Values of E-functions are not Liouville numbers

Stéphane Fischler, Tanguy Rivoal

Values of E-functions are not Liouville numbers

S. Fischler and T. Rivoal

January 3, 2023

Abstract

Shidlovskii has given a linear independence measure of values of E-functions with rational Taylor coefficients at a rational point not a singularity of the underlying differential system satisfied by these E-functions. His measure holds as well for E-functions with coefficients in an imaginary quadratic field, but not for other number fields. Recently, Beukers has proved a remarkable *qualitative* linear independence theorem for the values at an algebraic point of E-functions with arbitrary algebraic Taylor coefficients. But no *quantitative* analogue of Shidlovskii's measure has been given in Beukers' setting. The goal of this paper it to obtain such a measure, in an even more general setting where the point can be a singularity. This enables us to solve a long standing problem: the value of an E-function at an algebraic point is never a Liouville number, a result which had been obtained before only under additional assumptions. We deduce various explicit irrationality measures, in particular for values of the exponential and Bessel's J_0 function at non-zero algebraic points. We also prove that the values at rational points of E-functions with rational Taylor coefficients are linearly independent over $\overline{\mathbb{Q}}$ if and only if they are linearly independent over $\mathbb{Q}$. Our methods rest upon improvements of results recently obtained by André and Beukers by means of the theory of E-operators.

1 Introduction

Siegel [14] defined in 1929 the class of E-functions in order to generalize the Diophantine properties of the exponential function (namely the Lindemann-Weierstrass Theorem) to other special functions such as Bessel's function $J_0(z) := \sum_{n=0}^{\infty}(-1)^n(z/2)^{2n}/n!^2$ or hypergeometric series ${}_pF_p$ with rational parameters. A power series $\sum_{n=0}^{\infty}\frac{a_n}{n!}z^n \in \overline{\mathbb{Q}}[[z]]$ is said to be an E-function when it is solution of a linear differential equation over $\overline{\mathbb{Q}}(z)$ (i.e., holonomic), and $|\sigma(a_n)|$ (for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) and the least common denominator of $a_0, a_1, \dots, a_n$ all grow at most exponentially in n. Note that Siegel's original definition of E-functions is more general: see the end of this introduction. Throughout this paper we fix an embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$.

A lot of important qualitative results are known on the arithmetic nature of the values taken by E-functions at algebraic points, amongst which we cite the celebrated Siegel-Shidlovskii Theorem. It has been improved in [11]. However, these results are not always

strong enough, in particular they do not imply the linear independence of values of E-functions solutions of a differential system of order 1 and evaluated at a non-singular point. Quantitative versions of certain of these results exist, but only under very strict assumptions on algebraic independence or rationality of the coefficients of the E-functions. The main result in this direction, in the setting of linear independence, is the following one. It is due to Shidlovskii [13, p. 358, Theorem 1, Eq. (32)].

Theorem A (Shidlovskii)**.** *Let $\underline{f} = {}^t(f_1, \dots, f_N) \in \mathbb{Q}[[z]]^N$ be a vector of E-functions solution of a differential system $\underline{f'} = A\underline{f}$ for some $A \in M_N(\mathbb{Q}(z))$. Assume that $f_1, \dots, f_N$ are linearly independent over $\mathbb{Q}(z)$ and that $z_0 \in \mathbb{Q}^*$ is not a pole of an entry of A. Then for any $\varepsilon > 0$, there exists $c = c(\varepsilon, z_0, f_1, \dots, f_N) > 0$ such that for all $\lambda_1, \dots, \lambda_N \in \mathbb{Z}$ not all zero, we have*

$$\left| \sum_{j=1}^{N} \lambda_j f_j(z_0) \right| > cH^{-N+1-\varepsilon} \qquad \text{where } H := \max_{1 \le j \le N} |\lambda_j|.$$

This theorem holds *verbatim* with $\mathbb{Q}$ replaced by an imaginary quadratic number field and $\mathbb{Z}$ replaced by its ring of integers. However no such result is known for other number fields $\mathbb{K}$. The point is that all known quantitative results are based on the Siegel-Shidlovskii method only, which provides linear independence of the full set of the values of E-functions in Theorem A only when $\mathbb{K}$ is either $\mathbb{Q}$ or imaginary quadratic. Even the qualitative part of Theorem A (namely, $\sum_{j=1}^{N} \lambda_j f_j(z_0) \neq 0$) has been proved only recently by Beukers [4, Corollary 1.4] for arbitrary number fields, using André's theory of E-operators [1].

Theorem B (Beukers)**.** *Let $\underline{f} = {}^t(f_1, \dots, f_N) \in \overline{\mathbb{Q}}[[z]]^N$ be a vector of E-functions solution of a differential system $\underline{f}' = A\underline{f}$ for some $A \in M_N(\overline{\mathbb{Q}}(z))$. Assume that $f_1, \dots, f_N$ are linearly independent over $\overline{\mathbb{Q}}(z)$ and that $z_0 \in \overline{\mathbb{Q}}^*$ is not a pole of an entry of A. Then the numbers $f_1(z_0), \dots, f_N(z_0)$ are linearly independent over $\overline{\mathbb{Q}}$.*

The purpose of this paper is to prove new Diophantine results using this approach of André and Beukers. Our first main result is the following theorem, where we generalize Theorem A to any E-functions, by removing the rationality assumption on the coefficients and also the non-singularity assumption on z_0. We recall that for a non-zero algebraic number α, its house $\overline{|\alpha|}$ is the maximum of the moduli of α and of all its Galois conjugates over $\mathbb{Q}$. We also denote by $\mathcal{O}_{\mathbb{K}}$ the ring of integers of a number field $\mathbb{K}$.

Theorem 1. *Let $\mathbb{K}$ be a number field of degree d over $\mathbb{Q}$, $z_0 \in \mathbb{K}$, and $\underline{f} = {}^t(f_1, \dots, f_N)$ be a vector of E-functions with coefficients in $\mathbb{K}$ such that $\underline{f}' = A\underline{f}$ for some $A \in M_N(\mathbb{K}(z))$. Then for any $\varepsilon > 0$, there exists $c = c(\varepsilon, \mathbb{K}, z_0, f_1, \dots, f_N) > 0$ with the following property.*

For any $\lambda_1, \dots, \lambda_N \in \mathcal{O}_{\mathbb{K}}$, if $\Lambda := \lambda_1 f_1(z_0) + \dots + \lambda_N f_N(z_0)$ is non-zero, then

$$|\Lambda| > cH^{-d^{d+1}N^d+1-\varepsilon} \qquad \text{where } H := \max_{1 \le j \le N} \overline{|\lambda_j|}.$$

Remarks. – Given arbitrary E-functions $f_1, \dots, f_N$ and any $z_0 \in \overline{\mathbb{Q}}$, this theorem applies because there exists a number field $\mathbb{K}$ containing z_0 and all coefficients of $f_1, \dots, f_N$, and the family $(f_1, \dots, f_N)$ can always be enlarged to satisfy a first-order differential system. This shows, without any assumption on $f_1, \dots, f_N$ and z_0, the existence of $\kappa, c > 0$ such that $|\Lambda| > cH^{-\kappa}$ provided $\Lambda \neq 0$.

– Note that in Theorem 1, and even in the previous remark, we do not assume that $f_1(z_0), \dots, f_N(z_0)$ are linearly independent over $\mathbb{K}$, and we do not wonder whether z_0 is a singularity or not of a differential system involving the f_j. Therefore with $\mathbb{K} = \mathbb{Q}$, Theorem 1 is a generalization of Theorem A: we obtain the same lower bound under milder assumptions (using Beukers' results in [4] and improvements of the latter).

– We shall prove that if $\lambda_1, \dots, \lambda_N \in \mathbb{Z}$, the lower bound in Theorem 1 can be refined to $cH^{-dN^d+1-\varepsilon}$.

– To our knowledge, Theorem 1 provides the first quantitative version of Beukers' Theorem B, when it is further assumed in Theorem 1 that $f_1, \dots, f_N$ are linearly independent over $\mathbb{K}(z)$ and that $z_0 \in \mathbb{K}^*$ is not a pole of A, ensuring that $\Lambda \neq 0$.

An important consequence of Theorem 1 is the following result, which completely settles the problem of deciding whether (real) values of E-functions can be Liouville numbers or not. We recall that a Liouville number is a real number ξ such that there exist two sequences of rational integers p_n, q_n such that $0 < |q_n\xi - p_n| < 1/q_n^n$ for all sufficiently large integers n (*a fortiori* $p_n q_n \neq 0$).

Corollary 1. *Let f be an E-function, and z_0 be an algebraic number. Then $f(z_0)$ is not a Liouville number.*

The proof of Corollary 1 runs as follows: in Theorem 1, let $z_0 \in \overline{\mathbb{Q}}$, take $f_1 := 1$, $f_2 := f$ and consider a vector ${}^t(f_1, f_2 \dots, f_N)$ of E-functions with coefficients in a number field $\mathbb{K}$ such that $\underline{f}' = A\underline{f}$ for some $A \in M_N(\mathbb{K}(z))$, where $\mathbb{K}$ is large enough to contain z_0. If $f(z_0) \in \mathbb{Q}$, then $f(z_0)$ is not a Liouville number. If $f(z_0) \notin \mathbb{Q}$, then $\lambda_1 + \lambda_2 f(z_0) \neq 0$ for all $\lambda_1, \lambda_2 \in \mathbb{Z}$ not both zero, so that Theorem 1 yields $|\lambda_1 + \lambda_2 f(z_0)| > c \max(|\lambda_1|, |\lambda_2|)^{-\kappa}$ for some $c, \kappa > 0$. This rules out the possibility that $f(z_0)$ is a Liouville number.

Of course Corollary 1 is interesting only when $f(z_0) \in \mathbb{R}$. If we do not assume this, note however that the real and imaginary parts of $f(z_0)$ are values of E-functions (see the remark in §2.1 below), so that none of them is a Liouville number.

Let us also mention another interesting corollary, which is a consequence of the third remark that follows Theorem 1 with $N = 2$ and $N = 3$ respectively (recall that $J_0(z)$ is solution of $zy''(z) + y'(z) + zy(z) = 0$).

Corollary 2. *For any algebraic number $\alpha \in \overline{\mathbb{Q}}^*$ of degree d over $\mathbb{Q}$ and any $\varepsilon > 0$, there exists $c = c(\alpha, \varepsilon)$ such that, for all $(p, q) \in \mathbb{Z} \times \mathbb{N}$ with $q \neq 0$,*

$$\left|e^\alpha - \frac{p}{q}\right| > \frac{c}{q^{d2^d+\varepsilon}}, \quad \text{respectively} \quad \left|J_0(\alpha) - \frac{p}{q}\right| > \frac{c}{q^{d3^d+\varepsilon}}.$$

A general transcendence measure for E-functions due to Lang and Galochkin [6, p. 238, Theorem 5.29 and remarks] (applied with $m = 1$ and $m = 2$ respectively) gives $4d^2 + 1$

instead of $d2^d$, and $16d^3+1$ instead of $d3^d$; see also [13, p. 403]. This is of course much better than Corollary 2 for large d but our bounds turn out to be smaller for $d \in \{1,2,3,4\}$ and $d \in \{1,2,3,4,5\}$ respectively.

A less classical example is the following: for any $\alpha \in \overline{\mathbb{Q}}^*$ and any integers $p, q \geq 1$, the value at $z = \alpha$ of the function $\mathcal{A}_{p,q}(z) := \sum_{n=0}^{\infty}(\sum_{k=0}^{n}\binom{n}{k}^p\binom{n+k}{n}^q)z^n/n!$ is not a Liouville number; $\mathcal{A}_{p,q}(\alpha)$ is proved to be a transcendental number in [5, §4.6] when $(p,q) \in \{1,2,3,4\}^2$, the situation in general being unknown. More specifically, it is also proved in [5, §4.6, Table 1] that when $(p,q) = (2,2)$, the minimal inhomogeneous differential equation over $\mathbb{Q}(z)$ satisfied by $\mathcal{A}_{2,2}$ is of order 4 and 0 is its only singularity. Hence, the following holds by the third remark that follows Theorem 1 with $N = 5$: for all $\alpha \in \overline{\mathbb{Q}}^*$ of degree d over $\mathbb{Q}$ and all $\varepsilon > 0$, there exists $c = c(\varepsilon, \alpha) > 0$ such that for all $\lambda_j \in \mathbb{Z}$ not all 0, we have

$$\left|\lambda_4 + \sum_{j=0}^{3} \lambda_j \mathcal{A}_{2,2}^{(j)}(\alpha)\right| > c \max_{0 \leq j \leq 4} |\lambda_j|^{-d5^d+1-\varepsilon}.$$

In particular, for any $\alpha \in \overline{\mathbb{Q}}^*$ of degree d and $\varepsilon > 0$, there exists $c = c(\varepsilon, \alpha) > 0$ such that for any $(p,q) \in \mathbb{Z} \times \mathbb{N}$ with $q \neq 0$,

$$\left|\mathcal{A}_{2,2}(\alpha) - \frac{p}{q}\right| > \frac{c}{q^{d5^d+\varepsilon}}. \tag{1.1}$$

It seems reasonable to make the following conjecture, which probably belongs to folklore. This conjecture is Roth's Theorem if $f(z_0)$ is algebraic.

Conjecture 1. *Let f be an E-function and $z_0 \in \overline{\mathbb{Q}}$. For any $\varepsilon > 0$, there exists $c > 0$ such that for any $(p,q) \in \mathbb{Z} \times \mathbb{N}$ with $q \neq 0$, either $qf(z_0) - p = 0$ or*

$$\left|f(z_0) - \frac{p}{q}\right| > \frac{c}{q^{2+\varepsilon}}.$$

Zudilin has proved this conjecture in [15] in a stronger form but under additional assumptions (which even imply $f(z_0) \notin \mathbb{Q}$), namely: f is an E-function with rational coefficients, $z_0 \in \mathbb{Q}^*$ is not a singularity of a differential system satisfied by $1, f, f_2, \ldots, f_N$ over $\mathbb{Q}(z)$ (for some $N \geq 2$) and $f, f_2, \ldots, f_N$ are algebraically independent over $\mathbb{Q}(z)$. It would be interesting to know if $\mathcal{A}_{2,2}, \mathcal{A}'_{2,2}, \mathcal{A}''_{2,2}, \mathcal{A}'''_{2,2}$ are algebraically independent over $\mathbb{Q}(z)$, in which case the exponent 5 could be improved to 2 in (1.1) when $\alpha \in \mathbb{Q}^*$.

The second goal of this paper is to understand the structure of the ring $\mathbf{E}$ of all values at algebraic points of E-functions; this algebraic point can always be assumed to be 1 because if $f(z)$ is an E-function, so is $f(\alpha z)$ for any $\alpha \in \overline{\mathbb{Q}}$. Elements of $\mathbf{E}$ are related to exponential periods (see [9, §4.3]).

For any subfield $\mathbb{K}$ of $\overline{\mathbb{Q}}$, we shall also consider the subring $\mathbf{E}_{\mathbb{K}}$ of $\mathbf{E}$ which consists of the evaluations $f(1)$ where f is an E-function with coefficients in $\mathbb{K}$ (the number 1 could be replaced by any non-zero element of $\mathbb{K}$ without changing $\mathbf{E}_{\mathbb{K}}$). Note that $\mathbf{E}$ is the union of all $\mathbf{E}_{\mathbb{K}}$, where $\mathbb{K}$ is a number field, since for any E-function f the holonomy property implies the existence of a number field that contains all coefficients of f.

We have defined and studied [7] analogous rings $\mathbf{G}_{\mathbb{K}}$ with G-functions instead of E-functions; it turns out that $\mathbf{G}_{\mathbb{K}}$ is nearly independent from $\mathbb{K}$ (precisely, $\mathbf{G}_{\mathbb{K}} = \mathbf{G}_{\mathbb{Q}}$ if $\mathbb{K} \subset \mathbb{R}$, and $\mathbf{G}_{\mathbb{K}} = \mathbf{G}_{\mathbb{Q}(i)}$ otherwise). The situation is completely different for E-functions. A first hint in this direction was given in [8, Theorem 4] (stated as Lemma 1 in §4 below). The way $\mathbf{E}_{\mathbb{K}}$ depends on $\mathbb{K}$ is completely described by the following result.

Theorem 2. *Elements of $\mathbf{E}_{\mathbb{Q}}$ are linearly independent over $\overline{\mathbb{Q}}$ if, and only if, they are linearly independent over $\mathbb{Q}$. In other words, the $\mathbb{Q}$-algebras $\mathbf{E}_{\mathbb{Q}}$ and $\overline{\mathbb{Q}}$ are linearly disjoint, and the natural map $\mathbf{E}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to \mathbf{E}$ (sending $\xi \otimes z$ to ξz) is a $\mathbb{Q}$-algebra isomorphism.*

We refer to [3, Chapter V, §2, No. 5] for the definition and properties of linearly disjoint algebras, which imply the following.

Corollary 3. *Let $\mathbb{K}$ be a number field, and $(\omega_1, \ldots, \omega_d)$ be a basis of the $\mathbb{Q}$-vector space $\mathbb{K}$. Then*

$$\mathbf{E}_{\mathbb{K}} = \omega_1 \mathbf{E}_{\mathbb{Q}} \oplus \ldots \oplus \omega_d \mathbf{E}_{\mathbb{Q}}.$$

In other words, for any $\xi \in \mathbf{E}_{\mathbb{K}}$ there exists a unique d-tuple $(\xi_1, \ldots, \xi_d) \in \mathbf{E}_{\mathbb{Q}}^d$ such that $\xi = \omega_1 \xi_1 + \ldots + \omega_d \xi_d$.

Theorems 1 and 2 may seem disjoint at first sight but their proofs share many common aspects, in particular both use Proposition 1 stated in §2.1. Another consequence of Proposition 1 is the existence of an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathbf{E}$, of which the fixed points are exactly the elements of $\mathbf{E}_{\mathbb{Q}}$. For instance, with the notation of Corollary 3, we have $\sigma(\xi) = \sigma(\omega_1)\xi_1 + \ldots + \sigma(\omega_d)\xi_d$ for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. As a first application of this Galois action, we explain in §6 why our proof of Theorem 1 is similar to Liouville's proof that Liouville numbers are transcendental. This makes sense because Theorem 1 is a generalization of this result, since $\overline{\mathbb{Q}} \subset \mathbf{E}$. We hope this action can have other Diophantine applications.

The original definition of E-functions, given by Siegel [14], is slightly less restrictive: instead of geometric bounds, he allowed growths bounded by $n!^{\varepsilon}$ (for any given $\varepsilon > 0$, provided n is large enough with respect to ε). Shidlovskii's Theorem A holds for E-functions in Siegel's sense, and Beukers' Theorem B was later proved by André [2] in this general setting, by a different method. All other results in Beukers' paper [4] have been adapted by Lepetit [10]. Therefore all the results of the present paper also hold for E-functions in Siegel's sense.

The structure of this paper is as follows. In §2 we prove the main tool of this paper, namely Proposition 1, and use it to obtain a version of Beukers' desingularization process over a number field. This enables us to prove Theorem 1 in §3, and also to obtain in §4 a decomposition of an E-function over a number field, involving an E-function that takes only transcendental values at non-zero algebraic points. At last we apply the previous results in §5 to study the structure of $\mathbf{E}_{\mathbb{K}}$ and prove Theorem 2. We conclude in §6 with the above-mentioned Galois action on values of E-functions.

2 Main tools

2.1 Conjugates of E-functions

Let $f(z) = \sum_{n=0}^{\infty} a_n z^n$ be an E-function with coefficients $a_n \in \overline{\mathbb{Q}}$. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we let $f^\sigma(z) = \sum_{n=0}^{\infty} \sigma(a_n) z^n$. Then f^σ is also an E-function, and if g is an E-function then for any σ, τ we have $(f+g)^\sigma = f^\sigma + g^\sigma$, $(fg)^\sigma = f^\sigma g^\sigma$ and $(f^\sigma)^\tau = f^{\tau\circ\sigma}$. Moreover if f has coefficients in a number field $\mathbb{K}$, then f^σ has coefficients in the number field $\sigma(\mathbb{K})$.

Remark. Denoting by σ the complex conjugation, for any E-function f we can consider $\frac{1}{2}(f + f^\sigma)$ and $\frac{1}{2i}(f - f^\sigma)$. These E-functions have real coefficients, which are respectively the real and imaginary parts of those of f. In particular, the real and imaginary parts of any element of $\mathbf{E}$ belong to $\mathbf{E}$.

The following result is central in the present paper; we refer to [5, Proposition 3.5] for a similar result. Throughout this paper we agree that minimal polynomials of algebraic elements have leading coefficient 1.

Proposition 1. *Let f be an E-function with coefficients in a number field $\mathbb{K}$, and $z_0 \in \overline{\mathbb{Q}}^*$. Then the following assertions are equivalent:*

(*i*) *f vanishes at z_0.*

(*ii*) *There exists $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that f^σ vanishes at $\sigma(z_0)$.*

(*iii*) *For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, f^σ vanishes at $\sigma(z_0)$.*

(*iv*) *There exists an E-function g with coefficients in $\mathbb{K}$ such that*

$$f(z) = D(z)g(z) \text{ where } D \text{ is the minimal polynomial of } z_0 \text{ over } \mathbb{K}.$$

In particular, if z_0 is rational and f vanishes at z_0, then all conjugates f^σ of f also vanish at z_0. Also, if an E-function f with rational coefficients vanishes at some $z_0 \in \overline{\mathbb{Q}}^*$, then it vanishes at all Galois conjugates of z_0.

We remark that with $z_0 = 1$, the implication $(i) \Rightarrow (iii)$ is used already in the proof of [4, Proposition 4.1], which is the main result Proposition 1 is based on.

Proof of Proposition 1. $(iv) \Rightarrow (iii)$ Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $f^\sigma(z) = D^\sigma(z)g^\sigma(z)$, and $D^\sigma(\sigma(z_0)) = \sigma(D(z_0)) = 0$. Therefore $f^\sigma(\sigma(z_0)) = 0$.

$(iii) \Rightarrow (ii)$ is trivial.

$(ii) \Rightarrow (i)$ Enlarging $\mathbb{K}$ if necessary, we may assume the extension $\mathbb{K}/\mathbb{Q}$ to be Galois and to contain z_0. Then f^σ has coefficients in $\mathbb{K}$, and $\sigma(z_0) \in \mathbb{K}^*$. Using [4, Proposition 4.1] there exists an E-function g such that $f^\sigma(z) = (z - \sigma(z_0))g(z)$. Then g has coefficients in $\mathbb{K}$; applying σ^{-1} yields $f(z) = (z - z_0)g^{\sigma^{-1}}(z)$ so that $f(z_0) = 0$.

$(i) \Rightarrow (iv)$ Using [4, Proposition 4.1] there exists an E-function h such that $f(z) = (z - z_0)h(z)$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$, that is: σ is a field automorphism of $\overline{\mathbb{Q}}$ such that $\sigma(x) = x$ for any $x \in \mathbb{K}$. Then $f(z) = f^\sigma(z) = (z - \sigma(z_0))h^\sigma(z)$ so that f vanishes at $\sigma(z_0)$. Let $z_1 := z_0, z_2, \ldots, z_\ell$ denote the (pairwise distinct) Galois conjugates of z_0 over $\mathbb{K}$, i.e. the elements of the form $\sigma(z_0)$ with $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$; we have proved that f vanishes at $z_1, \ldots, z_\ell$. Applying [4, Proposition 4.1] yields, by induction on $j \in \{0, \ldots, \ell\}$, the existence of an E-function g_j such that $f(z) = g_j(z) \prod_{i=1}^{j}(z - z_i)$. Since $D(z) = \prod_{i=1}^{\ell}(z - z_i)$, we have $f(z) = D(z)g_\ell(z)$. Now $D(z) \in \mathbb{K}[z] \setminus \{0\}$ so that all coefficients of g_ℓ belong to $\mathbb{K}$. This concludes the proof of Proposition 1. □

2.2 Beukers' desingularization process

In the proof of Theorem 1 we shall use the following version of Beukers' desingularization theorem (namely [4, Theorem 1.5]). The new point is that $e_1, \ldots, e_N$ and the coefficients of B and M have coefficients in the number field $\mathbb{K}$ (whereas in [4, Theorem 1.5] these coefficients are simply algebraic numbers).

Proposition 2. *Let $\mathbb{K}$ be a number field, and $f_1, \ldots, f_N$ be E-functions with coefficients in $\mathbb{K}$, linearly independent over $\mathbb{C}(z)$. Assume that the vector $\underline{f} = {}^t(f_1, \ldots, f_N)$ satisfies a first-order differential system $\underline{f}' = A\underline{f}$ with $A \in M_n(\mathbb{K}(z))$.*

Then there exist E-functions $e_1, \ldots, e_N$ with coefficients in $\mathbb{K}$, linearly independent over $\mathbb{C}(z)$, a matrix $B \in M_n(\mathbb{K}[z, 1/z])$ and a matrix $M \in M_n(\mathbb{K}[z])$, such that with $\underline{e} = {}^t(e_1, \ldots, e_N)$:

$$\underline{e}' = B\underline{e} \quad \text{and} \quad \underline{f} = M\underline{e}.$$

The proof follows [4, p. 378], using also the additional details given in [5]. Actually Proposition 2 is already proved implicitly (for $\mathbb{K} = \mathbb{Q}$) by the implementation described in [5].

In what follows we simply mention the parts of the proof where a special attention has to be paid. Let α be a singularity of the differential system $Y' = AY$, and $Q \in \mathbb{K}[X]$ denote the minimal polynomial of α over $\mathbb{K}$. Let $k \geq 1$ be the maximal order of α as a pole of a coefficient of A, and (i_0, j_0) be such that A_{i_0,j_0} has a pole of order exactly k at α. Then $Q^k A\underline{f} = Q^k \underline{f}'$ vanishes at α; the i_0-th coordinate of this vector provides a linear relation

$$\sum_{j=1}^{N} (Q^k A_{i_0,j})(\alpha) f_j(\alpha) = 0.$$

Note that for any j, the rational function $Q(z)^k A_{i_0,j}(z) \in \mathbb{K}(z)$ is holomorphic at α, and for $j = j_0$ it does not vanish at that point. Multiplying by a suitable element of $\mathbb{K}[z]$ which does not vanish at α, we obtain $P_1, \ldots, P_N \in \mathbb{K}[z]$ such that

$$P_{j_0}(\alpha) \neq 0 \quad \text{and} \quad \sum_{j=1}^{N} P_j(\alpha) f_j(\alpha) = 0.$$

Upon dividing by their gcd, we may assume the polynomials $P_1, \dots, P_N$ to be coprime. If $N = 1$ we let $P_{1,1} = 1$; otherwise there exist polynomials $P_{i,j} \in \mathbb{K}[z]$, for $2 \le i \le N$ and $1 \le j \le N$, such that letting $P_{1,j} = P_j$, the matrix $S = (P_{i,j})_{1 \le i,j \le N} \in M_N(\mathbb{K}[z])$ has determinant 1. Then $S\underline{f}$ is a vector of E-functions, with coefficients in $\mathbb{K}$, of which the first coordinate $\sum_{j=1}^N P_j(z) f_j(z)$ vanishes at α. Using Proposition 1, we deduce that $\sum_{j=1}^N P_j(z) f_j(z)$ vanishes at $\sigma(\alpha)$ for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$. Denoting by $\mathcal{F}$ a fundamental system of solutions of which $\underline{f}$ is the first column, and considering the differential Galois group as in [4], yields a matrix $\mathcal{F}_1$ with coefficients holomorphic at α, such that $S\mathcal{F} = D\mathcal{F}_1$ where D is the diagonal matrix with diagonal coefficients $Q(z)$, 1, ..., 1. This concludes the proof as in [4].

3 Proof of Theorem 1

The proof of Theorem 1 falls into 3 steps.

Step 1. Let us prove Theorem 1 in the special case where $\mathbb{K} = \mathbb{Q}$ (i.e., $d = 1$). In other words, we assume that $z_0 \in \mathbb{Q}$, $\lambda_1, \dots, \lambda_N \in \mathbb{Z}$, and $f_1, \dots, f_N$ have coefficients in $\mathbb{Q}$.

If $z_0 = 0$ then $f_1(z_0), \dots, f_N(z_0)$ are algebraic numbers, so the conclusion follows from Schmidt's subspace theorem (see for instance [6, Chapter 1, §8.2, Theorem 1.37]).

Therefore we assume $z_0 \neq 0$, and even $z_0 = 1$ by considering the E-functions $f_j(z_0 z)$ instead of $f_j(z)$.

Recall that we do not assume that $f_1(1), \dots, f_N(1)$ are linearly independent over $\mathbb{Q}$. Denoting by N' the maximal number of linearly independent numbers among them, we may assume (up to a permutation of the indices) that $f_1(1), \dots, f_{N'}(1)$ are linearly independent over $\mathbb{Q}$, and $f_{N'+1}(1), \dots, f_N(1)$ belong to the $\mathbb{Q}$-vector space they span. There exist rational numbers $\varrho_{i,j}$ such that $f_j(1) = \sum_{i=1}^{N'} \varrho_{i,j} f_i(1)$ for any $1 \le j \le N$, so that

$$\Lambda = \sum_{j=1}^{N} \lambda_j f_j(1) = \sum_{i=1}^{N'} \mu_i f_i(1) \quad \text{with} \quad \mu_i := \sum_{j=1}^{N} \lambda_j \varrho_{i,j} \in \mathbb{Q}. \tag{3.1}$$

Observe that the E-functions $f_1, \dots, f_{N'}$ are linearly independent over $\mathbb{C}(z)$. Indeed, otherwise they would be linearly dependent over $\mathbb{Q}(z)$ (since they have coefficients in $\mathbb{Q}$), and a relation $\sum_{j=1}^{N'} S_j(z) f_j(z) = 0$ would exist with $S_1, \dots, S_{N'} \in \mathbb{Q}(z)$ not all zero. Upon multiplying by $(z-1)^k$ for a suitable $k \in \mathbb{Z}$, we may assume that none of the S_j has a pole at 1, and that at least of them does not vanish at 1. This provides a non-trivial linear relation $\sum_{j=1}^{N'} S_j(1) f_j(1) = 0$, which contradicts the definition of N'.

Therefore $f_1, \dots, f_{N'}$ are linearly independent over $\mathbb{C}(z)$. Denote by N'' the dimension of the vector space generated over $\mathbb{C}(z)$ by $f_1, \dots, f_N$; we have $N' \le N'' \le N$. Notice that it could happen that $N'' > N'$, for instance if $f_{N'+1}(1) = 0$. Up to a permutation of the indices, we may assume that $f_1, \dots, f_{N''}$ are linearly independent over $\mathbb{C}(z)$, and that $f_{N''+1}, \dots, f_N$ belong to the vector space they span over $\mathbb{C}(z)$.

Since $f_1, \dots, f_{N''}$ are linearly independent over $\mathbb{C}(z)$, and satisfy a linear differential system of order 1 by definition of N'', Proposition 2 (applied with $\mathbb{K} = \mathbb{Q}$) provides E-functions $e_1, \dots, e_{N''}$ with rational coefficients and matrices B and $M = (P_{i,j})$ with $P_{i,j} \in \mathbb{Q}[z]$ such that $f_i(z) = \sum_{j=1}^{N''} P_{i,j}(z) e_j(z)$. Since $N' \leq N''$, Eq. (3.1) yields

$$\Lambda = \sum_{j=1}^{N''} \nu_j e_j(1) \quad \text{with} \quad \nu_j := \sum_{i=1}^{N'} \mu_i P_{i,j}(1) \in \mathbb{Q}. \tag{3.2}$$

Now Shidlovskii's lower bound stated as Theorem A in the introduction applies to the E-functions $e_1, \dots, e_{N''}$ with rational coefficients, which are linearly independent over $\mathbb{C}(z)$ and solution of a linear differential system of order 1 of which 1 is not a singularity. Denoting by δ a common denominator of the rational numbers $P_{i,j}(1)$ and $\varrho_{i,j}$ (appearing in Eqns. (3.1) and (3.2)), we obtain that $\delta^2\Lambda$ is a $\mathbb{Z}$-linear combination of $e_1(1), \dots, e_{N''}(1)$ with coefficients bounded (in absolue value) by cH, where $c > 0$ and δ depend only on $f_1, \dots, f_N$. For any $\varepsilon > 0$, Theorem A yields $|\delta^2\Lambda| > c_0 H^{-N''+1-\varepsilon} \geq c_0 H^{-N+1-\varepsilon}$ for some $c_0 > 0$ which depends only on $f_1, \dots, f_N$. This concludes the proof of Theorem 1 in the case where $\mathbb{K} = \mathbb{Q}$.

Step 2. Let us prove Theorem 1 for any number field $\mathbb{K}$, in the case where $\lambda_j \in \mathbb{Z}$ for any j. As announced in the introduction (after the statement of Theorem 1), we shall refine the lower bound $H^{-d^{d+1}N^d+1-\varepsilon}$ to $H^{-dN^d+1-\varepsilon}$ in this case.

For simplicity of the exposition, we assume $\mathbb{K}$ to be a Galois extension of $\mathbb{Q}$; see the end of Step 2 for the general case. We denote by G the Galois group of $\mathbb{K}/\mathbb{Q}$, and consider the complex number

$$\varpi = \prod_{\sigma \in G} \Big(\sum_{j=1}^{N} \lambda_j f_j^\sigma(1) \Big). \tag{3.3}$$

To begin with, let us prove that $\varpi \neq 0$. Indeed, consider the E-function $g(z) = \sum_{j=1}^{N} \lambda_j f_j(z)$; it has coefficients in $\mathbb{K}$ (because $f_1, \dots, f_N$ do), and $g(1) = \Lambda \neq 0$. For any $\sigma \in G$, Proposition 1 yields $g^\sigma(1) \neq 0$. Now $g^\sigma(1) = \sum_{j=1}^{N} \lambda_j f_j^\sigma(1)$ since $\lambda_j \in \mathbb{Z}$, so that $\varpi = \prod_{\sigma \in G} g^\sigma(1) \neq 0$.

Now we are going to expand the product in the definition (3.3) of ϖ. Denote by $\mathcal{N}$ the set of all tuples $\underline{n} = (n_1, \dots, n_N)$ of non-negative integers such that $n_1 + \ldots + n_N = d$. For any $\underline{n} \in \mathcal{N}$, we denote by $I(\underline{n})$ the set of all families $\underline{i} = (i_\sigma)_{\sigma \in G}$ consisting in integers $i_\sigma \in \{1, \dots, N\}$ such that for any $j \in \{1, \dots, N\}$ we have:

$$\mathrm{Card}\{\sigma \in G,\ i_\sigma = j\} = n_j.$$

Then Eq. (3.3) yields

$$\varpi = \sum_{\underline{n} \in \mathcal{N}} \lambda_1^{n_1} \cdot \ldots \cdot \lambda_N^{n_N} \varphi_{\underline{n}}(1) \quad \text{upon letting} \quad \varphi_{\underline{n}}(z) := \sum_{\underline{i} \in I(\underline{n})} \prod_{\sigma \in G} f_{i_\sigma}^\sigma(z). \tag{3.4}$$

Let us prove that $\varphi_{\underline{n}}(z)$, which is an E-function with coefficients in $\mathbb{K}$, actually has coefficients in $\mathbb{Q}$ for any $\underline{n} \in \mathcal{N}$. For any $\tau \in G$ we have:

$$\begin{aligned}
\varphi_{\underline{n}}^{\tau} &= \sum_{\underline{i} \in I(\underline{n})} \prod_{\sigma \in G} \left(f_{i_\sigma}^{\sigma}\right)^{\tau} \\
&= \sum_{\underline{i} \in I(\underline{n})} \prod_{\sigma \in G} f_{i_\sigma}^{\tau \circ \sigma} \\
&= \sum_{\underline{i} \in I(\underline{n})} \prod_{\sigma' \in G} f_{i_{\tau^{-1} \circ \sigma'}}^{\sigma'} \quad \text{by letting } \sigma' = \tau \circ \sigma \\
&= \sum_{\underline{i}' \in I(\underline{n})} \prod_{\sigma' \in G} f_{i'_{\sigma'}}^{\sigma'}
\end{aligned}$$

where the last equality comes from letting $i'_\sigma = i_{\tau^{-1} \circ \sigma}$ for any $\sigma \in G$; indeed this defines a bijective map $I(\underline{n}) \to I(\underline{n})$. Therefore $\varphi_{\underline{n}}^{\tau} = \varphi_{\underline{n}}$ for any $\tau \in G$, and the E-function $\varphi_{\underline{n}}(z)$ has coefficients in $\mathbb{Q}$.

We denote by $\mathcal{E}$ the vector space spanned over $\overline{\mathbb{Q}}(z)$ by the functions $\prod_{\sigma \in G} f_{i_\sigma}^{\sigma}$ for all families $\underline{i} = (i_\sigma)_{\sigma \in G}$ consisting in integers $i_\sigma \in \{1, \dots, N\}$. There are N^d such families, so $\dim \mathcal{E} \leq N^d$. Moreover we have $g' \in \mathcal{E}$ for any $g \in \mathcal{E}$.

Let δ denote the dimension of the vector space spanned over $\mathbb{Q}(z)$ by the functions $\varphi_{\underline{n}}$ for $\underline{n} \in \mathcal{N}$. We can choose δ functions $h_1, \dots, h_\delta$ among the $\varphi_{\underline{n}}$ which are linearly independent, and span the same $\mathbb{Q}(z)$-vector space. Choosing among the successive derivatives of $h_1, \dots, h_\delta$ it is possible to find an integer $\delta' \geq \delta$ and functions h_i, for $\delta + 1 \leq i \leq \delta'$, such that $h_1, \dots, h_{\delta'}$ are linearly independent over $\mathbb{Q}(z)$ and satisfy a linear differential system of order 1. Since they have rational coefficients, they are also linearly independent over $\overline{\mathbb{Q}}(z)$; now they all belong to $\mathcal{E}$, so we have $\delta' \leq \dim \mathcal{E} \leq N^d$.

Proposition 2 with $\mathbb{K} = \mathbb{Q}$ yields a vector of E-functions $e_1, \dots, e_{\delta'}$ with rational coefficients, solution of a first-order differential system with no finite non-zero singularity, such that each h_i is a linear combination of $e_1, \dots, e_{\delta'}$ with coefficients in $\mathbb{Q}[z]$. There exist $R_{\underline{n},i}, S_{\underline{n},i} \in \mathbb{Q}(z)$ for $\underline{n} \in \mathcal{N}$ and $1 \leq i \leq \delta'$ such that, for any $\underline{n}$,

$$\varphi_{\underline{n}}(z) = \sum_{i=1}^{\delta'} R_{\underline{n},i}(z) h_i(z) = \sum_{i=1}^{\delta'} S_{\underline{n},i}(z) e_i(z).$$

If no $S_{\underline{n},i}$ has a pole at $z = 1$, we can take $z = 1$ in this equation. To deal with the general case, we expand the right hand side as a polynomial in $1/(z-1)$, up to an additive term which is holomorphic and vanishes at $z = 1$. Since $\varphi_{\underline{n}}(z)$ is holomorphic at 1, all polar contributions cancel out and the value at $z = 1$ is given by the constant term of the above-mentioned polynomial. This provides an expression of the form

$$\varphi_{\underline{n}}(1) = \sum_{i=1}^{\delta'} \sum_{j=0}^{J} a_{\underline{n},i,j} e_i^{(j)}(1)$$

with $a_{\underline{n},i,j} \in \mathbb{Q}$. Since ${}^t(e_1, \dots, e_{\delta'})$ is solution of a first-order differential system with coefficients in $\mathbb{Q}[z, 1/z]$, hence with no finite non-zero singularity, we obtain finally

$$\varphi_{\underline{n}}(1) = \sum_{i=1}^{\delta'} b_{\underline{n},i} e_i(1) \tag{3.5}$$

with $b_{\underline{n},i} \in \mathbb{Q}$ (where simply $b_{\underline{n},i} := S_{\underline{n},i}(1)$ in the "no pole at $z = 1$" case considered above). Using Eq. (3.5) into Eq. (3.4) yields

$$\varpi = \sum_{i=1}^{\delta'} \mu_i e_i(1) \quad \text{with} \quad \mu_i = \sum_{\underline{n} \in \mathcal{N}} \lambda_1^{n_1} \cdot \ldots \cdot \lambda_N^{n_N} b_{\underline{n},i} \in \mathbb{Q}.$$

This enables us to apply the special case of Theorem 1 where $\mathbb{K} = \mathbb{Q}$, proved in Step 1, with N replaced with $\delta' \leq N^d$. Indeed we denote by $\alpha \in \mathbb{Z}$ a common positive denominator of the rational numbers $b_{\underline{n},i}$; then we have $\alpha\mu_1, \dots, \alpha\mu_{\delta'} \in \mathbb{Z}$. Since $\varpi \neq 0$ we obtain $|\alpha\varpi| > cH'^{-N^d+1-\varepsilon}$ where

$$H' = \max_{1 \leq i \leq \delta} |\alpha\mu_i| \leq \beta \max_{\underline{n} \in \mathcal{N}} \left|\lambda_1^{n_1} \cdot \ldots \cdot \lambda_N^{n_N}\right| \leq \beta H^d$$

where $\beta > 0$ depends only on $f_1, \dots, f_N$ and $\mathbb{K}$. Now Eq. (3.3) yields $|\varpi| \leq c' H^{d-1} |\Lambda|$ by bounding trivially the factors corresponding to all $\sigma \neq \mathrm{Id}$; here c' is a positive constant that depends only on $f_1, \dots, f_N$ and $\mathbb{K}$. Combining these estimates yields $|\Lambda| > c'' H^{-dN^d+1-d\varepsilon}$ for some constant c''; this concludes Step 2 in the case where $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$.

If $\mathbb{K}/\mathbb{Q}$ (of degree d) is not assumed to be Galois, we consider a finite Galois extension $\mathbb{L}$ of $\mathbb{Q}$ such that $\mathbb{K} \subset \mathbb{L}$. We let $G_0 = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ and $H = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. In the definition of ϖ, namely Eq. (3.3), the product is now taken over the d cosets $\sigma \in G_0/H$; indeed f_j^σ is the same for all σ in a given coset, because f_j has coefficients in $\mathbb{K}$. The same remark holds with Eq. (3.4). Then we have $\varphi_{\underline{n}}^\tau = \varphi_{\underline{n}}$ for any $\tau \in G_0$, so that $\varphi_{\underline{n}}$ has coefficients in $\mathbb{Q}$. The other parts of the proof of Step 2 remain unchanged.

Step 3. Let us conclude the proof of Theorem 1.

Let $(\omega_1, \dots, \omega_d)$ be a $\mathbb{Z}$-basis of $\mathcal{O}_\mathbb{K}$. Each λ_j may be written as $\sum_{t=1}^d \lambda_{j,t}\omega_t$ with $\lambda_{j,t} \in \mathbb{Z}$ such that $|\lambda_{j,t}| \leq c_1 \left|\overline{\lambda_j}\right| \leq c_1 H$, where c_1 depends only on $\mathbb{K}$ (see [13, Chapter 3, Lemma 12]). Then $\Lambda = \sum_{j=1}^N \sum_{t=1}^d \lambda_{j,t}\omega_t f_j(1)$, and the conclusion of Theorem 1 follows from the special case proved in Step 2, applied to the dN E-functions $\omega_t f_j(z)$ with $\lambda_{j,t} \in \mathbb{Z}$.

4 Decomposition of E-functions over a number field

In the same spirit as Proposition 2, it is possible to prove the following result. The weaker version with $\mathbb{K}$ replaced by $\overline{\mathbb{Q}}$ was first proved in the unpublished note [12], and the special case $\mathbb{K} = \mathbb{Q}$ in [5].

Proposition 3. *Let f be an E-function with coefficients in a number field $\mathbb{K}$. Then there exist polynomials $P, Q \in \mathbb{K}[z]$, and an E-function g with coefficients in $\mathbb{K}$, such that*

$$f(z) = P(z) + Q(z)g(z) \text{ and } g(z_0) \text{ is transcendental for any } z_0 \in \overline{\mathbb{Q}}^*.$$

In this setting, the non-zero algebraic numbers z at which a transcendental f takes an algebraic value are exactly the roots of Q. Moreover, replacing P with its remainder in its Euclidean division by Q, we may assume $\deg P < \deg Q$ provided $Q \neq 0$ (i.e., when f is not a polynomial); see [5, Proposition 3.3].

Proposition 3 is a generalization of the following result, which will be used in the proof. It is stated as [8, Theorem 4] and its proof is due to the referee of [7]:

Lemma 1. *Let f be an E-function with coefficients in a number field $\mathbb{K}$, and $\alpha \in \overline{\mathbb{Q}}$ be such that $f(\alpha)$ is algebraic. Then $f(\alpha) \in \mathbb{K}(\alpha)$.*

For the convenience of the reader, let us deduce this lemma from Proposition 1. Let $\beta = f(\alpha)$, and $\mathbb{L}$ be a finite Galois extension of $\mathbb{K}(\alpha)$ such that $\beta \in \mathbb{L}$. Since $f(z) - \beta$ vanishes at α, Proposition 1 shows that for any $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}(\alpha))$ the E-function $f(z) - \sigma(\beta) = f^\sigma(z) - \sigma(\beta)$ vanishes at $\sigma(\alpha) = \alpha$, so that $\sigma(\beta) = f(\alpha) = \beta$. This concludes the proof of Lemma 1.

Proof of Proposition 3. To prove Proposition 3, we first remark that the result is obvious if f is algebraic, hence a polynomial: we simply take $P = f$ and $Q = 0$. Let us now assume that f is transcendental. We argue by induction on the number of non-zero algebraic points α such that $f(\alpha) \in \overline{\mathbb{Q}}$; this number is finite because f is transcendental and of Beukers' theorem: any such α is a singularity of the first-order differential system satisfied by 1, f, f', $\ldots$, $f^{(\mu-1)}$ (where $\mu \geq 1$ is the minimal order of an inhomogeneous linear differential equation with coefficients in $\mathbb{K}(z)$ satisfied by f).

If this number is 0, one may choose $P = 0$ and $Q = 1$. Now if $f(\alpha) \in \overline{\mathbb{Q}}$, Lemma 1 proves that $f(\alpha)$ belongs to $\mathbb{K}(\alpha)$: there exists $P_0 \in \mathbb{K}[X]$ such that $f(\alpha) = P_0(\alpha)$. Therefore the E-function $f - P_0$, with coefficients in $\mathbb{K}$, vanishes at α. Proposition 1 yields an E-function g_0 with coefficients in $\mathbb{K}$ such that $f = P_0 + Dg_0$ where D is the minimal polynomial of α over $\mathbb{K}$. If $g_0(\alpha) \in \overline{\mathbb{Q}}$, the same procedure can be carried out with g_0, leading to $P_1 \in \mathbb{K}[z]$ and an E-function g_1 with coefficients in $\mathbb{K}$ such that $g_0 = P_1 + Dg_1$. After finitely many steps, this procedure terminates and provides g_ℓ such that $g_\ell(\alpha) \notin \overline{\mathbb{Q}}$ (see the proof of [5, Theorem 3.4]). This concludes the proof of Proposition 3. □

5 Structure of $\mathbf{E}_{\mathbb{K}}$

Let $\mathbb{K}$ be a subfield of $\overline{\mathbb{Q}}$. As in the introduction, we denote by $\mathbf{E}_{\mathbb{K}}$ the ring of all values $f(1)$ where f is an E-function with coefficients in $\mathbb{K}$; in particular $\mathbf{E}_{\overline{\mathbb{Q}}} = \mathbf{E}$.

The following result contains Theorem 2 stated in the introduction (as a special case $\mathbb{K} = \mathbb{Q}$).

Theorem 3. *Elements of $\mathbf{E}_{\mathbb{K}}$ are linearly independent over $\overline{\mathbb{Q}}$ if, and only if, they are linearly independent over $\mathbb{K}$. In other words, the $\mathbb{K}$-algebras $\mathbf{E}_{\mathbb{K}}$ and $\overline{\mathbb{Q}}$ are linearly disjoint, and the natural map $\mathbf{E}_{\mathbb{K}} \otimes_{\mathbb{K}} \overline{\mathbb{Q}} \to \mathbf{E}$ is a $\mathbb{K}$-algebra isomorphism.*

This result implies $\mathbf{E}_{\mathbb{K}} \cap \overline{\mathbb{Q}} = \mathbb{K}$, which is an equivalent form of Lemma 1 stated in §4.

Proof of Theorem 3. Let $f_1, \ldots, f_N$ be E-functions with coefficients in $\mathbb{K}$. If $f_1(1), \ldots, f_N(1)$ are linearly independent over $\overline{\mathbb{Q}}$, then obviously they are linearly independent over $\mathbb{K}$. Conversely, let us assume that they are linearly independent over $\mathbb{K}$. Let $\lambda_1, \ldots, \lambda_N$ be algebraic numbers, not all zero, such that $\lambda_1 f_1(1) + \ldots + \lambda_N f_N(1) = 0$. Up to a permutation of the indices we may assume that $\lambda_1 \neq 0$; then dividing by λ_1 we assume that $\lambda_1 = 1$. Let us consider a finite Galois extension $\mathbb{L}$ of $\mathbb{K}$ that contains $\lambda_2, \ldots, \lambda_N$. Then $g(z) = \sum_{i=1}^{N} \lambda_i f_i(z)$ is an E-function with coefficients in $\mathbb{L}$, and it vanishes at $z = 1$. For any $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, Proposition 1 yields $g^\sigma(1) = 0$, that is $\sum_{i=1}^{N} \sigma(\lambda_i) f_i(1) = 0$ since all f_i have coefficients in $\mathbb{K}$. Summing these relations, as σ varies, yields

$$\sum_{i=1}^{N} \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\lambda_i) f_i(1) = 0$$

with $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\lambda_i) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} \sigma(\lambda_i) \in \mathbb{K}$ and $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\lambda_1) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(1) = [\mathbb{L} : \mathbb{K}] \neq 0$. This is a non-trivial linear relation, with coefficients in $\mathbb{K}$, between $f_1(1), \ldots, f_N(1)$. This contradiction concludes the proof that elements of $\mathbf{E}_{\mathbb{K}}$ are linearly independent over $\overline{\mathbb{Q}}$ if, and only if, they are linearly independent over $\mathbb{K}$.

What remains of Theorem 3 follows directly from this property (see [3, Chapter V, §2, No. 5]). □

6 A Galois action on values of E-functions

In this section we define and study an action of the absolute Galois group of $\mathbb{Q}$, namely $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, on the set $\mathbf{E}$ of values of E-functions.

The definition is as follows: given $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\xi \in \mathbf{E}$, there exists an E-function f such that $\xi = f(1)$. Then we let $\sigma(\xi) = f^\sigma(1)$. The crucial point is to prove that $\sigma(\xi)$ depends only on σ and ξ, not on the choice of f. Indeed if g is another E-function such that $\xi = g(1)$, then $f - g$ vanishes at the point 1. Proposition 1 shows that $f^\sigma - g^\sigma$ vanishes at 1 too, so that $g^\sigma(1) = f^\sigma(1)$: this concludes the proof.

Proposition 4. *Let $\mathbb{K}$ be a number field, and $\xi \in \mathbf{E}$. Then ξ belongs to $\mathbf{E}_{\mathbb{K}}$ if, and only if, $\sigma(\xi) = \xi$ for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$.*

In other words, the fixed points of $\mathbf{E}$ under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ are exactly the elements of $\mathbf{E}_{\mathbb{K}}$.

Proof of Proposition 4. If $\xi \in \mathbf{E}_{\mathbb{K}}$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ then $\sigma(\xi) = \xi$ by definition, since $f^\sigma = f$ for any E-function f with coefficients in $\mathbb{K}$.

Now let $\xi \in \mathbf{E}$ be such that $\sigma(\xi) = \xi$ for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$. Let f be an E-function such that $f(1) = \xi$, and $\mathbb{L}$ denote a finite Galois extension of $\mathbb{K}$ that contains all coefficients of f. Let $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$; then σ is the restriction to $\mathbb{L}$ of an element, again denoted by σ, of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$. We have $\sigma(\xi) = \xi$ by assumption, and also $\sigma(\xi) = f^\sigma(1)$ by definition. Summing the identity $\xi = f^\sigma(1)$ over all σ yields $\xi = g(1)$ where $g(z) = \frac{1}{[\mathbb{L}:\mathbb{K}]} \sum_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} f^\sigma(z)$ is an E-function with coefficients in $\mathbb{K}$. Therefore $\xi \in \mathbf{E}_{\mathbb{K}}$; this concludes the proof of Proposition 4. □

This Galois action sheds a new light on the proof of Theorem 1 (see §3): it is very similar to Liouville's proof that irrational algebraic numbers are not too well approximated by rationals (i.e., are not Liouville numbers).

Indeed let us recall briefly Liouville's proof, stated in terms of Galois action. Let ξ be an algebraic number of degree $d \geq 2$, and assume (for simplicity) that the extension $\mathbb{Q}(\xi)/\mathbb{Q}$ is Galois. To bound from below $|q\xi - p|$ for $(p, q) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, consider

$$\varpi := \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})} \big(q\sigma(\xi) - p\big).$$

Then $\varpi \neq 0$ (since $\sigma(\xi)$ is irrational for any σ), and $\varpi \in \mathbb{Q}$ (since it is the norm of $q\xi - p$ with respect to the extension $\mathbb{Q}(\xi)/\mathbb{Q}$). Letting $\delta \in \mathbb{Z}$ denote a positive integer such that $\delta\xi$ is an algebraic integer, we have $\delta^d\varpi \in \mathbb{Z} \setminus \{0\}$ since $\mathcal{O}_{\mathbb{Q}(\xi)} \cap \mathbb{Q} = \mathbb{Z}$. Therefore $|\delta^d\varpi| \geq 1$ so that

$$\delta^{-d} \leq |\varpi| \leq |q\xi - p|(\boxed{\xi} + 1)^{d-1} H^{d-1}$$

by bounding $|q\sigma(\xi) - p|$ trivially for $\sigma \neq \mathrm{Id}$, where $H = \max(|p|, |q|)$. Dividing by q yields $|\xi - p/q| \geq cH^{-d}$ where $c > 0$ depends only on ξ.

Step 2 of the proof of Theorem 1 is very similar, except that elements of $\mathbb{K} \subset \overline{\mathbb{Q}}$ are replaced with values of E-functions in $\mathbf{E}_{\mathbb{K}}$; the lower bound used by Liouville (namely, $\delta^d\varpi \in \mathbb{Z} \setminus \{0\}$ implies $|\delta^d\varpi| \geq 1$) is replaced accordingly by Shidlovskii's lower bound recalled in Theorem A.

References

[1] Y. André, Séries Gevrey de type arithmétique I. Théorèmes de pureté et de dualité, *Annals of Math.* **151**.2 (2000), 705–740.

[2] Y. André, Solution algebras of differential equations and quasi-homogeneous varieties: a new differential Galois correspondence, *Ann. Sci. Éc. Norm. Supér.* **47**.2 (2014), 449—467.

[3] N. Bourbaki, Elements of Mathematics, Algebra II, Chapters 4–7, Springer, 2003.

[4] F. Beukers, A refined version of the Siegel-Shidlovskii theorem, *Annals of Math.* **163** (2006), 369–379.

[5] A. Bostan, T. Rivoal, B. Salvy, Minimization of differential equations and algebraic values of E-functions, preprint (2022), 37 pages.

[6] N. I. Feldman, Yu. V. Nesterenko, Transcendental Numbers, in *Encyclopaedia of Mathematical Sciences*, Vol. **44**: Number Theory IV (Springer, 1998).

[7] S. Fischler, T. Rivoal, On the values of G-functions, *Commentarii Math. Helv.* **89**.2 (2014), 313–341.

[8] S. Fischler, T. Rivoal, Arithmetic theory of E-operators, *Journal de l'École polytechnique – Mathématiques* **3** (2016), 31–65.

[9] S. Fischler, T. Rivoal, Microsolutions of differential operators and values of arithmetic Gevrey series, *American J. of Math.* **140.2** (2018), 317–348.

[10] G. Lepetit, Le théorème d'André-Chudnovsky-Katz au sens large, *North-West. Eur. J. Math.* **7** (2021), 83–149.

[11] Yu. V. Nesterenko, A. B. Shidlovskii, On the linear independence of values of E-functions, *Sb. Math.* **187** (1996), 1197–1211; translation from the russian *Math. Sb.* **187** (1996), 93–108.

[12] T. Rivoal, Valeurs algébriques de E-fonctions aux points algébriques, unpublished note (2016), 4 pages, available at `https://hal.archives-ouvertes.fr/hal-03676576`

[13] A. B. Shidlovskii, *Transcendental numbers*, de Gruyter Studies in Math., no. 12, de Gruyter, Berlin, 1989.

[14] C. Siegel, Über einige Anwendungen diophantischer Approximationen, vol. 1 S. *Abhandlungen Akad.*, Berlin, 1929.

[15] W. Zudilin, On rational approximations of values of a certain class of entire functions, *Sb. Math.* **186**.4, 555–590 (1995); translation from the russian *Mat. Sb.* **186**.4, 89–124 (1995).

S. Fischler, Université Paris-Saclay, CNRS, Laboratoire de mathématiques d'Orsay, 91405 Orsay, France.

T. Rivoal, Institut Fourier, CNRS et Université Grenoble Alpes, CS 40700, 38058 Grenoble cedex 9, France.

Keywords: E-functions, André-Beukers Theorems, Linear independence measures, Irrationality measures, Liouville numbers, Shidlovskii's Theorem.

MSC 2020: 11J82 (Primary), 11J91 (Secondary)