ACTA ARITHMETICA
XVIII (1971)

Algebraic integers near the unit circle

by

P. E. Blanksby (Columbus, Ohio)* and
H. L. Montgomery (Cambridge, England)

Dedicated to the memory of Professor H. Davenport

§ 1. Introduction. In this paper we investigate questions of D. H. Lehmer and of Schinzel and Zassenhaus concerning algebraic integers near the unit circle. Throughout α will denote an algebraic integer of degree $n > 1$ over the rationals, with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$. We write $n = r + 2s$, where r is the number of real conjugates of α and s is the number of pairs of complex conjugates of α. As is customary, we set

$$|\alpha| = \max_{1 \leqslant j \leqslant n} |\alpha_j|.$$

It is clear that for any algebraic integer $|\alpha| \geqslant 1$. In 1857 Kronecker [4] showed that $|\alpha| = 1$ if and only if α is a root of unity. In 1933 Lehmer [5] asked whether there is a constant $c > 0$ such that if

$$\prod_{j=1}^{n} \max(1, |\alpha_j|) \leqslant 1 + c \tag{1}$$

then α is a root of unity; more recently Schinzel and Zassenhaus [8] have asked whether there is a constant $c' > 0$ such that if

$$|\alpha| \leqslant 1 + \frac{c'}{n} \tag{2}$$

then α is a root of unity. It is obvious that an affirmative answer to the former question would imply an affirmative answer to the latter, and the results would be the best of their sort, as we see from the example $\alpha = 2^{1/n}$. Towards a solution of these problems we prove

* Work supported in part by an 1851 Overseas Scholarship.

THEOREM 1. *Let α be an algebraic integer of degree $n > 1$ over the rationals, with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$. If*

$$\prod_{j=1}^{n} \max(1, |\alpha_j|) \leqslant 1 + \frac{1}{52 n \log 6n} \tag{3}$$

then α is a root of unity (see the note at the end of this paper).

COROLLARY. *If α is an algebraic integer of degree $n > 1$ and if*

$$|\overline{\alpha}| \leqslant 1 + \frac{1}{30 n^2 \log 6n} \tag{4}$$

then α is a root of unity.

The first strengthening of Kronecker's theorem is due to Ore [6], whose condition on $|\overline{\alpha}|$ depends not only on n but also on the field generated by α over the rationals. Rather weaker versions of the Corollary have been given previously, in which the condition

$$|\overline{\alpha}| \leqslant 1 + \frac{c}{A^n} \tag{5}$$

stood in place of (4). Schinzel and Zassenhaus [8] gave this with $A = 2$, Blanksby [1] obtained $A = 2^{1/2} + \varepsilon$, and Schinzel (unpublished) improved this to $A = 2^{1/2}$.

Our method would enable us to replace (4) by

$$|\overline{\alpha}| \leqslant 1 + \frac{c}{(s+1)^2 \log(s+2)}, \tag{6}$$

which is a weaker hypothesis. But the result is not really stronger, for Schinzel (unpublished) has shown that if

$$|\overline{\alpha}| \leqslant 1 + \frac{1}{8s+3} \tag{7}$$

then $s \geqslant n/3$, and so $s \asymp n$. In fact we can show that if (6) holds then α has no real conjugates (i.e. $n = 2s$). More precisely, we have

THEOREM 2. *If α is an algebraic integer of degree $n > 1$ with*

$$|\overline{\alpha}| \leqslant 1 + \frac{\log(s+2)}{16(s+2)^2}, \tag{8}$$

then $n = 2s$.

Kronecker used his theorem, mentioned above, to prove that if α is a totally real algebraic integer for which $|\overline{\alpha}| \leqslant 2$ then α is twice the real part of a root of unity, $\alpha = 2\cos 2\pi \frac{a}{b}$. If we follow his argument we find we can replace the interval $[-2, 2]$ by an ellipse containing it: If α and all its conjugates lie in the ellipse

$$\frac{u^2}{(\lambda + \lambda^{-1})^2} + \frac{v^2}{(\lambda - \lambda^{-1})^2} \leqslant 1,$$

where λ is the number on the right hand side of (4), with n replaced by $2n$, then α is twice the real part of a root of unity. In the case of a totally real α this allows us to replace Kronecker's condition $|\overline{\alpha}| \leqslant 2$ by the weaker condition $|\overline{\alpha}| \leqslant 2 + cn^{-4}(\log n)^{-2}$. However, in this special case we can obtain a stronger result, as follows.

THEOREM 3. *Let α be a totally real algebraic integer of degree $n > 1$. If*

$$|\overline{\alpha}| \leqslant 2 + \frac{1}{300(n \log n)^2} \tag{9}$$

then α is twice the real part of a root of unity; $\alpha = 2\cos 2\pi \frac{a}{b}$.

In the opposite direction R. M. Robinson [7] has given examples of totally real algebraic integers α with $2 < |\overline{\alpha}| < 2 + \varepsilon$.

In the proof of each theorem our first step is to reduce the problem at hand to one of simultaneous Diophantine approximation. We then treat the latter problem, using ideas found in a paper of Cassels [2]. To further illustrate the power and flexibility of this analytic method, in § 6 we use the method to prove Dirichlet's theorem on Diophantine approximation. Dirichlet's theorem was used in obtaining the previous results in which (5) was the hypothesis.

We take pleasure in thanking Professor Cassels for his suggestions and advice. We are especially grateful to him for pointing out certain improvements which led to a weakening of the hypothesis in the Corollary from $|\overline{\alpha}| \leqslant 1 + cn^{-3}(\log n)^{-2}$ to $|\overline{\alpha}| \leqslant 1 + cn^{-2}(\log n)^2$. We also thank Professor Schinzel for making his unpublished work available to us.

§ 2. Basic lemmas. The fundamental principle in our analytic approach to Diophantine approximation is stated in the following lemma; it generalizes a result of Cassels [2].

LEMMA 1. *Let $f(x_1, x_2, \ldots, x_N) = f(\boldsymbol{x})$ be a continuous real valued function of the real vector $\boldsymbol{x}$, with periods 1, and Fourier expansion*

$$f(\boldsymbol{x}) \sim \sum_{\boldsymbol{m}} a(\boldsymbol{m}) e(\boldsymbol{m} \cdot \boldsymbol{x}), \tag{10}$$

where the summation is extended over all points $\boldsymbol{m}$ *of the integral lattice, and* $\boldsymbol{m}\cdot\boldsymbol{x} = m_1x_1+m_2x_2+\ldots+m_Nx_N$. *Suppose that* $a(\boldsymbol{m}) = a(-\boldsymbol{m}) \geqslant 0$ *for all* $\boldsymbol{m}$. *Then for any positive integer* K *and any* $\boldsymbol{\theta}$

$$\sum_{k=1}^{K}\left(1-\frac{k}{K+1}\right)f(k\boldsymbol{\theta}) \geqslant \frac{K+1}{2}a(\boldsymbol{0})-\frac{1}{2}f(\boldsymbol{0}), \tag{11}$$

and

$$\sum_{k=1}^{K}\left(1-\frac{k}{K+1}\right)|f(k\boldsymbol{\theta})|^2 \geqslant \frac{K+1}{2}\left(\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m})^2\right)-f(\boldsymbol{0})\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m}), \tag{12}$$

where $\mathscr{S}$ *is any set of lattice points for which* $\boldsymbol{m}\in\mathscr{S}$ *if and only if* $-\boldsymbol{m}\in\mathscr{S}$.

Proof. We first show that the expansion (10) converges absolutely uniformly to $f(\boldsymbol{x})$. By Fejér's theorem (see [11], p. 304) the expansion (10) sums $(C,1)$ to $f(\boldsymbol{x})$:

$$f(\boldsymbol{x}) = \lim_{M\to\infty}\sum_{\boldsymbol{m}}a(\boldsymbol{m})e(\boldsymbol{m}\cdot\boldsymbol{x})\prod_{j=1}^{N}\max(0,1-|m_j|M^{-1}).$$

Taking $\boldsymbol{x}=\boldsymbol{0}$ we have

$$\sum_{\boldsymbol{m}}|a(\boldsymbol{m})| = \lim_{M\to\infty}\sum_{\boldsymbol{m}}|a(\boldsymbol{m})|\prod_{j=1}^{N}\max(1,1-|m_j|M^{-1}) = f(\boldsymbol{0}) < \infty,$$

because the $a(\boldsymbol{m})$ are non-negative. Thus the series (10) converges absolutely uniformly. Since its value must agree with its $(C,1)$ sum, its value is $f(\boldsymbol{x})$.

Let

$$T_K(\theta) = \sum_{k=1}^{K}\left(1-\frac{k}{K+1}\right)\cos 2\pi k\theta.$$

By comparison with Fejér's kernel, we see that $T_K(\theta) \geqslant -\frac{1}{2}$ for all positive integers K and all real θ. As $a(\boldsymbol{m}) = a(-\boldsymbol{m}) \geqslant 0$ for all $\boldsymbol{m}$, the left hand side of (11) is

$$= \sum_{\boldsymbol{m}}a(\boldsymbol{m})T_K(\boldsymbol{m}\cdot\boldsymbol{\theta}) \geqslant a(\boldsymbol{0})T_K(0)-\tfrac{1}{2}\sum_{\boldsymbol{m}\neq\boldsymbol{0}}a(\boldsymbol{m}) = \frac{K+1}{2}a(\boldsymbol{0})-\tfrac{1}{2}f(\boldsymbol{0}),$$

so (11) is proved.

Let

$$T_K(\theta,\psi) = \sum_{k=1}^{K}\left(1-\frac{k}{K+1}\right)(\cos 2\pi k\theta)(\cos 2\pi k\psi).$$

From the identity $\cos u\cos v = \frac{1}{2}\cos(u+v)+\frac{1}{2}\cos(u-v)$ we see that

$$T_K(\theta,\psi) = \tfrac{1}{2}T_K(\theta+\psi)+\tfrac{1}{2}T_K(\theta-\psi).$$

Thus

$$T_K(\theta,\psi) \geqslant -\tfrac{1}{2}, \quad \text{and} \quad T_K(\theta,\pm\theta) = \tfrac{1}{2}T_K(0)+\tfrac{1}{2}T_K(2\theta) \geqslant (K-1)/4.$$

Now

$$\begin{aligned}|f(\boldsymbol{x})|^2 &= \Big(\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m})e(\boldsymbol{m}\cdot\boldsymbol{x})+\sum_{\boldsymbol{m}\notin\mathscr{S}}a(\boldsymbol{m})e(\boldsymbol{m}\cdot\boldsymbol{x})\Big)^2\\ &\geqslant \Big(\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m})e(\boldsymbol{m}\cdot\boldsymbol{x})\Big)^2+2\Big(\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m})e(\boldsymbol{m}\cdot\boldsymbol{x})\Big)\Big(\sum_{\boldsymbol{m}\notin\mathscr{S}}a(\boldsymbol{m})e(\boldsymbol{m}\cdot\boldsymbol{x})\Big),\end{aligned}$$

so the left hand side of (12) is

$$\begin{aligned}&\geqslant \sum_{\boldsymbol{m}_1\in\mathscr{S}}\sum_{\boldsymbol{m}_2\in\mathscr{S}}a(\boldsymbol{m}_1)a(\boldsymbol{m}_2)T_K(\boldsymbol{m}_1\cdot\boldsymbol{\theta},\boldsymbol{m}_2\cdot\boldsymbol{\theta})+\\ &\qquad+2\sum_{\boldsymbol{m}_1\in\mathscr{S}}\sum_{\boldsymbol{m}_2\notin\mathscr{S}}a(\boldsymbol{m}_1)a(\boldsymbol{m}_2)T_K(\boldsymbol{m}_1\cdot\boldsymbol{\theta},\boldsymbol{m}_2\cdot\boldsymbol{\theta})\\ &\geqslant \frac{K-1}{4}\sum_{\substack{\boldsymbol{m}_1=\pm\boldsymbol{m}_2\\ \boldsymbol{m}_1\in\mathscr{S}}}a(\boldsymbol{m}_1)a(\boldsymbol{m}_2)-\tfrac{1}{2}\sum_{\substack{\boldsymbol{m}_1\neq\pm\boldsymbol{m}_2\\ \boldsymbol{m}_1,\boldsymbol{m}_2\in\mathscr{S}}}a(\boldsymbol{m}_1)a(\boldsymbol{m}_2)-\\ &\qquad-\sum_{\boldsymbol{m}_1\in\mathscr{S}}\sum_{\boldsymbol{m}_2\notin\mathscr{S}}a(\boldsymbol{m}_1)a(\boldsymbol{m}_2)\\ &= \frac{K+1}{2}\Big(\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m})^2\Big)-\tfrac{1}{2}\Big(\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m})\Big)^2-\Big(\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m})\Big)\Big(\sum_{\boldsymbol{m}\notin\mathscr{S}}a(\boldsymbol{m})\Big)\\ &\geqslant \frac{K+1}{2}\Big(\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m})^2\Big)-\Big(\sum_{\boldsymbol{m}\in\mathscr{S}}a(\boldsymbol{m})\Big)\Big(\sum_{\boldsymbol{m}}a(\boldsymbol{m})\Big),\end{aligned}$$

and this last expression is the right hand side of (12).

Note that a change of $a(\boldsymbol{0})$ in (11) alters both sides by the same amount, so that as far as (11) is concerned, the hypothesis $a(\boldsymbol{0}) \geqslant 0$ is superfluous. If in (12) we take $\mathscr{S}$ to be the set of all lattice points then (12) follows from (11), on replacing $f(\boldsymbol{x})$ by $|f(\boldsymbol{x})|^2$. However, the point $\boldsymbol{m}$ contributes a positive quantity to the right hand side of (12) only if

$$a(\boldsymbol{m}) > 2f(\boldsymbol{0})(K+1)^{-1}.$$

Thus we obtain a sharper inequality by restricting $\mathscr{S}$ somewhat.

We now introduce some of the notation that arises in the proofs of our theorems. Let ϱ, ϱ', ϱ_j, θ_j be real numbers for which

$$0 \leqslant \varrho \leqslant \varrho_j \leqslant \varrho' < 1 \quad (1 \leqslant j \leqslant N). \tag{13}$$

We put

$$R = (1-\varrho')^{-1}, \tag{14}$$

and set

$$\sigma_k = \sum_{j=1}^{N} \log|\varrho_j e(k\theta_j) - 1|. \tag{15}$$

We obtain the following lemma as an application of Lemma 1.

LEMMA 2. *If* (13), (14), *and* (15) *hold, then*

$$\sum_{k=1}^{K}\left(1-\frac{k}{K+1}\right)\sigma_k \leqslant \frac{N}{2}\log R. \tag{16}$$

If we write $K = [BN\log R]$, *where* B *is a positive real number, then*

$$\sum_{k=1}^{K}\left(1-\frac{k}{K+1}\right)(\sigma_k)^2 \geqslant (N^2\log R)(\tfrac{1}{4}B\varrho^2-1). \tag{17}$$

Proof. We take

$$f(\boldsymbol{x}) = -\sum_{j=1}^{N}\log|\varrho_j e(kx_j)-1| = \tfrac{1}{2}\sum_{j=1}^{N}\sum_{m=1}^{\infty} m^{-1}\varrho_j^m\big(e(mx_j)+e(-mx_j)\big)$$

in Lemma 1. Thus $f(k\boldsymbol{\theta}) = -\sigma_k$, and (11) gives (16), since $a(\mathbf{0}) = 0$ and

$$f(\mathbf{0}) = \sum_{j=1}^{N}\log(1-\varrho_j)^{-1} \leqslant N\log R.$$

We take $\mathscr{S}$ to be the set of those $\boldsymbol{m} = (m_1, m_2, \ldots, m_N)$ for which $m_j = \pm 1$ for some j, and $m_k = 0$ for $k \neq j$. Then (12) gives

$$\sum_{k=1}^{K}\left(1-\frac{k}{K+1}\right)(\sigma_k)^2 \geqslant \frac{K+1}{4}\sum_{j=1}^{N}\varrho_j^2 - N\log R\sum_{j=1}^{N}\varrho_j \geqslant (N^2\log R)(\tfrac{1}{4}B\varrho^2-1),$$

which is (17).

Let us suppose that $\varrho > 0$ and that A is the positive real number for which

$$\varrho = \exp(-A^{-1}). \tag{18}$$

Inequalities (16) and (17) enable us to show that if A and B are sufficiently large then there are values of k for which $\sigma_k < 0$. More precisely we have

LEMMA 3. *In the notation of* (13), (14), (15), *and* (18), *if* $A \geqslant 8$ *and* $B \geqslant 8$ *then*

$$\min_{1\leqslant k\leqslant K}\sigma_k \leqslant -c_1 + c_2A^{-1} + c_3B^{-1}, \tag{19}$$

where we may take $c_1 = (2\log 2)^{-1}$, $c_2 = (\log 2)^{-1}$, *and* $c_3 = 1+2(\log 2)^{-1}$.

Proof. Let M denote the left hand side of (19), so that $\sigma_k - M \geqslant 0$ for $1 \leqslant k \leqslant K$. We have

$$\sum_{k=1}^{K}\left(1-\frac{k}{K+1}\right)(\sigma_k)^2 = \sum_{k=1}^{K}\left(1-\frac{k}{K+1}\right)\big((\sigma_k-M)^2+2M(\sigma_k-M)+M^2\big).$$

Now $\sigma_k \leqslant N\log 2$ for any k, so the above is

$$\begin{aligned}&\leqslant (N\log 2+M)(\tfrac{1}{2}N\log R - \tfrac{1}{2}KM) + \tfrac{1}{2}M^2K\\ &= \tfrac{1}{2}N\big((\log 2)N\log R - M(K\log 2-\log R)\big).\end{aligned}$$

We take this with (17). The right hand side of (17) is

$$\geqslant (N^2\log R)\big(\tfrac{1}{4}B(1-2A^{-1})-1\big),$$

so we have in all

$$M(K\log 2-\log R) \leqslant \big(\log 2+2-\tfrac{1}{2}B(1-2A^{-1})\big)N\log R.$$

Now for $A \geqslant 8, B \geqslant 8$ the right hand side is negative and $K\log 2 - \log R > 0$, so $M < 0$ and hence

$$M(K\log 2-\log R) \geqslant MBN(\log R)(\log 2).$$

Thus

$$M \leqslant B^{-1}(\log 2)^{-1}\big(\log 2+2-\tfrac{1}{2}B(1-2A^{-1})\big),$$

which is (19).

We require the following lemma for technical reasons.

LEMMA 4. *If* $0 < \varrho \leqslant 1$ *and* $\varrho \leqslant |z| \leqslant \varrho^{-1}$, *then*

$$|z-1| \leqslant \varrho^{-1}\left|\varrho\frac{z}{|z|}-1\right|. \tag{20}$$

Proof. If $1 \leqslant |z| \leqslant \varrho^{-1}$ then

$$|z-1| \leqslant \left|\varrho^{-1}\frac{z}{|z|}-1\right| = \varrho^{-1}\left|\varrho\frac{z}{|z|}-1\right|. \tag{21}$$

If $\varrho \leqslant |z| \leqslant 1$ then $|z-1| = |z|\,|z^{-1}-1|$, so (21) applies, and

$$|z-1| \leqslant |z|\varrho^{-1}\left|\varrho\frac{z}{|z|}-1\right| \leqslant \varrho^{-1}\left|\varrho\frac{z}{|z|}-1\right|.$$

The following is a result of Cassels [3]; we state it here for convenience.

LEMMA 5 (Cassels). *Let α be an algebraic integer of degree $n > 1$ over the rationals. If*

$$\overline{|\alpha|} \leqslant 1 + \frac{1}{10n} \tag{22}$$

then α^{-1} is a conjugate of α.

Recently C. J. Smyth strengthened this result; he replaced the condition (22) by the weaker hypothesis

$$\prod_{j=1}^{n} \max(1, |\alpha_j|) \leqslant \tfrac{1}{2}\sqrt{5}. \tag{23}$$

§ 3. Proof of Theorem 1. To prove that α is a root of unity it suffices to show that there is a positive integer k for which

$$\prod_{j=1}^{n} (\alpha_j^k - 1) = 0.$$

The product is a rational integer (since it is symmetric in the α_j), so to prove our result it suffices to show that there is a k for which

$$\prod_{j=1}^{n} |\alpha_j^k - 1| < 1. \tag{24}$$

We observe that $\overline{|\alpha|}$ does not exceed the left hand side of (3), so from (3) we have (22). Hence we may write

$$\begin{aligned} &n = 2N, \quad \alpha_{j+N} = \alpha_j^{-1}, \\ &\alpha_j = z_j e(\theta_j), \quad 0 < z_j \leqslant 1, \end{aligned} \qquad (1 \leqslant j \leqslant N). \tag{25}$$

We suppose that $1 \leqslant k \leqslant K$, and for $1 \leqslant j \leqslant N$ we put

$$\varrho_j = \begin{cases} \varrho' & \text{if} \quad \varrho' \leqslant z_j^K \leqslant 1, \\ z_j^K & \text{if} \quad z_j^K < \varrho'; \end{cases} \tag{26}$$

we choose $\varrho' < 1$ later. From Lemma 4 we see that

$$\prod_{j=1}^{n} |\alpha_j^k - 1| \leqslant \prod_{j=1}^{N} \varrho_j^{-2} |\varrho_j e(k\theta_j) - 1|^2$$

for $1 \leqslant k \leqslant K$. Let σ_k be as in (15). Then to satisfy (24) it suffices to show that

$$\sigma_k < \log \prod_{j=1}^{N} \varrho_j$$

for some k, $1 \leqslant k \leqslant K$. We now assume that

$$\prod_{j=1}^{N} z_j^{-1} \leqslant \exp\bigl((AK)^{-1}\bigr), \tag{27}$$

and we take

$$\varrho' = \exp\bigl(-(AN)^{-1}\bigr),$$

where $A > 0$ will be chosen below. From (26) we see that

$$\prod_{j=1}^{N} \varrho_j \geqslant \prod_{j=1}^{N} z_j^K \varrho' \geqslant \exp(-2A^{-1}).$$

Hence to complete our proof it suffices to show that

$$\sigma_k < -2A^{-1} \tag{28}$$

for some k in the range $1 \leqslant k \leqslant K$.

We have now reduced the proof of Theorem 1 to a problem of Diophantine approximation, in which we require the $\|k\theta_j\|$ to be small in the sense that (28) holds. We wish to know how large to take K so as to be assured that (28) holds for some positive k not exceeding K. Previously Dirichlet's theorem was used in this connection; we now see that it was wasteful for the purpose. Lemma 1 has allowed us to treat the σ_k directly, in Lemma 2. The inequalities (16) and (17) assert that on average σ_k is small and $(\sigma_k)^2$ is large. (The right hand side of (16) depends only on N, while the right hand side of (17) increases with K.) This can be the case only if there is some cancellation in (16), which is to say that σ_k is sometimes negative. We have formulated a precise result in Lemma 3.

The number z_j^{-1} does not exceed the left hand side of (27), so from (26) we see that our ϱ_j satisfy (13) with ϱ as in (18). Thus we are in a position to quote Lemma 3. We see that (28) holds if

$$(2 + 4\log 2)A^{-1} + (4 + 2\log 2)B^{-1} < 1.$$

But $\log 2 < 0.7$, so the above holds if we take $A = 9.6 > 4 + 8\log 2$ and $B = 10.8 > 8 + 4\log 2$. The left hand sides of (3) and (27) are equal, so (3) implies (27), as $1 + \delta \leqslant e^{\delta}$ and

$$AK \leqslant ABN \log R \leqslant 104N \log 12N = 52n \log 6n.$$

To deduce the Corollary we note that (4) implies (22), so that the left hand side of (3) is no larger than $\overline{|\alpha|}^{n/2}$. But $1 + \delta \leqslant e^{\delta}$ and $e^{\delta'} \leqslant 1 + \delta'(1-\Delta)^{-1}$ for $0 \leqslant \delta' \leqslant \Delta < 1$, so

$$\left(1 + \frac{1}{30n^2 \log 6n}\right)^{n/2} < 1 + \frac{1}{52n \log 6n}$$

for $n \geqslant 2$, and the Corollary follows.

§ 4. Proof of Theorem 2. We first establish

LEMMA 6. *Let α be an algebraic integer of degree $n > 1$. If $|\overline{\alpha}| \leqslant 13/12$ then $s > n/4$.*

Proof. Following the unpublished work of Schinzel, we consider the product

$$\prod_{j=1}^{n} \alpha_j^2(1-\alpha_j^2).$$

This product is a non-zero rational integer, since it is symmetric in the α_j. Now $|z^2(1-z^2)| \leqslant |z|^2(1+|z|^2) < 4$ for $|z| \leqslant 13/12$, and $z^2|1-z^2| \leqslant 1/4$ for real z satisfying $-13/12 \leqslant z \leqslant 13/12$. Thus

$$1 \leqslant \prod_{j=1}^{n} |\alpha_j|^2|1-\alpha_j^2| < 4^{-r}4^{2s},$$

so $2s > r$, and hence $s > n/4$.

Our hypothesis (8) makes Lemma 6 applicable, so (8) implies that $|\overline{\alpha}| \leqslant 1+(4en)^{-1}$, in view of the inequality $\log u \leqslant e^{-1}u$. Hence Lemma 5 applies. We employ the notation (25), and suppose that α_j, $\alpha_{j+N} = \alpha_j^{-1}$ are real for $1 \leqslant j \leqslant t$, where $r = 2t$, $t \geqslant 0$. We consider the product

$$\prod_{j=1}^{n} (\alpha_j^{2k}-1), \tag{29}$$

which is an integer. If the product vanishes then α is a root of unity and $n = 2s$; hence we assume that the product is non-zero. Now $|\alpha_j^{\pm 2k}-1| \leqslant |\overline{\alpha}|^{2K}-1$ for $1 \leqslant j \leqslant t$, $1 \leqslant k \leqslant K$. For the $2N-2t = 2s$ remaining values of j we use Lemma 4 with $\varrho = |\overline{\alpha}|^{-2K}$. We see that

$$1 \leqslant \prod_{j=1}^{n} |\alpha_j^{2k}-1| \leqslant \bigl((|\overline{\alpha}|^{2K}-1)^t \varrho^{-s} \prod_{j=1}^{N} |\varrho e(2k\theta_j)-1|\bigr)^2. \tag{30}$$

We now appeal to Lemma 2. From (16) we see that there is a $k \leqslant K$ for which

$$\sum_{j=t+1}^{N} \log|\varrho e(2k\theta_j)-1| \leqslant K^{-1}s\log R. \tag{31}$$

Here R is given by (14) with $\varrho = \varrho'$, so $R = (1-|\overline{\alpha}|^{-2K})^{-1}$. We take $K = 2s$; from (30) and (31) we see that

$$\begin{aligned} 0 &\leqslant t\log(|\overline{\alpha}|^{4s}-1)+4s^2\log|\overline{\alpha}|-\tfrac{1}{2}\log(1-|\overline{\alpha}|^{-4s}) \\ &= (t-\tfrac{1}{2})\log(|\overline{\alpha}|^{4s}-1)+2s(2s+1)\log|\overline{\alpha}|. \end{aligned} \tag{32}$$

Now if (8) holds then

$$|\alpha|^{4s} < \exp\bigl((4s+8)^{-1}\log(s+2)\bigr).$$

We have $e^{\delta} \leqslant 1+\delta(1-\Delta)^{-1}$ for $0 \leqslant \delta \leqslant \Delta < 1$, so the above is

$$\begin{aligned} &< 1+\tfrac{1}{3}(s+2)^{-1}\log(s+2) \\ &= 1+(s+2)^{-1}\log(s+2)^{1/3}. \end{aligned}$$

But $\log u < u$, so the above is

$$< 1+(s+2)^{-2/3},$$

and hence

$$\log(|\overline{\alpha}|^{4s}-1) < -\tfrac{2}{3}\log(s+2). \tag{33}$$

From (8) and the relation $\log(1+\delta) \leqslant \delta$ we also have

$$2s(2s+1)\log|\overline{\alpha}| < \tfrac{1}{4}\log(s+2). \tag{34}$$

If $t \geqslant 1$ then from (32), (33), and (34) we see that

$$0 \leqslant -\tfrac{2}{3}(t-\tfrac{1}{2})+\tfrac{1}{4}.$$

As this is false for $t \geqslant 1$ we must have $t = 0$, so $n = 2s$.

We note that the hypothesis in Lemma 6 is much weaker than the one in Schinzel's result (7), while the conclusions drawn are much the same. From the stronger hypothesis (7) one might obtain a sharper result; by modifying the above proof we could show that if $|\overline{\alpha}| \leqslant 1+(40s+1)^{-1}$ then $s > \frac{1}{2}n-cn^{1/2}(\log n)^{-1/2}$.

§ 5. Proof of Theorem 3. We suppose that α is a totally real algebraic integer of degree $n > 1$ with conjugates $\alpha_1, \alpha_2, \ldots, \alpha_n$ and minimal polynomial $p(x)$. Now the polynomial $q(x) = x^n p(x+x^{-1})$ has roots β_j, β_j^{-1}, $1 \leqslant j \leqslant n$, where

$$\alpha_j = \beta_j+\beta_j^{-1}. \tag{35}$$

We consider the product

$$\prod_{j=1}^{n} (\beta_j^{2k}-1)(\beta_j^{-2k}-1),$$

which is a rational integer. If this product is zero then some β_j is a root of unity, so $q(x)$ is irreducible and some α_j is twice the real part of a root of unity; hence they all are. Thus it suffices to find a $k \neq 0$ for which

$$\prod_{j=1}^{n} |\beta_j^{2k}-1|\,|\beta_j^{-2k}-1| < 1.$$

If $|\alpha_j| \leqslant 2$ then β_j and β_j^{-1} lie on the unit circle, while if $|\alpha_j| > 2$ then β_j and β_j^{-1} are real, and we may suppose that $|\beta_j| > 1 > |\beta_j|^{-1}$. We choose t so that $|\alpha_j| > 2$ for $1 \leqslant j \leqslant t$ and $|\alpha_j| \leqslant 2$ for $t+1 \leqslant j \leqslant n$. We may assume that $t > 0$, for if $t = 0$ then $|\beta_1| = 1$ so β_1 is a root of unity and we are finished. If $\alpha = \beta + \beta^{-1}$ and $\alpha = 2+\delta$ then $\beta \leqslant 1 + \delta^{1/2} + \delta$ for $0 \leqslant \delta \leqslant 1$, so from our hypothesis (9) we have

$$\beta_j < 1 + \frac{1}{17n\log n} + \frac{1}{300(n\log n)^2} < 1 + \frac{1}{16n\log n}.$$

We put $\varrho = 1 - 1/n$ and apply Lemma 4 to the terms $t+1 \leqslant j \leqslant n$ to obtain

$$(36)\qquad 1 \leqslant \prod_{j=1}^{n} |\beta_j^{2k} - 1|\,|\beta_j^{-2k} - 1|$$

$$\leqslant \left(\left(1 + \frac{1}{16n\log n}\right)^{2K} - 1\right)^{2t} \left(1 - \frac{1}{n}\right)^{-2(n-t)} \prod_{j=t+1}^{n} |\varrho e(2k\theta_j) - 1|^2$$

for $1 \leqslant k \leqslant K$. From (16) we see that we may choose $k \leqslant K$ so that

$$\sum_{j=t+1}^{n} \log|\varrho e(2k\theta_j) - 1| \leqslant K^{-1}(n-t)\log n.$$

We take $K = [n\log n]$. From (36) we see that if $t \geqslant 1$ then

$$0 \leqslant t\log(e^{1/8} - 1) + 1 + 1 < -(2.01)t + 2.$$

As this is false for $t \geqslant 1$ we must have $t = 0$, so the theorem is proved.

§ 6. Dirichlet's theorem. We now use (11) of Lemma 1 to derive Dirichlet's theorem. Let $\boldsymbol{\theta}$ and $\boldsymbol{\eta}$ be given, where $0 < \eta_j \leqslant \frac{1}{2}$ for $1 \leqslant j \leqslant N$. Take

$$f(\boldsymbol{x}) = \prod_{j=1}^{N} \max(0, 1 - \eta_j^{-1}\|x_j\|).$$

Now for $0 < \eta \leqslant \frac{1}{2}$ we have

$$\max(0, 1 - \eta^{-1}\|x\|) = \eta + \sum_{\substack{m=-\infty \\ m\neq 0}}^{+\infty} a_m e(mx),$$

where $a_m = \pi^{-2}\eta^{-1}m^{-2}(\sin\pi m\eta)^2$ for $m \neq 0$. Thus $f(\boldsymbol{x})$ satisfies the hypotheses of Lemma 1 with $a(\mathbf{0}) = \prod_{j=1}^{N} \eta_j$ and $f(\mathbf{0}) = 1$. From (11) we see that if $(K+1)\prod \eta_j > 1$ then there is a $k \leqslant K$ for which $f(k\boldsymbol{\theta}) > 0$. That is there is a $k \leqslant K$ for which

$$\|k\theta_j\| \leqslant \eta_j \qquad (1 \leqslant j \leqslant N),$$

provided $0 < \eta_j \leqslant \frac{1}{2}$ and

$$K+1 \geqslant \prod_{j=1}^{N} \eta_j^{-1}.$$

Previously Cassels [2] used similar ideas to obtain a somewhat weaker result.

To obtain a result of greater generality, let $\mathscr{R}$ be a closed N-dimensional convex region, symmetric about the origin, with Jordan content V, and such that $2\mathscr{R}$ contains no non-zero point of the integral lattice. We may construct a function $f(\boldsymbol{x})$ which vanishes outside $\mathscr{R}$ (modulo the N-dimensional unit cube), and which satisfies the conditions of Lemma 1 with $a(\mathbf{0}) = V^2 2^{-2N}$ and $f(\mathbf{0}) = V 2^{-N}$. It follows that there is a value of $k \leqslant K$ such that $k\boldsymbol{\theta} - \boldsymbol{m} \in \mathscr{R}$ for some lattice point $\boldsymbol{m}$, provided that $K+1 \geqslant 2^N V^{-1}$.

We construct $f(\boldsymbol{x})$ as follows. Let $g(\boldsymbol{x})$ be the characteristic function of $\frac{1}{2}\mathscr{R}$, and set

$$h(\boldsymbol{x}) = \sum_{\boldsymbol{m}} g(\boldsymbol{x}+\boldsymbol{m}),$$

$$h(\boldsymbol{x}) \sim \sum_{\boldsymbol{m}} b(\boldsymbol{m})\, e(\boldsymbol{m}\cdot\boldsymbol{x}).$$

Finally, take $f(\boldsymbol{x}) = \int h(\boldsymbol{t})h(\boldsymbol{x}-\boldsymbol{t})\,d\boldsymbol{t}$, where the integration runs over an N-dimensional unit cube. From our hypotheses concerning $\mathscr{R}$ we see that $f(\boldsymbol{x})$ is continuous, $a(\boldsymbol{m}) = |b(\boldsymbol{m})|^2$, $a(\boldsymbol{m}) = a(-\boldsymbol{m})$, $a(\mathbf{0}) = V^2 2^{-2N}$, and $f(\mathbf{0}) = V 2^{-N}$.

The above construction is due to Siegel [9]; he also showed that if $\mathscr{R}$ is an ellipsoid and if one stipulates further that the $a(\boldsymbol{m})$ be smooth in a certain sense, then this construction gives the f for which $a(\mathbf{0})/f(\mathbf{0})$ is maximum.

Of course the results of this section can be obtained by simple counting arguments; the advantage of Lemma 1 is that it leads to sharp results in situations in which the elementary methods seem inappropriate. We remark that Lemma 1 may be considered to lie within the sphere of Turán's method; Turán [10] has expressed a wish for a proof of Dirichlet's theorem such as the one above.

Note. In an earlier draft of this paper we proved only the Corollary with (4) replaced by

$$(37)\qquad |\alpha| \leqslant 1 + \frac{1}{40n^2\log n}.$$

Schinzel (*Reducibility of lacunary polynomials I*, Acta Arith. 16 (1969), p. 127) has used (37) in showing that

$$(*) \qquad e(\alpha, \Omega) \leqslant 20\,|\Omega|^{2}\log|\Omega|^{*}\log\|F\|.$$

As (4) implies (37) only for large n, it is important that Schinzel has found that (*) can be derived from our Theorem 1 as follows: If $\alpha = \zeta_q \beta^e$, $\beta \in Q(\alpha)$, then

$$\log \prod_{|\alpha_i|>1} |\alpha_i| = e \log \prod_{|\beta_i|>1} |\beta_i|,$$

and by Theorem 1 the right hand side is

$$(**) \qquad \geqslant \frac{e}{52\,|Q(\alpha)|\log 6\,|Q(\alpha)|^{*}}.$$

But by a known result (see M. Marden, *Geometry of Polynomials*, Providence 1966, p. 129) the left hand side does not exceed $\frac{1}{2}\log\|F\|$, where F is monic and $F(\alpha) = 0$. Hence

$$e\big(\alpha, Q(\alpha)\big) \leqslant 26\,|Q(\alpha)|\log 6\,|Q(\alpha)|^{*}\log\|F\|.$$

By the second part of Schinzel's Lemma 1

$$e(\alpha, \Omega) \leqslant 26\,|\Omega|\log 6\,|\Omega|^{*}\log\|F\|$$

which implies (*) for $|\Omega| > 3$. For $|\Omega| = 2$ or $|\Omega| = 3$ we use instead of (**) the bound

$$e\log\frac{1+\sqrt{5}}{2} \quad \text{or} \quad e\log\vartheta$$

respectively, where ϑ is the least Pisot–Vijayaraghavan number (> 1.3).

References

[1] P. E. Blanksby, *A note on algebraic integers*, J. Number Theory 1 (1969), pp. 155–160.

[2] J. W. S. Cassels, *On the sums of powers of complex numbers*, Acta Math. Hung. 7 (1957), pp. 283–289.

[3] — *On a problem of Schinzel and Zassenhaus*, J. Math. Sci. 1 (1966), pp. 1–8.

[4] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. 53 (1857), pp. 173–175.

[5] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. (2) 34 (1933), pp. 461–479.

[6] O. Ore, *Les corps algébriques et la théorie des idéaux*, Paris 1934.

[7] R. M. Robinson, *Intervals containing infinitely many sets of conjugate algebraic integers*, Studies in mathematical analysis and related topics, Stanford 1962, pp. 305–315.

[8] A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Mich. Math. J. 12 (1965), pp. 81–84.

[9] C. L. Siegel, *Über Gitterpunkte in convexen Körpern und ein damit zusammenhängendes Extremalproblem*, Acta Math. 65 (1935), pp. 307–323.

[10] P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest 1953.

[11] A. Zygmund, *Trigonometric Series*, second edition, Cambridge 1959.

OHIO STATE UNIVERSITY
Columbus, Ohio

TRINITY COLLEGE,
Cambridge, U. K.

Received on 26. 3. 1970