TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 1, January 2018, Pages 321–355
http://dx.doi.org/10.1090/tran/6945
Article electronically published on July 13, 2017

ON THE ALGEBRAIC RELATIONS BETWEEN MAHLER FUNCTIONS

JULIEN ROQUES

Abstract. In the last years, a number of authors have studied the algebraic relations between the generating series of automatic sequences. It turns out that these series are solutions of Mahler type equations. This paper is mainly concerned with the difference Galois groups of Mahler type equations (these groups reflect the algebraic relations between the solutions of the equations). In particular, we study in detail the equations of order 2 and compute the difference Galois groups of classical equations related to the Baum-Sweet and to the Rudin-Shapiro automatic sequences.

Contents

1. Introduction

A number of authors have studied the algebraic relations between the generating series of certain p-automatic sequences. For instance, the generating series of the so-called Baum-Sweet and Rudin-Shapiro sequences (see sections 9.1 and 9.2) were studied by Nishioka and Nishioka in [NN12]: they are algebraically independent over $\overline{\mathbb{Q}}(z)$.[1] It turns out that the generating series $f(z) = \sum_{k\geq 0} s_k z^k$ of any p-automatic sequence $(s_k)_{k\geq 0} \in \overline{\mathbb{Q}}^{\mathbb{N}}$ (and, actually, of any p-regular sequence) satisfies

Received by the editors April 10, 2015 and, in revised form, March 21, 2016.
2010 *Mathematics Subject Classification.* Primary 39A06, 12H10.
Key words and phrases. Linear difference equations, difference Galois theory.

[1]For the relevance of the algebraic properties of the generating series coming from combinatorics, we refer for instance to Bousquet-Mélou's paper [BM06].

a functional equation of the form

$$a_n(z)f(z^{p^n}) + a_{n-1}(z)f(z^{p^{n-1}}) + \cdots + a_0(z)f(z) = 0$$

with coefficients $a_0(z), \ldots, a_n(z) \in \overline{\mathbb{Q}}(z)$; see Becker's paper [Bec94] and the references therein, especially to the works of Dumas and Randé. Such a functional equation is called a p-Mahler equation, in honor of the work of Mahler in [Mah30b, Mah30c, Mah30a].[2] So, the study of the algebraic relations between the generating series issued from p-automatic sequences is a special case of the study of the algebraic relations between solutions of Mahler equations.

The principal aim of the present work is to study the algebraic relations between the solutions of p-Mahler equations of order $n = 2$ via difference Galois theory.

We shall now describe more carefully the content of this paper. Section 2 contains general prerequisites and complements on difference Galois theory. In section 3, we establish fundamental properties of the difference Galois groups of the Mahler equations. In section 4, we study the factorization of the Mahler operators on the field of Puiseux series, and we define and study the notion of local exponents at 0 and ∞ (this will be used several times in the rest of this paper: for the algorithmic aspects studied in section 6, and also for the calculation of the difference Galois groups of the Baum-Sweet and of the Rudin-Shapiro equations, and of their direct sum, in section 9). Section 5 is an aside on a special type of Mahler equation, called regular singular, for which one can describe explicitly the universal Picard-Vessiot ring over the field of Puiseux series. We then focus our attention on the Mahler equations of order $n = 2$: in section 6, we give an algorithm to determine whether or not the difference Galois group of a given Mahler equation of order 2 is irreducible, and, in the irreducible case, whether or not it is imprimitive. This is inspired by the analogue of Kovacic's algorithm introduced by Hendricks in [Hen97, Hen98]. Note that in the irreducible and not imprimitive case, the Galois group, which can be determined explicitly, contains $\mathrm{SL}_2(\overline{\mathbb{Q}})$. For instance, the Baum-Sweet and the Rudin-Shapiro equations (see sections 9.1 and 9.2) are Mahler equations of order 2, and hence the algorithm applies in these cases. It would lead to the fact that these Galois groups are $\mu_4\,\mathrm{SL}_2(\overline{\mathbb{Q}})$ and $\mathrm{GL}_2(\overline{\mathbb{Q}})$ respectively, where $\mu_4 \subset \mathbb{C}^\times$ is the group of 4th roots of the unity. However, in section 9, we give a shorter way (which could be of interest for other equations) to compute these groups. We also compute the Galois group of the "direct sum" of the Baum-Sweet and of the Rudin-Shapiro equations (via the Goursat-Kolchin-Ribet lemma), which turns out to be equal to the direct product of the Galois groups of the Baum-Sweet and of the Rudin-Shapiro equations. For instance, this gives a Galoisian proof of the following result obtained by Nishioka and Nishioka in [NN12]: if we let $f_1(z) = f(z)$ (resp. $g(z)$) be the generating series of the Rudin-Shapiro (resp. Baum-Sweet) sequence, then the series $f_1(z) = f(z)$, $f_2(z) = f(-z)$, $g(z)$ and $g(z^2)$ are algebraically independent over $\overline{\mathbb{Q}}(z)$.

2. Difference Galois theory: Reminders and complements

2.1. **Generalities on difference Galois theory.** For details on what follows, we refer to [vdPS97, Chapter 1].

[2] For an introduction to this aspect of Mahler's work, we refer to Pellarin's [Pel09] and to Nishioka's [Nis96]. We also point out the recent paper [Ph15] by Philippon (which uses difference Galois theory).

A difference ring is a couple (R, ϕ) where R is a ring and ϕ is a ring automorphism of 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

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

Two difference rings (R, ϕ) and $(\widetilde{R}, \widetilde{\phi})$ are isomorphic if there exists a 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 ring isomorphism $\varphi : \widetilde{R}_1 \to \widetilde{R}_2$ such that $\varphi_{|R} = \mathrm{Id}_R$ and $\varphi \circ \widetilde{\phi}_1 = \widetilde{\phi}_2 \circ \varphi$.

A difference ring (R, ϕ) is a difference subring of a difference ring $(\widetilde{R}, \widetilde{\phi})$ if $(\widetilde{R}, \widetilde{\phi})$ is a difference ring extension of (R, ϕ).

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.

In what follows, we will frequently denote the difference ring (R, ϕ) by R.

Consider a difference system

$$\phi Y = AY \text{ with } A \in \mathrm{GL}_n(k). \tag{1}$$

According to [vdPS97, §1.1], there exists a difference ring extension R 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 (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 are $\{0\}$ and R.

Such a difference ring R is called a Picard-Vessiot ring for (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 [vdPS97, Lemma 1.8].

The corresponding difference Galois group G over (k, ϕ) of (1) is the group of the k-linear ring automorphisms of R commuting with ϕ :

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

The Picard-Vessiot ring R is not a domain in general. According to [vdPS97, Corollary 1.16], we can decompose R as a direct product of rings

$$R = \bigoplus_{x \in X} R_x \text{ with } R_x = Re_x$$

where

- $X = \mathbb{Z}/t\mathbb{Z}$ for some integer $t \geq 1$,
- for all $x \in X$, e_x is an idempotent element of R,
- for all $x \in X$, R_x is a domain,
- for all $x \in X$, $\phi(e_x) = e_{x+1_X}$ and, hence, $\phi(R_x) = R_{x+1_X}$.

Let us consider the total quotient ring K of R, which can be described as

$$K = \bigoplus_{x \in X} K_x$$

where K_x is the field of fractions of R_x. It is easily seen that ϕ admits a unique extension into a ring automorphism of K. Therefore, K is a difference ring extension of R, called the total Picard-Vessiot ring of (1) over (k, ϕ). We have $K^\phi = C$. The action of G on R extends to K.

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 [vdPS97, 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 system of solutions U, we find a conjugate representation.

Remark 1. To the difference equation

$$a_n \phi^n(y) + \cdots + a_1 \phi(y) + a_0 y = 0, \tag{2}$$

with $a_0, \ldots, a_n \in k$ and $a_0 a_n \neq 0$, we associate the difference system

$$\phi Y = AY, \text{ with } A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ -\frac{a_0}{a_n} & -\frac{a_1}{a_n} & \cdots & \cdots & -\frac{a_{n-1}}{a_n} \end{pmatrix} \in \mathrm{GL}_n(k). \tag{3}$$

By "Galois group of the difference equation (2)" we will mean "Galois group of the difference system (3)".

The Galois correspondence [vdPS97, Theorem 1.29] reads as follows.

Theorem 2. *Let $\mathcal{F}$ be the set of difference subrings F of K such that $k \subset F$ and such that every non-zero divisor of F is actually a unit of F. Let $\mathcal{G}$ be the set of algebraic subgroups of G. Then:*

- *for any $F \in \mathcal{F}$, the set $G(K/F)$ of elements of G which fix F pointwise is an algebraic subgroup of G;*
- *for any algebraic subgroup H of G, $K^H := \{x \in K \mid \forall \sigma \in H, \sigma(x) = x\}$ belongs to $\mathcal{F}$;*
- *the maps $\mathcal{F} \to \mathcal{G}$, $F \mapsto G(K/F)$ and $\mathcal{G} \to \mathcal{F}$, $H \mapsto K^H$ are each other's inverses.*

The Galois group G reflects the algebraic relations between the entries of any fundamental matrix of solutions $U \in \mathrm{GL}_n(R)$ of (1). The point is that $\mathrm{Spec}(R)$ is a G-torsor over k; see [vdPS97, Theorem 1.13]. This implies that there exists a finite extension k' of k such that the $\mathrm{Spec}(k')$-schemes $G_{k'} := G \times_{\mathrm{Spec}(C)} \mathrm{Spec}(k')$ and $\mathrm{Spec}(R) \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k')$ are isomorphic, i.e. such that there is a k'-algebra isomorphism

$$R \otimes_k k' \cong C[G] \otimes_C k'. \tag{4}$$

Therefore, equation (4) holds true when k' is replaced by an algebraic closure $\overline{k}$ of k. Note that if G is connected and k is a $\mathcal{C}^1$-field,[3] then we can take $k' = k$; i.e. there is a k-algebra isomorphism

$$R \cong C[G] \otimes_C k.$$

For instance, if $n = 2$, $G = \mathrm{SL}_2(C)$ and k is a $\mathcal{C}^1$-field, then there is a k-algebra isomorphism

$$R \cong k[X_{i,j} \mid 1 \leq i, j \leq 2]/(\det(X_{i,j})_{1 \leq i,j \leq 2} = 1);$$

in other words, the ideal of polynomial relations with coefficients in k between the entries of U is generated by $\det(X_{i,j})_{1 \leq i,j \leq 2} = 1$.

We shall now introduce a property relative to the base difference field (k, ϕ) which appeared in [vdPS97].

Definition 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;
- 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 there exists $T \in \mathrm{GL}_n(k)$ such that $\phi(T)A = BT$.

Theorem 4. *Assume that (k, ϕ) satisfies property $(\mathcal{P})$. Let $G \subset \mathrm{GL}_n(C)$ be the difference Galois group over (k, ϕ) of*

$$\phi Y = AY, \text{ with } A \in \mathrm{GL}_n(k). \tag{5}$$

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 (5) 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 [vdPS97, 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. □

[3]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. For instance, the function field of any algebraic curve over an algebraically closed field is a $\mathcal{C}^1$-field by virtue of Tsen's theorem [Lan52].

2.2. **Base difference field extensions.** Let (k', ϕ) be a difference field extension of (k, ϕ) such that $(k')^\phi = C$. We shall first explain how one can see the difference Galois group G' of the difference system (1) over (k', ϕ) as a subgroup of the difference Galois group G of the difference system (1) over (k, ϕ).

Let R' be a Picard-Vessiot ring over (k', ϕ) for the difference system (1). Let $U \in \mathrm{GL}_n(R')$ be a fundamental matrix of solutions of (1). We consider the sub-k-algebra R of R' generated by the entires of U and by $\det(U)^{-1}$. It is clear that R is a difference subring of R'.

Lemma 5. *An element of R is a zero divisor of R if and only if it is a zero divisor of R'.*

Proof. It is obvious that if $a \in R$ is a zero divisor of R, then it is a zero divisor of R'. Conversely, let $a \in R$ be a zero divisor of R'. As recalled in section 2.1, we can decompose R' as follows:

$$R' = \bigoplus_{x \in X} R'_x,$$

where

- $X = \mathbb{Z}/t\mathbb{Z}$,
- for all $x \in X$, R'_x is a domain,
- for all $x \in X$, ϕ induces an isomorphism from R'_x to R'_{x+1_X}.

Consider the corresponding decomposition $a = \sum_{x \in X} a_x$. The fact that a is a zero divisor of R' ensures that $a_x = 0$ for some $x \in X$. It follows that $a\phi(a) \cdots \phi^{t-1}(a) = 0$. Therefore, there exists $i \in \{0, \dots, t-1\}$ such that $\phi^i(a)$ is a zero divisor of R. Since ϕ^i is a ring automorphism of R, we get that a is a zero divisor of R, as expected. □

Thanks to Lemma 5, one can see the total quotient ring K of R as a difference subring of the total quotient ring K' of R':

$$K \subset K'.$$

Proposition 6. *The difference ring (R, ϕ) is a Picard-Vessiot ring over (k, ϕ) for (1). Therefore, the difference ring (K, ϕ) is a total Picard-Vessiot ring over (k, ϕ) for (1).*

Proof. According to [vdPS97, Corollary 1.24], in order to prove that R is a Picard-Vessiot ring over (k, ϕ) for (1), it is sufficient to prove that the following properties hold true:

- R has no nilpotent elements;
- the ring of constants of K is C;
- there is a fundamental matrix of solutions of (1) in $\mathrm{GL}_n(R)$;
- R is minimal with respect to the previous properties.

The first property follows from the facts that $R \subset R'$ and that R' has no nilpotent elements (recall that R' is a direct product of domains). The second property follows from the facts that $K \subset K'$ and that $(K')^\phi = C$ (because K' is a total Picard-Vessiot ring). The third property follows from the fact that U is a fundamental matrix of solutions of (1) in $\mathrm{GL}_n(R)$. The minimality property of R is obvious. □

Consider the Galois group G' of (1) over (k', ϕ) given by

$$G' = \{\sigma \in \mathrm{Aut}(R'/k') \mid \phi \circ \sigma = \sigma \circ \phi\}$$

and the Galois group G of (1) over (k, ϕ) given by

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

Then, the restriction map $\sigma \mapsto \sigma_{|R}$ gives a closed immersion

$$G' \subset G.$$

We shall now focus our attention on the case when k' is an algebraic extension of k.

Theorem 7. *Assume that k' is an algebraic extension of k. Then, G' and G have the same identity component.*

Proof. As recalled in section 2.1, the scheme $G_{\overline{k'}} := G \times_{\mathrm{Spec}(C)} \mathrm{Spec}(\overline{k'})$ is isomorphic to $\mathrm{Spec}(R) \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k'})$, and the scheme $G'_{\overline{k'}} := G' \times_{\mathrm{Spec}(C)} \mathrm{Spec}(\overline{k'})$ is isomorphic to $\mathrm{Spec}(R') \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k'})$. Therefore, the dimension of G, which is equal to the dimension of $G_{\overline{k'}}$, is equal to the dimension of $\mathrm{Spec}(R) \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k'})$, which is itself equal to the dimension of $\mathrm{Spec}(R)$. Similarly, the dimension of G' is equal to the dimension of $\mathrm{Spec}(R')$. But the ring extension $R \subset R'$ is integral, so $\mathrm{Spec}(R)$ and $\mathrm{Spec}(R')$ have the same dimensions. Hence G and G' have the same dimensions. So, we have a closed immersion $G' \subset G$ of algebraic groups with the same dimensions. It follows that G and G' have the same identity component. □

With the notation and hypotheses of Theorem 7, one can ask the following question: Is G' a normal subgroup of G? Let us study this question in detail. Since G' is an algebraic subgroup of G, the Galois correspondence [vdPS97, Theorem 1.29] ensures that there exists a difference subring F of K containing k such that every non-zero divisor of F is a unit of F and such that

$$G' = \{\sigma \in \mathrm{Aut}(K/F) \mid \phi \circ \sigma = \sigma \circ \phi\}.$$

By Galois correspondence again,

$$F = K^{G'} = (K')^{G'} \cap K = k' \cap K.$$

Using [vdPS97, Corollary 1.30], we obtain the following result.

Proposition 8 (Normality criterion)**.** *The algebraic group G' is normal in G if and only if the set of elements of $k' \cap K$ which are fixed by the natural action of the group*

$$\{\sigma \in \mathrm{Aut}(k' \cap K/k) \mid \phi \circ \sigma = \sigma \circ \phi\}$$

is reduced to k.

We shall now give an example illustrating the fact that G' is not a normal subgroup of G in general, in contrast with the differential case [Kat87, Proposition 1.4.5].

We consider the difference field (l, ϕ) which is given by

$$l = \bigcup_{d \geq 1} \overline{\mathbb{Q}}(z^{1/d}) \text{ and } \phi\left(f(z^{1/d})\right) = f(z^{p/d}).$$

We consider the difference subfields k and k' of l given by

$$k = \bigcup_{m \geq 0} \overline{\mathbb{Q}}(z^{1/p^m})$$

and

$$k' = k(z^{\frac{1}{p^2-1}}) = \bigcup_{m\geq 0} \overline{\mathbb{Q}}(z^{\frac{1}{p^m(p^2-1)}}).$$

Consider the difference system

$$\phi Y = AY, \quad A \in \mathrm{GL}_2(k)$$

associated to the difference equation $\phi^2 y = zy$. A total Picard-Vessiot ring over (k', ϕ) for this system is given by the difference ring (K', ϕ) defined as follows:

- as a ring, $K' = k' \oplus k'$ is the direct sum of two copies of k';
- the action of ϕ on $(a, b) \in K'$ is given by $\phi(a, b) = (\phi(b), \phi(a))$.

Note that k' is seen as a difference subfield of K' via $a \in k' \mapsto (a, a) \in K'$. A total Picard-Vessiot ring over (k, ϕ) is given by $K := K'$. Therefore, we have $k' \cap K = k'$, and it is easily seen that

$$\{\sigma \in \mathrm{Aut}(k' \cap K/k) \mid \phi \circ \sigma = \sigma \circ \phi\} = \{\mathrm{Id}\}.$$

The above normality criterion implies that G' is not a normal subgroup of G.

2.3. **Iterations.** Let $d \geq 1$ be an integer and consider the iterated difference system

$$\phi^d Y = A_d Y \text{ with } A_d = \phi^{d-1}(A)\phi^{d-2}(A)\cdots A \in \mathrm{GL}_n(k). \tag{6}$$

The aim of this section is to study the relations between the difference Galois groups of this difference system and of the original difference system (1) and to generalize van der Put and Singer's [vdPS97, Corollary 1.17] (which is concerned with the case $d = t$ with the notation introduced below).

Let R be a Picard-Vessiot ring over (k, ϕ) for the difference system (1). As recalled in section 2.1, we can decompose R as a direct product of rings

$$R = \bigoplus_{x\in X} R_x \text{ with } R_x = Re_x$$

where

- $X = \mathbb{Z}/t\mathbb{Z}$ for some integer $t \geq 1$,
- for all $x \in X$, e_x is an idempotent element of R,
- for all $x \in X$, R_x is a domain,
- for all $x \in X$, $\phi(e_x) = e_{x+1_X}$ and, hence, $\phi(R_x) = R_{x+1_X}$.

We denote by Y the quotient of X by its ideal generated by $d1_X$. For all $y \in Y$, we introduce the ring

$$S_y = \bigoplus_{x\in y} R_x.$$

We have

$$R = \bigoplus_{y\in Y} S_y \text{ and, for all } y \in Y,\ \phi(S_y) = S_{y+1_Y}.$$

In particular, if $r = |Y| = \gcd(d, t)$, then, for all $y \in Y$,

$$\phi^r(S_y) = S_y \text{ and, hence, } \phi^d(S_y) = S_y.$$

Therefore, (S_y, ϕ^d) (resp. (S_y, ϕ^r)) is a difference ring extension of (k, ϕ^d) (resp. (k, ϕ^r)), when k is identified with $k1_{S_y}$.

Proposition 9. *The difference ring (S_{0_Y}, ϕ^d) is a Picard-Vessiot ring over (k, ϕ^d) for the difference system* (6).

Proof. Let $U \in \mathrm{GL}_n(R)$ be a fundamental matrix of solutions of (1). We can decompose U as follows:

$$U = \sum_{y \in Y} U_y$$

where, for all $y \in Y$, $U_y \in \mathrm{GL}_n(S_y)$. We have

$$\phi^d(U) = \sum_{y \in Y} \phi^d(U_y) \text{ and } \phi^d(U) = A_d U = \sum_{y \in Y} A_d U_y.$$

Since $\phi^d(U_y) \in \mathrm{GL}_n(S_y)$ and $A_d U_y \in \mathrm{GL}_n(S_y)$, it follows that, for all $y \in Y$, $\phi^d(U_y) = A_d U_y$.

Since R is generated as a k-algebra by the entries of U and $\det U^{-1}$, we get that, for all $y \in Y$, S_y is generated as a k-algebra by the entries of U_y and $\det U_y^{-1}$.

It remains to prove that (S_{0_Y}, ϕ^d) is a simple difference ring. Let I be a minimal non-zero difference ideal of (S_{0_Y}, ϕ^d). Since $\phi^d(I)$ is a non-zero difference ideal of (S_{0_Y}, ϕ^d) included in I, we get that $\phi^d(I) = I$. Since $S_{0_Y} = \bigoplus_{x \in 0_Y} R_x$, we can decompose I as follows:

$$I = \bigoplus_{x \in 0_Y} I_x$$

where, for all $x \in 0_Y$, I_x is an ideal of R_x. Since I is non-zero, there exists $x \in 0_Y$ such that I_x is non-zero. But $\phi^d(I) \subset I$ and, for all integer $j \geq 0$, $\phi^{jd}(R_x) \subset R_{x+jd1_X}$, so $\phi^{jd}(I_x) \subset I_{x+jd1_X}$. Therefore, for any $x \in 0_Y$, I_x is non-zero. Using the fact that, for all $j \in \mathbb{N}$, ϕ^{jr} induces a permutation of $\{R_x \mid x \in 0_Y\}$, we see that

$$\phi^{jr}(I) = \bigoplus_{x \in 0_Y} I_{j,x}$$

where, for all integers $j \geq 0$ and $x \in 0_Y$, $I_{j,x}$ is a non-zero ideal of R_x.

We now consider

$$J_0 = \bigcap_{j \in \mathbb{N}} \phi^{jr} I = \bigcap_{j=0}^{d/r-1} \phi^{jr}(I) \subset S_{0_Y},$$

which is a difference ideal of (S_{0_Y}, ϕ^r). The decomposition

$$J_0 = \bigoplus_{x \in 0_Y} \bigcap_{j=0}^{d/r-1} I_{j,x},$$

together with the fact that a finite intersection of non-zero ideals of a domain is non-zero, shows that J_0 is non-zero.

We set

$$J = \bigoplus_{k=0}^{r-1} \phi^k(J_0) \subset \bigoplus_{y \in Y} S_y,$$

which is a non-zero difference ideal of (R, ϕ). Therefore, $J = R$. So, $J_0 = S_{0_Y}$ and, hence, $I = S_{0_Y}$ as expected. □

We will also use the iterated difference system

$$\phi^r Y = A_r Y \text{ with } A_r = \phi^{r-1}(A)\phi^{r-2}(A) \cdots A \in \mathrm{GL}_n(k). \tag{7}$$

The following result is the particular case $d = r$ of the previous proposition.

Proposition 10. *The difference ring (S_{0_Y}, ϕ^r) is a Picard-Vessiot ring over (k, ϕ^r) for the difference system* (7).

Let K be the total quotient ring of R over (k, ϕ). So $K = \bigoplus_{x \in X} K_x$ with $K_x = \mathrm{Frac}(R_x)$. Then, (K, ϕ) is a total Picard-Vessiot ring for the difference system (1). For any $y \in Y$, we set $L_y = \bigoplus_{x \in y} K_x$, which is the total quotient ring of S_y. According to Proposition 9 (resp. Proposition 10), (L_{0_Y}, ϕ^d) (resp. (L_{0_Y}, ϕ^r)) is a total Picard-Vessiot ring for the difference system (6) over (k, ϕ^d) (resp. (7) over (k, ϕ^r)).

We consider the difference Galois group over (k, ϕ) of the difference system (1) given by

$$G = \{\sigma \in \mathrm{Aut}(K/k) \mid \phi \circ \sigma = \sigma \circ \phi\},$$

the difference Galois group over (k, ϕ^d) of the difference system (6) given by

$$G' = \{\sigma \in \mathrm{Aut}(L_{0_Y}/k) \mid \phi^d \circ \sigma = \sigma \circ \phi^d\}$$

and the difference Galois group over (k, ϕ^r) of the difference system (7) given by

$$G'' = \{\sigma \in \mathrm{Aut}(L_{0_Y}/k) \mid \phi^r \circ \sigma = \sigma \circ \phi^r\}.$$

Proposition 11. *We have $G' = G''$.*

Proof. We have an obvious closed immersion of algebraic groups $G'' \subset G'$ (because r divides d). By Galois correspondence for the difference system (7), we have $L_{0_Y}^{G''} = k$. By Galois correspondence again, but for the difference system (6), we get that the inclusion of algebraic groups $G'' \subset G'$ is actually an equality. □

We consider the map $\alpha : G'' \to G$ defined as follows. For all $\sigma \in G''$, $\alpha(\sigma) : K \to K$ is the unique k-linear endomorphism of K such that, for all $y = j1_Y \in Y$, $\alpha(\sigma)_{|L_y} = \phi^j \sigma \phi^{-j}$. The map $\alpha(\sigma)$ is well-defined because

- ϕ^j induces a ring isomorphism between L_{0_Y} and $L_{j1_Y} = L_y$;
- if $j, j' \in \mathbb{Z}$ are such that $y = j1_Y = j'1_Y$, then $\phi^j \sigma \phi^{-j} = \phi^{j'} \sigma \phi^{-j'}$ (indeed, in this case, we have $j \equiv j' \mod r$ and, hence, $\phi^j \sigma \phi^{-j} = \phi^{j'} \sigma \phi^{-j'}$ because σ commutes with ϕ^r).

The fact that $\alpha(\sigma)$ is an element of G is straightforward.

We consider the map $\beta : G \to Y$ defined as follows. It is easily seen that any $\sigma \in G$ induces a permutation of $\{e_x \mid x \in X\}$. More precisely, if $\sigma(e_{0_X}) = e_{\ell 1_X}$, then, for all $x' \in X$, $\sigma(e_{x'}) = e_{x' + \ell 1_X}$ (indeed, if $x' = j1_X$, then $e_{x'} = e_{j1_X} = \phi^j(e_{0_X})$, so $\sigma(e_{x'}) = \sigma(\phi^j(e_{0_X})) = \phi^j(\sigma(e_{0_X})) = \phi^j(e_{\ell 1_X}) = e_{\ell 1_X + j1_K} = e_{x' + \ell 1_X}$). Therefore, σ induces a permutation of $\{1_{L_y} = \sum_{x \in y} e_x \mid y \in Y\}$. We denote by $\beta(\sigma)$ the unique element of Y such that $\sigma(1_{L_{0_Y}}) = 1_{L_{\beta(\sigma)}}$. Note that, for any $y \in Y$, we have $\sigma(1_{L_y}) = 1_{L_{y + \beta(\sigma)}}$. Equivalently, one can define $\beta(\sigma)$ as the unique element of Y such that

$$\sigma(L_{0_Y}) = L_{\beta(\sigma)}.$$

Moreover, for any $\sigma \in G$ and $y \in Y$, we have

$$\sigma(L_y) = L_{y + \beta(\sigma)}.$$

It is easily seen that α and β are morphisms of algebraic groups.

Theorem 12. *We have the following exact sequence of algebraic groups:*

$$0 \to G' = G'' \xrightarrow{\alpha} G \xrightarrow{\beta} Y \to 0.$$

Proof. The fact that α is injective is obvious.

For any $\sigma \in G''$, we have $\alpha(\sigma)(1_{L_{0_Y}}) = \sigma(1_{L_{0_Y}})$ because $1_{L_{0_Y}} \in L_{0_Y}$. And, $\sigma(1_{L_{0_Y}}) = 1_{L_{0_Y}}$ because σ is a ring endomorphism of L_{0_Y}. Therefore, $\beta \circ \alpha(\sigma) = 0_Y$.

Consider $\sigma \in \ker \beta$. Then, $\sigma' := \sigma_{|L_{0_Y}}$ leaves L_{0_Y} globally invariant and belongs to G'. It is easily seen that $\sigma = \alpha(\sigma') \in \mathrm{im}(\alpha)$.

It remains to prove that β is surjective. Consider $x = \sum_{y \in \mathrm{im}(\beta)} 1_{L_y}$. For all $\sigma \in G$, we have $\sigma(x) = \sum_{y \in \mathrm{im}(\beta)} 1_{L_{y+\beta(\sigma)}} = x$ (the last equality follows from the fact that $\beta(\sigma)$ belongs to the group $\mathrm{im}(\beta)$). According to Galois correspondence, we have $x \in k$. But x is idempotent, so $x = 0_K$ or 1_K. Since $x \neq 0_K$, we get $x = 1_K$. Therefore, $\mathrm{im}(\beta) = Y$. □

2.4. **Systems, equations and modules.** In linear algebra, it is usual to work either with matrices with entries in a field k, with endomorphisms of a finite dimensional k-vector space or with $k[X]$-modules of finite type. This can be imitated in the context of difference algebra, as we shall now explain.

One can rewrite the difference system

$$\phi Y = AY \text{ with } A \in \mathrm{GL}_n(k) \tag{8}$$

as the fixed point equation $\Phi_A(Y) = Y$ where $\Phi_A : k^n \to k^n$ is defined by $\Phi_A(Y) = A^{-1}\phi(Y)$ (here ϕ acts component-wise on the elements of k^n, which are seen as column vectors). The map Φ_A is a ϕ-linear automorphism of the k-vector space k^n, i.e. $\Phi_A(X + \lambda Y) = \Phi_A(X) + \phi(\lambda)\Phi_A(Y)$ for all $X, Y \in k^n$ and $\lambda \in k$. This leads to the following concept: a difference module is a pair (V, Φ) where V is a finite dimensional k-vector space and $\Phi : V \to V$ is a ϕ-linear automorphism of V. So, we have attached the difference module (k^n, Φ_A) to the difference system (8). Conversely, we can attach a difference system to any difference module (V, Φ) by choosing some basis of V.

Here is an alternate description of the difference modules. Consider the Öre algebra $\mathcal{D}_k = k[\phi, \phi^{-1}]$ of non-commutative Laurent polynomials with coefficients in k such that $\phi a = \phi(a)\phi$ for all $a \in k$. By "$\mathcal{D}_k$-module" we will mean "left $\mathcal{D}_k$-module of finite length" (it is equivalent to require that the k-vector space obtained by restriction of scalars has finite dimension). There is a natural correspondence between difference modules and $\mathcal{D}_k$-modules. Indeed, we can attach to the difference module (V, Φ) the $\mathcal{D}_k$-module M whose underlying abelian group is the underlying group of V and such that $L = \sum a_i \phi^i \in \mathcal{D}_k$ acts on $m \in M$ as $Lm = \sum a_i \Phi^i(m)$. Conversely, we can attach to the $\mathcal{D}_k$-module M the difference module (V, Φ) where V is the k-vector space obtained from M by restriction of scalars and where $\Phi(v) = \phi v$, for any $v \in V$.

The following result, known as the cyclic vector lemma, ensures that any $\mathcal{D}_k$-module (and, hence, any difference system and difference module) "comes from" an equation.

Proposition 13. *Let M be a $\mathcal{D}_k$-module. There exists $L \in \mathcal{D}_k$ such that $M \cong \mathcal{D}_k/\mathcal{D}_k L$.*

The category of $\mathcal{D}_k$-modules is a C-linear rigid tensor category. The dual of a $\mathcal{D}_k$-module M will be denoted by $M^\vee$ and the tensor product by the usual symbol $\otimes$. For details, we refer to [vdPS97, §1.4].

2.5. **Tannakian duality.** For details on what follows, see [vdPS97, §1.4]. For tannakian categories in general, we refer to Deligne and Milne's [DM82]. We let $\langle M \rangle$ be the smallest full subcategory of the category of $\mathcal{D}_k$-modules containing M and closed under all constructions of linear algebra, namely direct sums, tensor products, duals and subquotients. We let (R, ϕ) be a Picard-Vessiot ring of M over (k, ϕ) and we let G be the corresponding difference Galois group over (k, ϕ). There is a C-linear equivalence of categories between $\langle M \rangle$ and the category of rational C-linear representations of the linear algebraic group G which is compatible with all constructions of linear algebra (this is called tannakian duality). Such an equivalence is given by a functor sending an object N of $\langle M \rangle$ to the representation

$$\begin{array}{rcl} \rho_N : G & \to & \mathrm{GL}(\omega(N)) \\ \sigma & \mapsto & (\sigma \otimes Id_N)_{|\omega(N)} \end{array}$$

where

$$\omega(N) = \ker(\phi \otimes \phi - 1 : R \otimes_k N \to R \otimes_k N).$$

The difference Galois group of N over (k, ϕ) can be identified with the image of ρ_N.

We now focus on a specific situation that we will encounter later in this paper. If N_1 and N_2 are objects of $\langle M \rangle$, then the Galois group of $N_1 \oplus N_2$ can be identified with

$$(\rho_{N_1} \oplus \rho_{N_2})(G) \subset G_1 \times G_2,$$

where G_1 (resp. G_2) is the difference Galois group of N_1 (resp. N_2) over (k, ϕ) identified with $\rho_{N_1}(G)$ (resp. $\rho_{N_2}(G)$). We have the following result.

Proposition 14. *Assume that:*

- *N_1 and N_2 have rank 2,*
- *G_1 (resp. G_2) contains $\mathrm{SL}(\omega(N_1))$ (resp. $\mathrm{SL}(\omega(N_2))$),*
- *for any object N of rank one of $\langle N_1 \oplus N_2 \rangle$, N_1 is isomorphic to neither $N \otimes N_2$ nor $N \otimes N_2^\vee$.*

Then, the Galois group of $N_1 \oplus N_2$, seen in $G_1 \times G_2$, contains $\mathrm{SL}(\omega(N_1)) \times \mathrm{SL}(\omega(N_2))$.

Proof. Indeed, this is a direct consequence of Goursat-Kolchin-Ribet's [Kat90, Proposition 1.8.2] (applied to $\rho_1 := \rho_{N_1}$ and $\rho_2 := \rho_{N_2}$) and tannkian duality. □

Note that if $G_1 \times G_2$ contains $\mathrm{SL}(\omega(N_1)) \times \mathrm{SL}(\omega(N_2))$, then

$$G = \{(\sigma_1, \sigma_2) \in \mathrm{GL}(\omega(N_1)) \times \mathrm{GL}(\omega(N_2)) \mid (\det \sigma_1, \det \sigma_2) \in H\},$$

where H is the Galois group of $\det M_1 \oplus \det M_2$.

3. Difference Galois theory: More specific results for Mahler equations

We consider the field of Puiseux series with coefficients in $\overline{\mathbb{Q}}$ given by

$$\widehat{\mathbf{K}} = \bigcup_{d \geq 1} \widehat{\mathbf{K}}_d \text{ with } \widehat{\mathbf{K}}_d = \overline{\mathbb{Q}}((z^{1/d})).$$

We will use the notation $z_d = z^{1/d}$. We endow $\widehat{\mathbf{K}}$ with the field automorphism ϕ_p defined by

$$\phi_p\left(f(z^{1/d})\right) = f(z^{p/d}).$$

This makes $\widehat{\mathbf{K}}$ a difference field with field of constants $\widehat{\mathbf{K}}^{\phi_p} = \overline{\mathbb{Q}}$.

We also consider the difference subfield of $\widehat{\mathbf{K}}$ given by

$$\mathbf{K} = \bigcup_{d\geq 1} \mathbf{K}_d \text{ with } \mathbf{K}_d = \overline{\mathbb{Q}}(z^{1/d}).$$

The corresponding Öre algebras $\mathcal{D}_{\widehat{\mathbf{K}}}$ and $\mathcal{D}_{\mathbf{K}}$ (see section 2.4) will be denoted by $\widehat{\mathcal{D}}$ and $\mathcal{D}$. An element of such an algebra will be called a Mahler operator. A Mahler equation, system or module is a difference equation, system or module over one of the above difference fields.

The following result will be useful.

Proposition 15. *The difference field $(\mathbf{K}, \phi_p)$ satisfies property $(\mathcal{P})$ (see Definition 3). Therefore, the conclusions of Theorem 4 are valid for $(\mathbf{K}, \phi_p)$.*

The proof of this proposition, given below, will use the following geometric result.

Proposition 16. *Let X be of smooth projective curve over $\overline{\mathbb{Q}}$ with genus $g \geq 2$. Then, the following properties hold:*

1. *any non-constant endomorphism of X is an automorphism;*
2. *the group of automorphisms of X is finite, of order at most $84(g-1)$.*

Proof. Let $\varphi : X \to X$ be a non-constant endomorphism of X. Hurwitz's formula (see [Har77, Corollary 2.4]) ensures that

$$-2(N-1)(g-1) = \sum_P (e_P - 1)$$

where $N \geq 1$ is the degree of φ and where the sum is taken over the ramification points P of φ with ramification index $e_P \geq 1$. The fact that the right hand side of this equality is ≥ 0 implies that $N = 1$, i.e. that φ has degree 1 and hence is an automorphism.

The fact that the group of automorphisms of X is finite and has order at most $84(g-1)$ is a classical result due to Hurwitz [Hur92]. □

Proof of Proposition 15. Since $\mathbf{K} = \bigcup_{d\geq 1} \mathbf{K}_{d!}$ is the increasing union of the fields $\mathbf{K}_{d!}$, the fact that $\mathbf{K}$ is a $\mathcal{C}^1$-field follows from Tsen's theorem [Lan52] (according to which the function field of any algebraic curve over an algebraically closed field, e.g. $\mathbf{K}_{d!}$, is $\mathcal{C}^1$).

Let L be a finite extension of $\mathbf{K}$ such that ϕ_p extends to a field endomorphism of L; we have to prove that $L = \mathbf{K}$. The primitive element theorem ensures that there exists $u \in L$ such that $L = \mathbf{K}(u)$. Let $d \in \mathbb{Z}_{\geq 1}$ be such that

- u is algebraic over $\mathbf{K}_d$,
- $\phi_p(u) \in \mathbf{K}_d(u)$.

Then, $\mathbf{K}_d(u)$ is a finite extension of $\mathbf{K}_d$, and ϕ_p induces an endomorphism of $\mathbf{K}_d(u)$.

Consider a morphism of smooth projective curves $\varphi : X \to \mathbb{P}^1(\overline{\mathbb{Q}})$ whose induced morphism of function fields "is" the inclusion $\mathbf{K}_d \subset \mathbf{K}_d(u)$. Then ϕ_p induces an endomorphism f of X such that the following diagram is commutative:

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} \\ \mathbb{P}^1(\overline{\mathbb{Q}}) & \xrightarrow[z\mapsto z^p]{} & \mathbb{P}^1(\overline{\mathbb{Q}}). \end{array}$$

Observe that

- X has genus $g = 0$ or 1 (this follows from Proposition 16 since f has infinite order);
- f has degree p (take degrees in the above commutative diagram);
- $f^{-1}(\varphi^{-1}(0)) \subset \varphi^{-1}(0)$ and $f^{-1}(\varphi^{-1}(\infty)) \subset \varphi^{-1}(\infty)$ (immediate from the above commutative diagram);
- f is totally ramified above any point of $Z = \varphi^{-1}(0) \cup \varphi^{-1}(\infty)$ (indeed, since f is not constant, it is surjective and, for cardinality reasons, the inclusion $f^{-1}(\varphi^{-1}(0)) \subset \varphi^{-1}(0)$ implies that the fiber of f above any element of $\varphi^{-1}(0)$ has exactly one element).

Assume that $g = 0$, so that we can replace X by $\mathbb{P}^1(\overline{\mathbb{Q}})$. Hurwitz's formula (see [Har77, Corollary 2.4]) applied to f yields the equation

$$-2 = -2p + \sum_P (e_P - 1) = -2p + \underbrace{\sum_{Q \in Z} \left(p - \sharp f^{-1}(Q)\right)}_{= \sharp Z \cdot (p-1) \geq 2(p-1)} + \sum_{Q \notin Z} \left(p - \sharp f^{-1}(Q)\right),$$

where the sum in the middle term is taken over the ramification points P of f with ramification index $e_P \geq 1$. This implies that $\sharp Z = 2$, so $\sharp\varphi^{-1}(0) = \sharp\varphi^{-1}(\infty) = 1$, and that f is unramified above $X \setminus Z$. Let c be an automorphism of $\mathbb{P}^1(\overline{\mathbb{Q}})$ such that $c(\varphi^{-1}(0)) = 0$ and $c(\varphi^{-1}(\infty)) = \infty$. Then, cfc^{-1} is totally ramified at 0 and ∞, unramified elsewhere, of degree p, and fixes 0 and ∞, so $cfc^{-1}(z) = z^p$. It follows from the commutative diagram

$$\begin{array}{ccc} \mathbb{P}^1(\overline{\mathbb{Q}}) & \xrightarrow{cfc^{-1}} & \mathbb{P}^1(\overline{\mathbb{Q}}) \\ {\scriptstyle \varphi c^{-1}}\downarrow & & \downarrow{\scriptstyle \varphi c^{-1}} \\ \mathbb{P}^1(\overline{\mathbb{Q}}) & \xrightarrow[z \mapsto z^p]{} & \mathbb{P}^1(\overline{\mathbb{Q}}) \end{array}$$

that $\varphi c^{-1}(z) = z^N$ for some $N \in \mathbb{Z}_{\geq 1}$. That is, $\varphi = c^N$ and $f(z) = c^{-1}(c(z)^p)$. It follows that $\mathbf{K}_d(u) = \overline{\mathbb{Q}}(z_d^{1/N})$. In particular, u belongs to $\mathbf{K}$ and hence $L = \mathbf{K}$.

Assume that $g = 1$, i.e. that X is an elliptic curve. Then f is unramified (as any non-constant endomorphism of an elliptic curve) of degree p. Considering cardinals in the inclusion $f^{-1}(\varphi^{-1}(0)) \subset \varphi^{-1}(0)$, we get that the degree of f is equal to 1, so $p = 1$, which is excluded. □

We will mainly work with the base fields $\mathbf{K}$ and $\widehat{\mathbf{K}}$; however, we will also use the difference subfield of $\widehat{\mathbf{K}}$ given by

$$\widehat{\mathbf{K}}_{p^\infty} = \bigcup_{d \geq 0} \overline{\mathbb{Q}}((z^{1/p^d}))$$

and its difference subfield given by

$$\mathbf{K}_{p^\infty} = \bigcup_{d \geq 0} \overline{\mathbb{Q}}(z^{1/p^d}).$$

We will use the following result.

Proposition 17. *Let L be a finite field extension of $\mathbf{K}_{p^\infty}$ such that ϕ_p extends to an endomorphism of L. Then, there exists $\alpha \in L$ such that $\alpha^n = z$ for some integer $n \geq 1$, and $L = \mathbf{K}_{p^\infty}(\alpha)$.*

Proof. Same arguments as for the proof of Proposition 15. □

4. Factorization, triangularization and local exponents

4.1. **Factorization of Mahler operators.** In order to avoid heavy notation, we work in this section with

$$L = \sum_{i=0}^{n} a_i \phi_p^i \text{ where } n \geq 1,\ a_0, \dots, a_n \in \overline{\mathbb{Q}}((z)) \text{ and } a_0 a_n \neq 0.$$

The extension of the results below to an arbitrary $L \in \widehat{\mathcal{D}}$ is straightforward.

We shall now introduce some notation and terminology. Let a, r be elements of some difference field extension of $\widehat{\mathbf{K}}$ such that $\phi_p(r) = ar$. We will denote by $L^{[r]}$ the operator defined by

$$L^{[r]} := r^{-1} L r = \sum_{i=0}^{n} a \phi_p(a) \cdots \phi_p^{i-1}(a) a_i \phi_p^i,$$

so that $L^{[r]}(f) = 0$ if and only if $L(rf) = 0$. In particular:

- for any $\mu \in \mathbb{Q}$, we consider θ_μ such that $\phi_p(\theta_\mu) = z^\mu \theta_\mu$ so that

$$L^{[\theta_\mu]} = \sum_{i=0}^{n} z^{(1+p+\cdots+p^{i-1})\mu} a_i \phi_p^i;$$

- for any $c \in \overline{\mathbb{Q}}^\times$, we consider e_c such that $\phi_p(e_c) = c e_c$ so that

$$L^{[e_c]} = \sum_{i=0}^{n} c^i a_i \phi_p^i.$$

We define the Newton polygon $\mathcal{N}(L)$ of L as the convex hull in $\mathbb{R}^2$ of

$$\{(i, j) \in \mathbb{Z} \times \mathbb{R} \mid j \geq v_z(a_{n-i})\}$$

where $v_z : \widehat{\mathbf{K}} \to \mathbb{Q} \cup \{+\infty\}$ denotes the z-adic valuation. This polygon is delimited by two vertical half lines and by k vectors $(r_1, d_1), \dots, (r_k, d_k) \in \mathbb{N}^* \times \mathbb{Q}$ having pairwise distinct slopes, called the Newton-slopes of L. For any $i \in \{1, \dots, k\}$, r_i is called the multiplicity of the Newton-slope $\frac{d_i}{r_i}$.

Lemma 18. *There exists a unique $\mu_1 \in \mathbb{Q}$ such that the greatest Newton-slope of $L^{[\theta_{\mu_1}]}$ is 0.*

Proof. The fact that the greatest Newton-slope of $L^{[\theta_{\mu_1}]}$ is 0 means that, for all $i \in \{1, \dots, n\}$,

$$v_z(a_i) + (1 + p + \cdots + p^{i-1})\mu_1 \geq v_z(a_0)$$

and that this inequality is an equality for some $i \in \{1, \dots, n\}$. It is easily seen that there exists a unique $\mu_1 \in \mathbb{Q}$ with these properties. □

Definition 19. The rational number μ_1 given by Lemma 18 will be called the first theta-slope of L. Set $L^{[\theta_{\mu_1}]} = \sum_{i=0}^n b_i \phi_p^i$. The characteristic polynomial associated to the first theta-slope μ_1 of L is $\sum_{i=0}^n \left(b_i z^{-v_z(b_0)}\right)_{|z=0} X^i \in \overline{\mathbb{Q}}[X]$; this is a polynomial of degree ≥ 1 with non-zero constant coefficient.

Lemma 20. *Let μ_1 be the first theta-slope of L and let c_1 be a root of the corresponding characteristic polynomial. Let $d_1 \in \mathbb{Z}_{\geq 1}$ be a denominator of μ_1. Then, there exists $f_1 \in 1 + z_{d_1}\overline{\mathbb{Q}}[[z_{d_1}]]$ such that $L(\theta_{\mu_1} e_{c_1} f_1) = 0$.*

Proof. We set $\mu = \mu_1$, $c = c_1$ and $d = d_1$. Note that the coefficients of $L^{[\theta_\mu]}$ belong to $\overline{\mathbb{Q}}((z_d))$. We set $L^{[\theta_\mu]} = \sum_{i=0}^n b_i \phi_p^i$ with $b_i = \sum_j b_{i,j} z_d^j \in \overline{\mathbb{Q}}((z_d))$. Using the fact that the greatest Newton-slope of $L^{[\theta_\mu]}$ is 0, we see that, up to left multiplication by some element of $\overline{\mathbb{Q}}((z_d))^\times$, we can assume that $b_0, \dots, b_n \in \overline{\mathbb{Q}}[[z_d]]$ and $b_{0,0} \neq 0$. The characteristic polynomial attached to the first theta-slope μ of L is given, up to multiplication by some constant in $\overline{\mathbb{Q}}^\times$, by $\sum_{i=0}^n b_{i,0} X^i$. For $f = \sum_{k\geq 0} f_k z_d^k \in 1 + z_d\overline{\mathbb{Q}}[[z_d]]$, we have

$$L(\theta_\mu e_c f) = \theta_\mu e_c \sum_{i,j,k\geq 0} b_{i,j} c^i f_k z_d^{j+kp^i} = 0$$

if and only if, for all $\ell \in \mathbb{Z}_{\geq 0}$,

$$\sum_{\substack{i,j,k\geq 0 \\ j+kp^i=\ell}} b_{i,j} c^i f_k = 0. \tag{9}$$

This equation is automatically satisfied for $\ell = 0$ because

$$\sum_{\substack{i,j,k\geq 0 \\ j+kp^i=0}} b_{i,j} c^i f_k = \left(\sum_i b_{i,0} c^i\right) f_0$$

and $\sum_i b_{i,0} c^i = 0$ because c is a root of the characteristic polynomial. For $\ell > 0$, equation (9) can be rewritten as

$$\sum_{\substack{i,j,k\geq 0 \\ k<\ell, j+kp^i=\ell}} b_{i,j} c^i f_k = -b_{0,0} f_\ell$$

so that the coefficients of f are (uniquely) recursively determined. □

Lemma 21. *Maintaining the notation of Lemma 20, we can factorize L as*

$$L = L_2(\phi_p - z^{\mu_1} c_1) f_1^{-1}$$

where $L_2 \in \widehat{\mathcal{D}}$ has coefficients in $\overline{\mathbb{Q}}((z^{1/(p^m d_1)}))$ for some $m \in \mathbb{Z}$.

Proof. This follows by euclidean division of L by the operator $(\phi_p - z^{\mu_1} c_1) f_1^{-1}$ which annihilates $\theta_{\mu_1} e_{c_1} f_1$. □

A repeated application of the previous lemma leads to the following result.

Theorem 22. *The operator L admits a factorization of the form*

$$L = a_n \phi_p^n(f_1) \cdots \phi_p(f_n)(\phi_p - z^{\mu_n} c_n) f_n^{-1} \cdots (\phi_p - z^{\mu_1} c_1) f_1^{-1}$$

where, for all $i \in \{1, \dots, n\}$, $c_i \in \overline{\mathbb{Q}}^\times$, $\mu_i \in \mathbb{Q}$ and $f_i \in 1 + z_d\overline{\mathbb{Q}}[[z_d]]$ for some integer $d \geq 1$.

4.2. **Triangularization and local exponents of the $\widehat{\mathcal{D}}$-modules.** We shall first study the $\widehat{\mathcal{D}}$-modules of rank one. For any $\alpha \in \widehat{\mathbf{K}}^\times$, we denote by I_α the $\widehat{\mathcal{D}}$-module of rank one defined by

$$I_\alpha = \widehat{\mathcal{D}}/\widehat{\mathcal{D}}(\phi_p - \alpha).$$

In what follows, we will denote by $\mathrm{cld}(\alpha)$ the coefficient of the term of lowest degree of $\alpha \in \widehat{\mathbf{K}}^\times$. Note that $\mathrm{cld} : \widehat{\mathbf{K}}^\times \to \overline{\mathbb{Q}}^\times$ is a group morphism.

Proposition 23.

(i) *For any $\alpha, \beta \in \widehat{\mathbf{K}}^\times$, the $\widehat{\mathcal{D}}$-modules I_α and I_β are isomorphic if and only if* $\mathrm{cld}(\alpha) = \mathrm{cld}(\beta)$.

(ii) *For any $\alpha \in \widehat{\mathbf{K}}^\times$, the $\widehat{\mathcal{D}}$-modules I_α and $I_{\mathrm{cld}(\alpha)}$ are isomorphic.*

(iii) *For any $\widehat{\mathcal{D}}$-module M of rank one, there exists a unique $c \in \overline{\mathbb{Q}}^\times$ such that M is isomorphic to I_c.*

Proof. It is easily seen that the set of $\widehat{\mathcal{D}}$-module morphisms from I_α to I_β is given by

$$\mathrm{Hom}(I_\alpha, I_\beta) = \{\varphi_u \mid u \in \widehat{\mathbf{K}}, \alpha u = \phi_p(u)\beta\}$$

where $\varphi_u : I_\alpha \to I_\beta$ is defined by $\varphi_u(\overline{P}) = \overline{Pu}$ and that φ_u is an isomorphism if and only if $u \in \widehat{\mathbf{K}}^\times$. Therefore, $I_\alpha \cong I_\beta$ if and only if there exists $u \in \widehat{\mathbf{K}}^\times$ such that $\alpha u = \phi_p(u)\beta$. But $\{\phi_p(u)/u \mid u \in \widehat{\mathbf{K}}^\times\} = \ker(\mathrm{cld} : \widehat{\mathbf{K}}^\times \to \overline{\mathbb{Q}}^\times)$. So $I_\alpha \cong I_\beta$ if and only if $\mathrm{cld}(\alpha) = \mathrm{cld}(\beta)$. This proves (i). The remaining assertions follow easily. □

Theorem 24. *Let M be a $\widehat{\mathcal{D}}$-module of rank $n \geq 1$.*

(i) *The $\widehat{\mathcal{D}}$-module M is triangularizable; i.e. there exists a filtration*

$$\{0\} = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

by submodules of M such that, for all $i \in \{0, \ldots, n-1\}$, the quotient $\widehat{\mathcal{D}}$-module M_{i+1}/M_i has rank one.

(ii) *For all $i \in \{0, \ldots, n-1\}$, we let $c_i \in \overline{\mathbb{Q}}^\times$ be such that $M_{i+1}/M_i \cong I_{c_i}$. The list $c_1, \ldots, c_n$ does not depend (up to permutation) on the chosen filtration.*

Proof. According to the cyclic vector lemma (Proposition 13), there exists $L \in \widehat{\mathcal{D}}$ such that $M \cong \widehat{\mathcal{D}}/\widehat{\mathcal{D}}L$. Theorem 22 ensures that

$$L = c(\phi_p - z^{\mu_n} c_n) f_n^{-1} \cdots (\phi_p - z^{\mu_1} c_1) f_1^{-1}$$

with $c \in \overline{\mathbb{Q}}((z_d))$, $c_i \in \overline{\mathbb{Q}}^\times$, $\mu_i \in \mathbb{Q}$ and $f_i \in 1 + z_d\overline{\mathbb{Q}}[[z_d]]$ for some $d \in \mathbb{Z}_{\geq 1}$. We deduce from this factorization a filtration

$$\{0\} = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

such that, for all $i \in \{0, \ldots, n-1\}$, $M_{i+1}/M_i \cong I_{z^{\mu_i} c_i} \cong I_{c_i}$ has rank one. This proves (i).

By the Jordan-Hölder theorem, if

$$\{0\} = N_0 \subset N_1 \subset \cdots \subset N_m = M$$

is another filtration of M such that, for all $i \in \{0, \ldots, m-1\}$, N_{i+1}/N_i has rank one and hence is isomorphic to I_{d_i} for some $d_i \in \overline{\mathbb{Q}}^\times$, then $m = n$ and there exists a permutation σ of $\{1, \ldots, n\}$ such that $M_{\sigma(i)+1}/M_{\sigma(i)} \cong N_{i+1}/N_i$. Proposition 23 ensures that $c_{\sigma(i)} = d_i$, whence (ii). □

Definition 25. The exponents at 0 of the $\widehat{\mathcal{D}}$-module M are the non-zero complex numbers $c_1, \dots, c_n$ introduced in Theorem 24.

It will be convenient to introduce the notion of exponents for Mahler operators.

Definition 26. The exponents at 0 of $L \in \widehat{\mathcal{D}}$ are the exponents of the $\widehat{\mathcal{D}}$-module $\widehat{\mathcal{D}}/\widehat{\mathcal{D}}L$.

Note the following result.

Proposition 27. *Let M be a $\widehat{\mathcal{D}}$-module of rank $n \geq 1$. Assume that $M \cong \widehat{\mathcal{D}}/\widehat{\mathcal{D}}L$ for some $L \in \widehat{\mathcal{D}}$ such that $L = c(\phi_p - \alpha_n)\cdots(\phi_p - \alpha_1)$ for some $c, \alpha_1, \dots, \alpha_n \in \widehat{\mathbf{K}}^\times$. Then, the exponents of L and of M at 0 are $\mathrm{cld}(\alpha_1), \dots, \mathrm{cld}(\alpha_n)$.*

Proof. Indeed, the factorization $L = c(\phi_p - \alpha_n)\cdots(\phi_p - \alpha_1)$ induces a filtration

$$\{0\} = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

of M such that, for all $i \in \{0, \dots, n-1\}$, $M_{i+1}/M_i \cong I_{\alpha_i} \cong I_{\mathrm{cld}(\alpha_i)}$. □

4.3. **Focus on the operators of order 2.** We shall now collect some results about the operators of order 2, which will be used later in the paper. Consider an operator of order 2:

$$L = \phi_p^2 + a\phi_p + b \in \widehat{\mathcal{D}} \text{ with } a \in \overline{\mathbb{Q}}((z)) \text{ and } b \in \overline{\mathbb{Q}}((z))^\times.$$

The proof of Lemma 18 shows that the first theta-slope μ_1 of L is the unique rational number such that

- $(1+p)\mu_1 \geq v_z(b)$,
- $v_z(a) + \mu_1 \geq v_z(b)$,
- either $(1+p)\mu_1 = v_z(b)$ or $v_z(a) + \mu_1 = v_z(b)$,

i.e.

$$\mu_1 = \max\left\{\frac{v_z(b)}{1+p}, v_z(b) - v_z(a)\right\}.$$

Let $d_1 \in \mathbb{Z}_{\geq 1}$ be a denominator of μ_1. Let $c_1 \in \overline{\mathbb{Q}}^\times$ be a root of the characteristic polynomial of L associated to its first theta-slope μ_1. Theorem 22 ensures that

$$L = \phi_p^2(f_1)\phi_p(f_2)(\phi_p - c_2 z^{\mu_2})f_2^{-1}(\phi_p - c_1 z^{\mu_1})f_1^{-1} \tag{10}$$

for some $f_1 \in 1 + z_{d_1}\overline{\mathbb{Q}}[[z_{d_1}]]$, $c_2 \in \overline{\mathbb{Q}}^\times$, $\mu_2 \in \mathbb{Q}$ and $f_2 \in 1 + z_{d_2}\overline{\mathbb{Q}}[[z_{d_2}]]$ ($d_2 \in \mathbb{Z}_{\geq 1}$). Equating the terms of degree 0 in (10), we get

$$c_1 z^{\mu_1} c_2 z^{\mu_2} \phi_p^2(f_1)\phi_p(f_2)f_1^{-1}f_2^{-1} = b.$$

Therefore, $c_1 c_2 = \mathrm{cld}(b)$, $\mu_1 + \mu_2 = v_z(b)$ (so d_1 is also a denominator of μ_2) and $f_2 \in 1 + z_{d_1}\overline{\mathbb{Q}}[[z_{d_1}]]$.

The following result will be used later in this paper.

Proposition 28. *Let $f \in \widehat{\mathbf{K}}$ be such that $L(f) = 0$. Then $f \in \overline{\mathbb{Q}}((z_{d_1' p^j}))$ for some $j \in \mathbb{Z}$, where $d_1' = (p-1)d_1$.*

We will give the proof after the following two lemmas.

Lemma 29. *We can decompose L as follows:*

$$L = \phi_p^2(g_1)\phi_p(g_2)(\phi_p - c_2)g_2^{-1}(\phi_p - c_1)g_1^{-1} \tag{11}$$

for some $g_1, g_2 \in \overline{\mathbb{Q}}((z_{d_1'}))$.

Proof. This follows from equation (10) by using the identity

$$\phi_p - c_i z^{\mu_i} = \phi_p(z^{\frac{\mu_i}{p-1}})(\phi_p - c_i)(z^{\frac{\mu_i}{p-1}})^{-1}.$$

□

Lemma 30. *Let $f \in \widehat{\mathbf{K}}$ be such that $(\phi_p - c)(f) \in \overline{\mathbb{Q}}((z_m))$ for some $m \in \mathbb{Z}_{\geq 1}$ and $c \in \overline{\mathbb{Q}}^{\times}$. Then, there exists $j \in \mathbb{Z}$ such that $f \in \overline{\mathbb{Q}}((z_{mp^j}))$.*

Proof. Let $f = \sum_{k\in\mathbb{Z}} f_k z_n^k \in \overline{\mathbb{Q}}((z_n))$ be such that

$$(\phi_p - c)(f) = \sum_{k\in p\mathbb{Z}} (f_{k/p} - cf_k) z_n^k - \sum_{k\in\mathbb{Z}\setminus p\mathbb{Z}} cf_k z_n^k \in \overline{\mathbb{Q}}((z_m)). \tag{12}$$

Consider $k \in \mathbb{Z}$ such that $p \nmid k$ and $k/n \notin \frac{1}{m}p^{\mathbb{Z}}\mathbb{Z}$. In particular, we have $p \nmid k$ and $k/n \notin \frac{1}{m}\mathbb{Z}$. Equation (12) ensures that $f_k = 0$. Moreover, we have $p \mid kp$ and $kp/n \notin \frac{1}{m}\mathbb{Z}$. Equation (12) ensures that $f_k - cf_{kp} = 0$ and, hence, $f_{kp} = 0$. Repeating this argument, we obtain that $f_{kp^j} = 0$ for all integers $j \geq 0$. So, we have proved that $f_k = 0$ if $k/n \notin \frac{1}{m}p^{\mathbb{Z}}\mathbb{Z}$, whence the result. □

Proof of Proposition 28. Follows from the decomposition of L given by formula (11) and Lemma 30. □

The following corollary will be essential for the algorithmic considerations of section 6.

Corollary 31. *Let us consider $u, v \in \widehat{\mathbf{K}}$ such that $L = (\phi_p - v)(\phi_p - u)$. Then $u, v \in \overline{\mathbb{Q}}((z_{d_1'}))$.*

Proof. Let $c = \mathrm{cld}(u)$ and $\alpha = v_z(u)$, so that $u \in cz^{\alpha}(1 + z_n\overline{\mathbb{Q}}[[z_n]])$ for some $n \in \mathbb{Z}_{\geq 1}$. There exists $f \in 1 + z_n\overline{\mathbb{Q}}[[z_n]]$ such that $y = e_c z^{\frac{\alpha}{p-1}} f$ satisfies $(\phi_p - u)(y) = 0$ so $z^{\frac{\alpha}{p-1}} f$ is a solution of $L^{[e_c]}$. It follows from Proposition 28 (applied to $L^{[e_c]}$) that $z^{\frac{\alpha}{p-1}} f \in \overline{\mathbb{Q}}((z_{d_1'p^j}))$ for some $j \in \mathbb{Z}_{\geq 0}$. So $\alpha \in \frac{(p-1)}{d_1'p^j}\mathbb{Z} = \frac{1}{d_1p^j}\mathbb{Z}$ and $f \in \overline{\mathbb{Q}}((z_{d_1'p^j}))$. Therefore, $u = \frac{\phi_p(y)}{y} \in \overline{\mathbb{Q}}((z_{d_1'p^j}))$.

Now, a straightforward calculation shows that the equality $L = (\phi_p - v)(\phi_p - u)$ holds true if and only if $uv = b$ and $u(\phi_p(u) + a) = -b$. So $u = \frac{-b}{\phi_p(u)+a} \in \overline{\mathbb{Q}}\,(a, b, \phi_p(u)) \subset \overline{\mathbb{Q}}\,(z, \phi_p(u))$. It follows that $u \in \overline{\mathbb{Q}}((z_{d_1'}))$ and $v = b/u \in \overline{\mathbb{Q}}((z_{d_1'}))$. □

Note also the following result for further use.

Proposition 32. *Let us consider $u, v \in \widehat{\mathbf{K}}$ such that $L = (\phi_p - v)(\phi_p - u)$. Then, up to permuting u and v, we have $\mathrm{cld}(u) = c_1$ and $\mathrm{cld}(v) = c_2 = \mathrm{cld}(b)/c_1$.*

Proof. This a particular case of Proposition 27. □

5. The regular singular systems

5.1. **Definition.**

Definition 33. We say that the system $\phi_p Y = AY$ with $A \in \mathrm{GL}_n(\widehat{\mathbf{K}})$ is regular singular at 0 if there exists $F \in \mathrm{GL}_n(\widehat{\mathbf{K}})$ such that $\phi_p(F)A = A_0F$ for some $A_0 \in \mathrm{GL}_n(\overline{\mathbb{Q}})$.

If A_0 exists, then it is unique up to conjugation by an element of $\mathrm{GL}_n(\overline{\mathbb{Q}})$, and its list of eigenvalues, counted with multiplicities, coincides with the list of the exponents of $\phi_p Y = AY$ at 0.

Proposition 34. *If the z-adic valuations of the entries of $A \in \mathrm{GL}_n(\widehat{\mathbf{K}})$ are ≥ 0 and if $A(0) \in \mathrm{GL}_n(\overline{\mathbb{Q}})$, then $\phi_p Y = AY$ is regular singular at 0. Moreover, the exponents of $\phi_p Y = AY$ are the eigenvalues of $A(0)$.*

Proof. We claim that there exists a unique $F \in I_n + z_d \,\mathrm{M}_n(\overline{\mathbb{Q}}[[z_d]])$ such that $\phi_p(F)A = A(0)F$, where $d \in \mathbb{Z}_{\geq 1}$ is such that $A = \sum_{j\geq 0} A_j z_d^j \in \mathrm{GL}_n(\overline{\mathbb{Q}}((z_d)))$. Indeed, for any $F = \sum_{k\geq 0} F_k z^k \in I_n + z_d \,\mathrm{M}_n(\overline{\mathbb{Q}}[[z_d]])$, we have $\phi_p(F)A = \sum_{\ell\geq 0} \left(\sum_{\substack{j,k\geq 0 \\ kp+j=\ell}} F_k A_j \right) z_d^\ell$, so $\phi_p(F)A = A(0)F$ if and only if, for all $\ell \in \mathbb{Z}_{\geq 0}$,

$$\sum_{\substack{j,k\geq 0 \\ kp+j=\ell}} F_k A_j = A(0)F_\ell.$$

This equation is satisfied for $\ell = 0$, and the coefficients F_ℓ, $\ell \geq 1$, are determined inductively. Therefore, the system $\phi_p Y = AY$ is regular singular, and its exponents are the eigenvalues of $A(0)$. □

5.2. **Universal Picard-Vessiot ring and Galois group.** Let $(X_c)_{c\in\overline{\mathbb{Q}}^\times}$ and Y be indeterminates over $\widehat{\mathbf{K}}$, and consider the quotient ring

$$\mathscr{U} := \widehat{\mathbf{K}}[(X_c)_{c\in\overline{\mathbb{Q}}^\times}, Y]/I$$

of the polynomial ring $\widehat{\mathbf{K}}[(X_c)_{c\in\overline{\mathbb{Q}}^\times}, Y]$ by its ideal I generated by $\{X_c X_d - X_{cd} \mid c, d \in \overline{\mathbb{Q}}^\times\} \cup \{X_1 - 1\}$. Let e_c (resp. ℓ) be the image of X_c (resp. Y) in $\mathscr{U}$, so that

$$\mathscr{U} = \widehat{\mathbf{K}}[(e_c)_{c\in\overline{\mathbb{Q}}^\times}, \ell].$$

We endow $\mathscr{U}$ with its ring automorphism ϕ such that $\phi_{|\widehat{\mathbf{K}}} = \phi_p$,

$$\forall c \in \mathbb{C}^\times,\ \phi(e_c) = c e_c \text{ and } \phi(\ell) = \ell + 1.$$

Hence, $(\mathscr{U}, \phi)$ is a difference ring extension of $(\widehat{\mathbf{K}}, \phi_p)$.

Theorem 35. *The difference ring $\mathscr{U}$ is the universal Picard-Vessiot ring for the regular singular Mahler systems over $\widehat{\mathbf{K}}$, i.e.:*

- *$\mathscr{U}$ is a simple difference ring extension of $\widehat{\mathbf{K}}$;*
- *the ring of constants $\mathscr{U}^\phi$ of $\mathscr{U}$ is $\overline{\mathbb{Q}}$;*
- *every regular singular Mahler system with coefficients in $\widehat{\mathbf{K}}$ has a fundamental matrix of solutions with entries in $\mathscr{U}$;*
- *no proper difference subring of $\mathscr{U}$ has the above three properties.*

We shall first prove a series of lemmas.

Lemma 36. *We let $B = \widehat{\mathbf{K}}[(e_c)_{c\in\overline{\mathbb{Q}}^\times}] \subset \mathscr{U} = B[\ell]$. The following properties hold:*

(i) *$(e_c)_{c\in\overline{\mathbb{Q}}^\times}$ is a basis of the $\widehat{\mathbf{K}}$-vector space B;*
(ii) *ℓ is transcendental over B.*

Proof. The relations $e_c e_d = e_{cd}$ and $e_1 = 1$ ensure that B is generated as a $\widehat{\mathbf{K}}$-vector space by $(e_c)_{c\in\overline{\mathbb{Q}}^\times}$. Let $(\lambda_c)_{c\in\overline{\mathbb{Q}}^\times} \in \widehat{\mathbf{K}}^{(\overline{\mathbb{Q}}^\times)}$ be such that $\sum_{c\in\overline{\mathbb{Q}}^\times} \lambda_c e_c = 0$. This means that $\sum_{c\in\overline{\mathbb{Q}}^\times} \lambda_c X_c \in I$. For all $m \in \mathbb{Z}$, taking the image of this relation by the evaluation morphism $\widehat{\mathbf{K}}[(X_c)_{c\in\overline{\mathbb{Q}}^\times}, Y] \to \overline{\mathbb{Q}}$ defined by $X_c \mapsto c^m$ and $Y \mapsto 0$, we get $\sum_{c\in\overline{\mathbb{Q}}^\times} \lambda_c c^m = 0$. It follows that, for all $c \in \overline{\mathbb{Q}}^\times$, $\lambda_c = 0$ and hence $(e_c)_{c\in\overline{\mathbb{Q}}^\times}$ is free over $\widehat{\mathbf{K}}$. This proves (i).

The proof of claim (ii) is left to the reader. □

Lemma 37. *Consider $c \in \overline{\mathbb{Q}}^\times$ and $\lambda \in \widehat{\mathbf{K}}$. If $\phi(\lambda) = c\lambda$ and $c \neq 1$, then $\lambda = 0$.*

Proof. Up to replacing z by z^d, for a suitable integer $d \geq 1$, we can assume that $\lambda = \sum_{k\geq N} a_k z^k \in \overline{\mathbb{Q}}((z))$. We have

$$\phi(\lambda) - c\lambda = -c \sum_{k\geq N, p\nmid k} a_k z^k + \sum_{k\geq N, p\mid k} (a_{k/p} - ca_k) z^k = 0.$$

So $a_k = 0$ if $p \nmid k$. Moreover, for $k \neq 0$, $p \mid k$, we have $a_k = c^{-1} a_{k/p} = \cdots = c^{-v_p(k)} a_{k/p^{v_p(k)}} = 0$, where v_p denotes the p-adic valuation. Lastly, $a_0 - ca_0 = 0$ and hence $a_0 = 0$. □

Lemma 38. *Consider $c \in \overline{\mathbb{Q}}$ and $\lambda \in \widehat{\mathbf{K}}$. If $\phi(\lambda) = \lambda + c$, then $c = 0$.*

Proof. Follows from the fact that the constant coefficient of $\phi(\lambda) - \lambda$ is 0. □

Proof of Theorem 35. We shall first prove that $\mathscr{U}^\phi = \overline{\mathbb{Q}}$. Let $y = \sum_{k=0}^n a_k \ell^k$ ($a_k \in B$) be a non-zero element of $\mathscr{U}^\phi$ of minimal degree n in ℓ. So, we have

$$0 = \phi(y) - y = \sum_{k=0}^n \phi(a_k)(\ell+1)^k - \sum_{k=0}^n a_k \ell^k. \tag{13}$$

Identifying the coefficients of degree n in ℓ, we obtain

$$\phi(a_n) - a_n = 0.$$

Let $(\lambda_{n,c})_{c\in\overline{\mathbb{Q}}^\times} \in \widehat{\mathbf{K}}^{(\overline{\mathbb{Q}}^\times)}$ be such that $a_n = \sum_{c\in\overline{\mathbb{Q}}^\times} \lambda_{n,c} e_c$. We have

$$\phi(a_n) - a_n = \sum_{c\in\overline{\mathbb{Q}}^\times} (\phi(\lambda_{n,c})c - \lambda_{n,c}) e_c = 0$$

so $\phi(\lambda_{n,c})c - \lambda_{n,c} = 0$. According to Lemma 37, we must have $\lambda_{n,c} = 0$ for $c \neq 1$ and we have $\lambda_{n,1} \in \overline{\mathbb{Q}}$. So $a_n \in \overline{\mathbb{Q}}^\times$. If $n = 0$, then we get $y \in \overline{\mathbb{Q}}^\times$, as expected. We shall now prove that we necessarily have $n = 0$. Assume to the contrary that $n \geq 1$. Equating the coefficients of degree $n-1$ in ℓ in equation (13), we get

$$\phi(a_{n-1}) - a_{n-1} = -na_n.$$

Let $(\lambda_{n-1,c})_{c\in\overline{\mathbb{Q}}^\times} \in \widehat{\mathbf{K}}^{(\overline{\mathbb{Q}}^\times)}$ be such that $a_{n-1} = \sum_{c\in\overline{\mathbb{Q}}^\times} \lambda_{n-1,c} e_c$. We have

$$\phi(a_{n-1}) - a_{n-1} = \sum_{c\in\overline{\mathbb{Q}}^\times} (\phi(\lambda_{n-1,c})c - \lambda_{n-1,c}) e_c = -na_n = -na_n e_1$$

so $\phi(\lambda_{n-1,c})c - \lambda_{n-1,c} = 0$ for $c \neq 1$ and $\phi(\lambda_{n-1,1}) - \lambda_{n-1,1} = -na_n$. According to Lemma 38, the last equation is impossible.

Note that ϕ induces a ring automorphism of B, so that (B, ϕ) is a difference ring (simply denoted by B). We shall now prove that B is a simple difference ring.

Let J be a non-zero difference ideal of B. Let $b = \sum_{c\in\overline{\mathbb{Q}}^\times} \lambda_c e_c$ ($(\lambda_c)_{c\in\overline{\mathbb{Q}}^\times} \in \widehat{\mathbf{K}}^{(\overline{\mathbb{Q}}^\times)}$) be a non-zero element of J such that the cardinality of the support of $(\lambda_c)_{c\in\overline{\mathbb{Q}}^\times}$ is minimal. Let $c_0 \in \overline{\mathbb{Q}}^\times$ be such that $\lambda_{c_0} \neq 0$; up to replacing b by b/λ_{c_0} we can assume that $\lambda_{c_0} = 1$. Then, considering the cardinality of the support of $b - \phi(b) \in J$, we get $0 = b - \phi(b) = \sum_{c\in\overline{\mathbb{Q}}^\times} (\lambda_c - \phi(\lambda_c)c)e_c$. Therefore, for all $c \in \overline{\mathbb{Q}}^\times$, $\lambda_c - c\phi(\lambda_c) = 0$, so, according to Lemma 37, $\lambda_c = 0$ for $c \neq 1$ and $\lambda_1 \in \overline{\mathbb{Q}}$. It follows that $b = \lambda_1 \in \mathscr{U}^\times$ and hence $J = B$.

We shall now prove that $\mathscr{U}$ is a simple difference ring. Let J be a non-zero difference ideal of $\mathscr{U}$. Let n be the minimal degree in ℓ of the non-zero elements of J. The set E made up of the coefficients of ℓ^n in the elements of J of degree $\leq n$ in ℓ is a non-zero difference ideal of B. Therefore, $E = B$. So, there exists a non-zero element $y = \ell^n + \sum_{k=0}^{n-1} a_k \ell^k \in \mathscr{U} = B[\ell]$ ($a_k \in B$) of degree n in ℓ, which is unitary in ℓ. Considering the degree in ℓ of $\phi(y) - y \in J$, we get $\phi(y) - y = 0$, i.e. $y \in \mathscr{U}^\phi = \overline{\mathbb{Q}}$. As $y \neq 0$, we deduce that $J = \mathscr{U}$, as expected.

In order to prove that any regular singular difference system $\phi_p Y = AY$ over $\widehat{\mathbf{K}}$ has a fundamental matrix of solutions with entries in $\mathscr{U}$, it is clearly sufficient to consider the case that $A \in \mathrm{GL}_n(\overline{\mathbb{Q}})$. Using Dunford decomposition, we are reduced to the cases $n = 1$ or A unipotent of maximal unipotent index. Here are explicit constructions of fundamental systems of solutions in these two cases:

- for $c \in \overline{\mathbb{Q}}^\times$, e_c is a fundamental solution in $\mathscr{U}$ of $\phi_p y = cy$;
- for $A = U \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ unipotent,

$$e_A := \exp(\ell \log(U)) = \sum_{k=0}^{n} \binom{\ell}{k} (U - I_n)^k,$$

  where $I_n \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ is the identity matrix, is a fundamental matrix of solutions in $\mathscr{U}$ of $\phi_p Y = UY$.

The minimality property of $\mathscr{U}$ is easy to deduce from what precedes, and the details are left to the reader. □

We shall now describe the corresponding universal difference Galois group

$$G := \{\sigma \in \mathrm{Aut}(\mathscr{U}/\widehat{\mathbf{K}}) \mid \phi \circ \sigma = \sigma \circ \phi\}.$$

We have $\phi(\sigma(e_c)) = \sigma(\phi(e_c)) = \sigma(ce_c) = c\sigma(e_c)$. It follows that there exists $h(c) \in \overline{\mathbb{Q}}^\times$ such that $\sigma(e_c) = h(c)e_c$. Since $\sigma(e_{cd}) = \sigma(e_c)\sigma(e_d) = h(c)e_c h(d)e_d = h(c)h(d)e_{cd}$, we have $h(cd) = h(c)h(d)$. In other words, $h = \overline{\mathbb{Q}}^\times \to \overline{\mathbb{Q}}^\times$ is a group morphism. Moreover, $\phi(\sigma(\ell)) = \sigma(\phi(\ell)) = \sigma(\ell + 1) = \sigma(\ell) + 1$. It follows that $\sigma(\ell) = \ell + a$, for some $a \in \overline{\mathbb{Q}}$.

It follows clearly that G is made up of the $\widehat{\mathbf{K}}$-algebra morphism $\sigma : \mathscr{U} \to \mathscr{U}$ such that

$$\forall c \in \overline{\mathbb{Q}}^\times,\ \sigma(e_c) = h(c)e_c \text{ and } \sigma(\ell) = \ell + a$$

for some group morphism $h = \overline{\mathbb{Q}}^\times \to \overline{\mathbb{Q}}^\times$ and some $a \in \overline{\mathbb{Q}}$.

6. Difference Galois groups of the Mahler equations of order 2: Algorithmic aspects

Consider the Mahler equation

$$\phi_p^2(y) + a\phi_p(y) + by = 0 \text{ with } a \in \overline{\mathbb{Q}}(z) \text{ and } b \in \overline{\mathbb{Q}}(z)^\times \tag{14}$$

and denote by

$$\phi_p Y = AY \text{ with } A = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{Q}}(z))$$

the associated Mahler system.

Remark 39. We consider Mahler equations with coefficients in $\overline{\mathbb{Q}}(z)$ (instead of $\mathbf{K}$) in order to avoid heavy notation. What follows can be easily extended to equations with coefficients in $\mathbf{K}$.

We let $G \subset \mathrm{GL}_2(\overline{\mathbb{Q}})$ be the difference Galois group over $(\mathbf{K}, \phi_p)$ of equation (14). According to Proposition 15, G is an algebraic subgroup of $\mathrm{GL}_2(\overline{\mathbb{Q}})$ 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 $\mathrm{GL}_2(\overline{\mathbb{Q}})$ given in [NvdPT08, 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 $\mathrm{GL}_2(\overline{\mathbb{Q}})$). If G is reducible, we distinguish the following subcases:
  - The group G is completely reducible (i.e. is conjugate to some subgroup of the group of diagonal matrices in $\mathrm{GL}_2(\overline{\mathbb{Q}})$).
  - The group G is not completely reducible.
- The group G is irreducible (i.e. not reducible) and imprimitive (see section 7 for the definition).
- The group G is irreducible and is not imprimitive, and, in this case, there exists an algebraic subgroup μ of $\overline{\mathbb{Q}}^\times$ such that $G = \mu\,\mathrm{SL}_2(\overline{\mathbb{Q}})$. Therefore, $G = \{M \in \mathrm{GL}_2(\overline{\mathbb{Q}}) \mid \det(M) \in H\}$ where $H = \det(G) \subset \overline{\mathbb{Q}}^\times$. In order to determine H, one can use the fact that $H = \det(G)$ is the difference Galois group of $\phi_p y = (\det A)y = by$ (this follows for instance from tannakian duality).

Our first task, undertaken in the present section, is to study the reducibility of G. The imprimitivity of G will be considered in section 7.

6.1. **Riccati equation and irreducibility.** A straightforward calculation shows that, for $u \in \mathbf{K}$, $\phi_p - u$ is a right factor of $\phi_p^2 + a\phi_p + b$ if and only if

$$u(\phi_p(u) + a) = -b. \tag{15}$$

This non-linear difference equation is called the Riccati equation associated to equation (14).

Lemma 40. *The following statements hold:*

1. *If* (15) *has one and only one solution in* $\mathbf{K}$*, then* G *is reducible but not completely reducible.*
2. *If* (15) *has exactly two solutions in* $\mathbf{K}$*, then* G *is completely reducible but not an algebraic subgroup of* $\overline{\mathbb{Q}}^\times I_2$*.*
3. *If* (15) *has at least three solutions in* $\mathbf{K}$*, then it has infinitely many solutions in* $\mathbf{K}$ *and* G *is an algebraic subgroup of* $\overline{\mathbb{Q}}^\times I_2$*.*
4. *If none of the previous cases occur, then* G *is irreducible.*

Proof. The proof of this lemma is identical to that of [Hen98, Theorem 4.2]. However, we give a sketch of the proof here because some details will be used later in this paper.

(1) We assume that (15) has one and only one solution $u \in \mathbf{K}$. A straightforward calculation shows that

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

We deduce from this and from Proposition 15 that G is reducible.

Moreover, if G were completely reducible, then, according to Proposition 15, $\phi_p(T)AT^{-1}$ would be diagonal for some $T := (t_{i,j})_{1\leq i,j\leq 2} \in \mathrm{GL}_2(\mathbf{K})$. Equating the entries of the antidiagonal of $\phi_p(T)AT^{-1}$ with 0, we find that $-\frac{t_{21}}{t_{22}}, -\frac{t_{11}}{t_{12}} \in \mathbf{K}$ are solutions of the Riccati equation (15). Since $\det(T) \neq 0$, these solutions are distinct, whence a contradiction.

(2) Assume that (15) has exactly two solutions $u_1, u_2 \in \mathbf{K}$. We have

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

We deduce from this and from Proposition 15 that G is completely reducible.

Moreover, if G were an algebraic subgroup of $\overline{\mathbb{Q}}^\times I_2$, then, according to Proposition 15, there would exist $u \in \mathbf{K}$ and $T = (t_{i,j})_{1\leq i,j\leq 2} \in \mathrm{GL}_2(\mathbf{K})$ such that

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

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

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

is a solution of (15). It is easily seen that we get in this way infinitely many solutions of the Riccati equation. This is a contradiction.

(3) Assume that (15) has at least three solutions: $u_1, u_2, u_3 \in \mathbf{K}$. The proof of assertion (2) of the present lemma shows that $\phi_p Y = AY$ is isomorphic over $\mathbf{K}$ to $\phi_p Y = \begin{pmatrix} u_i & 0 \\ 0 & u_j \end{pmatrix} Y$ for all $1 \leq i < j \leq 3$. Therefore, there exists $T \in \mathrm{GL}_2(\mathbf{K})$ such that

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

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

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

and, according to Proposition 15, G is an algebraic subgroup of $\overline{\mathbb{Q}}^\times I_2$. We have shown during the proof of statement (2) that this implies that the Riccati equation (15) has infinitely many solutions in $\mathbf{K}$.

(4) Assume that G is reducible. According to Proposition 15, there exists $T = (t_{i,j})_{1\leq i,j\leq 2} \in \mathrm{GL}_2(\mathbf{K})$ such that $\phi_p(T)AT^{-1}$ is upper triangular. Then $t_{22} \neq 0$ and $-\frac{t_{21}}{t_{22}} \in \mathbf{K}$ is a solution of Riccati equation (15). This proves claim (4). □

6.2. **Irreducibility over K: An algorithm.** We know that G is reducible if and only if the Riccati equation

$$u(\phi_p(u)+a)=-b \tag{16}$$

has a solution in $\mathbf{K}$. We shall now describe an algorithm that decides whether or not equation (16) has a solution in $\mathbf{K}$.

Let $u\in\mathbf{K}$ be a hypothetic solution of equation (16).

Thanks to Corollary 31, we can find an explicit $N\in\mathbb{Z}_{\geq 1}$ such that $u\in\mathbf{K}\cap\overline{\mathbb{Q}}((z_N))=\overline{\mathbb{Q}}(z_N)$.

Let $c\in\overline{\mathbb{Q}}^{\times}$ and let n,d be coprime non-zero monic elements of $\overline{\mathbb{Q}}[z_N]$ such that $u=cn/d$. Let r be the greatest common divisor[4] of $\phi_p^{-1}(n)$ and d in $\overline{\mathbb{Q}}[z_{Np}]$ and consider the coprime monic elements of $\overline{\mathbb{Q}}[z_{Np}]$ given by $s=n/\phi_p(r)$ and $t=d/r$. Then, we have

$$u=c\frac{\phi_p(r)}{r}\frac{s}{t}$$

with $\gcd(s,\phi_p(t))=\gcd(\phi_p(r)s,rt)=1$.

According to Proposition 32, we have $c=\mathrm{cld}(u)\in\{c_1,\mathrm{cld}(b)/c_1\}$ where c_1 is a root of the characteristic polynomial associated to the first theta-slope of L.

Let k be a number field such that $a,b\in k(z)$. Let $p_1,p_2,p_3\in k[z]$ be such that

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

Then, the Riccati equation (15) becomes

$$p_3c\frac{\phi_p r}{r}\frac{s}{t}\phi_p\left(c\frac{\phi_p r}{r}\frac{s}{t}\right)+p_1c\frac{\phi_p r}{r}\frac{s}{t}=-p_2,$$

i.e.

$$c^2p_3\phi_p^2(r)s\phi_p(s)+cp_1\phi_p(r)s\phi_p(t)=-p_2rt\phi_p(t). \tag{17}$$

Let l_1 be the field obtained from k by adjoining the splitting fields of p_2 and $\phi_p^{-1}(p_3)$ seen as elements of $k[z_{Np}]$. Equation (17) shows that s and t are divisors in $l_1[z_{Np}]$ of p_2 and $\phi_p^{-1}(p_3)$ respectively.

So far, c, s and t are fixed (among finitely many possible cases), and it remains to decide whether or not equation (17) has a solution $r\in\overline{\mathbb{Q}}[z_{Np}]$. But, this is a linear Mahler equation in r, which can be interpreted as a system of linear equations with coefficients in $l=l_1(c)$, whose unknowns are the coefficients of r. Note that this implies that if there is a solution r in $\overline{\mathbb{Q}}[z_{Np}]$, then there is also a solution in $l[z_{Np}]$ and hence the Riccati equation has a solution in $l(z_N)$. In order to determine whether or not such an r exists, it remains to have a bound on the degree of the potential solutions r of (17) (i.e. a bound on the number of unknowns of the system of linear equations we are interested in). Rewriting equation (17) as

$$c^2=-\frac{cp_1\phi_p(r)s\phi_p(t)+p_2rt\phi_p(t)}{p_3\phi_p^2(r)s\phi_p(s)}$$

and taking degrees, we get

$$0\leq\max\{d_1+p\deg r,d_2+\deg r\}-(d_3+p^2\deg r)$$

where $d_1=\deg p_1+\deg s+p\deg t$, $d_2=\deg p_2+(p+1)\deg t$ and $d_3=\deg p_3+(p+1)\deg s$. We deduce from this an explicit constant C such that $\deg r\leq C$.

[4]By "greatest common divisor" we mean the "monic greatest common divisor".

If we are able to compute l, then what precedes gives an algorithm to decide whether or not the Riccati equation has a solution in $\mathbf{K}$ and to compute such a solution if there is one.

We shall now prove that it is actually sufficient to work (at worst) in the quadratic extensions of k contained in l.

Lemma 41. *If the Riccati equation* (16) *has a solution in* $\mathbf{K}$*, then it has a solution in* $l'(z_N)$ *for some extension* l' *of* k *of degree at most* 2 *contained in* l*.*

Proof. This proof is a straightforward modification of the proof of [Hen98, Theorem 4.2]. We have seen above that if the Riccati equation (16) has a solution in $\mathbf{K}$, then it has a solution in $l(z_N)$. We distinguish three cases.

(a) Assume that the Riccati equation (15) has a unique solution u in $l(z_N)$. For any $\sigma \in \mathrm{Gal}(l(z_N)/k(z_N))$, $\sigma(u) \in l(z_N)$ is a solution of (15), so $\sigma(u) = u$. Since $l(z_N)$ is a Galois extension of $k(z_N)$, we get $u \in k(z_N)$.

(b) Assume that the Riccati equation (15) has exactly two solutions u, v in $l(z_N)$. The kernel H of the natural group morphism $\mathrm{Gal}(l(z_N)/k(z_N)) \to \mathfrak{S}(\{u,v\})$, with values in the group of permutations $\mathfrak{S}(\{u,v\})$ of $\{u,v\}$, has index ≤ 2 in $\mathrm{Gal}(l(z_N)/k(z_N))$. Since u and v are fixed by H, they belong to $l'(z_N)$ for some extension l' of k of degree 2 contained in l.

(c) Assume that the Riccati equation (15) has at least three solutions in $l(z_N)$. The proof of assertion (3) of Lemma 40 shows that there exist $T = (t_{i,j})_{1\leq i,j\leq 2} \in \mathrm{GL}_2(l(z_N))$ and some solution $u \in l(z_N)$ of the Riccati equation (15) such that

$$\phi_p(T) A T^{-1} = u I_2. \tag{18}$$

For any $\sigma \in \mathrm{Gal}(l(z_N)/k(z_N))$, we have

$$\phi_p(\sigma(T)) A \sigma(T)^{-1} = \sigma(u) I_2.$$

Therefore, we have

$$\phi_p(S) u = \sigma(u) S, \text{ with } S := \sigma(T) T^{-1} \in \mathrm{GL}_2(l(z_N)).$$

It follows that there exists $g_\sigma \in l(z_N)^\times$ (namely, one of the non-zero entries of S) such that

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

Note that g_σ is uniquely determined by this equation if we require that it is monic, as we shall now assume. Then, the map $\sigma \mapsto g_\sigma$ is a 1 cocycle for the action of $\mathrm{Gal}(l(z_N)/k(z_N))$ over $l(z_N)$. Hilbert's 90 Theorem [Ser68, §10.1] ensures that there exists $m \in l(z_N)^\times$ such that, for all $\sigma \in \mathrm{Gal}(l(z_N)/k(z_N))$,

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

A straightforward calculation shows that

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

is invariant under the action of $\mathrm{Gal}(l(z_N)/k(z_N))$ and hence belongs to $k(z_N)^\times$. Moreover, we have

$$\phi_p\left(T'\right) A \left(T'\right)^{-1} = \widetilde{u} I_2, \text{ with } T' := mT.$$

Applying $\sigma \in \mathrm{Gal}(l(z_N)/k(z_N))$ to this equality, we get

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

It follows that

$$C_\sigma := T'\sigma\left(T'^{-1}\right) \in \mathrm{GL}_2(l(z_N))$$

satisfies $\phi_p(C_\sigma) = C_\sigma$ and hence that its entries belong to l. Identifying $\mathrm{Gal}(l(z_N)/k(z_N))$ with $\mathrm{Gal}(l/k)$, we can see that $\sigma \mapsto C_\sigma$ has a 1-cocyle for the natural action of $\mathrm{Gal}(l/k)$ on $\mathrm{GL}_2(l)$. Since l is a Galois extension of k, Hilbert's 90 Theorem [Ser68, §10.1] ensures that this cocycle is trivial, i.e. that there exists $C \in \mathrm{GL}_2(l)$ such that, for all $\sigma \in \mathrm{Gal}(l(z_N)/k(z_N))$, $C_\sigma = C\sigma(C^{-1})$. Then, $T'' = C^{-1}T'$, which is a priori an element of $\mathrm{GL}_2(l(z_N))$, is invariant by the action of $\mathrm{Gal}(l(z_N)/k(z_N))$ and hence has entries in $k(z_N)$. Note that

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

It follows that $u_1 := \frac{-t''_{11}}{t''_{12}}$ and $v_1 := \frac{-t''_{21}}{t''_{22}}$ are solutions in $k(z_N)$ of the Riccati equation (15) (this was already used in the proof of assertion (2) of Lemma 40). Since $\det T'' \neq 0$, we get that u_1 and v_1 are distinct solutions in $k(z_N)$ of the Riccati equation (15). □

It is explained in [Hen97, after Theorem 14] how to find the (finitely many) extensions of k of degree at most 2 and contained in l. Now, for any such extension l', a straightforward modification of the foregoing discussion gives an algorithm to determine whether or not the Riccati equation (16) has a solution in $l'(z_N)$, whence an algorithm to determine whether or not the Riccati equation (16) has a solution in $\mathbf{K}$.

7. Imprimitivity of the difference Galois group

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

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

Theorem 42. *Assume that G is irreducible and that $a \neq 0$. Then, G is imprimitive if and only if there exists $u \in \mathbf{K}$ such that*

$$\left(\phi_p^2(u) + \left(\phi_p^2\left(\frac{b}{a}\right) - \phi_p(a) + \frac{\phi_p(b)}{a}\right)\right) u = -\frac{\phi_p(b)b}{a^2}. \tag{19}$$

Proof. Same proof as [Hen98, Theorem 4.6]. □

Remark 43. If $a = 0$, then G is imprimitive by virtue of Proposition 15.

Note that the equation (19) is a Riccati type equation, with respect to $\phi_p^2 = \phi_{p^2}$ instead of ϕ_p. Therefore, using section 6.2, one can determine algorithmically whether or not the equation (19) has a solution in $\mathbf{K}$.

8. A connectedness criterion

Consider a Mahler equation

$$a_n\phi_p^n(y) + \cdots + a_1\phi_p(y) + a_0 y = 0, \tag{20}$$

with $a_0, \ldots, a_n \in \overline{\mathbb{Q}}(z)$. We denote by

$$L = a_n\phi_p^n + \cdots + a_1\phi_p + a_0$$

the corresponding Mahler operator.

8.1. **Over $\widehat{\mathbf{K}}$ and $\mathbf{K}$.** We let $\widehat{R}$ be a Picard-Vessiot ring for L over $\widehat{\mathbf{K}}$ and $R \subset \widehat{R}$ be a Picard-Vessiot ring for L over $\mathbf{K}$ (see section 2.2). We denote by $\widehat{G}$ and G the corresponding difference Galois groups, and we see $\widehat{G}$ as a subgroup of G (see section 2.2). The following result is inspired by Gabber and Katz's [Kat87, Proposition 1.2.5] and van der Put and Singer's [vdPS97, Proposition 12.1].

Proposition 44. *The morphism $\widehat{G}/(\widehat{G})^\circ \to G/G^\circ$ induced by the natural inclusion $\widehat{G} \subset G$ is surjective.*

Proof. Let H be the subgroup of G generated, as an abstract group, by G° and $\widehat{G}$. Note that H has finite index in G (because $G^\circ \subset H \subset G$) and hence is an algebraic subgroup of G. We have to prove that $H = G$. By Galois correspondence, it is equivalent to prove that $R^H = \mathbf{K}$. We have $R^H \subset \widehat{R}^H \subset \widehat{R}^{\widehat{G}} = \widehat{\mathbf{K}}$. Moreover $R^H \subset R^{G^\circ}$ and, according to [vdPS97, Corollary 1.31], R^{G° is a finite dimension vector space over $\mathbf{K}$. So $R^H \subset \widehat{\mathbf{K}}$ is a finite field extension of $\mathbf{K}$, endowed with an endomorphism φ such that $\varphi_{|\mathbf{K}} = \phi_p$. Proposition 15 ensures that $R^H = \mathbf{K}$. □

Corollary 45. *If $\widehat{G}$ is connected, then G is connected.*

Corollary 46. *Let $c_1, \dots, c_n$ be the exponents of L at 0. If the algebraic group generated by* $\mathrm{diag}(c_1, \dots, c_n)$ *in* $\mathrm{GL}_n(\overline{\mathbb{Q}})$ *is connected, then G is connected.*

Proof. Up to renumbering the c_i, there exist $g_1, \dots, g_n \in \widehat{\mathbf{K}}$ such that, for all $i \in \{1, \dots, n\}$, $\mathrm{cld}(g_i) = c_i$ and

$$L = (\phi_p - g_n) \cdots (\phi_p - g_1).$$

Let T_n (resp. D_n) be the group of upper-triangular (resp. diagonal) matrices in $\mathrm{GL}_n(\overline{\mathbb{Q}})$. The above factorization of L allows us to see $\widehat{G}$ as a subgroup of T_n such that the image $\widehat{G}'$ of the morphism

$$\begin{array}{ccc} \widehat{G} & \to & D_n \\ (a_{i,j})_{1 \leq i,j \leq n} & \mapsto & \mathrm{diag}(a_{1,1}, \dots, a_{n,n}) \end{array}$$

is the Galois group over $\widehat{\mathbf{K}}$ of $\phi_p Y = \mathrm{diag}(g_1, \dots, g_n) Y$ (follows from tannakian duality for instance). The connectedness of $\widehat{G}$ is equivalent to that of $\widehat{G}'$. But $\widehat{G}'$ is the intersection of the kernels of the characters $\chi : D_n \to \overline{\mathbb{Q}}^\times$ which are trivial on $\widehat{G}'$. By tannakian duality, a character $\chi : D_n \to \overline{\mathbb{Q}}^\times$, given by $\chi(\mathrm{diag}(x_1, \dots, x_n)) = x_1^{m_1} \cdots x_n^{m_n}$ for some $m_1, \dots, m_n \in \mathbb{Z}$, is trivial on $\widehat{G}'$ if and only if $g_1^{m_1} \cdots g_n^{m_n} = u/\phi_p(u)$ for some $u \in \widehat{\mathbf{K}}$. This is equivalent to $c_1^{m_1} \cdots c_2^{m_n} = 1$. So, $\widehat{G}'$ is the algebraic subgroup of D_n generated by $\mathrm{diag}(c_1, \dots, c_n)$ which is connected. Therefore $\widehat{G}$ is connected, and the result follows from Corollary 45. □

8.2. **Over $\widehat{\mathbf{K}}_{p^\infty}$ and $\mathbf{K}_{p^\infty}$.** We shall now give results analogous to those stated in section 8.1 but with $\widehat{\mathbf{K}}$ replaced by $\widehat{\mathbf{K}}_{p^\infty}$ and $\mathbf{K}$ replaced by $\mathbf{K}_{p^\infty}$ (these difference fields are defined at the end of section 3).

We let $\widehat{R}$ be a Picard-Vessiot ring for L over $\widehat{\mathbf{K}}_{p^\infty}$ and $R \subset \widehat{R}$ be a Picard-Vessiot ring for L over $\mathbf{K}_{p^\infty}$ (see section 2.2). We denote by $\widehat{G}$ and G the corresponding difference Galois groups, and we see $\widehat{G}$ as a subgroup of G (see section 2.2).

Proposition 47. *The morphism $\widehat{G}/(\widehat{G})^\circ \to G/G^\circ$ induced by the natural inclusion $\widehat{G} \subset G$ is surjective.*

Proof. Same proof as Proposition 44, using Proposition 17 instead of Proposition 15 at the end of the proof. □

Corollary 48. *If $\widehat{G}$ is connected, then G is connected.*

Corollary 49. *Assume that there exist $g_1, \dots, g_n \in \widehat{\mathbf{K}}_{p^\infty}$ such that*

$$L = (\phi_p - g_n) \cdots (\phi_p - g_1).$$

Let $I = \{(m_1, \dots, m_n) \in \mathbb{Z}^n \mid g_1^{m_1} \cdots g_n^{m_n} = u/\phi_p(u)$ for some $u \in \widehat{\mathbf{K}}_{p^\infty}\}$. Assume that $\{(x_1, \dots, x_n) \in (\overline{\mathbb{Q}}^\times)^n \mid x_1^{m_1} \cdots x_n^{m_n} = 1\}$ is connected. Then, G is connected.

Proof. Similar to the proof of Proposition 46. □

9. Examples: The Baum-Sweet and the Rudin-Shapiro sequences

9.1. **The Baum-Sweet sequence.** The Baum-Sweet sequence $(a_n)_{n\geq 0}$ is the automatic sequence defined by $a_n = 1$ if the binary representation of n contains no block of consecutive 0 of odd length, and $a_n = 0$ otherwise. It is characterized by the following recursive equations:

$$a_0 = 1, \quad a_{2n+1} = a_n, \quad a_{4n} = a_n, \quad a_{4n+2} = 0.$$

Let $g(z) = \sum_{n\geq 0} a_n z^n$ be the corresponding generating series. The above recursive equations show that $Y(z) = \begin{pmatrix} g(z) \\ g(z^2) \end{pmatrix}$ satisfies

$$\phi_2 Y = AY \text{ where } A = \begin{pmatrix} 0 & 1 \\ 1 & -z \end{pmatrix} \tag{21}$$

and, hence,

$$\phi_4 Y = BY \text{ where } B = \phi_2(A)\, A = \begin{pmatrix} 1 & -z^2 \\ -z & 1+z^3 \end{pmatrix}. \tag{22}$$

We let G be the Galois group of (21) over $\mathbf{K}$. We let G' (resp. H) be the Galois group of (21) (resp. (22)) over $\mathbf{K}_{2^\infty}$ (resp. $\mathbf{K}_{4^\infty}$).

Theorem 50. *We have $H = \mathrm{SL}_2(\overline{\mathbb{Q}})$ and $G = G' = \mu_4 \mathrm{SL}_2(\overline{\mathbb{Q}})$, where $\mu_4 \subset \mathbb{Q}^\times$ is the group of 4th roots of the unity.*

This theorem will follow from a series of simple lemmas.

Lemma 51. *The Galois group H is connected.*

Proof. We have $B(0) = I_2$. So, the system (22) is equivalent to $\phi_4 Y = Y$ over $\widehat{\mathbf{K}}_{4^\infty}$, and, hence, its Galois group over $\widehat{\mathbf{K}}_{4^\infty}$ is trivial. Corollary 48 yields the desired result. □

Lemma 52. *The system* (22) *is equivalent to the following equation:*

$$\phi_4^2 - (z^9 + z^6 + 1)\phi_4 + z^6. \tag{23}$$

Proof. We have

$$B^{-1} = \begin{pmatrix} 1+z^3 & z^2 \\ z & 1 \end{pmatrix}.$$

The vectors

$$e := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ and } \Phi_B(e) = B^{-1}\phi_4(e) = \begin{pmatrix} z^2 \\ 1 \end{pmatrix}$$

form a $\mathbf{K}_{4\infty}$-basis of $(\mathbf{K}_{4\infty})^2$ so that e is a cyclic vector for the system (22). Moreover, we have

$$\Phi_B^2(e) = B^{-1}\phi_4\begin{pmatrix} z^2 \\ 1\end{pmatrix} = \begin{pmatrix} z^{11}+z^8+z^2 \\ z^9+1\end{pmatrix} = (z^9+z^6+1)\Phi_B(e) - z^6 e.$$

□

Lemma 53. *The Galois group H is irreducible.*

Proof. This amounts to showing that the operator (23) is irreducible over $\mathbf{K}_{4\infty}$, that is, that the Riccati equation

$$u(\phi_4(u) - (z^9+z^6+1)) = -z^6 \tag{24}$$

does not have any solution $u \in \mathbf{K}_{4\infty}$. Assume to the contrary that it has a solution $u \in \mathbf{K}_{4\infty}$. We have $u \in \overline{\mathbb{Q}}(z)$, because $u = \frac{-z^6}{\phi_4(u)-(z^9+z^6+1)} \in \overline{\mathbb{Q}}(z, \phi_4(u))$. Let s, t be coprime elements of $\overline{\mathbb{Q}}[z]$ such that $u = s/t$. We have

$$\frac{s(z)}{t(z)}\left(\frac{s(z^4) - (z^9+z^6+1)t(z^4)}{t(z^4)}\right) = -z^6.$$

Using the fact that s is coprime to t, we see that

$$\frac{s(z)}{t(z^4)} \in \overline{\mathbb{Q}}[z] \text{ and } \frac{s(z^4) - (z^9+z^6+1)t(z^4)}{t(z)} \in \overline{\mathbb{Q}}[z].$$

Since their product is a monomial, these polynomials are monomials. Moreover, it is easily seen that they cannot both vanish at 0, so one of the following properties holds:

(i) either $\frac{s(z)}{t(z^4)} = cz^6$ and $\frac{s(z^4)-(z^9+z^6+1)t(z^4)}{t(z)} = c'$
(ii) or $\frac{s(z)}{t(z^4)} = c$ and $\frac{s(z^4)-(z^9+z^6+1)t(z^4)}{t(z)} = c'z^6$

for some constants $c, c' \in \overline{\mathbb{Q}}^\times$.

If (i) holds, then

$$s(z) = cz^6 t(z^4) \text{ and } s(z^4) = (z^9+z^6+1)t(z^4) + c't(z).$$

So

$$1 = \frac{(z^9+z^6+1)t(z^4)+c't(z)}{s(z^4)} = \frac{(z^9+z^6+1)t(z^4)+c't(z)}{cz^{24}t(z^{16})}.$$

Letting $z \to \infty$, we get $1 = 0$.

If (ii) holds, then

$$s(z) = ct(z^4) \text{ and } s(z^4) = (z^9+z^6+1)t(z^4) + c'z^6 t(z).$$

So,

$$ct(z^{16}) = (z^9+z^6+1)t(z^4) + c'z^6 t(z). \tag{25}$$

But $\deg\big((z^9+z^6+1)t(z^4)\big) = 9 + 4\deg t(z)$ and $\deg(z^6 t(z)) = 6 + \deg t(z)$, so the degree of the right hand side of (25) is equal to $9 + 4\deg t(z)$. Moreover, the degree of the left hand side of (25) is equal to $16\deg t(z)$. So, we obtain the equality $9 + 4\deg t(z) = 16\deg t(z)$, which is impossible.

In any case we get a contradiction. □

Proof of Theorem 50. The fact that H is connected and irreducible implies that H contains $\mathrm{SL}_2(\overline{\mathbb{Q}})$. Moreover, we have $H \subset \mathrm{SL}_2(\overline{\mathbb{Q}})$ because $\det B = 1$. So $H = \mathrm{SL}_2(\overline{\mathbb{Q}})$. Theorem 12 ensures that the Galois group over $\mathbf{K}_{4^\infty}$ of equation (21) contains $\mathrm{SL}_2(\overline{\mathbb{Q}})$. Theorem 7 implies that G' contains $\mathrm{SL}_2(\overline{\mathbb{Q}})$. But $\det A = -1$, so $G' = \{M \in \mathrm{GL}_2(\overline{\mathbb{Q}}) \mid \det M = \pm 1\} = \mu_4 \mathrm{SL}_2(\overline{\mathbb{Q}})$. Using Theorem 7, we see that $G = \mu_4 \mathrm{SL}_2(\overline{\mathbb{Q}})$. □

For instance, we have the following consequence.

Corollary 54. *The series $g(z)$ and $g(z^2)$ are algebraically independent over $\mathbf{K}$.*

Proof. Let R be a Picard-Vessiot ring for the system (21) over $\overline{\mathbf{K}}$ containing $g(z)$ and $g(z^2)$. Let $U = (u_{i,j})_{1\le i,j\le 2} \in \mathrm{GL}_2(R)$ be a corresponding fundamental matrix of solutions whose first column is $(g(z), g(z^2))^t$. Let $G'' \subset \mathrm{GL}_2(\overline{\mathbb{Q}})$ be the corresponding difference Galois group over $\overline{\mathbf{K}}$. Theorem 50 and Theorem 7 ensure that $G'' = \mathrm{SL}_2(\overline{\mathbb{Q}})$. Let $X = (X_{i,j})_{1\le i,j\le 2}$ be a matrix of indeterminates over $\overline{\mathbf{K}}$. Let I be the ideal of relations in $\overline{\mathbf{K}}[X, \det(X)^{-1}]$ between the entries of U. According to the results recalled in section 2.1, $\mathrm{Spec}(R)$ is a trivial G''-torsor over $\overline{\mathbf{K}}$. Therefore, there exists $d \in \overline{\mathbf{K}}^\times$ such that I is the ideal generated by $\det((X_{i,j})_{1\le i,j\le 2}) - d$. In particular, we get $I \cap \overline{\mathbf{K}}[X_{1,1}, X_{2,1}] = \{0\}$, whence the result. □

9.2. **The Rudin-Shapiro sequence.** The Rudin-Shapiro sequence $(a_n)_{n\ge 0}$ is the automatic sequence defined by $a_n = (-1)^{b_n}$ where b_n is the number of pairs of consecutive 1 in the binary representation of n. It is characterized by the following recurrence relations:

$$a_0 = 1, \quad a_{2n} = a_n, \quad a_{2n+1} = (-1)^n a_n.$$

We let $f(z) = \sum_{n\ge 0} a_n z^n$ be the corresponding generating function. We set $f_1(z) = f(z)$ and $f_2(z) = f(-z)$. The recursive equations above show that the vector

$$Y(z) = \begin{pmatrix} f_1(z) \\ f_2(z) \end{pmatrix}$$

satisfies the following Mahler system:

$$\phi_2 Y = AY \text{ where } A = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ \frac{1}{z} & -\frac{1}{z} \end{pmatrix}. \tag{26}$$

We let G (resp. H) be the Galois group of (26) over $\mathbf{K}$ (resp. over $\mathbf{K}_{2^\infty}$).

Theorem 55. *We have $G = H = \mathrm{GL}_2(\overline{\mathbb{Q}})$.*

This theorem will follow from a series of simple lemmas.

Lemma 56. *The system* (26) *is equivalent to the equation*

$$\phi_2^2 - (1-z)\phi_2 - 2z. \tag{27}$$

Proof. We have

$$A^{-1} = \begin{pmatrix} 1 & z \\ 1 & -z \end{pmatrix}.$$

The vectors

$$e := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } \Phi_A(e) = A^{-1}\phi_2(e) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

form a $\mathbf{K}_{2^\infty}$-basis of $(\mathbf{K}_{2^\infty})^2$ so that e is a cyclic vector for (26). Moreover, we have

$$\Phi_A^2(e) = A^{-1}\phi_2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1+z \\ 1-z \end{pmatrix} = (1-z)\Phi_A(e) + 2ze.$$

□

Lemma 57. *The Galois group H is irreducible.*

Proof. This amounts to showing that the operator (27) is irreducible over $\mathbf{K}_{2^\infty}$, that is, that the Riccati equation

$$u(\phi_2(u) - (1-z)) = -2z \tag{28}$$

does not have any solution $u \in \mathbf{K}_{2^\infty}$. Assume to the contrary that it has a solution $u \in \mathbf{K}_{2^\infty}$. We have $u \in \overline{\mathbb{Q}}(z)$, because $u = \frac{-2z}{\phi_2(u)-(1-z)} \in \overline{\mathbb{Q}}(z, \phi_2(u))$. Let s, t be coprime elements of $\overline{\mathbb{Q}}[z]$ such that $u = s/t$. We have

$$\frac{s(z)}{t(z)} \left(\frac{s(z^2) - (1-z)t(z^2)}{t(z^2)} \right) = -2z.$$

Using the fact that s is coprime to t, we see that

$$\frac{s(z)}{t(z^2)} \in \overline{\mathbb{Q}}[z] \text{ and } \frac{s(z^2) - (1-z)t(z^2)}{t(z)} \in \overline{\mathbb{Q}}[z].$$

Since their product is a monomial, these polynomials are monomials. So, one of the following properties holds:

(i) either $\frac{s(z)}{t(z^2)} = cz$ and $\frac{s(z^2)-(1-z)t(z^2)}{t(z)} = c'$
(ii) or $\frac{s(z)}{t(z^2)} = c$ and $\frac{s(z^2)-(1-z)t(z^2)}{t(z)} = c'z$

for some constants $c, c' \in \overline{\mathbb{Q}}^\times$.

If (i) holds, then

$$s(z) = czt(z^2) \text{ and } s(z^2) = (1-z)t(z^2) + c't(z).$$

So

$$1 = \frac{(1-z)t(z^2) + c't(z)}{s(z^2)} = \frac{(1-z)t(z^2) + c't(z)}{cz^2t(z^4)}.$$

Letting $z \to \infty$, we get $1 = 0$.

If (ii) holds, then

$$s(z) = ct(z^2) \text{ and } s(z^2) = (1-z)t(z^2) + c'zt(z).$$

So

$$ct(z^4) = (1-z)t(z^2) + c'zt(z). \tag{29}$$

Let us first assume that $\deg t(z) > 0$. We have $\deg\big((1-z)t(z^2)\big) = 1 + 2\deg t(z)$ and $\deg(zt(z)) = 1+\deg t(z)$, so the degree of the right-hand side of (25) is equal to $1+2\deg t(z)$. Moreover, the degree of the left-hand side of (25) is equal to $4\deg t(z)$. So we obtain the equality $1+2\deg t(z) = 4\deg t(z)$, which is impossible. It remains to consider the case that $t(z) = t \in \overline{\mathbb{Q}}^\times$ and hence $s(z) = s \in \overline{\mathbb{Q}}^\times$. The second equation in (ii) above entails that $s = t$. So $\frac{s(z)}{t(z^2)} = 1$ and $\frac{s(z^2)-(1-z)t(z^2)}{t(z)} = z$, so

$$\frac{s(z)}{t(z^2)}\left(\frac{s(z^2)-(1-z)t(z^2)}{t(z)}\right) = z,$$

which is a contradiction.

In any case, we get a contradiction. □

Lemma 58. *The Galois group G is connected.*

Proof. The first theta-slope is 1 and we have

$$L^{[\theta_1]} = z^3\phi_2^2 - (1-z)z\phi_2 - 2z.$$

So

$$L = (\phi_2 - a)(\phi_2 - b) = \phi_2^2 - (a + \phi_2(b))\phi_2 + ab$$

with $b \in -2z(1 + z\overline{\mathbb{Q}}[[z]])$. Since $ab = -2z$, we get $a \in 1 + z\overline{\mathbb{Q}}[[z]]$.

Using Corollary 49, we get that G is connected. □

Proof of Theorem 55. The fact that H is connected and irreducible implies that H contains $\mathrm{SL}_2(\overline{\mathbb{Q}})$. Moreover, $\det A = -2z$, so the Galois group of $\phi_2 y = (\det A)y$ is $\overline{\mathbb{Q}}^\times$. It follows that $H = \mathrm{GL}_2(\overline{\mathbb{Q}})$. Using Theorem 7, we get $G = \mathrm{GL}_2(\overline{\mathbb{Q}})$. □

For instance, we have the following consequence, whose proof is similar to the proof of Corollary 54.

Corollary 59. *The series $f_1(z)$ and $f_2(z)$ are algebraically independent over $\mathbf{K}$.*

9.3. **Galois group of Baum-Sweet $\oplus$ Rudin-Shapiro.** Let N_1 (resp. N_2) be the difference module over $\mathbf{K}$ corresponding to the Baum-Sweet equation (21) (resp. to the Rudin-Shapiro equation (26)). We use the notation of section 2.5 for these specific N_1 and N_2. We have seen that the difference Galois group G_1 (resp. G_2) of N_1 (resp. N_2) over $\mathbf{K}$ is $\mu_4\,\mathrm{SL}(\omega(N_1))$ (resp. $\mathrm{GL}(\omega(N_2))$). Let $G \subset G_1 \times G_2$ be the difference Galois group of $N_1 \oplus N_2$ over $\mathbf{K}$. The Baum-Sweet equation (21) is regular singular at 0, and its exponents at 0 are the eigenvalues of

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

i.e. ± 1. On the other hand, we have seen during the proof of Lemma 58 that the exponents at 0 of the Rudin-Shapiro equation (26) are 1 and -2. Let N be a difference module of rank one over $\mathbf{K}$, and denote by c its exponent at 0. Then, the exponents of $N \otimes N_2$ are $c, -2c$, and the exponents of $N \otimes N_2^\vee$ are $c, -c/2$. So neither $N \otimes N_2$ nor $N \otimes N_2^\vee$ has the same exponents at 0 as N_1. Therefore, N_1 is isomorphic to neither $N \otimes N_2$ nor $N \otimes N_2^\vee$. Proposition 14 ensures that

$$G = \{(\sigma_1, \sigma_2) \in \mathrm{GL}(\omega(N_1)) \times \mathrm{GL}(\omega(N_2)) \mid (\det\sigma_1, \det\sigma_2) \in H\},$$

where H is the Galois group of $\det M_1 \oplus \det M_2$. But $\det M_1$ corresponds to the equation $\phi_2 y = -1$ and $\det M_2$ to $\phi_2 y = -2z$. Therefore, the Galois group of $\det M_1 \oplus \det M_2$ is $\mu_2 \times \overline{\mathbb{Q}}^{\times}$. So,

$$G = \mu_4 \,\mathrm{SL}(\omega(N_1)) \times \mathrm{GL}(\omega(N_2)).$$

In particular, arguing as in the proof of Corollary 54, we see that the series $f_1(z) = f(z)$, $f_2(z) = f(-z)$, $g(z)$ and $g(z^2)$ are algebraically independent over $\overline{\mathbb{Q}}(z)$.

Acknowledgement

The author thanks the anonymous referee for a careful reading and helpful suggestions.

References

[Bec94] Paul-Georg Becker, *k-regular power series and Mahler-type functional equations*, J. Number Theory **49** (1994), no. 3, 269–286, DOI 10.1006/jnth.1994.1093. MR1307967

[BM06] Mireille Bousquet-Mélou, *Rational and algebraic series in combinatorial enumeration*, International Congress of Mathematicians. Vol. III, Eur. Math. Soc., Zürich, 2006, pp. 789–826. MR2275707

[DM82] Pierre Deligne and James S. Milne, *Tannakian categories*, in Hodge Cycles, Motives, and Shimura Varieties, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin-New York, 1982. MR654325

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977. MR0463157

[Hen97] Peter A. Hendriks, *An algorithm for computing a standard form for second-order linear q-difference equations*, J. Pure Appl. Algebra **117/118** (1997), 331–352, DOI 10.1016/S0022-4049(97)00017-0. MR1457845

[Hen98] Peter A. Hendriks, *An algorithm determining the difference Galois group of second order linear difference equations*, J. Symbolic Comput. **26** (1998), no. 4, 445–461, DOI 10.1006/jsco.1998.0223. MR1646675

[Hur92] A. Hurwitz, *Ueber algebraische Gebilde mit eindeutigen Transformationen in sich* (German), Math. Ann. **41** (1892), no. 3, 403–442, DOI 10.1007/BF01443420. MR1510753

[Kat87] Nicholas M. Katz, *On the calculation of some differential Galois groups*, Invent. Math. **87** (1987), no. 1, 13–61, DOI 10.1007/BF01389152. MR862711

[Kat90] Nicholas M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies, vol. 124, Princeton University Press, Princeton, NJ, 1990. MR1081536

[Lan52] Serge Lang, *On quasi algebraic closure*, Ann. of Math. (2) **55** (1952), 373–390. MR0046388

[Mah30a] Kurt Mahler, *Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen* (German), Math. Ann. **103** (1930), no. 1, 532, DOI 10.1007/BF01455708. MR1512635

[Mah30b] Kurt Mahler, *Arithmetische Eigenschaften einer Klasse transzendental-transzendenter Funktionen* (German), Math. Z. **32** (1930), no. 1, 545–585, DOI 10.1007/BF01194652. MR1545184

[Mah30c] Kurt Mahler, *Uber das Verschwinden von Potenzreihen mehrerer Veränderlichen in speziellen Punktfolgen* (German), Math. Ann. **103** (1930), no. 1, 573–587, DOI 10.1007/BF01455711. MR1512638

[Nis96] Kumiko Nishioka, *Mahler functions and transcendence*, Lecture Notes in Mathematics, vol. 1631, Springer-Verlag, Berlin, 1996. MR1439966

[NN12] Kumiko Nishioka and Seiji Nishioka, *Algebraic theory of difference equations and Mahler functions*, Aequationes Math. **84** (2012), no. 3, 245–259, DOI 10.1007/s00010-012-0132-3. MR2996417

[NvdPT08] K. A. Nguyen, M. van der Put, and J. Top, *Algebraic subgroups of* $\mathrm{GL}_2(\mathbb{C})$, Indag. Math. (N.S.) **19** (2008), no. 2, 287–297, DOI 10.1016/S0019-3577(08)80004-3. MR2489331

[Pel09] F. Pellarin, *An introduction to Mahler's method for transcendence and algebraic independence*, in the EMS proceedings of the conference "Hodge structures, transcendence and other motivic aspects", G. Boeckle, D. Goss, U. Hartl, and M. Papanikolas, eds., 2009.

[Ph15] Patrice Philippon, *Groupes de Galois et nombres automatiques*, J. Lond. Math. Soc. (2) **92** (2015), no. 3, 596–614, DOI 10.1112/jlms/jdv056. MR3431652

[Ser68] Jean-Pierre Serre, *Corps locaux*, Deuxième édition; Publications de l'Université de Nancago, No. VIII, Hermann, Paris, 1968. MR0354618

[vdPS97] Marius van der Put and Michael F. Singer, *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666, Springer-Verlag, Berlin, 1997. MR1480919

Institut Fourier, Université Grenoble 1, CNRS UMR 5582, 100 rue des Maths, BP 74, 38402 St. Martin d'Hères, France

Current address: Université Grenoble Alpes, Institut Fourier, CNRS UMR 5582, CS 40700, 38058 Grenoble Cedex 09, France

E-mail address: Julien.Roques@univ-grenoble-alpes.fr