WORKSHEET 1.3: GRÖBNER BASES PT. I

Polynomial Division. Recall the following classical theorem:

Theorem 1. *Let $g \in \mathbb{K}[x]$ be a non-zero polynomial. Every polynomial $f \in \mathbb{K}[x]$ can be written uniquely as $f = qg + r$ where $q, r \in \mathbb{K}[x]$, and either $r = 0$ or $\deg(r) < \deg(g)$.*

While this theorem might seem innocuous when first learned as a teenager, it turns out to be very powerful when studying ideals and polynomials in $\mathbb{K}[x]$. The proof of this theorem also provides an algorithm for computing q and r, which when presented in pseudocode looks something like

Algorithm 1 Division Algorithm

Require: g, f
Ensure: q, r
  $q \leftarrow 0$; $r \leftarrow f$
  while $r \neq 0$ **and** $\mathrm{LT}(g)$ divides $\mathrm{LT}(r)$ **do**
    $q \leftarrow q + \mathrm{LT}(r)/\mathrm{LT}(g)$
    $r \leftarrow r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$
  end while

The goal of this worksheet is to begin exploring how we might extend this theorem to polynomial rings in more variables. Along the way we will see how these explorations will lead to both computational tools for studying the commutative algebra of polynomial rings over fields, but also gives us useful tools for proving theorems in this setting as well.

---

(1) Use Theorem 1 to prove the following:

  (a) If $f \in \mathbb{K}[x]$ is a non-zero polynomial then f has at most $\deg(f)$ roots in $\mathbb{K}$.

  (b) If $g \in \mathbb{K}[x]$ is a non-zero polynomial then $f \in \langle g \rangle$ if and only if $r = 0$.

(2) Implement the algorithm above in Macaulay2, and use your code to compute q and r for the following polynomials. (If you want to test your code versus the built-in functions use `time f//g` and `time f%g` to compute q and r respectively and time the computation.)

  (a) $f = x^3 + x + 1, \quad g = x + 1.$

  (b) $f = x^5 - 1, \quad g = x - 1.$

  (c) $f = x^2 + 1, \quad g = x^3 + x.$

  (d) $f = x^{100} - 1, \quad g = x^2 - 1.$

  (e) $f = x^{1000} - 1, \quad g = x - 1.$

  (f) $f = \sum_{i=0}^{500} x^i, \quad g = x^2 + x + 1.$

The computations in Question (2) are deliberately familiar: in one variable division works because there is a canonical notion of "largest term," namely highest degree. In several variables there is no such natural choice. To imitate the division algorithm we must first choose an ordering on monomials, and the next questions explain exactly what properties that ordering must satisfy.

Definition 2. A monomial ordering on $\mathbb{K}[x_1,\dots,x_n]$ is a relation $<$ on $\mathbb{Z}^n_{\geq 0}$ satisfying the following:

(i) $<$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$,

(ii) if $\alpha < \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$ then $\alpha+\gamma < \beta+\gamma$, and

(iii) $<$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$.

Recall that a *total ordering* means that of any two elements $\alpha,\beta \in \mathbb{Z}^n_{\geq 0}$ exactly one of the following statements is true: $\alpha<\beta$, $\alpha=\beta$, or $\beta<\alpha$. That $<$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$ means that every non-empty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element with respect to $<$.

Once a monomial ordering has been fixed, every non-zero polynomial acquires a distinguished piece of data: its leading monomial, leading coefficient, and leading term. These are the ingredients that drive the multivariable division process just as degree and leading coefficient drive ordinary polynomial division.

---

(3) Prove that a monomial ordering $<$ on $\mathbb{Z}^n_{\geq 0}$ is equivalent to a relation $<$ on the set of monomials in $\mathbb{K}[x_1,\dots,x_n]$ satisfying analogous conditions to (i), (ii), and (iii) above. Explain why this justifies the moniker "monomial ordering".

(4) Prove or disprove that the following are monomial orderings:

(a) Lexicographic (Lex) Order: Given $\alpha=(\alpha_1,\dots,\alpha_n)$ and $\beta=(\beta_1,\dots,\beta_n)$ in $\mathbb{Z}^n_{\geq 0}$ we say $\beta <_{\text{lex}} \alpha$ if and only if the left-most non-zero entry of $\alpha-\beta$ is positive.

(b) Graded Lex Order: With α and β as in (a) we say that $\beta <_{\text{grlex}} \alpha$ if and only if

$$|\beta| := \sum_{i=1}^n \beta_i < |\alpha| = \sum_{i=1}^n \alpha_i \qquad \text{or} \qquad |\beta| = |\alpha| \text{ and } \beta <_{\text{lex}} \alpha.$$

(c) Reverse Lex (RevLex) Order: With α and β as in (a) we say that $\beta <_{\text{revlex}} \alpha$ if and only if the right-most non-zero entry of $\alpha-\beta$ is negative.

(d) Graded RevLex Order: With α and β as in (a) we say that $\beta <_{\text{grevlex}} \alpha$ if and only if

$$|\beta| := \sum_{i=1}^n \beta_i < |\alpha| = \sum_{i=1}^n \alpha_i \qquad \text{or} \qquad |\beta| = |\alpha| \text{ and } \beta <_{\text{revlex}} \alpha.$$

(e) Weight Order: Fix a vector $w = (w_1, \ldots, w_n) \in \mathbb{Z}^n$. With α and β as in (a) say $\beta <_w \alpha$ if and only if

$$\beta \cdot w = \sum_{i=1}^{n} \beta_i w_i < \alpha \cdot w = \sum_{i=1}^{n} \alpha_i w_i$$

(5) **Leading Terms.** Fix a monomial ordering $<$ on $\mathbb{Z}^n_{\geq 0}$, and use the corresponding ordering on monomials in $\mathbb{K}[x_1, \ldots, x_n]$. Let $f = \sum_\alpha c_\alpha x^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ be a non-zero polynomial. Define the *leading monomial* $\mathrm{LM}(f)$, *leading coefficient* $\mathrm{LC}(f)$, and *leading term* $\mathrm{LT}(f)$ with respect to the fixed monomial ordering.

(a) Compute $\mathrm{LM}(f)$, $\mathrm{LC}(f)$, and $\mathrm{LT}(f)$ for

$$f = x^3 + 3x^2y + 5xy^3 - 7z^2 \in \mathbb{K}[x, y, z]$$

with respect to Lex, Graded Lex, and Graded RevLex orderings (assume $x > y > z$).

(b) Prove that if $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ are non-zero, then

$$\mathrm{LM}(fg) = \mathrm{LM}(f)\,\mathrm{LM}(g) \qquad \text{and} \qquad \mathrm{LT}(fg) = \mathrm{LT}(f)\,\mathrm{LT}(g).$$

(c) Explain which property of a monomial ordering is used in part (b).

(6) Let $G = (g_1, \ldots, g_s)$ be an ordered list of non-zero polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.

(a) Write pseudocode for a division algorithm which takes as input f and G and returns polynomials $q_1, \ldots, q_s, r$ such that $f = q_1 g_1 + \cdots + q_s g_s + r$, where no monomial appearing in r is divisible by any of the monomials $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$.

(b) In the algorithm above, what should happen if the leading monomial of the current polynomial is not divisible by any $\mathrm{LM}(g_i)$?

(c) Prove that your algorithm terminates. What plays the role of "degree" in the proof of termination?

(7) Work in $\mathbb{K}[x, y]$ with Lex order and $x > y$. Let $= xy^2 - x$, $g_1 = xy - 1$, and $g_2 = y^2 - 1$.

(a) Divide f by the ordered list (g_1, g_2).

(b) Divide f by the ordered list (g_2, g_1).

(c) Show directly that $f \in \langle g_1, g_2 \rangle$.

(d) What do your computations show about division in several variables? In particular, is the remainder uniquely determined by the ideal $\langle g_1, g_2 \rangle$?

Question 7 shows the central obstacle in several variables: ordinary division is no longer canonical, so ideal membership cannot be read off from a unique remainder. In several variables, a zero remainder of f divided by $g_1, \ldots, g_s$ implies that $f \in \langle g_1, \ldots, g_s \rangle$, but a non-zero remainder does not rule out ideal membership. Fixing this will led to the theory of Gröbner bases, which we shall see later in the course.
