ON THE REMAK HEIGHT, THE MAHLER MEASURE AND CONJUGATE SETS OF ALGEBRAIC NUMBERS LYING ON TWO CIRCLES

A. DUBICKAS[1] AND C. J. SMYTH[2]

[1]*Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius 2006, Lithuania* (arturas.dubickas@maf.vu.lt)
[2]*Department of Mathematics and Statistics, Edinburgh University, James Clerk Maxwell Building, King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, UK* (chris@maths.ed.ac.uk)

Abstract   We define a new height function $\mathcal{R}(\alpha)$, the *Remak height* of an algebraic number α. We give sharp upper and lower bounds for $\mathcal{R}(\alpha)$ in terms of the classical Mahler measure $M(\alpha)$. Study of when one of these bounds is exact leads us to consideration of conjugate sets of algebraic numbers of norm ± 1 lying on two circles centred at 0. We give a complete characterization of such conjugate sets. They turn out to be of two types: one related to certain cubic algebraic numbers, and the other related to a non-integer generalization of Salem numbers which we call *extended* Salem numbers.

1. Introduction

Let α be an algebraic number, of degree $d \geqslant 2$, with minimal polynomial $a_0 z^d + \cdots + a_d \in \mathbb{Z}[z]$ over the rationals, conjugates $\alpha_1, \alpha_2, \ldots, \alpha_d$ (with α one of these) labelled so that $|\alpha_1| \geqslant |\alpha_2| \geqslant \cdots \geqslant |\alpha_d|$. In 1952 Remak [**10**] gave a new upper bound for the modulus of a Vandermonde determinant. When applied to the discriminant

$$\Delta = a_0^{2d-2} \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

his bound is

$$\sqrt{|\Delta|} \leqslant d^{d/2} |a_0|^{d-1} |\alpha_1|^{d-1} |\alpha_2|^{d-2} \ldots |\alpha_{d-1}|.$$

As we shall see from Theorem 1.1 below, this bound is at least as strong as the classical bound

$$\sqrt{|\Delta|} \leqslant d^{d/2} M(\alpha)^{d-1}, \tag{1.1}$$

1

which comes straight from Hadamard's inequality (see [**7**] and [**8**, p. 34]); sometimes Remak's bound is significantly stronger. Here $M(\alpha)$ is the Mahler measure (height)

$$M(\alpha) = |a_0| \prod_{i=1}^{d} \max(1, |\alpha_i|). \tag{1.2}$$

See, for example, Everest and Ward [**5**] for an introduction to Mahler measure.

Accordingly, we define the *Remak height* $\mathcal{R}(\alpha)$ by

$$\mathcal{R}(\alpha) = |a_0| \, |\alpha_1| \, |\alpha_2|^{(d-2)/(d-1)} |\alpha_3|^{(d-3)/(d-1)} \cdots |\alpha_{d-1}|^{1/(d-1)}, \tag{1.3}$$

so that Remak's bound can be written

$$\sqrt{|\Delta|} \leqslant d^{d/2} \mathcal{R}(\alpha)^{d-1}, \tag{1.4}$$

resembling (1.1).

In this paper we obtain sharp upper and lower bounds for $\mathcal{R}(\alpha)$ in terms of $M(\alpha)$, and describe in turn those α for which each of these bounds is in fact an equality. This leads us to the study of algebraic numbers lying with their conjugates on two circles (Theorem 2.1). Here and throughout the paper all circles are assumed to be centred at 0.

We first need some definitions. Recall that a *Salem number* is an algebraic integer $\tau > 1$ of degree at least 4, conjugate to τ^{-1}, whose other conjugates all lie on $|z| = 1$. Define an *extended Salem number* to be an algebraic number $\tau > 1$, of degree at least 4, conjugate to τ^{-1}, whose other conjugates all lie on $|z| = 1$. So the extended Salem numbers which are algebraic integers are the Salem numbers.*

An algebraic number α is *reciprocal* if α^{-1} is a conjugate of α. Say that an algebraic number α is *unit-circular* if α lies with its conjugates on $|z| = 1$. So, by Kronecker's Theorem [**5**, p. 27] the unit-circular algebraic integers are the roots of unity.

We now state our first main result.

Theorem 1.1. *Let α be an algebraic number of degree $d \geqslant 2$, and minimal polynomial $a_0 z^d + \cdots + a_d$ over the rationals. Then*

$$\left(M(\alpha)^{d/(d-1)} \frac{\min(|a_0|, |a_d|)}{(\max(|a_0|, |a_d|))^{1/(d-1)}} \right)^{1/2} \leqslant \mathcal{R}(\alpha) \leqslant M(\alpha). \tag{1.5}$$

The first inequality is an equality precisely when either

(i) $|a_0| = |a_d|$ *and α lies with its conjugates on two circles (but not on just one), or*

(ii) α *lies with its conjugates on one circle.*

The second inequality is an equality precisely when either

(iii) $d = 2$ *and $|\alpha_1| \geqslant 1 \geqslant |\alpha_2|$, or*

(iv) $d \geqslant 4$ *and α is either unit-circular or is $\pm$ an extended Salem number.*

---

* If Salem numbers were renamed Salem *integers*, then extended Salem numbers could simply be called Salem numbers!

Notes

(1) Since $M(\alpha) \geqslant \max(|a_0|, |a_d|)$, it follows from (1.5) that also

$$\mathcal{R}(\alpha) \geqslant \sqrt{M(\alpha)\min(|a_0|, |a_d|)}, \tag{1.6}$$

and so certainly

$$\mathcal{R}(\alpha) \geqslant \sqrt{|a_0 a_d|} \geqslant 1.$$

This last inequality was proved earlier in [**4**]. If α is not a unit, then $\mathcal{R}(\alpha) \geqslant \sqrt{2}$, with $\mathcal{R}(\alpha) = \sqrt{2}$ for $\alpha^d = \pm 2$ or $\pm 1/2$.

(2) From (1.5) and (1.6), $\mathcal{R}(\alpha) = 1$ if and only if $M(\alpha) = 1$. So $\mathcal{R}(\alpha) = 1$ if and only if α is a root of unity.

(3) Inequality (1.5) in fact holds for any $P \in \mathbb{C}[z]$ with $a_0 a_d \neq 0$ and $M(\alpha)$, $\mathcal{R}(\alpha)$ replaced by their polynomial versions $M(P)$ and $\mathcal{R}(P)$ defined as in (1.2) and (1.3), respectively, with the α_i being the zeros of P.

If we restrict Theorem 1.1 to α being a unit, we immediately get the following theorem.

Theorem 1.1′. *Let α be a unit of degree $d \geqslant 2$. Then*

$$M(\alpha)^{d/(2(d-1))} \leqslant \mathcal{R}(\alpha) \leqslant M(\alpha). \tag{1.5′}$$

The first inequality is an equality when either α lies with its conjugates on two circles, or α is cyclotomic.
The second inequality is an equality when either

(i) *$d = 2$, or*

(ii) *$d \geqslant 4$ and α is either cyclotomic or $\pm$ a Salem number.*

2. Conjugate sets of algebraic numbers on circles: results

In this section we describe those algebraic numbers α which satisfy either condition (i) or condition (ii) of Theorem 1.1. To do this, it is convenient at this point to make two more new definitions.

Define a *unit-norm* to be an algebraic number α with $|a_0| = |a_d|$. So the unit-norm algebraic integers are the units. Note that extended Salem numbers are unit-norms.

Let τ be an extended Salem number or a reciprocal quadratic, of degree $2s$, with conjugate set $\{\tau^{\pm 1}, \tau_2^{\pm 1}, \ldots, \tau_s^{\pm 1}\}$. We define an algebraic number ψ to be a *Salem half-norm* if $\psi = \tau^{\varepsilon_1} \tau_2^{\varepsilon_2} \ldots \tau_s^{\varepsilon_s}$ for some such τ and some $\varepsilon_i = \pm 1$ $(i = 1, \ldots, s)$. All 2^s such numbers are distinct (see Corollary 4.8).

Note that all conjugates of such a ψ are of the form $\psi' = \tau^{\delta_1} \tau_2^{\delta_2} \ldots \tau_s^{\delta_s}$ for some $\delta_i = \pm 1$ $(i = 1, \ldots, s)$, and so lie on the two circles $|z| = \tau$ and $|z| = \tau^{-1}$. In fact, as ψ is a unit-norm (by Lemma 4.5), half of its conjugates must lie on one circle, and half on the other. Clearly, $\deg \psi \leqslant 2^s$. It need not equal 2^s, however; the celebrated Lehmer degree $2s = 10$

example [**5**, p. 13] gives rise to two non-conjugate Salem half-norms, having minimal polynomials $P(z)$ and $z^{16}P(1/z)$, where

$$P(z) = z^{16}+2z^{15}+z^{14}-2z^{13}-4z^{12}-2z^{11}+3z^{10}+5z^9+3z^8+z^7-z^5-z^4-z^3+z^2+z+1.$$

We can now state our second main result, elucidating condition (i) of Theorem 1.1.

Theorem 2.1. *Suppose that a unit-norm α of degree d lies, with all its conjugates, on two circles $|z| = r$ and $|z| = R$, but not just on one, with (without loss of generality) at most half of the conjugates on $|z| = r$. Then one of the following holds.*

(a) *d is a multiple of 3, $R = r^{-1/2}$ with α having $d/3$ conjugates on $|z| = r$ and $2d/3$ conjugates on $|z| = r^{-1/2}$. Assuming (without loss of generality) that $|\alpha| = r$ we have, furthermore, that for some positive integer n, r^n $(= \sigma$ say) is a real, but non-totally real, cubic unit-norm, and $\alpha^n = \rho\sigma$, where ρ is unit-circular.*

(b) *d is even, $R = r^{-1}$, where $R > 1$ without loss of generality, and $d/2$ of the conjugates of α lie on each circle. Furthermore, for some positive integer n, R^n $(= \tau$ say) is either an extended Salem number or is reciprocal quadratic, and $\alpha^n = \rho\psi$, where ψ is a Salem half-norm defined by τ, and ρ is unit circular.*

Conversely, it is immediately clear that any α satisfying equations of the above type $\alpha^n = \rho\sigma$ or $\alpha^n = \rho\psi$ lies, with its conjugates, on two circles, of radii $\sigma^{1/n}$ and $\sigma^{-1/(2n)}$ in the first case, and of radii $\tau^{\pm 1/n}$ in the second case.

Further information on the degree of τ in case (b) is given in Lemma 8.1.

Again, if we restrict α to be a unit, we have the following theorem.

Theorem 2.1′. *Suppose that α is a unit of degree d lying, with its conjugates, on two circles, as in Theorem 2.1. Then d, R and r must satisfy one of the two alternatives (a) or (b) of Theorem 2.1. In case (a), for some m, $\alpha^m = \sigma$ is a non-totally real cubic unit, while in case (b), for some m, $\alpha^m = \psi$ is a Salem half-norm defined by a Salem number or a reciprocal quadratic.*

To clarify further how to construct α satisfying (ii) of Theorem 1.1, we need only quote the following result, due essentially to Robinson.

Proposition 2.2 (see § 2 in Robinson [11]). *Suppose that an algebraic number α lies with its conjugates on the circle $|z| = R$. Then, for some integer n, R^n is rational $(= q$ say), and $\alpha^n = \rho q$, where ρ is unit-circular.*

Conversely, given a positive rational q and ρ unit-circular, then α, defined as a root of $\alpha^n = \rho q$, lies with its conjugates, on the circle $|z| = q^{1/n}$.

Robinson's original result is formulated somewhat differently, as it incorporates the following characterization of unit-circular numbers (Proposition 2.3 (a) below). This, together with a similar characterization of extended Salem numbers (Proposition 2.3 (b)), shows that one can readily construct unit-circular numbers and extended Salem numbers.

Proposition 2.3.

(a) *The algebraic number ρ is unit-circular if and only if $\rho + \rho^{-1}$ is totally real and lies, with its conjugates, in the interval $[-2, 2]$. Thus, a unit-circular number is an algebraic number having minimal polynomial of the form*

$$A\prod_i (z^2 - \gamma_i z + 1) \in \mathbb{Z}[z]$$

for some $A \in \mathbb{N}$. Here the γ_i all lie in $[-2, 2]$, and together form a complete set of conjugates of γ_1.

(b) *The algebraic number $\tau > 1$ of degree greater than 2 is an extended Salem number if $\tau + \tau^{-1} > 2$ is totally real, with all its other conjugates in $(-2, 2)$. Thus an extended Salem number is an algebraic number having minimal polynomial of the form*

$$A\prod_i (z^2 - \gamma_i z + 1) \in \mathbb{Z}[z]$$

for some $A \in \mathbb{N}$. Here $\gamma_1 > 2$, all other γ_i lie in $(-2, 2)$, and the set of all γ_i forms a complete set of conjugates of γ_1.

3. Applications and some properties of $\mathcal{R}$

In this section we give some further results, readily deducible from our main result and from work of other authors. We also (Proposition 3.3) show how $\mathcal{R}(\alpha)$ can sometimes be written as a product of Mahler measures.

Firstly we have the following corollary.

Corollary 3.1. *Given $d \geqslant 2$, then there is a unit-norm (and indeed a unit) of degree d lying with its conjugates on two circles, but not one, if and only if $d \neq \pm 1 \bmod 6$.*

The proof follows using Theorem 2.1, which tells us that if such a unit-norm exists then $d \neq \pm 1 \bmod 6$. Conversely, if d is even then $z^d - z^{d/2} - 1$ is irreducible, while if d is a multiple of 3 then $z^d - z^{d/3} - 1$ is irreducible [9]. Each of these polynomials has its zeros on two circles.

Next, recall the known lower bounds for $M(\alpha)$, where α is a non-cyclotomic algebraic number of degree $d \geqslant 2$ [14, 17]

$$M(\alpha) \geqslant \begin{cases} \theta_0 & \text{if } \alpha \text{ is non-reciprocal,} \\ 1 + \dfrac{1}{4}\left(\dfrac{\log\log d}{\log d}\right)^3 & \text{unconditionally.} \end{cases}$$

Here $\theta_0 > 1$ is the real root of $x^3 - x - 1 = 0$. (It is the smallest Pisot number [13].) For $\mathcal{R}(\alpha)$ we have a corresponding result as follows.

Corollary 3.2. *For non-cyclotomic α of degree $d \geqslant 2$*

$$\mathcal{R}(\alpha) \geqslant \begin{cases} \theta_0^{d/(2(d-1))} & \text{if } \alpha \text{ is non-reciprocal,} \\ 1 + \dfrac{1}{9} \left(\dfrac{\log \log d}{\log d} \right)^3 & \text{unconditionally.} \end{cases}$$

This result comes simply from applying (1.6) to the above inequality for $M(\alpha)$, and then using the fact that

$$(1 + \tfrac{1}{4}\delta)^{1/2} > 1 + \tfrac{1}{9}\delta \quad \text{for } 0 < \delta < \tfrac{9}{4}.$$

Proposition 3.3. *For α in $\bar{\mathbb{Q}}^*$, $\mathcal{R}(\alpha^{-1}) = \mathcal{R}(\alpha)$. Furthermore, if α is a unit of degree $d \geqslant 2$, then*

$$\mathcal{R}(\alpha) = \left(\prod M\left(\frac{\alpha_i}{\alpha_j} \right) \right)^{1/(2(d-1))},$$

where the product is taken over a maximal set of non-conjugate ratios α_i/α_j of conjugates α_i, α_j of α. In particular, if α_1/α_2 has full degree $d(d-1)$, then

$$\mathcal{R}(\alpha) = M(\alpha_1/\alpha_2)^{1/(2(d-1))}.$$

Proof. From the definition of $\mathcal{R}$,

$$\frac{\mathcal{R}(\alpha)}{\mathcal{R}(\alpha^{-1})} = \frac{|a_0|}{|a_d|} \prod_{i=1}^{d} |\alpha_i| = 1,$$

which proves the first statement.

For the second statement, we have, for α a unit,

$$\begin{aligned} \mathcal{R}(\alpha)^{2(d-1)} &= \mathcal{R}(\alpha)^{d-1} \mathcal{R}(\alpha^{-1})^{d-1} \\ &= \frac{|\alpha_1|^{d-1} |\alpha_2|^{d-2} \dots |\alpha_{d-1}|}{|\alpha_2||\alpha_3|^2 \dots |\alpha_d|^{d-1}} \\ &= \prod \left| \frac{\alpha_i}{\alpha_j} \right|, \end{aligned}$$

the product being taken over all $i, j \in \{1, \dots, d\}$ such that $|\alpha_i| \geqslant |\alpha_j|$. This product is clearly $\prod M(\alpha_i/\alpha_j)$ with the product as in the statement of the proposition. $\qquad \square$

Notes

(1) If $P(z) = \prod_i (z - \alpha_i) \in \mathbb{C}[z]$ has $P(0) \neq 0$, and we put

$$Q(z) = \prod_{i \neq j} (z - \alpha_i/\alpha_j),$$

then the same proof as in the proposition gives $\mathcal{R}(P) = \sqrt{|P(0)|} M(Q)^{1/(2(d-1))}$.

(2) If α is a unit and α_1/α_2 has degree $d(d-1)$, then, by the proposition, Remak's inequality (1.4) becomes

$$|\Delta| \leqslant M(\alpha_1/\alpha_2) d^d.$$

4. Lemmas for the proof

We need the following simple results.

Lemma 4.1. *Suppose that $\beta, \beta_2, \ldots, \beta_k$ are conjugate algebraic numbers satisfying $\beta^{n_1} \beta_2^{n_2} \ldots \beta_k^{n_k} = 1$, where $n_1, n_2, \ldots, n_k$ are integers with $|n_1| > |n_2| + \cdots + |n_k|$. Then β is unit-circular. Furthermore, if β has any real conjugates, then $\beta = \pm 1$.*

This is in fact a weak version of Corollary 2 of [**16**], which had the stronger conclusion that β is a root of unity. However, we give a self-contained proof.

Proof. As usual, let $\overline{|\beta|}$, the *house* of β, be the maximum of the absolute values of β and its other conjugates. If $\overline{|1/\beta|} > \overline{|\beta|}$, replace β by $1/\beta$ so that we can assume that $\overline{|\beta|} \geqslant \overline{|1/\beta|}$ and thus

$$|\beta_i| \geqslant 1/\overline{|\beta|} \tag{4.1}$$

for any conjugate β_i of β. Clearly, $\overline{|\beta|} \geqslant 1$. Now choose an automorphism of a suitable finite normal extension of $\mathbb{Q}$ containing β which maps β to a conjugate β' of absolute value $\overline{|\beta|}$ and $\beta_i \mapsto \beta_i'$ $(i = 2, \ldots, k)$ so that $\beta'^{n_1} \beta_2'^{n_2} \ldots \beta_k'^{n_k} = 1$. Now, using (4.1) we see that

$$\begin{aligned} 1 &= \overline{|\beta|}^{n_1} |\beta_2'|^{n_2} \ldots |\beta_k'|^{n_k} \\ &\geqslant \overline{|\beta|}^{n_1 - n_2 - \cdots - n_k} \geqslant \overline{|\beta|}, \end{aligned}$$

giving $\overline{|\beta|} = 1$. Hence, from (4.1) again, β is unit-circular.

The final statement is immediate. $\qquad\qquad\square$

Lemma 4.2 (see [15]). *If β is an algebraic number with conjugates β', β'' satisfying $\beta'\beta'' = \beta^{2\varepsilon}$, where $\varepsilon = \pm 1$, then for some positive integer n, $\beta'^n = \beta^{\varepsilon n}$.*

Proof. (A simplified version of that in [**15**].) We can assume $\beta \neq 0$. Also, using Dirichlet's Theorem, we can find a positive integer n such that, on replacing β and its conjugates by their nth powers, we can assume that β and its conjugates all have positive real part. Next, among all conjugates β^* of β with $|\log|\beta^*||$ maximal, choose the conjugate (β_1 say) with largest argument (in absolute value). Now, use a suitable automorphism to map β to β_1, the same automorphism taking $\beta' \mapsto \beta_2$, $\beta'' \mapsto \beta_3$ say. Then $\beta_2\beta_3 = \beta_1^{2\varepsilon}$, which, by argument considerations shows that $\arg \beta_2 = \varepsilon \arg \beta_1$, and by modulus considerations shows that $|\beta_2| = |\beta_1^\varepsilon|$. Hence $\beta_2 = \beta_1^\varepsilon$ which, on applying the inverse automorphism to the one just used, gives $\beta' = \beta^\varepsilon$ (so in fact, reverting to the original βs, $\beta'^n = \beta^{\varepsilon n}$). $\quad\square$

The following result is due essentially to Boyd [**2**] and Ferguson [**6**]. However, it is readily deducible from Lemma 4.2 (which is what Ferguson does), so we give the proof.

Lemma 4.3. *Given a real algebraic number $\beta > 0$, there is a positive integer m such that no conjugate of β^m, except β^m itself, has modulus β^m.*

Proof. If no other conjugate of β has modulus β, we can take $m = 1$. Otherwise, suppose that $\beta' \neq \beta$ is a conjugate of β having modulus β. Then $\beta' \overline{\beta'} = \beta^2$ and so, by Lemma 4.2, $\beta'^n = \beta^n$ for some $n \in \mathbb{N}$. Doing the same for every conjugate of β having modulus β, and taking the least common multiple (lcm) (N, say) of all the corresponding integers n obtained, we see that β^N has no other conjugates of modulus β^N. $\square$

We note in passing that, on applying the lemma to all real conjugates of any algebraic β, we have the following corollary.

Corollary 4.4. *For any algebraic number β there is a positive integer n such that the set of moduli of the non-real conjugates of β^n is distinct from the set of moduli of the real conjugates of β^n.*

Lemma 4.5. *The unit-norms form a subgroup of $\bar{\mathbb{Q}}^*$.*

Proof. Denote by $\mathcal{N}(\alpha)$ the modulus of the norm of α $(= |a_d/a_0|)$ and by $\mathcal{N}_K(\alpha)$ the modulus of its field norm $(= \mathcal{N}(\alpha)^{[K:\mathbb{Q}(\alpha)]})$ for a number field K containing α. Now assume that α and α' are unit norms, and that $\alpha\alpha'$ has degree d^*. Then, since $\mathcal{N}_K(\alpha) = \mathcal{N}_K(\alpha') = 1$ and the field norm is multiplicative we have, for $K = \mathbb{Q}(\alpha, \alpha')$ with $[K : \mathbb{Q}] = D$,

$$\mathcal{N}(\alpha\alpha') = \mathcal{N}_K(\alpha\alpha')^{d^*/D} = \mathcal{N}_K(\alpha)^{d^*/D} \mathcal{N}_K(\alpha')^{d^*/D} = 1.$$

Since $\mathcal{N}(\alpha^{-1}) = 1/\mathcal{N}(\alpha) = 1$, the result is proved. $\square$

Lemma 4.6. *Suppose that $b_1 \geqslant b_2 \geqslant \cdots \geqslant b_m \geqslant 0$ and $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_m \geqslant 0$, with*

$$\overline{\lambda} = \frac{1}{m} \sum \lambda_i.$$

Then

$$\sum \lambda_i b_i \geqslant \overline{\lambda} \sum b_i \geqslant \sum \lambda_{m+1-i} b_i.$$

If in fact the λ_i are strictly decreasing, then

$$\sum \lambda_i b_i = \overline{\lambda} \sum b_i \quad \text{or} \quad \sum \lambda_{m+1-i} b_i = \overline{\lambda} \sum b_i$$

only if all the b_i are equal.

Proof. From [**8**, p. 286] we know that if $\lambda'_1, \ldots, \lambda'_m$ are any permutation of $\lambda_1, \ldots, \lambda_m$, then the sum $\sum \lambda'_i b_i$ is largest when $\lambda'_i = \lambda_i$ $(i = 1, \ldots, m)$. Hence $\sum \lambda_i b_i$ is at least as large as the average of $\sum \lambda'_i b_i$ taken over all possible permutations $\lambda'_1, \ldots, \lambda'_m$ of $\lambda_1, \ldots, \lambda_m$.

Hence

$$\sum \lambda_i b_i \geqslant \sum_i (\text{average of } \lambda'_i) \, b_i = \bar{\lambda} \sum b_i.$$

Replacing λ_i by $\lambda_1 - \lambda_{m+1-i}$, this inequality gives

$$\sum (\lambda_1 - \lambda_{m+1-i}) b_i \geqslant (\lambda_1 - \bar{\lambda}) \sum b_i,$$

so that

$$\bar{\lambda} \sum b_i \geqslant \sum \lambda_{m+1-i} b_i,$$

as required.

Suppose now that the λ_i are strictly decreasing, and that two of the b_i are different, say $b_k \neq b_\ell$. Then the sum $\sum \lambda_i b_i$ is decreased by interchanging λ_k and λ_ℓ, so that the averaging process above gives a strict inequality. A similar argument applies for $\sum \lambda_{m+1-i} b_i$. $\qquad \square$

We also need the following lemma.

Lemma 4.7. *(Salem [12], p. 32) Let $\tau > 1$ be an extended Salem number of degree $2s$, with other conjugates τ^{-1} and $\tau_2^{\pm 1}, \ldots, \tau_s^{\pm 1}$. Then the number of π and the arguments of $\tau_2, \ldots, \tau_s$ are linearly independent over $\mathbb{Q}$.*

Proof. Suppose on the contrary that $\tau_2^{q_2} \ldots \tau_s^{q_s}$ is a root of unity, where the q_i are rational, and not all zero. By taking an appropriate positive integer power, one can assume that the q_i are integers, and that $\tau_2^{q_2} \ldots \tau_s^{q_s} = 1$. Take i such that $q_i \neq 0$, and an automorphism ϑ of $\mathbb{Q}(\tau_2, \ldots, \tau_s)/\mathbb{Q}$ taking $\tau_i \mapsto \tau$. Then $|\vartheta(\tau_2^{q_2} \ldots \tau_s^{q_s})| = \tau^{q_i} \neq 1$, a contradiction. $\qquad \square$

Corollary 4.8. *For any positive integer m, all 2^s numbers $\tau^{\pm m} \tau_2^{\pm m} \ldots \tau_s^{\pm m}$ are distinct.*

5. Proof of Theorem 1.1

Suppose that

$$|\alpha_1| \geqslant |\alpha_2| \geqslant \cdots \geqslant |\alpha_k| \geqslant 1 \geqslant |\alpha_{k+1}| \geqslant \cdots \geqslant |\alpha_d|, \qquad (5.1)$$

where $k \in \{0, 1, \ldots, d\}$. Then, by (1.3),

$$\mathcal{R}(\alpha)^{d-1} = |a_0|^{d-1} |\alpha_1|^{d-1} |\alpha_2|^{d-2} \ldots |\alpha_k|^{d-k} \left(\left(\frac{1}{|\alpha_{k+1}|} \right)^{d-(k+1)} \ldots \left(\frac{1}{|\alpha_d|} \right)^{d-d} \right)^{-1}$$

$$\geqslant |a_0|^{d-1} \left(\prod_{i=1}^{k} |\alpha_i| \right)^{d-(k+1)/2} \left(\prod_{i=k+1}^{d} |\alpha_i| \right)^{(d-(k+1))/2}$$

on applying the first inequality of Lemma 4.6 to $b_i = \log|\alpha_i|$ $(i = 1, \ldots, k)$, and the second inequality of Lemma 4.6 to $b_i = \log(1/|\alpha_{k+i}|)$ $(i = 1, \ldots, d-k)$. Now

$$\prod_{i=1}^{k} |\alpha_i| = M(\alpha)/|a_0|,$$

while

$$\prod_{i=k+1}^{d} |\alpha_i| = |a_d|/M(\alpha),$$

so that

$$\mathcal{R}(\alpha)^{d-1} \geqslant |a_0|^{(k-1)/2}|a_d|^{(d-k-1)/2}M(\alpha)^{d/2}. \tag{5.2}$$

If $k = 0$ then $|a_0| \geqslant |a_d|$, while if $k = d$ then $|a_d| \geqslant |a_0|$. Thus from (5.2) we get, in either case

$$\mathcal{R}(\alpha)^{d-1} \geqslant (\max(|a_0|, |a_d|))^{-1/2}(\min(|a_0|, |a_d|))^{(d-1)/2}M(\alpha)^{d/2}. \tag{5.3}$$

If $k \in \{1, \dots, d-1\}$ then both $(k-1)/2$ and $(d-k-1)/2$ are non-negative, so that again

$$\begin{aligned}
\mathcal{R}(\alpha)^{d-1} &\geqslant (\min(|a_0|, |a_d|))^{d/2-1}M(\alpha)^{d/2} \\
&\geqslant (\max(|a_0|, |a_d|))^{-1/2}(\min(|a_0|, |a_d|))^{(d-1)/2}M(\alpha)^{d/2}, \tag{5.4}
\end{aligned}$$

which gives (5.3). From above, and the second part of Lemma 4.6, we see that equality in (5.4) occurs when either

(i) $k \in \{1, 2, \dots, d-1\}$, $|a_0| = |a_d|$, and all α_i lie on the two circles $|z| = (M(\alpha)/|a_0|)^{1/k}$ and $|z| = (|a_d|/M(\alpha))^{1/(d-k)}$, with k on the first circle and $d - k$ on the second, or

(ii) $k = 0$ or d and all α_i lie on the circle $|z| = |a_d/a_0|^{1/d}$.

Conversely, if all the α_i lie on one circle $|z| = r$, or $|a_0| = |a_d|$ and all α_i lie on two circles $|z| = r$ and $|z| = R$, it is easily checked that equality holds.

For the theorem's second inequality $\mathcal{R}(\alpha) \leqslant M(\alpha)$, simply note that, defining k by (5.1), we have

$$\begin{aligned}
\mathcal{R}(\alpha)^{d-1} &\leqslant |a_0|^{d-1}|\alpha_1|^{d-1}\dots|\alpha_k|^{d-k} \\
&\leqslant |a_0|^{d-1}\left(\prod_{i=1}^{k}|\alpha_i|\right)^{d-1} \\
&\leqslant M(\alpha)^{d-1},
\end{aligned}$$

with equality throughout if all of $|\alpha_2| = \dots = |\alpha_{d-1}| = 1$. If this happens, then for $d > 2$, $|\alpha_2| = 1$ implies that α is reciprocal (α_2 being conjugate to $\bar{\alpha}_2 = 1/\alpha_2$), so that α must be either unit-circular or $\pm$ an extended Salem number. If, however, $d = 2$, then equality clearly occurs provided $|\alpha_1| \geqslant 1 \geqslant |\alpha_2|$.

6. Conjugate sets of algebraic numbers on two circles

In Theorem 2.1, we described conjugate sets of algebraic numbers lying on two circles, with the additional property that $|a_0| = |a_d|$. The first step in proving this theorem is the following.

Lemma 6.1. *Let α be a unit-norm lying with its conjugates on two circles, but not just on one circle, with k conjugates on $|z| = R$ say, and ℓ conjugates on $|z| = r$, where of course $R \neq r$ and (without loss of generality) $k \geqslant \ell$. Then either*

(i) 'the two-to-one case': $k = 2\ell$ and $r = R^{-2}$; or

(ii) 'the one-to-one case': $k = \ell$ and $r = R^{-1}$.

Proof. We may suppose that α is on $|z| = R$, with a conjugate α_1 say on $|z| = r$. Then as α is a unit-norm, the product of the conjugates of α is ± 1, giving

$$(\alpha\bar\alpha)^k(\alpha_1\bar\alpha_1)^\ell = 1, \tag{6.1}$$

and so also

$$r = R^{-k/\ell}. \tag{6.2}$$

Now apply an automorphism of some suitable normal extension of $\mathbb{Q}$ containing α, this automorphism taking $\alpha_1 \mapsto \alpha$, and say α, $\bar\alpha$ and $\bar\alpha_1$ to conjugates α_2, α_3, α_4, respectively. Then from (6.1) $(\alpha_2\alpha_3)^k(\alpha\alpha_4)^\ell = 1$, and so certainly

$$|\alpha_2|^k|\alpha_3|^k|\alpha|^\ell|\alpha_4|^\ell = 1. \tag{6.3}$$

(We do not claim that these αs are distinct and indeed if α_1 is real, $\alpha_4 = \alpha$.) Since α_2, α_3 and α_4 are either on $|z| = R$ or $|z| = r$, the left-hand side of (6.3) can take one of only six values: $R^{2k+2\ell}$, $R^{2k+\ell}r^\ell$, $R^{k+2\ell}r^k$, $R^{k+\ell}r^{k+\ell}$, $R^{2l}r^{2k}$ or $R^\ell r^{2k+\ell}$.

Substituting for r using (6.2), we see that these six values are powers of R, where the exponent can be $2k + 2\ell$, $k + \ell$, $(2\ell - k)(1 + k/\ell)$, $(\ell - k)(1 + k/\ell)$, $2(\ell - k)(\ell + k)$ or $(\ell - 2k)(1 + k/\ell)$. However, α_1 is a unit-norm, as $R \neq 1$ so that, by (6.3), this power must be 0. Since $k \geqslant \ell$, this can happen only if $k = 2\ell$ (third case) or $k = \ell$ (fourth and fifth cases). Finally, the use of (6.2) completes the proof. $\square$

In the following two sections we study the radius R for each of the two cases (i) and (ii) in the previous lemma. As we shall see, in each case some power R^n of R is very tightly constrained.

7. The two-to-one case

In this section we analyse further the two-to-one case of Lemma 6.1.

Lemma 7.1. *Suppose that α is a unit-norm with $2d/3$ conjugates on $|z| = R$, with the remaining $d/3$ conjugates on $|z| = 1/R^2(= r)$. Then, for some positive integer n, r^n is a real cubic unit-norm whose two other conjugates are non-real.*

Proof. We may assume that $|\alpha| = R$. Then, by Lemma 4.3, there is an integer n such that $|\alpha|^{2n}$ has no other conjugates of modulus $|\alpha|^{2n}$. Hence, on renaming α^n as α and R^n as R, and putting $\beta = \alpha\bar\alpha = R^2$, we can assume that β has no other conjugates of modulus β.

Next, note that β cannot be rational. For otherwise we could choose an automorphism taking $\alpha \mapsto \alpha_1$, where α_1 is on $|z| = 1/R^2$, say $\bar\alpha \mapsto \alpha_2$ and of course $\beta \mapsto \beta$. Then we would have $\beta = \alpha_1\alpha_2$, from which $|\alpha_2| = \beta/|\alpha_1| = R^4$, which is impossible. Hence β

has at least one conjugate not equal to β. Let β' be any such conjugate. Now, choose an automorphism taking $\beta \mapsto \beta'$, and say $\alpha \mapsto \alpha_3$, $\bar{\alpha} \mapsto \alpha_4$. Since $\beta' = \alpha_3 \alpha_4$, by the first paragraph of the proof, α_3 and α_4 cannot both have modulus R. On the other hand, they cannot both have modulus $1/R^2$ either, for then $\beta^4 \beta' \overline{\beta'} = 1$, contradicting Lemma 4.1. Hence one of α_3 and α_4 is on each circle, $|\beta'| = 1/R$, and so $\beta \beta' \overline{\beta'} = 1$. Note that β' cannot be real, as $\beta \beta'^2 = 1$ also contradicts Lemma 4.1. So all other conjugates β' of β lie on $|z| = 1/R$. Suppose that there are 2ℓ of them, so that the norm of β is $\beta^{1-\ell}$. But $\beta = \alpha\bar{\alpha}$ is a unit-norm, by Lemma 4.5. Hence $\ell = 1$ and β^{-1} $(= r^n = R^{-2n}$ for the original $R)$ is real, cubic, non-totally real and a unit norm. $\qquad\square$

Lemma 7.2. *Let α be as in the statement of Lemma 7.1. Then for some positive integer n some conjugate of α^n is of the form $\rho\sigma$, where ρ is unit-circular and σ is real, cubic, non-totally real and a unit-norm.*

Proof. This time take α with $|\alpha| = r = 1/R^2$. By replacing α by a power α^n and R by R^n we can, as in the proof of the previous lemma, assume that

$$(\beta\alpha)(\beta\bar{\alpha}) = 1, \tag{7.1}$$

where $\beta = R^2$ is cubic with conjugates β', $\overline{\beta'}$ of modulus $1/R$. Now consider the possible moduli of conjugates of $\beta\alpha$ and $\beta\bar{\alpha}$. For any conjugate α' of α, $\beta\alpha'$ can have modulus R^3 or 1, while $\beta'\alpha'$ (or $\overline{\beta'}\alpha'$) can have modulus 1 or $1/R^3$. So, no pair of conjugates of $\beta\alpha$ and $\beta\bar{\alpha}$ can be reciprocals of one another unless both are of modulus 1. But applying an automorphism to (7.1) we see that every conjugate of $\beta\alpha$ must be part of such a reciprocal pair. Hence $\beta\alpha$ is unit-circular ($= \rho$ say), and so $\alpha = \rho\sigma$, where $\sigma = 1/\beta$. Finally, $\alpha^n = \rho\sigma$ for the original α. $\qquad\square$

We have thus completed the proof of alternative (a) of Theorem 2.1.

8. The one-to-one case

The following lemma describes the radii R, R^{-1} of the circles in the 'one-to-one case' of Theorem 2.1. We can clearly assume that $R > 1$.

Lemma 8.1. *Let α be an algebraic number of degree d with half of its conjugates on $|z| = R > 1$, and the other half on $|z| = R^{-1}$. Then there is a natural number n such that R^{2n} $(= \tau$, say$)$ is either a reciprocal quadratic or an extended Salem number, and of degree at most*

$$\begin{cases} d_n & \text{if } \alpha^n \text{ is reciprocal,} \\ d_n + 2 & \text{otherwise.} \end{cases}$$

Here $d_n = \deg(\alpha^n) \leqslant d$.

Proof. First, we use Lemma 4.3 to find an even integer $2n$ such that $|\alpha|^{2n}$ has no other conjugates of modulus $|\alpha|^{2n}$. So we replace α^n by α, write d for d_n, and put $\tau = R^2 = \alpha\bar{\alpha}$ $(=$ the old $|\alpha|^{2n})$. Then τ has no other conjugates of modulus τ. We can

clearly assume that $\tau > 1$, and, by doubling n if necessary, that all real conjugates of τ are positive. Note that any conjugate of τ, excluding τ itself, being of the form $\alpha'\alpha''$ for some conjugates α', α'' of α, has modulus 1 or $R^{-2} = \tau^{-1}$. Now since α and $\bar{\alpha}$ are unit-norms, so is τ by Lemma 4.5. Hence τ in fact has exactly one conjugate of modulus τ^{-1}, which must therefore be τ^{-1}. All conjugates of τ, except τ and τ^{-1}, therefore have modulus 1, making τ an extended Salem number, or reciprocal quadratic.

To bound the degree of τ, consider

$$T(x) = \prod_{1 \leqslant i < j \leqslant d} (x - \alpha_i \alpha_j) \in \mathbb{Q}[x],$$

a polynomial of degree $\binom{d}{2}$. This has $(x - \tau)^{d/4}$ as a factor, there being $d/4$ sets $\{\alpha, \bar{\alpha}\}$ on $|z| = R$. Hence $T(x)$ is divisible by $P_\tau(x)^{d/4}$, where P_τ is the minimal polynomial of τ over $\mathbb{Q}$. But note that none of the non-real $\alpha_i \alpha_j$ on $|z| = \tau$ or $|z| = \tau^{-1}$ are conjugates of τ. There are

$$2\left(\binom{d/2}{2} - \frac{d}{4}\right) = \frac{d}{4}(d - 4)$$

of these. Hence

$$\deg \tau \times \frac{d}{4} \leqslant \binom{d}{2} - \frac{d}{4}(d - 4) = \frac{d}{4}(d + 2), \tag{8.1}$$

giving $\deg \tau \leqslant d + 2$.

If α is reciprocal, then $T(x)$ is also divisible by $(x-1)^{d/2}$ coming from $\alpha_i \times (1/\alpha_i) = 1$, $d/2$ times. This modifies (8.1) to

$$\deg \tau \times \frac{d}{4} \leqslant \frac{d}{4}(d + 2) - \frac{d}{2}$$

so that $\deg \tau \leqslant d$, as claimed. $\qquad\square$

The following result will complete the proof of Theorem 2.1.

Lemma 8.2. *Let $\tau > 1$ be a reciprocal quadratic or an extended Salem number, of degree $2s$, with conjugate set $\{\tau^{\pm 1}, \tau_2^{\pm 1}, \ldots, \tau_s^{\pm 1}\}$. Suppose that α, of degree d, lies with its conjugates on $|z| = \tau$ and $|z| = \tau^{-1}$, half of the conjugates being on each circle. Then $\alpha = \rho\tau^{\varepsilon_1}\tau_2^{\varepsilon_2} \ldots \tau_s^{\varepsilon_s}$, where $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$ are each ± 1, and ρ is unit-circular.*

Proof. For the proof, it is convenient to define a graph G with d vertices, labelled by α and its conjugates. The edges of G, labelled by one of the $2s$ elements of $\{\pm 1, \pm 2, \ldots, \pm s\}$, are as follows: there is an edge joining α and α' with label i if $\alpha\alpha' = \tau_i^2$, and such an edge with label $-i$ if $\alpha\alpha' = \tau_i^{-2}$.

We summarize the properties of G (not all of which are, in fact, needed for the proof) as follows.
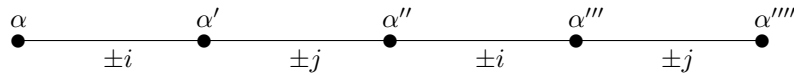
Sublemma.

(a) *The graph G is s-regular, with the s edges incident at every vertex labelled by $\varepsilon_1 1, \varepsilon_2 2, \ldots, \varepsilon_s s$ for some choice of signs $\varepsilon_i = \pm(i = 1, \ldots, s)$.*

(b) *The subgraph G_i consisting of the edges of G labelled $\pm i$ consists of $d/2$ disconnected edges, with $d/4$ labelled i and $d/4$ labelled $-i$.*

(c) *The subgraph G_{ij} consisting of the edges of G labelled $\pm i$ or $\pm j$ is composed of $d/4$ disconnected 4-cycles, each 4-cycle being labelled with i, $-i$, j, $-j$ in an order such that the $\pm i$ and $\pm j$ alternate.*

Proof of the sublemma. We prove part (b) first. Consider the subgraph G_1 of G, having edges labelled ± 1, corresponding to the identities $\alpha\bar{\alpha} = \tau^2$ or $\alpha\bar{\alpha} = \tau^{-2}$. Clearly, every vertex has exactly one such edge incident to it, so that G_1 consists of $d/2$ disconnected edges. Now, applying an automorphism to a normal extension of $\mathbb{Q}$ containing α (and so τ^2) which takes $\tau \mapsto \tau_i$, we see that these $d/2$ identities (and so $d/2$ edges of G labelled ± 1) above give $d/2$ identities for every i, and so $d/2$ edges of G labelled $\pm i$. In this way we obtain, for each vertex of G and for each i, an edge labelled i or $-i$ incident to that vertex.

We claim that we have found all the edges in this way, so that each vertex has for each i *exactly* one edge labelled i or $-i$ incident to it. To see this, note that if $\alpha\alpha' = \tau_i^2$, then α' is determined by α and i. If also $\alpha\alpha'' = \tau_i^{-2}$, then $\alpha^2\alpha'\alpha'' = 1$, so that, by Lemma 2, $\alpha'^n = \alpha^{-n}$ for some $n \in \mathbb{N}$. Thus $\alpha\alpha' = \tau_i^2$ is a root of unity, which is clearly false. This proves (b), and hence (a).

To prove (c), let $i \neq j$ be in $\{1, \ldots, s\}$, and consider a path

$$
\begin{array}{ccccccccc}
\alpha & & \alpha' & & \alpha'' & & \alpha''' & & \alpha'''' \\
\bullet & \rule[0.5ex]{3em}{0.4pt} & \bullet & \rule[0.5ex]{3em}{0.4pt} & \bullet & \rule[0.5ex]{3em}{0.4pt} & \bullet & \rule[0.5ex]{3em}{0.4pt} & \bullet \\
& \pm i & & \pm j & & \pm i & & \pm j &
\end{array}
$$

where the $\pm$ signs are, say, ε_0, ε_1, ε_2 and ε_3, respectively. From the associated identities we have

$$\alpha'''' = \frac{\tau_j^{2\varepsilon_3}}{\alpha'''} = \frac{\tau_j^{2\varepsilon_3}\alpha''}{\tau_i^{2\varepsilon_2}} = \frac{\tau_j^{2(\varepsilon_3+\varepsilon_1)}}{\tau_i^{2\varepsilon_2}\alpha'} = \frac{\tau_j^{2(\varepsilon_3+\varepsilon_1)}\alpha}{\tau_i^{2(\varepsilon_2+\varepsilon_0)}}. \tag{8.2}$$

Now, mapping $\tau_i \mapsto \tau$ and, say, $\alpha'''' \mapsto \alpha^*$, $\alpha \mapsto \alpha^{**}$, $\tau_j \mapsto \tau_\ell$, we get

$$\alpha^* = \frac{\tau_\ell^{2(\varepsilon_3+\varepsilon_1)}\alpha^{**}}{\tau^{2(\varepsilon_2+\varepsilon_0)}}.$$

Since α^* and α^{**} have modulus τ or τ^{-1}, we must have $\varepsilon_2 = -\varepsilon_0$. Similarly, mapping $\tau_j \mapsto \tau$ we get $\varepsilon_3 = -\varepsilon_1$, and hence, from (8.2), $\alpha'''' = \alpha$. This proves (c) and hence the sublemma. $\qquad\square$

We can now complete the proof of Lemma 8.2. Consider the vertex α of G, with its s incident edges, labelled $\varepsilon_1 1, \varepsilon_2 2, \ldots, \varepsilon_s s$ say. Define ρ by $\alpha = \rho\tau^{\varepsilon_1}\tau_2^{\varepsilon_2}\ldots\tau_s^{\varepsilon_s}$. Note that, from the identity $\alpha\bar{\alpha} = \tau^{2\varepsilon_1}$ associated to the first of the edges, we have $|\rho| = 1$. Suppose

that ρ has a conjugate ρ' with $|\rho'| > 1$. Take an automorphism mapping $\rho \mapsto \rho'$ and $\alpha \mapsto \alpha'$ say, with $|\alpha'| = |\rho'|\tau^\delta$, where say $\tau_k^{\varepsilon_k} \mapsto \tau^\delta$, with $\delta = \pm 1$. If $\delta = 1$, then $|\alpha'| > \tau$, so $\delta = -1$, $|\rho'| = \tau^2$ and $|\alpha'| = \tau$. Now let α_k be the vertex adjacent to α with label $\varepsilon_k k$, and associated identity $\alpha\alpha_k = \tau_k^{2\varepsilon_k}$. If $\alpha_k \mapsto \alpha'_k$ under this automorphism, then $|\alpha'_k| = \tau^{-2}/|\alpha'| = \tau^{-3}$, which is impossible.

The same argument applied to $\alpha^{-1} = \rho^{-1}\tau^{-\varepsilon_0}\tau_2^{-\varepsilon_2}\ldots\tau_s^{-\varepsilon_s}$ shows that ρ^{-1} has no conjugate greater than 1 in modulus. Hence ρ is unit circular, and $\alpha = \rho\tau^{\varepsilon_1}\tau_2^{\varepsilon_2}\ldots\tau_s^{\varepsilon_s}$. $\quad\square$

This completes the proof of Theorem 2.1.

9. Proof of Theorem 2.1$'$

For Theorem 2.1$'$, we need the following.

Observation. *If η is algebraic, ρ is unit-circular and $\rho\eta$ is a unit, then $\eta\bar\eta$ is also a unit.*

This simply follows from the fact that $\eta\bar\eta = (\rho\eta)(\bar\rho\eta)$.

To deduce Theorem 2.1$'$ from Theorem 2.1, take α a unit lying with its conjugates on two (but not one) circles. Note that, on replacing α by a conjugate if necessary, we have $\alpha^n = \rho\eta$, where $\eta = \sigma$ is a real, non-totally real, cubic in case (a), and $\eta = \psi = \tau^{\varepsilon_1}\tau_2^{\varepsilon_2}\ldots\tau_s^{\varepsilon_s}$ is a Salem half-norm in case (b).

Assume that α, and so α^n, is a unit. Then, by the observation, $\eta\bar\eta$ is also a unit. Hence in case (a) $\sigma = \eta^{1/2}$ is a real cubic unit. In case (b), $\tau = (\psi\bar\psi)^{\varepsilon_1/2}$ is a unit, and so a Salem number, and ψ is also a unit. Thus, in either case $\eta = \sigma$ or ψ is a unit, and therefore so is $\rho = (\rho\eta)\eta^{-1}$. Hence ρ is a root of unity, say with $\rho^m = 1$. It follows that

$$\alpha^{nm} = \eta^m = \sigma^m \text{ or } \psi^m.$$

So σ^m is a real, non-totally real, cubic unit and, by Corollary 4.8, ψ^m is a Salem half-norm defined by the Salem number (or the reciprocal quadratic) τ^m. Finally, on replacing σ^m by σ, ψ^m by ψ and nm by m, we obtain Theorem 2.1$'$.

10. Further remarks

(1) *Remak's and Hadamard's inequalities.* When applied to totally real α, Bertin [1] showed that the $d^{d/2}$ in (1.4) could be replaced by $4^{\lfloor d/2\rfloor}$.

There is an inequality combining both Hadamard's and Remak's inequalities. If, for $1 \leqslant i, j \leqslant d$, $a_{ij} \in \mathbb{C}$ and $x_j \in \mathbb{C}$ with $|x_1| \geqslant |x_2| \geqslant \cdots \geqslant |x_d|$, then

$$|\det((a_{ij}x_j^{i-1}))| \leqslant |x_1|^{d-1}|x_2|^{d-2}\ldots|x_{d-1}|\prod_{j=1}^d\left(\sum_{i=1}^d|a_{ij}|^2\right)^{1/2}$$

(see [3]).

(2) Schinzel (see [**5**, p. 13]) proved that the Mahler measure of a totally positive algebraic integer α of degree d is at least $((1 + \sqrt{5})/2)^d$. Zaïmi [**18**] obtained a similar inequality

$$\mathcal{R}(\alpha) \geqslant \left(\frac{1 + \sqrt{5}}{2} \right)^{d/2} \tag{10.1}$$

for such α. It is easy to see that Schinzel's inequality combined with (1.6) also yields (10.1).

(3) *The graph G and the degree of a Salem half-norm.* We have seen that a Salem half-norm ψ defined by a Salem number of degree $2s$ has degree at most 2^s. Can ψ have a degree d which is not a power of 2? If so, the corresponding graph G would have d vertices, d not a power of 2. For this to happen it must be possible for two Salem half-norms defined by the same extended Salem number to have different degrees.

Which graphs G arise in this construction? Note that (taking the $d = 4$ case) every totally non-real quartic unit-norm α lies with its conjugates on two circles. One can readily show that here, if α is reciprocal, then $s = 2$ and G is a square, while if α is non-reciprocal then $s = 3$ and G is the complete 4-vertex graph K_4.

References

1. M.-J. Bertin, Sur une conjecture de Pohst, *Acta Arith.* **74** (1996), 347–349.
2. D. Boyd, Irreducible polynomials with many roots of equal modulus, *Acta Arith.* **68** (1994), 85–88.
3. A. Dubickas, On a conjecture of A. Schinzel and H. Zassenhaus, *Acta Arith.* **63** (1993), 15–20.
4. A. Dubickas, On the distribution of roots of polynomials in sectors. II, *Liet. Matem. Rink.* **38** (1998), 151–168.
5. G. Everest and T. Ward, *Heights of polynomials and entropy in dynamical systems* (Springer, 1999).
6. R. Ferguson, Irreducible polynomials with many roots of equal modulus, *Acta Arith.* **78** (1997), 221–225.
7. J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. Sci. Math.* (2) **17** (1893), 240–248.
8. G. H. Hardy, J. E. Littlewood and G. Polya, *Inequalities*, 2nd edn (Cambridge University Press, 1952).
9. W. Ljunggren, On the irreducibility of certain trinomials and quadrinomials, *Math. Scand.* **8** (1960), 65–70.
10. R. Remak, Über Grössenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers, *Compositio Math.* **10** (1952), 245–285.
11. R. M. Robinson, Conjugate algebraic integers on a circle, *Math. Z.* **110** (1969), 41–45.
12. R. Salem, *Algebraic numbers and Fourier analysis* (D. C. Heath and Co., Boston, MA, 1963).
13. C. L. Siegel, Algebraic integers whose conjugates lie in the unit circle, *Duke Math. J.* **11** (1944), 597–602.

14. C. J. SMYTH, On the product of the conjugates outside the unit circle of an algebraic integer, *Bull. Lond. Math. Soc.* **3** (1971), 169–175.
15. C. J. SMYTH, Conjugate algebraic numbers on conics, *Acta Arith.* **40** (1982), 333–346.
16. C. J. SMYTH, Additive and multiplicative relations connecting conjugate algebraic numbers, *J. Number Theory* **23** (1984), 243–254.
17. P. M. VOUTIER, An effective lower bound for the height of algebraic numbers, *Acta Arith.* **74** (1996), 81–95.
18. T. ZAÏMI, Minoration d'un produit pondéré des conjugués d'un entier algébrique totalement réel, *C. R. Acad. Sci. Paris, Sér. I Math.* **318** (1994), 1–4.