MAS345 Algebraic Geometry of Curves: Notes

AJ Duncan, September 29, 2003

0 Introduction

Background

As we shall see in due course an *Affine Algebraic Curve* C is the collection of points

$$C = \{(u, v) \in\ k \times k | f(u, v) = 0\}$$

where k is a field and $f(x, y)$ is a polynomial with coefficients in k (e.g. the set of points (x, y) satisfying $2x^2 + y^3 - xy = 0$ in $\mathbb{R} \times \mathbb{R}$).

Real algebraic curves, that is curves

$$C = \{(u, v) \in\ \mathbb{R} \times \mathbb{R} | f(u, v) = 0\}$$

where $f(x, y)$ is a polynomial with coefficients in $\mathbb{R}$ have been studied for over two thousand years. For instance, the Greeks described Real curves as loci of points: a circle is the locus of points at a fixed distance from a point O. Nowadays the theory of real algebraic curves has applications in many areas, for example mechanical engineering, optics, computer visualisation and coding theory.

A problem studied by the Greeks was that of 'Doubling the cube'. Given a cube D with edges of length a (and so of volume a^3) construct a cube of volume $2a^3$. The problem is to find the length of an edge of such a cube. That is, to find x with $x^3 = 2a^3$. In about 350 *b.c.* Menaechmus gave the solution as the intersection of the two curves $a^3y = x^2$ and $xy = 2$. The Greeks wasted a lot of time trying to construct these two conics with ruler and compasses; a task we now know to be impossible (see any account of *Galois* Theory).

With the introduction of a systematic algebraic notation in 17th Century and the idea developed by Descartes and Fermat of describing the plane in terms of Cartesian coordinates the theory of algebraic curves took on new life. In due course, around 1700, Newton made a study of *cubic* curves, which are those described by polynomials of degree 3. He classified them and described 72 different kinds. His investigations also included an examination of *singularities* of curves, that is points at which they have no uniquely defined tangent. Much of this course is based on modern interpretation of the methods of Newton.

Later it was realized that it was useful, and in many cases more illuminating, to look at curves in the complex plane, described by polynomials with complex coefficients. Furthermore it was discovered that adding points at infinity to the line to obtain projective space made it easier to understand the behaviour of curves. By the end of the nineteenth century Dedekind and Weber had begun the study of curves and surfaces in projective spaces over an arbitrary field (instead of the complex or real numbers).

Algebraic curves are today reasonably well understood: that is a classification of curves has been made and the intersections of curves can be described. For higher dimensional objects (zeroes of $f(x_1, ..., x_n) = 0$, etc.) no such classification exists and the description of intersections is a difficult task. However the successful theory of algebraic curves provides a base from which to work on the general theory.

Applications

In almost all branches of mathematics some aspect of algebraic geometry is lurking. Here is one example. A famous problem of number theory is Fermat's conjecture: if n is an integer $n > 2$ then there are no positive integer solutions to

$$x^n + y^n = z^n \,.$$

Reformulate the equation as

$$(\frac{x}{z})^n + (\frac{y}{z})^n = 1$$

and this problem becomes that of deciding whether the curve

$$r^n + s^n - 1 = 0$$

has any points in $\mathbb{Q} \times \mathbb{Q}$. The recent proof of this result by Wiles is based to a large extent on the theory of Elliptic curves.

The theory of Algebraic Curves is the basis for an encryption system that is widely used in commercial applications. In the last part of the course the construction underlying these codes will be studied briefly.

Aims of the Course

The course is an introduction to Algebraic Geometry. We shall concentrate on the simplest case of the objects studied in this field, that is on Algebraic Curves, mainly over fields of characteristic zero, namely $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{Q}$, but sometimes also over fields of finite characteristic ($\mathbb{Z}_p$, $\mathbb{Z}_{p^2}, ...$). We shall study curves in Affine and Projective space. The primary object is to understand how curves intersect, both with each other and themselves.

Further Reading

Library: Section 514.2
E Brieskorn & Knörrer, Plane Algebraic Curves, (nice pictures).
J Dieudonne, History of Algebraic Geometry, (worth browsing through).
C G Gibson, Elementary Geometry of Algebraic Curves, (well written, lots of examples).
F Kirwan, Complex Algebraic Curves, (well presented at about the right level).
M Reid, Undergraduate Algebraic Geometry, (also about the right level but not as well explained as Kirwan's book).
R J Walker, Algebraic Curves, (good background reading).

1 Fields and Polynomials

Fields

This subsection is mainly for background reading. The only parts of the section you need to know for assessment are Examples 1.1 numbers 1 and 3. A **field** consists of a set k together with binary operations of addition $+$ and multiplication $*$ on k that satisfy the field axioms listed below.

Field Axioms

$k1$. $x + y \in k$, for all $x, y \in k$ *(closure of* $+$*).*

$k2$. There exists an element $0 \in k$ such that $x + 0 = x$, for all $x \in k$ *(identity for* $+$*)*;

$k3$. If $x \in k$ then there exists an element $-x \in k$ such that $x + (-x) = 0$ *(inverse law for* $+$*).*

$k4$. $x + y = y + x$, for all $x, y \in k$ *(commutative law for* $+$).

$k5$. $(x + y) + z = x + (y + z)$, for all $x, y, z \in k$ *(associative law for* $+$*).*

$k6$. $x * y \in k$, for all $x, y \in k$ *(closure of* $*$*).*

$k7$. There exists an element $1 \in k$ such that $x * 1 = x$, for all $x \in k\backslash\{0\}$ *(identity for* $*$*).*

$k8$. If $x \in k\backslash\{0\}$ then there exists an element $y \in k$ such that $x * y = 1$ *(inverse law for* $*$*).*

$k9$. $x * y = y * x$, for all $x, y \in k$ *(commutative law for* $*$*).*

$k10$. $(x * y) * z = x * (y * z)$, for all $x, y, z \in k$ *(associative law for* $*$*).*

$k11$. $(x + y) * z = (x * z) + (y * z)$, for all $x, y, z \in k$ *(distributive law).*

Note: We usually write ab instead of $a * b$.

Example 1.1.

1. Familiar fields are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

2. Another common example of a field is $\mathbb{Q}[i]$ the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and i. Elements of $\mathbb{Q}[i]$ are all of the form $a + bi$, where a and b are in $\mathbb{Q}$. All these fields contain $\mathbb{Z}$.

3. The number of elements of a field is called its *order*. Fields $\mathbb{Z}_2$, $\mathbb{Z}_3$,$\mathbb{Z}_5$ and in general $\mathbb{Z}_p$, where p is a prime are finite of order 2, 3, 5 and p, respectively.

4. Any finite field has order p^n, for some prime p and positive integer n. In fact, up to isomorphism, there is exactly one field of order p^n, called GF(p^n), for each prime p and positive integer n. The field GF(p^n) contains $\mathbb{Z}_p$, that is GF(p). The field GF(4) has 4 distinct elements $\{0, 1, \alpha, \beta\}$ and addition and multiplication are defined according to the following tables.

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$*$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Note that $\alpha^2 = \beta$ and that $1 + \alpha + \alpha^2 = 2\beta = 0$. Others finite fields of order p^n are constructed similarly.

Every field either contains $\mathbb{Z}$ (and is infinite) or contains $\mathbb{Z}_p = \text{GF}(p)$, for some prime p. A field containing $\mathbb{Z}$ is said to have **characteristic** 0 whilst a field containing $\mathbb{Z}_p$ has **characteristic** p. Given any prime p the field $\text{GF}(p^n) \subseteq \text{GF}(p^{n+1})$. We may construct an infinite field of characteristic p by taking the union $\cup_{n\geq 1}\text{GF}(p^n)$.

There are many cases of sets k in which the field axioms all hold except for axiom $k8$. In this case we call k a **commutative ring**. For example, the integers, $\mathbb{Z}$, and the integers modulo n, denoted $\mathbb{Z}_n$, are commutative rings (even when n is not prime). If k is a field and t a variable the set of polynomials in t with coefficients in k is a commutative ring (when polynomials are added and multiplied in the usual way). We shall define polynomials in several variables and find that these also form commutative rings.

Monomials and Polynomials

Definition 1.2. A **monomial** in $x_1, \ldots, x_n$ is and expression of the form

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

where $x_1, \ldots, x_n$ are distinct variables and $\alpha_1, \ldots \alpha_n$ are non–negative integers. The **degree** of the monomial above is $\alpha_1 + \ldots + \alpha_n$. The **degree** of the variable x_i is α_i.

Two monomials $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $x_1^{\beta_1} \cdots x_n^{\beta_n}$ are equal if and only if $\alpha_i = \beta_i$, for $i = 1, \ldots, n$.

Product of monomials

Multiplication of monomials is defined by the rule

$$(x_1^{\alpha_1} \cdots x_n^{\alpha_n})(x_1^{\beta_1} \cdots x_n^{\beta_n}) = x_1^{\alpha_1+\beta_1} \cdots x_n^{\alpha_n+\beta_n}.$$

Note: From the definition we have

$$(x_1^0 \cdots x_n^0)(x_1^{\beta_1} \cdots x_n^{\beta_n}) = x_1^{\beta_1} \cdots x_n^{\beta_n}$$

and

$$(x_1^{\alpha_1} \cdots x_n^{\alpha_n})(x_1^{\beta_1} \cdots x_n^{\beta_n}) = (x_1^{\beta_1} \cdots x_n^{\beta_n})(x_1^{\alpha_1} \cdots x_n^{\alpha_n}).$$

Definition 1.3. Let k be a field. A **polynomial** f over k in variables $x_1, \dots, x_n$ is a sum

$$f = f(x_1, \dots, x_n) = \sum_{\alpha_1,\dots,\alpha_n} a_{\alpha_1,\dots,\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

where

1. $\alpha_1, \dots, \alpha_n$ runs over all n–tuples of non–negative integers,
2. $a_{\alpha_1,\dots,\alpha_n} \in k$, for all $\alpha_1, \dots, \alpha_n$ and
3. $a_{\alpha_1,\dots,\alpha_n} = 0$, for all but finitely many $\alpha_1, \dots, \alpha_n$.

When convient we write α for the n–tuple $\alpha_1, \dots, \alpha_n$ and $a_\alpha \mathbf{x}^\alpha$ for $a_{\alpha_1,\dots,\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Two polynomials $\sum_\alpha a_\alpha \mathbf{x}^\alpha$ and $\sum_\alpha b_\alpha \mathbf{x}^\alpha$ are equal if and only if $a_\alpha = b_\alpha$, for all α. When writing polynomials we use the following conventions.

1. We do not write down $a_{\alpha_1,\dots,\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for any α such that $a_\alpha = 0$. We call the polynomial with $a_\alpha = 0$, for all α, the **zero** polynomial and write it as 0.
2. We omit $x_i^{\alpha_i}$ from $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ if $\alpha_i = 0$. In particular we write a instead of $a x_1^0 \cdots x_n^0$. Thus $2x_1^2 x_2^0 x_3^3$ is written as $2x_1^2 x_3^3$ and $3x_1^0 x_2^0 x_3^4$ as $3x_3^4$.

Definition 1.4. Let

$$f(x_1, \dots, x_n) = \sum_{\alpha_1,\dots,\alpha_n} a_{\alpha_1,\dots,\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

be a polynomial over k.

1. $a_{\alpha_1,\dots,\alpha_n}$ is called the **coefficient** of the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.
2. If $a_\alpha \neq 0$ we call $a_\alpha \mathbf{x}^\alpha$ a **term** of f.
3. The **degree** of the term $a_\alpha \mathbf{x}^\alpha$ is the degree of the monomial $\mathbf{x}^\alpha$. The **degree** of x_i in the term $a_\alpha \mathbf{x}^\alpha$ is the degree of x_i in $\mathbf{x}^\alpha$.
4. If f is not the zero polynomial then the **degree** of f is the maximum of the degrees of the terms of f and the **degree** of x_i in f is the maximum of the degrees of x_i in the terms of f. If f is the zero polynomial then f has **degree** $-\infty$.

Example 1.5.

1. The following are polynomials in variables x_1, x_2 and x_3. The first two are monomials

polynomial	**degree**	**degree in x_1**
x_1	1	1
$x_1^7x_2^3x_3^{11}$	21	7
$1+x_1+x_2+2x_1^2+x_1x_2+3x_2^3x_3^2$	5	2
0	$-\infty$	$-\infty$
1	0	0
$x_1^2+x_2^2$	2	2
$x_3^7+x_2^3+3x_3x_2+3$	7	0

2. The following is a polynomial in x, y and z.

$$f(x,y,z) = 3x^3y^{19} + 2xyz^8 - 2zy^{12} + 5xyz + 13x - 3z + 2.$$

The polynomial f has degree 22 and the degree of z in f is 8. The terms of f are

$$3x^3y^{19},\ 2xyz^8,\ -2zy^{12},\ 5xyz,\ 13x,\ -3z,\ 2$$

which have degree 22, 10, 13, 3, 1, 1 and 2, respectively.

3. The polynomial 2 has one term, namely 2, of degree 0. The polynomial 0 has no terms and

is of degree $-\infty$.

The set of all polynomials over k in variables $x_1, \ldots, x_n$ is denoted $k[x_1, \ldots, x_n]$. We wish to define addition of polynomials in such a way as to make $k[x_1, \ldots, x_n]$ a vector space over k with basis the set of all monomials in variables $x_1, \ldots, x_n$. In particular this means that if $f = a\mathbf{x}^\alpha$ and $g = b\mathbf{x}^\alpha$, for some $a, b \in k$, we require

$$f + g = (a + b)\mathbf{x}^\alpha.$$

This leads to the following definition

Definition 1.6. Let

$$f = \sum_\alpha a_\alpha \mathbf{x}^\alpha \text{ and } g = \sum_\alpha b_\alpha \mathbf{x}^\alpha$$

be polynomials. The **sum** $f + g$ of f and g is

$$f + g = \sum_\alpha (a_\alpha + b_\alpha)\mathbf{x}^\alpha.$$

It is easy to check that, with this definition of addition, $k[x_1, \ldots, x_n]$ is a vector space over k with the required basis.

Example 1.7.

1. Let

$$f = x_1^2 + x_2^2 + x_1^2 x_2$$

and $g = 2x_1^2 + x_1x_2 - 3x_2^2 + 1$ then

$$f + g = 3x_1^2 - 2x_2^2 + x_1^2x_2 + x_1x_2 + 1.$$

2. Let $f = 71x^4y^{11}z^9 - 15xy^5z + 33xyz + 4$ and $g = 9x^4y^{10}z^9 + 10xy^5z - 23xzy - 9$ then

$$f + g = 71x^4y^{11}z^9 + 9x^4y^{10}z^9 - 5xy^5z + 10xyz - 5.$$

We now wish to extend the definition of multiplication of monomials to multiplication of polynomials in such a way as to make the vector space $k[x_1, \ldots, x_n]$ into a commutative ring. To simplify notation, if $\alpha = \alpha_1, \ldots, \alpha_n$ and $\beta = \beta_1, \ldots, \beta_n$ we write $\alpha + \beta = \alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n$. To meet our requirement we need to define multiplication so that if $f = a\mathbf{x}^\alpha$ and $g = b\mathbf{x}^\beta$ then

$$fg = ab\mathbf{x}^\alpha\mathbf{x}^\beta = ab\mathbf{x}^{\alpha+\beta},$$

(where the second equality follows from the definition of product of monomials). Using axiom $F11$ this means that if $f = \sum_\alpha a_\alpha\mathbf{x}^\alpha$ and g is as above then we require

$$fg = \sum_\alpha a_\alpha b\mathbf{x}^{\alpha+\beta}.$$

We are thus led to following definition of product.

Definition 1.8. Let

$$f = \sum_\alpha a_\alpha\mathbf{x}^\alpha \text{ and } g = \sum_\alpha b_\alpha\mathbf{x}^\alpha$$

be polynomials. The **product** fg of f and g is

$$fg = \sum_\gamma c_\gamma\mathbf{x}^\gamma,$$

where

$$c_\gamma = \sum_{\alpha+\beta=\gamma} a_\alpha b_\beta.$$

Example 1.9.

1. Let $f = xy + 1$ and $g = x + y^2$. Then

$$fg = x^2y + xy^3 + x + y^2.$$

2. Let $f = x^2 + y^2 + 1$ and $g = xy^2 + x^3 + 2$ then

$$fg = x^3y^2 + x^5 + 2x^2 + xy^4 + x^3y^2 + 2y^2 + xy^2 + x^3 + 2 = 2x^3y^2 + x^5 + 2x^2 + xy^4 + 2y^2 + xy^2 + x^3 + 2.$$

2 Affine curves

Definition 2.1. Let k be a field and let n be a positive integer. **Affine $\mathbf{n}$–space over** k is the set

$$\mathbb{A}_n(k) = \{(a_1, \ldots, a_n) : a_i \in k, \text{ for } i = 1, \ldots, n\}.$$

We call the elements $(a_1, \ldots, a_n)$ **points** of $\mathbb{A}_n(k)$.

Example 2.2.

1. The affine line $\mathbb{A}_1(k)$ when k is $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ and $GF(p)$.

2. The affine plane $\mathbb{A}_2(k)$, for the same fields.

3. $\mathbb{A}_3(k)$, for these fields.

A polynomial $f \in k[x_1, \dots x_n]$ may be written as $f(x_1, \dots, x_n)$ and then $f(a_1, \dots, a_n)$ used to denote the element of k obtained by substituting a_i for x_i, for $i = 1, \dots, n$, throughout f. If $f(a_1, \dots, a_n) = 0$ we say that $(a_1, \dots, a_n)$ is a **zero** of f.

Definition 2.3. Let f be a non–constant polynomial of degree d in variables x, y over the field k. Then the set of points

$$C_f = \{(a, b) \in \mathbb{A}_2(k) : f(a, b) = 0\}$$

is called a **curve over** k with **equation** $f = 0$. We say that C_f has **degree** d and is a curve **in** $\mathbb{A}_2(k)$.

We shall refer to C_f as the curve **defined** by f and with **polynomial** f. Note that a curve may have many different equations as can be seen from the following examples. In spite of this we often refer to the curve C_f merely as C.

Example 2.4.

1. Examples of introduction and Exercises 1, Drawing curves.

2. A curve of degree 1 is called a **line**.

3. A curve of degree 2 is called a **conic**.

4. Curves of degree 3, 4 and 5 are called a **cubic**, **quartic** and **quintic**, respectively.

5. Consider the curves C_f and C_g, where $f = x^2 - y$ and $g = x^4 - 2x^2y + y^2$.

   In $\mathbb{A}_2(\mathbb{R})$ both these curves are parabolas and $C_f = C_g$. This is no coincidence as (for arbitrary k)

$$g = x^4 - 2x^2y + y^2 = (x^2 - y)^2 = f^2.$$

   Hence $g(a, b) = 0$ if and only if $f(a, b) = 0$. In some sense C_g is C_f repeated twice. To make this precise and to cope with the ambiguity inherent in this situation we look again at polynomials.

Polynomials again

Lemma 2.5. *Let f and g be elements of $k[x_1, \ldots, x_n]$. Then*

1. degree(fg) = degree(f) + degree(g) *and*

2. degree$(f+g) \leq \max\{\text{degree}(f), \text{degree}(g)\}$

Furthermore, for $1 \leq i \leq n$*,*

3. *the degree of* x_i *in* fg *is equal to* $[$*degree of* x_i *in* $f] + [$*degree of* x_i *in* $g]$ *and*
4. *the degree of* x_i *in* $f+g \leq \max\{$*degree of* x_i *in* f*, degree of* x_i *in* $g\}$.

For example with $f = x^2 - y$ and $g = x^3y - 1$ we have $fg = x^5y - x^3y^2 - x^2 + y$ while degree$(f) = 2$, degree$(g) = 4$ and degree$(fg) = 6$. Furthermore the degrees of x in f, g and fg are 2, 3 and 5, respectively. Also $f + g = x^3y + x^2 - y - 1$ which has degree 4 and in which the degree of x is 3. Note that if f is as above and $h = 1 - x^2$ then the degree of $f + h$ is 1, which is strictly less than $\max\{\text{degree}(f), \text{degree}(h)\}$.

Definition 2.6. Let f and g be elements of $k[x_1, \ldots, x_n]$. We say that g **divides** f or g is a **factor of** f, written $g|f$, if there exists an element $h \in k[x_1, \ldots, x_n]$ such that $f = gh$.

For example $x^2yz - xz^2 - xy^3 + y^2z$ has factors $xy - z$ and $xz - y^2$.

Definition 2.7. A non–constant polynomial f over a field k is **reducible** if there exist non–constant polynomials g and h, over k, such that $f = gh$. A non–constant polynomial is **irreducible** if it is not reducible.

Example 2.8.

1. The polynomial x^n is reducible if $n > 1$ and irreducible if $n = 1$.
2. The polynomial $x^2 - y^2$ is reducible as $x^2 - y^2 = (x + y)(x - y)$.

3. Let $f = x^2yz - xz^2 - xy^3 + y^2z$.

   Then $f = gh$, where $g = xy - z$ and $h = xz - y^2$, so f is reducible.

4. All polynomials of degree 1 are irreducible.

   To see this suppose that f is a polynomial of degree 1 and that $f = gh$, where g and h are non–constant polynomials. Then

$$1 = \text{degree}(f) = \text{degree}(g) + \text{degree}(h).$$

   If g and h are non–constant then degree$(g) \geq 1$ and degree$(h) \geq 1$. Hence $1 = \text{degree}(g) + \text{degree}(h) \geq 2$, a contradiction. Thus f is not reducible.

5. The polynomial $f = x^2 - y$ is irreducible.

   We shall prove this. Suppose that f is reducible. Then there exist non–constant polynomials g and h such that $f = gh$. As g and h are non–constant they both have degree at least

1. As $2 = \text{degree}(f) = \text{degree}(g) + \text{degree}(h)$ it follows, from Lemma 2.5 part 1, that $\text{degree}(g) = \text{degree}(h) = 1$. Hence we may write $g = ax + by + c$ and $h = px + qy + r$, for some elements $a, b, c, p, q, r \in k$. We now have

$$f = x^2 - y = gh = apx^2 + (aq + bp)xy + bqy^2 + (ar + cp)x + (br + cq)y + cr.$$

Comparing coefficients we have

$$ap = 1, \tag{2.1}$$

$$br + qc = -1, \tag{2.2}$$

$$aq + bp = bq = ar + cp = cr = 0. \tag{2.3}$$

From (2.1), $a \neq 0$ and $p \neq 0$. Given that $cr = 0$, either $c = 0$ or $r = 0$. Let us first assume that $c = 0$. Then, from (2.3) we have $ar = 0$, and since $a \neq 0$ so $r = 0$. Similarly, if $r = 0$ we obtain $c = 0$. Therefore $c = r = 0$. Similarly $b = q = 0$. However (2.2) now implies $0 = -1$, a contradiction. We conclude that f is irreducible.

6. In contrast to the last example the reducibility of the polynomial $f = x^2 + y^2$ depends upon the ground field k.

   If $k = \mathbb{C}$ the polynomial factorizes as $f = (x + iy)(x - iy)$, so f is reducible over $\mathbb{C}$. If $k = \mathbb{R}$ the polynomial is irreducible. This follows from the uniqueness of factorization, below. If $k = \mathbb{Z}_2$ then

$$(x + y)^2 = x^2 + 2xy + y^2 = x^2 + y^2,$$

   so f is reducible over $\mathbb{Z}_2$. If $k = \mathbb{Z}_3$ it is easy to show, using the method of the above example, that f is irreducible.

7. As a final example we show that the polynomial $f = x^2 - y^3$ is irreducible over an arbitrary field k.

Suppose then that $f = gh$, where g and h are non–constant polynomials. It follows from Lemma 2.5.3 that the degree of x in g is $0, 1$ or 2 and that the degree of x in h is $2-($degree of x in $g)$. Suppose first that the degree of x in g is 0. Then $g \in k[y]$ and $h = ax^2 + bxy + cx + h'$, where $h' \in k[y]$. Then

$$f = gh = gax^2 + gbxy + gcx + gh'.$$

The coefficient of $y^r x^2$ in f, for $r > 0$, is equal to 0 and it follows on comparing coefficients that g is constant, a contradiction. Hence the degree of x in g is not 0. Since the same applies to h it follows that the degree of x in both g and h is 1. Therefore there are polynomials g' and h' in $k[y]$ such that $g = ax + g'$ and $h = bx + h'$, with a, b non–zero elements of k. We have

$$f = gh = abx^2 + (ah' + bg')x + g'h'.$$

Now f has no terms of degree 1 in x, so $ah' + bg' = 0$. Furthermore $g'h' = -y^3$. We may assume that $g' = py^2$ and $h' = qy$, with $p, q \in k$ and $pq = -1$. Then $p \neq 0$ and $q \neq 0$, so $ah' + bg' = aqy + bpy^2 \neq 0$, a contradiction. We conclude that f is irreducible.

Remark: A non–constant polynomial is irreducible if its only factors are constants and constant multiples of itself. That is, if f is irreducible and $g|f$ then either g is a constant or $g = af$, for some $a \in k$. Compare this to the situation in the integers $\mathbb{Z}$. In $\mathbb{Z}$ the irreducible elements are primes. The factors of a prime p are ± 1 and $\pm p$.

Given a reducible polynomial f, of degree d, we can, as we have seen in the examples above, write $f = gh$, where $1 \leq \text{degree}(g) \leq d - 1$ and $1 \leq \text{degree}(h) \leq d - 1$. If either g or h is reducible then we can repeat the process, factorizing into polynomials of lower degree. Eventually we obtain an expression

$$f = q_1 \cdots q_s,$$

where q_i is an irreducible polynomial. A factorization of f into a product of irreducible polynomials is called an **irreducible factorization** of f.

Theorem 2.9. *Let f be a polynomial in $k[x_1, \ldots, x_n]$. Then f has an irreducible factorization. This factorization is unique up to the order of the irreducible factors and multiplication by constants.*

Partial proof. We have shown above that a polynomial has an irreducible factorization. The second sentence of the theorem means that if f has irreducible factorizations $f = q_1 \cdots q_s$ and $f = q'_1 \cdots q'_t$, then $t = s$ and that

$$q_1 = a_1 q'_{i_1}, \ldots, q_s = a_s q'_{i_s},$$

for some $a_1, \ldots, a_s \in k$ and permutation $(i_1, \ldots, i_s)$ of $(1, \ldots, s)$. We shall not attempt to prove this here.

Example 2.10.

1. The polynomial $x^2 - y^2$ has irrreducible factorisation $(x + y)(x - y)$.
2. Let $f = x^2yz - xz^2 - xy^3 + y^2z$. Then f has irreducible factorisation gh, where $g = xy - z$ and $h = xz - y^2$. This follows from the previous example and the fact (which you should check) that g and h are irreducible.

Reducible and irreducible affine curves

Lemma 2.11. *If f, g and h are non-constant polynomials in $k[x, y]$ with $f = gh$ then $C_f = C_g \cup C_h$.*

Proof. If $f = gh$ where g and h are non–constant polynomials then, for all $(a, b) \in \mathbb{A}_2(k)$ we have $f(a, b) = 0$ if and only if either $g(a, b) = 0$ or $h(a, b) = 0$. Hence $(a, b) \in C_f$ if and only if

$(a, b) \in C_g \cup C_h$. Thus $C_f = C_g \cup C_h$, as required.

Example 2.12.

1. The curve with equation $x^2 - y^2 = 0$.

2. The curve with equation $(x^2 + (y-1)^2 - 1)(x^2 + (y-2)^2 - 4)(x^2 + (y-3)^2 - 9) = 0$.

Definition 2.13. Let f be an irreducible polynomial in $k[x, y]$. Then the curve C_f is called an **irreducible** affine curve.

Definition 2.14. Let f be a reducible polynomial in $k[x, y]$ with irreducible factorization $f = q_1 \cdots q_s$. Then we say that C_f is a **reducible** curve and has **irreducible components** $C_{q_1}, \dots, C_{q_s}$.

Note: If C_f has, as above, irreducible components $C_{q_1}, \dots, C_{q_s}$ then it follows from Lemma 2.11 that

$$C_f = C_{q_1} \cup \cdots \cup C_{q_s}.$$

Therefore every curve is a union of irreducible curves.

Example 2.15.

1. Lines are irreducible curves.

2. The curve with polynomial $x^2 - y^2$ has two irreducible components: the lines $x + y = 0$ and $x - y = 0$.

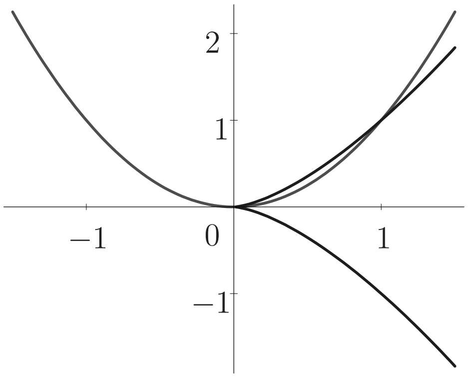


Figure 2.1: The curve with equation $x^5 - x^3y - x^2y^2 + y^3 = 0$.

3. Let $f = x^5 - x^3y - x^2y^2 + y^3$. Then f has irreducible factorization $f = gh$, where $g = x^2 - y$ and $h = x^3 - y^2$, and so C_f has irreducible components C_g and C_h. If $k = \mathbb{R}$ we can draw the curve, using Maple, and obtain a drawing: which looks as though it has two components (Figure 2.1).

4. The last example may be misleading as, in $\mathbb{A}_2(\mathbb{R})$, curves which appear to have several components may in fact be irreducible. For example the curve with equation $y^2 - x(x^2 - 1) = 0$, shown in Figure 2.2 is irreducible over $\mathbb{R}$.

5. The curve with equation $x^3 + x^2 + y^3 + y^2 = 0$ in $\mathbb{A}_2(\mathbb{R})$ behaves even worse, having an isolated point at the origin even though it is irreducible: see Figure 2.3.

6. On the other hand curves which, when drawn, look irreducible may not be. For example let $f = x^2 - 2xy + y^2$. Then $f = g^2$, where $g = x - y$. The curve C_f has 2 irreducible components both equal to C_g, which is the line $y = x$.

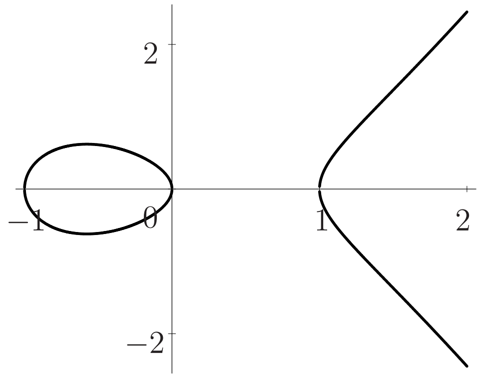


Figure 2.2: The curve with equation $y^2 - x(x^2 - 1) = 0$.

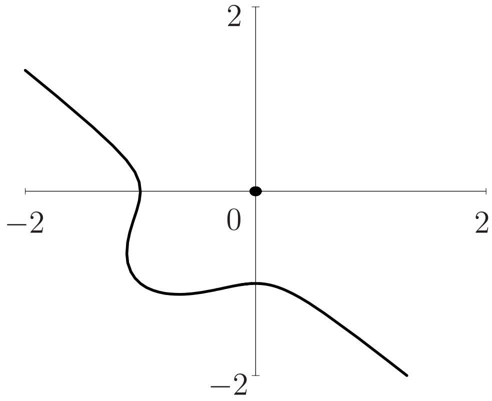


Figure 2.3: The curve with equation $x^3 + x^2 + y^3 + y^2 = 0$.

The Nullstellensatz

As we have seen above, if f and g are polynomials in $k[x, y]$ and $g|f$ then $C_g \subset C_f$. However, this raises a question. Namely, if $C_g \subset C_f$, for some polynomials f and g, does it follow that $g|f$. The answer to this question depends on g and the field k and requires a further definition. First we state the following result which gives a partial answer.

Theorem 2.16. *Let k be a field and let $f \in k[t]$ be a polynomial of degree $d \geq 0$. Then the following hold.*

1. *If $a \in k$ then $f(a) = 0$ if and only if $(t - a)|f$.*
2. *f has at most d zeros.*

Proof.

1. If $(t-a)|f$ then $f(t) = (t-a)q(t)$, for some $q \in k[t]$, so $f(a) = 0$, as required. The proof of the converse depends on the fact that we can write $f(t) = (t - a)q(t) + r(t)$, where q and r are polynomials in $k[t]$ and degree$(r) <$ degree$(t - a)$. Given this fact, which we shall not prove here, it follows that r is constant, since degree$(t-a) = 1$. Now if $f(a) = 0$ we have $0 = f(a) = r$. Hence $f(t) = (t - a)q(t)$ and $t - a|f$, as required.
2. This is proved by induction on d. It is clearly true if $d = 1$. If $d \geq 1$ and f has a zero a then we can write $f = (t - a)q$, for some $q \in k[t]$. As degree$(q) = d - 1$ the inductive hypothesis implies that q has at most $d - 1$ zeros. The result follows.

The first part of this theorem answers the analogue of question posed above for case of polynomials of one variable (under the the restriction that g is linear).

If a field k has the property that every non–constant polynomial $f \in k[t]$ has at least one zero then we say that k is **algebraically closed**. From Theorem 2.16 we may conclude that if k is algebraically closed and f is non–constant polynomial of degree d in $k[t]$ then

$$f = a_0(t - a_1) \cdots (t - a_n),$$

for some $a_i \in k$, with $a_0 \neq 0$. This follows by induction on the degree d of f. Note that, in this expression for f, the a_i's are not necessarily distinct. If we collect together all the repeated linear factors then we can write

$$f = a_0 \prod_{i=1}^{k} (t - b_i)^{r_i},$$

with $a_0 \neq 0$, $b_i \neq b_j$ when $i \neq j$ and $r_1 + \cdots + r_k = d$. In this case we say that the **multiplicity** of the zero b_i is r_i.

Example 2.17.

1. The field $\mathbb{C}$ is algebraically closed.

   This follows from a theorem of Complex Analysis. Hence any polynomial in one variable

   over $\mathbb{C}$ is a product of linear factors. For example

   $$t^4 - 2it^3 - 2it - 1 = (t+i)(t-i)^3,$$

   so has one zero $-i$, of multiplicity 1, and another zero i, of multiplicity 3.

2. The field $\mathbb{R}$ is not algebraically closed.

   For example $t^2 + 1$ has no zero in $\mathbb{R}$.

We also have the following which will be useful later.

Theorem 2.18. *Let k be an infinite field and let $f \in k[x_1, \dots x_n]$. If $f(a_1, \dots, a_n) = 0$ for all $(a_1, \dots, a_n) \in \mathbb{A}_n(k)$ then f is the zero polynomial.*

Again, this theorem answers a question similar to the one above. Note that we did not allow the zero polynomial to be the equation of a curve and so the theorem tells us that no curve contains all points of $\mathbb{A}_2(k)$, as long as k is infinite. The answer to our question is contained in the following theorem.

Theorem 2.19 (Hilbert's Nullstellensatz). *Let k be an algebraically closed field and let f and g be non–constant polynomials in $k[x_1, \dots x_n]$. Suppose that*

1. *g is irreducible and*
2. *$f(a_1, \dots, a_n) = 0$ for all $(a_1, \dots, a_n) \in \mathbb{A}_n(k)$ such that $g(a_1, \dots, a_n) = 0$.*

Then $g|f$.

We shall not prove this theorem. To see more plainly what it means for curves we state a Corollary.

Corollary 2.20. *Let g and f be polynomials in $k[x, y]$, where k is an algebraically closed field. Assume g has irreducible factorization $g = q_1 \cdots q_s$. If*

1. *$C_g \subset C_f$ and*
2. *$q_i \neq q_j$, when $i \neq j$,*

then $g|f$. In particular if g is irreducible and $C_g \subset C_f$ then $g|f$.

Proof. Fix i with $1 \leq i \leq s$. Since $q_i|g$, if $(a, b) \in \mathbb{A}_2(k)$ is such that $q_i(a, b) = 0$ we have $g(a, b) = 0$. As $C_g \subset C_f$ this means that $f(a, b) = 0$, for all $(a, b) \in \mathbb{A}_2(k)$ such that $q_i(a, b) = 0$. As q_i is irreducible it follows from the theorem that $q_i|f$. It now follows from the uniqueness of factorization, and the fact that all the q_i are distinct, that $q_1 \cdots q_s|f$. That is, $g|f$, as required.

The corollary tells us that if we stick to algebraically closed fields then we have a good correspondance between curves and polynomials without repeated irreducible factors. In particular if f and g are irreducible polynomials and $C_f = C_g$ then $g = af$, for some $a \in k$. If we drop the requirement that k is algebraically closed this theorem is far from true, as the next example shows.

Example 2.21. Let $k = \mathbb{R}$ and consider the curve C with equation $x^2 + y^2 + 1 = 0$. This curve has no points. Therefore it is contained in every other curve. Furthermore its polynomial is irreducible over $\mathbb{R}$. However this polynomial does not divide the polynomial of every other curve: in particular it does not divide any linear polynomial. This means Corollary 2.20 does not hold in $\mathbb{A}_2(\mathbb{R})$. Note also that the polynomial $g = x^2 + y^2 + 2$ defines the same (empty) curve in $\mathbb{A}_2(\mathbb{R})$, but that g is not a constant multiple of $x^2 + y^2 + 1$.

3 Intersection Number

How can curves intersect with themselves and with each other? We start with intersections of line and curve.

We'll look at the ways in which curves and lines intersect. In particular we want to understand tangents to points on a curve, because near a point we expect the curve to be approximated by its tangent(s) at that point.

Parametric form of a line

Let l be an affine line with equation $ax + by + c = 0$. Note that $(a, b) \neq (0, 0)$ as the polynomial $ax + by + c$ is of degree 1. Suppose that a point (x_0, y_0) belongs to l. Then we make the following description of the line.

The set of points of the line l is

$$\{(x_0 - bs, y_0 + as) \;:\; s \in k\}. \tag{3.1}$$

To see that this holds suppose first that we have a point (u, v) of the form (3.1). That is, for

some $s \in k$

$$(u, v) = (x_0 - bs, y_0 + as).$$

Then

$$au + bv + c = ax_0 - abs + by_0 + abs + c$$

$$= ax_0 + by_0 + c$$

$$= 0.$$

Hence $(u,v) \in l$ and $\{(x_0 - bs, y_0 + as) \,:\, s \in k\} \subseteq l$.

On the other hand suppose that $(x_1, x_2) \in l$. First assume that $a \neq 0$. In this case set

$$s = \frac{y_1 - y_0}{a}.$$

Then

$$x_0 - bs = x_0 - b\left(\frac{y_1 - y_0}{a}\right)$$

$$= \left(\frac{ax_0 - by_1 + by_0}{a}\right)$$

$$= \frac{-c - by_1}{a}$$

$$= \frac{ax_1}{a}$$

$$= x_1.$$

Also

$$y_0 + as = y_0 + a\left(\frac{y_1 - y_0}{a}\right) = y_1.$$

Therefore

$$(x_1, y_1) \in \{(x_0 - bs, y_0 + as) \,:\, s \in k\}$$

and so

$$l \subseteq \{(x_0 - bs, y_0 + as) \,:\, s \in k\}.$$

If $a = 0$ then $b \neq 0$ and a similar argument holds. The result follows.

Now suppose we're given any $a, b, x_0, y_0 \in k$ with $(a, b) \neq (0, 0)$. If we set

$$c = -(ax_0 + by_0)$$

then it follows from the above that the set (3.1) defines a line, with equation $ax + by + c = 0$, passing through the point (x_0, y_0).

We call (3.1) a **parametric form** of the line l with equation $ax + by + c = 0$ through point (x_0, y_0). If the meaning is clear we abbreviate this by saying l has parametric form $(x_0 - bs, y_0 + as)$. Note that the parametric form of the line l depends on the choice of point $(x_0, y_0) \in l$. We call the ratio $(-b : a)$ the **direction ratio** of l.

Example 3.1.

The line l with equation $2x + 5y + 1 = 0$ contains the point $(-3, 1)$ so has parametric form

$(-3-5s, 1+2s)$ and direction ratio $(-5:2)$.

The point $(7,-3)$ also lies on l so $(7-5s, -3+2s)$ is another parametric form of l.

The line with parametric form $(5-3s, 2-9s)$ has equation $-9x+3y+39=0$, direction

ratio $(-3:-9)=(1:3)$ and passes through $(5,2)$.

Intersection polynomials

Let l be an affine line passing through the point (x_0, y_0) with parametric form (x_0-bs, y_0+as), for $s \in k$. Let f be a polynomial in $k[x,y]$ and let $C=C_f$ be the curve with equation $f=0$. A point $q \in \mathbb{A}_2(k)$ lies on l and C if and only if $q=(x_0-bu, y_0+au)$, for some $u \in k$ such that

$$f(x_0-bu, y_0+au)=0. \tag{3.2}$$

This leads to the following definition.

Definition 3.2. We call the polynomial

$$\phi(s)=f(x_0-bs, y_0+as)$$

an **intersection polynomial** of l and C.

Note that ϕ depends on the choice of parametrisation of l.

From (3.2) the points of intersection of l and C correspond to those $u \in k$ such that $\phi(u)=0$. Now $\phi(u)=0$ if and only if $(s-u)|\phi(s)$. (This follows from Theorem 2.16.) Hence points of $l \cap C$ are precisely the points (x_0-bu, y_0+au) such that $(s-u)|\phi(s)$. This prompts the next definition.

Definition 3.3. Let $q=(x_0-bu, y_0+au)$ be a point of l, for some $u \in k$. The **intersection number** $I(q,f,l)$ of C and l at q is the largest integer r such that $(s-u)^r|\phi(s)$.

Example 3.4. Let $f = x^2 - y$ and let l_1 be the line with equation $x - y = 0$, let l_0 be the line with equation $y = 0$ and let l' be the line with equation $y + 1 = 0$.

Then l_1 has parametric form (s, s), l_0 has parametric form $(s, 0)$ and l' has parametric form $(s, -1)$.

The intersection polynomials of l_1, l_0 and l' are

$$\phi_1(s) = s^2 - s = s(s-1),$$

$$\phi_0(s) = s^2 \text{ and}$$

$$\phi'(s) = s^2 + 1,$$

respectively.

1. $\phi_1(s)$ has zeros $s = 0$ and $s = 1$. These correspond to points $q_0 = (0, 0)$ and $q_1 = (1, 1)$ on $C \cap l_1$. The intersection numbers of these points are $I(q_0, f, l_1) = I(q_1, f, l_1) = 1$, as zeros of ϕ_1 have multiplicity 1.

If $u \neq 1$ and $u \neq 0$ and we set $q = (u, u)$ then $I(q, f, l_1) = 0$, as $(s - u)$ does not divide ϕ_1 in this case. Note that this is a general principle: if $q \notin l \cap C_f$ then $I(q, f, l) = 0$ (as long as $l \not\subseteq C_f$).

2. $\phi_0(s) = s^2$ and has only one zero $s = 0$. This corresponds to the point $q_0 = (0, 0)$ as before but now $I(q_0, f, l_0) = 2$.

3. The zeros of $\phi'(s)$ depend on k. If $k = \mathbb{R}$ then $\phi'(s)$ has no zeros so $I(q, f, l') = 0$, for all points q on l'. If you sketch the real curve you will see that it does not meet l'.

   If $k = \mathbb{C}$ then $\phi'(s) = (s - i)(s + i)$ so there are two points of intersection, $q_+ = (i, -1)$ corresponding to $s = i$ and $q_- = (-i, -1)$ corresponding to $s = -i$. Both factors of ϕ' are linear so $I(q_+, f, l') = I(q_-, f, l') = 1$. All other points of l' lie outside C and have intersection number zero.

If $k = \mathbb{Z}_3$ then $\phi'(s)$ has no zeros as can be easily verified (as k has 3 elements $0, 1$ and 2).

Therefore all points of the line l' have intersection number zero. In $\mathbb{Z}_3$ the line l' consists of the 3 points $(0, 2)$, $(1, 2)$ and $(2, 2)$. Recalling the diagram of Example 2.4 we see that none of these points lie on C.

If $k = \mathbb{Z}_5$ then $\phi'(s)$ has zeros 2 and 3 and we can check that $\phi_1(s) = s^2+1 = (s-2)(s-3)$.

Therefore there are two points of intersection, $(2, -1) = (2, 4)$ corresponding to $s = 2$, and $(3, -1) = (3, 4)$ corresponding to $s = 3$. Both these points have intersection number 1.

Example 3.5. Let $f = x^2 - y$ and let l_m be the line with equation $y = mx$, where $m \in k$. We've covered the cases $m = 0$ and 1 in the previous example. Then l_m has parametric form (s, ms).

The intersection polynomials of l_m is

$$\phi_m(s) = s^2 - ms = s(s - m).$$

We've covered the case $m = 0$ above. When $m \neq 0$ then $\phi_m(s)$ has zeros $s = 0$ and $s = m$. These correspond to points $q_0 = (0, 0)$ and $q_m = (m, m^2)$ on $C \cap l_m$. The intersection numbers of these points are $I(q_0, f, l_m) = I(q_m, f, l_m) = 1$, as zeros of ϕ_m have multiplicity 1. Note that, if we are working over $\mathbb{R}$ or $\mathbb{C}$, as $|m|$ becomes very small the second point of intersection becomes close to $(0, 0)$. When m reaches zero the two points of intersection coalesce and we have one point of intersection with intersection number 2.

Suppose $(x_0, y_0) \in l$ and that l has parametric form $(x_0 - bs, y_0 + as)$. If $l \subseteq C_f$ then $\phi(s) = 0$, for all $s \in k$. It follows from Theorem 2.18, that ϕ is the zero polynomial (as long as k is an infinite field). In this case $(s - u)^r | \phi(s)$, for all $r \geq 0$. Hence the intersection number $I(q, f, l) = \infty$, for all $q \in \mathbb{A}_2(k)$.

Theorem 3.6. *If C is an affine curve, with polynomial f of degree $d \geq 0$, and l is a line with $l \not\subseteq C$ then $l \cap C$ has at most d points, counted with multiplicity. That is*

$$\sum_{p \in l \cap C} I(p, f, l) \leq d.$$

The definition of intersection number depends on an intersection polynomial for l and C. The intersection polynomial depends in turn on the parametric form for the line l. The parametric form for l is determined by the choice of the point (x_0, y_0) on l. Note that the line with parametric form $(x_0 - bs, y_0 + as)$ has equation $ax + by + c = 0$. Therefore it also has equation $\lambda ax + \lambda by + \lambda c = 0$, where λ is any non–zero element of k. It follows that another parametric form for l is $(x_0 - \lambda b, y_0 + \lambda a)$: that is we may replace (a, b) with $(\lambda a, \lambda b)$. We now show that the intersection number is the same no matter which parametric form we choose for l. The remainder of this section is background reading and not required for assessment.

Let $p = (x_0, y_0)$ and define

$$L_p(s) = (x_0 - bs, y_0 + as).$$

First we investigate the result of changing (x_0, y_0). The original parametric form for l is $L_p(s)$. Suppose now that $p' = (x_1, y_1)$ is a different point of l. Then l also has parametric form

$$L_{p'}(t) = (x_1 - bt, y_1 + at), t \in k.$$

As $p' = (x_1, y_1)$ is a point of l we have $v \in k$ such that

$$p' = (x_1, y_1) = (x_0 - bv, y_0 + av). \tag{3.3}$$

There is also an intersection polynomial ϕ' corresponding to the new parametric form for l, namely

$$\phi'(t) = f(x_1 - bt, y_1 + at).$$

Now suppose that q is some point of l, say $q = L_p(u)$, for some $u \in k$, and that using the original intersection polynomial ϕ we have $I(q, f, l) = r$. That is $(s-u)^r|\phi(s)$ but $(s-u)^{r+1} \nmid \phi(s)$. Then there exists a polynomial q such that $\phi(s) = (s-u)^r q(s)$ and $(s-u) \nmid q(s)$. Now

$$\begin{aligned}(s-u)^r q(s) = \phi(s) &= f(x_0 - bs, y_0 + as)\\ &= f(x_0 - bv + bv - bs, y_0 + av - av + as)\\ &= f(x_1 + bv - bs, y_1 - av + as) \qquad \text{using (3.3)}\\ &= f(x_1 - b(s-v), y_1 + a(s-v)).\end{aligned}$$

Setting $t = s - v$ and substituting in the above we obtain

$$\begin{aligned}(t-(u-v))^r q(t+v) &= f(x_1 - bt, y_1 + at)\\ &= \phi'(t).\end{aligned}$$

That is, if $(s-u)^r|\phi(s)$ then $(t-(u-v))^r|\phi'(t)$. Appealing to the symmetry of the situation the converse of the last statement also holds, so in fact $(s-u)^r|\phi(s)$ if and only if $(t-(u-v))^r|\phi'(t)$. Therefore the intersection number of $q = L_p(u)$ calculated using ϕ is equal to the intersection number of $L_{p'}(u-v)$ calculated using ϕ'. Now the point

$$\begin{aligned}L_{p'}(u-v) &= (x_1 - b(u-v), y_1 + a(u-v))\\ &= (x_0 - bu, y_0 + au) \qquad \text{using (3.3)}\\ &= L_p(u) = q.\end{aligned}$$

Thus q is the point of l corresponding to the zero $t = (u-v)$ of $\phi'(t)$ and from the above we obtain the same intersection number whichever parametric form we use.

Next we consider the effect of changing a and b. We can replace the parametric form $L_p(s) = (x_0 - bs, y_0 + as)$ with the parametric form $L'_p(t) = (x_0 - b's, y_0 + a's)$ if and only if $(-b : a) = (-b' : a')$. Suppose then that $d \in k$, $d \neq 0$, $a = da'$, $b = db'$ and $L'_p(t)$ is as above. The intersection polynomial corresponding to the parametric form $L'_p(t)$ is

$$\phi'(t) = f(x_0 - b's, y_0 + a's).$$

Now let $q = L_p(u)$ be a point of l. Then

$$\begin{aligned}q = L_p(u) &= (x_0 - bu, y_0 + au)\\ &= (x_0 - db'u, y_0 + da'u)\\ &= L'_p(du).\end{aligned}$$

Furthermore if $(s-u)^r|\phi(s)$ then there is a polynomial $q(s)$ such that

$$\begin{aligned}(s-u)^r q(s) = \phi(s) &= f(x_0 - bs, y_0 + as)\\ &= f(x_0 - db's, y_0 + da's)\\ &= \phi'(ds).\end{aligned}$$

Setting $t = ds$ and substituting in the above we obtain

$$((t/d)-u)^r q(t/d) = \phi'(t).$$

Now, since $d \in k$, $q(t/d)$ is a polynomial of the same degree as q in $k[t]$ and

$$((t/d)-u)^r = \frac{1}{d^r}(t-du)^r.$$

It follows, appealing to symmetry again, that $(s-u)^r|\phi(s)$ if and only if $(t-du)^r|\phi'(t)$. Hence the intersection number of q is the same whether we use $\phi(s)$ or $\phi'(t)$ to compute it. We conclude therefore that intersection number is independent of choice of parametric form for l.

4 Singularities, Multiplicity and Tangents

Example 4.1. The curve $y - x^2 = 0$.

Example 4.2. The curve $y^2 - x^3 - x^2 = 0$.

In order to make these ideas precise we first need to look again at polynomial algebra.

Polynomials and Taylor's theorem

First of all we define derivatives of polynomials, of one variable, algebraically (the definition involves no limits).

Definition 4.3. Let $f = a_0 + a_1x + \cdots a_nx^n$ be a polynomial in $k[x]$. Then the **derivative** of f with respect to x is

$$f' = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

We can prove all the usual rules for differentiation using this definition and we use the usual notation for higher derivatives. In particular we have the Taylor expansion for polynomials of one variable given by the next theorem. In this theorem and in the remainder of the section on multiplicities we shall assume that if f is a polynomial of degree d in $k[x_1, \ldots, x_n]$ then k is a field containing $\mathbb{Z}$ or $\mathbb{Z}_p$, where $p > d$. Otherwise k would be a field containing $\mathbb{Z}_p$ with $p \leq d$ and then we should not be able to make statements involving $1/d!$.

Theorem 4.4. *Let f be a polynomial of degree d in $k[x]$ and let u be an element of k. Then the* **Taylor expansion** *of f is*

$$f(x) = f(u) + (x-u)f'(u) + \frac{(x-u)^2}{2!}f''(u) + \cdots + \frac{(x-u)^d}{d!}f^{(d)}(u).$$

Proof. The polynomial $f(x+u)$ has degree d and we can write $f(x+u) = a_0 + a_1x + \cdots a_nx^d$, with $a_i \in k$. The rth derivative of $f(x+u)$ with respect to x is then

$$f^{(r)}(x+u) = r!a_r + (r+1)!a_{r+1}x + \cdots + \frac{d!}{(d-r)!}a_dx^{d-r}.$$

Setting $x = 0$ in the above expression we obtain $f^{(r)}(u) = r!a_r$. Therefore

$$f(x+u) = f(u) + xf'(u) + \frac{x^2}{2!}f''(u) + \cdots + \frac{x^d}{d!}f^{(d)}(u).$$

Substitution of $x - u$ for x above gives the required result.

Partial derivatives of polynomials of several variables are defined in the obvious way and we use the notation

$$\frac{\partial f}{\partial x_i} \text{ or } f_{x_i} \text{ or } f_i$$

for the partial derivative of f with respect to x_i. Thus if $f(x,y) = x^8y^3 + 3x^2y^6 + 17x + y^{10} + 3$ we have

$$\frac{\partial f}{\partial x}(x,y) = 8x^7y^3 + 6xy^6 + 17$$

and
$$\frac{\partial f}{\partial y}(x,y) = 3x^8y^2 + 18x^2y^5 + 10y^9.$$
We can now state the chain rule.

Theorem 4.5. *Let $f(x_1,\ldots,x_n)$ be an element of $k[x_1,\ldots,x_n]$ and let $g_1(s)$, ... ,$g_n(s)$ be elements of $k[s]$. Then, differentiating $f(g_1(s),\ldots,g_n(s))$ with respect to s, we obtain*
$$f'(g_1(s),\ldots,g_n(s)) = \sum_{i=1}^{n} f_{x_i}(g_1(s),\ldots,g_n(s))g_i'(s).$$

The chain rule is used in the proof of Taylor's theorem for polynomials of several variables, which is as follows.

Theorem 4.6. *Let $f \in k[x,y]$ be a polynomial of degree n and let $a, b, x_0, y_0 \in k$. Then*
$$\begin{aligned} f(sa+x_0, sb+y_0) &= f(x_0,y_0) \\ &\quad + s(a\frac{\partial f}{\partial x}(x_0,y_0) + b\frac{\partial f}{\partial y}(x_0,y_0)) \\ &\quad \vdots \\ &\quad + \frac{s^n}{n!}\sum_{j=0}^{n}\left(\begin{array}{c} n \\ j \end{array}\right) a^{n-j}b^j \frac{\partial^n f}{\partial x^{n-j}\partial y^j}(x_0,y_0). \end{aligned}$$

Proof.

Let $\phi(s) = f(sa+x_0, sb+y_0)$. Using Taylor's theorem for polynomials of one variable (Theorem 4.4) we have
$$\phi(s) = \phi(0) + s\phi'(0) + \frac{s^2}{2!}\phi''(0) + \cdots + \frac{s^n}{n!}\phi^{(n)}(0).$$
Using the chain rule
$$\begin{aligned} \phi(0) &= f(x_0,y_0) \\ \phi'(0) &= a\frac{\partial f}{\partial x}(x_0,y_0) + b\frac{\partial f}{\partial y}(x_0,y_0) \\ &\vdots \\ \phi^{(k)}(0) &= \sum_{j=0}^{k}\left(\begin{array}{c} k \\ j \end{array}\right) a^{k-j}b^j \frac{\partial^k f}{\partial x^{k-j}\partial y^j}(x_0,y_0). \end{aligned}$$

The result follows.

Corollary 4.7. *Let $f \in k[x,y]$ be a polynomial of degree n and let $x_0, y_0 \in k$. Then*

$$\begin{aligned} f(x,y) &= f(x_0,y_0) \\ &\quad + \left((x-x_0)\frac{\partial f}{\partial x}(x_0,y_0) + (y-y_0)\frac{\partial f}{\partial y}(x_0,y_0)\right) \\ &\quad \vdots \\ &\quad + \frac{1}{n!}\sum_{j=0}^{n}\binom{n}{j}(x-x_0)^{n-j}(y-y_0)^j\frac{\partial^n f}{\partial x^{n-j}\partial y^j}(x_0,y_0). \end{aligned}$$

Proof.

Set $s = 1$, $a = x - x_0$ and $b = y - y_0$ in the Theorem and this follows immediately.

Next we prove a useful result about homogeneous polynomials in 2 variables (an analogue of Theorem 2.16). We say a ratio $(a : b)$ is **non–zero** if $(a,b) \neq (0,0)$.

Lemma 4.8. *Let $f(x,y)$ be a homogenous polynomial of degree $d \geq 0$ in $k[x,y]$. Then there are at most d non–zero ratios $(a : b)$ such that $f(a,b) = 0$. If $k = \mathbb{C}$ then*

$$f(x,y) = a_0\prod_{i=1}^{d}(b_i x - a_i y),$$

for some $a_i, b_i \in \mathbb{C}$.

Proof. Since the degree of f is non–zero we may write

$$f = \sum_{j=0}^{d} c_j x^j y^{d-j},$$

where $c_j \neq 0$, for some j. Now, using the result of one of Exercises 2, given (a,b) we have $f(a,b) = 0$ if and only if $f(ta,tb) = 0$, for all $t \neq 0$. Hence (a,b) is a zero of f if and only if (c,d) is a zero of f, for all (c,d) with $(c : d) = (a : b)$. Hence we need only prove the result for one representative (a,b) of each non–zero ratio $(a : b)$. Note that any non–zero ratio $(a : 0)$ is equal to $(1 : 0)$ and that any ratio $(a : b)$ with $b \neq 0$ is equal to $(t : 1)$, with $t = a/b$.

Firstly suppose that $(1,0)$ is not a zero of f. Then $c_d \neq 0$ and any ratio which is a zero of f has a representative of the form $(t : 1)$. Thus

$$f(t,1) = \sum_{j=0}^{d} c_j t^j,$$

is a polynomial of degree d. From Theorem 2.16, there are at most d zeros of $f(t,1)$ and this proves the first statement of the lemma. If $k = \mathbb{C}$ then

$$f(t,1) = a_0\prod_{i=1}^{d}(t - a_i),$$

for some $a_i \in \mathbb{C}$. In this case let
$$t = \frac{x}{y}.$$
Then
$$f(t, 1) = a_0 \prod_{i=1}^{d} \left(\frac{x}{y} - a_i \right)$$
and so
$$f(x, y) = y^d f(t, 1) = a_0 \prod_{i=1}^{d} (x - a_i y).$$
Now suppose that $(1, 0)$ is a zero of f. Then $c_d = 0$ so there is $e \geq 1$ such that
$$c_d = c_{d-1} = \cdots = c_{d-e+1} = 0 \text{ and } c_{d-e} \neq 0.$$
Thus
$$f = \sum_{j=0}^{d-e} c_j x^j y^{d-j} = y^e \sum_{j=0}^{d-e} c_j x^j y^{d-e-j}.$$
Since $c_{d-e} \neq 0$ the result now follows from the previous case.

Singular points

Definition 4.9. Let C be an affine curve with polynomial f. A point (x_0, y_0) of C is called **singular** if
$$f_x(x_0, y_0) = f_y(x_0, y_0) = 0.$$
Otherwise (x_0, y_0) is called **non–singular**. If all its points are non–singular then the curve C is called **non–singular**.

Example 4.10. Find all singular points of the curve with equation $f(x, y) = x^3 + y^3 - 3xy$.

Example 4.11. Find all singular points of the curve with equation

$$f(x, y) = x^3 + y^3 - 2x^2 + y^2 + x.$$

(The real curve with this equation is shown in Figure 4.4.) We have

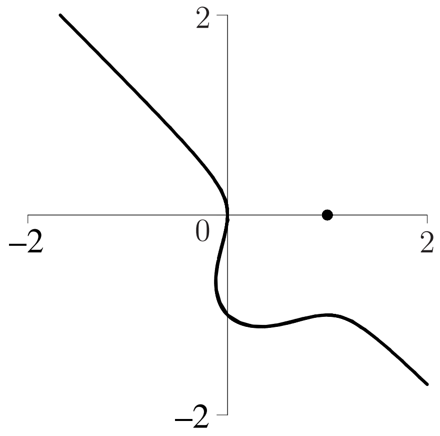


Figure 4.4: The curve with equation $x^3 + y^3 - 2x^2 + y^2 + x = 0$.

$$f_x = 3x^2 - 4x + 1 \text{ and } f_y = 3y^2 + 2y.$$

Hence $f_y = 0$ if and only if $y = 0$ or $y = -2/3$.

Case 1, $y = 0$**:** In this case $f(x, y) = x^3 - 2x^2 + x = x(x-1)^2 = 0$ if and only if $x = 0$ or $x = 1$.

If $x = 0$ then $y = x = 0$ and so $f_x = 1 \neq 0$. Hence $(0, 0)$ is not

a singular point.

If $x = 1$ then $f_x = 0$, so we have $f(1, 0) = f_x(1, 0) = f_y(1, 0) = 0$. Hence $(1, 0)$ is a singularity.

Case 2, $y = -2/3$**:** In this case $f_x = 0$ if and only if $x = 1$ or $1/3$. Also

$$f(x, -2/3) = x^3 - 2x^2 + x - (2/3)^3 + (2/3)^2.$$

As $f(1, -2/3) \neq 0$ and $f(1/3, -2/3) \neq 0$ there are no singular points with y-coordinate $-2/3$.

The curve has one singular point $(1, 0)$.

Multiplicity

At a singular point the first partial derivatives of the polynomial vanish. What about second partial derivatives? We single out the degree of the first non–vanishing partial derivative with the following definition.

Definition 4.12.
Let C be a curve with equation $f = 0$. A point $p = (x_0, y_0)$ of C has **multiplicity** r if

1.
$$f(x_0, y_0) = 0,$$
$$\frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0,$$
$$\vdots$$
$$\frac{\partial^{r-1} f}{\partial x^{r-1}}(x_0, y_0) = \frac{\partial^{r-1} f}{\partial x^{r-2}\partial y}(x_0, y_0) = \ldots = \frac{\partial^{r-1} f}{\partial x \partial y^{r-2}}(x_0, y_0) = \frac{\partial^{r-1} f}{\partial y^{r-1}}(x_0, y_0) = 0$$
and

2.
$$\frac{\partial^r f}{\partial x^{r-j}\partial y^j}(x_0, y_0) \neq 0, \text{ for some } j \text{ with } 0 \leq j \leq r.$$

It follows immediately from this definition that a point of C is singular if and only if it has multiplicity greater than 1.

Definition 4.13.

1. Points of multiplicity 1 are called **simple** points.
2. Points of multiplicity 2 are called **double** points.
3. Points of multiplicity 3 are called **triple** points.
4. Points of multiplicity r are called r**–tuple** points.

Example 4.14. We shall find the multiplicity of each singular point of the curve with equation

$$f(x, y) = x^3 + y^3 - 3xy.$$

From Example 4.10 we know that the curve has one singular point $(0, 0)$.

Example 4.15. We shall find the multiplicity of each singular point of the curve with equation

$$f(x, y) = x^3 + y^3 - 2x^2 + y^2 + x.$$

From Example 4.11 we know that the curve has one singular point $(1, 0)$. We have

$$f_{xx} = 6x - 4,\ f_{xy} = 0 \ \text{ and } \ f_{yy} = 6y + 2.$$

As $f_{xx}(1, 0) = 2 \neq 0$ it follows that $(1, 0)$ is a double point.

Tangents

Now let $p = (x_0, y_0)$ be a point on the curve C with equation $f = 0$. Suppose f has degree d and, for $t = 0, \ldots, d$, define the polynomial F_t in two variables α and β as follows.

$$F_0(\alpha, \beta) = f(x_0, y_0) \quad \text{and}$$

$$F_t(\alpha, \beta) = \sum_{j=0}^{t} \binom{t}{j} \alpha^{t-j} \beta^j \frac{\partial^t f}{\partial x^{t-j} \partial y^j}(x_0, y_0), \quad \text{for } t > 0. \tag{4.1}$$

Then F_t is either zero or homogeneous of degree t. A line l through p with direction ratio $(a : b)$ has parametric form $(x_0 + as, y_0 + bs)$.

Definition 4.16. Let $p = (x_0, y_0)$ be a point of multiplicity r on C. The line l with parametric form $(x_0 + as, y_0 + bs)$ is called a **tangent** to C at p if

$$F_r(a, b) = 0.$$

As F_r is non–zero it is homogeneous of degree r and it follows, from Lemma 4.8, that there are at most r tangents at a point of multiplicity r.

Example 4.17. Find all tangents to the complex curve with equation

$$f(x, y) = x^3 + y^3 - 3xy$$

at the points $(0, 0)$ and $(3/2, 3/2)$.

From Example 4.14 we know that the curve has one singular point $(0, 0)$ of multiplicity 2. Therefore $(3/2, 3/2)$ is a simple point.

Example 4.18. Find all tangents to the complex curve with equation

$$f(x,y) = x^3 + y^3 - 2x^2 + y^2 + x$$

at singular points.

From Example 4.15 the curve has one singularity: the double point $(1,0)$. As $(1,0)$ is a point of multiplicity 2 the tangents must have direction ratios $(a : b)$ which are zeroes of

$$x^2 f_{xx}(1,0) + 2xy f_{xy}(1,0) + y^2 f_{yy}(1,0) = 2x^2 + 2y^2.$$

We have $2x^2 + 2y^2 = 0$ if and only if $(x+iy)(x-iy) = 0$ so $(a : b) = (i : 1)$ or $(i : -1)$. The tangents at $(1,0)$ are therefore the lines $l_1 = \{(is+1, s) | s \in k\}$ and $l_2 = \{(is+1, -s) | s \in k\}$.

Tangents and Intersection numbers

As before let $p = (x_0, y_0)$ be a point on the curve C with equation $f = 0$. A line l through p with direction ratio $(a : b)$ has parametric form $(x_0 + as, y_0 + bs)$. Define

$$\phi_{(a,b)}(s) = f(x_0 + as, y_0 + bs).$$

Then $I(p, f, l)$ is the highest power of s dividing $\phi_{(a,b)}(s)$. That is

$$I(p,f,l) = m \quad \text{if and only if} \quad s^m | \phi_{(a,b)}(s) \quad \text{and} \quad s^{m+1} \nmid \phi_{(a,b)}(s).$$

From Theorem 4.6,

$$\phi_{(a,b)}(s) = \sum_{t=0}^{d} \frac{s^t}{t!} F_t(a,b),$$

where $F_t(\alpha, \beta)$ is defined in (4.1). If p is a point of multiplicity r then we have

$$F_0(\alpha,\beta) = \cdots = F_{r-1}(\alpha,\beta) = 0$$

so that in fact

$$\phi_{(a,b)}(s) = \sum_{t=r}^{d} \frac{s^t}{t!} F_t(a,b).$$

Therefore, for all ratios $(a:b)$,

$$s^r | \phi_{(a,b)}(s).$$

That is, for all lines l through a point p of multiplicity r,

$$I(p,f,l) \geq r.$$

Furthermore, for a given line l with direction ration (a,b),

$$\begin{aligned} I(p,f,l) > r \quad &\iff \quad s^{r+1} | \phi_{(a,b)}(s) \\ &\iff \quad F_r(a,b) = 0. \end{aligned}$$

From Lemma 4.8, there are at most r ratios $(a:b)$ such that $F_r(a,b) = 0$. There are therefore at most r lines through the point p such that $I(p,f,l) > r$: each such line has direction ratio $(a:b)$ where $F_r(a,b) = 0$. We have proved the following Theorem.

Theorem 4.19. *Let p be and r–tuple point of a curve C. Then a line l is a tangent to C at p if and only if $I(p,f,l) > r$.*

Example 4.20. As we saw in Example 4.17, the tangents to the curve curve with equation

$$f(x,y) = x^3 + y^3 - 3xy$$

at the point $(0,0)$ are the lines $x = 0$ and $y = 0$ with parametric forms $(0,s)$ and $(s,0)$, respectively.

Multiplicity and tangents at the origin

The multiplicity of the point $(0,0)$ is particularly easy to compute. If f is a polynomial then the terms of f of least degree are called **lowest order terms** of f. Thus the polynomial $x^7y^4 + 3x^6y^2 + 17x^2y^{16} + 2xy^7$ has lowest order terms $3x^6y^2$ and $2xy^7$. We can write any polynomial f of degree d as

$$f = G_0 + G_1 + \cdots + G_d,$$

where G_k is either zero or homogenous of degree k and G_d is non–zero. In this case the sum of lowest order terms of f is G_s, where G_r is the zero polynomial for $k = 0, \dots, s-1$ and G_s is not the zero polynomial.

Corollary 4.21. *Let C be a curve with equation $f = 0$ containing the point $(0,0)$. Then $(0,0)$ has multiplicity r on C if and only if the lowest order terms of f have degree r. In this case let G_r be the sum of lowest order terms of f. Then a line l through $(0,0)$ is tangent to C at $(0,0)$ if and only if l has parametric form (as, bs) where $G_r(a,b) = 0$.*

Proof. Write $f = G_0 + G_1 + \cdots + G_d$, where G_t is either zero or homogenous of degree t and G_d is non–zero. From Corollary 4.7, with $(x_0, y_0) = (0,0)$, we see that

$$G_t(x,y) = \frac{1}{t!}F_t(x,y),$$

where F_t is defined in (4.1). Hence $(0,0)$ has multiplicity r if and only if

$$G_0 = \cdots = G_{r-1} = 0 \quad \text{and} \quad G_r \neq 0.$$

This proves the first statement. The second follows similarly.

Example 4.22. Let C be the curve with polynomial $f = (x^2 + y^2)^2 + 3x^2y - y^3$. The point $(0,0)$ belongs to C and the sum of lowest order terms of f is $3x^2y - y^3$. Therefore $(0,0)$ has multiplicity 3. The line with parametric form (as, bs) is tangent to C at $(0,0)$ if and only if (a,b) is a zero of $3x^2y - y^3$, that is if and only if $b = 0$ or $3a^2 - b^2 = 0$. When $b = 0$ we have a tangent l with parametric form $(s, 0)$. When $3a^2 - b^2 = 0$ we may assume $a = 1$ and so $b = \pm\sqrt{3}$. In this case we obtain two tangents l' and l'' with parametric forms $(s, s\sqrt{3})$ and $(s, -s\sqrt{3})$, respectively.

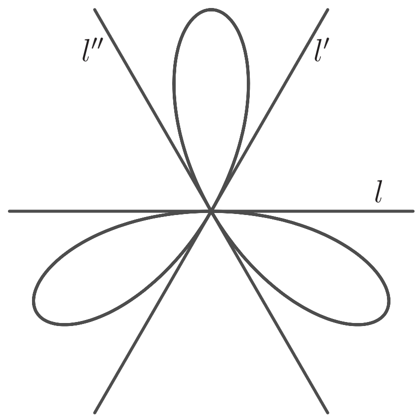


Figure 4.5: The real curve $(x^2 + y^2)^2 + 3x^2y - y^3 = 0$ and its tangents at $(0,0)$

5 Projective spaces and projective curves

We shall add new points "at infinity" to the affine plane and discover that by doing so we obtain a plane in which the geometry is simplified but nonetheless gives insight into the behaviour of affine curves.

Ratios

A **ratio**, over k, is an n–tuple $(a_1 : \ldots : a_n)$ of elements of k. Two ratios $(a_1 : \ldots : a_n)$ and $(b_1 : \ldots : b_n)$ are defined to be equal if there exists a non–zero element $\lambda \in k$ with

$$a_1 = \lambda b_1, a_2 = \lambda b_2, \ldots, a_n = \lambda b_n.$$

Lines in the affine plane

We have used Cartesian coordinates to describe points of $\mathbb{A}_2(k)$: a point is represented by an ordered pair (u, v) of elements of k. Lines are sets of points satisfying equations of the form

$$ax + by + c = 0, \quad \text{where} \quad (a, b) \neq (0, 0).$$

Two points of $\mathbb{A}_2(k)$ lie on a unique line. In fact (x_0, y_0) and (x_1, y_1) lie on the line with parametric form

$$((x_1 - x_0)s + x_0, (y_1 - y_0)s + y_0).$$

However it is not always the case that two lines meet at a unique point: they may be parallel. In fact two distinct lines are parallel if and only if their direction ratios are equal. (The direction ratio of the line above is $(-b : a)$.)

To see this suppose we have two lines l and L with equations

$$ax + by + c = 0 \text{ and} \tag{5.1}$$

$$Ax + By + C = 0, \tag{5.2}$$

respectively. Assume that $a \neq 0$. If $A = 0$ then $(-B : A) \neq (-b : a)$ and L has equation

$$y = -C/B.$$

In this case we obtain a unique point of intersection by substitution of this value of y in the equation of l.

We may assume then that $a \neq 0$ and $A \neq 0$. Note that in this case

$$(-b : a) = (-B : A) \iff b = \lambda B \quad \text{and} \quad a = \lambda A,$$

for some non–zero $\lambda \in k$ and the latter holds if and only if

$$b = \frac{a}{A}B \iff Ab - aB = 0,$$

since $A \neq 0$. Multiplying equation (5.1) by A and equation (5.2) by a we find that the y coordinate of any point of intersection must satisfy

$$(Ab - aB)y + (Ac - aC) = 0.$$

If $Ab - aB \neq 0$ then $(-b : a) \neq (-B : A)$ and we obtain a unique point of intersection. If, on the other hand $Ab - aB = 0$, so $(-b : a) = (-B : A)$ then there are two cases to consider. First suppose that $Ac - aC \neq 0$. Then there can be no solution, so no point of intersection and the lines are parallel. Now suppose that $Ac - aC = 0$. Since both a and A are non–zero we have

$$c = \frac{a}{A}C.$$

From the above it's now clear that both l and L are the same line.

Homogeneous coordinates for $\mathbb{A}_2(k)$

To see how to extend the affine plane to a plane in which any two lines do meet at a unique point we first replace Cartesian coordinates with a new coordinate system.

Definition 5.1. The point (u, v) of $\mathbb{A}_2(k)$ has **homogeneous coordinates**

$$(U : V : W), \quad \text{where} \quad W \neq 0 \quad \text{and} \quad u = \frac{U}{W}, v = \frac{V}{W}.$$

Example 5.2. The coordinates $(1 + i : 2 + i : 3)$ and $(3 + i : 5 : 6 - 3i)$ in $\mathbb{A}_2(\mathbb{C})$.

Extension to points with third coordinate zero

We now extend the plane by allowing points with homogeneous coordinates $(U : V : W)$, where $W = 0$. We exclude only the ratio $(0 : 0 : 0)$. Thus $(1 : 2 : 0)$ and $(0 : 5 : 0)$ are points of the extended plane. The definition for spaces of dimension n other than 3 is analogous.

Definition 5.3. Projective n–space over k, denoted $\mathbb{P}_n(k)$, is the set of non–zero ratios

$$(a_1 : \ldots : a_{n+1}), \quad \text{where} \quad a_i \in k.$$

Elements of $\mathbb{P}_n(k)$ are called **points** of $\mathbb{P}_n(k)$.

Thus the extended plane $\mathbb{P}_2(k)$ consists of

1. points $(u : v : w) \in \mathbb{A}_2(k)$, that is those with $w \neq 0$, and
2. new points $(u : v : 0)$, where $(u, v) \neq (0, 0)$.

In the projective plane, as in the affine plane $(u : v : w) = (\lambda u : \lambda v : \lambda w)$, for all non–zero $\lambda \in k$. Note that, given a fixed non–zero triple (u, v, w) the set

$$\{(\lambda u, \lambda v, \lambda w) : \lambda \in k\} = \langle (u, v, w) \rangle$$

is a one–dimensional subspace of the vector space k^3. Therefore there is a one to one correspondence between points of $\mathbb{P}_2(k)$ and one–dimensional vector subspaces of k^3:

$$(u : v : w) \text{ corresponds to } \langle (u, v, w) \rangle .$$

A similar statement holds for points of $\mathbb{P}_n(k)$, for any $n \geq 1$.

Lines in the projective plane

Suppose that l is a line in the affine plane with equation $ax + by + c = 0$. A point $(u : v : w)$ of $\mathbb{A}_2(k)$ belongs to l if and only if

$$a\left(\frac{u}{w}\right) + b\left(\frac{v}{w}\right) + c = 0$$

that is if and only if

$$au + bv + cw = 0.$$

Therefore $(u : v : w)$ belongs to l if and only if $(x, y, z) = (u, v, w)$ is a solution to the equation

$$ax + by + cz = 0.$$

Note that

$$au + bv + cw = 0 \iff \lambda au + \lambda bv + \lambda cw = 0,$$

so it makes sense to speak of $(u : v : w)$ as a solution of $ax + by + cz = 0$.

Definition 5.4. Suppose $(A, B, C) \neq (0, 0, 0)$. The **projective line** with equation

$$Ax + By + Cz = 0$$

is the set of points

$$(u : v : w) \in \mathbb{P}_2(k) \quad \text{such that} \quad Au + Bv + Cw = 0.$$

As in the affine plane, two points determine a line.

Lemma 5.5. *Two distinct points p and q of $\mathbb{P}_2(k)$ lie on a unique line.*

Proof. The points $(a : b : c)$ and $(u : v : w)$ lie on the line with equation

$$(bw - cv)x + (cu - aw)y + (av - bu)z = 0.$$

That is, with equation

$$\begin{vmatrix} x & y & z \\ a & b & c \\ u & v & w \end{vmatrix} = 0. \tag{5.3}$$

The uniqueness part of the proof is left to the exercises.

In contrast to the affine plane, here, in the projective plane two lines determine a unique point: their point of intersection.

Lemma 5.6. *Distinct lines in $\mathbb{P}_2(k)$ meet at a unique point.*

Proof. Suppose we have two lines with equations

$$Ax + By + Cz = 0 \quad \text{and} \quad A'x + B'y + C'z = 0.$$

To find their point of intersection, if it exists, we solve these equations simultaneously. As we have two equations in three unknowns there will be at least one solution. As the two lines are distinct it follows that

$$(A : B : C) \neq (A' : B' : C').$$

Therefore there is exactly one solution. For details see the exercises.

$$\boxed{\text{There are no parallel lines in } \mathbb{P}_2(k)}$$

Parametric form of a projective line

Let l be a line in $\mathbb{P}_2(k)$ through the points $(a : b : c)$ and $(u : v : w)$. Then l has equation given by (5.3) above. A point $(x_0 : y_0 : z_0)$ is a solution to this equation if and only if the vector $(x_0, y_0, z_0) \in k^3$ is a linear combination of the vectors (a, b, c) and (u, v, w): otherwise the matrix in (5.3) will have non–zero determinant. That is, $(x_0 : y_0 : z_0)$ is a point of l if and only if

$$(x_0, y_0, z_0) = (as + ut, bs + vt, cs + wt), \quad \text{for some} \quad s, t \in k.$$

Therefore

$$\begin{aligned} l &= \{(x : y : z) \in \mathbb{P}_2(k) | (x, y, z) = (as + ut, bs + vt, cs + wt), \text{ with } s, t \in k\} \\ &= \{(as + ut : bs + vt : cs + wt) \in \mathbb{P}_2(k) | s, t \in k\}. \end{aligned} \tag{5.4}$$

The expression (5.4) is called the **parametric form** of the line l. As in the affine case we'll say that l has parametric form

$$(as + ut : bs + vt : cs + wt), \quad \text{for} \quad s, t \in k$$

when the meaning is clear.

Projective curves

Definition 5.7. A linear combination of monomials of degree $d \geq 0$, with at least one non–zero coefficient, is called a **homogeneous polynomial of degree** d.

Theorem 5.8. *A polynomial* $f \in k[x_1, \ldots, x_n]$ *is homogeneous of degree* d *if and only if* $f(tx_1, \ldots, tx_n) = t^d f(x_1, \ldots, x_n)$*, for all* $t \in k$*.*

Proof. See solutions to exercises 2.

From the above it follows that if $f(x, y, z)$ is homogeneous of degree d then $f(a, b, c) = 0$ if and only if $f(u, v, w) = 0$, for all $(u, v, w) \in k^3$ such that $(a : b : c) = (u : v : w)$.

Definition 5.9. Let f be a homogeneous polynomial of degree $d > 0$ in $k[x, y, z]$. The set

$$C_f = \{(a : b : c) \in \mathbb{P}_2(k) : f(a, b, c) = 0\}$$

is called a **projective curve** of **degree** d in $\mathbb{P}_2(k)$.

Theorem 5.10. *If* f *is homogeneous and* $g|f$ *then* g *is homogeneous.*

Proof. See solutions to exercises 2.

Let f be an irreducible homogeneous polynomial in $k[x, y, z]$. Then the curve C_f is called an **irreducible** projective curve. (Compare this with definition 2.13.) If C_f is a projective curve and f has irreducible factorisation $f = q_1 \cdots q_n$ then

$$C_f = C_{q_1} \cup \cdots \cup C_{q_n}$$

and the projective curves C_{q_i} are called the **irreducible components** of C_f.

Note that a homogeneous polynomial of degree 1 defines what we called a line in definition 5.4. That is, as in the affine plane, lines are curves of degree 1.

Dehomogenization

Let F be a homogeneous polynomial of degree d in $k[x, y, z]$. The **dehomogenization** of F, with respect to $z = 1$, is the polynomial $f(x, y) = F(x, y, 1)$. Note that f is a polynomial of degree at most d in $k[x, y]$. Moreover if $F \neq az^d$ then f is non–constant and if $z \nmid F$ then f has degree d.

If the dehomogenization f of the polynomial F is non–constant then we call the affine curve C_f the **dehomogenization** of C_F, with respect to $z = 1$.

Example 5.11.

1. The projective curve with equation $y^3 - x^2z = 0$ has dehomogenization the affine curve with equation $y^3 - x^2 = 0$. We can view the real projective curve as a set of lines through $(0, 0)$ in $\mathbb{R}^3$. We obtain the real affine curve by intersecting the projective curve with the plane $z = 1$: see Figure 5.6.

2. The projective curve with polynomial $x^3 + y^3 - 3xyz$ has dehomogenization the affine curve with polynomial $x^3 + y^3 - 3xy$. The real curves with these equations are shown in Figure 5.7. In the left hand drawing the z axis points straight up out of the page, whilst the x axis points to the left and the y axis points upwards in the plane of the page. The right hand drawing is first rotated so that the z axis points out to the left and then its tilted towards you.

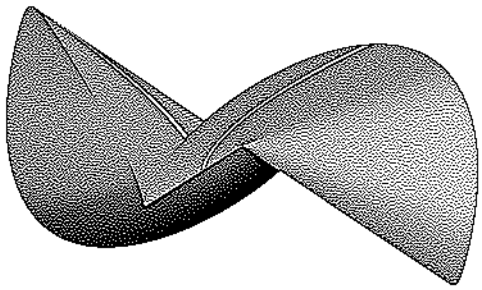


Figure 5.6: The projective curve with equation $y^3 - x^2z = 0$ and its dehomogenization with respect to $z = 1$.

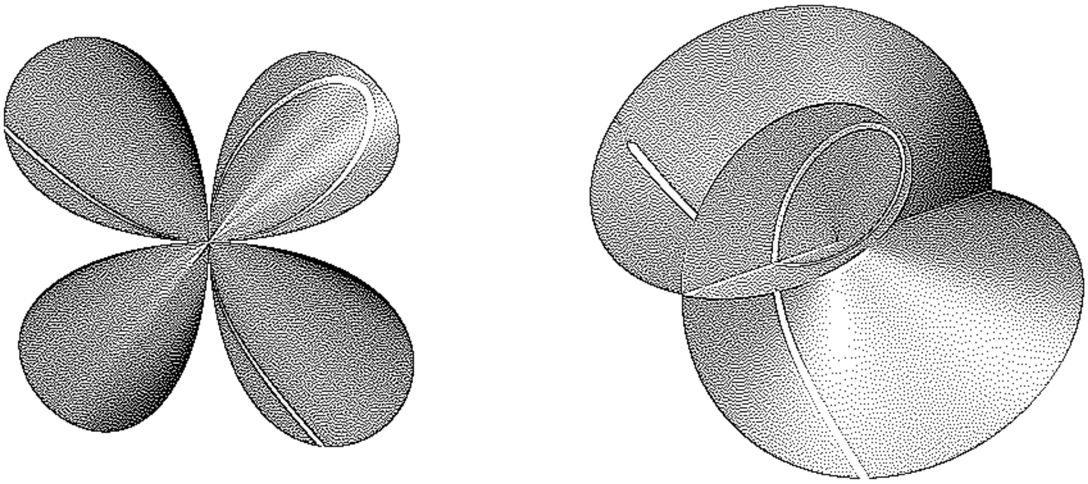


Figure 5.7: The projective curve with equation $x^3 + y^3 - 3xyz = 0$ and its dehomogenization with respect to $z = 1$.

The only curves which do not have a dehomogenization are those with equation $z^d = 0$. We call the line

$$z = 0$$

the **line at infinity** (with respect to $z = 1$). If $(u : v : w)$ is a point of $\mathbb{P}_2(k)$ then either

1. $w = 0$ and it lies on the line at infinity, or
2. $w \neq 0$ and it's a point of $\mathbb{A}_2(k)$.

That is, the line at infinity consists precisely of all the new points we added to $\mathbb{A}_2(k)$ to form $\mathbb{P}_2(k)$.

Now let C_F be a projective curve of degree d with equation $F = 0$ and let $f(x, y) = F(x, y, 1)$ be the dehomogenization of F. Suppose that $(u : v : w)$ is a point of C_F. Then either

1. $w = 0$, in which case $(u : v : w)$ lies on both the line at infinity and C_F, or
2. $w \neq 0$, in which case
$$F(u/w, v/w, 1) = 0,$$
so
$$f(u/w, v/w) = 0.$$
In this case the point $(u : v : w)$ is a point of the affine curve C_f.

Thus C_F consists of the points of C_f together with the points where C_F intersects the line at infinity. Furthermore the polynomial $F(x, y, 0)$ is homogeneous of degree d in two variables x, y or it is the zero polynomial. If $F(x, y, 0)$ is not the zero polynomial there are at most d ratios $(x : y : 0)$ such that $F(x, y, 0) = 0$ (Lemma 4.8). Therefore, either

1. $F(x, y, 0)$ is non–zero and the set C_F has at most d points on the line at infinity or
2. $F(x, y, 0) = 0$ and the line at infinity is contained in C_F.

We also define the **dehomogenization** of F and C_F with respect to $x = 1$:

$$g(y, z) = F(1, y, z) \text{ and } C_g$$

and with respect to $y = 1$:

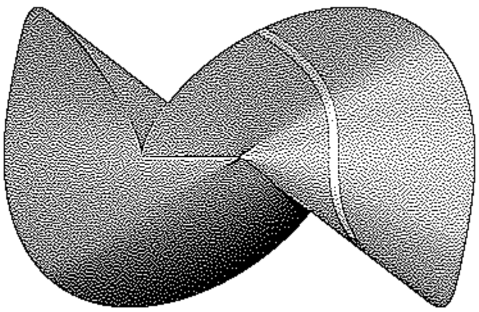
$$h(x, z) = F(x, 1, z) \text{ and } C_h.$$

The lines $x = 0$ and $y = 0$ are called the **lines at infinity** with respect to $x = 1$ and $y = 1$, respectively.

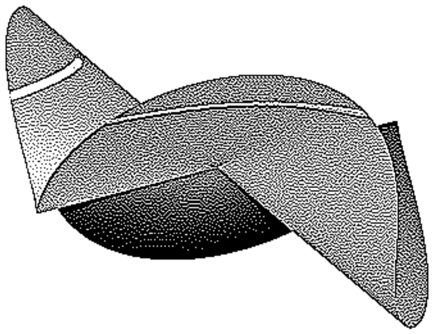
Example 5.12. The projective curve $y^3 - x^2z = 0$ has dehomogenizations $y^3 - z = 0$ and $1 - x^2z = 0$ with respect to $x = 1$ and $y = 1$ respectively. These dehomogenizations in the case $\mathbb{R} = k$ are shown in Figure 5.8.

Homogenization

Let f be a polynomial of degree d in $k[x, y]$. We form the **homogenization** of f by multiplying every term of degree $d - k$ by z^k. The resulting polynomial $F(x, y, z)$ is homogeneous of



(a) Dehomogenization with respect to $x = 1$



(b) Dehomogenization with respect to $y = 1$

Figure 5.8: The real projective curve with equation $y^3 - x^2z = 0$

degree d. Formally

$$F(x, y, z) = z^d f\left(\frac{x}{z}, \frac{y}{z}\right).$$

For example consider the polynomial $F = x^3z - yz^3$. The dehomogenization of F is $f = x^3 - y$. The homogenization of f is $x^3 - yz^2$ instead of F.

Caution Dehomogenization is not always the reverse of homogenization.

The **homogenization** of the affine curve C_f is the projective curve C_F.

Example 5.13. The line with equation $x+y+1=0$ has homogenization the line $x+y+z=0$.

This line meets the line $z=0$ at points $(u:v:w)$ where $w=0$ and $u+v=0$. That is at the unique point $(-1:1:0)$. Note that the direction ratio of this line is $(-1:1:0)$.

The line $ax+by+c=0$ has homogenization the line $ax+by+cz=0$. This line meets the line $z=0$ at points $(u:v:w)$ where $w=0$ and $au+bv=0$. That is at the unique point $(-b:a:0)$. Note that the direction ratio of this line is $(-b:a:0)$. All affine lines which are parallel have the same direction ratio and so meet $z=0$ at the same point.

Example 5.14. The homogenization of affine conics.

1. The affine parabola with equation $x-y^2=0$ has homogenization with equation $xz-y^2=0$. This curve meets $z=0$ when $y^2=0$: at the unique point $(1:0:0)$.

2. The affine circle with equation $x^2+y^2-1=0$ has homogenization with equation $x^2+y^2-z^2=0$. This curve meets $z=0$ where $x^2+y^2=0$: at points $(1:i:0)$ and $(1:-i:0)$. The real projective curve does not meet $z=0$. (Recall that $(0:0:0)$ is not a point of $\mathbb{P}_2(k)$ so is not a point of intersection.)

3. The affine hyperbola with equation $x^2-y^2-1=0$ has homogenization with equation $x^2-y^2-z^2=0$. This curve meets $z=0$ where $x^2-y^2=0$: at points $(1:1:0)$ and $(1:-1:0)$.

The real curves with these equations are shown in Figures 5.9, 5.10 and 5.11. In fact all these affine curves may be obtained by dehomogenization, with respect to appropriate planes, from a single projective quadratic. For more details see the exercises.

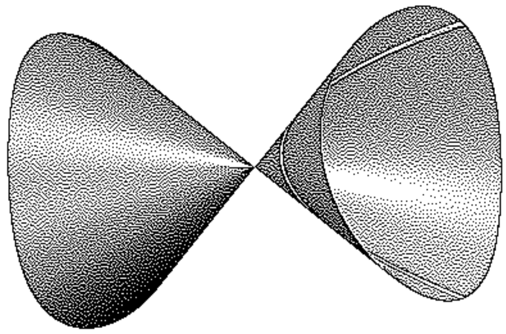


Figure 5.9: The projective curve with equation $xz - y^2 = 0$ and its dehomgenization with respect to $z = 1$.

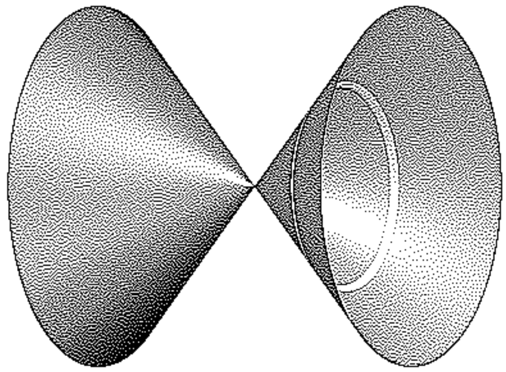


Figure 5.10: The projective curve with equation $x^2 + y^2 - z^2 = 0$ and its dehomgenization with respect to $z = 1$.

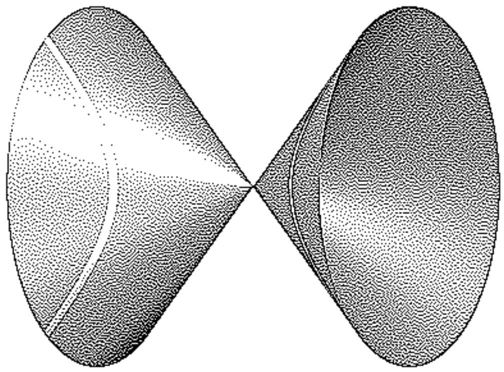


Figure 5.11: The projective curve with equation $x^2 - y^2 - z^2 = 0$ and its dehomgenization with respect to $z = 1$.

Intersection of line and curve

Let l be a projective line with parametric form $(as + ut : bs + vt : cs + wt)$, for $s, t \in k$ and let $C = C_f$ be the projective curve with equation $f = 0$. A point $p \in \mathbb{P}_2(k)$ lies on l and C if and only if $p = (as_0 + ut_0 : bs_0 + vt_0 : cs_0 + wt_0)$, for some $s_0, t_0 \in k$ and

$$f(as_0 + ut_0, bs_0 + vt_0, cs_0 + wt_0) = 0.$$

This leads to the following definition.

Definition 5.15. We call the polynomial

$$\phi(s, t) = f(as + ut, bs + vt, cs + wt)$$

an **intersection polynomial** of l and C. If $p = (as_0 + ut_0 : bs_0 + vt_0 : cs_0 + wt_0) \in l$ the **intersection number** $I(p, f, l)$ of C and l at p is the largest integer r such that $(t_0 s - s_0 t)^r | \phi(s, t)$.

It can be shown that, as in the affine case, intersection number is independant of choice of parametric form for l.

Note that if $p = (a : b : c) \in \mathbb{P}_2(k)$ then either $a \neq 0$, $b \neq 0$ or $c \neq 0$. That is we can rewrite the homogeneous coordinates of p as either $(1 : b' : c')$ or $(a' : 1 : c')$ or $(a' : b' : 1)$. Hence p becomes a point of the affine plane obtained by dehomogenizing with respect to at least one of $x = 1$, $y = 1$ or $z = 1$.

The following lemma shows that we can always reduce calculation of intersection number on a projective line to calculation of intersection number on an affine line.

Lemma 5.16. *Given a projective curve C_F and projective line L let C_f and l be the dehomogenization of C_F and L, respectively, with respect to $z = 1$. Let $p = (u : v : 1) \in \mathbb{A}_2(k)$. Then*

$$I(p, f, l) = I(p, F, L).$$

Similar statements hold for dehomogenization with respect to $x = 1$ or $y = 1$ instead of $z = 1$.

A field which contains a copy of $\mathbb{Z}_p$, for some prime p, is said to have **characteristic** p. A field containing $\mathbb{Z}$ is said to have **characteristic** ∞. If you don't like finite fields just assume $k = \mathbb{C}$ in the following Lemma.

Lemma 5.17. *Let C be a projective curve of degree d in $\mathbb{P}_2(k)$, with equation $F = 0$, where k is an algebraically closed field of characteristic greater than d. Let l be a line such that $l \nsubseteq C$. Then*

$$\sum_{p \in l \cap C} I(p, F, l) = d.$$

Proof. If $l \nsubseteq C$ then $\phi(s,t)$ is not the zero polynomial and so is homogeneous of degree d. Hence the result follows from the proof of Lemma 4.8 and the remark following Theorem 2.16.

Multiplicity

Definition 5.18. Let p be a point of a projective curve C with equation $f = 0$. We say that p has **multiplicity** r (on C) if

1. for all non–negative i, j, k such that $i + j + k = r - 1$
$$\frac{\partial f}{\partial x^i y^j z^k}(a,b,c) = 0$$
and

2. for at least one triple of non–negative integers i, j, k with $i + j + k = r$
$$\frac{\partial f}{\partial x^i y^j z^k}(a,b,c) \neq 0.$$

The terms **singular**, **non–singular**, **simple**, **double**, **triple** and **r–tuple** are defined as in the affine case (see Definition 4.13).

Example 5.19. Let C be the projective curve with equation $x^3 - yz^2 = 0$. Find the multiplicity of all singular points of C.

Tangents to projective curves could be defined, as for affine curves, by reference to partial derivatives. However the notation becomes even more cumbersome in this case and it is easier to make the following equivalent definition.

Definition 5.20. Let p be an r–tuple point of a projective curve C with polynomial f. A line l through p is called **tangent** to C at p if $I(p, f, l) > r$.

It's often easiest to find multiplicity and tangents to points of projective curves by dehomogenizing and using the following theorem, rather than working in the projective plane with the above definitions.

Theorem 5.21. *Let C_F be a projective curve with equation $F = 0$, let f be the dehomogenization of F (with respect to $z = 1$) and let C_f be the affine curve with equation $f = 0$. Suppose that $p = (u : v : 1)$ is a point of $\mathbb{P}_2(k)$. Then p has multiplicity r on C_F if and only if p has multiplicity r on C_f. Furthermore, the projective line L is tangent to C_F at p if and only if the affine line l is tangent to C_f at p, where l is the dehomogenization of L. Similar statements hold for dehomogenization with respect to $x = 1$ or $y = 1$.*

Before proving the theorem we'll look at some examples.

Example 5.22. Let C be the curve with equation $x^3 - yz^2 = 0$, as in the previous example.

Example 5.23. Find the tangents to the curve $x^3 - yz^2 = 0$ at the points $(1 : 0 : 0)$ and $(0 : 0 : 1)$.

Example 5.24. Find all singular points of the curve $x^3 + y^3 - 3xyz = 0$. Find the multiplicity of each singular point and its tangents.

In some cases we may find it easier to calculate tangents directly using the following corollary to Theorem 5.21, rather than dehomogenizing.

Corollary 5.25. *A line l is tangent to a non–singular point $p = (a : b : c)$ of a projective curve C_F if and only if l has equation*

$$xF_x(a, b, c) + yF_y(a, b, c) + zF_z(a, b, c) = 0.$$

The proof of this lemma is left to the exercises.

Example 5.26. Find the tangent to C_F at $(3 : 3 : 2)$, where $F = x^3 + y^3 - 3xyz$.

Proof of Theorem 5.21

First we consider partial derivatives of homgeneous polynomials and establish a relationship between the partial derivatives of a polynomial in 3 variables and its dehomogenization.

Lemma 5.27. *Let $F(x, y, z)$ be a homgeneous polynomial of degree d and let f be the dehomogenization of f with respect to $z = 1$. Then*

1. *F_x is either zero or homogeneous of degree $d - 1$ and*
2. *$F_x(x, y, 1) = f_x(x, y)$.*

Similar statements hold for y or z in place of x.

Proof. Let

$$F(x, y, z) = \sum a_{i,j,k} x^i y^j z^k.$$

Then

$$F_x(x, y, z) = \sum i a_{i,j,k} x^{i-1} y^j z^k.$$

Each of these terms is either zero (if $i = 0$) or of degree $d - 1$.

e.g. $x^2yz + xy^2z + xz^3 + y^2z^2$

$$f(x, y) = \sum a_{i,j,k} x^i y^j,$$

so

$$f_x(x, y) = \sum i a_{i,j,k} x^{i-1} y^j = F_x(x, y, 1).$$

We have immediately the following corollary.

Corollary 5.28.

1. *$F_{x^i y^j z^k}$ is either zero or homogeneous of degree $d - (i + j + k)$ and*
2. *$F_{x^i y^j}(x, y, 1) = f_{x^i y^j}(x, y)$.*

To prove Theorem 5.21 we need one more result.

Theorem 5.29 (Euler's Theorem). *Let $F(x, y, z)$ be a homogeneous polynomial of degree m. Then*

$$mF(x, y, z) = xF_x(x, y, z) + yF_y(x, y, z) + zF_z(x, y, z).$$

Proof. We have $t^m F(x, y, z) = F(tx, ty, tz)$. Differentiating with respect to t we obtain

$$mt^{m-1} F(x, y, z) = xF_x(tx, ty, tz) + yF_y(tx, ty, tz) + zF_z(tx, ty, tz).$$

The result follows on setting $t = 1$.

Proof of Theorem 5.21. We shall prove here that $p = (u : v : 1)$ is a singular point of C_F if and only if it is a singular point of C_f. The full statement follows from this using an obvious induction and Corollary 5.28: see the exercises. By definition p is a singular point of C_F if and only if

$$\begin{aligned} & F_x(u,v,1) = F_y(u,v,1) = F_y(u,v,1) = 0 \\ \iff & F(u,v,1) = F_x(u,v,1) = F_y(u,v,1) = 0 \quad \text{(using Euler's Theorem)} \\ \iff & f(u,v) = f_x(u,v) = f_y(u,v) = 0 \quad \text{(using Lemma 5.27)} \\ \iff & p \text{ is a singular point of } C_f. \end{aligned}$$

The statement concerning tangents follows from Lemma 5.16 and Theorem 4.19.

Asymptotes

Definition 5.30. Let C_f be an affine curve and let F be the homogenization of f. Let L be a projective line tangent to C_F at some point p on the line $z = 0$. If L is not itself the line $z = 0$ then the dehomogenization l of L is called an **asymptote** to C_f.

Example 5.32. Let $f = x^3 - y$ and so $F = x^3 - yz^2$.

There is only one point of intersection of C_F with $z = 0$ namely $(0 : 1 : 0)$. We have

$F_x = 3x^2$, $F_y = z^2$ and $F_z = 2yz$. As $F_x = F_y = 0$ implies $x = z = 0$ there is only one possible

singular point, namely $(0 : 1 : 0)$. As $F(0,1,0)_x = F_y(0,1,0) = F_z(0,1,0) = 0$ it follows that

$(0 : 1 : 0)$ is a singular point of C_F. As $F_{zz} = 2y$ we have$F_{zz}(0,1,0) \neq 0$ so $(0 : 1 : 0)$ is a double point. Note that since the only singularity of C_F lies on $z = 0$ the affine curve C_f is non–singular.

To find the equation of the tangent to C_F at $(0 : 1 : 0)$ we dehomomogenize to obtain an affine view of $(0 : 1 : 0)$. Dehomogenizing F with respect to $y = 1$ gives the polynomial $g(x, z) = x^3 - z^2$. The homogeneous coordinates $(0 : 1 : 0)$ correspond to the affine point. Note that $(0 : 1 : 0)$ is the unique singular point of C_F whilst, from Corollary 4.21, we see that $(0, 0)$ is a double point of C_g, verifying Theorem 5.21. The tangent to C_g at $(0, 0)$ is the line with parametric form $(s, 0)$, that is $z = 0$ (repeated twice). The homogenization of the affine line $z = 0$ is the projective line $z = 0$. Therefore $z = 0$ is the tangent to C_F at $(0 : 1 : 0)$. The curve C_f has no asymptote.

Note that we now have two different affine curves, C_f and C_g corresponding to the projective curve C_F. We shall now find the asymptotes of C_g. As C_g is obtained by dehomogenization with respect to $y = 1$ the corresponding line at infinity is $y = 0$. The curve C_F meets the line $y = 0$ at $(0 : 0 : 1)$, which is a non-singular point of the curve. We have

$$F_x(0, 0, 1) = 0,\ F_y(0, 0, 1) = 1 \text{ and } F_z(0, 0, 1) = 0.$$

Hence the tangent to C_F at $(0 : 0 : 1)$ has equation $y = 0$ (Theorem 5.25). Again the affine curve C_g has no asymptote.

Finally we dehomogenize F with respect to $x = 1$. This gives the polynomial $h(y, z) = 1 - yz^2$. This time the line at infinity is $x = 0$. The curve C_F meets $x = 0$ at points $(0 : y : z)$ where $yz^2 = 0$, that is at points $(0 : 0 : 1)$ and $(0 : 1 : 0)$. The first of these is non-singular with tangent $y = 0$ as we have determined above. The tangent $y = 0$ dehomogenized with respect to

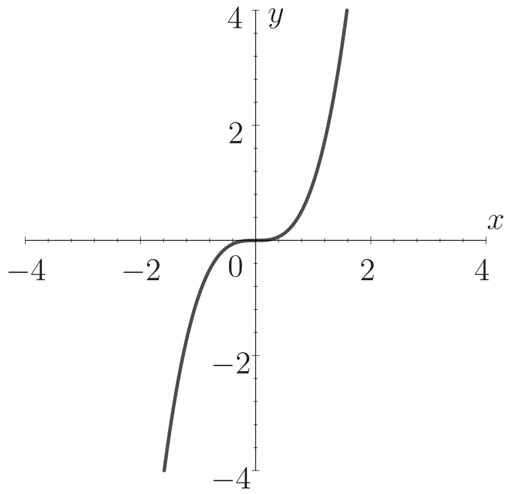


Figure 5.12: The real curve with equation $x^3 - y = 0$

$x = 1$ becomes the affine line with equation $y = 0$, which is therefore an asymptote to C_h. The second point, $(0 : 1 : 0)$, is a double point of C_F with tangent $z = 0$. Again the tangent $z = 0$ dehomogenized with respect to $x = 1$ becomes the affine line with equation $z = 0$, which is also an asymptote to C_h. Hence the curve C_h has two asymptotes.

We plot the real affine curves C_f, C_g and C_h in figures 5.12, 5.13 and 5.14 below.

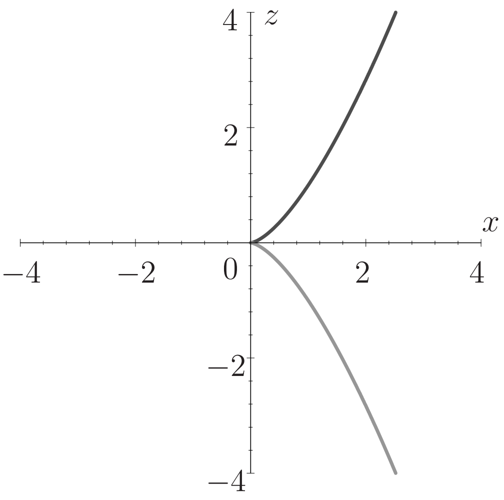


Figure 5.13: The real curve with equation $x^3 - z^2 = 0$

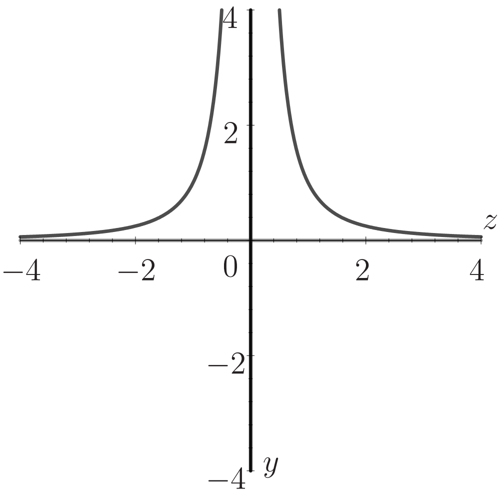


Figure 5.14: The real curve with equation $1 - yz^2 = 0$ and its asymptotes $y = 0$ and $z = 0$.

6 Bézout's Theorem

We shall not prove the following two theorems. Proofs can be found in any of the recommended texts.

Theorem 6.1. *If C and D are projective curves then C and D meet in at least one point.*

Recall that two curves C and D are said to have a common component if there is a curve E such that $E \subseteq C$ and $E \subseteq D$. From the Nullstellensatz it follows that if E is irreducible then the polynomial of E divides that of C.

Theorem 6.2 (Weak form of Bézout's Theorem). *Let C and D be two projective curves of degrees m and n, respectively. If C and D have no common component then their intersection $C \cap D$ contains at most mn points.*

Corollary 6.3. 1. *A non–singular projective curve is irreducible.*

2. *An irreducible projective curve has finitely many singular points.*

Proof.

7 Inflexions

Definition 7.1. A point p of a projective curve C_F is called an **inflexion** if

1. p is non–singular and
2. the tangent l to C at p satisfies $I(p, F, l) \geq 3$.

Example 7.2. Let F be the polynomial $y^3 - xz^2$ and C the curve with polynomial F.

We shall give a characterisation of inflexions in terms of second partial derivatives.

Definition 7.3. Let F be a non–constant homogeneous polynomial. The **Hessian** of F is

$$H_F = \begin{vmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{vmatrix}.$$

Note that if F has degree $d \geq 2$ then H_F is a homogeneous polynomial of degree $3(d-2)$. Next we prove a preliminary lemma.

Lemma 7.4. *Suppose F has degree $d \geq 1$. Then*

$$z^2 H_F = (d-1)^2 \begin{vmatrix} F_{xx} & F_{xy} & F_x \\ F_{yx} & F_{yy} & F_y \\ F_x & F_y & \left(\frac{d}{d-1}\right) F \end{vmatrix}.$$

Proof. Multiply row 3 of the matrix in the definition of H_F by z. Then multiply column 3 by z. The result is

$$z^2 H_F = \begin{vmatrix} F_{xx} & F_{xy} & zF_{xy} \\ F_{yx} & F_{yy} & zF_{yz} \\ zF_{zx} & zF_{zy} & z^2F_{zz} \end{vmatrix}.$$

Now add $x \cdot (\text{row } 1) + y \cdot (\text{row } 2)$ to row 3. Euler's Theorem for the degree $d-1$ polynomial F_x is

$$(d-1)F_x = xF_{xx} + yF_{yx} + zF_{zx},$$

so we obtain

$$z^2 H_F = \begin{vmatrix} F_{xx} & F_{xy} & zF_{xy} \\ F_{yx} & F_{yy} & zF_{yz} \\ (d-1)F_x & (d-1)F_y & z(d-1)F_z \end{vmatrix}.$$

Adding $x \cdot (\text{column } 1) + y \cdot (\text{column } 2)$ to column 3, and using Euler's theorem again, gives the required result.

Theorem 7.5. *Let F have degree at least 2. A point $p = (u : v : w)$ of the curve C_F is an inflexion if and only if*

1. *p is non–singular and*
2. *$H_F(u, v, w) = 0$.*

Proof. Assume that p has coordinates $(u : v : 1)$. (The other cases follow using a similar argument.) Define $f(x, y) = F(x, y, 1)$ and let $q = (u, v)$, so $q \in C_f$. Then from Theorem 5.21 and Lemma 5.16 it follows that p is an inflexion of C_F if and only if q is a non–singular point of C_f and the tangent l to C_f at q satisfies $I(q, f, l) \geq 3$. It therefore suffices to show that, given q is non–singular, then $I(q, f, l) \geq 3$ if and only if $H_F(u, v, 1) = 0$.

Write $f_x = f_x(u, v)$ and $f_y = f_y(u, v)$ and similarly for higher order derivatives. Then, using Definition 4.16, the tangent l to C_f at q is the line with parametric form $(as + u, bs + v)$, $s \in k$, where

$$af_x + bf_y = 0.$$

This has solution $a = -f_y$ and $b = f_x$. Set $a = -f_y$ and $b = f_x$. Now $I(q, f, l)$ is the largest integer r such that $s^r | f(as + u, bs + v)$ and

$$\begin{aligned} f(as + u, bs + v) = f(u, v) & \\ + s(af_x + bf_y) & \\ + \frac{s^2}{2!}(a^2 f_{xx} + 2ab f_{xy} + b^2 f_{yy}) + s^3 R(s), & \end{aligned}$$

where $R(s)$ is a polynomial. As $q \in C_f$ so $f(u, v) = 0$ and we have

$$f(as + u, bs + v) = \frac{s^2}{2!}(a^2 f_{xx} + 2ab f_{xy} + b^2 f_{yy}) + s^3 R(s).$$

Thus

$$I(q,f,l) \geq 3 \quad \text{if and only if} \quad a^2 f_{xx} + 2ab f_{xy} + b^2 f_{yy} = 0. \tag{7.1}$$

As $p \in C_F$ we have, using Lemma 7.4

$$H_F(u,v,1) = (d-1)^2 \begin{vmatrix} F_{xx} & F_{xy} & F_x \\ F_{yx} & F_{yy} & F_y \\ F_x & F_y & 0 \end{vmatrix}.$$

Furthermore $F_x(u,v,1) = f_x(u,v)$ and similarly for all the other partial derivatives (of first and higher orders). Thus

$$\begin{aligned} H_F(u,v,1) &= (d-1)^2 \begin{vmatrix} f_{xx} & f_{xy} & f_x \\ f_{yx} & f_{yy} & f_y \\ f_x & f_y & 0 \end{vmatrix} \\ &= (d-1)^2[-f_x^2 f_{yy} + 2 f_x f_y f_{xy} - f_y^2 f_{xx}] \\ &= (d-1)^2[-b^2 f_{yy} - 2ab f_{xy} - a^2 f_{xx}]. \end{aligned}$$

Hence

$$H_F(u,v,1) = 0 \quad \text{if and only if (7.1) holds.}$$

Thus p is an inflexion if and only if q is non–singular and $I(q,f,l) \geq 3$ which is true if and only if p is non–singular and $H_F(u,v,1) = 0$. This completes the proof of the Theorem.

Example 7.6. Find all the inflexions of C_F, where $F = x^3 + y^3 - 3xyz$.

8 Cubics and the group law

A curve of degree 3 is a **cubic**. It can be shown that (when k is algebraically closed)

a non–singular cubic in $\mathbb{P}_2(k)$ has exactly nine inflexions.

We shall assume througout this section that all curves are defined over an algebraically closed field.

Theorem 8.1. *Let C be a non–singular projective cubic with equation $F = 0$ and let l be a line. Then the intersection of l and C consists of either*

1. *3 distinct points p_1, p_2 and p_3 with $I(p_i, F, l) = 1$, for $i = 1, 2, 3$, so that l is not tangent to C at p_i; or*
2. *2 distinct points p_1 and p_2 with $I(p_1, F, l) = 1$ and $I(p_2, F, l) = 2$ so that l is tangent to C at p_2 but not at p_1; or*
3. *1 point p with $I(p, F, l) = 3$ so l is tangent to C at p and p is an inflexion.*

Proof. This follows from Lemma 5.17.

The group law on the cubic

Here we shall denote the line through points A and B by AB. Let $\mathcal{C}$ be a non–singular projective cubic and let O be an inflexion of $\mathcal{C}$.

Definition 8.2. Given $X \in \mathcal{C}$ let $\overline{X}$ denote the third point of intersection of OX with $\mathcal{C}$ (where intersections are counted according to intersection number).

In particular we interpret this definition to mean that $\overline{O} = O$, as O is an inflexion. Next we define an operation of addition on the points of $\mathcal{C}$.

Definition 8.3. Given points $P, Q \in \mathcal{C}$ we define a point $P + Q$ of $\mathcal{C}$ as follows. First let X be the third point of intersection of PQ with $\mathcal{C}$. Now set $P + Q = \overline{X}$.

Theorem 8.4. *The set of points of $\mathcal{C}$ with the operation of addition defined above forms an Abelian group.*

Proof. It follows from Theorem 8.1 that $P + Q$ is a unique point of $\mathcal{C}$. Therefore the given operation of addition is a binary operation on the set of points of $\mathcal{C}$. We need to check that it has an identity, that there are inverses, that it is associative and that it is commutative.

Identity: The point O is the identity element. To see this suppose that P is a point of $\mathcal{C}$. We must show that $P + O = P = O + P$. Let X be the third point of intersection of PO and $\mathcal{C}$. Now we have the line PO passing through O, P and X.

By definition $P+O = \overline{X}$, the third point of intersection of OX with $\mathcal{C}$. That is $P+O = P$. Similarly $O + P = P$, so O is the identity as claimed.

Inverse: Let P be a point of $\mathcal{C}$. Then $\overline{P}$ is the third point of intersection of OP and $\mathcal{C}$.

Thus $\overline{P}P$ passes through O, P and $\overline{P}$. It follows that $P + \overline{P} = \overline{O} = O$. Similarly $\overline{P} + P = O$. Hence the inverse of P is $\overline{P}$.

Associative: This is the only group axiom that is non–trivial to check and we omit it.

Commutative: The line PQ is the same as the line QP so $P+Q=Q+P$.

Example 8.5. Consider the curve $\mathcal{C}_F$, where $F=x^3+y^3-z^3$. We have

$$F_x=3x^2,\ F_y=3y^2 \text{ and } F_z=-3z^2.$$

As $F_x=F_y=F_z=0$ implies $x=y=z=0$ the curve is non–singular. We have

$$F_{xx}=6x,\ F_{yy}=6y,\ F_{zz}=-6z \text{ and } F_{xy}=F_{xz}=F_{yz}=0.$$

Hence

$$H_F=\begin{vmatrix} 6x & 0 & 0 \\ 0 & 6y & 0 \\ 0 & 0 & -6z \end{vmatrix}=-6^3xyz.$$

Therefore $H_F=0$ if and only if $x=0$, $y=0$ or $z=0$.

$x=0$**:** In this case $F(0,y,z)=y^3-z^3=0$ and we may assume $y=1$ (as $y=0$ implies $x=y=z=0$). We find z by solving $1-z^3=0$, to give $z=1$, ω or ω^2, where $\omega^3=1$ and $\omega\neq 1$. The points of inflexion with $x=0$ are therefore

$$(0:1:1),\ (0:1:\omega) \text{ and } (0:1:\omega^2).$$

$y=0$**:** In this case $F(x,0,z)=x^3-z^3=0$ and we may assume $z=1$ (as $z=0$ implies $x=y=z=0$). We find x by solving $x^3-1=0$, to give $x=1$, ω or ω^2, where $\omega^3=1$ and $\omega\neq 1$. The points of inflexion with $y=0$ are therefore

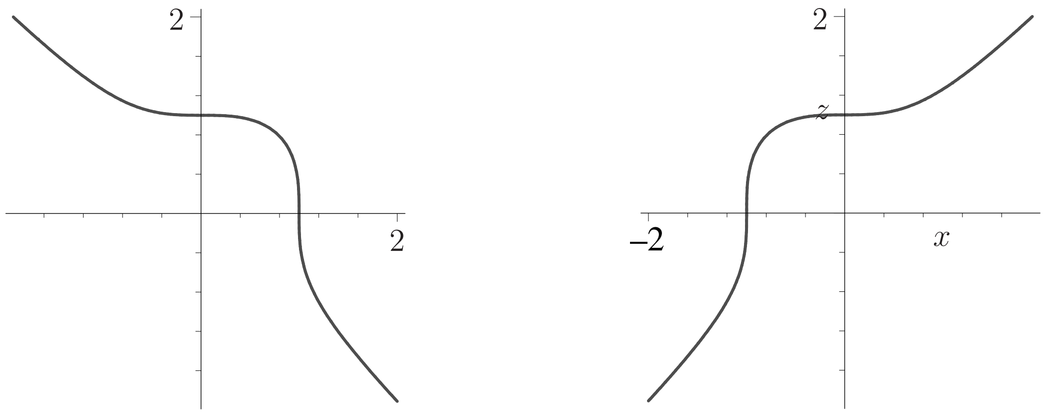
$$(1:0:1),\ (1:0:\omega) \text{ and } (1:0:\omega^2).$$

$z=0$**:** In this case $F(x,y,0)=x^3+y^3=0$ and we may assume $x=1$ (as $x=0$ implies $x=y=z=0$). We find y by solving $1+y^3=0$, to give $y=-1$, $-\omega$ or $-\omega^2$, where $\omega^3=1$ and $\omega\neq 1$. The points of inflexion with $z=0$ are therefore

$$(1:-1:0),\ (1:-\omega:0) \text{ and } (1:-\omega^2:0).$$

There are a total of nine inflexions as expected. The inflexions on the real curve at $(0:1:1)$ and $(1:0:1)$ can be shown by dehomogenizing with respect to $z=1$. This gives the affine curve $x^3+y^3-1=0$ with inflexions at $(0,1)$ and $(1,0)$ (see Figure 8.15(a)). The inflexions at $(0:1:1)$ and $(-1:1:0)=(1:-1:0)$ can be seen by dehomogenizing with respect to $y=1$. This gives the affine curve $x^3+1-z^3=0$ with inflexions at $(0,1)$ and $(-1,0)$ see Figure 8.15(b)).

Now consider the group law on $\mathcal{C}$ with base point $O=(0:1:1)$. Let $P=(1:0:\omega)$ and $Q=(1:-\omega^2:0)$. We shall compute $P+Q$. The line PQ has parametric form $(s+t:-\omega^2t:$



(a) The curve $x^3 + y^3 - 1 = 0$ (b) The curve $x^3 + 1 - z^3 = 0$

Figure 8.15: Dehomogenizations of the real curve $x^3 + y^3 - z^3 = 0$

$\omega s)$, for $s, t \in k$. To find the third point of intersection of PQ and $\mathcal{C}$ we substitute these values into the equation of $\mathcal{C}$ to obtain

$$\phi(s,t) = (s+t)^3 + (-\omega^2 t)^3 - (\omega s)^3 = 3s^2t + 3st^2 = 3st(s+t).$$

Thus $\phi(s,t) = 0$ if $s = 0$, $t = 0$ or $s + t = 0$. The zeros $s = 0$ and $t = 0$ correspond to P and Q so the third point of intersection X, corresponding to $s+t = 0$ is $X = (0 : \omega^2 : \omega) = (0 : 1 : \omega^2)$. To compute $P+Q$ we must find $\overline{X}$. As O and X both have x–coordinate 0 it follows that the line OX is $x = 0$. Substituting $x = 0$ in F we see that this line meets $\mathcal{C}$ at O, X and $\overline{X} = (0 : 1 : \omega)$. Hence

$$P + Q = (0 : 1 : \omega).$$