ACTA ARITHMETICA
XXIV (1973)

On the product of the conjugates outside the unit circle of an algebraic number

by

A. Schinzel (Warszawa)

To Professor Carl Ludwig Siegel

C. J. Smyth [7] has recently proved the following theorem.

If $P(x) \neq x$ is a monic non reciprocal irreducible polynomial with integral coefficients, then

$$\prod_{|\alpha_j|>1} |\alpha_j| \geqslant \theta_0,$$

where α_j are the zeros of $P(x)$ and θ_0 is the real root of the equation $\theta^3 = \theta + 1$.
(A polynomial P of degree $|P|$ is called *reciprocal* if $x^{|P|}P(x^{-1}) = \pm P(x)$.)

This theorem is a far reaching generalization of Siegel's theorem [6] about the least Pisot–Vijayaraghvan number being θ_0. On the other hand, it has interesting applications to the arithmetic of polynomials. The aim of this paper is to prove two extensions of Smyth's result to polynomials with coefficients in an algebraic number field and to apply one of them to reducibility questions. For a given polynomial F we denote by $|F|$ its degree, by $C(F)$ its content and by $\|F\|$ the sum of squares of the absolute values of the coefficients. Q denotes the rational field and $N_{K/Q}$ the norm from a number field K to Q. ζ_m is a primitive mth root of unity.

Theorem 1. *Let K be a totally real algebraic number field, P a monic non-reciprocal polynomial with coefficients integers in K and $P(0) \neq 0$. Then*

$$\max_{i=1,\ldots,|K|} \prod_{|\alpha_{ij}|>1} |\alpha_{ij}| \geqslant \theta_0, \tag{1}$$

where $|K|$ is the degree of K, $P^{(i)}$ $(i = 1, \ldots, |K|)$ the polynomials conjugate to $P(z)$ and α_{ij} the zeros of $P^{(i)}(z)$.

Theorem 2. *Let K be a totally real algebraic number field or a totally complex quadratic extension of such a field and $P \in K[z]$ a polynomial with the leading coefficient p_0 such that $z^{|P|}\overline{P}(z^{-1}) \neq \text{const}P(z)$, $P(0) \neq 0$.*

Then in the notation of Theorem 1

$$(2)\qquad \prod_{i=1}^{|K|}\prod_{|a_{ij}|>1}|a_{ij}| \geqslant \begin{cases} \left(\frac{1+\sqrt{5}}{2}\right)^{|K|/2}\left(N_{K/Q}\frac{C(P)}{(p_0)}\right)^{1/2+1/\sqrt{5}}\left(N_{K/Q}\frac{(P(0))}{C(P)}\right)^{1/2-1/\sqrt{5}} \\ \qquad\qquad \text{if } |P(0)| \neq |p_0|, \\ \left(\frac{1+\sqrt{17}}{4}\right)^{|K|}\left(N_{K/Q}\frac{C(P)}{(p_0)}\right)^{1/\sqrt{17}} \\ \quad \text{if } |P(0)| = |p_0| \text{ and } (\overline{P(0)})C(P) = (p_0)C(\overline{P}), \\ \left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2}\left(N_{K/Q}\frac{C(P)}{(p_0)}\right)^{1/\sqrt{17}} \\ \qquad\qquad \text{if } |P(0)| = |p_0|, \text{ and } P \text{ is irreducible,} \end{cases}$$

where the equality can hold only if $\sqrt{5}\in K$, $C(P) = (p_0)$ *and* $|P(0)/p_0| = (\pm 1+\sqrt{5})/2$. (The bar denotes the complex conjugation.)

Corollary 1. *If* $z^P\overline{P}(z^{-1}) \neq \text{const}P(z), P(0) \neq 0$ *then*

$$\prod_{i=1}^{|K|}\prod_{|a_{ij}|>1}|a_{ij}| > \left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2} N_{K/Q}\frac{C(P)}{(p_0)}.$$

It seems likely that the equality in (2) holds if and only if $P(z)/p_0$ is a product of cyclotomic factors and of a binomial $z^j - \frac{1\pm\sqrt{5}}{2}\zeta_i$. (This has just been proved by A. Bazylewicz.) It is also conjectured that in Corollary 1 $(1+\sqrt{17})/4$ can be replaced by $(1+\sqrt{5})/2$ provided the equality is allowed.

Theorem 3. *Let* K *satisfy the assumptions of Theorem* 2, L *be a subfield of* K, $f(z)\in L[z]$ *and* f_0 *be the leading coefficient of* f. *The number* n *of irreducible factors* P *of* f *such that* $z^{|P|}\overline{P}(z^{-1}) \neq \text{const}P(z), P(0)\neq 0$ *counted with their multiplicities satisfies the inequality*

$$(3_1)\qquad n < \frac{\log\left|N_{L/Q}\|f\|N_{L/Q}^{-2}C(f)\right|}{|L|\log\frac{1+\sqrt{17}}{4}}.$$

If all prime ideal factors $\mathfrak{p}$ *of* $(f_0, f(0))C(f)^{-1}$ *in* K *satisfy* $\overline{\mathfrak{p}} = \mathfrak{p}$ *then the following stronger inequality holds*

$$(3_2)\qquad \left(\frac{1+\sqrt{5}}{2}\right)^{n|L|} + \left(\frac{1+\sqrt{5}}{2}\right)^{-n|L|} \leqslant N_{L/Q}\|f\|N_{L/Q}^{-2}C(f)$$

with the equality attained if and only if either $L = Q$, $f(z) = c(z^{|f|}\pm 1)$ *or* $K\supset Q(\sqrt{5}, \zeta_m)$, $L = Q$

$$(4)\qquad z^{|f|}f(z)f\left(\frac{1}{z}\right) = c\left(z^{4lm} - \left[\left(\frac{1+\sqrt{5}}{2}\right)^{2m} + \left(\frac{1-\sqrt{5}}{2}\right)^{2m}\right]z^{2lm} + 1\right)$$

l, m integers, m odd.

Corollary 2. *If* K *satisfies the assumptions of Theorem* 2 *then*

$$\varphi(x) = x^p + \varepsilon x^q + \eta \qquad (\varepsilon = \pm 1, \eta = \pm 1)$$

divided by its largest cyclotomic factor is irreducible in K *except when* $\sqrt{5}\in K$ *and*

$$\varphi(x) = x^{2q} \pm x^q - 1 = \left(x^q \pm \frac{1+\sqrt{5}}{2}\right)\left(x^q \pm \frac{1-\sqrt{5}}{2}\right).$$

The constant $(1+\sqrt{17})/4$ occurring in the first assertion of Theorem 3 can probably be replaced by $(1+\sqrt{5})/2$. Further improvement is impossible since for every pair l, m (m odd) there exists a polynomial $f(z)$ satisfying (4) namely

$$f(z) = z^{2lm} \pm \left[\left(\frac{1+\sqrt{5}}{2}\right)^m + \left(\frac{1-\sqrt{5}}{2}\right)^m\right]z^{lm} - 1.$$

(There are also other instances of such polynomials, e.g. for $l = 1$, $m = 3$

$$f(z) = z^6 - 2z^5 + 2z^4 - 2z^2 - 2z - 1.)$$

The major problem is to find an estimate analogous to that given in Theorem 3 for the number of all non-cyclotomic factors of f.

Corollary 2 for $K = Q$ has been proved by W. Ljunggren [4] and H. Tverberg [8] by different methods and by Smyth on the same lines two years ago (in a letter to the writer).

Proofs are based on two lemmata both essentially due to Smyth.

Lemma 1. *Let* $f(z) = \sum_{i=0}^{\infty} e_i z^i$ *be holomorphic in an open disc containing* $|z|\leqslant 1$, *and satisfy* $|f(z)|\leqslant 1$ *on* $|z| = 1$. *Then*

$$(5)\qquad |e_i| \leqslant 1 - |e_0|^2 \qquad (i = 1, 2, \ldots)$$

and if e_i *are real* $(i = 0, 1, \ldots)$, $e_0 \neq 0$, *then*

$$(6)\qquad -\left(1 - e_0^2 - \frac{e_i^2}{1+e_0}\right) \leqslant e_{2i} \leqslant 1 - e_0^2 - \frac{e_i^2}{1-e_0} \qquad (i = 1, 2, \ldots).$$

Proof. To prove (5) we exclude the trivial case $e_0 = 0$, apply Parseval's Formula to $f(z)(\beta + z^i)$ and obtain

$$|e_0\beta|^2 + |e_1\beta|^2 + \ldots + |e_{i-1}\beta|^2 + |e_0 + e_i\beta|^2 + \ldots$$

$$= \frac{1}{2\pi}\int_0^{2\pi} |\beta + z^i|^2\, d\varphi \qquad (z = e^{i\varphi})$$

$$\leqslant \frac{1}{2\pi}\int_0^{2\pi} |\beta + z^i|^2\, d\varphi = |\beta|^2 + 1.$$

So

$$|e_0\beta|^2 + |e_0 + e_i\beta|^2 \leqslant 1 + |\beta|^2.$$

Putting $\beta = |e_i|/\bar{e}_0 e_i$ (this choice of β was suggested by Dr. H. Iwaniec; Smyth considered only real e_i) we get

$$\left| e_0 + \frac{|e_i|}{\bar{e}_0} \right| \leqslant |e_0|^{-1}$$

and hence (5) holds. The proof of (6) is given by Smyth [7], p. 170.

Lemma 2. *If $P(z)$ is a polynomial with the leading coefficient p_0, $|P(0)| = |p_0|$, $Q(z) = z^{|P|}\overline{P}(z^{-1}) \neq \mathrm{const} P(z)$ then*

$$\frac{P(0)P(z)}{p_0 Q(z)} = \frac{f(z)}{g(z)}$$

where $f(z)$ and $g(z)$ are holomorphic in an open disc containing $|z| \leqslant 1$, have absolute value 1 on $|z| = 1$ and $f(0) = g(0) = \pm \prod_{|a_j|>1} a_j^{-1}$ where a_j runs over the zeros of P.

Moreover if $P(z)$ has real coefficients then the Taylor coefficients of f and g are also real, $f(0) = g(0)$ is positive.

Proof. We set

$$f(z) = \pm \prod_{|a_j|=1}(-a_j) \prod_{|a_j|<1}\left(\frac{z - a_j}{1 - \bar{a}_j z}\right), \qquad g(z) = \pm P(0) \prod_{|a_j|>1}\left(\frac{1 - \bar{a}_j z}{z - a_j}\right)$$

and verify directly all the statements of the lemma, but the last one. To see the latter notice that for P with real coefficients the sequence $\{\bar{a}_j\}$ is a permutation of $\{a_j\}$, hence

$$\overline{f(z)} = f(\bar{z}), \qquad \overline{g(z)} = g(\bar{z});$$

$f(0) > 0$ can be achieved by a suitable choice of the sign $\pm$.

Proof of Theorem 1 follows closely Smyth's proof of his own theorem. We set

$$\Lambda = \max_{i=1,2,\ldots,n} \prod_{|a_{ij}|>1} |a_{ij}|,$$

and denote the zeros of P by a_j. Since $\sqrt{2} > \theta_0$ we are entitled to assume that $\Lambda < \sqrt{2}$. First of all we must have $P(0) = \pm 1$ for otherwise by a theorem of Kronecker [3] about the conjugates of a totally real algebraic integer

$$\Lambda \geqslant \overline{|P(0)|} \geqslant \sqrt{2}$$

($\overline{|a|}$ denotes the maximum absolute value of the conjugates of a). Secondly $P(z)/Q(z)$ is non-constant. Accordingly, put

$$\frac{P(0)P(z)}{Q(z)} = 1 + a_k z^k + a_l z^l + \ldots \tag{7}$$

where k, l are the first two indices for which the corresponding a's are non zero. Since a_k, a_l are totally real algebraic integers we have by the theorem of Kronecker $\overline{|a_l|} \geqslant 1$ and either $\overline{|a_k|} \geqslant \sqrt{2}$ or $a_k = \pm 1$. If $\overline{|a_k|} \geqslant \sqrt{2}$ we may assume that $|a_k| \geqslant \sqrt{2}$, otherwise if $|a_k^{(i)}| \geqslant \sqrt{2}$ we replace $P(z)$ by $P^{(i)}(z)$, which does not affect the value of Λ.

Now by Lemma 2

$$\frac{P(0)P(z)}{Q(z)} = \frac{f(z)}{g(z)} = \frac{c + c_1 z + c_2 z^2 + \ldots}{d + d_1 z + d_2 z^2 + \ldots} \tag{8}$$

where $f(z) = c + c_1 z + c_2 z^2 + \ldots$, $g(z) = d + d_1 z + d_2 z^2 + \ldots$ are functions holomorphic in an open disc containing $|z| \leqslant 1$, have real coefficients and

$$|f(z)| = |g(z)| = 1 \quad \text{for} \quad |z| = 1, \tag{9}$$

$$c = d = \prod_{|a_j|>1} |a_j|^{-1}. \tag{10}$$

On comparing the series in (5) and (6) we obtain

$$c_i = d_i \quad (i = 1, 2, \ldots, k-1);$$

$$\begin{cases} a_k c + d_k = c_k, \\ a_k d_i + d_{k+i} = c_{k+i} \quad (i = 1, 2, \ldots, l-k-1); \end{cases} \tag{11}$$

$$a_l c + a_k d_{l-k} + d_l = c_l. \tag{12}$$

Now if $|a_k| \geqslant \sqrt{2}$, $\max(|c_k|, |d_k|) \geqslant c/\sqrt{2}$ by (11) and so from (5), $c/\sqrt{2} \leqslant 1 - c^2$. This gives by (10) $\Lambda \geqslant c^{-1} \geqslant \sqrt{2}$ a contradiction. Therefore

$a_k = \pm 1$. We may assume that $a_k = 1$; otherwise, by interchanging the roles of $P(z)$ and $Q(z)$ (this does not affect the value of Λ), we may replace $1 + a_k z^k + a_l z^l + \ldots$ by its formal reciprocal, and so change the sign of a_k.

Further, we may assume that $|a_l| \geqslant 1$, otherwise if $|a_l^{(i)}| \geqslant 1$ we replace $P(z)$ by $P^{(i)}(z)$ which affects neither the value of Λ nor $a_k = 1$. It follows from (11) that

$$|c_k| + |d_k| = c \tag{13}$$

for otherwise we would have $\max(|c_k|, |d_k|) \geqslant c \geqslant c/\sqrt{2}$ and again $\Lambda \geqslant \sqrt{2}$. Thus $\max(|c_k|, |d_k|) \geqslant c/\sqrt{2}$ and from (5) $c/\sqrt{2} \leqslant 1 - c^2$, $c \leqslant (\sqrt{17} - 1)/4$. Since by (10) c^{-1} is an algebraic integer

$$c < (\sqrt{17} - 1)/4. \tag{14}$$

The argument now divides into two cases.

The case $l < 2k$. Following Smyth [7], pp. 172–173, we get from (9), (11), (12) and $a_k = 1$ that for all real β, γ

$$E = \tfrac{5}{4}c^2 + (c_{l-k} + \gamma c)^2 + \left(\frac{a_l c + c_{l-k}}{2}\right) + \left(\frac{\gamma c}{2} - c_{l-k} + \beta c\right)^2 \leqslant 2 + \gamma^2 + \beta^2. \tag{15}$$

$E - \gamma^2 - \beta^2$ is a quadratic polynomial say, $F(\beta, \gamma, c_{l-k})$. The matrix of the corresponding quadratic form $t^2 F\left(\frac{\beta}{t}; \frac{\gamma}{t}, \frac{c_{l-k}}{t}\right)$ is

$$\begin{bmatrix} c^2 - 1 & \frac{c^2}{2} & -\frac{c}{2} & \frac{a_l c^2}{2} \\ \frac{c^2}{2} & \frac{5}{4}c^2 - 1 & \frac{3}{4}c & \frac{a_l c^2}{4} \\ -\frac{c}{2} & \frac{3}{4}c & \frac{5}{4} & -\frac{a_l c}{4} \\ \frac{a_l c^2}{2} & \frac{a_l c^2}{4} & -\frac{a_l c}{4} & \frac{a_l c^2}{4} + \frac{5}{4}c^2 \end{bmatrix}.$$

The diagonal minors satisfy in virtue of (14) and of $|a_l| \geqslant 1$

$$\begin{gathered} M_1 = c^2 - 1 < 0, \qquad M_2 = c^4 - \tfrac{9}{4}c^2 + 1 > 0, \qquad M_3 = \tfrac{5}{4} - 2c^2 > 0, \\ M_4 = \tfrac{25}{16}c^2 - \tfrac{5}{2}c^4 + \frac{c^2 a_l^2}{4} \geqslant \tfrac{29}{16}c^2 - \tfrac{5}{2}c^4. \end{gathered} \tag{16}$$

It follows (cf. [1], p. 160) that

$$F(\beta, \gamma, c_{l-k}) = M_1(\beta + \ldots)^2 + \frac{M_2}{M_1}(\gamma + \ldots)^2 + \frac{M_3}{M_2}(c_{l-k} + \ldots)^2 + \frac{M_4}{M_3}$$

and by (15)

$$\frac{M_4}{M_3} = \min_{c_{l-k}} \max_{\beta, \gamma} F(\beta, \gamma, c_{l-k}) \leqslant 2,$$

which gives by (16)

$$40c^4 - 93c^2 + 40 \geqslant 16(2M_3 - M_4) \geqslant 0$$

and (cf. [7], p. 174)

$$\Lambda \geqslant c^{-1} > \theta_0.$$

The case $l \geqslant 2k$. It follows from (11), (12) and $a_k = 1$ that

$$a_{2k} c + d_k + d_{2k} = c_{2k}. \tag{17}$$

We now apply (6) to f and g, and obtain

$$\begin{gathered} -\left(1 - c^2 - \frac{c_k^2}{1+c}\right) \leqslant c_{2k} \leqslant 1 - c^2 - \frac{c_k^2}{1-c}, \\ -\left(1 - c^2 - \frac{d_k^2}{1-c}\right) \leqslant -d_{2k} \leqslant 1 - c^2 - \frac{d_k^2}{1+c}. \end{gathered}$$

Adding these inequalities, and using (17), we have

$$-2(1-c^2) + \frac{d_k^2}{1-c} + \frac{c_k^2}{1+c} \leqslant a_{2k} c + d_k \leqslant 2(1-c^2) - \left(\frac{d_k^2}{1+c} + \frac{c_k^2}{1-c}\right). \tag{18}$$

Now from (5) and (13) we know that

$$1 - c^2 \geqslant |d_k| \geqslant c^2 + c - 1.$$

If $l = 2k$, $a_{2k} \geqslant 1$ we use the right hand side inequality of (18) and obtain

$$c^2 + c - 1 \leqslant c - |d_k| \leqslant 2(1-c^2) - \left(\frac{d_k^2}{1+c} + \frac{c_k^2}{1-c}\right) \leqslant M,$$

where

$$M = \max_{c^2 + c - 1 \leqslant x \leqslant 1 - c^2} \left(2(1-c^2) - \frac{x^2}{1+c} - \frac{(c-x)^2}{1-c}\right).$$

If $l = 2k$, $a_{2k} \leqslant -1$ we use the left hand side inequality of (18) and obtain

$$c^2 + c - 1 \leqslant c - |d_k| \leqslant 2(1-c^2) - \left(\frac{d_k^2}{1-c} + \frac{c_k^2}{1+c}\right) \leqslant M.$$

If $l > 2k$ the inequality $c^2 + c - 1 \leqslant M$ follows at once from (18). However as Smyth has shown ([7], p. 175) this inequality implies $1 - c - c^3 \geqslant 0$, thus $\Lambda \geqslant c^{-1} \geqslant \theta_0$. The proof is complete.

LEMMA 3. *The following inequalities hold*:

$$\prod_{i=1}^{n}(y_i-1)\leqslant\bigl((y_1\dots y_n)^{1/n}-1\bigr)^n \quad \text{for} \quad y_i>1, \tag{19}$$

with the equality attained only if $y_1=y_2=\dots=y_n$;

$$y+\sqrt{c+y^2}\geqslant(1+\sqrt{c+1})\,y^{\frac{1}{\sqrt{c+1}}} \quad (c>0,\ y>0) \tag{20}$$

with the equality attained only for $y=1$.

Proof. We have

$$\frac{d^2}{dx^2}\log(e^x-1)=\frac{-e^x}{(e^x-1)^2}<0,$$

$$\frac{d^2}{dx^2}\log(e^x+\sqrt{c+e^{2x}})=\frac{ce^x}{(c+e^{2x})^{3/2}}>0.$$

The inequality (19) as well as the subsequent statement follows by the substitution $y=e^x$ from the concavity of $\log(e^x-1)$. The inequality (20) and the subsequent statement follow by the same substitution from the Taylor expansion of $\log(e^x+\sqrt{c+e^{2x}})$ at $x=0$.

Proof of Theorem 2. Note first that if $a\in K$ then $\overline{a}\in K$ and

$$\overline{a}^{(i)}=\overline{a}^{(i)},\qquad |a^{(i)}|^2=(|a|^2)^{(i)}. \tag{21}$$

Since the conditions on P and the inequality (2) are invariant with respect to multiplication of P by a constant factor we assume that the coefficients of P are integers. If $|P(0)|\neq|p_0|$ we consider the product

$$\prod_{i=1}^{|K|}\bigl||P^{(i)}(0)|^2-|p_0^{(i)}|^2\bigr|=\bigl|N_{K/Q}\bigl(|P(0)|^2-|p_0|^2\bigr)\bigr| \tag{22}$$

$$\geqslant N_{K/Q}\bigl(C(P)C(\overline{P})\bigr)=N_{K/Q}\bigl(C(P)\bigr)^2.$$

Let $\Pi=\prod_{i=1}^{|k|}\max\bigl(|P^{(i)}(0)/p_0^{(i)}|,1\bigr)$ have k factors equal $|P^{(i)}(0)/p_0^{(i)}|$ corresponding to $i=1,\dots,k$ and set $N_{K/Q}(p_0)=N_0$, $N_{K/Q}\bigl(P(0)\bigr)=N_1$, $N_{K/Q}\bigl(C(P)\bigr)=N_2$.

We have the identities

$$\prod_{i=1}^{|K|}\bigl||P^{(i)}(0)|^2-|p_0^{(i)}|^2\bigr|=\frac{N_1^2}{\Pi^2}\prod_{i=1}^{k}\left|\left|\frac{P^{(i)}(0)}{p_0^{(i)}}\right|^2-1\right|\prod_{i=k+1}^{|K|}\left|\left|\frac{p_0^{(i)}}{P^{(i)}(0)}\right|^2-1\right|,$$

$$\prod_{i=1}^{k}\left|\frac{P^{(i)}(0)}{p_0^{(i)}}\right|\cdot\prod_{i=k+1}^{|K|}\left|\frac{p_0^{(i)}}{P^{(i)}(0)}\right|=\Pi^2\left|\frac{N_0}{N_1}\right|.$$

Hence by (21), (22) and (19)

$$N_2^2\leqslant\frac{N_1^2}{\Pi^2}\bigl(\Pi^{4/|K|}|N_0N_1^{-1}|^{2/|K|}-1\bigr)=\bigl((\Pi N_0)^{2/|K|}-|N_1|^{2/|K|}\Pi^{-2/|K|}\bigr)^{|K|}; \tag{23}$$

$$N_2^{2/|K|}\leqslant(\Pi N_0)^{2/|K|}-|N_1|^{2/|K|}\Pi^{-2/|K|};$$

$$\Pi^{2/|K|}\geqslant\frac{N_2^{2/|K|}+\sqrt{4\,|N_0N_1|^{2/|K|}+N_2^{4/|K|}}}{2N_0^{2/|K|}}.$$

Thus by (20) with $c=4$, $y=|N_2^2/N_0N_1|$

$$\Pi^{2/|K|}\left|\frac{N_0}{N_1}\right|^{1/|K|}\geqslant\frac{1+\sqrt{5}}{2}\left|\frac{N_2^2}{N_0N_1}\right|^{1/|K|\sqrt{5}}, \tag{24}$$

$$\Pi\geqslant\left(\frac{1+\sqrt{5}}{2}\right)^{|K|/2}\left|\frac{N_2}{N_0}\right|^{1/2+1/\sqrt{5}}\left|\frac{N_1}{N_2}\right|^{1/2-1/\sqrt{5}}$$

and since $\prod_{|a_{ij}|>1}|a_{ij}|\geqslant\max\bigl(|P^{(i)}(0)/p_0^{(i)}|,1\bigr)$ the inequality (2) follows.

The equality is possible only if we have equality in (23) and (24) hence by Lemma 3 only if

$$\left|\frac{P^{(i)}(0)}{p_0^{(i)}}\right|^{2k}=\begin{cases}|P^{(1)}(0)/p_0^{(1)}| & \text{for} \quad i=1,\dots,k,\\ |P^{(1)}(0)/p_0^{(1)}|^{-1} & \text{for} \quad i=k+1,\dots,|K|;\end{cases} \tag{25}$$

$$N_2^2=|N_0N_1|.$$

Since $N_2|N_0$ and $N_2|N_1$ the last equality implies $|N_0|=|N_1|=N_2$ and $C(P)=(p_0)$. Moreover by (25) the equality in (24) gives

$$\left|\frac{P^{(1)}(0)}{p_0^{(1)}}\right|^{2k}=\left(\frac{1+\sqrt{5}}{2}\right)^{|K|}$$

hence $\sqrt{5}\in K$. Besides by (25)

$$\left|\frac{P^{(i)}(0)}{p_0^{(i)}}\right|^{2k}=\begin{cases}\left(\dfrac{1+\sqrt{5}}{2}\right)^{|K|} & \text{for} \quad i=1,\dots,k,\\ \left(\dfrac{1-\sqrt{5}}{2}\right)^{|K|} & \text{for} \quad i=k+1,\dots,|K|,\end{cases}$$

which implies $k=|K|/2$, $|P(0)/p_0|=\dfrac{\pm1+\sqrt{5}}{2}$.

In this way the theorem is proved in full for the case where $|P(0)|\neq|p_0|$. If $|P(0)|=|p_0|$ then by Lemma 2

$$\frac{\overline{P^{(i)}(0)}P^{(i)}(z)}{p_0^{(i)}Q_i(z)}=\frac{f_i(z)}{g_i(z)}, \tag{26}$$

where $Q_i(z) = z^{|P|}\overline{P^{(i)}}(z^{-1})$; $f_i(z), g_i(z)$ are holomorphic in an open disc containing $|z| \leqslant 1$, have absolute value 1 on $|z| = 1$ and

$$f_i(0) = g_i(0) = \pm \prod_{|a_{ij}|>1} a_{ij}^{-1}. \tag{27}$$

However by (21) $\overline{P^{(i)}(0)} = \overline{P(0)}^{(i)}$, $Q_i(z) = Q^{(i)}(z)$, thus

$$\frac{\overline{P^{(i)}(0)}P^{(i)}(z)}{p_0^{(i)}Q_i(z)} = 1 + a_k^{(i)}z^k + \dots \tag{28}$$

where $a_k^{(i)}$ is the first non-zero coefficient. Setting

$$f_i(z) = c_{i0} + c_{i1}z + c_{i2}z^2 + \dots,$$
$$g_i(z) = d_{i0} + d_{i1}z + d_{i2}z^2 + \dots$$

we get from (27) and (28)

$$a_k^{(i)}c_{i0} + d_{ik} = c_{ik}.$$

By (5)

$$|c_{ik}| \leqslant 1 - |c_{i0}|^2, \qquad |d_{ik}| \leqslant 1 - |d_{i0}|^2,$$

hence

$$|a_k^{(i)}|\,|c_{i0}| \leqslant 2 - 2|c_{i0}|^2$$

and by (20) with $c = 16$, $y = |a_k^{(i)}|$

$$|c_{i0}|^{-1} \geqslant \frac{|a_k^{(i)}|}{4} + \sqrt{1 + \left(\frac{|a_k^{(i)}|}{4}\right)^2} \geqslant \frac{1+\sqrt{17}}{4}\,|a_k^{(i)}|^{1/\sqrt{17}}.$$

Hence by (27)

$$\prod_{i=1}^{|K|}\prod_{|a_{ij}|>1}|a_{ij}| = \prod_{i=1}^{|K|}|c_{i0}|^{-1} \geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|K|}|N_{K/Q}\,a_k^{(1)}|^{1/\sqrt{17}}.$$

Now, if $\overline{(P(0))}C(P) = (p_0)C(\overline{P})$ then by (28) $p_0^{(i)}a_k^{(i)}$ is an integer divisible by $C(P^{(i)})$, thus

$$|N_{K/Q}\,a_k^{(1)}| \geqslant N_{K/Q}\frac{C(P)}{(p_0)}$$

and

$$\prod_{i=1}^{|K|}\prod_{|a_{ij}|>1}|a_{ij}| \geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|K|}\left(N_{K/Q}\frac{C(P)}{(p_0)}\right)^{1/\sqrt{17}}.$$

The equality is impossible here since it implies by Lemma 3 that $a_k^{(i)} = 1$ and $C(P) = (p_0)$, but then the left hand side is an algebraic integer while the right hand side is not.

It remains to consider the case where $|P(0)| = |p_0|$ and P is irreducible.

Let m be the greatest integer such that $P(z) = R(z^{2^m})$ with $R \in K[z]$. Then $R(z) \neq R(-z)$. Since P and R have the same leading coefficients, $R(0) = P(0)$, $C(R) = C(P)$ and both sides of (2) have the same value for P and for R we may assume at once that $P(z) \neq P(-z)$. Also $P(z) \neq -P(-z)$ since $P(0) \neq 0$ and we can choose $\varepsilon = \pm 1$ such that $z^{|P|}P(z^{-1}) \neq \mathrm{const}\,P(\varepsilon z)$.

Consider now the polynomial $S(z) = P(z)\overline{P}(\varepsilon z)$. It satisfies the condition

$$z^{|S|}\overline{S}(z^{-1}) \neq \mathrm{const}\,S(z),$$

since the irreducible factor $z^{|P|}\overline{P}(z^{-1})$ of the left hand side is not proportional to either factor of the right hand side. Moreover the leading coefficient s_0 of S equals $\pm|p_0|^2 = \pm|P(0)|^2 = \pm S(0)$, $C(S) = C(P)C(\overline{P})$ and $\overline{(S(0))}C(S) = (s_0)C(\overline{S})$.

Applying to S the part of (2) already proved and using the fact that the zeros of S coincide in absolute value with those of P we get

$$\prod_{i=1}^{|K|}\Big(\prod_{|a_{ij}|>1}|a_{ij}|\Big)^2 > \left(\frac{1+\sqrt{17}}{4}\right)^{|K|}\left(N_{K/Q}\frac{C(S)}{(s_0)}\right)^{1/\sqrt{17}},$$

hence

$$\prod_{i=1}^{|K|}\prod_{|a_{ij}|>1}|a_{ij}| \geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2}\left(N_{K/Q}\frac{C(P)}{(p_0)}\right)^{1/\sqrt{17}}$$

and the proof is complete.

Proof of Corollary 1. Since $z^{|P|}\overline{P}(z^{-1}) \neq \mathrm{const}P(z)$ at least one irreducible factor of P, say R satisfies $z^{|R|}\overline{R}(z^{-1}) \neq \mathrm{const}\,R(z)$. Denoting the leading coefficient of R by r_0 and the zeros of $R^{(i)}$ by β_{ij} we have

$$\prod_{i=1}^{|K|}\prod_{|a_{ij}|>1}|a_{ij}| \geqslant \prod_{i=1}^{|K|}\prod_{|\beta_{ij}|>1}|\beta_{ij}|$$
$$\geqslant \min\left\{\left(\frac{1+\sqrt{5}}{2}\right)^{|K|/2}\left(N_{K/Q}\frac{C(R)}{(r_0)}\right)^{1/2+1/\sqrt{5}}, \left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2}\left(N_{K/Q}\frac{C(R)}{(r_0)}\right)^{1/\sqrt{17}}\right\}$$
$$\geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2}N_{K/Q}\frac{C(P)}{(p_0)},$$

since by the multiplicative property of the content $(p_0)C(P)^{-1}$ is divisible by $(r_0)C(R)^{-1}$. In the above sequence of inequalities at least one must be strict, which proves the corollary.

Lemma 4. *If f is a monic polynomial with complex coefficients and the zeros z_j then*

$$\prod_{|z_j|>1}|z_j|^2 + \prod_{|z_j|<1}|z_j|^2 \leqslant \|f\| \tag{29}$$

(*empty products denote* 1) *with the equality attained only if*

$$z^{|f|}f(z)\overline{f}(z^{-1}) = \overline{f(0)}z^{2|f|} + \|f\|z^{|f|} + f(0).$$

Proof. The inequality (29) is due to J. V. Gonçalves [2], it is only the last assertion of the lemma, which requires the proof. This is obtained easily from Ostrowski's proof of (29). Ostrowski [5] shows namely that $\|f\| = \|g\|$, where

$$g(z) = \prod_{|z_j|>1}(z-z_j)\prod_{|z_j|<1}(1-z\bar{z}_j) = z^{|f|}\prod_{|z_j|<1}(-\bar{z}_j) + \ldots + \prod_{|z_j|>1}(-z_j).$$

Therefore equality in (23) implies that

$$g(z) = z^{|f|}\prod_{|z_j|<1}(-z_j) + \prod_{|z_j|>1}(-z_j),$$

whence

$$z^{|f|}f(z)\overline{f}(z^{-1}) = \overline{f(0)}z^{2\|f\|} + \|f\|z^{|f|} + f(0).$$

Proof of Theorem 3. Since the inequalities (3) are invariant with respect to multiplication of f by a constant factor we may assume that f is monic. Let the conjugates of K be numbered so that all different conjugates of f occur equally often among $f^{(i)}$ $(i = 1, \ldots, |L|)$.

Let z_{ij} be the zeros of $f^{(i)}$. Let finally

$$f = P_0P_1 \ldots P_n,$$

where P_ν are monic and for $\nu > 0$ satisfy $z^{|P_\nu|}\overline{P}_\nu(z^{-1}) \neq \mathrm{const}P_\nu(z)$. We have

$$N_{K/Q}\big(C(P_0)\big) \leqslant 1 \quad \text{and} \quad \prod_{\nu=0}^{n} C(P_\nu) = C(f).$$

Hence by Corollary 1

$$\Big(\prod_{i=1}^{|L|}\prod_{|z_{ij}|>1}|z_{ij}|\Big)^{|K|/|L|} = \prod_{i=1}^{|K|}\prod_{|z_{ij}|>1}|z_{ij}| = \prod_{\nu=0}^{n}\prod_{i=1}^{|K|}\prod_{\substack{P_\nu^{(i)}(z_{ij})=0\\ |z_{ij}|>1}}|z_{ij}|$$

$$\geqslant \Big(\frac{1+\sqrt{17}}{4}\Big)^{|K|n/2}\prod_{\nu=0}^{n}N_{K/Q}\big(C(P_\nu)\big) = \Big(\frac{1+\sqrt{17}}{4}\Big)^{|K|n/2}N_{L/Q}\big(C(f)\big)^{|K|/|L|}$$

and

$$(30_1)\qquad \Pi = \prod_{i=1}^{|L|}\prod_{|z_{ij}|>1}|z_{ij}| \geqslant \Big(\frac{1+\sqrt{17}}{4}\Big)^{|L|n/2}N_{L/Q}\big(C(f)\big).$$

If all prime ideal factors $\mathfrak{p}$ of $(1, f(0))C(f)^{-1}$ in K satisfy $\overline{\mathfrak{p}} = \mathfrak{p}$ then in view of the divisibility

$$(1, P_\nu(0))C(P_\nu)^{-1}\,\big|\,(1, f(0))C(f)^{-1}$$

we have $(1, P_\nu(0))C(P_\nu)^{-1} = (1, \overline{P_\nu(0)})C(\overline{P}_\nu)^{-1} = \mathfrak{a}_\nu$. Hence either $|P_\nu(0)| \neq 1$ or

$$(\overline{P_\nu(0)})C(P_\nu) = (\overline{P_\nu(0)})(1, P_\nu(0))\mathfrak{a}_\nu^{-1} = (\overline{P_\nu(0)}, |P_\nu(0)|^2)\mathfrak{a}_\nu^{-1} = (\overline{P_\nu(0)}, 1)\mathfrak{a}_\nu^{-1} = C(\overline{P}_\nu)$$

and using Theorem 2 instead of Corollary 1 we get

$$(30_2)\qquad \Pi = \prod_{i=1}^{|L|}\prod_{|z_{ij}|>1}|z_{ij}| \geqslant \Big(\frac{1+\sqrt{5}}{2}\Big)^{|L|n/2}N_{L/Q}\big(C(f)\big).$$

On the other hand, by Lemma 4

$$(31)\qquad \prod_{|z_{ij}|>1}|z_{ij}|^2 + \prod_{|z_{ij}|<1}|z_{ij}|^2 \leqslant \|f^{(i)}\| \quad (i = 1, \ldots, |L|),$$

hence

$$(32)\qquad \prod_{i=1}^{|L|}\prod_{|z_{ij}|>1}|z_{ij}|^2 + \prod_{i=1}^{|L|}\prod_{|z_{ij}|<1}|z_{ij}|^2 \leqslant N_{L/Q}\|f\|.$$

However

$$(33)\qquad \prod_{i=1}^{|L|}\prod_{|z_{ij}|<1}|z_{ij}|^2 = \Pi^{-2}N_{L/Q}|f(0)|^2 \geqslant \Pi^{-2}N_{L/Q}^4\big(C(f)\big)$$

for $N_{L/Q}\big(C(f)\big) \leqslant \min\big(1, |Nf(0)|\big)$. Thus

$$\Pi^2 + N_{L/Q}^4\big(C(f)\big)\Pi^{-2} \leqslant N_{L/Q}\|f\|$$

and by (30) the inequalities (3) follow. The equality in (3_2) implies the equality in (30_2), (31), (32) and (33). The equality in (31) and (32) imply that $|L| = 1$. The equality in (33) implies $C(f) = |f(0)| = 1$. By Lemma 4 the equality in (31) implies

$$(34)\qquad z^{|f|}f(z)f\Big(\frac{1}{z}\Big) = \pm z^{2|f|} + \Big[\Big(\frac{1+\sqrt{5}}{2}\Big)^n + \Big(\frac{1+\sqrt{5}}{2}\Big)^{-n}\Big]z^{|f|} \pm 1.$$

Since $\Big(\frac{1+\sqrt{5}}{2}\Big)^n + \Big(\frac{1+\sqrt{5}}{2}\Big)^{-n}$ is an integer, n must be even, $n = 2m$. If $n = 0$ then

$$z^{|f|}f(z)f\Big(\frac{1}{z}\Big) = \pm(z^{|f|} \pm 1)^2$$

and since all cyclotomic polynomials are reciprocal

$$z^{|f|}f\left(\frac{1}{z}\right) = \pm f(z); \quad f(z)^2 = (z^{|f|} \pm 1)^2; \quad f(z) = z^{|f|} \pm 1.$$

If $n > 0$ then the equality in (30_2) implies in virtue of Theorem 2 that $\sqrt{5} \in K$ and $|P_\nu(0)| = \dfrac{1+\sqrt{5}}{2}$ for $\nu = 1, 2, \ldots, n$.

Now, the right hand side of (34) equals

$$\pm\left(z^{|f|} \pm \left(\frac{1+\sqrt{5}}{2}\right)^{2m}\right)\left(z^{|f|} \pm \left(\frac{1-\sqrt{5}}{2}\right)^{2m}\right)$$

hence $g(z) = z^{|f|} \pm \left(\dfrac{1+\sqrt{5}}{2}\right)^{2m}$ has in K $2m$ monic factors P such that $|P(0)| = \dfrac{1+\sqrt{5}}{2}$. Since the zeros of $g(z)$ have absolute value $\left(\dfrac{1+\sqrt{5}}{2}\right)^{2m/|f|}$ it follows that the degree of each factor is $|f|/2m$, hence $|f| = 2lm$, l integer. Let $\alpha = \operatorname{ord}_2 m + \frac{1}{2} \pm \frac{1}{2}$, where the sign is that occurring in (34). We have

$$g_1(z) = z^{2^{\alpha}l} + \left(\frac{1+\sqrt{5}}{2}\right)^{2^{\alpha}} \Big| g(z).$$

By Capelli's theorem $g_1(z)$ is irreducible in $Q(\sqrt{5})$ hence by (34)

$$g_1(z) | f(z) \quad \text{or} \quad g_1(z) | z^{|f|} f\left(\frac{1}{z}\right).$$

Assuming without loss of generality the first possibility we get

$$z^{2^{\alpha}l} + \left(\frac{1-\sqrt{5}}{2}\right)^{2^{\alpha}} \Big| f(z),$$

$$z^{2^{\alpha}l} + (-1)^{2^{\alpha}}\left(\frac{1+\sqrt{5}}{2}\right)^{2^{\alpha}} \Big| z^{|f|} f\left(\frac{1}{z}\right)$$

and if $\alpha > 0$

$$g_1(z)^2 \Big| \pm z^{2|f|} + \left[\left(\frac{1+\sqrt{5}}{2}\right)^{2m} + \left(\frac{1+\sqrt{5}}{2}\right)^{-2m}\right] z^{|f|} \pm 1,$$

which is impossible. Therefore $\alpha = 0$, the sign is lower and m is odd. It remains to show that $K \supset Q(\sqrt{5}, e^{2\pi i/m})$. Assume that any of the considered factors of $g(z)$ in K is not binomial. Then it has a coefficient of the form $c\left(\dfrac{1+\sqrt{5}}{2}\right)^{k/l}$, where $0 < k < l$, $c \neq 0$ and $c \in Q(\zeta_{2lm})$. It follows that

$$\left(\frac{1+\sqrt{5}}{2}\right)^{k/l} \in K(\zeta_{2lm}),$$

which is impossible since the field $K(\zeta_{2lm})$ satisfies again the assumptions of Theorem 2 and $\left(\dfrac{1+\sqrt{5}}{2}\right)^{k/l}$ has some real and some complex conjugates. Thus the required factorization of $g(x)$ in K is

$$z^{2lm} - \left(\frac{1+\sqrt{5}}{2}\right)^{2m} = \prod_{j=0}^{2m-1}\left(z^l - \frac{1+\sqrt{5}}{2}\zeta_{2m}^j\right)$$

and $K \supset Q(\sqrt{5}, \zeta_m)$. Conversely, if $K \supset Q(\sqrt{5}, \zeta_m)$, $L = Q$ and f satisfies (4) then $z^{|f|}f(z)f(z^{-1})$ has $4m$ factors in K, $f(z)$ has $2m$ factors and the equality holds in (3_2).

Proof of Corollary 2. $\varphi(z)$ satisfies the conditions of (3_2). If $z^{|P|}\overline{P}(z^{-1}) = \text{const}\, P(z)$ and $P(z)|\varphi(z)$ then $P(z)|z^{|\varphi|}\varphi(z^{-1})$, thus

$$P(z) | (z^p + \varepsilon z^q + \eta) - (z^p + \varepsilon\eta z^{p-q} + \eta) = \varepsilon z^q - \varepsilon\eta z^{p-q}$$

and P is cyclotomic. Therefore, it remains to consider the case where n occurring in (3_2) for $f = \varphi$, $L = Q$ equals 2. Then (3_2) becomes an equality and by Theorem 3 $\sqrt{5} \in K$,

$$z^p\varphi(z)\varphi\left(\frac{1}{z}\right) = c(z^{2p} - 3z^p + 1).$$

It follows that $\varphi(z) = z^{2q} \pm z^q - 1$.

References

[1] R. Fricke, *Lehrbuch der Algebra I*, Braunschweig 1924.

[2] J. Vicente Gonçalves, *L'inégalité de W. Specht*, Univ. Lisboa Revista Fac. Ci. (2) A 1 (1956), pp. 167–171.

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

[4] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. 8 (1960), pp. 65–70.

[5] A. M. Ostrowski, *On an inequality of J. Vicente Gonçalves*, Univ. Lisboa Revista Fac. Ci. (2) A 8 (1960), pp. 115–119.

[6] C. L. Siegel, *Algebraic integers whose conjugates lie in the unit circle*, Duke Math. J. 11 (1944), pp. 597–602.

[7] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), pp. 169–175.

[8] H. Tverberg, *On the irreducibility of* $x^n \pm x^m \pm 1$, Math. Scand. 8 (1960), pp. 121–126.

Received on 8. 12. 1972 (358)