Galois Groups of Difference Equations of Order Two on Elliptic Curves*

Thomas DREYFUS † *and Julien ROQUES* ‡

† *Université Paul Sabatier - Institut de Mathématiques de Toulouse, 18 route de Narbonne, 31062 Toulouse, France*
E-mail: *tdreyfus@math.univ-toulouse.fr*
URL: https://sites.google.com/site/thomasdreyfusmaths/

‡ *Institut Fourier, Université Grenoble 1, CNRS UMR 5582, 100 rue des Maths, BP 74, 38402 St Martin d'Hères, France*
E-mail: *Julien.Roques@ujf-grenoble.fr*
URL: www-fourier.ujf-grenoble.fr/~jroques/

Received August 06, 2014, in final form January 08, 2015; Published online January 13, 2015
http://dx.doi.org/10.3842/SIGMA.2015.003

Abstract. This paper is concerned with difference equations on elliptic curves. We establish some general properties of the difference Galois groups of equations of order two, and give applications to the calculation of some difference Galois groups. For instance, our results combined with a result from transcendence theory due to Schneider allow us to identify a large class of discrete Lamé equations with difference Galois group $\mathrm{GL}_2(\mathbb{C})$.

Key words: linear difference equations; difference Galois theory; elliptic curves

2010 Mathematics Subject Classification: 39A06; 12H10

1 Introduction

Let $\mathcal{E} \subset \mathbb{P}^2$ be the elliptic curve defined by the projectivization of the Weierstrass equation

$$y^2 = 4x^3 - g_2 x - g_3 \qquad \text{with} \quad g_2, g_3 \in \mathbb{C}. \tag{1.1}$$

We denote by $\mathcal{E}(\mathbb{C})$ the group of $\mathbb{C}$-points of $\mathcal{E}$. Its abelian group law is denoted by $\oplus$.

In this paper, we study the difference Galois groups of linear difference equations of order two on $\mathcal{E}(\mathbb{C})$ of the form:

$$\underline{y}(\underline{z} \oplus 2\underline{h}) + \underline{a}(\underline{z})\underline{y}(\underline{z} \oplus \underline{h}) + \underline{b}(\underline{z})\underline{y}(\underline{z}) = 0, \tag{1.2}$$

where $\underline{y}$ is an unknown function of the variable $\underline{z} \in \mathcal{E}(\mathbb{C})$, $\underline{h}$ is a fixed non torsion point of $\mathcal{E}(\mathbb{C})$ and $\underline{a}$, $\underline{b}$ are given rational functions on $\mathcal{E}$.

This equation can be seen as a difference equation over $\mathbb{C}$. Indeed, if $\Lambda \subset \mathbb{C}$ is a lattice of periods of $\mathcal{E}$ and if $\wp$ is the corresponding Weierstrass function, then $\mathbb{C}/\Lambda$ is identified with $\mathcal{E}(\mathbb{C})$ via the factorization through $\mathbb{C}/\Lambda$ of

$$\varphi : \ z \in \mathbb{C} \mapsto (\wp(z) : \wp'(z) : 1) \in \mathcal{E}(\mathbb{C}).$$

Pulling back the equation (1.2) via φ, which is a group morphism from $(\mathbb{C}, +)$ to $(\mathcal{E}(\mathbb{C}), \oplus)$, we obtain the following difference equation on $\mathbb{C}$:

$$y(z + 2h) + a(z)y(z + h) + b(z)y(z) = 0, \tag{1.3}$$

*This paper is a contribution to the Special Issue on Algebraic Methods in Dynamical Systems. The full collection is available at http://www.emis.de/journals/SIGMA/AMDS2014.html

where y is an unknown function of the variable $z \in \mathbb{C}$, $a := \underline{a} \circ \varphi$ and $b := \underline{b} \circ \varphi$ are Λ-periodic elliptic functions and $h \in \varphi^{-1}(\underline{h})$. So, we have the following relations between the equations (1.2) and (1.3): $\underline{z} = \varphi(z)$, $\underline{h} = \varphi(h)$ and $\underline{y}(\underline{z}) = y(z)$.

These equations are discrete counterparts of differential equations on elliptic curves, a famous example of which is Lamé differential equation

$$y''(z) = (A\wp(z) + B)y(z),$$

where $A, B \in \mathbb{C}$. The main results of this paper allow us to compute the difference Galois groups of some equations such as the discrete Lamé equation

$$\Delta_h^2 y = (A\wp(z) + B)y, \qquad \text{where} \quad \Delta_h y(z) = \frac{y(z+h) - y(z)}{h}. \tag{1.4}$$

For instance, the following theorem is a consequence of our main results combined with a result from transcendence theory due to Schneider in [31] (see also Bertrand and Masser's papers [3, 21]).

Theorem. *Assume that $\mathcal{E}$ is defined over $\overline{\mathbb{Q}}$ (i.e., $g_2, g_3 \in \overline{\mathbb{Q}}$) and that $h, A, B \in \overline{\mathbb{Q}}$ with $A \neq 0$. Then, the difference Galois group of equation (1.4) is $\mathrm{GL}_2(\mathbb{C})$.*

To be precise, the base field for the difference Galois groups considered in the present paper is not the field of Λ-periodic meromorphic functions over $\mathbb{C}$, but the field constituted of the meromorphic functions over $\mathbb{C}$ which are Λ'-periodic for some sub-lattice Λ' of Λ.

The galoisian aspects of the theory of difference equations have attracted the attention of many authors in the past years, e.g., [1, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 24, 25, 26, 27, 28, 30, 34, 35]. The calculation of the difference Galois groups of finite difference or q-difference equations of order two on $\mathbb{P}^1$ has been considered by Hendricks [18, 19] and by the second author [29]. The work of Hendricks served as a basis for the present work, but, to the best of our knowledge, the present paper is the first to consider the difference Galois groups of difference equations on a non rational variety. The study of dynamical systems on elliptic curves appears in several areas of mathematics (e.g., discrete dynamical systems, QRT maps). In particular, it is very likely that the equations considered in the present paper will arise as linearizations of discrete dynamical systems, in connection with discrete Morales–Ramis theories [5, 6]. In this context, the difference Galois groups are used to obtain non-integrability results.

This paper is organized as follows. Section 2 contains reminders and complements on difference Galois theory (for equations of arbitrary order) with a special emphasis on difference equations on elliptic curves. We insist on the fact that the base difference field for the difference Galois groups considered in the present paper is not the field of Λ-periodic elliptic functions but the field of elliptic functions which are Λ'-periodic for some sub-lattice Λ' of Λ. In Section 3, we introduce some notations related to the special functions used in this paper (theta functions, Weierstrass $\wp$-functions) and we collect some useful results. In Section 4, we study the relations between the irreducibility of the difference Galois group of equation (1.3) and the solutions of an associated Riccati-type equation. We then study this Riccati equation assuming that we have *a priori* informations on the divisors of the coefficients a and b. In Section 5, we show that there is a similar relation between the imprimitivity of the Galois group and some Riccati-type equation. Section 6 is devoted to the calculation of some difference Galois groups, including those of the discrete Lamé equations mentioned above.

2 Difference Galois theory: reminders and complements

2.1 Generalities on difference Galois theory

For details on what follows, we refer to [35, Chapter 1].

A difference ring (R,ϕ) is a ring R together with a ring automorphism $\phi : R \to R$. An ideal of R stabilized by ϕ is called a difference ideal of (R,ϕ). If R is a field then (R,ϕ) is called a difference field.

The ring of constants R^ϕ of the difference ring (R,ϕ) is defined by

$$R^\phi := \{f \in R \,|\, \phi(f) = f\}.$$

A difference ring morphism (resp. difference ring isomorphism) from the difference ring (R,ϕ) to the difference ring $(\widetilde{R},\widetilde{\phi})$ is a ring morphism (resp. ring isomorphism) $\varphi : R \to \widetilde{R}$ such that $\varphi \circ \phi = \widetilde{\phi} \circ \varphi$.

A difference ring $(\widetilde{R},\widetilde{\phi})$ is a difference ring extension of a difference ring (R,ϕ) if $\widetilde{R}$ is a ring extension of R and $\widetilde{\phi}_{|R} = \phi$; in this case, we will often denote $\widetilde{\phi}$ by ϕ. Two difference ring extensions $(\widetilde{R}_1,\widetilde{\phi}_1)$ and $(\widetilde{R}_2,\widetilde{\phi}_2)$ of a difference ring (R,ϕ) are isomorphic over (R,ϕ) if there exists a difference ring isomorphism φ from $(\widetilde{R}_1,\widetilde{\phi}_1)$ to $(\widetilde{R}_2,\widetilde{\phi}_2)$ such that $\varphi_{|R} = \mathrm{Id}_R$.

We now let (K,ϕ) be a difference field. We assume that its field of constants $C := K^\phi$ is algebraically closed and that the characteristic of K is 0.

Consider a linear difference system

$$\phi Y = AY \qquad \text{with} \quad A \in \mathrm{GL}_n(K). \tag{2.1}$$

According to [35, Section 1.1], there exists a difference ring extension (R,ϕ) of (K,ϕ) such that

1) there exists $U \in \mathrm{GL}_n(R)$ such that $\phi(U) = AU$ (such a U is called a fundamental matrix of solutions of (2.1));
2) R is generated, as a K-algebra, by the entries of U and $\det(U)^{-1}$;
3) the only difference ideals of (R,ϕ) are $\{0\}$ and R.

Such a difference ring (R,ϕ) is called a Picard–Vessiot ring for (2.1) over (K,ϕ). It is unique up to isomorphism of difference rings over (K,ϕ). It is worth mentioning that $R^\phi = C$; see [35, Lemma 1.8].

Remark 2.1. Picard–Vessiot rings are not domains in general: they are finite direct sums of domains cyclically permuted by ϕ; see [35, Corollary 1.16].

The corresponding difference Galois group G over (K,ϕ) of (2.1) is the group of K-linear ring automorphisms of R commuting with ϕ:

$$G := \{\sigma \in \mathrm{Aut}(R/K) \,|\, \phi \circ \sigma = \sigma \circ \phi\}.$$

The choice of the base field is by no way innocent. The bigger the base field is, the smaller the Galois group is.

A straightforward computation shows that, for any $\sigma \in G$, there exists a unique $C(\sigma) \in \mathrm{GL}_n(C)$ such that $\sigma(U) = UC(\sigma)$. According to [35, Theorem 1.13], one can identify G with an *algebraic* subgroup of $\mathrm{GL}_n(C)$ via the faithful representation

$$\sigma \in G \mapsto C(\sigma) \in \mathrm{GL}_n(C).$$

If we choose another fundamental matrix of solutions U, we find a conjugate representation.

Remark 2.2. Given an nth order difference equation

$$a_n\phi^n(y) + \cdots + a_1\phi(y) + a_0 y = 0, \tag{2.2}$$

with $a_0, \dots, a_n \in K$ and $a_0 a_n \neq 0$, we can consider the equivalent linear difference system

$$\phi Y = AY, \qquad \text{with} \quad A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \\ -\frac{a_0}{a_n} & -\frac{a_1}{a_n} & \dots & \dots & -\frac{a_{n-1}}{a_n} \end{pmatrix} \in \mathrm{GL}_n(K). \tag{2.3}$$

By "Galois group of the difference equation (2.2)" we mean "Galois group of the difference system (2.3)".

We shall now introduce a property relative to the difference base field, which appears in [35, Lemma 1.19].

Definition 2.3. We say that the difference field (K, ϕ) satisfies property $(\mathcal{P})$ if the following properties hold:

- the field K is a $\mathcal{C}^1$-field[1];
- if L is a finite field extension of K such that ϕ extends to a field endomorphism of L then $L = K$.

The following result is due to van der Put and Singer. We recall that two difference systems $\phi Y = AY$ and $\phi Y = BY$ with $A, B \in \mathrm{GL}_n(K)$ are isomorphic over K if and only if there exists $T \in \mathrm{GL}_n(K)$ such that $\phi(T)A = BT$.

Theorem 2.4. *Assume that (K, ϕ) satisfies property $(\mathcal{P})$. Let $K^\phi = C$. Let $G \subset \mathrm{GL}_n(C)$ be the difference Galois group over (K, ϕ) of*

$$\phi(Y) = AY, \qquad \text{with} \quad A \in \mathrm{GL}_n(K). \tag{2.4}$$

Then, the following properties hold:

- *G/G° is cyclic, where G° is the identity component of G;*
- *there exists $B \in G(K)$ such that (2.4) is isomorphic to $\phi Y = BY$ over K.*

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

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

Proof. The proof of [35, Propositions 1.20 and 1.21] in the special case where $K := C(z)$ and ϕ is the shift $\phi(f(z)) := f(z+h)$ with $h \in C^\times$, extends *mutatis mutandis* to the present case. ■

[1] Recall that K is a $\mathcal{C}^1$-field if every non-constant homogeneous polynomial P over K has a non-trivial zero provided that the number of its variables is more than its degree.

2.2 Difference equations on elliptic curves

Let $\Lambda \subset \mathbb{C}$ be a lattice. Without loss of generality, we can assume that

$$\Lambda = \mathbb{Z} + \mathbb{Z}\tau, \qquad \text{with} \quad \Im(\tau) > 0,$$

where $\Im(\cdot)$ denotes the imaginary part. For any lattice $\Lambda' \subset \mathbb{C}$, we let $\mathrm{M}_{\Lambda'}$ be the field of Λ'-periodic meromorphic functions. We denote by K the field defined by

$$K := \bigcup_{\Lambda' \text{ sub-lattice of } \Lambda} \mathrm{M}_{\Lambda'} = \bigcup_{k \geq 1} \mathrm{M}_{k\Lambda}\,.$$

Let $h \in \mathbb{C}$ such that $h \mod \Lambda$ is not a torsion point of $\mathbb{C}/\Lambda$. We endow K with the non-cyclic field automorphism ϕ defined by

$$\phi(f)(z) := f(z+h).$$

Then, (K, ϕ) is a difference field.

Proposition 2.5. *The field of constants of (K, ϕ) is*

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

Proof. Consider $f \in K^{\phi}$. Let Λ' be a sub-lattice of Λ such that $f \in \mathrm{M}_{\Lambda'}$. Note that f is Λ'-periodic (because $f \in \mathrm{M}_{\Lambda'}$) and h-periodic (because $\phi(f) = f$), so f is a $(\Lambda' + h\mathbb{Z})$-periodic meromorphic function. But $\Lambda' + h\mathbb{Z}$ has an accumulation point because $h \mod \Lambda$ is not a torsion point of $\mathbb{C}/\Lambda$. Therefore, f is constant. ■

Proposition 2.6. *The difference field (K, ϕ) satisfies property $(\mathcal{P})$ (see Definition 2.3).*

Proof. Since $K = \bigcup_{k \geq 1} \mathrm{M}_{k\Lambda}$ is the increasing union of the fields $\mathrm{M}_{k\Lambda}$, the fact that K is a $\mathcal{C}^1$-field follows from Tsen's theorem [20] (according to which the function field of any algebraic curve over an algebraically closed field, e.g., $\mathrm{M}_{k\Lambda}$, is $\mathcal{C}^1$).

Let L be a finite extension of K such that ϕ extends to a field endomorphism of L. We have to prove that $L = K$. The primitive element theorem ensures that there exists $u \in L$ such that $L = K(u)$. Let Λ' be a sub-lattice of Λ such that

- u is algebraic over $\mathrm{M}_{\Lambda'}$,
- $\phi(u) \in \mathrm{M}_{\Lambda'}(u)$.

Then, $\mathrm{M}_{\Lambda'}(u)$ is a finite extension of $\mathrm{M}_{\Lambda'}$ and ϕ induces an automorphism of $\mathrm{M}_{\Lambda'}(u)$.

Using the equivalence of categories between between smooth projective curves and function fields of dimension 1 [16, Corollary 6.12], we see that there exists a commutative diagram of the form

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ \mathbb{C}/\Lambda' & \xrightarrow[z \mapsto z+h]{} & \mathbb{C}/\Lambda' \end{array}$$

where $\varphi : X \to \mathbb{C}/\Lambda'$ is a morphism of smooth projective curves, whose induced morphism of function fields "is" the inclusion $\mathrm{M}_{\Lambda'} \subset \mathrm{M}_{\Lambda'}(u)$, and where f is an endomorphism of X, whose induced morphism on function fields "is" $\phi : \mathrm{M}_{\Lambda'}(u) \to \mathrm{M}_{\Lambda'}(u)$. Considering this commutative diagram, we see that f has degree 1 and that, if φ is ramified above $y \in \mathbb{C}/\Lambda'$, then φ is also

ramified above $y-h$. So, the set of ramification values of φ is stable by $z \mapsto z-h$. This set being finite, it has to be empty. So, φ is unramified.

Hurwitz's formula implies that X has genus 1, i.e., that X is an elliptic curve. So, there exist a lattice $\Lambda'' \subset \mathbb{C}$ and an isomorphism $\psi : \mathrm{M}_{\Lambda'}(u) \to \mathrm{M}_{\Lambda''}$. There exists $(a,b) \in \mathbb{C}^\times \times \mathbb{C}$ such that $a\Lambda'' \subset \Lambda'$ and such that the restriction $\psi_{|\mathrm{M}_{\Lambda'}}$ is given, for all $f \in \mathrm{M}_{\Lambda'}$, by $\psi(f)(z) = f(az+b)$. (Indeed, $\psi_{|\mathrm{M}_{\Lambda'}} : \mathrm{M}_{\Lambda'} \to \mathrm{M}_{\Lambda''}$ is a field morphism from the function field of the elliptic curve $\mathbb{C}/\Lambda'$ to the function field of the elliptic curve $\mathbb{C}/\Lambda''$. So, $\psi_{|\mathrm{M}_{\Lambda'}}$ is induced by a morphism from the elliptic curve $\mathbb{C}/\Lambda''$ to the elliptic curve $\mathbb{C}/\Lambda'$. Now, our claim follows from the fact that the morphisms from $\mathbb{C}/\Lambda''$ to $\mathbb{C}/\Lambda'$ are of the form $z \mod \Lambda'' \mapsto az+b \mod \Lambda'$ for some $(a,b) \in \mathbb{C}^\times \times \mathbb{C}$ such that $a\Lambda'' \subset \Lambda'$.) The commutative diagram

$$\begin{array}{ccccc} \mathrm{M}_{\Lambda'} & \hookrightarrow & \mathrm{M}_{\Lambda'}(u) & & \\ & \searrow^{v(z)\mapsto v(az+b)} & \downarrow \psi & \searrow & \\ & & \mathrm{M}_{\Lambda''} & \xrightarrow[w(z)\mapsto w(\frac{z-b}{a})]{} & \mathrm{M}_{a\Lambda''} \end{array}$$

shows that the fields $\mathrm{M}_{\Lambda'}(u)$ and $\mathrm{M}_{a\Lambda''}$ are $\mathrm{M}_{\Lambda'}$-isomorphic. But the extension $\mathrm{M}_{a\Lambda''} / \mathrm{M}_{\Lambda'}$ is Galois (indeed, this is equivalent to the fact that the corresponding morphism of smooth projective curves $\mathbb{C}/\Lambda' \to \mathbb{C}/a\Lambda''$ is Galois, and this is easily seen from the explicit description of the morphisms between these curves). Therefore, any $\mathrm{M}_{\Lambda'}$-morphism from $\mathrm{M}_{a\Lambda''}$ to $K(u)$ must leave $\mathrm{M}_{a\Lambda''}$ globally invariant. But, $\mathrm{M}_{a\Lambda''}$ and $\mathrm{M}_{\Lambda'}(u)$ are $\mathrm{M}_{\Lambda'}$-isomorphic subfields of $K(u)$. So $\mathrm{M}_{\Lambda'}(u) \subset \mathrm{M}_{a\Lambda''}$, and therefore $u \in \mathrm{M}_{a\Lambda''} \subset K$ and $L = K(u) \subset K$. ■

Corollary 2.7. *The conclusions of Theorem 2.4 are valid for (K, ϕ).*

3 Theta functions and Weierstrass $\wp$-function

3.1 Theta functions

We recall that

$$\Lambda = \mathbb{Z} + \tau\mathbb{Z} \subset \mathbb{C} \qquad \text{with} \quad \Im(\tau) > 0.$$

Let θ be the Jacobi theta function defined by

$$\theta(z) = \sum_{m\in\mathbb{Z}} (-1)^m e^{i\pi m(m-1)\tau} e^{2i\pi mz}.$$

We shall now recall some basic facts about this function. We refer to [22, Chapter I] for details and proofs.

Remark 3.1. The classical theta function is defined by $\vartheta(z,\tau) = \sum_{m\in\mathbb{Z}} e^{i\pi m^2\tau + 2i\pi mz}$. Actually, this is the function studied in [22, Chapter I]. But, there is a simple relation between θ and ϑ, namely $\theta(z) = \vartheta(z + \frac{1-\tau}{2}, \tau)$. So that any statement for ϑ can be immediately translated into a statement for θ.

We recall that θ is a 1-periodic entire function such that

$$\theta(z+\tau) = -e^{-2i\pi z}\theta(z).$$

Moreover, we have the following formula, known as Jacobi's triple product formula:

$$\theta(z) = \prod_{m=1}^{\infty} \big(1 - e^{2i\pi\tau m}\big)\big(1 - e^{2i\pi((m-1)\tau+z)}\big)\big(1 - e^{2i\pi(m\tau-z)}\big).$$

For any integer $k \geq 1$, we let θ_k be the function given by

$$\theta_k(z) := \theta(z/k).$$

This k-periodic entire function satisfies the following functional equation:

$$\theta_k(z + k\tau) = -e^{-2i\pi z/k}\theta_k(z). \tag{3.1}$$

It follows from Jacobi's triple product formula that the zeroes of θ_k are simple and that its set of zeroes is $k\Lambda$.

Let Θ_k be the set of entire functions of the form

$$c\prod_{\xi\in\mathbb{C}} \theta_k(z-\xi)^{n_\xi}$$

with $c \in \mathbb{C}^\times$ and $(n_\xi)_{\xi\in\mathbb{C}} \in \mathbb{N}^{(\mathbb{C})}$ with finite support. We denote by Θ_k^{quot} the set of meromorphic functions over $\mathbb{C}$ that can be written as quotient of two elements of Θ_k.

We define the divisor $\mathrm{div}_k(f)$ of $f \in \Theta_k^{\mathrm{quot}}$ as the following formal sum of points of $\mathbb{C}/k\Lambda$:

$$\mathrm{div}_k(f) := \sum_{\lambda\in\mathbb{C}/k\Lambda} \mathrm{ord}_\lambda(f)[\lambda],$$

where $\mathrm{ord}_\lambda(f)$ is the $(z-\xi)$-adic valuation of f, for an arbitrary $\xi \in \lambda$ (it does not depend on the chosen $\xi \in \lambda$). For any $\lambda \in \mathbb{C}/k\Lambda$ and any $\xi \in \lambda$, we set

$$[\xi]_k := [\lambda].$$

Moreover, we will write

$$\sum_{\lambda\in\mathbb{C}/k\Lambda} n_\lambda[\lambda] \leq \sum_{\lambda\in\mathbb{C}/k\Lambda} m_\lambda[\lambda]$$

if, for all $\lambda \in \mathbb{C}/k\Lambda$, $n_\lambda \leq m_\lambda$. We also introduce the weight $\omega_k(f)$ of f defined by

$$\omega_k(f) := \sum_{\lambda\in\mathbb{C}/k\Lambda} \mathrm{ord}_\lambda(f)\lambda \in \mathbb{C}/k\Lambda$$

and its degree $\deg_k(f)$ given by

$$\deg_k(f) := \sum_{\lambda\in\mathbb{C}/k\Lambda} \mathrm{ord}_\lambda(f) \in \mathbb{Z}.$$

If $f = c\prod_{\xi\in\mathbb{C}} \theta_k(z-\xi)^{n_\xi} \in \Theta_k^{\mathrm{quot}}$, then

$$\mathrm{div}_k(f) = \sum_{\xi\in\mathbb{C}} n_\xi[\xi]_k, \qquad \omega_k(f) = \sum_{\xi\in\mathbb{C}} n_\xi\xi \mod k\Lambda \qquad \text{and} \qquad \deg_k(f) = \sum_{\xi\in\mathbb{C}} n_\xi.$$

The interest of Θ_k^{quot} in our context is given by the following classical result.

Proposition 3.2. *We have*

$$\mathrm{M}_{k\Lambda}^\times \subset \Theta_k^{\mathrm{quot}}.$$

Proof. This inclusion means that any $k\Lambda$-periodic meromorphic function can be written, up to some multiplicative constant in $\mathbb{C}^\times$, as a quotient of product of functions of the form $\theta_k(z-\xi)$. This is classical, see [22, Chapter I, Section 6]. ■

We now state a couple of lemmas, which will be used freely in the rest of the paper.

Lemma 3.3. *Any* $f = c\prod_{\xi\in\mathbb{C}} \theta_k(z-\xi)^{n_\xi} \in \Theta_k^{\mathrm{quot}}$ *is* k*-periodic and satisfies*

$$f(z+k\tau) = (-1)^{\deg_k(f)} e^{2i\pi\omega} e^{-2i\pi \deg_k(f) z/k} f(z), \tag{3.2}$$

where $\omega = \sum_{\xi\in\mathbb{C}} n_\xi \xi$ *is a representative of* $\omega_k(f)$[2]*. Conversely, any non zero* k*-periodic meromorphic function* f *over* $\mathbb{C}$ *such that*

$$f(z+k\tau) = ce^{-2i\pi n z/k} f(z), \tag{3.3}$$

for some $c\in\mathbb{C}^\times$ *and* $n\in\mathbb{Z}$*, belongs to* Θ_k^{quot}*.*

Proof. The fact that any $f\in\Theta_k^{\mathrm{quot}}$ is k-periodic and satisfies the functional equation (3.2) follows from the fact that θ_k is k-periodic and satisfies the functional equation (3.1). Conversely, consider a non zero k-periodic meromorphic function f over $\mathbb{C}$ satisfying an equation of the form (3.3). Using the functional equation (3.1), we see that the k-periodic meromorphic function $g(z) = \frac{f(z)\theta_k(z-\xi)}{\theta_k(z)^n\theta_k(z)}$, where $\xi\in\mathbb{C}$ is such that $e^{-2i\pi\xi/k} = (-1)^n c$, satisfies $g(z+k\tau) = g(z)$. So g belongs to $\mathrm{M}_{k\Lambda}^\times \subset \Theta_k^{\mathrm{quot}}$, whence the result. ■

Lemma 3.4. *If* $f\in\Theta_k$ *is such that* $\deg_k(f) = 0$ *then* f *is constant.*

Proof. Consider $f\in\Theta_k$. There exists $c\in\mathbb{C}^\times$ and $(n_\xi)_{\xi\in\mathbb{C}}\in\mathbb{N}^{(\mathbb{C})}$ with finite support such that

$$f(z) = c\prod_{\xi\in\mathbb{C}} \theta_k(z-\xi)^{n_\xi}.$$

Then, $\deg_k(f) = \sum_{\xi\in\mathbb{C}} n_\xi$ is equal to 0 by hypothesis. Thus, for all $\xi\in\mathbb{C}$, $n_\xi = 0$ and hence $f = c$ is constant. ■

3.2 Weierstrass $\wp$-function

For details on what follows, we refer to [33, Chapter VI]. Recall that

$$\wp(z) := \frac{1}{z^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \in \mathrm{M}_\Lambda$$

denotes the Weierstrass elliptic function associated to the lattice Λ. For any integer $k\geq 1$, we denote by $\wp_k\in\mathrm{M}_{k\Lambda}$ the Weierstrass function defined by

$$\wp_k(z) := \wp(z/k) \in \mathrm{M}_{k\Lambda}\,.$$

This $k\Lambda$-periodic meromorphic function is an even function, its poles are of order two and its set of poles is $k\Lambda$. Therefore, its derivative $\wp_k'$ is an odd function, its poles are of order three and its set of poles is $k\Lambda$.

Any $k\Lambda$-periodic elliptic function is a rational function in $\wp_k$ and $\wp_k'$, that is

$$\mathrm{M}_{k\Lambda} = \mathbb{C}(\wp_k, \wp_k').$$

[2] It follows from this formula that f belongs to $\mathrm{M}_{k\Lambda}$ if and only if $\deg_k(f) = \sum_{\xi\in\mathbb{C}} n_\xi = 0$ and $\omega = \sum_{\xi\in\mathbb{C}} n_\xi\xi \in \mathbb{Z}$.

Lemma 3.5. *Assume that $f \in \mathrm{M}_{k\Lambda}$, seen has a meromorphic function over $\mathbb{C}/k\Lambda$, has at most N poles counted with multiplicities (or, equivalently, that $f = p/q$ with $p, q \in \Theta_k$ such that $\deg_k p, \deg_k q \leq N$). Then, there exist $A = P/Q$ and $B = R/S$ with $P, Q \in \mathbb{C}[X]$ of degree at most $2N$ and $R, S \in \mathbb{C}[X]$ of degree at most $2N + 3$ such that*

$$f = A(\wp_k) + \wp_k' B(\wp_k).$$

Proof. Using the fact that $f(z)$ belongs to $\mathrm{M}_{k\Lambda}$ if and only if $f(kz)$ belongs to M_Λ, it is easily seen that it is sufficient to prove the lemma for $k = 1$. In what follows, we see the Λ-periodic elliptic functions as meromorphic functions on $\mathbb{C}/\Lambda$. Let $A, B \in \mathbb{C}(X)$ be such that $f = A(\wp) + \wp' B(\wp)$. It follows from the formula

$$A(\wp(z)) = \frac{f(z) + f(-z)}{2}$$

that $A(\wp)$ has at most $2N$ poles counted with multiplicities in $\mathbb{C}/\Lambda$. But, if $A = P/Q$ with $\gcd(P, Q) = 1$ then $A(\wp)$ has at least $\deg Q$ poles counted with multiplicities in $\mathbb{C}/\Lambda$ (namely, the zeroes of $Q(\wp)$). So $\deg Q \leq 2N$.

Using the fact that elliptic functions have the same numbers of zeroes and poles, the same argument applied to $1/A(\wp)$ shows that $\deg P \leq 2N$.

Using the formula

$$B(\wp(z)) = \frac{f(z) - f(-z)}{2\wp'(z)},$$

similar arguments show that $\deg R \leq 2N + 3$ and $\deg S \leq 2N + 3$. ■

4 Irreducibility of the difference Galois group

We let

$$\phi^2(y) + a\phi(y) + by = 0 \qquad \text{with} \quad a \in \mathrm{M}_\Lambda \quad \text{and} \quad b \in \mathrm{M}_\Lambda^\times \tag{4.1}$$

be a difference equation of order 2 with coefficients in M_Λ and we denote by

$$\phi Y = AY \qquad \text{with} \quad A = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \in \mathrm{GL}_2(\mathrm{M}_\Lambda)$$

the associated difference system. For the notations M_Λ, ϕ, K, etc, we refer to Sections 2 and 3.

We let $G \subset \mathrm{GL}_2(\mathbb{C})$ be the difference Galois group over (K, ϕ) of equation (4.1). According to Corollary 2.7, G is an algebraic subgroup of $\mathrm{GL}_2(\mathbb{C})$ such that the quotient G/G° of G by its identity component G° is cyclic. A direct inspection of the classification, up to conjugation, of the algebraic subgroups of $\mathrm{GL}_2(\mathbb{C})$ given in [23, Theorem 4] shows that G satisfies one of the following properties:

- The group G is reducible (i.e., conjugate to some subgroup of the group of upper-triangular matrices in $\mathrm{GL}_2(\mathbb{C})$). If G is reducible, we distinguish the following sub-cases:
  - the group G is completely reducible (i.e., is conjugate to some subgroup of the group of diagonal matrices in $\mathrm{GL}_2(\mathbb{C})$);
  - the group G is not completely reducible.
- The group G is irreducible (i.e., not reducible) and imprimitive (see Section 5 for the definition).

- The group G is irreducible and is not imprimitive, and, in this case, there exists an algebraic subgroup μ of $\mathbb{C}^\times$ such that $G = \mu\,\mathrm{SL}_2(\mathbb{C})$. Therefore, $G = \{M \in \mathrm{GL}_2(\mathbb{C}) \mid \det(M) \in H\}$ where $H = \det(G) \subset \mathbb{C}^\times$. In order to determine H, one can use the fact that $H = \det(G)$ is the difference Galois group of $\phi y = (\det A)y = by$ (this follows for instance from Tannakian duality [35, Section 1.4]).

Our first task, undertaken in the present section, is to study the reducibility of G. The imprimitivity of G will be considered in Section 5.

4.1 Riccati equation and irreducibility

The non linear difference equation

$$(\phi(u) + a)u = -b \tag{4.2}$$

is called the Riccati equation associated to equation (4.1). A straightforward calculation shows that u is a solution of this equation if and only if $\phi - u$ is a right factor of $\phi^2 + a\phi + b$, whence its link with irreducibility.

In what follows, we denote by I_2 the identity matrix of $\mathrm{GL}_2(\mathbb{C})$.

Lemma 4.1. *The following statements hold:*

1. *If (4.2) has one and only one solution in K then G is reducible but not completely reducible.*
2. *If (4.2) has exactly two solutions in K then G is completely reducible but not an algebraic subgroup of $\mathbb{C}^\times I_2$.*
3. *If (4.2) has at least three solutions in K then it has infinitely many solutions in K and G is an algebraic subgroup of $\mathbb{C}^\times I_2$.*
4. *If none of the previous cases occur then G is irreducible.*

Proof. The proof of this lemma is identical to that of [19, Theorem 4.2], to whom we refer for more details.

(1) We assume that (4.2) has one and only one solution $u \in K$. A straightforward calculation shows that

$$\phi(T)AT^{-1} = \begin{pmatrix} u & * \\ 0 & b/u \end{pmatrix} \qquad \text{for} \quad T := \begin{pmatrix} 1-u & 1 \\ -u & 1 \end{pmatrix} \in \mathrm{GL}_2(K).$$

We deduce from this and from Corollary 2.7 that G is reducible.

Moreover, if G was completely reducible then, in virtue of Corollary 2.7, $\phi(T)AT^{-1}$ would be diagonal for some $T := (t_{i,j})_{1\le i,j\le 2} \in \mathrm{GL}_2(K)$. Equating the entries of the antidiagonal of $\phi(T)AT^{-1}$ with 0, we find that $-\frac{t_{21}}{t_{22}}, -\frac{t_{11}}{t_{12}} \in K$ are solutions of the Riccati equation. Since $\det(T) \neq 0$, these solutions are distinct, whence a contradiction.

(2) Assume that (4.2) has exactly two solutions $u_1, u_2 \in K$. We have

$$\phi(T)AT^{-1} = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix} \qquad \text{for} \quad T := \frac{1}{u_1 - u_2}\begin{pmatrix} -u_2 & 1 \\ -u_1 & 1 \end{pmatrix} \in \mathrm{GL}_2(K).$$

We deduce from this and from Corollary 2.7 that G is completely reducible.

Moreover, if G was an algebraic subgroup of $\mathbb{C}^\times I_2$ then, according to Corollary 2.7, there would exist $u \in K$ and $T = (t_{i,j})_{1\le i,j\le 2} \in \mathrm{GL}_2(K)$ such that

$$\phi(T)AT^{-1} = uI_2.$$

This equality implies that t_{21} and t_{22} are non zero and that, for all $c, d \in \mathbb{C}$ with $ct_{2,2}+dt_{1,2} \neq 0$,

$$-\frac{ct_{21}+dt_{11}}{ct_{22}+dt_{12}} \in K$$

is a solution of (4.2). It is easily seen that we get in this way infinitely many solutions of the Riccati equation, this is a contradiction.

(3) Assume that (4.2) has at least three solutions $u_1, u_2, u_3 \in K$. The proof of assertion (2) of the present lemma shows that $\phi Y = AY$ is isomorphic over K to $\phi Y = \begin{pmatrix} u_i & 0 \\ 0 & u_j \end{pmatrix} Y$ for all $1 \leq i < j \leq 3$. Therefore, there exists $T \in \mathrm{GL}_2(K)$ such that

$$\phi(T) \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix} = \begin{pmatrix} u_1 & 0 \\ 0 & u_3 \end{pmatrix} T.$$

Equating the second columns in this equality, we see that there exists $f \in K^\times$ such that either $u_1 = \frac{\phi f}{f} u_2$ or $u_3 = \frac{\phi f}{f} u_2$; up to renumbering, one can assume that the former case holds true. It follows that $\phi Y = AY$ is isomorphic over K to

$$\phi Y = (u_1 I_2) Y$$

and, according to Corollary 2.7, G is an algebraic subgroup of $\mathbb{C}^\times I_2$. We have shown during the proof of statement (2) that this implies that the Riccati equation (4.2) has infinitely many solutions in K.

(4) Assume that G is reducible. According to Corollary 2.7, there exists $T = (t_{i,j})_{1 \leq i,j \leq 2} \in \mathrm{GL}_2(K)$ such that $\phi(T) A T^{-1}$ is upper triangular. Then $t_{22} \neq 0$ and $-\frac{t_{21}}{t_{22}} \in K$ is a solution of the Riccati equation (4.2). This proves claim (4). ■

In the proof of the previous lemma, we have shown the following result, which we state independently for ease of reference.

Lemma 4.2. *The following properties are equivalent:*

- *The Riccati equation (4.2) has at least three solutions in K.*
- *The Riccati equation (4.2) has infinitely many solutions in K.*
- *The difference Galois group G is a subgroup of $\mathbb{C}^\times I_2$.*
- *There exist $u \in K^\times$ and $T \in \mathrm{GL}_2(K)$ such that $\phi(T) A T^{-1} = u I_2$.*

We shall now state and prove one more lemma.

Lemma 4.3. *Let $\Lambda'' \subset \Lambda'$ be sublattices of Λ such that the quotient Λ'/Λ'' is cyclic. Assume that there exist $u \in \mathrm{M}_{\Lambda''}^\times$ and $T \in \mathrm{GL}_2(\mathrm{M}_{\Lambda''})$ such that*

$$\phi(T) A T^{-1} = u I_2. \tag{4.3}$$

Then, the Riccati equation (4.2) has at least two distinct solutions in $\mathrm{M}_{\Lambda'}$.

Proof. The Galois extension $\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'}$ is cyclic of order $k := [\mathrm{M}_{\Lambda''} : \mathrm{M}_{\Lambda'}]$. Its Galois group $\mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$ is generated by the field automorphism σ_1 given by $\sigma_1(f(z)) = f(z+\lambda')$, where $\lambda' \in \Lambda'$ is a representative of a generator of Λ'/Λ''. Note that the action of $\mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$ on $\mathrm{M}_{\Lambda''}$ commutes with the action of ϕ. Applying σ_1 to equation (4.3), we get

$$\phi(\sigma_1(T)) A \sigma_1(T)^{-1} = \sigma_1(u) I_2,$$

so

$$\phi(S)u = \sigma_1(u)S, \qquad \text{with} \quad S := \sigma_1(T)T^{-1} \in \mathrm{GL}_2(\mathrm{M}_{\Lambda''}).$$

It follows that there exists $g_{\sigma_1} \in \mathrm{M}_{\Lambda''}^\times$ (namely, one of the non zero entries of S) such that

$$\sigma_1(u) = \frac{\phi(g_{\sigma_1})}{g_{\sigma_1}} u.$$

Consider the norm

$$\mathrm{N} := \mathrm{N}_{\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'}}(g_{\sigma_1}) = \prod_{\sigma \in \mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})} \sigma(g_{\sigma_1}) \in \mathrm{M}_{\Lambda'}^\times .$$

We have

$$\phi(\mathrm{N}) = \prod_{\sigma \in \mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})} \sigma\left(\frac{\sigma_1(u) g_{\sigma_1}}{u}\right) = \prod_{\sigma \in \mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})} \sigma(g_{\sigma_1}) = \mathrm{N},$$

so $\mathrm{N} = c \in (K^\phi)^\times = \mathbb{C}^\times$. Up to replacing g_{σ_1} by $g_{\sigma_1} c^{-1/k}$, we may assume that

$$\mathrm{N}_{\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'}}(g_{\sigma_1}) = 1.$$

Hilbert's 90 theorem [32, Section X.1] ensures that there exists $m \in \mathrm{M}_{\Lambda''}^\times$ such that

$$g_{\sigma_1} = \frac{m}{\sigma_1(m)}.$$

For any $\sigma = \sigma_1^j \in \mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$, we set

$$g_\sigma := g_{\sigma_1} \sigma_1(g_{\sigma_1}) \cdots \sigma_1^{j-1}(g_{\sigma_1}) = m/\sigma(m) \in \mathrm{M}_{\Lambda''}^\times;$$

we have

$$\sigma(u) = \frac{\phi(g_\sigma)}{g_\sigma} u.$$

It follows that

$$\widetilde{u} := \frac{\phi(m)}{m} u$$

is invariant under the action of $\mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$ and hence belongs to $\mathrm{M}_{\Lambda'}^\times$. We have

$$\phi\left(T'\right) A \left(T'\right)^{-1} = \widetilde{u} I_2, \qquad \text{with} \quad T' := mT \in \mathrm{GL}_2(\mathrm{M}_{\Lambda''}).$$

Applying $\sigma \in \mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$ to this equality, we get

$$\phi\left(\sigma(T')\right) A \left(\sigma(T')\right)^{-1} = \widetilde{u} I_2.$$

It follows that the matrix

$$C_\sigma := T' \sigma(T')^{-1} \in \mathrm{GL}_2(\mathrm{M}_{\Lambda''})$$

satisfies $\phi(C_\sigma) = C_\sigma$ and, hence, that its entries belong to $K^\phi = \mathbb{C}$. Moreover, $\sigma \mapsto C_\sigma$ is a 1-cocyle for the natural action of $\mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$ on $\mathrm{GL}_2(\mathbb{C})$ but this action is trivial so $\sigma \mapsto C_\sigma$ is a group morphism from $\mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$ to $\mathrm{GL}_2(\mathbb{C})$. Since $\mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$ is cyclic,

this implies that there exists $P \in \mathrm{GL}_2(\mathbb{C})$ such that, for all $\sigma \in \mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$, the matrix $D_\sigma := P^{-1}C_\sigma^{-1}P \in \mathrm{GL}_2(\mathbb{C})$ is diagonal. We have, for all $\sigma \in \mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$,

$$\sigma(T'') = D_\sigma T'', \qquad \text{where} \quad T'' = (t''_{i,j})_{1\le i,j\le 2} := P^{-1}T' \in \mathrm{GL}_2(\mathrm{M}_{k\Lambda}).$$

It follows that $u_1 := \frac{-t''_{11}}{t''_{12}}$ and $v_1 := \frac{-t''_{21}}{t''_{22}}$ are invariant by the action of $\mathrm{Gal}(\mathrm{M}_{\Lambda''} \,|\, \mathrm{M}_{\Lambda'})$ and hence belong to $\mathrm{M}_{\Lambda'}$. But u_1 and v_1 are solutions of the Riccati equation (4.2) (this was already used in the proof of assertion (2) of Lemma 4.1). So u_1 and v_1 are solutions in $\mathrm{M}_{\Lambda'}$ of the Riccati equation (4.2). ■

We now come to the main result of this subsection.

Theorem 4.4. *The following statements hold:*

1. *The Galois group G is reducible if and only if the Riccati equation (4.2) has at least one solution in $\mathrm{M}_{2\Lambda}$.*
2. *The Galois group G is completely reducible if and only if the Riccati equation (4.2) has at least two solutions in $\mathrm{M}_{2\Lambda}$.*

Proof. In virtue of Lemma 4.1, it is sufficient to prove that:

(a) If the Riccati equation (4.2) has a unique solution in K, then it belongs to M_Λ.

(b) If the Riccati equation (4.2) has exactly two solutions in K, then they belong to $\mathrm{M}_{2\Lambda}$.

(c) If the Riccati equation (4.2) has at least three solutions in K, then the Riccati equation (4.2) has at least two solutions in $\mathrm{M}_{2\Lambda}$.

(a) Assume that the Riccati equation (4.2) has a unique solution u in K. Since $u(z)$, $u(z+1)$ and $u(z+\tau)$ are solutions of (4.2), we get

$$u(z) = u(z+1) = u(z+\tau)$$

and hence $u \in \mathrm{M}_\Lambda$.

(b) Assume that the Riccati equation (4.2) has exactly two solutions in K and let $u \in K$ be one of these solutions. Since $u(z)$, $u(z+1)$ and $u(z+2)$ are solutions of (4.2), we get $u(z+2) = u(z)$. Similarly, we have $u(z+2\tau) = u(z)$. So $u \in \mathrm{M}_{2\Lambda}$.

(c) What follows is inspired by [19, Theorem 4.2], but is a little bit subtler. Assume that the Riccati equation (4.2) has at least three solutions in K. According to Lemma 4.2, there exist $u \in K$ and $T = (t_{i,j})_{1\le i,j\le 2} \in \mathrm{GL}_2(K)$ such that

$$\phi(T)AT^{-1} = uI_2. \tag{4.4}$$

Let $k \in \mathbb{N}^*$ be such that the entries of T and u belong to $\mathrm{M}_{k\Lambda}$. Consider the following field extensions:

$$\mathrm{M}_\Lambda \subset L \subset \mathrm{M}_{k\Lambda}, \qquad \text{with} \quad L := \mathrm{M}_{\mathbb{Z}+k\tau\mathbb{Z}}\,.$$

Applying Lemma 4.3 to the extension $\mathrm{M}_{k\Lambda}\,|L$ and to the equation (4.4), we get that the Riccati equation (4.2) has two distinct solution u_1 and v_1 in L. If both of them belong to $\mathrm{M}_{2\Lambda}$ then the proof is completed. Otherwise, up to renumbering, we can assume that $u_1 \notin \mathrm{M}_{2\Lambda}$, i.e., that u_1 is not 2τ-periodic. Then

$$u_1(z), u_2(z) := u_1(z+\tau) \qquad \text{and} \qquad u_3(z) := u_1(z+2\tau)$$

are distinct solutions in L of the Riccati equation. For all integers $i, j \in \{1,2,3\}$ with $i<j$ we set $T_{i,j} := \frac{1}{u_i-u_j}\begin{pmatrix} -u_j & 1 \\ -u_i & 1 \end{pmatrix} \in \mathrm{GL}_2(L)$ and we have

$$\phi(T_{i,j})A(T_{i,j})^{-1} = \begin{pmatrix} u_i & 0 \\ 0 & u_j \end{pmatrix}$$

(this was already used in the proof of assertion (2) of Lemma 4.1). Therefore,

$$\phi\big(T_{1,3}(T_{1,2})^{-1}\big)\begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix} = \begin{pmatrix} u_1 & 0 \\ 0 & u_3 \end{pmatrix} T_{1,3}(T_{1,2})^{-1}.$$

Equating the second columns in this equality, we see that there exists $f \in L^\times$ such that either $u_1 = \frac{\phi f}{f} u_2$ or $u_3 = \frac{\phi f}{f} u_2$; up to renumbering, we may assume that the former equality holds true. Then, we have

$$\phi\big(\widetilde{T}\big)A\widetilde{T}^{-1} = u_1 I_2 \tag{4.5}$$

with

$$u_1 \in L^\times \qquad \text{and} \qquad \widetilde{T} := \begin{pmatrix} 1 & 0 \\ 0 & f \end{pmatrix} T_{1,2} \in \mathrm{GL}_2(L).$$

Applying Lemma 4.3 to the extension $L|\,\mathrm{M}_\Lambda$ and to the equation (4.5), we see that the Riccati equation (4.2) has 2 distinct solutions in M_Λ. This concludes the proof. ■

4.2 On the solutions of the Riccati equation

We refer to Section 3.1 for the notations (div_k, $\deg_k$, ω_k, etc.) used in this subsection. Let $k \geq 1$ be an integer. Consider $p_1 \in \Theta_k \cup \{0\}$ and $p_2, p_3 \in \Theta_k$ such that

$$a = \frac{p_1}{p_3} \qquad \text{and} \qquad b = \frac{p_2}{p_3}.$$

We let $u \in \mathrm{M}_{k\Lambda}$ be a potential solution of the Riccati equation (4.2).

Proposition 4.5. *We have*

$$u = \frac{\phi(r)}{r}\frac{p}{q}$$

for some $p, q, r \in \Theta_k$ such that

(*i*) $\mathrm{div}_k(p) \leq \mathrm{div}_k(p_2)$,
(*ii*) $\mathrm{div}_k(q) \leq \mathrm{div}_k(\phi^{-1}(p_3))$,
(*iii*) $\deg_k(p) = \deg_k(q)$,
(*iv*) $\omega_k(p/q) = \deg_k(r)h \mod k\Lambda$.

Proof. In what follows, the greatest common divisors (gcd) has to be understood in the ring $\mathcal{O}(\mathbb{C})$ of entire functions[3]. Let $p_4, p_5 \in \Theta_k$, with $\gcd(p_4, p_5) = 1$, be such that $u = p_4/p_5$. Let $r \in \Theta_k$ be a greatest common divisor of $\phi^{-1}(p_4)$ and p_5 and consider

$$p := \frac{p_4}{\phi(r)} \in \Theta_k \qquad \text{and} \qquad q := \frac{p_5}{r} \in \Theta_k.$$

[3]According to [17], any finitely generated ideal of $\mathcal{O}(\mathbb{C})$ is principal, whence the existence of the greatest common divisor of any couple of elements of $\mathcal{O}(\mathbb{C})$. Such a greatest common divisor is unique up to multiplication by an unit of $\mathcal{O}(\mathbb{C})$.

By construction, we have

$$u = \frac{\phi r}{r}\frac{p}{q}$$

with $\gcd(p, \phi(q)) = \gcd(\phi(r)p, rq) = 1$. Then, the Riccati equation (4.2) becomes

$$p_3 \frac{\phi r}{r}\frac{p}{q}\phi\left(\frac{\phi r}{r}\frac{p}{q}\right) + p_1 \frac{\phi r}{r}\frac{p}{q} = -p_2,$$

i.e.,

$$p_3\phi^2(r)p\phi(p) + p_1\phi(r)p\phi(q) = -p_2 rq\phi(q).$$

It is now easily seen that p divides p_2 and that q divides $\phi^{-1}(p_3)$ in $\mathcal{O}(\mathbb{C})$. In terms of divisors, this is exactly (i) and (ii).

According to Lemma 3.3, we have

$$\frac{p}{q}(z + k\tau) = (-1)^{\deg_k(p/q)} e^{2i\pi\omega/k} e^{-2i\pi \deg_k(p/q) z/k} \frac{p}{q}(z)$$

for some representative ω of $\omega_k(p/q)$, and

$$\frac{\phi(r)}{r}(z + k\tau) = e^{-2i\pi \deg_k(r) h/k} \frac{\phi(r)}{r}(z).$$

Therefore

$$u(z + k\tau) = (-1)^{\deg_k(p/q)} e^{2i\pi\omega/k} e^{-2i\pi \deg_k(p/q) z/k} e^{-2i\pi \deg_k(r) h/k} u(z).$$

But $u \in \mathrm{M}_{k\Lambda}$, so $u(z + k\tau) = u(z)$ and, hence,

$$(-1)^{\deg_k(p/q)} e^{2i\pi\omega/k} e^{-2i\pi \deg_k(p/q) z/k} e^{-2i\pi \deg_k(r) h/k} = 1.$$

Hence $\deg_k(p/q) = 0$ and $\omega = \deg_k(r)h \mod k\Lambda$. This proves (iii) and (iv). ■

We will see in Section 6.1 that Proposition 4.5 is a useful theoretic tool in order to determine the difference Galois groups of families of equations, such as the discrete Lamé equations mentioned in the introduction.

We shall now conclude this section with a few words about Proposition 4.5.

Remark 4.6. How to use Proposition 4.5 in order to decide whether G is irreducible? Theorem 4.4 ensures that G is irreducible if and only if the Riccati equation (4.2) has a solution $u \in \mathrm{M}_{2\Lambda}$; we let p, q, r be as in Proposition 4.5. Assertions (i) and (ii) of Proposition 4.5, show that there are *finitely* many explicit possibilities for the divisors $\mathrm{div}_2(p)$ and $\mathrm{div}_2(q)$. But $\deg_2(r)$ is entirely determined by these divisors in virtue of (iv) of Proposition 4.5. So, we can compute an integer $N \geq 0$ such that if the Riccati equation (4.2) has a solution $u \in \mathrm{M}_{2\Lambda}$, then

$$u = p_0/q_0$$

with $p_0, q_0 \in \Theta_2$ such that $\deg_2(p_0) \leq N$ and $\deg_2(q_0) \leq N$. Lemma 3.5 ensures that

$$u = A(\wp_2) + \wp_2' B(\wp_2)$$

for some $A = P/Q$ and $B = R/S$ with $P, Q \in \mathbb{C}[X]$ of degree at most $2N$ and $R, S \in \mathbb{C}[X]$ of degree at most $2N + 3$.

So, in order to determine whether or not the Riccati equation (4.2) has at least one solution in $\mathrm{M}_{2\Lambda}$, we are lead to the following question: do there exist $A = P/Q$ and $B = R/S$ with $P, Q \in \mathbb{C}[X]$ of degree at most $2N$ and $R, S \in \mathbb{C}[X]$ of degree at most $2N+3$ such that $u = A(\wp_2) + \wp_2' B(\wp_2)$ is a solution of the Riccati equation (4.2)? Substituting $u = A(\wp_2) + \wp_2' B(\wp_2)$ in the Riccati equation (4.2) and using the addition formula:

$$\wp_2(z) + \wp_2(h) + \wp_2(z+h) = \frac{1}{4}\left(\frac{\wp_2'(z) - \wp_2'(h)}{\wp_2(z) - \wp_2(h)}\right)^2,$$

we are lead to decide whether multivariate polynomials, whose indeterminates are the coefficients of P, Q, R and S, have a common complex solution. This can be decided by using Gröbner bases.

Note however that, in order to make this method an effective tool, we have to know the divisors of a and b, and to be able to deduce $\deg_k(r)$ from assertion (iv) of Proposition 4.5.

5 Imprimitivity of the difference Galois group

We want to determine whether G is imprimitive, that is whether G is conjugate to a subgroup of

$$\left\{\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix} \mid \alpha, \beta \in \mathbb{C}^\times\right\} \bigcup \left\{\begin{pmatrix}0 & \gamma\\ \delta & 0\end{pmatrix} \mid \gamma, \delta \in \mathbb{C}^\times\right\}.$$

Theorem 5.1. *Assume that G is irreducible and that $a \neq 0$. Then, G is imprimitive if and only if there exists $u \in \mathrm{M}_{2\Lambda}$ such that*

$$\left(\phi^2(u) + \left(\phi^2\left(\frac{b}{a}\right) - \phi(a) + \frac{\phi(b)}{a}\right)\right) u = -\frac{\phi(b)b}{a^2}. \tag{5.1}$$

Proof. Arguing exactly as in [19, Theorem 4.6], we get that G is imprimitive if and only if equation (5.1) has a solution in K. But this is a Riccati-type equation, with ϕ replaced by ϕ^2. Therefore, the assertions (a), (b) and (c) given at the beginning of the proof of Theorem 4.4 allow us to conclude. ■

Remark 5.2. If $a = 0$ then G is imprimitive in virtue of Corollary 2.7.

Note that Proposition 4.5 can be used in order to find restrictions on the solutions of the above Riccati-type equation, but with ϕ replaced by ϕ^2.

6 Applications

We recall that $h \in \mathbb{C}$ is such that $h \mod \Lambda$ is not a torsion point of $\mathbb{C}/\Lambda$, i.e., that the corresponding point $\underline{h}$ of $\mathcal{E}(\mathbb{C})$ is not a torsion point.

6.1 A discrete version of Lamé equation

Let us consider the difference equation

$$\Delta_h^2 y = (A\wp(z) + B)y, \qquad \text{where} \quad \Delta_h y(z) = \frac{y(z+h) - y(z)}{h} \tag{6.1}$$

and $A, B \in \mathbb{C}$. This is a discrete version of the so-called Lamé differential equation

$$y''(z) = (A\wp(z) + B)y(z).$$

Theorem 6.1. *Assume that $\mathcal{E}$ is defined over $\overline{\mathbb{Q}}$ (i.e., $g_2, g_3 \in \overline{\mathbb{Q}}$) and that $h, A, B \in \overline{\mathbb{Q}}$ with $A \neq 0$. Then, the difference Galois group over (K, ϕ) of equation (6.1) is $\mathrm{GL}_2(\mathbb{C})$.*

A straightforward calculation shows that equation (6.1) can be rewritten as follows:

$$\phi^2 y - 2\phi y + \big(-Ah^2 \wp(z) - Bh^2 + 1\big) y = 0.$$

We will deduce Theorem 6.1 from the following theorem combined with a transcendence result due to Schneider.

Theorem 6.2. *Consider $a \in \mathbb{C}^\times$ and $b(z) = \alpha\wp(z) + \beta$ with $(\alpha, \beta) \in \mathbb{C}^\times \times \mathbb{C}$. Let $z_0 \in \mathbb{C}$ be such that $\wp(z_0) = -\beta/\alpha$.[4] If $\mathbb{Z}h \cap (\ell z_0 + \Lambda) = \{0\}$ for all $\ell \in \{-8, \dots, 8\}$ (this holds in particular if $\mathbb{Z}h \cap (\mathbb{Z}z_0 + \Lambda) = \{0\}$) then the difference Galois group over (K, ϕ) of $\phi^2 y + a\phi y + by = 0$ is $\mathrm{GL}_2(\mathbb{C})$.*

Proof of Theorem 6.2. For the notations, div_k, $[\cdot]_k$, etc, we refer to Section 3.1. Note that

$$\mathrm{div}_1(b) = [z_0]_1 + [-z_0]_1 - 2[0]_1.$$

So, we can write $a = \frac{p_1}{p_3}$ and $b = \frac{p_2}{p_3}$ for some $p_1, p_2, p_3 \in \Theta_1$ with

$$\mathrm{div}_1(p_2) = [z_0]_1 + [-z_0]_1$$

and

$$\mathrm{div}_1(p_3) = 2[0]_1.$$

We claim that G is irreducible, i.e., in virtue of Theorem 4.4, that the Riccati equation

$$(\phi(u) + a)u = -b \tag{6.2}$$

does not have any solution in $\mathrm{M}_{2\Lambda}$. Suppose to the contrary that it has a solution $u \in \mathrm{M}_{2\Lambda}$. Proposition 4.5 ensures that there exist $p, q, r \in \Theta_2$ such that

$$u = \frac{\phi(r)}{r}\frac{p}{q}$$

and

(i) $\mathrm{div}_2(p) \leq \sum_{\ell_1,\ell_2 \in \{0,1\}} [\ell_1 + \ell_2\tau - z_0]_2 + [\ell_1 + \ell_2\tau + z_0]_2$,

(ii) $\mathrm{div}_2(q) \leq \sum_{\ell_1,\ell_2 \in \{0,1\}} 2[\ell_1 + \ell_2\tau + h]_2$,

(iii) $\deg_2(p) = \deg_2(q)$,

(iv) $\omega_2(p/q) = \deg_2(r)h \mod 2\Lambda$.

Properties (i) and (ii) above imply that

$$\omega_2\left(p/q\right) = \ell z_0 - \deg_2(q)h \mod \Lambda$$

for some $\ell \in \{-4, \dots, 4\}$. We infer from this and from (iv) that

$$(\deg_2(r) + \deg_2(q))h = \ell z_0 \mod \Lambda.$$

[4] Any non constant elliptic function $f(z)$ has at least one zero (otherwise, $1/f(z)$ would be an entire elliptic function and hence would be constant). In particular, $\wp(z) + \beta/\alpha$ has a least one zero in $\mathbb{C}$.

The assumption on z_0 ensures that $\deg_2(r) = \deg_2(q) = 0$. It follows from (iii) that $\deg_2(p) = 0$ and hence u is a constant. But it is easily seen that equation (6.2) does not have any constant solution; this proves our claim.

We claim that G is not imprimitive, i.e., in virtue of Theorem 5.1, that

$$\left(\phi^2(u) + \frac{\phi^2(b)}{a} - a + \frac{\phi(b)}{a}\right) u = -\frac{\phi(b)b}{a^2} \tag{6.3}$$

does not have any solution in $\mathrm{M}_{2\Lambda}$. Suppose to the contrary that it has a solution $u \in \mathrm{M}_{2\Lambda}$. Equation (6.3) is of the form:

$$u\left(\phi^2(u) + \frac{p_1}{p_3}\right) = \frac{p_2}{p_3},$$

for some $p_1, p_2, p_3 \in \Theta_1$ with

$$\mathrm{div}_1(p_2) = 2[-2h]_1 + [z_0]_1 + [-z_0]_1 + [z_0 - h]_1 + [-z_0 - h]_1$$

and

$$\mathrm{div}_1(p_3) = 2[-2h]_1 + 2[-h]_1 + 2[0]_1.$$

We apply Proposition 4.5 with ϕ replaced by ϕ^2 to obtain the existence of $p, q, r \in \Theta_2$ such that

$$u = \frac{\phi^2(r)}{r}\frac{p}{q},$$

where

(v)
$$\mathrm{div}_2(p) \le \sum_{\ell_1,\ell_2\in\{0,1\}} 2[\ell_1 + \ell_2\tau - 2h]_2 + [\ell_1 + \ell_2\tau + z_0]_2 + [\ell_1 + \ell_2\tau - z_0]_2 + [\ell_1 + \ell_2\tau + z_0 - h]_2 + [\ell_1 + \ell_2\tau - z_0 - h]_2,$$

(vi) $\mathrm{div}_2(q) \le \sum_{\ell_1,\ell_2\in\{0,1\}} 2[\ell_1 + \ell_2\tau]_2 + 2[\ell_1 + \ell_2\tau + h]_2 + 2[\ell_1 + \ell_2\tau + 2h]_2,$

(vii) $\deg_2(p) = \deg_2(q),$

(viii) $\omega_2(p/q) = 2\deg_2(r)h \mod 2\Lambda.$

We claim that

(v′) $\mathrm{div}_2(p) \le \sum_{\ell_1,\ell_2\in\{0,1\}} [\ell_1 + \ell_2\tau + z_0]_2 + [\ell_1 + \ell_2\tau - z_0]_2,$

(vi′) $\mathrm{div}_2(q) \le \sum_{\ell_1,\ell_2\in\{0,1\}} 2[\ell_1 + \ell_2\tau]_2.$

Indeed, otherwise, arguing as for the proof of the irreducibility of G, we see that (v), (vi) and (viii) would lead to a relation of the form

$$(2\deg_2(r) + d)h = \ell z_0 \mod \Lambda$$

for some integer $\ell \in \{-8, \dots, 8\}$ and some integer $d > 0$ and this would contradict our assumption on z_0. Then, (viii) shows that

$$2\deg_2(r)h = \ell z_0 \mod \Lambda$$

for some integer $\ell \in \{-4, \dots, 4\}$ and hence $\deg_2(r) = 0$. Therefore, $u = p/q$ with $p, q \in \Theta_2$ satisfying (v′) and (vi′) above. Now remark that

$$\phi^2(u) + \frac{\phi^2(b)}{a} - a + \frac{\phi(b)}{a}$$

does not have poles in Λ. But any element of Λ is a pole of order 2 of the right hand side of equation (6.3), so any element of Λ is a pole of order at least 2 of u. It follows that (vi′) is an equality. Then, using (vii), we see that (v′) is also an equality.

So $\mathrm{div}_2(u) = \mathrm{div}_2(b)$ and hence $u = cb$ for some $c \in \mathbb{C}^\times$. We now plug $u = cb$ into equation (6.3) and we get:

$$c\left(\left(c + \frac{1}{a}\right)\phi^2(b) - a + \frac{\phi(b)}{a}\right) = -\frac{\phi(b)}{a^2}.$$

Since $-2h$ is a pole of $\phi^2(b)$ but not of $\phi(b)$, we get $c = -1/a$ and the above equation simplifies as follows:

$$\frac{-1}{a}\left(-a + \frac{\phi(b)}{a}\right) = -\frac{\phi(b)}{a^2}.$$

This gives $1 = 0$, whence a contradiction.

Therefore, G is irreducible and not imprimitive. So, as explained at the beginning of Section 4, $G = \{M \in \mathrm{GL}_2(\mathbb{C}) \mid \det(M) \in H\}$ where $H \subset \mathbb{C}^\times$ is the Galois group of $\phi y = by$, which is easily seen to be the multiplicative group $(\mathbb{C}^\times, \cdot)$. This concludes the proof. ■

Proof of Theorem 6.1. In virtue of Theorem 6.2, it is sufficient to prove that $\mathbb{Z}h \cap (\mathbb{Z}z_0 + \Lambda) = \{0\}$. Consider $m_1, m_2 \in \mathbb{Z}$ and $\lambda \in \Lambda$ such that $m_1 h = m_2 z_0 + \lambda$. We have $\wp(z_0) = \frac{-Bh^2+1}{Ah^2} \in \overline{\mathbb{Q}}$. It follows that either $m_2 z_0 + \lambda \in \Lambda$ or $\wp(m_2 z_0 + \lambda) \in \overline{\mathbb{Q}}$. (Indeed, suppose that $m_2 z_0 + \lambda \notin \Lambda$. Using equation (1.1), we see that $\wp'(z_0) \in \overline{\mathbb{Q}}$. Therefore, $\varphi(z_0)$ belongs to $\mathcal{E}(\overline{\mathbb{Q}})$, the map φ being defined in the introduction. Using the fact that φ is a group morphism and that $\mathcal{E}(\overline{\mathbb{Q}})$ is a subgroup of $\mathcal{E}(\mathbb{C})$, we get $\varphi(mz_0) \in \mathcal{E}(\overline{\mathbb{Q}})$. Therefore, $\wp(mz_0 + \lambda) = \wp(mz_0) \in \overline{\mathbb{Q}}$.) In the former case, we get $m_1 h \in \Lambda$ and hence $m_1 = 0$. In the later case, it follows from the work of Schneider [31] (for a reference in english, see Baker's book [2, Theorem 6.2]; see also Bertrand and Masser's papers [3, 21]) that $m_2 z_0 + \lambda$ and hence $m_1 h$ are transcendental numbers, which is excluded. ■

6.2 A family of examples with Galois groups between $\mathrm{SL}_2(\mathbb{C})$ and $\mathrm{GL}_2(\mathbb{C})$

Theorem 6.3. *Let us consider $b \in \mathbb{C}^\times$, and $a(z) := \alpha\wp(z) + \beta$ with $(\alpha, \beta) \in \mathbb{C}^\times \times \mathbb{C}$. Let $z_0 \in \mathbb{C}$ be such that $\wp(z_0) = -\beta/\alpha$. If $\mathbb{Z}h \cap (\ell z_0 + \Lambda) = \{0\}$ for all $\ell \in \{-16, \dots, 16\}$ (this holds in particular if $\mathbb{Z}h \cap (\mathbb{Z}z_0 + \Lambda) = \{0\}$) then the difference Galois group over (K, ϕ) of $\phi^2 y + a\phi y + by = 0$ is $\mu_{2k}\,\mathrm{SL}_2(\mathbb{C})$ if b is a primitive kth root of the unity and $\mathrm{GL}_2(\mathbb{C})$ otherwise, where μ_{2k} is the group of complex kth roots of the unity.*

The proof will be given after the following corollary.

Corollary 6.4. *Assume that $\mathcal{E}$ is defined over $\overline{\mathbb{Q}}$ (i.e., $g_2, g_3 \in \overline{\mathbb{Q}}$). Consider $b \in \overline{\mathbb{Q}}^\times$ and $a(z) := \alpha\wp(z) + \beta$ with $\alpha, \beta \in \overline{\mathbb{Q}}$ and $\alpha \neq 0$. Then, the difference Galois group over (K, ϕ) of $\phi^2 y + a\phi y + by = 0$ is $\mu_{2k}\,\mathrm{SL}_2(\mathbb{C})$ if b is a primitive kth root of the unity and $\mathrm{GL}_2(\mathbb{C})$ otherwise.*

Proof. Similar to deduction of Theorem 6.1 from Theorem 6.2. ■

Proof of Theorem 6.3. Note that

$$\mathrm{div}_1(a) = [z_0]_1 + [-z_0]_1 - 2[0]_1.$$

So, we can write $a = \frac{p_1}{p_3}$ and $b = \frac{p_2}{p_3}$ for some $p_1, p_2, p_3 \in \Theta_1$ with

$$\mathrm{div}_1(p_2) = 2[0]_1$$

and

$$\mathrm{div}_1(p_3) = 2[0]_1.$$

We claim that G is irreducible, i.e., in virtue of Theorem 4.4, that the Riccati equation

$$(\phi(u) + a)u = -b \tag{6.4}$$

does not have any solution in $\mathrm{M}_{2\Lambda}$. Suppose to the contrary that it has a solution $u \in \mathrm{M}_{2\Lambda}$. Proposition 4.5 ensures that there exist $p, q, r \in \Theta_2$ such that

$$u = \frac{\phi(r)}{r}\frac{p}{q}$$

and

(i) $\mathrm{div}_2(p) \le \sum_{\ell_1,\ell_2\in\{0,1\}} 2[\ell_1 + \ell_2\tau]_2$,

(ii) $\mathrm{div}_2(q) \le \sum_{\ell_1,\ell_2\in\{0,1\}} 2[\ell_1 + \ell_2\tau + h]_2$,

(iii) $\deg_2(p) = \deg_2(q)$,

(iv) $\omega_2(p/q) = \deg_2(r)h \mod 2\Lambda$.

Properties (i) and (ii) above imply that

$$\omega_2(p/q) = -h\deg_2(q) \mod \Lambda.$$

We infer from this and from (iv) that

$$(\deg_2(r) + \deg_2(q))h = 0 \mod \Lambda.$$

This yields $\deg_2(r) = \deg_2(q) = 0$. It follows from (iii) that $\deg_2(p) = 0$ and hence u is a constant. But it is easily seen that equation (6.4) does not have any constant solution; this proves our claim.

We claim that G is not imprimitive, i.e., in virtue of Theorem 5.1, that (we recall that b is constant)

$$\left(\phi^2(u) + \frac{b}{\phi^2(a)} - \phi(a) + \frac{b}{a}\right)u = -\frac{b^2}{a^2} \tag{6.5}$$

does not have any solution in $\mathrm{M}_{2\Lambda}$. Suppose to the contrary that it has a solution $u \in \mathrm{M}_{2\Lambda}$. Equation (6.5) is of the form:

$$u\left(\phi^2(u) + \frac{p_1}{p_3}\right) = \frac{p_2}{p_3},$$

for some $p_1, p_2, p_3 \in \Theta_1$ with

$$\mathrm{div}_1(p_2) = 4[0]_1 + 2[-h]_1 + [z_0 - 2h]_1 + [-z_0 - 2h]_1$$

and

$$\operatorname{div}_1(p_3) = 2[-h]_1 + 2[z_0]_1 + 2[-z_0]_1 + [z_0 - 2h]_1 + [-z_0 - 2h]_1.$$

Proposition 4.5 ensures that there exist $p, q, r \in \Theta_2$ such that

$$u = \frac{\phi^2(r)}{r}\frac{p}{q},$$

and

(v)
$$\operatorname{div}_2(p) \le \sum_{\ell_1,\ell_2\in\{0,1\}} 4[\ell_1 + \ell_2\tau]_2 + 2[\ell_1 + \ell_2\tau - h]_2 + [\ell_1 + \ell_2\tau + z_0 - 2h]_2 + [\ell_1 + \ell_2\tau - z_0 - 2h]_2,$$

(vi)
$$\operatorname{div}_2(q) \le \sum_{\ell_1,\ell_2\in\{0,1\}} 2[\ell_1 + \ell_2\tau + h]_2 + 2[\ell_1 + \ell_2\tau + z_0 + 2h]_2 + 2[\ell_1 + \ell_2\tau - z_0 + 2h]_2 + [\ell_1 + \ell_2\tau + z_0]_2 + [\ell_1 + \ell_2\tau - z_0]_2,$$

(vii) $\deg_2(p) = \deg_2(q)$,

(viii) $\omega_2(p/q) = 2\deg_2(r)h \mod 2\Lambda$.

We claim that

(v′) $\operatorname{div}_2(p) \le \sum_{\ell_1,\ell_2\in\{0,1\}} 4[\ell_1 + \ell_2\tau]_2$,

(vi′) $\operatorname{div}_2(q) \le \sum_{\ell_1,\ell_2\in\{0,1\}} [\ell_1 + \ell_2\tau + z_0]_2 + [\ell_1 + \ell_2\tau - z_0]_2$.

Otherwise, arguing as for the proof of the irreducibility of G, we see that (v), (vi) and (viii) would lead to a relation of the form

$$(2\deg_2(r) + d)h = \ell z_0 \mod \Lambda$$

for some integer $\ell \in \{-16, \dots, 16\}$ and some integer $d > 0$ and this would contradict our assumption on z_0. Then, (viii) shows that

$$2\deg_2(r)h = \ell z_0 \mod \Lambda$$

for some integer $\ell \in \{-4, \dots, 4\}$ and hence $\deg_2(r) = 0$. So $u = p/q$ with $p, q \in \Theta_2$ satisfying (v′) and (vi′) above. In particular, $-h$ is not a zero of u. But $-h$ (which is a pole of $\phi(a)$) is a pole of

$$\phi^2(u) + \frac{b}{\phi^2(a)} - \phi(a) + \frac{b}{a}.$$

So $-h$ is a pole of the left hand side of (6.5). This a contradiction because $-h$ is not a pole of the right hand side of (6.5).

Therefore, G is irreducible and not imprimitive. So, as explained at the beginning of Section 4, $G = \{M \in \mathrm{GL}_2(\mathbb{C}) \mid \det(M) \in H\}$ where $H \subset \mathbb{C}^\times$ is the Galois group of $\phi y = by$, which is easily seen to be μ_k if b is a kth root of the unity and $\mathbb{C}^\times$ otherwise. ■

Acknowledgements

Our original interest in difference equations on elliptic curves arose from discussions with Jean-Pierre Ramis some years ago. We thank Jean-Pierre Ramis and Michael Singer for interesting discussions. We thank the referees for their careful reading and useful suggestions. The first author is founded by the labex CIMI. The second author is partially funded by the French ANR project QDIFF (ANR-2010-JCJC-010501).

References

[1] André Y., Différentielles non commutatives et théorie de Galois différentielle ou aux différences, *Ann. Sci. École Norm. Sup. (4)* **34** (2001), 685–739, math.GM/0203274.

[2] Baker A., Transcendental number theory, 2nd ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990.

[3] Bertrand D., Masser D., Linear forms in elliptic integrals, *Invent. Math.* **58** (1980), 283–288.

[4] Bugeaud V., Groupe de Galois local des équations aux q-différences irrégulières, Ph.D. Thesis, Institut de Mathématiques de Toulouse, 2012.

[5] Casale G., Roques J., Dynamics of rational symplectic mappings and difference Galois theory, *Int. Math. Res. Not.* **2008** (2008), 103, 23 pages, arXiv:0803.3951.

[6] Casale G., Roques J., Non-integrability by discrete quadratures, *J. Reine Angew. Math.* **687** (2014), 87–112.

[7] Chatzidakis Z., Hardouin C., Singer M.F., On the definitions of difference Galois groups, in Model Theory with Applications to Algebra and Analysis, Vol. 1, *London Math. Soc. Lecture Note Ser.*, Vol. 349, Cambridge University Press, Cambridge, 2008, 73–109, arXiv:0705.2975.

[8] Di Vizio L., Arithmetic theory of q-difference equations: the q-analogue of Grothendieck–Katz's conjecture on p-curvatures, *Invent. Math.* **150** (2002), 517–578, math.NT/0104178.

[9] Di Vizio L., Hardouin C., Courbures, groupes de Galois génériques et D-groupoïde de Galois d'un système aux q-différences, *C. R. Math. Acad. Sci. Paris* **348** (2010), 951–954.

[10] Etingof P.I., Galois groups and connection matrices of q-difference equations, *Electron. Res. Announc. Amer. Math. Soc.* **1** (1995), 1–9.

[11] Franke C.H., Picard–Vessiot theory of linear homogeneous difference equations, *Trans. Amer. Math. Soc.* **108** (1963), 491–515.

[12] Franke C.H., Solvability of linear homogeneous difference equations by elementary operations, *Proc. Amer. Math. Soc.* **17** (1966), 240–246.

[13] Franke C.H., A note on the Galois theory of linear homogeneous difference equations, *Proc. Amer. Math. Soc.* **18** (1967), 548–551.

[14] Franke C.H., A characterization of linear difference equations which are solvable by elementary operations, *Aequationes Math.* **10** (1974), 97–104.

[15] Hardouin C., Singer M.F., Differential Galois theory of linear difference equations, *Math. Ann.* **342** (2008), 333–377, arXiv:0801.1493.

[16] Hartshorne R., Algebraic geometry, *Graduate Texts in Mathematics*, Vol. 52, Springer-Verlag, New York – Heidelberg, 1977.

[17] Helmer O., Divisibility properties of integral functions, *Duke Math. J.* **6** (1940), 345–356.

[18] Hendriks P.A., An algorithm for computing a standard form for second-order linear q-difference equations, *J. Pure Appl. Algebra* **117/118** (1997), 331–352.

[19] Hendriks P.A., An algorithm determining the difference Galois group of second order linear difference equations, *J. Symbolic Comput.* **26** (1998), 445–461.

[20] Lang S., On quasi algebraic closure, *Ann. of Math.* **55** (1952), 373–390.

[21] Masser D., Elliptic functions and transcendence, *Lecture Notes in Math.*, Vol. 437, Springer-Verlag, Berlin – New York, 1975.

[22] Mumford D., Tata lectures on theta. I, *Progress in Mathematics*, Vol. 28, Birkhäuser Boston, Inc., Boston, MA, 1983.

[23] Nguyen K.A., van der Put M., Top J., Algebraic subgroups of $\mathrm{GL}_2(\mathbb{C})$, *Indag. Math. (N.S.)* **19** (2008), 287–297.

[24] Nguyen P., Hypertranscedance de fonctions de Mahler du premier ordre, *C. R. Math. Acad. Sci. Paris* **349** (2011), 943–946.

[25] Ovchinnikov A., Wibmer M., σ-Galois theory of linear difference equations, *Int. Math. Res. Not.*, to appear, arXiv:1304.2649.

[26] Ramis J.-P., Sauloy J., The q-analogue of the wild fundamental group. I, in Algebraic, Analytic and Geometric Aspects of Complex Differential Equations and their Deformations. Painlevé Hierarchies, *RIMS Kôkyûroku Bessatsu*, B2, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007, 167–193, math.QA/0611521.

[27] Ramis J.-P., Sauloy J., The q-analogue of the wild fundamental group. II, *Astérisque* (2009), 301–324, arXiv:0711.4034.

[28] Ramis J.-P., Sauloy J., The q-analogue of the wild fundamental group and the inverse problem of the galois theory of q-difference equations, *Ann. Sci. École Norm. Sup.*, to appear, arXiv:1207.0107.

[29] Roques J., Galois groups of the basic hypergeometric equations, *Pacific J. Math.* **235** (2008), 303–322.

[30] Sauloy J., Galois theory of Fuchsian q-difference equations, *Ann. Sci. École Norm. Sup.* **36** (2003), 925–968, math.QA/0210221.

[31] Schneider T., Arithmetische Untersuchungen elliptischer Integrale, *Math. Ann.* **113** (1936), 1–13.

[32] Serre J.-P., Corps locaux, Hermann, Paris, 1968.

[33] Silverman J.H., The arithmetic of elliptic curves, *Graduate Texts in Mathematics*, Vol. 106, 2nd ed., Springer, Dordrecht, 2009.

[34] van der Put M., Reversat M., Galois theory of q-difference equations, *Ann. Fac. Sci. Toulouse Math.* **16** (2007), 665–718, math.QA/0507098.

[35] van der Put M., Singer M.F., Galois theory of difference equations, *Lecture Notes in Math.*, Vol. 1666, Springer-Verlag, Berlin, 1997.