die im Beweis von Satz 5 in [2] hergeleitet wurde: Da

$$f(x) = x(1-x)^{a-1} \quad \text{für} \quad x \in [0, 1/a)$$

streng monoton wachsend und für $x \in (1/a, 1]$ streng monoton fallend ist, gibt es zu jedem $x \in (1/a, 1]$ genau ein $x_1 \in [0, 1/a)$, so daß

$$y = x(1-x)^{a-1} = x_1(1-x_1)^{a-1}$$

gilt. Damit folgt sofort

$$N(F_a;\ x) < N(F_a;\ x_1) = 1.$$

Für $a \in \boldsymbol{R} \setminus \boldsymbol{Q}$, $a > 1$, beweisen wir die obige Aussage mit Hilfe von Satz 6 in [2], der unter anderem besagt, daß $N(F';x) \leqslant N(F;x)$ für alle $x \in [0, 1]$ gilt, wenn F' aus F durch Vergrößerung eines Folgengliedes von F um 1 entsteht, ohne daß dabei die Monotoniebedingung verletzt wird.

Ist $x \in (1/a, 1]$, so gibt es $\varrho \in \boldsymbol{Q}$ mit $1/a < 1/\varrho < x$. Damit gilt einerseits nach dem oben Bewiesenen $N(F_\varrho;\ x) < 1$; andererseits ist $N(F_a;\ x) \leqslant N(F_\varrho; x)$, da wegen $[\varrho k]+c \leqslant [ak]+c$ für alle $k \in \boldsymbol{N}_0$ F_ϱ in F_a überführt werden kann, indem man sukzessive jeweils endlich viele oder unendlich viele aufeinanderfolgende Glieder um 1 erhöht.

In unserem Falle ist also $\sum\limits_{k=0}^{\infty} c_k(d-1)^k d^{-s_k} < 1$, wenn $1-\dfrac{1}{d} > \dfrac{\log d}{\log m}$, d.h. $m > d^{d/(d-1)}$ gilt. Da der Fall $m = d^{d/(d-1)}$ nicht eintreten kann, ist damit Satz 4 vollständig bewiesen.

Der Beweis von Satz 1 ergibt sich nun sofort aus (11) und Satz 4: Für $m < d^{d/(d-1)}$ ist $\delta^*(\mathscr{L}) \geqslant 1$, also wegen (8) $\delta^*(\mathscr{L}) = \bar{\delta}^*(\mathscr{L}) = 1$, so daß auch die natürliche Dichte von $\mathscr{L}$ existiert und gleich 1 ist.

Ergänzung bei Drucklegung. Der Beweis des Hauptergebnisses der anfangs erwähnten Arbeit [5] ist fehlerhaft.

Literaturverzeichnis

[1] K. Hensel, *Zahlentheorie*, Leipzig 1913.
[2] H. Möller, *F-Normalreihen*, J. Reine Angew. Math. 289(1977), S. 135–143.
[3] H.-H. Ostmann, *Additive Zahlentheorie I*, Berlin–Heidelberg–New York 1968.
[4] C. J. Everett, *Iteration of the number-theoretic function $f(2n) = n$, $f(2n+1) = 3n+1$*, Advances in Math. 25 (1977), S. 42–45.
[5] R. Terras, *A stopping time problem on the positive integers*, Acta Arith. 30 (1976), S. 241–252.

Eingegangen am 7. 9. 1976 (875)

ACTA ARITHMETICA
XXXIV (1978)

Reducibility of lacunary polynomials, III

by

A. Schinzel (Warszawa)

1. The present paper is a sequel to [11] and the notation of that paper is used throughout. All the polynomials considered are supposed to have integral coefficients unless stated to the contrary. Reducibility means reducibility over the rational field $\boldsymbol{Q}$.

If $f(x_1, \ldots, x_k) \neq 0$ is a polynomial then

$$f(x_1, \ldots, x_k) \overset{\text{can}}{=} \operatorname{const} \prod_{\sigma=1}^{s} f_\sigma(x_1, \ldots, x_k)^{e_\sigma}$$

means that the polynomials f_σ are irreducible and prime to each other.

If $\Phi(x_1, \ldots, x_k) = f(x_1, \ldots, x_k) \prod\limits_{i=1}^{k} x_i^{a_i}$, where f is a polynomial prime to $x_1 x_2 \ldots x_k$ and a_i are integers, then we set

$$J\Phi(x_1, \ldots, x_k) = f(x_1, \ldots, x_k).$$

A polynomial g such that

$$Jg(x_1^{-1}, \ldots, x_k^{-1}) = \pm g(x_1, \ldots, x_k)$$

is called *reciprocal*. Let

$$J\Phi(x_1, \ldots, x_k) \overset{\text{can}}{=} \operatorname{const} \prod_{\sigma=1}^{s} f_\sigma(x_1, \ldots, x_k)^{e_\sigma}.$$

We set

$$K\Phi(x_1, \ldots, x_k) = \operatorname{const} \Pi_1 f_\sigma(x_1, \ldots, x_k)^{e_\sigma},$$

$$L\Phi(x_1, \ldots, x_k) = \operatorname{const} \Pi_2 f_\sigma(x_1, \ldots, x_k)^{e_\sigma},$$

where Π_1 is extended over all f_σ that do not divide $J(x_1^{\delta_1} \ldots x_k^{\delta_k}-1)$ for any $[\delta_1, \ldots, \delta_k] \neq 0$, Π_2 is extended over all f_σ that are non-reciprocal. The leading coefficients of $K\Phi$ and $L\Phi$ are assumed equal to that of $J\Phi$. In particular for $k = 1$ $K\Phi(x)$ equals $J\Phi(x)$ deprived of all its cyclotomic factors and is called the kernel of Φ.

For a polynomial $F(x_1, \ldots, x_k)$, $\|F\|$ is the sum of squares of the coefficients of F; if $F \neq 0$, $|F|$ is the maximum of the degrees of F with respect to x_i $(1 \leqslant i \leqslant k)$, $\Omega(F)$ is the number of irreducible factors of F counted with multiplicities, $\exp_k$ and $\log_k$ denote the kth iteration of the exponential and the logarithmic function respectively. $\tau(n)$ is the number of divisors and $\Omega_0(n)$ the number of prime divisors of n counted with multiplicities.

The main object of [11] has been to describe the canonical factorization of $LF(x^{n_1}, \ldots, x^{n_k})$ for any fixed polynomial F and a variable integral vector $[n_1, \ldots, n_k]$. The much more difficult problem of describing the factorization of $KF(x^{n_1}, \ldots, x^{n_k})$ has been solved only for $k = 1$ and for $k = 2$ provided $KF(x_1, x_2) = LF(x_1, x_2)$, in particular if $F(x_1, x_2) = a_0 + a_1 x_1 + a_2 x_2$. For $k > 2$ even the simplest case $F(x_1, x_2, x_3) = a_0 + \sum_{j=1}^{3} a_j x_j$ $(n_1 < n_2 < n_3)$ has been settled only under very restrictive assumption about the a_j's (see [3]).

The aim of the present paper is to improve and to extend the above results in several ways. First, due to the recent progress made by Blanksby and Montgomery [1] and by Smyth [20] in the problem of distribution of the conjugates of an algebraic integer on the plane it has been possible to improve the result on $KF(x^n)$ mentioned above. We have

THEOREM 1. *For any polynomial $F(x) \neq 0$ such that $KF(x) \neq \mathrm{const}$ and for any positive integer n there exist positive integers ν and u such that*

(i) $\nu \mid c(F)$,

(ii) $n = u\nu$,

(iii) $KF(x^\nu) \overset{\mathrm{can}}{=} \mathrm{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma}$ *implies*

$$KF(x^n) \overset{\mathrm{can}}{=} \mathrm{const} \prod_{\sigma=1}^{s} F_\sigma(x^u)^{e_\sigma}.$$

Moreover,

$$\log c(F) \leqslant \left(|KF| \log(2|KF|) \log\|F\|\right)^{1/3} (\log 2|KF| + \log_2\|F\|)^{2/3}$$

and if $KF(x) = LF(x)$

$$\log c(F) \leqslant \sqrt{\frac{\log\|F\| \log_2\|F\|}{2 \log \vartheta_0}} + O\left(\sqrt{\log\|F\| \log_3\|F\|}\right),$$

where ϑ_0 is the real zero of $x^3 - x - 1$.

In any case

$$\Omega\left(KF(x^n)\right) = \sum_{\sigma=1}^{s} e_\sigma \leqslant \min\left(|KF|\tau(n),\ |KF|^{1+o(1)} \exp\left(\frac{\log 2 + o(1)}{\log_3\|F\|} \log_2\|F\|\right)\right).$$

Examples will be given to show that in the first of the estimates for $\log c(F)$ the exponent $1/3$ cannot be lowered, in the second the main term is best possible and the estimate for $\Omega\left(KF(x^n)\right)$ is sharp with respect to all three parameters involved n, $|KF|$ and $\|F\|$.

COROLLARY 1. *For any polynomial $F(x)$ such that $F(0) \neq 0$ and any n we have*

$$\Omega\left(F(x^n)\right) \leqslant |F| \tau(n).$$

COROLLARY 2. *For any binomial $b(x)$ we have*

$$\Omega\left(Kb(x)\right) \leqslant \exp\left(\frac{\log 2 + o(1)}{\log_3\|b\|} \log_2\|b\|\right).$$

COROLLARY 3. *For any trinomial $t(x)$ we have*

$$\Omega\left(Kt(x)\right) \leqslant \frac{\log\|t\|}{2 \log \vartheta_0 + o(1)}.$$

The corollaries are of interest because for a general polynomial $f(x)$ only $\Omega\left(Lf(x)\right)$ is known to be $O(\log\|f\|)$ and the estimates for $\Omega\left(Kf(x)\right)$ depend upon $|f|$ (see [15] and the Corollary to Lemma 1).

Coming back to [11] it is possible to improve also the estimates given there for the case $k > 1$. The improvements are however not drastic and the new estimates are probably still far from best possible, thus we shall not go into the matter. On the other hand using the result of E. Gourin [4] it is possible to describe the canonical factorization of $KF(x_1^{n_1}, \ldots, x_k^{n_k})$ for any k.

We have

THEOREM 2. *For any polynomial $F(x_1, \ldots, x_k) \neq 0$ and any positive integers $n_1, \ldots, n_k$ there exist positive integers $\nu_1, \ldots, \nu_k$ and $v_1, \ldots, v_k$ such that*

(iv) $\nu_j \mid c(F)$ $\quad (1 \leqslant j \leqslant k)$,

(v) $n_j = \nu_j v_j$ $\quad (1 \leqslant j \leqslant k)$,

(vi) $KF(x_1^{\nu_1}, \ldots, x_k^{\nu_k}) \overset{\mathrm{can}}{=} \mathrm{const} \prod_{\sigma=1}^{s} F_\sigma(x_1, \ldots, x_k)^{e_\sigma}$ *implies*

$$KF(x_1^{n_1}, \ldots, x_k^{n_k}) \overset{\mathrm{can}}{=} \mathrm{const} \prod_{\sigma=1}^{s} F_\sigma(x_1^{v_1}, \ldots, x_k^{v_k})^{e_\sigma}.$$

The constant $c(F) \neq 0$ is effectively computable.

This theorem is clearly stronger than its analogue with L in place of K announced in [13]. In the latter case it follows by the method of [11] that

$$\log c(F) \leqslant 9\cdot 2^{\|F\|-5};$$

it seems however that this estimate is far from the best possible.

Turning again to polynomials in one variable we shall obtain

THEOREM 3. *Let $k \geqslant 3$, a_j $(0 \leqslant j \leqslant k)$ be non-zero integers and $n_1 < n_2 < \ldots < n_k$ positive integers. Then either there exist integers γ_j $(1 \leqslant j \leqslant k)$ such that*

(vii) $\sum_{j=1}^{k} \gamma_j n_j = 0$

and

(viii) $0 < \max_{1\leqslant j\leqslant k} |\gamma_j| < \exp_{2k-4}\Big(k2^{\sum_{j=0}^{k} a_j^2+2} \log \sum_{j=0}^{k} a_j^2\Big)$

or all primitive irreducible factors of $f(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ except a single simple one are reciprocal and monic, moreover if

(ix) $|a_0| + |a_k| \geqslant \sum_{j=1}^{k-1} |a_j|$

they are cyclotomic and if for some g, $h \leqslant k$

(x) $a_g^2 \not\equiv a_h^2 \bmod \underset{0\leqslant j\leqslant k}{\text{g.c.d.}}\, a_j \cdot \underset{j\neq g,h}{\text{g.c.d.}}\, a_j$

none whatever.

Besides, (ix) *and* (x) *imply*

$$\Omega\big(Kf(x)/Lf(x)\big) \leqslant \Omega_0\big((a_0, a_k)\big) \quad \textit{and} \quad \Omega\big(f(x)/Lf(x)\big) \leqslant \Omega_0\big((a_0, a_k)\big),$$

respectively.

This is a refinement of Theorem 4 of [11]. A refinement in a different direction has been given in [14].

The last part of the paper is concerned with quadrinomials. Improving the results of [3] we shall prove

THEOREM 4. *Let a_j $(0 \leqslant j \leqslant 3)$ be non-zero integers and*

(xi) *either* $|a_0| + |a_3| \geqslant |a_1| + |a_2|$ *or for some* g, $h \leqslant 3$

$$a_g^2 \not\equiv a_h^2 \bmod \underset{0\leqslant j\leqslant 3}{\text{g.c.d.}}\, a_j \cdot \underset{j\neq g,h}{\text{g.c.d.}}\, a_j$$

or $|a_0| = |a_3|$, $|a_1| = |a_2|$.

Then for any quadrinomial $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ $(0 < n_1 < n_2 < n_3)$ that is not reciprocal we have one of the following four possibilities.

(xii) *$Kq(x)$ is irreducible.*

(xiii) *$q(x)$ can be divided into two parts that have the highest common factor $d(x)$ being a non-reciprocal binomial. $K\big(q(x)d^{-1}(x)\big)$ is then irreducible unless $q(x)d^{-1}(x)$ is a binomial.*

(xiv) *$q(x)$ can be represented in one of the forms*

$$
\begin{aligned}
&k(T^2 - 4TUVW - U^2V^4 - 4U^2W^4)\\
&\qquad = k(T - UV^2 - 2UVW - 2UW^2)(T + UV^2 - 2UVW + 2UW^2),\\
(1)\quad &k(U^3 + V^3 + W^3 - 3UVW)\\
&\qquad\qquad = k(U + V + W)(U^2 + V^2 + W^2 - UV - UW - VW),\\
&k(U^2 + 2UV + V^2 - W^2) = k(U + V + W)(U + V - W),
\end{aligned}
$$

where $k = \pm(a_0, a_1, a_2, a_3)$ and T, U, V, W are monomials in $\boldsymbol{Z}[x]$. The factors on the right hand side of (1) *have irreducible kernels.*

(xv) *$n_j = vv_j$ $(1 \leqslant j \leqslant 3)$; v and v_j are positive integers,*

$$v_3 < \exp_2(12\cdot 2^{\|q\|} \log \|q\|)$$

and $K(a_0 + \sum_{j=1}^{3} a_j x^{v_j})$ is reducible.

Moreover

$$K\Big(a_0 + \sum_{j=1}^{3} a_j x^{v_j}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma}$$

implies

$$Kq(x) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^v)^{e_\sigma}.$$

Besides

$$\Omega\big(q(x)\big) = \sum_{\sigma=1}^{s} e_\sigma \leqslant \left(\frac{1}{2\log\vartheta_0} + \frac{1}{2\log 2}\right)\log\|q\|.$$

The condition (xi) is fulfilled for about $82^0/_0$ of quadruples (a_0, a_1, a_2, a_3) of height $\leqslant H \to \infty$. Since a rule for obtaining the canonical factorization of binomials is contained in Theorem 1 (and a more practical one in Lemma 5 below), Theorem 4 gives a satisfactory description of the canonical factorization of the kernel of $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ $(0 < n_1 < n_2 < n_3)$ for all those quadruples (a_0, a_1, a_2, a_3) provided only $q(x)$ is not reciprocal.

The factorization of $q(x)/Kq(x)$ can be obtained easily by means of the results of Mann [8]. We content ourselves with stating the following

COROLLARY 4. *A non-reciprocal quadrinomial $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ $(0 < n_1 < n_2 < n_3)$ satisfying* (xi) *is reducible if and only if we have one of the conditions* (xii)–(xv) *or $q(x)$ can be divided into two parts with the highest common factor equal $x^\delta \pm 1$ or finally*

$$a_0 + \sum_{j=1}^{3} a_j \zeta^{n_j/(n_1,n_2,n_3)} = 0, \quad \textit{where} \quad \zeta^6 = 1.$$

A real enigma is the reducibility of reciprocal quadrinomials. A new idea seems to be needed even to solve the following simple

PROBLEM. *Given a, b with $|a| \neq |b|$ do there exist infinitely many quotients r such that for suitable integers m, n: $m/n = r$ and $K(ax^{m+n}+bx^{m}+$ $+bx^{n}+a)$ is reducible?*

The proofs of Theorems 1, 2, 3 and 4 are given in Sections 2, 3, 4, 5 respectively. Before proceeding to the proofs we call the attention of the reader to an error in [11] repeated also in [12]. At the bottom of p. 133 in [11] certain inequalities for determinants are said to follow from Hadamard's inequality. Now the inequalities in question are true but need not follow from Hadamard's inequality. A detailed explanation is given at the end of the present paper.

2. In addition to the notation introduced in § 1 we shall use the following: ζ_q is a primitive root of unity of degree q, X_q is the qth cyclotomic polynomial.

If $\boldsymbol{\Omega}$ is a field and $\alpha \in \boldsymbol{\Omega}$, $\alpha \neq 0$, then

$$e(\alpha, \boldsymbol{\Omega}) = \begin{cases} 0 \quad \text{if } \alpha = \zeta_q \text{ for some } q, \\ \text{maximal } e \text{ such that } \alpha = \zeta_q \beta^e \text{ with some } q \text{ and } \beta \in \boldsymbol{\Omega} \\ \hfill \text{otherwise;} \end{cases}$$

$$E(\alpha, \boldsymbol{\Omega}) = \begin{cases} 0 \quad \text{if } \alpha = \zeta_q \text{ for some } q, \\ \text{maximal } n \text{ such that } \alpha = \vartheta^n,\ \vartheta \in \boldsymbol{\Omega}(\zeta_n) \quad \text{otherwise.} \end{cases}$$

For a given polynomial $f = \sum_{j=0}^{k} a_j x^j$

$$l(f) = \sum_{j=0}^{|k|} |a_j|, \qquad C(f) = (a_0, a_1, \ldots, a_k).$$

Small bold face letters denote vectors, capital bold face letters denote matrices except $\boldsymbol{Q}, \boldsymbol{C}$ and $\boldsymbol{\Omega}$ that are fields and $\boldsymbol{Z}$ that is the ring of integers. N_{Ω_2/Ω_1} is the norm from Ω_2 to Ω_1 or from $\Omega_2(x)$ to $\Omega_1(x)$.

LEMMA 1. *Let α_i $(i = 1, \ldots, \varrho)$ be a system of pairwise not conjugate zeros of Kf, where f is a polynomial and let ε_i be the multiplicity of α_i. Then*

$$\sum_{i=1}^{\varrho} \varepsilon_i \sqrt{e\big(\alpha_i, \boldsymbol{Q}(\alpha_i)\big)} \leqslant \sqrt{26\,|Kf|\log(7\,|Kf|)\log\|f\|}\,, \tag{2}$$

$$\sum{}' \varepsilon_i e\big(\alpha_i, \boldsymbol{Q}(\alpha_i)\big) \leqslant \frac{\log\|f\|}{2\log\vartheta_0}, \tag{2'}$$

where the sum $\sum'$ is taken over all α_i not conjugate to α_i^{-1} and ϑ_0 is the real zero of x^3-x-1.

Proof. Let us consider the product

$$P = |a_0| \prod_{f(\alpha)=0,\, |\alpha|>1} |\alpha|,$$

where a_0 is the leading coefficient of f. By the inequality of Landau [6]

$$P < \|f\|^{1/2}. \tag{3}$$

On the other hand, let

$$Kf(x) \overset{\text{can}}{=} c \prod_{i=1}^{\varrho} f_i^{\varepsilon_i}(x),$$

where $f_i(\alpha_i) = 0$ and f_i is primitive. We have

$$P = c \prod_{i=1}^{\varrho} |a_i|^{\varepsilon_i} \prod_{|\alpha_i^{(j)}|>1} |\alpha_i^{(j)}|^{\varepsilon_i}, \tag{4}$$

where $\alpha_i^{(j)}$ runs over the conjugates of α_i and a_i is the leading coefficient of f_i. We shall show that

$$|a_i| \prod_{|\alpha_i^{(j)}|>1} |\alpha_i^{(j)}| > \begin{cases} \exp \dfrac{e\big(\alpha_i, \boldsymbol{Q}(\alpha_i)\big)}{52\,|f_i|\log 7\,|f_i|} \quad \text{always,} \\ \vartheta_0^{e(\alpha_i, \boldsymbol{Q}(\alpha_i))} \quad \text{if } \alpha_i \text{ is not conjugate to } \alpha_i^{-1}. \end{cases} \tag{5}$$

Since α_i is not a root of unity, we have by the definition of $e\big(\alpha_i, \boldsymbol{Q}(\alpha_i)\big)$

$$\alpha_i = \zeta_q \beta^e, \quad \beta \in \boldsymbol{Q}(\alpha_i), \quad e = e\big(\alpha_i, \boldsymbol{Q}(\alpha_i)\big). \tag{6}$$

If a_i is not an integer we use an argument due to J. Wójcik and set $\alpha_i = \mu/\nu$, $(\mu) = \mathfrak{d}\mathfrak{m}$, $(\nu) = \mathfrak{d}\mathfrak{n}$, where $\mathfrak{d}, \mathfrak{m}, \mathfrak{n}$ are ideals of $\boldsymbol{Q}(\alpha_i)$ and $(\mathfrak{m}, \mathfrak{n}) = 1$. By Gauss's Lemma the polynomial $N(\mathfrak{d})^{-1} \prod_{j=1}^{|f_i|} (\nu^{(j)} x - \mu^{(j)})$ is primitive, N denoting the norm from $\boldsymbol{Q}(\alpha_i)$ to $\boldsymbol{Q}$. Since it is also irreducible it coincides with f_i up to a sign.

It follows that

$$a_i = \pm N\mathfrak{d}^{-1} N\nu = \pm N\mathfrak{n}.$$

By (6) $\mathfrak{n} = \mathfrak{r}^e$ and $|a_i| = N\mathfrak{r}^e \geqslant 2^e$ thus (5) holds. If a_i is an integer β is also. We have

$$\prod_{|\alpha_i^{(j)}|>1} |\alpha_i^{(j)}| = \prod_{|\beta_i^{(j)}|>1} |\beta_i^{(j)}|^e. \tag{7}$$

By the theorem of Blanksby and Montgomery [1]

$$\prod_{|\beta_i^{(j)}|>1} |\beta_i^{(j)}| > 1+\frac{1}{52\,|f_i|\log 6\,|f_i|} > \exp\left(\frac{1}{52\,|f_i|\log 6\,|f_i|+1}\right)$$
$$> \exp\left(\frac{1}{52\,|f_i|\log 7\,|f_i|}\right),$$

which together with (7) gives the first part of (5).

If α_i is not conjugate to α_i^{-1} then by the result of [18] applied with $\boldsymbol{K}=\boldsymbol{Q}$, $\zeta_q^r\beta$ is not conjugate to $\zeta_q^{-r}\beta^{-1}$ for a suitable r. By Smyth's theorem [20]

$$\prod_{|\beta^{(j)}|>1} |\beta^{(j)}| = \prod_{|\beta^{(j)}|>1} |(\zeta_q^r\beta)^{(j)}| \geqslant \vartheta_0,$$

which together with (7) gives the second part of (5).

Now (3), (4) and (5) give

$$\sum_{i=1}^{\varrho} \varepsilon_i \frac{e\big(\alpha_i, \boldsymbol{Q}(\alpha_i)\big)}{52\,|f_i|\log 7\,|f_i|} < \tfrac{1}{2}\log\|f\|, \tag{8}$$
$$\sum{}' \varepsilon_i e\big(\alpha_i, \boldsymbol{Q}(\alpha_i)\big) < \frac{\log\|f\|}{2\log\vartheta_0}.$$

The inequality (2′) follows at once. In order to prove (2) let us notice that

$$\sum_{i=1}^{\varrho} 52\,|f_i|\log 7\,|f_i| \leqslant 52\,|Kf|\log 7\,|Kf|.$$

Since

$$\varepsilon_i\sqrt{e\big(\alpha_i, \boldsymbol{Q}(\alpha_i)\big)} = \sqrt{\frac{e\big(\alpha_i, \boldsymbol{Q}(\alpha_i)\big)\,\varepsilon_i}{52\,|f_i|\log 7\,|f_i|}}\cdot\sqrt{52\,\varepsilon_i\,|f_i|\log 7\,|f_i|}$$

(2) follows from (8) by the Schwarz inequality.

Corollary. *We have*

$$\Omega(Kf) < \sqrt{26\,|Kf|\log(7\,|Kf|)\log\|f\|},$$
$$\Omega(Lf) < \frac{\log\|f\|}{2\log\vartheta_0}.$$

Remark. The bound given in (2) cannot be improved as it is shown by the example

$$\begin{aligned} f_m(x) &= N_{\boldsymbol{Q}(\vartheta_0)/\boldsymbol{Q}}(x-\vartheta_0^m) \\ &= x^3-(\vartheta_0^m+\vartheta_1^m+\vartheta_2^m)x^2+(\vartheta_0^{-m}+\vartheta_1^{-m}+\vartheta_2^{-m})x-1, \end{aligned} \tag{9}$$

where ϑ_1, ϑ_2 are the two conjugates of ϑ_0.

Clearly $e\big(\vartheta_0^m, \boldsymbol{Q}(\vartheta_0)\big) \geqslant m$. On the other hand, since $|\vartheta_1| = |\vartheta_2| = |\vartheta_0|^{-1/2}$,

$$\begin{aligned} \log\|f_m\| &= \log\big(2+(\vartheta_0^m+\vartheta_1^m+\vartheta_2^m)^2+(\vartheta_0^{-m}+\vartheta_1^{-m}+\vartheta_2^{-m})^2\big) \\ &= \log\big(\vartheta_0^{2m}+O(\vartheta_0^m)\big) = 2m\log\vartheta_0+O(\vartheta_0^{-m}). \end{aligned}$$

For further reference note that similarly

$$\log l(f_m) = m\log\vartheta_0+O(\vartheta_0^{-m/2}). \tag{10}$$

Lemma 2. *For any algebraic number field $\boldsymbol{\Omega}$ and any $\alpha\in\boldsymbol{\Omega}$, $\alpha\neq 0$, we have*

$$E(\alpha, \boldsymbol{\Omega})\,|\,e(\alpha, \boldsymbol{\Omega})\Big(w(\boldsymbol{\Omega}),\, 2\operatorname*{l.c.m.}_{\substack{p|e(\alpha,\Omega)\\ p\text{ prime}}}(p-1)\Big), \tag{11}$$

where $w(\boldsymbol{\Omega})$ is the number of roots of unity contained in $\boldsymbol{\Omega}$. Moreover, if $\alpha=\beta^m$, $\beta\in\boldsymbol{\Omega}_1\subset\boldsymbol{\Omega}(\zeta_m)$, then

$$mE(\beta, \boldsymbol{\Omega}_1)\,|\,E(\alpha, \boldsymbol{\Omega}). \tag{12}$$

Proof. The equality

$$\alpha = \vartheta^n, \quad \vartheta\in\boldsymbol{\Omega}(\zeta_n) \tag{13}$$

implies by Theorem 3 of [16]

$$\alpha^\sigma = \gamma^n, \quad \gamma\in\boldsymbol{\Omega},$$

where

$$\sigma = \Big(n,\, w(\boldsymbol{\Omega}),\, \operatorname*{l.c.m.}_{\substack{q|n\\ q\text{ prime or }q=4}}[\boldsymbol{\Omega}(\zeta_q):\boldsymbol{\Omega}]\Big). \tag{14}$$

Hence by Lemma 1 of [10]

$$n\,|\,e(\alpha, \boldsymbol{\Omega})\sigma \tag{15}$$

and by (14)

$$n\,|\,e(\alpha, \boldsymbol{\Omega})w(\boldsymbol{\Omega}).$$

It follows that if $e(\alpha, \boldsymbol{\Omega})\neq 0$, i.e. α is not a root of unity, there are only finitely many n satisfying (13). The greatest of them $E(\alpha, \boldsymbol{\Omega}) = E$ satisfies by (14) and (15)

$$E\,|\,e(\alpha, \boldsymbol{\Omega})w(\boldsymbol{\Omega}), \tag{16}$$
$$E\,|\,e(\alpha, \boldsymbol{\Omega})\operatorname*{l.c.m.}_{\substack{q|e(\alpha,\Omega)w(\Omega)\\ q\text{ prime or }q=4}}[\boldsymbol{\Omega}(\zeta_q):\boldsymbol{\Omega}]. \tag{17}$$

However, if $q\,|\,w(\boldsymbol{\Omega})$ then $[\boldsymbol{\Omega}(\zeta_q):\boldsymbol{\Omega}] = 1$, thus those factors q contribute nothing to $\text{l.c.m.}[\boldsymbol{\Omega}(\zeta_q):\boldsymbol{\Omega}]$ occurring in (17). It is enough therefore to consider $q\,|\,2e(\alpha, \boldsymbol{\Omega})$.

For q being a prime we have

$$[\boldsymbol{\Omega}(\zeta_q):\boldsymbol{\Omega}] = \frac{[\boldsymbol{Q}(\zeta_q):\boldsymbol{Q}]}{[\boldsymbol{\Omega}\cap\boldsymbol{Q}(\zeta_q):\boldsymbol{Q}]} \,\Big|\, q-1.$$

For $q = 4$ the degree $[\boldsymbol{\Omega}(\zeta_q):\boldsymbol{\Omega}]$ divides 2. Thus if $e(\alpha, \boldsymbol{\Omega}) \neq 0$ (11) follows from (16) and (17). If $e(\alpha, \boldsymbol{\Omega}) = 0$ (11) is obvious, as is (12) if $E(\alpha, \boldsymbol{\Omega}) = 0$. If $E(\alpha, \boldsymbol{\Omega}) \neq 0$ α is not a root of unity, hence by Lemma 1 of [10] $0 \neq e(\alpha, \boldsymbol{\Omega}_1) = me(\beta, \boldsymbol{\Omega}_1)$, and by (11) applied to β and $\boldsymbol{\Omega}_1$

$$E_1 = E(\beta, \boldsymbol{\Omega}_1) \neq 0.$$

If

$$\beta = \vartheta_1^{E_1}, \qquad \vartheta_1 \in \boldsymbol{\Omega}_1(\zeta_{E_1})$$

and r, s are rational integers satisfying

$$rE+smE_1 = (E, mE_1)$$

we get from (13) with $n = E$ and from $\alpha = \vartheta_1^{mE_1}$ the equality

$$\alpha = (\vartheta^s\vartheta_1^r)^{[E,mE_1]}, \qquad \vartheta^s\vartheta_1^r \in \boldsymbol{\Omega}(\zeta_{[E,mE_1]}).$$

By the definition of E this implies $[E, mE_1] \leqslant E$, hence $E \equiv 0 \bmod mE_1$.

Lemma 3. *Let $\boldsymbol{\Omega}$ be an algebraic number field and $\alpha \in \boldsymbol{\Omega}$, $\alpha \neq 0$. For every positive integer n we put*

$$\nu = \big(n, E(\alpha, \boldsymbol{\Omega})\big).$$

If $g(x) \in \boldsymbol{\Omega}[x]$ is a monic polynomial irreducible over $\boldsymbol{\Omega}$ and $g(x) \mid x^n-\alpha$, then $g(x) = G(x^{n/\nu})$, where $G(x)$ is a polynomial over $\boldsymbol{\Omega}$.

Proof. We proceed by induction with respect to $E(\alpha, \boldsymbol{\Omega})$. If $E(\alpha, \boldsymbol{\Omega}) = 0$ the assertion is trivial. Assume that the lemma is true for all $\boldsymbol{\Omega}'$ and α' with $E(\alpha', \boldsymbol{\Omega}') < E(\alpha, \boldsymbol{\Omega})$ and let $g(x) \mid x^n-\alpha$.

If $x^n-\alpha$ is irreducible, then the lemma is trivially true with $G(x) = x^\nu-\alpha$. If it is reducible, then by Capelli's theorem either

(A) $$\alpha = \beta^p, \quad p \mid n, \quad p \text{ prime}, \quad \beta \in \boldsymbol{\Omega}$$

or

(B) $$\alpha = -4\beta^4, \quad 4 \mid n, \quad \beta \in \boldsymbol{\Omega}.$$

We consider these cases successively using the following notation: $\boldsymbol{\Omega}_q = \boldsymbol{\Omega}(\zeta_q)$, $d_q = [\boldsymbol{\Omega}_q:\boldsymbol{\Omega}]$.

(A) We have here

(18) $$g(x) \mid x^n-\beta^p = (x^{n/p}-\beta)\prod_{r=1}^{p-1}(x^{n/p}-\zeta_p^r\beta).$$

If $g(x) \mid x^{n/p}-\beta$ our inductive assumption applies directly, since by (A) and Lemma 2 $E(\beta, \boldsymbol{\Omega}) \,\Big|\, \frac{1}{p}E(\alpha, \boldsymbol{\Omega})$.

Putting $\nu_0 = \left(\frac{n}{p}, E(\beta, \boldsymbol{\Omega})\right)$ we have

$$\nu_0 \,\Big|\, \frac{\nu}{p}, \qquad g(x) = G_0(x^{n/p\nu_0}),$$

$G_0(x) \in \boldsymbol{\Omega}[x]$ and it is sufficient to take $G(x) = G_0(x^{\nu/p\nu_0})$.

If $g(x) \nmid x^{n/p}-\beta$, let $h(x)$ be a monic factor of $g(x)$ irreducible over $\boldsymbol{\Omega}_p$. By (18)

$$h(x) \mid g(x) \,\Big|\, \prod_{r=1}^{p-1}(x^{n/p}-\zeta_p^r\beta),$$

thus for some positive $r < p$

(19) $$h(x) \mid x^{n/p}-\zeta_p^r\beta.$$

Let $h^{(1)}(x) = h(x), \ldots, h^{(d_p)}(x)$ be all the conjugates of $h(x)$ relative to $\boldsymbol{\Omega}(x)$. It follows from (19) that

$$\big(h^{(i)}(x), h^{(j)}(x)\big) \,\big|\, \beta(\zeta_p^{(i)r}-\zeta^{(j)r}) \qquad (1 \leqslant i < j \leqslant d_p),$$

thus $h^{(i)}(x)$ $(i = 1, 2, \ldots, d_p)$ are relatively prime in pairs. Since $h^{(i)}(x) \mid g(x)$ it follows that

(20) $$g(x) = N_{\boldsymbol{\Omega}_p/\boldsymbol{\Omega}}\big(h(x)\big).$$

On the other hand, we have by Lemma 2

$$E(\zeta_p^r\beta, \boldsymbol{\Omega}_p) \,\Big|\, \frac{1}{p}E(\alpha, \boldsymbol{\Omega}).$$

Applying the inductive assumption to (19) and putting

$$\nu_1 = \left(\frac{n}{p}, E(\zeta_p^r\beta, \boldsymbol{\Omega}_p)\right)$$

we get

(21) $$\nu_1 \,\Big|\, \frac{\nu}{p}, \qquad h(x) = H(x^{n/p\nu_1}), \qquad H(x) \in \boldsymbol{\Omega}_p[x].$$

It is sufficient now to take

$$G(x) = N_{\boldsymbol{\Omega}_p/\boldsymbol{\Omega}}\big(H(x^{\nu/p\nu_1})\big).$$

Indeed, by (20) and (21)

$$g(x) = N_{\boldsymbol{\Omega}_p/\boldsymbol{\Omega}}\big(H(x^{n/p\nu_1})\big) = G(x^{n/\nu}).$$

(B) We have here

$$g(x) \mid x^n + 4\beta^4 = \prod_{r=0}^{3} \left(x^{n/4} - \zeta_4^r (1+\zeta_4)\beta\right).$$

Let $h(x)$ be a monic factor of $g(x)$ irreducible over Ω_4. We have for an $r \leqslant 3$

$$(22) \qquad h(x) \mid x^{n/4} - \zeta_4^r (1+\zeta_4)\beta$$

and it follows in the same way as (20) from (19) that

$$(23) \qquad g(x) = N_{\Omega_4/\Omega}\big(h(x)\big).$$

On the other hand, by Lemma 2

$$E\big(\zeta_4^r(1+\zeta_4)\beta,\ \Omega_4\big) \mid \tfrac{1}{4} E(\alpha,\ \Omega).$$

Applying the inductive assumption to (22) and putting

$$\nu_2 = \left(\frac{n}{4},\ E\big(\zeta_4^r(1+\zeta_4)\beta,\ \Omega_4\big)\right)$$

we get

$$(24) \qquad \nu_2 \,\Big|\, \frac{\nu}{4}, \qquad h(x) = H(x^{n/4\nu_2}), \qquad H(x) \in \Omega_4[x].$$

It is sufficient now to take

$$G(x) = N_{\Omega_4/\Omega}\big(H(x^{\nu/4\nu_2})\big).$$

Indeed by (23) and (24)

$$g(x) = N_{\Omega_4/\Omega}\big(H(x^{n/4\nu_2})\big) = G(x^{n/\nu}).$$

Remark. One can show by induction with respect to $E(\alpha,\ \Omega)$ that for $n = E(\alpha, \Omega)$ there is no $\nu < n$ with the property asserted in the lemma.

Moreover, Lemma 2 and 3 remain valid for any field Ω, not necessarily algebraic, n not divisible by char Ω and those $\alpha \in \Omega$ for which $e(\alpha,\ \Omega)$ is defined. $w(\Omega)$ is then to be replaced by the number of roots of unity of degree $E(\alpha,\ \Omega)$ contained in Ω.

LEMMA 4. *If $a \mid b$ then*

$$\sum_{(j,b)=1} (a, j-1) = \tau(a)\varphi(b),$$

where the sum is taken over any reduced system of residues mod b.

Proof. This is a special case of the theorem due to R. Sivaramakrishnan [19]. I owe the reference to Mr. A. Mąkowski.

LEMMA 5. *If $\Phi(x)$ is an irreducible polynomial, $\alpha \neq 0$ is any of its zeros, $n > 0$ is an integer,*

$$\nu = \big(n,\ E\big(\alpha, \boldsymbol{Q}(\alpha)\big)\big)$$

then

$$\Phi(x^\nu) \overset{\text{can}}{=} \Phi_1(x) \ldots \Phi_r(x)$$

implies

$$\Phi(x^n) \overset{\text{can}}{=} \Phi_1(x^{n/\nu}) \ldots \Phi_r(x^{n/\nu}).$$

Moreover

$$r \leqslant |\Phi|\,\tau(\nu).$$

Proof. Since Φ is irreducible, $\Phi(x)$ and hence also $\Phi(x^\nu)$ has no multiple factors. Clearly $\Phi_j(x^{n/\nu})$ $(1 \leqslant j \leqslant r)$ are prime to each other and to prove the first assertion of the lemma we have only to show that they are irreducible. Let $f_j(x)$ be an irreducible factor of $\Phi_j(x^{n/\nu})$. Clearly

$$(25) \qquad f_j(x) \mid \Phi(x^n).$$

We now use the following Lemma of Capelli (cf. [21], p. 289): if

$$(26) \qquad x^n - \alpha = \prod_{i=1}^{l} g_i(x)$$

is the canonical factorization of $x^n - \alpha$ in $\Omega = \boldsymbol{Q}(\alpha)$ then

$$(27) \qquad \Phi(x^n) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{l} N_{\Omega/\boldsymbol{Q}}\, g_i(x).$$

It follows from (25) and (27) that for some $i \leqslant l$

$$(28) \qquad \text{const} f_j(x) = N_{\Omega/\boldsymbol{Q}}\, g_i(x).$$

On the other hand, it follows from (26) and Lemma 3 that

$$(29) \qquad g_i(x) = G_i(x^{n/\nu}),$$

where $G_i(x) \in \Omega[x]$. By (28), (29) and the choice of f_j

$$(30) \qquad \text{const} f_j(x) = N_{\Omega/\boldsymbol{Q}}\, G_i(x^{n/\nu}) \mid \Phi_j(x^{n/\nu}),$$

thus $N_{\Omega/\boldsymbol{Q}} G_i(x) \mid \Phi_j(x)$.

Since Φ_j is irreducible

$$\Phi_j(x) = \text{const}\, N_{\Omega/\boldsymbol{Q}}\, G_i(x),$$

thus by (30)

$$\Phi_j(x^{n/\nu}) = \text{const} f_j(x)$$

and by the choice of $f_j(x)$, $\Phi_j(x^{n/\nu})$ is irreducible.

To prove the second assertion of the lemma we first remark that by (27)

$$r = l. \tag{31}$$

By the definition of $E(a, \Omega) = E$ we have $E > 0$ or a is a root of unity. In the former case

$$a = \vartheta(\zeta_E)^E, \quad \text{where} \quad \vartheta \in \boldsymbol{\Omega}[x]. \tag{32}$$

Let the Galois group $\mathscr{G}$ of $\boldsymbol{\Omega}(\zeta_E)/\boldsymbol{\Omega}$ be represented as a subgroup $\mathscr{J}$ of the multiplicative group $\mathscr{E}$ of reduced residues mod E, so that

$$\mathscr{J} = \{j \in \mathscr{E} : \exists_{g \in \mathscr{G}}\ \zeta_E^j = g(\zeta_E)\}. \tag{33}$$

For any $j \in \mathscr{J}$ we have by (32)

$$\vartheta(\zeta_E^j)^E = a = \vartheta(\zeta_E)^E,$$

hence

$$\vartheta(\zeta_E^j) = \zeta_E^{e(j)}\vartheta(\zeta_E) \tag{34}$$

for a suitable integer $e(j)$.

On the other hand, by (32)

$$x^\nu - a = \prod_{i=1}^{\nu}\left(x - \zeta_\nu^i \vartheta(\zeta_E)^{E/\nu}\right)$$

and taking norms from $\boldsymbol{\Omega}(\zeta_E, x)$ to $\boldsymbol{\Omega}(x)$

$$(x^\nu - a)^{|\mathscr{G}|} = \prod_{i=1}^{\nu} N_{\boldsymbol{\Omega}(\zeta_E)/\boldsymbol{\Omega}}\left(x - \zeta_\nu^i \vartheta(\zeta_E)^{E/\nu}\right), \tag{35}$$

where $|\mathscr{G}|$ is the order of $\mathscr{G}$.

The ith factor on the right hand side is a power of a polynomial irreducible in $\boldsymbol{\Omega}$ with the exponent equal to the number n_i of those elements of $\mathscr{G}$ that leave $x - \zeta_\nu^i \vartheta(\zeta_E^{E/\nu})$ invariant. By (33) we have

$$n_i = |\{j \in \mathscr{J} : \zeta_\nu^{ij}\vartheta(\zeta_E^j)^{E/\nu} = \zeta_\nu^i \vartheta(\zeta_E)^{E/\nu}\}|$$

and by (34)

$$n_i = |\{j \in \mathscr{J} : ij + e(j) \equiv i \bmod \nu\}|. \tag{36}$$

Comparing the number of factors irreducible over $\boldsymbol{\Omega}$ on both sides of (35) we get by (26), (31) and (36)

$$r|\mathscr{G}| = \sum_{i=1}^{\nu} n_i = \sum_{i=1}^{\nu} |\{j \in \mathscr{J} : ij + e(j) \equiv i \bmod \nu\}|$$
$$= \sum_{i \in \mathscr{J}} |\{1 \leqslant i \leqslant \nu : ij + e(j) \equiv i \bmod \nu\}| \leqslant \sum_{j \in \mathscr{J}} (\nu, j-1) \leqslant \sum_{(j,E)=1} (\nu, j-1).$$

Now

$$|\mathscr{G}| = [\boldsymbol{\Omega}(\zeta_E) : \boldsymbol{\Omega}] \geqslant \frac{\varphi(E)}{|\Phi|},$$

by Lemma 4

$$\sum_{(j,E)=1} (\nu, j-1) = \tau(\nu)\varphi(E),$$

and it follows that $r \leqslant |\Phi|\tau(\nu)$.

It remains to consider the case, where a is a root of unity. We have then for a suitable q $\Phi(x) = \text{const}\, X_q(x)$.

Let now $n = n_1 n_2$, where every prime factor of n_1 divides q and $(n_2, q) = 1$. It follows from the identity

$$X_q(x^n) = \prod_{d|n_2} X_{qn_1d}(x)$$

and from the irreducibility of cyclotomic polynomials that

$$r \leqslant \tau(n_2) \leqslant \tau(n) = \tau(\nu).$$

In the next three lemmata we use the notation $m(x) = \underset{p|x}{\text{l.c.m.}}(p-1)$ for any positive integer x.

Lemma 6. *For any integer $x > 1$ either there exist three positive integers x_1, x_2, x_3 such that*

$$xm(x) | [x_1 m(x_1), x_2 m(x_2), x_3 m(x_3)] \tag{37}$$

and $\sqrt{x_1} + \sqrt{x_2} + \sqrt{x_3} < \sqrt{x}$ or $x = q^\alpha r^\beta s$, where q, r are primes $r < 50$, $s < 50$, $\alpha > 0$, $\beta \geqslant 0$.

Proof. Let q be the greatest prime factor of x, $x = q^\alpha y$, $q \nmid y$. If $y \geqslant 50$, but $(q-1, y) = 1$ we set $x_1 = q^\alpha$, $x_2 = y$, $x_3 = 1$ and get

$$\sqrt{x} - \sqrt{x_1} - \sqrt{x_2} - \sqrt{x_3} \geqslant (\sqrt{q}-1)(\sqrt{y}-1) - 2 > (\sqrt{3}-1)(\sqrt{50}-1) - 2 > 0.$$

If $(q-1, y) > 1$ let r be a common prime factor of y and $q-1$

$$y = r^\beta s, \quad q - 1 = r^\gamma t, \quad r \nmid st.$$

If either $r \geqslant 50$ or $s \geqslant 50$ we set

$$x_1 = q^\alpha, \quad x_2 = r^{\beta+\gamma}, \quad x_3 = r^\beta st,$$

easily verify (37) and get

$$\sqrt{x} - \sqrt{x_1} - \sqrt{x_2} - \sqrt{x_3} \geqslant q^{\alpha/2} r^{\beta/2} s^{1/2} - q^{\alpha/2} - r^{(\beta+\gamma)/2} - r^{\beta/2}(st)^{1/2}$$
$$> \sqrt{x}\left(1 - \frac{1}{r^{\beta/2}s^{1/2}} - \frac{1}{(st)^{1/2}} - \frac{1}{(r^\gamma)^{1/2}}\right) > \sqrt{x}\left(1 - \frac{2}{\sqrt{50}} - \frac{1}{\sqrt{2}}\right) > 0.$$

The case $st = 1$ is excluded since $q - 1 = r^\gamma$ implies $r = 2 < 50$.

LEMMA 7. *If x_i are positive integers and $\sum_{i=1}^{j}\sqrt{x_i}\leqslant\sqrt{x}$ then*

$$\log \mathop{\mathrm{l.c.m.}}\limits_{i=1,\dots,j} x_i m(x_i) \ll x^{1/3}(\log x)^{2/3}.$$

Proof. Let $M = \max \mathop{\mathrm{l.c.m.}}\limits_{i=1,\dots,j} x_i m(x_i)$, where the maximum is taken over (finitely many) integral points $(x_1,\dots,x_j)$ satisfying $x_i>1$, $\sum_{i=1}^{j}\sqrt{x_i}\leqslant\sqrt{x}$. Let $(x_1^0,\dots,x_k^0)$ be a point in which the maximum is attained with the least value of $\sum_{i=1}^{j}\sqrt{x_i}$. By Lemma 6 we have $x_i^0 = q_i^{a_i}r_i^{\beta_i}s_i$ $(i=1,\dots,k)$, where q_i, r_i are primes and $a_i>0$, $r_i<50$, $s_i<50$. It follows that

$$M = \mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k} x_i^0 m(x_i^0) \leqslant \mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k} q_i^{a_i}(q_i-1)\mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k} r_i^{\beta_i}\mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k}(r_i-1)s_i m(s_i) \tag{38}$$
$$\ll \mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k} q_i^{a_i}(q_i-1)\ \mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k} r_i^{\beta_i}.$$

Since $r_i^{\beta_i}\leqslant x$ and $r_i<50$ we have

$$\log \mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k} r_i^{\beta_i} \leqslant \pi(50)\log x = 15\log x. \tag{39}$$

Similarly

$$\log \mathop{\mathrm{l.c.m.}}\limits_{i=1,\dots,k} q_i^{a_i}(q_i-1) \leqslant 2n\log x, \tag{40}$$

where n is the number of distinct terms among $q_i^{a_i}$ $(i=1,\dots,k)$. Let n_1, n_2 be the number of distinct terms with $a_i=1$ and $a_i\geqslant 2$, respectively. The condition $\sum_{i=1}^{k} q_i^{a_i/2}\leqslant\sqrt{x}$ implies $\sum_{i=1}^{n_1} p_i^{1/2}\leqslant\sqrt{x}'$, where p_i is the ith prime and $\sum_{i=1}^{n_2}P_i^{1/2}\leqslant\sqrt{x}$, where P_i is the ith perfect power with an exponent $\geqslant 2$. Using $p_i\gg i\log i$ and $P_i\gg i^2$ we get

$$n_1^{3/2}(\log n_1)^{1/2}\ll\sqrt{x} \quad\text{and}\quad n_2^2\ll\sqrt{x}.$$

Hence

$$n = n_1 n_2 \ll x^{1/3}(\log x)^{-1/3}, \tag{41}$$

and the lemma follows from (38)–(41).

LEMMA 8. *If x_i are positive integers and $\sum_{i=1}^{j}x_i\leqslant x$ then*

$$\log \mathop{\mathrm{l.c.m.}}\limits_{i=1,\dots,j} x_i m(x_i) \leqslant \sqrt{x\log x}+O(\sqrt{x\log_2 x}).$$

Proof. Let $M = \max \mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant j} x_i m(x_i)$, where the maximum is taken over all integral points $(x_1,\dots,x_j)$ satisfying $x_i>1$, $\sum_{i=1}^{j}x_i\leqslant x$, and let $x_1^0,\dots,x_k^0$ be a point in which the maximum is attained with the least value of $\sum_{i=1}^{k}x_i$. Since $\sqrt{x_1}+\sqrt{x_2}+\sqrt{x_3}<\sqrt{x}$ implies $x_1+x_2+x_3<x$ it follows from Lemma 6 that

$$x_i^0 = q_i^{a_i}r_i^{\beta_i}s_i,\quad \text{where}\quad q_i, r_i \text{ are primes and } r_i<50,\ s_i<50,\ a_i>0$$

and as in the proof of Lemma 7 we find

$$\log M < \log \mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k} q_i^{a_i}(q_i-1)+15\log x+O(1). \tag{42}$$

Now by the classical result of Landau ([7], § 61) if $\sum_{i=1}^{k}x_i\leqslant x$ then

$$\log \mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k} x_i \leqslant \sqrt{x\log x}+O(\sqrt{x}),$$

hence

$$\log \mathop{\mathrm{l.c.m.}}\limits_{1\leqslant i\leqslant k} q_i^{a_i} \leqslant \sqrt{x\log x}+O(\sqrt{x}). \tag{43}$$

In order to estimate $\mathop{\mathrm{l.c.m.}}\limits_{i=1,\dots,k}(q_i-1)$ we divide the primes q_i into two classes C_1 and C_2 assigning q_i to C_1 if q_i-1 has a prime factor t_i between $a=\log x/\log_2 x$ and $b=\sqrt{x\log_2 x}$ and to C_2 otherwise. Since

$$\sum_{q_i\in C_1}\frac{q_i-1}{t_i}\leqslant\frac{x}{\log x}\log_2 x$$

we have by the quoted Landau's result

$$\log \mathop{\mathrm{l.c.m.}}\limits_{q_i\in C_1}\frac{q_i-1}{t_i}\leqslant\sqrt{x\log_2 x}+O(\sqrt{x})$$

and

$$\log \mathop{\mathrm{l.c.m.}}\limits_{q_i\in C_1}(q_i-1)\leqslant\log \mathop{\mathrm{l.c.m.}}\limits_{q_i\in C_1}t_i+\log \mathop{\mathrm{l.c.m.}}\limits_{q_i\in C_1}\frac{q_i-1}{t_i} \tag{44}$$
$$\leqslant b+O\left(\frac{b}{\log b}\right)+\sqrt{x\log_2 x}+O(\sqrt{x})$$
$$= 2\sqrt{x\log_2 x}+O(\sqrt{x}).$$

In order to estimate $\mathop{\mathrm{l.c.m.}}\limits_{q_i\in C_2}(q_i-1)$ we may assume without loss of generality that $C_2=\{q_1,q_2,\dots,q_n\}$ and $q_1<q_2<\dots<q_n$. By the upper sieve theory (see [5], p. 134, Theorem 4.2) the number $C_2(t)$ of $q_i\in C_2$,

$q_i \leqslant t$ satisfies for $t \geqslant b$

$$C_2(t) \ll \frac{t}{\log t} \prod_{a<p<b} \left(1 - \frac{1}{p}\right) \ll \frac{t}{\log t} \frac{\log_2 x}{\log x}.$$

For $i > b/\log b$, we have $q_i \gg b$, hence

$$\frac{b}{\log b} < i = C_2(q_i) \ll \frac{q_i}{\log q_i} \frac{\log_2 x}{\log x} \ll \frac{q_i}{\log^2 x} \log_2 x$$

and

$$q_i \gg \frac{b}{\log b} \frac{\log^2 x}{\log_2 x} \gg \sqrt{\frac{x}{\log_2 x}} \log x.$$

The inequality $\sum_{i=1}^{n} q_i \leqslant x$ implies

$$\left(n - \frac{b}{\log b}\right) \sqrt{\frac{x}{\log_2 x}} \log x \ll x,$$

hence

$$n \ll \frac{b}{\log b} + \sqrt{\frac{x \log_2 x}{\log x}} \ll \sqrt{\frac{x \log_2 x}{\log x}}.$$

It follows that

$$\log \underset{q_i \in C_2}{\mathrm{l.c.m.}} (q_i - 1) \leqslant n \log x \ll \sqrt{x \log_2 x}, \tag{45}$$

and the lemma results from (42)–(45).

Proof of Theorem 1. Let

$$KF(x) \overset{\mathrm{can}}{=} \mathrm{const} \prod_{i=1}^{\varrho} \Phi_i(x)^{\varepsilon_i}. \tag{46}$$

For each Φ_i we denote by α_i, ν_i the relevant parameters from Lemma 5 and set $c(F) = \underset{1 \leqslant i \leqslant \varrho}{\mathrm{l.c.m.}} E\big(\alpha_i, Q(\alpha_i)\big)$;

$$\nu = \underset{1 \leqslant i \leqslant \varrho}{\mathrm{l.c.m.}} \nu_i = \big(n, c(F)\big), \qquad u = n\nu^{-1}.$$

(i) and (ii) follow immediately. By Lemma 2

$$c(F) \,|\, 2 \underset{1 \leqslant i \leqslant \varrho}{\mathrm{l.c.m.}} e\big(\alpha_i, Q(\alpha_i)\big) m\Big(e\big(\alpha_i, Q(\alpha_i)\big)\Big),$$

where $m(x) = \underset{p|x}{\mathrm{l.c.m.}} (p-1)$.

On the other hand, by Lemma 1

$$\sum_{i=1}^{\varrho} \sqrt{e\big(\alpha_i, Q(\alpha_i)\big)} \ll \sqrt{|KF| \log(2|KF|) \log \|F\|},$$

and if $KF(x) = LF(x)$

$$\sum_{i=1}^{\varrho} e\big(\alpha_i, Q(\alpha_i)\big) \leqslant \frac{\log \|F\|}{2 \log \vartheta_0}.$$

Hence by Lemma 7

$$\log c(F) \ll \big(|KF| \log(2|KF|) \log \|F\|\big)^{1/3} (\log |KF| + \log_2 \|F\|)^{2/3}$$

and if $KF(x) = LF(x)$, by Lemma 8

$$\log c(F) \leqslant \sqrt{\frac{\log \|F\| \log_2 \|F\|}{2 \log \vartheta_0}} + O(\sqrt{\log \|F\| \log_3 \|F\|})$$

(note that $|KF| \geqslant 1$ implies $\|F\| \geqslant 3$, $\log_2 \|F\| > 0$).

In order to prove (iii) we note that by Lemma 5

$$\Phi_i(x^{\nu_i}) \overset{\mathrm{can}}{=} \prod_{j=1}^{r_i} \Phi_{ij}(x)$$

implies

$$\Phi_i(x^n) \overset{\mathrm{can}}{=} \prod_{j=1}^{r_i} \Phi_{ij}(x^{n/\nu_i}),$$

whence by (46)

$$KF(x^{\nu}) \overset{\mathrm{can}}{=} \mathrm{const} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} \Phi_{ij}(x^{\nu/\nu_i})^{\varepsilon_i},$$

$$KF(x^n) \overset{\mathrm{can}}{=} \mathrm{const} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} \Phi_{ij}(x^{n/\nu_i})^{\varepsilon_i}.$$

Denoting the polynomials $\Phi_{ij}(x^{\nu/\nu_i})$ $(1 \leqslant i \leqslant \varrho,\ 1 \leqslant j \leqslant r)$ by $F_1, \ldots, F_s$ we obtain (iii).

It remains to estimate $\Omega = \Omega\big(KF(x^n)\big) = \sum_{i=1}^{\varrho} \varepsilon_i r_i$. By Lemma 5 we have $r_i \leqslant |\Phi_i| \tau(\nu_i)$, hence

$$\Omega \leqslant \sum_{i=1}^{\varrho} \varepsilon_i |\Phi_i| \tau(\nu_i). \tag{47}$$

Since $\nu_i | n$ and by (46)

$$\sum_{i=1}^{\varrho} \varepsilon_i |\Phi_i| = |KF|, \tag{48}$$

we get $\Omega \leqslant |KF| \tau(n)$. In order to get the other bound for Ω given in the theorem we note that (the α_i's not being roots of unity) $E\big(\alpha_i, Q(\alpha_i)\big) \neq 0$ and $\nu_i | E\big(\alpha_i, Q(\alpha_i)\big)$ implies

$$\tau(\nu_i) \leqslant \tau\Big(E\big(\alpha_i, Q(\alpha_i)\big)\Big). \tag{49}$$

By Lemma 2

$$E\big(\alpha_i, Q(\alpha_i)\big) \leqslant w_i e\big(\alpha_i, Q(\alpha_i)\big), \tag{50}$$

where w_i is the number of roots of unity contained in $Q(\alpha_i)$. Clearly $\varphi(w_i) \leqslant |\Phi_i| \leqslant |KF|$ hence by the classical Landau's result ([7], § 59)

$$w_i \ll |KF|\log_2|KF|, \quad w_i \leqslant 2|KF|^{1+o(1)}.$$

On the other hand, by Lemma 1

$$e\big(\alpha_i, Q(\alpha_i)\big) \leqslant 26|KF|\log(7|KF|)\log\|F\|,$$

hence by (50)

$$E\big(\alpha_i, Q(\alpha_i)\big) \leqslant 100|KF|^{2+o(1)}\log\|F\|. \tag{51}$$

Now by the result of Wigert (cf. [7], § 60)

$$\tau(x) < \tau_0(x)^{1+o(1)}, \tag{52}$$

where

$$\tau_0(x) = \exp\left(\frac{\log 2}{\log_2 x}\log x\right)$$

and $o(1)\to 0$ as $x\to\infty$.

The function $\tau_0(x)$ is increasing to infinity and we easily deduce from (52) the apparently stronger estimate

$$\tau(y) < \tau_0(x)^{1+o(1)} \quad \text{for all } y \leqslant x.$$

Moreover, for $x, y > e$

$$\tau_0(xy) \leqslant \tau_0(x)\tau_0(y) \leqslant x^{o(1)}\tau_0(y).$$

Hence by (51)

$$\begin{aligned}\tau\Big(E\big(\alpha_i, Q(\alpha_i)\big)\Big) &\leqslant \tau_0(100|KF|^{2+o(1)}\log\|F\|)^{1+o(1)}\\ &\leqslant 10|KF|^{o(1)}\tau_0(10\log\|F\|)^{1+o(1)}\\ &= |KF|^{o(1)}\exp\left(\frac{\log 2+o(1)}{\log_3\|F\|}\log_2\|F\|\right),\end{aligned}$$

and the desired estimate for $\Omega\big(KF(x^n)\big)$ follows in view of (47), (48) and (49).

Proof of Corollary 1. Since $F(0)\neq 0$ we have for some q_i, ε_i

$$F(x) = JF(x) = KF(x)\prod_{i=1}^{j} X_{q_i}(x)^{\varepsilon_i}.$$

By the easy case of Lemma 5 ($\nu = n$) we get

$$\Omega\big(X_{q_i}(x^n)\big) \leqslant |X_{q_i}|\tau(n).$$

Hence

$$\begin{aligned}\Omega\big(F(x^n)\big) &= \Omega\big(KF(x^n)\big) + \sum_{i=1}^{j}\varepsilon_i\Omega\big(X_{q_i}(x^n)\big)\\ &\leqslant |KF|\tau(n) + \sum_{i=1}^{j}\varepsilon_i|X_{q_i}|\tau(n) = |F|\tau(n).\end{aligned}$$

Proof of Corollary 2. If $b(x) = a_0 + a_1x^n$ it is sufficient to take in the theorem $F(x) = a_0 + a_1x$.

Proof of Corollary 3. By Corollary to Lemma 1

$$\Omega\big(Lt(x)\big) < \frac{\log\|t\|}{2\log\vartheta_0}.$$

On the other hand, if $t(x) = a_0 + a_1x^{n_1} + a_2x^{n_2}$ we have

$$\begin{aligned}\frac{t(x)}{Lt(x)}\,\Big|\,(a_0x^{n_2}+a_2)t(x) - a_1x^{n_1+n_2}t(x^{-1})&\\ = a_0a_2x^{2n_2} + (a_0^2+a_2^2-a_1^2)x^{n_2} + a_0a_2.&\end{aligned} \tag{53}$$

Taking in the theorem $F(x) = a_0a_2x^2 + (a_0^2+a_2^2-a_1^2)x + a_0a_2$ we get $\|F\| \leqslant 2\|t\|^2$,

$$\Omega\big(KF(x^{n_2})\big) \ll \exp\left(\frac{\log 2+o(1)}{\log_3\|t\|}\log_2\|t\|\right) = o(\log\|t\|)$$

and since by (53)

$$\frac{Kt(x)}{Lt(x)}\,\Big|\,KF(x^{n_2})$$

the corollary follows.

Examples. In order to show that the estimates for $e(F)$ and $\Omega\big(KF(x^n)\big)$ given in Theorem 1 are sharp we consider the following two examples

1. $n = \prod_{p\leqslant t} p$, $F(x) = \prod_{p\leqslant t} f_p(x)$;
2. $n = \prod_{p\leqslant t} p$, $F(x) = (2^nx-1)^m$,

where p runs over primes, $f_p(x)$ is given by (9) and t, m are parameters.

In the case 1 we have $F = KF = LF$ since f_p are non-reciprocal,

$$|KF| = 3\pi(t) \ll t/\log t,$$

and by (10)

$$\begin{aligned}\log\|F\| &\leqslant 2\log l(F) \leqslant 2\sum_{p\leqslant t}\log l(f_p)\\ &\leqslant 2\sum_{p\leqslant t}\big(p\log\nu_0 + O(\vartheta_0^{-p/2})\big) = \log\vartheta_0\frac{t^2}{\log t} + O\left(\frac{t^2}{(\log t)^2}\right).\end{aligned}$$

Hence

$$(|KF|\log(2|KF|)\log\|F\|)^{1/3}(\log|KF|+\log_2\|F\|)^{2/3} \leqslant t(\log t)^{1/3},$$

$$\sqrt{\frac{\log\|F\|\log_2\|F\|}{2\log\vartheta_0}} \leqslant t+O\left(\frac{t}{\log t}\right).$$

On the other hand, by Lemma 1

$$e\big(\vartheta_0, \boldsymbol{Q}(\vartheta_0)\big) \leqslant \frac{\log 3}{2\log\vartheta_0} < 2,$$

hence $e\big(\vartheta_0, \boldsymbol{Q}(\vartheta_0)\big) = 1$, $e\big(\vartheta_0^p, \boldsymbol{Q}(\vartheta_0)\big) = p$. By Capelli's theorem $x^\nu - \vartheta_0^{p}$ is reducible in $\boldsymbol{Q}(\vartheta_0)$ if and only if $\nu \equiv 0 \bmod p$. By (9) and Capelli's lemma $\nu \equiv 0 \bmod p$ is also a necessary and sufficient condition for the reducibility of $f_p(x)$. Hence for all proper divisors ν of n

$$\Omega\big(F(x^\nu)\big) < \Omega\big(F(x^n)\big)$$

and if ν satisfies (ii) and (iii) we have $\nu = n$,

$$\log\nu = \sum_{p\leqslant t}\log p = t+O\left(\frac{t}{\log t}\right).$$

In the case 2 we have

$$|KF| = |F| = m,$$

$$\log\|F\| \leqslant 2\log l(F) \leqslant 2m\log(2^n+1) \leqslant 3mn,$$

$$\frac{\log_2\|F\|}{\log_3\|F\|} \leqslant o(\log m)+\frac{\log n}{\log_2 n} = o(\log m)+\frac{t}{\log t}+O\left(\frac{t}{\log^2 t}\right)$$
$$= o(\log m)+\pi(t)+o\big(\pi(t)\big).$$

Hence

$$|KF|\tau(n) = m\cdot 2^{\pi(t)},$$

$$|KF|^{1+o(1)}\exp\left(\frac{\log 2+o(1)}{\log_3\|F\|}\log_2\|F\|\right) < m^{1+o(1)}\cdot 2^{\pi(t)+o(\pi(t))}.$$

On the other hand

$$KF(x^n) = \prod_{d|n} X_d(2x)^m, \qquad \Omega\big(KF(x^n)\big) = m\tau(n) = m\cdot 2^{\pi(t)}.$$

3. LEMMA 9. *Let $P(x_1, \ldots, x_k)$, $Q(x_1, \ldots, x_k)$ be polynomials, $(P, Q) = G$. For any positive integers $n_1, \ldots, n_k$ we have*

$$\big(P(x_1^{n_1}, \ldots, x_k^{n_k}),\ Q(x_1^{n_1}, \ldots, x_k^{n_k})\big) = G(x_1^{n_1}, x_2^{n_2}, \ldots, x_k^{n_k}).$$

Proof. Let $P = GP_0$, $Q = GQ_0$ and let $R(x_2, \ldots, x_k)$ be the resultant of P_0 and Q_0 with respect to x_1. There exist polynomials U and V such that

$$UP_0+VQ_0 = R.$$

From

$$U(x_1^{n_1}, \ldots, x_k^{n_k})P_0(x_1^{n_1}, \ldots, x_k^{n_k})+V(x_1^{n_1}, \ldots, x_k^{n_k})Q_0(x_1^{n_1}, \ldots, x_k^{n_k})$$
$$= R(x_2^{n_2}, \ldots, x_k^{n_k})$$

we infer that $\big(P_0(x_1^{n_1}, \ldots, x_k^{n_k}),\ Q_0(x_1^{n_1}, \ldots, x_k^{n_k})\big)$ does not depend upon x_1. Since the same argument applies to other variables we have

$$\big(P_0(x_1^{n_1}, \ldots, x_k^{n_k}),\ Q_0(x_1^{n_1}, \ldots, x_k^{n_k})\big) = \text{const}$$

and the lemma follows.

LEMMA 10. *If Ψ is an absolutely irreducible polynomial with algebraic coefficients, one of which is rational $\neq 0$ and $\boldsymbol{\Omega}$ is the field generated by these coefficients then $N_{\boldsymbol{\Omega}/\boldsymbol{Q}}\Psi(X)$ is irreducible $(X = (x_1, \ldots, x_k))$.*

Proof. Let Φ be the irreducible factor of $N_{\boldsymbol{\Omega}/\boldsymbol{Q}}\Psi(X)$ divisible by $\Psi(X)$. For all isomorphic injections σ of $\boldsymbol{\Omega}$ into the complex field $\boldsymbol{C}$ we have

$$\Psi^\sigma(X)\,|\,\Phi(X)$$

hence

$$\prod_\sigma \Psi^\sigma(X) = N_{\boldsymbol{\Omega}/\boldsymbol{Q}}\Psi(X)\,|\,\Phi(X)^{[\boldsymbol{\Omega}:\boldsymbol{Q}]}.$$

Since $\Phi(X)$ is irreducible

(54) $$N_{\boldsymbol{\Omega}/\boldsymbol{Q}}\Psi(X) = \text{const}\,\Phi(X)^a, \qquad \Psi(X)^a\,|\,N_{\boldsymbol{\Omega}/\boldsymbol{Q}}\Psi(X)$$

and

(55) $$\Psi(X)^{a-1}\,\Big|\,\prod{}'\Psi^\sigma(X),$$

where $\prod'$ is taken over all injections σ different from the identity e. However for such injections

$$\Psi^\sigma(X) \neq \Psi(X)$$

by the definition of $\boldsymbol{\Omega}$, and since $\Psi^\sigma(X)$, $\Psi(X)$ have a common non-zero coefficient

$$\Psi^\sigma(X) \neq \text{const}\,\Psi(X).$$

Since $\Psi(X)$ is absolutely irreducible and of the same degree as $\Psi^\sigma(X)$ with respect to all the variables it follows that

$$\big(\Psi(X), \Psi^\sigma(X)\big) = 1 \qquad (\sigma \neq e).$$

Hence by (55) $a = 1$ and the lemma follows from (54).

LEMMA 11. *If $\Phi(x)$ is irreducible, $\gamma_1, \ldots, \gamma_k$ are integers and $(\gamma_1, \ldots, \gamma_k) = 1$ then $J\Phi(x_1^{\gamma_1}\ldots x_k^{\gamma_k})$ is irreducible.*

Proof. Let $\Phi(\alpha) = 0$. If, say, $\gamma_1 \neq 0$ then

$$b(x_1, \ldots, x_k) = J(x_1^{\gamma_1} \ldots x_k^{\gamma_k} - \alpha)$$

is a binomial with respect to x_1 over $C(x_2, \ldots, x_k)$. By Capelli's theorem it is irreducible over that field. But b has no factor independent of x_1, hence it is irreducible over $\boldsymbol{C}$. Since

$$J\Phi(x_1^{\gamma_1} \ldots x_k^{\gamma_k}) = \mathrm{const}\, N_{\boldsymbol{Q}(\alpha)/\boldsymbol{Q}}\, b(x_1, \ldots, x_k)$$

the lemma follows from the preceding one.

LEMMA 12. *Let $\Phi(x_1, \ldots, x_k) \neq \mathrm{const}\, x_j$ be irreducible and not of the form $J\Phi_0(x_1^{\delta_1} \ldots x_k^{\delta_k})$, where $\Phi_0 \in \boldsymbol{Q}[x]$ and $\delta_1, \ldots, \delta_k$ are integers. For any positive integers $n_1, \ldots, n_k$ there exist positive integers $\mu_1, \ldots, \mu_k$, $u_1, \ldots, u_k$ such that*

$$\mu_j \leqslant |\Phi|^2, \tag{56}$$

$$n_j = \mu_j u_j, \tag{57}$$

and

$$\Phi(x_1^{\mu_1}, \ldots, x_k^{\mu_k}) \overset{\text{can}}{=} \mathrm{const} \prod_{g=1}^{h} \Phi_g(x_1, \ldots, x_k)^{e_g} \tag{58}$$

implies $e_g = 1$ $(1 \leqslant g \leqslant h)$ and

$$\Phi(x_1^{n_1}, \ldots, x_k^{n_k}) \overset{\text{can}}{=} \mathrm{const} \prod_{g=1}^{h} \Phi_g(x_1^{u_1}, \ldots, x_k^{u_k}).$$

Proof. Let Ψ be an absolutely irreducible factor of Φ with the leading coefficient 1. (By the leading coefficient we mean here the coefficient of the first term in the antilexicographic order.) By the classical theorem of Kronecker the coefficients of Ψ are algebraic. If $\boldsymbol{\Omega}_0$ is the field generated by them then by Lemma 10

$$N_{\Omega_0/\boldsymbol{Q}}\Psi(x_1, \ldots, x_k)$$

is irreducible, and since it has a factor in common with $\Phi(x_1, \ldots, x_k)$

$$\Phi(x_1, \ldots, x_k) = \mathrm{const}\, N_{\Omega_0/\boldsymbol{Q}}\Psi(x_1, \ldots, x_k). \tag{59}$$

If Ψ has only two terms then

$$\Psi = J(x_1^{\delta_1} \ldots x_k^{\delta_k} - \alpha)$$

for a suitable α and suitable integers $\delta_1, \ldots, \delta_k$. Here $\boldsymbol{\Omega}_0 = \boldsymbol{Q}(\alpha)$ and if Φ_0 is the minimal polynomial of α

$$N_{\Omega_0/\boldsymbol{Q}}\Psi(x_1, \ldots, x_k) = J\Phi_0(x_1^{\delta_1} \ldots x_k^{\delta_k}),$$

which together with (59) contradicts the assumption. Thus Ψ has more than two terms and by Gourin's theorem there exist positive integers $\mu_1, \ldots, \mu_k$; $u_1, \ldots, u_k$ such that

$$\mu_j \leqslant |\Psi|^2, \quad n_j = \mu_j u_j$$

and

(60) every absolutely irreducible factor of $\Psi(x_1^{n_1}, \ldots, x_k^{n_k})$ is of the form $T(x_1^{u_1}, \ldots, x_k^{u_k})$, where $T \in \boldsymbol{C}[x_1, \ldots, x_k]$.

Since $|\Psi| \leqslant |\Phi|$ the numbers μ_j, u_j satisfy the conditions (56) and (57). Assume now (58). For at least one $j \leqslant k$ we have

$$\frac{\partial\Phi}{\partial x_j}(x_1, \ldots, x_k) \neq 0,$$

hence by the irreducibility of Φ

$$\left(\Phi(x_1, \ldots, x_k), \frac{\partial\Phi}{\partial x_j}(x_1, \ldots, x_k)\right) = 1$$

and by Lemma 9

$$\left(\Phi(x_1^{\mu_1}, \ldots, x_k^{\mu_k}), \frac{\partial\Phi}{\partial x_j}(x_1^{\mu_1}, \ldots, x_k^{\mu_k})\right) = 1.$$

Since also

$$\left(\Phi(x_1^{\mu_1}, \ldots, x_k^{\mu_k}), x_j\right) = 1$$

it follows that

$$\left(\Phi(x_1^{\mu_1}, \ldots, x_k^{\mu_k}), \frac{\partial}{\partial x_j}\Phi(x_1^{\mu_1}, \ldots, x_k^{\mu_k})\right) = 1,$$

which proves that $e_g = 1$ $(g \leqslant h)$. (Cf. Remark on p. 148 in [11].) The polynomials $\Phi_g(x_1^{u_1}, \ldots, x_k^{u_k})$ are clearly non-constant, and by Lemma 9 they are prime to each other. To show that they are irreducible let Ψ_g denote an absolutely irreducible factor of $\Phi_g(x_1^{u_1}, \ldots, x_k^{u_k})$ with the leading coefficient 1. By Kronecker's theorem the coefficients of Ψ_g are algebraic. By (57) and (58) we have

$$\Psi_g(x_1, \ldots, x_k) \mid \Phi(x_1^{n_1}, \ldots, x_k^{n_k})$$

and in view of (59) there exists a conjugate Ψ_g^σ of Ψ_g such that

$$\Psi_g^\sigma(x_1, \ldots, x_k) \mid \Psi(x_1, \ldots, x_k).$$

Ψ_g^σ is absolutely irreducible and by (60)

$$\Psi_g^\sigma(x_1, \ldots, x_k) = T(x_1^{u_1}, \ldots, x_k^{u_k}), \tag{61}$$

where $T \in \boldsymbol{C}[x_1, \ldots, x_k]$.

The coefficients of Ψ_g^σ generate an algebraic number field $\boldsymbol{\Omega}_g$ and by Lemma 10

$$N = N_{\Omega_g/\boldsymbol{Q}}\Psi_g^\sigma(x_1, \ldots, x_k) \text{ is irreducible.} \tag{62}$$

Since N has with $\Phi_g(x_1^{u_1}, \ldots, x_k^{u_k})$ the common factor Ψ_g we have

$$N \mid \Phi_g(x_1^{u_1}, \ldots, x_k^{u_k})$$

and by (61)

$$N_{\Omega_g/\boldsymbol{Q}}\big(T(x_1^{u_1}, \ldots, x_k^{u_k})\big) \mid \Phi_g(x_1^{u_1}, \ldots, x_k^{u_k}).$$

However $T \in \boldsymbol{\Omega}_g[x_1, \ldots, x_k]$

$$N_{\Omega_g/\boldsymbol{Q}}\big(T(x_1^{u_1}, \ldots, x_k^{u_k})\big) = (N_{\Omega_g/\boldsymbol{Q}}T)\,(x_1^{u_1}, \ldots, x_k^{u_k}).$$

Therefore it follows from Lemma 9 that

$$N_{\Omega_g/\boldsymbol{Q}}T(x_1, \ldots, x_k) \mid \Phi_g(x_1, \ldots, x_k)$$

and from the irreducibility of Φ_g that

$$\Phi_g(x_1, \ldots, x_k) = \operatorname{const} N_{\Omega_g/\boldsymbol{Q}}(Tx_1, \ldots, x_k).$$

Thus by (61)

$$\Phi_g(x_1^{u_1}, \ldots, x_k^{u_k}) = \operatorname{const} N_{\Omega_g/\boldsymbol{Q}}T(x_1^{u_1}, \ldots, x_k^{u_k}) = \operatorname{const} N$$

and the missing assertion of the lemma follows from (62).

Remark. Lemma 12 remains true for polynomials over any field $\boldsymbol{\Omega}$ of characteristic 0. If the characteristic is positive the lemma has to be modified.

Proof of Theorem 2. Let us observe first that

$$KF(x_1^{n_1}, \ldots, x_k^{n_k}) = (KF)\,(x_1^{n_1}, \ldots, x_k^{n_k}). \tag{63}$$

Indeed, if $f(x_1, \ldots, x_k) \mid J(x_1^{\delta_1} \ldots x_k^{\delta_k} - 1)$ then

$$f(x_1^{n_1}, \ldots, x_k^{n_k}) \mid J(x_1^{n_1\delta_1} \ldots x_k^{n_k\delta_k} - 1)$$

hence the left hand side of (63) divides the right hand side. On the other hand for any integral vector $[\delta_1, \ldots, \delta_k] \neq 0$

$$\big(KF(x_1, \ldots, x_k),\, J(x_1^{n\delta_1/n_1} \ldots x_k^{n\delta_k/n_k} - 1)\big) = 1, \quad \text{where} \quad n = n_1 \ldots n_k.$$

Hence by Lemma 9

$$\big((KF)\,(x_1^{n_1}, \ldots, x_k^{n_k}),\, J(x_1^{n\delta_1} \ldots x_k^{n\delta_k} - 1)\big) = 1$$

and since

$$J(x_1^{\delta_1} \ldots x_k^{\delta_k} - 1) \mid J(x_1^{n\delta_1} \ldots x_k^{n\delta_k} - 1)$$

we get

$$\big((KF)\,(x_1^{n_1}, \ldots, x_k^{n_k}),\, J(x_1^{\delta_1} \ldots x_k^{\delta_k} - 1)\big) = 1.$$

This proves (63). Let now

$$KF(x_1, \ldots, x_k) \overset{\text{can}}{=} \operatorname{const} \prod_{i=1}^{r} \Phi_i(x_1, \ldots, x_k)^{e_i}, \tag{64}$$

where for $i \leqslant r_0$ Φ_i is of the form $J\Phi_{i0}\,(x_1^{\delta_{i1}} \ldots x_k^{\delta_{ik}})$ for a suitable Φ_{i0} and suitable integers $\delta_{i1}, \ldots, \delta_{ik}$ while for $i > r_0$ Φ_i is not of the latter form. Clearly for each $i \leqslant r_0$ Φ_{i0} is irreducible and non-cyclotomic, hence denoting any of its zeros by a_i we have $c_i = E\big(a_i, \boldsymbol{Q}(a_i)\big) \neq 0$. Let us set

$$c(F) = \text{l.c.m.}\,\{c_1, \ldots, c_{r_0}, 1, 2, \ldots, \max_{i > r_0} |\Phi_i|^2\},$$

$$\nu_j = \big(c(F), n_j\big), \quad v_j = n_j \nu_j^{-1} \quad (1 \leqslant j \leqslant k),$$

$$\delta_i(\boldsymbol{n}) = (\delta_{i1}n_1, \ldots, \delta_{ik}n_k) \quad (1 \leqslant i \leqslant r_0),$$

$$\delta_i = \big(\delta_i(\boldsymbol{n}), c_i\big) \quad (1 \leqslant i \leqslant r_0).$$

The conditions (iv) and (v) are clearly satisfied.

By Lemma 5 for each $i \leqslant r_0$

$$\Phi_{i0}(x^{\delta_i}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} \Phi_{ig}(x)$$

implies

$$\Phi_{i0}(x^{\delta_i(\boldsymbol{n})}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} \Phi_{ig}(x^{\delta_i(\boldsymbol{n})/\delta_i}).$$

Setting in Lemma 11

$$\gamma_j = \delta_{ij} n_j / \delta_i(\boldsymbol{n}) \quad (1 \leqslant j \leqslant k)$$

we infer that for all $g \leqslant h_i$ the polynomials

$$J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\gamma_j\delta_i(\boldsymbol{n})/\delta_i}\Big) = J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}n_j/\delta_i}\Big)$$

are irreducible. Since

$$J\Phi_{i0}\Big(\prod_{j=1}^{k} x_j^{\gamma_j\delta_i(\boldsymbol{n})}\Big) = J\Phi_{i0}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}n_j}\Big) = \Phi_i(x_1^{n_1}, \ldots, x_k^{n_k})$$

we get

$$\Phi_i(x_1^{n_1}, \ldots, x_k^{n_k}) \overset{\text{can}}{=} J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}n_j/\delta_i}\Big) \quad (1 \leqslant i \leqslant r_0). \tag{65}$$

Since by the definition of $c(F)$ and ν_j, $\delta_i \mid \delta_{ij}\nu_j$ $(1 \leqslant j \leqslant k)$ the substitution $x_j \to x_j^{1/\nu_j}$ $(1 \leqslant j \leqslant k)$ gives

$$\Phi_i(x_1^{\nu_1}, \ldots, x_k^{\nu_k}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}\nu_j/\delta_i}\Big) \quad (1 \leqslant i \leqslant r_0). \tag{65'}$$

For $i > r_0$ there exist by Lemma 12 positive integers μ_{ij} and u_{ij} $(1 \leqslant j \leqslant k)$ such that

$$\mu_{ij} \leqslant |\Phi_i|^2, \quad n_j = \mu_{ij}u_{ij},$$

and

$$\Phi_i(x_1^{\mu_{i1}}, \ldots, x_k^{\mu_{ik}}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} \Phi_{ig}(x_1, \ldots, x_k)$$

implies

$$\Phi_i(x_1^{n_1}, \ldots, x_k^{n_k}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} \Phi_{ig}(x_1^{u_{i1}}, \ldots, x_k^{u_{ik}}). \tag{66}$$

By the definition of $c(F)$ we have $\mu_{ij} | c(F)$, hence

$$\mu_{ij} | r_j, \quad v_j | u_{ij} \quad (r_0 < i \leqslant r,\ 1 \leqslant j \leqslant k).$$

The substitution $x_j \to x_j^{1/v_j}$ applied to (66) gives

$$\Phi_i(x_1^{v_1}, \ldots, x_k^{v_k}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} \Phi_{ig}(x_1^{v_1/\mu_{i1}}, \ldots, x_k^{v_k/\mu_{ik}}). \tag{66'}$$

From (63), (64), (65), (65′), (66), (66′) and Lemma 9 we infer that

$$KF(x_1^{n_1}, \ldots, x_k^{n_k}) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{r_0} \prod_{g=1}^{h_i} J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}n_j/\delta_i}\Big)^{\varepsilon_i} \times$$
$$\times \prod_{i=r_0+1}^{r} \prod_{g=1}^{h_i} \Phi_{ig}(x_1^{u_{i1}}, \ldots, x_k^{u_{ik}})^{\varepsilon_i},$$

$$KF(x_1^{v_1}, \ldots, x_k^{v_k}) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{r_0} \prod_{g=1}^{h_i} J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}v_j/\delta_i}\Big)^{\varepsilon_i} \times$$
$$\times \prod_{i=r_0+1}^{r} \prod_{g=1}^{h_i} \Phi_{ig}(x_1^{v_1/\mu_{i1}}, \ldots, x_k^{v_k/\mu_{ik}})^{\varepsilon_i}.$$

Denoting the polynomials

$$J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}v_j/\delta_i}\Big) \quad (1 \leqslant i \leqslant r_0,\ 1 \leqslant g \leqslant h_i)$$

and

$$\Phi_{ig}(x_1^{v_1/\mu_{i1}}, \ldots, x_k^{v_k/\mu_{ik}}) \quad (r_0 < i \leqslant r,\ 1 \leqslant g \leqslant h_i)$$

by $F_1, \ldots, F_s$ we get (vi).

4. Lemma 13. *Let a_j $(0 \leqslant j \leqslant k)$ be non-zero integers. If*

$$a_0 + \sum_{j=1}^{k} a_j \lambda^{n_j} = a_0 + \sum_{j=1}^{k} a_j \lambda^{-n_j} = 0 \tag{67}$$

then either λ is an algebraic unit or there exist integers γ_j $(1 \leqslant j \leqslant k)$ such that

$$\sum_{j=1}^{k} \gamma_j n_j = 0 \tag{68}$$

and

$$0 < \max_{1 \leqslant j \leqslant k} |\gamma_j| < \max_{0 \leqslant j \leqslant k} \frac{\log a_j^2}{\log 2}. \tag{69}$$

Proof. If λ is not a unit then for a certain prime ideal $\mathfrak{p}$ of $\boldsymbol{Q}(\lambda)$ we have $\operatorname{ord}_{\mathfrak{p}} \lambda = \xi \neq 0$. Let p be the rational prime divisible by $\mathfrak{p}$ and let $\operatorname{ord}_{\mathfrak{p}} p = e$, $\operatorname{ord}_{\mathfrak{p}} a_j = \alpha_j$ $(0 \leqslant j \leqslant k)$. It follows from (67) that for $\varepsilon = \pm 1$ the minimal term of the sequence $\{e\alpha_j + \varepsilon n_j \xi\}$ $(j = 0, 1, \ldots, k)$ must occur in it at least twice (we take $n_0 = 0$). Thus we have for suitable non-negative indices g, h, i, j

$$\begin{aligned} e\alpha_g - n_g \xi &= e\alpha_h - n_h \xi, \quad g < h, \\ e\alpha_i + n_i \xi &= e\alpha_j + n_j \xi, \quad i < j. \end{aligned} \tag{70}$$

Hence

$$e(\alpha_i - \alpha_j)(n_h - n_g)\xi = e(\alpha_h - \alpha_g)(n_j - n_i)\xi,$$

and since $\xi \neq 0$

$$(\alpha_i - \alpha_j)(n_h - n_g) - (\alpha_h - \alpha_g)(n_j - n_i) = 0. \tag{71}$$

This gives the desired relation (68) unless

$$\alpha_i - \alpha_j = \alpha_h - \alpha_y = 0$$

or

$$\alpha_i - \alpha_j = \alpha_h - \alpha_g \quad \text{and} \quad i = g,\ j = h.$$

The latter possibility however reduces to the former and both give by (70) $n_g = n_h$, $n_i = n_j$. In order to get (69) we notice that the coefficients of n_g, n_h, n_i, n_j in (71) do not exceed

$$2 \max_{0 \leqslant j \leqslant k} \alpha_j \leqslant 2 \max_{0 \leqslant j \leqslant k} \frac{\log |a_j|}{\log p} \leqslant \max_{0 \leqslant j \leqslant k} \frac{\log a_j^2}{\log 2}.$$

Lemma 14. *If real numbers a_j $(0 \leqslant j \leqslant k)$ and a certain λ satisfy* (67) *and moreover*

$$0 < n_1 < n_2 < \ldots < n_k, \quad |a_0| + |a_k| \geqslant \sum_{j=1}^{k-1} |a_j| > 0 \tag{72}$$

then $|\lambda| = 1$.

Proof. Chose $\varepsilon = \pm 1$ so that $|a_k + \varepsilon a_0| = |a_k| + |a_0|$ and consider the polynomial

$$F(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j} + x^{n_k}\Big(a_0 + \sum_{j=1}^{k} a_j x^{-n_j}\Big).$$

$F(x)$ is reciprocal of degree n_k. By a theorem of A. Cohn ([2], p. 113) the equations $F(x) = 0$ and $x^{n_k - 1} F'(x) = 0$ have the same number of zeros inside the unit circle. We have

$$G(x) = x^{n_k-1}F'(x^{-1}) = x^{n_k-1}\Big(\sum_{j=1}^{k} a_j n_j x^{1-n_j} + \varepsilon a_0 n_k x^{1-n_k} + \varepsilon \sum_{j=1}^{k-1} a_j(n_k-n_j)x^{1+n_j-n_k}\Big)$$

$$= (a_k + a_0)n_k + \sum_{j=1}^{k-1} a_j n_j x^{n_k-n_j} + \sum_{j=1}^{k-1} a_j(n_k-n_j)x^{n_j}.$$

Assuming $G(x) = 0$ for $|x| < 1$ we get

$$|a_k+\varepsilon a_0|n_k < \sum_{j=1}^{k-1} |a_j|n_j + \sum_{j=1}^{k-1} |a_j|(n_k-n_j) = n_k \sum_{j=1}^{k-1} |a_j|,$$

$$|a_k| + |a_0| = |a_k + \varepsilon a_0| < \sum_{j=1}^{k-1} |a_j|,$$

a contradiction. Thus all zeros of $G(x)$ and $F(x)$ are on the unit circle. Since by (67) $F(\lambda) = 0$ we get $|\lambda| = 1$.

LEMMA 15. *If* $f(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ *satisfies* (72) *then either* $Kf(x) = Lf(x)$ *or there exist integers* $\gamma_1, \ldots, \gamma_k$ *satisfying* (68) *and* (69). *In any case*

$$\Omega\big(Kf(x)/Lf(x)\big) \leqslant \Omega_0\big((a_0, a_k)\big).$$

Proof. Let

$$\frac{Kf(x)}{Lf(x)} \overset{\text{can}}{=} c\prod_{i=1}^{h} f_i(x)^{e_i},$$

where $f_i(x)$ are primitive polynomials with the leading coefficients $c_i > 0$ $(1 \leqslant i \leqslant h)$. Comparing the leading coefficients on both sides we get

$$c = \prod_{i=1}^{h} c_i^{-e_i}.$$

Comparing the contents we get

$$C(Lf) = C(Kf)\prod_{i=1}^{h} c_i^{e_i}.$$

Since Lf has the same leading coefficient as f and the same up to a sign constant term it follows that

$$\prod_{i=1}^{h} c_i^{e_i} \,\Big|\, (a_0, a_k). \tag{73}$$

If for any $i \leqslant h$ we had $c_i = 1$ the zeros of f_i, which by Lemma 13 lie on the unit circle, by Kronecker's theorem would have to be roots of unity contrary to the definition of Kf. Thus for all $i \leqslant h$ we have $c_i > 1$ and (73) gives the second part of the lemma. To prove the first note that if $h > 0$ we can take for λ in Lemma 13 any zero of f_1.

LEMMA 16. *Let* $0 < n_1 < \ldots < n_k$ *and let* a_j $(0 \leqslant j \leqslant k)$ *be non-zero integers. If* $f(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ *satisfies for some* $g, h \leqslant k$

$$a_g^2 \not\equiv a_h^2 \bmod \underset{0\leqslant j\leqslant k}{\text{g.c.d.}}\, a_j \underset{j\neq g,h}{\text{g.c.d.}}\, a_j \tag{74}$$

then either $Lf(x) = Jf(x)$ *or there exist integers* γ_j $(1 \leqslant j \leqslant k)$ *satisfying* (68) *and* (69). *In any case* $\Omega\big(f(x)/Lf(x)\big) \leqslant \Omega_0\big((a_0, a_k)\big)$.

Proof. Let

$$\frac{f(x)}{Lf(x)} \overset{\text{can}}{=} c\prod_{i=1}^{h} f_i(x)^{e_i},$$

where $f_i(x)$ are primitive polynomials with the leading coefficients $c_i > 0$. By the argument used in the proof of Lemma 15 we deduce again the divisibility (73).

If for $i \leqslant h$ we had $c_i = 1$ any zero λ of f_i would be a unit and would satisfy (67). Setting

$$\underset{0\leqslant j\leqslant k}{\text{g.c.d.}}\, a_j = \delta, \qquad \underset{j\neq g,h}{\text{g.c.d.}}\, a_j = d$$

we would get from (67)

$$a_g\lambda^{n_g} + a_h\lambda^{n_h} \equiv 0 \bmod d, \qquad a_g\lambda^{-n_g} + a_h\lambda^{-n_h} \equiv 0 \bmod d;$$

$$a_g\delta^{-1} \equiv -a_h\delta^{-1}\lambda^{n_h-n_g} \bmod d\delta^{-1}, \qquad a_g\delta^{-1} \equiv -a_h\delta^{-1}\lambda^{n_g-n_h} \bmod d\delta^{-1};$$

$$a_g^2\delta^{-2} \equiv a_h^2\delta^{-2} \bmod d\delta^{-1}; \qquad a_g^2 = a_h^2 \bmod d\delta$$

contrary to (74). Thus for $i \leqslant h$ we have $c_i > 1$ and (73) gives the second part of the lemma. The first follows from Lemma 13 on taking for λ any hypothetical zero of $f(x)/Lf(x)$.

Proof of Theorem 3. By Theorem 4 of [11] either $Lf(x)$ is irreducible or there are integers $\gamma_1, \ldots, \gamma_k$ satisfying (vii) and (viii). All zeros of the quotient $f(x)/Lf(x)$ satisfy the assumptions of Lemma 13. Since (69) implies (viii) it follows that unless (vii) and (viii) are satisfied all primitive factors of $f(x)/Lf(x)$ are reciprocal and monic. The remaining part of the theorem follows at once from Lemmata 15 and 16.

5. LEMMA 17. *If* $|a_0| = |a_3| > 0$, $|a_1| = |a_2| > 0$ *and* $0 < n_1 < n_2 < n_3$ *then either the quadrinomial* $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ *is reciprocal or* $Kq(x) = Lq(x)$.

Proof. $q(\lambda) = q(\lambda^{-1}) = 0$ implies

$$a_0 + a_3\lambda^{n_3} = -a_1\lambda^{n_1} - a_2\lambda^{n_2},$$
$$a_0 + a_3\lambda^{-n_3} = -a_1\lambda^{-n_1} - a_2\lambda^{-n_2}.$$

Dividing the above equalities side by side we get

$$\frac{a_3}{a_0}\lambda^{n_3} = \frac{a_2}{a_1}\lambda^{n_2+n_1},$$

and either λ is a root of unity or $n_3 = n_2 + n_1$ and $a_3/a_0 = a_2/a_1$ in which case $q(x)$ is reciprocal.

Lemma 18. *If a quadrinomial $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ is representable in one of the forms* (1), *where k, T, U, V, W are monomials in $\boldsymbol{Q}(x)$ then it is also representable in the same form where $\pm k = C(q)$, T, U, V, W are monomials in $\boldsymbol{Z}[x]$ and the factors on the right hand side of* (1) *differ from the original ones by monomial factors.*

Proof. Let $T = \frac{t}{m^3}x^{\tau}$, $U = \frac{u}{m}x^{\varphi}$, $V = \frac{v}{m}x^{\psi}$, $W = \frac{w}{m}x^{\omega}$, $k = k'x^{\varkappa}$, where $m, t, u, v, w \in \boldsymbol{Z}$, $m > 0$.

If

$$q(x) = k(T^2 - 4TUVW - U^2V^4 - 4U^2W^4)$$

we have

$$\begin{aligned}\varkappa &= -\min(2\tau, \tau+\varphi+\psi+\omega, 2\varphi+4\psi, 2\varphi+4\omega)\\ &= -2\min(\tau, \varphi+2\psi, \varphi+2\omega),\end{aligned}$$

(75)

$$C(q) = |k'|\frac{(t^2, 4tuvw, u^2v^4, 4u^2w^4)}{m^6} = |k'|\frac{(t, uv^2, 2uw^2)^2}{m^6}.$$

Taking

$$k_0 = C(q)\operatorname{sgn}k', \quad T_0 = \frac{m^3}{(t, uv^2, 2uw^2)}Tx^{\varkappa/2},$$

$$U_0 = \frac{m(v^2, 2w^2)}{(t, uv^2, 2uw^2)}Ux^{\varkappa/2+2\min(\psi,\omega)},$$

$$V_0 = \frac{m}{(v, 2w)}Vx^{-\min(\psi,\omega)}, \quad W_0 = \frac{m}{(v, w)}Wx^{-\min(\psi,\omega)}$$

we find in view of (75)

$$q(x) = k_0(T_0^2 - 4T_0U_0V_0W_0 - U_0^2V_0^4 - 4U_0^2W_0^4)$$

and clearly

(76) $$T_0, U_0, V_0, W_0 \in \boldsymbol{Z}[x].$$

Moreover the factors on the right hand side of (1) differ from the original ones by the factor $x^{\varkappa/2}$.

If

$$q(x) = k(U^3 + V^3 + W^3 - 3UVW)$$

we have

$$\varkappa = -\min(3\varphi, 3\psi, 3\omega, \varphi+\psi+\omega) = -3\min(\varphi, \psi, \omega),$$

(77)

$$C(q) = |k'|\frac{(u^3, v^3, w^3, 3uvw)}{m^3} = \frac{|k'|}{m^3}(u, v, w)^3.$$

Taking

$$k_0 = C(q)\operatorname{sgn}k', \quad U_0 = U\frac{m}{(u, vw)}x^{\varkappa/3}, \quad V_0 = V\frac{m}{(u, v, w)}x^{\varkappa/3},$$

$$W_0 = W\frac{m}{(u, v, w)}x^{\varkappa/3}$$

we find in view of (77)

$$q(x) = k_0(U_0^3 + V_0^3 + W_0^3 - 3U_0V_0W_0)$$

and again (76). The first and the second factor on the right hand side of (1) differ from the original ones by the factor $x^{\varkappa/3}$ and $x^{2\varkappa/3}$, respectively.

Finally, if

$$q(x) = k(U^2 + 2UV + V^2 - W^2)$$

we have

$$\varkappa = -\min(2\varphi, \varphi+\psi, 2\psi, 2\omega) = -2\min(\varphi, \psi, \omega),$$

(78)

$$C(q) = |k'|\frac{(u^2, 2uv, v^2, w^2)}{m^2} = |k'|\frac{(u, v, w)^2}{m^2}.$$

Taking

$$k_0 = C(q)\operatorname{sgn}k', \quad U_0 = U\frac{m}{(u, v, w)}x^{\varkappa/2}, \quad V_0 = V\frac{m}{(u, v, w)}x^{\varkappa/2},$$

$$W_0 = W\frac{m}{(u, v, w)}x^{\varkappa/2}$$

we find in view of (78)

$$q(x) = k_0(U_0^2 + 2U_0V_0 + V_0^2 - W_0^2)$$

and again (76). The factors on the right hand side of (1) differ now from the original ones by the factor $x^{\varkappa/2}$.

Proof of Theorem 4. With $Kq(x)$ replaced by $Lq(x)$ the theorem has been actually proved in the course of proof of Theorem 2 in [3], see namely formula (20) there and the subsequent argument. We shall have soon to go through the same argument again and then we shall supply a few details missing there or peculiar to the present context (e.g. the application of Lemma 18), taking them now for granted.

By Lemma 15, 16 and 17 we have $Kq(x) = Lq(x)$ unless (68) and (69) hold with $k = 3$. Therefore we shall assume these relations for a certain integral vector $\gamma = [\gamma_1, \gamma_2, \gamma_3]$. Integral vectors perpendicular to γ form a module, say $\mathfrak{N}$. We have $[\gamma_2, \gamma_1, 0]$, $[\gamma_3, 0, -\gamma_1]$, $[0, \gamma_3, -\gamma_2] \in \mathfrak{N}$ and since $\gamma \neq 0$ two among these three vectors are linearly independent. By Lemma 6 of [11] $\mathfrak{N}$ has a basis which written in the form of a matrix $\Delta = [\delta_{tj}]_{\substack{t\leqslant 2\\ j\leqslant 3}}$ satisfies

(79) $$\max_{t,j}|\delta_{tj}| \leqslant 2\max_j|\gamma_j| \leqslant 4\frac{\log\|q\|}{\log 2}.$$

Moreover,

(80) $$\operatorname{rank}\Delta = 2$$

and by (67)

(81) $$[n_1, n_2, n_3] = [m_1, m_2]\Delta, \qquad [m_1, m_2] \text{ integral} \neq 0.$$

Since $0 < n_1 < n_2 < n_3$ the vectors $[\delta_{1j}, \delta_{2j}]$ $(j = 1, 2, 3)$ are distinct and different from $[0, 0]$. Let us set

(82) $$Q_0(y_1, y_2) = J\Big(a_0 + \sum_{j=1}^{3} a_j y_1^{\delta_{1j}} y_2^{\delta_{2j}}\Big).$$

By (81) we have

(83) $$q(x) = JQ_0(x^{m_1}, x^{m_2}).$$

Since $q(x)$ is not reciprocal $Q_0(y_1, y_2)$ is also not reciprocal. Thus by Theorem 1 of [3]

(84) $$LQ_0(y_1, y_2) = Q_0(y_1, y_2) \quad \text{or} \quad \frac{Q_0(y_1, y_2)}{D_0(y_1, y_2)}LD_0(y_1, y_2),$$

where D_0 is a certain binomial defined there. Now, for binomials

$$KLD_0(y_1, y_2) = KD_0(y_1, y_2);$$

on the other hand by Lemma 11 of [11]

$$KLQ_0(y_1, y_2) = LQ_0(y_1, y_2).$$

Applying the operation K to both sides of (84) we get

$$LQ_0(y_1, y_2) = KQ_0(y_1, y_2).$$

Now we apply Theorem 3 of [11] setting there $F(x_1, x_2) = Q_0(x_1, x_2)$. By that theorem there exists an integral matrix $\boldsymbol{M} = [\mu_{ij}]_{\substack{i\leqslant r\\ j\leqslant 2}}$ of rank $r \leqslant 2$ and an integral vector $\boldsymbol{v} = [v_1, v_r]$ such that

(85) $$\max_{i,j}|\mu_{ij}| \leqslant \begin{cases} \exp 9\cdot 2^{\|Q_0\|-4} & \text{if} \quad r = 2,\\ \exp\big(500\,\|Q_0\|^2(2\,|Q_0|^*)^{2\|Q_0\|+1}\big) & \text{if} \quad r = 1;\end{cases}$$

(86) $$[m_1, m_2] = \boldsymbol{vM};$$

(87) $$KQ_0\Big(\prod_{i=1}^{r} y_i^{\mu_{i1}}, \prod_{i=1}^{r} y_i^{\mu_{i2}}\Big) \overset{\text{can}}{=} \text{const}\prod_{\sigma=1}^{s} F_\sigma(y_1, y_r)^{e_\sigma}$$

implies

(88) $$KQ_0(x^{m_1}, x^{m_r}) \overset{\text{can}}{=} \text{const}\prod_{\sigma=1}^{s} KF(x^{v_1}, x^{v_r})^{e_\sigma}.$$

In (86) $|Q_0|^* = \sqrt{\max\{2, |Q_0|^2\} + 2}$.

Let us set

(89) $$\boldsymbol{N} = [\nu_{ij}]_{\substack{i\leqslant r\\ j\leqslant 3}} = \boldsymbol{M}\Delta.$$

It follows from (80) that $\boldsymbol{N}$ is of rank r and from (81) and (86) that

(90) $$[n_1, n_2, n_3] = \boldsymbol{vN}.$$

Consider first the case $r = 2$ and put

$$Q(y_1, y_2) = JQ_0\Big(\prod_{i=1}^{2} y_i^{\mu_{i1}}, \prod_{i=1}^{2} y_i^{\mu_{i2}}\Big).$$

By (82) and (89)

$$Q(y_1, y_2) = J\Big(a_0 + \sum_{j=1}^{3} a_j y_1^{\nu_{1j}} y_2^{\nu_{2j}}\Big).$$

By (90) the vectors $[\nu_{1j}, \nu_{2j}]$ are distinct and different from $[0, 0]$, moreover

(91) $$q(x) = JQ(x^{v_1}, x^{v_2}).$$

Now by Theorem 1 of [3] we have the following possibilities.

(92) $Q(y_1, y_2)$ is irreducible.

(93) $Q(y_1, y_2)$ can be divided into two parts with the highest common factor $D(y_1, y_2)$ being a binomial. Then QD^{-1} is either irreducible and non-reciprocal or binomial.

(94) $Q(y_1, y_2)$ can be represented in one of the forms (1), where $k \in \boldsymbol{Q}$ and T, U, V, W are monomials in $\boldsymbol{Q}[y_1, y_2]$. The factors on the right hand side of (1) are irreducible and non-reciprocal.

(We have made in comparison to [3] a certain permutation of letters and formulae.)

In the case (92) we have on the right hand side of (87) at most one irreducible factor. By (83) and (88) the same applies to the canonical factorization of $Kq(x)$. Since $q(x)$ is not reciprocal, $Kq(x) \neq \text{const}$ and (xii) follows.

In the case (93) in virtue of (91) $q(x)$ can be divided into two parts that have the common factor $JD(x^{v_1}, x^{v_2}) = d(x)$ which is either binomial or constant. We get

$$q(x)d^{-1}(x) = JQ(x^{v_1}, x^{v_2})D^{-1}(x^{v_1}, x^{v_2}).$$

If qd^{-1} is not a binomial we conclude that QD^{-1} is not a binomial either. Hence QD^{-1} is irreducible and non-reciprocal. From $LQD^{-1} = QD^{-1}$ we infer by Lemma 11 of [11] that $KQD^{-1} = QD^{-1}$. Thus by (88)

$$K\big(Q(x^{v_1}, x^{v_2})D^{-1}(x^{v_1}, x^{v_2})\big) = K\big(q(x)d^{-1}(x)\big)$$

is irreducible. If $d(x)$ is reciprocal, $Kd(x) = \text{const}$ and we get (xii); if $d(x)$ is not reciprocal we get (xiii).

In the case (94) we get from Lemma 11 of [11] that $KQ = Q$. The factorization (87) is given by the formulae (1). Taking for F_1, F_2 the two factors occurring on the right hand side of (1) we infer from (88) that $KF_\sigma(x^{v_1}, x^{v_2})$ $(\sigma = 1, 2)$ are irreducible. Now by (91) to the representation of $Q(y_1, y_2)$ in any one of the forms (1) there corresponds a representation of $q(x)$ in the same form, where k, T, U, V, W are now monomials in $Q(x)$ and the factors on the right hand side of (1) are $F_\sigma(x^{v_1}, x^{v_2})$ $(\sigma = 1, 2)$. By Lemma 18 there exists a representation of $q(x)$ in the form in question in which $k = \pm(a_0, a_1, a_2, a_3)$ and T, U, V, W are monomials in $\boldsymbol{Z}[x]$. Since the relevant factors differ from $F_\sigma(x^{v_1}, x^{v_2})$ $(\sigma = 1, 2)$ only by monomial factors we infer that their kernels are irreducible. This gives (xiv). It remains to consider the case $r = 1$. The change of signs of μ_{1i} $(1 \leqslant i \leqslant 3)$ in (87) leads to a replacement of $F_\sigma(y_1)$ by $JF_\sigma(y_1^{-1})$ but does not affect the implication (87)→(88). Therefore, changing the signs of μ_{1i} if necessary we can assume that $v = v_1 > 0$. Hence by (90)

$$0 < \nu_{11} < \nu_{12} < \nu_{13}. \tag{95}$$

By (79), (85) and (95) we have

$$\nu_{13} = \max_{1 \leqslant j \leqslant 3} |\nu_{1j}| \leqslant 8\,\frac{\log\|q\|}{\log 2}\exp\big(500\,\|Q_0\|^2(2\,|Q_0|^*)^{2\|Q_0\|+1}\big).$$

Now by (82) and (79)

$$\|Q_0\| = \|q\|,$$

$$|Q_0|^* \leqslant |Q_0| + 1 \leqslant 2\max_{i,j}|\delta_{ij}| + 1 \leqslant 8\,\frac{\log\|q\|}{\log 2} + 1 < 13\log\|q\|$$

and we get

$$\nu_{13} \leqslant 12\log\|q\|\exp\big(500\,\|q\|^2(26\log\|q\|)^{2\|q\|+1}\big)$$
$$< \exp\big(600\,\|q\|^2(26\log\|q\|)^{2\|q\|+1}\big) < \exp_2(12\cdot 2^{\|q\|}\log\|q\|).$$

Let us set $\nu_{1j} = \nu_j$ $(1 \leqslant j \leqslant 3)$. By (90) we have

$$n_j = v\nu_j \quad (1 \leqslant j \leqslant 3).$$

By (82) and (89)

$$JQ_0(y_1^{\mu_{11}}, y_1^{\mu_{12}}) = J\Big(a_0 + \sum_{j=1}^{3} a_j y_1^{\nu_{1j}}\Big).$$

The last assertion of (xiv) follows now from the implication (87)→(88).

To estimate $\Omega\big(Kq(x)\big)$ we use Corollary to Lemma 1, Theorem 3 and Lemma 17. We get

$$\Omega\big(Kq(x)\big) \leqslant \Omega\big(Lq(x)\big) + \Omega_0\big((a_0, a_3)\big) \leqslant \frac{\log\|q\|}{2\log\vartheta_0} + \frac{\log a_0^2}{2\log 2}$$
$$< \Big(\frac{1}{2\log\vartheta_0} + \frac{1}{2\log 2}\Big)\log\|q\|.$$

Proof of Corollary 4 does not differ from the proof of Corollary in [3]. We note only that if

$$a_0 + \sum_{i=1}^{3} a_i \zeta^{n_i/(n_1, n_2, n_3)} = 0, \qquad \zeta^6 = 1$$

then $q(x)$ is indeed reducible since none of the cyclotomic polynomials of index d $(d|6)$ is a quadrinomial.

Note concerning the paper [11]

On p. 133 the writer considered the system of equations

$$\begin{aligned} x_0 &= 0, \\ x_j - x_i - x_{h_{ij}} + x_{g_{ij}} &= 0, \quad \langle i, j\rangle \neq \langle i_1, j_1\rangle, \ldots, \langle i_{p_0}, j_{p_0}\rangle, \\ x_{jp} - x_{ip} - \sum_{q=1}^{k} c_{pq} y_q &= 0 \quad (1 \leqslant p \leqslant p_0) \end{aligned} \tag{96}$$

satisfied by distinct integers x_i $(0 \leqslant i \leqslant l)$ and y_q $(1 \leqslant q \leqslant k)$, where $0 < x_1 < \ldots < x_l$. Here c_{pq} are integers and $\langle h_{ij}, g_{ij}\rangle \neq \langle i, j\rangle$.

The matrix of the system obtained from (96) by cancelling the first equation and substituting $x_0 = 0$ in the others has been denoted by $\boldsymbol{A}$, the matrix of the resulting coefficients of the x's by $\boldsymbol{B}$ and of the y's by $-\boldsymbol{\Gamma}$.

$\varDelta$ has been a nonsingular submatrix of $\boldsymbol{B}$ of degree l containing a row $[0, \ldots, 0, 1]$, and $\boldsymbol{K}'$ a matrix formed of determinants obtained from $\varDelta$ by replacing one column by a column of $\boldsymbol{\varGamma}$. It has been stated that by Hadamard's inequality

$$(97)\qquad |D| \leqslant 2^{l-1}, \quad h(\boldsymbol{K}') \leqslant (\max\{c^2, 2\}+2)^{l/2}$$

where $D = \det\varDelta$, $h(\boldsymbol{K}')$ is the maximum of the absolute values of the elements of $\boldsymbol{K}'$ and $|c_{pq}| \leqslant c$.

Now it may happen, although not simultaneously, that $j = g_{ij}$ or $i = h_{ij}$ and then Hadamard's inequality gives only

$$(98)\qquad |D| \leqslant \sqrt{6}^{l-1}, \quad h(\boldsymbol{K}') \leqslant (\max\{c^2, 4\}+2)^{l/2}.$$

Nevertheless the inequalities (97) are valid in virtue of the following inequality true for determinants with real entries (see [17]):

$$(99)\qquad |\det(a_{ij})_{i,j\leqslant k}| \leqslant \prod_{i=1}^{k} \max\Big(\sum_{\substack{j\\ a_{ij}>0}} a_{ij},\ -\sum_{\substack{j\\ a_{ij}<0}} a_{ij}\Big).$$

In the case of $D = \det\varDelta$ all the factors on the right hand side of (99) are at most 2 and one of them corresponding to the distinguished row is 1.

In the case of $h(\boldsymbol{K}')$ the difference between (97) and (98) occurs only if $c < 2$. But then $|c_{pq}| \leqslant 1$ and the application of (99) gives $h(\boldsymbol{K}') \leqslant 2^l$, i.e. again (97).

Note added in proof. Very recently E. Dobrowolski has proved the following improvement of Blanksby–Montgomery's theorem.

If $a^{(j)}$ are conjugates of an algebraic integer a different from 0 and roots of unity then

$$\prod_{|a^{(j)}|>1} |a^{(j)}| > 1 + c\left(\frac{\log\log n}{\log n}\right)^3, \quad c > 0.$$

This result allows one to improve the estimates given in Lemma 1 and Theorem 1 and in particular to obtain

$$\log c(E) \ll (|KF|\log\|F\|)^{1/3}(\log 2|KF| + \log_2\|F\|)^{2/3}.$$

Here neither the exponent 1/3 nor the exponent 2/3 can be lowered.

References

[1] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. 18 (1971), pp. 358–369.

[2] A. Cohn, *Über die Anzahl der Wurzeln einer algebraischen Gleichung in einem Kreise*, Math. Zeitschr. 14 (1922), pp. 110–148.

[3] M. Fried and A. Schinzel, *Reducibility of quadrinomials*, Acta Arith. 21 (1972), pp. 153–171.

[4] E. Gourin, *On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves*, Trans. Amer. Math. Soc. 32 (1931), pp. 485–501.

[5] H. Halberstam and H. E. Richert, *Sieve methods*, London–New York–San Francisco 1974.

[6] E. Landau, *Sur quelques théorèmes de M. Petrovitch relatifs aux zéros des fonctions analytiques*, Bull. Soc. Math. France 33 (1905), pp. 1–11.

[7] — *Handbuch der Lehre von der Verteilung der Primzahlen*, reprint New York 1953.

[8] H. B. Mann, *Linear relations between roots of unity*, Mathematika 12 (1965), pp. 107–117.

[9] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), pp. 64–89.

[10] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11 (1965), pp. 1–34.

[11] — *Reducibility of lacunary polynomials I*, ibid. 16 (1969), pp. 123–159.

[12] — *Reducibility of lacunary polynomials*, Proc. Symposia Pure Math. 20 (1971), pp. 135–149.

[13] — *Reducibility of polynomials*, Actes du Congrès International des mathématiciens 1970, vol. 1, Paris 1971, pp. 491–496.

[14] — *A general irreducibility criterion*, J. Indian Math. Soc. 37 (1973), pp. 1–8.

[15] — *On the number of irreducible factors of a polynomial*, Colloq. Math. Soc. János Bolyai 13 (1976), pp. 305–314.

[16] — *Abelian binomials, power residues and exponential congruences*, Acta Arith. 32 (1976), pp. 245–274.

[17] — *An inequality for determinants with real entries*, Colloq. Math. 38 (1978), pp. 319–321.

[18] A. Schinzel and J. Wójcik, *A note on the paper "Reducibility of lacunary polynomials I"*, Acta Arith. 19 (1971), pp. 195–201.

[19] R. Sivaramakrishnan, *Generalization of an arithmetic function*, J. Indian Math. Soc. 33 (1969), pp. 127–132.

[20] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), pp. 163–175.

[21] N. Tschebotaröw und H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie*, Groningen-Djakarta 1950.

Corrections to [3], [11], [13] and [14]

[3] p. 166 line 14 for (2) read (3)
p. 168 line -14 for $g(x)$ read $q(x)$
p. 169 line 8 for $LF_\sigma(x^{\nu_1}, x^{\nu_2})$ read $LF_\sigma(x^{v_1}, x^{v_2})$
p. 170 line -4 for $a\varepsilon p\lambda^{n+m-p}$ read $c\varepsilon p\lambda^{n+m-p}$

[11] in addition to those given in [18]
p. 124 line -11 for $F_\sigma(x^u)^{e_\sigma}$ read $JF_\sigma(x^u)^{e_\sigma}$
p. 127 line -2 for Mongomery read Montgomery
p. 134 line 6 for $\varLambda$ read $\boldsymbol{A}$
p. 136 line -3 for $F(x^{n_1}, \ldots, x^{n_k})$ read $JF(x^{n_1}, \ldots, x^{n_k})$
p. 137 line 2 for $f(x)$ read $f(x^{-1})$
p. 158 line 15 for 19 read 18

[13] p. 49 line 10 for F read an irreducible F

[14] p. 2 line -3 for x_1 read x_i
p. 5 line 5 for μ_{1s} read μ_{2s}
line 8 for $\mu_{10}, \ldots, \mu_{1t}$ read $\mu_{20}, \ldots, \mu_{2t}$
p. 8 line -13 for $\sum\limits_{j=1}^{2l-1}$ read $\sum\limits_{j=l}^{2l-1}$
line -10 for $m-2$ read twice $m-1$
line -7 for $j \leqslant l$ read $j < l$
for $\sum\limits_{j=1}^{l} \gamma_j = 0$ read $\sum\limits_{j=1}^{l-1} \gamma_j = \gamma_l$
line -6 for $[0, \ldots, 0, 1, 0, \ldots, 0, -1, 0, \ldots, 0, -1, 0, \ldots, 0]$
read $[0, \ldots, 0, 1, 0, \ldots, 0, 1, 0, \ldots, 0, -1, 0, \ldots, 0]$

Received on 1. 10. 1976 (8