

0.2.6 Example. Consider the polynomial map $\rho\colon \mathbb{A}^2 \to \mathbb{A}^3$ defined by $(s,t) \mapsto (s+t, s-t, s+2t)$. It follows that

$$\left\{\begin{aligned} x &= s + t \\ y &= s - t \\ z &= s + 2t \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} s + t - x &= 0 \\ s - t - y &= 0 \\ s + 2t - z &= 0 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} s + t - x &= 0 \\ -2t + x - y &= 0 \\ t + x - z &= 0 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} s + t - x &= 0 \\ t + x - z &= 0 \\ 3x - y - 2z &= 0 \end{aligned}\right\}$$

Hence, the image is the hyperplane $\mathrm{V}(3x - y - 2z) \subset \mathbb{A}^3$. ◇

0.2.7 Example. For any nonnegative integer n, let $\rho\colon \mathbb{A}^2 \to \mathbb{A}^n$ be the polynomial map defined by $t \mapsto (t, t^2, \dots, t^n)$. The quadratic equations $x_i\, x_j = x_k\, x_\ell$, for all $i + j = k + \ell$, vanish on the image. Are there more polynomial equations that vanish on the image? ◇

In this course, we will see that the implicitization problem has an algorithmic solution. However, the converse is much harder.

0.2.8 Definition. A *rational parametrization* of an affine subvariety X in $\mathbb{A}^n$ is a rational map $\rho\colon \mathbb{A}^m \dashrightarrow \mathbb{A}^n$ such that X is the Zariski closure of the image of ρ. An affine subvariety X is *unirational* if it admits a rational parametrization.

0.2.9 Example. The unit circle is, by Example 0.2.2, unirational. ◇

0.2.10 Example. The affine subvariety $\mathrm{V}(x^2 + y^2 + z^2 - 1) \subset \mathbb{A}^3$ is unirational with a polynomial parametrization given by

$$(t_0, t_1) \mapsto \left(\frac{2\,t_0}{t_0^2 + t + 1^1 + 1}, \frac{2\,t_1}{t_0^2 + t_1^1 + 1}, \frac{t_0^2 + t_1^2 - 1}{t_0^2 + t_1^2 + 1} \right) . \qquad ◇$$

0.2.11 Example. The Fermat hypersurface $\mathrm{V}(w^3 + x^3 + y^3 + z^3) \subset \mathbb{A}^4$ is unirational with a parametrization given by

$$\begin{pmatrix} t_0 \\ t_1 \\ t_2 \end{pmatrix} \mapsto \begin{pmatrix} -(t_0 + t_1)t_2^2 + (t_1^2 + 2t_0^2)t_2 - t_1^3 + t_0 t_1^2 - 2t_0^2 t_1 - t_0^3 \\ t_2^3 - (t_0 + t_1)t_2^2 + (t_1^2 + 2t_0^2)t_2^3 + t_0 t_1^2 - 2t_0^2 t_1 + t_0^3 \\ -t_2^3 + (t_0 + t_1)t_2^2 - (t_1^2 + 2t_0^2)t_2 + 2t_0 t_1^2 - t_0^2 t_1 + 2t_0^3 \\ (t_1 - 2t_0)t_2^2 + (t_1^2 - t_0^2)t_2 + t_1^3 - t_0 t_1^2 + 2t_0^2 t_1 - 2t_1^3 \end{pmatrix} . \qquad ◇$$

0.2.12 Remark. For a general low-degree hypersurface, there are no techniques for disproving unrationality. However, unirationality has been established only when $\deg(f) = 2$ and $n \geqslant 2$, $\deg(f) = 3$ and $n \geqslant 3$, or $n \gg \deg(f)$. For a fixed degree greater than 3, there are many values of n for which unirationality is an open problem. In contrast, a general degree d hypersurface in $\mathbb{A}^n(\mathbb{C})$ does not admit a rational parametrization whenever $d > n$. For instance, the quartic hypersurface $\mathrm{V}(x^4 + y^4 + z^4 - 1)$ in $\mathbb{A}^3$ lacks one.

1 *Polynomial Ideals*

As an counterpart to affine subvarieties, this chapter develops 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 $S := \mathbb{K}[x_1, x_2, \ldots, x_n]$ is an ***ideal*** if it is nonempty and the relations $r, s \in S$ and $f, g \in I$ imply that $r\,f + s\,g \in I$. 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 Problem (Ideal membership)**.** Given a finite set of polynomial $f_1, f_2, \ldots, f_m \in S$, decide whether a polynomial $g \in S$ belongs to the ideal $\langle f_1, f_2, \ldots, f_m \rangle$.

We will demonstrate that the ideal membership problem has an 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 $\mathbb{Q}[x, y, z]$. ◇

1.0.3 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 $\mathrm{V}(f_\beta \mid \beta \in \mathcal{B}) \subseteq \mathrm{V}(g_\alpha \mid \alpha \in \mathcal{A})$.*

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 $h_{\beta,\alpha}$ 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. □

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

1.0.5 Corollary. *For any ideals I and J in $S := \mathbb{K}[x_1, x_2, \ldots, x_n]$ satisfying $I \subseteq J$, the associated affine subvarieties satisfy $\mathrm{V}(J) \subseteq \mathrm{V}(I)$.* □

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

1.0.6 Definition. For any subset $W \subseteq \mathbb{A}^n$, the ***(vanishing) ideal*** of W is $\mathrm{I}(W) := \{f \in S = \mathbb{K}[x_1, x_2, \dots, x_n] \mid f(a) = 0 \text{ for all } a \in W\}$. 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.

1.0.7 Examples.

(i) We have $\mathrm{I}\big(\mathbb{A}^n(\mathbb{C})\big) = \langle 0 \rangle$ and $\mathrm{I}(\varnothing) = \langle 1 \rangle$.

(ii) For a singleton $(a_1, a_2, \dots, a_n) \in \mathbb{A}^n$, one may show that

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

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

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

1.0.8 Lemma (Properties of vanishing ideals)**.**

(i) *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 $J \subseteq \mathrm{I}\big(\mathrm{V}(J)\big)$ and $W \subseteq \mathrm{V}\big(\mathrm{I}(W)\big)$.*

(ii) *For any nested subsets $W \subseteq X$ in $\mathbb{A}^n$, we have $\mathrm{I}(X) \subseteq \mathrm{I}(W)$.*

(iii) *For any subsets W and X in $\mathbb{A}^n$, we have $\mathrm{I}(W \cup X) = \mathrm{I}(W) \cap \mathrm{I}(X)$.*

(iv) *For any subset W of $\mathbb{A}^n$, we have $\mathrm{V}\big(\mathrm{I}(W)\big) = \overline{W}$ where $\overline{W}$ denotes the Zariski closure of W.*

(v) *For any two affine subvarieties X and Y in $\mathbb{A}^n$, we have $X = Y$ if and only if $\mathrm{I}(X) = \mathrm{I}(Y)$.*

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

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

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

Proof.

(i) Any polynomial in the ideal J vanishes at every point in $\mathrm{V}(J)$. Similarly, every polynomial in $\mathrm{I}(W)$ vanishes at every point in W.

(ii) Any polynomial vanishing on X must also vanish on W.

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

(iii) A polynomial vanishes on $W \cup X$ if and only if it vanishes at every point in W and every point in X.

(iv) Since $\mathrm{V}\big(\mathrm{I}(W)\big)$ is Zariski closed, part (i) demonstrates that $\overline{W} \subseteq \mathrm{V}\big(\mathrm{I}(W)\big)$. Conversely, there exists an ideal J in S such that $\overline{W} = \mathrm{V}(J)$. Since $W \subseteq \overline{W} = \mathrm{V}(J)$, parts (i)–(ii) imply that $J \subseteq \mathrm{I}\big(\mathrm{V}(J)\big) \subseteq \mathrm{I}(W)$. Using Corollary 1.0.5, we obtain $\mathrm{V}\big(\mathrm{I}(W)\big) \subseteq \mathrm{V}(J) = \overline{W}$, so we conclude that $\mathrm{V}\big(\mathrm{I}(W)\big) = \overline{W}$.

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

(v) Part (ii) shows that $X = Y$ implies that $\mathrm{I}(X) = \mathrm{I}(Y)$. For any affine subvariety Z, part (iv) proves that $\mathrm{V}\big(\mathrm{I}(Z)\big) = Z$. Thus, Corollary 1.0.5 yields the final statement follows. $\square$

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 $I = \langle x^a \mid a \in \mathcal{A} \rangle$.

A monomial ideal is generated by monomials.

1.1.1 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, if $x^b = \sum_{a \in \mathcal{A}} h_a\, x^a$ where $h_a \in S$ and only finite many of the h_a are nonzero, then every term on the right side is divisible by some $x^a \in I$. Hence, the left side must have the same property. $\square$

1.1.2 Corollary. *Two monomial ideals in S are equal if and only if they contain the same monomials.* $\square$

1.1.3 Lemma. *For any monomial ideal I in S and 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 1.1.1. $\square$

1.1.4 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.*

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.

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 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 $\mathcal{B}$. Since $\mathcal{B}$ is finite, there exists a nonnegative index m such that $\mathcal{B} \subseteq \mathcal{B}_0 \cup \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_m$. It suffices to show that the finite set $\{x^a\, x_n^i \mid x^a \in \mathcal{B}_i \text{ and } 0 \leqslant i \leqslant m\}$ 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 $i \leqslant m$, 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 $j \leqslant m$ and $x^d \in \mathcal{B}_j$ such that x^d divides x^c. Thus, the monomial $x^d\, x_n^j$ divides $x^a\, x_n^i$. $\square$

1.1.5 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 $1 \leqslant i \leqslant n$, we have $x_i > 1_S$.

1.1.6 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.

$x >_{\text{lex}} y^2 >_{\text{lex}} yz >_{\text{lex}} z^{100}$

1.1.7 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 $x^u >_{\text{lex}} x^v$.

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

1.1.8 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.

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

The next result justifies the definition of a monomial ordering.

1.1.9 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 least element);*
(b) *Every decreasing sequence $x^{u_1} > x^{u_2} > x^{u_3} > \cdots$ eventually stabilizes;*
(c) *For all $1 \leqslant i \leqslant n$, 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) ⇒ (b): For any decreasing sequence $x^{u_1} > x^{u_2} > x^{u_3} > \cdots$, the nonempty set $\{u_1, u_2, u_3, \dots\}$ has no smallest element, so the relation $>$ is not a well-order.
(b) ⇒ (c): Suppose that $1 > x_i$ for some $1 \leqslant i \leqslant n$. It follows that, for all $m \in \mathbb{N}$, we have $x_i^m > x_i^{m+1}$, so $1 > x_i > x_i^2 > x_i^3 > \cdots$ is an infinite decreasing sequence.
(c) ⇒ (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 $1 \leqslant i \leqslant n$. It follows that $x^u > x^v$. Since $|v| = |u| - 1$, the induction hypothesis implies that $x^v > 1$.
(d) ⇒ (e): Suppose that $u_i \geqslant v_i$ for all $1 \leqslant i \leqslant n$ and $u \neq v$. Setting $w = u - v$, we have $x^w > 1$ and $x^u = x^w\, x^v > x^v$.
(e) ⇒ (a): Let $\mathcal{M}$ be a nonempty set of monomials. By the Dickson Lemma 1.1.4, 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 $>$. □

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 $f = a_1\, x^{u_1} + a_2\, x^{u_2} + \cdots + a_m\, x^{u_m}$ where and $x^{u_1} > x^{u_2} > \cdots > x^{u_m}$ and $a_1, a_2, \dots, a_m \in \mathbb{K}$. We introduce the following terminology.

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

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 $\operatorname{LM}(f) = x^5$, $\operatorname{LC}(f) = 3$, and $\operatorname{LT}(f) = 3x^5$. Under the graded lexicographic order $>_{\text{grevlex}}$, it follows that $\operatorname{LM}(f) = y^4z^3$, $\operatorname{LC}(f) = 1$, and $\operatorname{LT}(f) = y^4z^3$. $\diamond$

1.2.2 Theorem (Division algorithm)**.** *Fix a monomial order $>$ on S and let $\mathbf{G} := [g_1 \;\; g_2 \;\; \cdots \;\; g_m]^{\mathsf{T}}$ 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 $\langle \operatorname{LM}(g_1), \operatorname{LM}(g_2), \dots, \operatorname{LM}(g_m) \rangle$, and $\operatorname{LM}(f) \geqslant \operatorname{LM}(q_j\, g_j)$ for all $1 \leqslant j \leqslant m$.

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

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 ∈ S and a matrix G := [g_1  g_2  ···  g_m]^T.
output: The reminder r ∈ S and the matrix Q := [q_1  q_2  ···  q_m].
Set (r, p) := (0, f).
For j from 1 to m do set q_j := 0.
While p ≠ 0 do
   i := 1;
   While (i ⩽ m) and LM(g_i) does not divide LM(p) do
      Set i := i + 1.
   If i ⩽ m then (q_i, p) := (q_i + LT(p)/LT(g_i), p − (LT(p)/LT(g_i)) g_i)
      else (r, p) := (r + LT(p), p − 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 $\operatorname{LM}(g_i)$ divides $\operatorname{LM}(p)$, we have

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

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

Since each term added to q_i satisfies $\operatorname{LM}(f) \geqslant \frac{\operatorname{LM}(p)}{\operatorname{LM}(g_i)} \operatorname{LM}(g_i)$, we see that $\operatorname{LM}(f) \geqslant \operatorname{LM}(q_j\, g_j)$ for all $1 \leqslant j \leqslant m$. Similarly, a term $\operatorname{LT}(p)$ is added to r only if the monomial $\operatorname{LM}(p)$ is not divisible by an element of $\{\operatorname{LM}(g_1), \operatorname{LM}(g_2), \dots, \operatorname{LM}(g_m)\}$. 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. □

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 $[x \;\; y]^{\mathsf{T}}$, the division algorithm gives $f = (x^2 + 1)x + (y + 1)y + 2z^2 + 1$. ◇

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

In general, the reminder 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*** $\operatorname{LT}(I)$ is the monomial ideal generated by the leading terms of all elements in the ideal I, so we have $\operatorname{LT}(I) := \langle \operatorname{LT}(f) \mid f \in I \rangle$.

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 $\langle x^2, xy \rangle \subseteq \operatorname{LT}(I)$. The equation $x(xy - x) + (1 - y)(x^2 - y) = y^2 - y \in I$ also shows that $y^2 \in \operatorname{LT}(I)$. How can one verify that $\operatorname{LT}(I) = \langle x^2, xy, y^2 \rangle$? ◇

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

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

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

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. ◇

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 $\operatorname{LT}(I)$ is generated by the monomials $\operatorname{LM}(f)$ for all $f \in I$. The Dickson Lemma 1.1.4 shows that $\operatorname{LT}(I)$ is finitely generated. It follows that there are $g_1, g_2, \dots, g_m \in I$ such that $\operatorname{LT}(I) = \langle \operatorname{LM}(g_1), \operatorname{LM}(g_2), \dots, \operatorname{LM}(g_m) \rangle$. The polynomials $g_1, g_2, \dots, g_m$ form a Gröbner basis for I. □