BÉZOUT'S THEOREM & ITS APPLICATIONS

Praneat Data
B.S. Mathematics & Scientific Computing
IIT Kanpur
Kanpur
praneat21@iitk.ac.in

ABSTRACT

Bézout's Theorem is a cornerstone of algebraic geometry, providing a fundamental result on the intersection of algebraic curves. This theorem is not only a significant theoretical result but also has practical applications across mathematics and related fields. This report presents an overview of Bézout's Theorem, covering the essential concepts and definitions, such as projective space, degree, and intersection multiplicity, which are crucial for understanding the theorem's statement and implications. We outline the proof of the theorem, highlighting the use of algebraic tools such as ideals, local rings, and dimension arguments. Additionally, the report explores some applications of Bézout's Theorem.

1 Introduction

Bézout's Theorem is a central result in algebraic geometry that describes the intersection behavior of curves in the projective plane, playing a crucial role in connecting geometry with algebra. Its generality and elegance make it foundational in understanding how solutions to polynomial equations intersect, especially when counting intersections with multiplicities.

In modern contexts, Bézout's Theorem finds applications across fields like computer-aided design, robotics, and physics, where it aids in solving polynomial systems and calculating critical intersections. This paper explores the theorem's theoretical basis, providing a structured proof and examining key applications. Through these discussions, we highlight Bézout's lasting significance and practical impact in both mathematics and applied sciences.

2 Preliminaries

2.1 Intersection Numbers in Algebraic Geometry

2.1.1 Main Definition

For plane curves $V(F), V(G) \subset \mathbb{A}^2$ and a point $P \in \mathbb{A}^2$, the intersection number $I(P, V(F) \cap V(G))$ is defined as:

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

where:

- $\mathcal{O}_P(\mathbb{A}^2)$ is the local ring at P
- (F, G) is the ideal generated by F and G
- $\dim_k$ denotes dimension as a k-vector space

2.1.2 Properties of Intersection Numbers

We say $V(F)$ and $V(G)$ intersect properly at P if $V(F)$ and $V(G)$ have no common component passing through P.

1. **Non-negativity and Finiteness**
   - $I(P, V(F) \cap V(G))$ is a non-negative integer when $V(F)$ and $V(G)$ intersect properly at P.
   - $I(P, V(F) \cap V(G)) = \infty$ if $V(F)$ and $V(G)$ do not intersect properly at P.
2. **Zero Conditions**
   - $I(P, V(F) \cap V(G)) = 0$ if and only if $P \notin V(F) \cap V(G)$.
   - $I(P, V(F) \cap V(G))$ depends only on components of $V(F)$ and $V(G)$ through P.
   - $I(P, V(F) \cap V(G)) = 0$ if either F or G is a nonzero constant.
3. **Coordinate Independence**
   - If T is an affine change of coordinates on $\mathbb{A}^2$,
   - and if $T(Q) = P$,
   - then $I(P, V(F) \cap V(G)) = I(Q, V(F^T) \cap V(G^T))$.
4. **Symmetry**
$$I(P, V(F) \cap V(G)) = I(P, V(G) \cap V(F))$$
5. **Multiplicity Bound**
   - $I(P, V(F) \cap V(G)) \geq m_P(V(F))m_P(V(G))$.
   - Equality holds if and only if $V(F)$ and $V(G)$ have no common tangent lines at P.
   - Where $m_P(V(F))$ is the multiplicity of $V(F)$ at P.
6. **Additivity** If $V(F) = \bigcup_i V(F_i)$ and $V(G) = \bigcup_j V(G_j)$, then:
$$I(P, V(F) \cap V(G)) = \sum_{i,j} r_i s_j I(P, V(F_i) \cap V(G_j))$$
   where r_i and s_j are the multiplicities of components.
7. **Ideal Property**
   - For irreducible F: $I(P, V(F) \cap V(G))$ depends only on the image of G in $\mathcal{O}_{V(F)}$.
   - For arbitrary F: $I(P, V(F) \cap V(G)) = I(P, V(F) \cap V(G + AF))$ for any $A \in k[X, Y]$.
8. **Global Intersection Sum** If $V(F)$ and $V(G)$ have no common components, then:
$$\sum_P I(P, V(F) \cap V(G)) = \dim_k(k[X, Y]/(F, G))$$

2.1.3 Transversal Intersection

$V(F)$ and $V(G)$ intersect transversally at P if:

- P is a simple point on both $V(F)$ and $V(G)$.
- The tangent line to $V(F)$ at P differs from the tangent line to $V(G)$ at P.

In this case, $I(P, V(F) \cap V(G)) = 1$.

2.2 Key Examples

Consider $V(F) = V(Y - X^2)$ and $V(G) = V(Y)$ at $P = (0, 0)$:

- These curves are tangent at P.
- $I(P, V(F) \cap V(G)) = 2$ (not 1).
- Shows intersection number captures tangency.

For $V(F) = V(Y)$ and $V(G) = V(X)$ at $P = (0, 0)$:

- These curves intersect transversally.
- $I(P, V(F) \cap V(G)) = 1$.
- Simple crossing point.

2.3 Degree d Forms in Polynomial and Quotient Rings

Let $R = k[X, Y, Z]$ denote the polynomial ring in three variables over a field k, and let $\Gamma = k[X, Y, Z]/(F, G)$, where F and G are homogeneous polynomials.

1. **Forms of Degree d in R:**
   - A form of degree d is a homogeneous polynomial in which every term has a total degree d.
   - Denoted as $R_d = \{\text{homogeneous polynomials of degree } d \text{ in } R\}$.
   - *Example (for $d = 2$)*: $aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2$.
2. **Forms of Degree d in Γ:**
   - Defined as $\Gamma_d = R_d/(F, G)_d$, the space of degree d forms modulo the relations induced by F and G.
   - Elements of Γ_d are equivalence classes of degree d forms, subject to these relations.

It follows that the spaces R_d and Γ_d are vector spaces, with bases given by the monomials of degree d.

2.3.1 Dimension Analysis of R_d

$$\dim_k R_d = \binom{d+2}{2} = \frac{(d+1)(d+2)}{2},$$

which counts the number of possible monomials of degree d in three variables.

2.3.2 Concrete Example

Let $F = X^2 + Y^2 - Z^2$ and $G = XY - Z^2$ be curves in $\mathbb{P}^2$.

1. **In R_2:**
   - General form: $aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ$.
   - Dimension: $\dim_k R_2 = 6$.
2. **In Γ_2:**
   - Relations:
   $$X^2 + Y^2 \equiv Z^2 \quad \text{and} \quad XY \equiv Z^2.$$
   - These relations reduce the dimension of Γ_2.

2.4 Multiplicity of a Point

The *multiplicity* of a point P on a curve F, denoted $m_P(F)$, is defined as:

$$m_P(F) = \max\{m \geq 0 : F \in \mathfrak{m}_P^m\},$$

where $\mathfrak{m}_P$ is the maximal ideal of the local ring $\mathcal{O}_P$.

2.4.1 Alternative Definitions

Via Taylor Series Expansion: After translating P to the origin (via a projective change of coordinates):

$$F = F_m + F_{m+1} + \cdots,$$

where F_i are homogeneous components of degree i. The multiplicity $m_P(F)$ is the smallest m such that $F_m \neq 0$.

2.4.2 Basic Properties

1. **Non-Negativity:**
   - $m_P(F) \geq 0$ for all P.
   - $m_P(F) = 0$ if and only if $P \notin F$.
2. **Simple Points:**
   - P is a *simple point* if $m_P(F) = 1$, meaning F has a well-defined tangent at P.
3. **Singular Points:**
   - P is *singular* if $m_P(F) > 1$, indicating a more complex local structure.
4. **Product Rule:**
   $$m_P(FG) = m_P(F) + m_P(G).$$

2.4.3 Geometric Interpretation

1. $m_P(F)$ represents the number of intersections of a generic line through P with F, counted with multiplicity.
2. $m_P(F) = 1$: F is locally linear.
3. $m_P(F) = 2$: F has a double point (e.g., a node or cusp).

2.4.4 Examples

For $F = Y^2 - X^2 - X^3$ at $P = (0, 0)$:

- $m_P(F) = 2$.
- Two distinct tangent lines form a *node*.

For $F = Y^2 - X^3$ at $P = (0, 0)$:

- $m_P(F) = 2$.
- A single tangent line with multiplicity 2 forms a *cusp*.

3 Bézout's Theorem

Theorem 1 (Bézout's Theorem)**.** *Let F and G be homogeneous polynomials in $k[X, Y, Z]$ of degrees m and n respectively, defining projective plane curves with no common component. Then*

$$\sum_P I(P, V(F) \cap V(G)) = m \cdot n,$$

where $I(P, V(F) \cap V(G))$ denotes the intersection number at point P.

Proof. We prove the theorem by reducing the problem to the affine case, constructing a dimension-counting argument, and using an exact sequence.

Preliminary Step: Reduction to the Affine Case

1. Since $V(F)$ and $V(G)$ have no common components, their intersection $V(F) \cap V(G)$ is finite.
2. By applying a projective change of coordinates, we may assume that no intersection points lie on the line at infinity ($Z = 0$).
$$\sum_P I(P, V(F) \cap V(G)) = \sum_P I(P, V(F_*) \cap V(G_*)),$$
3. Setting $Z = 1$, the curves $V(F)$ and $V(G)$ correspond to affine polynomials:
$$F_*(X, Y) = F(X, Y, 1), \quad G_*(X, Y) = G(X, Y, 1).$$
4. The affine intersection numbers satisfy:
$$\sum_P I(P, V(F_*) \cap V(G_*)) = \dim_k k[X, Y]/(F_*, G_*),$$
where the dimension of the quotient algebra equals the sum of the multiplicities of intersection points.

Step 1: Construction of the Exact Sequence

1. Define the maps:
$$\psi : R \times R \to R, \quad \psi(A, B) = AF + BG,$$
$$\chi : R \to R \times R, \quad \chi(C) = (GC, -FC).$$

2. These maps yield the following exact sequence:

$$0 \to R \xrightarrow{\chi} R \times R \xrightarrow{\psi} R \xrightarrow{\varphi} \Gamma \to 0,$$

where $\Gamma = k[X, Y, Z]/(F, G)$ is the quotient ring associated with the projective curves. The exactness of the sequence can be easily checked here.

3. Restricting to forms of degree d, we have:

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

Step 2: Dimension Counting

1. For forms of degree d in three variables:

$$\dim_k R_d = \binom{d+2}{2}.$$

2. Using the exact sequence:

$$\begin{aligned} \dim \Gamma_d &= \dim R_d - \dim \mathrm{Im}(\psi) \\ &= \dim R_d - (\dim R_{d-m} + \dim R_{d-n} - \dim R_{d-m-n}). \end{aligned}$$

3. For $d \geq m + n$, the dimension simplifies to:

$$\dim \Gamma_d = m \cdot n.$$

Step 3: Injectivity of Multiplication by Z

Lemma 2. *The map $\alpha : \Gamma \to \Gamma$, defined by $\alpha(\overline{H}) = \overline{ZH}$, is injective.*

Proof. Suppose $ZH = AF + BG$ for some $A, B \in R$. Let $H_0 = H(X, Y, 0)$. Then:

$$H_0 = A_0 F_0 + B_0 G_0,$$

where $F_0 = F(X, Y, 0)$ and $G_0 = G(X, Y, 0)$. Since F_0 and G_0 are relatively prime, it follows that:

$$A_0 = -G_0 C \quad \text{and} \quad B_0 = F_0 C \quad \text{for some } C \in R.$$

Defining $A' = A + CG$ and $B' = B - CF$, we have:

$$ZH = A'F + B'G,$$

where A' and B' are divisible by Z. Dividing out Z, we conclude that $H \in (F, G)$, proving α is injective. □

Step 4: Final Dimension Argument

1. For $d \geq m + n$, choose a basis $\{A_1, \ldots, A_{mn}\}$ of Γ_d.
2. Let $A_{i*} = A_i(X, Y, 1)$ and a_i be their residues in the affine ring $\Gamma_* = k[X, Y]/(F_*, G_*)$.
3. The set $\{a_1, \ldots, a_{mn}\}$ spans Γ_*, and the injectivity of α ensures their linear independence.
4. Thus, $\dim_k \Gamma_* = m \cdot n$, completing the proof.

This establishes Bézout's Theorem. □

4 Applications of Bézout's Theorem

The following results are direct consequences of Bézout's theorem:

1. **Line-Curve Intersection**:

- A line intersects a curve of degree d in exactly d points (counting multiplicity)
- Every line through a point of multiplicity m intersects the curve in $d - m$ additional points

2. **Conic Intersections**:

- Two distinct conics intersect in exactly 4 points (counting multiplicity)
- A line and a conic intersect in exactly 2 points
- Three conics with no common component can't share more than 9 points

3. **Multiplicity Bounds**:

- For a curve of degree d, any point has multiplicity at most d
- A singular point has multiplicity at most $d - 1$
- The sum of multiplicities of all singular points is at most $\frac{(d-1)(d-2)}{2}$

Bezout's Theorem gives rise to some amazing results few of the results are:

4. **Pascal's Theorem**: If a hexagon is inscribed in an irreducible conic, then the opposite sides meet in collinear points.

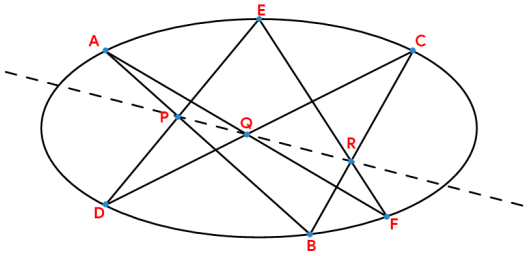

Figure 1: Pascal Theorem

Proof:

Let $ABCDEF$ describe a hexagon inscribed in a conic C. Let $L_1, L_2, L_3, L_4, L_5, L_6$ describe the lines AB, BC, CD, DE, EF, FA, respectively. Define two degree 3 curves:

$$C_1 = V(L_1 \cdot L_3 \cdot L_5), \quad C_2 = V(L_2 \cdot L_4 \cdot L_6).$$

By Bézout's theorem, C_1 and C_2 intersect at 9 points: $A, B, C, D, E, F, P, Q, R$, all with multiplicity 1.

Now, construct the polynomial:

$$H = aC_1 + bC_2,$$

where $a, b \in \mathbb{R}$. This polynomial H is also a degree 3 curve.

Step 1: Degree of H: Since both C_1 and C_2 are cubic curves, their linear combination H is also cubic.

Step 2: Intersection points: The curves C_1 and C_2 intersect at exactly 9 points: $A, B, C, D, E, F, P, Q, R$.

Step 3: Collinearity of P, Q, R: Since A, B, C, D, E, F are points on the conic C, H also vanishes at these points and at the intersection points P, Q, R of the opposite sides of the hexagon.

Step 4: Unique cubic curve: By the properties of algebraic curves, through any 9 distinct points in the plane, there exists a unique cubic curve. Here, H is this unique cubic curve.

Step 5: Verifying collinearity: Suppose P, Q, R were not collinear. Then H would represent a cubic curve that intersects the conic C at more than 9 points, which violates Bézout's theorem.

Thus, P, Q, R must be collinear. In this case, H is a degenerate cubic curve that decomposes into the conic C and the line through P, Q, R.

Conclusion: The line containing P, Q, R is uniquely defined, proving that the opposite sides of the hexagon meet in collinear points, as stated in Pascal's theorem. □

5. **Pappus Theorem**: Let A, B, C be three points on one line, and A', B', C' be three points on another line. Then the intersection points of the pairs of lines $(AB' \cap A'B)$, $(AC' \cap A'C)$, and $(BC' \cap B'C)$ are collinear.

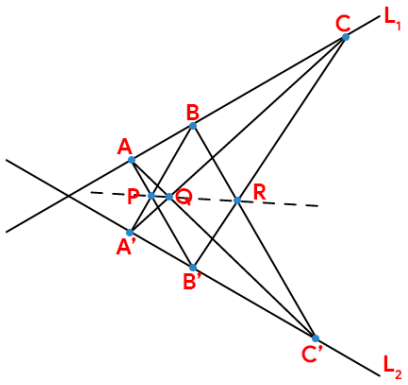

Figure 2: Pappus Theorem

Proof: Pappus' Theorem is a special case of Pascal's Theorem. To see this, consider a degenerate conic formed by two lines, L_1 and L_2. The points A, B, C lie on L_1, and the points A', B', C' lie on L_2.

In Pascal's Theorem, a hexagon inscribed in a conic is considered, and the intersection points of opposite sides are collinear. Here, let the hexagon be $AB'C'A'BC$. The opposite sides of the hexagon are:

$$AB' \cap A'B, \quad AC' \cap A'C, \quad BC' \cap B'C.$$

These correspond to the points P, Q, R, respectively.

Since the hexagon is inscribed in the degenerate conic formed by L_1 and L_2, Pascal's Theorem guarantees that the points P, Q, R are collinear.

Conclusion: By applying Pascal's Theorem to the degenerate conic, Pappus' Theorem is proven. □

Further Bezout's theorem is also used in the following fields:

1. **Elliptic Curve Group Law**
   - Collinear points on elliptic curves sum to zero.
   - Basis for elliptic curve cryptography.
2. **Polynomial Systems**
   - Upper bounds on polynomial solution intersections.
   - Key in computational algebraic geometry.
3. **Computer Graphics**
   - Ray tracing and Bézier curve intersections.
4. **Cryptography**
   - Elliptic curves and point counting for security.
5. **Robotics**
   - Path intersection and collision detection.
6. **Fermat's Curve**

- Intersection of $X^n + Y^n = Z^n$ with lines yields n points, linking geometry and number theory.

7. **Newton's Result**
   - Nine points of intersection between two cubics imply collinearity, derived from Bézout's theorem.

Acknowledgments

The author would like to express their sincere gratitude to Prof. Narasimha Chary Bonala, whose guidance, encouragement, and insightful feedback were invaluable throughout the preparation of this work. Special thanks are extended to Indian Institute of Technology Kanpur for providing the necessary resources and a stimulating research environment.

Additionally, the author acknowledges the support of colleagues and friends who offered constructive suggestions and discussions, contributing to the refinement of this manuscript.

References

[1] W. Fulton, *Intersection Theory*, 2nd ed., Springer-Verlag, New York, 1998. An essential resource on intersection numbers and their geometric and algebraic interpretations.

[2] I. R. Shafarevich, *Basic Algebraic Geometry 1: Varieties in Projective Space*, 2nd ed., Springer-Verlag, Berlin, 1994. Covers the properties of plane curves, local rings, and multiplicity.

[3] Richard E. Borcherds, *Introduction to Intersection Theory - Lecture 4*, YouTube, 2023. Available at: `https://youtu.be/UJssb0-e2yw`. Accessed: November 21, 2024.