Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
23(2) (2007), 105–114
www.emis.de/journals
ISSN 1786-0091

PRIMARY DECOMPOSITION OF MODULES OVER DEDEKIND DOMAINS USING GRÖBNER BASES

OSWALDO LEZAMA AND HÉCTOR SUÁREZ

Abstract. In [6] was proved that if R is a principal ideal domain and $N \subset M$ are submodules of $R[x_1, \ldots, x_n]^s$, then the primary decomposition for N in M can be computed using Gröbner bases. In this paper we extend this result to Dedekind domains. The procedure that computed the primary decomposition is illustrated with an example.

1. Introduction

Let $N \subset M$ be submodules of $R[X]^s$, where $R[X] = R[x_1, \ldots, x_n]$ is the polynomial ring over the Noetherian commutative ring R. In [6] is presented the algorithm MPD that computes the primary decomposition of N in M using Gröbner bases when R is a principal ideal domain. In this paper we prove that the procedure MPD could be adapted if we assume that R is a Dedekind domain.

The algorithm MPD in [6] is supported in some preliminary results that we will adapt in Section 3. For this purpose we will establish other additional results that we will prove in Section 2. Examples illustrating the algorithm MPD are not included in [6], we will show in Section 4 an example for this algorithm following the procedure described in Theorem 15 of Section 3.

2. Preliminary results

In this section we present some preliminary results that we will use in Section 3.

Proposition 1. *Let R be an integral domain and $f, g \in R - \{0\}$. Then $T = \{f^\mu g^\nu | \mu, \nu \geq 0\}$ is a multiplicative system of R and*

$$R[X]_{f,g} \cong R[X, y, z]/\langle yf - 1, zg - 1\rangle.$$

2000 *Mathematics Subject Classification.* 13P10, 13F05.
Key words and phrases. Dedekind domains, primary decomposition, modules, Gröbner bases.

Proof. $0 \notin T$, $1 = f^0 g^0 \in T$ and $(f^\kappa g^\lambda)(f^\mu g^\nu) = f^{\kappa+\mu} g^{\lambda+\nu} \in T$. We define

$$\begin{aligned} R[X, y, z] &\xrightarrow{\alpha} R[X]_{f,g} \subset K(X) \\ p(X, y, z) &\mapsto p\Big(X, \frac{1}{f}, \frac{1}{g}\Big), \end{aligned}$$

where K is the field of fractions of R and $K(X)$ is the field of fractions of $R[X]$. We note that α is a ring homomorphism. Moreover, α is surjective since $\frac{a(X)}{f^\mu g^\nu} = \alpha\big(a(X) y^\mu z^\nu\big)$. Now, we will prove that $ker(\alpha) = \langle yf - 1, zg - 1\rangle$. Let $p(X, y, z) \in \langle yf-1, zg-1\rangle$ then $p(X, y, z) = h(X, y, z)(yf-1)+t(X, y, z)(zg-1)$, with $h(X, y, z), t(X, y, z) \in R[X, y, z]$, and hence, $\alpha(p(X, y, z)) = 0$. Thus, $\langle yf - 1, zg - 1\rangle \subseteq ker(\alpha)$. On the other hand, let $p(X, y, z) \in ker(\alpha)$, then $p(X, \frac{1}{f}, \frac{1}{g}) = 0$, but $p(X, y, z) \in (R[X])[y, z] \subset K(X)[y, z]$, from this we get that $(\frac{1}{f}, \frac{1}{g})$ is a zero of $p(X, y, z)$. Thus, $\{(\frac{1}{f}, \frac{1}{g})\} \subseteq V(\langle p\rangle)$, where $V(\langle p\rangle)$ is the variety of the ideal generated by $p = p(X, y, z)$ (see [3]). Then, $I(V(\langle p\rangle)) \subseteq I(\{(V(\frac{1}{f}, \frac{1}{g})\})$, i.e., $\langle p\rangle \subseteq \langle y - \frac{1}{f}, z - \frac{1}{g}\rangle$. Hence, $p(X, y, z) = a'(X, y, z)(y - \frac{1}{f}) + b'(X, y, z)(z - \frac{1}{g})$ with $a'(X, y, z), b'(X, y, z) \in K(X)[y, z]$.

Eliminating denominators we find $w \in R[X]-\{0\}$ such that $wfgp(X, y, z) = a(X, y, z)(yf - 1) + b(X, y, z)(gz - 1)$ with $a(X, y, z), b(X, y, z) \in R[X, y, z]$. Then, $wfgp(X, y, z) \in \langle yf - 1, gz - 1\rangle \subseteq R[X, y, z]$. But, $\langle yf - 1, gz - 1\rangle$ is a prime ideal of $R[X, y, z]$. In fact, $\{(\frac{1}{f}, \frac{1}{g})\}$ is an irreducible algebraic set, then $\langle y-\frac{1}{f}, z-\frac{1}{g}\rangle$ is a prime ideal of $K(X)[y, z]$, but $\langle y-\frac{1}{f}, z-\frac{1}{g}\rangle = \langle yf-1, zg-1\rangle$ in $K(X)[y, z]$. Thus, $\langle yf-1, zg-1\rangle$ is a prime ideal of $K(X)[y, z]$. We consider the canonical inclusion $R[X, y, z] \xrightarrow{\iota} K(X)[y, z]$, then $\iota^{-1}(\langle yf - 1, gz - 1\rangle) = \langle yf - 1, gz - 1\rangle$ is a prime ideal of $R[X, y, z]$.

Now, we can conclude the proof. From $wfgp(X, y, z) \in \langle yf - 1, gz - 1\rangle$ we get that $wfg \in \langle yf - 1, gz - 1\rangle$ or $p(X, y, z) \in \langle yf - 1, gz - 1\rangle$. If $wfg \in \langle yf - 1, gz - 1\rangle$, then $wfg = c(yf - 1) + d(gz - 1)$ with $c, d \in R[X, y, z]$. Setting $y = \frac{1}{f}$ and $z = \frac{1}{g}$ we get $wfg = 0$, but this is impossible. Hence, $p(X, y, z) \in \langle yf - 1, gz - 1\rangle$. □

The previous result can be extended to any finite set of nonzero elements of R including the well known case $t = 1$.

Corollary 2. *Let R be an integral domain and $f_1, \ldots, f_t \in R - \{0\}$, $t \geq 1$. Then,*

$$R[X]_{f_1,\ldots,f_t} \cong R[X, y_1, \ldots, y_t]/\langle y_1 f_1 - 1, \ldots, y_t f_t - 1\rangle.$$

From this corollary we get the following computational property.

Proposition 3. *Let R be an integral domain, $f_1, \ldots, f_t \in R-\{0\}$, $t \geq 1$, and I an ideal of $R[X]$. Then,*

$$IR[X]_{f_1,\ldots,f_t} \cap R[X] = \langle I, y_1 f_1 - 1, \ldots, y_t f_t - 1\rangle R[X, y_1, \ldots, y_t] \cap R[X].$$

Proof. We consider the canonical homomorphism

$$\varphi : R[X] \to R[X]_{f_1,\dots,f_t}$$
$$p(X) \mapsto \frac{p(X)}{1}.$$

$IR[X]_{f_1,\dots,f_t}$ is the ideal of $R[X]_{f_1,\dots,f_t}$ generated by $\varphi(I)$, so

$$IR[X]_{f_1,\dots,f_t} = \Big\{ \frac{h(X)}{f^{\mu_1}\dots f^{\mu_t}} | h(X) \in I, \mu_1, \dots, \mu_t \geq 0 \Big\}.$$

By the above corollary we have the isomorphism

$$R[X, y_1, \dots, y_t]/\langle y_1 f_1 - 1, \dots y_t f_t - 1\rangle \overset{\overline{\alpha}}{\cong} R[X]_{f_1,\dots,f_t}$$

and also

$$\overline{\alpha}(\langle I, y_1 f_1 - 1, \dots y_t f_t - 1\rangle R[X, y_1, \dots, y_t]/\langle y_1 f_1 - 1, \dots y_t f_t - 1\rangle) = IR[X]_{f_1,\dots,f_t}.$$

We observe that $R[X] \hookrightarrow R[X, y_1, \dots, y_t]/\langle y_1 f_1 - 1, \dots y_t f_t - 1\rangle$. In fact, we define $p(X) \mapsto \overline{p(X)}$, if $\overline{p(X)} = \overline{0}$ then $p(X) \in \langle y_1 f_1 - 1, \dots y_t f_t - 1\rangle$, and hence $p(X) = c_1(y_1 f_1 - 1) + \cdots + c_t(y_t f_t - 1)$ with $c_i \in R[X, y_1, \dots, y_t]$, $1 \leq i \leq t$. Setting $y_i = \frac{1}{f_i}$ we get $p(X) = 0$. From this we have that $IR[X]_{f,g} \cap R[X]$ coincides with $\langle I, y_1 f_1 - 1, \dots y_t f_t - 1\rangle R[X, y_1, \dots, y_t] \cap R[X]$. $\square$

This result is a particular case of the following more general property.

Theorem 4. *Let N, M be submodules of $R[X]^s$ and $f_1, \dots, f_t \in R[X] - \{0\}$, $t \geq 1$, then*

$$N_{f_1,\dots,f_t} \cap M = (NR[X, y_1, \dots, y_t] + (y_1 f_1 - 1)R[X, y_1, \dots, y_t]^s + \cdots +$$
$$+ (y_t f_t - 1)R[X, y_1, \dots, y_t]^s) \cap M.$$

Proof. The proof is an easy adaptation of the proof of the previous proposition. $\square$

Proposition 5. *Let R be an integral domain, S a multiplicative set of R and I an ideal of $R[X]$. If for $a_1, \dots, a_t \in S$ and $t \geq 1$, $Lt(I)_S \cap R[X] = (Lt(I)R_{a_1,\dots,a_t}[X]) \cap R[X]$, then*

$$I_S \cap R[X] = IR_{a_1,\dots,a_t}[X] \cap R[X].$$

Proof. This is a direct consequence of Lemma 3.5 in [4] taking the multiplicative subset $V = \{a_1^{\mu_1} \cdots a_t^{\mu_t} | \mu_i \geq 0, 1 \leq i \leq t\} \subset S$. $\square$

More generally, we have the following property.

Theorem 6. *Let R be an integral domain, S a multiplicative set of R and N a submodule of $R[X]^s$. If for $a_1, \dots, a_t \in S$ and $t \geq 1$, $Lt(N)_S \cap R[X]^s = (Lt(N)R_{a_1,\dots,a_t}[X]) \cap R[X]^s$, then*

$$N_S \cap R[X]^s = NR_{a_1,\dots,a_t}[X] \cap R[X]^s.$$

Proof. This is a direct consequence of Lemma 4.4 in [6] taking the multiplicative subset $V = \{a_1^{\mu_1} \cdots a_t^{\mu_t} | \mu_i \geq 0, 1 \leq i \leq t\} \subset S$. $\square$

Proposition 7. *Let R be a Noetherian integral domain and P a prime ideal of R such that PR_P is principal. Then, for a given ideal I of $R[X]$ there exists $a \in R - P$ such that*

$$IR_P[X] \cap R[X] = IR_a[X] \cap R[X].$$

Proof. Let $PR_P =< \frac{p}{1} >$ with $p \in P$. Since, R_P is a Noetherian integral domain, by the Krull Intersection Theorem we have $\cap_{k=0}^{\infty} \langle \frac{p}{1} \rangle^k = 0$, let $r \neq 0, r \in R$, then $\frac{r}{1} \neq \frac{0}{1} \in R_P$ and hence there exists $k \geq 0$ such that $\frac{r}{1} \in \langle \frac{p}{1} \rangle^k$ and $\frac{r}{1} \notin \langle \frac{p}{1} \rangle^{k+1}$. From this we have $\frac{r}{1} = \frac{a}{a'} \frac{p^k}{1}$ with $\frac{a}{a'} \notin \langle \frac{p}{1} \rangle$. Then $\frac{a}{1} \notin \langle \frac{p}{1} \rangle$ and $a' \notin P$. Moreover, $\langle \frac{a}{1} \rangle + \langle \frac{p}{1} \rangle = R_P$, hence $\frac{1}{1} = \frac{b}{u} \frac{a}{1} + \frac{c}{v} \frac{p}{1}$, where $u, v \notin P$. Thus, $uv = abv + cup$, and since $p \in P$, then $a \notin P$.

Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for I, with $lt(g_i) = r_i X_i$, where $r_i \in R - \{0\}$ and X_i is the leading monomial of g_i. There exist $a_i, a_i' \notin P$ and $k_i \geq 0$ such that $\frac{r_i}{1} = \frac{a_i}{a_i'} \frac{p^{k_i}}{1}$, $1 \leq i \leq t$. Since, $Lt(G) = Lt(I)$, then $Lt(G)_S = Lt(I)_S$ with $S = R - P$. Moreover, in $R[X]_S = R_S[X] = R_P[X]$ the set $\{\frac{g_1}{1}, \ldots, \frac{g_m}{1}\}$ is a Gröbner basis for $I_S = IR[X]_S = IR_S[X] = IR_P[X]$ (see Proposition 4.4.2 in [1]). Thus,

$$\begin{aligned} Lt(I)_S = Lt(I)R[X]_S &= Lt(I)_S[X] = Lt(I)R_P[X] \\ &= \langle \frac{a_1}{a_1'} p^{k_1} X_1, \ldots, \frac{a_t}{a_t'} p^{k_t} X_t \rangle_{R_P[X]} \\ &= \langle a_1 p^{k_1} X_1, \ldots, a_t p^{k_t} X_t \rangle_{R_P[X]} \\ &= \langle \frac{p^{k_1}}{1} X_1, \ldots, \frac{p^{k_t}}{1} X_t \rangle_{R_P[X]}, \text{ since } a_1, \ldots, a_t \notin P. \end{aligned}$$

Then,

$$Lt(I)R_P[X] \cap R[X] = \langle p^{k_1} X_1, \ldots, p^{k_t} X_t \rangle_{R[X]}.$$

Setting $a = a_1 \cdots a_t a_1' \cdots a_t'$ we get

$$\begin{aligned} Lt(I)R_a[X] &= \langle a_1 (a_1')^{-1} p^{k_1} X_1, \ldots, a_t (a_t')^{-1} p^{k_1} X_t \rangle_{R_a[X]} \\ &= \langle \frac{p^{k_1}}{1} X_1, \ldots, \frac{p^{k_t}}{1} X_t \rangle_{R_a[X]}. \end{aligned}$$

Then,

$$\begin{aligned} Lt(I)R_a[X] \cap R[X] &= \langle p^{k_1} X_1, \ldots, p^{k_1} X_t \rangle_{R_a[X]} \cap R[X] \\ &= \langle p^{k_1} X_1, \ldots, p^{k_1} X_t \rangle_{R[X]}. \end{aligned}$$

By Proposition 5 with $t = 1$ we have

$$IR_P[X] \cap R[X] = IR_a[X] \cap R[X].$$

$\square$

For modules we have the following more general result.

Theorem 8. *Let R be a Noetherian integral domain, N a submodule of $R[X]^s$ and P a prime ideal of R such that PR_P is principal. Then, there exists $a \in R - P$ such that*

$$NR_P[X] \cap R[X]^s = NR_a[X] \cap R[X]^s.$$

Proof. We can repeat the previous proof. But, considering the fact that if $G = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_t\}$ is a Gröbner basis for N, then $\{\frac{\boldsymbol{g}_1}{1}, \ldots, \frac{\boldsymbol{g}_m}{1}\}$ is a Gröbner basis for $N_S = NR[X]_S = NR_S[X] = NR_P[X]$, with $S = R - P$. □

Another elementary and probably known result we need in the next section is the following lemma.

Lemma 9. *Let R be a Noetherian commutative ring, $P_i \subset R$ ideals of R such that $P_i + P_j = R$ for $i \neq j$, $1 \leq i, j \leq t$. Let $Q = \prod_{i=1}^{t} P_i^{\nu_i}$ and $Q_i = P_1^{\nu_1} \cdots P_{i-1}^{\nu_{i-1}} P_{i+1}^{\nu_{i+1}} \cdots P_t^{\nu_t}$. Then,*

$$Q_1 + \cdots + Q_t = R.$$

Proof. First, we will prove that $P_i^{\nu_i} + P_j^{\nu_j} = R$ for each $i \neq j$. Since, $(P_i + P_j)^{\nu_i + \nu_j} = R$ we can express 1 as a finite sum of elements of the form $x_1 \cdots x_s$ with $s = \nu_i + \nu_j$ and $x_l \in P_i + P_j$, $1 \leq l \leq s$. In order to prove that $1 \in P_i^{\nu_i} + P_j^{\nu_j}$ we will see that each of these elements belongs to $P_i^{\nu_i} + P_j^{\nu_j}$. In fact,

$$x_l = a_l + b_l \text{ with } a_l \in P_i, b_l \in P_j,\ 1 \leq l \leq s.$$

Hence, $x_1 \cdots x_s = (a_1 + b_1) \cdots (a_s + b_s)$, expanding this product we get a summa such that each summand has of the form $a_{i_1} \cdots a_{i_u} b_{j_1} \cdots b_{j_v}$ with $a_{i_1}, \ldots, a_{i_u} \in P_i$ and $b_{j_1}, \cdots, b_{j_v} \in P_j$.

We note that $u + v = s = \nu_i + \nu_j$, where $0 \leq u, v \leq s$. Thus, $u \geq \nu_i$ or $v \geq \nu_j$ (if $u < \nu_i$ and $v < \nu_j$ then $u + v < \nu_i + \nu_j$). So $a_{i_1} \cdots a_{i_u} \in P_i^{\nu_i}$ or $b_{j_1} \cdots b_{j_v} \in P_j^{\nu_j}$. Hence, $x_1 \cdots x_s \in P_i^{\nu_i} + P_j^{\nu_j}$.

From this we get that

$$\prod_{1 \leq i < j \leq t} (P_i^{\nu_i} + P_j^{\nu_j}) = R,$$

so $1 \in \prod_{1 \leq i < j \leq t} (P_i^{\nu_i} + P_j^{\nu_j})$. Each element in $\prod_{1 \leq i < j \leq t} (P_i^{\nu_i} + P_j^{\nu_j})$ is a finite summa of products with $\frac{t(t-1)}{2}$ factors, each of these factors is an element in $P_i^{\nu_i}$ with $1 \leq i \leq t$. But, in each product there is at least $t - 1$ factors taken from $t-1$ different ideals of collection $\{P_1^{\nu_1}, \ldots P_t^{\nu_t}\}$, i.e., each product belongs to some Q_i, and hence $1 \in Q_1 + \cdots + Q_t$. □

3. The main result

With the results of the previous section we can extend Theorem 8.5 of [6] to Dedekind domains. The preliminary results of [6] could be reformulated in the following way.

Proposition 10. *Let R be a Dedekind domain, $P \subset R$ a maximal ideal of R and $J \subseteq R[x]$ an ideal. We suppose that $J \cap R$ is a $P-$primary and $J \nsubseteq PR[x]$. Then, $J = R[x]$ or $\dim(J) = 0$.*

Proof. We can repeat the proof of the Lemma 8.1 in [6] but changing the prime element p there by the maximal ideal P. □

Proposition 11. *Let R be an integral domain, N a submodule of $R[X]^s$, $P \subset R$ a prime ideal of R such that PR_P is principal. Then, there exists $g \in R - P$ such that*

$$N = (N + gR[X]^s) \cap (NR_P[X] \cap R[X]^s).$$

Proof. We can repeat the proof of Lemma 8.2 in [6] but using Theorem 8 instead of Proposition 4.6 of [6]. □

Proposition 12. *Let R be an integral domain, $N \subset M$ submodules of $R[X]^s$, $P \subset R$ a prime ideal of R such that PR_P is principal. Then, there exists $g \in R - P$ such that $N = (N + gM) \cap (NR_P[X] \cap M)$.*

Proof. We can repeat the proof of Corollary 8.3 of [6] but using the previous proposition instead of Lemma 8.2 of [6]. □

The following lemma is the key for the proof of the main theorem.

Lemma 13. *Let R be a Dedekind domain. Then, for each prime ideal P of R the maximal ideal Q of $R[x]_{P[x]}$ is principal, and hence, $R[x]_{P[x]}$ is a principal ideal domain.*

Proof. By Corollary 6.2.4 of [2], $R[X]$ is a $G-GCD$ domain (an integral domain S is a $G-GCD$ domain if the intersection of any two integral invertible ideals of S is invertible. This is equivalent to the intersection of any finite set of fractional invertible ideals of R is invertible). But the localizations of $G-GCD$ domains by prime ideals are GCD domains (see [2], Corollary 6.2.2. An integral domain S is a GCD domain if the intersection of any two integral principal ideals of R is principal. This is equivalent to the intersection of any finite set of fractional principal ideals of R is principal).

Let P a prime ideal of R and let $S = R[x]_{P[x]}$, then S is a GCD domain. By Theorem 16.2 of [5], each v-ideal of finite type of S is principal (a fractional ideal I of an integral domain S is a v-ideal of finite type if there exists a finitely generated fractional ideal J of S such that $I = J_v$, where $J_v = (J^{-1})^{-1}$ with $J^{-1} = \{\alpha \in K | \alpha J \subseteq S\}$ and K is the field of fractions of S). Let Q be the maximal ideal of S, in order to prove that Q is principal we will prove that Q is generated by two elements and $Q = Q_v$.

Since R is Noetherian, then S is also Noetherian and Q is finitely generated, $Q =< \frac{p_i(x)}{s_i(x)} >_{1 \leq i \leq n}$, with $p_i(x) \in P[x]$ and $s_i(x) \notin P[x]$, this implies that $Q =< p_i(x) >_{1 \leq i \leq n}$. Let $p_i(x) = p_i^{(0)} + p_i^{(1)} x + \cdots + p_i^{(m)} x^m$ with $p_i^{(j)} \in P$, $1 \leq j \leq m$, then since R is a Dedekind domain there exists $r, s \in R$ such that $< p_i^{(j)} >_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} =< r, s >$, so $< r, s >\subseteq P$. We observe that each $p_i(x) \in < r, s >_{R[x]}$ (the ideal of $R[x]$ generated by r and s). Thus, $Q \subseteq < r, s >_S$, but $< r, s >_S \subseteq P[x]_{P[x]} = Q$, and hence, $Q =< r, s >_S$.

On the other hand, by Lemma 6.1.1 of [2] and since R is Dedekind we have

$$(< r, s >_R R[x])_v = (< r, s >_R)_v R[x] = (< r, s >_R^{-1})^{-1} R[x] =< r, s >_R R[x].$$

Moreover,

$$\begin{aligned}(R[x] :< r, s >_{R[x]}) &= (< r, s >_{R[x]})^{-1} = (< r >_{R[x]} + < s >_{R[x]})^{-1}\\ &=< r >_{R[x]}^{-1} \cap < s >_{R[x]}^{-1} =< \frac{1}{r} >_{K(x)} \cap < \frac{1}{s} >_{K(x)},\end{aligned}$$

where K is the field of fractions of R and $K(x)$ is the field of fractions of $R[x]$. Since $R[x]$ is a GCD domain, then $< \frac{1}{r} >_{K(x)} \cap < \frac{1}{s} >_{K(x)}$ is principal. This implies that $(R[x] :< r, s >_{R[x]})$ is finitely generated. Hence,

$$\begin{aligned}Q &= (< r, s >_R R[x])_{P[x]} = ((< r, s >_R R[x])_v)_{P[x]}\\ &= (R[x] : (R[x] :< r, s >_R R[x]))_{P[x]}\\ &= (R[x]_{P[x]} : (R[x]_{P[x]} : (< r, s >_R R[x])_{P[x]}))\\ &= (R[x]_{P[x]} : (R[x]_{P[x]} : Q))\\ &= Q_v.\end{aligned}$$

The last statement of the lemma is a direct consequence of we just proved (see also Proposition 4 of Chapter 2 in [3]). □

Proposition 14. *Let R be a Dedekind domain, $N \subset M$ be submodules of $R[X]^s$. Let $\mathrm{Ann}(M/N) \cap R$ be a $Q-$primary ideal, where $Q \subset R$ is a maximal ideal. Then the primary decomposition for N in M can be computed.*

Proof. By the previous lemma, for each $1 \leq i \leq n$, $R[x_i]_{QR[x_i]}$ is a principal ideal domain and we can use Proposition 11 and repeat the proof of Lemma 8.4 of [6], but using Proposition 10 instead of Lemma 8.1 of [6]. □

Now, we are able to prove the main result that gives a procedure for computing the primary decomposition of N in M (compare with the Theorem 8.5 of [6]).

Theorem 15. *Let R be a Dedekind domain and $N \subset M$ be submodules of $R[X]^s$. Then the primary decomposition for N in M can be computed.*

Proof. If $\dim(\mathrm{Ann}(M/N) \cap R) \neq 0$ then $\mathrm{Ann}(M/N) \cap R = \langle 0\rangle$ and R is not a field. By Proposition 12, we find $a \in R - \langle 0\rangle$ such that

$$N = (N + aM) \cap N^{ec}, \text{ where } N^{ec} = NR_{\langle 0\rangle}[X] \cap M.$$

As in the proof of Lemma 8.4 in [6], we have $N \neq N + aM$. Thus, we can decompose N^{ec} and $N + aM$. We start with N^{ec}. Since, $R_{\langle 0\rangle}$ is a Dedekind domain we can use Proposition 14 for computing a primary decomposition of N^e in M^e, where $N^e = NR_{\langle 0\rangle}[X]$ and $M^e = MR_{\langle 0\rangle}[X]$ are submodules of

$R_{\langle 0\rangle}[X]^s$, and then we can make the contraction with M. We observe that $\mathrm{Ann}(M^e/N^e)\cap R$ is a $0-$ primary ideal.

Now, we must decompose $N+aM$. Since $a\in \mathrm{Ann}(M/N+aM)\cap R$, then $\mathrm{Ann}(M/N+aM)\cap R\neq\langle 0\rangle$, and $\dim(\mathrm{Ann}(M/N+aM)\cap R)=0$. Hence, in this case we have

$$\mathrm{Ann}(M/N)\cap R=\prod_{i=1}^{t}P_i^{\nu_i},\ \text{where } P_i\subset R \text{ is a prime ideal.}$$

Let

$$N_i=N+P_i^{\nu_i}M \text{ for } i=1,\dots,t,$$

then the following properties hold for each $i=1,\dots,t$:

(i) $P_i^{\nu_i}\subseteq \mathrm{Ann}(M/N_i)\cap R$.
(ii) $\mathrm{Ann}(M/N_i)\cap R\subseteq P_i$.
(iii) $\mathrm{Ann}(M/N_i)\cap R$ is P_i-primary.

In fact, since $P_i^{\nu_i}M\subseteq N_i$ then $P_i^{\nu_i}\subseteq \mathrm{Ann}(M/N_i)\cap R$. If $x\in \mathrm{Ann}(M/N_i)\cap R$ and $x\notin P_i$ then $P_i+\langle x\rangle=R$, so $p_i+rx=1$, where $p_i\in P_i$ and $r\in R$. Thus, $p_i^{\nu_i}+\nu_i p^{\nu_i-1}rx+\cdots+(rx)^{\nu_i}=1=p_i^{\nu_i}+r'x$. For $\boldsymbol{m}\in M$ we have $p_i^{\nu_i}\boldsymbol{m}+r'x\boldsymbol{m}=\boldsymbol{m}\in N_i$. Thus, $M\subseteq N_i$, but this is a contradiction.

In order to prove (iii) we will see that $\sqrt{\mathrm{Ann}(M/N_i)\cap R}=P_i$. From (i) we have $P_i^{\nu_i}\subseteq \mathrm{Ann}(M/N_i)\cap R$, and hence, $P_i\subseteq\sqrt{\mathrm{Ann}(M/N_i)\cap R}$. Finally, from (ii) we have $\mathrm{Ann}(M/N_i)\cap R\subseteq P_i$, and then $\sqrt{\mathrm{Ann}(M/N_i)\cap R}\subseteq\sqrt{P_i}=P_i$.

Thus, we have that R is a Dedekind domain, and for $1\leq i\leq n$, $N_i\subset M$, $\mathrm{Ann}(M/N_i)\cap R$ is P_i-primary, $P_i\subset R$ is a maximal ideal and the maximal ideal of $R[x_i]_{QR[x_i]}$ is principal. Then, by the Proposition 14, we can compute the primary decomposition of N_i in M.

In order to conclude the proof we will show that $N=\cap_{i=1}^t N_i$. Since, $N\subseteq N_i$ for each $i=1,\dots t$, then $N\subseteq\cap_{i=1}^t N_i$. Let $\boldsymbol{f}\in\cap_{i=1}^t N_i$. Then for each $i=1,\dots,t$ there exist $\boldsymbol{n}_i\in N$, $\boldsymbol{m}_i\in M$ and $p_i\in P_i^{\nu_i}$ such that

$$\begin{aligned}\boldsymbol{f}&=\boldsymbol{n}_1+p_1\boldsymbol{m}_1,\\&\ \vdots\\ \boldsymbol{f}&=\boldsymbol{n}_t+p_t\boldsymbol{m}_t.\end{aligned}$$

Using Lemma 9 we get $Q_1+\cdots+Q_t=R$, and then

$$1=q_1r_1+\cdots+q_tr_t,\ \text{where } q_i\in Q_i, r_i\in R.$$

Hence,

$$\boldsymbol{f}=q_1r_1\boldsymbol{f}+\cdots+q_tr_t\boldsymbol{f}$$

and $\boldsymbol{f}=q_1r_1(\boldsymbol{n}_1+p_1\boldsymbol{m}_1)+\cdots+q_tr_t(\boldsymbol{n}_t+p_t\boldsymbol{m}_t)=q_1r_1\boldsymbol{n}_1+q_1r_1p_1\boldsymbol{m}_1+\cdots+q_tr_t\boldsymbol{n}_t+q_tr_tp_t\boldsymbol{m}_t$. Since, $p_i\in P_i^{\nu_i}$ and $q_i\in Q_i=P_1^{\nu_1}\cdots P_{i-1}^{\nu_{i-1}}P_{i+1}^{\nu_{i+1}}\cdots P_t^{\nu_t}$, then $p_iq_i\in Q=P_1^{\nu_1}\cdots P_t^{\nu_t}=\mathrm{Ann}(M/N)\cap R$, and hence, $q_ir_ip_i\boldsymbol{m}_i\in N$, for $i=1,\dots,t$. Thus, $\boldsymbol{f}\in N$. $\square$

4. Examples

In this section we illustrate the algorithm MPD of [6] using the procedure described in Theorem 15.

Example 16. Let $N = \langle(0,x^3),(y-x^2,0),(x^3+1,x),(0,y-x^2)\rangle$ and $M = (\mathbb{Q}[x])[y]^2$ be submodules of $(\mathbb{Q}[x])[y]^2$. Using Theorem 15 we will compute a primary decomposition of N in M. With the lexicographical order in $(\mathbb{Q}[x])[y]$ and the POT order in $(\mathbb{Q}[x])[y]^2$ we get a Gröbner basis for N, denoted by $G = \{\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3, \mathbf{g}_4\}$, where $\mathbf{g}_1 = (0,x^3)$, $\mathbf{g}_2 = (y-x^2,0)$, $\mathbf{g}_3 = (x^3+1,x)$ and $\mathbf{g}_4 = (0,y-x^2)$. With this we can compute $\mathrm{Ann}(\mathbb{Q}[x])[y]^2/N) = (N : M) = \langle y-x^2, x^6+x^3\rangle$, we observe that $\{y-x^2, x^6+x^3\}$ is a Gröbner basis for the ideal $\langle y-x^2, x^6+x^3\rangle$. Then, $\mathrm{Ann}(\mathbb{Q}[x])[y]^2/N) \cap R = \langle x^6+x^3\rangle$. Since, $\dim(\mathrm{Ann}(\mathbb{Q}[x])[y]^2/N) \cap R) = \dim(\langle x^6+x^3\rangle) = 0$ then, according to the proof of the Theorem 15, we have $\mathrm{Ann}(\mathbb{Q}[x])[y]^2/N) \cap R = \langle x^6+x^3\rangle = \langle x\rangle^3\langle x^2-x+1\rangle\langle x+1\rangle$.

We set $N_1 = N + \langle x\rangle^3 M$, $N_2 = N + \langle x^2-x+1\rangle M$ and $N_3 = N + \langle x+1\rangle M$. We know that $N = N_1 \cap N_2 \cap N_3$. Thus, $N_1 = \langle(x^3,0),(0,x^3),(y-x^2,0),(x^3+1,x),(0,y-x^2)\rangle$, $N_2 = \langle(x^2-x+1,0),(0,x^2-x+1),(0,x^3),(y-x^2,0),(x^3+1,x),(0,y-x^2)\rangle$ and $N_3 = \langle(x+1,0),(0,x+1),(0,x^3),(y-x^2,0),(x^3+1,x),(0,y-x^2)\rangle$. Gröbner bases for these submodules are

$$\begin{aligned}
G_1 &= \{(0,y-x^2),(0,x^3),(1,x)\},\\
G_2 &= \{(x^2-x+1,0),(0,1),(y-x+1,0)\},\\
G_3 &= \{(x+1,0),(0,1),(y-1,0)\}.
\end{aligned}$$

Now, we apply Proposition 14 in order to compute the primary decomposition of N_1, N_2 and N_3 in M. We will show how to do this for N_1, for N_2 and N_3 the procedure is identical. First we need to check if $\dim(\mathrm{Ann}(M/N_1)) = 0$. For this purpose we consider Corollary 6.9 of [6], i.e., we will verify if $N_1 \cap R^2$ is a primary submodule of R^2 and $\dim(R^2/N_1 \cap R^2) = 0$. We have $N_1 \cap R^2 = \langle(0,x^3),(1,x)\rangle$, $\mathrm{Ann}(R^2/\langle(0,x^3),(1,x)\rangle) = \langle(0,x^3),(1,x)\rangle : M = \langle x^3\rangle$, so $\sqrt{\mathrm{Ann}(R^2/N_1\cap R^2)} = \langle x\rangle$ is a maximal ideal. Thus, $\mathrm{Ann}(R^2/N_1\cap R^2)$ is a primary submodule of R^2 and $\dim(\mathrm{Ann}(R^2/N_1\cap R^2)) = 0$. Since, $\mathrm{Ann}(R^2/N_1\cap R^2)$ is $\langle x\rangle-$primary, where $\langle x\rangle$ is a maximal ideal of R, then by Lemma 5.1 of [6], $N_1\cap R^2$ is $\langle x\rangle-$primary in R^2. Moreover, in $G_1 = \{(0,y-x^2),(0,x^3),(1,x)\}$ the elements $\boldsymbol{w}_{11} = \boldsymbol{e}_1 + x\boldsymbol{e}_2$ and $\boldsymbol{w}_{12} = y\boldsymbol{e}_2 - x^2\boldsymbol{e}_2$ satisfy the conditions of Corollary 6.9 of [6], i.e., $lt(\boldsymbol{w}_{11}) = 1y^0\boldsymbol{e}_1$ and $lt(\boldsymbol{w}_{12}) = 1y\boldsymbol{e}_2$. In both cases the leader coefficient is 1. Hence, $\dim(R[y]/N_1) = 0$.

Now, we can apply the algorithm MZPD of [6]. $\mathrm{Ann}(M/N_1) = \langle y-x^2, x^3\rangle$, a minimal Gröbner basis for $\mathrm{Ann}(M/N_1)\cap R[y]$ is $G = \{y-x^2, x^3\}$, we select $g = y-x^2$ and we factorize g mod $\langle x\rangle$: $y-x^2 \equiv y \pmod{\langle x\rangle}$. We find $t=2$ such that $y^t \in \langle y-x^2, x^3\rangle$, thus $P_1 = y^2M + N_1 = \langle(y^2,0),(0,y^2),(0,y-x^2),(0,x^3),(1,x)\rangle = \langle(1,x),(0,y-x^2),(0,x^3)\rangle$, i.e., P_1 coincides with N_1.

We repeat the above procedure for N_2 and N_3 and we get the primary decomposition of N in $(\mathbb{Q}[x])[y]^2$,

$$\begin{aligned} N &= N_1 \cap N_2 \cap N_3 \\ &= \langle (0, y - x^2), (0, x^3), (1, x) \rangle \cap \langle (x^2 - x + 1, 0), (0, 1), (y - x + 1, 0) \rangle \\ &\quad \cap \langle (x + 1, 0), (0, 1), (y - 1, 0) \rangle. \end{aligned}$$

References

[1] W. W. Adams and P. Loustaunau. *An introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1994.

[2] M. Fontana, J. A. Huckaba, and I. J. Papick. *Prüfer domains*, volume 203 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1997.

[3] W. Fulton. *Algebraic curves. An introduction to algebraic geometry*. W. A. Benjamin, Inc., New York-Amsterdam, 1969. Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series.

[4] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Comput.*, 6(2-3):149–167, 1988. Computational aspects of commutative algebra.

[5] R. Gilmer. *Multiplicative ideal theory*. Marcel Dekker Inc., New York, 1972. Pure and Applied Mathematics, No. 12.

[6] E. W. Rutman. Gröbner bases and primary decomposition of modules. *J. Symbolic Comput.*, 14(5):483–503, 1992.

Received February 28, 2007.

Oswaldo Lezama
Grupo de Álgebra Conmutativa Computacional - SAC^2
Departamento de Matemáticas
Universidad Nacional de Colombia, Bogotá, Colombia

Héctor Suárez
Escuela de Matemáticas y Estadística
UPTC, Tunja, Colombia