Comments on the height reducing property

Shigeki AKIYAMA and Toufik ZAIMI

ABSTRACT. *A complex number α is said to satisfy the height reducing property if there is a finite subset, say F, of the ring $\mathbb{Z}$ of the rational integers such that $\mathbb{Z}[\alpha] = F[\alpha]$. This property has been considered by several authors, especially in contexts related to self affine tilings, and expansions of real numbers in non-integer bases. We prove, in this paper, that a number satisfying the height reducing property, is an algebraic number whose conjugates, over the field of the rationals, are all of modulus one, or all of modulus greater than one. Expecting the converse of the last statement, we also show some theoretical and experimental results, which support this conjecture.*

1. Introduction

For a subset F of the complex field $\mathbb{C}$, and for $\alpha \in \mathbb{C}$, we denote by $F[\alpha]$ the set of polynomials with coefficients in F, evaluated at α, i. e.,

$$F[\alpha] = \{\sum_{j=0}^{n} \varepsilon_j \alpha^j \mid (\varepsilon_0, ..., \varepsilon_n) \in F^{n+1}, \ n \in \mathbb{N}\},$$

where $\mathbb{N}$ is the set of non-negative rational integers. In particular, when F is the ring $\mathbb{Z}$ of the rational integers, the set $F[\alpha]$ is the $\mathbb{Z}-$module generated by the integral powers of α. It is well known that there is $N \in \mathbb{N}$ such that $\mathbb{Z}[\alpha] = \{\varepsilon_0 + \cdots + \varepsilon_N \alpha^N \mid (\varepsilon_0, ..., \varepsilon_N) \in \mathbb{Z}^{N+1}\}$ if, and only if, α is an algebraic integer; moreover, the smallest possible value for N, in this case, is $\deg(\alpha) - 1$, where $\deg(\alpha)$ is the degree of α [12].

Mathematics Subject Classification (2010): 11R04, 12D10, 11R06, 11A63
Key words and phrases: roots of polynomials, height of polynomials, special algebraic numbers, quantitative Kronecker's approximation theorem.

Following [1], we say that α satisfies the *height reducing property*, in short HRP, if there is a finite subset, say again F, of $\mathbb{Z}$ such that $F[\alpha] = \mathbb{Z}[\alpha]$. 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. These two problems, unified into a problem of *shift radix system,* are extensively studied. Readers may consult [2, 3] and the references therein.

A result of Lagarias and Wang, cited in [1, 7], implies that an expanding algebraic integer α, that is an algebraic integer whose conjugates are of modulus greater than one, satisfies HRP with $F = \{0, \pm 1, ..., \pm(|Norm(\alpha)| - 1)\}$. Recently, Akiyama, Drungilas and Jankauskas obtained a direct proof of this last mentioned result, but with a greater finite set F [1]. It is worth noting that Proposition 3.1 of [8] yields to the same conclusion. Also, Lemma 1 of [1] asserts that an algebraic integer, with modulus greater than 1, satisfying HRP, is an expanding algebraic integer. Next we continue the description of the numbers which satisfy this property.

Theorem 1 *Let $\alpha \in \mathbb{C}$. Then, the following propositions are true.*

(i) If α satisfies the height reducing property , then α is an algebraic number whose conjugates are all of modulus 1, or all of modulus greater than 1.

(ii) If α is a root of unity, or an algebraic number whose conjugates are of modulus greater than 1, then α satisfies the height reducing property.

It is clear, by Kronecker's theorem (see for instance [12]), that an algebraic integer whose conjugates belong to the unit circle is a root of unity. To obtain a characterization of the numbers which satisfy HRP, it remains to consider the case where all conjugates of the algebraic number α belong to the unit circle, and are not roots of unity. In this last situation the minimal polynomial M_α of α is reciprocal, i. e., $M_\alpha(x) = x^{\deg(M_\alpha)} M_\alpha(1/x)$, $\deg(M_\alpha)$ (which is equal to $\deg(\alpha)$) is even, and the greatest number, say $m(\alpha)$, of conjugates of α which are multiplicatively independent (see the definition in Lemma 1 below) satisfies the relation $1 \leq m(\alpha) \leq \deg(\alpha)/2$, since the roots of M_α are pairwise complex conjugates and $\arg(\alpha)/\pi \notin \mathbb{Q}$ (i.e., α is not a root of unity), where $\mathbb{Q}$ is the field of the rational numbers.

Theorem 2 *Let α be an algebraic number whose all conjugates lie on the unit circle. If $m(\alpha) \geq \deg(\alpha)/2 - 1$, or $m(\alpha) = 1$, then α satisfies the height reducing property.*

Remark 1 *It follows immediately from Theorem 2 that α satisfies HRP when $\deg(\alpha) \leq 6$. We expect that this property holds for any algebraic α whose conjugates lie on the unit circle. However we find, in the Appendix, two examples of degree 12 that none of our methods apply.*

Remark 2 *There is an algorithm to determine $m(\alpha)$. In fact if $\alpha_1, \dots \alpha_m$ are multiplicatively dependent, then Lemma 4.1 in Waldschmidt [14] gives an explicit upper bound B so that the equation $\prod_{i=1}^{m} \alpha_i^{k_i} = 1$ has a non-trivial solution $(k_1, ..., k_m) \in (\mathbb{Z} \cap [-B, B])^m$. However the bound B is too large to examine. We employ Lemma 3.7 of de Weger [6] to reduce this bound by LLL algorithm. Details and numerical results will be shown in the Appendix.*

In these pages when we speak about conjugates, norm, minimal polynomial and degree of an algebraic number we mean over the field $\mathbb{Q}$. A unit is an algebraic integer whose norm is ± 1.The proofs of the theorems above appear in the last section. Lemmas 5 and 6 of [7], and some parts of the proofs of Lemmas 1 and 6 of [1] are used to show Theorem 1; these results, together with some auxiliary ones, we need to prove Theorem 2, are exhibited in the next section.

2. Some lemmas

The following result is the main tool of the first part of the proof of Theorem 2.

Lemma 1 *Let $\alpha_1, \dots, \alpha_m$ be conjugates, with modulus one, of an algebraic number α. Assume that $\alpha_1, \dots, \alpha_m$ are multiplicatively independent, i.e., each equation of the form $\prod_{j=1}^{m} \alpha_j^{k_j} = 1$ where $(k_1, \dots, k_m) \in \mathbb{Z}^m$, implies $(k_1, \dots, k_m) = (0, \dots, 0)$. Then for every $\varepsilon > 0$, there is a positive rational* *integer* $K = K(\alpha, m, \varepsilon)$ *such that for each* $(\beta_1, \ldots, \beta_m) \in \mathbb{C}^m$, *with* $\prod_{j=1}^{m} \beta_j \neq 0$, *there is a non-negative rational integer* $l \leq K$ *satisfying* $|\arg(\beta_j \alpha_j^l)| \leq \varepsilon$, $\forall$ $j \in \{1, \ldots, m\}$.

Proof. The existence of the constant K, satisfying the above mentioned condition, is a corollary of a quantitative version of Kronecker's approximation theorem due to Mahler [10] (c.f. Vorselen [13]). The necessary assumption of the lower bound follows from Baker's theory of linear forms in logarithms (see [4, 5]). $\square$

To simplify the computation in the proof of Theorem 2, let us show the following lemma.

Lemma 2 *Let* z *and* w *be complex numbers satisfying* $z \neq 0$, $|\arg(z)| \leq 2\pi/5$ *and* $|w| \leq 1$. *Then for all real numbers* $r \in (0, 4|z|/145)$, *we have*

$$|z + r(w-5)| < |z|.$$

Proof. Set $z := \delta \exp(i\theta)$, $w := \rho \exp(i\phi)$ and $(z + r(w-5)) \exp(-i\theta) := a + ib$, where $i^2 = -1$, $\{\delta,\ \theta,\ \rho,\ \phi,\ a,\ b\} \subset \mathbb{R}$ and $\mathbb{R}$ is the real field. Then $a = \delta + r\rho\cos(\phi - \theta) - 5r\cos(\theta)$, $b = r\rho\sin(\phi-\theta) + 5r\sin(\theta)$, $0 < \delta - 6r \leq a \leq \delta - (5\cos(2\pi/5) - 1)r \leq \delta - r/2$, $\quad |b| \leq 6r$ and so

$$|z + r(w-5)| \leq \sqrt{(\delta - r/2)^2 + 36r^2} < \delta. \ \square$$

Lemma 3 *Let* α *be an algebraic number of degree* d. *Then* $\mathbb{Z}[\alpha] \cap \mathbb{Z}[1/\alpha]$ *is an order, i.e., a subring of the ring of the integers of* $\mathbb{Q}(\alpha)$, *sharing the identity as well as a free* $\mathbb{Z}$*-submodule of rank* d.

Proof. Put $\mathcal{O} = \mathbb{Z}[\alpha] \cap \mathbb{Z}[1/\alpha]$. If α is an algebraic integer, then we have $\mathbb{Z}[\alpha] \subset \mathbb{Z}[1/\alpha]$ and the statement is trivial. Assume that α is not an algebraic integer, and take an ideal $\mathfrak{p}$ which divides the denominator of the fractional ideal (α). Then the denominator of the principal ideal (x) for $x \in \mathcal{O}$ is not divisible by $\mathfrak{p}$. This shows that every element of $\mathcal{O}$ is an algebraic integer and $\mathcal{O}$ is a $\mathbb{Z}$-module of rank not greater than d. Denote by $\sum_{n=0}^{d} c_n x^n$ the minimal polynomial of α. Then from the relation

$$c_d \alpha = -\sum_{n=0}^{d-1} c_n \alpha^{n-d+1} \in \mathbb{Z}[1/\alpha],$$

and the fact that $c_d \alpha$ is an algebraic integer, we see that

$$\mathbb{Z}[c_d \alpha] \subset \mathbb{Z}[\alpha] \cap \mathbb{Z}[1/\alpha].$$

This shows that the rank of $\mathcal{O}$ is not less than d. $\square$

Lemma 4 *Let α be an algebraic number of degree $2d$ whose all conjugates are of modulus one. Let α_j $(j = 1, \ldots, d)$ be the conjugates of α lying in the upper half plane. If $m(\alpha) = d - 1$, then there is a vector $(a_1, \ldots, a_d) \in \{-1, 1\}^d$ and a root of unity ζ such that $\prod_{j=1}^{d} \alpha_j^{a_j} = \zeta$.*

Proof. If $m(\alpha) = 0$ then $\alpha = \pm i$ and α is a root of unity. Suppose $m(\alpha) \geq 1$. Then $d \geq 2$, and by $m(\alpha) = d - 1$, there is $(b_1, \ldots, b_d) \in \mathbb{Z}^d \setminus \{(0, \ldots, 0)\}$ such that $\prod_{j=1}^{d} \alpha_j^{b_j} = 1$. It suffices to show that there is $b \in \mathbb{N}^* := \mathbb{N} \setminus \{0\}$ satisfying $|b_j| = b$ for all j. If not, then we may assume that $|b_1| > |b_2| = \min_{j=1}^{d} |b_j|$. Applying the embedding σ of $\mathbb{Q}(\alpha_2)$ into $\mathbb{C}$, which sends α_2 to α_1, we obtain $\prod_{j=1}^{d} \alpha_j^{c_j} = 1$, with $c_1 = b_2$, and so

$$\prod_{i=2}^{d} \alpha_i^{b_1 c_i - b_2 b_i} = 1.$$

Since $|c_j| = |b_1|$ for some j, this last multiplicative relation is non trivial, and yields, together with the equation $\prod_{j=1}^{d} \alpha_j^{b_j} = 1$, the inequality $m(\alpha) < d-1$. $\square$

Lemma 5 *Let α be an algebraic number of degree $2d \geq 6$ whose all conjugates are of modulus one. Let α_j $(j = 1, \ldots, d)$ be the conjugates of α lying in the upper half plane. If $m(\alpha) = d - 1$ then there is a positive integer $K = K(\alpha)$ such that for every $(\beta_1, \ldots, \beta_d) \in \mathbb{C}^d$, with $\prod_{j=1}^{d} \beta_j \neq 0$, there is a non-negative integer $\ell \leq K$ such that $|\arg(\beta_j \alpha_j^\ell)| \leq 2\pi/5$ for $j = 1, \ldots, d$.*

Proof. Lemma 4 asserts that there is a positive rational integer b such that

$$\alpha_1^b = \alpha_2^{\pm b} \ldots \alpha_d^{\pm b}$$

for a fixed choice of $\pm$'s, and $\alpha_2^b, \ldots, \alpha_d^b$ are multiplicatively independent. So substituting $\alpha_j^{\pm b}$ to α_j for each j, we may assume that

$$\alpha_1 = \alpha_2 \ldots \alpha_d.$$

This implies

$$\beta_1 \alpha_1^\ell = \beta_1 \Big(\prod_{j=2}^{d} \beta_j \alpha_j^\ell\Big) / \Big(\prod_{j=2}^{d} \beta_j\Big) \tag{1}$$

for any ℓ. Fix a small $0 < \varepsilon < \pi/15$ and apply Kronecker's approximation theorem as in Lemma 1 to the following three sets of $(d-1)$ inequalities:

- $\left|\arg(\beta_2 \alpha_2^\ell) - \frac{\pi}{3}\right| < \varepsilon,\ \left|\arg(\beta_3 \alpha_3^\ell) - \frac{\pi}{3}\right| < \varepsilon,\ \left|\arg(\beta_j \alpha_j^\ell)\right| < \varepsilon\ (j \geq 4)$;
- $\left|\arg(\beta_2 \alpha_2^\ell) + \frac{\pi}{3}\right| < \varepsilon,\ \left|\arg(\beta_3 \alpha_3^\ell) - \frac{\pi}{3}\right| < \varepsilon,\ \left|\arg(\beta_j \alpha_j^\ell)\right| < \varepsilon\ (j \geq 4)$;
- $\left|\arg(\beta_2 \alpha_2^\ell) + \frac{\pi}{3}\right| < \varepsilon,\ \left|\arg(\beta_3 \alpha_3^\ell) + \frac{\pi}{3}\right| < \varepsilon,\ \left|\arg(\beta_j \alpha_j^\ell)\right| < \varepsilon\ (j \geq 4)$.

Then we can find a common $K = K(\alpha)$ such that these three systems are solvable. Denote the three respective solutions by ℓ_j $(j = 1, 2, 3)$, with $\ell_j \leq K$. If $\left|\arg(\beta_1 \alpha_1^{\ell_2})\right| < 2\pi/5$ then ℓ_2 is the required solution. Otherwise, from (1), one of the inequalities $\left|\arg(\beta_1 \alpha_1^{\ell_1})\right| < 2\pi/5$ and $\left|\arg(\beta_1 \alpha_1^{\ell_3})\right| < 2\pi/5$, is true, for a sufficiently small ε. Thus, there is $l \in \{l_1, l_2, l_3\}$ such that $|\arg(\beta_j \alpha_j^\ell)| \leq 2\pi/5$, $\forall\ j = 1, \ldots, d$. $\square$

Lemma 6 *Let α_1, α_2 be two conjugates of an algebraic number α. Assume that α is not a unit and there is $(a, b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ with $\alpha_1^a \alpha_2^b = 1$. Then $|a| = |b|$.*

Proof. By the prime ideal decomposition of the fractional ideals (α_1) and (α_2) in the minimum decomposition field of α, we have

$$(\prod_{j=1}^{s} \mathfrak{p}_j^{ae_j})(\prod_{j=1}^{s} \mathfrak{p}_j^{be'_j}) = (1),$$

and so $ae_j + be'_j = 0$ for each j. If $|a| < |b|$, then $|e_j| > |e'_j|$ for all j, and we claim that this is impossible. Indeed, consider an index l with $|e_l| = \max_{1 \leq j \leq s} |e_j|$. As there is an embedding of $\mathbb{Q}(\alpha_1)$ into $\mathbb{C}$, which sends (α_1) to (α_2), there exists an index k such that $e'_k = e_l$, and the inequality $|e_k| > |e'_k|$ leads immediately to a contradiction. $\square$

Following [7], we say that a non-zero polynomial $P = P(x) = c_0 + \cdots + c_{\deg(P)} x^{\deg(P)} \in \mathbb{C}[x]$ has a dominant term (resp., has a dominant constant term) if there is $k \in \{0, ..., \deg(P)\}$ such that $|c_k| \geq \sum\limits_{j \neq k} |c_j|$ (resp., such that $|c_0| \geq \sum\limits_{1 \leq j} |c_j|$). In connection with a property studied by Frougny and Steiner [8], about minimal weight expansions, Dubickas obtained recently [7], some characterizations of complex numbers which are roots of integer polynomials (i. e., polynomials with rational integer coefficients) having a dominant term.

Lemma A ([7]) *Let $\alpha \in \mathbb{C}$. Then, the following assertions are true.*

(i) The number α is a root of an integer polynomial with dominant term if, and only if, α is a root of unity, or α is an algebraic number without conjugates of modulus 1.

(ii) The number α is a root of an integer polynomial with dominant constant term if, and only if, α is a root of unity, or α is an algebraic number all of whose conjugates are of modulus greater than 1.

The result below, we need to show Theorem 1, gives two simple generalizations of Lemma A. The first one is an integral version of Lemma A (i). To state the second one, let us introduce the following "definition-precision": *We say that the non-zero polynomial P, defined above, has a $k-th$ dominant* *term, (resp., has a $k-$th strictly dominant term), where* $k \in \{0, ..., \deg(P)\}$, *if* $|c_k| \geq \sum_{j \neq k} |c_j|$ *(resp., if* $|c_k| > \sum_{j \neq k} |c_j|$*). The polynomial P has a strictly dominant term, when it has some $k-$th strictly dominant term.*

Lemma 7 *Let $\alpha \in \mathbb{C}$. Then, the following propositions are true.*

(i) The number α is a root of an (resp., of a monic) integer polynomial with k-th dominant term if, and only if, α is a root of unity, or α is an algebraic number (resp., algebraic integer) having at most k conjugates inside the unit disk and no conjugates on the unit circle.

(ii) The number α is a root of an (resp., of a monic) integer polynomial with k-th strictly dominant term if, and only if, α is an algebraic number (resp., algebraic integer) having at most k conjugates inside the unit disk and no conjugates on the unit circle.

Proof. A direct application of Rouché's theorem gives that a polynomial $P \in \mathbb{C}[x]$, with $k-$th strictly dominant term, has exactly k roots with modulus less than 1. The same argument applied, in this case, to the polynomial $x^{\deg(P)}P(1/x)$ shows that P has $(\deg(P) - k)$ roots outside the closed unit disk (see also [11, p. 225]); thus P has no roots on the unit circle. Now, suppose that α is a root of a non-zero (resp., of a monic) integer polynomial, say again $P(x) = c_0 + c_1 x + \cdots + c_{\deg(P)} x^{\deg(P)}$, such that

$$|c_k| \geq \sum_{j \neq k} |c_j| \, ,$$

for some $k \in \{0, ..., \deg(P)\}$. Then, α is an algebraic number (resp., an algebraic integer), and by the above we have that the direct implication in Lemma 7 (ii) is true, since the conjugates of α are among the roots of P. To show the direct implication of Lemma 7 (i), notice first, by Lemma 5 of [**7**], that α is root of unity, when it has a conjugate lying on the unit circle. Assume that α is not a root of unity (so α has no conjugates on the unit circle) and consider the polynomial

$$P_n(x) = P(x) + (\varepsilon/n)x^k,$$

where $n \in \mathbb{N}^*$ and $\varepsilon = \operatorname{sgn}(c_k)$. Also, by the above the polynomial P_n has exactly k roots inside the unit disk. Let $\beta_{1,n}, ..., \beta_{\deg(P),n}$ be the roots of P_n, and let β be a root of P with modulus less than 1. Then, $|P_n(\beta)| = \left|\beta^k/n\right| < 1/n$ and so $\lim_{n\to\infty} P_n(\beta) = 0$. It follows by the equation $\lim_{n\to\infty} \prod_{1\leq j\leq \deg(P)} (\beta - \beta_{j,n}) = 0$, that there is a subsequence of some sequence $(\beta_{j_0,n})_{n\geq 1}$, where j_0 is fixed in $\{1, ..., \deg(P)\}$, which converges to β. Hence, P has at most k distinct roots with modulus less than 1, and so α has at most k conjugates inside the unit disk, since its minimal polynomial is separable. To prove the other implications in Lemma 7, consider an algebraic number (resp., an algebraic integer), say again α, having $l \geq 0$ conjugates with modulus less than 1 and no conjugates on the unit circle. Then, from the proof of Lemma 6 of **[7]**, we see that there is $N \in \mathbb{N}^*$ such that the polynomial $Q(x) := \prod_{1\leq j\leq d} (x - \alpha_j^N)$, where $\alpha_1, ..., \alpha_d$ are the conjugates of α, has an $l-$th strictly dominant term. Moreover, since $Q(x) \in \mathbb{Q}[x]$, there is $v \in \mathbb{N}^*$ such that $vQ(x) \in \mathbb{Z}[x]$, and so α is a root of the integer polynomial $R(x) = vQ(x^N)$ (resp., since $Q(x) \in \mathbb{Z}[x]$, α is a root of the monic integer polynomial $R(x) = Q(x^N)$) with an $l-$th strictly dominant term. Now, let $k \in \mathbb{N} \cap [l, \infty[$. Then, α has at most k conjugates inside the unit disk, and is a root of the polynomial

$$\sum_{j=0}^{k-l-1} c'_j x^j + x^{k-l} R(x),$$

where $c'_j = 0$ for all $j \in \{0, ..., k-l-1\}$, with $k-$th strictly dominant term; this ends the proof of Lemma 7 (ii). Notice finally, if α is an $N-$th root of unity, then α is a root of the monic integer polynomial $x^{2N+k} + (B-1)x^{N+k} - Bx^k$, where $B \in \mathbb{N}^*$ and $k \in \mathbb{N}$, with $k-$th dominant term, and this completes the proof of Lemma 7 (i). $\square$

It is worth noting that Lemma A (ii) is a corollary of Lemma 7 (i) (with $k = 0$) and Lemma 7 (i) implies Lemma A (i), too. It follows also from Lemma 7 (ii) that a complex number is a root of some (resp., some monic) integer polynomial with strictly dominant term if, and only if, it is an algebraic number (resp., algebraic integer) without conjugates on the unit circle.

3. The proofs

Proof of Theorem 1. (i) With the notation above, assume that α satisfies HRP with some finite set F. Let $m = \max\{|\varepsilon|, \varepsilon \in F\}$ and choose $N \in \mathbb{N} \cap (m, \infty)$. By $N \in F[\alpha] = \mathbb{Z}[\alpha]$ it follows immediately that α is an algebraic number. Let β be a conjugate of α. Then $|\beta| \geq 1$, since otherwise any element of the set $\mathbb{N} \cap (\frac{m}{1-|\beta|}, \infty)$ does not belong to $F[\alpha]$. Now, suppose that $|\beta| = 1$, we have to show that the conjugates of α lie on the unit circle. If $\deg(\alpha) = 1$, then $\alpha = \pm 1$ and the result is true. Assume that $\deg(\alpha) \geq 2$. Then, the complex conjugate $\overline{\beta}$ of β is also a conjugate of α. Let γ be a conjugate of α, and let σ be an embedding of $\mathbb{Q}(\beta)$ into $\mathbb{C}$ such that $\sigma(\beta) = \gamma$. Then, $1/\gamma = 1/\sigma(\beta) = \sigma(1/\beta) = \sigma(\overline{\beta})$ and so $1/\gamma$ is a conjugate of α. Thus $|\gamma| = 1$, since otherwise one of the numbers γ and $1/\gamma$ has modulus less than 1, and by the above this leads to a contradiction.

(ii) It is clear when α is an $N-$th root of unity, where $N \in \mathbb{N}^*$ that any sum of the form $\sum\limits_{j=0}^{s} a_j \alpha^j$, where $a_j \in \mathbb{Z}$ and $s \in \mathbb{N}$, may be written

$$\sum_{j=0}^{s} \varepsilon_j \left(\sum_{k=1}^{|a_j|} \alpha^{kN}\right) \alpha^{\left(j + \sum\limits_{l=0}^{j-1} |a_l| N\right)},$$

where $\varepsilon_j = \operatorname{sgn}(a_j)$, and so $\{0, \pm 1\}[\alpha] = \mathbb{Z}[\alpha]$.

Now suppose that α is an algebraic number whose conjugates are of modulus greater than 1. Then Lemma 7 (ii) shows that α is a root of some polynomial $C(x) = c_0 + c_1 x + \cdots + c_d x^d \in \mathbb{Z}[x]$, with $c_d \neq 0$ and

$$|c_0| > \sum_{j=1}^{d} |c_j|.$$

Let $R \in \mathbb{Z}[x]$. To prove the relation $R(\alpha) \in F[\alpha]$, where

$$F := \{0, \pm 1, ..., \pm(|c_0| - 1)\},$$

suppose first that $\deg(R) \in \{0, ..., d-1\}$. Then, $R(x) = A_0 + \cdots + A_{d-1} x^{d-1}$, for some $(A_0, ..., A_{d-1}) \in \mathbb{Z}^d$, and similarly as in the proof of Theorem 4 of [1], it suffices to show, when $A_0 \notin F$, that

$$R(\alpha) = \varepsilon + \alpha(a_0 + \cdots + a_{d-1}\alpha^{d-1}), \qquad (2)$$

where $\varepsilon \in F$, $(a_0, ..., a_{d-1}) \in \mathbb{Z}^d$ and $\sum_{j=0}^{d-1} |a_j| < \sum_{j=0}^{d-1} |A_j|$. Since $|A_0| \geq |c_0|$, we see that $|A_0| = q|c_0| + \varepsilon$, for some $q \in \mathbb{N}^*$ and $\varepsilon \in \mathbb{N} \cap F$. It follows by the equation $c_0 = -c_1\alpha - \cdots - c_d\alpha^d$, that

$$A_0 \mathrm{sgn}(A_0) = qc_0\mathrm{sgn}(c_0) + \varepsilon = \varepsilon - (qc_1\alpha + \cdots + qc_d\alpha^d)\mathrm{sgn}(c_0),$$

and so

$$A_0 + \cdots + A_{d-1}\alpha^{d-1} = \mathrm{sgn}(A_0)\varepsilon + \alpha(a_0 + \cdots + a_{d-1}\alpha^{d-1}),$$

where $a_{d-1} = -\mathrm{sgn}(c_0)\mathrm{sgn}(A_0)qc_d$ and $a_j = A_{j+1} - \mathrm{sgn}(c_0)\mathrm{sgn}(A_0)qc_{j+1}$ for all $j \in \{0, ..., d-2\}$. Moreover, we have $\mathrm{sgn}(A_0)\varepsilon \in F = -F$, and

$$\sum_{j=0}^{d-1} |a_j| \leq q(\sum_{j=1}^{d} |c_j|) + \sum_{j=1}^{d-1} |A_j| < q|c_0| + \sum_{j=1}^{d-1} |A_j| \leq \sum_{j=0}^{d-1} |A_j|.$$

This also ends the proof of Theorem 1 (ii), when α is an algebraic integer, because by Lemma 7 (ii) we may choose the polynomial C so that $c_d = 1$, and the Euclidean division of any element $Q \in \mathbb{Z}[x]$ by C gives that $Q(\alpha) = A_0 + \cdots + A_{d-1}\alpha^{d-1}$ for some $(A_0, ..., A_{d-1}) \in \mathbb{Z}^d$.

Now, we use a simple induction on $\deg(R)$ to complete the proof of Theorem 1. By the above, we have $R(\alpha) \in F[\alpha]$, when $\deg(R) \leq d-1$. Let

$$R(x) = A_0 + A_1x + \cdots + A_Dx^D \in \mathbb{Z}[x],$$

where $D \geq d$, and suppose that $P(\alpha) \in F[\alpha]$ for all $P \in \mathbb{Z}[x]$, with $\deg(P) < D$. Since $\deg(A_0) = 0 \leq d-1$, the relation (2) implies that

$$A_0 = \varepsilon + \alpha(a_0 + \cdots + a_{d-1}\alpha^{d-1}),$$

for some $\varepsilon \in F$ and $a_j \in \mathbb{Z}$. Hence,

$$R(\alpha) = \varepsilon + \alpha((a_0 + A_1) + \cdots + (a_{D-1} + A_D)\alpha^{D-1}),$$

where $a_d = ... = a_{D-1} = 0$, and the induction hypothesis, applied to the polynomial $(a_0 + A_1) + \cdots + (a_{D-1} + A_D)x^{D-1} \in \mathbb{Z}[x]$, leads to the desired result. $\square$

Proof of Theorem 2. Let α be an algebraic number, whose conjugates $\alpha^{(1)}, ..., \alpha^{(\deg(\alpha))}$ lie on the unit circle. Since Theorem 2 is true when α is a root of unity, suppose that α is not an algebraic integer and the leading coefficient c of its minimal polynomial M_α satisfies $c \geq 2$.

Case $m(\alpha) = \deg(\alpha)/2$. Set $m := m(\alpha)$ and let $\alpha^{(1)}, \ldots, \alpha^{(m)}$ be m conjugates of α which are multiplicatively independent. Without loss of generality, we may assume that $\mathrm{Im}(\alpha^{(j)}) > 0$ for all $j \in \{1, ..., m\}$. Then, the map Φ defined, from the field $\mathbb{Q}(\alpha)$ into the ring $\mathbb{C}^m$, by the relation

$$\Phi(\beta) = (\beta^{(1)}, \ldots, \beta^{(m)}),$$

where $\beta^{(j)}$ is the image of β by the embedding of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$, which sends α to $\alpha^{(j)}$, $\forall j \in \{1, ..., m\}$, is also an embedding. It suffices to show that there exist two positive real numbers $B = B(\alpha)$ and $R = R(\alpha)$, such that for any $\beta_0 \in \mathbb{Z}[\alpha]$ there are $N = N(\alpha, \beta_0)$ elements $s_1, ..., s_N$ of set $[0, B] \cap \mathbb{N}$, and a number $\gamma \in \mathcal{O} := \mathbb{Z}[\alpha] \cap \mathbb{Z}[1/\alpha]$ satisfying

$$\beta_0 = (\sum_{j=1}^{N} s_j \alpha^{j-1}) + \gamma \alpha^N \text{ and } \|\Phi(\gamma)\| \leq R, \tag{3}$$

where $\|.\|$ is the sup norm on the vector space $\mathbb{C}^m$. Indeed, define the integer

$$h := \max\{h(\gamma) \mid \gamma \in E\},$$

where $h(\gamma)$ is the greatest modulus of the coefficients of a fixed representation of γ in $\mathbb{Z}[\alpha]$, and the set

$$E := \{\gamma \in \mathcal{O} \mid \|\Phi(\gamma)\| \leq R\},$$

which is finite by Lemma 3. Then, by the above, α satisfies HRP with a finite subset of $\mathbb{Z} \cap [-\max\{B, h\}, \max\{B, h\}]$.

If

$$\beta = a_0 + \cdots + a_n \alpha^n \tag{4}$$

for some $n \in \mathbb{N}$ and $\{a_0, ..., a_n\} \subset \mathbb{Z}$, then the Euclidean division of a_0 by c gives that there is $d \in \{0, 1, ..., c-1\}$ such that $\beta \equiv d \bmod \alpha$, i. e., $(\beta - d)/\alpha \in \mathbb{Z}[\alpha]$. Moreover, since $M_\alpha(0) = c$, the number d is unique. Hence, the map

$$T : \beta \mapsto (\beta - d)/\alpha,$$

is well defined from $\mathbb{Z}[\alpha]$ into itself. Now, fix $\beta_0 \in \mathbb{Z}[\alpha]$, and set

$$\beta_k := \alpha\beta_{k+1} + d_{k+1},$$

where $k \in \mathbb{N}$, $\beta_{k+1} = T(\beta_k)$ and $d_{k+1} \in \{0, 1, ..., c-1\}$. Then

$$\beta_{k+1} = \frac{\beta_0}{\alpha^{k+1}} - \frac{d_1}{\alpha^{k+1}} - \cdots - \frac{d_{k+1}}{\alpha^1}.$$

With the notation of Lemma 1, set $R := (43K(\alpha, m, 2\pi/5)+10)c$. By Lemma 1, there is $l \in \mathbb{N} \cap [0, K]$ such that $\left|\arg(\beta_0^{(j)}/(\alpha^{(j)})^l)\right| \leq 2\pi/5$ for $j = 1, \dots, m$. Select d^*_{l+1} such that $5Kc \leq d^*_{l+1} < (5K+1)c$, and $\beta_l \equiv d^*_{l+1} \bmod \alpha$. Let $\beta^*_{l+1} := (\beta_l - d^*_{l+1})/\alpha$. Putting $r := d^*_{l+1}/5$ and $z := \beta_0^{(j)}/(\alpha^{(j)})^l$ in Lemma 2, we obtain

$$\left|\beta^{*(j)}_{l+1}\right| = \left|\frac{\beta_0^{(j)}}{(\alpha^{(j)})^l} - \sum_{v=1}^{l} \frac{d_v}{(\alpha^{(j)})^{l-v+1}} - d^*_{l+1}\right| < |\beta_0^{(j)}| \leq \|\Phi(\beta_0)\|,$$

when $(37K+8)c \leq |\beta_0^{(j)}|$. On the other hand, if $|\beta_0^{(j)}| < (37K+8)c$, then

$$\left|\beta^{*(j)}_{l+1}\right| \leq (43K+9)c < R.$$

This implies

$$\|\Phi(\beta^*_{l+1})\| < \max\{R, \|\Phi(\beta_0)\|\}$$

and

$$\beta_0 = (\sum_{j=1}^{l} d_j \alpha^{j-1}) + d^*_{l+1}\alpha^l + \beta^*_{l+1}\alpha^{l+1}.$$

So we have

$$\beta^*_{l+1} \in \beta_0/\alpha^{l+1} + \mathbb{Z}[1/\alpha] \subset \alpha^u \mathbb{Z}[1/\alpha]$$

with $u = \max\{0, n-l-1\}$, where n is defined by the expression (4). Iterating this procedure, we obtain a sequence $(\beta^*_{l(j)+1})_{j=1,2,\dots}$ with $l = l(1)$ and $\beta^*_{l(j)+1} \in \mathbb{Z}[1/\alpha] \cap \mathbb{Z}[\alpha]$ for sufficiently large j. From Lemma 3, $\Phi(\mathcal{O})$ has no accumulation points in $\mathbb{C}^m$, and we see that β_0 can be written

$$\beta_0 = (\sum_{j=1}^{N} s_j \alpha^{j-1}) + \gamma\alpha^N,$$

where $N \in \mathbb{N}^*$, $s_j \in [0, B] \cap \mathbb{N}$, $B := (5K+1)c$ and $\gamma \in E$. Hence, (3) is true and this completes the proof of the first implication in Theorem 2.

It follows immediately, from the case above, that α satisfies HRP, when $\deg(\alpha) = 2$, as $m(\alpha) = \deg(\alpha)/2$ (in this case the constant K is much smaller and one can make explicit the height given by the above proof).

Case $m(\alpha) = \deg(\alpha)/2 - 1$. The proof is almost the same but we use Lemma 5 instead of Lemma 1.

We are left to show the case $m(\alpha) = 1$. From Lemma 6, any two distinct conjugates α_l and α_j, of α, in the upper half plane, satisfy $\alpha_l^b \alpha_j^b = 1$ or $\alpha_l^b \overline{\alpha_j}^b = 1$ for some positive rational integer b. In both cases, α^b has less number of conjugates than α. We can iterate this discussion until we find an integer, say again b, such that the only other conjugate of α^b is $\overline{\alpha}^b$. Then α^b is quadratic and so by the case $m(\alpha^b) = \deg(\alpha^b)/2$, there is a finite subset F of $\mathbb{Z}$ such that $\mathbb{Z}[\alpha^b] = F[\alpha^b]$; thus $\mathbb{Z}[\alpha] = F \cup \{0\}\,[\alpha]$, since any sum of the form $\sum_{j=0}^{s} c_j \alpha^j$, where $c_j \in \mathbb{Z}$, may be written

$$\sum_{j=0}^{s} c_{jb} \alpha^{jb} + \alpha \sum_{j=0}^{s} c_{1+jb} \alpha^{jb} + \cdots + \alpha^{b-1} \sum_{j=0}^{s} c_{b-1+jb} \alpha^{jb},$$

with $c_j = 0$ when $j \geq s+1$. $\square$

Appendix.

Continuing Remark 2, we describe briefly a practical method to study multiplicative dependence of α_i's, by using Lemma 3.7 of [6]. Set $\theta_{m+1} = 2\pi$ and $\theta_j = \log \alpha_j$, $\forall\ j = 1, \ldots, m$, choose a large constant C (we may set $C := B^{m+2}$ where B is the maximum of constants appearing in Lemma 4.1 of [14]), and apply LLL algorithm for the lattice generated by the following $m+1$ vectors:

$$\begin{gathered}
(1, 0, \ldots, 0, 0, \lfloor C\theta_1 \rfloor) \\
(0, 1, 0, \ldots, 0, \lfloor C\theta_2 \rfloor) \\
\vdots \\
(0, 0, 0, \ldots, 1, \lfloor C\theta_m \rfloor) \\
(0, 0, \ldots, 0, \lfloor C\theta_{m+1} \rfloor)
\end{gathered}$$

where the notation $\lfloor . \rfloor$ designates the integer part function. Using Proposition 1.11 of [9], if the first vector v, found by LLL algorithm, satisfies

$$\|v\| > B2^{m/2}\sqrt{(m^2+5m+4)}, \tag{5}$$

then, $\alpha_1, \dots, \alpha_m$ are multiplicatively independent, since we can choose δ in Lemma 3.7 of de Weger [6] as large as possible. If the inequality (5) is not true, then the first vector $v = (k_1, \dots, k_{m+1})$ becomes small and it is highly possible that it gives a multiplicative dependence $\prod_{j=1}^{m} \alpha_j^{k_j} = 1$. We check the validity by rigorous symbolic computation.

Hereafter we present some numerical results on the multiplicative dependency of α. It suggests that $m(\alpha) < \deg(\alpha)/2$ rarely happens.

Let us fix an even degree d and a leading coefficient $c \geq 2$. We are interested in the number of primitive irreducible reciprocal polynomials of degree d, with leading coefficient c, whose all roots have modulus one. Further if there is a positive rational integer b such that $\deg(\alpha^b) < \deg(\alpha)$, then we can reduce the problem to lower degree. By Lemma 6, this occurs when and only when there are two distinct multiplicatively dependent conjugates of α which are not complex conjugates. We call this α *power-reducible*. For e.g., α is power-reducible if the minimal polynomial M_α of α has the form $g(x^m)$ for some rational integer $m \geq 2$ and some polynomial g. We wish to exclude power-reducible cases to obtain non trivial examples. If $\deg(\alpha) \geq 4$ and $m(\alpha) = 1$ then α is certainly power-reducible by Lemma 6. The first non trivial case holds when $d = 6$ and $m(\alpha) = 2$.

Put

$$T_n^*(y) = \begin{cases} 2T_n(y/2) & n = 1, 2, \dots \\ 1 & n = 0 \end{cases}$$

where $T_n(x)$ is the n-th Chebyshev polynomial of the 1-st kind. Fix a positive rational integer h. To produce polynomials whose all roots are of modulus one, we search integer polynomials

$$g(y) = \sum_{j=0}^{d/2} c_j T_{d/2-j}^*(y)$$

with $c_0 = c$ and $|c_j| \leq h$ for all j. The reciprocal polynomial

$$c_{d/2}x^{d/2} + \sum_{j=0}^{d/2-1} c_j(x^j + x^{d-j})$$

has d roots on the unit circle if and only if $g(y) = 0$ has $d/2$ real roots in $[-2, 2]$. We pick out such polynomials and check multiplicative dependence by the method in Remark 2. The result is shown in Table 1 for $c = 2$ and $c = 3$.

We explain Table 1 by examples. Hereafter the index of complex roots in the upper half plane is sorted by real parts. For $(d, c, h) = (6, 2, 50)$, among 1030301 polynomials there are 287 polynomials whose all roots are of modulus one. Within them there are 62 primitive irreducible ones. There remain 58 polynomials which do not have the form $g(x^m)$ with $m \geq 2$. Finally using the method of Remark 2, we find 8 polynomials with $m(\alpha) < \deg(\alpha)/2$. All of them satisfies $m(\alpha) = \deg(\alpha)/2-1$. For e.g., $2-2x+3x^2-2x^3+3x^4-2x^5+2x^6$ gives $\alpha_1\alpha_2^{-1}\alpha_3 = \sqrt{-1}$. For $(d, c, h) = (8, 2, 12)$, the above sieving process does not suffice, because there are $16 - 10 = 6$ power-reducible polynomials which does not have the form $g(x^m)$ with $m \geq 2$. For e.g, let α be a root of

$$2 + 4x + 2x^2 - 4x^3 - 7x^4 - 4x^5 + 2x^6 + 4x^7 + 2x^8.$$

Then α^8 is a root of $16+8x+x^2+8x^3+16x^4$. The remaining 10 polynomials satisfy $m(\alpha) = \deg(\alpha)/2 - 1$.

We did not find any example which is not covered by Theorem 2 for degree not greater than 10. Thus height reducing property is valid in this search range of c and h.

However in degrees 12 and 16, we find cases with

$$m(\alpha) = \deg(\alpha)/2 - 2 \text{ or } m(\alpha) = \deg(\alpha)/2 - 3.$$

Such cases form pairs $\pm\alpha$ and we shall present one representative in each pair.

Case $m(\alpha) = \deg(\alpha)/2 - 2$.

$$2 + 4x + 4x^2 + 2x^3 + x^4 + x^8 + 2x^9 + 4x^{10} + 4x^{11} + 2x^{12}$$

whose dependencies are generated by $\alpha_1 = \alpha_4\alpha_5^{-1}$ and $\alpha_2 = \alpha_3\alpha_6^{-1}$.

$$3 - 3x + x^2 + x^3 - 2x^4 + 2x^5 - x^6 + 2x^7 - 2x^8 + x^9 + x^{10} - 3x^{11} + 3x^{12}$$

gives $\alpha_1\alpha_6/\alpha_2 = \alpha_3\alpha_5/\alpha_4 = \frac{1+\sqrt{-3}}{2}$.

$$3 + 3x^2 - x^4 - 2x^5 - 3x^6 - 2x^7 - x^8 + 3x^{10} + 3x^{12}$$

gives $\alpha_1\alpha_3/\alpha_4 = \alpha_2\alpha_5/\alpha_6 = -1$. For degree 16,

$$2-2x-x^2+x^3+x^4-2x^6+x^7+x^8+x^9-2x^{10}+x^{12}+x^{13}-x^{14}-2x^{15}+2x^{16}$$

gives generating dependencies: $\alpha_1\alpha_3/(\alpha_4\alpha_8) = \alpha_2\alpha_5\alpha_7/\alpha_6 = -1$. Adapting the idea of Lemma 5 simultaneously to two multiplicative dependences, we can prove height reducing property for these 4 polynomials, by solving 9 systems of inequalities.

Case $m(\alpha) = \deg(\alpha)/2 - 3$.

$$2+4x+4x^2+3x^3+3x^4+2x^5+x^6+2x^7+3x^8+3x^9+4x^{10}+4x^{11}+2x^{12}$$

gives $\alpha_2\alpha_3\alpha_4 = \alpha_1\alpha_3\alpha_5 = 1$ and $\alpha_4 = \alpha_5\alpha_6$.

$$3-3x^2+2x^3+3x^4-x^6+3x^8+2x^9-3x^{10}+3x^{12}$$

gives $\alpha_3\alpha_4/\alpha_1 = \alpha_3\alpha_5/\alpha_2 = \alpha_2\alpha_6/\alpha_1 = 1$. We are not able to show height reducing property for these last two polynomials so far.

d	c	h	poly	circle	irred	prim	non x^m	dep	npr	-1	-2	-3
6	2	50	1030301	287	71	62	58	8	8	8	0	0
6	3	50	1030301	805	325	318	310	22	22	22	0	0
8	2	12	390625	1069	210	200	182	16	10	10	0	0
8	3	12	390625	3991	1565	1558	1502	42	40	40	0	0
10	2	6	371293	2931	518	516	512	8	8	8	0	0
10	3	6	372193	13244	5640	5638	5630	72	72	72	0	0
12	2	4	531441	6557	1386	1380	1310	32	24	20	2	2
12	3	4	531441	33202	15858	15852	15620	98	90	84	4	2
14	2	3	823543	12185	2510	2510	2506	12	12	12	0	0
14	3	3	823543	70951	37548	37548	37544	120	120	120	0	0
16	2	2	390625	15143	3940	3934	3828	34	32	30	2	0

Table 1: Multiplicative Dependency

- d: the degree of α
- c: the leading coefficient of the minimal polynomial M_α of α.
- h: the maximum modulus of the coefficients of M_α.

- *poly*: the number of polynomials.
- *circle*: the number of polynomials whose all roots have modulus one.
- *irred*: the number of irreducible polynomials in *circle*.
- *prim*: the number of primitive polynomials in *irred*.
- *non* x^m: the number of polynomials satisfying $M_\alpha(x) \neq g(x^m)$ in *prim*.
- *dep*: the number of multiplicatively dependent cases among *non* x^m.
- *npr*: the number of non-power reducible polynomials in *dep*.
- -1: the number of polynomials with $m(\alpha) = \deg(\alpha)/2 - 1$ in *npr*.
- -2: the number of polynomials with $m(\alpha) = \deg(\alpha)/2 - 2$ in *npr*.
- -3: the number of polynomials with $m(\alpha) = \deg(\alpha)/2 - 3$ in *npr*.

Acknowledgment. We would like to express our gratitude to Professor Attila Pethő for his advices concerning the practical computation of $m(\alpha)$ in Remark 2 and Appendix. We also thank the referees for their valuable suggestions about the presentation of this manuscript.

References

[1] S. Akiyama, P. Drungilas and J. Jankauskas, *Height reducing problem on algebraic integers*, Functiones et Approximatio, Commentarii Mathematici (to appear).

[2] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. M. Thuswaldner, *Generalized radix representations and dynamical systems I*, Acta Math. Hungar., 108 (2005) no. 3, 207-238.

[3] S. Akiyama and K. Scheicher, *From number systems to shift radix systems*, Nihonkai Math. J. 16 (2005) no. 2, 95-106.

[4] A. Baker, *The theory of linear forms in logarithms,* Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), Academic Press, London, 1977, pp. 1–27.

[5] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties,* J. Reine Angew. Math. **442** (1993), 19–62.

[6] B. M. M. de Weger, *Algorithms for Diophantine equations*, CMI Tracts **65**, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989. viii+212 pp.

[7] A. Dubickas, *Roots of polynomials with dominant term*, Intern. J. Number Theory, **7** (5) (2011), 1217-1228.

[8] C. Frougny and W. Steiner, *Minimal weight expansions in Pisot bases*, J. Math. Cryptology, **2** (4) (2008), 365-392.

[9] A. K. Lenstra, H.W. Lenstra, L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515-534.

[10] K. Mahler, *A remark on Kronecker's theorem,* Enseignement Math., **12** (2) (1966), 183–189.

[11] D. S. Mitrinović, *Analytic inequalities*, Springer-Verlag, 1970.

[12] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 3rd ed., Springer, Berlin, 2004.

[13] T. Vorselen, *On Kronecker's Theorem over the adéles,* Master thesis, Universiteit Leiden, 2010.

[14] M. Waldschmidt, *A lower bound for linear forms in logarithms*, Acta Arith. **37** (1980), 257–283.

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

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

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

E-mail address: toufikzaimi@yahoo.com