On a mixed problem in Diophantine approximation

by

YANN BUGEAUD (Strasbourg) and BERNARD DE MATHAN (Bordeaux)

1. Introduction. In analogy with the Littlewood conjecture, de Mathan and Teulié [7] proposed recently a “mixed Littlewood conjecture”. For any prime number $p$, the usual $p$-adic absolute value $| \cdot |_p$ is normalized in such a way that $|p|_p = p^{-1}$. We denote by $\| \cdot \|$ the distance to the nearest integer.

**De Mathan–Teulié Conjecture.** For every real number $\alpha$ and every prime number $p$, we have

$$
\inf_{q \geq 1} q \cdot \|q\alpha\| \cdot |q|_p = 0.
$$

Obviously, the above conjecture holds if $\alpha$ is rational or has unbounded partial quotients in its continued fraction expansion. Thus, it only remains to consider the case when $\alpha$ is an element of the set $\text{Bad}_1$ of badly approximable real numbers, that is,

$$
\text{Bad}_1 = \{ \alpha \in \mathbb{R} : \inf_{q \geq 1} q \cdot \|q\alpha\| > 0 \}.
$$

De Mathan and Teulié [7] proved that (1.1) holds for every quadratic real number $\alpha$ (recall that such a number is in $\text{Bad}_1$) but, despite several recent results [4, 3], the general conjecture is still unsolved.

If we rewrite (1.1) in the form

$$
\inf_{a,q \geq 1, \gcd(a,q)=1} q^2 \cdot \left| \alpha - \frac{a}{q} \right| \cdot |q|_p = 0,
$$

then we have $|q|_p = \min\{|\text{Norm}(q/a)|_p, 1\}$. Hence, upon replacing $\alpha$ by $1/\alpha$, the de Mathan–Teulié conjecture can be reformulated as follows: For every irrational real number $\alpha$, for every prime number $p$ and every positive real number $\varepsilon$, there exists a non-zero rational number $\xi$ satisfying

$$
|\alpha - \xi| \cdot \min\{|\text{Norm}(\xi)|_p, 1\} < \varepsilon H(\xi)^{-2}.
$$

2000 Mathematics Subject Classification: Primary 11J04; Secondary 11J61, 11J68.

Key words and phrases: Diophantine approximation, approximation to algebraic numbers, non-Archimedean valuation.

DOI: 10.4064/aa139-1-6
Throughout this paper, the height $H(P)$ of an integer polynomial $P(X)$ is the maximal of the absolute values of its coefficients. The height $H(\xi)$ of an algebraic number $\xi$ is the height of its minimal defining polynomial over the rational integers $a_0 + a_1 X + \cdots + a_d X^d$, and the norm of $\xi$, denoted by $\text{Norm}(\xi)$, is the rational number $(-1)^d a_0/a_d$.

The above reformulation suggests asking the following question.

**Problem 1.** Let $d$ be a positive integer. Let $\alpha$ be a real number that is not algebraic of degree less than or equal to $d$. For every prime number $p$ and every positive real number $\varepsilon$, does there exist a non-zero real algebraic number $\xi$ of degree at most $d$ satisfying

$$|\alpha - \xi| \cdot \min\{\text{Norm}(\xi)|_p, 1\} < \varepsilon H(\xi)^{-d-1}?$$

The answer to Problem 1 is clearly positive, unless (perhaps) when $\alpha$ is an element of the set $\text{Bad}_d$ of real numbers that are badly approximable by algebraic numbers of degree at most $d$, where

$$\text{Bad}_d = \{\alpha \in \mathbb{R} : \text{there exists } c > 0 \text{ such that } |\alpha - \xi| > cH(\xi)^{-d-1}$$

for all algebraic numbers $\xi$ of degree at most $d$.

For $d \geq 1$, the set $\text{Bad}_d$ contains the set of algebraic numbers of degree $d + 1$, but it remains an open problem to decide whether this inclusion is strict for $d \geq 2$; see the monograph [2] for more information. The purpose of the present note is to give a positive answer to Problem 1 for every positive integer $d$ and every real algebraic number $\alpha$ of degree $d + 1$. This extends the result from [7], which deals with the case $d = 1$.

**2. Results.** Throughout this paper, for a prime number $p$, a number field $\mathbb{K}$, and a non-Archimedean place $v$ on $\mathbb{K}$ lying above $p$, we normalize the absolute value $|\cdot|_v$ in such a way that $|\cdot|_v$ and $|\cdot|_p$ coincide on $\mathbb{Q}$.

Our main result includes a positive answer to Problem 1 when $\alpha$ is a real algebraic number of degree $d + 1$.

**Theorem 1.** Let $d$ be a positive integer. Let $\alpha$ be a real algebraic number of degree $d + 1$ and denote by $r$ the unit rank of $\mathbb{Q}(\alpha)$. Let $p$ be a prime number. There exist positive constants $c_1, c_2, c_3$, depending on $\alpha$ and $p$, and infinitely many real algebraic numbers $\xi$ of degree $d$ such that

\begin{align*}
|\alpha - \xi| &< c_1 H(\xi)^{-d-1}, \\
|\xi|_v &< c_2 (\log 3H(\xi))^{-1/(rd)}
\end{align*}

for every absolute value $|\cdot|_v$ on $\mathbb{Q}(\xi)$ above the prime $p$, and

\begin{align*}
|\alpha - \xi| \cdot \min\{\text{Norm}(\xi)|_p, 1\} &< c_3 H(\xi)^{-d-1}(\log 3H(\xi))^{-1/r}.
\end{align*}

Theorem 1 extends Théorème 2.1 of [7], which only concerns the case $d = 1$. 
Under the assumptions of Theorem 1, Wirsing [9] established that there are infinitely many real algebraic numbers $\xi$ satisfying (2.1).

The proof of Theorem 1 is very much inspired by a paper of Peck [8] on simultaneous rational approximation to real algebraic numbers. Roughly speaking, we use a method dual to Peck’s to construct integer polynomials $P(X)$ that take small values at $\alpha$, and we need an extra argument to ensure that our polynomials have a root $\xi$ very close to $\alpha$.

De Mathan [6] used the theory of linear forms in non-Archimedean logarithms to prove that Theorem 1 for $d = 1$ is best possible, in the sense that the absolute value of the exponent of $\log 3H(\xi)$ in (2.2) cannot be too large. The next theorem extends this result to all values of $d$.

**Theorem 2.** Let $p$ be a prime number, $d$ a positive integer and $\alpha$ a real algebraic number of degree $d+1$. Let $\lambda$ be a positive real number. There exists a positive real number $\kappa = \kappa(\lambda)$ such that for every non-zero real algebraic number $\xi$ of degree $d$ satisfying

$$
|\alpha - \xi| \leq \lambda H(\xi)^{-d-1}
$$

we have

$$
|\xi|_v \geq (\log 3H(\xi))^{-\kappa}
$$

for at least one absolute value $|\cdot|_v$ on $\mathbb{Q}(\xi)$ above the prime $p$.

As in [6], the proof of Theorem 2 rests on the theory of linear forms in non-Archimedean logarithms.

Let $d$ be a positive integer. We recall that it follows from the $p$-adic version of the Schmidt Subspace Theorem that for every algebraic number $\alpha$ of degree $d+1$ and for every positive real number $\varepsilon$, there are only finitely many non-zero integer polynomials $P(X) = a_0 + a_1X + \cdots + a_dX^d$ of degree at most $d$, with $a_0 \neq 0$, that satisfy

$$
|P(\alpha)| \cdot |a_0|_p < H(P)^{-d-\varepsilon}.
$$

Let $\xi$ be a real algebraic number of degree at most $d$, and denote by $P(X) = a_0 + a_1X + \cdots + a_dX^d$ its minimal polynomial over $\mathbb{Z}$. Then

$$
\min\{|\text{Norm}(\xi)|_p, 1\} \geq |a_0|_p
$$

and there exists a constant $c(\alpha)$, depending only on $\alpha$, such that

$$
|P(\alpha)| \leq c(\alpha)H(\xi) \cdot |\xi - \alpha|.
$$

Let $\varepsilon$ be a positive real number. Applying the above statement deduced from the $p$-adic version of the Schmidt Subspace Theorem to these polynomials $P(X)$, we deduce that

$$
|\alpha - \xi| \cdot \min\{|\text{Norm}(\xi)|_p, 1\} \geq H(P)^{-d-1-\varepsilon}
$$
holds if $H(P)$ is sufficiently large. This implies that if $\xi$ satisfies (2.4) and if $H(\xi)$ is sufficiently large, then

$$|\text{Norm}(\xi)|_p \geq H(\xi)^{-\varepsilon},$$

accordingly

$$\max_{v|p} |\xi|_v \geq H(\xi)^{-\varepsilon/d}.$$ 

The result of Theorem 2 is more precise, but we cannot obtain a good lower bound for $|\text{Norm}(\xi)|_p$.

We conclude this section by pointing out that Einsiedler and Kleinbock [4] showed that a slight modification of the de Mathan–Teulié conjecture easily follows from a theorem of Furstenberg [5, 1].

**Theorem EK.** Let $p_1$ and $p_2$ be distinct prime numbers. Then

$$\inf_{q \geq 1} q \cdot \|q\alpha\| \cdot |q|_{p_1} \cdot |q|_{p_2} = 0$$

for every real number $\alpha$.

In view of Theorem EK, we formulate the following question, presumably easier to solve than Problem 1.

**Problem 2.** Let $d$ be a positive integer. Let $\alpha$ be a real number that is not algebraic of degree less than or equal to $d$. For any distinct prime numbers $p_1$, $p_2$ and every positive real number $\varepsilon$, does there exist a non-zero real algebraic number $\xi$ of degree at most $d$ satisfying

$$|\alpha - \xi| \cdot \min\{|\text{Norm}(\xi)|_{p_1}, 1\} \cdot \min\{|\text{Norm}(\xi)|_{p_2}, 1\} < \varepsilon H(\xi)^{-d-1}.$$ 

Theorem EK gives a positive answer to Problem 2 when $d = 1$.

The remainder of the paper is organized as follows. We gather several auxiliary results in Section 3, and Theorems 1 and 2 are established in Sections 4 and 5, respectively.

In the next sections, we fix a real algebraic number field $K$ of degree $d + 1$. The notation $A \ll B$ means, unless specifically indicated otherwise, that the implicit constant depends on $K$. Furthermore, we write $A \asymp B$ if $A \ll B$ and $B \ll A$ simultaneously.

**3. Auxiliary lemmas.** Let $K$ be a real algebraic number field of degree $d + 1$. Let $O$ denote its ring of integers, and let $\alpha_0 = 1, \alpha_1, \ldots, \alpha_d$ be a basis of $K$. Let $D$ be a positive integer satisfying

$$D(\mathbb{Z} + \alpha_1\mathbb{Z} + \cdots + \alpha_d\mathbb{Z}) \subset O \subset \frac{1}{D} (\mathbb{Z} + \alpha_1\mathbb{Z} + \cdots + \alpha_d\mathbb{Z})$$

and the corresponding inequalities for the dual basis $\beta_0, \ldots, \beta_d$ defined by

$$\text{Tr}(\alpha_i\beta_j) = \delta_{i,j},$$

where Tr is the trace and $\delta_{i,j}$ is the Kronecker symbol.
We denote by $\sigma_0 = \text{Id}, \ldots, \sigma_d$ the complex embeddings of $K$, numbered in such a way that $\sigma_0, \ldots, \sigma_{r_1-1}$ are real, $\sigma_{r_1}, \ldots, \sigma_d$ are imaginary and $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ for $0 \leq j < r_2$. Set also $r = r_1 + r_2 - 1$, and let $\varepsilon_1, \ldots, \varepsilon_r$ be multiplicatively independent units in $K$.

**Lemma 1.** Let $\eta$ be a unit in $\mathcal{O}$ such that $-1 < \eta < 1$ and define the real number $N$ by $|\eta| = N^{-1}$. The conditions

$$|\sigma_j(\eta)| \asymp N^{1/d}, \quad 0 < j \leq d, \tag{3.1}$$

and

$$|\sigma_i(\eta)| \asymp |\sigma_j(\eta)|, \quad 0 < i < j \leq d, \tag{3.2}$$

are equivalent. Let $\gamma \neq 0$ be in $K$ and let $\Delta$ be a positive integer such that $\Delta \gamma \in \mathcal{O}$. If $\eta$ satisfies (3.1) or (3.2), write

$$\gamma \eta = a_0 + \cdots + a_d \alpha_d$$

with $a_0, \ldots, a_d$ in $Q$. Then $D \Delta a_k \in \mathbb{Z}$ for $k = 0, \ldots, d$ and

$$\max_{k=0,\ldots,d} |a_k| \asymp N^{1/d},$$

where the implicit constants depend on $\gamma$.

**Proof.** Since $\eta$ is a unit, we have $\prod_{0 \leq j \leq d} \sigma_j(\eta) = \pm 1$, and (3.1) and (3.2) are clearly equivalent. The formula

$$a_k = \text{Tr}(\gamma \eta \beta_k) = \gamma \eta \beta_k + \sum_{j=1}^{d} \sigma_j(\eta) \sigma_j(\gamma \beta_k)$$

implies that if $\eta$ satisfies (3.1), then

$$|a_k| \ll N^{1/d}, \quad 0 \leq k \leq d.$$

Combined with

$$\sigma_1(\gamma) \sigma_1(\eta) = a_0 + \cdots + a_d \sigma_1(\alpha_d),$$

this shows that $N^{1/d} \asymp |\sigma_1(\eta)| \ll \max_{k=0,\ldots,d} |a_k|$.

Let $\alpha$ be a real algebraic number of degree $d+1$. We keep the above notation with the field $K = \mathbb{Q}(\alpha)$ and the basis $1, \alpha, \ldots, \alpha^d$ of $K$ over $\mathbb{Q}$, and we display an immediate consequence of Lemma 1.

**Corollary 1.** Let $\eta$ be a unit in $\mathcal{O}$ such that $-1 < \eta < 1$ and set $N = |\eta|^{-1}$. Then

$$D \Delta \gamma \eta = P(\alpha),$$

where $P(X)$ is an integral polynomial of degree at most $d$ satisfying

$$H(P) \asymp N^{1/d}, \quad |P(\alpha)| \asymp N^{-1},$$

and thus $|P(\alpha)| \asymp H(P)^{-d}$. 

Denote by $\tau_j$, $j = 0, \ldots, d$ the embeddings of $K$ into $\mathbb{C}_p$. Recall that the absolute value $|\cdot|_p$ on $\mathbb{Q}$ has an extension to $\mathbb{C}_p$, that we also denote by $|\cdot|_p$. In Lemmata 2 to 4 below we work in $\mathbb{C}_p$. Let $P(X)$ be an irreducible integer polynomial of degree $n \geq 1$. Let $\xi$ be a complex root of $P(X)$ and $\xi_1, \ldots, \xi_n$ be the roots of $P(X)$ in $\mathbb{C}_p$. We point out that the sets 

$$\{ |\xi|_v : v \text{ is above } p \text{ on } \mathbb{Q}(\xi) \} \quad \text{and} \quad \{ |\xi_i|_p : 1 \leq i \leq n \}$$

coincide, since all the absolute values above $p$ over $\mathbb{Q}(\xi)$ are obtained by starting from $|\cdot|_p$ over $\mathbb{C}_p$, after embedding $\mathbb{Q}(\xi)$ in $\mathbb{C}_p$.

Keeping the notation of Lemma 1, we have the following auxiliary result.

**Lemma 2.** Assume that $\gamma = \alpha d$. Then

$$|a_k|_p \ll \max_{0 \leq j \leq d} |\tau_j(\eta) - 1|_p, \quad 0 \leq k < d,$$

and

$$|a_d - 1|_p \ll \max_{0 \leq j \leq d} |\tau_j(\eta) - 1|_p.$$

**Proof.** Since $\text{Tr}(\alpha d \beta_k) = 0$ for $k = 0, \ldots, d - 1$, we get

$$a_k = \text{Tr}(\gamma \eta \beta_k) = \text{Tr}(\alpha_d (\eta - 1) \beta_k) = \sum_{j=0}^{d} (\tau_j(\eta) - 1) \tau_j(\alpha_d \beta_k),$$

and deduce that

$$|a_k|_p \ll \max_{0 \leq j \leq d} |\tau_j(\eta) - 1|_p, \quad 0 \leq k < d.$$

It follows from $\text{Tr}(\alpha_d \beta_d) = 1$ that

$$a_d = 1 + \text{Tr}(\alpha_d \beta_d (\eta - 1)) = 1 + \sum_{j=0}^{d} (\tau_j(\eta) - 1) \tau_j(\alpha_d \beta_d),$$

and we derive the last conclusion of the lemma. $\blacksquare$

**Lemma 3.** Let $0 < \delta < 1$. There exist arbitrarily large positive real numbers $H$ and units $\eta$ satisfying $\eta = H^{-d}$,

$$\left| \frac{\sigma_j(\eta)}{\sigma_1(\eta)} - 1 \right| \leq \delta, \quad 2 \leq j \leq d,$$

and

$$|\tau_j(\eta) - 1|_p \ll (\log H)^{-1/r}, \quad 0 \leq j \leq d.$$

**Proof.** By replacing $\varepsilon_i$ by $\varepsilon_i^{2^m_i (p-1)(p^2-1) \cdots (p^{d+1}-1)}$ with a suitable positive integer $m_i$, we can assume that $\varepsilon_i$ is positive, together with its real conjugates, and that $|\tau_j(\varepsilon_i) - 1|_p < p^{-1/(p-1)}$ for $i = 1, \ldots, r$ and $j = 0, \ldots, d$. This is possible since $|\tau_j(\varepsilon_i)|_p = 1$ for $i = 1, \ldots, r$ and $j = 0, \ldots, d$. This allows us to consider the $p$-adic logarithms of each $\tau_j(\varepsilon_i)$. Our aim is to
construct a suitable unit $\eta$ of the form

$$\eta = \varepsilon_1^{\mu_1}p^s \cdots \varepsilon_r^{\mu_r}p^s,$$

where $\mu_i \in \mathbb{Z}$. The conditions for (3.3) are then

$$p^s\mu_1 \log \frac{|\sigma_j(\varepsilon_1)|}{|\sigma_1(\varepsilon_1)|} + \cdots + \mu_r \log \frac{|\sigma_j(\varepsilon_r)|}{|\sigma_r(\varepsilon_r)|} \leq C_1, \quad 2 \leq j \leq r,$$

where $C_1 = C_1(\delta) > 0$ is a constant, and

$$\left| \frac{p^s}{2\pi} (\mu_1 \arg \sigma_j(\varepsilon_1) + \cdots + \mu_r \arg \sigma_j(\varepsilon_r)) \right| \leq C_2, \quad r_1 \leq j \leq r,$$

with $C_2 = C_2(\delta) > 0$. Set

$$Y_j = \frac{p^s}{2\pi} \left( \mu_1 \log \frac{|\sigma_1(\varepsilon_1)|}{|\sigma_1(\varepsilon_1)|} + \cdots + \mu_r \log \frac{|\sigma_1(\varepsilon_r)|}{|\sigma_r(\varepsilon_r)|} \right), \quad 2 \leq j \leq r,$$

$$Z_k = \frac{p^s}{2\pi} (\mu_1 \arg \sigma_k(\varepsilon_1) + \cdots + \mu_r \arg \sigma_k(\varepsilon_r)) \in \mathbb{R}/\mathbb{Z}, \quad r_1 \leq k \leq r.$$

Taking $0 \leq \mu_i < M$, we have $M^r$ points $(\mu_i)_{1 \leq i \leq r}$. The $(Y_j, Z_k)_{2 \leq j \leq r, \ r_1 \leq k \leq r}$ are in the product of intervals $I_j$, $2 \leq j \leq r$, of lengths $O(Mp^s)$ and of $r_2$ factors identical to $\mathbb{R}/\mathbb{Z}$. This set can be covered by $C_3(Mp^s)^{r-1}$ sets of diameter at most $\max\{C_1, C_2\}$, where $C_3$ is a constant depending on $\delta$. By Dirichlet’s Schubfachprinzip, choosing $M$ such that

$$C_3(Mp^s)^{r-1} < M^r,$$

which can be done with $M \asymp p^{(r-1)s}$, we deduce that there is $(\mu_1, \ldots, \mu_r) \in \mathbb{Z}^r \setminus \{0\}$ such that

$$\max_{1 \leq i \leq r} |\mu_i| \ll M,$$

$$|Y_j| \leq C_1, \quad 2 \leq j \leq r,$$

$$||Z_k|| \leq C_2, \quad r_1 \leq k \leq r.$$

Set then $\eta = (\varepsilon_1^{\mu_1} \cdots \varepsilon_r^{\mu_r})p^s$ in such a way that $0 < \eta < 1$ (if needed, just consider $1/\eta$). This choice implies that

$$|\tau_i(\eta) - 1|_p = |\log_p \tau_i(\eta)|_p \leq p^{-s}, \quad 0 \leq i \leq d,$$

and

$$|\log \eta| \ll p^s M \ll p^{rs}. \quad \blacksquare$$

**Lemma 4.** Let $P(X) = a_0 + \cdots + a_dX^d \in \mathbb{C}_p[X]$ be a polynomial of degree $d$. Let $\xi_i$ ($1 \leq i \leq d$) be the roots of $P(X)$ in $\mathbb{C}_p$. Let $c$ be a real number satisfying $0 \leq c \leq 1$. If

$$|\xi_i|_p \leq c, \quad 1 \leq i \leq d,$$

then

$$|a_k|_p \leq c|a_d|_p, \quad 0 \leq k < d.$$
Conversely, if (3.4) holds, then
\[ |\xi_i|_p \leq c^{1/d}, \quad 1 \leq i \leq d. \]

Proof. Since \( P(X) = a_d \prod_{1 \leq i \leq d} (X - \xi_i) \), if \( |\xi_i|_p \leq c \leq 1 \) for \( i = 1, \ldots, d \) then
\[ |a_k|_p \leq c|a_d|_p \quad \text{for} \quad k = 0, \ldots, d - 1. \]
Conversely, if
\[ |a_k|_p \leq c|a_d|_p, \quad 0 \leq k < d, \]
and if \( \xi \in \mathbb{C}_p \) is such that \( a_d \xi^d + \cdots + a_0 = 0 \), then there exists \( k \) with \( 0 \leq k < d \) and
\[ |a_k \xi^k|_p \geq |a_d \xi^d|_p, \quad \text{thus} \quad |\xi|_p^{d-k} \leq c. \]

We conclude this section with two lemmas used in the proof of Theorem 2. The first of them was proved by Peck [8].

**Lemma 5.** There exists a sequence \( (\eta_m)_{m \geq 1} \) of positive units in \( \mathcal{O} \) such that
\[ \eta_m \asymp e^{-dm}, \quad |\sigma_j(\eta_m)| \asymp e^m, \quad 1 \leq j \leq d. \]

Proof. Let us search for the unit \( \eta_m \) in the form \( \eta_m = \varepsilon_1^{\mu_1} \cdots \varepsilon_r^{\mu_r} \) with \( \mu_i \in \mathbb{Z} \). We construct real numbers \( \nu_1, \ldots, \nu_r \) such that
\[ \nu_1 \log \varepsilon_1 + \cdots + \nu_r \log \varepsilon_r = -dm \]
and
\[ \nu_1 \log |\sigma_j(\varepsilon_1)| + \cdots + \nu_r \log |\sigma_j(\varepsilon_r)| = m, \quad 1 \leq j \leq d. \]

Taking into account that, by complex conjugation, the equations (3.6) corresponding to an index \( j \) with \( r_1 \leq j < r_1 + r_2 \) and to the index \( j + r_2 \) are identical, and that the sum of (3.5) and (3.6) is zero, we simply have to deal with a Cramer system, since the matrix \( (\sigma_j(\varepsilon_i))^{1 \leq j \leq r, 1 \leq i \leq r} \) is regular. We solve this system and then replace every \( \nu_i \) by a rational integer \( \mu_i \) such that \( |\mu_i - \nu_i| \leq 1/2. \)

**Lemma 6.** Let \( \lambda' \) be a positive real number. Let \( (\eta_m)_{m \geq 1} \) be a sequence of positive units as in Lemma 5. There exists a finite set \( \Gamma = \Gamma(\lambda') \) of non-zero elements of \( \mathbb{K} \) such that for every integer polynomial \( P(X) \) of degree at most \( d \) that satisfies
\[ |P(\alpha)| \leq \lambda'H(P)^{-d}, \]
there exist a positive integer \( m \) and \( \gamma \) in \( \Gamma \) for which
\[ P(\alpha) = \gamma \eta_m. \]

Proof. Below, all the constants implicit in \( \ll \) depend on \( \mathbb{K} \) and on \( \lambda' \). Let \( m \) be a positive integer such that
\[ H(P) \asymp e^m, \]
and set
\[ \gamma = P(\alpha)\eta_m^{-1}. \]
Since \( D\alpha^k \) is an algebraic integer for \( k = 0, \ldots, d \), the algebraic number \( D\gamma \) is an algebraic integer, and, by (3.7),
\[ |\gamma| \ll 1. \]
Furthermore, for \( j = 1, \ldots, d \), we have
\[ |\sigma_j(\gamma)| = |P(\sigma_j(\alpha))| \cdot |\sigma_j(\eta_m^{-1})| \ll H(P)e^{-m} \ll 1. \]
The algebraic integers \( D\gamma \in \mathcal{O} \) and all their complex conjugates being bounded, they form a finite set.

4. Proof of Theorem 1. Let \( \delta \) be in \((0, 1)\), to be selected later. Apply Lemma 3 with this \( \delta \) to get a unit \( \eta \) and apply Lemma 1 with this unit and with \( \gamma = \alpha^d \). Since \( D^2\alpha^d\eta \in \mathbb{Z} + \cdots + \alpha^d\mathbb{Z} \), we obtain
\[ D^2\eta\alpha^d = a_0 + a_1\alpha + \cdots + a_d\alpha^d = P(\alpha), \]
where, by Corollary 1, \( P(X) \) is an integer polynomial of degree \( d \) and
\[ |P(\alpha)| \asymp H(P)^{-d} \asymp H^{-d}. \]
By Lemmata 2 and 3, each coefficient of \( P(X) \) has its \( p \)-adic absolute value \( \ll (\log 3H(P))^{-1/r} \), except the leading coefficient, whose \( p \)-adic absolute value equals \( |D|^2 / p^r \).

We then infer from Lemma 4 that all the roots of \( P(X) \) in \( \mathbb{C}_p \) have their \( p \)-adic absolute value \( \ll (\log 3H(P))^{-1/(d^r)} \). This proves (2.2).

It now remains to guarantee that \( P(X) \) has a root very close to \( \alpha \). To this end, we proceed to check that
\[ |P'(\alpha)| \gg H(P). \]
Since
\[ P'(\alpha) = a_1 + \cdots + da_d\alpha^{d-1}, \]
we get
\[ P'(\alpha) = D^2(\text{Tr}(\eta\alpha^d\beta_1) + 2\alpha\text{Tr}(\eta\alpha^d\beta_2) + \cdots + d\alpha^{d-1}\text{Tr}(\eta\alpha^d\beta_d)), \]
hence,
\[ P'(\alpha) = D^2 \sum_{i=0}^d \sum_{k=1}^d k\alpha^{k-1}\sigma_i(\eta\alpha^d\beta_k). \]
Let us write
\[ P'(\alpha) = D^2 \sum_{i=0}^d A_i\sigma_i(\eta) \]
with
\[ A_i = \sigma_i(\alpha^d) \sum_{k=1}^{d} k\alpha^{k-1}\sigma_i(\beta_k), \quad i = 0, \ldots, d. \]

Observe first that
\[ \sum_{i=1}^{d} A_i \neq 0. \]

Indeed, if this is not the case, note that the above formulæ hold for any unit \( \eta \) in \( K \), thus we can in particular work with the unit \( \eta = 1 \), that is, with \( P(X) = D^2X^d \) and \( P'(\alpha) = dD^2\alpha^{d-1} \); we get
\[ d\alpha^{d-1} = A_0 = \alpha^d \sum_{k=1}^{d} k\alpha^{k-1}\beta_k, \]
hence,
\[ d = \sum_{k=1}^{d} k\alpha^k\beta_k. \]

Taking the trace, and recalling that \( \text{Tr}(\alpha^k\beta_k) = 1 \), we get \( d(d+1) = \sum_{k=1}^{d} k \), a contradiction.

Write
\[ P'(\alpha) = D^2 \sum_{i=1}^{d} A_i\sigma_i(\eta) + O(H^{-d}) = D^2\sigma_1(\eta) \sum_{i=1}^{d} A_i + B \]
with
\[ |B| \leq D^2 \sum_{2 \leq i \leq d} |A_i| \cdot |\sigma_1(\eta)| \cdot \left| \frac{\sigma_i(\eta)}{\sigma_1(\eta)} - 1 \right| + O(H^{-d}). \]

Selecting now \( \delta \) such that
\[ \delta \sum_{2 \leq i \leq d} |A_i| \leq \frac{1}{3} \sum_{i=1}^{d} |A_i|, \]
we infer from Lemma 3 that
\[ |P'(\alpha)| \geq \frac{1}{2} D^2|\sigma_1(\eta)\sum_{i=1}^{d} A_i| \]
when \( H \) is sufficiently large. This gives
\[ |P'(\alpha)| \gg |\sigma_1(\eta)| \gg H. \]
Consequently, \( P(X) \) has a root \( \xi \) such that
\[ |\alpha - \xi| \ll H(P)^{-d-1} \ll H(\xi)^{-d-1}. \]
Classical arguments (see end of the proof of Theorem 2.11 in [2]) show that \( \xi \) must be real and of degree \( d \) if \( H \) is sufficiently large. This proves (2.1). Inequality (2.3) follows from (2.1) and (2.2) together with the fact that \( \xi \) is of degree \( d \).

5. Proof of Theorem 2. The constants implicit in \( \ll \) and \( \gg \) below depend on \( \mathbb{K}, p \) and \( \lambda \). By Rolle’s theorem, there exists a positive real number \( \lambda' \), depending on \( \lambda \) and on \( d \), such that the minimal polynomial \( P(X) \) of any real number \( \xi \) of sufficiently large height and for which (2.4) holds is of degree \( d \) and satisfies

\[
|P(\alpha)| \leq \lambda' H(P)^{-d}.
\]

Let \( (\eta_m)_{m \geq 1} \) be as in Lemma 5. By Lemma 6, it is sufficient to prove Theorem 2 for the integer polynomials \( P(X) \) as above such that

\[
P(\alpha) = \gamma \eta_m = a_0 + a_1 \alpha + \cdots + a_d \alpha^d.
\]

Let \( \xi_i \) be the roots of \( P(X) \) in \( \mathbb{C}_p \) and set

\[
u := \max_{1 \leq i \leq d} |\xi_i|_p.
\]

Assume that \( u \leq 1 \). It follows from Lemma 4 that

\[
|a_k|_p \leq u|a_d|_p, \quad 0 \leq k < d,
\]

thus, taking \( |a_d|_p P(X) \), which is still an integer polynomial, in place of \( P(X) \), we can assume that \( |a_d|_p = 1 \) and

\[
|a_k|_p \leq u, \quad 0 \leq k < d.
\]

For \( j = 1, \ldots, d \), we then have

\[
\gamma \eta_m \alpha^{-d} - \tau_j(\gamma \eta_m \alpha^{-d}) = \sum_{k=0}^{d-1} a_k (\alpha^{k-d} - \tau_j(\alpha^{k-d})),
\]

hence,

\[
|\gamma \eta_m \alpha^{-d} - \tau_j(\gamma \eta_m \alpha^{-d})|_p \ll u.
\]

Since \( |\eta_m|_p = 1 \), we get

\[
\left| \frac{\tau_j(\eta_m)}{\eta_m} \frac{\tau_j(\gamma) \alpha^d}{\gamma \tau_j(\alpha^d)} - 1 \right|_p \ll u.
\]

Upon writing

\[
\eta_m = \varepsilon_1^{\mu_1,m} \cdots \varepsilon_r^{\mu_r,m},
\]

we thus have

\[
u \gg \left| \left( \frac{\tau_j(\varepsilon_1)}{\varepsilon_1} \right)^{-\mu_1,m} \cdots \left( \frac{\tau_j(\varepsilon_r)}{\varepsilon_r} \right)^{-\mu_r,m} \frac{\tau_j(\gamma) \alpha^d}{\gamma \tau_j(\alpha^d)} - 1 \right|_p.
\]
If
\[
\frac{\tau_j(\eta_m)}{\eta_m} = \frac{\gamma \tau_j(\alpha^d)}{\tau_j(\gamma)\alpha^d}
\]
for \(j = 1, \ldots, d\), then the number \(\gamma \eta_m \alpha^{-d}\) is equal to all its conjugates, hence is rational, and we have
\[
P(\alpha) = b\alpha^d
\]
with \(b \in \mathbb{Q}\), hence \(P(X) = bX^d\), a contradiction. For every \(m\), there thus exists an index \(j\) such that \(1 \leq j \leq d\) and
\[
\left(\frac{\tau_j(\epsilon_1)}{\epsilon_1}\right)^{-\mu_{1,m}} \cdots \left(\frac{\tau_j(\epsilon_r)}{\epsilon_r}\right)^{-\mu_{r,m}} \frac{\tau_j(\gamma)\alpha^d}{\gamma \tau_j(\alpha^d)} \neq 1.
\]
Consequently, by the theory of linear forms in non-Archimedean logarithms (see e.g. Yu [10]), there exists a positive constant \(\kappa\) such that
\[
u \gg \left(\max_{1 \leq i \leq r} |\mu_{i,m}| \right)^{-\kappa}.
\]
As in the proof of Lemma 5, the matrix \((\log |\sigma_j(\epsilon_i)|)_{1 \leq i \leq r, 1 \leq j \leq r}\) being regular, we have
\[
|\log \eta_m| \asymp \max_{1 \leq i \leq r} |\mu_{i,m}|.
\]
Combined with \(\eta_m \asymp H(P)^{-d}\) and (5.1), this gives
\[
u \gg (\log 3H(\xi))^{-\kappa}.
\]

References


Mathématiques
Université Louis Pasteur
7, rue René Descartes
67084 Strasbourg Cedex, France
E-mail: bugeaud@math.u-strasbg.fr

Institut de Mathématiques
Université Bordeaux I
351, cours de la Libération
33405 Talence Cedex, France
E-mail: demathan@math.u-bordeaux1.fr

Received on 7.11.2008
and in revised form on 5.3.2009