CRITERIA OF ALGEBRAIC INDEPENDENCE WITH MULTIPLICITIES AND INTERPOLATION DETERMINANTS

MICHEL LAURENT AND DAMIEN ROY

ABSTRACT. We generalize Gel'fond's criterion of algebraic independence by taking into account the values of the derivatives of the polynomials, and show how the new criterion applies to proving results of algebraic independence using interpolation determinants. We also establish a new result of approximation of a transcendental number by algebraic numbers of bounded degree and size. It contains an earlier result of E. Wirsing [13] and also a result announced by A. Durand in [2].

1. INTRODUCTION.

The problem of adapting the method of Interpolation Determinants to questions of algebraic independence has been open since 1989 (see [4]). Very recently, a solution has been proposed in [7] and [8]. It combines techniques introduced in [5] in the context of linear forms in logarithms, together with approximation results of complex numbers by algebraic numbers with large degree. In this paper, we propose another solution, in some sense more traditional, because it relies on a criterion of algebraic independence which is nevertheless of a new type. We shall restrict ourselves to problems of algebraic independence in transcendence degree 1, for which the standard tool is a criterion of Gel'fond (see for example [1]).

The principle of the method is very simple. Consider the interpolation determinant attached to a given situation of algebraic independence. Suppose that its entries belong to a field of transcendence degree 1 over $\mathbf{Q}$, say for simplicity a field of rational functions $\mathbf{Q}(\theta)$. The absolute value of such a determinant is in general small for analytic reasons. Viewing this determinant as a function of θ, the crucial point consists in the observation that its derivatives with respect to θ are also small in absolute value for similar reasons.

This leads us to a new criterion of algebraic independence analogous to Gel'fond's criterion but taking into account the values of the derivatives of the sequence of polynomials. We give two different proofs of this criterion of algebraic independence with multiplicities. The first proof uses the construction of algebraic approximations to θ, which is the basic step in [7] and [8]. The result that we need for our purposes is Proposition 2 below. It certainly has its own interest. This statement contains E. Wirsing's theorem [13], which was used in [7], and provides more flexibility by controlling the size of the algebraic approximations. Proposition 2 also contains a result of the same type announced by A. Durand in [2]. Our second proof is based on elimination techniques initiated by Gel'fond. We shall adapt his

1991 *Mathematics Subject Classification.* Primary 11J85; Secondary 11J04.

Second author partially supported by NSERC and CICMA

method to multiplicities. In this way, we obtain the same criterion (Proposition 1) with a much better numerical value of the constant γ involved.

The criterion of algebraic independence having been firmly established, we explain how to use it in the context of interpolation determinants, and show by an example that our method allows us to recover the known results in transcendence degree 1. More precisely, we provide in the last section a new proof of Gel'fond's theorem about the algebraic independence of the two numbers α^β and α^{β^2} when β is a cubic number and α an algebraic number $\neq 0, 1$. We felt the necessity to give a detailed proof of this very classical result, first of all because it indicates clearly the general ideas behind our method, and secondly because it emphasizes the generalized Wronskians obtained by differentiating interpolation determinants. Here we need only to establish elementary properties of these Wronskians to recover Gel'fond's theorem and more generally all the known results in transcendence degree 1. We hope that a deeper analysis of the involved Wronskians would lead to further progress in algebraic independence.

2. A version of Gel'fond's criterion with multiplicities.

Let us first fix some notations. The *size* of a polynomial $P \in \mathbf{C}[X]$ will be measured by the quantity

$$t(P) := \log H(P) + (\log 2) \deg P,$$

where $H(P)$ denotes the *height* of the polynomial P, that is the maximum of the absolute values of its coefficients. We also denote by $L(P)$ the *length* of the polynomial P, defined as the sum of the absolute values of its coefficients. If $\alpha \in \overline{\mathbf{Q}}$ is an algebraic number, we denote by $P_{(\alpha)}$ the irreducible polynomial of α over $\mathbf{Z}$, by $d(\alpha)$ its degree, by $M(\alpha)$ its Mahler measure, and by

$$t(\alpha) := t(P_{(\alpha)})$$

its size. In the sequel, we write $f^{(k)}$ to denote the k-th derivative of a function f divided by $k!$.

Proposition 1. *Let a, b be real numbers > 1, let $(s_n)_{n\in\mathbf{N}}$ be a sequence of positive integers, and let $(t_n)_{n\in\mathbf{N}}$ and $(d_n)_{n\in\mathbf{N}}$ be sequences of positive real numbers. Assume*

$$\frac{t_n}{s_n} \leq \frac{t_{n+1}}{s_{n+1}} \leq a\frac{t_n}{s_n}, \quad \frac{d_n}{s_n} \leq \frac{d_{n+1}}{s_{n+1}} \leq b\frac{d_n}{s_n}, \quad (n \in \mathbf{N})$$

and that the ratio t_n/s_n tends to infinity with n. Then there exists a constant $\gamma > 0$, depending only on a and b, which satisfies the following property. If there exists a complex number θ and a sequence $(P_n)_{n\in\mathbf{N}}$ of nonzero polynomials in $\mathbf{Z}[X]$ with

$$\deg P_n \leq d_n, \quad t(P_n) \leq t_n, \quad \max_{0\leq\sigma<s_n} |P_n^{(\sigma)}(\theta)| \leq e^{-\gamma d_n t_n/s_n}, \quad (n \in \mathbf{N}),$$

then $\theta \in \overline{\mathbf{Q}}$ (and $P_n(\theta) = 0$ for n sufficiently large).

The value of γ is explicit. Our first proof based on the construction of algebraic approximations of θ gives $\gamma = 3000 \max\{a, b\}$. The second one, which uses arguments from elimination theory, as in the standard proof of Gel'fond's theorem without multiplicities, improves this constant by giving $\gamma = 10(a + b + 1)$.

3. Preliminary Lemmas.

We shall use the following version of the classical lemma of Gel'fond on the size of a product of polynomials.

Lemma 1. *Let $Q_1, \dots, Q_n$ be polynomials in $\mathbf{C}[X]$, and let Q be their product. Then,*

$$t(Q) - (\log 2)\,\deg Q \;\le\; \sum_{\nu=1}^{n} t(Q_\nu) \;\le\; t(Q) + (\log 2)\,\deg Q, \tag{1}$$

$$L(Q) \;\le\; \prod_{\nu=1}^{n} L(Q_\nu) \;\le\; 2^{\deg Q} L(Q). \tag{2}$$

Proof. We essentially follow the proof by K. Mahler of Gel'fond's lemma which is based on the multiplicative property of Mahler measure. We also make use of the following inequalities of comparison (see for example the annex of Chapter 3 in [10]):

$$\frac{1}{\sqrt{d+1}} M(P) \le H(P) \le \binom{d}{[d/2]} M(P), \qquad M(P) \le L(P) \le 2^d M(P),$$

where d denotes the degree of the polynomial $P \in \mathbf{C}[X]$.

Put

$$d_\nu = \deg Q_\nu \quad \text{and} \quad d = \deg Q = \sum_{\nu=1}^{n} d_\nu.$$

The left inequality in (1) follows immediately from the elementary estimates

$$H(Q) \le \prod_{\nu=1}^{n} (d_\nu + 1) H(Q_\nu) \le \prod_{\nu=1}^{n} 2^{d_\nu} H(Q_\nu) = \exp\left(\sum_{\nu=1}^{n} t(Q_\nu)\right).$$

For the upper bound on the right, it suffices to observe that

$$\begin{aligned}
\sum_{\nu=1}^{n} \log H(Q_\nu) &\le \log\left(\prod_{\nu=1}^{n} \binom{d_\nu}{[d_\nu/2]} M(Q_\nu)\right) = \log\left(\prod_{\nu=1}^{n} \binom{d_\nu}{[d_\nu/2]}\right) + \log M(Q) \\
&\le \log\left(\sqrt{d+1} \prod_{\nu=1}^{n} \binom{d_\nu}{[d_\nu/2]}\right) + \log H(Q) \\
&\le d \log 2 + \log H(Q) = t(Q),
\end{aligned}$$

since

$$\prod_{\nu=1}^{n} \binom{d_\nu}{[d_\nu/2]} \le \binom{\sum d_\nu}{\sum [d_\nu/2]} \le \binom{d}{[d/2]}$$

and that $\binom{d}{[d/2]}\sqrt{d+1} \le 2^d$ for any integer $d \ge 1$. Note that the last upper bound is essentially optimal since the ratio $\binom{d}{[d/2]}\sqrt{d+1} \Big/ 2^d$ tends to $\sqrt{2/\pi}$ when d tends to infinity.

The second pair of inequalities (2) is proved in a similar way. □

Liouville's inequality takes the following form in terms of size and incidentally of length:

Lemma 2. *Let $P \in \mathbf{Z}[X]$ and $\alpha \in \overline{\mathbf{Q}}$ satisfy $P(\alpha) \neq 0$. Then,*

$$|P(\alpha)| \geq L(P) e^{-t(P)d(\alpha) - \deg(P)t(\alpha)}.$$

Lemma 3. *Let α and β be distinct algebraic numbers. Then,*

$$|\alpha - \beta| \geq 2e^{-d(\alpha)t(\beta) - d(\beta)t(\alpha)}.$$

Proof. Lemmas 2 and 3 are corollaries of Liouville's inequality expressed in terms of absolute height, whose statement is the following (cf. Lemma 3.14 of [10]). Let $\alpha_1, \dots, \alpha_n$ be algebraic numbers generating a number field of degree D over $\mathbf{Q}$, and let P be a polynomial in $\mathbf{Z}[X_1, \dots, X_n]$ such that $P(\alpha_1, \dots, \alpha_n) \neq 0$. Then we have the lower bound

$$\log |P(\alpha_1, \dots, \alpha_n)| \geq -(D-1) \log L(P) - D \left(\sum_{\nu=1}^{n} \deg_{X_\nu}(P) \frac{\log M(\alpha_\nu)}{d(\alpha_\nu)} \right).$$

To deduce Lemma 2 from this, it suffices to use the standard estimates

$$L(P) \leq (\deg(P) + 1) H(P) \leq e^{t(P)}, \quad M(\alpha) \leq \sqrt{d(\alpha) + 1}\, H(\alpha) \leq e^{t(\alpha)}.$$

To establish Lemma 3, apply the inequality to the polynomial $P(X, Y) = X - Y$ and bound $D = [\mathbf{Q}(\alpha, \beta) : \mathbf{Q}]$ from above by $d(\alpha)d(\beta)$. We obtain

$$\begin{aligned}
\log |\alpha - \beta| &\geq -\Big(d(\alpha)d(\beta) - 1 \Big) \log 2 - d(\beta) \log M(\alpha) - d(\alpha) \log M(\beta) \\
&\geq \log 2 - d(\beta) \left(\log H(\alpha) + d(\alpha) \frac{\log 2}{2} + \frac{\log(d(\alpha) + 1)}{2} \right) \\
&\qquad - d(\alpha) \left(\log H(\beta) + d(\beta) \frac{\log 2}{2} + \frac{\log(d(\beta) + 1)}{2} \right) \\
&\geq \log 2 - d(\beta)t(\alpha) - d(\alpha)t(\beta),
\end{aligned}$$

using $d(\alpha) + 1 \leq 2^{d(\alpha)}$, $d(\beta) + 1 \leq 2^{d(\beta)}$. □

4. Algebraic approximations to a complex number.

In this section, we generalize a result of approximation by algebraic numbers of bounded size due to Alain Durand [2]. Here, we separate size and degree.

Proposition 2. *Let $\theta \in \mathbf{C}$. For any pair of real numbers D, T verifying*

$$D \geq 50, \quad T \geq D \log 16 \quad \text{and} \quad T \geq 100 \log(4 + |\theta|),$$

there exists an algebraic number α such that

$$d(\alpha) \leq D, \quad t(\alpha) \leq T \quad \text{and} \quad |\theta - \alpha| \leq \exp\left(-\frac{t(\alpha)D + d(\alpha)T}{90} \right).$$

If this proposition is applied with $D = T/\log 16$ for the choice of a real number $T \geq 100\log(4+|\theta|)$, it ensures the existence of an algebraic number α of size $\leq T$ such that

$$|\theta - \alpha| \leq \exp\Big(-4\times 10^{-3} t(\alpha) T\Big).$$

Up to the value of the numerical constant, this is essentially the result of Alain Durand. Now, if the integer D is kept fixed with $D \geq 50$, if θ is chosen to be transcendental or algebraic of degree $> D$, and if we let T tend to infinity, Proposition 2 asserts the existence of infinitely many algebraic numbers α of degree $\leq D$ such that

$$|\theta - \alpha| \leq H(\alpha)^{-D/90}.$$

Results of this sort have been proved by E. Wirsing in [13]. In general, since we have $d(\alpha)\log 2 \leq t(\alpha)$ and since we require $T \geq D\log 16$, the two terms $t(\alpha)D$ and $d(\alpha)T$ which come into the upper bound for $|\theta-\alpha|$ cannot be compared a priori. The separation of size and degree thus allow more flexibility in the construction of algebraic approximations to θ.

The proof of Proposition 2 uses some lemmas. It relies on the existence of polynomials whose value at the point θ is small in terms of their degree and height:

Lemma 4. *Let $\theta \in \mathbf{C}$ and let D and H be positive real numbers with*

$$D \geq 50 \quad \textit{and} \quad \log H \geq 50\log(4+|\theta|).$$

Then there exists a nonzero polynomial $P(X) \in \mathbf{Z}[X]$ which satisfy

$$\deg P \leq D, \quad H(P) \leq H \quad \textit{and} \quad |P(\theta)| \leq \exp(-0.455 D\log H).$$

Proof. Let D_0 and H_0 be the integral parts of D and H respectively. For a polynomial $P \in \mathbf{R}[X]$ of degree $\leq D$, the real and imaginary parts of $P(\theta)$ are linear forms in the coefficients of P and, as such, the sum of the absolute values of their coefficients are $\leq (1+|\theta|+\cdots+|\theta|^{D_0})$. By virtue of Dirichlet box principle (cf. Lemma 1.3.2 of [11]), there exists therefore a nonzero polynomial $P \in \mathbf{Z}[X]$, of degree $\leq D$, of height $\leq H$, such that the real and imaginary parts of $P(\theta)$ are, in absolute value, bounded above by

$$(1+|\theta|+\cdots+|\theta|^{D_0})H_0^{-(D_0-1)/2}.$$

Since $D \geq 50$ and $\log H \geq 50\log(4+|\theta|)$, this implies, if $P(\theta)\neq 0$,

$$\log|P(\theta)| \leq \log\sqrt{2} + D\log(1+|\theta|) - \frac{1}{2}(D-2)\log(H-1) \leq -0.455 D\log H. \qquad \square$$

The next lemma provides an upper bound for the discriminant of a polynomial F, which takes into account the distance from θ to the set of zeros of F. Its proof is based on ideas of Wirsing in [13].

Lemma 5. *Let $\theta \in \mathbf{C}$, let d and s be positive integers with $s < d$, let $F \in \mathbf{C}[X]$ be a nonzero polynomial of degree d, and let ρ be the distance from θ to the set of zeros of F. Then we have*

$$\rho^{s(s+1)/2}|\mathrm{Disc}(F)|^{1/2} \le 2^{d(d-1)/2} M(F)^{d-s-1}|F(\theta)|^s,$$

where $\mathrm{Disc}(F)$ *denotes the discriminant of F.*

Proof. Write $F(X) = a_0X^d + \cdots + a_d$ with $a_0 \neq 0$, and order the roots $\alpha_1, \dots, \alpha_d$ of F so that the numbers $p_i = |\theta - \alpha_i|$, $(i = 1, \dots, d)$, which measure their distance to θ, satisfy

$$p_1 \le p_2 \le \cdots \le p_d.$$

Then, for each pair of integers (i, j) with $1 \le i < j \le d$, we obtain

$$|\alpha_i - \alpha_j| \le 2p_j.$$

We also have

$$|\alpha_i - \alpha_j| \le 2\max\{1, |\alpha_i|\}\max\{1, |\alpha_j|\}.$$

Using the first upper bound when $i \le s$ and the second when $i > s$, we find

$$\begin{aligned} |\mathrm{Disc}(F)|^{1/2} &= |a_0|^{d-1}\prod_{i<j}|\alpha_i - \alpha_j| \\ &\le 2^{d(d-1)/2}|a_0|^{d-1}\Big(\prod_{\substack{i<j \\ i\le s}} p_j\Big)\prod_{\substack{i<j \\ i>s}}\Big(\max\{1, |\alpha_i|\}\max\{1, |\alpha_j|\}\Big) \\ &= 2^{d(d-1)/2}|a_0|^{d-1}\Big(\prod_{j=1}^{s} p_j^{j-1}\Big)\Big(\prod_{j=s+1}^{d} p_j^{s}\Big)\prod_{j=s+1}^{d}\max\{1, |\alpha_j|\}^{d-s-1}. \end{aligned}$$

Since $\rho = p_1$, this implies

$$\begin{aligned} \rho^{s(s+1)/2}|\mathrm{Disc}(F)|^{1/2} &\le 2^{d(d-1)/2}\Big(|a_0|\prod_{j=1}^{d} p_j\Big)^{s}\Big(|a_0|\prod_{j=1}^{d}\max\{1, |\alpha_j|\}\Big)^{d-s-1} \\ &= 2^{d(d-1)/2}M(F)^{d-s-1}|F(\theta)|^s. \qquad \square \end{aligned}$$

In the case where F has integral coefficients and only simple roots, $|\mathrm{Disc}(F)|$ is a positive integer and so, is bounded below by 1. Then, choosing $s = d-1$ if $d \ge 2$, Lemma 5 yields:

Lemma 6. *Let θ be a complex number, d an integer ≥ 2, and $F \in \mathbf{Z}[X]$ a nonzero polynomial of degree d with integral coefficients, without multiple roots. Then the distance ρ from θ to the set of zeros of F satisfies*

$$\rho \le 2|F(\theta)|^{2/d}.$$

The next lemma allows, in the case of a polynomial with integral coefficients, to avoid the constraints $s < d$ and $d = \deg F$ which appear in Lemma 5.

Lemma 7. *Let θ be a complex number, let d and s be positive integers, and let $F \in \mathbf{Z}[X]$ be a nonzero polynomial of degree $\le d$ with integral coefficients, without multiple roots. Suppose $F(\theta) \neq 0$. Then the distance ρ from θ to the set of zeros of F satisfies*

$$\frac{s(s+1)}{2} \min\{0, \log \rho\} \le (d-1)t(F) + s \log |F(\theta)|.$$

Proof. We may assume $d = \deg F$ and $|F(\theta)| \le 1$, thus $\rho \le 1$. If $d = 1$, we find more precisely

$$\frac{s(s+1)}{2} \log \rho \le \frac{s(s+1)}{2} \log |F(\theta)| \le s \log |F(\theta)|.$$

Now, suppose $d \ge 2$. We consider two cases. If $s < d$, Lemma 5 gives, using $|\mathrm{Disc}(F)| \ge 1$,

$$\begin{aligned}\frac{s(s+1)}{2} \log \rho &\le \frac{\log 2}{2} d(d-1) + (d-1) \log M(F) + s \log |F(\theta)| \\ &\le (d-1)\Big(\frac{\log 2}{2} d + \frac{1}{2} \log(1+d) + \log H(F)\Big) + s \log |F(\theta)| \\ &\le (d-1)t(F) + s \log |F(\theta)|.\end{aligned}$$

If $s \ge d$, we define $k = s - d + 1$. Then Lemma 6 together with the inequality $\rho^d \le |F(\theta)| \le 1$ yields

$$\begin{aligned}\frac{s(s+1)}{2} \log \rho &\le \frac{d(d-1)}{2} \log \rho + dk \log \rho \\ &\le \frac{d(d-1)}{2} \log \Big(2|F(\theta)|^{2/d}\Big) + k \log |F(\theta)| \\ &\le \frac{\log 2}{2}(d-1)d + s \log |F(\theta)|. \qquad \square\end{aligned}$$

Proof of Proposition 2.

Let D and T be as in the statement of Proposition 2, and let H be the real number defined by the condition $T = \log H + D \log 4$. Since $T \ge D \log 16$, we get

$$\log H \ge T/2 \ge 50 \log(4 + |\theta|).$$

Let P be the polynomial supplied by Lemma 4 for this choice of D and H. We shall show that at least one of the roots α of P fulfills the requirements of the proposition. For this, we may assume that $P(\theta) \neq 0$. Put $c_1 = 0.455$. Since $\log H \ge T/2$ and $\deg(P) \le D$, we find

$$\begin{aligned}\log |P(\theta)| &\le -c_1 D \log H \\ &\le -\frac{c_1}{2} DT \\ &\le -\frac{c_1}{4}\Big(\deg(P)T + DT\Big).\end{aligned}$$

Write $P = mF_1 \cdots F_k$ where m is an integer and $F_1, \dots, F_k$ are non constant irreducible polynomials of $\mathbf{Z}[X]$. By Lemma 1, the sum of the sizes of $F_1, \dots, F_k$ is bounded above by

$$t(P) + \deg(P)\log 2 \le \log H + 2D\log 2 = T.$$

The preceding inequality therefore yields

$$\sum_{i=1}^{k} \log|F_i(\theta)| \le -\frac{c_1}{4} \sum_{i=1}^{k} \big(\deg(F_i)T + Dt(F_i)\big).$$

This implies that at least one of the irreducible factors F_i of P, call it F, satisfies

$$\log|F(\theta)| \le -\frac{c_1}{4}\big(\deg(F)T + t(F)D\big).$$

Let α be a root of F whose distance to θ is minimal. Lemma 7 applied to F gives, for any positive integer s,

$$\frac{s(s+1)}{2}\log|\theta - \alpha| \le d(\alpha)t(\alpha) + s\log|F(\theta)|.$$

Since $d(\alpha)$ is bounded above by D and, since by Lemma 1, $t(\alpha)$ is bounded above by T, we may write

$$d(\alpha)t(\alpha) \le \frac{1}{2}\big(d(\alpha)T + t(\alpha)D\big).$$

We deduce

$$\log|\theta - \alpha| \le -\frac{2}{s(s+1)}\Big(\frac{sc_1}{4} - \frac{1}{2}\Big)\big(d(\alpha)T + t(\alpha)D\big),$$

and the conclusion follows by taking $s = 9$. □

5. A first proof of Proposition 1.

We shall need two technical lemmas. The first shows that the constraint $T \ge 100\log(4 + |\theta|)$ which appears in the statement of Proposition 2 is necessary, up to the numerical factor 100. Recall that, given a polynomial $P \in \mathbf{C}[X]$, the notation $P^{(\sigma)}$ stands for the σ-th derivative of P divided by $\sigma!$.

Lemma 8. *Let $\theta \in \mathbf{C}$ and $\alpha \in \overline{\mathbf{Q}}$ be such that $|\theta - \alpha| \le 1$. Then we have*

$$\log(1 + |\theta|) < d(\alpha)\log 2 + t(\alpha).$$

Proof. If $|\theta| \le 3$, we find $\log(1 + |\theta|) < 2\log 2 \le d(\alpha)\log 2 + t(\alpha)$. Otherwise, we obtain $|\alpha| \ge |\theta| - 1 \ge (|\theta| + 1)/2$, thus

$$\log(1 + |\theta|) \le \log(2|\alpha|) \le \log 2 + \log M(\alpha) \le d(\alpha)\log 2 + t(\alpha). \qquad \square$$

Lemma 9. *Let s be a positive integer, and let d, t be positive real numbers. Suppose that there exists a complex number θ and a nonzero polynomial $P \in \mathbf{Z}[X]$ which satisfy*

$$\deg P \leq d, \quad t(P) \leq t \quad \textit{and} \quad \max_{0 \leq \sigma < s} |P^{(\sigma)}(\theta)| \leq e^{-3dt/s}.$$

Then we have $d \geq s$, $t \geq s \log 2$ and $d + t \geq s \log(1 + |\theta|)$.

Proof. Since $P^{(\sigma)}(\theta)$ is a nonzero integer when $\sigma = \deg P$, the conditions on P imply $\deg P \geq s$, thus $d \geq s$ and $t \geq s \log 2$. It remains to show $d + t \geq s \log(1 + |\theta|)$. To this end, we may assume $|\theta| \geq 1$. By truncating to the order s the Taylor expansion of P at the point θ, we get

$$P(X) = Q(X)(X - \theta)^s + \sum_{\sigma=0}^{s-1} P^{(\sigma)}(\theta)(X - \theta)^\sigma,$$

where $Q \in \mathbf{C}[X]$ has height ≥ 1. This implies

$$\begin{aligned}
L(P) &\geq L\big(Q(X)(X - \theta)^s\big) - \sum_{\sigma=0}^{s-1} |P^{(\sigma)}(\theta)| \; L\big((X - \theta)^\sigma\big) \\
&\geq 2^{-d} L(Q) L\big((X - \theta)^s\big) - e^{-3dt/s} \sum_{\sigma=0}^{s-1} L\big((X - \theta)^\sigma\big) \\
&\geq 2^{-d}(1 + |\theta|)^s - 8^{-d} \sum_{\sigma=0}^{s-1} (1 + |\theta|)^\sigma \\
&\geq 2^{-d}(1 + |\theta|)^s \left(1 - 4^{-d} \sum_{\sigma=1}^{s} \frac{1}{2^\sigma}\right) \\
&\geq \frac{3}{4} 2^{-d}(1 + |\theta|)^s,
\end{aligned}$$

thus $s \log(1 + |\theta|) \leq d \log 2 + \log L(P) + \log \frac{4}{3} \leq d + t$. □

The following lemma is the heart of our first proof of Proposition 1. It gives a precise formulation to the underlying principle that a polynomial with rational coefficients which is small, together with its derivatives, at some complex number θ, should be divisible by a large power of the minimal polynomial of some good algebraic approximation of θ.

Lemma 10. *Let s be a positive integer, let t and d be real numbers satisfying $t/\log 4 \geq d \geq s$, and let a be a real number ≥ 1. Suppose that there exists a complex number θ and a polynomial $P \in \mathbf{Z}[X]$ such that*

$$\deg P \leq d, \quad t(P) \leq t \quad \textit{and} \quad \max_{0 \leq \sigma < s} |P^{(\sigma)}(\theta)| \leq \exp\Big(- 1500a\frac{dt}{s}\Big).$$

Then there exists an algebraic number α which is a zero of each of the polynomials $P^{(\sigma)}$ with $0 \leq \sigma \leq s/2$, and which satisfies

$$d(\alpha) \leq \frac{2d}{s}, \quad t(\alpha) \leq \frac{4t}{s} \quad \textit{and} \quad |\theta - \alpha| \leq \exp\Big(- 8ad(\alpha)\frac{t}{s} - 4at(\alpha)\frac{d}{s}\Big).$$

Proof. Denote by $c = 90$ the numerical constant which appears in Proposition 2. Put

$$D = 4ac\frac{d}{s}\ , \quad T = 8ac\frac{t}{s}\ .$$

Since $t/\log 4 \geq d \geq s$, we find $D \geq 4c \geq 50$, $T \geq D\log 16$ and, by Lemma 9,

$$100\log(4+|\theta|) \leq 100(2+(d+t)/s) \leq 400t/s \leq T.$$

Proposition 2 then provides us with an algebraic number α such that $d(\alpha) \leq D$, $t(\alpha) \leq T$ and

$$|\theta-\alpha| \leq \exp\big(-c^{-1}\big(Td(\alpha)+Dt(\alpha)\big)\big) = \exp\left(-8ad(\alpha)\frac{t}{s} - 4at(\alpha)\frac{d}{s}\right).$$

We will show that α fulfills all the conditions of the lemma, starting with the fact that the polynomials $P^{(\sigma)}$ with $0 \leq \sigma \leq s/2$ vanish at that point.

Suppose, on the contrary, that there exists an integer σ with $0 \leq \sigma \leq s/2$ for which $P^{(\sigma)}(\alpha) \neq 0$. Put $Q = P^{(\sigma)}$. We use the Taylor expansion of Q around the point θ:

$$Q(\alpha) = \sum_{0\leq\tau<s/2} Q^{(\tau)}(\theta)(\alpha-\theta)^\tau + \sum_{\tau\geq s/2} Q^{(\tau)}(\theta)(\alpha-\theta)^\tau.$$

Let τ be an integer for which the product $Q^{(\tau)}(\theta)(\alpha-\theta)^\tau$ has largest absolute value. We have:

$$\log|Q(\alpha)| \leq \log(d+1) + \log|Q^{(\tau)}(\theta)(\alpha-\theta)^\tau|.$$

If $\tau < s/2$, the factor $Q^{(\tau)}(\theta)$ is small. Since $|\alpha-\theta| \leq 1$, we obtain in this case

$$\begin{aligned}
\log|Q(\alpha)| &\leq \log(d+1) + \log\binom{\sigma+\tau}{\tau} + \log|P^{(\sigma+\tau)}(\theta)| \\
&\leq \log(d+1) + s\log 2 - 1500a\frac{dt}{s} \\
&\leq -16ac\frac{dt}{s} \\
&= -(2Dt+Td) \\
&\leq -\big(2d(\alpha)t + t(\alpha)d\big).
\end{aligned}$$

Else, if τ is $\geq s/2$, we have $\alpha \neq \theta$, and the factor $(\alpha-\theta)^\tau$ becomes small, although nonzero. Using $\deg Q \leq d$ and the fact that, by Lemma 8, $\log(1+|\theta|)$ is bounded above by $d(\alpha)\log 2 + t(\alpha)$, we obtain

$$\begin{aligned}
\log|Q(\alpha)| &\leq \log(d+1) + \log|Q^{(\tau)}(\theta)| + \frac{s}{2}\log|\alpha-\theta| \\
&\leq \log(d+1) + \log L(Q) + \deg(Q)\log(1+|\theta|) + \frac{s}{2}\log|\alpha-\theta| \\
&\leq \log(d+1) + \log L(Q) + d\Big(d(\alpha)\log 2 + t(\alpha)\Big) - 4ad(\alpha)t - 2at(\alpha)d \\
&\leq \log L(Q) - \big(2d(\alpha)t + t(\alpha)d\big)
\end{aligned}$$

(given that $\log(d+1) \le d\log 2$ is $\le t$, and that $a \ge 1$). This last inequality therefore holds in both cases. On the other hand, it is clear that

$$t(Q) \le t(P) + d\log 2 \le \frac{3}{2}t < 2t.$$

So, Lemma 2 gives

$$\begin{aligned}\log|Q(\alpha)| &\ge \log L(Q) - d(\alpha)t(Q) - t(\alpha)\deg(Q)\\ &> \log L(Q) - \big(2d(\alpha)t + t(\alpha)d\big),\end{aligned}$$

which contradicts the upper bound for $\log|Q(\alpha)|$ previously established.

It follows that $P^{(\sigma)}(\alpha) = 0$ for $0 \le \sigma \le s/2$. If u denotes the smallest integer $> s/2$, the polynomial P is therefore divisible by $(P_{(\alpha)})^u$, where $P_{(\alpha)}$ stands for the irreducible polynomial of α over $\mathbf{Z}$. By Lemma 1, we then have

$$d \ge ud(\alpha) \ge \frac{s}{2}d(\alpha), \quad t \ge t(P) \ge \frac{u}{2}t(\alpha) \ge \frac{s}{4}t(\alpha).$$

This establishes the upper bounds

$$d(\alpha) \le 2\frac{d}{s}, \quad t(\alpha) \le 4\frac{t}{s},$$

which refine the initial estimates $d(\alpha) \le D$, $t(\alpha) \le T$. □

Proof of Proposition 1.

Suppose the existence of a number θ and a sequence of polynomials $(P_n)_{n\in\mathbf{N}}$ satisfying the hypotheses of Proposition 1 with $\gamma = 3000\max\{a,b\}$. By replacing a and b by $\max\{a,b\}$ if necessary, we may assume $a = b$. Lemma 9 shows that $d_n \ge s_n$ and that $t_n \ge s_n \log 2$ for any $n \in \mathbf{N}$. Consider the two sequences $(d'_n)_{n\in\mathbf{N}}$ and $(t'_n)_{n\in\mathbf{N}}$ given by

$$d'_n = \min\{d_n, t_n/\log 2\}, \quad t'_n = 2t_n.$$

For any $n \in \mathbf{N}$, they satisfy $s_n \le d'_n \le t'_n/\log 4$,

$$\frac{d'_n}{s_n} \le \frac{d'_{n+1}}{s_{n+1}} \le a\frac{d'_n}{s_n}, \quad \frac{t'_n}{s_n} \le \frac{t'_{n+1}}{s_{n+1}} \le a\frac{t'_n}{s_n},$$

as well as $\deg P_n \le d'_n, t(P_n) \le t'_n$ and

$$\max_{0\le\sigma<s_n} |P^{(\sigma)}(\theta)| \le e^{-\gamma' d'_n t'_n/s_n},$$

where $\gamma' = \gamma/2$. Thus, by replacing the sequence $(d_n)_{n\in\mathbf{N}}$ and $(t_n)_{n\in\mathbf{N}}$ with $(d'_n)_{n\in\mathbf{N}}$ and $(t'_n)_{n\in\mathbf{N}}$, we may assume, at the cost of dividing γ by 2, that we have $s_n \le d_n \le t_n/\log 4$ for any $n \in \mathbf{N}$.

Now for each integer $n \in \mathbf{N}$, Lemma 10 provides us with an approximation α_n of θ which satisfies the estimates

$$d(\alpha_n) \le 2\frac{d_n}{s_n}, \quad t(\alpha_n) \le 4\frac{t_n}{s_n}, \quad |\theta - \alpha_n| \le \exp\left(-8ad(\alpha_n)\frac{t_n}{s_n} - 4at(\alpha_n)\frac{d_n}{s_n}\right),$$

and the condition $P_n^{(\sigma)}(\alpha_n) = 0$ for each integer σ in the interval $0 \le \sigma \le s_n/2$. Since t_n/s_n tends to infinity with n, the sequence $(\alpha_n)_{n\in\mathbf{N}}$ converges to θ. We will show that this sequence is constant. This will imply that θ is algebraic and satisfies $P_n^{(\sigma)}(\theta) = 0$ for any pair of integers (n, σ) with $n \in \mathbf{N}$ and $0 \le \sigma \le s_n/2$.

Suppose on the contrary that there exists an integer n such that $\alpha_n \neq \alpha_{n+1}$. If $|\alpha_n - \theta| \ge |\alpha_{n+1} - \theta|$, we find

$$\begin{aligned}\log|\alpha_n - \alpha_{n+1}| &\le \log 2 + \log|\alpha_n - \theta| \\ &\le \log 2 - 8ad(\alpha_n)\frac{t_n}{s_n} - 4at(\alpha_n)\frac{d_n}{s_n} \\ &\le \log 2 - 8d(\alpha_n)\frac{t_{n+1}}{s_{n+1}} - 4t(\alpha_n)\frac{d_{n+1}}{s_{n+1}} \\ &\le \log 2 - 2d(\alpha_n)t(\alpha_{n+1}) - 2t(\alpha_n)d(\alpha_{n+1}).\end{aligned}$$

Otherwise, we obtain

$$\begin{aligned}\log|\alpha_n - \alpha_{n+1}| &\le \log 2 + \log|\alpha_{n+1} - \theta| \\ &\le \log 2 - 8ad(\alpha_{n+1})\frac{t_{n+1}}{s_{n+1}} - 4at(\alpha_{n+1})\frac{d_{n+1}}{s_{n+1}} \\ &\le \log 2 - 8d(\alpha_{n+1})\frac{t_n}{s_n} - 4t(\alpha_{n+1})\frac{d_n}{s_n} \\ &\le \log 2 - 2d(\alpha_{n+1})t(\alpha_n) - 2t(\alpha_{n+1})d(\alpha_n).\end{aligned}$$

In both cases, this inequality contradicts Liouville's inequality in its form given in Lemma 3. So, the sequence $(\alpha_n)_{n\in\mathbf{N}}$ is constant, and the proof is complete. □

6. Multiplicities and resultants.

We now turn to an alternative proof of Proposition 1 which is based on arguments from elimination theory as the usual proof of Gel'fond's criterion. This second proof provides a smaller numerical value for the constant γ. In practice, the precise value of this constant does not matter much, but the arguments developed in this approach seem sufficiently different from the preceding ones to justify a new proof. We shall now use the resultant in the form of a determinant, while it appeared in section 4 in the form of a product of differences of roots.

We set in this section the tools of elimination which we shall need in the new proof of Proposition 1. Recall that we use divided derivatives (see §1).

Lemma 11. *Let u be an integer ≥ 0 and let P be a nonzero polynomial of $\mathbf{C}[X]$. A greatest common divisor of the polynomials $P^{(\sigma)}$, $(0 \le \sigma \le u)$, is given by the product*

$$\prod_{\substack{i \\ \mu_i > u}} (X - \alpha_i)^{\mu_i - u}$$

where α_i runs through the set of roots of P and where μ_i denotes the multiplicity of α_i as a zero of P.

Proof. By localization, we reduce to the case where P is a power of $X - \alpha$ for some $\alpha \in \mathbf{C}$, in which case the result is clear. □

The following result is a version of a classical lemma used in commutative algebra and in questions of zero estimates.

Lemma 12. *Let $(P_\sigma)_{\sigma\in\mathcal{E}}$ be a finite set of polynomials of $\mathbf{C}[X]$, not all zero, of degree $\le d$, where d is a real number ≥ 1. Let Q be their greatest common divisor. For any nonzero linear combination F of the polynomials $(P_\sigma)_{\sigma\in\mathcal{E}}$, there exist integers g_σ, with $0\le g_\sigma\le d$, such that Q is a greatest common divisor of the two polynomials F and $G := \sum_{\sigma\in\mathcal{E}} g_\sigma P_\sigma$.*

Proof. Write $P_\sigma = QQ_\sigma$. The polynomials Q_σ, $(\sigma\in\mathcal{E})$, are relatively prime. It suffices therefore to impose the conditions

$$\sum_{\sigma\in\mathcal{E}} g_\sigma Q_\sigma(\theta_i) \neq 0, \quad (1\le i\le \delta),$$

where $\theta_1,\dots,\theta_\delta$ denote the distinct roots of F. But, the polynomial

$$\prod_{i=1}^{\delta}\left(\sum_{\sigma\in\mathcal{E}} Y_\sigma Q_\sigma(\theta_i)\right) \in \mathbf{C}[Y_\sigma]_{\sigma\in\mathcal{E}}$$

is not identically zero and has degree $\le\delta\le d$ in each of the variables Y_σ. It is therefore possible to specialize these variables to integers g_σ with $0\le g_\sigma\le d$, in such a way that the value of this polynomial is nonzero. □

We now come to the argument of elimination which is the key of our proposition. We state it in terms of the usual resultant $\mathrm{Res}(F,G)$ of two polynomials F and G of $\mathbf{C}[X]$, although the notion implicitly used is the sub-resultant (see for example [3]).

Lemma 13. *Let F and G be nonzero polynomials of $\mathbf{C}[X]$ both divisible by a polynomial Q of $\mathbf{C}[X]$. Denote by m and n the respective degrees of F/Q and G/Q. Then, for any complex number θ and any integer v with $1\le v\le m+n$, we have the estimate*

$$\begin{aligned}|Q(\theta)|^v \times \left|\mathrm{Res}\Big(\frac{F}{Q},\frac{G}{Q}\Big)\right| \le 2^{v(m+n)} \max_{0\le\tau<v}\max\Big\{|F^{(\tau)}(\theta)|, |G^{(\tau)}(\theta)|\Big\}^v \\ \times \max\Big\{1, L\Big(\frac{F}{Q}\Big)\Big\}^n \max\Big\{1, L\Big(\frac{G}{Q}\Big)\Big\}^m .\end{aligned}$$

Moreover, if $|\mathrm{Res}(F/Q,G/Q)|\ge 1$, this inequality holds for any integer $v\ge 1$, without restriction.

Proof. Write $A = F/Q = \sum_{i=0}^m a_iX^i$ and $B = G/Q = \sum_{i=0}^n b_iX^i$, and fix a positive integer v. The number $\mathrm{Res}(A,B)$ is the determinant of the square matrix of order $m+n$

$$\begin{pmatrix} a_0 & a_1 & \dots & a_m & & \\ 0 & \ddots & & & \ddots & 0 \\ & & a_0 & a_1 & \dots & a_m \\ b_0 & b_1 & \dots & b_n & & \\ 0 & \ddots & & & \ddots & 0 \\ & & b_0 & b_1 & \dots & b_n \end{pmatrix}$$

whose rows consist of the coefficients of the polynomials

$$A, XA, \dots, X^{n-1}A,\ B, XB, \dots, X^{m-1}B,$$

written as linear combinations of $1, X, \dots, X^{m+n-1}$. Consider the sequence of polynomials $(C_i)_{i\geq 1}$ defined by

$$C_i(X) = \begin{cases} (X-\theta)^{i-1} & \text{if } i \leq v \\ (X-\theta)^v X^{i-v-1} & \text{if } i > v. \end{cases}$$

For each integer $k \geq 1$, the set $\{C_1, \dots, C_k\}$ constitutes a basis of the vector space E_k of polynomials of $\mathbf{C}[X]$ of degree $< k$. The transition matrix between this basis of E_k and its standard basis $\{1, X, \dots, X^{k-1}\}$ has determinant 1. Therefore, since the determinant of a matrix is not affected by row operations with determinant 1, we deduce that $\mathrm{Res}(A, B)$ is also equal to the determinant of the square matrix of order $m+n$ whose rows are made up by the coefficients of the polynomials

$$C_1A, C_2A, \dots, C_nA, C_1B, C_2B, \dots, C_mB. \tag{3}$$

First assume $v < m+n$ and $|\theta| \leq 1$, and consider the linear maps φ and ψ from E_{m+n} to $\mathbf{C}^{m+n}$ given by

$$\varphi(P) = \big((QP)(\theta), (QP)'(\theta), \dots, (QP)^{(v-1)}(\theta), \\ P^{(v)}(0), P^{(v+1)}(0), \dots, P^{(m+n-1)}(0)\big)$$

and

$$\psi(P) = \big(P(\theta), P'(\theta), \dots, P^{(v-1)}(\theta),\ P^{(v)}(0), P^{(v+1)}(0), \dots, P^{(m+n-1)}(0)\big)$$

for any $P \in E_{m+n}$. The formula

$$\begin{aligned} (QP)^{(j)}(\theta) &= \sum_{i=0}^{j} Q^{(i)}(\theta) P^{(j-i)}(\theta) \\ &= Q(\theta)P^{(j)}(\theta) + \begin{pmatrix} \text{linear combination of } P(\theta), \dots, P^{(j-1)}(\theta) \text{ where} \\ \text{the coefficients depend only on } Q \text{ and } \theta \end{pmatrix} \end{aligned}$$

shows that

$$\det[\varphi] = Q(\theta)^v \det[\psi],$$

where $[\varphi]$ and $[\psi]$ denote respectively the matrices of φ and ψ relative to the usual basis $\{1, X, \dots, X^{m+n-1}\}$ of E_{m+n} and to the canonical basis of $\mathbf{C}^{m+n}$. Since $[\psi]$ is a triangular matrix with 1 everywhere on the diagonal, we also have $\det[\psi] = 1$. So, we obtain $\det[\varphi] = Q(\theta)^v$. Since $\mathrm{Res}(A, B)$ is the determinant of the matrix whose rows are the coordinates of the polynomials of (3) in the above basis of E_{m+n}, we deduce that

$$|Q(\theta)|^v\, |\mathrm{Res}(A, B)| = |\det M|,$$

where M is the square matrix of order $m+n$ whose rows are the images under φ of the polynomials of the family (3).

For a positive integer $i \le v$, the first v coordinates of $\varphi(C_iA)$ are

$$0, \dots, 0, F(\theta), F'(\theta), \dots, F^{(v-i)}(\theta)$$

and those of $\varphi(C_iB)$ are

$$0, \dots, 0, G(\theta), G'(\theta), \dots, G^{(v-i)}(\theta).$$

These coordinates vanish if $i > v$. It follows that, for each of the first v columns of M, the sum of the absolute values of its coefficients, its *length*, is bounded above by

$$2v \max_{0 \le \tau < v} \max\left\{ |F^{(\tau)}(\theta)|, |G^{(\tau)}(\theta)| \right\}.$$

Furthermore, for each positive integer $i \le m+n$ and each polynomial P of degree $\le m+n-i$, the last $m+n-v$ coordinates of $\varphi(C_iP)$ are simply the last $m+n-v$ coefficients of the polynomial C_iP written as a linear combination of $1, X, \dots, X^{m+n-1}$. The sum of the absolute values of these coordinates is thus bounded above by

$$(1+|\theta|)^v L(P) \le 2^v L(P).$$

Put $u = m+n-v$. We estimate $|\det M|$ using Laplace formula by writing the determinant of M as the sum of the products of the minors of order v taken from the first v columns of M multiplied by their complementary minors of order u taken from the last u columns, with the appropriate choice of signs. The absolute value of each of the minors of order u is bounded above by the product of the lengths of its row vectors. A crude upper bound for this product is

$$2^{uv} \max\{1, L(A)\}^n \max\{1, L(B)\}^m.$$

On the other hand, the sum of the absolute values of the minors of order v taken from the first v columns of M is bounded above by the product of the lengths of these v columns. So, it is bounded above by

$$\left(2v \max_{0 \le \tau < v} \max\left\{ |F^{(\tau)}(\theta)|, |G^{(\tau)}(\theta)| \right\}\right)^v. \tag{4}$$

Since $2v \le 2^v$, we get

$$|\det M| \le 2^{(m+n)v} \left(\max_{0 \le \tau < v} \max\left\{ |F^{(\tau)}(\theta)|, |G^{(\tau)}(\theta)| \right\}\right)^v \times \max\{1, L(A)\}^n \max\{1, L(B)\}^m,$$

which proves the inequality of the lemma in the case $v < m+n$ and $|\theta| \le 1$.

To handle the case where $v < m+n$ and $|\theta| \ge 1$, replace φ and ψ by the linear maps $\tilde{\varphi}$ and $\tilde{\psi}$ from E_{m+n} to $\mathbf{C}^{m+n}$ given by

$$\tilde{\varphi}(P) = \big((QP)(\theta), (QP)'(\theta), \dots, (QP)^{(v-1)}(\theta),\ P(0), P'(0), \dots, P^{(u-1)}(0)\big)$$
$$\tilde{\psi}(P) = \big(P(\theta), P'(\theta), \dots, P^{(v-1)}(\theta),\ P(0), P'(0), \dots, P^{(u-1)}(0)\big)$$

where, as before, u stands for $m+n-v$. We still have

$$\det[\tilde{\varphi}] = Q(\theta)^v \det[\tilde{\psi}],$$

but the matrix $[\tilde{\psi}]$ is no longer triangular. Nevertheless, its determinant $\det[\tilde{\psi}]$ is the same as the determinant of the matrix of $\tilde{\psi}$ relative to the basis $\{C_1, \dots, C_{m+n}\}$ of E_{m+n} and to the canonical basis of $\mathbf{C}^{m+n}$. Since the latter matrix is triangular with diagonal

$$(\underbrace{1, \dots, 1}_{v \text{ times}}, \underbrace{(-\theta)^v, \dots, (-\theta)^v}_{u \text{ times}}),$$

we get $\det[\tilde{\psi}] = \pm\theta^{uv}$. So, we have $\det[\tilde{\varphi}] = \pm\theta^{uv} Q(\theta)^v$ and, if we denote by $\tilde{M}$ the matrix of order $m+n$ whose rows are the images under $\tilde{\varphi}$ of the polynomials of the family (3), we obtain as above

$$|\theta|^{uv}\, |Q(\theta)|^v\, |\mathrm{Res}(A,B)| = |\det \tilde{M}|.$$

By construction, the first v columns of $\tilde{M}$ coincide with those of M. So, the sum of the absolute values of the minors of order v taken from the first v columns of $\tilde{M}$ is bounded above by (4). Moreover, for any positive integer $i \le m+n$ and any polynomial P of degree $\le m+n-i$, the last u coordinates of $\tilde{\varphi}(C_i P)$ coincide with the first u coefficients of $C_i P$ written as a linear combination of $1, X, \dots, X^{m+n-1}$. The sum of the absolute values of these coordinates is therefore bounded above by

$$(1+|\theta|)^v L(P) \le 2^v |\theta|^v L(P),$$

and each of the minors of order u taken from the last u columns of $\tilde{M}$ has absolute value at most

$$2^{uv} |\theta|^{uv} \max\{1, L(A)\}^n \max\{1, L(B)\}^m.$$

We deduce

$$\begin{aligned} |\det \tilde{M}| \le 2^{(m+n)v} |\theta|^{uv} \Big(\max_{0 \le \tau < v} \max \Big\{ |F^{(\tau)}(\theta)|, |G^{(\tau)}(\theta)| \Big\} \Big)^v \\ \times \max\{1, L(A)\}^n \max\{1, L(B)\}^m, \end{aligned}$$

which gives the inequality of the lemma in the case $v < m+n$ and $|\theta| \ge 1$.

The lemma is thus proved for any value of θ if $v < m+n$. When $v = m+n$, the computations are simpler. We find, independently of θ,

$$\begin{aligned} |Q(\theta)|^{m+n}\, |\mathrm{Res}(A,B)| &= |\det M| \\ &\le 2^{(m+n)^2} \Big(\max_{0 \le \tau < v} \max \Big\{ |F^{(\tau)}(\theta)|, |G^{(\tau)}(\theta)| \Big\} \Big)^{m+n}, \end{aligned}$$

and the lemma is again verified. If $|\mathrm{Res}(A,B)| \ge 1$, this implies

$$|Q(\theta)|^v\, |\mathrm{Res}(A,B)| \le 2^{(m+n)v} \Big(\max_{0 \le \tau < v} \max \Big\{ |F^{(\tau)}(\theta)|, |G^{(\tau)}(\theta)| \Big\} \Big)^v$$

for any $v \ge m+n$. So, in this case, the inequality of the lemma holds for any $v \ge 1$. □

By taking derivatives, we shall construct a sequence of polynomials to which we shall apply the usual Gel'fond's lemma. Here, is a version of this lemma:

Lemma 14. *Let a and b be real numbers ≥ 1, and let $(t_n)_{n\in\mathbf{N}}$ and $(d_n)_{n\in\mathbf{N}}$ be sequences of positive real numbers such that*

$$t_n \leq t_{n+1} \leq a t_n, \quad d_n \leq d_{n+1} \leq b d_n, \quad (n \in \mathbf{N}).$$

Moreover, assume that t_n tends to infinity with n. Let $\theta \in \mathbf{C}$ and let γ be a real number $> a+b+1$. If there exist a sequence $(P_n)_{n\in\mathbf{N}}$ of nonzero polynomials in $\mathbf{Z}[X]$ satisfying

$$\deg P_n \leq d_n, \quad t(P_n) \leq t_n, \quad |P_n(\theta)| \leq e^{-\gamma d_n t_n}, \quad (n \in \mathbf{N}),$$

then $\theta \in \overline{\mathbf{Q}}$ (and $P_n(\theta) = 0$ for each n sufficiently large).

Proof. This is essentially Theorem 1 of [1]. See also the criterion 2.4 in [12], expressed in terms of size, with an arbitrary sequence $(t_n)_{n\in\mathbf{N}}$. There are however few minor differences with these two references. In [1], the hypotheses include a sequence $(\gamma_n)_{n\in\mathbf{N}}$ of upper bounds for the logarithmic heights of the polynomials P_n. It satisfies a moderated growth condition as above but, in fact, only upper bounds t_n for the sequence $\log H(P_n) + \deg P_n \leq \gamma_n + d_n$ enter into the estimates. This suggests to use size and degree instead of height and degree, in these questions. Moreover, we may replace the size $\log H(P) + \deg P$ used in [12] by the quantity $t(P) = \log H(P) + (\log 2)\deg P$ considered here. When the sequence $(d_n)_{n\in\mathbf{N}}$ is bounded, the notion of size which is used does not matter really because we request the strict inequality $\gamma > a+b+1$, while it is possible asymptotically to substitute $t_n = \gamma_n + d_n \log 2$ for $\gamma_n + d_n$ in all height estimates when the sequence $(d_n)_{n\in\mathbf{N}}$ tends to infinity. For example, in Lemma 1 above, which is one of the main tools of the proof, the correction factor which appears is $2^{\deg P}$. The factor $e^{\deg P}$ is used in [1] instead of $2^{\deg P}$ in order to compensate for other terms which become asymptotically negligible.

Note that $t(P)$ is essentially the logarithm of the quantity $\Lambda(P) = 2^{\deg P} L(P)$ used by A. Durand in [2] to measure the size of the polynomial P. ☐

7. A second proof of Proposition 1.

Suppose that there exists a complex number θ and a sequence of polynomials $(P_n)_{n\in\mathbf{N}}$ as in the statement of Proposition 1, with a constant $\gamma \geq 10(a+b+1)$. We will show that, for any integer n sufficiently large, there exists a factor $\tilde{P}_n$ of P_n in $\mathbf{Z}[X]$ which satisfies

$$\deg \tilde{P}_n \leq \frac{2d_n}{s_n}, \quad t(\tilde{P}_n) \leq \frac{4t_n}{s_n} \quad \text{and} \quad |\tilde{P}_n(\theta)| \leq \exp\Big(-\frac{5\gamma d_n t_n}{6 s_n^2}\Big).$$

If we accept this result for the moment, Lemma 14 shows that θ is algebraic and is a zero of each of the polynomials $\tilde{P}_n$ for n large enough. Since $\tilde{P}_n$ divides P_n, this implies $P_n(\theta) = 0$ for the same values of n.

So, fix an integer n arbitrarily large and, for simplicity, let us omit the index n. Set

$$P = P_n, \quad s = s_n, \quad t = t_n \quad \text{and} \quad d = d_n.$$

Let u be the integral part of $s/2$, and let $v = s - u$. Write

$$P = m \prod_i Q_i^{\mu_i}$$

for the prime decomposition in $\mathbf{Z}[X]$ of the polynomial P, and define

$$\tilde{P} := \prod_{\substack{\mu_i > u \\ |Q_i(\theta)| \le 1}} Q_i^{[\mu_i/(u+1)]}.$$

Since $\tilde{P}^{u+1}$ divides P, Lemma 1 gives

$$\deg \tilde{P} \le \frac{d}{u+1} \le \frac{2d}{s}, \quad t(\tilde{P}) \le \frac{2t}{u+1} \le \frac{4t}{s},$$

because $u+1 \ge s/2$. It remains to estimate $|\tilde{P}(\theta)|$. To this end, consider the gcd of the polynomials $P^{(\sigma)}(X)$, with $0 \le \sigma \le u$. Lemma 11 shows that it is equal to the product

$$Q := \prod_{\substack{i \\ \mu_i > u}} Q_i^{\mu_i - u}.$$

Since any integer $\mu > u$ satisfies

$$\left[\frac{\mu}{u+1}\right](u+1) \ge \mu - u,$$

we can write

$$|\tilde{P}(\theta)|^{u+1} \le \prod_{\substack{\mu_i > u \\ |Q_i(\theta)| \le 1}} |Q_i(\theta)|^{\mu_i - u} \le |Q(\theta)|.$$

The problem thus reduces to estimating $|Q(\theta)|$. Note that we necessarily have $d \ge \deg P \ge 1$ since P is a nonzero polynomial with integer coefficients such that $|P(\theta)| < 1$. Lemma 12 then provides us with a linear combination

$$G = \sum_{\sigma \le u} g_\sigma P^{(\sigma)},$$

such that the gcd of P and G is precisely Q. The estimates $0 \le g_\sigma \le \deg P$ show that, for any integer τ with $0 \le \tau < v$, we have

$$\begin{aligned} |G^{(\tau)}(\theta)| \le \sum_{\sigma=0}^{u} \binom{\sigma+\tau}{\tau} g_\sigma |P^{(\sigma+\tau)}(\theta)| &= \sum_{\sigma=\tau}^{\min(\deg P, \tau+u)} \binom{\sigma}{\tau} g_{\sigma-\tau} |P^{(\sigma)}(\theta)| \\ &\le \exp\Big(-\frac{\gamma dt}{s} + \mathcal{O}(d)\Big). \end{aligned}$$

The second inequality is obtained simply using $\deg P \le d$ and observing that

$$\sum_{\sigma=\tau}^{\min(\deg P, \tau+u)} \binom{\sigma}{\tau} g_{\sigma-\tau} \le d(d+1)2^d.$$

We deduce

$$\max_{0 \le \tau < v} \max\Big\{|P^{(\tau)}(\theta)|, |G^{(\tau)}(\theta)|\Big\} \le \exp\Big(-\frac{\gamma dt}{s} + \mathcal{O}(d)\Big).$$

Similarly, using $\deg P \le 2t$, we obtain the estimate

$$t(G) \le t + \log\Big(\deg(P)\sum_{\sigma=0}^{u}\binom{\deg P}{\sigma}\Big) \le t + \log\Big(2ts\binom{2t}{s}\Big) \le t + o(t),$$

because the ratio t/s tends to infinity with n. Furthermore, Lemma 1 yields the upper bounds

$$\log L(G/Q) \le \log H(G/Q) + \log(1+\deg P) \le t(G) + o(t) \le t + o(t)$$

and, similarly,

$$\log L(P/Q) \le t + o(t).$$

Now, apply Lemma 13 with the above choice of v, using the trivial bounds

$$\deg(P/Q) \le d, \quad \deg(G/Q) \le d.$$

Since P/Q and G/Q are relatively prime polynomials with integral coefficients, their resultant $\mathrm{Res}(P/Q, G/Q)$ is a nonzero rational integer and we get

$$\begin{aligned}\log|Q(\theta)| &\le -\frac{\gamma dt}{s} + \mathcal{O}(d) + \frac{d}{v}(2t + o(t))\\ &\le -\frac{\gamma dt}{s} + \frac{4dt}{s} + o(\frac{dt}{s}) \qquad (\text{since } v \ge s/2)\\ &\le -\frac{5\gamma dt}{6s} \qquad (\text{since } \gamma > 24)\end{aligned}$$

for n sufficiently large. Since $|\tilde{P}(\theta)|^{u+1} \le |Q(\theta)|$, and since $u+1 \le s$, we deduce

$$|\tilde{P}(\theta)| \le \exp\Big(-\frac{5\gamma dt}{6s^2}\Big)$$

as claimed. □

8. Derivatives of interpolation determinants.

Let $\xi_1, \dots, \xi_n$ be complex numbers which generate a field $F = \mathbf{Q}(\xi_1, \dots, \xi_n)$ of transcendence degree 1 over $\mathbf{Q}$. Fix an element $\theta \in F$ such that F has finite degree over $\mathbf{Q}(\theta)$. Since the extension $F/\mathbf{Q}(\theta)$ is separable, the usual derivation $\phi(\theta) \mapsto \phi'(\theta)$ of the subfield $\mathbf{Q}(\theta)$ extends in a unique way to a derivation $\partial: F \to F$ of the field F. For any integer $\sigma \ge 0$, we denote by $\partial^{(\sigma)}$ the σ-th iterate of the map ∂ divided by $\sigma!$.

In this section, we point out some properties of the operators $\partial^{(\sigma)}$ which we shall need in order to establish upper bounds for the interpolation determinants and their derivatives.

Lemma 15. *There exist constants $c > 0, c_1 \ge 1, \dots, c_n \ge 1$, depending only on the extension $F/\mathbf{Q}(\theta)$, such that, for any integer $\sigma \ge 0$ and any polynomial Q of $\mathbf{Q}[X_1, \dots, X_n]$, we have the upper bound*

$$|\partial^{(\sigma)} Q(\xi_1, \dots, \xi_n)| \;\le\; L(Q)\, c^{\sigma} \prod_{\nu=1}^{n} c_\nu^{\deg_\nu(Q)},$$

where $L(Q)$ denotes the length of Q and $\deg_\nu(Q)$ its partial degree in the variable X_ν for $\nu = 1, \dots, n$.

Proof. Each ξ_ν satisfies a relation of algebraic dependence $P_\nu(\theta, \xi_\nu) = 0$, where P_ν is an irreducible polynomial of $\mathbf{Q}[X, Y]$. The equation $P_\nu(x, y_\nu) = 0$ defines y_ν as an implicit function of x in a neighborhood of θ, with $y_\nu(\theta) = \xi_\nu$. In this respect, $\partial^{(\sigma)} Q(\xi_1, \dots, \xi_n)$ is nothing else than the coefficient of $(x-\theta)^\sigma$ in the Taylor expansion of the function $\phi(x) = Q\left(y_1(x), \dots, y_n(x)\right)$ at the point θ, because this is so in the subfield $\mathbf{Q}(\theta)$. Let R be a positive real number such that the functions $y_1, \dots, y_n$ are analytic in the closed disk with center θ and radius R. Cauchy's formula

$$\phi^{(\sigma)}(\theta) = \frac{1}{2\pi\sqrt{-1}} \int_{|\zeta-\theta|=R} \frac{\phi(\zeta)}{(\zeta-\theta)^{\sigma+1}} d\zeta$$

then implies the estimate of the lemma with

$$c = 1/R, \quad c_\nu = \sup\left\{1, \max_{|\zeta-\theta|\le R} |y_\nu(\zeta)|\right\}, \quad (1 \le \nu \le n). \qquad \square$$

Lemma 16. *Let N be a positive integer and let $\phi_{i,j}$ be elements of F indexed by $1 \le i \le N$, $1 \le j \le N$. Put $\Delta = \det\left(\phi_{i,j}\right)_{\substack{1\le i\le N\\ 1\le j\le N}}$. For each integer $\sigma \ge 0$, we have the formula*

$$\partial^{(\sigma)}\Delta = \sum_{\sigma_1+\cdots+\sigma_N=\sigma} \det\left(\partial^{(\sigma_i)}\phi_{i,j}\right)_{\substack{1\le i\le N\\ 1\le j\le N}}.$$

Proof. In terms of the divided derivation operators $\partial^{(\sigma)}$, Leibniz' formula takes the form

$$\partial^{(\sigma)}\left(\prod_{\nu=1}^N \phi_\nu\right) = \sum_{\sigma_1+\cdots+\sigma_N=\sigma} \prod_{\nu=1}^N \partial^{(\sigma_\nu)}\phi_\nu .$$

It suffices then to expand the determinant Δ. $\square$

Now, assume that $\Delta = \det(\phi_{i,j})$ is an *interpolation determinant of order* N (also called *alternant*). This means that $(\phi_{i,j})$ is a square matrix of order N and that we can write

$$\phi_{i,j} = \varphi_i(\zeta_j), \quad (1 \le i \le N, 1 \le j \le N),$$

for a sequence of entire functions $\varphi_1, \dots, \varphi_N$ and a sequence of points $\zeta_1, \dots, \zeta_N$. Let S be an integer $\le N$. In any sequence of integers $\sigma_1, \dots, \sigma_N \ge 0$ such that $\sigma_1 + \cdots + \sigma_N \le S$, at least $N - S$ terms σ_ν must vanish. Therefore, when σ is $\le S$, Lemma 16 together with Laplace's expansion formula yields $\partial^{(\sigma)}\Delta$ as a linear combination of interpolation determinants of order $\ge N - S$, constructed on subsets of the set of functions $\{\varphi_1, \dots, \varphi_N\}$ and of the set of points $\{\zeta_1, \dots, \zeta_N\}$. Moreover, Lemma 15 provides a control on the absolute values of the coefficients of this linear combination. Now, in a given situation of transcendence, we know how to bound analytically in a non-trivial way such interpolation determinants, for example see [5]. Choosing then for S a fixed fraction of N, say $N/2$, we recover the same constraints as those we get by constructing auxiliary functions, using crude estimates for the degree and size of the determinant Δ. Actually, when we consider an $N \times N$ determinant, degree and size are at most multiplied by N. The introduction of S derivatives allows to divide the product (size) $\times$ (degree) by S, thanks to Proposition 1. This brings a factor $N^2/S \sim 2N$ into the arithmetic estimates. We can conclude because the analytic argument also multiplies by N the logarithmic bounds. In the next section, we apply this sketch of proof to recover a classical result.

9. A new proof of a theorem of Gel'fond.

Let α be an algebraic number $\neq 0, 1$ and let β be a cubic irrational. Gel'fond proved in 1949 that the two numbers α^β and α^{β^2} are algebraically independent over $\mathbf{Q}$. We intend to recover this famous result by considering the derivatives of the interpolation determinants which appear naturally in Gel'fond's construction. Actually, as in [9] or in Chapter 7 of [11], the formalization of the proof leads to the following more general statement.

Theorem. *Let m and n be integers ≥ 2 such that $mn \geq 2m + n$. Let $u_1, \dots, u_m$ and $v_1, \dots, v_n$ be families of $\mathbf{Q}$-linearly independent complex numbers. Then the transcendence degree over $\mathbf{Q}$ of the field*

$$\mathbf{Q}\left(v_\nu, e^{u_\mu v_\nu} \,;\, 1 \leq \mu \leq m, 1 \leq \nu \leq n\right)$$

is ≥ 2.

The algebraic independence of α^β and α^{β^2} follows immediately by taking $m = n = 3$ and

$$(u_1, u_2, u_3) = (\log\alpha, \beta\log\alpha, \beta^2\log\alpha), \quad (v_1, v_2, v_3) = (1, \beta, \beta^2).$$

To prove the above theorem, we argue by contradiction. Thus, suppose on the contrary that the field $\mathbf{Q}\left(v_\nu, e^{u_\mu v_\nu} \,;\, 1 \leq \mu \leq m, 1 \leq \nu \leq n\right)$ has transcendence degree ≤ 1 over $\mathbf{Q}$. Then the six exponentials theorem (see for example Corollary 2.2.3 of [11]) shows that this degree is precisely equal to 1. Using Noether's normalization theorem, we choose an element θ of the algebra $\mathbf{Q}\left[v_\nu, e^{u_\mu v_\nu} \,;\, 1 \leq \mu \leq m, 1 \leq \nu \leq n\right]$ such that this algebra is integral over $\mathbf{Q}[\theta]$. Let F be the subfield of $\mathbf{C}$ generated over $\mathbf{Q}$ by the numbers $v_\nu, e^{u_\mu v_\nu}$ and their conjugates over $\mathbf{Q}(\theta)$. As in the preceding section, we extend the map $\phi(\theta) \mapsto \phi'(\theta)$ into a derivation ∂ of the field F.

9.1. Construction of a matrix of evaluation.

Let K, L, R be integers ≥ 1. Consider the matrix

$$\mathcal{M} = \left(\left(\sum_{\nu=1}^{n} r_\nu v_\nu\right)^k \prod_{\mu=1}^{m}\prod_{\nu=1}^{n} \left(e^{u_\mu v_\nu}\right)^{\ell_\mu r_\nu}\right)$$

of size $KL^m \times R^n$ where the rows are indexed by the $(m+1)$-tuples of integers $(k, \ell_1, \dots, \ell_m)$ with $0 \leq k < K$, $0 \leq \ell_\mu < L$, $(1 \leq \mu \leq m)$, and the columns by the n-tuples of integers $(r_1, \dots, r_n)$ with $0 \leq r_\nu < R$, $(1 \leq \nu \leq n)$. By its very construction, $\mathcal{M}$ is the matrix of evaluation of the KL^m functions

$$z^k \exp\left(\left(\sum_{\mu=1}^{m} \ell_\mu u_\mu\right) z\right), \quad (0 \leq k < K, 0 \leq \ell_\mu < L, 1 \leq \mu \leq m)$$

at the R^n points
$$\sum_{\nu=1}^{n} r_\nu v_\nu, \quad (0 \le r_\nu < R,\ 1 \le \nu \le n).$$

Lemma 17. *Assume $R^n \ge (m+1)^{m+n} K L^m$. Then the matrix $\mathcal{M}$ has maximal rank equal to the number $N := KL^m$ of its rows.*

Proof. This is a corollary of the zero estimate of [6]. Denote by G the algebraic group $\big(\mathbf{G}_{\mathtt{a}} \times \mathbf{G}_{\mathtt{m}}^m\big)(\mathbf{C}) = \mathbf{C} \times (\mathbf{C}^*)^m$, and, for any real number $S > 0$, denote by $\Gamma(S)$ the subset of G consisting of the points
$$\left(\sum_{\nu=1}^{n} s_\nu v_\nu, \prod_{\nu=1}^{n} \left(e^{u_1 v_\nu}\right)^{s_\nu}, \dots, \prod_{\nu=1}^{n} \left(e^{u_m v_\nu}\right)^{s_\nu}\right), \quad (0 \le s_\nu < S,\ 1 \le \nu \le n).$$

We will argue by contradiction, assuming that there is a non-trivial relation of linear dependence between the rows of $\mathcal{M}$. This translates into the existence of a nonzero polynomial of $\mathbf{C}[X, Y_1, \dots, Y_m]$ with degree $\le K-1$ in X and degree $\le L-1$ in each of the variables $Y_1, \dots, Y_m$, which vanishes at all points of $\Gamma(R)$. Put $R' = R/(m+1)$. The sum $\Gamma(R') + \cdots + \Gamma(R')$ of $m+1$ copies of $\Gamma(R')$ in the group G is clearly contained in $\Gamma(R)$. Theorem 2.1 of [6] then implies the existence of a connected algebraic subgroup $G' \simeq (\mathbf{G}_{\mathtt{a}}^{\delta_0} \times \mathbf{G}_{\mathtt{m}}^{\delta_1})(\mathbf{C})$ of G, distinct from G, such that

$$(\delta_0 + \delta_1)!\,\mathrm{Card}\left(\frac{\Gamma(R') + G'}{G'}\right) \le (m+1)!(K-1)^{1-\delta_0}(L-1)^{m-\delta_1}. \tag{5}$$

Let us analyze the different possibilities for the pair of dimensions (δ_0, δ_1).

If $\delta_0 = 0$, the linear independence over $\mathbf{Q}$ of $v_1, \dots, v_n$ shows, by projection on the factor $\mathbf{G}_{\mathtt{a}}$, that
$$\begin{aligned}\mathrm{Card}\left(\frac{\Gamma(R') + G'}{G'}\right) &= \mathrm{Card}\Big\{(r_1, \dots, r_n)\,;\ 0 \le r_\nu < R',\ \nu = 1, \dots, n\Big\}\\ &\ge (R')^n = \frac{R^n}{(m+1)^n}.\end{aligned}$$

Substituting this lower bound into (5), we get
$$\frac{R^n}{(m+1)^n} \le (m+1)!(K-1)(L-1)^{m-\delta_1} < (m+1)^m K L^m$$
in contradiction with the hypothesis.

Suppose now that $\delta_0 = 1$. Then G' takes the form $\mathbf{C} \times \mathbf{T}$ where $\mathbf{T}$ is a proper subtorus of $(\mathbf{C}^*)^m$. We view $\mathbf{T}$ as the common kernel of the elements in a non-trivial additive subgroup $\mathcal{T}$ of the group
$$\mathrm{Hom}(\mathbf{G}_{\mathtt{m}}^m, \mathbf{G}_{\mathtt{m}}) = \mathbf{Z}^m$$
of algebraic characters of $\mathbf{G}_{\mathtt{m}}$:
$$\mathbf{T} = \left\{(y_1, \dots, y_m) \in (\mathbf{C}^*)^m\,;\ \prod_{\mu=1}^{m} y_\mu^{t_\mu} = 1 \quad \text{for any } (t_1, \dots, t_m) \in \mathcal{T}\right\}.$$

This gives a bijection between $(\Gamma(R')+G')/G'$ and the set of equivalence classes of integral points contained in the hypercube $[0,R'[^m$, modulo the relation

$$\left(\sum_{\nu=1}^{n}(r_\nu - r'_\nu)v_\nu\right)\left(\sum_{\mu=1}^{m} t_\mu u_\mu\right) \in 2\pi\sqrt{-1}\,\mathbf{Z} \quad \text{for any } (t_1,\dots,t_m)\in\mathcal{T} \tag{6}$$

which identifies the points with coordinates $(r_1,\dots,r_m)$ and $(r'_1,\dots,r'_m)$. Note that the rank of $\mathcal{T}$ is equal to $m-\delta_1$, so it is positive. If the rank of $\mathcal{T}$ is ≥ 2, relation (6), together with the hypothesis of linear independence of the families $u_1,\dots,u_m$ and $v_1,\dots,v_n$, implies $r_1-r'_1=\cdots=r_m-r'_m=0$. The conclusion then follows as in the case $\delta_0=0$. Without loss of generality, we may therefore assume that the rank of $\mathcal{T}$ is equal to 1. In this case, we have $\delta_1=m-1$, and there is a line passing through the origin in $\mathbf{R}^n$ such that (6) holds only when the point $(r_1-r'_1,\dots,r_n-r'_n)$ is located on that line. Moreover, since $n\geq 2$, we may assume that this line is not contained in the hyperplane $0\times\mathbf{R}^{n-1}$. Then the canonical projection $\Gamma(R')\longrightarrow\big(\Gamma(R')+G'\big)/G'$ is injective on the set of points of $\Gamma(R')$ for which $r_1=0$. It follows that

$$\begin{aligned}\operatorname{Card}\left(\frac{\Gamma(R')+G'}{G'}\right) &\geq \operatorname{Card}\Big\{(r_2,\dots,r_n)\,;\, 0\leq r_\nu < R',\, \nu=2,\dots,n\Big\}\\ &\geq (R')^{n-1} = \frac{R^{n-1}}{(m+1)^{n-1}}.\end{aligned}$$

Inequality (5) then implies that $R^{n-1}<(m+1)^nL$. Since $mn\geq m+n$ and $n\geq 2$, this upper bound for R contradicts the lower bound $R^n\geq(m+1)^{n+2}L^m$ coming from the hypotheses. This completes the proof of the lemma. □

9.2. Analytic estimates.

From now on, we assume that the triple of integers K, L, R satisfies the inequality $R^n\geq(m+1)^{m+n}KL^m$ of Lemma 17. Fix a nonzero minor Δ of maximal size $N\times N$ taken from $\mathcal{M}$. Denote by $\tilde F$ the subfield $\mathbf{Q}\left(v_1,\dots,v_n,e^{u_1v_1},\dots,e^{u_mv_n}\right)$ of F. Since Δ is integral over $\mathbf{Q}[\theta]$, its norm in the extension $\tilde F/\mathbf{Q}(\theta)$ belongs to $\mathbf{Q}[\theta]$. Let Q be the polynomial of $\mathbf{Q}[X]$ such that

$$Q(\theta)=N_{\tilde F/\mathbf{Q}(\theta)}(\Delta):=\prod_{\iota}\iota\Delta,$$

where ι runs through the set of embeddings of $\tilde F$ into $\mathbf{C}$ whose restriction to the subfield $\mathbf{Q}(\theta)$ is the identity.

We denote by the symbol $\mathcal{O}(*)$ any quantity which is bounded above by the product of the argument of $\mathcal{O}$ by a positive constant independent of K, L, R. We shall essentially carry out asymptotic estimates, meaning that the integers K, L, R are assumed to be sufficiently large in each inequality under consideration.

Lemma 18. *For any integer σ with $0\leq\sigma<S:=[N/2]$, and any real number $\rho\geq 1$, we have the estimate*

$$\log|Q^{(\sigma)}(\theta)|\leq-\frac{N^2\log\rho}{8}+\mathcal{O}\Big(N\big(K\log(\rho R)+\rho LR\big)\Big).$$

Proof. Let $(k_i, \ell_{1i}, \dots, \ell_{mi})$, $(1 \le i \le N)$, be the row indices of the matrix $\mathcal{M}$, and let $(r_{1j}, \dots, r_{nj})$, $(1 \le j \le N)$, be the indices of the N columns of $\mathcal{M}$ which enter into the minor Δ. Then we have $\Delta = \det(\phi_{i,j})_{1\le i,j\le N}$, where $\phi_{i,j} = \varphi_i(\zeta_j)$ with

$$\varphi_i(z) = z^{k_i} \exp\Big(\Big(\sum_{\mu=1}^{m} \ell_{\mu i} u_\mu\Big) z\Big), \quad \zeta_j = \sum_{\nu=1}^{n} r_{\nu j} v_\nu, \quad (1 \le i, j \le N).$$

It is clear that $\phi_{i,j}$ can be written in the form

$$\phi_{i,j} = \left(\sum_{\nu=1}^{n} r_{\nu j} v_\nu\right)^{k_i} \prod_{\mu=1}^{m} \prod_{\nu=1}^{n} \left(e^{u_\mu v_\nu}\right)^{\ell_{\mu i} r_{\nu j}} = Q_{i,j}\left(v_1, \dots, v_n, e^{u_1 v_1}, \dots, e^{u_m v_n}\right),$$

where $Q_{i,j}$ denotes a polynomial of $\mathbf{Z}[X_1, \dots, X_n, Y_1, \dots, Y_{mn}]$ whose partial degrees are bounded above by K in the variables X_μ, and by LR in the variables $Y_{\mu,\nu}$, $(1 \le \mu \le m, 1 \le \nu \le n)$. It is also easy to estimate the length of the polynomials $Q_{i,j}$:

$$\log L(Q_{i,j}) = \mathcal{O}(K \log R).$$

On the other hand, Leibniz' formula together with Lemma 16 shows that

$$\begin{aligned} Q^{(\sigma)}(\theta) &= \partial^{(\sigma)} Q(\theta) \\ &= \sum_{(\sigma_\iota)} \prod_{\iota} \partial^{(\sigma_\iota)}(\iota\Delta) \\ &= \sum_{(\sigma_{\iota i})} \prod_{\iota} \det\Big(\partial^{(\sigma_{\iota i})} Q_{i,j}\left(\iota v_1, \dots, \iota v_n, \iota e^{u_1 v_1}, \dots, \iota e^{u_m v_n}\right)\Big)_{\substack{1\le i\le N\\ 1\le j\le N}}, \end{aligned}$$

where the first sum is indexed by the $[\tilde{F} : \mathbf{Q}(\theta)]$-tuples of integers (σ_ι) with $\sum_\iota \sigma_\iota = \sigma$, while the second sum is indexed by the $\big([\tilde{F} : \mathbf{Q}(\theta)] \times N\big)$-tuples of integers satisfying $\sum_\iota \sum_i \sigma_{\iota i} = \sigma$. In each of the products indexed by ι, we isolate the factor corresponding to the identity. Lemma 15 provides a bound for the remaining factors. We get

$$\log \left| \prod_{\iota \ne \text{ identity}} \det\Big(\partial^{(\sigma_{\iota i})} Q_{i,j}\left(\iota v_1, \dots, \iota v_n, \iota e^{u_1 v_1}, \dots, \iota e^{u_m v_n}\right)\Big)_{\substack{1\le i\le N\\ 1\le j\le N}} \right| = \mathcal{O}\Big(N(K \log R + LR)\Big),$$

by using the above mentioned estimates for the degrees and length of the polynomials $Q_{i,j}$, and by expanding determinants and products. It remains to prove that for any $\sigma \le S$, and any $\rho \ge 1$, we have

$$\log \left|\partial^{(\sigma)}(\Delta)\right| \le -\frac{N^2 \log \rho}{8} + \mathcal{O}\Big(N\big(K \log(\rho R) + \rho L R\big)\Big).$$

Lemma 16 yields the formula

$$\partial^{(\sigma)}(\Delta) = \sum_{\sigma_1 + \cdots + \sigma_N = \sigma} \det\Big(\partial^{(\sigma_i)} \phi_{i,j}\Big)_{\substack{1\le i\le N\\ 1\le j\le N}}.$$

For each summand $\det\left(\partial^{(\sigma_i)}\phi_{i,j}\right)$, consider the set $I \subset \{1,\dots,N\}$ of row indices i for which $\sigma_i = 0$. Since $\sigma_1 + \cdots + \sigma_N \le S \le N/2$, it is clear that the cardinality of I is $\ge N/2$. Using Laplace's expansion formula, we can then write $\partial^{(\sigma)}(\Delta)$ as a linear combination

$$\partial^{(\sigma)}(\Delta) = \sum_{\substack{(I,J)\\ N/2 \le |I|=|J| \le N}} C_{I,J} \det\Big(\varphi_i(\zeta_j)\Big)_{\substack{i\in I\\ j\in J}},$$

of interpolation determinants of order $\ge N/2$. As above, Lemma 15 provides an upper bound for the coefficients:

$$\log|C_{I,J}| = \mathcal{O}\Big(N(K\log R + LR)\Big).$$

Moreover, if we put $\nu = \operatorname{Card} I = \operatorname{Card} J$, the function $z \mapsto \det\Big(\varphi_i(z\zeta_j)\Big)_{\substack{i\in I\\ j\in J}}$ of the complex variable z admits a zero at the origin of multiplicity $\ge (\nu^2-\nu)/2$. The usual Schwarz lemma then yields the upper bound

$$\log\left|\det\Big(\varphi_i\left(\zeta_j\right)\Big)_{\substack{i\in I\\ j\in J}}\right| \le -\frac{\nu^2-\nu}{2}\log\rho + \log(\nu!) + \sum_{i\in I}\log\max_{|z|=\rho\max_j|\zeta_j|}|\varphi_i(z)|,$$

for any real number $\rho \ge 1$. See for example Lemma 7 of [5] for more details on this argument which is fundamental to the method of interpolation determinants. The required estimate follows from the trivial bounds

$$\begin{aligned}
\max_{|z|=\rho\max|\zeta_j|}|\varphi_i(z)| &\le \max_{|z|=\rho R(\sum_\nu |v_\nu|)}|\varphi_i(z)| \\
&\le \left(\rho R\Big(\sum_\nu |v_\nu|\Big)\right)^K \times \exp\left(\rho LR\Big(\sum_\mu |u_\mu|\Big)\Big(\sum_\nu |v_\nu|\Big)\right) \\
&\le \exp\left(\mathcal{O}\Big(K\log(\rho R) + \rho LR\Big)\right),
\end{aligned}$$

and the lower bound $\nu \ge N/2$. □

9.3. Proof of the theorem.

For $\nu = 1,\dots,n$, denote by a_ν the smallest positive integer a for which av_ν is integral over the ring $\mathbf{Z}[\theta]$. Such an integer exists since v_ν is integral over the algebra $\mathbf{Q}[\theta]$. Similarly, define $b_{\mu\nu}$ to be the smallest positive integer b for which $be^{u_\mu v_\nu}$ is integral over $\mathbf{Z}[\theta]$, for $1 \le \mu \le m$, $1 \le \nu \le n$. Since the coefficients ϕ_{ij} of the determinant Δ can be written as values of polynomials $Q_{ij}(v_1,\dots,v_n,e^{u_1v_1},\dots,e^{u_mv_n})$, of degree $\le K$ in each of the first n variables and degree $\le LR$ in each of the mn others, it is clear that

$$\tilde\Delta = \left(\prod_{\nu=1}^n a_\nu^K \prod_{\mu=1}^m\prod_{\nu=1}^n b_{\mu\nu}^{LR}\right)^N \Delta$$

belongs to the ring $\mathbf{Z}\left[a_1v_1,\dots,a_nv_n,b_{11}e^{u_1v_1},\dots,b_{mn}e^{u_mv_n}\right]$. Since this ring is integral over $\mathbf{Z}[\theta]$, the norm $N_{\tilde F/\mathbf{Q}(\theta)}(\tilde\Delta)$ thus belongs to $\mathbf{Z}[\theta]$. It follows that the coefficients of the polynomial

$$P(X) = \left(\prod_{\mu=1}^m a_\mu^K \prod_{\mu=1}^m\prod_{\nu=1}^n b_{\mu\nu}^{LR}\right)^{N[\tilde F:\mathbf{Q}(\theta)]} Q(X)$$

are rational integers. Furthermore, standard arguments of algebraic reduction (see for example Lemmas 4.2.5 and 4.2.20 of [10]) show that

$$\deg P = \mathcal{O}\Big(N(K+LR)\Big), \quad t(P) = \mathcal{O}\Big(N(K\log R + LR)\Big).$$

The proof then goes on as in the classical context of auxiliary functions, with essentially the same constraints on the parameters. Consider the sequence of polynomials $(P_R)_{R\in\mathbf{N}}$ defined as above for the choice of parameters (K, L, R) given by the formulas

$$K = \Big[R^{\frac{m+n}{m+1}}(\log R)^{-\frac{m}{m+1}}\Big], \quad L = \Big[(m+1)^{-n}R^{\frac{n-1}{m+1}}(\log R)^{\frac{1}{m+1}}\Big].$$

The condition $R^n \geq (m+1)^{m+n}KL^m$ of Lemma 17 is then satisfied. Lemma 18 with $\rho = R^{\frac{1}{m+1}}$ yields the upper bound

$$\log \max_{0\leq\sigma\leq[N/2]} \Big|P_R^{(\sigma)}(\theta)\Big| \leq -\frac{1}{8(m+1)}N^2\log R + o\Big(N^2\log R\Big).$$

On the other hand, we have the estimates

$$(K\log R + LR)^2 = \mathcal{O}\Big(R^{\frac{2(m+n)}{m+1}}(\log R)^{\frac{2}{m+1}}\Big) = o\Big(R^n\log R\Big) = o\Big(N\log R\Big),$$

since $mn \geq 2m+n$. Proposition 1, together with the previous estimates for the degree and size of P_R, shows that the number θ is algebraic. This is a contradiction. $\square$

References

1. W. D. Brownawell, *Sequences of Diophantine approximations*, J. Number Theory **6** (1974), 10–21.
2. A. Durand, *Approximations algébriques d'un nombre transcendant*, Cinquante ans de polynômes, Lecture Notes in Math. 1415 (M. Langevin and M. Waldschmidt, eds.), Springer-Verlag, 1990, pp. 94–96.
3. K. Geddes, S. Czapor and G. Labahn, *Algorithms for Computer Algebra*, Kluwer Academic Publishers, 1992, pp. 285–300.
4. M. Laurent, *Sur quelques résultats récents de transcendance*, Journées Arithmétiques de Luminy 1989, Astérisque 198-200, pp. 209–230.
5. M. Laurent, *Linear forms in two logarithms and interpolation determinants*, Acta Arithmetica **LXVI.2** (1994), 181–199.
6. P. Philippon, *Lemme de zéros dans les groupes algébriques commutatifs*, Bull. Soc. Math. France **114** (1986), 355-383 and **115** (1987), 397–398.
7. D. Roy and M. Waldschmidt, *Quadratic relations between logarithms of algebraic numbers*, Proc. Japan Acad. Ser. A Math. Sci. **71** (1995), 151–153.
8. D. Roy et M. Waldschmidt, *Approximation diophantienne et indépendance algébrique de logarithmes*, Ann. Sci. École Norm. Sup. **30** (1997), 753–796.

9. R. Tijdeman, *On the algebraic independence of certain numbers*, Indag. Math. **33** (1971), 146–162.

10. M. Waldschmidt, *Linear independence of logarithms of algebraic numbers*, The Institute of Mathematical Sciences, Madras, IMSc. Report 116, 1992 http://www.math.jussieu.fr/∼miw.

11. M. Waldschmidt, *Nombres transcendants, Lecture Notes in Math. 402*, Springer-Verlag, 1974.

12. M. Waldschmidt, *Suites colorées*, Séminaire Delange–Pisot–Poitou, (Groupe d'étude de théorie des nombres), 17-ième année, 1975/76, exposé 21, 11 pages.

13. E. Wirsing, *Approximation mit algebraischen Zahlen beschränkten Grades*, J. reine angew. Math. **206** (1961), 67-77.

Institut de Mathématiques de Luminy, CNRS, 163 Avenue de Luminy, Case 930, 13288 MARSEILLE Cédex 9, FRANCE.
E-mail address: `laurent@iml.univ-mrs.fr`

Département de Mathématiques, Université d'Ottawa, 585 King Edward, Ottawa, Ontario, CANADA K1N 6N5.
E-mail address: `droy@mathstat.uottawa.ca`