

Preface

Invariant theory is a subject with a long tradition and an astounding ability to rejuvenate itself whenever it reappears on the mathematical stage. Throughout the history of invariant theory, two features of it have always been at the center of attention: computation and applications. This book is about the computational aspects of invariant theory. We present algorithms for calculating the invariant ring of a group that is linearly reductive or finite, including the modular case. These algorithms form the central pillars around which the book is built. To prepare the ground for the algorithms, we present Gröbner basis methods and some general theory of invariants. Moreover, the algorithms and their behavior depend heavily on structural properties of the invariant ring to be computed. Large parts of the book are devoted to studying such properties. Finally, most of the applications of invariant theory depend on the ability to calculate invariant rings. The last chapter of this book provides a sample of applications inside and outside of mathematics.

Acknowledgments. Vladimir Popov and Bernd Sturmfels brought us together as a team of authors. In early 1999 Vladimir Popov asked us to write a contribution on algorithmic invariant theory for Springer's Encyclopaedia series. After we agreed to do that, it was an invitation by Bernd Sturmfels to spend two weeks together in Berkeley that really got us started on this book project. We thank Bernd for his strong encouragement and very helpful advice. During the stay at Berkeley, we started outlining the book, making decisions about notation, etc. After that, we worked separately and communicated by e-mail. Most of the work was done at MIT, Queen's University at Kingston, Ontario, Canada, the University of Heidelberg, and the University of Michigan at Ann Arbor. In early 2001 we spent another week together at Queen's University, where we finalized most of the book. Our thanks go to Eddy Campbell, Ian Hughes, and David Wehlau for inviting us to Queen's.

The book benefited greatly from numerous comments, suggestions, and corrections we received from a number of people who read a pre-circulated version. Among these people are Karin Gatermann, Steven Gilbert, Julia Hartmann, Gerhard Hiß, Jürgen Klüners, Hanspeter Kraft, Martin Lorenz, Kay Magaard, Gunter Malle, B. Heinrich Matzat, Vladimir Popov, Jim Shank, Bernd Sturmfels, Nicolas Thiéry, David Wehlau, and Jerzy Weyman.

We owe them many thanks for working through the manuscript and offering their expertise. The first author likes to thank the National Science Foundation for partial support under the grant 0102193. Last but not least, we are grateful to the anonymous referees for further valuable comments and to Ms. Ruth Allewelt and Dr. Martin Peters at Springer-Verlag for the swift and efficient handling of the manuscript.

Ann Arbor and Heidelberg,
March 2002

Harm Derksen
Gregor Kemper

1 Constructive Ideal Theory

In this chapter we will provide the basic algorithmic tools which will be used in later chapters. More precisely, we introduce some algorithms of constructive ideal theory, almost all of which are based on Gröbner bases. As the reader will find out, these algorithms and thus Gröbner bases literally permeate this book. When Sturmfels' book [239] was published, not much introductory literature on Gröbner bases and their applications was available. In contrast, we now have the books by Becker and Weispfenning [15], Adams and Loustaunau [6], Cox et al. [48], Vasconcelos [250], Cox et al. [49], Kreuzer and Robbiano [155], and a chapter from Eisenbud [59]. This list of references could be continued further. We will draw heavily on these sources and restrict ourselves to giving a rather short overview of the part of the theory that we require. The algorithms introduced in Sections 1.1–1.3 of this chapter have efficient implementations in various computer algebra systems, such as CoCoA [40], MACAULAY (2) [97], MAGMA [24], or SINGULAR [99], to name just a few, rather specialized ones. The normalization algorithm explained in Section 1.6 is implemented in MACAULAY and SINGULAR.

We will be looking at ideals $I \subseteq K[x_1, \dots, x_n]$ in a polynomial ring over a field K . For polynomials $f_1, \dots, f_k \in K[x_1, \dots, x_n]$, the ideal generated by the f_i will be denoted by $(f_1, \dots, f_k)K[x_1, \dots, x_n]$ or by (f_1, \dots, f_k) if no misunderstanding can arise. The algorithms in this chapter will be mostly about questions in algebraic geometry, so let us introduce some basic notation. An **affine variety** is a subset X of the n -dimensional affine space $\mathbb{A}^n = \mathbb{A}^n(K) := K^n$ defined by a set $S \subseteq K[x_1, \dots, x_n]$ of polynomials as

$$X = \mathcal{V}(S) := \{(\xi_1, \dots, \xi_n) \in K^n \mid f(\xi_1, \dots, \xi_n) = 0 \text{ for all } f \in S\}.$$

When we talk about varieties, we usually assume that K is algebraically closed. (Otherwise, we could work in the language of schemes.) The **Zariski topology** on \mathbb{A}^n is defined by taking the affine varieties as closed sets. An affine variety (or any other subset of \mathbb{A}^n) inherits the Zariski topology from \mathbb{A}^n . A non-empty affine variety X is called **irreducible** if it is not the union of two non-empty, closed proper subsets. (In the literature varieties are often defined to be irreducible, but we do not make this assumption here.) The (Krull-) **dimension** of X is the maximal length k of a strictly increasing chain

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_k \subseteq X$$

of irreducible closed subsets.

For an affine variety $X = \mathcal{V}(S)$, let I be the radical ideal of the ideal in $K[x_1, \dots, x_n]$ generated by S . Then $X = \mathcal{V}(I)$, and the quotient ring $K[X] := K[x_1, \dots, x_n]/I$ is called the **coordinate ring**. X is irreducible if and only if $K[X]$ is an integral domain, and the dimension of X equals the Krull dimension of $K[X]$, i.e., the maximal length of a strictly increasing chain of prime ideals in $K[X]$. By Hilbert's Nullstellensatz, we can identify $K[X]$ with a subset of the ring K^X of functions from X into K . Elements from $K[X]$ are called **regular functions** on X . If X and Y are affine varieties, a **morphism** $\varphi: X \rightarrow Y$ is a mapping from X into Y such that the image of the induced mapping

$$\varphi^*: K[Y] \rightarrow K^X, \quad f \mapsto f \circ \varphi,$$

lies in $K[X]$.

1.1 Ideals and Gröbner Bases

In this section we introduce the basic machinery of monomial orderings and Gröbner bases.

1.1.1 Monomial Orderings

By a **monomial** in $K[x_1, \dots, x_n]$ we understand an element of the form $x_1^{e_1} \cdots x_n^{e_n}$ with e_i non-negative integers. Let M be the set of all monomials. A **term** is an expression $c \cdot t$ with $0 \neq c \in K$ and $t \in M$. Thus every polynomial is a sum of terms.

Definition 1.1.1. *A monomial ordering is a total order " $>$ " on M satisfying the following conditions:*

- (i) $t > 1$ for all $t \in M \setminus \{1\}$,
- (ii) $t_1 > t_2$ implies $st_1 > st_2$ for all $s, t_1, t_2 \in M$.

We also use a monomial ordering to compare terms. A non-zero polynomial $f \in K[x_1, \dots, x_n]$ can be written uniquely as $f = ct + g$ such that $t \in M$, $c \in K \setminus \{0\}$, and every term of g is smaller (with respect to the order " $>$ ") than t . Then we write

$$\text{LT}(f) = ct, \quad \text{LM}(f) = t, \quad \text{and} \quad \text{LC}(f) = c$$

for the leading term, leading monomial, and leading coefficient of f . For $f = 0$, all three values are defined to be zero.

A monomial ordering is always a well-ordering. This follows from the fact that ideals in $K[x_1, \dots, x_n]$ are finitely generated. We note that the usage of terminology is not uniform in the literature. Some authors (e.g. Becker and Weispfenning [15]) have monomials and terms interchanged, and some speak of initial or head terms, monomials and coefficients. Monomial orderings are often called term orders. When browsing through the literature one can find almost any combination of these pieces of terminology.

Example 1.1.2. We give a few examples of monomial orderings. Let $t = x_1^{e_1} \cdots x_n^{e_n}$ and $t' = x_1^{e'_1} \cdots x_n^{e'_n}$ be two distinct monomials.

- (a) The lexicographic monomial ordering (with $x_1 > x_2 > \cdots > x_n$): t is considered greater than t' if $e_i > e'_i$ for the smallest i with $e_i \neq e'_i$. We sometimes write $t >_{\text{lex}} t'$ in this case. As an example, we have

$$\text{LM}_{\text{lex}}(x_1 + x_2x_4 + x_3^2) = x_1.$$

The lexicographic monomial ordering is useful for solving systems of algebraic equations.

- (b) The graded lexicographic monomial ordering: $t >_{\text{glex}} t'$ if $\deg(t) > \deg(t')$, or if $\deg(t) = \deg(t')$ and $t >_{\text{lex}} t'$. Here $\deg(t)$ is the total degree $e_1 + \cdots + e_n$. For example,

$$\text{LM}_{\text{glex}}(x_1 + x_2x_4 + x_3^2) = x_2x_4.$$

The graded lexicographic monomial ordering can be generalized by using a weighted degree $\deg(t) := w_1e_1 + \cdots + w_n e_n$ with w_i fixed positive real numbers.

- (c) The graded reverse lexicographic monomial ordering (grevlex-ordering for short): $t >_{\text{grevlex}} t'$ if $\deg(t) > \deg(t')$, or if $\deg(t) = \deg(t')$ and $e_i < e'_i$ for the *largest* i with $e_i \neq e'_i$. For example,

$$\text{LM}_{\text{grevlex}}(x_1 + x_2x_4 + x_3^2) = x_3^2.$$

The grevlex ordering is often very efficient for computations. It can also be generalized by using a weighted degree.

- (d) Block orderings: Let $>_1$ be a monomial ordering on the monomials in x_1, \dots, x_r , and $>_2$ a monomial ordering on the monomials in x_{r+1}, \dots, x_n . Then the block ordering formed from $>_1$ and $>_2$ is defined as follows: $t > t'$ if $x_1^{e_1} \cdots x_r^{e_r} >_1 x_1^{e'_1} \cdots x_r^{e'_r}$, or if $x_1^{e_1} \cdots x_r^{e_r} = x_1^{e'_1} \cdots x_r^{e'_r}$ and $x_{r+1}^{e_{r+1}} \cdots x_n^{e_n} >_2 x_{r+1}^{e'_{r+1}} \cdots x_n^{e'_n}$. For example, the lexicographic monomial ordering is a block ordering. Block orderings are useful for the computation of elimination ideals (see Section 1.2). ◁

We say that a monomial ordering is **graded** if $\deg(t) > \deg(t')$ implies $t > t'$. So the orderings in (b) and (c) of the previous example are graded.

Given a monomial ordering, we write $x_i \gg x_j$ if $x_i > x_j^e$ for all non-negative integers e . For example, in the lexicographic monomial ordering we

have $x_1 \gg x_2 \gg \cdots \gg x_n$. Moreover, if “ \gg ” is a block ordering with blocks x_1, \dots, x_r and x_{r+1}, \dots, x_n , then $x_i \gg x_j$ for $i \leq r$ and $j > r$. If $x_i \gg x_j$ for all $j \in J$ for some $J \subset \{1, \dots, n\}$, then x_i is greater than any monomial in the indeterminates $x_j, j \in J$. This follows directly from Definition 1.1.1.

1.1.2 Gröbner Bases

We fix a monomial ordering on $K[x_1, \dots, x_n]$.

Definition 1.1.3. Let $S \subseteq K[x_1, \dots, x_n]$ be a set of polynomials. We write

$$L(S) = (\text{LM}(g) \mid g \in S)$$

for the ideal generated by the leading monomials from S . $L(S)$ is called the **leading ideal** of S (by some authors also called the *initial ideal*).

Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal. Then a finite subset $\mathcal{G} \subseteq I$ is called a **Gröbner basis** of I (with respect to the chosen monomial ordering) if

$$L(I) = L(\mathcal{G}).$$

It is clear that a Gröbner basis of I generates I as an ideal. Indeed, a (hypothetical) element $f \in I \setminus (\mathcal{G})$ with minimal leading monomial could be transformed into $g \in I \setminus (\mathcal{G})$ with smaller leading monomial by subtracting a multiple of an element from \mathcal{G} , which yields a contradiction. It is also clear that Gröbner bases always exist. Indeed, $\{\text{LM}(f) \mid f \in I\}$ generates $L(I)$ by definition, hence by the Noether property a finite subset $\{\text{LM}(f_1), \dots, \text{LM}(f_m)\}$ also generates $L(I)$, and so $\{f_1, \dots, f_m\}$ is a Gröbner basis. This argument, however, is non-constructive. But we will see in Section 1.1.4 that there is in fact an algorithm for computing Gröbner bases.

The most obvious question about an ideal $I \subseteq K[x_1, \dots, x_n]$ that can be decided with Gröbner bases is whether $I = K[x_1, \dots, x_n]$. Indeed, this is the case if and only if \mathcal{G} contains a (non-zero) constant polynomial.

1.1.3 Normal Forms

A central element in the construction and usage of Gröbner bases is the computation of so-called normal forms.

Definition 1.1.4. Let $S \subseteq K[x_1, \dots, x_n]$ be a set of polynomials.

- (a) A polynomial $f \in K[x_1, \dots, x_n]$ is said to be in **normal form** with respect to S if no term of f is divisible by the leading monomial of any $g \in S$.
- (b) If f and \tilde{f} are polynomials in $K[x_1, \dots, x_n]$, then \tilde{f} is said to be a **normal form** of f with respect to S if \tilde{f} is in normal form with respect to S and $f - \tilde{f}$ lies in the ideal generated by S .

The following algorithm, which mimics division with remainder in the univariate case, calculates a normal form with respect to a finite set S of polynomials.

Algorithm 1.1.5 (Normal form). Given a polynomial $f \in K[x_1, \dots, x_n]$ and a finite subset $S = \{g_1, \dots, g_s\} \subset K[x_1, \dots, x_n]$, perform the following steps to obtain a normal form \tilde{f} of f with respect to S , together with polynomials $h_1, \dots, h_s \in K[x_1, \dots, x_n]$ such that

$$f = \tilde{f} + \sum_{i=1}^s h_i g_i.$$

- (1) Set $\tilde{f} := f$ and $h_i := 0$ for all i , and repeat the steps (2)–(4).
- (2) If no term of \tilde{f} is divisible by the leading monomial of any $g_i \in S$, return \tilde{f} as a normal form of f , and return the h_i .
- (3) Let ct be the maximal term of \tilde{f} such that there exists $g_i \in S$ with $\text{LM}(g_i)$ dividing t .
- (4) Set

$$\tilde{f} := \tilde{f} - \frac{ct}{\text{LT}(g_i)} g_i \quad \text{and} \quad h_i := h_i + \frac{ct}{\text{LT}(g_i)}.$$

Of course the computation of the h_i can be omitted if only a normal form is desired. The termination of Algorithm 1.1.5 is guaranteed by the fact that the maximal monomials t of \tilde{f} divisible by some $\text{LM}(g_i)$ form a strictly decreasing sequence, but such a sequence is finite by the well-ordering property. The result of Algorithm 1.1.5 is in general not unique, since it depends on the choice of the g_i in step (3). However, if \mathcal{G} is a Gröbner basis of an ideal I , then normal forms with respect to \mathcal{G} are unique. In fact, if \tilde{f} and \hat{f} are two normal forms of f with respect to \mathcal{G} , then $\tilde{f} - \hat{f} \in I$, so $\text{LM}(\tilde{f} - \hat{f})$ is divisible by some $\text{LM}(g)$ with $g \in \mathcal{G}$. But if $\tilde{f} \neq \hat{f}$, then $\text{LM}(\tilde{f} - \hat{f})$ must appear as a monomial in \tilde{f} or \hat{f} , contradicting the fact that \tilde{f} and \hat{f} are in normal form. In the case of a Gröbner basis \mathcal{G} we write $\tilde{f} =: \text{NF}(f) = \text{NF}_{\mathcal{G}}(f)$ for the normal form.

It should be mentioned that there is a variant of the normal form algorithm which stops when the leading term of \tilde{f} is zero or not divisible by any $\text{LM}(g)$, $g \in S$ (“top-reduction”).

Using Algorithm 1.1.5, we obtain a membership test for ideals.

Algorithm 1.1.6 (Membership test in ideals). Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal, \mathcal{G} a Gröbner basis of I , and $f \in K[x_1, \dots, x_n]$ a polynomial. Then

$$f \in I \iff \text{NF}_{\mathcal{G}}(f) = 0.$$

One can also substitute $\text{NF}_{\mathcal{G}}(f)$ by the result of top-reducing f .

Thus the map $\text{NF}_{\mathcal{G}}: K[x_1, \dots, x_n] \rightarrow K[x_1, \dots, x_n]$ is K -linear with kernel I , and therefore provides a way to perform explicit calculations in the

quotient ring $K[x_1, \dots, x_n]/I$. In fact, this was the main objective for which Gröbner bases were invented.

A Gröbner basis \mathcal{G} of an ideal I can be transformed into a **reduced Gröbner basis** by iteratively substituting an element from \mathcal{G} by a normal form with respect to the other elements, until every element is in normal form. After deleting zero from the resulting set and making all leading coefficients equal to 1, the resulting monic reduced Gröbner basis is unique (i.e., it only depends on I and the chosen monomial ordering, see Becker and Weispfenning [15, Theorem 5.43]).

1.1.4 The Buchberger Algorithm

In order to present Buchberger's algorithm for the construction of Gröbner bases, we need to introduce s-polynomials. Let $f, g \in K[x_1, \dots, x_n]$ be two non-zero polynomials, and set $t := \text{lcm}(\text{LM}(f), \text{LM}(g))$ (the least common multiple). Then the **s-polynomial** of f and g is defined as

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

Note that the coefficients of t cancel in $\text{spol}(f, g)$, and that $\text{spol}(f, g) \in (f, g)$. The following lemma is the key step toward finding an algorithm for the construction of a Gröbner basis.

Lemma 1.1.7 (Buchberger [32]). *Let \mathcal{G} be a basis (=generating set) of an ideal $I \subseteq K[x_1, \dots, x_n]$. Then the following conditions are equivalent.*

- (a) \mathcal{G} is a Gröbner basis of I .
- (b) If $f, g \in \mathcal{G}$, then $\text{spol}(f, g)$ has 0 as a normal form with respect to \mathcal{G} .
- (c) If $f, g \in \mathcal{G}$, then every normal form of $\text{spol}(f, g)$ with respect to \mathcal{G} is 0.

See Becker and Weispfenning [15, Theorem 5.48] for a proof. We can give Buchberger's algorithm in a rather coarse form now.

Algorithm 1.1.8 (Buchberger's algorithm). Given a finite basis S for an ideal $I \subseteq K[x_1, \dots, x_n]$, construct a Gröbner basis (with respect to a given monomial ordering) by performing the following steps:

- (1) Set $\mathcal{G} := S$ and repeat steps (2)–(4).
- (2) For $f, g \in \mathcal{G}$ compute a normal form h of $\text{spol}(f, g)$ with respect to \mathcal{G} .
- (3) If $h \neq 0$, include h into \mathcal{G} .
- (4) If h was found to be zero for all $f, g \in \mathcal{G}$, then \mathcal{G} is the desired Gröbner basis.

This algorithm terminates after a finite number of steps since $L(S)$ strictly increases with every performance of steps (2)–(4).

Remark 1.1.9. The theoretical cost of Buchberger’s algorithm is extremely high. In fact, no general upper bound for the running time is known. But Möller and Mora [168] proved an upper bound for the maximal degree of the Gröbner basis elements which depends doubly exponentially on the number of variables. They also proved that this doubly exponential behavior cannot be improved. What makes things even worse is the phenomenon of “intermediate expression swell”, meaning that during the computation the number and size of polynomials can become much bigger than in the final result. It is known that the memory space required for the computation of Gröbner bases increases at most exponentially with the size of the input, and all problems with this behavior can be reduced to the problem of testing ideal membership; so the problem of computing Gröbner bases is “EXPSPACE-complete”. We refer to von zur Gathen and Gerhard [79, Section 21.7] for a more detailed account of what is known about the complexity of Gröbner bases.

In spite of all this bad news, practical experience shows that the algorithm often terminates after a reasonable time (although this is usually not predictable in advance). Much depends on improvements of the algorithm given above, such as omitting some pairs f, g (by Buchberger’s first and second criterion, see Becker and Weispfenning [15, Section 5.5]), by having a good strategy which pairs to treat first, and by choosing a suitable monomial ordering (if there is any freedom of choice). There are also algorithms which transform a Gröbner basis with respect to one monomial ordering into one with respect to another ordering (see Faugère et al. [66], Collart et al. [46]).
◁

There is a variant of Buchberger’s algorithm which keeps track of how the polynomials in the Gröbner basis \mathcal{G} arise as linear combinations of the polynomials in the original ideal basis S . This variant is called the extended Buchberger algorithm, and its output is an (ordered) Gröbner basis $\mathcal{G} = \{g_1, \dots, g_r\}$ and an $r \times s$ -matrix A with coefficients in $K[x_1, \dots, x_n]$ such that

$$\begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix} = A \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix},$$

where $S = \{f_1, \dots, f_s\}$. On the other hand, it is straightforward to obtain an $s \times r$ -matrix B such that $(f_1, \dots, f_s)^{\text{tr}} = B(g_1, \dots, g_r)^{\text{tr}}$ by applying the Normal Form Algorithm 1.1.5 to the f_i .

1.2 Elimination Ideals

Given an ideal $I \subseteq K[x_1, \dots, x_n]$ and an integer $k \in \{1, \dots, n\}$, the **elimination ideal** of I with respect to x_k, \dots, x_n is defined as the intersection $I \cap K[x_1, \dots, x_k]$. It has the following geometric interpretation: If

$$\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-k+1}, (\xi_1, \dots, \xi_n) \mapsto (\xi_k, \dots, \xi_n)$$

is the canonical projection, then for K algebraically closed we have

$$\overline{\pi(\mathcal{V}(I))} = \mathcal{V}(I \cap K[x_k, \dots, x_n]), \quad (1.2.1)$$

where the left hand side is the Zariski-closure. (In scheme theoretic language, π is the intersection of a prime ideal in $K[x_1, \dots, x_n]$ with $K[x_k, \dots, x_n]$, and we do not need the hypothesis that K is algebraically closed.) An important feature of Gröbner bases is that they can be used to compute elimination ideals.

Algorithm 1.2.1 (Computing elimination ideals). Given an ideal $I \subseteq K[x_1, \dots, x_n]$ and an integer $k \in \{1, \dots, n\}$, compute the elimination ideal $I \cap K[x_k, \dots, x_n]$ as follows:

- (1) Choose a monomial ordering such that $x_i \gg x_j$ for $i < k$ and $j \geq k$ (e.g., the lexicographic monomial ordering or a block ordering).
- (2) Compute a Gröbner basis \mathcal{G} of I with respect to this monomial ordering.
- (3) $\mathcal{G} \cap K[x_k, \dots, x_n]$ is a Gröbner basis of $I \cap K[x_1, \dots, x_n]$.

It is elementary to see that this algorithm is correct (see Becker and Weispfenning [15, Proposition 6.15]). Equation (1.2.1) shows how elimination ideals can be used to solve a system of algebraic equations with a finite set of solutions.

We continue by presenting some applications of elimination ideals (and thus of Gröbner bases) which will be needed in the following chapters of this book.

1.2.1 Image Closure of Morphisms

Let X and Y be affine varieties and $f: X \rightarrow Y$ a morphism. (Again we assume that K is algebraically closed or use the language of schemes.) We want to compute the Zariski-closure of the image $f(X)$. Assume that X is embedded into \mathbb{A}^n and Y into \mathbb{A}^m for some n and m . Without loss of generality we can assume that $Y = \mathbb{A}^m$. If f is given by polynomials (f_1, \dots, f_m) with $f_i \in K[x_1, \dots, x_n]$, and X is given by an ideal $I \subseteq K[x_1, \dots, x_n]$, then the graph of f is given by the ideal

$$J := I \cdot K[x_1, \dots, x_n, y_1, \dots, y_m] + (f_1 - y_1, \dots, f_m - y_m)$$

in $K[x_1, \dots, x_n, y_1, \dots, y_m]$. Thus by Equation (1.2.1), the closure of the image is

$$\overline{f(X)} = \mathcal{V}(J \cap K[y_1, \dots, y_m])$$

(see Vasconcelos [250, Proposition 2.1.3]), and can therefore be calculated by Algorithm 1.2.1.

1.2.2 Relations Between Polynomials

A further application of elimination ideals is the computation of relations between polynomials. More precisely, let $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ be polynomials. We are interested in the kernel of the homomorphism

$$\Phi: K[t_1, \dots, t_m] \rightarrow K[x_1, \dots, x_n], \quad t_i \mapsto f_i,$$

of K -algebras (where t_1, \dots, t_m are further indeterminates). The answer is as follows: Define the ideal

$$I := (f_1 - t_1, \dots, f_m - t_m)$$

in $K[x_1, \dots, x_n, t_1, \dots, t_m]$. Then it is easy to show that

$$\ker(\Phi) = I \cap K[t_1, \dots, t_m], \quad (1.2.2)$$

so the desired kernel is again an elimination ideal (see Eisenbud [59, Proposition 15.30]). Notice that generators for $\ker(\Phi)$ together with the f_i provide a presentation of the algebra generated by the f_i .

1.2.3 The Intersection of Ideals

The intersection of two ideals $I, J \subseteq K[x_1, \dots, x_n]$ (which geometrically corresponds to the union of varieties) can be computed as follows: With a new indeterminate t , form the ideal L in $K[x_1, \dots, x_n, t]$ generated by

$$I \cdot t + J \cdot (1 - t),$$

where the products are formed by multiplying each generator of I and J by t and $1 - t$, respectively. Then

$$I \cap J = L \cap K[x_1, \dots, x_n] \quad (1.2.3)$$

(see Vasconcelos [250, Corollary 2.1.1]). A different method for computing the intersection of I and J involves the calculation of a syzygy module (see Vasconcelos [250, page 29]). We can apply any of these methods iteratively to obtain the intersection of a finite number of ideals, but there is also a direct method (involving further auxiliary indeterminates) given by Becker and Weispfenning [15, Corollary 6.20].

1.2.4 The Quotient of Ideals

Given two ideals $I, J \subseteq K[x_1, \dots, x_n]$, it is often important to be able to calculate the **quotient ideal**

$$I : J := \{g \in K[x_1, \dots, x_n] \mid gf \in I \forall f \in J\}.$$

Sometimes $I : J$ is also referred to as the colon ideal. The quotient ideal has the following geometric interpretation: If I is a radical ideal and K is algebraically closed, then $I : J$ is precisely the ideal of all polynomials vanishing on $\mathcal{V}(I) \setminus \mathcal{V}(J)$. The quotient ideal is also of crucial importance for the computation of radical ideals (see Section 1.5) and primary decomposition.

If $J = (f)$ is a principal ideal, we sometimes write $I : f$ for the quotient ideal $I : (f)$. If $J = (f_1, \dots, f_k)$, then clearly

$$I : J = \bigcap_{i=1}^k I : f_i,$$

which reduces the task to the case that J is a principal ideal. But clearly

$$I : f = (I \cap (f)) \cdot f^{-1} \quad (1.2.4)$$

(see Vasconcelos [250, Proposition 2.1.4(a)]), which can be computed by Equation (1.2.3). Thus quotient ideals can be obtained by using any algorithm for the intersection of ideals.

For an ideal $I \subseteq K[x_1, \dots, x_n]$ and a polynomial $f \in K[x_1, \dots, x_n]$ we can also consider the ideal

$$I : f^\infty := \bigcup_{i \in \mathbb{N}} I : f^i,$$

which is sometimes referred to as the saturation ideal of I with respect to f . The saturation ideal can be calculated by successively computing the quotient ideals $J_i := I : f^i = J_{i-1} : f$. This gives an ascending chain of ideals, thus eventually we get $J_{k+1} = J_k$, so $I : f^\infty = J_k$. But there is a more efficient algorithm, based on the following proposition.

Proposition 1.2.2. *Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal and $f \in K[x_1, \dots, x_n]$ a polynomial. Introduce an additional indeterminate t and form the ideal J in $K[x_1, \dots, x_n, t]$ generated by I and $tf - 1$. Then*

$$I : f^\infty = J \cap K[x_1, \dots, x_n].$$

A proof can be found in Becker and Weispfenning [15, Proposition 6.37].

1.2.5 The Krull Dimension

We define the dimension of an ideal $I \subseteq K[x_1, \dots, x_n]$ to be the Krull dimension of the quotient $K[x_1, \dots, x_n]/I$. There is a method which computes the dimension by using elimination ideals (Becker and Weispfenning [15, Section 6.3]). However, this technique involves a large number of Gröbner basis computations and is therefore not very efficient. A better algorithm (also given in the book of Becker and Weispfenning [15]) is based on the following lemma, which follows from Cox et al. [48, Proposition 4 of Chapter 9, §3].

Lemma 1.2.3. *If “ $>$ ” is a graded monomial ordering, then the dimensions of I and of the leading ideal $L(I)$ coincide.*

To prove this lemma, one uses the fact that the normal form provides an isomorphism of K -vector spaces (not of algebras) between $K[x_1, \dots, x_n]/I$ and $K[x_1, \dots, x_n]/L(I)$. Lemma 1.2.3 reduces our problem to the computation of the dimension of $L(I)$, which is a monomial ideal. But the variety defined by a monomial ideal is a finite union of so-called coordinate subspaces, i.e., varieties of the form $\mathcal{V}(\mathcal{M})$ with $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$. Clearly such a variety is contained in the zero set of the monomial ideal J if and only if every generator of J involves at least one variable x_i lying in \mathcal{M} . We obtain the following algorithm (see Cox et al. [48, Proposition 3 of Chapter 9, §1]).

Algorithm 1.2.4 (Dimension of an ideal).

Given an ideal $I \subseteq K[x_1, \dots, x_n]$, calculate the dimension of I by performing the following steps:

- (1) Compute a Gröbner basis \mathcal{G} of I with respect to a graded monomial ordering.
- (2) If \mathcal{G} contains a non-zero constant, then $I = K[x_1, \dots, x_n]$, and the dimension is (by convention) -1 .
- (3) Otherwise, find a subset $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$ of minimal cardinality such that for every non-zero $g \in \mathcal{G}$ the leading monomial $\text{LM}(g)$ involves at least one variable from \mathcal{M} .
- (4) The dimension of I is $n - |\mathcal{M}|$.

Step (3) of the above algorithm is purely combinatorial and therefore usually much faster than the Gröbner basis computation. An optimized version of this step can be found in Becker and Weispfenning [15, Algorithm 9.6].

The set $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$ occurring in Algorithm 1.2.4 has an interesting interpretation. In fact, let $\mathcal{M}' := \{x_1, \dots, x_n\} \setminus \mathcal{M}$ be the complement of \mathcal{M} . Then for every non-zero $g \in \mathcal{G}$ the leading monomial $\text{LM}(g)$ involves at least one variable *not* in \mathcal{M}' . This implies that every non-zero polynomial in $L(I)$ involves a variable not in \mathcal{M}' , so $L(I) \cap K[\mathcal{M}'] = \{0\}$. From this it follows that

$$I \cap K[\mathcal{M}'] = \{0\}. \quad (1.2.5)$$

Indeed, if $f \in I \cap K[\mathcal{M}']$ were non-zero, then $\text{LM}(f)$ would lie in $L(I) \cap K[\mathcal{M}']$. Subsets $\mathcal{M}' \subseteq \{x_1, \dots, x_n\}$ which satisfy (1.2.5) are called independent modulo I (see Becker and Weispfenning [15, Definition 6.46]). Consider the rational function field $L := K(\mathcal{M}')$ in the variables lying in \mathcal{M}' , and let $L[\mathcal{M}]$ be the polynomial ring over L in the variables from \mathcal{M} . Then (1.2.5) is equivalent to the condition that the ideal $IL[\mathcal{M}]$ generated by I in $L[\mathcal{M}]$ is not equal to $L[\mathcal{M}]$. Since we have $|\mathcal{M}'| = \dim(I)$, it follows that \mathcal{M}' is *maximally* independent modulo I . (Indeed, if there existed a strict superset $\mathcal{N} \supsetneq \mathcal{M}'$ of variables which is independent modulo I , the \mathcal{N} would also be independent modulo some minimal prime P containing I . But this would imply that the transcendence degree of $K[x_1, \dots, x_n]/P$ is at least $|\mathcal{N}|$, hence by Eisenbud [59,

Section 8.2, Theorem A] we would get $\dim(I) \geq \dim(P) \geq |\mathcal{N}| > |\mathcal{M}'|$.) The maximality of \mathcal{M}' means that no non-empty subset of \mathcal{M} is independent modulo $IL[\mathcal{M}]$. By Algorithm 1.2.4, the dimension of $IL[\mathcal{M}]$ must therefore be zero. Thus we have shown:

Proposition 1.2.5. *Let $I \subsetneq K[x_1, \dots, x_n]$ be an ideal and $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$ as in Algorithm 1.2.4. Set $\mathcal{M}' := \{x_1, \dots, x_n\} \setminus \mathcal{M}$, and take the rational function field $L := K(\mathcal{M}')$ in the variables lying in \mathcal{M}' , and the polynomial ring $L[\mathcal{M}]$. Then the ideal $J := IL[\mathcal{M}]$ generated by I in $L[\mathcal{M}]$ is not equal to $L[\mathcal{M}]$, and $\dim(J) = 0$.*

1.3 Syzygy Modules

In this section we write $R := K[x_1, \dots, x_n]$ for the polynomial ring and R^k for a free R -module of rank k . The standard basis vectors of R^k are denoted by e_1, \dots, e_k . Given polynomials $f_1, \dots, f_k \in R$, we ask for the set of all $(h_1, \dots, h_k) \in R^k$ such that $h_1 f_1 + \dots + h_k f_k = 0$. This set is a submodule of R^k , called the **syzygy module** of f_1, \dots, f_k and denoted by $\text{Syz}(f_1, \dots, f_k)$. More generally, we ask for the kernel of an R -homomorphism $\varphi: R^k \rightarrow R^l$ between two free R -modules. If $f_i := \varphi(e_i) \in R^l$, then the kernel of φ consists of all $(h_1, \dots, h_k) \in R^k$ with $h_1 f_1 + \dots + h_k f_k = 0$. Again $\text{Syz}(f_1, \dots, f_k) := \ker(\varphi)$ is called the syzygy module of the f_i .

1.3.1 Computing Syzygies

In order to explain an algorithm which computes syzygy modules, we have to give a brief introduction into Gröbner bases of submodules of R^k . A **monomial** in R^k is an expression of the form te_i with t a monomial in R . The notion of a monomial ordering is given as in Definition 1.1.1, with condition (i) replaced by $te_i > e_i$ for all i and $1 \neq t$ a monomial in R , and demanding (ii) for monomials $t_1, t_2 \in R^k$ and $s \in R$. Given a monomial ordering, we can now define the leading submodule $L(M)$ of a submodule $M \subseteq R^k$ and the concept of a Gröbner basis of M as in Definition 1.1.3. Normal forms are calculated by Algorithm 1.1.5, with the extra specification that te_i is said to be divisible by $t'e_j$ if $i = j$ and t divides t' , so the quotients are always elements in R . Moreover, the s-polynomial of f and $g \in R^k$ with $\text{LM}(f) = te_i$ and $\text{LM}(g) = t'e_j$ is defined to be zero if $i \neq j$. With these provisions, Buchberger's algorithm can be formulated as in Algorithm 1.1.8.

Suppose that $\mathcal{G} = \{g_1, \dots, g_k\}$ is a Gröbner basis of a submodule $M \subseteq R^l$. Then for $g_i, g_j \in \mathcal{G}$ we have that $\text{NF}_{\mathcal{G}}(\text{spol}(g_i, g_j)) = 0$, so there exist $h_1, \dots, h_k \in R$ with

$$\text{spol}(g_i, g_j) = h_1 g_1 + \dots + h_k g_k, \quad (1.3.1)$$

and the h_i can be computed by the Normal Form Algorithm 1.1.5. Since $\text{spol}(g_i, g_j)$ is an R -linear combination of g_i and g_j , Equation (1.3.1) yields a syzygy $r_{i,j} \in \text{Syz}(g_1, \dots, g_k)$. Of course $r_{i,j} = 0$ if the leading monomials of g_i and of g_j lie in different components of R^l .

The following monomial ordering “ $>_{\mathcal{G}}$ ” on R^k , which depends on \mathcal{G} , was introduced by Schreyer [210]: te_i is considered bigger than $t'e_j$ if $t\text{LM}(g_i) > t'\text{LM}(g_j)$ (with “ $>$ ” the given ordering on R^l), or if $t\text{LM}(g_i) = t'\text{LM}(g_j)$ and $i < j$. It is easy to see that “ $>_{\mathcal{G}}$ ” satisfies the properties of a monomial ordering.

Theorem 1.3.1 (Schreyer [210]). *Let $\mathcal{G} = \{g_1, \dots, g_k\}$ be a Gröbner basis with respect to an arbitrary monomial ordering “ $>$ ” of a submodule $M \subseteq R^l$. Then, with the above notation, the $r_{i,j}$ ($1 \leq i < j \leq k$) form a Gröbner basis of $\text{Syz}(g_1, \dots, g_k)$ with respect to the monomial ordering “ $>_{\mathcal{G}}$ ”.*

This settles the case of syzygies for Gröbner bases. Now assume that $f_1, \dots, f_k \in R^l$ are arbitrary. Using the extended Buchberger algorithm (see at the end of Section 1.1), we can calculate a Gröbner basis $\{g_1, \dots, g_{k'}\}$ of the submodule generated by f_1, \dots, f_k , along with representations of the g_i as R -linear combinations of the f_j . Using the Normal Form Algorithm 1.1.5, we can also express the f_j in terms of the g_i . The choice of the f_j and g_i is equivalent to giving homomorphisms $R^k \rightarrow R^l$ and $R^{k'} \rightarrow R^l$, and expressing the f_j in terms of the g_i and vice versa is equivalent to giving homomorphisms φ and ψ such that the diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & N & \longrightarrow & R^{k'} & \longrightarrow & R^l \\
 & & & & \uparrow \varphi & & \nearrow \\
 & & & & R^k & & \\
 & & & & \downarrow \psi & &
 \end{array}$$

commutes (both along φ and ψ), where $N := \text{Syz}(g_1, \dots, g_{k'})$ can be computed by Theorem 1.3.1. The following lemma tells us how to compute $\text{Syz}(f_1, \dots, f_k) = \ker(R^k \rightarrow R^l)$.

Lemma 1.3.2. *Let A be a commutative ring and*

$$\begin{array}{ccccccc}
 0 & \longrightarrow & N & \longrightarrow & M_1 & \longrightarrow & M \\
 & & & & \uparrow \varphi & & \nearrow \theta \\
 & & & & M_2 & &
 \end{array}$$

a commutative diagram (both along φ and ψ) of A -modules, with the upper row exact. Then we have an exact sequence

$$0 \longrightarrow (\text{id} - \psi \circ \varphi)(M_1) \longrightarrow N \oplus (\text{id} - \varphi \circ \psi)(M_2) \longrightarrow M_2 \xrightarrow{\theta} M$$

with maps

$$\begin{aligned} (\text{id} - \psi \circ \varphi)(M_1) &\rightarrow N \oplus (\text{id} - \varphi \circ \psi)(M_2), & m &\mapsto (m, -\varphi(m)), & \text{and} \\ N \oplus (\text{id} - \varphi \circ \psi)(M_2) &\rightarrow M_2, & (n, m) &\mapsto \varphi(n) + m. \end{aligned}$$

In particular,

$$\ker(\theta) = \varphi(N) + (\text{id} - \varphi \circ \psi)(M_2).$$

Proof. It follows by a simple diagram chase that $(\text{id} - \psi \circ \varphi)(M_1) \subseteq N$, so the first map is indeed into $N \oplus (\text{id} - \varphi \circ \psi)(M_2)$. We show the exactness at M_2 . Again by a diagram chase $\theta(\varphi(n) + m) = 0$ for $n \in N$ and $m \in (\text{id} - \varphi \circ \psi)(M_2)$. Conversely, for $m \in \ker(\theta)$ we have

$$m = \varphi(\psi(m)) + (\text{id} - \varphi \circ \psi)(m)$$

with $\psi(m) \in N$. To show the exactness at $N \oplus (\text{id} - \varphi \circ \psi)(M_2)$, take $(n, m_2 - \varphi(\psi(m_2))) \in N \oplus (\text{id} - \varphi \circ \psi)(M_2)$ with $\varphi(n) + m_2 - \varphi(\psi(m_2)) = 0$. Then

$$n = (\text{id} - \psi \circ \varphi)(n - \psi(m_2)) \in (\text{id} - \psi \circ \varphi)(M_1),$$

and $(n, -\varphi(n)) = (n, m_2 - \varphi(\psi(m_2)))$. This completes the proof. \square

In summary, we obtain the following algorithm.

Algorithm 1.3.3 (Calculation of a syzygy module). Given elements $f_1, \dots, f_k \in R^l$, perform the following steps to find the syzygy module $\text{Syz}(f_1, \dots, f_k)$:

- (1) Using the extended Buchberger algorithm, calculate a Gröbner basis $\{g_1, \dots, g_{k'}\}$ of the submodule of R^l generated by the f_i together with a matrix $A \in R^{k' \times k}$ such that

$$\begin{pmatrix} g_1 \\ \vdots \\ g_{k'} \end{pmatrix} = A \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix}.$$

- (2) Using the Normal Form Algorithm 1.1.5, compute a matrix $B \in R^{k \times k'}$ with

$$\begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix} = B \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_{k'} \end{pmatrix}.$$

- (3) For $1 \leq i < j \leq k'$, compute the syzygies $r_{i,j} \in \text{Syz}(g_1, \dots, g_{k'})$ given by Equation (1.3.1).
- (4) $\text{Syz}(f_1, \dots, f_k)$ is generated by the $r_{i,j} \cdot A$ and the rows of $I_k - BA$.

1.3.2 Free Resolutions

For a submodule $M \subseteq R^l$ (with $R = K[x_1, \dots, x_n]$ as before) with generating set f_1, \dots, f_k , we can compute generators for $N := \text{Syz}(f_1, \dots, f_k) \subseteq R^k$ by using Algorithm 1.3.3. Continuing by computing the syzygies of these generators and so on, we obtain a free resolution of M , i.e., an exact sequence

$$0 \longrightarrow F_r \longrightarrow F_{r-1} \longrightarrow \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \quad (1.3.2)$$

with the F_i free R -modules. Hilbert's syzygy theorem (see Eisenbud [59, Corollary 19.8] or the "original" reference Hilbert [107]) guarantees that there exists a free resolution of finite length (bounded by n , in fact), as given above. Free resolutions are of great interest because they contain a lot of information about the structure of M . Theorem 1.3.1 provides the following method for calculating a free resolution with only a single Gröbner basis computation.

Algorithm 1.3.4 (Schreyer's algorithm). Let $M \subseteq R^l$ be a submodule given by a generating set. Obtain a free resolution of M as follows:

- (1) Compute a Gröbner basis $\mathcal{G} = \{g_1, \dots, g_k\}$ of M with respect to an arbitrary monomial ordering " $>$ ". Set $i := 0$ and repeat steps (2)–(4).
- (2) Set $F_i := R^k$ and obtain the map $F_i \rightarrow F_{i-1}$ (with $F_{-1} := M$) from (1.3.2) by $(h_1, \dots, h_k) \mapsto h_1g_1 + \cdots + h_kg_k$.
- (3) Compute the relations $r_{i,j}$ from Equation (1.3.1). By Theorem 1.3.1, the $r_{i,j}$ form a Gröbner basis with respect to " $>_{\mathcal{G}}$ " of the kernel of the map defined in (2).
- (4) If all $r_{i,j}$ are zero, the resolution is complete. Otherwise, let $\mathcal{G} \subseteq R^k$ be the set of the non-zero $r_{i,j}$ and set $i := i + 1$.

The termination of Algorithm 1.3.4 after at most n iterations is guaranteed by (the proof of) Theorem 2.1 in Chapter 6 of Cox et al. [49] (which provides a new, constructive proof of Hilbert's syzygy theorem).

Now suppose that the polynomial ring R is made into a graded algebra by defining the degrees $\deg(x_i)$ of the indeterminates to be positive integers. Then the free module R^l can be made into a graded R -module by defining the $\deg(e_i)$ to be integers. Moreover, suppose that M is a graded submodule, i.e., generated by homogeneous elements. Then we want to find a graded free resolution, i.e., one that consists of graded free modules F_i with all mappings degree-preserving. Applying Buchberger's algorithm to a homogeneous generating set of M yields a homogeneous Gröbner basis, too, and by inspection of the way in which the syzygies $r_{i,j}$ are formed from Equation (1.3.1), we see that the resolution obtained by Algorithm 1.3.4 is indeed graded (with the proper choice of the degrees of the free generators, i.e., each generator gets the same degree as the relation to which it is mapped).

In the case that R^l is graded and M is a graded submodule, we are also interested in obtaining a **minimal free resolution** of M , i.e., a free resolution

such that the free generators of each F_i are mapped to a minimal generating set of the image of F_i . Such a resolution is unique up to isomorphism of complexes (see Eisenbud [59, Theorem 20,2]), and in particular its length is unique. This length is called the **homological dimension** of M , written as $\text{hdim}(M)$, and is an important structural invariant of M . A graded resolution (1.3.2) calculated by Algorithm 1.3.4 is usually not minimal, so how can it be transformed into a minimal resolution, preferably without computing any further Gröbner bases? As a first step, we can use linear algebra to select a minimal subset of the free generators of F_0 whose image in M generates M . Thus we obtain a free submodule $F'_0 \subseteq F_0$ and a commutative diagram

$$\begin{array}{ccccccc} \cdots & \longrightarrow & F_1 & \xrightarrow{\rho} & F_0 & \longrightarrow & M \\ & & & & \uparrow \varphi & & \parallel \\ & & & & F'_0 & \longrightarrow & M, \end{array}$$

where $\varphi \circ \psi = \text{id}$. Lemma 1.3.2 yields an exact sequence

$$0 \longrightarrow (\text{id} - \psi \circ \varphi)(F_0) \longrightarrow \text{im}(\rho) \xrightarrow{\varphi} F'_0 \longrightarrow M. \quad (1.3.3)$$

Observe that $(\text{id} - \psi \circ \varphi)$ maps a free generator e_i from F_0 either to zero (if it is also a generator of F'_0) or to a non-zero element of $(\text{id} - \psi \circ \varphi)(F_0)$ corresponding to the representation of the image of e_i in M in terms of the images of those e_j contained in F'_0 . These non-zero elements are linearly independent, hence $(\text{id} - \psi \circ \varphi)(F_0)$ is a free module. We can use linear algebra to compute preimages under ρ of the free generators of $(\text{id} - \psi \circ \varphi)(F_0)$ in F_1 . This yields a free submodule $\hat{F}_1 \subseteq F_1$ such that $\rho(\hat{F}_1) = (\text{id} - \psi \circ \varphi)(F_0)$ and the restriction of ρ to \hat{F}_1 is injective. Now it is easy to see that (1.3.3) and (1.3.2) lead to the exact sequence

$$0 \longrightarrow F_r \longrightarrow F_{r-1} \longrightarrow \cdots \longrightarrow F_3 \longrightarrow F_2 \oplus \hat{F}_1 \longrightarrow F_1 \xrightarrow{\varphi \circ \rho} F'_0 \longrightarrow M \longrightarrow 0.$$

Thus we have managed to replace (1.3.2) by a free resolution with the first free module minimal. Iterating this process, we obtain the desired minimal free resolution of M . Notice that the only computationally significant steps are the selection of minimal generators for M and the computation of preimages of $e_i - \psi(\varphi(e_i))$ for some free generators e_i of F_0 . Both of these are accomplished by linear algebra. Thus a minimal resolution of M can be computed by just one Gröbner basis computation and linear algebra.

1.4 Hilbert Series

In this section, we prove some results about Hilbert series of rings, and how we can use ideal theory to compute them.

Definition 1.4.1. For a graded vector space $V = \bigoplus_{d=k}^{\infty} V_d$ with V_d finite dimensional for all d we define the **Hilbert series** of V as the formal Laurent series

$$H(V, t) := \sum_{d=k}^{\infty} \dim(V_d) t^d.$$

In the literature, Hilbert series are sometimes called Poincaré series. In our applications, V will always be a graded algebra or a graded module.

Example 1.4.2. Let us compute the Hilbert series of $K[x_1, \dots, x_n]$. There are $\binom{n+d-1}{n-1}$ monomials of degree d , therefore the Hilbert series is

$$H(K[x_1, \dots, x_n], t) = \sum_{d=0}^{\infty} \binom{n+d-1}{n-1} t^d.$$

This is exactly the power series expansion of $(1-t)^{-n}$. ◁

Remark 1.4.3. If V and W are two graded vector spaces, then the tensor product $V \otimes W$ also has a natural grading, namely

$$(V \otimes W)_d = \bigoplus_{d_1+d_2=d} V_{d_1} \otimes W_{d_2}.$$

It is obvious from this formula that $H(V \otimes W, t) = H(V, t)H(W, t)$. Suppose that $R = K[x_1, \dots, x_n]$ and x_i has degree $d_i > 0$. Then we have $R = K[x_1] \otimes K[x_2] \otimes \dots \otimes K[x_n]$ as graded algebras and $H(K[x_i], t) = (1-t^{d_i})^{-1}$. It follows that

$$H(R, t) = \frac{1}{(1-t^{d_1}) \dots (1-t^{d_n})} \quad (1.4.1)$$

◁

Remark 1.4.4. If

$$0 \rightarrow V^{(1)} \rightarrow V^{(2)} \rightarrow \dots \rightarrow V^{(r)} \rightarrow 0 \quad (1.4.2)$$

is an exact sequence of graded vector spaces (all maps respect degree) with $V_d^{(i)}$ finite dimensional for all i and d , then

$$\sum_{i=1}^r (-1)^i H(V^{(i)}, t) = 0.$$

This is clear because the degree d part of (1.4.2) is exact for all d . ◁

Proposition 1.4.5 (Hilbert). *If $R = \bigoplus_{d=0}^{\infty} R_d$ is a finitely generated graded algebra over a field $K = R_0$, then $H(R, t)$ is the power series of a rational function. The radius of convergence of this power series is at least 1. Moreover, if $M = \bigoplus_{d=k}^{\infty} M_d$ is a finitely generated graded R -module, then $H(M, t)$ is the Laurent series of a rational function (which may have a pole at 0).*

Proof. Let $A = K[x_1, x_2, \dots, x_n]$ be the polynomial ring, graded in such a way that $\deg(x_i) = d_i > 0$. Then $H(A, t)$ is a rational function by (1.4.1), and the radius of convergence of the power series is 1 if $n > 0$, and ∞ if $n = 0$. For any integer e , we define the A -module $A(e)$ by $A(e) = \bigoplus_{d=-e}^{\infty} A(e)_d$ with $A(e)_d := A_{e+d}$. It is clear that $H(A(e), t) = t^{-e}H(A, t)$ is again a rational function. A module is free if it is isomorphic to a direct sum $\bigoplus_i A(e_i)$. The Hilbert series of a finitely generated free module M is a rational function. If M is a finitely generated A -module, then by Hilbert's syzygy theorem (see Eisenbud [59, Theorem 1.13]), there exists a resolution

$$0 \rightarrow F^{(r)} \rightarrow F^{(r-1)} \rightarrow \dots \rightarrow F^{(1)} \rightarrow F^{(0)} \rightarrow M \rightarrow 0, \quad (1.4.3)$$

where $F^{(i)}$ is a finitely generated free A -module for all i , and the sequence is exact. It follows from Remark 1.4.4 that

$$H(M, t) = \sum_{i=0}^r (-1)^i H(F^{(i)}, t), \quad (1.4.4)$$

so $H(M, t)$ is a rational function. If M is non-negatively graded, then the same is true for all F_i , so the radius of convergence of $H(M, t)$ is at least 1.

Let R be an arbitrary finitely generated graded algebra over $K = R_0$. Then for some n and some $d_1, \dots, d_n > 0$, there exists a homogeneous ideal $I \subseteq A$ such that $A/I \cong R$. Hence R is a finitely generated, non-negatively graded A -module, and the claim follows. Moreover, any finitely generated graded R -module M is also a finitely generated graded A -module. \square

The above proof gives an easy way to compute the Hilbert series of a graded module M over a graded polynomial ring $R = K[x_1, \dots, x_n]$, if we have a graded free resolution (1.4.3) of M . Indeed, we only have to combine (1.4.4) and (1.4.1). A graded free resolution can be calculated by Algorithm 1.3.4, which involves the computation of a Gröbner basis of M . Given a Gröbner basis of M , there is also a more direct way to find the Hilbert series, which will be discussed in Section 1.4.1.

The Hilbert series encodes geometric information as the following lemma shows.

Lemma 1.4.6. *Let $R = \bigoplus_{d \geq 0} R_d$ be a graded algebra, finitely generated over the field $R_0 = K$. Then $r := \dim(R)$ is equal to the pole order of $H(R, t)$ at $t = 1$.*

Proof. The proof requires the concept of homogeneous systems of parameters. For the definition and the proof of existence, we refer forward to Section 2.4.2. Let f_1, \dots, f_r be a homogeneous system of parameters for R , and set $A := K[f_1, \dots, f_r]$. It follows from (1.4.1) that $H(A, t)$ has pole order r . In fact, $\lim_{t \nearrow 1} (1-t)^r H(A, t) = \prod_{i=1}^r d_i^{-1}$, where $\lim_{t \nearrow 1}$ denotes the limit from below (see Example 1.4.8 below). There exists an A -free resolution

$$0 \rightarrow F^{(r)} \rightarrow F^{(r-1)} \rightarrow \dots \rightarrow F^{(0)} \rightarrow R \rightarrow 0.$$

Using (1.4.4) we conclude that $H(R, t)$ has pole order $\leq r$ because the same holds for all $H(F^{(i)}, t)$. Note that $H(R, t) \geq H(A, t)$ for $0 < t < 1$ since $A \subseteq R$. If the pole order of $H(R, t)$ were strictly smaller than r , then

$$0 = \lim_{t \nearrow 1} (1-t)^r H(R, t) \geq \lim_{t \nearrow 1} (1-t)^r H(A, t) = \prod_{i=1}^r d_i^{-1} > 0.$$

This contradiction shows that $H(R, t)$ has in fact pole order r . □

Definition 1.4.7. Let $R = \bigoplus_d R_d$ be a graded algebra, finitely generated over $R_0 = K$. Then the **degree of R** is defined as

$$\deg(R) = \lim_{t \nearrow 1} (1-t)^r H(R, t)$$

where $r := \dim(R)$ is the Krull dimension of R and $\lim_{t \nearrow 1}$ means the limit from below.

Up to a sign, the degree of R is the first coefficient of the Laurent series expansion of $H(R, t)$ at $t = 1$.

Example 1.4.8. If $A = K[x_1, \dots, x_n]$ with $\deg(x_i) = d_i$, then

$$\deg(A) = \lim_{t \nearrow 1} \frac{(1-t)^n}{\prod_{i=1}^n (1-t^{d_i})} = \lim_{t \nearrow 1} \frac{1}{\prod_{i=1}^n (1+t+\dots+t^{d_i-1})} = \frac{1}{\prod_{i=1}^n d_i},$$

so we have $\deg(A) = (\prod_{i=1}^n d_i)^{-1}$. ◁

If $A = K[x_1, \dots, x_n]$ (all x_i of degree 1) and $I \subset A$ is a homogeneous ideal, then I corresponds to a projective variety $Y \subset \mathbb{P}^{n-1}$. Then the degree of A/I is the same as the degree of Y as a projective variety (see Hartshorne [102, page 52]).

1.4.1 Computation of Hilbert Series

Again, let $R = K[x_1, \dots, x_n]$ be a polynomial ring, graded by $\deg(x_i) = d_i$, and suppose that $I \subseteq R$ is a homogeneous ideal. We want to compute $H(R/I, t)$, or equivalently $H(I, t) = H(R, t) - H(R/I, t)$. We choose a monomial ordering “ $>$ ” on R and use the Buchberger Algorithm 1.1.8 to compute a Gröbner basis $\mathcal{G} = \{g_1, \dots, g_r\}$ of I with respect to “ $>$ ”. The leading monomials $\text{LM}(g_1), \dots, \text{LM}(g_r)$ generate the leading ideal $L(I)$. If $m_1, \dots, m_l \in L(I)$ are distinct monomials which span $L(I)_d$, then we can find homogeneous $f_1, \dots, f_l \in I_d$ such that $\text{LM}(f_i) = m_i$. It is clear that f_1, \dots, f_l is a basis of I_d . It follows that

$$\dim(L(I)_d) = \dim(I_d).$$

We conclude $H(L(I), t) = H(I, t)$, so we have reduced the problem to computing the Hilbert series of a monomial ideal.

So suppose that $I = (m_1, \dots, m_l) \subseteq R$ is a monomial ideal. We will show how to compute $H(I, t)$ using recursion with respect to l . Let $J = (m_1, \dots, m_{l-1})$, then we have an isomorphism

$$J/(J \cap (m_l)) \cong I/(m_l)$$

of graded R -modules. Notice that

$$J \cap (m_l) = (\text{lcm}(m_1, m_l), \text{lcm}(m_2, m_l), \dots, \text{lcm}(m_{l-1}, m_l)),$$

where lcm means least common multiple. By recursion we have $H(J, t)$ and $H(J \cap (m_l), t)$, and $H((m_l), t) = t^{\deg(m_l)} \prod_{i=1}^n (1 - t^{d_i})^{-1}$. So we can compute $H(I, t)$ as

$$H(I, t) = H((m_l), t) + H(J, t) - H(J \cap (m_l), t). \quad (1.4.5)$$

See Bayer and Stillman [13] for more details. A slightly different approach was taken in Bigatti et al. [21].

Example 1.4.9. Let us compute the Hilbert series of the ideal $I = (xz - y^2, xw - yz, yw - z^2) \subset A := K[x, y, z, w]$, where all indeterminates have degree 1. Note that $H(A, t) = (1 - t)^{-4}$ and $H((f), t) = t^d(1 - t)^{-4}$ if f is a homogeneous polynomial of degree d . We choose the lexicographic ordering “ $>$ ” with $x > y > z > w$. Then $\mathcal{G} = \{xz - y^2, xw - yz, yw - z^2\}$ is a Gröbner basis of I . It follows that the initial ideal $L(I)$ is generated by xz, xw, yw . Observe that $(xz, xw) \cap (yw) = (xyzw, xyw) = (xyw)$. By (1.4.5) we get

$$H(L(I), t) = H((xz, xw, yw), t) = H((yw), t) + H((xz, xw), t) - H((xyw), t). \quad (1.4.6)$$

We know that $H((yw), t) = t^2/(1 - t)^4$ and $H((xyw), t) = t^3/(1 - t)^4$. We only need to find $H((xz, xw), t)$. Repeating the above process and making use of $(xz, xw) \cap (xw) = (xzw)$, we obtain (again by 1.4.5)

$$H((xz, xw), t) = H((xw), t) + H((xz), t) - H((xzw), t) = \frac{2t^2 - t^3}{(1 - t)^4}. \quad (1.4.7)$$

Substituting (1.4.7) in (1.4.6) gives

$$H(I, t) = H(L(I), t) = \frac{t^2}{(1 - t)^4} + \frac{2t^2 - t^3}{(1 - t)^4} - \frac{t^3}{(1 - t)^4} = \frac{3t^2 - 2t^3}{(1 - t)^4},$$

and finally

$$H(A/I, t) = H(A, t) - H(I, t) = \frac{1}{(1 - t)^4} - \frac{3t^2 - 2t^3}{(1 - t)^4} = \frac{1 + 2t}{(1 - t)^2}.$$

The pole order of $H(A/I, t)$ at $t = 1$ is 2, so $\dim(A/I) = 2$. If we take $\lim_{t \nearrow 1} (1 - t)^2 H(A/I, t)$, we get $\deg(A/I) = 3$. The ideal I defines a curve of degree 3 in \mathbb{P}^3 (the twisted cubic curve). \triangleleft

1.5 The Radical Ideal

The computation of the radical ideal \sqrt{I} of an ideal $I \subseteq K[x_1, \dots, x_n]$ is one of the basic tasks of constructive ideal theory. For the purposes of this book, radical computation is important since it is used in de Jong's normalization algorithm, which we present in Section 1.6. An important point for us is that we want an algorithm which works in any characteristic. As we will see, radical computation is a quite cumbersome task. Almost all methods that were proposed approach the problem by reducing it to the zero-dimensional case (see, for example, Gianni et al. [83], Krick and Logar [156], Alonso et al. [10], Becker and Weispfenning [15]). To the best of our knowledge, the only exception is a "direct" method given by Eisenbud et al. [60]. However, the limitation of this algorithm is that it requires the ground field K to be of characteristic 0, or that $K[x_1, \dots, x_n]/I$ is generated by elements whose index of nilpotency is less than $\text{char}(K)$ (see Theorem 2.7 in [60]). In our presentation, we will adhere to the strategy of reducing to the zero-dimensional case. We first explain how this reduction works, and then address the problem of zero-dimensional radical computation. Concerning the latter problem, we present a new variant of the "traditional" algorithm, which was given by Kemper [139] and works in positive characteristic.

1.5.1 Reduction to Dimension Zero

The material in this subsection is largely drawn from Becker and Weispfenning [15, Section 8.7]. Given an ideal $I \subseteq K[x_1, \dots, x_n]$, we may apply Algorithm 1.2.4 to find the dimension of \sqrt{I} and a subset $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$ such that the complement $\mathcal{M}' := \{x_1, \dots, x_n\} \setminus \mathcal{M}$ is independent modulo I , and $|\mathcal{M}'| = \dim(I)$. Changing the ordering of the variables, we may assume that $\mathcal{M} = \{x_1, \dots, x_r\}$ and $\mathcal{M}' = \{x_{r+1}, \dots, x_n\}$. By Proposition 1.2.5, the ideal $J := IK(x_{r+1}, \dots, x_n)[x_1, \dots, x_r]$ is zero-dimensional. The main idea in the reduction step is to calculate \sqrt{J} first. In order to work out the radical of I from this, one first has to be able to form the intersection of \sqrt{J} with $K[x_1, \dots, x_n]$. An algorithm for this purpose is given by the following lemma.

Lemma 1.5.1 (Becker and Weispfenning [15, Lemma 8.91]). *Let $L = K(x_{r+1}, \dots, x_n)$ be a rational function field and $J \subseteq L[x_1, \dots, x_r]$ an ideal in a polynomial ring over L . Furthermore, let \mathcal{G} be a Gröbner basis of J with respect to any monomial ordering such that $\mathcal{G} \subset K[x_1, \dots, x_n]$. Set*

$$f := \text{lcm}\{\text{LC}(g) \mid g \in \mathcal{G}\},$$

where the least common multiple is taken in $K[x_{r+1}, \dots, x_n]$, and let I be the ideal in $K[x_1, \dots, x_n]$ generated by \mathcal{G} . Then

$$J \cap K[x_1, \dots, x_n] = I : f^\infty.$$

In the above lemma, the condition $\mathcal{G} \subset K[x_1, \dots, x_n]$ can always be achieved by multiplying each element from the Gröbner basis by the least common multiple of the denominators of its coefficients. The saturation $I : f^\infty$ can be calculated by means of Proposition 1.2.2. Thus we are able to compute the intersection $J \cap K[x_1, \dots, x_n]$, which is sometimes called the contraction ideal of J .

If $I \subseteq K[x_1, \dots, x_n]$ is an ideal, we can form the ideal J in $K(x_{r+1}, \dots, x_n)[x_1, \dots, x_r]$ generated by I and then calculate the contraction ideal of J . However, this is not enough for our purposes, since we also need to be able to express I as the intersection of the contraction ideal of J with another ideal. This is achieved by the following lemma.

Lemma 1.5.2 (Becker and Weispfenning [15, Propos. 8.94, Lemma 8.95]). *Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal. Choose monomial orders “ $>_1$ ” and “ $>_2$ ” on $K[x_1, \dots, x_r]$ and $K[x_{r+1}, \dots, x_n]$, respectively, and let “ $>$ ” be the block ordering obtained from “ $>_1$ ” and “ $>_2$ ” (see Example 1.1.2(d)). Furthermore, let \mathcal{G} be a Gröbner basis of I with respect to “ $>$ ” and form*

$$f := \text{lcm}\{\text{LC}_{>_1}(g) \mid g \in \mathcal{G}\},$$

where $\text{LC}_{>_1}(g)$ is formed by considering g as a polynomial in $K(x_{r+1}, \dots, x_n)[x_1, \dots, x_r]$ and taking the leading coefficient with respect to “ $>_1$ ”. Then the contraction ideal of $J := IK(x_{r+1}, \dots, x_n)[x_1, \dots, x_r]$ is

$$J \cap K[x_1, \dots, x_n] = I : f^\infty.$$

Moreover, if $I : f^\infty = I : f^k$ for some $k \in \mathbb{N}$, then

$$I = (I + (f^k)) \cap (I : f^\infty).$$

We have now provided all ingredients which allow to reduce the problem of radical computation to the zero-dimensional case.

Algorithm 1.5.3 (Higher dimensional radical computation). Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal. Perform the following steps to obtain the radical ideal \sqrt{I} .

- (1) Use Algorithm 1.2.4 to compute the dimension d of I . If $d = -1$, then $I = K[x_1, \dots, x_n] = \sqrt{I}$, and we are done. Otherwise, let $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$ be the subset produced by Algorithm 1.2.4. Renumber the variables such that $\mathcal{M} = \{x_1, \dots, x_r\}$.
- (2) Use Lemma 1.5.2 to find $f \in K[x_{r+1}, \dots, x_n]$ such that

$$I = (I + (f^k)) \cap (IL[x_1, \dots, x_r] \cap K[x_1, \dots, x_n]) \quad (1.5.1)$$

for some $k \in \mathbb{N}$, where $L := K(x_{r+1}, \dots, x_n)$.

- (3) Compute $J := \sqrt{IL[x_1, \dots, x_r]}$. (Note that $IL[x_1, \dots, x_r]$ is zero-dimensional by Proposition 1.2.5.)

(4) Use Lemma 1.5.1 to compute

$$J^c := J \cap K[x_1, \dots, x_n].$$

(5) Apply this algorithm recursively to compute $\sqrt{I + (f)}$. Then

$$\sqrt{I} = \sqrt{I + (f)} \cap J^c, \quad (1.5.2)$$

which can be computed by Equation (1.2.3).

In order to convince ourselves that Algorithm 1.5.3 works correctly, we must show that (1.5.2) holds, and that the recursion will terminate. Indeed, (1.5.1) yields

$$\begin{aligned} \sqrt{I} &= \sqrt{I + (f^k)} \cap \sqrt{IL[x_1, \dots, x_r] \cap K[x_1, \dots, x_n]} = \\ &= \sqrt{I + (f)} \cap (J \cap K[x_1, \dots, x_n]), \end{aligned}$$

which is (1.5.2). Moreover, $I \cap K[x_{r+1}, \dots, x_n] = \{0\}$ by Equation (1.2.5). Therefore $f \notin I$, so $I + (f)$ is a strictly larger ideal than I . Hence the recursion terminates since $K[x_1, \dots, x_n]$ is Noetherian.

1.5.2 Zero-dimensional Radicals

Algorithm 1.5.3 reduces the computation of a radical ideal to the zero-dimensional case, but at the expense of having to compute over a larger field L . This field L is a rational function field over the original ground field K , so if K is a finite field, for example, then in general L is no longer perfect.

Let K be a field and $f \in K[x]$ a non-zero polynomial with coefficients in K . We call f **separable** if f has no multiple roots in a splitting field $L \geq K$. This is equivalent with $\gcd(f, f') = 1$ (see Becker and Weispfenning [15, Proposition 7.33]). If

$$f = c \cdot \prod_{i=1}^m (x - \alpha_i)^{e_i}$$

with $c \in K \setminus \{0\}$ and $\alpha_i \in L$ pairwise distinct roots of f , we write

$$\text{sep}(f) := c \cdot \prod_{i=1}^m (x - \alpha_i) \in L[x]$$

for the **separable part** of f . If $\text{char}(K) = 0$, then we have

$$\text{sep}(f) = \frac{f}{\gcd(f, f')},$$

where the greatest common divisor is taken to be monic. Note that the computation of the gcd can be performed by the Euclidean algorithm (see Geddes

et al. [80, Section 2.4]). Thus in characteristic 0 the separable part is very easy to get, and it coincides with the squarefree part. We will consider the case of positive characteristic below. The algorithm for zero-dimensional radical computation is based on the following result.

Proposition 1.5.4 (Seidenberg [214, Lemma 92]). *Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal in a polynomial ring over a field K . If $I \cap K[x_i]$ contains a separable polynomial for each $i = 1, \dots, n$, then $I = \sqrt{I}$.*

A proof can also be found in Becker and Weispfenning [15, Lemma 8.13]. If I is zero-dimensional, then $I \cap K[x_i] \neq \{0\}$ for every i , since there exists no variables which are independent modulo I (see after Algorithm 1.2.4). Non-zero polynomials in $I \cap K[x_i]$ can most easily be found by the following algorithm, which goes back to Faugère et al. [66].

Algorithm 1.5.5 (Finding univariate polynomials). Given an ideal $I \subseteq K[x_1, \dots, x_n]$ and an index $i \in \{1, \dots, n\}$ such that $I \cap K[x_i] \neq \{0\}$, find a non-zero polynomial $f \in I \cap K[x_i]$ as follows:

- (1) Compute a Gröbner basis \mathcal{G} of I with respect to an arbitrary monomial ordering.
- (2) For $d = 0, 1, 2, \dots$ perform steps (3)–(4).
- (3) Compute the normal form $\text{NF}_{\mathcal{G}}(x_i^d)$.
- (4) Test whether the sequence $\text{NF}_{\mathcal{G}}(x_i^0), \dots, \text{NF}_{\mathcal{G}}(x_i^d)$ is linearly independent over K . If it is, continue the loop for the next d . Otherwise, go to step 5.
- (5) If

$$\sum_{j=0}^d \alpha_j \text{NF}_{\mathcal{G}}(x_i^j) = 0$$

is a K -linear relation found in step (4), then $f := \sum_{j=0}^d \alpha_j x_i^j \in I$ is the desired polynomial.

It is clear that the f from Algorithm 1.5.5 lies in I , since $\text{NF}_{\mathcal{G}}(f) = 0$ by the linearity of the normal form. We can now present the algorithm for zero-dimensional radical computation in characteristic 0.

Algorithm 1.5.6 (Zero-dimensional radical in characteristic 0). Given a zero-dimensional ideal $I \subseteq K[x_1, \dots, x_n]$ with $\text{char}(K) = 0$, perform the following steps:

- (1) For $i = 1, \dots, n$, use Algorithm 1.5.5 to obtain a non-zero $f_i \in I \cap K[x_i]$.
- (2) For each i , compute $g_i := \text{sep}(f_i) = f_i / \gcd(f_i, f_i')$, where the derivative is with respect to x_i .
- (3) Set $\sqrt{I} := I + (g_1, \dots, g_n)$.

The correctness of the above algorithm follows from Proposition 1.5.4. Now we come to the case of positive characteristic. Our presentation is largely drawn from Kemper [139]. The following example shows that applying Algorithm 1.5.6 may produce false results in this case.

Example 1.5.7 (Becker and Weispfenning [15, Example 8.16]). Let $K = \mathbb{F}_p(t)$ be the rational function field over \mathbb{F}_p and consider the ideal

$$I = (x^p - t, y^p - t) \subseteq K[x, y].$$

$x^p - t$ and $y^p - t$ are both squarefree (in fact, irreducible), but $(x - y)^p = x^p - y^p \in I$. Hence $x - y \in \sqrt{I}$, so I is not a radical ideal. \triangleleft

The trouble is that in positive characteristic a univariate may be squarefree but not separable, and the separable part is only defined over a larger field. We have the following algorithm, which works over a rational function field over a finite field.

Algorithm 1.5.8 (Separable part). Given a non-zero polynomial $f \in k(t_1, \dots, t_m)[x]$ with coefficients in a rational function field over a perfect field k of characteristic $p > 0$, compute the separable part of f as a polynomial in $k(\sqrt[p]{t_1}, \dots, \sqrt[p]{t_m})[x]$ with q a power of p .

- (1) Set $h := \gcd(f, f')$.
- (2) Set $g_1 := f/h$.
- (3) Set $\tilde{h} := \gcd(h, h')$.
- (4) If $\tilde{h} = h$, go to (6).
- (5) Set $h := \tilde{h}$ and go to (3).
- (6) If $h = 1$ then return g_1 .
- (7) Write $h = u(x^p)$ with $u \in k(t_1, \dots, t_m)[x]$. (*This is possible since $h' = 0$.*)
- (8) Form $v \in k(\sqrt[p]{t_1}, \dots, \sqrt[p]{t_m})[x]$ from u by replacing every t_i occurring in u with $\sqrt[p]{t_i}$ and every $a \in k$ in u with $\sqrt[p]{a} \in k$. (*Thus $v^p = h$.*)
- (9) Compute $g_2 := \text{sep}(v)$ by a recursive call.
- (10) Compute $g_3 := \text{sep}(g_1 g_2)$ by a recursive call and return g_3 .

The proof of correctness of Algorithm 1.5.8 is straightforward and can be found in Kemper [139] or Kreuzer and Robbiano [155, Proposition 3.7.12] (the latter contains essentially the same algorithm). The following algorithm uses the separable part, as computed by Algorithm 1.5.8, to obtain the radical of a zero-dimensional ideal in positive characteristic.

Algorithm 1.5.9 (Zero-dimensional radical in characteristic p). Given a zero-dimensional ideal $I \subseteq K[x_1, \dots, x_n]$ in a polynomial ring over the rational function field $K = k(t_1, \dots, t_m)$ with k a perfect field of characteristic $p > 0$, obtain \sqrt{I} as follows:

- (1) For $i = 1, \dots, n$, use Algorithm 1.5.5 to obtain a non-zero $f_i \in I \cap K[x_i]$.
- (2) For each i , compute $\text{sep}(f_i) \in k(\sqrt[p^{r_i}]{t_1}, \dots, \sqrt[p^{r_i}]{t_m})[x_i]$ by using Algorithm 1.5.8.
- (3) For each i , write $\text{sep}(f_i) = g_i(\sqrt[q]{t_1}, \dots, \sqrt[q]{t_m}, x_i)$, where $q := p^r$, $r := \max\{r_1, \dots, r_n\}$, and $g_i \in K[y_1, \dots, y_m, x_i]$ with new indeterminates y_1, \dots, y_m .

(4) Form the ideal

$$\begin{aligned} J &:= IK[y_1, \dots, y_m, x_1, \dots, x_n] + (g_1, \dots, g_n) + (y_1^q - t_1, \dots, y_m^q - t_m) \\ &\subseteq K[y_1, \dots, y_m, x_1, \dots, x_n]. \end{aligned}$$

(5) Calculate the elimination ideal

$$\tilde{J} := J \cap K[x_1, \dots, x_n]$$

by using Algorithm 1.2.1 and return $\sqrt{I} = \tilde{J}$.

Again, it is straightforward to see that Algorithm 1.5.9 is correct. In fact, the g_i together with I generate the radical ideal over the larger field $k(\sqrt[q]{t_1}, \dots, \sqrt[q]{t_m})$, and then in step (5) this radical is intersected with the original polynomial ring $k(t_1, \dots, t_m)[x_1, \dots, x_n]$. A formal proof is given in Kemper [139].

Remark 1.5.10. Although we formulated Algorithm 1.5.9 only for ground fields that are rational function fields over a perfect field, it can be made to work over any field of positive characteristic which is finitely generated over a perfect field. For details, we refer to Kemper [139]. \triangleleft

Example 1.5.11. It is interesting to see how Algorithm 1.5.9 handles Example 1.5.7. So consider the ideal $I = (x_1^p - t, x_2^p - t) \subseteq \mathbb{F}_p(t)[x_1, x_2]$. We have

$$\text{sep}(x_i^p - t) = x_i - \sqrt[p]{t},$$

so in step (4) of Algorithm 1.5.9 we obtain the ideal

$$J = (x_1 - y, x_2 - y, y^p - t) \subseteq \mathbb{F}_p(t)[x_1, x_2, y].$$

We choose the lexicographic monomial ordering with $y > x_1 > x_2$ on $\mathbb{F}_p(t)[x_1, x_2, y]$. By replacing $x_1 - y$ and $y^p - t$ by their normal forms with respect to $x_2 - y$, we obtain the new basis

$$\mathcal{G} = \{x_1 - x_2, x_2 - y, x_2^p - t\}.$$

\mathcal{G} is a Gröbner basis since the polynomials in \mathcal{G} have pairwise coprime leading monomials. Hence step (5) of Algorithm 1.5.9 yields

$$\sqrt{I} = J \cap \mathbb{F}_p(t)[x_1, x_2] = (x_1 - x_2, x_2^p - t),$$

which is the correct result. \triangleleft

1.6 Normalization

Let R be an integral domain and \tilde{R} the integral closure of R in its field of fractions. We call \tilde{R} the **normalization** of R . If $\tilde{R} = R$, we say that R is

normal. One reason why normalization is interesting in invariant theory, is that every invariant ring $K[x_1, \dots, x_n]^G$ is normal (see Proposition 2.3.11). The usefulness of normalization is further underlined by Theorem 3.9.15. In this section we will describe a new (or at least newly re-discovered) algorithm by de Jong [121] for computing the normalization of an integral domain that is finitely generated as an algebra over a field (i.e., an “affine domain”). In fact, the algorithm is based on a theorem by Grauert and Remmert (see the references in [121]). Let R be a Noetherian integral domain. If $I \subseteq R$ is a non-zero ideal, choose $0 \neq f \in I$ and consider the mapping

$$\Psi: \text{Hom}_R(I, R) \rightarrow \text{Quot}(R), \varphi \mapsto \frac{\varphi(f)}{f},$$

where $\text{Quot}(R)$ denotes the field of fractions of R .

Lemma 1.6.1. *The map Ψ is independent of the choice of f , and it is a monomorphism of R -modules. Moreover, the restriction of Ψ to $\text{End}_R(I)$ is a homomorphism of R -algebras, and*

$$R \subseteq \Psi(\text{End}_R(I)) \subseteq \tilde{R}.$$

Proof. For $0 \neq g \in I$ we have

$$\frac{\varphi(g)}{g} = \frac{f\varphi(g)}{fg} = \frac{\varphi(fg)}{fg} = \frac{g\varphi(f)}{fg} = \frac{\varphi(f)}{f}.$$

This implies the independence of f and the injectivity of Ψ . It is clear that Ψ is a homomorphism of R -modules, and of R -algebras if restricted to $\text{End}_R(I)$. The image of $\text{End}_R(I)$ is contained in \tilde{R} since $\text{End}_R(I)$ is finitely generated as an R -module, and R is naturally embedded into $\text{End}_R(I)$. \square

Lemma 1.6.2. *Let $I \subseteq R$ be a non-zero radical ideal. Then*

$$\text{End}_R(I) = \Psi^{-1}(\tilde{R}).$$

Proof. The inclusion “ \subseteq ” follows from Lemma 1.6.1. For the reverse inclusion, take $\varphi \in \text{Hom}_R(I, R)$ such that $h := \Psi(\varphi) \in \tilde{R}$. Then $hI \subseteq R$, and we have to show that $hI \subseteq I$. There exists an equation

$$h^k = a_0 + a_1 h + \dots + a_{k-1} h^{k-1}$$

with $a_i \in R$. Hence for $f \in I$ we have

$$(hf)^k = a_0 f^k + a_1 (hf) f^{k-1} + \dots + a_{k-1} (hf)^{k-1} f \in I,$$

hence $hf \in I$ by the hypothesis. This proves the lemma. \square

By Lemma 1.6.1, normality of R implies $\Psi(\text{End}_R(I)) = R$ for all non-zero ideals I . We can now give conditions on I under which the converse holds. We write $X := \text{Spec}(R)$ and

$$X_{\text{nn}} := \{x \in X \mid R_x \text{ is not normal}\}$$

for the non-normal locus. For an ideal $I \subseteq R$ we write $\mathcal{V}_X(I) := \{x \in X \mid I \subseteq x\}$. (The inclusion makes sense since the $x \in X$ are prime ideals in R .)

Theorem 1.6.3. *With the notation introduced above, let $I \subseteq R$ be a non-zero radical ideal such that $X_{\text{nn}} \subseteq \mathcal{V}_X(I)$. Then the equivalence*

$$R \text{ is normal} \iff \Psi(\text{End}_R(I)) = R$$

holds.

Proof. The implication “ \implies ” follows from Lemma 1.6.1. For the converse, assume that $\Psi(\text{End}_R(I)) = R$ and take $h \in \tilde{R}$. With $J := \{f \in R \mid fh \in R\}$ we have

$$P(h) := \{x \in X \mid h \notin R_x\} = \mathcal{V}_X(J).$$

On the other hand, $P(h) \subseteq X_{\text{nn}}$ by definition of $P(h)$. By hypothesis, $P(h) \subseteq \mathcal{V}_X(I)$, and therefore $I = \sqrt{I} \subseteq \sqrt{J}$. Thus there exists a non-negative integer d with $I^d \subseteq J$, hence $hI^d \subseteq R$ by definition of J . Let d be minimal with this property and assume, by way of contradiction, that $d > 0$. Then there exists an element $a \in I^{d-1}$ with $ha \notin R$. We have $ha \in \tilde{R}$ and $haI \subseteq hI^d \subseteq R$, hence $ha \in \Psi(\text{Hom}_R(I, R)) \cap \tilde{R}$. Lemma 1.6.2 yields $haI \subseteq I$ and therefore, by the hypothesis that $\Psi(\text{End}_R(I)) = R$, ha lies in R , a contradiction. Hence $d = 0$ after all, so $h \in R$. Since h was an arbitrary element from \tilde{R} , this completes the proof. \square

An apparent difficulty about Theorem 1.6.3 is that it seems to be hard to get one’s hands on $\text{End}_R(I)$. But this turns out to be surprisingly easy. In fact, multiplication by a non-zero $f \in I$ gives an isomorphism

$$\Psi(\text{End}_R(I)) \rightarrow (f \cdot I) : I$$

(see Greuel and Pfister [98, Remark 3.1]). Thus we only need to compute a quotient ideal to obtain $\text{End}_R(I)$. We summarize the results and translate them to the situation where $R = K[x_1, \dots, x_n]/I$ is an affine domain.

Theorem 1.6.4. *Let $I \subset K[x_1, \dots, x_n]$ be a prime ideal, $J \subseteq K[x_1, \dots, x_n]$ an ideal containing I , and $f \in J \setminus I$. Then with $R := K[x_1, \dots, x_n]/I$ we have:*

(a) *For every $g \in (f \cdot J + I) : J$, the quotient $(g + I)/(f + I)$ lies in the normalization \tilde{R} .*

(b) Assume moreover that J is a radical ideal such that the non-normal locus of $X := \text{Spec}(R)$ is contained in $\mathcal{V}_X(J)$. Then R is normal if and only if

$$(f) + I = (f \cdot J + I) : J.$$

Remark 1.6.5. If K is a perfect field, an ideal J satisfying the conditions of Theorem 1.6.4(b) can be found as follows. Let f_1, \dots, f_m be generators of I and let $\mathfrak{J} = (\partial f_i / \partial x_j)_{i,j}$ be the Jacobian matrix. Then by Eisenbud [59, Theorem 16.19], the singular locus of $X = \text{Spec}(R)$ is

$$X_{\text{sing}} = \{P \in X \mid \mathfrak{J} \text{ reduced modulo } P \text{ has rank } < n - \dim(R)\}.$$

But the non-normal locus X_{nn} is contained in X_{sing} (see Eisenbud [59, Theorem 19.19]). If $J_0 \subseteq K[x_1, \dots, x_n]$ is the ideal generated by I and all $(h \times h)$ -minors of \mathfrak{J} , where $h := n - \dim(R)$, it follows that

$$X_{\text{nn}} \subseteq X_{\text{sing}} = \mathcal{V}_X(J_0).$$

In particular, $J_0 \not\subseteq I$. But then for any ideal J with $I \subseteq J \subseteq \sqrt{J_0}$ we have

$$X_{\text{nn}} \subseteq \mathcal{V}_X(J).$$

Therefore J can be chosen by taking an $(h \times h)$ -minor f of \mathfrak{J} which is not contained in I , and setting $J := \sqrt{I + (f)}$. \triangleleft

We can use Theorem 1.6.4 to calculate the normalization by iteratively adding new generators $(g + I)/(f + I)$ to R until the condition in (b) is satisfied. But for each new iteration we need a presentation for the updated algebra R . De Jong [121] proposed a method for getting a presentation of $\text{End}_R(I)$ consisting of relations of degree one and two. We take a somewhat different approach, given by the following lemma which reduces the task to the computation of an elimination ideal.

Lemma 1.6.6. *Let $K \subseteq L$ be a field extension and $\varphi: K[x_1, \dots, x_n] \rightarrow L$ a homomorphism of K -algebras with kernel I . Furthermore, let $a = \varphi(g)/\varphi(f) \in L$ and consider the homomorphism*

$$\Phi: K[x_1, \dots, x_n, y] \rightarrow L, \quad x_i \mapsto \varphi(x_i), \quad y \mapsto a,$$

where y is an indeterminate. With an additional indeterminate t , set

$$J := I \cdot K[x_1, \dots, x_n, y, t] + (fy - g, ft - 1).$$

Then

$$\ker(\Phi) = J \cap K[x_1, \dots, x_n, y].$$

Proof. J lies in the kernel of the homomorphism $K[x_1, \dots, x_n, y, t] \rightarrow L$ with $x_i \mapsto \varphi(x_i)$, $y \mapsto a$, $t \mapsto 1/\varphi(f)$. Hence $J \cap K[x_1, \dots, x_n, y] \subseteq \ker(\Phi)$. To

prove the converse, we first remark that $fh \in J$ for $h \in K[x_1, \dots, x_n, y, t]$ implies $h \in J$, since

$$h = tfh - h(tf - 1).$$

Furthermore, $f^i y^i - g^i \in J$ for any non-negative integer i , since

$$f^{i+1} y^{i+1} - g^{i+1} = (f^i y^i - g^i)fy + g^i(fy - g).$$

It follows that $f^d (y^i - (g/f)^i) \in J$ for $d \geq i$. Let $h \in \ker(\Phi)$ and set $d := \deg_y(h)$. Write $h(g/f)$ for the result of substituting y by g/f in h . Then $\varphi(f^d h(g/f)) = 0$, so $f^d h(g/f) \in I$. By the preceding argument we also have $f^d (h - h(g/f)) \in J$, hence $f^d h \in J$. But this implies $h \in J$, completing the proof. \square

We can now give the ensuing algorithm, whose termination is guaranteed by the fact that it generates a strictly ascending sequence of R -modules between R and \tilde{R} , with \tilde{R} being Noetherian.

Algorithm 1.6.7 (de Jong's algorithm). Given a prime ideal $I \subseteq K[x_1, \dots, x_n]$ with K a perfect field, perform the following steps to obtain the normalization \tilde{R} of $R := K[x_1, \dots, x_n]/I$, given by a presentation $\tilde{R} \cong K[x_1, \dots, x_{n+m}]/\tilde{I}$ (and the embedding $R \subseteq \tilde{R}$ given by $x_i + I \mapsto x_i + \tilde{I}$):

- (1) Set $m := 0$ and $\tilde{I} := I$.
- (2) Compute the Jacobian matrix $\mathfrak{J} := (\partial f_i / \partial x_j)_{i,j}$, where $\tilde{I} = (f_1, \dots, f_k)$.
- (3) With $l := n + m - \dim(R)$, compute the ideal generated by \tilde{I} and the $(l \times l)$ -minors of \mathfrak{J} . Call this ideal J_{sing} . Choose an ideal J_0 such that $\tilde{I} \subsetneq J_0 \subseteq J_{\text{sing}}$ and an element $f \in J_0 \setminus \tilde{I}$.
- (4) Compute $J := \sqrt{J_0}$ and the quotient ideal $(f \cdot J + \tilde{I}) : J$.
- (5) If $(f \cdot J + \tilde{I}) : J \subseteq \tilde{I} + (f)$ (test this by computing normal forms of the generators of the left hand side with respect to a Gröbner basis of the right hand side), we are done.
- (6) Otherwise, choose $g \in ((f \cdot J + \tilde{I}) : J) \setminus (\tilde{I} + (f))$.
- (7) Set $m := m + 1$ and form the ideal

$$J' := \tilde{I} \cdot K[x_1, \dots, x_{n+m}, t] + (fx_{n+m} - g, ft - 1)$$

in $K[x_1, \dots, x_{n+m}, t]$ with x_{n+m} and t new indeterminates.

- (8) Compute $\tilde{I} := J' \cap K[x_1, \dots, x_{n+m}]$ and go to step (2).

Remark. It is in step (4) that Algorithm 1.6.7 requires radical computation. This is the reason why the ability to calculate radical ideals is important in this book. \triangleleft

We conclude the section with an example.

Example 1.6.8. We can use Algorithm 1.6.7 to de-singularize curves. As an example, consider the curve \mathcal{C} in \mathbb{C}^2 given by the ideal

$$I = (x^6 + y^6 - xy),$$

which has genus 9 and a double point at the origin. A Gröbner basis of $J_{\text{sing}} = (x^6 + y^6 - xy, 6x^5 - y, 6y^5 - x)$ is $\{x, y\}$. Therefore we can choose $f = x$ and $J = J_0 = J_{\text{sing}}$. We obtain

$$(f \cdot J + \tilde{I}) : J = (x, y^5) \quad \text{and} \quad \tilde{I} + (f) = (x, y^6).$$

Thus we can choose $g := y^5$ to obtain a new element $a := (g + I)/(f + I)$ in \tilde{R} . By step (8) of Algorithm 1.6.7 we calculate the kernel \tilde{I} of the map

$$\mathbb{C}[x, y, z] \rightarrow \tilde{R}, \quad x \mapsto x + I, \quad y \mapsto y + I, \quad z \mapsto a$$

and obtain

$$\tilde{I} = (y^5 - xz, x^5 + yz - y, x^4y^4 + z^2 - z).$$

The last equation confirms the integrality of a over R . Going into the next iteration of Algorithm 1.6.7 yields no new elements in \tilde{R} , hence $\tilde{R} = \mathbb{C}[x, y, z]/\tilde{I}$. \tilde{I} defines a curve $\tilde{\mathcal{C}}$ in \mathbb{C}^3 which maps onto \mathcal{C} by projecting on the first two coordinates. With the exception of the origin, every point of \mathcal{C} has a fiber consisting of a single point, and the fiber of the origin consists of the points $(0, 0, 0)$ and $(0, 0, 1)$. \triangleleft