2020

Curving Towards Bézout: An Examination of Plane Curves and Their Intersection

Camron Alexander Robey Cohen

Oberlin College

CURVING TOWARDS BÉZOUT: AN EXAMINATION OF PLANE CURVES AND THEIR INTERSECTION

OBERLIN COLLEGE

CAMRON COHEN

1. Abstract

One area of interest in studying plane curves is intersection. Namely, given two plane curves, we are interested in understanding how they intersect. In this paper, we will build the machinery necessary to describe this intersection. Our discussion will include developing algebraic tools, describing how two curves intersect at a given point, and accounting for points at infinity by way of projective space. With all these tools, we will prove Bézout's theorem, a robust description of the intersection between two curves relating the degrees of the defining polynomials to the number of points in the intersection.

2. Affine Space

2.1. **Background.** We assume the reader has some background in algebraic geometry. Namely, an understanding of the correspondence between ideals in polynomial rings and varieties is assumed. If I is an ideal and V is a variety, we will use $\mathbf{V}(I)$ to refer to the set of points on which all $f \in I$ vanish and $\mathbf{I}(V)$ to refer to the ideal of polynomials that vanish on all $p \in V$.

We also assume some familiarity with quotient rings and local rings. Note, throughout the paper, we will use k to refer to an algebraically closed field. Given a variety $V \subseteq k^n$, we will use the following notation

$$\Gamma(V) := k[x_1, \ldots, x_n]/\mathbf{I}(V)$$
$$\mathcal{O}_P(V) := \left\{ \frac{F}{G} \mid F, G \in \Gamma(V), G(P) \neq 0 \right\},$$

where $P \in k^n$. We will usually, however, be working in either $\mathbb{A}^2$, affine 2-space over k, or $\mathbb{P}^2$, projective 2-space over k. Furthermore, if $F \in R$, where R is a ring, I is an ideal in R, and $S := R/I$, we will use the notation $\overline{F}^I$ or $\overline{F}^S$ to denote the residue of $F \in S$. It will be clear in context which notation we are using. Sometimes, given $H \in k[x_1, \ldots, x_n]$, we will write $\mathcal{O}_P(H)$. In this case, we mean $\mathcal{O}_P(\mathbf{V}(H))$, but shorten it for simplicity.

Additionally, we note there is a natural relationship between polynomials in $k[x, y]$ and curves in $\mathbb{A}^2$. Namely, if $F \in k[x, y]$ and F is not the zero polynomial, the points where F vanishes define a curve in $\mathbb{A}^2$. We will refer to the curve defined by $F = 0$ as F_C. Thus, if we give a curve, F_C, we will refer to the defining polynomial as F. We address this explicitly for ease of reference when giving explicit definitions for F.

Finally, if $F \in k[x_1, \ldots, x_n]$, we will refer to F as a form if the degree of each term of F is the same, i.e., F is a homogeneous polynomial. Furthermore, if F is a form, we define F_* as the dehomogenization of F. Note, if $F \in k[x_1, \ldots, x_n]$, then $F_* \in k[x_1, \ldots, x_{n-1}]$. As an explicit example, if $F \in k[x, y, z]$, we may say $F_* = F(x, y, 1)$. As we will see later, however, we may dehomogenize with respect to any variable. In fact, we may dehomogenize with respect to any projective line without affecting our definitions of intersection number in projective space. Thus, in many cases, we will not be explicit with which projective line we are using to dehomogenize F, and simply refer to the dehomogenization, F_*. Conversely, if we have an affine curve F_C, we use F^* to refer to the homogenization of F. Namely, if $F = F_m + \dots F_l$, where F_i are forms, $F^* = z^{l-m}F_m + \dots + z^0 F_l$. Note, if $F \in k[x_1, \dots, x_n]$, $F^* \in k[x_1, \dots, x_{n+1}]$.

2.2. **Algebra.** Before we begin our discussion of curves, we first prove a few important theorems we will use in our discussion. First, we examine a useful algebraic result. Here, we present a proof outlined in [2, p. 148] with additional details. Note, we will refer to the local ring $\mathcal{O}_P(\mathbb{A}^2)$ as $\mathcal{O}_P$ for ease of notation.

Theorem 2.1. *If I is a zero-dimensional ideal in $k[x_1, \dots, x_n]$, then if $V := \mathbf{V}(I) = \{P_1, \dots, P_m\}$, there is an isomorphism between $k[x_1, \dots, x_n]/I$ and the direct product of the rings $A_i := \mathcal{O}_{P_i}/I\mathcal{O}_{P_i}$.*

Lemma 2.2. *Let I and V be as in the theorem. Then, if $M_i := \mathbf{I}(\{P_i\})$, for all $P_i \in V$, we have the following*

- (a) *There exists $d \geqslant 1$ such that $(\bigcap_{i=1}^m M_i)^d \subseteq I$*
- (b) *There are polynomials $E_i \in k[x_1, \dots, x_n]$ for each i such that*
    - (i) $-1 + \sum_{i=1}^m E_i \in I$
    - (ii) $E_i E_j \in I$ *when* $i \neq j$
    - (iii) $E_i^2 - E_i \in I$
    - (iv) $E_i \in I\mathcal{O}_{P_j}$ *when* $i \neq j$
    - (v) $E_i - 1 \in I\mathcal{O}_{P_i}$ *for each* i
- (c) *If $G \in k[x_1, \dots, x_n] \backslash M_i$, then there exists $H \in k[x_1, \dots, x_n]$ such that $GH - E_i \in I$*

Proof. First, we note (a) can be found as a simple application of the Nullstellensatz. Namely, $\mathbf{I}(V) = \mathbf{I}(\{P_1\}) \cap \dots \cap \mathbf{I}(\{P_m\}) = \bigcap_{i=1}^m M_i$. But we also know $\mathbf{I}(V) = \sqrt{I}$, by the strong Nullstellensatz [3, p. 179], so our result follows since I is finitely generated.

For (b) we must put in a bit more work. We begin by noting, by Lemma 2.9 in [2, p. 43], for each index i, there exists a $G_i \in k[x_1, \dots, x_n]$ such that

$$G_i(P_j) = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}.$$

Now, we propose a definition for E_i, and we will show all of $(i) - (v)$ are satisfied. Let

$$E_i := 1 - (1 - G_i^d)^d \text{ for all } i \tag{1}$$

where d is as in (a). To prove (i), we will show $-1 + \sum_{i=1}^m E_i \in \bigcap_{i=1}^m M_i^d$. But since all the M_i are distinct maximal ideals, we know that the set of all M_i

is pairwise comaximal. Thus, by Proposition 5.2 (see Appendix), we conclude $\bigcap_{i=1}^m M_i^d = (\bigcap_{i=1}^m M_i)^d$.

Therefore, we need only show $-1 + \sum_{i=1}^m E_i \in \bigcap_{i=1}^m M_i^d$. To accomplish this task, we will demonstrate $E_i \in M_j^d, i \neq j$, and $E_i - 1 \in M_i^d$, for all i. First we argue the former case.

Note that $G_i \in M_j$ when $i \neq j$, since M_j is a maximal ideal for P_j and $G_i(P_j) = 0$. But if we expand the right side of equation (1), we find

$$E_i = -\binom{d}{1}G_i^d + \cdots \pm \binom{d}{d}G_i^{d^2}$$

where the $\pm$ is determined by whether d is odd or even. Then G_i^d divides E_i, and since $G_i \in M_j$, we conclude $E_i \in M_j^d$ when $i \neq j$.

To see M_i^d contains $E_i - 1$, we first observe $1 - G_i^d$ vanishes at P_i by our definition of G_i. Consequently, M_i contains $1 - G_i^d$, and $(1 - G_i^d)^d \in M_i^d$. Since $E_i - 1 = (1 - G_i^d)^d$, we are done.

As noted earlier, to show $E_i - 1 \in M_i$ for all i, begin with the observation that $G_i - 1 \in M_i$ by the same logic as before, and repeat the above argument.

Notice that we have shown $E_i \in M_j^d$ when $i \neq j$ and $E_i - 1 \in M_i^d$ for any choice of i. Then, for any i, $-1 + \sum_{i=1}^m E_i = -1 + E_i + \sum_{j \neq i} E_j \in M_i^d$, so $-1 + \sum_{i=1}^m E_i \in \bigcap M_i^d$. Thus, by our earlier observation, $-1 + \sum_{i=1}^m E_i \in (\bigcap M_i)^d$. But by (a), $(\bigcap M_i)^d \subseteq I$, so we have established (i).

Directing our attention to (ii), we can see this follows quickly from our earlier argument. Namely, since for any choice of $i \neq k$, $E_i \in M_k^d$. But we are examining $E_iE_j, i \neq j$, so $E_j \in M_i^d$. The result follows.

Property (iii) will follow from our earlier proof that $-1 + \sum_{j=1}^m E_j \in (\bigcap M_i)^d$. Letting i be fixed and multiplying by E_i, we get a term still in I, namely

$$-E_i + E_i \sum_{j=1}^m E_j = E_i^2 - E_i + \sum_{j \neq i} E_j E_i.$$

But (ii) tells us $\sum_{j \neq i} E_j E_i$ is in I, so it must be the case that $E_i^2 - E_i$ is in I as well.

To finish (b), we must show properties (iv) and (v). In both cases, we will leverage (iii) and the definition of our local ring. Notice, $E_i^2 - E_i = E_i(E_i - 1) \in I\mathcal{O}_{P_j}$. Then, if $(E_i - 1)^{-1}$ were in $\mathcal{O}_{P_j}$, we would have established (iv). But by our definition of E_i in (1), $E_i(P_j) = 0, i \neq j$. Thus, $E_i - 1$ does not vanish at P_j, so its inverse exists in $\mathcal{O}_{P_j}$, as desired. Similarly, if E_i^{-1} were in $\mathcal{O}_{P_i}$, (v) would be established. The argument here mirrors that of (iv), but we note $E_i(P_i) = 1$ instead.

Finally, we will show (c). First, fix i and let $G \in k[x_1, \dots, x_n] \backslash M_i$. Without loss of generality, let $G(P_i) = 1$. If $G(P_i) = c \in k$, we may simply scale G by $\frac{1}{c}$, since these polynomials have identical zeros. Then, notice that since M_i is a maximal ideal, and $1 - G$ vanishes on P_i, $1 - G \in M_i$. Now, we propose $H := (1 + (1 - G) + \cdots + (1 - G)^{d-1})E_i$. But then,

$$GH = (1 - (1 - G))H = (1 - (1 - G)^d)E_i = E_i - (1 - G)^d E_i \tag{2}$$

Recall that $E_i \in M_j^d, i \neq j$, and $1-G \in M_i$ by our earlier observation. Therefore, $(1-G)^d E_i \in (\bigcap M_i)^d \subseteq I$. Consequently, by equation (2), $GH - E_i = -(1-G)^d E_i$ is in I, as desired.

□

Proof of Theorem. We will show that the map

$$\phi : k[x_1, \dots, x_n] \to A_1 \times \cdots \times A_m,$$
$$\phi(F) = (\overline{F}^{A_1}, \dots, \overline{F}^{A_m})$$

has kernel equal to I and is surjective. This will complete our proof by the fundamental theorem of ring homomorphisms.

To begin, notice ϕ is defined componentwise by the natural homomorphisms from the polynomial ring $k[x_1, \dots, x_n]$ to our local rings A_i. Thus, it is clear that if $F \in I$, then $\overline{F}^{A_i} = \overline{0}^{A_i}$ for any i. Hence, it suffices to show $\ker(\phi) \subseteq I$.

Let $F \in \ker(\phi)$. First note we may apply $(b)(i)$ to conclude

$$F \sum_{i=1}^{m} (E_i) - F \in I. \tag{3}$$

Second, if $F \in \ker(\phi)$, then $F \in I\mathcal{O}_{P_i}$ for all i. Hence, $F = F' \frac{F_i}{G_i}$, where $F' \in I, \frac{F_i}{G_i} \in \mathcal{O}_{P_i}$. We can rearrange this equation to get $FG_i = F'F_i \in I$, since $F' \in I$. Notice that $G_i \notin M_i$, since $G_i(P_i) \neq 0$ by definition of A_i, so we can invoke (c) from our lemma to find H_i for each G_i such that $G_i H_i - E_i \in I$. Observe that

$$F \sum_{i=1}^{m} H_i G_i = \sum_{i=1}^{m} H_i (FG_i) \in I, \tag{4}$$

since each of the terms in our sum contains $FG_i \in I$ for all i. Finally, we subtract equation (3) from equation (4) to get

$$F \sum_{i=1}^{m} (H_i G_i - E_i) + F \in I$$

But if this is the case, F must be in I, since $H_i G_i - E_i \in I$ by (c) of Lemma 2.2. We conclude $I = \ker(\phi)$.

By the fundamental theorem of ring homomorphisms, our proof will be complete once we see that ϕ is surjective. That being the case, let $(\frac{N_1}{D_1}, \ldots, \frac{N_m}{D_m}) \in A_1 \times \cdots \times A_m$. Again, by (c) of our lemma, for each D_i there exists H_i such that $H_iD_i - E_i \in I$. Now, let $F := \sum_{i=1}^{m} H_iN_iE_i$ and notice $\overline{F}_i^A = H_iN_iE_i$, since $E_j \in I\mathcal{O}_{P_i}, j \neq i$ by $(b)(iv)$ of Lemma 2.2. Thus, we need only show $H_iN_iE_i - \frac{N_i}{D_i} \in I\mathcal{O}_{P_i}$. First, we simplify

$$H_iN_iE_i - \frac{N_i}{D_i} = \frac{N_i}{D_i}(D_iH_iE_i - 1)$$

and note

$$D_iH_iE_i - 1 - (E_i^2 - 1) = E_i(D_iH_i - E_i).$$

Since $D_iH_i - E_i \in I$ by part (c) of Lemma 2.2, $D_iH_iE_i - 1 \in I\mathcal{O}_{P_i}$ if $E_i^2 - 1 \in I\mathcal{O}_{P_i}$. Furthermore,

$$E_i^2 - 1 - (E_i - 1) = E_i^2 - E_i \in I \text{ by } (b)(iii) \text{ of Lemma 2.2},$$

so $E_i^2 - 1 \in I\mathcal{O}_i$ if $E_i - 1 \in I\mathcal{O}_i$. But, $E_i - 1 \in I\mathcal{O}_i$ by $(b)(v)$ of our lemma, so we may conclude $\overline{F}_i^A = \frac{N_i}{D_i}$, as desired. As noted earlier, this completes our proof. $\square$

2.3. **Exact Sequences.** Exact sequences will be useful in both establishing validity of our subsequent definition of intersection number and proving Bézout's theorem, so we introduce them here. Let M, M', M'' be R-modules for some ring R. Then we define

$$M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$$

as a sequence when ϕ and ψ are R-module homomorphisms, and we say the sequence is exact when $\operatorname{im}\phi = \ker\psi$. This latter feature can be generalized to arbitrarily long sequences

$$M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_m} M_{m+1}$$

by defining exactness to be when $\operatorname{im}\phi_i = \ker\phi_{i+1}$ for $1 \leqslant i \leqslant m$. Much of our work will involve considering the dimension of local rings, so the following application of the rank-nullity theorem will be useful. The proof may be found in [1, Section 2.10], but additional details are given here.

Proposition 2.1. *(1) Let* $0 \to V' \xrightarrow{\phi} V \xrightarrow{\psi} V'' \to 0$ *be an exact sequence of finite-dimensional vector spaces. Then* $\dim V' + \dim V'' = \dim V$.

(2) Let $0 \to V_1 \xrightarrow{\phi_1} V_2 \xrightarrow{\phi_2} V_3 \xrightarrow{\phi_3} V_4 \to 0$ *be an exact sequence of finite-dimensional vector spaces. Then* $\dim V_4 = \dim V_3 - \dim V_2 + \dim V_1$.

Proof. (1) First, notice $0 \to V' \xrightarrow{\phi} V$ is exact if and only if ϕ is injective. Similarly, $V \xrightarrow{\psi} V'' \to 0$ is exact if and only if ψ is surjective. Then, consider the linear map $\psi : V \to V''$. By the rank-nullity theorem, $\dim V = \dim\operatorname{im}\psi + \dim\ker\psi$. But, since ψ is onto, ϕ is one-to-one, and $\operatorname{im}\phi = \ker\psi$, our result follows.

(2) First, define $W = \operatorname{im} \phi_2 = \ker \phi_3$. Then, consider the sequences

$$0 \to V_1 \xrightarrow{\phi_1} V_2 \xrightarrow{\phi_2} W \to 0$$

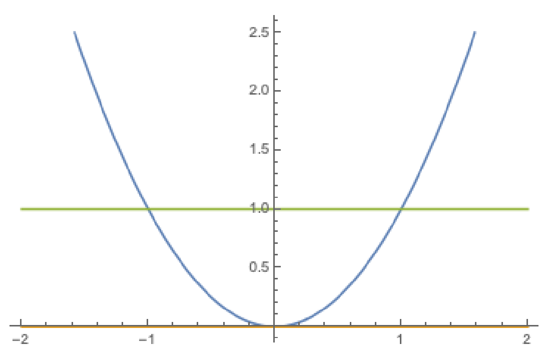
$$0 \to W \xrightarrow{\psi} V_3 \xrightarrow{\phi_3} V_4 \to 0$$

where $\psi(w) = w$. Then, applying (1) to both the above sequences and subtracting the results will give the desired relation.

□

2.4. **Plane Curves.** As we noted in our abstract, given two plane curves defined by the vanishing of polynomials F and G in $k[x, y]$, we are interested in describing their intersection more completely than simply computing how many times the curves intersect. This question is only interesting if F and G do not share any common components. Otherwise, F_C and G_C intersect an infinite number of times. An upper bound of $\deg(F)\deg(G)$ can be found using resultants [3, Section 8.7], but will not be proven here.

With this upper bound in place, a question naturally arises: why does equality not always hold? Answering this question will be the main focus of this paper, but first, we give a motivating example. Consider the curves F_C, G_C, and H_C described by $0 = F = x^2 - y$, $0 = G = y$, and $0 = H = y - 1$. These curves are graphed below.



Notice, F_C and H_C intersect at 2 points, and $\deg(F) = 2, \deg(H) = 1$. In this case, equality holds. By comparison, F_C and G_C intersect at exactly one point, but $\deg(F)\deg(G) = 2$. This disparity can be understood by examining how G_C and H_C intersect F_C. In the case of the latter, H_C is not tangent to F_C at either point. By comparison, G_C is tangent to F_C at the point of intersection. Then, we may be able to understand why the number of points of intersection between, in this case, F_C and G_C is less than $\deg(F)\deg(G)$ by accounting for tangency in some way.

This is not, however, the only case in which we find fewer points of intersection than $\deg(F)\deg(G)$ for curves F_C and G_C. Consider the curves defined by $x^2 - y^2 = 0$ and $y = 0$. By graphing these curves, the reader will find the point of intersection, $(0, 0)$, is a singular point on our curved defined by $x^2 - y^2 = 0$. Thus, we would also like account for singularities in our consideration for why the number of points of intersection of two curves F_C and G_C is less than $\deg(F)\deg(G)$.

With these motivations, we move on to our discussion of intersection numbers, which will provide this method of counting we desire.

2.5. **Intersection Numbers.** We have noted that, given two plane curves F_C and G_C, F_C and G_C intersect in at most $\deg(F)\deg(G)$ points. Our main theorem, Bézout's theorem, characterizes when equality holds in this inequality. First, we will develop some machinery necessary to quantify how curves intersect. Namely, we will discuss the intersection number of two curves, F_C and G_C at a point P in their intersection, denoted $I(P, F \cap G)$. We will first propose some properties we would like the intersection number to satisfy, prove these properties determine a unique number, and then give a definition for this quantity.

Before we begin listing our desired properties, we first give some relevant definitions. We say two curves *intersect properly* at a point if they share no common components through that point. Similarly, we say two curves *intersect transversely* at a point if they share no common tangents at that point. Finally, we define the multiplicity of a curve, F_C, at $P = (0, 0)$, denoted $m_P(F)$ to be the degree of the lowest degree form in F. It will be useful throughout to note the tangents to F_C at the origin are given by the zeros of the lowest degree form in F [1, p. 33]. This observation may seem strange, but note as you approach the origin on F_C, the lowest degree form approaches 0 the slowest out of all forms in F. Thus, the smallest degree form affects the shape of F_C the most when close to the origin. With these definitions, we continue with our defining properties.

Defining Properties:

(1) $I(P, F \cap G) \in \mathbb{Z}_{\geqslant 0}$ when F_C and G_C intersect properly at P. Otherwise $I(P, F \cap G) = \infty$.
(2) $I(P, F \cap G) = 0$ if and only if $P \notin F_C \cap G_C$ and $I(P, F \cap G)$ depends only on the components of F and G which vanish at P.
(3) $I(P, F \cap G)$ is unchanged when applying an affine change in coordinates to F and G
(4) $I(P, F \cap G) = I(P, G \cap F)$. That is, the intersection number is a property of the two curves intersecting, not the order of their intersection.
(5) $I(P, F \cap G) \geqslant m_P(F)m_P(G)$ with equality holding exactly when F_C and G_C intersect transversely at P.
(6) The intersection number sums over unions of curves. Namely, if $F = \Pi F_i^{r_i}, G = \Pi G_j^{s_j}$, then $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$.

(7) Adding factors of F to G should not affect $I(P, F \cap G)$. Namely, $I(P, F \cap G) = I(P, F \cap (G + AF)), A \in k[x, y]$.

The following theorem has been adapted from [1, Section 3.3].

Theorem 2.3. *The unique intersection number for any two plane curves F_C, G_C at a point P is given by*

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

Proof of Uniqueness. First, we prove the properties given above determine a unique intersection number for any two plane curves F_C, G_C and point P in their intersection. Let $I(P, F \cap G)$ satisfy properties (1) – (7). Then, we may assume $I(P, F \cap G)$ is finite and P is the origin by properties (1) and (3). Furthermore, since $I(P, F \cap G) = 0$ is described in (2), we may use induction on $I(P, F \cap G)$. Thus, assume $I(P, F \cap G)$ is determined uniquely when $I(P, F \cap G) < n \in \mathbb{N}$. We will show that then $I(P, F \cap G)$ can be computed when $I(P, F \cap G) = n$. Consider the polynomials $F(x, 0), G(x, 0) \in k[x]$ of degrees r, s, respectively. We will consider $r, s = 0$ if $F(x, 0), G(x, 0)$ are the zero polynomial in $k[x]$, respectively. Furthermore, by (4), we may swap F and G if necessary, so that $r \leqslant s$. Now, we divide our proof into two cases. For our first case, we will argue that if $r = 0$, then the intersection number is uniquely determined. In the second case (when $r > 0$), we will reduce our analysis to the first case using property (7) of the intersection number.

Case 1: In the case of $r = 0$, our key observation is that F is divisible by y. That is, $F = yH$, for some $H \in k[x, y], \deg(H) < n$. Then, by property (6) of our intersection number,

$$I(P, F \cap G) = I(P, y \cap G) + I(P, H \cap G). \tag{5}$$

It is unclear how to proceed with the second term in this sum, so we will examine the first term. Namely, we will show this intersection number is positive. In turn, we will have shown that $I(P, H \cap G) < n$, making it uniquely determined by our inductive hypothesis.

We begin by noting $G \neq yL$ for any $L \in k[x, y]$. Otherwise, F_C and G_C would share a component passing through the origin, but the case of an infinite intersection number is already handled by (1). Then, we note $G(x, 0) = x^m(a_0 + a_1x + \cdots + a_lx^l)$, where $a_0 \neq 0$, for some $m \in \mathbb{N}$. Now, we apply property (6) again to split our intersection number into the sum

$$I(P, y \cap G) = I(P, y \cap x^m) + I(P, y \cap (a_0 + a_1x + \cdots + a_lx^l))$$

The second term in our sum, however, is 0 since P is the origin, and $a_0 \neq 0$, and $a_0 + a_1x + \cdots + a_lx^l$ does not vanish at the origin. Therefore, we need only examine $I(P, y \cap x^m)$. But, these two curves share no tangents at the origin, so applying property (5), we find $I(P, y \cap x^m) = 1m = m$. Then, if $m > 0$, we know $I(P, F \cap H) < n$ by equation (5). Thus, $I(P, F \cap G)$ is unique by our earlier argument.

Thus, we need to show $m > 0$. Recall that F_C and G_C both pass through the origin, by assumption, and that $G \neq yL$ for any $L \in k[x, y]$. Then, if G_C passes through the origin, it must be the case that $G = x^l L$ for some $l > 0, L \in k[x, y]$. Thus, we have our desired result that $m > 0$.

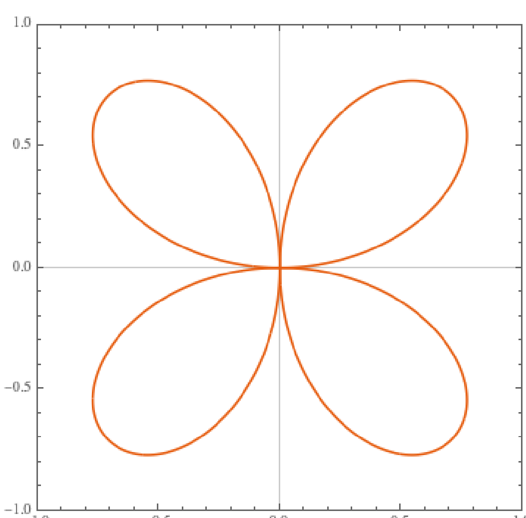
Case 2: For $r > 0$, we would like to reduce to the case of $r = 0$. To accomplish this, we will propose an algorithm that uses property (7) of our intersection number to eliminate terms not in $\langle y \rangle$ from our polynomials until one is in $\langle y \rangle$. This process is rather straightforward.

First, take $F(x, 0), G(x, 0)$ to be monic (we may multiply by constants otherwise). Next, let $H := G - x^{s-r}F$. Notice, $t := \deg(H) < s$ since the leading terms $G(x, 0)$ and $x^{s-r}F(x, 0)$ cancel. Furthermore, by (7), $I(P, F \cap G) = I(P, F \cap H)$. Since this relation between t and s is strict, we may continue until $t = 0$ or $t < r$. In the latter case, we simply switch the roles of F and G and proceed.

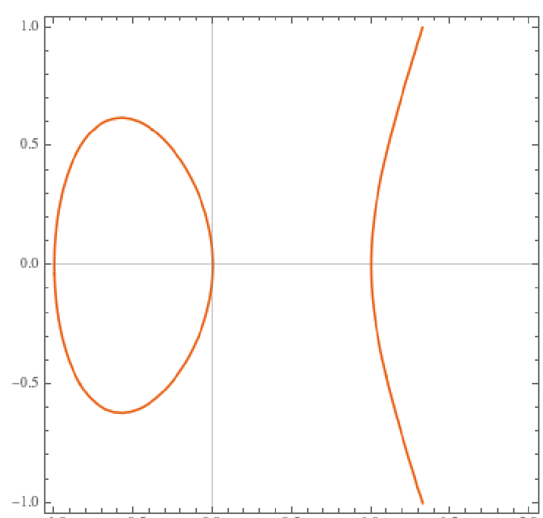
□

Notice, this proof also suggests a method for computing the intersection number. Namely, eliminate leading terms in $F(x, 0)$ and $G(x, 0)$ until one is in $\langle y \rangle$. Then, examine the multiplicity of the other polynomial, substituting $y = 0$. Consider the following example, where our point of intersection P is the origin.

Example:



$A := (x^2 + y^2)^3 - 4x^2y^2$



$B := y^2 - x^3 + x$

First, we expand A to get

$$A = x^6 + 3x^4y^2 + x^2y^4 + y^6 - 4x^2y^2$$

Notice that $\deg(A(x,0)) > \deg(B(x,0))$, so we follow the described procedure in case 2, letting $G = A, F = B$. Thus, we define

$$A_1 := A + x^3B = x^4 + x^3y^2 + 3x^4y^2 + 3x^2y^4 + y^6 - 4x^2y^2.$$

Again, $\deg(A_1(x,0) > \deg(B(x,0))$, so we continue letting

$$A_2 := A_1 + xB = xy^2 + x^2 + x^3y^2 + 3x^4y^2 + 3x^2y^4 + y^6 - 4x^2y^2.$$

Now, $\deg(B(x,0)) > \deg(A_2(x,0))$, so we take

$$B_1 := B + xA_2 = y^2 + x^2y^2 + x^4y^2 + 3x^5y^2 + 3x^3y^4 + y^6x - 4x^3y^2 + x.$$

Finally,

$$A_3 := A_2 - xB_1 = y^2(-x^5 - 3x^6 - 3x^4y^2 - x^2y^4 - x^4 + 3x^2y^2 + y^4 - 4x^2).$$

By our earlier argument, $I(P, A \cap B) = I(P, A_3 \cap B_1) = I(P, y^2 \cap B_1) + I(P, A_4 \cap B_1)$, where $A_4 := -x^5 - 3x^6 - 3x^4y^2 - x^2y^4 - x^4 + 3x^2y^2 + y^4 - 4x^2$.

Notice that the y^2 and B_1 share no tangents at the origin, since the tangents at $(0,0)$ for B_1 are determined by x, the lowest degree form in B_1. Thus, $I(P, y^2 \cap B_1) = m_P(y^2)m_P(B_1) = 2$. It remains to find $I(P, A_4 \cap B_1)$. Observe that A_4 and B_1 share tangents at the origin, so we must reduce these curves further. Thus,

$$\begin{aligned} A_5 :=& A_4 + 4xB_1 = 4xy^2 + 4x^5y^2 + 12x^6y^2 + 12x^4y^4 + 4x^2y^6 - \\ & 16x^4y^2 - x^5 - 3x^6 - 3x^4y^2 - x^2y^4 - x^4 + 3x^2y^2 + y^4. \end{aligned}$$

Now the tangents for A_5 are determined by $-x^4 + 3x^2y^2 + y^4$, so $x = 0$ is no longer a tangent to A_5. Since $x = 0$ is the only possible tangent to B_1, we now have two polynomials, A_5 and B_1, that share no tangents at P. Thus, $I(P, A_4 \cap B_1) = I(P, A_5 \cap B_1) = m_P(A_5)m_P(B_1) = 4$. Thus, $I(P, A \cap B) = 2 + 4 = 6$.

Now, we continue proving our proposed definition for the intersection number is correct by demonstrating the definition satisfies properties $(1) - (7)$.

Proof of Correctness. Now, before we begin the proof of correctness, we note for ease of notation, when we write $\mathcal{O}_P$ we are referring to $\mathcal{O}_P(\mathbb{A}^2)$. First, we note property (4) is obvious since $\langle F, G \rangle = \langle G, F \rangle$.

(7) Almost just as easily, $G + AF \in \langle F, G \rangle$ for all $A \in k[x,y]$, and $G = G + AF - AF \in \langle F, F + AF \rangle$. Hence, property (7) holds.

(3) For (3), we show an affine change in coordinates T yields an isomorphism of local rings at P and $T(P)$. Thus, let $T = (T_1(x_1, \ldots, T_n), \ldots, T_n(x_1, \ldots, x_n))$ be a affine change of coordinates and define $\tilde{T} : \mathcal{O}_{T(P)} \to \mathcal{O}_P$ as

$$\tilde{T}\left(\frac{F}{G}\right) = \frac{F(T_1(x_1, \ldots, x_n), \ldots, T_n(x_1, \ldots, x_n))}{G(T_1(x_1, \ldots, x_n), \ldots, T_n(x_1, \ldots, x_n))}.$$

For injectivity of $\tilde{T}$, notice, if

$$\frac{F_1(T_1(x_1, \ldots, x_n), \ldots, T_n(x_1, \ldots, x_n))}{F_2(T_1(x_1, \ldots, x_n), \ldots, T_n(x_1, \ldots, x_n))} = \frac{G_1(T_1(x_1, \ldots, x_n), \ldots, T_n(x_1, \ldots, x_n))}{G_2(T_1(x_1, \ldots, x_n), \ldots, T_n(x_1, \ldots, x_n))},$$

by substituting y_i for T_i, the property is clear. Furthermore, surjectivity follows from the fact that T has an inverse, since it is an affine change in coordinates. Finally, addition and multiplication are preserved by the definition of evaluating sums and products of polynomials. Namely, $\tilde{T}(F+G) = (F+G)(T_1, \ldots, T_n) = F(T_1, \ldots, T_n)+G(T_1, \ldots, T_n)$. Likewise for multiplication. Thus, (3) is satisfied.

(2) First, we prove $I(P, F \cap G) = 0$ if and only if $P \notin F_C \cap G_C$.
- $\Leftarrow$ If $P \notin F_C \cap G_C$, at least one of F or G does not vanish at P. Without loss of generality, let this be the case for F. Then, F is a unit in $\mathcal{O}_P$, so $1 \in \langle F, G\rangle\mathcal{O}_P$. Thus, $\dim_k(\mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P) = 0$.
- $\Rightarrow$ On the other hand, if $P \in F_C \cap G_C$, both F and G vanish at P. Then, both F and G are in the maximal ideal for the local ring $\mathcal{O}_P$ since neither is unit. Then, consider the evaluation map $E_P : \mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P \to k$, where we evaluate each element in the quotient ring at P. This map is a surjective and a homomorphism. The former is obvious since each element of k is in our quotient ring, and the latter can be observed by applying the definitions of evaluating polynomials. Thus, $\dim_k(\mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P) \geqslant \dim_k(k) = 1$, as desired.

Moving onto the second part of (2), note for any $H \in \mathcal{O}_P$ with $P \notin H_C$, H is a unit in $\mathcal{O}_P$. Thus, for any component H of F which does not pass through P, we observe

$$\langle F, G\rangle\mathcal{O}_P = \langle F\frac{1}{H}, G\rangle\mathcal{O}_P.$$

Then $\mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P$ and $\mathcal{O}_P/\langle F\frac{1}{H}, G\rangle\mathcal{O}_P$ are equivalent, and the result follows.

(1) First, we show $I(P, F \cap G) \geqslant 0$ when F_C and G_C intersect properly. Let F_C and G_C intersect at P with no shared component. Then, by Theorem 2.1, if $\langle F, G\rangle$ is a 0-dimensional ideal, $\dim_k(\mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P) \leqslant \dim_k(k[x, y]/\langle F, G\rangle)$, which is finite and non-negative. But, $\langle F, G\rangle$ is a 0-dimensional ideal if $\mathbf{V}(F, G)$ is finite. Furthermore, $\mathbf{V}(F, G) = \{p \in$

$\mathbb{A}^2|F(p) = 0 = G(p)\}$ and $F = 0 = G$ is a system of two equations in two variables. Consequently, since F and G share no common component, the points $p \in \mathbb{A}^2$ satisfying this system must be finite, meaning $\langle F, G\rangle$ is 0-dimensional.

Now, we show that $I(P, F \cap G)$ is infinite if F_C and G_C do not intersect properly at P. Since F_C and G_C do not intersect properly, their defining polynomials must share a common component, H. Furthermore, $\langle F, G\rangle \subseteq \langle H\rangle$. We now make the following observations

(*a*) There is a natural homomorphism $\mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P \to \mathcal{O}_P/\langle H\rangle\mathcal{O}_P$.

(*b*) $\mathcal{O}_P/\langle H\rangle\mathcal{O}_P \cong \mathcal{O}_P(H)$ by letting $J = \langle H\rangle$ in Proposition 5.1 (see Appendix).

(*c*) $\mathbf{V}(H)$ defines a plane curve, so $\dim_k(\Gamma(H))$ is infinite by Corollary 4 to Hilbert's Nullstelensatz [1, p. 11].

(*d*) $\Gamma(H) \subseteq \mathcal{O}_P(H)$

Putting these four observations together, we have

$$\dim_k(\mathcal{O}_P/\langle F, G\rangle) \geqslant \dim_k(\mathcal{O}_P/\langle H\rangle\mathcal{O}_P) = \dim_k(\mathcal{O}_P(H)) \geqslant \dim_k(\Gamma(H)) = \infty,$$

which completes our proof of (1).

(6) We will show $I(P, F \cap GH) = I(P, F \cap G) + I(P, G \cap H)$ as the case with more components follows by induction. Furthermore, we assume F_C and $G_C H_C$, defined by the points at which either G or H vanish, intersect properly. Otherwise, $I(P, F \cap GH) = \infty$ and at least one of $I(P, F \cap G)$ or $I(P, F \cap H)$ is ∞ as well.

Begin by letting $\phi : \mathcal{O}_P/\langle F, GH\rangle\mathcal{O}_P \to \mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P$ be the natural homomorphism and $\psi : \mathcal{O}_P/\langle F, H\rangle\mathcal{O}_P \to \langle F, GH\rangle\mathcal{O}_P$ be defined as $\psi(\overline{L}^{\langle F,H\rangle}) = \overline{GL}^{\langle F,GH\rangle}, L \in \mathcal{O}_P$. Consider the following sequence

$$0 \to \mathcal{O}_P/\langle F, H\rangle\mathcal{O}_P \xrightarrow{\psi} \mathcal{O}_P/\langle F, GH\rangle\mathcal{O}_P \xrightarrow{\phi} \mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P \to 0$$

and note, Proposition 2.1 guarantees

$$\dim_k(\mathcal{O}_P/\langle F, GH\rangle\mathcal{O}_P = \dim_k \mathcal{O}_P/\langle F, H\rangle\mathcal{O}_P + \dim_k \mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P,$$

if the above sequence is exact. Furthermore, we have an exact sequence if ϕ is surjective, ψ is injective, and $\ker\phi = \operatorname{im}\psi$. The last condition is immediate, from the definitions of ϕ and ψ. Additionally, the first condition is obvious, since $\langle F, GH\rangle \subseteq \langle F, G\rangle$. It remains to examine the injectivity of ψ.

Since ψ is a ring homomorphism, we will show $\ker(\psi) = \overline{0}^{\langle F,H\rangle}$, which will complete the claim. Let $\overline{L}^{\langle F,H\rangle} \in \ker(\psi)$. Then, $GL \in \langle F, GH\rangle$, so $GL = UF + VGH$ for $U, V \in \mathcal{O}_P$. Consequently, $G(L - VH) = UF$, so F divides $L - VH$, since F and G have no common factors by assumption. Then, $DF = L - VH$ for some $D \in \mathcal{O}_P$, so $L = DF + VH$. Since

$L \in \langle F, H\rangle$, $\overline{L}^{\langle F,H\rangle} = \overline{0}^{\langle F,H\rangle}$, as desired.

(5) For ease of notation, let $m := m_P(F), n := m_P(G), I := \langle x, y\rangle k[x, y]$. For our proof, we will make use of the following sequence

$$k[x,y]/I^n \times k[x,y]/I^m \xrightarrow{\psi} k[x,y]/I^{m+n} \xrightarrow{\phi} k[x,y]/\langle \text{gen}(I^{m+n}), F, G\rangle \to 0,$$

where $\text{gen}(I^{m+n})$ denotes the generators for I^{m+n}, ϕ is the natural ring homomorphism, and $\psi(\overline{A}^{I^n}, \overline{B}^{I^m}) = \overline{AF + BG}^{I^{m+n}}$. We will first obtain the inequality $I(P, F \cap G) \geqslant mn$

Notice that $\text{im}(\psi) = \ker(\phi)$ by our definition of ψ. Furthermore, it is clear ψ preserves addition and scalar multiplication. Combining these two observations with the rank-nullity theorem, we have

$$\dim(k[x,y]/I^n) + \dim(k[x,y]/I^m) \geqslant \dim(\text{im}(\psi)) = \dim(\ker(\phi)). \tag{6}$$

We also note ϕ is surjective, since $\langle \text{gen}(I^{m+n}), F, G\rangle \subseteq I^{m+n}$. Thus,

$$\dim(k[x,y]/\langle \text{gen}(I^{m+n}), F, G\rangle) = \dim(k[x,y]/I^{m+n}) - \dim(\ker(\phi)). \tag{7}$$

Now, the following string of inequalities will give us our desired relation. Observe,

(8)

$$\begin{aligned} I(P, F \cap G) = \dim(\mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P) &\geqslant \dim(\mathcal{O}_P/\langle \text{gen}(I^{m+n}), F, G\rangle\mathcal{O}_P) \\ &\overset{(a)}{=} \dim(k[x,y]/\langle \text{gen}(I^{m+n}), F, G\rangle) \\ &\overset{(b)}{\geqslant} \dim(k[x,y]/I^{m+n}) - \dim(k[x,y]/I^m) - \dim(k[x,y]/I^n) \\ &\overset{(c)}{=} \frac{(m+n)(m+n+1)}{2} - \frac{m(m+1)}{2} - \frac{n(n+1)}{2} \\ &= mn. \end{aligned}$$

We get (a) by noticing $\mathbf{V}(\text{gen}(I^{m+n}), F, G) = \{(0,0)\}$ and applying Theorem 2.1. On the other hand, (b) follows from observations (6) and (7), and (c) follows from Proposition 5.3 (see Appendix). Thus, we have the desired inequality, so it remains to show the equality holds if and only if F_C and G_C intersect transversely at P.

For our examination, we will consider the two inequalities in the above string. Namely, we must examine when equality holds in

(i) $\dim(\mathcal{O}_P/\langle F, G\rangle\mathcal{O}_P) \geqslant \dim(\mathcal{O}_P/\langle \text{gen}(I^{m+n}), F, G\rangle\mathcal{O}_P)$,

(ii) $\dim(k[x,y]/I^n) + \dim(k[x,y]/I^m) \geqslant \dim(\text{im}(\psi))$.

In (i), we will prove that if F_C and G_C intersect transversely, then we have equality. In (ii), we will demonstrate both directions, which is sufficient to conclude equality holds if and only if F_C and G_C intersect transversely at P.

We begin with (i). Notice, (i) holds exactly when $I^{m+n} \subseteq \langle F, G\rangle \mathcal{O}_P$. But I^{m+n} is generated by $S := \{x^i y^j \mid i + j = m + n\}$, which is a basis for forms of degree $m + n$. Thus, if we can show some basis for forms of degree $m + n$ is in $\langle F, G\rangle \mathcal{O}_P$, we will be done.

Let $L_1, \ldots, L_m$ and $M_1, \ldots M_n$ be the tangents to F_C and G_C, respectively at P; we will consider $A_{ij} := L_1 \cdots L_i M_1 \cdots M_j$. If $i > m$, we define $L_i := L_m$ and if $j > n$, we say $M_j := M_n$. Furthermore, we may assume P is the origin, by (3).

Notice $\{A_{ij} \mid i + j = m + n\}$ contains $m + n + 1$ elements (the same number as S), is linearly independent (since F_C and G_C do not share any common tangents) and each L_i, M_j is a linear form since $P = (0, 0)$. Thus, the set constitutes a basis for forms of degree $m + n$. Consequently, if we show A_{ij} for $i + j = m + n$ are in $\langle F, G\rangle \mathcal{O}_P$, we will be done.

For this task, we will show $I^{t+1} \subseteq \langle F, G\rangle \mathcal{O}_P$ implies the same holds for I^t for $t \geqslant m+n-1$. This reduces our proof to demonstrating $I^t \subseteq \langle F, G\rangle \mathcal{O}_P$ for large enough t.

Let $i + j \geqslant m + n - 1$. Then, at least one of $i \geqslant m$ or $n \geqslant n$ must hold. Without loss of generality, assume $i \geqslant m$. Then, $A_{ij} = A_{m0}B$, where B is a form of degree $i + j - m$. Note that $A_{m0} = L_1 \cdots L_m$ and $P = (0, 0)$, so $F = A_{m0} + F'$, where $m_P(F') \geqslant m+1$. Thus, $A_{ij} = FB - F'B$. But $FB \in \langle F, G\rangle \mathcal{O}_P$, so we need only show $F'B \in \langle F, G\rangle \mathcal{O}_P$ to reach our desired result. The key observation here is that since $m_P(F') \geqslant m + 1$ and B is a form of degree $m + n - 1$, the lowest degree term in $F'B$ must be at least $i+j+1$. Thus, we have reduced showing $A_{ij} \in \langle F, G\rangle \mathcal{O}_P, i+j \geqslant m+n-1$ to demonstrating $A_{i_0 j_0} \in \langle F, G\rangle \mathcal{O}_P, i_0 + j_0 = i + j + 1$.

As noted, we may now simply show $I^t \subseteq \langle F, G\rangle \mathcal{O}_P$ for large enough t. For this proof, we will apply the strong Nullstellensatz [3, p. 179]. We will show $X^N, Y^N \in \langle F, G\rangle \mathcal{O}_P$ for large enough N. Let $\mathbf{V}(F, G) = \{P, Q_1, \ldots, Q_r\}$ and choose H such that $H(P) = 1, H(Q_i) = 0$ for all i.[1] Now, if $H(Q_i) = 0$ for all i, XH, YH vanish on all Q_i and P, so $(XH)^N, (YH)^N \in \langle F, G\rangle \mathcal{O}_P$ for some N. But since $H(P) \neq 0$, H is a unit in $\mathcal{O}_P$. Thus, $X^N, Y^N \in \langle F, G\rangle \mathcal{O}_P$. Hence, $I^{2N} \subseteq \langle F, G\rangle \mathcal{O}_P$, so we have our result for (i).

[1] Note, we may assume this variety is finite, since we assume F_C and G_C intersect transversely at P, and (2) allows us to say F and G only contain components vanishing at P. Then, if there was a shared component, F_C and G_C would share a tangent.

We now move on to (ii). Namely, ψ is injective if and only if F_C and G_C share no common tangents at P.

For the reverse direction, we first note ψ is a linear map, since addition and scalar multiplication are clearly preserved. Thus, we will show $\ker(\psi) = (\overline{0}^{I^n}, \overline{0}^{I^m})$. Assume F and G share no tangents at P and let $A, B \in k[x, y]$ such that $\psi(\overline{A}^{I^n}, \overline{B}^{I^m}) = \overline{0}^{I^{n+m}}$. Then, $FA + BG$ consists of terms of degree at least $m + n$ by our definition of I.

Now, let $r = m_P(A), s = m_P(B)$ and assume $m \leqslant n$. Notice that if $r \geqslant n, s \geqslant m$, we are done, since A and B would both be 0 modulo I^n and I^m, respectively. Therefore, consider $r < n$. But this implies some terms in AF will have a degree less than $m+n$. Then, for $\psi(\overline{A}^{I^n}, \overline{B}^{I^m}) = \overline{0}^{I^{n+m}}$, the resulting terms in AF with degree less than $m + n$ must cancel with some other terms of the same degree. It follows $s < m$, or else there would be no terms with which the low degree terms in AF could cancel. Thus, $r < n$ and $s < m$. We may, then, write

$$A = A_r + \text{ higher order terms; } B = B_s + \text{ higher order terms.}$$

With this notation, it is clear $A_r F_m$ and $B_s G_n$ are the lowest order terms in AF and BG respectively, so they must cancel for $\psi(\overline{A}^{I^n}, \overline{B}^{I^m}) = \overline{0}^{I^{n+m}}$. Alternatively, $A_r F_m = -B_s G_n$. But, F and G share no tangents at P, so F_m and G_n have no common components. Hence, our equation says that G_n and F_m divide A_r and B_s, respectively. This contradicts our assumption that $r < n$ and $s < m$, so it must be the case that $(\overline{A}^{I^n}, \overline{B}^{I^m}) = (\overline{0}^{I^n}, \overline{0}^{I^m})$, as desired.

For the forwards direction, we will prove the contrapositive. Let L be a common tangent of F and G. Then,

$$F_m = LF'_{m-1}, G_n = LG'_{n-1}.$$

Now, observe

$$\begin{aligned}
\psi(\overline{G'_{n-1}}^{I^n}, \overline{F'_{m-1}}^{I^m}) &= \overline{FG'_{n-1} + GF'_{m-1}}^{I^{n+m}} \\
&\overset{(a)}{=} \overline{F_m G'_{n-1} + G_n F'_{m-1}}^{I^{n+m}} \\
&= \overline{LF'_{m-1}G'_{n-1} + LG'_{n-1}F'_{m-1}}^{I^{n+m}} = \overline{0}^{I^{n+m}}
\end{aligned}$$

where equality (a) is obtained by observing F_m and G_n are the lowest degree forms in F and G respectively, so all other terms in FG'_{n-1} and $G_n F'_{m-1}$ are $\overline{0}^{I^{n+m}}$. Thus, the kernel is non-zero, and ψ is not injective.

With these facts, we may conclude for the inequality string in equation (6), equality holds if and only if F_C and G_C share no tangents at P, completing our proof of (5) and the proof of correctness.

□

Returning to our motivating examples, we should check this idea of intersection number will solve our dilemma. By property (7) and (5) of the intersection number, we have

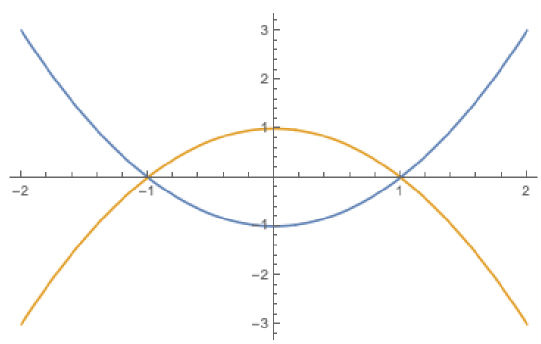
$$I((0,0), x^2 - y \cap y) = I((0,0), x^2 \cap y) = 2.$$

Then counting points of intersection on the curves defined by $x^2 - y = 0$ and $y = 0$ by intersection number, we find the sum is $2 = \deg(x^2 - y)\deg(y)$. A similar analysis will reveal for F_C and G_C where $F := x^2 - y^2$ and $G := y$ that $\sum_{P \in F_C \cap G_C} I(P, F_C \cap G_C) = 2$, as desired.

It is still too early to celebrate, however, as there are still some curves, F_C, G_C, for which we find the sum of the intersection numbers of points in $F_C \cap G_C$ is less than $\deg(F)\deg(G)$.

3. Projective Space

While in Section 2, we solved one disparity in considering why two plane curves F_C, G_C intersect in less than $\deg(F)\deg(G)$ points, we still have some work to do. Consider the curves defined by $0 = F := -y - x^2 + 1$, and $0 = G := -y + x^2 - 1$. The curves are graphed below.

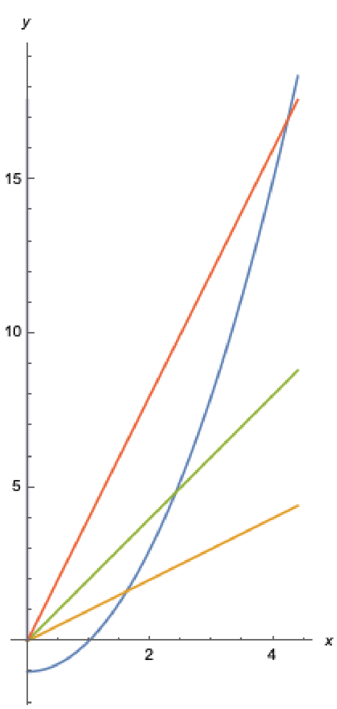


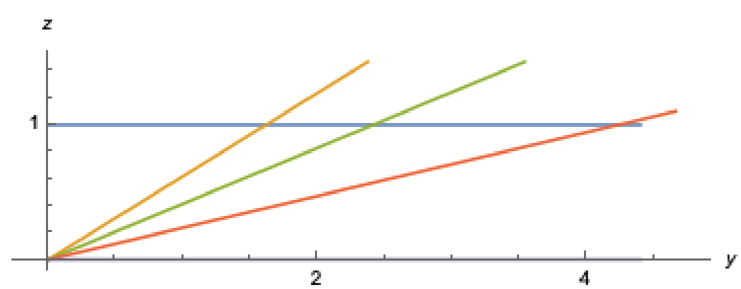
Solving for their intersection, we find $x = \pm 1, y = 0$. Thus, F_C and G_C have two points of intersection, despite the defining polynomials both being of degree 2. Furthermore, our discussion of intersection number above does not seem to apply, since F_C and G_C intersect transversely at both $(1,0)$ and $(-1,0)$. Notice, however, both ends of the parabolas trail off in similar, but opposite, directions. Perhaps including this behavior more formally might give us the results we desire.

3.1. **Projective Plane.** Formally, what we would like to do is include the behavior as our curves approach ∞ as a point. The projective plane, it turns out, will allow us to do just that.

The projective plane, essentially, completes the affine plane by adding points at infinity. To add these points at infinity, we use homogeneous coordinates. In our case, each coordinate will have three values $(x : y : z)$, just as in affine three space. The distinction, however, is that now, we consider two homogenous points $(x_1 : y_1 : z_1)$ and $(x_2 : y_2 : z_2)$ to be equal if $(x_1 : y_1 : z_1) = \lambda(x_2 : y_2 : z_2)$ for some nonzero $\lambda \in k$. This requirement for λ to be nonzero is essential, or else every point in the projective plane would be equal. Geometrically, two points are equal if they lie on the same line through the origin. Thus, for every point $(x : y : z)$ where $z \neq 0$, we may associate it with the point $(\frac{x}{z} : \frac{y}{z} : 1)$. This plane at $z = 1$ is our usual affine plane.

Notice, however, we also have points in $\mathbb{P}^2$ for which $z = 0$. These are the points at ∞ we desired. While we will not formally discuss why these are indeed the points at infinity we want (see [3, Chapter 8] for a more complete discussion on the projective plane and points at infinity), we will motivate the fact with our example of $0 = F := -y + x^2 - 1, 0 = G := -y - x^2 + 1$. A portion of F_C is graphed below, along with some lines passing along the origin. The left graph depicts the XY-plane, whereas the right depicts the YZ-plane. Like colored lines on the two planes correspond to the same line in $\mathbb{A}^3$.





Our motivating observation is that, as we continue to move towards ∞ along the parabola in the XY-plane, the slope of the line through the origin approaches the vertical purple line. A similar observation can be made in the YZ-plane. Thus, it is reasonable to consider the point $(0 : 1 : 0)$ in homogeneous coordinates, which corresponds to the purple line, as the line at ∞ for our parabola. A similar analysis on G_C yields the point $(0 : -1 : 0) = (0 : 1 : 0)$ in homogeneous coordinates. Then, we find another point of intersection for the curves F_C and G_C in the projective plane. This embedding will allow us to make a strong statement relating intersection numbers and polynomial degrees in Bézout's Theorem.

3.2. **From Affine to Projective.** Before we begin our coverage of Bezout's Theorem, we first mention many affine results, such as the strong Nullstellensatz and intersection numbers, may be extended to work in projective space as well. For a discussion on extending algebraic results, see [3, Section 8.3].

Furthermore, our definitions of multiplicity and intersection number carry over nicely to projective space by considering our projective plane $\mathbb{P}^2$ as embedded in $\mathbb{A}^3$. This is covered in [1, Section 5.1], but we provide a brief summary here with some additional details.

We define the multiplicity of a point $P \in \mathbb{P}^2$ on a projective plane curve F_C to be $m_P(F_*)$, where F_* is the dehomogenization of F with respect to z. This may raise concerns, since it is unclear if this definition is affected by a projective change in coordinates or is dependent on which variable we use to dehomogenize F. Fortunately, in both instances, this is not the case.

As to why a projective change in coordinates does not affect this definition, note if we are examining the multiplicity at $P = (x : y : z)$ and $z \neq 0$, we may identify P with $(\frac{x}{z} : \frac{y}{z} : 1)$. Then, $\mathcal{O}_P(F) \cong \mathcal{O}_{(x,y)}(F(x, y, 1))$, trivially. A similar result holds for dehomogenization with respect to either x or y. Furthermore, if T is a projective change in coordinates, let $F^T := F(T(x : y : z))$. Now, assume we have some point $P = (x : y : 0)$ on F^T_C; note we may apply our projective change of coordinates, T, so that $T(P) = (x_0 : y_0 : z_0)$ for some $z_0 \neq 0$. But, a projective change of coordinates in $\mathbb{P}^2$ can be considered an affine change of coordinates in $\mathbb{A}^3$. Furthermore, we know affine changes of coordinates preserve the structure of local rings from (3) in our proof of correctness for Theorem 2.3, so we have

$$\mathcal{O}_{(\frac{x}{y},1,0)}(F^T(x, 1, z)) \cong \mathcal{O}_P(F^T) \cong \mathcal{O}_{T(P)}(F) \cong \mathcal{O}_{(\frac{x_0}{z_0},\frac{y_0}{z_0},1)}(F(x, y, 1)).$$

Thus, our definition of multiplicity is unchanged for a projective change in coordinates.

Similarly, our definition of multiplicity is independent of our choice of homogenization variable, since the local rings will be isomorphic.

The last piece we need to extend is the intersection number of two curves F_C and G_C. We propose

$$I(P, F \cap G) = \mathcal{O}_P(\mathbb{P})/\langle F_*, G_*\rangle\mathcal{O}_P(\mathbb{P})$$

for our definition of intersection number. This may be concerning, since F_* and G_* will be different depending on how we dehomogenize. It turns out, however, that if F_* and F'_* are distinct dehomogenizations of F, $\langle F_*, G_*\rangle \mathcal{O}_P(\mathbb{P}) = \langle F'_*, G_*\rangle \mathcal{O}_P(\mathbb{P})$. To see this, let $F_* = F/L^d$ be a dehomogenization of the degree d form F with respect to L. In this case, L is a line in $\mathbb{P}^2$ not passing through any points in the finite variety $\mathbf{V}(F, G)$. Then, if we pick some other line L' also not passing through any points in our variety, we notice $F'_* = F/L'^d = F_*(\frac{L}{L'})^d$, so the two ideals are the same in our local ring, since L and L' do not vanish on any points in the variety.

With these extensions of our affine results to projective results, we move onto our main theorem, Bézout's theorem.

4. Bezout's Theorem and Consequences

4.1. **Bézout's Thoerem.**

Our proof of Bézout's theorem follows the outline provided by Fulton, [1, Section 5.3], but we include additional details.

Theorem. *Let F_C, G_C be projective plane curves of degree m, n, respectively. Then, if F and G share no common components, and $F \cap G = \{P_1, \ldots, P_N\}$, we have*

$$\sum_{i=1}^{N} I(P_i, F \cap G) = mn.$$

Proof. We begin with some important facts and definitions. Recall that we have shown that the intersection number at a point on projective curves F_C, G_C is equivalent to the intersection number of the dehomogenized affine curves F_{*_C}, G_{*_C}. Then we have

$$\sum_{i=1}^{N} I(P_i, F \cap G) = \sum_{i=1}^{N} I(P_i, F_* \cap G_*) = \dim_k k[x, y]/\langle F_*, G_*\rangle. \tag{9}$$

We get the second equality by observing $I(P_i, F_* \cap G_*) = \mathcal{O}_{P_i}(\mathbb{A}^2)/\langle F_*, G_*\rangle$ and applying Theorem 2.1. Furthermore, since F_C, G_C intersect at a finite number of points, we may apply a projective change of coordinates to ensure no points in $F_C \cap G_C$ lie on the line at infinity ($z = 0$). Finally, we define the following:

$$\begin{aligned} R &:= k[x, y, z], \\ \Gamma &:= R/\langle F, G\rangle, \\ \Gamma_* &:= k[x, y]/\langle F_*, G_*\rangle, \\ \Gamma_d &:= \{H \in \Gamma \mid H \text{ is a form of degree d}\}, \\ R_d &:= \{H \in R \mid H \text{ is a form of degree d}\}. \end{aligned}$$

We will prove the following:

(1) $\dim \Gamma_d = mn$,

(2) $\dim \Gamma_* = \dim \Gamma_d$

for sufficiently large d. Then, by our earlier observation in (9), this will complete our proof.

(1) To show $\dim \Gamma_d = mn$, we will argue the claim holds when $d \geqslant m + n$. Now, consider the following sequence

$$0 \to R \xrightarrow{\psi} R \times R \xrightarrow{\phi} R \xrightarrow{\pi} \Gamma \to 0,$$

where ψ, ϕ, and π are defined as follows:

$$\psi(C) = (GC, -FC),$$
$$\phi(A, B) = AF + BG,$$
$$\pi(H) = \overline{H}.$$

We will use the fact that if the above sequence is exact, then $\dim \Gamma = \dim R - \dim(R \times R) + \dim R$ by Proposition 2.1. When we restrict the sequence to forms of specific degree, we get

$$0 \to R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\phi} R_d \xrightarrow{\pi} \Gamma_d \to 0$$

Note that R_{d-m-n} is well-defined since we assume $d \geqslant m + n$. Then, since $\dim R_d = \frac{(d+1)(d+2)}{2}$, it follows that $\dim \Gamma_d = \dim R_d - \dim(R_{d-m} \times R_{d-n}) + \dim R_{d-m-n} = mn$, as desired. Thus, we will show the initial sequence is exact. For the sequence to be exact, the following must be true

(a) ψ is injective;
(b) $\mathrm{im}(\psi) = \ker(\phi)$;
(c) $\mathrm{im}(\phi) = \ker(\pi)$;
(d) π is surjective.

We begin by noting the injectivity of ψ and surjectivity of π are obvious. Similarly, that $\mathrm{im}(\phi) = \ker(\pi)$ is straightforward from our definitions. It remains to consider (b).

To see $\mathrm{im}(\psi) \subseteq \ker(\phi)$, first observe that

$$\phi(\psi(C)) = \phi(GC, -FC) = FGC - FGC = 0$$

It remains to show the other inclusion. If $(A, B) \in \ker(\phi)$, then $AF + BG = 0$, so $AF = -BG$. But, we assume F, G share no common components, so $A = GC$, $B = -FC$, for some $C \in R$. Hence, $\psi(C) = (A, B)$, as desired. Thus, our result follows.

(2) To see $\dim \Gamma_* = \dim \Gamma_d$, we will need to make use of the following map $\alpha : \Gamma \to \Gamma$ where $\alpha(\overline{H}) = \overline{ZH}$. Note that α is a linear map. We will now show α is injective.

Since α is a linear map, we need only show $\ker(\alpha) = 0$. Thus, let $\overline{ZH} = \overline{0}$ in Γ_{d+1}, so $ZH = AF + BG$, where $A, B \in R$. We want to show $H = A'F + B'G, A', B' \in R$.

We begin by defining $F_0 = F(x, y, 0)$ and G_0 similarly. Recall that we assume $F \cap G$ contains no points on the line at infinity, $z = 0$. Then F, G, Z share no common zeros, so F_0, G_0 must have no common components. Thus F_0, G_0 are relatively prime in $k[x, y]$.

But $ZH = AF + BG$, so $(ZH)_0 = 0 = A_0F_0 + B_0G_0$. Thus, $A_0F_0 = -B_0G_0$. Since F_0 and G_0 are relatively prime, by a similar argument as in the previous part of the proof, we conclude $A_0 = G_0C, B_0 = -F_0C$, for some $C \in k[x, y]$.

Next, let $A_1 = A - CG$ and $B_1 = B + CF$, and observe that

$$(A_1)_0 = A_0 - CG_0 = A_0 - A_0 = 0,$$
$$(B_1)_0 = B_0 + CF_0 = B_0 - B_0 = 0,$$

since C contains no terms with Z. But if $(A_1)_0 = 0, (B_1)_0 = 0$, every term in both must contain Z. Thus, $A_1 = ZA', B_1 = ZB'$. But

$$ZH = AF + BG = AF + BG - CFG + CFG = A_1F + B_1G = Z(A'F + B'G)$$

so $H = A'F + B'G$, as desired.

Now we have developed the tools needed to prove $\dim \Gamma_* = \dim \Gamma_d$. First, we choose $A_1, \ldots, A_{mn} \in R_d$ such that $\overline{A_1}, \ldots, \overline{A_{mn}} \in \Gamma_d$ form a basis for Γ_d. We will show if $A_{i*} = A_i(x, y, 1)$, then $a_i = \overline{A_{i*}}, i = 1, \ldots, mn$ form a basis for Γ_*.

First, we note α maps degree d forms to degree $d + 1$ forms in Γ. Let $\alpha_d : \Gamma_d \to \Gamma_{d+1}$ be the restriction of the domain of α to forms in Γ of degree d. Furthermore α is injective and a linear map. Thus, α_d is an isomorphism between vector spaces, so $\dim \Gamma_{d+r} = mn$ for all $r \geqslant 0$. Furthermore, $\overline{Z^rA_1}, \ldots, \overline{Z^rA_{mn}}$ form a basis for Γ_{d+r}.

Now, we will show $a_1, \ldots, a_{mn}$ generate Γ_*. Let $h = \overline{H} \in \Gamma_*$. Then $H \in k[x, y]$, so $Z^MH^* \in \Gamma_{d+r}$ where $M \geqslant 0$ and H^* is the homogenization of H. But, we may express Z^MH^* in terms of our basis for Γ_{d+r} and an element of $\langle F, G\rangle$. Namely,

$$Z^MH^* = \sum_{i=1}^{mn} \lambda_i Z^r A_i + BF + CG, \quad B, C \in k[x, y, z], \lambda_i \in k.$$

But then,

$$H = (Z^MH^*)_* = \sum_{i=1}^{mn} \lambda_i A_{i*} + B_*F_* + C_*G_*$$

so,

$$h = \overline{H} = \sum_{i=1}^{mn} \lambda_i a_i.$$

Next, we show $\{a_1, \ldots, a_{mn}\}$ is a linearly independent set. Let $\sum_{i=1}^{mn} \lambda_i a_i = 0$. Then, $\sum_{i=1}^{mn} \lambda_i A_i = BF_* + CG_*$ for some $B, C \in k[x, y]$. Hence by Proposition 5 [1, Section 2.6],

$$Z^r \sum_{i=1}^{mn} \lambda_i A_i = Z^s B^* F + Z^t C^* G, \ \ s, t \in \mathbb{Z}_{\geqslant 0}.$$

Then $\sum_{i=1}^{mn} \lambda_i \overline{Z^r A_i} = 0$ in Γ_{d+r}. But $\{\overline{Z^r A_i}, \ldots, \overline{Z^r A_{mn}}\}$ is a basis for Γ_{d+r}, so it must be the case that $\lambda_i = 0$ for all i. Thus, $\{a_1, \ldots, a_{mn}\}$ is a basis for Γ_*, as desired.

Then we have that $\dim \Gamma_* = mn$, which completes our proof by (9).

□

4.2. **Applications.** We address a few immediate consequences of Bézout's Theorem below.

Proposition. *If H_C is a non-singular plane curve, then H is irreducible.*

Proof. Assume H_C is non-singular but reducible. Then $H = FG$ for some forms F, G. Note that we may assume F and G share no components. If they did, we could regroup our factorization $H = F'G'$ such that F' and G' share no components. Then Bézout's theorem guarantees F and G intersect at at least one point p. Hence, $F(p) = 0 = G(p)$. But if $H = FG$, then

$$\nabla H = (F_x G + F G_x, F_y G + F G_y).$$

But then $\nabla H(p) = (0, 0)$, so p is a singular point on H_C. Contradiction. □

Proposition. *For a projective plane curve F_C with defining polynomial of degree n, the sum of the multiplicities at points in $F_C \cap \frac{d}{dx} F_C$, where $\frac{d}{dx} F_C$ is the curve defined by the vanishing of $\frac{d}{dx} F$, is at most $n(n-1)$ when $\frac{d}{dx} F \neq 0$.*

Proof. Once we note that F and $\frac{d}{dx} F$ share no common components, since F is irreducible, we see that the latter result follows immediately from property (5) of the intersection number and Bézout's theorem. But to apply Bézout's theorem, $\frac{d}{dx} F$ must be a nonzero form. Since we assume $\frac{d}{dx} F \neq 0$, one concern is addressed. Furthermore, note that for each term in F without x^m for some $m > 0$, the term vanishes when taking the partial derivative of F with respect to x. Similarly, for each term in F with x^m for any $m > 0$, the corresponding term in $\frac{d}{dx} F$ contains the same powers for y and z, but the power for x will be $m-1$. Thus, $\frac{d}{dx} F$ is also a form of degree $n - 1$. As noted earlier, the result then follows. □

5. Appendix

Proposition 5.1. *Let V be a variety in $\mathbb{A}^n$, $I = \mathbf{I}(V)$, and J be an ideal containing I. Then, letting J' be the natural image of J in $\Gamma(V)$, we have*

$$\mathcal{O}_P / J\mathcal{O}_P \cong \mathcal{O}_P(V) / J'\mathcal{O}_P(V).$$

Proof. Consider the sequence of natural homomorphisms

$$\mathcal{O}_P \xrightarrow{\phi_1} \mathcal{O}_P(V) \xrightarrow{\phi_2} \mathcal{O}_P(V)/J'\mathcal{O}_P(V),$$

and let $\phi := \phi_2 \circ \phi_1$. We will show $\ker(\phi) = J$. Then, since J' is the image of J in $\Gamma(V)$, $J\mathcal{O}_P(V) = J'\mathbb{O}_P(V)$. By the fundamental theorem of ring homomorphisms, this will complete our proof.

Note that $\ker(\phi_1) = I$ and $\ker(\phi_2) = J'$. Then, since $I \subseteq J$ and $\phi_1(J) = J'$, $\ker(\phi_1) \subseteq \ker(\phi_2)$, so $\ker(\phi) = J$. □

Proposition 5.2. *Let $M_1, \ldots, M_n$ be pairwise comaximal ideals of some ring R. Then for $d \geqslant 1$,*

$$\bigcap_{i=1}^{n}(M_i^d) = (\bigcap_{i=1}^{n} M_i)^d$$

Proof. We will first prove the following to reach our desired result

(1) If I and J are comaximal ideals of R, then $IJ = I + J$.
(2) If I and J are as above and $d \geqslant 1$, $I^d \cap J^d = (I \cap J)^d$.
(3) $M_i + \Pi_{j\neq i} M_j = R$.
(4) $M_1 \ldots M_n = \bigcap_{i=1}^{n} M_i$.

(**1**) We will use double containment. For the forwards direction, let $F \in IJ$. Then, $F = F_iF_j$ for some $F_i \in I$ and $F_j \in J$. By this observation, it is obvious $F \in I, J$, so F is in their intersection.

The backwards direction requires more work, but is not hard. Let $F \in I \cap J$. Then F is in both I and J. But $I + J = R$, by the comaximality of I and J, so there exists $F_i \in I$ and $F_j \in J$ such that $F_i + F_j = 1$. Observe

$$F = F(F_i + F_j) = FF_i + FF_j.$$

Notice $FF_i \in IJ$ since $F \in J$ and $F_i \in I$, and $FF_j \in IJ$ since $F \in I$ and $F_j \in J$. Thus, $F \in IJ$.

(**2**) First, we note

$$(I \cap J)^d = (IJ)^d = I^dJ^d = I^d \cap J^d,$$

if I^d and J^d are comaximal, by (1). But

$$R = R^{2d} = (I + J)^{2d} = I^{2d}J^0 + \cdots + I^dJ^d + \cdots + I^0J^{2d} \subseteq I^d + J^d,$$

where the rightmost containment can be seen by noting each term in the expansion of $(I + J)^{2d}$ is of the form I^rJ^l with at least one of $r \geqslant d$ or $l \geqslant d$. Hence, $R \subseteq I^d + J^d$, so I^d and J^d are comaximal.

(**3**) Let $S := \{j \mid j \neq i\}$ and observe

$$\begin{aligned} R = R^{|S|} &= \Pi_{j\in S}(M_i + M_j) \\ &= \Pi_{j\in S}(M_j) + M_i(\text{other terms}) \subseteq M_i + \Pi_{j\in S}M_j \subseteq M_i + M_k = R, \end{aligned}$$

where k is any index in S. Thus, $R \subseteq M_i + \Pi_{j\in S}M_j \subseteq R$, so $M_i + \Pi_{j\in S}M_j = R$.

(**4**) Observe

$$\bigcap_{i=1}^{n} M_i \overset{(a)}{=} M_1 \cap \cdots \cap M_n \overset{(a)}{=} M_1M_2 \cap M_3 \cap \cdots \cap M_n$$
$$\overset{(b)}{=} M_1M_2M_3 \cap M_4 \cap \cdots \cap M_n$$
$$\vdots$$
$$= M_1 \cdots M_n.$$

Equality (a) follows from identifying M_1 and M_2 with I and J in (1). Similarly, equality (b) can be seen by noting (3) implies $M_1M_2 \cap M_3 = R$ (since $\{M_1, M_2, M_3\}$ is a collection of pairwise comaximal ideals) and applying (1) (taking M_1M_2 as I and M_3 as J). This process is continued inductively until we arrive at $M_1 \cdots M_n$.

Finally, we prove our main claim. We will induct on n, with (2) serving as our base case. Observe

$$\bigcap_{i=1}^{n+1} M_i^d = \bigcap_{i=1}^{n} (M_i^d) \cap M_{n+1}^d = (\bigcap_{i=1}^{n} M_i)^d \cap M_{n+1}^d \text{ by our inductive hypothesis,}$$
$$= (M_1 \cdots M_n)^d \cap M_{n+1}^d \text{ by (4),}$$
$$= (M_1 \cdots M_n \cap M_{n+1})^d \text{ by (2) and (3),}$$
$$= (\bigcap_{i=1}^{n+1} M_i)^d \text{ by (1) and (3).}$$

□

Proposition 5.3. *Let* $I = \langle x, y \rangle \subseteq k[x, y]$*. Then,*

$$\dim_k(k[x, y]/I^n) = 1 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof. First, we characterize I^n by $I^n = \{P \in k[x, y] \mid \text{the degree of each term in } P \text{ is at least } n\}$. Then it is clear $\{x^\alpha \mid |\alpha| = n\}$ is a set of generators for I^n, so any element of $k[x, y]/I^n$ can be identified with a polynomial with terms of total degree less than n. Thus, the dimension of $k[x, y]/I^n$ as a vector space over k can be determined by counting the monomials with total degree less than n. The reader will find there are $1 + \cdots + n$ such monomials. □

References

[1] W. Fulton. *Algebraic Curves*, Third Edition, 2008. http://www.math.lsa.umich.edu/ wfulton/CurveBook.pdf.

[2] J. Little, D. Cox, D. O'Shea. *Using Algebraic Geometry*, New York, NY. Springer, Second Edition, 2005.

[3] J. Little, D. Cox, D. O'Shea. *Ideals, Varieties, and Algorithms*, New York, NY. Springer, Third Edition, 2007.