J. Symbolic Computation (2002) **33**, 609–625
doi:10.1006/jsco.2002.0525
Available online at http://www.idealibrary.com on IDEAL®

Derivations and Radicals of Polynomial Ideals over Fields of Arbitrary Characteristic

E. FORTUNA†, P. GIANNI† AND B. TRAGER‡

†*Dipartimento di Matematica, Università di Pisa, via Buonarroti 2, I–56127 Pisa, Italy*
‡*IBM Research, Route 134, Yorktown Heights, NY 10598, U.S.A.*

The purpose of this paper is to give a complete effective solution to the problem of computing radicals of polynomial ideals over general fields of arbitrary characteristic. We prove that Seidenberg's "Condition P" is both a necessary and sufficient property of the coefficient field in order to be able to perform this computation. Since Condition P is an expensive additional requirement on the ground field, we use derivations and ideal quotients to recover as much of the radical as possible. If we have a basis for the vector space of derivations on our ground field, then the problem of computing radicals can be reduced to computing pth roots of elements in finite dimensional algebras.

Introduction

The problem of finding efficient algorithms for computing the radical of ideals in polynomial rings over fields has been investigated by many researchers (Gianni *et al.*, 1988; Alonso *et al.*, 1991; Krick and Logar, 1991; Vasconcelos, 1991; Eisenbud *et al.*, 1992; Caboara *et al.*, 1997; Matsumoto, 2001). Most of these results make the simplifying assumption that the characteristic of the ground field is either zero or sufficiently large. The papers by Krick and Logar (1991) and Matsumoto (2001) provide solutions which are valid for any positive characteristic but assume a ground field which is finitely generated over a perfect field. They are based on Gröbner basis computations, that require additional variables and relations. Although their condition on the coefficient field is satisfied in the most common situations, we want to explore what is the most general context in which one can compute radicals. Moreover, our construction is based on computing ideal quotients of zero-dimensional ideals, which can be performed using linear algebra (Lakshman, 1990) without the introduction of any additional variables. Also Caboara *et al.* (1997) gives an algorithm which is valid for ideals over any perfect field; their approach is based on computing projections to hypersurfaces and performing square-free decompositions. In some cases they may require a large number of projections in order to compute the radical.

The purpose of this paper is to give a complete effective solution to the problem with no assumptions about the characteristic. We assume that the coefficient fields are computable, in the sense that we are given effective algorithms to perform rational operations and to decide whether or not a given element is zero. In the case of fields of characteristic zero, these assumptions are sufficient to be able to compute the radical of

0747–7171/02/050609 + 17 $35.00/0

polynomial ideals. However, for fields of positive characteristic, additional complications arise due to inseparability problems. In general one is no longer able to compute radicals without making additional assumptions about the ground field. One such assumption due to Seidenberg is that we can solve systems of homogeneous linear equations for solutions which are pth powers. Seidenberg (1974) shows that this assumption, which he calls "Condition P", is both necessary and sufficient to be able to compute radicals of primary ideals. We show in this paper that this is precisely the additional information we need to compute radicals under all circumstances.

Mines *et al.* (1988) have shown that a field K satisfies "Condition P" if and only if any finite dimensional K-algebra has a computable radical. Along with the reduction to zero-dimensional construction in this paper, this would give another demonstration that "Condition P" is necessary and sufficient to compute radicals of polynomial ideals. Their algorithm essentially involves repeated direct use of Condition P to construct elements in the radical. They are only interested in showing that the radical is constructible, not necessarily giving efficient algorithms. Since in general applying Condition P can be very expensive computationally, we try to perform as much of the radical computation as possible without using Condition P. Only in the final stage, if there remain inseparability problems, we may need to make use of Condition P.

We show that, over any computable field, we can reduce the radical computation to that of zero-dimensional ideals. We compute the radical of zero-dimensional ideals by an induction on the number of variables. Our inductive hypothesis is that we have an ideal whose contraction to the polynomial ring in one fewer variable is radical, and we show how to use this to compute the radical of the entire ideal. Along the way we are able to perform a partial radical computation which presents the ideal as an intersection of radical ideals evaluated in pth powers. This can be done over any computable field, but to finish the process we need to use Seidenberg's additional assumption.

Since Condition P is an expensive additional requirement on the ground field, we use derivations and ideal quotients to recover as much of the radical as possible. If we have a basis for the vector space of derivations on our ground field, then the problem of computing radicals can be reduced to computing pth roots of elements in finite dimensional algebras.

Throughout the paper K will denote a computable field of characteristic $p \geq 0$. In every section except for the last two we will be dealing only with zero-dimensional ideals. Sections 1 and 2 are independent of the rest of the paper and give some constructions which can be used to provide shortcuts for computing the radical. Section 1 investigates projections, while Section 2 shows which portion of the radical can be computed using the Jacobian criterion. Section 3 begins a general investigation of the use of derivatives in computing the radical; this is used in Section 4 to give a complete algorithm for the radical of zero-dimensional ideals over general fields satisfying Seidenberg's Condition P. In Section 5 we show that for finitely generated fields over perfect fields, multiple derivations can be used to replace Condition P with the ability of computing pth roots. In Section 6 we will show how to reduce the general problem to the zero-dimensional case and in the final section we conclude with some illustrative examples.

1. Radicals Using Projections

In this section we show that the radical of an ideal can be reconstructed from the radicals of two suitable projections provided that at least one of them is separable.

DEFINITION 1.1. Let K be a field. A K-algebra A is called separable over K if, for any finite extension K' of K, $A \otimes_K K'$ is reduced (i.e. it contains no nilpotent elements). An ideal $I \subseteq K[x_1, \ldots, x_n]$ is called separable if the algebra $A = K[x_1, \ldots, x_n]/I$ is separable over K.

Observe that an ideal $I \subseteq K[x_1, \ldots, x_n]$ is separable if and only if $I \otimes_K K'$ is radical for any finite extension K' of K.

LEMMA 1.2. *Let I, J be zero-dimensional ideals in a ring. If $J \subseteq I$, then $\sqrt{I} = I + \sqrt{J}$.*

PROOF. If $\sqrt{I} = \bigcap M_i$ is the primary decomposition of $\sqrt{I}$, any M_i will be one of the associated primes of J, so that $\sqrt{J} = \sqrt{I} \cap H$ for a suitable ideal H such that $I \not\subseteq H$, which implies the thesis. □

PROPOSITION 1.3. *Let I_1 be a zero-dimensional ideal in $R_1 = K[x_1, \ldots, x_k]$ and I_2 a zero-dimensional ideal in $R_2 = K[x_{k+1}, \ldots, x_n]$. If $\sqrt{I_1}$ is separable, then*

$$\sqrt{I_1 + I_2} = \sqrt{I_1} + \sqrt{I_2}.$$

PROOF. Observe that $I_1 + I_2$ is zero-dimensional in $K[x_1, \ldots, x_n]$. Since $\sqrt{I_1} + \sqrt{I_2} \subseteq \sqrt{I_1 + I_2}$, by Lemma 1.2 it is sufficient to prove that $H = \sqrt{I_1} + \sqrt{I_2}$ is radical.

If we set $X = (x_1, \ldots, x_n)$, let us show that $K[X]/H$ is reduced.

If we denote $J_1 = \sqrt{I_1}$ and $J_2 = \sqrt{I_2}$, we have that

$$K[X]/H \simeq (R_1/J_1) \otimes_K (R_2/J_2).$$

Since J_2 is radical, R_2/J_2 is isomorphic to $\oplus_i K_i$, with K_i finite extensions of K, so that (cf. Lang, 1984, Proposition 3, Chapter XVI, Section 2)

$$K[X]/H \simeq (R_1/J_1) \otimes_K (\oplus_i K_i) \simeq \oplus_i ((R_1/J_1) \otimes_K K_i).$$

By hypothesis R_1/J_1 is separable, hence $(R_1/J_1) \otimes_K K_i$ is reduced for all i and therefore also their direct sum. So $K[X]/H$ is reduced and then H is radical. □

REMARK 1.4. If an ideal $I \subseteq K[x_1, \ldots, x_n]$ is zero-dimensional, let $f_1, \ldots, f_n$ be univariate polynomials such that $(f_i) = K[x_i] \cap I$ and consider the polynomials $g_1, \ldots, g_n$ such that $(g_i) = \sqrt{(f_i)}$ (in other words, g_i is the square-free part of f_i). Using Lemma 1.2 and Proposition 1.3 we see that, if at most one of the g_i's is not separable, then

$$\sqrt{I} = I + (g_1, \ldots, g_n).$$

This remark shows that, with the hypothesis of separability, it is possible to extend Lemma 2.4 of Krick and Logar (1991) to fields of positive characteristic. This has also been observed by Kemper (2000, Proposition 5) but our remark is somewhat stronger, because we only require that all but one of the polynomials are separable.

2. Jacobian Criterion in Arbitrary Characteristic

The result of Lemma 1.2 can be used to reduce the problem of computing the radical of a zero-dimensional ideal to the case of complete intersections. If I is a zero-dimensional ideal in $K[x_1, \ldots, x_n]$ and G denotes a Gröbner basis for I with respect to the lexicographical order with $x_1 > \cdots > x_n$, then for each $i = 1, \ldots, n$ there exists a $g_i \in G$ such

that the leading term $lt(g_i) = {x_i}^{m_i}$. If we denote $\widetilde{I} = (g_1, \ldots, g_n)$, by Lemma 1.2 we have that $\sqrt{I} = I + \sqrt{\widetilde{I}}$, so that we need only to compute the radical of $\widetilde{I}$.

The following proposition shows that much of the radical of a zero-dimensional ideal can be recovered with a single ideal quotient. If the characteristic is 0 or sufficiently large we obtain the entire radical in one step.

PROPOSITION 2.1. *Let I be a zero-dimensional ideal in $K[x_1, \ldots, x_n]$ and $I = \bigcap_i Q_i$ its primary decomposition with $P_i = \sqrt{Q_i}$. Assume that the reduced Gröbner basis G for I with respect to the lexicographical order with $x_1 > \cdots > x_n$ is formed by exactly n polynomials, say $G = \{f_1, \ldots, f_n\}$ with $f_i \in K[x_i, \ldots, x_n]$. Let $F = \prod_{i=1}^{n} \frac{\partial f_i}{\partial x_i}$. Then*

(1) $(I : F) = \bigcap_{F \notin Q_i} P_i$
(2) *if $F \notin Q_i$, then P_i is separable*
(3) *if $char(K) = 0$ or $char(K) > \max\{\deg_{x_i} f_i\}$, then $\sqrt{I} = (I : F)$.*

PROOF. (1) Since $(I : F) = \bigcap_{F \notin Q_i} (Q_i : F)$, we have only to prove that, for all i such that $F \notin Q_i$, then $(Q_i : F) = P_i$. Denote by Q one of the Q_i's such that $F \notin Q_i$ and $P = \sqrt{Q}$ and let us prove that $(Q : F) = P$.

Consider the reduced Gröbner basis G_Q for Q with respect to the lexicographical order with $x_1 > \cdots > x_n$ and denote by $q_1, \ldots, q_n$ polynomials in G_Q such that $lt(q_i) = {x_i}^{m_i}$.

Let $\{h_1, \ldots, h_n\}$ be the reduced Gröbner basis for $P = \sqrt{Q}$. By Gianni *et al.* (1988, Proposition 5.8), for each $i = 1, \ldots, n$ there exists an integer s_i such that

$$q_i = {h_i}^{s_i} + \sum_{k=i+1}^{n} d_{ik} h_k \tag{1}$$

with $d_{ik}, h_i \in K[x_i, \ldots, x_n]$. In particular $q_n = {h_n}^{s_n}$.

In order to prove that $(Q : F) = P$, it is sufficient to prove that $h_i \in (Q : F)$ for all $i = 1, \ldots, n$. If we denote $F_j = \prod_{k=j}^{n} \frac{\partial f_k}{\partial x_k}$ (so that $F = F_1$), we will get the thesis proving by induction that $h_i F_i \in Q \ \forall i = 1, \ldots, n$.

For all i, $f_i \in Q \cap K[x_i, \ldots, x_n]$ and it is monic in x_i, so it must reduce to 0 modulo $G_Q \cap K[x_i, \ldots, x_n]$ and hence

$$f_i = u_i {h_i}^{s_i} + \sum_{k=i+1}^{n} c_{ik} h_k \tag{2}$$

with $u_i, c_{ik} \in K[x_i, \ldots, x_n]$.

We immediately see that $h_n F_n \in Q$ because, using that $f_n = u_n {h_n}^{s_n}$, we have

$$h_n F_n = h_n \frac{\partial f_n}{\partial x_n} = h_n \frac{\partial u_n}{\partial x_n} {h_n}^{s_n} + s_n h_n u_n \frac{\partial h_n}{\partial x_n} {h_n}^{s_n - 1} = {h_n}^{s_n} \left(h_n \frac{\partial u_n}{\partial x_n} + s_n u_n \frac{\partial h_n}{\partial x_n} \right).$$

Assume now that $h_j F_j \in Q \ \forall j = i+1, \ldots, n$ (and hence that $h_j F_m \in Q \ \forall m \leq j$) and let us prove that $h_i F_i \in Q$.

Observe that ${h_i}^{s_i} F_{i+1} \in Q$ because, using (1), we can write

$$ {h_i}^{s_i} F_{i+1} = \left(q_i - \sum_{k=i+1}^{n} d_{ik} h_k \right) F_{i+1}$$

which belongs to Q because each $h_k F_{i+1}$ in the sum belongs to Q, since $i + 1 \leq k$.

Differentiating the relation (2), we get

$$\frac{\partial f_i}{\partial x_i} = {h_i}^{s_i-1}\left(\frac{\partial u_i}{\partial x_i}h_i + s_i u_i \frac{\partial h_i}{\partial x_i}\right) + \sum_{k=i+1}^{n} \frac{\partial c_{ik}}{\partial x_i}h_k. \tag{3}$$

Then

$$h_i F_i = h_i \frac{\partial f_i}{\partial x_i}F_{i+1} = {h_i}^{s_i}\left(\frac{\partial u_i}{\partial x_i}h_i + s_i u_i \frac{\partial h_i}{\partial x_i}\right)F_{i+1} + h_i \sum_{k=i+1}^{n} \frac{\partial c_{ik}}{\partial x_i}h_k F_{i+1}.$$

The second summand in the right-hand sum belongs to Q because $h_k F_{i+1} \in Q$ whenever $i+1 \le k$. Having already seen that ${h_i}^{s_i} F_{i+1} \in Q$, we get that $h_i F_i \in Q$.

(2) We want now to prove that, if $F \notin Q$, then P is separable, or equivalently $\frac{\partial h_i}{\partial x_i} \notin P$ for all i.

Assume, for contradiction, there exists an index i such that $\frac{\partial h_i}{\partial x_i} \in P$. Since the set $\{h_1, \ldots, h_n\}$ is the reduced Gröbner basis for P and $\frac{\partial h_i}{\partial x_i}$ cannot be reduced by any of the h_i's, we have that $\frac{\partial h_i}{\partial x_i} \in P$ implies that $\frac{\partial h_i}{\partial x_i} = 0$.

Using (3),

$$F_i = \frac{\partial f_i}{\partial x_i}F_{i+1} = \left({h_i}^{s_i}\frac{\partial u_i}{\partial x_i} + \sum_{k=i+1}^{n} \frac{\partial c_{ik}}{\partial x_i}h_k\right)F_{i+1}$$

and therefore, as above, $F_i \in Q$; then also $F \in Q$, which is a contradiction.

(3) When $char(K) = 0$ or $char(K) > \max\{\deg_{x_i} f_i\}$, P is separable as follows from the beginning of part (2). Thus we need to show that, since P is separable, then $F \notin Q$. This will be proved by induction on the number n of variables.

If $n = 1$, then $I = (f_n)$, $Q = (q_n)$, $P = (h_n)$ with $q_n = {h_n}^{s_n}$, $f_n = u_n {h_n}^{s_n}$ and $\gcd(u_n, q_n) = 1$. Since P is separable, $\frac{\partial h_n}{\partial x_n} \notin P$. Differentiating the relation $f_n = u_n {h_n}^{s_n}$, we get

$$F_n = \frac{\partial f_n}{\partial x_n} = \frac{\partial u_n}{\partial x_n}{h_n}^{s_n} + s_n u_n \frac{\partial h_n}{\partial x_n}{h_n}^{s_n-1} = {h_n}^{s_n-1}\left(h_n \frac{\partial u_n}{\partial x_n} + s_n u_n \frac{\partial h_n}{\partial x_n}\right).$$

Assume, for contradiction, that $F_n \in Q$; then, since ${h_n}^{s_n-1} \notin Q$, we have that $h_n \frac{\partial u_n}{\partial x_n} + s_n u_n \frac{\partial h_n}{\partial x_n} \in P$ and hence $s_n u_n \frac{\partial h_n}{\partial x_n} \in P$. Because of the hypothesis on the characteristic and since $u_n \notin P$, this would imply that $\frac{\partial h_n}{\partial x_n} \in P$, which contradicts the separability of P.

Let us now prove the inductive step. Denote $P_2 = (h_2, \ldots, h_n)$; since P is separable, $\frac{\partial h_i}{\partial x_i} \notin P$ for all i and therefore P_2 is separable too. By the inductive hypothesis $F_2 = \frac{\partial f_2}{\partial x_2} \cdots \frac{\partial f_n}{\partial x_n} \notin Q_2$ and hence $F_2 \notin Q$. Observe that

$$F = \frac{\partial f_1}{\partial x_1}F_2 = \left({h_1}^{s_1-1}\left(\frac{\partial u_1}{\partial x_1}h_1 + s_1 u_1 \frac{\partial h_1}{\partial x_1}\right) + \sum_{k=2}^{n} \frac{\partial c_{1k}}{\partial x_1}h_k\right)F_2.$$

Assume, for contradiction, that $F \in Q$. As already said above, $\left(\sum_{k=2}^{n} \frac{\partial c_{1k}}{\partial x_1}h_k\right)F_2 \in Q$. Moreover ${h_1}^{s_1-1}F_2 \notin Q$, because $F_2 \in K[x_2, \ldots, x_n]$ and $F_2 \notin Q$. Thus we get that $\frac{\partial u_1}{\partial x_1}h_1 + s_1 u_1 \frac{\partial h_1}{\partial x_1} \in P$ and hence $s_1 u_1 \frac{\partial h_1}{\partial x_1} \in P$. Since $s_1 \neq 0$ and $u_1 \notin P$, we would get that $\frac{\partial h_1}{\partial x_1} \in P$ which is impossible. □

The previous proposition is a special case, with an elementary proof, of the Jacobian criterion in Eisenbud *et al.* (1992, Theorem 2.1). In that theorem the hypothesis that the characteristic is sufficiently large is included, whereas, using our proof, we show that $(I : F)$ gives a portion of the radical even when the characteristic is very small.

3. Derivations

This section shows how general derivations can be used to recover portions of the radical of an ideal.

Recall that a *derivation* on a ring R is a map $D : R \to R$ such that, for all $x, y \in R$,

$$D(x + y) = D(x) + D(y) \qquad \text{and} \qquad D(xy) = D(x)y + xD(y).$$

If J is an ideal in R and a derivation D is such that $D(J) \subseteq J$, then D induces a derivation on R/J.

In the case when $X = (x_1, \ldots, x_n)$ and $R = K[X]$, the next proposition shows that any derivation on $K[X]/I$ comes from a derivation on $K[X]$:

LEMMA 3.1. *Let I be an ideal in $K[X]$ and let D be a derivation on $K[X]/I$. Then there exists a derivation D^* of $K[X]$ such that $D^*(I) \subseteq I$ and which induces D on $K[X]/I$.*

PROOF. The derivation D is determined by $D_{|K}$ and by $D([x_i]) = a_i \in K[X]/I$ for all i. If we choose $b_i \in K[X]$ such that $[b_i] = a_i$, then it is enough to define D^* by setting ${D^*}_{|K} = D_{|K}$ and $D^*(x_i) = b_i$. □

LEMMA 3.2. *Let D be a derivation on a ring R and assume that J is an ideal of R such that $J = \bigcap_i M_i$, where M_i are pairwise coprime maximal ideals. Then $D(J) \subseteq J$ if and only if $D(M_i) \subseteq M_i$ for all i.*

PROOF. One implication being trivial, assume that $D(J) \subseteq J$. For each i, there exists $m_i \in \bigcap_{j \neq i} M_j$ and $m_i \notin M_i$. Then for every $x \in M_i$ we have that $D(xm_i) = D(x)m_i + xD(m_i) \in J \subseteq M_i$; so $D(x)m_i \in M_i$ and hence $D(x) \in M_i$. □

In the situation of Lemma 3.2, for each i the derivation D induces a derivation on the field R/M_i which, by abuse of language, we will also denote by D.

The derivations of a field K form a K-vector space Der_K. Any derivation D of a field K has a natural extension to $K[x]$ obtained by applying D to all coefficients of $f \in K[x]$, i.e. if $f(x) = \sum_i a_i x^i$ then $D(f)(x) = \sum_i D(a_i)x^i$.

DEFINITION 3.3. Let K be a field and D a derivation of $K[x]$. We will say that D is proper if, for every monic irreducible $f \in K[x]$ such that $D(f) \neq 0$, we have $\gcd(f, D(f)) = 1$.

For example, the map $f \to f'$ from $K[x] \to K[x]$, where $'$ denotes the ordinary derivation with respect to x, is a proper derivation. In addition, any derivation on K lifts to a proper derivation on $K[x]$.

DEFINITION 3.4. Let $\mathcal{B} = \{g_1, \ldots, g_m\}$ be a set of generators for a zero-dimensional ideal $I \subseteq R[x]$ and let D be a derivation on $R[x]$. We will denote by $D(\mathcal{B})$ the ideal of $R[x]$ generated by the polynomials $D(g_1), \ldots, D(g_m)$.

We will denote by $(I : L^\infty)$ the stable limit of $(I : L^n)$, i.e. the saturation of I by an ideal L.

Although in general the ideal $D(\mathcal{B})$ may depend on the chosen set of generators for I, for the quotient we have:

PROPOSITION 3.5. *Let $\mathcal{B} = \{g_1, \ldots, g_m\}$ be a set of generators for a zero-dimensional ideal $I \subseteq R[x]$. If $J = I \cap R$ is radical and D is a proper derivation on $R[x]$ such that $D(J) \subseteq J$, then*

(a) *the ideal $(I : D(\mathcal{B}))$ does not depend on the choice of $\mathcal{B}$, hence we can denote it simply by $(I : D(I))$*
(b) *the ideal $L = (I : D(I))$ is radical*
(c) *if $H = (I : L^\infty)$, then $(H : D(H)) = (1)$.*

PROOF. Let $J = \bigcap_i M_i$ be the decomposition of J as intersection of pairwise coprime maximal ideals in R. By Lemma 3.2 we have $D(M_i) \subseteq M_i$ for all i.

For any i denote by $\mathcal{B}_i$ a set of generators for (I, M_i) obtained as $\mathcal{B}_i = \mathcal{B} \cup \mathcal{S}_i$ where $\mathcal{S}_i \subset M_i$. Then

$$(I : D(\mathcal{B})) = \bigcap_i ((I, M_i) : D(\mathcal{B}_i)).$$

So it is sufficient to prove the result for each ideal (I, M_i), whose intersection with R is maximal; the thesis will follow directly from the fact that being radical is a local condition.

Therefore, with no loss of generality, we can assume that J is maximal.

(a) Observe that there exists $f \in R[x]$ such that $I = (f, J)$. So we have

$$f = \sum a_i g_i \qquad \text{and} \qquad g_i \equiv c_i f (\text{mod } J)$$

hence

$$D(f) = \sum D(a_i) g_i + \sum a_i D(g_i) \equiv \sum a_i D(g_i) (\text{mod } I)$$

and $$D(g_i) \equiv D(c_i) f + c_i D(f) \equiv c_i D(f) (\text{mod } I).$$

This proves that $D(\mathcal{B}) \equiv (D(f)) (\text{mod } I)$, which easily implies that $(I : D(\mathcal{B})) \equiv (f : D(f)) (\text{mod } J)$, and (a) follows.

(b) If $f = \prod_{j \in A} q_j(x)^{s_j}$ is the irreducible factorization of f in $(R/J)[x]$, then $(f : D(f)) = \left(\frac{f}{\gcd(f, D(f))}\right)$, and

$$\gcd(f, D(f)) = \prod_{j \in A_1} q_j(x)^{s_j - 1} \prod_{j \in A_2} q_j(x)^{s_j} \tag{4}$$

where $A_1 = \{j \in A \mid s_j D(q_j) \neq 0\}$ and $A_2 = \{j \in A \mid s_j D(q_j) = 0\}$.
Thus, modulo J, the ideal $(f : D(f)) \equiv \left(\prod_{j \in A_1} q_j(x)\right)$ is radical; hence the ideal $L = (I : D(I)) = ((f, J) : D(f))$ is radical.

(c) From (4) it follows that $H = (I : L^\infty) = \left(\prod_{j \in A_2} q_j(x)^{s_j}, J\right)$. By definition of A_2, we get that $D\left(\prod_{j \in A_2} q_j(x)^{s_j}\right) \in J$ and hence, using (a), $(H : D(H)) = (1)$. □

From the proof of point (c) in the previous proposition we have the following

COROLLARY 3.6. *With the notations of Proposition* 3.5*, let* $J = \bigcap_i M_i$ *be the decomposition of* J *as intersection of pairwise coprime maximal ideals in* R*. If* $H = \bigcap_i (h_i, M_i)$*, then* $D(h_i) \in M_i$ *for all* i*.*

PROPOSITION 3.7. *With the notations of Proposition* 3.5*, let* $\{D_1, \ldots, D_r\}$ *be a set of proper derivations on* $R[x]$ *such that* $D_i(J) \subseteq J$ *for all* $i = 1, \ldots, r$*. Then*

1. *the ideal* $L = (I : (D_1(I), \ldots, D_r(I)))$ *is radical*
2. *if* $H = (I : L^\infty)$*, then* $(H : D_j(H)) = (1)$ *for all* j
3. *if* $H = \bigcap(h_i, M_i)$*, then* $D_j(h_i) \in M_i$ $\forall i, j$*.*

PROOF. As in the proof of Proposition 3.5 we can reduce to the case when J is maximal in R and $I = (f, J)$. Let $f = \prod_{j \in A} q_j(x)^{s_j}$ be the irreducible factorization of f in $(R/J)[x]$. If

$$A_1 = \{j \in A | \exists k \text{ such that } s_j D_k(q_j) \neq 0\} \qquad \text{and} \qquad A_2 = \{j \in A |\ \forall k\ s_j D_k(q_j) = 0\},$$

then $L \equiv (f : (D_1(f), \ldots, D_r(f))) \equiv \big(\prod_{j \in A_1} q_j\big) (\text{mod } J)$.

Hence $(I : L^\infty) \equiv \big(\prod_{j \in A_2} {q_j}^{s_j}\big) (\text{mod } J)$.

In particular $D_i\big(\prod_{j \in A_2} {q_j}^{s_j}\big) \equiv 0 (\text{mod } J)$ for all i. □

COROLLARY 3.8. *With the notations of Proposition* 3.7*, it is possible to compute monic polynomials* $g_1, \ldots, g_s$ *and radical ideals* $J_1, \ldots, J_s \subseteq R$ *such that* $H = \bigcap(g_i, J_i)$*; moreover* $D_j(g_i) \in J_i$ $\forall i, j$*.*

PROOF. From Proposition 3.7 we know that, if $H = \bigcap(h_i, M_i)$, then $D_j(h_i) \in M_i$ $\forall i, j$.

Compute a Gröbner basis for H, say $\{p_1, \ldots, p_n, q_1, \ldots, q_t\}$ with $p_i \in R[x]$, $q_j \in R$, and consider the ideal $G_1 = (H, lc(p_2), \ldots, lc(p_n))$. Then (see, for instance, Gianni, 1989) a Gröbner basis for G_1 is of the form (g_1, S_1) where S_1 is a set of polynomials generating an ideal $J_1 \subseteq R$ such that $J_1 = \bigcap_{i \in B} M_i$ where $B = \{i \mid \deg h_i = \deg p_1\}$ and $g_1 \equiv h_i \pmod{M_i}$ $\forall i \in B$. Hence $D_j(g_1) \in M_i$ $\forall i, j$.

Write $H = G_1 \cap (H : G_1)$; by construction the ideal $H_1 = (H : G_1)$ is such that $(H_1 : D(H_1)) = (1)$; so we can iterate the previous construction. □

4. Radicals Over General Fields With Condition P

In this section we present a procedure to compute the radical of a zero-dimensional ideal I in $K[x_1, \ldots, x_n]$ where K is an arbitrary computable field of characteristic p.

Denote by G a Gröbner basis for I with respect to the lex order with $x_1 > x_2 > \cdots > x_n$. For any $m = 1, \ldots, n$ consider the mth elimination ideal $I_m = I \cap K[x_m, \ldots, x_n]$.

Our strategy to compute the radical of I is to start from the last elimination ideal, I_n, and add the next elimination ideal to the radical computed at the previous stage. Thus we are always working with an ideal whose contraction to the polynomial ring in one fewer variable is radical.

Under this hypothesis we will employ the following simplified notation. We will denote $R = K[x_2, \ldots, x_n]$ and $x = x_1$, so that $I \subseteq R[x]$. Moreover we will assume that $J = I \cap R$ is a radical ideal. We will denote with " ' " the derivation with respect to the variable x on $R[x]$ and with I' the ideal generated by the derivatives of generators of I.

If $J = \bigcap_i M_i$ is the decomposition of J as intersection of pairwise coprime maximal ideals in R, then we have $\sqrt{I} = \bigcap_i \sqrt{(I, M_i)}$ and I is radical if and only if each ideal (I, M_i) is radical.

Since, for any i, R/M_i is a field, the ideals $(I, M_i)/M_i$ are principal in $(R/M_i)[x]$; moreover, as is well known, (I, M_i) is radical if and only if the principal generator in $(R/M_i)[x]$ is square-free.

DEFINITION 4.1. Let I be a zero-dimensional ideal in $R[x]$ with $I \cap R = \bigcap_i M_i$ where M_i are maximal ideals in R. We will say that I is relatively separable over R if $R[x]/(I, M_i)$ is a separable algebra over R/M_i for all i.

We remark that a relatively separable ideal is also a radical ideal.

PROPOSITION 4.2. *Let I be a zero-dimensional ideal in $R[x]$ with $R = K[x_2, \ldots, x_n]$ and $char(K) = p$. Denote by d the maximum of the degrees (with respect to x) of the polynomials in some set of generators for I. Assume that $J = I \cap R$ is radical and consider the ideals $L = (I : I')$ and $Q = (I : L^\infty)$.*

1 *If $p = 0$ or $p > d$, then $\sqrt{I} = L$.*
2 *If $0 < p \leq d$, then $\sqrt{I} = L \cap \sqrt{Q}$ and the reduced Gröbner basis of Q is contained in $R[x^p]$.*

PROOF. (1) Using the arguments and notations of the proof of Proposition 3.5, since in our present hypothesis locally $\deg_x f \leq d$, then f has no inseparable factor; so $A_2 = \emptyset$ and $A_1 = A$.

(2) The fact that $\sqrt{I} = L \cap \sqrt{Q}$ follows easily from the proof of Proposition 3.5, since locally at each M_i we have

$$Q \equiv (f_i : (f_i : {f_i}')^\infty) \equiv \left(\prod_{A_{i2}} q_{ij}(x)^{s_{ij}} \right) \pmod{M_i}.$$

So, if we set $h_i = \prod_{A_{i2}} q_{ij}(x)^{s_{ij}}$, we have that ${h_i}'(x) = 0$ and hence $h_i \in R[x^p]$. Via the Chinese Remainder Theorem there exists $h \in R[x^p]$ such that $h \equiv h_i \pmod{M_i}$ and therefore $(h, J) = Q$. So the reduced Gröbner basis of Q is contained in $R[x^p]$. □

This is essentially a special case of Proposition 3.5 which shows that Q can be generated by polynomials in x^p; therefore this is true for a Gröbner basis of Q under any ordering.

COROLLARY 4.3. *Let I be a zero-dimensional ideal in $R[x]$ such that $I \cap R$ is radical. If $I = (I : I')$, then $I = \sqrt{I}$ with no restrictions on the characteristic.*

From now on we will restrict to the case when $0 < p \leq d$ and show how to complete the process by giving an algorithmic procedure for computing the radical of Q, the inseparable part of I.

DEFINITION 4.4. Let H be the ideal of $R[x]$ generated by the polynomials $\{h_1, \ldots, h_t\}$. We will denote by $H(x^{p^k})$ the ideal generated by the polynomials $h_1(x^{p^k}), \ldots, h_t(x^{p^k})$ obtained by evaluating the generators of H in x^{p^k}.

PROPOSITION 4.5. *Let I be a zero-dimensional ideal in $R[x]$ and assume that $J = I \cap R$ is radical. Then it is possible to compute a finite number of zero-dimensional, relatively separable ideals L_i in $R[x]$ such that*

$$\sqrt{I} = \bigcap \sqrt{L_j(x^{p^j})}.$$

PROOF. Consider the radical ideal $L_0 = (I : I')$.

If $L_0 = I$, then I is radical and we are done. So assume that $L_0 \neq I$ and consider $\widetilde{I_0} = (I : {L_0}^{\infty})$.

Recall that, by Proposition 4.2, $\sqrt{I} = L_0 \cap \sqrt{\widetilde{I_0}}$ and that the polynomials of the reduced Gröbner basis G of $\widetilde{I_0}$ are contained in $R[x^p]$.

Of course we can suppose $\widetilde{I_0} \neq (1)$, because otherwise $\sqrt{I} = L_0$ and we are done.

If, using the basis G, we set $I_1 = \widetilde{I_0}(x^{1/p})$, then $\sqrt{I} = L_0 \cap \sqrt{I_1(x^p)}$.

Start again with the ideal $I_1 \subseteq R[x]$, where the degrees in x have been divided by p, and consider

$$L_1 = (I_1 : {I_1}'), \quad \widetilde{I_1} = (I_1 : {L_1}^{\infty}) \qquad \text{and} \qquad I_2 = \widetilde{I_1}(x^{1/p}).$$

So $\sqrt{I_1} = L_1 \cap \sqrt{\widetilde{I_1}} = L_1 \cap \sqrt{I_2(x^p)}$ and

$$\sqrt{I} = L_0 \cap \sqrt{L_1(x^p)} \cap \sqrt{I_2(x^{p^2})}.$$

After a finite number of steps, we find I_n such that $\sqrt{I_n} = L_n$ with L_n relatively separable. The ideals $L_0, \ldots, L_n$ satisfy the thesis. □

The previous result holds for any field K, but it will represent an algorithm to compute the radical of I only if we are able to compute the radical of $L(x^{p^i})$ for any relatively separable ideal L and for all i.

Before seeing how we can compute the radical of $L(x^p)$, let us recall some results from Gianni and Trager (1996) that we will use.

LEMMA 4.6. (GIANNI AND TRAGER, 1996) *Let k be a field of characteristic p and let $f(x) \in k[x]$ be separable. Then $f(x^p)$ decomposes as $f(x^p) = (f_1(x))^p f_2(x^p)$, where $f_1(x)$ is separable, $f_2(x^p)$ is square-free, and $f_1(x)$ and $f_2(x^p)$ are coprime.*

LEMMA 4.7. (GIANNI AND TRAGER, 1996) *Let k be a field of characteristic p. If $f(x^p) \in k[x]$ is a square-free polynomial, then $f(x^{p^i})$ is also square-free for any integer $i \geq 1$.*

PROPOSITION 4.8. *Let L be a zero-dimensional, relatively separable ideal in $R[x]$ such that $L \cap R$ is radical. Let q be a polynomial such that $q \notin L(x^p)$ but $q \in \sqrt{L(x^p)}$. If we set $N = (L(x^p), q)$, then*

1. *$S = (N : N')$ is relatively separable*
2. *$T = (N : S^{\infty})$ is radical*
3. *$T(x^{p^i})$ is radical for all i*
4. *$\sqrt{L(x^p)} = S \cap T$.*

PROOF. If $J = L \cap R = \bigcap_i M_i$ is the decomposition of J as the intersection of maximal ideals in R, it is sufficient to prove that the thesis holds locally at each M_i, i.e. in $(R/M_i)[x]$. In other words we can assume that $L \subseteq k[x]$ with k a field of characteristic p.

By hypothesis L is generated by a separable polynomial $\varphi(x)$ and hence $L(x^p)$ is generated by $\varphi(x^p)$. By Lemma 4.6 we have that $\varphi(x^p) = h_1(x)^p h_2(x^p)$ with h_1 separable and $h_2(x^p)$ square-free.

Let r be a positive integer such that $q^r \in L(x^p) = (\varphi(x^p))$. Since $q \notin L(x^p)$, then $q(x) = c(x)h_1(x)^j h_2(x^p)^m$ with $j < p$ and for some $m \in \mathbf{N}$ and $c(x)$ coprime with $\varphi(x^p)$.

Then $N = (L(x^p), q)$ is generated by $\gcd(\varphi(x^p), q) = h_1(x)^j h_2(x^p)$.

Consequently $S = (N : N') = (h_1(x))$, so it is relatively separable (which was already assured by Proposition 3.5) and $T = (N : S^\infty) = (h_2(x^p))$, so T is radical since $h_2(x^p)$ is square-free.

Moreover, for all i, the ideal $T(x^{p^i})$ is generated by $h_2(x^{p^{i+1}})$ which is square-free by Lemma 4.7, so that it is radical.

Finally $\sqrt{L(x^p)} = (L(x^p), h_1(x)h_2(x^p)) = S \cap T$. □

The previous result guarantees that, if we can compute q such that $q \notin L(x^p)$ but $q \in \sqrt{L(x^p)}$, then we can compute algorithmically the radical of I.

Observe that

$$\sqrt{L(x^{p^2})} = \sqrt{S(x^p)} \cap \sqrt{T(x^p)} = \sqrt{S(x^p)} \cap T(x^p),$$

where we used the fact that $T(x^p)$ is already radical. Now S is separable, so we can compute $\sqrt{S(x^p)}$ using Proposition 4.8. Thus, applying iteratively Proposition 4.8, we are able to compute the radical of $L(x^{p^i})$ for any integer i, and hence $\sqrt{I}$ (see Proposition 4.5), if we can compute a polynomial q with the properties mentioned above.

As a matter of fact, it is enough to compute a q such that $q \notin L(x^p)$ but $q^p \in L(x^p)$.

In fact, if $L(x^p)$ is not radical, there exists a polynomial f such that $f \notin L(x^p)$ but $f^m \in L(x^p)$ for some positive integer m. If $m \leq p$, then also $f^p \in L(x^p)$ and $q = f$ has the requested property. If $m > p$ (and m is the least positive integer such that $f \notin L(x^p)$ but $f^m \in L(x^p)$), let s be the least positive integer multiple of p and greater than m, say $s = pr$. Then $q = f^r$ is a polynomial such that $q^p = f^{rp} = f^s \in L(x^p)$ since $s > m$; moreover $q \notin L(x^p)$ because $r \leq m$.

It will be possible to compute such an element q (and therefore to compute the radical of $L(x^p)$) if the field K satisfies a condition introduced by Seidenberg, who called it Condition P (see Seidenberg, 1974).

DEFINITION 4.9. Let K be a field of characteristic p. We say that K satisfies *Condition P* if, given a system of homogeneous linear equations over K, it is possible to decide if it has a non-trivial solution in K^p and, if so, exhibit one.

PROPOSITION 4.10. (SEIDENBERG, 1974) *If a computable field K satisfies Condition P, then so does any finitely generated extension of K.*

If K satisfies Condition P and I is a zero-dimensional ideal in $R[x]$, let us therefore see how we can compute an element q such that $q \notin I$ and $q^p \in I$.

Consider the finite dimensional vector space $R[x]/I$ over K and let $\{b_1, \ldots, b_r\}$ be a linear basis of it. In $R[x]/I$ the element q we are looking for can be written as

$q = \sum_i c_i b_i$ for suitable coefficients $c_i \in K$. Imposing that $q^p = 0$ modulo I, we get that $\sum_i {c_i}^p {b_i}^p = 0$. If we express each ${b_i}^p$ as a linear combination of the fixed basis, we get that $\sum_i {c_i}^p \left(\sum_j \alpha_{ij} b_j\right) = 0$, that is $\sum_j b_j \left(\sum_i \alpha_{ij} {c_i}^p\right) = 0$. The b_j's are linearly independent, which implies that $\sum_i \alpha_{ij} {c_i}^p = 0$. Since we are looking for a non-trivial solution in K^p, we can decide if it exists, and exhibit one, using Condition P.

5. Multiple Derivations and *p*th Powers

In the previous section we used derivations to reduce the problem of computing radicals to applying Condition P to ideals of the form $L(x^{p^k})$. Since Condition P can be very expensive to use, in this section we will see that, in the case when the ground field is finitely generated over a perfect field, we can use additional derivations to reduce the problem of computing radicals to computing pth roots.

Let us recall a result that, using derivations, characterizes the elements which are pth powers in a finitely generated extension K of a perfect field k.

THEOREM 5.1. (CF. LANG, 1984) *Let K be a finitely generated extension of a perfect field k. Then*

- *the K-vector space Der_K has dimension equal to the transcendence degree of K over k*
- *if $\beta \in K$, then $\beta \in K^p \iff D(\beta) = 0 \ \forall D \in Der_K$.*

We intend to generalize this result to the case of finitely generated K-algebras; as a first step we will examine how to find a generating set of derivations on such algebras.

Let therefore K be a finitely generated extension of a perfect field k. Assume $J = (f_1, \ldots, f_m)$ is a zero-dimensional ideal in $R = K[y_1, \ldots, y_n]$ and consider the finitely generated K-algebra $A = R/J$.

First of all observe that, if J is radical, since A is isomorphic to a finite product of fields k_i, there exists a $1-1$ correspondence between Der_A and $\prod Der_{k_i}$ induced by the projections $\pi_i : A \to k_i$.

If $s = tr.deg._k K$, denote by $\widetilde{D_1}, \ldots, \widetilde{D_s}$ a basis of the s-dimensional K-vector space Der_K. If $Y = (y_1, \ldots, y_n)$, for any $g \in R$, $g = \sum_{I \in \mathbf{N}^n} a_I Y^I$, denote

$$D_i(g) = \frac{\partial g}{\partial y_i} \qquad i = 1, \ldots, n$$
$$D_i(g) = \sum_{I \in \mathbf{N}^n} \widetilde{D_{i-n}}(a_I) Y^I \qquad i = n+1, \ldots, n+s.$$

So we have a set $\{D_1, \ldots, D_{n+s}\}$ of derivations on R and we can consider the $m \times (n+s)$ matrix Jac whose (i,j)-entry is defined by

$$Jac_{i,j} = D_j(f_i).$$

A derivation D of $K[Y]$ induces a derivation of $A = K[Y]/J$ if and only if $D(J) \subseteq J$; the matrix Jac provides a method to characterize such derivations:

PROPOSITION 5.2. *Let $v = (v_1, \ldots, v_{n+s}) \in K[Y]^{n+s}$. Then the following facts are equivalent:*

1. $D = \sum_{i=1}^{n+s} v_i D_i$ *is such that* $D(J) \subseteq J$
2. $\forall j = 1, \ldots, m \qquad \sum_{i=1}^{n+s} v_i D_i(f_j) \equiv 0 \, (mod \; J)$
3. $Jac \cdot v \equiv 0 \, (mod \; J)$.

Thus the syzygies of the Jacobian matrix modulo J generate the derivations on A.

PROPOSITION 5.3. *Let K be a field and J a radical, zero-dimensional ideal in $K[Y]$. Consider the K-algebra $A = K[Y]/J$ and let α be an element in A. Then $D(\alpha) = 0$ for all $D \in Der_A$ if and only if there exists $\beta \in A$ such that $\alpha = \beta^p$.*

PROOF. Since J is radical, A is isomorphic to a finite product of fields k_i and any derivation on A induces a derivation on k_i and vice versa. So our thesis follows from the analogous result for derivation on fields (see Theorem 5.1). □

PROPOSITION 5.4. *Let $R = K[Y]$. Let I be an ideal in $R[x]$ and $J = I \cap R = \bigcap M_i$. Denote $D_0 = \frac{\partial}{\partial x}$ and let $D_1, \ldots, D_r$ be a set of generators of the derivations on R/J. Define $L = (I : (D_0(I), \ldots, D_r(I)))$ and $H = (I : L^\infty)$. Then*

1. $\sqrt{I} = L \cap \sqrt{H}$
2. *it is possible to compute monic polynomials $g_1, \ldots, g_s$ and radical ideals $J_1, \ldots, J_s$ such that $H = \bigcap (g_i, J_i)$, $g_i \equiv {h_i}^p (\text{mod } J_i)$.*

PROOF. By Proposition 3.7 L is radical and by Corollary 3.8 we can compute monic polynomials $g_1, \ldots, g_s$ and radical ideals $J_1, \ldots, J_s \subseteq R$ such that $D_j(g_i) \in J_i \; \forall i, j$. We can assume that g_i is reduced modulo J_i.

Since $D_0(g_i) \in J_i \subseteq R$ and g_i is reduced modulo J_i, then $D_0(g_i) = 0$ for all i, which implies that $g_i(x, Y) = \widetilde{g_i}(x^p, Y)$. Since also $D_j(\widetilde{g_i}(x^p, Y)) \in J_i \; \forall j > 0$ and $D_1, \ldots, D_r$ generate all the derivations on R/J, the coefficients of the $\widetilde{g_i}$'s are pth powers modulo J_i by Proposition 5.3. Hence there exists $h_i \in R[x]$ such that $g_i \equiv {h_i}^p \pmod{J_i}$. □

As a result of the previous proposition we have constructed polynomials which are known to be pth powers modulo radical ideals and we need to construct their pth roots. After computing the h_i's which are the pth roots of g_i, we apply our radical construction to the ideals (h_i, J_i) in order to finish the computation.

One approach to computing pth roots is to use Condition P; we should note that the situation is improved since, with respect to the previous section, we are using Condition P in the algebra R/J which is a lower dimensional subalgebra. In our situation J is a radical, zero-dimensional ideal in $K[Y]$; let $\{b_1, \ldots, b_r\}$ be a basis of the K-algebra $B = K[Y]/J$. If $q = \sum_i c_i b_i$, with $c_i \in K$, is an element of B^p, then there exists an element $a = \sum_i a_i b_i$ with $a_i \in K$ such that $a^p = q$. If we express each ${b_i}^p$ as a linear combination of the fixed basis, say ${b_i}^p = \sum_j \beta_{ij} b_j$, then the coefficients a_i are solutions of the system $\sum_i \beta_{ij} {a_i}^p = c_j$.

In order to find a solution $(a_1, \ldots, a_r)$ of the latter system, we can think of using Condition P which, however, deals with the existence of non-trivial solutions in K^p only for homogeneous systems. Nevertheless we can find a solution of our system by solving the homogeneous system $\sum_i \beta_{ij} {a_i}^p - c_j t = 0$ where t is an additional unknown, because all the non-trivial solutions of this system have the last entry different from 0 since the radical algebra B contains no nilpotent elements.

The situation turns out to be simpler when the K-algebra is separable over K, in fact recall that

PROPOSITION 5.5. *Let B be a finite dimensional K-algebra and let $\{b_1, \ldots, b_r\}$ be a basis of B. If B is separable then $\{{b_1}^p, \ldots, {b_r}^p\}$ is a basis of B.*

PROOF. It is enough to prove that $\{{b_1}^p, \ldots, {b_r}^p\}$ are linearly independent over K. Otherwise let $\sum_i c_i {b_i}^p = 0$ be a non-trivial dependence relation with $c_i \in K$. In some finite extension $\tilde{K}$ of K there exists a_i such that ${a_i}^p = c_i$. Consider $\sum_i a_i b_i$; this element is nilpotent in $B \otimes_K \tilde{K}$, but that would imply that B is not separable, which is a contradiction. □

Therefore in this case the matrix (β_{ij}) is invertible so the system $\sum_i \beta_{ij} {a_i}^p = c_j$ has a unique solution $({a_1}^p, \ldots, {a_r}^p)$ and computing the a_i's reduces to compute pth roots in the field K. Since K is finitely generated over a perfect field, this problem is constructive (see Gianni and Trager, 1996).

6. Higher Dimensional Ideals

To conclude this paper we want to show how to use the computation obtained for zero-dimensional ideals in order to compute the radical of ideals of any dimension.

Given an ideal I of positive dimension d one can determine a set of variables $\{x_{i_1}, \ldots, x_{i_d}\}$ such that $I \cap K[x_{i_1}, \ldots, x_{i_d}] = 0$. Such a maximal independent set can be found using a Gröbner basis for I under any term ordering as explained in Becker and Weispfenning (1993).

Without loss of generality we will relabel the variables so that our independent set is $\{x_1, \ldots, x_d\}$. The ideal $I^e = IK(x_1, \ldots, x_d)[x_{d+1}, \ldots, x_n]$ is zero-dimensional and we can compute its radical using the result in the previous section. After computing $L = \sqrt{I^e}$, we need to contract L back to the original polynomial ring, i.e. compute $L^c = L \cap K[x_1, \ldots, x_n]$. This contraction can be performed by saturating with respect to a principal ideal as in the following proposition:

PROPOSITION 6.1. (GIANNI *et al.*, 1988) *Let $G = \{f_1, \ldots, f_k\}$ be a Gröbner basis for an ideal $I \subseteq K(x_1, \ldots, x_d)[x_{d+1}, \ldots, x_n]$ under any term ordering. We can assume that the f_i are monic and we compute a polynomial $g \in K[x_1, \ldots, x_d]$ such that $gf_i \in K[x_1, \ldots, x_n]$ for all $1 \leq i \leq k$; then we have:*

$$I \cap K[x_1, \ldots, x_n] = (gt - 1, gf_1, \ldots, gf_k) \cap K[x_1, \ldots, x_n]$$

where t is a new variable.

This allows us to compute $L^c = \sqrt{I^e} \cap K[x_1, \ldots, x_n]$ which is a radical ideal whose associated primes are the associated primes of I whose intersection with $K[x_1, \ldots, x_d]$ is zero. We must now find a complementary ideal J such that $\sqrt{I} = L^c \cap \sqrt{J}$. One way to compute such a J is to use a simple corollary to Proposition 6.1.

COROLLARY 6.2. (GIANNI *et al.*, 1988) *Let $G = \{f_1, \ldots, f_r\}$ be the reduced Gröbner basis of an ideal $I \subseteq K[x_1, \ldots, x_d][x_{d+1}, \ldots, x_n]$ under a block term ordering. Assume that $I \cap K[x_1, \ldots, x_d] = 0$ and let $I^{ec} = IK(x_1, \ldots, x_d)[x_{d+1}, \ldots, x_n] \cap K[x_1, \ldots, x_n]$.*

If we denote by $g \in K[x_1, \ldots, x_d]$ the lcm of the leading coefficients of the polynomials f_i, then we have:

$$\sqrt{I} = \sqrt{I^{ec}} \cap \sqrt{(I, g)}.$$

COROLLARY 6.3. *Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal of dimension $d > 0$, where K is a computable field satisfying Condition P. Then it is possible to compute the radical of I.*

PROOF. Let S be a maximal independent set for I and let $X = \{x_1, \ldots, x_n\}$. Let I^e be the extension of the ideal I to $K(S)[X - S]$ and I^{ec} be the contraction of I^e to $K[X]$. We have

$$\sqrt{I} = \sqrt{(I, g)} \cap \sqrt{I^{ec}} = \sqrt{(I, g)} \cap (\sqrt{I^e})^c.$$

Now I^e is a zero-dimensional ideal, and (I, g) is an ideal where S is no longer a maximal set of independent variables. So repeating this process, we reduce the problem to the computation of radicals of zero-dimensional ideals. □

One problem with this kind of construction, though, is that in general the ideal (I, g) can have some components which contain some components of I^{ec} and are thus redundant. Since we want to compute the radical and so we are not concerned about multiplicity, we can avoid this problem. In fact, as remarked in both Alonso *et al.* (1991) and Caboara *et al.* (1997), the redundancies can be eliminated by replacing (I, g) by the saturation of I by $\sqrt{I^{ec}}$, since the following holds:

PROPOSITION 6.4. *Let $I \subset J$ be ideals, then we have*

$$\sqrt{I} = \sqrt{J} \cap \sqrt{I : J^\infty}$$

and the associated primes of $(I : J^\infty)$ are the associated primes of I which do not contain J.

In Alonso *et al.* (1991) it is shown that, by first putting the ideal in a sufficiently general position, one can replace the general saturation in the previous proposition, by saturating with respect to a suitable principal ideal. However arguments requiring general linear changes of coordinates require special handling when the coefficient fields are finite.

7. Examples

EXAMPLE 1. The following "challenge" ideal was presented in Eisenbud *et al.* (1992).

Let $I = (x^7 - zyu^5, y^4 - z^3u) \subseteq Z_7[x, y, z, u]$. This ideal is two-dimensional but it is in *Noether normal form* and equidimensional, so we can consider directly its zero-dimensional extension to the ring $Z_7(z, u)[x, y]$.

We proceed as in Section 1 by computing the univariate projections. Since the second generator is separable, it is enough to add the square-free part of the generator of $I \cap Z_7(z, u)[x]$; this polynomial is $x^{28} - u^{21}z^7$ and its square-free part is $x^4 - u^3z$. Then $(I, x^4 - u^3z) = (xz^2 - y^3, y^4 - uz^3)$ is a radical ideal in $Z_7(z, u)[x, y]$. Now it remains to compute the contraction to $Z_7[x, y, z, u]$. Since the lcm of the leading coefficients is z^2, it is enough to compute the saturation with respect to z, finally yielding the radical of the original ideal I

$$\sqrt{I} = (x^3 - yu^2, y^3 - xz^2, x^2z - y^2u, xy - zu).$$

EXAMPLE 2. Let $I = (x^p - u, y^p - u) \subseteq Z_p(u)[x, y]$, where u is transcendental over Z_p. This ideal is zero-dimensional and the two generators are square-free, but this ideal is not radical. This example shows that it is not sufficient that I contains square-free univariate polynomials in each variable in order that I be radical, unless the coefficient field is perfect. Although Z_p is perfect, $Z_p(u)$ is not. If we let $R = Z_p(u)[y]$, then $J = I \cap R = (y^p - u)$ is radical since it is principal, generated by a square-free polynomial. $I' = 0$, so to finish the computation we need to choose a strategy: in this example we use derivations. The only derivation on R/J is $\frac{\partial}{\partial y}$, so, since $\frac{\partial(x^p-u)}{\partial x} = 0$ and $\frac{\partial(x^p-u)}{\partial y} = 0$ we deduce that $x^p - u$ is a pth power modulo $(y^p - u)$. We need then to compute the pth root of u modulo $(y^p - u)$: this is y, then $(x^p - u) = (x - y)^p$ modulo $(y^p - u)$ and so the radical is the ideal $(x - y, y^p - u)$.

EXAMPLE 3. Let $I = (x^6 + 2x^3y^3 + 1, y^4 + y^2 + 1) \subseteq Z_3[x, y]$. First we compute the radical of the contracted ideal $M = (y^4 + y^2 + 1)$. Let $J = (M : M') = (y^2 + 2)$. Since $(M : J^2) = (1)$, we have that $J = \sqrt{M}$. Now consider the ideal $(I, J) = (x^6+2x^3y+1, y^2+2)$ and call it again I. Then $I' = 0$, so we compute $I_1 = I(x^{1/3}) = (x^2 + 2xy + 1, y^2 + 2)$. Moreover $L_1 = (I_1 : I'_1) = (x + y, y^2 + 2)$. Since $\deg_x I_1 < 3$, we have that $L_1 = \sqrt{I_1}$. The final step is to compute the radical of $L_1(x^3) = (x^3 + y, y^2 + 2)$. Since there are no non-trivial derivations on Z_3 we immediately obtain that $x^3 + y$ is a perfect cube modulo $(y^2 + 2)$. The algebra $Z_3[y]/(y^2 + 2)$ is separable, so we can find the cubic root of y by solving a 2×2 linear system over Z_3. In this case we find that $y^3 = y$ so that $x^3 + y = (x + y)^3$ modulo $(y^2 + 2)$ and then the radical of I is $(x + y, y^2 + 2)$.

Acknowledgement

This research was partially performed with the contribution of M.U.R.S.T.

References

Alonso, M. E., Mora, T., Raimondo, M. (1991). Local decomposition algorithms. In *Proceedings of AAECC-8 (Tokyo, 1990)*, Springer LNCS **508**, pp. 208–221.

Becker, T., Weispfenning, V. (1993). *Gröbner Bases. A Computational Approach to Commutative Algebra*. New York, NY, Springer.

Caboara, M., Conti, P., Traverso, C. (1997). Yet another ideal decomposition algorithm. In *Proceedings of AAECC (Toulouse, 1997)*, Springer LNCS **1255**, pp. 39–54.

Eisenbud, D., Huneke, C., Vasconcelos, W. (1992). Direct methods for primary decomposition. *Invent. Math.*, **110**, 207–235.

Gianni, P. (1989). Properties of Gröbner bases under specializations. In *EUROCAL '87 (Leipzig, 1987)*, pp. 293–297. Berlin, Springer.

Gianni, P., Trager, B. (1996). Square-free algorithms in positive characteristic. *Appl. Algebra Eng. Commun. Comput.*, **7**, 1–14.

Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.*, **6**, 149–167.

Kemper, G. (2000). The calculation of radical ideals in positive characteristic. (Preprint).

Krick, T., Logar, A. (1991). An algorithm for the computation of the radical of an ideal in the ring of polynomials. In *Proceedings of AAECC-9 (New Orleans, 1991)*, Springer LNCS **539**, pp. 195–205.

Lakshman, Y. N. (1990). On the complexity of computing Gröbner bases for zero-dimensional polynomial ideals. Ph.D. Thesis, Rensselaer Polytechnic Institute, New York.

Lang, S. (1984). *Algebra*, 2nd edn. Reading, MA, Addison-Wesley Publishing Company Advanced Book Program.

Matsumoto, R. (2001). Computing the radical of an ideal in positive characteristic. *J. Symb. Comput.*, **32**, 263–271.

Mines, R., Richman, F., Ruitenburg, W. (1988). *A Course in Constructive Algebra*. New York, NY, Springer.
Seidenberg, A. (1974). Constructions in algebra. *Trans. Am. Math. Soc.*, **197**, 273–313.
Vasconcelos, W. (1991). Jacobian matrices and constructions in algebra. In *Proceedings of AAECC-9 (New Orleans, 1991)*, Springer LNCS **539**, pp. 48–64.