WORKSHEET 6.3: GRÖBNER BASES PT. III

Fix a field $\mathbb{K}$ and set $S = \mathbb{K}[x_1, \dots, x_n]$. Unless otherwise specified, all ideals live in S and all monomial orders are denoted by $<$. In the previous Gröbner basis worksheets we introduced monomial orders, multivariable division, monomial ideals, initial ideals, and the definition of a Gröbner basis. We also proved that Gröbner bases exist and that they solve the ideal membership problem. This worksheet is the last Gröbner basis worksheet of the course. Its goal is to consolidate the definitions, introduce the standard monomial basis of a quotient, and give the computational theorem which makes Gröbner bases effective: Buchberger's criterion and algorithm. The guiding principle is that a Gröbner basis lets us replace questions about a complicated ideal I by questions about the monomial ideal $\text{in}_<(I)$.

Recall a *monomial ordering* on $\mathbb{K}[x_1, \dots, x_n]$ 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 $\mathbb{K}[x_1, \dots, x_n]$ 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 $\alpha < \beta$. Recall that for a nonzero polynomial $f \in S$ we write $\text{LT}(f) = \text{LC}(f)\text{LM}(f)$ where $\text{LM}(f)$ is the largest monomial appearing in f, $\text{LC}(f) \in \mathbb{K}^\times$ is its coefficient, and $\text{LT}(f)$ is the corresponding term.

Definition 1. 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:

$$\text{in}_<(I) := \langle \text{LT}(f) \mid f \in I \rangle.$$

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

It is standard to set $\text{in}_<(\langle 0 \rangle) = \langle 0 \rangle$.

---

(1) **Reviewing leading terms and initial ideals.** Let $S = \mathbb{K}[x, y, z]$.

(a) For

$$f = 3x^2z - 5xy^3 + 7y^4z + xz^5$$

compute $\text{LM}(f)$, $\text{LC}(f)$, and $\text{LT}(f)$ using each of the following orders: lex with $x > y > z$, grlex with $x > y > z$, and grevlex with $x > y > z$.

(b) Prove that if $f, g \in S$ are nonzero, then

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

Where do you use the defining property of a monomial order?

(c) Let $I = \langle xy - 1, y^2 - 1 \rangle \subset \mathbb{K}[x, y]$ and use lex order with $x > y$. Show that

$$\langle \text{LT}(xy - 1), \text{LT}(y^2 - 1) \rangle = \langle xy, y^2 \rangle.$$

Then show that $x - y \in I$ and explain why this proves $\{xy - 1, y^2 - 1\}$ is not a Gröbner basis.

(d) Give an example of an ideal I and a generating set $F = \{f_1, \ldots, f_s\}$ such that

$$\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \subsetneq \mathrm{in}_<(I).$$

Your example may be the one from part (c), but make sure to identify an explicit element of $\mathrm{in}_<(I)$ missing from the smaller ideal.

(2) **Division and normal forms.** Let $G = (g_1, \ldots, g_t)$ be an ordered list of nonzero polynomials in S. Dividing f by G produces an expression

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

where no term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. We call such an r a *remainder* or *normal form* of f with respect to G and sometimes write $r = \overline{f}^G$ or $r = \mathrm{NF}_G(f)$.

(a) Explain why the remainder can depend on the order of the list G if G is not a Gröbner basis.

(b) Prove that if G is a Gröbner basis for $I = \langle G \rangle$, then $f \in I$ if and only if the remainder on division by G is zero.

(c) Prove that if G is a Gröbner basis for I, then the remainder of f on division by G is independent of all choices made during the division algorithm. Hint: If two remainders r and r' occur, compare $r - r'$.

(d) Let $I = \langle xy - 1, y^2 - 1 \rangle \subset \mathbb{K}[x, y]$ with lex order $x > y$. Divide $x - y$ by the ordered list $(xy - 1, y^2 - 1)$. Explain why the answer is consistent with part (b).

(3) **Minimal and reduced Gröbner bases.** A Gröbner basis $G = \{g_1, \ldots, g_t\}$ is *minimal* if every g_i is monic and no $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(g_j)$ for $i \neq j$. It is *reduced* if every g_i is monic and no monomial appearing in $g_i - \mathrm{LT}(g_i)$ is divisible by any $\mathrm{LM}(g_j)$.

(a) Prove that every reduced Gröbner basis is minimal.

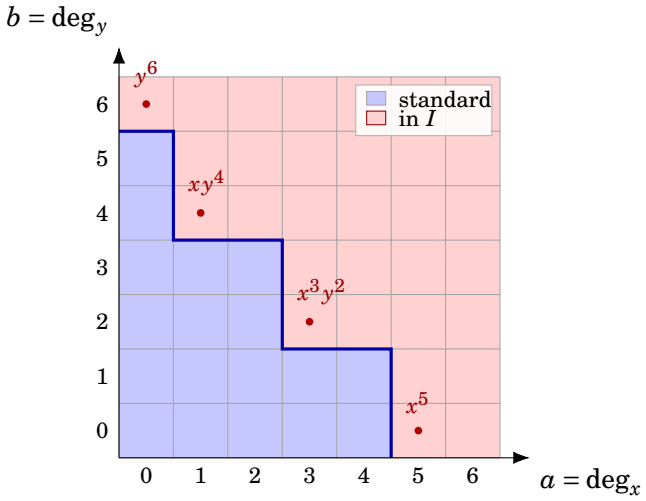
(b) Starting from any Gröbner basis G, explain how to produce a minimal Gröbner basis by rescaling and deleting redundant elements.

(c) Starting from a minimal Gröbner basis, explain how to reduce the non-leading terms of each g_i by the other basis elements. Why does this process produce a reduced Gröbner basis?

(d) Prove uniqueness of reduced Gröbner bases for a fixed ideal and fixed monomial order. Hint: If G and H are reduced Gröbner bases for I, first compare their leading monomials using the uniqueness of minimal monomial generators of $\mathrm{in}_<(I)$. Then compare the two basis elements with the same leading monomial.

For monomial ideals, the monomials outside the ideal form a "staircase." For example if we consider the ideal $I = \langle x^5, x^3y^2, xy^4, y^6 \rangle$ in $\mathbb{K}[x, y]$ we can picture it as via the diagram below. The monomials in I are

shown in red while those that are non-zero in the quotient S/I are shown in blue. For a general ideal, the same staircase is obtained from the initial ideal. These monomials give canonical basis for S/I.



Definition 2. Let $I \subset S$ be an ideal. A monomial x^α is called a *standard monomial* for I with respect to $<$ if $x^\alpha \notin \text{in}_<(I)$.

We denote the set of standard monomials by $\text{std}_<(I)$. If $G = \{g_1, \ldots, g_t\}$ is a finite set of nonzero polynomials, we say x^α is *standard for* G if no $\text{LM}(g_i)$ divides x^α. If G is a Gröbner basis for I, then being standard for I is the same as being standard for G. Thus the standard monomials can be read off from the leading monomials of any Gröbner basis.

Theorem 3 (Standard Monomial Basis Theorem)**.** *Let $I \subset S$ be an ideal and fix a monomial order. The residue classes of the standard monomials form a $\mathbb{K}$-basis of S/I.*

---

(4) **Proving the Standard Monomial Basis Theorem.** Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for I.

- (a) Show that the remainder obtained by dividing any $f \in S$ by G is a $\mathbb{K}$-linear combination of standard monomials.
- (b) Deduce that the residue classes of the standard monomials span S/I.
- (c) Suppose h is a nonzero $\mathbb{K}$-linear combination of standard monomials. Prove that $h \notin I$. Hint: What can you say about $\text{LT}(h)$ if $h \in I$?
- (d) Deduce linear independence and conclude Theorem **??**.
- (e) Explain why Theorem **??** gives another proof that normal forms with respect to a Gröbner basis are unique.

(5) **Computing standard monomials.** In each part, list the standard monomials and draw the staircase picture when there are only two variables.

(a) $M = \langle x^3, x^2y, y^4 \rangle \subset \mathbb{K}[x,y]$.

(b) $M = \langle x^2, xy, y^3 \rangle \subset \mathbb{K}[x,y]$.

(c) $M = \langle x^2z, xyz, y^2z, z^3 \rangle \subset \mathbb{K}[x,y,z]$.

(d) Let $I = \langle x - y^2, y^3 - 1 \rangle \subset \mathbb{K}[x,y]$ with lex order $x > y$. Verify that the displayed generators are a reduced Gröbner basis. List $\mathrm{std}_<(I)$ and compute $\dim_{\mathbb{K}}(S/I)$.

(e) With I as in part (d), compute the normal forms of x^5, $x^2y + y^7$, and $xy^2 + x + y$.

(6) **Finite quotients and powers of variables.** Let $I \subset S$ be an ideal and fix a monomial order.

(a) Prove that S/I is finite-dimensional as a $\mathbb{K}$-vector space if and only if $\mathrm{std}_<(I)$ is finite. In this case,

$$\dim_{\mathbb{K}}(S/I) = \#\,\mathrm{std}_<(I).$$

(b) Let $M \subset S$ be a monomial ideal. Prove that S/M is finite-dimensional over $\mathbb{K}$ if and only if, for every variable x_i, there exists an integer $a_i \geq 1$ such that $x_i^{a_i} \in M$.

(c) Deduce that S/I is finite-dimensional over $\mathbb{K}$ if and only if, for every variable x_i, there exists $a_i \geq 1$ such that $x_i^{a_i} \in \mathrm{in}_<(I)$.

(d) Apply part (c) to the ideals

$$\langle x - y^2, y^3 - 1 \rangle, \qquad \langle xy - 1 \rangle, \qquad \langle x^2, y^2, z^2, xy - yz \rangle.$$

We now turn to the computational heart of the subject. The obstruction to a generating set being a Gröbner basis is cancellation of leading terms. Buchberger's insight was that it is enough to check the simplest possible cancellations, namely pairwise cancellations.

Definition 4. Let $f, g \in S$ be nonzero. Write $\mathrm{LT}(f) = c_f x^\alpha$ and $\mathrm{LT}(g) = c_g x^\beta$, and let $x^\gamma = \mathrm{lcm}(x^\alpha, x^\beta)$. The *$S$-polynomial* of f and g is

$$S(f,g) = \frac{x^{\gamma-\alpha}}{c_f} f - \frac{x^{\gamma-\beta}}{c_g} g.$$

Thus the leading terms of the two summands cancel.

Theorem 5 (Buchberger's Criterion)**.** *Let $G = \{g_1, \ldots, g_t\} \subset S$ and set $I = \langle G \rangle$. Then G is a Gröbner basis for I if and only if every $S(g_i, g_j)$ has remainder zero on division by G.*

---

(7) **S-polynomials by hand.** Work in $\mathbb{K}[x,y]$ with lex order $x > y$.

(a) Let $g_1 = xy - 1$ and $g_2 = y^2 - 1$. Compute $S(g_1, g_2)$ and reduce it by the ordered list (g_1, g_2).

(b) Add the nonzero remainder from part (a) to the list. Call it g_3. Compute $S(g_1, g_3)$ and $S(g_2, g_3)$ and reduce both by (g_1, g_2, g_3).

(c) Conclude that $\{g_1, g_2, g_3\}$ is a Gröbner basis for $\langle xy-1, y^2-1\rangle$.

(d) Reduce this Gröbner basis to the unique reduced Gröbner basis.

(8) **Another full Buchberger computation.** Work in $\mathbb{K}[x,y]$ with lex order $x > y$. Let

$$f_1 = x^2 - y, \qquad f_2 = xy - 1,$$

and set $I = \langle f_1, f_2\rangle$.

(a) Compute $S(f_1, f_2)$ and reduce it by (f_1, f_2).

(b) Continue Buchberger's algorithm until every pair reduces to zero.

(c) Show that the reduced Gröbner basis is $\{x - y^2,\ y^3 - 1\}$.

(d) Find the standard monomials of S/I and to solve the system $x^2 - y = xy - 1 = 0$ over $\mathbb{C}$.

(9) **Proving Buchberger's Criterion.** We prove Theorem **??** in pieces. Let $G = \{g_1, \ldots, g_t\}$ and $I = \langle G\rangle$.

(a) Prove the easy direction: if G is a Gröbner basis, then every $S(g_i, g_j)$ reduces to zero modulo G.

(b) For the converse, let $f \in I$ and write $f = q_1 g_1 + \cdots + q_t g_t$. For such a representation, define

$$\delta(q_1, \ldots, q_t) = \max_i \mathrm{LM}(q_i g_i).$$

Choose a representation of f for which δ is as small as possible. Explain why this makes sense.

(c) Show that if the terms of monomial δ in the sum $\sum q_i g_i$ do not cancel, then $\mathrm{LT}(f)$ is divisible by some $\mathrm{LT}(g_i)$.

(d) Suppose instead that the terms of monomial δ cancel. Show that the cancellation gives a nontrivial relation among leading terms of some g_i's.

(e) Use the assumption that every $S(g_i, g_j)$ reduces to zero to replace this relation by a combination of the g_i's whose terms all have monomial strictly smaller than δ.

(f) Explain why part (e) contradicts the minimal choice of the representation unless $\mathrm{LT}(f)$ is divisible by some $\mathrm{LT}(g_i)$.

(g) Conclude that $\mathrm{in}_<(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$.

(10) **Buchberger's Algorithm.** Buchberger's criterion leads directly to an algorithm.

Algorithm 1 Buchberger's Algorithm

Input: nonzero polynomials $F = \{f_1, \dots, f_s\} \subset S$ and a monomial order $<$
$G \leftarrow F$
$P \leftarrow \{\{g,h\} \mid g,h \in G,\ g \neq h\}$
while $P \neq \varnothing$ **do**
    choose a pair $\{g,h\} \in P$ and remove it from P
    divide $S(g,h)$ by G and let r be the remainder
    if $r \neq 0$ **then**
        $P \leftarrow P \cup \{\{r,k\} \mid k \in G\}$
        $G \leftarrow G \cup \{r\}$
    end if
end while
return G

(a) Prove that whenever a nonzero remainder r is added, the monomial ideal $\langle \mathrm{LT}(g) \mid g \in G \rangle$ strictly increases.

(b) Use the Noetherian property of S (or Dickson's Lemma for monomial ideals) to prove that the algorithm terminates.

(c) Prove that the output is a Gröbner basis for $\langle F \rangle$.

(11) **Ideal membership, inclusion, and equality.** Let $I = \langle f_1, \dots, f_s \rangle$ and $J = \langle h_1, \dots, h_r \rangle$ be ideals of S.

(a) Suppose G_J is a Gröbner basis for J. Prove that $I \subseteq J$ if and only if every $\mathrm{NF}_{G_J}(f_i) = 0$.

(b) Explain how to test whether $I = J$ using two Gröbner basis computations.

(c) Use part (a) to decide whether

$$\langle x^2 - y, xy - 1 \rangle \subseteq \langle x - y^2, y^3 - 1 \rangle$$

in $\mathbb{K}[x,y]$ with lex order $x > y$.

(d) Let G be a Gröbner basis for I. Prove that f and g have the same image in S/I if and only if $\mathrm{NF}_G(f) = \mathrm{NF}_G(g)$.

(12) **Radical membership: the Rabinowitsch trick.** Let $I = \langle f_1, \dots, f_s \rangle \subset S$ and let $f \in S$. Introduce a new variable u.

(a) Prove that

$$f \in \sqrt{I} \quad \Longleftrightarrow \quad 1 \in \langle f_1, \dots, f_s, 1 - uf \rangle \subset S[u].$$

Hint: Interpret $S[u]/\langle 1 - uf \rangle$ as the localization $S[f^{-1}]$.

(b) Explain how this turns radical membership into an ideal membership test using a Gröbner basis.

(c) Use this criterion to show that $x \in \sqrt{\langle x^2, xy \rangle} \subset \mathbb{K}[x,y]$.

(d) Is $y \in \sqrt{\langle x^2, xy \rangle}$? Justify your answer algebraically and with the Gröbner basis criterion.

(13) **Computer check.** Use *Macaulay2* to verify at least two computations from this worksheet.

(a) Compute a Gröbner basis for $\langle xy - 1, y^2 - 1 \rangle$ with lex order $x > y$.

(b) Compute a Gröbner basis for $\langle x^2 - y, xy - 1 \rangle$ with lex order $x > y$.

(c) Compute the standard monomials for one zero-dimensional ideal above.

(d) Compute one intersection ideal from Problems 15 and 16.

(e) Compare the reduced Gröbner basis returned by the computer with your hand computation. Which intermediate choices differed, and why did the reduced answer not depend on those choices?