Math 361 lecture for Wednesday, Week 5

Hilbert basis theorem

As a motivation question, let t be an indeterminate, and consider the ideal

$$I = \{f \in \mathbb{R}[x, y, z] : f(t, t^2, t^3) = 0\}.$$

Examples of elements of I include $x^i y^j - z^k$ for all $(i, j, k) \in \mathbb{N}$ such that $i + 2j = 3k$, i.e., $x^{3k-2j}y^j - z^k$ where $3k \geq 2j$. For example, $xy - z, x - z^3$, etc. Similarly, I includes all $x^i z^j - y^k$ such that $(i, j, k) \in \mathbb{N}$ and $i + 3k = 2j$. For example, $x - y^2 \in I$ It also includes all $\mathbb{C}[x, y, z$-linear combinations of these elements.

Question. Is this ideal finitely generated?

Theorem 1. (Hilbert basis theorem.) Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remark 2.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \dots, s_n \in S$ such that $S = \{f(s_1, \dots, s_n) : f \in R[x_1, \dots, x_n]\}$.
- Recall that to say a ring R is Noetherian, we consider R as an R-module. The submodules of R are exactly the ideals in R. Thus, R is Noetherian if all of its ideals are finitely generated.
- Letting $R = K$ be a field and $S = K[x_1, \dots, x_n]$, the Hilbert basis theorem says that every ideal a polynomial ring with coefficients in a field is finitely generated. For instance, in the example above, we have $I = (y^2 - xz, xy - z, x^2 - y)$. [Aside: Consider the curve in $\mathbb{R}^3$ parametrized by $t \mapsto (t, t^2, t^3)$. This curve is the intersection of the two surfaces, $S = \left\{(x, y, z) \in \mathbb{R} : y = x^2\right\}$ and math $T = \left\{(x, y, z) \in \mathbb{R} : z = x^3\right\}$. One might think that I would generated by just the two equations $y - x^2$ and $z - x^3$, but it turns out that a minimum of three generators is required.

Proof of Hilbert basis theorem. Suppose that $s_1, \dots, s_n$ generate S as a ring over R. Then there exists an R-module surjection

$$\begin{aligned} R[x_1, \dots, x_n] &\to S \\ f(x_1, \dots, x_n) &\mapsto f(s_1, \dots, s_n). \end{aligned}$$

Since the image of a Noetherian R-module is Noetherian, it suffices to prove that the polynomial ring $R[x_1, \ldots, x_n]$ is a Noetherian R-module. Since $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$, by induction, it suffices to show that the polynomial ring $R[x]$ is Noetherian.

So we need to show that $R[x]$ is Noetherian. Let I be an ideal in $R[x]$. We must show that I is finitely generated, i.e,. $I = (f_1, \ldots, f_k)$ for some polynomials $f_1, \ldots, f_k \in R[x]$ for some k.[1] Given any polynomial $f = \sum_{i=1}^{d} a_i x^i \in R[x]$ with $a_d \neq 0$, we call a_d the *leading coefficient of* f. For completeness, we say that zero polynomial has leading coefficient 0. Let A be the collection of all leading coefficients of elements of I. We claim that A is an ideal in R. We must show that A is nonempty, closed under addition, and closed under "in-out" multiplication. Since I is an ideal, it contains the zero polynomial, whose leading coefficient is $0 \in R$. Thus, $0 \in A$. Next, suppose that $a, b \in A$. Then there exist $f, g \in R[x]$ with leading terms a, b, respectively. Without loss of generality, say $\deg(f) \leq \deg(g)$, and let $j = \deg(g) - \deg(f)$. Define $h := x^j f$. Then $h \in I$, the leading term of h is a, and $\deg(h) = \deg(g)$. Then $h + g \in I$ and the leading term of $h + g$ is $a + b$. We have shown that A is closed under addition. Finally, suppose that $f \in I$ with leading coefficient a and $r \in R$. Then $ra \in A$ since it is the leading coefficient of $rf \in I$. This proves the claim.

Since R is Noetherian, and A is an ideal in R, it follows that $A = (a_1, \ldots, a_s)$ for some $a_i \in R$ and some $s \geq 1$. For each i, take $g_i \in I$ with leading coefficient a_i. By multiplying by appropriate powers of x, we may assume that all of the g_i had the same degree d. Let $I_{<d} \subset R[x]$ be the set of all elements of I that have degree strictly less than d. Then $I_{<d}$ is an R-module (but not an ideal in $R[x]$). Let M be the R-submodule of $R[x]$ generated by $1, x, \ldots, x^{d-1}$. Since R is Noetherian and M is a finitely generated R-module, M is Noetherian. Since $I_{<d}$ is a submodule of M, it follows that $I_{<d}$ is a finitely generated R-module. Say $h_1, \ldots, h_t$ are generators. So every element of $f \in I_{<d}$ may be written $f = \sum_{i=1}^{t} r_i h_i$ for some $r_i \in R$.

We finish by showing that I is generated by $s + t$ elements:

$$I = (g_1, \ldots, g_s, h_1, \ldots, h_t).$$

First note that the g_i and h_j are elements of I. Then take $f \in I$. We will prove by induction on the degree of f that f is an $R[x]$-linear combination of the g_i and h_j. If $\deg(f) < d$, then $f \in I_{<d}$, an R-submodule of $R[x]$ generated by the h_i. So in that case, $f = \sum_{i=1}^{t} r_i h_i$ for some $r_i \in R$, and we are done.

Next, suppose that $\deg(f) = e \geq d$. Say $a \in R$ is the leading coefficient of f. So $a \in A$, and it follows that $a = \sum_{i=}^{s} r_i a_i$ for some $r_i \in R$. Recall that all g_i have degree d. Therefore,

$$f - \sum_{i=1}^{s} r_i x^{e-d} g_i$$

is an element of I having degree strictly less than e. By induction, $f - \sum_{i=1}^{s} r_i x^{e-d} g_i$ is an $R[x]$-linear combination of the g_i and h_j. Hence, so is f. $\square$

[1] If R is a field, we would be done since $R[x]$ would then be a PID by the division algorithm. However, we only know that R is Noetherian.