HILBERT POLYNOMIALS AND THE DEGREE OF A PROJECTIVE VARIETY

EMILY CLADER

1. Introduction

If $X \subset \mathbb{P}^n$ is an irreducible projective variety, then the homogeneous coordinate ring $\Gamma(X)$ has a natural grading, and it is reasonable to ask how the size of the graded components $\Gamma(X)_m$ varies with m. Geometrically, this is tantamount to asking how many hypersurfaces of each degree m contain X, for such a hypersurface is given by a homogeneous polynomial of degree m in $I(X)$– that is, an element of $I(X)_m$– and the dimension of $\Gamma(X)_m$ is equal to the codimension of $I(X)_m$ in $k[X_0, \ldots, X_n]_m$. We will define a function h_X, called the Hilbert function of the projective variety, that records this data. The first surprising feature of the Hilbert function is that it is extremely well-behaved; for large values of m, $h_X(m)$ agrees with a polynomial. Furthermore, this polynomial encodes a host of numerical invariants of X. We will discuss one such invariant, namely the degree of the projective variety. While our definition of degree via the Hilbert function will suffer from a lack of geometric motivation, we will prove that, at least in certain cases, it coincides with a more intuitive notion of the degree of a variety.

2. The Hilbert Function

Let $X \subset \mathbb{P}^n$ be a projective variety, and let $\Gamma(X) = k[X_0, \ldots, X_n]/I(X)$ denote its homogeneous coordinate ring. We define a function $h_X : \mathbb{N} \to \mathbb{N}$ by

$$h_X(m) = \dim_k(\Gamma(X)_m),$$

where the subscript denotes the m^{th} graded piece. The function h_X is called the *Hilbert function* of the variety X.

In some specific cases, it is possible to compute the Hilbert function directly. For example, if $X = \{p_1, p_2, p_3\}$ consists of three points in $\mathbb{P}^2$, then there are two possible Hilbert functions. We have

$$h_X(1) = \dim_k(\Gamma(X)_1) = \operatorname{codim}_k(I(X)_1, k[X_0, X_1, X_2]_1) = 3 - \dim_k(I(X)_1).$$

Here, $I(X)_1$ is the space of homogeneous linear polynomials vanishing at p_1, p_2, and p_3. There is no such polynomial unless the three points are colinear, in which case the space is 1-dimensional, generated by the line on which they lie. Thus,

$$h_X(1) = \begin{cases} 2 & \text{if } p_1, p_2, p_3 \text{ are colinear,} \\ 3 & \text{otherwise.} \end{cases}$$

On the other hand, $h_X(2) = 3$ regardless of the configuration of the points. Indeed, by choosing representatives $v_1, v_2, v_3 \in \mathbb{A}^3 \setminus \{0\}$ for the three points, one defines a map

$$\varphi : k[X_0, X_1, X_2]_2 \to k^3$$

by evaluation at v_1, v_2, and v_3. Multiplying a homogeneous linear polynomial vanishing at p_1 but not p_3 by one vanishing at p_2 but not p_3 gives a homogeneous quadratic polynomial vanishing at the first two points but not the third. In the same manner, one can find homogeneous quadratic polynomials vanishing at any two of the three points; it follows that the image of φ contains the standard basis vectors, and hence φ is surjective. Thus,

$$h_X(2) = \mathrm{codim}_k(I(X)_2, k[X_0, X_1, X_2]_2) = \dim(k[X_0, X_1, X_2]_2) - \dim_k(\ker \varphi) = \dim_k(k^3) = 3,$$

as claimed. The same proof shows that $h_X(m) = 3$ for all $m \geq 2$, so we have completely determined the Hilbert function of X.

Let us consider a higher-dimensional example, lest we give the impression that Hilbert functions are only computable in rather uninteresting cases. Suppose X is the rational normal curve; that is, X is the image of the d-fold Veronese embedding $\nu_d : \mathbb{P}^1 \to \mathbb{P}^d$. Then ν_d^* gives an identification between homogeneous polynomials of degree m on X and homogeneous polynomials of degree dm on $\mathbb{P}^1$. Thus, $\Gamma(X)_m \cong k[X_0, X_1]_{dm}$, so that

$$h_X(m) = \dim_k(k[X_0, X_1]_{dm}) = \left(\begin{array}{c} dm+1 \\ 1 \end{array} \right) = dm + 1.$$

Generalizing this example, one sees that if Y is the image of the d-fold Veronese embedding $\mathbb{P}^n \to \mathbb{P}^N$, then $\Gamma(Y)_m \cong k[X_0, \ldots, X_n]_{dm}$, so

$$h_Y(m) = \dim_k(k[X_0, \ldots, X_n]_{dm}) = \left(\begin{array}{c} dm+n \\ n \end{array} \right) = \frac{d^n}{n!} m^n + \cdots .$$

Two natural observations present themselves at this moment. First, the Hilbert function exhibits quite controlled behavior; in the second two examples considered above, it is a polynomial function, while in the first example it at least agrees with a polynomial (namely a constant) for $m \geq 2$. Additionally, the degree of this polynomial in each case coincides with the dimension of the variety. These are not accidental features, but are general properties enjoyed by the Hilbert function of any projective variety.

3. The Hilbert Polynomial

The goal of this section is to prove the following theorem:

Theorem 1. *Let $X \subset \mathbb{P}^n$ be an embedded projective variety of dimension r. Then there exists a polynomial p_X such that $h_X(m) = p_X(m)$ for all sufficiently large m, and the degree of p_X is equal to r.*

The polynomial p_X is called the *Hilbert polynomial* of X. We should remark that there is nothing special about the fact that $\Gamma(X)$ is the coordinate ring of a projective variety. In fact, if M is any finitely-generated graded module over the ring $S = k[X_0, \ldots, X_n]$ (that is, $M = \bigoplus M_d$ and $S_d \cdot M_e \subset M_{de}$ for all d, e), then one can define the Hilbert function of M exactly as above, and the same proof will show that this function eventually agrees with a polynomial.

We will require three lemmas:

Lemma 2. *If $P \in \mathbb{Q}[z]$ is a polynomial such that $P(n) \in \mathbb{Z}$ for all sufficiently large integers n, then there exist integers $c_0, \ldots, c_r$ such that*

$$P(z) = c_0 \binom{z}{r} + c_1 \binom{z}{r-1} + \cdots + c_r.$$

Proof. Observe that

$$\binom{z}{r} = \frac{1}{r!}z^r + \cdots ,$$

so we can write z^r in the form $c_0\binom{z}{r} + c_1\binom{z}{r-1} + \cdots + c_r$ with $c_i \in \mathbb{Q}$. It follows that we can write any polynomial with rational coefficients in this form, so all we need to show is that if $P(n) \in \mathbb{Z}$ for all sufficiently large integers n, then in fact $c_i \in \mathbb{Z}$.

The proof is by induction on the degree of P. If $\deg(P) = 0$, then $P(z) = c_r$, and since $P(n)$ is eventually an integer we must have $c_r \in \mathbb{Z}$. If $P(z) = c_0\binom{z}{r} + \cdots + c_r$ for $r > 1$, then let $\Delta P(n) = P(n+1) - P(n)$ denote the successive difference function of P. Since $\Delta\binom{z}{r} = \binom{z+1}{r} - \binom{z}{r} = \binom{z}{r-1}$, we have

$$\Delta P(z) = c_0\binom{z}{r-1} + c_1\binom{z}{r-2} + \cdots + c_{r-1}.$$

But $\Delta P(z)$ is a polynomial of degree $r-1$ with rational coefficients that is also eventually an integer, so by induction, $c_0, \ldots, c_{r-1} \in \mathbb{Z}$. Since $P(n) \in \mathbb{Z}$ for all $n \gg 0$, it follows that $c_r \in \mathbb{Z}$, as required. □

A polynomial $P \in \mathbb{Q}[z]$ such that $P(n) \in \mathbb{Z}$ for all sufficiently large integers n is known as a *numerical polynomial.*

Lemma 3. *If $f : \mathbb{Z} \to \mathbb{Z}$ is any function for which there exists a numerical polynomial $Q(z)$ such that the successive difference function $\Delta f(n) = f(n+1) - f(n)$ is equal to $Q(n)$ for all $n \gg 0$, then there exists a numerical polynomial P such that $f(n) = P(n)$ for all $n \gg 0$. Furthermore,* $\deg(P) = \deg(Q) + 1$.

Proof. By Lemma 2, we can write

$$Q(z) = c_0\binom{z}{r} + c_1\binom{z}{r-1} + \cdots + c_r$$

with $c_i \in \mathbb{Z}$. Let $P(z) = c_0\binom{z}{r+1} + c_1\binom{z}{r} + \cdots + c_r$. Then $\Delta P = Q$, so $\Delta(f-P)(n) = \Delta f(n) - \Delta P(n) = 0$ for all $n \gg 0$. So for sufficiently large n, $(f-P)(n)$ is a constant, say $(f-P)(n) = c_{r+1}$. This implies that

$$f(n) = P(n) + c_{r+1}$$

for all $n \gg 0$, and hence $f(n)$ eventually agrees with a numerical polynomial. The last statement is immediate from the proof. □

For the third lemma, we require a bit of notation. If M is a graded S-module and $r \in \mathbb{Z}$, then $M[r]$ denotes the S-module obtained from M by shifting the degrees by r; that is $M[r]_s = M_{r+s}$ for all s.

Lemma 4. *Let M be a finitely-generated graded module over a Noetherian ring S. Then there exists a filtration*

$$0 = M^0 \subset M^1 \subset \cdots \subset M^r = M$$

by graded submodules such that for all i,

$$M^i/M^{i-1} \cong (S/\mathfrak{p}_i)[\ell_i]$$

as graded S-modules, where $\mathfrak{p}_i$ is a homogeneous prime ideal of S and $\ell_i \in \mathbb{Z}$.

Proof. Let Σ denote the collection of graded submodules of M that admit such a filtration. This set is nonempty, since the zero module certainly has the required filtration. Therefore, since M is a finitely-generated module over a Noetherian ring and hence is a Noetherian module, the collection Σ has a maximal element M'.

Let $M'' = M/M'$. If $M'' = 0$, we are done. If not, then the set

$$\mathcal{I} = \{I_m = \mathrm{Ann}(m) \mid m \in M'' \text{ nonzero and homogeneous }\}$$

is a nonempty set of ideals in S. So since S is Noetherian, $\mathcal{I}$ has a maximal element I_m. We claim that I_m is prime. Since m is a homogeneous element of M'', I_m is a homogeneous ideal, and hence an element of S lies in I_m if and only if each of its homogeneous components does; therefore, it suffices to prove that a product of elements outside I_m does not lie in I_m in the case where those elements are homogeneous. Let a and b be homogeneous elements of S for which $ab \in I_m$ but $b \notin I_m$. Then bm is a nonzero homogeneous element of M'', so $I_{bm} \in \mathcal{I}$. Clearly $I_m \subset I_{bm}$, so by maximality, $I_m = I_{bm}$. But $ab \in I_m$, hence $abm = 0$. This says that $a \in I_{bm}$, so $a \in I_m$, as required.

This proves that I_m is a homogeneous prime ideal of S, which we will denote by $\mathfrak{p}$. Suppose that $m \in M_\ell$. Then the submodule $A \cdot m \subset M''$ is isomorphic as a graded module to $(S/\mathfrak{p})[-\ell]$. Letting $N \subset M$ be the inverse image of $A \cdot m$ in M, we have

$$N/M' \cong A \cdot n \cong (S/\mathfrak{p})[-\ell].$$

Thus, N has a filtration $0 \subset M' \subset N$ of the form claimed in the statement of the lemma. But $M' \subsetneq N$, so this contradicts the maximality of M', and hence completes the proof. $\square$

We are now ready to prove the theorem:

Proof of Theorem 1. We will actually prove a slightly more general statement: If M is a finitely-generated graded module over the ring $S = k[X_0, \ldots, X_n]$, and $h_M(m) = \dim_k(M_m)$ denotes its Hilbert function, then there exists a polynomial $p_M(z)$ such that $h_M(m) = p_M(m)$ for all sufficiently large integers m. Moreover, the degree of this polynomial is equal to $\dim(V(\mathrm{Ann}(M))$, where $V(\mathrm{Ann}(M))$ denotes the variety in $\mathbb{P}^n$ defined by the homogeneous ideal $\mathrm{Ann}(M)$. In case $M = \Gamma(X) = S/I(X)$ for a projective variety X, we have $V(\mathrm{Ann}(M)) = V(I(X)) = X$, so this indeed generalizes the theorem.

Suppose that

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of S-modules and the claim is true for both M' and M'' Then $h_M = h_{M'} + h_{M''}$, so h_M is eventually a polynomial. Furthermore,

$$V(\mathrm{Ann}(M)) = V(\mathrm{Ann}(M')) \cup V(\mathrm{Ann}(M'')),$$

so

$$\dim V(\mathrm{Ann}(M)) = \max(\dim V(\mathrm{Ann}(M')), \dim V(\mathrm{Ann}(M''))) = \deg(p_{M'} + p_{M''}) = \deg p_M,$$

and hence the claim is also true for M.

Therefore, by induction on the pieces of the filtration in Lemma 4, it suffices to prove the claim for modules of the form $(S/\mathfrak{p})[\ell]$ with $\mathfrak{p}$ a homogeneous prime ideal of S and $\ell \in \mathbb{Z}$. In fact, the degree shift simply yields a change of variables $z \mapsto z + \ell$ in the Hilbert function, so it suffices to prove the claim for $M = S/\mathfrak{p}$.

One case must be treated slightly differently than the rest. If $\mathfrak{p} = (X_0, \ldots, X_n)$, then $h_M(m) = 0$ for all $m > 0$, and hence we can take $p_M \equiv 0$. Under the convention that the degree of the zero polynomial and the dimension of the empty set are both -1, we have $\deg(p_M) = \dim(V(\mathfrak{p}))$, as required.

Assume, now, that $\mathfrak{p} \neq (X_0, \ldots, X_n)$. Choose any $X_i \notin \mathfrak{p}$, and consider the exact sequence

$$0 \to M[-1] \xrightarrow{\cdot X_i} M \to M/X_iM \to 0.$$

Then, since all the above homomorphisms are homogeneous of degree zero, we have

$$h_{M/X_iM}(m) = h_M(m) - h_M(m-1) = \Delta h_M(m-1).$$

Furthermore,

$$V(\mathrm{Ann}(M/X_iM)) = V(\mathfrak{p}) \cap V(X_i).$$

So $V(\mathrm{Ann}(M/X_iM))$ is a hypersurface in $V(\mathfrak{p})$, and hence $\dim(V(\mathrm{Ann}(M/X_iM))) = \dim(V(\mathfrak{p})) - 1$. Therefore, by induction on $\dim(V(\mathrm{Ann}(M))) = \dim(V(\mathfrak{p}))$, we may assume that h_{M/X_iM} eventually agrees with a polynomial of degree equal to $\dim(V(\mathrm{Ann}(M/X_iM)))$.

By the above, this implies that Δh_M eventually agrees with a polynomial whose degree is $\dim(V(\mathrm{Ann}(M/X_iM)))$. So by Lemma 3, h_M eventually agrees with a polynomial of degree

$$\dim(V(\mathrm{Ann}(M/X_iM))) + 1 = \dim(V(\mathfrak{p})) = \dim(V(\mathrm{Ann}(M))),$$

as claimed. □

4. The Degree of a Projective Variety

One of the most useful features of the Hilbert polynomial is that it allows us to define the notion of degree. If $X \subset \mathbb{P}^n$ is an embedded projective variety of dimension r, the *degree* of X is defined to be $r!$ times the leading coefficient of $p_X(m)$.

Proposition 5. *Let $X \subset \mathbb{P}^n$ be an embedded projective variety.*

(a) The degree of X is a positive integer.

(b) If $X = V(F)$ is a hypersurface of degree d (in the sense that F is a homogeneous polynomial of degree d), then the degree of X is d.

(c) If $X = \{p_1, \ldots, p_d\}$ is a finite collection of distinct points, then the degree of X is d.

Proof. Since p_X is a numerical polynomial of degree r, Lemma 2 implies that we can write it as

$$p_X(m) = c_0 \binom{m}{r} + \cdots + c_r = \frac{c_0}{r!} z^r + \cdots,$$

where $c_i \in \mathbb{Z}$. Therefore, $\deg(X) = c_0$ is an integer. It is positive because for $m \gg 0$, $p_X(m) = h_X(m)$ is positive.

For part (b), we explicitly compute the Hilbert function of $X = V(F)$. If $S = k[X_0, \ldots, X_n]$ and $\Gamma(X) = S/(F)$ is the homogeneous coordinate ring of X, we have an exact sequence

$$0 \to S[-d] \xrightarrow{\cdot F} S \to \Gamma(X) \to 0.$$

These homomorphisms are homogeneous of degree zero, so

$$h_X(m) = \dim_k(\Gamma(X)_m) = \dim_k(S_m) - \dim_k(S_{m-d}).$$

One computes directly that

$$\begin{aligned} h_X(m) &= \left(\begin{array}{c} m+n \\ n \end{array} \right) - \left(\begin{array}{c} m+n-d \\ n \end{array} \right) \\ &= \frac{1}{n!}\left((m^n + \frac{n(n+1)}{2}m^{n-1} + \cdots) - (m^n + \frac{n(-2d+n+1)}{2} + \cdots) \right) \\ &= \frac{d}{(n-1)!}m^{n-1} + \cdots . \end{aligned}$$

Since we know that a hypersurface has dimension $n-1$, it follows that $\deg(X) = d$, as claimed.

Part (c) is equivalent to the claim that $h_X(m) = d$ for all $m \gg 0$. The proof of this assertion is almost identical to the proof that $h_X(m) = 3$ for all $m \geq 2$ in the case where X consists of three points in $\mathbb{P}^2$. Specifically, choose representatives $v_1, \ldots, v_d$ in $\mathbb{A}^{n+1}$ for the points $p_1, \ldots, p_d \in \mathbb{P}^n$, and define a a map

$$\varphi : k[X_0, \ldots, X_n]_m \to k^d$$

by evaluation at $v_1, \ldots, v_d$. As long as $m \geq d-1$, this is surjective. Indeed, for any $j \in \{1, \ldots, d\}$, we can construct a homogeneous polynomial of degree $d-1$ vanishing at each of the points except for p_j by multiplying linear forms L_i vanishing at p_i but not p_j. By raising some L_i's to powers, we can increase the degree of this polynomial to m. We find, therefore, that each of the standard basis vectors lies in the image of φ, and hence φ is surjective. So for $m \geq d-1$, we have

$$h_X(m) = \dim_k(k[X_0, \ldots, X_n]_m) - \dim_k(\ker(\varphi)) = \dim_k(k^d) = d,$$

as claimed. $\square$

An important observation should be made at this point: the degree of a projective variety is highly dependent on its embedding in projective space. For example, from our computation of the Hilbert function $h_X(m) = dm+1$ of the rational normal curve X given previously, it follows that the degree of the rational normal curve is d. On the other hand,

$$h_{\mathbb{P}^1}(m) = \dim_k(k[X_0, X_1]_m) = \binom{m+1}{1} = m+1,$$

so $\deg(\mathbb{P}^1) = 1$. But $\nu_d : \mathbb{P}^1 \to \mathbb{P}^d$ is an isomorphism onto its image! Thus, while the degree of a projective variety is clearly invariant under linear automorphisms of $\mathbb{P}^n$, it is not invariant under isomorphisms in general.

There are many other ways to define the degree of a projective variety besides the one we have presented here. While ours has the advantage of being fairly easy to compute, its geometric meaning is entirely mysterious. To contrast, if $X \subset \mathbb{P}^n$ has dimension r, one can define the degree of X as the number of points of intersection of X with a general linear subspace of dimension $n-r$. To get a sense of why this is reasonable, we observe that a general linear subspace L of dimension $n-r$ meets X in a finite collection of points. Indeed, it is sufficient to prove this is true when X and L are subvarieties of $\mathbb{A}^n$, since in general we can intersect each with the standard affine charts. In the affine case, Noether Normalization implies that a general projection $\mathbb{A}^n \to \mathbb{A}^r$ induces a finite map $\pi : X \to \mathbb{A}^r$. Such a projection comes from a general coordinate change $\mathbb{A}^n \to \mathbb{A}^n$ followed by projection onto the last r coordinates; and after such a coordinate change, the first $n-r$ coordinates span a subspace L for which $X \cap L = \pi^{-1}(0)$, which is a finite collection of points by the finiteness of the morphism π.

Of course, it is unclear why the number of points of intersection is independent of L once L is sufficiently general, and even less apparent why this number should coincide with the normalized leading coefficient of the Hilbert polynomial. We will prove in Proposition 6 that the two definitions of degree agree in the case where X is a projective plane curve. Before doing so, however, let us consider an example to solidify our intuition.

Let $X = V(YZ - X^2) \subset \mathbb{P}^2$. Since this is a hypersurface defined by a degree-2 polynomial, Proposition 5(b) implies that its degree as defined by way of the Hilbert polynomial is 2. We will show that a general line in $\mathbb{P}^2$ meets X in exactly 2 points. Looking at the affine chart where $Z \neq 0$, the real picture makes this assertion plausible:

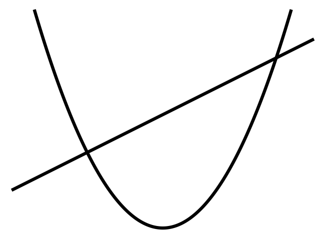

Figure 1: A general line meets $V(YZ - X^2) \subset \mathbb{P}^2$ in two points.

Let L be given by the equation $aX + bY + cZ = 0$. Assuming $b \neq 0$, it is easy to check that $X \cap L$ is contained in the affine chart where $Z \neq 0$. On this affine chart, we have

$$X \cap L \cong \{(X, Y) \in \mathbb{A}^2 \mid Y = X^2,\ bX^2 + aX + c = 0\}.$$

As long as $a^2 - 4bc \neq 0$, this intersection consists of exactly 2 points. Thus, all lines $L = \{aX + bY + cZ = 0\}$ for which $b \neq 0$ and $a^2 - 4bc \neq 0$ intersect X in exactly 2 points. These are polynomial nonvanishing conditions, and hence define an open subset of the Grassmannian of lines in $\mathbb{P}^1$, so a general line has the desired property.

Proposition 6. *Let $X = V(F) \subset \mathbb{P}^2$ be a curve of degree d (in the sense that F is a homogeneous polynomial of degree d, or equivalently, the leading coefficient of h_X is d). Then a general line in $\mathbb{P}^2$ meets Y in exactly d points.*

Proof. Denote a line L by $\{aX + bY + cZ = 0\}$. We will first prove that a general line has the property that none of its intersections with X is either a singular point of X or a point of tangency. Indeed, X has only finitely many singular points, and the condition that L not pass through one of these is a polynomial nonvanishing condition on a, b, and c; thus, the condition that L not pass through any of them is a finite collection of open conditions, hence is an open condition on L.

As for the points of tangency, let

$$Y = \{(p, L) \in \mathbb{P}^2 \times (\mathbb{P}^2)^* \mid p \in X,\ L \text{ is tangent to } X \text{ at } p\}.$$

This is a closed subset of $\mathbb{P}^2 \times (\mathbb{P}^2)^*$, because if L is as above, then the condition that L is tangent to X at p is equivalent to

$$\left[\frac{\partial F}{\partial X}(p) : \frac{\partial F}{\partial Y}(p) : \frac{\partial F}{\partial Z}(p)\right] = [a : b : c].$$

Thus,

$$Y = V\left(F, b\frac{\partial F}{\partial X} - a\frac{\partial F}{\partial Y}, c\frac{\partial F}{\partial Y} - b\frac{\partial F}{\partial Z}\right),$$

which is closed. Since the projection $\pi : \mathbb{P}^2 \times (\mathbb{P}^2)^* \to (\mathbb{P}^2)^*$ is a morphism between projective varieties, it is a closed map, and hence the set $\pi(X)$ is a closed subset of the Grassmannian $(\mathbb{P}^2)^*$ of lines in $\mathbb{P}^2$. Its complement, which consists precisely of lines that are not tangent to X at any point, is therefore an open set.

It follows that a general line indeed meets X transversally at nonsingular points. We claim that such a line must intersect X in exactly d points. To prove this, first assume without loss of generality that $X_* = \{F(X,Y,1) = 0\} \subset \mathbb{A}^2$ is still a plane curve of degree d; this can always be achieved after a change of coordinates. After imposing one more open condition, we may assume that L does not meet X in the hyperplane $\{Z = 0\}$. This reduces our problem to the corresponding claim in the affine case. But in this case, we have seen as a corollary of Bézout's Theorem that, since Y_* and L_* meet transversally at nonsingular points, the number of points of intersection is equal to

$$\dim_k\left(\frac{k[X,Y]}{(F_*, aX + bY)}\right).$$

Either a or b is nonzero, so we may assume that $b \neq 0$. Then the above is equal to

$$\dim_k\left(\frac{k[X]}{(F_*(X, -\frac{a}{b}X))}\right) = d,$$

since $F_*(X, \frac{-a}{b}X)$ is a polynomial of degree d. Thus, a general line meets X in exactly d points, as claimed. □

5. Bézout's Theorem

We close by mentioning one important application of the notion of degree. Let $X \subset \mathbb{P}^n$ be a projective variety of dimension r, and let H be a hypersurface not containing any irreducible component of X. Write

$$X \cap H = Z_1 \cup \cdots \cup Z_s,$$

where the Z_j are irreducible varieties with corresponding homogeneous prime ideals $\mathfrak{p}_j$. Define the *intersection multiplicity* of X and H along Z_j, denoted $i(X, H; Z_j)$, as the length of $(k[X_0, \ldots, X_n]/(I(X) + I(H)))_{\mathfrak{p}_j}$ as a $k[X_0, \ldots, X_n]_{\mathfrak{p}_j}$-module, that is, the length of the longest increasing chain of $k[X_0, \ldots, X_n]_{\mathfrak{p}_j}$-submodules.

In case X and H are both projective plane curves (with no common components), each Z_j is a point, and the definition of intersection mutliplicity at each such point agrees with the the intersection numbers we have previously defined for plane curves. To prove this, we will make use of the following algebraic fact:

Lemma 7. *Let A be a local ring with maximal ideal $\mathfrak{m}$, and suppose that A contains an isomorphic copy of $A/\mathfrak{m}$. Let $\ell_A(M)$ denote the length of an A-module M. Then*

$$\ell_A(M) = \dim_{A/\mathfrak{m}}(M).$$

Proof. The proof is by induction on $\dim_{A/\mathfrak{m}}(M)$. As a base case, suppose that $\dim_{A/\mathfrak{m}}(M) = 1$. Then $M \cong A/\mathfrak{m}$, and the fact that $\mathfrak{m}$ is maximal implies that the longest chain of A-submodules of $A/\mathfrak{m}$ is $\{0\} \subsetneq A/\mathfrak{m}$, which has length 1.

Assume, now, that $\dim_{A/\mathfrak{m}}(M) > 1$. We claim that M has a proper nontrivial submodule. For if not, choose any nonzero element $x \in M$. Then $A \cdot x = M$, since otherwise $A \cdot x$ would be a proper nontrivial submodule. Thus, $M \cong A/I$ for $I = \mathrm{Ann}(x)$. But since $A/\mathfrak{m} \subset A$, M is also an $(A/\mathfrak{m})$-module, so this implies that $\mathfrak{m} \subset I$ and hence that $\mathfrak{m} = I$ by maximality. This contradicts our assumption that $\dim_{A/\mathfrak{m}}(M) > 1$.

Thus, we can choose a proper nontrivial submodule N of M. Consider the short exact sequence

$$0 \to N \to M \to M/N \to 0.$$

The dimensions over $A/\mathfrak{m}$ of both N and M/N are strictly smaller than that of M, so by induction we have $\dim_{A/\mathfrak{m}}(N) = \ell_A(N)$ and $\dim_{A/\mathfrak{m}}(M/N) = \ell_A(M/N)$. Since both dimension and length are additive functions, this implies the same equality for M, and thus completes the proof. □

Proposition 8. *Let $X = V(F) \subset \mathbb{P}^2$ and $H = V(G) \subset \mathbb{P}^2$ be plane curves over an algebraically closed field with no common components. For any point p in $X \cap H$, the intersection mutliplicity $i(X, H; p)$ is equal to the intersection number of X and H at p, defined as*

$$\dim_k(\mathcal{O}_p(\mathbb{P}^2)/(f, g)),$$

where f and g are local equations for F and H at p.

Proof. Since both types of intersection numbers are local, it suffices to assume that X and H are actually affine plane curves, with $F, G \in k[X, Y]$. Let $A = (k[X, Y]/(F, G))_{\mathfrak{m}}$, where $\mathfrak{m}$ is the maximal ideal corresponding to p. Then $i(X, H; p)$ is the length of A as a $k[X, Y]_{\mathfrak{m}}$-module. Notice, however, that this is the same as the length of A as an A-module, since the A-module structure is identical to the $k[X, Y]_{\mathfrak{m}}$-module structure except that $(F, G)_{\mathfrak{m}}$ acts trivially; hence, a chain of $k[X, Y]_{\mathfrak{m}}$-submodules gives rise to a chain of A-submodules and vice versa. Thus, the claim is that

$$\ell_A(A) = \dim_k(A).$$

Now, A is a local ring. Denoting its maximal ideal by $\mathfrak{n}$, we observe that $A/\mathfrak{n}$ is a ring-finite extension of k. Since it is also a field, the algebraic Nullstellensatz implies that it is a module-finite extension, so since k is algebraically closed, we have $k = A/\mathfrak{n}$. Thus, taking $M = A$, the claim follows from the lemma. □

Having proved this, it is natural to expect that with these generalized intersection numbers comes a generalization of Bézout's Theorem. This is indeed the case, though a proof is beyond the scope of the current paper:

Theorem 9. *Let $X \subset \mathbb{P}^n$ be a variety of dimension ≥ 1, and let H be a hypersurface not containing X. Let $Z_1, \ldots, Z_s$ be the irreducible components of $X \cap H$. Then*

$$\sum_{j=1}^{s} i(X, H; Z_j) \cdot \deg Z_j = (\deg X)(\deg H).$$

References

[1] Eisenbud, D. *Commutative Algebra with a View Toward Algebraic Geometry*, Spring-Verlag, New York, 1995.
[2] Harris, J. *Algebraic Geometry*, Springer-Verlag, New York, 1992.
[3] Hartshorne, R. *Algebraic Geometry*, Springer-Verlag, New York, 1977.
[4] Smith, K. *An Invitation to Algebraic Geometry*, Spring-Verlag, New York, 2000.