Polynomials

Definition 1.1. Let k be a field. A **polynomial** f over k in variables $x_1, \ldots, x_n$ is a sum

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

where

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

When convient we write α for the n–tuple $\alpha_1, \ldots, \alpha_n$ and $a_\alpha \mathbf{x}^\alpha$ for $a_{\alpha_1, \ldots, \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

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.

Writing polynomials

When writing polynomials we use the following conventions.

1. We do not write down $a_{\alpha_1,\ldots,\alpha_n}x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ 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 $ax_1^0\cdots x_n^0$. Thus $2x_1^2x_2^0x_3^3$ is written as $2x_1^2x_3^3$ and $3x_1^0x_2^0x_3^4$ as $3x_3^4$.

Polynomial terminology

Definition 1.3. Let

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

be a polynomial over k.

1. $a_{\alpha_1, \ldots, \alpha_n}$ 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 terms of f. If f is the zero polynomial then f has **degree** $-\infty$.

Addition of polynomials

Definition 1.4. 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 1.5.
Let $f = x_1^2 + x_2^2 + x_1^2 x_2$ and $g = 2x_1^2 + x_1 x_2 - 3x_2^2 + 1$ then

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

Multiplication of polynomials

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 **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 1.7.

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

$$\begin{aligned} fg &= x^3y^2 + x^5 + 2x^2 + xy^4 + x^3y^2 + 2y^2 + xy^2 + x^3 + 2 \\ &= 2x^3y^2 + x^5 + 2x^2 + xy^4 + 2y^2 + xy^2 + x^3 + 2. \end{aligned}$$

Affine space

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 $\mathbb{A}_n(k)$.

Affine space

Definition 2.1.

Let k be a field and let n be a positive integer.

Affine 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.

Affine curves

Definition 2.3.

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

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** $f = 0$.

Affine curves

Definition 2.3.

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

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** $f = 0$.

C_f has **degree** d and is a curve **in** $\mathbb{A}_2(k)$.

Affine curves

Definition 2.3.

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

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** $f = 0$.

C_f has **degree** d and is a curve **in** $\mathbb{A}_2(k)$.

C_f is **defined** by f and has **polynomial** f.

Affine curves

Definition 2.3.

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

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** $f = 0$.

C_f has **degree** d and is a curve **in** $\mathbb{A}_2(k)$.

C_f is **defined** by f and has **polynomial** f.

A curve may have many different equations.

Example 2.4.

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

Some well known curves

Example 2.4.

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

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

Some well known curves

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**.

Some well known curves

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.

Some well known curves

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 $g = x^4 - 2x^2y + y^2$.

Polynomials again

Lemma 2.5.

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

Then

1. $\mathrm{degree}(fg) = \mathrm{degree}(f) + \mathrm{degree}(g)$ *and*

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

Polynomials again

Lemma 2.5.

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

Then

1. $\text{degree}(fg) = \text{degree}(f) + \text{degree}(g)$ *and*

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

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

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

4. *the degree of x_i in $f + g$* $\leq \max\{\textit{degree of } x_i \textit{ in } f,\ \textit{degree of } x_i \textit{ in } g\}$.

Reducible and irreducible polynomials

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 $f = gh$.

Reducible and irreducible polynomials

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 $f = gh$.

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.

Examples: reducible and irreducible polynomials

Example 2.8.

1. The polynomial x^n is reducible if $n > 0$ and irreducible if $n = 0$.

Examples: reducible and irreducible polynomials

Example 2.8.

1. The polynomial x^n is reducible if $n > 0$ and irreducible if $n = 0$.

2. The polynomial $x^2 - y^2$ is reducible as $x^2 - y^2 = (x + y)(x - y)$.

Examples: reducible and irreducible polynomials

Example 2.8.

1. The polynomial x^n is reducible if $n > 0$ and irreducible if $n = 0$.

2. The polynomial $x^2 - y^2$ is reducible as $x^2 - y^2 = (x + y)(x - y)$.

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

Examples: reducible and irreducible polynomials

Example 2.8.

1. The polynomial x^n is reducible if $n > 0$ and irreducible if $n = 0$.

2. The polynomial $x^2 - y^2$ is reducible as $x^2 - y^2 = (x + y)(x - y)$.

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

4. All polynomials of degree 1 are irreducible.

Examples: reducible and irreducible polynomials

Example 2.8.

1. The polynomial x^n is reducible if $n > 0$ and irreducible if $n = 0$.
2. The polynomial $x^2 - y^2$ is reducible as $x^2 - y^2 = (x + y)(x - y)$.
3. Let $f = x^2yz - xz^2 - xy^3 + y^2z$.
4. All polynomials of degree 1 are irreducible.
5. The polynomial $f = x^2 - y$ is irreducible.

Examples: reducible and irreducible polynomials

Example 2.8.

1. The polynomial x^n is reducible if $n > 0$ and irreducible if $n = 0$.

2. The polynomial $x^2 - y^2$ is reducible as $x^2 - y^2 = (x + y)(x - y)$.

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

4. All polynomials of degree 1 are irreducible.

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

Examples: reducible and irreducible polynomials

Example 2.8.

1. The polynomial x^n is reducible if $n > 0$ and irreducible if $n = 0$.

2. The polynomial $x^2 - y^2$ is reducible as $x^2 - y^2 = (x+y)(x-y)$.

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

4. All polynomials of degree 1 are irreducible.

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

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

Irreducible polynomials

irreducible $\iff$ any factor is constant or a constant multiple

Irreducible polynomials

irreducible $\iff$ any factor is constant or a constant multiple

That is,

if f is irreducible and $g|f$ then

either g is a constant

or $g = af$, for some $a \in k$.

Irreducible polynomials

irreducible $\iff$ any factor is constant or a constant multiple

That is,

if f is irreducible and $g|f$ then

either g is a constant

or $g = af$, for some $a \in k$.

(In $\mathbb{Z}$ the irreducible elements are primes.)

Irreducible factorisation

Let f be reducible and of degree d.

Write $f = gh$, where

$$1 \leq \text{degree}(g) \leq d-1 \quad \text{and} \quad 1 \leq \text{degree}(h) \leq d-1.$$

Irreducible factorisation

Let f be reducible and of degree d.

Write $f = gh$, where

$$1 \leq \text{degree}(g) \leq d-1 \quad \text{and} \quad 1 \leq \text{degree}(h) \leq d-1.$$

If either g or h is reducible then we can repeat the process, factorizing into polynomials of lower degree.

Irreducible factorisation

Let f be reducible and of degree d.

Write $f = gh$, where

$$1 \leq \text{degree}(g) \leq d - 1 \quad \text{and} \quad 1 \leq \text{degree}(h) \leq d - 1.$$

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.

Irreducible factorisation

Let f be reducible and of degree d.

Write $f = gh$, where

$$1 \leq \mathrm{degree}(g) \leq d-1 \quad \text{and} \quad 1 \leq \mathrm{degree}(h) \leq d-1.$$

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* $k[x_1, \dots, x_n]$.

Then f *has an irreducible factorization.*

This factorization is unique up to the order of the irreducible factors and multiplication by constants.

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.

Example 2.10.

1. The polynomial $x^2 - y^2$ has irrreducible factorisation $(x+y)(x-y)$.

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.

Example 2.10.

1. The polynomial $x^2 - y^2$ has irrreducible factorisation $(x+y)(x-y)$.

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

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.

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 $h = xz - y^2$.

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.

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.

Irreducible curves

Lemma 2.11.

If f, g *and* h *are non-constant polynomials in* $k[x, y]$ *with* $f = gh$ *then*

$$C_f = C_g \cup C_h.$$

Irreducible curves

Lemma 2.11.

If f, g and h are non-constant polynomials in $k[x, y]$ with $f = gh$ then

$$C_f = C_g \cup C_h.$$

Example 2.12.

1. The curve with equation

$$x^2 - y^2 = 0.$$

Irreducible curves

Lemma 2.11.

If f, g and h are non-constant polynomials in $k[x, y]$ with $f = gh$ then

$$C_f = C_g \cup C_h.$$

Example 2.12.

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

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

Irreducible components

Definition 2.13.

Let f be an irreducible polynomial in $k[x, y]$.

Then the curve C_f is called an **irreducible** affine curve.

Irreducible components

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** $C_{q_1}, \ldots, C_{q_s}$.

Note: If C_f has irreducible components

$$C_{q_1}, \ldots, C_{q_s}$$

then

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

(Lemma 2.11)

Note: If C_f has irreducible components

$$C_{q_1}, \ldots, C_{q_s}$$

then

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

(Lemma 2.11)

Therefore every curve is a union of irreducible curves.

Example 2.15.

1. Lines are 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 $x - y = 0$.

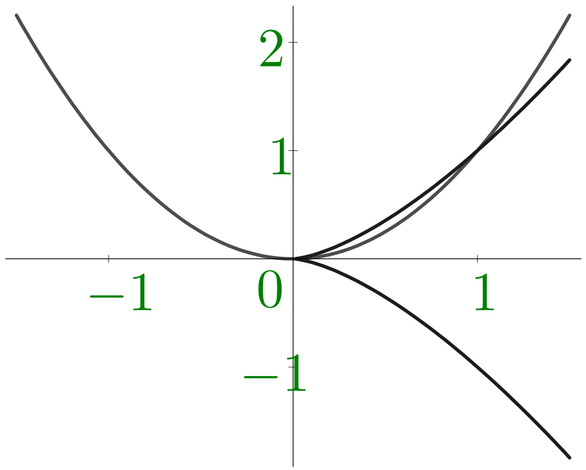
Example 2.15.

1. Lines are irreducible curves.

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

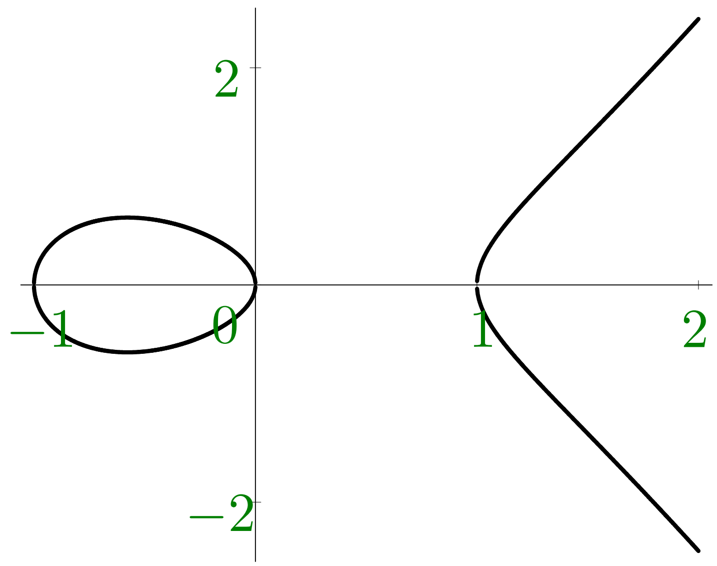
3. Let $f = x^5 - x^3y - x^2y^2 + y^3$.

   C_f has irreducible components C_g and C_h.



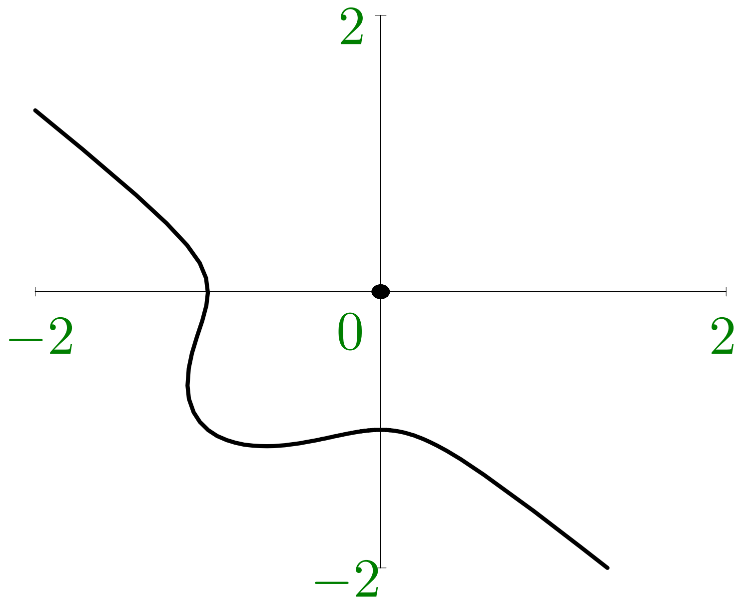
An irreducible curve with 2 branches

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 $y^2 - x(x^2 - 1) = 0$ is irreducible over $\mathbb{R}$.



An irreducible curve with an isolated point

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:



A curve repeated twice

6. On the other hand curves which, when drawn, look irreducible may not be.

   For example let $f = x^2 - 2xy + y2$. 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 $y = x$.

Polynomials of one variable

Theorem 2.16.

Let k *be a field and let* $f \in k[t]$ *be a polynomial of degree* d*.*

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.*

Algebraically closed fields

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**.

Algebraically closed fields

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**.

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 $a_0 \neq 0$.

Algebraically closed fields

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**.

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 from Theorem 2.16 by induction on the degree d of f.

Algebraically closed fields

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**.

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 from Theorem 2.16 by induction on the degree d of f.

The a_i's are not necessarily distinct.

Multiplicity of roots of a polynomial

Collect together all the repeated linear factors and 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 $r_1 + \cdots + r_k = d$.

Multiplicity of roots of a polynomial

Collect together all the repeated linear factors and 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 $r_1 + \cdots + r_k = d$.

The **multiplicity** of the zero b_i is r_i.

Example 2.17.

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

Example 2.17.

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

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

Theorem 2.18.

Let k *be an infinite field and let* $f \in k[x_1, \ldots x_n]$*.*

If

$$f(a_1, \ldots, a_n) = 0 \quad \textit{for all} \quad (a_1, \ldots, a_n) \in \mathbb{A}_n(k)$$

then f *is the zero polynomial.*

Hilbert's Nullstellensatz

Theorem 2.19.

Let k *be an algebraically closed field and let* f *and* g *be non–constant polynomials in* $k[x_1, \ldots x_n]$.

Suppose that

1. g *is irreducible and*

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

Then $g|f$.

Implication for curves

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 $C_g \subset C_f$ *and* g *is irreducible then* $g|f$.

When k is algebraically closed:

$$\text{Curves} \iff \text{Polynomials without repeated factors.}$$

When k is algebraically closed:

$$\text{Curves} \iff \text{Polynomials without repeated factors.}$$

In particular:

if f and g are irreducible polynomials and $C_f = C_g$ then $g = af$, for some $a \in k$.

When k is algebraically closed:

$$\text{Curves} \iff \text{Polynomials without repeated factors.}$$

In particular:

if f and g are irreducible polynomials and $C_f = C_g$ then $g = af$, for some $a \in k$.

Drop the requirement that k is algebraically closed and the theorem fails.

Example 2.21.

Let $k = \mathbb{R}$ and consider the curve C with equation $x^2 + y^2 + 1 = 0$.

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.

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.

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.

Its equation is irreducible over $\mathbb{R}$.

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.

Its equation is irreducible over $\mathbb{R}$.

However the polynomial f does not divide the polynomial of every other curve:

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.

Its equation is irreducible over $\mathbb{R}$.

However the polynomial f does not divide the polynomial of every other curve:

in particular it does not divide any linear polynomial.

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.

Its equation is irreducible over $\mathbb{R}$.

However the polynomial f 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 $\mathbb{A}_2(\mathbb{R})$.

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.

Its equation is irreducible over $\mathbb{R}$.

However the polynomial f 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 f.

Parametric form of a line

Suppose l is a line with equation $ax + by + c = 0$, where $(a, b) \neq (0, 0)$, and (x_0, y_0) a point of l.

Then l is

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

Parametric form of a line

Suppose l is a line with equation $ax + by + c = 0$, where $(a, b) \neq (0, 0)$, and (x_0, y_0) a point of l.

Then l is

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

On the other hand, given $a, b, x_0, y_0 \in k$ with $(a, b) \neq (0, 0)$ set

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

Parametric form of a line

Suppose l is a line with equation $ax + by + c = 0$, where $(a, b) \neq (0, 0)$, and (x_0, y_0) a point of l.

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

On the other hand, given $a, b, x_0, y_0 \in k$ with $(a, b) \neq (0, 0)$ set

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

Then (3.1) defines a line, with equation

$$ax + by + c = 0,$$

passing through (x_0, y_0).

(3.1) is the **parametric form** of the line l.

abbreviated to $(x_0 - bs, y_0 + as)$

(3.1) is the **parametric form** of the line l.

abbreviated to $(x_0 - bs, y_0 + as)$

- The parametric form of l depends on the choice of point $(x_0, y_0) \in l$.

(3.1) is the **parametric form** of the line l.

abbreviated to $(x_0 - bs, y_0 + as)$

- The parametric form of l depends on the choice of point $(x_0, y_0) \in l$.
- The ratio $(-b : a)$ is the **direction ratio** of l.

(3.1) is the **parametric form** of the line l.

abbreviated to $(x_0 - bs, y_0 + as)$

- The parametric form of l depends on the choice of point $(x_0, y_0) \in l$.
- The ratio $(-b : a)$ is the **direction ratio** of l.

Example 3.1. The line l with equation $2x + 5y + 1 = 0$ ...

Intersection polynomials

Let l contain (x_0, y_0) and have parametric form $(x_0 - bs, y_0 + as)$.

Let C be the curve with equation $f = 0$.

Intersection polynomials

Let l contain (x_0, y_0) and have parametric form $(x_0 - bs, y_0 + as)$.

Let C 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

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

Intersection polynomials

Let l contain (x_0, y_0) and have parametric form $(x_0 - bs, y_0 + as)$.

Let C 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

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

Definition 3.2. We call the polynomial

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

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

Intersection polynomials

Let l contain (x_0, y_0) and have parametric form $(x_0 - bs, y_0 + as)$.

Let C 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

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

Definition 3.2. We call the polynomial

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

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

ϕ depends on the choice of parametrisation of l.

Intersection number

Point of intersection of l and $C \iff u \in k$ such that $\phi(u) = 0$ (3.2)

Intersection number

Point of intersection of l and $C \iff u \in k$ such that $\phi(u) = 0$ (3.2)

$\phi(u) = 0 \iff (s - u) | \phi(s)$. (Theorem 2.16.)

Intersection number

Point of intersection of l and $C \iff u \in k$ such that $\phi(u) = 0$ (3.2)

$\phi(u) = 0 \iff (s-u)|\phi(s)$. (Theorem 2.16.)

$l \cap C$ is the set of points $(x_0 - bu, y_0 + au)$ such that $(s-u)|\phi(s)$.

Intersection number

Point of intersection of l and $C \iff u \in k$ such that $\phi(u) = 0$ (3.2)

$\phi(u) = 0 \iff (s-u)|\phi(s)$. (Theorem 2.16.)

$l \cap C$ is the set of points $(x_0 - bu, y_0 + au)$ such that $(s-u)|\phi(s)$.

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 $y + 1 = 0$.

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 $(s, -1)$, where $s \in k$.

Example 3.5. Let $f = x^2 - y$ and

let l_m be the line with equation $y = mx$.

Example 3.5. Let $f = x^2 - y$ and

let l_m be the line with equation $y = mx$.

Then l_m has parametric form (s, ms), where $s \in k$.

Number of intersections

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 $s \in k$.

Number of intersections

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 $s \in k$.

Theorem 2.18 $\Rightarrow$ that ϕ is the zero polynomial (as long as k is an infinite field),

Number of intersections

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 $s \in k$.

Theorem 2.18 $\Rightarrow$ that ϕ is the zero polynomial (as long as k is an infinite field),

so $(s-u)^r|\phi(s)$, for all $r \geq 0$

Number of intersections

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 $s \in k$.

Theorem 2.18 $\Rightarrow$ that ϕ is the zero polynomial (as long as k is an infinite field),

so $(s-u)^r|\phi(s)$, for all $r \geq 0$

and the intersection number $I(q, f, l) = \infty$, for all $q \in \mathbb{A}_2(k)$.

Number of intersections

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 $s \in k$.

Theorem 2.18 $\Rightarrow$ that ϕ is the zero polynomial (as long as k is an infinite field),

so $(s-u)^r|\phi(s)$, for all $r \geq 0$

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

Lines and curves

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

Lines and curves

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

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

Polynomials and Taylor's theorem

Definition 4.3. Let $f = a_0 + a_1 x + \cdots a_n x^n$ be a polynomial in $k[x]$. Then the **derivative** of f with respect to x is

$$f' = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Polynomials and Taylor's theorem

Definition 4.3. Let $f = a_0 + a_1 x + \cdots a_n x^n$ be a polynomial in $k[x]$. Then the **derivative** of f with respect to x is

$$f' = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

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 of Taylor's theorem

The polynomial $f(x+u)$ has degree d and we can write

$$f(x+u) = a_0 + a_1 x + \cdots a_n x^d, \qquad \text{with } a_i \in k.$$

Proof of Taylor's theorem

The polynomial $f(x+u)$ has degree d and we can write

$$f(x+u) = a_0 + a_1 x + \cdots a_n x^d, \qquad \text{with } a_i \in k.$$

The rth derivative of $f(x+u)$ with respect to x is then

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

Proof of Taylor's theorem

The polynomial $f(x+u)$ has degree d and we can write

$$f(x+u) = a_0 + a_1 x + \cdots a_n x^d, \qquad \text{with } a_i \in k.$$

The rth derivative of $f(x+u)$ with respect to x is then

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

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

Proof of Taylor's theorem

The polynomial $f(x+u)$ has degree d and we can write

$$f(x+u) = a_0 + a_1 x + \cdots a_n x^d, \qquad \text{with } a_i \in k.$$

The rth derivative of $f(x+u)$ with respect to x is then

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

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

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

Proof of Taylor's theorem

The polynomial $f(x+u)$ has degree d and we can write

$$f(x+u) = a_0 + a_1 x + \cdots a_n x^d, \qquad \text{with } a_i \in k.$$

The rth derivative of $f(x+u)$ with respect to x is then

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

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

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.

Partial derivatives of polynomials

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.

Example

If $f(x,y) = x^8y^3 + 3x^2y^6 + 17x + y^{10} + 3$ then

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

and

$$\frac{\partial f}{\partial y}(x,y) = 3x^8y^2 + 18x^2y^5 + 10y^9.$$

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*

$$f'(g_1(s), \ldots, g_n(s)) = \sum_{i=1}^{n} f_{x_i}(g_1(s), \ldots, g_n(s))g_i'(s).$$

Taylor's Theorem

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

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

Proof of Taylor's theorem (several variables)

Let $\phi(s) = f(sa + x_0, sb + y_0)$. Using Taylor's theorem for polynomials of one variable (Theorem 4.4) we have

$$\phi(s) = \phi(0) + s\phi'(0) + \frac{s^2}{2!}\phi''(0) + \cdots + \frac{s^n}{n!}\phi^{(n)}(0).$$

Proof of Taylor's theorem (several variables)

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

$$\begin{aligned}
\phi(0) &= f(x_0, y_0) \\
\phi'(0) &= a\frac{\partial f}{\partial x}(x_0, y_0) + b\frac{\partial f}{\partial y}(x_0, y_0) \\
&\vdots \\
\phi^{(k)}(0) &= \sum_{j=0}^{k} \binom{k}{j} a^{k-j} b^j \frac{\partial^k f}{\partial x^{k-j}\partial y^j}(x_0, y_0).
\end{aligned}$$

Taylor's theorem again

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

Then

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

Taylor's theorem again

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.

Homogenous polynomials of 2 variables

A ratio $(a : b)$ is **non–zero** if $(a, b) \neq (0, 0)$.

Homogenous polynomials of 2 variables

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 2 variables.*

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

Write

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

where $c_j \neq 0$, for some j.

Proof

Write

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

where $c_j \neq 0$, for some j.

Given (a, b) we have $f(a, b) = 0$ if and only if $f(ta, tb) = 0$, for all $t \neq 0$.

Proof

Write

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

where $c_j \neq 0$, for some j.

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 $(c : d) = (a : b)$.

Proof

Write

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

where $c_j \neq 0$, for some j.

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 $(c : d) = (a : b)$.

Any non–zero ratio $(a : 0)$ is equal to $(1 : 0)$

and 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 $(t : 1)$.

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.

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 $f(t,1)$. 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 $a_i \in \mathbb{C}$.

If $k = \mathbb{C}$ then

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

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

Let

$$t = \frac{x}{y}.$$

Then

$$f(t,1) = a_0 \prod_{i=1}^{d} \left(\frac{x}{y} - a_i \right)$$

If $k = \mathbb{C}$ then

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

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

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

$$c_d = c_{d-1} = \cdots = c_{d-e+1} = 0 \text{ and } c_{d-e} \neq 0.$$

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

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

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

$$f_x(x_0, y_0) = f_y(x_0, y_0) = 0.$$

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**.

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**.

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

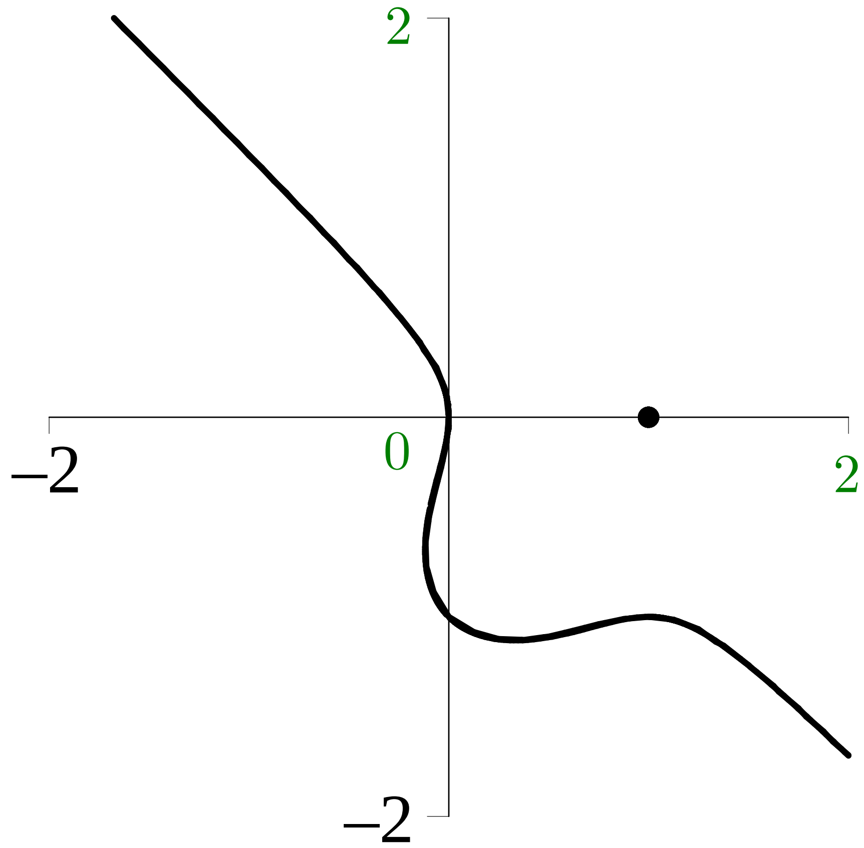
$$f(x, y) = x^3 + y^3 - 3xy.$$

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

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

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

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



We have

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

We have

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

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

We have

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

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 $x = 1$.

We have

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

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 $f_x = 1 \neq 0$.

We have

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

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.

We have

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

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

$$f(1, 0) = f_x(1, 0) = f_y(1, 0) = 0.$$

We have

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

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 $1/3$.

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

Also

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

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

$$f(1, -2/3) \neq 0 \text{ and } f(1/3, -2/3) \neq 0$$

there are no singular points with y-coordinate $-2/3$.

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
$$f(1, -2/3) \neq 0 \text{ and } f(1/3, -2/3) \neq 0$$

there are no singular points with y-coordinate $-2/3$.

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

Multiplicity

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

Simple, double, ...

Definition 4.13. A point of C of multiplicity 1 is called **non–singular**. A point of multiplicity greater than 1 is called **singular**.

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.

Simple, double, ...

Definition 4.13. A point of C of multiplicity 1 is called **non–singular**. A point of multiplicity greater than 1 is called **singular**.

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.

$$\text{non–singular} = \text{simple}$$

Simple, double, ...

Definition 4.13. A point of C of multiplicity 1 is called **non–singular**. A point of multiplicity greater than 1 is called **singular**.

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.

$$\text{non–singular} = \text{simple}$$

$$\text{singular} \iff \text{multiplicity} > 1$$

Example 4.14. Find the multiplicity of each singular point of the curve with equation

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

Example 4.14. 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. Find the multiplicity of each singular point of the curve with equation

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

Example 4.15. 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 $(1, 0)$.

Example 4.15. 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

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

Example 4.15. 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

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

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

Tangents

Let $p = (x_0, y_0)$ be a point on the curve C of degree d with equation $f = 0$.

Tangents

Let $p = (x_0, y_0)$ be a point on the curve C of degree d with equation $f = 0$.

For $t = 0, \ldots, d$, define the polynomial F_t in two variables α and β as follows.

Tangents

Let $p = (x_0, y_0)$ be a point on the curve C of degree d with equation $f = 0$.

For $t = 0, \ldots, d$, define the polynomial F_t in two variables α and β as follows.

$$F_0(\alpha, \beta) = f(x_0, y_0) \quad \text{and} \tag{4.1}$$

Tangents

Let $p = (x_0, y_0)$ be a point on the curve C of degree d with equation $f = 0$.

For $t = 0, \ldots, d$, define the polynomial F_t in two variables α and β as follows.

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

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

Tangents

Let $p = (x_0, y_0)$ be a point on the curve C of degree d with equation $f = 0$.

For $t = 0, \ldots, d$, define the polynomial F_t in two variables α and β as follows.

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

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

Then F_t is either zero or homogeneous of degree t.

A line l through p with direction ratio $(a : b)$ has parametric form $(x_0 + as, y_0 + bs)$.

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

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

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 $(3/2, 3/2)$.

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.

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.

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 $(1,0)$.

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

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

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 $(i : -1)$.

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

$$l_1 = \{(is+1, s) | s \in k\} \quad \text{and} \quad l_2 = \{(is+1, -s) | s \in k\}.$$

Tangents and Intersection numbers

Let $p = (x_0, y_0)$ be a point on the curve C with equation $f = 0$.

Tangents and Intersection numbers

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 $(x_0 + as, y_0 + bs)$.

Tangents and Intersection numbers

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

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

Tangents and Intersection numbers

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

Tangents and Intersection numbers

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).

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

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

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 $(a : b)$,

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

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,

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

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),

$$I(p, f, l) > r \quad \Longleftrightarrow \quad s^{r+1} | \phi_{(a,b)}(s)$$

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),

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

From Lemma 4.8, there are at most r ratios $(a : b)$ such that $F_r(a, b) = 0$.

From Lemma 4.8, there are at most r ratios $(a : b)$ such that $F_r(a, b) = 0$.

So there are at most r lines through the point p such that $I(p, f, l) > r$:

From Lemma 4.8, there are at most r ratios $(a : b)$ such that $F_r(a, b) = 0$.

So there are at most r lines through the point p such that $I(p, f, l) > r$:

each such line has direction ratio $(a : b)$ where $F_r(a, b) = 0$.

From Lemma 4.8, there are at most r ratios $(a:b)$ such that $F_r(a,b)=0$.

So there are at most r lines through the point p such that $I(p,f,l)>r$:

each such line has direction ratio $(a:b)$ where $F_r(a,b)=0$.

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 at $(0, 0)$

Corollary 4.21. *Let* C *be a curve with equation* $f = 0$ *and assume that* $p = (0, 0)$ *is a point of* C.

Then p *has multiplicity* r *on* C *if and only if the lowest order terms of* f *have degree* r.

Multiplicity at $(0, 0)$

Corollary 4.21. *Let* C *be a curve with equation* $f = 0$ *and assume that* $p = (0, 0)$ *is a point of* C*.*

Then p *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* p *is tangent to* C *at* p *if and only if* l *has a 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.

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).

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

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

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 $3x^2y - y^3$.

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.

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 $3a^2 - b^2 = 0$.

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 $(s, 0)$.

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 $b = \pm\sqrt{3}$.

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 $(s, 0)$.

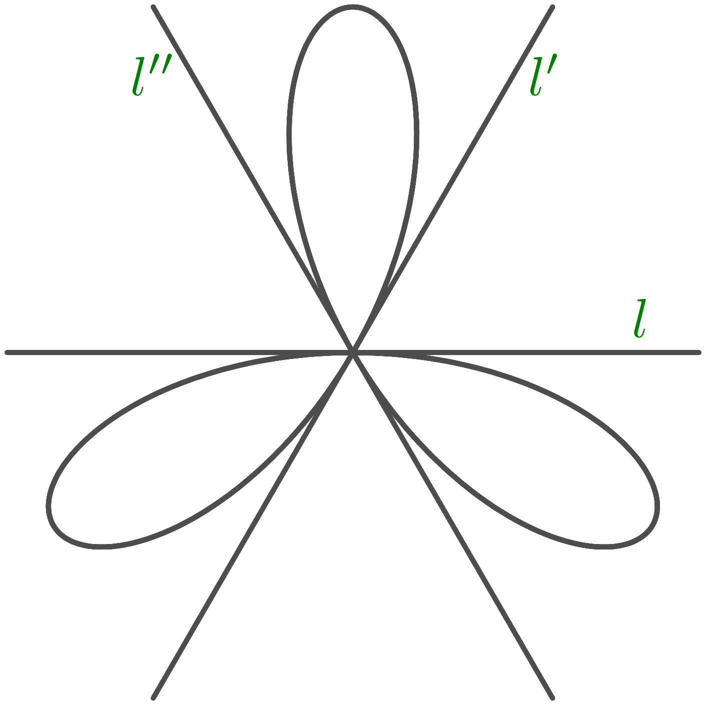
When $3a^2 - b^2 = 0$ we may assume $a = 1$ and so $b = \pm\sqrt{3}$.

In this case we obtain two tangents l' and l'' with parametric forms

$$(s, s\sqrt{3}) \quad \text{and} \quad (s, -s\sqrt{3}),$$

respectively.

The real curve $(x^2 + y^2)^2 + 3x^2y - y^3 = 0$



Ratios

A **ratio**, over k, is an n–tuple

$$(a_1 : \ldots : a_n)$$

of elements of k.

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 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

In $\mathbb{A}_2(k)$ a point is represented by an ordered pair (u, v).

Lines in the affine plane

In $\mathbb{A}_2(k)$ a point is represented by an ordered pair (u, v).

Lines:

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

Lines in the affine plane

In $\mathbb{A}_2(k)$ a point is represented by an ordered pair (u, v).

Lines:

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

Two points of $\mathbb{A}_2(k)$ lie on a unique line.

Lines in the affine plane

In $\mathbb{A}_2(k)$ a point is represented by an ordered pair (u, v).

Lines:

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

Two points of $\mathbb{A}_2(k)$ lie on a unique line.

(x_0, y_0) and (x_1, y_1) lie on the line with parametric form

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

Lines in the affine plane

In $\mathbb{A}_2(k)$ a point is represented by an ordered pair (u, v).

Lines:

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

Two points of $\mathbb{A}_2(k)$ lie on a unique line.

(x_0, y_0) and (x_1, y_1) lie on the line with parametric form

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

Lines may be parallel: two distinct lines are parallel if and only if their direction ratios are equal.

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

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.

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

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**

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

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

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 $(0 : 0 : 0)$.

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.

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.

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 $\mathbb{P}_n(k)$.

The projective plane

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

The projective plane

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 $(u, v) \neq (0, 0)$.

Vector notation

In the projective plane, as in the affine plane

$$(u : v : w) = (\lambda u : \lambda v : \lambda w), \qquad \text{for all non–zero} \qquad \lambda \in k.$$

Vector notation

In the projective plane, as in the affine plane

$$(u : v : w) = (\lambda u : \lambda v : \lambda w), \qquad \text{for all non–zero} \qquad \lambda \in k.$$

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.

Vector notation

In the projective plane, as in the affine plane

$$(u : v : w) = (\lambda u : \lambda v : \lambda w), \qquad \text{for all non–zero} \qquad \lambda \in k.$$

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:

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

Vector notation

In the projective plane, as in the affine plane

$$(u : v : w) = (\lambda u : \lambda v : \lambda w), \qquad \text{for all non–zero} \qquad \lambda \in k.$$

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 $ax + by + c = 0$.

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

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

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

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

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 $ax + by + cz = 0$.

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

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

Two points determine a line

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

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

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

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

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

Two lines determine a point

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

Two lines determine a point

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

Proof. Suppose we have two lines with equations

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

Two lines determine a point

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

Proof. Suppose we have two lines with equations

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

As we have two equations in three unknowns there will be at least one solution.

Two lines determine a point

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

Proof. Suppose we have two lines with equations

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

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.

Two lines determine a point

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

Proof. Suppose we have two lines with equations

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

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.

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

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.

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.

$(x_0 : y_0 : z_0) \in l$ 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.

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.

$(x_0 : y_0 : z_0) \in l$ 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

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

Therefore

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

Therefore

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

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.

Therefore

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

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.

Homogeneous polynomials

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.

Homogeneous polynomials

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* $t \in k$.

Homogeneous polynomials

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* $t \in k$.

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 $(a : b : c) = (u : v : w)$.

Projective curves

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 $\mathbb{P}_2(k)$.

Irreducible components

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

Irreducible components

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

Let f be an irreducible homogeneous polynomial in $k[x, y, z]$.

Then the curve C_f is called an **irreducible** projective curve.

Irreducible components

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

Let f be an irreducible homogeneous polynomial in $k[x,y,z]$.

Then the curve C_f is called an **irreducible** projective curve.

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.

Irreducible components

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

Let f be an irreducible homogeneous polynomial in $k[x, y, z]$.

Then the curve C_f is called an **irreducible** projective curve.

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

$$f(x, y) = F(x, y, 1).$$

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

$$f(x, y) = F(x, y, 1).$$

f is a polynomial of degree at most d in $k[x, y]$.

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

$$f(x, y) = F(x, y, 1).$$

f is a polynomial of degree at most d in $k[x, y]$.

If $F \neq az^d$ then f is non–constant and if $z \nmid F$ then f has degree d.

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

$$f(x, y) = F(x, y, 1).$$

f is a polynomial of degree at most d in $k[x, y]$.

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 $y^3 - x^2 z = 0$ has dehomogenization the affine curve with equation $y^3 - x^2 = 0$.

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 $\mathbb{R}^3$.

Example 5.11.

1. The projective curve with equation $y^3 - x^2 z = 0$ 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 $\mathbb{R}^3$.

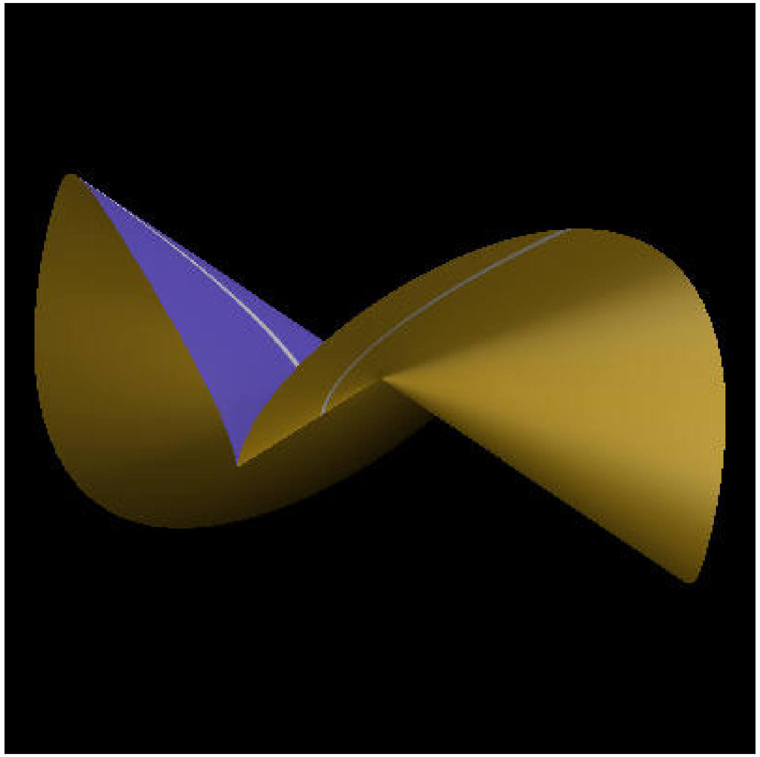
   We obtain the real affine curve by intersecting the projective curve with the plane $z = 1$:

Example 5.11.

1. The projective curve with equation $y^3 - x^2 z = 0$ 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 $\mathbb{R}^3$.

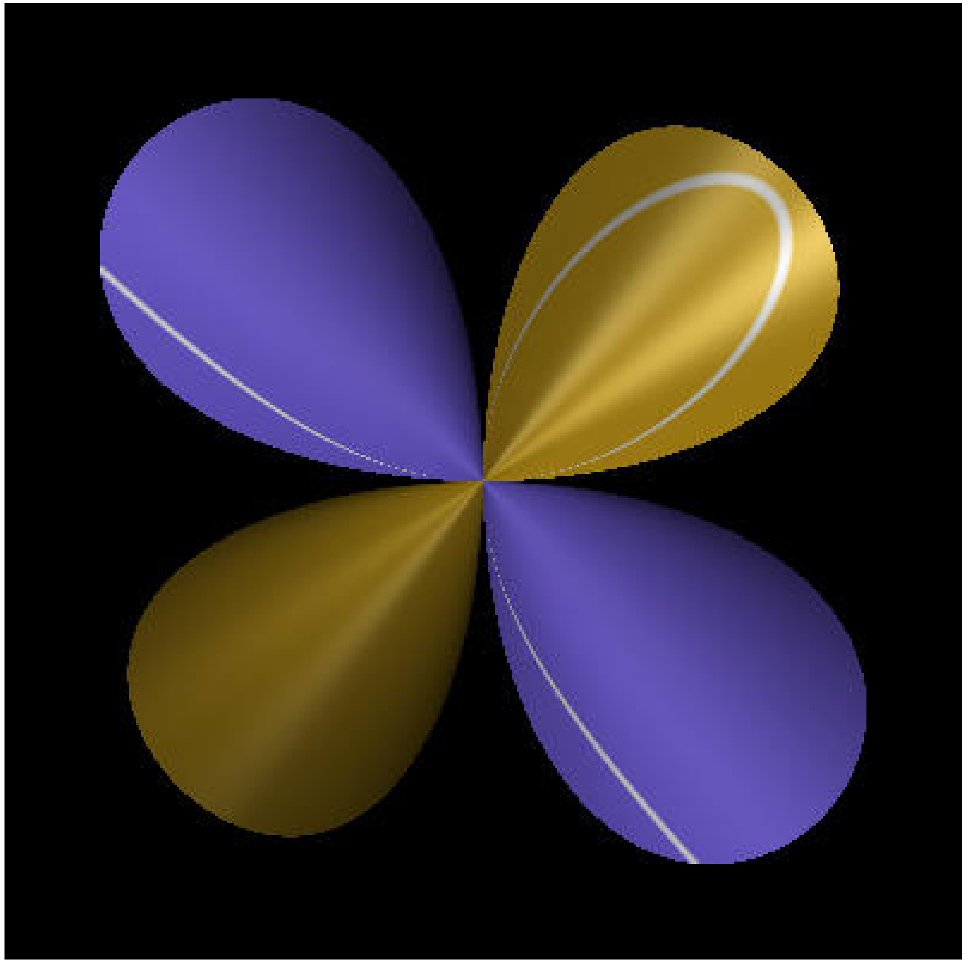
   We obtain the real affine curve by intersecting the projective curve with the plane $z = 1$:



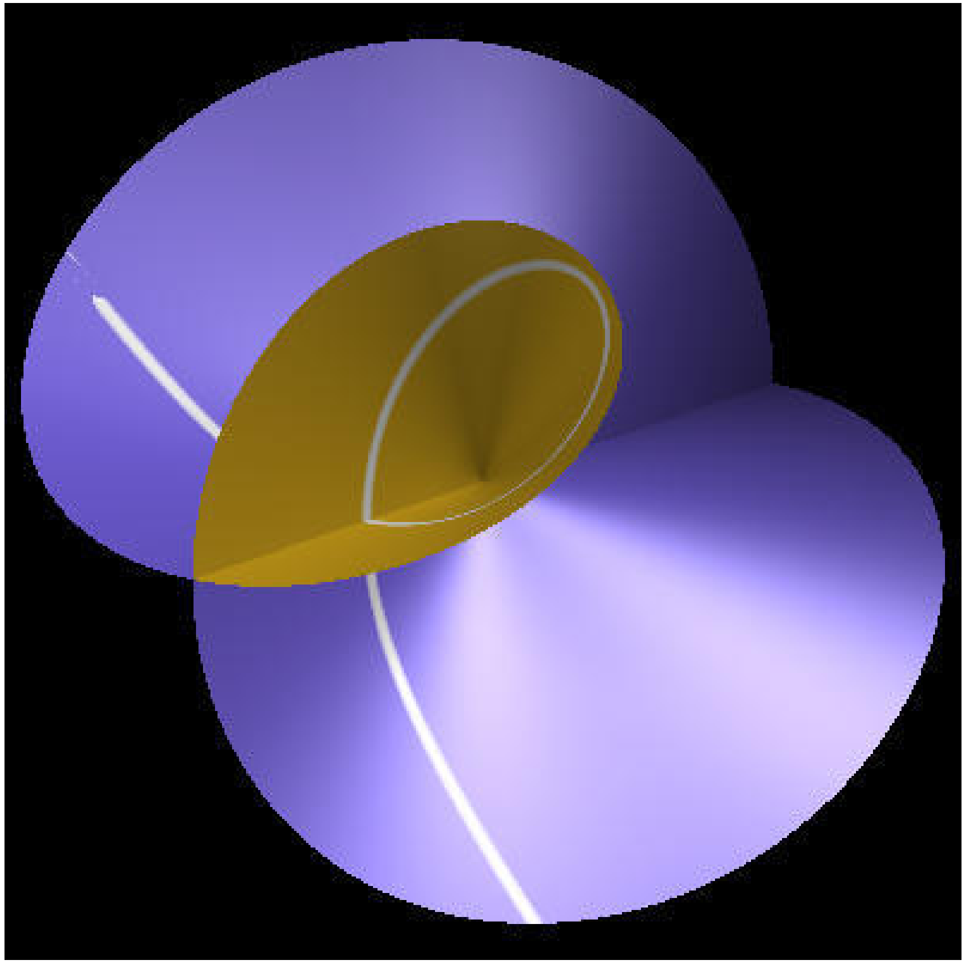
2. The projective curve with polynomial $x^3 + y^3 - 3xyz$ has dehomogenization the affine curve with polynomial $x^3 + y^3 - 3xy$.

2. The projective curve with polynomial $x^3 + y^3 - 3xyz$ has dehomogenization the affine curve with polynomial $x^3 + y^3 - 3xy$.

   In this 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 next drawing is first rotated so that the z axis points out to the left and then its tilted towards you.



The line at infinity

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

The line at infinity

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 $z = 1$).

The line at infinity

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

The line at infinity

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 $\mathbb{A}_2(k)$.

The line at infinity

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 of all the new points we added to $\mathbb{A}_2(k)$ to form $\mathbb{P}_2(k)$.

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.

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

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.

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.

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).

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

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.

Dehomogenisation with respect to x and y

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

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

Dehomogenisation with respect to x and y

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 $y = 1$:

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

Dehomogenisation with respect to x and y

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 $y = 1$:

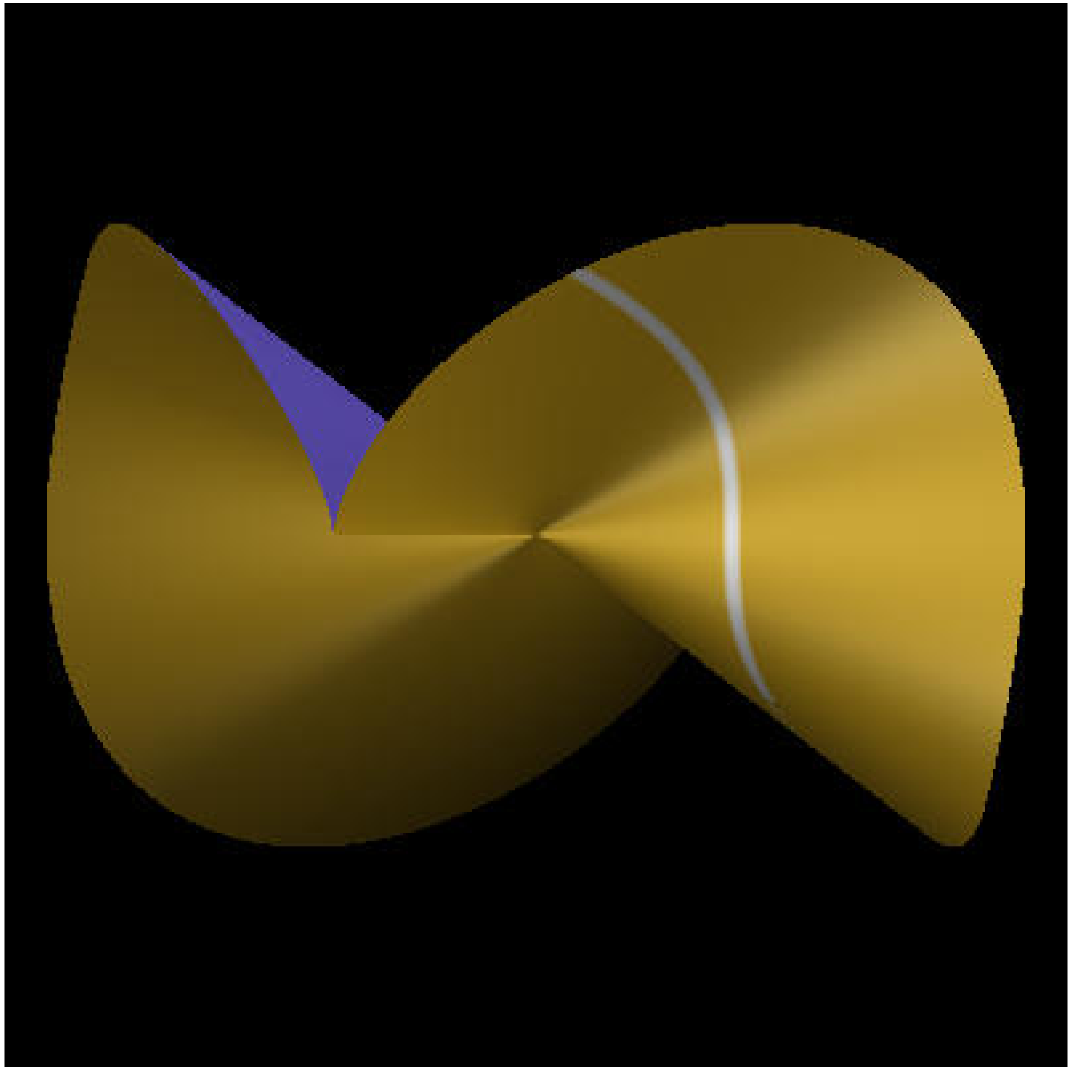
$$h(x, z) = F(x, 1, z) \text{ and } C_h.$$

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

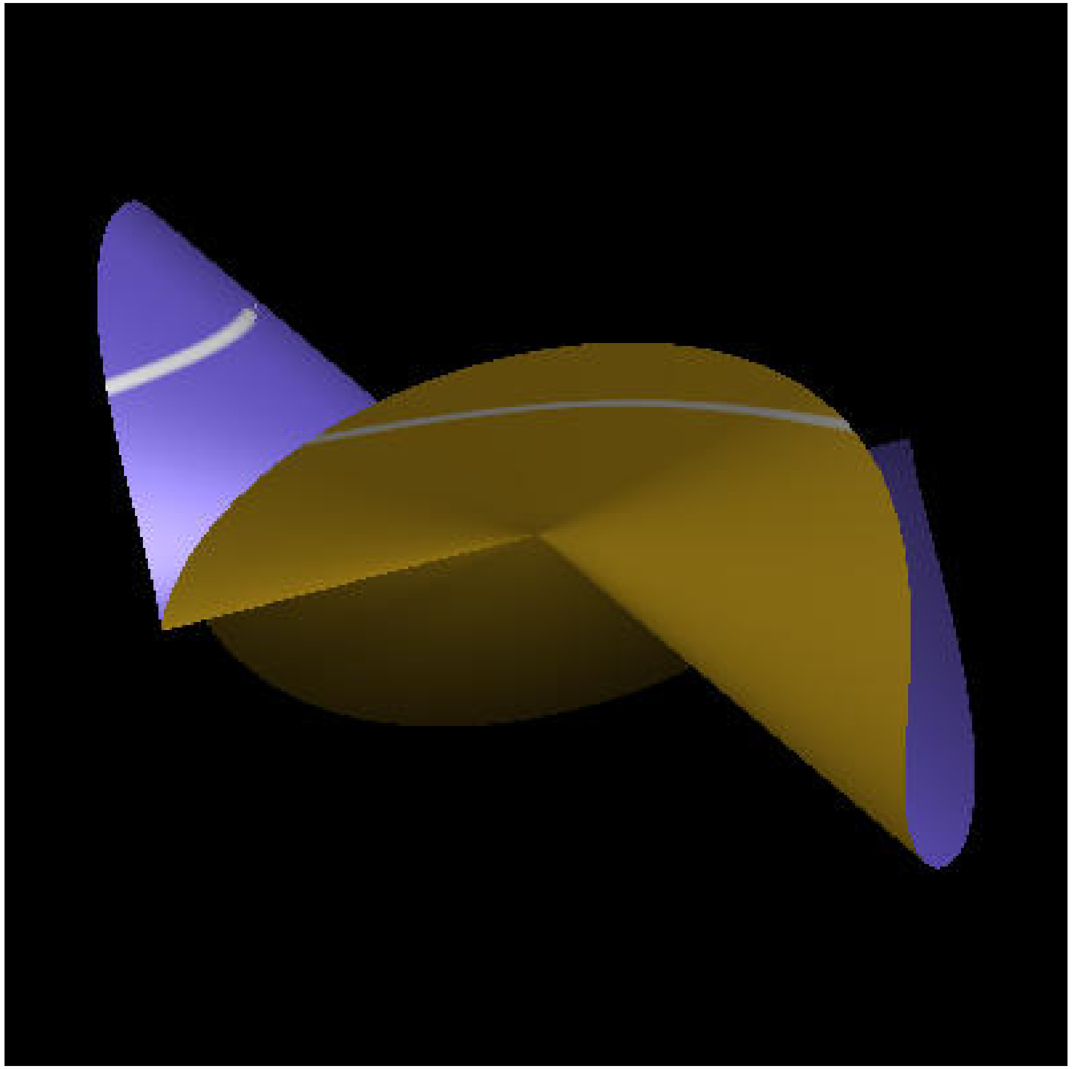
Example 5.12. The projective curve $y^3 - x^2 z = 0$ has dehomogenizations $y^3 - z = 0$ and $1 - x^2 z = 0$ with respect to $x = 1$ and $y = 1$ respectively.

Example 5.12. The projective curve $y^3 - x^2 z = 0$ has dehomogenizations $y^3 - z = 0$ and $1 - x^2 z = 0$ with respect to $x = 1$ and $y = 1$ respectively.

These dehomogenizations in the case $\mathbb{R} = k$ are, with respect to $x = 1$,



and with respect to $y = 1$,



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 degree d.

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 degree d.

Formally

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

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 degree d.

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

Caution Dehomogenization is not always the reverse of homogenization.

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 degree d.

Formally

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

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 $x + y + z = 0$.

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

The line $ax+by+c=0$ has homogenization the line $ax+by+cz=0$.

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

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 $au+bv=0$.

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

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 $(-b : a : 0)$.

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

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 $(-b:a:0)$.

The direction ratio of this line is $(-b:a:0)$.

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

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 $(-b:a:0)$.

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.

The homogenization of affine conics

Example 5.14.

1. The affine parabola $x - y^2 = 0$ has homogenization $xz - y^2 = 0$.

   This curve meets $z = 0$ when $y^2 = 0$: at the unique point $(1 : 0 : 0)$.

The homogenization of affine conics

Example 5.14.

1. The affine parabola $x - y^2 = 0$ has homogenization $xz - y^2 = 0$.

   This curve meets $z = 0$ when $y^2 = 0$: at the unique point $(1 : 0 : 0)$.

2. The affine circle $x^2 + y^2 - 1 = 0$ has homogenization $x^2 + y^2 - z^2 = 0$.

   This curve meets $z = 0$ where $x^2 + y^2 = 0$: at points $(1 : i : 0)$ and $(1 : -i : 0)$.

The homogenization of affine conics

Example 5.14.

1. The affine parabola $x - y^2 = 0$ has homogenization $xz - y^2 = 0$.

   This curve meets $z = 0$ when $y^2 = 0$: at the unique point $(1 : 0 : 0)$.

2. The affine circle $x^2 + y^2 - 1 = 0$ has homogenization $x^2 + y^2 - z^2 = 0$.

   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 $z = 0$. [$(0 : 0 : 0)$ is not a point of $\mathbb{P}_2(k)$.]

The homogenization of affine conics

Example 5.14.

1. The affine parabola $x - y^2 = 0$ has homogenization $xz - y^2 = 0$.

   This curve meets $z = 0$ when $y^2 = 0$: at the unique point $(1 : 0 : 0)$.

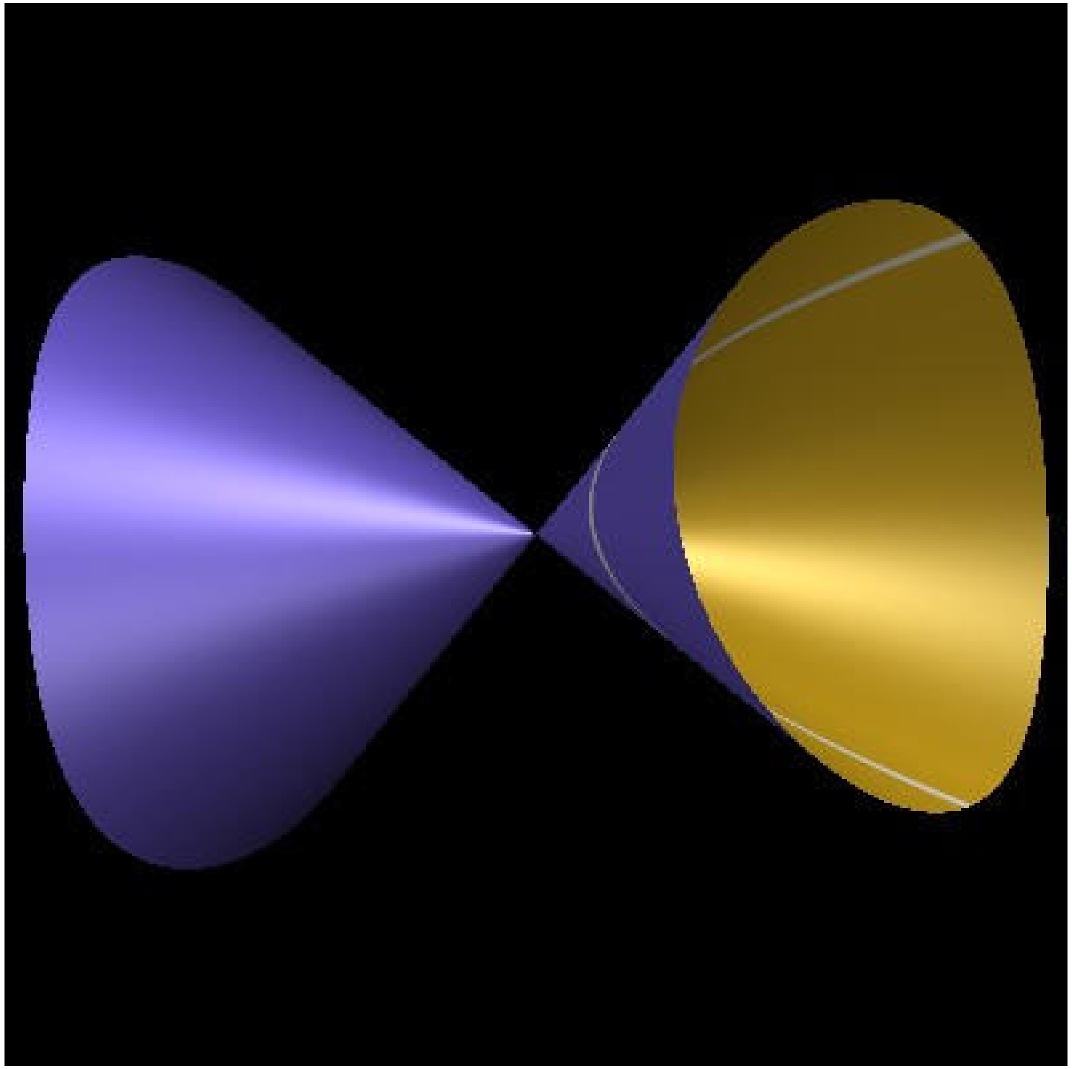
2. The affine circle $x^2 + y^2 - 1 = 0$ has homogenization $x^2 + y^2 - z^2 = 0$.

   This curve meets $z = 0$ where $x^2 + y^2 = 0$: at points $(1 : i : 0)$ and $(1 : -i : 0)$.

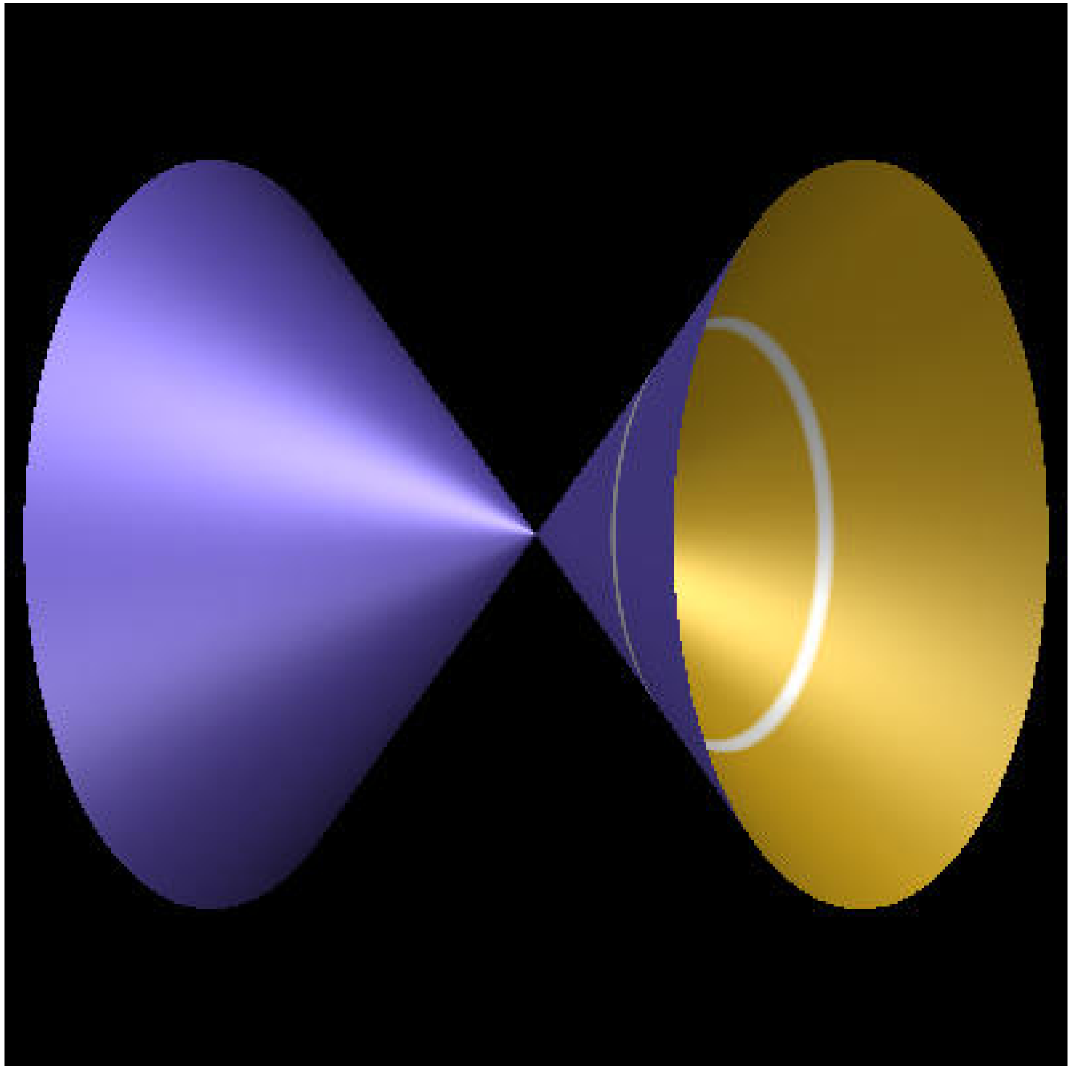
   The real projective curve does not meet $z = 0$. [$(0 : 0 : 0)$ is not a point of $\mathbb{P}_2(k)$.]

3. The affine hyperbola $x^2 - y^2 - 1 = 0$ has homogenization $x^2 - y^2 - z^2 = 0$.

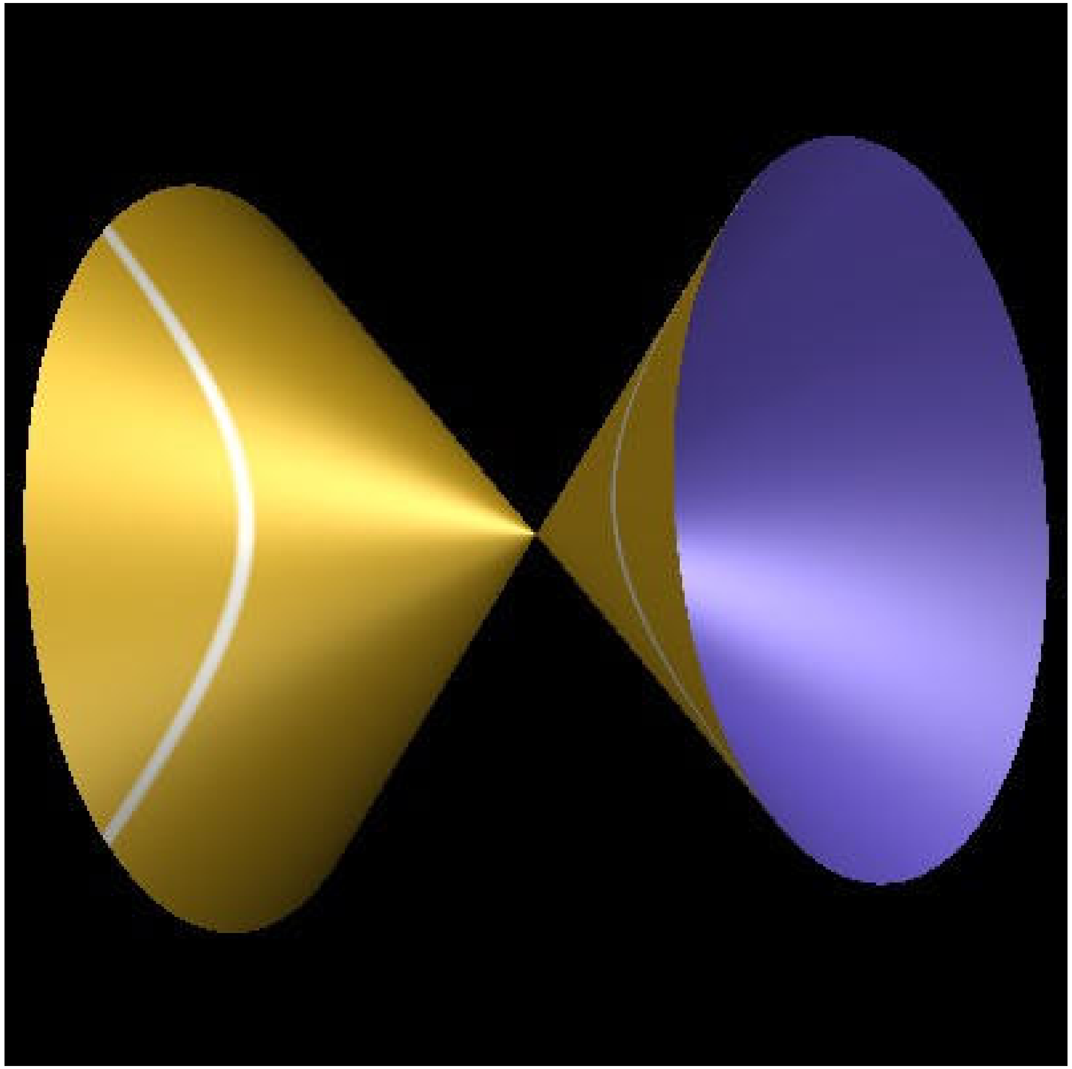
   This curve meets $z = 0$ where $x^2 - y^2 = 0$: at points $(1 : 1 : 0)$ and $(1 : -1 : 0)$.



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



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



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 $f = 0$.

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 $p = (as_0 + ut_0 : bs_0 + vt_0 : cs_0 + wt_0)$ lies on l and C if and only if

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

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 $p = (as_0 + ut_0 : bs_0 + vt_0 : cs_0 + wt_0)$ lies on l and C if and only if

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

Definition 5.15. We call the polynomial

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

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

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 $p = (as_0 + ut_0 : bs_0 + vt_0 : cs_0 + wt_0)$ lies on l and C if and only if

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

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 $(t_0 s - s_0 t)^r | \phi(s, t)$.

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 $p = (as_0 + ut_0 : bs_0 + vt_0 : cs_0 + wt_0)$ lies on l and C if and only if

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

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 $(t_0 s - s_0 t)^r | \phi(s,t)$.

Intersection number is independant of choice of parametric form for l.

Affine and projective intersection numbers

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 $z = 1$.

Number of intersections: line and curve

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** ∞.

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 $l \not\subseteq C$. Then

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

Number of intersections: line and curve

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** ∞.

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 $l \not\subseteq C$. Then

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

Proof. If $l \not\subseteq C$ then $\phi(s, t)$ is not the zero polynomial and so is homogeneous of degree d.

Number of intersections: line and curve

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** ∞.

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 $l \not\subseteq C$. Then

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

Proof. If $l \not\subseteq C$ 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 $i + j + k = r$

$$\frac{\partial f}{\partial x^i y^j z^k}(a, b, c) \neq 0.$$

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

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 $I(p, f, l) > r$.

Tangents

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 $I(p, f, l) > r$.

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 $y = 1$.

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

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 $y^3 - xz$ at the points $(1:0:0)$ and $(0:0:1)$.

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 $y^3 - xz$ 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.

Tangent to a simple point

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*

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

Tangent to a simple point

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*

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

Example 5.26.

Proof of Theorem 5.21

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 of Theorem 5.21

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.

Corollary 5.28.

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

Proof of Theorem 5.21

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.

Corollary 5.28.

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

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 of Theorem 5.21 continued

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.

Proof of Theorem 5.21 continued

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

$$F_x(u, v, 1) = F_y(u, v, 1) = F_y(u, v, 1) = 0$$

Proof of Theorem 5.21 continued

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

$$F_x(u, v, 1) = F_y(u, v, 1) = F_y(u, v, 1) = 0$$

$$\iff F(u, v, 1) = F_x(u, v, 1) = F_y(u, v, 1) = 0 \quad \text{(using Euler's Theorem)}$$

Proof of Theorem 5.21 continued

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

$$F_x(u, v, 1) = F_y(u, v, 1) = F_y(u, v, 1) = 0$$

$$\Longleftrightarrow \; F(u, v, 1) = F_x(u, v, 1) = F_y(u, v, 1) = 0 \quad \text{(using Euler's Theorem)}$$

$$\Longleftrightarrow \; f(u, v) = f_x(u, v) = f_y(u, v) = 0 \quad \text{(using Lemma 5.27)}$$

Proof of Theorem 5.21 continued

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

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

Proof of Theorem 5.21 continued

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.

Asymptotes

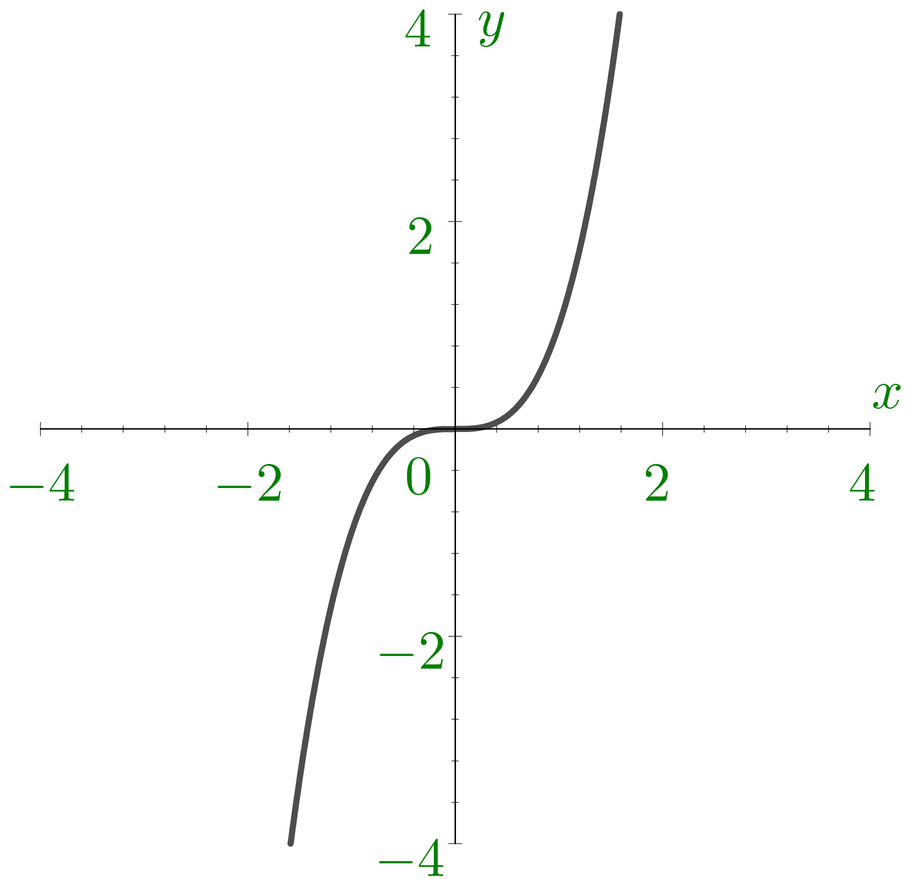
Definition 5.30. Let C_f be an affine curve and let F be the homogenization of f.

Let L be a projective line tangent to C_F at some point p on the line $z = 0$.

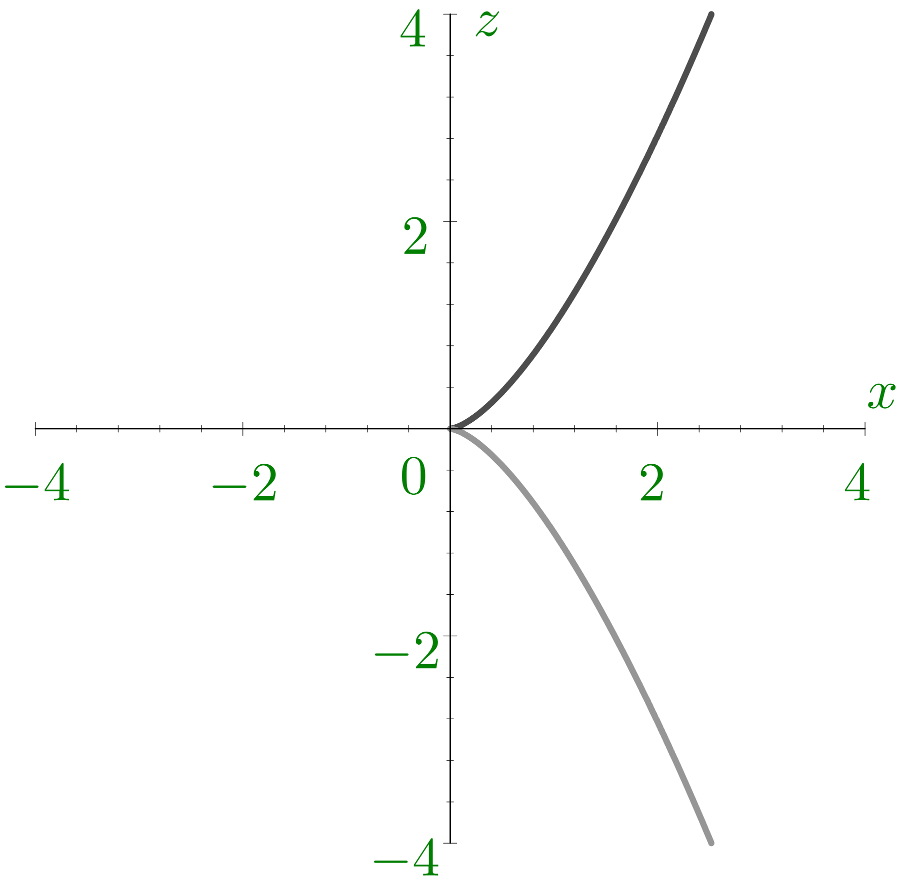
If L is not itself the line $z = 0$ then the dehomogenization l of L is called an **asymptote** to C_f.

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

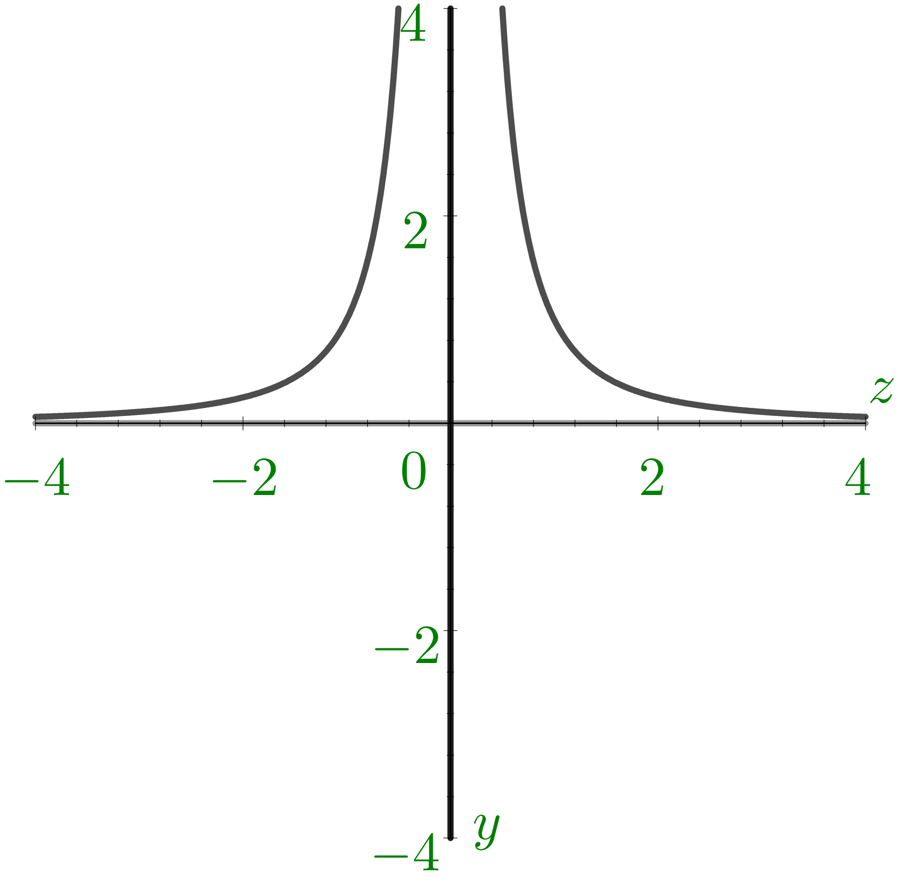
The real curve with equation $x^3 - y = 0$



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



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



Bézout's Theorem

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

Bézout's Theorem

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

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.*

Bézout's Theorem

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

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.*

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 $I(p, F, l) \geq 3$.

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.

The Hessian

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

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

The Hessian

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 $3(d-2)$.

The affine version of the Hessian

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

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

The affine version of the Hessian

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

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

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

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

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

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

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.

Inflexions and the Hessian

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. $H_F(u, v, w) = 0$.

Inflexions and the Hessian

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 $q \in C_f$.

Inflexions and the Hessian

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 $I(q, f, l) \geq 3$.

Inflexions and the Hessian

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

$$af_x + bf_y = 0.$$

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 $b = f_x$.

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

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

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 $q \in C_f$ 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

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

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

$$H_F(u,v,1) = (d-1)^2 \begin{vmatrix} f_{xx} & f_{xy} & f_x \\ f_{yx} & f_{yy} & f_y \\ f_x & f_y & 0 \end{vmatrix}$$

$$= (d-1)^2[-f_x^2 f_{yy} + 2f_x f_y f_{xy} - f_y^2 f_{xx}]$$

Thus

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

Thus

$$H_F(u,v,1) = (d-1)^2 \begin{vmatrix} f_{xx} & f_{xy} & f_x \\ f_{yx} & f_{yy} & f_y \\ f_x & f_y & 0 \end{vmatrix}$$

$$= (d-1)^2[-f_x^2 f_{yy} + 2 f_x f_y f_{xy} - f_y^2 f_{xx}]$$

$$= (d-1)^2[-b^2 f_{yy} - 2ab f_{xy} - a^2 f_{xx}].$$

Hence

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

Thus

$$H_F(u,v,1) = (d-1)^2 \begin{vmatrix} f_{xx} & f_{xy} & f_x \\ f_{yx} & f_{yy} & f_y \\ f_x & f_y & 0 \end{vmatrix}$$

$$= (d-1)^2[-f_x^2 f_{yy} + 2 f_x f_y f_{xy} - f_y^2 f_{xx}]$$

$$= (d-1)^2[-b^2 f_{yy} - 2ab f_{xy} - a^2 f_{xx}].$$

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 $H_F(u,v,1) = 0$.

Thus

$$H_F(u,v,1) = (d-1)^2 \begin{vmatrix} f_{xx} & f_{xy} & f_x \\ f_{yx} & f_{yy} & f_y \\ f_x & f_y & 0 \end{vmatrix}$$

$$= (d-1)^2[-f_x^2 f_{yy} + 2 f_x f_y f_{xy} - f_y^2 f_{xx}]$$

$$= (d-1)^2[-b^2 f_{yy} - 2ab f_{xy} - a^2 f_{xx}].$$

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 $F = x^3 + y^3 - 3xyz$.

Cubics and lines

A curve of degree 3 is a **cubic**.

Cubics and lines

A curve of degree 3 is a **cubic**.

A non–singular cubic in $\mathbb{P}_2(k)$ (where k is algebraically closed) has exactly nine inflexions.

Cubics and lines

A curve of degree 3 is a **cubic**.

A non–singular cubic in $\mathbb{P}_2(k)$ (where k is algebraically closed) has exactly nine inflexions.

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.*

Cubics and lines

A curve of degree 3 is a **cubic**.

A non–singular cubic in $\mathbb{P}_2(k)$ (where k is algebraically closed) has exactly nine inflexions.

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

The line through A and B is AB.

$\mathcal{C}_F$ is a non–singular projective cubic

O is an inflexion of $\mathcal{C}$.

The group law on the cubic

The line through A and B is AB.

$\mathcal{C}_F$ is a non–singular projective cubic

O is 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).

The group law on the cubic

The line through A and B is AB.

$\mathcal{C}_F$ is a non–singular projective cubic

O is 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).

$\overline{O} = O$, because O is an inflexion.

The group law on the cubic

The line through A and B is AB.

$\mathcal{C}_F$ is a non–singular projective cubic

O is 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).

$\overline{O} = O$, because O is an inflexion.

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 $P + Q = \overline{X}$.

The group law on the cubic

The line through A and B is AB.

$\mathcal{C}_F$ is a non–singular projective cubic

O is 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).

$\overline{O} = O$, because O is an inflexion.

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 of Theorem 8.4

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 $\mathcal{C}$.

Proof of Theorem 8.4

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.

Proof of Theorem 8.4

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 $P + O = P = O + P$.

Proof of Theorem 8.4

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 $\mathcal{C}$.

Proof of Theorem 8.4

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.

Proof of Theorem 8.4

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 $P+O=P$.

Proof of Theorem 8.4

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 $\mathcal{C}$.

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 $\overline{P}$.

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 $P + \overline{P} = \overline{O} = O$.

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 $\overline{P}$.

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.

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. $F = x^3 + y^3 - z^3$.

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

Example 8.5. $F = x^3 + y^3 - z^3$.

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

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

Example 8.5. $F = x^3 + y^3 - z^3$.

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

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

$$F_{xx} = 6x,\ F_{yy} = 6y,\ F_{zz} = -6z \text{ and } F_{xy} = F_{xz} = F_{yz} = 0.$$
$$H_F = \begin{vmatrix} 6x & 0 & 0 \\ 0 & 6y & 0 \\ 0 & 0 & -6z \end{vmatrix} = -6^3xyz.$$

Example 8.5. $F = x^3 + y^3 - z^3$.

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

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

$$F_{xx} = 6x,\ F_{yy} = 6y,\ F_{zz} = -6z \text{ and } F_{xy} = F_{xz} = F_{yz} = 0.$$
$$H_F = \begin{vmatrix} 6x & 0 & 0 \\ 0 & 6y & 0 \\ 0 & 0 & -6z \end{vmatrix} = -6^3 xyz.$$

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

When $x = 0$

In this case $F(0, y, z) = y^3 - z^3 = 0$.

When $x = 0$

In this case $F(0, y, z) = y^3 - z^3 = 0$.

Assume $y = 1$ and find z by solving $1 - z^3 = 0$.

$$z = 1,\ \omega \text{ or } \omega^2,$$

where $\omega^3 = 1$ and $\omega \neq 1$.

When $x = 0$

In this case $F(0, y, z) = y^3 - z^3 = 0$.

Assume $y = 1$ and find z by solving $1 - z^3 = 0$.

$$z = 1, \omega \text{ or } \omega^2,$$

where $\omega^3 = 1$ and $\omega \neq 1$.

Points of inflexion with $x = 0$:

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

When $y = 0$

In this case $F(x, 0, z) = x^3 - z^3 = 0$.

When $y = 0$

In this case $F(x, 0, z) = x^3 - z^3 = 0$.

Assume $z = 1$ and find x by solving $x^3 - 1 = 0$.

$$x = 1,\, \omega, \;\; \text{or } \omega^2,$$

where $\omega^3 = 1$ and $\omega \neq 1$.

When $y = 0$

In this case $F(x, 0, z) = x^3 - z^3 = 0$.

Assume $z = 1$ and find x by solving $x^3 - 1 = 0$.

$$x = 1, \omega, \text{ or } \omega^2,$$

where $\omega^3 = 1$ and $\omega \neq 1$.

Points of inflexion with $y = 0$:

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

When $z = 0$

In this case $F(x, y, 0) = x^3 + y^3 = 0$.

When $z = 0$

In this case $F(x, y, 0) = x^3 + y^3 = 0$.

Assume $x = 1$ and find y by solving $1 + y^3 = 0$.

$$y = -1,\ -\omega \text{ or } -\omega^2,$$

where $\omega^3 = 1$ and $\omega \neq 1$.

When $z = 0$

In this case $F(x, y, 0) = x^3 + y^3 = 0$.

Assume $x = 1$ and find y by solving $1 + y^3 = 0$.

$$y = -1,\ -\omega \text{ or } -\omega^2,$$

where $\omega^3 = 1$ and $\omega \neq 1$.

Points of inflexion with $z = 0$:

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

There are a total of nine inflexions as expected.

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 $z = 1$.

There are a total of nine inflexions as expected.

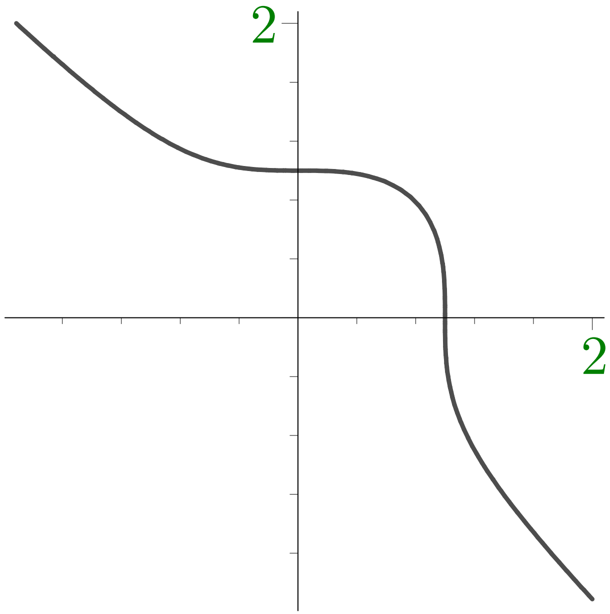
The inflexions on the real curve at $(0:1:1)$ and $(1:0:1)$ can be shown by dehomogenizing with respect to $z = 1$.

This gives the affine curve $x^3 + y^3 - 1 = 0$ with inflexions at $(0, 1)$ and $(1, 0)$

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 $(1, 0)$



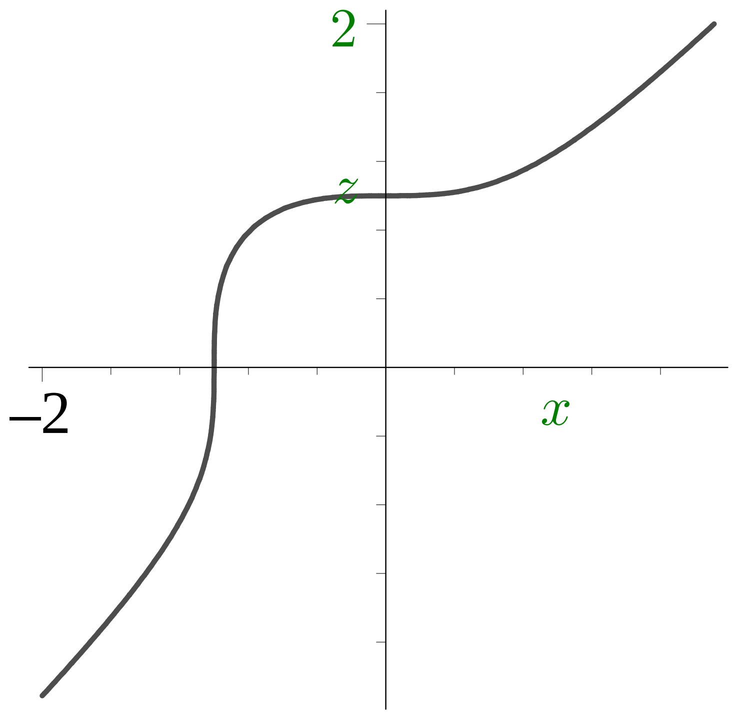
The inflexions at $(0:1:1)$ and $(-1:1:0) = (1:-1:0)$ can be seen by dehomogenizing with respect to $y = 1$.

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 $(-1, 0)$.

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 $(-1,0)$.



The group law on $\mathcal{C}$ with base point $O = (0 : 1 : 1)$

$P = (1 : 0 : \omega)$ and $Q = (1 : -\omega^2 : 0)$.

We shall compute $P + Q$.

The group law on $\mathcal{C}$ with base point $O = (0 : 1 : 1)$

$P = (1 : 0 : \omega)$ and $Q = (1 : -\omega^2 : 0)$.

We shall compute $P + Q$.

The line PQ has parametric form $(s + t : -\omega^2 t : \omega s)$, for $s, t \in k$.

The group law on $\mathcal{C}$ with base point $O = (0 : 1 : 1)$

$P = (1 : 0 : \omega)$ and $Q = (1 : -\omega^2 : 0)$.

We shall compute $P + Q$.

The line PQ has parametric form $(s + t : -\omega^2 t : \omega s)$, for $s, t \in k$.

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

The group law on $\mathcal{C}$ with base point $O = (0 : 1 : 1)$

$P = (1 : 0 : \omega)$ and $Q = (1 : -\omega^2 : 0)$.

We shall compute $P + Q$.

The line PQ has parametric form $(s + t : -\omega^2 t : \omega s)$, for $s, t \in k$.

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

Thus $\phi(s,t) = 0$ if $s = 0$, $t = 0$ or $s + t = 0$.

The group law on $\mathcal{C}$ with base point $O = (0 : 1 : 1)$

$P = (1 : 0 : \omega)$ and $Q = (1 : -\omega^2 : 0)$.

We shall compute $P + Q$.

The line PQ has parametric form $(s + t : -\omega^2 t : \omega s)$, for $s, t \in k$.

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

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.

The third point of intersection of PQ with $\mathcal{C}$ is X, corresponding to $s + t = 0$ so

$$X = (0 : \omega^2 : \omega) = (0 : 1 : \omega^2).$$

The third point of intersection of PQ with $\mathcal{C}$ is X, corresponding to $s+t=0$ so

$$X = (0 : \omega^2 : \omega) = (0 : 1 : \omega^2).$$

As O and X both have x–coordinate 0 it follows that the line OX is $x = 0$.

The third point of intersection of PQ with $\mathcal{C}$ is X, corresponding to $s + t = 0$ so

$$X = (0 : \omega^2 : \omega) = (0 : 1 : \omega^2).$$

As O and X both have x–coordinate 0 it follows that the line OX is $x = 0$.

This line meets $\mathcal{C}$ at O, X and $\overline{X} = (0 : 1 : \omega)$. Hence

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