J. Austral. Math. Soc. (Series A) 30 (1980), 137–149

ON THE MEASURE OF TOTALLY REAL ALGEBRAIC INTEGERS

C. J. SMYTH

(Received 4 October 1979)

Communicated by A. J. van der Poorten

Abstract

For totally real algebraic integers α of degree $D(\alpha)$, we examine the stucture of the set of values $M(\alpha)^{1/D(\alpha)}$, where $M(\alpha)$ is the measure of α. We find a small limit point ℓ of this set, and show that the set is everywhere dense in (ℓ, ∞).

1980 Mathematics subject classification (Amer. Math. Soc.): 12 A 95.

1. Introduction

Let $\alpha \neq 0$ be an algebraic integer, not a root of unity, with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_{D(\alpha)}$. There has been much recent work on the product $M(\alpha) = \prod_{i=1}^{D(\alpha)} \max(1, |\alpha_i|)$ (see Boyd (1978), Mignotte (1978), Stewart (1978) and forthcoming papers of Dobrowolski, Lawton and Schinzel).

Here we shall be concerned with $M(\alpha)$ for α a totally real algebraic integer, $\alpha \neq 0$, ± 1. In this situation, a reformulation of a special case of a result of Schinzel (1973), Theorem 2, states that

$$M(\alpha) \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{1}{2}D(\alpha)},$$

with equality when $\alpha = \frac{1}{2}(1+\sqrt{5})$. It therefore seems reasonable to put $\Omega(\alpha) = M(\alpha)^{1/D(\alpha)}$ and look at the set

$$\mathscr{L} = \{\Omega(\alpha) \mid \alpha \text{ totally real}, \alpha \neq 0, \pm 1\}.$$

Then by Schinzel's result, $\mathscr{L}$ has smallest element $(\frac{1}{2}(1+\sqrt{5}))^{\frac{1}{2}} = 1.2720196\ldots$.

We shall prove the following results:

THEOREM 1. *Define* $\beta_0 = 1$ *and* $\beta_{n+1} > 0$ *by* $H\beta_{n+1} = \beta_n$ $(n = 0, 1, \ldots)$, *where*

$$Hx = x - x^{-1}. \tag{1.1}$$

Then β_n has degree 2^n over the rationals, and the sequence

$$\Omega(\beta_1), \Omega(\beta_2), \Omega(\beta_3), \Omega(\beta_4), \Omega(\beta_5), \ldots \approx 1.272, 1.298, 1.308, 1.312, 1.313, \ldots$$

of elements of $\mathscr{L}$ has limit point

$$\ell = \exp \int_1^\infty \log x \, dF(x) = 1.31427\ldots,$$

where $F(x)$ is the function defined by Theorem 3.

THEOREM 2. *The set $\mathscr{L}$ is everywhere dense in the interval (ℓ, ∞).*

THEOREM 3. *There is a unique strictly increasing function $F(x)$, defined on $[0, \infty]$ and satisfying $F(0) = 0$ and*

$$|2F(x) - 1| = F(|x - x^{-1}|)(x \geqslant 0). \tag{1.2}$$

The function $F(x)$ is in fact the limiting distribution, as $n \to \infty$, of the absolute values of the conjugates of β_n.

It would be interesting to determine the precise structure of $\mathscr{L}$ in $((\frac{1}{2}(1+\sqrt{5}))^{\frac{1}{2}}, \ell)$. It seems likely that the $\Omega(\beta_n)$ $(n = 1, 2, \ldots)$ form an increasing sequence lying entirely within this interval, though I have not been able to prove this. Apart from the $\Omega(\beta_n)$, there are other elements of $\mathscr{L}$ in this interval. They are connected with fixed points of iterates H^k of H. These are discussed in Section 6.

One might expect that the numbers $\Omega(\alpha_q)$, where

$$\alpha_q = 2\cos(2\pi/q) \tag{1.3}$$

could give small elements of $\mathscr{L}$. In fact, $\lim_{q\to\infty} \Omega(\alpha_q) = 1.38135\ldots > \ell$ (Lemma 11), and I know of no $\Omega(\alpha_q)$ on $((\frac{1}{2}(1+\sqrt{5}))^{\frac{1}{2}}, \ell)$ which is not also equal to $\Omega(\beta_n)$ for some n, or $\Omega(\beta')$ for some fixed point β' of H^k for some k (see Section 6 for details).

In Section 2 we calculate the degree of β_n. In Section 3 we prove Theorem 3, and derive some other properties of β_n and F. In Section 4 we complete the proof of Theorem 1, and in Section 5 we prove Theorem 2.

I would like to thank Professor J. W. S. Cassels for useful discussions concerning the degree of β_n.

https://doi.org/10.1017/S1446788700016426 Published online by Cambridge University Press

2. Degree of β_n

LEMMA 1 (Albert (1956), Theorem 22, p. 140). *Let p be a prime and $\gamma \in \mathrm{GF}(p^n)$ for some n. Then $x^p - x - \gamma$ is irreducible over $\mathrm{GF}(p^n)$ if and only if the trace $\mathrm{Tr}_{\mathrm{GF}(p^n)/\mathrm{GF}(p)}\gamma \neq 0$.*

LEMMA 2. *If $x \neq 0$ belongs to a field of characteristic* 2, and $\mu = x^{-1} + x$ *satisfies $\mu^{2\uparrow n} = \mu$ for some n, then $x^{2\uparrow n} = x$ or x^{-1}. Here $2 \uparrow n$ denotes 2^{2^n}.*

PROOF. Now $(x + x^{-1})^{2\uparrow n} = x^{2\uparrow n} + x^{-2\uparrow n} = \mu^{2\uparrow n} = \mu$. So $x^{2\uparrow n}$ is one of the roots of $x + x^{-1} = \mu$.

LEMMA 3. *In a suitable extenstion of $F_2 = \mathrm{GF}(2)$, define $\gamma_0 = 1$ and*

$$\gamma_{n+1} + \gamma_{n+1}^{-1} = \gamma_n \quad (n = 0, 1, 2, \ldots). \tag{2.1}$$

Then $[F_2(\gamma_n) : F_2] = 2n$.

PROOF. Assume for inductive purposes that $[F_2(\gamma_n) : F_2] = 2^n$, $\mathrm{Tr}_{F_2(\gamma_n)/F_2}\gamma_n = 1$ and $\gamma_n^{2\uparrow(n-1)} = \gamma_n^{-1}$. This is easily verified for $n = 1$. Then $(\gamma_{n+1}/\gamma_n)^2 + \gamma_{n+1}/\gamma_n = \gamma_n^{-2}$, and $\mathrm{Tr}\,\gamma_n^{-2} = \mathrm{Tr}\,\gamma_n$ as $\gamma_n^{-2} = \gamma_n^{2(2\uparrow(n-1))}$ and $\mathrm{Tr}\,\gamma_n = \sum_{j=1}^{2^n-1}\gamma_n^{2^j}$. So by Lemma 1, $\gamma_{n+1}/\gamma_n \notin F_2(\gamma_n)$, and hence $[F_2(\gamma_{n+1}) : F_2] = 2^{n+1}$. Since $\gamma_{n+1} \notin F_2(\gamma_n)$, $\gamma_{n+1}^{2\uparrow n} \neq \gamma_{n+1}$, so $\gamma_{n+1}^{2\uparrow n} = \gamma_{n+1}^{-1}$ by Lemma 2. Further, from (2.1)

$$\gamma_{n+1}^{2^k} + \gamma_{n+1}^{-2^k} = \gamma_n^{2^k} \quad (k = 0, 1, \ldots, 2^n - 1).$$

Since $(\gamma_{n+1}^{2^e})^2 = \gamma_{n+1}^{2\uparrow n} = \gamma_{n+1}^{-1}$, where $e = 2^n - 1$, it follows that

$$\mathrm{Tr}\,\gamma_{n+1} = \sum_{k=1}^{2^n-1}(\gamma_{n+1}^{2^k} + \gamma_{n+1}^{-2^k}) = \sum_{k=1}^{2^n-1}\gamma_n^{2^k} = 1,$$

by the induction hypothesis. This completes the induction.

We can now prove

LEMMA 4. *Let β_0 be an odd rational integer, and $H\beta_{n+1} = \beta_n$ $(n = 0, 1, \ldots)$. Then β_n* has degree 2^n *over the rationals Q.*

PROOF. We show that $Q_2(\beta_n)/Q_2$ is unramified of degree 2^n, where Q_2 is the field of 2-adic numbers. Assume inductively that $Q_2(\beta_n)$ has residue class field $F_2(\gamma_n)$, and that $\beta_n \equiv \gamma_n \pmod 2$ (clearly true for $n = 0$). Then if $f(x) = x^2 - \beta_n x + 1$, $f(\gamma_{n+1}) \equiv 0 \pmod 2$, and $f'(\gamma_{n+1}) \equiv \gamma_n\gamma_{n+1} \not\equiv 0 \pmod 2$. So by Hensel's Lemma, $f(x) = 0$ has a root β_{n+1} with $\beta_{n+1} \equiv \gamma_{n+1} \pmod 2$. Then $Q_2(\beta_{n+1})$ has residue class field $F_2(\gamma_n, \gamma_{n+1}) = F_2(\gamma_{n+1})$ of degree 2^{n+1} over F_2, by Lemma 3. Hence

https://doi.org/10.1017/S1446788700016426 Published online by Cambridge University Press

$$[Q_2(\beta_{n+1}):Q_2] \geqslant [F_2(\gamma_{n+1}):F_2] = 2^{n+1},$$

and $Q_2(\beta_{n+1})/Q_2$ is unramified of degree 2^{n+1}.

3. Proof of Theorem 3

Let B_n be the set of absolute values of conjugates of β_n ($n = 0, 1, \dots$). By Lemma 4, B_n has 2^n elements $\beta_n = \beta_{n,1} \geqslant \beta_{n,2} \geqslant \dots \geqslant \beta_{n,2^n}$ say. For $x \geqslant 0$, put $F_n(x) = 2^{-n} \times$ (number of $\beta_{n,j}$ in $[0, x]$). Clearly $F_n(0) = 0$. Since $-\beta_n^{-1}$ is a conjugate of β_n,

$$F_n(x) = \begin{cases} 1 - F_n(x^{-1}) & \text{if } x \neq \text{any } \beta_{n,j}, \\ 1 - F_n(x^{-1}) + 2^{-n} & \text{if } x = \text{some } \beta_{n,j}. \end{cases} \tag{3.1}$$

Also, for $x > 1$ there is a 1-1 correspondence between the $\beta_{n,j}$ in (x, ∞) and the $\beta_{n-1,j}$ in $(x - x^{-1}, \infty)$. So $2^n(1 - F_n(x)) = 2^{n-1}(1 - F_{n-1}(x - x^{-1}))$, or

$$F_n(x) = \tfrac{1}{2}(1 + F_{n-1}(x - x^{-1})), \quad x > 1. \tag{3.2}$$

Now take any $x \geqslant 0$. If $x \in \bigcup_{j=0}^n B_j$, replace x by $x' > x$: $F_n(x') = F_n(x)$, $F_{n-1}(x') = F_{n-1}(x)$ and $x' \notin \bigcup_{j=0}^n B_j$. So we can assume in what follows that $x \notin \bigcup_{j=0}^n B_j$, which implies by (3.1) that

$$F_j(x) + F_j(x^{-1}) = 1 \quad (j = 0, \dots, n). \tag{3.3}$$

From (3.2) and (3.3), for $y \notin B_j$, B_{j-1}, $y > 0$,

$$|F_j(y) - F_{j-1}(y)| = \tfrac{1}{2}|F_{j-1}(|y - y^{-1}|) - F_{j-2}(|y - y^{-1}|)|.$$

Since $y \notin \bigcup_{j=0}^n B_j$ implies $|y - y^{-1}| \notin \bigcup_{j=0}^n B_j$, we have by induction that

$$|F_n(x) - F_{n-1}(x)| = 2^{-(n-2)}|F_2(z) - F_1(z)| \leqslant 2^{-(n-2)} \quad \text{for some } z.$$

By the Weierstrass M-test, $F_n(x)$ tends uniformly in x to a limit function $F(x)$ say, as $|F(x) - F(x+\delta)| \leqslant 2^{-k} < \varepsilon$, from which continuity follows.

$$F(x) + F(x^{-1}) = 1 \tag{3.4}$$

$$F(x) = \tfrac{1}{2}(1 + F(x - x^{-1})), \quad x \geqslant 1 \tag{3.5}$$

and hence

$$F(x) = \tfrac{1}{2}(1 - F(x^{-1} - x)) = \tfrac{1}{2}F((x^{-1} - x)^{-1}) \quad (0 \leqslant x \leqslant 1). \tag{3.6}$$

Combining (3.5), (3.6) we can write them as (1.2). Conversely, under the assumption that F is strictly increasing, (1.2) easily implies (3.4), (3.5) and (3.6). We shall show in Lemma 8 that F is indeed strictly increasing.

We now show how to use (3.5) and (3.6) to obtain, for given x, the value of $F(x)$ to any specified degree of accuracy. Suppose we have obtained an equation of the form

(3.7) $$F(x) = a_k + \varepsilon_k 2^{-k} F(|H^k x|),$$

where a_k is a rational, $\varepsilon_k = \pm 1$ and $H^k x = H(H^{k-1} x)$. (We start with $k = 0$, $a_0 = 0$, $\varepsilon_0 = 1$, $H^0 x = x$.) Then, applying (3.5) or (3.6),

$$F(x) = a_k + \varepsilon_k 2^{-k}(\tfrac{1}{2} + \tfrac{1}{2}\varepsilon'_{k+1} F(|H^{k+1} x|)$$
$$= a_{k+1} + \varepsilon_{k+1} 2^{-(k+1)} F(|H^{k+1} x|) \quad \text{say.}$$

So we can get an equation of the form (3.7) for any k, and then $|F(x) - a_k| \leqslant 2^{-k}$. This shows also that F is uniquely defined by (3.5) and (3.6).

For later use, we need the following facts:

LEMMA 5. (a) *Define* $H^{-1} x = \frac{1}{2}(x + (x^2+4)^{\frac{1}{2}})$, *so that* $H(H^{-1} x) = x$ (*and also* $H((-H^{-1} x)^{-1}) = x$). *Then for* $x, y > 0$

$$|H^{-1} x - H^{-1} y| < |x - y|.$$

(b) *We have*

(3.8) $$B_{n-1} = H^{-1} B_n \cup (H^{-1} B_n)^{-1}$$

and for $n \geqslant 0$,

(3.9) $$\beta_{n+1,i} = H^{-1} \beta_{n,i} \quad , \beta_{n+1,i'} = (H^{-1} \beta_{n,i})^{-1} \quad (i = 1, \ldots, 2^n)$$

where $i' = 2^{n+1} + 1 - i$.

(c) $(n+1)^{\frac{1}{2}} \leqslant \beta_n \leqslant (2n+1)^{\frac{1}{2}}$ *for* $n \geqslant 0$.

(d) $\beta_n - \beta_{n,2} \geqslant \beta_{n-1}^{-1}$ *for* $n \geqslant 1$ (*recall* $\beta_n, \beta_{n,2}$ *are the largest two elements of* B_n).

(e) $\max_{j=1,\ldots,2^n-1} (\beta_{n,j} - \beta_{n,j+1}) = \beta_n - \beta_{n,2}$, *which is* $O(n^{-\frac{1}{2}})$.

PROOF. (a) Direct application of the mean value theorem.

(b) (3.8) follows from (1.1), and (3.9) from (3.8).

(c) First note that $\beta_{n+1} = H^{-1} \beta_n = \frac{1}{2}(\beta_n + (\beta_n^2+4)^{\frac{1}{2}}) > \beta_n + (1/(2\beta_n))$ as $\beta_n^2 + 4 > (\beta_n + \beta_n^{-1})^2$. Now assume $\beta_n \geqslant (n+1)^{\frac{1}{2}}$, which is true for $n = 0$. Then

$$\beta_{n-1}^2 > ((n+1)^{\frac{1}{2}} + \tfrac{1}{2}(n+1)^{\frac{1}{2}})^2 > n+2.$$

Next assume $\beta_n \leqslant (2n+1)^{\frac{1}{2}}$, also true for $n = 0$. Then

$$\beta_{n+1} \leqslant \tfrac{1}{2}((2n+1)^{\frac{1}{2}} + (2n+5)^{\frac{1}{2}}) \leqslant (2n+3)^{\frac{1}{2}}$$

by convexity.

(d) We must first show that for $n \geqslant 1$

(3.10) $$\beta_n - \beta_{n-1} \geqslant \beta_{n,2} - \beta_{n-2}$$

https://doi.org/10.1017/S1446788700016426 Published online by Cambridge University Press

(put $\beta_{-1} = 0$). This holds with equality for $n = 1$. Now, using (3.9),

$$\beta_n = H^{-(n-1)}(H^{-1}1), \quad \beta_{n-1} = H^{-(n-1)}1,$$

$\beta_{n,2} = H^{-(n-1)}((H^{-1}1)^{-1}), \quad \beta_{n-2} = H^{-(n-1)}0$ and $H^{-1}1 > 1 > (H^{-1}1)^{-1} > 0$

Further, $(d/dx)(H^{-1}x)$ is an increasing function of x, so using the mean value theorem we have that if $a > b > c > d$ and $a-b > c-d$, then $H^{-1}a - H^{-1}b > H^{-1}c - H^{-1}d$. Applying this result $n-1$ times, (3.10) follows. Then (d) follows from the fact that $\beta_{n-2} = \beta_{n-1} - \beta_{n-1}^{-1}$.

(e) Now $|x^{-1} - y^{-1}| < |x-y|$ for $x, y-1$. So, using (3.8), the greatest distance between adjacent elements of B_{n+1} must either occur between two elements of $H^{-1}B_n$, or between the smallest element $H^{-1}(\beta_n^{-1})$ of $H^{-1}B_n$ and the largest element $(H^{-1}(\beta_n^{-1}))^{-1}$ of $(H^{-1}B_n)^{-1}$. But

$$H^{-1}\beta_n^{-1} - (H^{-1}\beta_n^{-1})^{-1} = HH^{-1}\beta_n^{-1} = \beta_n^{-1} \leqslant \beta_{n+1} - \beta_{n+1,2}$$

by (d), so if the result is true for n it is also true for $n+1$. For the order of magnitude, first note that

$$H\beta_j - H\beta_{j,2} = (\beta_j - \beta_{j,2})\left(1 + \frac{1}{x^2}\right),$$

for some $x \in (\beta_{j,2}, \beta_j)$. Hence

$$\beta_{j-1} - \beta_{j-1,2} \geqslant (\beta_j - \beta_{j,2})\left(1 + \frac{1}{\beta_j^2}\right) \geqslant (\beta_j - \beta_{j,2})\left(\frac{2j+2}{2j+1}\right)$$

by (c). Hence by induction, for $n \geqslant 2$

$$\beta_n - \beta_{n,2} \leqslant \frac{2n+1}{2n+2} \cdot \frac{2n-1}{2n} \cdot \ldots \cdot \frac{5}{6},$$

as $\beta_1 - \beta_{1,2} = 1$. Since this product is $O(n^{-\frac{1}{2}})$, the result follows.

LEMMA 6. *F is continuous on* $(0, \infty)$.

PROOF. Given $x, \varepsilon > 0$, choose $k : 2^{-k} < \varepsilon$, and $\delta > 0$ such that for $j = 0, 1, \ldots, k-1$. $|H^j x|$ and $|H^j(x+\delta)|$ are not on opposite sides of 1 (one of them may equal 1). This is possible by the continuity of H on $R \cup \{\infty\}$ (with its usual topology). Then (3.7) holds for x and $x+\delta$, with the same values of a_k and ε_k. Hence $|F(x) - F(x+\delta)| \leqslant 2^{-k} < \varepsilon$ from which continuity follows.

LEMMA 7. *For* $j = 1, \ldots, 2^n$, $F(\beta_{n,j}) = 1 - (2j-1)/2^{n+1}$.

PROOF. If $F(|\beta|) = j'/2^{n+1}$, where j' is odd, then repeated use of (1.2) shows that $H^n(\pm\beta) = 1$. Hence by the definition of β_n, one of β or $-\beta$ is a conjugate of β_n. Since

https://doi.org/10.1017/S1446788700016426 Published online by Cambridge University Press

$F(x)$ is continuous, $F(0) = 0$, $F(\infty) = 1$, $F(x) = j'/2^{n+1}$ has a solution $x_{j'}$ say. So the 2^n odd values of j' in $[1, 2^{n+1} - 1]$ must correspond to the absolute values of the 2^n roots of $H^n x = 1$. The exact correspondence follows from the ordering of the $\beta_{n,j}$'s and the fact that F is non-decreasing.

Finally in this section we can show

LEMMA 8. *F is strictly increasing in* $(0, \infty)$.

PROOF. Let $0 < a < b$. Choose n large enough so that there are two elements $\beta_{n,j}$, $\beta_{n,j-1}$ of B_n in (a, b). This is possible by Lemma 5(c), (e). Then $F(a) \leqslant F(\beta_{n,j}) < F(\beta_{n,j-1}) \leqslant F(b)$.

The above result completes the proof of Theorem 2.

4. Proof of Theorem 1

LEMMA 9. *We have*

(a)

$$\int_1^\infty \log x \, dF(x) = \log \ell$$

for some ℓ with $1 < \ell < \infty$.

(b)

$$\lim_{n\to\infty} \int_1^\infty \log x \, dF_n(x) = \log \ell.$$

PROOF. (a)

$$\begin{aligned}\int_1^\infty \log x \, dF(x) &= \sum_{i=0}^\infty \int_{\beta_i}^{\beta_{i+1}} \log x \, dF(x) \\ &\leqslant \sum_{i=0}^\infty \log \beta_{i+1} \int_{\beta_i}^{\beta_{i+1}} dF(x) \\ &= \sum_{i=0}^\infty 2^{-(i+2)} \log \beta_{i+1} \leqslant \sum_{i=0}^\infty 2^{-(i+3)} \log(2i+3) < \infty.\end{aligned}$$

by Lemma 7 and Lemma 5(c).

(b) Given $\varepsilon > 0$, put $e = 2^n - 1$ and choose n:

$$\left| \int_1^{\beta_{n,e}} \log x \, dF(x) - 2^{-n} \log \beta_{n,e} \right| + \int_{\beta_n}^\infty \log x \, dF(x) < \frac{\varepsilon}{2}. \tag{4.1}$$

https://doi.org/10.1017/S1446788700016426 Published online by Cambridge University Press

Then

$$\left|\int_1^{\infty} \log x\, dF_n(x) - \int_1^{\infty} \log x\, dF(x)\right|$$
$$< \frac{\varepsilon}{2} + \left|\frac{1}{2^n}\sum_{i=1}^{2^{n-1}-1} \log \beta_{n,i} - \int_{\beta_{n,e}}^{\beta_n} \log x\, dF(x)\right|$$
$$\leqslant \frac{\varepsilon}{2} + \frac{1}{2^n}\sum_{i=1}^{2^{n-1}-1} \log(\beta_{n,i}/\beta_{n,i+1})$$

as F has weight 2^{-n} in each interval $(\beta_{n,i+1}, \beta_{n,i})$, by Lemma 7

$$= \frac{\varepsilon}{2} + 2^{-n}\log \beta_n < \varepsilon$$

for n sufficiently large, using 5(c) again.

This lemma, combined with Lemma 4, proves Theorem 1.

5. Proof of Theorem 2

We now generalize the sequence $\{\beta_n\}$ by setting $\beta_0^{(b)} = b$, where b is an odd positive integer, and $\beta_{n+1}^{(b)} > 0$ by $H\beta_{n+1}^{(b)} = \beta_n^{(b)}$ $(n = 0, 1, \ldots)$. By Lemma 4, $\beta_n^{(b)}$ has degree 2^n over Q. Also, let $B_n^{(b)}$ be the generalisation of the set B_n, $B_n^{(b)} = \{\beta_n^{(b)} = \beta_{n,1}^{(b)} \geqslant \beta_{n,2}^{(b)} \geqslant \beta_{n,3}^{(b)} \geqslant \ldots \geqslant \beta_{n,2^n}^{(b)}\}$.

The next lemma allows us to approximate most elements of $B_n^{(b)}$ by elements of some B_j.

LEMMA 10. *Apart from $\beta_n^{(b)}$ and $(\beta_n^{(b)})^{-1}$, the other $2^n - 2$ elements of $B_n^{(b)}$ can be arranged into disjoint pairs, so that there is a 1–1 correspondence between each pair $\beta_{n,i_1}^{(b)}, \beta_{n,i_2}^{(b)}$ and each element $\beta_{j,l}^{(1)}$ of $B_0 \cup B_1 \cup \ldots \cup B_{n-2}$, in such a way that $|\beta_{n,i_1}^{(b)} - \beta_{j,l}^{(1)}|$ and $|\beta_{n,i_2}^{(b)} - \beta_{j,l}^{(1)}|$ are less then b^{-1}.*

PROOF. The lemma is trivial for $n = 1$. Assume it is true for n. For $B_{n+1}^{(b)}$, let the pair $H^{-1}\beta_{n,i_1}^{(b)}$, $H^{-1}\beta_{n,i_2}^{(b)}$ correspond to $H^{-1}\beta_{j,l}^{(1)}$. Then

$$|H^{-1}\beta_{n,i_1}^{(b)} - H^{-1}\beta_{j,}^{(1)}| < |\beta_{n,i_1}^{(b)} - \beta_{j,l}^{(1)}| < b^{-1},$$

by Lemma 5(a). This defines the correspondence for all elements of $B_{n+1}^{(b)}$ except $(H^{-1}\beta_n^{(b)})^{\pm 1}$ and $(H^{-1}(\beta_n^{(b)})^{-1})^{\pm 1}$. The first two of these are $(\beta_{n+1}^{(b)})^{\pm 1}$, and so are excluded from the correspondence. Let the other two correspond to 1. Then

$$H^{-1}(\beta_n^{(b)})^{-1} - 1 = H^{-1}(\beta_n^{(b)})^{-1} - H^{-1}0 < (\beta_n^{(b)})^{-1} \leqslant (\beta_0^{(b)})^{-1} = b^{-1}$$

by Lemma 5(a). Since $|x^{-1}-1|<|x-1|$ for $x>1$, the relevant inequality also holds for $(H^{-1}(\beta_n^{(b)})^{-1})^{-1}$. We have therefore obtained the required correspondence between $B_{n+1}^{(b)}$ and

$$\{1\} \cup H^{-1}(B_0 \cup \ldots \cup B_{n-2}) \cup (H^{-1}(B_0 \cup B_1 \cup \ldots \cup B_{n-2}))^{-1}$$
$$= B_0 \cup B_1 \cup \ldots \cup B_{n-1}.$$

We can now prove Theorem 2.

Let $a > \ell$ and $\varepsilon > 0$ be given. We shall exhibit a $\beta_n^{(b)}$ with $|\log \ell_n^{(b)} - \log a| < \varepsilon$, where $\ell_n^{(b)} = \Omega(\beta_n^{(b)})$. We first observe that a straightforward generalization of Lemma 5(c) gives

$$(5.1) \qquad b \leqslant \beta_n^{(b)} \leqslant (2n+b^2)^{\frac{1}{2}}.$$

Also note that from Lemma 9(b) we may put

$$(5.2) \qquad \log \ell_j^{(1)} = (1-\varepsilon_j)\log \ell$$

where $\varepsilon_j \to 0$ as $j \to \infty$. Then by Lemma (10) and (5.1),

$$(5.3) \qquad \log \ell_n^{(b)} = \frac{1}{2^n}\sum_{i=1}^{2^n-1} \log \beta_{n,i}^{(b)}$$
$$\geqslant \frac{1}{2^n}\left\{\log b + 2\sum_{j=0}^{n-2}\sum_{i=1}^{2^j-1} \log|\beta_{j,i}^{(1)} - b^{-1}|\right\}$$
$$\geqslant 2^{-n}\log b + 2\sum_{j=0}^{n-2} 2^{-(n-j)}\log \ell_j^{(1)} + 2\sum_{j=0}^{n-2} 2^{-(n-j)}\log(1-b^{-1})$$
$$\geqslant 2^{-n}\log b + (1-2^{-(n-1)})\log \ell - T_n - \log(1-b^{-1})^{-1},$$

where

$$T_n = 2\sum_{j=0}^{n-2} 2^{-(n-j)}|\varepsilon_j|\log \ell.$$

Similarly, in the other direction

$$(5.4) \qquad \log \ell_n^{(b)} \leqslant 2^{-n}\log b + n2^{-n}b^{-2} + \log \ell + T_n + \log(1+b^{-1}).$$

Now choose N_1 large enough so that

$$n2^{-n} + 2^{-(n-1)}\log \ell + T_n < \frac{\varepsilon}{3} \quad \text{for } n \geqslant N_1.$$

https://doi.org/10.1017/S1446788700016426 Published online by Cambridge University Press

We also want

$$|2^{-n}\log b-\log(a/\ell)|<\frac{\varepsilon}{3},$$

or

$$b\in\left(\left(\frac{a}{\ell}\exp\left(\frac{-\varepsilon}{3}\right)\right)^{2^n},\ \left(\frac{a}{\ell}\exp\left(\frac{\varepsilon}{3}\right)\right)^{2^n}\right).$$

Choose $N_2 \geqslant N_1$ such that this interval contains an odd integer for $n \geqslant N_2$. Finally choose $N_3 \geqslant N_2$ so that $\max(\log(1-b^{-1})^{-1}), \log(1+b^{-1})) < \varepsilon/3$ for $n \geqslant N_3$. The three $\varepsilon/3$-inequalities now combine with (5.3) and (5.4) to give the required result.

6. Small elements of $\mathscr{L}$

We define a small element of $\mathscr{L}$ to be one in $[1,\ell]$. We now show that for α_q defined by (1.3), $\Omega(\alpha_q)$ can only be small for finitely many q.

LEMMA 11. *We have*

$$\lim_{q\to\infty}\Omega(\alpha_q)=\exp\frac{1}{2\pi}\int_0^{2\pi}\log_+|1-e^{i\theta}|\,d\theta=1.38135\ldots.$$

PROOF. Now

$$\log\Omega(\alpha_q)=(\tfrac{1}{2}\phi(q))^{-1}\sum_{\substack{i=1\\(i,q)=1}}^{[q/2]}\log_+|2\cos(2\pi i/q)|$$

$$\to\frac{1}{2\pi}\int_0^{2\pi}\log_+|1-e^{i\theta}|\,d\theta\quad\text{as } q\to\infty,$$

since the discrepancy, on the unit circle, of the primitive qth roots of 1 tends to 0 as $q\to\infty$. This fact follows, for instance, from Kuipers and Niederreiter (1974), Chapter 2, Theorem 2.5, and Hardy and Wright (1960), Theorem 272.

Now $\Omega(\alpha_5)=\Omega(\beta_1)$ is small, and $\Omega(\alpha_7)=1.309784\ldots$ and $\Omega(\alpha_{60})=1.311254\ldots$ are also small. We shall show, however, that these numbers also belong to a sequence of elements of $\mathscr{L}$ connected with fixed points of H^k for some k. We need

LEMMA 12. *For* $k=1,2,\ldots, H^k x=P_k(x^2)/xQ_k(x^2)$, *where* $P_1(y)=y-1$, $Q_1(y)=1$ *and*

(6.1) $$P_{k+1}(y)=P_k^2(y)-yQ_k^2(y)\quad(k=1,2,\ldots),$$

(6.2) $$Q_{k+1}(y) = P_k(y)Q_k(y) = \prod_{j=1}^{k} P_k(y),$$

(6.3) $$P_k(y) = y^{2^{k-1}} - (2^k - 1)\, y^{2^{k-1}-1} + \dots + 1 \quad (k \geqslant 2),$$

(6.4) $$Q_k(y) = y^{2^{k-1}-1} - (2^k - k - 1)\, y^{2^{k-1}-2} + \dots - 1 \quad (k \geqslant 2),$$

(6.5) $$R_k^+(y) = -P_k(y) + yQ_k(y) = k y^{2^{k-1}-1} - \dots - 1,$$

(6.6) $$R_k^-(y) = P_k(y) + yQ_k(y) = 2y^{2^{k-1}} - \dots + 1.$$

Further, P_k is the minimal polynomial of β_{k-1}^2.

PROOF. Equation (6.1)–(6.6) all follow by induction, using the fact that

$$H^{k+1}x = H(H^k x) = \frac{P_k(x^2)}{xQ_k(x^2)} - \frac{xQ_k(x^2)}{P_k(x^2)}.$$

The final remark follows from the fact that $H\beta_j = \beta_{j-1}$, $H^k \beta_{k-1} = 0$ and $H^k(-\beta_{k-1}) = 0$.

Note that for $\varepsilon = \pm$, the roots of $H^k x = \varepsilon x$ are the zeros of $R_\mu^\varepsilon(x^2)$.

We now establish a connection between the fixed points of H^k and the values of x where $F(x)$ is rational.

LEMMA 13. (a) *The values of x where $F(x) = j/(2^k - 1)$ ($j = 1, 2, \dots, 2^k - 2$) are the positive roots of $H^k x = x$ and of $H^k x^{-1} = x^{-1}$.*

(b) *The values of x where $F(x) = j/(2^k + 1)$ ($j = 1, 2, \dots, 2^k$) are the positive roots of $H^k x = -x$ and of $H^k x^{-1} = -x^{-1}$.*

PROOF. From (6.5), $H^k x = x$ and $H^k x^{-1} = x^{-1}$ each have $2^{k-1} - 1$ positive roots, a total of $2k - 2$. Let $F(x) = j/2^k - 1$, where $j \in \{1, 2, \dots, 2^k - 2\}$. From (1.2), $F(\varepsilon H x) = \operatorname{res}(2j\varepsilon)/2^k - 1$, where

$$\varepsilon = \begin{cases} 1 & \text{if } x > 1 \\ -1 & \text{if } x < 1 \end{cases}$$

and

$$\operatorname{res}(a) \equiv a (\operatorname{mod} 2^k - 1), \quad \operatorname{res}(a) \in \{1, 2, \dots, 2^k - 2\}.$$

Hence, as $H(\varepsilon H^i x) = \varepsilon H^{i+1} x$, we can show by induction that for $\varepsilon' = \operatorname{sgn}(H^k x - 1)$,

$$F(\varepsilon' H^k x) = \frac{\operatorname{res}(2^k j\varepsilon')}{2^k - 1}.$$

Since $\operatorname{res}(2^k j) = j$, $\operatorname{res}(-2^k j) = 2^k - 1 - j$, and $\varepsilon' H^k x = H^k x^{\varepsilon'}$, $F(H^k x^{\varepsilon'}) = F(x^{\varepsilon'})$.

Part (b) follows similarly.

We now note that $H^k x = \pm x$ implies $H^{2k} x = x$, and $Hx = -x$ implies $H^{2k+1} x = -x$. Hence, from Lemma 12, $R^+_{2k}(y) = 2ky^{2^{2k-1}-1} - \dots - 1$ is divisible by $R^+_k(y)R^-_k(y) = 2ky^{2^{k}-1} - \dots - 1$, and $R^-_1(y) = 2y - 1$ divides $R^-_{2k+1}(y) = 2y^{2^{2k}} - \dots + 1$. Therefore, by defining

$$S_{2k}(y) = \frac{R^+_{2k}(y)}{R^+_k(y)R^-_k(y)}, \quad S_{2k+1}(y) = \frac{R^-_{2k+1}(y)}{2y-1},$$

we obtain an infinite sequence of monic integral polynomials with constant term ± 1. Note that S_{2k} has degree $2^{2k-1} - 2^k$, and S_{2k+1} degree $2^{2k} - 1$. The S_i need not be irreducible, as, for example, $S_3 \mid S_9$. However, we can use the Möbius μ-function to define, in a manner analogous to the formulae for irreducible cyclotomic polymials,

$$S^*_{2k}(y) = \prod_{j \mid k} S_{2j}(y)^{\mu(k/j)}, \quad S^*_{2k+1}(y) = \prod_{j \mid 2k+1} S_j(y)^{\mu((2k+1)/j)}.$$

It is then possible that the S^*_i may be irreducible. We have

$$S^*_1 = S^*_2 = 1, \quad S^*_3(y) = y^3 - 5y^2 + 6y - 1, \quad S^*_4(y) = y^4 - 7y^3 + 14y^2 - 8y + 1,$$
$$S^*_5(y) = y^{15} - 28y^{14} + 339y^{13} \dots - 1, \quad \text{etc.}$$

It is easily checked that $S^*_3(y)$, $S^*_4(y)$ are the minimal polynomials of α_7^2, α_{60}^2. Thus α_7, α_{60} arise naturally as roots of $H^3 x = -x$, and $H^4 x = x$, respectively.

Assuming that S^*_{2k} is irreducible, with γ_{2k} a zero, then the absolute values of the conjugates of $\gamma_{2k}^{\frac{1}{2}}$ are the values of x where $F(x) = j/(2^{2k} - 1)$, where

$$\frac{j}{2^k - 1} \neq \frac{j'}{2^{k'} - 1} \quad \text{for any } k' < 2k.$$

Under the (likely) further assumption that these special values of $j/(2^{2k} - 1)$ have small discrepancy in $[0, 1]$, then

$$\frac{1}{2\deg(\gamma_{2k})} \sum_{\substack{\gamma \text{ conjugate} \\ \text{of } \gamma_{2k}}} \log_+ |\gamma|$$

will be near

$$\int_1^x \log x \, dF(x),$$

i.e. $\Omega(\gamma_{2k}^{\frac{1}{2}})$ will be near ℓ. This will be true whether $\deg \gamma_{2k}^{\frac{1}{2}} = 2 \deg \gamma_{2k}$ or $\deg \gamma_{2k}$.

References

A. A. Albert (1965), *Fundamental concepts of higher algebra* (University of Chicago Press).

D. W. Boyd (1978), 'Variations on a theme of Kronecker', *Canad. Math. Bull.* **21** (2), 129–133.

E. Dobrowolski (1979), 'On a question of Lehmer and the number of irreducible factors of a polynomial', *Acta Arith.* **34**, 391–401.

G. M. Hardy and E. M. Wright (1960), *An introduction to the theory of numbers*, 4th ed. (Oxford).

L. Kuipers and H. Niederreiter (1974), *Uniform distribution of sequences* (Wiley).

M. Mignotte (1978), 'Entiers algébriques dont les conjugués sont proches du cercle unité, *Séminaire Delange-Pisot-Poitou* (*Théorie des nombres*), 19e année, No. 39.

A. Schinzel (1973), 'On the product of the conjugates outside the unit circle of an algebraic number', *Acta Arith.* **24**, 385–399.

C. L. Stewart (1978), 'Algebraic integers whose conjugates lie near the unit circle', *Bull. Soc. Math. France* **106**, 169–176.

Department of Mathematics
James Cook University
Townsville, Queensland
Australia 4811