

Irreducible decomposition of polynomial ideals[☆]

E. Fortuna^{a,*}, P. Gianni^a, B. Trager^b

^a*Dipartimento di Matematica, Università di Pisa, Via F. Buonarroti 2, I-56127 Pisa, Italy*

^b*IBM T.J. Watson Research Center, Route 134, Yorktown Heights, NY 10598, USA*

Received 16 September 2003; accepted 1 November 2004

Abstract

In this paper we present some algorithms for computing an irreducible decomposition of an ideal in a polynomial ring $R = K[x_1, \dots, x_n]$ where K is an arbitrary effective field.

© 2005 Elsevier Ltd. All rights reserved.

Keywords: Polynomial ideals; Irreducible decomposition; Duality

1. Introduction

In this paper we present some algorithms for computing an irreducible decomposition of an ideal in a polynomial ring $R = K[x_1, \dots, x_n]$ where K is an arbitrary effective field. Some of the earliest proofs of primary decomposition were based on the existence of an irreducible decomposition, using the fact that every irreducible ideal is primary, even though not every primary ideal is irreducible. Although the isolated primary components of an ideal are unique, the irreducible components are not. However the number of irreducible components in an irredundant decomposition is uniquely determined. In fact in Gröbner (1934) it is shown that in zero-dimensional local rings there is a special ideal, the socle, such that the minimal number of its generators is precisely the minimal number of irreducible components of the zero ideal. For each generator of the socle, Gröbner shows

[☆] This research was partially performed with the contribution of M.U.R.S.T. and of Eurocontract HPRN-CT-2001-00271.

* Corresponding author. Tel.: +39 050 2213226; fax: +39 050 2213224.

E-mail addresses: fortuna@dm.unipi.it (E. Fortuna), gianni@dm.unipi.it (P. Gianni), bmt@us.ibm.com (B. Trager).

that the largest ideal in the local ring which does not contain that generator must be irreducible and the set of these ideals gives a minimal decomposition of the zero ideal. This is an important characterization of irreducible decompositions, but does not directly lead to a constructive algorithm.

Given a primary ideal, we can localize to reduce to the zero-dimensional case. If we then form the quotient ring modulo that zero-dimensional ideal, we get a finite-dimensional algebra. We will show how to exploit the relationship between this algebra and its dual module in order to find the irreducible components of the zero ideal using linear algebra.

Our discussion of dual modules is in the same context as that contained in Heiß et al. (2002); we do not necessarily assume that the zeros of our ideal are contained in the ground field, unlike for instance Marinari et al. (1993) and Mourrain (1997). Thus we do not use techniques such as inverse systems; instead we use an explicit presentation of the dual module as the dual vector space of our finite-dimensional algebra.

We then examine the situation when the algebra is isomorphic to its dual module. Such algebras are Gorenstein rings and have been intensively studied e.g. in Bass (1963), Buchsbaum and Eisenbud (1977) and Huneke (1999). In this case one can compute irreducible components of primary ideals simply using ideal quotients. If we extract the subideal generated by the monic elements in a Gröbner basis of our original ideal, we obtain a complete intersection. The quotient algebra formed using this subideal is isomorphic to its dual module. Thus exploiting the relationship between our original ideal and the constructed complete intersection subideal, we obtain a simple, direct approach to determining its irreducible components.

We next extend our construction to the non-local case. We show how to express any zero-dimensional ideal as an intersection of ideals whose primary components are irreducible, i.e. whose quotient rings are locally Gorenstein. If we want to minimize the number of components in this representation, we need to be able to find a minimal set of generators for finitely generated modules over zero-dimensional rings. We present an algorithm for finding these minimal generators without first performing a primary decomposition as was done in Heiß et al. (2002).

This decomposition of ideals into components whose quotient rings are locally Gorenstein is interesting from both a numerical and an algebraic point of view. As observed in Becker et al. (1996), these Gorenstein rings (also called Frobenius algebras) have the property that the eigenspaces associated with the linear operator of multiplication by a generic element are all one-dimensional. Thus fixed-point techniques converging to the eigenspace can be used, leading to numerically stable algorithms for finding the zeros of the original polynomial ideal. Becker et al. (1996) have also noted that Frobenius algebras possess non-degenerate bilinear forms, which have been used by Mourrain and Pan (1999) to develop asymptotically fast algorithms for solving polynomial systems.

2. Duality

In this section we assume that A is a finite-dimensional K -algebra. Recall that $\hat{A} = \text{Hom}_K(A, K)$ has a natural structure of an A -module using the map $A \times \hat{A} \rightarrow \hat{A}$ given by $(a, f) \rightarrow a \cdot f$ where $a \cdot f$ is the K -linear map defined by $(a \cdot f)(x) = f(ax) \forall x \in A$. We

will denote by $\langle g_1, \dots, g_t \rangle$ the A -module generated by $g_1, \dots, g_t \in \widehat{A}$ and by (a_1, \dots, a_s) the ideal of A generated by $a_1, \dots, a_s \in A$.

Definition 2.1. (1) For any ideal I of A , denote by I^\perp the submodule of \widehat{A}

$$I^\perp = \{f \in \widehat{A} \mid f(x) = 0 \ \forall x \in I\}.$$

(2) For any submodule H of \widehat{A} , denote by H^\perp the ideal of A

$$H^\perp = \{x \in A \mid h(x) = 0 \ \forall h \in H\}.$$

It is immediate that:

Proposition 2.2. For any ideals I_1, I_2 of A and for any submodules H_1, H_2 of \widehat{A} , we have

- (a) $I_1 \subseteq I_2 \implies I_1^\perp \supseteq I_2^\perp$ and $H_1 \subseteq H_2 \implies H_1^\perp \supseteq H_2^\perp$
- (b) $(I_1 + I_2)^\perp = I_1^\perp \cap I_2^\perp$ and $(H_1 + H_2)^\perp = H_1^\perp \cap H_2^\perp$
- (c) $I_1^{\perp\perp} = I_1$ and $H_1^{\perp\perp} = H_1$
- (d) $(I_1 \cap I_2)^\perp = I_1^\perp + I_2^\perp$ and $(H_1 \cap H_2)^\perp = H_1^\perp + H_2^\perp$.

Thus we have a 1–1 order reversing correspondence between the lattice of ideals of A and the lattice of submodules of \widehat{A} . This duality also gives us a natural way to decompose ideals:

Corollary 2.3. Given an ideal I of A and generators $\{g_1, \dots, g_k\}$ of I^\perp as an A -module, we have that

$$I = \bigcap_{i=1}^k \langle g_i \rangle^\perp.$$

A set of generators for an ideal (resp. for a submodule of a module) will be called *irredundant* if no proper subset of it generates the same ideal (resp. submodule). Note that if the set of generators $\{g_1, \dots, g_k\}$ in the previous corollary is irredundant, then by duality the induced decomposition of I is irredundant, meaning that no $\langle g_i \rangle^\perp$ can be dropped.

Recall that an ideal is called *irreducible* if it is not the intersection of two strictly larger ideals. When A is a local ring, Nakayama's Lemma guarantees that the components of the decomposition obtained in [Corollary 2.3](#) are irreducible as shown in the following proposition:

Proposition 2.4. If A is a zero-dimensional local ring, then, for any $f \in \widehat{A}$, $\langle f \rangle^\perp$ is an irreducible ideal of A .

Proof. Assume that $\langle f \rangle^\perp$ is not irreducible, say $\langle f \rangle^\perp = I_1 \cap I_2$ with I_1, I_2 ideals of A properly containing $\langle f \rangle^\perp$. Then $\langle f \rangle = \langle f \rangle^{\perp\perp} = (I_1 \cap I_2)^\perp = I_1^\perp + I_2^\perp$. If g_1, \dots, g_s generate I_1^\perp and g_{s+1}, \dots, g_t generate I_2^\perp , then, by Nakayama's Lemma, there exists j such that g_j generates $I_1^\perp + I_2^\perp$. If, for instance, $g_j \in I_1^\perp$, then $I_2^\perp \subseteq I_1^\perp$; hence $I_1 \subseteq I_2$ which is impossible. \square

Proposition 2.5. Let I be an ideal of A . If I is irreducible, then there exists $g \in \widehat{A}$ such that $I^\perp = \langle g \rangle$.

Proof. Let h_1, \dots, h_m be generators of I^\perp , so that $I^\perp = \langle h_1 \rangle + \dots + \langle h_m \rangle$. Then $I = I^{\perp\perp} = \bigcap_{i=1}^m \langle h_i \rangle^\perp$. Since I is irreducible, there exists i such that $I = \langle h_i \rangle^\perp$ and hence $I^\perp = \langle h_i \rangle^{\perp\perp} = \langle h_i \rangle$. \square

3. Irreducible decomposition of primary ideals

Definition 3.1. Let I be an ideal of R . A set of irreducible ideals $\{Q_i\}_{i=1,\dots,s}$ is called an irredundant irreducible decomposition (for short, an IID) of I if $I = \bigcap_{i=1}^s Q_i$ and $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$ for all i .

As is well known, any ideal in R can be expressed as the intersection of finitely many irreducible ideals; although the irreducible components are not unique, their number is independent of the irredundant representation chosen (see [Noether, 1921](#)).

Since every irreducible ideal is primary, in this section we will describe an effective procedure for computing an irredundant irreducible decomposition of a P -primary ideal Q of R .

We first observe that all the irreducible components of a P -primary ideal are P -primary:

Lemma 3.2. Let Q be a P -primary ideal and let $Q = \bigcap_{i=1}^s Q_i$ be an irredundant irreducible decomposition of Q . Then, for all i , Q_i is a P -primary ideal.

Proof. Up to reordering, we can assume that $\{1, \dots, k\} = \{i \mid \sqrt{Q_i} = P\}$. If $k = s$ we are done. Otherwise, we can write $Q = \bigcap_{i=1}^k Q_i \cap \bigcap_{i=k+1}^s Q_i$, where $\bigcap_{i=1}^k Q_i$ is a P -primary ideal, while $\bigcap_{i=k+1}^s Q_i \not\subseteq P$. If $x \in \bigcap_{i=k+1}^s Q_i \setminus P$, we have that $Q = (Q : x) = (\bigcap_{i=1}^k Q_i : x) \cap (\bigcap_{i=k+1}^s Q_i : x) = \bigcap_{i=1}^k Q_i$, which contradicts the fact that the decomposition was irredundant. \square

Now we reduce to the case when Q is zero-dimensional. If, up to reordering, $\{x_1, \dots, x_d\}$ is a maximal set of variables such that $Q \cap K[x_1, \dots, x_d] = (0)$, then the ideal $Q\tilde{R} \subseteq \tilde{R} = K(x_1, \dots, x_d)[x_{d+1}, \dots, x_n]$ is zero-dimensional, $P\tilde{R}$ -primary and $Q\tilde{R} \cap R = Q$. So, if $Q\tilde{R} = \bigcap_{i=1}^s \tilde{Q}_i$ is an IID for $Q\tilde{R}$, then, by [Lemma 3.2](#), \tilde{Q}_i is $P\tilde{R}$ -primary for all i . Hence $Q = \bigcap_{i=1}^s (\tilde{Q}_i \cap R)$ is an IID for Q , since there exists a 1–1 correspondence between P -primary ideals in R and $P\tilde{R}$ -primary ideals in \tilde{R} .

Thus, from now on we will assume that the ideal $Q \subset K[x_1, \dots, x_n]$ is zero-dimensional and primary. Moreover it is sufficient to solve the problem in $A = R/Q = \pi(R)$, which is a local ring in addition to being a finite-dimensional K -vector space: if $(0) = \bigcap_{i=1}^s \overline{Q}_i$ is an IID for the ideal (0) , then $Q = \bigcap_{i=1}^s \pi^{-1}(\overline{Q}_i)$ is an IID for Q .

In order to find an IID for the ideal (0) in a local finite-dimensional K -algebra A with maximal ideal P , by [Corollary 2.3](#) and [Proposition 2.4](#) it is sufficient to find an irredundant set of generators for $(0)^\perp = \hat{A}$. Observe that, since A is local, by Nakayama's Lemma any irredundant set of generators of an ideal in A is a *minimal basis* of the ideal, that is a set of generators of minimal cardinality in the family of all sets of generators.

It will be helpful to consider the ideal

$$S = (0 : P) = \{x \in A \mid xP = (0)\},$$

called the *socle* of A . Since $PS = (0)$, the ideal S is also an A/P -vector space, and, by Nakayama's Lemma, any basis of S as an A/P -vector space is a minimal basis of S as an ideal.

Another useful property of the socle is the following:

Proposition 3.3. *For any ideal $I \neq (0)$ of A , we have $S \cap I \neq (0)$.*

Proof. There exists $r \in \mathbb{N}$ such that $P^r = (0)$. Let $n \in \mathbb{N}$ be the minimal integer such that $P^n I = (0)$. Then $(0) \neq P^{n-1} I \subseteq S \cap I$. \square

We can use the socle to find a minimal set of generators for $(0)^\perp = \widehat{A}$:

Theorem 3.4. *Let $\{u_1, \dots, u_s\}$ be a minimal set of generators for the socle S and let $\{c_1 = 1, c_2, \dots, c_r\}$ be a K -vector space basis for A/P . Consider the sr elements $\{u_1, c_2 u_1, \dots, c_r u_1, \dots, u_s, \dots, c_r u_s\}$ which form a K -vector space basis for the socle S . Denote by $U = \{\widehat{u}_1, \dots, \widehat{u}_s\} \subset \widehat{A}$ a set of linear maps such that $\widehat{u}_i(u_i) = 1$ and $\widehat{u}_i(u_j c_k) = 0$ for $i \neq j$ and $\forall k = 1, \dots, r$. Then U is a minimal set of generators for \widehat{A} as an A -module.*

Proof. To prove that the elements of U generate \widehat{A} , it is enough to show that $J = \langle U \rangle^\perp$ is the ideal (0) in A .

Using Proposition 2.2 we see that $J = \langle U \rangle^\perp = \bigcap_{i=1}^s \langle \widehat{u}_i \rangle^\perp$. If on the contrary J is non-zero, then $J \cap S$ is also non-zero. Let v be a non-zero element of $J \cap S$ and write $v = \sum_{i=1}^s a_i u_i$ with $a_i \in A$. Since $v \neq 0$, we can assume for instance that $a_1 u_1 \neq 0$; thus $a_1 \notin P$ because $PS = (0)$.

For all $a \in A$ we can write $\bar{a} \in A/P$ as $\bar{a} = \sum_{i=1}^r r_i c_i$ with $r_i \in K$; hence $a = \sum_{i=1}^r r_i c_i + p$ for some $p \in P$. Thus $au_j = \sum_{i=1}^r r_i c_i u_j$ and so Au_j is generated as a K -vector space by $\{c_1 u_j, \dots, c_r u_j\}$. Since $\widehat{u}_1(c_i u_j) = 0$ for all $i = 1, \dots, r$ and for all $j = 2, \dots, s$, then $(A\widehat{u}_1)(u_j) = \widehat{u}_1(Au_j) = 0$ and thus $u_j \in \langle \widehat{u}_1 \rangle^\perp \quad \forall j = 2, \dots, s$. This implies that $a_1 u_1 = v - \sum_{i=2}^s a_i u_i \in \langle \widehat{u}_1 \rangle^\perp$. The element a_1 is invertible because $a_1 \notin P$, so we would get $u_1 \in \langle \widehat{u}_1 \rangle^\perp$ which is a contradiction as $\widehat{u}_1(u_1) = 1$.

Thus we have shown that $J = (0)$ and that the elements of U generate \widehat{A} . To show that these generators are minimal, it is enough to observe that if we exclude \widehat{u}_j from our set of generators, then the element u_j is contained in all the other $\langle \widehat{u}_k \rangle^\perp$ and hence their intersection is non-zero. \square

Note that the maps \widehat{u}_i are not uniquely determined by the conditions requested in the previous statement; any such set of maps will do the job.

Corollary 3.5. *The ideals $\mathcal{Q}_i = \langle \widehat{u}_i \rangle^\perp$, $i = 1, \dots, s$, give an irredundant irreducible decomposition of (0) . In particular the number of irreducible components coincides with the dimension of S as an A/P -vector space.*

To make this decomposition effective we will also need to compute the kernels of the principal submodules generated by each of the functionals $\widehat{u}_1, \dots, \widehat{u}_s$. Let $\{u_1, \dots, u_s, u_{s+1}, \dots, u_p\}$ be a basis of A as a K -vector space. Recall that $x \in \langle \widehat{u}_i \rangle^\perp$ if and only if, for all $j = 1, \dots, p$, we have $(u_j \cdot \widehat{u}_i)(x) = \widehat{u}_i(xu_j) = 0$. If we write $x = \sum_{h=1}^p b_h u_h$ in terms of the linear basis $\{u_1, \dots, u_p\}$ with coefficients $b_h \in K$, we get

that $x \in \langle \widehat{u}_i \rangle^\perp$ if and only if $\widehat{u}_i(xu_j) = \widehat{u}_i(\sum_{h=1}^P b_h u_h u_j) = \sum_{h=1}^P b_h \widehat{u}_i(u_h u_j) = 0$ for all j , and so the b_h 's are the solutions of this linear system.

By [Theorem 3.4](#), if we know a minimal set of generators for the socle S , and hence in particular a basis of S as an A/P -vector space, we get an IID of (0) . We can extract a minimal basis of S from a set of generators using the module Σ of syzygies of S and Gaussian elimination (see [Greuel and Pfister, 2002](#)). Namely, an element s in a set of generators is redundant if and only if there exists a syzygy in Σ in which the coefficient of s is invertible, i.e. it does not belong to P . Once we have removed this element, we can find the syzygies among the remaining generators by Gaussian elimination.

An alternative approach is based on the following:

Proposition 3.6. *It is possible to compute a minimal set of generators for any ideal L of a local finite-dimensional K -algebra (A, P) .*

Proof. Consider first the case when L is an A/P -vector space. Let $\{u_1, \dots, u_m\}$ be any set of generators for the ideal L and compute a basis $\{c_1 = 1, c_2, \dots, c_r\}$ of A/P as a K -vector space. We can assume that $u_1 \neq 0$. For $j = 2, \dots, m$ remove u_j from the list of generators if $u_j \in \text{Span}_{A/P}(u_1, \dots, u_{j-1})$, which we can test by checking if $u_j \in \text{Span}_K(c_1 u_1, \dots, c_r u_1, \dots, c_1 u_{j-1}, \dots, c_r u_{j-1})$. The set $\{u_1, \dots, u_s\}$ we get at the end of this process is a basis of L as an A/P -vector space and therefore, by Nakayama's Lemma, a minimal set of generators for L as an ideal.

In the case of a general ideal L , we note that $\overline{L} = L/PL$ is an A/P -vector space. Representatives in L of an A/P -vector space basis of \overline{L} , which can be computed as before, will be a minimal basis for L . \square

In [Gröbner \(1934\)](#) it is proved that, if $\{b_1, \dots, b_s\}$ is a minimal basis for the socle S and L_i is a maximal ideal in A not containing b_i , then $\{L_1, \dots, L_s\}$ is an IID of (0) . Using the previous results, we can give a constructive version of Gröbner's theorem.

4. Principal dual modules

In this section we will consider the case when \widehat{A} is generated by one single functional over A , say $\widehat{A} = \langle \phi \rangle$. If g_1, \dots, g_k are generators of a submodule of \widehat{A} , then each g_i is a multiple of ϕ , i.e. $g_i = a_i \phi$ for some $a_i \in A$. Thus the submodule of \widehat{A} generated by the g_i 's can also be represented by operating on ϕ with the ideal in A generated by the a_i 's, and we have:

Lemma 4.1. *If $\widehat{A} = \langle \phi \rangle$, then there is a one-to-one correspondence between ideals of A and submodules of \widehat{A} :*

$$(I \subseteq A) \longleftrightarrow (\langle I\phi \rangle \subseteq \widehat{A}).$$

Lemma 4.2. *If $\widehat{A} = \langle \phi \rangle$ and I is an ideal of A such that $\phi(I) = 0$, then $I = (0)$.*

Proof. If $\phi(I) = 0$, then also $(A\phi)(I) = \phi(IA) = \phi(I) = 0$, so I is contained in $\langle \phi \rangle^\perp = (\widehat{A})^\perp = (0)$. \square

Using the previous properties, we can express orthogonals in terms of quotients:

Proposition 4.3. *If $\widehat{A} = \langle \phi \rangle$, then for any ideal $I \subseteq A$ and for any A submodule $\langle J\phi \rangle \subseteq \widehat{A}$ we have*

$$I^\perp = \langle (0 : I)\phi \rangle$$

$$\langle J\phi \rangle^\perp = (0 : J).$$

Proof. Let $I^\perp = \langle L\phi \rangle$ for some ideal $L \subseteq A$. Then $\phi(IL) = L\phi(I) = 0$; hence $IL = (0)$ and therefore $L \subseteq (0 : I)$. Since $((0 : I)\phi)(I) = 0$, then $\langle (0 : I)\phi \rangle \subseteq I^\perp$ and hence $(0 : I) \subseteq L$. Thus $L = (0 : I)$.

The second identity is proved similarly. \square

Corollary 4.4. *If $\widehat{A} = \langle \phi \rangle$ and $I \subseteq A$, then*

$$(0 : (0 : I)) = I.$$

We have thus obtained a well known duality for ideals in zero-dimensional Gorenstein rings, that already appeared in Gröbner (1934).

Corollary 4.5. *Let $I \subseteq A$ be an ideal and let $(0 : I) = (a_1, \dots, a_k)$. If $\widehat{A} = \langle \phi \rangle$, then:*

- (1) $I = \bigcap_{i=1}^k (0 : a_i)$.
- (2) *The decomposition above is irredundant if and only the generating set is irredundant.*
- (3) *If we also assume that A is local, then any ideal of the form $(0 : a)$ is irreducible.*

Proof. (1) $I^\perp = \langle (0 : I)\phi \rangle = \langle a_1\phi, \dots, a_k\phi \rangle$; hence we have $I = \bigcap_{i=1}^k \langle a_i\phi \rangle^\perp = \bigcap_{i=1}^k (0 : a_i)$.

(2) and (3) easily follow from the results of Section 2. \square

In particular we remark that the computation of the previous decomposition for I does not require the knowledge of a specific generator of \widehat{A} .

The previous results suggest a second strategy for computing an irreducible decomposition of a zero-dimensional primary ideal. The key observation we will use is that, if a zero-dimensional ideal $I \subseteq R = K[x_1, \dots, x_n]$ is a complete intersection, then $A = R/I$ is Gorenstein and hence $\widehat{A} \cong A$ (see e.g. Kunz, 1985 or Eisenbud, 1996).

Lemma 4.6. *Let Q be a zero-dimensional P -primary ideal in R and consider q_1, \dots, q_n , with $q_i \in K[x_i, \dots, x_n]$, the polynomials in the reduced lex Gröbner basis for Q such that each q_i is monic in x_i . Then the ideal $J = (q_1, \dots, q_n)$ is P -primary.*

Proof. The thesis immediately follows from the structure theorem for Gröbner bases for primary zero-dimensional ideals in Gianni et al. (1988). The theorem asserts that, if \mathcal{G} is the reduced lex Gröbner basis for Q , then $\mathcal{G} = \{q_{11}, \dots, q_{1s_1}, \dots, q_{n1}\}$ where

- (i) $q_{ij} \in K[x_i, \dots, x_n]$,
- (ii) q_{i1} is monic in x_i and $q_{i1} \equiv h_i^{k_i} \pmod{\sqrt{Q} \cap K[x_{i+1}, \dots, x_n]}$ with h_i an irreducible polynomial,
- (iii) $q_{ij} \equiv 0 \pmod{\sqrt{Q} \cap K[x_{i+1}, \dots, x_n]}$ for all $j > 1$.

Then $\sqrt{J} = (h_1, \dots, h_n) = P$ and hence the zero-dimensional ideal J is P -primary. \square

Thus, by [Lemma 4.6](#), the ideal J generated by the monic elements in the reduced lex Gröbner basis for the zero-dimensional primary ideal Q is primary. Since it is also a complete intersection, then $A = R/J$ is zero-dimensional, local and Gorenstein. Consider $\overline{Q} = Q/J$ and, using the method given above, compute a minimal basis of generators f_1, \dots, f_s for the ideal $(0 : \overline{Q})$ in A . Then $\{(0 : f_i)\}_{i=1, \dots, s}$ is an irredundant irreducible decomposition for \overline{Q} in A and $\{(J : f_i)\}_{i=1, \dots, s}$ is an irredundant irreducible decomposition for Q in R . This shows:

Proposition 4.7. *Let Q be a zero-dimensional primary ideal in R and denote by J the ideal of R generated by the monic elements in the reduced Gröbner basis for Q in lex order. Let f_1, \dots, f_s be a minimal set of generators for the ideal $(0 : Q/J)$. Then $Q = \bigcap_{i=1}^s (J : f_i)$ is an IID for Q .*

Remark 4.8. Note that to compute $(J : f_i)$ we can exploit the fact that J is zero-dimensional and therefore one can use algorithms based on linear algebra (see [Lakshman, 1990](#) and [Möller and Tenberg, 2001](#)).

5. Decomposition of zero-dimensional ideals

In this section we will obtain a decomposition into locally irreducible components for a zero-dimensional ideal of R , not necessarily primary. First of all observe that:

Proposition 5.1. *Let I be a zero-dimensional ideal in R and denote by J the ideal of R generated by the monic elements in a reduced Gröbner basis for I (with respect to any fixed monomial ordering). Let f_1, \dots, f_s be any set of generators for the ideal $(J : I)$. Then*

- (a) $I = \bigcap_{i=1}^s (J : f_i)$.
- (b) *The components $(J : f_i)$ are locally irreducible (i.e. their primary components are irreducible).*

Proof. Since J is a complete intersection, R/J is Gorenstein. As we observed before, this implies that $\widehat{R/J}$ is a principal R/J -module and the decomposition of [Corollary 4.5](#) applies. \square

Remark 5.2. A similar decomposition (computed without Gröbner bases) was used in [Dickenstein and Sessa \(1991\)](#) to reduce the problem of ideal membership to complete intersection ideals.

The construction used in [Proposition 5.1](#) also allows us to obtain a presentation of $\widehat{R/I}$ as an R/I -module that does not require the knowledge of a primary decomposition for I , unlike [Heiß et al. \(2002\)](#). Namely:

Corollary 5.3. *Let I and J be as in [Proposition 5.1](#). Then $\widehat{R/I} \cong (J : I)/J$.*

Proof. Let $A = R/J$. Then $R/I \cong A/(I/J)$ and therefore $\widehat{R/I} \cong \widehat{A/(I/J)}$. Thus, as an R/I -module, $\widehat{R/I}$ is isomorphic to $\{f \in \widehat{A} \mid f(I/J) = 0\} = (I/J)^\perp$. On the other hand, since $A \cong \widehat{A} = \langle \phi \rangle$, we have also that $(I/J)^\perp = \langle (0 : (I/J))\phi \rangle \cong (J : I)/J$ as an R/I -module. \square

Proposition 5.1 gives a decomposition of any zero-dimensional ideal into components $(J : f_i)$ such that $R/(J : f_i)$ is Gorenstein. Note that this decomposition does not require polynomial factorization and could be used to produce simpler components of ideals as a preliminary step to primary decomposition. In the case of polynomial rings in two variables, these components are complete intersections (see Eisenbud, 1996); properties of Gorenstein rings in three variables were explored in Buchsbaum and Eisenbud (1977).

Example. Let $I = (x^2y^2 + x^2y, y^4 + 2y^3 + y^2, x^3 - xy^2 - xy)$ be an ideal given by its Gröbner basis under graded reverse lex ordering. In this case $J = (y^4 + 2y^3 + y^2, x^3 - xy^2 - xy)$ and hence $(J : I) = (y^2 + y, x)$. So we can decompose I as

$$\begin{aligned} I &= (J : y^2 + y) \cap (J : x) \\ &= (x^3, y^2 + y) \cap (y^4 + 2y^3 + y^2, x^2 - y^2 - y) = I_1 \cap I_2. \end{aligned}$$

The ideals I_1 and I_2 are complete intersections and their primary components are irreducible, since $I_1 = (x^3, y+1) \cap (x^3, y)$ and $I_2 = (y^2+2y+1, x^2+y+1) \cap (x^2-y, y^2)$.

From the previous results we also get the following characterization of zero-dimensional Gorenstein rings:

Corollary 5.4. *Let I and J be as in Proposition 5.1. Then R/I is Gorenstein if and only if there exists $f \in R$ such that $I = (J : f)$.*

If the elements f_1, \dots, f_s in Proposition 5.1 are chosen to be a minimal set of generators of $(0 : I/J)$, then the decomposition given in Proposition 5.1 is minimal among the decompositions of that form.

We now present an algorithm for computing a minimal set of generators for a finitely generated R/J -module; we can apply this algorithm to $(0 : I/J)$ to obtain a shortest decomposition in Proposition 5.1. This will also construct the required polynomial f in Corollary 5.4 in the case when R/I is Gorenstein.

Let A be a finite-dimensional K -algebra and M a finitely generated A -module. The problem of finding a minimal basis for M is, by Nakayama's Lemma, equivalent to solving the same problem for the (A/\sqrt{A}) -module $M/\sqrt{A}M = (A/\sqrt{A}) \otimes_A M$, where \sqrt{A} denotes the Jacobson radical of A . So we can assume that $\sqrt{A} = (0)$.

Observe also that, if $A = K[x_1, \dots, x_n]/L$, then $A/\sqrt{A} \cong K[x_1, \dots, x_n]/\sqrt{L}$.

Denote by P_1, \dots, P_t the prime (and therefore maximal) ideals of A , and $T = \{1, \dots, t\}$. In our situation $\sqrt{A} = (0) = \bigcap_{i \in T} P_i$. In particular

$$A \cong \prod_{i \in T} A/P_i \cong \prod_{i \in T} A_{P_i}.$$

Any basis of M projects onto a set of generators of M_{P_i} for all i ; if the basis is also minimal, as an easy consequence of the Chinese Remainder Algorithm there exists at least one index i such that its projection is a basis of M_{P_i} as an A_{P_i} -vector space. Hence any minimal basis must contain as many elements as the maximal dimension of the localizations of M .

Obviously, a necessary condition for an element $m \in M$ to belong to a minimal basis for every localization M_{P_i} of M is that $m_{P_i} \neq 0$ for all i ; in such a case m cannot be a zero-divisor in M , that is $(0 : m) = (0)$.

It will therefore be helpful to consider some properties of $(0 : m)$, the annihilator of m , in our situation:

Proposition 5.5. *For all $m \in M$ we have*

$$(0 : m) = \bigcap_{i \in T_1} P_i$$

where $T_1 = \{i \in T \mid m_{P_i} \neq 0\}$.

Proof. Observe that if $m_{P_i} \neq 0$ then $(P_i : m) = P_i$; else $(P_i : m) = (1)$. Hence

$$(0 : m) = \bigcap_{i \in T} (P_i : m) = \bigcap_{i \in T_1} P_i. \quad \square$$

Corollary 5.6. *For all $m \in M$ we have*

- (1) $(0 : m) = (0)$ if and only if $m_{P_i} \neq 0$ for all i .
- (2) $(0 : (0 : m)) = (0 : (\bigcap_{i \in T_1} P_i)) = \bigcap_{i \in T \setminus T_1} P_i$.
- (3) $(0 : m) + (0 : (0 : m)) = (1)$.
- (4) $(0 : m) \cap (0 : (0 : m)) = (0)$.
- (5) $(0 : m) = (1)$ in $A/(0 : (0 : m))$.

The previous results suggest a method for computing a minimal set of generators \mathcal{B} for the module M starting from any set of generators m_1, \dots, m_k .

Let $N_1 = (0 : m_1)$.

If $N_1 = (1)$, then m_1 is redundant and we discard it.

If $N_1 = (0)$, then we insert m_1 in \mathcal{B} and continue the computation working in $M/\langle m_1 \rangle$ with $\overline{m_2}, \dots, \overline{m_k}$ as generators.

Finally, if $(0) \neq N_1 \neq (1)$, we denote $N_2 = (0 : (0 : m_1))$ and, for $i = 1, 2$, we consider the A_i -module $M_i = A_i \otimes_A M$ where $A_i = A/N_i$. Then we can continue our search for minimal generators working independently in M_1 and in M_2 : over A_1 we have $(0 : m_1) = (0)$, and hence m_1 can belong to a minimal basis for the localizations M_P at all primes P in A_1 ; instead, by Corollary 5.6, step (5), over A_2 we have $(0 : m_1) = (1)$, and hence m_1 is redundant and we can discard it.

If we know two minimal bases $\mathcal{B}_1 = \{m_1^{(1)}, \dots, m_{k_1}^{(1)}\}$ and $\mathcal{B}_2 = \{m_1^{(2)}, \dots, m_{k_2}^{(2)}\}$ respectively for M_1 and M_2 , we can reconstruct a minimal basis for M over A using the following procedure, based on the Chinese Remainder Algorithm, that we will denote by CRA-M($\mathcal{B}_1, \mathcal{B}_2, N_1, N_2$). First of all, if, say, \mathcal{B}_2 has fewer elements than \mathcal{B}_1 , we extend \mathcal{B}_2 by zero elements until it has as many elements as \mathcal{B}_1 . Next we compute $n_i \in N_i$ such that $n_1 + n_2 = 1$. Then the set $\{m_i\}_{i=1, \dots, k_1}$, where $m_i = n_2 m_i^{(1)} + n_1 m_i^{(2)}$, is a set of generators for M ; moreover they are also a minimal basis since, by construction, they are a minimal basis in at least one localization M_{P_i} .

The previous procedures can be implemented by the following algorithm:

MIN-GEN($M, N, \mathcal{M}, \mathcal{B}$)

Input :

N a zero-dimensional radical ideal of $K[x_1, \dots, x_n]$, $A = K[x_1, \dots, x_n]/N$,

M an A -module,

\mathcal{B} , a minimal set of generators of a submodule of M ,

$\mathcal{M} = \{m_1, \dots, m_k\}$, elements of M such that $\mathcal{M} \cup \mathcal{B}$ generates M .

Output : a minimal set of generators for M .

$\mathcal{M} = \emptyset \implies \mathcal{B}$

-- basic recursive step

$m := m_1$

$N_1 := (\langle \mathcal{B} \rangle : m)$

$\mathcal{M} := \mathcal{M} \setminus \{m\}$

-- case 1: m is redundant

$N_1 = (1) \implies \text{MIN-GEN}(M, N, \mathcal{M}, \mathcal{B})$

-- case 2: m is a good element in all localizations

$N_1 \subset N \implies \text{MIN-GEN}(M, N, \mathcal{M}, \mathcal{B} \cup \{m\})$

-- case 3: m is a good element for the localizations at a proper subset of

-- primes; we select them, split the module M and reconstruct a minimal

-- basis via Chinese Remainder Theorem

$N_2 := (N : N_1)$

$M_1 := A/N_1 \otimes_A M$

$M_2 := A/N_2 \otimes_A M$

$\text{CRA-M}(\text{MIN-GEN}(M_1, N_1, \mathcal{M}, \mathcal{B} \cup \{m\}), \text{MIN-GEN}(M_2, N_2, \mathcal{M}, \mathcal{B}), N_1, N_2)$

Corollary 5.7. *If L is a zero-dimensional radical ideal of $R = K[x_1, \dots, x_n]$, $A = R/L$ and M is the A -module generated by the elements m_1, \dots, m_k , then $\text{MIN-GEN}(M, L, \{m_1, \dots, m_k\}, \emptyset)$ is a minimal set of generators for M .*

References

- Bass, H., 1963. On the ubiquity of Gorenstein rings. *Math. Z.* 82, 8–28.
- Becker, E., Cardinal, J.P., Roy, M.-F., Szafraniec, Z., 1996. Multivariate Bezoutians, Kronecker symbol and Eisenbud–Levine formula. In: *Algorithms in Algebraic Geometry and Applications*. Santander, 1994. In: *Progr. Math.*, vol. 143. Birkhäuser, Basel.
- Buchsbaum, D.A., Eisenbud, D., 1977. Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3. *Amer. J. Math.* 99, 447–485.
- Dickenstein, A., Sessa, C., 1991. Duality methods for the membership problem. In: *Effective Methods in Algebraic Geometry*. Castiglione, 1990. In: *Progr. Math.*, vol. 94. Birkhäuser, Boston.
- Eisenbud, D., 1996. Commutative algebra with a view toward algebraic geometry. In: *Graduate Texts in Math.*, vol. 150. Springer-Verlag, New York.
- Gianni, P., Trager, B., Zacharias, G., 1988. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Comput.* 6, 149–167.
- Greuel, G., Pfister, G., 2002. *A Singular Introduction to Commutative Algebra*. Springer-Verlag, Berlin.
- Gröbner, W., 1934. Über irreduzible Ideale in kommutativen Ringen. *Math. Ann.* 110, 197–222.
- Heiß, W., Oberst, U., Pauer, F., 2002. On inverse systems and squarefree decomposition of zero-dimensional polynomial ideals. In: *Proceedings of LMCS 2002*. RISC-Linz, Hagenberg, pp. 147–161.
- Huneke, C., 1997. Hyman Bass and ubiquity: Gorenstein rings. In: *Algebra, K-theory, groups, and education*. In: *Contemp. Math.*, vol. 243. Amer. Math. Soc., New York, pp. 55–78.
- Kunz, E., 1985. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser Boston Inc., Boston.
- Lakshman, Y.N., 1990. On the complexity of computing Gröbner bases for zero dimensional polynomial ideals. Ph.D. Thesis, Rensselaer Polytechnic Institute, New York.
- Marinari, M.G., Möller, H.M., Mora, T., 1993. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Appl. Algebra Engrg. Comm. Comput.* 4, 103–145.

- Möller, H.M., Tenberg, R., 2001. Multivariate polynomial system solving using intersections of eigenspaces. *J. Symbolic Comput.* 32 (5), 513–531.
- Mourrain, B., 1997. Isolated points, duality and residues. *J. Pure Appl. Algebra* 117–118, 469–493.
- Mourrain, B., Pan, V., 1999. Asymptotic acceleration of solving multivariate polynomial systems of equations. In: *STOC '98*. Dallas, TX. ACM, New York, pp. 488–496.
- Noether, E., 1921. Idealtheorie in Ringbereichen. *Math. Ann.* 83, 24–66.