Publ. Math. Debrecen
80/3-4 (2012), 417–426
DOI: 10.5486/PMD.2012.5098

Comments on the distribution modulo one of powers of Pisot and Salem numbers

By TOUFIK ZAÏMI (Oum El Bouaghi)

Abstract. We consider the sequence of distances to the nearest integer $\|\lambda\alpha^n\|$, $n = 1, 2, 3, \ldots$, where λ is a real number and α is a Salem number. We prove a characterization of the numbers λ satisfying the inequality $\limsup_{n\to\infty} \|\lambda\alpha^n\| < \varepsilon$, where $\varepsilon \in]0, C(\alpha)]$ and $C(\alpha)$ is the inverse of the length of the minimal polynomial of α. This allows us to extend a related result, on Salem numbers, due to A. H. Fan and J. Schmeling [5].

1. Introduction

Let throughout θ be a real number greater than 1, n an element of the set $\mathbb{N}$ of nonnegative rational integers, and λ a nonzero real number. For a point t of the real line $\mathbb{R}$ we denote by $\|t\|$ the usual distance from t to the ring of rational integers $\mathbb{Z}$, that is $\|t\| = \min_{k\in\mathbb{Z}} |t - k|$. Nearly a century ago, A. Thue [10] proved that θ is an algebraic number when there are some positive constants c_0 and $c_1 < 1$ such that $\|\theta^n\| \leq c_0 c_1^n$ for all n. Some years after this, G.-H. Hardy [6] showed that this last condition implies in fact that θ belongs to the set S of Pisot numbers. A Pisot number is a real algebraic integer greater than 1 whose other conjugates over the field of the rationals $\mathbb{Q}$ are of modulus less than 1. Conversely, it is easy to check (see also the proof of the Theorem below) that if $\theta \in S$ and β is an integer of the field $\mathbb{Q}(\theta)$, then there are positive quantities, say again c_0 and c_1, depending only on θ and β, such that $\|\beta\theta^n\| \leq c_0 c_1^n < c_0$ for all n. Using arguments from complex analysis, C. Pisot proved, in 1938, that

Mathematics Subject Classification: 11J71, 11R06, 11R04.
Key words and phrases: distrubition modulo one, special algebraic numbers.

if $\sum_{n\in\mathbb{N}} \|\lambda\theta^n\|^2 < \infty$ for some λ, then $\theta \in S$ and $\lambda \in \mathbb{Q}(\theta)$ [7]. Almost in the same period, T. Vijayaraghavan and C. Pisot showed independently the following characterization of elements of S among real algebraic numbers greater than 1 (see for example [1, Theorem 5.4.1]).

Theorem A. *If θ is an algebraic number, then $\theta \in S$ if and only if $\lim_{n\to\infty} \|\lambda\theta^n\| = 0$ for some λ.*

The question whether there is a transcendental number θ satisfying the equality $\lim_{n\to\infty} \|\lambda\theta^n\| = 0$ for some λ, is still unsolved, and the above mentioned result of Pisot [7] is the most significant partial answer to this problem.

Notice also that an important partial answer to the analogous question, where λ is restricted to the interval $[1, \infty[$, is due to D. W. Boyd [2]. Another remarkable class of algebraic numbers is the set T of Salem numbers. A Salem number is a real algebraic integer greater than 1 whose other conjugates over $\mathbb{Q}$ are of modulus at most 1 and with a conjugate of modulus 1. By the same arguments as in the proof of Theorem A it is easy to deduce the following well-known characterization of elements of $S \cup T$ among algebraic numbers in the interval $]1, \infty[$.

Theorem B. *If θ is an algebraic number, then $\theta \in S \cup T$ if and only if for each $\varepsilon > 0$ there is $\lambda = \lambda(\theta, \varepsilon)$ such that $\|\lambda\theta^n\| < \varepsilon$ for all n.*

When we speak about conjugate, minimal polynomial and degree of an algebraic number, say α, we mean over $\mathbb{Q}$. If $M_\alpha(x) = x^d + (a_{d-1}/b_{d-1})x^{d-1} + \cdots + a_0/b_0$ is the minimal polynomial of α, where $(a_k, b_k) \in \mathbb{Z} \times \mathbb{N}$ and $\gcd(a_k, b_k) = 1$ for $k \in \{0, \ldots, d-1\}$, then we denote by $C(\alpha)$ the inverse of the quantity $\left(1 + \sum_{k=0}^{d-1} |a_k/b_k|\right) \operatorname{lcm}(b_0, \ldots, b_{d-1})$. As usual the set of polynomials with coefficients in $\mathbb{Z}$ evaluated at α is noted $\mathbb{Z}[\alpha]$. The aim of this note is to prove the following result.

Theorem. *Let α be an algebraic number greater than 1. Then:*

(i) *If $\limsup_{n\to\infty} \|\lambda\alpha^n\| < C(\alpha)$ for some λ, then $\alpha \in S \cup T$ and λ belongs to the set $\Lambda(\alpha)$ of numbers of the form $\beta/\alpha^p M'_\alpha(\alpha)$, where $p \in \mathbb{N}$ and $\beta \in \mathbb{Z}[\alpha]$.*

(ii) *$\lim_{n\to\infty} \|\lambda\alpha^n\| = 0$ if and only if $\alpha \in S$ and $\lambda \in \Lambda(\alpha)$.*

(iii) *Let $\alpha \in T$ and $\varepsilon \in \,]0, C(\alpha)]$. Then, $\limsup_{n\to\infty} \|\lambda\alpha^n\| < \varepsilon$ if and only if $\lambda \in \Omega(\alpha, \varepsilon) := \left\{t \in \Lambda(\alpha),\ \sum_{i\in I} |\sigma_i(t)| < \varepsilon\right\}$, where $\{\sigma_i,\ i \in I\}$ is the set of nonreal embeddings of $\mathbb{Q}(\alpha)$ into the complex field $\mathbb{C}$.*

In fact the proof of the Theorem (ii) is essentially contained in the papers of Pisot and Vijayaraghavan, see, e.g., [3, Chapter VIII]. With the same technique

as in the last mentioned book one can characterize the numbers λ in part (i) of the Theorem, too. We prefer to state these results together with the Theorem (iii) for convenience of reference. In the next section we show some auxiliary results. The proofs of the Theorem and the corollaries below, appear in the last section.

For example if $\alpha = (1+\sqrt{5})/2$, then $M_\alpha(x) = x^2 - x - 1$, $\alpha \in S$ and $C(\alpha) = 1/3$. By the Theorem (ii) we have $\lim_{n\to\infty} \|\lambda\alpha^n\| = 0 \Leftrightarrow \lambda \in \Lambda(\alpha) = \{\beta/\sqrt{5}, \beta \in \mathbb{Z}[\alpha]\}$ (α is a unit), and the Theorem (i) yields $\limsup_{n\to\infty} \|\lambda\alpha^n\| \geq 1/3$ when $\lambda \notin \Lambda(\alpha)$. A corollary of a recent result of A. Dubickas [4, Theorem 1] asserts that when α is an algebraic number greater than 1, there is a constant, say $c_2(\alpha)$, such that $\limsup_{n\to\infty} \|\lambda\alpha^n\| \geq c_2(\alpha)$, unless $\alpha \in S \cup T$ and $\lambda \in \mathbb{Q}(\alpha)$. The Theorem (i) implies immediately the following.

Corollary 1. *Let α be an algebraic number greater than* 1. *Then*

$$\limsup_{n\to\infty} \|\lambda\alpha^n\| \geq C(\alpha),$$

unless $\alpha \in S \cup T$ and $\lambda \in \Lambda(\alpha)$.

It is worth noting that the quantity $c_2(\alpha)$ in the above mentioned result of Dubickas satisfies $c_2(\alpha) \geq C(\alpha)$, and so Corollary 1 extends only the set of values of λ when $\alpha \in S \cup T$.

In [5], A. H. Fan and J. Schmeling proved that for any $\alpha \in T$ and any $\varepsilon > 0$, the set $X(\alpha, \varepsilon)$ of real numbers, say s, satisfying

$$\|s\alpha^n\| < \varepsilon \quad \text{for all } n, \tag{1}$$

contains a relatively dense subset $R = R(\alpha, \varepsilon)$ of $\mathbb{R}$ (there is a positive constant ρ such that each interval with length ρ meets R). More precisely, they proved that R is the set of integers β of $\mathbb{Q}(\alpha)$ such that the other conjugates of β are of modulus less than ε. It is clear that $X(\alpha, \varepsilon) = \mathbb{R}$ when $\varepsilon > 1/2$, and it is easy to check that the last mentioned result of Fan and Schmeling remains true when $\alpha \in S$. The Theorem above implies that the solutions of (1) cannot go beyond the set $\Lambda(\alpha)$ when $\varepsilon < C(\alpha)$. More precisely, we have the following.

Corollary 2. *Let $\alpha \in S \cup T$ and $\varepsilon \in]\,0, C(\alpha)[\,$. Then, $X(\alpha, \varepsilon) \subset \Lambda(\alpha)$. Moreover, if $\alpha \in T$ then $X(\alpha, \varepsilon) \subset \Omega(\alpha, \rho)$, where $\rho \in]\,\varepsilon, C(\alpha)]$.*

2. Some lemmas

For an algebraic number α we denote by $\sigma_1, \ldots, \sigma_d$ the distinct embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$, where σ_1 is the identity of $\mathbb{Q}(\alpha)$. The trace, of the extension

$\mathbb{Q}(\alpha) \supset \mathbb{Q}$, of an element $\beta \in \mathbb{Q}(\alpha)$ is $\mathrm{Tr}(\beta) = \mathrm{Tr}_{\mathbb{Q}(\alpha)}(\beta) := \sum_{l=1}^{d} \sigma_l(\beta)$. As usual we denote by $\mathbb{Z}_{\mathbb{Q}(\alpha)}$ the ring of the integers of the field $\mathbb{Q}(\alpha)$. Let us now prove the following simple statements from linear algebra.

Lemma 1. *Let α be an algebraic number and $M_\alpha(x) = \prod_{l=1}^{d}(x - \alpha_l) = x^d + r_{d-1}x^{d-1} + \cdots + r_0$. Then, the set $\{\gamma_0, \ldots, \gamma_{d-1}\}$, where*

$$\gamma_k = \frac{\sum_{i=1+k}^{d} r_i \alpha^{i-1-k}}{M'_\alpha(\alpha)} \quad \text{for } k \in \{0, \ldots, d-1\}$$

and $r_d = 1$, is a base of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ satisfying

$$\mathrm{Tr}_{\mathbb{Q}(\alpha)}(\gamma_k \alpha^i) = \begin{cases} 1 & \text{if } k = i \text{ and } (i,k) \in \{0, \ldots, d-1\}^2 \\ 0 & \text{if } k \neq i \text{ and } (i,k) \in \{0, \ldots, d-1\}^2. \end{cases} \tag{2}$$

In terms of matrices, the relation (2) *may also be written*

$$[\alpha_l^{j-1}][\sigma_j(\gamma_{l-1})] = [\sigma_j(\gamma_{l-1})][\alpha_l^{j-1}] = I_d, \tag{3}$$

where I_d is the identity matrix, and j and $l \in \{1, \ldots, d\}$ denote the row and column number, respectively.

Proof. It is clear that $M'_\alpha(\alpha) = dr_d\alpha^{d-1} + \cdots + r_1$ is a nonzero element of $\mathbb{Q}(\alpha)$. Since each quantity of the form $\sum_{i=k+1}^{d} r_i \alpha^{i-(k+1)}$, where $k \in \{0, \ldots, d-1\}$, is a polynomial in α with degree $d-(k+1)$ having rational coefficients, the numbers $\gamma_0, \ldots, \gamma_{d-1}$ belong to $\mathbb{Q}(\alpha)$ and are $\mathbb{Q}-$linearly independent; thus $\{\gamma_0, \ldots, \gamma_{d-1}\}$ is a base of $\mathbb{Q}(\alpha)$. Set $\sigma_j(\alpha) = \alpha_j$ for $j \in \{1, \ldots, d\}$. Then, the known equalities [9, p. 56] $\mathrm{Tr}(\alpha^{d-1}/M'_\alpha(\alpha)) = 1$ and $\mathrm{Tr}(\alpha^k/M'_\alpha(\alpha)) = 0$ for $k \in \{0, \ldots, d-2\}$ and $d \geq 2$, together with the relation $\mathrm{Tr}(\gamma_k\alpha^n) = r_{k+1}\,\mathrm{Tr}(\alpha^n/M'_\alpha(\alpha)) + \cdots + r_d\,\mathrm{Tr}(\alpha^{d-1-k+n}/M'_\alpha(\alpha))$, yield $\mathrm{Tr}(\gamma_k\alpha^k) = r_d$ and $\mathrm{Tr}(\gamma_k\alpha^i) = 0$ when $i \in \{0, \ldots, k-1\}$. By the identity $\gamma_k = -\big(\sum_{i=0}^{k} r_i\alpha^i\big)/(M'_\alpha(\alpha)\alpha^{k+1})$, we obtain $\mathrm{Tr}(\gamma_k\alpha^i) = 0$ when $(i,k) \in \{k+1, \ldots, d-1\} \times \{0, \ldots, d-2\}$, and the relation (2) follows immediately.

For each $(j,l) \in \{1, \ldots, d\}^2$ we have $\mathrm{Tr}(\alpha^{j-1}\gamma_{l-1}) = \alpha_1^{j-1}\sigma_1(\gamma_{l-1}) + \ldots$ $\cdots + \alpha_d^{j-1}\sigma_d(\gamma_{l-1}) = \sigma_1(\alpha_1^{j-1}\gamma_{l-1}) + \cdots + \sigma_d(\alpha_1^{j-1}\gamma_{l-1})$, and so (2) implies $[\alpha_l^{j-1}][\sigma_j(\gamma_{l-1})] = I_d$. The last equality yields the relation (3), and the assertion (3) $\Rightarrow$ (2) is trivially true. □

Lemma 2. *Let α be an algebraic integer. Then,*

$$\{\varsigma \in \mathbb{Q}(\alpha),\ \mathrm{Tr}_{\mathbb{Q}(\alpha)}(\varsigma\mathbb{Z}[\alpha]) \subset \mathbb{Z}\} = \left\{\frac{\beta}{M'_\alpha(\alpha)},\ \beta \in \mathbb{Z}[\alpha]\right\}.$$

PROOF. Let $\varsigma \in \mathbb{Q}(\alpha)$. With the notation of Lemma 1 there is a subset $\{x_0, \dots, x_{d-1}\}$ of $\mathbb{Q}$ such that $\varsigma = \sum_{k=0}^{d-1} x_k \gamma_k$. Then, the relation (2) yields $\mathrm{Tr}(\varsigma) = x_0$, $\mathrm{Tr}(\varsigma\alpha) = x_1, \dots, \mathrm{Tr}(\varsigma\alpha^{d-1}) = x_{d-1}$. It follows when $\mathrm{Tr}(\varsigma\mathbb{Z}[\alpha]) \subset \mathbb{Z}$ that $\{x_0, \dots, x_{d-1}\} \subset \mathbb{Z}$, and so $\varsigma = \beta/M'_\alpha(\alpha)$ for some $\beta \in \mathbb{Z}[\alpha]$, since α is an algebraic integer. Conversely, let β and η be two elements of the ring $\mathbb{Z}[\alpha]$ and let $\{m_0, \dots, m_{d-1}\}$ be a subset of $\mathbb{Z}$ such that $\beta\eta = \sum_{k=0}^{d-1} m_k \alpha^k$. Then, $\mathrm{Tr}(\beta\eta/M'_\alpha(\alpha)) = \sum_{k=0}^{d-1} m_k \,\mathrm{Tr}(\alpha^k/M'_\alpha(\alpha)) = m_{d-1}$ and so $\mathrm{Tr}(\beta\eta/M'_\alpha(\alpha)) \in \mathbb{Z}$; thus $\mathrm{Tr}((\beta/M'_\alpha(\alpha))\mathbb{Z}[\alpha]) \subset \mathbb{Z}$. □

The following lemma is a well-known result on Salem numbers.

Lemma 3. *Let α be a Salem number of degree d. Then, d is even, $1/\alpha$ is a conjugate of α, $d \geq 4$ and α has $d-2$ conjugates, say $\alpha_3, \dots, \alpha_d$, of modulus 1. If these last numbers are labelled so that $\alpha_{2j} = \overline{\alpha_{2j-1}}$ for $j \in \{2, \dots, d/2\}$, then for any $\varepsilon > 0$ and any subset $\{\beta_3, \dots, \beta_d\}$ of $\mathbb{C}$, where $\beta_{2j} = \overline{\beta_{2j-1}}$ and $|\beta_{2j}| = 1$ for $j \in \{2, \dots, d/2\}$, there is n arbitrarily large such that $|\alpha_k^n - \beta_k| < \varepsilon$ for $k \in \{3, \dots, d\}$.*

A proof of Lemma 3 may be found in [11] and is based on a result of C. Pisot on the arguments of $\alpha_3, \dots, \alpha_d$ (see, for example [8, p. 32]). Let us also show the following.

Lemma 4. *Let a be a nonzero rational integer and α an algebraic number of degree d. If there are at least $\big((2|a|-1)\sum_{b|a,\, b\in\mathbb{N}} 1\big)^d + 1$ distinct algebraic integers of the form $a\alpha^n$, where $n \in \mathbb{N}$, then α is an algebraic integer.*

PROOF. Let $M := \{n \in \mathbb{N},\ a\alpha^n \in \mathbb{Z}_{\mathbb{Q}(\alpha)}\}$. By hypothesis, there exists $m \in M \cap [1, \infty[$. Let $\{\omega_1, \dots, \omega_d\}$ be a base of the $\mathbb{Z}$-module $\mathbb{Z}_{\mathbb{Q}(\alpha)}$. Then, $\alpha^m = \sum_{j=1}^{d} (p_{m,j}/q_{m,j})\omega_j$, where $(p_{m,j}, q_{m,j}) \in \mathbb{Z}\times\mathbb{N}$ and $\gcd(p_{m,j}, q_{m,j}) = 1$,

$$a\alpha^m = \frac{a}{q_{m,1}} p_{m,1}\omega_1 + \cdots + \frac{a}{q_{m,d}} p_{m,d}\omega_d,$$

and so $(q_{m,1}, \dots, q_{m,d}) \in D \times \cdots \times D$, where D is the set of positive divisors of a in the ring $\mathbb{Z}$. As $\mathrm{Card}(D) = \sum_{b|a,\, b\in\mathbb{N}} 1$ and $\mathrm{Card}(M) > (2|a|-1)^d \,\mathrm{Card}(D \times \cdots \times D)$, by the pigeonhole principle we obtain that there is $(q_1, \dots, q_d) \in D \times \cdots \times D$ such that $\mathrm{Card}\{n \in M,\ (q_{n,1}, \dots, q_{n,d}) = (q_1, \dots, q_d)\} > (2|a|-1)^d$. Set $N = \{n \in M,\ (q_{n,1}, \dots, q_{n,d}) = (q_1, \dots, q_d)\}$. Then for any $m \in N$ and any $j \in \{1, \dots, d\}$ there exist $k_{m,j} \in \mathbb{Z}$ and $r_{m,j} \in \{-(q_j - 1), \dots, 0, \dots, q_j - 1\}$ such that

$$p_{m,j} = k_{m,j} q_j + r_{m,j},$$

and so

$$\alpha^m = \beta_m + r_m,$$

where $\beta_m := \sum_{j=1}^{d} k_{m,j}\omega_j \in \mathbb{Z}_{\mathbb{Q}(\alpha)}$ and $r_m := \sum_{j=1}^{d}(r_{m,j}/q_j)\omega_j$ belongs to a finite set with cardinality $\leq \prod_{j=1}^{d}(2q_j - 1) \leq (2|a| - 1)^d$. It follows again from the pigeonhole principle that there is $(k, l) \in N \times N$ such that $k > l$ and $\alpha^k - \beta_k = \alpha^l - \beta_l$; thus $\alpha^k - \alpha^l = \beta_k - \beta_l \in \mathbb{Z}_{\mathbb{Q}(\alpha)}$. Replacing in the minimal polynomial of $\beta_k - \beta_l$ the quantity $\beta_k - \beta_l$ by the number $\alpha^k - \alpha^l$, we obtain immediately that α is a root of a monic polynomial with rational integer coefficients. □

3. The proofs

Proof of the Theorem. Set

$$\lambda\alpha^n = u_n + \varepsilon_n, \tag{4}$$

where $u_n \in \mathbb{Z}$ and $\varepsilon_n \in]-1/2, 1/2]$, that is u_n is "the" nearest rational integer to $\lambda\alpha^n$ (if $\varepsilon_n = 1/2$, then $u_n + 1$ satisfies $|\lambda\alpha^n - (u_n + 1)| = |\lambda\alpha^n - u_n|$) and $\|\lambda\alpha^n\| = |\varepsilon_n|$. With the notation of Lemma 1, we have $\lambda\alpha^{n+d} + r_{d-1}\lambda\alpha^{n+d-1} + \cdots + r_0\lambda\alpha^n = 0$ and so

$$u_{n+d} + r_{d-1}u_{n+d-1} + \cdots + r_0u_n = -(\varepsilon_{n+d} + r_{d-1}\varepsilon_{n+d-1} + \cdots + r_0\varepsilon_n). \tag{5}$$

To prove the Theorem (i) and the direct implication in the Theorem (iii) suppose that

$$\limsup_{n\to\infty} |\varepsilon_n| < \varepsilon, \tag{6}$$

where ε is fixed in the interval $]0, C(\alpha)]$ (resp., to prove the direct implication in the Theorem (ii) suppose that

$$\lim_{n\to\infty} \varepsilon_n = 0). \tag{7}$$

It is clear that (7) $\Rightarrow$ (6) $\Rightarrow$ there is $n_0 = n_0(\alpha, \lambda, \varepsilon) \in \mathbb{N}$ such that

$$|\varepsilon_n| < \varepsilon \quad \text{for all } n \geq n_0. \tag{8}$$

From now on, assume $n \geq n_0$. Then, the relations (5) and (8) give

$$|u_{n+d} + r_{d-1}u_{n+d-1} + \cdots + r_0u_n| < \left(\sum_{i=0}^{d} |r_i|\right)\varepsilon \leq \left(\sum_{i=0}^{d} |r_i|\right)C(\alpha)$$

and so $u_{n+d}+r_{d-1}u_{n+d-1}+\cdots+r_0u_n=0$, since $\left(\sum_{i=0}^{d} r_iu_{n+i}\right)\operatorname{lcm}(b_0,\ldots,b_{d-1})\in \mathbb{Z}\cap]-1,1[$. It follows again by (5) that $\varepsilon_{n+d}+r_{d-1}\varepsilon_{n+d-1}+\cdots+r_0\varepsilon_n=0$ and so there are complex numbers, say $\zeta_1,\zeta_2,\ldots,\zeta_d$, such that

$$\varepsilon_n=\zeta_1\alpha_1^n+\zeta_2\alpha_2^n+\cdots+\zeta_d\alpha_d^n. \tag{9}$$

Fix n for a moment. Then, the equality (9) yields

$$[\alpha_l^{j-1}]\begin{bmatrix}\zeta_1\alpha_1^n\\ \zeta_2\alpha_2^n\\ \vdots\\ \zeta_d\alpha_d^n\end{bmatrix}=\begin{bmatrix}\varepsilon_n\\ \varepsilon_{n+1}\\ \vdots\\ \varepsilon_{n+d-1}\end{bmatrix}$$

and so by (3) we obtain $\zeta_j\alpha_j^n=\sigma_j(\gamma_0)\varepsilon_n+\sigma_j(\gamma_1)\varepsilon_{n+1}+\cdots+\sigma_j(\gamma_{d-1})\varepsilon_{n+d-1}$, where $j\in\{1,\ldots,d\}$, $\sigma_j(\alpha)=\alpha_j$ and $\alpha:=\alpha_1$; thus

$$|\zeta_j|\le\frac{H\sum_{k=0}^{d-1}|\varepsilon_{n+k}|}{|\alpha_j^n|}<\frac{Hd\varepsilon}{|\alpha_j|^n}, \tag{10}$$

where $H=\max_{(j,l)\in\{1,\ldots,d\}^2}|\sigma_j(\gamma_{l-1})|$ depends only on α. As we may choose n arbitrarily large, we obtain immediately by (10) that $\zeta_j=0$ when $|\alpha_j|>1$ (resp., $\zeta_j=0$ when $|\alpha_j|\ge 1$); in particular we have $\zeta_1=0$. Let $\alpha_1,\ldots,\alpha_t$, where $1\le t\le d$, be the conjugates of α of modulus greater than 1 (resp., of modulus greater than or equal to 1). Then, the relation (9) gives $\varepsilon_n=\zeta_2\alpha_2^n+\cdots+\zeta_d\alpha_d^n$, where $\zeta_j=0$ when $2\le j\le t$, and the equality (4) may also be written

$$\lambda\alpha^n-\zeta_2\alpha_2^n-\cdots-\zeta_d\alpha_d^n\ =u_n. \tag{11}$$

Fix again n for a moment. Then, the relation (11) implies

$$[\alpha_l^{j-1}]\begin{bmatrix}\lambda\alpha^n\\ -\zeta_2\alpha_2^n\\ \vdots\\ -\zeta_d\alpha_d^n\end{bmatrix}=\begin{bmatrix}u_n\\ u_{n+1}\\ \vdots\\ u_{n+d-1}\end{bmatrix},$$

and so by (3) we obtain

$$\lambda=\frac{\gamma_0u_n+\gamma_1u_{n+1}+\cdots+\gamma_{d-1}u_{n+d-1}}{\alpha^n}\in\mathbb{Q}(\alpha), \tag{12}$$

$-\zeta_j = (\sigma_j(\gamma_0)u_n + \sigma_j(\gamma_1)u_{n+1} + \cdots + \sigma_j(\gamma_{d-1})u_{n+d-1})/\alpha_j^n = \sigma_j(\lambda)$ when $j \geq 2$; thus the other conjugates of the algebraic number λ are $\lambda_2 := -\zeta_2, \ldots, \lambda_d := -\zeta_d$. Consequently, we have $t = 1$, since otherwise $\zeta_2 = 0$ and so $\lambda = 0$, that is the other conjugates of α are of modulus at most 1 (resp., of modulus less than 1). Notice also that the equality (11) may also be written

$$\lambda\alpha^n + \lambda_2\alpha_2^n + \cdots + \lambda_d\alpha_d^n \ = u_n. \tag{13}$$

Let a be a nonzero rational integer such that $\{a\gamma_0/\lambda, a\gamma_1/\lambda, \ldots, a\gamma_{d-1}/\lambda\} \subset \mathbb{Z}_{\mathbb{Q}(\alpha)}$. Then (12) gives

$$a\alpha^n \in \mathbb{Z}_{\mathbb{Q}(\alpha)},$$

since $u_n \in \mathbb{Z}$ for all n. It follows by Lemma 4 that α is an algebraic integer and so $\alpha \in S \cup T$ (resp., so $\alpha \in S$). Moreover, the relation (12) implies $\alpha^{n_0}\lambda = \beta/M'_\alpha(\alpha)$ for some $\beta \in \mathbb{Z}[\alpha]$, and so $\lambda \in \Lambda(\alpha)$. This ends the proof of the Theorem (i) (with $\varepsilon = C(\alpha)$) (resp., the proof of the implication: $\lim_{n\to\infty} \|\lambda\alpha^n\| = 0 \Rightarrow \alpha \in S$ and $\lambda \in \Lambda(\alpha)$). To complete the proof of the first implication in the Theorem (iii) and also to show the two remaining implications we shall consider the cases $\alpha \in S$ and $\alpha \in T$ separately.

First suppose $\alpha \in S$, and let $\lambda^* \in \Lambda(\alpha)$. Then, there is $p \in \mathbb{N}$ such that $\alpha^p\lambda^* = \beta^*/M'_\alpha(\alpha)$ for some $\beta^* \in \mathbb{Z}[\alpha]$, and so Lemma 2 gives

$$v_n := \mathrm{Tr}_{\mathbb{Q}(\alpha)}(\lambda^*\alpha^p\alpha^{n-p}) = \lambda^*\alpha^n + \lambda_2^*\alpha_2^n + \cdots + \lambda_d^*\alpha_d^n \ \in \mathbb{Z},$$

where $\lambda_2^* = \sigma_2(\lambda^*), \ldots, \lambda_d^* = \sigma_d(\lambda^*)$ and $n \in \mathbb{N} \cap [p, \infty[$. Hence, $|\lambda^*\alpha^n - v_n| = |\lambda_2^*\alpha_2^n + \cdots + \lambda_d^*\alpha_d^n| \leq \left(\sum_{j=2}^d |\lambda_j^*|\right) \max_{2\leq j\leq d} |\alpha_j|^n$ and so $\lim_{n\to\infty} |\lambda^*\alpha^n - v_n| = 0$; thus $\lim_{n\to\infty} \|\lambda^*\alpha^n\| = 0$ and this ends the proof of the Theorem (ii).

Finally, assume $\alpha \in T$. Without loss of generality set $\alpha_2 := 1/\alpha$ and $\alpha_{2j} = \overline{\alpha_{2j-1}}$ for $j \in \{2, \ldots, d/2\}$ (see Lemma 3). To show the relation: $\lambda \in \Omega(\alpha, \varepsilon)$, we shall prove

$$\limsup_{n\to\infty} |\varepsilon_n| = \sum_{j=3}^{d} |\lambda_j|. \tag{14}$$

Notice by (4) and (13) that

$$\lambda_2\alpha_2^n + \lambda_3\alpha_3^n \cdots + \lambda_d\alpha_d^n = -\varepsilon_n, \tag{15}$$

$|\lambda_2\alpha_2^n + \lambda_3\alpha_3^n \cdots + \lambda_d\alpha_d^n| \leq |\lambda_2|/\alpha^n + \sum_{j=3}^d |\lambda_j|$ and so $\limsup_{n\to\infty} |\varepsilon_n| \leq \sum_{j=3}^d |\lambda_j|$. To complete the proof of the equality (14) fix $\delta > 0$. Then, there is $n_1 \in \mathbb{N}$ such that $|\lambda_2\alpha_2^n| < \delta/2$ when $n \geq n_1$. For $k \in \{3, \ldots, d\}$ and $n \geq n_1$ set

$$t_{k,n} := \alpha_k^n + \frac{|\lambda_k|}{\lambda_k}.$$

Since λ is a polynomial in α with rational coefficients, we have $\lambda_{2j} = \sigma_{2j}(\lambda) = \overline{\sigma_{2j-1}(\lambda)} = \overline{\lambda_{2j-1}}$ for $j \in \{2, \dots, d/2\}$. It follows from Lemma 3 that there are infinitely many n such that

$$|t_{k,n}| < \frac{\delta}{2(d-2)\max\{|\lambda_3|, \dots, |\lambda_d|\}}$$

for all $k \in \{3, \dots, d\}$. Hence, for these n's we have, by (15),

$$|-\varepsilon_n + |\lambda_3| + \cdots + |\lambda_d|| = |\lambda_2\alpha_2^n + \lambda_3 t_{3,n} + \cdots + \lambda_d t_{d,n}| < \delta,$$

$(|\lambda_3| + \cdots + |\lambda_d|) - \delta < |\varepsilon_n|$ and so $\limsup_{n\to\infty} |\varepsilon_n| \geq \sum_{j=3}^{d} |\lambda_j| - \delta$. Letting δ tend to 0 we obtain $\limsup_{n\to\infty} |\varepsilon_n| \geq \sum_{j=3}^{d} |\lambda_j|$ and the relation (14) follows. Conversely, if $\lambda^* \in \Omega(\alpha, \varepsilon)$, where $\varepsilon \in]0, C(\alpha)]$, then similarly as for the case where $\alpha \in S$, and with the same notation, we obtain $\sum_{j=3}^{d} |\lambda_j^*| < \varepsilon$, $|\lambda^*\alpha^n - v_n| = |\lambda_2^*/\alpha^n + \lambda_3^*\alpha_3^n + \cdots + \lambda_d^*\alpha_d^n|$, $\limsup_{n\to\infty} |\lambda^*\alpha^n - v_n| \leq \sum_{j=3}^{d} |\lambda_j^*|$ and so $\limsup_{n\to\infty} \|\lambda^*\alpha^n\| < \varepsilon$. □

Proof of Corollary 1. The proof follows immediately from the Theorem (i). □

Proof of Corollary 2. Let $\alpha \in S \cup T$ and let $s \in X(\alpha, \varepsilon)$, where $\varepsilon \in]0, C(\alpha)[$. Then, $\|s\alpha^n\| < \varepsilon$ for all n, and so $\limsup_{n\to\infty} \|s\alpha^n\| \leq \varepsilon$. It follows by the Theorem (i) that $s \in \Lambda(\alpha)$. Similarly if $\alpha \in T$, then the Theorem (iii) gives $s \in \Omega(\alpha, \rho)$, where $\rho \in]\varepsilon, C(\alpha)]$. □

References

[1] M.-J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse and J.-P. Schreiber, Pisot and Salem numbers, *Birkhäuser Verlag, Basel*, 1992.

[2] D. W. Boyd, Transcendental numbers with badly distributed powers, *Proc. Amer. Math. Soc.* **23** (1969), 424–427.

[3] J. W. S. Cassels, An Introduction to Diophantine Approximation, *Cambridge University Press, Cambridge*, 1957.

[4] A. Dubickas, On the distance from a rational power to the nearest integer, *J. Number Theory* **117** (2006), 222–239.

[5] A. H. Fan and J. Schmeling, ε-Pisot numbers in any real algebraic number field are relatively dense, *J. Algebra* **272** (2004), 470–475.

[6] G.-H. Hardy, A problem of diophantine approximation, *J. Indian Math. Soc.* **11** (1919), 162–166.

[7] C. Pisot, La répartition modulo un et les nombres algébriques, *Annali Scuola Norm. Sup. Pisa* **7** (1938), 205–248.

[8] R. Salem, Algebraic Numbers and Fourier Analysis, *D. C. Heath and Co., Boston, Mass., Boston*, 1963.

[9] J. P. Serre, Local Fields, *Springer, Berlin*, 1979.

[10] A. Thue, Über eine Eigenschaft die keine transzendente Grösse haben kann, *Skrifter Videnskap Kristiania* **20** (1912), 1–15.

[11] T. Zaïmi, An arithmetical property of powers of Salem numbers, *J. Number Theory* **120** (2006), 179–191.

TOUFIK ZAÏMI
DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ LARBI BEN M'HIDI
OUM EL BOUAGHI 04000
ALGERIE

E-mail: toufikzaimi@yahoo.com

(Received January 19, 2011; revised June 14, 2011)