Computing and Using Minimal Polynomials

John Abbott

Dip. di Matematica, Università degli Studi di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Anna Maria Bigatti

Dip. di Matematica, Università degli Studi di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Elisa Palezzato

Dip. di Matematica, Università degli Studi di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Lorenzo Robbiano

Dip. di Matematica, Università degli Studi di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Abstract

Given a zero-dimensional ideal I in a polynomial ring, many computations start by finding univariate polynomials in I. Searching for a univariate polynomial in I is a particular case of considering the minimal polynomial of an element in P/I. It is well known that minimal polynomials may be computed via elimination, therefore this is considered to be a "resolved problem". But being the key of so many computations, it is worth investigating its meaning, its optimization, its applications.

Key words: Minimal polynomial
1991 MSC: [2010] 13P25, 13P10, 13-04, 14Q10, 68W30, ???

Email addresses: abbott@dima.unige.it (John Abbott), bigatti@dima.unige.it (Anna Maria Bigatti), bigatti@dima.unige.it (Elisa Palezzato), robbiano@dima.unige.it (Lorenzo Robbiano).

[1] This research was partly supported by the "National Group for Algebraic and Geometric Structures, and their Applications"(GNSAGA – INDAM)

Preprint submitted to Elsevier *February 24, 2017*

1. Introduction

In linear algebra it is frequently necessary to use non-linear objects such as minimal and characteristic polynomials since they encode fundamental information about endomorphisms of finite-dimensional vector spaces. It is well-known that if K is a field and R is a zero-dimensional affine K-algebra, *i.e.* a zero-dimensional algebra of type $R = K[x_1, \ldots, x_n]/I$, then R is a finite-dimensional K-vector space (see Proposition 3.7.1 of [6]). Consequently, it not surprising that minimal and characteristic polynomials can be successfully used to detect properties of R.

This point of view was taken systematically in the new book [7] where the particular importance of minimal polynomials (rather greater than that of characteristic polynomials) emerged quite clearly. The book also described several algorithms which use minimal polynomials as a crucial tool. The approach taken there was a good source of inspiration for our research, so that we decided to dig into the theory of minimal polynomials, their uses, and their applications.

The first step was to implement algorithms for computing the minimal polynomial of an element of R and of a K-endomorphism of R (see Algorithms 3.1, 3.2, 3.4). They are described in Section 3, refine similar algorithms examined in [7], and have been implemented in CoCoA (see [3] and [2]) as indeed have all other algorithms described in this paper.

Sections 4 and 5 constitute a contribution of decisive practical significance: they address the problem of computing minimal polynomials of elements of a $\mathbb{Q}$-algebra using a modular approach. As always with a modular approach, various obstacles have to be overcome (see for instance the discussion contained in [4]). In particular, we deal with the notion of reduction of an ideal modulo p, and we do it by introducing the notion of σ-denominator of an ideal (see Definition 4.4 and Theorem 4.6), which enables us to overcome the obstacles. Then ugly, usable, good and bad primes show up (see Definition 5.5 and 5.6). Fortunately, almost all primes are good (see Theorem 5.8 and Corollary 5.9) which paves the way to the construction of the fundamental Algorithm 5.10.

Section 6 presents non-trivial examples of minimal polynomials computed with CoCoA, and Section 7 shows how minimal polynomials can be successfully and efficiently used to compute several important invariants of zero-dimensional affine K-algebras. More specifically, in Subsection 7.1 we describe Algorithms 7.7 and 7.8 which show how to determine whether a zero-dimensional ideal is radical, and how to compute the radical of a zero-dimensional ideal. In Subsection 7.2 we present several algorithms which determine whether a zero-dimensional ideal is maximal or primary. The techniques used depend very much on the field K. The main distinction is between small finite fields and fields of characteristic zero or big fields of positive characteristic. In particular, it is noteworthy that in the first case Frobenius spaces (see Section 5.2 of [7]) play a fundamental role.

Finally, in Section 7.5 a series of algorithms (see 7.20, 7.23, 7.24, and 7.25) describe how to compute the primary decomposition of a zero-dimensional affine K-algebra. They are inspired by the content of Chapter 5 of [7], but they present many novelties.

As we said, all the algorithms described in this paper have been implemented in CoCoA. Their merits are also illustrated by the tables of examples contained in Sections 6 and at the end of Section 7. The experiments were performed on a MacBook Pro 2.9GHz Intel Core i7, using our implementation in CoCoA 5.

2. Notation, First Definitions, and Terminology

Here we introduce the notation and terminology we shall use and the definition of minimal polynomial which is the fundamental object studied in the paper.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring in n indeterminates, and let $\mathbb{T}^n$ denote the monoid of power products in $x_1, \ldots, x_n$. Let I be a zero-dimensional ideal in P; this implies that the ring $R = P/I$ is a zero-dimensional affine K-algebra, hence it is a finite dimensional K-vector space. Then, for any f in P there is a linear dependency mod I among the powers of f: in other words, there is a polynomial $g(z) = \sum_{i=0}^{d} \lambda_i z^i \in K[z]$ which vanishes modulo I when evaluated at $z = f$.

Definition 2.1. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let I be a zero-dimensional ideal. Given a polynomial $f \in P$, we have a K-algebra homomorphism $K[z] \to P/I$ given by $z \mapsto f \bmod I$. The monic generator of the kernel of this homomorphism is called the **minimal polynomial** of $f \bmod I$ (or simply "of f" when the ideal I is obvious), and is denoted by $\mu_{f,I}(z)$.

Remark 2.2. The particular case of $\mu_{x_i,I}(x_i)$, where x_i is an indeterminate, is a very important and popular object when computing: in fact $\mu_{x_i,I}(x_i)$ is the lowest degree polynomial in x_i belonging to I, that is $I \cap K[x_i] = \langle \mu_{x_i,I}(x_i) \rangle$. It is well known that this polynomial may be computed via elimination of all the other indeterminates x_j (see for example Corollary 3.4.6 of [6]). However the algorithm which derives from this observation is usually impractically slow.

Remark 2.3. For the basic properties of Gröbner bases we refer to [6]. Let σ be a term ordering on $\mathbb{T}^n$, and let I be an ideal in the polynomial ring P. For every polynomial $f \in P$ it is known that $\mathrm{NF}_{\sigma,I}(f)$, the σ-normal form of f with respect to I, does not depend on which σ-Gröbner basis of I is used nor on which specific rewriting steps were used to calculate it (see Proposition 2.4.7 of [6]). If I is clear from the context, we write simply $\mathrm{NF}_\sigma(f)$.

Definition 2.4. Following convention, for $0 \neq \delta \in \mathbb{N}$ we use the symbol $\mathbb{Z}_\delta$ to denote the **localization** of $\mathbb{Z}$ by the multiplicative set generated by δ, *i.e.* the subring of $\mathbb{Q}$ consisting of numbers represented by fractions of type $\frac{a}{\delta^k}$ where $a \in \mathbb{Z}$, $k \in \mathbb{N}$.

Observe that $\mathbb{Z}_\delta$ depends only on the radical $\mathrm{Rad}(\delta)$, *i.e.* the product of all primes dividing δ. Furthermore, if $\delta_1, \delta_2 \in \mathbb{N}_+$ then $\mathrm{Rad}(\delta_1)$ divides $\mathrm{Rad}(\delta_2)$ if and only if $\mathbb{Z}_{\delta_1}$ is a subring of $\mathbb{Z}_{\delta_2}$.

If p is a prime number we use the symbol $\mathbb{F}_p$ to denote the **finite field** $\mathbb{Z}/p\mathbb{Z}$. Note that some authors write $\mathbb{Z}_p$ to mean the field $\mathbb{F}_p$: this is clearly ambiguous.

3. Algorithms for Computing Minimal Polynomials

Let K be a field, let $P = K[x_1, \ldots, x_n]$, let I be a zero-dimensional ideal, and let $f \in P$. A well-known method for computing $\mu_{f,I}(z)$ is by elimination. One extends P with a new indeterminate to produce $R = K[x_1, \ldots, x_n,\ z]$, then defines the ideal $J = IR + \langle z - f \rangle$ in R, and finally eliminates the indeterminates $x_1, \ldots, x_n$. Here we give a refined version of Algorithm 5.1.1 of [7].

```
Algorithm 3.1. (MinPolyQuotElim)
notation: $P = K[x_1, \dots, x_n]$
Input  $I$, a zero-dimensional ideal in $P$, and a polynomial $f \in P$
1 create the polynomial ring $R = K[x_1, \dots, x_n,\ z]$
2 define the ideal $J = I \cdot R + \langle z - f \rangle$
3 return the monic, minimal generator of $J \cap K[z]$
Output  $\mu_{f,I}(z) \in K[z]$
```

Another way to compute $\mu_{f,I}(z)$ is via multiplication endomorphisms on P/I. Let $f \in P$ then we write $\vartheta_{\bar{f}} : P/I \to P/I$ for the endomorphism "multiplication by $\bar{f}$". There is a natural isomorphism between P/I and $K[\vartheta_{\bar{f}} \mid \bar{f} \in P/I]$ associating $\bar{f}$ with $\vartheta_{\bar{f}}$ (see Proposition 4.1.2 in [7]). The minimal polynomial of f with respect to I is the same as the minimal polynomial of the endomorphism $\vartheta_{\bar{f}}$. Thus, if the matrix A represents $\vartheta_{\bar{f}}$ with respect to some K-basis of P/I, we can compute the minimal polynomial of A (and thus of $\vartheta_{\bar{f}}$) using the following algorithm which is a refined version of Algorithm 1.1.8 of [7].

```
Algorithm 3.2. (MinPolyQuotMat)
notation: $P = K[x_1, \dots, x_n]$ with term ordering $\sigma$
Input  $I$, a zero-dimensional ideal in $P$, and a polynomial $f \in P$
1 compute $GB$, a $\sigma$-Gröbner basis for $I$;
    from $GB$ compute $QB$, the corresponding monomial quotient basis of $P/I$
2 compute $A$, the matrix representing the map $\vartheta_{\bar{f}}$ w.r.t. $QB$
3 let $B_0 = A^0$ (= Id) and $L = \{B_0\}$
4 Main Loop: for $i = 1, 2, \dots, \mathrm{len}(QB)$ do
    4.1 let $B_i = A \cdot B_{i-1}$ (hence $B_i = A^i$)
    4.2 is there a linear dependency $B_i = \sum_{j=0}^{i-1} c_j B_j,\ \ c_j \in K$?
        yes  return $\mu_{f,I}(z) = z^i - \sum_{j=0}^{i-1} c_j z^j$
        no  append $B_i$ to $L$
Output  $\mu_{f,I}(z) \in K[z]$
```

Remark 3.3. Note that in step MinPolyQuotMat-4.2 a linear dependency among the matrices A^i is equivalent to a linear dependency among just their *first columns*. The reason is that the first column contains the coefficients of $\bar{f}^i \cdot 1 = \bar{f}^i$ assuming that the monomial 1 appears as the first element of QB.

There is a still more direct approach. It comes from considering the very definition of minimal polynomial: we look for the first linear dependency among the powers $\bar{f}^i$ in P/I. Here we give a refined version of Algorithm 5.1.2 of [7].

Algorithm 3.4. (MinPolyQuotDef)

```
notation: $P = K[x_1, \dots, x_n]$ with term ordering $\sigma$
Input  $I$, a zero-dimensional ideal in $P$, and a polynomial $f \in P$
1 compute $GB$, a $\sigma$-Gröbner basis for $I$;
    from $GB$ compute $QB$, the corresponding monomial quotient basis of $P/I$
2 let $f = \mathrm{NF}_{\sigma,I}(f)$
3 let $r_0 = f^0\ (= 1)$ and $L = \{r_0\}$
4 Main Loop: for $i = 1, 2, \dots, \mathrm{len}(QB)$ do
    4.1 compute $r_i = \mathrm{NF}_{\sigma,I}(f \cdot r_{i-1})$; consequently $r_i = \mathrm{NF}_{\sigma,I}(f^i)$
    4.2 is there a linear dependency $r_i = \sum_{j=0}^{i-1} c_j r_j,\ \ c_j \in K$?
        yes return $\boldsymbol{\mu_{f,I}(z) = z^i - \sum_{j=0}^{i-1} c_j z^j}$
        no append $r_i$ to $L$
Output  $\mu_{f,I}(z) \in K[z]$
```

Remark 3.5. Notice that MinPolyQuotMat and MinPolyQuotDef essentially do the same computation: the first using a matrix (dense) representation, and the second a polynomial (sparse) representation.

Remark 3.6. These two algorithms, MinPolyQuotMat and MinPolyQuotDef, are indeed quite simple and natural, but we want to emphasize that a careful implementation is essential for making them efficient. The reward is performance which is dramatically better than the well known elimination approach (see the timings in Section 6.1).

There are two crucial steps for achieving an efficient implementation. The first is when computing the powers of A^i (in step MinPolyQuotMat-4.1) and $\mathrm{NF}_{\sigma,I}(f^i)$ (in step MinPolyQuotDef-4.1): the *incremental approach* we give, using the last computed value, is very important.

The second is the search for a linear dependency (in steps MinPolyQuotMat-4.2 and MinPolyQuotDef-4.2). We implemented it creating a C++ object called `LinDepMill`. This object accepts vectors one at a time, and says whether the last vector it was given is linearly dependent on the earlier vectors; if so, then it makes available the representation of the last vector as a linear combination of the earlier vectors. Internally `LinDepMill` simply builds up and stores a row-reduced matrix and the linear relations as new vectors are supplied.

4. Reductions of Ideals modulo p

The topic of Section 5 is to show how to compute the minimal polynomial of an element of a zero-dimensional affine $\mathbb{Q}$-algebra using a modular approach. In this section we describe the necessary tools to achieve such goal.

Given an ideal I in $\mathbb{Q}[x_1, \dots, x_n]$ what does it mean to reduce I modulo a prime number p? Since there is no homomorphism from $\mathbb{Q}$ to $\mathbb{F}_p$, there is no immediate answer to this question. In this section we let $P = \mathbb{Q}[x_1, \dots, x_n]$, investigate the problem, and provide a useful answer. We shall also assume that P comes with a term ordering σ.

We start with the following lemma (recall the notation in Remark 2.4).

Lemma 4.1. *Let $\delta \in \mathbb{N}_+$, let I be a non-zero ideal in P, let G be its reduced σ-Gröbner basis, and let $f \in P$. Assume that f and G have all coefficients in $\mathbb{Z}_\delta$.*

(a) Every intermediate step of rewriting of f via G has all coefficients in $\mathbb{Z}_\delta$.

(b) The polynomial $\mathrm{NF}_\sigma(f)$ has all coefficients in $\mathbb{Z}_\delta$.

Proof. If $f = 0$, the result is trivially true. So we now assume $f \neq 0$. If f can be reduced by G then there exists $\tau \in \mathrm{Supp}(f)$ such that $\tau = t \cdot \mathrm{LT}_\sigma(g)$ for some $g \in G$ and some power-product $t \in \mathbb{T}^n$. Let c be the coefficient of τ in f; by hypothesis $c \in \mathbb{Z}_\delta$. Then the first step of rewriting gives $f_1 = f - c \cdot t \cdot g$ which has all coefficients in $\mathbb{Z}_\delta$. We can now repeat the same argument for rewriting f_1, and so on. Using Remark 2.3, we deduce that the final result, when no further such rewriting is possible, is the normal form of f. It is reached after a finite number of steps. These considerations prove both claims. □

The following example illustrates the lemma.

Example 4.2. Let $P = \mathbb{Q}[x, y]$, let $I = \langle f_1, f_2 \rangle$ where $f_1 = 3x^3 - x^2 + 1$, $f_2 = x^2 - y$, and let $\sigma =$ `DegRevLex`. The reduced σ-Gröbner basis of I is $G = \{g_1, g_2, g_3\}$ where $g_1 = y^2 + \frac{1}{3}x - \frac{1}{9}y + \frac{1}{9}$, $g_2 = xy - \frac{1}{3}y + \frac{1}{3}$, $g_3 = x^2 - y$. We let $f = y^3$ so that $f, g_1, g_2, g_3 \in \mathbb{Z}_3[x, y]$. We have $\mathrm{NF}_\sigma(f) = -\frac{1}{27}x - \frac{17}{81}y + \frac{8}{81}$, and it is easy to check that the explicit coefficients in the equality

$$f = \mathrm{NF}_\sigma(f) + (xy + \tfrac{1}{9}x + \tfrac{1}{3}y - \tfrac{8}{27})\, g_2 - (y^2 + \tfrac{1}{9}y)\, g_3$$

are the coefficients of a sequence of rewriting steps from f to $\mathrm{NF}_\sigma(f)$. As shown by the lemma, they all lie in $\mathbb{Z}_3$.

The following easy example shows that the number δ introduced in the above lemma depends on σ.

Example 4.3. Let $P = \mathbb{Q}[x, y, z]$, let $I = \langle f \rangle$ where $f = 2x + 3y + 5z$. Depending on the term ordering chosen, the number δ can be 2, 3 or 5.

Definition 4.4. Let δ be a positive integer, and p be a prime number not dividing δ. We write π_p to denote both the canonical homomorphism $\mathbb{Z}_\delta \longrightarrow \mathbb{F}_p$ and its natural "coefficientwise" extensions to $\mathbb{Z}_\delta[x_1, \ldots, x_n] \longrightarrow \mathbb{F}_p[x_1, \ldots, x_n]$; we call them all **reduction homomorphisms modulo** p.

Now we need more definitions.

Definition 4.5. Let $P = \mathbb{Q}[x_1, \ldots, x_n]$.

(a) Given a polynomial $f \in P$, we define the **denominator of** f, denoted by $\mathrm{den}(f)$, to be 1 if $f = 0$, and otherwise the least common multiple of the denominators of the coefficients of f.

(b) Given a non-zero ideal I in P, with reduced σ-Gröbner basis G, we define the **σ-denominator of** I, denoted by $\mathrm{den}_\sigma(I)$, to be the least common multiple of $\{\mathrm{den}(g) \mid g \in G\}$.

The following theorem illustrates the importance of the σ-denominator of an ideal.

Theorem 4.6. ***(Reduction modulo*** p ***of Gröbner Bases)***
Let I be a non-zero ideal in $\mathbb{Q}[x_1,\dots,x_n]$ with reduced σ-Gröbner basis G. Let p be a prime number which does not divide $\mathrm{den}_\sigma(I)$.

- *(a) The set $\pi_p(G)$ is the reduced σ-Gröbner basis of the ideal $\langle\pi_p(G)\rangle$.*
- *(b) The set of the residue classes of the elements in $\mathbb{T}^n\setminus\mathrm{LT}_\sigma(I)$ is an $\mathbb{F}_p$-basis of the quotient ring $\mathbb{F}_p[x_1,\dots,x_n]/\langle\pi_p(G)\rangle$.*
- *(c) For every polynomial $f\in\mathbb{Q}[x_1,\dots,x_n]$ such that $p\not|\,\mathrm{den}(f)$ we have the equality $\pi_p(\mathrm{NF}_{\sigma,I}(f))=\mathrm{NF}_{\sigma,\langle\pi_p(G)\rangle}(\pi_p(f))$.*

Proof. We start by proving claim (a). Every polynomial g in G is monic, so $\pi_p(g)$ is monic and $\mathrm{LT}_\sigma(\pi_p(g))=\mathrm{LT}_\sigma(g)$. Next we show that $\pi_p(G)$ is a reduced σ-Gröbner basis. So assume $G=\{g_1,\dots,g_s\}$, let $1\le i<j\le s$ and let $f_0=t_jg_i-t_ig_j$ be the S-polynomial of (g_i,g_j). It rewrites to zero via a finite number of steps of rewriting: $f_{k+1}=f_k-c_k\cdot t_k\cdot g_{i_k}$ for $k=1,2,\dots,r-1$. Let $\delta=\mathrm{den}_\sigma(I)$, then f_0 and every g_i have all coefficients in $\mathbb{Z}_\delta$. Lemma 4.1 implies that each c_k is in $\mathbb{Z}_\delta$ and that all coefficients of each f_k are in $\mathbb{Z}_\delta$.

We now show that the S-polynomial of the p-reduced pair $(\pi_p(g_i),\pi_p(g_j))$ rewrites to zero via the set $\pi_p(G)$. First we see that $\pi_p(f_0)=t_j\pi_p(g_i)-t_i\pi_p(g_j)$. Now applying π_p to each rewriting step we get $\pi_p(f_{k+1})=\pi_p(f_k)-\pi_p(c_k)\cdot t_k\cdot\pi_p(g_{i_k})$. If $\pi_p(c_k)\neq 0$, this is a rewriting step for $\pi_p(f_k)$, otherwise “nothing happens” and we simply have $\pi_p(f_{k+1})=\pi_p(f_k)$.

This shows that all the S-polynomials of $\pi_p(G)$ rewrite to zero, and hence that $\pi_p(G)$ is a σ-Gröbner basis. Finally we observe that $\mathrm{Supp}(\pi_p(g_i))\subseteq\mathrm{Supp}(g_i)$ for all $i=1,\dots,s$, hence $\pi_p(G)$ is actually the reduced σ-Gröbner basis of the ideal $\langle\pi_p(G)\rangle$.

As already observed, we have $\mathrm{LT}_\sigma(g_i)=\mathrm{LT}_\sigma(\pi_p(g_i))$ for all $i=1,\dots,s$, hence claim (b) follows from (a).

For part (c) we let $\delta=\mathrm{LCM}(\mathrm{den}(f),\mathrm{den}_\sigma(I))$. We use the same method as in the proof of part (a) but starting with $f_0=f$. Once again all rewriting steps have coefficients in $\mathbb{Z}_\delta$, and applying π_p to them we get either a rewriting step for $\pi_p(f)$ or possibly a “nothing happens” step. Therefore the image of the final remainder $\pi_p(\mathrm{NF}(f))$ is the normal form of $\pi_p(f)$. □

The following example illustrates some claims of the theorem.

Example 4.7. We continue the discussion of Example 4.2. We choose $p=2$ and get $\langle y^2+x+y+1,\ xy+y+1,\ x^2+y\rangle$ as the (p,σ)-reduction of I. From Theorem 4.6 we know that $\{y^2+x+y+1,\ xy+y+1,\ x^2+y\}$ is the reduced σ-Gröbner basis of $\langle\pi_p(G)\rangle$.

Theorem 4.6, in particular claim (c), motivates the following definition.

Definition 4.8. If p is a prime number which does not divide $\mathrm{den}_\sigma(I)$, then the ideal generated by the $\pi_p(G)=\{\pi_p(g_1),\dots,\pi_p(g_s)\}$ in the polynomial ring $\mathbb{F}_p[x_1,\dots,x_n]$ is called the (p,σ)**-reduction of** I, and will be denoted by $I_{(p,\sigma)}$. Observe that if I is zero-dimensional so is $I_{(p,\sigma)}$.

The following example shows the necessity of considering the reduced Gröbner basis in Theorem 4.6.

Example 4.9. Let $P = \mathbb{Q}[x]$, let a be the product of many primes, for instance the product of the first 10^6 prime numbers, and let $I = \langle ax,\, x^2\rangle$. The set $S = \{ax,\, x^2\}$ is a Gröbner basis of I, while the set $G = \{x\}$ is the reduced Gröbner basis of I. Reducing S modulo p where $p \,|\, a$ produces the ideal $\langle x^2\rangle$, while reducing G produces the ideal $\langle x\rangle$.

More investigation about (p, σ)-reductions is done in [5].

5. A Modular Approach to the Computation of Minimal Polynomials

The topic of this section is to show how to compute the minimal polynomial of an element of a zero-dimensional affine $\mathbb{Q}$-algebra using a modular approach. Modular reduction is a very well-known technique, however there is no universal method for addressing the specific problems of bad reduction arising in every application. Our problem is no exception as we shall explain shortly. For more details on this topic we recommend reading Section 6 of [4].

For this entire section the ideal I will be zero-dimensional, and since in Theorem 4.6.(b) we have seen that the set of power-products $\mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ can be mapped both to a basis of $\mathbb{Q}[x_1, \ldots, x_n]/I$ and also to a basis of $\mathbb{F}_p[x_1, \ldots, x_n]/I_{(p,\sigma)}$, we are motivated to provide the following definition.

Definition 5.1. Let $P = \mathbb{Q}[x_1, \ldots, x_n]$ with term ordering σ. Let I be a zero-dimensional ideal in P. Let $d = \dim_K(P/I)$ and let $B = (1, t_2, \ldots, t_d) = \mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ with elements in increasing σ-order. So the natural image of B in P/I is a $\mathbb{Q}$-basis of monomials for P/I. We denote the natural image of B in $\mathbb{Q}[x_1, \ldots, x_n]$ by $B_{\mathbb{Q}}$ and the natural image of B in $\mathbb{F}_p[x_1, \ldots, x_n]$ by B_p.

Given $f \in P$ we denote by $M_{B_{\mathbb{Q}}}(f, r)$ the $d \times (r + 1)$ matrix whose j-th column (for $j = 1, \ldots, r + 1$) contains the coordinates of $\mathrm{NF}_{\sigma,I}(f^{j-1})$ in the basis $B_{\mathbb{Q}}$. Similarly, we denote by $M_{B_p}(\pi_p(f), r)$ the $d \times (r+1)$ matrix whose j-th column contains the coordinates of $\mathrm{NF}_{\sigma,I_{(p,\sigma)}}(\pi_p(f^{j-1}))$ in the basis B_p. We observe that these matrices depend on both σ and the corresponding ideals.

The following proposition contains useful information about reduction of matrices.

Proposition 5.2. *Let $f \in P$ be a polynomial and let $\delta = \mathrm{den}(f) \cdot \mathrm{den}_\sigma(I)$.*

(a) For every r, all the entries of the matrix $M_{B_{\mathbb{Q}}}(f, r)$ are in $\mathbb{Z}_\delta$.

(b) For every r, we have $\pi_p(M_{B_{\mathbb{Q}}}(f, r)) = M_{B_p}(\pi_p(f), r)$ for any prime $p \nmid \delta$.

Proof. Claim (a) follows from Lemma 4.1 applied to f^j, and claim (b) follows directly from Theorem 4.6.(c). □

5.1. Usable and ugly primes

We start this subsection with an elementary result which is placed here for the sake of completeness.

Lemma 5.3. *Let $f, g \in \mathbb{Q}[z]$ be monic polynomials such that g divides f, and let $\delta \in \mathbb{N}_+$. If f has coefficients in $\mathbb{Z}_\delta$ then also g has coefficients in $\mathbb{Z}_\delta$.*

Proof. By hypothesis we have a factorization $f = gh$ in $\mathbb{Q}[z]$. Set $D_f = \operatorname{den}(f)$, $D_g = \operatorname{den}(g)$ and $D_h = \operatorname{den}(h)$; so each of $D_f f$, $D_g g$ and $D_h h$ is a primitive polynomial with integer coefficients. By Gauss's Lemma $(D_g g)(D_h h) = D_g D_h f$ is a primitive polynomial with integer coefficients. Hence $D_f = \pm D_g D_h$; in particular $D_g | D_f$, and consequently $\operatorname{Rad}(D_g) | \operatorname{Rad}(D_f)$. Since $f \in \mathbb{Z}_\delta[z]$ we have $\operatorname{Rad}(D_f) | \operatorname{Rad}(\delta)$, hence also $\operatorname{Rad}(D_g) | \operatorname{Rad}(\delta)$ which implies that $g \in \mathbb{Z}_\delta[z]$. $\square$

We now give a proposition which tells us which primes could appear in the denominator of a minimal polynomial.

Proposition 5.4. *Let $f \in P$, and let $\delta = \operatorname{den}(f) \cdot \operatorname{den}_\sigma(I)$. Then the minimal polynomial $\mu_{f,I}(z)$ has all coefficients in $\mathbb{Z}_\delta$.*

Proof. Let $\vartheta_{\bar{f}}$ be the $\mathbb{Q}$-endomorphism of P/I given by multiplication by $\bar{f}$. It is known that $\mu_{f,I}(z) = \mu_{\vartheta_{\bar{f}}}(z)$ (see Remark 4.1.3.(a) of [7]). Let $\chi_{\vartheta_{\bar{f}}}(z)$ be the characteristic polynomial of the endomorphism $\vartheta_{\bar{f}}$; by definition $\chi_{\vartheta_{\bar{f}}}(z) = \det(z\,\mathrm{id} - \vartheta_{\bar{f}})$. Next, let $d = \dim_{\mathbb{Q}}(P/I)$, let $B = (1, t_2, \ldots, t_d) = \mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$, let I_d be the identity matrix of size d, and let $M_B(\vartheta_{\bar{f}})$ be the matrix which represents $\vartheta_{\bar{f}}$ with respect to the basis B. Then we have $\det(z\,\mathrm{id} - \vartheta_{\bar{f}}) = \det(z\, I_d - M_B(\vartheta_{\bar{f}}))$. The entries of $M_B(\vartheta_{\bar{f}})$ are the coefficients of the representations of $\mathrm{NF}_\sigma(t_i f)$ in the basis B for all $t_i \in B$. They are in $\mathbb{Z}_\delta$ by Lemma 4.1. So we have proved that $\chi_{\vartheta_{\bar{f}}}(z) \in \mathbb{Z}_\delta[z]$. From the Cayley-Hamilton Theorem we deduce that $\mu_{\vartheta_{\bar{f}}}(z)$ is a divisor of $\chi_{\vartheta_{\bar{f}}}(z)$. It follows from Lemma 5.3 that also $\mu_{\vartheta_{\bar{f}}}(z) \in \mathbb{Z}_\delta[z]$. $\square$

The conclusion of the proposition above motivates the following definition.

Definition 5.5. Let $f \in P$ be a polynomial, and let p be a prime number. Then p is called a **usable prime for f with respect to** (I, σ) if it does not divide $\operatorname{den}(f) \cdot \operatorname{den}_\sigma(I)$. If I and σ are clear from the context, we say simply a **usable prime**. A prime which is not usable is called **ugly**. It follows from the definition that, for a given input (f, I, σ), there are only finitely many ugly primes, and it is easy to recognize and avoid them.

5.2. Good and bad primes

In this subsection we refine the definition of usable.

Definition 5.6. Let p be a usable prime for f with respect to (I, σ); consequently, by Proposition 5.4, $\pi_p(\mu_{f,I}(z))$ is well-defined. We say that p is a **good prime for f** if $\mu_{\pi_p(f), I_{(p,\sigma)}}(z) = \pi_p(\mu_{f,I}(z))$, in other words if the minimal polynomial of the p-reduction of f modulo the (p, σ)-reduction of I equals the p-reduction of the minimal polynomial of f modulo I over the rationals. Otherwise, it is called **bad**.

The following simple example illustrates how a prime can be bad even if it is usable.

Example 5.7. Let $P = \mathbb{Q}[x, y]$, let $I = \langle x^2,\, y^2 \rangle$, and let $f = x + y$. The set $\{x^2,\, y^2\}$ is a reduced Gröbner basis of I for every ordering, $B = (1, x, y, xy)$ is a quotient basis of $\mathbb{Q}[x, y]/I$ regardless of ordering. Moreover we have $\operatorname{den}(f) \cdot \operatorname{den}_\sigma(I) = 1$ regardless of ordering, and thus every prime number is usable. Over $\mathbb{Q}$ we have $M_B(f, 3) = \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \end{smallmatrix}\right)$.

Whence we deduce that $\mu_{f,I}(z) = z^3$. If we change the base field to the finite field $\mathbb{F}_2$, we get $M_B(\pi_2(f), 3) = \left(\begin{smallmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&1&0&0 \\ 0&0&0&0 \end{smallmatrix}\right)$ which shows that $\mu_{f,I} = z^2$. It is easy to see that 2 is the only bad prime in this case.

Next we show that there are only finitely many bad primes.

Theorem 5.8. ***(Finitely many bad primes)***
Let $P = \mathbb{Q}[x_1, \dots, x_n]$, let I be a zero-dimensional ideal in P, let σ be a term ordering on $\mathbb{T}^n$, let $f \in P$, and p be a usable prime.

(a) Then $\pi_p(\mu_{f,I}(z))$ is a multiple of $\mu_{\pi_p(f), I_{(p,\sigma)}}(z)$.
(b) There are only finitely many bad primes.
(c) The prime p is good if and only if $\deg(\mu_{\pi_p(f), I_{(p,\sigma)}}(z)) = \deg(\mu_{f,I}(z))$.

Proof. To simplify the presentation we let $\mu(z) = \mu_{f,I}(z)$ and $\mu_p(z) = \mu_{\pi_p(f), I_{(p,\sigma)}}(z)$. Let $\mu(z){=}z^r + c_{r-1}z^{r-1} + \cdots c_0$, and set $\delta = \mathrm{den}(f) \cdot \mathrm{den}_\sigma(I)$. By Proposition 5.4 we have $\mu(z) \in \mathbb{Z}_\delta[z]$. By the definition of minimal polynomial we have $f^r + c_{r-1}f^{r-1} + \cdots c_0 \in I$. Therefore we have an equality $f^r + c_{r-1}f^{r-1} + \cdots c_0 = \sum h_i g_i$ for certain $h_i \in P$ where $\{g_1, \dots, g_s\}$ is the reduced σ-Gröbner basis of the ideal I. By Lemma 4.1 we know that each $h_i \in \mathbb{Z}_\delta$. Since p is a usable prime, it follows from Proposition 5.4 that we can apply π_p to get

$$\pi_p(f)^r + \pi_p(c_{r-1})\, \pi_p(f)^{r-1} + \cdots + \pi_p(c_0) = \sum_{i=1}^{s} \pi_p(h_i)\, \pi_p(g_i)$$

which shows that $\pi_p(\mu(f)) \in I_{(p,\sigma)}$, and hence that $\pi_p(\mu(z))$ it is a multiple of $\mu_p(z)$. So claim (a) is proved.

To prove (b) and (c) it suffices to show that only a finite number of usable primes are such that $\pi_p(\mu(z))$ is a non-trivial multiple of $\mu_p(z)$, and we argue as follows. Since r is the degree of $\mu(z)$ we deduce that the matrix $M_{B_\mathbb{Q}}(f, r-1)$ has rank r, hence there exists an $r{\times}r$-submatrix of $M_{B_\mathbb{Q}}(f, r{-}1)$ with non-zero determinant; moreover this determinant lies in $\mathbb{Z}_\delta$, so can be written as $\frac{a}{\delta^s}$ for some non-zero $a \in \mathbb{Z}$ and some $s \in \mathbb{N}$. For any prime p not dividing $a\delta$, the matrix $\pi_p(M_{B_\mathbb{Q}}(f, r-1))$ has maximal rank: by Proposition 5.2 we have $\pi_p(M_{B_\mathbb{Q}}(f, r-1)) = M_{B_p}(\pi_p(f), r-1)$. Hence for these primes the degree of $\mu_p(z)$ is r, and the conclusion follows. □

We do not have an absolute means of detecting bad primes but, for two different usable primes p_1 and p_2 we can compute the minimal polynomials of $\pi_{p_i}(f)$ with respect to $I_{(p_i,\sigma)}$, and by comparing degrees we can sometimes detect that one prime is surely bad, though without being certain that the other is good.

Corollary 5.9. ***(Detecting some bad primes)***
Let p_1, p_2 be two usable primes, and let $\mu_1 = \mu_{\pi_{p_1}(f), I_{(p_1,\sigma)}}(z)$ and $\mu_2 = \mu_{\pi_{p_2}(f), I_{(p_2,\sigma)}}(z)$ be the minimal polynomials of the corresponding modular reductions.

(a) If $\deg(\mu_1) < \deg(\mu_2)$ then p_1 is a bad prime.
(b) If $\deg(\mu_1) = \dim_K(P/I)$ then p_1 is a good prime.

Proof. Claim (a) follows from parts (a) and (c) of Theorem 5.8. Claim (b) follows from Theorem 5.8.(c) since $\dim_K(P/I)$ is an upper bound for the degrees of the minimal polynomials. □

Combining these results we get the following algorithm.

```
Algorithm 5.10. (MinPolyQuotModular)
notation: $P = \mathbb{Q}[x_1, \ldots, x_n]$ with term ordering $\sigma$
Input  $I$, a zero-dimensional ideal in $P$, and a polynomial $f \in P$
1 compute the $\sigma$-reduced Gröbner basis of $I$
2 choose a usable prime $p$ — see Definition 5.5.
3 compute $f_p = \pi_p(f)$ and $I_{(p,\sigma)}$.
4 compute $\mu_p = \mu_{f_p, I_{(p,\sigma)}} \in \mathbb{F}_p[z]$, the minimal polynomial of $f_p$.
5 let $\mu_{\mathrm{crt}} = \mu_p$ and $p_{\mathrm{crt}} = p$.
6 Main Loop:
    6.1 choose a new usable prime $p$.
    6.2 compute the minimal polynomial $\mu_p \in \mathbb{F}_p[z]$.
    6.3 if $\deg(\mu_{\mathrm{crt}}) \neq \deg(\mu_p)$ then
        6.3.1 if $\deg(\mu_{\mathrm{crt}}) < \deg(\mu_p)$ then let $\mu_{\mathrm{crt}} = \mu_p$ and $p_{\mathrm{crt}} = p$.
        6.3.2 continue with next iteration of Main Loop
    6.4 let $\tilde{p}_{\mathrm{crt}} = p \cdot p_{\mathrm{crt}}$, and let $\tilde{\mu}_{\mathrm{crt}}$ be the polynomial whose coefficients are obtained
        by the Chinese Remainder Theorem from the coefficients of $\mu_{\mathrm{crt}}$ and $\mu_p$.
    6.5 compute the polynomial $\mu_{\mathrm{calc}} \in \mathbb{Q}[z]$ whose coefficients are obtained as the
        fault-tolerant rational reconstructions of the coefficients of $\tilde{\mu}_{\mathrm{crt}}$ modulo $\tilde{p}_{\mathrm{crt}}$.
    6.6 were all coefficients "reliably" reconstructed?
        yes if $\mu_{\mathrm{calc}} \neq 0$ and $\mu_{\mathrm{calc}}(g) \in I$ return $\boldsymbol{\mu_{\mathrm{calc}}}$
        no  let $\mu_{\mathrm{crt}} = \tilde{\mu}_{\mathrm{crt}}$ and $p_{\mathrm{crt}} = \tilde{p}_{\mathrm{crt}}$.
Output  $\mu_{\mathrm{calc}} \in \mathbb{Q}[z]$, the minimal polynomial $\mu_{f,I}$.
```

Proof. The correctness of this algorithm follows from Theorem 5.8 and the termination from Corollary 5.9. □

Remark 5.11. Termination of the *Main Loop* depends on the test $\mu_{\mathrm{calc}}(g) \in I$ in step MinPolyQuotModular-6.6(yes); however evaluating $\mu_{\mathrm{calc}}(g)$ modulo I is typically computationally expensive compared to the cost of a single iteration. For this reason, in step MinPolyQuotModular-6.5 we use the fault-tolerant rational reconstruction implemented in CoCoA (see [1]) which gives also an indication whether the reconstructed rational is "reliable" (*i.e.* heuristically probably correct). This is a computationally cheap criterion which surely indicates "reliable" almost as soon as $\tilde{p}_{\mathrm{crt}}$ becomes large enough to allow correct reconstruction, while also almost certainly indicating "not reliable" before then.

Once μ_{crt} has the correct degree, the degree check in step MinPolyQuotModular-6.3 ensures that only results from good primes are used; in this situation our fault-tolerant reconstruction is equivalent to Monagan's MQRR [8].

Remark 5.12. A disadvantage of Algorithm 5.10 is that it needs a Gröbner basis over $\mathbb{Q}$, requiring a potentially costly computation. We can make a faster heuristic variant of the algorithm by working directly with the given generators for I. Let G' be the set of given generators. We shall skip all "ugly" primes which divide $\mathrm{den}(G')$.

In steps MinPolyQuotModular-3 and 4 we use the ideal $\langle \pi_p(G') \rangle$ instead of $I_{(p,\sigma)}$. In the *Main Loop* we skip step MinPolyQuotModular-6.3, since there are no guarantees on the degrees of bad μ_p. In other words, we keep all the μ_p but when using the chinese remainder theorem to combine, we take only those polynomials having the same degree as the current μ_p. In step MinPolyQuotModular-6.6(yes) we return directly μ_{calc} skipping the check that $\mu_{\text{calc}}(g)$ is in I (since we want to avoid computing its Gröbner basis).

This heuristic algorithm may sometimes give a wrong answer: *e.g.* if given as input the generators in Example 4.9 — in this instance the answer would be obviously wrong since it is reducible.

There are only finitely many primes giving a bad μ_p. We can see this by picking some term ordering σ, and tracing through the steps to compute the reduced σ-Gröbner basis from the generators G'. Any prime which divides a denominator or a leading coefficient at any point in the computation may give a bad μ_p; to these we add the (finitely many) bad primes for that reduced Gröbner basis. All remaining primes will give a good μ_p.

6. Timings

In this section we illustrate the merits of the algorithms explained in the paper. Each example is described by introducing a polynomial ring P, an ideal I in P, and a polynomial f in P which is denoted either by ℓ if it is linear or by f if it is not linear. The task is to compute $\mu_{f,I}(z)$, the minimal polynomial of $\bar{f}$ in P/I.

6.1. Computing Minimal Polynomials in Finite Characteristic

In this subsection we present some timings for the computation of minimal polynomials of elements in zero-dimensional affine $\mathbb{F}_p$-algebras.

The column **Example** gives the reference number to the examples listed below. The column **GB** gives the times to compute the Gröbner basis (in seconds); the columns **Def, Mat, Elim** give the times (in seconds) of the computation of the algorithms 3.4, 3.2, and 3.1 respectively. The column **deg** gives the degree of the answer, as an indication of the complexity of the output.

Example	**GB**	**MinPoly**			
		Def	**Mat**	**Elim**	**deg**
6.1 f_1	0.38	7.00	9.28	50.54	500
6.1 f_2	0.38	21.50	13.75	∞	500
6.2	0.00	11.73	23.82	∞	720
6.3	0.17	9.34	14.15	∞	590
6.4	0.01	3.47	6.28	∞	462
6.5	0.00	18.00	42.31	∞	880

Example 6.1. The following is an example in characteristic 101.

Let $P = \mathbb{F}_{101}[x, y, z, t]$. Let $g_1 = xyzt + 83y^3 + 73x^2 - 85z^2 - 437t$, $g_2 = y^3zt + z - t$, $g_3 = t^4 + zt^2 - 324z^3 + 94x^2 + 76y$, $g_4 = x^{11}z + 26t^3 + 625y$.
Let $I = \langle g_1,\ g_2,\ g_3,\ g_4\rangle$, $\quad f_1 = x^5 - 3y^4 + 5z - t$ and $f_2 = x^{16} + 12y^{20} - z^{30}$.

Example 6.2. This is an example which uses the defining ideal of the splitting algebra of a polynomial of degree 6.

We let $P = \mathbb{F}_{101}[a_1, a_2, a_3, a_4, a_5, a_6]$, and for $j = 1, \dots, 6$ let s_j be the elementary symmetric polynomial in the indeterminates $a_1, a_2, a_3, a_4, a_5, a_6$. Then the ideal $I = \langle s_1,\ s_2,\ s_3,\ s_4,\ s_5 - 7,\ s_6 - 1\rangle$ is the defining ideal of the splitting algebra of the polynomial $x^6 - 7x + 1$. We let $\ell = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6$

Example 6.3. This is an example in characteristic $p = 32003$.

Let $P = \mathbb{F}_p[x, y, z, t]$, let $g_1 = xyzt^5 + x^3 + 73y^2 - z^2 - 2t$, $g_2 = x^6zt + z - t$, $g_3 = zt^2 + 7xy^2 - 34z^3 - 2t^4$, $g_4 = y^4z + x + 26t^3$. Let $I = \langle g_1,\ g_2,\ g_3,\ g_4\rangle$ and $f = xt^2 + 5z$.

Example 6.4. This is an example in characteristic $p = 101$.

Let $P = \mathbb{F}_p[x, y, z]$, let $f_1 = (x^7 - y - 3z)^2$, $f_2 = xy^5 - 7z^2 - 2$, $f_3 = yz^6 - x - z + 14$. Then let $J_1 = \langle f_1, f_2, f_3\rangle$, let $J_2 = \langle x, y, z\rangle^2$, let $I = J_1 \cap J_2$, and let $f = x^2 - 3xy - z$.

Example 6.5. This is an example in characteristic $p = 23$.

Let $P = \mathbb{F}_p[x, y, z]$, let $g_1 = x^{16} + 8x^{15} - 6x^{14} - 8x^{13} + 4x^{12} - 4x^{11} + 5x^{10} + 8x^9 + 5x^8 - 4x^7 + 5x^6 + 2x^5 - 7x^4 + 4x^3 + 10x^2 + 3x + 8$, $g_2 = y^5 - 7y^4 + 2y^3 + 11y^2 - y + 5$, $g_3 = z^{11} + 9z^{10} - 9z^9 + 7z^8 - 8z^7 - 4z^6 + 9z^5 + z^4 - 5z^3 + 7z^2 + z + 10$.

Let $I = \langle g_1,\ g_2,\ g_3\rangle$ and $\ell = 3x - 2y + 5z$.

6.2. Computing Minimal Polynomials in Characteristic Zero

In this subsection we present some timings for the computation of minimal polynomials of elements in zero-dimensional affine $\mathbb{Q}$-algebras.

The column **Example** gives the reference number to the examples listed below. The column **GB** gives the times to compute the Gröbner basis (in seconds); the columns **(MinPoly)** $\mathbb{Q}$, and **Modular** give respectively the times (in seconds) of the computation of the MinPolyQuotDef over $\mathbb{Q}$, and MinPolyQuotModular (using MinPolyQuotDef for the modular computations). The columns **(**$\#p$**)**, **coeff**, and **deg** give an indication of the complexity of the output: the first is the number of primes used to reconstruct the answer, the second expresses the maximum magnitude of the numerators and denominators of the coefficients, and the third is the degree.

Remark 6.6. CoCoA also offers `RingTwinFloat` arithmetic, an implementation of *heuristically guaranteed* floating point numbers (see [1]). We have also tried our algorithms using this representation of $\mathbb{Q}$, but the modular approach gave us better timings.

Example 6.7. This is an example with no particular structure.

Let $P = \mathbb{Q}[x, y, z, t]$, let $g_1 = xyzt + 83x^3 + 73y^2 - 85z^2 - 437t$, $g_2 = x^3zt + z - t$, $g_3 = zt^2 + 76x + 94y^2 - 324z^3 - 255t^4$, $g_4 = y^2z + 625x + 26t^3$, and let $I = \langle g_1,\ g_2,\ g_3,\ g_4\rangle$. Let $f = t^2 + 5z$.

The following two examples use ideals which are complete intersections; their reduced Gröbner basis are straightforward to compute.

Example	**GB**	**MinPoly**				
		$\mathbb{Q}$	**Modular**	$(\#p)$	**coeff**	**deg**
6.7	0.15	∞	26.86	130	$10^{389}, 10^{188}$	116
6.8 ℓ_1	0.00	47.86	1.29	24	$10^{93}, 10^{0}$	107
6.8 ℓ_2	0.00	226.34	3.77	50	$10^{210}, 10^{0}$	108
6.9	0.00	∞	12.29	77	$10^{330}, 10^{0}$	144
6.10	0.00	∞	1.43	17	$10^{64}, 10^{0}$	120
6.11	0.00	∞	1513.09	118	$10^{503}, 10^{0}$	720
6.12	1.50	134.44	5.92	59	$10^{246}, 10^{1}$	87
6.13	0.00	233.24	2.41	9	$10^{29}, 10^{4}$	230
6.14	0.42	∞	14.76	60	$10^{234}, 10^{19}$	149
6.15	0.33	5.33	0.85	31	$10^{108}, 10^{12}$	55

Example 6.8. Let $P = \mathbb{Q}[x, y, z, t]$, let $g_1 = x^4 + 83x^3 + 73y^2 - 85z^2 - 437t$, $g_2 = y^3 - x$, $g_3 = z^3 + z - t$, $g_4 = t^3 - 324z^2 + 94y^2 + 76x$. Let $I = \langle g_1,\ g_2,\ g_3,\ g_4 \rangle$ and $\ell_1 = x$, $\ell_2 = 2x + 3y - 4z + 12t$.

Example 6.9. Let $P = \mathbb{Q}[x, y, z, t]$, let $g_1 = x^4 + 83x^3 + 73y^2 - 85z^2 - 437t$, $g_2 = y^3 - z - t$, $g_3 = z^3 + z - t$, $g_4 = t^4 - 12z^2 + 77y^2 + 15x$. Let $I = \langle g_1,\ g_2,\ g_3,\ g_4 \rangle$ and $\ell = x - 3y - 12z + 62t$.

Example 6.10. This is an example which uses the defining ideal of the splitting algebra of a polynomial of degree 5.

We let $P = \mathbb{Q}[a_1, a_2, a_3, a_4, a_5]$, and for $j = 1, \ldots, 5$ let s_j be the elementary symmetric polynomial in the indeterminates a_1, a_2, a_3, a_4, a_5. Then we introduce the ideal $I = \langle s_1,\ s_2,\ s_3,\ s_4 + 1,\ s_5 - 2 \rangle$ which is the defining ideal of the splitting algebra of the polynomial $x^5 - x - 2$. We let $\ell = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5$.

Example 6.11. This is an example which uses the defining ideal of the splitting algebra of a polynomial of degree 6 (see also 6.2) We let $P = \mathbb{Q}[a_1, a_2, a_3, a_4, a_5, a_6]$, and for $j = 1, \ldots, 6$ let s_j be the elementary symmetric polynomial in the indeterminates $a_1, a_2, a_3, a_4, a_5, a_6$. The ideal $I = \langle s_1,\ s_2,\ s_3,\ s_4,\ s_5 - 7,\ s_6 - 1 \rangle$ is the defining ideal of the splitting algebra of the polynomial $x^6 - 7x + 1$. We let $\ell = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6$.

Example 6.12. We take as I the vanishing ideal of 87 random points with integer coordinates x, y, z (each with absolute value < 10000). Then we let $\ell = 44x + 3y - z$.

Example 6.13. In this example we let $g_1 = x^7 - y - 3z$, $g_2 = xy^5 - 5057z^2 - 2$, $g_3 = yz^6 - x - z + 14$, and $I = \langle g_1, g_2, g_3 \rangle$. Finally we let $\ell = x$.

Example 6.14. In this example we let $f_1 = x^5 - y - 3z$, $f_2 = xy^5 - 5057z^2 - 2$, $f_3 = yz^5 - x - z + 14$ and $J_1 = \langle f_1, f_2, f_3 \rangle$. Then we let $g_1 = x^2 - y - 3z$, $g_2 = xy - 5z^2 - 12$, $g_3 = z^3 - x - y + 4$ and $J_2 = \langle g_1, g_2, g_3 \rangle$. Then we let $I = J_1 \cap J_2$. Generators of I have very large coefficients, so we do not give them explicitly here. Finally we let $\ell = 7x - 5y + 2z$.

Example 6.15. This is a simplified version of Example 6.14, in the sense that J_2 and ℓ are the same. Instead we let $g_1 = x^3 - y - 3z$, $g_2 = xy^3 - 5057z^2 - 2$, $g_3 = yz^4 - x - z + 14$ and let $J_1 = \langle g_1, g_2, g_3 \rangle$.

7. Uses of Minimal Polynomials

In this section we let K be a field of characteristic zero or a perfect field of characteristic $p > 0$ having effective p-th roots, and let I be a zero-dimensional ideal in the polynomial ring $P = K[x_1, \ldots, x_n]$. We start the section by recalling a useful definition.

Definition 7.1. Let $f \in P$ be a non-zero polynomial with positive degree. We define the **square-free part**, $\operatorname{sqfree}(f)$, to be the product of all distinct irreducible factors of f (which are defined up to a constant factor). Equivalently, $\operatorname{sqfree}(f)$ is a generator of the radical of the principal ideal generated by f. If f is univariate, and the coefficient field has characteristic zero then $\operatorname{sqfree}(g)$ is $\frac{g}{\operatorname{GCD}(g,g')}$ up to a constant factor; if the characteristic is positive then we can use the algorithm described in Proposition 3.7.12 of [6].

In the next proposition we collect important results which will be used throughout the entire section.

Proposition 7.2. *Let K be a perfect field, let $P = K[x_1, \ldots, x_n]$, let I be a zero-dimensional ideal in P, and let $R = P/I$.*

(a) Let K be infinite.
  - *(a_1) If I is radical, the generic linear form $\ell \in P$ is such that we have the equality $\deg(\mu_{\ell,I}(z)) = \dim_K(P/I)$.*
  - *(a_2) If I is maximal, the generic linear form $\ell \in P$ is such that $\bar{\ell}$ is a primitive element of the field P/I.*

(b) Let K be finite. If I is maximal, there exists $f \in P$ such that $\bar{f}$ is a primitive element of the field P/I.

Proof. To prove claim (a) we observe that (a_2) is a special case of (a_1), hence we prove (a_1). Since I is radical and K is infinite, the Shape Lemma (see Theorem 3.7.25 of [6]) guarantees the existence of a linear change of coordinates which brings I into normal x_n-position, hence after the transformation the last indeterminate has squarefree minimal polynomial of degree $\dim_K(P/I)$. Equivalently, the generic linear change of coordinates yields a situation where the minimal polynomial of the last indeterminate is squarefree and has degree $\dim_K(P/I)$. If I is maximal then this polynomial is necessarily irreducible. This is exactly what Algorithm 7.13 tries to achieve via randomization in step IsMaximal-5 (the *Second Loop*).

The proof of claim (b) follows from the well-known fact that the multiplicative group of a finite field $L = P/I$ is cyclic, so that if a is a generator of $L\backslash\{0\}$ we have $L = K[a]$ which implies that $\deg(\mu_{a,I}(z)) = \dim_K(P/I)$. We then choose $f \in P$ such that $\bar{f} = a$. □

The following example shows that if K is finite, and I is radical but not maximal then it is possible that no element $f \in P$ exists such that $\deg(\mu_{\ell,I}(z)) = \dim_K(P/I)$.

Example 7.3. Let $K = \mathbb{F}_2$, let $P = K[x,y]$, $I = \langle x^2 + y,\ y^2 + y \rangle$. Then we have $I = M_1 \cap M_2 \cap M_3 \cap M_4$ where $M_1 = \langle x,\ y \rangle$, $M_2 = \langle x,\ y + 1 \rangle$, $M_3 = \langle x + 1,\ y \rangle$,

$M_4 = \langle x+1,\, y+1\rangle$. Whatever element $f \in P$ we choose we have $\deg(\mu_{f,I}(z)) \le 2$ while $\dim_K(P/I) = 4$.

7.1. IsRadical and Radical for a Zero-Dimensional Ideal

The goal of this subsection is to describe algorithms for checking if I is radical, and for computing the radical of I. We need the following results.

Proposition 7.4. *Let K be a perfect field, let $P = K[x_1, \ldots, x_n]$, let I be a zero-dimensional ideal in P, let $f_i(x_i)$ be such that $I \cap K[x_i] = \langle f_i(x_i)\rangle$ for $i = 1, \ldots, n$, and let $g_i = \mathrm{sqfree}(f_i(x_i))$. Then we have the equality $\sqrt{I} = I + \langle g_1, \ldots, g_n\rangle$.*

Proof. By Proposition 3.7.1 of [6], the polynomials $f_i(x_i)$ are non-zero. Since the ideal $J = I + \langle g_1, \ldots, g_n\rangle$ satisfies $I \subseteq J \subseteq \sqrt{I}$, we have $\sqrt{J} = \sqrt{I}$. By Proposition 3.7.9 of [6] we have $\mathrm{GCD}(g_i, g_i') = 1$ for all $i = 1, \ldots, n$, hence the conclusion follows from Seidenberg's Lemma (see Proposition 3.7.15 of [6]). □

Since $I \cap K[x_i] = \langle \mu_{x_i}(x_i)\rangle$, the above proposition can be rewritten as follows.

Corollary 7.5. *Let K be a perfect field, let $P = K[x_1, \ldots, x_n]$, let I be a zero-dimensional ideal in P, and let $g_i = \mathrm{sqfree}(\mu_{x_i}(x_i))$. Then we have $\sqrt{I} = I + \langle g_1, \ldots, g_n\rangle$.*

The following proposition shows that in some cases it is particularly easy to show that an ideal is radical.

Proposition 7.6. *Let K be a perfect field, let I be a zero-dimensional ideal in the polynomial ring $P = K[x_1, \ldots, x_n]$, and let $f \in P$. If the polynomial $\mu_{f,I}(z)$ is squarefree and $\deg(\mu_{f,I}(z)) = \dim_K(P/I)$, then I is a radical ideal.*

Proof. Consider the map $\alpha_f \colon K[z]/\langle \mu_{f,I}(z)\rangle \to P/I$ defined by $\bar{z} \mapsto \bar{f}$ which is injective by definition. Since $\dim_K(K[z]/\langle \mu_{f,I}(z)\rangle) = \deg(\mu_{f,I}(z)) = \dim_K(P/I)$, then α_f is also surjective and hence an isomorphism. By assumption, the polynomial $\mu_{f,I}(z)$ is squarefree and hence $P/I \cong K[z]/\langle \mu_{f,I}(z)\rangle$ is a reduced K-algebra which means that I is a radical ideal. □

The following algorithm determines whether a zero-dimensional ideal is radical.

```
Algorithm 7.7. (IsRadical0Dim)
notation: $K$ a perfect field and $P = K[x_1, \ldots, x_n]$
Input  $I$, a zero-dimensional ideal in $P$
1 compute $d = \dim_K(P/I)$
2 Main Loop: for $i = 1, \ldots, n$ do
    2.1 compute $\mu = \mu_{x_i,I}$
    2.2 if $\mu$ is not square-free then return false
    2.3 if $\deg(\mu) = d$ then return true
3 return true
Output  true/false indicating whether $I$ is radical or not.
```

Proof. Clearly, the algorithm ends after a finite number of steps and its correctness follows from Corollary 7.5 and Proposition 7.6 □

Similarly, we can describe an algorithm which computes the radical of a zero-dimensional ideal.

Algorithm 7.8. (Radical0Dim)

```
notation: $K$ a perfect field and $P = K[x_1, \dots, x_n]$
Input  $I$, a zero-dimensional ideal in $P$
1 let $J = I$ and compute $d = \dim_K(P/J)$
2 Main Loop: for $i = 1, \dots, n$ do
    2.1 compute $\mu = \mu_{x_i,J}$
    2.2 if $\mu$ is not square-free then
        2.2.1 let $\mu = \mathrm{sqfree}(\mu)$
        2.2.2 let $J = J + \langle \mu(x_i) \rangle$
        2.2.3 compute $d = \dim_K(P/J)$
    2.3 if $\deg(\mu) = d$ then return $J$
3 return $J$
Output  $J$: the radical of $I$
```

Proof. Clearly, the algorithm ends after a finite number of steps and its correctness follows from Proposition 7.6 and Corollary 7.5. □

One can imagine a fast, randomized heuristic version of this algorithm: we replace the *Main Loop* by the following steps: pick a random linear form ℓ, and set $\mu = \mathrm{sqfree}(\mu_{\ell,J})$; update $J = J + \langle \mu(\ell) \rangle$. The following example shows that picking a single random linear form is not sufficient in some cases; in fact, in this example n linearly independent linear forms must be used before the correct result is obtained.

Example 7.9. Let K be a field, let $P = K[x_1, \dots, x_n]$ with $n \geq 2$, and let the ideal $I = \langle x_1, \dots, x_n \rangle^2$. Now let $\ell \in P$ be any non-zero linear form. Clearly $\mu_{\ell,I}(z) = z^2$. Hence $2 = \deg(\mu_{\ell,I}(z)) < \dim(P/I) = n + 1$, and adding $\langle \ell \rangle$ to I does not yield $\langle x_1, \dots, x_n \rangle$.

7.2. IsMaximal, and IsPrimary for a Zero-Dimensional Ideal

In this subsection, we describe methods for checking if a zero-dimensional ideal is primary or is maximal. To do this we use different strategies depending on the characteristic of the base field. In particular, when K is a finite field with q elements we can use a specific tool, namely a K-vector subspace of $R = P/I$, called the **Frobenius space of** R and denoted by $\mathrm{Frob}_q(R)$. The main property is that its dimension is exactly the number of primary components of I. For the definition and basic properties of Frobenius spaces we refer to Section 5.2 of [7]. For convenience, we recall the definition here.

Definition 7.10. Let K be a finite field with q elements and let $R = P/I$ be a zero-dimensional K-algebra.

(a) The map $\Phi_q : R \to R$ defined by $a \mapsto a^q$ is a K-linear endomorphism of R called the q-**Frobenius endomorphism** of R.

(b) The fixed-point space of R with respect to Φ_q, namely the set $\{f \in R \mid f^q - f = 0\}$, is called the q-**Frobenius space** of R.

The following proposition describes some features of minimal polynomials when the zero-dimensional ideal I is primary or maximal.

Proposition 7.11. *Let I be a zero-dimensional ideal in $P = K[x_1, \ldots, x_n]$.*

(a) If I is primary then for any $f \in P$ its minimal polynomial $\mu_{f,I}(z)$ is a power of an irreducible polynomial.

(b) If I is maximal then for any $f \in P$ its minimal polynomial $\mu_{f,I}(z)$ is irreducible.

Proof. We use the same argument as in the proof of Proposition 7.6, so that we get an in injective K-algebra homomorphism $K[z]/\langle \mu_{f,I}(z) \rangle \to P/I$.

Now we prove claim (a). If I is primary then the only zero-divisors of P/I are nilpotent, hence the same property is shared by $K[z]/\langle \mu_{f,I}(z) \rangle$ which implies that $\mu_{f,I}(z)$ is a power of an irreducible element.

Analogously, if I is maximal then P/I is a field, hence $K[z]/\langle \mu_{f,I}(z) \rangle$ is an integral domain which concludes the proof. □

We have a sort of converse of the above proposition.

Proposition 7.12. *Let I be a zero-dimensional ideal in $P = K[x_1, \ldots, x_n]$, and let $f \in P$ be such that* $\deg(\mu_{f,I}(z)) = \dim(P/I)$.

(a) If $\mu_{f,I}(z)$ is a power of an irreducible factor then I is a primary ideal.

(b) If $\mu_{f,I}(z)$ is irreducible then I is a maximal ideal.

Proof. As in the proof of Proposition 7.11 we have an injective K-algebra homomorphism $K[z]/\langle \mu_{f,I}(z) \rangle \to P/I$. The assumption that $\deg(\mu_{f,I}(z)) = \dim(P/I)$ implies that this endomorphism is actually an isomorphism. Now if $K[z]/\langle \mu_{f,I}(z) \rangle$ has only one maximal ideal, the same property is shared by P/I which implies that I is a primary ideal and claim (a) is proved. Analogously, if $K[z]/\langle \mu_{f,I}(z) \rangle$ is a field, then also P/I is a field which means that I is a maximal ideal. □

7.3. IsMaximal

Our next goal is to check whether an ideal I in P is maximal, and the following algorithm provides an answer. Note that is a true algorithm when K is finite, whereas the termination is only heuristically guaranteed when K is infinite.

```
Algorithm 7.13. (IsMaximal)
notation: $K$ a perfect field and $P = K[x_1, \ldots, x_n]$
Input $I$, an ideal in $P$
1 if $I$ is not zero-dimensional, return false
2 compute $d = \dim_K(P/I)$
3 First Loop: for $i = 1, \ldots, n$ do
    3.1 compute $\mu = \mu_{x_i,I}$
    3.2 if $\mu$ is reducible, return false
    3.3 if $\deg(\mu) = d$ then return true
4 if $K$ is finite then
    4.1 compute $s = \dim_K(\mathrm{Frob}_q(P/I))$
    4.2 if $s = 1$ return true else return false
5 (else $K$ is infinite) Second Loop: repeat
    5.1 pick a random linear form $\ell \in P$
    5.1 compute $\mu = \mu_{\ell,I}$
    5.2 if $\mu$ is reducible, return false
    5.3 if $\deg(\mu) = d$ then return true
Output true/false indicating the maximality of $I$.
```

Proof. Let us show the correctness. In step 3.2, if μ is reducible, we conclude from Proposition 7.11.(b). In step 3.3, since μ is irreducible, if $\deg(\mu) = d$ then we conclude from Proposition 7.12.(b). If the *First Loop* completes without returning an answer, all polynomials $\mu_{x_i,I}(x_i)$ are irreducible and belong to I, hence I is radical by Seidenberg's Lemma (see [6], Proposition 3.7.15 and Corollary 3.7.16). Now we know that I is radical, we examine the two cases below.

First we consider the case when K is finite. Then the ideal I is maximal if and only if $\dim_K(\mathrm{Frob}_q(P/I)) = 1$ (see [7], Theorem 5.2.4.(b)). Therefore, when K is finite, steps 4.1 and 4.2 show that the algorithm is correct and terminates.

Now we consider the case when K is infinite. In step 5.2 if the minimal polynomial μ is reducible, Proposition 7.11.(b) tells us that I is not maximal. In step 5.3 we know that the polynomial μ is irreducible, so if $\deg(\mu) = d$, Proposition 7.12.(b) tells us that I is maximal. We conclude that also in this case the algorithm is correct. Its termination follows heuristically from Proposition 7.2.(a). □

Can we make this into a proper deterministic algorithm when K is infinite? The following remark answers this question.

Remark 7.14. If K is infinite, we can substitute the *Second Loop* with a check that in the ring P/I there are only trivial idempotents. How to do this is explained in Section 5.1.B of [7]. Although using that method would give us a deterministic algorithm, it is computationally very expensive.

Remark 7.15. Since the computation of the Frobenius space in step IsMaximal-4.1 might be costly, one could be tempted to first try a few random linear forms (as in the *Second Loop*). However, our experiments show that computing the minimal polynomial for a random linear form has a computational cost very similar to that for the Frobenius space, while potentially furnishing less information. In summary, there is no benefit from inserting such a "heuristic step" just before IsMaximal-4.1.

7.4. IsPrimary for a Zero-Dimensional Ideal

The goal of this subsection is to check whether a zero-dimensional ideal I in P is primary. The structure of the following algorithm is very similar to the structure of Algorithm 7.13. In particular, it is important to observe that also in this case it is a true algorithm when K is finite, whereas the termination is only heuristically guaranteed when K is infinite.

Algorithm 7.16. (IsPrimary0Dim)

```
notation: $P = K[x_1, \dots, x_n]$
Input $I$, a zero-dimensional ideal in $P$
1 let $J = I$ and compute $d = \dim_K(P/J)$
2 First Loop: for $i = 1$ to $n$ do
    2.1 compute $\mu = \mu_{x_i,J}$
    2.2 factorize $\mu$
    2.3 if $\mu$ is not a power of an irreducible factor return false
    2.4 if $\deg(\mu) = d$ then return true
    2.5 if $\mu$ is not square-free then
        2.5.1 let $\mu = \mathrm{sqfree}(\mu)$
        2.5.2 let $J = J + \langle \mu(x_i) \rangle$
        2.5.3 compute $d = \dim_K(P/J)$
        2.5.4 if $\deg(\mu) = d$ then return true
3 if $K$ is finite then
    3.1 compute $s = \dim_K(\mathrm{Frob}_q(P/I))$
    3.2 if $s = 1$ return true else return false
4 (else $K$ is infinite) Second Loop: repeat
    4.1 pick a random linear form $\ell \in P$
    4.2 compute $\mu = \mu_{\ell,J}$
    4.3 if $\mu$ is reducible return false
    4.4 if $\deg(\mu) = d$ then return true
Output true/false indicating whether $I$ is primary or not.
```

Proof. Let us show the correctness. In the *First Loop* we work with an ideal J such that $\sqrt{J} = \sqrt{I}$, because of the change we might perform in step 2.5. In particular J is primary if and only if I is primary. Moreover, at the end of the *First Loop*, $J = \sqrt{I}$ by Seidenberg's Lemma (see the proof of Algorithm 7.13).

In step 2.3, if μ is not a power of an irreducible, we conclude from Proposition 7.11.(a). In step 2.4, if $\deg(\mu) = d$ and μ is a power of an irreducible we conclude from Proposition 7.12.(a).

If the *First Loop* completes without returning an answer, we know that J is radical, and now examine the two cases.

First we look at the case when K is finite. As in the case of Algorithm 7.13, steps 3.1 and 3.2 guarantee the correctness and termination.

Now we look at the case when K is infinite. Since J is radical, checking that I is primary is equivalent to checking that J is maximal. Now, step 4 does exactly the same thing as step 5 of Algorithm 7.13 and the proof of the correctness is the same. Finally, the termination follows heuristically from Proposition 7.2.(a). □

Remark 7.17. When K is infinite, to turn this heuristically terminating algorithm into a true algorithm we can repeat the observations contained in Remark 7.14.

Remark 7.18. When K is finite, it would suffice to do simply steps IsPrimary0Dim-3.1 and IsPrimary0Dim-3.2 and conclude. However, our experiments suggest that nonetheless it is often faster to perform the *First Loop*, as it is quick and frequently determines the result.

Let us see an example which shows that the property of being primary strongly depends on the base field.

Example 7.19. Let K be a field, let $P = K[x]$, let $f(x) = x^4 - 10\,x^2 + 1$, and let $I = \langle f(x) \rangle$. Now, if $K = \mathbb{Q}$ we know that $f(x)$ is irreducible, hence we deduce that I is a maximal ideal. Conversely, if $K = \mathbb{F}_p$ it is known that $f(x)$ is reducible for every prime p, and hence I is not a primary ideal.

7.5. Primary Decomposition for a Zero-Dimensional Ideal

The theoretical background used in this paper for computing primary decompositions of zero-dimensional ideals in affine K-algebras is explained in Chapter 5 of [7]. The main aim of this approach is to exploit the efficient algorithms for computing minimal polynomials. Here we describe the algorithms implemented in CoCoA. In particular, we remark that the algorithm for characteristic 0 (or big characteristic) and for finite characteristic have the same structure except for the choice of a partially splitting polynomial.

First we show how the partially splitting polynomial is chosen. The function looking for a splitting polynomial has a *First Loop* over the indeterminates; if no splitting polynomial was found, it then calls the characteristic-dependent algorithm.

In particular, if the input ideal I is primary, it returns a polynomial f such that $\mu_{f,I}$ is a power of a single irreducible factor (together with the token `TotalSplit`). Otherwise it returns a polynomial f such that $\mu_{f,I}$ has at least two irreducible factors (together with the token `PartialSplit`).

The "unusual" returned values in steps PDSplitting-4(yes) and PDSplittingFiniteField-2 just emphasize that the ideal I is primary.

The three following functions reflect the implementation in CoCoA.

```
Algorithm 7.20. (PDSplitting)
notation: $P = K[x_1, \dots, x_n]$
Input $I$, a zero-dimensional ideal in $P$
1 compute $d = \dim_K(P/I)$
2 First Loop: for $i = 1, \dots, n$ do
    2.1 compute $\mu_i = \mu_{x_i,I}$
    2.2 factorize $\mu_i = \prod_j^s \mu_{ij}^{d_j}$
    2.3 if $\deg(\mu_i) = d$ then return ($x_i$, $\{\mu_{ij}^{d_j} \mid j = 1, \dots, s\}$, TotalSplit)
    2.4 if $s > 1$ then return ($x_i$, $\{\mu_{ij}^{d_j} \mid j = 1, \dots, s\}$, PartialSplit)
3 if $K$ is finite, return PDSplittingFiniteField($I$)
4 is $I + \langle \mathrm{sqfree}(\mu_i) \mid i = 1, \dots, n \rangle$ maximal?
    yes return (0, $\{z\}$, TotalSplit)
    no return PDSplittingInfiniteField($I$)
Output ($f$, factorization of $\mu_{f,I}$, TotalSplit/PartialSplit)
```

```
Algorithm 7.21. (PDSplittingFiniteField)
notation: $P = K[x_1, \dots, x_n]$, $K$ a finite field
Input $I$, a zero-dimensional ideal in $P$
1 compute FrB a $K$-basis of $\mathrm{Frob}_q(P/I)$ and let $s = \#(\mathrm{FrB})$
2 if $s = 1$ then return (0, $\{z\}$, TotalSplit)
3 pick a non-constant element $f$ of the basis FrB
4 compute $\mu = \mu_{f,I}$
5 factorize $\mu = \prod \mu_j$
6 if $\deg(\mu) = s$ then return ($f$, $\{\mu_j \mid j = 1, \dots, s\}$, TotalSplit)
7 return ($f$, $\{\mu_j \mid j = 1, \dots, s\}$, PartialSplit)
Output ($f$, factorization of $\mu_{f,I}$, TotalSplit/PartialSplit)
```

Remark 7.22. From Theorem 5.2.4 in [7] we know that for any zero-dimensional ideal I, $f \in \mathrm{Frob}_q(P/I)$ if and only if $\mu_{f,I}$ factorizes into distinct linear factors with multiplicity 1.

```
Algorithm 7.23. (PDSplittingInfiniteField)
notation: $P = K[x_1, \dots, x_n]$, $K$ an infinite field
Input $I$, a non-primary, zero-dimensional ideal in $P$
1 compute $d = \dim_K(P/I)$
2 Main Loop: repeat:
    2.1 pick a random linear form $\ell \in P$;
    2.2 compute $\mu = \mu_{\ell,I}$
    2.3 factorize $\mu = \prod_j^s \mu_j^{d_j}$
    2.4 if deg($\mu$) = $d$ then return ($\boldsymbol{\ell}$, $\{\boldsymbol{\mu_j^{d_j}} \mid \boldsymbol{j = 1, \ldots, s}\}$, TotalSplit)
    2.5 if $s > 1$ then return ($\boldsymbol{\ell}$, $\{\boldsymbol{\mu_j^{d_j}} \mid \boldsymbol{j = 1, \ldots, s}\}$, PartialSplit)
Output ($\ell$, factorization of $\mu_{\ell,I}$, TotalSplit/PartialSplit)
```

Now we are ready to see how the splittings are used to compute the primary decomposition.

```
Algorithm 7.24. PrimaryDecompositionCore
notation: $P = K[x_1, \ldots, x_n]$
Input $I$, a zero-dimensional ideal in $P$
1 let ($f$, $\{\mu_j^{d_j} \mid j{=}1, \ldots, s\}$, TotalSplit/PartialSplit) be the output of PDSplitting($I$)
2 if $s = 1$ then return ($\{\boldsymbol{I}\}$, TotalSplit)
3 else return ($\{\boldsymbol{I} + \langle \boldsymbol{\mu_j(f)^{d_j}} \rangle \mid \boldsymbol{j{=}1, \ldots, s}\}$, TotalSplit/PartialSplit)
Output ($\{J_1, \ldots, J_s\}$, TotalSplit/PartialSplit)    such that $I = J_1 \cap \cdots \cap J_s$
```

```
Algorithm 7.25. PrimaryDecomposition0Dim
notation: $P = K[x_1, \ldots, x_n]$
Input $I$, a zero-dimensional ideal in $P$
1 let ($\{J_1, \ldots, J_s\}$, TotalSplit/PartialSplit)
      be the output of $PrimaryDecompositionCore(I)$
2 if it is TotalSplit, return $\{\boldsymbol{J_1, \ldots, J_s}\}$
3 Main Loop: for $i = 1, \ldots, s$ do
    3.1 is $J_i$ primary?
          yes $Dec_i = \{J_i\}$
          no $Dec_i = PrimaryDecomposition0Dim(J_i)$    ⟵ recursive call
4 return $\boldsymbol{Dec_1} \cup \cdots \cup \boldsymbol{Dec_s}$
Output the primary decomposition of $I$
```

The column **Example** gives the reference number to the examples listed above. The other columns give, respectively, the timings (in seconds) of the computation of the algorithms 7.7, 7.13, 7.16, 7.8, and 7.25, and an indication of their answers.

Example	IsRadical		IsMaximal		IsPrimary		Radical	Primary Dec.	
									#Comp
6.1	6.07	false	5.13	false	5.19	false	9.77	6.94	5
6.2	0.03	true	0.00	false	0.00	false	0.02	8.31	144
6.3	9.90	false	9.72	false	9.90	false	67.92	11.78	11
6.4	2.94	false	2.72	false	2.66	false	7.65	6.06	6
6.5	0.02	true	18.02	true	18.06	true	0.02	18.38	1

Example	IsRadical		IsMaximal		IsPrimary		Radical	Primary Dec.	
									#Comp
6.7	22.44	false	6.14	false	6.23	false	159.44	13.86	2
6.8	1.68	false	1.33	false	1.33	false	1.69	2.81	2
6.9	3.94	false	3.19	false	3.15	false	4.14	6.41	2
6.10	0.01	true	4.45	true	3.90	true	0.01	4.11	1
6.12	2.72	true	1.10	false	0.95	false	2.80	45.87	87
6.13	2.54	true	2.58	true	2.52	true	2.48	2.66	1
6.14	1.46	true	1.48	false	1.49	false	1.44	8.11	2
6.15	0.17	true	0.15	false	0.16	false	0.15	0.54	2

References

[1] J. Abbott, *Fault-Tolerant Modular Reconstruction of Rational Numbers*, J. Symb. Comp. **80P3**, pp. 707–718.

[2] J. Abbott and A.M. Bigatti *CoCoALib: a C++ library for doing Computations in Commutative Algebra.* Available at `http://cocoa.dima.unige.it/cocoalib`

[3] J. Abbott, A.M. Bigatti, G. Lagorio *CoCoA-5: a system for doing Computations in Commutative Algebra.* Available at `http://cocoa.dima.unige.it`

[4] J. Abbott, A. Bigatti, L. Robbiano, *Implicitization of Hypersurfaces* J. Symb. Comput. **81** (2017), pag 20–40.

[5] J. Abbott, A. Bigatti, L. Robbiano, *Ideals Modulo p*, In progress.

[6] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 1*, Springer, Heidelberg 2000 (second edition 2008).

[7] M. Kreuzer and L. Robbiano, *Computational Linear and Commutative Algebra*, Springer, Heidelberg 2016.

[8] M. Monagan, *Maximal Quotient Rational Reconstruction: An Almost Optimal Algorithm for Rational Reconstruction.* Proc. ISSAC 2004, pp. 243–249, ACM 2004.