University of Sussex

Projective Plane Curves

A Dissertation

Presented to the Mathematical and Physical Sciences

School of Sussex University

by

Fatma Karaoglu

Submitted for the degree of Master of Science

University of Sussex

August 2014

Declaration

I hereby declare that this dissertation has not been submitted, either in the same or different form, to this or any other university for a degree.

Signature:

Date:

UNIVERSITY OF SUSSEX

Fatma Karaoglu, Master of Science

Projective Plane Curves

Abstract

Let C' and C'' be two projective curves in $\mathbb{P}_k^2$ such that $\deg(C') = n$ and $\deg(C'') = m$, with n and m positive integers. The curves C' and C'' intersect in at most nm points if they do not have any common factor. Furthermore, C' and C'' meet at exactly nm points if all the intersection points of C' with C'' are non-singular and the tangent lines to C' and C'' at such points are distinct. The above statements are part of the celebrated Bézout's Theorem.

A short historical note is necessary. The theorem was first stated by Isaac Newton. The French mathematician Étienne Bézout (1730–1783) gave a proof of the theorem. It was not the first proof, and it turned out it was not correct. In spite of this, the theorem was given the name of Bézout. The German mathematician Max Noether (1844-1921) added to the original statement of the the condition stating when a projective curve can be expressed in terms of two other projective curves.

The aim of this dissertation is to introduce the proof of Bézout's theorem for projective plane curves. In addition, we give some basic definitions and theorems in algebraic geometry and we investigate another important result, Max Noether's Fundamental Theorem.

To My Grandmother

Acknowledgements

I would like to express my thanks to Prof. James Hirschfeld firstly for giving me valuable guidance throughout this dissertation and for all his patience and advice. I am also appreciate for his remarks and suggestions in regard to typesetting problems in LaTeX.

I would like to thank Pinar Mete who is my ex-supervisor in Turkey for introducing me to the wonderful world of Algebraic Geometry.

My mother Gulsen Aslan and my sister Ayse Karaoglu deserve acknowledgements for their support. They give the meaning of my life. Thanks a bunch.

Many thanks to all of my friends for their support and love especially I thank Isilay Taban for her patience, understanding and sharing.

Lastly, special thanks to Bogdan Vioreanu for his invaluable encouragement throughout the course of my master studies and contribution to my knowledge of mathematics.

Contents

Chapter 1

Introduction

Let k be an algebraically closed field. The affine space $\mathbb{A}_k^n$ is defined as the $n-$cartesian product of k, i.e $\mathbb{A}_k^n$ is the set of n-tuples of elements of k. We usually write $\mathbb{A}^n$ to denote $\mathbb{A}_k^n$ if k is understood.

Let $\mathbb{A}_k^{n+1}$ be the affine $n+1$ space. We define the projective n space over k to be the space of all lines through the origin in $\mathbb{A}_k^{n+1}$; this space is usually denoted by $\mathbb{P}_k^n$.

As is well known, a point different from the origin on a line l passing through the origin in $\mathbb{A}^{n+1}$ uniquely identifies the line l. Let $(x_0, x_1, \ldots, x_n)$ be a nonzero point in $\mathbb{A}^{n+1}$, and let l be the unique line in $\mathbb{A}^{n+1}$ that passes through the origin and the point $(x_0, x_1, \ldots, x_n)$. This immediately implies that each $(\lambda x_0, \ldots, \lambda x_n)$ is on l as well. The line passing through the origin and $(x_0, x_1, \ldots, x_n)$ is denoted by $[x_0 : x_1 : \ldots : x_n]$. Hence, $\mathbb{P}^n$ can be identified with the set of equivalence classes of points in $\mathbb{A}^{n+1}$ under the relation $\sim$ where $a \sim b$ if and only if $a = \lambda b$ for some non-zero λ in k. There is a projection

$$T : \mathbb{A}^{n+1} \setminus (0, \ldots, 0) \longrightarrow \mathbb{P}^n$$

sending each point p in $\mathbb{A}^{n+1}$ to its equivalence class, i.e the line through p and the origin.

A *curve* in the affine plane $\mathbb{A}_k^2$ is defined to be the set of zeros $\{(X, Y)\}$ of a polynomial $f(X, Y)$. Any curve in the affine plane $\mathbb{A}_k^2$ uniquely corresponds to a curve C' in the projective plane $\mathbb{P}_k^2$, where C' can be defined as the set of zeros $\{(x, y, z)\}$ of a homogeneous polynomial $F(x, y, z)$.

In the projective plane we can define the points of $\mathbb{P}_k^2$ with $z = 0$ correspond to ratios $[x : y : 0]$. There is a bijection

$$\mathbb{P}_{\mathbb{R}}^1 \longrightarrow \mathbb{R} \cup \{\infty\}.$$

Hence these points we defined above shape the 'line at infinity'. Therefore we say parallel lines meet at infinity.

A projective curve C' defined by the non-constant homogeneous polynomial $F(x,y,z)$ consists of all zeros of $F(x,y,z)$, that is,

$$C' = \{(x,y,z) \in \mathbb{P}_k^2 : F(x,y,z) = 0\}.$$

In this dissertation we focus on two important results regarding projective plane curves. Firstly, we consider the intersection of two projective curves.

Question 1: In how many points do two projective curves intersect?

The famous theorem of Bézout solves Question 1. This theorem says that the number of intersection points of two projective curves equals the product of the degrees of these curves, counting multiplicities. Secondly, we consider the following question.

Question 2: When can a projective curve be decomposed in terms of two other curves?

Max Noether gave the conditions answering question 2; they are called Noether' s conditions:

Let C', C'' be two curves defining by F, G and they have no common components through $p \in \mathbb{P}_k^2$ and let D be a curve defined by H. If there are a, b in $O_p(\mathbb{P}_k^2)$ such that

$$H_* = aF_* + bG_*$$

then Noether conditions are satisfied at p with respect to C', C'' and D. Here

$$D_* = D(x,y,1), C'_* = C'(x,y,1), C''_* = C''(x,y,1)$$

are the corresponding affine curves defined by $F_*, G_*, H_*,$.

Max Noether' s Fundamental Theorem: Let C' and C'' be two plane curves defined by the polynomials F, G of the degrees m and n. By Bézout' s theorem we know that they intersect in mn points. Assume that D is a curve defined by the polynomials H of degree r such that $H = AF + BG = 0$ where A, B are the polynomials of degrees $r - m$ and $r - n$, respectively. Then the curves D passes through all the intersection points of C', C''.

The thesis is divided as follows.

In Chapter 2 we introduce some basic definitions and results required in the subsequent chapters.

Chapter 3 is devoted to the resultant of two polynomials, which is a very important technical tool in the proof of Bézout' s Theorem. First we give the definition of resultant in one variable, and then in several variables. After defining the resultant, we describe the relation between the resultant and the intersection points of two curves.

In Chapter 4 we give the proof of Bézout' s Theorem, and illustrate some of its applications.

In Chapter 5 we introduce Max Noether' s Fundamental theorem and its applications.

Finally, Chapter 6 contains conclusions.

Chapter 2

Algebraic and Geometrical Preliminaries

In this chapter we introduce the basic definitions and theorems that will come into play in the process of answering the two important questions posed in the introduction.

2.1 Algebraic Preliminaries

From here on we assume that the underlying ring k is commutative, and has multiplicative identity. Let $k[x_1, x_2, \ldots, x_n]$ denote the ring of polynomials in n variables whose coefficients are from the ring k.

Every polynomial f in $k[x_1, x_2, \ldots, x_n]$ can be uniquely written as

$$f(x) = \sum a_{(i)} x^{(i)} \tag{2.1}$$

where $x^{(i)}$ are the monomials with $x = (x_1, x_2, \ldots, x_n)$ and the coefficients $a_{(i)} \in k$.

Definition 2.1.1 *A non-zero polynomial f is called homogeneous of degree d if*

$$f(\mu x) = \mu^d f(x)$$

for all scalars μ. Equivalently, all coefficients a^i are zero apart from monomials of degree d in $f(x) = \sum a_{(i)} x^{(i)}$.

Any polynomial f can be written uniquely as a sum $f = f_0 + f_1 + \cdots + f_n$, where f_i is homogeneous of degree i. If $f_n \neq 0$ then n is the degree of f, and we write $\deg(f) = n$. When $f = f_0$, f is referred to as a constant polynomial; when $f = f_0 + f_1$, f is called linear; when $f = f_0 + f_1 + f_2$, f is a quadratic polynomial.

Lemma 2.1.2 *Let $f(x,y)$ be a non-zero homogeneous polynomial in two variables, with $\deg f = n$. Then f can be factorised as a product of linear polynomials*

$$f(x,y) = \prod_{i=1}^{n}(\alpha_i x + \beta_i y)$$

for some $\alpha_i, \beta_i \in k$. (10)

Proof We have

$$\begin{aligned} f(x,y) &= a_0 x^0 y^n + a_1 x^1 y^{n-1} + a_2 x^2 y^{n-2} + \cdots + a_n x^n y^0 \\ &= \sum_{i=0}^{n} a_i x^i y^{n-i} \\ &= y^d \sum_{i=0}^{d} a_i \left(\frac{x}{y}\right)^i \end{aligned}$$

where $a_0, a_1, \ldots, a_n \in k$ are not all zero. Let e be the largest element of $S = \{0, 1, 2, \ldots, n\}$ such that $a_e \neq 0$. Then g is a polynomial of degree e in one variable $\frac{x}{y}$ such that

$$g\left(\frac{x}{y}\right) = \sum_{i=0}^{n} a_i \left(\frac{x}{y}\right)^i.$$

So it factors as

$$\sum_{i=0}^{n} a_i \left(\frac{x}{y}\right)^i = a_e \prod_{r=1}^{e}\left(\frac{x}{y} - \lambda_r\right)$$

for some $\lambda_1, \lambda_2, \ldots, \lambda_e \in k$. Then

$$\begin{aligned} f(x,y) &= a_e y^d \prod_{r=1}^{e}(\frac{x}{y} - \lambda_r) \\ &= a_e y^{d-e} \prod_{r=1}^{e}(x - \lambda_r y)\,, \end{aligned}$$

and the result follows. □

Proposition 2.1.3 (Fundamental Theorem of Algebra) *Let $f(x)$ be non-zero one variable polynomial with $\deg f = n$ in $\mathbb{C}[x]$. There are exactly n roots of $f(x)$, counting multiplicities. Namely there exist $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{C}$ and $e_1, e_2, \ldots, e_r \in \mathbb{Z}$ such that*

$$f(x) = a_n(x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\cdots(x-\alpha_r)^{e_r}$$

with $e_1 + e_2 + \cdots + e_r = n$ where a_n is the leading coefficient of $f(x)$.

Proof One of the many proofs of this classical result is indicated in detail in (2). □

Definition 2.1.4 *A non-zero polynomial f in $k[x_1, x_2, \ldots, x_n]$ is called irreducible if $f = gh$, where g, h in $k[x_1, x_2, \ldots, x_n]$, implies that either g or h is constant. Otherwise we say f is reducible.*

Example 2.1.5 *Let* $\mathbb{R}[x]$ *be a polynomial ring and*

$$f(x) = 2x^4 + 9x^3 + 5x^2 - 11x + 3.$$

Here, f *is reducible since* f *can be factorised as a product of irreducible polynomials*

$$f(x) = (2x - 1)(x + 3)(x^2 + 2x - 1)$$

, whose degree is at least 1*.*

Example 2.1.6 *Let* $\mathbb{Z}_3[x]$ *be a polynomial ring with* $\mathbb{Z}_3 = \{0, 1, 2\}$ *and*

$$f = x^2 + x + 2.$$

Since f *does not have any root in* $\mathbb{Z}_3$*,* f *is irreducible.*

Definition 2.1.7 *An integral domain* R *is a unique factorization domain (or has a unique factorization), written UFD, if all non-zero* $a \in R$ *can be written uniquely as a product* $a = u \prod {p_i}^{d_i}$ *where* u *is a unit,* d_i *are integers and the* p_i *are irreducible.*

Example 2.1.8 *The rational numbers* $\mathbb{Q}$*, the real numbers* $\mathbb{R}$ *and the complex numbers* $\mathbb{C}$ *are integral domains and also they are all fields. Recall that every non-zero element in a field has an inverse. As is known any field has no irreducible elements so it follows that they are unique factorization domains.*

Theorem 2.1.9 $\mathbb{Z}$ *is a UFD. (2)*

Proof Let $a \in \mathbb{Z}$; by multiplying a by a unit it may be assumed $a > 1$. Let $S(n)$ denote the mathematical statement below, that is,

$$S(a) : a = u \prod {p_i}^{d_i}$$

where u is a unit, d_i are integers and the p_i are irreducible and u, p_i, d_i are unique. Let

$$S = \{a \in \mathbb{Z} : S(a) \, is \, true\}$$

We prove the existence of factorization of a by induction on a. First show that "$S(1)$ is true", i.e. $1 \in S$. The base case is trivial since there are no factors in the product.

Then suppose $S(b)$ is true such that $b < a$, that is every positive b has a unique factorization. Now it is shown that "$S(a)$ is true".

If a is prime, obviously it can be factorized with itself since there is only factor is a.

If $a = nm$ where both n and m are non-unit positive integers. Clearly from the induction hypothesis n and m have factorizations as $n, m < a$ such that

$$n = u' \prod {p_{i_n}}^{d_{in}},$$

$$m = u'' \prod {p_{i_m}}^{d_{im}}.$$

Hence, by combining the factorizations of n and m the factorization of a is obtained below:

$$a = u'u'' \prod {p_{i_n}}^{d_{in}} {p_{i_m}}^{d_{im}}.$$

□

Definition 2.1.10 *R is a Noetherian ring if every ideal of R is finitely generated.*

Theorem 2.1.11 *Hilbert Basis Theorem: If R is a Noetherian ring, then $R[x_1, x_2, \ldots, x_n]$ is a Noetherian ring.*

Proof A proof of this celebrated result can be found, for instance, in (10). □

Definition 2.1.12 *Let k be a field. If every polynomial f in $k[x_1, x_2, \ldots, x_n]$ has at least one root, then k is said to be algebraically closed.*

Example 2.1.13 *It is easy to verify that the field $\mathbb{C}$ is algebraically closed.*

In this dissertation when we speak of field, we mean an algebraically closed field.

Definition 2.1.14 *The derivative of a polynomial $f(x) = \sum a_i x^i$ in $k[x]$ is defined to be*

$$\frac{\partial f}{\partial x} = f_x = \sum i a_i x^{i-1}.$$

If $f \in k[x_1, \ldots, x_n]$,

$$\frac{\partial f}{\partial x_i} = f_{x_i}$$

Theorem 2.1.15 (Euler' s Theorem) *Let f be a polynomial in $k[x_1, x_2, \ldots, x_n]$ and* $\deg(f) = m$. *Then*

$$mf = \sum_{i=1}^{n} x_i f_{x_i}. \quad (10)$$

2.2 Geometrical Preliminaries

This section introduces the required background related to affine and projective planes, and algebraic curves. Furthermore, we describe the relation between the affine and the projective spaces.

Definition 2.2.1 *The affine plane is the 2-dimensional affine space, denoted by* $\mathbb{A}_k^2$.

Definition 2.2.2 *An algebraic set* V *is a set of values that satisfy a system of polynomial equations. More explicitly,*

$$V = \{x \in k^n : f_i(x) = 0\}$$

where k *is a field and* $\{f_i\}$ *is the set of polynomials in* $k[x_1, x_2, \ldots, x_n]$.

If V cannot be written as the union of two algebraic subsets, i.e it is irreducible, then V is an algebraic variety.

Example 2.2.3 *Let* $k = \mathbb{R}$. *Here are some classic example of algebraic sets:*

$$V(y^2 - x(x^2 - 1)) \subset \mathbb{A}^2$$

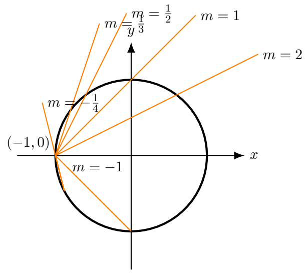
$$V(y^2 - x^2(x + 1)) \subset \mathbb{A}^2$$

Definition 2.2.4 *Let* C *be an algebraic curve defined by* $f(X, Y) = 0$, *where* f *is a non-constant polynomial in two variables. Then* C *consists of all zeros of* $f(X, Y)$. *Formally,*

$$C = \{(X, Y) \in \mathbb{A}_k^2 : f(X, Y) = 0\}$$

When $k = \mathbb{R}$ we shall call C real (algebraic) curves. If $k = \mathbb{C}$ we call C as complex (algebraic) curves.

Example 2.2.5 *The example follows one given in (7). The unit circle* $C : (X^2 + Y^2 = 1)$ *is an algebraic curve. It can be rationally parametrized by one variable. For example,*



The line through the point $(-1, 0)$ *with slope* m *is given by the linear equation* $Y = m(X + 1)$. *The intersection of this line with the unit circle is the another point on unit* *circle, so varying m every point of unit circle is identified. Combining the unit circle $X^2+Y^2=1$ and the line $Y=m(X+1)$ we have the equation,*

$$x^2+(m(x+1))^2=1$$

Then the roots of this equation are $X=-1$ and $X=\frac{1-m^2}{1+m^2}$. It follows that $Y=\frac{2m}{1+m^2}$.

Another example of a parametrised curve is

$$C:(2X^2+Y^2=5Z^2).$$

A parametrisation is $X=\frac{2\sqrt{5}\lambda}{1+2\lambda^2}$ and $Y=\frac{2\lambda^2-1}{1+2\lambda^2}$, for some λ constant.

Definition 2.2.6 *A projective plane consists of the lines of $\mathbb{R}^3$ through origin. It is denoted by $\mathbb{P}^2_{\mathbb{R}}$. Here, $\mathbb{P}^2_{\mathbb{R}}$ is the set of all ordinary points and points at infinity. (5)*

It is also represented by a ratio $x:y:z$ under the relation $\sim$ where $(x,y,z)\sim(\lambda x,\lambda y,\lambda z)$ for which $z\neq 0$ if $\lambda\in\mathbb{R}^3\setminus\{0\}$. We set $X=\frac{x}{z}$ and $Y=\frac{y}{z}$, the equivalence class of (x,y,z) has a unique representative under the relation $\sim$ and the ratio corresponds to just two real numbers. Also $\mathbb{P}^2_{\mathbb{R}}$ has a copy of $\mathbb{R}^2$.

We have the transformation which is from $\mathbb{R}^2$ into $\mathbb{R}^3\setminus\{0\}$ defined by $(X,Y)\to(x,y,1)$.

Definition 2.2.7 *Let $T:\mathbb{P}^n_k\to\mathbb{P}^n_k$ be a bijection induced by some linear isomorphism*

$$\alpha:\mathbb{A}^{n+1}\to\mathbb{A}^{n+1}.$$

Then T is called a projective transformation (or a change of coordinates) of $\mathbb{P}^n_k$.

Consider that for any given $P,Q\in\mathbb{P}^n_k$ there exists a projective transformation from P to Q.

Definition 2.2.8 *A projective curve C' is an algebraic curve in projective plane which is defined by $F(x,y,z)$ where F is non-constant homogeneous polynomial in three variables. More explicitly;*

$$C'=\{(x,y,z)\in\mathbb{P}^2_{\mathbb{R}}:F(x,y,z)=0\}$$

Example 2.2.9 *Let C' and C'' be two projective lines, i.e., C' and C'' be the curves of degree 1. They are defined by linear polynomials F,G such that*

$$F(x,y,z)=a_0x+a_1y+a_2z,\quad (a_0:a_1:a_2)\in\mathbb{P}^2_k$$
$$G(x,y,z)=b_0x+b_1y+b_2z,\quad (b_0:b_1:b_2)\in\mathbb{P}^2_k.$$

These two projective lines always intersect. They intersect exactly at one point if and only if they are different lines. The linear system of equations

$$F(x, y, z) = 0$$

$$G(x, y, z) = 0$$

has exactly one nontrivial solution if and only if $\operatorname{rank} A = 2$ *where* A *is the matrix:*

$$\begin{bmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{bmatrix}$$

Otherwise, $(a_0 : a_1 : a_2) = (b_0 : b_1 : b_2)$*, that is they give the same line.*

The projective curve

$$(C' = \{(x, y, z) \in \mathbb{P}^2_{\mathbb{R}} : F(x, y, z) = 0\})$$

is called conic (respectively conic, cubic, quartic, ...) if the degree of F is 2 (respectively $3, 4, \ldots$)

Definition 2.2.10 *Let* f *be an any polynomial of degree* d *in* $k[x_1, x_2, \ldots, x_n]$*; this polynomial can be written as*

$$f = f_0 + f_1 + \cdots + f_d$$

where each f_i *is a homogeneous polynomial with degree* i*. Define a new polynomial* $f^* \in k[x_1, x_2, \ldots, x_{n+1}]$ *by*

$$f_* = x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \cdots + x_{n+1}^0 f_d$$

where each term is a homogeneous polynomial of degree d*. So* f^* *is a homogeneous polynomial of degree* d*. This procces is called "homogenizing" polynomials in* $k[x_1, x_2, \ldots, x_n]$ *with respect to* x_{n+1}*.*

An example should suffice to explain this. Let

$$f = x^5 + x^3y - 2xy^2 + y^4$$

be an polynomial of degree 5*. Here*

$$f^* = x^5 + x^3yz - 2xy^2z^2 + y^4z$$

is the homogeneous polynomial of degree 5*.*

Conversely, every polynomial $F_* \in k[x_1, x_2, \ldots, x_{n+1}]$ *of degree* d *in* $k[x_1, x_2, \ldots, x_{n+1}]$ *has a dehomogenization obtained by setting*

$$F_* = F(x_1, \ldots, x_n, 1)\,,$$

as defined in (10).

Proposition 2.2.11 *Let F, G, f, g and F_*, G_*, f^*, g^* be as above. Then the following hold:*

(1) $(FG)_* = F_*G_*$ *and* $(fg)^* = f^*g^*$.

(2) *If F be a nonzero polynomial and r be the highest power of x_{n+1} that divides F, then* $x^r_{n+1}(F_*)^* = F$ *and* $(f^*)_* = f$.

(3) $(F + G)_* = F_* + G_*$

(4) $x^t_{n+1}(f+g)^* = x^r_{n+1}f^* + x^s_{n+1}g^*$ *where* $\deg g = r, \deg f = s$ *and* $t = r+s-\deg(f_g)$.

Proof A proof is indicated in (10). □

Homogenization and dehomogenization will allow us to study the relations between affine curves and projective curves.

Hilbert' s Nullstellensatz allows us to verify when two polynomials define the same curve.

Theorem 2.2.12 (Hilbert' s Nullstellensatz) *Let C and C' be two curves defined by $p(x, y)$ and $q(x, y)$, respectively. $C = C'$ if and only if there exist integers $m, n > 0$ such that $p \mid q^n$ and $q \mid p^m$, i.e. the polynomials have same irreducible factors with different scalars.*

Proof A proof can be found in (8). □

There is a correspondence between the inhomogeneous quadratic polynomial $f(X, Y)$ and the homogeneous quadratic polynomial $F(x, y, z)$ such that

$$f(X, Y) = kX^2 + lXY + mY^2 + nX + pY + r$$

$$F(x, y, z) = kx^2 + lxy + my^2 + nxz + pyz + rz^2.$$

Obviously there is a bijection $f \longleftrightarrow F$ given by $f(X, Y) = F(\frac{x}{z}, \frac{y}{z}, 1)$ and conversely; $F = z^2 f(\frac{x}{z}, \frac{y}{z})$.

Definition 2.2.13 *Let C' be a projective curve determined by $F(x, y, z) \in k[x, y, z]$. Consider partial derivatives*

$$F_x = \frac{\partial F}{\partial x}, F_y = \frac{\partial F}{\partial y}, F_z = \frac{\partial F}{\partial z}.$$

The point $p = (a, b, c)$ is called a singular point if

$$F(a, b, c) = F_x(a, b, c) = F_y(a, b, c) = F_z(a, b, c) = 0, \quad (10).$$

Definition 2.2.14 *The tangent line to a curve C' at a non-singular point $(a, b, c) \in C'$ is the line given by*

$$F_x(a, b, c)x + F_y(a, b, c)y + F_z(a, b, c)z = 0, (10).$$

Example 2.2.15 *Let C be an affine curve defined by the polynomial*

$$f(X,Y) = Y^2 - X^3 - X^2$$

and let $p = (0,0)$. The point $p = (0,0)$ is a singular point since $f(0,0) = 0$ and

$$f_X(X,Y) = -3x^2 - 2X \Rightarrow f_X(0,0) = 0$$
$$f_Y(X,Y) = 2Y \Rightarrow f_Y(0,0) = 0\,.$$

The lowest order homogeneous polynomial within f shows which lines are tangent lines to the curve C at $(0,0)$. The lowest order homogeneous polynomial is

$$Y^2 - X^2 = (Y - X)(Y + X).$$

The lines $Y + X$ and $Y - X$ are the tangent lines to C at $(0,0)$. The tangent line $Y + X$ can be seen in the figure below:

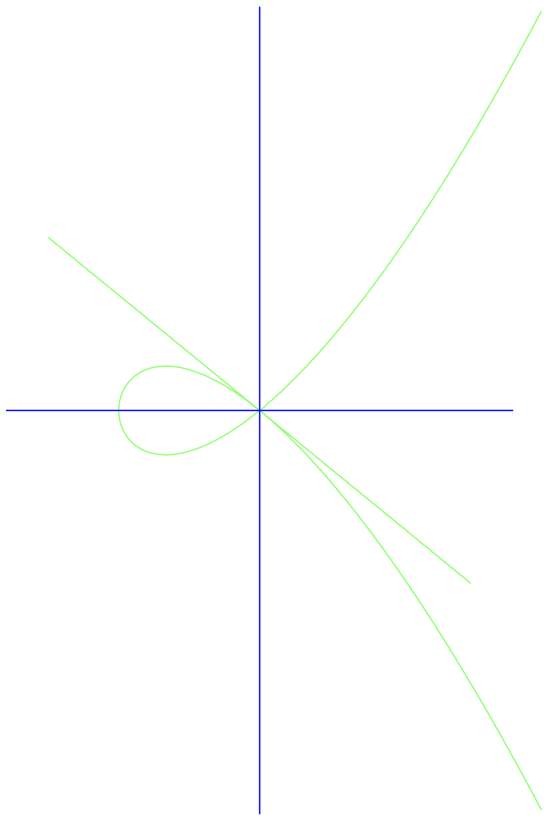


Figure 2.1: *The line $Y + X$ is tangent to the curve $Y^2 - X^3 - X^2$ at the origin*

Chapter 3

Intersection of Projective Curves

Consider the intersection of two algebraic curves which are given by F, Q. These intersection points are related to common solutions of the polynomials F, Q. To be able to solve this system of equations, it is needed to introduce the resultant of two polynomials.

3.1 The Geometric Idea

Let C' and C'' be two curves in $\mathbb{P}^2_k$ and defined by $F(x, y, z)$ and $G(x, y, z)$ where F and G are non-constant homogeneous polynomials in $k[x, y, z]$ such that $\deg F = s$, $\deg G = t$. Assume that the point $[0 : 0 : 1]$ belongs to neither C' nor C''. Then we have;

$$F(x, y, z) = z^s + a_1 z^{s-1} + \ldots + a_{s-1} z + a_s,$$

$$G(x, y, z) = z^t + a_1 z^{t-1} + \ldots + a_{t-1} z + a_t$$

where a_i and b_j are homogeneous polynomials in $k[X, Y]$ of degrees i and j, respectively.

Assume that $[X : Y : Z]$ is a intersection point. Then $F(X, Y, z)$ and $G(X, Y, z)$ have the common root $z = Z$, so by Corollary 3.1.5 the resultant $Res_{F,G}$ must vanish for $(x, y) = (X, Y)$. More explicitly, the intersection points of C' and C'' can be verified by the zeros of the resultant $Res_{F,G}$. (1)

The next two sections, we will give some properties and definitions about the resultant in order to find the intersection points of two curves. First of all, we will study very basic case on one variable field in the section 3.2. Then we generalise for two variables in the section 3.3.

3.2 Resultants in One Variable

Let k be an algebraically closed field and $k[x]$ denotes the ring of polynomials in one variable whose coefficients are from k.

Definition 3.2.1 *Let f, g be two polynomials of degrees s, t in $k[x]$.*

$$f(x) = a_0x^s + a_1x^{s-1} + a_2x^{s-2} + \cdots + a_s\ ,\ \ (a_0 \neq 0)$$
$$g(x) = b_0x^t + b_1x^{t-1} + b_2x^{t-2} + \cdots + b_t\ ,\ \ (b_0 \neq 0)\,.$$

Then the resultant of polynomials f, g is given by the determinant of the matrix:

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_s & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_{s-1} & a_s & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & a_s \\ b_0 & b_1 & \cdots & b_t & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & b_{t-1} & b_t & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & b_t \end{bmatrix}$$

where the matrix is $(s+t)\times(s+t)$ and the matrix is constituted by shifting $(a_0, a_1, a_2, \ldots, a_s)$ for the first t rows and for the last s rows by shifting $(b_0, b_1, b_2, \ldots, b_t)$. The resultant of two polynomials f, g is written as $Res_{f,g}$. (1)

Example 3.2.2 *Let f, g be polynomials in $\mathbb{R}[x]$ such that*

$$f(x) = a_0x^3 + a_1x^2 + a_2x + a_3\ ,\ \ \deg f(x) = 3$$
$$g(x) = b_0x^2 + b_1x + b_2\ ,\ \ \deg g(x) = 2\,.$$

The resultant of polynomials f, g is given by:

$$Res_{f,g} = \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{vmatrix}$$

Lemma 3.2.3 *Let k be a UFD and $f(x), g(x)$ be polynomials in $k[x]$ with $\deg f = s$, $\deg g = t$. Then $gcd(f(x), g(x)) \neq 1$ if and only if there exist non-zero polynomials $p(x), q(x)$ with $\deg p < s$ and $\deg q < t$ such that $fq = pg$.*

Proof Suppose $gcd(f, g) = h \neq 1$, i.e., there exist $0 \neq p(x)$, $0 \neq q(x)$ polynomials such that $f = hp$ and $g = hq$. Since $\deg h \geq 1$, $\deg p < s$ and $\deg g < t$. It is also clear that these polynomials p, q satisfy the relation $fq = gp$.

Conversely, suppose there are $p(x), q(x)$ polynomials such that $fq = pg$. All these polynomials can be uniquely factorized into irreducible factors. The factors of $q(x)$ cannot cover all factors of $g(x)$ because $\deg q < \deg g$, so g and f have at least one same factor. Therefore, $gcd(f, g) \neq 1$. □

Example 3.2.4 *Let f, g be polynomials in $\mathbb{R}[x]$ such that*

$$\begin{aligned} f(x) &= x^6 - 7x^5 + 4x^4 - 27x^3 - 7x^2 + 4x - 28 \\ &= (x^2+4)(x-7)(x^3+1) \\ g(x) &= x^7 + 4x^5 + x^2 + 4 \\ &= (x^2+4)(x^5+1)\,. \end{aligned}$$

We have $gcd(f, g) = x^2 + 4$, then,

$$\begin{aligned} p(x) &= x^4 - 7x^3 + x - 7 \\ &= (x-7)(x^3+1) \\ q(x) &= x^5 + 1\,. \end{aligned}$$

Therefore, these polynomials p, q satisfy the equation $fq = pg$.

Corollary 3.2.5 *The polynomials $f(x), g(x)$ have a common non-constant factor, i.e., $gcd(f, g) \neq 1$ if and only if $Res_{f,g} = 0$. Equivalently, $gcd(f, g) = 1 \iff Res_{f,g} \neq 0$. (1)*

Proof We would like to show that

$$\begin{aligned} Res_{f,g} = 0 &\iff gcd \neq 1 \\ &\iff \exists p, q \; with \; fq = pg\,. \end{aligned}$$

Set;

$$\begin{aligned} p(x) &= c_1x^{s-1} + c_2x^{s-2} + \ldots + c_s\,, \;\; (c_1 \neq 0) \\ q(x) &= d_1x^{t-1} + d_2x^{t-2} + \ldots + d_t\,, \;\; (d_1 \neq 0)\,. \end{aligned}$$

The equation $fq = pg$ implies that

$$a_0d_1x^{s+t-1} + (a_0d_2 + a_1d_1)x^{s+t-2} + (a_0d_3 + a_1d_2 + a_2d_1)x^{s+t-3} + \ldots + a_sd_t =$$

$$b_0c_1x^{s+t-1} + (b_0c_2 + b_1c_1)x^{s+t-2} + (b_0c_3 + b_1c_2 + b_2c_1)x^{s+t-3} + \ldots + b_tc_s$$

the relation $fq = pg$ is equivalent to the following linear system of $(s+t)$ equations in the $s+t$ unknowns $c_1, c_2, \ldots, c_s, d_1, d_2, \ldots, d_t$:

$$a_0 d_1 = b_0 c_1$$
$$a_1 d_1 + a_0 d_2 = b_1 c_1 + b_0 c_2$$
$$a_2 d_1 + a_1 d_2 + a_0 d_3 = b_2 c_1 + b_1 c_2 + b_0 c_3$$
$$\vdots = \vdots$$
$$a_s d_t = b_t c_s\,.$$

There exist non zero polynomials $p(x), q(x)$ satisfying the equation $fq = pg$ if and only if this linear system of equation has non-trivial solution if and only if the determinant of the matrix which is comprised of the coefficients of each equations vanishes. Multiplying available columns by -1 and transposing, the resultant matrix is obtained. □

Example 3.2.6 *Let f, g be two polynomials in $\mathbb{R}[x]$.*

$$f(x) = x^2 - 1\,,\ \ \deg f = 2$$
$$g(x) = x + 1\,,\ \ \deg g = 1\,.$$

It is clear that the polynomials f, g have a common non-constant factor $(x+1)$. The resultant of these polynomials as below:

$$Res_{f,g} = \begin{vmatrix} 1 & 0 & -1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{vmatrix}$$

As a result, $Res_{f,g} = 1 - 1 = 0$ as required in Corollary 3.2.5.

3.3 Resultants in Two Variables

Let C and D be two plane curves defined by $f(X, Y), g(X, Y)$ of degrees s, t, respectively. Let C' and C'' be two projective curves defined by $F(x, y, z), G(x, y, z)$ of degrees m, n. In this section, we define the resultant of polynomials $f(X, Y), g(X, Y)$ fistly. Then we define the resultant of homogeneous polynomials $F(x, y, z), G(x, y, z)$ and give some important tools to prove Bézout' s Theorem.

Definition 3.3.1 *Let $f(X,Y)$ and $g(X,Y)$ be two polynomials such that*

$$f(X,Y) = f_0(X)Y^s + f_1(X)Y^{s-1} + f_2(X)Y^{s-2} + \ldots + f_s(X)$$
$$g(X,Y) = g_0(X)Y^t + g_1(X)Y^{t-1} + g_2(X)Y^{t-2} + \ldots + g_t(X)\,.$$

Then the resultant of polynomials f, g is given by:

$$Res^Y_{f,g}(X) = \begin{vmatrix} f_0(X) & f_1(X) & \cdots & f_s(X) & 0 & \cdots & 0 \\ 0 & f_0(X) & \cdots & f_{s-1}(X) & f_s(X) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & f_s(X) \\ g_0(X) & g_1(X) & \cdots & g_t(X) & 0 & \cdots & 0 \\ 0 & g_0(X) & \cdots & g_{t-1}(X) & g_t(X) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & g_t(X) \end{vmatrix}$$

where the first t rows of the matrix consist of shifts of $(f_0(X), f_1(X), \ldots, f_s(X))$ and the last s rows of it consist of shifts $(g_0(X), g_1(X), \ldots, g_t(X))$ and is written as $Res^Y_{f,g}(X)$

Example 3.3.2 *Let f, g be polynomials in $k[X,Y]$ such that;*

$$\begin{aligned} f(X,Y) &= X^2 - 2XY + 3X = -2XY + X^2 + 3X \\ &= f_0(X)Y + f_1(X), \quad s = 1 \\ g(X,Y) &= Y^2 - 4X \\ &= g_0(X)Y^2 + 0Y + g_2(X), \quad t = 2\,. \end{aligned}$$

The resultant $Res^Y_{f,g}$ of polynomials f, g is as follows:

$$Res^Y_{f,g}(X) = \begin{vmatrix} -2X & X^2+3X & 0 \\ 0 & -2X & X^2+3X \\ 1 & 0 & -4X \end{vmatrix}$$

$Res^Y_{f,g} = X^2(X^2 - 10X + 9)$

$$\begin{aligned} f(X,Y) &= X^2 - 2XY + 3X = X^2 + (3-2Y)X + 0 \\ &= f_0(Y)X^2 + f_1(Y)X + 0, \quad s = 2 \\ g(X,Y) &= Y^2 - 4X = -4X + Y^2 \\ &= g_0(Y)X + g_1(Y), \quad t = 1\,. \end{aligned}$$

The resultant $Res^{X}_{f,g}$ *of polynomials* f, g *is as follows:*

$$Res^{Y}_{f,g}(X) = \begin{vmatrix} 1 & 3-2Y & 0 \\ -4 & Y^2 & 0 \\ 0 & -4 & Y^2 \end{vmatrix}$$

$Res^{X}_{f,g} = Y^2(Y^2 - 8Y + 12)$

Theorem 3.3.3 $gcd_Y(f, g) \in k[X] \iff Res^{Y}_{f,g}(X) = 0$

Proof The proof follows one given from Corollary 3.2.5. □

Theorem 3.3.4 *Assume that* $(f_0(a), g_0(a)) \neq (0, 0)$ *and* $(f_0(b), g_0(b)) \neq (0, 0)$*. There is a solution* (a, b) *of the system;*

$$f(X, Y) = 0$$
$$g(X, Y) = 0\,.$$

if and only if $Res^{Y}_{f,g}(a) = 0$*,* $Res^{X}_{f,g}(b) = 0$ *and* $(f_0(a), g_0(a)) \neq (0, 0)$*,* $(f_0(b), g_0(b)) \neq (0, 0)$*.*

Proof The proof is given in (9). □

Example 3.3.5 *Recall the polynomials* f, g *in Example* 3.3.2*. In order to find the common factor of* f, g*, the solution of the system* (a, b) *should be verified using the Theorem* 3.3.4*. Recall that;*

$$\begin{aligned} Res^{Y}_{f,g}(X) &= X^2(X^2 - 10X + 9) \\ Res^{Y}_{f,g}(a) &= a^2(a^2 - 10a + 9) = a^2(a-1)(a-9) = 0 \\ &\Rightarrow a = 0, 1, 9 \\ Res^{X}_{f,g}(Y) &= Y^2(Y^2 - 8Y + 12) \\ Res^{X}_{f,g}(b) &= b^2(b^2 - 8b + 12) = b^2(b-2)(b-6) = 0 \\ &\Rightarrow b = 0, 2, 6\,. \end{aligned}$$

The pairs of possible solutions of the system:

$$(0, 0), (0, 2), (0, 6), (1, 0), (1, 2), (1, 6), (9, 0), (9, 2), (9, 6)$$

It is easy to find that the solutions are only

$$(0, 0), (1, 2), (9, 6).$$

Definition 3.3.6 *Let F and G be two homogeneous polynomials in $k[x,y,z] = (k[y,z])[x]$ with $\deg F = m$ and $\deg G = n$ such that*

$$F(x,y,z) = F_0(y,z)x^m + F_1(y,z)x^{m-1} + F_2(y,z)x^{m-2} + \ldots + F_{m-1}(y,z)x + F_m(y,z),$$

$$G(x,y,z) = G_0(y,z)x^n + G_1(y,z)x^{n-1} + G_2(y,z)x^{n-2} + \ldots + G_{n-1}(y,z)x + G_n(y,z),$$

where $F_i(y,z)$, $G_j(y,z)$ are the homogeneous polynomials in $k[y,z]$ and the degrees of $F_i(y,z)$, $G_j(y,z)$ are i,j, respectively. Then, the resultant of F,G is a polynomial in $k[y,z]$ as below:

$$Res(y,z) = \begin{vmatrix} F_0(y,z) & F_1(y,z) & \cdots & F_m(y,z) & 0 & \cdots & 0 \\ 0 & F_0(y,z) & \cdots & F_{m-1}(y,z) & F_m(y,z) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & F_m(y,z) \\ G_0(y,z) & G_1(y,z) & \cdots & G_n(y,z) & 0 & \cdots & 0 \\ 0 & G_0(y,z) & \cdots & G_{n-1}(y,z) & G_n(y,z) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & G_n(y,z) \end{vmatrix}$$

It is denoted by $Res^x_{F,G}(y,z)$ or more simply $Res(y,z)$.

Example 3.3.7 *Let $f(X,Y) = Y - X^2 + 1$ and $g(X,Y) = Y - X^2 - 1$ be two parabolas in $\mathbb{C}^2$. The corresponding conics in $\mathbb{P}^2_{\mathbb{C}}$ are*

$$F(x,y,z) = yz - x^2 + z^2,$$

$$G(x,y,z) = yz - x^2 - z^2.$$

More explicitly,

$$\begin{aligned} F(x,y,z) &= z^2 + yz^1 - x^2z^0 \\ &= F_0(x,y)z^2 + F_1(x,y)z^1 + F_2(x,y)z^0 \\ G(x,y,z) &= -z^2 + yz^1 - x^2z^0 \\ &= G_0(x,y)z^2 + G_1(x,y)z^1 + G_2(x,y)z^0 \end{aligned}$$

They are irreducible polynomials and the point $[0:0:1]$ does not belong to any of these polynomials. The resultant of the polynomials F,G with respect to z is

$$Res(x,y) = \begin{vmatrix} 1 & y & -x^2 & 0 \\ 0 & 1 & y & -x^2 \\ -1 & y & -x^2 & 0 \\ 0 & -1 & y & -x^2 \end{vmatrix}$$

Therefore, $Res^z_{F,G} = Res(x, y) = 4x^4$.

Proposition 3.3.8 *Let* $F(x, y, z)$ *and* $G(x, y, z)$ *be two homogeneous polynomial in* $k[x, y, z]$ *and the leading coefficients of* x *are constants, i.e.,* $F(1, 0, 0) \neq 0$ *and* $G(1, 0, 0) \neq 0$. *Then,* $gcd(F, G) = H$ *where* H *is non-constant homogeneous if and only if the resultant of these polynomials vanish, i.e.,* $Res(y, z) = 0$.

Proof $Res^x_{F,G} = Res(y, z) = 0$

$\iff$ $F(x, y, z)$ and $G(x, y, z)$ have a common factor in $(k(y, z))[x]$ (By Corollary 3.2.5.)

$\iff$ $F(x, y, z)$ and $G(x, y, z)$ have a common factor in $(k[y, z])[x]$ (By Gauss Lemma.)

$\iff$ $F(x, y, z)$ and $G(x, y, z)$ have a common factor in $k[x, y, z]$.

Additionally, this common factor is homogeneous since every factor of homogeneous polynomial is homogeneous. □

Lemma 3.3.9 *Let* $F(x), G(x)$ *are two polynomials in* $k[x]$ *such that*

$$F(x) = (x - \lambda_1)(x - \lambda_2) \dots (x - \lambda_m),$$

$$G(x) = (x - \mu_1)(x - \mu_2) \dots (x - \mu_n)$$

where $\lambda_1, \dots, \lambda_m, \mu_1, \dots, \mu_n \in k$, *then the resultant of the polynomials* F, G *is*

$$Res_{F,G} = \prod (\mu_j - \lambda_i).$$

Particularly,

$$Res_{F,GH} = Res_{F,G} Res_{F,H}$$

where F, G *and* H *are polynomials in* $k[x]$.

The result is also true when F, G *and* H *are polynomials in* $k[x, y, z]$.

Proof [Geunho Gim, p:4] □

Proposition 3.3.10 *Let* F, G *be two homogeneous polynomials of degrees* m, n*, respectively. Then the resultant* $Res(y, z)$ *of the polynomials* F, G *with respect to* x *is a homogeneous polynomial of degree* mn *in* $k[y, z]$. *(4)*

Proof Recall that $Res(y, z)$ is the determinant of a $(m + n) \times (m + n)$ matrix. Let R be a $(m + n) \times (m + n)$ matrix such that $Res(y, z) = |R|$. Here,

$$R = [r_{ij}]_{(m+n)\times(m+n)}.$$

Due to the fact that F, G are homogeneous polynomials, r_{ij} is a homogeneous polynomial in $k[y, z]$ of degree d_{ij} where r_{ij} is the ijth entry of R. Owing to the definition of $Res(y, z)$ and constructing of the matrix R, the degree of r_{ij} is given by;

$$\{ \begin{array}{ll} m+i-j, & 1 \leq i \leq n \\ i-j & n+1 \leq i \leq m+n. \end{array}$$

Let κ be a permutation of $\{1, 2, \ldots, n+m\}$. Then, $Res(y, z)$ is a sum of terms of the form $\prod_{i=1}^{n+m} r_{i\kappa(i)}$. $Res(y, z)$ is a homogeneous polynomial since every $r_{i\kappa(i)}$ is a homogeneous polynomial in $k[y, z]$. Now, it will be shown that the degree of the homogeneous polynomial $Res(y, z)$ is mn.

Each summand $\prod r_{i\kappa(i)}$ has degree

$$\begin{aligned}
\sum_{i=1}^{m+n} d_{i\kappa(i)} &= \sum_{i=1}^{n}(m+i-\kappa(i)) + \sum_{i=n+1}^{m+n}(i-\kappa(i)) \\
&= \sum_{i=1}^{n} m + \sum_{i=1}^{n} i - \sum_{i=1}^{n} \kappa(i) + \sum_{i=n+1}^{m+n} i - \sum_{i=n+1}^{m+n} \kappa(i) \\
&= mn + \sum_{i=1}^{n} i + \sum_{i=n+1}^{m+n} i - (\sum_{i=1}^{n} \kappa(i) + \sum_{i=n+1}^{m+n} \kappa(i)) \\
&= mn + \sum_{i=1}^{m+n} i - \sum_{i=1}^{m+n} \kappa(i) \\
&= mn
\end{aligned}$$

Namely; $Res(y, z)$ has degree mn. □

Example 3.3.11 *Let $F(x, y, z)$ be unit circle*

$$x^2 + y^2 - z^2,$$

and $G(x, y, z)$ be the cubic

$$x^3 - x^2 z - xz^2 + z^3 - y^2 z.$$

Clearly; $[0 : 0 : 1]$ is on neither of these curves. The resultant of the polynomials F, G with respect to z is :

$$\begin{aligned}
F(x, y, z) &= x^2 + y^2 - z^2 \\
&= F_0(x, y)z^0 + 0z^1 + F_2(x, y)z^2 \\
G(x, y, z) &= x^3 - (x^2 + y^2)z + -xz^2 + z^3 \\
&= G_0(x, y) + G_1(x, y)z + G_2(x, y)z^2 + G_3(x, y)z^3
\end{aligned}$$

Here, $m = 2$, $n = 3$.

$$Res(x,y) = \begin{vmatrix} x^2+y^2 & 0 & -1 & 0 & 0 \\ 0 & x^2+y^2 & 0 & -1 & 0 \\ 0 & 0 & x^2+y^2 & 0 & -1 \\ x^3 & -x^2-y^2 & -x & 1 & 0 \\ 0 & x^3 & -x^2-y^2 & -x & 1 \end{vmatrix}$$

$Res^z_{F,G} = Res(x,y) = -x^2y^4$. There are two possibilities either $x = 0$ or $y = 0$.

First case: $x = 0$;

$$F(0,y,z) = y^2 - z^2 = 0$$
$$G(0,y,z) = z(y^2 - z^2) = 0\,.$$

Hence, the solutions of the system equation $[0 : 1 : 1]$ and $[0 : -1 : 1]$.

Similarly, second case: $y = 0$;

$$F(x,0,z) = x^2 - z^2 = 0$$
$$G(x,0,z) = x^3 - x^2z - xz^2 + z^3$$
$$= (x-z)(x^2 - z^2) = 0\,.$$

Moreover, this system of equation gives the points $[1 : 0 : 1]$ and $[-1 : 0 : 1]$. Here, four intersection points are obtained in the affine plane which are

$$(0,1), (0,-1), (1,0), (-1,0).$$

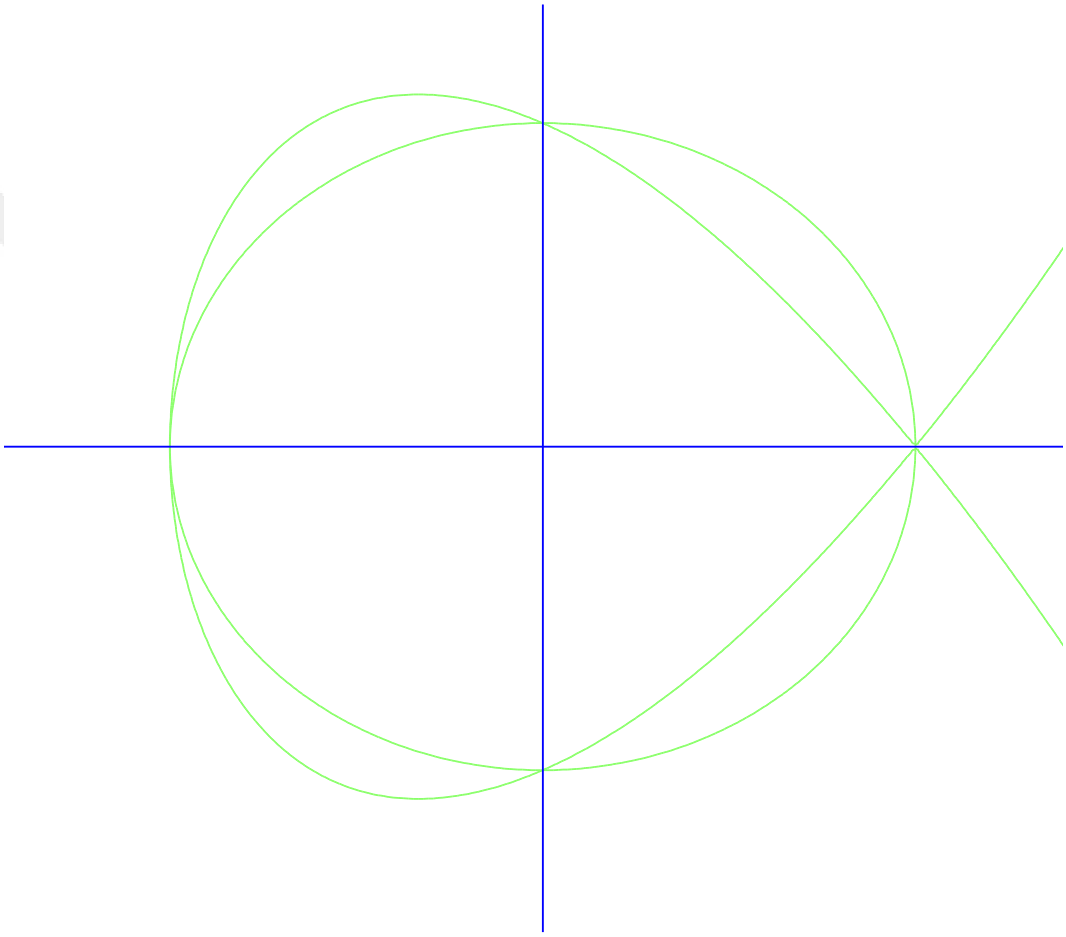


Figure 3.1: *The intersection of* $X^2 + Y^2 = 1$ *and* $Y^2 = X^3 - X^2 - X + 1$

Chapter 4

Bézout' s Theorem and Its Applications

4.1 The Proof of Bézout' s Theorem

Theorem 4.1.1 *Let C' and C'' be two projective curves in $\mathbb{P}_k^2$. They intersect in at least one point.*

Proof Let C' and C'' defined by homogeneous polynomials $F(x, y, z)$ and $G(x, y, z)$. Since $\deg F = m$ and $\deg G = n$ by Proposition 3.3.10 the resultant $Res(y, z)$ of F, G is a homogeneous polynomial of degree mn in $k[y, z]$. By Lemma 2.1.2 $Res(y, z)$ can be factorised of linear polynomials $\gamma y - \beta z$ where $\gamma, \beta \in k$, not both zero. In the case of $y = \beta$ and $z = \gamma$ the resultant vanishes, i.e., the resultant of $F(x, \beta, \gamma)$ and $G(x, \beta, \gamma)$ is zero ($Res(\beta, \gamma) = 0$). From Corollary 3.2.5 these polynomials have a common non-constant factor $\alpha \in k$. Then,

$$F(\alpha, \beta, \gamma) = 0 = G(\alpha, \beta, \gamma).$$

Furthermore, $[\alpha, \beta, \gamma]$ is the point where these two curves intersect. □

Theorem 4.1.2 (Weak Form of Bézout' s Theorem) *Let C' and C'' be two projective curves in $\mathbb{P}_k^2$ of degrees m, n. Assume that they do not have any common component, then they have at most mn intersection points. Equivalently; if C' and C'' have more than mn distinct points in common, then they have a common component. (4)*

Proof Suppose that the curves have more than mn distinct points in common, i.e. C' and C'' have at least $mn + 1$ intersection points. Let S be the set of $mn + 1$ points of intersection of C' and C''.

Choose the point with coordinates $[1:0:0]$ is not collinear with any two distinct points of S, that is $[1:0:0]$ does not lie on any of the finitely many lines in $\mathbb{P}^2_k$ passing through two distinct points of S. Also $[1:0:0]$ does not belong to C' or C''.

Let C' and C'' be defined by homogeneous polynomials $F(x,y,z)$ and $G(x,y,z)$ such that

$$F(x,y,z) = z^m + F_1(x,y)z^{m-1} + F_2(x,y)z^{m-2} + \ldots + F_{m-1}(x,y)z + F_m(x,y) = 0,$$

$$G(x,y,z) = z^n + G_1(x,y)z^{n-1} + G_2(x,y)z^{n-2} + \ldots + G_{n-1}(x,y)z + G_n(x,y) = 0,$$

where the $F_i(x,y)$ and $G_i(x,y)$ are homogeneous polynomials of degree i in $k[x,y]$ and since $[1:0:0]$ is not on the one of the curves

$$F(1,0,0) \neq 0 \neq G(1,0,0).$$

Let $[a:b:c]$ be the point of intersection in S. We have

$$F(a,b,c) = G(a,b,c) = 0.$$

Then, consider the polynomials $F(x) = F(x,b,c)$ and $G(x) = G(x,b,c)$. They have a common root a so by Corollary 3.2.5 the resultant of $F(x)$ and $G(x)$ is zero. Therefore

$$bz - cy \mid Res(y,z).$$

If $[a':b':c']$ is different point from the intersection point $[a:b:c]$, then $b'z - c'y$ is not a scalar multiple of $bz - cy$ because if so $[1:0:0]$, $[a:b:c]$ and $[a':b':c']$ would be collinear, that is, they would all lie on the line in $\mathbb{P}^2_k$ defined by

$$bz = cy,$$

contradicting the choice of coordinates $[1:0:0]$.

So, $mn+1$ distinct factor divide $Res(y,z)$. By Proposition 3.3.10 $Res(y,z)$ is a homogeneous polynomial of degree mn in $k[y,z]$. It follows that $Res(y,z)$ must vanish completely. C' and C'' have a common component by Proposition 3.3.8. □

Theorem 4.1.3 (Bézout' s Theorem) *Let C' and C'' be two projective curves in $\mathbb{P}^2_k$ of degrees m,n and assume that they have no common factor then they exactly intersect at mn distinct points counting multiplicities; i.e.*

$$\sum_{p \in C' \cap C''} I_p(C',C'') = mn, \quad (10)$$

Before we prove the stronger form of Bézout' s Theorem, first it must be defined the intersection multiplicity $I_p(C', C'')$ of two curves C' and C'' at a point $p = [a : b : c]$ in $\mathbb{P}^2_k$. Before we give the definition of the intersection number of C' and C'' at p, we will list some properties which the intersection number has to have. Then we conclude with one definition.

Theorem 4.1.4 *There is a unique intersection multiplicity $I_p(C', C'')$ defined for all projective curves C' and C'' in $\mathbb{P}^2_k$ satisfying the following properties* $(1) - (9)$.

(1) $I_p(C', C'') \geq 0$ *for any* C', C'' *and* p *such that* C' *and* C'' *intersect properly at* p, *that is,* C' *and* C'' *have no common component that passes through* p. *Otherwise*

$$I_p(C', C'') = \infty.$$

(2) $I_p(C', C'') = 0 \iff p \notin C' \cap C''$. $I_p(C', C'')$ *depends on the components of* C' *and* C'' *that pass through* p. $I_p(C', C'') = 0$ *if either* C' *or* C'' *is a non-zero constant.*

(3) *If* $\alpha(q) = p$ *where* α *is an affine change of coordinates on* $\mathbb{A}^2_k$, *then*

$$I_p(C', C'') = I_q(C' \circ \alpha, C'' \circ \alpha).$$

(4) $I_p(C', C'') = I_p(C'', C')$.

(5) $I_p(C', C'') \geq m_p(C')m_p(C'')$ *if and only if* C' *and* C'' *have no common tangent lines at* p.

(6) *The intersection number should add when it is taken unions of curves.*

(7) *If* C' *and* C'' *are defined by homogeneous polynomials* $F(x, y, z)$ *and* $G(x, y, z)$ *of degrees* m *and* n *and* E *is defined by* $FH + G$ *where* $H(x, y, z)$ *is homogeneous polynomials of degree* $n - m$ *then,*

$$I_p(C', C'') = I_p(C', E).$$

(8) *If* $gcd(C', C'') = 1$ *then,*

$$\sum_p I_p(C', C'') = dim_k(k[X, Y] \setminus (C', C'')).$$

(9) *If* p *is a non-singular point on* C' *then,*

$$I_p(C', C'') = ord_p^{C'}(C'').$$

Proof The proof can be found in (4). □

Definition 4.1.5 *Let* C' *and* C'' *be two projective curves and* p *belongs to* $\mathbb{P}^2_k$. *Then, the intersection number of* C' *and* C'' *is defined to be*

$$dim_k(O_p(\mathbb{P}^2) \setminus (C', C''))$$

where $O_p(\mathbb{P}^2_k)$ *is the set of rational functions on* $\mathbb{P}^2_k$ *which are defined at* p.

Equivalently, let $p = [a : b : c]$ *be point of intersection of the curves* C', C''. *The intersection multiplicity* $I_p(C', C'')$ *of* C', C'' *at any point* p *is the largest integer* k *such that* $(bz - cy)^k \mid Res(y, z)$.

Example 4.1.6 *The example follows one in (3).*

Let C *and* D *be two curves given by the polynomials*

$$f(X,Y) = (X^2 + Y^2)^2 + 3X^2Y - Y^3$$
$$g(X,Y) = (X^2 + Y^2)^3 - 4X^2Y^2$$

and let $p = (0,0)$. *By property* (7) g *can be written as*

$$\begin{aligned} g - (X^2 + Y^2)f &= Y((X^2 + Y^2)(Y^2 - 3X^2) - 4X^2Y) \\ &= YA \end{aligned}$$

where $A = (X^2 + Y^2)(Y^2 - 3X^2) - 4X^2Y$. *Here, by using property* (6) *it will be seen as below:*

$$I_p(C, D) = I_p(C, Y) + I_p(C, A).$$

A *can be written as*

$$\begin{aligned} A + 3f &= Y(5X^2 - 3Y^2 + 4Y^3 + 4X^2Y) \\ &= YB \end{aligned}$$

where $B = 5X^2 - 3Y^2 + 4Y^3 + 4X^2Y$. *So*

$$I_p(C, A) = I_p(C, Y) + I_p(C, B).$$

By applying the properties (6) *and* (7), *we will reach that*

$$I_p(C, Y) = I_p(X^4, Y) = 4.$$

Since C *and* B *do not have any common tangent lines at* $p = (0,0)$,*the property* (5) *can be applied. Hence,*

$$I_p(C, B) = m_p(C)m_p(B) = 6$$

where m_p *denotes multiplicity. As a result;*

$$\begin{aligned} I_p(C, D) &= I_p(C, Y) + I_p(C, A) \\ &= I_p(C, Y) + I_p(C, Y) + I_p(C, B) \\ &= 2I_p(C, Y) + I_p(C, B) \\ &= 8 + 6 \\ &= 14\,. \end{aligned}$$

Proof of Theorem 4.1.3 [Bézout' s Theorem]: Recall that two plane curves with no common components have a finite number of intersection points. We may assume that there does not exist any point which lies on a line at infinity ($\{[x : y : 0] \in \mathbb{P}^2\}$) by a projective change of coordinates. Recall the intersection number of C' and C'' at p is given by

$$I_p(C', C'') = dim_k(O_p(\mathbb{P}^2) \setminus (C', C'')).$$

The map $\alpha : k(V*) \to k(V)$ induces an isomorphism from $O_p(\mathbb{P}^2)$ to $O_p(\mathbb{A}^2)$ for the point of intersection p since $\mathbb{P}^2$ is the projective closure of $\mathbb{A}^2$ over k. Note that $\alpha(C') = C'_*$ and $\alpha(C'') = C''_*$ where C'_* and C''_* are the corresponding affine curves with $C'_* = C'(x, y, 1)$ and $C''_* = C''(x, y, 1)$. Therefore,

$$\begin{aligned} I_p(C', C'') &= dim_k(O_p(\mathbb{P}^2) \setminus (C'_*, C''_*)) \\ &= dim_k(O_p(\mathbb{A}^2) \setminus (C'_*, C''_*)) \\ &= I_p(C'_*, C''_*) . \end{aligned}$$

On the other hand, the intersection number of C'_* and C''_* is defined by

$$dim_k(k[X, Y] \setminus (C'_*, C''_*)).$$

Let $R = k[x, y, z]$, $\Gamma = k[x, y, z] \setminus (C', C'')$ and $\Gamma_* = k[X, Y] \setminus (C'_*, C''_*)$ and let Γ_d and R_d be the vector space of homogeneous polynomials of degree d in Γ and R. In order to prove this theorem, it will be enough to show that

$$dim\Gamma_* = dim\Gamma_d = mn$$

for d sufficiently large.

The proof will be proceed in steps. The first step shows that

$$dim\Gamma_d = mn$$

for all $d \geq m + n$. Let the map $\beta : \Gamma \to \Gamma$ be defined by

$$\beta(\overline{H}) = \overline{zH}$$

where the bar denotes the image of H under the natural projection $\pi : R \to \Gamma$. In step 2, it will be shown that the map β is injective. In the last step, it will be proved that

$$dim\Gamma_* = dim\Gamma_d$$

for all $d \geq m + n$.

Step 1 :

Let $\pi : R \to \Gamma$ be the natural projection homomorphism and $\varphi : R \times R \to R$ be the map which is given by

$$\varphi(A, B) = AC' + BC''$$

and $\psi : R \to R \times R$ be defined by

$$\psi(C) = (C''C, -C'C)$$

where $A, B, C \in R$. Set the sequence

$$0 \longrightarrow R \longrightarrow R \times R \longrightarrow R \longrightarrow \Gamma \longrightarrow 0$$

Claim: The sequence is exact, namely ψ is injective, $ker\varphi = Im\psi$, $ker\pi = Im\varphi$, and π is surjective.

Let $\psi^{-1}(C) = \psi^{-1}(D)$ then,

$$\begin{aligned}
&\Rightarrow (C''C, -C'C) = (C''D, -C'D) \\
&\Rightarrow C''C = C''D \text{ and } -C'C = -C'D \\
&\Rightarrow C = D \\
&\Rightarrow \psi \text{ is injective}.
\end{aligned}$$

Since C' and C'' have no common components, the kernel of φ is as follows:

$$\begin{aligned}
ker\varphi &= \{(A, B) : AC' + BC'' = 0\} \\
&= \{(C''C, -C'C) : C \in R\} \\
&= Im\psi\,.
\end{aligned}$$

Since the kernel of π is the set of all finite linear combinations of C' and C'' with coefficients in R, the kernel of π is as follows:

$$\begin{aligned}
ker\pi &= \{AC' + BC'' : A, B \in R\} \\
&= Im\varphi\,.
\end{aligned}$$

Lastly, the natural map π is always surjective. Therefore, the sequence is exact.

If we restrict these maps to the homogeneous polynomials of various degrees, we get the following sequence:

$$0 \longrightarrow R_{d-m-n} \longrightarrow R_{d-m} \times R_{d-n} \longrightarrow R_d \longrightarrow \Gamma_d \longrightarrow 0$$

Here, we need a proposition whose proof can be found in (10) as follows:

Let V_1, V_2, V_3 and V_4 be finite-dimensional vector spaces and the sequence

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V_3 \longrightarrow V_4 \longrightarrow 0$$

be exact. Then,

$$dimV_4 = dimV_3 - dimV_2 + dimV_1.$$

Since $dimR_d = \frac{(d+1)(d+2)}{2}$, it follows from the proposition,

$$\begin{aligned} dim(\Gamma_d) &= dim(R_d) - dim(R_{d-m} \times R_{d-n}) + dim(R_{d-m-n}) \\ &= mn \end{aligned}$$

for $d \geq m + n$.

Step 2:

Let the map $\beta : \Gamma \to \Gamma$ be defined by $\beta(\overline{H}) = \overline{zH}$. In order to show that β is injective it is enough to show that $H = A'C' + B'C''$ when $zH = AC' + BC''$ for some $A', B' \in R$. For any $J \in k[x, y, z]$, denote $J(x, y, 0)$ by J_0. Since C', C'' and z do not have any common zeros, C'_0 and C''_0 are relatively prime homogeneous polynomials in $k[X, Y]$. If $zH = AC' + BC''$ then,

$$\begin{aligned} &\Rightarrow A_0C'_0 + B_0C''_0 = 0 \\ &\Rightarrow A_0C'_0 = -B_0C''_0 \\ &\Rightarrow B_0 = C'_0C \quad \text{and} \quad A_0 = -C''_0C \end{aligned}$$

for some $C \in k[X, Y]$.

We can set A_1 and A_2 such that $A_1 = A + CC''$ and $B_1 = B - CC'$ since

$$\begin{aligned} (A_1)_0 &= A_0 + CC''_0 \\ &= -C''_0 + CC''_0 \\ &= 0 \end{aligned}$$

and similarly $(B_1)_0 = 0$. It follows that $A_1 = zA'$ and $B_1 = zB'$ for some $A', B' \in k[x, y, z]$. So,

$$\begin{aligned} zH &= A_1C' + B_1C'' \\ &= zA'C' + zB'C'' \\ &= z(A'C' + B'C'') \end{aligned}$$

which implies that

$$H = A'C' + B'C''.$$

Step 3:

Let $d \geq m+n$ and choose $A_1, A_2, \ldots, A_m n \in R$ whose images in Γ_d form a basis for Γ_d. Let

$$A_{i*} = A_i(X, Y, 1) \in k[X, Y]$$

and a_i be the image of A_{i*} in Γ_*.

Claim: $a_1, a_2, \ldots, a_{mn}$ form a basis for Γ_*:

An injective linear map of vector space with the same dimension is an isomorphism so, the map α restricts to an isomorphism between Γ_d and Γ_{d+1} for $d \geq m+n$ from step 2. Hence under the natural projection homomorphism, the image of $z^r A_1, \ldots, z^r A_{mn}$ form a basis for Γ_{d+r} for all $r \geq 0$.

First It will be indicated that $\{a_i\}$ span Γ_*.

Let $h \in \Gamma_*$ be the image of $H \in k[X, Y]$ under the natural projection. Then, some $z^m H^*$ is a homogeneous polynomial of degree $d+r$,

$$z^m H^* = \sum_{i=1}^{mn} \lambda_i A_i + BC' + CC''$$

for some $\lambda_i \in k$ and $B, C \in k[x, y, z]$. Then,

$$\begin{aligned} H &= (z^m H^*)_* \\ &= \sum_{i=1}^{mn} \lambda_i A_{i*} +_* BC'_* + C_* C''_* . \end{aligned}$$

Hence, $h = \sum_{i=1}^{mn} \lambda_i a_i$.

Secondly, we show that the $\{a_i\}$ are linearly independent in Γ_*. Suppose $\sum_{i=1}^{mn} \lambda_i a_i = 0$, then

$$\sum_i \lambda_i A_{i*} = BC'_* + CC''_*.$$

Therefore,

$$\begin{aligned} z^r (\sum_i \lambda_i A_{i*})^* &= z^r (BC'_* + CC''_*)^* \\ &= z^s (BC'_*)^* + z^t (CC''_*)^* \\ &= z^s B^* C' + z^t C^* C'' \\ &= z^r (\sum_i \lambda_i A_i) \end{aligned}$$

for some r, s, t. It is clear that

$$\sum \lambda_i \overline{z^r A_i} = 0, \quad \text{in } \Gamma_{d+r}.$$

As is known, $\{\overline{z^r A_i}\}$ form a basis for Γ_{d+r}, so every λ_i is zero. From this, it is clear that the $\{a_i\}$ are linearly independent. In addition to this, $\{a_i\}$ form a basis for Γ_*. This completes the proof. $\square$

Here, we give some basic examples:

Example 4.1.7 (1) *Let C be defined by x^2+y^2-1 and L be defined by $x-y$, with* $\deg C = 2$ *and* $\deg L = 1$. *By Bézout' s theorem, C and L intersect at two points which is the product of their degrees (see Figure 4.1).*

Figure 4.1: *The intersection of $X^2+Y^2=1$ and $X-Y=0$*

(2) *Let C be defined by x^2+y^2-1 and let L be defined by $x+1$ with* $\deg C = 2$ *and* $\deg L = 1$. *Here, C and L intersect at one point (see Figure 4.2). This does not contradict Bézout' s theorem since the multiplicity of the intersection point $p=(0,1)$ is two.*

Figure 4.2: *The intersection of $X^2+Y^2=1$ and $X+1=0$*

(3) *Let L_1 and L_2 be two parallel lines. By Bézout' s theorem they must intersect at one point. As is well known, two parallel lines intersect "at infinity" in the projective space (see Figure 4.3).*

Figure 4.3: *Parallel lines in afine space*

Example 4.1.8 (The example revisited) *Recall the Example* 3.3.11. *It was looked at the intersection of unit circle*

$$x^2 + y^2 - z^2 = 0$$

and the elliptic curve

$$x^3 - x^2 z - xz^2 + z^3 - y^2 z = 0.$$

The point $(0, 0, 1)$ *does not belong to any of these curves. However, it lies on the line through the points* $0, 1, 1$ *and* $0, -1, 1$. *Choose the different coordinate system to compute multiplicities. We have the equations as below replacing* x *by* $x - z$ *and* y *by* $y - z$

$$\begin{aligned} F(x, y, z) &= (x - z)^2 + (y - z)^2 - z^2 \\ &= (x^2 + y^2)z^0 - 2(x + y)z + z^2 \\ G(x, y, z) &= (x - z)^3 - (x - z)^2 z - (x - z)z^2 + z^3 - (y - z)^2 z \\ &= x^3 z^0 - (4x^2 + y^2)z + 2(2x + y)z^2 - z^3 . \end{aligned}$$

The resultant $Res^z_{F,G}$ *of* F *and* G *is*

$$\begin{vmatrix} x^2+y^2 & -2(x+y) & 1 & 0 & 0 \\ 0 & x^2+y^2 & -2(x+y) & 1 & 0 \\ 0 & 0 & x^2+y^2 & -2(x+y) & 1 \\ x^3 & -(4x^2+y^2) & 2(2x+y) & -1 & 0 \\ 0 & x^3 & -(4x^2+y^2) & 2(2x+y) & -1 \end{vmatrix}$$

$Res^z_{F,G} = Res(x,y) = x^2y(y-2x)(x-2y)^2$. *The possibilities* $Res(x,y) = 0$ *are as follows:*

(1) $y = 0$; *then*

$$F(x,0,z) = x^2 - 2xz + z^2 = (x-z)^2 = 0$$
$$G(x,0,z) = x^3 - 4x^2z + 4xz^2 - z^3 = 0\,.$$

Hence, the corresponding intersection point is $(1,0,1)$ *and it has multiplicity* 1.

(2) $y - 2x = 0 \Rightarrow y = 2x$; *then*

$$\begin{aligned} F(x,2x,z) &= x^2 + 4x^2 - 2(x+2x)z + z^2 \\ &= (5x-z)(x-z) = 0 \\ G(x,2x,z) &= x^3 - (4x^2 + (2x)^2)z + 2(2x+2x)z^2 - z^3 \\ &= x^3 - 8x^2z + 8xz^2 - z^3 = 0\,. \end{aligned}$$

Hence, $x = z$ *and the corresponding intersection point is* $(1,2,1)$.

(3) $x = 0$; *then*

$$F(0,y,z) = y^2 - 2yz + z^2 = (y-z)^2 = 0$$
$$G(0,y,z) = -y^2z + 2yz^2 - z^2 = 0\,.$$

Hence, the corresponding point is $(0,1,1)$ *with multiplicity* 2.

(4) $x - 2y = 0 \Rightarrow x = 2y$; *then*

$$F(2y,y,z) = (5y-z)(y-z) = 0$$
$$G(2y,y,z) = 8y^3 - 17y^2z + 10yz^2 - z^3 = 0\,.$$

Hence, the corresponding intersection point is $(2,1,1)$ *with multiplicity* 2.

4.2 The Applications of Bézout' s Theorem

Let $f(x)$ be a non-constant polynomial in $\mathbb{C}[x]$; (or more generally in $k[x]$ where k is algebraically closed field) and the degree of $f(x)$ be m.

Fundamental Theorem of Algebra solves exactly the problem (1.1) for the $x-$axis C and curves D which are given by

$$y = 0$$

$$y - f(x) = 0$$

respectively. The intersection points are of the form

$$(a, 0)$$

where $f(a) = 0$, that is, a is the root of $f(x)$. So there exist m different a's since the degree of the polynomial $f(x)$ is m, i.e. $\deg f(x) = m$ and the polynomial is defined over an algebraically closed field. Moreover, C and D has m distinct intersection points which is also required by Bézout' s Theorem. ($\deg C \times \deg D = 1 \times m = m$)

Corollary 4.2.1 *(i) If the projective curve C' is a non-singular in $\mathbb{P}^2_k$, then it is irreducible.*

(ii) Let the projective curve C' be an irreducible in $\mathbb{P}^2_k$, then it has at most finitely many singular points. (4)

Proof (i) Suppose that

$$C' = \{(x, y, z) \in \mathbb{P}^2_k : F(x, y, z) = 0\}$$

is a reducible projective curve in $\mathbb{P}^2_k$, that is, there exist $P, Q \in k[x, y, z]$ such that

$$F(x, y, z) = P(x, y, z)Q(x, y, z)$$

and $\deg P \geq 1$ and $\deg Q \geq 1$. Then, by Theorem 4.1.1 P and Q intersect in at least one point. Assume that $p = (a, b, c)$ is a common root of P and Q. Since $P(a, b, c) = 0$ and $Q(a, b, c) = 0$,

$$F(a, b, c) = P(a, b, c)Q(a, b, c)$$

. Moreover;

$$F_x(x, y, z) = \frac{\partial F}{\partial x} = P_x(x, y, z)Q(x, y, z) + P(x, y, z)Q_x(x, y, z)$$

and

$$F_x(a, b, c) = 0, \;\; F_y(a, b, c) = 0, \;\; F_z(a, b, c) = 0.$$

The point $p = (a, b, c)$ is a singular point of C'. It contradicts the assumption that C' is non-singular.

(ii) Let C' be an irreducible projective curve in $\mathbb{P}^2_k$, that is, there exists a homogeneous irreducible polynomial F of degree n such that

$$C' = \{(x, y, z) \in \mathbb{P}^2_k : F(x, y, z) = 0\}.$$

By changing a coordinates, assume that $(1, 0, 0) \notin C'$ which is the coefficient of x^n in $F(x, y, z)$. Then we have;

$$G(x, y, z) = P_x(x, y, z) = \frac{\partial P}{\partial x}.$$

Here G is the homogeneous polynomial of degree $(n-1)$ and G defines a curve C'' in $\mathbb{P}^2_k$.

C' and C'' have no common component since C' is irreducible and the degree of C'' is certainly less than C'. Therefore, C' and C'' intersect at most $n(n-1)$ points by Bézout' s theorem. Every singular point of C' is the intersection point of C' and C'' then the result follows. □

Recall that if the degree of the curve C' is two in $\mathbb{P}^2_k$ then C' is called conic.

Corollary 4.2.2 *Let C' be an irreducible projective conic in $\mathbb{P}^2_k$. It is equivalent to the conic*

$$x^2 - yz$$

under a projective transformation. In particular, it is non-singular.

Proof Let C' is an irreducible projective conic. By Corollary 4.2.1 there are at most finitely many singular points on C'. Choose a suitable projective transformation so that $(0, 1, 0)$ is a non-singular point of C' and the tangent line is given by $z = 0$. Then C' must be defined by the homogeneous F such that

$$F(x, y, z) = ayz + bx^2 + cxz + dz^2$$

for some $a, b, c, d \in k$. Hence, a and b cannot be both zero since C' is irreducible (if so $a = 0$ and $b = 0$ then $F(x, y, z) = cxz + dz^2 = z(cx + dz)$).

Let T be the projective transformation such that

$$T(x, y, z) = (\sqrt{bx}, ay + cx + dz, -z).$$

Then we get

$$F(x', y', z') = x'^2 - y'z'.$$

Hence, the projective transformation T takes C' to the conic

$$x^2 - yz.$$

Moreover, C' is non-singular since this conic is non-singular. □

Proposition 4.2.3 *Let C' and C'' be two projective curves in $\mathbb{P}_k^2$ of degrees m and D' be an irreducible curve of degree $n < m$. Assume that they intersect in exactly m^2 points and mn of these points lie on D'. Then the remaining $m^2 - mn = m(m-n)$ points lie on a curve D'' whose degree is at most $m - n$. (6)*

Proof Let C', C'' and D' be defined by the homogeneous polynomials $P, Q, R \in k[x, y, z]$. Choose a point (a, b, c) such that

$$(a, b, c \in D') \text{ and } (a, b, c) \geq C' \cap C''.$$

Set a new curve D'' which is defined by a homogeneous polynomial S

$$S(x, y, z) = Q(a, b, c)P(x, y, z) - P(a, b, c)Q(x, y, z).$$

Note that $p = (a, b, c)$ and the mn points of $C' \cap C''$ lie on D' by hypotesis. So D'' and D' intersect in at least $mn + 1$ points. D' and D'' must have a common component by Theorem 4.1.2. Recall that D' is irreducible so D'' must be reducible. And assume that the curve D'' is defined by the homogeneous polynomial S. such that

$$S = RT \quad for \;\; some \quad T \in k[x, y, z]$$

and $\deg T \leq m - n$. Every remaining point $p' = (a', b', c')$ which does not lie on D' satisfies

$$P(a', b', c') = 0 = Q(a', b', c').$$

It follows that

$$S(a', b', c').$$

$T(a', b', c')$ must be equal to zero, since $R(a', b', c')$ is not equal to zero. □

Corollary 4.2.4 (Pascal' s Mystic Hexagon) *The pairs of opposite sides of hexagon inscribed in an irreducible conic in $\mathbb{P}_k^2$ meet in three collinear points.*

Proof Let L_i be the line determined by p_i and p_{i+1} for $i = 1, \ldots, 5$ and let L_6 be determined by p_6 and p_0. The degree of each p_i in $k[x, y, z]$ is 1. Let L and L' be two cubics in $\mathbb{P}_k^2$ such that

$$L = L_1 L_3 L_5 \;\; and \;\; L' = L_2 L_4 L_6$$

with $\deg L = \deg L' = 3$. Since they have no common component they intersect in exact $\deg L \deg L' = 9$ points by Bézout' s theorem. By Proposition 4.2.3 six of these points are the vertices of the hexagon and the other three lie on a line. □

Chapter 5

Max Noether' s Fundamentalsatz

5.1 Max Noether' s Fundamental Theorem

Definition 5.1.1 *A zero-cycle on $\mathbb{P}^2_k$ is a formal sum*

$$\sum a_p p,$$

where $p \in \mathbb{P}^2_k$ and $\{a_p\}$ are integers and all but finitely many of the a'_p s are zero. (10)

Consider that the set of zero-cyles on $\mathbb{P}^2_k$ form a free abelian group with basis $X = \mathbb{P}^2_k$.

The degree of a zero-cycle $\sum a_p p$ is the sum of a'_ps. The zero-cycle is positive if each $a_p \geq 0$. If $a_p \geq m_p$ then

$$\sum a_p p > \sum m_p p,$$

where m_p denotes the multiplicity of the curve C' at the point p.

Definition 5.1.2 *Let C' and C'' be projective plane curves of degrees m, n and they do not have any common component. Then, the intersection cycle is a zero-cycle with*

$$a_p = I_p(C', C''),$$

where $I_p(C', C'')$ is the intersection multiplicity of C', C''. Namely, the intersection cycle $C' \bullet C''$ is

$$C' \bullet C'' = \sum_{p \in \mathbb{P}^2} I_p(C', C'')p.$$

The intersection cyle is a positive zero cycle of degree mn with $a_p = I_p(C', C'')$ by Bézout' s Theorem. Many features of the intersection number $I_p(C', C'')$ can be adapted well into properties of the intersection cycle. Here is some properties:

(i) In Theorem 4.1.4 (4) implies that

$$C' \bullet C'' = C'' \bullet C',$$

(ii) In Theorem 4.1.4 (6) implies that

$$C' \bullet C''D = C' \bullet C'' + C' \bullet D$$

where D is also a curve,

(iii) In Theorem 4.1.4 (7) implies that if A is a form and $\deg(A) = \deg(C'') - \deg(C')$ then,

$$C' \bullet (C'' + aC') = C' \bullet C''.$$

Suppose C', C'' and D are curves and D intersects C' in a bigger cycle than C'' intersects C', that is

$$D \bullet C' \geq C'' \bullet C'.$$

Max Noether' s theorem solves the following question which is stated in the introduction:

Question: When is there a curve E with $\deg(E) = \deg(D) - \deg(C'')$ *such that*

$$E \bullet C' = D \bullet C' - C'' \bullet C'?$$

It suffices to find forms A, E such that $H = AF + EG$ where F, G and H define the curves C', C'' and D, since then we would have by using the properties of intersection cycle

$$\begin{aligned} H \bullet F &= (AF + EG) \bullet F \\ &= EG \bullet F \\ &= E \bullet F + G \bullet F\,. \end{aligned}$$

Noether' s conditions is the necessary and sufficient conditions for the question (1.2). The conditions are as follows:

Let C', C'' be two curves and they have no common components through $p \in \mathbb{P}^2_k$. If there are a, b in $O_p(\mathbb{P}^2_k)$ such that

$$H_* = aF_* + bG_*$$

then Noether conditions are satisfied at p with respect to C', C'' and D. Here

$$D_* = D(x, y, 1), C'_* = C'(x, y, 1), C''_* = C''(x, y, 1)$$

are the corresponding affine curves defined by $F_*, G_*, H_*,$.

Theorem 5.1.3 (Max Noether' s Fundamental Theorem) *Let C' and C'' be two projective curves whose equations are $F = 0$ and $G = 0$ with no common components. Then there is an equation*

$$H = AF + EG$$

where A and E are homogeneous polynomials with the degrees $\deg(D) - \deg(C')$ *and* $\deg(D) - \deg(C'')$ *if and only if Noether' s conditions are satisfied at every point of intersection of* C', C'' $(p \in C' \cap C'')$*. (10)*

Proof Suppose that $H = AF + EG$. By dehomogenizing we have the following:

$$H_* = A_* F_* + E_* G_*$$

for any point p where D_*, C'_*, C''_* are the corresponding affine curves. In addition, Noether' s conditions are satisfied at every $p \in C' \cap C''$.

Conversely, suppose that Noether' s conditions hold. As in the proof of Bézout' s theorem it can be assumed that none of the intersection points of C' and C'' lie on the line at infinity by a projective change of coordinates: $(\{[x : y : 0] \in \mathbb{P}^2_k\})$ since C' and C'' do not have any common components. Since the image of H_* in $O_p(\mathbb{P}^2_k) \setminus (C'_*, C''_*)$ lies in the kernel of the natural projection, Noether' s conditions refer that it must be zero for every intersection point of C', C''. And also, the image of H_* is zero in $k[X, Y] \setminus (C'_*, C''_*)$ that is

$$H_* = aF_* + bG_*$$

for some $a, b \in k[X, Y]$. Now by implementing Proposition 2.2.11, we have

$$\begin{aligned} z^t H &= z^t (H_*)^* = z^t (aF_* + bG_*)^* \\ &= z^r a^* F + z^s b^* G \\ &= AF + EG \end{aligned}$$

where A and E are homogeneous polynomials in $k[x, y, z]$. However, the step 2 of the proof of Bézout' s theorem says that the map defined by multiplication by z on $k[x, y, z] \setminus (C', C'')$ is injective. The image of H in $k[x, y, z] \setminus (C', C'')$ is zero and

$$H = A'F + E'G$$

for some $A', E' \in k[x, y, z]$ since $z^t H = AF + EG$. Set $A' = \sum A'_i$ and $E' = \sum E'_i$ where A'_i and E'_i are homogeneous polynomials of degree i. Then

$$H = A'_n F + E'_m G$$

such that $n = \deg(H) - \deg(F)$ and $m = \deg(H) - \deg(G)$. □

Proposition 5.1.4 *Let C', C'' and D be plane curves and p is the intersection point of C' and C'', i.e. $p \in C' \cap C''$. Then Noether' s conditions are satisfied at p if any of the following are true:*

(i) C' and C'' intersect transversally at p, that is p is a non-singular point on both C' and C'' and the tangent line to C' at p is different from the tangent line to C'' at p, and $p \in D$.

(ii) p is a simple point on C', and $I_p(D, C') \geq I_p(C'', C')$.

(iii) C' and C'' have distinct tangents at p, and $m_p(D) \geq m_p(C') + m_p(C'') - 1$.

Proof The proof is indicated in (10). □

Corollary 5.1.5 *There is a curve E such that $E \bullet C' = D \bullet C' - C'' \bullet C'$, if any of the following is true:*

(i) C' and C'' intersect in $\deg(C') \deg(C'')$ distinct points, and D passes through these points.

(ii) All of the intersection points of C', C'' are simple points of C', and $D \bullet C' > C'' \bullet C'$.

5.2 Applications of Noether' s Theorem

This section illustrates the applications of Max Noether' s Fundamental Theorem.

Proposition 5.2.1 *Let A, B be cubics and the intersection cycle $A \bullet B$ is*

$$\sum_{i=1}^{9} p_i$$

such that $p_1, p_2, \ldots, p_9$ are the intersection points of A, B. Suppose that C is a conic, and the intersection cycle $C \bullet A$ is given by

$$\sum_{i=1}^{6} p_i.$$

Moreover, suppose that $p_1, \ldots, p_6$ are simple points on A, that is the multiplicity m_{p_i} of the curve A at the point p_i is 1, for $i = 1, 2, \ldots, 6$. Then p_7, p_8 and p_9 are collinear, i.e. they lie on a straight line.

Proof Consider the notations C', C'' and D in the Max Noether' s Fundamental theorem and assert $C' = A$, $C'' = C$ and $D = B$. By Proposition 5.1.4 and Corollary 5.1.5 give the proof. □

Corollary 5.2.2 (Pascal' s Theorem) *If a hexagon in $\mathbb{P}_k^2$ is inscribed in an irreducible conic, then the intersection points of the three pairs of opposite lines are collinear. (11)*

Proof Consider the cubics A, B which are defined by the following two triples and a quadratic C defining the conic. The first triple is a triple of lines such that no two of these lines meet in a vertex of the hexagon and second triple is the triple of opposite lines. Then the result follows from Proposition 5.2.1. □

Corollary 5.2.3 (Pappus' Theorem) *Let L_1, L_2 be two distinct lines in $\mathbb{P}^2_k$ such that*

$$p_1, p_2, p_3 \in L_1 \text{ and } p'_1, p'_2, p'_3 \in L_2$$

with any of these points is not intersection point of L_1, L_2. Let L_{ij} be the line between p_i and p'_j for each pair (i, j). For each triple i, j, k with $\{1, 2, 3\}$ set

$$s_k = L_{ij} \bullet L_{ji},$$

that is s_k is the point in which L_{ij} and L_{ji} intersect. Then s_1, s_2 and s_3 are collinear. (11)

Proof Consider the two lines L_1, L_2 form a conic and the proof is the same as in Corollary 5.2.2. □

Chapter 6

Conclusion

In this dissertation we introduced two important results for algebraic curves, namely Bézout' s theorem and Max Noether' s Fundamental theorem. In particular, we studied the case of projective plane curves.

Bézout' s theorem tells us that the number of intersection points of two projective plane curves is obtained as the product of the degrees of these two curves, counting multiplicities.

Max Noether' s Fundamental theorem states the necessary conditions for decomposing a projective curve in terms of two other projective curves. In other words, the theorem describes when the equation of an algebraic curve in the complex projective plane can be written in terms of the equations of two other algebraic curves. Together with Bézout' s theorem, these results are fundamental in the study of algebraic curves in particular, and algebraic geometry in general.

Bibliography

[1] C. G. Gibson, *Elementary Geometry of Algebraic Curves*, Cambridge University Press, 1998. 13, 14, 15

[2] D. S. Dummit, and R. M. Foote, *Abstract Algebra*, 3rd ed. USA: John Willey & Sons Inc., 2004. 5, 6

[3] D. Menon, *Bézout' s Theorem for Curves*, 2011, Available from: http://www.math.uchicago.edu/ may/VIGRE/VIGRE2011/REUPapers/Menon.pdf (Accessed 16 July 2014). 27

[4] F. Kirwan, *Complex Algebraic Curves*, Cambridge University Press, 1992. 20, 24, 26, 35

[5] G. Fischer, *Plane Algebraic Curves*, American Mathematical Society, 2001. 9

[6] G. Gim, *Bézout's Theorem and Its Applications*, Available from: http://www.math.ucla.edu/ ggim/F11-214A.pdf (Retrieved 16 July 2014). 37

[7] M. Reid, *Undergraduate Algebraic Geometry*, Cambridge University Press, 1988. 8

[8] M.F. Atiyah, and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969. 11

[9] P. Gladki, *Resultants and Bézout's Theorem*, 2004, Available from: http://math.usask.ca/ gladki/inedita/referat.pdf (Accessed 16 July 2014) 18

[10] W. Fulton, *Algebraic Curves An Introduction to Algebraic Geometry*, Brandeis University Press, 1969. 5, 7, 10, 11, 25, 29, 38, 40, 41

[11] W. Decker, and F. O. Schreyer, *Varieties, Gröbner Bases, and Algebraic Curves*, Springer, 2009. 41, 42