ACTA ARITHMETICA
XCII.1 (2000)

Algebraic independence of polynomials

by

Ivica Gusić (Zagreb)

Let k be an algebraically closed field, let $k \subseteq K$ be a field extension and let $K(x)$ be the field of rational functions of one variable over K. The aim of this paper is to prove the following

THEOREM. *Let $f, g \in K[x]$ be two nonconstant polynomials. Then f, g are algebraically dependent over k if and only if there exists $h \in K[x]$ such that $f \in k[h]$ and $g \in k[h]$.*

Proof. Assume first that $f, g \in k[h]$. Then $k(f,g) \subseteq k(h)$. Since $k(h)/k$ is of transcendence degree 1, f, g are algebraically dependent over k.

Conversely, assume that f, g are algebraically dependent over k. Then $k(f,g)/k$ is of transcendence degree 1. Since $K \subset K(f,g) \subseteq K(x)$, we conclude, by Lüroth's theorem [1, VI, Sect. 2, Cor. 3 of Th. 2], that the field $K(f,g)$ is of genus 0. Note that $K(f,g)$ is not algebraic over K and it is obtained from $k(f,g)$ by an extension of scalars (see [1, V, Sect. 4]). From [1, V, Sect. 6, Th. 5] we get

$$\text{genus}(k(f,g)) = \text{genus}(K(f,g)) \tag{1}$$

(note that K/k is a separable extension since k is algebraically closed). Therefore

$$\text{genus}(k(f,g)) = 0. \tag{2}$$

As k is algebraically closed, there exists $z \in K(x)$ such that

$$k(f,g) = k(z). \tag{3}$$

Using the arguments from [2, proof of Lemma 2] we conclude that there exists $h \in K[x]$ such that $k(z) = k(h)$ and $f \in k[h]$. Now it is easy to see that also $g \in k[h]$.

COROLLARY. *Let $f = ax^n$, $g = bx^m \in K[x]$ be two monomials, where $a, b \neq 0$ and $n, m \in \mathbb{N}$. Let $d = \gcd(n,m)$. Then f, g are algebraically*

1991 *Mathematics Subject Classification*: 12E05, 12F99.

dependent over k if and only if $f^{m/d}$, $g^{n/d}$ are linearly dependent over k (or equivalently, if $a^{m/d}$, $b^{n/d}$ are linearly dependent over k).

Proof. Suppose that f, g are algebraically dependent over k. By the Theorem, there exist $h \in K[x]$ and $F, G \in k[T]$ such that $f = F(h)$ and $g = G(h)$. Assume that $F(T) = a_0 + a_1T + \ldots + a_rT^r$, where $a_j \in k$. Then

$$ax^n = a_0 + a_1h + \ldots + a_rh^r. \tag{4}$$

From $F(h(0)) = 0$, we get $h(0) \in k$; hence, after a translation, we may assume that $h(0) = 0$, so $a_0 = 0$. We conclude that h is a monomial. Moreover,

$$ax^n = \omega h^r, \quad \omega \in k. \tag{5}$$

Similarly, we get

$$bx^m = wh^s, \quad s \in \mathbb{N},\ w \in k. \tag{6}$$

By (5) and (6), $a^{m/\deg h}$, $b^{n/\deg h}$ are linearly dependent over k, hence $a^{m/d}$, $b^{n/d}$ are linearly dependent over k.

Remark 1. The Corollary can be proved directly. Put $n_1 = n/d$ and $m_1 = m/d$. If f, g are algebraically dependent over k then so are f^{m_1} and g^{n_1}. Since $nm_1 = mn_1$, there is a nontrivial homogeneous polynomial F over k such that $F(a^{m_1}, b^{n_1}) = 0$. Therefore a^{m_1}/b^{n_1} is algebraic over k. Since k is algebraically closed, we get

$$a^{m_1} = \mu b^{n_1} \quad \text{for some } \mu \in k. \tag{7}$$

Remark 2. The fact that k is algebraically closed is essentially used in (3). We will weaken this condition in a special case:

Let k be algebraically closed in K, let $f \in K[x]$ be a monomial and let $g \in K[x]$ be a nonconstant polynomial. Assume that f and any proper power in $K[x]$ are not linearly dependent over k. Then f and g are algebraically dependent over k if and only if $g \in k[f]$.

We sketch a proof. Consider first the general situation: $f = ax^n + f_1$, $\deg f_1 < n$ and $g = bx^m + g_1$, $\deg g_1 < m$. Suppose that f, g satisfy a nontrivial relation $\sum a_{ij} f^i g^j = 0$, where $a_{ij} \in k$. Let M be the maximal exponent of x in the relation. Then

$$\sum_{in+jm=M} a_{ij}(ax^n)^i(bx^m)^j = 0,$$

hence ax^n and bx^m are algebraically dependent over k. Now (7) follows as in Remark 1. Since m_1 and n_1 are relatively prime, there exist $p, q \in \mathbb{Z}$ such that $pm_1 + qn_1 = 1$, hence $a = a^{pm_1+qn_1} = a^{pm_1}a^{qn_1} = \mu^p(b^pa^q)^{n_1}$.

From this we infer that if $f = ax^n$ and if f and any proper power in $K[x]$ are not linearly dependent over k, then $n_1 = 1$, so $n \mid m$. Suppose $m = n$. Then $m_1 = n_1 = 1$, so $a = \mu b$. If f and g are algebraically dependent over k, then so are f and $\mu g - f$. Therefore $\mu g_1 \in K$. It is easy to see that $\mu g_1 \in k$, so $g \in k[f]$. Now we continue by induction on m (starting with $m = n$), using the fact that k-algebraic dependence of f and g implies k-algebraic dependence of f and $g - \alpha f^s$ for every $\alpha \in k$ and $s \in \mathbb{N}$.

Acknowledgements. The author wishes to thank the referee for helpful comments and suggestions, and especially for pointing out several mistakes and a direct proof of the Corollary.

References

[1] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Amer. Math. Soc., Providence, 1951.

[2] A. Schinzel, *Reducibility of polynomials in several variables*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 11 (1963), 633–638.

Faculty of Chemical Engineering
and Technology
University of Zagreb
Marulićev trg 19, p.p. 177
10 000 Zagreb, Croatia
E-mail: igusic@pierre.fkit.hr

Received on 12.5.1998
and in revised form on 8.7.1999 (3381)