Characterization of the numbers which satisfy the height reducing property

Shigeki AKIYAMA, Jörg M. THUSWALDNER and Toufik ZAÏMI

ABSTRACT. *Let α be a complex number. We show that there is a finite subset F of the ring of the rational integers $\mathbb{Z}$, such that $F[\alpha] = \mathbb{Z}[\alpha]$, if and only if α is an algebraic number whose conjugates, over the field of the rationals, are all of modulus one, or all of modulus greater than one. This completes the answer to a question, on the numbers satisfying the height reducing property, posed in* [3].

1. Introduction

Following [1], we say that a complex number α satisfy the height reducing property, in short HRP, if there is a finite subset F of the ring of the rational integers $\mathbb{Z}$, such that each polynomial with coefficients in $\mathbb{Z}$, evaluated at α, belongs to the family $F[\alpha] := \left\{ \sum_{j=0}^{n} \varepsilon_j \alpha^j \mid (\varepsilon_0, ..., \varepsilon_n) \in F^{n+1}, n \in \mathbb{N} \right\}$, where $\mathbb{N}$ is the set of non-negative rational integers. In this case, we have, by [3, Theorem 1 (i)], that α is an algebraic number whose conjugates, over the field of the rationals $\mathbb{Q}$, are all of modulus one, or all of modulus greater than one (such a number α is called an expanding number [2]). Theorem 1 (ii) of [3], says also that α satisfies HRP, when it is a root of unity, or when it is an expanding number. Hence, to obtain a characterization of numbers satisfying HRP, it remains to consider the situation where the conjugates of the algebraic number α belong to the unit circle, and are not roots of unity; this case has been partially treated in [3, Theorem 2], when the greatest number of multiplicatively independent conjugates of α, over $\mathbb{Q}$, takes some optimal values.

Recall also, by [2, Theorem 1], that we may suppose that the set F, defined above, is contained in the complex field $\mathbb{C}$, without affecting the definition of the HRP; in other words, α satisfies HRP if and only if

$$\exists\ F \subset \mathbb{C} \text{ such that } \mathbb{Z}[\alpha] = F[\alpha] \text{ and } Card(F) < \infty. \qquad (1)$$

Mathematics Subject Classification (2010): 11R06, 12D10, 11R04

Key words and phrases: Height of polynomials, Special algebraic numbers, Representations of algebraic numbers

By an algebraic approach, we obtain, in this note, that the converse of Theorem 1 (i) of [3] is true, independently on the distribution, outside the open unit disc, of the conjugates of α :

Theorem. *Let* $\alpha \in \mathbb{C}$. *Then, there is a finite subset* F of $\mathbb{Z}$ *such that* $F[\alpha] = \mathbb{Z}[\alpha]$, *if and only if* α *is an algebraic number whose conjugates, over* $\mathbb{Q}$, *are all of modulus one, or all of modulus greater than one.*

The question to determine, for a number α satisfying the HRP, a corresponding complex set F with minimal cardinality, has been also partially solved in [2]. As mentioned in [3], the height reducing problem can be compared with canonical number systems and finiteness property of beta-expansions, where the set F has more specific shape (some related references may be found in [1, 2, 3, 5]). For example, a pair (α, F), satisfying (1), is called a number (resp., a canonical number) system of the ring $\mathbb{Z}[\alpha]$, if $0 \in F$ and $Card(F) = |M_\alpha(0)|$ (resp., if $F = \{0, 1, ..., |M_\alpha(0)| - 1\}$), where M_α designates, throughout, the minimal polynomial, over $\mathbb{Q}$, of the algebraic number α (the coefficients of M_α are supposed to be rational integers and their greatest common divisor is one). Recall also that a result of Lagarias and Wang implies that an expanding integer α, satisfies (1), with $F = \{0, \pm 1, ..., \pm(|M_\alpha(0)| - 1)\}$ [4].

To prove the relation (1), for some fixed pair (α, F), it is, generally, shown that there exists a positive constant $c = c(\alpha, F)$, such that for each $\beta \in \mathbb{Z}[\alpha]$, there is some $\varepsilon \in F$ verifying

$$\frac{\beta - \varepsilon}{\alpha} \in \mathbb{Z}[\alpha] \quad \text{and} \quad \left\| \phi_\alpha\left(\frac{\beta - \varepsilon}{\alpha}\right) \right\| < c,$$

where $\|.\|$ is the sup norm (for example) of the $\mathbb{Q}-$vector space

$$\mathbb{K}_\infty := \mathbb{R}^r \times \mathbb{C}^s,$$

r (resp., $2s$) denotes the number of real (resp., of non-real) conjugates, over $\mathbb{Q}$, of the algebraic number α, and Φ_∞ is the standard Minkowski's $\mathbb{Q}$-linear map

$$\Phi_\infty : \mathbb{Q}(\alpha) \to \mathbb{K}_\infty,$$

which sends α to its conjugates, over $\mathbb{Q}$, situated in $\{z \in \mathbb{C} \mid \mathrm{Im}(z) \geq 0\}$ (for example). This allows us to obtain number systems, when α is an expanding number, but not when $|\alpha| = 1$ (see for instance [2, Section 2]). An alternative solution to this problem is to add certain finite completions, corresponding to the divisors of the denominator of the fractional ideal (α), to enlarge the ring $\mathbb{K}_\infty$ and the range of the corresponding embedding Φ_∞ : this is the key of Lemma 3.1, which is the main result of this manuscript. This lemma is proved in the last section, and we recall in the next one some related notions.

2. Some definitions and notations

For each given prime $\mathfrak{p}$ of the field $K := \mathbb{Q}(\alpha)$, where α is a fixed algebraic number, choose an absolute value $|\cdot|_{\mathfrak{p}}$ in the following way. Let $\beta \in K$ be given. If $\mathfrak{p} \mid \infty$ (that is $\mathfrak{p}$ is not finite), then denote by $\beta^{(\mathfrak{p})}$ the associated conjugate of β, and set $|\beta|_{\mathfrak{p}} = |\beta^{(\mathfrak{p})}|$, (resp., $|\beta|_{\mathfrak{p}} = |\beta^{(\mathfrak{p})}|^2$), when $\mathfrak{p}$ is real (resp., is non-real). For $\mathfrak{p}$ being finite, put $|\beta|_{\mathfrak{p}} = \mathfrak{N}(\mathfrak{p})^{-v_{\mathfrak{p}}(\beta)}$, where $\mathfrak{N}(\cdot)$ is the norm of a (fractional) ideal and $v_{\mathfrak{p}}(\beta)$ denotes the exponent of $\mathfrak{p}$ in the prime ideal decomposition of the principal ideal (β). Write $K_{\mathfrak{p}}$ for the completion of K w. r. t. the absolute value $|\cdot|_{\mathfrak{p}}$ and recall that this absolute value induces a metric on $K_{\mathfrak{p}}$.

Let $\mathcal{O}$ be the ring of integers of K,

$$\alpha\,\mathcal{O} = \frac{\mathfrak{a}}{\mathfrak{b}} \tag{2}$$

with $\mathfrak{a}, \mathfrak{b}$ coprime ideals in $\mathcal{O}$,

$$S_\alpha = \{\mathfrak{p} : \mathfrak{p} \mid \infty \text{ or } \mathfrak{p} \mid \mathfrak{b}\},$$

and define

$$\mathbb{K}_\alpha = \prod_{\mathfrak{p} \in S_\alpha} K_{\mathfrak{p}} = \mathbb{K}_\infty \times \mathbb{K}_{\mathfrak{b}}, \quad \text{with} \quad \mathbb{K}_\infty = \prod_{\mathfrak{p} \mid \infty} K_{\mathfrak{p}} \quad \text{and} \quad \mathbb{K}_{\mathfrak{b}} = \prod_{\mathfrak{p} \mid \mathfrak{b}} K_{\mathfrak{p}}.$$

Then, $\mathbb{K}_\infty = \mathbb{R}^r \times \mathbb{C}^s$, and the elements of $\mathbb{Q}(\alpha)$ are embedded in $\mathbb{K}_\alpha$ "diagonally" by the canonical ring homomorphism

$$\Phi_\alpha : \mathbb{Q}(\alpha) \to \mathbb{K}_\alpha, \quad \beta \mapsto \prod_{\mathfrak{p} \in S_\alpha} \beta,$$

where $\mathbb{K}_\alpha$ is equipped with the product metric of the metrics induced by the absolute values $|\cdot|_{\mathfrak{p}}$. Finally, notice that $\mathbb{Q}(\alpha)$ acts multiplicatively on $\mathbb{K}_\alpha$ by the relation

$$\beta \cdot (z_{\mathfrak{p}})_{\mathfrak{p} \in S_\alpha} = (\beta z_{\mathfrak{p}})_{\mathfrak{p} \in S_\alpha},$$

where $\beta \in \mathbb{Q}(\alpha)$.

3. Proof of the Theorem

To make clear the proof of the theorem let us first show three auxiliary lemmas. The first one is the main tool in this proof.

Lemma 1. *Let α be an algebraic number, with degree n, and without conjugates, over $\mathbb{Q}$, strictly inside the unit circle. Then, there is a set $F \subset \mathbb{Z}[\alpha]$, with cardinality at most $2^n\,|M_\alpha(0)|$, and a constant $c > 0$ such that for each $\beta \in \mathbb{Z}[\alpha]$, we can choose $\varepsilon \in F$, in a way that $\alpha^{-1}(\beta - \varepsilon) \in \mathbb{Z}[\alpha]$ with*

$$\left|\alpha^{-1}(\beta - \varepsilon)\right|_{\mathfrak{p}} < \max\{|\beta|_{\mathfrak{p}}, c\}, \tag{3}$$

for each $\mathfrak{p} \in S_\alpha$.

Proof. Let R be a complete set of coset representatives of the finite ring $\mathbb{Z}[\alpha]/\alpha\mathbb{Z}[\alpha]$ and let $\mathcal{U}$ be the collection of the 2^n open orthants of $\mathbb{K}_\infty \simeq \mathbb{R}^n$, where $n = r + 2s$. Since $\Phi_\infty(\alpha\mathbb{Z}[\alpha])$ contains a lattice with rank n, of $\mathbb{K}_\infty$, for each $r \in R$ and each $U \in \mathcal{U}$, the set $\alpha\mathbb{Z}[\alpha] + r$ contains an element $\varepsilon = \varepsilon(r, U)$ with $\Phi_\infty(\varepsilon) \in U$. We define the finite set

$$F = \{\varepsilon(r, U) \,:\, r \in R,\, U \in \mathcal{U}\}.$$

Now, fix $\beta \in \mathbb{Z}[\alpha]$ and pick $\varepsilon \in F$ such that $\Phi_\infty(\varepsilon)$ lies in the same closed orthant as $\Phi_\infty(\beta)$ and satisfies $\alpha^{-1}(\beta - \varepsilon) \in \mathbb{Z}[\alpha]$. It remains to prove that the inequality (3) holds for each $\mathfrak{p} \in S_\alpha$.

Assume first that $\mathfrak{p} \mid \mathfrak{b}$. Then, as $|\alpha|_\mathfrak{p} > 1$ holds by (2), we gain, setting $c_{\varepsilon,\mathfrak{p}} = |\varepsilon|_\mathfrak{p}$, that

$$|\alpha^{-1}(\beta - \varepsilon)|_\mathfrak{p} < \max\{|\beta|_\mathfrak{p}, |\varepsilon|_\mathfrak{p}\} = \max\{|\beta|_\mathfrak{p}, c_{\varepsilon,\mathfrak{p}}\}. \quad (4)$$

Next, let $\mathfrak{p} \mid \infty$ be real. Since $\beta^{(\mathfrak{p})}\varepsilon^{(\mathfrak{p})} \geq 0$ by the choice of ε and $|\alpha|_\mathfrak{p} \geq 1$ holds by assumption, setting $c_{\varepsilon,\mathfrak{p}} = 2|\varepsilon|_\mathfrak{p}$ we have

$$|\alpha^{-1}(\beta - \varepsilon)|_\mathfrak{p} \leq |\beta - \varepsilon|_\mathfrak{p} = |\beta^{(\mathfrak{p})} - \varepsilon^{(\mathfrak{p})}| < \max\{|\beta|_\mathfrak{p}, c_{\varepsilon,\mathfrak{p}}\}. \quad (5)$$

Finally, let $\mathfrak{p} \mid \infty$ be non-real and note that $|\alpha|_\mathfrak{p} \geq 1$ holds by assumption also in this case. By the choice of ε, the complex numbers $\beta^{(\mathfrak{p})}$ and $\varepsilon^{(\mathfrak{p})}$ lie in the same quadrant of $\mathbb{C}$. As $\varepsilon^{(\mathfrak{p})}$ lies in the interior of this quadrant, there is $\eta > 0$ depending only on ε and $\mathfrak{p}$ such that $|\arg\beta^{(\mathfrak{p})} - \arg\varepsilon^{(\mathfrak{p})}| < \frac{\pi}{2} - \eta$. Using this fact, by an easy geometric consideration we obtain

$$|\alpha^{-1}(\beta - \varepsilon)|_\mathfrak{p} \leq |\beta - \varepsilon|_\mathfrak{p} = |\beta^{(\mathfrak{p})} - \varepsilon^{(\mathfrak{p})}|^2 < \max\{|\beta|_\mathfrak{p}, c_{\varepsilon,\mathfrak{p}}\} \quad (6)$$

for some $c_{\varepsilon,\mathfrak{p}} > 0$ depending only on ε and $\mathfrak{p}$. The inequality (3) now follows from (4), (5) and (6) with $c = \max\{c_{\varepsilon,\mathfrak{p}} \,:\, \varepsilon \in F,\, \mathfrak{p} \in S_\alpha\}$. ■

Lemma 2. ([6]) *The ring $\Phi_\alpha(\mathbb{Z}[\alpha])$ is a discrete subset of $\mathbb{K}_\alpha$.*

Proof. The result is a corollary of Lemmas 3.1 and 3.2 of [6], where it is shown that $\Phi_\alpha(\mathbb{Z}[\alpha])$ is a Delone set in $\mathbb{K}_\alpha$. ■

Lemma 3. ([2]) *If a pair (α, F) satisfies the relation (1), then there is a finite subset F' of $\mathbb{Z}$ such that $F'[\alpha] = F[\alpha]$.*

Proof. The result follows immediately, by [2, Theorem 1], where a upper bound (depending only on α and F) of $Card(F')$, is given. ■

Proof of the theorem. The direct implication is a corollary of Theorem 1 in [2]. By iterating Lemma 1, we obtain the other implication, using Lemmas 2 and 3. ■

References

[1] S. Akiyama, P. Drungilas and J. Jankauskas, *Height reducing problem on algebraic integers*, Functiones et Approximatio, Commentarii Mathematici, **47** (2012), 105-119.

[2] S. Akiyama and T. Zaïmi, *Comments on the height reducing problem II,* submitted.

[3] S. Akiyama and T. Zaïmi, *Comments on the height reducing problem,* Cent. Europ. J. Math., **11** (2013), 1616-1627.

[4] J. C. Lagarias and Y. Wang, *Integral self-affine tiles in* $\mathbb{R}^n$. *Part II : Lattice tilings*, J. Fourier Anal. Appl., **3** (1997), 83-102.

[5] A. Pethő, *Connections between power integral bases and radix representations in algebraic number fields*, Proceedings of the 2003 Nagoya Conference "Yokoi-Chowla Conjecture and Related Problems", 115-125, Saga Univ., Saga, 2004.

[6] W. Steiner and J. M. Thuswaldner, *Rational self-affine tiles,* Trans. Amer. Math. Soc., to appear.

Institute of mathematics, University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki, 350-0006 Japan

E-mail address: akiyama@math.tsukuba.ac.jp

Department of mathematics and statistics, Leoben University, Franz-Josef-Strasse 18, A-8700, Leoben, Austria

E-mail adress: joerg.thuswaldner@unileoben.ac.at

Department of mathematics and informatic, Larbi Ben M'hidi University, Oum El Bouaghi 04000, Algeria

E-mail address: toufikzaimi@yahoo.com