ACTA ARITHMETICA
XXVIII (1975)

On linear dependence of roots

by

A. SCHINZEL (Warszawa)

In memory of Professor L. J. Mordell

L. J. Mordell [4] has proved in 1953 the following theorem. Let K be an algebraic number field, $a_1, \ldots, a_k$ elements of K, $n_1, \ldots, n_k$ positive integers, $\xi_i^{n_i} = a_i$ $(1 \leqslant i \leqslant k)$. If $\prod_{i=1}^{k} \xi_i^{x_i} \in K$ implies $x_i \equiv 0 \bmod n_i$ and either the numbers ξ_i are real or K contains n_ith roots of unity $(1 \leqslant i \leqslant k)$ then the degree of the extension $K(\xi_1, \ldots, \xi_k)$ over K is $n_1 \ldots n_k$. This theorem has been recently extended by C. L. Siegel [7] and M. Kneser [3].

The latter obtained the following purely algebraic result. Let K be any field, $K(\xi_1, \ldots, \xi_k)$ a separable extension of K and $K^*\langle \xi_1, \ldots, \xi_k\rangle$ the multiplicative group generated by $\xi_1, \ldots, \xi_k$, all of finite order, over K^*. The degree $[K(\xi_1, \ldots, \xi_k):K]$ is equal to the index $[K^*\langle \xi_1, \ldots \ldots, \xi_k\rangle : K^*]$ if and only if for every prime p, $\zeta_p \in K^*\langle \xi_1, \ldots, \xi_k\rangle$ implies $\zeta_p \in K$ and $1+\zeta_4 \in K^*\langle \xi_1, \ldots, \xi_k\rangle$ implies $\zeta_4 \in K$, where ζ_q is a primitive qth root of unity.

We shall use Kneser's theorem to get a necessary and sufficient condition for the field $K(\xi_1, \ldots, \xi_k)$ to be of degree $n_1 \ldots n_k$ over K.

THEOREM 1. *Let K be any field. Assume that the characteristic of K does not divide $n_1 \ldots n_k$ and $\xi_i^{n_i} = a_i \in K^*$. $[K(\xi_1, \ldots, \xi_k):K] = n_1 \ldots n_k$ if and only if for all primes p $\prod_{p|n_i} a_i^{x_i} = \gamma^p$ implies $x_i \equiv 0 \bmod p$ $(p|n_i)$ and $\prod_{2|n_i} a_i^{x_i} = -4\gamma^4$, $n_i x_i \equiv 0 \bmod 4$ $(2|n_i)$ implies $x_i \equiv 0 \bmod 4$ $(2|n_i)$* (1).

The above theorem can be regarded as a generalization of Capelli's theorem which corresponds to the case $k = 1$. It should however be noted that Capelli's theorem holds without any condition on the characteristic of K (see [5], Theorem 428) while Theorem 1 does not, as it is shown by the example $K = Z_2(t)$, $n_1 = n_2 = 2$, $a_1 = t$, $a_2 = t+1$.

---

(1) $(p|n_i)$ means here "for all i such that $p|n_i$".

We have further

THEOREM 2. *Assume that the characteristic of K does not divide $n_1 \ldots n_k$. If either $\zeta_4 \in K$ or $n_i x_i \equiv 0 \bmod 4$ $(2|n_i)$ implies $\prod\limits_{2|n_i} a_i^{x_i} \neq -\gamma^4, -4\gamma^4$ then there exist elements $\xi_1, \ldots, \xi_k$ such that $\xi_i^{n_i} = a_i$ and*

$$[K(\xi_1, \ldots, \xi_k):K] = [K^*\langle\xi_1, \ldots, \xi_k\rangle:K^*]. \tag{1}$$

It follows from Kneser's theorem that if $\zeta_4 \notin K$ and for some x_i, $n_i x_i \equiv 0 \bmod 4$ $(2|n_i)$, $\prod\limits_{2|n_i} a_i^{x_i} = -4\gamma^4$ then for no choice of $\xi_1, \ldots, \xi_k$ satisfying $\xi_i^{n_i} = a_i$ the equality (1) holds. The example $K = Q$, $n_1 = n_2 = 8$, $a_1 = -1$, $a_2 = -16$ shows that the converse is not true. Indeed for any choice of ξ_1, ξ_2 we get

$$[K(\xi_1, \xi_2):K] = 8 < [K^*\langle\xi_1, \xi_2\rangle:K^*] = 16.$$

It seems difficult to give a simple necessary and sufficient condition for the existence of $\xi_1, \ldots, \xi_k$ satisfying (1). On the other hand Theorem 1 combined with some results of [6] leads to a necessary and sufficient condition for the following phenomenon: each of the fields $K(\xi_1, \ldots, \xi_k)$ contains at least one η with $\eta^n = \beta$ (β and n fixed, $n_i|n$). Condition given in [6] was necessary but not always sufficient. We shall prove even a more precise result.

THEOREM 3. *Let τ be the largest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$, if there are only finitely many of them, otherwise $\tau = \infty$. Let $n_1, \ldots, n_k$ be positive integers, $a_1, \ldots, a_k$ non-zero elements of K. There exist elements $\xi_1, \ldots, \xi_k$ with $\xi_i^{n_i} = a_i$ $(1 \leqslant i \leqslant k)$ such that for all n divisible by $n_1, \ldots, n_k$, but not by the characteristic of K and for all $\beta \in K$: if $K(\xi_1, \ldots, \xi_k)$ contains at least one η with $\eta^n = \beta$ then at least one of the following three conditions is satisfied for suitable rational integers $l_1, \ldots, l_k, q_1, \ldots, q_k$ and suitable $\gamma, \delta \in K$.*

(i) $\beta \prod\limits_{i=1}^{k} a_i^{q_i \frac{n}{n_i}} = \gamma^n$,

(ii) $n \not\equiv 0 \bmod 2^\tau$, $\prod\limits_{2|n_i} a_i^{l_i} = -\delta^2$, $\beta \prod\limits_{i=1}^{k} a_i^{q_i \frac{n}{n_i}} = -\gamma^n$,

(iii) $n \equiv 0 \bmod 2^\tau$, $\prod\limits_{2|n_i} a_i^{l_i} = -\delta^2$, $\beta \prod\limits_{i=1}^{k} a_i^{q_i \frac{n}{n_i}} = (-1)^{n/2^\tau}(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}\gamma^n$.

Conversely if any of the above conditions is satisfied then each of the fields $K(\xi_1, \ldots, \xi_k)$ where $\xi_i^{n_i} = a_i$ contains at least one η with $\eta^n = \beta$.

If $\zeta_4 \in K$ the conditions (ii), (iii) *imply* (i); *if $\tau = 2$* (ii) *implies* (i) *for not necessarily the same $q_1, \ldots, q_k$ and γ.*

This theorem can be regarded as an extension of the classical result concerning Kummer fields ([2], p. 42).

Let us write for two irreducible polynomials f and g over K $f \sim g$ if $f(a_1) = 0$ and $g(a_2) = 0$ where $K(a_1) = K(a_2)$. The relation $\sim$ introduced by Gerst [1] is reflexive, symmetric and transitive.

Theorem 3 implies

COROLLARY. *Two polynomials $f(x) = x^n - a$ and $g(x) = x^n - \beta$ irreducible over K satisfy $f \sim g$ if and only if either $\beta a^r = \gamma^n$ or $n \equiv 0 \pmod{2^{\tau+1}}$, $a = -\delta_1^2$, $\beta = -\delta_2^2$ and $\beta a^r = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}\gamma^n$ with $\gamma, \delta_1, \delta_2 \in K$.*

This is a generalization of Theorem 5 of Gerst [1] corresponding to the case $K = Q$. (Note that the irreducibility of g implies $(r, n) = 1$.)

For the proof we need several lemmata.

LEMMA 1. *If $(a_i, b_i) = 1$ and $b_i | m$ $(1 \leqslant i \leqslant k)$ then*

$$\left(m\frac{a_1}{b_1}, \ldots, m\frac{a_k}{b_k}\right) = m\frac{(a_1, \ldots, a_k)}{[b_1, \ldots, b_k]}.$$

Proof (by induction with respect to k). For $k = 1$ the formula is obvious, for $k = 2$ we have

$$\left(m\frac{a_1}{b_1}, m\frac{a_2}{b_2}\right) = \frac{m}{b_1 b_2}(a_1 b_2, a_2 b_1) = \frac{m}{b_1 b_2}(a_1, a_2)(b_1, b_2) = m\frac{(a_1, a_2)}{[b_1, b_2]}.$$

Now assume that the lemma holds for k terms. Then if $b_i | m$ $(1 \leqslant i \leqslant k+1)$ we have

$$\left(m\frac{a_1}{b_1}, \ldots, m\frac{a_{k+1}}{b_{k+1}}\right) = \left(m\frac{(a_1, \ldots, a_k)}{[b_1, \ldots, b_k]}, m\frac{a_{k+1}}{b_{k+1}}\right) = m\frac{(a_1, \ldots, a_k, a_{k+1})}{[b_1, \ldots, b_{k+1}]},$$

and the proof is complete.

Proof of Theorem 1. Necessity. Suppose that for a certain prime p, a certain $\gamma \in K$ and some x_i, $\prod\limits_{p|n_i} a_i^{x_i} = \gamma^p$, but for a certain i $p | n_i$, $p \nmid x_i$.

Then for a suitable j

$$\prod_{p|n_i} \xi_i^{x_i \frac{n_i}{p}} = \zeta_p^j \gamma, \tag{2}$$

$\zeta_p^j \in K^*\langle\xi_1, \ldots, \xi_k\rangle$ and by Kneser's theorem either $\zeta_p^j \in K$ or $[K(\xi_1, \ldots, \xi_k):K] < [K^*\langle\xi_1, \ldots, \xi_k\rangle:K^*]$.

In the former case by (2) $[K^*\langle\xi_1, \ldots, \xi_k\rangle:K^*] < n_1 \ldots n_k$, in both cases $[K(\xi_1, \ldots, \xi_k):K] < n_1 \ldots n_k$.

Suppose now that for some x_i and a certain $\gamma \in K$ $\prod\limits_{2|n_i} a_i^{x_i} = -4\gamma^4$, $n_i x_i \equiv 0 \bmod 4$ $(2|n_i)$ but for a certain i $2|n_i$, $4 \nmid x_i$. Then for a suitable j

$$\prod_{2|n_i} \xi_i^{\frac{x_i n_i}{4}} = \zeta_4^j (1 + \zeta_4)\gamma, \tag{3}$$

$1 + \zeta_4 \in K\langle\xi_1, \ldots, \xi_k\rangle$ (Note that $\zeta_4(1+\zeta_4) = -2(1+\zeta_4)^{-1}$.) and by Kneser's theorem either $\zeta_4 \in K$ or $[K(\xi_1, \ldots, \xi_k):K] < [K^*\langle\xi_1, \ldots, \xi_k\rangle:K^*]$.

In the former case by (3) $[K^*\langle\xi_1, \dots, \xi_k\rangle : K^*] < n_1 \dots n_k$, in both cases $[K(\xi_1, \dots, \xi_k):K] < n_1 n_2 \dots n_k$.

Sufficiency. Suppose that for a certain prime p and a $\gamma \in K$

$$\zeta_p = \gamma \prod_{i=1}^{k} \xi_i^{x_i}.$$

Let $m = [n_1/(n_1, x_1), \dots, n_k/(n_k, x_k)]$. If $p|m$ we get

$$\prod_{i=1}^{k} a_i^{\frac{mx_i}{n_i}} = (\gamma^{-\frac{m}{p}})^p$$

and by the assumption $mx_i/n_i \equiv 0 \bmod p$ $(1 \leqslant i \leqslant k)$. This gives by Lemma 1 $\big(x_1/(n_1, x_1), \dots, x_k/(n_k, x_k)\big) \equiv 0 \bmod p$, and for an $i \leqslant k$ $x_i/(n_i, x_i) \equiv n_i/(n_i, x_i) \equiv 0 \bmod p$, a contradiction.

If $p \nmid m$ we have

$$\zeta_p^m = \gamma^m \prod_{i=1}^{k} a_i^{\frac{mx_i}{n_i}} \in K, \qquad \zeta_p \in K.$$

Suppose now that for a $\gamma \in K$

$$1 + \zeta_4 = \gamma \prod_{i=1}^{k} \xi_i^{x_i} \tag{4}$$

and again $m = [n_1/(n_1, x_1), \dots, n_k/(n_k, x_k)]$. If $4|m$ then

$$(-4)^{\frac{m}{4}} = \gamma^m \prod_{i=1}^{k} a_i^{\frac{x_i m}{n_i}}$$

and by the assumption $x_i m/n_i \equiv 0 \bmod 2$ $(1 \leqslant i \leqslant k)$. This gives by Lemma 1 $\big(x_1/(n_1, x_1), \dots, x_k/(n_k, x_k)\big) \equiv 0 \bmod 2$ and for an $i \leqslant k$:

$$\frac{x_i}{(n_i, x_i)} \equiv \frac{n_i}{(n_i, x_i)} \equiv 0 \bmod 2,$$

a contradiction.

If $4 \nmid m$ then (4) gives

$$(2\zeta_4)^{\frac{m}{(2,m)}} = \gamma^{[m,2]} \prod_{i=1}^{k} a_i^{\frac{[m,2]x_i}{n_i}} \in K; \qquad \zeta_4 \in K.$$

Thus by Kneser's theorem $[K(\xi_1, \dots, \xi_k):K] = [K^*\langle\xi_1, \dots, \xi_k\rangle : K^*]$. Suppose now that

$$\prod_{i=1}^{k} \xi_i^{x_i} = \gamma \in K \quad \text{and} \quad m = [n_1/(n_1, x_1), \dots, n_k/(n_k, x_k)] \neq 1.$$

Then for a certain prime p, $p|m$ and

$$\prod_{i=1}^{k} a_i^{\frac{x_i m}{n_i}} = (\gamma^{\frac{m}{p}})^p$$

thus by the assumption $mx_i/n_i \equiv 0 \bmod p$ $(1 \leqslant i \leqslant k)$. This as before leads to a contradiction. Therefore $m = 1$, $x_i \equiv 0 \bmod n_i$ and we infer that $[K^*\langle\xi_1, \dots, \xi_k\rangle : K^*] = n_1 \dots n_k$, which completes the proof.

Lemma 2. *Let g be 0 or a power of 2, $\mathscr{G}$ a subgroup of K^* containing K^{*g}. If $n_i x_i \equiv 0 \bmod g$ $(1 \leqslant i \leqslant k)$ implies $-\prod_{i=1}^{k} a_i^{x_i} \notin \mathscr{G}$ then there exist elements $\xi_1, \dots, \xi_k, \eta_1, \dots, \eta_l$ and positive integers $m_1, \dots, m_l$ such that*

$$\xi_i^{n_i} = a_i \ (1 \leqslant i \leqslant k), \qquad \eta_j^{m_j} = \beta_j \in K^* \ (1 \leqslant j \leqslant l),$$

$$\langle\xi_1, \dots, \xi_k\rangle = \langle\eta_1, \dots, \eta_l\rangle,$$

$$[m_1, \dots, m_l] \,|\, [n_1, \dots, n_k], \tag{5}$$

$$\prod_{p|m_j} \beta_j^{x_j} = \gamma^p \text{ implies } x_j \equiv 0 \bmod p \qquad (p\,|\,m_j) \tag{6}$$

for all primes p and

$$m_j y_j \equiv 0 \bmod g \ (1 \leqslant j \leqslant l) \text{ implies } -\prod_{j=1}^{l} \beta_j^{y_j} \notin \mathscr{G}\,(^2). \tag{7}$$

Proof. Assume first that all n_i are powers of the same prime q. Consider all systems $\eta_1, \dots, \eta_k$, $m_1, \dots, m_k$ satisfying the following conditions: for suitable ξ_i and integral e_{ij}

$$\xi_i^{n_i} = a_i, \qquad \xi_i = \prod_{j=1}^{k} \eta_j^{e_{ij}}, \qquad \eta_j^{m_j} = \beta_j \in K^*; \tag{8}$$

$$\det[e_{ij}] = \pm 1, \qquad m_j \,|\, n_i e_{ij}$$

and

$$m_j y_j \equiv 0 \bmod g \ (1 \leqslant j \leqslant k) \text{ implies } -\prod_{j=1}^{k} \beta_j^{y_j} \notin \mathscr{G}. \tag{9}$$

Such systems do exist, e.g. $\eta_j = \xi_j$, where $\xi_j^{n_j} = a_j$, $m_j = n_j$; we take one with the least product $m_1 \dots m_k$ and assert that it has the required property. We note that by (8)

$$m_j \,\Big|\, \sum_{i=1}^{k} \frac{\max\limits_{1 \leqslant t \leqslant k} n_t}{n_i} n_i e_{ij} E_{ij} = \pm \max_{1 \leqslant t \leqslant k} n_t,$$

---

(2) $a \equiv 0 \bmod 0$ means $a = 0$.

E_{ij} being the algebraic complement of e_{ij}, hence (5) holds and each m_j is a power of q. We can assume without loss of generality that $m_1 \geqslant m_2 \geqslant \ldots \geqslant m_k$. The only prime p for which (6) needs verification is $p = q$.

Suppose that $\prod\limits_{p|m_j} \beta_j^{x_j} = \gamma^p$ but for some j $p \mid m_j$, $p \nmid x_j$. Let s be the greatest such j and let t satisfy the congruence

$$tx_s \equiv 1 \bmod p.$$

Then

$$\prod_{j=1}^{s-1} \beta_j^{tx_j} \cdot \beta_s = \delta^p. \tag{10}$$

Consider first the case $p = q = 2$. If $m_s \equiv 0 \bmod 2g$ there exists an $\varepsilon = \pm 1$ such that for every choice of z_j satisfying $z_s \equiv 1 \bmod 2$, $m_j z_j \equiv 0 \bmod g$ $(j > s)$ we have

$$-(\varepsilon\delta)^{z_s} \prod_{j \neq s} \beta_j^{z_j} \notin \mathscr{G}.$$

Indeed if

$$z_s \equiv 1 \bmod 2, \quad m_j z_j \equiv 0 \bmod g \ (j > s), \quad -\delta^{z_s} \prod_{j \neq s} \beta_j^{z_j} \in \mathscr{G}$$

and

$$z_s' \equiv 1 \bmod 2, \quad m_j z_j' \equiv 0 \bmod g \ (j > s), \quad -(-\delta)^{z_s'} \prod_{j \neq s} \beta_j^{z_j'} \in \mathscr{G}$$

then

$$z_s - z_s' \equiv 0 \bmod 2, \quad -\delta^{z_s - z_s'} \prod_{j \neq s} \beta_j^{z_j - z_j'} \in \mathscr{G}$$

and by (10)

$$-\prod_{j=1}^{s-1} \beta_j^{tx_j \frac{z_s - z_s'}{2} + z_j - z_j'} \beta_s^{\frac{z_s - z_s'}{2}} \prod_{j=s+1}^{k} \beta_j^{z_j - z_j'} \in \mathscr{G}$$

which contradicts (9) since

$$m_j \equiv 0 \bmod g \ (j \leqslant s), \quad m_j(z_j - z_j') \equiv 0 \bmod g \ (j > s).$$

Let us choose a root of unity $\zeta_{m_s}^r$ so that

$$\eta_s' = \zeta_{m_s}^r \eta_s \prod_{j=1}^{s-1} \eta_j^{tx_j \frac{m_j}{m_s}}$$

satisfies

$$\eta_s'^{\frac{m_s}{2}} = \beta_s' = \begin{cases} \delta & \text{if } m_s \not\equiv 0 \bmod 2g, \\ \varepsilon\delta & \text{otherwise}, \end{cases} \tag{11}$$

and set $m_s' = m_s/2$

$$\eta_j' = \eta_j, \quad m_j' = m_j, \quad \beta_j' = \beta_j \quad (j \neq s); \tag{12}$$

$$e_{ij}' = \begin{cases} e_{ij} - e_{is} tx_j \dfrac{m_j}{m_s} & \text{if } j < s, \\ e_{ij} & \text{if } j \geqslant s; \end{cases} \tag{13}$$

$$\xi_i' = \prod_{j=1}^{k} \eta_j'^{e_{ij}'}. \tag{14}$$

We find

$$\xi_i' = \xi_i \zeta_{m_s}^{e_{is}} \quad \text{and} \quad \xi_i'^{n_i} = \alpha_i \quad (1 \leqslant i \leqslant k)$$

because of (8).

The conditions $\det[e_{ij}'] = \pm 1$ and $m_j' \mid n_i e_{ij}'$ follow also from (8) since by (13)

$$[e_{ij}'] = [e_{ij}] \begin{array}{c} \\ s\left\{ \begin{array}{c} \\ \\ \\ \\ \end{array} \right. \\ \\ \\ \end{array} \begin{bmatrix} 1 & & & & & \\ \cdot\ \cdot & 1 & & & 0 & \\ \cdot & \cdot & \cdot & \cdot\ \cdot & & \\ & 0 & & 1 & & \\ -tx_1\dfrac{m_1}{s_1} & -tx_2\dfrac{m_2}{s_2} & \cdot\ \cdot & 1 & \cdot\ \cdot\ \cdot & \\ & & 0 & & 1 & \\ & & & & & 1 \end{bmatrix},$$

$\det[e_{ij}'] = \det[e_{ij}]$ and $m_j \mid n_i e_{ij}'$.

Finally suppose that $m_j' y_j \equiv 0 \bmod g$ $(1 \leqslant j \leqslant k)$ and $-\prod\limits_{j=1}^{k} \beta_j'^{y_j} \in \mathscr{G}$.

If $y_s \equiv 0 \bmod 2$ we have by (10), (11) and (12)

$$-\prod_{j=1}^{s-1} \beta_j^{tx_j \frac{y_s}{2} + y_j} \beta_s^{\frac{y_s}{2}} \prod_{j=s+1}^{k} \beta_j^{y_j} \in \mathscr{G}$$

which contradicts (9) since

$$m_j \frac{y_s}{2} = \frac{m_j}{m_s} m_s' y_s \equiv 0 \bmod g \ (j \leqslant s) \quad \text{and} \quad m_j y_j \equiv 0 \bmod g \ (j > s).$$

If $y_s \equiv 1 \bmod 2$ we have $m_s \equiv 0 \bmod 2g$ and by (11) and (12)

$$-(\varepsilon\delta)^{y_s} \prod_{j \neq s} \beta_j^{y_j} \in \mathscr{G}$$

contrary to the choice of ε.

Thus $\eta_1', \ldots, \eta_k', m_1', \ldots, m_k'$ satisfy all conditions imposed on $\eta_1, \ldots \ldots, \eta_k, m_1, \ldots, m_k$ and $m_1' \ldots m_k' < m_1 \ldots m_k$, a contradiction.

Consider next the case $p = q > 2$. Let us choose a root of unity $\zeta_{m_s}^r$ so that

$$\eta_s' = \zeta_{m_s}^r \eta_s \prod_{j=1}^{s-1} \eta_j^{tx_j \frac{m_j}{m_s}} \quad \text{satisfies} \quad \eta_s'^{m_s/p} = \delta.$$

Set $m_s' = m_s/p$ and define η_j', m_j' $(j \neq s)$, e_{ij}', ξ_i' by the formulae (12), (13), (14). We find as before that $\xi_i'^{n_i} = a_i$ $(1 \leqslant i \leqslant k)$, $\det[e_{ij}'] = \pm 1$ and $m_j' | n_i e_{ij}'$. If now $m_j' y_j \equiv 0 \bmod g$ $(1 \leqslant j \leqslant k)$ then $y_j \equiv 0 \bmod g$ $(1 \leqslant j \leqslant k)$ and since $K^{*g} \subset \mathscr{G}$, $-\prod_{j=1}^{k} \beta_j'^{y_j} \in \mathscr{G}$ implies $-1 \in \mathscr{G}$ which is impossible by (9). Since $m_1' \ldots m_k' < m_1 \ldots m_k$ we get a contradiction.

Consider now the general case. Let $n_i = \prod_{h=1}^{H} p_h^{r_{hi}}$ $(1 \leqslant i \leqslant k)$, where $p_1, \ldots, p_H$ are distinct primes. By the already proved case of the lemma for each $h \leqslant H$ there exist ξ_{hi}, η_{hi} and m_{hi} $(1 \leqslant i \leqslant k)$ such that

$$\xi_{hi}^{p_h^{r_{hi}}} = a_i, \qquad \eta_{hi}^{m_{hi}} = \beta_{hi},$$

$$\langle \xi_{h1}, \ldots, \xi_{hk} \rangle = \langle \eta_{h1}, \ldots, \eta_{hk} \rangle,$$

$$[m_{h1}, \ldots, m_{hk}] \,|\, p_h^{\max r_{hi}}, \tag{15}$$

$$\prod_{p_h | m_{hi}} \beta_{hi}^{x_i} = \gamma^{p_h} \quad \text{implies} \quad x_i \equiv 0 \bmod p_h \ (p_h | m_{hi}) \tag{16}$$

and

$$m_h y_i \equiv 0 \bmod g \quad \text{implies} \quad -\prod_{i=1}^{k} \beta_{hi}^{y_i} \notin \mathscr{G}. \tag{17}$$

We get

$$\langle \eta_{11}, \ldots, \eta_{1k}, \eta_{21}, \ldots, \eta_{2k}, \ldots, \eta_{H1}, \ldots, \eta_{Hk} \rangle$$
$$= \langle \xi_{11}, \ldots, \xi_{1k}, \xi_{21}, \ldots, \xi_{2k}, \ldots, \xi_{H1}, \ldots, \xi_{Hk} \rangle,$$

$$[m_{11}, \ldots, m_{1k}, m_{21}, \ldots, m_{2k}, \ldots, m_{H1}, \ldots, m_{Hk}] \,|\, [n_1, \ldots, n_k].$$

Let us choose integers t_{hi} so that $\frac{1}{n_i} = \sum_{h=1}^{H} \frac{t_{hi}}{p_h^{r_{hi}}}$. Then

$$\Big(\prod_{h=1}^{H} \xi_{hi}^{t_{hi}}\Big)^{n_i} = a_i, \qquad \xi_{ji} = \Big(\prod_{h=1}^{H} \xi_{hi}^{t_{hi}}\Big)^{\frac{n_i}{p_j^{r_{ji}}}} \qquad (1 \leqslant i \leqslant k),$$

hence

$$\langle \eta_1, \ldots, \eta_{Hk} \rangle = \Big\langle \prod_{h=1}^{H} \xi_{h1}^{t_{h1}}, \ldots, \prod_{h=1}^{H} \xi_{hk}^{t_{hk}} \Big\rangle.$$

Moreover

$$\prod_{p | m_h} \beta_{hi}^{x_{hi}} = \gamma^p$$

implies by (15) and (16) $x_{hi} \equiv 0 \bmod p$ $(p | m_{hi})$. Finally $m_{hi} y_{hi} \equiv 0 \bmod g$ implies $y_{hi} \equiv 0 \bmod g$ unless $p_h = 2$. Since $\mathscr{G} \supset K^{*g}$ the conditions

$$m_{hi} y_{hi} \equiv 0 \bmod g \ (1 \leqslant h \leqslant H,\ 1 \leqslant i \leqslant k) \quad \text{and} \quad -\prod_{h=1}^{H} \prod_{i=1}^{k} \beta_{hi}^{y_{hi}} \in \mathscr{G}$$

imply for $p_h = 2$

$$-\prod_{i=1}^{k} \beta_{hi}^{y_{hi}} \in \mathscr{G}$$

which contradicts (17). The proof is complete.

Remark. It is possible but not worthwhile to obtain $l = k$ in the general case.

Proof of Theorem 2. We apply Lemma 2 with $g = 0$, $\mathscr{G} = \{1\}$ if $\zeta_4 \in K$; with $g = 4$, $\mathscr{G} = K^{*4} \cup 4K^{*4}$ otherwise and find that for suitable $\xi_1, \ldots, \xi_k, \eta_1, \ldots, \eta_l$

$$\xi_i^{n_i} = a_i, \quad \eta_j^{m_j} = \beta_j \quad (1 \leqslant i \leqslant k, 1 \leqslant j \leqslant l), \quad \langle \xi_1, \ldots, \xi_k \rangle = \langle \eta_1, \ldots, \eta_l \rangle$$

$$\prod_{p | m_j} \beta_j^{x_j} = \gamma^p \quad \text{implies} \quad x_j \equiv 0 \bmod p \ (p | m_j) \tag{18}$$

and if $\zeta_4 \notin K$

$$m_j y_j \equiv 0 \bmod 4 \ (1 \leqslant j \leqslant k) \quad \text{implies} \quad \prod_{j=1}^{k} \beta_j^{y_j} \neq -\gamma^4, -4\gamma^4.$$

If $\zeta_4 \notin K$ we see at once that the conditions of Theorem 1 are satisfied; if $\zeta_4 \in K$ they are also satisfied since then by (18)

$$\prod_{2 | n_i} \beta_i^{x_i} = -4\gamma^4, n_i x_i \equiv 0 \bmod 4 \ (2 | n_i) \quad \text{implies} \quad \prod_{2 | n_i} \beta_i^{x_i} = (2\zeta_4 \gamma^2)^2,$$

$x_i \equiv 0 \bmod 2$, $\prod_{2|n_i} \beta_i^{x_i/2} = \pm 2\zeta_4 \gamma^2 = \big((1 \pm \zeta_4)\gamma\big)^2$, $x_i/2 \equiv 0 \bmod 2$, $x_i \equiv 0 \bmod 4$ $(1 \leqslant i \leqslant k)$.

By Theorem 1 we have $[K(\eta_1, \ldots, \eta_l) : K] = m_1 \ldots m_l = [K^* \langle \eta_1, \ldots \ldots, \eta_l \rangle : K^*]$, hence the theorem.

LEMMA 3. *If $\eta_1, \ldots, \eta_l, m_1, \ldots, m_l$ satisfy the conditions of Lemma 2 with $g = 2$, $\mathscr{G} = K^{*2}$, $\delta \in K^*$ and $\sqrt{\delta} \in K(\eta_1, \ldots, \eta_l)$ then*

$$\sqrt{\delta} \in K^*\langle \eta_1, \ldots, \eta_l \rangle \quad \textit{and} \quad \delta \neq -1.$$

Proof. If $\sqrt{\delta} \in K(\eta_1, \ldots, \eta_l)$ but $\sqrt{\delta} \notin K^*\langle \eta_1, \ldots, \eta_l \rangle$ then

$$[K^*\langle \sqrt{\delta}, \eta_1, \ldots, \eta_l \rangle : K^*] > [K^*\langle \eta_1, \ldots, \eta_l \rangle : K^*] \geqslant [K(\eta_1, \ldots, \eta_l) : K]$$
$$= [K(\sqrt{\delta}, \eta_1, \ldots, \eta_l) : K]$$

thus by Kneser's theorem we have for a certain prime p

$$\zeta_p \in K^*\langle \sqrt{\delta}, \eta_1, \ldots, \eta_l \rangle, \quad \zeta_p \notin K$$

or

$$1 + \zeta_4 \in K^*\langle \sqrt{\delta}, \eta_1, \ldots, \eta_l \rangle, \quad \zeta_4 \notin K.$$

However $\zeta_p = \gamma \sqrt{\delta}^{x_0} \prod_{j=1}^{l} \eta_j^{x_j}$, $\gamma \in K$, gives

$$\sqrt{\delta} \in K^*\langle \eta_1, \ldots, \eta_l \rangle$$

unless $x_0 \equiv 0 \bmod 2$. In the latter case let

$$m = [m_1/(m_1, x_1), \ldots, m_l/(m_l, x_l)].$$

If $p \mid m$ we get

$$\prod_{j=1}^{l} \beta_j^{\frac{mx_j}{m_j}} = \left(\gamma^{-\frac{m}{p}} \delta^{-\frac{m}{p}\frac{x_0}{2}}\right)^p$$

and by the assumption

$$\frac{mx_j}{m_j} \equiv 0 \bmod p \quad (1 \leqslant j \leqslant l).$$

This gives by Lemma 1 $\big(x_1/(m_1, x_1), \ldots, x_l/(m_l, x_l)\big) \equiv 0 \bmod p$ and for a $j \leqslant l$ $x_j/(m_j, x_j) \equiv m_j/(m_j, x_j) \equiv 0 \bmod p$, a contradiction.

If $p \nmid m$ we have

$$\zeta_p^m = (\gamma \delta^{\frac{x_0}{2}})^m \prod_{j=1}^{l} \beta_j^{\frac{mx_j}{m_j}} \in K; \quad \zeta_p \in K.$$

Suppose now that $\gamma \in K$,

$$(19) \qquad 1 + \zeta_4 = \gamma \sqrt{\delta}^{x_0} \prod_{j=1}^{l} \eta_j^{x_j} \quad \text{or} \quad \zeta_4 = \gamma \prod_{j=1}^{l} \eta_j^{x_j}$$

and set again $m = [m_1/(m_1, x_1), \ldots, m_l/(m_l, x_l)]$.

If $4 \mid m$ then

$$(-4)^{m/4} = \gamma^m \delta^{x_0 \frac{m}{2}} \prod_{j=1}^{l} \beta_j^{\frac{x_j m}{m_j}} \quad \text{or} \quad 1 = \gamma^m \prod_{j=1}^{l} \beta_j^{\frac{x_j m}{m_j}}$$

and by the assumption $x_j m/m_j \equiv 0 \bmod 2$ $(1 \leqslant j \leqslant l)$. This gives by Lemma 1 $\big(x_1/(m_1, x_1), \ldots, x_l/(m_l, x_l)\big) \equiv 0 \bmod 2$ and for a $j \leqslant l$

$$\frac{x_j}{(m_j, x_j)} \equiv \frac{m_j}{(m_j, x_j)} \equiv 0 \bmod 2,$$

a contradiction.

If $4 \nmid m$ then (19) gives

$$(2\zeta_4)^{\frac{m}{(m,2)}} = \gamma^{[m,2]} \delta^{x_0 \frac{m}{(m,2)}} \prod_{j=1}^{l} \beta_j^{\frac{x_j[m,2]}{m_j}} \in K; \quad \zeta_4 \in K$$

or

$$(-1)^{\frac{m}{(m,2)}} = \gamma^{[m,2]} \prod_{j=1}^{l} \beta_j^{\frac{x_j[m,2]}{m_j}}; \quad \prod_{2 \mid m_j} \beta_j^{\frac{x_j[m,2]}{m_j}} = -\delta_1^2.$$

The contradiction obtained completes the proof.

LEMMA 4. *Let K be an arbitrary field, n a positive integer not divisible by the characteristic of K, m_j divisors of n and $\beta_1, \ldots, \beta_l, \beta$ non-zero elements of K. If each of the fields $K(\eta_1, \ldots, \eta_l)$, where $\eta_j^{m_j} = \beta_j$ $(1 \leqslant j \leqslant l)$ contains at least one η with $\eta^n = \beta$ then for any choice of η_j and η and for suitable exponents $r_0, r_1, \ldots, r_l$*

$$\zeta_n^{r_0} \eta \eta_1^{r_1} \ldots \eta_l^{r_l} \in K(\zeta_4).$$

Proof. This is an immediate consequence of Lemma 6 of [6].

LEMMA 5. *Let K be an arbitrary field of characteristic different from 2 and τ be defined as in Theorem 3. $\Theta \in K$ is of the form ϑ^n, where $\vartheta \in K(\zeta_4)$ if and only if at least one of the following three conditions is satisfied for a suitable $\gamma \in K$:*

$$\Theta = \gamma^n,$$

$$n \not\equiv 0 \bmod 2^\tau, \quad \Theta = -\gamma^n,$$

$$n \equiv 0 \bmod 2^\tau, \quad \Theta = (-1)^{n/2^\tau} (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \gamma^n.$$

If $\zeta_4 \in K$ the last two conditions imply the first.

Proof. Necessity follows at once from Lemma 7 of [6]. Sufficiency of the first condition is obvious. In order to prove sufficiency of the other two note that if $n \not\equiv 0 \bmod 2^\tau$ and $qn \equiv 2^{\tau-1} \bmod 2^\tau$ then

$$-1 = (\zeta_{2^\tau}^q)^n$$

and if $n \equiv 0 \bmod 2^\tau$ then

$$(-1)^{n/2^\tau}(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{n/2} = (\zeta_{2^\tau}+1)^n.$$

On the other hand since $\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}\in K$,

$$\zeta_{2^\tau} = \tfrac{1}{2}(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}) \pm \tfrac{1}{2}\zeta_4(\zeta_{2^\tau}^{1-2^{\tau-2}}+\zeta_{2^\tau}^{-1+2^{\tau-2}})\in K(\zeta_4).$$

The last assertion of the lemma is obvious.

Proof of Theorem 3. Let us assume first that for all l_i

$$\prod_{2|n_i} \alpha_i^{l_i} \neq -\delta^2. \tag{20}$$

Then by Lemma 2 applied with $g=2$, $\mathscr{G} = K^{*2}$ there exist $\xi_1, \ldots, \xi_k, \eta_1, \ldots, \eta_l, m_1, \ldots, m_l$ such that

$$\xi_i^{n_i} = \alpha_i \ (1 \leqslant i \leqslant k), \qquad \eta_j^{m_j} = \beta_j \in K \ (1 \leqslant j \leqslant l),$$

$$\langle \xi_1, \ldots, \xi_k\rangle = \langle \eta_1, \ldots, \eta_l\rangle, \tag{21}$$

$$[m_1, \ldots, m_l] \,|\, [n_1, \ldots, n_k], \tag{22}$$

$$\prod_{p|m_j} \beta_j^{x_j} = \gamma^p \quad \text{implies} \quad p \,|\, x_j \ (p\,|\,m_j)$$

for all primes p and

$$\prod_{2|m_j} \beta_j^{y_j} \neq -\gamma^2 \text{ for any choice of } y_j. \tag{23}$$

By Theorem 1 $[K(\eta_1, \ldots, \eta_l):K] = m_1 \ldots m_l$ and thus all fields $K(\eta_1, \ldots, \eta_l)$, where $\eta_j^{m_j} = \beta_j$ are conjugate over K. If now $K(\xi_1, \ldots, \xi_k) = K(\eta_1, \ldots, \eta_l)$ contains an η with $\eta^n = \beta$ then each field $K(\eta_1, \ldots, \eta_l)$ contains such an η and by Lemma 4, Lemma 5, (22) and (23) we have either

$$\beta \prod_{j=1}^{l} \beta_j^{r_j \frac{n}{m_j}} = \gamma^n \tag{24}$$

or

$$n \equiv 0 \bmod 2^{\tau+1} \quad \text{and} \quad \beta \prod_{j=1}^{l} \beta_j^{r_j\frac{n}{m_j}} = (\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{n/2}\gamma^n \tag{25}$$

for suitable integers $r_1, \ldots, r_l$ and a suitable $\gamma \in K$. Indeed, if $n \equiv 0 \bmod 2$, $\beta\prod\limits_{j=1}^{l}\beta_j^{r_j\frac{n}{m_j}} = -\gamma^n$ or $n \equiv 2^\tau \bmod 2^{\tau+1}$, $\beta\prod\limits_{j=1}^{l}\beta_j^{r_j\frac{n}{m_j}} = -(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{n/2}\gamma^n$, we get on taking square-roots $\zeta_4 \in K(\eta, \eta_1, \ldots, \eta_l) = K(\eta_1, \ldots, \eta_l)$ contrary to Lemma 3.

The condition (21) implies that

$$\prod_{j=1}^{l} \beta_j^{r_j\frac{n}{m_j}} = \prod_{i=1}^{k} \alpha_i^{q_i\frac{n}{n_i}} \tag{26}$$

for suitable integers $q_1, \ldots, q_k$. Hence (24) leads to (i).

It remains to consider (25). If $L = K(\eta_1, \ldots, \eta_l)$ contains an η with $\eta^n = \beta$ then by (25) it contains $\zeta_n^r\sqrt{\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2}$ for a certain r.

If $n/(n, 2r) \equiv 1 \bmod 2$ then L contains

$$\zeta_n^{\frac{rn}{(n,2r)}}\sqrt{\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2} = \pm\sqrt{\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2};$$

if $n/(n, 2r) \equiv 2 \bmod 4$ then L contains

$$\zeta_n^{\frac{rn}{2(n,2r)}}\sqrt{\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2} = \pm\sqrt{-(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)};$$

if $n/(n, 2r) \equiv 0 \bmod 4$ then L contains $\zeta_n^{\frac{rn}{2(n,2r)}} = \pm\zeta_4$.

By Lemma 3 the last case is impossible and in the first two cases

$$\sqrt{\pm(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)} \in K^*\langle \eta_1, \ldots, \eta_l\rangle = K^*\langle \xi_1, \ldots, \xi_k\rangle.$$

Hence we obtain

$$(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{n/2} = \vartheta^n \prod_{i=1}^{k} \alpha_i^{s_i\frac{n}{n_i}}, \qquad \vartheta \in K,$$

which together with (25) and (26) gives again (i).

Assume now that for some $l_1, \ldots, l_k$

$$\prod_{2|n_i} \alpha_i^{l_i} = -\delta^2, \qquad \delta \in K.$$

Then we apply Lemma 2 for the field $K(\zeta_4)$ with $g=0$, $\mathscr{G} = \{1\}$ and we infer the existence of $\xi_1, \ldots, \xi_k, \eta_1, \ldots, \eta_l, m_1, \ldots, m_l$ such that

$$\xi_i^{n_i} = \alpha_i \ (1 \leqslant i \leqslant k), \qquad \eta_j^{m_j} = \beta_j \in K(\zeta_4) \ (1 \leqslant j \leqslant l),$$

$$\langle \xi_1, \ldots, \xi_k\rangle = \langle \eta_1, \ldots, \eta_l\rangle, \tag{27}$$

$$[m_1, \ldots, m_l] \,|\, [n_1, \ldots, n_k],$$

$$\prod_{p|m_j} \beta_j^{x_j} = \gamma^p,\ \gamma \in K(\zeta_4) \quad \text{implies} \quad p\,|\,x_j \ (p\,|\,m_j)$$

for all primes p.

By Theorem 1 $[K(\zeta_4, \eta_1, \ldots, \eta_l):K(\zeta_4)] = m_1 \ldots m_l$ (see the end of the proof of Theorem 2) and thus all fields $K(\zeta_4, \eta_1, \ldots, \eta_l)$, where $\eta_j^{m_j} = \beta_j$ are conjugate over $K(\zeta_4)$.

If now $K(\xi_1, \ldots, \xi_k) \subset K(\zeta_4, \eta_1, \ldots, \eta_l)$ contains an η with $\eta^n = \beta$ then each field $K(\zeta_4, \overline{\eta}_1, \ldots, \overline{\eta}_l)$ contains such an η and by Lemma 4 we have

$$\beta \prod_{j=1}^{l} \beta_j^{r_j \frac{n}{m_j}} = \vartheta^n, \quad \vartheta \in K(\zeta_4).$$

The condition (27) implies that

$$\prod_{j=1}^{l} \beta_j^{r_j \frac{n}{m_j}} = \prod_{i=1}^{k} a_i^{q_i \frac{n}{n_i}}$$

for suitable integers $q_1, \ldots, q_k$. Hence $\vartheta^n \in K$ and using Lemma 5 we get one of the cases (i)–(iii).

Conversely if (i) is satisfied then any field $K(\xi_1, \ldots, \xi_k)$, where $\xi_i^{n_i} = a_i$ $(1 \leqslant i \leqslant k)$ contains $\eta = \gamma \prod_{i=1}^{k} \xi_i^{-q_i}$ with $\eta^n = \beta$.

If (ii) or (iii) is satisfied then by Lemma 5

$$\beta \prod_{i=1}^{k} a_i^{q_i \frac{n}{n_i}} = \vartheta^n$$

where $\vartheta \in K(\zeta_4)$. On the other hand, the equality $\prod_{2|n_i} a_i^{l_i} = -\delta^2$ implies $\zeta_4 = \pm \prod_{2|n_i} \xi_i^{n_i l_i/2}$.

Thus $\vartheta \in K(\xi_1, \ldots, \xi_k)$ and $K(\xi_1, \ldots, \xi_k)$ contains $\eta = \vartheta \prod_{i=1}^{k} \xi_i^{-q_i}$ with $\eta^n = \beta$.

The last assertion of the Theorem if $\zeta_4 \in K$ follows from the last assertion of Lemma 5.

If $\tau = 2$ and $n \not\equiv 0 \bmod 2^\tau$ we have either $n \equiv 1 \bmod 2$, in which case $-\gamma^n = (-\gamma)^n$ or $n \equiv 2 \bmod 4$. In the latter case we get from (ii)

$$\beta \prod_{i=1}^{k} a_i^{q_i \frac{n}{n_i}} \prod_{2|n_i} a_i^{l_i \frac{n}{2}} = (\gamma\delta)^n$$

which leads to (i). The proof is complete.

Proof of Corollary. If the irreducible polynomials $f(x) = x^n - a$ and $g(x) = x^n - \beta$ satisfy the relation $f \sim g$ we have by Theorem 3 the following five possibilities

(28) $$a \stackrel{n}{=} \beta^t, \quad \beta \stackrel{n}{=} a^s;$$

(29) $$n \not\equiv 0 \bmod 2^\tau, \quad a = -\delta^2 \stackrel{n}{=} \beta^t, \quad \beta \stackrel{n}{=} -a^s;$$

(30) $$n \equiv 0 \bmod 2^\tau, \quad a = -\delta^2 \stackrel{n}{=} \beta^t, \quad \beta \stackrel{n}{=} \varepsilon\omega a^s;$$

(31) $$n \not\equiv 0 \bmod 2^\tau, \quad a = -\delta_1^2 \stackrel{n}{=} -\beta^t, \quad \beta = -\delta_2^2 \stackrel{n}{=} a^s;$$

(32) $$n \equiv 0 \bmod 2^\tau, \quad a = -\delta_1^2 \stackrel{n}{=} \varepsilon\omega\beta^t, \quad \beta = -\delta_2^2 \stackrel{n}{=} \varepsilon\omega a^s,$$

and two other possibilities obtained by the permutation of a and β in (29) and (30). Here $\gamma \stackrel{n}{=} \delta$ means that γ/δ is an nth power in K, $\varepsilon = (-1)^{n/2^\tau}$ and $\omega = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}$.

Moreover in (29) to (32) it is assumed that $\zeta_4 \notin K$. Now, (29) gives $t \equiv 1 \bmod 2$, $a \stackrel{n}{=} -a^{st}$, $a^{st-1} \stackrel{n}{=} -1$, $\beta \stackrel{n}{=} a^{s+st-1}$.

(30) gives $t \equiv 1 \bmod 2$, $a \stackrel{n}{=} \varepsilon\omega a^{st}$, $a^{st-1} \stackrel{n}{=} \varepsilon\omega$, $\beta \stackrel{n}{=} a^{s+st-1}$.

(31) gives $s \equiv t \equiv 0 \bmod 2$. Indeed, if for instance $t \equiv 1 \bmod 2$ then

$$-\delta_1^2 = -\beta^t = \delta_2^{2t} \quad \text{and} \quad \zeta_4 \in K.$$

If $s \equiv t \equiv 0 \bmod 2$ then

$$a \stackrel{n}{=} -a^{st}, \quad a^{st-1} \stackrel{n}{=} -1, \quad \beta \stackrel{n}{=} a^{s+st-1}.$$

(32) with $\varepsilon = -1$ gives like (31) that $s \equiv t \equiv 0 \bmod 2$. In that case

$$a \stackrel{n}{=} -\omega a^{st}, \quad a^{st-1} \stackrel{n}{=} -\omega, \quad \beta \stackrel{n}{=} a^{s+st-1}.$$

Thus in any case we have either $\beta \stackrel{n}{=} a^r$ or $n \equiv 0 \bmod 2^{\tau+1}$, $a = -\delta^2$, $\beta = \omega a^r$. On the other hand if at least one of these conditions is satisfied then by Theorem 3 each of the fields $K(\xi)$ with $f(\eta) = 0$ contains an η with $g(\eta) = 0$ and since f and g are irreducible and of the same degree $K(\xi) = K(\eta)$.

Note added in proof. Theorem 3 is incompatible with Theorem 2 of T. Nagell, *Bestimmung des Grades gewisser relativ-algebraischen Zahlen*, Monatsh. Math. Phys. 48 (1939), p. 63. However already the special case of the latter theorem given by Nagell as his Theorem 3 is not valid in general, as shown by the example $\Omega = Q$, $n = 8$, $a = -1$, $b = -16$ contained in Theorem 6 of Gerst [1].

References

[1] I. Gerst, *On the theory of n-th power residues and a conjecture of Kronecker*, Acta Arith. 17 (1970), pp. 121–139.

[2] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, 2nd ed., Vol. 2, Würzburg 1965.

[3] M. Kneser, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. 26 (1975), pp. 307–308.

[4] L. J. Mordell, *On the linear independence of algebraic numbers*, Pacific J. Math. 3 (1953), pp. 625–630.

[5] L. Rédei, *Algebra* I, Budapest 1967.

[6] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. 27 (1975), pp. 397–420.

[7] C. L. Siegel, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. 21 (1972), pp. 59–64.

Received on 2. 4. 1974
and in revised form on 2. 5. 1974 (551)

ACTA ARITHMETICA
XXVIII (1975)

On twin almost primes

by

ENRICO BOMBIERI* (Pisa)

Dedicated to the memory of my teacher, Giovanni Ricci

1. Introduction and results. Let p, P_k denote respectively a prime and an almost prime with at most k factors. We are interested here in counting solutions of the equation $P_k+2 = p$, attaching suitable weights depending on the prime factors of P_k.

Let $\Lambda_k = \Lambda_k(n)$ be the generalized von Mangoldt function

$$\Lambda_k = \mu * L^k, \tag{1.1}$$

k integral $\geqslant 1$, where μ denotes the Möbius function, L denotes the arithmetical function $\log n$, and $*$ denotes the Dirichlet convolution. Clearly $\Lambda_1 = \Lambda$, the von Mangoldt function, and it is easily shown that

$$\Lambda_k = \Lambda_{k-1} L + \Lambda_{k-1} * \Lambda, \tag{1.2}$$

therefore

$$\Lambda_2 = \Lambda L + \Lambda * \Lambda,$$

$$\Lambda_3 = \Lambda L^2 + 3\Lambda L * \Lambda + \Lambda * \Lambda * \Lambda,$$

and so on. An easy induction on k now shows that

$\Lambda_k(n) = 0$ *if n has more than k prime factors* and thus Λ_k can be taken as a weighting function for k-almost primes. Thus the natural sum to study is

$$\sum_{n \leqslant x} \Lambda(n+2) \Lambda_k(n), \tag{1.3}$$

and our purpose in this paper is to show that for large k the sum (1.3) is quite near to the expected asymptotic value. We shall also obtain the asymptotic behaviour of (1.3) for $k \geqslant 2$, but assuming the still unproved Halberstam–Richert conjecture on the distribution of primes in arithmetic progressions.

* Supported in part by N. S. F. grant number GP-36418X1.