

1 Polynomial Ideals

Copyright © 2025, Gregory G. Smith
Last updated: 4 February 2025

As a counterpart to affine subvarieties, we develop the theory of ideals in a polynomial ring. We introduce an analogue of Euclidean division algorithm for multivariate polynomials. This requires identifying the “leading term” of a polynomial.

1.0 Ideals

What are the basic algebraic objects?

1.0.0 Definition. A subset I of the ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ is an *ideal* if it is nonempty and the relations $r, s \in I$ and $f, g \in I$ imply that $rf + sg \in I$. For any index set $\mathcal{B}$, a **system of generators** for an ideal I is a family $\{f_\beta\}_{\beta \in \mathcal{B}}$ of polynomials such that $f_\beta \in I$, for all $\beta \in \mathcal{B}$, and every element in I is a finite linear combination of the generators f_β with coefficients in S . An ideal is *finitely generated* if it has a finite system of generators. The *ideal generated by a family* $\{f_\beta\}_{\beta \in \mathcal{B}}$ is denoted $\langle f_\beta \rangle_{\beta \in \mathcal{B}}$.

An ideal is closed under finite linear combinations where the coefficients are taken from the ring.

1.0.1 Ideal Membership Problem. Given a finite set of polynomials $f_1, f_2, \dots, f_m$ in S , decide whether a polynomial g in S belongs to the ideal $\langle f_1, f_2, \dots, f_m \rangle$.

We will demonstrate that the ideal membership problem has a solution by developing a generalization of the row reduction and the division algorithms.

1.0.2 Example. Since $xz - y^2 = x(z - xy) + y(x^2 - y)$, the polynomial $xz - y^2$ belongs to the ideal $\langle y - x^2, z - xy \rangle$ in $\mathbb{Q}[x, y, z]$. $\diamond$

When the polynomials $f_1, f_2, \dots, f_m, g \in S$ are all linear, we can solve the ideal membership problem using linear algebra—use Gaussian elimination. We already know how to solve the ideal membership problem in one other special case.

1.0.3 Theorem. For any nonzero f in $\mathbb{K}[x]$ and any g in $\mathbb{K}[x]$, there exists unique polynomials q and r in $\mathbb{K}[x]$ such that $g = qf + r$ where $r = 0$ or $\deg(r) < \deg(f)$. $\square$

1.0.4 Corollary. Any ideal $I \subseteq \mathbb{K}[x]$ is principal; in other words, there exists an f such that $I = \langle f \rangle$. Hence, $g \in I$ if and only if f divides g .

Proof. Let $0 \neq f \in I$ have minimal degree among nonzero elements of I . When $g \in I$, there exists q and r in $\mathbb{K}[x]$ such that $g = qf + r$ where $r = 0$ or $\deg(r) < \deg(f)$. Since $r = g - qf \in I$, our choice of f implies that $r = 0$. Therefore, g is a multiple of f and $I = \langle f \rangle$. $\square$

1.0.5 Proposition. Let $\{f_\beta\}_{\beta \in \mathcal{B}}$ be a family of polynomials in the ring S . For any family $\{g_\alpha\}_{\alpha \in \mathcal{A}}$ of polynomials in the ideal $\langle f_\beta \rangle_{\beta \in \mathcal{B}}$, the associated affine subvarieties in $\mathbb{A}^n$ satisfy $V(f_\beta \mid \beta \in \mathcal{B}) \subseteq V(g_\alpha \mid \alpha \in \mathcal{A})$.

Proof. By hypothesis, we have $g_\alpha \in \langle f_\beta \rangle_{\beta \in \mathcal{B}}$ for all $\alpha \in \mathcal{A}$, so g_α is a finite linear combination of the generators with coefficients in S . Hence, for each index $\alpha \in \mathcal{A}$, there exists polynomials $h_{\alpha, \beta} \in S$, for all $\beta \in \mathcal{B}$, such that $g_\alpha = \sum_{\beta} h_{\alpha, \beta} f_\beta$, where only finitely many of the $h_{\alpha, \beta}$ are nonzero. At every point in $\mathbb{A}^n$ where all the generators f_β vanish, we see that the polynomial g_α also vanishes. $\square$

1.0.6 Corollary. The affine subvariety $X := V(f_\beta \mid \beta \in \mathcal{B})$ only depends on the ideal $I := \langle f_\beta \rangle_{\beta \in \mathcal{B}}$. As a consequence, we write $X = V(I)$. $\square$

1.0.7 Corollary. For any ideals I and J in S satisfying $I \subseteq J$, the associated affine subvarieties satisfy $V(J) \subseteq V(I)$. $\square$

The operator V sending ideals in S to affine subvarieties in $\mathbb{A}^n$ reverses inclusions.

1.0.8 Definition. For any subset $W \subseteq \mathbb{A}^n$, the (*vanishing*) *ideal* of W is $I(W) := \{f \in S = \mathbb{K}[x_1, x_2, \dots, x_n] \mid f(a) = 0 \text{ for all } a \in W\}$. This set is an ideal: for any $r, s \in S$ and any $f, g \in S$ that vanish on W , the linear combination $r f + s g$ also vanishes on W .

1.0.9 Examples.

- We have $I(\mathbb{A}^n(\mathbb{C})) = \langle 0 \rangle$ and $I(\emptyset) = \langle 1 \rangle$.
- For a singleton $(a_1, a_2, \dots, a_n) \in \mathbb{A}^n$, one may show that

$$I(\{(a_1, a_2, \dots, a_n)\}) = \langle x_1 - a_1, x_2 - a_2, \dots, x_n - a_n \rangle.$$

- For the subset $W = \{(1, 1), (2, 3)\} \subset \mathbb{A}^2(\mathbb{Q})$, one verifies that

$$\begin{aligned} I(W) &= \langle (x-1)(y-3), (x-1)(x-2), (y-1)(x-2), (y-1)(y-3) \rangle \\ &= \langle 2x - y - 1, x^2 - 3x + 2 \rangle. \end{aligned} \quad \diamond$$

1.0.10 Lemma (Properties of vanishing ideals).

- For any ideal J in $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ and any subset W of $\mathbb{A}^n$, we have the inclusions $J \subseteq I(V(J))$ and $W \subseteq V(I(W))$.
- For any nested subsets $W \subseteq X$ in $\mathbb{A}^n$, we have $I(X) \subseteq I(W)$.
- For any subsets W and X in $\mathbb{A}^n$, we have $I(W \cup X) = I(W) \cap I(X)$.
- For any subset W of $\mathbb{A}^n$, we have $V(I(W)) = \overline{W}$ where $\overline{W}$ denotes the Zariski closure of W .
- For any affine subvarieties X and Y in $\mathbb{A}^n$, we have $X = Y$ if and only if $I(X) = I(Y)$.

The inclusions in part i may be proper. Since $V(x^2, y^2) = \{(0, 0)\}$, we have $\langle x^2, y^2 \rangle \subset I(V(x^2, y^2)) = \langle x, y \rangle$. For the subset

$$W := \{(a, b) \mid a^2 + b^2 = 1 \text{ and } a \neq 0\},$$

we have $I(W) = \langle x^2 + y^2 - 1 \rangle$ and $W \subset V(I(W))$.

Proof.

- Any polynomial in the ideal J vanishes at every point in $V(J)$. Similarly, every polynomial in $I(W)$ vanishes at every point in W .
- Any polynomial vanishing on X must also vanish on W .
- A polynomial vanishes on $W \cup X$ if and only if it vanishes at every point in W and every point in X .
- Since $V(I(W))$ is Zariski closed, part i shows that $\overline{W} \subseteq V(I(W))$. Conversely, there exists an ideal J in S such that $\overline{W} = V(J)$. Since $W \subseteq \overline{W} = V(J)$, parts i–ii imply that $J \subseteq I(V(J)) \subseteq I(W)$. Using Corollary 1.0.7, we obtain $V(I(W)) \subseteq V(J) = \overline{W}$, so we conclude that $V(I(W)) = \overline{W}$.
- When $X = Y$, it follows that $I(X) = I(Y)$. For any affine subvariety Z , part iv proves that $V(I(Z)) = Z$. Thus, Corollary 1.0.7 yields the final statement. $\square$

The operator I sending subsets in $\mathbb{A}^n$ to ideals in S reverses inclusions.

Restricting to affine subvarieties in $\mathbb{A}^n$, the operator I gives a one-sided inverse to the operator V .

1.1 Monomial Orders

To manipulate a multivariate polynomial, we must order its terms. What order should we use?

1.1.0 Definition. An ideal I in $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ is *monomial* if there exists a subset $\mathcal{A} \subseteq \mathbb{N}^n$ such that $I = \langle x^a := x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \mid a \in \mathcal{A} \rangle$.

A monomial ideal is generated by monomials.

1.1.1 Example. The $\mathbb{K}[x, y]$ -ideal $I = \langle x^4y^2, x^3y^3, x^2y^5 \rangle$ is generated by monomials. $\diamond$

1.1.2 Lemma. Let $I := \langle x^a \mid a \in \mathcal{A} \rangle$ be a monomial ideal. A monomial x^b belongs to I if and only if x^b is divisible by x^a for some $a \in \mathcal{A}$.

Proof. The monomial x^b is a multiple of x^a for some $a \in \mathcal{A}$ when there exists $c \in \mathbb{N}^n$ such that $x^b = x^c x^a$, so $x^b \in I$. Conversely, when $x^b = \sum_{a \in \mathcal{A}} h_a x^a$ where $h_a \in S$ and only finitely many of the h_a are nonzero, every term on the right side is divisible by some $x^a \in I$. Hence, the left side must have the same property. $\square$

1.1.3 Corollary. Monomial ideals in S are equal if and only if they contain the same monomials. $\square$

1.1.4 Lemma. Let I be a monomial ideal in S . For any polynomial $f \in S$, the following are equivalent.

- a. The polynomial f belongs to I .
- b. Every term in the polynomial f lies in I .
- c. The polynomial f is a $\mathbb{K}$ -linear combination of monomials in I .

Sketch of proof. The implications $c \Rightarrow b \Rightarrow a$ are trivial. The implication $a \Rightarrow c$ is very similar to the proof of Lemma 1.1.2. $\square$

1.1.5 Theorem (Dickson Lemma). Let n be a nonnegative integer. Every monomial ideal in the ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ is finitely generated.

Proof. Let I be a monomial ideal in S . We proceed by induction on n . When $n = 0$, the statement is vacuous. When $n = 1$, the univariate polynomial ring is a principal ideal domain and I is generated by the lowest degree monomial it contains.

Assume that $n > 1$. For each nonnegative integer i , consider the monomial ideal $J_i := \langle x^a \mid x^a x_n^i \in I \rangle$ in the smaller polynomial ring $\mathbb{K}[x_1, x_2, \dots, x_{n-1}]$. The induction hypothesis implies that each J_i has a finite generating set $\mathcal{B}_i$ and the monomial ideal $J := \langle \bigcup_i \mathcal{B}_i \rangle$ has a finite generating set $\mathcal{B}$. Because $\mathcal{B}$ is finite, there exists a nonnegative index m such that $\mathcal{B} \subseteq \mathcal{B}_0 \cup \mathcal{B}_1 \cup \dots \cup \mathcal{B}_m$. It suffices to show that the finite set $\{x^a x_n^i \mid x^a \in \mathcal{B}_i \text{ and } 0 \leq i \leq m\}$ generates I . Consider a monomial $x^a x_n^i \in I$. Since $x^a \in J_i = \langle \mathcal{B}_i \rangle$, there is a monomial $x^b \in \mathcal{B}_i$ that divides x^a . If $i \leq m$, then the monomial $x^b x_n^i$ divides $x^a x_n^i$. If $i > m$, then there exists $x^c \in \mathcal{B}$ such that x^c divides x^b and there exists $j \leq m$ and $x^d \in \mathcal{B}_j$ such that x^d divides x^c . Thus, the monomial $x^d x_n^j$ divides $x^a x_n^i$. $\square$

1.1.6 Definition. A *monomial order* on the polynomial ring S is a total order $>$ on the set $\{x^u \mid u \in \mathbb{N}^n\}$ of monomials such that

- for any $x^u > x^v$ and any $w \in \mathbb{N}^n$, we have $x^w x^u = x^{w+u} > x^{w+v}$;
- for all $1 \leq i \leq n$, we have $x_i > 1_S$.

1.1.7 Definition. The *lexicographic order* is monomial order $>_{\text{lex}}$ on $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ defined by $x^u >_{\text{lex}} x^v$ when the first nonzero entry in $u - v = (u_1 - v_1, u_2 - v_2, \dots, u_n - v_n)$ is positive.

This result is commonly attributed to [Leonard Dickson](#) who published it in 1913. However, it was certainly known earlier; [Paul Gordan](#) used a variant in 1899 as part of his proof of the Hilbert basis theorem.

In the lexicographic order, we have $x >_{\text{lex}} y^2 >_{\text{lex}} yz >_{\text{lex}} z^{100}$.

1.1.8 Definition. The *graded lexicographic order* is the monomial order $>_{\text{glex}}$ on $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ defined by $x^u >_{\text{glex}} x^v$ when either $|u| > |v|$ or $|u| = |v|$ and $x^u >_{\text{lex}} x^v$.

The graded lexicographic order gives $x^2 >_{\text{glex}} xy >_{\text{glex}} xz >_{\text{glex}} y^2 >_{\text{glex}} x$.

1.1.9 Definition. The *graded reverse lexicographic order* is the monomial order $>_{\text{grevlex}}$ on $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ defined by $x^u >_{\text{grevlex}} x^v$ when either $|u| > |v|$ or $|u| = |v|$ and the last nonzero entry in the difference $u - v = (u_1 - v_1, u_2 - v_2, \dots, u_n - v_n)$ is negative.

We have

$$x^2 >_{\text{grevlex}} xy >_{\text{grevlex}} y^2 >_{\text{grevlex}} xz.$$

The next result justifies the definition of a monomial ordering.

1.1.10 Proposition. For any total order on $\{x^u \mid u \in \mathbb{N}^n\}$ compatible with multiplication, the following conditions are equivalent.

- a. The relation $>$ is a well-order (every nonempty subset has a least element);
- b. Every decreasing sequence $x^{u_1} > x^{u_2} > x^{u_3} > \dots$ eventually stabilizes;
- c. For all $1 \leq i \leq n$, we have $x_i > 1$;
- d. For all $u \in \mathbb{N}^n$ such that $u \neq 0$, we have $x^u > 1$;
- e. When x^v divides x^u and $v \neq u$, we have $x^u > x^v$.

Proof.

- a $\Rightarrow$ b: For any decreasing sequence $x^{u_1} > x^{u_2} > x^{u_3} > \dots$ that does not stabilize, the nonempty set $\{u_1, u_2, u_3, \dots\}$ has no smallest element, so the relation $>$ is not a well-order.
- b $\Rightarrow$ c: Suppose that $1 > x_i$ for some $1 \leq i \leq n$. It follows that, for all $m \in \mathbb{N}$, we have $x_i^m > x_i^{m+1}$, so $1 > x_i > x_i^2 > x_i^3 > \dots$ is an infinite decreasing sequence.
- c $\Rightarrow$ d: We proceed by induction on $|u|$. Part c gives the base case $|u| = 1$. Next, write $x^u = x^v x_i$ where $v \in \mathbb{N}^n$ and $1 \leq i \leq n$. It follows that $x^u > x^v$. Since $|v| = |u| - 1$, the induction hypothesis implies that $x^v > 1$.
- d $\Rightarrow$ e: Suppose that $u_i \geq v_i$ for all $1 \leq i \leq n$ and $u \neq v$. Setting $w = u - v$, we have $x^w > 1$ and $x^u = x^w x^v > x^v$.
- e $\Rightarrow$ a: Let $\mathcal{M}$ be a nonempty set of monomials. By the Dickson Lemma 1.1.5, there is a finite subset $\mathcal{B} \subseteq \mathcal{M}$ such that, for each $x^u \in \mathcal{M}$, there is $x^v \in \mathcal{B}$ that divides x^u . Part e ensures that $x^u > x^v$ or $x^u = x^v$. Thus, $\mathcal{B}$ contains the least element in $\mathcal{M}$ with respect to the order $>$. $\square$

The graded lexicographic order is like judging an actor by their best movie whereas the graded reverse lexicographic order is like judging an actor by their worst movie.

1.2 Division

How do we divide multivariate polynomials?

1.2.0 Definition. Fix a monomial order $>$ on $S := \mathbb{K}[x_1, x_2, \dots, x_n]$. Any nonzero polynomial $f \in S$ can be written uniquely in the form $f = a_1 x^{u_1} + a_2 x^{u_2} + \dots + a_m x^{u_m}$ where $x^{u_1} > x^{u_2} > \dots > x^{u_m}$ and $a_1, a_2, \dots, a_m \in \mathbb{K}$. We introduce the following terminology.

- The *leading monomial* of f is $\text{LM}(f) := x^{u_1}$.
- The *leading coefficient* of f is $\text{LC}(f) := a_1$.
- The *leading term* of f is $\text{LT}(f) := \text{LC}(f) \text{LM}(f) = a_1 x^{u_1}$.

1.2.1 Example. Let $f = y^4z^3 + 2x^2y^2z^2 + 3x^5 + 4z^4 + 5y^2$ in $\mathbb{K}[x, y, z]$. Using the lexicographic order $>_{\text{lex}}$, we have $\text{LM}(f) = x^5$, $\text{LC}(f) = 3$, and $\text{LT}(f) = 3x^5$. Under the graded lexicographic order $>_{\text{grevlex}}$, it follows that $\text{LM}(f) = y^4z^3$, $\text{LC}(f) = 1$, and $\text{LT}(f) = y^4z^3$. $\diamond$

1.2.2 Theorem (Division algorithm). *Fix a monomial order $>$ on S and let $\mathbf{G} := [g_1 \ g_2 \ \cdots \ g_m]^T$ be an $(m \times 1)$ -matrix in S^m . For any polynomial f in S , there exists polynomials $q_1, q_2, \dots, q_m, r$ in S such that*

$$f = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m + r,$$

none of the monomials in r lie in the ideal $\langle \text{LM}(g_1), \text{LM}(g_2), \dots, \text{LM}(g_m) \rangle$, and $\text{LM}(f) \geq \text{LM}(q_j g_j)$ for all $1 \leq j \leq m$.

Proof. We establish the existence of the remainder $r \in S$ and the matrix $\mathbf{Q} := [q_1 \ q_2 \ \cdots \ q_m]$ of quotient polynomials by giving an algorithm.

Input: A polynomial $f \in S$ and a matrix $\mathbf{G} := [g_1 \ g_2 \ \cdots \ g_m]^T$.

Output: The remainder $r \in S$ and the matrix $\mathbf{Q} := [q_1 \ q_2 \ \cdots \ q_m]$.

Set $(r, p) := (0, f)$.

For j from 1 to m do set $q_j := 0$.

While $p \neq 0$ do

$i := 1$;

While $(i \leq m)$ and $\text{LM}(g_i)$ does not divide $\text{LM}(p)$ do
set $i := i + 1$.

If $i \leq m$ then $(q_i, p) := \left(q_i + \frac{\text{LT}(p)}{\text{LT}(g_i)}, p - \frac{\text{LT}(p)}{\text{LT}(g_i)} g_i \right)$
else $(r, p) := (r + \text{LT}(p), p - \text{LT}(p))$;

To demonstrate the correctness of this algorithm, we first show that $f = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m + p + r$ holds at every stage. It is clearly true for the initial values. When $\text{LM}(g_i)$ divides $\text{LM}(p)$, we have

$$q_i g_i + p = \left(q_i + \frac{\text{LT}(p)}{\text{LT}(g_i)} \right) g_i + \left(p - \frac{\text{LT}(p)}{\text{LT}(g_i)} g_i \right)$$

and otherwise $p + r = (r + \text{LT}(p)) + (p - \text{LT}(p))$.

Since each term added to q_i satisfies $\text{LM}(f) \geq \frac{\text{LM}(p)}{\text{LM}(g_i)} \text{LM}(g_i)$, we see that $\text{LM}(f) \geq \text{LM}(q_j g_j)$ for all $1 \leq j \leq m$. Similarly, a term $\text{LT}(p)$ is added to r only if the monomial $\text{LM}(p)$ is not divisible by an element of $\{\text{LM}(g_1), \text{LM}(g_2), \dots, \text{LM}(g_m)\}$. Because the algorithm halts when $p = 0$, we deduce that the output has the desired form.

The algorithm terminates because in each iteration of the main loop we remove the lead term of p . As $>$ is a monomial order, every decreasing sequence of monomials eventually terminates. $\square$

1.2.3 Example. Consider $f := x^3 + y^2 + 2z^2 + x + y + 1 \in \mathbb{Q}[x, y, z]$ and let $>$ be a monomial order such that $x > y > z$. For the matrix $[x \ y]^T$, the division algorithm gives $f = (x^2 + 1)x + (y + 1)y + 2z^2 + 1$. $\diamond$

1.2.4 Example. Consider $f := x^2y \in \mathbb{Q}[x, y]$ and let $>$ be a monomial order such that $x > y$. For the matrix $[xy - x \ x^2 - y]^T$, the division algorithm yields $f = x(xy - x) + (x^2 - y) + y$. However, for the matrix $[x^2 - y \ xy - x]^T$, it yields $f = y(x^2 - y) + 0(xy - x) + y^2$. $\diamond$

The **remainder** r of the polynomial f on division by the matrix $\mathbf{G}$ is often denoted by $f \% \mathbf{G}$.

In general, the remainder depends on the monomial order and the order of the entries in $\mathbf{G}$.

1.2.5 Definition. For an ideal I in S , the *leading term ideal* $\text{LT}(I)$ is the monomial ideal generated by the leading terms of all elements in the ideal I , so we have $\text{LT}(I) := \langle \text{LT}(f) \mid f \in I \rangle$.

The leading term ideal is not simply the ideal generated by the leading terms of any generating set.

1.2.6 Example. Let $>$ be a monomial order on $\mathbb{Q}[x, y]$ such that $x > y$. For the ideal $I := \langle x^2 - y, xy - x \rangle$, we clearly have $\langle x^2, xy \rangle \subseteq \text{LT}(I)$. The equation $x(xy - x) + (1 - y)(x^2 - y) = y^2 - y \in I$ also shows that $y^2 \in \text{LT}(I)$. How can one verify that $\text{LT}(I) = \langle x^2, xy, y^2 \rangle$? $\diamond$

1.2.7 Definition. For an ideal I in S , a finite collection $g_1, g_2, \dots, g_m$ of polynomials in I is a *Gröbner basis* if

$$\text{LT}(I) = \langle \text{LT}(g_1), \text{LT}(g_2), \dots, \text{LT}(g_m) \rangle.$$

Saying $g_1, g_2, \dots, g_m$ is a Gröbner basis means that the polynomials form a Gröbner basis of the ideal $\langle g_1, g_2, \dots, g_m \rangle$.

1.2.8 Examples. The generator of a principal ideal in a polynomial ring is a Gröbner basis. Any set of monomials is a Gröbner basis. Under any monomial order on $\mathbb{K}[x, y]$, one can show that the polynomials $y^2 - y, xy - x, x^2 - y$ form a Gröbner basis. $\diamond$

1.2.9 Proposition. Fix a monomial order on the polynomial ring S . Every ideal in S has admits a Gröbner basis.

Proof. Let I be an ideal in S . The leading term ideal $\text{LT}(I)$ is generated by the monomials $\text{LM}(f)$ for all $f \in I$. The Dickson Lemma 1.1.5 shows that $\text{LT}(I)$ is finitely generated. It follows that there are polynomials $g_1, g_2, \dots, g_m$ in I such that $\text{LT}(I) = \langle \text{LM}(g_1), \text{LM}(g_2), \dots, \text{LM}(g_m) \rangle$. The polynomials $g_1, g_2, \dots, g_m$ form a Gröbner basis for I . $\square$

A Gröbner basis implicitly depends on the choice of a monomial order.