ON MULTIPLICATIVE AND LINEAR INDEPENDENCE OF POLYNOMIAL ROOTS

Michael Drmota and Mariusz Skalba

Technical University of Vienna, Warsaw University

Abstract. Let K be a field, $f(x) \neq x^p + c$ an irreducible polynomial of degree p without multiple roots, where p is an odd prime, and $x_1, x_2, \ldots, x_p$ its roots. Then (under certain conditions on K) $\prod_{i=1}^p x_i^{k_i} \in K$ if and only if $k_1 = k_2 = \cdots = k_p$ (where k_i are arbitrary integers). A similar theorem holds for the additive case.

1. Introduction

Let K be a field and

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{1}$$

an irreducible polynomial over K of degree $n > 1$ and consider following question: *Does there exist an irreducible polynomial $f(x) \neq x^n + a_0$ such that one root is the product of two other roots of $f(x)$?*

An example of A. Schinzel shows that there exist such polynomials. Let $K = \mathbf{Q}$ and

$$\begin{aligned} f(x) &= x^6 - 2x^4 - 6x^3 - 2x^2 + 1 \\ &= \left(x^3 + \sqrt{2}x^2 + \sqrt{2}x - 1\right)\left(x^3 - \sqrt{2}x^2 - \sqrt{2}x - 1\right) \\ &= f_1(x)\, f_2(x). \end{aligned} \tag{2}$$

If x_1, x_2 are two roots of $f_1(x)$, then by Vieta $x_3 = (x_1x_2)^{-1}$ is the third root of $f_1(x)$. Of course x_1, x_2, x_3 are different because $f(x)$ is separable. Furthermore the reciprocals $x_1^{-1}, x_2^{-1}, x_3^{-1} = x_1x_2$ are also roots of $f(x)$ but they are not roots of $f_1(x)$. Therefore $x_1^{-1}, x_2^{-1}, x_1x_2$ are the three roots of $f_2(x)$.

But if n is an odd prime we have

Theorem 1. *Let p be an odd prime number, K a field, $f(x) \in K[x]$ an irreducible polynomial $\neq x^p + a_0$ of degree p over K without multiple roots, and $x_1, x_2, \ldots, x_p \in \overline{K}$ its roots. Furthermore let the degree of extension $(K(\zeta_m) : K)$ be different from p for all positive integers m, where ζ_m denotes a primitive m-th root of unity. Then we have for arbitrary integers $k_1, k_2, \ldots, k_p$*

$$\prod_{i=1}^p x_i^{k_i} \in K \tag{3}$$

The authors want to thank Prof. A. Schinzel for his many useful comments during the preparation of this paper.

if and only if $k_1 = k_2 = \cdots = k_p$.

Therefore there do not exist polynomials such that one root is the product of two other roots (in general) for n being a prime.

For example $K = \mathbf{Q}$ satisfies the condition $(K(\zeta_m) : K) = \varphi(m) \neq p$ since Euler's function $\varphi(m)$ is even for $m > 2$ and $\varphi(2) = 1 \neq p$

A similar theorem holds for the additive case:

Theorem 2. *Let p be an odd prime number, K a field with char$(K) \neq p$, $f(x) \in K[x]$ an irreducible polynomial of degree p over K without multiple roots, and $x_1, x_2, \ldots, x_p \in \overline{K}$ its roots. Furthermore assume that $(K(\zeta_p) : K) = p - 1$, where ζ_p denotes a primitive p-th root of unity. Then we have for arbitrary $k_1, k_2, \ldots, k_p \in K$*

$$\sum_{i=1}^{p} k_i\, x_i \in K \tag{4}$$

if and only if $k_1 = k_2 = \cdots = k_p$.

As an interesting corollary we deduce

Theorem 3. *Let p be a prime number, $f(x) = x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0$ an irreducible polynomial over $\mathbf{Q}$, and $x_1, x_2, \ldots, x_p$ its roots.*

If $p > 2$, $a_0 \neq -1$, and there is an $i \in \{1, 2, \ldots p-1\}$ with $a_i \neq 0$ then the numbers

$$\log x_1, \log x_2, \ldots, \log x_p$$

are linear independent over $\mathbf{Q}$ (where $\log$ denotes any fixed branch of the logarithm with $\log 1 = 0$).

If $a_{p-1} \neq 0$ then the numbers

$$x_1, x_2, \ldots, x_p$$

are linear independent over $\mathbf{Q}$.

Remark. It should be noticed that the problem of independence of polynomial roots has been considered several times (e.g. by L.J. Mordell [2]) but from another point of view. For example, in [2] the independence of $x_1, \ldots, x_s \in K$ that are roots of polynomials $x^{n_i} - a_i$, $a_i \in K$ $(i = 1, 2, \ldots, s)$ is discussed.

2. The Cyclic Determinant

For the proof of Theorems 1 and 2 we will need some facts of the cyclic determinant. Let $k_1, k_2, \ldots, k_n \in K$, then it is well known that the determinant D of the cyclic matrix

$$C = C(k_1, k_2, \ldots, k_n) = \begin{pmatrix} k_1 & k_2 & k_3 & \cdots & k_n \\ k_n & k_1 & k_2 & \cdots & k_{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ k_2 & k_3 & k_4 & \cdots & k_1 \end{pmatrix} \tag{5}$$

can be evaluated by

$$\begin{aligned} D = D(k_1, k_2, \ldots, k_n) &= \det(C(k_1, k_2, \ldots, k_n)) \\ &= \prod_{j=1}^{n} \left(\sum_{i=1}^{n} k_i \, \zeta_n^{(i-1)(j-1)} \right) \\ &= \sum_{i=1}^{n} k_i \cdot \prod_{j=2}^{n} \left(\sum_{i=1}^{n} k_i \, \zeta_n^{(i-1)(j-1)} \right), \end{aligned} \tag{6}$$

where ζ_n is a primitive n-th root of unity (see [3,p 561]). Therefore $D = 0$ if $\sum_{i=1}^{n} k_i = 0$. But exactly this case will be the interesting one in the proof of the first two theorems. In this case we have

Proposition 1. *Let K be a field, n a positive integer coprime to char(K), and $k_1, k_2, \ldots, k_n \in K$ with $\sum_{i=1}^{n} k_i = 0$. Then the minor D_{11} of the cyclic matix $C = C(k_1, k_2, \ldots, k_n)$ (that results after deleting the first row and first column) can be evaluated by*

$$D_{11} = \frac{1}{n} \prod_{j=2}^{n} \left(\sum_{i=1}^{n} k_i \, \zeta_n^{(i-1)(j-1)} \right), \tag{7}$$

where ζ_n is a primitive n-th root of unity.

Proof. For the proof let k_i be complex numbers. Namely, if (7) holds for complex numbers it is a polynomial identity in $k_1, k_2, \ldots, k_{n-1}$, $-(k_1 + k_2 + \cdots + k_{n-1})$ and therefore a formal polynomial identity, too.

Now vary k_n in a way such that $k_n(\eta) = k_n(0) + \eta$ $(\eta \neq 0)$. Then $\sum_{i=1}^{n} k_i = \eta$ and the determinants D, D_{ij} depend on η, too. (D_{ij} denotes the minor of C that results after deleting the i-th row and j-th column.) Furthermore let M_{1j} be the determinant, where the $(j-1)$-st column of D_{1j} is replaced by 1's. By Laplace's theorem $D(\eta)$ can be determined by

$$D(\eta) = \sum_{j=1}^{n} k_j (-1)^{j+1} \, D_{1j}(\eta). \tag{8}$$

It is interesting that (for $j > 1$)

$$(-1)^{j+1} \, D_{1j}(\eta) = D_{11}(\eta) - \eta \, M_{1j}(\eta). \tag{9}$$

We will indicate a proof of formula (9) for $j = 4$:

$$
\begin{aligned}
D_{11}(\eta) &= \begin{vmatrix} k_1 & k_2 & k_3 & \cdots & k_{n-1} \\ k_n & k_1 & k_2 & \cdots & k_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ k_3 & k_4 & k_5 & \cdots & k_1 \end{vmatrix} \\
&= \begin{vmatrix} k_1 & k_2 & (k_1+k_2+\cdots+k_{n-1}) & k_4 & \cdots & k_{n-1} \\ k_n & k_1 & (k_1+k_2+\cdots+k_{n-2}+k_n) & k_3 & \cdots & k_{n-2} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ k_3 & k_4 & (k_1+k_3+k_4+\cdots+k_n) & k_6 & \cdots & k_1 \end{vmatrix} \\
&= \begin{vmatrix} k_1 & k_2 & \eta-k_n & k_4 & \cdots & k_{n-1} \\ k_n & k_1 & \eta-k_{n-1} & k_3 & \cdots & k_{n-2} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ k_3 & k_4 & \eta-k_2 & k_6 & \cdots & k_1 \end{vmatrix} \\
&= \eta \begin{vmatrix} k_1 & k_2 & 1 & k_4 & \cdots & k_{n-1} \\ k_n & k_1 & 1 & k_3 & \cdots & k_{n-2} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ k_3 & k_4 & 1 & k_6 & \cdots & k_1 \end{vmatrix} - \begin{vmatrix} k_1 & k_2 & k_n & k_4 & \cdots & k_{n-1} \\ k_n & k_1 & k_{n-1} & k_3 & \cdots & k_{n-2} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ k_3 & k_4 & k_2 & k_6 & \cdots & k_1 \end{vmatrix} \\
&= \eta\, M_{14}(\eta) + (-1)^{4+1} D_{14}(\eta).
\end{aligned}
$$

Thus we get for $D(\eta)$

$$D(\eta) = \sum_{j=1}^{n} k_j (-1)^{j+1}\, D_{1j}(\eta) = \eta\, D_{11}(\eta) - \eta \sum_{j=2}^{n} k_j M_{1j}(\eta). \tag{10}$$

To get some information about the last sum consider the system of $n-1$ linear equations

$$C_{11}(\eta) \begin{pmatrix} y_2 \\ y_3 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}, \tag{11}$$

where $C_{11}(\eta)$ is the submatix of $C(\eta)$ that corresponds to the determinant $D_{11}(\eta)$. Trivially by Cramer's rule

$$y_j\, D_{11}(\eta) = M_{1j}(\eta). \tag{12}$$

Now sum up the $n-1$ equations of (11) to get

$$\sum_{j=2}^{n} (\eta - k_j) y_j = n - 1$$

and use (12) to conclude that

$$\sum_{j=2}^{n} k_j\, M_{1j}(\eta) = (1-n)\, D_{11}(\eta) + \eta \sum_{j=2}^{n} M_{1j}(\eta). \tag{13}$$

Inserting (13) into (10) gives

$$D(\eta) = \eta\, n\, D_{11}(\eta) - \eta^2 \sum_{j=2}^{n} M_{1j}(\eta). \tag{14}$$

After comparing (14) with (6), and setting $\eta = 0$ we finally get (7).

As a corollary we have

Proposition 2. *Let K be a field, p a prime number different from char(K) such that $(K(\zeta_p) : K) = p-1$ (where ζ_p denotes a primitve p-th root of unity) and $k_1, k_2, \dots, k_p \in K$ such that at least two of them are different. Then we have for the case $\sum_{i=1}^{p} k_i \neq 0$ that*

$$D(k_1, k_2, \dots, k_p) \neq 0 \tag{15}$$

and in the case $\sum_{i=1}^{p} k_i = 0$ that

$$D(k_1, k_2, \dots, k_p) = 0 \quad \textit{but} \quad D_{11}(k_1, k_2, \dots, k_p) \neq 0. \tag{16}$$

Proof. Since $(K(\zeta_p) : K) = p-1$, the primitive polynomial of ζ_p is $\varphi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ and therefore

$$\sum_{i=1}^{p} k_i \zeta_p^{(i-1)(j-1)} \neq 0$$

for $j > 1$, because at least two of the elements $k_1, k_2, \dots, k_p$ are different. Thus Proposition 2 follows from (6) and Proposition 1.

It should be remarked that Proposition 1 and 2 prove more that we really need for the proofs of Theorem 1 and 2. We will use Proposition 2 but essentially we only need that rank$(D) = p-1$ if $\sum_{i=1}^{p} k_i = 0$. This can be seen by following general theorem, too. (We want to thank Prof. A. Schinzel for this remark.)

Theorem. *Let K be a field, n a positive integer coprime to char(K), and $k_1, k_2, \dots, k_n \in K$. Then the number of distinct n-th roots of unity that satisfy the equation*

$$g(x) = k_1 + k_2 x + \cdots + k_n x^{n-1} = 0$$

is $n-$rank(C), where $C = C(k_1, k_2, \dots, k_n)$ denotes the cyclic matrix (5).

Proof. (A. Schinzel): Let ζ_n be a primitive n-th root of unity and

$$B = \begin{pmatrix} 1 & \zeta_n & \cdots & \zeta_n^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \zeta_n^{n} & \cdots & \zeta_n^{n(n-1)} \end{pmatrix}. \tag{17}$$

By the assumption that n is coprime to $\mathrm{char}(K)$ the matrix B is non-singular. Hence $\mathrm{rank}(C) = \mathrm{rank}(BC^t)$, while

$$BC^t = \begin{pmatrix} g(\zeta_n) & \zeta_n g(\zeta_n) & \cdots & \zeta_n^{(n-1)} g(\zeta_n) \\ \vdots & \vdots & & \vdots \\ g(\zeta_n^n) & \zeta_n^n g(\zeta_n^n) & \cdots & \zeta_n^{n(n-1)} g(\zeta_n^n) \end{pmatrix}. \tag{18}$$

Let S be the set of positive integers $j \le n$ such that $g(\zeta_n^j) = 0$ and $N = |S|$. We have $\mathrm{rank}(BC^t) \le n - N$ since N rows of the matrix BC^t consist of zeros. On the other hand $\mathrm{rank}(BC^t) \ge n - N$ since the minor of BC^t consisting of the rows $j_1, \ldots, j_{n-N} \notin S$ and colums $1, 2, \ldots, n-N$ equals

$$\prod_{j\in S} g(\zeta_n^j)\, V\left(\zeta_n^{j_1}, \ldots, \zeta_n^{j_{n-N}}\right), \tag{19}$$

where V is Vandermonde. Hence $\mathrm{rank}(C) = \mathrm{rank}(BC^t) = n - N$.

Remark. Note that this theorem is an analogon to the König—Rados-theorem (see [3,p 507]). But there only finite fields are considered.

Proof of Theorem 1 and 2

Before proving Theorem 1 and 2 let us state two propositions that are also valid for non-separable polynomials $f(x)$.

Proposition 3. *Let p be a prime number, K a field, $f(x)$ an irreducible polynomial of degree p over K, and $x_1, x_2, \ldots, x_p \in \overline{K}$ its roots. If there exist integers $k_1, k_2, \ldots, k_p$ satisfying*

$$\begin{aligned} &(i) \quad \text{at least two of them are different} \\ &(ii) \quad \sum_{i=1}^{p} k_i \ne 0 \\ &(iii) \quad \prod_{i=1}^{p} x_i^{k_i} \in K, \end{aligned} \tag{20}$$

then there exist positive integers m_i $(i = 1, 2, \ldots, p)$ such that

$$x_i^{m_i} \in K.$$

Moreover if we assume

$$(iii') \quad \prod_{i=1}^{p} x_i^{k_i} = 1 \tag{21}$$

instead of (iii), then there exist positive integers m_i such that

$$x_i^{m_i} = 1.$$

Proof. First consider the case that $f(x)$ has multiple roots. Then $f(x) \in K[x^q]$, where $q = \mathrm{char}(K)$. But $\deg(f) = p$, a prime number. Hence $p = q$ and $f(x) = x^p + c$ for some $c \in K$. Thus $m_i = p$ is a proper choice for the general case. Note that the assumptions (i), (ii), and (iii) have not been used. But now assume that (i), (ii), and (iii') are true. Then

$$1 = \left(\prod_{i=1}^{p} x_i^{k_i}\right)^p = (-c)^{\sum_{i=1}^{p} k_i}$$

implies that $m_i = |p \cdot \sum_{i=1}^{p} k_i|$ can be used to ensure that $x_i^{m_i} = 1$.

Now suppose that $f(x)$ has no multiple roots. Since

$$p = (K(x_1) : K) \,|\, (K(x_1, \dots, x_p)) = |\mathrm{Gal}(f)| \tag{22}$$

there exists a $\sigma \in \mathrm{Gal}(f)$ with $|[\sigma]| = p$. Furthermore $\mathrm{Gal}(f) \subseteq S_p$. So σ must be a cycle of period p. Without loss of generality set

$$\sigma = (x_1, x_2, \dots, x_p). \tag{23}$$

Now we have for $j = 0, 1, \dots, p-1$

$$\prod_{i=1}^{p} \sigma^j(x_i)^{k_i} = \prod_{i=1}^{p} x_{i+j (\mathrm{mod}\ p)}^{k_i} = a \in K. \tag{24}$$

Now Proposition 2 applied to $K = \mathbf{Q}$ gives $D = D(k_1, \dots, k_p) \neq 0$. Thus it is possible to find integers v_{ij} and positive intergers m_i such that

$$\sum_{j=0}^{p-1} v_{ij} k_{l-j (\mathrm{mod}\ p)} = \begin{cases} m_i & \text{for } l = i \\ 0 & \text{for } l \neq i \end{cases} \tag{25}$$

Therefore we get by (24)

$$\begin{aligned} x_i^{m_i} &= \prod_{l=1}^{p} x_l^{\sum_{j=0}^{p-1} v_{ij} k_{l-j (\mathrm{mod}\ p)}} \\ &= \prod_{j=0}^{p-1} \left(\prod_{l=1}^{p} x_l^{k_{l-j (\mathrm{mod}\ p)}}\right)^{v_{ij}} \\ &= a^{\sum_{j=0}^{p-1} v_{ij}} \in K. \end{aligned}$$

This proves both statements of Proposition 3.

Proposition 4. *Let p be a prime number, K a field, $f(x)$ an irreducible polynomial of degree p over K, and $x_1, x_2, \dots, x_p \in \overline{K}$ its roots. Furthermore let $(K(\zeta_p) : K) = p - 1$, where ζ_p is a primitive p-th root of unity. Then there do not exist $k_1, k_2, \dots, k_p \in K$ satisfying*

$$\begin{aligned} &(i) \quad \text{at least two of them are different} \\ &(ii) \quad \sum_{i=1}^{p} k_i \neq 0 \\ &(iii) \quad \sum_{i=1}^{p} k_i x_i \in K. \end{aligned} \tag{26}$$

Proof. First consider the case that $f(x)$ has a multiple root. As in the proof of Proposition 3 we have that $x_i^p = -c$ for some $c \in K$, where $p = \mathrm{char}(K)$. So $x_i^p = x_j^p$ for all i, j. Thus $(x_i - x_j)^p = 0$ implies that $x_i = x_j$ for all i, j. But then (ii) and (iii) yield $x_i \in K$ which contradicts the assumption that $f(x)$ is irreducible.

Now suppose that $f(x)$ has no multiple roots. Similarly to (24) we get p equations

$$\sum_{i=1}^{p} k_i\, \sigma^j(x_i) = \sum_{i=1}^{p} k_i\, x_{i+j (\mathrm{mod}\ p)} = a \in K. \tag{27}$$

By Proposition 2 $D = D(k_1, k_2, \ldots, k_p) \neq 0$. Notice that the assumption $\mathrm{char}(K) \neq p$ is not used in the case $\sum_{i=1}^{p} k_i \neq 0$. Thus $k_i \in K$ for all i implies that $x_i \in K$ which is again a contradiction to the assumption that $f(x)$ is irreducible.

It should be remarked that Proposition 3 and 4 are optimal in the sense that conditions (i) and (ii) are necessary. But (i) is only necessary in the non-separable case. This is of course the essential part of Theorem 1 and 2.

Proof of Theorem 1. If $k_1 = k_2 = \cdots = k_p = k$, then

$$\prod_{i=1}^{p} x_i^{k_i} = \mathrm{N}(x_1)^k \in K.$$

Thus the first implication is proved.

Now suppose that $\prod_{i=1}^{p} x_i^{k_i} \in K$ and assume that at least two of the integers k_i are different.

If $\sum_{i=1}^{p} k_i \neq 0$ then we have by Proposition 3 that there exists a positive integer $m > 1$ such that $x_1^m \in K$.

If $\sum_{i=1}^{p} k_i = 0$ let b_i, $i = 1, \ldots, p$, be defined by $b_i = x_i x_1^{-1}$. Then we have for $j = 1, 2, \ldots, p-1$

$$\sigma^j \left(\prod_{i=1}^{p} x_i^{k_i} \right) = \prod_{i=2}^{p} b_{i+j (\mathrm{mod}\ p)} = d \in K, \tag{28}$$

(where σ is defined in the proof of Propositon 3). Now we are in a similar situation as in the proof of Proposition 3. (Compare with (24).) Instead of x_i we have to use b_i and instead of $D = D(k_1, \ldots, k_p) \neq 0$ we need that $D_{11} = D_{11}(k_1, \ldots, k_p) \neq 0$. But this is ensured by Proposition 2. Thus we can conclude as before that there exist positive integers m_i such that $b_i^{m_i} \in K$. Set $m' = \mathrm{lcm}(m_2, m_3, \ldots, m_p)$. Then $b_i^{m'} \in K$ for all i. But now

$$\mathrm{N}(x_1)^{m'} = (x_1 x_2 \cdots x_p)^{m'} = x_1^{pm'} b_2^{m'} \cdots b_p^{m'} \in K$$

implies that $x_1^{pm'} \in K$. Thus we have the same conclusion as in the case $\sum_{i=1}^{p} k_i \neq 0$, namely that there exists a positive integer $m > 1$ such that $x_1^m \in K$.

Now let $n = \min\{m \in \mathbf{Z} \,|\, m > 0, x_1^m \in K\}$, that is of course > 1. Set $a = x_1^n \in K$. Then $f(x) | x^n - a$. If $a = 1$ then the definition of n will imply that x_1 is a n-th primitive root of unity and therefore $(K(x_1) : K) \neq p$. But this is a contradiction to $(K(x_1) : K) = \deg(f) = p$. Now let $a \neq 1$. The assumption

$f(x) \neq x^p + a_0$ implies that $x^n - a$ is reducible. Thus by [1,p.221] there exists a prime q dividing n and $b \in K$ with $b^q = a$ or $4|n$ and $a = -4c^4$ for some $c \in K$. The first possibility implies that there is a primitive q-the root of unity ζ_q satisfying $x_1^{n/q}\zeta_q = b$. Thus $zeta_q \in K(x_1) \setminus K$ and so $1 < (K(\zeta_q) : K)|(K(x_1) : K) = p$. But this is a contradiction to $(K(\zeta_q) : K) \neq p$ for $\zeta_q \notin K$. Now assume that $4|n$ and $a = -c^4$ for some $c \in K$. Set $n_1 = n/4$. Furthermore note that $-4c^4 = a \neq 0$ implies that $\mathrm{char}(K) \neq 2$. Now $x^n - a$ splits to at least two factors:

$$x^n - a = x^{4n_1} + 4c^4 = (x^{2n_1} + 2cx^{n_1} + 2c^2)(x^{2n_1} - 2cx^{n_1} + 2c^2). \tag{29}$$

Therefore we can assume (without loss of generality) that

$$f(x)|x^{2n_1} + 2cx^{n_1} + 2c^2.$$

Set $q(x) = x^2 + 2cx + 2c^2 = (x - c_1)(x - c_2)$. Since $q(x_1^{n_1}) = 0$ and $x_1^{n_1} \notin K$, $q(x)$ is irreducible over K. Furthermore $\mathrm{char}(K) \neq 2$ implies that $c_1 \neq c_2$. Now assume that $x_1^{n_1} = c_1$ and (without loss of generality) that $x_2^{n_1} = c_2$. Then $\sigma(c_1) = c_2$ and of course $\sigma(c_2) = c_1$. ($\sigma \in \mathrm{Gal}(f)$ is defined in (23).) But this is impossible because p is odd and so we would have $c_1 = \sigma^p(c_1) = c_2$. Therefore we can suppose (without loss of generality) that $x_i^{n_1} = c_1$ for all i. Thus $f(x)|x^{n_1} - c_1$. But now $(K(c_1) : K) = 2$ implies that there exists a

$$\pi \in G(K(x_1, \ldots, x_p)/K) \setminus G(K(x_1, \ldots, x_p)/K(c_1)).$$

Of course $\pi(c_1) = c_2$ and therefore $\pi(f(x)) = f(x)|\pi(x^{n_1} - c_1) = x^{n_1} - c_2$, which is a contradiction to $c_1 \neq c_2$. Thus $k_1 = k_2 = \cdots = k_p$ and Theorem 1 is proved.

Proof of Theorem 2. If $k_1 = k_2 = \cdots = k_p = k$, then

$$\sum_{i=1}^{p} k_i\, x_i = k \cdot \mathrm{Tr}(x_1) \in K.$$

Now suppose that $\sum_{i=1}^{p} k_i x_i \in K$ and that at least two of $k_i \in K$ are different. By Proposition 4 $\sum_{i=1}^{p} k_i = 0$ Now set $b_i = x_i - x_1$. Similarly to the considerations above we have for $j = 1, 2, \ldots, p-1$

$$\sigma^j \left(\sum_{i=1}^{p} k_i\, x_i \right) = \sum_{i=2}^{p} k_i\, b_{i+j (\mathrm{mod}\ p)} = d \in K.$$

By Proposition 2 $D_{11}(k_1, \ldots, k_p) \neq 0$, which implies that $b_i \in K$. But now

$$\mathrm{Tr}(x_1) = x_1 + \cdots + x_p = p\, x_1 + b_2 + \cdots + b_p \in K$$

yields that $x_1 \in K$, which contradicts the assumption that $f(x)$ is irreducible. Therefore Theorem 2 is proved.

References

1. Lang, S., *Algebra*, Addison—Wesley, Reading, 1969.
2. Mordell, L.J., *On the Linear Independence of Algebraic Numbers*, Pacific J. Math. **3** (1953), 625–630.
3. Rédei, L., *Algebra, Vol. 1*, Pergamon Press, Oxford, 1967.

Michael Drmota
Institute of Algebra and Discrete Mathematics
Technical University of Vienna
Wiedner Hauptstrasse 8–10/118
A-1040 Vienna, AUSTRIA
(MAILING ADDRESS)

Mariusz Skalba
Institute of Mathematics
Warsaw University
PL-00-901 Warsaw, POLAND

SHORT TITLE: On Independence of Polynomial Roots
CLASSIFICATION: 12 D 10, 12 E 05