Department of Mathematics
TUM School of Computation, Information and Technology
Technical University of Munich

The Computation of the Radical of an Ideal

Sebastian Bender

Thesis for the attainment of the academic degree

Bachelor of Science

at the TUM School of Computation, Information and Technology of the Technical University of Munich

Supervisor:
Prof. Dr. rer. nat. habil. Gregor Kemper

Advisor:
Dr. rer. nat. Fabian Reimers

Submitted:
Munich, 15.09.2024

I hereby declare that this thesis is entirely the result of my own work except where otherwise indicated. I have only used the resources given in the list of references.

Munich, 15.09.2024 Sebastian Bender

Acknowledgments

I would like to extend my sincere gratitude to Dorothea Knirsch, for her moral support during my research and writing process, as well as for helping me improve my wording and for finding countless typographical and grammatical errors.

Zusammenfassung

Die Hauptobjekte der vorliegenden Arbeit sind Ideale von Polynomringen in n Variablen und über einem perfekten Körper. Das Ziel dieser Bachelorarbeit ist es, einen Algorithmus vorzustellen, welcher das Radikal eines solchen Ideals berechnet. Nach der Einführung geben wir eine kurze Übersicht über einige wesentliche Resultate aus der kommutativen Algebra. Wir geben außerdem eine kurze Einführung in die Gröbner Basis Theorie, welche nahe an dem Kapitel über Gröbner Basen in Kemper's Buch [Kem11] angelegt ist. Für den Hauptteil dieser Arbeit werden wir dem Buch von Becker und Weißpfenning [BW93] folgen, in dem die zentrale Strategie für der Berechnung von Radikalen Idealen ist, das Problem auf den Fall zu reduzieren, wo das Ideal null-dimensional ist. Wenn wir uns mit diesem Fall beschäftigen, beweisen wir unter anderem Seidenberg's Lemma, welches besagt, dass man für ein Erzeugendensystem des Radikals eines Ideals I nur ein Erzeugendensystem von I und den quadratfreien Teil der monischen Erzeuger der Eliminationsideale von I braucht. Wir zeigen dafür, wie man monische Erzeuger in univariaten Polynomringen berechnet und wie man quadratfreie Teile von Polynomen in einer Variable berechnet. Hierbei muss man zwischen den zwei Fällen unterscheiden, wo der zugrundeliegende Körper Charakteristik 0 oder p, mit p einer Primzahl, hat. Für Letzteres richten wir uns nach dem Artikel von Gianni *et al.* [GT96] über quadratfreie Zerlegung, um eine Methode zur Berechnung von quadratfreien Teilen in perfekten Körpern mit Charakteristik p zu entwickeln. Danach geben wir eine Einführung in Idealquotienten und in die Theorie von Extensionen und Kontraktionen von Idealen. Diese Theorie erlaubt es uns, den Algorithmus, welcher Radikale von null-dimensionalen Idealen berechnet, für beliebig dimensionale Ideale zu generalisieren. Nachdem wir den Algorithmus für das Berechnen von Radikalen von Idealen präsentiert haben, geben wir eine Beispielrechnung, mit der wir den Algorithmus in der Praxis darstellen.

Abstract

The central objects of the present study are ideals of polynomial rings in n variables and over a perfect field. The goal of this thesis is to present an algorithm that computes the radical of such an ideal. After our introduction, we give a brief overview of some basic results from commutative algebra that are used when proving the correctness of the algorithms. Following the outline of the chapter on Gröbner bases in Kemper's book [Kem11], we also give a short introduction into the theory of Gröbner bases. For the main part of this thesis, we follow Becker and Weißpfenning's book [BW93], where the central strategy for computing the radical of an ideal is to reduce the problem to the case where the ideal is zero-dimensional. When looking at zero-dimensional ideals, we prove Seidenberg's Lemma, which shows that for a generating set of the radical of an ideal I, you only need a generating set of I and the squarefree parts of monic generators of elimination ideals of I. For this, we show how to compute the monic generator of an ideal in a univariate polynomial ring and how to compute squarefree parts of polynomials in one variable. Here we have to distinguish between the two cases where the underlying field has characteristic 0 or p, with p being a prime number. For the latter case we follow the paper by Gianni *et al.* [GT96] on squarefree decomposition, in order to develop a method of computing the squarefree part in perfect fields with characteristic p. After that, we introduce colon ideals and then the theory of extensions and contractions of ideals. This allows us to generalize the algorithm, that computes radicals of zero-dimensional ideals, to arbitrary dimensional ideals. After presenting the algorithm for computing the radical of an ideal, we show an example computation of the radical of an ideal, to demonstrate the algorithm in a realistic setting.

Contents

1 Introduction

In this thesis, we primarily concern ourselves with ideals of polynomial rings in n variables over a field K. Often, we will require K to be perfect, but sometimes we also work with general rings instead of polynomial rings. In that case R being a ring means that it is commutative and contains a 1. By definition, K being **perfect** means that every irreducible polynomial $f \in K[x]$ is **separable**; i.e. in the algebraic closure $\overline{K}$, the roots of f are distinct. There are many equivalent characterizations of K being perfect. In particular, if K has characteristic 0 or K is finite, it is perfect. We will see other equivalent statements in Section 2.1.

The **radical** of an ideal I in a ring R will be written as $\sqrt{I}$ and is defined as

$$\sqrt{I} := \{r \in R \mid \exists n \in \mathbb{N} : r^n \in I\}.$$

An ideal I is called a **radical ideal**, if

$$\sqrt{I} = I.$$

One can see that using our notation for the radical is not too misleading, since we can think of taking the radical of an ideal I, as taking n-th roots of elements of I and if they are in R, they also go into $\sqrt{I}$. It is therefore important over which ring we take the radical. Take as an example $I = (0)$, then if $\sqrt{I}$ is taken over an integral domain, then $\sqrt{0} = \{0\}$, but if R contains a nilpotent element $a \neq 0$, then there is some $n \in \mathbb{N}$ such that $a^n = 0$ and therefore $0 \neq a \in \sqrt{I}$. For that reason $\sqrt{(0)}$ is also often called the **nilradical**. Most of the time, we will take the radical over $K[x_1, \ldots, x_n]$, unless it is clear which other ring we use or when we explicitly state the ring.

Taking radicals can be quite easy, for example when looking at the ring of integers $\mathbb{Z}$, the radical of an ideal (n) is the ideal generated by $m \in \mathbb{Z}$, where m is the product of the prime factors of n. In fact, in Chapter 3, we will see a similar result for polynomial rings over perfect fields, which will be the basis for computing the radical of zero-dimensional ideals. However, most of the time it is not quite as easy. Looking at arbitrary ideals of $K[x_1, \ldots, x_n]$, it is not generally clear what the radical is or even whether it is already a radical ideal or not.

Nevertheless, the radicals of ideals are quite important, as they appear all over commutative algebra and other related fields. They appear quite naturally in the context of affine varieties, as one version of Hilbert's Nullstellensatz states that in a polynomial ring $K[x_1, \ldots, x_n]$, with K being algebraically closed, the vanishing ideal of an affine variety of an ideal I is equal to the radical of I; in symbols this means

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}.$$

A proof of this can be found in [Kem11].

It is also a curious fact that every finite intersection of maximal ideals is a radical ideal and furthermore that in an affine algebra every radical is a finite intersection of maximal ideals. The former is easy to prove and we will do so later. A proof of the latter result is much more difficult and can be found in the first chapter of [Kem11]. Radicals also play an important role in the computation of primary decomposition of ideals. Radical ideals are in fact so useful that Mary W. Gray wrote an algebra textbook, centered around the notion of the radical [Gra70].

All of these facts make it clear that it is very useful to be able to determine the radical of an ideal. Our goal in this thesis is therefore to develop the theory needed and to present an algorithm that computes the radical of an ideal I of a polynomial ring $K[x_1, \ldots, x_n]$ over a perfect and computable field K. We will follow the approach given in Chapter 8 of Becker and Weißpfenning's book [BW93] for this. However, since Becker and Weißpfenning only consider fields K that have characteristic 0 or are finite in their algorithm, we will extend their result to the case where K is an arbitrary perfect field using the approach to squarefree decomposition of the paper by Gianni *et al.* [GT96]. For the computational aspect of this thesis, we give a brief introduction to Gröbner basis theory, following the chapter on Gröbner bases in Kemper's book [Kem11]. Other approaches to computing the radical of an ideal in characteristic $p > 0$ can be found in [Kem02] and [Mat01]. Another notable method is by Eisenbud *et al.* [EHV92], as they don't rely on reducing the problem to the zero-dimensional case, it is however limited in other ways.

2 Mathematical Foundations

2.1 Some Terminology and Basics Theorems

Like mentioned above, this thesis mostly concerns itself with ideals of $K[x_1, \dots, x_n]$ over a field K, and other related rings. Since any field is **factorial**, this also holds for $K[x_1, \dots, x_n]$. In particular this means that being prime and being irreducible in $K[x_1, \dots, x_n]$ is the same. The ring of univariate polynomials $K[x]$, endowed it with what we call a Euclidean function, even becomes a Euclidean domain. This will be very important when we want to compute a generator of an ideal of $K[x]$. In particular, $K[x]$ being Euclidean implies that it is also a principal ideal domain. If we write nothing about K, we will always assume that it is a field.

As we will present and use some algorithms involving computations with polynomials in $K[x_1, \dots, x_n]$, we will sometimes require K to be **computable**, which simply means that the elements of K can be represented in a computer and the basic operations, i.e. addition, subtraction and multiplication can be effectively performed. It is clear, that if K is computable, we are also able to represent the elements of $K[x_1, \dots, x_n]$ and use the basic operations on them.

Since we have to write down these algorithms, we will try to make clear, how we write them. We will start every algorithm by its name, followed with the main input, one has to give; for example "**exampleAlgorithm**(S, f):". Then comes the body of the algorithm, in the n-th step of the algorithm, we write on the left-hand side of the line (n). For assigning values to variables, we write :=; e.g. $f := g$, or $G :=$ gröbner(S) means we assign g to f and return value of the algorithm gröbner(S) to G. For **while**- and **for** loops as well as for **if** statements, we write the condition in the same line as the "while", "for" or "if", and write the body with an indentation. We will write **end** at the end of a loop, which indicates that we end the current loop, to reexamine the condition. Every algorithm will have a **return** step, next to which we write the object or value that the algorithm returns.

Looking at the definition of the radical of an ideal I, it is not immediate, that $\sqrt{I}$ is itself again an ideal, but this is in fact true. It is easy to see that for $r \in R$ and $a \in \sqrt{I}$ their product ra is in $\sqrt{I}$, since if $a \in \sqrt{I}$ then there is some $n \in \mathbb{N}$ such that $a^n \in I$ and by I being an ideal $r^n a^n$ is also in I, which by the definition of the radical means that $ra \in I$. To show that $\sqrt{I}$ is an additive subgroup; i.e. that for $a, b \in \sqrt{I}$ their sum $a + b$ is in $\sqrt{I}$; is a bit more tricky. To prove it, first let $m \in \mathbb{N}$ such that $a^m, b^m \in I$, and let $n = 2m$. By the Binomial Theorem $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$. We can now see that every term has at least one of a^m and b^m as a factor and as both of these are contained in I every term is also in I, which in turn means that the whole sum is in I, and as a result $a + b \in \sqrt{I}$. Thus we have proved that $\sqrt{I}$ is an ideal.

We will often use the notation $I \trianglelefteq R$, when we mean to say that I is an ideal in R. We will also use $[n]$ to denote the set of natural numbers from 1 to n; i.e. $[n] = \{1, 2, \dots, n\}$.

When one recalls that an ideal P is a prime ideal if and only if for any $ab \in P$ one of a and b is contained in P, it is not difficult to see that every prime ideal is in particular a radical ideal. There is also a similar characterization to the ones of prime ideals and maximal ideals that say that $P \trianglelefteq R$ is a prime ideal iff R/I is an integral domain and $m \trianglelefteq R$ is a maximal ideal iff R/m is a field. That is to say, an ideal $I \trianglelefteq R$ is a radical ideal iff R/I is **reduced**, which means that it has no non-zero nilpotent elements; i.e. there is no $0 \neq a \in R/I$ such that $a^n = 0$ for some $n \in \mathbb{N}$.

We will now show some basic results that we need later on in this thesis.

Lemma 2.1.1 *Let R be a ring and I, J ideals in R, then*

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

Proof: "$\subseteq$": Let $a \in \sqrt{I \cap J}$, then there is some $n \in \mathbb{N}$ such that $a^n \in I \cap J$, that is to say $a^n \in I$ and $a^n \in J$. It is clear therefore that $a \in \sqrt{I}$ and $a \in \sqrt{J}$ and thus $a \in \sqrt{I} \cap \sqrt{J}$.
"$\supseteq$": Now let $a \in \sqrt{I} \cap \sqrt{J}$, then we again get $n, m \in \mathbb{N}$ such that $a^n \in I$ and $a^m \in J$, then clearly $a^{n+m} \in I \cap J$ and thus $a \in \sqrt{I \cap J}$. □

Theorem 2.1.2 *Let R, S be rings, $I \trianglelefteq R$, $J \trianglelefteq S$ ideals and $\varphi : R \to S$ a homomorphism of rings, then the following hold:*

(a) If φ is surjective, then $\varphi(I)$ is an ideal of S.

(b) $\varphi^{-1}(J)$ is an ideal of R and $\ker(\varphi) \subseteq \varphi^{-1}(J)$.

(c) If φ is surjective and J is a maximal ideal of S, then $\varphi^{-1}(J)$ is a maximal ideal of R.

Proof: Since $\varphi(0) = 0$ for all homomorphisms, neither $\varphi(I)$ nor $\varphi^{-1}(J)$ are empty.
(a): First let $b_1, b_2 \in \varphi(I)$, then there are $a_1, a_2 \in I$ such that $b_1 = \varphi(a_1)$ and $b_2 = \varphi(a_2)$. Then

$$b_1 + b_2 = \varphi(a_1) + \varphi(a_2) = \varphi(a_1 + a_2) \in \varphi(I)$$

by the "idealness" of I. Now let $b \in \varphi(I)$, $a \in I$ such that $b = \varphi(a)$ and $s \in S$, since φ is surjective there is an $r \in R$ such that $\varphi(r) = s$. With that it follows that

$$sb = \varphi(r)\varphi(a) = \varphi(ra) \in \varphi(I),$$

since $rb \in I$. This shows that $\varphi(I)$ is an ideal in S.
(b): Let $a_1, a_2 \in \varphi^{-1}(J)$. By the definition of the preimage $\varphi(a_1)$ and $\varphi(a_2)$ are contained in J and thus $\varphi(a_1) + \varphi(a_2) = \varphi(a_1 + a_2) \in J$. Again, by definition of the preimage this means that $a_1 + a_2 \in \varphi^{-1}(J)$. Now let $a \in \varphi^{-1}(J)$ and $r \in R$, then $\varphi(r) \in S$ and $\varphi(a) \in J$. Since J is an ideal $\varphi(r)\varphi(a) = \varphi(ra) \in J$ and thus $ra \in \varphi^{-1}(J)$. This shows that $\varphi^{-1}(J)$ is an ideal in R.
(c): Let J be a maximal ideal of S and $\psi : S \to S/J$ the canonical map. By the definition of a maximal ideal S/J is a field. It follows directly that $\psi \circ \varphi : R \to S/J$ is a surjective homomorphism and that $\ker(\psi \circ \varphi) = \varphi^{-1}(J)$, as $\psi(a) = 0 \Leftrightarrow a \in J$. By the first isomorphism theorem $R/\ker(\psi \circ \varphi) \cong S/J$, which means that $R/\ker(\psi \circ \varphi)$ is also a field and thus $\ker(\psi \circ \varphi) = \varphi^{-1}(J)$ is a maximal ideal. □

We will not prove the following well known equivalences, but as we work with perfect fields a lot, it is good to have them in mind.

Theorem 2.1.3 *Let K be a field, then the following are equivalent:*

(a) K is perfect.

(b) Every irreducible polynomial over K is separable.

(c) For every irreducible polynomial over K, its formal derivative is non-zero.

(d) char$(K) = 0$ or char$(K) = p > 0$ and for every $a \in K$ there is some $b \in K$ such that $b^p = a$.

(e) The separable closure of K is algebraically closed.

(f) Every finite extension of K is separable.

2.2 Gröbner Bases

As the theory of Gröbner Bases will be required for the algorithms that we are trying to develop in this thesis, we will give a brief overview of the most important concepts and results. In particular, given a finite set $S \subseteq K[x_1, \ldots, x_n]$, we will see how to compute a Gröbner basis of (S) using Buchberger's algorithm. We will primarily follow Kemper's book [Kem11] for this section.

First of all, we recall that a Gröbner Basis G of an ideal I of a polynomial ring $K[x_1, \ldots, x_n]$ can be roughly described, as being a finite subset of I such that for every element $f \in I$, its Gröbner basis G contains an element g such that the leading monomial of g divides the leading monomial of f. In order to precisely define what we mean by a "leading monomial" we have to introduce the concept of "monomial orderings". Before that however, we will clear up what we mean by monomials and other related terms.

A polynomial $f \in K[x_1, \ldots, x_n]$ is called a **monomial**, if it is of the form $f = x_1^{e_1} \cdots x_n^{e_n}$ with $e_1, \ldots, e_n \in \mathbb{N}$. If there is some $c \in K$ and a monomial $g \in K[x_1, \ldots, x_n]$, then $c \cdot g$ is called a **term**, with c being its **coefficient**.

Definition 2.2.1 (Monomial orderings) *Let $\mathcal{M}$ be the set of monomials in $K[x_1, \ldots, x_n]$, then we call an ordering $\leq$ on $\mathcal{M}$ a **monomial ordering** on $K[x_1, \ldots, x_n]$, if*

(a) $\leq$ is a total ordering; i.e. for any $a, b \in \mathcal{M}$, $a \leq b$ or $b \leq a$ holds,

(b) 1 is the smallest element in $\mathcal{M}$ with respect to $\leq$,

(c) for any $a, b, c \in \mathcal{M}$, $b \leq c$ implies $ab \leq ac$.

In general, monomial orderings can vary quite a lot, but there are two special types of monomial ordering, which we will need for this thesis. For the first one let $Y = \{y_1, \ldots, y_m\} \subseteq \{x_1, \ldots, x_n\}$ be a set of variables and $Z = \{z_1, \ldots, z_{n-m}\} = \{x_1, \ldots, x_n\} \backslash Y$. A monomial ordering $\leq$ on $K[x_1, \ldots, x_n]$ is a **Y-elimination ordering** if $g < z$ for any monomial $g \in K[y_1, \ldots, y_m]$ and any $z \in Z$. We will find out at the end of this chapter, in what way these monomial orderings can be useful.

The second kind of monomial ordering we will need is actually a special kind of elimination ordering. In order to define it, we first need two arbitrary monomial orderings $\leq_1$ and $\leq_2$ on $K[x_1, \ldots, x_k]$ and $K[x_{k+1}, \ldots, x_n]$ respectively. We will then call a monomial ordering $\leq$ on $K[x_1, \ldots, x_n]$ a **block ordering** with $\leq_1$ dominating, if for monomials $f_1, f_2 \in K[x_1, \ldots, x_k]$ and $g_1, g_2 \in K[x_{k+1}, \ldots, x_n]$, the inequality $f_1 g_1 \leq f_2 g_2$ holds, if $f_1 <_1 f_2$ or $f_1 = f_2$ and $g_1 \leq_2 g_2$. We can see that a block ordering with $\leq_1$ dominating is a $\{x_{k+1}, \ldots, x_n\}$-elimination ordering on $K[x_1, \ldots, x_n]$.

We can also see that on $K[x]$ there is precisely one monomial ordering. Since monomials in $K[x]$ are of the form x^m, a monomial $f = x^a$ is greater than a monomial $g = x^b$ if and only if $a \geq b$.

Since by our definition 0 is not a monomial, we will furthermore add that by convention $0 < 1$ and therefore also $0 < g$ for any monomial g. Naturally, the **leading monomial** of a polynomial $f \in K[x_1, \ldots, x_n]$; which will be written as $\mathrm{lm}(f)$; is the greatest element of the set of monomials of f, written $mon(f)$. The **leading term** $\mathrm{lt}(f)$ is defined as the leading monomial, but multiplied by its coefficient also called the **leading coefficient** $\mathrm{lc}(f)$, that is to say $\mathrm{lt}(f) = \mathrm{lc}(f) \cdot \mathrm{lm}(f)$. If a polynomial has leading coefficient 1, we will call it **monic**. In the case where $f = 0$, we will set $\mathrm{lm}(f) = \mathrm{lt}(f) = \mathrm{lc}(f) = 0$.

Lastly, given a set $S \subseteq K[x_1, \ldots, x_n]$ the **leading ideal** $L(S)$ of S is defined as the ideal generated by the leading monomials of the elements of S; i.e. $L(S) := (\{\mathrm{lm}(f) \in K[x_1, \ldots, x_n] \mid f \in S\})$.

With these technicalities sorted out, we can now define Gröbner bases.

Definition 2.2.2 *Let I be an ideal of $K[x_1, \ldots, x_n]$ and G a finite subset of I, then G is a **Gröbner Basis** of I with respect to $\leq$, if*

$$L(G) = L(I).$$

From the definition of a Gröbner basis G of I, it is not directly apparent that G generates the ideal I. However, we will later see that this is indeed the case. To prove this and in order to compute Gröbner bases with Buchberger's algorithm; which we will see later; we need the concept of a "normal form", which we will define now.

Definition 2.2.3 *Let $S = \{s_1, \dots, s_r\} \subseteq K[x_1, \dots, x_n]$ be a finite set and $f \in K[x_1, \dots, x_n]$, then*

*(a) f is in **normal form** with respect to S, if no monomial $m \in mon(f)$ of f has a divisor in S.*

*(b) $f^* \in K[x_1, \dots, x_n]$ is a **normal form** of f with respect to S, if f^* is in normal form with respect to S and there are $h_1, \dots, h_r \in K[x_1, \dots, x_n]$ such that*

$$f - f^* = \sum_{i=1}^{r} h_i s_i$$

and $lm(h_i s_i) \leq lm(f)$ for all $i \in [r]$.

From the definition of a normal form f^* of f with respect to S, it follows directly, that $f - f^* \in S$. We will now prove that every monomial ordering is a well ordering on the set of monomials $\mathcal{M} \subseteq K[x_1, \dots, x_n]$; i.e. that any non-empty subset $\mathcal{N} \subseteq \mathcal{M}$ contains a smallest element. Afterwards we will present an algorithm that computes a normal form of a polynomial, which simultaneously shows that a polynomial always possesses a normal form.

Lemma 2.2.4 *Let $\leq$ be a monomial ordering on $K[x_1, \dots, x_n]$ and $\mathcal{M}$ the set of monomials in $K[x_1, \dots, x_n]$, then $\leq$ is a well ordering on $\mathcal{M}$.*

Proof: Let $\mathcal{N} \subseteq \mathcal{M}$ be a non-empty subset, then $(\mathcal{N}) \neq (0)$ is an ideal in $K[x_1, \dots, x_n]$, which is a Noetherian ring and thus $(\mathcal{N})$ is finitely generated. Let $\{n_1, \dots, n_r\} \in \mathcal{N}$ be a generating set of $(\mathcal{N})$ such that $n_1 \leq \dots \leq n_r$, and $n \in \mathcal{N}$ some element, then there are $a_1, \dots, a_r \in K[x_1, \dots, x_n]$ such that $n = \sum_{i=1}^{r} a_i n_i$ and not all a_i are zero, since n is a monomial it must divide some multiple of some n_i, but since in particular $n_1 \leq n_i$ for all $i \in [r]$, we have $n_1 \leq n$ and thus n_1 is smallest element of $\mathcal{N}$. □

Algorithm 2.2.5 (Normal Form) *Let K be a computable field, $S = \{s_1, \dots, s_r\} \subseteq K[x_1, \dots, x_n]$ a finite set, $f \in K[x_1, \dots, x_n]$ and $\leq$ a monomial ordering. Then the following algorithm computes a normal form f^* of f with respect to S:*

```
normalForm(S, f):
(1)  $f^* := f$
(2)  $h_i := 0$ for all $i \in [r]$
(3)  while true
(4)     $M := \{(t, i) \subseteq mon(f^*) \times [r] \mid lm(s_i)$ divides $t\}$
(5)     if $M = \emptyset$
(6)        return $f^*$
(7)     else
(8)     $(t, i) := (t, i) \in M$ such that $t$ is maximal in $mon(f^*)$ with respect to $\leq$
(9)     $c := lc(t)$
(10)    $f^* := f^* - \frac{ct}{lt(s_i)} s_i$
(11)    $h_i := h_i + \frac{ct}{lt(s_i)}$
(12) end
```

Proof: In step (10), since $\text{lt}(s_i)$ divides t, the second term of the right-hand side becomes a polynomial with leading term ct. Since this is the greatest term of f^* with respect to $\leq$ that is divisible by some $\text{lm}(s_i)$, it gets cancelled out. As $\leq$ is a well ordering according to Lemma 2.2.4 and the greatest term of f^* some $\text{lm}(s_i)$ can divide gets smaller every loop, as explained above, the algorithm terminates in a finite amount of steps. By the construction of this algorithm we eliminate all monomials of f^* that are divisible by a leading monomial of some s_i and as a consequence, after terminating, f^* must be in normal form with respect to S. It is easy to see that $f - f^*$ is just the sum of the $\frac{ct}{\text{lt}(s_i)} s_i$ terms of step (10). From this it is clear that the h_i

as defined in the algorithm are precisely the h_i from the definition of a normal form. Moreover the leading monomials of the h_i are all monomials of f^* during different loops divided by $\text{lt}(s_i)$ and since the leading monomial of f is greater or equal to the leading monomial of f^* at any point, the same holds for the $h_i s_i$. This means that f^* is a normal form of f with respect to S. □

Theorem 2.2.6 *Let I be an ideal for $K[x_1, \ldots, x_n]$, $f \in I$ and G a Gröbner basis of I, then there exists precisely one normal form f^* of f with respect to G.*

Proof: With Algorithm 2.2.5 we have already constructively proved that any f has at least one normal form. We will now prove that a normal form with respect to G is also unique.
Let f_1^* and f_2^* be two normal forms of f with respect to G. By definition, G is a subset of I, so $(G) \subseteq I$ and since by definition of the normal form of f, the difference $f - f_i^*$ is contained in (G), we get $f - (f - f_i^*) = f_i^* \in (G) \subseteq I$. Now assume that $f_1^* - f_2^* \neq 0$, since $f_1^* - f_2^* = (f - f_1^*) - (f - f_2^*) \in I$ there exists some $g \in G$ such that $\text{lm}(g)$ divides $\text{lm}(f_1^* - f_2^*)$, but the leading monomial of $f_1^* - f_2^*$ is a monomial of either f_1^* or f_2^*. This is a contradiction to the fact that they are normal forms, thus $f_1^* - f_2^* = 0$, which shows that $f_1^* = f_2^*$. □

Theorem 2.2.7 *Let I be an ideal of $K[x_1, \ldots, x_n]$ and G a Gröbner basis of I, then $(G) = I$.*

Proof: "$\subseteq$": Since G is defined to be a subset of I, this inclusion is trivial.
"$\subseteq$": Let $f \in I$, then we know from Theorem 2.2.6 that f has precisely one normal form f^* with respect to G. We claim that $f^* = 0$.
To prove the claim, assume that $f^* \neq 0$, then by the fact that $f^* \in I$ and that G is a Gröbner basis of I, there is some $g \in G$ such that $\text{lm}(g)$ divides $\text{lm}(f^*)$. But this is a contradiction to f^* being in normal form with respect to G. Thus $f^* = 0$ and therefore $f - f^* = f \in (G)$. □

The following theorem will be very important in proving the correctness of Buchberger's algorithm. However, since the proof is quite lengthy and complicated, we will omit it in this thesis, it can be found in [Kem11] as Theorem 9.12. Furthermore, we will need something called the s**-polynomial** of f and g, where $f, g \in K[x_1, \ldots, x_n]$. It is defined as

$$\text{spol}(f, g) := \frac{\text{lt}(g)}{t} \cdot f - \frac{\text{lt}(f)}{t} \cdot g$$

with $t := \gcd(\text{lm}(f), \text{lm}(g))$. Since, by definition, the greatest common divisor of $\text{lm}(f)$ and $\text{lm}(g)$ divides both $\text{lt}(f)$ and $\text{lt}(g)$, the s-polynomial is, as the name suggests, indeed a polynomial.

Theorem 2.2.8 (Buchberger's criterion) *Let $G \subseteq K[x_1, \ldots, x_n]$ be a finite set with $0 \notin G$, then*

G is a Gröbner basis of (G) ⇔ For all $g, h \in G$, 0 is a normal form of spol(g, h).

Algorithm 2.2.9 (Buchberger's algorithm) *Let K be a computable field, $S \subseteq K[x_1, \ldots, x_n]$ a finite set and $\leq$ a monomial ordering, then the following algorithm computes a Gröbner basis G of (S) with respect to $\leq$:*

```
gröbner(S):
(1) $G := S \setminus \{0\}$
(2) for $g, h \in G$
(3)     $s := spol(g, h)$
(4)     $s^* := normalForm(G, s)$
(5)     if $s^* \neq 0$
(6)         $G := G \cup \{s^*\}$
(7)         go back to (2)
(8)     end (9) return $G$
```

Proof: We see that $L(G)$ increases after every loop and since $K[x_1,\dots,x_n]$ is a Noetherian ring, it satisfies the ascending chain condition; i.e. that for every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots$, there exists an $n \in \mathbb{N}$ such that $I_n = I_m$ for all $m \geq n$. This shows that the algorithm terminates after a finite number of steps. It is also clear that $s^* \in (S)$ for all the s^* defined during the different loops and therefore the equality $(G) = (S)$ is always preserved. With this and since the algorithm only terminates, if for every $g, h \in G$ the normal form of the s-polynomial of g and h is 0, Theorem 2.2.8 tells us that G is a Gröbner basis of $(G) = (S)$ with respect to $\leq$. □

We now know how to compute a Gröbner basis of an ideal. For the purposes of this thesis, we will also need the following two algorithms. First however, we need to introduce a new notion. For this, let $Y = \{y_1,\dots,y_m\} \subseteq \{x_1,\dots,x_n\}$ be a set of variables. We will call $I_Y = I \cap K[y_1,\dots,y_m]$ the **Y-elimination ideal** of I. In the case, where $Y = x_i$ for some i, we will often write $I_Y = I_{x_i}$.

Algorithm 2.2.10 *Let K be a computable field and $Y = \{y_1,\dots,y_m\} \subseteq \{x_1,\dots,x_n\}$ a set of variables. Let S be a finite subset of $K[x_1,\dots,x_n]$, then the following algorithm computes a Gröbner basis of the elimination ideal $I_Y = I \cap K[x_1,\dots,x_n]$:*

```
elim(S, Y):
(1) choose a Y-elimination ordering $\leq_Y$
(2) $G$ := gröbner($S$) with respect to $\leq_Y$
(3) $G_Y := G \cap K[y_1,\dots,y_m]$
(4) return $G_Y$
```

Proof: Let $I := (S)$. We have to prove that G_Y is a Gröbner Basis of $I_Y = I \cap K[y_1,\dots,y_m]$; i.e. that $L(G_Y) = L(I_Y)$.
"$\subseteq$": Since G is by definition a subset of I, the intersection $G \cap K[y_1,\dots,y_m]$ is also a subset of the intersection $I \cap K[y_1,\dots,y_m]$ and therefore clearly $L(G_Y) \subseteq L(I_Y)$.
"$\supseteq$": Let $f \in I_Y$, then in particular f also lies in I. Since G is a Gröbner basis of I, there exists a $g \in G$ such that $\text{lm}(f) = a \cdot \text{lm}(g)$ for some monomial $a \in K[x_1,\dots,x_n]$. But as f is a polynomial in $K[y_1,\dots,y_m]$, its leading monomial is of the form $y_1^{e_1}\cdots y_m^{e_m}$ and therefore $\text{lm}(g)$ must also lie in $K[y_1,\dots,y_m]$. Since we computed G to be a Gröbner basis with respect to a Y-elimination ordering $\leq_Y$, any monomial in $y_1,\dots,y_m$ is less than any monomial in $K[x_1,\dots,x_n]$ that does not contain any of the y_k. It follows that the leading monomial of g can only be a monomial in $y_1,\dots,y_m$ if all other monomials of g also only contain the variables $y_1,\dots,y_m$. So $g \in K[y_1,\dots,y_m]$, which means that $g \in G \cap K[y_1,\dots,y_m] = G_Y$. Since the a from above must also lie in $K[y_1,\dots,y_m]$, we can conclude that $\text{lm}(f) = a \cdot \text{lm}(g) \in G_Y$, which proves that G_Y is a Gröbner basis of I_Y. □

Algorithm 2.2.11 *Let K be a computable field and $t_1,\dots,t_r$ distinct variables from $x_1,\dots,x_n$. Let $S_1,\dots S_r$ be finite subsets of $K[x_1,\dots,x_n]$, then the following algorithm computes a Gröbner basis of the intersection of the ideals generated by $S_1,\dots,S_r$:*

```
int($S_1,\dots,S_r$):
(1) $G$ := elim($\{1-\sum_{k=1}^r t_k\} \cup \bigcup_{k=1}^r t_kS_k, \{x_1,\dots,x_n\}$) in $K[x_1,\dots,x_n,t_1,\dots,t_r]$
(2) return $G$
```

Proof: Let $J = (1-\sum_{k=1}^r t_k \cup \bigcup_{k=1}^r t_kS_k)$. In order to prove the correctness of the algorithm, we have to show that the elimination ideal $J_X := J \cap K[x_1,\dots,x_n]$ is equal to the intersection of the ideals generated by the S_k. That is to say, that $\bigcap_{k=1}^r (S_k) = J_X$.
"$\subseteq$": Let $f \in \bigcap_{k=1}^r (S_k) \subseteq K[x_1,\dots,x_n]$, then clearly $1-\sum_{k=1}^r t_k + \sum_{k=1}^r t_kf \in J$ and we can see that

$$f \cdot (1-\sum_{k=1}^r t_k + \sum_{k=1}^r t_kf) = f - f \cdot \sum_{k=1}^r t_k + \sum_{k=1}^r t_kf = f.$$

Thus f is in J and since obviously $f \in K[x_1, \ldots, x_n]$, we have $f \in J_X$.
"$\supseteq$": Now let $f \in J_X$. Since this means that $f \in J$, we can write

$$f = a \cdot (1 - \sum_{k=1}^{r} t_k) + \sum_{k=1}^{r} \sum_{i=1}^{n_k} a_{k,i} t_k s_{k,i}$$

with $a, a_{k,i} \in K[x_1, \ldots, x_n, t_1, \ldots, t_r]$, $n_k = |S_k|$ and $s_{k,i} \in S_k$ for $k \in [r]$ and $i \in [n_k]$. We can now choose some $j \in [r]$ and set $t_j = 1$ and $t_l = 0$ for $l \neq j$. Since $f \in J_X$ implies that $f \in K[x_1, \ldots, x_n]$ we get

$$f = a \cdot (1 - 1) + \sum_{i=1}^{n_j} b_{j,i} s_{j,i} = \sum_{i=1}^{n_j} b_{j,i} s_{j,i}$$

with $b_{j,i}$ being $a_{j,i}$ where the t_k got substituted for 1 and 0 like above. It follows that f is an element of the ideal generated by S_j and since we can do this for every $j \in [r]$, we get $f \in \bigcap_{k=1}^{r} (S_k)$.

With this we have proved that G is a Gröbner basis of $J_X = \bigcap_{k=1}^{r} (S_k)$ and therefore the algorithm runs correctly. □

3 Zero-dimensional Ideals

As the title may suggest, our goal in this chapter will be to develop an algorithm that computes the radical of a zero-dimensional ideal. Later we will use this to compute the radical of an ideal of arbitrary dimension. First of all, we will have to define what we mean by "zero-dimensional" and dimension of an ideal in general. Recall that for an ideal I of $K[x_1, \dots, x_n]$ and a subset $Y = \{y_1, \dots, y_m\} \subseteq \{x_1, \dots, x_n\}$ of the variables, I_Y denotes the Y-elimination ideal $I \cap K[y_1, \dots, y_m]$.

Definition 3.0.1 (Dimension of an Ideal) *Let I be a proper ideal of the polynomial ring $K[x_1, \dots, x_n]$ over a field K, then*

$$\dim(I) := \max\{|Y| \mid Y \subseteq \{x_1, \dots, x_n\} : I_Y = \{0\}\}.$$

Naturally, an ideal I with $dim(I) = 0$ will be called zero-dimensional.

From the definition it is apparent that an ideal I is zero-dimensional if and only if it contains a non-constant univariate polynomial in every variable $x_i \in \{x_1, \dots, x_n\}$, since if I fulfills that condition, I_{x_i} and thus also I_Y for all $\emptyset \neq Y \subseteq \{x_1, \dots, x_n\}$ contains at least one of those polynomials and if there is some variable x_i in which I has no univariate polynomial, then $I_{x_i} = \{0\}$ and therefore $\dim(I) \geq 1$.

In the following section, we will look at ideals I of univariate polynomial rings and try to compute generators for I. With what we've just seen, we know that if an ideal I of $K[x_1, \dots, x_n]$ is zero-dimensional, a generator of I_{x_i} would always be non-zero. And as we will see in Section 3.3, having a non-zero element of I_{x_i} will be very helpful in computing the radical of I.

3.1 Monic Generators of Ideals

We mentioned in the beginning of Chapter 2 that for a field K, its univariate polynomial ring $K[x]$ is a Euclidean domain. A suitable Euclidean function would be the map $\varphi : K[x] \to \mathbb{N}$, that assigns to every non-zero polynomial one more than its degree and zero to the constant zero polynomial. This means that for any $f, g \in K[x]$ with $g \neq 0$, there exist $h, r \in K[x]$ such that $f = h \cdot g + r$ and $\varphi(r) < \varphi(g)$ holds. This has an important result as a consequence.

Lemma 3.1.1 *Let $I \neq (0)$ be an ideal of $K[x]$, then any non-zero element of I of minimal degree generates I.*

Proof: Let φ be the Euclidean function of $K[x]$ as defined in the beginning of this section and set $D := \{\varphi(f) - 1 \in \mathbb{N} \mid f \in I \backslash \{0\}$. Then D is clearly non-empty and a subset of $\mathbb{N}$, hence there is a smallest element of D. Let $d := \min D$ and $g \in I$ such that $\varphi(g) = d$. We now claim that $I = (g)$.
"$\supseteq$": This is clear, as $g \in I$.
"$\subseteq$": Let $f \in I$. Since $K[x]$ is Euclidean and g is non-zero, there exist $h, r \in K[x]$ such that $f = h \cdot g + r$ and $\varphi(r) < \varphi(g)$. But $r = f - h \cdot g \in I$, which means that $r = 0$ as $\varphi(g)$ is minimal among non-zero polynomial in I, thus $f = h \cdot g \in (g)$. □

It is easy to see that the previous lemma actually holds for any Euclidean domain, when we replace the word "degree" with "Euclidean function value". For any ideal I of $K[x]$ we now have a class of elements, that are similar in the fact, that each element generates I and has the same polynomial degree. As it turns out however, if we fix any coefficient, there is precisely one polynomial with minimal degree that generates I.

Lemma 3.1.2 *Let $I \neq (0)$ be an ideal of $K[x]$, then I has a unique monic polynomial f with minimal degree such that $(f) = I$.*

Proof: Let $f, g \in I$ be two generators of minimal degree of I with leading coefficient 1. Since this means that $f \in (g)$ and $g \in (f)$, there are $r, s \in K[x]$ such that $f = r \cdot g$ and $g = s \cdot f$. Substituting the f in the second equation for the right-hand side of the first equation we get $f = r \cdot s \cdot f$ and therefore $r \cdot s = 1$. This means that r and s are units and therefore constants. But the only only constant r, that satisfies $f = r \cdot g$ and for which f and g retain the same leading coefficient, is $r = 1$. Therefore $f = g$, which shows that f is unique. □

We will call the polynomial f from the previous lemma the **monic generator** of I. In Algorithm 3.3.5 we are given a finite set $S \subseteq K[x_1, \ldots, x_n]$ such that $I = (S)$ is a zero-dimensional ideal of $K[x_1, \ldots, x_n]$. Our goal then is to compute the monic generator of $I_{x_i} = I \cap K[x_i]$ or $i \in [n]$. Since for a zero-dimensional ideal I the $\{x_i\}$-elimination ideal I_{x_i} is by definition not the zero ideal, we can gather from our previous results, that I_{x_i} does indeed have a monic generator. Given S, we will now show how to compute it.

Algorithm 3.1.3 (Monic generator) *Let K be a computable field and $S \subseteq K[x_1, \ldots, x_n]$ a finite set such that $I = (S)$ is a zero-dimensional ideal of $K[x_1, \ldots, x_n]$. Let $x \in \{x_1, \ldots, x_n\}$ be a variable and $\leq_x$ an $\{x\}$-elimination ordering on $K[x_1, \ldots, x_n]$. Then the following algorithm computes the monic generator of the $\{x\}$-elimination ideal I_x:*

```
monicGen$(S, x)$:
(1) $G :=$ elim$(S, \{x\})$
(2) $f \in G$ such that $f \neq 0$ and deg$(f)$ is minimal among non-zero elements of $G$
(3) $f := \frac{f}{lc(f)}$
(4) return $f$
```

Proof: We know how to compute Gröbner bases of elimination ideals and Gröbner bases are by definition finite. As this means, we can easily compute the degree of all elements of G and choose the one with the smallest degree, the correctness of the algorithm follows directly from our previous two lemmas. □

3.2 Squarefree Parts

As was noted in the beginning of Chapter 2, if K is a field $K[x_1, \ldots, x_n]$ is factorial, which means that for any $f \in K[x_1, \ldots, x_n]$, there are irreducible elements $p_1, \ldots, p_m \in K[x_1, \ldots, x_n]$ such that $f = p_1 \cdots p_m$. However, in many cases, some p_i will be associated with some p_j, but we can simply group these together and find some unit $u \in K[x_1, \ldots, x_n]$ such that $f = up_{i_1}^{e_1} \cdots p_{i_r}^{e_r}$ where $p_{i_1}, \ldots, p_{i_r}$ are the pairwise non-associated irreducible factors of f. We will call this representation of f its **irreducible decomposition**.

The idea of a squarefree decomposition is to not group the associated irreducible elements together, but to look at $p_{i_1}, \ldots, p_{i_r}$, and group those together, that have the same exponent, a **squarefree decomposition** would therefore look like $f = ug_1^1 \cdots g_s^s$, where g_i are the products of the pairwise non-associated irreducibles that have the same exponent i in their irreducible decomposition of f. This decomposition is "squarefree" in the sense, that every g_i is **squarefree**, which in turn means that for every element $p \in K[x_1, \ldots, x_n]$, its square p^2 doesn't divide g_i. For the purpose of the algorithm we're trying to develop, we will only need $ug_1 \cdots g_s$, which we will call the **squarefree part** of f. Our goal in this section is therefore to develop an algorithm, that computes the squarefree part of a polynomial $f \in K[x]$. Since the g_i are products or irreducibles that have no associated elements in any other g_j, we find that $g_1, \ldots, g_m$ are pairwise co-prime and squarefree, which clearly makes the squarefree part itself squarefree.

As it turns out however, the computations will have to be quite different depending on the characteristic of our field K. In [BW93] the authors only show algorithms for the squarefree decomposition of $f \in K[x]$, in the cases char$(K) = 0$ and char$(K) = p > 0$ with K being finite. However, there are also algorithms for the case where K is an arbitrary perfect field with characteristic $p > 0$; we will mostly follow [GT96] for that case. Since char$(K) = 0$ implies that K is perfect, we can develop an algorithm that computes the squarefree part of a polynomial in $K[x]$ over any perfect field K.

Since it will be quite useful in this section, we recall that for a polynomial $f \in K[x]$ with $f = \sum_{k=0}^{n} a_k x^k$, the **formal derivative** f' is defined to be $f' = \sum_{k=1}^{n} k a_k x^{k-1}$. We will now prove the standard rules for the formal derivative, as well as some other results, related to the formal derivative.

Lemma 3.2.1 *Let $a \in K$, $f, g \in K[x]$, with $f(g)$ and $f'(g)$ being the evaluation of f and f' at g, then the following hold:*

(a) $(a \cdot f)' = a \cdot f'$.

(b) $(f + g)' = f' + g'$.

(c) $(f \cdot g)' = f' \cdot g + f \cdot g'$.

(d) $(f^r)' = r f^{r-1} f'$ *for* $r \in \mathbb{N}$.

(e) $(f(g))' = f'(g) \cdot g'$.

Proof: We will write $f = \sum_{k=0}^{n} a_k x^k$ and $g = \sum_{j=0}^{m} b_j x^j$ and assume without loss of generality, that $n \geq m$, as the order of f and g does not matter, when the degree does. We will further set $a_k = b_j = 0$ for $k \notin \{0, \dots, n\}, j \notin \{0, \dots, m\}$.
(a): $(a \cdot f)' = (a \cdot \sum_{k=0}^{n} a_k x^k)' = (\sum_{k=0}^{n} a a_k x^k)' = \sum_{k=1}^{n} k a a_k x^{k-1} = a \cdot \sum_{k=0}^{n} k a_k x^{k-1} = a \cdot f'$.
(b): Since $f + g = \sum_{k=0}^{n} a_k x^k + \sum_{j=0}^{m} b_j x^j = \sum_{k=0}^{n} (a_k + b_k) x^k$, as it was assumed that $n \geq m$, and likewise $f' + g' = \sum_{k=1}^{n} k a_k x^{k-1} + \sum_{j=1}^{m} j b_j x^{j-1} = \sum_{k=1}^{n} k(a_k + b_k) x^{k-1}$ it follows that

$$(f+g)' = (\sum_{k=0}^{n} (a_k + b_k) x^k)' = \sum_{k=1}^{n} k(a_k + b_k) x^{k-1} = f' + g'.$$

(c): We will first prove the case where $g = x^m$ for some $m \geq 1$; i.e. that $(f \cdot x^m)' = f' \cdot x^m + f \cdot m x^{m-1}$. In particular, it is clear that $(f \cdot x^0)' = f'$.
By setting $j := k + m$ we get $f \cdot x^m = \sum_{k=0}^{n} a_k x^{k+m} = \sum_{j=m}^{n+m} a_{j-m} x^j$. Since $a_k = 0$ for $k \notin \{0, \dots, n\}$ we can write the last sum as $\sum_{j=0}^{n+m} a_{j-m} x^j$, with this we get $(f \cdot x^m)' = \sum_{j=1}^{n+m} j a_{j-m} x^{j-1}$ which is again the same as $\sum_{j=m}^{n+m} j a_{j-m} x^{j-1}$. By another index shift we get

$$\sum_{k=0}^{n} (k+m) a_k x^{k+m-1} = (\sum_{k=1}^{n} k a_k x^{k-1}) \cdot x^m + (\sum_{k=0}^{n} a_k x^k) \cdot m x^{m-1} = f' \cdot x^m + f \cdot m x^{m-1}.$$

Now $f \cdot g = f \cdot \sum_{j=0}^{m} b_j x^j = \sum_{j=0}^{m} b_j f x^j$, with what we proved so far and by the linearity of the formal derivative, which we showed with (a) and (b), we get

$$(f \cdot g)' = \sum_{j=0}^{m} b_j (f x^j)' = \sum_{j=0}^{m} b_j (f' \cdot x^j + f \cdot j x^{j-1}) = f' \cdot \sum_{j=0}^{m} b_j x^j + f \cdot \sum_{j=1}^{m} b_j j x^{j-1} = f' \cdot g + f \cdot g'.$$

(d): We will proof this part by induction on r:
$r = 0$: $(f^0)' = 1' = 0 = 0 \cdot f^{-1} \cdot f'$.
$r \rightsquigarrow r+1$: By part (c) of this lemma, $(f^{n+1})' = (f^n \cdot f)' = (f^r)' \cdot f + f^r \cdot f'$. Then by our induction hypothesis $(f^r)' \cdot f + f^r \cdot f' = r f^{r-1} f' \cdot f + f^r \cdot f' = (r f^r + f^r) f' = (r+1) f^r f'$ and thus $(f^{r+1})' = (r+1) f^r f'$.
(e): Using linearity, part (d) and the fact that derivatives of constants, like $g^0 = 1$ are zero, we get

$$(f(g))' = (\sum_{k=0}^{n} a_k g^k)' = \sum_{k=1}^{n} a_k k g^{k-1} g' = (\sum_{k=1}^{n} k a_k g^{k-1}) g' = f'(g) \cdot g'.$$

□

Theorem 3.2.2 *Let $f \in K[x]$ and let f' be the formal derivative of f, then the following hold:*

(a) If $char(K) = 0$, then $f' = 0$ if and only if f is constant.

(b) If $char(K) = p > 0$, then $f' = 0$ if and only if there exists some $g \in K[x]$ such that $f = g(x^p)$.

(c) If K is perfect and $char(K) = p > 0$, then $f' = 0$ if and only if there exists some $g \in K[x]$ such that $f = g^p$.

Proof: (a): "$\Rightarrow$": As before, we write the formal derivative of $f = \sum_{k=0}^{n} a_k x^k$ as $f' = \sum_{k=1}^{n} k a_k x^{k-1}$. Since we are in characteristic 0, the formal derivative f' being equal to 0 implies that $a_k = 0$ for all $k \in [n]$. As $f = \sum_{k=0}^{n} a_k x^k$, this means that f is equal to $a_0 x^0 = a_0$ and is therefore constant.
"$\Leftarrow$": If f is constant, $f = \sum_{k=0}^{0} a_k x^k$ and therefore $f' = \sum_{k=1}^{0} a_k x^k = 0$.
(b): "$\Rightarrow$": Since we are now in characteristic $p > 0$ and $f' = \sum_{j=1}^{m} k a_j x^k$ all terms where $k \mid p$ are zero, which means that $f' = 0$ merely implies that $a_k = 0$ for every $k \in [n]$ with $p \nmid k$. Consequently we can write $f = \sum_{k=0}^{m} a_{k \cdot p} x^{k \cdot p} = \sum_{k=0}^{m} a_{k \cdot p} (x^p)^k$ with $m = \lfloor \frac{n}{p} \rfloor$. Hence $g := \sum_{k=0}^{m} a_{k \cdot p} (x)^k$ fulfills $f = g(x^p)$.
"$\Leftarrow$": Let $f = g(x^p)$, then $f = \sum_{j=0}^{m} b_j (x^p)^j = \sum_{j=1}^{m} b_j x^{p \cdot j}$ and therefore $f' = \sum_{j=1}^{m} (p \cdot j) b_j x^{p+j}$. This means that every term of f' is a multiple of p and thus $f' = 0$.
(c): "$\Rightarrow$": From (b) we know there exists a polynomial $h \in K[x]$ such that $f = h(x^p)$, we write $h = \sum_{j=0}^{m} b_j x^j$. Since K is perfect, there is an element $c_j \in K$ such that $c_j^p = b_j$ for all $j \in [m]$, thus $f = \sum_{j=1}^{m} c_j^p (x^j)^p = \sum_{j=1}^{m} (c_j x^j)^p = (\sum_{j=1}^{m} c_j x^j)^p$. The last step works, because of what some authors call "freshman's dream", which is simply the fact that in characteristic p, the equation $(a+b)^p = a^p + b^p$ holds. It is easy to see that from this, that $(\sum_{k=1}^{n} a_i)^p = \sum_{k=1}^{n} a_i^p$ and therefore $g := \sum_{j=1}^{m} c_j x^j$ is the wanted polynomial.
"$\Leftarrow$": If $f = g^p$, then by Lemma 3.2.1(d), the formal derivative is $f' = (g^p)' = p g^{p-1} g'$, which is a multiple of p and therefore equal to 0. □

As we will make use of the concept of separable polynomials; i.e. polynomials $f \in K[x]$ that have distinct roots over the algebraic closure of K; we will take a look at a useful characterization of separability, as well as a connection between being separable and being squarefree.

Theorem 3.2.3 *Let $f \in K[x]$ and let f' be the formal derivative of f, then the following hold:*

(a) f is separable if and only if $gcd(f, f') = 1$.

(b) If f is separable, then f is squarefree.

(c) If K is perfect and f squarefree, then f is separable.

Proof: (a): "$\Rightarrow$": Since f is separable, it can be written as $f = u \prod_{i=1}^{n} (x - a_i)$ with $n = \deg(f)$, a unit $u \in K[x]$ and distinct elements $a_1, \ldots, a_n \in \overline{K}$ of the algebraic closure of K. Then $f' = \prod_{i=1}^{n-1} (x - b_i)$ with $b_i \in \overline{K}$ and $a_i \neq b_j$ for all $i \in [n], j \in [n-1]$, since if $a_i = b_j$, then f has a root of multiplicity at least 2. And because greatest common divisors over field extension of K are the same as over K, we get $gcd(f, f') = 1$.
"$\Leftarrow$": According to Bézout's lemma there exist polynomials $g, h \in K[x]$ such that $gcd(f, f') = g \cdot f + h \cdot f'$. Now let $a \in \overline{K}$ be a root of f, then $1 = h(a) \cdot f(a) + g(a) \cdot f'(a) = g(a) \cdot f'(a)$. This shows that $f'(a)$ can't be zero, which means a is a distinct root of f. As a was arbitrary, this makes f separable.
(b): Assume f is separable and not squarefree. Then there exists a non-constant polynomial $g \in K[x]$ such that $g^2 \mid f$. Since g is non-constant, it has at least one root in $\overline{K}$, which means that f has the same root with multiplicity at least 2, which is a contradiction to the fact that f is separable. Therefore f has to be squarefree.
(c): In the case where f is constant, the claim is trivial. Now let $f \in K[x]$ be a non-constant squarefree polynomial. Then it can then be written as $f = p_1 \cdots p_m$, where $p_1, \ldots, p_m \in K[x]$ are pairwise non-associated and irreducible. Let $a \in \overline{K}$ be an element of the algebraic closure of K and assume for a contradiction, that

$(x-a)^2 \mid f$. Then $(x-a) \mid p_i$ for some $i \in [m]$, because $(x-a)$ is irreducible. But since $gcd(p_i, p_j) = 1$ in $K[x]$ for $j \neq i$ and therefore also in $\overline{K}[x]$, no p_j with $j \neq i$ can be divisible by $(x-a)$ and therefore $(x-a)^2 \mid p_i$. As K was assumed to be perfect, p_i being irreducible means it is also separable, but that is a contradiction to $(x-a)^2 \mid p_i$ and therefore f must be separable as well. □

Lemma 3.2.4 *Let K be a perfect field, char$(K) = p > 0$ and $f \in K[x]$. Then there exists a polynomial $h \in K[x]$ and separable polynomials $g_1, \ldots, g_m \in K[x]$ such that $f = h \cdot g_1^1 \cdots g_m^m$ with $h' = 0$, $h, g_1, \ldots, g_m$ pairwise co-prime and if $k \mid p$ then $g_k = 1$.*

Proof: Since $K[x]$ is a factorial ring, we can write $f = q_1^{e_1} \cdots q_r^{e_r}$ with $q_1, \ldots, q_r \in K[x]$ being pairwise non-associated irreducible elements. We define $G_i := \{j \in [r] \mid e_j = i \text{ and } p \nmid e_j \text{ and } q_j' \neq 0\}$ and $H := \{j \in [r] \mid q_j' = 0 \text{ or } p \mid e_j\}$, then $g_i := \prod_{j \in G_i} q_j$ and $h := \prod_{i \in H} q_i^{e_i}$ satisfy the claims. The G_i are clearly pairwise disjoint, and since $j \in G_i$ implies $p \nmid e_j$ and $q_j' \neq 0$, the union $\bigcup_{i \in \mathbb{N}} G_i$ and H are also disjoint. Moreover, the $j \in [r]$, that are not contained in any G_i must satisfy either $p \mid e_j$ or $q_j' = 0$, because the e_j are positive integers. From this it follows that $\bigcup_{i \in \mathbb{N}} G_i \cup H$ is a disjoint union of $[r]$ and from the definition of G_i we can see that $f = hg_1g_2^2 \cdots g_m^m$.
By inductively using the product rule from Lemma 3.2.1(c) we get

$$h' = \sum_{j \in H} (q_j^{e_j})' \prod_{\substack{i \in H \\ i \neq j}} q_i^{e_i}.$$

Since by Lemma 3.2.1(d), we have $(q_j^{e_j})' = e_j q_j^{e_j - 1} q_j'$ and for $j \in H$, we get $q_j' = 0$ or $p \mid e_j$, this means that $(q_j^{e_j})' = 0$. With that we can conclude that $h' = 0$.
Since $q_1, \ldots, q_r$ are pairwise non-associated, it is easy to see that $g_1, \ldots, g_m, h$ are pairwise co-prime. And by definition of G_k, if $p \mid k$ then $G_i = \emptyset$ and so $g_k = 1$.
Lastly, as the g_k are products of pairwise non-associated irreducible polynomials they are squarefree and by Theorem 3.2.3(c) also separable. □

Lemma 3.2.5 *Let char$(K) = 0$ and $f, q \in K[x]$ with q being irreducible such that $q^k \mid f$ but $q^{k+1} \nmid f$ for some $k \in \mathbb{N}_{>0}$. Then*

$$q^{k-1} \mid f' \text{ but } q^k \nmid f'.$$

Proof: From $q^k \mid f$ it follows that there is some non-zero $g \in K[x]$ such that $f = gq^k$. And since $q^{k+1} \nmid f$, we conclude that $q \nmid g$. By Lemma 3.2.1(c) and (d) we get

$$f' = (gq^k)' = g' \cdot q^k + g \cdot (q^k)' = g' \cdot q^k + g \cdot kq^{k-1}q' = q^{k-1}(g'q + gkq')$$

and thus q^{k-1} doesn't divide f'. It is clear that for an irreducible element q the formal derivative q' has a smaller degree than q itself. With this, and since g is a prime element with $q \nmid g$, we can deduce that q doesn't divide gkq' and therefore also not $g'q + gkq'$. From this it follows that $q^k \nmid f'$. □

Theorem 3.2.6 *Let K be a field and $f \in K[x]$ a non-constant polynomial, then the following hold:*

(a) If char$(K) = 0$ and $f = ug_1g_2^2 \cdots g_m^m$ is the squarefree decomposition of f, then

$$gcd(f, f') = g_2g_3^2 \cdots g_m^{m-1}.$$

(b) If K is perfect, char$(K) = p > 0$ and $f = hg_1g_2^2 \cdots g_m^m$ as in Lemma 3.2.4, then

$$gcd(f, f') = hg_2g_3^2 \cdots g_m^{m-1}.$$

Proof: (a): Since the factors g_k of the squarefree decomposition of f are products of pairwise non-associated irreducible elements and the g_k share no common factors, Lemma 3.2.5 shows that $g_k^{k-1} \mid f'$, but $g_k^k \nmid f'$. As f has no other divisors, beside the g_k, it follows that $\gcd(f, f') = g_2 g_3^2 \cdots g_m^{m-1}$.
(b): As in the proof of the Lemma 3.2.4, by inductively using the product rule for formal derivatives, we get

$$f' = h' \cdot \prod_{k=1}^{m} g_k^k + h \sum_{j=1}^{m} (g_j^j)' \prod_{\substack{i=1 \\ i \neq j}}^{m} g_i^i.$$

Furthermore by Lemma 3.2.1(d), we have $(g_j^j)' = j g_j^{j-1} g_j'$ and because $h' = 0$ by Lemma 3.2.4, it follows that

$$f' = h \sum_{j=1}^{m} j g_j^{j-1} g_j' \prod_{\substack{i=1 \\ i \neq j}}^{m} g_i^i = h \prod_{i=1}^{m} g_i^{i-1} \Big(\sum_{j=1}^{m} j g_j' \prod_{\substack{i=1 \\ i \neq j}}^{m} g_i \Big).$$

From this, we know that $h g_2 g_3^2 \cdots g_m^{m-1}$ divides f', but as clearly no other g_k divides the sum in the last equation, we can conclude that $\gcd(f, f') = h g_2 g_3^2 \cdots g_m^{m-1}$. □

Algorithm 3.2.7 (Squarefree part) *Let K be a perfect and computable field with $\mathrm{char}(K) = p$ and $f \in K[x]$ a non-constant polynomial, then the following algorithm computes the squarefree part of f:*

```
sqfrPart($f$):
(1) $d := gcd(f, f')$
(2) $f := \frac{f}{d}$
(3) if $p = 0$
(4)     return $f$
(5) else
(6) $b := f$
(7) $c := d$
(8) while $b \neq 1$
(9)     $b := \gcd(c, b)$
(10)    $c := \frac{c}{b}$
(11) end
(12) if $c$ is constant
(13)    return $f$
(14) else
(15) $g := \sqrt[p]{c}$
(16) $f :=$ sqfrPart($g$) $\cdot \frac{f}{c}$
(17) return $f$
```

Proof: If $\mathrm{char}(K) = p = 0$, we can see with Theorem 3.2.6(a) that after step (2), we get $f = u g_1 g_2 \cdots g_m$ and the algorithm therefore terminates with the correct result.
If $\mathrm{char}(K) = p > 0$, we see with Theorem 3.2.6(b) that in the same step $f = h g_1 g_2 \cdots g_m$ with $g_1 g_2 \cdots g_m$ being squarefree and $h' = 0$. By Theorem 3.2.2(c) this means that there is a $g \in K[x]$ such that $h = g^p$. In steps (6) to (11) we compute said h, since during the i-th loop and after step (9), $b = g_{i+1} \dots g_m$ and $c = h g_{i+1} g_{i+2}^2 \cdots g_m^{m-i}$. Therefore b being equal to 1 means that $c = h$. If we write $f = \sum_{k=0}^{n} a_k x^k$, we can get $g = \sqrt[p]{h}$ by using the trick used in the proof of Theorem 3.2.2; i.e. set

$$g = \sum_{k=0}^{\lfloor \frac{n}{p} \rfloor} \sqrt[p]{a_{k \cdot p}} x^k$$

and because K was assumed to be perfect with $\mathrm{char}(K) = p > 0$ every element $a_{k \cdot p} \in K$ is a p-th power. We then go on to recursively compute the squarefree part of g and since f has only finitely many irreducible factors h will be constant after some recursive step and thus at last the algorithm will terminate. □

3.3 Computing the Radical of a Zero-dimensional Ideal

At the beginning of this chapter, we mentioned that a proper ideal I of $K[x_1, \dots, x_n]$ is zero-dimensional if and only if it has a non-constant univariate polynomial in every variable $x_i \in \{x_1, \dots, x_n\}$. If I is a radical ideal, it follows directly from the following lemma that it even contains a squarefree univariate polynomial in each variable. If K is a perfect field, the reverse implication does in fact also hold. This result, called "Seidenberg's lemma" in [BW93], will be a fundamental step for the algorithm.

Lemma 3.3.1 *Let K be a field and I, J ideals of the polynomial ring $K[x_1, \dots, x_n]$, then the following hold:*

(a) If $0 \neq f \in I$, then the squarefree part of f is in $\sqrt{I}$.

(b) If $I \subseteq J \subseteq \sqrt{I}$, then $\sqrt{I} = \sqrt{J}$.

Proof: (a): Let $f = ug_1g_2^2 \cdots g_m^m$ be the squarefree decomposition of f. Since I is, as an ideal, closed under scalar multiplication and $u^{m-1}g_1^{m-1}g_2^{m-2} \cdots g_m^0 \in K[x_1, \dots, x_n]$ it follows that

$$u^{m-1}g_1^{m-1}g_2^{m-2} \cdots g_m^0 \cdot ug_1g_2^2 \cdots g_m^m = u^m g_1^m g_2^m \cdots g_m^m = (ug_1g_2 \cdots g_m)^m \in I$$

and therefore $ug_1g_2 \cdots g_m \in \sqrt{I}$.
(b): "$\subseteq$": Let $g \in \sqrt{I}$ then there exists some $r \in \mathbb{N}$ such that $g^r \in I$. Since $I \subseteq J$ it also holds that $g^r \in J$ and thus $g \in \sqrt{J}$.
"$\supseteq$": Now let $h \in \sqrt{J}$. It follows again that $h^s \in J \subseteq \sqrt{I}$ for some $s \in \mathbb{N}$, but since we know that $\sqrt{I}$ is already a radical ideal, h itself already has to be contained in $\sqrt{I}$. □

Lemma 3.3.2 *Let I be an ideal of $K[x_1, \dots, x_n]$ and $f = p_1 \cdots p_m \in K[x_1]$ with $p_1, \dots, p_m \in K[x_1]$ being pairwise co-prime, then*

$$(I, f) = \bigcap_{i=1}^{m} (I, p_i)$$

and in particular

$$(f) = \bigcap_{i=1}^{m} (p_i).$$

Proof: "$\subseteq$": Since (f) is clearly contained in every (p_i), the ideal (I, f) is also contained in (I, p_i) for every $i \in [m]$ and therefore $(I, f) \subseteq \bigcap_{i=1}^{m}(I, p_i)$.
"$\supseteq$": Now let $g \in \bigcap_{i=1}^{m}(I, p_i)$. Then for every $i \in [m]$ we can write $g = a_i + r_i \cdot p_i$ with $a_i \in I, r_i \in K[x_1, \dots, x_n]$. Now let $h_i = p_1 \cdots p_{i-1}p_{i+1} \cdots p_m$, then $g \cdot h_i = a_i \cdot h_i + r_i \cdot f \in (I, f)$. Since the $p_1, \dots, p_m$ are pairwise co-prime, we get $gcd(h_1, \dots, h_m) = 1$ and therefore Bézout's lemma says that there are $u_i \in K[x_1]$ such that $g = g \cdot gcd(h_1, \dots, h_m) = g \sum_{i=1}^{m} u_i h_i = \sum_{i=1}^{m} u_i g h_i \in (I, f)$.
For the second part, let $I = (0)$. Then by applying the part above, we get

$$(f) = (I, f) = \bigcap_{i=1}^{m}(I, p_i) = \bigcap_{i=1}^{m}(p_i).$$

which concludes the proof. □

Theorem 3.3.3 (Seidenberg's lemma) *Let I be a zero-dimensional ideal of $K[x_1, \dots, x_n]$. If there exist separable polynomials $f_i \in I \cap K[x_i]$ for all $i \in [n]$, then I is a radical ideal.*

Proof: First, we will prove by induction on the number of variables that I is the intersection of finitely many maximal ideals. We will start by proving the case where $n = 1$.
"$n = 1$": We know that $K[x_1]$ is a principal ideal domain and therefore I is generated by a single $g \in K[x_1]$. Since by our condition I contains a separable, and by Theorem 3.2.3(b), squarefree polynomial, the generator g has to be squarefree as well, as otherwise every other element of I wouldn't be squarefree either. We can thus write $g = p_1 \cdots p_{m_1}$ with $p_1, \dots, p_{m_1} \in K[x_1]$ being pairwise non-associated irreducibles. Since $p_1, \dots p_{m_1}$ are non-associated they are co-prime and we can apply Lemma 3.3.2, which gives us

$$I = (g) = \bigcap_{i=1}^{m_1} (p_i).$$

Since $K[x_1]$ is a principal ideal domain and p_i is irreducible for $i \in [m_1]$, the ideal generated by p_i is a maximal ideal, which proves the claim for $n = 1$.
"$n - 1 \rightsquigarrow n$": Let $f_1 \in I \cap K[x_1]$ be the separable polynomial from our condition. Then like above, we get $f_1 = p_1 \cdots p_{m_2}$ with $p_1, \dots, p_{m_2} \in K[x_1]$ being pairwise non-associated irreducible polynomials. We apply the first part of Lemma 3.3.2 and get

$$I = (I, f_1) = \bigcap_{i=1}^{m_2} (I, p_i). \tag{3.1}$$

We now claim that for an irreducible element $p \in K[x_1]$, the ideal (I, p) is the intersection of finitely many maximal ideals.

To prove this claim, let $p \in K[x_1]$ be irreducible. Since $K[x_1]$ is a principal ideal domain, (p) is a maximal ideal and thus $K[x_1]/(p) =: L$ is a field. Now let

$$\varphi : K[x_1, \dots, x_n] \to L[x_2, \dots, x_n],\ x_1 \mapsto x_1 + (p),\ x_k \mapsto x_k \quad \forall k \geq 2.$$

As (p) is a proper ideal, the only constant polynomial it contains is the zero polynomial. We can therefore conclude that the homomorphism $K \to K[x_1]/(p), a \mapsto a + (p)$ is injective and L can be viewed as a field extension of K. From this fact it follows that $\varphi|_K = id_K$ and furthermore $\varphi|_{K[x_2,\dots,x_n]} = id_{K[x_2,\dots,x_n]}$. As a result $\varphi(f_i) = f_i$ for each of the separable polynomials $f_2, \dots, f_n$ from our assumption, as they are elements of $K[x_2, \dots, x_n] \subseteq L[x_2, \dots, x_n]$.

Since we can also view the f_i as elements of the univariate polynomial rings $K[x_i]$ and because the greatest common divisors over $K/(p)[x_i]$ are the same as over $K[x_i]$, we get $gcd(\varphi(f_i), \varphi(f_i)') = gcd(f_i, f_i') = 1$. Because φ is a surjective ring homomorphism, we can now see, that $J := \varphi((I, p)) = \varphi(I) \trianglelefteq L[x_2, \dots, x_n]$ is a zero-dimensional ideal of a polynomial ring over a field L in $n - 1$ variables and with a separable polynomial $f_i \in J \cap L[x_i]$ for $i \in \{2, \dots, n\}$. This means we can apply the induction hypothesis and get

$$J = \bigcap_{i=1}^{m_3} \mathfrak{n}_i$$

with $\mathfrak{n}_1, \dots, \mathfrak{n}_{m_3} \trianglelefteq L[x_2, \dots, x_n]$ being maximal ideals. By Theorem 2.1.2 the preimage $\varphi^{-1}(\mathfrak{n}_i)$ is a maximal ideal and thus

$$(I, p) = \varphi^{-1}(J) = \bigcap_{i=1}^{m_3} \varphi^{-1}(\mathfrak{n}_i)$$

is the intersection of finitely many maximal ideals.

With (3.1) we can now see that f is a finite intersection of finite intersections of maximal ideals; in other words, a finite intersection of maximal ideals $\mathfrak{m}_i$

$$I = \bigcap_{i=1}^{k} \mathfrak{m}_i.$$

Now let $a \in K[x_1, \ldots, x_n]$ and $n \in \mathbb{N}$ such that $a^n \in I$. Then $a^n \in \mathfrak{m}_i$ for all $i \in [k]$, since every maximal ideal is in particular a radical ideal, it follows that $a \in \mathfrak{m}_i$ for all $i \in [k]$ and thus $a \in \bigcap_{i=1}^{k} \mathfrak{m}_i = I$, which shows that I is a radical ideal. □

Corollary 3.3.4 *Let K be a perfect field and I a zero-dimensional ideal of $K[x_1, \ldots, x_n]$, then*

$$I = \sqrt{I} \Leftrightarrow \text{For all } i \in [n] \text{ there exists a squarefree polynomial } f_i \in I \cap K[x_i].$$

Proof: "$\Rightarrow$": As stated after the definition of the dimension of an ideal, this follows directly from Lemma 3.3.1(a).
"$\Leftarrow$": From Theorem 3.2.3(c) we know that all the f_i are also separable; from there we can apply Theorem 3.3.3, which gives us our desired result. □

This characterization of radicals of zero-dimensional ideals finally lets us obtain an algorithm to compute the radical of a zero-dimensional ideal.

Algorithm 3.3.5 (Radical of a zero-dimensional ideal) *Let K be a perfect and computable field and $S \subseteq K[x_1, \ldots, x_n]$ a finite set such that (S) is a zero-dimensional ideal of $K[x_1, \ldots, x_n]$. Then the following algorithm computes a finite Basis R of (S):*

```
zeroRadical($S$):
(1) $R := S$
(2) for $i \in [n]$
(3)     $f_i :=$ monicGen$(S, x_i)$
(4)     $g_i :=$ sqfrPart$(f_i)$
(5)     $R := R \cup g_i$
(6) end
(7) return $R$
```

Proof: Let $I := (S)$. Since we know how to compute the monic generator and the squarefree part of a univariate polynomial over a perfect and computable field usings Algorithms 3.1.3 and 3.2.7, all we have to show is that $\sqrt{I} = (R) = (S, g_1, \ldots, g_n)$, where g_i is the squarefree part of the monic generator f_i of the elimination ideal $I \cap K[x_i]$.
Clearly $I \subseteq (R)$ holds, since $S \subseteq R$ is already a generating set of I. By Lemma 3.3.1(a) all the g_i's are contained in $\sqrt{I}$ and thus $(R) \subseteq \sqrt{I}$. Since R contains squarefree univariate polynomials in every variable, namely the g_i, Corollary 3.3.4 tells us that (R) is a radical ideal and thus Lemma 3.3.1(b) gives us our equality. □

In many cases, it may happen that one doesn't want to compute the entire radical of an ideal, but one only wants to know, whether a given zero-dimensional ideal is radical or not. For this, we can reuse some of the ideas of the previous algorithm for the following one.

Algorithm 3.3.6 *Let K be a perfect and computable field and $S \subseteq K[x_1, \ldots, x_n]$ a finite set such that (S) is a zero-dimensional ideal of $K[x_1, \ldots, x_n]$. Then the following algorithm determines, whether (S) is a radical ideal or not:*

```
zeroRadicalTest($S$):
(1) for $i \in [n]$
(2)     $f_i :=$ monicGen$(S, x_i)$
(3)     if $\gcd(f_i, f_i') \neq 1$
(4)         return false
(5) end
```

```
$(6)$ return true
```

Proof: If I is a radical ideal every monic generator f_i must be squarefree by Corollary 3.3.4, which by Theorem 3.2.3 is equivalent to $\gcd(f_i, f_i') = 1$. Because the algorithm clearly returns *true* if every monic generator f_i satisfies $\gcd(f_i, f_i') = 1$ and false if $\gcd(f_i, f_i') \neq 1$ for any $i \in [n]$, we can see that it runs correctly. □

Remark 3.3.7 *In the case where $n = 1$, the equivalence of Corollary 3.3.4 holds for any field; i.e. let K be an arbitrary field and $(0) \neq I \trianglelefteq K[x]$, then*

$$I = \sqrt{I} \Leftrightarrow \text{There exists a squarefree polynomial } 0 \neq f \in I.$$

In particular this means that $\sqrt{I} = (I, g)$, where g is the squarefree part of some $f \in I$.

Proof: "$\Rightarrow$": Again, this follows from Lemma 3.3.1(a).
"$\Leftarrow$": Since $K[x]$ is a principal ideal domain $I = (g)$ for some $g \in K[x]$. From this it follows that the squarefree polynomial $f \in I$ of our assumption is of the form $r \cdot g$ with $r \in K[x]$, which means g has to be squarefree as well and there exist pairwise non-associated irreducibles $p_1, \ldots, p_n$ such that $g = p_1 \cdots p_n$. Applying Lemma 3.3.2, we get $I = ((0), g) = \bigcap_{i=1}^{n}(p_i)$. As an intersection of prime and therefore radical ideals we conclude that I is radical. □

To show that in the multivariate case the perfectness of K is still required, we will consider the following example.

Example 3.3.8 *Let p be a prime number, $K = \mathbb{F}_p(z)$ the rational function field over the finite field $\mathbb{F}_p$ and $I := (f, g)$ the ideal generated by $f = x^p - z,\ g = y^p - z$ in $K[x, y]$. Then I contains a squarefree univariate polynomial in every variable, but it is not a radical.*

Proof: Since f and g are irreducible, they are also squarefree. Clearly, they also each contain precisely one of the two variables.
Now let $h = x - y$, since the totaldegree of any non-zero polynomial in I is at least p and $totaldeg(h) = 1$, h cannot be contained in I. But $h^p = (x - y)^p = x^p - y^p = f - g \in I$ and hence I cannot be a radical. □

4 Higher-dimensional Ideals

4.1 Colon Ideals

In order to compute the radical of an ideal I of arbitrary dimension, we will now have to introduce some theory about "colon ideals", which are sometimes also called "ideal quotients". Let I and J be ideals of $K[x_1, \dots, x_n]$, then we will call

$$I : J := \{f \in K[x_1, \dots, x_n] \mid f \cdot g \in I \text{ for all } g \in J\}$$

the **colon ideal** of I by J. For $J = (f)$ we will write $I : f$. As we will find out in the next lemma, a colon ideal is indeed an ideal and if $S \subseteq K[x_1, \dots, x_n]$ is a finite generating set of J, then $I : J = \{f \in K[x_1, \dots, x_n] \mid f \cdot g \in I \text{ for all } g \in S\}$. We will therefore often write $I : S$ where S is just a generating set.

Lemma 4.1.1 *Let I, J be ideals of $K[x_1, \dots, x_n]$ with $J = (S)$ and $S \subseteq K[x_1, \dots, x_n]$ a finite set, then*

(a) $I : S$ is an ideal.

(b) $I : J = I : S$.

(c) $I : S = \bigcap_{s \in S} I : s$.

Proof: (a): Let $a, b \in I : S$ and $s \in S$. Then $as, bs \in I$ and therefore also $(a + b)s \in I$. As s was arbitrary, we get $(a + b) \in I : S$. Now let $r \in K[x_1, \dots, x_n]$. Since $as \in I$ and I is an ideal, ras is also contained in I and thus $ra \in I : S$.
(b): "$\subseteq$": Since $S \subseteq J$ and clearly $I : B \subseteq I : A$ holds for $A \subseteq B$, it follows that $I : J \subseteq I : S$.
"$\supseteq$": Let $a \in I : S$ and $g \in J$ such that $g = \sum_{k=1}^{m} r_k s_k$ with $r_k \in K[x_1, \dots, x_n]$ and $S = \{s_1, \dots, s_m\}$. Then $as_k \in I$ for all $k \in [m]$ and since, as an ideal, I is closed under scalar multiplication and under addition, we get $r_k a s_k \in I$ and therefore$\sum_{k=1}^{m} r_k a s_k = a \sum_{k=1}^{m} r_k s_k = a \cdot g \in I$, which shows $a \in I : J$.
(c): One can see that this equality is immediate from the definitions of the colon ideal and the intersection of sets. □

Lemma 4.1.2 *Let I_1, I_2, J_1, J_2 be ideals of $K[x_1, \dots, x_n]$, then the following hold:*

(a) $(I_1 \cap I_2) : (J_1 + J_2) = (I_1 : J_1) \cap (I_1 : J_2) \cap (I_2 : J_1) \cap (I_2 : J_2)$.

(b) If $I_1 \subseteq I_2$ and $J_2 \subseteq J_1$, then $I_1 : J_1 \subseteq I_2 : J_2$.

Proof: (a): Since $K[x_1, \dots, x_n]$ is Noetherian and thus every ideal is finitely generated, we can find finite generating sets $S_1, S_2 \subseteq K[x_1, \dots, x_n]$ of J_1 and J_2 respectively. Now Let $a \in (I_1 \cap I_2) : (J_1 + J_2)$. By Lemma 4.1.1$(b)$ and since $J_1 + J_2 = (S_1 \cup S_2)$, this is equivalent to $as \in (I_1 \cap I_2)$ for all $s \in (S_1 \cup S_2)$ and hence in particular $as \in I_1$ and $as \in I_2$ for all $s \in (S_1 \cup S_2)$. By definition of a colon ideal, this is the same as $a \in (I_1 : (S_1 \cup S_2) \cap I_2 : (S_1 \cup S_2))$, which by Lemma 4.1.1$(c)$ is then equivalent to $a \in (I_1 : J_1) \cap (I_1 : J_2) \cap (I_2 : J_1) \cap (I_2 : J_2)$.
(b): Let $a \in I_1 : J_1$, then $as \in I_1$ for all $s \in J_1$. Since $I_1 \subseteq I_2$ and $J_2 \subseteq J_1$, this implies that $as \in I_2$ for all $s \in J_2$, which then also means that $a \in I_2 : J_2$. □

We will now take a look at a certain type of colon ideal. For this, we will write $I : f^\infty := I : f^r$ if

$$I : f^r = I : f^m$$

for all $m \geq r$.

Lemma 4.1.3 *Let I be an ideal of $K[x_1,\dots,x_n]$ and $f \in K[x_1,\dots,x_n]$, then there exists an $r \in \mathbb{N}$ such that*

$$I : f^r = I : f^\infty.$$

Proof: Since clearly $(f^{k+1}) \subseteq (f^k)$ and I is a subset of itself, it follows by Lemma 4.1.2(b) and Lemma 4.1.1(a) that $I_k := I : f^k$ defines an ascending chain of ideals. Since $K[x_1,\dots,x_n]$ is Noetherian, there is by definition an $r \in \mathbb{N}$ such that $I_r = I_m$ for all $m \geq r$, which proves the claim. □

Theorem 4.1.4 *Let I be an ideal of $K[x_1,\dots,x_n]$, $J = (I, 1-yf) \trianglelefteq K[x_1,\dots,x_n,y]$ for some non-zero polynomial $f \in K[x_1,\dots,x_n]$ and J_X the elimination ideal at $\{x_1,\dots,x_n\}$, then*

(a) $I : f^\infty = J_X$,

(b) *if $\{f_1,\dots,f_k\}$ and $\{g_1,\dots,g_m\}$ are generating sets of I and J_X respectively, and we have elements $a_i, h_{ij} \in K[x_1,\dots,x_n]$ for $i \in [m]$, $j \in [k]$ such that*

$$g_i = a_i(1-yf) + \sum_{j=1}^{k} h_{ij} f_j$$

and $r := \max\{\deg_y(h_{ij}) \mid i \in [m], j \in [k]\}$, where $\deg_y(h_{ij})$ is the degree of h_{ij} with respect to y, then

$$I : f^r = I : f^\infty.$$

Proof: (a): "$\subseteq$": Let $r \in \mathbb{N}$ such that $I : f^\infty = I : f^r$, we know from the previous lemma that r exists. Now let $g \in I : f^\infty$, then $gf^r \in I \subseteq J$. Since $(1-yf) \in J$, we get that 1 and yf are equal modulo J and thus $1+(J) = 1^r + (J) = y^r f^r + (J)$. Since we said that $gf^r \in J$ and with J being an ideal in $K[x_1,\dots,x_n,y]$, we get $1 \cdot g + (J) = y^r f^r g + (J) = 0 + (J)$ and so $g \in J$. Because $g \in I \subseteq K[x_1,\dots,x_n]$, it follows that $g \in J_X$.
"$\supseteq$": Now let $g \in J_X$, then we can write $g = a \cdot h + b \cdot (1-yf)$ with $a, b \in K[x_1,\dots,x_n,y]$ and $h \in I$. Let $d = \deg_y(a)$ be the degree of a when seen as a polynomial in y. Since in particular $g \in K[x_1,\dots,x_n]$, we can pass to the rational function field $K(x_1,\dots,x_n,y)$ and substitute y for $\frac{1}{f}$. If we now multiply g by f^d we get $gf^d = a(\frac{1}{f}) \cdot f^d h$ with $a(\frac{1}{f})$ being the evaluation of a at $\frac{1}{f}$. By the definition of d, $a(\frac{1}{f}) \cdot f^d$ is in $K[x_1,\dots,x_n]$, from which we can gather that $gf^d \in I : f^d \subseteq I : f^\infty$.
(b): As the inclusion "$\subseteq$" is always true, we only have to proof the converse. For that, let $g \in I : f^\infty$. By (a) we therefore know that $g \in J_X$, which means we can write

$$g = \sum_{i=1}^{m} c_i \Big(a_i(1-yf) + \sum_{j=1}^{k} h_{ij} f_j \Big)$$

with $c_i \in K[x_1,\dots,x_n]$ for $i \in [m]$. If we now again substitute y for $\frac{1}{f}$ and this time multiply by f^r with $r = \max\{\deg_y(h_{ij}) \mid i \in [m], j \in [k]\}$, we get

$$gf^r = \sum_{i=1}^{m} c_i \sum_{j=1}^{k} t_{ij} f_j$$

with $t_{ij} = h_{ij}(\frac{1}{f}) \cdot f^r \in K[x_1,\dots,x_n]$. As in the proof of (a), we conclude that $gf^r \in I$ and therefore $I : f^\infty = I : f^r$. □

Algorithm 4.1.5 *Let K be a computable field, $S \subseteq K[x_1,\dots,x_n]$ a finite set and $f \in K[x_1,\dots,x_n]$ a non-zero polynomial. Then the following algorithm computes a pair (G, r), where G is a Gröbner basis of the colon ideal $(S) : f^\infty$, and $r \in \mathbb{N}$ such that $(S) : f^r = (S) : f^\infty$:*

```
*colonIdeal*$(S, f)$:
$H :=$ *gröbner*$(S \cup \{1 - yf\})$
$G :=$ *elim*$(H, \{x_1, \ldots, x_n\})$
$r := \max\{\deg_y(h_{gp}) \mid g \in G, p \in S\}$, with $g = a_g(1 - yf) + \sum_{p \in S} h_{gp} p$ for all $g \in G$
**return** $(G, r)$
```

Proof: We know from Theorem 4.1.4(a) that $I : f^\infty$ is equal to the elimination ideal $(S \cup \{1 - yf\})_X$. By the correctness of Algorithm 2.2.10, we therefore conclude that G is a Gröbner of $I : f^\infty$. It is also clear by Theorem 4.1.4(b) that r satisfies $I : f^r = I : f^\infty$. □

It's worth mentioning that the $r \in \mathbb{N}$ from Theorem 4.1.4(b), and therefore also the one computed in Algorithm 4.1.5, isn't necessarily minimal; i.e. there could be a positive integer $m < r$ such that $I : f^m = I : f^r$. There are ways to get the smallest natural number that satisfies that equation, but for our purposes a non-minimal one is all we need.

The last result of this section will be quite important for proving the correctness of the algorithm that computes the radical of an ideal. It is easy to see that $I \subseteq I : f^\infty$, the following theorem shows that we can even get an equality, if we intersect the right-hand side with a suitable ideal.

Theorem 4.1.6 *Let I be an ideal of $K[x_1, \ldots, x_n]$, $f \in K[x_1, \ldots, x_n]$ and $r \in \mathbb{N}$ such that $I : f^r = I : f^\infty$, then*

$$I = (I, f^r) \cap (I : f^r).$$

Proof: "$\subseteq$": Since $I \subseteq I : f^r$ and $I \subseteq (I, f^n)$, this inclusion is clear.
"$\supseteq$": Let $g \in (I, f^r) \cap (I : f^r)$, then from $g \in (I, f^r)$ we can conclude that $g = h + a \cdot f^r$ with $h \in I$ and $a \in K[x_1, \ldots, x_n]$, and from $g \in I : f^r$ that $gf^r \in I$. Since we also have $hf^r \in I$, it follows that $a \cdot f^{2r} = gf^r - hf^r \in I$. And since by definition of r we have $I : f^{2r} = I : f^r$, we can conclude that $a \cdot f^r \in I$ and therefore $g = h + a \cdot f^r \in I$. □

4.2 Extensions and Contractions of Ideals

We will now introduce some theory about extensions and contractions of ideals. In order to define what we mean by this, we first need to recall what a localization is. One can define localization for a normal ring R or even for an R-module. However, as we will mainly work with polynomial rings over fields in this thesis, we will limit ourselves to localizations of integral domains, as this will simplify quite a few things.

First, let R in our setting be an integral domain, M a multiplicative subset of R; i.e. $m_1, m_2 \in M$ implies that $m_1 \cdot m_2 \in M$; with $0 \notin M$. Now let $a_1, a_2 \in R$ and $m_1, m_2 \in M$, then $\sim$ is an equivalence relation on $R \times M$ by $(a_1, m_1) \sim (a_2, m_2)$ if and only if $a_1 m_2 = a_2 m_1$. It is clearly reflexive, as integral domains are commutative and by the symmetry of "$=$", the relation $\sim$ is also symmetric. Furthermore, let $(a_1, m_1) \sim (a_2, m_2)$ and $(a_2, m_2) \sim (a_3, m_3)$ with $a_2 \neq 0$. Then we get $a_1 m_2 = a_2 m_1$ and $a_2 m_3 = a_3 m_2$. From this it follows that $a_2 m_2 a_1 m_3 = a_2 m_2 a_3 m_1$. Since $a_2 m_2 \in R$ is neither a zero-divisor, nor zero itself, we therefore get $a_1 m_3 = a_3 m_1 \Leftrightarrow (a_1, m_1) \sim (a_3, m_3)$. The case where $a_2 = 0$ is clear as well. From this we can conclude that $\sim$ is reflexive and therefore an equivalence relation. We will write $\frac{a}{m} := [(a, m)]_\sim$ for the equivalence class of $(a, m) \in R \times M$.

Definition 4.2.1 (Localization) *Let R be an integral domain and M a multiplicative subset of R such that $1 \in M$ and $0 \notin M$, then*

$$M^{-1}R := \{\frac{a}{m} \in (R \times M)/\sim \mid a \in R,\ m \in M\}$$

*is called the **localization** of R by M.*

As the notation suggests, localization is a way of adding "denominators" to a ring and indeed a localization $M^{-1}R$ with addition and multiplication defined as $\frac{a_1}{m_1} + \frac{a_2}{m_2} := \frac{a_1m_2+a_2m_1}{m_1m_2}$ and $\frac{a_1}{m_1} \cdot \frac{a_2}{m_2} := \frac{a_1a_2}{m_1m_2}$ respectively, becomes itself again a ring. It is easy to see that the multiplicative and additive neutral element are $0_{M^{-1}R} = \frac{0}{1} = \frac{0}{s}$ and $1_{M^{-1}R} = \frac{1}{1} = \frac{r}{r}$ for all $r, s \in M$.

We will furthermore call $\varepsilon : R \to M^{-1}R,\ r \mapsto \frac{r}{1}$ the **canonical map** from R to $M^{-1}R$. It follows that ε is injective iff for $r \in R$ and $s \in M$, the equality of $\frac{r}{1}$ and $\frac{0}{s}$ implies that $r = 0$. Since $\frac{r}{1} = \frac{0}{s}$ means that $r \cdot s = 1 \cdot 0$ with $s \neq 0$ and R is by assumption an integral domain, this indeed implies that $r = 0$. We can now see that restricting ourselves to localizations of integral domains means that we can always embed R into a localization $M^{-1}R$, we will therefore often view R as a subset of $M^{-1}R$ and for $a \in R$ say $a = \frac{a}{1}$. Furthermore, if $\frac{b}{1} \in M^{-1}R$, then there is some $c \in M$ such that $bc \in R$.

Definition 4.2.2 (Extension and Contraction of an Ideal) *Let R be an integral domain, M a multiplicative subset of R with $1 \in M$ and $0 \notin M$, I an ideal of R and J an ideal of the localization of R by M. Then*

*(a) $I^e := (I)_{M^{-1}R}$, i.e. the ideal generated by I in $M^{-1}R$, is called the **extension** of I to $M^{-1}R$.*

*(b) $J^c := J \cap R$ is called the **contraction** of J to R.*

Lemma 4.2.3 *Let R be an integral domain, M a multiplicative subset of R with $1 \in M$ and $0 \notin M$. Let I an ideal of R and I^e its extension to $M^{-1}R$, then the following hold:*

(a) $I^e = \{\frac{a}{m} \in M^{-1}R \mid a \in I,\ m \in M\}$.

(b) I^e is a proper ideal in $M^{-1}R$ iff $I \cap M = \emptyset$.

(c) $I \subseteq I^{ec}$.

(d) If I is a prime ideal in R and $I \cap M = \emptyset$, then $I = I^{ec}$ and I^e is a prime ideal in $M^{-1}R$.

Proof: (a): "$\subseteq$": Let $b \in I^e$. By the definition of I^e, b is a finite sum of elements $\frac{a_i}{1}, \ldots, \frac{a_n}{1}$ with $a_1, \ldots, a_n \in I$ multiplied by elements $\frac{b_1}{m_1}, \ldots, \frac{b_n}{m_n} \in M^{-1}R$. Now let $m = m_1 \cdots m_n$ and $n_i = m_1 \cdots m_{i-1}m_{i+1} \cdots m_n$, then

$$b = \sum_{i=1}^{n} \frac{a_i}{1}\frac{b_i}{m_i} = \sum_{i=1}^{n} \frac{a_ib_i}{m_i} = \frac{\sum_{i=1}^{n} n_ia_ib_i}{m}$$

by inductively applying the addition operation of $M^{-1}R$. Clearly $m \in M$ and since $a_i \in I$ for all $i \in [n]$ the numerator of the last fraction is contained in I and thus $b = \frac{a}{m}$ with $a \in I$ and $m \in M$.
"$\supseteq$": By definition, $a \in I$ implies $\frac{a}{1} \in I^e$ and since for $m \in M$, the element $\frac{1}{m}$ is in $M^{-1}R$, we get $\frac{a}{m} = \frac{a}{1} \cdot \frac{1}{m} \in I^e$.
(b): I^e is a proper ideal iff it doesn't contain $1_{M^{-1}R}$, which is the case iff there is no element $r \in R$ such that $\frac{r}{r} \in I^e$. From (a) it now follows that this is precisely the case when $I \cap M = \emptyset$.
(c): Since by definition $I \subseteq I^e$ and $I \subseteq R$, it immediately follows that $I \subseteq I^{ec} = I^e \cap R$.
(d): Let $a \in I^{ec}$, then $\frac{a}{1} = \frac{sa}{s} \in I^e$ for some $s \in M$ and by (a), we have $sa \in I$. Since $I \cap M = \emptyset$, I doesn't contain s, but as I is a prime ideal, this implies that $a \in I$.
In order to prove that I^e is a prime ideal in $M^{-1}R$, let $a, b \in M^{-1}R$ with $ab \in I^e$ and assume $a \notin I^e$. Then there are $r, s \in M$ such that $a = \frac{ra}{r}$ and $b = \frac{sb}{s}$ with $ra, sb \in R$. From this we get that $(ra)(sb) = (rs)(ab) \in I^{ec}$ since $ab \in I^{ec}$. As we have $I = I^{ec}$ from above and therefore $M \cap I^{ec} = \emptyset$, neither r nor s is contained in I^{ec}. We also assumed that $a \notin I^e$, which then means that $a \notin I^{ec}$, and as $I = I^{ec}$ was assumed to be prime $(ra)(sb) \in I^{ec}$ implies that $b \in I^{ec} \subseteq I^e$ and hence I^e is a prime ideal. □

Lemma 4.2.4 *Let R be an integral domain, M a multiplicative subset of R with $1 \in M$ and $0 \notin M$. Let J an ideal of M^{-1} and J^c its contraction to R, then the following hold:*

(a) J^c is an ideal of R.

(b) If J is a proper ideal in $M^{-1}R$, then $J^c \cap M = \emptyset$.

(c) If J is a prime ideal in $M^{-1}R$, then J^c is a prime ideal in R.

(d) $J = J^{ce}$.

Proof: (a): Let $a, b \in J^c$, then $\frac{a}{1}, \frac{b}{1} \in J$ and since J is an ideal of $M^{-1}R$, $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} \in J$ and thus $a + b \in J^c$. Now let $r \in R$, then $\frac{r}{1} \cdot \frac{a}{1} = \frac{ra}{1} \in J$, and we get $ra \in J^c$.
(b): Assume J is a proper ideal and $J^c \cap M \neq \emptyset$. Now let $a \in J^c \cap M$, then $\frac{a}{1} \in J$ and $a \in M$ which means that $\frac{1}{a} \in M^{-1}R$, but since J is an ideal, $\frac{a}{1} \cdot \frac{1}{a} = \frac{a}{a} = 1_{M^{-1}R} \in J$. But this is a contradiction to J being a proper ideal and therefore $J^c \cap M = \emptyset$ has to hold.
(c): Since, as a prime ideal, J is proper, $J^c \cap M = \emptyset$ by (b) and therefore J^c is also a proper ideal. Now let $a, b \in R$ with $ab \in J^c$, then $\frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} \in J$. As J is a prime ideal, we get $a \in J$ or $b \in J$ and therefore $a, b \in J \cap R = J^c$. We can thus conclude that $a \in J^c$ or $b \in J^c$, which makes J^c a prime ideal.
(d): "$\subseteq$": Let $b \in J$ and $s \in M$ such that $sb \in R$ and with that $sb \in J^c$. From Lemma 4.2.3(a) we know that $\frac{sb}{s} = b \in J^{ce}$.
"$\supseteq$": Now let $b \in J^{ce}$, once more by Lemma 4.2.3(a) we get $b = \frac{a}{r}$ with $a \in J^c$ and $r \in M$. By definition $J^c \subseteq J$ and so $\frac{a}{1} \in J$. With this and since $\frac{1}{r} \in M^{-1}R$ we get $\frac{a}{1} \cdot \frac{1}{r} = \frac{a}{r} = b \in J$. □

Lemma 4.2.5 *Let R be an integral domain and M a multiplicative subset with $1 \in M$ and $0 \notin M$. Let I be an ideal of R with extension I^e to $M^{-1}R$ and let J be an ideal of $M^{-1}R$ with contraction J^c to R, then the following hold:*

(a) $\sqrt{I}^e = \sqrt{I^e}$.

(b) $\sqrt{J}^c = \sqrt{J^c}$.

Where the radicals $\sqrt{I}^e$ and $\sqrt{J^c}$ are in R, and $\sqrt{I^e}$ and $\sqrt{J}^c$ are in $M^{-1}R$.

Proof: (a): "$\subseteq$": Let $a \in \sqrt{I}^e$, by Lemma 4.2.3(a) we get $a = \frac{r}{m}$ with $r \in \sqrt{I}$ and $m \in M$. By definition of the radical, there is some $n \in \mathbb{N}$ such that $r^n \in I$. and so $\frac{r^n}{m} \in I^e$. Since M is multiplicative, we have $m^n \in M$, and by using Lemma 4.2.3(a) again, we get $\frac{r^n}{m^n} = (\frac{r}{m})^n \in I^e$, from which $a = \frac{r}{m} \in \sqrt{I^e}$ follows.
"$\supseteq$": For the converse, let $a \in \sqrt{I^e}$. Since $\sqrt{I^e}$ is an ideal in $M^{-1}R$, we can write $a = \frac{r}{m}$ with $r \in R$ and $m \in M$. From the definition of the radical, we then get that there is an $n \in \mathbb{N}$ such that $a^n = \frac{r^n}{m^n} \in I^e$. Because every element of I^e is of the form $\frac{s}{t}$ with $s \in I$ and $t \in M$ according to Lemma 4.2.3(a), we get $r^n \in I$ and therefore $r \in \sqrt{I}$, which shows $a = \frac{r}{m} \in \sqrt{I}^e$.
(b): "$\subseteq$": Now let $a \in \sqrt{J}^c$, then $a \in R$ and $a^n \in J$ for some $n \in \mathbb{N}$. Because obviously $a^n \in R$, we get $a^n \in J^c$ and therefore $a \in \sqrt{J^c}$.
"$\supseteq$": Let $a \in \sqrt{J^c}$, then there is some $n \in \mathbb{N}$ such that $a^n \in J^c \subseteq J \subseteq \sqrt{J}$ and thus $a \in \sqrt{J}$. And as $\sqrt{J^c}$ is a radical in R, by definition we get that $a \in R$ and therefore $a \in \sqrt{J}^c$. □

For the next lemma, we will need a concept, which we have already used implicitly in the definition of the dimension of an ideal.

Definition 4.2.6 *Let I be a proper ideal of $K[x_1, \ldots, x_n]$ and $Y \subseteq \{x_1, \ldots, x_n\}$, then*

(a) Y is called ***independent*** *modulo I, if $I_Y = \{0\}$.*

(b) Y is called ***maximally independent*** *modulo I, if it is independent modulo I and not properly contained in any other set that is independent modulo I.*

We can now see that an ideal I of $K[x_1, \ldots, x_n]$ is zero-dimensional, if and only if there is no non-empty subset of variables, that is independent modulo I.

Remark 4.2.7 *Since we will have to work with subsets of variables a lot, we will set $Y := \{y_1, \dots, y_m\}$ to be a subset of $X := \{x_1, \dots, x_n\}$ for the rest of this chapter, unless otherwise stated. Furthermore $Z := \{z_1 \dots, z_{n-m}\}$ is the complement of Y in X; i.e. $Z = X \backslash Y$. From now on, we will also mostly look at the localization $M^{-1}K[x_1, \dots, x_n]$ with $M = K[y_1, \dots, y_m] \backslash \{0\}$. We can see that we can write $M^{-1}K[x_1, \dots, x_n] = K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}]$ with $K(y_1, \dots, y_m)$ being the rational function field in $y_1, \dots, y_m$ over K. As before, we will view $K[x_1, \dots, x_n]$ as a subset of $K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}]$. Now when looking at a polynomial $f \in K[x_1, \dots, x_n] \subseteq K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}]$, it can be viewed as a polynomial in $x_1, \dots, x_n$ with coefficients in K, or as a polynomial in $z_1, \dots, z_{n-m}$ with coefficients in $K(y_1, \dots, y_m)$. This distinction will become quite important and we will try to make it as clear as possible, what we mean at any given moment.*

In order to work with these polynomial rings, we will need block orderings, which we already introduced in the section on Gröbner bases, right after Definition 2.2.1. For the rest of this chapter $\leq_1$ and $\leq_2$ will be monomial orderings on $K[z_1, \dots, z_{n-m}]$ and $K[y_1, \dots, y_m]$ respectively, and $\leq$ a block ordering on $K[x_1, \dots, x_n]$ with $\leq_1$ dominating.

Furthermore, when looking at elements $f \in K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}]$, we will write $lc_Z(f)$ and $lm_Z(f)$, when we mean the leading coefficient and leading monomial of f seen as a polynomial in the variables $z_1, \dots, z_{n-m}$ and with respect to the monomial ordering $\leq_1$. In this regard, we can again see that the leading coefficient $lc_Z(f)$ is an element of $K(y_1, \dots, y_m)$ and $lm_Z(f)$ an element of $K[z_1, \dots, z_{n-m}]$. Since the leading term is defined to be $lc(f) \cdot lm(f)$, which is the same as $lc_Z(f) \cdot lm_Z(f)$, it stays the same, no matter how we look at f. When looking at a polynomial f in the variables $x_1, \dots, x_n$, we will still write $lm(f)$ and $lc(f)$ as usual.

Lemma 4.2.8 *Let I be an ideal of $K[x_1, \dots, x_n]$ and I^e the extension of I to $K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}]$, then the following hold:*

(a) I^e is a proper ideal iff Y is independent modulo I.

(b) If Y is maximally independent modulo I, then I^e is zero-dimensional.

(c) If I is a prime ideal and I^e is zero-dimensional, then Y is maximally independent modulo I.

Proof: (a): Since $K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}] = (K[y_1, \dots, y_m] \backslash \{0\})^{-1}K[x_1, \dots, x_n]$, Lemma 4.2.3$(b)$ tells us that I^e is proper if and only if $I \cap K[y_1, \dots, y_n] \backslash \{0\} = \emptyset$, which is equivalent to $I \cap K[y_1, \dots, y_n] = I_Y = \{0\}$; i.e. to Y being independent modulo I.
(b): If Y is maximally independent modulo I, its extension I^e is proper by (a). We mentioned in Chapter 3, that an ideal of a polynomial ring is zero-dimensional if and only if the ideal contains a univariate polynomial in every variable of the underlying polynomial ring. By the definition of maximal independence, there is no $i \in [n-m]$ such that $I_{Y \cup \{z_i\}} = \{0\}$ and thus I contains a non-zero polynomial $f_i \in K[y_1, \dots, y_m, z_i]$ for every $i \in [n-m]$. We can therefore conclude that for $i \in [n-m]$, the f_i seen as polynomials in I^e are non-zero and univariate in the variable z_i and thus I^e is zero-dimensional.
(c): Since I^e must be a proper ideal by assumption of Definition 3.0.1, it follows from (a) that Y is independent modulo I; this in particular means that $I \cap K[y_1, \dots, y_m] \backslash \{0\} = \emptyset$. And since I^e is zero-dimensional, we again get non-zero univariate polynomials $f_i \in I^e$ in z_i for every $i \in [n-m]$, which are of the form $f_i = \sum_{k=0}^{n_i} \frac{g_{i,k}}{h_{i,k}} z_i^k$ with $g_{i,k}, h_{i,k} \in K[y_1, \dots, y_m]$ and $h_{i,k} \neq 0$. Now let $H_i = \prod_{k=0}^{n_i} h_{i,k}$ and $l_{i,k} = \frac{H_i}{h_{i,k}}$, then we can see that $H_i \cdot f_i = \sum_{k=0}^{n_i} \frac{g_{i,k} l_{i,k}}{1} z_i^k$ and thus $0 \neq H \cdot f_i \in I^{ec} \cap K[y_1, \dots, y_m, z_i]$ for all $i \in [n-m]$. This shows that Y is maximally independent modulo I^{ec} and since by Lemma 4.2.3, I being prime and $I \cap K[y_1, \dots, y_m] \backslash \{0\} = \emptyset$ implies $I = I^{ec}$, Y is maximally independent modulo I. □

Together with Algorithm 4.1.5, the following theorem will help us compute the contraction of an ideal $J \subseteq K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}]$ to $K[x_1, \dots, x_n]$.

Theorem 4.2.9 *Let J be an ideal of $K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}]$ and $G \subseteq K[x_1, \dots, x_n]$ a Gröbner basis of J with respect to $\leq_1$. Let $I = (G)_{K[x_1, \dots, x_n]}$ and $f = lcm\{lc_Z(g) \in K[y_1, \dots, y_m] \mid g \in G\}$, then*

$$I : f^\infty = J^c.$$

Proof: "$\subseteq$": Let $g \in I : f^\infty$ and $r \in \mathbb{N}$ such that $I : f^r = I : f^\infty$, then $gf^r \in I$. Since $f \in K[y_1, \ldots, y_m]$ and J is an ideal in $K(y_1, \ldots, y_n)[z_1, \ldots, z_{n-m}]$, we get

$$g = gf^r \frac{1}{f^r} \in J \cap K[x_1, \ldots, x_n] = J^c.$$

"$\supseteq$": Now let $g \in J^c$, then $g \in J = (G)_{K(y_1,\ldots,y_m)[z_1,\ldots z_{n-m}]}$. By the definition of Gröbner bases, we obtain polynomials $a \in K(y_1, \ldots, y_m)[z_1, \ldots, z_{n-m}]$ and $b \in G$ such that $a \cdot \mathrm{lm}_Z(b) = \mathrm{lm}_Z(g)$. If we now let $g_1 = g - \frac{\mathrm{lc}_Z(g)}{\mathrm{lc}_Z(b)} \cdot a \cdot b$, then it is immediate that $g_1 \in J$ and $\mathrm{lm}_Z(g_1) <_1 \mathrm{lm}_Z(g)$ if $g \neq 0$, since we cancelled out the leading term of g. We now define the sequence

$$g_{k+1} := g_k - \frac{\mathrm{lc}_Z(g_k)}{\mathrm{lc}_Z(b_k)} \cdot a_k \cdot b_k \tag{4.1}$$

where $a_k \in K(y_1, \ldots, y_m)[z_1, \ldots, z_{n-m}]$ and $b_k \in G$ are chosen such that $a_k \cdot \mathrm{lm}_Z(b_k) = \mathrm{lm}_Z(g_k)$ and we let $g_0 = g$. Because of $\mathrm{lm}_Z(g_{k+1}) <_1 \mathrm{lm}_Z(g_k)$ for $g_k \neq 0$, it follows from Lemma 2.2.4 that there is an $r \in \mathbb{N}$ such that $g_s = 0$ for all $s \geq r$. We will now prove by induction on r that $g_0 = g \in I : f^\infty$.
"$r = 0$": This case is trivial, as $r = 0$ means that $g_0 = g = 0$ and therefore $g \in I : f^\infty$.
"$r - 1 \rightsquigarrow r$": Choose $r \in \mathbb{N}$ such that we have $g_s = 0$, for the sequence from (4.1) with $g_0 = g$ and for $s \geq r$. Now let g_k^* be the same sequence, but with $g_0^* = fg_1$. Since f is in $K[y_1, \ldots, y_m]$, it is just a constant in $K(y_1, \ldots, y_m)[z_1, \ldots, z_{n-m}]$ and it is therefore clear that we get $g_s^* = 0$ for $s \geq r - 1$. Recall that $g_1 = g - \frac{\mathrm{lc}_Z(g)}{\mathrm{lc}_Z(b)} \cdot a \cdot b$, with $a \in K(y_1, \ldots, y_m)[z_1, \ldots, z_{n-m}]$ and $b \in G \subseteq K[x_1, \ldots, x_n]$ such that $a \cdot \mathrm{lm}_Z(b) = \mathrm{lm}_Z(g)$. We can see that a has to be a monomial with leading coefficient 1 and since $\mathrm{lc}_Z(b) \mid f$ by definition of f, we can conclude that $f \cdot \frac{\mathrm{lc}_Z(g)}{\mathrm{lc}_Z(b)} \cdot a \cdot b$ and therefore also fg_1 must be contained in J^c. By applying the induction hypothesis, we get $fg_1 \in I : f^\infty$ and since $fg = fg_1 + f \cdot \frac{\mathrm{lc}_Z(g)}{\mathrm{lc}_Z(b)} \cdot a \cdot b$, it follows that $fg \in I : f^\infty$, from which $g \in I : f^\infty$ directly follows. □

Algorithm 4.2.10 *Let $Y, Z, lc_Z(g)$ and $\leq$ be defined as in Remark 4.2.7. Let K be a computable field and S a finite subset of the ring $K(y_1, \ldots, y_m)[z_1, \ldots, z_{n-m}]$. Then the following algorithm computes a Gröbner basis G of the contraction $(S)^c$ to $K[x_1, \ldots, x_n]$:*

```
cont(S, Y):
(1) $H :=$ gröbner($S$) with respect to $\leq$
(2) for $h \in H$
(3)     $c := lcm\{s \in K[y_1, \ldots, y_m] \mid s$ is a denominator of any coefficient of $h\}$
(4)     $h := c \cdot h$
(5) end
(6) $f := lcm\{lc_Z(h) \in K[y_1, \ldots, y_n] \mid h \in H\}$
(7) $(G, r) :=$ colonIdeal($H, f$)
(8) return $G$
```

Proof: It is clear that if we multiply any $h \in H \subseteq K(y_1, \ldots, y_m)[z_1, \ldots, z_{n-m}]$ by any common multiple of the denominators of the coefficients of all its terms, in our case the least common multiple $c \in K[y_1, \ldots, y_m]$, it follows that $c \cdot h$ is then in $K[x_1, \ldots, x_n]$. Since in $K(y_1, \ldots, y_m)[z_1, \ldots, z_{n-m}]$, the c from step (3) is invertible, we can conclude that after the **for** loop in steps (2) to (5), H remains a Gröbner basis of (S) in $K(y_1, \ldots, y_m)[z_1, \ldots, z_{n-m}]$, but we have $H \subseteq K[x_1, \ldots, x_n]$. This means we can apply Theorem 4.2.9, which shows that by computing the colon ideal $I : f^\infty$ with Algorithm 4.1.5, we get a Gröbner basis G of the contraction J^c. □

Lemma 4.2.11 *Let $G \subseteq K[x_1, \ldots, x_n]$ be a Gröbner basis with respect to $\leq$, then it is also a Gröbner basis in $K(y_1, \ldots, y_m)[z_1, \ldots, z_{n-m}]$ with respect to $\leq_1$.*

Proof: Let $I = (G)_{K[x_1,\dots,x_n]}$ and $J = (G)_{K(y_1,\dots,y_m)[z_1,\dots,z_{n-m}]}$. We now want to show that G is a Gröbner basis of J with respect to $\leq_1$, in other words that $L(G) = L(J)$ as seen in $K(y_1,\dots,y_m)[z_1,\dots,z_{n-m}]$ and with respect to $\leq_1$.
"$\subseteq$": This is clear, as $G \subseteq J$ by definition.
"$\supseteq$": Let $f \in J$, then $f = \sum_{i=1}^{s} a_i g_i$ with $a_i \in K(y_1,\dots,y_m)[z_1,\dots,z_{n-m}]$ for all $i \in [s]$ and with $G = \{g_1,\dots,g_s\}$. Now let $c \in K[y_1,\dots,y_m]$ be the least common multiple of the denominators of the coefficients of $a_1,\dots,a_s$, then clearly $c \cdot a_i \in K[x_1,\dots,x_n]$ for all $i \in [s]$ and therefore $c \cdot f \in I$. Since G is a Gröbner basis of I, there is a $g \in G$ such that $\operatorname{lm}(g) \mid \operatorname{lm}(cf)$. When we now consider g and cf as polynomials in $K(y_1,\dots,y_m)[z_1,\dots,z_{n-m}]$ it is clear that the leading monomial of g still divides cf. But since $c \in K[y_1,\dots,y_m]$ and $\leq$ is a block ordering with $\leq_1$ dominating, it follows that $\operatorname{lm}_Z(cf) = \operatorname{lm}_Z(f)$ and therefore $\operatorname{lm}_Z(g) \mid \operatorname{lm}_Z(f)$, which shows that $\operatorname{lm}_Z(f) \in L(G)$. With that every generator of $L(J)$ is contained in $L(G)$ and therefore clearly $L(J) \subseteq L(G)$. □

Corollary 4.2.12 *Let I be an ideal of $K[x_1,\dots,x_n]$, $G \subseteq K[x_1,\dots,x_n]$ a Gröbner basis of I with respect to $\leq$ and $f = lcm\{lc_Z(g) \in K[y_1,\dots,y_m] \mid g \in G\}$, then*

$$I^{ec} = I : f^{\infty}.$$

Proof: Since G is a generating set of I in $K[x_1,\dots,x_n]$ by Theorem 2.2.7, it is also clearly a generating set of I^e in $K(y_1,\dots,y_m)[z_1,\dots,z_{n-m}]$. By Lemma 4.2.11 G is a Gröbner basis of I^e and thus we can apply Theorem 4.2.9 and get the result. □

The previous Corollary will now allow us to develop an algorithm that computes the contraction of an extension of an ideal I in $K[x_1,\dots,x_n]$. This will be the final piece of the puzzle, as we can then "lift" ideals into $K(y_1,\dots,y_n)[z_1,\dots,z_{n-m}]$, where they become zero-dimensional, which allows us to compute their radical via Algorithm 3.3.5. And then we can bring them back to $K[x_1,\dots,x_n]$ using said following algorithm.

Algorithm 4.2.13 *Let $Y, Z, lc_Z(g)$ and $\leq$ be defined as in Remark 4.2.7. Let K be a computable field and $S \subseteq K[x_1,\dots,x_n]$ a finite set, then the following algorithm computes $f \in K[y_1,\dots,y_m]$ and $r \in \mathbb{N}$ such that $(S) = (S, f^r) \cap (S)^{ec}$:*

```
extCont(S, Y):
(1) G := gröbner(S) with respect to $\leq$
(2) $f$ := lcm{$lc_Z(g) \in K[y_1,\dots,y_m] \mid g \in G$}
(3) $(G, r)$ := colonIdeal($S, f$)
(4) return $(f, r)$
```

Proof: By Theorem 4.1.6, if we have any $r \in \mathbb{N}$, that satisfies $I : f^r = I : f^{\infty}$ we get

$$I = (I, f^r) \cap (I \,:\, f^r) = (I, f^r) \cap (I : f^{\infty}).$$

Since we can compute such an $r \in \mathbb{N}$ with Algorithm 4.1.5, we can conclude from Corollary 4.2.12 that the algorithm above terminates with the correct result. □

4.3 Computing the Radical of an Ideal

We now have all the theory we need in order to compute the radical of an ideal I of arbitrary dimension. In the algorithm, we will have to determine a subset Y of $\{x_1,\dots,x_n\}$, that is maximally independent modulo I. We can do this by computing the Y-elimination ideal for every possible $Y \subseteq \{x_1,\dots,x_n\}$ and testing if it is the zero ideal. For large $n \in \mathbb{N}$, this will obviously become quite computationally intensive, Becker and Weißpfenning propose a more elegant solution in Chapter 9.3 in [BW93], but for our purposes our method suffices.

Algorithm 4.3.1 (Radical of an ideal) *Let $Y, Z, lc_Z(g)$ and $\leq$ be defined as in Remark 4.2.7. Let K be a computable and perfect field such that the rational function field $K(y_1, \dots, y_n)$ is perfect, and $S \subseteq K[x_1, \dots, x_n]$ a finite set, then the following algorithm computes a Gröbner basis G of the radical of (S):*

```
radical(S):
G := {1}
if 1 ∉ (S)
    Y ⊆ {x_1, ..., x_n} such that Y is maximally independent modulo (S)
    R := zeroRadical(S) computed over K(y_1, ..., y_n)[z_1, ..., z_{n-m}]
    C := cont(R, {y_1, ..., y_m})
    (f, r) := extCont(S, Y)
    G := int(radical(S ∪ {f^r}), C)
return G
```

Proof: Let $I := (S)$, since $1 \in I$ if and only if S contains any constants and S is finite, it is clear that we can determine whether $1 \in I$ or not. If $1 \in I$, then it is clear that the algorithm terminates with the correct result, as $\{1\}$ is a Gröbner basis of $\sqrt{I} = K[x_1, \dots, x_n]$. If $1 \notin I$, then by Y being independent modulo I, the elimination ideal $I_Y = I \cap K[y_1, \dots, y_m] = \{0\}$. Since f^r from Algorithm 4.2.13 is an element of $K[y_1, \dots, y_m]$, the inclusion $(S) \subseteq (S, f)$ is strict, unless $S = K[x_1, \dots, x_n]$. In particular, since $K[x_1, \dots, x_n]$ is Noetherian, this chain of ascending ideals ends after finitely many iterations. We can see that the algorithm terminates in a finite amount of steps. We will now prove that it also gives the correct result.

Let $s \in \mathbb{N}$ be the number of recursions radical(S) has to go through to terminate. We have shown that the result is correct, if $s = 0$. Assume radical$(S \cup f^r)$ runs correctly for f and r as in the algorithm. If we now prove that radical(S) gives the right result, then we will have inductively proven the correctness of the algorithm.

Since Y is maximally independent modulo I, Lemma 4.2.8(b) tells us that the extension of I to $K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}]$ is zero-dimensional. Since S generates I^e in $K(y_1, \dots, y_m)[z_1, \dots, z_{n-m}]$, we conclude that $R = \text{zeroRadical}(S)$ is a finite generating set of $\sqrt{I^e}$ and $(C) = (\text{cont}(R, Y)) = \sqrt{I^e}^c$. Since Theorem 4.1.6 tells us that

$$\sqrt{I} = \sqrt{(I, f^r) \cap (I : f^r)}$$

we can use Lemma 4.2.5(b), Corollary 4.2.12 and Lemma 2.1.1 to get

$$\sqrt{I} = \sqrt{(I, f^r)} \cap \sqrt{I^{ec}} = \sqrt{(I, f^r)} \cap (C).$$

Since we assumed that radical(S, f^r) gives the proper result, we can see that radical(S) does as well. And with this we have proved the correctness of the algorithm. □

We will now do an example computation, as an illustration of how the algorithm works. We will try to show every step in detail, even when the answer we will be obvious. However, since we will need to compute them quite often, we will skip the computation of Gröbner bases. Since we still need an explicit monomial ordering for that, we will now define the "lexicographic ordering".

Let $f = x_1^{a_1} \cdots x_n^{a_n}$ and $g = x_1^{b_1} \cdots x_n^{b_n}$ be monomials in $K[x_1, \dots, x_n]$. If $\leq$ is the **lexicographic ordering** on $K[x_1, \dots, x_n]$, then $f < g$ iff $a_1 < b_1$ or $a_1 = b_1$ and $a_2 < b_2$ or $a_1 = b_1$ and $a_2 = b_2$ and $a_3 < b_3$, and so on.

We can see that the lexicographic ordering is a block ordering with the lexicographic ordering on $K[x_1, \dots, x_k]$ dominating, for any $k \in [n-1]$. By renaming the variables, we can thus get any block- and elimination orderings on $K[x_1, \dots, x_n]$ that we need for our purposes.

Example 4.3.2 *Let $K = \mathbb{Q}$, $f = x^2 + 2xyz + z^4$, $g = yz - z^2$ and I the ideal generated by f and g in $K[x, y, z]$. Since char$(\mathbb{Q}) = 0$, K is a perfect field and for subset T of $\{x, y, z\}$, $K(T)$ also has* *characteristic zero and is therefore perfect. Using the lexicographic ordering, we get the Gröbner basis $G = \{x^2 + 2xz^2 + z^4, -z^2 + yz\}$ of I, for every rearrangement of the variables.*

In order to find a set $T = \{t_1, \dots, t_m\}$, that is maximally independent modulo I, we go through every subset of $\{x, y, z\}$ and test if the T-elimination ideal is $\{0\}$, by looking at the intersection of G with $K[t_1, \dots, t_m]$. We see that when T is a singleton, T is independent modulo I, but the only other subset of $\{x, y, z\}$ that is independent modulo I is $\{x, y\}$ and so we can see that $T = \{x, y\}$ is maximally independent modulo I.

Since by Lemma 4.2.8 the extension of I to $K(x, y)[z]$ is zero-dimensional, we can use Algorithm 3.3.5, zeroRadical$(\{f, g\})$ in $K(x, y)[z]$. For this, we have to determine the monic generator h and then the squarefree part of h. Since the elements of G are univariate $K(x, y)[z]$, we just pick the element with the lowest degree in terms of z, which is $h = -z^2 + yz$. To get the squarefree part of h, we first compute $\gcd(h, h') = \gcd(-z^2 + yz, -2z + y)$, which is equal to 1, since $-2z + y$ is irreducible in $K(x, y)[z]$ and it doesn't divide h. We therefore conclude that h is already squarefree and thus $R = \{x^2 + 2xz^2 + z^4, -z^2 + yz\}$ is a generating set of the radical $\sqrt{I^e}$.

Next, we compute the contraction of $\sqrt{I^e}$ to $K[x, y, z]$ using Algorithm 4.2.10, cont$(R, \{x, y\})$. Since the lexicographic ordering $\leq$, with the right order of variables, is a block ordering with the monomial ordering on $K[z]$ dominating, $H = R$ is already a suitable Gröbner basis of $\sqrt{I^e}$. It is clear that $H \subseteq K[x, y, z]$, but we can also see it by noting that all denominators of the coefficients of elements $h \in H$ are 1 and therefore their least common multiple is 1. We now set $f :=$ lcm$\{lc_{\{z\}}(h) \mid h \in H\}$, from which we get $f =$ lcm$\{lc_{\{z\}}(z^4 + 2xz^2 + x^2), lc_{\{z\}}(-z^2 + yz)\} =$ lcm$\{1, -1\} = 1$.

With this, we now compute the colon ideal $\sqrt{I^e} : f^\infty$ using Algorithm 4.1.5, colondIdeal(H, f). To do this, we must compute a Gröbner basis of the ideal generated by $H \cup \{1 - tf\}$ with respect to a $\{t\}$-elimination ordering, where t is a temporary variable. For this we can again use the lexicographic ordering and get $H^* = \{x^2 + 2xz^2 + z^4, -z^2 + yz, t - 1\}$. The $\{x, y, z\}$-elimination ideal clearly has $G^* = \{x^2 + 2xz^2 + z^4, -z^2 + yz\}$ as a Gröbner basis again. Since $G^* = H$, it is clear that the r from step (3) in the algorithm is 0. However, as Algorithm 4.2.10 doesn't use the r, it doesn't matter what r is for now. We conclude that in step (5), we get $C = \{x^2 + 2xz^2 + z^4, -z^2 + yz\}$.

We are now at step (6) in radical(S), where we use Algorithm 4.2.13 to calculate $(f, r) =$ extCont$(S, \{x, y\})$ such that $(S) = (S, f^r) \cap (S)^{ec}$. As the Gröbner basis G in Algorithm 4.2.13 is the same as the one we have computed at the beginning of this example and that we've been using for the previous steps, we can see that the f and r we computed in the previous step, are the same as the ones that we need now.

At last, using Algorithm 2.2.11, we compute a Gröbner basis of the intersection of the ideal generated by C and Algorithm 4.3.1 applied to $S^* := S \cup \{f^r\}$. Since $f = 1$, we obviously get $1 \in S^*$ and thus radical$(S^*) = \{1\}$. In order to compute int(radical$(S^*), C)$, we need to introduce the temporary variables t and s. We then compute the $\{x, y, z\}$-elimination ideal of the ideal J generated by $1 - (t + s) \cup t\{1\} \cup sC$. For this we need a Gröbner basis G' of J with respect to a $\{x, y, z\}$-elimination ordering. As always we use the lexicographic ordering and get $G' = \{s - 1, t, x^2 + 2xz^2 + z^4, -z^2 + yz\}$. For the Gröbner basis of the elimination ideal, we unsurprisingly get $G'_{\{x,y,z\}} = \{x^2 + 2xz^2 + z^4, -z^2 + yz\}$ again. And thus

$$\{x^2 + 2xz^2 + z^4, -z^2 + yz\}$$

is a Gröbner basis of the radical of $I = (x^2 + 2xyz + z^4, yz - z^2)$. Since this was also a Gröbner basis of I, we can conclude that I was a radical ideal all along.

From this example, we could see that the algorithm we presented is far from optimal and one can easily see several ways to skip redundant steps. However, as we've mentioned before, our goal in this thesis was not to find a computationally efficient algorithm, but to demonstrate the theory behind computing radical ideals and to present an algorithm that computes them.

Bibliography

[BW93] T. Becker and V. Weißpfenning. *Gröbner bases*. New York: Springer, 1993.

[EHV92] D. Eisenbud, C. Huneke, and W. Vasconcelos. "Computing the radical of an ideal in positive characteristic". In: *Journal of Symbolic Computation* (1992).

[GT96] P. Gianni and B. Trager. "Square-Free Algorithms in Positive Characteristic". In: *Applicable Algebra in Engineering, Communication and Computing* (1996).

[Gra70] M. W. Gray. *A Radical Approach to Algebra*. Addison-Wesley, 1970.

[Kem11] G. Kemper. *A course in commutative algebra*. Heidelberg: Springer, 2011.

[Kem02] G. Kemper. "The Calculation of Radical Ideals in Positive Characteristic". In: *Journal of Symbolic Computation* (2002).

[Mat01] R. Matsumoto. "Computing the radical of an ideal in positive characteristic". In: *Journal of Symbolic Computation* (2001).