Numerical invariants of ideals and modules

In our quest to understand properties of ideals, modules naturally occur, and are the more natural setting to study certain numerical properties of the objects we will be mostly concerned about: quotient rings $\mathbb{k}[x_1, \dots, x_n]/I$ of a polynomial ring by an ideal.

Usually, working with homogeneous ideals provides us with many advantages, and the results for the homogeneous case can often be translated to the non-homogeneous case (but not always, and geometrically there are important differences).

Let $R := \mathbb{k}[x_1, \dots, x_n]$ be our polynomial ring. We can grade it by degree, and $R := \bigoplus_{d \geq 0} R_d$, where

R_d is the $\mathbb{k}$-vector space of polynomials of degree d (zero has every degree). Note that $R_0 = \mathbb{k}$ in our case.

Definition (Graded module): given a graded ring R, a graded module over R is an R-module M with a grading $M = \bigoplus_{i \in \mathbb{Z}} M_i$ where $R_j M_i \subseteq M_{i+j}$

for all $i \in \mathbb{Z}$, $j \in \mathbb{N}$.

Examples:

- R^n is a graded R-module
- $I \subseteq R$ a homogeneous ideal is also a graded R-module
- if $I \subseteq R$ is a homogeneous ideal, then R/I is a graded R-module

Given a graded R-module M, we can construct another module $M(d)$ by simply "shifting" the degrees of M d steps. More precisely $M(d)$ is the graded R-module defined by its graded pieces as:

$$M(d)_e := M_{d+e}.$$

This will be very useful for us to "break down" maps between graded R-modules into (many) maps between $\mathbb{k}$-vector spaces.

From now until the end of the lecture, $R := \mathbb{k}[x_1, \dots, x_n]$ will denote our polynomial ring.
The definition of grading leads us to our first numerical invariant:

Definition (Hilbert function): let M be a finitely generated graded R-module. The function

$$HF_M : \mathbb{Z} \to \mathbb{N} \text{ given by } HF_M(t) := \dim_{\mathbb{k}} M_t$$

is called the Hilbert function of M.
(these dimensions are all finite since M is finitely generated)

Hilbert's insight (which also appeared in his 1890 paper!) is that all the information of the function HF_M can be extracted from finitely many values.

Theorem 1 (Hilbert function becomes a polynomial): if M is a finitely generated graded R-module (recall that $R = \mathbb{k}[x_1, \dots, x_n]$) then, there is $t_0 \in \mathbb{N}$ and a polynomial $HP_M(t) \in \mathbb{Q}[t]$ with $\deg P_M \leq n-1$ s.t.

$$HF_M(t) = HP_M(t) \quad \forall\, t \geq t_0.$$

The polynomial $HP_M(t)$ is called the Hilbert polynomial of M.

To prove the above theorem, we will use the following lemma, which you'll prove in your homework 2.

Lemma 1: let $H : \mathbb{N} \to \mathbb{Z}$ be a function such that its "first difference" $H'(s) := H(s) - H(s-1)$ agrees with a polynomial $Q'(s) \in \mathbb{Q}[s]$ with $\deg Q < n-1$ when $s \geq s_0$. Then $H(t)$ agrees with a polynomial $Q(t) \in \mathbb{Q}[t]$ with $\deg Q < n$ for all $t \geq s_0$.

Proof of Theorem 1: we will prove the theorem by induction on n, the number of variables of our polynomial ring R. When $n = 0$ (i.e. $R = \mathbb{k}$) then M is simply a finite dimensional vector space $\therefore HF_M(s) = 0$ for all large enough s, which is a polynomial of degree -1.
Now, suppose the theorem holds for polynomial rings with $\leq n-1$ variables. Let $\varphi_n : M \to M$ be the "multiplication by x_n" map, i.e. $\varphi_n(m) = x_n \cdot m$. Let $K = \ker \varphi_n$. Then we get the following exact sequence of graded R-modules

$$0 \to K(-1) \to M(-1) \xrightarrow{\varphi_n} M \to M/x_nM \to 0$$

(inclusion; inclusion map; quotient map; zero map)

Taking the component of degree s of each of the above modules, we have the exact sequence of $\mathbb{k}$-vector spaces

$$0 \to K(-1)_s \to M(-1)_s \to M_s \to M_s/x_nM_{s-1} \to 0$$

$$\Rightarrow 0 = \dim_{\mathbb{k}} K(-1)_s - \dim_{\mathbb{k}}(M(-1)_s) + \dim_{\mathbb{k}} M_s - \dim_{\mathbb{k}}\left(M_s/x_nM_{s-1}\right)$$

$$\Rightarrow HF_M(s) - HF_M(s-1) = HF_{M/x_nM}(s) - HF_K(s-1)$$

now note that both M/x_nM and K are isomorphic to modules over $\mathbb{k}[x_1, \dots, x_{n-1}]$ $\therefore \exists\, s_0 \in \mathbb{N}$ s.t. both HF_{M/x_nM} and HF_K agree with a polynomial of degree $< n-1$ $\therefore$ by Lemma 1 we have that $HF_M(t)$ agrees with a polynomial of degree $< n$ for $t \geq s_0$. □

The above proof is quite different than the one given by Hilbert, and Hilbert's original proof provides us with a lot more information which will be useful to us quite soon. Moreover Hilbert's proof provides us with another way to compute Hilbert functions via linear algebra in certain larger (but simpler) vector spaces.

Definition (complexes): a <u>complex</u> $\mathcal{F}$ of R-modules is a sequence of modules F_i with maps $F_i \xrightarrow{\partial_i} F_{i-1}$ such that $\operatorname{Im}(\partial_{i+1}) \subseteq \ker(\partial_i)$.

$$\mathcal{F} : F_0 \xleftarrow{\partial_1} F_1 \xleftarrow{\partial_2} F_2 \xleftarrow{\partial_3} \cdots$$

The <u>homology</u> of $\mathcal{F}$ at F_i is defined by

$$H_i(\mathcal{F}) := \ker \partial_i / \operatorname{Im} \partial_{i+1}.$$

As modules are complicated objects, it is often a good idea (as pioneered by Hilbert) to understand them via simpler objects (along with maps between them). This lead Hilbert to the definition of the following special type of complexes.

Definition (free resolution): a <u>free resolution</u> of an R-module M is a complex

$$\mathcal{F}_M : 0 \leftarrow M \xleftarrow{\partial_0} F_0 \xleftarrow{\partial_1} F_1 \xleftarrow{\partial_2} F_2 \leftarrow \cdots$$

where

1. each F_i is a free module (i.e. $F_i = R^{n_i}$ for some $n_i \in \mathbb{N}$)
2. $\operatorname{Im}(\partial_0) = M$
3. $\mathcal{F}$ is exact at each F_i, i.e. $\ker \partial_i = \operatorname{Im} \partial_{i+1}$ $\forall\, i \in \mathbb{N}$.

When M is a graded R-module, a <u>graded free resolution</u> of M is a free resolution where the maps ∂_i are also of degree 0 (i.e. they map $(F_i)_d$ to $(F_{i-1})_d$) for all $i \in \mathbb{N}$.

If for some $r \in \mathbb{N}$ we have that $F_{r+1} = 0$ but $F_i \neq 0$ for all $i \leq r$ then we say that $\mathcal{F}$ is a finite resolution of length r.

It is easy to see that every module has a free resolution, and every graded module has a graded free resolution.
What is amazing (and this was one of the hall of fame results of Hilbert) is that when $R = \mathbb{k}[x_1, \dots, x_n]$ (the case of most interest for us) every f.g. graded module has a finite graded free resolution!

Theorem 2 (Hilbert syzygy theorem): if $R := \mathbb{k}[x_1, \dots, x_n]$ then every finitely generated graded R-module has a finite graded free resolution of length $\leq n$, by finitely generated free modules.

Hilbert used theorem 2 to provide a method (via linear algebra) to compute Hilbert functions (and to prove theorem 1)

Hilbert's proof of theorem 1 (via theorem 2): let $R := \mathbb{k}[x_1, \dots, x_n]$. If $M = R(d)$, for some $d \in \mathbb{Z}$, then

$$HF_M(s) = HF_R(s+d) = \binom{s+d+r-1}{r-1}$$

which agrees for $s \geq -(d+r-1)$ with a polynomial in s of degree $r-1$ and rational coefficients.
If F is a finitely generated graded free module, then $F := \bigoplus_{i=1}^{a} R(d_i)^{e_i}$ $\therefore$

$$HF_F(s) = \sum_{i=1}^{a} e_i \cdot HF_{R(d_i)}(s) = \sum_{i=1}^{a} e_i\, HF_R(s+d_i).$$

Theorem 2 shows that any finitely generated graded free module M has a finite graded free resolution

$$\mathcal{F} : 0 \leftarrow M \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_n \leftarrow 0$$

$$\therefore HF_M(s) = \sum_{i=0}^{n} (-1)^i HF_{F_i}(s)$$

which is a linear combination of functions which eventually become polynomials of degree $\leq r-1$ □

In subsequent lectures we will study more properties of free resolutions and see numerical and geometric information arising from such resolutions.