WORKSHEET 3.1: GRÖBNER BASES PT. II

Fix a field $\mathbb{K}$. Unless otherwise specified the ring throughout this worksheet will be $\mathbb{K}[x_1,\ldots,x_n]$. In the previous worksheet we introduced monomial orderings and leading terms. In this worksheet we return to the multivariable division algorithm, and then use it to study monomial ideals, initial ideals, and Gröbner bases. The main goal is to push the story all the way to a major finiteness theorem: every ideal of $\mathbb{K}[x_1,\ldots,x_n]$ is finitely generated.

Recall a *monomial ordering* on $\mathbb{K}[x_1,\ldots,x_n]$ is a total well-ordering $<$ on $\mathbb{Z}^n_{\geq 0}$ such that if $\alpha < \beta$ then $\alpha+\gamma < \beta+\gamma$ for all $\gamma \in \mathbb{Z}^n_{\geq 0}$. Using the bijection between monomials in $\mathbb{K}[x_1,\ldots,x_n]$ and elements of $\mathbb{Z}^n_{\geq 0}$ we think of a monomial ordering as giving us a way to compare monomials by saying $x^\alpha < x^\beta$ if and only if $\alpha < \beta$. In Worksheet 1.3 we saw several important monomial orders: lexicographic (lex) order, graded lexicographic (grlex) order, and graded reverse lexicographic (grevlex) order. Please review that worksheet for their definitions.

Returning to our goal of having a division algorithm in $\mathbb{K}[x_1,\ldots,x_n]$ we are faced with two challenges compared to the familiar setting of $\mathbb{K}[x]$:

(i) In several variables the notion of "leading term" is ambiguous. In one variable, the leading term is simply the term of highest degree. In several variables this no longer suffices: for instance, what should the leading term of x^2+xy+y^2 be? All three terms have total degree 2.

(ii) We want a division algorithm that can answer questions about ideals, i.e., membership, intersections, sums, products, radicals. In $\mathbb{K}[x]$ every ideal is principal, so dividing by a single generator is enough. For $n>1$, however, $\mathbb{K}[x_1,\ldots,x_n]$ is no longer a PID, so ideals generally require multiple generators. We therefore need a way to divide a polynomial by an entire *list* of polynomials.

As seen on Worksheet 1.3, once a monomial ordering has been fixed, we give a meaningful definition of leading term, leading monomial, and leading coefficient; solving issue (i). Note while we normally write $\mathrm{LT}(f)$, $\mathrm{LM}(f)$ and $\mathrm{LC}(f)$ for these quantities; they do depend on the chosen order $<$, and so would more properly be called $\mathrm{LT}_<(f)$, $\mathrm{LM}_<(f)$ and $\mathrm{LC}_<(f)$ to highlight this fact.

To resolve issue (ii), we generalize long division as follows. In single-variable polynomial long division, we repeatedly ask: "Does the leading term of the divisor divide the current leading term of the dividend?" If yes, we subtract off the appropriate multiple; if not, we are done. The multivariable algorithm works the same way, except that instead of checking a single divisor we scan through an *ordered* list of divisors $G=(g_1,\ldots,g_s)$ and use the first one whose leading term divides the current leading term. More precisely, the algorithm maintains a "working polynomial" p (initialized to f), quotients $q_1,\ldots,q_s$ (initialized to 0), and a remainder r (initialized to 0), then repeats:

- **Try to Divide.** Walk through the list $g_1, g_2, \ldots, g_s$ in order. If you find some g_i whose leading term $\mathrm{LT}(g_i)$ divides $\mathrm{LT}(p)$, subtract the appropriate multiple: update $q_i \leftarrow q_i + \mathrm{LT}(p)/\mathrm{LT}(g_i)$ and $p \leftarrow p - (\mathrm{LT}(p)/\mathrm{LT}(g_i))g_i$. Then return to the start of the list and try again with the new p.
- **Move to Remainder.** If *no* g_i in the list has a leading term dividing $\mathrm{LT}(p)$, then the current leading term of p cannot be reduced further. Move it to the remainder: $r \leftarrow r + \mathrm{LT}(p)$ and $p \leftarrow p - \mathrm{LT}(p)$.

We continue until the working polynomial p is equal to 0. Proving this algorithm terminates as expected, which you will do later in this worksheet, amounts essentially to proving the following theorem

Theorem 1. *Fix a monomial ordering $<$ on $\mathbb{K}[x_1, \ldots, x_n]$ and let $G = (g_1, \ldots, g_s)$ be an ordered list of nonzero polynomials. If $f \in \mathbb{K}[x_1, \ldots, x_n]$ then there exist $q_1, \ldots, q_s, r \in \mathbb{K}[x_1, \ldots, x_n]$ such that*

$$f = q_1 g_1 + \cdots + q_s g_s + r,$$

where no monomial appearing in r is divisible by any of $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$.

Written in pseudocode the algorithm for multivariable polynomial division is shown below.

Algorithm 1 Division by an ordered list $G = (g_1, \ldots, g_s)$

Require: $f, g_1, \ldots, g_s$
Ensure: $q_1, \ldots, q_s, r$
  $q_1, \ldots, q_s \leftarrow 0$; $r \leftarrow 0$; $p \leftarrow f$
  while $p \neq 0$ **do**
    divides $\leftarrow 0$
    for $i = 1, \ldots, s$ **do**
      if $\mathrm{LT}(g_i)$ divides $\mathrm{LT}(p)$ **then**
        $q_i \leftarrow q_i + \mathrm{LT}(p)/\mathrm{LT}(g_i)$
        $p \leftarrow p - (\mathrm{LT}(p)/\mathrm{LT}(g_i))g_i$
        divides $\leftarrow 1$
        break
      end if
    end for
    if divides $= 0$ **then**
      $r \leftarrow r + \mathrm{LT}(p)$
      $p \leftarrow p - \mathrm{LT}(p)$
    end if
  end while

(1) **Review of Monomial Orders.** Work in $\mathbb{K}[x, y, z]$ and assume $x > y > z$.

(a) Order the monomials x^2y, xy^2, xz^2, y^3, yz^4 from largest to smallest with respect to lex, graded lex, and graded reverse lex.

(b) Compute LM(f), LC(f), and LT(f) for $f = 4x^2y - 3xy^2 + y^4 + 2z^5$ with respect to lex and grevlex.

(c) Prove that 1 is the smallest monomial for every monomial ordering.

(d) Deduce that every strictly decreasing sequence of monomials terminates.

(e) Explain why part (d) should make you optimistic that a division algorithm might terminate.

(2) **Examples of Multivariable Division.** For this question, we will work in $\mathbb{K}[x,y]$ considered with the lex order where $x > y$.

(a) Divide $f = x^2y + xy + y - x - 2$ by the ordered list $G = (xy-1, y-1)$. Record the successive values of p, the quotients, and the remainder after each update.

(b) Divide $f = xy^2 - x$ by the ordered list $G = (xy-1,\ y^2-1)$. Record the successive values of p, the quotients, and the remainder after each update.

(c) Repeat (b), but with the ordered list $(y^2-1,\ xy-1)$, i.e. where the order of G is swapped.

(d) Show directly that $xy^2 - x \in \langle xy-1, y^2-1\rangle$.

(e) What do your computations show about division in several variables? In particular, what is always true when the remainder is 0, and what can go wrong when the remainder is non-zero?

(3) **Termination of Division Algorithm** Let $G = (g_1,\ldots,g_s)$ be an ordered list of non-zero polynomials.

(a) Show that throughout the algorithm one always has $f = q_1g_1 + \cdots + q_sg_s + p + r$.

(b) Show that after each pass through the `while` loop, the leading monomial of p strictly decreases with respect to the given monomial order.

(c) Use Question 1(d) to prove that the algorithm terminates.

(d) Prove that on termination the output satisfies $f = q_1g_1 + \cdots + q_sg_s + r$, and no monomial appearing in r is divisible by any of $\mathrm{LM}(g_1),\ldots,\mathrm{LM}(g_s)$.

(e) Explain why a zero remainder certifies ideal membership: if dividing f by G produces remainder 0, then $f \in \langle g_1,\ldots,g_s\rangle$.

Question 2 reveals an important new feature of polynomial division in several variables. Unlike the one-variable case, the remainder obtained by dividing a polynomial f by polynomials $g_1,\ldots,g_t$ depends on two choices: i) the order of our list of divisors and ii) the monomial order we have fixed. Because of this, division does *not* immediately solve the ideal membership problem in several variables. In other words, even if dividing f by the list $(g_1,\ldots,g_t)$ produces a nonzero remainder, it may still happen that $f \in \langle g_1,\ldots,g_t\rangle$. So, in several variables, a nonzero remainder does *not* by itself show that $f \notin \langle g_1,\ldots,g_t\rangle$.

We will eventually develop a way to fix this problem. Before we do, however, it is useful to study a special class of ideals for which ideal membership *is* controlled purely by divisibility of monomials.

Definition 2. An ideal $I \subseteq \mathbb{K}[x_1,\dots,x_n]$ is a *monomial ideal* if it can be generated by monomials.

We shall see shortly that a monomial ideal is entirely determined by the set of monomials belonging to the ideal. Since monomials in $\mathbb{K}[x_1,\dots,x_n]$ are in bijection with $\mathbb{Z}^n_{\geq 0}$ this means we can – and often do think of monomial ideals as corresponding to subsets of $\mathbb{Z}^n_{\geq 0}$. With this viewpoint, the following classical result guarantees that monomial ideals are well-behaved.

Theorem 3 (Dickson's Lemma)**.** *Every subset of $\mathbb{Z}^n_{\geq 0}$ has only finitely many minimal elements with respect to the coordinatewise order $\leq$.*

Motivated by this theorem we say a *minimal monomial generating set* for a monomial ideal I is a finite set of monomials $\{m_1,\dots,m_t\}$ such that $I = \langle m_1,\dots,m_t\rangle$ and no m_i divides m_j for $i \neq j$. Equivalently, no generator is redundant: removing any m_i from the set yields a strictly smaller ideal.

---

(4) **Properties of Monomial Ideals.**

(a) Decide which of the following ideals are monomial ideals:

$$\langle x^2, xy^3, z\rangle, \qquad \langle x+y, y^2\rangle, \qquad \langle x^2-y, y^3\rangle, \qquad \langle x^2, xy, y^4+x\rangle.$$

(b) Let $m_1,\dots,m_t$ and m be monomials. Prove that $m \in \langle m_1,\dots,m_t\rangle$ if and only if $m_i \mid m$ for some i.

(c) Deduce that a polynomial $f \in \mathbb{K}[x_1,\dots,x_n]$ lies in I if and only if every monomial appearing in f is divisible by one of $m_1,\dots,m_t$.

(d) Find a minimal monomial generating set for each of the following ideals:

$$J = \langle x^3,\, x^2y,\, xy^2,\, y^4,\, x^4y,\, x^2y^3\rangle \qquad \text{and} \qquad L = \langle x^2z,\, xyz,\, y^2z,\, z^3,\, xz^4\rangle.$$

Draw a picture of the subset of $\mathbb{Z}^2_{\geq 0}$ corresponding to the monomials in J.

(5) **Understanding Dickson's Lemma.**

(a) Let $A \subseteq \mathbb{Z}^n_{\geq 0}$ and set $I_A := \langle x^\alpha \mid \alpha \in A\rangle$. If $A_{\min}$ denotes the set of minimal elements of A, show that every monomial in I_A is divisible by some x^α with $\alpha \in A_{\min}$.

(b) Explain why the statement "every subset of $\mathbb{Z}^n_{\geq 0}$ has finitely many minimal elements with respect to $\leq$" is equivalent to the statement "every monomial ideal in $\mathbb{K}[x_1,\dots,x_n]$ is finitely generated."

(c) Restate Dickson's Lemma entirely in terms of monomial ideals in $\mathbb{K}[x_1,\dots,x_n]$.

(d) Prove your monomial ideal version of Dickson's Lemma in the case when $n = 1$.

(6) **Proving Dickson's Lemma.** We now prove the monomial ideal version of Dickson's Lemma by induction on the number of variables. Your work in Question 5d serves as the base case. Assume Dickson's Lemma holds in $n-1$ variables. Let $I \subseteq \mathbb{K}[x_1,\dots,x_n]$ be a monomial ideal. For $k \geq 0$ let

$$J_k = \left\{ f \in \mathbb{K}[x_1,\dots,x_{n-1}] \;\middle|\; f x_n^k \in I \right\} \cup \{0\}.$$

(a) Prove that J_k is a monomial ideal in $\mathbb{K}[x_1,\dots,x_{n-1}]$ for all $k \geq 0$.

(b) Show that the J_k form an ascending chain.

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots.$$

(Hint: What happens when you multiply something in J_k by x_n?)

(c) Let $L = \bigcup_{d \geq 0} J_d$. Show that L is a monomial ideal in $\mathbb{K}[x_1,\dots,x_{n-1}]$.

(d) Prove that there exists $N \in \mathbb{Z}_{\geq 0}$ such that $L = J_k$ for all $k \geq N$. (Hint: Use the inductive hypothesis to show that L is finitely generated.)

(e) For each $0 \leq k \leq N$, choose monomial generators $m_{k,1},\dots,m_{k,r_k}$ for J_k. Via the inclusion $\mathbb{K}[x_1,\dots,x_{n-1}] \subset \mathbb{K}[x_1,\dots,x_n]$ view these as elements in $\mathbb{K}[x_1,\dots,x_n]$. Prove that I is generated by the finite set

$$\left\{ m_{k,i} x_n^k \;\middle|\; 0 \leq k \leq N,\ 1 \leq i \leq r_k \right\}.$$

(f) Conclude Dickson's Lemma for all n.

(7) **Minimal monomial generators.** Let I be a monomial ideal, and let $M(I)$ be the set of monomials in I which are minimal under divisibility.

(a) Use Dickson's Lemma to show that $M(I)$ is finite.

(b) Prove that $I = \langle M(I) \rangle$.

(c) Prove that every monomial generating set of I contains $M(I)$. Conclude that $M(I)$ is the unique minimal monomial generating set of I.

Monomial ideals are easier to study because membership is determined entirely by divisibility of monomials, and Dickson's Lemma gives strong finiteness properties. For a general ideal, we would like to recover similar structures by extracting the leading term of each polynomial. This leads to the following.

Definition 4. Let $<$ be a monomial order on $\mathbb{K}[x_1,\dots,x_n]$. The *initial ideal* of a nonzero ideal $I \subset \mathbb{K}[x_1,\dots,x_n]$ with respect to $<$ is:

$$\mathrm{in}_<(I) := \langle \mathrm{LT}(f) \;\middle|\; f \in I \rangle.$$

A finite subset $\mathcal{G} = \{g_1,\dots,g_s\} \subset I$ is a *Gröbner basis* for I with respect to $<$ if $\mathrm{in}_<(I) = \langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s) \rangle$.

It is standard to set $\text{in}_<(\langle 0 \rangle) = \langle 0 \rangle$. Note a priori there is no reason for Gröbner bases to exist in general or be interesting. In the next few exercises you will show that Dickson's Lemma not only implies that Gröbner bases exist, but also they will give an answer to the ideal membership problem.

---

(8) **Initial Ideals of Monomial Ideals.** Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be a monomial ideal. Prove that $\text{in}_<(I) = I$ for every monomial order $<$.

(9) For this problem consider $\mathbb{K}[x, y]$ with the lex order where $x > y$. Let $I = \langle xy - 1, y^2 - 1 \rangle$.

(a) Find explicit generators for the ideal generated by the leading terms of $xy - 1$ and $y^2 - 1$.

(b) Prove that $\{xy - 1, y^2 - 1\}$ is not a Gröbner basis for I by finding an element in I not contained in the ideal computed in 9a. (Hint: Consider the element $x - y$.)

(c) Use *Macaulay2* to find a Gröbner basis for I.

(10) **Existence of Gröbner Bases.** Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and $<$ be a monomial order.

(a) Show that $\text{in}_<(I)$ is a monomial ideal.

(b) By Dickson's Lemma, $\text{in}_<(I) = \langle m_1, \ldots, m_t \rangle$ for a minimal monomial generating set $m_1, \ldots, m_t$. Show that there exist elements $g_1, \ldots, g_t \in I$ such that $\text{LT}(g_i)$ divides m_i for all i.

(c) Show that the minimality of $m_1, \ldots, m_t$ implies $\text{LT}(g_i) = c_i m_i$ for some scalar $c_i \in \mathbb{K}^\times$

(d) Conclude that $\mathcal{G} = \{g_1, \ldots, g_t\}$ is a Gröbner basis of I.

(11) **Ideal Membership & Gröbner Bases.** Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and $<$ be a monomial order. Fix a Gröbner basis $G = (g_1, \ldots, g_t)$ for I, i.e. elements $g_i \in I$ such that $m_i := \text{LT}(g_i)$ generate $\text{in}_<(I)$.

(a) Given $f \in \mathbb{K}[x_1, \ldots, x_n]$ consider the division of f by $\mathcal{G} = (g_1, \ldots, g_t)$ obtaining

$$f = q_1 g_1 + \cdots + q_t g_t + r,$$

as in Theorem 1. Show that $f \in I$ if and only if $r \in I$.

(b) Assume $f \in I$ and $r \neq 0$. Show that $\text{LT}(r) \in \text{in}_<(I)$, and conclude $\text{LT}(r)$ is divisible by one of $m_1, \ldots, m_t$. Why does this contradict the defining property of the remainder? Conclude that every $f \in I$ has remainder 0 on division by G.

(c) Membership Test. Prove that if $\mathcal{G}$ is a Gröbner basis for I, then for any polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$

$$f \in I \iff \text{the remainder on dividing } f \text{ by } \mathcal{G} \text{ is } 0.$$

(d) Prove that $I = \langle g_1, \ldots, g_t \rangle$. (Hint: The inclusion $\langle g_1, \ldots, g_t \rangle \subset I$ should be clear. For the other, let $f \in I$ then apply the division algorithm and the membership test.)

Notice that Questions 10 and 11 together show; given any ideal $I \subseteq \mathbb{K}[x_1,\ldots,x_n]$ and any monomial order $<$, a Gröbner basis for I exists (Question 10), and every Gröbner basis generates I (Question 11(d)). Since a Gröbner basis is finite by construction, every ideal of $\mathbb{K}[x_1,\ldots,x_n]$ is finitely generated. This naturally leads us to our first encounter with the following important finiteness condition.

Definition 5. A ring R is *Noetherian* if and only if every ascending chain of ideals:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stabilizes in the sense that there exists $N \in \mathbb{Z}_{\geq 1}$ such that $I_n = I_{n+1}$ for all $n \geq N$.

It is common to say a ring is Noetherian if it has the ACC property where ACC is short for ascending chain condition. You will show below a ring R being Noetherian is equivalent to every ideal of R being finitely generated. Thus, you have proven that $\mathbb{K}[x_1,\ldots,x_n]$ is Noetherian. Since a field $\mathbb{K}$ is Noetherian, you have actually proven a special, but important case of the following theorem.

Theorem 6 (Hilbert's Basis Theorem)**.** *Let R be a ring. If R is Noetherian, then $R[x]$ is Noetherian.*

The remainder of this worksheet is devoted to proving the equivalence between the ACC and finite generation of ideals, and proving Hilbert's basis theorem in general.

---

(12) **Properties of Noetherian Rings.** For this question let R be any commutative ring, and consider an ascending chain of ideals in R:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots.$$

(a) Show that $J = \bigcup_{k\geq 1} I_k$ is an ideal of R.

(b) If J is finitely generated, say $J = \langle a_1,\ldots,a_t\rangle$, explain why there exists an integer $N \in \mathbb{Z}_{\geq 1}$ such that $a_1,\ldots,a_t \in I_N$. Conclude that the chain of ideals stabilizes.

(c) Explain why you just showed that if every ideal of R is finitely generated then R is Noetherian.

(d) Let I be an ideal of R and suppose every ascending chain of ideals in R stabilizes. Pick any $a_1 \in I$. If $\langle a_1\rangle \neq I$, pick $a_2 \in I \setminus \langle a_1\rangle$, obtaining $\langle a_1\rangle \subsetneq \langle a_1, a_2\rangle$. Continue in this way. Use the ascending chain condition to show this process must terminate, and conclude that I is finitely generated.

(e) Show that if R is Noetherian and $I \subseteq R$ is an ideal, then R/I is Noetherian.

(13) **Hilbert's Basis Theorem.** Let R be a Noetherian ring, and let $I \subseteq R[x]$ be an ideal. For $k \in \mathbb{Z}_{\geq 0}$, define

$$J_k := \left\{ a \in R \;\middle|\; \begin{array}{c}\text{there exists } f \in I \\ \mathrm{LT}(f) = ax^k\end{array} \right\} \cup \{0\}.$$

Equivalently, $a \in J_k$ if and only if there exists $f \in I$ with $\mathrm{LT}(f) = ax^k$ (or $a = 0$). Thus J_k is the set of all leading coefficients of polynomials of degree k in I, together with 0. Note that we are viewing

$R[x]$ as a polynomial ring in the single variable x over R. We define the leading term of a polynomial $f = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ (with $a_k \neq 0$) to be $\mathrm{LT}(f) = a_k x^k$.

(a) Show that J_k is an ideal of R for all $k \geq 0$.

(b) Show that the J_k form an ascending chain $J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots$.

(c) Let $L = \bigcup_{d \geq 0} J_d$. Show that L is an ideal in R.

(d) Prove that there exists $N \in \mathbb{Z}_{\geq 0}$ such that $L = J_k$ for all $k \geq N$. (Hint: Use that R is Noetherian.)

For each $0 \leq k \leq N$, choose generators $a_{k,1}, \ldots, a_{k,r_k}$ for J_k and polynomials $f_{k,i} \in I$ such that $\mathrm{LT}(f_{k,i}) = a_{k,i}x^k$. We will now show that I is equal to

$$M := \left\langle f_{k,i} \;\middle|\; 0 \leq k \leq N,\ 1 \leq i \leq r_k \right\rangle.$$

The inclusion $M \subset I$ is clear. We prove the reverse inclusion $I \subseteq M$ by induction on degree. For the base case suppose $g \in I$ and $\deg(g) = 0$. Since $g \in I$ and $\mathrm{LT}(g) = cx^0 = c$, we have $c \in J_0$. Using that $J_0 = \langle a_{0,1}, \ldots, a_{0,r_0} \rangle$ we may write c as $c = b_i a_{0,} + \cdots b_{r_0} a_{0,r_0}$ with $b_i \in R$. For each i we have $\mathrm{LT}(f_{0,i}) = a_{0,i}x^0 = a_{0,i}$ so $f_{0,i} = a_{0,i}$. Hence $a_{0,i}$ is in M for all i implying $g \in M$ proving the base case.

Now suppose every element of I with degree less than d belongs to M. Let $g \in I$ with $\deg(g) = d$ and $\mathrm{LT}(g) = cx^d$. Our goal is to find $h \in M$ with $\mathrm{LT}(h) = cx^d$, so that $g - h \in I$ has degree less than d and the inductive hypothesis applies. Set $n = \min\{d, N\}$. Since the ascending chain $J_0 \subseteq J_1 \subseteq \cdots$ stabilizes at J_N, we have $J_d = J_n$, so $c \in J_n = \langle a_{n,1}, \ldots, a_{n,r_n} \rangle$. Write

$$c = b_1 a_{n,1} + \cdots + b_{r_n} a_{n,r_n}$$

for some $b_i \in R$, and define

$$h = \sum_{i=1}^{r_n} b_i x^{d-n} f_{n,i}.$$

(Note: if $d \leq N$ then $n = \min\{d, N\} = d$ and the $x^{d-n} = 1$.) Each $f_{n,i} \in M$, so $h \in M$.

(e) Show that $\mathrm{LT}(h) = cx^d$. From this deduce that $g - h \in I$ and either $\deg(g - h) < d$ or $g - h = 0$.

(f) Using the inductive hypothesis conclude that $g - h \in M$, and show this implies $g \in M$. Conclude that $I \subset M$. Explain why this concludes the proof of Hilbert's Basis Theorem.

(g) Prove via induction on n that if R is Noetherian then $R[x_1, \ldots, x_n]$ is Noetherian.

(h) Compare this proof to the proof of Dickson's Lemma we gave above.

This worksheet has introduced two important concepts that will recur throughout the course: the usefulness of Gröbner bases and the importance of finiteness conditions such as Noetherianity. A significant open thread raised by this worksheet is that while we know theoretically that Gröbner bases exist, we do not yet know how to actually compute them. We will return to this question later.

It is fitting that Gröbner bases and Noetherianity are so linked. Hilbert's original proof of his Basis Theorem was non-constructive, even over $\mathbb{K}[x_1,\ldots,x_n]$, which – as the story goes – came as a shock to many mathematicians of the time. Paul Gordan, a prominent algebraist, reportedly remarked, perhaps seriously, perhaps in jest, *"This is not mathematics. This is theology."* (Gordan later gave another proof of the theorem, one which in a sense also proved Dickson's Lemma some 10 years before Dickson.) On the other hand, Gröbner bases have come to serve as the foundational tool of computational commutative algebra, allowing us to compute and make explicit a great many things that Hilbert's methods could not.
