Lecture notes in Computer Algebra

A first introduction to Computational Algebraic Geometry and Commutative Algebra

Yairon Cid-Ruiz

Department of Mathematics, SAS Hall 4214, North Carolina State University, Box 8205 Raleigh, NC 27695, USA.

Email address: ycidrui@ncsu.edu

URL: https://ycid.github.io

Contents

Introduction

What is this document?

This set of notes is designed to supply the course material for the course MA522 at North Carolina State University. This document indicates *all* the contents of the course. You are strongly advised to follow the content and instruction of these notes.

We aim to provide a first introduction to *Computer Algebra*. Computer algebra is a vast area that borrows and interconnects ideas from several fields of mathematics and computer science. However, we will focus on computations involving the solutions to systems of polynomial equations; these solutions are called *algebraic varieties*. Therefore, this course can be seen as a first introduction to *computational ideas in Algebraic Geometry and Commutative Algebra*. Our main tool will be the notion of *Gröbner bases* and we will see how they reduce complicated problems to questions relating *monomial ideals*. Consequently, we will spend some time studying combinatorial properties of monomial ideals.

The following textbooks will be our primary resources:

– Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra by David Cox, Donal O'Shea, and John Little ([3]).

– Monomial ideals by Jürgen Herzog and Takayuki Hibi ([5]).

– Using Algebraic Geometry by David Cox, Donal O'Shea, and John Little ([2]).

– Combinatorial commutative algebra by Ezra Miller and Bernd Sturmfels ([9]).

– A course in commutative algebra by Gregor Kemper ([6]).

Throughout this document we following the following conventions:

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of nonnegative integers.
- $\mathbb{Z}_+ = \{1, 2, \ldots\}$ is the set of positive integers.
- $\mathbb{k}$ is a field.
- $S = \mathbb{k}[x_1, \ldots, x_n]$ is polynomial ring in n variables $x_1, \ldots, x_n$ over the field $\mathbb{k}$.
- $[k] = \{1, \ldots, k\}$ for any $k \geqslant 1$.

CHAPTER 1

Polynomial rings, ideals and varieties

This chapter introduces the basic objects we shall study: *polynomial rings, ideals and varieties*. In this chapter we essentially follow [3, Chapter 1].

1.1. Polynomial rings

Let $\Bbbk$ be a field and $S = \Bbbk[x_1, \ldots, x_n]$ be a polynomial ring. In most of our situations, the field $\Bbbk$ will be:

(i) $\Bbbk = \mathbb{Q}$ the field of rational numbers (a good field for computers to work).
(ii) $\Bbbk = \mathbb{R}$ the field of real numbers (the field of *real life*).
(iii) $\Bbbk = \mathbb{C}$ the field of complex numbers (our preferred algebraically closed field).

The underlying set of the ring S has the structure of a $\Bbbk$-vector space. The basis elements are the *monomials*.

Definition 1.1.1. A *monomial* in S is a product of the form

$$x_1^{\alpha_1} \cdots x_n^{\alpha}$$

where all of the exponents $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ are nonnegative integers. We shall abbreviate $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. The (total) *degree* of this monomial is given by the sum $\deg(x^\alpha) := |\alpha| := \alpha_1 + \cdots + \alpha_n$.

Then the elements in the polynomial ring S are the polynomials.

Definition 1.1.2. A *polynomial* $f \in S$ is a finite linear combination (with coefficients in $\Bbbk$) of monomials. We will write a polynomial f in the form

$$f = \sum_\alpha c_\alpha x^\alpha, \qquad c_\alpha \in \Bbbk$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$.

Definition 1.1.3. Let $f = \sum_\alpha c_\alpha x^\alpha$ be a polynomial in S.

(i) We call c_α the *coefficient* of the monomial x^α.
(ii) If $c_\alpha \neq 0$, then we call $c_\alpha x^\alpha$ a *term* of f.
(iii) The (total) *degree* of $f \neq 0$, denoted $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient c_α is nonzero. The (total) degree of the zero polynomial is undefined.

(iv) If all the terms of $f \neq 0$ have the same degree, then we say that f is a *homogeneous* polynomial.

When the number of variables is small, we shall use the notation $S = \Bbbk[x]$, $S = \Bbbk[x,y]$ or $S = \Bbbk[x,y,z]$.

Example 1.1.4. (i) $2x^2 + 17xy^3z^2 + 5$ is a polynomial in $S = \mathbb{Q}[x,y,z]$ of degree 6 and it has 3 terms. But it is not homogeneous.

(ii) The polynomial $2x^6 + 17xy^3z^2 + 5z^6$ is homogeneous of degree 6 in $S = \mathbb{Q}[x,y,z]$.

The polynomial ring has the following direct sum decomposition

$$S = \bigoplus_{i \geqslant 0} S_i \quad \text{with} \quad S_i := \bigoplus_{|\alpha| = i} \Bbbk \cdot x^{\alpha}.$$

In other words, S_i is the vector space spanned by the monomials of degree i. With our conventions above, notice that S_i is the space of homogeneous polynomials of degree i. With this decomposition by total degree, we say that S is a *graded ring*.

We are interested in the following object, which is the geometrical counter part of the polynomial ring $S = \Bbbk[x_1, \ldots, x_n]$.

Definition 1.1.5. We define the n-dimensional *affine space* over $\Bbbk$ to be the set

$$\mathbb{A}^n_{\Bbbk} := \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \Bbbk\}.$$

As a set $\mathbb{A}^n_{\Bbbk}$ is just the n-dimensional $\Bbbk$-vector space $\Bbbk^n$. But we write $\mathbb{A}^n_{\Bbbk}$ to stress that we will be employing the *Zariski topology* (which will be introduced later in Section 1.3).

Now our discussion begs the following question: *what is the relation between the polynomial ring* $S = \Bbbk[x_1, \ldots, x_n]$ *and the affine space* $\mathbb{A}^n_{\Bbbk}$*?* Our answer will come from the fact that a polynomial $f \in S$ naturally gives function

$$f : \Bbbk^n \to \Bbbk, \qquad a = (a_1, \ldots, a_n) \in \Bbbk^n \mapsto f(a_1, \ldots, a_n) \in \Bbbk,$$

by evaluating the polynomial f. We can describe *algebraic geometry* as the area of mathematics that studies the set of zeroes of polynomial equations.

The following example shows that some care should be taken when working over a finite field. We can have a nonzero polynomial that yields the zero function.

Example 1.1.6. Let $p > 1$ be a prime number, $\Bbbk = \mathbb{Z}/p\mathbb{Z}$ be the field of p elements and $S = \Bbbk[x]$. Consider the *nonzero polynomial* $f(x) = x^p - x \in S$. By Fermat's little theorem, we have $a^p \equiv a (\text{mod}\, p)$ for all $a \in \mathbb{Z}$. Therefore the function $f : \Bbbk \to \Bbbk$, $a \in \Bbbk \mapsto f(a) = a^p - a$ obtained by evaluating f is the *zero function*.

The following proposition shows this phenomenon does appear when the field $\Bbbk$ is infinite.

PROPOSITION 1.1.7. *Suppose* $\Bbbk$ *is an infinite field and* $f \in S = \Bbbk[x_1,\dots,x_n]$ *is a polynomial. Then* $f = 0$ *in* S *if and only if* $f : \Bbbk^n \to \Bbbk$ *is the zero function.*

Before proving the proposition, we need the following basic result from linear algebra.

LEMMA 1.1.8 (Vandermonde determinant). *Let* $v_1,\dots,v_m \in \Bbbk$ *be elements in* $\Bbbk$ *and consider the following matrix*

$$V = V(v_1,\dots,v_m) := \begin{pmatrix} 1 & v_1 & v_1^2 & \cdots & v_1^{m-1} \\ 1 & v_2 & v_2^2 & \cdots & v_2^{m-1} \\ 1 & v_3 & v_3^2 & \cdots & v_3^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & v_m & v_m^2 & \cdots & v_m^{m-1} \end{pmatrix}.$$

Then $\det(V) = \prod_{1 \leqslant i<j \leqslant m}(v_j - v_i)$.

PROOF. We proceed by induction on m. For $m = 2$, it is clear that $\det(V) = v_2 - v_1$. Subtracting to the j-column the $(j-1)$-column multiplied by v_1, we obtain $\det(V) = \det(V')$ where

$$V' = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & v_2 - v_1 & v_2^2 - v_1v_2 & \cdots & v_2^{m-1} - v_1v_2^{m-2} \\ 1 & v_3 - v_1 & v_3^2 - v_1v_3 & \cdots & v_3^{m-1} - v_1v_3^{m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & v_m - v_1 & v_m^2 - v_1v_m & \cdots & v_m^{m-1} - v_1v_m^{m-2} \end{pmatrix}.$$

Let V'' be the $(m-1)\times(m-1)$ matrix obtained by deleting the first row and the first column of V'. Then, expanding across the first column of V' shows that $\det(V) = \det(V') = \det(V'')$. Notice that if we divide i-row of V'' by $v_{i+1} - v_1$ for all $1 \leqslant i \leqslant m-1$, then we get the Vandermonde matrix $V(v_2,\dots,v_m)$. Hence by the inductive hypothesis, we obtain

$$\det(V) = \prod_{i=2}^{m}(v_i - v_1)\cdot \det\left(V(v_2,\dots,v_m)\right) = \prod_{i=2}^{m}(v_i - v_1)\cdot \prod_{2 \leqslant i<j \leqslant m}^{m}(v_j - v_i) = \prod_{1 \leqslant i<j \leqslant m}^{m}(v_j - v_i),$$

as required. □

COROLLARY 1.1.9. *Let* $f = c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0 \in \Bbbk[x]$ *be a polynomial of degree* d. *Then* f *can have at most* d *distinct roots.*

PROOF. By contradiction, suppose that f has $d+1$ distinct roots; say $v_1, v_2, \dots, v_{d+1} \in \Bbbk$ with $f(v_i) = 0$ and $v_i \neq v_j$ for $i \neq j$. Consider the Vandermonde matrix $V = V(v_1,\dots,v_d,v_{d+1})$. We can form the following linear system

$$\begin{pmatrix} 1 & v_1 & v_1^2 & \cdots & v_1^d \\ 1 & v_2 & v_2^2 & \cdots & v_2^d \\ 1 & v_3 & v_3^2 & \cdots & v_3^d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & v_{d+1} & v_{d+1}^2 & \cdots & v_{d+1}^d \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ \vdots \\ c_{d-1} \\ c_d \end{pmatrix} = \begin{pmatrix} f(v_1) \\ \vdots \\ f(v_d) \\ f(v_{d+1}) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}.$$

From Lemma 1.1.8 and the fact that all the v_i are distinct, it follows that $\det(V) = \prod_{1 \leqslant i < j \leqslant d+1}(v_j - v_i) \neq 0$. Therefore, since V is an invertible matrix, we have $c_0 = \cdots = c_d = 0$. This means that $f = 0 \in \Bbbk[x]$ is the zero polynomial, a contradiction. □

Now we are ready for the proof of Proposition 1.1.7.

Proof of Proposition 1.1.7. If $f = 0$ is the zero polynomial in S, then it is clear that $f : \Bbbk^n \to \Bbbk$ is the zero function. Hence we only need to show the reverse implication.

Suppose that $f : \Bbbk^n \to \Bbbk$ is the zero function. We proceed by induction on the number of variables n. If $n = 1$, then Corollary 1.1.9 yields that $f = 0$ in S (because we are assuming $\Bbbk$ is an infinite field). Thus assume $n \geqslant 2$. We can write

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{e} g_i(x_1, \ldots, x_{n-1})\, x_n^i,$$

where each $g_i(x_1, \ldots, x_{n-1})$ is a polynomial in $\Bbbk[x_1, \ldots, x_{n-1}]$. Let $a = (a_1, \ldots, a_{n-1}) \in \Bbbk^{n-1}$ be any tuple and consider the polynomial

$$f_a(x_n) = \sum_{i=0}^{e} g_i(a_1, \ldots, a_{n-1})\, x_n^i \in \Bbbk[x_n].$$

For any $v \in \Bbbk$, by assumption $f_a(v) = f(a_1, \ldots, a_{n-1}, v) = 0$, and so Corollary 1.1.9 implies that $f_a(x_n) = 0$ in $\Bbbk[x_n]$. Hence we showed that $g_i(a_1, \ldots, a_{n-1}) = 0$ for any $(a_1, \ldots, a_{n-1}) \in \Bbbk^{n-1}$. By the induction hypothesis, we get $g_i(x_1, \ldots, x_{n-1}) = 0$ in $\Bbbk[x_1, \ldots, x_{n-1}]$. Finally, it follows that $f = 0$ in S. □

Corollary 1.1.10. *Suppose $\Bbbk$ is an infinite field and let $f, g \in S$ be two polynomials. Then $f = g$ in S if and only if $f : \Bbbk^n \to \Bbbk$ and $g : \Bbbk^n \to \Bbbk$ are the same function.*

Proof. Apply Proposition 1.1.7 to the polynomial $f - g \in S$. □

Below is the basic geometrical object we shall study.

Definition 1.1.11. Let $f_1, \ldots, f_s \in S$ be polynomials. The *affine variety* defined by $f_1, \ldots, f_s$ is given by

$$V(f_1, \ldots, f_s) := \left\{ (a_1, \ldots, a_n) \in \Bbbk^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leqslant i \leqslant s \right\} \subset \mathbb{A}^n_{\Bbbk}.$$

To close this section, we recall the following result.

THEOREM 1.1.12 (Fundamental theorem of algebra). *Every nonconstant polynomial* $f \in \mathbb{C}[x]$ *has a root in* $\mathbb{C}$ *(i.e.,* $\mathbb{C}$ *is algebraically closed).*

Consequently, the variety $V(f)$ defined by a nonconstant polynomial $f \in \mathbb{C}[x]$ with complex coefficients is nonempty. Notice that the above theorem does not hold for the real numbers. For instance, the polynomial $x^2+1 \in \mathbb{R}[x]$ does not have any root in $\mathbb{R}$.

1.2. Ideals

We now introduce the basic algebraic objects that we study.

DEFINITION 1.2.1. A subset $I \subset S = \Bbbk[x_1,...,x_n]$ is an *ideal* if it satisfies:

(i) $0 \in I$.
(ii) If $f, g \in I$, then $f+g \in I$.
(iii) If $f \in I$ and $h \in S$, then $hf \in I$.

We say that I is a *proper ideal* if $I \subsetneq S$ and that I is the *unit ideal* if $I = S$. Notice that $I = S$ is the unit ideal if and only if $1 \in I$. A natural way to present an ideal is by utilizing *generators*:

DEFINITION 1.2.2. Let $f_1,\dots,f_s \in S$ be polynomials. Then we write

$$(f_1,\dots,f_s) := \Big\{\sum_{i=1}^{s} h_i f_i \mid h_1,\dots,h_s \in S\Big\}.$$

More generally, given any (possibly infinite) set $A \subset S$ of polynomials, we also write

$$(A) := \Big\{\sum_{i=1}^{s} h_i f_i \mid s \geqslant 1, f_1,\dots,f_s \in A \text{ and } h_1,\dots,h_s \in S\Big\}.$$

If we are given two ideals $I \subset S$ and $J \subset S$, then we have the following basic operations:

(1) $I+J := \{f+g \mid f \in I, g \in J\}$ (*sum*).
(2) $I \cap J := \{f \in S \mid f \in I \text{ and } f \in J\}$ (*intersection*).
(3) $IJ := \{f_1g_1 + \dots + f_sg_s \mid s \geqslant 1, f_1,\dots,f_s \in I \text{ and } g_1,\dots,g_s \in J\}$ (*product*).

Notice that by definition we always have $IJ \subset I \cap J$.

The lemma below tells us that ideals behave well under these operations.

LEMMA 1.2.3. (i) *The sum* $I+J$ *of two ideals* $I, J \subset S$ *is an ideal.*
(ii) $(f_1,\dots,f_s)$ *is an ideal for any polynomials* $f_1,\dots,f_s \in S$. *Then, we shall say that* $(f_1,\dots,f_s)$ *is the ideal generated by the polynomials* $f_1,\dots,f_s$.
(iii) *The intersection* $I \cap J$ *of two ideals* $I, J \subset S$ *is an ideal.*
(iv) *The product* $I \cdot J$ *(also written* IJ*) of two ideals* $I, J \subset S$ *is an ideal.*
(v) (A) *is an ideal for any set of polynomials* $A \subset S$.

PROOF. (i) We check the three conditions of Definition 1.2.1. Notice that $0 \in I+J$ because by assumption $0 \in I$ and $0 \in J$, and, of course, $0 = 0+0$. Let $f, g \in I+J$. By definition, $f = f_1 + g_1$ and $g = f_2 + g_2$ with $f_1, f_2 \in I$ and $g_1, g_2 \in J$. Then we can write

$$f+g = (f_1+f_2)+(g_1+g_2).$$

As I and J are ideals, we have $f_1+f_2 \in I$ and $g_1+g_2 \in J$, and thus $f+g \in I+J$. Similarly, for any $h \in S$, we obtain that $hf = hf_1 + hg_1$ is in $I+J$ because I and J are ideals. This completes the proof that $I+J$ is an ideal.

(ii) It is easy to check that (f_i) is an ideal for each $1 \leqslant i \leqslant s$. Notice that $(f_1, \ldots, f_s) = \sum_{i=1}^{s} (f_i)$ (see Exercise 1.8). Therefore part (i) implies that $(f_1, \ldots, f_s)$ is an ideal.

(iii) Left as an exercise in Exercise 1.1.

(iv) Left as an exercise in Exercise 1.2.

(v) Left as an exercise in Exercise 1.3. □

Given an ideal $I \subset S$, the *radical* of I is given by

$$\sqrt{I} := \{f \in S \mid f^k \in I \text{ for some } k \geqslant 1\}.$$

We say I is a *radical ideal* if $I = \sqrt{I}$. We shall see that radical ideals are the algebraic counter part of varieties. We leave as an exercise to show some of the properties of radicals (see Exercise 1.9).

EXAMPLE 1.2.4. Let $S = \Bbbk[x, y]$.

(i) If $I = (x, y)$ and $J = (z^2 + x)$, then $I + J = (x, y, z^2 + x) = (x, y, z^2)$.
(ii) If $I = (xy)$ and $J = (x^2)$, then $I \cap J = (x^2 y)$ and $IJ = (x^3 y)$.
(iii) If $I = (x^2, y^2)$, then $\sqrt{I} = (x, y)$.
(iv) If $I = (x^2)$ and $J = (y^2)$, then $I \cap J = (x^2 y^2) = IJ$.

Given two ideals $I, J \subset S$, we have the *ideal quotient*

$$I : J := \{f \in S \mid fg \in I \textit{ for all } g \in J\}$$

and the *saturation ideal*

$$I : J^\infty := \bigcup_{k=1}^{\infty} I : J^k.$$

The fact that $I : J$ is an ideal follows straightforwardly by checking the conditions of Definition 1.2.1. Since $J^{k+1} \subset J^K$, we get $I : J^k \subset I : J^{k+1}$ (see Exercise 1.10(i)), and then Exercise 1.6 implies that $I : J^\infty$ is an ideal.

The following classes of ideals will play an important role.

DEFINITION 1.2.5. Let $I \subset S$ be a proper ideal.

(i) I is *prime* if whenever $f, g \in S$ and $fg \in I$, then either $f \in I$ or $g \in I$.

(ii) I is *maximal* if it is maximal with respect to inclusion among proper ideals (i.e., if $J \subset S$ is another ideal with $I \subset J$, then either $I = J$ or $J = S$).

(iii) I is *primary* if whenever $f, g \in S$ and $fg \in I$, then either $f \in I$ or some power $g^m \in I$ for some $m > 0$.

LEMMA 1.2.6. *A prime ideal is radical.*

PROOF. Let $P \subset S$ be a prime ideal. Let $f \in \sqrt{P}$, that is, $f^k \in P$ for some $k > 0$. By the definition of prime ideal, since $f^k = f \cdot f^{k-1} \in P$, we have $f \in P$ or $f^{k-1} \in P$. Thus inductively we should get $f \in P$. □

LEMMA 1.2.7. *A maximal ideal is a prime ideal.*

PROOF. Let $I \subset S$ be a maximal ideal. Let $f, g \in S$ with $fg \in I$. Suppose that $f \notin I$. Then $I : f$ is a proper ideal because $f \notin I$ is equivalent to $1 \notin I : f$. Since $I : f \supset I$ (see Exercise 1.10(ii)), the maximality of I yields the equality $I : f = I$. As $fg \in I$, it follows that $g \in I : f = I$. Therefore, I is a prime ideal. □

LEMMA 1.2.8. *If I is a primary ideal, then $\sqrt{I}$ is prime and is the smallest prime ideal containing I.*

PROOF. Let $P = \sqrt{I}$. Let $f, g \in S$ with $fg \in \sqrt{I}$, that is, there is some $m > 0$ such that $f^k g^k \in I$. Applying the definition of primary ideal to the elements f^k and g^k, it follows that either $f^k \in I$ or $f^{km} \in I$ for some $m > 0$. This means that either $f \in \sqrt{I}$ or $g \in \sqrt{I}$. So P is a prime ideal.

Let $P' \subset S$ be a prime ideal containing I. Then it follows that $P' = \sqrt{P'} \supset \sqrt{I} = P$. This means that P is the smallest prime containing I. □

DEFINITION 1.2.9. If $I \subset S$ is primary and $P = \sqrt{I}$, then we say that I is P-*primary*.

1.3. Zariski topology

We start with the definition of varieties.

DEFINITION 1.3.1. Let $I \subset S = \Bbbk[x_1, \dots, x_n]$ be an ideal. The *affine variety* defined by I is given by

$$V(I) := \left\{(a_1, \dots, a_n) \in \Bbbk^n \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in I\right\} \subset \mathbb{A}^n_{\Bbbk}.$$

Notice that if $f_1, \dots, f_s \in S$ are polynomials and $I = (f_1, \dots, f_s)$ is the ideal generated by them, then clearly $V(I) = V(f_1, \dots, f_s)$. Any possible discrepancy between the above definition and Definition 1.1.11 will be removed when prove the Hilbert basis theorem; indeed, we shall show that any ideal in S is generated by finitely many polynomials. It clear from the definition that for any two ideals $I, J \subset S$, if $I \subset J$, then $V(I) \supset V(J)$ (i.e., $V(-)$ reverses inclusions).

DEFINITION 1.3.2. A *topology* on a set X is given by declaring some subsets of X to be *closed*, such that the following properties hold:

(a) The empty set $\emptyset$ and the whole space X are closed.
(b) Arbitrary intersections of closed sets are closed.
(c) Finite unions of closed sets are closed.

Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a (possibly infinite) collection of ideals in S. Then we can consider the sum and the intersection

$$\sum_{\lambda\in\Lambda} I_\lambda := \left(\bigcup_{\lambda} I_\lambda\right) \subset S \qquad \text{and} \qquad \bigcap_{\lambda\in\Lambda} I_\lambda \subset S.$$

The next lemma describes how the operation $V(-)$ behaves with respect to sums and intersections of ideals.

LEMMA 1.3.3. (i) *Let* $\{I_\lambda\}_{\lambda\in\Lambda}$ *be a (possibly infinite) collection of ideals in* S. *Then we have the equality*

$$V\left(\sum_{\lambda\in\Lambda} I_\lambda\right) = \bigcap_{\lambda\in\Lambda} V(I_\lambda) \quad \subset \mathbb{A}^n_{\Bbbk}.$$

(ii) *Let* $I_1,\dots,I_k$ *be ideals in* S. *Then we have the equality*

$$V\left(\prod_{j=1}^{k} I_j\right) = V\left(\bigcap_{j=1}^{k} I_j\right) = \bigcup_{j=1}^{k} V(I_j) \quad \subset \mathbb{A}^n_{\Bbbk}.$$

PROOF. Let $a = (a_1\dots,a_n) \in \Bbbk^n$.

(i) We have that $a \in \bigcap_{\lambda\in\Lambda} V(I_\lambda)$ if and only if $f_\lambda(a) = 0$ for all $f_\lambda \in I_\lambda$ and $\lambda\in\Lambda$. Recall that a polynomial f in $\sum_{\lambda\in\Lambda} I_\lambda$ is by definition of the form

$$f = f_{\lambda_1} + \cdots + f_{\lambda_k}$$

with $f_{\lambda_i} \in I_{\lambda_i}$ and $\lambda_1,\dots,\lambda_k \in \Lambda$. As a consequence, we obtain the equivalence

$$f(a) = 0 \ \text{ for all } f \in \sum_{\lambda\in\Lambda} I_\lambda \qquad \Longleftrightarrow \qquad f(a) = 0 \ \text{ for all } f_\lambda \in I_\lambda \text{ and } \lambda\in\Lambda.$$

This shows the required equality.

(ii) By induction we can assume that $k = 2$ (see Exercise 1.8). Since $I_1I_2 \subset I_1 \cap I_2 \subset I_j$, we obtain

$$V(I_1I_2) \supset V(I_1 \cap I_2) \supset V(I_j) \quad \text{for } 1 \leqslant j \leqslant 2.$$

Taking the union yields the inclusions $V(I_1I_2) \supset V(I_1\cap I_2) \supset V(I_1) \cup V(I_2)$. Therefore, to conclude the proof it suffices to show the reverse inclusion $V(I_1)\cup V(I_2) \supset V(I_1I_2)$.

Suppose that $a \in V(I_1I_2)$. Hence, by definition, $(f\cdot g)(a) = f(a)g(a) = 0$ for all $f \in I_1$ and $g \in I_2$. If $a \in V(I_1)$, then $a \in V(I_1) \subset V(I_1)\cup V(I_2)$ and we are done. Thus we may assume

$a \notin V(I_1)$ and so there is a polynomial $f' \in I_1$ such $f'(a) \neq 0$. For all $g \in I_2$, since $f'(a)g(a) = 0$, it follows that $g(a) = 0$. This means precisely that $a \in V(I_2)$. Therefore, we proved the inclusion $V(I_1 I_2) \subset V(I_1) \cup V(I_2)$, and this concludes the proof. □

Definition-Proposition 1.3.4. The vector space $\Bbbk^n$ has a topology where the closed subsets are affine varieties. This topology is called the *Zariski topology*. The space $\Bbbk^n$ when is endowed with the Zariski topology is called the *affine n-space* $\mathbb{A}^n_{\Bbbk}$.

Proof. We need to show that algebraic varieties satisfy the three condition of Definition 1.3.2.

First we check property (a). The empty set $\emptyset = I(S)$ is the set of zeroes of the unit ideal. The whole space $\mathbb{A}^n_{\Bbbk} = I(0)$ is the set of zeroes of the zero ideal.

Properties (b) and (c) follow from Lemma 1.3.3. □

The following simple example shows that in general the operations $V(-)$ does not commute with arbitrary intersections of ideals.

Example 1.3.5. Let $S = \Bbbk[x]$ and consider the infinite collection of ideals $I_j = (x^j) \subset S$ for all $j \geqslant 1$. Notice that $\bigcap_{j \geqslant 1} I_j = 0$ is the zero ideal. On the other hand, we have $V(I_j) = \{0\} \subset \mathbb{A}^1_{\Bbbk}$ for all $j \geqslant 1$. Therefore we obtain

$$V\left(\bigcap_{j \geqslant 1} I_j\right) = \mathbb{A}^1_{\Bbbk} \quad \neq \quad \{0\} = \bigcup_{j \geqslant 1} V(I_j).$$

This shows that the finiteness assumption in Lemma 1.3.3(ii) is essential.

We now introduce the "inverse" operation to $V(-)$.

Definition 1.3.6. Let $X \subset \mathbb{A}^n_{\Bbbk}$ be an affine variety. Then the *ideal of* X is given by

$$I(X) := \big\{ f \in S \mid f(a) = 0 \text{ for all } a \in X \big\} \subset S$$

(see Exercise 1.11).

Example 1.3.7. In general, we trivially have $I(\emptyset) = S$. If the field $\Bbbk$ is infinite, then we have $I(\mathbb{A}^n_{\Bbbk}) = 0$. Also, see Exercise 1.12.

Let $I \subset S$ be an ideal and $X \subset \mathbb{A}^n_{\Bbbk}$ be a variety. Then we can perform the following operations

$$I \subset S \quad \mapsto \quad V(I) \subset \mathbb{A}^n_{\Bbbk} \quad \mapsto \quad I(V(I)) \subset S$$

and

$$X \subset \mathbb{A}^n_{\Bbbk} \quad \mapsto \quad I(X) \subset S \quad \mapsto \quad V(I(X)) \subset \mathbb{A}^n_{\Bbbk}.$$

These operations satisfy the following:

Lemma 1.3.8. *Let $I \subset S$ be an ideal and $X \subset \mathbb{A}^n_{\Bbbk}$ be a variety. Then:*

(i) $I \subset I(V(I))$ *and the inclusion can be strict (see Example 1.3.9).*

(ii) $X = V(I(X))$.

Proof. (i) Let $f \in I$. We need to show that $f(a) = 0$ for all $a \in V(I) \subset \mathbb{A}^n_{\Bbbk}$. Since $a \in V(I)$ if and only if $g(a) = 0$ for all $g \in I$, it clearly follows that $f(a) = 0$. Hence $I \subset I(V(I))$.

(ii) First we show $X \subset V(I(X))$. Let $a \in X$. We need to show that $f(a) = 0$ for all $f \in I(X) \subset S$. Since $f \in I(X)$ if and only if $f(b) = 0$ for all $b \in X$, it clearly follows that $f(a) = 0$. Hence $X \subset V(I(X))$.

We now show the reverse inclusion $X \supset V(I(X))$. By definition we can write $X = V(J) \subset \mathbb{A}^n_{\Bbbk}$ for some ideal $J \subset S$. From part (i) above, we get $I(X) = I(V(J)) \supset J$. Then the reverse inclusion property of $V(-)$ gives

$$V(I(X)) \subset V(J) = X.$$

So the equality $X = V(I(X))$ follows. □

Example 1.3.9. In $S = \Bbbk[x]$, we have the strict inclusion $(x^2) \subsetneq I(V(x^2)) = (x)$.

1.4. Polynomial rings in one variable

The instructions for this section are:

- **Read [3, §1.5].**

1.5. Exercises

Exercise 1.1. *Show that the intersection* $I \cap J$ *of two ideals* $I, J \subset S$ *is an ideal. In fact, show that a (possibly infinite) intersection of ideals is an ideal.*

Exercise 1.2. *Show that the product* $I \cdot J$ *of two ideals* $I, J \subset S$ *is an ideal.*

Exercise 1.3. *Show that* (A) *is an ideal for any set of polynomials* $A \subset S$.

Exercise 1.4. *Let* $I, J, K \subset S$ *be ideals. Show that:*

(i) $I \cdot (J + K) = IJ + IK$.

(ii) *If* $I \supset J$ *or* $I \supset K$, *then* $I \cap (J + K) = I \cap J + I \cap K$.

Exercise 1.5. *Give an example where the union* $I \cup J$ *of two ideals* $I, J \subset S$ *is* not *an ideal.*

Exercise 1.6. *Let* $\{I_j\}_{j \geqslant 1}$ *be a sequence of ideals in* S *such that* $I_j \subset I_{j+1}$ *for all* $j \geqslant 1$. *Show that* $\bigcup_{j \geqslant 1} I_j$ *is an ideal.*

Exercise 1.7. *Let* $I, J \subset S$ *be ideals. Show that* $I + J$ *is the smallest ideal containing both* I *and* J.

Exercise 1.8. *Given three ideals* $I, J, K \subset S$. *Show the following (associativity) equalities*

(i) $(I + J) + K = I + (J + K)$.

(ii) $(I \cap J) \cap K = I \cap (J \cap K)$.

(iii) $(I \cdot J) \cdot K = I \cdot (J \cdot K)$.

Therefore, for a sequence $I_1, \dots, I_k \subset S$, *we have well-defined ideals* $\sum_{j=1}^{k} I_j \subset S$, $\bigcap_{j=1}^{k} I_j \subset S$ *and* $\prod_{j=1}^{k} I_j \subset S$ *giving the sum, intersection and product, respectively.*

EXERCISE 1.9. *Let* $I, J \subset S$ *be ideals. Show that:*

(i) $\sqrt{I}$ *is an ideal.*
(ii) $\sqrt{\sqrt{I}} = \sqrt{I}$.
(iii) $\sqrt{I \cap J} = \sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$.
(iv) *If* $I \subset J$, *then* $\sqrt{I} \subset \sqrt{J}$.
(v) $\sqrt{I} + \sqrt{J} \subset \sqrt{I+J}$ *and* $\sqrt{\sqrt{I}+\sqrt{J}} = \sqrt{I+J}$.
(vi) $V(\sqrt{I}) = V(I) \subset \mathbb{A}^n_{\Bbbk}$.

EXERCISE 1.10. *Let* $I, J, K \subset S$ *be ideals. Show that:*

(i) *If* $J \subset K$, *then* $I : J \supset I : K$.
(ii) $I \subset (I : J)$.
(iii) $(I : J) \cdot J \subset I$.
(iv) $(I : J) : K = (I : JK) = (I : K) : J$.
(v) *If* $I_1, \dots, I_s \subset S$ *are ideals, then* $\left(\bigcap_{j=1}^{s} I_j\right) : J = \bigcap_{j=1}^{s} \left(I_j : J\right)$.
(vi) *If* $J_1, \dots, J_s \subset S$ *are ideals, then* $I : (\sum_{i=1}^{s} J_i) = \bigcap_{i=1}^{s} (I : J_i)$.

EXERCISE 1.11. *Let* $X \subset \mathbb{A}^n_{\Bbbk}$ *be an affine variety. Show that* $I(X) \subset S$ *is an ideal.*

EXERCISE 1.12. *Let* $p > 1$ *be a prime number,* $\Bbbk = \mathbb{Z}/p\mathbb{Z}$ *be the field of* p *elements and* $S = \Bbbk[x]$. *Show that* $I(\mathbb{A}^1_{\Bbbk}) = (x^p - x) \in S$.

EXERCISE 1.13. *Show that the following subsets are* not *affine varieties:*

(i) $X = \mathbb{Z}^n \subset \mathbb{A}^n_{\mathbb{R}}$.
(ii) $X = \mathbb{A}^n_{\mathbb{R}} \setminus \{(0, \dots, 0)\} \subset \mathbb{A}^n_{\mathbb{R}}$.
(iii) $X = \{(a,b) \in \mathbb{A}^2_{\mathbb{R}} \mid b = \sin(a)\} \subset \mathbb{A}^2_{\mathbb{R}}$.
(iv) $X = \{(a,b) \in \mathbb{A}^2_{\mathbb{R}} \mid b = e^a\} \subset \mathbb{A}^2_{\mathbb{R}}$.

EXERCISE 1.14. *Let* $X \subset \mathbb{A}^n_{\Bbbk}$ *and* $Y \subset \mathbb{A}^m_{\Bbbk}$. *Show that the Cartesian product* $X \times Y \subset \mathbb{A}^n_{\Bbbk} \times \mathbb{A}^m_{\Bbbk} \cong \mathbb{A}^{n+m}_{\Bbbk}$ *is also an affine variety.*

EXERCISE 1.15. *Identify* $\mathbb{A}^{mn}_{\Bbbk}$ *with the space of* $m \times n$ *matrices, and let* $r \geqslant 0$. *Show that the set of matrices with rank* $\leqslant r$ *is an affine variety in* $\mathbb{A}^{mn}_{\Bbbk}$.

EXERCISE 1.16. *Show that a finite set of points in* $\mathbb{A}^n_{\Bbbk}$ *is an affine variety.*

EXERCISE 1.17. *Show that the only affine varieties in* $\mathbb{A}^1_{\Bbbk}$ *are* (a) *the empty set,* (b) *the whole space* $\mathbb{A}^1_{\Bbbk}$, *and* (c) *a finite set of points.*

EXERCISE 1.18. *This exercise shows that affine varieties are not stable under projections. Consider the affine variety* $C = \left\{(a,b) \in \mathbb{A}^2_{\mathbb{R}} \mid a^2+b^2=1\right\}$ *(the circle of radius* 1*) and the natural projection* $\pi\colon \mathbb{A}^2_{\mathbb{R}} \to \mathbb{A}^1_{\mathbb{R}}$, $(a,b) \mapsto a$ *that forgets the second coordinate. Show that the set* $\pi(C) \subset \mathbb{A}^1_{\mathbb{R}}$ *is* not *an affine variety.*

CHAPTER 2

Algebra and combinatorics of monomial ideals

Throughout this chapter, we continue using the previous notation: $S = \Bbbk[x_1,\dots,x_n]$ is a polynomial ring in n variables over a field $\Bbbk$. We use the notation $\mathbf{x}^{\mathbf{a}} = x_1^{a_1}\cdots x_n^{a_n}$ for any $\mathbf{a} := (a_1,\dots,a_n) \in \mathbb{N}^n$.

2.1. Basic properties of monomial ideals

The instructions for this section are:

- **Read** [5, §1.1]**.**
- **Read** [5, §1.2]**.**
- **Read** [5, §1.3.1]**.**

2.2. Dickson's lemma

In this section, we present one of the central results we shall need.

Denote by $\operatorname{Mon}(S) = \{\mathbf{x}^{\mathbf{a}} = x_1^{a_1}\cdots x_n^{a_n} \mid \mathbf{a} = (a_1,\dots,a_n) \in \mathbb{N}^n\}$ the set of monomial in the polynomial ring $S = \Bbbk[x_1,\dots,x_n]$. For any polynomial $f = \sum_{\mathbf{a}\in\mathbb{N}^n} c_{\mathbf{a}}\mathbf{x}^{\mathbf{a}} \in S$, we denote the support of f by

$$\operatorname{supp}(f) := \left\{\mathbf{x}^{\mathbf{a}} \in \operatorname{Mon}(S) \mid c_{\mathbf{a}} \neq 0\right\}.$$

Let $\mathcal{M}$ be a nonempty subset of $\operatorname{Mon}(S)$. A monomial $\mathbf{x}^{\mathbf{a}} \in \mathcal{M}$ is said to be a minimal element of $\mathcal{M}$ with respect to divisibility if whenever $\mathbf{x}^{\mathbf{b}} \mid \mathbf{x}^{\mathbf{a}}$ with $\mathbf{x}^{\mathbf{b}} \in \mathcal{M}$, then $\mathbf{x}^{\mathbf{b}} = \mathbf{x}^{\mathbf{a}}$. Let $\mathcal{M}^{\min}$ denote the set of minimal elements of $\mathcal{M}$.

Definition 2.2.1. An ideal $I \subset S$ is called a *monomial ideal* if it is generated by monomials.

The following result tells us that the set of monomials $\operatorname{Mon}(S)$ is "almost well-ordered" with respect to divisibility.

Theorem 2.2.2 (Dickson lemma). *Let $\mathcal{M}$ be a nonempty subset of* $\operatorname{Mon}(S)$. *Then $\mathcal{M}^{\min}$ is a finite set.*

Proof. We prove Dickson's lemma by induction on n, the number of variables of S. If $n = 1$, then $\mathcal{M}$ consists of certain powers of x_1, and the set of minimal elements of $\mathcal{M}$ is the set $\{x_1^c\}$, where c is the smallest number such that $x_1^c \in \mathcal{M}$.

Now assume that $n \geqslant 2$. Let $\mathcal{N}$ be the set of monomials

$$\mathcal{N} := \left\{\mathbf{x}^{\mathbf{c}} = x_1^{c_1}\cdots x_{n-1}^{c_{n-1}} \in \Bbbk[x_1,\dots,x_{n-1}] \mid \mathbf{x}^{\mathbf{c}}x_n^d \in \mathcal{M} \text{ for some } d \geqslant 0\right\}.$$

By the induction hypothesis, the set $\mathcal{N}^{\min}$ of minimal elements of $\mathcal{N}$ is finite, say $\mathcal{N}^{\min} = \{\mathbf{x}^{\mathbf{c}_1}, \dots, \mathbf{x}^{\mathbf{c}_r}\} \subset \Bbbk[x_1, \dots, x_{n-1}]$ for some $\mathbf{c}_1, \dots, \mathbf{c}_r \in \mathbb{N}^{n-1}$. For each $\mathbf{x}^{\mathbf{c}_i}$ there exists $a_i \geqslant 0$ such that $\mathbf{x}^{\mathbf{c}_i} x_n^{a_i} \in \mathcal{M}^{\min}$. Let $a = \max\{a_1, \dots, a_r\}$, and for each b with $0 \leqslant b < a$ let

$$\mathcal{N}_b := \left\{\mathbf{x}^{\mathbf{c}} \in \Bbbk[x_1, \dots, x_{n-1}] \mid \mathbf{x}^{\mathbf{c}} x_n^b \in \mathcal{M}\right\}.$$

Again by the induction hypothesis, $\mathcal{N}_b^{\min}$ is a finite set. We use the notation

$$\mathcal{N}_b^{\min} x_n^b := \left\{\mathbf{x}^{\mathbf{c}} x_n^b \mid \mathbf{x}^{\mathbf{c}} \in \mathcal{N}_b^{\min}\right\}.$$

We claim that

$$\mathcal{M}^{\min} \subset \left\{\mathbf{x}^{\mathbf{c}_1} x_n^{a_1}, \dots, \mathbf{x}^{\mathbf{c}_r} x_n^{a_r}\right\} \cup \bigcup_{b=0}^{a-1} \mathcal{N}_b^{\min} x_n^b.$$

Since the right-hand side of this inclusion is a finite set, the assertion of the theorem follows from this claim.

In order to prove the claim, let $u = \mathbf{x}^{\mathbf{c}} x_n^d$ be a monomial in $\mathcal{M}$. If $d \geqslant a$, then some monomial in $\{\mathbf{x}^{\mathbf{c}_1} x_n^{a_1}, \dots, \mathbf{x}^{\mathbf{c}_r} x_n^{a_r}\}$ divides u. If $0 \leqslant d < a$, then u is divisible by a monomial in $\mathcal{N}_d^{\min} x_n^d$. This completes the proof of the theorem. □

The next corollary tells us that monomial ideals are finitely generated. This is a special case of Hilbert basis theorem for monomial ideals.

Corollary 2.2.3 (Hilbert basis theorem for monomial ideals). *Let I be a monomial ideal. Then each set of monomial generators of I contains a finite set which generates I.*

Proof. Let $\mathcal{M}$ be a set of monomial generators of I. By Theorem 2.2.2, the set of minimal elements of $\mathcal{M}$ is finite. This finite set is a set of monomial generators of I. □

Below a list of basic results regarding monomial ideals. The proofs are pretty straightforward and the reader is referred to [5, §1.1].

Theorem 2.2.4. *Let $I \subset S$ be a monomial ideal. The set $\mathcal{N}$ of monomials belonging to I is a $\Bbbk$-basis of I.*

Corollary 2.2.5. *Let $I \subset S$ be an ideal. The following conditions are equivalent:*

(a) *I is a monomial ideal.*
(b) *For all $f \in S$ one has: $f \in I$ if and only if* $\operatorname{supp}(f) \subset I$.

Corollary 2.2.6. *Let I be a monomial ideal. The residue classes of the monomials not belonging to I form a $\Bbbk$-basis of the residue class ring S/I.* (The monomials that do not belong to I are called *standard*.)

The set of monomials which belong to I can be described as follows:

Proposition 2.2.7. *Let $\{u_1,\dots,u_m\}$ be a monomial system of generators of the monomial ideal I. Then a monomial $v \in \mathrm{Mon}(S)$ belongs to I if and only if there exists a monomial w such that $v = wu_i$ for some $1 \leqslant i \leqslant m$.*

Proposition 2.2.8. *Each monomial ideal has a unique minimal monomial set of generators. More precisely, let G denote the set of monomials in I which are minimal with respect to divisibility. Then G is the unique minimal set of monomial generators.*

As a consequence we make the following definition.

Definition 2.2.9. The unique minimal set of monomial generators of the monomial ideal I is denoted by $G(I) \subset \mathrm{Mon}(S)$.

As another consequence of Dickson's lemma we have a "Noetherian property" for monomial ideals.

Proposition 2.2.10. *Each ascending sequence of monomial ideals $I_1 \subset I_2 \subset \cdots \subset I_j \subset \cdots$ in S terminates, that is, there exists an integer k such that $I_l = I_k$ for all $l \geqslant k$.*

Proof. Let $\mathcal{M} = \bigcup_{j=1}^{\infty} G(I_j)$. According to Dickson's lemma (see Theorem 2.2.2), the set $\mathcal{M}^{\min}$ is finite. Hence there is an integer k such that $\mathcal{M}^{\min} \subset \bigcup_{j=1}^{k} G(I_j)$. Now let $l \geqslant k$ and let u be a monomial in I_l. Then there exists $v \in \mathcal{M}^{\min}$ which divides u. This implies that $u \in \bigcup_{j=1}^{k} I_j = I_k$, as desired. □

We close this section with some basic properties of monomial ideals. Given two monomials $u = x_1^{a_1}\cdots x_n^{a_n}$ and $v = x_1^{b_1}\cdots x_n^{b_n}$, we have the following explicit descriptions

$$\gcd(u,v) \;=\; x_1^{\min\{a_1,b_1\}}\cdots x_n^{\min\{a_n,b_n\}}$$

and

$$\mathrm{lcm}(u,v) \;=\; x_1^{\max\{a_1,b_1\}}\cdots x_n^{\max\{a_n,b_n\}}.$$

We saw that the generators of the product or the sum of ideals are easy to find. On the other hand, it is difficult to find the generators of an intersection. However, in the case of ideals this process is quite explicit.

Lemma 2.2.11. *Let I and J be monomial ideals. Then $I \cap J$ is a monomial ideal, and*

$$\mathcal{G} \;=\; \big\{\mathrm{lcm}(u,v) \mid u \in G(I) \;\; \textit{and} \;\; v \in G(J)\big\}$$

is a set of generators of $I \cap J$.

Proof. Let $f \in I \cap J$. By Corollary 2.2.5, since I and J are monomial ideals, it follows that $\mathrm{supp}(f) \subset I \cap J$. Again applying Corollary 2.2.5, we see that $I \cap J$ is a monomial ideal.

Let $w \in \mathrm{Mon}(S)$ be a monomial in $I \cap J$. Due to Proposition 2.2.7, there exist $u \in G(I)$ and $v \in G(J)$ such that $u \mid w$ and $v \mid w$. It follows that $\mathrm{lcm}(u,v)$ divides w. Since $\mathrm{lcm}(u,v) \in I \cap J$ for all $u \in G(I)$ and $v \in G(J)$, we conclude that $\mathcal{G}$ is indeed a set of generators of $I \cap J$. □

Similarly, computing ideals quotients is difficult in general. However, for monomial ideals, the task is quite explicit.

LEMMA 2.2.12. *Let* I *and* J *be monomial ideals. Then* $I : J$ *is a monomial ideal, and*

$$I : J = \bigcap_{v \in G(J)} I : v.$$

Moreover, $\{u/\gcd(u,v) \mid u \in G(I)\}$ *is a set of generators of* $I : v$.

PROOF. Let $f \in I : J$. Then $fv \in I$ for all $v \in G(J)$. In view of Corollary 2.2.5 we have $\operatorname{supp}(f)v = \operatorname{supp}(fv) \subset I$. This implies that $\operatorname{supp}(f) \subset I : J$. Thus Corollary 2.2.5 yields that $I : J$ is a monomial ideal.

The given presentation follows from Exercise 1.10. It is clear that $\{u/\gcd(u,v) \mid u \in G(I)\} \subset I : v$. So now let $w \in I : v$. Then there exists $u \in G(I)$ such that u divides wv. This implies that $u/\gcd(u,v)$ divides w, as desired. □

2.3. Primary decomposition of monomial ideals

In this section, we discuss the notion of primary decomposition for monomial ideals. A decomposition of an ideal $I \subset S$ as an intersection $I = \bigcap_{i=1}^{m} Q_i$ of ideals is called *irredundant* if none of the ideals Q_i can be omitted in this presentation. The following important theorem does the job for monomial ideals.

THEOREM 2.3.1. *Let* $I \subset S = \Bbbk[x_1,\dots,x_n]$ *be a monomial ideal. Then* $I = \bigcap_{i=1}^{m} Q_i$*, where each* Q_i *is generated by pure powers of the variables. In other words, each* Q_i *is of the form* $(x_{i_1}^{a_1},\dots,x_{i_k}^{a_k}) \subset S$*. Moreover, an irredundant decomposition of this form is unique.*

PROOF. Let $G(I) = \{u_1,\dots,u_r\}$, and suppose some u_i is not a pure power, say u_1. Then we can write $u_1 = vw$ where v and w are coprime monomials, that is, $\gcd(v,w) = 1$ and $u \neq 1 \neq w$. We claim that $I = I_1 \cap I_2$ where $I_1 = (v,u_2,\dots,u_r)$ and $I_2 = (w,u_2,\dots,u_r)$. Indeed, since u and v are coprime, Lemma 2.2.11 yields the equality $I_1 \cap I_2 = (\operatorname{lcm}(v,w),u_2,\dots,u_r) = (u_1,u_2,\dots,u_r) = I$.

If either $G(I_1)$ or $G(I_2)$ contains an element which is not a pure power, we proceed as before and obtain after a finite number of steps a presentation of I as an intersection of monomial ideals generated by pure powers. By omitting those ideals which contain the intersection of the others we end up with an irredundant intersection.

So it remains to show uniqueness. Let $Q_1 \cap \cdots \cap Q_r = I = Q'_1 \cap \cdots \cap Q'_s$ be two irredundant intersections of ideals generated by pure powers. We will show that for each $1 \leqslant i \leqslant r$ there exists $1 \leqslant j \leqslant s$ such that $Q'_j \subset Q_i$. By symmetry we then also have that for each $1 \leqslant k \leqslant s$ there exists an $1 \leqslant l \leqslant r$ such that $Q_l \subset Q'_k$. This will then imply that $r = s$ and $\{Q_1,\dots,Q_r\} = \{Q'_1,\dots,Q'_s\}$.

Let $1 \leqslant i \leqslant r$. We may assume that $Q_i = (x_1^{a_1}, \ldots, x_k^{a_k})$. Suppose that $Q'_j \not\subset Q_i$ for all $1 \leqslant j \leqslant s$. Then for each j there exists $x_{\ell_j}^{b_j} \in Q'_j \setminus Q_i$. It follows that either $\ell_j > k$ or $b_j < a_{l_j}$. Let

$$u = \operatorname{lcm}\{x_{\ell_1}^{b_1}, \ldots, x_{\ell_s}^{b_s}\}.$$

We have $u \in \bigcap_{j=1}^{s} Q'_j = I \subset Q_i$. Therefore there exists $1 \leqslant c \leqslant k$ such that $x_c^{a_c}$ divides u. But this is obviously impossible, and so the proof is complete. □

A monomial ideal is called *irreducible* if it cannot be written as proper intersection of two other monomial ideals. Equivalently, I is irreducible if whenever $I = I_1 \cap I_2$ then either $I = I_2$ or $I = I_2$. It is called *reducible* if it is not irreducible.

Corollary 2.3.2. *A monomial ideal is irreducible if and only if it is generated by pure powers of the variables.*

Proof. Let $Q = (x_{i_1}^{a_1}, \ldots, x_{i_k}^{a_k})$. Suppose $Q = I \cap J$ where I and J are monomial ideals properly containing Q. By Theorem 2.3.1, we have two irredundant decompositions $I = \bigcap_{i=1}^{r} Q_i$ and $J = \bigcap_{j=1}^{s} Q'_j$ where the Q_i and Q'_j are generated by powers of the variables. Thus we get the decomposition

$$Q = \bigcap_{i=1}^{r} Q_i \cap \bigcap_{j=1}^{s} Q'_j.$$

The uniqueness statement of Theorem 2.3.1 implies that $r = s = 1$ and $Q = Q_1 = Q'_1$. This is a contradiction.

Conversely, if $G(Q)$ contains a monomial $u = vw$ with $\gcd(v, w) = 1$ and $v \neq 1 \neq w$, then, as in the proof of Theorem 2.3.1, Q can be written a proper intersection of monomial ideals. □

Lemma 2.3.3. *Let $I \subset S$ be an irreducible monomial ideal. Then I is primary.*

Proof. Let $f, g \in S$ and $fg \in I$. By Proposition 2.2.10, we have $I : g^\infty = \bigcup_{j=1}^{\infty} I : g^j = I : g^m$ for some $m > 0$; in particular, $I : g^{m+1} = I : g^m$.

We claim that we have the equality $(I + (f)) \cap (I + (g^m)) = I$. It is clear that $(I + (f)) \cap (I + (g^m)) \supset I$. Let $h \in (I + (f)) \cap (I + (g^m))$. Then we can write $h = h_1 + af = h_2 + bg^m$, where $h_1, h_2 \in I$ and $a, b \in S$. Multiplying by g yields the equality

$$h_1 g + afg - h_2 g = bg^{m+1},$$

and since $h_1, fg, h_2 \in I$, it follows that $b \in I : g^{m+1}$. From the assumption $I : g^{m+1} = I : g^m$, we obtain $h_3 = bg^m \in I$. Then dividing by g yields the equality

$$h_1 + af - h_2 = h_3,$$

from which we conclude that $af \in I$. As a consequence, $h = h_1 + af \in I$, and so we get the claim $(I + (f)) \cap (I + (g^m)) = I$.

Since I is irreducible, we obtain either $I = I + (f)$ or $I = I + (g^m)$. Therefore, either $f \in I$ or $g^m \in I$. This means precisely that I is primary. □

REMARK 2.3.4. Corollary 2.3.2 and Lemma 2.3.3 yield that an ideal $Q = (x_{i_1}^{a_1}, \dots, x_{i_k}^{a_k}) \subset S$ generated by pure powers of the variables is primary with respect to the prime ideal $\sqrt{Q} = (x_{i_1}, \dots, x_{i_k}) \subset S$.

REMARK 2.3.5. Theorem 2.3.1 in combination with Corollary 2.3.2 now says that each monomial ideal has a unique decomposition as an irredundant intersection of irreducible monomial ideals. Moreover, Lemma 2.3.3 tells us that such decomposition is primary.

2.4. Hilbert functions of monomial ideals

In this section, we study the Hilbert functions of monomial ideals. Our main goal is to provide a self-contained and combinatorial proof of the existence of Hilbert polynomials and Hilbert series. Our proof will heavily depend on the decomposition of monomial ideals into ideals generated by pure powers of the variables (see Theorem 2.3.1) and on the fact that we have distributive law of sums over intersections in the case of monomial ideals (see Exercise 2.1). Since the *dimension* of an affine space $\mathbb{A}^n_{\Bbbk}$ should be n, the following lemma yields a successful way to define the dimension of the variety determined by a monomial ideal.

DEFINITION-LEMMA 2.4.1. Let $I \subset S$ be a monomial ideal. From Theorem 2.3.1, let $I = \bigcap_{i=1}^m Q_i$ be an irredundant decomposition where each Q_i is generated by pure powers. Then $V(I)$ is a finite union of affine spaces and its dimension is equal to

$$\dim(V(I)) := \max\left\{\dim(V(Q_i)) \mid 1 \leqslant i \leqslant m\right\}.$$

PROOF. We have that $V(I) = \bigcup_{j=1}^m V(Q_i)$. Let $Q_i = (x_{i_1}^{a_1}, \dots, x_{i_k}^{a_k}) \subset S$. We have the following equality

$$V(Q_i) = \left\{(b_1, \dots, b_n) \in \mathbb{A}^n_{\Bbbk} \mid b_{i_1} = \dots = b_{i_k} = 0\right\} \cong \mathbb{A}^{n-k}_{\Bbbk}$$

that proves the claim. □

DEFINITION 2.4.2. An S-module is an Abelian group M on which S acts linearly by a mapping $S \times M \to M$ that satisfies the axioms

(i) $a(x+y) = ax + ay$.
(ii) $(a+b)x = ax + bx$.
(iii) $(ab)x = a(bx)$.
(iv) $1x = x$.

for all $a, b \in S$ and $x, y \in M$.

We say that M is a *graded* S-module, if it has a direct sum decomposition $M = \bigoplus_{i \in \mathbb{Z}} M_i$ as $\Bbbk$-vector spaces and $S_i M_j \subseteq M_{i+j}$ for all $i, j \in \mathbb{Z}$. For M and graded S-module and $p \geqslant 0$, we consider the graded module $M(-p)$ with graded parts $M(-p)_i = M_{i-p}$. Of particular interest for us is the free graded module $S(-p)$ defined by $S(-p)_i = S_{i-p}$, i.e., for $p \geqslant 0$ the module $S(-p)$ is shifted p degrees with $S(-p)_p = S_0 = \Bbbk$. Given a monomial ideal $I \subset S$, from Theorem 2.2.4 and Corollary 2.2.6, we obtain that

$$I = \bigoplus_{j \geqslant 0} I_j \qquad \text{and} \qquad S/I = \bigoplus_{j \geqslant 0} [S/I]_j = \bigoplus_{j \geqslant 0} S_j/I_j.$$

are graded S-modules where the graded parts are finite dimensional $\Bbbk$-vector spaces. We will see that this is also holds when I is a homogeneous ideal.

Definition 2.4.3. Let M be a graded S-module with finite dimensional parts. The *Hilbert series* of M is the following Laurent series

$$\mathrm{Hilb}_M(t) := \sum_{k \in \mathbb{Z}} \dim_{\Bbbk}(M_j)\, t^k.$$

Our primary case of interest is the Hilbert series of a quotient ring S/I; in this case, we have a power series $\mathrm{Hilb}_{S/I}(t) = \sum_{k \geqslant 0} \dim_{\Bbbk}([S/I]_k)\, t^k \in \mathbb{N}[\![t]\!]$ because $[S/I]_k = 0$ for $k < 0$.

Our goal is to prove the following important theorem.

Theorem 2.4.4 (Hilbert). *Let $I \subset S = \Bbbk[x_1, \ldots, x_n]$ be a monomial ideal and $X = V(I) \subset \mathbb{A}^n_{\Bbbk}$. Let $d = \dim(X)$ be the dimension of X. Then the following statements hold:*

(i) *We have the equality*

$$\mathrm{Hilb}_{S/I}(t) = \frac{Q(t)}{(1-t)^d}$$

where $Q(t) \in \mathbb{Z}[t]$ is a polynomial with integer coefficients and $Q(1) \in \mathbb{Z}_+$ is a positive integer.

(ii) *There is a unique polynomial*

$$P_X(z) = e_0 \frac{z^{d-1}}{(d-1)!} + (\text{lower degree terms}) \in \mathbb{Q}[z]$$

(called the Hilbert polynomial *of X) of degree $d-1$ such that $e_0 = Q(1)$ and*

$$P_X(k) = \dim_{\Bbbk}([S/I]_k)$$

for all $k \gg 0$.

Definition 2.4.5. Let $I \subset S$ be a monomial ideal and $X = V(I) \subset \mathbb{A}^n_{\Bbbk}$. Then the *degree* of X is given by $\deg(X) = e_0 = Q(1)$ where e_0 is the normalized leading coefficient of the Hilbert polynomial $P_X(z)$ and $Q(t)$ is the numerator of the Hilbert series $\mathrm{Hilb}_{S/I}(t)$.

To prove the above far-reaching theorem we shall need several technical results. We start with an import example.

EXAMPLE 2.4.6. In how many ways can you share k oranges with n people? This is a simple combinatorial problem whose solution is

$$\binom{k+n-1}{n-1} = \frac{(n+k-1)!}{(n-1)!k!}.$$

Equivalently, we can ask how many tuples $(a_1,\dots,a_n) \in \mathbb{N}^n$ do we have such that

$$a_1+\cdots+a_n = k?$$

Since the monomials of degree k give a $\Bbbk$-basis of S_k, we get

$$\dim_{\Bbbk}(S_k) = \binom{k+n-1}{n-1}.$$

On the other hand, the binomial theorem tells us that

$$\frac{1}{(1-t)^n} = \sum_{k=0}^{\infty}\binom{-n}{k}(-t)^k = \sum_{k=0}^{\infty}\binom{n+k-1}{k}t^k = \sum_{k=0}^{\infty}\binom{n+k-1}{n-1}t^k.$$

Therefore, we obtain the appealing fact

$$\mathrm{Hilb}_S(t) = \frac{1}{(1-t)^n} \in \mathbb{N}[\![t]\!].$$

We have that shifting makes a trivial change in terms of Hilbert series.

LEMMA 2.4.7. *Let M be a graded S-module with finite graded parts and $p \geqslant 0$. Then*

$$\mathrm{Hilb}_{M(-p)}(t) = t^p\mathrm{Hilb}_{M(p)}(t).$$

In particular, $\mathrm{Hilb}_{S(-p)}(t) = \frac{t^p}{(1-t)^n}$.

PROOF. Making the following simple algebraic manipulation

$$\mathrm{Hilb}_{M(-p)}(t) = \sum_{k\in\mathbb{Z}}\dim_{\Bbbk}\left(M_{k-p}\right)t^k = \sum_{k\in\mathbb{Z}}\dim_{\Bbbk}(M_k)\,t^{k+p} = t^p\mathrm{Hilb}_{M(p)}(t)$$

we get the equality. □

We say that an S-linear map $\varphi : M \to N$ graded S-modules is *graded* if $\varphi(M_k) \subset N_k$ for all $k \in \mathbb{Z}$. Let L, M, N be S-modules. We say that we have a short exact sequence

$$0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0;$$

if φ and ψ are S-linear maps, φ is injective, ψ is surjective and $\mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$. We say the short exact sequence is *graded* if the modules L, M, N and the maps φ, ψ are all graded.

The next lemma says that Hilbert series are additive.

LEMMA 2.4.8. *Let $0 \to L \to M \to N \to 0$ be a graded short exact sequence of graded S-modules with finite graded parts. Then*

$$\mathrm{Hilb}_M(t) = \mathrm{Hilb}_L(t) + \mathrm{Hilb}_N(t).$$

Proof. From the assumptions we get $M_k \cong L_k \bigoplus N_k$. So the required equality

$$\mathrm{Hilb}_M(t) = \sum_{j\in\mathbb{Z}} \dim_{\mathbb{k}}(M_j)\, t^j = \sum_{j\in\mathbb{Z}} \left(\dim_{\mathbb{k}}(L_j) + \dim_{\mathbb{k}}(N_j)\right) t^j = \mathrm{Hilb}_L(t) + \mathrm{Hilb}_N(t)$$

follows. □

We now discuss an “inclusion-exclusion” type of argument that will allow us to the express the Hilbert series of an intersection of monomial ideals. The starting point is with two ideals.

Lemma 2.4.9. *Let $I, J \subset S$ be two ideals. Then we have a natural short exact sequence*

$$0 \to S/I\cap J \xrightarrow{\varphi} S/I \oplus S/J \xrightarrow{\pi} S/I+J \to 0,$$

where $\varphi(f+I\cap J) = (f+I, f+J)$ *and* $\pi(f+I, g+J) = (f-g+I+J)$. *Moreover, if I and J are monomial ideals (or homogeneous as we will see later), then this short exact sequence is graded.*

Proof. For any $f+I+J \in S/I+J$, we have $\pi(f+I, 0+J) = f+I+J$; thus the map π is surjective. For any $f+I\cap J \in S/I\cap J$, if $\varphi(f+I\cap J) = (f+I, f+J) = (0+I, 0+J)$, then $f \in I\cap J$; thus the map φ is injective.

The inclusion $\mathrm{Im}(\varphi) \subset \mathrm{Ker}(\pi)$ is clear by construction. On the other hand, let $(f+I, g+J) \in \mathrm{Ker}(\pi)$. This means that $f-g \in I+J$, and so we can write $f-g = -a+b$ with $a \in I$ and $b \in J$. Since $f+a = g+b$, $a \in I$ and $b \in J$, it now follows that

$$\varphi(f+a+I\cap J) = (f+a+I, g+b+J) = (f+I, g+J);$$

hence $(f+I, g+J) \in \mathrm{Im}(\varphi)$. Therefore, $\mathrm{Im}(\varphi) = \mathrm{Ker}(\pi)$ and it follows that we have a short exact sequence.

If I and J are monomial ideals, then the modules $S/I\cap J$, $S/I \oplus S/J$, $S/I+J$ are graded (see Theorem 2.2.4 and Corollary 2.2.6) and the maps φ and π are clearly graded. □

Notation 2.4.10. Given a sequence of monomial ideals $I_1, \dots, I_k \subset S$ and a subset $\mathfrak{J} \subseteq [k]$, we define the ideal $I_{\mathfrak{J}} := \sum_{i\in\mathfrak{J}} I_i$. If $\mathfrak{J} = \emptyset$, we set $I_{\mathfrak{J}} = S$. We further specify

$$\mathrm{IE}(\{I_1, \dots, I_k\})(t) \;:=\; \sum_{\mathfrak{J}\subseteq[k]} (-1)^{|\mathfrak{J}|-1} \mathrm{Hilb}_{S/I_{\mathfrak{J}}}(t) \in \mathbb{N}[\![t]\!].$$

The next result is only valid for monomial ideals and it uses the distributive law from Exercise 2.1.

Proposition 2.4.11. *Let $I_1, \dots, I_k \subset S$ be monomial ideals and consider the intersection $I = I_1 \cap \dots \cap I_k \subset S$. Then we have the equality*

$$\mathrm{Hilb}_{S/I}(t) \;=\; \mathrm{IE}(\{I_1, \dots, I_k\})(t).$$

PROOF. We proceed by induction on k. The case $k = 1$ is clear. From Lemma 2.4.9, we have the short exact sequence

$$0 \to S/I \to S/I_1 \cap \cdots \cap I_{k-1} \oplus S/I_k \to S/(I_1 \cap \cdots \cap I_{k-1}) + I_k \to 0.$$

The additivity of Hilbert series (see Lemma 2.4.8) gives the equality

$$\mathrm{Hilb}_{S/I}(t) = \mathrm{Hilb}_{S/I_1\cap\cdots\cap I_{k-1}}(t) + \mathrm{Hilb}_{S/I_k}(t) - \mathrm{Hilb}_{S/(I_1\cap\cdots\cap I_{k-1})+I_k}(t).$$

Due to Exercise 2.1, we have the distributive equality

$$(I_1 \cap \cdots \cap I_{k-1}) + I_k \;=\; (I_1 + I_k) \cap \cdots \cap (I_{k-1} + I_k).$$

After applying the inductive hypothesis to the monomial ideals $J_1 = I_1 \cap \cdots \cap I_{k-1}$ and $J_2 = (I_1 + I_k) \cap \cdots \cap (I_{k-1} + I_k)$, we obtain

$$\begin{aligned}
\mathrm{Hilb}_{S/J}(t) &= \mathrm{Hilb}_{S/J_1}(t) + \mathrm{Hilb}_{S/I_k}(t) - \mathrm{Hilb}_{S/J_2}(t)\\
&= \mathrm{IE}(I_1, \ldots, I_{k-1})(t) + \mathrm{Hilb}_{S/I_k}(t) - \mathrm{IE}(I_1 + I_k, \ldots, I_{k-1} + I_k)(t)\\
&= \sum_{\mathfrak{J}\subseteq[k-1]} (-1)^{|\mathfrak{J}|-1}\mathrm{Hilb}_{S/I_{\mathfrak{J}}}(t) + \mathrm{Hilb}_{S/I_k}(t) + \sum_{\{k\}\subsetneq\mathfrak{J}\subseteq[k]} (-1)^{|\mathfrak{J}|-1}\mathrm{Hilb}_{S/I_{\mathfrak{J}}}(t)\\
&= \mathrm{IE}(\{I_1, \ldots, I_k\})(t)
\end{aligned}$$

whence the result follows. □

Another necessary ingredient is that of regular sequences. Given an S-module M, we say that $f \in S$ is regular (or a nonzerodivisor) on M if whenever $w \in M$ and $fw = 0 \in M$ then $w = 0 \in M$.

DEFINITION 2.4.12. A sequence of polynomials $f_1, \ldots, f_m$ in S is *regular* if the two following conditions hold:

(i) $(f_1, \ldots, f_m) \neq S$.
(ii) $f_1 \neq 0$ and f_i is regular on $S/(f_1, \ldots, f_{i-1})$ for all $i \geqslant 2$.

The lemma below gives another reason why ideals generated by pure powers of the variables are quite special.

PROPOSITION 2.4.13. *Let* $Q = (x_{i_1}^{a_1}, \ldots, x_{i_k}^{a_k}) \subset S$ *be an ideal generated by pure powers of the variables (with* $i_1 < \cdots < i_k$ *and* $a_j > 0$ *for all* $1 \leqslant j \leqslant k$*). Then the following statements hold:*

(i) $x_{i_1}^{a_1}, \ldots, x_{i_k}^{a_k}$ *form a regular sequence.*
(ii) *We have the equality*

$$\mathrm{Hilb}_{S/Q}(t) \;=\; \frac{\prod_{j=1}^{k}(1 + t + t^2 + \cdots + t^{a_j-1})}{(1-t)^d}$$

where $d = n - k = \dim(V(Q))$.

Proof. (i) By Lemma 2.2.12, we have

$$\left(x_{i_1}^{a_1},\dots,x_{i_{j-1}}^{a_{j-1}}\right):x_{i_j}^{a_j} \;=\; \left(x_{i_1}^{a_1},\dots,x_{i_{j-1}}^{a_{j-1}}\right).$$

Hence Exercise 2.6 implies that $x_{i_1}^{a_1},\dots,x_{i_k}^{a_k}$ form a regular sequence.

(ii) Let $j \geqslant 1$. Let $J = \left(x_{i_1}^{a_1},\dots,x_{i_j}^{a_j}\right) \subset S$ and $J' = \left(x_{i_1}^{a_1},\dots,x_{i_{j-1}}^{a_{j-1}}\right) \subset S$ (when $j=1$, we have by convention $J'=0$). We claim that we have a graded short exact sequence

$$0 \to S/J'(-a_j) \xrightarrow{\varphi} S/J' \xrightarrow{\pi} S/J \to 0,$$

where $\varphi(f+J') = x_{i_j}^{a_j}f+J'$ and $\pi(f+J')=f+J$.

For any $f+J \in S/J$, we have $\pi(f+J')=f+J$; thus the map π is surjective. Notice that $\operatorname{Im}(\varphi)=\operatorname{Ker}(\pi)$ because for any $f+J' \in S/J'$ we have $\pi(f+J')=f+J=0+J$ if and only if $f+J'=x_{i_j}^{a_j}g+J'$ for some $g \in S$. We know that φ is injective because $x_{i_j}^{a_j}$ is regular on S/J'. Thus we indeed have a short exact sequence.

It remains to show that the short exact sequence is graded. All the considered modules are graded since we are dealing with monomial ideals. The map π is clearly graded. For any $f+J' \in \left[S/J'(-a_j)\right]_k = [S/J']_{k-a_j}$ (i.e., $f \in S$ is a homogeneous polynomial with $\deg(f)=k-a_j$), we obtain

$$\varphi(f+J') \;=\; x_{i_j}^{a_j}f+J' \;\in\; \left[S/J'\right]_k;$$

so φ is also graded. This concludes the proof that we have a graded short exact sequence.

By combining Lemma 2.4.8 and Lemma 2.4.7, we get

$$\operatorname{Hilb}_{S/J}(t) \;=\; \operatorname{Hilb}_{S/J'}(t) - t^{a_j}\operatorname{Hilb}_{S/J'}(t) \;=\; (1-t^{a_j})\operatorname{Hilb}_{S/J'}(t).$$

Finally, proceeding inductively and utilizing the initial computation of Example 2.4.6, we obtain

$$\begin{aligned}
\operatorname{Hilb}_{S/Q}(t) \;&=\; \frac{\prod_{j=1}^{k}(1-t^{a_j})}{(1-t)^n}\\
&=\; \frac{\prod_{j=1}^{k}(1-t)(1+t+t^2+\cdots+t^{a_j-1})}{(1-t)^n}\\
&=\; \frac{\prod_{j=1}^{k}(1+t+t^2+\cdots+t^{a_j-1})}{(1-t)^d},
\end{aligned}$$

as required. □

Remark 2.4.14 (A very simple version of Bezout theorem). Let $Q=(x_{i_1}^{a_1},\dots,x_{i_k}^{a_k}) \subset S$ and $X = V(Q) \subset \mathbb{A}_{\mathbb{k}}^n$. Then Proposition 2.4.13(ii) yields the formula

$$\deg(X) \;=\; a_1\cdots a_k \neq 0.$$

Our last necessary ingredients is the following structural result regarding power series. First discuss a well-know characterization of *numerical polynomials*. Let $F:\mathbb{Z}\to\mathbb{Z}$ be a function. We define the *difference operator* by setting $(\Delta F)(n) := F(n+1) - F(n)$ for all $n \in \mathbb{Z}$. For all $i \geqslant 1$, we set $\Delta^i F = \Delta(\Delta^{i-1}F)$. Notice that $\Delta^i F$ is also a function from the integers to the integers.

LEMMA 2.4.15. *Let* $P(z) \in \mathbb{Q}[z]$ *be a polynomial of degree* $d-1$. *Then the following conditions are equivalent:*

(a) $P(k) \in \mathbb{Z}$ *for all* $k \in \mathbb{Z}$ (*this means that* $P(z)$ *is a numerical polynomial*).

(b) *There exist integers* $a_0, \dots, a_{d-1} \in \mathbb{Z}$ *such that*

$$P(z) = \sum_{i=0}^{d-1} a_i \binom{z+i}{i}.$$

PROOF. The implication (b) ⇒ (a) is clear.

Thus we concentrate on the implication (a) ⇒ (b). Notice that the polynomials $\binom{z+i}{i}$ form a $\mathbb{Q}$-basis of $\mathbb{Q}[z]$ (this can be proved for instance by utilizing the division algorithm on $\mathbb{Q}[z]$). Therefore we can write $P(z) = \sum_{i=0}^{d-1} a_i \binom{z+i}{i}$. The identity $\binom{z+i+1}{i} - \binom{z+i}{i} = \binom{z+i}{i-1}$. Thus we have

$$\Delta P(z) = \sum_{i=1}^{d-1} a_i \binom{z+i}{i-1},$$

and so applying the difference operator i-times yields

$$\Delta^i P(z) = \sum_{j=i}^{d-1} a_i \binom{z+j}{j-i}.$$

This implies that $a_i = \Delta^i P(-i-1) \in \mathbb{Z}$, as required. □

LEMMA 2.4.16. *Let* $H(t) = \frac{Q(t)}{(1-t)^d} = \sum_{k=0}^{\infty} a_k t^k \in \mathbb{N}[\![t]\!]$ *be a power series where* $Q(t) \in \mathbb{Z}[t]$ *is a polynomial with integer coefficients and* $Q(1) \neq 0$. *Then the following statements hold:*

(i) $Q(1) \in \mathbb{Z}_+$ *is a positive integer.*

(ii) *There is a polynomial* $P(z) = e_0 \frac{z^{d-1}}{(d-1)!} + (\text{lower degree terms}) \in \mathbb{Q}[z]$ *of degree* $d-1$ *such that* $e_0 = Q(1)$ *and* $P(k) = a_k$ *for all* $k \gg 0$.

PROOF. By assumption, we have $Q(t) = \sum_{j=0}^{m} c_j t^j$ where $c_j \in \mathbb{Z}$ is an integer. We can write $Q(t) = \sum_{j=0}^{\ell} e_j (1-t)^j$. It is then clear that $e_0 = Q(1) = \sum_{j=0}^{m} c_j$ is a nonzero integer. We can make the expansion

$$H(t) = \frac{\sum_{j=0}^{\ell} e_j (1-t)^j}{(1-t)^d} = \sum_{j=0}^{d-1} \frac{e_j}{(1-t)^{d-j}} + \sum_{j=d}^{\ell} e_j (1-t)^{j-d}.$$

Let $H'(t) = \sum_{j=0}^{d-1} \frac{e_j}{(1-t)^{d-j}} = \sum_{k\geqslant 0} b_k t^k$. Notice that $b_k = a_k$ for $k \gg 0$ because $\sum_{j=d}^{\ell} e_j(1-t)^{j-d}$ is a polynomial and so it has finitely many terms. Due to Example 2.4.6, we can expand

$$\begin{aligned} H'(t) &= \sum_{j=0}^{d-1} \frac{e_j}{(1-t)^{d-j}} \\ &= \sum_{j=0}^{d-1} e_j \sum_{k=0}^{\infty} \binom{k+d-j-1}{d-j-1} t^k \\ &= \sum_{k=0}^{\infty} \left(\sum_{j=0}^{d-1} e_j \binom{k+d-j-1}{d-j-1} \right) t^k. \end{aligned}$$

Consider the polynomial $P(z) = \sum_{j=0}^{d-1} e_j \binom{z+d-j-1}{d-j-1} \in \mathbb{Q}[z]$. By construction we have that $P(k) = b_k = a_k$ for $k \gg 0$ and that

$$P(z) = e_0 \frac{z^{d-1}}{(d-1)!} + (\text{lower degree terms}) \in \mathbb{Q}[z].$$

Finally, notice that

$$e_0 = (d-1)! \lim_{k\to\infty} \frac{P(k)}{k^{d-1}} = (d-1)! \lim_{k\to\infty} \frac{a_k}{k^{d-1}} \geqslant 0.$$

So the result follows. □

We now have all the ingredients to prove Theorem 2.4.4.

Proof of Theorem 2.4.4. Let $I \subset S = \mathbb{k}[x_1, \ldots, x_n]$ be a monomial ideal and $X = V(I) \subset \mathbb{A}_{\mathbb{k}}^n$. Let $d = \dim(X)$. By Theorem 2.3.1, let $I = \bigcap_{j=1}^k I_j$ be the irredundant decomposition into ideals generated by pure powers of the variables. Following Notation 2.4.10, for each subset $\mathfrak{J} \subset [k]$, we set $X_{\mathfrak{J}} = V(I_{\mathfrak{J}})$ and $d_{\mathfrak{J}} = \dim(X_{\mathfrak{J}})$, where $I_{\mathfrak{J}} = \sum_{j\in\mathfrak{J}} I_j \subset S$. Notice that each $I_{\mathfrak{J}}$ is an ideal generated by pure powers. We also have that $d_{\mathfrak{J}} = \dim(X_{\mathfrak{J}}) \leqslant d$. By utilizing Proposition 2.4.11 and Proposition 2.4.13, we obtain

$$\begin{aligned} \mathrm{Hilb}_{S/I}(t) &= \sum_{\mathfrak{J}\subseteq[k]} (-1)^{|\mathfrak{J}|-1} \mathrm{Hilb}_{S/I_{\mathfrak{J}}}(t) \\ &= \sum_{\mathfrak{J}\subseteq[k]} (-1)^{|\mathfrak{J}|-1} \frac{Q_{\mathfrak{J}}(t)}{(1-t)^{d_{\mathfrak{J}}}} \\ &= \frac{\sum_{\mathfrak{J}\subseteq[k]} (-1)^{|\mathfrak{J}|-1} (1-t)^{d-d_{\mathfrak{J}}} Q_{\mathfrak{J}}(t)}{(1-t)^d} \\ &= \frac{Q(t)}{(1-t)^d}, \end{aligned}$$

where each $Q_{\mathfrak{J}}(t) \in \mathbb{Z}[t]$ is a polynomial with integer coefficients. Thus $Q(t) \in \mathbb{Z}[t]$ is also a polynomial with integer coefficients. If we show that $Q(1) \neq 0$, then the proof would be completed by Lemma 2.4.16. Indeed, we would obtain that $Q(1) \in \mathbb{Z}_+$ and the existence of a polynomial $P_X(z) \in \mathbb{Q}[z]$ of degree $d-1$ with normalized leading coefficient equal to $Q(1)$ and such that $P_X(j) = \dim_{\mathbb{k}}\left([S/I]_j\right)$ for all $j \gg 0$.

By contradiction assume $Q(1) = 0$. Hence we can write $Q(t) = (1-t)^c Q'(t)$ with $Q'(1) \neq 0$ and $c \geqslant 1$. Notice that $Q'(t) = \frac{1}{(1-t)^c} Q(t)$ also have integer coefficients. Let $e = d-c$ and observe that $\mathrm{Hilb}_{S/I}(t) = \frac{Q'(t)}{(1-t)^e}$. From Lemma 2.4.16, we get a polynomial $P_X(z) \in \mathbb{Q}[z]$ of degree $e-1$ such $P_X(k) = \dim_{\mathbb{k}}([S/I]_j)$ for all $j \gg 0$. We may assume that the ideal $I_1 \subset S$ is generated by $n-d$ pure powers of the variables and thus $\dim(X_1) = d$. By applying Lemma 2.4.16 and Proposition 2.4.13 to the ideal $I_1 \subset S$ generated by pure powers of the variables, we get a polynomial $P_{X_1}(z) \in \mathbb{Q}[z]$ of degree $d-1$ such that $P_{X_1}(j) = \dim_{\mathbb{k}}([S/I_1]_j)$ for all $j \gg 0$. Since $I \subset I_1$, it follows that $\dim_{\mathbb{k}}([S/I_1]_j) \leqslant \dim_{\mathbb{k}}([S/I]_j)$ for all $j \in \mathbb{N}$ (see Theorem 2.2.4 and Corollary 2.2.6). However, this leads to the following clear contradiction

$$P_{X_1}(j) \;=\; \dim_{\mathbb{k}}([S/I_1]_j) \;\leqslant\; \dim_{\mathbb{k}}([S/I]_j) \;=\; P_X(j) \quad \text{for all} \quad j \gg 0,$$

because by assumption $\deg(P_X) = e-1 < d-1 = \deg(P_{X_1})$.

Finally, we should have $Q(1) \neq 0$, thus concluding the proof of the theorem. □

2.5. Maclagan's theorem (an extension of Dickson's lemma)

Here we discuss an interesting extension of Dickson's lemma given by Maclagan [7]. Given any collection of ideals $\mathscr{A} = \{I_\lambda\}_{\lambda \subset \Lambda}$ of ideals in S, we denote by $\mathscr{A}^{\max}$ the collection of ideals is $\mathscr{A}$ that are maximal with respect to inclusion. We prove the following finiteness theorem.

THEOREM 2.5.1 (Maclagan [7]). *Let $\mathscr{A} = \{I_\lambda\}_{\lambda \subset \Lambda}$ be a collection of monomial ideals in S. Then $\mathscr{A}^{\max}$ is a finite set.*

Notice that if each each $I_\lambda \subset S$ is a principal monomial ideal (i.e., generated by one monomial), then the above theorem is precisely Dickson's lemma (see Theorem 2.2.2). It should be mentioned that this finiteness result is false for not monomial ideals as shown by next easy example.

EXAMPLE 2.5.2. Let $S = \mathbb{k}[x]$ with $\mathbb{k}$ an infinite field. Consider the infinite collection of principal ideals $\mathscr{A} = \{I_a\}_{a \in \mathbb{k}}$ with $I_a = (x-a) \subset S$. Then $\mathscr{A}^{\max} = \mathscr{A}$.

An equivalent formulation of Theorem 2.5.1 is given in the next result.

LEMMA 2.5.3. *We have that Theorem 2.5.1 holds if and only if for any infinite collection $\mathscr{A}$ of monomial ideals in S there is an infinite chain $I_1 \supsetneq I_2 \supsetneq \cdots$ of ideals in $\mathscr{A}$.*

PROOF. Assume that Theorem 2.5.1 holds. Let $\mathscr{A}$ infinite collection of monomial ideals. Since $\mathscr{A}^{\max}$ is a finite set and $\mathscr{A}$ is infinite, there should be an ideal $I_1 \in \mathscr{A}^{\max}$ such that the collection $\mathscr{A}_1 = \{I \in \mathscr{A} \mid I_1 \supsetneq I\}$ is infinite. By applying the same argument, we can choose $I_2 \in \mathscr{A}_1^{\max}$ such that the collection $\mathscr{A}_2 = \{I \in \mathscr{A}_1 \mid I_2 \supsetneq I\}$ is infinite. Therefore, by proceeding inductively, we have infinite chain $I_1 \supsetneq I_2 \supsetneq \cdots$ of ideals in $\mathscr{A}$.

On the other hand, suppose that the other condition holds. Let $\mathscr{A}$ be a collection of monomial ideals. If $\mathscr{A}^{\max}$ were infinite, then we would obtain two ideals $I_1 \supsetneq I_2$ in $\mathscr{A}^{\max}$, but this is a contradiction because the ideals in $\mathscr{A}^{\max}$ are incomparable. Thus the proof is complete. □

We say that a monomial ideal $I \subset S$ is said to be *Artinian* if one has $\dim_{\Bbbk}(S/I) < \infty$ (see Exercise 2.7). By Corollary 2.2.6, a monomial ideal $I \subset S$ is Artinian if and only if it has finitely many standard monomials.

LEMMA 2.5.4. *Let $\mathscr{A}$ be collection of Artinian monomial ideals in S. Then $\mathscr{A}^{\max}$ is a finite set.*

PROOF. By contradiction assume that $\mathscr{B} = \mathscr{A}^{\max}$ is infinite. Choose $I_1 \in \mathscr{B}$. For each $I \in \mathscr{B} \setminus \{I_1\}$, since I and I_1 are incomparable, it follows that I contains some of the finite number of standard monomials of I_1. As a consequence, there are an infinite number of ideals in $\mathscr{B}$ which contain the same subset of standard monomials of I_1. We call this collection $\mathscr{B}_1$. Let $J_1 \subset S$ be the intersection of the ideals in $\mathscr{B}_1$. Notice that J_1 is a nonzero monomial ideal.

We will now build a strictly ascending chain of monomial ideals, which will be a contradiction by Proposition 2.2.10. Suppose $\mathscr{B}_k$ and J_k have been chosen. Choose an ideal $I_{k+1} \in \mathscr{B}_k$. We can again find an infinite collection of ideals in $\mathscr{B}_k$ which have the same nontrivial intersection with the standard monomials of I_{k+1}. Let $\mathscr{B}_{k+1}$ be this collection, and let J_{k+1} be the intersection of the ideals in $\mathscr{B}_{k+1}$. Since $J_k = \bigcap_{I \in \mathscr{B}_k} I$, $J_{k+1} = \bigcap_{I \in \mathscr{B}_{k+1}} I$ and $\mathscr{B}_k \supset \mathscr{B}_{k+1}$, we clearly have the inclusion $J_{k+1} \supseteq J_k$. However, we have a proper inclusion $J_{k+1} \supsetneq J_k$ because J_{k+1} contains some standard monomials of I_{k+1}. Therefore, with this procedure we get an infinite strictly ascending chain of monomial ideals in S, which is impossible by Proposition 2.2.10. Thus the proof is complete. □

Let $I \subset S$ be a monomial ideal. By Theorem 2.3.1, we have a unique irredundant decomposition

$$I = \bigcap_{i=1}^{m} Q_i$$

where each $Q_i \subset S$ is an ideal generated by pure powers. From Remark 2.3.4, we know that each Q_i is a primary ideal with respect ideal generated by variables. For each subset $\mathfrak{J} = \{j_1, \ldots, j_k\} \subseteq [n] = \{1, \ldots, n\}$, let $\sigma_{\mathfrak{J}}(I)$ be the intersection of the Q_i's that are primary with respect to $P_{\mathfrak{J}} = \left(x_{j_1}, \ldots, x_{j_k}\right) \subset S$. By convention, we have $\sigma_{\mathfrak{J}}(I) = S$ if no Q_i is $P_{\mathfrak{J}}$-primary. When $\sigma_{\mathfrak{J}}(I)$ is a proper ideals it is $P_{\mathfrak{J}}$-primary due to Exercise 2.8. Then we obtain the following primary decomposition

$$I = \bigcap_{\mathfrak{J}\subseteq[n]} \sigma_{\mathfrak{J}}(I).$$

We call this decomposition the *standard primary decomposition* of I. Notice that the monomial generators of $\sigma_{\mathfrak{J}}(I)$ only involve the variables in the set $\{x_j \mid j \in \mathfrak{J}\}$ and that when we regard $\sigma_{\mathfrak{J}}(I)$ as an ideal in the polynomial subring $\Bbbk[x_j \mid j \in \mathfrak{J}]$ it becomes Artinian.

Proof of Theorem 2.5.1. By Lemma 2.5.3, we may assume that $\mathscr{A}$ is an infinite collection of monomial ideals in S, and we need to show the existence of an infinite chain $I_1 \supsetneq I_2 \supsetneq \cdots$ of ideals in $\mathscr{A}$.

For each $\mathfrak{J} \subseteq [n]$, we consider the following collection

$$\sigma_{\mathfrak{J}}(\mathscr{A}) := \left\{\sigma_{\mathfrak{J}}(I) \mid I \in \mathscr{A}\right\}$$

of Artinian monomial ideals in $\Bbbk[x_j \mid j \in \mathfrak{J}]$.

Let $\mathfrak{J} \subseteq [n]$ be any subset. Then we have the following two cases:

(i) If $\sigma_{\mathfrak{J}}(\mathscr{A})$ is a finite set, then there should be an infinite collection of ideals $\mathscr{A}' \subset \mathscr{A}$ such that $\sigma_{\mathfrak{J}}(I)$ is the same for all $I \in \mathscr{A}'$.

(ii) If $\sigma_{\mathfrak{J}}(\mathscr{A})$ is an infinite set, then Lemma 2.5.4 and Lemma 2.5.3 give an infinite family $\{I_k\}_{k\geqslant 1} \subset \mathscr{A}$ such that $\sigma_{\mathfrak{J}}(I_1) \supsetneq \sigma_{\mathfrak{J}}(I_2) \supsetneq \cdots$.

In either case, we obtain an infinite family $\{I_k\}_{k\geqslant 1} \subset \mathscr{A}$ such that $\sigma_{\mathfrak{J}}(I_1) \supseteq \sigma_{\mathfrak{J}}(I_2) \supseteq \cdots$ for all $\mathfrak{J} \subseteq [n]$, although the inclusions need not be proper.

By running the above procedure over each $\mathfrak{J} \subseteq [n]$ and restricting at each step, we obtain an infinite family $\{I_k\}_{k\geqslant 1} \subset \mathscr{A}$ such that $\sigma_{\mathfrak{J}}(I_1) \supseteq \sigma_{\mathfrak{J}}(I_2) \supseteq \cdots$ for all $\mathfrak{J} \subseteq [n]$. Since $I_k = \bigcap_{\mathfrak{J}\subseteq[n]} \sigma_{\mathfrak{J}}(I_k)$, we have an infinite sequence $I_1 \supseteq I_2 \supseteq \cdots$ in $\mathscr{A}$. As all ideals are different we should have an infinite sequence $I_1 \supsetneq I_2 \supsetneq \cdots$ in $\mathscr{A}$. So the proof is complete. □

The theorem of Maclagan has some surprising consequences.

Corollary 2.5.5. *There are only finitely many monomial ideals in S with a given Hilbert series.*

Proof. Let $H(t) = \sum_{k=0}^{\infty} a_k t^k \in \mathbb{N}[\![t]\!]$ be a power series. Consider the collection

$$\mathscr{A} := \left\{I \subset S \text{ monomial ideal } \mid \operatorname{Hilb}_{S/I}(t) = H(t)\right\}$$

of monomial ideals with Hilbert series equal to $H(t)$. Notice that, for any two monomial ideals $I \subseteq J$ in $\mathscr{A}$, we should have $I = J$ (indeed, for all $k \geqslant 0$, we have $I_k \subseteq J_k$ and $\dim_{\Bbbk}(I_k) = \binom{k+n-1}{n-1} - a_k = \dim_{\Bbbk}(J_k)$). Thus every ideal of $\mathscr{A}$ is maximal. Finally, by Theorem 2.5.1, we obtain that $\mathscr{A} = \mathscr{A}^{\max}$ is a finite set. □

Remark 2.5.6. The finiteness result of Corollary 2.5.5 is quite potent. It tells us that many challenging problems can be reduced to studying finitely many monomial ideals. Just to mention one result: the celebrated proof of Hartshorne on the connectedness of Hilbert schemes inherently relies on the fact that there are finitely many monomial ideals with the same Hilbert polynomial (see [4, 10]).

2.6. Exercises

EXERCISE 2.1. *Let* I, J *and* K *be monomial ideals in* S. *Show that* $I + (J \cap K) = (I + J) \cap (I + K)$.

EXERCISE 2.2. *Let* I, J *and* K *be monomial ideals in* S. *Show that* $I \cap (J + K) = (I \cap J) + (I \cap K)$.

EXERCISE 2.3. *Show that a monomial ideal* $I \subset S$ *is a prime ideal if and only if* I *is generated by a subset of the variables.*

EXERCISE 2.4. *Let* $I, J \subset S$ *be monomial ideals. Show that* $I : J^\infty$ *is also a monomial ideal.*

EXERCISE 2.5. *Let* $I \subset S$ *be a monomial ideal. Show that* $\sqrt{I}$ *is also a monomial ideal.*

EXERCISE 2.6. *Let* $f_1, \ldots, f_m \in S$ *be polynomials such that* $(f_1, \ldots, f_m) \neq S$. *Show that* $f_1, \ldots, f_m$ *form a regular sequence if and only if* $f_1 \neq 0$ *and* $(f_1, \ldots, f_{i-1}) : f_i = (f_1, \ldots, f_{i-1})$ *for* $i \geqslant 2$.

EXERCISE 2.7. *Let* $I \subset S$ *be a proper monomial ideal. Show that the following conditions are equivalent:*

(a) I *is Artinian.*
(b) I *is* $\mathfrak{m}$*-primary where* $\mathfrak{m} = (x_1, \ldots, x_n)$ *is the ideal generated by all variables.*
(c) *For each* $1 \leqslant i \leqslant n$, *there is some* $a_i \geqslant 1$ *such that* $x_i^{a_i} \in I$.

EXERCISE 2.8. *Let* $P \subset S$ *be a prime ideal and* I, J *be two* P*-primary ideals. Show that* $I \cap J$ *is a* P*-primary ideal.*

EXERCISE 2.9. *Let* $X \subset \mathbb{A}^n_{\Bbbk}$ *and* $Y \subset \mathbb{A}^m_{\Bbbk}$ *be varieties determined by monomial ideals. Consider the product variety* $Z = X \times Y \subset \mathbb{A}^n_{\Bbbk} \times \mathbb{A}^m_{\Bbbk} \cong \mathbb{A}^{n+m}_{\Bbbk}$. *Notice that* $Z \subset \mathbb{A}^{n+m}_{\Bbbk}$ *is also determined by a monomial ideal. Show that*

$$\dim(Z) = \dim(X) + \dim(Y) \qquad \textit{and} \qquad \deg(Z) = \deg(X) \cdot \deg(Y).$$

CHAPTER 3

Gröbner bases

The instructions for this chapter are:

- **Read** [3, Chapter 2]**.**
- **Read** [5, Chapter 2]**.**

Here we shall only present relevant results without proofs.

3.1. Monomial orders

Let X be a set. A *partial order* on X is a binary relation $\leqslant$ over X which is *reflexive*, *antisymmetric* and *transitive*. That is, for all $a, b, c \in X$ we have

- $a \leqslant a$ (reflexivity);
- if $a \leqslant b$ and $b \leqslant a$, then $a = b$ (antisymmetry);
- if $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$ (transitivity).

It is common to write $a < b$ if $a \leqslant b$ and $a \neq b$. We also write $a \geqslant b$ ($a > b$), if $b \leqslant a$ ($b < a$). A typical example of a partially ordered set is the set of all subsets of a given set ordered by inclusion.

A partial order $\leqslant$ on X is called a *total order*, if for any two elements $a, b \in X$ one has $a \leqslant b$ or $b \leqslant a$.

Let $\Bbbk$ be a field and $S = \Bbbk[x_1, \ldots, x_n]$. We now define a total order on $\mathrm{Mon}(S)$, the set of all monomials in S, which respects the multiplicative structure on this set.

DEFINITION 3.1.1. A *monomial order* on S is a total order $\leqslant$ on $\mathrm{Mon}(S)$ with the properties:

(i) $1 \leqslant u$ for all $u \in \mathrm{Mon}(S)$.
(ii) If $u, v \in \mathrm{Mon}(S)$ and $u \leqslant v$, then $uw \leqslant vw$ for all $w \in \mathrm{Mon}(S)$.

A monomial order satisfies the following two conditions.

LEMMA 3.1.2. *Let $<$ be a monomial order on S. Then the following holds:*

(i) *If $u, v \in \mathrm{Mon}(S)$ with $u \mid v$, then $u \leqslant v$.*
(ii) *(Artinian order) If $u_1, u_2, \ldots$ is a sequence of monomials with $u_1 \geqslant u_2 \geqslant \cdots$, then there exists an integer m such that $u_i = u_m$ for all $i \geqslant m$.*

PROOF. (i) If $u \mid v$, then there exists a monomial w such that $v = uw$. Since $1 \leqslant w$, it follows that $u \leqslant wu = v$.

(ii) Let $\mathcal{M} = \{u_1, u_2, \ldots\}$. By Dickson's lemma (Theorem 2.2.2) this set has, with respect to divisibility, only a finite number of minimal elements, say $u_{i_1}, \ldots, u_{i_r}$ with $i_1 < i_2 < \cdots < i_r$. Let j be any integer $\geqslant i_r$. Then there exists an integer $1 \leqslant k \leqslant r$ such that $u_{i_k} \mid u_j$. By part (i), this implies that $u_{i_k} \leqslant u_j$. Hence $u_{i_k} \geqslant u_{i_r} \geqslant u_j \geqslant u_{i_k}$, and so $u_j = u_{i_r}$. Therefore we may choose $m = i_r$. □

The fact that a monomial order induces a well-ordering on $\mathrm{Mon}(S)$ is assumed as a condition in the definition of monomial orders given in [3, Definition 1, page 55]. This assumption is *not* necessary as it follows from Dickson's lemma.

Remark 3.1.3. Let $<$ be a monomial order. Then $<$ is a well-ordering on $\mathrm{Mon}(S)$. This means that every nonempty subset of $\mathrm{Mon}(S)$ has a smallest element under $<$. In other words, if $\mathcal{M} \subset \mathrm{Mon}(S)$ is nonempty, then there is $w \in M$ such that $v > w$ for every $v \neq w$ in $\mathcal{M}$.

Proof. Let $\mathcal{M} \subset \mathrm{Mon}(S)$ be a subset of monomials. By Dickson's lemma (Theorem 2.2.2), we have $\mathcal{M}^{\min} = \{u_1, \ldots, u_r\}$. Since a monomial order is multiplicative, for any $u \in \mathcal{M}$, we get $u \geqslant u_i$ for some $1 \leqslant i \leqslant r$. Therefore, by taking u_0 to be the smallest element among $\{u_1, \ldots, u_r\}$ with respect to the monomial order $<$, it follows that u_0 is the smallest element of $\mathcal{M}$. □

3.2. Basics of Gröbner basis

(Read the recommended references.)

3.3. Hilbert basis theorem

(Read the recommended references.)

3.4. Division algorithm and Buchberger algorithm

(Read the recommended references.)

3.5. Exercises

Exercise 3.1. *Let* $I, J \subset S$ *be two ideals and* $<$ *a monomial order on* S. *Let* $\mathcal{G}, \mathcal{G}'$ *be Gröbner bases of* I *and* J, *respectively, with respect to* $<$. *Prove that if* $\mathrm{in}_<(g)$ *and* $\mathrm{in}_<(g')$ *are relatively prime for any* $g \in \mathcal{G}, g' \in \mathcal{G}$, *then* $\mathcal{G} \cup \mathcal{G}'$ *is a Gröbner basis of* $I + J$.

Exercise 3.2. *Prove the following statements:*

(i) *There is a unique monomial order on* $\Bbbk[x_1]$.

(ii) *Let* $n \geqslant 2$. *Then there are infinite many monomial orders on* $S = \Bbbk[x_1, \ldots, x_n]$.

Exercise 3.3. *Let* $I \subset S$ *be an ideal and* $<$ *be a monomial order on* S. *Show that* $\mathrm{in}_<\left(\sqrt{I}\right) \subseteq \sqrt{\mathrm{in}_<(I)}$.

EXERCISE 3.4. *Let* $I \subset S$ *be an ideal and* $<$ *be a monomial order on* S. *Prove the following statements:*

(i) *If* $\mathrm{in}_<(I)$ *is radical, then* I *is radical.*
(ii) *If* $\mathrm{in}_<(I)$ *is prime, then* I *is prime.*

EXERCISE 3.5. *Let* $f_1, \ldots, f_m \in S$ *be polynomials and* $<$ *be a monomial order on* S. *Assume that* $\mathrm{in}_<(f_1), \ldots, \mathrm{in}_<(f_m)$ *is a regular sequence. Then prove the following statements:*

(i) $f_1, \ldots, f_m$ *is a regular sequence.*
(ii) $f_1, \ldots, f_m$ *is a Gröbner basis of* $I = (f_1, \ldots, f_m)$.

CHAPTER 4

The Algebra–Geometry Dictionary

4.1. Hilbert's Nullstellensatz (a first quick algebraic proof)

See, e.g., [8, §5]. The proof typically follows by utilizing Zariski's lemma.

4.2. Hilbert's Nullstellensatz (a second proof)

We follow the proof from [1].

Bibliography

[1] E. Arrondo, *Another elementary proof of the Nullstellensatz*, Amer. Math. Monthly **113** (2006), no. 2, 169–171. ↑34

[2] D. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*, Graduate Texts in Mathematics, vol. 185, Springer-Verlag, New York, 1998. ↑1

[3] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Fourth, Undergraduate Texts in Mathematics, Springer, Cham, 2015. An introduction to computational algebraic geometry and commutative algebra. ↑1, 2, 11, 31, 32

[4] R. Hartshorne, *Connectedness of the Hilbert scheme*, Inst. Hautes Études Sci. Publ. Math. **29** (1966), 5–48.↑30

[5] J. Herzog and T. Hibi, *Monomial ideals*, Graduate Texts in Mathematics, vol. 260, Springer-Verlag London, Ltd., London, 2011. ↑1, 14, 15, 31

[6] G. Kemper, *A course in commutative algebra*, Graduate Texts in Mathematics, vol. 256, Springer, Heidelberg, 2011. ↑1

[7] D. Maclagan, *Antichains of monomial ideals are finite*, Proc. Amer. Math. Soc. **129** (2001), no. 6, 1609–1615. ↑27

[8] H. Matsumura, *Commutative ring theory*, 1st ed., Cambridge Studies in Advanced Mathematics volume 8, Cambridge University Press, 1989. ↑34

[9] E. Miller and B. Sturmfels, *Combinatorial commutative algebra*, Graduate Texts in Mathematics, vol. 227, Springer-Verlag, New York, 2005. ↑1

[10] I. Peeva and M. Stillman, *Connectedness of Hilbert schemes*, J. Algebraic Geom. **14** (2005), no. 2, 193–211.↑30