I. Polynomial Rings: $R = k[x_0, \ldots, x_n]$.

A: Internal structure of R**:**

$a)$ Homogeneous Ideals, Chains of primes, height of a prime, Krull dimension of a ring, primary decomposition, regular sequences, principal ideal theorem

We will primarily think of the polynomial ring as a graded ring, $R = \oplus R_i$, where R_i is the k-vector space spanned by the monomials in R of degree i. Elements of R_i are called *forms of degree* i. R_i is a vector space over k of dimension $\binom{n+i}{i} = \binom{n+i}{n}$.

Notice that if we define the polynomial $f_i(x) \in \mathbb{Q}[x]$ by

$$f_i(x) = \binom{x}{i} := (1/i!)x(x-1)\cdots(x-(i-1)) \text{ for } i \geq 1, \text{ and } \binom{x}{0} = 1,$$

then f_i is a polynomial of degree exactly i and so the f_i are a basis for $\mathbb{Q}[x]$ as a $\mathbb{Q}$-vector space. One should also notice that $f_n(d+n)$ gives the dimension of R_d, for R as above. Thus, the dimensions of the vector spaces R_d grow as a polynomial function of degree n in d.

Since we are thinking of R as a graded ring, we will (mostly) be interested in *graded*, or *homogeneous*, ideals of R, i.e. ideals I such that if $I \cap R_d$ is denoted I_d then $I = \oplus I_d$.

If we denote by $\mathbb{P}^n(k)$ the projective space "built" on the vector space $V = k^{n+1}$, then a *point* $P = [a_0 : \ldots : a_n]$ of this $\mathbb{P}^n$ is the equivalence class of elements of $V - \{(0, \ldots, 0)\}$ which consists of all the vectors $\lambda(a_0, \ldots, a_n)$, $\lambda \in (k - 0)$.

Although the elements of R define k-valued functions on V, only the constant polynomials define k-valued functions on $\mathbb{P}^n$. Nevertheless, whenever $F \in R_i$ we have

$$F(\lambda a_0, \ldots, \lambda a_n) = \lambda^i F(a_0, \ldots, a_n) .$$

So, one can say whether or not F vanishes at P. If it does we call P a *zero* of F.

More generally, if $I = \oplus_d I_d$ is a homogeneous ideal then the *zero set* of I (denoted $Z(I)$) is defined by

$$Z(I) := \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ for all } F \in I_d \text{ and for all } d\}.$$

The subsets of $\mathbb{P}^n$ of the form $Z(I)$, where I is a homogeneous ideal in R, may be considered as the closed sets for a topology on $\mathbb{P}^n$ called the *Zariski topology.*

If $G \in I$ then G has a unique decomposition

$$G = \oplus_{d=0}^{\infty} G_d \text{ where } G_d \in R_d \text{ and almost all } G_d = 0.$$

From this it is easy to see that $G(P) = 0 \Leftrightarrow G_d(P) = 0$ for all $d = 0, 1, \ldots$.

Notice that $Z(I)$ doesn't uniquely determine I since it is clear that if we let $\sqrt{I}$ denote the *radical* of I i.e.

$$\sqrt{I} = \{g \in R \mid g^s \in I \text{ for some } s\}$$

then

1) I homogeneous $\Rightarrow \sqrt{I}$ homogeneous and
2) $Z(I) = Z(\sqrt{I})$.

In fact, if k is an algebraically closed field then (one) version of the *Hilbert Nullstellensatz* says:

Theorem:

$$Z(I) = Z(J) \Leftrightarrow \sqrt{I} = \sqrt{J}\ .$$

There is a unique homogeneous maximal ideal of R, namely $m = (x_0, \ldots, x_n)$ and it is usually referred to as the *irrelevant* maximal ideal since it's zero set in $\mathbb{P}^n(k)$ is empty. We'll see later that, from the algebraic point of view, and even from a geometric point of view, the ideal is far from "irrelevant"!

Definition: Let $\wp$ be a prime ideal of R. We define the *height* of $\wp$ to be the integer t (if it exists), and write $ht\ \wp = t$, if we can find prime ideals $\wp_i$ such that

$$\wp = \wp_t \supsetneq \wp_{t-1} \supsetneq \cdots \supsetneq \wp_1 \supsetneq \wp_0 = (0).$$

and no longer such chain can be found.

We can make this definition in any commutative ring, not just the polynomial ring R, by writing, instead of $\wp_0 = (0)$, $\wp_0$ is a minimal prime ideal of the ring.

We now recall a few facts:

Definition-Theorem: A ring A is called *noetherian* if either of the following equivalent conditions holds in A:

1) Every ideal of A is *finitely generated* (f.g.);
2) Every ascending chain of ideals of A stabilizes (ACC).

It is a very important fact, called the *Hilbert Basis Theorem*, that:

Theorem: If A is a noetherian ring so is $A[x]$. In particular, $k[x_0, \ldots, x_n]$ is a noetherian ring.

There are many things that are true for noetherian rings that are not true in general for arbitrary rings, so it is important to know which operations preserve this property. Hilbert's Basis Theorem says that passing to a polynomial ring preserves the property. There are other things we can do that preserve the property:

Theorem: Let A be a noetherian ring, I an ideal of A and S a multiplicatively closed subset of A then both A/I and $S^{-1}A$ are noetherian rings.

Some of the first nice properties that hold for noetherian rings come from the following:

Theorem: In a noetherian ring every prime ideal has finite height.

We can use the idea of "height" to give a (first) notion of *dimension* for a commutative ring.

Definition: Let A be a ring. The *Krull dimension of A*, denoted K-dim A, is

$$\text{K-dim} A \;:= \max\{\ ht\ \wp \quad | \quad \wp \quad \text{is prime in} \quad A\}$$

In spite of the fact that in a noetherian ring every prime has finite height, there are noetherian rings of infinite Krull dimension (Nagata).

Nevertheless, we have:

Theorem: If $R = k[x_0, \ldots, x_n]$ then:

1) K-dim $R = n + 1$;

2) If m is a maximal ideal of R then $ht\ m = n + 1$;

3) If, in addition, k is algebraically closed and m is maximal then $m = (x_0 - a_0, \dots, x_n - a_n)$ where the $a_i \in k$;

4) If $\wp$ is a prime ideal of R of height d then the Krull dimension of $R/\wp$ is exactly $n+1-d$ (i.e. every prime ideal of R is part of a chain of prime ideals of maximal length ($= n+1$) in R).

We extend our definition of *height* so as to apply it to any ideal of A.

Definition: Let I be an ideal of A then $ht\ I$ is defined as:

$$ht\ I \ := \min\{ \ ht\ \wp \ \mid \ \wp \supset I \ \}.$$

By Gauss' Lemma we know that $R = k[x_0, \dots, x_n]$ is a Unique Factorization Domain (UFD). Thus, if $f \in R$ then $f = f_1^{\alpha_1} \cdots f_s^{\alpha_s}$ where the f_i are irreducible. Again using the fact that R is a UFD we have that the ideals (f_i) are all prime ideals of height 1. Clearly $(f) \subseteq (f_i)$ and so $ht(f) = 1$ also. In fact, $(f) = (f_1)^{\alpha_1} \cap \cdots \cap (f_s)^{\alpha_s}$.

It is also easy to see that if $(f) \subseteq \wp$, where $\wp$ is a prime ideal, then $\wp \supseteq (f_i)$ for some i. Thus, the $(f_i) = \wp_i$ are *minimal primes* with respect to containing (f). They are called the *minimal primes of* (f). In this case we see that all the minimal primes of (f) have the same height. We say that (f) is *height unmixed.*

Example:

Consider the ideal $I = (xy, xz) \subset k[x, y, z]$. $I = (x) \cap (y, z)$ and both (x) and (y, z) are prime ideals. These are easily shown to be the minimal primes of I (as above) but they have different heights. This ideal is *not* height unmixed.

These considerations lead very naturally to the following notions.

Definition: An ideal I in the ring A is called *primary* if whenever $fg \in I$ then $f \in I$ or $g^n \in I$ for some integer n.

It is a simple exercise to show that if I is primary in A then $\sqrt{I}$ is a prime ideal. This motivates:

Definition: If I is a primary ideal and $\wp = \sqrt{I}$ is the prime ideal which is its radical then we say that *I is a $\wp$-primary ideal.*

Notes:

1) For R a UFD and f an irreducible element of R then (f^n) is an (f)-primary ideal.

2) If I and J are both $\wp$-primary ideals of A then so is $I \cap J$.

3) If $\sqrt{I} = m$ is a maximal ideal of A then I is an m-primary ideal. In general, if $\sqrt{I}$ is a prime ideal that does not mean that I is primary. E.g. consider $I = (x^2, xy, xz)$. Clearly if $\wp \supset I$ then $\wp \supset (x)$, so $(x) = \sqrt{I}$ is prime. But, clearly I is not radical since $xy \in I$ and $x \notin I$ and y^n is not in I for any n, since every element of I has a factor of x.

4) If $\wp$ is a prime ideal and $\wp^r$ is primary, then it is $\wp$-primary. But, in general, $\wp^r$ is not primary.

We can now state a theorem which shows that, in any noetherian ring, there is an analogy to the geometric fact that every variety is a union of irreducible varieties.

Theorem: (*primary decomposition*) Let A be a noetherian ring and I any ideal of A. Then I can be written:

$$I = q_1 \cap \cdots \cap q_s \quad \text{where} \quad q_i \quad \text{is} \quad \wp_i\text{-primary and,} \quad q_i \not\supseteq \cap_{j \neq i} q_j \ .$$

Moreover, the set $\{\wp_1, \ldots, \wp_s\}$, whose elements are called the *associated primes of I*, is uniquely determined by I.

If $\{\wp_1, \cdots, \wp_t\}$ are the minimal elements (using the ordering given by inclusion) among the associated primes of I, then the primary ideals $\{q_1, \ldots, q_t\}$ are also uniquely determined by I.

Notes:

1) The $\wp_i$, $i = 1, \ldots, t$ are also minimal in the sense we mentioned earlier, i.e. if $\wp$ is a prime ideal of A and $\wp \supseteq I$ then $\wp \supseteq \wp_i$ for some i with $1 \leq i \leq t$. Thus, $\cap_{i=1}^{t} \wp_i = \sqrt{I}$.

2) The q_i above are called the *primary components* of I and the associated primes $\wp_i$, for $i = 1, \ldots, t$, are called the *minimal associated primes of I*. The remaining associated primes are called *embedded* and the primary components associated to them (not uniquely) are called the *embedded primary components.*

3) If I is a *homogeneous* ideal in a graded ring then the associated primes are also all homogeneous prime ideals and the primary components are always homogeneous as well.

4) If I is a homogeneous ideal in $k[x_0, \ldots, x_n]$ (where k is an algebraically closed field) then $Z(I)$ is the union of $Z(\wp_i)$ where the $\wp_i$ are the minimal associated primes of I. These primes describe "what you see". I.e. the $Z(\wp_i)$ are the irreducible algebraic sets into which $Z(I)$ decomposes.

5) The fact that a particular minimal primary component is not necessarily prime corresponds to the fact that "what you see" is not really what you want to describe.

In the case where I is a homogeneous ideal in $k[x_0, \ldots, x_n]$ with primary decomposition given (say) as above, we see that by concentrating only on the zeroes of I we lose something; we lose the fact that a given primary component may not be prime. Worse yet, we lose the embedded components completely! Less drastic, but a real loss nonetheless, is that we definitely lose the irrelevant component of I (i.e. the primary component, if it's there, whose associated prime is the irrelevant ideal).

The notion of a *closed subscheme of* $\mathbb{P}^n$ is the (latest) attempt to deal with this problem. Closed subschemes of $\mathbb{P}^n$ are in 1-1 correspondence with those homogeneous ideals in $k[x_0, \ldots, x_n]$ which don't have an irrelevant component.

The primary decomposition of an ideal also permits us to give a good algebraic description of certain algebraic features of the ring A/I.

Proposition: Let A and I be as above where $I = q_1 \cap \ldots \cap q_s$ is the primary decomposition of I. Then:

i) $\bar{x}$ is a nilpotent element of $A/I \Leftrightarrow x \in \cap_{i=1}^{s} \wp_i = \cap_{i=1}^{t} \wp_i = \sqrt{I}$;

ii) $\bar{x}$ (not a unit) is a zero divisor in $A/I \Leftrightarrow x \in \wp_i$ for some i, $1 \le i \le s$ (we say that the zero divisors on A/I are the union of the associated primes of I.)

Note:

If $R = k[x_0, \ldots, x_n]$ and I is a homogeneous ideal of R and $A = R/I$, then we can find a non-constant form $F \in R$ for which $\bar{F}$ is not a zero-divisor in A if and only if $m = (x_0, \ldots, x_n)$ is not an associated prime of I.

This simple observation is the basis of a "profound" study which is, essentially, due to M. Auslander and D. Buchsbaum (although begun earlier, in a non-homological way by Groebner, Rees and Northcott.)

Let me start with a non-standard definition.

Definition: A homogeneous ideal $I \subset R = k[x_0, \dots, x_n]$ is called a *saturated ideal* if and only if the irrelevant maximal ideal of R is not an associated prime of I.

We'll see equivalent definitions later, e.g. in Juan's lecture.

From what we said above, I is a saturated ideal if and only if $A = R/I$ contains a homogeneous non-zero-divisor of degree > 1.

We continue to develop this idea with the following definition:

Definition: 1) Let $F_1, \dots, F_r$ be non-constant forms of R and I a homogeneous ideal of R.

We say that $F_1, \dots, F_r$ are a *regular sequence modulo* I or *give rise to a regular sequence in* R/I if and only if

i) $(I, F_1, \dots, F_r) \subseteq m$;

ii) $\bar{F}_1$ is not a zero divisor in R/I;

iii) $\bar{F}_i$ is not a zero divisor in $R/(I, F_1, \dots, F_{i-1})$ for $1 < i \leq r$.

From what we have seen above, another way to say this is the following:

$$F_1 \notin \text{the union of the associated primes of } I;$$

$$F_2 \notin \text{ the union of the associated primes of } (I, F_1);$$
$$\dots$$
$$F_i \notin \text{ the union of the associated primes of } (I, F_1, \dots, F_{i-1});$$
$$\dots$$
$$F_r \notin \text{ the union of the associated primes of } (I, F_1, \dots, F_{r-1}).$$

2) $F_1, \dots, F_r$ is called a *maximal regular sequence modulo* I if $F_1, \dots, F_r$ is a regular sequence modulo I which can not be lengthened i.e. $(I, F_1, \dots, F_r)$ is not a saturated ideal.

Remark: I have only given the notion of a regular sequence modulo an ideal I, but the notion is much more general. One can discuss the idea of an element of R being a non-zero divisor on a module M. I didn't want to go into all of that here in these notes, but it is a very fruitful idea which it is necessary to understand. In fact, the notion of a regular sequence modulo I becomes nothing more than the special case of a regular sequence on $M = R/I$.

To appreciate this idea of a regular sequence we need to recall another fundamental fact about noetherian rings.

Theorem: (Krull's Principal Ideal Theorem)

Let A be a noetherian ring and $I = (f)$ a principal ideal. Then $ht\ I \leq 1$. Moreover, $ht\ I = 0$ if and only if f is in a minimal prime ideal of A. In this case f belongs to an associated prime ideal of the ideal (0) in A.

It follows immediately from Krull's P.I. Theorem that:

if F (a form) is not in any associated prime of $I \subset R = k[x_0, \dots, x_n]$
then $ht\ (\bar{F}) = 1$ in R/I, i.e. $ht\ (I, F) = ht\ I + 1$ in R.

It follows that maximal regular sequences exist modulo I for $I \subset R = k[x_0, \dots, x_n]$. In fact:

If $F_1, \dots F_r$ give rise to a maximal regular sequence modulo I then

$$r \leq \text{K-dim } A$$

.

Some non-obvious facts about regular sequences are:

Theorem: Let $R = k[x_0, \dots, x_n]$ and $F_1, \dots, F_s$ nonconstant forms of R and I a homogeneous ideal of R.

$i)$ If $F_1, \dots, F_s$ are a regular sequence modulo I and σ a permutation of $\{1, \dots, s\}$ then $F_{\sigma(1)}, \dots, F_{\sigma(s)}$ is a regular sequence modulo I.

$ii)$ All maximal regular sequences modulo I have the same length.

Obviously, we now have a rather subtle integer invariant that we can attach to the ideal I or rather to the quotient module $A = R/I$.

Definition: Let I be a homogeneous ideal of $R = k[x_0, \dots, x_n]$.

The *depth of* R/I is the length of a maximal regular sequence modulo I.

Through a slight abuse of language we sometimes say this is the length of a maximal regular sequence in R/I. Given my remarks above, we can also say that this is the length of a maximal regular sequence in R on $M = R/I$.

As we noted above,

$$\text{depth}(R/I) \leq \text{K-dim } R/I.$$

As always when there is an inequality, the case of equality will bear notice.

Definition: I is called a *Cohen-Macaulay* ideal of R (equivalently, $A = R/I$ is called a *Cohen-Macaulay ring, CM ring*) if $\text{depth}(R/I) = \text{K-dim } R/I$.

Examples:

1) $R = k[x_0, \dots, x_n]$ is a CM ring since $\{x_0, \dots, x_n\}$ is a regular sequence of length $n+1$ – which is the Krull dimension of R.

2) If $F_1, \dots, F_r$ are a regular sequence in $R = k[x_0, \dots, x_n]$ and $I = (F_1, \dots, F_r)$ then $A = R/I$ is a CM ring. This follows from the fact that any regular sequence can be extended to a maximal regular sequence.

3) If F_1 and F_2 are two nonconstant forms in R which have no common factor then they form a regular sequence.

4) If $I \subset R$ is a saturated ideal of height n then $A = R/I$ is a CM ring. This applies, in particular, to any saturated ideal whose radical is the ideal of a finite set of points in $\mathbb{P}^n$, and more specifically to the ideal of a set of points itself.

5) (*The rational normal curve in* $\mathbb{P}^3$) Consider the map from $\mathbb{P}^1$ to $\mathbb{P}^3$ given by:

$$[s : t] \to [s^3 : s^2t : st^2 : t^3]$$

(where we will use coordinates $R = k[x, y, z, w]$ for the homogeneous coordinate ring of $\mathbb{P}^3$). It is not hard to show that the ideal of all forms vanishing on the image of this map, we'll call it the curve $\mathcal{C}$, is given by the ideal $\wp = (yw - z^2, yz - xw, xz - y^2)$. Then $A = R/\wp$ is the homogeneous coordinate ring of $\mathcal{C}$, $ht\wp = 2$ and $K\text{-dim}(R/\wp) = 2$.

If we let $L = x - z$ then the hyperplane of $\mathbb{P}^3$ defined by L meets $\mathcal{C}$ in the three points $P_1 = [0 : 0 : 0 : 1]$, $P_2 = [1 : 1 : 1 : 1]$ and $P_3 = [-1 : 1 : -1 : 1]$. The defining ideals of these three points is $\wp_1 = (x, y, z)$, $\wp_2 = (x - w, y - w, z - w)$ and $\wp_3 = (x + w, y - w, z + w)$.

Consider $J = (L, \wp) = (x - z, yw - z^2, yz - xw, xz - y^2)$ and $I = \wp_1 \cap \wp_2 \cap \wp_3$. One can easily check that $I = J$ (use CoCoA e.g.) and hence one can find another linear form which is not a zero divisor module J. Thus the ring A is Cohen Macaulay.

6) (*rational quartic curve in* $\mathbb{P}^3$) With the same notation as in example 5, now consider the map from $\mathbb{P}^1$ to $\mathbb{P}^3$ given by

$$[s : t] \to [s^4 : s^3t : st^3 : t^4] \ .$$

This time the image curve, call it $\mathcal{C}$, has defining prime ideal $\wp = (xw - yz, z^3 - yw^2, y^2w - xz^2, x^2z - y^3)$. Now if we consider the hyperplane defined by $L := 2x - 5y + 5z - 2w$ then that hyperplane meets $\mathcal{C}$ in 4 points: $P_1 = [1 : 1 : 1 : 1]$, $P_2 = [1 : -1 : -1 : 1]$, $P_3 = [16 : 8 : 2 : 1]$ and $P_4 = [1 : 2 : 8 : 16]$.

If we let I be the ideal of these four points and let $J = (L, \wp)$ as before, this time we find (using the Hilbert function of the four points) that there are 6 independent quadrics in the ideal I while J has (at most) 5 independent quadrics (in fact, exactly 5). Thus $I \neq J$ and so J is not saturated and we cannot find another non-zero divisor in R/J. So, R/J is not a Cohen Macaulay ring.

A very important (and useful) fact, which generalizes what we saw for principal ideals in the polynomial ring, is the following:

Theorem: Let $R = k[x_0, \ldots, x_n]$ and suppose that $A = R/I$ is a CM ring. Any ideal of A generated by a regular sequence is height unmixed.

More generally, if I is generated by a regular sequence then I^t is height unmixed.

Example:
Suppose the $P_1, \ldots, P_{mn}$ are mn distinct points of $\mathbb{P}^2$ which are the points of intersection of a curve of degree m and a curve of degree n. Let F and G be the equations of these curves. Then $I = (F, G) = \wp_1 \cap \ldots \cap \wp_{mn}$ is the primary decomposition of I where the ideals $\wp_i$ are the prime ideals of $k[x_0, x_1, x_2]$ which correspond to the points P_i. Recall that $\wp_i = (L_1, L_2)$, where L_1 and L_2 are linearly independent linear forms, and so each $\wp_i$ is generated by a regular sequence.

From the discussion above we get that:

$$I^t = \wp_1^t \cap \ldots \cap \wp_{mn}^t$$

If, instead, I were the ideal of an arbitrary set of s points in $\mathbb{P}^2$ then we would still have that $I = \wp_1 \cap \ldots \cap \wp_s$ but now we could only say that

$$I^t = \wp_1^t \cap \ldots \cap \wp_s^t \cap q$$

where q is an irrelevant component.

Since, in a noetherian ring any ideal contains a power of its radical, we get that $m^r \subseteq q$ ($m = (x_0, x_1, x_2)$). We then conclude that, for $\ell >> 0$ we have

$$(I^t)_\ell = (\wp_1^t \cap \ldots \cap \wp_s^t)_\ell$$

It's not clear how small ℓ can be chosen in order to have this equality.

Remark: I have deliberately stated most of the theorems above in the context of the polynomial ring, rather than in a more general context (e.g. for local rings). This is largely because I wanted to avoid some difficulties. The student should not assume that the results here are ONLY true for polynomial rings over a field. That special case is by far the most important example we have to deal with, but it shares many characteristics with more general rings. For the more general framework one should consult one of the standard texts in commutative algebra, of which there are several good ones.

B: R-modules

a) Graded modules

As we mentioned above, our main interest in these notes will be in quotients of $R = k[x_0, \ldots, x_n]$ with k a field (considered as a graded ring in the usual way) by homogeneous ideals I. These graded rings have a special property: they are k-algebras which are generated, as an algebra, by their forms of degree 1. Such k-algebras have been referred to in the literature as *standard.*

The modules we will consider over these rings will also be, in general, graded modules. I.e. if $A = R/I = \oplus_{i=0}^{\infty} A_i$, then a *graded* A-module M will be an A-module M such that $M = \oplus_{i \in \mathbb{Z}} M_i$ and the A-module action of A on M satisfies:

$$A_r \times M_s \longrightarrow M_{r+s} \ .$$

Given a graded A-module M we can also describe the "shifted" A-module, $M(n)$ (for $n \in \mathbb{Z}$), defined by:

$$[M(n)]_d := M_{n+d}$$

where the action on M_{n+d} is that originally given.

Shifting is very useful when we want to discuss homomorphisms of graded A-modules, as we'll see later.

In general we will be considering graded A-modules M which are finitely generated (f.g). In that case we have:

Proposition:

$i)$ $M_t = 0$ for all $t << 0$;

$ii)$ Each M_i is a finite dimensional vector space over k.

The sequence of dimensions $\{\dim_k M_i\}_{i\in\mathbb{Z}}$, gives a function $h_m : \mathbb{Z} \to \mathbb{Z}$ which is called the *Hilbert Function of* M. When M is a f.g. graded A-module this function is rather well behaved.

Theorem: (Hilbert-Samuel) Let A be a graded ring as above and M a f.g. graded A-module.

There is a unique polynomial $f(t) \in \mathbb{Q}[t]$ such that

$$f(d) = \dim_k M_d \quad \text{for all} \quad d >> 0.$$

Moreover, if $\dim_k A_1 = n+1$ then $deg\ f(t) \le n$ (independent of M).

Notation: The polynomial described in the theorem is usually called the *Hilbert Polynomial* of M and denoted (variously) by: $H_M(-)$ or $H(M,-)$.

Notice that the polynomial described by the theorem is somewhat special for polynomials with coefficients in $\mathbb{Q}$: for all large integer values of the argument the polynomial takes on only integer values.

It is not hard to classify such polynomials. In fact,

Proposition: Let $f(x) \in \mathbb{Q}[x]$, $deg\ f(x) = d$ and suppose that for all $n >> 0$, $n \in \mathbb{Z}$ we have $f(n) \in \mathbb{Z}$.

Then there are uniquely determined integers $a_0, \ldots, a_d$ such that

$$f(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + \cdots + a_d\binom{x}{d}.$$

Thus, associated to any f.g. graded A-module is a sequence of integers $a_0, \ldots, a_d$ (as well as the integer d itself) which we might reasonably call the "integer coefficients" of the Hilbert polynomial, and which cry out for interpretation.

We first give an interpretation for the number d, the degree of the Hilbert polynomial.

Theorem: Let $A = R/I$ and M be as above with $H_M(-)$ the Hilbert polynomial of M. Then $\deg H_M = [\text{K-dim } (A/ann(M))] - 1$.

Examples:

1) Let $M = R = k[x_0, \ldots, x_n]$, then $\mathrm{ann}(M) = (0)$ and we showed that $H_M(t) = \binom{t+n}{n}$ for all t. Thus, deg $H_M = n = [\text{K-dim } R] - 1$, as expected.

2) Let $M = R/I$ considered as an R-module. Then $\mathrm{ann}(M) = I$ and deg $H_M(t) = [\text{K-dim } (R/I)] - 1$. Notice that $[\text{K-dim } (R/I)] - 1$ is exactly the dimension of the closed subscheme of $\mathbb{P}^n$ defined by I.

3) In particular, when $I = \wp_1 \cap \cdots \cap \wp_s$ is the ideal of the set $X = \{P_1, \ldots, P_s\}$ of s points in $\mathbb{P}^n$ and $M = R/I$ then the Hilbert polynomial of M is a constant. What is that constant in this case?

Claim: The constant is the number s of points in X.

Pf: It will be enough to show that $\dim_k(R/I)_t = s$ for all $t >> 0$. Now, $\dim_k(R/I)_t \leq s$ for all t is easy to see by looking at the system of linear equations one needs to solve to find elements in I_t. Also, since R/I is a CM ring (we can assume that k is an infinite field) we can find a non-zero-divisor in $(R/I)_1$. This means that $\dim_k(R/I)_t$ is a non-decreasing function. Thus, it suffices to find one t for which the Hilbert function takes on the value s. We can show that this definitely happens for $t = s - 1$.

To see why that is so, choose hyperplanes H_i, $i = 1, \ldots, s$ such that P_i is only on the hyperplane H_i. Let L_i be the linear equation describing the hyperplane H_i. Consider the s forms of degree $s - 1$ described by $F_i = \Pi_{j=1, j\neq i}^{s} L_j$. One easily shows that no non-trivial linear combination of these forms is in I. That is enough to show that $\dim_k(R/I)_{s-1} = s$.

We not turn our attention to the top coefficient of the Hilbert polynomial.

Example:

1) Let F be a form of degree d in R and let $A = R/(F)$. Then K-dim $A = n$ and so deg $H_A(t) = n-1$. If we write

$$H_A(t) = a_0\binom{t}{0} + a_1\binom{t}{1} + \ldots + a_{n-1}\binom{t}{n-1}$$

then $a_{n-1} = d = \deg F$.

2) If $\wp$ is a prime ideal of R and $A = R/\wp$ then the top coefficient of $H_A(t)$ is, what was classically referred to as, the *degree* of the variety $Z(\wp) \subset \mathbb{P}^n$ (it is the number of distinct points that arise when a general complementary dimensional linear space meets $Z(\wp)$).

For this reason, the top coefficient of H_M is often referred to as the *degree* of M (some authors also use the term *multiplicity*).

The constant term of the Hilbert polynomial also has some interest. If one looks at Example 1 above in the case where $n = 2$, i.e. for F the equation of a plane curve, one finds that the constant term (a_0 in the notation above) satisfies

$$a_0 - 1 = -\frac{(d-1)(d-2)}{2}$$

That number is precisely the genus of a non-singular plane curve of degree d.

More generally, when $M = R/I$ and deg $H_{R/I}(t)$ is r then

$$(-1)^r(H_{R/I}(0) - 1)$$

is called the "arithmetic genus" of the subscheme of $\mathbb{P}^n$ defined by I.

Many problems from classical algebraic geometry can be phrased in terms of the Hilbert polynomial. E.g. the Halphen Problem, (resolved only about 20 years ago by R. Hartshorne) which asks for a description of all pairs (d, g) where d and g are, respectively, the degree and genus of a smooth curve in $\mathbb{P}^3$. From the discussion above, we see that these are (in some sense) questions about the two coefficients in the Hilbert polynomial of the coordinate ring of a smooth curve in $\mathbb{P}^3$.

This is a good example where one *restricts* the class of ideals of R and asks about the nature of the Hilbert polynomial for rings of the form R/I where I is a member of that special class of ideals. That has been a very fruitful way to examine both algebraic and geometric phenomena.

E.g. one can even ask a more general question. Start with the biggest set of ideals possible and ask: What are all the possible Hilbert polynomials of quotients of R, or even more generally, what are all the possible Hilbert **functions** of all cyclic R-modules, i.e. modules of the form R/I, with I homogeneous.

Interestingly enough, at the beginning of the 20th century, F.S. Macaulay gave a complete answer to this second question for cyclic R-modules. Let's quickly review Macaulay's solution to the problem.

Definition-Proposition: Let i and h be positive integers. The *i-binomial expansion of h* is the unique expression

$$h = \binom{m_i}{i} + \binom{m_{i-1}}{i-1} + \cdots + \binom{m_j}{j}$$

with $m_i > m_{i-1} > \cdots > m_j \geq j \geq 1$.

The i-tuple $(m_i, m_{i-1}, \ldots, m_j, 0, \ldots, 0)$ (where the final zeroes are inserted to make this an i-tuple) is the *i-binomial coefficient vector of h*.

Recall the *lexicographic* order on i-tuples:

$$(a_i, a_{i-1}, \ldots, a_1) \geq_{lex} (b_i, b_{i-1}, \ldots, b_1) \Leftrightarrow$$

the first non-zero entry in $(a_i - b_i, a_{i-1} - b_{i-1}, \ldots, a_1 - b_1)$ is positive.

Proposition: If $m,\ n,\ i$ are positive integers and $(a_i, a_{i-1}, \ldots, a_1)$ and $(b_i, b_{i-1}, \ldots, b_1)$ are the i-binomial coefficient vectors of m and n respectively, then

$$m \geq n \Leftrightarrow (a_i, a_{i-1}, \ldots, a_1) \geq_{lex} (b_i, b_{i-1}, \ldots, b_1)$$

Definition: (Macaulay's Functions)

Let h have i-binomial coefficient vector $(m_i, m_{i-1}, \ldots, m_j, 0, \ldots, 0)$ then the function

$$\_^{<i+1>} : \mathbb{N} \longrightarrow \mathbb{N}$$

is defined by

$$h^{<i+1>} = \binom{m_i+1}{i+1} + \ldots + \binom{m_j+1}{j+1} .$$

We can now state the first part of Macaulay's Theorem.

Theorem: Let $A = R/I$ and suppose that $h_A : \mathbb{N} \to \mathbb{N}$ is the Hilbert function of A where $h_A(t) = h_t = \dim_k A_t$.

Then, for any $i \geq 1$ we have

$$h_{i+1} \leq h_i^{<i+1>} .$$

In order to state the rest of Macaulay's theorem it will be convenient to have the following notation:

Definition: Let $S = (1, h_1, \ldots, h_i, \ldots)$ be a sequence on non-negative integers.

We say that S is an *O-sequence* if, for every $i \geq 1$ we have $h_{i+1} \leq h_i^{<i+1>}$.

Theorem: (Macaulay) Let S be an O-sequence (as above) and let $R = k[x_0, \ldots, x_{h_1-1}]$.

There is a homogeneous ideal $I \subset R$ (in fact, a monomial ideal, i.e. an ideal generated by monomials) such that

$$S = (1, h_{R/I}(1), \ldots, h_{R/I}(i), \ldots) .$$

One can rightly assert that Macaulay's theorem says all that can be said about Hilbert functions, but right away certain things become very clear when one tries to use the theorem. In general, the monomial ideals that Macaulay guarantees will exist are usually "ugly as sin", i.e. they often have embedded components and very often have irrelevant components. The irrelevant components don't affect the Hilbert polynomial (irrelevant components disappear after a while) but they do affect the Hilbert function! and for many applications it is precisely the Hilbert function, not the polynomial, which one needs to know.

Thus, in the spirit of the questions we asked above, let me mention some of the things that people have worried about, with greater or lesser success.

Questions:

1) What can be the Hilbert function of a set of s points in $\mathbb{P}^n$? (success).

2) What can be the Hilbert function of a domain? (some - few - results)

3) What can be the Hilbert function of a CM ring? (success)

4) What can be the Hilbert function of points with the Uniform Position Property? (some few, but notable, successes).

4) What can be the Hilbert function of ideals of the type $\wp_1^t \cap \cdots \cap \wp_s^t$ where the $\wp_i$ are the ideals of points in $\mathbb{P}^n$ and t is a positive integer. (very little known when $t > 1$).