Lesson 6 – Polynomials in One Variable

Our goal in the coming week is to develop a division algorithm for sets of multivariate polynomials. While today's lesson is largely a review of material you have seen in previous algebra courses (and I apologize for this), I feel the review is necessary for two reasons:

1. It's easier to understand the generalization of a process that is fresh in one's mind.
2. It will be very helpful to look at the one variable division algorithm *with the multivariate situation in mind*. In particular, we will define some notation and groundwork that will serve us well next lesson.

So bear with me!

I. The Division Algorithm in $\boldsymbol{k[x]}$

Given a nonzero polynomial $f \in k[x]$, recall that the **degree** of f is the largest power of x appearing in f. The **leading term**, $\mathrm{LT}(f)$, is that term of f of highest degree, and the **leading coefficient** $\mathrm{LC}(f)$ is the coefficient of $\mathrm{LT}(f)$.

Recall how we divide polynomials of one variable using the Division Algorithm:

Exercise 1 Find the quotient and remainder in $\mathbb{Q}[x]$ when dividing $f(x) = x^3 - 2x^2 + 2x + 8$ by $g(x) = 2x^2 + 3x + 1$.

Observe that the first step of the process focused on the leading terms of the polynomials f and g. In particular, we computed the polynomial: $f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} g$. This process was then applied again to $f_{new} = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} g$, so that step 2 of the algorithm yields the reduction $f_{new} - \frac{\mathrm{LT}(f_{new})}{\mathrm{LT}(g)} g$.

Definition (Reduction) We will say a polynomial h is a **reduction of $\boldsymbol{f}$ by $\boldsymbol{g}$** if

$$h = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} g.$$

If h is a reduction of f by g, we write: $f \xrightarrow{g} h$.

Repeated reductions, such as $f \xrightarrow{g} h \xrightarrow{g} r$, are denoted by $f \xrightarrow{g}_{+} r$.

As I said, our end goal is to generalize this process to sets of multivariate polynomials. We will use the single variable case as a guide.

Theorem (The Division Algorithm) Given $g \in k[x]$, $g \neq 0$ and $f \in k[x]$, there exist $q, r \in k[x]$, such that $f = qg + r$ with $\deg(r) < \deg(g)$ or $r = 0$. Moreover, q and r are unique.

Quick Sketch of Existence Proof

As the above Theorem states, if f, g are polynomials in $k[x]$, where k is a field, then we will be able to continually reduce f by g until we get to a reduction r having degree smaller than $\deg(g)$. In particular, the function $\deg: k[x] \to \mathbb{Z}_{\geq 0}$ is a Euclidean function and the existence of the Division Algorithm in $k[x]$ makes the polynomial ring a Euclidean Domain.

II. Important Consequences of the Division Algorithm:

Theorem ($k[x]$ is a PID) Every ideal of $k[x]$ is generated by a single polynomial (which is unique up to a constant multiple).

Proof.

Exercise 2 What does the previous theorem say about $I = \langle x^3 - 3x + 2, x^2 - 1\rangle \subseteq \mathbb{Q}[x]$?

Exercise 3 Is $f(x) = x - \frac{1}{2}$ an element of the ideal $I = \langle x^3 - 3x + 2, x^2 - 1\rangle$?

Question: As the previous exercise illustrates, it is easy to determine "ideal membership" when the ideal consists of polynomials of one variable. If $I = \langle f_1, f_2, \ldots, f_s\rangle = \langle f\rangle \subseteq k[x]$ is a nonzero ideal, then $g \in I$ iff $f|g$. So for a given an ideal $I = \langle f_1, f_2, \ldots, f_s\rangle$, how are we to arrive at the unique (up to constant multiple) generator f?

Definition. Given two polynomials $f_1, f_2 \in k[x]$, the **greatest common divisor**, $\mathrm{GCD}(f_1, f_2)$, is defined to be the polynomial g satisfying:

- g divides f_1 and f_2
- if h divides f_1, f_2 then h divides g
- $\mathrm{LC}(g) = 1$ (g is monic)

Theorem If $f_1, f_2 \in k[x]$ are not both zero, then $\mathrm{GCD}(f_1, f_2)$ exists and $I = \langle f_1, f_2 \rangle = \langle \mathrm{GCD}(f_1, f_2) \rangle$.

What we need is an algorithm for finding GCDs. This is the well known Euclidean algorithm.

The Euclidean Algorithm. Given $f_1, f_2 \in k[x]$,

- **INITIAL VALUES:** $f := f_1, g := f_2$.
- **ALGORITHM:** While $g \neq 0$

$$f \xrightarrow{g}_+ r$$

$$f := g$$
$$g := r$$

- $f := \frac{1}{\mathrm{LC}(f)} f$

Exercise 4 Use the Euclidean Algorithm to find the GCD of $f_1 = x^3 - 3x + 2$ and $f_2 = x^2 - 1$.

Solution:

$$f_1 = x^3 - 3x + 2 = x(x^2 - 1) + (-2x + 2)$$

$$x^2 - 1 = -\frac{1}{2}x(-2x + 2) + 0$$

$$f := (-2x + 2)$$

$$\mathrm{GCD}(x^3 - 3x + 2, x^2 - 1) = -\frac{1}{2}(-2x + 2) = x - 1.$$

III. What they should have told you in Linear Algebra

Having explored division for polynomials of one variable, we next consider multivariate polynomials. One situation where division arises is in the solution of linear equations, though this might not be immediately obvious. Let's work through a couple of examples from linear algebra:

Exercise 5

a) Employ row reduction on the coefficient matrix of the following system of linear equations and use it to describe the solution set $\mathbf{V}(f_1, f_2)$.

$$f_1 = x + y - z = 0$$
$$f_2 = 2x + 3y + 2z = 0.$$

b) The above simplification process was a matter of deciding how to combine rows to eliminate variables. I claim there is division going on though. Where is the division?

Exercise 6 Suppose you want to solve the system of equations:

$$\begin{aligned} g_1 &= x + 2y + 3z = 0 \\ g_2 &= \quad\;\; y - z = 0 \\ g_3 &= 3x - 4y + 2z = 0 \end{aligned}$$

Row reduction yields:

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & -1 \\ 3 & -4 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & -1 \\ 0 & -10 & -7 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & -1 \\ 0 & 0 & -17 \end{bmatrix}$$

a) Describe this row reduction using the "reduction of f by g" notation: $f \xrightarrow{g} h$.

b) Now describe this row reduction process using the language of quotient rings.

c) One last question...did the order of the variables matter in the above computation? That is, had we chosen to apply row reduction to the equations in the form

$$\begin{aligned} g_1 &= 3z + 2y + x = 0 \\ g_2 &= -z + y \quad\;\; = 0 \\ g_3 &= 2z - 4y + 3x = 0 \end{aligned}$$

would it have made any difference to the resulting quotient ring?