}{u}) \circ (\sigma - u),$$

as we saw in §4. This means that there is a C -basis of solutions $\{y_1, y_2\}$ in any $\sigma\delta$ -PV ring R for (4.1) such that $y_1, y_2 \neq 0$ satisfy $\sigma(y_1) = uy_1$ and $\sigma(y_2) - uy_2 = y_0$, where $y_0 \neq 0$ satisfies $\sigma(y_0) = \frac{b}{u}y_0$. A fundamental solution matrix for (4.2) is given by

$$\begin{pmatrix} y_1 & y_2 \\ \sigma(y_1) & \sigma(y_2) \end{pmatrix} = \begin{pmatrix} y_1 & y_2 \\ uy_1 & uy_2 + y_0 \end{pmatrix}. \quad (6.1)$$

If we now let $A = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}$, $T = \begin{pmatrix} 1-u & 1 \\ -u & 1 \end{pmatrix}$, and $v = \frac{b}{u} = -\sigma(u) - a$ (since u satisfies (4.3)), we have that

$$\sigma(T)AT^{-1} = \begin{pmatrix} 1-\sigma(u) & 1 \\ -\sigma(u) & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \begin{pmatrix} 1 & -1 \\ u & 1-u \end{pmatrix} = \begin{pmatrix} u & 1-u+v \\ 0 & v \end{pmatrix} =: B.$$

Therefore, the systems (4.2) and $\sigma(Z) = BZ$ are equivalent (in the sense of Definition 2.6), and a fundamental solution matrix for the latter system is given by

$$TY = \begin{pmatrix} 1-u & 1 \\ -u & 1 \end{pmatrix} \begin{pmatrix} y_1 & y_2 \\ uy_1 & uy_2 + y_0 \end{pmatrix} = \begin{pmatrix} y_1 & y_2 + y_0 \\ 0 & y_0 \end{pmatrix} = Z.$$

For any $\gamma \in H$, the σ -Galois group for (4.1), we have that

$$\gamma \begin{pmatrix} y_1 & y_2 + y_0 \\ 0 & y_0 \end{pmatrix} = \begin{pmatrix} y_1 & y_2 + y_0 \\ 0 & y_0 \end{pmatrix} \begin{pmatrix} \alpha_\gamma & \xi_\gamma \\ 0 & \lambda_\gamma \end{pmatrix} = \begin{pmatrix} \alpha_\gamma y_1 & \xi_\gamma y_1 + \lambda_\gamma y_2 + \lambda_\gamma y_0 \\ 0 & \lambda_\gamma y_0 \end{pmatrix}, \quad (6.2)$$

and therefore the action of H on the solutions is defined by

$$\gamma(y_1) = \alpha_\gamma y_1; \quad \gamma(y_0) = \lambda_\gamma y_0; \quad \text{and} \quad \gamma(y_2) = \lambda_\gamma y_2 + \xi_\gamma y_1. \quad (6.3)$$

It will be convenient to define the auxiliary elements

$$w = \frac{y_0}{uy_1} \quad \text{and} \quad z = \frac{y_2}{y_1}, \quad (6.4)$$

on which σ acts via

$$\sigma(w) = \frac{b}{u\sigma(u)}w; \quad \sigma(z) = z + w, \quad (6.5)$$

and H acts via

$$\gamma(w) = \frac{\lambda_\gamma}{\alpha_\gamma}w; \quad \gamma(z) = \frac{\lambda_\gamma}{\alpha_\gamma}z + \frac{\xi_\gamma}{\alpha_\gamma}. \quad (6.6)$$

We observe that the σ -PV ring

$$S = k[y_1, y_2 + y_0, y_0, (y_1 y_0)^{-1}] = k[y_1, w, z, (y_1 w)^{-1}]$$

and the $\sigma\delta$ -PV ring

$$R = k\{y_1, y_2 + y_0, y_0, (y_1 y_0)^{-1}\}_\delta = k\{y_1, w, z, (y_1 w)^{-1}\}_\delta.$$

Our computation of the $\sigma\delta$ -Galois group G for (4.1) in this section will be accomplished by studying the action of G on y_1 , w , and z . We begin by defining the *unipotent radicals*

$$R_u(H) = H \cap \left\{ \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \mid \xi \in C \right\} \quad \text{and} \quad R_u(G) = G \cap \left\{ \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \mid \xi \in C \right\}, \quad (6.7)$$

and observe that $R_u(H)$ (resp., $R_u(G)$) is an algebraic (resp., differential algebraic) subgroup of $\mathbb{G}_a(C)$, the additive group of C . By [11, Thm. 13(2)], $R_u(H) = \mathbb{G}_a(C)$ if and only if there exists exactly one solution $u \in k$ to (4.3). We observe that

$$R_u(G) = \{\gamma \in G \mid \gamma(y_i) = y_i \text{ for } i = 0, 1\}.$$

The reductive quotient

$$G/R_u(G) \simeq \left\{ \begin{pmatrix} \alpha_\gamma & 0 \\ 0 & \lambda_\gamma \end{pmatrix} \mid \gamma \in G \right\}$$

is the $\sigma\delta$ -Galois group corresponding to the matrix equation

$$\sigma(Y) = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} Y, \quad (6.8)$$

which we compute with Proposition 5.2 and Remark 5.3.

In the following result, we compute the defining equations for the $\sigma\delta$ -Galois group G for (4.1) in a special case. Recall that $u \in \bar{\mathbb{Q}}(x)$ denotes the unique solution to the Riccati equation (4.3), H denotes the σ -Galois group for (4.1), and w is as in (6.4).

Proposition 6.1. *Suppose there is exactly one solution $u \in k$ to (4.3) and H is commutative. Then H is a subgroup of*

$$\mathbb{G}_m(C) \times \mathbb{G}_a(C) = \left\{ \begin{pmatrix} \alpha & \xi \\ 0 & \alpha \end{pmatrix} \mid \alpha, \xi \in C, \alpha \neq 0 \right\} \quad (6.9)$$

with $R_u(H) = \mathbb{G}_a(C)$. Moreover, there exists $w \in \bar{\mathbb{Q}}(x)$ satisfying (6.5), and G is the subgroup of (6.9) defined by the following conditions on α and ξ .

- (i) There exist $m \in \mathbb{N}$ and $f \in \bar{\mathbb{Q}}(x)^\times$ such that $u^m = \frac{\sigma(f)}{f}$ if and only if $\alpha^m = 1$.
- (ii) There exist $c \in \mathbb{Z}$ and $f \in \bar{\mathbb{Q}}(x)$ such that $\frac{\delta(u)}{u} = \sigma(f) - f + c$ if and only if $\delta\left(\frac{\delta(\alpha)}{\alpha}\right) = 0$. Moreover, $c = 0$ if and only if $\delta(\alpha) = 0$.
- (iii) There exist: $c \in \bar{\mathbb{Q}}$; $f \in \bar{\mathbb{Q}}(x)$; and a homogeneous linear δ -polynomial $\mathcal{L} \in \bar{\mathbb{Q}}\{Y\}_\delta$ such that $\mathcal{L}\left(\frac{\delta(u)}{u}\right) - w = \sigma(f) - f + c$ if and only if $\delta\left(\frac{\xi}{\alpha}\right) = \mathcal{L}\left(\delta\left(\frac{\delta(\alpha)}{\alpha}\right)\right)$. Moreover, $c = 0$ if and only if $\xi = \alpha\mathcal{L}\left(\frac{\delta(\alpha)}{\alpha}\right)$.
- (iv) If none of the conditions above is satisfied, then $G = H = \mathbb{G}_m(C) \times \mathbb{G}_a(C)$.

Proof. First recall that when there is exactly one solution $u \in k$ to (4.3) the σ -Galois group H of (4.1) is reducible but not diagonalizable by [11, Thm. 13], and therefore H is a non-diagonalizable subgroup of

$$\mathbb{G}_m(C) \ltimes \mathbb{G}_a(C) = \left\{ \begin{pmatrix} \alpha & \xi \\ 0 & \lambda \end{pmatrix} \mid \alpha, \xi, \lambda \in C, \alpha\lambda \neq 0 \right\}.$$

In particular, $R_u(H) = \mathbb{G}_a(C)$ and a straightforward computation shows that H is commutative if and only if it is actually a subgroup of (6.9). We recall the notation

introduced at the beginning of this section: $v = \frac{b}{u}$, $\{y_1, y_2\}$ is a C -basis of solutions for (4.1) such that $\sigma(y_1) = uy_1$ and $\sigma(y_2) - uy_2 = y_0$, where $y_0 \neq 0$ satisfies $\sigma(y_0) = vy_0$. The embedding $H \hookrightarrow \text{GL}_2(C) : \gamma \mapsto M_\gamma$ is as in (6.2), and the action of H on the solutions is given in (6.3). The auxiliary elements w and z are defined as in (6.4); they are acted upon by σ as in (6.5) and by H as in (6.6). The relation $\gamma(w) = \frac{\lambda_\gamma}{\alpha_\gamma} w$ for each $\gamma \in H$ from (6.6), together with Theorem 2.9, imply that $w \in k$. Since $\sigma(w) = \frac{b}{u\sigma(u)} w$ from (6.5) and $b, u \in \bar{\mathbb{Q}}(x)$, if $w \in k$ we may actually take $w \in \bar{\mathbb{Q}}(x)$ by [10, Lem. 2.5] (cf. Remark 4.6). Thus, if we can find $f \in k$ witnessing the relations in items (i) or (ii), then we may take $f \in \bar{\mathbb{Q}}(x)$, as already discussed in the proof of Proposition 5.2, and similarly if we can find $f \in k$ and $c \in C$ witnessing the relation in item (iii), then we may take $f \in \bar{\mathbb{Q}}(x)$ and $c \in \bar{\mathbb{Q}}$.

Items (i) and (ii) were already established in Proposition 5.2. Let us prove item (iii). Setting $\frac{\delta(y_1)}{y_1} =: g \in R$ we have that

$$\sigma(g) - g = \frac{\delta(u)}{u} \quad \text{and} \quad \gamma(g) = g + \frac{\delta(\alpha_\gamma)}{\alpha_\gamma} \quad (6.10)$$

for $\gamma \in G$ (cf. the proof of Proposition 5.2). On the other hand, the actions of σ and $\gamma \in G$ on the element $z \in R$ defined in (6.4) in this case is given by

$$\sigma(z) - z = w \quad \text{and} \quad \gamma(z) = z + \frac{\xi_\gamma}{\alpha_\gamma}. \quad (6.11)$$

Consider the relation stipulated in item (iii):

$$\mathcal{L}\left(\frac{\delta(u)}{u}\right) - w = \sigma(f) - f + c, \quad (6.12)$$

where $\mathcal{L} \in \bar{\mathbb{Q}}\{Y\}_\delta$ is a linear differential polynomial, $f \in \bar{\mathbb{Q}}(x)$, and $c \in \bar{\mathbb{Q}}$. It follows from (6.10) and (6.11) that, for any homogeneous linear differential polynomial $\mathcal{L} \in C\{Y\}_\delta$ and $\gamma \in G$, we have that

$$\begin{aligned} \sigma(\mathcal{L}(g) - z) - (\mathcal{L}(g) - z) &= \mathcal{L}\left(\frac{\delta(u)}{u}\right) - w; \quad \text{and} \\ \gamma(\mathcal{L}(g) - z) &= (\mathcal{L}(g) - z) + \mathcal{L}\left(\frac{\delta(\alpha_\gamma)}{\alpha_\gamma}\right) - \frac{\xi_\gamma}{\alpha_\gamma}. \end{aligned}$$

Suppose there exist $f \in \bar{\mathbb{Q}}(x)$ and a homogeneous linear differential polynomial $\mathcal{L} \in \bar{\mathbb{Q}}\{Y\}_\delta$ satisfying (6.12) with $c = 0$. Then $\mathcal{L}(g) - z - f \in k^\sigma$, which implies that $\mathcal{L}(g) - z \in k$, and therefore $\mathcal{L}\left(\frac{\delta(\alpha_\gamma)}{\alpha_\gamma}\right) = \frac{\xi_\gamma}{\alpha_\gamma}$ for every $\gamma \in G$ by Theorem 2.9. On the other hand, if $\mathcal{L} \in \bar{\mathbb{Q}}\{Y\}_\delta$ is a linear differential polynomial such that $\mathcal{L}\left(\frac{\delta(\alpha_\gamma)}{\alpha_\gamma}\right) = \frac{\xi_\gamma}{\alpha_\gamma}$ for every $\gamma \in G$, then $\mathcal{L}(g) - z = f \in k$ satisfies (6.12) with $c = 0$.

More generally, suppose there exist $f \in \bar{\mathbb{Q}}(x)$, $c \in \bar{\mathbb{Q}}$, and a homogeneous linear differential polynomial $\mathcal{L} \in \bar{\mathbb{Q}}\{Y\}_\delta$ satisfying (6.12). Then we see that $\mathcal{L}(\delta(g)) - \delta(z) - \delta(f) \in k_\sigma$, and therefore $\mathcal{L}(\delta(g)) - \delta(z) \in k$, which implies that

$$\mathcal{L}\left(\delta\left(\frac{\delta(\alpha_\gamma)}{\alpha_\gamma}\right)\right) = \delta\left(\frac{\xi_\gamma}{\alpha_\gamma}\right) \quad (6.13)$$

for every $\gamma \in G$. On the other hand, if $\mathcal{L} \in \bar{\mathbb{Q}}\{Y\}_\delta$ is a homogeneous linear differential polynomial such that (6.13) holds for every $\gamma \in G$, then $\mathcal{L}(\delta(g)) - \delta(g) =: h \in k$, and therefore the element $\mathcal{L}(g) - z \in R$ is differentially dependent over k . It then follows from [13, Prop. 3.10(2.a)] that there exist $f \in k$ and $c \in C^\delta = \bar{\mathbb{Q}}$ satisfying (6.12). This concludes the proof of item (iii).

By [13, Cor. 3.2], g and z are differentially dependent over k if and only if there exist homogeneous linear differential polynomials $\mathcal{L}_1, \mathcal{L}_2 \in \bar{\mathbb{Q}}\{Y\}_\delta$, not both zero, and $\tilde{f} \in \bar{\mathbb{Q}}(x)$, such that

$$\mathcal{L}_1\left(\frac{\delta(u)}{u}\right) - \mathcal{L}_2(w) = \sigma(\tilde{f}) - \tilde{f}. \quad (6.14)$$

Hence if there do not exist such $\mathcal{L}_i$ and $\tilde{f}$, the elements $g, z \in R$ are differentially independent over k , which implies that $G = \mathbb{G}_m(C) \ltimes \mathbb{G}_a(C)$ by [13, Prop. 6.26]. Thus, assume there do exist $\mathcal{L}_1, \mathcal{L}_2 \in \bar{\mathbb{Q}}\{Y\}_\delta$, not both zero, and $\tilde{f}$ satisfying (6.14). If $\mathcal{L}_2 = 0$, then $\mathcal{L}_1 \neq 0$ and it follows from (6.14) and (6.10) that g is differentially dependent over k , and therefore so is y_1 . By Corollary 3.5, this implies that there exist $f \in \bar{\mathbb{Q}}(x)$ and $c \in \mathbb{Z}$ such that $\frac{\delta(u)}{u} = \sigma(f) - f + c$, as in item (ii). To prove item (iv), let us show that if there exist homogeneous linear differential polynomials $\mathcal{L}_1, \mathcal{L}_2 \in \bar{\mathbb{Q}}\{Y\}_\delta$ with $\mathcal{L}_2 \neq 0$ and $\tilde{f} \in \bar{\mathbb{Q}}(x)$ satisfying (6.14), then we can construct a linear δ -polynomial $\mathcal{L} \in \bar{\mathbb{Q}}\{Y\}_\delta$ and $c \in \bar{\mathbb{Q}}$ such that

$$\mathcal{L}\left(\frac{\delta(u)}{u}\right) - w = \sigma(f) - f + c \quad \text{for some } f \in \bar{\mathbb{Q}}(x),$$

as in item (iii). Let $\text{ord}(\mathcal{L}_i) = m_i$ and $\mathcal{L}_i = \sum_{j=0}^{m_i} c_{i,j} \delta^j(Y)$ for $i = 1, 2$; if $\mathcal{L}_1 = 0$, we set $m_1 = 0$, and we adopt the convention that $c_{i,j} := 0$ for every $j > m_i$. By Proposition 3.3, the existence of $\tilde{f} \in k$ as in (6.14) implies that

$$0 = q\text{-dres}\left(\mathcal{L}_1\left(\frac{\delta(u)}{u}\right) - \mathcal{L}_2(w), [\beta]_q, j\right) \quad (6.15)$$

for every $q^{\mathbb{Z}}$ -orbit $[\beta]_q$ with $\beta \in \bar{\mathbb{Q}}^\times$ and every $j \in \mathbb{N}$. Let $r \in \mathbb{N}$ be the largest order such that

$$q\text{-dres}(w, [\beta]_q, r) \neq 0 \quad \text{for some } q^{\mathbb{Z}}\text{-orbit } [\beta]_q.$$

Then it follows from (6.15) and Lemma 3.4 that, for each $q^{\mathbb{Z}}$ -orbit $[\beta]_q$ with $\beta \in \bar{\mathbb{Q}}^\times$, the q -discrete residues

$$\begin{aligned} c_{1,m_2+r-1}(-1)^{m_2+r-1}(m_2+r-1)!\beta^{m_2+r-1}q\text{-dres}\left(\frac{\delta(u)}{u}, [\beta]_q, 1\right) \\ = q\text{-dres}\left(\mathcal{L}_1\left(\frac{\delta(u)}{u}\right), [\beta]_q, m_2+r\right) \end{aligned}$$

and

$$c_{2,m_2}(-1)^{m_2}\frac{(m_2+r)!}{(r-1)!}\beta^{r-1}q\text{-dres}(w, [\beta]_q, r) = q\text{-dres}(\mathcal{L}_2(w), [\beta]_q, m_2+r)$$

are equal. Since $\beta \neq 0$, the above equality is equivalent to

$$\frac{c_{1,m_2+r-1}}{c_{2,m_2}}(-1)^{r-1}(r-1)!\beta^{r-1}q\text{-dres}\left(\frac{\delta(u)}{u}, [\beta]_q, 1\right) = q\text{-dres}(w, [\beta]_q, r) \quad (6.16)$$

Set $c_{r-1} = \frac{c_{1,m_2+r-1}}{c_{2,m_2}}$. Then (6.16) is equivalent to

$$q\text{-dres}\left(c_{r-1}\delta^{r-1}\left(\frac{\delta(u)}{u}\right) - w, [\beta]_q, r\right) = 0$$

for every $q^{\mathbb{Z}}$ -orbit $[\beta]_q$ with $\beta \in \bar{\mathbb{Q}}^\times$ simultaneously. We continue by taking the next highest $r' \leq r-1$ such that $q\text{-dres}(w, [\beta]_q, r') \neq 0$ for some $[\beta]_q$, and proceed as above to find the coefficient $c_{r'-1} \in \bar{\mathbb{Q}}$ of $\mathcal{L}$ such that

$$q\text{-dres}\left(c_{r-1}\delta^{r-1}\left(\frac{\delta(u)}{u}\right) + c_{r'-1}\delta^{r'-1}\left(\frac{\delta(u)}{u}\right) - w, [\beta]_q, j\right) = 0$$

for every $j \geq r'$ and every $q^{\mathbb{Z}}$ -orbit $[\beta]_q$ with $\beta \in \bar{\mathbb{Q}}^\times$ simultaneously. Eventually we will have constructed a homogeneous linear δ -polynomial $\mathcal{L} \in \bar{\mathbb{Q}}\{Y\}_\delta$ such that

$$q\text{-dres}\left(\mathcal{L}\left(\frac{\delta(u)}{u}\right) - w, [\beta]_q, j\right) = 0$$

for every $q^{\mathbb{Z}}$ -orbit $[\beta]_q$ with $\beta \in \bar{\mathbb{Q}}^\times$ and every $j \in \mathbb{N}$. Set $c = q\text{-dres}\left(\mathcal{L}\left(\frac{\delta(u)}{u}\right) - w, \infty\right) \in \bar{\mathbb{Q}}$. Then it follows from Proposition 3.3 that $\mathcal{L}\left(\frac{\delta(u)}{u}\right) - w - c = \sigma(f) - f$ for some $f \in k$. By [10, Lem. 2.4] (cf. Remark 4.6), we may take $f \in \bar{\mathbb{Q}}(x)$, so we are indeed in case (iii), as we wanted to show. $\square$

The main ideas for the proof of the following result were communicated to the first author by Singer in [23], during the development of the algorithm in [4].

Proposition 6.2. *Suppose there exists exactly one solution $u \in \bar{\mathbb{Q}}(x)$ to (4.3) and H is not commutative. Then $R_u(G) = R_u(H) = \mathbb{G}_a(C)$.*

Proof. We recall the notation introduced at the beginning of this section: $u \in \bar{\mathbb{Q}}(x)$ is the unique solution in k to the Riccati equation (4.3), $v = \frac{b}{u}$, $\{y_1, y_2\}$ is a C -basis of solutions for (4.1) such that $\sigma(y_1) = uy_1$ and $\sigma(y_2) - uy_2 = y_0$, where $y_0 \neq 0$ satisfies $\sigma(y_0) = vy_0$. The embedding $G \hookrightarrow \mathrm{GL}_2(C) : \gamma \mapsto M_\gamma$ is as in (6.2), and the action of G on the solutions is given in (6.3). The auxiliary elements w and z are defined as in (6.4); they are acted upon by σ as in (6.5) and by G as in (6.6).

By [7, Prop. 11], either $R_u(G) = \mathbb{G}_a(C)$, or else

$$R_u(G) = \left\{ \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \mid \beta \in C, \mathcal{L}(\xi) = 0 \right\}, \quad (6.17)$$

for some nonzero monic homogeneous linear δ -polynomial $\mathcal{L} \in C\{Y\}_\delta$. Since $R_u(G)$ is normal in G , this implies that (cf. [13, Lem. 3.6])

$$\begin{aligned} M_\gamma \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} M_\gamma^{-1} &= \begin{pmatrix} \alpha_\gamma & \xi_\gamma \\ 0 & \lambda_\gamma \end{pmatrix} \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_\gamma^{-1} & -\alpha_\gamma^{-1} \lambda_\gamma^{-1} \xi_\gamma \\ 0 & \lambda_\gamma^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \alpha_\gamma \lambda_\gamma^{-1} \xi \\ 0 & 1 \end{pmatrix} \in R_u(G) \end{aligned}$$

for each $\gamma \in G$ and $\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \in R_u(G)$. If $\mathcal{L}$ is as in (6.17), then $\mathcal{L}(\xi) = 0 \Rightarrow \mathcal{L}(\alpha_\gamma \lambda_\gamma^{-1} \xi) = 0$. By [13, Lem. 3.7], this implies that if $\mathrm{ord}(\mathcal{L}) \neq 0$, then $\delta(\alpha_\gamma \lambda_\gamma^{-1}) = 0$ for every $\gamma \in G$. But since $\mathcal{L} \neq 0$, $\mathrm{ord}(\mathcal{L}) = 0$ if and only if $R_u(G) = \{0\}$, which is impossible, for then we would have that

$$G \simeq G/R_u(G) \simeq \left\{ \begin{pmatrix} \alpha_\gamma & 0 \\ 0 & \lambda_\gamma \end{pmatrix} \mid \gamma \in G \right\}$$

is commutative, and since G is Zariski-dense in H by Proposition 2.10, this would force H to be commutative also, contradicting our hypotheses.

We proceed by contradiction: assuming $R_u(G) \neq \mathbb{G}_a(C)$, we will show that $R_u(H) = \{0\}$, contradicting our hypotheses. We have shown above that if $R_u(G) \neq \{0\}$ then there exists a monic homogeneous linear δ -polynomial $\mathcal{L} \in C\{Y\}_\delta$ with $\mathrm{ord}(\mathcal{L}) \geq 1$ such that $R_u(G)$ is as in (6.17) and $\delta\left(\frac{\alpha_\gamma}{\lambda_\gamma}\right) = 0$ for every $\gamma \in G$. It follows from (6.6) and Theorem 2.9 that the group $\{\lambda_\gamma \alpha_\gamma^{-1} \mid \gamma \in G\} \subseteq \mathbb{G}_m(\bar{\mathbb{Q}})$ is the $\sigma\delta$ -Galois group for the system

$$\sigma(W) = \left(\frac{b}{u\sigma(u)} \right) W,$$

which by [13, Prop. 2.9] must be integrable over k in the sense of [5, Def. 3.3]. It is shown in [5, Prop. 3.6] that this system must then be integrable over $\bar{\mathbb{Q}}(x)$, and therefore by [24, Thm. 2], there exist $t \in \bar{\mathbb{Q}}(x)^\times$ and $c, d \in \bar{\mathbb{Q}}$ with $c \neq 0$ such that $\tilde{w} := t^{-1}w$ satisfies

$$\sigma(\tilde{w}) = c\tilde{w};$$

$$\delta(\tilde{w}) = d\tilde{w}.$$

It is convenient to point out now that $c \neq q^r$ for any $r \in \mathbb{Z}$, because otherwise we would have $\tilde{w} = ex^r$ for some $e \in C$, which would imply that $w \in k$, contradicting our hypothesis that H is not commutative (cf. the proof of Proposition 6.1: H is commutative if and only if $\alpha_\gamma = \lambda_\gamma$ for every $\gamma \in H$ if and only if $w \in k$ by (6.6) and Theorem 2.9). We will need to use the fact that $c \notin q^{\mathbb{Z}}$ at the end of the proof.

We claim that

$$\tilde{w}^{-1}\mathcal{L}(w) =: f_{\mathcal{L}} \in k, \quad \text{and moreover} \quad f_{\mathcal{L}} = \tilde{\mathcal{L}}(t) \quad (6.18)$$

for some homogeneous linear differential polynomial $0 \neq \tilde{\mathcal{L}} \in C\{Y\}_\delta$. In fact, this is true for any non-zero homogeneous linear differential polynomial in $C\{Y\}_\delta$, not just for the specific $\mathcal{L} \in C\{Y\}_\delta$ in (6.17). It suffices to show that $\tilde{w}^{-1}\delta^n(w)$ belongs to the C -linear span $\mathcal{D}$ of $\{\delta^j(t) \mid j \in \mathbb{Z}_{\geq 0}\}$ for every $n \in \mathbb{N}$. We prove this by induction: the case $n = 0$ is clear, since $\tilde{w}^{-1}w = t \in \mathcal{D}$. Assuming that $\tilde{w}^{-1}\delta^n(w) = f_n \in \mathcal{D}$, we see that

$$\tilde{w}^{-1}\delta^{n+1}(w) = \tilde{w}^{-1}\delta(\delta^n(w)) = \tilde{w}^{-1}\delta(f_n\tilde{w}) = \delta(f_n) + df_n \in \mathcal{D}$$

as well. Moreover, this computation also shows that $\mathcal{L}, \tilde{\mathcal{L}} \in C\{Y\}_\delta$ have the same order and the same leading coefficient.

By (6.5) and (6.6), the element $\mathcal{L}(z) \in R$ satisfies

$$\sigma(\mathcal{L}(z)) - \mathcal{L}(z) = \mathcal{L}(w), \quad \text{and} \quad \gamma(\mathcal{L}(z)) = \frac{\lambda_\gamma}{\alpha_\gamma}\mathcal{L}(z) + \mathcal{L}\left(\frac{\xi_\gamma}{\alpha_\gamma}\right)$$

for every $\gamma \in G$, since $\delta(\lambda_\gamma\alpha_\gamma^{-1}) = 0$ for $\gamma \in G$. Hence $\gamma(\mathcal{L}(z)) = \mathcal{L}(z)$ for every $\gamma \in R_u(G)$, and therefore by Theorem 2.9 we have that $\mathcal{L}(z) \in k\langle y_0, y_1 \rangle_\delta =: F$, the total ring of fractions of the $\sigma\delta$ -PV ring $k\{y_0, y_1, (y_0y_1)^{-1}\}_\delta$ for (6.8); we emphasize that the latter ring is not necessarily a domain, so F is not necessarily a field.

For $\gamma \in G/R_u(G) \simeq \text{Gal}_{\sigma\delta}(F/k) =: \bar{G}$ given by $\begin{pmatrix} \alpha_\gamma & 0 \\ 0 & \lambda_\gamma \end{pmatrix} \in \mathbb{G}_m(C)^2$, let

$$\tau_\gamma := \gamma(\tilde{w}^{-1}\mathcal{L}(z)) - \tilde{w}^{-1}\mathcal{L}(z), \quad (6.19)$$

where we note that since $\mathcal{L}(z) \in F$ is fixed by $R_u(G)$, the action of the reductive quotient $\bar{G}$ on $\mathcal{L}(z)$ is well-defined. We claim that $\{\tau_\gamma \mid \gamma \in \bar{G}\}$ is a 1-cocycle of $\bar{G}$ with values in the $\bar{G}$ -module $M := C \cdot \tilde{w}^{-1}$ (see [18, VI.10]). Since M is the solution space for $\sigma(W) = c^{-1}W$ in F , it is clear that M is stabilized by $\bar{G}$. Moreover, it follows from (6.18) that

$$\sigma(\tau_\gamma) = ((\gamma - 1) \circ \sigma)(\tilde{w}^{-1}\mathcal{L}(z)) = (\gamma - 1)(c^{-1}\tilde{w}^{-1}\mathcal{L}(z) + c^{-1}\tilde{w}^{-1}\mathcal{L}(w)) = c^{-1}\tau_\gamma,$$

since $c^{-1}\tilde{w}^{-1}\mathcal{L}(w) = c^{-1}f_{\mathcal{L}} \in k$ and therefore $\gamma(c^{-1}f_{\mathcal{L}}) = c^{-1}f_{\mathcal{L}}$ for every $\gamma \in \bar{G}$. Hence $\tau_{\gamma} \in M$ for each $\gamma \in \bar{G}$. To verify the cocycle condition, note that for $\gamma, \theta \in \bar{G}$ we have that

$$\begin{aligned}\tau_{\gamma\theta} &= \gamma\theta(\tilde{w}^{-1}\mathcal{L}(z)) - \tilde{w}^{-1}\mathcal{L}(z) = \gamma(\theta(\tilde{w}^{-1}\mathcal{L}(z)) - \tilde{w}^{-1}\mathcal{L}(z)) + (\gamma(\tilde{w}^{-1}\mathcal{L}(z)) - \tilde{w}^{-1}\mathcal{L}(z)) \\ &= \gamma(\tau_{\theta}) + \tau_{\gamma}.\end{aligned}$$

Since G is not commutative (for otherwise H would be commutative, as discussed above and contrary to our hypotheses), there exists $\gamma \in \bar{G}$ such that $\alpha_{\gamma} \neq \lambda_{\gamma}$, and therefore $m \mapsto \gamma(m) - m$ is a $\bar{G}$ -automorphism of M for such a $\gamma \in \bar{G}$, since $\bar{G}$ is commutative. By Sah's Lemma [18, Lem. VI.10.2], the cohomology group $H^1(\bar{G}, M) = \{0\}$, and in particular $\{\tau_{\gamma} \mid \gamma \in \bar{G}\}$ is a 1-coboundary, i.e., there exists $e\tilde{w}^{-1} \in C \cdot \tilde{w}^{-1} = M$ such that $\tau_{\gamma} = \gamma(e\tilde{w}^{-1}) - e\tilde{w}^{-1}$. It follows from the definition of τ_{γ} in (6.19) that

$$\gamma(\tilde{w}^{-1}\mathcal{L}(z) - e\tilde{w}^{-1}) = \tilde{w}^{-1}\mathcal{L}(z) - e\tilde{w}^{-1}$$

for every $\gamma \in \bar{G}$, which implies that $\tilde{w}^{-1}\mathcal{L}(z) - e\tilde{w}^{-1} =: g \in k$ by Theorem 2.9. Hence

$$f_{\mathcal{L}}\tilde{w} = \mathcal{L}(w) = \sigma(\mathcal{L}(z)) - \mathcal{L}(z) = \sigma(g\tilde{w}) - g\tilde{w} = (c\sigma(g) - g)\tilde{w},$$

and therefore, since $c \in \bar{\mathbb{Q}}^{\times}$,

$$\tilde{\mathcal{L}}(c^{-1}t) = c^{-1}f_{\mathcal{L}} = \sigma(g) - c^{-1}g,$$

where $0 \neq \tilde{\mathcal{L}} \in C\{Y\}_{\delta}$ is the homogeneous linear differential polynomial defined implicitly in (6.18). Since $c \notin q^{\mathbb{Z}}$, it follows from [13, Prop. 6.4(2)] that there exists $h \in k$ such that

$$c^{-1}t = \sigma(h) - c^{-1}h.$$

But then $h\tilde{w}$ satisfies

$$\sigma(h\tilde{w}) - h\tilde{w} = (c\sigma(h) - h)\tilde{w} = t\tilde{w} = w,$$

and therefore $\sigma(z - h\tilde{w}) - (z - h\tilde{w}) = 0$ by (6.5), which implies that $z - h\tilde{w} \in C$ and therefore $z \in k[w]$ is fixed by $R_u(H)$. But $\gamma(z) = z + \xi_{\gamma}$ for every $\gamma \in R_u(H)$, and therefore $R_u(H) = \{0\}$, which contradicts our hypotheses and concludes the proof. $\square$

Remark 6.3. To compute the difference-differential Galois group G for (4.1) when there exists exactly one solution $u \in \bar{\mathbb{Q}}(x)$ to (4.3), we apply Propositions 5.2, 6.1, and 6.2 as follows. First, compute the defining equations for the reductive quotient

$$\bar{G} := G/R_u(G) = \left\{ \begin{pmatrix} \alpha_{\gamma} & 0 \\ 0 & \lambda_{\gamma} \end{pmatrix} \mid \gamma \in G \right\},$$

which is the $\sigma\delta$ -Galois group for the system (6.8), as in Proposition 5.2 and Remark 5.3, with $u_1 = u$ and $u_2 = v$. In particular, this requires computing the q -discrete residues $q\text{-dres}\left(\frac{\delta(u)}{u}, [\beta]_q, 1\right)$ for each $q^{\mathbb{Z}}$ -orbit $[\beta]_q$ with $\beta \in \bar{\mathbb{Q}}^\times$. Note that this will produce all the defining equations for G relating α and λ only, and it remains to compute the remaining defining equations for G , if there are any.

If $uv^{-1} \neq \frac{\sigma(w)}{w}$ for any $w \in \bar{\mathbb{Q}}(x)$ as in Proposition 5.2(i), then $R_u(G) = \mathbb{G}_a(C)$ by Proposition 6.2, and therefore there are no more defining equations for G . Otherwise, compute such a $w \in \bar{\mathbb{Q}}(x)$, as well as its q -discrete residues $q\text{-dres}(w, [\beta]_q, j)$ for every $q^{\mathbb{Z}}$ -orbit $[\beta]_q$ and $j \in \mathbb{N}$ (only finitely many of these are non-zero). In this case,

$$G \subseteq \bar{G} \times \mathbb{G}_a(C) = \left\{ \begin{pmatrix} \alpha & \xi \\ 0 & \alpha \end{pmatrix} \mid \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \in \bar{G}, \xi \in C \right\}, \quad (6.20)$$

and this containment is proper if and only if there exist $f \in \bar{\mathbb{Q}}(x)$, a homogeneous linear differential polynomial $\mathcal{L} \in \bar{\mathbb{Q}}\{Y\}_\delta$, and $c \in \bar{\mathbb{Q}}$ as in Proposition 6.1(iii).

Let us first compute the defining equations of G in (6.20) when $q\text{-dres}(w, [\beta]_q, j) = 0$ for every $q^{\mathbb{Z}}$ -orbit $[\beta]_q$ and $j \in \mathbb{N}$, in which case $q\text{-dres}(w, \infty) =: c \neq 0$ and $-w = \sigma(f) - f - c$ for some $f \in \bar{\mathbb{Q}}(x)$ by Proposition 3.3, as in Proposition 6.1(iii). In this case, G is contained in the subgroup of (6.20) defined by $\delta\left(\frac{\xi}{\alpha}\right) = 0$, and $R_u(G) \subseteq \mathbb{G}_a(C^\delta)$. If $\frac{\delta(u)}{u} = \sigma(\tilde{f}) - \tilde{f}$ for some $\tilde{f} \in \bar{\mathbb{Q}}(x)$ as in Proposition 5.2(ii), so that $\delta(\alpha_\gamma) = 0$ for every $\gamma \in G$, then G is the subgroup of (6.20) defined by $\delta(\xi) = 0$, and $R_u(G) = \mathbb{G}_a(C^\delta)$. If there exist $\tilde{f} \in \bar{\mathbb{Q}}(x)$ and $0 \neq \tilde{c} \in \mathbb{Z}$ as in Proposition 5.2(ii), so that $\delta\left(\frac{\delta(\alpha_\gamma)}{\alpha_\gamma}\right) = 0$ for every $\gamma \in G$ but there exists $\gamma \in G$ such that $\delta(\alpha_\gamma) \neq 0$, then G is the subgroup of (6.20) defined by $\tilde{c}\xi = c\delta(\alpha)$, and $R_u(G) = \{0\}$. If there are no $\tilde{f} \in \bar{\mathbb{Q}}(x)$ and $\tilde{c} \in \mathbb{Z}$ such that $\frac{\delta(u)}{u} = \sigma(\tilde{f}) - \tilde{f} + \tilde{c}$, then G is precisely the subgroup of (6.20) defined by $\delta\left(\frac{\xi}{\alpha}\right) = 0$, and $R_u(G) = \mathbb{G}_a(C^\delta)$.

Assuming now that some q -discrete residue $q\text{-dres}(w, [\beta]_q, j) \neq 0$, let $r \in \mathbb{N}$ be as large as possible such that $q\text{-dres}(w, [\beta]_q, r) \neq 0$ for some $q^{\mathbb{Z}}$ -orbit $[\beta]_q$. Write the linear differential polynomial

$$\mathcal{L} = \sum_{i=0}^{r-1} c_i \delta^i(Y) \in \bar{\mathbb{Q}}\{Y\}_\delta$$

with undetermined coefficients, and decide whether the system of linear equations over $\bar{\mathbb{Q}}$ defined by setting

$$q\text{-dres}\left(\mathcal{L}\left(\frac{\delta(u)}{u}\right) - w, [\beta]_q, j\right) = 0 \quad (6.21)$$

for every $q^{\mathbb{Z}}$ -orbit $[\beta]_q$ and $1 \leq j \leq r$ admits a solution. If there is no solution, then again we have that $R_u(G) = \mathbb{G}_a(C)$ and G is precisely the group in (6.20). If there is a solution, then it is unique and $c_{r-1} \neq 0$. In this case, setting

$$c := c_0 \cdot q\text{-dres} \left(\frac{\delta(u)}{u}, \infty \right) - q\text{-dres}(w, \infty), \quad (6.22)$$

there exists $f \in \bar{\mathbb{Q}}(x)$ as in Proposition 6.1(iii) by Proposition 3.3, and G is the subgroup of (6.20) defined by the corresponding relation stipulated in Proposition 6.1, depending on whether the $c \in \bar{\mathbb{Q}}$ defined in (6.22) is zero or not. If $c = 0$ then $R_u(G) = 0$, and if $c \neq 0$ then $R_u(G) = \mathbb{G}_a(C^\delta)$.

Since $R_u(G) = \{0\}$ whenever there is not exactly one solution $u \in \bar{\mathbb{Q}}(x)$ to (4.3) (i.e., either there is no solution or there is more than one solution to (4.3) in $\bar{\mathbb{Q}}(x)$), we deduce the following result from Remark 6.3, which generalizes [13, Prop. 4.3(2)].

Corollary 6.4. *If G is the $\sigma\delta$ -Galois group of (4.1), then the unipotent radical $R_u(G)$ is either $\{0\}$, $\mathbb{G}_a(C^\delta)$, or $\mathbb{G}_a(C)$.*

7. Irreducible and imprimitive groups

In this section we will denote $k_1 = C(x)$, where C is a δ -closure of $\bar{\mathbb{Q}}$, σ denotes the C -linear automorphism of k defined by $\sigma(x) = qx$, and $\delta(x) = 1$. It will be convenient to use similar notation as that of Section 4: fix once and for all $q_2 \in \bar{\mathbb{Q}}$ such that $q_2^2 = q$, and let $k_2 := C(x_2)$ be the $\sigma\delta$ -field extension of k_1 defined by setting $x_2^2 = x$, $\sigma(x_2) = q_2x_2$, and $\delta(x_2) = \frac{1}{2}x_2$.

Let us now suppose that there are no solutions in $\bar{\mathbb{Q}}(x)$ to the first Riccati equation (4.3). We claimed in the statement of Proposition 4.5, but have not yet proved, that under these conditions the σ -Galois group H for (4.1) over k should be irreducible, and that H should be imprimitive if and only if one of the following possibilities holds:

- (1) there exist two solutions $u_1, u_2 \in \bar{\mathbb{Q}}(x_2) \setminus \bar{\mathbb{Q}}(x)$ to the first Riccati equation (4.3) such that $u_2 = \bar{u}_1$ is the Galois conjugate of u_1 over $\bar{\mathbb{Q}}(x)$; or
- (2) either $a = 0$ or else there exists a solution $e \in \bar{\mathbb{Q}}(x)$ to the second Riccati equation (4.5); or
- (3) $a \neq 0$ and there exist two solutions $e_1, e_2 \in \bar{\mathbb{Q}}(x_2) \setminus \bar{\mathbb{Q}}(x)$ to the second Riccati equation (4.5) such that $e_2 = \bar{e}_1$ is the Galois conjugate of e_1 over $\bar{\mathbb{Q}}(x)$.

Note that (2) and (3) above are mutually exclusive and together exhaust the possibility that the more compact Proposition 4.5(5) holds. We will address each of the possibilities (1), (2), and (3) above in Sections 7.1, 7.2, and 7.3, respectively, and establish in each case that H is indeed irreducible and imprimitive in each of these scenarios, as stated in Proposition 4.5.

By [26, Prop. 12.2(1)], in any case the group of connected components H/H° must be bicyclic. The irreducible and imprimitive algebraic subgroups of $\text{GL}_2(\bar{\mathbb{Q}})$ with bicyclic group of connected components are listed in the following result, which we prove using the

classification of the algebraic subgroups of $\mathrm{GL}_2(C)$ developed in [21]. In the classification below we denote $\{\pm 1\} \times \{\pm 1\}$ by $\{\pm 1\}^2$ and $\mathbb{G}_m(C) \times \mathbb{G}_m(C)$ by $\mathbb{G}_m(C)^2$.

Lemma 7.1. *If H is an irreducible and imprimitive algebraic subgroup of $\mathrm{GL}_2(C)$ such that H/H° is bicyclic, then H is the subgroup of*

$$\{\pm 1\} \ltimes \mathbb{G}_m(C)^2 = \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C^\times \right\} \cup \left\{ \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix} \mid \lambda_1, \lambda_2 \in C^\times \right\} \quad (7.1)$$

defined by precisely one of the following sets of conditions on $\alpha_1, \alpha_2, \lambda_1$, and λ_2 .

- (1) $H = D_m^-$ for some $m \in \mathbb{N}$, defined as the subgroup of (7.1) such that $(\alpha_1 \alpha_2)^m = 1$ and $(\lambda_1 \lambda_2)^m = -1$; or
- (2) $H = D_m^+$ for some $m \in \mathbb{N}$, defined as the subgroup of (7.1) such that $(\alpha_1 \alpha_2)^m = 1$ and $(\lambda_1 \lambda_2)^m = 1$; or
- (3) $H = \{\pm 1\}^2 \ltimes \mathbb{G}_m(C)$, defined as the subgroup of (7.1) such that $\alpha_1^2 = \alpha_2^2$ and $\lambda_1^2 = \lambda_2^2$; or
- (4) $H = \{\pm 1\} \ltimes \mathbb{G}_m(C)^2$ as in (7.1), with no other conditions on $\alpha_1, \alpha_2, \lambda_1$, and λ_2 .

Proof. The algebraic subgroups $H \subseteq \mathrm{GL}_2(C)$ are classified in [21] according to their projective image $\bar{H} \subseteq \mathrm{PGL}_2(C)$. Since H is irreducible and imprimitive with bicyclic group of connected components, it is an infinite non-commutative subgroup of (7.1), and therefore its projective image is either $\bar{H} = D_n$, the dihedral group of order $2n$ for some $n \geq 2$, or else $\bar{H} = \bar{D}_\infty$, the projective image of

$$D_\infty = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \mid \alpha \in C^\times \right\} \cup \left\{ \begin{pmatrix} 0 & -\lambda \\ \lambda^{-1} & 0 \end{pmatrix} \mid \lambda \in C^\times \right\}.$$

If $\bar{H} = D_n$ then D_n must be commutative, since the algebraic quotient map $H \rightarrow \bar{H}$ factors through H/H° , which we are assuming is abelian, and therefore $n = 2$ (corresponding to $D_n \simeq K_4$, the Klein four-group) in this case. By [21, Thm. 4], the *minimal* subgroups (see [21, §2] for the definition) of $\mathrm{GL}_2(C)$ having projective image D_2 are $D_{2,\ell}$ for some $\ell \in \mathbb{Z}_{\geq 0}$, where

$$D_{2,\ell} := \left\langle \zeta_{2^{\ell+1}} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle$$

and $\zeta_{2^{\ell+1}}$ denotes a primitive $(2^{\ell+1})$ -th root of unity. Therefore the only infinite subgroups $H \subseteq \mathrm{GL}_2(C)$ having projective image D_2 are given by $C^\times \cdot D_{2,\ell}$, which are all equal to $\pi^{-1}(D_2)$, where $\pi : \mathrm{GL}_2(C) \rightarrow \mathrm{PGL}_2(C)$ is the projection map. Finally, note that $C^\times \cdot D_{2,\ell}$ for any $\ell \in \mathbb{Z}_{\geq 0}$ is precisely the subgroup of (7.1) defined by the conditions in item (3): $\alpha_1^2 = \alpha_2^2$ and $\lambda_1^2 = \lambda_2^2$.

If $\bar{H} = \bar{D}_\infty$, then either $H = \{\pm 1\} \rtimes \mathbb{G}_m(C)$ in (7.1) as in item (4), or else $H = \mu_n \cdot D_{\infty, \ell}$ for some $\ell \in \mathbb{Z}_{\geq 0}$ and some $n \in \mathbb{N}$, where μ_n denotes the group of n -th roots of unity, and

$$D_{\infty, \ell} := \left\langle \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \mid \alpha \in C^\times \right\}, \begin{pmatrix} 0 & \zeta_{2^{\ell+1}} \\ \zeta_{2^{\ell+1}} & 0 \end{pmatrix} \right\rangle,$$

where again $\zeta_{2^{\ell+1}}$ is a primitive $(2^{\ell+1})$ -th root of unity, since by [21, Thm. 4] the $D_{\infty, \ell}$ are all the minimal subgroups of $\mathrm{GL}_2(C)$ with projective image $\bar{D}_\infty$. All of these groups have the property that H/H° is bicyclic. It remains to show that for any $n \in \mathbb{N}$ and $\ell \in \mathbb{Z}_{\geq 0}$ the group $\mu_n \cdot D_{\infty, \ell}$ is one of the groups described by the conditions in either item (1) or item (2). Let us write $\Delta_{n, \ell} := \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C^\times \right\} \cap (\mu_n \cdot D_{\infty, \ell})$, the group of all diagonal matrices contained in $\mu_n \cdot D_{\infty, \ell}$, and $\nabla_{n, \ell} := \left\{ \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix} \mid \lambda_1, \lambda_2 \in C^\times \right\} \cap (\mu_n \cdot D_{\infty, \ell})$ for the complementary coset of $\Delta_{n, \ell}$ in $\mu_n \cdot D_{\infty, \ell}$ consisting of all the antidiagonal matrices contained in $\mu_n \cdot D_{\infty, \ell}$. Then we see that $\nabla_{n, \ell} = \zeta_{2^{\ell+1}} \cdot \Delta_{n, \ell} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and $\Delta_{n, \ell} = \langle \zeta_n, \zeta_{2^\ell} \rangle \cdot \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \mid \alpha \in C^\times \right\}$. Therefore,

$$\Delta_{n, \ell} = \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C^\times, (\alpha_1 \alpha_2)^m = 1 \right\}, \quad \text{where}$$

$$m := \begin{cases} \frac{1}{2} \mathrm{lcm}(n, 2^\ell) & \text{if } \ell \geq 1; \\ \frac{n}{2} & \text{if } \ell = 0 \text{ and } 2 \mid n; \\ n & \text{if } \ell = 0 \text{ and } 2 \nmid n; \end{cases}$$

because $(\langle \zeta_n, \zeta_{2^\ell} \rangle)^2 = \langle \zeta_m \rangle$ with m defined as above. Since

$$\nabla_{n, \ell} = \left\{ \begin{pmatrix} 0 & \alpha_1 \zeta_{2^{\ell+1}} \\ \alpha_2 \zeta_{2^{\ell+1}} & 0 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C^\times, (\alpha_1 \alpha_2)^m = 1 \right\},$$

we have that $\mu_n \cdot D_{\infty, \ell}$ is the group described in item (2) if and only if $2^\ell \mid m$ (which occurs precisely when either $\ell = 0$ or else $\ell \geq 1$ and $2^{\ell+1} \mid n$), and $\mu_n \cdot D_{\infty, \ell}$ is the group described in item (1) otherwise, since for $\ell \geq 1$ we always have that $2^{\ell-1} \mid m$, and therefore $(\zeta_{2^{\ell+1}}^2 \alpha_1 \alpha_2)^m = (\zeta_{2^\ell} \alpha_1 \alpha_2)^m = -1$, precisely when $2^\ell \nmid m$, $2^{\ell-1} \mid m$ (with $\ell \geq 1$), and $(\alpha_1 \alpha_2)^m = 1$. $\square$

Remark 7.2. Given an irreducible and imprimitive algebraic subgroup $H \subseteq \mathrm{GL}_2(C)$ such that the group of connected components H/H° is bicyclic, we can uniquely identify it among the possibilities listed in Lemma 7.1 by the knowledge of two auxiliary groups:

$$\Delta(H) := \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C^\times \right\} \cap H \quad \text{and}$$

$$\det(H) = \{\det(h) \mid h \in H\} \subseteq \mathbb{G}_m(C),$$

respectively the subgroup of diagonal matrices in H and the image of H under the determinant map. Indeed, $\Delta(H) = \mathbb{G}_m(C)^2$ if and only if $H = \{\pm 1\} \ltimes \mathbb{G}_m(C)^2$ as in Lemma 7.1(4); $\Delta(H) = \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C^\times, \alpha_1^2 = \alpha_2^2 \right\}$ if and only if $H = \{\pm 1\}^2 \ltimes \mathbb{G}_m(C)$ is as in Lemma 7.1(3); and $\Delta(H) = \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C^\times, (\alpha_1 \alpha_2)^m \right\}$ for some $m \in \mathbb{N}$ if and only if H is one of the groups D_m^- or D_m^+ described respectively in items (1) or (2) of Lemma 7.1. To decide between these cases, note that $\det(H) = \langle \alpha_1 \alpha_2, -\lambda_1 \lambda_2 \rangle$ has $\det(H)^m = \langle (-1)^m (\lambda_1 \lambda_2)^m \rangle$; hence, if m is even, then $H = D_m^-$ if and only if $\det(H) = \mu_{2m}$ and $H = D_m^+$ if and only if $\det(H) = \mu_m$; and if m is odd, then $H = D_m^-$ if and only if $\det(H) = \mu_m$ and $H = D_m^+$ if and only if $\det(H) = \mu_{2m}$.

7.1. Irreducible and imprimitive (1): diagonalizable over the quadratic extension

Supposing there are no solutions to (4.3) in $\bar{\mathbb{Q}}(x)$, but there are two solutions $u, \bar{u} \in \bar{\mathbb{Q}}(x_2)$ to (4.3), Galois-conjugate over $\bar{\mathbb{Q}}(x)$, the system (4.2)

$$\begin{aligned} \sigma(Y) &= \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} Y \quad \text{with fundamental solution matrix} \quad Y = \begin{pmatrix} y_1 & y_2 \\ \sigma(y_1) & \sigma(y_2) \end{pmatrix}; \text{ and} \\ \sigma(Z) &= \begin{pmatrix} u & 0 \\ 0 & \bar{u} \end{pmatrix} Z \quad \text{with fundamental solution matrix} \quad Z = \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} \end{aligned} \quad (7.2)$$

are equivalent over $\bar{\mathbb{Q}}(x_2)$ via the gauge transformation $Z = TY$, where (cf. Remark 5.1)

$$T := \begin{pmatrix} \frac{\bar{u}}{u-\bar{u}} & \frac{-1}{u-\bar{u}} \\ \frac{u}{u-\bar{u}} & \frac{-1}{\bar{u}-u} \end{pmatrix} \in \mathrm{GL}_2(\bar{\mathbb{Q}}(x_2)). \quad (7.3)$$

Let us write $S_2 = k_2[Y, \det(Y)^{-1}] = k_2[z_1, z_2, (z_1 z_2)^{-1}]$ for the σ -PV ring for (4.2) (or equivalently for (7.2)) over k_2 . Then $S_1 = k_1[Y, \det(Y)^{-1}] \subset S_2$ is a σ -PV ring for (4.2) over k_1 . Let us also write $H_i = \mathrm{Gal}_\sigma(S_i/k_i)$ for $i = 1, 2$, and $\tilde{H} = \mathrm{Gal}_\sigma(S_2/k_1)$. Since (7.2) is a diagonal system, the group H_2 is diagonalizable. By Proposition 4.2,

$$\tilde{H} \simeq H_1 \times_{\mu_m} \mu_2,$$

where $m \in \{1, 2\}$ is determined by the intersection $S_1 \cap k_2 = k_m$ inside S_2 , and H_2 is an index- m subgroup of H_1 . We claim that any $\tilde{\tau} \in \tilde{H}$ such that $\tilde{\tau}(x_2) = -x_2$ has the property that $\tau := \tilde{\tau}|_{S_1} \in H_1$ is given by an anti-diagonal matrix. From this it will follow that H_2 has index exactly 2 in H_1 , and $H_1 = H_2 \cup H_2 \cdot \tau$ is irreducible and imprimitive, as claimed in Proposition 4.5(4).

To see this, let $M_\tau \in \mathrm{GL}_2(C)$ such that $\tau(Y) = Y M_\tau$. Then for the gauge transformation T given in (7.3) we see that

$$\tilde{\tau}(Z) = \tilde{\tau}(TY) = \bar{T} Y M_\tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} Z M_\tau.$$

On the other hand, we see that $\sigma(\tilde{\tau}(z_1)) = \tilde{\tau}(\sigma(z_1)) = \tilde{\tau}(uz_1) = \bar{u}\tilde{\tau}(z_1)$, and therefore $\tilde{\tau}(z_1) = \lambda_2 z_2$ for some $\lambda_2 \in C^\times$. A similar computation shows that $\tilde{\tau}(z_2) = \lambda_1 z_1$ for some $\lambda_1 \in C^\times$. From this it follows that

$$\tilde{\tau}(Z) = \begin{pmatrix} \tilde{\tau}(z_1) & 0 \\ 0 & \tilde{\tau}(z_2) \end{pmatrix} = \begin{pmatrix} \lambda_2 z_2 & 0 \\ 0 & \lambda_1 z_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} Z \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix}.$$

Hence $M_\tau = \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix}$, as we wanted to show.

Remark 7.3. Having established that the σ -Galois group H_1 for (4.2) over k_1 is indeed irreducible and imprimitive as claimed in Proposition 4.5(4), we can compute this H_1 from among the possibilities listed in Lemma 7.1 as explained in Remark 7.2, by determining the subgroup $\Delta(H_1)$ of diagonal matrices in H_1 , and the group $\det(H_1) \subseteq \mathbb{G}_m(C)$.

Since $\det(H_1)$ is the σ -Galois group for the system $\sigma(y) = by$, we see that $\det(H_1) = \mu_m$ if and only if $m \in \mathbb{N}$ is the smallest positive integer such that $b^m = \frac{\sigma(f)}{f}$ for some $f \in \bar{\mathbb{Q}}(x)$, and if there is no such m then $\det(H_1) = \mathbb{G}_m(C)$.

Since $\Delta(H_1) = H_2$ is the σ -Galois group for (7.2) over k_2 , we can compute the defining equations for

$$\Delta(H_1) \subseteq \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C^\times \right\}$$

as follows:

- (1) $(\alpha_1 \alpha_2)^m = 1$ if and only if $(u\bar{u})^m = \frac{\sigma(f)}{f}$ for some $f \in \bar{\mathbb{Q}}(x_2)^\times$ (and in this case H_1 is D_m^- or D_m^+);
- (2) $\alpha_1^2 = \alpha_2^2$ if and only if $(\frac{u}{\bar{u}})^2 = \frac{\sigma(f)}{f}$ for some $f \in \bar{\mathbb{Q}}(x_2)$ (and in this case $H_1 = \{\pm 1\}^2 \rtimes \mathbb{G}_m(C)$);
- (3) if none of these possibilities holds, then $\Delta(H_1) = \mathbb{G}_m(C)^2$ (and in this case $H_1 = \{\pm 1\} \ltimes \mathbb{G}_m(C)^2$).

The computation of the $\sigma\delta$ -Galois group G_1 for (4.2) over k_1 , assuming that the corresponding σ -Galois group H_1 has already been computed as in Remark 7.3, will be achieved analogously in the following result, by studying the $\sigma\delta$ -Galois group G_2 for (4.2) over k_2 .

Proposition 7.4. Suppose there are no solutions to (4.3) in $\bar{\mathbb{Q}}(x)$, and let $u, \bar{u} \in \bar{\mathbb{Q}}(x_2)$ satisfy (4.3). Then G_1 is the subgroup of

$$\{\pm 1\} \ltimes \mathbb{G}_m(C)^2 = \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}, \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix} \mid \alpha_1 \alpha_2 \neq 0, \lambda_1 \lambda_2 \neq 0 \right\} \quad (7.4)$$

defined by the following conditions on $\alpha_1, \alpha_2, \lambda_1$, and λ_2 .

- (1) If $H_1 = D_m^-$ as in Lemma 7.1(1) or $H_1 = D_m^+$ as in Lemma 7.1(2), then $G_1 = H_1$.
 (2) If $H_1 = \{\pm 1\}^2 \ltimes \mathbb{G}_m(C)$ as in Lemma 7.1(3), then:

- (a) there exist $0 \neq c \in 2\mathbb{Z}$ and $g \in \bar{\mathbb{Q}}(x)$ such that $\frac{\delta(b)}{b} = \sigma(g) - g + c$ if and only if G_1 is the subgroup of H_1 defined by $\delta\left(\frac{\delta(\alpha_1)}{\alpha_1} + \frac{\delta(\alpha_2)}{\alpha_2}\right) = 0 = \delta\left(\frac{\delta(\lambda_1)}{\lambda_1} + \frac{\delta(\lambda_2)}{\lambda_2}\right)$;
 (b) otherwise, $G_1 = H_1$.

- (3) If $H_1 = \{\pm 1\} \ltimes \mathbb{G}_m(C)^2$ as in Lemma 7.1(4), then:

- (a) there exist $c \in 2\mathbb{Z}$ and $g \in \bar{\mathbb{Q}}(x)$ such that $\frac{\delta(b)}{b} = \sigma(g) - g + c$ if and only if $\delta\left(\frac{\delta(\alpha_1)}{\alpha_1} + \frac{\delta(\alpha_2)}{\alpha_2}\right) = 0 = \delta\left(\frac{\delta(\lambda_1)}{\lambda_1} + \frac{\delta(\lambda_2)}{\lambda_2}\right)$; moreover, $c = 0$ if and only if $\delta(\alpha_1\alpha_2) = 0 = \delta(\lambda_1\lambda_2)$;
 (b) otherwise, $G_1 = H_1$.

Proof. Since the systems (4.2) and (7.2) are equivalent over k_2 , and the latter system is diagonal, we can compute G_2 with Proposition 5.2 and Remark 5.3, but with a small caveat. Namely, after replacing δ with $\delta_2 := 2\delta$, we see that k_2 as a $\sigma\delta_2$ -field behaves just as k_1 : $\sigma(x_2) = q_2x_2$ and $\delta_2(x_2) = x_2$. Thus we may compute the δ_2 -algebraic group $G_2 \subseteq \mathbb{G}_m(C)^2$ over k_2 using the procedure described in Remark 5.3 exactly as stated there, and then simply replace every instance of δ_2 in the defining equations for G_2 with $\frac{1}{2}\delta$ a posteriori. But since the system (7.2) has such a special form, not every possibility listed in Proposition 5.2 may occur.

We saw in Remark 5.3 that G_2 is a proper subgroup of $\mathbb{G}_m(C)^2$ if and only if there exist: $m_1, m_2 \in \mathbb{Z}$, not both zero and with $\gcd(m_1, m_2) = 1$; $c \in \mathbb{Z}$; and $g \in \bar{\mathbb{Q}}(x_2)$, such that

$$m_1 \frac{\delta_2(u)}{u} + m_2 \frac{\delta_2(\bar{u})}{\bar{u}} = \sigma(g) - g + c \quad \Longleftrightarrow \quad m_2 \frac{\delta_2(u)}{u} + m_1 \frac{\delta_2(\bar{u})}{\bar{u}} = \sigma(\bar{g}) - \bar{g} + c. \quad (7.5)$$

Let us consider the submodule $M \subseteq \mathbb{Z}^2$ generated by relatively prime pairs (m_1, m_2) such that there exist $g \in \bar{\mathbb{Q}}(x_2)$ and $c \in \mathbb{Z}$ satisfying the above conditions. Then, as we saw in Remark 5.3, either $M = \{0\}$ is trivial; or $M = \mathbb{Z} \cdot (m_1, m_2)$ is infinite cyclic; or $M = \mathbb{Z}^2$. Moreover, $M = \{0\}$ is trivial if and only if the $\sigma\delta$ -Galois group G_2 for (7.2) is all of $\mathbb{G}_m(C)^2$. In this case we must have $G_1 = H_1 = \{\pm 1\} \ltimes \mathbb{G}_m(C)^2$, because G_1 is Zariski-dense in H_1 by Proposition 2.10, and therefore G_1 contains at least one anti-diagonal matrix, whence it contains all anti-diagonal matrices.

From now on we assume that M is not trivial. It follows from (7.5) that at least one of $(1, 1)$ or $(1, -1)$ belongs to M . In any case it is useful to observe that

$$q_2\text{-dres}\left(\frac{\delta_2(u)}{u}, \infty\right) = d = q_2\text{-dres}\left(\frac{\delta_2(\bar{u})}{\bar{u}}, \infty\right),$$

where $d \in \mathbb{Z}$ is the common degree of u and $\bar{u}$ considered as rational functions in x_2 . Therefore, $(1, -1) \in M$ if and only if $\delta(\alpha_1 \alpha_2) = 0$ for every $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in G_2$.

We claim that actually $(1, -1) \in M$ if and only if $H_1 = \{\pm 1\}^2 \rtimes \mathbb{G}_m(C)$ as in Lemma 7.1(3). As explained in Remark 7.3, $H_1 = \{\pm 1\}^2 \rtimes \mathbb{G}_m(C)$ if and only if there exists $f \in \bar{\mathbb{Q}}(x_2)^\times$ such that $\left(\frac{u}{\bar{u}}\right)^2 = \frac{\sigma(f)}{f}$, which in turn implies that

$$\frac{\delta_2(u)}{u} - \frac{\delta_2(\bar{u})}{\bar{u}} = \sigma\left(\frac{1}{2} \frac{\delta_2(f)}{f}\right) - \frac{1}{2} \frac{\delta_2(f)}{f}.$$

Thus if $H = \{\pm 1\} \rtimes \mathbb{G}_m(C)$ then $(1, -1) \in M$. To establish the opposite implication, let us study the *reduced form* of u : there exists $v \in \mathbb{Q}(\bar{x}_2)$ such that $u \frac{\sigma(v)}{v} = ex_2^n \frac{p_1}{p_2}$, where $e \in \bar{\mathbb{Q}}^\times$ is such that if $e \in q_2^{\mathbb{Z}}$ then $e = 1$, $n \in \mathbb{Z}$ is arbitrary, and $p_1, p_2 \in \bar{\mathbb{Q}}[x_2]$ are monic such that $\gcd(x_2, p_1) = \gcd(x_2, p_2) = \gcd(p_1, \sigma^m(p_2)) = 1$ for every $m \in \mathbb{Z}$. We say that $ex_2^n \frac{p_1}{p_2}$ is the *reduced form* of u . We then see that the reduced form of $\bar{u}$ is $(-1)^n ex_2^n \frac{\bar{p}_1}{\bar{p}_2}$. Although it need not be the case that the reduced form of $\frac{u}{\bar{u}}$ is exactly

$$(-1)^n \frac{p_1 \bar{p}_2}{p_2 \bar{p}_1},$$

(because it is possible for $\gcd(p_1, \sigma^m(\bar{p}_2)) \neq 1$ for some $m \in \mathbb{Z}$), we see that in any case the reduced form of $\frac{u}{\bar{u}}$ is similarly given by

$$(-1)^n \frac{\tilde{p}_1}{\tilde{p}_2}$$

for some $\tilde{p}_1, \tilde{p}_2 \in \bar{\mathbb{Q}}[x_2]$ monic and such that $\gcd(x_2, \tilde{p}_1) = \gcd(x_2, \tilde{p}_2) = \gcd(\tilde{p}_1, \sigma^m(\tilde{p}_2)) = 1$ for every $m \in \mathbb{Z}$. But then we see that if, say, $\tilde{p}_1 \neq 1$, then there exists $\beta \in \bar{\mathbb{Q}}^\times$ such that $\tilde{p}_1(\beta) = 0$, and we have that

$$q_2\text{-dres}\left(\frac{\delta_2(\tilde{p}_1)}{\tilde{p}_1}, [\beta]_{q_2}, 1\right) \neq 0 = q_2\text{-dres}\left(\frac{\delta_2(\tilde{p}_2)}{\tilde{p}_2}, [\beta]_{q_2}, 1\right),$$

and similarly if we assume instead that $\tilde{p}_2 \neq 1$. Therefore, if either $\tilde{p}_1 \neq 1$ or $\tilde{p}_2 \neq 1$, it is impossible to have $(1, -1) \in M$. Or in other words, if $(1, -1) \in M$ then $\frac{u}{\bar{u}} = (-1)^n \frac{\sigma(\tilde{f})}{\tilde{f}}$ for some $\tilde{f} \in \bar{\mathbb{Q}}(x_2)^\times$. But in this case we then see that n must be odd, for otherwise we would have that $\alpha_1 = \alpha_2$ for every $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in G_2$, and since G_2 is Zariski-dense in H_2 the same relation would be satisfied by every diagonal matrix in H_1 , but this does not occur for any of the possibilities for H_1 listed in Lemma 7.1. This concludes the proof that $(1, -1) \in M$ if and only if $H_1 = \{\pm 1\} \rtimes \mathbb{G}_m(C)$ as in Lemma 7.1(3).

In case we do have $(1, -1) \in M$, we must decide whether $M = \mathbb{Z} \cdot (1, -1)$ or $M = \mathbb{Z}^2$. We have that $M = \mathbb{Z} \cdot (1, -1)$ if and only if $G_2 = H_2$, which implies that $G_1 = H_1$. On the other hand, we have $M = \mathbb{Z}^2$ if and only if $(1, 1) \in M$ also, i.e., (7.5) is satisfied with

$m_1 = 1 = m_2$. But then after adding those two equations together we see that there exists $f \in \bar{\mathbb{Q}}(x)$ (not just in $\bar{\mathbb{Q}}(x_2)$), such that

$$\frac{\delta(b)}{b} = \frac{\delta(u)}{u} + \frac{\delta(\bar{u})}{\bar{u}} + \sigma\left(\frac{\delta(w)}{w}\right) - \frac{\delta(w)}{w} = \sigma(f) - f + 2c.$$

Indeed, writing $u - \bar{u} = x_2 w$ with $w \in \bar{\mathbb{Q}}(x)^\times$ and $f := \frac{1}{2}(g + \bar{g}) + \frac{\delta(w)}{w} \in \bar{\mathbb{Q}}(x)$, where $g \in \bar{\mathbb{Q}}(x_2)$ and $c \in \mathbb{Z}$ are as in (7.5), the above equation results from comparing determinants in $\sigma(T)AT^{-1} = \begin{pmatrix} u & 0 \\ 0 & \bar{u} \end{pmatrix}$ with T as in (7.3). Furthermore, in this case we must have $c \neq 0$, for otherwise we would have that $G_1 \subseteq \mathrm{GL}_2(C^\delta)$ is differentially constant, which by [5, Thm. 3.7(ii)] would imply that G_1 is commutative. But this is impossible, since G_1 is Zariski-dense in H_1 by Proposition 2.10, so H_1 would have to be commutative also, yielding a contradiction. Thus, G_2 is a proper subgroup of H_2 if and only if

$$G_2 = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix} \mid \alpha \in C^\times \text{ with } \delta\left(\frac{\delta(\alpha)}{\alpha}\right) = 0 \right\}.$$

Since for any $\begin{pmatrix} 0 & \pm\lambda \\ \lambda & 0 \end{pmatrix} \in G_1$ we have that $\lambda^2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G_2$, we see that $\delta\left(\frac{\delta(\lambda)}{\lambda}\right) = 0$ also, concluding the proof of item (2).

It remains to show that the statements in items (1) and (3) are correct when $M = \mathbb{Z} \cdot (1, 1)$. If $H_1 = D_m^-$ or $H_1 = D_m^+$, then $G_2 = H_2$ and therefore $G_1 = H_1$. This establishes item (1). Finally, supposing $H_1 = \{\pm 1\} \ltimes \mathbb{G}_m(C)^2$ and $M = \mathbb{Z} \cdot (1, 1)$, the arguments above and in Remark 5.3 show that this occurs if and only if $\frac{\delta(b)}{b} = \sigma(f) - f + 2c$, if and only if $\det(G_2) \subseteq \left\{ \alpha \in C^\times \mid \delta\left(\frac{\delta(\alpha)}{\alpha}\right) \right\}$, with equality if and only if $c \neq 0$, and moreover $c = 0$ if and only if $\det(G_2) = \{ \alpha \in C^\times \mid \delta(\alpha) = 0 \}$. Since G_2 has index 2 in G_1 , $\det(G_2)$ has index at most 2 in $\det(G_1)$; but since $\det(G_2)$ is divisible in either case, we see that $\det(G_2) = \det(G_1)$, concluding the proof of item (3). $\square$

7.2. Irreducible and imprimitive (2): rational system of imprimitivity

Supposing there are no solutions to (4.3) in $\bar{\mathbb{Q}}(x_2)$, and either $a = 0$ or there exists a solution $e \in \bar{\mathbb{Q}}(x)$ to (4.5), we proceed as follows. The non-existence of solutions to (4.3) in k_2 implies there are no solutions in k_∞ either, which in turn implies that the σ -Galois group H_∞ for (4.2) over k_∞ is irreducible, and since $H_\infty \subseteq H_1$, the σ -Galois group for (4.2) over k_1 , we then have that H_1 must be irreducible also.

The system (4.2) in this case is equivalent to

$$\sigma(Y) = \begin{pmatrix} 0 & 1 \\ -r & 0 \end{pmatrix} Y, \tag{7.6}$$

for some $r \in \bar{\mathbb{Q}}(x)$ as we saw in §4, which implies that H_∞ is imprimitive. Since H_∞ has finite index in H_1 , the classification of algebraic subgroups of $\mathrm{GL}_2(C)$ from [21] then

implies that H_1 must also be imprimitive, and therefore H_1 must be one of the irreducible imprimitive subgroups of $\mathrm{GL}_2(C)$ with bicyclic group of connected components listed in Lemma 7.1.

Remark 7.5. In this case, we can compute the σ -Galois group H_1 for (7.6) over k_1 from among the possibilities listed in Lemma 7.1 with the aid of Remark 7.2 by computing the diagonal subgroup $\Delta(H_1)$ and the image of the determinant $\det(H_1)$ as follows. As before, $\det(H_1) = \mu_m$, the group of m -th roots of unity, if and only if m is the smallest positive integer such that $b^m = \frac{\sigma(f)}{f}$ for some $f \in \bar{\mathbb{Q}}(x)^\times$; if there is no such m , then $\det(H_1) = \mathbb{G}_m(C)$. On the other hand, $\Delta(H_1)$ is precisely the σ^2 -Galois group for the system

$$\sigma^2(Z) = \begin{pmatrix} -r & 0 \\ 0 & -\sigma(r) \end{pmatrix} Z \quad (7.7)$$

over k_1 , which we can compute as in Proposition 5.2 and Remark 5.3 by considering k_1 as a σ^2 -field. We see that

$$\Delta(H_1) \subseteq \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \mid \alpha_1, \alpha_2 \in C^\times \right\}$$

is the subgroup defined by the following conditions on α_1 and α_2 :

- (1) $(\alpha_1 \alpha_2)^m = 1$ if and only if m is the smallest positive integer such that $(r\sigma(r))^m = \frac{\sigma^2(f)}{f}$ for some $f \in \bar{\mathbb{Q}}(x)^\times$;
- (2) otherwise $\Delta(H_1) = \mathbb{G}_m(C)^2$.

The omission of the possibility that $H_1 = \{\pm 1\}^2 \rtimes \mathbb{G}_m(C)$ as in Lemma 7.1(3) is deliberate. This is impossible under the present assumptions because $\alpha_1^2 = \alpha_2^2$ for every $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in \Delta(H_1)$ if and only if $\left(\frac{\sigma(r)}{r}\right)^2 = \frac{\sigma^2(f)}{f}$ for some $f \in \bar{\mathbb{Q}}(x)^\times$. But if we let $v \in \bar{\mathbb{Q}}(x)^\times$ such that $r\frac{\sigma(v)}{v} = ex^n\frac{p_1}{p_2}$ is reduced, with $e \in \bar{\mathbb{Q}}^\times$ such that $e \in q^\mathbb{Z}$ if and only if $e = 1$, $n \in \mathbb{Z}$, and $p_1, p_2 \in \bar{\mathbb{Q}}[x]$ monic such that $\gcd(x, p_1) = \gcd(x, p_2) = \gcd(p_1, \sigma^m(p_2))$ for every $m \in \mathbb{Z}$, we would then have that the reduced form of $\sigma(r)$ is exactly $\sigma(r)\frac{\sigma^2(v)}{\sigma(v)} = eq^n x^n \frac{\sigma(p_1)}{\sigma(p_2)}$, and therefore

$$\frac{\sigma(r)}{r} \frac{\sigma^2(v)}{v} = q^n \frac{\sigma(p_1)p_2}{p_1\sigma(p_2)}.$$

This element is not necessarily reduced with respect to σ^2 , but the reduced form of $\frac{\sigma(r)}{r}$ with respect to σ^2 is given by

$$q^\varepsilon \frac{\tilde{p}_1}{\tilde{p}_2},$$

where $\varepsilon = 0$ if n is even and $\varepsilon = 1$ if n is odd, and $\tilde{p}_1, \tilde{p}_2 \in \bar{\mathbb{Q}}[x]$ are again monic such that $\gcd(x, \tilde{p}_1) = \gcd(x, \tilde{p}_2) = \gcd(\tilde{p}_1, \sigma^{2m}(\tilde{p}_2)) = 1$ for every $m \in \mathbb{Z}$. We then have that the reduced form of $\frac{\sigma(r)}{r}$ with respect to σ^2 is $\left(\frac{\tilde{p}_1}{\tilde{p}_2}\right)^2$, and therefore $\left(\frac{\sigma(r)}{r}\right)^2 = \frac{\sigma^2(f)}{f}$ for some $f \in \bar{\mathbb{Q}}(x)^\times$ if and only if $\tilde{p}_1 = 1 = \tilde{p}_2$, but this would imply that $\frac{\sigma(r)}{r} = \frac{\sigma^2(\tilde{f})}{\tilde{f}}$ for some $\tilde{f} \in \bar{\mathbb{Q}}(x)^\times$ already, which in turn would imply that $\alpha_1 = \alpha_2$ for every $\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in \Delta(H_1)$, which is not possible according to the classification of Lemma 7.1.

In fact, we may pursue this further to conclude that it is also impossible to have

$$\frac{\delta(\sigma(r))}{\sigma(r)} - \frac{\delta(r)}{r} = \sigma^2(g) - g + c \quad (7.8)$$

for some $g \in \bar{\mathbb{Q}}(x)$ and $c \in \mathbb{Z}$. This is because if, say, $\tilde{p}_1 \neq 1$, then there would exist $\beta \in \bar{\mathbb{Q}}^\times$ such that $\tilde{p}_1(\beta) = 0$, and then we would have that

$$q^2\text{-dres}\left(\frac{\delta(\tilde{p}_1)}{\tilde{p}_1}, [\beta]_{q^2}, 1\right) \neq 0 = q^2\text{-dres}\left(\frac{\delta(\tilde{p}_2)}{\tilde{p}_2}, [\beta]_{q^2}, 1\right),$$

and similarly with the roles of $\tilde{p}_1$ and $\tilde{p}_2$ exchanged. But since

$$\frac{\delta(\sigma(r))}{\sigma(r)} - \frac{\delta(r)}{r} = \frac{\delta(\tilde{p}_1)}{\tilde{p}_1} - \frac{\delta(\tilde{p}_2)}{\tilde{p}_2}$$

modulo $(\sigma^2 - 1)(\bar{\mathbb{Q}}(x))$, we see that (7.8) is impossible unless $\tilde{p}_1 = 1 = \tilde{p}_2$, which we already ruled out above.

Having computed the σ -Galois group H_1 for (4.2) over k_1 as above, we can now compute the $\sigma\delta$ -Galois group G_1 for (4.2) over k_1 with the following result.

Proposition 7.6. *Suppose there are no solutions to (4.3) in $\bar{\mathbb{Q}}(x_2)$, and either $a = 0$ or there exists a solution to (4.5) in $\bar{\mathbb{Q}}(x)$. Then $H_1 \neq \{\pm 1\}^2 \ltimes \mathbb{G}_m(C)$ as in Lemma 7.1(3), and G_1 is the subgroup of*

$$\{\pm 1\} \ltimes \mathbb{G}_m(C)^2 = \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}, \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix} \mid \alpha_1\alpha_2 \neq 0, \lambda_1\lambda_2 \neq 0 \right\} \quad (7.9)$$

defined by the following conditions on $\alpha_1, \alpha_2, \lambda_1$, and λ_2 .

- (1) If $H_1 = D_m^-$ as in Lemma 7.1(1) or $H_1 = D_m^+$ as in Lemma 7.1(2), then $G_1 = H_1$.
- (2) If $H_1 = \{\pm 1\} \ltimes \mathbb{G}_m(C)^2$ as in Lemma 7.1(4), then:

- (a) there exist $c \in \mathbb{Z}$ and $g \in \bar{\mathbb{Q}}(x)$ such that $\frac{\delta(b)}{b} = \sigma(g) - g + c$ if and only if $\delta\left(\frac{\delta(\alpha_1)}{\alpha_1} + \frac{\delta(\alpha_2)}{\alpha_2}\right) = 0 = \delta\left(\frac{\delta(\lambda_1)}{\lambda_1} + \frac{\delta(\lambda_2)}{\lambda_2}\right)$; moreover, $c = 0$ if and only if $\delta(\alpha_1\alpha_2) = 0 = \delta(\lambda_1\lambda_2)$;

(b) otherwise, $G_1 = H_1$.

Proof. The fact that $H_1 \neq \{\pm 1\}^2 \ltimes \mathbb{G}_m(C)$ as in Lemma 7.1(3) under these conditions was already established in Remark 7.5. Let us denote by $\Delta(G_1)$ the subgroup of diagonal matrices in G_1 , which coincides with the $\sigma^2\delta$ -Galois group for (7.7) over k_1 . We may compute $\Delta(G_1)$ using the results of Proposition 5.2 and Remark 5.3. We again denote by $M \subseteq \mathbb{Z}^2$ the submodule generated by $(m_1, m_2) \in \mathbb{Z}^2$, not both zero and with $\gcd(m_1, m_2) = 1$, such that there exist $c \in \mathbb{Z}$ and $g \in \mathbb{Q}(x)$ such that

$$m_1 \frac{\delta(\sigma(r))}{\sigma(r)} + m_2 \frac{\delta(r)}{r} = \sigma^2(g) - g + c, \quad (7.10)$$

which is equivalent to

$$m_2 \frac{\delta(\sigma(r))}{\sigma(r)} + m_1 \frac{\delta(r)}{r} = \sigma^2 \left(\sigma(g) - m_1 \frac{\delta(r)}{r} \right) - \left(\sigma(g) - m_1 \frac{\delta(r)}{r} \right) + c.$$

As we saw in Remark 5.3, either $M = \{0\}$ is trivial; or $M = \mathbb{Z} \cdot (m_1, m_2)$; or $M = \mathbb{Z}^2$. But it follows from the above computation that if M is not trivial, then at least one of $(1, 1)$ or $(1, -1)$ belongs to M . But we saw in Remark 7.5 that we cannot have $(1, -1) \in M$, since the relation (7.8) is impossible. The only possibilities that remain are therefore $M = \{0\}$ or $M = \mathbb{Z} \cdot (1, 1)$.

If $M = \{0\}$, then $\Delta(G_1) = \mathbb{G}_m(C)^2$, and therefore $G_1 = H_1 = \{\pm 1\} \ltimes \mathbb{G}_m(C)^2$. Let us now suppose that $M = \mathbb{Z} \cdot (1, 1)$. Then if $H_1 = D_m^-$ as in Lemma 7.1(1) or $H_1 = D_m^+$ as in Lemma 7.1(2), then $\Delta(G_1) = \Delta(H_1)$, which implies that $G_1 = H_1$, as claimed in item (1). It remains to establish item (2) under the assumption that $M = \mathbb{Z} \cdot (1, 1)$. But here we again have that $\det(\Delta(G_1)) \subseteq \left\{ \alpha \in C^\times \mid \delta \left(\frac{\delta(\alpha)}{\alpha} \right) \right\}$ with equality if and only if $c \neq 0$ in (7.10), and moreover this $c = 0$ if and only if $\det(\Delta(G_1)) = \{\alpha \in C^\times \mid \delta(\alpha) = 0\}$. Since $\Delta(G_1)$ has finite index in G_1 and $\det(\Delta(G_1))$ is divisible in either case, we obtain that $\det(G_1) = \det(\Delta(G_1))$, which concludes the proof of item (2). $\square$

7.3. Irreducible and imprimitive (3): quadratic system of imprimitivity

Supposing there are no solutions to (4.3) in $\bar{\mathbb{Q}}(x_2)$, $a \neq 0$, and there are no solutions to (4.5) in $\bar{\mathbb{Q}}(x)$, let us now assume that there is a solution $e \in \bar{\mathbb{Q}}(x_2)$ to (4.5), and therefore the Galois conjugate $\bar{e}$ of e over $\mathbb{Q}(x)$ also satisfies (4.5), since this Riccati equation with respect to σ^2 is defined over $\bar{\mathbb{Q}}(x)$. Here again we have that the non-existence of solutions to (4.3) in $\bar{\mathbb{Q}}(x_2)$ implies that there are no solutions to (4.3) in all of k_∞ , which implies that H_∞ is irreducible as explained in §4. Since $H_\infty \subseteq H_2 \subseteq H_1$ (which again denote the σ -Galois groups for (4.2) over k_∞ , k_2 , and k_1 , respectively), we then have that H_2 and H_1 must also be irreducible. Moreover the existence of the solution $e \in k_2$ to (4.5) implies that H_∞ must be imprimitive, and since H_∞ has finite index in H_1 and in H_2 , the classification of the algebraic subgroups of $\mathrm{GL}_2(C)$ of [21] implies that H_1 and H_2

must be imprimitive also. By [26, Prop. 12.2(1)], both H_1 and H_2 must have bicyclic groups of connected components, and thus they must both be included in the list of irreducible imprimitive subgroups given in Lemma 7.1. By Corollary 4.3, $H_2 \subseteq H_1$ has index either 1 or 2. We will show that $H_2 \neq H_1$, which implies that the index of H_2 in H_1 is exactly 2. A straightforward computation shows that the only groups listed in Lemma 7.1 admitting another such group as an index-2 subgroup are $H_1 = D_m^+$ with m even, with H_2 then given by one of the groups $D_{m/2}^-$ or $D_{m/2}^+$.

To see that $H_2 \neq H_1$ in this case, recall from [11, Thm. 18] that $e \in \bar{\mathbb{Q}}(x_2)$ satisfies (4.5) if and only if $d := e + \frac{b}{a}$ has the property that $dy + \sigma(y) =: z_d$ satisfies $\sigma^2(z_d) + rz_d = 0$ with $r := -a\sigma(a) + \sigma(b) + a\sigma^2(d)$ if and only if y satisfies (4.1). We see that this is equivalent to $z_{\bar{d}} := \bar{d}y + \sigma(y)$ satisfying $\sigma^2(z_{\bar{d}}) + \bar{r}z_{\bar{d}} = 0$, where $\bar{d}$ and $\bar{r}$ denote the Galois conjugates of $d, r \in \bar{\mathbb{Q}}(x_2)$ over $\bar{\mathbb{Q}}(x)$. Since $e \neq \bar{e}$, we also have $d \neq \bar{d}$ and $r \neq \bar{r}$. At this point, we could compute H_2 directly as in Remark 7.5, where in particular the subgroup of diagonal matrices $\Delta(H_2)$ in H_2 corresponds to the σ^2 -Galois group for the system

$$\sigma^2(Y^{(2)}) = A^{(2)}Y^{(2)} \quad (7.11)$$

over k_2 , where $A^{(2)} := \sigma(A)A$. A computation shows that setting

$$T := \begin{pmatrix} d & 1 \\ \bar{d} & 1 \end{pmatrix} \in \text{GL}_2(\bar{\mathbb{Q}}(x_2))$$

we have that

$$\sigma^2(T)A^{(2)}T^{-1} = \begin{pmatrix} -r & 0 \\ 0 & -\bar{r} \end{pmatrix},$$

and therefore (7.11) is equivalent over k_2 to the system

$$\sigma^2(Z^{(2)}) = \begin{pmatrix} -r & 0 \\ 0 & -\bar{r} \end{pmatrix} Z^{(2)} \quad (7.12)$$

via the gauge transformation $Z^{(2)} = TY^{(2)}$.

If, contrary to our contention, we did have that $H_1 = H_2$, then the σ^2 -Galois group $H_1^{(2)}$ for the system (7.11) over k_1 would coincide with $\Delta(H_2)$, and in particular we would have $H_1^{(2)} = \Delta(H_1) = \Delta(H_2)$ being diagonal. We will show that this is not the case. For this, consider the system

$$\sigma^2(W) = \begin{pmatrix} A^{(2)} & 0 \\ 0 & q \end{pmatrix} W, \quad \text{with fundamental solution matrix } W = \begin{pmatrix} Y^{(2)} & 0 \\ 0 & x_2 \end{pmatrix}, \quad (7.13)$$

where $Y^{(2)}$ in turn denotes a (2×2) fundamental solution matrix for (7.11) over k_1 . Let $\tilde{H}^{(2)}$ denote the σ^2 -Galois group for the system (7.13) over k_1 . Let $\tilde{\tau} \in \tilde{H}^{(2)}$ such that

$\tilde{\tau}(x_2) = -x_2$, and let $\tau := \tilde{\tau}|_{S_1} \in H_1^{(2)}$ denote the restriction of $\tilde{\tau}$ to the σ^2 -PV ring corresponding to the system (7.11): $S_1^{(2)} := k_1[Y^{(2)}, \det(Y^{(2)})^{-1}]$. Let $M_\tau \in \mathrm{GL}_2(C)$ denote the matrix corresponding to $\tau \in H_1^{(2)}$, so that $\tau(Y^{(2)}) = Y^{(2)}M_\tau$. Since the system (7.12) is diagonal, we have that

$$TY^{(2)} = Z^{(2)} = \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix},$$

where $\sigma^2(z_1) = -rz_1$ and $\sigma^2(z_2) = -\bar{r}z_2$. But then we see that

$$\tilde{\tau}(Z^{(2)}) = \tilde{\tau}(TY^{(2)}) = \bar{T}Y^{(2)}M_\tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} Z^{(2)} M_\tau.$$

On the other hand, $\sigma^2(\tilde{\tau}(z_1)) = \tilde{\tau}(\sigma^2(z_1)) = \tilde{\tau}(-rz_1) = -\bar{r}\tilde{\tau}(z_1)$, and therefore $\tilde{\tau}(z_1) = \lambda_2 z_2$ for some $\lambda_2 \in C^\times$. Similarly we see that $\tilde{\tau}(z_2) = \lambda_1 z_1$ for some $\lambda_1 \in C^\times$, and therefore

$$\tilde{\tau}(Z^{(2)}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} Z^{(2)} \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix}.$$

This shows that $M_\tau = \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix}$, as we wanted to show.

Proposition 7.7. *Suppose there are no solutions to (4.3) in $\bar{\mathbb{Q}}(x_2)$, $a \neq 0$, and there are no solutions to (4.5) in $\bar{\mathbb{Q}}(x)$ but there exists a solution to (4.5) in $\bar{\mathbb{Q}}(x_2)$. Then $G_1 = H_1 = D_m^+$ for the smallest even positive integer $m \in 2\mathbb{N}$ such that $b^m = \frac{\sigma(f)}{f}$ for some $f \in \bar{\mathbb{Q}}(x)^\times$.*

Proof. The remarks above show that under these assumptions the σ -Galois group H_2 for (4.2) over k_1 has index exactly 2 in the σ -Galois group H_1 for (4.2) over k_1 . Thus $H_1 = D_m^+$ as in Lemma 7.1(2) for some even positive integer $m \in 2\mathbb{N}$, and H_2 is then one of $D_{m/2}^-$ or $D_{m/2}^+$. In either case, it follows from Proposition 7.6, applied over k_2 instead of k_1 , that $H_2 = G_2$ is also the $\sigma\delta$ -Galois group G_2 for (4.2) over k_2 . Since the index of G_2 in G_1 , the $\sigma\delta$ -Galois group for (4.2) over k_1 , is also $2 = [H_1 : H_2]$, it then follows that $G_1 = H_1 = D_m^+$ in this case, as claimed. $\square$

8. Irreducible and primitive groups

Let us denote again $k = C(x)$, where C is a δ -closure of $\bar{\mathbb{Q}}$, σ denotes the C -linear automorphism of k defined by $\sigma(x) = qx$, and $\delta(x) = 1$. We write H for the σ -Galois group and G for the $\sigma\delta$ -Galois group for

$$\sigma(Y) = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} Y \tag{8.1}$$

over k , where $a, b \in \bar{\mathbb{Q}}(x)$ and $b \neq 0$. In this section we consider the case where $a \neq 0$ and there are no solutions in $\bar{\mathbb{Q}}(x_2)$ to (4.3) nor to (4.5), which is equivalent to the condition that $\mathrm{SL}_2(C) \subseteq H$ by the results of [11] summarized in §4. In this case, H is reductive and the connected component of the identity H° is either $\mathrm{SL}_2(C)$ or $\mathrm{GL}_2(C)$, and in either case the derived subgroup $H^{\circ, \mathrm{der}} = \mathrm{SL}_2(C)$. Therefore by [5, Thm. 5.2] $\mathrm{SL}_2(C) \subseteq G$, and hence $G \subseteq \mathrm{GL}_2(C)$ is determined by the image the determinant map $\det(G) \subseteq \mathbb{G}_m(C)$, which is the $\sigma\delta$ -Galois group for $\sigma(y) = by$ over k . The proof of the following result is immediate.

Proposition 8.1. *Suppose there are no solutions to (4.3) in $\bar{\mathbb{Q}}(x_2)$, $a \neq 0$, and there are no solutions to (4.5) in $\bar{\mathbb{Q}}(x_2)$. Then $\det(G) \subseteq \mathbb{G}_m(C)$ is determined as follows.*

- (1) *There exist a smallest positive integer $m \in \mathbb{N}$ and $f \in \bar{\mathbb{Q}}(x)^\times$ such that $b^m = \frac{\sigma(f)}{f}$ if and only if $\det(G) = \mu_m$, the group of m -th roots of unity.*
- (2) *There exist $c \in \mathbb{Z}$ and $f \in \bar{\mathbb{Q}}(x)$ such that $\frac{\delta(b)}{b} = \sigma(f) - f + c$ if and only if $\det(G) \subseteq \left\{ \alpha \in C^\times \mid \delta\left(\frac{\delta(\alpha)}{\alpha}\right) = 0 \right\}$. Moreover, $c = 0$ if and only if this containment is proper, in which case $\det(G) = \{ \alpha \in C^\times \mid \delta(\alpha) = 0 \}$.*
- (3) *Otherwise, $\det(G) = \mathbb{G}_m(C)$.*

9. Examples

In this section we compute the $\sigma\delta$ -Galois group G associated to some concrete second-order linear difference equations

$$\sigma^2(y) + a\sigma(y) + by = 0 \quad (4.1)$$

over $\bar{\mathbb{Q}}(x)$ with respect to the q -dilation operator $\sigma(x) = qx$, where $q \in \mathbb{Q}^\times$ is not a root of unity. We will first apply the algorithm of [11] to compute the σ -Galois group H associated to the equation, and then apply our algorithm to compute G .

9.1. Example

Let us consider (4.1) with

$$b = q^3 x^6 \frac{(x-1)^4 (q^2 x^2 + 6qx + 6)}{x^2 + 6x + 6}; \quad \text{and}$$

$$a = -q^3 x^3 \frac{(2q^2)x^4 + 4(q^2 + q)x^3 + (7q^2 - 24q + 7)x^2 - 6(q+1)x + 12}{x^2 + 6x + 6}.$$

Applying the procedure in [11, §4.1] or using a computer algebra system (for example, with the QHypergeometricSolution command included in the Maple package QDifferenceEquations) one can verify that there is exactly one solution $u \in \bar{\mathbb{Q}}(x)$ to the first Riccati equation (4.3) in this case, given by

$$u := x^3(x-1)^2.$$

After computing

$$\frac{b}{u\sigma(u)} = \frac{(x-1)^2(q^2x^2 + 6qx + 6)}{(qx-1)^2(x^2 + 6x + 6)},$$

we see that

$$w := \frac{x^2 + 6x + 6}{(x-1)^2} \in \bar{\mathbb{Q}}(x)^\times$$

satisfies $\sigma(w) = \frac{b}{u\sigma(u)}w$, and therefore we are in the setting of Proposition 6.1. After verifying that

$$\frac{\delta(u)}{u} = 5 + \frac{2}{x-1} \neq \sigma(f) - f + c \quad \text{for any } f \in \bar{\mathbb{Q}}(x) \text{ and } c \in \mathbb{Z},$$

we proceed to attempt to find a linear differential operator $\mathcal{L} \in \bar{\mathbb{Q}}[\delta]$ of smallest possible order such that there exist $f \in \bar{\mathbb{Q}}(x)$ and $c \in \bar{\mathbb{Q}}$ satisfying

$$\mathcal{L}\left(\frac{\delta(u)}{u}\right) - w = \sigma(f) - f + c.$$

Since

$$w = \frac{x^2 + 6x + 6}{(x-1)^2} = \frac{5}{(x-1)^2} + \frac{8}{x-1} + 1$$

has as its only non-zero q -discrete residues:

$$q\text{-dres}(w, [1]_q, 2) = 5; \quad q\text{-dres}(w, [1]_q, 1) = 8; \quad \text{and} \quad q\text{-dres}(w, \infty) = 1,$$

we see that if there exists such an $\mathcal{L} \in \bar{\mathbb{Q}}[\delta]$ then its order must be exactly 1. Writing $\mathcal{L} = e_1\delta + e_0$, we find that

$$\mathcal{L}\left(\frac{\delta(u)}{u}\right) - w = \frac{-2e_1 - 5}{(x-1)^2} + \frac{-2e_1 + 2e_0 - 8}{x-1} + 5e_0 - 1,$$

which has the desired form $\sigma(f) - f + c$ for some $f \in \bar{\mathbb{Q}}(x)$ and $c \in \bar{\mathbb{Q}}$ if and only if

$$-2e_1 - 5 = 0 = -2e_1 + 2e_0 - 8 \iff e_1 = -\frac{5}{2} \text{ and } e_0 = \frac{3}{2}.$$

The corresponding value of $c = 5e_0 - 1 = \frac{13}{2} \neq 0$. With this, we conclude that the $\sigma\delta$ -Galois group for (4.1) over k_1 for this choice of coefficients $a, b \in \bar{\mathbb{Q}}(x)$ is

$$G = \left\{ \begin{pmatrix} \alpha & \xi \\ 0 & \alpha \end{pmatrix} \mid \alpha, \xi \in C, \alpha \neq 0, \delta\left(\frac{\xi}{\alpha}\right) = -\frac{5}{2}\delta^2\left(\frac{\delta(\alpha)}{\alpha}\right) + \frac{3}{2}\delta\left(\frac{\delta(\alpha)}{\alpha}\right) \right\}.$$

9.2. Example

Let us consider (4.1) with

$$a = -(q + q^{1/2})x \quad \text{and} \quad b = q^{1/2}(x^2 - x).$$

Since the valuations at $x = 0$ of the coefficients are $v(a) = 1$ and $v(b) = 1$, we are in the case where $v(b) \leq 2v(a)$ and $v(b)$ is odd, and therefore there are no solutions to (4.3) in $\bar{\mathbb{Q}}(x)$ (cf. [11, §4.1]). However, $u = x + x^{1/2} \in \bar{\mathbb{Q}}(x^{1/2})$ and $\bar{u} = x - x^{1/2} \in \bar{\mathbb{Q}}(x^{1/2})$ both satisfy (4.3). Since

$$\frac{\delta(b)}{b} = 2 + \frac{1}{x-1} \neq \sigma(f) - f + c \quad \text{for any } f \in \bar{\mathbb{Q}}(x) \text{ and } c \in \mathbb{Z},$$

we deduce that $\det(G) = \mathbb{G}_m(C)$. Since there is no $f \in \bar{\mathbb{Q}}(x^{1/2})^\times$ such that

$$\left(\frac{u}{\bar{u}}\right)^2 = x \left(\frac{x^{1/2} + 1}{x^{1/2} - 1}\right)^2 = \frac{\sigma(f)}{f},$$

we conclude that the $\sigma\delta$ -Galois group G for (4.1) over k_1 for this choice of coefficients $a, b \in \bar{\mathbb{Q}}(x)$ is

$$G = \{\pm 1\} \ltimes \mathbb{G}_m(C)^2 = \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}, \begin{pmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{pmatrix} \mid \alpha_1, \alpha_2, \lambda_1, \lambda_2 \in C^\times \right\}.$$

9.3. Example

Let us consider (4.1) with $a = 0$ and $b = -q^{1/2}x$. This example was discussed in [5, §4.1], as an example of a projectively integrable system whose σ -Galois group H was solvable but not abelian; in fact it was proved there using ad-hoc methods that

$$H = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}, \begin{pmatrix} 0 & \lambda \\ \lambda & 0 \end{pmatrix}, \begin{pmatrix} 0 & \lambda \\ -\lambda & 0 \end{pmatrix} \mid \alpha, \lambda \in C^\times \right\}.$$

We can now prove this systematically, as well as find the corresponding $\sigma\delta$ -Galois group G , using the results of §7.1. Since the valuations at $x = 0$ of the coefficients are $v(a) = \infty$ and $v(b) = 1$, we are in the case where $v(b) \leq 2v(a)$ and $v(b)$ is odd, and therefore there are no solutions to (4.3) in $\bar{\mathbb{Q}}(x)$ (cf. [11, §4.1]). However we see that $u = x^{1/2} \in \bar{\mathbb{Q}}(x^{1/2})$ and $\bar{u} = -u = -x^{1/2} \in \bar{\mathbb{Q}}(x^{1/2})$ both satisfy (4.3). Since $\frac{\delta(b)}{b} = 1$, we see that $\det(G) = \left\{ \alpha \in C^\times \mid \delta\left(\frac{\delta(\alpha)}{\alpha}\right) = 0 \right\}$. We also verify that $\left(\frac{u}{\bar{u}}\right) = (-1)^2 = 1$. This concludes the computation that

$$G = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}, \begin{pmatrix} 0 & \lambda \\ \lambda & 0 \end{pmatrix}, \begin{pmatrix} 0 & \lambda \\ -\lambda & 0 \end{pmatrix} \mid \alpha, \lambda \in C^\times, \right. \\ \left. \delta\left(\frac{\delta(\alpha)}{\alpha}\right) = 0 = \delta\left(\frac{\delta(\lambda)}{\lambda}\right) \right\}.$$

9.4. Example

In [16] the authors develop algorithms for desingularization of q -difference-differential operators. In [16, Example 5.2], those results were applied to study the difference equations satisfied by the *colored Jones polynomials* of several knots. In spite of the name, a colored Jones polynomial is not actually a polynomial in general, but rather consists of an infinite sequence of rational functions in $\mathbb{Q}(q)$, where q is a formal indeterminate. We refer to [16, §5] and the references therein for additional details. The second-order q -difference equation (4.1) with the following choice of coefficients is satisfied by the colored Jones polynomial (after normalization) of the knot K_{-1}^{twist} (see [16, §5, Fig. 1]):

$$a = \frac{(qx - 1)(qx + 1)(q^4x^4 - q^3x^3 - q^3x^2 - qx^2 - qx + 1)}{q^2x^2(qx^2 - 1)}$$

and

$$b = \frac{q^3x^2 - 1}{qx^2 - 1}$$

To compute the $\sigma\delta$ -Galois group for

$$y(q^2x) + a(x)y(qx) + b(x)y(x) = 0 \quad (9.1)$$

over $C(x)$, where C is a δ -closure of the δ -constant field $\overline{\mathbb{Q}(q)}$, we proceed as follows. Using the `QHypergeometricSolution` command included in the Maple package `QDifferenceEquations`, we have verified that the Riccati equations (4.3) and (4.5) do not admit any solutions in $C(x^{1/2})$. Therefore $\text{SL}_2(C) \subseteq G \subseteq H$, where H denotes the σ -Galois group, as discussed in §4 and §8. We see that

$$b = \frac{q^3x^2 - 1}{qx^2 - 1} = \frac{\sigma(qx^2 - 1)}{qx^2 - 1}.$$

Therefore, $G = \text{SL}_2(C)$ in this case.

Acknowledgments

We are thankful to the referees for their helpful comments. The authors also thank M.F. Singer for explaining to the first author the main ideas behind the proof of the essential Proposition 6.2.

References

- [1] Carlos E. Arreche, Computation of the unipotent radical of the differential Galois group for a parameterized second-order linear differential equation, Adv. Appl. Math. 57 (2014) 44–59, <https://doi.org/10.1016/j.aam.2014.03.001>.

- [2] Carlos E. Arreche, Computing the differential Galois group of a parameterized second-order linear differential equation, in: *Proceedings of ISSAC 2014*, 2014.
- [3] Carlos E. Arreche, On the computation of the parameterized differential Galois group for a second-order linear differential equation with differential parameters, *J. Symb. Comput.* 75 (2016) 25–55, <https://doi.org/10.1016/j.jsc.2015.11.006>.
- [4] Carlos E. Arreche, Computation of the difference-differential Galois group and differential relations among solutions for a second-order linear difference equation, *Commun. Contemp. Math.* 19 (6) (2017), <https://doi.org/10.1142/S0219199716500565>.
- [5] Carlos E. Arreche, Michael F. Singer, Galois groups for integrable and projectively integrable linear difference equations, *J. Algebra* 480 (2017) 423–449, <https://doi.org/10.1016/j.jalgebra.2017.02.032>.
- [6] F. Baldassarri, B. Dwork, On second order linear differential equations with algebraic solutions, *Am. J. Math.* 101 (1) (1979) 42–76.
- [7] Phyllis J. Cassidy, Differential algebraic groups, *Am. J. Math.* 94 (3) (1972) 891–954, <http://www.jstor.org/stable/2373764>.
- [8] Shaoshi Chen, Michael F. Singer, Residues and telescopers for bivariate rational functions, *Adv. Appl. Math.* 49 (2012) 111–133, <https://doi.org/10.1016/j.aam.2012.04.003>.
- [9] Thomas Dreyfus, Computing the Galois group of some parameterized linear differential equation of order two, *Proc. Am. Math. Soc.* 142 (1193–1207) (2014), <https://doi.org/10.1090/S0002-9939-2014-11826-0>.
- [10] Charlotte Hardouin, Hypertranscendence des systèmes aux différences diagonaux, *Compos. Math.* 144 (3) (2008) 565–581, <https://doi.org/10.1112/S0010437X07003430>.
- [11] Peter A. Hendriks, An algorithm for computing the standard form for second order linear q -difference equations, *J. Pure Appl. Algebra* 117–118 (1997) 331–352, [https://doi.org/10.1016/S0022-4049\(97\)00017-0](https://doi.org/10.1016/S0022-4049(97)00017-0).
- [12] Peter A. Hendriks, An algorithm determining the difference Galois group of second order linear difference equations, *J. Symb. Comput.* 26 (4) (1998) 445–461, <https://doi.org/10.1006/jsco.1998.0223>.
- [13] Charlotte Hardouin, Michael F. Singer, Differential Galois theory of linear difference equations, *Math. Ann.* 342 (2) (2008) 333–377, <https://doi.org/10.1007/s00208-008-0238-z>.
- [14] Ellis R. Kolchin, Constrained extensions of differential fields, *Adv. Math.* 12 (2) (1974) 141–170, [https://doi.org/10.1016/S0001-8708\(74\)80001-0](https://doi.org/10.1016/S0001-8708(74)80001-0).
- [15] Jerald J. Kovacic, An algorithm for solving second order linear homogeneous differential equations, *J. Symb. Comput.* 2 (1) (1986) 3–43, [https://doi.org/10.1016/S0747-7171\(86\)80010-4](https://doi.org/10.1016/S0747-7171(86)80010-4).
- [16] Christoph Koutschan, Yi Zhang, Desingularization in the q -Weyl algebra, *Adv. Appl. Math.* 97 (2018) 80–101, <https://doi.org/10.1016/j.aam.2018.02.005>.
- [17] S. Lang, On quasi algebraic closure, *Ann. Math.* 55 (2) (1952) 373–390, <https://doi.org/10.2307/1969785>.
- [18] S. Lang, *Algebra*, 3rd edition, *Graduate Texts in Mathematics*, vol. 211, Springer, 2002.
- [19] Andrey Minchenko, Alexey Ovchinnikov, Michael F. Singer, Unipotent differential algebraic groups as parameterized differential Galois groups, *J. Inst. Math. Jussieu* 13 (4) (2014) 671–700, <https://doi.org/10.1017/S1474748013000200>.
- [20] Andrey Minchenko, Alexey Ovchinnikov, Michael F. Singer, Reductive linear differential algebraic groups and the Galois groups of parameterized linear differential equations, *Int. Math. Res. Not.* 2015 (7) (2015) 1733–1793, <https://doi.org/10.1093/imrn/rnt344>.
- [21] K.A. Nguyen, M. van der Put, J. Top, Algebraic subgroups of $GL_2(\mathbb{C})$, *Indag. Math.* 19 (2) (2008) 287–297, [https://doi.org/10.1016/S0019-3577\(08\)80004-3](https://doi.org/10.1016/S0019-3577(08)80004-3).
- [22] Alexey Ovchinnikov, Differential Tannakian categories, *J. Algebra* 321 (10) (2009) 3043–3062, <https://doi.org/10.1016/j.jalgebra.2009.02.008>.
- [23] Michael F. Singer. Private correspondence, July 2015.
- [24] Reinhard Schäfer, Michael F. Singer, Consistent systems of linear differential and difference equations, *J. Eur. Math. Soc.* 21 (9) (2019) 2751–2792, <https://doi.org/10.4171/jems/891>.
- [25] Dmitry Trushin, Splitting fields and general differential Galois theory, *Sb. Math.* 201 (9) (2010) 1323–1353, <https://doi.org/10.1070/SM2010v201n09ABEH004114>.
- [26] Marius van der Put, Michael F. Singer, *Galois Theory of Difference Equations*, *Lecture Notes in Maths.*, vol. 1666, Springer-Verlag, Heidelberg, 1997.