Bézouts Theorem

Parvez Rasul
Roll : 204090001
1st year, Ph.D.

Department of Mathematics
Indian Institute of Technology, Bombay

November 4, 2020

Bézouts theorem : Introduction

Let C and D be two plane curves, described by equations $f(X, Y) = 0$ and $g(X, Y) = 0$, where f and g are nonzero polynomials of degree m and n, respectively. Bézout's theorem says that if "all is well", then C and D meet in precisely mn points.

- Rings are always assumed to be commutative with a unity element 1. k will always denote a fixed ground field.
- For $n \in \mathbb{N}$ we call $\mathbb{A}^n := \{(x_1, x_2, \ldots, x_n) : x_i \in k\} = k^n$ the affine n-space over k.
- For a subset $S \subset k[X_1, \ldots, X_n]$ of polynomials we call $V(S) := \{P \in \mathbb{A}^n : f(P) = 0 \quad \forall f \in S\} \subset \mathbb{A}^n$ the (affine) zero locus of S. Subsets of $\mathbb{A}^n$ of this form are called affine algebraic set. If $S = \{f_1, \ldots, f_i\}$ is a finite set, we will write $V(S) = V(f_1, \ldots, f_i)$.

Some facts from algebra

- If I be an ideal in $k[X_1, \ldots, X_n]$ generated by S, then $V(S) = V(I)$. So, every algebraic set is equal to $V(I)$ for some ideal I.
- If $V(f) \cup V(g) = V(fg)$ and $V(f) \cap V(g) = V(f, g) \quad \forall f, g \in k[X_1, X_2, \ldots, X_n]$.
- $V(0) = \mathbb{A}^n$
- $V(k[X_1, X_2, \ldots, X_n]) = V(1) = \phi$
- Hilbert Nullstellensatz : If k be algebraically closed and I be an ideal of $k[X_1, \ldots, X_n]$ such that $V(I) = \phi$, then $1 \in I$.
- For $f, g \in k[X_1, \ldots, X_n]$, $g|f$ then $V(g) \subset V(f)$.

Affine plane curves

Definition

$\mathbb{A}^2_k = \{(x, y) : x, y \in k\}$ is called the affine plane over k.

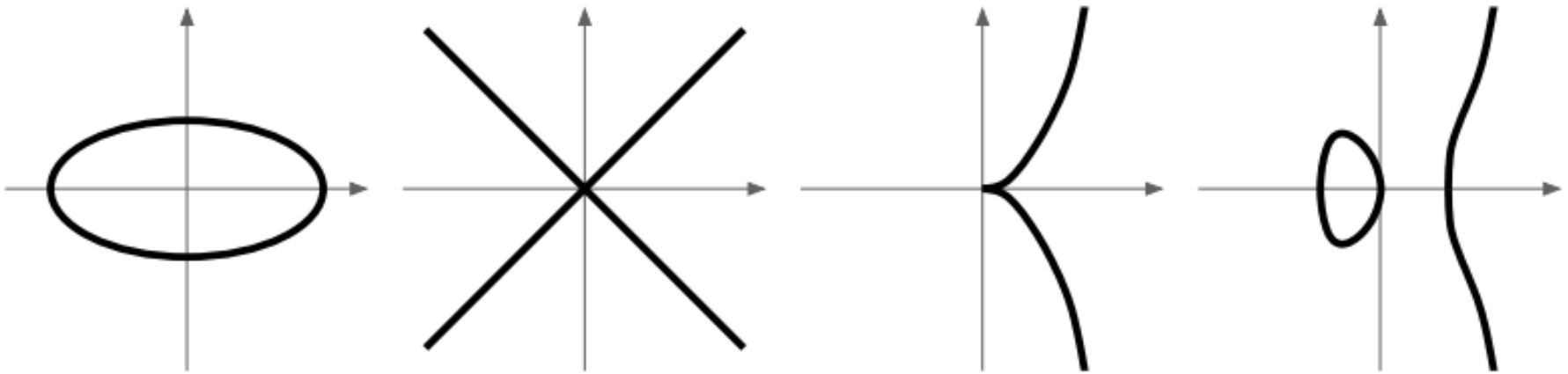
Definition

An affine plane curve $C \subset \mathbb{A}^2_k$ over K is just the zero locus of a nonconstant polynomial in two variables over K i.e. $V(f)$ for some nonconstant $f(X, Y) \in K[X, Y]$.

Observe that if C be an affine plane curve with $C = V(f)$, then $C = V(cf)$ for any nozero scalar $c \in k^*$. So affine curves are defined upto an equivalence relation.

Examples

Example 1 : Some plane curves over $\mathbb{R}$



$\frac{x^2}{4} + y^2 - 1 = 0$ (a)

$x^2 - y^2 = 0$ (b)

$y^2 - x^3 = 0$ (c)

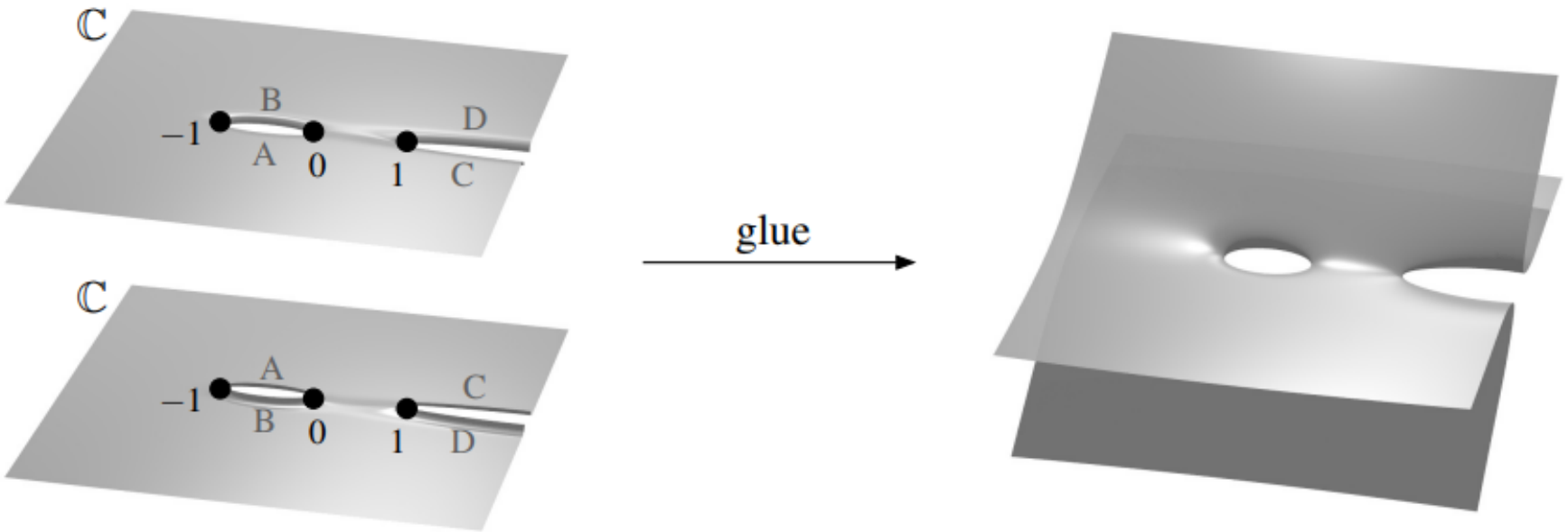
$y^2 + x - x^3 = 0$ (d)

Examples

Example 2 : Plane curves over $\mathbb{C}$

We take the polynomial $f(X, Y) = Y^2 + X - X^3$.

See that $f(x, y) = 0 \quad <=> \quad y^2 = x(x+1)(x-1)$



Conventions

- If $f \in k[X, Y]$, we say f is affine curve instead of $V(f)$.
- We will write $f \cap g$ instead of $V(f) \cap V(g)$.
- The degree of a curve is its degree as a polynomial.
- f and g are said to have no common component if $\gcd(f, g) = 1$.

Lemma

Let f be an affine curve.

(i) *If k is algebraically closed then $V(f)$ is infinite.*

(ii) *If k is infinite then $\mathbb{A}^2 \setminus V(f)$ is infinite.*

Lemma

If f and g be two affine curves over k of degree m and n such that f and g do not have a common component, then $\dim_k k[X,Y]/(f,g) \leq mn$.

Proof : Let R_d be the k-vector space of polynomials in $k[X,Y]$ of total degree at most d. So $\dim_k R_d = 1 + \cdots + (d+1) = \frac{1}{2}(d+1)(d+2)$. We call it $\sigma(d)$ i.e. $\sigma(d) = \dim_k R_d = \frac{1}{2}(d+1)(d+2)$. Now for $d \geq m+n$ consider the sequence of vector space homomorphisms :

$$R_{d-m} \times R_{d-n} \xrightarrow{\alpha} R_d \xrightarrow{\pi} R_d/(f,g)$$

where $\alpha(u,v) = uf + vg$ and π is the quotient map. It is clear that $\operatorname{im}\alpha \subset \ker\pi$. Now if $(u,v) \in \ker\alpha$ then $uf = -vg$. Since $(f,g) = 1$ this is equivalent to $u = cg$ and $v = -cf$ for some $c \in R_{d-m-n}$. So $\ker\alpha = (g,-f) \cdot R_{d-m-n}$.

So

$$\begin{aligned}
\dim_k R_d/(f,g) &= \dim \operatorname{im} \pi \\
&= \dim R_d - \dim \ker \pi \\
&\leq \dim R_d - \dim \operatorname{im} \alpha \\
&= \dim R_d - (\dim R_{d-m} + dim R_{d-n} - \dim \ker \alpha) \\
&= \dim R_d - \dim R_{d-m} - dim R_{d-n} + \dim R_{d-m-n} \\
&= \sigma(d) - \sigma(d-m) - \sigma(d-n) + \sigma(d-m-n) \\
&= mn
\end{aligned}$$

Now if $\dim_k k[X,Y]/(f,g) > mn$ then we will get more than mn linearly independent elements in $R_d/(f,g)$ for sufficiently large d which is a contradiction as we showed that $\dim R_d/(f,g) \leq mn$ for all $d \geq m+n$. So we get $\dim_k k[X,Y]/(f,g) \leq mn$. To 33

Motivating Question

For polynomials in one variable,we ask how many zeros a single polynomial $f \in k[X]$ has. At least if K is algebraically closed, the answer is that we always get $\deg f$ zeros (counted with multiplicities).

Geometrically this question becomes at how many points does the graph of f intersects the horizontal axis which is equivalently number of intersection points of the two curves $g(X,Y) = f(X) - Y$ and $h(X,Y) = Y$.

So we can ask how many intersection points any two curves in plane can have in total, i. e. how many common zeros we find for two polynomials $f, g \in k[X,Y]$ and we would also hope for a result that depends only on $\deg f$ and $\deg g$, and not on the chosen polynomials.

The First inequality :

Proposition (Bez 1)

Let $f, g \in k[x, y]$ be affine curves of degrees m, n respectively. If f and g do not have a common factor, then $|f \cap g| \leq mn$.

The First inequality :

Proposition (Bez 1)

Let $f, g \in k[x, y]$ be affine curves of degrees m, n respectively. If f and g do not have a common factor, then $|f \cap g| \leq mn$.

Proof : We show that $|f \cap g| \leq \dim_k k[x, y]/(f, g)$ and by previous lemma, we get $|f \cap g| \leq mn$. Let $\{P_1, \ldots, P_r\} \subset f \cap g$. If $P_i = (a_i, b_i)$ for $i = 1, \ldots, r$, and we set

$$h_i(X, Y) := \prod_{j: a_j \neq a_i} (X - a_j) \cdot \prod_{j: b_j \neq b_i} (Y - b_j) \quad \in k[X, Y]$$

- By construction for each i, $h_i(P_i) \neq 0$ and $h_i(P_j) = 0$ for $j \neq i$.

The First inequality :

Proposition (Bez 1)

Let $f, g \in k[x, y]$ be affine curves of degrees m, n respectively. If f and g do not have a common factor, then $|f \cap g| \leq mn$.

Proof : We show that $|f \cap g| \leq \dim_k k[x, y]/(f, g)$ and by previous lemma, we get $|f \cap g| \leq mn$. Let $\{P_1, \ldots, P_r\} \subset f \cap g$. If $P_i = (a_i, b_i)$ for $i = 1, \ldots, r$, and we set

$$h_i(X, Y) := \prod_{j: a_j \neq a_i} (X - a_j) \cdot \prod_{j: b_j \neq b_i} (Y - b_j) \quad \in k[X, Y]$$

- By construction for each i, $h_i(P_i) \neq 0$ and $h_i(P_j) = 0$ for $j \neq i$.
- If we have $\sum_{j=1}^{r} \bar{c_j} \bar{h_j} = 0$ in $k[X, Y]/(f, g)$, then we get $\sum_{j=1}^{r} c_j h_j = uf + vg$ for some $u, v \in k[X, Y]$. Evaluating both sides at P_i we have $c_i = 0$. So, $\{h_i\}_{i=1}^{r}$ is a linearly independent set in $k[X, Y]/(f, g)$ and hence $r \leq \dim_k k[x, y]/(f, g)$.

The First inequality :

Proposition (Bez 1)

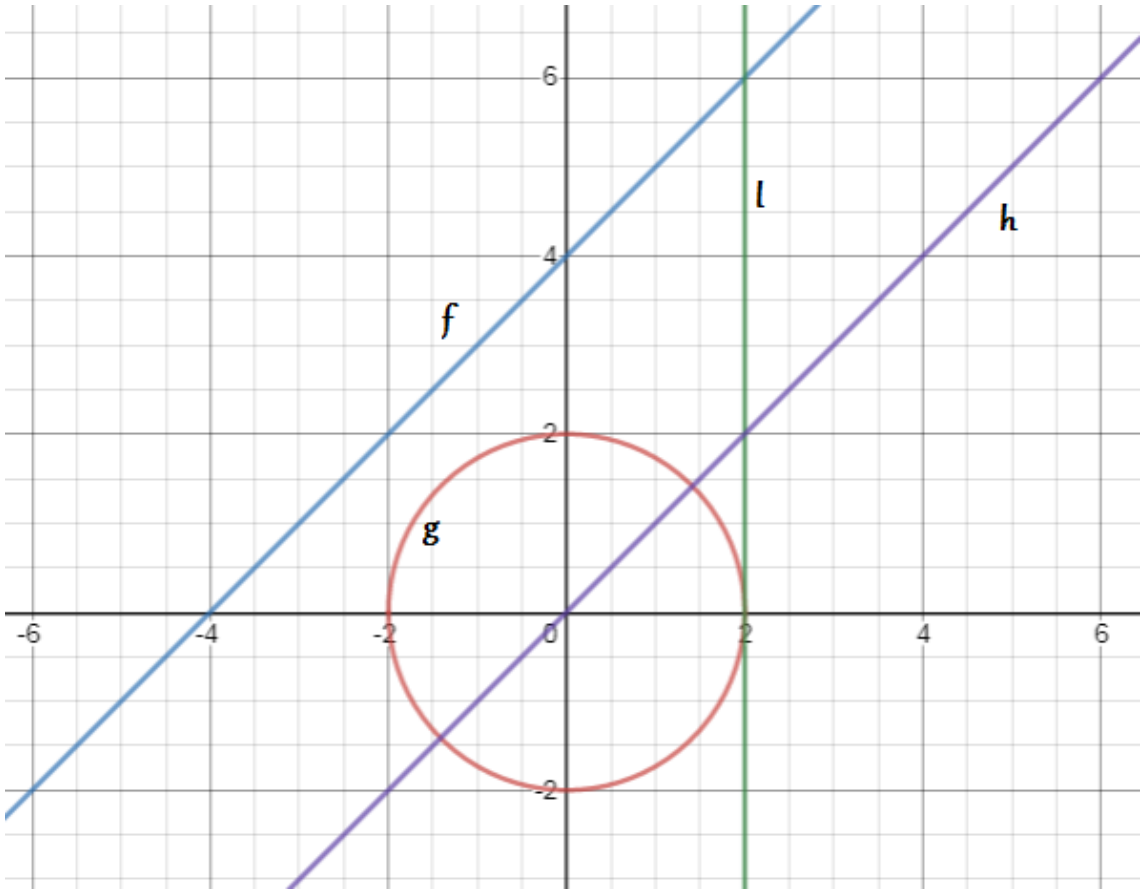
Let $f, g \in k[x,y]$ be affine curves of degrees m, n respectively. If f and g do not have a common factor, then $|f \cap g| \leq mn$.

Proof : We show that $|f \cap g| \leq \dim_k k[x,y]/(f,g)$ and by previous lemma, we get $|f \cap g| \leq mn$. Let $\{P_1, \ldots, P_r\} \subset f \cap g$. If $P_i = (a_i, b_i)$ for $i = 1, \ldots, r$, and we set

$$h_i(X,Y) := \prod_{j:a_j \neq a_i} (X - a_j) \cdot \prod_{j:b_j \neq b_i} (Y - b_j) \quad \in k[X,Y]$$

- By construction for each i, $h_i(P_i) \neq 0$ and $h_i(P_j) = 0$ for $j \neq i$.
- If we have $\sum_{j=1}^{r} \bar{c_j}\bar{h_j} = 0$ in $k[X,Y]/(f,g)$, then we get $\sum_{j=1}^{r} c_j h_j = uf + vg$ for some $u, v \in k[X,Y]$. Evaluating both sides at P_i we have $c_i = 0$. So, $\{h_i\}_{i=1}^{r}$ is a linearly independent set in $k[X,Y]/(f,g)$ and hence $r \leq \dim_k k[x,y]/(f,g)$.
- Now Since this holds for any subset $\{P_1, \ldots P_r\}$ of $f \cap g$ so this proves the proposition.

Examples



$$f(X,Y) = Y - X - 4, \quad g(X,Y) = (X^2 + Y^2 - 2^2),$$
$$h(X,Y) = (Y - X), \quad l(X,Y) = (Y - 2) \text{ in } \mathbb{A}^2_{\mathbb{R}}$$

What can go wrong!

There are several ways there can be 'missing' points of intersection.

- Missing points can have coordinates in an extension field.
  e.g. f and g in above example.
  Fix - Taking k to be algebraically closed.

What can go wrong!

There are several ways there can be 'missing' points of intersection.

- Missing points can have coordinates in an extension field.
  e.g. f and g in above example.
  Fix - Taking k to be algebraically closed.
- Missing points can coincide with other common points.
  e.g. g and l in above example.
  Fix - Counting multiplicities : Intersection Multiplicity

What can go wrong!

There are several ways there can be 'missing' points of intersection.

- Missing points can have coordinates in an extension field.
  e.g. f and g in above example.
  Fix - Taking k to be algebraically closed.
- Missing points can coincide with other common points.
  e.g. g and l in above example.
  Fix - Counting multiplicities : Intersection Multiplicity
- Missing points can lie at infinity.
  e.g. f and h in above example.
  Fix - Adding points at infinity : Projective Space

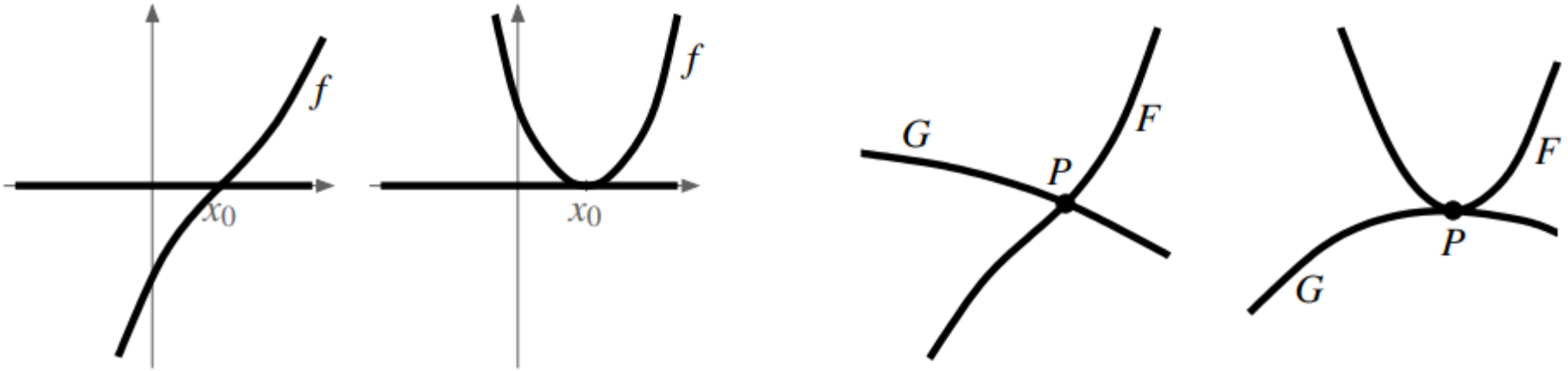
Bézouts theorem

Theorem

Let f and g be curves without common component over an algebraically closed field k. If we count the points at infinity and multiplicities of intersection points then total number of intersection points of f and g is $\deg f \cdot \deg g$.

Intersection Multiplicities

We have well-known notion of multiplicity of a zero of a univariate polynomial : If $f \in k[x]$ is a polynomial and $x_0 \in k$ such that $f = a(x - x_0)^m$ for a polynomial $a \in k[x]$ with $a(x_0) \neq 0$, then f is said to have multiplicity m at x_0.



multiplicity 1
$f = a(x - x_0)$

multiplicity 2
$f = a(x - x_0)^2$

multiplicity 1

multiplicity 2

This concept should also make sense for arbitrary curves f and g at an intersection point P: If they intersect transversely, i.e. with different tangent directions, we want to say that they have an intersection multiplicity of 1 at P, whereas equal tangents correspond to higher multiplicities.

Definition (Local ring of $\mathbb{A}^2$)

Let $P \in \mathbb{A}^2$ be a point. The local ring of $\mathbb{A}^2$ at P is defined as

$$\mathcal{O}_P := \left\{ \frac{f}{g} : f, g \in k[X,Y] \text{ with } g(P) \neq 0 \right\} \subset k(X,Y).$$

Definition (Local ring of $\mathbb{A}^2$)

Let $P \in \mathbb{A}^2$ be a point. The local ring of $\mathbb{A}^2$ at P is defined as

$$\mathcal{O}_P := \left\{ \frac{f}{g} : f, g \in k[X, Y] \text{ with } g(P) \neq 0 \right\} \subset k(X, Y).$$

Definition (Intersection multiplicities)

For a point $P \in \mathbb{A}^2$ and two curves (or polynomials) f and g we define the intersection multiplicity of f and g at P to be

$$I_P(f, g) := \dim_k \mathcal{O}_P/(f, g) \quad \in \mathbb{N} \cup \infty.$$

Some properties of Intersection multiplicities:

1. If T is the affine change of coordinates on $\mathbb{A}^2$ and $T(Q) = P$, then $I_P(f, g) = I_Q(f \circ T^{-1}, g \circ T^{-1})$

Some properties of Intersection multiplicities:

1. If T is the affine change of coordinates on $\mathbb{A}^2$ and $T(Q) = P$, then $I_P(f, g) = I_Q(f \circ T^{-1}, g \circ T^{-1})$
2. $I_P(f, g) = 0$ iff $P \notin f \cap g$.

Some properties of Intersection multiplicities:

1. If T is the affine change of coordinates on $\mathbb{A}^2$ and $T(Q) = P$, then $I_P(f,g) = I_Q(f \circ T^{-1}, g \circ T^{-1})$
2. $I_P(f,g) = 0$ iff $P \notin f \cap g$.
3. The intersection multiplicity is symmetric: We have $I_P(f,g) = I_P(g,f)$ for all f and g.

Some properties of Intersection multiplicities:

1. If T is the affine change of coordinates on $\mathbb{A}^2$ and $T(Q) = P$, then $I_P(f,g) = I_Q(f \circ T^{-1}, g \circ T^{-1})$
2. $I_P(f,g) = 0$ iff $P \notin f \cap g$.
3. The intersection multiplicity is symmetric: We have $I_P(f,g) = I_P(g,f)$ for all f and g.
4. For all f, g, h we have $(f, g + fh) = (f,g)$, and thus $I_P(f, g + fh) = I_P(f,g)$.

Some properties of Intersection multiplicities:

1. If T is the affine change of coordinates on $\mathbb{A}^2$ and $T(Q) = P$, then $I_P(f,g) = I_Q(f \circ T^{-1}, g \circ T^{-1})$
2. $I_P(f,g) = 0$ iff $P \notin f \cap g$.
3. The intersection multiplicity is symmetric: We have $I_P(f,g) = I_P(g,f)$ for all f and g.
4. For all f, g, h we have $(f, g + fh) = (f, g)$, and thus $I_P(f, g + fh) = I_P(f, g)$.
5. $I_P(f, gh) = I_P(f, g) + I_P(f, h)$ for all f, g, h.
   Consider the short exact sequence :

$$0 \to \mathcal{O}_P/(f,h) \xrightarrow{\times g} \mathcal{O}_P/(f,gh) \xrightarrow{\pi} \mathcal{O}_P/(f,g) \to 0$$

Lemma

If $f, g \in k[X, Y]$ be coprime and $P \in \mathbb{A}^2$ then $I_P(f, g) < \infty$.

Proof:

- First we observe that given finitely many elements of $\mathcal{O}_P$, we can write them with a common denominator.
- If the images of $\frac{u_1}{v}, \ldots, \frac{u_t}{v} \in \mathcal{O}_P$ are linearly independent in $\mathcal{O}_P/(f, g)$, then $u_1, \ldots, u_t$ are linearly independent in $k[X, Y]/(f, g)$ since $\frac{1}{v} \in \mathcal{O}_P$. So $\dim_k \mathcal{O}_P/(f, g) \leq \dim_k k[X, Y]/(f, g) \leq \deg f \cdot \deg g$ and hence finite.

Lemma

If $f, g \in k[X, Y]$ be coprime and $P \in \mathbb{A}^2$ then $I_P(f, g) < \infty$.

Proof:

- First we observe that given finitely many elements of $\mathcal{O}_P$, we can write them with a common denominator.
- If the images of $\frac{u_1}{v}, \ldots, \frac{u_t}{v} \in \mathcal{O}_P$ are linearly independent in $\mathcal{O}_P/(f, g)$, then $u_1, \ldots, u_t$ are linearly independent in $k[X, Y]/(f, g)$ since $\frac{1}{v} \in \mathcal{O}_P$. So $\dim_k \mathcal{O}_P/(f, g) \leq \dim_k k[X, Y]/(f, g) \leq \deg f \cdot \deg g$ and hence finite.

Lemma

If $f, g \in k[X, Y]$ be coprime and $P \in \mathbb{A}^2$ then every element in $\mathcal{O}_P/(f, g)$ has a polynomial representative.

Proof: If $\{\frac{\bar{u_1}}{v}, \ldots, \frac{\bar{u_t}}{v}\}$ be a basis of $\mathcal{O}_P/(f, g)$ where $u_i, v \in k[x, y]$ with $v(P) \neq 0$, then since $v \in \mathcal{O}_P$ is a unit, $\{\bar{u_1}, \ldots, \bar{u_t}\}$ is also a basis of $\mathcal{O}_P/(f, g)$. Thus every element in $\mathcal{O}_P/(f, g)$ has a polynomial representative.

Proposition (Bez2)

Let f and g be two affine curves over k with no common component then we have

$$\sum_P I_P(f,g) \leq \dim k[X,Y]/(f,g)$$

and equality holds if k is algebraically closed.

Proposition (Bez2)

Let f and g be two affine curves over k with no common component then we have

$$\sum_P I_P(f,g) \leq \dim k[X,Y]/(f,g)$$

and equality holds if k is algebraically closed.

Proof : $f \cap g$ is finite. Let $f \cap g = \{P_1, \ldots, P_r\}$. So we need to show

$$\sum_{i=1}^{r} I_{P_i}(f,g) \leq \dim k[X,Y]/(f,g)$$

We consider the natural homomorphism

$$\varphi : k[X,Y]/(f,g) \to \prod_{i=1}^{r} \mathcal{O}_{P_i}/(f,g)$$

that sends the class of a polynomial $h \in k[X,Y]$ to the class of $h \in \mathcal{O}_{P_i}$ in each factor $\mathcal{O}_{P_i}/(f,g)$. We show that φ is surjective, that proves the proposition.

In order to show surjectivity it suffices to find for any $i \in \{1, \ldots, r\}$ and arbitrary $z \in \mathcal{O}_{P_i}$ an element $h \in k[X, Y]$ such that $\bar{h}$ maps to the element $(0, \ldots, 0, \bar{z}, 0, \ldots, 0)$ with ith coordinate $\bar{z}$ and all other coordinates 0.

In order to show surjectivity it suffices to find for any $i \in \{1, \ldots, r\}$ and arbitrary $z \in \mathcal{O}_{P_i}$ an element $h \in k[X, Y]$ such that $\bar{h}$ maps to the element $(0, \ldots, 0, \bar{z}, 0, \ldots, 0)$ with ith coordinate $\bar{z}$ and all other coordinates 0.

- We can find polynomials $\{h_i\}_{i=1}^{r}$ in $k[X, Y]$ such that $h_i(P_i) = 1$ and $h_i(P_j) = 0$ for $j \neq i$.

In order to show surjectivity it suffices to find for any $i \in \{1, \ldots, r\}$ and arbitrary $z \in \mathcal{O}_{P_i}$ an element $h \in k[X, Y]$ such that $\bar{h}$ maps to the element $(0, \ldots, 0, \bar{z}, 0, \ldots, 0)$ with ith coordinate $\bar{z}$ and all other coordinates 0.

- We can find polynomials $\{h_i\}_{i=1}^{r}$ in $k[X, Y]$ such that $h_i(P_i) = 1$ and $h_i(P_j) = 0$ for $j \neq i$.
- If there is a natural number N such that $h_i^N \in (f, g)\mathcal{O}_{P_j}$ for all $j \neq i$, we pick a polynomial representative p of $(\frac{\bar{z}}{h_i^N}) \in \mathcal{O}_{P_i}/(f, g)$ (as we can by previous lemma).

In order to show surjectivity it suffices to find for any $i \in \{1, \ldots, r\}$ and arbitrary $z \in \mathcal{O}_{P_i}$ an element $h \in k[X, Y]$ such that $\bar{h}$ maps to the element $(0, \ldots, 0, \bar{z}, 0, \ldots, 0)$ with ith coordinate $\bar{z}$ and all other coordinates 0.

- We can find polynomials $\{h_i\}_{i=1}^{r}$ in $k[X, Y]$ such that $h_i(P_i) = 1$ and $h_i(P_j) = 0$ for $j \neq i$.
- If there is a natural number N such that $h_i^N \in (f, g)\mathcal{O}_{P_j}$ for all $j \neq i$, we pick a polynomial representative p of $(\frac{\bar{z}}{h_i^N}) \in \mathcal{O}_{P_i}/(f, g)$ (as we can by previous lemma).
- We take $h = ph_i^N$. This h clearly satisfies the requirement.

Remains to show the existence of N.

- Let $d_j := \dim_k \mathcal{O}_{P_j}/(f,g)$ and $N \geq d_j$ for all j. We show that $h_i^N \in (f,g)\mathcal{O}_{P_j}$ for all $j \neq i$.

- Let $d_j := \dim_k \mathcal{O}_{P_j}/(f,g)$ and $N \geq d_j$ for all j. We show that $h_i^N \in (f,g)\mathcal{O}_{P_j}$ for all $j \neq i$.
- Fix $j \neq i$ and $J_n := h_i^n \mathcal{O}_{P_j} + (f,g)\mathcal{O}_{P_j}$. Then $\{J_n\}_{n \geq 0}$ is a decreasing sequence of ideals.

- Let $d_j := \dim_k \mathcal{O}_{P_j}/(f,g)$ and $N \geq d_j$ for all j. We show that $h_i^N \in (f,g)\mathcal{O}_{P_j}$ for all $j \neq i$.
- Fix $j \neq i$ and $J_n := h_i^n \mathcal{O}_{P_j} + (f,g)\mathcal{O}_{P_j}$. Then $\{J_n\}_{n \geq 0}$ is a decreasing sequence of ideals.
- The sequence can have at most $d_j + 1$ different members. So there is an n_j with $0 \leq n_j \leq d_j$ such that $J_{n_j} = J_{n_j+1}$.

- Let $d_j := \dim_k \mathcal{O}_{P_j}/(f,g)$ and $N \geq d_j$ for all j. We show that $h_i^N \in (f,g)\mathcal{O}_{P_j}$ for all $j \neq i$.
- Fix $j \neq i$ and $J_n := h_i^n \mathcal{O}_{P_j} + (f,g)\mathcal{O}_{P_j}$. Then $\{J_n\}_{n \geq 0}$ is a decreasing sequence of ideals.
- The sequence can have at most $d_j + 1$ different members. So there is an n_j with $0 \leq n_j \leq d_j$ such that $J_{n_j} = J_{n_j+1}$.
- This means that $h_i^{n_j} = h_i^{n_j+1} u + v$ for some $u \in \mathcal{O}_{P_j}$ and $v \in (f,g)\mathcal{O}_{P_j}$. Since $1 - uh_i$ has value 1 at P_j so $1 - uh_i$ is a unit in $\mathcal{O}_{P_j}$ and hence $\frac{1}{1-h_i u} \in \mathcal{O}_{P_j}$, it follows that $h_i^{n_j} = \frac{v}{1-h_i u} \in (f,g)\mathcal{O}_{P_j}$.

- Let $d_j := \dim_k \mathcal{O}_{P_j}/(f,g)$ and $N \geq d_j$ for all j. We show that $h_i^N \in (f,g)\mathcal{O}_{P_j}$ for all $j \neq i$.
- Fix $j \neq i$ and $J_n := h_i^n \mathcal{O}_{P_j} + (f,g)\mathcal{O}_{P_j}$. Then $\{J_n\}_{n \geq 0}$ is a decreasing sequence of ideals.
- The sequence can have at most $d_j + 1$ different members. So there is an n_j with $0 \leq n_j \leq d_j$ such that $J_{n_j} = J_{n_j+1}$.
- This means that $h_i^{n_j} = h_i^{n_j+1} u + v$ for some $u \in \mathcal{O}_{P_j}$ and $v \in (f,g)\mathcal{O}_{P_j}$. Since $1 - uh_i$ has value 1 at P_j so $1 - uh_i$ is a unit in $\mathcal{O}_{P_j}$ and hence $\frac{1}{1-h_i u} \in \mathcal{O}_{P_j}$, it follows that $h_i^{n_j} = \frac{v}{1-h_i u} \in (f,g)\mathcal{O}_{P_j}$.
- Since $N \geq n_j$ for all j, so $h_i^N \in \mathcal{O}_{P_j}$ for all $j \neq i$.

For k algebraically closed, we need to show that φ is injective. Let $h \in \ker \varphi$.

- Consider the set $I := \{p \in k[X,Y] \quad | \quad ph \in (f,g)\}$. This is clearly an ideal containg (f,g). We claim $V(I) = \phi$.

For k algebraically closed, we need to show that φ is injective. Let $h \in \ker \varphi$.

- Consider the set $I := \{p \in k[X,Y] \quad | \quad ph \in (f,g)\}$. This is clearly an ideal containg (f,g). We claim $V(I) = \phi$.
- If not, say $P \in V(I)$. Since $f, g \in I$, so $P \in f \cap g$. So $P = P_i$ for some i.

For k algebraically closed, we need to show that φ is injective. Let $h \in \ker \varphi$.

- Consider the set $I := \{p \in k[X,Y] \quad | \quad ph \in (f,g)\}$. This is clearly an ideal containg (f,g). We claim $V(I) = \phi$.
- If not, say $P \in V(I)$. Since $f, g \in I$, so $P \in f \cap g$. So $P = P_i$ for some i.
- Since $\varphi(h) = 0$, so $\bar{h} = 0 \in \mathcal{O}_{P_i}/(f,g)$. So $h = \frac{a}{u}f + \frac{b}{u}g$ for some $a, b, u \in k[X,Y]$ with $u(P_i) \neq 0$. But then $uh = af + bg \in (f,g)$, hence $u \in I$, and since $P_i = P \in V(I)$ we arrive at the contradiction that $u(P_i) = 0$. So we conclude that $V(I) = \phi$.

For k algebraically closed, we need to show that φ is injective. Let $h \in \ker \varphi$.

- Consider the set $I := \{p \in k[X,Y] \quad | \quad ph \in (f,g)\}$. This is clearly an ideal containg (f,g). We claim $V(I) = \phi$.
- If not, say $P \in V(I)$. Since $f, g \in I$, so $P \in f \cap g$. So $P = P_i$ for some i.
- Since $\varphi(h) = 0$, so $\bar{h} = 0 \in \mathcal{O}_{P_i}/(f,g)$. So $h = \frac{a}{u}f + \frac{b}{u}g$ for some $a, b, u \in k[X,Y]$ with $u(P_i) \neq 0$. But then $uh = af + bg \in (f,g)$, hence $u \in I$, and since $P_i = P \in V(I)$ we arrive at the contradiction that $u(P_i) = 0$. So we conclude that $V(I) = \phi$.
- Since k is algebraically closed, by Hilbert Nullstellensatz we have $1 \in I$ and hence $h \in (f,g)$ and thus $\bar{h} = 0 \in k[X,Y]/(f,g)$.

Hence φ is an isomorphism for k algebraically closed.

Examples

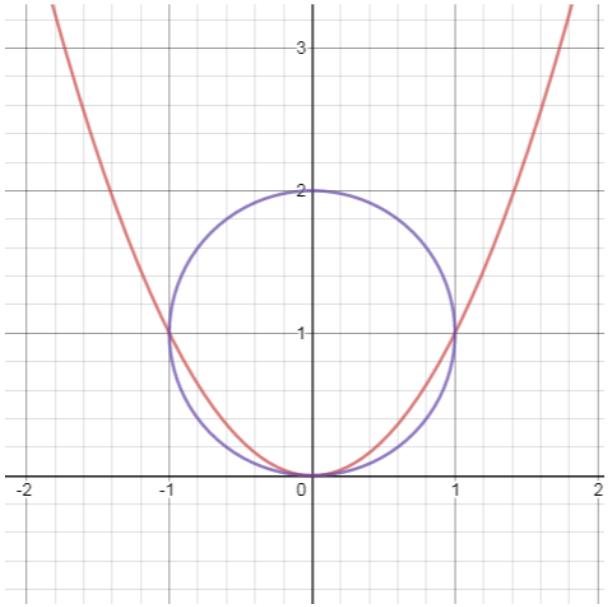
We take $f(X,Y) = X^2 - Y$ and $g(X,Y) = X^2 + (Y-1)^2 - 1$ over $\mathbb{R}$.

$f \cap g = \{(-1,1),(0,0),(1,1)\}$

Examples

We take $f(X,Y) = X^2 - Y$ and $g(X,Y) = X^2 + (Y-1)^2 - 1$ over $\mathbb{R}$.
$f \cap g = \{(-1,1),(0,0),(1,1)\}$

$$
\begin{aligned}
& I_{(0,0)}(f,g) \\
&= I_{(0,0)}(Y - X^2, X^2 + (Y-1)^2 - 1) \\
&= I_{(0,0)}(Y - X^2, X^2 + (Y-1)^2 - 1 + Y - X^2) \\
&= I_{(0,0)}(Y - X^2, Y^2 - Y) \\
&= I_{(0,0)}(Y - X^2, Y) + I_{(0,0)}(Y - X^2, Y - 1) \\
&= I_{(0,0)}(X^2, Y) + 0 \\
&= 2I_{(0,0)}(X,Y) = 2
\end{aligned}
$$



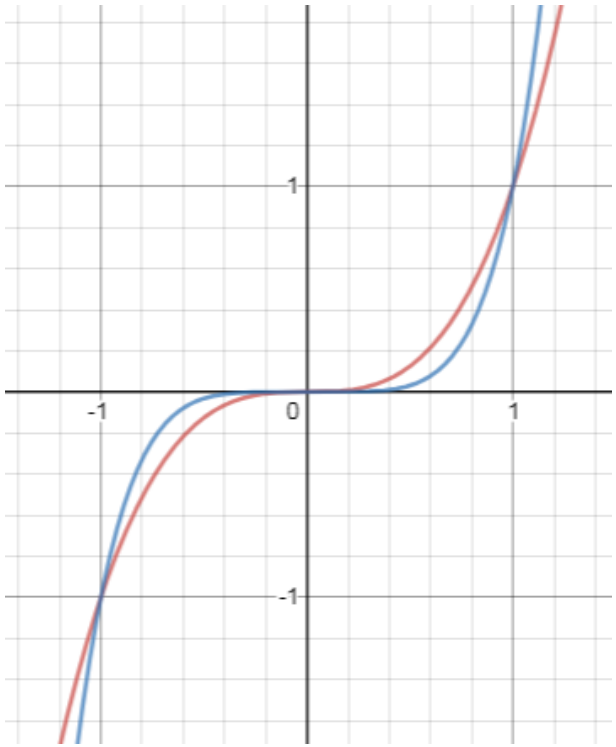
$I_{(1,1)}(f,g) = 1$ and $I_{(-1,1)}(f,g) = 1$.
So $\sum_P I_P(f,g) = 2 + 1 + 1 = 4 = \dim_{\mathbb{R}} \mathbb{R}[X,Y]/(f,g) = \deg f \cdot \deg g$

Examples

We take $f(X,Y) = Y - X^3$ and $g(X,Y) = Y - X^5$ over $\mathbb{C}$.

$f \cap g = \{(-1,-1),(0,0),(1,1)\}$

$$
\begin{aligned}
& I_{(0,0)}(f,g) \\
&= I_{(0,0)}(Y - X^3, Y - X^5) \\
&= I_{(0,0)}(Y - X^3, X^3 - X^5) \\
&= I_{(0,0)}(Y - X^3, X^3) + I_{(0,0)}(Y - X^3, 1 - X^2) \\
&= I_{(0,0)}(Y, X^3) + 0 \\
&= 3I_{(0,0)}(X,Y) = 3
\end{aligned}
$$



$I_{(1,1)}(f,g) = 1$ and $I_{(-1,-1)}(f,g) = 1$.

So $\sum_P I_P(f,g) = 3 + 1 + 1 = 5 = \dim_{\mathbb{C}} \mathbb{C}[X,Y]/(f,g) < \deg f \cdot \deg g$

Adding points at infninity

Consider the simplest case : f and g are two distinct lines this since f and g might intersect in one point or be parallel and hence have no intersection point.

Adding points at infninity

Consider the simplest case : f and g are two distinct lines this since f and g might intersect in one point or be parallel and hence have no intersection point.

- Add points at infinity to the affine plane $\mathbb{A}^2$, so that two parallen lines in $\mathbb{A}^2$ will meet there.

Adding points at infninity

Consider the simplest case : f and g are two distinct lines this since f and g might intersect in one point or be parallel and hence have no intersection point.

- Add points at infinity to the affine plane $\mathbb{A}^2$, so that two parallen lines in $\mathbb{A}^2$ will meet there.
- Two non-parallel lines (that intersect already in $\mathbb{A}^2$) should not meet at infinity any more as this would then lead to two intersection points.

Adding points at infninity

Consider the simplest case : f and g are two distinct lines this since f and g might intersect in one point or be parallel and hence have no intersection point.

- Add points at infinity to the affine plane $\mathbb{A}^2$, so that two parallen lines in $\mathbb{A}^2$ will meet there.
- Two non-parallel lines (that intersect already in $\mathbb{A}^2$) should not meet at infinity any more as this would then lead to two intersection points.

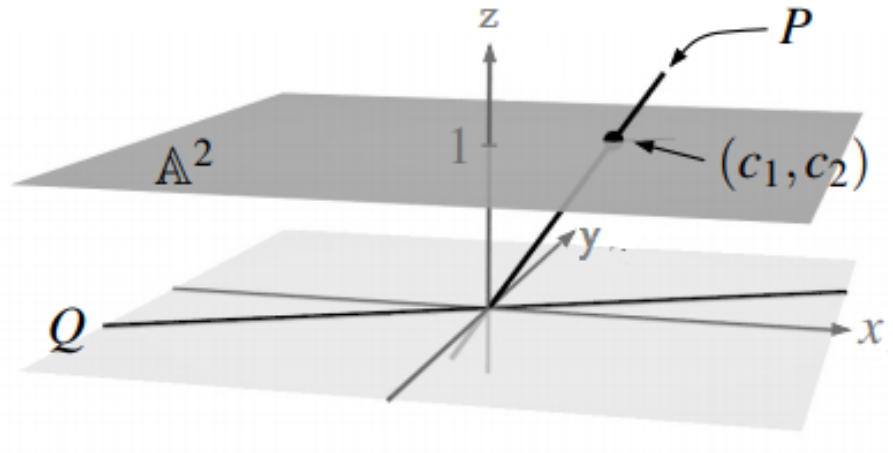
Hence, we have to add one point at infinity for each direction in the affine plane, so that parallel lines with the same direction meet there, whereas others do not. This new space with the added points at infinity will be called the projective plane.

Definition

We define a relation on $k^{n+1} \setminus ¶(0,\ldots,0)\}$ by, given $x = (x_0, x_1, \ldots, x_n), y = (y_0, \ldots, y_n) \in k^{n+1} \setminus \{(0,\ldots,0)\}$, we say $x \sim y$ iff $(x_0, x_1, \ldots, x_n) = (\lambda y_0, \ldots, \lambda y_n)$ for some $\lambda \in k^*$. Clearly $\sim$ is an equivalence relation, and we call the set of equivalence classes of $\sim$ Projective n-space, which we denote by,

$$\mathbb{P}^n = (k^{n+1} \setminus \{(0,\ldots,0)\})/\sim .$$

The equivalent class of $(a_0, \ldots, a_n)$ is denoted by $[a_0 : \cdots : a_n]$, called the homogenous coordinates of the points in $\mathbb{P}^n$.



We embed affine space in projective space by the map

$$\mathbb{A}^n \hookrightarrow \mathbb{P}^n, \quad (a_0, \ldots, a_{n-1}) \mapsto [a_0 : \cdots : a_{n-1} : 1]$$

with image is the subset $U_0 = \{[x_0 : x_1 : \cdots : x_n] : x_n \neq 0\}$ of $\mathbb{P}^n$. We call these points *Affine points* of $\mathbb{P}^n$.
The remaining points of $\mathbb{P}^n$ are of the form $[x_0 : \cdots : x_{n-1} : 0]$, we can regard them as *points at infinity*.

Projective varieties

Definition

A polynomial in $k[X_1, X_2, \ldots, X_n]$ is called homogenous of degree r or simply homogenous if all of its terms are of degree r.

For example, $X^2 + XY$ and $XY + YZ$ are homogenous of degree 2, but $X^2Y + XY$ and $X + 3$ are not.

Projective varieties

Definition

A polynomial in $k[X_1, X_2, \ldots, X_n]$ is called homogenous of degree r or simply homogenous if all of its terms are of degree r.

For example, $X^2 + XY$ and $XY + YZ$ are homogenous of degree 2, but $X^2Y + XY$ and $X + 3$ are not. If $f \in k[x_0, \ldots, k_n]$ be homogenous,

- $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ for all $\lambda \in k^*$.
- For $P = [x_0, \ldots, x_n] \in \mathbb{P}^n$, we define $f(P) = 0$ if $f(x_0, \ldots, x_n) = 0$.

Projective varieties

Definition

A polynomial in $k[X_1, X_2, \ldots, X_n]$ is called homogenous of degree r or simply homogenous if all of its terms are of degree r.

For example, $X^2 + XY$ and $XY + YZ$ are homogenous of degree 2, but $X^2Y + XY$ and $X + 3$ are not. If $f \in k[x_0, \ldots, k_n]$ be homogenous,

- $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ for all $\lambda \in k^*$.
- For $P = [x_0, \ldots, x_n] \in \mathbb{P}^n$, we define $f(P) = 0$ if $f(x_0, \ldots, x_n) = 0$.

Definition (Projective varieties)

For a subset $S \in k[X_0, \ldots, X_n]$ of homogenous polynomials we call

$$V_p(S) := \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all } f \in S\} \subset \mathbb{P}^n$$

the projective zero locus of S.

Projective curve

Definition

$\mathbb{P}^2_k$ is called the projective plane over k.

Definition

A projective plane curve over k is projective zero locus of a non-constant homogeneous polynomial $f \in k[x, y, z]$ (modulo units).

- For a polynomial $f = \sum_{i+j \leq d} a_{ij} X^i Y^j \in k[X, Y]$ of degree d we define the **homogenization** of f as

$$f^h(X, Y, Z) := \sum_{i+j \leq d} a_{ij} X^i Y^j Z^{d-i-j} \in k[X, Y, Z].$$

- For a polynomial $f = \sum_{i+j \leq d} a_{ij} X^i Y^j \in k[X, Y]$ of degree d we define the **homogenization** of f as

$$f^h(X, Y, Z) := \sum_{i+j \leq d} a_{ij} X^i Y^j Z^{d-i-j} \in k[X, Y, Z].$$

- For a homogeneous polynomial $f \in k[X, Y, Z]$, we define the **dehomogenization** of f as

$$f^i(X, Y) := f(X, Y, 1).$$

- For a polynomial $f = \sum_{i+j \leq d} a_{ij} X^i Y^j \in k[X, Y]$ of degree d we define the **homogenization** of f as

$$f^h(X, Y, Z) := \sum_{i+j \leq d} a_{ij} X^i Y^j Z^{d-i-j} \in k[X, Y, Z].$$

- For a homogeneous polynomial $f \in k[X, Y, Z]$, we define the **dehomogenization** of f as

$$f^i(X, Y) := f(X, Y, 1).$$

- For a projective curve f, its affine points are $V_p(f) \cap \mathbb{A}^2 = V(f^i)$. The points at infinity of f are given by $V_p(f(X, Y, 0))$.
- Line at infinity is a component of f iff $Z | f$.

- For a polynomial $f = \sum_{i+j \leq d} a_{ij} X^i Y^j \in k[X, Y]$ of degree d we define the **homogenization** of f as

$$f^h(X, Y, Z) := \sum_{i+j \leq d} a_{ij} X^i Y^j Z^{d-i-j} \in k[X, Y, Z].$$

- For a homogeneous polynomial $f \in k[X, Y, Z]$, we define the **dehomogenization** of f as

$$f^i(X, Y) := f(X, Y, 1).$$

- For a projective curve f, its affine points are $V_p(f) \cap \mathbb{A}^2 = V(f^i)$. The points at infinity of f are given by $V_p(f(X, Y, 0))$.
- Line at infinity is a component of f iff $Z | f$.
- For $f \in k[X, Y]$ define $f_*(X, Y) = f^h(X, Y, 0) \in k[X, Y]$. Observe that f_* is the leading term of f.

Proposition (Bez3)

Let f and g be two affine curves over k of degree m and n with no common component, such that their leading terms f_* and g_* have no common component. Then

$$\dim_k k[X,Y]/(f,g) = mn.$$

Proposition (Bez3)

Let f and g be two affine curves over k of degree m and n with no common component, such that their leading terms f_* and g_* have no common component. Then

$$\dim_k k[X,Y]/(f,g) = mn.$$

Proof : It suffices to establish equality in this lemma and for that we need $\ker \pi \subset \operatorname{im} \alpha$ for large enough d.

Proposition (Bez3)

Let f and g be two affine curves over k of degree m and n with no common component, such that their leading terms f_* and g_* have no common component. Then

$$\dim_k k[X,Y]/(f,g) = mn.$$

Proof : It suffices to establish equality in this lemma and for that we need $\ker \pi \subset \operatorname{im} \alpha$ for large enough d.

- So let $h \in k[x,y]$ is of degree d and $\bar{h} = 0 \in R_d/(f,g)$. We write $h = af + bg$ with $a, b \in k[X,Y]$ of smallest degree. We need to show $\deg a \leq d - m$ and $\deg b \leq d - n$.

Proposition (Bez3)

Let f and g be two affine curves over k of degree m and n with no common component, such that their leading terms f_* and g_* have no common component. Then

$$\dim_k k[X,Y]/(f,g) = mn.$$

Proof : It suffices to establish equality in ⏩ this lemma and for that we need $\ker \pi \subset \operatorname{im} \alpha$ for large enough d.

- So let $h \in k[x,y]$ is of degree d and $\bar{h} = 0 \in R_d/(f,g)$. We write $h = af + bg$ with $a, b \in k[X,Y]$ of smallest degree. We need to show $\deg a \leq d - m$ and $\deg b \leq d - n$.
- Assume for a contradiction that $\deg a > d - m$ or $\deg b > d - n$. Then af of bg contains terms of degree bigger that d. As $\deg h = d$, the leading terms of af and bg must cancel when added i.e. $a_* f_* = -b_* g_*$. Using $(f_*, g_*) = 1$ we have $a_* = cg_*$ and $b_* = -cf_*$ for some polynmial $c \in k[X,Y]$. This gives us a new representation $h = (a - cg)f + (b + cf)g$ in which $\deg(a - cg) < \deg a$, contradicting the minimality of $\deg a$.

Definition (Local rings of $\mathbb{P}^2$)

For $P \in \mathbb{P}^2$ we define the local ring of $\mathbb{P}^2$ at P as

$$\mathcal{O}_P := \left\{ \frac{f}{g} : f, g \in k[X, Y, Z] \text{ homogenous of the same degree with } g(P) \neq 0 \right\}$$

For a point $P = (a, b, 1)$ in the affine part of $\mathbb{P}^2$ it is easily checked that there is an isomorphism

$$\mathcal{O}_P \to \mathcal{O}_P \quad \text{given by} \quad \frac{f}{g} \mapsto \frac{f^i}{g^i}$$

Definition (Intersection multiplicities)

As in the affine case we can define the intersection multiplicity of two curves f, g at a point $P \in \mathbb{P}^2$ as

$$\mu_P(f,g) := \dim_k \mathscr{O}_P/(f,g) \quad \in \mathbb{N} \cup \infty.$$

For a point $P = (a,b,1)$ in the affine part of $\mathbb{P}^2$ one can verify directly that the isomorphism $\mathscr{O}_P \cong \mathcal{O}_P$ constructed above takes (f,g) to (f^i, g^i). Hence we have $\mu_{(a,b,1)}(f,g) = I_{(a,b,1)}(f^i, g^i)$.

Moreover, in the same way as in affine case intersection multiplicities are invariant under projective coordinate transformation and they satisfy all the other properties of the multiplicities in affine case.

Example revisited

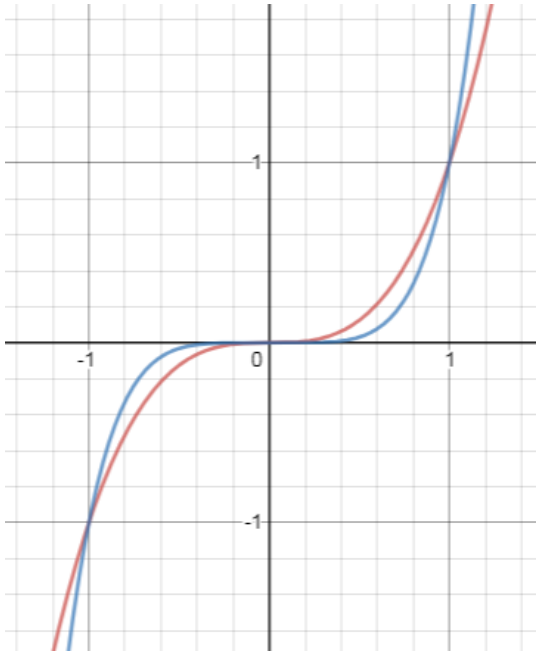
We take $f(X,Y) = Y - X^3$ and $g(X,Y) = Y - X^5$ over $\mathbb{C}$. So

$f^h(X,Y,Z) = YZ^2 - X^3$ and $g(X,Y,Z) = YZ^4 - X^5$

$f^h \cap g^h = \{(-1,-1,1),(0,0,1),(1,1,1),(0,1,0)\}$

$\mu_{(1,1,1)}(f^h,g^h) = 1$ and $\mu_{(-1,-1,1)}(f^h,g^h) = 1$ and $\mu_{(0,0,1)}(f^h,g^h) = 3$

$$
\begin{aligned}
&\mu_{(0,1,0)}(f^h,g^h) \\
&= I_{(0,0)}(f^h(X,1,Z), g^h(X,1,Z)) \\
&= I_{(0,0)}(Z^2 - X^3, Z^4 - X^5) \\
&= I_{(0,0)}(Z^2 - X^3, X^3Z^2 - X^5) \\
&= I_{(0,0)}(Z^2, X^3) + I_{(0,0)}(X^2, Z^3) \\
&= 10 I_{(0,0)}(X,Z) = 10
\end{aligned}
$$



So $\sum_P \mu_P(f^h,g^h) = 15 = \dim_{\mathbb{C}} \mathbb{C}[X,Y]/(f,g) = \deg f \cdot \deg g$

Bézouts theorem

We can now prove the main result.

Theorem (Bézouts theorem)

Let f and g be projective curves without common component over an algebraically closed field k. Then

$$\sum_{P \in f \cap g} \mu_P(f, g) = \deg f \cdot \deg g.$$

Proof.

As k is infinite but $f \cap g$ is finite, we can pick a line L which does not intersect $f \cap g$. Now we can make a projective coordinate transformation so that L becomes the line at infinity. Then neither f nor g contains the line at infnity as a component. So $\deg f = \deg f^i$ and $\deg g = \deg g^i$ and all intersection point of f and g lies in the affine part i.e. $f \cap g = f^i \cap g^i$. So applying proposition Bez2 and Bez3 we get,

$$\begin{aligned}
\sum_{P \in f \cap g} \mu_P(f, g) &= \sum_{P \in f \cap g} I_P(f^i, g^i) \\
&\overset{\text{Bez2}}{=\!=} \dim_k k[X, Y]/(f^i, g^i) \\
&\overset{\text{Bez3}}{=\!=} \deg f^i \cdot \deg g^i \\
&= \deg f \cdot \deg g
\end{aligned}$$



Thank you!

References


WILLIAM FULTON, *ALGEBRAIC CURVES: An Introduction to Algebraic Geometry*, January 28, 2008.


Andreas Gathmann, *Plane Algebraic Curves*, Class Notes TU Kaiserslautern 2018