Algebraic Curves, Projective Mappings and Bézout's Theorem

Mark Bell

May 12, 2009

1 Motivation

When considering a polynomial, f, in one variable over the complex numbers, the number of roots of the polynomial is clearly $\deg(f) < \infty$ by the Fundamental Theorem of Algebra. Infact, the Fundamental Theorem of Algebra goes even further, linking algebra and geometry by saying that a monic polynomial over the complex numbers, an algebraic object, is completely determined by its roots, a geometric property. However, once we start to consider polynomials in two variables there are, in general, an uncountable number of roots, however, a strong link between algebra and geometry still remains. We may consider the set of roots of a polynomial f in two variables as a collection of points in the $\mathbb{C}^2$ plane[1]. This set is, infact, the 0-level set of f and is called an algebraic curve.

In some cases, it may be possible to write an algebraic curve as the union of two 'smaller' algebraic curves in the same way that in some cases (non-prime cases infact) we may write an integer as the product of two 'smaller' factors. In this case, the properties of the algebraic curve can be determined by the properties of the 'smaller' algebraic curves that it is composed of.

We will see that the properties of one of these algebraic curves are determined by the properties of the polynomial from which it came. However, this polynomial is not unique and many other polynomials will have the same set of roots and so produce the same curve in the $\mathbb{C}^2$ plane. Therefore, polynomials that produce the same algebraic curve will share many key properties, most importantly, that they have the same minimal polynomial, denoted $\widehat{f}$.

To gain a better understanding of an algebraic curve, we will focus on one of its most important properties; its intersection with other algebraic curves. We will see that two algebraic curve always intersect, if not in the $\mathbb{C}^2$ plane then certainly when we project them into $\mathbb{CP}^2$ projective space, which we introduce to allow us to formalise the concept of a curve going 'to infinity'. Projective space will also provide the setting for Weak and Strong Bézout's Theorem, which determines the maximum number of intersections of two algebraic curves and, most importantly, the number of intersections when multiplicities are counted.

---

[1] When considered as a topological object, we see that this set of points is, infact, connected and so we may speak of it as a curve in the $\mathbb{C}^2$ plane [2, p18].

2 Notation

Throughout, we will use the following notation:

$\mathbb{N}$ - For the set of natural numbers, excluding zero

$\mathbb{N}_0$ - For the set of natural numbers, including zero

$\mathbb{Z}$ - For the group of integers

$\mathbb{R}$ - For the field of real numbers

$\mathbb{C}$ - For the field of complex numbers

$\mathbb{F}$ - For a general field

A^* - For the set of unital elements of the group A

$A \subseteq B$ - For the set A is contained in or equal to the set B

$A \subset B$ - For the set A is contained in but not equal to the set B

$S^n_{\mathbb{C}}$ - For the complex unit ball of dimension n

$H^n_{\mathbb{C}}$ - For the complex unit ball of dimension n in which antipodial points are equivalent[2]

3 Definitions

3.1 Polynomials in Several Variables

Let $\mathbb{F}$ be a field. We denote the set of all polynomials in one variable (x_1) over the field $\mathbb{F}$ by $\mathbb{F}[x_1]$ and, similarly, the set of all polynomials in two variables (x_1 and x_2) over the field $\mathbb{F}$ by $\mathbb{F}[x_1, x_2]$.

A polynomial in one variable $f \in \mathbb{F}[x_1]$ may be written as $f(x_1) = \sum_{i=0}^{n} \alpha_i x_1^i$ where $\alpha_i \in \mathbb{F}$ and $\alpha_n \neq 0$. Similarly, we may write a polynomial in two variables $f \in \mathbb{F}[x_1, x_2]$ as either;

$f(x_1, x_2) = \sum_{i=0}^{n} \sum_{j=0}^{m} \alpha_{ij} x_1^i x_2^j$ where $\alpha_{ij} \in \mathbb{F}$

$f(x_1, x_2) = \sum_{i=0}^{m} a_i x_1^i$ where $a_i \in \mathbb{F}[x_2]$ and $a_m \neq 0_{\mathbb{F}[x_2]}$

$f(x_1, x_2) = \sum_{j=0}^{n} b_j x_2^j$ where $b_j \in \mathbb{F}[x_1]$ and $b_n \neq 0_{\mathbb{F}[x_1]}$

These alternative notations will become useful later and can easily be extended to polynomials of 3 or more variables too.

---

[2] We will only be considering $H^n_{\mathbb{C}}$ for $n = 2$, although the more general notation is given.

3.1.1 Remark

Note that $\mathbb{F}[x_1, x_2]$ is a field with identity element of multiplication $1_{\mathbb{F}[x_1,x_2]}(x_1, x_2) = 1_{\mathbb{F}}$. Therefore, the unital elements of $\mathbb{F}[x_1, x_2]$ are the constant, unital functions.

$$\mathbb{F}[x_1, x_2]^* = \{f \in \mathbb{F}[x_1, x_2] \colon f(x_1, x_2) = \lambda \in \mathbb{F}^*\}$$

3.2 Degrees of Polynomials

We already know of the degree function for single variables polynomials.

$$\deg \colon \mathbb{F}[x_1] \to \mathbb{N}_0$$

However, in order to better understand the degree function for polynomials of two variables, we use the following, alternative, definition. If $f \in \mathbb{F}[x_1]$ then we define the degree of f by:

$$\deg(f(x_1)) = \deg(\sum_{i=0}^{n} \alpha_i x_1^i) = \max_{0 \le i \le n} \{i \colon \alpha_i \ne 0_{\mathbb{F}}\}$$

Where $\alpha_i \in \mathbb{F}$ and $\alpha_n \ne 0_{\mathbb{F}}$

However, as by definition $\alpha_n \ne 0_{\mathbb{F}}$, we observe that $\deg(f) = n$.

We can now easily extend this definition to polynomials in two variables by allowing $\deg \colon \mathbb{F}[x_1, x_2] \to \mathbb{N}_0$ and defining the define the degree of f, where $f \in \mathbb{F}[x_1, x_2]$, by

$$\deg(f(x_1, x_2)) = \deg(\sum_{i=0}^{n} \sum_{j=0}^{m} \alpha_{ij} x_1^i x_2^j) = \max_{0 \le i \le m, 0 \le j \le n} \{i + j \colon \alpha_{ij} \ne 0_{\mathbb{F}}\}$$

Where $\alpha_{ij} \in \mathbb{F}$

However, note that, as it is not required that $\alpha_{mn} \ne 0_{\mathbb{F}}$, the degree of f may be less than $m + n$.

If $f \in \mathbb{F}[x_1, x_2]$ then we will also define $\deg_{x_1}, \deg_{x_2} \colon \mathbb{F}[x_1, x_2] \to \mathbb{N}_0$ as the degree of f in x_1 and x_2 respectively by:

$$\deg_{x_1}(f(x_1, x_2)) = \deg_{x_1}(\sum_{i=0}^{m} a_i x_1^i) = \max_{0 \le i \le m} \{i \colon a_i \ne 0_{\mathbb{F}[x_2]}\}$$

$$\deg_{x_2}(f(x_1, x_2)) = \deg_{x_2}(\sum_{j=0}^{n} b_j x_2^j) = \max_{0 \le j \le n} \{j \colon b_j \ne 0_{\mathbb{F}[x_1]}\}$$

Where $a_i \in \mathbb{F}[x_2]$, $b_j \in \mathbb{F}[x_1]$ and $a_m \ne 0_{\mathbb{F}[x_2]}$ and $b_n \ne 0_{\mathbb{F}[x_1]}$

However, as by definition $a_m \ne 0_{\mathbb{F}[x_2]}$ and $b_n \ne 0_{\mathbb{F}[x_1]}$, we observe that $\deg_{x_1}(f(x_1, x_2)) = m$ and $\deg_{x_2}(f(x_1, x_2)) = n$.

Again, these definitions can easily be extended to polynomials of 3 or more variables too.

3.3 Variety

We now introduce the variety function, $\nu\colon \mathbb{F}[x_1, x_2] \to \mathbb{F}^2$, which will be essential in the construction of algebraic curves [2, p13].

If $f \in \mathbb{F}[x_1, x_2]$ and $\deg(f) \geq 1$ then the variety of f is the 0-level set of f [3, p8], i.e. the points in the plane that solve f. This is defined as

$$\nu(f) = \{(x_1, x_2) \in \mathbb{F}^2 \colon f(x_1, x_2) = 0\} \subseteq \mathbb{F}^2$$

Note that $\nu(f) = \mathbb{F}^2$ if and only if $f = 0_{\mathbb{F}[x_1,x_2]}$.

3.4 Algebraic Curves

With these tools we are now ready to begin to consider algebraic curves in the $\mathbb{F}^2$ plane.

Let $C \subseteq \mathbb{F}^2$. Then C is said to be an algebraic curve if and only if $\exists f \in \mathbb{F}[x_1, x_2]$ with $\deg(f) \geq 1$ such that $C = \nu(f)$. We say that f is an equation for C, although we will see later that it is not unique [2, p14].

However, the definition that we have given causes problems. For example, if our field is $\mathbb{R}$ and we consider the polynomials $f(x_1, x_2) = x_1^2 + x_2^2$ and $g(x_1, x_2) = x_1^2 + x_2^2 + 1$ then $\nu(f) = \{(0, 0)\}$ and $\nu(g) = \emptyset$. From this we conclude that $\{(0, 0)\}$ and $\emptyset$ are algebraic curves, which is a strange concept as we are refering to things as curves, despite the fact that they contain just one and no points respectively [2, p13].

We overcome this by requiring that every polynomial in one variable of degree at least 1, with coefficients in $\mathbb{F}$, has a root in $\mathbb{F}$. i.e. $\forall f \in \mathbb{F}[x_1]$ such that $\deg(f) \geq 1$, $\exists x \in \mathbb{F}$ such that $f(x) = 0_{\mathbb{F}}$, in which case our field $\mathbb{F}$ is said to be algebraically closed [3, p5].

Hence from this point on, we will only consider functions over the field $\mathbb{C}$ which, by the Fundamental Theorem of Algebra, is algebraically closed.

Note that we may actually make a stronger statement than what we have been stating so far and say that $\nu(f) = C \subset \mathbb{C}^2$ as, $\nu(f) = C = \mathbb{C}^2$ implies $f = 0_{\mathbb{C}[x_1,x_2]}$ and in this case $\deg(f) \ngeq 1$ and hence C is not an algebraic curve.

4 Properties of Variety

In order to explore some of the properties of algebraic curves, we begin by examining some of the fundamental properties of the variety function.

4.1 Theorem - Cardinality of $C = \nu(f)$

An algebraic curve $C = \nu(f)$ contains uncountably many points [2, pp15-17] [6, p7].

Proof

Let $C = \nu(f)$ be an algebraic curve. We consider the two cases; firstly when f is independent of x_2 and then the case when f is dependent on both x_1 and x_2.

Begin by considering the case in which f is independent of one variable, without loss of generality, assume it is x_2. Then $f(x_1, x_2) = a_0 + a_1x_1 + \cdots + a_nx_1^n \in \mathbb{C}[x_1]$ where $a_i \in \mathbb{C}$. As $\mathbb{C}$ is algebraically closed, $\exists x \in \mathbb{C}$ such that $f(x, x_2) = 0$. But then $\forall y \in \mathbb{C}$, $f(x, y) = 0$ and so $(x, y) \in \nu(f)$. Therefore $\nu(f)$ contains an uncountable number of points as $\mathbb{C}$ is uncountable.

Secondly, consider the case when f is dependent on both x_1 and x_2, i.e. $f(x_1, x_2) = a_0(x_2) + a_1(x_2)x_1 + \cdots + a_n(x_2)x_1^n \in \mathbb{C}[x_1, x_2]$ where $a_i \in \mathbb{C}[x_2]$ and $a_n \neq 0_{\mathbb{C}[x_2]}$. As f is dependent on both x_1 and x_2, $n \geq 1$. Let $A = \{x_2 \in \mathbb{C} \colon a_n(x_2) = 0\}$, clearly $|A| \leq \deg(a_n) < \infty$. Therefore, for all but at most $\deg(a_n)$ values, $a_n(x_2) \neq 0$ and so $\mathbb{C}\backslash A$ is uncountable.

Then $\forall y \in \mathbb{C}\backslash A$, $a_n(y) \neq 0$ and so $f(x_1, y) = \alpha_0 + \alpha_1x_1 + \cdots + \alpha_nx_1^n \in \mathbb{C}[x_1]$ where $\alpha_i = a_i(y) \in \mathbb{C}$. However, again as $\mathbb{C}$ is algebraically closed, $\exists x_y \in \mathbb{C}$ such that $f(x_y, y) = 0$ and so $(x_y, y) \in \nu(f)$. Therefore $\nu(f)$ contains an uncountable number of points as $\mathbb{C}\backslash A$ is uncountable.

$\square$

4.1.1 Remark

From this we may note that if $C = \nu(f)$ is an algebraic curve then $C \neq \emptyset$.

4.2 Scalars of Polynomials

Let $f \in \mathbb{C}[x_1, x_2]$ *then* $\forall \lambda \in \mathbb{C}^*$, $\nu(\lambda f) = \nu(f)$ *[2, p14].*

Proof

Let $(x, y) \in \nu(f)$ then $f(x, y) = 0$. Then $(\lambda f)(x, y) = \lambda f(x, y) = 0$ and so $(x, y) \in \nu(\lambda f)$. Similarly, if $(x, y) \in \nu(\lambda f)$ then $(\lambda f)(x, y) = \lambda f(x, y) = 0$ and so, as λ is unital and $\mathbb{C}$ is an integral domain, $f(x, y) = 0$, hence $(x, y) \in \nu(f)$. Therefore $\nu(f) = \nu(\lambda f)$.

$\square$

4.3 Product of Polynomials

Let $f, g \in \mathbb{C}[x_1, x_2]$ *then* $\nu(fg) = \nu(f) \cup \nu(g)$.

Proof

Firstly, let $(x, y) \in \nu(fg)$. Then $(fg)(x, y) = f(x, y)g(x, y) = 0$. As $\mathbb{C}$ is an integral domain, either $f(x, y) = 0$ or $g(x, y) = 0$ and so in either case $(x, y) \in \nu(f) \cup \nu(g)$. Therefore $\nu(fg) \subseteq \nu(f) \cup \nu(g)$.

Similarly, let $(x, y) \in \nu(f) \cup \nu(g)$, then $f(x, y) = 0$ or $g(x, y) = 0$. Without loss of generality, assume $f(x, y) = 0$. Then $(fg)(x, y) = f(x, y)g(x, y) = 0$. Hence $(x, y) \in \nu(fg)$ and so $\nu(f) \cup \nu(g) \subseteq \nu(fg)$.

Therefore $\nu(fg) = \nu(f) \cup \nu(g)$

$\square$

4.4 Powers of Polynomials

Let $f \in \mathbb{C}[x_1, x_2]$ *then* $\forall k \in \mathbb{N}$, $\nu(f^k) = \nu(f)$ *[2, p14].*

Proof

It is an immediate concequence of 4.3 that $\nu(f^k) = \bigcup_{i=1}^{k} \nu(f) = \nu(f)$

□

5 Components

If $C = \nu(f)$ is an algebraic curve then we have seen that in certain circumstances, for example if f can be written as the product of two other polynomials, C can be written as the union of 2 algebraic curves $C_1, C_2 \subset \mathbb{C}^2$. In this case, we may consider the properites of C_1 and C_2 separately.

5.1 Reducibility

An algebraic curve $C = \nu(f)$ is said to be reducible if and only if $\exists$ algebraic curves C_1, C_2 $(C_1 \neq C \neq C_2)$ such that $C = C_1 \cup C_2$ [3, p15].

An algebraic curve C is said to be irreducible if it is not reducible, i.e. $C = C_1 \cup C_2$, where C_1 and C_2 are algebraic curves, implies $C_1 = C = C_2$ [2, p17].

5.1.1 Remark

$C = \nu(f)$ is a reducible algebraic curve if and only if $\exists$ an algebraic curve C' such that $C' \subset C$.

5.2 Components

Let $C = \nu(f)$ be an algebraic curve. Let $f_1, f_2, \ldots, f_n \in \mathbb{C}[x_1, x_2]$, $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{N}$ and $\alpha \in \mathbb{C}$ be such that $f = \alpha f_1^{\lambda_1} f_2^{\lambda_2} \cdots f_n^{\lambda_n}$.

Then, by 4.2, 4.3 and 4.4, $C = C_1 \cup C_2 \cup \ldots \cup C_n$, where $C_i = \nu(f_i)$. In which case $C_1, C_2, \ldots, C_n$ are said to be components of C.

5.2.1 Remark

Note that $C_i = \nu(f_i)$ is a component of $C = \nu(f)$ if and only if $C_i \subseteq C$ and $C = \nu(f)$ is an irreducible algebraic curve if and only if the only component of C is C.

5.3 Irreducible Components

The components of C which are themselves irreducible are called the irreducible components of C.

If $C = \nu(f)$ where $f \in \mathbb{C}[x_1, x_2]$, as $\mathbb{C}[x_1, x_2]$ is a unique factorisation domain, $\exists! f_1, f_2, \ldots, f_n \in \mathbb{C}[x_1, x_2]$, $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{N}$ and $\alpha \in \mathbb{C}$ such that $f = \alpha f_1^{\lambda_1} f_2^{\lambda_2} \cdots f_n^{\lambda_n}$ where $f_1, f_2, \ldots, f_n$ are irreducible in $\mathbb{C}[x_1, x_2]$ and $n \leq \deg(f)$.

Hence, by 4.2, 4.3 and 4.4, $C = C_1 \cup C_2 \cup \ldots \cup C_n$, where $C_i = \nu(f_i)$ [2, pp17-18]. $C_1, C_2, \ldots, C_n$ are called the irreducible components of C. We donte the set of irreducible components of C by $Irr(C) = \{C_1, C_2, \ldots, C_n\}$ [3, p19].

Note that for an algebraic curve $C = \nu(f)$ there are at most $\deg(f)$ irreducible components of C and so $|Irr(C)| \leq \deg(f)$.

5.3.1 Remark

Every component of an algebraic curve is the finite union of irreducible components of C, i.e. if C' is a component of C then $\exists C_{\kappa_1}, C_{\kappa_2}, \ldots, C_{\kappa_m} \in Irr(C)$ such that $C' = \bigcup_{i=1}^{m} C_{\kappa_i}$.

Therefore an algebraic curve $C = \nu(f)$ has at most $2^{\deg(f)} - 1$ distinct components.

Note that, as $C = \bigcup_{C_i \in Irr(C)} C_i$, $C \subseteq D$ if and only if $Irr(C) \subseteq Irr(D)$ and $C = D$ if and only if $Irr(C) = Irr(D)$.

5.4 Common Components

Let $C = \nu(f)$ and $D = \nu(g)$ be algebraic curves. Then C and D are said to have a common component if and only if $\exists$ an algebraic curve $E = \nu(h)$ such that E is a component of both C and of D. Note, by 5.2.1, C and D have a common component if and only if $\exists$ an algebraic curve $E = \nu(h)$ such that $E \subseteq C \cap D$.

Similarly C and D are said to be relatively prime if they have no common component, i.e. if and only if $\nexists$ an algebraic curve $E = \nu(h)$ such that E is a component of both C and of D.

5.4.1 Remark

C and D have a common component if and only if they have a common irreducible component, therefore we need only talk about C and D having a common component.

Therefore C and D have a common component if and only if $Irr(C) \cap Irr(D) \neq \emptyset$ and are relatively prime if and only if $Irr(C) \cap Irr(D) = \emptyset$.

5.4.2 Remark

If $C = \nu(f)$ and $D = \nu(g)$ are algebraic curves where $f = \alpha \prod_{i=1}^{m} f_i^{\lambda_i}$, $g = \beta \prod_{j=1}^{n} g_j^{\mu_j}$ and f_i and g_j are irreducible in $\mathbb{C}[x_1, x_2]$. Then C and D have a common component if and only if $\gcd(f, g) \neq 1$. Which occurs if and only if $\exists i, j$ such that $f_i = \lambda g_j$ for some $\lambda \in \mathbb{C}^*$.

6 Minimal Polynomials

We have already seen from 4.2, 4.3 and 4.4 that, for any algebraic curve C, many equations of C exist. We will now consider the simplist of these polynomials, which will form a set, known as the set of minimal polynomials of C.

Let $C = \nu(f)$ be an algebraic curve where $f \in \mathbb{C}[x_1, x_2]$ and $\deg(f) \geq 1$. Then $\widehat{f} \in \mathbb{C}[x_1, x_2]$ is a minimal polynomial of f if and only if $\nu(\widehat{f}) = C$ and $\forall g \in \mathbb{C}[x_1, x_2]$ such that $0 < \deg(g) < \deg(\widehat{f})$, $\nu(g) \neq C$.

Notice that, if $C = \nu(f)$ is an algebraic curve and $\widehat{f_1}, \widehat{f_2} \in \mathbb{C}[x_1, x_2]$ are minimal polynomials of f then $\deg(\widehat{f_1}) = \deg(\widehat{f_2}) \leq \deg(f)$.

6.1 Lemma - The Degree of a Minimal Polynomial

If $C = \nu(f)$ is an algebraic curve and $\widehat{f}$ a minimal polynomial of f then $\deg(\widehat{f}) \geq |Irr(C)|$

Proof

Let $C = \nu(f)$ be an algebraic curve and $\widehat{f}$ a minimal polynomial of f.

Suppose $\deg(\widehat{f}) < |Irr(C)|$. Then by 5.3 $|Irr(\nu(\widehat{f}))| \leq \deg(\widehat{f}) < |Irr(C)|$ and so $Irr(\nu(\widehat{f})) \neq Irr(C)$. Therefore by 5.3.1 $\nu(\widehat{f}) \neq C$. Hence $\widehat{f}$ is not a minimal polynomial of C.

Therefore $\deg(\widehat{f}) \geq |Irr(C)|$.

$\square$

6.2 The Minimal Polynomials

If $C = \nu(f)$ is an algebraic curve, where $f = \alpha \prod_{i=1}^{m} f_i^{\lambda_i}$, $\alpha \in \mathbb{C}^*$ and f_i are irreducible in $\mathbb{C}[x_1, x_2]$, then $\widehat{f}$ is a minimal polynomial of f if and only if $\widehat{f} = \beta \prod_{i=1}^{m} f_i$ where $\beta \in \mathbb{C}^*$ [2, pp18-19].

Proof

If $f = \alpha \prod_{i=1}^{m} f_i^{\lambda_i}$, $\alpha \in \mathbb{C}^*$ and f_i are irreducible in $\mathbb{C}[x_1, x_2]$ then let $\widehat{f} = \beta \prod_{i=1}^{m} f_i$. First note that

$$\begin{aligned} C &= \nu(f) \\ &= \nu(\alpha \textstyle\prod_{i=1}^{m} f_i^{\lambda_i}) \\ &= \nu(\textstyle\prod_{i=1}^{m} f_i^{\lambda_i}) \text{ by 4.2} \\ &= \textstyle\bigcup_{i=1}^{m} \nu(f_i^{\lambda_i}) \text{ by 4.3} \\ &= \textstyle\bigcup_{i=1}^{m} \nu(f_i) \text{ by 4.4} \\ &= \nu(\textstyle\prod_{i=1}^{m} f_i) \text{ by 4.3} \\ &= \nu(\beta \textstyle\prod_{i=1}^{m} f_i) \text{ by 4.2} \end{aligned}$$

$= \nu(\widehat{f})$

Let $g \in \mathbb{C}[x_1, x_2]$ such that $0 < \deg(g) < \deg(\widehat{f})$. Suppose $\forall i,\ f_i | g$. Then $\deg(g) \geq \deg(\prod_{i=1}^m f_i) = \deg(\widehat{f})$ which is a contradiction, hence $\exists i$ such that $f_i \not| g$. Then $\nu(f_i) \in Irr(\nu(\widehat{f}))$ but $\nu(f_i) \notin Irr(\nu(g))$. Therefore $Irr(\nu(\widehat{f})) \neq Irr(\nu(g))$ and so $\nu(g) \neq \nu(\widehat{f}) = C$. Hence $\nu(\widehat{f}) = \nu(f) = C$ and $\forall g \in \mathbb{C}[x_1, x_2]$ such that $0 < \deg(g) < \deg(\widehat{f})$, $C \neq \nu(g)$. Therefore $\widehat{f}$ is a minimal polynomial of f.

Suppose $\widehat{g}$ is also a mininal polynomial of f. As $\widehat{f}$ is a minimal polynomial of f, $\deg(\widehat{g}) = \deg(\widehat{f})$.

Suppose $\exists i$ such that $f_i \not| \widehat{g}$. Then $\forall h \in \mathbb{C}[x_1, x_2]$, $\widehat{g} \neq f_i h$ and so $\nu(\widehat{g}) \neq \nu(f_i) \cup \nu(h)$. Hence $\nu(f_i) \nsubseteq C$ and so $f_i \notin Irr(C)$, which is a contradiction. Therefore $\forall i,\ f_i | \widehat{g}$ and so $\widehat{g} = \beta \prod_{i=1}^m f_i = \beta \widehat{f}$ where $\beta \in \mathbb{C}[x_1, x_2]$. However, $\deg(\widehat{g}) = \deg(\widehat{f})$ and so $\deg(\beta) = 0$. Therefore $\widehat{g} = \beta \prod_{i=1}^m f_i$ where $\beta \in \mathbb{C}^*$.

□

Therefore if $C = \nu(f)$ is an algebraic curve, where $f = \alpha \prod_{i=1}^m f_i^{\lambda_i}$, $\alpha \in \mathbb{C}^*$ and f_i are irriducible in $\mathbb{C}[x_1, x_2]$, then $\min(f) = \{\beta \prod_{i=1}^m f_i \colon \beta \in \mathbb{C}^*\}$ is the set of all minimal polynomials of f and $1 \prod_{i=1}^m f_i$ is said to be the minimal polynomial of f, from now on denoted by $\widehat{f}$ [2, pp18-19].

Note that, $\forall\ C = \nu(f)$ where $\deg(f) \geq 1$, $\widehat{f} | f$.

6.3 The Equations of C

Let $C = \nu(f)$ be an algebraic curve, where $f = \alpha \prod_{i=1}^m f_i^{\lambda_i}$, $\alpha \in \mathbb{C}^*$ and f_i are irreducible in $\mathbb{C}[x_1, x_2]$, and $g \in \mathbb{C}[x_1, x_2]$. Then $\nu(g) = C = \nu(f)$ if and only if $g = \beta \prod_{i=1}^m f_i^{\mu_i}$ where $\beta \in \mathbb{C}^*$ [2, p18].

Proof

Let $C = \nu(f)$ be an algebraic curve, where $f = \alpha \prod_{i=1}^m f_i^{\lambda_i}$, $\alpha \in \mathbb{C}$ and f_i are irreducible in $\mathbb{C}[x_1, x_2]$, and $g \in \mathbb{C}[x_1, x_2]$. Note that $\widehat{f} = \prod_{i=1}^m f_i$.

Suppose that $\nu(g) = C = \nu(f)$ and $g = \beta \prod_{j=1}^n g_j^{\mu_j}$ where g_j are irreducible in $\mathbb{C}[x_1, x_2]$. Then $\{f_i\} = Irr(C) = \{g_j\}$. Therefore $m = |\{f_i\}| = |\{g_j\}| = n$ and so g must be of the form $g = \beta \prod_{i=1}^m f_i^{\mu_i}$.

Conversly, suppose $g = \beta \prod_{i=1}^m f_i^{\mu_i}$ where $\beta \in \mathbb{C}$. Then, by 6.2, $\widehat{g} = \prod_{i=1}^m f_i = \widehat{f}$ and so $\nu(g) = \nu(\widehat{g}) = \nu(\widehat{f}) = \nu(f) = C$.

□

Hence, if $C = \nu(f)$, where $f = \alpha \prod_{i=1}^m f_i^{\lambda_i}$, $\alpha \in \mathbb{C}^*$ and f_i are irreducible in $\mathbb{C}[x_1, x_2]$, all equations of C are of the form $\beta \prod_{i=1}^m f_i^{\mu_i}$ where $\beta \in \mathbb{C}^*$.

6.4 Degree of an Algebraic Curve

As we have seen, for any algebraic curve $C = \nu(f)$, there is not a unique equation defining C. Therefore, in order to talk about the degree of a curve, we refer to the degree of the minimal polynomial of f [3, p63].

$$\deg(C) = \deg(\widehat{f})$$

6.5 Division of Polynomials

Let $f, g \in \mathbb{C}[x_1, x_2]$ *then* $\nu(f) \subseteq \nu(g) \Leftrightarrow \widehat{f}|g \Leftarrow f|g$.

Proof

Suppose $\nu(f) \subseteq \nu(g)$. By 6.2, $\widehat{f} = \alpha \prod_{i=0}^{m} f_i$ where $\alpha \in \mathbb{C}^*$ and f_i are irreducible in $\mathbb{C}[x_1, x_2]$. Suppose $\widehat{f} \not| g$, then $\exists i$ such that $f_i \not| g$. Therefore, $\nu(f_i) \in Irr(\nu(\widehat{f}))$ but $\nu(f_i) \notin Irr(\nu(g)g)$. Hence $Irr(\nu(f)) = Irr(\nu(\widehat{f})) \not\subseteq Irr(\nu(g))$ and so $\nu(f) \not\subseteq \nu(g)$, which is a contradiction. Therefore $\widehat{f}|g$.

Conversely, suppose $f|g$ then, as $\widehat{f}|f$ and division is transative, $\widehat{f}|g$.

Finally, suppose $\widehat{f}|g$. Then $\exists h \in \mathbb{C}[x_1, x_2]$ such that $g = \widehat{f}h$. Hence, by 4.3, $\nu(g) = \nu(\widehat{f}) \cup \nu(h) = \nu(f) \cup \nu(h)$ and so $\nu(f) \subseteq \nu(g)$.

□

6.6 Irreducibility of C

$C = \nu(f)$ *is irreducible if and only if* $\widehat{f}$ *is irreducible in* $\mathbb{C}[x_1, x_2]$

Proof

Let $C = \nu(f)$ be an irreducible algebraic curve. Suppose that $\widehat{f}$ is reducible, then $\exists f_1, f_2 \in \mathbb{C}[x_1, x_2]$ with $0 < \deg(f_1), \deg(f_2) < \deg(\widehat{f})$ such that $\widehat{f} = f_1 f_2$. Then, by 4.3, $\nu(f_1) \cup \nu(f_2) = \nu(\widehat{f}) = C$ but, as C is irreducible, $\nu(f_1) = C = \nu(f_2)$. But $\deg(f_1) < \deg(\widehat{f})$ and so, as $\widehat{f}$ is the minimal polynomial of f, $C \neq \nu(f_1)$ which is a contradiction. Hence $\widehat{f}$ is irreducible in $\mathbb{C}[x_1, x_2]$.

Let $C = \nu(f)$ be an algebraic curve such that $\widehat{f}$ is irreducible in $\mathbb{C}[x_1, x_2]$. Suppose C is reducible, then $\exists g \in \mathbb{C}[x_1, x_2]$ with $\deg(g) \geq 1$ such that $\nu(g) \subset C = \nu(f)$. Then by 6.5, $g|\widehat{f} \Rightarrow \widehat{f} = gh$ where $h \in \mathbb{C}[x_1, x_2]$. But $\deg(g) \geq 1$ and $\widehat{f}$ is irreducible. Therefore $h \in \mathbb{C}^*$ and so by 4.2 $\nu(\widehat{f}) = \nu(g)$, which is a contradiction. Hence C is an irreducible algebraic curve.

□

7 Intersection of Algebraic Curves

One of the key properties of an algebraic curve is it's intersection with other curves. We observe that there are infact two distinct cases that can occur; depending on whether the two curves share a common component or not.

7.1 Lemma - Cancellation of Terms

Let $f, g \in \mathbb{C}[x_1, x_2]$ *be relatively prime. Then* $\exists a, b, a', b' \in \mathbb{C}[x_1, x_2]$ *such that* $af + bg = d \in \mathbb{C}[x_1]\backslash\{0_{\mathbb{C}[x_1]}\}$ *and* $a'f + b'g = d' \in \mathbb{C}[x_2]\backslash\{0_{\mathbb{C}[x_2]}\}$ *[6, pp7-8].*

Proof

Let $f, g \in \mathbb{C}[x_1, x_2]$ be relatively prime. Then $f(x_1, x_2) = \sum_{i=0}^{m} a_i(x_1)x_2^i$ and $g(x_1, x_2) = \sum_{j=0}^{n} b_j(x_1)x_2^j$ where $a_i, b_j \in \mathbb{C}[x_1]$. Note that $\deg_{x_2}(f) = m$ and $\deg_{x_2}(g) = n$. Without loss of generality we may assume that $m \leq n$.

As $\mathbb{C}$ is a field, $\mathbb{C}[x_1, x_2]$ is a Euclidean domain. Then $\exists q_0, q_1, \dots, q_l, r_0, r_1, \dots, r_l \in \mathbb{C}[x_1, x_2]$ where $r_i = \sum_{k=0}^{\lambda_i} c_{ik}(x_1)x_2^k$ with $l \leq \deg_{x_2}(g) = n < \infty$ such that:

- $p_0 g = q_0 f + r_0$ where $p_0(x_1) = \prod_{i=0}^{m} a_i(x_1)$, $\deg_{x_2}(r_0) < \deg_{x_2}(f)$ and $r_0 \neq 0$
- $p_1 f = q_1 r_0 + r_1$ where $p_1(x_1) = \prod_{k=0}^{\lambda_0} c_{0k}(x_1)$ $\deg_{x_2}(r_1) < \deg_{x_2}(r_0)$ and $r_0 \neq 0$
- For $i = 2, 3, \dots, l-1$, $p_i r_{i-2} = q_i r_{i-1} + r_i$ where $p_i(x_1) = \prod_{k=0}^{\lambda_{i-1}} c_{(i-1)k}(x_1)$, $0 < \deg_{x_2}(r_i) < \deg_{x_2}(r_{i-1})$ and $r_i \neq 0$
- $p_l r_{l-2} = q_l r_{l-1} + r_l$ where $p_l(x_1) = \prod_{k=0}^{\lambda_{l-1}} c_{(l-1)k}(x_1)$ and either $\deg_{x_2}(r_l) = 0$ or $r_l = 0$

Reversing this process, we easily obtain that $\exists a, b \in \mathbb{C}[x_1, x_2]$ such that $r_l = af + bg$.

We claim that $r_l \neq 0$. Assume otherwise, then consider r_{l-1}. By the Euclidean algorithm, $r_{l-1} = \gcd(f, g)$ but $\deg_{x_2}(r_{l-1}) > 0$, contradicting the statement that f and g are relativly prime. Hence

$$af + bg = d \in \mathbb{C}[x_1]\backslash\{0_{\mathbb{C}[x_1]}\}$$

By symmetry, we may repeat this process with x_2, obtaining that $\exists a', b' \in \mathbb{C}[x_1, x_2]$ such that

$$a'f + b'g = d' \in \mathbb{C}[x_2]\backslash\{0_{\mathbb{C}[x_1]}\}$$

□

7.2 Theorem - Intersection of Relatively Prime Algebraic Curves

Let $C = \nu(f)$ *and* $D = \nu(g)$ *be relatively prime algebraic curves. Then* $C \cap D$ *is a finite collection of points in* $\mathbb{C}^2$ *[6, p8].*

Proof

Let $C = \nu(f)$ and $D = \nu(g)$ be relatively prime algebraic curves. Then, by 7.1, $\exists a, b, a', b' \in \mathbb{C}[x_1, x_2]$ such that $af + bg = d \in \mathbb{C}[x_1]\backslash\{0_{\mathbb{C}[x_1]}\}$ and $a'f + b'g = d' \in \mathbb{C}[x_2]\backslash\{0_{\mathbb{C}[x_2]}\}$.

Assume $(x, y) \in \nu(f) \cap \nu(g)$, then $d(x) = a(x, y)f(x, y) + b(x, y)g(x, y) = a(x, y)0 + b(x, y)0 = 0$ and so x must be a root of d. Similarly y must be a root of d'. However, as $\deg(d) < \infty$ and $\deg(d') < \infty$, there are at most $\deg(d)\deg(d') < \infty$ distinct (x, y) pairs solving these equations. Hence $|C \cap D| = |\nu(f) \cap \nu(g)| = |\{(x, y) \in \mathbb{C}^2 \colon f(x, y) = 0, g(x, y) = 0\}| \leq \deg(d)\deg(d') < \infty$.

□

This fact gives us an easy test to see if $C \subset \mathbb{C}^2$ is possibly an algebraic curve or not. If $C \subset \mathbb{C}^2$ and D is an irreducible algebraic curve such that $D \nsubseteq C$ then C is an algebraic curve only if $|C \cap D| < \infty$. If, for example, $C = \nu(x_2 - \sin(x_1))$ and we consider $D = \nu(x_2)$ which is an irreducible algebraic curve such that $D \nsubseteq C$ the we see that $\forall n \in \mathbb{Z}$, $(2\pi n, 0) \in C \cap D$. Therefore C and D intersect at more than a finite number of points and so $C = \nu(x_2 - \sin(x_1))$ cannot be an algebraic curve [3, p10].

7.3 Theorem - Intersection of Algebraic Curves with a Common Component

If $C = \nu(f)$ and $D = \nu(g)$ are algebraic curves with a common component then $C \cap D$ is uncountable.

Proof

Let $C = \nu(f)$ and $D = \nu(g)$ be algebraic curves with a common component E. As E is a component of C and of D, $E \subseteq C \cap D$. But E is also an algebraic curve and so, by 4.1, contains an uncountable number of points. Therefore $C \cap D$ also contains an uncountable number of points.

□

8 Projective Mappings

Consider the algebraic curves $C = \nu(x_2 - 1)$ and $D = \nu(x_2 - x_1^2)$, which give a linear and elliptic equation in the $\mathbb{C}^2$ plane respectivly. However, the behavior 'at infinity' of $\nu(x_2 - 1)$ is very different from that of $\nu(x_2 - x_1^2)$. It is difficult, however, to make the concept of 'at infinity' meaningful if we restrict ourselves to working in just the $\mathbb{C}^2$ plane [2, p23] [3, p85].

To overcome this, we introduce the notion of complex projective space, which allows us to make precise the notion of 'at infinity' by including extra points [1, p17]. The behavior of an algebraic curve at these points gives us additional information about it [6, p17]. As it turns out, $\nu(x_2 - 1)$ has a singularity at one of those extra points while $\nu(x_2 - x_1^2)$ is 'smooth'.

8.1 Complex Projective Space

We define complex projective space by

$$\mathbb{CP}^2 = (\mathbb{C}^3 \backslash \{0\}, \sim)$$

In which $\sim$ is the equivalence relation $(a, b, c) \sim (x, y, z) \Leftrightarrow \exists \lambda \in \mathbb{C}^*$ such that $x = \lambda a, y = \lambda b$ and $z = \lambda c$ [2, pp23-24].

The equivalence classes of $\mathbb{CP}^2$ therefore consists of the straight lines in $\mathbb{C}^3$ passing through $(0, 0, 0)$. We may therefore talk about one of these lines simply by specifying a non-zero point on it, usually the point unit distance from $(0, 0, 0)$ on $S^2_{\mathbb{C}}$. We therefore differentiate between a point in complex projective space (x_1, x_2, x_3) and the equivalence class that it belongs to $[x_1 : x_2 : x_3]$.

We may therefore relate a point in the $\mathbb{C}^2$ plane with a line (equivalence class) in complex projective space it lies on by the embedding $\phi\colon \mathbb{C}^2 \to \mathbb{CP}^2$ [1, pp19-20] defined to be

$$\phi(x_1, x_2) = [x_1 : x_2 : 1]$$

We may think of the mapping ϕ as the preimage of the stereographic projection from $(0, 0, 0)$ of the complex unit ball ($S^2_{\mathbb{C}} \subset \mathbb{C}^3$) onto the $\mathbb{C}^2$ plane passing through, and perpendicular to, $(0, 0, 1)$. However, as antipodal points in $\mathbb{CP}^2$ lie in the same equivalence class, we need only consider a subset of it, denoted $H^2_{\mathbb{C}}$.

Therefore we may consider $\phi\colon \mathbb{C}^2 \to H^2_{\mathbb{C}} \cong \mathbb{CP}^2$ by

$$\phi(x_1, x_2) = \left(\frac{x_1}{\sqrt{x_1^2 + x_2^2 + 1}}, \frac{x_2}{\sqrt{x_1^2 + x_2^2 + 1}}, \frac{1}{\sqrt{x_1^2 + x_2^2 + 1}} \right) \cong [x_1 : x_2 : 1]$$

8.2 Projected Algebraic Curves

Let $C = \nu(f)$ be an algebraic curve in $\mathbb{C}^2$. We define the projected algebraic curve $\widetilde{C} \subset H^2_{\mathbb{C}}$ of C to be the image of C under ϕ [2, pp25-26], that is

$$\widetilde{C} = \phi(C) = \{\phi(x, y) \colon (x, y) \in C\}$$

Note that, as ϕ is an injective mapping and $C = \nu(f)$ contains an uncountable number of points, $\widetilde{C}$ does too.

Returning to our previous example of $C = \nu(x_2 - 1)$ and $D = \nu(x_2 - x_1^2)$ we see that:

If $(x, y) \in C$ then $\phi(x, y) = \left(\frac{x}{\sqrt{x^2+2}}, \frac{1}{\sqrt{x^2+2}}, \frac{1}{\sqrt{x^2+2}} \right)$ as $y = 1$

If $(x', y') \in D$ then $\phi(x', y') = \left(\frac{x'}{\sqrt{x'^4+x'^2+1}}, \frac{x'^2}{\sqrt{x'^4+x'^2+1}}, \frac{1}{\sqrt{x'^4+x'^2+1}} \right)$ as $y' = x'^2$

In order to understand these curves better 'at infinity', we may trace out the surface formed in $\mathbb{C}^2$, and thus $\mathbb{CP}^2$, by letting $v \in \mathbb{C}$ such that $\|v\| = 1$ and considering $\lim_{h \to \pm\infty} \phi(hv, y(hv))$.

In C we see that $\lim_{h \to \infty} \phi(hv, 1) = (v, 0, 0)$ and $\lim_{h \to -\infty} \phi(hv, 1) = (-v, 0, 0)$. However, for D, $\lim_{h \to \infty} \phi(hv, (hv)^2) = (0, v^2, 0) = \lim_{h \to -\infty} \phi(hv, (hv)^2)$. Thus, 'at infinity' D forms what appears to be a 'closed curve' in projective space and, although $(v, 0, 0) \sim (-v, 0, 0)$, as $h \to \infty$, the curve traced out on C tends to the 'opposite' point on $H^2_{\mathbb{C}}$ than when $h \to -\infty$. Thus, 'at infinity' the curves C and D are fundamentally different

Using projective space also allows us to formalise the concept from geometry that 'parallel lines intersect at infinity'. For example, let $C = \nu(ax_1 + bx_2 + c)$ and $D = \nu(ax_1 + bx_2 + d)$ where $a, b, c, d \in \mathbb{C}^*$ and $c \neq d$ which define lines in $\mathbb{C}^2$. Then we clearly see that, in the $\mathbb{C}^2$ plane, $\nexists (x, y) \in \mathbb{C}^2$ such that $(x, y) \in C \cap D$. However, in complex projective space, $\widetilde{C}$ and $\widetilde{D}$ intersect at the point $(\frac{b}{\sqrt{a^2+b^2}}, -\frac{a}{\sqrt{a^2+b^2}}, 0)$. This corresponds to the point 'at infinity' that both the lines pass through in the $\mathbb{C}^2$ plane.

8.3 Homogeneous Polynomials

Suppose $\widetilde{C}$ is the projection of an algebraic curve $C = \nu(f)$ into complex projective space. We have seen that a point (x, y) lies on C if and only if $f(x, y) = 0$. We therefore wish to see if we can find a similar situation for points (x, y, z) on $\widetilde{C}$.

As it turns out, it is possible to construct a polynomial $\widetilde{f}$ such that $(x, y, z) \in \widetilde{C}$ if and only if $\widetilde{f}(x, y, z) = 0$.

If $C = \nu(f)$ and $f(x_1, x_2) = \sum_{i=0}^{n} \sum_{j=0}^{m} \alpha_{ij} x_1^i x_2^j$ where $\alpha_{ij} \in \mathbb{C}$ and $p = \deg(f)$ then we claim that $(x, y, z) \in \widetilde{C}$ if and only if $\widetilde{f}(x, y, z) = 0$ [2, pp25-26], where $\widetilde{f}\colon \mathbb{C}^3 \to \mathbb{C}$ by

$$\widetilde{f}(x_1, x_2, x_3) = \sum_{i=0}^{n} \sum_{j=0}^{m} \alpha_{ij} x_1^i x_2^j x_3^{p-(i+j)} = f(\frac{x_1}{x_3}, \frac{x_2}{x_3}) x_3^p$$

We give the following sketch proof.

Let $(x, y, z) \in \widetilde{C}$. Suppose $z \neq 0$, then $\phi^{-1}(x, y, z) = (\frac{x}{z}, \frac{y}{z}) \in C$. Hence $0 = f(\phi^{-1}(x, y, z)) = \frac{\widetilde{f}(x,y,z)}{z^p}$ and so $\widetilde{f}(x, y, z) = 0$.

Suppose $z = 0$, then $\exists (x_i, y_i)_{i=1}^{\infty} \in C$ such that $\lim_{i\to\infty}(a_i, b_i, c_i) = (x, y, z)$ where $(a_i, b_i, c_i) = \phi(x_i, y_i)$. But $\forall i$, $\widetilde{f}(x_i, y_i, z_i) = f(\phi^{-1}(x_i, y_i, z_i)) z_i^p$. Hence $\widetilde{f}(x, y, z) = \lim_{i\to\infty} \widetilde{f}(a_i, b_i, c_i) = \lim_{i\to\infty} f(x_i, y_i) c_i^p = 0$.

Conversely, suppose $\widetilde{f}(x, y, z) = 0$. Suppose $z \neq 0$, then $f(\phi^{-1}(x, y, z)) = \frac{\widetilde{f}(x,y,z)}{z^p} = 0$. Hence $\phi^{-1}(x, y, z) = (\frac{x}{z}, \frac{y}{z}) \in C$ and so $(x, y, z) \in \widetilde{C}$.

Suppose $z = 0$, then $0 = \widetilde{f}(x, y, 0) = g(x, y)$ where $g(x_1, x_2) = \sum_{i=0}^{p} \alpha_{i(p-i)} x_1^i x_2^{p-i}$. Then $\lim_{h\to\infty} f(hx, hy) = g(x, y) = 0$ and so $\lim_{h\to 0} f(\phi^{-1}(x, y, h)) = 0$. Hence $(x, y, 0) \in \widetilde{C}$.

We say that $\widetilde{f}$ is the homogeneous polynomial of f and that, as $(x, y, z) \in \widetilde{C}$ if and only if $\widetilde{f}(x, y, z) = 0$, $\widetilde{f}$ defines the curve $\widetilde{C}$ [1, pp32-33].

8.4 Projective Transforms

When considering an algebraic curve C, we note that the properties of this curve (such as reducibility and degree) are invarient under a general linear transformation $A \in GL(2, \mathbb{C})$ [1, pp35-37]. Correspondingly, when considering a projected algebraic curve $\widetilde{C}$, we note that properties of this curve (again such as reducibility and degree) are invarient under a general linear transformation $A \in GL(3, \mathbb{C})$ [4, p39].

Suppose $\widetilde{f} \in \mathbb{C}[x_1, x_2, x_3]$ is the homogeneous polynomial of $f \in \mathbb{C}[x_1, x_2]$ and defines the curve $\widetilde{C}$ in $\mathbb{CP}^2$. Let $A \in GL(3, \mathbb{C})$ and define $g(x_1, x_2, x_3) = (f \circ A^{-1})(x_1, x_2, x_3)$. Then $g(x_1, x_2, x_3) \in \mathbb{C}[x_1, x_2, x_3]$ is a homogeneous polynomial defining the projective algebraic curve $\widetilde{D}$ in $\mathbb{CP}^2$ with the same properties as $\widetilde{C}$ [1, p40].

8.5 The Intersection of Two Projected Algebraic Curves

If C and D are two algebraic curves which intersect at $(x, y) \in \mathbb{C}^2$ then $\widetilde{C}$ and $\widetilde{D}$ intersect at $\phi(x, y) \in \mathbb{CP}^2$, although the converse is not necessarily true. For example, we have already seen that the parallel lines $C = \nu(ax_1 + bx_2 + c)$ and $D = \nu(ax_1 + bx_2 + d)$, where $a, b, c, d \in \mathbb{C}^*$ and $c \neq d$, intersect in $\mathbb{CP}^2$ but don't in $\mathbb{C}^2$. However, in 7.2 we saw that two relatively prime algebraic curves C and D intersect at only a finite number of points in $\mathbb{C}^2$, we therefore ask does the intersection of two projected algebraic curves still only contain a finite number of points in $H^2_{\mathbb{C}}$?

8.6 Theorem - Intersection of Relatively Prime Projected Algebraic Curves

Let $C = \nu(f)$ and $D = \nu(g)$ be relatively prime algebraic curves in $\mathbb{C}^2$. Then $\widetilde{C} \cap \widetilde{D}$ contains only finitely many points in $H^2_{\mathbb{C}}$.

Proof

Let $C = \nu(f)$ and $D = \nu(g)$ be relatively prime algebraic curves in $\mathbb{C}^2$.

We define A_1 and A_2 as follows:

$$A_1 = \{(x, y, z) \in H^2_{\mathbb{C}} \colon (x, y, z) \in \widetilde{C} \cap \widetilde{D}, z \neq 0\}$$

$$A_2 = \{(x, y, z) \in H^2_{\mathbb{C}} \colon (x, y, z) \in \widetilde{C} \cap \widetilde{D}, z = 0\}$$

Note that $\widetilde{C} \cap \widetilde{D} = A_1 \cup A_2$.

Firstly, consider $(x, y, z) \in A_1$. Consider $(\frac{x}{z}, \frac{y}{z})$, which exists and is well defined as $z \neq 0$. Then $\phi(\frac{x}{z}, \frac{y}{z}) = (x, y, z)$ and, as ϕ is injective, $(\frac{x}{z}, \frac{y}{z})$ is the only point in $\mathbb{C}^2$ mapping to (x, y, z). Therefore $(\frac{x}{z}, \frac{y}{z}) \in C \cap D$. But we have already seen in 7.2 that $C \cap D$ contains only a finite number of points and so A_1 does too.

Next consider A_2. If $p = \deg(f)$ and $q = \deg(g)$ and $f(x_1, x_2) = \sum_{i=0}^{n} \sum_{j=0}^{m} \alpha_{ij} x_1^i x_2^j$ and $g(x_1, x_2) = \sum_{i=0}^{n'} \sum_{j=0}^{m'} \beta_{ij} x_1^i x_2^j$ where $\alpha_{ij}, \beta_{ij} \in \mathbb{C}$. Then consider the homogenous equations of f and g, i.e. $f'(x_1, x_2, x_3) = \sum_{i=0}^{n} \sum_{j=0}^{m} \alpha_{ij} x_1^i x_2^j x_3^{p-(i+j)}$ and $g'(x_1, x_2, x_3) = \sum_{i=0}^{n'} \sum_{j=0}^{m'} \beta_{ij} x_1^i x_2^j x_3^{q-(i+j)}$. Then $f'(x_1, x_2, 0) = \sum_{i=0}^{p} \alpha_{i(p-i)} x_1^i x_2^{p-i} \in \mathbb{C}[x_1, x_2]$ and $g'(x_1, x_2, 0) = \sum_{i=0}^{q} \beta_{i(q-i)} x_1^i x_2^{q-i} \in \mathbb{C}[x_1, x_2]$. We can then see that $(x, y, 0) \in A_2$ if and only if $f'(x, y, 0) = 0 = g'(x, y, 0)$ and that this occurs if and only if $(x, y) \in \nu(f'(x_1, x_2, 0)) \cap \nu(g'(x_1, x_2, 0))$, i.e. (x, y) is in the intersection of two algebraic curves. Hence $A_2 = \nu(f'(x_1, x_2, 0)) \cap \nu(g'(x_1, x_2, 0))$ which, by 7.2, is a finite set. Hence A_2 contains only a finite number of points in the $\mathbb{C}^2$ plane.

Therefore, as A_1 and A_2 both contain a finite number of points, $\widetilde{C} \cap \widetilde{D}$ does too.

$\square$

9 Resultant

To further understand projected algebraic curves and their intersections, we now introduce the resultant function $\mathcal{R}_{\widetilde{f}\widetilde{g}} \colon \mathbb{C}[x_1, x_2, x_3] \times \mathbb{C}[x_1, x_2, x_3] \to \mathbb{C}[x_1, x_2]$. This gives us additional information about the homogeneous form of the polynomials f and g. This will in turn tell us more about the properties of the curve $C = \nu(f)$ and $D = \nu(g)$.

9.1 The Resultant Function

Let $\widetilde{f}, \widetilde{g} \in \mathbb{C}[x_1, x_2, x_3]$ be the homogeneous forms of the polynomials $f, g \in \mathbb{C}[x_1, x_2]$ respectivly. We may write $\widetilde{f}$ as $\widetilde{f}(x_1, x_2, x_3) = \sum_{i=0}^{m} \alpha_i x_3^i$ and $\widetilde{g}$ as $\widetilde{g}(x_1, x_2, x_3) = \sum_{j=0}^{n} \beta_j x_3^j$ where $\alpha_i, \beta_j \in \mathbb{C}[x_1, x_2]$. We define the resultant of $\widetilde{f}$ and $\widetilde{g}$ as the determinant of the Sylvester matrix whose elements have come from the coefficients α_i and β_j [4, p52]. Therefore the resultant of $\widetilde{f}$ and $\widetilde{g}$ is defined to be

$$\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2) = \det \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_m & 0 & 0 & \cdots & 0 \\ 0 & \alpha_0 & \alpha_1 & \cdots & \alpha_m & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_0 & \alpha_1 & \cdots & \alpha_m & 0 \\ 0 & 0 & \cdots & 0 & \alpha_0 & \alpha_1 & \cdots & \alpha_m \\ \beta_0 & \beta_1 & \cdots & \beta_n & 0 & 0 & \cdots & 0 \\ 0 & \beta_0 & \beta_1 & \cdots & \beta_n & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \beta_0 & \beta_1 & \cdots & \beta_n & 0 \\ 0 & 0 & \cdots & 0 & \beta_0 & \beta_1 & \cdots & \beta_n \end{pmatrix}$$

9.2 Properties of Resultant

Let $\widetilde{f}, \widetilde{g} \in \mathbb{C}[x_1, x_2, x_3]$ be homogeneous polynomials of f and g. The following properties of the resultant function $\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2)$ are given without proof [4, pp53-54]:

1. If $\widetilde{f}(0,0,1) \neq 0 \neq \widetilde{g}(0,0,1)$ then $\widetilde{f}$ and $\widetilde{g}$ are relatively prime if and only if $\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2) \neq 0_{\mathbb{C}[x_1,x_2]}$.
2. Let $\widetilde{f}(x_1, x_2, x_3) = \prod_{i=0}^{m}(x_3 - \alpha_i)$ and $\widetilde{g}(x_1, x_2, x_3) = \prod_{j=0}^{n}(x_3 - \beta_j)$ where $\alpha_i, \beta_j \in \mathbb{C}[x_1, x_2]$. Then $\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2) = \prod_{1 \leq i \leq m, 1 \leq j \leq n}(\alpha_i(x_1, x_2) - \beta_j(x_1, x_2))$.
3. Suppose $\widetilde{f}$ and $\widetilde{g}$ are relatively prime. Let $m = \deg(\widetilde{f}) = \deg(f)$ and $n = \deg(\widetilde{g}) = \deg(g)$. Then $\deg(\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2)) = mn$.
4. Suppose $\widetilde{f}$ and $\widetilde{g}$ are relatively prime. Then $\mathcal{R}_{\widetilde{f}\widetilde{g}}(a, b) = 0$ if and only if $ax_2 - bx_1 | \mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2)$.
5. Suppose $\widetilde{f}$ and $\widetilde{g}$ are relatively prime. Then $\mathcal{R}_{\widetilde{f}\widetilde{g}}(a, b) = 0$ if and only if $\exists c \in \mathbb{C}$ such that $\widetilde{f}(a, b, c) = 0 = \widetilde{g}(a, b, c)$.

10 Bézout's Theorem

We have already seen that the number of points of intersection of both two relatively prime algebraic curves and two relatively prime projected algebraic curves is finite. Using Bézout's Theorem and the newly defined resultant function we are now able to calculate a specific upper and lower bound for the number of points of intersection of two relatively prime projected algebraic curves. This upper bound will therefore also apply to relatively prime algebraic curves too, as the number of points of intersection of two relatively prime algebraic curves is less than or equal to the number of points of intersection when these curves are projected into complex projective space.

10.1 Lemma - Intersection of Projected Algebraic Curves is Non-Empty

Let $C = \nu(f)$ and $D = \nu(g)$ be algebraic curves in $\mathbb{C}^2$. Then $\widetilde{C} \cap \widetilde{D} \neq \emptyset$ [4, p54].

Proof

Let $C = \nu(f)$ and $D = \nu(g)$ be algebraic curves in $\mathbb{C}^2$, f' and g' be the homogeneous polynomials of f and g respectivly and $m = \deg(f)$ and $n = \deg(g)$. If $\gcd(f', g') > 1$, then, by 9.2 (1), $\mathcal{R}_{f'g'} = 0_{\mathbb{C}[x_1,x_2,x_3]}$. If f' and g' are relatively prime then, by 9.2 (3), $\deg(\mathcal{R}_{f'g'}) = mn$. In both cases $\exists (a, b) \in \mathbb{C}^2 \backslash (0, 0)$ such that $\mathcal{R}_{f'g'}(a, b) = 0$ and so by 9.2 (5) $\exists c \in \mathbb{C}$ such that $f'(a, b, c) = 0 = g'(a, b, c)$. Hence $(a, b, c) \in \widetilde{C} \cap \widetilde{D}$ and so $\widetilde{C} \cap \widetilde{D} \neq \emptyset$.

□

10.2 Weak Bézout's Theorem

Let $C = \nu(f)$ *and* $D = \nu(g)$ *be relatively prime algebraic curves. Then* $|\widetilde{C} \cap \widetilde{D}| \leq mn$ *where* $m = \deg(C)$ *and* $n = \deg(D)$ *[2, pp30-31] [4, pp54-55].*

Proof

Assume $|\widetilde{C} \cap \widetilde{D}| > mn$. Then $\exists p_0, p_1, \dots, p_{mn} \in H^2_{\mathbb{C}}$ such that $p_i \in \widetilde{C} \cap \widetilde{D}$. Let L_{ij} (with $i < j$) be the line in $\mathbb{C}^2$, with equation $l_{ij}(x_1, x_2)$, whose projection, $\widetilde{L_{ij}}$ in $\mathbb{CP}^2$, passes through p_i and p_j. Let $h = fg \prod_{0 \leq i < j \leq mn} l_{ij}$. Assume $\forall q \in H^2_{\mathbb{C}}$, $q \in \widetilde{\nu(f)} \cup \widetilde{\nu(g)} \cup \bigcup_{0 \leq i < j \leq mn} \widetilde{L_{ij}}$. Then $\forall q \in \mathbb{C}^2$, $q \in \nu(f) \cup \nu(g) \cup \bigcup_{0 \leq i < j \leq mn} L_{ij}$ and so $\nu(h) = \mathbb{C}^2$. Therefore $h(q) = 0 \Rightarrow h = 0_{\mathbb{C}[x_1, x_2]}$, which is a contradiction. Hence $\exists q \in H^2_{\mathbb{C}}$ such that

$$q \notin \widetilde{\nu(f)} \cup \widetilde{\nu(g)} \cup \bigcup_{0 \leq i < j \leq mn} \widetilde{L_{ij}}$$

Without loss of generality, we may assume that $q = (0, 0, 1)$, as, if it is not, we may apply a projective transform, A, in order to make it so [3, p104].

Then, as $(0, 0, 1) \notin \widetilde{\nu(f)} \cup \widetilde{\nu(g)} \cup \bigcup_{0 \leq i < j \leq mn} \widetilde{L_{ij}}$, $\widetilde{f}(0, 0, 1) \neq 0 \neq \widetilde{g}(0, 0, 1)$. As C and D are relatively prime, $\widetilde{C}$ and $\widetilde{D}$ are too and so, by 9.2 (1), $\mathcal{R}_{\widetilde{f}\widetilde{g}} \neq 0$. As $\deg(\widetilde{f}) = \deg(f) = \deg(C) = m$ and $\deg(\widetilde{g}) = \deg(g) = \deg(D) = n$, by 9.2 (3), $\deg(\mathcal{R}_{\widetilde{f}\widetilde{g}}) = mn$. Let $(a_i, b_i, c_i) = p_i$ then $\mathcal{R}_{\widetilde{f}\widetilde{g}}(a_i, b_i) = 0$ and so, by 9.2 (4), $a_i x_2 - b_i x_1 | \mathcal{R}_{\widetilde{f}\widetilde{g}}$.

Suppose $\exists i, j \in \mathbb{N}_0, \lambda \in \mathbb{C}$ such that $i < j$ and $a_i x_2 - b_i x_1 = \lambda(a_j x_2 - b_j x_1)$. Then $(a_i, b_i, c_i) = \lambda(a_j, b_j, c_j)$ and so $l_{ij} = a_i x_2 - b_i x_1$. Hence $(0, 0, 1) = q \in \widetilde{L_{ij}}$, which is a contradiction as q was assumed not to lie on any of the $\widetilde{L_{ij}}$ lines. Hence all of the pairs of $a_i x_2 - b_i x_1$ factors are relatively prime.

Therefore $\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2) = \alpha(x_1, x_2) \prod_{i=0}^{mn} (a_i x_2 - b_i x_1)$. But this implies that $\deg(\mathcal{R}_{\widetilde{f}\widetilde{g}}) > mn$, which is a contradiction. Hence $|\widetilde{C} \cap \widetilde{D}| \leq mn$.

□

Note that, as $(x, y) \in C \cap D \Rightarrow \phi(x, y) \in \widetilde{C} \cap \widetilde{D}$, we observe that $|C \cap D| \leq |\widetilde{C} \cap \widetilde{D}| \leq \deg(C) \deg(D)$.

10.3 Intersection Number

We have seen that 2 relatively prime algebraic curves intersect at at most $\deg(C) \deg(D)$ distinct points in $\mathbb{C}^2$ and $\mathbb{CP}^2$. However, by considering the situation of 'multiple intersections', we may construct an even stronger statement.

When considering polynomials in one variable, we say that $f \in \mathbb{C}[x_1]$ has a root of multiplictiy m at $\alpha \in \mathbb{C}$ if and only if $f(\alpha) = f'(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$ and $f^{(m)}(\alpha) \neq 0$.

Similarly, when considering polynomials in two variable we say that $f \in \mathbb{C}[x_1, x_2]$ has a root of multiplictiy m at $\alpha \in \mathbb{C}^2$ if and only if $f(\alpha) = \frac{\partial}{\partial x_1} f(\alpha) =$

$\frac{\partial}{\partial x_2} f(\alpha) = \frac{\partial^2}{\partial x_1^2} f(\alpha) = \frac{\partial^2}{\partial x_2^2} f(\alpha) = \cdots = \frac{\partial^{m-1}}{\partial x_1^{m-1}} f(\alpha) = \frac{\partial^{m-1}}{\partial x_2^{m-1}} f(\alpha) = 0$ and either $\frac{\partial^m}{\partial x_1^m} f(\alpha) \neq 0$ or $\frac{\partial^m}{\partial x_2^m} f(\alpha) \neq 0$.[3]

Let C and D be algebraic curves. Suppose that $\widetilde{C} \cap \widetilde{D} = \{p_1, p_2, \dots p_k\}$ where, by 10.2, $k \leq \deg(C)\deg(D)$ and $p_i = (a_i, b_i, c_i)$. We have seen that, without loss of generality, we may assume that

$$(0,0,1) \notin \widetilde{\nu(f)} \cup \widetilde{\nu(g)} \cup \bigcup_{0 \leq i < j \leq mn} \widetilde{L_{ij}}$$

Where L_{ij} (with $i < j$) is the line whose projection $\widetilde{L_{ij}}$ passes through p_i and p_j in $\mathbb{CP}^2$

This implies that $\widetilde{f}(0,0,1) \neq 0 \neq \widetilde{g}(0,0,1)$. As C and D are relatively prime, $\widetilde{C}$ and $\widetilde{D}$ are too and so, by 9.2 (1), $\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2) \neq 0$. As $\deg(\widetilde{f}) = \deg(f) = \deg(C) = m$ and $\deg(\widetilde{g}) = \deg(g) = \deg(D) = n$, by 9.2 (3) $\deg(\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2)) = mn$. Then $\forall i$, $\mathcal{R}_{\widetilde{f}\widetilde{g}}(a_i, b_i) = 0$ and so, by 9.2 (4), $a_i x_2 - b_i x_1 | \mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2)$.

Using this we may now define the intersection multiplicity of f and g at $p = (a, b, c) \in \mathbb{CP}^2$ [4, p59], $I \colon \mathbb{CP}^2 \times \mathbb{C}[x_1, x_2] \times \mathbb{C}[x_1, x_2] \to \mathbb{N}_0 \cup \{\infty\}$, by

$$I(p, f, g) = \max\{i \in \mathbb{N}_0 \cup \{\infty\} \colon (a x_2 - b x_1)^i | \mathcal{R}_{f'g'}(x_1, x_2)\}$$

10.3.1 Remark

Note that I satisfies the following key properties[4] [1, p42] [4, p59] [5, p478]:

- $I(p, f, g) = I(p, g, f)$
- $I(p, f, g) = \infty$ if and only if $\gcd(f, g)(p) = 0$
- $I(p, f, g) = 0$ if and only if $f(p) \neq 0$ or $g(p) \neq 0$
- $I(p, x_1 - a, x_2 - b) = 1$
- $I(p, f, hg) = I(p, f, h) + I(p, f, g)$, $\forall h \in \mathbb{C}[x_1, x_2]$
- $I(p, f + gh, g) = I(p, f, g)$, $\forall h \in \mathbb{C}[x_1, x_2]$

10.4 Strong Bézout's Theorem

Let $C = \nu(f)$ *and* $D = \nu(g)$ *be relatively prime algebraic curves. Then* $\sum_{p \in \widetilde{C} \cap \widetilde{D}} I(p, f, g) = mn$ *where* $m = \deg(C)$ *and* $n = \deg(D)$. *[2, p31] [3, pp112-115]*

Proof

---

[3] If f and g intersect at p, we may think of the intersection multiplicity of f and g at p as the maximum number of intersections it is possible to 'split' p into by applying small perterbations to the polynomials f and g [1, p35].

[4] Infact it is by these properties that $I(p, f, g)$ is actually computed for a particular point p.

Assume that we have $\widetilde{C} \cap \widetilde{D} = \{p_1, p_2, \dots p_k\}$ where, by 10.2 $k \leq \deg(C)\deg(D)$, and $p_i = (a_i, b_i, c_i)$. Let L_{ij} (with $i < j$) be the line in $\mathbb{C}^2$, with equation $l_{ij}(x_1, x_2)$, whose projection, $\widetilde{L_{ij}}$ in $\mathbb{CP}^2$, passes through p_i and p_j. As before, without loss of generality, we may assume that

$$(0,0,1) \notin \widetilde{\nu(f)} \cup \widetilde{\nu(g)} \cup \bigcup_{0 \leq i < j \leq mn} \widetilde{L_{ij}}$$

We claim that

$$\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2) = \alpha \prod_{i=1}^{k} (a_i x_2 - b_i x_1)^{I(p,f,g)}$$

Clearly, from the definition of $I(p, f, g)$, $\prod_{i=1}^{k}(a_i x_2 - b_i x_1)^{I(p,f,g)} | \mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2)$. Therefore $\mathcal{R}_{f'g'}(x_1, x_2) = \alpha(x_1, x_2) \prod_{i=1}^{k}(a_i x_2 - b_i x_1)^{I(p,f,g)}$ where $\alpha \in \mathbb{C}[x_1, x_2]$ and $\forall i$, $\gcd(\alpha(x_1, x_2), a_i x_2 - b_i x_1) = 1$. Suppose $\deg(\alpha(x_1, x_2)) > 0$ then $\nu(\alpha(x_1, x_2))$ is an algebraic curve and so, by 4.1, $\nu(\alpha) \neq \emptyset$. Let $(a', b') \in \mathbb{C}^2$ be such that $\alpha(a', b') = 0$. Then $\mathcal{R}_{\widetilde{f}\widetilde{g}}(a', b') = 0$ and so $\exists c' \in \mathbb{C}$ such that $\widetilde{f}(a', b', c') = 0 = \widetilde{g}(a', b', c')$. Therefore $(a', b', c') \in \widetilde{C} \cap \widetilde{D}$ and so $\exists i$ such that $(a', b', c') = p_i$, which is a contradiction. Hence $\deg(\alpha) = 0$ and so $\mathcal{R}_{\widetilde{f}\widetilde{g}}(x_1, x_2) = \alpha \prod_{i=1}^{k}(a_i x_2 - b_i x_1)^{I(p,f,g)}$ where $\alpha \in \mathbb{C}^*$

Therefore by considering the degree of each side of this equation we see that

$$\sum_{p \in \widetilde{C} \cap \widetilde{D}} I(p, f, g) = \deg(\alpha \prod_{i=1}^{k}(a_i x_2 - b_i x_1)^{I(p,f,g)}) = \deg(\mathcal{R}_{f'g'}(x_1, x_2)) = mn$$

□

Hence from 10.1,10.2 and 10.4 we conclude that, if $\widetilde{C}$ and $\widetilde{D}$ are projections of algebraic curves $C = \nu(f)$ and $D = \nu(g)$ with no common components into complex projective space, then

$$1, |C \cap D| \leq |\widetilde{C} \cap \widetilde{D}| \leq \sum_{p \in \widetilde{C} \cap \widetilde{D}} I(p, f, g) = \deg(C)\deg(D)$$

References

[1] Robert Bix. *Conics and Cubics.* Springer, second edition, 2006.

[2] Gerd Fischer. *Plane Algebraic Curves*, volume 15 of *Student Mathematical Library.* AMS, 2001.

[3] Fulton. *Algebraic Curves.* Addison-Wesley Publishing Company Inc., 1969.

[4] Frances Kirwan. *Complex Algebraic Curves.* London Mathematical Society Student Texts. Cambridge University Press, 1992.

[5] Anthony W. Knapp. *Advanced Algebra.* Cornerstones. Springer, 2008.

[6] Ernst Kunz. *Introduction to Plane Algebraic Curves.* Springer, 2005.