ACTA ARITHMETICA
123.4 (2006)

Some classes of irreducible polynomials

by

ANCA IULIANA BONCIOCAT and
NICOLAE CIPRIAN BONCIOCAT (Bucureşti)

1. Introduction. Lipka [10] obtained some irreducibility criteria for integer polynomials of the form $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0p^k$ with $a_0a_n \neq 0$, p a prime number and k a positive integer. For instance, he proved that *for fixed* $p, a_0, a_1, \ldots, a_n$ *with* $a_0a_1a_n \neq 0$, f *is irreducible over* $\mathbb{Q}$ *for all but finitely many positive integers* k.

Another criterion proved in [10] is that *given integers* $a_0, a_1, \ldots, a_n$ *with* $a_0a_n \neq 0$, *the polynomial* $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0p$ *is irreducible over* $\mathbb{Q}$ *for all but finitely many prime numbers* p, this result being a consequence of a theorem of Ore [14, Th. 5, p. 151].

These results can be formulated equivalently as in the earlier paper of Weisner [23]:

If a polynomial $f(X) \in \mathbb{Z}[X]$ *has a simple rational root, then for a fixed integer* $c \neq 0$ *and a fixed prime number* p, *the polynomial* $f(X) + cp^k$ *is irreducible over* $\mathbb{Q}$ *for all but finitely many positive integers* k.

If $f(X) \in \mathbb{Z}[X]$ *has a rational root and* $c \neq 0$ *is a fixed integer, then* $f(X) + cp$ *is irreducible over* $\mathbb{Q}$ *for all but finitely many prime numbers* p.

Inspired by some results of Fried [6] and Langmann [7] in connection with Hilbert's irreducibility theorem, Cavachi [2] studied the irreducibility of polynomials of the form $f(X)+pg(X)$ with p prime and f, g relatively prime, and proved that for any relatively prime $f, g \in \mathbb{Q}[X]$ with $\deg f < \deg g$, the polynomial $f(X) + pg(X)$ is irreducible over $\mathbb{Q}$ for all but finitely many prime numbers p. In [3] this result was strengthened, by providing an explicit bound α depending on f and g such that for all primes $p > \alpha$ the polynomial $f(X) + pg(X)$ is irreducible over $\mathbb{Q}$. Explicit upper bounds for the number of factors over $\mathbb{Q}$ of a linear combination $n_1f(X) + n_2g(X)$, in particular irreducibility criteria covering also the case $\deg f = \deg g$, have been derived

2000 *Mathematics Subject Classification*: Primary 11C08, 11R09.

Work partially supported by the CERES Program 4-147/2004 of the Romanian Ministry of Education and Research.

in [1]. Similar irreducibility criteria have also been obtained for polynomials in several variables over a given field. More specifically, the following result has been proved in [4].

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 is relatively prime to 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 $K(X_1, \ldots, X_{n-1})$.

Here, for any polynomial $F \in K(X_1, \ldots, X_{n-1})[X_n]$, written in the form $F = (a_0 + a_1 X_n + \cdots + a_d X_n^d)/q$, with $a_0, a_1, \ldots, a_d, q \in K[X_1, \ldots, X_{n-1}]$, $a_d \neq 0$, q relatively prime to $\gcd(a_0, \ldots, a_d)$, and for any index j with $1 \leq j < n$, $H_j(F)$ stands for $\max\{\deg_{X_j} a_0, \ldots, \deg_{X_j} a_d, \deg_{X_j} q\}$.

The problem of the reducibility of lacunary polynomials has been investigated by Schinzel in a series of papers including [15]–[21], and by Filaseta and Schinzel [5], H. W. Lenstra Jr. [8], [9] and Ljunggren [11]. For the study of lacunary polynomials over arbitrary fields, and over Kroneckerian fields, the reader is referred to Chapters 2 and 6, respectively, of Schinzel's book [22].

In this paper we first prove an irreducibility criterion for lacunary polynomials with integer coefficients, which is similar to the first result of Lipka mentioned above. Then, by using technics similar to those employed in [1], [4] and [10], we extend this criterion, as well as the first result of Lipka, to polynomials in several variables over a given field. Our proofs are effective, providing explicit conditions on the leading coefficient, which ensure the irreducibility of the polynomials considered. For lacunary polynomials with integer coefficients we prove the following results.

Theorem 1. *Let*

$$f(X) = a_0 + \cdots + a_{n-3}X^{n-3} + p^e a_{n-2}X^{n-2} + p^m a_n X^n \in \mathbb{Z}[X]$$

with $n \geq 3$, $a_0 a_{n-2} a_n \neq 0$ and p a prime number, $p \nmid a_{n-2}a_n$. If

$$p^m > |a_n a_{n-2}| p^{3e} + \sum_{i=3}^{n} |a_n^{i-1} a_{n-i}| p^{ie} \tag{1}$$

and $m \not\equiv e \bmod 2$, then f is irreducible over $\mathbb{Q}$.

Corollary 1. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 3$, having a rational root α/β of multiplicity 2. Let $c \neq 0$ be a fixed integer and p a prime number, $p \nmid c\beta$. Denote by e the multiplicity of p in the prime decomposition* *of* $\beta^{n-2}f''(\alpha/\beta)/2$. *If* $m \not\equiv e \bmod 2$ *and*

$$p^m > \sum_{i=2}^{n} |c|^{i-1}|\beta|^{i(n-2)} \frac{|f^{(i)}(\alpha/\beta)|}{i!} p^{ie},$$

then the polynomial $f(X) + cp^m$ *is irreducible over* $\mathbb{Q}$.

The irreducibility criteria for polynomials in several variables will be deduced from the following two results for polynomials in two variables X, Y over a field K.

Theorem 2. *Let* K *be a field*, $n \geq 2$ *a fixed integer*, *and let*

$$f(X,Y) = a_0 + a_1Y + \cdots + a_{n-2}Y^{n-2} + p^e a_{n-1}Y^{n-1} + p^m a_n Y^n \in K[X,Y]$$

with $a_0, \ldots, a_n, p \in K[X]$, $a_0a_{n-1}a_n \neq 0$, p *irreducible over* K *and* $p \nmid a_{n-1}a_n$. *If*

$$(2) \qquad m > ne + \frac{(n-1)\deg a_n + \max\{\deg a_0, \ldots, \deg a_{n-2}, \deg p^e a_{n-1}\}}{\deg p},$$

then f *is irreducible over* $K(X)$.

Theorem 3. *Let* K *be a field*, $n \geq 3$ *a fixed integer*, *and let*

$$f(X,Y) = a_0 + a_1Y + \cdots + a_{n-3}Y^{n-3} + p^e a_{n-2}Y^{n-2} + p^m a_n Y^n \in K[X,Y]$$

with $a_0, \ldots, a_{n-2}, a_n, p \in K[X]$, $a_0a_{n-2}a_n \neq 0$, p *irreducible over* K *and* $p \nmid a_{n-2}a_n$. *If* $m \not\equiv e \bmod 2$ *and*

$$(3) \qquad m > ne + \frac{(n-1)\deg a_n + \max\{\deg a_0, \ldots, \deg a_{n-3}, \deg p^e a_{n-2}\}}{\deg p},$$

then f *is irreducible over* $K(X)$.

Immediate consequences of Theorems 2 and 3 above are two irreducibility criteria for polynomials in $r \geq 2$ variables $X_1, \ldots, X_r$ over K. For any $f \in K[X_1, \ldots, X_r]$ and any $j \in \{1, \ldots, r\}$ we denote by $\deg_j f$ the degree of f as a polynomial in X_j with coefficients in $K[X_1, \ldots, \widehat{X}_j, \ldots, X_r]$, where the hat denotes omission of the corresponding variable. With this notation, one has the following results, obtained by writing Y for X_r and X for a suitable X_j, and by replacing the field K with the field $K(X_1, \ldots, \widehat{X}_j, \ldots, X_{r-1})$ of rational functions.

Corollary 2. *Let* K *be a field*, *fix integers* $n, r \geq 2$, *and let*

$$f(X_1, \ldots, X_r) = a_0 + a_1X_r + \cdots + a_{n-2}X_r^{n-2} + p^e a_{n-1}X_r^{n-1} + p^m a_n X_r^n$$

with $a_0, \ldots, a_n, p \in K[X_1, \ldots, X_{r-1}]$, $a_0a_{n-1}a_n \neq 0$ *and* $p \nmid a_{n-1}a_n$. *Assume that for some* $j \in \{1, \ldots, r-1\}$, p *as a polynomial in* X_j *is irreducible over*

$K(X_1,\dots,\widehat{X}_j,\dots,X_{r-1})$. If

$$m > ne + \frac{(n-1)\deg_j a_n + \max\{\deg_j a_0,\dots,\deg_j a_{n-2},\deg_j p^e a_{n-1}\}}{\deg_j p},$$

then f is irreducible over $K(X_1,\dots,X_{r-1})$.

COROLLARY 3. *Let K be a field, fix integers $n \geq 3$, $r \geq 2$, and let*

$$f(X_1,\dots,X_r) = a_0 + a_1X_r + \cdots + a_{n-3}X_r^{n-3} + p^e a_{n-2}X_r^{n-2} + p^m a_n X_r^n$$

with $a_0,\dots,a_{n-2},a_n,p \in K[X_1,\dots,X_{r-1}]$, $a_0a_{n-2}a_n \neq 0$ and $p \nmid a_{n-2}a_n$. Assume that for some $j \in \{1,\dots,r-1\}$, p as a polynomial in X_j is irreducible over $K(X_1,\dots,\widehat{X}_j,\dots,X_{r-1})$. If $m \not\equiv e \bmod 2$ and

$$m > ne + \frac{(n-1)\deg_j a_n + \max\{\deg_j a_0,\dots,\deg_j a_{n-3},\deg_j p^e a_{n-2}\}}{\deg_j p},$$

then f is irreducible over $K(X_1,\dots,X_{r-1})$.

In the last section of the paper we give a couple of applications of Corollaries 2 and 3, which are in some sense analogous to the first result of Weisner mentioned above, and to Corollary 1, respectively. The proofs of the main results are presented in Sections 2 and 3 below.

2. Proof of Theorem 1. Assume by contradiction that f decomposes as $f(X) = f_1(X)\cdot f_2(X)$ with

$$f_1(X) = b_0 + b_1X + \cdots + b_{j-1}X^{j-1} + p^d b_j X^j,$$
$$f_2(X) = c_0 + c_1X + \cdots + c_{k-1}X^{k-1} + p^{m-d} c_k X^k,$$

where $d \geq 0$, $j,k \geq 1$, $j+k=n$, $b_0,\dots,b_j,c_0,\dots,c_k \in \mathbb{Z}$, $b_jc_k = a_n$, and $b_0c_0 = a_0$. One may obviously assume that

$$d \leq m-d. \tag{4}$$

Let us further assume that $j,k \geq 2$. Equating the coefficients in the equality $f(X) = f_1(X)\cdot f_2(X)$, we obtain

$$p^d b_j c_{k-1} + p^{m-d} b_{j-1} c_k = 0, \tag{5}$$

$$p^d b_j c_{k-2} + b_{j-1}c_{k-1} + p^{m-d} b_{j-2} c_k = p^e a_{n-2}. \tag{6}$$

Let $b_{j-1} = p^{n_1}g_1$ and $c_{k-1} = p^{n_2}g_2$ with $n_1,n_2 \geq 0$ and $p \nmid g_1g_2$. By (5) we then find

$$d + n_2 = m - d + n_1,$$

so (6) becomes

$$p^d b_j c_{k-2} + p^{m-2d+2n_1} g_1 g_2 + p^{m-d} b_{j-2} c_k = p^e a_{n-2}. \tag{7}$$

If we now assume that $e < d$, it follows by (4) and (7) that we must have $e = m - 2d + 2n_1$, which contradicts the fact that $m \not\equiv e \bmod 2$. Therefore,

$e \geq d$, and one may easily check that this conclusion still holds for $j = 1$ or $k = 1$. Consider now the factorizations of f and f_1, say

$$f(X) = p^m a_n (X - \xi_1) \cdots (X - \xi_n),$$
$$f_1(X) = p^d b_j (X - \xi_1) \cdots (X - \xi_j),$$

with $\xi_1, \ldots, \xi_n \in \mathbb{C}$. It is well known that if the leading coefficient of a complex polynomial $F(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n$ satisfies the inequality $|\alpha_n| > |\alpha_{n-1}| + |\alpha_{n-2}| + \cdots + |\alpha_0|$, then all the roots of F lie in the disk $|z| < 1$. Let us now fix an arbitrarily chosen real $\delta \geq 1$ and assume that

$$|p^m a_n| > \delta^2 |p^e a_{n-2}| + \delta^3 |a_{n-3}| + \cdots + \delta^n |a_0|. \tag{8}$$

Then all the roots of $f(X/\delta)$ will lie in the disk $|z| < 1$, so for any $i \in \{1, \ldots, n\}$ one must have $|\xi_i| < 1/\delta$, and therefore

$$|\xi_1 \cdots \xi_j| < \frac{1}{\delta^j}. \tag{9}$$

On the other hand, $b_0 \neq 0$ and hence $|b_0| \geq 1$, and since $b_j \mid a_n$ and $d \leq e$, we must have

$$|\xi_1 \cdots \xi_j| = \left| \frac{b_0}{p^d b_j} \right| \geq \frac{1}{p^e |a_n|}. \tag{10}$$

In view of (9) and (10), to reach a contradiction we will choose δ satisfying

$$\frac{1}{p^e |a_n|} \geq \frac{1}{\delta^j}. \tag{11}$$

Since $j \geq 1$, instead of (11) it will be sufficient to have $\delta \geq p^e |a_n|$. A suitable candidate for δ is therefore $p^e |a_n|$, so one derives the desired contradiction for all integers $m \not\equiv e \bmod 2$ satisfying

$$p^m > |a_n a_{n-2}| p^{3e} + \sum_{i=3}^{n} |a_n^{i-1} a_{n-i}| p^{ie},$$

which completes the proof. ■

For the proof of Corollary 1, we first use the fact that $f(X) + cp^m$ is irreducible over $\mathbb{Q}$ if and only if $f(X + \alpha/\beta) + cp^m$ is. It will therefore be sufficient to test the irreducibility of $\beta^{n-2}[f(X + \alpha/\beta) + cp^m]$. Since by our assumption $f(\alpha/\beta) = f'(\alpha/\beta) = 0$ and $f''(\alpha/\beta) \neq 0$, we have

$$\beta^{n-2}\left[f\left(X + \frac{\alpha}{\beta}\right) + cp^m\right] = p^m c \beta^{n-2} + p^e \, \frac{\beta^{n-2} f''(\alpha/\beta)}{2! p^e} \, X^2 + \sum_{i=3}^{n} \frac{\beta^{n-2} f^{(i)}(\alpha/\beta)}{i!} \, X^i.$$

If we now replace f by $X^{\deg f} \cdot f(1/X)$ in Theorem 1, we see that a polynomial of the form $f(X) = p^m a_0 + p^e a_2 X^2 + a_3 X^3 + \cdots + a_n X^n$ with $n \geq 3$,

$a_0a_2a_n \neq 0$ and p a prime number, $p \nmid a_0a_2$, must be irreducible over $\mathbb{Q}$ if $m \not\equiv e \bmod 2$ and

$$p^m > |a_0a_2|p^{3e} + \sum_{i=3}^{n} |a_0^{i-1}a_i|p^{ie}. \tag{12}$$

The conclusion follows by applying (12) to $\beta^{n-2}[f(X+\alpha/\beta)+cp^m]$. ∎

Remarks. 1. Without our assumption that $m \not\equiv e \bmod 2$, the conclusion of Theorem 1 may be false, as seen from the following example. Take an integer $k > 1$ and let $f_k(X) = 2^{2k}X^4 + (2^{k+1}-1)X^2 + 1$. Here we have $p = 2$, $m = 2k$, $e = 0$, and hence $m \equiv e \bmod 2$. Although condition (1) is fulfilled, being equivalent to $2^{2k} > 2^{k+1}$, our polynomials f_k are all reducible over $\mathbb{Q}$, since

$$2^{2k}X^4 + (2^{k+1}-1)X^2 + 1 = (2^kX^2 + X + 1)(2^kX^2 - X + 1).$$

2. Some additional information on the coefficients of f may allow one to obtain sharper bounds than those exhibited in Theorem 1, by searching for sharper estimates for the moduli of the roots of f. Such estimates may be obtained by using ideas of Mignotte [12] and Mignotte and Ştefănescu [13]. However, our assumption on the size of p^m is in some cases best possible, in the sense that there exist polynomials for which equality in (1) holds and $m \not\equiv e \bmod 2$, and which are reducible over $\mathbb{Q}$. To see this, take $k \geq 2$ and let

$$f_k(X) = 1 + X + X^2 + \cdots + X^{2k-4} + 2X^{2k-3} - 2^{2k}X^{2k-1}.$$

Here $p = 2$, $m = 2k$, $e = 1$, and hence $m \not\equiv e \bmod 2$. On the other hand we have equality in (1), since $2^{2k} = 2^3 + \sum_{i=3}^{2k-1} 2^i$, and f_k is reducible over $\mathbb{Q}$, since $f_k(1/2) = 0$.

3. Note that once we fix the integers $a_0, \ldots, a_{n-2}, a_n, m, e$ such that $a_0a_{n-2}a_n \neq 0$, $m \not\equiv e \bmod 2$ and $m > ne$, the inequality (1) will hold for all but finitely many prime numbers p.

3. Proof of Theorems 2 and 3. Let $a_0, \ldots, a_n, p$ be as in the statement of Theorem 2, and assume by contradiction that $f(X,Y) = f_1(X,Y) \cdot f_2(X,Y)$ with

$$f_1(X,Y) = b_0 + b_1Y + \cdots + b_{j-1}Y^{j-1} + p^d b_jY^j,$$
$$f_2(X,Y) = c_0 + c_1Y + \cdots + c_{k-1}Y^{k-1} + p^{m-d} c_kY^k,$$

where $d \geq 0$, $j, k \geq 1$, $j + k = n$, $b_0, \ldots, b_j, c_0, \ldots, c_k \in K[X]$, $b_jc_k = a_n$ and $b_0c_0 = a_0$. One may obviously assume that

$$d \leq m - d. \tag{13}$$

Equating the coefficients, we find that $p^e a_{n-1} = p^d b_jc_{k-1} + p^{m-d} b_{j-1}c_k$, so in view of (13) we must have $e \geq d$.

We now introduce a nonarchimedean absolute value $|\cdot|$ on $K(X)$ as follows. We fix a real number $\varrho > 1$, and for any $F(X) \in K[X]$ we define

$$|F(X)| = \varrho^{\deg F(X)}.$$

We then extend $|\cdot|$ to $K(X)$ by multiplicativity. Thus for any $H(X) = F(X)/G(X)$ with $F(X), G(X) \in K[X]$, $G(X) \neq 0$, we let $|H(X)| = |F(X)|/|G(X)|$. Note that for any non-zero element u of $K[X]$ one has $|u| \geq 1$. Let then $\overline{K(X)}$ be a fixed algebraic closure of $K(X)$, and fix an extension of the absolute value $|\cdot|$ to $\overline{K(X)}$, which we will also denote by $|\cdot|$. Consider the factorizations of f and f_1, say

$$f(X,Y) = p^m a_n (Y-\xi_1)\cdots(Y-\xi_n),$$
$$f_1(X,Y) = p^d b_j (Y-\xi_1)\cdots(Y-\xi_j),$$

with $\xi_1, \ldots, \xi_n \in \overline{K(X)}$. If we now fix an arbitrarily chosen real $\delta \geq 0$ and assume that

$$|p^m a_n| > \varrho^{\delta} \max\{|a_0|, \ldots, |a_{n-2}|, |p^e a_{n-1}|\}, \tag{14}$$

then for any $j \in \{1, \ldots, n\}$ we must have

$$|\xi_j| < 1/\varrho^{\delta/n}. \tag{15}$$

Indeed, since our absolute value also satisfies the triangle inequality, we have

$$\begin{aligned} 0 &= |a_0 + a_1\xi_j + \cdots + a_{n-2}\xi_j^{n-2} + p^e a_{n-1}\xi_j^{n-1} + p^m a_n \xi_j^n| \\ &\geq |p^m a_n| \cdot |\xi_j^n| - |a_0 + a_1\xi_j + \cdots + a_{n-2}\xi_j^{n-2} + p^e a_{n-1}\xi_j^{n-1}| \\ &\geq |p^m a_n| \cdot |\xi_j^n| - \max\{|a_0|, |a_1\xi_j|, \ldots, |a_{n-2}\xi_j^{n-2}|, |p^e a_{n-1}\xi_j^{n-1}|\}. \end{aligned}$$

Therefore, if $|\xi_j| > 1$ we find

$$\begin{aligned} 0 &\geq |p^m a_n| \cdot |\xi_j|^n - \max\{|a_0|, |a_1|, \ldots, |a_{n-2}|, |p^e a_{n-1}|\} \cdot |\xi_j|^{n-1} \\ &= |\xi_j|^{n-1}(|p^m a_n| \cdot |\xi_j| - \max\{|a_0|, |a_1|, \ldots, |a_{n-2}|, |p^e a_{n-1}|\}) \\ &> |\xi_j|^{n-1}(|p^m a_n| - \varrho^{\delta} \max\{|a_0|, |a_1|, \ldots, |a_{n-2}|, |p^e a_{n-1}|\}) > 0, \end{aligned}$$

while if $1 \geq |\xi_j| \geq 1/\varrho^{\delta/n}$ we obtain

$$0 \geq |p^m a_n| \cdot \frac{1}{\varrho^{\delta}} - \max\{|a_0|, |a_1|, \ldots, |a_{n-2}|, |p^e a_{n-1}|\} > 0,$$

again a contradiction.

Using (15) one obtains

$$|\xi_1 \cdots \xi_j| < 1/\varrho^{j\delta/n}. \tag{16}$$

On the other hand, $b_0 \neq 0$ and hence $|b_0| \geq 1$, and since $b_j \mid a_n$ and $d \leq e$ we obviously have

$$|\xi_1 \cdots \xi_j| = \left|\frac{b_0}{p^d b_j}\right| \geq \frac{1}{|p|^e |a_n|}. \tag{17}$$

Recalling the definition of our absolute value, inequality (14) reads

$$\varrho^{m\deg p+\deg a_n}>\varrho^{\delta+\max\{\deg a_0,\ldots,\deg a_{n-2},\deg p^e a_{n-1}\}},$$

or equivalently,

$$m\deg p>\delta+\max\{\deg a_0,\ldots,\deg a_{n-2},\deg p^e a_{n-1}\}-\deg a_n. \tag{18}$$

In view of (16) and (17), to reach a contradiction it remains to choose δ such that

$$\frac{1}{|p|^e|a_n|}\geq 1/\varrho^{j\delta/n}. \tag{19}$$

Since $j\geq 1$, instead of (19) it will be sufficient to have $\varrho^{\delta/n}\geq|p|^e|a_n|$, or equivalently

$$\delta\geq n\deg a_n+ne\deg p.$$

A suitable candidate for δ is therefore $n\deg a_n+ne\deg p$, so we derive a contradiction if

$$(m-ne)\deg p>(n-1)\deg a_n+\max\{\deg a_0,\ldots,\deg a_{n-2},\deg p^e a_{n-1}\},$$

and this completes the proof. ∎

For the proof of Theorem 3, we assume as before that f decomposes as $f(X,Y)=f_1(X,Y)\cdot f_2(X,Y)$ with

$$f_1(X,Y)=b_0+b_1Y+\cdots+b_{j-1}Y^{j-1}+p^d b_jY^j,$$
$$f_2(X,Y)=c_0+c_1Y+\cdots+c_{k-1}Y^{k-1}+p^{m-d}c_kY^k,$$

where $d\geq 0$, $j,k\geq 1$, $j+k=n$, $b_0,\ldots,b_j,c_0,\ldots,c_k\in K[X]$, $b_jc_k=a_n$, and $b_0c_0=a_0$. One may again assume that $d\leq m-d$. Then, with exactly the same arguments as in the proof of Theorem 1, one shows that $e\geq d$. The remainder of the proof is similar to that of Theorem 2, with $\max\{|a_0|,\ldots,|a_{n-2}|,|p^e a_{n-1}|\}$ replaced by $\max\{|a_0|,\ldots,|a_{n-3}|,|p^e a_{n-2}|\}$. ∎

Remarks. 1. Here too, one may find polynomials for which equality in (2) holds, and which are reducible over $K(X)$. To see this, take $p\in K[X]$, p irreducible over K, let $n\geq 3$ and choose $a_0,a_2,\ldots,a_{n-1}\in K[X]$ of degree less than or equal to $m\deg p$ and such that $a_0a_{n-1}\neq 0$, $p\nmid a_{n-1}$. Define then $a_1\in K[X]$ by the equality $a_1(X)=-p(X)^m-a_0(X)-a_2(X)-\cdots-a_{n-1}(X)$, and let $f(X,Y)=a_0+a_1Y+\cdots+a_{n-1}Y^{n-1}+p^mY^n$. Here $e=0$ and obviously $m\deg p=\max\{\deg a_0,\ldots,\deg a_{n-1}\}$, so one has equality in (2). On the other hand, f is reducible over $K(X)$, being divisible by $Y-1$.

In a similar way one can find polynomials for which $m\not\equiv e \bmod 2$ and equality in (3) holds, and which are reducible over $K(X)$.

2. Let $K=\mathbb{Q}$, take an integer $k\geq 1$ and consider the polynomials $f_k(X,Y)=X^{2k}Y^4+(2X^k-1)Y^2+1$. Here we have $p(X)=X$, $m=2k$,

$e = 0$, and hence $m \equiv e \bmod 2$. Although condition (3) is fulfilled, our polynomials f_k are all reducible over $\mathbb{Q}(X)$, since

$$X^{2k}Y^4 + (2X^k - 1)Y^2 + 1 = (X^kY^2 + Y + 1)(X^kY^2 - Y + 1).$$

So in the case of Theorem 3 too, one has to assume that $m \not\equiv e \bmod 2$.

3. If we fix the polynomials $a_0, \dots, a_n$ as in Theorem 2, and take integers m, e with $m > (n+1)e$, the inequality (2) will hold for all the irreducible polynomials $p \in K[X]$ with

$$\deg p^e a_{n-1} \geq \max\{\deg a_0, \dots, \deg a_{n-2}\},$$
$$\deg p > (n-1)\deg a_n + \deg a_{n-1}.$$

Similarly, if we fix the polynomials $a_0, \dots, a_{n-2}, a_n$ as in Theorem 3, and take integers m, e with $m > (n+1)e$ and $m \not\equiv e \bmod 2$, the inequality (3) will hold for all the irreducible polynomials $p \in K[X]$ with

$$\deg p^e a_{n-2} \geq \max\{\deg a_0, \dots, \deg a_{n-3}\},$$
$$\deg p > (n-1)\deg a_n + \deg a_{n-2}.$$

We end with two immediate applications of Corollaries 2 and 3.

Corollary 4. *Let K be a field of characteristic 0, $r \geq 2$ a fixed integer, and $f(X_1, \dots, X_r) \in K[X_1, \dots, X_r]$ a polynomial of degree $n \geq 2$ in X_r. Assume that f has a linear factor in X_r of multiplicity 1, say $\beta X_r - \alpha$, with $\alpha, \beta \in K[X_1, \dots, X_{r-1}]$, $\beta \neq 0$. Let $p, c \in K[X_1, \dots, X_{r-1}]$, $c \neq 0$, $p \nmid c\beta$, and assume that for some $j \in \{1, \dots, r-1\}$, p as a polynomial in X_j is irreducible over $K(X_1, \dots, \widehat{X}_j, \dots, X_{r-1})$. Let e be maximum with the property that*

$$p^e \mid \beta^{n-1} \frac{\partial f}{\partial X_r}\left(X_1, \dots, X_{r-1}, \frac{\alpha(X_1, \dots, X_{r-1})}{\beta(X_1, \dots, X_{r-1})}\right).$$

Then for every integer m satisfying

$$m > ne + \frac{(n-1)\deg_j c\beta^{n-1} + \max\limits_{1 \leq i \leq n} \deg_j \beta^{n-1} \frac{\partial^i f}{\partial X_r^i}\left(X_1, \dots, X_{r-1}, \frac{\alpha(X_1, \dots, X_{r-1})}{\beta(X_1, \dots, X_{r-1})}\right)}{\deg_j p}$$

the polynomial $f + cp^m$ is irreducible over $K(X_1, \dots, X_{r-1})$.

Corollary 5. *Let K be a field of characteristic 0, $r \geq 2$ a fixed integer, and $f(X_1, \dots, X_r) \in K[X_1, \dots, X_r]$ a polynomial of degree $n \geq 3$ in X_r. Assume that f has a linear factor in X_r of multiplicity 2, say $\beta X_r - \alpha$, with $\alpha, \beta \in K[X_1, \dots, X_{r-1}]$, $\beta \neq 0$. Let $p, c \in K[X_1, \dots, X_{r-1}]$, $c \neq 0$, $p \nmid c\beta$, and assume that for some $j \in \{1, \dots, r-1\}$, p as a polynomial in X_j is irreducible over $K(X_1, \dots, \widehat{X}_j, \dots, X_{r-1})$. Let e be maximum with the* *property that*

$$p^e \mid \beta^{n-2}\frac{\partial^2 f}{\partial X_r^2}\left(X_1,\ldots,X_{r-1},\frac{\alpha(X_1,\ldots,X_{r-1})}{\beta(X_1,\ldots,X_{r-1})}\right).$$

Then for every integer $m \not\equiv e \bmod 2$ *satisfying*

$$m>ne+\frac{(n-1)\deg_j c\beta^{n-2}+\max\limits_{2\le i\le n}\deg_j \beta^{n-2}\frac{\partial^i f}{\partial X_r^i}\left(X_1,\ldots,X_{r-1},\frac{\alpha(X_1,\ldots,X_{r-1})}{\beta(X_1,\ldots,X_{r-1})}\right)}{\deg_j p}$$

the polynomial $f+cp^m$ *is irreducible over* $K(X_1,\ldots,X_{r-1})$.

For the proof of Corollary 4 it will be sufficient to test the irreducibility over $K(X_1,\ldots,X_{r-1})$ of the polynomial g defined by

$$g(X_1,\ldots,X_r)=\beta^{n-1}\left\{f\left(X_1,\ldots,X_{r-1},X_r+\frac{\alpha(X_1,\ldots,X_{r-1})}{\beta(X_1,\ldots,X_{r-1})}\right)+cp^m\right\}.$$

Let us denote the r-tuple $\left(X_1,\ldots,X_{r-1},\frac{\alpha(X_1,\ldots,X_{r-1})}{\beta(X_1,\ldots,X_{r-1})}\right)$ by $\overline{X}$. Since by our assumption we have $f(\overline{X})=0$ and $\frac{\partial f}{\partial X_r}(\overline{X})\neq 0$, we obtain

$$g(X_1,\ldots,X_r)=p^m c\beta^{n-1}+p^e\,\frac{\beta^{n-1}\frac{\partial f}{\partial X_r}(\overline{X})}{1!p^e}\cdot X_r+\sum_{i=2}^{n}\frac{\beta^{n-1}}{i!}\,\frac{\partial^i f}{\partial X_r^i}(\overline{X})\cdot X_r^i.$$

If we replace now f by $X_r^{\deg f}\cdot f(1/X_r)$ in Corollary 2, we see that a polynomial of the form $f(X_1,\ldots,X_r)=p^m a_0+p^e a_1X_r+a_2X_r^2+a_3X_r^3+\cdots+a_nX_r^n$ with $a_0,\ldots,a_n,p\in K[X_1,\ldots,X_{r-1}]$, $a_0a_1a_n\neq 0$, $p\nmid a_0a_1$, must be irreducible over $K(X_1,\ldots,X_{r-1})$ if for some $j\in\{1,\ldots,r-1\}$, p as a polynomial in X_j is irreducible over $K(X_1,\ldots,\widehat{X}_j,\ldots,X_{r-1})$ and

$$m>ne+\frac{(n-1)\deg_j a_0+\max\{\deg_j p^e a_1,\deg_j a_2,\ldots,\deg_j a_n\}}{\deg_j p}. \tag{20}$$

The conclusion now follows by applying (20) to $g(X_1,\ldots,X_r)$. ■

In order to prove Corollary 5, we first see from Corollary 3 that a polynomial of the form $f(X_1,\ldots,X_r)=p^m a_0+p^e a_2X_r^2+a_3X_r^3+\cdots+a_nX_r^n$ with $a_0,a_2,\ldots,a_n,p\in K[X_1,\ldots,X_{r-1}]$, $a_0a_2a_n\neq 0$, $p\nmid a_0a_2$, $m\not\equiv e \bmod 2$ will be irreducible over $K(X_1,\ldots,X_{r-1})$ if for some $j\in\{1,\ldots,r-1\}$, p as a polynomial in X_j is irreducible over $K(X_1,\ldots,\widehat{X}_j,\ldots,X_{r-1})$ and

$$m>ne+\frac{(n-1)\deg_j a_0+\max\{\deg_j p^e a_2,\deg_j a_3,\ldots,\deg_j a_n\}}{\deg_j p}. \tag{21}$$

Here it will be sufficient to test the irreducibility over $K(X_1,\ldots,X_{r-1})$ of the polynomial $\overline{g}$ defined by

$$\overline{g}(X_1,\ldots,X_r)=\beta^{n-2}\left\{f\left(X_1,\ldots,X_{r-1},X_r+\frac{\alpha(X_1,\ldots,X_{r-1})}{\beta(X_1,\ldots,X_{r-1})}\right)+cp^m\right\}.$$

Since now the linear factor $\beta X_r - \alpha$ has multiplicity 2, we have $f(\overline{X}) = 0$, $\frac{\partial f}{\partial X_r}(\overline{X}) = 0$ and $\frac{\partial^2 f}{\partial X_r^2}(\overline{X}) \neq 0$. Thus, we obtain

$$\overline{g}(X_1, \ldots, X_r) = p^m c\beta^{n-2} + p^e \frac{\beta^{n-2}\frac{\partial^2 f}{\partial X_r^2}(\overline{X})}{2!p^e} \cdot X_r^2 + \sum_{i=3}^{n} \frac{\beta^{n-2}}{i!} \frac{\partial^i f}{\partial X_r^i}(\overline{X}) \cdot X_r^i,$$

and the proof finishes by applying (21) to $\overline{g}(X_1, \ldots, X_r)$. ∎

Acknowledgements. The authors are grateful to Marian Vâjâitu and Alexandru Zaharescu for useful discussions, and to an anonymous referee for valuable suggestions.

References

[1] N. C. Bonciocat, *Upper bounds for the number of factors for a class of polynomials with rational coefficients*, Acta Arith. 113 (2004), 175–187.

[2] M. Cavachi, *On a special case of Hilbert's irreducibility theorem*, J. Number Theory 82 (2000), 96–99.

[3] M. Cavachi, M. Vâjâitu and A. Zaharescu, *A class of irreducible polynomials*, J. Ramanujan Math. Soc. 17 (2002), 161–172.

[4] —, —, —, *An irreducibility criterion for polynomials in several variables*, Acta Math. Inform. Univ. Ostraviensis, to appear.

[5] M. Filaseta and A. Schinzel, *On testing the divisibility of lacunary polynomials by cyclotomic polynomials*, Math. Comp. 73 (2004), 957–965.

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

[7] K. Langmann, *Der Hilbertsche Irreduzibilitätssatz und Primzahlfragen*, J. Reine Angew. Math. 413 (1991), 213–219.

[8] H. W. Lenstra, Jr., *Finding small degree factors of lacunary polynomials*, in: Number Theory in Progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, 267–276.

[9] —, *On the factorization of lacunary polynomials*, ibid. 277–291.

[10] S. Lipka, *Über die Irreduzibilität von Polynomen*, Math. Ann. 118 (1941), 235–245.

[11] W. Ljunggren, *On the irreducibility of certain lacunary polynomials*, Norske Vid. Selsk. Forh. (Trondheim) 36 (1963), 159–164.

[12] M. Mignotte, *Bounds for the roots of lacunary polynomials*, J. Symbolic Comput. 30 (2000), 325–327.

[13] M. Mignotte and D. Ştefănescu, *On the roots of lacunary polynomials*, Math. Inequal. Appl. 2 (1999), 1–13.

[14] O. Ore, *Einige Bemerkungen über Irreduzibilität*, Jahresber. Deutsch. Math. Verein. 44 (1934), 147–151.

[15] A. Schinzel, *Reducibility of lacunary polynomials I*, Acta Arith. 16 (1969), 123–159.

[16] —, *Reducibility of lacunary polynomials III*, ibid. 34 (1978), 227–266.

[17] —, *Reducibility of lacunary polynomials VII*, Monatsh. Math. 102 (1986), 309–337.

[18] —, *Reducibility of lacunary polynomials VIII*, Acta Arith. 50 (1988), 91–106.

[19] —, *Reducibility of lacunary polynomials X*, ibid. 53 (1989), 47–97.

[20] —, *Reducibility of lacunary polynomials XI*, ibid. 57 (1991), 165–175.

[21] —, *Reducibility of lacunary polynomials XII*, ibid. 90 (1999), 273–289.

[22] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia Math. Appl. 77, Cambridge Univ. Press, 2000.
[23] L. Weisner, *Criteria for the irreducibility of polynomials*, Bull. Amer. Math. Soc. 40 (1934), 864–870.

Institute of Mathematics "Simion Stoilow"
of the Romanian Academy
P.O. Box 1–764
RO–014700 Bucureşti, Romania
E-mail: Anca.Bonciocat@imar.ro
Nicolae.Bonciocat@imar.ro

Received on 9.5.2005
and in revised form on 14.3.2006 (4986)