Lesson 10 – Groebner Bases and the Hilbert Basis Theorem

I. The Hilbert Basis Theorem We want to accomplish two things today. First we will prove the Hilbert Basis Theorem and discuss the consequences that this theorem has in algebraic geometry. And second, we will define Groebner bases - a mathematical object that will arise naturally in the proof of the Hilbert Basis Theorem.

Theorem (Hilbert Basis Theorem) Every ideal $I \subseteq k[x_1, x_2, \dots, x_n]$ has a finite generating set. That is, $I = \langle g_1, g_2, \dots, g_t \rangle$ for some $g_1, g_2, \dots, g_t \in I$.

Before proving this result, we need a definition:

Definition Fix a monomial ordering on $k[x_1, x_2, \dots, x_n]$, and let $I \subseteq k[x_1, x_2, \dots, x_n]$ be a nonzero ideal. The **ideal of leading terms** of I, $\langle \mathrm{LT}(I) \rangle$, is the ideal generated by the set of leading terms:

$$\mathrm{LT}(I) = \{cx^\alpha : \text{there exists } f \in I \text{ with } \mathrm{LT}(f) = cx^\alpha\}.$$

Exercise 1 – Identify some elements of $\langle \mathrm{LT}(I) \rangle$, where $I = \langle x^2y - z, xy - 1 \rangle \subseteq k[x, y, z]$.

And we remind you of Property 1 from last lesson; it will be useful.

Property 1 for Monomial Ideals:
If $I = \langle x^\alpha : \alpha \in A \rangle$, then $x^\beta \in I \Rightarrow x^\beta = x^\gamma \cdot x^\alpha$ for some $\alpha \in A$.

The proof of the Hilbert Basis Theorem now follows from the next two exercises.

Exercise 2. Let $I \subseteq k[x_1, x_2, \dots, x_n]$ be an ideal. Show that the monomial ideal $\langle \mathrm{LT}(I) \rangle$ is generated by a set of monomials $\mathrm{LT}(g_1), \mathrm{LT}(g_2), \dots, \mathrm{LT}(g_t)$ for some $g_1, g_2, \dots, g_t \in I$. That is, $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \dots, \mathrm{LT}(g_t) \rangle$ for some $g_1, g_2, \dots, g_t \in I$.

Exercise 3 From Exercise 2 we know that if $I \subseteq k[x_1, x_2, \ldots, x_n]$ is an ideal, then $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle$ for some $g_1, g_2, \ldots, g_t \in I$. Prove that, in fact, $I = \langle g_1, g_2, \ldots, g_t \rangle$.

II. The Definition of a Groebner Basis

The proof of Hilbert's Basis Theorem should motivate the following definition.

Definition. Given a non-zero ideal $I \subseteq k[x_1, x_2, \ldots, x_n]$ and a monomial ordering on $k[x_1, x_2, \ldots, x_n]$, a set $G = \{g_1, g_2, \ldots, g_t\} \subseteq I$ is a **Groebner basis** or **standard basis** for I if

$$I = \langle g_1, g_2, \ldots, g_t \rangle \text{ and } \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle.$$

Remark. Since $\{g_1, g_2, \ldots, g_t\} \subseteq I$, it is certainly true that $\mathrm{LT}(g_i) \in \mathrm{LT}(I)$ for all $1 \leq i \leq t$. Hence we always have the inclusion $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle \subseteq \langle \mathrm{LT}(I) \rangle$. To show that a given set $\{g_1, g_2, \ldots, g_t\}$ is a Groebner Basis, it suffices to show $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle \supseteq \langle \mathrm{LT}(I) \rangle$.

Question: What does it mean, exactly, to choose an arbitrary element in $\langle \mathrm{LT}(I) \rangle$?

Exercise 4 Explain how the proof of the Hilbert Basis Theorem ensures the existence of a Groebner Basis for any ideal $I \subseteq k[x_1, x_2, \ldots, x_n]$. That is, why is the following corollary true?

Corollary (Existence of Groebner Bases) Fix a monomial order. Then every nonzero ideal $I \subseteq k[x_1, x_2, \ldots, x_n]$ has a Groebner basis. That is, there exist $g_1, g_2, \ldots, g_t \in I$, such that

$$I = \langle g_1, g_2, \ldots, g_t \rangle \text{ and } \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle.$$

Exercise 5 Show that if $I = \langle g \rangle \subseteq k[x_1, x_2, \ldots, x_n]$ where g is nonzero, then $G = \{g\}$ is a Groebner basis for I. (This is true for any monomial ordering.)

Exercise 6 Choose the lexicographic order, $x > y$, and consider the ideal $I = \langle x^2y - z, xy - 1 \rangle \subseteq k[x, y, z]$. Define $g_1(x, y, z) = x^2y - z$ and $g_2(x, y, z) = xy - 1$. Show that $\{x^2y - z, xy - 1\}$ is not a Groebner Basis for I. (This was the ideal from the ideal membership example we covered last Friday.)

Exercise 7 Consider the ideal $I = \langle x - z^2, y - z^3 \rangle \subseteq \mathbb{R}[x, y, z]$.

a) Explain why $\{x - z^2, y - z^3\}$ is a Groebner basis for I iff any relation of the form

$$f(x, y, z)(x - z^2) + g(x, y, z)(y - z^3) = h(z), \qquad f, g \in \mathbb{R}[x, y, z], h \in \mathbb{R}[z]$$

implies $h = 0$.

b) Show that $\{x - z^2, y - z^3\}$ is, indeed, a Groebner basis for I.

c) Do you think $\{x - z^2, y - z^3\}$ would be a Groebner basis for I under any monomial order?

III. Consequences of the Hilbert Basis Theorem

Probably the most important consequence of the Hilbert Basis Theorem is the fact that every **affine variety defined by an ideal** is "carved out" by finitely many polynomial equations. We recall our (old) definition of an affine variety and define what we mean by an affine variety defined by an ideal.

Definition (old) Let k be a field, and let $f_1, f_2, \dots, f_d \in k[x_1, x_2, \dots, x_n]$,. Then the **affine variety**, denoted by $\mathbf{V}(f_1, f_2, \dots, f_d)$, is defined by:

$$\mathbf{V}(f_1, f_2, \dots, f_d) = \{(a_1, a_2, \dots, a_n) \in k^n : f_i(a_1, a_2, \dots, a_n) = 0 \text{ for all } 1 \leq i \leq d\}.$$

Definition Let $I \subseteq k[x_1, x_2, \dots, x_n]$ be an ideal. Then the variety associated with this ideal is

$$\mathbf{V}(I) = \{(a_1, a_2, \dots, a_n) : f(a_1, a_2, \dots, a_n) = 0 \text{ for all } f \in I\}$$

Theorem If $I \subseteq k[x_1, x_2, \dots, x_n]$ is an ideal, then there is a finite set $\{f_1, f_2, \dots, f_s\} \subseteq I$ such that $\mathbf{V}(I) = \mathbf{V}(f_1, f_2, \dots, f_s)$.