Acta Mathematica Universitatis Ostraviensis

Marius Cavachi; Marian Vâjâitu; Alexandru Zaharescu

An irreducibility criterion for polynomials in several variables

Acta Mathematica Universitatis Ostraviensis, Vol. 12 (2004), No. 1, 13--18

Persistent URL: http://dml.cz/dmlcz/120599

An irreducibility criterion for polynomials in several variables

Marius Cavachi, Marian Vâjâitu and Alexandru Zaharescu

Abstract. For any field K and any polynomial F in two variables T, X over K denote by $\deg_X F$ and $\deg_T F$ the degree of F as a polynomial in X and respectively as a polynomial in T. Write any $F \in K(T)[X]$ in the form

$$F = \frac{a_0 + a_1X + \cdots + a_dX^d}{q},$$

with $a_0, a_1, \ldots, a_d, q \in K[T]$, $a_d \neq 0$ and q relatively prime with the greatest common divisor of $a_0, \ldots, a_d$. Then set

$$H(F) = \max\{\deg_T a_0, \ldots, \deg_T a_d, \deg_T q\}.$$

We show that for any relatively prime polynomials $f, g \in K(T)[X]$ with $\deg_X f < d = \deg_X g$, and any irreducible polynomial $p \in K[T]$ with $\deg_T p - (d+1)H(f) - 3dH(g) > 0$, the polynomial $f + pg$ is irreducible over $K(T)$.

1. Introduction

In [1], [3], [4] some results related to Hilbert's irreducibility theorem have been provided. A class of irreducible polynomials over a number field K is obtained in [1] as follows. Let $f(X), g(X) \in K[X]$ be relatively prime and assume $\deg f < \deg g$. Then it is shown that there are only finitely many prime numbers p which remain prime in K, for which the polynomial $f(X) + pg(X)$ is reducible. An improved version of this result has been obtained in [2], where explicit bounds for p in terms of K, $f(X)$ and $g(X)$ are provided, which ensure the irreducibility of the polynomial $f(X) + pg(X)$. In the present paper we obtain an irreducibility criterion for polynomials in n variables over an arbitrary field K. As we shall se below, the result follows immediately from the case $n = 2$. In this case we denote the variables by T and X. We also denote by $\deg_T f$ and $\deg_X g$ the degree of f as

Received: April 25, 2003.
2000 *Mathematics Subject Classification:* 11C08.
Key words and phrases: polynomials in several variables, irreducibility criterion.

a polynomial in T and respectively the degree of g as a polynomial in X, for any $f \in K[T]$ and any $g \in K(T)[X]$. For any $F \in K(T)[X]$, we write F in the form

$$F = \frac{a_0 + a_1 X + \cdots + a_d X^d}{q}, \tag{1}$$

with $a_0, a_1, \ldots, a_d, q \in K[T]$, $a_d \neq 0$ and q relatively prime with the greatest common divisor of $a_0, \ldots, a_d$. We then set

$$H(F) = \max\{\deg_T a_0, \ldots, \deg_T a_d, \deg_T q\}. \tag{2}$$

We will prove the following result.

Theorem 1. *Let K be a field and let $g \in K(T)[X]$ with $\deg_X g = d$. For any polynomial $p \in K[T]$, irreducible over K, and any $f \in K(T)[X]$ such that $\deg_X f < d$, f relatively prime with g in $K(T)[X]$ and $\deg_T p - (d+1)H(f) - 3dH(g) > 0$, the polynomial $f + pg$ is irreducible over $K(T)$.*

Corollary 1. *Let K be a field and let $g \in K(T)[X]$ with $\deg_X g = d$ and g irreducible over $K(T)$. For any polynomial $p \in K[T]$, irreducible over K, and any $f \in K(T)[X]$ such that $\deg_X f < d$ and $\deg_T p - (d+1)H(f) - 3dH(g) > 0$, the polynomial $f + pg$ is irreducible over $K(T)$.*

Theorem 1 above also implies an irreducibility result for polynomials in n variables $X_1, \ldots, X_n$ over K. For any $f \in K[X_1, \ldots, X_n]$ and any $j \in \{1, \ldots, n\}$ denote by $\deg_{X_j} f$ the degree of f as a polynomial in X_j. For any

$$F \in K(X_1, \ldots, X_{n-1})[X_n],$$

write F in the form

$$F = \frac{a_0 + a_1 X_n + \cdots + a_d X_n^d}{q},$$

with $a_0, a_1, \ldots, a_d, q \in K[X_1, \ldots, X_{n-1}]$, $a_d \neq 0$ and q relatively prime with the greatest common divisor of $a_0, \ldots, a_d$. For any $1 \leq j < n$, set

$$H_j(F) = \max\{\deg_{X_j} a_0, \ldots, \deg_{X_j} a_d, \deg_{X_j} q\}.$$

Then one has the following result.

Corollary 2. *Let K be a field, $n \geq 2$ and $g \in K(X_1, \ldots, X_{n-1})[X_n]$ with $\deg_{X_n} g = d$. For any polynomial $p \in K[X_1, \ldots, X_{n-1}]$, irreducible over K, and any f in $K(X_1, \ldots, X_{n-1})[X_n]$ such that $\deg_{X_n} f < d$, f relatively prime with g in $K(X_1, \ldots, X_{n-1})[X_n]$ and*

$$\max_{1 \leq j \leq n-1} \{\deg_{X_j} p - (d+1)H_j(f) - 3dH_j(g)\} > 0,$$

the polynomial $f + pg$ is irreducible over $K(X_1, \ldots, X_{n-1})$.

If j is the index for which the bound equality holds in the statement of Corollary 2, then one can let the new field $\hat{K}$ be the field generated by K and the variables $X_1, X_2, \ldots, X_{n-1}$ except for X_j. Writing T for X_j, and X for X_n, the polynomials f and g are now in $\hat{K}(T)[X]$, and p is an irreducible polynomial in $\hat{K}[T]$. Then Corollary 2 follows from Theorem 1.

In case g is irreducible, Corollary 2 reduces to Corollary 3 below.

Corollary 3. *Let K be a field, $n \geq 2$ and $g \in K(X_1,\dots,X_{n-1})[X_n]$, with $\deg_{X_n} g = d$ and g irreducible over $K(X_1,\dots,X_{n-1})$. For any polynomial $p \in K[X_1,\dots,X_{n-1}]$, irreducible over field K, and any polynomial f in $K(X_1,\dots,X_{n-1})[X_n]$ such that $\deg_{X_n} f < d$ and*

$$\max_{1\leq j\leq n-1}\{\deg_{X_j} p - (d+1)H_j(f) - 3dH_j(g)\} > 0,$$

the polynomial $f + pg$ is irreducible over $K(X_1,\dots,X_{n-1})$.

The above results provide us with an easy way of producing irreducible polynomials in practice. We end this section with a couple of examples.

Let $K = \mathbb{Q}$ and $g = X^5 - TX$. Thus $d = 5$ and $H(g) = 1$. Next, choose $p = T^{100} + 4006T + 2003$. This is an Eisenstein polynomial relative to the prime number 2003, and so p is irreducible over $\mathbb{Q}$. Take now any $f \in \mathbb{Q}(T)[X]$ with $\deg_X f \leq 4$. The condition $\deg_T p - (d+1)H(f) - 3dH(g) > 0$ from the statement of Theorem 1 reduces in our case to the inequality $100 - 6H(f) - 15 > 0$, which is satisfied provided $H(f) \leq 14$. This is the same as saying that f has the form

$$f = \frac{a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4}{b}, \tag{3}$$

where a_0, a_1, a_2, a_3, a_4 and b are polynomials in T of degree ≤ 14 over $\mathbb{Q}$. Let us assume that f has this form. If now $a_0 = 0$, then $f + pg$ is not irreducible over $\mathbb{Q}(T)$, being divisible by X. Similarly, if $a_1 = a_2 = a_3 = 0$ and $a_0 = -Ta_4$, then $f + pg$ is not irreducible over $\mathbb{Q}(T)$, being divisible by $X^4 - T$. In any other case, $f + pg$ is irreducible over $\mathbb{Q}(T)$ by Theorem 1.

For a second example, let $K = \mathbb{Q}$, and set $g = X^5 - T$. Thus $d = 5$ and $H(g) = 1$ as before. If we again choose $p = T^{100} + 4006T + 2003$, we end up with the same inequality $H(f) \leq 14$. Since in this example g is irreducible over $\mathbb{Q}(T)$, Corollary 1 shows that for any f of the form (3), with a_0, a_1, a_2, a_3, a_4 and b polynomials in T of degree ≤ 14 over $\mathbb{Q}$, $f + pg$ is irreducible over $\mathbb{Q}(T)$.

2. Proof of Theorem 1

Let K, g, f and p be as in the statement of the theorem. We start by putting f, g and $f + pg$ in the form

$$f = \frac{a_0 + a_1X + \cdots + a_{d-1}X^{d-1}}{q_2}, \tag{4}$$

$$g = \frac{b_0 + b_1X + \cdots + b_dX^d}{q_1} \tag{5}$$

and

$$f + pg = \frac{u_0 + u_1X + \cdots + u_dX^d}{q}, \tag{6}$$

with $a_0, \dots, a_{d-1} \in K[T]$ not all zero, $b_0, \dots, b_d, u_0, \dots, u_d, q, q_1, q_2 \in K[T]$, $b_d \neq 0$, and such that q_1 is relatively prime with $g.c.d.(b_0, \dots, b_d)$, q_2 is relatively prime with $g.c.d.(a_0, \dots, a_{d-1})$ and q is relatively prime with $g.c.d.(u_0, \dots, u_d)$. One has

$$\deg_T q \leq \deg_T q_1 + \deg_T q_2 \leq H(f) + H(g). \tag{7}$$

Note also that

$$u_d = \frac{qpb_d}{q_1} \neq 0. \tag{8}$$

Let us denote $F = u_0+u_1X+\cdots+u_dX^d = q(f+pg)$ and $G = b_0+b_1X+\cdots+b_dX^d = q_1g$. We need to show that F is irreducible over the field $K(T)$. Let us assume that F is reducible over $K(T)$. Then one has a factorization

$$F = F_1F_2 \tag{9}$$

where $F_1 = s_0+s_1X+\cdots+s_mX^m$, $F_2 = v_0+v_1X+\cdots+v_rX^r$, $s_0,\ldots,s_m,v_0,\ldots,v_r \in K[T]$, $s_m \neq 0, v_r \neq 0$.

Note that $s_mv_r = u_d$, and from (8) one obtains an equality in $K[T]$,

$$q_1s_mv_r = qpb_d \neq 0. \tag{10}$$

By our assumption on p, one has that $\deg_T q_1 \leq H(g) < \deg_T p$, so p does not divide q_1 in the ring $K[T]$. Since p is a prime element of $K[T]$, it follows that p divides s_m or p divides v_r. To make a choice, let us assume that p divides s_m, and let $z \in K[T]$ be such that $s_m = pz$. Then

$$q_1zv_r = qb_d. \tag{11}$$

As a consequence of (11), note that

$$\deg_T v_r \leq \deg_T q + \deg_T b_d. \tag{12}$$

By combining (7) with (12) we see that

$$\deg_T v_r \leq H(f) + 2H(g). \tag{13}$$

Recall that G and F_2 are polynomials in X with coefficients in $K[T]$. We consider the resultant $R(G,F_2)$ of G and F_2. Since f is relatively prime with g, it follows that G is relatively prime with F_2, and hence $R(G,F_2)$ is a nonzero element of $K[T]$.

At this point we fix a real number $0 < \rho < 1$, and consider the nonarchimedean absolute value $|\cdot|$ on $K[T]$ given by

$$|F| = \rho^{-\deg_T F}, \tag{14}$$

for any $F \in K[T]$. The absolute value $|\cdot|$ is extended to $K(T)$ by multiplicativity. Thus for any $L \in K(T)$, $L = \frac{F}{G}$, with $F, G \in K[T]$, $G \neq 0$, we have $|L| = \frac{|F|}{|G|}$. Note that $|z| \geq 1$ for any $0 \neq z \in K[T]$. In particular one has

$$|R(G,F_2)| \geq 1. \tag{15}$$

Let us choose an extension of $|\cdot|$ to a fixed algebraic closure $\overline{K(T)}$ of $K(T)$, and denote it also by $|\cdot|$. Next, we estimate $|R(G,F_2)|$ in a different way. We factor G and F_2 over $\overline{K(T)}$,

$$G = b_d(X_n - \eta_1)\cdots(X_n - \eta_d), \tag{16}$$

and

$$F_2 = v_r(X_n - \theta_1)\cdots(X_n - \theta_r), \tag{17}$$

with $\eta_1,\ldots,\eta_d,\theta_1,\ldots,\theta_r \in \overline{K(T)}$. We have

$$R(G,F_2) = b_d^r v_r^d \prod_{1\leq i\leq d}\prod_{1\leq j\leq r}(\eta_i - \theta_j) = v_r^d(-1)^{d}r \prod_{1\leq j\leq r} G(\theta_j). \tag{18}$$

For any $j \in \{1, \ldots, r\}$, θ_j is a root of F_2, and hence it is also a root of F. Therefore

$$g(\theta_j) = -\frac{f(\theta_j)}{p}. \tag{19}$$

It follows that

$$|G(\theta_j)| = |q_1 g(\theta_j)| = \frac{|q_1||f(\theta_j)|}{|p|}. \tag{20}$$

Since $\deg_T q_1 \leq H(g)$, we see that

$$|q_1| \leq \rho^{-H(g)}. \tag{21}$$

Using (21) in (20), we obtain

$$|G(\theta_j)| \leq \frac{|f(\theta_j)|}{|p|}\rho^{-H(g)}. \tag{22}$$

By (18) and (22) we find that

$$|R(G, F_2)| \leq \frac{|v_r|^d \rho^{-rH(g)}}{|p|^r} \prod_{1\leq j\leq r} |f(\theta_j)|. \tag{23}$$

The inequality (13) implies that

$$|v_r| \leq \rho^{-(H(f)+2H(g))}. \tag{24}$$

Inserting (24) in (23) one has

$$|R(G, F_2)| \leq |p|^{-r}\rho^{-dH(f)-(2d+r)H(g)} \prod_{1\leq j\leq r} |f(\theta_j)|. \tag{25}$$

For $|f(\theta_j)|$ we use the upper bound

$$\begin{aligned} |f(\theta_j)| &= \Big|\frac{a_0 + a_1\theta_j + \cdots + a_{d-1}\theta_j^{d-1}}{q_2}\Big| \leq \frac{\max_{0\leq i\leq d-1} |a_i\theta_j^i|}{|q_2|} \\ &\leq \Big(\max_{0\leq i\leq d-1} |a_i|\Big) \max\{1, |\theta_j|^{d-1}\} \leq \rho^{-H(f)} \max\{1, |\theta_j|\}^{d-1}. \end{aligned} \tag{26}$$

Note also that the equality

$$0 = f(\theta_j) + pg(\theta_j) = \frac{pb_d\theta_j^d}{q_1} + \Big(\frac{a_{d-1}}{q_2} + \frac{pb_{d-1}}{q_1}\Big)\theta_j^{d-1} + \cdots + \Big(\frac{a_0}{q_2} + \frac{pb_0}{q_1}\Big)$$

implies

$$\begin{aligned} |p||\theta_j|^d \leq |pb_d\theta_j^d| &\leq \max\Big\{\Big|\frac{q_1 a_{d-1}\theta_j^{d-1}}{q_2}\Big|, |pb_{d-1}\theta_j^{d-1}|, \ldots, \Big|\frac{q_1 a_0}{q_2}\Big|, |pb_0|\Big\} \\ &\leq \max\{1, |\theta_j|^{d-1}\} \max\{|q_1 a_{d-1}|, |pb_{d-1}|, \ldots, |q_1 a_0|, |pb_d|\} \\ &\leq \max\{1, |\theta_j|^{d-1}\}\rho^{-H(g)} \max\{|p|, \rho^{-H(f)}\}. \end{aligned} \tag{27}$$

By the assumption from the statement of the theorem it is clear that

$$|p| \geq \rho^{-H(f)}. \tag{28}$$

By (27) and (28) we find that

$$|\theta_j|^d \leq \max\{1, |\theta_j|^{d-1}\}\rho^{-H(g)}.$$

Here we either have $|\theta_j| \leq 1$, or, if not, then

$$|\theta_j|^d \leq |\theta_j|^{d-1} \rho^{-H(g)}.$$

In both cases, one has

$$|\theta_j| \leq \rho^{-H(g)}, \tag{29}$$

for any $1 \leq j \leq r$. By combining (26) with (29) we derive

$$|f(\theta_j)| \leq \rho^{-H(f)-(d-1)H(g)}, \tag{30}$$

for $1 \leq j \leq r$. Using (30) in (25) we obtain

$$|R(G, F_2)| \leq |p|^{-r} \rho^{-(d+r)H(f)-d(r+2)H(g)}. \tag{31}$$

By comparing (31) with (15), we deduce that

$$|p| \leq \rho^{-\left(\frac{d}{r}+1\right)H(f)-d\left(1+\frac{2}{r}\right)H(g)} \leq \rho^{-(d+1)H(f)-3dH(g)}. \tag{32}$$

Since $|p| = \rho^{-\deg_T p}$, from (32) one obtains

$$\deg_T p \leq (d+1)H(f) + 3dH(g), \tag{33}$$

which contradicts the assumption from the statement of the theorem. In conclusion, F is irreducible over $K(T)$, and this completes the proof of the theorem.

Acknowledgement. The authors are grateful to the referee for very useful comments and suggestions.

References

[1] CAVACHI M. *On a special case of Hilbert's irreducibility theorem*, J. Number Theory **82** (2000), no. 1, 96-99.

[2] CAVACHI M., VÂJÂITU M. and ZAHARESCU A. *A class of irreducible polynomials*, J. Ramanujan Math. Soc. **17** (2002), no. 3, 161-172.

[3] FRIED M. *On Hilbert's irreducibility theorem*, J.Number Theory **6** (1974), 211-231.

[4] LANGMANN M. *Der Hilbertsche Irreduzibilitatssatz und Primzahlfragen*, J. Reine Angew. Math. **413** (1991), 213-219.

Author(s) Address(es):

M. Cavachi, Faculty of Mathematics, "Ovidius" University of Constanta, Bd. Mamaia 124, 8700 Constanta, Romania.

M. Vâjâitu, Institute of Mathematics of the Romanian Academy, P. O. Box 1-764, Bucharest 70700, Romania

E-mail address: mvajaitu@stoilow.imar.ro

A. Zaharescu, Department of Mathematics, University of Illinois at Urbana-Champaign, Altgeld Hall, 1409 W. Green Street, Urbana, IL, 61801, USA.

Institute of Mathematics of the Romanian Academy, P. O. Box 1-764, Bucharest 70700, Romania.

E-mail address: zaharesc@math.uiuc.edu