ELSEVIER Journal of Pure and Applied Algebra 121 (1997) 1–15

JOURNAL OF
PURE AND
APPLIED ALGEBRA

Gröbner bases and primary decomposition in polynomial rings in one variable over Dedekind domains

W.W. Adams[a], P. Loustaunau[b,*]

[a]*Department of Mathematics, University of Maryland, College Park, MD 20742-4015, USA*
[b]*Department of Mathematics, George Mason University, Fairfax, VA 22030-4444, USA*

Communicated by L. Robbiano; received September 1994

Abstract

Let D be a Dedekind domain with quotient field K, let x be a single variable, and let I be an ideal in $D[x]$. In this paper we will describe explicitly the structure of a Gröbner basis for I and we will use this Gröbner basis to compute the primary decomposition of I. This Gröbner basis also has a property similar to that of strong Gröbner bases over PID's ([7], see also [1]). © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: 13P10

1. Introduction

Let D be a Dedekind domain with quotient field K and let x be a single variable. Let I be an ideal in $D[x]$. The main result in Section 2 is a structure theorem for a special Gröbner basis for I. First, in Proposition 2.2, we factor out the greatest common divisor of I which, by Corollary 2.8, reduces the problem to the case of ideals J such that $J \cap D \neq \{0\}$. In this case we show, in Theorem 2.4, that J has a Gröbner basis of the form $G = \{\mathfrak{a}_1, \mathfrak{a}_2 h_2, \ldots, \mathfrak{a}_t h_t\}$, where $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_t$ are ideals in D, $h_2, \ldots, h_t$ are *monic* polynomials in $D[x]$ of increasing degree satisfying one additional condition. This structure theorem is similar to the one of Szekeres [10] and Lazard [7] in the case where D is a PID (see also [1]). In Corollary 2.5 we give a uniqueness result for this Gröbner basis. We show, in Corollary 2.9, that this Gröbner basis has the following "strong Gröbner basis" property: if $g \in J$ then there is an i such that $\mathfrak{a}_i \operatorname{lt}(h_i) | \operatorname{lt}(g)$, where $\operatorname{lt}(f)$ denotes the leading term of the polynomial f. In Corollary 2.11 we show

[*] Corresponding author. E-mail: ploust@gmu.edu.

PII S0022-4049(96)00052-7

that the $\mathfrak{a}_i$'s are essentially the invariant factors of $D[x]/J$ when this D-module is torsion and finitely generated.

In Section 3 we use the results of Section 2 to obtain a primary decomposition for any ideal I in $D[x]$. First, in Theorem 3.3, we show that $I = \langle c(f)^{-1}f\rangle \cap \mathfrak{a}[x] \cap \langle \mathfrak{a}_1, \mathfrak{a}_2 h_2, \ldots, \mathfrak{a}_{t-1}h_{t-1}, h_t\rangle$, where $f \in K[x]$ is a greatest common divisor of I, $c(f)$ is its content, $\mathfrak{a}$ is an ideal in D, and the remaining ideal is determined in Theorem 2.4 as above. The primary decomposition of the first ideal is determined by the prime factorization of f in $K[x]$. The primary decomposition of the second ideal is determined by the prime factorization of $\mathfrak{a}$ in D. We use a technique of Lazard [7] to compute the primary decomposition of the third ideal. This is done in two steps. In Theorem 3.5 we first compute the maximal ideals containing the third ideal. For each of these we compute, in Theorem 3.6, the associated primary component.

In Section 4 we summarize the algorithm and discuss the computational prerequisites for D in order to implement the constructions presented in the previous two sections. Two examples of Dedekind domains for which these constructions can be carried out are the ring of integers of an algebraic number field (see [4]) and the quotient ring $k[y,z]/\langle f\rangle$, where k is a field and $f(y,z)$ defines a non singular curve (see [5]). We give an example of these constructions for $D = \mathbb{Z}[\sqrt{-5}]$.

We will adopt the following notation. For polynomials $f_1, \ldots, f_s \in K[x]$, we denote by $\langle f_1, \ldots, f_s\rangle$ the $D[x]$-submodule of $K[x]$ generated by $f_1, \ldots, f_s$. In particular, if $f_1, \ldots, f_s \in D[x]$, then $\langle f_1, \ldots, f_s\rangle$ is the ideal in $D[x]$ generated by $f_1, \ldots, f_s$. Similarly, if $a_1, \ldots, a_s \in K$, we denote by $\langle a_1, \ldots, a_s\rangle_D$ the D-submodule of K generated by $a_1, \ldots, a_s$. For $f \in K[x]$ we denote by $\operatorname{lc}(f), \operatorname{lp}(f)$, and $\operatorname{lt}(f)$ the leading coefficient, leading power product and leading term of f, respectively. Also, for a subset $S \subseteq D[x]$, we define $\operatorname{Lt}(S) = \langle \operatorname{lt}(f) \mid f \in S\rangle$. Finally, we say that G is a Gröbner basis for an ideal I of $D[x]$ provided that $G \subseteq I$ and $\operatorname{Lt}(G) = \operatorname{Lt}(I)$. See [1] for more details and equivalent definitions of a Gröbner basis.

2. Gröbner bases for ideals in $D[x]$

Let f be a polynomial in $K[x]$. We define the *content* of f, denoted $c(f)$, to be the D-module generated by the coefficients of f. Of course $c(f)$ is a fractional ideal of D. It is well known that the Gauss Lemma holds in this situation, that is, if $f, g \in K[x]$ then

$$c(fg) = c(f)c(g).$$

(As noted in [2], this is readily proved by localizing at each non-zero prime ideal of D.)

It is also useful to note the following elementary fact.

Lemma 2.1. *Let $f \in K[x]$. Then the $D[x]$-module $\langle c(f)^{-1}f\rangle$ is an ideal of $D[x]$. Indeed $\langle c(f)^{-1}f\rangle = fK[x] \cap D[x]$. So if $g \in D[x]$, then $g \in \langle c(f)^{-1}f\rangle$ if and only if f divides g in $K[x]$.*

We first factor out a greatest common divisor over K of an ideal.

Proposition 2.2. *Let $f_1,\dots,f_s \in D[x]$ and $I=\langle f_1,\dots,f_s\rangle$. Let f be a greatest common divisor of $f_1,\dots,f_s$ in $K[x]$. Then $J=c(f)\frac{1}{f}I$ is an ideal in $D[x]$ such that*

$$J\cap D \neq \{0\}.$$

Moreover, $I=\langle c(f)^{-1}f\rangle J$.

Proof. To see that J is an ideal in $D[x]$, we note that, in $K[x]$, we can write $f_i=fg_i$ for some $g_i\in K[x]$, for $i=1,\dots,s$. Thus, $c(f_i)=c(f)c(g_i)\subseteq D$, and so $\langle c(f)g_i\rangle\subseteq D[x]$. Therefore, $c(f)\frac{1}{f}I=\langle c(f)g_1,\dots,c(f)g_s\rangle\subseteq D[x]$.

Now, in $K[x]$, we can write $f=\sum_{i=1}^{s}\ell_i f_i$ for some $\ell_i\in K[x]$. Therefore, we can find $0\neq d\in D$ such that $df=\sum_{i=1}^{s}d\ell_i f_i$, where $d\ell_i\in D[x]$. Therefore, $df\in I$ and hence, since $c(df)=dc(f)\subseteq D$, we have $\langle dc(f)\rangle\subseteq J\cap D$ and so $J\cap D\neq\{0\}$.

The equality $I=\langle c(f)^{-1}f\rangle J$ is clear. □

We note that the discussion in the last paragraph of the previous proof gives an effective method for determining non-zero elements in $J\cap D$ which uses only the Euclidean Algorithm in $K[x]$.

Our strategy is to first determine the structure of a special Gröbner basis for J and use it to get a special Gröbner basis for I. We first give the following definition.

Definition 2.3. Let I be an ideal in $D[x]$, let $\mathfrak{a}_1,\mathfrak{a}_2,\dots,\mathfrak{a}_t$ be ideals in D, and let $h_1,h_2,\dots,h_t$ be polynomials in $D[x]$. We say that $G=\{\mathfrak{a}_1h_1,\mathfrak{a}_2h_2,\dots,\mathfrak{a}_th_t\}$ is a Gröbner basis for I provided that given any set of generators $\{a_{ij}\mid 1\le j\le v_i\}$ for $\mathfrak{a}_i$, $1\le i\le t$, in D we have that $\{a_{ij}h_i\mid 1\le j\le v_i, 1\le i\le t\}$ is a Gröbner basis for I.

Since, in the situation of Definition 2.3, the leading term ideal $\mathrm{Lt}(I)$ of I is equal to

$$\langle a_{ij}\,\mathrm{lt}(h_i)\mid 1\le j\le v_i, 1\le i\le t\rangle=\langle \mathfrak{a}_i\,\mathrm{lt}(h_i)\mid 1\le i\le t\rangle,$$

in order to verify the condition in Definition 2.3, it suffices to verify that we have a Gröbner basis for any single set of generators for each of the $\mathfrak{a}_i$'s.

Theorem 2.4. *Let J be an ideal in $D[x]$ such that $J\cap D\neq\{0\}$. Then there exists a Gröbner basis G for J of the form*

$$G=\{\mathfrak{a}_1,\mathfrak{a}_2h_2,\dots,\mathfrak{a}_th_t\},$$

where $\mathfrak{a}_1\subsetneq\mathfrak{a}_2\subsetneq\cdots\subsetneq\mathfrak{a}_t$ are ideals in D, $h_2,\dots,h_t$ are monic *polynomials in $D[x]$ with $\deg(h_2)<\deg(h_3)<\cdots<\deg(h_t)$, and for $i=2,\dots,t-1$ we have*

$$h_{i+1}\in\langle h_i,\mathfrak{a}_i^{-1}\mathfrak{a}_{i-1}h_{i-1},\dots,\mathfrak{a}_i^{-1}\mathfrak{a}_2h_2,\mathfrak{a}_i^{-1}\mathfrak{a}_1\rangle.$$

Conversely, any such set G satisfying the above conditions is a Gröbner basis for the ideal it generates.

Proof. Let G be any Gröbner basis for J. We will modify G to obtain a Gröbner basis for J which has the desired form. Assume the distinct degrees of the elements of G are $v_1 < v_2 < \cdots < v_t$. For $i = 1,\dots,t$ let $G_i = \{g \in G \mid \deg(g) \leq v_i\}$ and let $\mathfrak{a}_i$ denote the ideal in D generated by $\{\mathrm{lc}(g) \mid g \in G_i\}$. Since $J \cap D \neq \{0\}$ and G is a Gröbner basis for J, we have that $v_1 = 0$ and so $\mathfrak{a}_1 = \langle G_1 \rangle_D$.

We first note that for $i = 1,\dots,t-1$ we have

$$\mathfrak{a}_{i+1}^{-1}\mathfrak{a}_i\langle G_{i+1}\rangle \subseteq \langle G_i\rangle. \tag{1}$$

To see this, let $g \in G_{i+1} - G_i$ and $d \in \mathfrak{a}_{i+1}^{-1}\mathfrak{a}_i$. (Note that $\mathfrak{a}_{i+1}^{-1}\mathfrak{a}_i$ is an ideal in D, since $\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$.) Then $d\,\mathrm{lc}(g) \in \mathfrak{a}_i$, say

$$d\,\mathrm{lc}(g) = \sum_{f \in G_i} d_f\,\mathrm{lc}(f), \quad \text{where } d_f \in D.$$

Define

$$h = dg - \sum_{f \in G_i} d_f x^{v_{i+1}-\deg(f)} f.$$

Then $h \in J$ and $\deg(h) < \deg(g) = v_{i+1}$. Since G is a Gröbner basis for J, h must reduce to zero using G, and it is clear that only $g \in G_i$ can be used. Thus, we must have $h \in \langle G_i\rangle$, and so $dg \in \langle G_i\rangle$ as desired.

We next show that for $i = 1,\dots,t$, we have

$$\langle G_i\rangle \subseteq \mathfrak{a}_i[x]. \tag{2}$$

This can be seen using induction on i. Clearly for $i = 1$ we have $\langle G_1\rangle = \mathfrak{a}_1[x]$. Now assume that the result is true for i. By Eq. (1) and the induction hypothesis, we have $\mathfrak{a}_{i+1}^{-1}\mathfrak{a}_i\langle G_{i+1}\rangle \subseteq \langle G_i\rangle \subseteq \mathfrak{a}_i[x]$, and so we are done.

It follows from Eq. (2) that, for each $i = 1,\dots,t$, we have that $\mathfrak{a}_i^{-1}\langle G_i\rangle$ is an ideal in $D[x]$. This ideal must contain a polynomial h_i of degree v_i which is monic, since we have $\sum_{g \in G_i} a_g\,\mathrm{lc}(g) = 1$, for some $a_g \in \mathfrak{a}_i^{-1}$, and we may take $h_i = \sum_{g \in G_i} a_g x^{v_i - \deg(g)} g \in D[x]$.

Since G and $\{\mathfrak{a}_1, \mathfrak{a}_2h_2,\dots,\mathfrak{a}_th_t\} \subseteq J$ have the same leading term ideal, the set $\{\mathfrak{a}_1, \mathfrak{a}_2h_2,\dots,\mathfrak{a}_th_t\}$ is also a Gröbner basis for J. If for some i, $\mathfrak{a}_i = \mathfrak{a}_{i+1}$, then the polynomials in $\mathfrak{a}_{i+1}h_{i+1}$ can be reduced using $\mathfrak{a}_ih_i$ and so the polynomials $\mathfrak{a}_{i+1}h_{i+1}$ are not needed in the Gröbner basis. Thus, we may assume that $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_t$. We now replace G by $\{\mathfrak{a}_1, \mathfrak{a}_2h_2,\dots,\mathfrak{a}_th_t\}$ so that $G_i = \{\mathfrak{a}_1, \mathfrak{a}_2h_2,\dots,\mathfrak{a}_ih_i\}$.

It remains to show that for $i = 2,\dots,t-1$

$$h_{i+1} \in \langle h_i, \mathfrak{a}_i^{-1}\mathfrak{a}_{i-1}h_{i-1},\dots,\mathfrak{a}_i^{-1}\mathfrak{a}_2h_2, \mathfrak{a}_i^{-1}\mathfrak{a}_1\rangle.$$

Since, by construction, $h_{i+1} \in \mathfrak{a}_{i+1}^{-1}\langle G_{i+1}\rangle$, we have

$$\langle \mathfrak{a}_ih_{i+1}\rangle \subseteq \mathfrak{a}_{i+1}^{-1}\mathfrak{a}_i\langle G_{i+1}\rangle \subseteq \langle G_i\rangle = \langle \mathfrak{a}_1, \mathfrak{a}_2h_2,\dots,\mathfrak{a}_ih_i\rangle,$$

by Eq. (1), and this gives the desired result.

To prove the converse, let us assume that we have a collection of polynomials in $D[x]$ and ideals in D as in the statement of the theorem. We prove by induction on i that $\{\mathfrak{a}_1, \mathfrak{a}_2 h_2, \dots, \mathfrak{a}_i h_i\}$ is a Gröbner basis for the ideal it generates.

Clearly, $\{\mathfrak{a}_1\}$ is a Gröbner basis for the ideal it generates and now we assume the result for i. We will show that for any homogeneous syzygy of the leading terms of $\{\mathfrak{a}_1, \mathfrak{a}_2 h_2, \dots, \mathfrak{a}_{i+1} h_{i+1}\}$, the corresponding S-polynomial reduces to zero using $\{\mathfrak{a}_1, \mathfrak{a}_2 h_2, \dots, \mathfrak{a}_{i+1} h_{i+1}\}$ (see, e.g. [1] for this equivalent definition of a Gröbner basis). For $\ell = 1, \dots, i+1$, let $\mathfrak{a}_\ell = \langle a_{\ell j} \mid 1 \le j \le t_\ell \rangle_D$. Any homogeneous syzygy gives rise to an equation of the form

$$\sum_{\ell=1}^{i+1} \sum_{j=1}^{t_\ell} c_{\ell j} x^{\nu_{i+1} - \nu_\ell} a_{\ell j} \operatorname{lt}(h_\ell) = 0,$$

where $c_{\ell j} \in D$. Therefore, since h_ℓ is monic, we have

$$\sum_{\ell=1}^{i+1} \sum_{j=1}^{t_\ell} c_{\ell j} a_{\ell j} = 0$$

and, hence,

$$\sum_{j=1}^{t_{i+1}} c_{i+1,j} a_{i+1,j} \in \mathfrak{a}_i.$$

Since, by hypothesis $\mathfrak{a}_i h_{i+1} \subseteq \langle \mathfrak{a}_1, \mathfrak{a}_2 h_2, \dots, \mathfrak{a}_i h_i \rangle$, we have

$$\sum_{\ell=1}^{i+1} \sum_{j=1}^{t_\ell} c_{\ell j} x^{\nu_{i+1} - \nu_\ell} a_{\ell j} h_\ell \in \langle \mathfrak{a}_1, \mathfrak{a}_2 h_2, \dots, \mathfrak{a}_i h_i \rangle,$$

and so reduces to zero using $\{\mathfrak{a}_1, \mathfrak{a}_2 h_2, \dots, \mathfrak{a}_i h_i\}$, since, by induction, this set is a Gröbner basis. □

The Gröbner basis given in Theorem 2.4 has the following uniqueness property.

Corollary 2.5. *Let J be an ideal of $D[x]$ such that $J \cap D \neq \{0\}$. Let $G = \{\mathfrak{a}_1, \mathfrak{a}_2 h_2, \dots, \mathfrak{a}_t h_t\}$ and $G' = \{\mathfrak{a}'_1, \mathfrak{a}'_2 h'_2, \dots, \mathfrak{a}'_{t'} h'_{t'}\}$ be two Gröbner bases of the type given in Theorem 2.4. Then $t = t'$, $\deg(h_i) = \deg(h'_i)$ for $2 \le i \le t$, and for $1 \le i \le t$, $\mathfrak{a}_i = \mathfrak{a}'_i$ and $\langle \mathfrak{a}_1, \mathfrak{a}_2 h_2, \dots, \mathfrak{a}_i h_i \rangle = \langle \mathfrak{a}_1, \mathfrak{a}_2 h'_2, \dots, \mathfrak{a}_i h'_i \rangle$.*

Proof. We prove by induction on i that $\mathfrak{a}_i = \mathfrak{a}'_i$ and $\deg(h_i) = \deg(h'_i)$. To begin the induction, we note that $\mathfrak{a}_1 = J \cap D = \mathfrak{a}'_1$. So assume the result for $1 \le j \le i-1$. If $\deg(h_i) > \deg(h'_i)$, then, since $\mathfrak{a}'_i h'_i \subseteq J$, $\mathfrak{a}'_i h'_i$ can be reduced by G. If j is largest such that $\deg(h_j) \le \deg(h'_i)$ then $1 \le j \le i-1$ and $\mathfrak{a}_j \operatorname{lt}(h_j) | \mathfrak{a}'_i \operatorname{lt}(h'_i)$. Since $\mathfrak{a}_j = \mathfrak{a}'_j$ by induction, and the polynomials h_j and h'_i are monic, we have that $\mathfrak{a}'_j | \mathfrak{a}'_i$, which contradicts the fact that $\mathfrak{a}'_i \subsetneq \mathfrak{a}'_j$. Thus $\deg(h_i) \le \deg(h'_i)$ and so, by symmetry,

$\deg(h_i) = \deg(h_i')$. A similar argument shows that $\mathfrak{a}_i' | \mathfrak{a}_i$ and $\mathfrak{a}_i | \mathfrak{a}_i'$ and so $\mathfrak{a}_i = \mathfrak{a}_i'$. Again, a similar argument shows that $t = t'$. The last statement is an easy induction. □

In the next corollary we show that the polynomials h_i arise as certain greatest common divisors modulo certain prime ideals in D. For a similar result, see [6].

Corollary 2.6. *Let J be an ideal of $D[x]$ such that $J \cap D \neq \{0\}$. Let $G = \{\mathfrak{a}_1, \mathfrak{a}_2 h_2, \ldots, \mathfrak{a}_t h_t\}$ be the Gröbner basis given in Theorem 2.4. Also, let $\mathfrak{p}$ be a prime ideal in D dividing $\mathfrak{a}_1$ but not $\mathfrak{a}_t$. Let i be least such that $\mathfrak{p}$ does not divide $\mathfrak{a}_i$. Then the image of h_i in $(D/\mathfrak{p})[x]$ is the generator of the image of J in $(D/\mathfrak{p})[x]$.*

Proof. Let $\bar{h}_i$ and $\bar{J}$ be the image of h_i and J in $(D/\mathfrak{p})[x]$, respectively. By the choice of i, we have $\bar{J} = \langle \bar{h}_i, \ldots, \bar{h}_t \rangle$. We prove by induction on j that $\bar{h}_{i+j} \in \langle \bar{h}_i \rangle$. Since $h_{i+1} \in \langle h_i, \mathfrak{a}_i^{-1}\mathfrak{a}_{i-1}h_{i-1}, \ldots, \mathfrak{a}_i^{-1}\mathfrak{a}_1 \rangle$, we have $\bar{h}_{i+1} \in \langle \bar{h}_i \rangle$. For $j > 0$, we have $h_{i+j+1} \in \langle h_{i+j}, \mathfrak{a}_{i+j}^{-1}\mathfrak{a}_{i+j-1}h_{i+j-1}, \ldots, \mathfrak{a}_{i+j}^{-1}\mathfrak{a}_1 \rangle$, and so $\bar{h}_{i+j+1} \in \langle \bar{h}_{i+j}, \ldots, \bar{h}_i \rangle$, and so, by induction hypothesis, $\bar{h}_{i+j+1} \in \langle \bar{h}_i \rangle$. □

We next prove a result that allows us to give a Gröbner basis for the original ideal I.

Corollary 2.7. *Let I be an ideal of $D[x]$ and let $\mathfrak{a}$ be a fractional ideal of D such that $\mathfrak{a}I \subseteq D[x]$. Then*

$$\mathrm{Lt}(\mathfrak{a}I) = \mathfrak{a}\,\mathrm{Lt}(I).[1]$$

Thus if $G = \{g_1, \ldots, g_t\} \subseteq I$, then $\{g_1, \ldots, g_t\}$ is a Gröbner basis for I if and only if $\{\mathfrak{a}g_1, \ldots, \mathfrak{a}g_t\}$ is a Gröbner basis for $\mathfrak{a}I$. More generally, if $f \in K[x]$ then $\{g_1, \ldots, g_t\}$ is a Gröbner basis for I if and only if $\{\mathfrak{a}c(f)^{-1}fg_1, \ldots, \mathfrak{a}c(f)^{-1}fg_t\}$ is a Gröbner basis for $\mathfrak{a}c(f)^{-1}fI$.

Proof. We first assume that $I \cap D \neq \{0\}$. Then it follows from Theorem 2.4 that I has a Gröbner basis $G = \{\mathfrak{a}_1, \mathfrak{a}_2 h_2, \ldots, \mathfrak{a}_t h_t\}$ of the type described there. By the converse in Theorem 2.4 we see that $\mathfrak{a}G = \{\mathfrak{a}\mathfrak{a}_1, \mathfrak{a}\mathfrak{a}_2 h_2, \ldots, \mathfrak{a}\mathfrak{a}_t h_t\}$ is a Gröbner basis for $\mathfrak{a}I$. Thus it is clear that $\mathrm{Lt}(\mathfrak{a}I) = \mathfrak{a}\,\mathrm{Lt}(I)$ in this case.

[1] We note that this result is very similar to Theorem 3.6 in [3] and, indeed, can be proved in the same way, using the flatness of ideals in D. We can, in fact, make a general statement which includes both our result and Theorem 3.6 in [3]:

Proposition. Let R be a commutative ring and let M be an R-module. Then the following are equivalent:

(1) For all positive integers n, variables $x_1, \ldots, x_n$, term orders on $R[x_1, \ldots, x_n]$, and ideals $I \subseteq R[x_1, \ldots, x_n]$ we have

$$\mathrm{Lt}(IM[x_1, \ldots, x_n]) = \mathrm{Lt}(I)M[x_1, \ldots, x_n]$$

(2) M is a flat R-module.

For an arbitrary ideal I, we write $I = c(f)^{-1}fJ$ as in Proposition 2.2. We choose $d, e \in D$ such that $dc(f)^{-1} \subseteq D$ and $ef \in D[x]$. It is clear that if $h \in D[x]$ and H is any ideal in $D[x]$, then $\mathrm{Lt}(hH) = \mathrm{lt}(h)\mathrm{Lt}(H)$. Then, using the first case, we have

$$\begin{aligned} de\,\mathrm{Lt}(\mathfrak{a}I) &= \mathrm{Lt}(de\mathfrak{a}I) = \mathrm{Lt}(dc(f)^{-1}ef\mathfrak{a}J) = e\,\mathrm{lt}(f)\,\mathrm{Lt}(dc(f)^{-1}\mathfrak{a}J) \\ &= e\,\mathrm{lt}(f)\mathfrak{a}\,\mathrm{Lt}(dc(f)^{-1}J) = \mathfrak{a}\,\mathrm{Lt}(dc(f)^{-1}efJ) = \mathfrak{a}\,\mathrm{Lt}(deI) = de\mathfrak{a}\,\mathrm{Lt}(I) \end{aligned}$$

from which the desired result is obtained.

The last statement follows immediately. □

Combining Theorem 2.4 and Corollary 2.7 we obtain:

Corollary 2.8. *Let I be an ideal in $D[x]$. Then there exists a Gröbner basis G for I of the form*

$$G = \{c(f)^{-1}f\mathfrak{a}_1, c(f)^{-1}f\mathfrak{a}_2h_2, \ldots, c(f)^{-1}f\mathfrak{a}_th_t\},$$

where $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots \subsetneq \mathfrak{a}_t$ are ideals in D, $h_2, \ldots, h_t$ are monic polynomials in $D[x]$ with $\deg(h_2) < \deg(h_3) < \cdots < \deg(h_t)$, and for $i = 2, \ldots, t-1$ we have

$$h_{i+1} \in \langle h_i, \mathfrak{a}_i^{-1}\mathfrak{a}_{i-1}h_{i-1}, \ldots, \mathfrak{a}_i^{-1}\mathfrak{a}_2h_2, \mathfrak{a}_i^{-1}\mathfrak{a}_1\rangle.$$

We also have the following analog of the concept of a strong Gröbner basis over a PID (see [8] or [1]).

Corollary 2.9. *Let I be an ideal of $D[x]$. Then I has a Gröbner basis $G = \{\mathfrak{b}_1g_1, \ldots, \mathfrak{b}_tg_t\}$, such that, for each i, $\mathfrak{b}_i$ is a fractional ideal of D, $g_i \in K[x]$ and $\mathfrak{b}_ig_i \subseteq D[x]$, with the following property: for all $g \in I$ there is an i such that $\mathfrak{b}_i\,\mathrm{lt}(g_i) \mid \mathrm{lt}(g)$.*

Proof. Let $\mathfrak{b}_i = c(f)^{-1}\mathfrak{a}_i$ and $g_i = fh_i$ in Corollary 2.8. Now let $g \in I$. Since we have $\mathfrak{b}_1 \subsetneq \mathfrak{b}_2 \subsetneq \cdots \subsetneq \mathfrak{b}_t$, g can be reduced using $\mathfrak{b}_ig_i$, where i is the largest index such that $\deg(g_i) \leq \deg(g)$. Therefore $\mathfrak{b}_i\,\mathrm{lt}(g_i) \mid \mathrm{lt}(g)$ as desired. □

Using this corollary and the fact that every ideal in a Dedekind domain D can be generated by one or two elements, we also have

Corollary 2.10. *Let I be an ideal of $D[x]$. Then I has a Gröbner basis $H = \{h_1, \ldots, h_r\}$ such that for all $h \neq 0$ in I, h can be reduced by either a single h_i or by two h_i's.*

For a final corollary, we consider the D-module $M = D[x]/J$ for an ideal J of $D[x]$. Now, M is torsion as a D-module if and only if $J \cap D \neq \{0\}$, which we assume. Moreover, M is finitely generated as a D-module if and only if J contains a monic polynomial (since this is equivalent to the coset of x being integral over D), which we further assume. In this case, we know that M is a direct sum of cyclic D-modules, $M \cong D/\mathfrak{b}_1 \oplus \cdots \oplus D/\mathfrak{b}_n$ where $\mathfrak{b}_n | \mathfrak{b}_{n-1} | \cdots | \mathfrak{b}_1$. (This is the analogue of the classical result concerning finitely generated torsion modules over PID's and is obtained by first using the Chinese Remainder Theorem and then localizing the module at primes of D.) Alternatively, when M is given as the quotient of a free D-module F by a submodule E, then there is a free basis $\ell_1,\dots,\ell_n$ of F such that E is the internal direct sum $E=\mathfrak{b}_1\ell_1\oplus\cdots\oplus\mathfrak{b}_n\ell_n$. The ideals $\mathfrak{b}_1,\dots,\mathfrak{b}_n$ are called the *invariant factors* of M. We will see how to get this representation explicitly for $M=D[x]/J$ from Theorem 2.4.

In the notation of Theorem 2.4, using Corollary 2.9, we note that J contains a monic polynomial if and only if $\mathfrak{a}_t=D$. Let $F=D[x]/\langle h_t\rangle$ and $E=J/\langle h_t\rangle$. Then $M\cong F/E$ and F is free of rank $n=v_t$ (recall that $\deg(h_i)=v_i$). Let $\mathfrak{b}_1=\mathfrak{a}_1$ and $\ell_1=1+\langle h_t\rangle$. For $1\le v\le v_2$ let $\mathfrak{b}_v=\mathfrak{a}_1$ and $\ell_v=x^{v-1}+\langle h_t\rangle$. In general, for $1\le j<t$ and for $v_j+1\le v\le v_{j+1}$ let $\mathfrak{b}_v=\mathfrak{a}_j$ and $\ell_v=x^{v-v_j-1}h_j+\langle h_t\rangle$.

Corollary 2.11. *Assume that $J\subseteq D[x]$ is an ideal such that $M=D[x]/J$ is a finitely generated torsion D-module. Then, with the notation above, a free D-basis for F is $\{\ell_1,\dots,\ell_n\}$ and E is the internal direct sum $E=\mathfrak{b}_1\ell_1\oplus\cdots\oplus\mathfrak{b}_n\ell_n$. Thus the ideals $\mathfrak{b}_1,\dots,\mathfrak{b}_n$ are the invariant factors of $M=D[x]/J$.*

Proof. Since ℓ_v $(1\le v\le v_t=n)$ is defined by a polynomial of degree $v-1$ and h_t has degree $n>v-1$ it is clear that $\{\ell_1,\dots,\ell_n\}$ is a free basis for F. It then suffices to show that $E=\mathfrak{b}_1\ell_1\oplus\cdots\oplus\mathfrak{b}_n\ell_n$. So let $f\in J$. Then, since h_t is monic, we can write $f=h_tq+r$ for some polynomials $q,r\in D[x]$ with $\deg(r)<n$. Now $r\in J$ and so, by Corollary 2.9 there is a j such that $\operatorname{lt}(\mathfrak{a}_jh_j)|\operatorname{lt}(r)$. It is then clear that if $\deg(r)=v-1$, we have $\operatorname{lc}(r)\in\mathfrak{b}_v$ and we can write $r=b_v\ell_v+r_1$, where $\deg(r_1)<v-1$ and $b_v\in\mathfrak{b}_v$. In this way we get a representation of $f+\langle h_t\rangle=r+\langle h_t\rangle$ as an element of $\mathfrak{b}_1\ell_1\oplus\cdots\oplus\mathfrak{b}_n\ell_n$. □

To conclude this section we observe that the ideals $\mathfrak{a}_i$ in Theorem 2.4 arise naturally in a different way. Indeed, if n is a positive integer and if we define $c_n(J)=\langle\operatorname{lc}(f)|f\in J,\deg(f)\le n\rangle_D$, then it is easy to see that $c_n(J)=\mathfrak{a}_i$, where i is the greatest index such that $v_i\le n$. We note that the ideals $c_n(J)$ are also obtained in [9] with explicit formulas using resultants.

3. Primary decomposition for ideals in $D[x]$

Let $I\subseteq D[x]$ be an ideal. In this section we will give an algorithm for determining a primary decomposition for I. The starting point will be Proposition 2.2. We will first show how to turn this product decomposition into an intersection of ideals and then show how we can compute the primary decomposition of each of these ideals. We will obtain three types of ideals:

- $\mathfrak{a}[x]$ for ideals $\mathfrak{a}\subseteq D$,
- $\langle c(f)^{-1}f\rangle$ for polynomials $f\in K[x]$.
- Ideals J as in Theorem 2.4 with $\mathfrak{a}_t=D=\langle 1\rangle_D$.

The primary decomposition of the first two ideals is easily done (see Proposition 3.4 and the discussion before it) and that of the third ideal can be obtained by adopting the ideas of Lazard [7].

We begin with two results which show how to change a product of certain ideals into an intersection.

Lemma 3.1. *Let* $\mathfrak{a}$ *be an ideal in* D *and let* $f \in K[x]$. *Then*

$$\mathfrak{a}\langle c(f)^{-1}f\rangle = \mathfrak{a}[x] \cap \langle c(f)^{-1}f\rangle.$$

Proof. The inclusion $\mathfrak{a}\langle c(f)^{-1}f\rangle \subseteq \mathfrak{a}[x]\cap\langle c(f)^{-1}f\rangle$ is clear. For the reverse inclusion, let $h \in \mathfrak{a}[x]\cap\langle c(f)^{-1}f\rangle$. Then, using Lemma 2.1, in $K[x]$ we have that $h=fg$ for some $g \in K[x]$. By the Gauss Lemma, $c(h)=c(f)c(g) \subseteq \mathfrak{a}$, and so $\langle c(f)g\rangle \subseteq \mathfrak{a}[x]$. Thus, we have

$$\langle h\rangle = \langle c(f)g\rangle\langle c(f)^{-1}f\rangle \subseteq \mathfrak{a}[x]\langle c(f)^{-1}f\rangle = \mathfrak{a}\langle c(f)^{-1}f\rangle,$$

as desired. □

Proposition 3.2. *Let* $\mathfrak{a}$ *be an ideal of* D, A *be an ideal of* $D[x]$, *and let* $f \in K[x]$. *Then*

(1) $\mathfrak{a}\langle A, c(f)^{-1}f\rangle = \mathfrak{a}[x] \cap \langle \mathfrak{a}A, c(f)^{-1}f\rangle$

(2) $\langle c(f)^{-1}f\rangle\langle \mathfrak{a}, A\rangle = \langle c(f)^{-1}f\rangle \cap \langle \mathfrak{a}, c(f)^{-1}fA\rangle$.

Proof. Using Lemma 3.1, we have

$$\begin{aligned}\mathfrak{a}(A + \langle c(f)^{-1}f\rangle) &= \mathfrak{a}A + \mathfrak{a}\langle c(f)^{-1}f\rangle\\ &= \mathfrak{a}A + \mathfrak{a}[x] \cap \langle c(f)^{-1}f\rangle\\ &= \mathfrak{a}[x] \cap (\mathfrak{a}A + \langle c(f)^{-1}f\rangle)\end{aligned}$$

since $\mathfrak{a}A \subseteq \mathfrak{a}[x]$. The second identity is proved in the same way. □

We are now ready to decompose an ideal $I = \langle f_1, \dots, f_s\rangle \subseteq D[x]$ into an intersection for which we can compute a primary decomposition for each piece. Let f be the greatest common divisor of $f_1, \dots, f_s$ in $K[x]$. Set $J_1 = c(f)\frac{1}{f}I$. As noted after the proof of Proposition 2.2, we may determine a non-zero ideal $\mathfrak{a}$ contained in $J_1 \cap D$. Set $J = \langle \mathfrak{a}, I\rangle$. Then we may write $J = \langle \mathfrak{a}_1, \mathfrak{a}_2h_2, \dots, \mathfrak{a}_th_t\rangle$ as in Theorem 2.4 (note that this is not the same J as in Proposition 2.2).

Theorem 3.3. *In the notation above, we have that*

$$I = \langle c(f)^{-1}f\rangle \cap \mathfrak{a}_t[x] \cap \langle \mathfrak{a}_1, \mathfrak{a}_2h_2, \dots, \mathfrak{a}_{t-1}h_{t-1}, h_t\rangle.$$

Proof. By Proposition 3.2, part (2), we have $I = \langle c(f)^{-1}f\rangle J_1 = \langle c(f)^{-1}f\rangle\langle \mathfrak{a}, J_1\rangle = \langle c(f)^{-1}f\rangle \cap J$. Then, using the representation of J in Theorem 2.4 and noting that $\mathfrak{a}_t|\mathfrak{a}_i$ for all i, we have $J = \mathfrak{a}_t\langle \mathfrak{a}_t^{-1}\mathfrak{a}_1, a_t^{-1}\mathfrak{a}_2h_2, \ldots, a_t^{-1}\mathfrak{a}_{t-1}h_{t-1}, h_t\rangle = \mathfrak{a}_t[x] \cap \langle \mathfrak{a}_1, \mathfrak{a}_2h_2, \ldots, \mathfrak{a}_{t-1}h_{t-1}, h_t\rangle$, using Proposition 3.2, part (1), since h_t is monic (and so $c(h_t) = D$). □

The method for determining the primary decomposition of the ideal $\mathfrak{a}_t[x]$ is easy and well-known. Namely, in D write $\mathfrak{a}_t = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_v^{e_v}$, for distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_v$ of D. Then each $\mathfrak{p}_i^{e_i}[x]$ is $\mathfrak{p}_i[x]$-primary and

$$\mathfrak{a}_t[x] = \mathfrak{p}_1^{e_1}[x] \cap \cdots \cap \mathfrak{p}_v^{e_v}[x]$$

is the primary decomposition of $\mathfrak{a}_t[x]$.

Next we find the primary decomposition of $\langle c(f)^{-1}f\rangle$. The relevant facts are summed up in the following proposition.

Proposition 3.4. (1) *If $p, q \in K[x]$ are relatively prime, then $\langle c(p)^{-1}p\rangle\langle c(q)^{-1}q\rangle = \langle c(p)^{-1}p\rangle \cap \langle c(q)^{-1}q\rangle$.*

(2) *If $p \in K[x]$ is irreducible, then $\langle c(p)^{-e}p^e\rangle$ is $\langle c(p)^{-1}p\rangle$-primary.*

(3) *If $f \in K[x]$ and $f = p_1^{e_1} \cdots p_v^{e_v}$ is the prime factorization of f in $K[x]$, then*

$$\langle c(f)^{-1}f\rangle = \langle c(p_1)^{-e_1}p_1^{e_1}\rangle \cap \cdots \cap \langle c(p_v)^{-e_v}p_v^{e_v}\rangle$$

is the primary decomposition of $\langle c(f)^{-1}f\rangle$.

Proof. (1) Let $a \in c(p)^{-1}[x]$ be such that $ap \in \langle c(q)^{-1}q\rangle$. Then, in $K[x]$, q divides ap and so $q|a$; set $a = qr$. Now $c(q)c(r) = c(a) \subseteq c(p)^{-1}$ implies $c(r) \subseteq c(p)^{-1}c(q)^{-1}$ and so $ap = rpq$ has the desired form.

(2) Let $f, g \in D[x]$ with $fg \in \langle c(p)^{-e}p^e\rangle$ and $g \notin \langle c(p)^{-e}p^e\rangle$. Then, using Lemma 2.1, we see that in $K[x]$ we have p^e does not divide g and so p divides f and thus p^e divides f^e and so $f^e \in \langle c(p)^{-e}p^e\rangle$. Similarly, we see that $\langle c(p)^{-1}p\rangle$ is a prime ideal. Then, since $\langle c(p)^{-1}p\rangle^e = \langle c(p)^{-e}p^e\rangle$, $\sqrt{\langle c(p)^{-e}p^e\rangle} = \langle c(p)^{-1}p\rangle$, we are done.

(3) This is clear from parts (1) and (2). □

Following [7], we now show how to compute the primary decomposition of the ideal J in Theorem 2.4 for the case $\mathfrak{a}_t = \langle 1\rangle_D = D$ (see Theorem 3.3). We may assume that $t \geq 2$. Since we have $\mathfrak{a}_{t-1}|\mathfrak{a}_{t-2}|\cdots|\mathfrak{a}_1$, the ideal $\mathfrak{b}_i = \mathfrak{a}_i^{-1}\mathfrak{a}_{i-1}$ is an ideal in D for $i = 2, \ldots, t$. Thus,

$$J = \langle \mathfrak{b}_2\mathfrak{b}_3 \cdots \mathfrak{b}_t, \mathfrak{b}_3 \cdots \mathfrak{b}_th_2, \ldots, \mathfrak{b}_th_{t-1}, h_t\rangle,$$

where $\mathrm{lt}(h_i) = x^{v_i}$, $v_2 < v_3 < \cdots < v_t$, and

$$h_{i+1} \in \langle h_i, \mathfrak{b}_ih_{i-1}, \ldots, \mathfrak{b}_3 \cdots \mathfrak{b}_ih_2, \mathfrak{b}_2\mathfrak{b}_3 \cdots \mathfrak{b}_i\rangle.$$

We first show how to compute the prime ideals containing J. That is, as we shall see, since J is zero-dimensional, we compute all of the maximal ideals containing J.

Theorem 3.5. *Let P be a prime ideal of $D[x]$. Then in the notation above:*

(1) *$J \subseteq P$ if and only if there is an $i \geq 2$ such that $\langle \mathfrak{b}_i, h_i \rangle \subseteq P$.*

(2) *Let $i = 2, 3, \ldots, t$. If $\langle \mathfrak{b}_i, h_i \rangle \subseteq P$, then $P = \langle \mathfrak{p}, v \rangle$ where $\mathfrak{p}$ is a prime ideal factor of $\mathfrak{b}_i$ and v is an irreducible factor of h_i modulo $\mathfrak{p}$.*

(3) *If $J \subseteq P$, then P is maximal.*

Proof. To prove (1), let $J \subseteq P$. Then $\mathfrak{b}_2 \mathfrak{b}_3 \cdots \mathfrak{b}_t \subseteq P$, so that there exists $i \geq 2$ such that $\mathfrak{b}_i \subseteq P$, and we choose i largest with that property. Now $\mathfrak{b}_{i+1} \cdots \mathfrak{b}_t h_i \subseteq P$, but $\mathfrak{b}_{i+1} \cdots \mathfrak{b}_t \not\subseteq P$ by the choice of i, and so $h_i \in P$. Therefore $\langle \mathfrak{b}_i, h_i \rangle \subseteq P$. For the converse, let $i \geq 2$ and assume that $\langle \mathfrak{b}_i, h_i \rangle \subseteq P$. First note that for $j = 1, \ldots, i$ we have $\mathfrak{b}_{j+1} \cdots \mathfrak{b}_t h_j \subseteq \langle \mathfrak{b}_i, h_i \rangle$. Moreover for $j = i + 1, \ldots t$, since $h_j \in \langle h_{j-1}, \mathfrak{b}_{j-1} h_{j-2}, \ldots, \mathfrak{b}_2 \cdots \mathfrak{b}_{j-1} \rangle$, it is an easy induction on j to show that

$$\langle h_{j-1}, \mathfrak{b}_{j-1} h_{j-2}, \ldots, \mathfrak{b}_2 \cdots \mathfrak{b}_{j-1} \rangle \subseteq \langle \mathfrak{b}_i, h_i \rangle,$$

and so $\mathfrak{b}_{j+1} \cdots \mathfrak{b}_t h_j \subseteq \langle \mathfrak{b}_i, h_i \rangle$ for $j = i + 1, \ldots, t$, as well. We now see that $J \subseteq \langle \mathfrak{b}_i, h_i \rangle$. So, since $\langle \mathfrak{b}_i, h_i \rangle \subseteq P$, we have $J \subseteq P$.

We now prove (2). Let $\langle \mathfrak{b}_i, h_i \rangle \subseteq P$. Since $\mathfrak{b}_i \subseteq P$, a prime ideal factor of $\mathfrak{b}_i$, say $\mathfrak{p}$, is contained in P. Note that the ideal $\mathfrak{p}$ is a maximal ideal of D, and so, since h_i is monic, we easily see that there is a $v \in P$ which is an irreducible factor of h_i modulo $\mathfrak{p}$. Since $\langle \mathfrak{p}, v \rangle$ is a maximal ideal of $D[x]$ and is contained in P we have $P = \langle \mathfrak{p}, v \rangle$.

Statement (3) is now immediate. □

Now that we know the maximal ideals containing J we can determine the primary ideals associated to them. Since J is zero-dimensional, these are precisely the ideals that occur in the primary decomposition of J. So let M be such a maximal ideal. Choose i such that $\langle \mathfrak{b}_i, h_i \rangle \subseteq M$ and, as in the theorem, choose a prime ideal factor $\mathfrak{p}$ of $\mathfrak{b}_i$ and an irreducible factor v of h_i modulo $\mathfrak{p}$ such that $M = \langle \mathfrak{p}, v \rangle$. Let m be the largest power of $\mathfrak{p}$ dividing $\mathfrak{b}_2 \mathfrak{b}_3 \cdots \mathfrak{b}_t$. Now, since in the proof of Theorem 3.5 we saw that $J \subseteq \langle \mathfrak{b}_i, h_i \rangle$, we have $h_t \in \langle \mathfrak{b}_i, h_i \rangle \subseteq M$. Since v generates the image of M in $(D/\mathfrak{p})[x]$, we have that v divides h_t modulo $\mathfrak{p}$. Let n be the largest power of v dividing h_t modulo $\mathfrak{p}$ and write $h_t \equiv v^n w \pmod{\mathfrak{p}}$ for some $w \in D[x]$ with w prime to v modulo $\mathfrak{p}$.

Theorem 3.6. *With the notation above, let $V, W \in D[x]$ be such that*

$$h_t \equiv VW \pmod{\mathfrak{p}^m}, \qquad V \equiv v^n \pmod{\mathfrak{p}}, \quad \textit{and} \quad W \equiv w \pmod{\mathfrak{p}}.$$

Then $Q = \langle \mathfrak{p}^m, \mathfrak{b}_3 \cdots \mathfrak{b}_t h_2, \ldots, \mathfrak{b}_t h_{t-1}, V \rangle$ is M-primary and is the M-primary component of J.

Proof. It is easy to see that $J \subseteq Q \subseteq M = \langle \mathfrak{p}, v \rangle$. In order to show that Q is M-primary, it is well-known that it suffices to show that $\mathfrak{p}^m \subseteq Q$ and $v^{nm} \in Q$. The former is clear. For the latter write $V = v^n + p$ for $p \in \mathfrak{p}[x]$ so that $v^{nm} = (V - p)^m \in Q$.

Let $Q' = \{f \in D[x] \mid J : f \not\subseteq M\}$. Then it is well known that Q' is the M-primary component of J; so we show that $Q' = Q$. Let $f \in Q'$ and let $g \in J : f - M$. Then $fg \in J \subseteq Q$. Since Q is M-primary, and $g \notin M = \sqrt{Q}$ we see that $f \in Q$. Thus, $Q' \subseteq Q$.

It remains to show that $Q \subseteq Q'$. Since $\mathfrak{b}_2 \cdots \mathfrak{b}_t \mathfrak{p}^{-m}$ and $\mathfrak{p}$ are relatively prime ideals in D and $\mathfrak{p} \subseteq M$ we see that there is an $a \in \mathfrak{b}_2 \cdots \mathfrak{b}_t \mathfrak{p}^{-m}$ such that $a \notin M$. We have $a\mathfrak{p}^m \subseteq M$ and so $\mathfrak{p}^m \subseteq Q'$. Since $\mathfrak{b}_{i+1} \cdots \mathfrak{b}_t h_i \subseteq J$ and $1 \notin M$, we see that $\mathfrak{b}_{i+1} \cdots \mathfrak{b}_t h_i \subseteq Q'$. Finally, we need $V \in Q'$. Now $W \notin M$, since if we could write $W = p + hv$ for some $p \in \mathfrak{p}[x]$ and $h \in D[x]$ we would have $w \equiv W \equiv hv \pmod{\mathfrak{p}}$ which contradicts the choice of w. Thus there is a $b \in \mathfrak{b}_2 \cdots \mathfrak{b}_t \mathfrak{p}^{-m}$ such that $Wb \notin M$. Then writing $VW = h_t + q$ for $q \in \mathfrak{p}^m[x]$ we see that

$$VWb = (h_t + q)b \in J$$

and so we see that $V \in Q'$. □

We note that the computation of V and W can be done using Hensel's Lemma. (See [4] for the case where $D = \mathbb{Z}$; the computational issues in Dedekind domains are similar.)

Finally, we note that if we use the constructions described in this section, we do not get, in general, a minimal primary decomposition of I. We do get a minimal decomposition of each of the ideals in the decomposition of I in Theorem 3.3, but primary ideals from one of them may be contained in primary ideals of another.

4. The algorithm and an example

In this section we summarize the constructions given in the previous sections and we discuss their implementation. So let the ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq D[x]$ be given.

We first show how to compute the Gröbner basis of Theorem 2.4 and Corollary 2.8. The first step is to compute a greatest common divisor f in $K[x]$ (using the Euclidean Algorithm) and factor $c(f)^{-1}f$ out of I. The second step is to compute a Gröbner basis for $J = c(f)\frac{1}{f}I$. This can be done using the generalization of Buchberger's Algorithm to rings as presented, say, in [8] (see also [1]). We next convert this Gröbner basis into the one given in Theorem 2.4 following the steps in the proof of Theorem 2.4. The final Gröbner basis for I is obtained by multiplying through by $c(f)^{-1}f$.

We next discuss the computation of a primary decomposition of I. As above, we first use the Euclidean Algorithm to compute a greatest common divisor f in $K[x]$ and factor $c(f)^{-1}f$ out of I to obtain the ideal $J_1 = c(f)\frac{1}{f}I$. We again use the Euclidean Algorithm to compute non-zero elements of $J_1 \cap D$, and we let $\mathfrak{a}$ be the ideal in D generated by these elements. (A different choice of $\mathfrak{a}$ will lead to a possibly different ideal J, and so a possibly different primary decomposition of I.) Next, we compute a Gröbner basis for $J = \langle \mathfrak{a}, I \rangle$ and transform it into the form of Theorem 2.4. We now have the representation of I as in Theorem 3.3. Then we factor f into its prime factorization in $K[x]$. Moreover, we factor the ideal $\mathfrak{a}_t$ into its prime ideal factors in D.

We use these factorizations to obtain the primary decompositions of $\langle c(f)^{-1}f\rangle$ and $\mathfrak{a}_t[x]$ as described in Proposition 3.4 and the discussion preceding it. The next step is to factor all of the ideals $\mathfrak{b}_i = \mathfrak{a}_i^{-1}\mathfrak{a}_{i-1}$ into prime ideals. For each prime ideal $\mathfrak{p}$ which divides $\mathfrak{b}_i$, we compute the prime factorization of h_i in $(D/\mathfrak{p})[x]$. Finally, for each irreducible factor v of h_i modulo $\mathfrak{p}$, $\langle \mathfrak{p}, v\rangle$ is a maximal ideal belonging to J and so we compute the primary component Q which belongs to J and which is $\langle \mathfrak{p}, v\rangle$-primary using Theorem 3.6.

We now summarize the computational assumptions we need to make in order to carry out the constructions described above.

- To compute the special Gröbner basis we need to be able to:
  (1) Solve the ideal membership problem in D.
  (2) Compute syzygy modules in D.
  (3) Compute the inverse of fractional ideals of D.
  (4) Perform the Euclidean Algorithm in $K[x]$.
- To compute the primary decomposition we need to be able to:
  (1) Do all of the above.
  (2) Compute prime factorizations of ideals in D.
  (3) Compute prime factorizations of polynomials in $K[x]$.
  (4) Compute prime factorizations of polynomials in $(D/\mathfrak{p})[x]$.
  (5) Perform Hensel lifting.

We give an example of the above construction in $D = \mathbb{Z}[\sqrt{-5}]$.

Example 4.1. Throughout this example we let $\alpha = \sqrt{-5}$. Also, we use the following notation for prime ideals in $\mathbb{Z}[\alpha]$. Let p be a prime in $\mathbb{Z}$ for which -5 is a quadratic residue. Then for a fixed u such that $u^2 \equiv -5 \pmod{p}$, we set $\mathfrak{p}_p = \langle p, u+\alpha\rangle_{\mathbb{Z}[\alpha]}$ and $\mathfrak{p}'_p = \langle p, u-\alpha\rangle_{\mathbb{Z}[\alpha]}$. We note that $\mathfrak{p}_p^{-1} = \frac{1}{p}\mathfrak{p}'_p$ and $\mathfrak{p}_2^2 = \langle 2\rangle_{\mathbb{Z}[\alpha]}$.

We use the notation set in the previous sections.

We consider the ideal $I = \langle f_1, f_2, f_3, f_4, f_5\rangle \subseteq (\mathbb{Z}[\alpha])[x]$, where

$$
\begin{aligned}
f_1 &= (26+22\alpha)x + (-28+16\alpha),\\
f_2 &= (12-30\alpha)x + (54-6\alpha),\\
f_3 &= (6+6\alpha)x^2 + (4+4\alpha)x + (4+4\alpha),\\
f_4 &= (4+2\alpha)x^3 + (-14+2\alpha)x^2 + (-2846+48\alpha)x - (1034+930\alpha),\\
f_5 &= (2-2\alpha)x^5 + (7147+2457\alpha)x^4 + (-1718+3198\alpha)x^3\\
&\quad +(3-3\alpha)x^2 + (372-370\alpha)x + 740.
\end{aligned}
$$

We wish to compute a primary decomposition of I.

We first compute a greatest common divisor f for f_1, f_2, f_3, f_4, f_5 in $K[x]$. We find $f = 3x + (1+\alpha)$, so that $c(f) = \langle 3, 1+\alpha\rangle_{\mathbb{Z}[\alpha]} = \mathfrak{p}_3$. To find an ideal $\mathfrak{a}$ contained in $J_1 \cap \mathbb{Z}[\alpha] = c(f)\frac{1}{f}I \cap \mathbb{Z}[\alpha] = \mathfrak{p}_3\frac{1}{f}I \cap \mathbb{Z}[\alpha]$, it is enough to compute $\mathfrak{p}_3\frac{1}{f}\langle f_1, f_2\rangle = \langle 26+22\alpha, -28+16\alpha, 12-30\alpha, 54-6\alpha\rangle_{\mathbb{Z}[\alpha]} = 2\mathfrak{p}'_3 = \langle 6, 2-2\alpha\rangle_{\mathbb{Z}[\alpha]}$.

Therefore, we have $J = \langle 2\mathfrak{p}_3', I\rangle$. We now compute a Gröbner basis for J.

After inter-reducing the seven polynomials $6, 2-2\alpha, f_1, f_2, f_3, f_4, f_5$, we obtain

$$\begin{aligned}
\ell_1 &= 6,\\
\ell_2 &= 2-2\alpha,\\
\ell_3 &= (4+4\alpha)x + (4+4\alpha),\\
\ell_4 &= (1+3\alpha)x^4 + 4x^3 + (3-3\alpha)x^2 + 2\alpha x + 2.
\end{aligned}$$

It is straightforward, but tedious, to verify that these four polynomials form a Gröbner basis for $J = \langle 2\mathfrak{p}_3', I\rangle$. So we have

$$\begin{aligned}
\mathfrak{a}_1 &= \langle 6, 2-2\alpha\rangle_{\mathbb{Z}[\alpha]} = 2\mathfrak{p}_3' = \mathfrak{p}_2^2\mathfrak{p}_3',\\
\mathfrak{a}_2 &= \langle 6, 2-2\alpha, 4+4\alpha\rangle_{\mathbb{Z}[\alpha]} = \langle 2\rangle_{\mathbb{Z}[\alpha]} = \mathfrak{p}_2^2,\\
\mathfrak{a}_3 &= \langle 6, 2-2\alpha, 4+4\alpha, 1+3\alpha\rangle_{\mathbb{Z}[\alpha]} = \mathfrak{p}_2.
\end{aligned}$$

We now compute the polynomials h_2 and h_3 of Theorem 2.4. Since,

$$\mathfrak{a}_2^{-1}\langle G_2\rangle = \frac{1}{2}\langle 2\mathfrak{p}_3', \ell_3\rangle = \langle 3, 1-\alpha, (2+2\alpha)x + (2+2\alpha)\rangle,$$

and $1 = -3 + 2(1-\alpha) + (2+2\alpha)$, we can choose

$$h_2 = -3x + 2(1-\alpha)x + (2+2\alpha)x + (2+2\alpha) = x + (2+2\alpha).$$

We can now replace ℓ_3 by $\mathfrak{p}_2^2 h_2 = 2h_2$. Similarly, we can choose

$$\begin{aligned}
h_3 &= (-3+\alpha)2h_2x^3 - \frac{1+\alpha}{2}\ell_4\\
&= x^4 - (34+10\alpha)x^3 - 9x^2 + (5-\alpha)x - (1+\alpha) \in \mathfrak{a}_3^{-1}\langle G_3\rangle.
\end{aligned}$$

(This polynomial could be simplified using $\mathfrak{p}_2\mathfrak{p}_3'$ and $\mathfrak{p}_2 h_2$, but this does not simplify the rest of the computation.) So we obtain a Gröbner basis G for J of the form in Theorem 2.4,

$$G = \{\mathfrak{p}_2^2\mathfrak{p}_3', \mathfrak{p}_2^2 h_2, \mathfrak{p}_2 h_3\}.$$

Therefore we have, as in Theorem 3.3

$$I = \left\langle \frac{1}{3}\mathfrak{p}_3' f\right\rangle \cap \mathfrak{p}_2[x] \cap \langle \mathfrak{p}_2^2\mathfrak{p}_3', \mathfrak{p}_2^2 h_2, h_3\rangle.$$

We note that both $\langle \frac{1}{3}\mathfrak{p}_3' f\rangle$ and $\mathfrak{p}_2[x]$ are prime ideals of $(\mathbb{Z}[\alpha])[x]$. So it remains to compute a primary decomposition of $\langle \mathfrak{p}_2^2\mathfrak{p}_3', \mathfrak{p}_2^2 h_2, h_3\rangle$.

We have

$$\mathfrak{b}_2 = \mathfrak{a}_2^{-1}\mathfrak{a}_1 = \mathfrak{p}_3' \quad \text{and} \quad \mathfrak{b}_3 = \mathfrak{a}_2 = \mathfrak{p}_2^2.$$

So we first compute the maximal ideals which contain $\langle \mathfrak{b}_2, h_2\rangle = \langle \mathfrak{p}_3', x + (2+2\alpha)\rangle$. There is only one such maximal ideal, namely $M_1 = \langle \mathfrak{p}_3', x+1\rangle$. Next we compute the maximal ideals which contain $\langle \mathfrak{b}_3, h_3\rangle = \langle 2, x^4 - (34+10\alpha)x^3 - 9x^2 + (5-\alpha)x - (1+\alpha)\rangle$. Since $h_3 \equiv x^4 + x^2 \equiv x^2(x+1)^2 \pmod{\mathfrak{p}_2}$, there are two such maximal ideals, $M_2 = \langle \mathfrak{p}_2, x\rangle$, and $M_3 = \langle \mathfrak{p}_2, x+1\rangle$.

We now compute the primary components of $\langle \mathfrak{p}_2^2\mathfrak{p}_3', \mathfrak{p}_2^2 h_2, h_3\rangle$ which correspond to the three maximal ideals M_1, M_2, M_3. For M_1, we first note that $h_3 \equiv x^4 + x^3 + x + 1 \equiv (x+1)^4 \pmod{\mathfrak{p}_3'}$, and so (using the notation of Theorem 3.6) $V = (x+1)^4$ and the primary component corresponding to M_1 is $Q_1 = \langle \mathfrak{p}_3', 2h_2, (x+1)^4\rangle$. For M_2, since $h_3 \equiv x^2(x+1)^2 \pmod{\mathfrak{p}_2}$, we have $m = n = 2$, $v = x$ and $w = (x+1)^2$. We need to find, since $2 \in \mathfrak{p}_2^2$, u_1, u_2 such that $V = x^2 + (1-\alpha)u_1$, $W = (x+1)^2 + (1-\alpha)u_2$ with $h_3 \equiv VW \pmod{\mathfrak{p}_2^2}$. We have

$$\begin{aligned} h_3 &\equiv x^4 + x^2 + (1-\alpha)x - (1-\alpha) \\ &\equiv VW \\ &\equiv x^4 + x^2 + (1-\alpha)x^2u_2 + (1-\alpha)(x^2+1)u_1 \pmod{\mathfrak{p}_2^2}, \end{aligned}$$

and we may choose $u_1 = x+1$ and $u_2 = x$. Therefore the primary component corresponding to M_2 is $Q_2 = \langle \mathfrak{p}_2^2, \mathfrak{p}_2^2 h_2, x^2 + (1-\alpha)(x+1)\rangle = \langle 2, x^2 + (1-\alpha)x + (1-\alpha)\rangle$. Similarly, the primary component corresponding to M_3 is $Q_3 = \langle 2, x^2 + (1-\alpha)x + 1\rangle$.

Therefore, we have

$$\begin{aligned} I = &\left\langle \frac{1}{3}\mathfrak{p}_3' f \right\rangle \cap \mathfrak{p}_2[x] \cap \langle \mathfrak{p}_3', 2h_2, (x+1)^4\rangle \cap \langle 2, x^2 + (1-\alpha)x + (1-\alpha)\rangle \\ &\cap \langle 2, x^2 + (1-\alpha)x + 1\rangle. \end{aligned}$$

References

[1] W.W. Adams and P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Mathematics, Vol. 3 (American Mathematical Society, Providence, RI, 1994).

[2] M.F. Atiyah and I.G. MacDonald, Introduction to Commutative Algebra (Addison-Wesley, Reading, MA, 1969).

[3] D. Bayer, A. Galligo and M. Stillman, Gröbner Bases and Extensions of Scalars, in: D. Eisenbud and L. Robbiano eds. Computational Algebraic Geometry and Commutative Algebra, Symposia Mathematica Vol. XXXIV, (Cambridge Univ. Press, Cambridge, 1993).

[4] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, Vol. 138 (Springer, Berlin, 1993).

[5] J.A. Hillman, Polynomials determining Dedekind domains, Bull. Austral. Math. Soc. 29 (1984) 167–175.

[6] M. Kalkbrener, Mathematical software, an introduction to computational commutative algebra, ETH Zürich, Mathematik Report No. 94-01.

[7] D. Lazard, Ideal bases and primary decomposition: case of two variables, J. Symb. Comp. 1 (1985) 261–270.

[8] H.M. Möller, On the construction of Gröbner bases using syzygies, J. Symb. Comp. **6** (1988) 345–359.

[9] A. Schinzel and J. Wroblewski, On ideals in the ring of polynomials in one variable over a Dedekind domain, Studia Scientiarum Mathematicarum Hungarica 16 (1981) 415–425.

[10] G. Szekeres, A canonical basis for the ideals of a polynomial domain, Am. Math. Mon. 59 (1952) 379–386.