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, $a_1, \ldots, a_n$ elements of $K$, $n_1, \ldots, n_k$ positive integers, $\xi_i^r = a_i (1 \leq i \leq k)$. If $\prod \xi_i^r \in K$ implies $a_i = 0 \mod n_i$ and either the numbers $\xi_i$ are real or $K$ contains $n_i$th roots of unity $(1 \leq i \leq k)$ then the degree of the extension $K(\xi_1, \ldots, \xi_k)$ over $K$ is $n_1 \cdots n_k$. 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 $[K':K] \langle \xi_1, \ldots, \xi_k \rangle$ 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 $1 + \zeta_p \in K' \langle \xi_1, \ldots, \xi_k \rangle$ implies $\zeta_p \in K$, where $\zeta_p$ is a primitive $p$th 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 $n_1 \cdots n_k$ over $K$.

**Theorem 1.** Let $K$ be any field. Assume that the characteristic of $K$ does not divide $n_1 \cdots n_k$ and $\xi_i^r = a_i \in K'$. $[K(\xi_1, \ldots, \xi_k):K] = n_1 \cdots n_k$ if and only if for all primes $p$, $\prod q_i^{r_i} = \gamma^p$ implies $a_i = 0 \mod p$ and $\prod q_i^{r_i} = 4y_1^2 \div n_i x_1 = 0 \mod 4 (2 | n_i)$ implies $a_i = 0 \mod 4 (2 | n_i)^{\left(\gamma^p\right)}$.

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 $K = Z_2 (i)$, $n_1 = n_2 = 2$, $a_1 = i$, $a_2 = i + 1$.

\(^{(1)} (p | n_i)\) 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 \( \zeta_i \notin K \) or \( n_i a_i = 0 \mod 4 \) \( (2|n_i) \), \( i = 1, \ldots, k \), then there exist elements \( \xi_1, \ldots, \xi_k \) such that \( \xi_i^{n_i} = a_i \) and

\[
[K(\xi_1, \ldots, \xi_k) : K] = [K^* \langle \xi_1, \ldots, \xi_k \rangle : K^*].
\]

It follows from Knesser's theorem that if \( \zeta_i \notin K \) and for some \( n_i, a_i = 0 \mod 4 \) \( (2|n_i) \), \( i = 1, \ldots, k \), satisfying \( \xi_i^{n_i} = a_i \), the equality (1) holds. The example \( K = \mathbb{Q}, n_3 = n_8 = 8, a_1 = -1, a_8 = -16 \) shows that the converse is not true. Indeed for any choice of \( \xi_1, \xi_2 \) 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 \( \eta \) with \( \eta^n = \beta \) \( (\beta \text{ fixed}, \eta n_i) \). Condition given in [6] was necessary but not always sufficient. We shall prove even a more precise result.

**Theorem 3.** Let \( \tau \) be the largest integer such that \( \zeta^{\tau} \in \mathbb{Q}^{*} \cdot K \), 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 \( \xi_i^{n_i} = a_i \) \( (1 \leq i \leq k) \) 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 \( \eta \) with \( \eta^n = \beta \) then at least one of the following three conditions is satisfied for suitable rational integers \( l_1, \ldots, l_k, \gamma_1, \ldots, \gamma_k \) and suitable \( \gamma, \delta \in K^*.

(i) \( \beta \prod_{i=1}^{k} a_i^{l_i} = \gamma^n \),

(ii) \( n \neq 0 \mod 2^l \), \( \prod_{i=1}^{k} a_i^{l_i} = -\delta^n, \beta \prod_{i=1}^{k} a_i^{l_i} = -\gamma^n \),

(iii) \( n = 0 \mod 2^l \), \( \prod_{i=1}^{k} a_i^{l_i} = -\delta^n, \beta \prod_{i=1}^{k} a_i^{l_i} = (-1)^{n/2^n}(\zeta^{\tau} + \zeta^{\tau + 1}) + m^n \gamma^n \),

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 \( \eta \) with \( \eta^n = \beta \).

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

This theorem can be regarded as an extension of the classical result concerning Kummer fields ([3], p. 42).

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

**Theorem 3** implies

**Corollary.** Two polynomials \( f(x) = x^n - \alpha \) and \( g(x) = x^n - \beta \) irreducible over \( K \) satisfy \( f \sim g \) if and only if either \( \beta \alpha = \gamma^n \) or \( n = 0 \mod 2^r \), \( \alpha = -\gamma^n, \beta = -\delta^n \), and \( \beta \alpha = (\zeta^{\tau} + \zeta^{\tau + 1}) + m^n \gamma^n \), with \( \gamma, \delta, \beta \in K^* \).

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

For the proof we need several lemmata.

**Lemma 1.** If \( (a_{i1}, b_i) = 1 \) and \( b_i | m \), \( (1 \leq i \leq k) \) then

\[
\left( m \frac{a_{i1}}{b_i}, \ldots, m \frac{a_{ik}}{b_i} \right) = \left( \frac{a_{i1}}{b_i}, \ldots, \frac{a_{ik}}{b_i} \right) - \left( \frac{a_{i1}, \ldots, a_{ik}}{b_i} \right).
\]

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

\[
\left( m \frac{a_{i1}}{b_i}, m \frac{a_{i1}}{b_i} \right) = \left( \frac{a_{i1}}{b_i}, \frac{a_{i2}}{b_i}, \frac{a_{i1}}{b_i}, \frac{a_{i2}}{b_i} \right) = \left( \frac{a_{i1}}{b_i}, \frac{a_{i2}}{b_i} \right) = \left( \frac{a_{i1}, a_{i2}}{b_i} \right).
\]

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

\[
\left( m \frac{a_{i1}}{b_i}, \ldots, m \frac{a_{ik+1}}{b_i} \right) = \left( \frac{a_{i1}, \ldots, a_{ik}}{b_i}, \frac{a_{ik+1}}{b_{i+1}} \right) = \left( \frac{a_{i1}, \ldots, a_{ik}, a_{ik+1}}{b_{i+1}} \right),
\]

and the proof is complete.

**Proof of Theorem 1.** Necessity. Suppose that for a certain prime \( p \) and a certain \( \gamma \in K \) and some \( n_a, \prod_{i=1}^{k} a_i^{l_i} = \gamma^p \), but for a certain \( i p | n_i, \gamma^p \mid a_i^{l_i} \).

Then for a suitable \( j \)

\[
\prod_{i=1}^{k} a_i^{l_i} = \gamma^p,
\]

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

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

Suppose now that for some \( n_a \) and a certain \( \gamma \in K \) \( \prod_{i=1}^{k} a_i^{l_i} = \gamma^p \), \( n_a a_i = 0 \mod 4 \), \( (2 | n_i) \) but for a certain \( i p | n_i, \gamma^p \mid a_i^{l_i} \). Then for a suitable \( j \)

\[
\prod_{i=1}^{k} a_i^{l_i} = \gamma^p,
\]

and the proof is complete.

\[1 + \zeta_j \cdot K^* \langle \xi_1, \ldots, \xi_k \rangle \] (Note that \( \zeta_j (1 + \zeta_j) = -2(1 + \zeta_j)^{-1} \) and by Knesser's theorem either \( \zeta_j \in K \) or \( [K^* \langle \xi_1, \ldots, \xi_k \rangle : K^*] < [K^* \langle \xi_1, \ldots, \xi_k \rangle : K^*] \).}
In the former case by (3) $[K^* \langle \xi_1, \ldots, \xi_h \rangle: K^*] < n_1 \ldots n_h$, in both cases $[K(\xi_1, \ldots, \xi_h): K] < n_1 n_2 \ldots n_h$.

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

$$\xi_p = \gamma \prod_{i=1}^{k} \xi_i^m_i.$$

Let $m = [n_1/(n_1, x_1), \ldots, n_h/(n_h, x_h)]$. If $p|m$ we get

$$\prod_{i=1}^{k} \frac{m_i}{\alpha_i} \equiv (\gamma^p \gamma^p)^p$$

and by the assumption $m_i/n_i \equiv 0 \mod p \ (1 \leq i \leq k)$. This gives by Lemma 1 $(x_i/(n_i, x_1), \ldots, x_h/(n_h, x_h)) = 0 \mod p$, and for an $i \leq k$ $x_i/(n_i, x_i) = n_i/(n_i, x_i) = 0 \mod p$, a contradiction.

If $p \nmid m$ we have

$$\xi_p^m = \gamma^m \prod_{i=1}^{k} \frac{m_i}{\alpha_i} \xi_i^{m_i} \epsilon K, \quad \xi_p^e \epsilon K.$$

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

$$1 + \xi_4 = \gamma \prod_{i=1}^{k} \xi_i^{m_i}$$

and again $m = [n_1/(n_1, x_1), \ldots, n_h/(n_h, x_h)]$. If $4|m$ then

$$(-4)^m \equiv \gamma^m \prod_{i=1}^{k} \frac{m_i}{\alpha_i} \xi_i^{m_i} \equiv 0 \mod 2$$

and by the assumption $a_i m_i / a_i \equiv 0 \mod 2 \ (1 \leq i \leq k)$. This gives by Lemma 1 $(x_i/(n_i, x_1), \ldots, x_h/(n_h, x_h)) = 0 \mod 2$ and for an $i \leq k$:

$$\frac{x_i}{(n_i, x_i)} = \frac{n_i}{(n_i, x_i)} = 0 \mod 2,$$

a contradiction.

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

$$(2\xi_4)_{m} = \gamma^m \prod_{i=1}^{k} \frac{m_i}{\alpha_i} \xi_i^{m_i} \epsilon K, \quad \xi_4 \epsilon K.$$

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

$$\prod_{i=1}^{k} \xi_i^{m_i} = \gamma \epsilon K \quad \text{and} \quad m = [n_1/(n_1, x_1), \ldots, n_h/(n_h, x_h)] \neq 1.$$

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

$$\prod_{i=1}^{k} \frac{m_i}{\alpha_i} = (\gamma^p \gamma^p)^p$$

thus by the assumption $m_i/n_i = 0 \mod p \ (1 \leq i \leq k)$. This as before leads to a contradiction. Therefore $m = 1$, $a_i = 0 \mod n_i$ and we infer that $[K^* \langle \xi_1, \ldots, \xi_h \rangle : K^*] = n_1 \ldots n_h$, which completes the proof.

Lemma 2. Let $g$ be 0 or a power of 2, $\mathcal{I}$ a subgroup of $K^*$ containing $K^g$. If $n_i a_i \equiv 0 \mod g \ (1 \leq i \leq k)$ implies $-\prod_{i=1}^{k} \alpha_i \not\in \mathcal{I}$ then there exist elements $\xi_1, \ldots, \xi_k, \eta_1, \ldots, \eta_i$ and positive integers $m_1, \ldots, m_k$ such that

$$\xi_i^{m_i} = a_i \ (1 \leq i \leq k), \quad \eta_j^{m_j} = \beta_j K^* \ (1 \leq j \leq l),$$

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

$$[m_1, \ldots, m_k] = [n_1, \ldots, n_k],$$

and

$$\prod_{i=1}^{k} \beta_i = \gamma^p \mod p \quad (p|m)$$

for all primes $p$ and

$$m_j a_j = 0 \mod g \ (1 \leq j \leq k) \quad \text{implies} \quad -\prod_{i=1}^{k} \alpha_i \not\in \mathcal{I}^{(2)}.$$

Proof. Assume first that all $n_i$ are powers of the same prime $q$. Consider all systems $\eta_1, \ldots, \eta_l, m_1, \ldots, m_k$ satisfying the following conditions:

- Suitable $\xi_i$ and integral $\alpha_i$.

Then

$$\xi_i^{m_i} = a_i \quad \text{and} \quad \xi_i = \prod_{j=1}^{k} \eta_j^{m_i}, \quad \eta_j = \beta_j K^*;$$

$$\det(\xi_i) = \pm 1,$$

and

$$m_j a_j = 0 \mod g \ (1 \leq j \leq k) \quad \text{implies} \quad -\prod_{i=1}^{k} \alpha_i \not\in \mathcal{I}^{(2)}.$$

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

$$m_j \sum_{i=1}^{k} \frac{\max n_i}{n_i} = \pm \sum_{i=1}^{k} \frac{\max_{1 \leq i \leq k} n_i}{n_i} \xi_i \epsilon K.$$
\[ B_j \] being the algebraic complement of \( a_{ij} \), hence (5) holds and each \( m_j \) is a power of \( q \). We can assume without loss of generality that \( m_1 \geq m_2 \geq \ldots \geq m_k \). The only prime \( p \) for which (6) needs verification is \( p = q \).

Suppose that \( \prod_{j=1}^{k} \beta_j^q = \gamma^q \) but for some \( j \mid m_j \), \( p \nmid x_j \). Let \( s \) be the greatest such \( j \) and let \( t \) satisfy the congruence

\[ t x_j = 1 \mod p. \]

Then

\[ \prod_{j=1}^{s} \beta_j^{x_j} \cdot \beta_s = \beta^q. \quad (10) \]

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

\[ -(\varepsilon \delta)^{\frac{s-1}{2}} \prod_{j=s}^{s-1} \beta_j^{x_j} \in \mathbb{G}. \]

Indeed if

\[ x_s = 1 \mod 2, \quad m_s x_s = 0 \mod g \quad (j > s); \quad -\delta^s \prod_{j=s}^{s-1} \beta_j^{x_j} \in \mathbb{G} \]

and

\[ x'_s = 1 \mod 2, \quad m_s x'_s = 0 \mod g \quad (j > s); \quad -(-\delta)^{s} \prod_{j=s}^{s-1} \beta_j^{x'_j} \in \mathbb{G} \]

then

\[ x_s - x'_s = 0 \mod 2, \quad -\delta^{s-1} \prod_{j=s}^{s-1} \beta_j^{x_j - x'_j} \in \mathbb{G} \]

and by (10)

\[ -\prod_{j=1}^{s-1} \beta_j^{x_j} \prod_{j=s}^{s-1} \beta_j^{x'_j} \in \mathbb{G} \]

which contradicts (9) since

\[ m_j = 0 \mod g \quad (j \leq s), \quad m_j (x_j - x'_j) = 0 \mod g \quad (j > s). \]

Let us choose a root of unity \( \gamma^m \) so that

\[ \gamma^m = \gamma^m \gamma_n \prod_{j=1}^{s-1} \gamma_j^{y_j m_j} \]

satisfies

\[ \prod_{j=1}^{s-1} \beta_j^{x_j} = \delta \quad \text{if} \quad m_s \not\equiv 0 \mod 2g, \]

\[ \prod_{j=1}^{s-1} \beta_j^{x'_j} = \delta \quad \text{if} \quad m_s \equiv 0 \mod 2g, \quad (11) \]

and set \( m'_j = m_j/2 \)

\[ \eta_j = \eta_j, \quad m'_j = m_j, \quad \beta'_j = \beta_j \quad (j \neq s); \]

\[ \eta_j = \eta_j - \eta_j m_j \beta_j, \quad (12) \]

\[ \beta'_j = \beta_j \quad j > s; \]

\[ \epsilon_{ij} = \begin{cases} \varepsilon_{ij} - \varepsilon_{ij} m_j \beta_j & \text{if} \quad j \neq s, \\ \varepsilon_{ij} & \text{if} \quad j \geq s; \end{cases} \]

\[ \varepsilon_i = \prod_{j=1}^{k} \eta_j^{\epsilon_{ij}} \cdot \mathbb{G}. \quad (13) \]

We find

\[ \varepsilon_i = \varepsilon_i^{\eta_i \gamma_i} \quad \text{and} \quad \varepsilon_i^{\eta_i} = \eta_i \quad (1 \leq i \leq k) \]

because of (8).

The conditions \( \det[\varepsilon_{ij}] = \pm 1 \) and \( m'_j \mid n_i \varepsilon'_{ij} \) follow also from (8) since by (13)

\[ \begin{vmatrix} 1 & 0 \\ \vdots & \ddots \\ 0 & 1 \end{vmatrix} \]

\[ \varepsilon_{ij} = \begin{vmatrix} \varepsilon_{ij} \\ \vdots \\ \varepsilon_{ij} \end{vmatrix} \quad (1 \leq j \leq k) \]

\[ \det[\varepsilon_{ij}] = \det[\varepsilon_{ij}] \quad \text{and} \quad m_j \mid n_i \varepsilon'_{ij}. \]

Finally suppose that \( m'_j y'_j = 0 \mod g \quad (1 \leq j \leq k) \) and \( \prod_{j=1}^{k} \beta_j^{y_j} \in \mathbb{G} \).

If \( y_s = 0 \mod 2 \) we have by (10), (11) and (12)

\[ -\prod_{j=1}^{s-1} \beta_j^{y_j} - \prod_{j=s}^{s-1} \beta_j^{y'_j} \in \mathbb{G} \]

which contradicts (9) since

\[ \prod_{j=1}^{s-1} \beta_j^{y_j} = \prod_{j=1}^{s-1} \beta_j^{y'_j} \quad (1 \leq j \leq s) \]

\[ \prod_{j=s}^{s-1} \beta_j^{y'_j} = \prod_{j=s}^{s-1} \beta_j^{y'_j} \quad (1 \leq j \leq s). \]

If \( y_s = 1 \mod 2 \) we have \( m_s = 0 \mod 2g \) and by (11) and (12)

\[ -(\varepsilon \delta)^{s} \prod_{j=1}^{s-1} \beta_j^{y_j} \in \mathbb{G} \]

contrary to the choice of \( s \).
Thus $\eta'_1, \ldots, \eta'_j, m_1, \ldots, m_k$ satisfy all conditions imposed on $\eta_1, \ldots, \eta_k, m_1, \ldots, m_k$, and $m'_1 \ldots m'_j < m_1 \ldots m_k$, a contradiction.

Consider next the case $p = q > 2$. Let us choose a root of unity
\[
\zeta_m' = \zeta_m' \eta_1 \prod_{i=1}^{j-1} \eta_i^{m_i' \delta_i},
\]
satisfies $\eta_i^{m_i' \delta_i} = \delta_i$.

Set $m'_i = m_i/p$ and define $\eta'_i, m'_i (j \neq \delta), \zeta'_i, \xi'_i$ by the formulas (12), (13), (14). We find as before that $\xi'^i_j = a_i (1 \leq i \leq k), \det [\xi'_j] = -1 \lambda$ and $m'_i | m_i \eta_\delta$. If now $m'_i | \eta_i = 0 \mod g (1 \leq j \leq k)$ then $\xi'_i = 0 \mod g (1 \leq i \leq k)$ and since $K^q \subseteq \mathcal{S}$, $-\prod_{i=1}^{k} \beta'^i_j \xi^j \notin \mathcal{S}$ implies $-1 \epsilon \mathcal{S}$ 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 $n_i = \prod_{h=1}^{H} p_i^{\delta_{ih}} (1 \leq i \leq k)$, where $p_1, \ldots, p_H$ are distinct primes. By the already proved case of the lemma for each $h \leq H$ there exist $\xi_{ih}, \eta_{ih}$ and $m_{ih} (1 \leq i \leq k)$ such that
\[
\begin{align*}
\xi_{ih}^{m_{ih} a_i} = a_i, & \quad \eta_{ih}^{m_{ih} \delta_i} = \beta_{ih}, \\
\langle \xi_{ih}, \ldots, \xi_{ih} \rangle = \langle \eta_{ih}, \ldots, \eta_{ih} \rangle, & \\
[m_{ih}, \ldots, m_{ih}] | p_i^{H_{ih}},
\end{align*}
\]
implies $a_i = 0 \mod p_h (p_h | m_{ih})$ and
\[
m_{ih} \eta_{ih} = 0 \mod g \quad \text{implies} \quad -\prod_{i=1}^{k} \beta_{ih}^j \notin \mathcal{S}.
\]

We get
\[
\begin{align*}
\langle \eta_{1h}, \ldots, \eta_{kh}, \eta_{1h}, \ldots, \eta_{1h}, \ldots, \eta_{kh} \rangle &= \langle \xi_{1h}, \ldots, \xi_{1h}, \xi_{2h}, \ldots, \xi_{2h}, \ldots, \xi_{kh} \rangle, \\
[m_{1h}, \ldots, m_{kh}, m_{1h}, \ldots, m_{kh}, \ldots, m_{kh}] | [m_{1h}, \ldots, m_{kh}],
\end{align*}
\]
implies $a_j = 0 \mod p (p | m_j)$ and if $\xi_i \in K$
\[
m_{ih} \eta_{ih} = 0 \mod 4 (1 \leq j \leq k) \quad \text{implies} \quad \prod_{i=1}^{k} \beta_{ih}^j \notin \mathcal{S}, -4^q, -4^q.$

If $\xi_i \notin K$ we see at once that the conditions of Theorem 1 are satisfied; if $\xi_i \in K$ they are also satisfied since then by (18)
\[
\prod_{i=1}^{k} \beta_{ih}^j = -4^q, n_i \alpha_i = 0 \mod 4 (2 | n_i) \quad \text{implies} \quad \prod_{i=1}^{k} \beta_{ih}^j = (2 \xi_i \gamma)^q,
\]
\[
a_i = 0 \mod 2, \prod_{i=1}^{k} \beta_{ih}^j = 0 \mod 4 (1 \leq i \leq k). \]

By Theorem 1 we have $[K(\eta_1, \ldots, \eta_k) : K] = m_1 \ldots m_k = [K^q(\eta_1, \ldots, \eta_k) : K^q]$, hence the theorem.
Lemma 3. If \( \eta_1, \ldots, \eta_l, n_1, \ldots, n_l \) satisfy the conditions of Lemma 2 with \( g = 2 \), \( \delta = K^n \), \( \delta = K^n \) and \( \sqrt{\delta} K^{\langle \eta_1, \ldots, \eta_l \rangle} \) then

\[
\sqrt{\delta} K^{\langle \eta_1, \ldots, \eta_l \rangle} \quad \text{and} \quad \delta \neq -1.
\]

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

\[
[K^{\langle \sqrt{\delta}, \eta_1, \ldots, \eta_l \rangle}; K^n] = [K^{\langle \sqrt{\delta}, \eta_1, \ldots, \eta_l \rangle}; K^n] = [K, \eta_1, \ldots, \eta_l; K^n]
\]

thus by Kneser’s theorem we have for a certain prime \( p \)

\[
\zeta_p \in K^{\langle \sqrt{\delta}, \eta_1, \ldots, \eta_l \rangle} \quad \text{or} \quad \zeta_p \in K
\]

or

\[
1 + \zeta_4 \in K^{\langle \sqrt{\delta}, \eta_1, \ldots, \eta_l \rangle} \quad \text{or} \quad \zeta_4 \in K.
\]

However \( \zeta_p = \gamma \sqrt{\delta} \prod_{j=1} \eta_j^{\beta_j} \gamma \in K \), gives

\[
\sqrt{\delta} K^{\langle \eta_1, \ldots, \eta_l \rangle} \quad \text{unless} \quad x_0 = 0 \mod 2. \text{ In the later case let}
\]

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

If \( p \mid m \) we get

\[
\prod_{j=1} \beta_j^{m_j} = \gamma \sqrt{\delta} \prod_{j=1} \eta_j^{\beta_j} \gamma \in K
\]

and by the assumption

\[
\frac{m_j}{m_j} = 0 \mod p \quad (1 \leq j \leq l).
\]

This gives by Lemma 1 \( [x_i/(m_i, x_1), \ldots, x_i/(m_i, x_l)] = 0 \mod p \) and for a \( j \leq l \) \( x_i/(m_i, x_j) = m_j/(m_j, x_j) = 0 \mod p \), a contradiction.

If \( p \not\mid m \) we have

\[
\zeta_p = \gamma \sqrt{\delta} \prod_{j=1} \eta_j^{\beta_j} \gamma \in K; \quad \zeta_p \in K.
\]

Suppose now that \( \gamma \in K \),

\[
1 + \zeta_4 = \gamma \sqrt{\delta} \prod_{j=1} \eta_j^{\beta_j} \quad \text{or} \quad \zeta_4 = \sqrt{\gamma} \prod_{j=1} \eta_j^{\beta_j} 
\]

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

If \( 4 \mid m \) then

\[
(\gamma \sqrt{\delta})^m = \gamma m \beta_j^{m_j} \prod_{j=1} \beta_j^{m_j} \quad \text{or} \quad (\gamma \sqrt{\delta})^m = \gamma m \beta_j^{m_j}
\]

and by the assumption \( x_j/m_j = 0 \mod 2 \) (1 \( \leq j \leq l \). This gives by Lemma 1 \( [x_i/(m_1, x_1), \ldots, x_i/(m_l, x_l)] = 0 \mod 2 \) and for a \( j \leq l \)

\[
\frac{x_j}{m_j} = \frac{m_j}{m_j} = 0 \mod 2,
\]

a contradiction.

If \( 4 \not\mid m \) then (19) gives

\[
(2\zeta_4)^{m_l} = \gamma^{m_l} \gamma \sqrt{\delta} \gamma \prod_{j=1} \beta_j^{m_j} \quad \text{or} \quad (2\zeta_4)^{m_l} = \gamma^{m_l} \gamma \sqrt{\delta} \gamma
\]

or

\[
(-1)^{m_l} = \gamma^{m_l} \gamma \sqrt{\delta} \gamma \prod_{j=1} \beta_j^{m_j} \quad \text{or} \quad (-1)^{m_l} = \gamma^{m_l} \gamma \sqrt{\delta} \gamma
\]

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 \( \beta_1, \ldots, \beta_l \) non-zero elements of \( K \). If each of the fields \( K^{\langle \eta_1, \ldots, \eta_l \rangle} \), where \( \eta_j^{m_j} = \beta_j (1 \leq j \leq l) \) contains at least one \( \eta \) with \( \eta^n = \beta \) then for any choice of \( \eta_j \) and \( \eta \) and for suitable exponents \( 0, r, \ldots, r_l \)

\[
\zeta_\eta \eta_1^{r_1} \cdots \eta_l^{r_l} \in K
\]

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 \( \gamma \) be defined as in Thoerem 3. \( \delta \in K \) is of the form \( \gamma \), where \( \delta \in K \) if and only if at least one of the following three conditions is satisfied for a suitable \( \gamma \in K \):.

\[
\theta = \gamma
\]

\[
n \neq 0 \mod 2 \quad \gamma
\]

\[
n \neq 0 \mod 2 \quad \gamma
\]

If \( \zeta_\eta \) the two last 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 \( n \neq 0 \mod 2 \) and \( n \neq 0 \mod 2 \) then

\[
-1 = (\zeta_\eta)^n
\]
and if \( n = 0 \mod 2^r \) then
\[
(-1)^{m_2^*}(\zeta_{2^r} + \zeta_{2^r}^{-1} + 2)^{m_2^*} = (\zeta_{2^r} + 1)^n.
\]
On the other hand since \( \zeta_{2^r} + \zeta_{2^r}^3 \in K \),
\[
\zeta_{2^r} = \frac{1}{2}(\zeta_{2^r} + \zeta_{2^r}^{-1}) \pm \frac{1}{2} \zeta_4 (\zeta_{2^r}^{2^r - 2} + \zeta_{2^r}^{2^r + 2r - 2}) \in K(\zeta_4).
\]
The last assertion of the lemma is obvious.

Proof of Theorem 3. Let us assume first that for all \( l \)
\[
\prod_{i \equiv l} a_i^{l_i} \neq -\delta^2.
\]
Then by Lemma 2 applied with \( g = 2 \), \( \mathcal{A} = \mathcal{K}^{12} \) there exist \( \xi_1, \ldots, \xi_k \), \( n_1, n_2, \ldots, n_k \), \( m_1, \ldots, m_k \) such that
\[
\xi_i^{n_i} = a_i \ (1 \leqslant i \leqslant k), \quad \eta_i^{n_i} = \beta_i \mathcal{K} \quad (1 \leqslant j \leqslant l),
\]
\[
\langle \xi_1, \ldots, \xi_k \rangle = \langle n_1, \ldots, n_k \rangle,
\]
\[
[m_1, \ldots, m_k] [n_1, \ldots, n_k],
\]
\[
\prod_{p | m_j} \beta_j^{n_j} = \gamma \quad \text{implies} \quad p | x_j \ (p | m_j)
\]
for all primes \( p \) and
\[
\prod_{i \equiv l} a_i^{l_i} \neq -\gamma^2 \quad \text{for any choice of} \quad y_j.
\]
By Theorem 1 \( [K(\eta_1, \ldots, \eta_l) : K] = m_1 \ldots m_k \) and thus all fields \( K(\eta_1, \ldots, \eta_l) \), where \( \eta_j^{n_j} = \beta_j \) are conjugate over \( K \). If now \( K(\xi_1, \ldots, \xi_k) = K(\eta_1, \ldots, \eta_l) \) contains an \( \eta_j \) with \( \eta_j^{n_j} = \beta_j \) then each field \( K(\eta_1, \ldots, \eta_l) \) contains such an \( \eta \) and by Lemma 4, Lemma 5, (22) and (23) we have either
\[
\beta \prod_{j=1}^{l} \beta_j^{n_j} = \gamma^2
\]
or
\[
\beta \prod_{j=1}^{l} \beta_j^{n_j} = (\xi_{2^r} + \xi_{2^r}^{-1} + 2)^{m_2^*} \gamma^2
\]
for suitable integers \( r_1, \ldots, r_l \) and a suitable \( \gamma \in K \). Indeed, if \( n = 0 \mod 2 \), \( \beta \prod_{j=1}^{l} \beta_j^{n_j} = -\gamma^6 \) or \( n = 2^r \mod 2^r + 1 \), \( \beta \prod_{j=1}^{l} \beta_j^{n_j} = -(\zeta_{2^r} + \zeta_{2^r}^{-1} + 2)^{m_2^*} \gamma^6 \).

The condition (21) implies that
\[
\prod_{j=1}^{l} \beta_j^{n_j} = \prod_{j=1}^{l} \alpha_i^{n_i} = \prod_{i=1}^{b} \alpha_i^{n_i} \quad \text{for suitable integers} \quad q_1, \ldots, q_l \quad \text{Hence (24) leads to (i).}
\]
It remains to consider (25). If \( L = K(\xi_1, \ldots, \eta_l) \) contains an \( \eta \) with \( \eta^\eta = \beta \) then by (25) it contains \( \eta_\eta^{n_\eta} = \beta_\eta \mathcal{K} \) for a certain \( \eta \).

If \( \eta(n, 2^r) = 1 \mod 2 \) then \( L \) contains
\[
\zeta_4^{n_\eta} \left( \frac{\zeta_{2^r} + \zeta_{2^r}^{-1} + 2}{\zeta_{2^r} + \zeta_{2^r}^{-1} + 2} \right) = \pm \zeta_{2^r} + \zeta_{2^r}^{-1} + 2;
\]
if \( \eta(n, 2^r) = 2 \mod 4 \) then \( L \) contains
\[
\zeta_4^{n_\eta} \left( \frac{\zeta_{2^r} + \zeta_{2^r}^{-1} + 2}{\zeta_{2^r} + \zeta_{2^r}^{-1} + 2} \right) = \pm \zeta_{2^r} + \zeta_{2^r}^{-1} + 2;
\]
if \( \eta(n, 2^r) = 0 \mod 4 \) then \( L \) contains \( \zeta_4^{n_\eta} \pm \eta_\eta^{n_\eta} = \pm \zeta_4 \).

By Lemma 3 the last case is impossible and in the first two cases
\[
\sqrt[\eta/2]{(\zeta_{2^r} + \zeta_{2^r}^{-1} + 2)} \in \mathcal{K} \left( \eta_1, \ldots, \eta_l \right) = \mathcal{K} = \mathcal{K} \langle \xi_1, \ldots, \xi_k \rangle.
\]
Hence we obtain
\[
(\zeta_{2^r} + \zeta_{2^r}^{-1} + 2)^{n_\eta} = \phi^2 \prod_{i=1}^{b} \alpha_i^{n_i} \quad \phi \in K,
\]
which together with (26) and (25) gives again (i).

Assume now that for some \( l_1, \ldots, l_k \)
\[
\prod_{x_i^{l_i}} a_i^{l_i} = -\delta^2, \quad \delta \in K.
\]
Then we apply Lemma 2 for the field \( \mathcal{K}(\zeta_4) \) with \( g = 0 \), \( \mathcal{A} = \{1\} \) and we infer the existence of \( \zeta_4 \), \( \eta_4 \), \( \eta_4 \), \( \eta_4 \), \( \eta_4 \), \( m_1, \ldots, m_k \) such that
\[
\zeta_4^{n_4} = a_i (1 \leqslant i \leqslant k), \quad \eta_4^{n_4} = \beta_4 \mathcal{K}(\zeta_4) \quad (1 \leqslant j \leqslant l),
\]
\[
\langle \zeta_4, \ldots, \zeta_4 \rangle = \langle \eta_4, \ldots, \eta_4 \rangle,
\]
\[
[m_1, \ldots, m_k] [n_1, \ldots, n_k],
\]
\[
\prod_{p | m_j} \beta_j^{n_j} = \gamma^2, \quad \gamma \in K(\zeta_4) \quad \text{implies} \quad p | x_j \ (p | m_j)
\]
for all primes \( p \).

By Theorem 1 \( [K(\zeta_4, \eta_4, \ldots, \eta_4) : K(\zeta_4)] = m_2 \ldots m_k \) (see the end of the proof of Theorem 2) and thus all fields \( K(\zeta_4, \eta_1, \ldots, \eta_l) \), where \( \eta_4^{n_4} = \beta_4 \) are conjugate over \( K(\zeta_4) \).
If now $K(\xi_1, \ldots, \xi_k) = K(\zeta_1, \eta_1, \ldots, \eta_l)$ contains an $\eta$ with $\eta^n = \beta$ then each field $K(\xi_1, \eta_1, \ldots, \eta_l)$ contains such an $\eta$ and by Lemma 4 we have

$$\beta \prod_{i=1}^{l} \beta_j \xi_i^{n_{ij}} = \beta^n, \quad \delta \subset K(\zeta_k).$$

The condition (27) implies that

$$\prod_{i=1}^{l} \beta_j \xi_i^{n_{ij}} = \prod_{i=1}^{k} \alpha_i^{n_{ij}}$$

for suitable integers $n_1, \ldots, n_k$. Hence $\delta \subset K$ 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 $\xi_i^{n_i} = n_i$ $(1 \leq i \leq k)$ contains $\eta = \gamma \prod_{i=1}^{k} \xi_i^{-n_i}$ with $\eta^n = \beta$.

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

$$\beta \prod_{i=1}^{k} \alpha_i^{n_{ij}} = \beta^n$$

where $\delta \subset K(\zeta_k)$. On the other hand, the equality $\prod_{i=1}^{l} \alpha_i^{n_i} = \beta^n$ implies

$$\zeta_k = \pm \prod_{i=1}^{l} \xi_i \xi^{n_i}. \delta^n.$$

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

The last assertion of the Theorem if $\zeta_k \subset K$ follows from the last assertion of Lemma 5.

If $\tau = 2$ and $n \neq 0 \mod 2^s$ we have either $n = 1 \mod 2$, in which case $-\delta^n = (-\gamma)^n$ or $n = 2 \mod 4$. In the latter case we get from (ii)

$$\beta \prod_{i=1}^{k} \alpha_i^{n_{ij}} \prod_{i=1}^{l} \alpha_i^{-n_i} = (\gamma \beta)^n$$

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

\begin{align*}
(28) \quad & a^n = \beta^n, \quad \beta = a^n; \\
(29) \quad & n \neq 0 \mod 2^s, \quad a = -\beta^n = -a^n; \\
(30) \quad & a = -\beta^n = \beta^n = -a^n; \\
(31) \quad & n \neq 0 \mod 2^s, \quad \beta = -\beta^n = a^n; \\
(32) \quad & n = 0 \mod 2^s, \quad a = -\beta^n = -\beta^n; \\
& \beta = -\beta^n = a^n,
\end{align*}

and two other possibilities obtained by the permutation of $a$ and $\beta$ in (29) and (30). Here $\gamma^n = \beta$ means that $\gamma \beta$ is an $n$th power in $K$, $s = (-1)^{n/2}$ and $\omega = (\gamma^n + \gamma^{-n})/2$.

Moreover in (29) to (32) it is assumed that $\zeta_k \subset K$. Now, (29) gives $t = 1 \mod 2$, $a = -a^n$, $a^n = -a^n$, $\beta = a^n$.

(30) gives $t = 1 \mod 2$, $a = -a^n$, $a^n = -a^n$, $\beta = a^n$.

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

$$-\delta^n = -\beta^n = \delta^n$$

and $\zeta_k \subset K$.

If $s = t = 0 \mod 2$ then

$$a = -a^n, \quad a^n = -a^n, \quad \beta = a^n.$$

Thus in any case we have either $\beta = a^n$ or $n = 0 \mod 2^{s+1}$, $a = -\delta^n$, $\beta = \delta^n$. On the other hand if at least one of these conditions is satisfied then by Theorem 3 each of the fields $K(\xi)$ with $f(\xi) = 0$ contains an $\eta$ 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 relativer algebraischer Zahlen, Monatsh. Math. Phys. 49 (1939), p. 63. However already the special case of the latter theorem given by Nagell in his Theorem 3 is not valid in general, as shown by the example $\Omega = Q$, $n = 3$, $a = -1$, $b = -16$ contained in Theorem 6 of Gerst [1].

References


Received on 2, 4, 1974 and in revised form on 2, 5, 1974 (561)
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 $A_k = A_k(n)$ be the generalized von Mangoldt function

\begin{equation}
A_k = \mu \ast L^k, \tag{1.1}
\end{equation}

$k$ integral $\geq 1$, where $\mu$ denotes the Möbius function, $L$ denotes the arithmetical function $\log n$, and $\ast$ denotes the Dirichlet convolution. Clearly $A_1 = A$, the von Mangoldt function, and it is easily shown that

\begin{equation}
A_k = A_{k-1}L + A_{k-1} \ast A, \tag{1.2}
\end{equation}

therefore

\begin{align*}
A_2 &= A L + A \ast A, \\
A_3 &= A L^2 + 3AL \ast A + A \ast A \ast A,
\end{align*}

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

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

\begin{equation}
\sum_{n \leq x} A(n + 2) A_k(n), \tag{1.3}
\end{equation}

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 $k \geq 2$, 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.