INTRODUCTION TO BEZOUT'S THEOREM

ISABEL ZDENA VARGAS-HURLSTON

Abstract. This paper provides a proof of Bezout's theorem using the resultant. As such, it provides relevant background on the resultant, as well as projective space. A simple proof of the theorem in the case of a conic and another curve is also included to help the reader visualize what the theorem states and why it is true.

Contents

1. Introduction

Bezout's theorem states that two polynomials of degree n and m will have nm intersections in complex projective space, counted with multiplicity. Bezout's theorem in the case of plane curves was stated in Isaac Newton's *Principia* in 1687. Bezout gave a proof for simpler cases that did not involve projective space and multiplicity in 1779 [4].

Further progress came in the 20th century, once Serre achieved an algebraic description of multiplicity.

1.1. Pascal's Theorem.

Due to its characterization of curves in projective space, Bezout's theorem is important in algebraic geometry and topology. For example, Bezout's theorem has been used to elegantly prove Theorem 1.1, Pascal's Theorem [5] [6].

Theorem 1.1. *Let $ABCDEF$ be a hexagon inscribed in a conic. Then the intersections X, Y, Z of opposite sides of this hexagon are collinear. See Figure 1 for a visualization of this statement.*

Date: DEADLINES: Draft AUGUST 14 and Final version AUGUST 28, 2024.

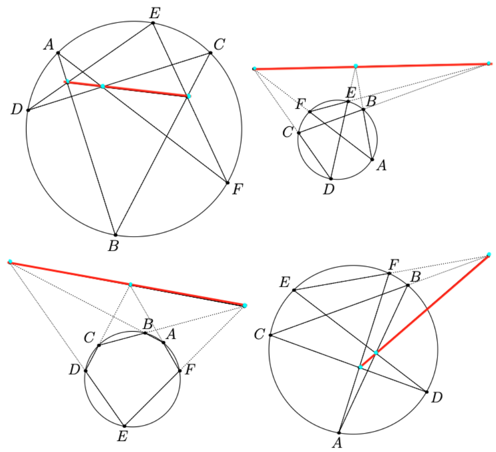

Figure 1. Examples [5] of Pascal's theorem applied to hexagons inscribed in circles. The lines formed by the intersection points of opposite sides of the hexagon are shown in red.

Proof. We will now sketch the proof of this theorem. For a full proof, see [5] [6].

In the case that all pairs of opposite sides on the hexagon are parallel, the points of intersection all lie on the line at infinity (see Section 2 for a description of projective space and the line at infinity, and Figure 2 for a visual).

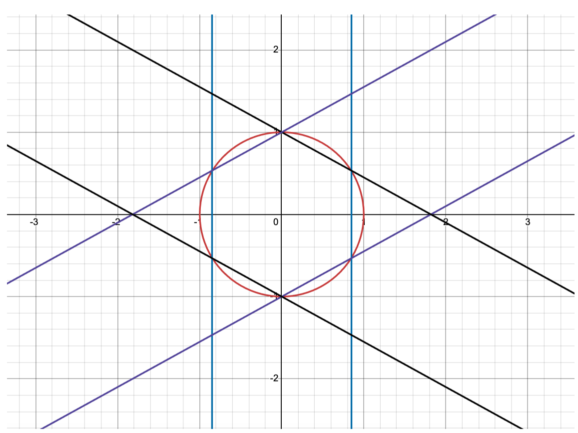

Figure 2. A regular hexagon inscribed in a circle [22]. Opposite sides (shown in the same color) are parallel.

Opposite sides of the hexagon in Figure 2 do not intersect in Euclidean space. However, in projective space parallel lines do intersect (each set or pencil of parallel lines intersecting at one point at infinity). Therefore, all three intersection points for the hexagon shown lie on the "line at infinity".

Similarly, if one pair of opposite sides is parallel, then the intersection points of the other pairs must form a line parallel to the parallel pair of sides, so that this line contains the point at infinity where the parallel sides intersect [6]. As such, Pascal's theorem is true in projective space without exceptions.

From this description, it is obvious that projective space plays a role in Pascal's theorem. Similarly, we can define two cubic curves, each defined to vanish on three of the six lines of our hexagon and containing no opposite or adjacent sides. In this case, each cubic will contain all six points of the hexagon. Then we can choose a seventh point on the conic within which the hexagon is inscribed and create a linear combination of the two cubics that vanishes there [6].

Since both cubics vanish at the six points of the hexagon, this new cubic will vanish at all of these points as well. Thus, it will have seven points in common with the conic [6]. However, Bezout's theorem states that if the cubic and conic are distinct, then they must have $2 \cdot 3 = 6$ (the product of the degrees of the two curves) points in common. Thus, the curves cannot be distinct, and the cubic must be the union (product) of the conic and a line (degree one polynomial).

Since the intersections of opposite sides cannot lie on the conic (opposite sides cannot intersect the conic at the same point), they must lie on this line, and thus be collinear. With this observation, the proof of Pascal's theorem is complete.

□

1.2. **Singular Points.** Bezout's theorem can also be used to count the singular points (where the curve crosses over itself or otherwise breaks differentiability [10]) of an irreducible [13] projective curve of degree d [7] [9] [8] in an algebraically closed field [13]. Specifically, there are no more than $\binom{d-1}{2}$ singular points for a curve of degree d.

In order to prove this claim, we can create a curve of degree $d-2$ through $\binom{d-1}{2} + d - 2 = \binom{d}{2} - 1$ points, and assume that $\binom{d-1}{2} + 1$ of these points are singular [7] (the other $d-3$ points are arbitrary points on the curve). Bezout's theorem states that there should be

$$(d-2)d = d^2 - 2d$$

intersections between these curves, counted with multiplicity.

However, there are at least

$$2 \cdot \left(\binom{d-1}{2} + 1 \right) + d - 3 = 2 \cdot \left(\frac{d^2 - 3d + 4}{2} \right) + d - 3$$

points, since singular points must have a multiplicity greater than one. Since $d(d-2)+1 > d(d-2)$, it follows by Bezout's theorem that the curve of degree $d-2$ that we constructed is a factor of the curve of degree d, which is a contradiction because the curve is given to be irreducible [7].

1.3. **Loops.** It can similarly be shown that an irreducible smooth curve of degree d can have at most $\binom{d-1}{2}+1$ loops.

For the purposes of this proof, we define an *even* loop as one whose complement is split into two disjoint components, an interior and an exterior. In contrast, an *odd* loop has only one connected component. See Figure 3 for a visual of such loops in projective space.

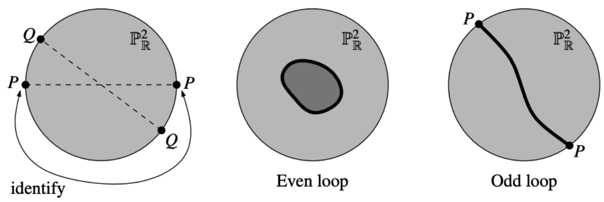

FIGURE 3. An example of odd and even loops in projective space [7]. Note that antipodal points are identified with each other, as shown in the leftmost figure, such that the odd loop shown is indeed a closed loop.

The identification of antipodal points also implies that the complement of the odd loop consists of only one connected component, as asserted in the definition of even and odd loops.

Consider a curve that has been decomposed into distinct loops (see Figure 4). Since the complement of an odd loop is a disc, it is impossible for the curve to consist of more than one odd loop, as all loops constructed within a disc have an interior and an exterior [7].

Specifically, one can consider that the identification of antipodal points can only be taken advantage of once. There is no way to connect two pairs of antipodal points in a circle without one line crossing the other, implying that there is no way to create two disjoint odd loops. Therefore, any curve can have at most one odd loop. This fact will be utilized in our proof.

The proof will now follow similarly to the proof that a projective curve of degree d can have no more than $\binom{d-1}{2}$ singular points. To begin, we construct a curve through $\binom{d-1}{2}+2$ points and assume that each point is on a separate loop of the curve [7].

In this case, there are $\binom{d-1}{2}+1$ additional points, as an even loop will be intersected in two points or have an intersection of multiplicity two (we count intersections with multiplicity for Bezout's theorem). As in the previous proof, we can choose $d-3$ additional points on any curve, and show that there are more than

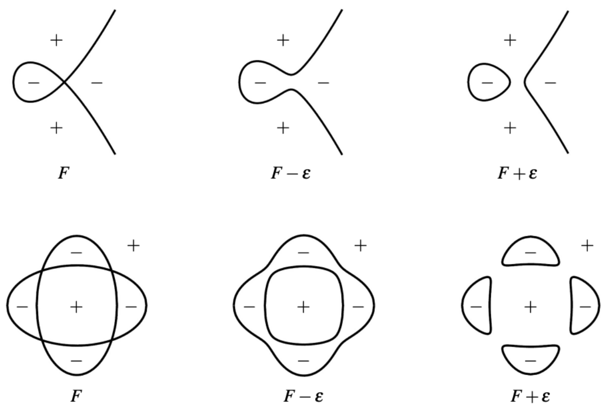

Figure 4. The decomposition of a cubic curve and two conic curves into disjoint loops. This decomposition is achieved through a perturbation of the curves by a small number ϵ [7]. Note that there is at most one odd loop in the decompositions.

$d(d-2)$ intersection points [7]. Again, this result contradicts Bezout's theorem since the curve of degree d is irreducible.

Bezout's theorem also has applications in topology, including determining the genus of a smooth curve in projective space [7] [11] [12]. These examples emphasize that Bezout's theorem is applicable to a wide variety of problems. Overall, the importance of understanding how two curves will intersect encourages the study of this theorem.

2. Projective Spaces

The proof of Bezout's theorem will require an understanding of projective spaces, as alluded to in the introduction.

Definition 2.1. A projective space $\mathbb{P}^n_{\mathbb{R}}$ is the set of all lines through the origin in $\mathbb{R}^{n+1}$ [2].

This definition is best explained through visuals. We will begin with the simplest space, $\mathbb{P}^1_{\mathbb{R}}$, and consider the lines through the origin in $\mathbb{R}^2$. Several such lines are shown in Figure 5.

Importantly, we can characterize each of these lines by one real number: its slope. The only exception is the line $x = 0$. Note that the closer that a line is to the y-axis, the larger its slope is. As such, we consider this line to have infinite slope, and allow a point at infinity as a member of $\mathbb{P}^1_{\mathbb{R}}$. It follows that $\mathbb{P}^1_{\mathbb{R}} = \mathbb{R}^1 \cup \{\infty\}$.

This example gives a general feel for how projective spaces work: $\mathbb{P}^n_{\mathbb{R}}$ contains a full copy of $\mathbb{R}^n$. As shown by the additional point at infinity in $\mathbb{P}^1_{\mathbb{R}}$, however,

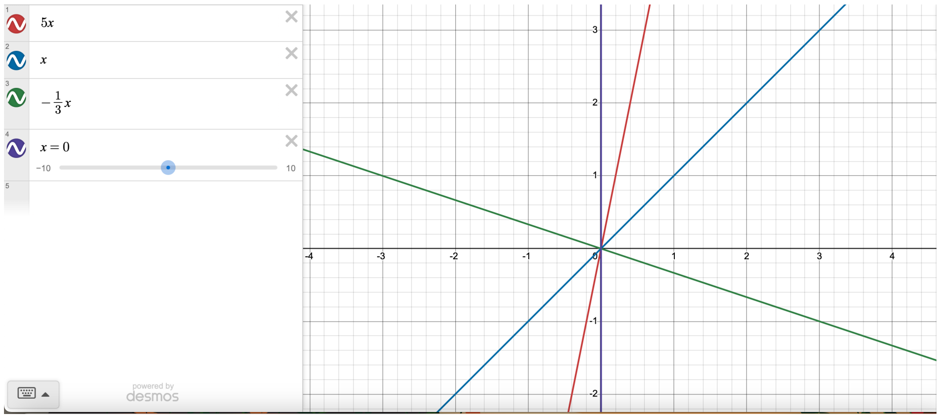

FIGURE 5. Selected lines through the origin in the plane $\mathbb{R}^2$ [22]. Note that the vertical line ($x = 0$) is a valid member of $\mathbb{P}^1_{\mathbb{R}}$.

equality does not necessarily hold. In other words, while $\mathbb{R}^n \subset \mathbb{P}^n_{\mathbb{R}}$, it is not true that $\mathbb{P}^n_{\mathbb{R}} = \mathbb{R}^n$.

Our focus for this paper will be $\mathbb{P}^2_{\mathbb{R}}$, the set of all lines through the origin in $\mathbb{R}^3$. We can characterize each line by the point where it intersects the plane $z = 1$. However, lines that lie in the xy plane are not accounted for by this characterization. Each of these lines represents a point at infinity. This observation leads us to Lemma 2.5.

Definition 2.2. A line in projective space is defined as the set of lines that coincide with a *plane* through the origin (see Figure 6). As such, it can be characterized by the equation of the plane that defines it [19].

For example, in $\mathbb{R}^3$, the equation $z = 0$ characterizes the xy plane. Since the line in $\mathbb{P}^2_{\mathbb{R}}$ that this plane delineates contains only points at infinity, we call this line the line at infinity.

Remark 2.3. Note that all lines through the plane in Figure 6 must be perpendicular to the red vector shown in the figure, because this vector is perpendicular to the plane itself.

Furthermore, any line perpendicular to the red vector must lie in the plane shown, because we are working in $\mathbb{R}^3$ and can thus form an orthogonal basis using the red vector and two vectors that are orthogonal to each other and lie in the plane.

Thus, we can also consider a projective line in $\mathbb{P}^2_{\mathbb{R}}$ as the set of all lines through the origin that are perpendicular to a given vector.

Lemma 2.4. *All projective lines in $\mathbb{P}^2_{\mathbb{R}}$ except for the line at infinity contain exactly one point at infinity*

Proof. Consider some arbitrary projective line that is not the line at infinity. We know that the plane defining the projective line contains the point $(0, 0, 0)$. Thus,

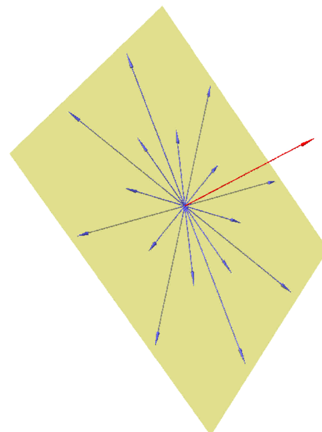

FIGURE 6. An example [21] of a projective line, visualized as the set of lines through the origin that coincide with a plane through the origin (each pair of blue vectors represents a line).

this plane intersects but is not equal to the xy plane. It follows that the planes are not parallel.

The equations of the planes in $\mathbb{R}^3$ will be in three variables [20] [19]. Thus, we have two equations and three variables. The solution to such a system of equations cannot be a single point. Knowing that the intersection is nonzero and that the planes are not equal, we conclude that the intersection of the xy plane and our plane is a line.

Indeed, the intersection between two planes in $\mathbb{R}^3$ that are not parallel or equal is a single line [20] (see Figure 7). Since this line lies on the xy plane, it is clearly a point at infinity.

Since this line is the only line on the xy plane that belongs to the plane defining our projective line, our arbitrary projective line contains one and only one point at infinity. We conclude that this statement holds for all projective lines in $\mathbb{R}^3$, except for the line at infinity. □

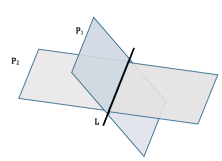

FIGURE 7. In $\mathbb{R}^3$, two nonequal intersecting planes will intersect in a line [20].

Lemma 2.5. *Any two nonequal lines in $\mathbb{P}^2_{\mathbb{R}}$ have exactly one shared point.*

Proof. We can prove this assertion by the same logic used in Lemma 2.4: the planes defining any two projective lines have a shared point at the origin. Thus, they are not parallel. Given also that the planes are not equal, their intersection points will form a single line.

This line must contain the shared point at the origin. As such, it is a line through the origin, and thus a point in projective space. This point is our single intersection point. Note that the point can be a line in the xy plane (a point at infinity).

In this case, the lines are parallel, since they do not converge in $\mathbb{R}^2$ (recall that $\mathbb{R}^2 \subset \mathbb{P}^2_{\mathbb{R}}$). As such, we state that parallel lines converge at infinity in projective space.

□

We must also introduce a convention for projective coordinates. As is common practice, we will follow the notation described in Construction 2.6.

Construction 2.6. Homogenous coordinates: We denote points in $\mathbb{P}^n$ as an equivalence class $[x_1 : x_2 \cdots : x_n]$, where $[x_1 : x_2 \cdots : x_n] \sim [y_1 : y_2 \cdots : y_n]$ if some constant c satisfies $[c \cdot x_1 : c \cdot x_2 \cdots : c \cdot x_n] = [y_1 : y_2 \cdots : y_n]$ [15] [16].

Essentially, since a point in $\mathbb{P}^n$ is a line through the origin in $\mathbb{R}^{n+1}$, we can represent a point in $\mathbb{P}^n$ using any point on the line that defines it. In this way, we represent points in $\mathbb{P}^n$ as equivalence classes of $n+1$-tuples, or points in $\mathbb{R}^{n+1}$.

We will prove that equivalent points must lie on the same line through the origin in Theorem 2.7. Note that, due to the nature of projective space, $[0 : 0 \cdots : 0]$ is not a valid point in homogeneous coordinates.

Theorem 2.7. *Two points in $\mathbb{P}^n$ are equivalent if and only if they lie on the same line through the origin.*

Proof. We will accept without proof that two points are connected by one and only one line in $\mathbb{R}^n$. If $[c \cdot x_1 : c \cdot x_2 \cdots : c \cdot x_n] = [y_1 : y_2 \cdots : y_n]$, then we can show that the line connecting $(x_1, x_2, ..., x_n)$ and $(y_1, y_2, ..., y_n)$ must pass through the origin. We will consider two distinct points; if the points are equal then they certainly lie on the same line through the origin.

Specifically, we know that $(x_1, x_2, ..., x_n)$ belongs to this line, and that it points in the direction of the vector $\vec{v}$ between $(x_1, x_2, ..., x_n)$ and $(y_1, y_2, ..., y_n)$, which can also be written as the vector

$$\vec{v} = \begin{bmatrix} y_1 - x_1 \\ y_2 - x_2 \\ \vdots \\ y_n - x_n \end{bmatrix}$$

centered at the origin.

We can parametrize [1] the line using this point and this vector, as the set of points p satisfying

$$p = (t \cdot (y_1 - x_1) + x_1, t \cdot (y_2 - x_2) + x_2, \cdots, t \cdot (y_n - x_n) + x_n),$$

where t is some constant. Note that $(x_1, x_2, ..., x_n)$ and $(y_1, y_2, ..., y_n)$ both satisfy this condition, for $t = 0$ and $t = 1$ respectively.

We now wish to show that $\mathbf{0}$ belongs to this line. Thus, we substitute each y_k with $c \cdot x_k$ to yield

$$p = (t \cdot (c-1) \cdot x_1 + x_1, t \cdot (c-1) \cdot x_2 + x_2, \cdots, t \cdot (c-1) \cdot x_n + x_n).$$

Thus, we see that for $t = \frac{1}{1-c}$, the expression evaluates to $\mathbf{0}$ as expected ($\frac{c-1}{1-c} = -1$). Note that $\frac{1}{1-c}$ is only undefined for $c = 1$; the previously mentioned trivial case in which the points are equal.

We now wish to prove that if two points $(x_1, x_2, ..., x_n)$ and $(y_1, y_2, ..., y_n)$ lie on the same line through the origin, then they will be equivalent. Thus, we must return to the parameterization of a line by a vector and a point.

To simplify our calculations, we will choose our point and vector carefully. Specifically, we choose $\mathbf{0}$ as our point. Our vector will be centered at the origin and end at $(x_1, x_2, ..., x_n)$. This line goes through two of our three points, and thus must contain y since all three are collinear.

The line can also be considered as the set of points p satisfying

$$p = (t \cdot x_1, t \cdot x_2, \cdots, t \cdot x_n)$$

for some constant t. Since $(y_1, y_2, ..., y_n)$ satisfies this equation, we know that for some constant c, it must be true that $(y_1, y_2, ..., y_n) = (c \cdot x_1, c \cdot x_2, \cdots, c \cdot x_n)$.

Then $(y_1, y_2, ..., y_n) \sim (x_1, x_2, ..., x_n)$ by definition. Therefore, we conclude that two points in $\mathbb{P}^n$ are equivalent if and only if they lie on the same line through the origin. □

For this paper, we will be working in complex projective space (see Definition 2.8).

Definition 2.8. A complex projective space $\mathbb{P}^n_{\mathbb{C}}$ is similar to the corresponding real projective space, except that each coordinate x_i of a given point is a complex number, and can thus have an imaginary component.

Notation 2.9. This paper will now denote $\mathbb{P}^n_{\mathbb{C}}$ as $\mathbb{P}^n$, omitting the $\mathbb{C}$ subscript.

We now know enough about projective spaces to consider a simple visual proof as an introduction to Bezout's theorem.

3. Visual Proof of Bezout

We will now include a few examples in order to get a feel for the mechanics of projective space. Rather than a rigorous proof, this section focuses on an intuition for the theorem. We begin by stating Bezout's theorem in Theorem 3.1. However, first we must understand intersection multiplicity.

While a formal definition of intersection multiplicity will not be given in this work, some sense of the meaning of this term is necessary. By the fundamental theorem of algebra, a polynomial of degree n has n roots. Thus, any polynomial can be expressed as $\prod_{i \leq n}(x - a_i)$, where each a_i represents a root of the polynomial.

However, in some cases $a_i = a_j$ for some $i, j \leq n$ such that $i \neq j$. In these cases, the polynomial has n roots but does not have n *distinct* roots. The root a_i is said to have multiplicity 2. For example, the polynomial $x^2 = 0$ has one root $(x = 0)$ with multiplicity 2. Similarly, if a root is repeated k times, it has multiplicity k. With this meaning in mind, we can now address Bezout's theorem.

Theorem 3.1. *Bezout's theorem: Let P and Q be projective curves of degree n and m respectively. Then P and Q have nm intersections with multiplicity, given that we allow complex solutions.*

It follows that two conics should have four intersections in projective space. We will model $\mathbb{P}^2$ by the transformation $(x, y) \to (\frac{x}{\sqrt{x^2+y^2+1}}, \frac{y}{\sqrt{x^2+y^2+1}})$. This transformation divides by a value strictly larger than the norm of (x, y), keeping all values within the unit circle (adding one within the radical also prevents division by zero).

Furthermore, antipodal points in this representation are equivalent (the same line through the origin passes through them). An example of the transformation applied to a parabola can be seen in Figure 8.

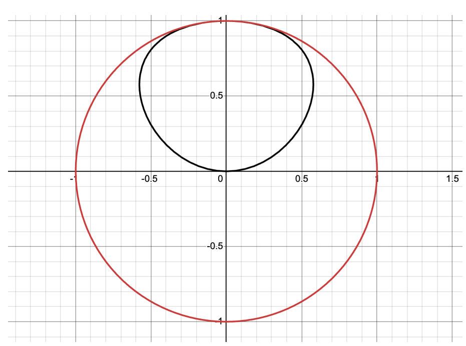

Figure 8. Parabola in our model of projective space [22]. Note that the legs of the parabola converge at infinity, as the limit of both slopes is vertical.

We will also need to consider the decomposition of conics into lines. The graphs shown in Figure 3 demonstrate this decomposition for a generic homogeneous conic $ax^2 + bxy + cy^2 = 1$ (note that in a homogeneous polynomial, all terms have the same overall degree). Such a conic will take the form of a hyperbola or an ellipse.

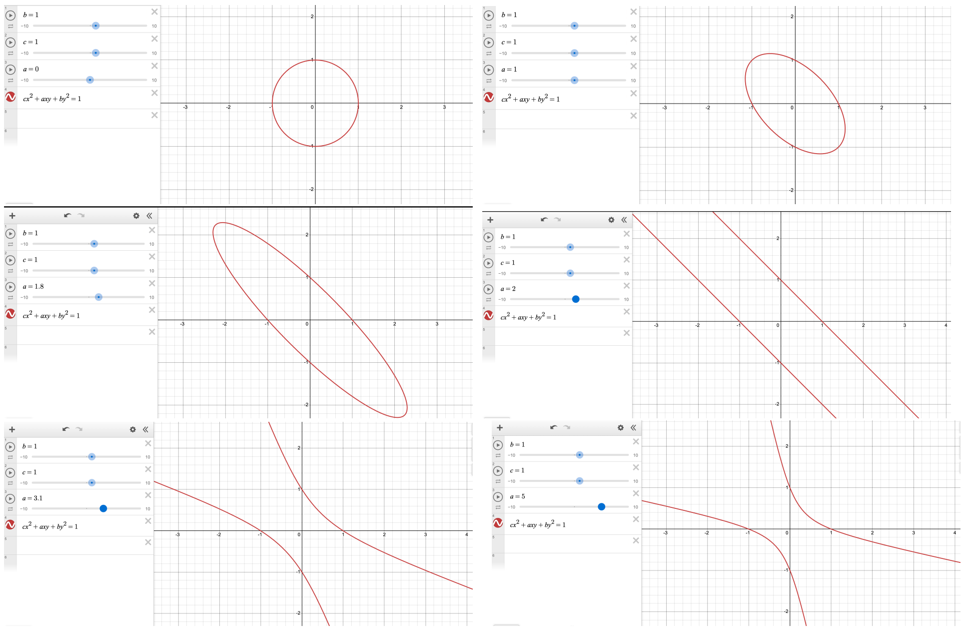

FIGURE 9. As b increases, we see the unit circle stretch out into an ellipse, and then into two lines parallel to $y = -x$. Increasing further results in a hyperbola [22].

Alterations in a or c sill similarly result in vertical and horizontal lines, respectively, due to a similar "stretching" of an ellipse along the vertical or horizontal axes.

We would like to show that such transformations do not change the number of intersections between two curves. Since we are not in the complex plane, visuals can be deceptive here. However, for polynomials without complex intersections a visual will be enlightening. We return to our model of projective space in Figure 10 to support our intuition with visuals.

From this perspective, we can consider the transformation as one from an ellipse to an ellipse with a major axis "at infinity". Since form is still elliptical, and we have essentially merely dilated one axis, the number of intersections should be preserved under this transformation.

This transformation will allow us to prove Bezout's theorem in the case of a conic. Consider the intersections of an arbitrary homogeneous polynomial of degree n with

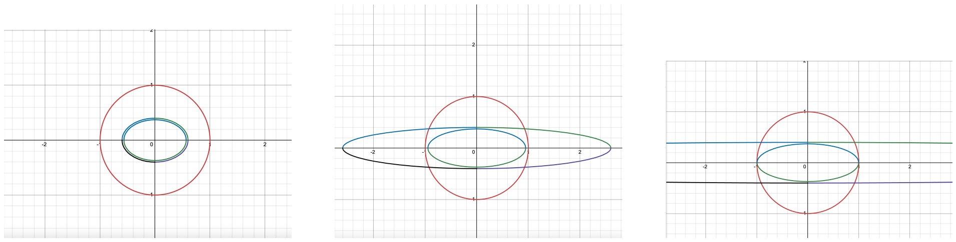

FIGURE 10. The transformation of an ellipse into lines, similar to that shown in Figure 3, now within our model of projective space [22]. The Euclidean depiction is also included for clarity

the lines shown in Figure 10. We wish to prove that there are $2n$ such intersections.

In order to do so, we need only apply a linear transformation, and bring one of the lines to the origin. A translation will certainly not change the number of intersections between the polynomials, nor their degrees. Note that this transformation is generalizable: any line can be brought to the origin by a rotation and translation of the plane.

Now, we can use the fundamental theorem of algebra to state that our curve of degree n has n zeros, given multiplicity and allowing complex solutions. Thus, the curve intersects the line mapped to the origin n times. By a similar logic and transformation, we can conclude that the curve intersects both lines n times.

We thus find a total of $2n$ intersections between a homogeneous degree two polynomial and an arbitrary homogeneous polynomial of degree n. This simple case provides an intuition as to what Bezout's theorem states: in projective space, distinct lines must intersect once and only once. Thus, if we decompose polynomials of degree n and m into n and m lines, respectively, these lines will intersect nm times in projective space.

Another way to address this question is to note that, once homogenized, conics can be expressed as a symmetric bilinear form [16], which satisfies Definition 3.2.

Definition 3.2. Given a vector space V and field K, symmetric bilinear map is a transformation $B\colon V \times V \longrightarrow K$. This transformation must be symmetric, such that $B(u, v) = B(v, u)$ [17].

It must also be bilinear, or linear in both u and v. Thus, we can state that $B(u+w, v) = B(u, v) + B(w, v)$ or $B(u, v+w) = B(u, v) + B(u, w)$ and $B(\lambda u, v) = B(u, \lambda v) = \lambda B(u, v)$ [17].

In our case, the symmetric bilinear form will be defined by the product of two vectors u and v with a matrix. In $\mathbb{P}^2$, this transformation will be a 3×3 matrix, as the projective coordinates will take the form $[X : Y : Z]$. See an example below for clarity.

Example 3.3. Consider the homogeneous polynomial $X^2 + Y^2 + 2YZ$. We want to express the polynomial as $v^T \cdot M \cdot u$, where

$$u = \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$$

and

$$v = \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix}$$

are vectors. Since we specifically want a symmetric bilinear form, we need to make the given polynomial symmetric and write it in terms of u and v.

Thus, our polynomial becomes

$$x_1x_2 + y_1y_2 + y_1z_2 + y_2z_1.$$

Note that in order to create a symmetric polynomial, $2YZ$ is written as $y_1z_2+y_2z_1$, and the coefficient of 2 vanishes.

It follows that the matrix for this transformation is $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$, as

$$\begin{bmatrix} x_2 & y_2 & z_2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} = x_1x_2 + y_1y_2 + y_1z_2 + y_2z_1.$$

Note also that in the case of a non-invertible 3×3 matrix, the domain of the transformation must be one degree down from the domain of the given space, since two columns of the matrix must be linearly dependent. Thus, in this case the conic represented by the matrix is degenerate.

When we orthogonalize [18] the columns of this matrix, the polynomial takes the form

$$\epsilon_1 x_1^2 + \epsilon_2 x_2^2 \cdots \epsilon_n + x_n^2,$$

where n is the dimension of our vector space [16] (to see why, consider that the identity matrix represents a polynomial of the form $x_1^2 + x_2^2 \cdots + x_n^2$).

We can now express any nondegenerate conic in $\mathbb{P}^2$ as $X^2 + Y^2 - Z^2 = 0$ with the appropriate change of basis (coefficients disappear with a transformation of the form $x_1 \longrightarrow \sqrt{\epsilon_1}x_1$). This observation is consistent with Figure 8 and Figure 3, which give a sense of parabolas and hyperbolas in projective space as circles with points at infinity.

We can further simplify the case of a nondegenerate conic by parameterizing the equation $X^2 + Y^2 - Z^2 = 0$. Let $X' = Z + X$ and $Z' = Z - X$ [16]. Further let $Y' = Y$. Then our equation becomes $X'Z' = Y'^2$ in our new system of coordinates. We can now consider parameters U and V such that $X' = U^2$ and $Z' = V^2$. By substitution, $Y'^2 = U^2V^2$. Thus, we can parameterize the equation by $(U^2 : UV : V^2)$.

We can consider $(U : V)$ as a homogeneous coordinate in $\mathbb{P}^1$. Then there is also an inverse map from the conic to $\mathbb{P}^1$: both $(X : Y)$ and $(Y : Z)$ yield $(U : V)$, since we are working in homogeneous coordinates.

We need only one more piece to prove Bezout's theorem in the case of a nondegenerate conic. Given a homogeneous polynomial $Q = a_0U^d + a_1U^{d-1}V + \cdots + a_dV^d$, there exists a corresponding inhomogeneous polynomial $q = a_0u^d + a_1u^{d-1} \cdots + a_d$. Note that the zeroes of this inhomogeneous polynomial are the points α for which $(u - \alpha) \mid q$. It follows that $(U - \alpha V) \mid Q$, and thus that $(\alpha, 1)$ is a zero of Q.

It is also important to consider the case in which $V^k \mid Q$, where k is an arbitrary degree such that $0 < k \leq d$. In this case, the degree of q will be less than the degree of Q. We thus consider Q as having a zero of multiplicity k at the coordinate $(1, 0)$. Note that if $U^{d-k}V^k$ were not a term in Q, then Q would be divisible by V^{k+1}. Thus, q must be a polynomial of degree $d - k$.

Remark 3.4. By the fundamental theorem of algebra, Q has d total zeros. Specifically, Q is the product $V^k \prod_{i \leq d-k}(U - \alpha_i V)$, and each term in this product represents a zero. Here, $0 \leq k \leq d$, as we are no longer considering only the case in which $k > 0$.

Now, we can use the parameterization $(U^2 : UV : V^2)$ for a nondegenerate conic. As described in Example 5.1, our conic can be represented as $Q = M \cdot \begin{bmatrix} U^2 \\ UV \\ V^2 \end{bmatrix}$, where M is a nonsingular 3×3 matrix.

We wish to consider the number of intersections of this conic with some arbitrary curve G of degree d. Thus, we wish to find the points $(X : Y : Z)$ for which $G(X : Y : Z) = 0 = Q(X : Y : Z)$. It follows that $(X : Y : Z)$ can be writted as $M \cdot \begin{bmatrix} U^2 \\ UV \\ V^2 \end{bmatrix}$.

Thus, we end up with the degree $2d$ polynomial $G(M \cdot \begin{bmatrix} U^2 \\ UV \\ V^2 \end{bmatrix})$. The zeros of this polynomial represent the intersections of G and Q. Since this polynomial is a homogeneous polynomial in $\mathbb{P}^2$, it must have $2d$ zeros, as shown in Remark 3.4. We thus conclude that there are $2d$ intersections between G and the conic, proving Bezout's theorem in the case of a conic.

With this background, we will now introduce an important tool necessary for a more rigorous proof of this theorem.

4. The Resultant

The resultant will allow us to analyze the common zeros of two polynomials, thus allowing us to prove Bezout's Theorem more rigorously.

Definition 4.1. If $f_1 = A \cdot (x - r_1) \cdot (x - r_2) \cdots (x - r_n)$ and $f_2 = B \cdot (x - s_1) \cdot (x - s_2) \cdots (x - s_m)$, then the resultant [3] is the product

$$\text{Res}(f_1, f_2) = A^m \cdot B^n \prod_{i=1}^{n} \prod_{j=1}^{m} (r_i - s_j).$$

Note that the resultant evaluates to 0 if and only if some element $(r_i - s_j)$ in the product is zero, unless either A or B is zero, in which case *any* zero of the other curve is a common zero between the two curves (whichever curve has a zero coefficient evaluates to zero everywhere).

In this case, we are guaranteed a common zero by the fundamental theorem of algebra, as the other curve must have at least one zero if its degree is one or greater. If both lines are horizontal, they are parallel and will intersect at infinity in projective space. Thus, they have a common zero at infinity. If both curves have zero coefficients, they similarly have a common zero everywhere.

Thus, the resultant of two polynomials is 0 if and only if they share a common zero, though the zero may only exist in complex projective space, as points with imaginary components and points at infinity are valid intersection points. This product has several other important properties, including Remark 4.2 and Theorem 4.8, which will be useful for our purposes.

Remark 4.2. Consider two arbitrary polynomials $a_n + a_{n-1} \cdot y + \cdots a_0 \cdot y^n$ and $b_m + b_{m-1} \cdot y + \cdots b_0 \cdot y^m$. The resultant is given by the determinant [14] of the square matrix with dimension $n + m$ [3]

$$\begin{bmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n & 0 & 0 & \cdots & b_m \end{bmatrix}.$$

See [3] for a proof of this fact. As an example of this calculation, the resultant of $x + 1$ and $3x + 2$ with respect to y is the determinant of the matrix

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix},$$

or $3 - 2 = 1$. It follows that these curves have no shared zeros. Indeed, the lines intersect exactly once (as we should expect) at the point $(-.5, .5)$, which is not a zero point.

Lemma 4.3. *Let P and Q be polynomials in n variables. Then the resultant of P and Q can be taken with respect to one of these variables x_k. All other variables are treated as parameters. Thus, we essentially treat P and Q as univariate polynomials in some variable x_k, and take the resultant as previously defined in Definition 4.1.*

Example 4.4. Let $P = X^2 + XY + Z^2$ and $Q = Y^2 + ZY + XZ$. Then $Res(P, Q)$ with respect to Z is given by the determinant of the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & X+Y & 0 \\ X^2+XY & 0 & Y^2 & X+Y \\ 0 & X^2+XY & 0 & Y^2 \end{bmatrix}.$$

Note that X and Y are treated like parameters and included in our matrix of coefficients, while Z is treated like a variable.

Definition 4.5. The *weighted degree* of a constant is calculated similarly to the degree of a polynomial in many variables (using the highest degree term). In this case, however, our variables are the parameters included in our coefficients and determinant.

Example 4.6. For the polynomials in Example 4.4, the coefficient $X^2 + XY$ has weighted degree two. The coefficient is homogeneous, because both of its terms have weighted degree two. Similarly, $X + Y$ is a homogeneous coefficient of weighted degree one.

Remark 4.7. Using Definition 4.5 and Lemma 4.3, we can write polynomials in many variables as polynomials in our chosen variable, with coefficients of a certain weighted degree. For example, P and Q as defined in Example 4.4 could be abstracted as

$$a_2 + a_0 \cdot Z^2 \text{ and } b_2 + b_1 \cdot Z,$$

where a_n and b_n represent coefficients of weighted degree n.

We can still tell that the polynomials are homogeneous, as all terms have a total degree of two (adding the weighted degree of each coefficient with the degree of the corresponding term in Z).

Theorem 4.8. *Let P be a homogeneous polynomial of degree k in n variables and Q be a homogeneous polynomial of degree m in n variables. Then the resultant of P and Q with respect to one variable y (as described in Lemma 4.3) is a homogeneous polynomial of degree km in $n - 1$ variables* [3].

Proof. We will assume that the univariate forms of P and Q are of the same degree as the homogeneous forms. In other words, P and Q must contain a term in which y takes the degree of the homogeneous polynomial. These terms take the form

$$a_0 y^k \text{ and } b_0 y^m,$$

respectively. As shown in Example 5.1, any polynomial can be parameterized such that at least one variable satisfies this requirement. Note that since P and Q are of degree k and m, respectively, the coefficients a_0 and b_0 must be of weighted degree zero, as defined in Definition 4.5. In other words, these coefficients are constants.

As in Definition 4.1, we can state that

$$Res(P, Q) = A^m \cdot B^k \prod_{i=1}^{k} \prod_{j=1}^{m} (s_i - t_j),$$

where the set of all s_i and the set of all t_j represent the roots of P and the roots of Q as polynomials in y, respectively. We will now work with P, understanding that the statements we will prove hold for Q as well (with appropriate modifications), and can be proven by similar logic.

To begin, we note that by the fundamental theorem of algebra, there are k values s_i such that $(y - s_i) \mid P$, because we have assumed that P is degree k in y. Then

$$P = A \prod_{i=1}^{k} (y - s_i)$$

for some coefficient A. Since $A \mid P$, our assumption that P has a coefficient a_0 of weighted degree 0 implies that, of all n variables, none but y can divide A.

Specifically, if some $x_s \mid A$, then $x_s \mid P$, and if $x_s \neq y$ and $x_s \mid a_0 \cdot y^k$ both hold, then $x_s \mid a_0$, which would imply that a_0 is of weighted degree one or greater. Note that if $x_s \mid y^k$ and $x_s \neq y$, then our variables are not independent, and the equation is no longer in n variables.

Furthermore, if $y \mid P$, we consider $(y - 0)$ a term of P. As such, $y \mid \prod_{i=1}^{k}(y - s_i)$, not $y \mid A$, holds in this case. It follows that A must be of weighted degree zero. By a similar logic, B is of weighted degree zero. Therefore, $A^m B^k$ is of weighted degree zero.

We conclude that the degree of the product $\prod_{i=1}^{k} \prod_{j=1}^{m} (s_i - t_j)$ is the degree of the resultant. It is thus important to consider the weighted degree of each s_i and t_j. Since P is a homogeneous polynomial, we note that the term $a_k = A \cdot \prod_{i=1}^{k} -s_i$ of P must be of degree k or equal to zero.

In the first case, all s_i must be of weighted degree one, such that their product a_k is of weighted degree k. Note that no term s_q can take the form $(y - \alpha x_q + c)$, where c has weighted degree zero. Otherwise, the term

$$A \cdot c \cdot \prod_{i \leq k | i \neq q} -s_i$$

would be of degree $k - 1$, and P would not be homogeneous.

We must also consider the case in which $a_k = 0$. In this case, at least one s_i must be zero, so $y^t \mid P$ for some $t > 0$. As such, if some zeros t_j of Q are also zero, then the resultant itself is zero, since $0 - 0$ is a term in the product $\prod_{i=1}^{k} \prod_{j=1}^{m} (s_i - t_j)$.

On the other hand, if all zeros of Q have weighted degree one, the difference $-t_j$ between zero and t_j is a degree one polynomial. Furthermore, we note that

$$A \cdot y^t \cdot \prod_{i \leq k | -s_i \neq 0} -s_i$$

is a valid nonzero term of P (as it contains only nonzero s_i).

Since P is homogeneous, $A \cdot \prod_{i \leq k | -s_i \neq 0} -s_i$ must be of weighted degree $k - t$. There are t values of i such that $s_i = 0$, so there are $k - t$ values of i such that s_i

is nonzero. Therefore, all nonzero s_i must be of weighted degree one.

Once again, and by similar logic as before, we note that no s_i or t_j can be of the form $(y - \alpha x_q + c)$, where c is of weighted degree zero. It follows that $s_i - t_j$ for arbitrary i, j must be of weighted degree one or equal to zero, as the difference between two degree one polynomials with no constant terms.

Specifically, the difference cannot be a nonzero constant, and certainly cannot be of a higher degree than s_i and t_j, leaving these two options. The same logic holds if $y \mid Q$ and all s_i are nonzero, or indeed if all s_i and t_j are nonzero (in which case we again deal with differences $s_i - t_j$ between degree one polynomials). Thus, $Res(P, Q)$ is either the product of degree one polynomials or is zero.

It follows that any nonzero resultant of two such polynomials will be of weighted degree km, as the product of km degree one terms. Furthermore, y is not included in our resultant. If $y \mid s_i$ for some s_i, then $(y - s_i) = c \cdot y$ for some constant c, and $s_i = 0$. Thus, as asserted, the polynomial is in $n - 1$ variables.

To prove that the polynomial is homogeneous, consider that *all* of its terms are given by the choice of one degree one element from each of km terms. For example, the resultant of $(x - y)(2x + y)$ and $(2x - y)(x + y)$ in y is

$$(x + x)(2x + 2x)(x + 2x)(2x + x).$$

Each term of this resultant will take the form (for some $n \leq 4$)

$$\prod_{i=1}^{n} 2x \cdot \prod_{i=1}^{4-n} x.$$

Thus, each term is degree four in x. Any resultant of homogeneous polynomials in any number of variables should behave similarly, since the individual terms are still of degree one and there are still km of them.

□

5. Rigorous Proof of Bezout

Let us consider two homogeneous polynomials P and Q, of degree n and m respectively. Note that the intersection points of these curves are zeros of these polynomials.

As in our simpler proof, we will consider these polynomials as polynomials in one variable. Specifically, we again create a construction

$$\sum_{0 \leq i \leq n} a_{n-i} y^i,$$

where we treat y as a variable of degree i and a_{n-i} as a parameter or constant of degree $n - i$.

We will perform a linear transformation such that no zeros are points at infinity and no zeros have the same x coordinate [4] (these changes will make it easier to identify zeros and their multiplicities). The second goal can be achieved by a rotation, which will not change the number or multiplicity of intersections.

The first can be achieved by a parametrization such that at least one variable x_1 takes the degree of the polynomial in at least one term (for example, x_1^d as a term in a degree d polynomial), followed by the selection of a variable satisfying this requirement.

If we do so, the resulting polynomial in x_1 will also be of degree d, and thus have d zeros in the complex plane. It follows that no zeros are points at infinity. This parametrization occurs as shown in Example 5.1. See also the parameterization of a conic in the simple proof.

Example 5.1. We are given the homogeneous polynomial XY, and we want a symmetric bilinear form. Thus, we rewrite the polynomial as

$$F(\vec{x}, \vec{y}) = X_1Y_2 + X_2Y_1$$

for $\vec{x} = \begin{bmatrix} X_1 \\ Y_1 \end{bmatrix}$ and $\vec{y} = \begin{bmatrix} X_2 \\ Y_2 \end{bmatrix}$.

This form is symmetric, as $Y_1X_2 + Y_2X_1 = X_1Y_2 + X_2Y_1$. It is also bilinear, because for $\vec{w} = \begin{bmatrix} W_1 \\ W_2 \end{bmatrix}$ we find that

$$F(\vec{x} + \vec{w}, \vec{y}) = (X_1 + W_1)Y_2 + X_2(W_2 + Y_1),$$

which after distributing becomes

$$X_1Y_2 + X_2Y_1 + W_1Y_2 + W_2X_2 \text{ or } F(\vec{x}, \vec{y}) + F(\vec{w}, \vec{y}).$$

Furthermore,

$$F(\alpha \cdot \vec{x}, \vec{y}) = \alpha \cdot X_1Y_2 + \alpha \cdot X_2Y_1 = \alpha \cdot F(\vec{x}, \vec{y})$$

if α is a constant. The other cases ($F(\vec{x}, \alpha \cdot \vec{y})$ and $F(\vec{x}, \vec{y} + \vec{w})$) follow similarly, and must by the symmetry of the form.

Now, we will consider the vectors $\vec{w} = (1, -1)$ and $\vec{v} = (1, 1)$. As we will show, parameterizing F using these vectors will yield a homogeneous conic that takes degree two in at least one term.

Since $F(\vec{w}, \vec{v}) = 0$ and we have a symmetric bilinear form,

$$F(\lambda_1\vec{v} + \psi_1\vec{w}, \lambda_2\vec{v} + \psi_2\vec{w}) = \lambda_1\lambda_2(\vec{v}, \vec{v}) + \psi_1\psi_2(\vec{w}, \vec{w}).$$

Thus, the conic becomes $2\lambda_1\lambda_2 - 2\psi_1\psi_2$. Through this parameterization, then, we rewrite the conic as $2X^2 - 2Y^2$, a homogeneous conic of degree two in both X and Y.

As stated in Theorem 4.8, the resultant of these polynomials must be a homogeneous polynomial of degree nm, since P and Q are homogeneous polynomials of degrees n and m respectively. Thus, the fundamental theorem of algebra states that this resultant polynomial has nm zeros (with multiplicity and allowing complex solutions).

Since the resultant of two polynomials evaluates to zero only when they have a common zero, each of these zeros represents a shared point of P and Q [4]. It follows that there are exactly nm points of intersection between P and Q.

Acknowledgments

I would like to thank my mentor, Michael Barz, for all of his support in writing this paper. Thank you for opening my mind to many new and wonderful areas of mathematics! I really appreciate all of the time and effort that you put in to guiding everyone in our group. Similarly, I would like to thank J. Peter May and all of the professors who spoke at the REU, as well as my classmates, for making this amazing program possible and successful.

References

[1] Will Boney. Lines and Planes in $\mathbb{R}^3$. 2015. https://people.math.harvard.edu/ wboney/fall15/LinesPlanes.pdf
[2] Adam Marsh. Projective Spaces. 2018. https://www.mathphysicsbook.com/mathematics/topological-spaces/constructing-spaces/projective-spaces/
[3] Eric W. Weisstein. Resultant. https://mathworld.wolfram.com/Resultant.html
[4] Kevin Brown. Bezout's theorem. 2023. https://www.mathpages.com/home/kmath544/kmath544.htm
[5] Carl Joshua Quines. Pascal's theorem. 2017. https://cjquines.com/files/pascals.pdf
[6] John Conway and Alex Ryba. The Pascal Mysticum Demystified. Math Intelligencer 34, 4–8. 2012.
[7] Andreas Gathmann. Applications of Bezout's Theorem. University of Kaiserslautern-Landau. 2023. https://agag-gathmann.math.rptu.de/class/curves-2023/curves-2023-c5.pdf
[8] Kevin Tucker. Math 552 Algebraic Geometry I. University of Illinois Chicago. 2018. https://kftucker.people.uic.edu/Math552Fall2018/recaps/Nov26.pdf
[9] Eric W. Weisstein. Jacobian. https://mathworld.wolfram.com/Jacobian.html
[10] The Editors of Encyclopaedia Britannica. Singularity. 1998. https://www.britannica.com/science/Lagrangian-function
[11] Eric W. Weisstein. Fundamental Group. https://mathworld.wolfram.com/FundamentalGroup.html
[12] Allen Hatcher. Algebraic Topology. Cambridge University Press. 2002.
[13] Serge Lang. Algebra. Graduate Texts in Mathematics volume 211 (revised third edition). Springer. New York, New York. 2002.
[14] Günter Rote. Division-Free Algorithms for the Determinant and the Pfaffian: Algebraic and Combinatorial Approaches. Computational Discrete Mathematics. Lecture Notes in Computer Science, vol 2122. Springer. Berlin, Heidelberg. 2001.
[15] David A. Cox, John Little, and Donal O'Shea. Using Algebraic Geometry. Graduate Texts in Mathematics volume 185 (2nd edition). Springer. New York, New York. 2005.
[16] Miles Reid. Undergraduate Algebraic Geometry. Cambridge University Press. 1989.
[17] William A. Adkins and Steven H. Weintraub. Algebra: An Approach via Module Theory. Graduate Texts in Mathematics volume 136. Springer. New York, New York. 1992.
[18] C. E. Soliverez and E. R. Gagliano. Orthonormalization on the Plane: a Geometric Approach. Revista Mexicana de Física 31 no. 4 (1985) 743-758.
[19] Richard Evan Schwartz. The Projective Plane. 2009. https://www.math.brown.edu/reschwar/M154/proj.pdf
[20] Royal Melbourne Institute of Technology. Intersecting Planes. https://learninglab.rmit.edu.au/content/v9-intersecting-planes.html
[21] David Guichard. Lines and Planes. https://www.whitman.edu/mathematics/calculus_online/section12.05.html
[22] Eli Luberoff. Desmos Graphing Calculator. https://www.desmos.com/calculator