Compositio Math. 140 (2004) 593–612
DOI: 10.1112/S0010437X03000708

Diophantine approximation by conjugate algebraic integers

Damien Roy and Michel Waldschmidt

Abstract

Building on the work of Davenport and Schmidt, we mainly prove two results. The first one is a version of Gel'fond's transcendence criterion which provides a sufficient condition for a complex or p-adic number ξ to be algebraic in terms of the existence of polynomials of bounded degree taking small values at ξ together with most of their derivatives. The second one, which follows from this criterion by an argument of duality, is a result of simultaneous approximation by conjugate algebraic integers for a fixed number ξ that is either transcendental or algebraic of sufficiently large degree. We also present several constructions showing that these results are essentially optimal.

1. Introduction

Motivated by the work of Wirsing [Wir60], Davenport and Schmidt investigated, in their 1969 seminal paper [DS69], the approximation of an arbitrary fixed real number ξ by algebraic integers of bounded degree. They proved that, if $n \geqslant 3$ is an integer and if ξ is not algebraic over $\mathbb{Q}$ of degree at most $(n-1)/2$, then there are infinitely many algebraic integers α of degree at most n such that

$$|\xi - \alpha| \leqslant c\mathrm{H}(\alpha)^{-[(n+1)/2]},$$

where c is a positive constant depending only on n and ξ and where $\mathrm{H}(\alpha)$ denotes the usual *height* of α, that is the maximum absolute value of the coefficients of its irreducible polynomial over $\mathbb{Z}$. They also provided refinements for $n \leqslant 4$. Recently, Bugeaud and Teulié revisited this result and showed in [BT00] that we may also impose that all approximations α have degree exactly n over $\mathbb{Q}$. Moreover, a p-adic analog was proven by Teulié [Teu02].

Here we establish a similar result for simultaneous approximation by several conjugate algebraic integers. In order to cover the case where ξ is a complex or p-adic number, we will assume more generally that ξ belongs to the completion of a number field K at some place w.

Thus, we fix an algebraic extension K of $\mathbb{Q}$ of finite degree d. For each place v of K, we denote by K_v the completion of K at v and by d_v its local degree at v. We also normalize the corresponding absolute value $|\ |_v$ as in [BV83] by asking that, when v is above a prime number p of $\mathbb{Q}$, we have $|p|_v = p^{-d_v/d}$ and that, when v is an Archimedean place, we have $|x|_v = |x|^{d_v/d}$ for any $x \in \mathbb{Q}$. Then, our result of approximation reads as follows.

Theorem A. *Let n and t be integers with $1 \leqslant t \leqslant n/4$. Let w be a place of K and let ξ be an element of K_w which is not algebraic over K of degree $\leqslant (n+1)/(2t)$. Assume further that $|\xi|_w \leqslant 1$*

Received 11 March 2002, accepted in final form 24 July 2002.
2000 Mathematics Subject Classification 11J13 (primary), 11J61, 11J82 (secondary).
Keywords: algebraic integers, algebraic numbers, approximation, convex bodies, degree, derivatives, duality, Gel'fond's criterion, height, polynomials, transcendence criterion.
The work of the first author is partially supported by NSERC and CICMA.

if w is ultrametric. Then there exist infinitely many algebraic integers α which have degree $n+1$ over K, degree $d(n+1)$ over $\mathbb{Q}$ and admit, over K, t distinct conjugates $\alpha_1, \dots, \alpha_t$ in K_w satisfying

$$\max_{1\leqslant i\leqslant t} |\xi - \alpha_i|_w \leqslant c\mathrm{H}(\alpha)^{-(n+1)/(4dt^2)}, \tag{1.1}$$

where c is a constant depending only on K, n, w and ξ.

Note that, for $t = 1$, $K = \mathbb{Q}$ and $K_w = \mathbb{R}$, this result is comparable to Theorem 2 of [DS69] mentioned above (with a shift of 1 in the degree of the approximation). Note also that, if w is ultrametric, any algebraic integer α in K_w satisfies $|\alpha|_w \leqslant 1$ and so the condition $|\xi|_w \leqslant 1$ is necessary to approximate ξ by such numbers.

In § 10, we show that the exponent of approximation $(n+1)/(4dt^2)$ in (1.1) is essentially best possible up to its numerical factor of $1/4$ and that this factor cannot be replaced by a real number greater than 2, although its value can be slightly improved using more precise estimates along the lines of the present work. For the sake of simplicity, we do not go into such estimates here, nor do we try to sharpen the exponent of approximation for small values of n. It is difficult to predict an optimal value for this exponent (see [Roy04]).

In answer to a question of K. Tishchenko, we also show that one cannot hope to obtain a similar exponent for simultaneous approximation of t numbers. Taking $K = \mathbb{Q}$ and $K_w = \mathbb{R}$, we prove a result which implies that, if $2 \leqslant t \leqslant n$, then there exist a constant $c > 0$ and t real numbers $\xi_1, \dots, \xi_t$ such that

$$\max_{1\leqslant i\leqslant t} |\xi_i - \alpha_i| \geqslant c\mathrm{H}(\alpha)^{-3n^{1/t}}$$

for any choice of t distinct conjugates $\alpha_1, \dots, \alpha_t \in \mathbb{C}$ of an algebraic number α of degree between t and n.

The proof of Theorem A uses the same general strategy as Davenport and Schmidt in [DS69]. It relies on a duality argument combined with the following version of Gel'fond's criterion of algebraic independence where, for a polynomial $Q \in K[T]$, an integer $j \geqslant 0$ and a place v of K, the notation $\|Q\|_v$ stands for the maximal v-adic absolute value of the coefficients of Q, while $Q^{(j)}$ denotes the jth derivative of Q.

Theorem B. *Let n and t be integers with $1 \leqslant t \leqslant n/4$ and let $k = [n/4]$ denote the integral part of $n/4$. Let w be a place of K and let ξ be an element of K_w. There exists a constant $c > 0$ which depends only on K, n, w and ξ and has the following property. Assume that, for each sufficiently large real number X, there exists a non-zero polynomial $Q \in K[T]$ of degree at most n which satisfies $\|Q\|_v \leqslant 1$ for each place v of K distinct from w and also*

$$\max_{0\leqslant j\leqslant n-t} |Q^{(j)}(\xi)|_w \leqslant cX^{-t/(k+1-t)} \quad \text{and} \quad \max_{n-t<j\leqslant n} |Q^{(j)}(\xi)|_w \leqslant X. \tag{1.2}$$

Then, ξ is algebraic over K of degree $\leqslant (n-k+1)/(2t)$.

Note that Theorem B may still hold with an exponent smaller than $t/([n/4]+1-t)$ in the above conditions (1.2). However, we will see in § 3 that it would not hold with an exponent smaller than $t/(n+1-t)$.

It is also interesting to compare this result with the criterion of algebraic independence with multiplicities of [LR99]. A main difference is that the above theorem requires from the polynomial Q that a large proportion of its derivatives at ξ are small (at least three quarters of them), while the conditions in Proposition 1 of [LR99] are sharp only when a small proportion of these derivatives are taken into account (say, at most the first half of them).

This paper is organized as follows. Section 2 sets the various notions of heights that we use throughout the paper. The results of duality which are needed to deduce Theorem A from Theorem B are given in § 3, but the proof of this implication is postponed to § 9. Sections 4–7 are devoted to preliminary results towards the proof of Theorem B which is completed in § 8. In particular, we establish in § 4 a version of Gel'fond's criterion (without multiplicities) which includes Theorem 2b of [DS69] and § 5 presents a height estimate which generalizes Theorem 3 of [DS69]. We conclude in § 10 with two remarks on the exponent of approximation in Theorem A.

Notation. Throughout this paper, n denotes a positive integer, w denotes a place of K and ξ an element of K_w. For conciseness, we will sometimes use the expressions $a \ll b$ or $b \gg a$ to mean that the given non-negative real numbers a and b satisfy $a \leqslant cb$ for some positive constant c which depends only on K, n, w and ξ. Overall, we tried to be coherent with the notation of [DS69].

2. Heights

Recall that K is a fixed algebraic extension of $\mathbb{Q}$ of degree d. With the normalization of its absolute values given in the Introduction, the product formula reads

$$\prod_v |a|_v = 1$$

for any non-zero element a of K.

Let n be a positive integer. For any place v of K and any n-tuple $\underline{a} = (a_1, \ldots, a_n) \in K_v^n$, we define the *norm* of $\underline{a}$ as its maximum norm $\|\underline{a}\|_v = \max\{|a_1|_v, \ldots, |a_n|_v\}$. Accordingly, the (absolute) *height* of a point $\underline{a}$ of K^n is defined by

$$\mathrm{H}(\underline{a}) = \prod_v \|\underline{a}\|_v.$$

If m is a positive integer with $1 \leqslant m \leqslant n$ and if M is an $m \times n$ matrix with coefficients in K_v for some place v of K, we define $\|M\|_v$ as the norm of the $\binom{n}{m}$-tuple formed by the minors of order m of M in some order. When M has coefficients in K, we define $\mathrm{H}(M)$ as the height of the same point. In particular, for an $m \times n$ matrix M of rank m with coefficients in K we have $\mathrm{H}(M) \geqslant 1$.

If V is a subspace of K^n of dimension $m \geqslant 1$, we define the *height* $\mathrm{H}(V)$ of V to be the height of a set of Plücker coordinates of V. In other words, we define $\mathrm{H}(V) = \mathrm{H}(M)$ where M is an $m \times n$ matrix whose rows form a basis of V. This is independent of the choice of M. According to a well-known duality principle, we also have $\mathrm{H}(V) = \mathrm{H}(N)$ where N is any $(n-m) \times n$ matrix such that V is the solution set $\{\underline{a} \in K^n; N\underline{a} = 0\}$ of the homogeneous system attached to N (see [Sch67, formula (4), p. 433]). When $V = 0$, we set $\mathrm{H}(V) = 1$.

We denote by E_n the subspace of $K[T]$ consisting of all polynomials of degree $\leqslant n$, and for each place v of K, we denote by $E_{n,v}$ the closure of E_n in $K_v[T]$. We also identify E_n with K^{n+1} and $E_{n,v}$ with K_v^{n+1} by mapping a polynomial $a_0 + a_1T + \cdots + a_nT^n$ to the $(n+1)$-tuple $(a_0, \ldots, a_n)$ of its coefficients. Accordingly, we define the norm $\|P\|_v$ of a polynomial $P \in E_{n,v}$ as the maximum of the absolute values of its coefficients, and the height $\mathrm{H}(P)$ of a polynomial $P \in E_n$ as the height of the $(n+1)$-tuple of its coefficients. In the sequel, we will repeatedly use the fact that, if $P_1, \ldots, P_s \in K[T]$ have product $P = P_1 \cdots P_s$ of degree $\leqslant n$, with $P \neq 0$ and $n \geqslant 1$, then we have

$$e^{-n}\mathrm{H}(P_1)\cdots\mathrm{H}(P_s) < \mathrm{H}(P) < e^{n}\mathrm{H}(P_1)\cdots\mathrm{H}(P_s),$$

as one gets for instance by comparing $\|P_1\|_v \cdots \|P_s\|_v$ and $\|P\|_v$ at all places v of K using the various estimates of [Lan83, ch. 3, § 2]. Finally, note that, if P is an irreducible polynomial of $K[T]$ of degree n, if α is a root of P in some extension of K and if $\deg(\alpha)$ denotes the degree of α over $\mathbb{Q}$, then there exist positive constants c_1 and c_2 depending only on n and $\deg(\alpha)$ such that

$$c_1\mathrm{H}(\alpha)^n \leqslant \mathrm{H}(P)^{\deg(\alpha)} \leqslant c_2\mathrm{H}(\alpha)^n.$$

This follows from Proposition 2.5 in Chapter 3 of [Lan83] applied once to P and once to the irreducible polynomial of α over $\mathbb{Z}$ (since we defined $\mathrm{H}(\alpha)$ to be the height of the latter polynomial).

3. Duality

In this section, we fix a positive integer n, a place w of K and an element ξ of K_w. We define below a family of adelic convex bodies and establish about them a result of duality that we will need in order to deduce Theorem A from Theorem B. We also describe consequences of the adelic Minkowski's theorem of Macfeat [McF71] and Bombieri and Vaaler [BV83] for this type of convex.

For any $(n+1)$-tuple of positive real numbers $\underline{X} = (X_0, X_1, \ldots, X_n)$, we define an adelic convex body

$$\mathcal{C}(\underline{X}) = \prod_v \mathcal{C}_v(\underline{X}) \subset \prod_v E_{n,v}$$

by putting

$$\mathcal{C}_w(\underline{X}) = \{P \in E_{n,w}; |P^{(j)}(\xi)|_w \leqslant X_j \text{ for } j = 0, \ldots, n\}$$

at the selected place w and

$$\mathcal{C}_v(\underline{X}) = \{P \in E_{n,v}; \|P\|_v \leqslant 1\}$$

at the other places $v \neq w$. For $i = 1, \ldots, n+1$, we denote by $\lambda_i(\underline{X}) = \lambda_i(\mathcal{C}(\underline{X}))$ the ith minimum of $\mathcal{C}(\underline{X})$ in E_n. By definition, this is the smallest positive real number λ such that $\lambda\mathcal{C}(\underline{X})$ contains i linearly independent elements of E_n, where $\lambda\mathcal{C}(\underline{X})$ is the adelic convex body whose component at any Archimedean place v consists of all products λP with $P \in \mathcal{C}_v(\underline{X})$ and whose component at any ultrametric place v is $\mathcal{C}_v(\underline{X})$.

In order to apply the adelic Minkowski's theorem of [BV83] in this context, we identify each space $E_{n,v}$ with K_v^{n+1} in the natural way described in § 2. This identifies $\prod_v E_{n,v}$ with $(K_{\mathbf{A}})^{n+1}$ where $K_{\mathbf{A}}$ denotes the ring of adèles of K, and we use the same Haar measure as in [BV83] on this space. Explicitly, this means that, for an Archimedean place v of K, we choose the Haar measure on K_v to be the Lebesgue measure if $K_v = \mathbb{R}$ and twice the Lebesgue measure if $K_v = \mathbb{C}$. For an ultrametric place v, we normalize the measure so that the ring of integers $\mathcal{O}_v$ of K_v has volume $|\mathcal{D}_v|_v^{d/2}$ where $\mathcal{D}_v$ denotes the local different of K at v. On each factor $E_{n,v} \simeq K_v^{n+1}$ we use the product measure, and we take the product of these measures on $\prod_v E_{n,v}$.

Lemma 3.1. *There are two constants c_1 and c_2 which depend only on K, n and w such that*

$$c_1(X_0 \cdots X_n)^d \leqslant \mathrm{Vol}(\mathcal{C}(\underline{X})) \leqslant c_2(X_0 \cdots X_n)^d$$

for any $(n+1)$-tuple of positive real numbers $\underline{X} = (X_0, X_1, \ldots, X_n)$.

Proof. Since the linear map from $E_{n,w}$ to itself sending a polynomial $P(T)$ to $P(T+\xi)$ has determinant 1, the volume of $\mathcal{C}_w(\underline{X})$ is equal to that of

$$\{P \in E_{n,w}; |P^{(j)}(0)|_w \leqslant X_j \text{ for } j = 0, \ldots, n\} \simeq \prod_{j=0}^{n} \{a \in K_w; |j!a|_w \leqslant X_j\},$$

which in turn is bounded above and below by $c'_w(X_0 \cdots X_n)^d$ and $c''_w(X_0 \cdots X_n)^d$, respectively, for some positive constants c'_w and c''_w depending only on K, n and w. For the other places $v \neq w$, the volume of $\mathcal{C}_v(\underline{X})$ is a positive constant c_v also depending only on K, n and v, with $c_v = 1$ for almost all places. The conclusion follows. □

Lemma 3.2. *Let κ be a positive real number and let $\underline{X} = (X_0, X_1, \dots, X_n)$ be an $(n+1)$-tuple of positive real numbers with*

$$X_0 \cdots X_n \geqslant c_1^{-1/d} (2/\kappa)^{n+1}, \tag{3.1}$$

where c_1 is the constant of Lemma 3.1. Then, $\kappa\mathcal{C}(\underline{X})$ contains a non-zero element of E_n.

Proof. According to Theorem 3 of [BV83], we have

$$\big(\lambda_1(\underline{X}) \cdots \lambda_{n+1}(\underline{X})\big)^d \operatorname{Vol}(\mathcal{C}(\underline{X})) \leqslant 2^{d(n+1)}. \tag{3.2}$$

Since $\lambda_1(\underline{X}) \leqslant \cdots \leqslant \lambda_{n+1}(\underline{X})$ and since $\operatorname{Vol}(\mathcal{C}(\underline{X})) \geqslant (2/\kappa)^{d(n+1)}$ by Lemma 3.1 and condition (3.1), this implies $\lambda_1(\underline{X}) \leqslant \kappa$, as required. □

Note that, for any integer t with $1 \leqslant t \leqslant n$ and any real number $X \geqslant 1$, the condition (3.1) is satisfied with

$$\kappa = 1, \quad X_0 = \cdots = X_{n-t} = cX^{-t/(n+1-t)} \quad \text{and} \quad X_{n-t+1} = \cdots = X_n = X$$

for an appropriate constant c. Then, the corresponding convex body $\mathcal{C}(\underline{X})$ contains a non-zero element of E_n. In other words, for any integer t with $1 \leqslant t \leqslant n$ and any real number $X \geqslant 1$, there exists a non-zero polynomial $Q \in K[T]$ of degree at most n which satisfies $\|Q\|_v \leqslant 1$ at each place v of K distinct from w and also

$$\max_{0 \leqslant j \leqslant n-t} |Q^{(j)}(\xi)|_w \leqslant cX^{-t/(n+1-t)} \quad \text{and} \quad \max_{n-t < j \leqslant n} |Q^{(j)}(\xi)|_w \leqslant X.$$

This justifies the remark made after the statement of Theorem B, on comparing with the conditions (1.2) of that theorem.

Our last objective of this section is to relate the successive minima of a convex $\mathcal{C}(X_0, \dots, X_n)$ with those of $\mathcal{C}(X_n^{-1}, \dots, X_0^{-1})$. We achieve this, following ideas that go back to Mahler (see [Mah39] and § VIII.5 of [Cas71]), by showing that these convex bodies are almost reciprocal with respect to some bilinear form g on E_n. This will require two lemmas. The first one defines this bilinear form g and shows a translation invariance property of it.

Lemma 3.3. *Let $g\colon E_n \times E_n \to K$ be the K-bilinear form given by the formula*

$$g(P, Q) = \sum_{j=0}^{n} (-1)^j P^{(j)}(0) Q^{(n-j)}(0)$$

for any choice of polynomials $P, Q \in E_n$. For each place v of K, denote by $g_v\colon E_{n,v} \times E_{n,v} \to K_v$ the K_v-bilinear form which extends g. Then, for any polynomials $P, Q \in E_{n,w}$, we have

$$g_w(P, Q) = \sum_{j=0}^{n} (-1)^j P^{(j)}(\xi) Q^{(n-j)}(\xi).$$

Proof. For fixed $P, Q \in E_{n,w}$, the polynomial

$$A(T) = \sum_{j=0}^{n} (-1)^j P^{(j)}(T) Q^{(n-j)}(T)$$

has derivative

$$A'(T) = \sum_{j=0}^{n-1} (-1)^j P^{(j+1)}(T) Q^{(n-j)}(T) + \sum_{j=1}^{n} (-1)^j P^{(j)}(T) Q^{(n-j+1)}(T) = 0.$$

So $A(T)$ is a constant. This implies $A(\xi) = A(0) = g_w(P, Q)$. □

Using this we get the following estimate.

Lemma 3.4. *Let* $\underline{X} = (X_0, X_1, \ldots, X_n)$ *and* $\underline{Y} = (Y_0, Y_1, \ldots, Y_n)$ *be* $(n+1)$*-tuples of positive real numbers. Suppose that, for each place* v *of* K*, we are given polynomials* $P_v \in \mathcal{C}_v(\underline{X})$ *and* $Q_v \in \mathcal{C}_v(\underline{Y})$*. Then, with the notation of Lemma 3.3, we have*

$$\prod_v |g_v(P_v, Q_v)|_v \leqslant (n+1)! \max_{0 \leqslant j \leqslant n} X_j Y_{n-j}.$$

Proof. For any place v of K with $v \neq w$, we have, if v is Archimedean,

$$\begin{aligned} |g_v(P_v, Q_v)|_v &\leqslant (n+1)^{d_v/d} \max_{0 \leqslant j \leqslant n} |P_v^{(j)}(0)|_v |Q_v^{(n-j)}(0)|_v \\ &\leqslant ((n+1)!)^{d_v/d} \|P_v\|_v \|Q_v\|_v \\ &\leqslant ((n+1)!)^{d_v/d}, \end{aligned}$$

and, if v is ultrametric,

$$\begin{aligned} |g_v(P_v, Q_v)|_v &\leqslant \max_{0 \leqslant j \leqslant n} |P_v^{(j)}(0)|_v |Q_v^{(n-j)}(0)|_v \\ &\leqslant \|P_v\|_v \|Q_v\|_v \\ &\leqslant 1. \end{aligned}$$

Similarly, if w is Archimedean, the formula of Lemma 3.3 leads to

$$\begin{aligned} |g_w(P_w, Q_w)|_w &\leqslant (n+1)^{d_w/d} \max_{0 \leqslant j \leqslant n} |P_w^{(j)}(\xi)|_w |Q_w^{(n-j)}(\xi)|_w \\ &\leqslant (n+1)^{d_w/d} \max_{0 \leqslant j \leqslant n} X_j Y_{n-j}, \end{aligned}$$

while, if w is non-Archimedean, it gives

$$\begin{aligned} |g_w(P_w, Q_w)|_w &\leqslant \max_{0 \leqslant j \leqslant n} |P_w^{(j)}(\xi)|_w |Q_w^{(n-j)}(\xi)|_w \\ &\leqslant \max_{0 \leqslant j \leqslant n} X_j Y_{n-j}. \end{aligned}$$

The conclusion follows. □

Proposition 3.5. *Let* $\underline{X} = (X_0, X_1, \ldots, X_n)$ *be an* $(n+1)$*-tuple of positive real numbers. Define* $\underline{Y} = (Y_0, \ldots, Y_n)$ *where* $Y_i = X_{n-i}^{-1}$ *for* $i = 0, \ldots, n$*. Then the products*

$$\lambda_i(\underline{X}) \lambda_{n-i+2}(\underline{Y}) \quad (1 \leqslant i \leqslant n+1)$$

are bounded below and above by positive constants that depend only on K*,* n *and* w*.*

Proof. Fix an integer i with $1 \leqslant i \leqslant n+1$. Put $\lambda = \lambda_i(\underline{X})$ and $\mu = \lambda_{n-i+2}(\underline{Y})$. By definition of the successive minima of a convex body, the polynomials of $K[T]$ contained in $\lambda\mathcal{C}(\underline{X})$ generate a subspace U of E_n of dimension $\geqslant i$ while those contained in $\mu\mathcal{C}(\underline{Y})$ generate a subspace V of E_n of dimension $\geqslant n-i+2$. Since the sum of these dimensions is strictly greater than that of E_n and since the bilinear form g of Lemma 3.3 is non-degenerate, it follows that U and V are not orthogonal with respect to g. Thus, there exist non-zero polynomials $P \in \lambda\mathcal{C}(\underline{X})$ and $Q \in \mu\mathcal{C}(\underline{Y})$ which belong to E_n and satisfy $g(P, Q) \neq 0$. For any Archimedean place v of K, we view λ and μ as elements of K_v under the natural embedding of $\mathbb{R}$ in K_v and define $P_v = \lambda^{-1} P$ and $Q_v = \mu^{-1} Q$. For all the other places of K, we put $P_v = P$ and $Q_v = Q$. Then, we have $P_v \in \mathcal{C}_v(\underline{X})$ and $Q_v \in \mathcal{C}_v(\underline{Y})$ for all places v of K, and applying Lemma 3.4 we get

$$\prod_{v \nmid \infty} |g(P, Q)|_v \prod_{v \mid \infty} |g_v(\lambda^{-1} P, \mu^{-1} Q)|_v \leqslant (n+1)!.$$

On noting that, for any Archimedean place v of K, the real numbers λ and μ viewed as elements of K_v satisfy $|\lambda|_v = \lambda^{d_v/d}$ and $|\mu|_v = \mu^{d_v/d}$, we find that the left-hand side of the above inequality is

$$\prod_{v|\infty}(\lambda\mu)^{-d_v/d}\prod_{v}|g(P,Q)|_v = (\lambda\mu)^{-1},$$

by virtue of the product formula applied to the non-zero element $g(P,Q)$ of K. This shows that $\lambda\mu \geqslant ((n+1)!)^{-1}$, and so all products $\lambda_i(\underline{X})\lambda_{n-i+2}(\underline{Y})$ are bounded below by $((n+1)!)^{-1}$, for $i = 1,\dots,n+1$.

On the other hand, applying Theorem 3 of [BV83] to both $\mathcal{C}(\underline{X})$ and $\mathcal{C}(\underline{Y})$ (see (3.2) above), we find

$$\begin{aligned}\prod_{i=1}^{n+1}(\lambda_i(\underline{X})\lambda_{n-i+2}(\underline{Y})) &= \biggl(\prod_{i=1}^{n+1}\lambda_i(\underline{X})\biggr)\biggl(\prod_{i=1}^{n+1}\lambda_i(\underline{Y})\biggr)\\ &\leqslant 4^{n+1}\,\mathrm{Vol}(\mathcal{C}(\underline{X}))^{-1/d}\,\mathrm{Vol}(\mathcal{C}(\underline{Y}))^{-1/d}\\ &\leqslant 4^{n+1}c_1^{-2/d},\end{aligned}$$

where c_1 is the constant of Lemma 3.1. Thus the products $\lambda_i(\underline{X})\lambda_{n-i+2}(\underline{Y})$ are also bounded above by $4^{n+1}c_1^{-2/d}((n+1)!)^n$. □

4. A version of Gel'fond's criterion

Let n, w and ξ be as in the preceding section. In this section, we prove a specialized version of Gel'fond's transcendence criterion which contains Theorem 2b of [DS69] and which we will need in order to conclude the proof of Theorem B. It applies as well to the situation of Lemma 12 in § 10 of [DS69]. For its proof, we need the following estimate (cf. Lemma 1 of [Bro74]).

Lemma 4.1. *Let $P, Q \in K[T]$ be relatively prime non-zero polynomials of degree at most n. Then, we have*

$$1 \leqslant c_3 \max\biggl\{\frac{|P(\xi)|_w}{\|P\|_w}, \frac{|Q(\xi)|_w}{\|Q\|_w}\biggr\}\,\mathrm{H}(P)^{\deg(Q)}\mathrm{H}(Q)^{\deg(P)},$$

where $c_3 = (2n)!$.

Proof. Since P and Q are relatively prime, their resultant $\mathrm{Res}(P,Q)$ is a non-zero element of K. For any place v of K, the usual representation of $\mathrm{Res}(P,Q)$ as a Sylvester determinant leads to the estimate

$$|\mathrm{Res}(P,Q)|_v \leqslant c_v\|P\|_v^{\deg(Q)}\|Q\|_v^{\deg(P)},$$

where $c_v = 1$ if $v \nmid \infty$ and $c_v = ((2n)!)^{d_v/d}$ if $v|\infty$. Arguing as Brownawell in the proof of Lemma 1 of [Bro74], we also find

$$|\mathrm{Res}(P,Q)|_w \leqslant c_w \max\biggl\{\frac{|P(\xi)|_w}{\|P\|_w}, \frac{|Q(\xi)|_w}{\|Q\|_w}\biggr\}\,\|P\|_w^{\deg(Q)}\|Q\|_w^{\deg(P)}$$

with the same value of c_w as above. The conclusion follows by applying these estimates to the product formula $1 = \prod_v |\mathrm{Res}(P,Q)|_v$. □

Theorem 4.2. *Suppose that, for any sufficiently large real number X, there is a non-zero polynomial $P = P_X \in K[T]$ of degree $\leqslant n$ and height $\leqslant X$ such that*

$$\frac{|P(\xi)|_w}{\|P\|_w} \leqslant c_4^{-1}\mathrm{H}(P)^{-n}X^{-\deg(P)},$$

where $c_4 = e^{2n(n+1)}c_3^n$. Then, ξ is algebraic over K of degree $\leqslant n$ and the above polynomials vanish at ξ for any sufficiently large X.

Proof. We first reduce to a situation where we have monic irreducible polynomials. To this end, choose $X_0 \geqslant 1$ such that P_X is defined for any $X \geqslant X_0$. For a fixed $X \geqslant X_0$, write $P = P_X$ in the form $P = aQ_1 \cdots Q_s$, where $a \in K^\times$ is the leading coefficient of P and $Q_1, \dots, Q_s$ are monic irreducible polynomials. Since $\mathrm{H}(a) = 1$, we have $\mathrm{H}(Q_1)\cdots\mathrm{H}(Q_s) \leqslant e^n\mathrm{H}(P)$ (see § 2) and so each Q_i has height at most e^nX. Using this as well as the simple estimate

$$\|P\|_w \leqslant |a|_w \prod_{i=1}^{s}((1+\deg(Q_i))\|Q_i\|_w) \leqslant e^n|a|_w \prod_{i=1}^{s}\|Q_i\|_w,$$

we deduce

$$\prod_{i=1}^{s}\left(\frac{|Q_i(\xi)|_w}{\|Q_i\|_w}\mathrm{H}(Q_i)^n(e^{n+1}X)^{\deg(Q_i)}\right) \leqslant e^{2n(n+1)}\frac{|P(\xi)|_w}{\|P\|_w}\mathrm{H}(P)^nX^{\deg(P)} \leqslant c_3^{-n}.$$

Writing $Y = e^nX$, we conclude that P has at least one monic irreducible factor Q of degree $\leqslant n$ and height $\leqslant Y$ which satisfies

$$\frac{|Q(\xi)|_w}{\|Q\|_w}\mathrm{H}(Q)^n(eY)^{\deg(Q)} \leqslant c_3^{-1}.$$

Fix such a choice of polynomial $Q_Y = Q$ for each $Y \geqslant Y_0 = e^nX_0$. Applying Lemma 4.1 to Q_Y and $Q_{Y'}$ for values of Y and Y' satisfying $e^nX_0 \leqslant Y \leqslant Y' < eY$, we find that these polynomials are not relatively prime. Being monic and irreducible, they are therefore equal to each other. So, we have more generally that $Q_Y = Q_{Y_0}$ for any $Y \geqslant Y_0$. As $|Q_Y(\xi)|_w/\|Q_Y\|_w$ is bounded above by $c_3^{-1}(eY)^{-1}$ which tends to 0 as Y goes to infinity, this ratio must be 0 independently of $Y \geqslant Y_0$. This gives $Q_Y(\xi) = 0$ for any $Y \geqslant Y_0$ and therefore $P_X(\xi) = 0$ for any $X \geqslant X_0$. □

5. A height estimate

Here we establish a height estimate which, in our application, will play the role of Theorem 3 of [DS69]. Again, we start with a lemma.

Lemma 5.1. *Let $\ell \geqslant 0$ be an integer and let $x_0, \dots, x_\ell$ be indeterminates. For any integer $k \geqslant 1$, the set $\mathbb{Z}[x_0, \dots, x_\ell]_k$ of homogeneous polynomials of $\mathbb{Z}[x_0, \dots, x_\ell]$ of degree k is generated, as a $\mathbb{Z}$-module, by the minors of order k of the $k \times (k+\ell)$ matrix*

$$R(k,\ell) = \begin{pmatrix} x_0 & x_1 & \dots & x_\ell & 0 & \dots & 0 \\ 0 & x_0 & x_1 & \dots & x_\ell & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & 0 & x_0 & x_1 & \dots & x_\ell \end{pmatrix} \quad \Bigg\} \quad k \text{ rows.}$$

Proof. We proceed by induction on $k+\ell$. If $k=1$ or $\ell=0$ the result is clear. Assume $k \geqslant 2$ and $\ell \geqslant 1$ and that the result is true for a smaller number of rows or a smaller number of indeterminates. Denote by M the subgroup of $\mathbb{Z}[x_0, \dots, x_\ell]_k$ generated by the minors of order k of the matrix $R(k,\ell)$. The ring homomorphism φ from $\mathbb{Z}[x_0, \dots, x_\ell]$ to $\mathbb{Z}[x_0, \dots, x_{\ell-1}]$ sending x_ℓ to 0 and all other indeterminates to themselves maps M onto the subgroup of $\mathbb{Z}[x_0, \dots, x_{\ell-1}]_k$ generated by the minors of order k of $R(k,\ell-1)$. Thus, by the induction hypothesis, we have

$$\varphi(M) = \mathbb{Z}[x_0, \dots, x_{\ell-1}]_k.$$

On the other hand, the determinants of the $k \times k$ sub-matrices which contain the last column of $R(k,\ell)$ are the products $x_\ell d$ where d is a minor of order $k-1$ of $R(k-1,\ell)$. Thus, by the induction hypothesis, we also have

$$M \supseteq x_\ell\mathbb{Z}[x_0, \dots, x_\ell]_{k-1} = \mathbb{Z}[x_0, \dots, x_\ell]_k \cap \ker(\varphi).$$

These properties imply $M = \mathbb{Z}[x_0, \dots, x_\ell]_k$. □

PROPOSITION 5.2. *Let k and ℓ be integers with $k \geqslant 1$ and $\ell \geqslant 0$. For any $P \in E_\ell$, we have*

$$c^{-1}\mathrm{H}(P)^k \leqslant \mathrm{H}(P \cdot E_{k-1}) \leqslant c\mathrm{H}(P)^k,$$

where c is a positive constant depending only on k and ℓ and where $P \cdot E_{k-1}$ denotes the subspace of $E_{k+\ell-1}$ consisting of all products PQ with $Q \in E_{k-1}$.

Proof. Write $P = a_0 + a_1T + \cdots + a_\ell T^\ell$. Then the height of $P \cdot E_{k-1}$ is simply the height of the matrix with k rows

$$R = \begin{pmatrix} a_0 & a_1 & \dots & a_\ell & & 0 \\ & \ddots & \ddots & & \ddots & \\ 0 & & a_0 & a_1 & \dots & a_\ell \end{pmatrix}.$$

By virtue of the preceding lemma, every monomial of degree k in $a_0, \dots, a_\ell$ can be expressed as a linear combination of the minors of order k of this matrix with integral coefficients that do not depend on P. Conversely, the minors of order k of R can be written as linear combinations of monomials of degree k in $a_0, \dots, a_\ell$ with integral coefficients that do not depend on P. Thus, for each place v of K, we have $c_v^{-1}\|R\|_v \leqslant \|P\|_v^k \leqslant c_v\|R\|_v$ for some constant $c_v \geqslant 1$ independent of P, with $c_v = 1$ when v is not Archimedean. The conclusion follows with $c = \prod_{v|\infty} c_v$. □

6. Construction of a polynomial

Let n, w and ξ be as in § 3. We fix a non-decreasing sequence of positive real numbers $X_0 \leqslant \cdots \leqslant X_n$ and assume that the corresponding convex body $\mathcal{C}(X_0, \dots, X_n)$ contains a non-zero polynomial Q of $K[T]$. Let

$$V = \{P \in E_n; g(P, Q) = 0\},$$

where $g\colon E_n \times E_n \to K$ is the K-bilinear form of Lemma 3.3. For each integer ℓ with $0 \leqslant \ell \leqslant n$, we define a K-bilinear form $B_\ell\colon E_\ell \times E_{n-\ell} \to K$ by the formula

$$B_\ell(F, G) = g(FG, Q)$$

for $F \in E_\ell$ and $G \in E_{n-\ell}$. Its right kernel is

$$V_\ell = \{G \in E_{n-\ell}; G \cdot E_\ell \subseteq V\}.$$

We also denote by $B_{\ell,w}\colon E_{\ell,w} \times E_{n-\ell,w} \to K_w$ the K_w-bilinear form which extends B_ℓ. Finally, we put

$$y_i = (-1)^i i! Q^{(n-i)}(0) \quad \text{and} \quad z_i = (-1)^i i! Q^{(n-i)}(\xi) \quad (0 \leqslant i \leqslant n),$$

and, for each integer $\ell = 0, 1, \dots, n$, we define

$$M_\ell = \begin{pmatrix} y_0 & y_1 & \cdots & y_{n-\ell} \\ y_1 & y_2 & \cdots & y_{n-\ell+1} \\ \vdots & \vdots & & \vdots \\ y_\ell & y_{\ell+1} & \cdots & y_n \end{pmatrix} \quad \text{and} \quad N_\ell = \begin{pmatrix} z_0 & z_1 & \cdots & z_{n-\ell} \\ z_1 & z_2 & \cdots & z_{n-\ell+1} \\ \vdots & \vdots & & \vdots \\ z_\ell & z_{\ell+1} & \cdots & z_n \end{pmatrix}.$$

With this notation, we will prove below a series of lemmas leading, under some condition on $X_0, \dots, X_n$, to the construction of a polynomial $P \in K[T]$ with several properties. The method overall follows that of Davenport and Schmidt [DS69, §§ 7–9]. The first lemma is the following observation.

LEMMA 6.1. *Fix an integer ℓ with $0 \leqslant \ell \leqslant n$. Then,*

i) *M_ℓ is the matrix of B_ℓ relative to the bases $\{1, T, \dots, T^\ell\}$ of E_ℓ and $\{1, T, \dots, T^{n-\ell}\}$ of $E_{n-\ell}$;*

ii) *N_ℓ is the matrix of $B_{\ell,w}$ relative to the basis $\{1, T-\xi, \dots, (T-\xi)^\ell\}$ of $E_{\ell,w}$ and the basis $\{1, T-\xi, \dots, (T-\xi)^{n-\ell}\}$ of $E_{n-\ell,w}$.*

Proof. This follows upon noting that, for $i = 0, \dots, \ell$ and $j = 0, \dots, n-\ell$, we have

$$B_\ell(T^i, T^j) = g(T^{i+j}, Q(T)) = y_{i+j}$$

and, by Lemma 3.3,

$$B_{\ell,w}((T-\xi)^i, (T-\xi)^j) = g_w((T-\xi)^{i+j}, Q(T)) = z_{i+j}. \qquad \square$$

In particular, this result implies that M_ℓ and N_ℓ have the same rank for any value of ℓ. Note that the number of rows of these matrices is less than or equal to their number of columns if and only if $\ell \leqslant n/2$. Under this hypothesis, we have the following estimates.

Lemma 6.2. *There are constants $c_5, c_6, c_7 \geqslant 1$ depending only on K, n, w and ξ such that, for any integer ℓ with $0 \leqslant \ell \leqslant n/2$, we have*

i) $\|N_\ell\|_w \leqslant c_5 X_{n-\ell} \cdots X_n$,
ii) $c_6^{-1}\|N_\ell\|_w \leqslant \|M_\ell\|_w \leqslant c_6\|N_\ell\|_w$,
iii) $\mathrm{H}(M_\ell) \leqslant c_7\|N_\ell\|_w$ *when M_ℓ has rank $\ell+1$.*

Proof. i) The upper bound on $\|N_\ell\|_w$ follows from the fact that, for $i = 1, \dots, \ell+1$, all the elements of the ith row of N_ℓ have their absolute value bounded above by a constant times X_{n+1-i}.

ii) By Lemma 6.1, M_ℓ and N_ℓ are matrices of $B_{\ell,w}$ corresponding to different choices of bases for $E_{\ell,w}$ and $E_{n-\ell,w}$. Accordingly, we have $M_\ell = {}^{\mathrm{t}}U N_\ell V$, where U and V are matrices of change of bases which depend only on ξ, ℓ and n. Since U and V are invertible, this implies that any minor of order $\ell+1$ of M_ℓ (respectively N_ℓ) can be expressed as a linear combination of the minors of order $\ell+1$ of N_ℓ (respectively M_ℓ) with coefficients that are independent of Q, and the second assertion follows.

iii) At any place v of K with $v \neq w$, the elements of M_ℓ have their absolute value bounded above by a constant which depends only on n and which can be taken to be 1 when $v \nmid \infty$. So, the same is true of $\|M_\ell\|_v$. The height of M_ℓ is thus bounded above by a constant times $\|M_\ell\|_w$ or, according to assertion ii, by a constant times $\|N_\ell\|_w$. $\square$

Lemma 6.3. *For any integer ℓ with $0 \leqslant \ell \leqslant n$, we have*

$$\dim V_\ell = n - \ell + 1 - \mathrm{rank}(M_\ell).$$

When M_ℓ has rank $\ell+1$, we also have $\mathrm{H}(V_\ell) = \mathrm{H}(M_\ell)$.

Proof. A polynomial $P = a_0 + a_1 T + \cdots + a_{n-\ell}T^{n-\ell}$ of $E_{n-\ell}$ belongs to V_ℓ if and only if, for $i = 0, \dots, \ell$, it satisfies

$$0 = g(T^i P(T), Q(T)) = B_\ell(T^i, P(T)) = \sum_{j=0}^{n-\ell} y_{i+j} a_j.$$

Thus, identifying $E_{n-\ell}$ with $K^{n-\ell+1}$ in the usual way, the subspace V_ℓ of $E_{n-\ell}$ is identified with the solution space of the homogeneous system associated to M_ℓ. This proves the formula for $\dim V_\ell$. Moreover, if M_ℓ has rank $\ell+1$, then, according to the duality principle mentioned in § 2, we have $\mathrm{H}(V_\ell) = \mathrm{H}(M_\ell)$. $\square$

Lemma 6.4. *Suppose that there exists an integer h with $1 \leqslant h \leqslant n/2$ such that M_{h-1} has rank h and M_h has rank $\leqslant h$. Then, V_{n-h} contains a non-zero element P. Such a polynomial P has degree $\leqslant h$ and satisfies $P \cdot E_{n-2h+1} = V_{h-1}$. In particular, P divides any polynomial of V_{h-1}.*

Proof. Since M_{n-h} is the transpose of M_h, the two matrices have the same rank. By Lemma 6.3, this gives

$$\dim V_{n-h} = (h+1) - \mathrm{rank}(M_{n-h}) \geqslant 1.$$

So, V_{n-h} contains a non-zero element P. Using Lemma 6.3, we also find

$$\dim V_{h-1} = (n-h+2) - \operatorname{rank}(M_{h-1}) = n-2h+2.$$

Since V_{h-1} contains $P \cdot E_{n-2h+1}$, and since the latter subspace of E_{n-h+1} also has dimension $n-2h+2$, this inclusion is an equality. □

LEMMA 6.5. *Let ℓ and t be integers with $0 \leqslant \ell < n/2$ and $1 \leqslant t \leqslant n-2\ell$. Suppose that N_ℓ has rank $\ell+1$ and that there exists a non-zero polynomial $P \in K[T]$ such that $P \cdot E_{t-1} \subseteq V_\ell$. Then, we have*

$$\left(\frac{|P(\xi)|_w}{\|P\|_w}\right)^t \ll \frac{X_{n-t-\ell} \cdots X_{n-t}}{\|N_\ell\|_w}.$$

Proof. Denote by $\mathbf{z}_0, \ldots, \mathbf{z}_{n-\ell}$ the columns of N_ℓ and, for each integer s with $1 \leqslant s \leqslant t+1$, denote by $N_\ell^{(s)}$ the sub-matrix of N_ℓ consisting of the columns $\mathbf{z}_{s-1}, \ldots, \mathbf{z}_{n-\ell}$. Observe that, since $t \leqslant n-2\ell$, these matrices all have at least $\ell+1$ columns. Write

$$P = b_0 + b_1(T-\xi) + \cdots + b_h(T-\xi)^h,$$

where h is the degree of P. For any integer s as above, we have $(T-\xi)^{s-1}P(T) \in V_\ell$ and so, for $i = 0, \ldots, \ell$, we find

$$0 = B_{\ell,w}((T-\xi)^i, (T-\xi)^{s-1}P(T)) = \sum_{j=0}^{h} z_{i+s-1+j} b_j.$$

This means that the columns of N_ℓ satisfy the recurrence relation

$$b_0\mathbf{z}_{s-1} + b_1\mathbf{z}_s + \cdots + b_h\mathbf{z}_{s-1+h} = 0 \quad (1 \leqslant s \leqslant t).$$

Now, fix an integer s with $1 \leqslant s \leqslant t$ and choose indices $j_0, j_1, \ldots, j_\ell$ satisfying the inequalities $s-1 \leqslant j_0 < j_1 < \cdots < j_\ell \leqslant n-\ell$ such that

$$\|N_\ell^{(s)}\|_w = |\det(\mathbf{z}_{j_0}, \ldots, \mathbf{z}_{j_\ell})|_w. \tag{6.1}$$

If $j_0 = s-1$, we find, using the recurrence relation, that

$$\begin{aligned}
|P(\xi)|_w \|N_\ell^{(s)}\|_w &= |\det(b_0\mathbf{z}_{s-1}, \mathbf{z}_{j_1}, \ldots, \mathbf{z}_{j_\ell})|_w \\
&= \left|\det\left(-\sum_{j=1}^{h} b_j\mathbf{z}_{s-1+j}, \mathbf{z}_{j_1}, \ldots, \mathbf{z}_{j_\ell}\right)\right|_w \\
&= \left|\sum_{j=1}^{h} b_j \det(\mathbf{z}_{s-1+j}, \mathbf{z}_{j_1}, \ldots, \mathbf{z}_{j_\ell})\right|_w \\
&\leqslant c\|P\|_w \|N_\ell^{(s+1)}\|_w
\end{aligned}$$

for some positive constant c depending only on n and $|\xi|_w$. If $j_0 \geqslant s$, this is still true because (6.1) then implies $\|N_\ell^{(s)}\|_w \leqslant \|N_\ell^{(s+1)}\|_w$. Since $\|N_\ell^{(1)}\|_w = \|N_\ell\|_w \neq 0$, this inequality implies by induction on s that we have $\|N_\ell^{(s)}\|_w \neq 0$ for $s = 1, \ldots, t+1$, and therefore we can write

$$\frac{|P(\xi)|_w}{\|P\|_w} \leqslant c\frac{\|N_\ell^{(s+1)}\|_w}{\|N_\ell^{(s)}\|_w} \quad (1 \leqslant s \leqslant t).$$

Multiplying term by term these inequalities, we get

$$\left(\frac{|P(\xi)|_w}{\|P\|_w}\right)^t \leqslant c^t \frac{\|N_\ell^{(t+1)}\|_w}{\|N_\ell\|_w},$$

and the conclusion follows upon noting that, for $i = 1, \ldots, \ell+1$, the ith row of $N_\ell^{(t+1)}$ has norm $\ll X_{n-t-i+1}$ and thus $\|N_\ell^{(t+1)}\|_w \ll X_{n-t-\ell} \cdots X_{n-t}$. □

Proposition 6.6. *Let k be an integer with $1 \leqslant k \leqslant n/2$. Assume that there is an integer t with $1 \leqslant t \leqslant n+2-2k$ such that*

$$X_0 \leqslant \cdots \leqslant X_{n-t} < 1 \quad \text{and} \quad 1 \leqslant X_{n-t+1} \leqslant \cdots \leqslant X_n.$$

Put $\delta = X_{n-t}$ and $Y = X_{n-t+1} \cdots X_n$, and assume moreover that

$$Y\delta^{k+1-t} < (c_5c_7)^{-1}, \tag{6.2}$$

where c_5 and c_7 are defined in Lemma 6.2. Then there exists an integer h with $1 \leqslant h \leqslant k$ and a non-zero polynomial $P \in K[T]$ of degree $\leqslant h$ and height $\ll \delta^{-k/n}$ which divides any polynomial of V_{h-1} and satisfies

$$\left(\frac{|P(\xi)|_w}{\|P\|_w}\right)^t \leqslant c_8\delta^h \mathrm{H}(P)^{-(n+2-2h)}, \tag{6.3}$$

where c_8 is a constant depending only on K, n, w and ξ.

Proof. For any integer ℓ for which M_ℓ has rank $\ell+1$, we find, using Lemma 6.2,

$$\mathrm{H}(M_\ell) \leqslant c_7\|N_\ell\|_w \leqslant c_5c_7X_{n-\ell}\cdots X_n \leqslant c_5c_7Y\delta^{\ell+1-t}. \tag{6.4}$$

Since we also have $\mathrm{H}(M_\ell) \geqslant 1$ for these values of ℓ, the assumption (6.2) implies that M_k has rank $\leqslant k$. The rank of M_0 being 1, we conclude that there exists an integer h with $1 \leqslant h \leqslant k$ such that M_{h-1} has rank h and M_h has rank $\leqslant h$. Then, according to Lemma 6.4, there exists a non-zero polynomial $P \in E_h$ such that $P \cdot E_{n-2h+1} = V_{h-1}$. This implies that P divides any polynomial of V_{h-1} and, by Proposition 5.2, that

$$\mathrm{H}(P)^{n+2-2h} \ll \mathrm{H}(V_{h-1}) \ll \mathrm{H}(P)^{n+2-2h}. \tag{6.5}$$

Combining Lemma 6.3 with (6.2) and (6.4) (for $\ell = h-1$), we also find

$$\mathrm{H}(V_{h-1}) = \mathrm{H}(M_{h-1}) \leqslant c_5c_7Y\delta^{h-t} < \delta^{-(k+1-h)}. \tag{6.6}$$

Note that, since $k \leqslant n/2$, the ratio $(k+1-h)/(n+2-2h)$ is a decreasing function of h in the range $1 \leqslant h \leqslant k$. So, it is bounded above by k/n. Combining this observation with the above estimates (6.5) and (6.6), we get

$$\mathrm{H}(P) \ll \delta^{-(k+1-h)/(n+2-2h)} \ll \delta^{-k/n}. \tag{6.7}$$

Since $t \leqslant n+2-2k$, we have $P \cdot E_{t-1} \subseteq P \cdot E_{n-2h+1} \subseteq V_{h-1}$ and applying Lemma 6.5 with $\ell = h-1$ gives

$$\left(\frac{|P(\xi)|_w}{\|P\|_w}\right)^t \ll \frac{\delta^h}{\|N_{h-1}\|_w}.$$

Moreover, Lemma 6.2 part iii, Lemma 6.3 and (6.5) provide

$$\|N_{h-1}\|_w \geqslant c_7^{-1}\mathrm{H}(M_{h-1}) = c_7^{-1}\mathrm{H}(V_{h-1}) \gg \mathrm{H}(P)^{n+2-2h},$$

and the conclusion follows. □

In our application, we will simply need the following consequence of this proposition.

Corollary 6.7. *Assume that all the hypotheses of Proposition 6.6 are satisfied and that we have $\delta < c_8^{-1}$. Then there exists an irreducible polynomial $P \in K[T]$ which divides any polynomial of V_{k-1} and satisfies*

$$\left(\frac{|P(\xi)|_w}{\|P\|_w}\right)^t \leqslant c_9\delta^{\deg(P)} \mathrm{H}(P)^{-(n+2-2k)}, \tag{6.8}$$

where $c_9 = \max\{1, e^{n^2}c_8\}$.

Proof. Let h and P be as in the conclusion of Proposition 6.6. Since $\mathrm{H}(P) \geqslant 1$, the right-hand side of (6.3) is bounded above by $c_8\delta^h \leqslant c_8\delta < 1$. So P cannot be a constant. Moreover, since $\deg(P) \leqslant h \leqslant k$, the same inequality (6.3) gives

$$\left(\frac{|P(\xi)|_w}{\|P\|_w}\right)^t \leqslant c_8\delta^{\deg(P)}\mathrm{H}(P)^{-(n+2-2k)}.$$

Write P as a product $P = P_1 \cdots P_s$ of irreducible polynomials of $K[T]$. Then the above inequality leads to

$$\prod_{i=1}^{s}\left(\left(\frac{|P_i(\xi)|_w}{\|P_i\|_w}\right)^t \delta^{-\deg(P_i)}\mathrm{H}(P_i)^{n+2-2k}\right) \leqslant e^{n^2}c_8 \leqslant c_9^s.$$

So, at least one factor of the product on the left must be bounded above by c_9. The corresponding polynomial P_i divides every element of V_{k-1} since it divides P and V_{k-1} is contained in V_{h-1}. □

Note that this statement provides no upper bound on the degree and height of P. We will get such upper bounds by an indirect argument, using the construction of an auxiliary polynomial in the next section.

7. Degree and height estimates

The notation is as in the preceding section. We assume that the adelic convex body $\mathcal{C}(X_0, \dots, X_n)$ contains a non-zero polynomial Q of $K[T]$ for some non-decreasing sequence of positive real numbers $X_0 \leqslant \cdots \leqslant X_n$, and we define corresponding subspaces V_ℓ of $E_{n-\ell}$ for $\ell = 0, \dots, n$ as in § 6.

Lemma 7.1. *Put $c = ((n+1)!)^{-2}$. Then, for any integer ℓ with $0 \leqslant \ell \leqslant n$ we have*

$$\mathcal{C}(cX_n^{-1}, \dots, cX_\ell^{-1}) \cap E_{n-\ell} \subseteq V_\ell. \tag{7.1}$$

Proof. Let ℓ be an integer with $0 \leqslant \ell \leqslant n$, and let G be an element of the set on the left-hand side of (7.1). We need to show that $g(T^mG, Q) = 0$ for $m = 0, \dots, \ell$. To this end, we proceed by induction. We fix an integer m with $0 \leqslant m \leqslant \ell$ and assume, when $m \geqslant 1$, that we have $g(T^jG, Q) = 0$ for $j = 0, \dots, m-1$. Let $P = T^mG(T)$. We define $P_w = (T-\xi)^mG(T)$ and $Q_w = Q$ and, for the other places $v \neq w$ of K, we put $P_v = P$ and $Q_v = Q$. These polynomials satisfy $P_v \in \mathcal{C}_v(\underline{Y})$ and $Q_v \in \mathcal{C}_v(\underline{X})$ for each place v of K, where $\underline{Y} = (Y_0, \dots, Y_n)$ denotes the $(n+1)$-tuple of positive real numbers given by $Y_i = n!cX_{n-i}^{-1}$ for $i = 0, \dots, n$. Moreover, the hypotheses imply

$$g_w(P_w, Q_w) = g(P, Q),$$

since the difference $P_w - P$ can be written as a linear combination of $G, \dots, T^{m-1}G$ with coefficients in K_w in the case $m \geqslant 1$ and is zero when $m = 0$. Using Lemma 3.4, we therefore get

$$\prod_v |g(P,Q)|_v = \prod_v |g_v(P_v, Q_v)|_v \leqslant (n+1)!n!c < 1.$$

By the product formula, this implies $g(P, Q) = 0$. □

Proposition 7.2. *There is a constant $c_{10} > 0$ which depends only on K, n, w and ξ and has the following property. Suppose that ℓ and u are non-negative integers with $\ell + u < n$, such that*

$$X_n^{u+1}X_{n-1} \cdots X_{\ell+u} \leqslant c_{10}. \tag{7.2}$$

Then, there is a non-zero polynomial G of $K[T]$ of degree $\leqslant n - \ell$ and height $\ll X_{\ell+u}^{-1}$ such that $G^{(i)} \in V_\ell$ for $i = 0, \dots, u$.

Proof. Let c be as in Lemma 7.1. Put $\kappa = (n!)^{-1}$ and define real numbers $Y_0, \dots, Y_{n-\ell}$ by

$$Y_i = \begin{cases} cX_n^{-1} & \text{for } i = 0, \dots, u, \\ cX_{n-i+u}^{-1} & \text{for } i = u+1, \dots, n-\ell. \end{cases}$$

Lemma 3.2 shows that the convex $\kappa\mathcal{C}(Y_0, \dots, Y_{n-\ell})$ contains a non-zero element G of $E_{n-\ell}$ if the condition (7.2) is satisfied for a sufficiently small constant $c_{10} > 0$. Such a polynomial has height $\mathrm{H}(G) \ll Y_{n-\ell} \ll X_{\ell+u}^{-1}$. Moreover, for $i = 0, \dots, u$, we find

$$G^{(i)} \in \mathcal{C}(Y_i, \dots, Y_{n-\ell}) \subseteq \mathcal{C}(cX_n^{-1}, \dots, cX_\ell^{-1}),$$

and so $G^{(i)} \in V_\ell$ by Lemma 7.1. □

We will apply this proposition in the following context.

Corollary 7.3. *Let ℓ and u be as in Proposition 7.2, and assume that there exists an irreducible polynomial $P \in K[T]$ which divides every element of V_ℓ. Then, we have*

$$\deg(P) \leqslant \frac{n-\ell}{u+1} \quad \textit{and} \quad \mathrm{H}(P) \ll X_{\ell+u}^{-1/(u+1)}.$$

Proof. The hypotheses imply that P divides all derivatives of the polynomial G of Proposition 7.2, up to order u. So, P^{u+1} divides G and the conclusion follows. □

8. Proof of Theorem B

Let the notation be as in Theorem B (stated in § 1) and assume that the hypothesis of this theorem holds with a constant $c < \min\{1, (c_5c_7)^{-1}\}$. Then, for any real number $X \geqslant 1$ the condition (6.2) of Proposition 6.6 is satisfied with

$$\delta = X_0 = X_1 = \cdots = X_{n-t} = cX^{-t/(k+1-t)} \quad \text{and} \quad X_{n-t+1} = \cdots = X_n = X.$$

Moreover, if X is sufficiently large, the hypothesis of Theorem B is that the corresponding convex $\mathcal{C}(\underline{X})$ with $\underline{X} = (X_0, \dots, X_n)$ contains a non-zero element Q of E_n. Since $t \leqslant n + 2 - 2k$, we may then apply Corollary 6.7. It shows that, if X is sufficiently large so that $\delta < c_8^{-1}$, then there is an irreducible polynomial $P \in K[T]$ which divides every element of the vector space V_{k-1} attached to Q and satisfies

$$\frac{|P(\xi)|_w}{\|P\|_w} \ll \mathrm{H}(P)^{-(n+2-2k)/t} \delta^{\deg(P)/t}.$$

Since $c \leqslant 1$ and $n - t \geqslant 2t + k - 2$, we also find

$$X_n^{2t} X_{n-1} \cdots X_{2t+k-2} = X^{3t-1} \delta^{n-3t-k+3} \leqslant X^{3t-1} \delta^{3k-3t+3} \leqslant X^{-1}.$$

So, the condition (7.2) of Proposition 7.2 is satisfied with $\ell = k-1$ and $u = 2t-1$ provided that X is sufficiently large. Assuming that this is the case, Corollary 7.3 then shows that

$$\deg(P) \leqslant \frac{n-k+1}{2t} \quad \text{and} \quad \mathrm{H}(P) \leqslant \kappa\delta^{-1/(2t)}$$

for some constant $\kappa > 0$. Putting $m = [(n-k+1)/(2t)]$ and $Y = \kappa\delta^{-1/(2t)}$, and noting that $(n+2-2k)/t \geqslant m$, we thus have found the existence of a polynomial $P \in K[T]$ of degree $\leqslant m$ and height $\leqslant Y$ such that

$$\frac{|P(\xi)|_w}{\|P\|_w} \ll \mathrm{H}(P)^{-m} Y^{-2\deg(P)}.$$

Since Y is a monotone increasing unbounded continuous function of X, for $X \geqslant 1$, Theorem 4.2 then shows that ξ is algebraic over K of degree $\leqslant m$. This completes the proof.

9. Proof of Theorem A

We first generalize the construction of Davenport and Schmidt [DS69, § 2].

Lemma 9.1. *Let t be an integer with $1 \leqslant t \leqslant n$ and let δ, κ and Y be real numbers satisfying $0 < \delta < 1 < Y$ and $\kappa \geqslant 1$. Assume that $\underline{Y} = (Y_0, \dots, Y_n)$ is an $(n+1)$-tuple of positive real numbers satisfying*

$$\lambda_{n+1}(\underline{Y}) \leqslant \kappa \quad \text{and} \quad Y_j \leqslant \begin{cases} Y\delta^{t-j} & \text{for } j = 0, \dots, t-1, \\ Y & \text{for } j = t, \dots, n. \end{cases}$$

Assume moreover that $|\xi|_w \leqslant 1$ in the case where w is ultrametric. Then there exists a monic polynomial $P \in \mathcal{O}_K[T]$ which is irreducible over K of degree $n+1$, has height $\mathrm{H}(P) \ll \kappa Y$ (as defined in § 2), admits d distinct conjugates over $\mathbb{Q}$, and has at least t distinct roots in the closed disk of K_w centered at ξ of radius δ.

Proof. Let ϵ be a fixed but arbitrarily small positive real number with $\epsilon \leqslant 1$. Put $\delta_0 = \min\{\delta, \epsilon\}$ and choose elements $P_1, \dots, P_{n+1}$ in E_n realizing the successive minima of $\mathcal{C}(\underline{Y})$ in E_n. Since we have $\lambda_{n+1}(\underline{Y}) \leqslant \kappa$, these polynomials all belong to $\kappa\mathcal{C}(\underline{Y})$. In particular, they have integral coefficients at any ultrametric place v of K distinct from w. Moreover, they form a basis of E_n over K. We will construct the required polynomial P in the form

$$P(T) = T^{n+1} + \sum_{i=1}^{n+1} b_i P_i(T)$$

for suitable elements $b_1, \dots, b_{n+1}$ of K. Each b_i will be obtained as the solution of a system of inhomogeneous inequalities using the strong approximation theorem (see Theorem 3, p. 440 of [Mah64] or § 15 of [Cas67]). According to this result, there is a constant $C > 0$ depending only on K with the following property. For any finite set $\mathcal{S}$ of places of K, any choice of elements $\beta_v \in K_v$ $(v \in \mathcal{S})$, and any choice of positive real numbers ϵ_v $(v \in \mathcal{S})$, with $\prod_{v\in\mathcal{S}} \epsilon_v \geqslant C$, there exists an element b of K satisfying $|b - \beta_v|_v \leqslant \epsilon_v$ for $v \in \mathcal{S}$ and $|b|_v \leqslant 1$ for $v \notin \mathcal{S}$.

To ensure that P is irreducible over K and admits d distinct conjugates over $\mathbb{Q}$, we proceed essentially as Bugeaud and Teulié in [BT00]. We choose a prime number q of $\mathbb{Z}$ which splits completely in $\mathcal{O}_K$ into a product of d distinct prime ideals none of which defines the place w. We fix a place v_0 among the corresponding d places of K above q and we choose an element π of K satisfying $|\pi|_{v_0} = |q|_{v_0}$ and $|\pi|_v = 1$ for $v|q$ with $v \neq v_0$. We write

$$\pi = \sum_{i=1}^{n+1} \gamma_i P_i(T)$$

with $\gamma_1, \dots, \gamma_{n+1} \in K$ and we ask that

$$|b_i - \gamma_i|_v \leqslant |q|_v^2 = q^{-2/d} \quad (v|q,\ 1 \leqslant i \leqslant n+1). \tag{9.1}$$

Under these conditions, the corresponding polynomial P satisfies

$$\|P(T) - T^{n+1} - \pi\|_v = \left\| \sum_{i=1}^{n+1} (b_i - \gamma_i) P_i(T) \right\|_v \leqslant |q|_v^2$$

for $v|q$. Thus, P has integral coefficients at the places of K above q. Since π is a uniformizing parameter for v_0, the above relation implies that P is an Eisenstein polynomial of $K[T]$ at v_0 and thus it is irreducible over K (see for instance Theorem 24 in § 3, Chapter III of [FT93]). Moreover this relation also gives $|P(0)|_{v_0} < 1$ and $|P(0)|_v = 1$ for $v|q$ with $v \neq v_0$. Thus the constant coefficient $P(0)$ of P admits d distinct conjugates over $\mathbb{Q}$.

To ensure that P has t roots close to ξ in K_w, we fix a monic polynomial $B \in K_w[T]$ of degree t with t (simple) distinct roots in the open unit disk $D_w = \{z \in K_w; |z|_w < 1\}$ of K_w and we use the fact that, by explicit forms of the inverse function theorem such as Theorem 4.4.1 in Chapter I of [Car77], any polynomial $S(T) \in K_w[T]$ of degree $\leqslant n+1$ for which $\|S - B\|_w$ is sufficiently small also has t distinct roots in D_w. We proceed as follows.

If w is ultrametric, lying above an ordinary prime number p, we choose an element r of K_w with $p^{-1}\delta_0 \leqslant |r|_w \leqslant \delta_0$ and put $s = r^t$. If w is Archimedean, we choose $r, s \in K_w$ with $|r|_w = \delta_0$ and $|s|_w = \kappa^{d_w/d}\epsilon^{-t-2}\delta_0^t Y$. In both cases, we define

$$R(T) = (T-\xi)^{n+1} + sB\left(\frac{T-\xi}{r}\right) \in K_w[T].$$

We write this polynomial in the form

$$R(T) = T^{n+1} + \sum_{i=1}^{n+1} \theta_i P_i(T)$$

with $\theta_1, \dots, \theta_{n+1} \in K_w$ and ask that

$$|b_i - \theta_i|_w \leqslant \begin{cases} \epsilon^{-1} & \text{if } w \text{ is Archimedean,} \\ \epsilon^{n+1}Y^{-1} & \text{if } w \text{ is ultrametric.} \end{cases} \tag{9.2}$$

The polynomial $S = s^{-1}P(rT+\xi)$ then satisfies

$$\|S - B\|_w = \left\| s^{-1}r^{n+1}T^{n+1} + s^{-1}\sum_{i=1}^{n+1}(b_i - \theta_i)P_i(rT+\xi)\right\|_w \ll \epsilon,$$

using $|s|_w^{-1}|r|_w^{n+1} \ll \delta_0 \ll \epsilon$ and noting that, for $i = 1, \dots, n+1$, we have

$$\|P_i(rT+\xi)\|_w \ll \begin{cases} \kappa^{d_w/d}\delta^t Y & \text{if } w \text{ is Archimedean,} \\ \delta^t Y & \text{if } w \text{ is ultrametric.} \end{cases}$$

If ϵ is sufficiently small, this implies that S has t roots in the disk D_w and, therefore, that P has at least t distinct roots in the disk of K_w centered at ξ with radius δ.

If w is Archimedean and again if ϵ is small enough, the strong approximation theorem allows us to require, aside from (9.1) and (9.2), that

$$|b_i|_v \leqslant 1 \quad (1 \leqslant i \leqslant n+1), \tag{9.3}$$

for all places v of K with $v \neq w$ and $v \nmid q$. Then P has integral coefficients at v for each ultrametric place v of K and therefore it has coefficients in $\mathcal{O}_K$. Moreover, as we may take $\epsilon \gg 1$, we find $\|P\|_w \ll \kappa^{d_w/d}\epsilon^{-t-2}Y \ll \kappa^{d_w/d}Y$. Since $\|P\|_v \ll \kappa^{d_v/d}$ for all the other Archimedean places v of K, this implies $\mathrm{H}(P) \ll \prod_{v|\infty}\|P\|_v \ll \kappa Y$.

If w is ultrametric, we choose an Archimedean place v_1. We require that (9.1) and (9.2) hold, that (9.3) holds for all places v of K with $v \neq w$, $v \neq v_1$ and $v \nmid q$, and that

$$|b_i|_{v_1} \leqslant \epsilon^{-n-2}Y \quad (1 \leqslant i \leqslant n+1).$$

Again, the strong approximation theorem shows that these conditions have solutions $b_i \in K$ for $i = 1, \dots, n+1$ provided that ϵ is small enough. Then, the corresponding polynomial P has integral coefficients at v for each ultrametric place v of K with $v \neq w$. At the place w, we find

$$\|P - R\|_w = \left\|\sum_{i=1}^{n+1}(b_i - \theta_i)P_i(T)\right\|_w \leqslant \epsilon^{n+1}Y^{-1}\max_{1\leqslant i\leqslant n+1}\|P_i\|_w \ll \epsilon^{n+1}.$$

Moreover, R has coefficients in $\mathcal{O}_w$ since $|\xi|_w \leqslant 1$ and $\|B\|_w \leqslant 1$. Thus, P also has coefficients in $\mathcal{O}_w$ if ϵ is sufficiently small, and then it has coefficients in $\mathcal{O}_K$. Since we may take $\epsilon \gg 1$, this gives $\|P\|_{v_1} \ll \kappa^{d_{v_1}/d} Y$ and, since $\|P\|_v \ll \kappa^{d_v/d}$ for all Archimedean places $v \neq v_1$, we find $\mathrm{H}(P) \ll \prod_{v|\infty} \|P\|_v \ll \kappa Y$. □

Finally, we can move on to the proof of Theorem A.

9.1 Proof of Theorem A

Let t, n and ξ be as in Theorem A (see § 1), let $k = [n/4]$, and let c be the constant of Theorem B corresponding to these data. Since ξ is not algebraic over K of degree $\leqslant (n-k+1)/(2t)$, Theorem B shows that there are arbitrary large positive real numbers X for which the $(n+1)$-tuple $\underline{X} = (X_0, \ldots, X_n)$ given by

$$X_j = \begin{cases} cX^{-t/(k+1-t)} & \text{for } j = 0, \ldots, n-t, \\ X & \text{for } j = n-t+1, \ldots, n \end{cases}$$

satisfies $\lambda_1(\underline{X}) > 1$. According to Proposition 3.5, this implies that the $(n+1)$-tuple $\underline{Y} = (Y_0, \ldots, Y_n)$ given by

$$Y_j = X_{n-j}^{-1} = \begin{cases} X^{-1} & \text{for } j = 0, \ldots, t-1, \\ c^{-1}X^{t/(k+1-t)} & \text{for } j = t, \ldots, n \end{cases}$$

satisfies $\lambda_{n+1}(\underline{Y}) \leqslant \kappa$ with a constant $\kappa \geqslant 1$ depending only on K, n and w. Assuming X sufficiently large, we may thus apply Lemma 9.1 with

$$Y = c^{-1}X^{t/(k+1-t)} \quad \text{and} \quad \delta = c^{1/t}X^{-(k+1)/(t(k+1-t))}.$$

It shows the existence of a monic polynomial $P \in \mathcal{O}_K[T]$ which is irreducible over K of degree $n+1$ and height $\ll \kappa Y$, admits d distinct conjugates over $\mathbb{Q}$, and has at least t distinct roots $\alpha_1, \ldots, \alpha_t \in K_w$ with

$$\max_{1\leqslant i\leqslant t} |\xi - \alpha_i|_w \ll Y^{-(k+1)/t^2}. \tag{9.4}$$

In particular, $\alpha = \alpha_1$ is an algebraic integer of degree $n+1$ over K and degree $d(n+1)$ over $\mathbb{Q}$. From the remark at the end of § 2, we find $\mathrm{H}(\alpha) \ll \mathrm{H}(P)^d \ll Y^d$. Combining this with (9.4), we obtain that the conjugates $\alpha_1, \ldots, \alpha_t$ of α over K satisfy

$$\max_{1\leqslant i\leqslant t} |\xi - \alpha_i|_w \ll \mathrm{H}(\alpha)^{-(k+1)/(dt^2)} \ll \mathrm{H}(\alpha)^{-(n+1)/(4dt^2)}.$$

Moreover, since the right-hand side of (9.4) can be made arbitrarily small by choosing X sufficiently large, we produce an infinity of such numbers α by varying X.

10. Remarks on simultaneous approximations

We fix a place w of K and an algebraic closure $\bar{K}_w$ of K_w, and we extend the absolute value $|\ |_w$ of K_w to an absolute value of $\bar{K}_w$ also denoted $|\ |_w$. Our first result below shows that, for $t \geqslant 2$, the exponent $(n+1)/(4dt^2)$ in the inequality (1.1) of Theorem A cannot be replaced by a real number greater than $2n/(dt(t-1))$.

Proposition 10.1. *Let n and t be integers with $2 \leqslant t \leqslant n$, and let ξ be an element of K_w. There exists a constant $c = c(n,t) > 0$ such that, for any algebraic number α of degree n over K*

and any choice of t distinct conjugates $\alpha_1, \dots, \alpha_t$ of α in $\bar{K}_w$, we have

$$\max_{1\leqslant i\leqslant t} |\xi - \alpha_i|_w \geqslant c\mathrm{H}(\alpha)^{-2n(n-1)/(\deg(\alpha)t(t-1))},$$

where $\deg(\alpha)$ denotes the degree of α over $\mathbb{Q}$.

Proof. Let $P \in K[T]$ be an irreducible polynomial of degree n, let a_0 be its leading coefficient, and let $\alpha_1, \dots, \alpha_n$ be the roots of P ordered so that $|\xi - \alpha_1|_w \leqslant \cdots \leqslant |\xi - \alpha_n|_w$. The discriminant of P is the non-zero element of K given by

$$\mathrm{Disc}(P) = {a_0}^{2(n-1)} \prod_{1\leqslant i<j\leqslant n} (\alpha_i - \alpha_j)^2.$$

Using the estimates

$$|\alpha_i - \alpha_j|_w \leqslant \begin{cases} 2^{c_w} \max\{1, |\alpha_i|_w\} \max\{1, |\alpha_j|_w\} |\xi - \alpha_j|_w & \text{when } 1 \leqslant i < j \leqslant t, \\ 2^{c_w} \max\{1, |\alpha_i|_w\} \max\{1, |\alpha_j|_w\} & \text{otherwise,} \end{cases}$$

with $c_w = 0$ if w is ultrametric and $c_w = d_w/d$ otherwise, we find

$$|\mathrm{Disc}(P)|_w \leqslant 2^{n(n-1)c_w} M_w(P)^{2(n-1)} \prod_{j=1}^{t} |\xi - \alpha_j|_w^{2(j-1)},$$

where $M_w(P) = |a_0|_w \prod_{i=1}^m \max\{1, |\alpha_i|_w\}$ denotes the Mahler measure of P at w. Since $M_w(P) \leqslant (n+1)^{c_w/2} \|P\|_w$ (see Chapter 3 of [Lan83]), this gives

$$|\mathrm{Disc}(P)|_w \leqslant (2^n(n+1))^{(n-1)c_w} \|P\|_w^{2(n-1)} |\xi - \alpha_t|_w^{t(t-1)}.$$

Similarly, for all other places v of K, we find, with the same definition of c_v,

$$|\mathrm{Disc}(P)|_v \leqslant (2^n(n+1))^{(n-1)c_v} \|P\|_v^{2(n-1)}.$$

Applying the product formula we therefore obtain

$$1 = \prod_v |\mathrm{Disc}(P)|_v \leqslant \big(2^n(n+1)\big)^{n-1} \mathrm{H}(P)^{2(n-1)} |\xi - \alpha_t|_w^{t(t-1)}.$$

The conclusion follows since we have $\mathrm{H}(P) \ll \mathrm{H}(\alpha)^{n/\deg(\alpha)}$ for a root α of P (see § 2). □

Our last result justifies the remark made in the Introduction concerning simultaneous approximation of several numbers by conjugate algebraic numbers.

Proposition 10.2. *Assume that $K = \mathbb{Q}$. Let n and t be positive integers, and let κ be a real number with*

$$\kappa > t^{-1}(t+1)^{1+(1/t)}.$$

Then, there exist elements $\xi_1, \dots, \xi_t$ of $\mathbb{Q}_w$ and a constant $H_0 \geqslant 1$ (depending on n, t, w, κ) with the following property. For any real number $H \geqslant H_0$ and any choice of numbers $\alpha_1, \dots, \alpha_t \in \bar{\mathbb{Q}}_w$ that are algebraic over $\mathbb{Q}$ of degree $\leqslant n$ and height $\leqslant H$, we have

$$\max_{1\leqslant j\leqslant t} |\xi_j - \alpha_j|_w \geqslant H^{-\kappa n^{1/t}}.$$

Note that $t^{-1}(t+1)^{1+(1/t)}$ is a decreasing function of t for $t > 0$ tending to 1 as t tends to infinity. For $t \geqslant 2$, we can take $\kappa = 3$.

Proof. Put $b = (t+1)n$ and define a sequence of positive integers $(a_\ell)_{\ell\geqslant 1}$ by the formula $a_\ell = [b^{\ell/t}]$. Define also $\pi = 1/2$ if w is the place at infinity of $\mathbb{Q}$ and $\pi = p$ if w corresponds to a prime number p.

We claim that the elements of $\mathbb{Q}_w$ given by

$$\xi_j = \sum_{i=0}^{\infty} \pi^{a_{j+ti}} \quad (j = 1, \dots, t)$$

have the required property.

To prove this, we choose a real number ϵ with $0 < \epsilon < 1$ such that

$$\kappa > \frac{t+1+\epsilon}{t-\epsilon}(t+1)^{1/t},$$

and consider the sequence of closed intervals $(I_\ell)_{\ell \geqslant 1}$ of $\mathbb{R}$ given by

$$I_\ell = [\kappa^{-1}(t+1+\epsilon)a_\ell n^{1-(1/t)},\ (t-\epsilon)a_\ell n].$$

Two consecutive such intervals I_ℓ and $I_{\ell+1}$ overlap for sufficiently large values of ℓ since

$$\lim_{\ell\to\infty} \frac{(t-\epsilon)a_\ell n}{\kappa^{-1}(t+1+\epsilon)a_{\ell+1}n^{1-(1/t)}} = \frac{(t-\epsilon)\kappa}{(t+1+\epsilon)(t+1)^{1/t}} > 1.$$

Therefore, the union of these intervals contains a half line $[c, \infty)$ for some constant $c > 0$. Choose a real number H with $H \geqslant |\pi|_w^{-c}$, and let $\alpha_1, \dots, \alpha_t \in \bar{\mathbb{Q}}_w$ be algebraic over $\mathbb{Q}$ of degree $\leqslant n$ and height $\leqslant H$. By definition of c, there exists an integer $\ell \geqslant 1$ such that $-\log H/\log|\pi|_w \in I_\ell$. Writing ℓ in the form $\ell = j + tm$ for some integers j and m with $1 \leqslant j \leqslant t$ and $m \geqslant 0$, we claim more precisely that, if H is sufficiently large (so that ℓ is large), we have

$$|\xi_j - \alpha_j|_w \geqslant H^{-\kappa n^{1/t}}.$$

For brevity, since the ultrametric case is simpler, we shall only prove this refined claim in the case where $w = \infty$. Then, we have $\mathbb{Q}_w = \mathbb{R}$, $\bar{\mathbb{Q}}_w = \mathbb{C}$, $\pi = \frac{1}{2}$ and $\log H/\log 2 \in I_\ell$. From now on, we drop the subscript w on the absolute value and consider the rational number

$$r = \sum_{i=0}^{m} 2^{-a_{j+ti}}.$$

Since $(a_{j+ti})_{i\geqslant 0}$ is a strictly increasing sequence of positive integers, it satisfies

$$\mathrm{H}(r) = 2^{a_\ell} \quad \text{and} \quad 2^{-a_{\ell+t}} \leqslant \xi_j - r = \sum_{i=1}^{\infty} 2^{-a_{\ell+ti}} \leqslant 2^{-a_{\ell+t}+1}.$$

If $\alpha_j = r$, we find

$$|\xi_j - \alpha_j| = \xi_j - r \geqslant 2^{-a_{\ell+t}} \geqslant H^{-\kappa n^{1/t}},$$

assuming that H (and thus ℓ) is sufficiently large so that

$$a_{\ell+t} \leqslant (t+1+\epsilon)na_\ell \leqslant \kappa n^{1/t} \log H/\log 2.$$

If $\alpha_j \neq r$, Liouville's inequality (see for example Proposition 3.14 of [Wal00]) gives

$$|\alpha_j - r| \geqslant \gamma \mathrm{H}(\alpha_j)^{-1}\mathrm{H}(r)^{-n} \geqslant \gamma H^{-1} 2^{-a_\ell n},$$

with $\gamma = \gamma(n) = 2^{1-n}(n+1)^{-1/2}$. This implies

$$|\alpha_j - r| \geqslant \gamma 2^{-(t-\epsilon)a_\ell n - a_\ell n} \geqslant 2^{-a_{\ell+t}+2} \geqslant 2|\xi_j - r|,$$

assuming that H is sufficiently large, so that

$$(t+1-\epsilon)a_\ell n \leqslant a_{\ell+t} - 2 + \log\gamma/\log 2.$$

Since $\kappa > (t+1+\epsilon)/(t+\epsilon)$, we may also assume $(\gamma/2)H^{-1} \geqslant H^{-((t+\epsilon)/(t+1+\epsilon))\kappa n^{1/t}}$ and so we get

$$|\xi_j - \alpha_j| \geqslant |\alpha_j - r| - |\xi_j - r| \geqslant \frac{1}{2}|\alpha_j - r| \geqslant \frac{\gamma}{2} H^{-1} 2^{-a_\ell n} \geqslant H^{-\kappa n^{1/t}}. \qquad \square$$

References

Bro74 W. D. Brownawell, *Sequences of Diophantine approximations*, J. Number Theory **6** (1974), 11–21.

BT00 Y. Bugeaud and O. Teulié, *Approximation d'un nombre réel par des nombres algébriques de degré donné*, Acta Arith. **93** (2000), 77–86.

BV83 E. Bombieri and J. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), 11–32.

DS69 H. Davenport and W. M. Schmidt, *Approximation to real numbers by algebraic integers*, Acta Arith. **15** (1969), 393–416.

Car77 H. Cartan, *Cours de calcul différentiel* (Hermann, Paris, 1977).

Cas71 J. W. S. Cassels, *An introduction to the geometry of numbers* (Springer-Verlag, Berlin, 1971).

Cas67 J. W. S. Cassels, *Global fields*, in *Algebraic number theory*, eds J. W. S. Cassels and A. Fröhlich (Academic Press, New York, 1967), ch. II.

FT93 A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27 (Cambridge University Press, Cambridge, 1993).

Lan83 S. Lang, *Fundamentals of Diophantine geometry* (Springer-Verlag, New York, 1983).

LR99 M. Laurent and D. Roy, *Criteria of algebraic independence with multiplicities and interpolation determinants*, Trans. Amer. Math. Soc. **351** (1999), 1845–1870.

Mah39 K. Mahler, *Ein Übertragungsprinzip für konvexe Körper*, Časopis Pěst. Mat. **68** (1939), 93–102.

Mah64 K. Mahler, *Inequalities for ideal bases in algebraic number fields*, J. Aust. Math. Soc. **4** (1964), 425–448.

McF71 R. B. McFeat, *Geometry of numbers in adele spaces*, Diss. Math. Rozprawy Mat. **88** (1971), 54.

Roy04 D. Roy, *Approximation to real numbers by cubic algebraic integers I*, Proc. London Math. Soc. (3) **88** (2004), 42–62; *II*, Ann. of Math. (2) **158** (2003), 1081–1087.

Sch67 W. M. Schmidt, *On heights of algebraic subspaces and diophantine approximations*, Ann. of Math. (2) **85** (1967), 430–472.

Teu02 O. Teulié, *Approximation d'un nombre p-adique par des nombres algébriques*, Acta Arith. **102** (2002), 137–155.

Wal00 M. Waldschmidt, *Diophantine approximation on linear algebraic groups: transcendence properties of the exponential function in several variables* (Springer-Verlag, New York, 2000).

Wir60 E. Wirsing, *Approximation mit algebraischen Zahlen beschränkten Grades*, J. Reine Angew. Math. **206** (1960), 67–77.

Damien Roy droy@uottawa.ca
Département de Mathématiques, Université d'Ottawa, 585 King Edward, Ottawa, Ontario, K1N 6N5, Canada

Michel Waldschmidt miw@math.jussieu.fr
Université Pierre et Marie Curie (Paris VI), Institut de Mathématiques CNRS UMR 7586, Théorie des Nombres, Case 247, 175 rue du Chevaleret, 75013 Paris, France