Bézout's Theorem: A Tale of Two Curves

Peter Goetz

Math Mondays
Saint Mary's College of California

April 13, 2015

Outline

1) Introduction
2) Complex Solutions
3) The Projective Plane
4) Intersection Number
5) Bézout's Theorem

$f(x, y)$, a polynomial over the complex numbers, $\mathbb{C}$

Ex. $f(x, y) = 1 + x + iy^2 - x^2 - x^3y$, $\deg(f(x, y)) = 4$

$f(x, y)$ determines a complex-valued function on the complex plane, $\mathbb{C}^2$

An **affine algebraic curve**, C, is the zero set of some $f(x, y)$, i.e.,

$$C = \{(a, b) \in \mathbb{C}^2 \mid f(a, b) = 0\}.$$

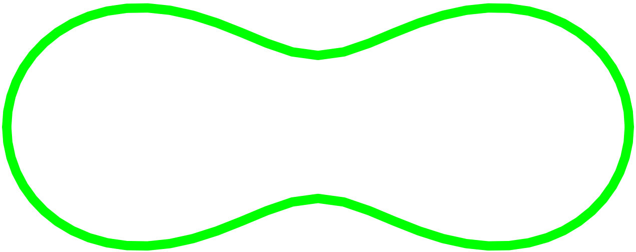
Define **degree of** C to be $\deg(f(x, y))$.

Folium of Descartes

Ex. $x^3 + y^3 - 6xy$, degree: 3

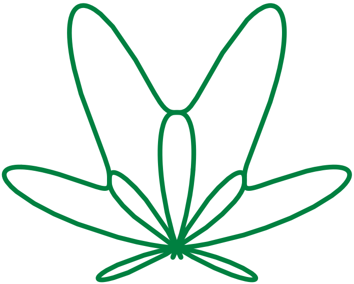
Oval of Cassini

Ex. : $(x^2 + y^2 + 9)^2 - 36x^2 - 100$, degree: 4



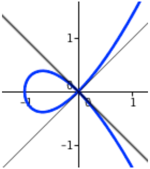
Frog Curve

Ex. $r - \sin\theta - \sin^3 4\theta$, degree: 26



Multiplicity of p

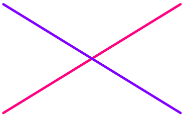
$p = (0, 0)$
Write $f = f_m + f_{m+1} + \cdots + f_k$, where f_i is **homogeneous** of degree i, $f_m \neq 0$.
The **multiplicity of** p **on** f, $m_p(f)$, is defined to be m.
The **tangent lines at** p are determined by the linear factors of f_m.
Ex. Nodal cubic: $y^2 - x^2 - x^3$



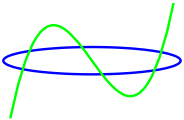
Two Curves

Problem: Given two algebraic curves C and D, count the number of points in $C \cap D$.

Ex. Two lines: $1 = 1 \cdot 1$



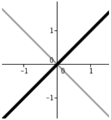
Ex. Ellipse and Cubic: $6 = 2 \cdot 3$



Elegant Guess: Suppose $\deg(C) = m$, $\deg(D) = n$. Then $|C \cap D| = mn$.

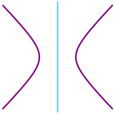
Examples

Ex. $y^2 - x^2$, $y - x$, $\infty \neq 2 \cdot 1$



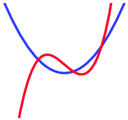
From now on, assume that C and D have no common components.

Ex. Line and Hyperbola: $0 \neq 1 \cdot 2$

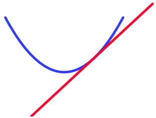


Examples

Ex. Parabola and Cubic: $3 \neq 2 \cdot 3$

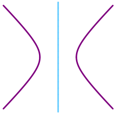


Ex. Parabola and Tangent Line: $1 \neq 2 \cdot 1$



Complex Solutions

Ex. $x^2 - y^2 = 1$, $x = 0$.

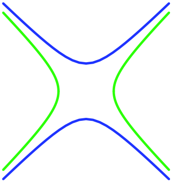


Substituting $x = 0$ yields $y^2 = -1$, so we get two *complex* points: $(0, \pm i)$.

Therefore we should count points in $\mathbb{C}^2$, and remember that we can draw pictures in $\mathbb{R}^2$.

Points at Infinity?

Ex. Two Hyperbolas: $x^2 - y^2 = 1$, $y^2 - x^2 = 1$



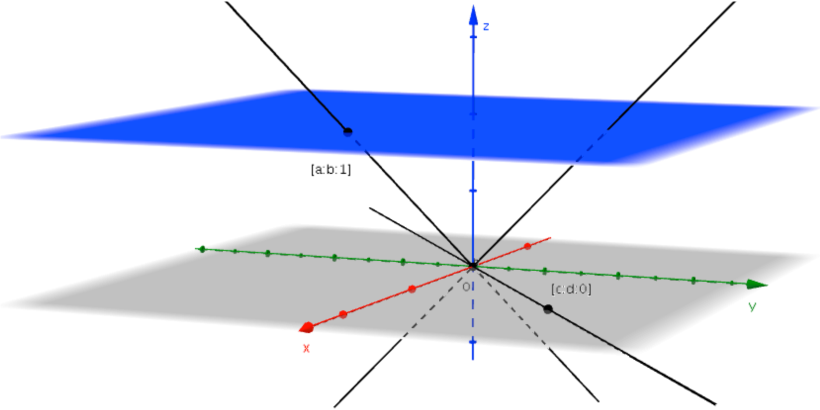
It is easy to check that there are no complex points on both hyperbolas.

Where might we find four points?

Idea: Enlarge the plane and add "points at ∞" corresponding to directions.

The Complex Projective Plane

Let $\mathbb{P}^2$ denote the set of all lines through the origin in $\mathbb{C}^3$.



Homogeneous Coordinates

A point $(a, b, c) \neq (0, 0, 0)$ in $\mathbb{C}^3$ determines a unique line through the origin.

(a, b, c), (a', b', c'), determine the same line if and only if there is some $0 \neq \lambda \in \mathbb{C}$ such that $(a, b, c) = \lambda(a', b', c')$.

Write $[a : b : c]$ for the equivalence class of (a, b, c).

$$\begin{aligned} \mathbb{P}^2 &= \left\{[a : b : c] \mid (0,0,0) \neq (a,b,c) \in \mathbb{C}^3\right\} \\ &= \mathbb{C}^2 \cup \mathbb{P}^1, \text{ where} \end{aligned}$$

$$\mathbb{C}^2 \leftrightarrow \{[a : b : 1] \mid a, b \in \mathbb{C}\}$$

$$\mathbb{P}^1 \leftrightarrow \{[a : b : 0] \mid a, b \in \mathbb{C}, \text{ not both zero}\}$$

Homogenous Polynomials on $\mathbb{P}^2$

In general, a polynomial $f(x, y, z)$ will not define a function on $\mathbb{P}^2$:

$$f(x, y, z) = x^2 - y + z; f([1 : 1 : 1]) = 1, f([2 : 2 : 2]) = 4.$$

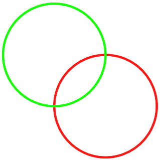
However, if $F(x, y, z)$ is **homogenous** of degree d (all terms in F have degree d) and $F([a : b : c]) = 0$, then

$$F([\lambda a : \lambda b : \lambda c]) = \lambda^d F([a : b : c]) = 0.$$

A **projective plane curve** is the zero set of a *homogeneous* polynomial $F(x, y, z)$.

Two Circles

Ex. $C : (x - \frac{1}{2})^2 + y^2 = \frac{1}{4}$; $D : x^2 + (y - \frac{1}{2})^2 = \frac{1}{4}$.



Visually, there are two points of intersection in $\mathbb{C}^2$.

Homogenize:

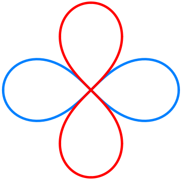
$C^* : (x - \frac{1}{2}z)^2 + y^2 = \frac{1}{4}z^2$
$D^* : x^2 + (y - \frac{1}{2}z)^2 = \frac{1}{4}z^2$

$z = 0 \Rightarrow x^2 + y^2 = 0$, yielding two intersection points $[1 : \pm i : 0]$

$4 = 2 \cdot 2$

Lemniscates of Bernoulli

Ex. $C : (x^2 + y^2)^2 + y^2 - x^2 = 0$; $D : (x^2 + y^2)^2 + x^2 - y^2 = 0$



The only complex point of intersection is $(0, 0)$.

There are only two points at ∞, namely $[1 : \pm i : 0]$.

Now $4 \cdot 4 = 16$, so we would like to count sixteen points of intersection.

Somehow, we have to count the **multiplicities** of the intersection points.

Axioms for Intersection Number

Let $p \in \mathbb{C}^2$, and let C and D be affine plane curves.

Axioms:

1. $I(p, C \cap D)$ is a nonnegative integer or ∞.
2. $I(p, C \cap D) = 0$ if and only if $p \notin C \cap D$.
3. If $p = T(q)$ for some affine transformation T, then $I(p, C \cap D) = I(q, C^T \cap D^T)$.
4. $I(p, C \cap D) = I(p, D \cap C)$.
5. $I(p, C \cap D) \geq m_p(C)m_p(D)$, with equality if and only if C and D have no common tangent lines at p.
6. If $C = C_1C_2$, then $I(p, C \cap D) = I(p, C_1 \cap D) + I(p, C_2 \cap D)$.
7. $I(p, C \cap D) = I(p, C \cap (D + AC))$ for any polynomial $A(x, y)$.

Existence and Uniqueness of $I(p, C \cap D)$

It is not too hard to show that if $I(p, C \cap D)$ exists, then it is unique.

In fact, assuming $I(p, C \cap D)$ exists, there is an inductive proof showing that there is a finite algorithm for computing $I(p, C \cap D)$.

The hard part is to prove that $I(p, C \cap D)$ exists.

Next, we are going to show that algebra gives a way to rigorously define $I(p, C \cap D)$. Then it can be proved that our definition satisfies the seven axioms.

Algebra-Geometry Correspondence

Recall the set of polynomials, $R = \mathbb{C}[x, y]$, is a commutative ring (also a vector space over $\mathbb{C}$).

For a subset $I \subseteq \mathbb{C}[x, y]$, let

$$V(I) = \{(a, b) \in \mathbb{C}^2 \mid f(a, b) = 0 \text{ for every } f(x, y) \in I\}.$$

For a subset $X \subseteq \mathbb{C}^2$, let

$$I(X) = \{f(x, y) \in R \mid f(a, b) = 0 \text{ for every } (a, b) \in X\}.$$

Hilbert's Nullstellensatz:

$$\Big\{\text{algebraic sets, } V(I)\Big\} \rightleftarrows \Big\{\text{radical ideals, } \sqrt{I}\Big\}.$$

The collection of all algebraic sets form the closed sets of a topology on $\mathbb{C}^2$ called the **Zariski topology**.

Rings of Functions on Algebraic Sets

Let $X = V(I)$ be an algebraic set. The **coordinate ring of** X is the quotient ring $\mathbb{C}[x, y]/I(X)$.

We should think of $\mathbb{C}[x, y]/I(X)$ as the ring of polynomial functions defined on X.

Ex. $C = V(y - x^2)$, coordinate ring: $\mathbb{C}[x, y]/(y - x^2)$. Note that y and x^2 are the same function if we restrict their domains to C.

Local Properties

We want to study local properties: $m_p(C)$ or $I(p, C \cap D)$, of a curve or curves at a point p.

The right things to consider are the rational functions on the curve which are defined at p.

We get **local rings:** $\mathcal{O}_p(C)$. Local rings have a unique maximal ideal; in this case, that maximal ideal is denoted by $\mathfrak{m}_p(C)$.

Theorem: Let p be a point on an irreducible curve C. Then for all sufficiently large n,

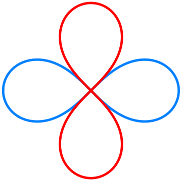
$$m_p(C) = \dim(\mathfrak{m}_p(C)^n / \mathfrak{m}_p(C)^{n+1}).$$

Define $I(p, C \cap D) = \dim(\mathcal{O}_p(\mathbb{C}^2)/(C, D))$.

Theorem: With this definition, $I(p, C \cap D)$ satisfies axioms (1)-(7) for an intersection number.

Lemniscates of Bernoulli

Ex. $C : (x^2 + y^2)^2 + y^2 - x^2$; $D : (x^2 + y^2)^2 + x^2 - y^2$



Points of Intersection in $\mathbb{P}^2$:

$p = (0, 0) \leftrightarrow [0 : 0 : 1]$, $q_1 = [1 : i : 0]$, $q_2 = [1 : -i : 0]$

$$I(p, C \cap D) + I(q_1, C \cap D) + I(q_2, C \cap D) = 16?$$

$I(p, C \cap D)$

$C : (x^2 + y^2)^2 + y^2 - x^2$; $D : (x^2 + y^2)^2 + x^2 - y^2$

$C + D = 2(x^2 + y^2)^2$, so $m_p(C + D) = 4$,
tangent lines at p: $y = \pm ix$.

$m_p(C) = 2$, tangent lines at p: $y = \pm x$

Then

$$\begin{aligned} I(p, C \cap D) &= I(C \cap (C + D)) && \text{by (7)} \\ &= m_p(C) m_p(C + D) && \text{by (5)} \\ &= 4 \cdot 2 = 8. \end{aligned}$$

$I(q_{\{1,2\}}, C \cap D)$

$C^* : (x^2+y^2)^2 + (y^2-x^2)z^2$; $D^* : (x^2+y^2)^2 + (x^2-y^2)z^2$
Set $x = 1$:
$C^*(1,y,z) = (1+y^2)^2 + (y^2-1)z^2$,
$D^*(1,y,z) = (1+y^2)^2 + (1-y^2)z^2$
Translate $(i,0)$ to the origin by the substitutions: $y \mapsto y - i$, $z \mapsto z$.
$C' : y^4 + y^2z^2 - 4iy^3 - 2iyz^2 - 2(2y^2+z^2)$,
$D' : y^4 - y^2z^2 - 4iy^3 + 2iyz^2 - 2(2y^2-z^2)$
Then

$$\begin{aligned} I(q_1, C \cap D) &= I((0,0), C' \cap D') && \text{by (3)} \\ &= m_{(0,0)}(C')m_{(0,0)}(D') && \text{by (5)} \\ &= 2 \cdot 2 = 4. \end{aligned}$$

By symmetry, $I(q_2, C \cap D) = 4$.
Therefore,

$$I(p, C \cap D) + I(q_1, C \cap D) + I(q_2, C \cap D) = 8 + 4 + 4 = 16.$$

Bézout's Theorem

Bézout's Theorem: Let C and D be projective plane curves of degrees m and n respectively. Suppose that C and D have no common components. Then

$$\sum_{p \in C \cap D} I(p, C \cap D) = mn.$$

History

Isaac Newton in his Principia, Book I, Lemma 28:

"*Hence it is that the intersections of the conic sections with the curves of the third order, because they may amount to six, ...; and the intersections of two curves of the third order, because they may amount to nine, ...*"

Étienne Bézout, in 1779, published the theorem in *Théorie générale des équations algébriques*.

Georges-Henri Halphen, in 1873, gave the, generally accepted, first correct proof.

Thank you for listening!

References

1) W. Fulton, *Algebraic Curves*; pdf available for free download at http://www.math.lsa.umich.edu/ ∼wfulton/CurveBook.pdf

2) R. Hartshorne, *Algebraic Geometry*

3) I.R. Shafarevich, *Basic Algebraic Geometry I: Varieties in Projective Space*

4) K. Smith, et. al., *An Invitation to Algebraic Geometry*

5) R. Walker, *Algebraic Curves*