UNIVERSITATIS IAGELLONICAE ACTA MATHEMATICA, FASCICULUS XXXIX
2001

A FIBRE CRITERION FOR A POLYNOMIAL TO BELONG TO AN IDEAL

by Marcin Dumnicki

Abstract. In the paper we generalize a fibre criterion for a polynomial f to belong to a primary ideal I in the polynomial ring $\mathbb{K}[X,Y]$. We also investigate the general case where the ideal I is not primary.

Let $\{X_1,\ldots,X_n\}$ be any set of variables. We shall write $\mathbb{K}[X]$ instead of $\mathbb{K}[X_1,\ldots,X_n]$. If $f \in \mathbb{K}[X,Y]$, where X and Y are sets of variables, $\mathbb{K}$ is an algebraically closed field, $Y = \{Y_1,\ldots,Y_m\}$, $a \in \mathbb{K}^m$, then $f_a := f(X_1,\ldots,X_n,a_1,\ldots,a_m)$. For a subset I of $\mathbb{K}[X,Y]$ we define $I_a = \{f_a \mid f \in I\}$. Of course, if I is an ideal then is I_a. We shall also write I_Y for $I \cap \mathbb{K}[Y]$.

The following theorem was proved by Jarnicki-O'Carroll-Winiarski [**2**] (see also preprint, proposition 12):

> *Let I be an ideal in $\mathbb{K}[X,Y]$ such that $I \cap \mathbb{K}[Y] = (0)$, where $\mathbb{K}$ is an algebraically closed field. Assume that for all $a \in \mathbb{K}^m$ the ideal I_a is proper and zero-dimentional. Then the following holds true:*
> $$\forall f \in \mathbb{K}[X,Y] \qquad \forall a \in \mathbb{K}^m \ f_a \in I_a \Longrightarrow f \in I. \quad (*)$$

We generalize the above to the following:

Theorem. *Let $\mathbb{K}$ be an algebraically closed field, I be a primary ideal in $\mathbb{K}[X,Y]$. Then the following conditions are equivalent:*

(1) $\forall f \in \mathbb{K}[X,Y] \qquad \forall a \in \mathbb{K}^m \ f_a \in I_a \Longrightarrow f \in I,$

(2) I_Y *is radical.*

We also investigate the case where the ideal I is not primary. The original proof by W. Jarnicki, L. O'Carroll and T. Winiarski uses comprehensive Gröbner bases and cannot be carried over to the general case. Our approach makes use of reduced Gröbner bases, and is essentially based on a lemma on specialization for a Gröbner basis. Although this lemma is well known, we give its proof for the reader's convenience. Another, purely algebraic proof of the fibre criterion is presented by K. J. Nowak [**3**], who does not use the theory of Gröbner bases.

We begin by recalling some basic definitions and facts concerning Gröbner bases, which are used in the proof of the main result of this paper. For a thorough introduction to the theory of Gröbner bases, we refer the reader to [**1**].

Definition. A term is a product of the form $X_1^{e_1} \cdots X_n^{e_n}$, with $e_i \in \mathbb{N}$ for $1 \le i \le n$. We denote by $T(X)$, or simply by T the set of all terms in these variables.

Definition. A term order (denoted by $\preceq$) is a linear order on T that satisfies the following conditions:
(1) $\forall t \in T \qquad 1 \preceq t$,
(2) $\forall s, t_1, t_2 \in T \quad t_1 \preceq t_2 \Longrightarrow t_1 s \preceq t_2 s$.

Definition. Let $1 \le i < n$, $T_1 = T(X_1, \ldots, X_i)$, $T_2 = T(X_{i+1}, \ldots, X_n)$, and let $\preceq_1$ and $\preceq_2$ be term orders on T_1 and T_2 respectively. Any $t \in T$ may be written uniquely as $t = t_1 t_2$ with $t_i \in T_i$ for $i = 1, 2$. Then term order $\preceq$ on T defined as follows: $s \preceq t$ if
$s_1 \prec_1 t_1$, or
$(s_1 = t_1$ and $s_2 \preceq_2 t_2)$
is called a block order on T where $T_1 \ll T_2$.

Definition. Let $f \in \mathbb{K}[X]$, $f \neq 0$, and let $\preceq$ be a term order on T. Write the polynomial f in the following form:

$$f(X) = \sum_{\alpha} c_\alpha X^\alpha.$$

We define the support, leading term and leading coefficient of f as follows:

$$\operatorname{supp}(f) = \{X^\alpha \mid c_\alpha \neq 0\}$$

$$\mathrm{LT}(f) = \max(f)$$

$$\mathrm{LC}(f) = \text{the coefficient of } \mathrm{LT}(f) \text{ in } f,$$

where $\max(f)$ denotes the maximal element, with respect to $\preceq$, among terms of f with non-zero coefficients. For f, $g \in \mathbb{K}[X]$ we say that $f \le g$ if $\mathrm{LT}(f) \preceq \mathrm{LT}(g)$.

Definition. Let P be a finite subset of $\mathbb{K}[X]$, $f \in \mathbb{K}[X]$. We say that f is reducible mod P if $\exists p \in P$ and $t \in \operatorname{supp}(f)$ such that $\mathrm{LT}(p) | t$. If f is not reducible mod P then we say that f *is in normal form mod* P. Assume that f is reducible mod P, $\mathrm{LT}(p)|t$ for some $t \in \mathrm{supp}(f)$, and

$$g = \mathrm{LC}(p)f - asp,$$

where $s \in T$ satisfies $\mathrm{LT}(p)s = \mathrm{LT}(f)$, and a is the coefficient of the term t in the polynomial f. Than we say that f *reduces to* g *mod* P (notation $f \longrightarrow g$).

Definition. Let P be a finite subset of $\mathbb{K}[X]$, $f \in \mathbb{K}[X]$. We say, that f is top-reducible mod P if $\exists p \in P$ such that $\mathrm{LT}(p)|\mathrm{LT}(f)$.

Definition. For any polynomials g and f we say, that g *is a normal form of* f *mod* P if g is in normal form mod P, and there exists $g_1, \ldots, g_r$ for some $r \in \mathbb{N}$ such that $g_1 = f$, $g_r = g$, and

$$\forall i \in \{1, \ldots, r-1\} \qquad g_i \longrightarrow g_{i+1}.$$

Definition. Let $0 \neq f \in \mathbb{K}[X]$, G a finite subset of $\mathbb{K}[X]$, $0 \notin G$. A representation

$$f = \sum_{i=1}^{k} q_i g_i$$

with polynomials $0 \neq q_i \in \mathbb{K}[X]$ and $g_i \in G$ $(1 \leq i \leq k)$ is called a standard representation of f with respect to (w.r.t) G if

$$\max\{\mathrm{LT}(q_i g_i) \mid 1 \leq i \leq k\} \ \preceq \ \mathrm{LT}(f).$$

Definition. By a Gröbner basis G (with respect to a term order $\preceq$) we mean a finite set of polynomials that satisfies one of the following equivalent conditions: (cf. [**1**])

(1) $\forall f \in I \quad f \neq 0 \Longrightarrow f$ is reducible mod G
(2) $\forall f \in I \quad f \neq 0 \Longrightarrow f$ is top-reducible mod G
(3) $\forall f \in \mathbb{K}[X] \quad f \in I \iff$ some normal form of $f = 0$
(4) $\forall f \in \mathbb{K}[X] \quad f \in I \iff$ the unique normal form of $f = 0$
(5) $\forall f \in I \quad f \neq 0 \Longrightarrow f$ has a standard representation w.r.t. G,

where I is the ideal generated by G.

We say that a Gröbner basis is reduced if for all $1 \leq i \leq r$, g_i is in normal form mod $G \setminus \{g_i\}$, and $\mathrm{LC}(g_i) = 1$.

Remark. Since the conditions (1) and (2) in the above definition are equivalent, whenether we write that the polynomial is reducible we mean that is top-reducible.

Now let I be an ideal in $\mathbb{K}[X]$, and let $\preceq$ be a term order on T. Then there exists (exactly one) reduced Gröbner basis of I with respect to $\preceq$ (cf. [**1**]).

Definition. Let f and g be in $\mathbb{K}[X]$, q be the least common multiple (lcm) of $\mathrm{LT}(f)$ and $\mathrm{LT}(g)$ in T, and let s, $t \in T$ such that $\mathrm{LT}(f)s = q$, $\mathrm{LT}(g)t = q$, then we define the S-polynomial of f and g:

$$S\text{-poly}(f, g) = \mathrm{LC}(g)sf - \mathrm{LC}(f)tg.$$

The idea of the S-poly is to multiply leading terms of f and g by some terms and coefficients in order to "cancel" them.

We will make use of the following well known theorem (cf. [**1**]):
Let G be a finite subset of $\mathbb{K}[X]$, $0 \notin G$, and let $\preceq$ be a term order on T. Assume that for all $g_1, g_2 \in G$, $S\text{-poly}(g_1, g_2)$ equals 0 or has a standard representation with respect to G. Then G is a Gröbner basis.

All above definitions and theorems are classical and can be found in any book about Gröbner bases. The next lemma is known, however is not so classical.

We shall use the following notation to deal with Gröbner bases in $\mathbb{K}[X, Y]$. Every $f \in \mathbb{K}[X, Y]$ can be written in the following form:

$$f = \sum_{\alpha \in \mathbb{N}^n} W_\alpha(Y) X^\alpha.$$

If $\mathrm{LT}(f) = X^\beta Y^\delta$, then we define

$$\mathrm{LT}_X(f) = X^\beta, \qquad \mathrm{LC}_X(f) = W_\beta(Y).$$

For $G \subset \mathbb{K}[X, Y]$ we shall write $G_{X\setminus Y} = G \setminus (G \cap \mathbb{K}[Y])$.
To prove the main theorem we need the following

Lemma. *Let $\mathbb{K}$ be an algebraically closed field, I an ideal in $\mathbb{K}[X, Y]$, and let $\preceq$ be any block order on $T(X, Y)$ where $Y \ll X$. Let G be the reduced Gröbner basis [1] of I with respect to $\preceq$. We denote by $V(I_Y)$ the algebraic set generated by I_Y in $\mathbb{K}^m$, where m is the number of variables Y. If I_Y is prime, then there exists an non-empty, open (in Zariski topology) set $U \subset V(I_Y)$, such that if $a \in U$ then $(G_{X\setminus Y})_a$ is a Gröbner basis of I_a with respect to the restriction $\preceq_X$ of $\preceq$ to $T(X)$.*

Remark. In the above lemma we take $(G_{X\setminus Y})_a$ instead of G_a to avoid a situation when $0 \in G_a$. We recall the fact, that $G_Y = G \cap \mathbb{K}[Y]$ is a Gröbner basis of I_Y. We shall also write $\preceq$ instead of $\preceq_X$ and $\preceq_Y$, because these restrictions have only formal meaning.

[1]In fact, we do not need a reduced Gröbner basis, it is enough to have a minimal one.

Proof. We want to prove the condition concerning the S-polynomials. First observe that in our case $V(I_Y)$ is irreducible, and if we take an $f \in \mathbb{K}[Y]$, $f \notin I_Y$, than there exists an open, non-empty dense subset $U_f \subset V(I_Y)$ such that for $a \in U_f$ $f(a) \neq 0$.
For g_i and g_j in $G_{X\setminus Y}$, define

$$\widetilde{S}\text{-poly}(g_i, g_j) = \mathrm{LC}_X(g_j)X^{\alpha}g_i - \mathrm{LC}_X(g_j)X^{\beta}g_i,$$

where

$$\mathrm{LT}_X(g_i)X^{\alpha} = \mathrm{LT}_X(g_j)X^{\beta} = \mathrm{lcm}(\mathrm{LT}_X(g_i), \mathrm{LT}_X(g_j)).$$

We want to know that for a generic a

$$\widetilde{S}\text{-poly}(g_i, g_j)_a = S\text{-poly}(g_{i_a}, g_{j_a}). \tag{1}$$

First observe that $\mathrm{LC}_X(g_i) \notin I_Y$. Otherwise $\mathrm{LC}_X(g_i)$ would be reducible mod G_Y and, in fact, g_i would be reducible mod $G\setminus\{g_i\}$. Now, if we take a belonging to $U_{g_i} := U_{\mathrm{LC}_X(g_i)}$ and $U_{g_j} := U_{\mathrm{LC}_X(g_j)}$ we have

$$\mathrm{LT}(g_{i_a}) = \mathrm{LT}_X(g_i), \qquad \mathrm{LT}(g_{j_a}) = \mathrm{LT}_X(g_j),$$

because $\mathrm{LC}_X(g_i)(a) \neq 0$ and $\mathrm{LC}_X(g_j)(a) \neq 0$. Then the equality (1) holds for $a \in U_{g_i} \cap U_{g_j}$.

Reducing an $\widetilde{S}$-poly(g_i, g_j) mod G_Y we obtain a polynomial $S_{i,j}$ which is either 0 or not reducible mod G_Y, and

$$S_{i,j} = \widetilde{S}\text{-poly}(g_i, g_j) + q,$$

where $q \in I_Y$. From the above equality we have, for an $a \in V(I_Y)$

$$S_{i,j_a} = \widetilde{S}\text{-poly}(g_i, g_j)_a.$$

Because $S_{i,j}$ is not reducible mod G_Y, $\mathrm{LC}_X(S_{i,j}) \notin G_Y$ and for $a \in U_{S_{i,j}} = U_{\mathrm{LC}_X(S_{i,j})}$ we have $\mathrm{LC}_X(S_{i,j})(a) \neq 0$. $S_{i,j} \in I$, so it has the standard representation

$$S_{i,j} = \sum_{\ell=1}^{r} h_\ell g_\ell,$$

where for $1 \leq \ell \leq r$

$$\mathrm{LT}(h_\ell g_\ell) \preceq \mathrm{LT}(S_{i,j}).$$

For $a \in U_{S_{i,j}}$ we have

$$\mathrm{LT}(h_{\ell a} g_{\ell a}) \preceq \mathrm{LT}_X(h_\ell g_\ell) \preceq \mathrm{LT}_X(S_{i,j}) = \mathrm{LT}(S_{i,j_a}),$$

and thus the representation

$$S_{i,j_a} = \sum_{\ell=1}^{r} h_{\ell a} g_{\ell a}$$

(after deleting the components which become 0) is a standard representation. Therefore

$$U = \bigcap_{(g_i,g_j)\in(G_{X\setminus Y})^2} U_{S_{i,j}} \cap \bigcap_{g_i\in G_{X\setminus Y}} U_{g_i}$$

is a non-empty open set, required in the Lemma. $\square$

Now we state the following main theorem

Theorem 1. *Let $\mathbb{K}$ be an algebraically closed field, I be a primary ideal in $\mathbb{K}[X,Y]$. Then the following conditions are equivalent:*
(1) $\quad \forall f \in \mathbb{K}[X,Y] \quad \forall a \in \mathbb{K}^m \; f_a \in I_a \Longrightarrow f \in I,$
(2) $\quad I_Y$ *is radical.*

Proof. To show (2) $\Longrightarrow$ (1), we assume that it is not true. Let G be a reduced Gröbner basis of I with respect to a block order $\preceq$, like in the Lemma. Define the set

$$M := \{f \in \mathbb{K}[X,Y] \mid \; f \notin I, \; \forall a \in \mathbb{K}^m \; f_a \in I_a\}.$$

Then $M \neq \emptyset$, and we can choose a minimal element f_0 of M with respect to $\leq$ (that means that $\mathrm{LT}(f_0)$ is smaller or equal to leading term of any other element in M with respect to $\preceq$). Moreover, we take f_0 which is in normal form mod G. Take U from the previous Lemma (I_Y is prime because it is primary and radical).

We have two cases:

Case 1. $f_0 \notin \mathbb{K}[Y]$. Take an $a \in U$ such that $\mathrm{LC}_X(f_0)(a) \neq 0$ (f_0 is in normal form mod G, so $\mathrm{LC}_X(f_0)$ is not reducible mod G_Y). Then $(f_0)_a \in I_a$, $(G_{X\setminus Y})_a$ is a Gröbner basis of I_a, so for some i and some α we have the following:

$$\mathrm{LT}((f_0)_a) = \mathrm{LT}(g_{i_a})X^\alpha.$$

But we can also see that

$$\mathrm{LT}_X(f_0) = \mathrm{LT}_X(g_i)X^\alpha$$

and take

$$f' = \mathrm{LC}_X(g_i)f_0 - \mathrm{LC}_X(f_0)X^\alpha g_i.$$

Then $f' < f_0$ (the leading term of f_0 is cancelled), $\forall a \in \mathbb{K}^m \; {f'}_a \in I_a$, hence $f' \in I$ (from the minimal choice of f_0), and $\mathrm{LC}_X(g_i)f_0 \in I$. Now $\mathrm{LC}_X(g_i)^d \in I$, for some natural d (because I is primary) and $\mathrm{LC}_X(g_i) \in I_Y$ (because I_Y is radical), a contradiction.

Case 2. $f_0 \in \mathbb{K}[Y]$. For $a \in U$ the ideal I_a is proper (1 is not reducible mod $(G_{X\setminus Y})_a$ since none of the $g_i \in G_{X\setminus Y}$ becomes a non-zero constant). Then $f_a \in I_a$ means that for all $a \in U$ $f_a = f(a)$ is zero. Hence f is zero on the open, non-empty set in $V(I_Y)$, and then $f \in \mathrm{rad}(I_Y) = I_Y \subset I$, a contradiction.

The proof of the converse implication is easy. Take any $f \notin I_Y$, $f \in \mathrm{rad}(I_Y)$. Then
if $f(a) = 0$, then $f_a = f(a) \in I_a$,
if $f(a) \neq 0$, then $0 \neq {f_a}^d \in I_a$ for some d, so $I_a = (1)$, and $f_a \in I_a$,
but $f \notin I$. $\square$

The case of an arbitrary (possibly non-primary) ideal will be considered in the following theorem

THEOREM 2. *Let $\mathbb{K}$ be an algebraically closed field, I any ideal in $\mathbb{K}[X, Y]$, $I = \bigcap_{k=1}^{r} I_k$ a primary decomposition of I. Then*
(1) if $\forall k\ 1 \leq k \leq r\ I_{kY}$ is radical, then I has property $(*)$.
(2) if $\exists k\ 1 \leq k \leq r$, such that I_{kY} is not radical, and I_k is the isolated component of I, then I has not property $(*)$.

PROOF. (1) Take an $f \in \mathbb{K}[X, Y], \forall a\ f_a \in I_a$. Then we have

$$I_a \subset \bigcap_{k=1}^{r} (I_k)_a,$$

so $\forall a,\ \forall k\ f_a \in (I_k)_a$. From Theorem 1 we have $\forall k\ f \in I_k$, and consequently $f \in I$.

(2) Take $f \in \mathbb{K}[Y]$ such that $f \notin I_k, f \in \mathrm{rad}(I_k)$. For all $i \in \{1, \ldots, r\}\ i \neq k$ take $g_i \in I_i$ such that $g_i \notin \mathrm{rad}(I_k)$. (This is possible since I_k is isolated.) Let $g = g_1 \ldots g_{k-1} g_{k+1} \ldots g_r$. Then $g \notin \mathrm{rad} I_k$. Now if $gf \in I$ then $gf \in I_k, f \notin I_k$ $\Longrightarrow \exists d\ g^d \in I_k \Longrightarrow g \in \mathrm{rad}(I_k)$, which is false. But $f^d \in I_k$ for some d, hence $gf^d \in I$. Now the theorem follows from the following lemma:

LEMMA. *Let I be an ideal in $\mathbb{K}[X, Y]$ which has property $(*)$. Then*

$$\forall g \in \mathbb{K}[X, Y],\ \forall f \in \mathbb{K}[Y],\ \forall d \in \mathbb{N},\ d \neq 0 \qquad gf^d \in I \Longrightarrow gf \in I.$$

$\square$

PROOF. Take any $a \in \mathbb{K}^m$. Then

$$g_a {f^d}_a = g_a f(a)^d \in I_a.$$

If $f(a) = 0$ then $g_a f_a = g_a f(a) = 0 \in I_a$, and otherwise $\frac{1}{f(a)} \in K$ gives $g_a f(a) \in I_a$. Property $(*)$ gives $gf \in I$, since we can do the same for an arbitrary a. $\square$

We can look at some simple examples in $\mathbb{K}[X, Y_1, Y_2]$:

$I = (X)$	has the property, is primary, $I_Y = (0)$,
$I = (X, Y_1)$	has the property, is primary, but $I_Y = (Y_1)$,
$I = (XY_1{}^2)$	has not the property, is not primary,
$I = (XY_1)$	has the property, but is not primary,
$I = (X, Y_1{}^2)$	has not the property, is primary, but $I_Y = (Y_1{}^2)$,
$I = (X, Y_1{}^2 - Y_2)$	has the property, is primary, but $I_Y = (Y_1{}^2 - Y_2)$.

To observe that the assumption that the primary component is isolated cannot be dropped, consider the following example of primary decomposition $\mathbb{K}[X, Y]$:

$$(X^2, XY) = (X) \cap (X^2, XY, Y^2),$$

and the second component, which is embedded, contracted to $\mathbb{K}[Y]$ is not radical. However the decomposition

$$(X^2, XY) = (X) \cap (X^2, Y)$$

shows that the ideal (X^2, XY) has property $(*)$.

References

1. Becker T., Weispfenning V., *Gröbner bases,* Springer-Verlag, (1993).
2. Jarnicki W., O'Carroll L., Winiarski T., *Ideal as an intersection of zero-dimensional ideals and the noether exponent,* Univ. Iagel. Acta Math. (to appear).
3. Nowak K.J., *A short proof of a fibre criterion for polynomials to belong to an ideal,* Univ. Iagel. Acta Math. (to appear).

Received March 12, 2001

Jagiellonian University
Institute of Mathematics
Reymonta 4
30-059 Kraków
Poland
e-mail: dumnicki@omega.im.uj.edu.pl