Conspectus materiae tomi XLI, fasciculi 2

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-905 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-02968-4 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XLI (1982)

Traces of monomials in algebraic numbers

by

A. Bazylewicz (Warszawa)

A. Schinzel ([2]) put forward the following conjecture: For every number field K that is neither a totally real nor a totally complex quadratic extension of a totally real field and for every nonconstant polynomial $f \in K\overline{K}[x]$, there exists a β in K such that $\mathrm{Tr}\big(f(\beta\overline{\beta})\big) > 0$ (the bar denotes the complex conjugation and Tr stands for the trace from $K\overline{K}$ to Q).

In the same paper he has proved the above conjecture for K being a real field.

In Theorem 1 we consider the monomial cx^m, where $c \in K$ and m is a positive rational integer. We obtain that if $c+\overline{c} = 0$ then $\mathrm{Tr}(c\beta^m\overline{\beta}^m) = 0$ for every β in K and that besides this trivial case Schinzel's conjecture fails if and only if K and $\overline{K}$ are linearly disjoint over $K \cap \overline{K}$ and the latter field is a quadratic extension of a totally real field satisfying some technical conditions.

On the other hand there are primitive fields K and numbers d of $K\overline{K}$ such that $d+\overline{d} \neq 0$ and $\mathrm{Tr}(d\beta^m\overline{\beta}^m) \geqslant 0$ for every $\beta \in K$ and every positive integer m.

The relevant example is shown at the end of the paper.

The remaining results presented here are consequences of Theorem 1, in particular, Theorem 2 is just Schinzel's conjecture properly modified.

G. Shimura and Y. Taniyama [3] have proved the equivalence of the following two statements:

(i) K is a totally complex quadratic extension of a totally real field or a totally real field,

(ii) $K = \overline{K}$ and $\mathrm{Tr}(\alpha\overline{\alpha}) > 0$ for every nonzero α of K.

K. Györy [1] has shown that in (ii) $\mathrm{Tr}(\alpha\overline{\alpha})$ can be replaced by $E_r(\alpha\overline{\alpha})$ (the elementary symmetric function of degree r of the conjugates of $\alpha\overline{\alpha}$) for each $r < [K:Q]$.

Theorem 3 asserts that the assumption $K = \overline{K}$ in (ii) can be omitted. Now we introduce some definitions and fix the terminology used in the sequel. Q, R, C denote the field of rational, real and complex numbers respectively. A field $K \subset C$ will be called *complex* if $K \not\subset R$. Let K be a finite extension of Q and let g be any embedding of K into C. The image of K under g will be denoted by gK. If K is a real field we say that a finite extension L/K is *totally real* (*complex*) over K if for every embedding h of L into C trivial on K, the field hL is real (complex).

An extension L/K is imprimitive if there is a field M such that $K \underset{\neq}{\subset} M \underset{\neq}{\subset} L$.

For a complex number x, $\bar{x}$ denotes its complex conjugate. We set $2\operatorname{Re} x = x+\bar{x}$.

The main result of this paper is

THEOREM 1. *Let K be a finite complex extension of the field of rationals, K_0 be the maximal totally real subfield of K, $K_1 = K \cap \bar{K}$.*

A. *If c is an element of K with $\operatorname{Re} c = 0$ and m is a positive integer, then for all β in K we have*

$$\operatorname{Tr}(c\beta^m\bar{\beta}^m) = 0.$$

B. *Let c be an element of K with $\operatorname{Re} c \neq 0$. Then*

(*) $\operatorname{Tr}(c\beta^m\bar{\beta}^m) \geqslant 0$ *for all $\beta \in K$ and for all positive integers m*

if and only if the following conditions are satisfied:

(i) $[K_1 : K_0] = 2$,

(ii) $[K\bar{K} : \bar{K}] = [K : K_1]$,

(iii) *if m is odd then K_1/K_0 is totally complex; if m is even then for every embedding g of K into C either gK_1 is real and gK/gK_0 is totally real over gK_0 or gK_1 is complex and gK/gK_0 is totally complex over gK_0.*

(iv) *$c \in K_1$ and $\operatorname{Re} c$ is totally positive.*

Let us define $\operatorname{Re} f = \sum_{i=0}^{r} (\operatorname{Re} c_i)x^i$ for any polynomial $f(x) = \sum_{i=0}^{r} c_i x^i \in K[x]$. Then we have

THEOREM 2. *Let K be a complex field not containing any totally real subfield K_0 with $[K : K_0] = 2[K\bar{K} : \bar{K}]$. Then for every $f \in K[x]$ with $\operatorname{Re} f \neq \text{const}$ there is a β in K satisfying $\operatorname{Tr}\big(f(\beta\bar{\beta})\big) > 0$.*

The following theorem is a new version of the result of Shimura and Taniyama.

THEOREM 3. *If K is neither a totally real nor a totally complex quadratic extension of a totally real field then there is a nonzero $\beta \in K$ with $\operatorname{Tr}(\beta\bar{\beta}) \leqslant 0$.*

We note that if K is a totally real field or a totally complex quadratic extension of a totally real field then $\operatorname{Tr}(\beta\bar{\beta}) > 0$ for every nonzero $\beta \in K$. Hence we obtain the following

COROLLARY. *K is a totally real field or a totally complex quadratic extension of a totally real field if and only if $\operatorname{Tr}(\beta\bar{\beta}) > 0$ for every nonzero β in K.*

We proceed to the proof of Theorem 1. Let $\varphi_1, \varphi_2, \ldots, \varphi_s, \varphi_{s+1} = \bar{\varphi}_1, \ldots, \varphi_{2s} = \bar{\varphi}_s$ be the complex embeddings of K and let $\varphi_{2s+1}, \ldots, \varphi_n$ be the real ones. For any x in K we shall denote $\varphi_i(x)$ by x_i. In particular, if $K = Q(a)$, then $a_1 = a, a_2, \ldots, a_n$ are all conjugates of a. In the sequel a will denote a fixed generator of K.

Let us denote by $N(K)$ the least normal field containing K and by G its Galois group. The action of G on $K\bar{K}$ is determined by its action on the pair $(a, \bar{a})$.

We define S as the set of all distinct pairs $(ga, g\tau a)$, where g lies in G and τ denotes a complex conjugation.

This set has the following properties:

(1a) $(a_i, a_i) \notin S$ for all i, $1 \leqslant i \leqslant n$,

(1b) If $(a_i, a_j) \in S$ then $(a_j, a_i) \in S$,

(1c) If $(a_i, a_j) \in S$ then $(\bar{a}_i, \bar{a}_j) \in S$,

(1d) For every i, $1 \leqslant i \leqslant n$,

$$\#\{j\colon (a_i, a_j) \in S\} = [K\bar{K} : \bar{K}],$$

where $\# A$ denotes the cardinality of A.

The proof of (1a), (1b), (1c) is trivial and in order to obtain (1d) it is sufficient to observe that

$$\begin{aligned}\#\{j\colon (a_i, a_j) \in S\} &= \#\{g\tau a\colon g \in G,\ ga = g_0 a\}\\ &= \#\{g\tau a\colon g \in G,\ ga = a\}\\ &= [K\bar{K} : \bar{K}] = [K\bar{K} : K].\end{aligned}$$

Here g_0 denotes a fixed element of G such that $g_0 a = a_i$.

Proof of Theorem 1A. Let $c, \beta \in K$. By the definition of S we have

$$\operatorname{Tr}(c\beta^m\bar{\beta}^m) = \sum_{\substack{(i,j)\\ (a_i,a_j)\in S}} c_i\beta_i^m\beta_j^m. \tag{2}$$

Since $c\beta^m\bar{\beta}^m$ and $\bar{c}\beta^m\bar{\beta}^m$ are conjugate we have

$$\operatorname{Tr}(c\beta^m\bar{\beta}^m) = \operatorname{Tr}(\bar{c}\beta^m\bar{\beta}^m),$$

which implies

$$2\operatorname{Tr}(c\beta^m\bar{\beta}^m) = \operatorname{Tr}\big((c+\bar{c})\beta^m\bar{\beta}^m\big). \tag{3}$$

Hence if $2\operatorname{Re} c = c + \bar{c} = 0$ then

$$\operatorname{Tr} c\beta^m \bar{\beta}^m = 0 \quad \text{for all } \beta \text{ in } K.$$

Thus we have just proved Theorem 1A.

We now proceed to the proof of Theorem 1B. In the sequel we shall assume that $\operatorname{Re} c \neq 0$. Comparing (2) and (3) we obtain

$$(3') \qquad 2\operatorname{Tr}(c\beta^m \bar{\beta}^m) = \sum_{\substack{(i,j) \\ (\alpha_i, \alpha_j) \in S}} (c_i + c_j) \beta_i^m \beta_j^m.$$

We set

$$\mathscr{T}_m(X) = \sum_{1 \leqslant i \leqslant j \leqslant n} e_{ij} x_i^m x_j^m,$$

where

$$X = (x_1, \ldots, x_n) \in C^n \quad \text{and} \quad e_{ij} = \begin{cases} c_i + c_j & \text{if} \quad (\alpha_i, \alpha_j) \in S, \\ 0 & \text{otherwise.} \end{cases}$$

We note that $e_{ij} = e_{ji}$ and $e_{ij} \neq 0$ if and only if $(\alpha_i, \alpha_j) \in S$, since in this case e_{ij} and $c + \bar{c} \neq 0$ are conjugate.

For $i \in \{1, 2, \ldots, n\}$ we set

$$(4) \qquad i' = \begin{cases} i & \text{if} \quad \varphi_i \text{ is real,} \\ i+s & \text{if} \quad \varphi_i \text{ is complex and } i \leqslant s, \\ i-s & \text{if} \quad \varphi_i \text{ is complex and } i > s. \end{cases}$$

Then for every x in K we have $x_{i'} = \bar{x}_i$.

One can easily check the following properties of the coefficients e_{ij}:

(5a) $e_{ij} \cdot e_{ii'} \cdot e_{jj'} \neq 0$ implies

$$|e_{ij}|^2 - e_{ii'} \cdot e_{jj'} = |c_i - \bar{c}_j|^2;$$

(5b) $e_{i'j} \cdot e_{ii'} \cdot e_{jj'} \neq 0$ implies

$$|e_{i'j}|^2 - e_{ii'} \cdot e_{jj'} = |c_i - c_j|^2;$$

$$(5c) \qquad |e_{ij}|^2 - e_{ii'} \cdot e_{jj'} \geqslant 0 \quad \text{if} \quad e_{ij} \neq 0;$$

$$(5d) \qquad |e_{i'j}|^2 - e_{ii'} \cdot e_{jj'} \geqslant 0 \quad \text{if} \quad e_{i'j} \neq 0.$$

We set

$$W = \{X = (x_1, \ldots, x_n):\ x_i \in C \text{ and } x_{i+s} = \bar{x}_i \text{ for } 1 \leqslant i \leqslant s, \\ x_i \in R \text{ for } 2s < i \leqslant n\}.$$

By the definition of W and (1c) $\mathscr{T}_m(X)$ takes real values for $X \in W$. Let us denote by T_m the restriction of $\mathscr{T}_m$ to W. For β in K we put U_1: $\beta \mapsto (\beta_1, \ldots, \beta_n) \in W$ and denote by O'_K the image of the ring of integers O_K of K under U_1.

The transformation

$$U_2\colon\ y_1 = \frac{x_1 + \bar{x}_1}{2},\ y_2 = \frac{x_1 - \bar{x}_1}{2\sqrt{-1}}, \ldots, y_{2s-1} = \frac{x_s + \bar{x}_s}{2},$$

$$y_{2s} = \frac{x_s - \bar{x}_s}{2\sqrt{-1}},\ y_{2s+i} = x_{2s+i} \quad \text{for } i = 1, \ldots, n-2s$$

is a linear isomorphism of W and $\boldsymbol{R}^n$. It is well known that O''_K, the image of O'_K under U_2, is a complete n-dimensional lattice. We can represent $T_m(X)$ as a form $\Phi_m(y_1, \ldots, y_n)$ with real coefficients and of real variables.

The following lemmata will be useful in the proof of the theorem.

Lemma 1. *Let Φ be a form with real coefficients and of n real variables $X = (x_1, \ldots, x_n)$, $V^- = \{X \in \boldsymbol{R}^n\colon\ \Phi(X) < 0\}$, $V^+ = \{X \in \boldsymbol{R}^n\colon\ \Phi(X) > 0\}$ and let Λ be a complete n-dimensional lattice. Then*

(a) *if V^- is not empty then there exists a nonzero $\eta \in V^- \cap \Lambda$,*

(b) *if V^+ is not empty then there exists a nonzero $\theta \in V^+ \cap \Lambda$.*

Proof. As Φ is continuous and for positive t the signs of $\Phi(X)$ and $\Phi(tX)$ coincide, V^+ and V^- are either empty or contain a cone in $\boldsymbol{R}^n$. But such a cone meets every complete lattice.

Lemma 2. *The following two statements are equivalent:*

(a) *There exists a $0 \neq \beta \in K$ $(0 \neq \gamma \in K)$ such that*

$$\operatorname{Tr}(c\beta^m \bar{\beta}^m) > 0 \qquad (\operatorname{Tr}(c\gamma^m \bar{\gamma}^m) < 0).$$

(b) *There exists a $\theta \in W$ $(\eta \in W)$ with $T_m(\theta) > 0$ $(T_m(\eta) < 0)$.*

Proof. (a) $\Rightarrow$ (b). This implication follows from the fact that for $\beta \in K$ and $\theta = U_1(\beta)$

$$\operatorname{Tr}(c\beta^m \bar{\beta}^m) = T_m(\theta).$$

(b) $\Rightarrow$ (a). Suppose that we have θ in W with $T_m(\theta) > 0$. Using the isomorphism U_2 of W and $\boldsymbol{R}^n$, we obtain a real vector θ' with $\Phi_m(\theta') > 0$.

In virtue of Lemma 1 there is a nonzero $\delta \in O''_K$ with $\Phi_m(\delta) > 0$, which is equivalent to the existence of $\beta \in O^*_K$ $(O^*_K = O_K - \{0\})$ satisfying $\operatorname{Tr}(c\beta^m \bar{\beta}^m) > 0$.

Similarly, if we can choose $\eta \in W$ with $T_m(\eta) < 0$ then there is a $\gamma \in O^*_K$ with $\operatorname{Tr}(c\gamma^m \bar{\gamma}^m) < 0$.

Corollary 2.1. *Under the condition* (*) *of Theorem* 1B *we have* $e_{11'} > 0$.

Proof. By the assumption $e_{11'} = 2\operatorname{Re} c \neq 0$. If $e_{11'} < 0$ we set $\theta_k = 1$ for $k = 1$ or $1'$, $\theta_k = 0$ otherwise. Then $\theta = (\theta_1, \ldots, \theta_n) \in W$, $T_m(\theta) = e_{11'} < 0$ and Lemma 2 gives a contradiction with the condition (*).

COROLLARY 2.2 *If for a certain j we have*

$$e_{11'} > 0, \quad e_{1j} = e_{1'j'} = 0 \quad \text{and} \quad e_{11'} \cdot e_{jj'} \neq |e_{1j'}|^2 \neq 0$$

then there is a $\beta \in K$ such that $\mathrm{Tr}(c\beta^m \bar{\beta}^m) < 0$.

Proof. We choose a complex number θ_1 satisfying $e_{11'}\theta_1^m + e_{1'j} = 0$ and put

$$\theta_k = \begin{cases} \theta_1 & \text{if} \quad k = 1, \\ \bar{\theta}_1 & \text{if} \quad k = 1', \\ 1 & \text{if} \quad k = j, j', \\ 0 & \text{otherwise}. \end{cases}$$

We get

$$\theta = (\theta_1, \ldots, \theta_n) \in W \quad \text{and} \quad T_m(\theta) = \frac{e_{11'} e_{jj'} - |e_{1j'}|^2}{e_{11'}}.$$

Since by (5d) $e_{11'} e_{jj'} - |e_{1j'}|^2 \leqslant 0$ we have either $e_{11'} e_{jj'} = |e_{1j'}|^2$ or by Corollary 2.1 $T_m(\theta) < 0$.

In the latter case Lemma 2 applies.

LEMMA 3. *Let $J_i = \{j\colon (\bar{\alpha}_i, \alpha_j) \in S\}$, $J_i' = \{j'\colon j \in J_i\}$. Under condition $(*)$ of Theorem 1B we have*

$$J_i \cap J_i' = \emptyset \quad \textit{whenever } i \neq i'.$$

Proof. Suppose that $j \in J_i \cap J_i'$. We assume first that $j = j'$. Then by (1a) $e_{jj'} = 0$ moreover $e_{i'j} = \bar{e}_{ij}$. For X in W we have

$$T_m(X) = e_{ij} x_i^m x_j^m + e_{i'j} \bar{x}_i^m x_j^m + e_{ii'} |x_i|^{2m} + T_m^{(1)}(X),$$

where every term of $T_m^{(1)}(X)$ contains a factor x_k with $k \neq i, i', j$. We choose a complex number θ_i such that $\theta_i^m = -\bar{e}_{ij}$ and a real number θ_j with $2\theta_j^m > e_{ii'}$. Then we put $\theta_{i'} = \bar{\theta}_i$ and $\theta_k = 0$ for all remaining subscripts k. We have

$$\theta = (\theta_1, \ldots, \theta_n) \in W, \quad T_m(\theta) = -2\theta_j^m |e_{ij}|^2 + e_{ii'} |e_{ij}|^2 < 0$$

and Lemma 2 applies giving a contradiction.

Now let $j \neq j'$. By (5c) and (5d) there exists a positive real number e satisfying the inequalities

$$e \geqslant e_{jj'}, \quad \text{and} \quad (|e_{j'i}| + |e_{j'i'}|)^2 > e e_{ii'}.$$

We have for $X \in W$

$$eT_m(X) = \Big|e x_j^m + \sum_{\substack{u=1 \\ u \neq j, j'}}^{n} e_{j'u} x_u^m\Big|^2 - |e_{j'i} x_i^m + e_{j'i'} \bar{x}_i^m|^2 +$$
$$+ (e e_{jj'} - e^2) |x_j|^{2m} + e e_{ii'} |x_i|^{2m} + T_m^{(1)}(X),$$

where every term of $T_m^{(1)}(X)$ contains a factor x_k with $k \neq i, i', j, j'$. We note that since $j \in J_i \cap J_i'$ we have $e_{j'i} \neq 0 \neq e_{j'i'}$ hence we can choose θ_i such that

$$\theta_i^{2m} = e_{j'i'} \cdot |e_{j'i}| / |e_{j'i'}| \cdot e_{j'i}.$$

Then

$$|e_{j'i}\theta_i^m + e_{j'i'} \bar{\theta}_i^m| = |e_{j'i}| + |e_{j'i'}|.$$

Further we take $\theta_{i'} = \bar{\theta}_i$, choose θ_j satisfying $e\theta_j^m + e_{j'i}\theta_i^m + e_{j'i'}\bar{\theta}_i^m = 0$ (this is possible since $e \neq 0$), $\theta_{j'} = \bar{\theta}_j$ and put $\theta_k = 0$ for all $k \neq i, i', j, j'$. $\theta = (\theta_1, \ldots, \theta_n)$ obtained in this way belongs to W and by the choice of e satisfies:

$$eT_m(\theta) = -(|e_{j'i}| + |e_{j'i'}|)^2 + e(e_{jj'} - e)|\theta_j|^{2m} + e e_{ii'} < 0.$$

Hence $T_m(\theta) < 0$ and Lemma 2 applies giving a contradiction.

COROLLARY 3.1. *Let $J = J_1$. Under the assumptions of Lemma 3 we have $J_i \cap J_i' = \emptyset$ for all $i \in J$.*

Proof. Since $1 \neq 1'$ we have by Lemma 3 $J \cap J' = \emptyset$ hence $i \neq i'$ for all $i \in J$. To obtain the corollary it suffices to apply Lemma 3 again.

LEMMA 4. *Let $J = J_1$. Under the assumptions of Lemma 3 we have*

$$J_i \subset J \cup J' \quad \textit{for all } i \in J.$$

Proof. Let us suppose that for some i, j we have $J_i \not\subset J \cup J'$ and $j \in J_i - (J \cup J')$. We have $e_{j'i} \neq 0, e_{1i'} \neq 0, e_{i'j} \neq 0, e_{ij'} \neq 0$ but $e_{1'j} = e_{1'i'} = e_{1j} = e_{1j'} = 0$. From Corollary 3.1 we get also $e_{1i} = e_{1'i'} = e_{ij} = e_{i'j'} = 0$. Let us choose a positive real number $e > \frac{1}{2} e_{11'} \cdot e_{jj'}$.

For all X in W we have

$$e_{11'} T_m(X) = \Big|\sum_{k=1}^{n} e_{1'k} x_k^m\Big|^2 + (e_{11'} e_{ii'} - |e_{1'i}|^2)|x_i|^{2m} + T_m^{(1)}(X),$$

where $x_1, \bar{x}_1$ do not appear in $T_m^{(1)}(X)$ and every term of $T_m^{(1)}(X)$ contains a factor x_k with $k \neq 1, 1', i, i'$.

Moreover

$$eT_m^{(1)}(X) = \Big|e x_j^m + \sum_{\substack{k=2 \\ k \neq j}}^{n} e_{11'} e_{j'k} x_k^m\Big|^2 + (e e_{11'} e_{jj'} - e^2)|x_j|^{2m} -$$
$$- e_{11'}^2 |e_{j'i}|^2 |x_i|^{2m} + T_m^{(2)}(X),$$

where every term of $T_m^{(2)}(X)$ contains a factor x_k with $k \neq 1, 1', i, i', j, j'$.

By Corollary 2.2 we have $e_{11'} e_{ii'} - |e_{1'i}|^2 = 0$. Hence

$$e e_{11'} T_m(X) = e\Big|\sum_{k=1}^{n} e_{1'k} x_k^m\Big|^2 + \Big|e x_j^m + \sum_{\substack{k=2 \\ k \neq j}}^{n} e_{11'} e_{j'k} x_k^m\Big|^2 +$$
$$+ (e e_{11'} e_{jj'} - e^2)|x_j|^{2m} - e_{11'} |e_{j'i}|^2 |x_i|^{2m} + T_m^{(2)}(X).$$

We take $\theta_j = \theta_{j'} = 1$. Next we choose θ_i such that $e + e_{11'}e_{j'i}\theta_i^m = 0$ and put $\theta_{i'} = \bar{\theta}_i$. Since $e > 0$ we have $\theta_i \neq 0$. Then we take θ_1 satisfying $e_{11'}\theta_1^m + e_{1'i}\theta_i^m = 0$, $\theta_{1'} = \bar{\theta}_1$ and put $\theta_k = 0$ for all remaining $k \leqslant n$. We have $\theta \in W$ and $T_m(\theta) = (e_{11'}e_{jj'} - 2e)/e_{11'} < 0$. An application of Lemma 2 gives a contradiction with condition (*) of Theorem 1B.

LEMMA 5. *Under condition* (*) *of Theorem* 1B *we have*

$$c_i = c \quad \text{for} \quad i \in J \tag{6}$$

and for $X \in W$

$$\sum_{\substack{i,j\in J\cup J'\\ i<j}} e_{ij}x_i^m x_j^m = (c+\bar{c})\Big|\sum_{i\in J} x_i^m\Big|^2 + \sum_{\substack{i,j\in J\\ i<j,\, e_{i'j}=0}} [2(cx_i^m x_j^m + \bar{c}\bar{x}_i^m \bar{x}_j^m) - (c+\bar{c})(x_i^m \bar{x}_j^m + \bar{x}_i^m x_j^m)]. \tag{7}$$

Proof. By the definition of J $e_{1j'} \neq 0$ for all $j \in J$ and by Corollary 3.1 $e_{1j} = e_{1'j'} = 0$. Thus by Corollary 2.2 $e_{11'}e_{jj'} = |e_{1'j}|^2 \neq 0$ for all $j \in J$ and since $e_{11'}e_{jj'}e_{1j'} \neq 0$ (5b) gives (6).

Now we calculate the left-hand side L of (7). We have

$$\begin{aligned} \mathrm{L} &= \sum_{\substack{i,j\in J\\ i<j}} (e_{ij}x_i^m x_j^m + e_{ij'}x_i^m \bar{x}_j^m + e_{i'j}\bar{x}_i^m x_j^m + e_{i'j'}\bar{x}_i^m \bar{x}_j^m) + \sum_{i\in J} e_{ii'}x_i^m \bar{x}_i^m \\ &= \sum_{\substack{i,j\in J\\ i<j,\, e_{ij}\neq 0}} 2(cx_i^m x_j^m + \bar{c}\bar{x}_i^m \bar{x}_j^m) + \sum_{\substack{i,j\in J\\ e_{ij'}\neq 0}} (c+\bar{c})x_i^m \bar{x}_j^m. \end{aligned}$$

Hence

$$\mathrm{L} = (c+\bar{c})\Big|\sum_{i\in J} x_i^m\Big|^2 - (c+\bar{c})\sum_{\substack{i,j\in J\\ e_{ij'}=0}} x_i^m \bar{x}_j^m + 2\sum_{\substack{i,j\in J\\ i<j,\, e_{ij}\neq 0}} (cx_i^m x_j^m + \bar{c}\bar{x}_i^m \bar{x}_j^m).$$

By Lemmata 3 and 4 for $i, j \in J$ the conditions $e_{ij'} = 0$ and $e_{ij} \neq 0$ are equivalent, thus we get (7).

LEMMA 6. *Under condition* (*) *of Theorem* 1B *we have* $J_i = J$ *for* $i \in J$.

Proof. By Lemma 4 we have $e_{ij} = 0$ if $i \in J\cup J'$, $j \notin J\cup J'$, hence

$$T_m(X) = \sum_{\substack{i,j\in J\cup J'\\ i<j}} e_{ij}x_i^m x_j^m + \sum_{\substack{i,j\notin J\cup J'\\ i<j}} e_{ij}x_i^m x_j^m. \tag{8}$$

Now by Lemma 5

$$\begin{aligned} \sum_{\substack{i,j\in J\cup J'\\ i<j}} e_{ij}x_i^m x_j^m &= (c+\bar{c})\Big|\sum_{i\in J} x_i^m\Big|^2 \\ &\quad + \sum_{\substack{i,j\\ i<j,\, e_{i'j}=0}} [2(cx_i^m x_j^m + \bar{c}\bar{x}_i^m \bar{x}_j^m) - (c+\bar{c})(x_i^m \bar{x}_j^m + \bar{x}_i^m x_j^m)] \\ &= \Sigma_1 + \Sigma_2. \end{aligned} \tag{9}$$

Let $i, j \in J$ and $j \notin J_i$. Since $j \in J\cup J'$ we have $j \in J_i'$. This means that there is a $g \in G$ such that $ga = a_i$, $g\bar{a} = a_j$. For this g we have $gc = c_i$, $g\bar{c} = c_j$. Since $c_i = c_j$ by (6) it follows that $c = \bar{c}$. Hence by (6) and Corollary 2.1

$$0 < c = c_k \quad (k \in J) \tag{10}$$

and for the second sum Σ_2 on the right-hand side of (9) we get

$$\Sigma_2 = 2c \sum_{\substack{i,j\in J\\ i<j,\, j\notin J_i}} (x_i^m - \bar{x}_i^m)(x_j^m - \bar{x}_j^m). \tag{11}$$

If $J_i \neq J$ the above sum is non empty; let for instance $j_0 \notin J_{i_0}$. We take $\theta_{i_0}, \theta_{j_0}$ with $\theta_{i_0}^m = \theta_{j_0}^m = \sqrt{-1}$, $\theta_{i_0'} = \bar{\theta}_{i_0}$, $\theta_{j_0'} = \bar{\theta}_{j_0}$. Next we choose θ_1 such that $\theta_1^m + 2\sqrt{-1} = 0$, $\theta_{1'} = \bar{\theta}_1$ and put $\theta_k = 0$ for all $k \neq 1, 1', i_0, i_0', j_0, j_0'$. Then $\theta = (\theta_1, \ldots, \theta_n) \in W$ and by (8), (9), (10) and (11) $T_m(\theta) = 2c(\sqrt{-1})^2 = -2c < 0$. Now using Lemma 2 we get a contradiction with condition (*) of Theorem 1B.

COROLLARY 6.1. *Under the assumptions of Lemma* 6

$$\sum_{\substack{i,j\in J\cup J'\\ i<j}} e_{ij}x_i^m x_j^m = (c+\bar{c})\Big|\sum_{i\in J} x_i^m\Big|^2.$$

Proof. The above formula follows from (7), since by Lemma 6 the second sum on the right-hand side of (7) is empty.

LEMMA 7. *Let* $A = \{a_i\colon i \in J\}$, $A' = \{a_i\colon i \in J'\}$. *Under the condition* (*) *of Theorem* 1B *the sets* A *and* $A\cup A'$ *are blocks of imprimitivity of the group* G *represented as a permutation group on* $\{a_1, \ldots, a_n\}$.

Proof. By Lemma 6 we have

(12) for every $\beta \in A$ and $\gamma \in \{a_1, \ldots, a_n\}$ the relations $(\beta, \bar{\gamma}) \in S$ and $\gamma \in A$ are equivalent.

On the other hand to prove that a finite set B is a block of imprimitivity of the group G we need only to show that $gB \cap B \neq \emptyset$ implies $gB \subset B$ for all $g \in G$. Then $gB = B$ since B is finite. We suppose that for a $g \in G$ we have $gA \cap A \neq \emptyset$. Let β be an element of A such that $g\beta \in A$. Since $(\beta, \bar{\beta}) \in S$ we get $(\overline{g\beta}, \overline{g\bar{\beta}}) \in S$. Using (12) we obtain $\overline{g\bar{\beta}} \in A$, $g\bar{\beta} \in A'$. Let γ be an arbitrary element of A. Then $(\gamma, \bar{\beta}) \in S$ implies $(g\gamma, g\bar{\beta}) \in S$. By (12) with β replaced by $\overline{g\bar{\beta}}$ we get $g\gamma \in A$. We have proved that $gA \cap A \neq \emptyset$ implies $gA \subset A$.

Now we assume that for a $g \in G$ we have $g(A\cup A') \cap (A\cup A') \neq \emptyset$. Then there is a $\beta \in A\cup A'$ with $g\beta \in A\cup A'$. Without loss of generality we can assume $\beta \in A$. For every $\gamma \in A$ we have $g\gamma \in A$ because A is a block of imprimitivity of G and *a fortiori* $g\gamma \in A\cup A'$. Assume that $\delta \in A'$.

If $g\beta \in A$ then from $(\beta, \delta) \in S$ it follows that $(g\beta, g\delta) \in S$ and by (12) we obtain $g\delta \in A'$. If $g\beta \in A'$ then since $(\overline{g\beta}, \overline{g\delta}) \in S$ using (12) we get $g\delta \in A$. Thus

$$g(A \cup A') \cap (A \cup A') \neq \emptyset \quad \text{implies} \quad g(A \cup A') \subset A \cup A'.$$

COROLLARY 7.1. *Let A and A' be defined as in Lemma 7, $q = \frac{1}{2}\frac{n}{\# A}$ and let h be an unit element of G. Under the condition $(*)$ of Theorem 1B*

(a) *there are elements $h_1 = h, h_2, \ldots, h_q$ of G such that $\{h_p(A \cup A'): p \leqslant q\}$ is a decomposition of $\{a_1, \ldots, a_n\}$ into disjoint subsets.*

(b) *If for some $p, r: 1 \leqslant p \leqslant q, 1 \leqslant r \leqslant q$,*

$$h'_p(A \cup A') \cap h_r(A \cup A') \neq \emptyset$$

then either $h'_p A = h_r A$ and $h'_p A' = h_r A'$ or $h'_p A = h_r A'$ and $h'_p A' = h_r A$ (h'_p is defined by the equality $h_p\beta = \overline{h_p\beta}$ for $\beta \in K$).

Proof. (a) This is a direct consequence of Lemma 7 since by Corollary 3.1

$$\#(A \cup A') = \#(J \cup J') = 2 \# J = 2 \# A.$$

(b) By Lemma 7 and the assumption we have

$$h'_p A \cup h'_p A' = h_r A \cup h_r A'. \tag{13}$$

Hence $h'_p A \cap h_r A \neq \emptyset$ or $h'_p A \cap h_r A' \neq \emptyset$. By Lemma 7 it follows that $h'_p A = h_r A$ or $h'_p A = h_r A'$ respectively.

Substituting this into (13) and using

$$h'_p A \cap h'_p A' = h'_p(A \cap A') = \emptyset = h_r(A \cap A') = h_r A \cap h_r A'$$

we obtain also $h'_p A' = h_r A'$ or $h'_p A' = h_r A$ respectively.

LEMMA 8. *Let h_p $(p \leqslant q)$ have the meaning of Corollary 7.1 and for $i \leqslant n$ let $h_p(i)$ denote the unique index h such that $a_h = h_p a_i$. Under the condition $(*)$ of Theorem 1B we have*

$$T_m(X) = \sum_{p=1}^{q} h_p(c+\bar{c}) \sum_{i\in J} (x_{h_p(i)})^m \sum_{i\in J} (x_{h_p(i')})^m \tag{14}$$

Moreover $c+\bar{c}$ is totally positive.

Proof. (14) follows from Corollary 6.1 and Corollary 7.1(a).

If for some $p \leqslant q$ we had $h_p(c+\bar{c}) < 0$ then taking

$$\theta_k = \begin{cases} 1 & \text{for } k = h_p(1), h_p(1'), h'_p(1), h'_p(1'), \\ 0 & \text{otherwise} \end{cases}$$

we should obtain $\theta = (\theta_1, \ldots, \theta_n) \in W$, $T_m(\theta) = h_p(c+\bar{c}) < 0$ and using

Lemma 2 we should get a contradiction with the condition $(*)$ of Theorem 1B. Hence

$$h_p(c+\bar{c}) > 0 \quad \text{if} \quad h_p(c+\bar{c}) \text{ is real, } 1 \leqslant p \leqslant q. \tag{15}$$

From $\operatorname{Re} c \neq 0$, (6) and (15) it follows that $c+\bar{c}$ is totally positive.

LEMMA 9. *Let in the notation of Corollary 7.1*

$$I = \{1, \ldots, q\}, \quad I_1 = \{p \in I: h_p A' = h'_p A\},$$

$$I_2 = \{p \in I - I_1: h_p\beta = h'_p\beta \text{ for all } \beta \in (A \cup A')\}.$$

Then under the condition $(*)$ of Theorem 1B

$$I = I_1 \cup I_2 \tag{16a}$$

and if m is odd,

$$I = I_1. \tag{16b}$$

Proof. By Corollary 7.1 for every $p \leqslant q$ there exists a unique $p_* \leqslant q$ such that $h'_p(A \cup A') = h_{p_*}(A \cup A')$ and for all $r \leqslant q$, $r \neq p_*$ we have $h_r(A \cup A') \cap h_{p_*}(A \cup A') = \emptyset$.

If $p = p_*$ then using Corollary 7.1(b) we have

$$h_p A' = h'_p A \text{ and } h'_p A' = h_p A \quad \text{or} \quad h'_p A = h_p A \text{ and } h'_p A' = h_p A'.$$

In the first case $p \in I_1$, in the second case by Lemma 3 we infer that all elements of $h_p(A \cup A')$ are real, thus $p \in I_2$. Hence if $p \in I - (I_1 \cup I_2)$ we have $p \neq p_*$ and

$$h_{p_*}(A \cup A') \cap h_p(A \cup A') = \emptyset.$$

Since $c \in K = Q(a)$ we can write $c = w(a)$, where $w(x) \in Q[x]$. By (6) $c = w(a_i)$ and $\bar{c} = w(\bar{a}_i)$; $i \in J$. Then

$$\begin{aligned} h'_p(c+\bar{c}) &= w(h'_p a) + w(h'_p \bar{a}) = w(\bar{a}_{h_p(i)}) + w(\bar{a}_{h_p(i')}) \\ &= h_{p_*} c + h_{p_*} \bar{c} = h_{p_*}(c+\bar{c}), \end{aligned}$$

because by Corollary 7.1(b) either $\bar{a}_{h_p(1)} \in h_{p_*} A$ and $\bar{a}_{h_p(1')} \in h_{p_*} A'$ or $\bar{a}_{h_p(1)} \in h_{p_*} A'$ and $\bar{a}_{h_p(1')} h_{p_*} A$. Now by (14)

$$\begin{aligned} T_m(X) = (c+\bar{c}) \Big| \sum_{i\in J} x_i^m \Big|^2 &+ h_p(c+\bar{c}) \sum_{i\in J} (x_{h_p(i)})^m \sum_{i\in J} (x_{h_p(i')})^m + \\ &+ h_{p_*}(c+\bar{c}) \sum_{i\in J} (x_{h_p(i)})^m \sum_{i\in J} (x_{h_p(i')})^m + T_m^{(1)}(X), \end{aligned}$$

where every term of $T_m^{(1)}(X)$ contains a factor x_k with $k \neq i, i', h_p(i)$, $h_p(i')$, $h'_p(i)$, $h'_p(i')$ $(i \in J)$. Since the sums $\sum_{i\in J} (x_{h_p(i)})^m$, $\sum_{i\in J} (x_{h_p(i')})^m$ are equal in some order to

$$\sum_{i\in J} (\bar{x}_{h_p(i)})^m, \quad \sum_{i\in J} (\bar{x}_{h_p(i')})^m$$

we get

$$T_m(X) = (c+\bar{c})\Big|\sum_{i\in J} x_i^m\Big|^2 + 2\Big(\operatorname{Re} h_p(c+\bar{c})\sum_{i\in J}(x_{h_p(i)})^m \sum_{i\in J}(x_{h_p(i')})^m\Big) + T_m^{(1)}(X).$$

We note that $h'_p(A\cup A')\cap h_p(A\cup A') = \emptyset$ implies that $a_{h_p(1)}$ is not real. We choose a complex number $\theta_{h_p(1)}$ such that $\theta^m_{h_p(1)} = -h'_p(c+\bar{c})$ and set $\theta_{h'_p(1)} = \bar{\theta}_{h_p(1)}$. Then we take $\theta_{h_p(1')} = \theta_{h'_p(1')} = 1$ and put $\theta_k = 0$ for all $k \neq h_p(1), h_p(1'), h'_p(1), h'_p(1')$. We get

$$\theta = (\theta_1, \ldots, \theta_n) \in W \quad \text{and} \quad T_m(\theta) = -2\,|h_p(c+\bar{c})|^2 < 0.$$

Lemma 2 gives a contradiction with the assumption $(*)$ of Theorem 1B. Therefore there is no $p\in I-(I_1\cup I_2)$, which shows (16a).

In order to show (16b) assume that m is odd and that $p\in I_2$. The pth term of the sum on the right-hand side of (14) is

$$h_p(c+\bar{c})\sum_{i\in J} x^m_{h_p(i)} \sum_{i\in J} x^m_{h_p(i')}.$$

For $X\in W$ all variables occurring above are real. Taking

$$\theta_k = \begin{cases} -1 & \text{if } k = h_p(1),\\ 1 & \text{if } k = h_p(1'),\\ 0 & \text{otherwise}\end{cases}$$

we get $\theta = (\theta_1, \ldots, \theta_n)\in W$ and $T_m(\theta) = -h_p(c+\bar{c}) < 0$, which by Lemmata 2 and 8 gives a contradiction with the condition $(*)$ of Theorem 1B.

LEMMA 10. *If B is a block of imprimitivity of G represented as a permutation group on $\{a_1, \ldots, a_n\}$ then there exists a subfield M of K such that B is the set of conjugates of a over M. Moreover M is the subfield of K fixed by all elements of G that transform B into itself.*

Proof. See [4], p. 183 and 233.

We prove

LEMMA 11. *Under the conditions* (i)–(iii) *of Theorem* 1B *for all $\beta\in K$ and all $c\in K_1$ we have the equality*

$$\operatorname{Tr}_{K\bar{K}/Q}(c\beta\bar{\beta}) = \operatorname{Tr}_{K_0/Q}\big((c+\bar{c})\,|\operatorname{Tr}_{K/K_1}\beta|^2\big).$$

Proof. Let $\gamma\in K_1$ be a generator of the extension K_1/K_0 and let $\{\gamma_1 = \gamma, \gamma_2, \ldots, \gamma_k\}$ be the set of all $k = [K\colon K_1]$ conjugates of γ over K_1. Then $\bar{\gamma}, \bar{\gamma}_2, \ldots, \bar{\gamma}_k$ is the set of all conjugates of $\bar{\gamma}$ over $K_1 = \bar{K}_1$. Let us denote by G_1 the set of all embeddings of $K\bar{K}$ into C trivial on K_1. The action of an element of G_1 on $K\bar{K}$ is determined by its action on the pair $(\gamma, \bar{\gamma})$. Moreover for every $h\in G_1$ we have $hc = c$, $h\gamma\in\{\gamma, \gamma_2, \ldots, \gamma_k\}$ and $h\bar{\gamma}\in\{\bar{\gamma}, \bar{\gamma}_2, \ldots, \bar{\gamma}_k\}$.

We define S_1 as the set of all pairs $(h\gamma, h\bar{\gamma})$, where $h\in G_1$. This set has the following properties:

(a) $S_1 = \{(\gamma_i, \bar{\gamma}_j)\colon 1\leqslant i\leqslant k, 1\leqslant j\leqslant k\}$,

(b) If $(\gamma_i, \bar{\gamma}_j)\in S_1$ then there exists exactly one h in G_1 such that $h\gamma = \gamma_i$, $h\bar{\gamma} = \bar{\gamma}_j$.

In order to prove (a) let us denote by D_i the set $\{j\colon (\gamma_i, \bar{\gamma}_j)\in S_1\}$. By (ii) we have $D_1 = \{1, 2, \ldots, k\}$. Since $D_i = h_i D_1$ for some $h_i\in G_1$ we get $\# D_i = k$. On the other hand $D_i\subset\{1, 2, \ldots, k\}$ thus $D_i = D_1$ and (a) follows.

As to (b) it trivially follows from the identity

$$\{g\in G_1\colon g\gamma = \gamma,\ g\bar{\gamma} = \bar{\gamma}\} = \{\mathrm{Id}_{K\bar{K}}\}.$$

Each element β of K can be uniquely represented as $w(\gamma)$ with $w\in K_1[x]$, $\deg w < k$. Then $\bar{w}(\bar{\gamma}) = \overline{w(\gamma)}$ and $\bar{w}\in K_1[x]$. Hence for all $h\in G_1$ we have

$$hw(\gamma) = w(h\gamma) \quad\text{and}\quad h\bar{w}(\bar{\gamma}) = \bar{w}(h\bar{\gamma}).$$

By the definition of S_1 we have for $c\in K_1$

$$\operatorname{Tr}_{K\bar{K}/K_1}\big(cw(\gamma)\bar{w}(\bar{\gamma})\big) = \sum_{(\gamma_i,\bar{\gamma}_j)\in S_1} cw(\gamma_i)\bar{w}(\bar{\gamma}_j).$$

By the properties (a), (b) of S_1 we have further

$$\sum_{(\gamma_i,\bar{\gamma}_j)\in S_1} cw(\gamma_i)\bar{w}(\bar{\gamma}_j) = c\sum_{i=1}^{k} w(\gamma_i)\cdot\sum_{i=1}^{k}\bar{w}(\bar{\gamma}_i)$$
$$= c\Big|\sum_{i=1}^{n} w(\gamma_i)\Big|^2 = c\,|\operatorname{Tr}_{K/K_1}\beta|^2.$$

Since by (i) and (iii) K_1 is a complex quadratic extension of K_0 we have

$$|\operatorname{Tr}_{K/K_1}\beta|^2\in K_0.$$

Hence

$$\operatorname{Tr}_{K\bar{K}/K_0}(c\beta\bar{\beta}) = (c+\bar{c})\,|\operatorname{Tr}_{K/K_1}\beta|^2$$

and the lemma follows on applying the tower formula for trace.

Proof of Theorem 1B. We shall prove first the implication

$$(*) \to \text{(i)–(iv)}. \tag{17}$$

By Lemma 7 the sets A and $A\cup A'$ defined there are blocks of imprimitivity of the group G represented as a permutation group on $\{a_1, \ldots, a_n\}$. By Lemma 3 we have $A\cap A' = \emptyset$. By Lemma 10 there exist subfields of K, say L and M such that A is the set of conjugates of a with respect to L, $A\cup A'$ is the set of conjugates of a with respect to M. Hence

$$[K:L] = \# A = \# J = [K\bar{K}:\bar{K}]$$

because of formula (1d). Moreover L and M are the fields fixed by all the elements of G that transform A into itself or $A\cup A'$ into itself respectively. Hence

$$M\subset L \quad \text{and} \quad [L:M]=\frac{\#(A\cup A')}{\# A}=2.$$

Now M is a totally real field. Indeed for every $g\in G$ we have $g'(A\cup A') = g(A\cup A')$ by (16a), hence the complex conjugation fixes the field gM conjugate to M. It follows that $M\subset K_0$.

Since L is a quadratic extension of M we have $L=\bar{L}$, thus $L\subset K_1$. The sequence of inequalities

$$[K:K_1]\geqslant [K\bar{K}:\bar{K}]=[K:L]\geqslant [K:K_1]$$

implies that $K_1=L$ and $[K:K_1]=[K\bar{K}:\bar{K}]$, i.e. the condition (ii).

Furthermore by (6) $c\in K_1$ and by Lemma 8 $c+\bar{c}$ is totally positive, hence (iv).

In order to prove (i) let us observe that since

$$M\subset K_0\subset K_1=L \quad \text{and} \quad [L:M]=2 \tag{18}$$

we have either $M=K_0$ or $K_0=K_1$. The latter equality is impossible since it would imply K_1 real and $A=A'$ contrary to $A\cap A'=\emptyset$. Thus $M=K_0$ and (i) follows from (18).

It remains to show (iii). By Corollary 7.1 for every $g\in G$ we have $g=h_jh$, where $h(A\cup A')=A\cup A'$ and $hA=A$ or A'. If $j\in I_1$ then gK_1 is complex. Indeed, if gK_1 were real then $gA=g'A$, hence $h_jhA = h_j'hA$ and $h_j(A\cup A')\cap h_j'(A\cup A')\neq\emptyset$. From Corollary 7.1(b) and the condition $h_jA'=h_j'A$ it follows that $h_jA=h_j'A'$. This together with $hA=A$ or A' and $h_jhA=h_j'hA$ gives $A\cap A'\neq\emptyset$, a contradiction. Hence gK_1 is complex and by Lemma 9 the condition (iii) holds for m odd. For m even we have to consider embeddings $g=h_jh$ where $j\in I_2$, $h(A\cup A')=A\cup A'$. For such an embedding the extension gK/gK_0 is totally real over gK_0 since all elements of $g(A\cup A')=h_j(A\cup A')$ are real by the definition of I_2. Thus the proof of the implication (17) is complete and we proceed to the proof of the implication

$$\text{(i)–(iv)}\to(*).$$

By Lemma 11 we have

$$\mathrm{Tr}_{K\bar{K}/Q}(c\beta^m\bar{\beta}^m)=\mathrm{Tr}_{K_0/Q}\big((c+\bar{c})|\eta|^2\big) \tag{19}$$

where $\eta=\mathrm{Tr}_{K/K_1}(\beta^m)$.

We shall show that $|\eta|^2$ is either 0 or a totally positive element of K_0. If m is odd K_1 is by (iii) a totally complex quadratic extension of K_0 hence the latter assertion is true for every $|\gamma|^2$ with $\gamma\in K_1$. If m is even we have to use the definition of η. Let β_j $(j=1,2,\ldots,k)$ be the conjugates of β with respect to K_1 and let g be an embedding of K into C. By (iii) either gK_1 is real and gK/gK_0 is totally real over gK_0 or gK_1 is complex and gK/gK_0 is totally complex over gK_0.

In the first case $g\beta_i$ and $g\bar{\beta}_i$ are real for $i=1,2,\ldots,k$ hence $g\eta = \sum_{j=1}^{k} g(\beta_j)^m\geqslant 0$, $g\bar{\eta}=\sum_{j=1}^{k} g(\bar{\beta}_j)^m\geqslant 0$ and $g|\eta|^2=g\eta\cdot g\bar{\eta}\geqslant 0$.

In the second case gK_1/gK_0 is a complex quadratic extension. Since $\eta\in K_1$ the degree of η over K_0 is $\leqslant 2$ and $\{\eta,\bar{\eta}\}$ is the set of conjugates of η over K_0. Hence $\{g\eta, g\bar{\eta}\}$ is the set of conjugates of $g\eta$ over gK_0. Since gK_1 is complex and gK_0 is real, $g\eta$ and $\overline{g\eta}$ are all the conjugates of $g\eta$ over gK_0.

Thus we have $g\bar{\eta}=\overline{g\eta}$ and $g(\eta\bar{\eta})=|g\eta|^2\geqslant 0$. Since by (iv) $c+\bar{c}$ is totally positive we get from (19)

$$\mathrm{Tr}_{K\bar{K}/Q}(c\beta^m\bar{\beta}^m)\geqslant 0.$$

Now the proof of Theorem 1 is complete.

Proof of Theorem 2. We assume that $f=\sum_{j=1}^{t} c_jx^j\in K[x]$ has $\mathrm{Re}f\neq\text{const}$. Let r be the greatest index i such that $\mathrm{Re}\,c_i\neq 0$. We have $r\geqslant 1$ by our assumption $\mathrm{Re}f\neq\text{const}$.

Using Theorem 1 we can find $\beta_*\in K$ with $\mathrm{Tr}(c_r\beta_*^r\bar{\beta}_*^r)>0$. We shall choose $\beta=M\beta_*$, where M will be a large positive integer. If $i>r$ then $\mathrm{Tr}(c_i|M\beta_*|^{2i})=0$ by Theorem 1A. If $0<i<r$ then

$$\mathrm{Tr}(c_i|M\beta_*|^{2i})=M^{2i}\,\mathrm{Tr}(c_i|\beta_*|^{2i})\leqslant M^{2r-2}D,$$

where the constant D depends only on β_* and $c_0, c_1, \ldots, c_{r-1}$. We take

$$M>\left(\frac{rD}{\mathrm{Tr}(c_r|\beta_*|^{2r})}\right)^{1/2}.$$

Then

$$\mathrm{Tr}\,f\big((\beta\bar{\beta})^2\big)\geqslant M^{2r}\,\mathrm{Tr}(c_r|\beta_*|^{2r})-rDM^{2r-2}>0.$$

Proof of Theorem 3. By Theorem 1 either there is a $\beta\in K$ with $\mathrm{Tr}(\beta\bar{\beta})<0$ or the two distinguished subfields K_0 and K_1 satisfy the conditions stated in the part B of Theorem 1.

For such K_0, K_1, K the assumptions of Lemma 11 are satisfied, so for every $\beta\in K$

$$\mathrm{Tr}_{K\bar{K}/Q}(\beta\bar{\beta})=\mathrm{Tr}_{K_0/Q}(2\,|\mathrm{Tr}_{K/K_1}\beta|^2).$$

We take any $\beta_0\in K$, but $\beta_0\notin K_1$ and put

$$\beta=\beta_0-\frac{\mathrm{Tr}_{K/K_1}\beta_0}{[K:K_1]}.$$

By definition $\mathrm{Tr}_{K/K_1}(|\beta|^2) = 0$. Thus we have $\mathrm{Tr}_{K\bar{K}/Q}(|\beta|^2) = 0$, which completes the proof of Theorem 3.

Now we give an example showing that results like Theorem 1 and 2 are no longer true for polynomials $f(x) \in K\bar{K}[x]$.

EXAMPLE. K is a totally complex field of fourth degree, the normal closure of which has a symmetric Galois group G.

By the Dirichlet Unit Theorem we have a unit α, $|\alpha| > 1$ with conjugates α, $\bar{\alpha}$, α_2, $\bar{\alpha}_2$. Then $|\alpha\alpha_2| = |\alpha\bar{\alpha}_2| = 1$. Replacing if necessary α by α^m, where m is a large positive integer, we can assume that

$$(1+|\alpha|^2)(1+|\alpha_2|^2) > 17.$$

We put $d = 1+|\alpha|^2$. We shall use the following notations:

$$d_{11'} = 1+|\alpha|^2, \quad d_{22'} = 1+|\alpha_2|^2, \quad d_{12} = 1+\alpha\alpha_2, \quad d_{1'2'} = 1+\bar{\alpha}\bar{\alpha}_2,$$
$$d_{1'2} = 1+\bar{\alpha}\alpha_2, \quad d_{12'} = 1+\alpha\bar{\alpha}_2.$$

Since G is symmetric all d_{ij} are conjugate.

Let γ be a nonzero element of K, m be a positive integer and let $\{\gamma, \bar{\gamma}, \gamma_2, \bar{\gamma}_2\}$ be the set of all conjugates of γ. Then we can write:

$$\begin{aligned} d_{11'}\mathrm{Tr}(d|\gamma|^{2m}) &= |d_{11'}\gamma^m + d_{1'2}\gamma_2^m + d_{1'2'}\bar{\gamma}_2^m|^2 + \\ &\quad + (d_{11'}d_{22'} - |d_{1'2}|^2 - |d_{12}|^2)|\gamma_2|^{2m} - d_{1'2}d_{12}\gamma_2^{2m} - d_{12'}d_{1'2'}\bar{\gamma}_2^{2m} \\ &= |d_{11'}\gamma^m + d_{1'2}\gamma_2^m + d_{1'2'}\bar{\gamma}_2^m|^2 + (d_{11'}d_{22'} - |d_{1'2}|^2 - \\ &\quad - |d_{12}|^2)|\gamma_2|^{2m} + 2\mathrm{Re}(d_{1'2}d_{12}\gamma_2^m) \\ &\geqslant \big(d_{11'}d_{22'} - (|d_{12}| + |d_{1'2}|)^2\big)|\gamma_2|^{2m}. \end{aligned}$$

But $|d_{12}| = |1+\alpha\alpha_2| \leqslant 2$, $|d_{1'2}| = |1+\bar{\alpha}\alpha_2| \leqslant 2$ and $d_{11'}d_{22'} > 17$. Hence

$$\mathrm{Tr}(d|\gamma|^{2m}) \geqslant \frac{|\gamma_2|^{2m}}{1+|\alpha|^2} > 0.$$

References

[1] K. Győry, *Sur une classe des corps de nombres algebriques et ses applications*, Publ. Math. Debrecen 22 (1975), pp. 151–175.

[2] A. Schinzel, *Traces of polynomial in algebraic numbers*, K. Norske. Vidensk. Selsk. Skr. 6 (1975), pp. 1–3.

[3] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its application to number theory*, Math. Soc. Japan 1961.

[4] N. Tschebotaröw und H. Schwerdtfeger, *Grundzüge der Galoisschen Theorie*, Groningen, Djakarta 1950.

Received on 17.11.1978
and in revised form on 10.6.1980 (1111)

ACTA ARITHMETICA
XLI (1982)

On the density of some sets of primes connected with cyclotomic polynomials

by

J. Wójcik (Warszawa)

I proved in [6] a certain result (Theorem 3 of [6]) about the so-called Lehmer numbers:

$$P_n' = P_n(\alpha, \beta) = \begin{cases} (\alpha^n-\beta^n)/(\alpha-\beta) & \text{if } n \text{ is odd,} \\ (\alpha^n-\beta^n)/(\alpha^2-\beta^2) & \text{if } n \text{ is even,} \end{cases}$$

where α, β are roots of the trinomial $z^2-\sqrt{L}z+M$ and L, M are rational integers.

The result in question is the following:

THEOREM. *If α, β are different from zero and α/β is not a root of unity, then there exists a positive integer k_0 such that for every positive integer k divisible by k_0 and for all positive integers D and r where $(D, r) = 1$ and $r \equiv 1 \bmod (D, k)$ there exist infinitely many primes q satisfying the conditions: $q \equiv r \bmod D$, $q \equiv 1 \bmod k$, $q \mid P_{(q-1)/k}(\alpha, \beta)$.*

The Dirichlet density of this set of primes is equal to $\dfrac{wT}{k\varphi([k, D])}$, where w, T are given in (24) of [6].

$[k, D]$ denotes the least common multiple of k and D.

The main aim of this paper is to generalize and to refine the above theorem. We shall also prove Theorem 2, connected with Schinzel's Conjecture H.

The afore said conjecture H reads as follows:

H. *If $f_1, f_2, \ldots, f_k$ are irreducible polynomials with integral coefficients and the leading coefficients positive such that $f_1(x)\ldots f_k(x)$ has no constant factor > 1 then there exist infinitely many positive integers x such that $f_1(x), \ldots, f_k(x)$ are primes.*

Definitions and notation. The terminology and notation are taken from [6]. $F_n(x)$ denotes the nth cyclotomic polynomial, $F_n(x, y) = y^{\varphi(n)}F_n(x/y)$.