HILBERT'S LEGACY

ROGER WIEGAND
PREPARATORY TALK #1
TRIBHUVAN UNIVERSITY

Toward the end of the 19th Century, David Hilbert did groundbreaking work that has had a profound and lasting effect on many areas of mathematics. Here we focus on two of his famous theorems, the Hilbert Basis Theorem and the Syzygy Theorem, which are indispensable tools in modern algebra and algebraic geometry.

sec:HBT

1. The Hilbert Basis Theorem

For simplicity, we work throughout with commutative rings, even though some results hold more generally.

thm:HBT **Theorem 1.1.** *Let k be a field, and let $x_1, \dots, x_n$ be indeterminates. Then every ideal in the polynomial ring $\mathsf{k}[x_1, \dots, x_n]$ is finitely generated.*

About thirty years after Hilbert's proof, Emmy Noether observed that a commutative ring R has the property that every ideal is finitely generated if and only if R has the *ascending chain condition* (ACC) on ideals, that is, there is no infinite strictly ascending chain

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

of ideals in R. Equivalently, for every ascending chain

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots ,$$

there is an integer N such that $I_N = I_{N+1} = I_{N+2} = \dots$. Rings with these equivalent properties are now known as *Noetherian* rings.

exc:ACC **Exercise 1.2.** Prove that a commutative ring R has ACC if and only if every ideal of R is finitely generated.

Theorem **??** is an immediate consequence of the following more general result:

thm:HBTind **Theorem 1.3.** *Let R be a commutative Noetherian ring. Then the polynomial ring $R[x]$ is Noetherian.*

There are many proofs of this theorem in the literature. Typically, they involve both the finite generation property and the ascending chain condition. Here is a typical proof:

Proof of Theorem **??**. Let J be an ideal of $R[x]$. We'll find a finite set of generators for J. For each $n \geq 0$, let L_n be the set of elements $b \in R$ such that b is the leading coefficient of some non-zero polynomial $f \in J$ with $\deg f \leq n\}$. Check easily that $I_n := L_n \cup \{0\}$ is an ideal of R and that $I_n \subseteq I_{n+1}$ for each $n \geq 0$. Since R is Noetherian there is an integer N such that $I_N = I_{N+1} = I_{N+2} = \dots$.

Date: 20 April, 2015.

For each $n \leq N$, choose a generating set $\{b_{n1}, \dots, b_{nt}\}$ for I_n, choose polynomials $f_{nj} = b_{nj}x^{p_{nj}}$ + lower-degree terms, with $f_{nj} \in J$ and $p_{nj} \leq n$. (We allow the possibility that $f_{nj} = b_{nj} = 0$. This is necessary, since L_n may be empty for small values of n.) We claim that J is generated by the $(N+1)t$ elements f_{nj}. If not, let f be an element *of least degree* in J but outside the ideal (f_{nj}) generated by the f_{nj}. We shall obtain a contradiction. Write $f = cx^d +$ lower-degree terms, with $c \neq 0$.

Case 1: $d \leq N$. Since $c \in I_d$, we can write $c = r_1 b_{d1} + \dots r_t b_{dt}$, where the coefficients r_j are in R. Put $g = r_1 f_{d1} + \cdots + r_t f_{dt}$. Notice that $g = cx^d +$ lower-degree terms, so $\deg(f-g) < d$ (the leading terms cancel). Now $g \in (f_{nj}) \subseteq J$, and it follows that $f-g$ is in J but outside (f_{nj}). This contradicts the minimality of $\deg f$.

Case 2: $d > N$. Then $c \in I_d = I_N$, and we write $c = r_1 b_{N1} + \dots r_t b_{Nt}$. Put $g = r_1 x^{d-p_{N1}} f_{N1} + \cdots + r_t x^{d-p_{Nt}} f_{Nt}$. Again, we have $g = cx^d +$ lower-degree terms, so $\deg(f-g) < d$, and we obtain a contradiction as before. □

2. Noetherian modules

An R-module M is said to be *Noetherian* provided M has ACC on submodules. As in Exercise **??** one checks that M is Noetherian if and only if every submodule is finitely generated. The ring R is Noetherian if and only if it is Noetherian as an R-module.

exc:SES **Exercise 2.1.** Suppose $0 \to U \to V \to W \to 0$ is an exact sequence of R-modules. Then V is Noetherian if and only if both U and W are Noetherian.

For any positive integer n, there is an exact sequence

$$0 \to R \to R^{n+1} \to R^n \to 0\,.$$

It follows (by induction) that if R is a Noetherian ring then R^n is a Noetherian module for every n. Now, given a finitely generated module M, with generators $x_1, \dots, x_n$, there is an exact sequence

eq:syz
$$0 \to K \to R^n \to M \to 0\,, \tag{2.1}$$

where the map $R^n \to M$ take the standard basis element e_i to x_i, and K is the kernel of this map. This proves:

prop:NoethMod **Proposition 2.2.** *Every finitely generated module over a Noetherian ring is a Noetherian module.*

3. Hilbert's Syzygy Theorem

The word "basis" in the name "Hilbert Basis Theorem" is misleading. A set of generators for an ideal is classically referred to as a "basis", though in modern terminology the word "basis" means something much stronger: It's a linearly independent set of generators for the ideal. Notice that a non-principal ideal in a commutative ring cannot have a basis: Any two non-zero elements f and g of an ideal satisfy the non-trivial dependence relation

eq:SyzRel
$$(-g) \cdot f + f \cdot g = 0\,. \tag{3.1}$$

Incidentally, a polynomial ring in more than one variable always has non-principal ideals, in fact, ideals requiring arbitrarily (but finitely!) many generators. For example, in the polynomial ring $\mathbb{C}[x,y]$, the ideal $I := (x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n)$ cannot be generated by fewer than $n+1$ generators.

exc:BigIdeal

Exercise 3.1. Prove this! (Hint: Let $\mathfrak{m} = (x,y)$. If I could be generated by fewer than $n+1$ elements, so could $I/\mathfrak{m}I$. Show that $I/\mathfrak{m}I$ is a $\mathbb{C}$-vector space of dimension $n+1$, to obtain a contradiction.)

Equation (**??**) is an example of a *syzygy relation*, that is, a linear relation among generators of a module (in this case the ideal (f,g)). Now let R be a commutative Noetherian ring and M a finitely generated R-module, with generating set $\{f_1, \ldots, f_n\}$. As in Equation (**??**), we have an exact sequence

$$0 \to K \to R^n \xrightarrow{\varepsilon} M \to 0\,,$$

where K is the kernel of the map $\epsilon : e_i \mapsto f_i, i = 1, \ldots, n$. Here

$$e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i \qquad \text{and} \qquad K = \{ \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} \in R^n \mid r_1 f_1 + \ldots r_n f_n = 0\}\,.$$

Elements of K are called "syzygies of M", and the module K is called the "first syzygy of M" (with respect to the given presentation $\varepsilon : R^n \twoheadrightarrow M$) and is denoted $\operatorname{Syz}_1^R M$. The notation is somewhat imprecise, as the module depends on the presentation. Fortunately, $\operatorname{Syz}_1^R M$ is well defined "up to free summands". Indeed, Schanuel's Lemma states:

prop:Schanuel

Proposition 3.2. *Let*

$$0 \to K \to F \to M \to 0 \qquad \textit{and} \qquad 0 \to L \to G \to M \to 0$$

be exact sequences, in which both F and G are projective modules. Then $K \oplus G \cong L \oplus F$.

We can take syzygies of syzygies, and so on: Let $\operatorname{Syz}_2(M) = \operatorname{Syz}_1(\operatorname{Syz}_1(M))$, and, in general, $\operatorname{Syz}_{n+1}(M) = \operatorname{Syz}_1(\operatorname{Syz}_n(M))$. Do we eventually get a free module as an n^{th} syzygy?

eg:Koszul2

Example 3.3. Let $R = \mathsf{k}[x,y]$, where k is a field, and let $M = R/(x,y) \cong \mathsf{k}$. Obviously $\operatorname{Syz}_1 M$ is the ideal (x,y). Let us compute $\operatorname{Syz}_2 M = \operatorname{Syz}_1(x,y)$. We have the exact sequence

$$0 \to \operatorname{Syz}_2 M \to R^2 \to (x,y) \to 0\,,$$

where the map $R^2 \to (x,y)$ takes $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ to x and $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$ to y. As in Equation (**??**), we have $\left[\begin{smallmatrix}-y\\x\end{smallmatrix}\right] \in \operatorname{Syz}_2 M$. In fact, $\operatorname{Syz}_2(x,y)$ is generated by $\left[\begin{smallmatrix}-y\\x\end{smallmatrix}\right]$ and hence is a free module (of rank one). To see this, suppose $\left[\begin{smallmatrix}f\\g\end{smallmatrix}\right] \in \operatorname{Syz}_1(x,y)$. Then $xf + yg = 0$, so $x \mid yg$. Since R is a unique factorization domain and x and y are relatively prime, it follows that $x \mid g$, say, $g = xh$. Now $xf + yxh = 0$, so $f + yh = 0$. Therefore $\left[\begin{smallmatrix}f\\g\end{smallmatrix}\right] = h\left[\begin{smallmatrix}-y\\x\end{smallmatrix}\right]$.

The following exact sequence (a *free resolution* of M), encodes all of this information:

$$0 \leftarrow M \leftarrow R \xleftarrow{[x\ y]} R^2 \xleftarrow{\left[\begin{smallmatrix}-y\\x\end{smallmatrix}\right]} R \leftarrow 0\,.$$

I arranged the maps from right to left in order to make matrix multiplication (representing composition of maps) more transparent. The first syzygy is the image of $\left[\begin{smallmatrix} x & y \end{smallmatrix}\right]$, and the second syzygy is the image of $\left[\begin{smallmatrix} -y \\ x \end{smallmatrix}\right]$. The condition that we eventually get a free module as an n^{th} syzygy amounts to the condition that M has a finite free resolution.

eg:Koszul3 **Example 3.4.** Let $R = \mathsf{k}[x,y,z]$, and let $M = R/(x,y,z) \cong \mathsf{k}$. Again, we get a free resolution, this time of length three:

$$0 \leftarrow M \leftarrow R \xleftarrow{\left[\begin{smallmatrix} x & y & z \end{smallmatrix}\right]} R^3 \xleftarrow{\left[\begin{smallmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{smallmatrix}\right]} R^3 \xleftarrow{\left[\begin{smallmatrix} x \\ y \\ z \end{smallmatrix}\right]} R \leftarrow 0\,.$$

The third syzygy $\operatorname{Syz}_3 M$ is a free module.

Of course the modules M in the examples above are in some sense the simplest interesting R-modules. The remarkable thing is that similar behavior is exhibited by *every* module over a polynomial ring, in any number of variables.

Here is a modern version of Hilbert's Syzygy Theorem:

thm:HST **Theorem 3.5.** *Let M be a finitely generated module over the polynomial ring $\mathsf{k}[x_1,\dots,x_n]$ over a field k. Then M has a free resolution of length at most n, that is, there is an exact sequence*

$$0 \leftarrow M \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_m \leftarrow 0\,.$$

in which each F_i is a free R-module and $m \le n$. In other words, $\operatorname{Syz}_m M$ *is free for some $m \le n$.*

Hilbert did not actually prove this; his proof applied only to graded modules. The statement above includes the assertion that projective modules are free over $\mathsf{k}[x_1,\dots,x_n]$. This assertion was known as *Serre's Conjecture* and inspired and motivated two decades of deep and important discoveries. It was finally proved independently by Quillen and Suslin in 1976.

We conclude with a couple of examples where *none* of the syzygies $\operatorname{Syz}_n M$ is free, that is, the free resolution goes on forever. (In fact, this behavior is typical; polynomial rings are very special in this regard.)

eg:4 **Example 3.6.** Let $R = \mathbb{Z}/(4)$, and let $M = R/(2) \cong \mathbb{Z}/(2)$. The free resolution of M is

$$0 \leftarrow M \leftarrow R \overset{2}{\leftarrow} R \overset{2}{\leftarrow} R \overset{2}{\leftarrow} R \leftarrow \dots\,.$$

eg:cusp **Example 3.7.** Let $R = \mathbb{C}[t^2, t^3]$, the ring of polynomials with no linear term, and let $M = R/(t^2,t^3) \cong \mathbb{C}$. After one step, the free resolution of M becomes periodic with period two:

$$0 \leftarrow M \leftarrow R \xleftarrow{\left[\begin{smallmatrix} t^2 & t^3 \end{smallmatrix}\right]} R^2 \xleftarrow{\left[\begin{smallmatrix} t^3 & -t^4 \\ -t^2 & t^3 \end{smallmatrix}\right]} R^2 \xleftarrow{\left[\begin{smallmatrix} t^3 & t^4 \\ t^2 & t^3 \end{smallmatrix}\right]} R^2 \xleftarrow{\left[\begin{smallmatrix} t^3 & -t^4 \\ -t^2 & t^3 \end{smallmatrix}\right]} R^2 \xleftarrow{\left[\begin{smallmatrix} t^3 & t^4 \\ t^2 & t^3 \end{smallmatrix}\right]} R^2 \leftarrow \dots\,.$$

In these examples the ranks of the free modules in the minimal resolutions are bounded. Even this behavior is far from typical and, roughly speaking, happens only when the ring is defined by a single equation. Over the ring $\mathsf{k}[t^4,t^5,t^6]$, for example, the ranks of the free modules in the minimal resolution of k grow linearly; and over $\mathsf{k}[t^3,t^4,t^5]$ they grow exponentially.

For more information on syzygies, see my paper [**?**].

References

[1] D. Hilbert, Über der Theorie der algebraischen Formen. *Math. Ann.* **36** (1890), 473–534.
[2] E. Noether, Idealtheorie in Ringbereichen, *Math. Ann.* **83** (1921), 24–66.
[3] R. Wiegand, What is ... a syzygy? *Notices Amer. Math. Soc.* **53** (2006), 456–457.