2013

Intersection Number of Plane Curves

Margaret E. Nichols
Oberlin College

INTERSECTION NUMBER OF PLANE CURVES

MARGARET E. NICHOLS

1. Introduction

One of the most familiar objects in algebraic geometry is the plane curve. A plane curve is the vanishing set of a polynomial in two variables. One of the goals in algebraic geometry is to describe properties of geometric objects such as these curves in algebraic terms. Intersection theory is a branch of algebraic geometry motivated by the following geometric and topological question:

> Given a space X and a collection of subspaces $X_1, \ldots, X_n \subseteq X$, how many points lie in the intersection $\cap_{k=1}^{n} X_k$?

In this paper we highlight the special case where X has dimension 2, and the subspaces in question are two plane curves F and G. We are also concerned with counting how many times F and G intersect at a given point P, which is called the intersection number of F and G at P. Intuitively, the intersection number should be the product of the multiplicities of the curves at P, but this is only true in the simplest of cases. Examining the more complicated situations, we can produce a list of additional geometrically-motivated properties the intersection number should satisfy. Given the rich and delicate geometry at play here, it is perhaps unexpected that we can state the intersection number of two curves as an explicit, simple algebraic quantity.

In order to answer the questions above, we must specify our ambient space X. We have stated that it should have dimension 2, but that is all. Different spaces can yield significantly different answers. The distinction between affine and projective spaces is particularly important. Projective n-space over a field k is a completion of affine n-space to include a set of points at infinity. The inclusion of these points gives projective space a nicer geometry than affine space, and in some cases includes intersection points that may have been "missed" in affine space. The choice of k is also important. While it is often convenient to visualize a curve in $\mathbb{R}^2$, many important results only hold over an algebraically closed field such as $\mathbb{C}$.

For this reason, throughout this paper we will always be working over an algebraically closed field. Nevertheless, many interesting and important results are true over fields which are not algebraically closed. For instance, working over the rationals has many important applications to algebraic number theory.

Date: May 22, 2013.

We begin this paper by developing the algebraic background needed to understand the intersection number. In Section 3, we introduce projective n-space. Section 4 brings us to the main focus of this paper, the intersection number of two algebraic curves at a point. In it, we formally define the multiplicity of a curve at a point, followed by the intersection number. Finally, we will move to a central application of the intersection number — Bézout's Theorem. This theorem gives the exact number of intersections of two projective curves over an algebraically closed field. In the case that they have a common component, the two curves have infinitely many points in common, and the intersection number is infinite. Otherwise, the intersection number is finite, and it is simply the product of the degrees of the polynomials defining the curves. Much of the approach here follows Fulton's *Algebraic Curves* [3], especially Chapters 3 and 5.

2. Algebraic Background

We begin by introducing the algebraic objects and ideas we require throughout the rest of the paper. For the purposes of this paper, we shall always assume our field k is algebraically closed. For now we will be working over *affine n-space*, $\mathbb{A}^n(k)$, the cartesian product of n copies of k. When unambiguous, we omit k and simply write $\mathbb{A}^n$. We denote the set of polynomials over k in the n variables $X_1, \ldots, X_n$ by $k[X_1, \ldots, X_n]$. This set forms a ring in the expected way. We will mainly be working in the *affine plane*, $\mathbb{A}^2$, and in the polynomial ring $k[X, Y]$. While all algebraic notation we use is introduced in this section, we assume some knowledge of commutative algebra and, in particular, ring theory. Atiyah and MacDonald provide a concise account of the requisite material (and much more) in [1].

Our main object of study is a *plane curve*, or, more simply, a *curve*. A curve is the zero locus in $\mathbb{A}^2$ of a polynomial in two variables — the set of points at which the polynomial is zero. Given a polynomial $F \in k[X, Y]$, we denote this set by $\mathbb{V}(F)$. When we speak of a curve we will often refer to the polynomial F and not the set $\mathbb{V}(F)$; it will be clear from context what is meant.

The set $\mathbb{V}(F)$ above is an example of an *affine algebraic set*. For any subset $S \subseteq k[X_1, \ldots, X_n]$, we define $\mathbb{V}(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ for all } F \in S\}$. Then an affine algebraic set is any set $X \subseteq \mathbb{A}^n$ such that $X = \mathbb{V}(S)$ for some $S \subseteq k[X_1, \ldots, X_n]$. It is easy to check that if I is the ideal generated by S, then $\mathbb{V}(S) = \mathbb{V}(I)$. Although there is no restriction on the size of such a set S, the Hilbert Basis Theorem tells us that $k[X_1, \ldots, X_n]$ is Noetherian, so every ideal of $k[X_1, \ldots, X_n]$ is finitely generated.[1] It follows that every affine algebraic set is the zero locus of a finite set of polynomials. Given an affine algebraic set X, we define the *ideal* of X, denoted $\mathbb{I}(X)$, to be the set of polynomials that vanish on all points of X.

We are particularly interested in *irreducible* affine algebraic sets, which are affine algebraic sets that cannot be written as the union of two smaller affine algebraic sets.

[1] There are several equivalent statements of the Hilbert Basis Theorem. See [3], p. 7, for the statement we use here.

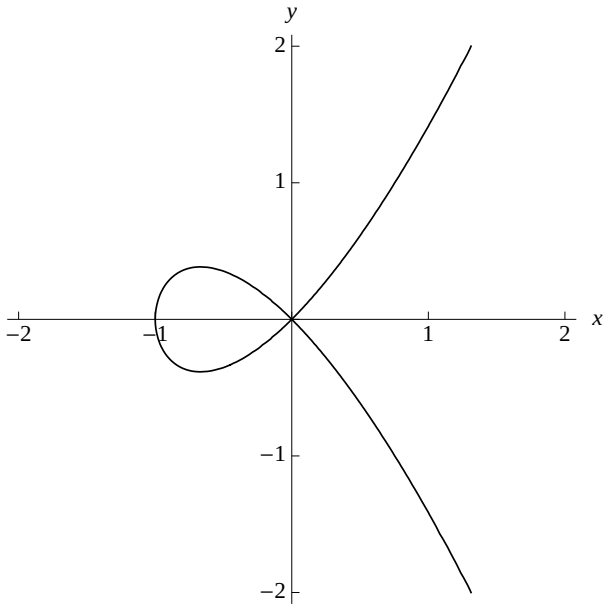

FIGURE 1. The curve $V = \mathbb{V}(X^3 + X^2 - Y^2)$.

That is, if X is irreducible and $X = U \cup V$, then $X = U$ or $X = V$. We call such an algebraic set an *affine variety*. Affine varieties have the following nice algebraic property. The proof here is the one given to Proposition 3, p. 198, of [2].

Proposition 2.1. *An algebraic set V is irreducible if and only if $\mathbb{I}(V)$ is prime.*

Proof. Suppose V is irreducible, and $FG \in \mathbb{I}(V)$. Let $V_1 = V \cap \mathbb{V}(F)$ and $V_2 = V \cap \mathbb{V}(G)$. Since $FG \in \mathbb{I}(V)$, then $V = V_1 \cup V_2$. Well, V is irreducible, so without loss of generality, suppose $V = V_1$. Then $F(P) = 0$ for all $P \in V$, so $F \in \mathbb{I}(V)$.

Conversely, suppose $\mathbb{I}(V)$ is prime and that $V = V_1 \cup V_2$, where $V \neq V_1$. Since $V_2 \subseteq V$, it is easy to see that $\mathbb{I}(V) \subseteq \mathbb{I}(V_2)$. Additionally, since $V_1 \subsetneq V$, $\mathbb{I}(V) \subsetneq \mathbb{I}(V_1)$, so we can pick $F \in \mathbb{I}(V_1) - \mathbb{I}(V)$. Let $G \in \mathbb{I}(V_2)$. Then F vanishes on V_1 and G vanishes on V_2, so FG vanishes on $V = V_1 \cup V_2$. Thus $FG \in \mathbb{I}(V)$. This ideal is prime, so either $F \in \mathbb{I}(V)$ or $G \in \mathbb{I}(V)$. By our choice of F, we must have $G \in \mathbb{I}(V)$. Hence $\mathbb{I}(V) = \mathbb{I}(V_2)$. But this is only true if $V = V_2$, so V is irreducible. □

This establishes a one-to-one correspondence between affine varieties and prime ideals of $k[X_1, \ldots, X_n]$. This correspondence is one example illustrating the close relationship between algebraic sets and ideals of $k[X_1, \ldots, X_n]$.

We will often be interested in two curves whose defining polynomials have no common factors. We say that two such curves have no common components. In the case that these are plane curves, this condition allows us to say something quite strong about their intersection — it must be finite.

Proposition 2.2. *Let F and G be polynomials in $k[X, Y]$ with no common factors. Then $\mathbb{V}(F, G) = \mathbb{V}(F) \cap \mathbb{V}(G)$ is a finite set of points.*

Proof. We first note that $k[X, Y] \cong k[X][Y]$. If F and G have no common factors in $k[X, Y]$, then they gain no common factor when we pass to the ring $k(X)[Y]$, which allows coefficients to be rational functions in X. Since F and G are coprime and $k(X)[Y]$ is a principal ideal domain, that is, a ring in which every ideal is generated by a single element, it follows that $(F, G) = (1)$. Then we can write $RF + SG = 1$ for some $R, S \in k(X)[Y]$. We can choose a polynomial $D \in k[X]$ such that $A = RD$ and $B = SD$ are polynomials in $k[X, Y]$. Then $AF + BG = D$. But notice for any $(a, b) \in \mathbb{V}(F, G)$, we have $AF + BG = 0$, so a must be a root of D. D has finitely many roots, so there are only finitely many such a values. By a similar argument, instead considering F and G in $k(Y)[X]$, we also have finitely many b values for $(a, b) \in \mathbb{V}(F, G)$. Thus $\mathbb{V}(F, G)$ is finite. □

We now define some of the key objects with which we will be working. Given an affine variety V, let $\Gamma(V) = k[X_1, \ldots, X_n]/\mathbb{I}(V)$. We call $\Gamma(V)$ the *coordinate ring* of V. Since $\mathbb{I}(V)$ is prime, $\Gamma(V)$ is an integral domain. This allows us to form its quotient field, which we denote $k(V)$. This is called the *field of rational functions on V*. Given any $P \in V$, we say that $f \in k(V)$ is defined at P if we can write $f = g/h$, where $g, h \in \Gamma(V)$ and $h(P) \neq 0$. We define $\mathcal{O}_P(V)$ to be the subset of $k(V)$ of rational functions defined at P. This subset is a subring of $k(V)$ which contains $\Gamma(V)$ and is called the *local ring of V at P*. If $V = \mathbb{A}^n$, then $\mathbb{I}(V) = \{0\}$, so $\Gamma(\mathbb{A}^n) = k[X_1, \ldots, X_n]$. Thus $\mathcal{O}_P(\mathbb{A}^n)$ consists of all rational functions defined at P.

Recall that a ring is *local* if it has a unique maximal ideal. True to its name, our ring $\mathcal{O}_P(V)$ is a local ring whose maximal ideal is $\mathfrak{m}_P(V) = \{g/h \mid g(P) = 0, h(P) \neq 0\}$. This consists of exactly the non-units in $\mathcal{O}_P(V)$, as any $g/h \notin \mathfrak{m}_P(V)$ satisfies $g(P) \neq 0$, so $h/g \in \mathcal{O}_P(V)$.

One of the most important and useful tools for studying the relationship between affine algebraic sets and ideals is the following theorem, known as the Nullstellensatz. Recall that the *radical* of an ideal I in a commutative ring R is the ideal $r(I) = \{a \in R \mid a^n \in I \text{ for some } n > 0\}$.

Theorem 2.3 (Hilbert's Nullstellensatz)**.** *Let I be an ideal in $k[X_1, \ldots, X_n]$, where k is algebraically closed. Then $\mathbb{I}(\mathbb{V}(I)) = r(I)$.*

The proof of this theorem relies on what is known as the Weak Nullstellensatz, which states that $\mathbb{V}(I)$ is nonempty if I is a proper ideal in $k[X_1, \ldots, X_n]$. This result is only true over algebraically closed fields: if we take $k = \mathbb{R}$ and $I = (X^2 + 1)$, then $\mathbb{V}(I) = \varnothing$, but $I \neq \mathbb{R}[X]$. A proof of the both theorems can be found in Chapter 4 of [2].

Recall that $k[X_1, \ldots, X_n]$ can be realized as an infinite-dimensional vector space over k whose basis is the set of all monomials in $X_1, \ldots, X_n$. If I is an ideal of $k[X_1, \ldots, X_n]$, then $k[X_1, \ldots, X_n]/I$ is also a vector space. In this case a basis consists of the residues

the monomials from $k[X_1, \ldots, X_n]$. The following is an important corollary to the Nullstellensatz.

Corollary 2.4. *Let I be an ideal in $k[X_1, \ldots, X_n]$. Then $\mathbb{V}(I)$ is a finite set if and only if $k[X_1, \ldots, X_n]/I$ is a finite-dimensional vector space over k. In this case, the size of $\mathbb{V}(I)$ is at most $\dim_k(k[X_1, \ldots, X_n]/I)$.*

We illustrate this corollary with the following example. A proof of the corollary is given in [3] (proof of Corollary 4, p. 11).

Example 2.5. Let $F(X, Y) = X^3 + X^2 - Y^2$, as in Figure 1. Then $\mathbb{V}(F)$ is an infinite set. By Corollary 2.4, $k[X, Y]/(F)$ should be infinite-dimensional. To see why this is the case, note that in $k[X, Y]/(F)$, we have $Y^2 = X^3 + X^2$. Given any polynomial $G \in k[X, Y]/(F)$, we can express G as a polynomial of the from $G(X, Y) = G_1(X) + YG_2(X)$, by reducing any term of G containing Y^2. Then it's clear $k[X, Y]/(F)$ is infinite dimensional, since (the residues of) $1, X, X^2, \ldots$ are linearly independent.

Let $H(X, Y) = X - Y + 1$. It's clear from the figure below that $\mathbb{V}(F, H)$ consists of three points. A little algebra shows that these points are $(-1, 0)$, $(\frac{1}{2}(1-\sqrt{5}), \frac{1}{2}(3-\sqrt{5}))$, and $(\frac{1}{2}(1+\sqrt{5}), \frac{1}{2}(3+\sqrt{5}))$, which are the roots of the polynomial $F(X, X+1) = X^3 - 2X - 1$. Notice also that $k[X, Y]/(F, H) \cong k[X]/(F(X, X+1))$. We can use the identification $X^3 = 2X - 1$ to reduce any polynomial in this ring to one with degree at most 2, so as a vector space, this ring has dimension 3.

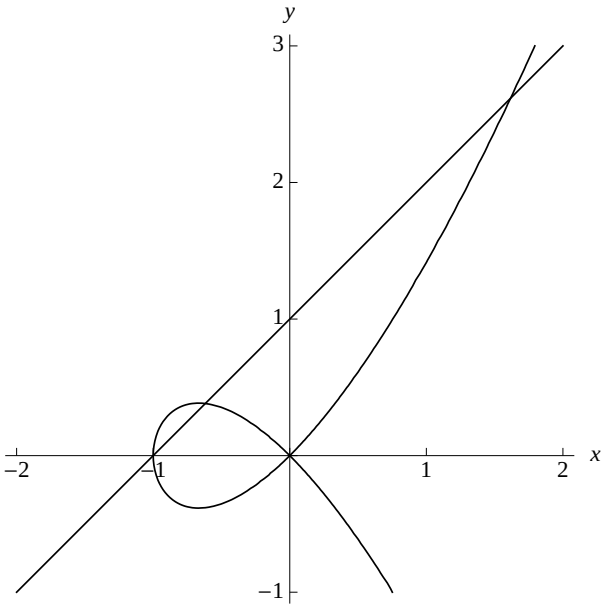

FIGURE 2. The curves $V = \mathbb{V}(X^3 + X^2 - Y^2)$ and $V' = \mathbb{V}(X - Y + 1)$.

In the same vein, in the case that $\mathbb{V}(I)$ is finite, we are able to relate the ideal $k[X_1, \ldots, X_n]/I$ to the local rings of the points of $\mathbb{V}(I)$.

Proposition 2.6. *Let I be an ideal in $k[X_1, \ldots, X_n]$, and suppose $\mathbb{V}(I) = \{P_1, \ldots, P_N\}$ is a finite set. Then there is a natural isomorphism between $k[X_1, \ldots, X_n]/I$ and $\prod_{i=1}^{N} \mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n)$.*

The isomorphism here is straightforward to define. Since there is a natural injection of $k[X_1, \ldots, X_n]$ into $\mathcal{O}_{P_i}(\mathbb{A}^n)$, there's a natural map $\varphi_i \colon k[X_1, \ldots, X_n]/I \to \mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n)$ for each i. Then we can define a homomorphism $\varphi \colon k[X_1, \ldots, X_n]/I \to \prod_{i=1}^{N} \mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n)$ such that $\varphi(F) = (\varphi_1(F), \ldots, \varphi_N(F))$. The real work here is in showing the map φ is an isomorphism; full details may be found in the proof of Proposition 6, p. 26, of [3].

There are two immediate consequences of this proposition.

Corollary 2.7. *If $\mathbb{V}(I) = \{P_1, \ldots, P_N\}$, then*

$$\dim_k(k[X_1, \ldots, X_n]/I) = \sum_{i=1}^{N} \dim_k(\mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n)).$$

Corollary 2.8. *If $\mathbb{V}(I) = \{P\}$, then there is an isomorphism between $k[X_1, \ldots, X_n]/I$ and $\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n)$.*

Given an ideal I, Proposition 2.6 relates $k[X_1, \ldots, X_n]/I$ to the local rings of $\mathbb{A}^n$ at the points in $\mathbb{V}(I)$. However, we are often more interested in the local rings of some affine variety V at these points. If $I = \mathbb{I}(V)$ for some affine variety V, then these rings are related in the following way.

Proposition 2.9. *Let V be a variety in $\mathbb{A}^n$, let $I = \mathbb{I}(V) \subseteq k[X_1, \ldots, X_n]$, let $P \in V$, and let J be an ideal of $k[X_1, \ldots, X_n]$ that contains I. Let J' be the image of J in $\Gamma(V)$. Then there is a natural isomorphism φ from $\mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n)$ to $\mathcal{O}_P(V)/J'\mathcal{O}_P(V)$.*

Proof. Consider the following diagram

$$\begin{array}{ccc} \mathcal{O}_P(\mathbb{A}^n) & \xrightarrow{\quad\alpha\quad} & \mathcal{O}_P(V) \\ {\scriptstyle q_1}\downarrow & & \downarrow{\scriptstyle q_2} \\ \mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) & \xrightarrow{\varphi} & \mathcal{O}_P(V)/J'\mathcal{O}_P(V). \end{array}$$

Here $\alpha(f/g) = \overline{f}/\overline{g}$, where $\overline{f}$ and $\overline{g}$ are the residues of f and g in $\Gamma(V)$, and q_1 and q_2 are the natural quotient maps. We then define φ so the diagram commutes, that is, so that $\varphi(\overline{f/g}) = q_2(\alpha(f/g))$.

Since α and q_2 are surjective, it follows that φ is surjective. We then check φ is injective. If $\varphi(\overline{f/g}) = 0$, then $q_2(\alpha(f/g)) = 0$, so $\alpha(f/g) \in J'\mathcal{O}_P(V)$. However, because $\ker\alpha = I\mathcal{O}_P(\mathbb{A}^n) \subseteq J\mathcal{O}_P(\mathbb{A}^n)$, we have $\alpha^{-1}(J'\mathcal{O}_P(V)) = J\mathcal{O}_P(\mathbb{A}^n)$, so $f/g \in \ker q_1$. Hence $\overline{f/g} = 0$. Thus φ is an isomorphism. □

It follows from this result that $\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n) \cong \mathcal{O}_P(V)$, since in the case that $J = I$, then $J' = 0$.

We saw earlier that we can realize $k[X_1, \ldots, X_n]/I$ as a vector space; treating this ring and $\mathcal{O}_P(V)$ as vector spaces will prove to be a useful tool for understanding the intersection number of curves. For this reason, we recall the rank-nullity theorem, a standard fact from linear algebra.

Theorem 2.10. *If $\varphi\colon U \to V$ is a linear transformation, then*

$$\dim(\mathrm{Im}\varphi) + \dim(\ker\varphi) = \dim U.$$

This theorem has an important and useful corollary pertaining to short exact sequences.

Corollary 2.11. *If*

$$0 \longrightarrow U \xrightarrow{\psi} V \xrightarrow{\varphi} W \longrightarrow 0$$

is an exact sequence of vector spaces, then $\dim U + \dim W = \dim V$.

Proof. Consider the map $\varphi\colon V \to W$. By Theorem 2.10, $\dim(\mathrm{Im}\varphi) + \dim(\ker\varphi) = \dim V$. Since the sequence is exact, φ is surjective, ψ is injective, and $\ker\varphi = \mathrm{Im}\psi$. Then $\mathrm{Im}\varphi = W$ and $\ker\varphi = U$, so $\dim U + \dim W = \dim(\ker\varphi) + \dim(\mathrm{Im}\varphi) = \dim V$. □

We conclude this section with a quick discussion of affine changes of coordinates. We will often be examining the behavior of one or more polynomials at a particular point $P \in \mathbb{A}^2$. For many reasons, it is convenient to assume P is the origin. We are able to do this due to the homogeneity of affine space,[2] however we must give special care to how we transform the polynomials in question. Although we will only deal with affine changes of coordinates on $\mathbb{A}^2$, we introduce it here in arbitrary dimension.

An *affine change of coordinates* on $\mathbb{A}^n$ is a map $T = (T_1, \ldots T_n)\colon \mathbb{A}^n \to \mathbb{A}^n$, where each T_i is linear and T is bijective. In particular, we can always write T as the composition of a linear map and a translation; it follows that T is a bijection if and only if the linear map is invertible. We apply our change of coordinates T to a polynomial F by defining $F^T = F(T_1, \ldots, T_n)$. This allows us define a map $\widetilde{T}\colon k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]$ by $\widetilde{T}(F) = F^T$. Notice that for all $P \in \mathbb{A}^n$, we have $F(T(P)) = F^T(P)$. We can also apply T to ideals and affine algebraic sets, where we let I^T be the ideal generated by $\{F^T \mid F \in I\}$ and $V^T = T^{-1}(V) = \mathbb{V}(I^T)$.

3. Projective Space

Although much can be said about algebraic curves in the affine plane, at some point the limitations of affine space become apparent. Consider the number of intersections

[2]Imprecisely, a space is homogeneous if it "looks the same" everywhere. With regard to the study of curves, this means that the relevant behavior of one or more curves is invariant under translation or other isometries.

of two distinct lines in $\mathbb{A}^2$. Ideally, we'd like to say any two lines meet in a single point; however, this isn't the case if the two lines are parallel. For another example, consider the intersection of the hyperbola $F(X,Y) = X^2 - Y^2 - 1$ and the line $G(X,Y) = Y - aX$ for any $a \in k$, where k is algebraically closed. In most cases, the intersection $F \cap G$ consists of two points. However, if $a = \pm 1$, F and G do not intersect at all, as G is an asymptote of F.

These two examples illustrate an incompleteness to the affine plane. We would like to give a uniform answer, one which does not depend on the position of the line or lines in question. In order to complete the plane, we add the missing intersection points as points at infinity, where parallel or asymptotic lines meet. With this in mind, we give the formal definition of this larger space.

Definition 3.1. *Projective n-space* over a field k, written $\mathbb{P}^n(k)$, is the set of lines through the origin in $\mathbb{A}^{n+1}(k)$.

Each point in $\mathbb{A}^{n+1}(k) - \{0\}$ determines a line through the origin, with two points describing the same line if and only if one is a nonzero scalar multiple of the other. Then we can identify $\mathbb{P}^n(k)$ with the space $(\mathbb{A}^{n+1}(k) - \{0\})/\sim$, where $x \sim y$ if $x = \lambda y$ for some nonzero $\lambda \in k$. This gives us a more natural way to talk about the space. We write a point $P \in \mathbb{P}^n(k)$ as $P = [x_1 : \ldots : x_{n+1}]$; any specific coordinates $x_1, \ldots, x_{n+1}$ are called *homogeneous coordinates* for P.

In general, a coordinate x_i of P is not well-defined, since by our equivalence relation, $[x_1 : \ldots : x_{n+1}] = [\lambda x_1 : \ldots : \lambda x_{n+1}]$ for all $\lambda \neq 0$. The exception is when $x_i = 0$. Notice that the set of points $\{[x_1 : \ldots : x_{n+1}] \mid x_i = 0\}$ is in one-to-one correspondence with $\mathbb{P}^{n-1}(k)$ via deletion of the ith coordinate. When $i = n+1$ we call this set the *hyperplane at infinity*, written H_∞. On the other hand, if we fix $x_i = 1$, then all n-tuples $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n+1})$ determine a point $[x_1 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_{n+1}]$ of $\mathbb{P}^n(k)$. In this way we can identify $n+1$ copies of $\mathbb{A}^n(k)$ with subsets of $\mathbb{P}^n(k)$. We let U_i denote the set of all points of $\mathbb{P}^n(k)$ with a nonzero ith coordinate. Thus we can write $\mathbb{P}^n(k) = U_{n+1} \cup H_\infty = \mathbb{A}^n(k) \cup \mathbb{P}^{n-1}(k)$.

Example 3.2. If $k = \mathbb{C}$ and $n = 1$, then the complex projective line $\mathbb{P}^1(\mathbb{C})$ is the set of lines through the origin in $\mathbb{C}^2$. Here we can identify $\mathbb{C}$ with the points $[z : 1] \in \mathbb{P}^1(\mathbb{C})$. There is a single point in $\mathbb{P}^1(\mathbb{C})$ which this map misses, $[1 : 0]$, which is the point at infinity. This space is known as the *extended complex plane* or the *Riemann sphere*.

At this point, as with affine n-space, we will write $\mathbb{P}^n$ instead of $\mathbb{P}^n(k)$ when k is clear from context.

Returning to our earlier examples, we see that the projective versions of these curves now intersect the expected number of times. The missing intersection points from the affine case lie in the hyperplane at infinity. Suppose we have two parallel lines $F(X,Y) = aX + bY + c$ and $G(X,Y) = aX + bY + d$. Each point (X,Y) on F corresponds to a point $[X : Y : 1]$ which satisfies the equation $aX + bY + cZ = 0$, and similarly each point (X',Y') on G corresponds to a point $[X' : Y' : 1]$ such that

$aX' + bY' + dZ' = 0$. These two equations define projective lines containing F and G. The point $[b : -a : 0]$ lies on both projective lines, and is the point at infinity at which the two lines intersect.

Similarly, in our example with the hyperbola $F(X, Y) = X^2 - Y^2 - 1$ and a line $G(X, Y) = Y - aX$, the zero locus of F is contained in the projective curve defined by $F'(X, Y, Z) = X^2 - Y^2 - Z^2 = 0$. This intersects the line $Z = 0$ at the points $[1 : 1 : 0]$ and $[1 : -1 : 0]$, which also lie on the projective lines $Y = \pm X$.

In these two examples, we had to alter our curves when we moved from affine space to projective space. For a general polynomial $F \in k[X_1, \ldots, X_{n+1}]$, if $F(x_1, \ldots, x_{n+1}) = 0$, it is not necessarily the case that $F(\lambda x_1, \ldots, \lambda x_{n+1}) = 0$ as well, although $[x_1 : \ldots : x_{n+1}]$ and $[\lambda x_1 : \ldots : \lambda x_{n+1}]$ define the same point in $\mathbb{P}^n$. Only when F is a form, a polynomial in which every term has the same degree, does F vanish on a well-defined subset of $\mathbb{P}^n$. We say that a point $P \in \mathbb{P}^n$ is a *zero* of F if F vanishes for all homogeneous coordinates for P.

This allows us to define the projective analogue of an affine algebraic set.

Definition 3.3. Let $S \subseteq k[X_1, \ldots, X_{n+1}]$. Let $\mathbb{V}(S) = \{P \mid P \text{ is a zero of each } F \in S\}$. Then a set $X \subseteq \mathbb{P}^n$ is a *projective algebraic set* if $X = \mathbb{V}(S)$ for some set of polynomials $S \subseteq k[X_1, \ldots, X_{n+1}]$.

As in the affine case, we define a *projective variety* to be an irreducible projective algebraic set.

We can also give analogous projective definitions for the objects $\Gamma(V)$, $k(V)$, $\mathcal{O}_P(V)$, and $\mathfrak{m}_P(V)$ for a projective variety V. If we let V be a nonempty projective variety, then, as in the affine case, $\mathbb{I}(V)$ is prime. Then $\Gamma(V) = k[X_1, \ldots, X_{n+1}]/\mathbb{I}(V)$ is an integral domain; we call this the *homogeneous coordinate ring* of V. We say that $f \in \Gamma(V)$ is a *form* if there is a form in $k[X_1, \ldots, X_n]$ whose residue is f. Since $\Gamma(V)$ is a domain, we can define its quotient field. However, most elements of this quotient field will not be well-defined as functions, since different homogeneous coordinates for the same point may give different values for the rational function. By restricting to only quotients of forms of the same degree, we resolve this problem, since if f and g are both forms of degree d, then $f(\lambda x)/g(\lambda x) = \lambda^d f(x)/\lambda^d g(x) = f(x)/g(x)$. This motivates our definition of the function field of V, $k(V)$, to be the set of rational functions f/g such that f and g are forms of the same degree. Then we let the local ring of V at a point P, $\mathcal{O}_P(V)$, be the set of rational functions in $k(V)$ which are defined at P. As in the affine case, we let $\mathfrak{m}_P(V)$ denote its unique maximal ideal.

We finish this section by describing a useful way we can move between forms in $k[X_1, \ldots, X_{n+1}]$ and polynomials in $k[X_1, \ldots, X_n]$. Given a polynomial $F \in k[X_1, \ldots, X_n]$, we may decompose F into a sum of forms $F = \sum_{i=0}^{m} F_i$, where every term in F_i has degree i. Then the polynomial $F^* = \sum_{i=0}^{m} X_{n+1}^{m-i} F_i$ is a form in $k[X_1, \ldots, X_{n+1}]$. This process is known as *homogenization*, and F^* is the homogenization of F. Note that if $(x_1, \ldots, x_n) \in \mathbb{V}(F)$, then $[x_1 : \ldots : x_n : 1] \in \mathbb{V}(F^*)$.

We may reverse this process to take a form F in $k[X_1, \ldots, X_{n+1}]$ to a polynomial in $k[X_1, \ldots, X_n]$, by letting $F_*(X_1, \ldots, X_n) = F(X_1, \ldots, X_n, 1)$; F_* is called the *dehomogenization* of F. If F is a form of degree m, then F_* will be a polynomial of degree at most m.

This process of homogenization and dehomogenization may also be applied to ideals and varieties. Given an ideal in $I \in k[X_1, \ldots, X_n]$, we define $I^* = \{F^* \mid F \in I\}$; if $I = \mathbb{I}(V)$ for some affine variety V, then we define $V^* = \mathbb{V}(I^*)$. We call V^* the projective closure of V, as it is the smallest projective variety containing V. Conversely, if I lives in $k[X_1, \ldots, X_{n+1}]$, then $I_* = \{F_* \mid F \in I\}$. If V is a projective variety such that $I = \mathbb{I}(V)$, then we define $V_* = \mathbb{V}(I_*)$.

4. Intersection Number

Before discussing intersection number, we will introduce a related concept, the multiplicity of a curve F at a point P. If $P = (0, 0)$, the multiplicity of F at P can be found by writing the polynomial $F = F_m + F_{m+1} + \ldots + F_n$, where F_k is a form of degree k in $k[X, Y]$, $F_m \neq 0$, and $n = \deg F$. Then F has multiplicity $m_P(F) = m$. If $P = (a, b) \neq (0, 0)$, we can compute $m_P(F)$ by applying the affine change of coordinates given by $T(X, Y) = (X + a, Y + b)$, which takes the origin to P. Then $m_P(F) = m_{(0,0)}(F^T)$.

Geometrically, $m_P(F)$ is the number of tangents to F at P, counting with multiplicity. In the case that $P = (0, 0)$, the form F_m is the product of the tangent lines to F at P. The following theorem shows that the multiplicity only depends on the local ring $\mathcal{O}_P(F)$, and in particular, the dimension of a particular quotient ring determined by $\mathcal{O}_P(F)$. Though more cumbersome to actually compute, this illustrates the relationship between the curve F and the algebraic structures introduced in Section 2.

Theorem 4.1. *Let P be a point on an irreducible curve F. Then for all sufficiently large n,*

$$m_P(F) = \dim_k(\mathfrak{m}_P(F)^n / \mathfrak{m}_P(F)^{n+1}).$$

Proof. For this proof, we shall write $\mathcal{O}$ for $\mathcal{O}_P(F)$ and $\mathfrak{m}$ for $\mathfrak{m}_P(F)$. We begin by considering the sequence

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^n \longrightarrow 0, \tag{4.2}$$

which is exact since $\mathfrak{m}^n \subseteq \mathcal{O}$ and $(\mathcal{O}/\mathfrak{m}^{n+1})/(\mathfrak{m}^n/\mathfrak{m}^{n+1}) \cong \mathcal{O}/\mathfrak{m}^n$ by the isomorphism theorems of rings. Each of the rings in (4.2) is a finite dimensional vector space, so by Corollary 2.11, $\dim_k(\mathcal{O}/\mathfrak{m}^{n+1}) = \dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) + \dim_k(\mathcal{O}/\mathfrak{m}^n)$. Note that if $\dim_k(\mathcal{O}/\mathfrak{m}^n) = nm_P(F) + s$ for a constant s, then

$$\begin{aligned}
\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) &= \dim_k(\mathcal{O}/\mathfrak{m}^{n+1}) - \dim_k(\mathcal{O}/\mathfrak{m}^n), \\
&= (n+1)m_P(F) + s - (nm_P(F) + s), \\
&= m_P(F).
\end{aligned}$$

Thus it suffices to show $\dim_k(\mathcal{O}/\mathfrak{m}^n) = nm_P(F) + s$ for sufficiently large n; it turns out that $n \geq m_P(F)$ suffices.

We may assume $P = (0,0)$ by applying an affine change of coordinates to P and F.

Let $I = (X, Y) \subseteq k[X, Y]$. We claim then that $\mathfrak{m}^n = I^n\mathcal{O}$. Note that $\mathfrak{m}^n$ is generated by products of n rational functions $f_i/g_i \in \mathfrak{m}$. Then each f_i vanishes at P and therefore is in I, so $f = f_1 \cdots f_n \in I^n$. Each g_i is nonzero at P, so their product doesn't vanish at P, either. Thus the reciprocal of $g_1 \cdots g_n$ is in $\mathcal{O}$, and therefore $\mathfrak{m}^n \subseteq I^n\mathcal{O}$. Conversely, I^n is generated by products of n polynomials f_i which vanish at P. Consider any $h/g \in \mathcal{O}$. Then $g(P) \neq 0$, so $f_n h/g \in \mathfrak{m}$. For $i < n$, we can take the rational functions $f_i/1 \in \mathfrak{m}$, so $(f_1/1) \cdots (f_n h/g) \in \mathfrak{m}^n$. Thus $I^n\mathcal{O} \subseteq \mathfrak{m}^n$.

Since $V(I^n, F) = \{P\}$, by Corollary 2.8 and Proposition 2.9,

$$k[X, Y]/(I^n, F) \cong \mathcal{O}_P(\mathbb{A}^2)/(I^n, F)\mathcal{O}_P(\mathbb{A}^2) \cong \mathcal{O}_P(F)/I^n\mathcal{O}_P(F).$$

As we just showed, $\mathcal{O}_P(F)/I^n\mathcal{O}_P(F) = \mathcal{O}/\mathfrak{m}^n$, so it suffices to compute the dimension of $k[X, Y]/(I^n, F)$. As above, we compute this by constructing an exact sequence of vector spaces. Let $m = m_P(F)$. Then $F \in I^m$, so $FG \in I^n$ whenever $G \in I^{n-m}$, for $n \geq m$. We then define $\psi\colon k[X, Y]/I^{n-m} \to k[X, Y]/I^n$ by $\psi(\overline{G}) = \overline{FG}$, the residue of FG modulo I^n. We similarly define $\varphi\colon k[X, Y]/I^n \to k[X, Y]/(I^n, F)$ by mapping $\varphi(\overline{H})$ to the residue of $\overline{H}$ modulo F. Then the sequence

$$0 \longrightarrow k[X, Y]/I^{n-m} \xrightarrow{\psi} k[X, Y]/I^n \xrightarrow{\varphi} k[X, Y]/(I^n, F) \longrightarrow 0$$

is exact; it's clear ψ is injective and φ is surjective, and moreover by the construction of ψ, $\ker\varphi = \mathrm{Im}\psi$. Thus

$$\begin{aligned}\dim_k(k[X, Y]/(I^n, F)) &= \dim_k(k[X, Y]/I^n) - \dim_k(k[X, Y]/I^{n-m}),\\ &= \frac{n(n+1)}{2} - \frac{(n-m)(n-m+1)}{2},\\ &= nm - \frac{m(m-1)}{2}.\end{aligned}$$

Since $-\frac{m(m-1)}{2}$ does not depend on n, it is the constant s such that $\dim_k(\mathcal{O}/\mathfrak{m}^n) = nm_P(F) + s$. Hence whenever $n \geq m$, we have $m = \dim_k(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1})$. □

For the remainder of this section, we will denote $\mathcal{O}_P(\mathbb{A}^2)$ by $\mathcal{O}$ and $\mathfrak{m}_P(\mathbb{A}^2)$ by $\mathfrak{m}$ when P is clear, unless otherwise noted.

The following properties describe properties we want the intersection number of two curves to satisfy. They begin broadly, specifying generally when the intersection number should be infinite or zero. We also want the intersection number to be independent of where in the affine plane our curves are located, and therefore it should be invariant under affine changes of coordinates. The fourth property describes the symmetry of the intersection number, in a sense: since $F \cap G = G \cap F$, we desire that the intersection number of these be equal. The last three properties specify how the intersection number can be calculated, and suggest a method for doing so.

(1) $I(P, F \cap G)$ is a nonnegative integer for any F, G, and P such that F and G share no common component which passes through P (in which case we say F and G *intersect properly* at P). $I(P, F \cap G) = \infty$ if F and G do not intersect properly at P.
(2) $I(P, F \cap G) = 0$ if and only if $P \notin F \cap G$. $I(P, F \cap G)$ depends only on the components of F and G that pass through P. And $I(P, F \cap G) = 0$ if F or G is a nonzero constant.
(3) If T is an affine change of coordinates on $\mathbb{A}^2$, and $T(Q) = P$, then $I(P, F \cap G) = I(Q, F^T \cap G^T)$.
(4) $I(P, F \cap G) = I(P, G \cap F)$.
(5) If $F = \prod F_i^{r_i}$ and $G = \prod G_j^{s_j}$, then $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$, that is, intersection number is additive over unions.
(6) $I(P, F \cap G) = I(P, F \cap (G + AF))$ for any $A \in k[X, Y]$.
(7) $I(P, F \cap G) \geq m_P(F) m_P(G)$, with equality if and only if F and G have no tangent lines in common at P.

Many of these properties are intuitive, and they also give us a straightforward method for computing the intersection number of two curves, which ultimately relies on computing the multiplicity of certain curves at the given point. The following example illustrates how this can be done.

Example 4.3. Consider the two curves

$$E = (X^2 + Y^2)^2 + 3X^2Y - Y^3,$$
$$F = (X^2 + Y^2)^3 - 4X^2Y^2,$$

and the point $P = (0, 0)$. We want to compute $I(P, E \cap F)$, using the properties above to simplify E and F. Consider $F - (X^2+Y^2)E = -4X^2Y^2 - (X^2+Y^2)(3X^2Y - Y^3)$. Since Y divides this, we may write $F - (X^2+Y^2)E = YG$ for the appropriate polynomial G. Now we may replace G with $G + 3E$ to get the polynomial $4X^2Y^2 + 4Y^4 + 5X^2Y - 3Y^3 = YH$ for another polynomial H. Using properties (6) and (7), then

$$\begin{aligned} I(P, E \cap F) &= I(P, E \cap YG), \\ &= I(P, E \cap Y) + I(P, E \cap G), \\ &= I(P, E \cap Y) + I(P, E \cap YH), \\ &= 2I(P, E \cap Y) + I(P, E \cap H). \end{aligned}$$

Note that $E - (2X^2Y + Y^3 + 3X^2 - Y^2)Y = X^4$, so $I(P, E \cap Y) = I(P, X^4 \cap Y)$, again by property (7), and property (4). Since X^4 and Y clearly share no tangent lines at P, we may use property (5) to compute $I(P, X^4 \cap Y) = m_P(X^4) m_P(Y) = 4$. We can also use property (5) to compute $I(P, E \cap H)$, since the tangent lines of each at $P = (0, 0)$ are simply the linear factors of the lowest degree form in the homogeneous decomposition of each curve. For E, this form is $3X^2Y - Y^3 = Y(\sqrt{3}X - Y)(\sqrt{3}X + Y)$, and for H it's

$5X^2-3Y^2 = (\sqrt{5}X-\sqrt{3}Y)(\sqrt{5}X+\sqrt{3}Y)$, thus E and F do not share tangent lines at P. Hence by property (5), $I(P, E\cap H) = m_P(E)m_P(H) = 6$, so $I(P, E\cap F) = 2\cdot 4+6 = 14$.

This example suggests a systematic method for computing the intersection number of two curves at a given point, but it's not immediate that this process always works, nor that it determines a unique number. In fact this is the case, as we prove below. We are also able to write down an explicit expression for the intersection number in terms of the dimension of a particular quotient ring. The approach here is an expanded version of the proof given in [3].

Theorem 4.4. *Given any two curves $F, G \in k[X, Y]$ and any point $P \in \mathbb{A}^2$, properties* (1)–(7) *uniquely determine their intersection number,*

$$I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G)).$$

There are two parts to this proof; the first formalizes the process used in the example above to show the seven properties give a unique intersection number, and the second part shows the intersection number is the quantity claimed, that is, that $\dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G))$ satisfies the seven properties given. Roughly, these are uniqueness and existence proofs, respectively. We begin with the proof of uniqueness.

Proof of Uniqueness. By property (3), we may assume $P = (0, 0)$. If F and G share a common component, then by property (1), $I(P, F \cap G) = \infty$, so we may assume they share no component, and $I(P, F \cap G) < \infty$. We then proceed by induction on the intersection number. For the base case, property (2) tells us that $I(P, F\cap G) = 0$ if and only if $P \notin F \cap G$.

Now suppose $I(P, F \cap G) = n > 0$, and for all curves A and B such that $I(P, A \cap B) < n$, we have a method to compute $I(P, A \cap B)$ from properties (1)–(7). Let $r = \deg(F(X, 0))$ and $s = \deg(G(X, 0))$, where we take either to be 0 if the corresponding polynomial is zero. By property (4), $I(P, F \cap G) = I(P, G \cap F)$, so we may assume $r \leq s$. We consider two cases, based on r.

Case 1: $r = 0$. Then $F(X, 0) = 0$, so $Y \mid F$. Then we can write $F = YH$, and by property (6), $I(P, F \cap G) = I(P, Y \cap G) + I(P, H \cap G)$. Now consider writing $G(X, 0) = X^m(a_0 + a_1X + \ldots + a_{s-m}X^{s-m})$. Note that since $I(P, F \cap G) < \infty$, by property (1), F and G cannot share a common component. In particular, Y does not divide G, so $m > 0$. Note that $I(P, Y \cap G) = I(P, Y \cap G(X, 0))$ by property (7), which allows us to subtract off all terms containing Y from G without changing the intersection number. Then

$$\begin{aligned} I(P, Y \cap G) &= I(P, Y \cap G(X, 0)), \\ &= I(P, Y \cap X^m) + I(P, Y \cap (a_0 + a_1X + \ldots + a_{s-m}X^{s-m})), \\ &= m + 0 = m, \end{aligned}$$

by properties (2), (5), and (6). Since m is positive, $I(P, H \cap G) < n$, so by our inductive hypothesis we have a method to compute $I(P, H \cap G)$, and therefore we can compute $I(P, F \cap G)$.

Case 2: $r > 0$. Multiplying by constants if necessary, we may assume both $F(X, 0)$ and $G(X, 0)$ are monic. Let $H = G - X^{s-r}F$. By property (7), $I(P, F \cap G) = I(P, F \cap H)$, and $\deg H(X, 0) = t < s$, since the leading terms of G and $X^{s-r}F$ cancel. We may repeat this process, using property (4) whenever the degree of the first polynomial exceeds that of the second, until we reach two curves A and B such that $A(X, 0) = 0$. This process preserves intersection number, so $I(P, F \cap G) = I(P, A \cap B)$, and so by Case 1, we can compute $I(P, F \cap G)$. □

Proof of Existence. Let $I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G))$. We show $I(P, F \cap G)$ satisfies properties (1)–(7).

(1): By Corollary 2.7, if F and G intersect properly at P, then $I(P, F \cap G) = \dim_k(\mathcal{O}/(F, G))$ is finite. Now suppose F and G have a common component H, and therefore do not intersect properly. Then $(F, G) \subseteq (H)$. We can then define a natural ring homomorphism from $\mathcal{O}/(F, G)$ onto $\mathcal{O}/(H)$. Thus $I(P, F \cap G) = \dim_k(\mathcal{O}/(F, G)) \geq \dim_k(\mathcal{O}/(H))$, so it is enough to show $\mathcal{O}/(H)$ is infinite-dimensional. Well, by Proposition 2.9, $\mathcal{O}/(H) \cong \mathcal{O}_P(H)$. By construction, this latter ring contains $\Gamma(H)$, so $\dim_k(\mathcal{O}/(H)) \geq \dim_k(\Gamma(H))$. Since $\mathbb{V}(H)$ is infinite, by Corollary 2.4, $\Gamma(H)$ is infinite-dimensional. Thus $I(P, F \cap G) = \infty$.

(2): Suppose $I(P, F \cap G) = 0$. Then $\dim_k(\mathcal{O}/(F, G)) = 0$, so $(F, G) = \mathcal{O}$. Then for some $A, B \in \mathcal{O}$, $AF + BG = 1$. But then either $F(P) \neq 0$ or $G(P) \neq 0$, so $P \notin F \cap G$. On the other hand, if $P \notin F \cap G$, then without loss of generality assume that $F(P) \neq 0$. Then $\frac{1}{F} \in \mathcal{O}$, so $1 = \frac{1}{F} \cdot F \in (F, G)$, and thus $I(P, F \cap G) = 0$. The second statement follows because $I(P, F \cap G)$ only depends on $(F, G) \subseteq \mathcal{O}$ and $\frac{1}{H} \in \mathcal{O}$ for any component H of F or G which does not contain P. Lastly, if, say, $F = a \neq 0$, then $(F, G) = \mathcal{O}$, so $I(P, F \cap G) = 0$.

(3): Consider the change of coordinates $T(X, Y) = (aX + b, cY + d)$, for $a, b, c, d \in k$. T induces the map $\widetilde{T}\colon \mathcal{O}_P(\mathbb{A}^2) \to \mathcal{O}_Q(\mathbb{A}^2)$ given by $\widetilde{T}(F) = F^T$, where $Q = T(P)$. Since T is an isomorphism, $\widetilde{T}$ is as well. But then

$$I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G)) = \dim_k(\mathcal{O}_Q(\mathbb{A}^2)/(F^T, G^T)) = I(Q, F^T \cap G^T).$$

(4): The fourth property is perhaps the simplest. Note that $(F, G) = (G, F)$, so

$$I(P, F \cap G) = \dim_k(\mathcal{O}/(F, G)) = \dim_k(\mathcal{O}/(G, F)) = I(P, G \cap F).$$

(5): It suffices to show $I(P, F \cap GH) = I(P, F \cap G) + I(P, F \cap H)$, since we may then extend to any finite product by induction. If F and GH have a common component, F and either G or H must also have a common component, so $I(P, F \cap GH) = \infty = I(P, F \cap G) + I(P, F \cap H)$ by property (1). Then we may assume F and GH do not have a common component. Define $\varphi\colon \mathcal{O}/(F, GH) \to \mathcal{O}/(F, G)$ which takes $\overline{z}$ to its residue modulo G. Then define $\psi\colon \mathcal{O}/(F, H) \to \mathcal{O}/(F, GH)$ by $\psi(\overline{z}) = \overline{Gz}$. Consider

the sequence

$$0 \longrightarrow \mathcal{O}/(F,H) \xrightarrow{\psi} \mathcal{O}/(F,GH) \xrightarrow{\varphi} \mathcal{O}/(F,G) \longrightarrow 0.$$

We first see that ψ is injective. Suppose $\psi(\overline{z}) = \overline{Gz} = 0$. Then we can write $Gz = uF + vGH$ for some $u, v \in \mathcal{O}$. Choose a polynomial $S \in k[X,Y]$ such that $S(P) \neq 0$. Let $A = Su$, $B = Sv$, and $C = Sz$. Then $GC = AF + BGH$, so $G(C - BH) = AF$. By assumption, F and G have no common component, so F must divide $C - BH$, say $C - BH = DF$. But then $C = BH + DF$, so, dividing through by S, $z = (B/S)H + (D/S)F$. Since $S(P) \neq 0$, B/S and D/S are in $\mathcal{O}$, so $\overline{z} = 0$.

Note that $\varphi(\overline{Gz}) = 0$ for all $z \in \mathcal{O}$, and if $\varphi(\overline{z}) = 0$, then $\overline{z} = G\overline{y} = \overline{Gy}$ for some $y \in \mathcal{O}$, so $\overline{z} = \psi(\overline{y})$. Hence $\mathrm{Im}\psi = \ker\varphi$. Finally, it's clear that φ is surjective, so the above sequence is exact. Since the three rings in our sequence are finite-dimensional vector spaces, two applications of Corollary 2.11 tell us

$$\begin{aligned} I(P, F \cap GH) &= \dim_k(\mathcal{O}/(F,GH)), \\ &= \dim_k(\mathcal{O}/(F,G)) + \dim_k(\mathcal{O}/(F,H)) = I(P,F\cap G) + I(P,F\cap H). \end{aligned}$$

(6): Like property (4), property (6) follows from the fact that $I(P, F \cap G)$ depends only on the ideal generated by F and G. Since $(F,G) = (F, G+AF)$ for any $A \in k[X,Y]$, it follows that

$$\begin{aligned} I(P, F \cap G) &= \dim_k(\mathcal{O}/(F,G)), \\ &= \dim_k(\mathcal{O}/(F,G+AF)) = I(P, F \cap (G+AF)). \end{aligned}$$

(7): This proof relies heavily on computing the dimensions of different vector spaces. Let $m = m_P(F)$ and $n = m_P(G)$. We wish to show $I(P, F \cap G) \geq mn$. Property (3) allows us to apply an affine change of coordinates without changing the intersection number, so we may assume $P = (0,0)$. Recall that $I = (X,Y) \subseteq k[X,Y]$. Consider the commutative diagram

$$\begin{array}{ccccccc} k[X,Y]/I^n \times k[X,Y]/I^m & \xrightarrow{\psi} & k[X,Y]/I^{m+n} & \xrightarrow{\varphi} & k[X,Y]/(I^{m+n},F,G) & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \alpha} & & \\ & & \mathcal{O}/(F,G) & \xrightarrow{\pi} & \mathcal{O}/(I^{m+n},F,G) & \longrightarrow & 0, \end{array}$$

where φ and π are the natural surjections, and α is the map induced by the map from $k[X,Y]$ to $\mathcal{O}$. Note that the top row is exact: φ is surjective and $\varphi(\overline{C}) = 0$ if and only if $\overline{C} = \overline{A}F + \overline{B}G$ for some $\overline{A} \in k[X,Y]/I^n$ and $\overline{B} \in k[X,Y]/I^m$, which is true if and only if $\overline{C} = \psi(\overline{A}, \overline{B})$, so $\mathrm{Im}\psi = \ker\varphi$. Then

$$\begin{aligned} \dim_k(k[X,Y]/I^n) + \dim(k[X,Y]/I^m) &= \dim(k[X,Y]/I^n \times k[X,Y]/I^m), \\ &\geq \dim_k(\mathrm{Im}\psi) = \dim_k(\ker\varphi). \end{aligned} \tag{4.5}$$

By Theorem 2.10,

$$\dim_k(k[X,Y]/(I^{m+n},F,G)) + \dim_k(\ker\varphi) = \dim_k(k[X,Y]/I^{m+n}). \tag{4.6}$$

Additionally, since $\mathbb{V}(I^{m+n},F,G) \subseteq \{P\}$, by Corollary 2.8, α is an isomorphism. Combining all of these facts, we have that

$$\begin{aligned}
I(P,F\cap G) &= \dim_k(\mathcal{O}/(F,G)),\\
&\geq \dim_k(\mathcal{O}/(I^{m+n},F,G)) && \text{since } \pi \text{ is surjective,}\\
&= \dim_k(k[X,Y]/(I^{m+n},F,G)) && \text{since } \alpha \text{ is an isomorphism,}\\
&= \dim_k(k[X,Y]/I^{m+n}) - \dim_k(\ker\varphi) && \text{by (4.6),}\\
&\geq \dim_k(k[X,Y]/I^{m+n}) - \dim_k(k[X,Y]/I^n)\\
&\quad - \dim_k(k[X,Y]/I^m) && \text{by (4.5).}
\end{aligned}$$

Lastly, since $\dim_k(k[X,Y]/I^k) = \binom{k}{2}$, we have that

$$I(P,F\cap G) \geq \binom{m+n}{2} - \binom{m}{2} - \binom{n}{2} = mn.$$

Then we have that $I(P,F\cap G) = mn$ if and only if the two inequalities in the previous equation hold at equality. The first inequality holds if $I^{m+n} \subseteq (F,G)\mathcal{O}$, in which case π is the identity map. The second holds when (4.5) is equality, that is, if and only if ψ is injective. By Lemmas 4.7 and 4.8 below, both are equalities exactly when F and G have no common tangents at P, as desired. □

As in the proof above, let F and G be curves with multiplicities m and n, respectively, at the point $P = (0,0)$.

Lemma 4.7. *If F and G have no common tangents at P, then $I^t \subseteq (F,G)\mathcal{O}$ for $t \geq m+n-1$.*

Proof. Let $L_1,\dots,L_m$ denote the tangents to F at P, and similarly $M_1,\dots,M_n$ denote the tangents to G at P; let $L_i = L_m$ when $i > m$ and $M_j = M_n$ when $j > n$. Lastly, let $A_{ij} = L_1\cdots L_iM_1\cdots M_j$ for all $i,j \geq 0$, with $A_{00} = 1$.

We claim that the set $\{A_{ij} \mid i+j = t\}$ is a basis for forms of degree t in $k[X,Y]$. Note that this vector space has dimension $t+1$, since the monomials X^iY^{t-i}, for $0 \leq i \leq t$, form a basis for it. Since there are $t+1$ forms A_{ij} with $i+j=t$, it suffices to show the A_{ij}'s are linearly independent. Suppose they are not, so for some ℓ, we can write $A_{\ell\, t-\ell} = \sum_{i=0}^{\ell-1}\lambda_iA_{i\,t-i}$ for $\lambda_i \in k$. But by construction, the form $M_{t-\ell+1}$ divides $A_{i\,t-i}$ for $i < \ell$, but does not divide $A_{\ell\,t-\ell}$, a contradiction. Thus $\{A_{ij} \mid i+j=t\}$ is a basis. It follows then that I^t is generated by the forms A_{ij} where $i+j \geq t$, so we are done if we can show $A_{ij} \in (F,G)\mathcal{O}$ for $i+j \geq m+n-1$.

Note that if $i+j \geq m+n-1$, then we must have $i \geq m$ or $j \geq n$. Without loss of generality, suppose $i \geq m$. Then $A_{ij} = A_{m0}B$, where the degree of B is $i+j-m$. Since $A_{m0} = F_m$, we can write $F = A_{m0} + F'$, where F' is a polynomial in I^{m+1}. Then

$A_{ij} = A_{m0}B = FB - F'B$, and each term in $F'B$ has degree at least $(i+j-m)+(m+1) = i+j+1$.

It now suffices to show that $F'B \in (F,G)\mathcal{O}$, as then $A_{ij} \in (F,G)\mathcal{O}$ whenever $i+j \geq m+n-1$. We can do this by repeating the argument above for each form F_iB of $F'B$, $i > m$. Then if $I^t \subseteq (F,G)\mathcal{O}$ for some sufficiently large t, then we can work backwards to see $F'B \in (F,G)\mathcal{O}$.

To see why such a t exists, let $\mathbb{V}(F,G) = \{P, Q_1, \ldots, Q_s\}$. We can then find a polynomial H that vanishes at each Q_i, but $H(P) \neq 0$. Consider the polynomials HX and HY. Since $P = (0,0)$, both vanish at P, so $HX, HY \in \mathbb{I}(\mathbb{V}(F,G))$. By the Nullstellensatz, for some N, $(HX)^N, (HY)^N \in (F,G)$. Additionally, since $H(P) \neq 0$, $\frac{1}{H} \in \mathcal{O}$, so $\frac{1}{H^N}(HX)^N = X^N \in (F,G)\mathcal{O}$, and similarly $Y^N \in (F,G)\mathcal{O}$. Lastly, note that $I^{2N} \subseteq (X^N, Y^N) \subseteq (F,G)\mathcal{O}$, since if $X^aY^b \in I^{2N}$, then $a+b \geq 2N$, so $a \geq N$ or $b \geq N$. □

Lemma 4.8. *Let*

$$\psi\colon k[X,Y]/I^n \times k[X,Y]/I^m \to k[X,Y]/I^{m+n}$$

be defined by $\psi(\overline{A}, \overline{B}) = \overline{AF + BG}$*, as above. Then* ψ *is one-to-one if and only if* F *and* G *have distinct tangents at* P*.*

Proof. ($\Leftarrow$) Suppose F and G have distinct tangents at P, and $\psi(\overline{A}, \overline{B}) = \overline{AF - BG} = 0$. Then every term of $AF + BG$ must have degree at least $m+n$. Let $r = m_P(A)$ and $s = m_P(B)$. Then $AF + BG = A_rF_m + B_sG_n + \ldots$. Suppose $r < n$ or $s < m$. Then A_rF_m or B_sG_n has degree less than $m+n$. In fact, we see that both must have the same degree, and $A_rF_m + B_sG_n = 0$. Then $A_rF_m = -B_sG_n$, however since F and G have distinct tangents, F_m and G_n share no common factors. Thus F_m divides B_s and G_n divides A_r. But then $r \geq n$ and $s \geq m$, a contradiction. Hence $(\overline{A}, \overline{B}) = (0,0)$.

($\Rightarrow$) Suppose L were a common tangent to F and G, so $F_m = LF'_{m-1}$ and $G_n = LG'_{n-1}$ for some forms F'_{m-1} and G'_{n-1}. Then $\psi(\overline{G'_{n-1}}, -\overline{F'_{m-1}}) = \overline{FG'_{n-1} - F'_{m-1}G}$. The lowest degree terms here cancel, since $F_mG'_{n-1} = F'_{m-1}LG'_{n-1} = F'_{m-1}G_n$. Thus every term has degree at least $m+n$, so $\psi(\overline{G'_{n-1}}, -\overline{F'_{m-1}}) = 0$, and ψ is not one-to-one. □

Example 4.9. Consider the intersection number of $F = X^2$ and $G = Y^2$ at $P = (0,0)$. Since F and G share no tangent lines at the origin, by property (5), $I(P, F \cap G) = m_P(F)m_P(G) = 2 \cdot 2 = 4$. On the other hand, we may compute $I(P, F \cap G)$ as the dimension of $\mathcal{O}_P(\mathbb{A}^2)/(F,G)$. Note that in this space, any polynomial can have terms with degree at most 1 in each X and Y, since $X^2 = 0 = Y^2$. Then $\{1, X, Y, XY\}$ forms a basis for $\mathcal{O}_P(\mathbb{A}^2)/(F,G)$, so $I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F,G)) = 4$, which agrees with our first calculation.

We end this section with one last property of the intersection number, which follows as a corollary.

Corollary 4.10. *If F and G have no common components, then*

$$\sum_P I(P, F \cap G) = \dim_k(k[X,Y]/(F,G)).$$

Proof. Since $\mathbb{V}(F,G)$ is finite, by Corollary 2.7,

$$\dim_k(k[X,Y]/(F,G)) = \sum_P \dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F,G)) = \sum_P I(P, F \cap G). \qquad \square$$

5. Bézout's Theorem

Although everything in the preceding section was done in the context of affine space, we now move to an application of the intersection number which requires that we work in projective space. The key theorem of this section is Bézout's Theorem, which gives a closed form for the total number of intersections of two projective plane curves, counting multiplicity.

There are many treatments of Bézout's Theorem, including generalizations to higher dimensional projective space. A proof of the theorem over $\mathbb{P}^2(\mathbb{C})$ in particular can be found in Chapter 8 of [2]; this proof uses resultants, an important tool in computational algebra, and takes a significantly more hands-on approach than the proof we give.

Theorem 5.1 (Bézout's Theorem)**.** *Let F and G be projective plane curves of degree m and n, respectively. If F and G have no common component, then*

$$\sum_{P \in \mathbb{P}^2} I(P, F \cap G) = mn.$$

Proof. We first show that if $F \cap G$ is infinite, then F and G must have a common component. Note that at least one of the three projective axes will miss infinitely many points in $F \cap G$. Then we can dehomogenize F and G, perhaps by choosing a coordinate other than Z to be 1, such that $F_* \cap G_*$ is infinite. But then by Proposition 2.2, F_* and G_* have a common component H. Rehomogenizing, H^* will be a common component of $(F_*)^*$ and $(G_*)^*$, so H^* is also a common component of F and G. By hypothesis, F and G do not share a common component, thus $F \cap G$ is finite.

Then we may apply a projective change of coordinates so that none of these points lie on the line $Z = 0$, that is, $F \cap G$ is contained in U_3, the copy of the affine plane determined by $Z \neq 0$. Dehomogenizing F and G, we then have

$$\sum_{P \in \mathbb{P}^2} I(P, F \cap G) = \sum_{P \in \mathbb{A}^2} I(P, F_* \cap G_*) = \dim_k(k[X,Y]/(F_*, G_*)),$$

by Corollary 4.10.

Let $\Gamma_* = k[X,Y]/(F_*, G_*)$, $\Gamma = k[X,Y,Z]/(F,G)$, and $R = k[X,Y,Z]$. Let R_d denote the forms of degree d in R, and similarly let Γ_d denote their images in Γ, that is, the forms of degree d in Γ. We will prove that $\dim \Gamma_* = \dim \Gamma_d = mn$ for $d \geq m + n$.

First we show $\dim \Gamma_d = mn$ when $d \geq m+n$. Consider the sequence

$$0 \longrightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\varphi} R \xrightarrow{\pi} \Gamma \longrightarrow 0, \tag{5.2}$$

where $\psi(C) = (GC, -FC)$, $\varphi(A, B) = AF + BG$, and π is the natural quotient map. It is not difficult to see this sequence is exact. Suppose $\psi(C) = (GC, -FC) = 0$. Then $C = 0$, so ψ is injective. Since $\varphi(A, B) = AF + BG$, and F and G have no common component, $(A, B) \in \ker \varphi$ if and only if $AF = -BG$ if and only if $A = GC$ and $B = -FC$ for some $C \in k[X, Y, Z]$. Thus $\mathrm{Im}\psi = \ker \varphi$. Note that $\pi(C) = 0$ if and only if $C = AF + BG$ for some $A, B \in k[X, Y, Z]$, so $\mathrm{Im}\varphi = \ker \pi$. Lastly, since π is a quotient map, it is surjective.

Let $d \geq m+n$ be given. We may restrict the sequence (5.2) by noting that ψ, φ, and π behave nicely on forms. In particular, (5.2) restricts to

$$0 \longrightarrow R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\varphi} R_d \xrightarrow{\pi} \Gamma_d \longrightarrow 0.$$

For a fixed k, R_k is a vector space with basis $\{X^a Y^b Z^c \mid a+b+c = k\}$. This basis has $\sum_{a=0}^{k} \sum_{b=0}^{k-a} 1 = \frac{(k+1)(k+2)}{2}$ elements. By the Corollary 2.11,

$$\begin{aligned}
\dim \Gamma_d &= \dim R_d - \dim(R_{d-m} \times R_{d-n}) + \dim R_{d-m-n}, \\
&= \frac{(d+1)(d+2)}{2} - \frac{(d-m+1)(d-m+2)}{2} \cdot \frac{(d-n+1)(d-n+2)}{2} \\
&\quad + \frac{(d-m-n+1)(d-m-n+2)}{2}, \\
&= mn.
\end{aligned}$$

Next we show that $\dim \Gamma_* = \dim \Gamma_d$ for $d \geq m+n$. Choose $A_1, \ldots, A_{mn} \in R_d$ such that their residues $\overline{A}_1, \ldots, \overline{A}_{mn}$ form a basis for Γ_d. Let A_{i*} denote the dehomogenization of A_i, that is, $A_{i*} = A_i(X, Y, 1)$, and a_i be the residue of A_{i*} in Γ_*. We are finished if we can show $\{a_1, \ldots, a_{mn}\}$ is a basis for Γ_*.

To do so, we first define a map $\alpha \colon \Gamma \to \Gamma$ by $\alpha(\overline{H}) = \overline{ZH}$. This map restricts to one on Γ_d, with $\alpha(\Gamma_d) \subseteq \Gamma_{d+1}$. In fact, this restriction is an isomorphism of vector spaces. As we showed above, $\dim \Gamma_d = \dim \Gamma_{d+1} = mn$, so it remains to see that α is injective.

Suppose $ZH = AF + BG$, so $\alpha(\overline{H}) = \overline{ZH} = 0$. Let J_0 denote $J(X, Y, 0)$ for any $J \in k[X, Y, Z]$. Since we chose $F \cap G$ to have no zeroes on $Z = 0$, F_0 and G_0, both forms in $k[X, Y]$, have no common factors. Since $ZH = AF + BG$, then $0 = A_0 F_0 + B_0 G_0$, so $A_0 F_0 = -B_0 G_0$. By our previous comment, $B_0 = F_0 C$ and $A_0 = -G_0 C$ for some $C \in k[X, Y]$. Let $A_1 = A + CG$ and $B_1 = B - CF$, so $ZH = AF + BG = AF + CGF + BG - CFG = A_1 F + B_1 G$. Moreover, $(A_1)_0 = A_0 + CG_0 = 0$ and $(B_1)_0 = B_0 - CF_0 = 0$, so Z must divide both. Thus we can write $A_1 = A'Z$ and $B_1 = B'Z$ for some $A', B' \in k[X, Y, Z]$. But then $H = A'F + B'G$, so $\overline{H} = 0$, as desired.

Now, since $\alpha \colon \Gamma_d \to \Gamma_{d+1}$ is an isomorphism, by applying it r times to our basis for Γ_d, we can use it to produce a basis for Γ_{d+r} for all $r \geq 0$, namely the residues of $\{Z^r A_1, \ldots, Z^r A_{mn}\}$. We now show that our a_i vectors form a basis for Γ_*.

Let $\overline{H} \in \Gamma_*$, where $H \in k[X,Y]$. We can pick an $N \geq 0$ such that $Z^N H^* \in k[X,Y,Z]$ is a form of degree $d+r$. We can then write $\overline{Z^N H^*}$ in terms of our basis for Γ_{d+r}, so $Z^N H^* = (\sum_{i=1}^{mn} \lambda_i Z^r A_i) + BF + CG$ for some $\lambda_i \in k$ and $B, C \in k[X,Y,Z]$. If we dehomogenize, we see that $H = (Z^N H^*)_* = (\sum_{i=1}^{mn} \lambda_i A_{i*}) + B_* F_* + C_* G_*$. Finally, we can take the residue of H (with respect to (F_*, G_*)) to see $\overline{H} = \sum_{i=1}^{mn} \lambda_i a_i$. Thus the a_i's generate Γ_*.

Now suppose $\sum_{i=1}^{mn} \lambda_i a_i = 0$. Then in $k[X,Y]$, the sum $\sum_{i=1}^{mn} \lambda_i A_{i*} = BF_* + CG_*$ for some $B, C \in k[X,Y]$. We now want to consider the homogenized form of this. Note that since the A_{i*}'s all have the same degree d, homogenizing this sum may be done termwise. For $BF_* + CG_*$, however, it is not as simple, but for appropriate powers of Z, $(BF_* + CG_*)^* = Z^s B^* F + Z^t C^* G$. In particular, one of s and t will be zero. Then

$$\sum_{i=1}^{mn} \lambda_i A_i = \left(\sum_{i=1}^{mn} \lambda_i A_{i*} \right)^* = (BF_* + CG_*)^* = Z^s B^* F + Z^t C^* G.$$

Then the residue of this in Γ_d is zero, so $\overline{\sum_{i=1}^{mn} \lambda_i A_i} = \sum_{i=1}^{mn} \lambda_i \overline{A}_i = 0$. But the $\overline{A}_i$'s were chosen to form a basis for Γ_d, so each λ_i must be zero. Hence the a_i's are independent.

Thus we have shown $\dim \Gamma_* = \dim \Gamma_d = mn$, and we may conclude our desired result, that $\sum_P I(P, F \cap G) = mn$. □

6. Conclusion

Although Bézout's Theorem gives a concise solution to our motivating question for two curves in $\mathbb{P}^2(k)$, the story of intersection number does not end here. This is just the tip of a mathematical iceberg and a rich field of study. From here, two natural next steps would be to consider the intersection of n curves, where $n > 2$, or consider the intersection of curves in higher dimensions. Pursuing either of these paths immediately becomes much more difficult, and requires a significantly more sophistication than used by the approach taken here; [4] is a treatise on the subject.

References

[1] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusetts, 1969.
[2] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, 3rd ed., Undergraduate Texts in Mathematics, Springer, New York, 2007.
[3] W. Fulton, *Algebraic Curves*, http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf, 2008.
[4] W. Fulton, *Intersection Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, vol. 2, Springer, Berlin, 1984.

Department of Mathematics, The University of Chicago, Chicago, Illinois 60637
E-mail address: mnichols@math.uchicago.edu