Lesson 14 – Properties of Groebner Bases

I. Groebner Bases Yield Unique Remainders

**Theorem** Let \( G = \{g_1, g_2, ..., g_t\} \) be a Groebner basis for an ideal \( I \subseteq k[x_1, x_2, ..., x_n] \), and let \( f \in k[x_1, x_2, ..., x_n] \). Then there is a unique \( r \) with the following properties

(i) No term of \( r \) is divisible by any of \( \text{LT}(g_1), \text{LT}(g_2), ..., \text{LT}(g_t) \).
(ii) There is \( g \in I \) such that \( f = g + r \).

In particular, \( r \) is the remainder on division of \( f \) by \( G \) no matter how the elements of \( G \) are listed when using the division algorithm.

**Proof:** The existence of \( r \) follows from the division algorithm, which yields \( f = a_1g_1 + a_2g_2 + \cdots + a_tg_t + r = g + r \), where \( a_i \in k[x_1, x_2, ..., x_n] \), and \( r \) satisfies condition (i). It suffices, then, to prove the uniqueness of \( r \).

**Exercise 1** Prove the uniqueness of \( r \).

**Exercise 2** We know from the above theorem that dividing a polynomial \( f \in k[x_1, x_2, ..., x_n] \) by a Groebner basis \( G = \{g_1, g_2, ..., g_t\} \) produces a unique remainder (regardless of the order of the set). Are the quotients unique too? Let’s examine this question...

The set \( G = \{x + z, y - z\} \) is a Groebner basis for \( I = \langle x + z, y - z \rangle \) using the lex order w/ \( x > y > z \).

a) Divide \( xy \) by the 2-tuple \((x + z, y - z)\).

**Solution.**

\[
\begin{array}{c|c}
  x + z & xy \\ \\
  y - z & - (xy + yz) \\
\end{array}
\]

\[
\begin{array}{c|c}
  & -yz \\
  & -yz + z^2 \\
\end{array}
\]

So \( xy = y(x + z) - z(y - z) - z^2 \). The remainder is \( r = -z^2 \).
b) Now divide $xy$ by $(y - z, x + z)$. What do you discover?

**Solution.**

\[
\begin{array}{c|c}
xy & x \\
- (xy - xz) & \hline \\
xy & xz \\
\end{array}
\]

So $xy = z(x + z) + x(y - z) - z^2$. The remainder is $r = -z^2$ is the same as expected, but the quotients are different.

**Notation.** We will write $f^F$ to denote the remainder of $f$ upon division by an *ordered* $t$-tuple of polynomials $F = \{f_1, f_2, ..., f_t\}$. If $G = \{f_1, f_2, ..., f_t\}$ is a Groebner basis, then we can regard the $t$-tuple as a set (without any particular order), and we call $f^G$ the **normal form** of $f$.

As a corollary to Theorem 1, we now know that the division algorithm decides the ideal membership problem as long as we divide the polynomial in question by a Groebner basis.

**Corollary (Ideal Membership)** Let $G = \{g_1, g_2, ..., g_t\}$ be a Groebner basis for an ideal $I \subseteq k[x_1, x_2, ..., x_n]$, and let $f \in k[x_1, x_2, ..., x_n]$. Then $f \in I$ if and only if $f^G = 0$.

**BUT HOW DO WE KNOW IF WE HAVE A GROEBNER BASIS???**

**II. S-Polynomials and Buchberger’s Criterion**

Let’s assume we have a potential Groebner basis $G = \{g_1, g_2, ..., g_t\}$ for an ideal $I \subseteq k[x_1, x_2, ..., x_n]$, with $g_1, g_2, ..., g_t \in I$. It follows from the definition that $\langle \text{LT}(g_1), \text{LT}(g_2), ..., \text{LT}(g_t) \rangle \subseteq \langle \text{LT}(I) \rangle$.

However, it could be that $\langle \text{LT}(g_1), \text{LT}(g_2), ..., \text{LT}(g_t) \rangle \not\subseteq \langle \text{LT}(I) \rangle$. Let’s remind ourselves of how this can happen with an example...

**Exercise 3** Consider the ideal $I = \langle g_1, g_2 \rangle \subseteq k[x, y]$, where $g_1(x, y) = x^3 - 2x$ and $g_2(x, y) = x^4 - 3x$. Show that $\langle \text{LT}(g_1), \text{LT}(g_2) \rangle \not\subseteq \langle \text{LT}(I) \rangle$. 
**Question:** What is the basic source of the obstruction to Groebner bases?

Hence we define the “$S$-polynomial”.

**Definition**  Let $f, g \in k[x_1, x_2, ..., x_n]$ be nonzero polynomials.

(i) If $\text{multideg}(f) = \alpha$ and $\text{multideg}(g) = \beta$, then let $\gamma = (\gamma_1, \gamma_2, ..., \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each $1 \leq i \leq n$. We call the least common multiple of $\text{LM}(f)$ and $\text{LM}(g)$, written $x^\gamma = \text{LCM}(\text{LM}(f), \text{LM}(g))$.

(ii) The $S$-polynomial of $f$ and $g$ is the combination

\[
S(f, g) = \frac{x^\gamma}{\text{LT}(f)} \cdot f - \frac{x^\gamma}{\text{LT}(g)} \cdot g.
\]

(Note that we are inverting the leading coefficients here as well.)

**Exercise 4** Compute the $S$-polynomial of $f(x, y) = x^3y^2 - x^2y^3$ and $g(x, y) = 3x^4y + y^2$ under the grlex order.

Notice that the $S$-polynomial is basically designed to cancel the leading terms of $f$ and $g$, so what we get is another element of the ideal $I = \langle f, g \rangle$ with a different leading term. Therefore, if we have a Groebner basis $G$, $G$ must also generate all of the $S$-polynomials. This is, in fact, one way of checking that we have a Groebner basis, via the following theorem.

**Theorem (Buchberger’s Criterion)** Let $I \subseteq k[x_1, x_2, ..., x_n]$ be an ideal. Then $G = \{g_1, g_2, ..., g_t\}$ is a Groebner basis for $I$ if and only if for all $i \neq j$, the remainder upon division of $S(g_i, g_j)$ by $G$ is zero.

This theorem gives a fairly simple test for whether or not we have a Groebner basis.
**Exercise 5** Consider the ideal \( I = \langle x - z^2, y - z^3 \rangle \subseteq k[x, y, z] \).

a) Is \( G = \{ x - z^2, y - z^3 \} \) a Groebner bases for \( I \) under the lex order with \( x > y > z \)?

b) Is \( G = \{ x - z^2, y - z^3 \} \) a Groebner bases for \( I \) under the lex order with \( z > y > x \)?

**Remark** You can check that \( G = \{ x - z^2, y - z^3 \} \) is not a Groebner bases for \( I \) under the grlex order (with any ordering of the variables). Hence, a set of generators for a given ideal may form a Groebner basis under one monomial order, but not under another.

**III. A Sketch of the Proof of Buchberger’s Criterion**

If \( f = \sum_{i=1}^{s} h_i f_i \in I \) is such that \( \text{LT}(f) \notin \langle \text{LT}(f_1), \text{LT}(f_2), ..., \text{LT}(f_t) \rangle \) then several of the leading terms of the summands with a common leading power must cancel, leaving lower power terms that aren’t generated by the \( \{ \text{LT}(f_i) \} \). This happens, of course, because the leading coefficients cancel. So it is useful to consider scalar combinations of the \( f_i \).

**Lemma** If \( f = \sum_{i=1}^{s} c_i f_i \in k[x_1, x_2, ..., x_n] \) where \( c_i \in k \) and \( \text{multideg}(f_i) = \delta \) for all \( 1 \leq i \leq s \), and \( \text{multideg}(f) < \delta \), then \( f = \sum_{i=1}^{s} c_i f_i \) is a \( k \)-linear combination of the \( S \) polynomials \( S(f_i, f_j) \); that is,

\[
f = \sum_{i=1}^{s} c_i f_i = \sum_{j,k} c_{jk} S(f_i, f_j), \quad \text{for some } c_{jk} \in k
\]

**Exercise 6** Compute \( S(f_i, f_j) \), where \( 1 \leq i, j \leq s, i \neq j \), and the polynomials \( f_i, f_j \) satisfy the hypotheses of the above lemma (so they have the same multidegree).
Exercise 7 Write $\sum_{i=1}^{s} c_i f_i$ as a $k$-linear combination of the $S$ polynomials $S(f_i, f_j)$, where $1 \leq i, j \leq s$. (We’re assuming all of the hypotheses of the lemma.)

Theorem (Buchberger’s Criterion) Let $I \subseteq k[x_1, x_2, \ldots, x_n]$ be an ideal. Then $G = \{g_1, g_2, \ldots, g_l\}$ is a Groebner basis for $I$ if and only if $S(g_i, g_j)^G = 0$ for all $i \neq j$.

Sketch of Proof.