Polynomials, Ideals, and Gröbner Bases

Notes by Bernd Sturmfels
for the lecture on April 10, 2018, in the
IMPRS Ringvorlesung *Introduction to Nonlinear Algebra*

We fix a field K. Some examples of fields are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the finite field $\mathbb{F}_q$ with q elements, or the field $\mathbb{Q}_p$ of p-adic numbers. Some of our fields are not algebraically closed, and we may consider their algebraic closures. Those fields are denoted $\overline{\mathbb{Q}}$, $\overline{\mathbb{F}_q}$, $\overline{\mathbb{Q}_p}$. Other fields occurring in this course are the rational functions $\mathbb{Q}(t)$, along with its algebraic closure, and Puiseux series $\mathbb{C}\{\{t\}\} = \overline{\mathbb{C}\{\{t\}\}}$.

The set of all polynomials in n variables $x_1, x_2, \ldots, x_n$ with coefficients in our field K is denoted $K[\mathbf{x}] = K[x_1, x_2, \ldots, x_n]$. This is a commutative ring. 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 $n \leq 3$.

The polynomial ring $K[\mathbf{x}]$ is an infinite-dimensional K-vector space. A distinguished basis is given by the monomials $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, one for each nonnegative integer vector $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$. Thus every polynomial $f \in K[\mathbf{x}]$ is written uniquely as a finite sum

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

The *degree* of the polynomial f is the maximum of the quantities $|\mathbf{a}| = a_1 + a_2 + \cdots + a_n$, where $c_{\mathbf{a}} \neq 0$. Polynomials of degree $1, 2, 3, 4$ are called *linear*, *quadratic*, *cubic*, *quartic*.

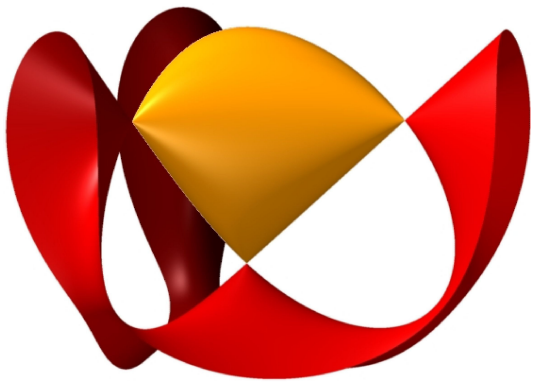

Figure 1: A cubic surface with four singular points.

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

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

The zero set of the polynomial f is the surface in $\mathbb{R}^3$ that is shown in Figure 1. This *determinantal surface* consists of all points at which the rank of the 3×3-matrix in (1) drops.

We note that our cubic surface has four singular points, namely the points $(1, 1, 1)$, $(1, -1, -1)$, $(-1, 1, -1)$, and $(-1, -1, 1)$. These four points are the common zeros in $\mathbb{R}^3$ of the cubic f and its three partial derivatives of f:

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

Equivalently, they are the points at which the rank of the 3×3-matrix in (1) drops to 1.

Definition 1. An *ideal* is a subset I of the polynomial ring $K[\mathbf{x}]$ such that

(a) if $f \in K[\mathbf{x}]$ and $g \in I$ then $fg \in I$;

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

Equivalently, I is closed under taking linear combination with polynomial coefficients. Given any subset $\mathcal{F}$ of $K[\mathbf{x}]$, we write $\langle \mathcal{F} \rangle$ for the smallest ideal containing $\mathcal{F}$. This is the *ideal generated by* $\mathcal{F}$. It is the set of a polynomial linear combinations of finite subsets of $\mathcal{F}$.

Proposition 2. *If I and J are ideals in $K[\mathbf{x}]$ then the following subsets are ideals as well: the sum $I + J$, the intersection $I \cap J$, the product IJ and the quotient $(I : J)$. The latter two are defined as follows: $IJ = \langle\, fg \,:\, f \in I, g \in J \,\rangle$ and $(I : J) = \big\{ f \in K[\mathbf{x}] : fJ \subseteq I \big\}$.*

Proof. The product IJ is an ideal by definition. For the others one checks (a) and (b).

We shall carry out this check 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 $f, g \in (I : J)$. We have:

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

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

The *Euclidean algorithm* works in the polynomial ring $K[x]$ in one variable. This implies that $K[x]$ is a *principal ideal domain* (PID), i.e. every ideal I is generated by one element. That generator can be uniquely factored into irreducible polynomials. Every polynomial ring $K[\mathbf{x}]$ is a *unique factorization domain* (UFD). However, $K[\mathbf{x}]$ is not a PID when $n \geq 2$.

Example 3 ($n = 1$)**.** 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 wish to compute the four new ideals in Proposition 2. For this, it helps to factor:

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

We then find

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

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

Ideals in a commutative ring play the same role as normal subgroups in a group. These are the subobjects that can be used to define quotients. Consider the quotient of K-vector spaces $K[\mathbf{x}]/I$. Its elements are the congruence classes $f + I$ modulo the subvectorspace I. The ideal axioms (a) and (b) in Definition 1 ensure that the following identities hold:

$$(f + I) + (g + I) \,=\, (f + g) + I \quad \text{and} \quad (f + I)(g + I) \,=\, fg + I. \tag{2}$$

Corollary 4. *If $I \subset K[\mathbf{x}]$ is an ideal then $K[\mathbf{x}]/I$ is a ring. We call this the* quotient ring.

Properties of the ideal I correspond to properties of the quotient ring $K[\mathbf{x}]/I$, as follows:

property of the ideal	**definition**	**property of the quotient ring**
I is *maximal*	$f \notin I \,\Rightarrow\, f$ invertible mod I	$K[x]/I$ is a *field*
I is *prime*	$fg \in I \,\Rightarrow\, f \in I$ or $g \in I$	$K[\mathbf{x}]/I$ is an *integral domain*
I is *radical*	$(\exists s : f^s \in I) \,\Rightarrow\, f \in I$	there are no *nilpotent* elements
I is *primary*	$fg \in I$ and $g \notin I \,\Rightarrow\, (\exists s : f^s \in I)$	every *zerodivisor* is nilpotent

Example 5. The ideal $I = \langle x^2 + 10x + 34, 3y - 2x - 13 \rangle$ is maximal in $\mathbb{R}[x, y]$. The field $\mathbb{R}[x, y]/I$ is isomorphic to the complex numbers $\mathbb{C} = \mathbb{R}[i]/\langle i^2 + 1 \rangle$. One isomorphism is gotten by sending $i = \sqrt{-1}$ to $\frac{1}{\sqrt{169}}(x + 5y)$. The square of that expression is -1 mod I.

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

Proposition 6. *We have the following implications: I maximal $\Rightarrow$ I prime $\begin{array}{l}\Rightarrow\ I\ \textit{radical},\\ \Rightarrow\ I\ \textit{primary}.\end{array}$ None of these implications is reversible. Every intersection of prime ideals is radical.*

Proof. The first implication holds because there are no zerodivisors in a field. Take $g = f^{s-1}$ to see that prime implies radical. Prime implies primary is clear. To see that no implication is reversible consider the following three ideals in the polynomial ring $\mathbb{R}[x, y]$ with $n = 2$:

- $I = \langle\, x^2 \,\rangle$ 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 because every intersection of radical ideals is a radical ideal. $\square$

We now revisit the singular surface in Figure 1 from the perspective of ideals.

Example 7 ($n = 3$)**.** Consider the ideal generated by the partial derivatives of the cubic f:

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

The given cubic f is not in this ideal because any polynomial in I has zero constant term. The ideal I is radical because we can write it as the intersection of five maximal ideals:

$$I \;=\; \langle x,y,z\rangle \cap \langle x{-}1,y{-}1,z{-}1\rangle \cap \langle x{-}1,y{+}1,z{+}1\rangle \cap \langle x{+}1,y{-}1,z{+}1\rangle \cap \langle x{+}1,y{+}1,z{-}1\rangle.$$

The *Chinese Remainder Theorem* implies that the quotient ring is a product of fields:

$$\mathbb{R}[x,y]/I \;\simeq\; \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}.$$

The cubic f lies in the last four maximal ideals. Their intersection is equal to $I + \langle f \rangle$. The zero set of the radical ideal $I + \langle f \rangle$ consists of the four singular points on the surface.

Every ideal has many different generating sets, and there is no canonical notion of basis. For instance, the set $\mathcal{F} = \{x^6 - 1, x^{10} - 1, x^{15} - 1\}$ minimally generates the ideal $\langle x - 1 \rangle$. Of course, the singleton $\{x - 1\}$ is a preferable generating set, given that every ideal in $K[x]$ is *principal* for $n = 1$. The *Euclidean algorithm* transforms the set $\mathcal{F}$ into the set $\{x - 1\}$.

A certificate for the fact that $x - 1$ lies in the ideal generated by $\mathcal{F}$ is the identity

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

Such certificates can be found with the *Extended Euclidean Algorithm*. Finding certificates for ideal membership when $n \geq 2$ comes up when we discuss the Nullstellensatz in Lecture 5.

Gaussian elimination carries out a similar transformation for ideals that are generated by linear polynomials. For example, the following two ideals in $\mathbb{Q}[x,y,z]$ are identical:

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

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.

We next introduce Gröbner bases. This theory offers a method for computing with ideals in a polynomial ring $K[\mathbf{x}]$. Implementations of Gröbner bases are available in all major computer algebra systems, and we strongly encourage our readers to experiment with this.

Informally, we can think of Gröbner bases as a version of the Euclidean algorithm for polynomials in $n \geq 2$ variables, and as version of Gaussian elimination for polynomials of degree ≥ 2. Gröbner bases for ideals in $K[\mathbf{x}]$ are fundamental in non-linear algebra, just like Gaussian elimination for matrices were fundamental when we studied linear algebra.

We identify the set $\mathbb{N}^n$ with the monomial basis of $K[\mathbf{x}]$. The coordinatewise order on $\mathbb{N}^n$ corresponds to divisibility of monomials, i.e. we have $\mathbf{a} \leq \mathbf{b}$ if and only if $\mathbf{x}^\mathbf{a}$ divides $\mathbf{x}^\mathbf{b}$.

Theorem 8 (Dickson's Lemma)**.** *Any infinite subset of* $\mathbb{N}^n$ *contains a pair satisfying* $\mathbf{a} \leq \mathbf{b}$*.*

Proof. We proceed by induction on n. The statement is trivial for $n = 1$. Any subset of cardinality at least two 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 induction. Hence each $\mathcal{M}_i$ is finite, and we have $\mathcal{M}_i \neq \emptyset$ for infinitely many i.

The infinite subset $\cup_{i=0}^{\infty}\mathcal{M}_i$ of $\mathbb{N}^{n-1}$ satisfies the assertion. This means that its subset of minimal elements with respect to the coordinatewise order is finite. Hence there exists an index j such that all minimal elements are contained in the finite set $\cup_{i=0}^{j}\mathcal{M}_i$. Pick any element $(\mathbf{b}, k) \in \mathcal{M}_k$ for $k > j$. Since $\mathbf{b}$ is not minimal in $\cup_{i=0}^{\infty}\mathcal{M}_i$, there exists an index i with $i \leq j < k$ and an element $\mathbf{a} \in \mathcal{M}_i$ with $\mathbf{a} \leq \mathbf{b}$. Then we have $(\mathbf{a}, i) \leq (\mathbf{b}, k)$ in $\mathcal{M}$. $\square$

Corollary 9. *For any set* $\mathcal{M} \subset \mathbb{N}^n$*, its subset of coordinatewise minimal elements is finite.*

Definition 10. A total ordering $\prec$ on $\mathbb{N}^n$ is a *monomial order* if, for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$ we have

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

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

- *the lexicographic ordering*: $\mathbf{a} \prec_{\text{lex}} \mathbf{b}$ if the leftmost non-zero entry of $\mathbf{b} - \mathbf{a}$ is positive.
- *the degree lexicographic order*: we set $\mathbf{a} \prec_{\text{deglex}} \mathbf{b}$ if either $|\mathbf{a}| < |\mathbf{b}|$, or $|\mathbf{a}| = |\mathbf{b}|$ and the leftmost non-zero entry of $\mathbf{b} - \mathbf{a}$ is positive.
- *the degree reverse lexicographic order*: we set $\mathbf{a} \prec_{\text{revlex}} \mathbf{b}$ if either $|\mathbf{a}| < |\mathbf{b}|$, or $|\mathbf{a}| = |\mathbf{b}|$ and the rightmost non-zero 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.

Throughout this course 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 $y \prec z \prec x$". Further choices of monomial orderings can be obtained by assigning positive weights to the variables. See [1, Exercise 11 in §2.4].

Remark 11. Fix a monomial order $\prec$ and let $\mathcal{M}$ be any infinite subset of $\mathbb{N}^n$. Then $\mathcal{M}$ has a unique minimal element with respect to $\prec$. To see this, apply Dickson's Lemma. Our set $\mathcal{M}$ has a finite subset of minimal elements with respect to the component-wise partial order on $\mathbb{N}^n$. This finite subset is linearly ordered by $\prec$, and 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 non-zero coefficient. For a comparison among our orders, let $n = 3$ with variable order $x \succ y \succ z$:

$$\text{If } f = x^2 + xz^2 + y^3 \text{ then } \text{in}_{\prec_{\text{lex}}}(f) = x^2,\ \text{in}_{\prec_{\text{deglex}}}(f) = xz^2, \text{ and } \text{in}_{\prec_{\text{revlex}}}(f) = y^3.$$

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

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

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.

Proposition 12. *Fix a monomial order $\prec$. Every ideal I 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. □

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

Theorem 13. *If $\mathcal{G}$ is a Gröbner basis for an ideal I then $I = \langle \mathcal{G} \rangle$.*

Proof. Suppose that $\mathcal{G}$ does not generate I. Among all polynomials f in the set difference $I \backslash \langle \mathcal{G} \rangle$, 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 11. Since $\mathbf{x}^\mathbf{b} \in \mathrm{in}_\prec(I)$, there exists an element $g \in \mathcal{G}$ that divides $\mathbf{x}^\mathbf{b}$, say $\mathbf{x}^\mathbf{b} = \mathbf{x}^\mathbf{c} \cdot g$. Now, $f - \mathbf{x}^\mathbf{c} g$ is a polynomial with strictly smaller leading monomial. It lies in I but it does not lie in the ideal $\langle \mathcal{G} \rangle$. This is a contradiction to the choice of f. □

Corollary 14 (Hilbert's Basis Theorem)**.** *Every ideal I in $K[\mathbf{x}]$ is finitely generated.*

Proof. Fix any monomial order $\prec$. By Proposition 12, the ideal I has a finite Gröbner basis $\mathcal{G}$. By Theorem 13, I is generated by $\mathcal{G}$. □

Gröbner bases are not unique. If $\mathcal{G}$ is a Gröbner basis of I with respect to $\prec$ 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 15. Fix I and $\prec$. A Gröbner basis $\mathcal{G}$ is *reduced* if the following conditions hold:

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

(b) For any two distinct $g, h \in \mathcal{G}$, no monomial occurring 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 ordering $\prec$.

Theorem 16. *The ideal I has a unique reduced Gröbner basis with respect to $\prec$.*

Proof idea. We refer to [1, §2.7, Theorem 5]. The idea is as follows. We start with any Gröbner basis $\mathcal{G}$ and we turn it into a reduced Gröbner basis by the following steps. First we divide each $g \in \mathcal{G}$ by its leading coefficient to make it monic, so that (a) holds. We remove all elements g from $\mathcal{G}$ 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 [1, §2.3] to any trailing monomial until no more trailing monomial is divisible by any leading monomial. The resulting set is the reduced Gröbner basis. □

Let $\mathcal{S}_\prec(\mathcal{I})$ 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 17. *The set $\mathcal{S}_\prec(I)$ of standard monomials is a basis for the K-vectorspace $K[\mathbf{x}]/I$.*

Proof. The image of $\mathcal{S}_\prec(I)$ in $K[\mathbf{x}]/I$ is linearly independent because every non-zero polynomial f has at least one monomial, namely $\mathrm{in}_\prec(f)$, that is not in $\mathcal{S}$. We next prove that $\mathcal{S}_\prec(I)$ span $K[\mathbf{x}]/I$. 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 term 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 $\mathbf{x^c}$ has the same property. This is a contradiction. □

Software for Gröbner bases rests on the *Buchberger Algorithm* [1, S 2.7]. This is implemented in all major computer algebra systems. It takes as its input a monomial order $\prec$ and a finite set $\mathcal{F}$ of polynomials in $K[\mathbf{x}]$, and its output is the unique reduced Gröbner basis $\mathcal{G}$ for the ideal $I = \langle \mathcal{F} \rangle$ with respect to $\prec$. In what follows we present some examples of pairs $(\mathcal{F}, \mathcal{G})$ for $n = 3$. In each case we take the lexicographic term order with $x \succ y \succ z$.

Example 18. The input $\mathcal{F} \subset \mathbb{Q}[x, y, z]$ is transformed into the reduced Gröbner basis $\mathcal{G}$:

- For $n = 1$, the reduced Gröbner basis consists of the greatest common divisor:
  $\mathcal{F} = \{x^3-6x^2-5x-14, 3x^3+8x^2+11x+10, 4x^4+4x^3+7x^2-x-2\}$, $\mathcal{G} = \{\underline{x^2}+x+2\}$.

- 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 $\mathcal{G} = \{\underline{x} - \frac{16}{7},\ \underline{y} + \frac{12}{7},\ \underline{z} + \frac{9}{7}\}$. Leading monomials are underlined.

- Here is another ideal we saw earlier: $\mathcal{F} = \{xy - z, xz - y, yz - x\}$, $\mathcal{G} = \{\underline{x} - yz, \underline{y^2} - z^2, \underline{yz^2} - y, \underline{z^3} - z\}$. There are precisely 5 standard monomials: $\mathcal{S}_\prec(I) = \{1, y, z, yz, \underline{z^2}\}$. This is consistent with Example 7, where we saw that $\mathcal{F}$ has precisely 5 zeros in $\mathbb{C}^3$.

- This input is a curve in the (y, z)-plane parametrized by two cubics in one variable x: $\mathcal{F} = \{y - x^3 + 4x, z - x^3 - x + 1\}$. The Gröbner basis reveals its implicit equation: $\mathcal{G} = \{\, \underline{x} + \frac{1}{5}y + \frac{1}{5}z - \frac{1}{5},\ \underline{y^3} - 3y^2z - 3y^2 + 3yz^2 + 6yz + 28y - z^3 - 3z^2 + 97z + 99 \,\}$.

- Let z be the sum of $x = \sqrt[3]{7}$ and $y = \sqrt[4]{5}$. We write this as $\mathcal{F} = \{x^3-7, y^4-5, z-x-y\}$. Then $z = \sqrt[3]{7} + \sqrt[4]{5}$ is algebraic of degree 12 over $\mathbb{Q}$. Its minimal polynomial is seen in $\mathcal{G} = \{\underline{z^{12}} - 28z^9 - 15z^8 + 294z^6 - 1680z^5 + 75z^4 - 1372z^3 - 7350z^2 - 2100z + 2276, \ldots\}$.

- The elementary symmetric polynomials $\mathcal{F} = \{x+y+z, xy+xz+yz, xyz\}$ have the Gröbner basis $\mathcal{G} = \{\underline{x}+y+z, \underline{y^2}+yz+z^2, \underline{z^3}\}$. There are six standard monomials. The quotient $\mathbb{Q}[x,y,z]/I$ carries the regular representation of the symmetric group S_3.

For these instances, what is the reduced Gröbner basis for the degree lexicographic order?

In general, the choice of monomial order can make a huge difference in the complexity of the size of the reduced Gröbner basis, even if the input polynomials are homogeneous.

Example 19 (Intersecting two quartic surfaces in $\mathbb{P}^3$)**.** Consider the ideal I generated by two random homogeneous polynomials of degree 4 in $n = 4$ variables. If $\prec$ is the degree reverse lexicographic order then the reduced Gröbner basis $\mathcal{G}$ contains 5 elements of degree up to 7. If $\prec$ is the lexicographic order then $\mathcal{G}$ contains 150 elements of degree up to 73.

Naturally, one uses a computer to find the 150 elements in the aforementioned Gröbner basis. Many computer algebra systems offer an implementation of Buchberger's algorithm for Gröbner bases. Our readers are strongly encouraged to use a computer algebra system.

Exercises

1. Show that the polynomial $f = 5x^3 - 25x^2y + 25y^3 + 15xy - 50y^2 - 5x + 25y - 1$ is a product of three linear factors in $\mathbb{R}[x,y]$. Draw the plane curve $\{f = 0\}$.

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

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

4. The *radical* $\sqrt{I}$ of an ideal I is the smallest radical ideal containing I. Prove:

   - The radical of a primary ideal is prime.
   - The radical of a principal ideal is principal.
   - The radical of a monomial ideal is a monomial ideal.

5. Show that the following inclusions always hold, and that they are strict in general:

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

6. Using Gröbner bases, find the minimal polynomials of $\sqrt[5]{6} + \sqrt[7]{8}$ and $\sqrt[5]{6} - \sqrt[7]{8}$.

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

8. Investigate the ideal $I = \langle x^3 - yz, y^3 - xz, z^3 - xy \rangle$. Is it radical? If not, find $\sqrt{I}$. Regarding I as a system of 3 equations in 3 unknowns, what are the solutions in $\mathbb{R}^3$?

9. Find an ideal in $\mathbb{Q}[x, y]$ whose reduced Gröbner basis (for the lexicographic monomial order) consists of precisely 5 elements and there are precisely 19 standard monomials.

10. Prove: An ideal is principal if and only if its reduced Gröbner basis is a singleton.

11. Let I be the ideal generated by the n elementary symmetric polynomials in n variables. Pick a monomial ordering and determine the initial monomial ideal $\text{in}_{\prec}(I)$.

12. Let X be 2×2-matrix whose $n = 4$ 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.

13. A symmetric 3×3-matrix with unknown entries 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 among these determinants? Use lexicographic Gröbner bases to answer this question.

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

15. Does the cubic surface in Figure 1 contain any straight line? Find all such lines.

References

[1] D. Cox, J. Little and D. O'Shea: *Ideals, Varieties, and Algorithms*. An introduction to computational algebraic geometry and commutative algebra, Third edition, Undergraduate Texts in Mathematics, Springer, New York, 2007.