Chapter 1

Polynomial Rings

"*Algebra is but written geometry*", Sophie Germain

After a course in linear algebra one often encounters abstract algebra. In that course one studies algebraic structures such as fields, rings and ideals. In this first chapter we introduce basics, with a focus on polynomials and Gröbner bases. We show how to use these for computing invariants of a polynomial ideal, such as the dimension or degree. The formalism we develop now will be applied to geometric situations in later chapters.

1.1. Ideals

Our most basic algebraic structure is that of a *field*. The elements of the field serve as numbers, also called scalars. We can add, subtract, multiply and divide them. It is customary to denote fields by the letter K, for the German word *Körper*. Our favorite field is the set $K = \mathbb{Q}$ of rational numbers. Another important field is the set $K = \mathbb{R}$ of real numbers. In practice, these two fields are very different. Numbers in $\mathbb{Q}$ can be manipulated by exact *symbolic computation*, whereas numbers in $\mathbb{R}$ are approximated by floating point representations and manipulated by *numerical computation*.

Other widely used fields are the set of complex numbers $\mathbb{C}$ and the finite field $\mathbb{F}_q$ with q elements. If K is not algebraically closed then we write $\overline{K}$ for its algebraic closure. This is the smallest field in which every nonconstant polynomial with coefficients in K has a root. For instance, $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}_q}$ are the algebraic closures of the two fields above. Another important example is the field of rational functions $\mathbb{Q}(t)$. Its algebraic closure $\overline{\mathbb{Q}(t)}$ is contained in the field of *Puiseux series*, denoted by $\mathbb{C}\{\{t\}\}$, which is also algebraically

closed. The elements of $\mathbb{C}\{\{t\}\}$ are formal expressions $\sum_{a=a_0}^{\infty} c_a t^{\frac{a}{m}}$, where m is a fixed positive integer, a_0 is an integer and $c_a \in \mathbb{C}$. The fields $\overline{\mathbb{Q}(t)}$ and $\mathbb{C}\{\{t\}\}$ may be unfamiliar to many of our readers. Their importance will be seen in Chapter 7, when we pass from classical algebra to tropical algebra.

In this section we study the ring of polynomials in n variables $x_1, \ldots, x_n$ with coefficients in our field K. This polynomial ring is denoted by $K[\mathbf{x}] = K[x_1, \ldots, x_n]$. If the number n is small, then we typically use letters without indices to denote the variables. For instance, we often write $K[x], K[x, y]$, or $K[x, y, z]$ for the polynomial ring when $n = 1, 2$, or 3.

Many of the constructions we present work not just for the polynomial ring $K[\mathbf{x}]$ but also for an arbitrary commutative ring R with unit 1. We allow $1 = 0$, i.e. R as a set may contain just one element 0. For the most part, the reader may assume $R = K[\mathbf{x}]$. But it would not hurt to peruse a standard textbook on *abstract algebra* and look up the axioms of a *ring* and the formal definitions of *commutative* and *unit*. Important examples of commutative rings are the integers $\mathbb{Z}$, the polynomial ring over the integers $\mathbb{Z}[\mathbf{x}]$, and the quotient of a polynomial ring by an ideal. The latter will be discussed soon.

The polynomial ring $K[\mathbf{x}]$ is an infinite-dimensional K-vector space. A distinguished basis of this vector space consists of the monomials $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$. There is one monomial for each nonnegative integer vector $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$. Every polynomial $f \in K[\mathbf{x}]$ is written uniquely as a finite K-linear combination of monomials:

$$f \;=\; \sum_{\mathbf{a}} c_{\mathbf{a}}\, \mathbf{x}^{\mathbf{a}}.$$

The *degree* of f is the maximum of the quantities $|\mathbf{a}| = a_1 + \cdots + a_n$ where $c_{\mathbf{a}} \neq 0$. For polynomials of degree $1, 2, 3, 4, 5$ and 6 we use the words *linear*, *quadratic*, *cubic*, *quartic*, *quintic* and *sextic*. These can be adjectives or nouns. It is also common to use the term *quadric* for a quadratic polynomial.

For example, the following is a cubic polynomial in $n = 3$ variables:

$$f \;=\; \det \begin{pmatrix} 1 & x & y \\ x & 1 & z \\ y & z & 1 \end{pmatrix} \;=\; 2xyz - x^2 - y^2 - z^2 + 1. \tag{1.1}$$

The zero set of f is a surface in $\mathbb{R}^3$. It consists of all points at which the rank of the 3×3 matrix in (1.1) decreases. It has four singular points, namely the points $(1, 1, 1)$, $(1, -1, -1)$, $(-1, 1, -1)$, and $(-1, -1, 1)$. These points are the common zeros in $\mathbb{R}^3$ of the cubic f and its three partial derivatives

$$\frac{\partial f}{\partial x} \;=\; 2yz - 2x\,, \quad \frac{\partial f}{\partial y} \;=\; 2xz - 2y\,, \quad \frac{\partial f}{\partial z} \;=\; 2xy - 2z.$$

These are the points at which the rank of the 3×3 matrix in (1.1) equals 1. The formal definition of singular points will appear at the end of Section 2.1.

Figure 1.1. A cubic surface with four singular points.

Figure 1.1 illustrates the cubic surface $\{f = 0\}$. However, the picture is drawn in a different coordinate system. Namely, we divide each of the three coordinates by $\frac{1}{3}(1 - x - y - z)$ and clear denominators to get $g = 8x^3 + 6x^2y + 6x^2z + \cdots - 3z + 1$. Figure 1.1 shows the part of the surface $\{g = 0\}$ that lies in the box $-1.5 < x, y, z < 1.5$. This change of coordinates amounts to applying a *projective transformation* to our surface. From the vantage point of projective geometry, to be adopted in Section 2.2, it is natural to regard two varieties as being the same if they differ by a projective transformation. We therefore assert, from now on, that Figure 1.1 shows the surface $\{f = 0\}$. This will serve as a running example throughout the book.

Definition 1.1. All rings in this book are commutative and have a unit 1. An *ideal* in such a ring R is a nonempty subset I of R such that

(a) if $f \in R$ and $g \in I$, then $fg \in I$;

(b) if $f, g \in I$, then $f + g \in I$.

If $R = K[\mathbf{x}]$ then an ideal I is a nonempty subset of $K[\mathbf{x}]$ that is closed under taking linear combinations with polynomial coefficients. An alternative definition is as follows: A subset I of a ring R is an ideal if and only if there exists a ring homomorphism $\phi : R \to S$ whose kernel $\ker \phi = \phi^{-1}(0)$ is equal to I. For instance, if $R = \mathbb{Z}$ then the set I of even integers is an ideal. It is the kernel of the ring homomorphism $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ that takes an integer to either 0 or 1, depending on its parity.

Ideals in a ring play the same role as normal subgroups in a group. They are the subobjects used to define quotients. Consider the quotient of abelian

groups R/I. Its elements are the congruence classes $f+I$ modulo I. The axioms (a) and (b) in Definition 1.1 ensure that the following identities hold:

$$(1.2) \quad (f+I)+(g+I) \,=\, (f+g)+I \quad \text{and} \quad (f+I)(g+I) \,=\, fg+I.$$

Proposition 1.2. *If $I \subset R$ is an ideal, then the quotient R/I is a ring.*

Given any subset $\mathcal{F}$ of a ring R, we write $\langle \mathcal{F} \rangle$ for the smallest ideal containing $\mathcal{F}$. This is the *ideal generated by* $\mathcal{F}$. If $R = K[\mathbf{x}]$ then the ideal $\langle \mathcal{F} \rangle$ is the set of all polynomial linear combinations of finite subsets of $\mathcal{F}$.

Proposition 1.3. *If I and J are ideals in a ring R, then the following subsets of R are ideals as well: the sum $I+J$, the intersection $I \cap J$, the product IJ, and the quotient $(I:J)$. The latter two subsets of R are defined as follows:*

$$IJ \,=\, \langle\, fg \,:\, f \in I, g \in J \,\rangle \quad \text{and} \quad (I:J) \,=\, \bigl\{ f \in R : fJ \subseteq I \bigr\}.$$

Proof. The product IJ is an ideal by definition. For the others one checks that conditions (a) and (b) hold. We shall carry this out for the ideal quotient $(I:J)$. To show (a), suppose that $f \in R$ and $g \in (I:J)$. We have

$$(fg)J = f(gJ) \,\subset\, fI \,\subset\, I.$$

For (b), suppose f and g are in $(I:J)$. We have

$$(f+g)J \,\subset\, fJ+gJ \,\subset\, I+I \,=\, I.$$

This implies $f+g \in (I:J)$. We have shown that $(I:J)$ is an ideal. □

The *Euclidean algorithm* works in the polynomial ring $K[x]$ in one variable x over a field K. This implies that $K[x]$ is a *principal ideal domain* (PID), i.e. every ideal I in $K[x]$ is generated by one element. That generator can be uniquely factored into irreducible polynomials.

Unique factorization of polynomials also holds when the number of variables satisfies $n \geq 2$. We say that the polynomial ring $K[\mathbf{x}]$ is a *unique factorization domain* (UFD). However, $K[\mathbf{x}]$ is not a PID when $n \geq 2$. For instance, for $n=2$, the ideal $\langle x_1, x_2 \rangle$ is not principal. But let's first go back to the univariate case in order to illustrate the operations in Proposition 1.3.

Example 1.4 ($n=1$)**.** Consider the following two ideals in $\mathbb{Q}[x]$:

$$I \,=\, \langle\, x^3+6x^2+12x+8 \,\rangle \quad \text{and} \quad J \,=\, \langle\, x^2+x-2 \,\rangle.$$

We compute the four ideals in Proposition 1.3. For this, it helps to factor:

$$I \,=\, \langle\, (x+2)^3 \,\rangle \qquad \text{and} \qquad J \,=\, \langle\, (x-1)(x+2) \,\rangle.$$

The four new ideals are

$$\begin{aligned} I \cap J &= \langle\, (x-1)(x+2)^3 \,\rangle, & IJ &= \langle\, (x-1)(x+2)^4 \,\rangle, \\ I+J &= \langle\, x+2 \,\rangle, & I:J &= \langle\, (x+2)^2 \,\rangle. \end{aligned}$$

We see that arithmetic in $\mathbb{Q}[x]$ is just like arithmetic in the ring of integers $\mathbb{Z}$.

A nonzero element f in a ring R is called

- a *nilpotent* if $f^m = 0$ for some positive integer m;
- a *zero divisor* if there exists $0 \neq g \in R$ such that $gf = 0$.

A ring R is called an *integral domain* if it has no zero divisors and $1 \neq 0$ in R. For instance, the set $\{0\}$ is a ring but not an integral domain.

We examine these properties for the quotient ring R/I where I is an ideal in R. Properties of the ideal I correspond to properties of the ring R/I. This correspondence is summarized in the following table:

Property	**Definition**	**The quotient ring R/I**
I is *maximal*	No other proper ideal contains I	is a *field*
I is *prime*	$fg \in I \Rightarrow f \in I$ or $g \in I$	is an *integral domain*
I is *radical*	$(\exists s : f^s \in I) \Rightarrow f \in I$	has no *nilpotent* elements
I is *primary*	$fg \in I$ and $g \notin I \Rightarrow (\exists s : f^s \in I)$	*zero divisors* are nilpotent

Maximal, prime and primary ideals are proper. In other words, the ring R itself is an ideal in R, but it is neither maximal, nor prime, nor primary.

Example 1.5. The ideal $I = \langle x^2 + 10x + 34, 3y - 2x - 13 \rangle$ is maximal in the polynomial ring $\mathbb{R}[x, y]$. The field $\mathbb{R}[x, y]/I$ is isomorphic to the field of complex numbers $\mathbb{C} = \mathbb{R}[i]/\langle i^2 + 1 \rangle$. One isomorphism is obtained by sending $i = \sqrt{-1}$ to $\frac{1}{13}(x + 5y)$. The square of that expression is -1 mod I. The principal ideal $J = \langle x^2 + 10x + 34 \rangle$ is prime, but it is not maximal. The quotient $\mathbb{R}[x, y]/J$ is an integral domain. It is isomorphic to $\mathbb{C}[y]$.

Examples for the other two classes of ideals are given in the next proof.

Proposition 1.6. *We have the following implications for an ideal I in R:*

$$I \text{ maximal} \Rightarrow I \text{ prime} \begin{array}{l} \Rightarrow I \text{ radical}, \\ \Rightarrow I \text{ primary}. \end{array}$$

None of these implications is reversible. However, every ideal that is both radical and primary is prime. Every intersection of prime ideals is radical.

Proof. The first implication holds because there are no zero divisors in a field. To see that prime implies radical, we take $g = f^{s-1}$ and use induction on s. That prime implies primary is clear. To prove that every radical primary ideal is prime, assume $fg \in I$ and $f \notin I$. Then, as I is primary, we have $g^s \in I$ for some $s \in \mathbb{N}$. As I is radical, we conclude that $g \in I$.

To see that no implication is reversible, we consider the following three ideals in the polynomial ring $\mathbb{R}[x, y]$ with $n = 2$ variables:

- $I = \langle x^2 \rangle$ is primary but not radical;
- $I = \langle x(x-1) \rangle$ is radical but not primary;
- $I = \langle x \rangle$ is prime but not maximal.

The last statement holds since intersections of radical ideals are radical. □

We now revisit the surface in Figure 1.1 from the perspective of ideals.

Example 1.7 ($n = 3$)**.** We consider the ideal generated by the partial derivatives of the cubic $f = 2xyz - x^2 - y^2 - z^2 + 1$. This is the ideal

$$I \;=\; \langle \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z} \rangle \;=\; \langle yz - x,\; xz - y,\; xy - z \rangle \;\subset\; \mathbb{R}[x, y, z].$$

The cubic f is not in this ideal because every polynomial in I has zero constant term. The ideal I is radical because we can write it as the intersection of five maximal ideals. Namely, using a computer algebra system, we find

$$\begin{aligned} I = \langle x,y,z \rangle \cap \langle x-1, y-1, z-1 \rangle \cap \langle x-1, y+1, z+1 \rangle \\ \cap \;\langle x+1, y-1, z+1 \rangle \cap \langle x+1, y+1, z-1 \rangle. \end{aligned} \tag{1.3}$$

This is a primary decomposition of I, as discussed in detail in Chapter 3.

The cubic f lies in the last four maximal ideals. Their intersection equals $I + \langle f \rangle$. The zero set of the radical ideal $I + \langle f \rangle$ consists of the four singular points on the surface seen in Figure 1.1. The *Chinese Remainder Theorem* for rings implies that the quotient ring is a product of fields. Namely, we have an isomorphism $\mathbb{R}[x, y, z]/I \;\simeq\; \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. It takes each polynomial modulo I to its residue classes modulo the intersectands in (1.3).

1.2. Gröbner Bases

Every ideal has many different generating sets. There is no canonical notion of a basis for an ideal. For instance, the set $\mathcal{F} = \{x^6 - 1, x^{10} - 1, x^{15} - 1\}$ minimally generates the ideal $\langle x - 1 \rangle$ in the polynomial ring $\mathbb{Q}[x]$ in one variable. Of course, the singleton $\{x - 1\}$ is a preferable generating set for that ideal. Recall that every ideal in $\mathbb{Q}[x]$ is *principal*, since we here have $n = 1$. The *Euclidean algorithm* transforms the set $\mathcal{F}$ into the set $\{x - 1\}$.

Here is a certificate for the fact that $x - 1$ is in the ideal generated by $\mathcal{F}$:

$$x^5 \cdot (x^6 - 1) \;-\; (x^5 + x) \cdot (x^{10} - 1) \;+\; 1 \cdot (x^{15} - 1) \;=\; x - 1.$$

Such identities can be found with the *extended Euclidean algorithm*. Please google this. Finding certificates for ideal membership when $n \geq 2$ is a harder problem. This topic comes up when we discuss Hilbert's Nullstellensatz in Chapter 6. In this section we introduce the basics of computing with ideals.

Gaussian elimination is familiar from linear algebra. It gives a process for manipulating ideals that are generated by linear polynomials. For example, the following two ideals are identical in the polynomial ring $\mathbb{Q}[x, y, z]$:

$$\langle\, 2x + 3y + 5z + 7,\ 11x + 13y + 17z + 19,\ 23x + 29y + 31z + 37 \,\rangle$$
$$= \langle\, 7x - 16,\ 7y + 12,\ 7z + 9 \,\rangle.$$

Undergraduate linear algebra taught us how to transform the three generators on the left into the simpler ones on the right. This is the process of solving a system of linear equations. In our example, the three linear equations have a unique solution, namely the point $\left(\frac{16}{7}, -\frac{12}{7}, -\frac{9}{7}\right)$ in $\mathbb{R}^3$.

We next introduce Gröbner bases. The framework of Gröbner bases offers practical methods for computing with ideals in a polynomial ring $K[\mathbf{x}]$ in n variables. Here K is a field whose arithmetic we can compute. Implementations of Gröbner bases are available in many computer algebra systems. We strongly encourage readers to experiment with these tools.

Informally, we can think of computing Gröbner bases as a version of the Euclidean algorithm for polynomials in $n \geq 2$ variables, or as a version of Gaussian elimination for polynomials of degree ≥ 2. Gröbner bases for ideals are fundamental to nonlinear algebra, just like Gaussian elimination for matrices is fundamental to linear algebra. The premise of this book is that *nonlinear algebra is the next step after linear algebra*.

We identify the set $\mathbb{N}^n$ of nonnegative integer vectors with the monomial basis of the polynomial ring $K[\mathbf{x}]$. The coordinatewise partial order on $\mathbb{N}^n$ corresponds to divisibility of monomials. To be precise, we have $\mathbf{a} \leq \mathbf{b}$ in the poset $\mathbb{N}^n$ if and only if the monomial $\mathbf{x}^{\mathbf{a}}$ divides the monomial $\mathbf{x}^{\mathbf{b}}$.

Theorem 1.8 (Dickson's Lemma)**.** *Any infinite subset of $\mathbb{N}^n$ contains a pair $\{\mathbf{a}, \mathbf{b}\}$ that satisfies $\mathbf{a} \leq \mathbf{b}$.*

Corollary 1.9. *For any nonempty set $\mathcal{M} \subset \mathbb{N}^n$, its subset of coordinatewise minimal elements is finite and nonempty.*

Proof. The fact that the subset is nonempty follows by induction on n. The subset is finite by Dickson's Lemma. □

Proof of Theorem 1.8. We proceed by induction on n. The statement is trivial for $n = 1$. Any subset of cardinality at least 2 in $\mathbb{N}$ contains a comparable pair. Suppose now that Dickson's Lemma has been proved for $n-1$, and consider an infinite subset $\mathcal{M}$ of $\mathbb{N}^n$. For each $i \in \mathbb{N}$ let $\mathcal{M}_i$ denote the set of all vectors $\mathbf{a} \in \mathbb{N}^{n-1}$ such that $(\mathbf{a}, i) \in \mathcal{M}$. If some $\mathcal{M}_i$ is infinite then we are done by the induction hypothesis. Hence we may assume that each $\mathcal{M}_i$ is a finite subset of $\mathbb{N}^{n-1}$ and that $\mathcal{M}_i \neq \emptyset$ for infinitely many i.

Consider the (possibly infinite) subset $\bigcup_{i=0}^{\infty} \mathcal{M}_i$ of $\mathbb{N}^{n-1}$. We claim that the subset of its minimal elements with respect to the coordinatewise order

is finite. This is clear when $\bigcup_{i=0}^{\infty} \mathcal{M}_i$ is finite. Otherwise, by the induction hypothesis we may apply Corollary 1.9 to this subset. Hence, there is always an index j such that all minimal elements are in the finite set $\bigcup_{i=0}^{j} \mathcal{M}_i$. Pick any $\mathbf{b} \in \mathcal{M}_k$ for $k > j$. Since the element $\mathbf{b}$ must be greater than or equal to some minimal element, there exists an index i with $i \leq j < k$ and an element $\mathbf{a} \in \mathcal{M}_i$ with $\mathbf{a} \leq \mathbf{b}$. We have $(\mathbf{a}, i) \leq (\mathbf{b}, k)$ in $\mathcal{M}$. □

Definition 1.10. Consider a total ordering $\prec$ of the set $\mathbb{N}^n$. We write $\mathbf{a} \preceq \mathbf{b}$ if $\mathbf{a} \prec \mathbf{b}$ or $\mathbf{a} = \mathbf{b}$. The ordering $\prec$ is a *monomial order* if for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$,

- $(0, 0, \ldots, 0) \preceq \mathbf{a}$;
- $\mathbf{a} \preceq \mathbf{b}$ implies $\mathbf{a} + \mathbf{c} \preceq \mathbf{b} + \mathbf{c}$.

This gives a total order on monomials in $K[\mathbf{x}]$. Three standard examples are

- *the lexicographic order*: $\mathbf{a} \prec_{\text{lex}} \mathbf{b}$ if the leftmost nonzero entry of $\mathbf{b} - \mathbf{a}$ is positive. This ordering is important for elimination.
- *the degree lexicographic order*: $\mathbf{a} \prec_{\text{deglex}} \mathbf{b}$ if either $|\mathbf{a}| < |\mathbf{b}|$, or $|\mathbf{a}| = |\mathbf{b}|$ and the leftmost nonzero entry of $\mathbf{b} - \mathbf{a}$ is positive.
- *the degree reverse lexicographic order*: $\mathbf{a} \prec_{\text{revlex}} \mathbf{b}$ if either $|\mathbf{a}| < |\mathbf{b}|$, or $|\mathbf{a}| = |\mathbf{b}|$ and the rightmost nonzero entry of $\mathbf{b} - \mathbf{a}$ is negative.

All three orders satisfy $x_1 \succ x_2 \succ \cdots \succ x_n$, but they differ on monomials of higher degree. We recommend that the reader list the 10 quadratic monomials for $n = 4$ in each of the three orderings above.

Throughout this book we specify a monomial order by giving the name of the order and how the variables are sorted. For instance, we might say: "let $\prec$ denote the degree lexicographic order on $K[x, y, z]$ given by $y \prec z \prec x$". Other choices of monomial orders are obtained by assigning positive weights to the variables; see [**10**, Exercise 11 in §2.4]. We also note that any monomial order is a refinement of the coordinatewise partial order on $\mathbb{N}^n$:

$$\text{if } \mathbf{x}^{\mathbf{a}} \text{ divides } \mathbf{x}^{\mathbf{b}}, \quad \text{then } \mathbf{a} \preceq \mathbf{b}.$$

Remark 1.11. Fix a monomial order $\prec$ and let $\mathcal{M}$ be any nonempty subset of $\mathbb{N}^n$. Then $\mathcal{M}$ has a unique minimal element with respect to $\prec$. To show this, we apply Dickson's Lemma as in Corollary 1.9. Our set $\mathcal{M}$ has a finite, nonempty subset of minimal elements in the componentwise order on $\mathbb{N}^n$. This finite subset is linearly ordered by $\prec$. We select its minimal element.

We now fix a monomial order $\prec$. Given any nonzero polynomial $f \in K[\mathbf{x}]$, its *initial monomial* $\text{in}_{\prec}(f)$ is the $\prec$-largest monomial $\mathbf{x}^{\mathbf{a}}$ among those that appear in f with nonzero coefficient. To illustrate this for the orders above, let $n = 3$ with variable order $x \succ y \succ z$: Fix the polynomial $f = x^2 + xz^2 + y^3$. Then $\text{in}_{\prec_{\text{lex}}}(f) = x^2$, $\text{in}_{\prec_{\text{deglex}}}(f) = xz^2$ and $\text{in}_{\prec_{\text{revlex}}}(f) = y^3$.

For any ideal $I \subset K[\mathbf{x}]$, we define the *initial ideal* of I with respect to a given monomial order $\prec$ as follows:

$$\mathrm{in}_\prec(I) \;=\; \langle\, \mathrm{in}_\prec(f) \,:\, f \in I \backslash \{0\} \,\rangle.$$

This is a *monomial ideal*, i.e. it is generated by a set of monomials. A priori, this generating set is infinite. However, it turns out that we can always choose a finite subset that suffices to generate this monomial ideal.

Proposition 1.12. *Fix a monomial order $\prec$. Every ideal I in the polynomial ring $K[\mathbf{x}]$ has a finite subset $\mathcal{G}$ such that*

$$\mathrm{in}_\prec(I) \;=\; \langle\, \mathrm{in}_\prec(f) \,:\, f \in \mathcal{G} \,\rangle.$$

Such a finite subset $\mathcal{G}$ of I is called a Gröbner basis *for I with respect to $\prec$.*

Proof. Suppose no such finite set $\mathcal{G}$ exists. Then we can create a list of infinitely many polynomials $f_1, f_2, f_3, \ldots$ in I such that none of the initial monomials $\mathrm{in}_\prec(f_i)$ divides any other initial monomial $\mathrm{in}_\prec(f_j)$. This would be a contradiction to Dickson's Lemma (Theorem 1.8). □

We next show that every Gröbner basis actually generates its ideal.

Theorem 1.13. *If $\mathcal{G}$ is a Gröbner basis for an ideal I in $K[\mathbf{x}]$, then $I = \langle \mathcal{G} \rangle$.*

Proof. Suppose that $\mathcal{G}$ does not generate I. Among all polynomials f in the set $I \backslash \langle \mathcal{G} \rangle$, there exists an f whose initial monomial $\mathbf{x}^{\mathbf{b}} = \mathrm{in}_\prec(f)$ is minimal with respect to $\prec$. This follows from Remark 1.11. Since $\mathbf{x}^{\mathbf{b}} \in \mathrm{in}_\prec(I)$, there exists $g \in \mathcal{G}$ whose initial monomial divides $\mathbf{x}^{\mathbf{b}}$, say $\mathbf{x}^{\mathbf{b}} = \mathbf{x}^{\mathbf{c}} \cdot \mathrm{in}_\prec(g)$. Now, $f - \mathbf{x}^{\mathbf{c}} g$ is a polynomial with strictly smaller initial monomial. It lies in I but does not lie in the ideal $\langle \mathcal{G} \rangle$. This contradicts our choice of f. □

Corollary 1.14 (Hilbert's Basis Theorem)**.** *Every ideal I in the polynomial ring $K[\mathbf{x}]$ is finitely generated.*

Proof. Fix any monomial order $\prec$. By Proposition 1.12, the ideal I has a finite Gröbner basis $\mathcal{G}$. By Theorem 1.13, the finite set $\mathcal{G}$ generates I. □

Gröbner bases are not unique. If $\mathcal{G}$ is a Gröbner basis of an ideal I with respect to a monomial order $\prec$, then so is every other finite subset of I that contains $\mathcal{G}$. In that sense, Gröbner bases differ from the bases we know from linear algebra. The issue of minimality and uniqueness is addressed next.

Definition 1.15. Fix I and $\prec$. A Gröbner basis $\mathcal{G}$ is *reduced* if the following two conditions hold:

(a) The leading coefficient of each polynomial $g \in \mathcal{G}$ is 1.

(b) For distinct $g, h \in \mathcal{G}$, no monomial in g is a multiple of $\mathrm{in}_\prec(h)$.

In what follows we fix an ideal $I \subset K[\mathbf{x}]$ and a monomial order $\prec$.

Theorem 1.16. *The ideal I has a unique reduced Gröbner basis for $\prec$.*

Proof idea. We refer to [**10**, §2.7, Theorem 5]. The idea is as follows. We start with any Gröbner basis $\mathcal{G}$ and turn it into a reduced Gröbner basis by applying the following steps. First we divide each $g \in \mathcal{G}$ by its leading coefficient to make it monic, so that (a) holds. We then remove from $\mathcal{G}$ all elements g whose initial monomial is not a minimal generator of $\mathrm{in}_\prec(I)$. For any pair of polynomials with the same initial monomial, we delete one of them. Next we apply the division algorithm [**10**, §2.3] to any nonleading monomial until there are no more nonleading monomials divisible by any leading monomial. The resulting set is the reduced Gröbner basis. □

Let $\mathcal{S}_\prec(I)$ be the set of all monomials $\mathbf{x^b}$ that are not in the initial ideal $\mathrm{in}_\prec(I)$. We call these $\mathbf{x^b}$ the *standard monomials* of I with respect to $\prec$.

Theorem 1.17. *The set $\mathcal{S}_\prec(I)$ of standard monomials is a basis for the K-vector space $K[\mathbf{x}]/I$.*

Proof. The image of $\mathcal{S}_\prec(I)$ in $K[\mathbf{x}]/I$ is linearly independent because every nonzero polynomial f whose image is zero in $K[\mathbf{x}]/I$ lies in the ideal I. Any such f has at least one monomial, namely $\mathrm{in}_\prec(f)$, that is not in $\mathcal{S}_\prec(I)$.

We next prove that $\mathcal{S}_\prec(I)$ spans $K[\mathbf{x}]/I$. Suppose not. Then there exists a monomial $\mathbf{x^c}$ which is not in the K-span of $\mathcal{S}_\prec(I)$ modulo I. We may assume that $\mathbf{x^c}$ is minimal with respect to the monomial order $\prec$. Since $\mathbf{x^c}$ is not in $\mathcal{S}_\prec(I)$, it lies in the initial ideal $\mathrm{in}_\prec(I)$. Hence there exists $h \in I$ with $\mathrm{in}_\prec(h) = \mathbf{x^c}$. Each monomial in h other than $\mathbf{x^c}$ is smaller with respect to $\prec$, so it lies in the K-span of $\mathcal{S}_\prec(I)$ modulo I. Hence $\mathbf{x^c}$ lies in the K-span of $\mathcal{S}_\prec(I)$ modulo I. This is a contradiction. □

The most well-known tool for computing Gröbner bases is *Buchberger's algorithm* [**10**, §2.7]. Variants of this algorithm are implemented in all major computer algebra systems. The algorithm takes as its input a monomial order $\prec$ and a finite set $\mathcal{F}$ of polynomials in $K[\mathbf{x}]$. The output is the unique reduced Gröbner basis $\mathcal{G}$ for the ideal $I = \langle \mathcal{F} \rangle$ with respect to $\prec$. Experimenting with such an implementation is strongly recommended.

In what follows we present some examples of input-output pairs $(\mathcal{F}, \mathcal{G})$ for $n = 3$. Here we take the lexicographic monomial order with $x \succ y \succ z$.

Example 1.18. A computer algebra system, such as `Maple`, `Mathematica`, `Magma`, `Macaulay2`, or `Singular`, transforms the input $\mathcal{F} \subset \mathbb{Q}[x, y, z]$ into

its reduced Gröbner basis $\mathcal{G}$. The initial monomials are always underlined:

- For $n = 1$, computing the reduced Gröbner basis means computing the greatest common divisor of the input polynomials: $\mathcal{F} = \{x^3-6x^2-5x-14, 3x^3+8x^2+11x+10, 4x^4+4x^3+7x^2-x-2\}$, $\mathcal{G} = \{\underline{x^2} + x + 2\}$.
- For linear polynomials, running Buchberger's algorithm amounts to Gaussian elimination. For $\mathcal{F} = \{2x + 3y + 5z + 7,\ 11x + 13y + 17z+19,\ 23x+29y+31z+37\}$, the reduced Gröbner basis is found to be $\mathcal{G} = \{\underline{x} - \frac{16}{7},\ \underline{y} + \frac{12}{7},\ \underline{z} + \frac{9}{7}\}$.
- The input $\mathcal{F} = \{xy - z, xz - y, yz - x\}$ yields the output $\mathcal{G} = \{\underline{x} - yz, \underline{y^2} - z^2, \underline{yz^2} - y, \underline{z^3} - z\}$. There are precisely five standard monomials: $\mathcal{S}_\prec(I) = \{1, y, z, yz, z^2\}$. The number five also occurred in Example 1.7, where we saw that $\mathcal{F}$ has five zeros in $\mathbb{C}^3$.
- Let the input be the curve in the (y, z)-plane parametrized by the two cubics $(x^3 - 4x,\ x^3 + x - 1)$ in one variable x. We write this as $\mathcal{F} = \{y - x^3 + 4x, z - x^3 - x + 1\}$. The Gröbner basis has the implicit equation of this curve as its second element: $\mathcal{G} = \{\,\underline{x} + \frac{1}{5}y + \frac{1}{5}z - \frac{1}{5},\ \underline{y^3} - 3y^2z - 3y^2 + 3yz^2 + 6yz + 28y - z^3 - 3z^2 + 97z + 99\,\}$.
- Let z be the sum of $x = \sqrt[3]{7}$ and $y = \sqrt[4]{5}$. We encode this in the set $\mathcal{F} = \{x^3 - 7, y^4 - 5, z - x - y\}$. The real number $z = \sqrt[3]{7} + \sqrt[4]{5}$ is algebraic of degree 12 over $\mathbb{Q}$. Its minimal polynomial is the first element in the Gröbner basis $\mathcal{G} = \{\underline{z^{12}} - 28z^9 - 15z^8 + 294z^6 - 1680z^5 + 75z^4 - 1372z^3 - 7350z^2 - 2100z + 2276, \ldots\}$.
- The elementary symmetric polynomials $\mathcal{F} = \{x + y + z, xy + xz + yz, xyz\}$ have the reduced Gröbner basis $\mathcal{G} = \{\,\underline{x} + y + z,\ \underline{y^2} + yz + z^2,\ \underline{z^3}\,\}$. There are six standard monomials. The quotient $\mathbb{Q}[x, y, z]/I$ is the regular representation of the symmetric group S_3.

For each of the six ideals above, what is the reduced Gröbner basis for the degree lexicographic order? What are the possible initial monomial ideals?

Many such examples boil down to the fact that lexicographic Gröbner bases are useful for eliminating variables. We shall see this in Theorem 4.5.

In general, the choice of monomial order can make a huge difference in the complexity of the reduced Gröbner basis, even for two input polynomials.

Example 1.19 (Intersecting two quartic surfaces in projective 3-space $\mathbb{P}^3$)**.** A random homogeneous polynomial of degree 4 in $n = 4$ variables has 35 monomials. Consider the ideal I generated by two such random polynomials. If $\prec$ is the degree reverse lexicographic order, then the reduced Gröbner basis

$\mathcal{G}$ consists of 5 elements of degree up to 7. If $\prec$ is the lexicographic order, then $\mathcal{G}$ consists of 150 elements of degree up to 73.

Naturally, one uses a computer to find the 150 polynomials above. Many computer algebra systems offer an implementation of Buchberger's algorithm for Gröbner bases. We reiterate that readers are strongly encouraged to experiment with a computer algebra system while studying this book.

For an introduction to Buchberger's algorithm and many further details regarding Gröbner bases, we refer to the textbooks by Cox-Little-O'Shea [**10**], Greuel-Pfister [**23**] and Kreuzer-Robbiano [**30**]. In later chapters we shall freely use concepts from this area, such as S-polynomials and Buchberger's criterion. After all, our book is nothing but an "invitation".

1.3. Dimension and Degree

The two most important invariants of an ideal I in a polynomial ring $K[\mathbf{x}]$ are its dimension and its degree. We shall define these invariants, starting with the case of monomial ideals. In this section we focus on combinatorial aspects. The geometric interpretation will be presented in Chapter 2.

Definition 1.20 (Hilbert function)**.** Let $I \subset K[\mathbf{x}]$ be a monomial ideal. The *Hilbert function* h_I takes nonnegative integers to nonnegative integers. The value $h_I(q)$ is the number of monomials of degree q *not* belonging to I.

A convenient way to represent a function $\mathbb{N} \to \mathbb{N}$ is by its generating function. This is a formal power series with nonnegative integer coefficients. The generating function for the Hilbert function is called the *Hilbert series*.

Definition 1.21 (Hilbert series)**.** Let $I \subset K[\mathbf{x}]$ be a monomial ideal. We fix a formal variable z. The Hilbert series of I is the generating function

$$\mathrm{HS}_I(z) \quad = \quad \sum_{q=0}^{\infty} h_I(q) z^q.$$

We begin with the zero ideal $I = \{0\}$. We count all monomials in $K[\mathbf{x}]$.

Example 1.22. The Hilbert series of the zero ideal is the rational function

$$\mathrm{HS}_{\{0\}}(z) \;=\; \frac{1}{(1-z)^n} \;=\; \sum_{q=0}^{\infty} \binom{n+q-1}{n-1} z^q.$$

The number of monomials of degree q in n variables is $h_I(q) = \binom{n+q-1}{n-1}$. Note that the Hilbert function $h_{\{0\}}(q)$ is a polynomial of degree $n-1$ in q.

We next consider the case of a principal ideal.

Example 1.23. Let $I = \langle x_1^{a_1} \cdots x_n^{a_n} \rangle$, where $\sum_{i=1}^n a_i = e$. We must count monomials of degree q that are not divisible by the generator of I. To do this, we count all monomials and then subtract those that are in I. This yields

$$\mathrm{HS}_I(z) \;=\; \frac{1-z^e}{(1-z)^n} \;=\; \sum_{q=0}^{\infty} \left[\binom{n+q-1}{n-1} - \binom{n+q-e-1}{n-1} \right] z^q.$$

The second binomial coefficient is zero when $q < e$. For all $q \geq e$, the Hilbert function $h_I(q) = \binom{n+q-1}{n-1} - \binom{n+q-e-1}{n-1}$ is a polynomial in q of degree $n-2$. The highest-order term of this polynomial is found to be $\frac{e}{(n-2)!} q^{n-2}$.

Our third example concerns ideals generated by two monomials:

Example 1.24. Fix an ideal $I = \langle m_1, m_2 \rangle$ in $K[\mathbf{x}]$, where m_i is a monomial of degree e_i for $i = 1, 2$. We count the monomials in I of degree q by

(1) computing the number of monomials divisible by m_1,

(2) adding the number of monomials divisible by m_2, and

(3) subtracting the number of monomials divisible by both m_1 and m_2.

Step (3) concerns monomials that are divisible by the least common multiple $m_{12} = \mathrm{lcm}(m_1, m_2)$. Let e_{12} denote the degree of m_{12}. The Hilbert series is

$$\mathrm{HS}_I(z) \;=\; \frac{1 - z^{e_1} - z^{e_2} + z^{e_{12}}}{(1-z)^n}.$$

Therefore, the Hilbert function is an alternating sum of binomial coefficients:

$$h_I(q) \;=\; \tbinom{n+q-1}{n-1} - \tbinom{n+q-e_1-1}{n-1} - \tbinom{n+q-e_2-1}{n-1} + \tbinom{n+q-e_{12}-1}{n-1}.$$

This expression agrees with a polynomial in q, provided $q \geq e_{12}$.

Theorem 1.25. *The Hilbert series of a monomial ideal $I \subset K[\mathbf{x}]$ is*

$$\mathrm{HS}_I(z) \;=\; \frac{\kappa_I(z)}{(1-z)^n}, \tag{1.4}$$

where $\kappa_I(z)$ is a polynomial with integer coefficients and $\kappa_I(0) = 1$. There exists a polynomial HP *in one unknown q of degree $\leq n-1$, known as the* Hilbert polynomial *of the ideal I, such that $\mathrm{HP}(q) = h_I(q)$ for all values of the integer q that are sufficiently large.*

Proof. We prove this result by counting monomials. This is done using the inclusion-exclusion principle, as hinted at in the three examples above. Let $m_1, m_2, \ldots, m_r$ be the monomials that minimally generate I. For any subset τ of the index set $\{1, 2, \ldots, r\}$, we write m_τ for the least common multiple of the set $\{m_i : i \in \tau\}$, and we set $e_\tau = \mathrm{degree}(m_\tau)$. This includes

the empty set $\tau = \emptyset$, for which $m_\emptyset = 1$ and $e_\emptyset = 0$. The desired numerator polynomial (1.4) can be written as alternating sums of 2^r powers of z:

$$\kappa_I(z) \quad = \sum_{\tau \subseteq \{1,2,\ldots,r\}} (-1)^{|\tau|} \cdot z^{e_\tau}.$$

The cases $r = 0, 1, 2$ were seen above. The general case is inclusion-exclusion. Note that $\kappa_I \in \mathbb{Z}[z]$ with $\kappa_I(0) = 1$. By regrouping the terms of (1.4),

$$h_I(q) \quad = \sum_{\tau \subseteq \{1,2,\ldots,r\}} (-1)^{|\tau|} \binom{n+q-e_\tau-1}{n-1}. \tag{1.5}$$

This is a polynomial for $q \gg 0$. More precisely, the Hilbert function $h_I(q)$ equals the Hilbert polynomial $\mathrm{HP}_I(q)$ for all q that exceed $e_{\{1,2,\ldots,r\}}$. This bound is the degree of the least common multiple of all generators of I. □

Remark 1.26. The inclusion-exclusion principle carried out in the proof of Theorem 1.25 is a powerful idea, but it also hints at possible simplifications. We wrote the numerator polynomial $\kappa_I(z)$ and the Hilbert polynomial $\mathrm{HP}_I(q)$ as alternating sums of 2^r terms. However, in most applications r is much larger than n, and the vast majority of terms will cancel each other. Doing the correct bookkeeping leads us to the topic of *minimal free resolutions* of monomial ideals. This is a main theme in a subject area known as *combinatorial commutative algebra*. Yes, please google this.

Example 1.27. Let $n = 2$ and consider the monomial ideal

$$I \;=\; \langle x \rangle \cap \langle y \rangle \cap \langle x, y \rangle^{r+1} \quad = \quad \langle x^r y, x^{r-1} y^2, x^{r-2} y^3, \ldots, x^2 y^{r-1}, x y^r \rangle.$$

Our formula for κ_I involves 2^r terms. After cancellations, only $2r$ remain:

$$\kappa_I(z) \;=\; 1 \;-\; r z^{r+1} \;+\; (r-1) z^{r+2}.$$

The Hilbert polynomial is the constant $\mathrm{HP}(q) \equiv 2$. This is also the value of the Hilbert function $h_I(q)$ for $q > r$. Note that $h_I(q) = q + 1$ for $q \leq r$.

Definition 1.28 (Dimension and degree)**.** Let I be a monomial ideal and write

$$\mathrm{HP}_I(q) \;=\; \frac{g}{(d-1)!} q^{d-1} \;+\; \text{lower-order terms in } q.$$

If the Hilbert polynomial HP is nonzero, the *dimension* of I is d and the *degree* of I is g. Here g is a positive integer. If $\mathrm{HP}_I(q) \equiv 0$ then we say that I is 0-dimensional. In this case, $K[\mathbf{x}]/I$ is a finite-dimensional K-vector space. We define the degree of I to be the dimension of that vector space.

Remark 1.29. The fact that g is a positive integer is a result in combinatorics. The proof is omitted here, but we revisit this theme in Chapter 13. From the inclusion-exclusion formulas above, one can show that the numerator of the Hilbert series factors as $\kappa_I(z) = \lambda_I(z) \cdot (1-z)^{n-d}$, where $\lambda_I(z)$ is also a polynomial with integer coefficients. The degree of I equals $g = \lambda_I(1)$.

Remark 1.30. It may seem artificial to define dimension and degree by distinguishing between the cases where the Hilbert polynomial is zero or not. However, if the zero polynomial has degree -1, then the two definitions are compatible. Furthermore, given any ideal I in $K[\mathbf{x}]$, the degree of $\tilde{I}$ in $K[\mathbf{x}, z]$, with one extra variable z but the same generators as I, remains the same. Hence, we could equivalently define the degree of I by adding z and extracting the leading coefficient of $\mathrm{HP}_{\tilde{I}}(q)$. This operation increases the dimension by 1.

Example 1.31. Let I be a principal ideal as in Example 1.23, generated by a monomial of degree $e > 0$. Then the dimension of I is $n-1$ and the degree of I is e. This follows from the formula we gave for the Hilbert function, which reveals that the Hilbert polynomial satisfies $\mathrm{HP}(I) = \frac{e}{(n-2)!}q^{n-2} + O(q^{n-3})$.

Example 1.32. Let $n = 2m$ be even and consider the monomial ideal

$$I \;=\; \langle\, x_1x_2,\, x_3x_4,\, x_5x_6,\, \ldots\,,\, x_{2m-3}x_{2m-2},\, x_{2m-1}x_{2m} \,\rangle.$$

The dimension of I equals m and the degree of I equals 2^m. It is instructive to work out the Hilbert series and the Hilbert polynomial of I for $m = 3, 4$.

We now consider an arbitrary ideal I in $K[\mathbf{x}]$. We no longer assume that I is generated by monomials. Let $\prec$ be any *degree-compatible* monomial order. This means that $|\mathbf{a}| < |\mathbf{b}|$ implies $\mathbf{a} \prec \mathbf{b}$ for all $\mathbf{a}$ and $\mathbf{b}$.

Lemma 1.33. *The number of standard monomials of I of degree q is independent of the choice of monomial order $\prec$, provided $\prec$ is degree-compatible.*

Proof. Let $K[\mathbf{x}]_{\leq q}$ denote the vector space of polynomials of degree $\leq q$. We write $I_{\leq q} := I \cap K[\mathbf{x}]_{\leq q}$ for the subspace of polynomials that lie in the ideal I. Also, consider the set of standard monomials of degree at most q:

$$\mathcal{S}_\prec(I)_{\leq q} \;=\; \mathcal{S}_\prec(I) \,\cap\, K[\mathbf{x}]_{\leq q}.$$

We claim that $\mathcal{S}_\prec(I)_{\leq q}$ is a K-vector space basis for the quotient space $K[\mathbf{x}]_{\leq q}/I_{\leq q}$. This set is linearly independent since no K-linear combination of $\mathcal{S}_\prec(I)$ lies in I. But, given that $\prec$ is degree-compatible, it also spans. This is because taking the normal form of a polynomial modulo the Gröbner basis can never increase the total degree. □

Definition 1.34. Let I be an arbitrary ideal in a polynomial ring $K[\mathbf{x}]$. The function from $\mathbb{N}$ to $\mathbb{N}$ that associates to q the dimension of the quotient space $\dim K[\mathbf{x}]_{\leq q}/I_{\leq q}$ is known as the *affine Hilbert function*. We also define the *Hilbert function* h_I of I to be the Hilbert function of the initial ideal $\mathrm{in}_\prec(I)$, where $\prec$ is any degree-compatible term order. For all $q \in \mathbb{N}$ we have

$$\begin{aligned} h_I(q) \;=\; h_{\mathrm{in}_\prec(I)}(q) \;&=\; |\mathcal{S}_\prec(I)_{\leq q}| \;-\; |\mathcal{S}_\prec(I)_{\leq q-1}| \\ &=\; \dim(K[\mathbf{x}]_{\leq q}/I_{\leq q}) - \dim(K[\mathbf{x}]_{\leq q-1}/I_{\leq q-1}). \end{aligned}$$

This is the number of standard monomials whose degree equals q. This number is independent of $\prec$, thanks to Lemma 1.33. Thus the affine Hilbert function $q \mapsto \sum_{j=0}^{q} h_I(j)$ is determined by the Hilbert function and vice versa.

We also define the *Hilbert series* and the *Hilbert polynomial* to be the series and polynomial of any degree-compatible initial monomial ideal. Namely, we set

$$\text{HS}_I(z) \,:=\, \text{HS}_{\text{in}_\prec(I)}(z) \quad \text{and} \quad \text{HP}_I(q) \,:=\, \text{HP}_{\text{in}_\prec(I)}(q). \tag{1.6}$$

We similarly define the *affine Hilbert series* and the *affine Hilbert polynomial* of I. These can also be defined by the formulas in (1.6), assuming we take $\text{in}_\prec(I)$ in a polynomial ring $K[\mathbf{x}, y]$ that has one more dummy variable y.

We define the *dimension* and *degree* of I as the dimension and degree of $\text{in}_\prec(I)$. These concepts are now well-defined, thanks to Lemma 1.33.

Example 1.35. Let I be a principal ideal generated by a polynomial f of degree e in $n \geq 1$ variables. The Hilbert series of I is $\text{HS}_I(q) = \frac{1-q^e}{(1-q)^n}$. The affine Hilbert series equals $\frac{1-q^e}{(1-q)^{n+1}}$. The dimension of I is $n-1$. The degree of I is e. This follows from Example 1.31 because the singleton $\{f\}$ is a Gröbner basis and its initial monomial $\text{in}_\prec(f)$ has degree e in any degree-compatible monomial order $\prec$.

Remark 1.36. The prefix "affine" for the Hilbert function is important in order to distinguish affine varieties from projective varieties. We will discuss these geometric concepts in Chapter 2. Later on in the book, and elsewhere in algebraic geometry, it will usually be clear from the context whether the affine version or the projective version is meant. However, in this chapter we want to be precise and make that distinction.

What we have accomplished in this section is to give a purely combinatorial definition of the dimension and degree of an ideal I. In Chapter 2 we shall see that this notion of dimension agrees with the intuitive one for the associated algebraic variety $\mathcal{V}(I)$. Namely, a variety has dimension 0 if and only if it consists of finitely many points. The number of these points is counted by the degree of the corresponding radical ideal. Likewise, the ideal of a curve has dimension 1, the ideal of a surface has dimension 2, etc. The degree is a measure of how curvy these shapes are. One can show that a prime ideal has degree 1 if and only if it is generated by linear polynomials.

Example 1.37. Fix the polynomial ring $K[x, y, z]$ and let $f = xyz - x^2 - y^2 - z^2 + 1$ as in (1.1). The ideal $\langle f \rangle$ has dimension 2 and degree 3. Let I be the ideal generated by its partial derivatives, as in Example 1.7. Then I has dimension 0 and degree 5. The ideal $I + \langle f \rangle$, whose zeros are the four singular points of the surface in Figure 1.1, has dimension 0 and degree 4.

Exercises

(1) Prove that an ideal in a polynomial ring $K[\mathbf{x}]$ is principal if and only if its reduced Gröbner basis is a singleton.

(2) Draw the plane curve $\{f = 0\}$ that is defined by polynomial $f = 5x^3 - 25x^2y + 25y^3 + 15xy - 50y^2 - 5x + 25y - 1$. What do you observe?

(3) For $n = 2$, define a monomial order $\prec$ such that $(2,3) \prec (4,2) \prec (1,4)$.

(4) Let $n = 2$ and fix the monomial ideals $I = \langle x, y^2 \rangle$ and $J = \langle x^2, y \rangle$. Compute the ideals $I + J$, $I \cap J$, IJ and $I^3J^4 = IIIJJJJ$. How many minimal generators does the ideal $I^{123}J^{234}$ have?

(5) The *radical* $\mathrm{rad}(I)$ of an ideal I in a ring R is the smallest radical ideal containing I. Prove that the radical of a primary ideal is prime.

(6) For ideals in a polynomial ring $K[\mathbf{x}]$, prove that
- the radical of a principal ideal is principal;
- the radical of a monomial ideal is a monomial ideal.

(7) Show that the following inclusions always hold and are strict in general:

$$\mathrm{rad}(I)\,\mathrm{rad}(J) \;\subseteq\; \mathrm{rad}(IJ) \quad \text{and} \quad \mathrm{in}_\prec(\mathrm{rad}(I)\,) \;\subseteq\; \mathrm{rad}(\mathrm{in}_\prec(I)).$$

(8) Using Gröbner bases, find the minimal polynomials of $\sqrt[5]{6} + \sqrt[7]{8}$ and $\sqrt[5]{6} - \sqrt[7]{8}$. This is analogous to the fifth item in Example 1.18.

(9) Find the implicit equation of the curve $\{(x^5 - 6, x^7 - 8) \in \mathbb{R}^2 \,:\, x \in \mathbb{R}\}$.

(10) Study the ideal $I = \langle x^3 - yz, y^3 - xz, z^3 - xy \rangle$. Is it radical? If not, find $\mathrm{rad}(I)$. Regarding I as a system of three equations, what are its solutions in $\mathbb{R}^3$?

(11) For the ideals I and $\mathrm{rad}(I)$ in the previous exercise, determine the Hilbert function, Hilbert series, Hilbert polynomial, dimension, and degree. Find these same objects and quantities preceded by the adjective "affine" where possible.

(12) Find an ideal in $\mathbb{Q}[x, y]$ whose reduced Gröbner basis (in lexicographic order) has cardinality 5 and there are precisely 19 standard monomials.

(13) Let I be the ideal generated by the n elementary symmetric polynomials in $x_1, \ldots, x_n$. Pick a monomial order and find the initial ideal $\mathrm{in}_\prec(I)$.

(14) Let X be a 2×2 matrix whose entries are variables. Let I_s be the ideal generated by the entries of the matrix power X^s for $s = 2, 3, 4, \ldots$. Investigate these ideals. What are the dimension and the degree of I_s?

(15) A symmetric 3×3 matrix has seven principal minors: three of size 1×1, three of size 2×2, and one of size 3×3. Does there exist an algebraic relation between these minors? Hint: Use the lexicographic Gröbner basis.

(16) Prove that if $\text{in}_\prec(I)$ is radical then I is radical. Does the converse hold?

(17) Determine all straight lines that lie on the cubic surface in Figure 1.1.

(18) Identify maximal, prime, radical and primary ideals in the ring $R = \mathbb{Z}$.

(19) Let I be the ideal generated by all 2×2 minors of a $2 \times n$ matrix filled with $2n$ variables. What are the degree and dimension of I for $n = 2, 3, 4$?

(20) Find a prime ideal I of degree 3 and dimension 1 in n variables for $n = 2$ and $n = 3$. In the latter case, we require further that $h_I(1) = 3$.

(21) Compute the dimension and degree of the ideal generated by two random homogeneous polynomials of degree 4 in $n = 4$ variables, as in Example 1.19. Next drop the hypothesis "homogeneous" and redo.