Marius Cavachi; Marian Vâjâitu; Alexandru Zaharescu
An irreducibility criterion for polynomials in several variables


Persistent URL: [http://dml.cz/dmlcz/120599](http://dml.cz/dmlcz/120599)

Terms of use:

© University of Ostrava, 2004

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* [http://project.dml.cz](http://project.dml.cz)
An irreducibility criterion for polynomials in several variables

Marius Cavachi, Marian Văjâitu and Alexandru Zaharescu

Abstract. For any field $K$ and any polynomial $F$ in two variables $T$, $X$ over $K$ denote by $\deg_T F$ and $\deg_X F$ 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

$$F = a_0 + a_1 X + \cdots + a_d X^d,$$

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 see 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

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

(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

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

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 $K$. 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 $\deg_{X_j}$ 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 $\deg_{X_j} f < d$, $f$ 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 $\tilde{K}$ be the field generated by $K$ and the variables $X_1, X_2, \ldots, X_n$ except for $X_j$. Writing $T$ for $X_j$, and $X$ for $X_n$, the polynomials $f$ and $g$ are now in $K(T)[X]$, and $p$ is an irreducible polynomial in $K[T]$. Then Corollary 2 follows from Theorem 1.

In case $g$ is irreducible, Corollary 2 reduces to Corollary 3 below.
An irreducibility criterion for polynomials in several variables

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

$$\max_{1 \leq i \leq n-1} \{\deg_{X_i} p - (d+1)H(f) - 3dH(g)\} > 0,$$

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

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 $g = X_5 - 5X$. 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 $\deg_T f \leq 4$. 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 $H(f) < 14$. This is the same as saying that $f$ has the form

$$f = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4,$$

where $a_0, a_1, a_2, a_3, a_4$ and $b$ are polynomials in $T$ of degree $\leq 14$ 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 $a_0 = -T a_4$, 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 $g = X^5 - 5$. 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 $\leq 14$ 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

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

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

and

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

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

$$\deg_T q \leq \deg_T q_1 + \deg_T q_2 \leq H(f) + H(g).$$
Note also that
\[ u_d = \frac{q b_d}{q_1} \neq 0. \quad (8) \]
Let us denote
\[ F = u_0 + u_1 X + \cdots + u_d X^d = q(f + pg) \]
and
\[ G = b_0 + b_1 X + \cdots + b_d X^d = q_1 g. \]
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
\[ F = F_1 F_2 \quad (9) \]
where
\[ F_1 = s_0 + s_1 X + \cdots + s_m X^m, \quad F_2 = v_0 + v_1 X + \cdots + v_r X^r, \quad s_0, \ldots, s_m, v_0, \ldots, v_r \in K[T], \]
and \( s_m \neq 0, v_r \neq 0 \).

Note that \( s_m v_r = u_d \), and from (8) one obtains an equality in \( K[T] \),
\[ q_1 s_m v_r = q b_d \neq 0. \quad (10) \]

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 \( s_m = p z \).

Then
\[ q_1 z v_r = q b_d. \quad (11) \]

As a consequence of (11), note that
\[ \deg_T v_r \leq \deg_T q + \deg_T b_d. \quad (12) \]

By combining (7) with (12) we see that
\[ \deg_T v_r \leq H(f) + 2H(g). \quad (13) \]

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
\[ |F| = \rho^{-\deg F}, \]
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 \( |L| = \left| \frac{f}{g} \right| \). Note that \( |z| \geq 1 \) for any \( 0 \neq z \in K[T] \). In particular one has
\[ |R(G, F_2)| \geq 1. \quad (15) \]

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 \( \overline{K(T)} \),
\[ G = b_d (X_n - \eta_1) \cdots (X_n - \eta_k), \quad (16) \]
and
\[ F_2 = v_r (X_n - \theta_1) \cdots (X_n - \theta_t), \quad (17) \]
with \( \eta_1, \ldots, \eta_k, \theta_1, \ldots, \theta_t \in \overline{K(T)} \). We have
\[ R(G, F_2) = b_d v_r \prod_{1 \leq d \leq m} \prod_{1 \leq r \leq r^*} (\eta_i - \theta_j) = v_r^d (-1)^d \prod_{1 \leq r \leq r^*} G(\theta_j). \quad (18) \]
For any \( j \in \{1, \ldots, r\} \), \( \theta_j \) is a root of \( F_2 \), and hence it is also a root of \( F \). Therefore
\[
g(\theta_j) = -\frac{f(\theta_j)}{p}.
\]
It follows that
\[
|G(\theta_j)| = |q_j g(\theta_j)| = \frac{|q_j||f(\theta_j)|}{|p|}.
\]
Since \( \deg q_j \leq H(g) \), we see that
\[
|q_j| \leq \rho^{-H(g)}.
\]
Using (21) in (20), we obtain
\[
|G(\theta_j)| \leq \frac{|f(\theta_j)|}{|p|}\rho^{-H(g)}.
\]
By (18) and (22) we find that
\[
|R(G, F)| \leq \frac{|v_j|\rho^{-H(g)}}{|p|^r} \prod_{1 \leq j \leq r} |f(\theta_j)|.
\]
The inequality (13) implies that
\[
|v_j| \leq \rho^{-(H(f) + 2H(g))}.
\]
Inserting (24) in (23) one has
\[
|R(G, F)| \leq |p|^{-r} \rho^{-AH(g)} \prod_{1 \leq j \leq r} |f(\theta_j)|.
\]
For \( |f(\theta_j)| \) we use the upper bound
\[
|f(\theta_j)| = \left| \frac{a_0 + a_1 \theta_j + \cdots + a_{d-1} \theta_j^{d-1}}{q_2} \right| \leq \max_{0 \leq \ell \leq d-1} |a_{\ell}| |q_2|^{-\ell}.
\]
Note also that the equality
\[
0 = f(\theta_j) + p g(\theta_j) = \frac{pb \theta_j^d}{q_1} + \left( \frac{a_{d-1} \theta_j^{d-1}}{q_2} + \frac{pb_{d-1}}{q_1} \theta_j^{d-1} + \cdots + \left( \frac{a_0}{q_2} + \frac{pb_0}{q_1} \right) \right)
\]
implies
\[
|\theta_j|^d \leq \max \left\{ \frac{q_0 a_0 \theta_j^{d-1}}{q_2}, \frac{qa_0 \theta_j^{d-1}}{q_2}, \cdots, \frac{q_{d-1} a_0}{q_2}, |pb_0| \right\} \leq \max \{1, |\theta_j|^{d-1} \} \max \{|q_0 a_0|, |pq_2 q_{d-1} a_0|, \cdots, |q_{d-1} a_{d-1}|, |pb_0| \} \leq \max \{1, |\theta_j|^{d-1} \} \rho^{-H(g)} \max \{|p|, \rho^{-H(f)}\}.
\]
By the assumption from the statement of the theorem it is clear that
\[
|p| \geq \rho^{-H(f)}.
\]
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

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

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

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

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

$$|R(G, F_j)| \leq |p| + \rho^{-d+H(f)-d(r+1)H(g)}.$$  

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

$$|p| \leq \rho^{-((d+1)H(f)-d(1+\gamma)H(g))} \leq \rho^{-d+H(f)-3dH(g)}.$$  

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

$$deg(p) \leq (d+1)H(f) + 3dH(g),$$  

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