Eidgenössische Technische Hochschule Zürich

Computational Theory of Polynomial Ideals

a Bachelor Thesis

written by
Paul Steinmann

supervised by
Prof. Dr. Richard Pink

Abstract

We provide methods to do explicit calculations in a polynomial ring in finitely many variables over a field. We develop algorithms to compute quotients of ideals, the radical of an ideal and a primary decomposition of an ideal. We also present methods to solve explicit tasks such as testing for prime ideals or identical ideals.

February 2015

Contents

1 Introduction 3

2 Notation 4

3 Gröbner Bases 5
- 3.1 Basic definitions 5
- 3.2 Computing Gröbner Bases 8

4 Quotients of Ideals 14

5 Radicals 16
- 5.1 Basics 16
- 5.2 Ideals of finite codimension 17
- 5.3 The general case 20

6 Primary Decomposition 24
- 6.1 Ideals of finite codimension 24
- 6.2 The general case 32

7 Complexity 34

8 Conclusion 35

References 36

1 Introduction

Polynomial rings over fields arise in many areas of mathematics, for instance in algebraic geometry. It is natural to ask to which extent explicit computation in such polynomial rings are possible. Today, computer algebra systems like MAPLE or MATHEMATICA are very useful tools to test conjectures in special cases before trying to prove them. There is a lot of computational theory for algorithms used to compute even the simplest objects in a polynomial ring. Computations in one variable are fairly simple, due to the fact that a polynomial ring in one variable over a field is a principal ideal domain and hence the very powerful Euclidean algorithm can be used. However, computations become more complicated when dealing with multivariate polynomial rings. Some of the computational theory will be presented and explained in this thesis. Certain objects, for example the radical of an ideal, can be computed using different characterisations, which result in different algorithms. There will be a short discussion of this fact and a comparison between algorithms at the end.

A key concept in this setting of computational algebra is the one of Gröbner bases. Presented in section 3, this concept will be used throughout the whole thesis. We lay our focus on three objects associated to polynomial ideals: quotients of ideals, the radical of an ideal and a primary decomposition of an ideal. We develop algorithms to compute these objects. There are also several other tasks that we will be able to do computationally. The main algorithms are marked as "Algorithm" and are written in pseudo-code, whereas the simpler tasks such as testing for prime ideals are marked as "Task" and have no special syntactical structure. In the end we will be able to do almost every computation that a standard computer algebra system can do in the area of polynomial ideals.

The prerequisites for this thesis are a standard algebra course and some basic knowledge of commutative algebra, mainly radical ideals and primary decompositions. Everything needed can be found in the first few chapters of Atiyah and Macdonald's standard introduction [1].

2 Notation

We will always consider a field K and denote by $\overline{K}$ its algebraic closure. Let $X_1, \ldots, X_n$ be n independent variables and define $\underline{X} := \{X_1, \ldots, X_n\}$. We denote the polynomial ring in n variables over K by $K[\underline{X}]$. Later on, we will invert some of the variables to form a rational function field. In doing so, we will write $\underline{X} = \underline{Y} \sqcup \underline{Z}$ and mean that $\underline{Y}$ and $\underline{Z}$ are disjoint subsets of $\underline{X}$ and their union is $\underline{X}$. We can then, for instance, form the ring $K(\underline{Y})[\underline{Z}]$ of polynomials in $\underline{Z}$ over the rational function field $K(\underline{Y})$. The integer $n > 0$ is arbitrary but will always denote the total number of variables.

For computations with an ideal, we need a finite generating set of the ideal. Thus, in the algorithms and tasks we tacitly assume that a finite generating set of I is given. For a finite subset $F \subset K[\underline{X}]$ we denote by $\langle F \rangle \subset K[\underline{X}]$ the ideal generated by F. If the ring in which the ideal is generated is not clear from the context, we indicate the ring as a subscript. For instance, we will write $\langle F \rangle_{K(\underline{Y})[\underline{Z}]}$. For elements $f_1, \ldots, f_m \in K[\underline{X}]$ we write $\langle f_1, \ldots, f_m \rangle$ instead of $\langle \{f_1, \ldots, f_m\} \rangle$.

Let R and S be two rings and $\varphi : R \to S$ be a ring homomorphism. Let $I \subset R$ and $J \subset S$ be ideals. We use Atiyah and Macdonald's ([1]) notation and write $I^e := \langle \varphi(I) \rangle$ for the extension ideal of I and $J^c := \varphi^{-1}(J)$ for the contraction ideal of J. We will not state the homomorphism explicitly if it is clear from the context. We also use the notation $I^{ec} := (I^e)^c$ and $J^{ce} := (I^c)^e$.

3 Gröbner Bases

This section follows the book of Cox, Little and O'Shea [3].

3.1 Basic definitions

We will generalize the concept of degree and the Euclidean algorithm for polynomial rings in one variable to an algorithm for a ring of multivariate polynomials $K[\underline{X}]$.

Definition 3.1. A **monomial ordering** $\succeq$ on $K[\underline{X}]$ is a binary relation $\succeq$ on $\mathbb{Z}_{\geq 0}^n$ with the following properties:

(i) The relation $\succeq$ is a total ordering on $\mathbb{Z}_{\geq 0}^n$.

(ii) For all $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$ such that $\alpha \succeq \beta$ it follows that $\alpha + \gamma \succeq \beta + \gamma$.

(iii) Every non-empty subset has a smallest element, i.e. $\succeq$ is a well-ordering on $\mathbb{Z}_{\geq 0}^n$.

Example 3.2. The standard ordering relation $\geq$ on $\mathbb{Z}_{\geq 0}$ is a total ordering and a well-ordering. Furthermore, for all $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}$ such that $\alpha \geq \beta$ we have $\alpha + \gamma \geq \beta + \gamma$. Therefore $\geq$ is a monomial ordering on $K[X_1]$.

Example 3.3. We define the monomial ordering $\succeq_{\text{lex}}$ on $K[\underline{X}]$ such that for all $\alpha := (\alpha_1, \ldots, \alpha_n)$, $\beta := (\beta_1, \ldots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$ we have $\alpha \succeq_{\text{lex}} \beta$ if and only if the leftmost non-zero entry in $(\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$ is positive. This is called the **lexicographical ordering**. For instance, in the lexicographical ordering we have $(0, 1, 5, 2) \succeq_{\text{lex}} (0, 1, 2, 4)$ since $(0, 1, 5, 2) - (0, 1, 2, 4) = (0, 0, 3, -2)$ and the leftmost non-zero entry 3 is positive. Using the result of Example 3.2 we deduce that $\succeq_{\text{lex}}$ is a monomial ordering.

Definition 3.4. Let $f = \sum_\alpha a_\alpha X^\alpha \in K[\underline{X}]$ with multi-index notation and let $\succeq$ be a monomial ordering on $K[\underline{X}]$.

(i) The **degree** of f with respect to $\succeq$ is $\deg(f) := \max\{\alpha \in \mathbb{Z}_{\geq 0}^n \mid a_\alpha \neq 0\}$ if f is non-zero and $\deg(0) := -\infty$. Here, the maximum is taken with respect to $\succeq$.

(ii) The **leading coefficient** of f is $\text{LC}(f) := a_{\deg(f)} \in K$ if f is non-zero, and $\text{LC}(0) := 0$.

(iii) The **leading monomial** of f is $\text{LM}(f) := X^{\deg(f)}$ if f is non-zero, and $\text{LM}(0) := 1$.

(iv) The **leading term** of f is $\text{LT}(f) := \text{LC}(f) \cdot \text{LM}(f)$.

Remark 3.5. Later on, we will need to distinguish leading terms in different rings. For this purpose, if $\underline{X} = \underline{Y} \sqcup \underline{Z}$ and $f \in K[\underline{X}]$ we write $\text{LT}_{\underline{Z}}(f)$ for the leading term of f in the ring $K(\underline{Y})[\underline{Z}]$ and $\text{LT}_{\underline{X}}(f)$ for the leading term in $K[\underline{X}]$. We denote $\text{LC}(f)$ analogously.

Definition 3.6. For any subset $F \subset K[\underline{X}]$ we define the set of leading terms $\text{LT}(F) := \{\text{LT}(f) \mid f \in F\}$ and the set of leading monomials $\text{LM}(F) := \{\text{LM}(f) \mid f \in F\}$.

Now we can define Gröbner bases. There are several equivalent definitions and the one below is not the most intuitive one. However, this technical property is easier to use:

Definition 3.7. Let $\succeq$ be a monomial ordering on $K[\underline{X}]$ and let $I \subset K[\underline{X}]$ be an ideal. A **Gröbner basis** of I is a finite subset $G \subset I$ such that $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$.

Remark 3.8. From now on, we will always assume that some monomial ordering $\succeq$ has been chosen and that all Gröbner bases and leading terms are taken with respect to this ordering unless stated otherwise.

In order to use Gröbner bases we need some basic statements.

Lemma 3.9. *Let $I \subset K[\underline{X}]$ be an ideal and let $f, g_1, \ldots, g_m \in I$. If $LT(f)$ lies in the ideal $\langle LT(g_1), \ldots, LT(g_m)\rangle$, then $f = 0$ or there is some $1 \leq k \leq m$ such that $LT(g_k)$ divides $LT(f)$.*

Proof. By assumption, there exist $h_1, \ldots, h_m \in K[\underline{X}]$ such that $\mathrm{LT}(f) = \sum_{i=1}^m h_i \mathrm{LT}(g_i)$. For each $1 \leq i \leq m$ write $h_i = \sum_\alpha a_\alpha^i X^\alpha$ with $a_\alpha^i \in K$ for all α. Then $\mathrm{LT}(f) = \sum_{i=1}^m \sum_\alpha a_\alpha^i X^\alpha \mathrm{LT}(g_i)$. If f is non-zero, then $\mathrm{LT}(f)$ is a non-zero monomial. It follows that, on the right hand side, there is only one non-zero monomial. Thus there is a constant $\beta \in K$ such that $\mathrm{LT}(f) = \beta a_\alpha^k X^\alpha \mathrm{LT}(g_k)$ for some $1 \leq k \leq m$ and some α. Hence $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g_k)$ or $f = 0$. □

Proposition 3.10. *Every ideal $I \subset K[\underline{X}]$ has a Gröbner basis. Furthermore, every Gröbner basis of I is a generating set of I.*

Proof. (i) Let $M := \{\langle \mathrm{LT}(F)\rangle \mid F \subset I \text{ is a finite subset}\}$. Since $K[\underline{X}]$ is a Noetherian ring, the ideal $\langle \mathrm{LT}(I)\rangle$ is Noetherian as a module over $K[\underline{X}]$. Therefore M has a maximal element $\langle \mathrm{LT}(G)\rangle \in M$, where $G \subset I$ is a finite subset. Let $f \in I$. Since $\langle \mathrm{LT}(G)\rangle$ is a maximal element of M, we have that $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(G \cup \{f\})\rangle$. Hence $\mathrm{LT}(f) \in \langle \mathrm{LT}(G)\rangle$ and G is thus a Gröbner basis of I.

(ii) If $I = \langle 0\rangle$, the only possible Gröbner bases are $\emptyset$ and $\{0\}$. Both of them generate I.

Let G be a Gröbner basis of $I \neq \langle 0\rangle$. We prove that $I = \langle G\rangle$ by transfinite induction on the degree of elements in I. If $f = 0 \in I$ then $f \in \langle G\rangle$. So let $f \in I$ be non-zero. Assume that for all $f' \in I$ the condition $\deg(f) \succ \deg(f')$ implies that $f' \in \langle G\rangle$. By definition of a Gröbner basis, we have $\mathrm{LT}(f) \in \langle \mathrm{LT}(G)\rangle$. By Lemma 3.9 there exists an element $g \in G$ such that $\mathrm{LT}(g)$ divides $\mathrm{LT}(f)$. Thus $\mathrm{LT}(f) = h\mathrm{LT}(g)$ for some $h \in K[\underline{X}]$. Since $\mathrm{LT}(f)$ and $\mathrm{LT}(g)$ consist of only one term and are both non-zero, the polynomial h has the same property. Hence $h = \mathrm{LT}(h)$ and $\mathrm{LT}(f) = \mathrm{LT}(h)\mathrm{LT}(g) = \mathrm{LT}(hg)$. We have $\deg(f) \succ \deg(f - hg)$ by definition of the leading term. By induction hypothesis $f - hg \in \langle G\rangle$ and hence $f \in \langle G\rangle$. The claim follows with transfinite induction. □

We turn to the generalization of the Euclidean algorithm.

Definition 3.11. Let $f_1, \ldots, f_m \in K[\underline{X}]$ and define $F := \{f_1, \ldots, f_m\}$. Let $f \in K[\underline{X}]$. A **remainder on division** of f with respect to F is an element $\overline{f}^F \in K[\underline{X}]$ such that there exist $h_1, \ldots, h_m \in K[\underline{X}]$ with the following properties:

(i) The polynomial f can be written as $f = \sum_{i=1}^m h_i f_i + \overline{f}^F$.

(ii) No term of $\overline{f}^F$ is divisible by any of $(\mathrm{LT}(f_i))_{i=1}^m$.

(iii) For all $1 \leq i \leq m$ we have $\deg(h_i f_i) \preceq \deg(f)$.

Algorithm 3.12. Let $f_1, \ldots, f_m \in K[\underline{X}]$ and define $F := \{f_1, \ldots, f_m\}$. Let $f \in K[\underline{X}]$. The following algorithm computes a remainder on division $\overline{f}^F$ and elements $h_1, \ldots, h_m \in K[\underline{X}]$ as in Definition 3.11.

Input: $F = (f_1, ..., f_m),\ f \in K[\underline{X}]$
Output: $r = \overline{f}^F$, some remainder on division; $h_1, \ldots, h_m$
begin
  $h_i := 0$ for all $1 \leq i \leq m$
  $r := 0$
  $p := f$
  while $p \neq 0$ **do**
    $i := 1$
    divisionoccured := false
    while $i \leq m$ **and** *divisionoccured = false* **do**
      if *LT*(f_i) *divides LT*(p) **then**
        $h_i := h_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
        $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$
        divisionoccured := true
      else
        $i := i + 1$
      end
    end
    if *divisionoccured = false* **then**
      $r := r + \mathrm{LT}(p)$
      $p := p - \mathrm{LT}(p)$
    end
  end
end

Proof. We first show that the algorithm terminates after finitely many steps. Note that the inner while-loop has at most m steps and thus terminates in every step of the outer while-loop. So the only possibility that the algorithm does not terminate is if p is non-zero at all times. If $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ for some $1 \leq i \leq m$, then in the next step p is reduced to $p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$. Then $\deg(p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i) \prec \deg(p)$. If on the other hand no $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$, then the inner while-loop terminates with *divisionoccured* = $false$. This implies that p is reduced to $p - \mathrm{LT}(p)$ for the next step, due to the if-statement at the bottom. Then $\deg(p - \mathrm{LT}(p)) \prec \deg(p)$. So in each step of the outer while-loop, the degree of p strictly decreases. If the loop did not terminate, we would have an infinitely decreasing sequence. This cannot exist because of the well-ordering condition of monomial orderings. Thus the algorithm terminates after finitely many steps. For later use, note that $\deg(p) \preceq \deg(f)$ during the whole algorithm.

We now show that after every step of the outer while-loop we have $f = \sum_{i=1}^{m} h_i f_i + r + p$ with $\deg(h_i f_i) \preceq \deg(f)$ for all $1 \leq i \leq m$. This is true before the first step. Now fix a

step of the outer while-loop. Let $r, p, (h_i)_{i=1}^m$ denote the elements before the step which have the desired property and let $r', p', (h_i')_{i=1}^m$ denote the elements after the step. If no $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ then $h_i' = h_i$ for all $1 \leq i \leq m$. Also $r' = r + \mathrm{LT}(p)$ and $p' = p - \mathrm{LT}(p)$. It follows that $f = \sum_{i=1}^m h_i' f_i + r' + p'$ and $\deg(h_i' f_i) \preceq \deg(f)$ for all $1 \leq i \leq m$. If, on the other hand, some $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$, then $h_j' = h_j$ for all $j \neq i$ and $r' = r$. Furthermore $h_i' = h_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$ and $p' = p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$, so $h_i' f_i + p' = h_i f_i + p$. Thus $f = \sum_{i=1}^m h_i' f_i + r' + p'$ and $\deg(h_i' f_i) \preceq \max\{\deg(h_i f_i), \deg(p)\} \preceq \deg(f)$ for all $1 \leq i \leq m$. Because the property holds after each step, it also holds for the output.

It remains to show that the output r is not divisible by any of $(\mathrm{LT}(f_i))_{i=1}^m$. At the beginning $r = 0$, and the only place where a term is added to r is in the if-statement at the bottom. But the term is only added if it was not divisible by any of $(\mathrm{LT}(f_i))_{i=1}^m$. So r has the desired property and is thus a remainder on division. □

Remark 3.13. Algorithm 3.12 shows that for all finite subsets $F \subset K[\underline{X}]$ and elements $f \in K[\underline{X}]$ there is a remainder on division of f with respect to F. However, in general it need not be unique. Whenever we use a remainder on division $\overline{f}^F$, we assume that some choice has been made. This choice will only affect the explicit calculations and not the general statements.

Proposition 3.14. *Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis of an ideal $I \subset K[\underline{X}]$. For all $f \in K[\underline{X}]$, there is a unique remainder on division of f with respect to G.*

Proof. Let $f \in K[\underline{X}]$ and let $r, r' \in K[\underline{X}]$ be two polynomials both satisfying the properties of a remainder on division of f with respect to G. Then we have $r - r' = (f - r') - (f - r) \in I$. Assume that $r - r' \neq 0$. By Lemma 3.9, there exists an element $g_i \in G$ such that $\mathrm{LT}(g_i)$ divides $\mathrm{LT}(r - r')$. Since $r - r' \neq 0$, this implies that some term of r or of r' must be divisible by $\mathrm{LT}(g_i)$, which is not true. So $r - r' = 0$. □

The following proposition was, historically, the motivation to introduce Gröbner bases. In fact, it is one of the equivalent definitions of a Gröbner basis.

Proposition 3.15. *Let $I \subset K[\underline{X}]$ be an ideal and $G = \{g_1, \ldots, g_m\} \subset I$ a Gröbner basis of I. Then a polynomial $f \in K[\underline{X}]$ lies in I if and only if $\overline{f}^G = 0$.*

Proof. Let $f \in I$. Then $\overline{f}^G \in I$ by definition of a remainder on division, and no term of $\overline{f}^G$ is divisible by any element of $\mathrm{LT}(G)$. But G is a Gröbner basis, so $\mathrm{LT}(\overline{f}^G) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G) \rangle$. It follows by Lemma 3.9 that $\overline{f}^G = 0$.
Conversely, if $\overline{f}^G = 0$, then f is a linear combination of elements of G, so $f \in I$. □

3.2 Computing Gröbner Bases

The key to an algorithm which computes a Gröbner basis is a technical criterion for Gröbner bases developed by Buchberger.

Definition 3.16. Let $f, g \in K[\underline{X}]$ be non-zero and let $\alpha := \deg(f)$ and $\beta := \deg(g)$. Set $\gamma := (\gamma_1, \ldots, \gamma_n)$ where $\gamma_i := \max(\alpha_i, \beta_i)$ for each $1 \leq i \leq n$. The ***S*-polynomial** of f and g is defined by

$$S(f,g) := \frac{X^\gamma}{\mathrm{LT}(f)} f - \frac{X^\gamma}{\mathrm{LT}(g)} g,$$

using multi-index notation.

Lemma 3.17. *Let $f_1, \ldots, f_s \in K[\underline{X}]$ be all non-zero with $\delta := \deg(f_1) = \cdots = \deg(f_s)$. For all $i \neq j$ we have $\deg(S(f_i, f_j)) \prec \deg(f_i)$. Let $c_1, \ldots, c_s \in K$ satisfy $\deg(\sum_{i=1}^s c_i f_i) \prec \delta$. Then there are coefficients $d_{ij} \in K$ for all $1 \leq i, j \leq s$ such that $\sum_{i=1}^s c_i f_i = \sum_{i \neq j} d_{ij} S(f_i, f_j)$.*

Proof. For all $1 \leq i \leq s$ define $p_i := \frac{f_i}{\mathrm{LC}(f_i)}$ and $d_i := c_i \mathrm{LC}(f_i)$. Then for all $i \neq j$ we have $S(f_i, f_j) = \frac{X^\delta}{\mathrm{LT}(f_i)} f_i - \frac{X^\delta}{\mathrm{LT}(f_j)} f_j = p_i - p_j$. Since every p_i has leading coefficient 1 and they all have the same degree we find that $\deg(p_i - p_j) \prec \deg(p_i) = \deg(f_i)$, proving the first statement of the lemma. Now consider the following sum:

$$\sum_{i=1}^s c_i f_i = \sum_{i=1}^s d_i p_i = \sum_{i=1}^s d_i (p_i - p_1) + \left(\sum_{i=1}^s d_i \right) p_1 \tag{1}$$

Since $\deg(\sum_{i=1}^s c_i f_i) \prec \delta$ we know that $\sum_{j=1}^s d_j = 0$, so the second sum of the right hand side of equation (1) vanishes. Thus $\sum_{i=1}^s c_i f_i = \sum_{i=1}^s d_i S(f_i, f_1)$. □

Theorem 3.18 (Buchberger's Criterion)**.**
Let $I \subset K[\underline{X}]$ be an ideal and let $G = \{g_1, \ldots, g_m\} \subset I$ be a generating set of I not containing 0. Then G is a Gröbner basis of I if and only if $\forall i \neq j : \overline{S(g_i, g_j)}^G = 0$.

Proof. Assume that G is a Gröbner basis. Then by definition of the S-polynomial, we have $S(g_i, g_j) \in I$ for all $i \neq j$. Thus $\overline{S(g_i, g_j)}^G = 0$ by Proposition 3.15. This proves one direction of the equivalence.

Conversely, assume that $\overline{S(g_i, g_j)}^G = 0$ for all $i \neq j$. Using Definition 3.7 of a Gröbner basis, we need to show that $\mathrm{LT}(f) \in \langle \mathrm{LT}(G) \rangle$ for all $f \in I$. If f is zero, this is true, so let $f \in I$ be non-zero. Since G generates I, there exist $h_1, \ldots, h_m \in K[\underline{X}]$ such that $f = \sum_{i=1}^m h_i g_i$. Since a monomial ordering is a well-ordering, we can choose the h_i such that $\delta := \max\{\deg(h_1 g_1), \ldots, \deg(h_m g_m)\}$ is minimal. Set $d(i) := \deg(h_i g_i)$ for all $1 \leq i \leq m$ and write

$$f = \sum_{d(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{d(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{d(i) \prec \delta} h_i g_i \tag{2}$$

Note that only the first sum has terms of degree equal to δ. We claim that $\deg(f) = \delta$. Suppose $\deg(f) \prec \delta$. By Lemma 3.17, there exist coefficients $c_{ij} \in K$ for $i \neq j$ such that $\sum_{d(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{i \neq j} c_{ij} S(\mathrm{LT}(h_i) g_i, \mathrm{LT}(h_j) g_j)$, where $c_{ij} = 0$ whenever $d(i) \prec \delta$

or $d(j) \prec \delta$. For all $i \neq j$ with $d(i) = d(j) = \delta$ we have

$$S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j) = \frac{X^\delta}{\mathrm{LT}(h_i g_i)}\mathrm{LT}(h_i)g_i - \frac{X^\delta}{\mathrm{LT}(h_j g_j)}\mathrm{LT}(h_j)g_j = X^{\delta-\gamma_{ij}}S(g_i, g_j)$$

for some $\gamma_{ij} \in \mathbb{Z}^n_{\geq 0}$. By assumption $\overline{S(g_i, g_j)}^G = 0$ for all $i \neq j$. Hence there exist $r_\ell^{ij} \in K[\underline{X}]$ for all $1 \leq \ell \leq m$ and $i \neq j$ such that $\deg(r_\ell^{ij} g_\ell) \preceq \deg(S(g_i, g_j))$ and $S(g_i, g_j) = \sum_{\ell=1}^m r_\ell^{ij} g_\ell$. We thus find:

$$\sum_{d(i)=\delta} \mathrm{LT}(h_i)g_i = \sum_{i\neq j} c_{ij} S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j) = \sum_{i\neq j}\sum_{\ell=1}^m c_{ij} X^{\delta-\gamma_{ij}} r_\ell^{ij} g_\ell \tag{3}$$

Furthermore, for all $1 \leq \ell \leq m$ and $i \neq j$ we have

$$\deg(X^{\delta-\gamma_{ij}} r_\ell^{ij} g_\ell) \preceq \deg(X^{\delta-\gamma_{ij}} S(g_i, g_j)) = \deg(S(\mathrm{LT}(h_i)g_i, \mathrm{LT}(h_j)g_j)) \prec \deg(h_i g_i)$$

where the last inequality follows from Lemma 3.17. Combining equation (2) and (3) yields f as a linear combination of $(g_i)_{i=1}^m$ such that every term has degree strictly less than δ. This contradicts the minimality of δ, and thus the degree of f must equal δ. So $\mathrm{LT}(g_k)$ divides $\mathrm{LT}(f)$ for some $1 \leq k \leq m$ and therefore $\mathrm{LT}(f) \in \langle \mathrm{LT}(G) \rangle$. □

Using Buchberger's criterion, we can now check whether a given generating set of an ideal is a Gröbner basis. More importantly, we have an algorithm which computes a Gröbner basis of a given ideal.

Algorithm 3.19 (Buchberger)**.** Let $I \subset K[\underline{X}]$ be an ideal and $\succeq$ a monomial ordering on $K[\underline{X}]$. The following algorithm computes a Gröbner basis of I with respect to $\succeq$.

Input: $F = (f_1, ..., f_m)$, a generating set of I
Output: $G =$ a Gröbner basis of I w.r.t. $\succeq$
begin
  $G := F$
  repeat
    $G' := G$
    foreach *pair* $p, q \in G'$ *with* $p \neq q$ **do**
      $S := \overline{S(p,q)}^{G'}$ with respect to $\succeq$ (Algorithm 3.12)
      if $S \neq 0$ **then**
        $G := G' \cup \{S\}$
      end
    end
  until $G = G'$
end

Proof. Assume that the algorithm never terminates. This is only possible if G and G' never coincide in the outer loop. This implies $S = \overline{S(p,q)}^{G'} \neq 0$ for some $p, q \in G'$ with

$p \neq q$. By definition of a remainder on division and Lemma 3.9, we have $\mathrm{LT}(S) \notin \langle \mathrm{LT}(G') \rangle$. But $\mathrm{LT}(S) \in \langle \mathrm{LT}(G) \rangle$ and $G' \subset G$. Thus $\langle \mathrm{LT}(G') \rangle \subsetneq \langle \mathrm{LT}(G) \rangle$. So if the algorithm never terminates, there is a strictly increasing sequence of ideals in $K[\underline{X}]$. But this contradicts $K[\underline{X}]$ being Noetherian. So the algorithm must terminate after finitely many steps.

Now consider the output G of the algorithm. The algorithm has terminated, so $G' = G$ in the outer loop. If $S := \overline{S(p,q)}^{G'} \neq 0$ for some $p, q \in G'$, then $S \notin G'$ by definition of a remainder on division. Thus $G' \subsetneq G = G' \cup \{S\}$. This is a contradiction. So when the algorithm terminates, we have $\overline{S(p,q)}^{G} = 0$ for all $p, q \in G$. Note also that $F \subset G \subset I$ at all times, so G is always a generating set of I. It follows by Theorem 3.18 that G is a Gröbner basis of I. □

Task 3.20 (Ideal Membership)**.** Let $I \subset K[\underline{X}]$ be an ideal and let $f \in K[\underline{X}]$. Is f an element of I?

Solution. Compute a Gröbner basis G of I using Algorithm 3.19. Compute $\overline{f}^{G}$ using Algorithm 3.12. Then $f \in I \iff \overline{f}^{G} = 0$ by Proposition 3.15.

By requiring more structure on a Gröbner basis we obtain even stronger statements.

Definition 3.21. A Gröbner basis is called **reduced** if

(i) Every element $g \in G$ is monic, i.e. $\mathrm{LC}(g) = 1$.

(ii) For all $g \in G$, no term of g lies in $\langle \mathrm{LT}(G \setminus \{g\}) \rangle$.

Algorithm 3.22. Let $I \subset K[\underline{X}]$ be an ideal and G a Gröbner basis of I. Then the following algorithm computes a reduced Gröbner basis G' of I.

Input: G, a Gröbner basis of I
Output: G', a reduced Gröbner basis of I
begin
  $G' := G$
  foreach $g \in G$ **do**
    if $LT(g) \in \langle LT(G \setminus \{g\}) \rangle$ **then**
      $G' := G' \setminus \{g\}$
    else
      $g' := \overline{g}^{G \setminus \{g\}}$ (Algorithm 3.12)
      $G' := (G' \setminus \{g\}) \cup \{\frac{g'}{\mathrm{LC}(g')}\}$
    end
  end
end

Proof. For all $g \in G$ the condition $\mathrm{LT}(g) \in \langle \mathrm{LT}(G \setminus \{g\}) \rangle$ is equivalent to $\mathrm{LT}(g')$ dividing $\mathrm{LT}(g)$ for some $g' \in G \setminus \{g\}$, by Lemma 3.9. This can be checked algorithmically.

Let $G = \{g_1, \ldots, g_m\}$ be the input Gröbner basis of I. Then the algorithm terminates after m steps. We need to show that the output G' is indeed a reduced Gröbner basis of I.

Note that for any $g \in G$ with $\mathrm{LT}(g) \in \langle \mathrm{LT}(G \setminus \{g\})\rangle$ the set $G \setminus \{g\}$ is still a Gröbner basis of I.

Let $1 \leq k \leq m$ with $\mathrm{LT}(g_k) \notin \langle \mathrm{LT}(G \setminus \{g_k\})\rangle$ and define $g' := \overline{g_k}^{G\setminus\{g_k\}}$. Then there exist $h_i \in K[\underline{X}]$ for all $i \neq k$ such that $g_k = \sum_{i\neq k} h_i g_i + g'$ and $\deg(h_i g_i) \preceq \deg(g_k)$ for all $i \neq k$. Since $\mathrm{LT}(g_k) \notin \langle \mathrm{LT}(G \setminus \{g_k\})\rangle$ we find that $\deg(h_i g_i)$ is even strictly smaller than $\deg(g_k)$ for all $i \neq k$ and hence $\mathrm{LT}(g_k) = \mathrm{LT}(g')$. Then $\mathrm{LT}\left((G \setminus \{g_k\}) \cup \{\frac{g'}{\mathrm{LC}(g')}\}\right) = \mathrm{LT}(G)$ and thus $(G \setminus \{g_k\}) \cup \{\frac{g'}{\mathrm{LC}(g')}\}$ is still a Gröbner basis of I.

Hence G' is a Gröbner basis of I at all times in the algorithm. Furthermore, the above argument shows that no term of g lies in $\langle \mathrm{LT}(G' \setminus \{g\})\rangle$ for all $g \in G'$. Also, every element of G' has leading coefficient 1. Hence G' is a reduced Gröbner basis of I. □

Proposition 3.23. *Let $I \subset K[\underline{X}]$ be an ideal. For every monomial ordering, there is a unique reduced Gröbner basis of I.*

Proof. The existence follows from the existence of a Gröbner basis and Algorithm 3.22. Let G and G' be two reduced Gröbner bases of I and let $g \in G$. In particular g is a non-zero element of I. Since G' is a Gröbner basis of I, we have $\mathrm{LT}(g) \in \langle \mathrm{LT}(G')\rangle$. By Lemma 3.9, there exists an element $g' \in G'$ such that $\mathrm{LT}(g')$ divides $\mathrm{LT}(g)$. Using the same argument for g' and G we obtain an element $\tilde{g} \in G$ such that $\mathrm{LT}(\tilde{g})$ divides $\mathrm{LT}(g')$. Hence $\mathrm{LT}(\tilde{g})$ divides $\mathrm{LT}(g)$ and thus $g = \tilde{g}$ since G is a reduced Gröbner basis. We deduce that $\mathrm{LT}(g) = \mathrm{LT}(g')$. We will show that $g = g'$.

Note that $g - g' \in I$ and $\deg(g - g') \prec \deg(g) = \deg(g')$. Assume that $g - g'$ is non-zero. By the same argument as before, there exists an element $f \in G$ such that $\mathrm{LT}(f)$ divides $\mathrm{LT}(g - g')$. Then $\deg(f) \preceq \deg(g - g')$. This implies that $\mathrm{LT}(f)$ divides some term of g or some term of g'. The first case is not possible, because G is reduced and $\deg(f) \prec \deg(g)$, so $f \neq g$. Therefore, $\mathrm{LT}(f)$ divides some term of g'. Repeating once again the above argument, we obtain $f' \in G'$ such that $\mathrm{LT}(f')$ divides $\mathrm{LT}(f)$. Then $\mathrm{LT}(f')$ divides some term of g'. This implies that $f' = g'$ because G' is reduced. But this is impossible since $\deg(f') \preceq \deg(f) \prec \deg(g')$. Therefore the assumption that $g - g'$ is non-zero was false. Hence $G \subset G'$ and analogously $G' \subset G$. □

Task 3.24 (Ideal Equality)**.** Let I, J be two ideals of $K[\underline{X}]$. Do I and J coincide?

Solution. Compute reduced Gröbner bases G and G' of I and J, respectively, by means of Algorithm 3.19 and Algorithm 3.22. Then $I = J \iff G = G'$ by Proposition 3.23.

Task 3.25 (Subideal)**.** Let $I, J \subset K[\underline{X}]$ be two ideals. Is I a subideal of J?

Solution. For every generator f of I check whether $f \in J$ using Task 3.20.

Lemma 3.26. *Let $\underline{X} = \underline{Y} \sqcup \underline{Z}$ and let $I \subset K[\underline{Y}][\underline{Z}]$ be an ideal. Let r denote the cardinality of $\underline{Y}$. Let $\succeq$ be the lexicographical ordering on $K[\underline{Y}][\underline{Z}]$ such that $\deg(Z_{n-r}) \succeq \cdots \succeq \deg(Z_1) \succeq \deg(Y_r) \succeq \cdots \succeq \deg(Y_1)$. Let $G \subset I$ be a Gröbner basis of I with respect to $\succeq$. Then $G \cap K[\underline{Y}]$ is a Gröbner basis of $I \cap K[\underline{Y}]$.*

Proof. Set $G' := G \cap K[\underline{Y}]$. Note that $G' \subset I \cap K[\underline{Y}]$ and G' is finite. Let $f \in I \cap K[\underline{Y}]$ be non-zero. Since G is a Gröbner basis $\mathrm{LT}(f)$ is an element of $\langle \mathrm{LT}(G) \rangle$. By Lemma 3.9, there exists an element $g \in G$ such that $\mathrm{LT}(g)$ divides $\mathrm{LT}(f)$. In particular, this implies that $\mathrm{LT}(g) \in K[\underline{Y}]$. But by our choice of lexicographical ordering this implies that no term of g contains any variable of $\underline{Z}$. Thus $g \in G'$ and $\mathrm{LT}(f) \in \langle \mathrm{LT}(G') \rangle$. Hence G' is a Gröbner basis of $I \cap K[\underline{Y}]$. □

Task 3.27. Let $\underline{X} = \underline{Y} \sqcup \underline{Z}$ and let $I \subset K[\underline{Y}][\underline{Z}]$ be an ideal. Compute a Gröbner basis G of $I \cap K[\underline{Y}]$ with respect to a monomial ordering $\succeq'$.

Solution. Let r denote the cardinality of $\underline{Y}$. Let $\succeq$ be the lexicographical ordering on $K[\underline{Y}][\underline{Z}]$ as in Lemma 3.26. Compute a Gröbner basis $G' \subset I$ of I with respect to $\succeq$ using Algorithm 3.19. Compute $\tilde{G} := G' \cap K[\underline{Y}]$ by ignoring every polynomial of G' with a term containing any variable of $\underline{Z}$. Then $\tilde{G}$ is a Gröbner basis of $I \cap K[\underline{Y}]$, by Lemma 3.26, and thus a generating set of $I \cap K[\underline{Y}]$. Compute a Gröbner basis G of $I \cap K[\underline{Y}]$ with respect to $\succeq'$ using Algorithm 3.19.

Lemma 3.28. *Let $I = \langle f_1, \ldots, f_m \rangle$ and $J = \langle h_1, \ldots, h_\ell \rangle$ be two ideals of $K[\underline{X}]$. Define $L := \langle tf_1, \ldots, tf_m, (1-t)h_1, \ldots, (1-t)h_\ell \rangle \subset K[\underline{X}][t]$. Then $I \cap J = L \cap K[\underline{X}]$.*

Proof. "$\subset$": Let $f \in I \cap J$. Then $tf \in L$ and $(1-t)f \in L$, so $f \in L$. Since $I \subset K[\underline{X}]$ we have $f \in L \cap K[\underline{X}]$.

"$\supset$": For each $c \in K$ consider the homomorphism $\varphi_c : K[\underline{X}][t] \to K[\underline{X}]$, $f(t) \mapsto f(c)$. Let $f \in L \cap K[\underline{X}]$. Then there exist polynomials $a_1, \ldots, a_m, b_1, \ldots, b_\ell \in K[\underline{X}][t]$ such that $f = \sum_{i=1}^{m} a_i t f_i + \sum_{j=1}^{\ell} b_j (1-t) h_j$. Note that $\varphi_0(f) = f = \varphi_1(f)$ since f is independent of t. Then $\varphi_0(f) = \sum_{j=1}^{\ell} b_j h_j \in J$ and similarly $\varphi_1(f) \in I$. Hence $f \in I \cap J$. □

Task 3.29 (Intersection)**.** Let $I_1, \ldots, I_m \subset K[\underline{X}]$ be ideals with given generators. Compute a Gröbner basis of $\bigcap_{i=1}^{m} I_i$.

Solution. By induction we only need to consider the case $m = 2$. Assume that $I_1 = \langle f_1, \ldots, f_k \rangle$ and $I_2 = \langle h_1, \ldots, h_\ell \rangle$. Set $L := \langle tf_1, \ldots, tf_k, (1-t)h_1, \ldots, (1-t)h_\ell \rangle \subset K[\underline{X}][t]$. Compute a Gröbner basis G of $L \cap K[\underline{X}]$ using Task 3.27. Then G is a Gröbner basis of $I_1 \cap I_2$ by Lemma 3.28.

4 Quotients of Ideals

The following section was inspired by the book of Cox, Little and O'Shea [3].

Definition 4.1. Let $I, J \subset K[\underline{X}]$ be two ideals. The **ideal quotient** of I with respect to J is $(I : J) := \{a \in K[\underline{X}] \mid aJ \subset I\}$. For $f \in K[\underline{X}]$ we write $(I : f)$ instead of $(I : \langle f \rangle)$.

Remark 4.2. For two ideals $I, J \subset K[\underline{X}]$ their ideal quotient $(I : J)$ is an ideal of $K[\underline{X}]$.

Lemma 4.3. *Let $I, J \subset K[\underline{X}]$ be two ideals with $J = \langle f_1, \ldots, f_m \rangle$. Then $(I : J) = \bigcap_{i=1}^{m} (I : f_i)$.*

Proof. "$\subset$": Let $g \in (I : J)$. Then $gJ \subset I$, so in particular $gf_i \in I$ for all $1 \leq i \leq m$. Hence $g \in \bigcap_{i=1}^{m} (I : f_i)$.

"$\supset$": Let $g \in \bigcap_{i=1}^{m} (I : f_i)$. Then $gf_i \in I$ for all $1 \leq i \leq m$. Since every $h \in J$ is of the form $h = \sum_{i=1}^{m} \alpha_i f_i$ for polynomials $\alpha_1, \ldots, \alpha_m \in K[\underline{X}]$, we have $gh \in I$ for all $h \in J$. Hence $gJ \subset I$. □

Lemma 4.4. *Let $f \in K[\underline{X}]$ be a non-zero polynomial and let $I \subset K[\underline{X}]$ be an ideal. Let $g_1, \ldots, g_m \in I \cap \langle f \rangle$ be generators of $I \cap \langle f \rangle$. Then $\langle g_1/f, \ldots, g_m/f \rangle = (I : f)$.*

Proof. "$\subset$": First, we note that each g_i is divisible by f since $g_1, \ldots, g_m \in \langle f \rangle$. Hence $g_1/f, \ldots, g_m/f$ are indeed polynomials in $K[\underline{X}]$. Furthermore, for all $1 \leq i \leq m$ we have $(g_i/f) \langle f \rangle = \langle g_i \rangle \subset I$, so $(g_i/f) \in (I : f)$.

"$\supset$": Let $h \in (I : f)$. Then $hf \in I \cap \langle f \rangle$ and we can write $hf = \sum_{i=1}^{m} \alpha_i g_i$ for some $\alpha_1, \ldots, \alpha_m \in K[\underline{X}]$. Dividing by f yields $h = \sum_{i=1}^{m} \alpha_i g_i / f$ and thus $h \in \langle g_1/f, \ldots, g_m/f \rangle$. □

Algorithm 4.5. Let I and J be two ideals of $K[\underline{X}]$. The following algorithm computes a Gröbner basis G of $(I : J)$.

Input: a generating set $(f_1, \ldots, f_m)$ of I and a generating set $(g_1, \ldots, g_r)$ of J not containing zero
Output: G, a generating set of $(I : J)$
begin
  for $1 \leq i \leq r$ **do**
    $H_i :=$ generating set of $I \cap \langle g_i \rangle$ (Task 3.29)
    $G_i := \{g/g_i \mid g \in H_i\}$ (Division Algorithm 3.12)
  end
  $G :=$ Gröbner basis of $\bigcap_{i=1}^{r} \langle G_i \rangle$ (Task 3.29)
end

Proof. The for-loop has r steps, so the algorithm terminates after finitely many steps. By Lemma 4.4, the set G_i is a generating set of $(I : g_i)$ for all $1 \leq i \leq r$. By lemma 4.3, the

intersection $\bigcap_{i=1}^{r} \langle G_i \rangle = \bigcap_{i=1}^{r} (I : g_i)$ is precisely the ideal quotient $(I : J)$. Hence G is a Gröbner basis of $(I : J)$. □

The following task will be useful later.

Task 4.6. Let $I \subset K[\underline{X}]$ be an ideal and $f \in K[\underline{X}]$. Compute an integer s such that $(I : f^s) = \bigcup_{i \geq 1} (I : f^i)$.

Solution. For all $i \leq j$ we have the inclusion $(I : f^i) \subset (I : f^j)$. Furthermore, if $(I : f^k) = (I : f^{k+1})$ for some $k \geq 1$, then $(I : f^{k+1}) = (I : f^{k+2})$. To see this, let $a \in (I : f^{k+2})$. Then $fa \in (I : f^{k+1}) = (I : f^k)$, so $f^{k+1}a \in I$. Hence $a \in (I : f^{k+1})$.

Compute ideals $(I : f), (I : f^2), \ldots$ using Algorithm 4.5 until $(I : f^s) = (I : f^{s+1})$ for some $s \geq 1$. This must occur eventually, since $K[\underline{X}]$ is Noetherian. The argument above then yields $\bigcup_{i \geq 1} (I : f^i) = \bigcup_{i=1}^{s} (I : f^i) = (I : f^s)$.

5 Radicals

The ideas in this section are mainly found in the book of Becker and Weispfenning [2]. Some ideas around Seidenberg's Lemma were inspired by the book of Kreuzer and Robbiano [5].

In all of this section K is a field of characteristic zero.

5.1 Basics

Proposition 5.1. *Let $I = \langle f_1, \dots, f_m \rangle \subset K[\underline{X}]$ be an ideal and let $f \in K[\underline{X}]$. Then $f \in Rad(I)$ if and only if $\langle f_1, \dots, f_m, 1 - Zf \rangle_{K[\underline{X}][Z]} = K[\underline{X}][Z]$.*

Proof. "$\Rightarrow$": Assume that $f \in \mathrm{Rad}(I)$. Then there exists $n > 0$ such that $f^n \in I$. Then $f^{n-1} = Zf^n + (1 - Zf)f^{n-1} \in \langle f_1, \dots, f_m, 1 - Zf \rangle_{K[\underline{X}][Z]}$. Inductively this yields $f^0 = 1 \in \langle f_1, \dots, f_m, 1 - Zf \rangle_{K[\underline{X}][Z]}$.

"$\Leftarrow$": If $f = 0$, then $f \in \mathrm{Rad}(I)$. So assume that f is non-zero. Let $h(Z), h_1(Z), \dots, h_m(Z) \in K[\underline{X}][Z]$ be such that $1 = \sum_{i=1}^m f_i \cdot h_i(Z) + (1 - Zf) \cdot h(Z)$ and set $Z := 1/f$ in the rational function field $K(\underline{X})$. Since $f_1, \dots, f_m$ are independent of Z, we have $1 = \sum_{i=1}^m f_i \cdot h_i(1/f) \in K(\underline{X})$. Let $k := \max\{\deg_Z(h_i) \mid 1 \leq i \leq m\}$. Then $\widetilde{h}_i := f^k \cdot h_i(1/f) \in K[\underline{X}]$ for all $1 \leq i \leq m$ and thus $f^k = \sum_{i=1}^m \widetilde{h}_i f_i \in I$. □

Task 5.2 (Radical Membership)**.** Let $I = \langle f_1, \dots, f_m \rangle \subset K[\underline{X}]$ be an ideal and let $f \in K[\underline{X}]$. Is f an element of $\mathrm{Rad}(I)$?

Solution. Compute a Gröbner basis of $L := \langle f_1, \dots, f_m, 1 - Zf \rangle_{K[\underline{X}][Z]} \subset K[\underline{X}][Z]$ using Algorithm 3.19. Then check if $1 \in L$ with Task 3.20. By Proposition 5.1, we have $f \in \mathrm{Rad}(I) \iff 1 \in L$.

We will see that the key to computing the radical of an ideal is the square-free part of a polynomial:

Definition 5.3. Let $f \in K[Z]$ be a non-zero univariate polynomial. Let $f = a \prod_{i=1}^{\ell} g_i^{r_i}$ be the unique factorization of f into monic pairwise non-equivalent irreducible polynomials $g_1, \dots, g_\ell \in K[Z]$ and $a \in K^\times$. The **square-free part** of f is defined as $\prod_{i=1}^{\ell} g_i$.

A polynomial $f \in K[Z]$ is said to be **square-free** if it is non-zero and equal to its square-free part.

Lemma 5.4. *Let $f \in K[Z]$ be non-constant. Let f' denote the formal derivative of f. Then f is square-free if and only if $\gcd(f, f') = 1$.*

Proof. "$\Leftarrow$": Assume that $\gcd(f, f') = 1$ and that f is not square-free. Then $f = f_1^2 f_2$ for some $f_1, f_2 \in K[Z]$, where $f_1 \notin K$. Then $f' = 2f_1 f_1' f_2 + f_1^2 f_2'$, so $f_1 | \gcd(f, f')$. This is a contradiction to $\gcd(f, f') = 1$.

"$\Rightarrow$": Assume that $\gcd(f, f') \neq 1$ and let $h \in K[Z]$ be an irreducible divisor of $\gcd(f, f')$. Then there exists a polynomial $a \in K[Z]$ such that $ah = f$ and thus $a'h + ah' = f'$. Since h

divides f' it follows that h must divide ah'. Note that h does not divide h' since $\mathrm{char}(K) = 0$ and h is irreducible, so $\deg(h') = \deg(h) - 1 \geq 0$. This implies that h divides a. Hence h^2 divides f and f is not square-free. □

Claim 5.5. *Let $f \in K[Z]$ be non-constant and monic. Then $g := \frac{f}{\gcd(f,f')}$ is the square-free part of f.*

Proof. Note that since f is not constant, it is non-zero. Hence $\gcd(f, f') \neq 0$ and g is thus well-defined. First we will show that g is square-free. Due to Lemma 5.4 we only need to show that $\gcd(g, g') = 1$. We know that $f = g \gcd(f, f')$ and thus $\gcd(g, f') = 1$. Hence $f' = g' \gcd(f, f') + g(\gcd(f, f'))'$ implies that $\gcd(g, g') = 1$.

Let $p \in K[Z]$ be an irreducible divisor of f. Then $f = bp^\ell$ for some $b \in K[Z]$ with $\gcd(b, p) = 1$ and some $\ell > 0$. We thus have $f' = b'p^\ell + \ell bp^{\ell-1}p'$. Since p is irreducible, it follows that p^ℓ does not divide $\gcd(f, f')$. We deduce that $\gcd(f, f')$ divides $bp^{\ell-1}$. Hence p divides g. This shows that the square-free part of f divides g. Furthermore g is square-free by the above. Since f and g are both monic, the square-free part of f must be equal to g. □

Task 5.6. Let $f \in K[Z]$ be non-zero. Compute the square-free part of f.

Solution. If $f \in K$, then the square-free part of f is 1. So assume that f is not constant. Then $\gcd(f, f')$ is non-zero. Define $g := \frac{f}{\mathrm{LC}(f)\gcd(f,f')}$. The square-free part of f and $\frac{f}{\mathrm{LC}(f)}$ are equal. Thus, it follows by Claim 5.5 that g is the square-free part of f.

5.2 Ideals of finite codimension

In order to compute the radical of an arbitrary ideal we start with a special case.

Proposition 5.7. *An ideal $I \subset K[\underline{X}]$ has finite codimension (as a vector space over K) if and only if $I \cap K[X_i] \neq \{0\}$ for all $1 \leq i \leq n$.*

Proof. "⇐": For each $1 \leq i \leq n$ choose non-zero polynomials $f_i \in I \cap K[X_i]$. Let $d := \max\{\deg(f_i) \mid 1 \leq i \leq n\}$. Then $K[\underline{X}] = K[\underline{X}]^{\deg \leq (d,\ldots,d)} + I$ by the division algorithm. The vector space $K[\underline{X}]^{\deg \leq (d,\ldots,d)}$ is finite dimensional. Hence I has finite codimension.

"⇒": Assume that $n := \dim_K(K[\underline{X}]/I) < \infty$. Let $1 \leq i \leq n$. The elements $(X_i^j)_{j=1}^{n+1}$ are linearly dependent in this quotient space. This yields a non-trivial K-linear combination of $(X_i^j)_{j=1}^{n+1}$, i.e. a non-zero polynomial $f \in K[X_i]$, which maps to zero in the quotient space. Thus f is a non-zero element of $I \cap K[X_i]$. □

Lemma 5.8. *Let $I \subset K[\underline{X}]$ be an ideal such that there is a non-constant square-free $g \in I \cap K[X_1]$. Let $g = \prod_{i=1}^m h_i$ be the factorization into pairwise non-equivalent irreducible $h_1, \ldots, h_m \in K[X_1]$. Then $I = \bigcap_{i=1}^m (I + \langle h_i \rangle)$.*

Proof. Clearly $I \subset \bigcap_{i=1}^m (I + \langle h_i \rangle)$. For the other inclusion, let $f \in \bigcap_{i=1}^m (I + \langle h_i \rangle)$. There exist $r_1, \ldots, r_m \in I$ and $q_1, \ldots, q_m \in K[\underline{X}]$ such that $f = r_i + q_i h_i$ for all $1 \leq i \leq m$. It follows that $f \prod_{j \neq i} h_i \in I$ for all $1 \leq i \leq m$, because $g = \prod_{i=1}^m h_i \in I$. Note that

$\gcd(\prod_{j\neq 1} h_j, \ldots, \prod_{j\neq m} h_j) = 1$ and $K[X_1]$ is a principal ideal domain. Therefore, there exist $p_1, \ldots, p_m \in K[X_1]$ such that $\sum_{i=1}^m p_i \prod_{j\neq i} h_j = 1$. Together this yields $f = \sum_{i=1}^m p_i f \prod_{j\neq i} h_j \in I$. Hence $I \supset \bigcap_{i=1}^m (I + \langle h_i \rangle)$. □

Lemma 5.9 (Seidenberg)**.** *Let $I \subset K[\underline{X}]$ be an ideal of finite codimension. Then I is a radical ideal if and only if for each $1 \leq i \leq n$ there is a non-constant square-free $g_i \in I \cap K[X_i]$.*

Proof. "⇒" Let $1 \leq i \leq n$ and let $f \in I \cap K[X_i]$ be a monic non-constant polynomial. Let $f = \prod_{j=1}^{\ell} h_j^{\alpha_j}$ be the unique factorization of f into pairwise non-equivalent monic irreducible polynomials $h_1, \ldots, h_\ell \in K[X_i]$. Set $\alpha := \max\{\alpha_j \mid 1 \leq j \leq \ell\}$. Then $\prod_{j=1}^{\ell} h_j^{\alpha} \in I \cap K[X_i]$. With I being radical it follows that $g_i := \prod_{j=1}^{\ell} h_j \in I \cap K[X_i]$, which is square-free.

"⇐" For the converse we proceed by induction on the number of variables n for arbitrary fields K. For $n = 1$ the ideal I is a principal ideal, so there is a generator $h \in I$. Then there is some $a \in K[X_1]$ such that $g_1 = ah$. Since g_1 is square-free h must also be square-free, by uniqueness of factorization. Now for every $f \in K[\underline{X}]$ with $f^k \in I$ we know that h divides f^k. Since h is square-free this implies that h divides f. Hence $f \in I$ and I is a radical ideal.

Now let $n > 1$. Since g_1 is square-free, there are pairwise non-equivalent irreducible polynomials $h_1, \ldots, h_m \in K[X_1]$ such that $g_1 = \prod_{i=1}^m h_i$. Let $1 \leq k \leq m$. We claim that the ideal $J := I + \langle h_k \rangle$ is radical. Since h_k is irreducible $L := K[X_1]/\langle h_k \rangle$ is a finite field extension of K. Let $\varphi : K[\underline{X}] \to L[X_2, \ldots, X_n]$ be the canonical homomorphism. We know that φ is surjective and that $\ker \varphi = \langle h_k \rangle \subset J$. Hence $L[X_2, \ldots, X_n]/(J^e) \cong K[\underline{X}]/J$ where J^e is the extension of J with respect to φ. Thus J^e is again of finite codimension. Furthermore $\varphi(g_i) \in J^e \cap L[X_i]$ for all $2 \leq i \leq n$. Each g_i is square-free, thus $\gcd(g_i, g_i') = 1$ by Lemma 5.4. This is still true for the image in $L[X_2, \ldots, X_n]$, so again by Lemma 5.4, the g_i are all square-free in $L[X_i]$. By induction hypothesis, it follows that J^e is radical. This implies that $L[X_2, \ldots, X_n]/(J^e) \cong K[\underline{X}]/J$ has no nilpotent elements. Therefore, the ideal $J = I + \langle h_k \rangle$ is radical. Since k was arbitrary, the statement holds for all $1 \leq k \leq m$.

Lemma 5.8 yields a decomposition $I = \bigcap_{i=1}^m (I + \langle h_i \rangle)$. Taking the radical of an ideal commutes with intersections, so $\operatorname{Rad}(I) = \bigcap_{i=1}^m \operatorname{Rad}(I + \langle h_i \rangle) = \bigcap_{i=1}^m (I + \langle h_i \rangle) = I$. Hence I is a radical ideal. □

Seidenberg's Lemma provides a nice method to compute the radical of an ideal of finite codimension:

Algorithm 5.10. Let $I \subset K[\underline{X}]$ be an ideal of finite codimension. Then the following algorithm computes a generating set G of $\mathrm{Rad}(I)$.

Input: $(f_1, \ldots, f_m)$, a generating set of I
Output: G, a finite generating set of $\mathrm{Rad}(I)$
begin
  $G := \{f_1, \ldots, f_m\}$
  for $1 \leq i \leq n$ **do**
    $\widetilde{G}_i :=$ reduced Gröbner basis of $I \cap K[X_i]$ (Task 3.27, Algorithm 3.22)
    $h_i :=$ the only element of $\widetilde{G}_i$
    $g_i :=$ square-free part of h_i (Task 5.6)
  end
  $G := \{f_1, \ldots, f_m, g_1, \ldots, g_n\}$
end

Proof. Note that the algorithm terminates after n steps.

Let $1 \leq i \leq n$. Since $K[X_i]$ is a principal ideal domain there is monic polynomial $h \in K[X_i]$ generating $I \cap K[X_i]$. Furthermore h is non-zero by Proposition 5.7. Then $\{h\}$ is a reduced Gröbner basis of $I \cap K[X_i]$. Proposition 3.23 implies that this is necessarily the one computed by the algorithm. Thus the Gröbner basis contains only one element, so h_i in the algorithm is well-defined.

We have $f_1, \ldots, f_m \in \mathrm{Rad}(I)$. Let $1 \leq i \leq m$ and let $h_i = a \prod_{i=1}^{\ell} p_i^{r_i}$ be the unique factorization of h_i into monic pairwise non-equivalent irreducible polynomials $p_1, \ldots, p_\ell \in K[\underline{X}]$. By definition, the square-free part of h_i is $g_i = \prod_{i=1}^{\ell} p_i$. For $r := \max\{r_i \mid 1 \leq i \leq \ell\}$ we have that h_i divides $g_i^r = \prod_{i=1}^{\ell} p_i^r$, so $g_i^r \in I$. Hence $g_i \in \mathrm{Rad}(I)$. This shows that $G \subset \mathrm{Rad}(I)$ at all times in the algorithm.

Now assume that the algorithm has terminated. If $I = \langle 1 \rangle$, then $\mathrm{Rad}(I) = I = \langle G \rangle$. If not, then by construction of the algorithm, the ideal $J := \langle G \rangle$ has the property that for all $1 \leq i \leq n$ we have $g_i \in J \cap K[X_i]$ and g_i is square-free and non-constant. In particular J is of finite codimension and we can apply Lemma 5.9. It follows that J is radical. Since $I \subset J \subset \mathrm{Rad}(I)$ we conclude that $J = \mathrm{Rad}(I)$. □

Remark 5.11. Algorithm 5.10 also works for perfect fields of positive characteristic, provided there is an algorithm to compute the square-free part of any polynomial in $K[Z]$. However, for non-perfect fields the algorithm might fail. To see this, let $p > 0$ be a prime number. Consider the ideal $I := \langle X^p - t, Y^p - t \rangle \subset \mathbb{F}_p(t)[X, Y]$. Algorithm 5.10 would give us $G = \{X^p - t, Y^p - t\}$ as Gröbner basis for $\mathrm{Rad}(I)$, because both elements are square-free. Note that $(X - Y)^p = X^p - Y^p \in I$ and thus $X - Y \in \mathrm{Rad}(I)$. But $\mathrm{LT}(X - Y)$ is not an element of $\langle \mathrm{LT}(G) \rangle = \langle X^p, Y^p \rangle$. Hence G is not a Gröbner basis of $\mathrm{Rad}(I)$.

5.3 The general case

Having solved the problem for ideals of finite codimension, we are closer to our goal of computing radicals. However, more theory is needed in order to write an algorithm for the general case.

Lemma 5.12. *Let $H \subset K[\underline{X}]$ be a subset and $f \in K[\underline{X}]$ be a non-zero polynomial. Then*

$$\langle H \cup \{1 - Zf\}\rangle_{K[\underline{X}][Z]} \cap K[\underline{X}] = \bigcup_{i\geq 0}(\langle H\rangle : f^i)$$

Proof. "$\subset$": Let $g \in \langle H \cup \{1 - Zf\}\rangle_{K[\underline{X}][Z]} \cap K[\underline{X}]$. There exist $\alpha_1(Z), \ldots, \alpha_\ell(Z), \beta(Z) \in K[\underline{X}][Z]$ and $h_1, \ldots, h_\ell \in H$ such that $g(Z) = \sum_{i=1}^{\ell} h_i \cdot \alpha_i(Z) + (1 - Zf) \cdot \beta(Z)$. Set $Z := 1/f$ in the field of fractions $K(\underline{X})$. Since $g, h_1, \ldots, h_\ell$ are polynomials, we have $g = g(1/f) = \sum_{i=1}^{\ell} h_i \cdot \alpha_i(1/f)$. Then there exists a $k > 0$ such that $f^k \cdot \alpha_i(1/f)$ is a polynomial for all $1 \leq i \leq \ell$. Hence $gf^k \in \langle H\rangle$, so $g \in (\langle H\rangle : f^k)$.

"$\supset$": Let $g \in \bigcup_{i\geq 0}(\langle H\rangle : f^i)$. Let $k > 0$ such that $gf^k \in \langle H\rangle$. Then $gf^{k-1} = Zgf^k + gf^{k-1}(1 - Zf) \in \langle H \cup \{1 - Zf\}\rangle_{K[\underline{X}][Z]}$. Inductively, we obtain $g \in \langle H \cup \{1 - Zf\}\rangle_{K[\underline{X}][Z]}$. Since g is a polynomial, we have $g \in \langle H \cup \{1 - Zf\}\rangle_{K[\underline{X}][Z]} \cap K[\underline{X}]$. □

Algorithm 5.13. Let $\underline{X} = \underline{Y} \sqcup \underline{Z}$ and let $F \subset K(\underline{Y})[\underline{Z}]$ be a finite subset. Then the following algorithm computes a Gröbner basis of the contraction ideal $\langle F\rangle^c \subset K[\underline{X}]$.

Input: $F \subset K(\underline{Y})[\underline{Z}]$, a finite subset
Output: G, a Gröbner basis of $\langle F\rangle^c$
begin
  $H :=$ Gröbner basis of $\langle F\rangle \subset K(\underline{Y})[\underline{Z}]$ (Algorithm 3.19)
  foreach $h \in H$ **do**
    $q :=$ multiple of all denominators of coefficients in $K(\underline{Y})$ of h
    $h := qh \in K[\underline{X}]$
  end
  $f := \operatorname{lcm}\{\mathrm{LC}_{\underline{Z}}(h) \mid h \in H\}$
  $G :=$ Gröbner basis of $\langle H \cup \{1 - Uf\}\rangle_{K[\underline{X}][U]} \cap K[\underline{X}]$ (Task 3.27)
end

Proof. The algorithm terminates after finitely many steps. Assume that the algorithm has terminated. During the algorithm, the set H is only changed by multiplying its elements with some units of $K(\underline{Y})$. Therefore, at the end H is still a Gröbner basis of $\langle F\rangle \subset K(\underline{Y})[\underline{Z}]$. Let $J := \bigcup_{i\geq 0}(\langle H\rangle_{K[\underline{X}]} : f^i)$. We will show that $J = \langle F\rangle^c$.

Let $g \in J$. Then there exists a $k > 0$ such that $gf^k \in \langle H\rangle_{K[\underline{X}]} \subset \langle F\rangle^c$. But f is a unit in $K(\underline{Y})[\underline{Z}]$ since $f \in K[\underline{Y}] \setminus \{0\}$. Thus $g = gf^k f^{-k} \in \langle F\rangle$ and hence $g \in \langle F\rangle^c$. This implies that $J \subset \langle F\rangle^c$.

We will show that $p \in J$ for all $p \in \langle F\rangle^c$ by transfinite induction on $\deg_{\underline{Z}}(p)$. Since H is

a Gröbner basis of $\langle F\rangle$, there is an element $h \in H$ such that $\mathrm{LT}_{\underline{Z}}(h)$ divides $\mathrm{LT}_{\underline{Z}}(p)$. This implies that there exists a monomial $\alpha \in K[\underline{Z}]$ and an element $s \in K(\underline{Y})$ such that $\mathrm{LT}_{\underline{Z}}(p) = s\alpha\mathrm{LT}_{\underline{Z}}(h)$. The left hand side $\mathrm{LT}_{\underline{Z}}(p)$ lies in $K[\underline{X}]$ and so must the right hand side. Therefore $s\mathrm{LC}_{\underline{Z}}(h) \in K[\underline{Y}]$. Since f is the lcm of all leading coefficients of elements in H, in particular $sf \in K[\underline{Y}]$. Define $p' := pf - s\alpha hf \in K[\underline{X}]$. Then $p' \in \langle F\rangle^c$. Furthermore, by construction $\deg_{\underline{Z}}(p') \prec \deg_{\underline{Z}}(p)$, since f is a unit in $K(\underline{Y})[\underline{Z}]$. If $\deg_{\underline{Z}}(p)$ is minimal (as for the base case) then $p' = 0 \in J$. Otherwise, by induction hypothesis, we deduce that $p' \in J$. Either way there exists a $k > 0$ such that $p'f^k \in \langle H\rangle_{K[\underline{X}]}$. Thus $pf^{k+1} = p'f^k + s\alpha hf^{k+1} \in \langle H\rangle_{K[\underline{X}]}$, so $p \in J$. Hence $J = \langle F\rangle^c$.

It follows by Lemma 5.12 that $J = \langle H \cup \{1 - Uf\}\rangle_{K[\underline{X}][U]} \cap K[\underline{X}]$. Hence G is a Gröbner basis of $\langle F\rangle^c$. □

Definition 5.14. Let $\underline{X} = \underline{Y} \sqcup \underline{Z}$. Let $\succeq_Y$ be a monomial ordering on $K[\underline{Y}]$ and $\succeq_Z$ a monomial ordering on $K[\underline{Z}]$. The **block ordering** $\succeq$ on $K[\underline{X}]$ with respect to $\underline{Z}$ is the monomial ordering defined as follows: for monomials $a, c \in K[\underline{Y}]$ and $b, d \in K[\underline{Z}]$ let $ab \succeq cd$ if and only if $b \succeq_Z d$ or ($b = d$ and $a \succeq_Y c$).

Lemma 5.15. *Let $\underline{X} = \underline{Y} \sqcup \underline{Z}$ and consider a block ordering on $K[\underline{X}]$ with respect to $\underline{Z}$. Let $g, h \in K[\underline{X}]$ such that $LT_{\underline{X}}(g)$ divides $LT_{\underline{X}}(h)$. Then $LT_{\underline{Z}}(g)$ divides $LT_{\underline{Z}}(h)$ in $K(\underline{Y})[\underline{Z}]$.*

Proof. Since $\mathrm{LT}_{\underline{X}}(g)$ and $\mathrm{LT}_{\underline{X}}(h)$ are monomials, there are monomials $p, q \in K[\underline{Y}]$ and $m, m' \in K[\underline{Z}]$ such that $\mathrm{LT}_{\underline{X}}(g) = pm$ and $\mathrm{LT}_{\underline{X}}(h) = qm'$. Since $\mathrm{LT}_{\underline{X}}(g)$ divides $\mathrm{LT}_{\underline{X}}(h)$, it follows that m divides m'. Looking at the definition of a block ordering we see that there must be polynomials $a, b \in K[\underline{Y}]$ such that $\mathrm{LT}_{\underline{Z}}(g) = am$ and $\mathrm{LT}_{\underline{Z}}(h) = bm'$. Since a and b are units in $K(\underline{Y})[\underline{Z}]$ we conclude that $\mathrm{LT}_{\underline{Z}}(g)$ divides $\mathrm{LT}_{\underline{Z}}(h)$. □

Algorithm 5.16. Let $I \subset K[\underline{X}]$ be an ideal and let $\underline{X} = \underline{Y} \sqcup \underline{Z}$. Consider extensions of ideals to $K(\underline{Y})[\underline{Z}]$. Then the following algorithm computes a non-zero polynomial $f \in K[\underline{Y}]$ such that $I = (I + \langle f\rangle) \cap I^{ec}$.

Input: $f_1, \ldots, f_m \in I$, generators of I
Output: $f \in K[\underline{Y}]$ with $I = (I + \langle f\rangle) \cap I^{ec}$
begin
  $\succeq$:= some block ordering on $K[\underline{X}]$ with respect to $\underline{Z}$
  $\succeq'$:= restriction of $\succeq$ to $K[\underline{Z}]$
  H := Gröbner basis of I with respect to $\succeq$ (Algorithm 3.19)
  $g := \mathrm{lcm}\{\mathrm{LC}_{\underline{Z}}(h) \mid h \in H\}$, where $\mathrm{LC}_{\underline{Z}}$ is with respect to $\succeq'$
  s := an integer such that $(I : g^s) = \bigcup_{i \geq 1}(I : g^i)$ (Task 4.6)
  $f := g^s$
end

Proof. Clearly the algorithm terminates and we therefore will only have to prove correctness. Let f be the output of the algorithm and g, s as in the algorithm such that $f = g^s$. We will prove that $H \subset K[\underline{X}]$ is not only a Gröbner basis of I but $H \subset K(\underline{Y})[\underline{Z}]$ is also a Gröbner

basis of I^e. Let $p \in I^e$. Then there exist $a_1, \ldots, a_m \in K(\underline{Y})[\underline{Z}]$ and $g_1, \ldots, g_m \in I$ such that $p = \sum_{i=1}^m a_i g_i$. Let $r \in K[\underline{Y}]$ be the least common multiple of all denominators of $(a_i)_{i=1}^m$. Then $rp = \sum_{i=1}^m r a_i g_i \in I$. Since H is a Gröbner basis of I, there is an element $h \in H$ such that $\mathrm{LT}_{\underline{X}}(h)$ divides $\mathrm{LT}_{\underline{X}}(rp)$. Hence $\mathrm{LT}_{\underline{Z}}(h)$ divides $\mathrm{LT}_{\underline{Z}}(rp)$ by Lemma 5.15. Since r is a unit in $K(\underline{Y})[\underline{Z}]$ it follows that $\mathrm{LT}_{\underline{Z}}(h)$ divides $\mathrm{LT}_{\underline{Z}}(p)$. Thus $H \subset K(\underline{Y})[\underline{Z}]$ is a Gröbner basis of I^e.

We will next prove that $I^{ec} = (I : f)$. We show that $p \in (I : f)$ for all $p \in I^{ec}$ by transfinite induction on the degree $\deg_{\underline{Z}}(p)$. Since H is a Gröbner basis of I^e, there is an element $h \in H$ such that $\mathrm{LT}_{\underline{Z}}(h)$ divides $\mathrm{LT}_{\underline{Z}}(p)$ in $K(\underline{Y})[\underline{Z}]$. Thus there exists $\alpha \in K(\underline{Y})[\underline{Z}]$ such that $\mathrm{LT}_{\underline{Z}}(p) = \alpha \mathrm{LT}_{\underline{Z}}(h)$. Since $\mathrm{LT}_{\underline{Z}}(p)$ is a polynomial in $K[\underline{X}]$ the denominator in $K[\underline{Y}]$ of α has to divide $\mathrm{LC}_{\underline{Z}}(h)$ and thus has to divide g. Hence $\alpha g \in K[\underline{X}]$ and $gp - g\alpha h \in I^{ec}$. Furthermore $\deg_{\underline{Z}}(gp - g\alpha h) \prec \deg_{\underline{Z}}(p)$. If $\deg_{\underline{Z}}(p)$ is minimal (as in the base case) then $gp - g\alpha h = 0 \in (I : g^s)$. Otherwise, the induction hypothesis implies that $gp - g\alpha h \in (I : g^s)$. So either way $g^s(gp - g\alpha h) = g^{s+1}p - g^{s+1}\alpha h \in I$. Hence $g^{s+1}p \in I$. This implies that $p \in \bigcup_{i \geq 1}(I : g^i) = (I : g^s) = (I : f)$. Thus $I^{ec} \subset (I : f)$.

For the other inclusion, let $p \in (I : f)$. Then $fp \in I$. Since f is a non-zero polynomial in $K[\underline{Y}]$, it is a unit in $K(\underline{Y})[\underline{Z}]$. It follows that $p = pff^{-1} \in I^e$, so $p \in I^{ec}$. Hence $I^{ec} = (I : f)$.

We now only need to prove that $I = (I + \langle f \rangle) \cap (I : f)$. The inclusion $\subset$ is clearly true. Let $p \in (I + \langle f \rangle) \cap (I : f)$. Then there exists $h \in I$ and $\alpha \in K[\underline{X}]$ such that $p = h + \alpha f$. Furthermore $fp = fh + f^2\alpha \in I$ and thus $f^2\alpha \in I$. Since $(I : f^2) = (I : g^{2s}) \subset \bigcap_{i=1}^{\infty}(I : g^i) = (I : g^s) = (I : f)$ we have $f\alpha \in I$. Hence $p \in I$. This concludes the proof. □

Claim 5.17. *Let $I \subset K[\underline{X}]$ be an ideal. Let $\underline{Y} \subset \underline{X}$ be a maximal set of variables whose image in $K[\underline{X}]/I$ is algebraically independent. Let $\underline{Z} := \underline{X} \setminus \underline{Y}$. Then the extension ideal $I^e \subset K(\underline{Y})[\underline{Z}]$ is of finite codimension.*

Proof. Let ℓ denote the cardinality of $\underline{Z}$. By choice of $\underline{Y}$, for each $1 \leq i \leq \ell$ there exists a non-zero polynomial $f \in K[\underline{Y}][Z_i]$ such that $f \in I$. Then $f \in I^e \cap K(\underline{Y})[Z_i]$ for all $1 \leq i \leq \ell$. It follows the claim by Proposition 5.7. □

Finally we are able to formulate an algorithm to compute the radical of an ideal:

Algorithm 5.18. Let $I \subset K[\underline{X}]$ be an ideal. Then the following algorithm computes a finite generating set of $\mathrm{Rad}(I)$.

Input: $f_1, \ldots, f_m \in I$, generators of I
Output: $G \subset \mathrm{Rad}(I)$, finite generating set of $\mathrm{Rad}(I)$
begin
  $G := \{1\}$
  if $1 \notin I$ **then**
    $\underline{Y} \subset \underline{X}$ maximal algebraically independent variables mod I
    $\underline{Z} := \underline{X} \setminus \underline{Y}$
    $F :=$ generating set of $\mathrm{Rad}(I^e) \subset K(\underline{Y})[\underline{Z}]$ (Algorithm 5.10)
    $J :=$ generating set of $\langle F \rangle^c \subset K[\underline{X}]$ (Algorithm 5.13)
    $f :=$ an element in $K[\underline{Y}]$ such that $I = (I + \langle f \rangle) \cap I^{ec}$ (Algorithm 5.16)
    $G' :=$ generating set of $\mathrm{Rad}(\langle f_1, \ldots, f_m, f \rangle)$ (recursively)
    $G :=$ Gröbner basis of $\langle G' \rangle \cap \langle J \rangle$ (Algorithm 3.19)
  end
end

Proof. We first prove that the algorithm terminates. We do not have any loops in the algorithm, but there is a recursion. For any $i \geq 1$ denote f_{i+m} for the f in the algorithm constructed in the ith recursion. Let $I_1 := I$. Then $I_{i+1} = I_i + \langle f_{i+m} \rangle$ is the input of the $(i+1)$th recursion step for all $i \geq 1$. Let $\underline{Y}_i$ be the maximal algebraically independent variables mod I in the ith recursion step. Then we have $f_{i+m} \in K[\,\underline{Y}_i\,]$. Thus $\underline{Y}_i$ being algebraically independent implies that $f_{i+m} \notin I_i$. Therefore, we have a strictly ascending chain $I_{m+1} \subset I_{m+2} \subset \ldots$ of ideals. But we know that $K[\underline{X}]$ is Noetherian. Hence there exists a $k \geq 1$ such that $I_k = K[\underline{X}]$. Then in the kth recursion step we have $1 \in I_k$ and thus the step terminates. This implies that the algorithm terminates.

We now show correctness. The algorithm works if $1 \in I$. So by induction we can assume that $\langle G' \rangle = \mathrm{Rad}(I + \langle f \rangle)$. Let G be the output of the algorithm. We have $\mathrm{Rad}(I^{ec}) = \mathrm{Rad}(I^e)^c = \langle F \rangle^c = \langle J \rangle$. By construction of f it follows that $\mathrm{Rad}(I) = \mathrm{Rad}((I + \langle f \rangle) \cap I^{ec}) = \mathrm{Rad}(I + \langle f \rangle) \cap \mathrm{Rad}(I^{ec}) = \langle G' \rangle \cap \langle J \rangle = \langle G \rangle$. Hence the algorithm is correct. □

Remark 5.19. In general, Algorithm 5.18 does not work for fields K of strictly positive characteristic. The requirement that we need for the algorithm would be that every rational function field over K is perfect. This restriction comes from the fact that we use Algorithm 5.10 in such a rational function field. This requirement, however, is equivalent to $\mathrm{char}(K) = 0$.

As of late we do not have to give up on fields of characteristic non-zero. In 2001 Ryutaroh Matsumoto published an algorithm to compute radicals in the polynomial ring over a finite field extension of a perfect field of positive characteristic (see [7]). It uses a - very interesting - totally different approach that does not need computations for ideals of finite codimension.

6 Primary Decomposition

The ideas contained in this section are mainly taken from the book of Becker and Weispfenning [2].

Let K be a field of characteristic zero. Furthermore, assume that we know an algorithm to compute a factorization of any polynomial $f \in K[Z]$ into irreducible polynomials.

6.1 Ideals of finite codimension

Lemma 6.1. *Let $I \subset K[\underline{X}]$ be a radical ideal and let $c_1, \ldots, c_n \in K$. Define $J := \langle I, Z - \sum_{i=1}^{n} c_i X_i \rangle \subset K[\underline{X}][Z]$. Then*

(i) We have $J \cap K[\underline{X}] = I$.

(ii) The ideal J is radical.

(iii) If I is of finite codimension, then so is J.

Proof. Define $g := Z - \sum_{i=1}^{n} c_i X_i$.

(i) The inclusion $I \subset J \cap K[\underline{X}]$ is given by definition of J. For the other inclusion, let $f \in J \cap K[\underline{X}]$. Then there exist $h_1(Z), h_2(Z) \in K[\underline{X}][Z]$ and $p \in I$ such that $f = p \cdot h_1(Z) + g \cdot h_2(Z)$. Set $Z = \sum_{i=1}^{n} c_i X_i$. Then $f = f(\sum_{i=1}^{n} c_i X_i) = p \cdot h_1(\sum_{i=1}^{n} c_i X_i) \in I$, since f is a polynomial in $K[\underline{X}]$. Hence $J \cap K[\underline{X}] \subset I$.

(ii) Let $f(Z) \in \mathrm{Rad}(J)$. Then there exists an $m > 0$ such that $f^m \in J$. Define $h := f(\sum_{i=1}^{n} c_i X_i) \in K[\underline{X}]$. Then $h \equiv f \mod \langle g \rangle$ and thus $h^m \equiv f^m \mod \langle g \rangle$. Hence $h^m \in (f^m + \langle g \rangle) \cap K[\underline{X}] \subset J \cap K[\underline{X}] = I$ by (i). Since I is radical h is an element of I. Hence $f \in (h + \langle g \rangle) \subset J$. Therefore $\mathrm{Rad}(J) = J$.

(iii) Let $f(Z) \in K[\underline{X}][Z]$. Then $f(Z) \equiv f(\sum_{j=1}^{n} c_i X_i) \mod J$ and thus the homomorphism $\varphi : K[\underline{X}] \to K[\underline{X}][Z]/J$ is surjective. It follows by (i) that $\ker(\varphi) = J \cap K[\underline{X}] = I$. Hence $K[\underline{X}]/I \cong K[\underline{X}][Z]/J$ and in particular J is of finite codimension, provided that I is of finite codimension. □

Claim 6.2. *Let $I \subset K[\underline{X}]$ be an ideal and $G \subset I$ be a Gröbner basis of I. Let M be the set of all monomials in $K[\underline{X}]$ which are not divisible by any element of $LM(G)$. Then the set M maps bijectively to a basis of the K-vector space $K[\underline{X}]/I$.*

Proof. First, we prove that the image of M generates $K[\underline{X}]/I$ as K-vector space. Let $f \in K[\underline{X}]/I$. Then $f - \overline{f}^G \in I$ by definition of a remainder on division. Thus $f \equiv \overline{f}^G \mod I$. No term of $\overline{f}^G$ is divisible by any element of $\mathrm{LT}(G)$. So, in particular, no term of $\overline{f}^G$ is divisible by any element of $\mathrm{LM}(G)$. Hence $\overline{f}^G$ is a K-linear combination of monomials in M.

On the other hand, the elements of M are linearly independent. To see this let $f \in K[\underline{X}]$ be a linear combination of finitely many elements of M such that $f \equiv 0 \mod I$. This implies that $f \in I$ and no term of f is divisible by any element of $\mathrm{LT}(G)$. It follows by Lemma 3.9 that

$f = 0 \in K[\underline{X}]$. Hence the elements of M are linearly independent. A linearly independent generating set of a vector space is a basis. This concludes the proof. □

Proposition 6.3. *Let $I \subset K[\underline{X}]$ be a radical ideal of finite codimension. Denote by m the number of zeroes of I in $\overline{K}^n$. Then $\dim_K(K[\underline{X}]/I) = m$.*

Proof. Let $G \subset I$ be a Gröbner basis of I. We will work in the ring $\overline{K}[\underline{X}]$. For all $g_1, g_2 \in G$ the S-polynomial $S(g_1, g_2)$ in $\overline{K}[\underline{X}]$ is the same as in $K[\underline{X}]$. Also, a remainder on division with respect to G in $K[\underline{X}]$ is also a remainder on division with respect to G in $\overline{K}[\underline{X}]$. It follows by Theorem 3.18 that G is a Gröbner basis of $J := \langle G \rangle$. The number of zeroes of an ideal only depend on its generating set and thus m is also the number of zeroes of J. Furthermore, the set of monomials in $K[\underline{X}]$ is independent of the field K. Hence $\dim_K(K[\underline{X}]/I) = \dim_{\overline{K}}(\overline{K}[\underline{X}]/J)$ by Claim 6.2. In particular J is of finite codimension. We need to show that $\dim_{\overline{K}}(\overline{K}[\underline{X}]/J) = m$.

The image in $\overline{K}[\underline{X}]$ of a square-free polynomial $f \in K[\underline{X}]$ is square-free by Lemma 5.4 and the fact that the gcd is invariant under the extension. It follows by Lemma 5.9 and the fact that I is radical, that J is also a radical ideal. Let $(a_1^i, \ldots, a_n^i) \in \overline{K}^n$ for $1 \leq i \leq m$ be the zeroes of J. For each $1 \leq i \leq m$ define the maximal ideal $M_i := \langle X_1 - a_1^i, \ldots, X_n - a_n^i \rangle \subset \overline{K}[\underline{X}]$. Consider the homomorphism

$$\begin{aligned} \varphi : \overline{K}[\underline{X}] &\to \prod_{j=1}^{m} \overline{K}[\underline{X}]/M_j \\ f &\mapsto (f + M_1, \ldots, f + M_m) \end{aligned}$$

Note that $(M_j)_{j=1}^m$ are pairwise coprime. Thus there exist $u_2, \ldots, u_m \in M_1$ and $v_j \in M_j$ for all $2 \leq j \leq m$ such that $u_i + v_i = 1$ for all $2 \leq i \leq m$. Let $f := \prod_{j=2}^m (1 - u_j) \in \overline{K}[\underline{X}]$. Then $\varphi(f) = (1, 0, \ldots, 0)$. Repeating this argument for all $(M_j)_{j=2}^m$, we obtain that φ is surjective.

On the other hand $\ker(\varphi) = \bigcap_{j=1}^m M_j \supset J$. Every element $h \in \bigcap_{j=1}^m M_j$ has the m zeroes $(a_1^i, \ldots, a_n^i)_{i=1}^m$. By Hilbert's Nullstellensatz and the fact that J is radical it follows that $h \in J$. Thus $\ker(\varphi) = J$.

Hence we have an isomorphism $\overline{K}[\underline{X}]/J \cong \prod_{j=1}^m \overline{K}[\underline{X}]/M_j$ which is in particular $\overline{K}$-linear. Since $\overline{K}$ is algebraically closed, we have $\overline{K}[\underline{X}]/M_j \cong \overline{K}$. Hence $\overline{K}[\underline{X}]/J \cong \overline{K}^m$. This yields $\dim_{\overline{K}}(\overline{K}[\underline{X}]/J) = m$ and thus concludes the proof. □

Lemma 6.4. *Let $I \subset K[\underline{X}]$ be a proper radical ideal of finite codimension and let $c_1, \ldots, c_n \in K$. Assume that for each pair of two different zeroes $(z_1, \underline{x}), (z_2, \underline{y}) \in K^{n+1}$ of $J := \langle I, Z - \sum_{i=1}^n c_i X_i \rangle$ we have $z_1 \neq z_2$. Let $\succeq$ be a monomial ordering such that $\deg(X_i) \succeq \deg(Z)$ for all $1 \leq i \leq n$. Then there exist $g, g_1, \ldots, g_n \in K[Z]$ such that $\{g, X_1 - g_1, \ldots, X_n - g_n\}$ is the reduced Gröbner basis of J with respect to $\succeq$. Moreover g is square-free.*

Proof. It follows by Lemma 6.1 that J is radical and of finite codimension. Let m be the number of zeroes of J in $\overline{K}^{n+1}$. Then $\dim_K(K[\underline{X}][Z]/J) = m$ by Proposition 6.3. Let $g \in J \cap K[Z]$ be the monic generator of $J \cap K[Z]$. Lemma 5.9 implies that g is square-free.

By assumptions on J there are m pairwise different Z-components of zeroes of J. All of those must be a zero of g. Thus $m \leq \deg(g) =: d$. On the other hand, there is no polynomial in $J \cap K[Z]$ with lower degree than g. This implies that $(Z^i)_{i=0}^{d-1}$ are linearly independent mod J. Hence $d \leq \dim_K(K[\underline{X}][Z]/J) = m \leq d$, so $(Z^i)_{i=0}^{d-1}$ is a basis of $K[\underline{X}][Z]/J$. Thus there exist $a_0^i, \ldots, a_{d-1}^i \in K$ for all $1 \leq i \leq n$ such that $X_i - g_i \in J$, where $g_i := \sum_{j=0}^{d-1} a_j^i Z^j$.

Let $G := \{g, X_1 - g_1, \ldots, X_n - g_n\}$. Let $f \in J$. If $f \in K[Z]$, then g divides f and thus $\mathrm{LT}(g)$ divides $\mathrm{LT}(f)$, where we take LT with respect to $\succeq$. Otherwise $\mathrm{LT}(f)$ is divisible by X_i for an index $1 \leq i \leq n$. This follows by choice of $\succeq$. Hence G is indeed a Gröbner basis of J. But we can see that G is even a reduced Gröbner basis. This concludes the proof. □

Lemma 6.5. *Let $I \subset K[\underline{X}]$ be an ideal. Let $m_1, \ldots, m_n \in \mathbb{Z}^{>0}$. For each $1 \leq i \leq n$ let $A_i \subset K$ with $|A_i| \leq m_i$ and $k_i := \prod_{j=1}^{i} m_j$. For each $1 \leq i \leq n$ let $C_i := \{1, 2, \ldots, \binom{k_i+1}{2}\}$. Then there exists $(c_1, \ldots, c_n) \in C := C_1 \times \cdots \times C_n$ such that $\sum_{i=1}^n c_i x_i \neq \sum_{i=1}^n c_i y_i$ for all $x, y \in A_1 \times \cdots \times A_n$ with $x \neq y$.*

Proof. We proceed by induction on n. If $n = 1$ the statement follows directly.

Let $n > 1$ and assume that the statement is true for n. Thus we can choose $(c_1, \ldots, c_n) \in C$ such that for each choice of two different $x, y \in A_1 \times \cdots \times A_n$ we have $\sum_{i=1}^n c_i x_i \neq \sum_{i=1}^n c_i y_i$. Every $c_{n+1} \in C_{n+1}$ not satisfying the statement is a solution of the linear equation $\sum_{i=1}^n c_i a_i + Y a_{n+1} = \sum_{i=1}^n c_i b_i + Y b_{n+1}$ for two different $a, b \in A_1 \times \cdots \times A_{n+1}$. It follows by choice of $(c_i)_{i=1}^n$ that $a_{n+1} \neq b_{n+1}$. The unique solution to this equation is $Y = \frac{\sum_{i=1}^n c_i(a_i - b_i)}{b_{n+1} - a_{n+1}}$. There are as many such equations as we can choose two different $a, b \in A_1 \times \cdots \times A_{n+1}$. This yields a total of $l := \binom{\prod_{i=1}^{n+1} |A_i|}{2} = \binom{k_{n+1}}{2}$ such equations. Since $|C_{n+1}| > l$ we can choose an element $c_{n+1} \in C_{n+1}$ which is not a solution to such an equation. Then $(c_1, \ldots, c_{n+1})$ satisfies the statement. □

Algorithm 6.6. Let $I \subset K[\underline{X}]$ be a proper radical ideal of finite codimension. The following algorithm computes a finite set $G = \{g, X_1 - g_1, \ldots, X_n - g_n\} \subset K[\underline{X}][Z]$ with $g, g_1, \ldots, g_n \in K[Z]$ such that $\langle G \rangle \cap K[\underline{X}] = I$. Furthermore g is square-free.

Input: $f_1, \ldots, f_m$, generators of I
Output: G, as above
begin
  $m := 1$
  for $1 \leq i \leq n$ **do**
    $F_i :=$ the reduced Gröbner basis of $I \cap K[X_i]$ (Task 3.27, Algorithm 3.22)
    $f_i :=$ the only element of F_i
    $m_i := \deg(f_i)$
    $m := m \cdot m_i$
    $C_i := \{1, 2, \ldots, \binom{m+1}{2}\}$
  end
  $C := C_1 \times \cdots \times C_n$
  repeat
    select $c := (c_1, \ldots, c_n) \in C$
    $C := C \setminus \{c\}$
    $\succeq$, a monomial ordering such that $X_i \succeq Z$ for all i
    $G :=$ the reduced Gröbner basis of $\langle I, Z - \sum_{i=1}^n c_i X_i \rangle$ w.r.t. $\succeq$ (Algorithms 3.19 and 3.22)
  until G *is of the form* $\{g, X_1 - g_1, \ldots, X_n - g_n\}$
end

Proof. Note that $m \geq 1$ at all times in the algorithm, since I is a proper ideal. Therefore, the sets C_i are well-defined. We first show that the algorithm terminates. For all $1 \leq i \leq n$ let $A_i := \{x \in K \mid x \text{ is zero of } I \cap K[X_i]\}$. Note that if $(z, x_1, \ldots, x_n) \in K^{n+1}$ is a zero of $\langle I, Z - \sum_{i=1}^n c_i X_i \rangle$ then $x_i \in A_i$ for all i. Furthermore $|A_i| \leq m_i$ for all $1 \leq i \leq n$ and for m_i defined in the algorithm, since m_i is the degree of the generator of $I \cap K[X_i]$. It follows by Lemma 6.5 that there is $(c_1, \ldots, c_n) \in C$ such that for two different zeroes $(z_1, \underline{x}), (z_2, \underline{y}) \in K^{n+1}$ of $\langle I, Z - \sum_{i=1}^n c_i X_i \rangle$ we have $\sum_{i=1}^n c_i x_i \neq \sum_{i=1}^n c_i y_i$. This implies that $z_1 \neq z_2$. By Lemma 6.4, the reduced Gröbner basis G of $\langle I, Z - \sum_{i=1}^n c_i X_i \rangle$ has the desired form. Thus the algorithm must terminate. Moreover, it follows by Lemma 6.4 that the only element g of $G \cap K[Z]$ is square-free. Furthermore, Lemma 6.1 implies that $\langle G \rangle \cap K[\underline{X}] = I$. Hence the algorithm is correct. □

Definition 6.7. Let $I \subset K[\underline{X}]$ be an ideal of finite codimension. For each $1 \leq i \leq n$ let $f_i \in I \cap K[X_i]$ be the unique monic generator of $I \cap K[X_i]$. For all $1 \leq i \leq n$ define $\mu_i := \max\{\ell \in \mathbb{Z}^{>0} \mid p^\ell \text{ divides } f_i \text{ for some irreducible } p \in K[X_i]\}$. Then the integer $\mu := 1 + \sum_{i=1}^n (\mu_i - 1)$ is called **univariate exponent** of I.

From commutative algebra we know that in a Noetherian ring every ideal contains a power of its radical. In this special case we can determine such a (not necessarily minimal) power:

Claim 6.8. *Let $I \subset K[\underline{X}]$ be an ideal of finite codimension. Let μ be the univariate exponent of I. Then $\langle (Rad(I))^\mu \rangle \subset I$.*

Proof. For each $1 \leq i \leq n$ let $f_i \in K[X_i]$ be the monic generator of $I \cap K[X_i]$ with square-free part g_i. Let μ_i be as in the definition of the univariate exponent, Definition 6.7. Then f_i divides $g_i^{\mu_i}$. Define the ideal $J := \langle I, g_1, \ldots, g_n \rangle$. We claim that $J = \mathrm{Rad}(I)$. To see this note that $J \subset \mathrm{Rad}(I)$, since every $g_i \in \mathrm{Rad}(I)$. It follows by Lemma 5.9 that J is radical. Hence $J = \mathrm{Rad}(I)$.

Let $f \in J^\mu$. Then there exist $s_1, \ldots, s_\mu \in I$ and $h_{ij} \in K[\underline{X}]$ for all $1 \leq i \leq \mu$ and $1 \leq j \leq n$ such that

$$f = \prod_{i=1}^{\mu} \left(s_i + \sum_{j=1}^{n} h_{ij} g_j \right)$$

Expanding this product there exists $s \in I$ such that

$$f = s + \prod_{i=1}^{\mu} \sum_{j=1}^{n} h_{ij} g_j$$

Again expanding the product every resulting term is of the form

$$h \prod_{i=1}^{n} g_i^{\nu_i} \tag{4}$$

for a polynomial $h \in K[\underline{X}]$ and $\nu_1, \ldots, \nu_n \in \mathbb{Z}^{\geq 0}$ with $\sum_{i=1}^n \nu_i = \mu$. Since $\mu = 1 + \sum_{i=1}^n (\mu_i - 1)$ there is an index k such that $\nu_k \geq \mu_k$. Then f_k divides $g_k^{\nu_k}$ and thus $g_k^{\nu_k} \in I$. Hence the whole term (4) lies in I. We have shown that every term of f in the expansion lies in I. Thus $f \in I$. We conclude that $J^\mu \subset I$. □

Task 6.9. (Univariate Exponent) Let $I \subset K[\underline{X}]$ be an ideal of finite codimension. Compute the univariate exponent of I.

Solution. Compute the monic generator $f_i \in I \cap K[X_i]$ for all $1 \leq i \leq n$ using Task 3.27. By assumption on the field K we can factorize each f_i into irreducible factors. For each $1 \leq i \leq n$ define μ_i to be the maximal multiplicity of such an irreducible factor. Then define $\mu := 1 + \sum_{i=1}^n (\mu_i - 1)$. By definition μ is the univariate exponent of I.

Proposition 6.10. *Let $P \subset K[\underline{X}]$ be an ideal. Then P is a maximal ideal if and only if P is prime and of finite codimension. In particular, if $I \subset K[\underline{X}]$ is an ideal of finite codimension and I is contained in a prime ideal $P \subset K[\underline{X}]$, then P is maximal.*

Proof. "⇒": Let $J \subset K[\underline{X}]$ be a prime ideal of infinite codimension. Since J is prime it is in particular proper. Therefore there exists a zero $(z_1, \ldots, z_n) \in \overline{K}^n$ of J. Since J is of infinite codimension, there is a $k > 0$ such that $J \cap K[X_k] = \{0\}$. Let $f \in K[X_k]$ be such that $f(z_k) = 0$. Since $\overline{K}$ is algebraic over K such an f must exist. The ideal $\langle J, f \rangle$ is proper since $(z_1, \ldots, z_n)$ is a zero. Furthermore, it extends J non-trivially. Thus J is not maximal. Hence every maximal ideal is prime and of finite codimension.

"⇐": Let $P \subset K[\underline{X}]$ be a prime ideal of finite codimension. Let $f \in K[\underline{X}]/P$ be non-zero. Consider the K-linear map $K[\underline{X}]/P \to K[\underline{X}]/P$, $g \mapsto fg$. Since P is a prime ideal, the ring $K[\underline{X}]/P$ is an integral domain. Thus the map is injective. Since $K[\underline{X}]/P$ is finite dimensional, we know from linear algebra that the map is therefore also surjective. Thus there is some $g \in K[\underline{X}]/P$ with $fg = 1$. This implies that $K[\underline{X}]/P$ is a field. Hence P is a maximal ideal.

To show the last statement, note that if $I \subset K[\underline{X}]$ is of finite codimension and $P \supset I$ is a prime ideal, then P is also of finite codimension, hence by the above statement maximal. □

Lemma 6.11. *Let $I \subset K[\underline{X}]$ be an ideal of finite codimension. Let μ be the univariate exponent of I. For every associated prime ideal P of I the P-primary component of I is $Q = I + \langle P^\mu \rangle$.*

Proof. Let $(P_i)_{i=1}^m$ be the associated prime ideals of I. Proposition 6.10 tells us that they are all maximal. Therefore they are isolated associated prime ideals and thus their primary components are unique. Define $Q_i := I + \langle P_i^\mu \rangle$ for all $1 \leq i \leq m$. Let $1 \leq i \leq m$. From commutative algebra we know that if $\mathrm{Rad}(Q_i)$ is maximal, then Q_i is $\mathrm{Rad}(Q_i)$-primary. We indeed have $\mathrm{Rad}(Q_i) = \mathrm{Rad}(\mathrm{Rad}(I) + \mathrm{Rad}(\langle P_i^\mu \rangle)) = \mathrm{Rad}(P_i) = P_i$. Thus Q_i is P_i-primary.

It remains to show that $\bigcap_{i=1}^m Q_i = I$. The inclusion "$\supset$" holds by definition. For the other inclusion, let $1 \leq i \leq m$ and let Q_i' be the P_i-primary component of I. Let ν_i be the univariate exponent of Q_i'. By definition of the univariate exponent $\nu_i \leq \mu$, since $I \subset Q_i'$. Note that $\mathrm{Rad}(Q_i') = P_i$. It follows by Claim 6.8 that $\langle P_i^\mu \rangle \subset \langle P_i^{\nu_i} \rangle \subset Q_i'$. Thus $Q_i \subset Q_i'$. Hence $I \subset \bigcap_{i=1}^m Q_i \subset \bigcap_{i=1}^m Q_i' = I$ proves the lemma. □

Now we have gathered enough statements to write and prove an algorithm that computes a primary decomposition of an ideal of finite codimension:

Algorithm 6.12. Let $I \subset K[\underline{X}]$ be a proper ideal of finite codimension. The following algorithm computes the associated prime ideals of I together with their primary components.

Input: $f_1, \ldots, f_m$, generators of I
Output: $D = \{(Q, P) \mid Q, P \subset K[\underline{X}]$ finite subsets such that
$\langle P \rangle$ is an associated prime ideal of I and $\langle Q \rangle$ is the $\langle P \rangle$-primary component$\}$
begin
$R :=$ a finite generating set of $\mathrm{Rad}(I)$ (Algorithm 5.10)
$G :=$ the output of Algorithm 6.6 with input R
$A := \emptyset$
$g :=$ the only element of $G \cap K[Z]$
while g *is not constant* **do**
$p :=$ an irreducible divisor of g (assumed factorization algorithm)
$g := g/p$
$A := A \cup \{G \cup \{p\}\}$
end
$D := \emptyset$
$\mu :=$ the univariate exponent of I (Task 6.9)
while $A \neq \emptyset$ **do**
select $C \in A$
$A := A \setminus \{C\}$
$P :=$ a generating set of $\langle C \rangle_{K[\underline{X}][Z]} \cap K[\underline{X}]$ (Task 3.27)
$Q := \{f_1, \ldots, f_m\} \cup P^\mu$
$D := D \cup \{(Q, P)\}$
end
end

Proof. There are two while-loops where the algorithm could possibly not terminate. In the first one, we loop as long as the polynomial g is not constant. In each step we divide g by some irreducible factor. So the degree of g decreases strictly in every step of the loop. Thus the first loop must terminate. In the second while-loop we loop as long as the set A is non-empty. By construction of A, it is finite before the while-loop. In every step we take one element out of A decreasing strictly its cardinality. Thus the second while-loop terminates. Hence the algorithm terminates after finitely many steps.

The output of Algorithm 6.6 is $G = \{g, X_1 - g_1, \ldots, X_n - g_n\}$, where $g, g_1, \ldots, g_n \in K[Z]$. Indeed, g is the only element of $G \cap K[Z]$. Moreover g is square-free and $\langle G \rangle \cap K[\underline{X}] = I$.

We will show that every $\langle P \rangle$ constructed in the second while-loop is a maximal ideal. By construction P is a generating set of $\langle C \rangle \cap K[\underline{X}]$, where $C = G \cup \{p\}$ for an irreducible divisor p of g. We show that $\langle G \cup \{p\} \rangle \subset K[\underline{X}][Z]$ is a maximal ideal. Let $f \in K[\underline{X}][Z]$. The remainder on division of f with respect to G is an element of $K[Z]$. This follows from the fact that no term of $\overline{f}^G$ is divisible by any element of $\mathrm{LT}(G) = \{\mathrm{LT}(g), X_1, \ldots, X_n\}$. If $\overline{f}^G$ and p are not coprime, then $f \in \langle G \cup \{p\} \rangle$. Otherwise $\gcd(\overline{f}^G, p) = 1 \in \langle G \cup \{p\} \cup \{f\} \rangle$,

since $\overline{f}^G \in \langle G \cup \{p\} \cup \{f\}\rangle$. Hence $\langle G \cup \{p\}\rangle$ is a maximal ideal and in particular prime. Note that P is the contraction of $\langle G \cup \{p\}\rangle$ with respect to the embedding homomorphism $K[\underline{X}] \hookrightarrow K[\underline{X}][Z]$ and the contraction of a prime ideal is prime. Thus P is a prime ideal. By construction it is also true that $I \subset P$. It follows by Proposition 6.10 that P is a maximal ideal.

Now we show that each pair of two such $\langle P\rangle$ is distinct. Let P_1, P_2 be two such P constructed in the algorithm. For $i = 1, 2$ the set P_i is a generating set of $\langle G \cup \{p_i\}\rangle \cap K[\underline{X}]$, where $p_1, p_2 \in K[Z]$ are irreducible divisors of g. Since g is square-free p_1 and p_2 are coprime. Then $\langle G \cup \{p_1\}\rangle$ and $\langle G \cup \{p_2\}\rangle$ are distinct and both maximal. Therefore we can find $h_1 \in \langle G \cup \{p_1\}\rangle$ and $h_2 \in \langle G \cup \{p_2\}\rangle$ such that $h_1 + h_2 = 1$. Set $Z = \sum_{i=1}^n c_i X_i$ where $c_1, \ldots, c_n \in K$ are such that $\langle G\rangle = \langle I, Z - \sum_{i=1}^n c_i X_i\rangle$. We obtain the equation $\widehat{h}_1 + \widehat{h}_2 = 1$ with $\widehat{h}_1 \in (h_1 + \langle Z - \sum_{i=1}^n c_i X_i\rangle) \cap K[\underline{X}] \subset \langle G \cup \{p_1\}\rangle \cap K[\underline{X}] = P_1$ and analogously $\widehat{h}_2 \in P_2$. Hence P_1 and P_2 are distinct.

By Proposition 6.10, every associated prime ideal is maximal. Note that a maximal ideal that contains an intersection of other maximal ideals must be equal to one of the other ideals. We can deduce that the constructed ideals $\langle P\rangle$ must be associated prime ideals of I.

Therefore, it remains to prove that we have constructed all associated prime ideals of I. Let $P' \subset K[\underline{X}][Z]$ be an associated prime ideal of $\langle G\rangle$. In particular we have $g \in P'$. Since P' is prime, we deduce that there is an irreducible factor p of g such that $p \in P'$. Therefore $\langle G \cup \{p\}\rangle \subset P'$ and since the first one is maximal we even have equality. So the associated prime ideals of $\langle G\rangle$ are all of the form $\langle G \cup \{p\}\rangle$ for an irreducible factor p of g. Hence we can choose a primary decomposition $\bigcap_{i=1}^{\ell} Q'_i = \langle G\rangle$ of $\langle G\rangle$ such that $\mathrm{Rad}(Q'_i) = \langle G \cup \{p_i\}\rangle$ for $(p_i)_{i=1}^{\ell}$ the irreducible factors of g. Then

$$\bigcap_{i=1}^{\ell} \langle G \cup \{p_i\}\rangle \cap K[\underline{X}] = \mathrm{Rad}\left(\bigcap_{i=1}^{\ell} (Q'_i \cap K[\underline{X}])\right) = \mathrm{Rad}(\langle G\rangle \cap K[\underline{X}]) = \mathrm{Rad}(I)$$

This implies that the associated prime ideals of I are all of the form $\langle G \cup \{p\}\rangle \cap K[\underline{X}]$ for an irreducible factor p of g. In the algorithm we have constructed every such prime ideal. Hence, the algorithm has constructed every associated prime ideal of I.

By Lemma 6.11, for every associated prime $\langle P\rangle$ of I the primary component is $Q = I + \langle P^{\mu}\rangle$. This concludes the proof of the correctness of the algorithm. □

6.2 The general case

The general case is a direct consequence of the finite codimension case:

Algorithm 6.13. Let $I \subset K[\underline{X}]$ be an ideal. The following algorithm computes a primary decomposition of I.

Input: $f_1, \ldots, f_m$, generators of I
Output: $D = \{(Q, P) \mid Q, P \subset K[\underline{X}]$ finite subsets such that
$\langle Q \rangle$ runs through all primary ideals of a primary decomposition of I and
$\langle P \rangle = \mathrm{Rad}(\langle Q \rangle)\}$
begin
$D := \emptyset$
if $1 \notin I$ **then**
$\underline{Y} \subset \underline{X}$, maximal algebraically independent variables mod I
$\underline{Z} := \underline{X} \setminus \underline{Y}$
$C :=$ the output of Algorithm 6.12 with input $\{f_1, \ldots, f_m\} \subset K(\underline{Y})[\underline{Z}]$
$A := \emptyset$
while $C \neq \emptyset$ **do**
select $(G, H) \in C$
$C := C \setminus \{(G, H)\}$
$Q :=$ a generating set of $\langle G \rangle^c \subset K[\underline{X}]$ (Algorithm 5.13)
$P :=$ a generating set of $\langle H \rangle^c \subset K[\underline{X}]$ (Algorithm 5.13)
$A := A \cup \{(Q, P)\}$
end
$f :=$ an element in $K[\underline{Y}]$ such that $I = (I + \langle f \rangle) \cap I^{ec}$ (Algorithm 5.16)
$D' :=$ the output of Algorithm 6.13 with input $\{f_1, \ldots, f_m, f\}$ (recursively)
$D := A \cup D'$
end
end

Proof. First, we prove that the algorithm terminates. The while-loop terminates since C is a finite set and in each step we decrease its cardinality strictly. We also use the algorithm recursively and need to show that the recursion stops. For every $i \geq 1$ denote $\bar{f}_i$ for the f in the algorithm constructed in the ith recursion step. Let $I_1 := I$. Then $I_{i+1} = I_i + \langle \bar{f}_i \rangle$ is the input of the $(i+1)$th recursion step for $i \geq 1$. Let $\underline{Y}_i$ be the maximal algebraically independent variables mod I_i in the ith recursion step. Then we have $\bar{f}_i \in K[\ \underline{Y}_i\ ]$ and $\underline{Y}_i$ being algebraically independent mod I_i implies that $\bar{f}_i \notin I_i$. Hence, we have a strictly ascending chain $I_1 \subset I_2 \subset \ldots$ of ideals as long as the algorithm does not terminate. But we know that $K[\underline{X}]$ is Noetherian and thus there is a $k \geq 1$ with $I_k = K[\underline{X}]$. Then $1 \in I_k$ in the kth recursion step and thus the recursion stops. This implies that the algorithm terminates.

Next we prove correctness. We note that the elements of C form a primary decomposition of I^e. Let $(G_1, H_1), \ldots, (G_k, H_k) \in C$ be all the elements of C. Then $\langle H_i \rangle^c$ is prime for all

$1 \leq i \leq k$, since the contraction of a prime ideal is prime. The contraction of a primary ideal is a primary ideal and $\mathrm{Rad}(\langle G_i \rangle^c) = \mathrm{Rad}(\langle G_i \rangle)^c = \langle H_i \rangle^c$ for all $1 \leq i \leq k$. Thus $\langle G_i \rangle^c$ is $\langle H_i \rangle^c$-primary for all $1 \leq i \leq k$. Also $\bigcap_{i=1}^k \langle G_i \rangle^c = (\bigcap_{i=1}^k \langle G_i \rangle)^c = I^{ec}$. Let Q_i be a generating set of $\langle G_i \rangle^c$ and P_i a generating set of $\langle H_i \rangle^c$. Then this argument shows that the elements of $\{(Q_i^c, P_i^c) \mid 1 \leq i \leq k\} = A$ form a primary decomposition of I^{ec}.

Let $(Q_1', P_1'), \ldots, (Q_\ell', P_\ell') \in D'$ be all the elements of D'. Then $\bigcap_{i=1}^\ell \langle Q_i' \rangle = I + \langle f \rangle$. Thus $\bigcap_{i=1}^k \langle Q_i \rangle^c \cap \bigcap_{j=1}^\ell \left\langle Q_j' \right\rangle = I^{ec} \cap (I + \langle f \rangle) = I$. So indeed the elements of $D = A \cup D'$ form a primary decomposition of I. □

Task 6.14 (Associated Prime Ideals)**.** Let $I \subset K[\underline{X}]$ be an ideal. Compute the associated prime ideals of I together with their primary components of a primary decomposition of I.

Solution. By definition, the associated prime ideals are the prime ideals of a minimal primary decomposition. Use Algorithm 6.13 to compute a primary decomposition $\bigcap_{i=1}^m Q_i = I$ of I with prime ideals $P_i := \mathrm{Rad}(Q_i)$ for all $1 \leq i \leq m$. If $P_k = P_\ell$ for any $k \neq \ell$, then define $\tilde{Q} := Q_k \cap Q_\ell$. This can be checked using Task 3.24. Then $\tilde{Q}$ is again P_k-primary. So $\bigcap_{i \neq k,\ell} Q_i \cap \tilde{Q} = I$ is again a primary decomposition. Inductively we can thus construct a primary decomposition $\bigcap_{i=1}^r \tilde{Q}_i = I$ such that $\mathrm{Rad}(\tilde{Q}_i) \neq \mathrm{Rad}(\tilde{Q}_j)$ for all $i \neq j$. Check for each $1 \leq k \leq r$ if $\tilde{Q}_k \supset \bigcap_{i \neq k} \tilde{Q}_i$ using Tasks 3.25 and 3.29 and if yes, then omit $\tilde{Q}_k$. Finally, we arrive at a minimal primary decomposition which gives us the associated prime ideals of I and their primary components of a primary decomposition.

Task 6.15 (Primary)**.** Let $I \subset K[\underline{X}]$ be an ideal. Is I a primary ideal?

Solution. Compute the associated prime ideals of I using Task 6.14. Use the fact that an ideal I is primary if and only if it has only one associated prime ideal.

Task 6.16 (Prime)**.** Let $I \subset K[\underline{X}]$ be an ideal. Is I a prime ideal?

Solution. Compute the associated prime ideals of I together with their primary components using Task 6.14. Use that an ideal I is prime if and only if there is only one associated prime ideal and its primary component is equal to this associated prime ideal.

Task 6.17 (Maximal)**.** Let $I \subset K[\underline{X}]$ be an ideal. Is I a maximal ideal?

Solution. Check if I is a prime ideal using Task 6.16. Compute every intersection $I \cap K[X_i]$ for all $1 \leq i \leq n$ using Task 3.27. Then Proposition 6.10 implies that I is maximal if and only if I is prime and every computed intersection is non-trivial.

7 Complexity

We have proven that the algorithms given in this thesis are correct. However, we never mentioned the efficiency. This would be very important if we were to implement those algorithms in a computer program. In the following section we give a brief overview of the complexity of the algorithms without claiming to treat it rigorously.

The Division Algorithm 3.12 has polynomial complexity: Let r be the number of terms of $f \in K[\underline{X}]$ and let m denote the cardinality of F for $F \subset K[\underline{X}]$. Then, in the worst case, the algorithm computes in $m \cdot r$ steps a remainder on division of f with respect to F. Thus using Task 3.20, if we have a Gröbner basis, the ideal membership problem can be solved in polynomial time. Interestingly enough, the ideal membership problem, as treated in Task 3.20, is NP-hard as shown by Huynh [4]. Hence computing a Gröbner basis is also NP-hard. But if we are given a finite subset of $K[\underline{X}]$, we can check, in polynomial time, if it is a Gröbner basis or not by Theorem 3.18. So computing a Gröbner basis is NP-complete. Therefore, finding an efficient algorithm (in polynomial time) is equivalent to the problem P = NP, which is still open. Hence, we cannot hope to find such an algorithm. The same holds for most of the other algorithms deduced in this thesis, as they use Buchberger's Algorithm 3.19.

However, we can still try to improve our algorithms a bit. For instance in Buchberger's Algorithm 3.19 we repeatedly compute $\overline{S(p,q)}^{G'}$ for the same pair $p, q \in G'$. But if $\overline{S(p,q)}^{G'} \neq 0$ in some step of the while-loop, then in every further step we will have $\overline{S(p,q)}^{G'} = 0$. So in principle, we only need to compute this remainder on division for the newly added elements of G'. Also, the S-polynomial is anti-symmetric, so we only need to consider ordered pairs of G'. But there are also more improvements that can be done. Cox, Little and O'Shea give a discussion about some improvements in §9 of Chapter 2 in their book [3]. With such improvements the algorithm gets efficient enough to be used in computer algebra systems.

We can also improve our algorithm for computing the radical of an ideal. Some improvements that lead to a slightly different algorithm were suggested by Laplagne [6]. He does a critical analysis of the complexity of his algorithm and arrives at a doubly exponential bound. Nevertheless, his algorithm can be used to compute radicals in practice, as his performance evaluation shows.

Another thing to keep in mind when designing an algorithm are the prerequisites. For instance, the radical of an ideal can also be computed using a primary decomposition. But for a primary decomposition, we need to be able to factorize a polynomial in one variable into irreducible polynomials. This is a stronger assumption on the field than is needed for computing the radical directly. In some cases, such an indirect approach may be possible and more efficient. Therefore, we need different algorithms for different cases. But often, one cannot decide a priori whether one or the other is better.

8 Conclusion

Using the algorithms and tasks of this thesis we can do most of the calculations a contemporary computer algebra system can do in the area of polynomial ideals. With the improvements mentioned in section 7 we can directly implement them. We have seen that the results of the standard theory of commutative algebra are not enough to do explicit calculations. We need a theory that is tailored to computation. This computational theory is part of an active research area. From time to time new algorithms are designed to either improve existing ones or provide a totally different approach that is more efficient in some cases.

To give a final overview of our achievements in this thesis we provide a list of the most useful algorithms and tasks that we have seen:

- Algorithm 3.12: Division algorithm; computes a **remainder on division**.
- Algorithm 3.19: Buchberger algorithm; computes a **Gröbner basis** of an ideal.
- Task 3.20: **ideal membership**; decides whether a polynomial lies in the given ideal.
- Algorithm 3.22: computes a **reduced Gröbner basis** of an ideal.
- Task 3.24: **ideal equality**; decides whether two given ideals are equal.
- Task 3.25: **subideal**; decides for two ideals whether one is a subideal of the other.
- Task 3.29: computes the **intersection** of ideals.
- Algorithm 4.5: computes the **quotient** of two ideals.
- Task 5.2: **radical membership**; decides whether a polynomial lies in the radical of a given ideal.
- Task 5.6: computes the **square-free part** of a polynomial.
- Algorithm 5.10: computes the **radical** of an ideal of **finite codimension**.
- Algorithm 5.18: computes the **radical** of an ideal.
- Algorithm 6.12: computes a **primary decomposition** of an ideal of **finite codimension**.
- Algorithm 6.13: computes a **primary decomposition** of an ideal.
- Task 6.14: computes the **associated prime ideals** of a given ideal.
- Task 6.15: decides whether a given ideal is **primary**.
- Task 6.16: decides whether a given ideal is **prime**.
- Task 6.17: decides whether a given ideal is **maximal**.

References

[1] Atiyah, M.F.; MacDonald, I.G.: *Introduction to Commutative Algebra.* Addison-Wesley Series in Mathematics. Westview Press, 1969.

[2] Becker, T.; Weispfenning, V.: *Gröbner Bases.* Graduate Texts in Mathematics 141. Springer, 1993.

[3] Cox, D.; Little, J.; O'Shea, D.: *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics 0172-6056. Springer, 2007.

[4] Huynh, D.T.: *The complexity of the membership problem for two sub- classes of polynomial ideals.* SIAM Journal on Computing, Volume 15, Issue 2, 1986, pages 581-594.

[5] Kreuzer, M.; Robbiano, L.: *Computational Commutative Algebra 1.* Springer, 2000.

[6] Laplagne, S.: *An algorithm for the computation of the radical of an ideal.* 2006, In Proceedings of the 2006 international symposium on Symbolic and algebraic computation (ISSAC '06). ACM, New York, pages 191-195.

[7] Matsumoto, R.: *Computing the Radical of an Ideal in Positive Characteristic.* Journal of Symbolic Computation, Volume 32, Issue 3, September 2001, Pages 263-271, ISSN 0747-7171.