Rational parametrization of algebraic curves
(An appetizer)

Veronika Pillwein

Notation

- K is an algebraically closed field, $\mathbb{Q} \subseteq K$
- $K(t)$ denotes the field of rational functions over K
- $K[x_1, \ldots, x_n]$ denotes the ring of polynomials in the indeterminates $x_1, \ldots, x_n$

Notation

- K is an algebraically closed field, $\mathbb{Q} \subseteq K$
- $K(t)$ denotes the field of rational functions over K
- $K[x_1, \ldots, x_n]$ denotes the ring of polynomials in the indeterminates $x_1, \ldots, x_n$
- $\mathbb{A}^n(K) = \{(a_1, \ldots, a_n) \mid a_k \in K\} = \mathbb{A}^n$ the n-dimensional affine space over K

Notation

- K is an algebraically closed field, $\mathbb{Q} \subseteq K$
- $K(t)$ denotes the field of rational functions over K
- $K[x_1, \ldots, x_n]$ denotes the ring of polynomials in the indeterminates $x_1, \ldots, x_n$
- $\mathbb{A}^n(K) = \{(a_1, \ldots, a_n) \mid a_k \in K\} = \mathbb{A}^n$ the n-dimensional affine space over K
- $\mathcal{C} = \{(a, b) \in \mathbb{A}^2 \mid f(a, b) = 0\}$ is the affine algebraic curve with defining polynomial $f \in K[x, y]$;
  $\mathcal{C}$ is irreducible, iff it has an irreducible defining polynomial

Examples

$$
\begin{aligned}
f_1(x, y) &= x^3 + x^2 - y^2 \\
f_2(x, y) &= y^2 - x^3 + x \\
f_3(x, y) &= (x^2 + 4y + y^2)^2 - 16(x^2 + y^2) \\
f_4(x, y) &= 2x^4 - 3x^2y + y^2 - 2y^3 + y^4
\end{aligned}
$$

Examples

$$
\begin{aligned}
f_1(x,y) &= x^3 + x^2 - y^2\\
f_2(x,y) &= y^2 - x^3 + x\\
f_3(x,y) &= (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)\\
f_4(x,y) &= 2x^4 - 3x^2y + y^2 - 2y^3 + y^4
\end{aligned}
$$

Question: Is this a good representation for an algebraic curve?

Examples

$$f_1(x,y) = x^3 + x^2 - y^2$$
$$f_2(x,y) = y^2 - x^3 + x$$
$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$
$$f_4(x,y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$$

Answer: Depends on what we want to do!

Examples

$$f_1(x,y) = x^3 + x^2 - y^2$$
$$f_2(x,y) = y^2 - x^3 + x$$
$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$
$$f_4(x,y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$$

Question: Is $P = (-1, 1)$ a point on the curve $\mathcal{C}_i$ defined by f_i?

Examples

$$f_1(x, y) = x^3 + x^2 - y^2 \qquad f_1(-1, 1) = -1$$

$$f_2(x, y) = y^2 - x^3 + x$$

$$f_3(x, y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$

$$f_4(x, y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$$

Question: Is $P = (-1, 1)$ a point on the curve $\mathcal{C}_i$ defined by f_i?

Examples

$$f_1(x,y) = x^3 + x^2 - y^2 \qquad f_1(-1,1) = -1$$
$$f_2(x,y) = y^2 - x^3 + x \qquad f_2(-1,1) = 1$$
$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$
$$f_4(x,y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$$

Question: Is $P = (-1,1)$ a point on the curve $\mathcal{C}_i$ defined by f_i?

Examples

$$f_1(x,y) = x^3 + x^2 - y^2 \qquad f_1(-1,1) = -1$$

$$f_2(x,y) = y^2 - x^3 + x \qquad f_2(-1,1) = 1$$

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2) \qquad f_3(-1,1) = 0$$

$$f_4(x,y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$$

Question: Is $P = (-1,1)$ a point on the curve $\mathcal{C}_i$ defined by f_i?

Examples

$$f_1(x,y) = x^3 + x^2 - y^2 \qquad f_1(-1,1) = -1$$

$$f_2(x,y) = y^2 - x^3 + x \qquad f_2(-1,1) = 1$$

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2) \qquad f_3(-1,1) = 0$$

$$f_4(x,y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$$

Question: Is $P = (-1,1)$ a point on the curve $\mathcal{C}_i$ defined by f_i?

Examples

$$f_1(x,y) = x^3 + x^2 - y^2 \qquad f_1(-1,1) = -1$$

$$f_2(x,y) = y^2 - x^3 + x \qquad f_2(-1,1) = 1$$

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2) \qquad f_3(-1,1) = 0$$

$$f_4(x,y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 \qquad f_4(-1,1) = -1$$

Question: Is $P = (-1,1)$ a point on the curve $\mathcal{C}_i$ defined by f_i?

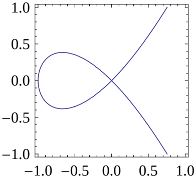
Examples

$$f_1(x,y) = x^3 + x^2 - y^2$$
$$f_2(x,y) = y^2 - x^3 + x$$
$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$
$$f_4(x,y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$$

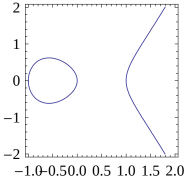
Question: Can we generate arbitrary many real points on $\mathcal{C}_i$?

Examples

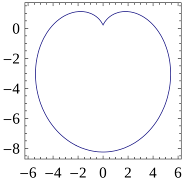
$f_1(x, y)$



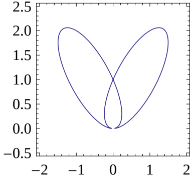
$f_2(x, y)$



$f_3(x, y)$



$f_4(x, y)$



Parametrization

Instead of the implicit representation $f(x, y) = 0$, we seek for a parametrization

$$t \mapsto (r_1(t), r_2(t)) \quad \text{such that} \quad f(r_1(t), r_2(t)) = 0, \quad \forall\, t$$

Rational Parametrization

Instead of the implicit representation $f(x, y) = 0$, we seek for a parametrization

$$t \mapsto (r_1(t), r_2(t)) \quad \text{such that} \quad f(r_1(t), r_2(t)) = 0, \quad \forall\, t$$

- $r_1, r_2 \in K(t)$
- for almost all $t_0 \in K$, $(r_1(t_0), r_2(t_0))$ is a point on $\mathcal{C}$
- for almost all (x_0, y_0) on $\mathcal{C}$ there is a $t_0 \in K$ sucht that $(x_0, y_0) = (r_1(t_0), r_2(t_0))$

Rational Parametrization

Instead of the implicit representation $f(x, y) = 0$, we seek for a parametrization

$$t \mapsto (r_1(t), r_2(t)) \quad \text{such that} \quad f(r_1(t), r_2(t)) = 0, \quad \forall\, t$$

- $r_1, r_2 \in K(t)$
- for almost all $t_0 \in K$, $(r_1(t_0), r_2(t_0))$ is a point on $\mathcal{C}$
- for almost all (x_0, y_0) on $\mathcal{C}$ there is a $t_0 \in K$ sucht that $(x_0, y_0) = (r_1(t_0), r_2(t_0))$

Questions:

Rational Parametrization

Instead of the implicit representation $f(x,y)=0$, we seek for a parametrization

$$t \mapsto (r_1(t), r_2(t)) \quad \text{such that} \quad f(r_1(t), r_2(t)) = 0, \quad \forall\, t$$

- $r_1, r_2 \in K(t)$
- for almost all $t_0 \in K$, $(r_1(t_0), r_2(t_0))$ is a point on $\mathcal{C}$
- for almost all (x_0, y_0) on $\mathcal{C}$ there is a $t_0 \in K$ sucht that $(x_0, y_0) = (r_1(t_0), r_2(t_0))$

Questions:

- When can we rationally parametrize a given curve?

Rational Parametrization

Instead of the implicit representation $f(x,y)=0$, we seek for a parametrization

$$t \mapsto (r_1(t), r_2(t)) \quad \text{such that} \quad f(r_1(t), r_2(t)) = 0, \quad \forall\, t$$

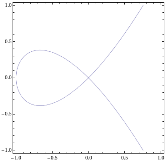
- $r_1, r_2 \in K(t)$
- for almost all $t_0 \in K$, $(r_1(t_0), r_2(t_0))$ is a point on $\mathcal{C}$
- for almost all (x_0, y_0) on $\mathcal{C}$ there is a $t_0 \in K$ sucht that $(x_0, y_0) = (r_1(t_0), r_2(t_0))$

Questions:

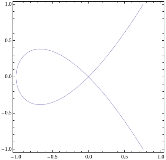
- When can we rationally parametrize a given curve?
- How do we do it?

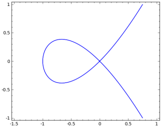
Mathematica	Sage	Maple
ContourPlot	implicit_plot	implicitplot

Mathematica	Sage	Maple
ContourPlot	implicit_plot	implicitplot



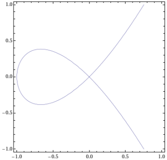
Mathematica	Sage	Maple
ContourPlot	implicit_plot	implicitplot





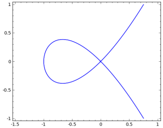
Mathematica

ContourPlot



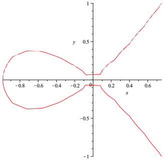
Sage

implicit_plot



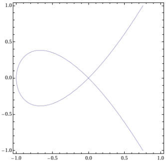
Maple

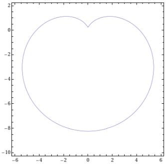
implicitplot



Mathematica

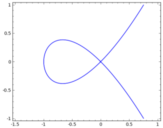
ContourPlot





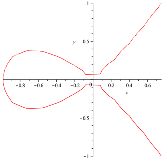
Sage

implicit_plot

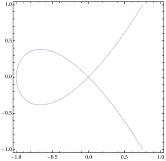


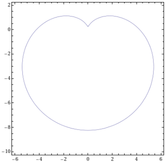
Maple

implicitplot

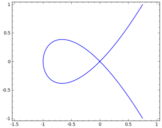


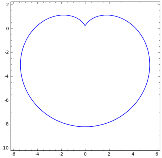
Mathematica
ContourPlot



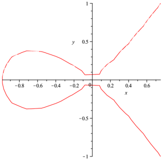


Sage
implicit_plot

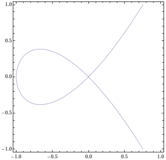


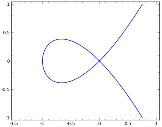


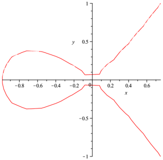
Maple
implicitplot

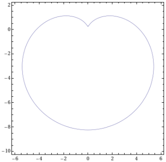


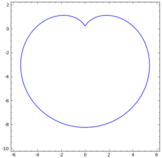
Mathematica	Sage	Maple
ContourPlot	implicit_plot	implicitplot

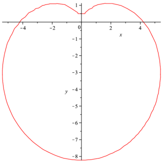




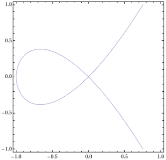


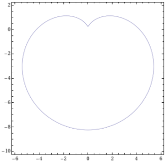


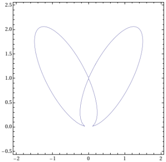




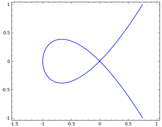
Mathematica
ContourPlot

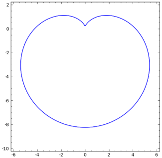




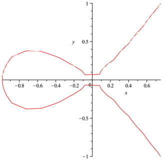


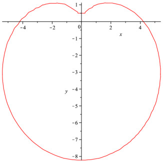
Sage
implicit_plot



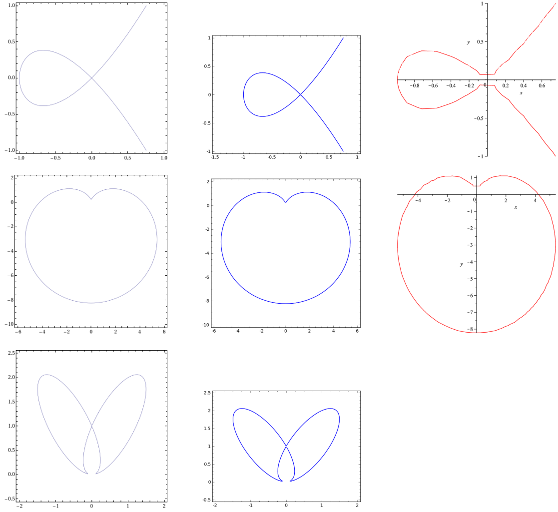


Maple
implicitplot





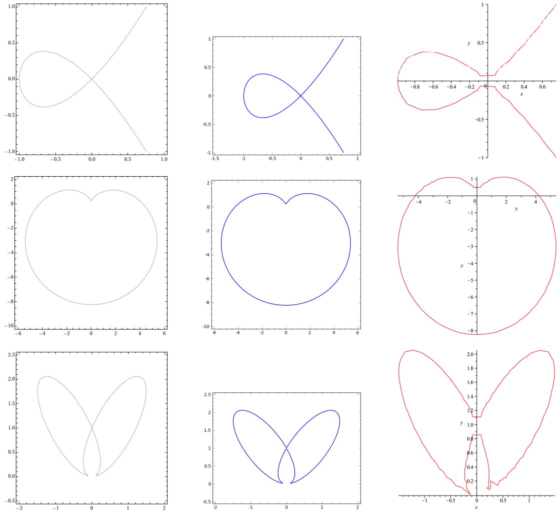
Mathematica	Sage	Maple
ContourPlot	implicit_plot	implicitplot



Mathematica
ContourPlot

Sage
implicit_plot

Maple
implicitplot



Properties

Definition. Let $\mathcal{C}$ be a curve, $f \in K[x, y]$ its defining polynomial, and $P = (a, b) \in \mathbb{A}^2$. P is a point on $\mathcal{C}$ if $f(a, b) = 0$.

P is a simple point on $\mathcal{C}$, if

$$f(a, b) = 0 \quad \text{and} \quad \left(\frac{\partial f}{\partial x}(a, b) \neq 0 \quad \text{or} \quad \frac{\partial f}{\partial y}(a, b) \neq 0 \right).$$

If P is a simple point, then the tangent to $\mathcal{C}$ at P is given by

$$\frac{\partial f}{\partial x}(a, b) \cdot (x - a) + \frac{\partial f}{\partial y}(a, b) \cdot (y - b) = 0.$$

A point on $\mathcal{C}$ that is not simple is called multiple or singular point.

A curve having only simple points is called a non-singular curve.

Properties

Definition. Let $\mathcal{C}$ be a curve, $f \in K[x, y]$ its defining polynomial, and $P = (a, b) \in \mathbb{A}^2$ a point on $\mathcal{C}$. P is a point of multiplicity m, iff

- all partial derivatives $\frac{\partial^{i+j} f}{\partial x^i \partial y^j}(a, b)$ vanish for $i + j < m$
- at least one of the partial derivatives of order m does not vanish

The multiplicity of P on $\mathcal{C}$ is denoted by $m_P(\mathcal{C})$ or just m_P.

Properties

Definition. Let $\mathcal{C}$ be a curve, $f \in K[x,y]$ its defining polynomial, and $P = (a,b) \in \mathbb{A}^2$ a point on $\mathcal{C}$. P is a point of multiplicity m, iff

- all partial derivatives $\frac{\partial^{i+j} f}{\partial x^i \partial y^j}(a,b)$ vanish for $i+j < m$
- at least one of the partial derivatives of order m does not vanish

The multiplicity of P on $\mathcal{C}$ is denoted by $m_P(\mathcal{C})$ or just m_P.

Example. Let $\mathcal{C}$ be defined by the polynomial $f_1(x,y)=x^3+x^2-y^2$. Then $P = (0,0)$ is a double point on $\mathcal{C}$:

$$f(0,0) = 0, \quad \frac{\partial f}{\partial x}(0,0) = 0, \quad \frac{\partial f}{\partial y}(0,0) = 0, \quad \frac{\partial^2 f}{\partial y^2}(0,0) = -2.$$

Tangents at multiple points

Let $1 \leq m = m_P(\mathcal{C})$ be the multiplicity of $P = (a, b)$ on $\mathcal{C}$. The linear factors of

$$\sum_{i=0}^{m} \binom{m}{i} \frac{\partial m f}{\partial x^i \partial y^{m-i}}(a, b)(x - a)^i (y - b)^{m-i}$$

are the tangents to $\mathcal{C}$ at P. An m-fold point is called ordinary, iff all the tangents are different.

Tangents at multiple points

Let $1 \leq m = m_P(\mathcal{C})$ be the multiplicity of $P = (a, b)$ on $\mathcal{C}$. The linear factors of

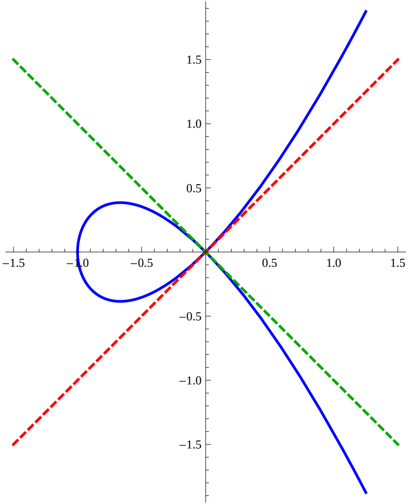
$$\sum_{i=0}^{m} \binom{m}{i} \frac{\partial m f}{\partial x^i \partial y^{m-i}}(a, b)(x-a)^i (y-b)^{m-i}$$

are the tangents to $\mathcal{C}$ at P. An m-fold point is called ordinary, iff all the tangents are different.

Example. Let $\mathcal{C}$ be defined by the polynomial $f_1(x,y) = x^3 + x^2 - y^2$ and $P = (0, 0)$. Then

$$\sum_{i=0}^{2} \binom{2}{i} \frac{\partial^2 f}{\partial x^i \partial y^{2-i}}(0, 0) x^i y^{2-i} = 2(x-y)(x+y)$$

Loop with tangents



More on multiplicities

Let $\mathcal{C}$ be defined by $f \in K[x, y]$, $\deg f = d$. There is an upper bound for the number of singularities:

$$\frac{1}{2}(d-1)(d-2) \geq \sum_{P \in \mathcal{C}} \frac{1}{2} m_P(m_P - 1).$$

More on multiplicities

Let $\mathcal{C}$ be defined by $f \in K[x,y]$, $\deg f = d$. There is an upper bound for the number of singularities:

$$\tfrac{1}{2}(d-1)(d-2) \geq \sum_{P \in \mathcal{C}} \tfrac{1}{2} m_P(m_P - 1).$$

Example. $\mathcal{C}$ defined by $f_1(x,y) = x^3 + x^2 - y^2$ has the double point $P = (0,0)$ and no other singularities:

$$\tfrac{1}{2}(d-1)(d-2) = \tfrac{1}{2} 2 \cdot 1 = 1 \quad \text{and} \quad \sum_{P \in \mathcal{C}} \tfrac{1}{2} m_P(m_P - 1) = \tfrac{1}{2} 2 \cdot 1 = 1.$$

More on multiplicities

Let $\mathcal{C}$ be defined by $f \in K[x,y]$, $\deg f = d$. There is an upper bound for the number of singularities:

$$\tfrac{1}{2}(d-1)(d-2) \geq \sum_{P\in\mathcal{C}} \tfrac{1}{2} m_P(m_P-1).$$

Example. $\mathcal{C}$ defined by $f_3(x,y) = (x^2+4y+y^2)^2 - 16(x^2+y^2)$ has the double point $P=(0,0)$ and no other singularities:

$$\tfrac{1}{2}(d-1)(d-2) = \tfrac{1}{2}3\cdot 2 = 3 \quad \text{and} \quad \sum_{P\in\mathcal{C}} \tfrac{1}{2} m_P(m_P-1) = \tfrac{1}{2}2\cdot 1 = 1.$$

Homogeneous polynomials

- A polynomial $f \in K[x_1, \ldots, x_n]$ is called homogeneous of degree d iff all its terms are of total degree d.

Homogeneous polynomials

- A polynomial $f \in K[x_1, \dots, x_n]$ is called homogeneous of degree d iff all its terms are of total degree d.
- If $f \in K[x_1, \dots, x_n]$ is homogeneous and defines the curve $\mathcal{C}$, then for any $P = (a_1, \dots, a_n) \in \mathcal{C}$ and any $\lambda \in K$ also $(\lambda a_1, \dots, \lambda a_n) \in \mathcal{C}$.

Homogeneous polynomials

- A polynomial $f \in K[x_1, \ldots, x_n]$ is called homogeneous of degree d iff all its terms are of total degree d.
- If $f \in K[x_1, \ldots, x_n]$ is homogeneous and defines the curve $\mathcal{C}$, then for any $P = (a_1, \ldots, a_n) \in \mathcal{C}$ and any $\lambda \in K$ also $(\lambda a_1, \ldots, \lambda a_n) \in \mathcal{C}$.
- Given $f \in K[x, y]$ of degree d, we define its homogenization as $f^*(x, y, z) = z^d f(x/z, y/z)$, i.e., if

  $$f(x, y) = f_0(x, y) + f_1(x, y) + \cdots + f_d(x, y), \text{ with } \deg f_i = i,$$

  then

  $$f^*(x, y, z) = z^d f_0(x, y) + z^{d-1} f_1(x, y) + \cdots + f_d(x, y).$$

Homogeneous polynomials

- A polynomial $f \in K[x_1, \ldots, x_n]$ is called homogeneous of degree d iff all its terms are of total degree d.
- If $f \in K[x_1, \ldots, x_n]$ is homogeneous and defines the curve $\mathcal{C}$, then for any $P = (a_1, \ldots, a_n) \in \mathcal{C}$ and any $\lambda \in K$ also $(\lambda a_1, \ldots, \lambda a_n) \in \mathcal{C}$.
- Given $f \in K[x, y]$ of degree d, we define its homogenization as $f^*(x, y, z) = z^d f(x/z, y/z)$, i.e., if

  $$f(x, y) = f_0(x, y) + f_1(x, y) + \cdots + f_d(x, y), \text{ with } \deg f_i = i,$$

  then

  $$f^*(x, y, z) = z^d f_0(x, y) + z^{d-1} f_1(x, y) + \cdots + f_d(x, y).$$

- If $f^* \in K[x, y, z]$ is a homogeneous polynomial, then its dehomogenization is defined as $f(x, y) = f^*(x, y, 1)$.

Projective space

Definition. The n-dimensional projective space over K is defined as

$$\mathbb{P}^n(K) = \{(c_1 : \cdots : c_{n+1}) \mid (c_1 : \cdots : c_{n+1}) \in K^{n+1} \setminus \{(0, \ldots, 0)\}\},$$

where

$$(c_1 : \cdots : c_{n+1}) = \{(\lambda c_1 : \cdots : \lambda c_{n+1}) \mid \lambda \in K \setminus \{0\}\}.$$

Projective space

Definition. The n-dimensional projective space over K is defined as

$$\mathbb{P}^n(K) = \{(c_1 : \cdots : c_{n+1}) \mid (c_1 : \cdots : c_{n+1}) \in K^{n+1} \backslash \{(0, \ldots, 0)\}\},$$

where

$$(c_1 : \cdots : c_{n+1}) = \{(\lambda c_1 : \cdots : \lambda c_{n+1}) \mid \lambda \in K \backslash \{0\}\}.$$

- A point $P = (a, b) \in \mathbb{A}^2$ corresponds to a line in $\mathbb{A}^3$ through $(a, b, 1)$ and $(0, 0, 0)$ written as $(a : b : 1)$.

Projective space

Definition. The n-dimensional projective space over K is defined as

$$\mathbb{P}^n(K) = \{(c_1 : \cdots : c_{n+1}) \mid (c_1 : \cdots : c_{n+1}) \in K^{n+1} \backslash \{(0, \ldots, 0)\}\},$$

where

$$(c_1 : \cdots : c_{n+1}) = \{(\lambda c_1 : \cdots : \lambda c_{n+1}) \mid \lambda \in K \backslash \{0\}\}.$$

- A point $P = (a, b) \in \mathbb{A}^2$ corresponds to a line in $\mathbb{A}^3$ through $(a, b, 1)$ and $(0, 0, 0)$ written as $(a : b : 1)$.
- The lines in $\mathbb{A}^3$ through $(a, b, 0)$ and $(0, 0, 0)$ correspond to the points at infinity in $\mathbb{P}^2$ in direction $(a, b, 1)$.

Projective space

Definition. The n-dimensional projective space over K is defined as

$$\mathbb{P}^n(K) = \{(c_1 : \cdots : c_{n+1}) \mid (c_1 : \cdots : c_{n+1}) \in K^{n+1} \backslash \{(0, \ldots, 0)\}\},$$

where

$$(c_1 : \cdots : c_{n+1}) = \{(\lambda c_1 : \cdots : \lambda c_{n+1}) \mid \lambda \in K \backslash \{0\}\}.$$

- A point $P = (a, b) \in \mathbb{A}^2$ corresponds to a line in $\mathbb{A}^3$ through $(a, b, 1)$ and $(0, 0, 0)$ written as $(a : b : 1)$.
- The lines in $\mathbb{A}^3$ through $(a, b, 0)$ and $(0, 0, 0)$ correspond to the points at infinity in $\mathbb{P}^2$ in direction $(a, b, 1)$.

Let $f^* \in K[x, y, z]$ be a homogenous polynomial, then the projective plane algebraic curve $\mathcal{C}^*$ in $\mathbb{P}^2$ with defining polynomial f^* is

$$\mathcal{C}* = \{(c_1 : c_2 : c_3) \in \mathbb{P}^2 \mid f^*(c_1, c_2, c_3) = 0\}.$$

Bezout's theorem

Let $f^*, g^* \in K[x, y, z]$ be relatively prime, homogeneous polynomials and let $\mathcal{C}^*, \mathcal{D}^*$ be the corresponding projective curves. Then $\mathcal{C}^*$ and $\mathcal{D}^*$ have exactly $\deg(f^*) \cdot \deg(g^*)$ projective points in common counting multiplicities.

Bezout's theorem

Let $f^*, g^* \in K[x, y, z]$ be relatively prime, homogeneous polynomials and let $\mathcal{C}^*, \mathcal{D}^*$ be the corresponding projective curves. Then $\mathcal{C}^*$ and $\mathcal{D}^*$ have exactly $\deg(f^*) \cdot \deg(g^*)$ projective points in common counting multiplicities.

Example. Intersection of two parallel lines:

$$f_1(x, y) = x + y - 2, \qquad f_2(x, y) = x + y + 1.$$

Bezout's theorem

Let $f^*, g^* \in K[x, y, z]$ be relatively prime, homogeneous polynomials and let $\mathcal{C}^*, \mathcal{D}^*$ be the corresponding projective curves. Then $\mathcal{C}^*$ and $\mathcal{D}^*$ have exactly $\deg(f^*) \cdot \deg(g^*)$ projective points in common counting multiplicities.

Example. Intersection of two parallel lines:

$$f_1(x, y) = x + y - 2, \qquad f_2(x, y) = x + y + 1.$$

Pass to the homogenization of f_1, f_2 and determine the intersection in $\mathbb{P}^2$:

$$f_1^*(x, y, z) = x + y - 2z, \qquad f_2^*(x, y, z) = x + y + z.$$

Bezout's theorem

Let $f^*, g^* \in K[x, y, z]$ be relatively prime, homogeneous polynomials and let $\mathcal{C}^*, \mathcal{D}^*$ be the corresponding projective curves. Then $\mathcal{C}^*$ and $\mathcal{D}^*$ have exactly $\deg(f^*) \cdot \deg(g^*)$ projective points in common counting multiplicities.

Example. Intersection of two parallel lines:

$$f_1(x, y) = x + y - 2, \qquad f_2(x, y) = x + y + 1.$$

Pass to the homogenization of f_1, f_2 and determine the intersection in $\mathbb{P}^2$:

$$f_1^*(x, y, z) = x + y - 2z, \qquad f_2^*(x, y, z) = x + y + z.$$

In $\mathbb{P}^2$ we find the point at infinity $(1 : -1 : 0)$.

Genus of a curve

Let $\mathcal{C}^*$ be an irreducible curve of degree d in $\mathbb{P}^2$ having only ordinary points. Then

$$\text{genus}(\mathcal{C}^*) = \frac{1}{2}\left((d-1)(d-2) - \sum_{P\in\mathcal{C}^*} m_P(m_P-1)\right).$$

The genus of an irreducible affine curve is the genus of the associated projective curve.

Genus of a curve

Let $\mathcal{C}^*$ be an irreducible curve of degree d in $\mathbb{P}^2$ having only ordinary points. Then

$$\operatorname{genus}(\mathcal{C}^*) = \frac{1}{2}\left((d-1)(d-2) - \sum_{P\in\mathcal{C}^*} m_P(m_P-1)\right).$$

The genus of an irreducible affine curve is the genus of the associated projective curve.

Example. $\mathcal{C}$ defined by $f_1(x,y) = x^3 + x^2 - y^2$ has the double point $P = (0,0)$ and no other singularities:

$\frac{1}{2}(d-1)(d-2) = \frac{1}{2}2\cdot 1 = 1$ and $\displaystyle\sum_{P\in\mathcal{C}} \frac{1}{2} m_P(m_P-1) = \frac{1}{2}2\cdot 1 = 1.$

Genus of a curve

Let $\mathcal{C}^*$ be an irreducible curve of degree d in $\mathbb{P}^2$ having only ordinary points. Then

$$\operatorname{genus}(\mathcal{C}^*) = \frac{1}{2}\left((d-1)(d-2) - \sum_{P\in\mathcal{C}^*} m_P(m_P-1)\right).$$

The genus of an irreducible affine curve is the genus of the associated projective curve.

Example. $\mathcal{C}^*$ defined by $f_1^*(x,y) = x^3 + x^2z - y^2z$ has the double point $P = (0:0:1)$ and no other singularities:

$$\tfrac{1}{2}(d-1)(d-2) = \tfrac{1}{2}2\cdot 1 = 1 \quad \text{and} \quad \sum_{P\in\mathcal{C}} \tfrac{1}{2}m_P(m_P-1) = \tfrac{1}{2}2\cdot 1 = 1.$$

Genus of a curve

Let $\mathcal{C}^*$ be an irreducible curve of degree d in $\mathbb{P}^2$ having only ordinary points. Then

$$\mathrm{genus}(\mathcal{C}^*) = \frac{1}{2}\left((d-1)(d-2) - \sum_{P\in\mathcal{C}^*} m_P(m_P - 1)\right).$$

The genus of an irreducible affine curve is the genus of the associated projective curve.

Example. $\mathcal{C}$ defined by $f_3(x,y) = (x^2+4y+y^2)^2 - 16(x^2+y^2)$ has the double point $P=(0,0)$ and no other singularities:

$\frac{1}{2}(d-1)(d-2) = \frac{1}{2}3\cdot 2 = 3$ and $\displaystyle\sum_{P\in\mathcal{C}} \frac{1}{2}m_P(m_P-1) = \frac{1}{2}2\cdot 1 = 1.$

Genus of a curve

Let $\mathcal{C}^*$ be an irreducible curve of degree d in $\mathbb{P}^2$ having only ordinary points. Then

$$\mathrm{genus}(\mathcal{C}^*) = \frac{1}{2}\left((d-1)(d-2) - \sum_{P\in\mathcal{C}^*} m_P(m_P-1)\right).$$

The genus of an irreducible affine curve is the genus of the associated projective curve.

Example. $\mathcal{C}^*$ defined by $f_3^*(x,y) = (x^2+4yz+y^2)^2 - 16(x^2+y^2)z^2$ has the double points $P_1 = (0:0:1)$ and $P_{2,3} = (1:\pm\mathrm{i}:0)$:

$$\tfrac{1}{2}(d-1)(d-2) = \tfrac{1}{2}3\cdot 2 = 3 \quad \text{and} \quad \sum_{P\in\mathcal{C}} \tfrac{1}{2}m_P(m_P-1) = 3\cdot\tfrac{1}{2}2\cdot 1 = 3.$$

Genus of a curve

Let $\mathcal{C}^*$ be an irreducible curve of degree d in $\mathbb{P}^2$ having only ordinary points. Then

$$\mathrm{genus}(\mathcal{C}^*) = \frac{1}{2}\left((d-1)(d-2) - \sum_{P\in\mathcal{C}^*} m_P(m_P - 1)\right).$$

The genus of an irreducible affine curve is the genus of the associated projective curve.

Theorem. An algebraic curve $\mathcal{C}$ (having only ordinary singularities) is rationally parametrizable if and only if $\mathrm{genus}(\mathcal{C}) = 0$.

Simple case

- Let $\mathcal{C}_1$ be the curve defined by $f_1(x, y) = x^3 + x^2 - y^2$.

Simple case

- Let $\mathcal{C}_1$ be the curve defined by $f_1(x, y) = x^3 + x^2 - y^2$.
- We know $\mathrm{genus}(\mathcal{C}_1) = 0$ and $P = (0, 0)$ is a double point.

Simple case

- Let $\mathcal{C}_1$ be the curve defined by $f_1(x, y) = x^3 + x^2 - y^2$.
- We know $\text{genus}(\mathcal{C}_1) = 0$ and $P = (0, 0)$ is a double point.
- Then the curves defined by the parametrized lines $g_t(x, y) = y - tx$ are intersecting $f_1(x, y)$ in exactly one point.

Simple case

- Let $\mathcal{C}_1$ be the curve defined by $f_1(x, y) = x^3 + x^2 - y^2$.
- We know $\mathrm{genus}(\mathcal{C}_1) = 0$ and $P = (0, 0)$ is a double point.
- Then the curves defined by the parametrized lines $g_t(x, y) = y - tx$ are intersecting $f_1(x, y)$ in exactly one point.
- To compute the intersection points we use resultants.

Simple case

- Let $\mathcal{C}_1$ be the curve defined by $f_1(x,y) = x^3 + x^2 - y^2$.
- We know $\mathrm{genus}(\mathcal{C}_1) = 0$ and $P = (0,0)$ is a double point.
- Then the curves defined by the parametrized lines $g_t(x,y) = y - tx$ are intersecting $f_1(x,y)$ in exactly one point.
- To compute the intersection points we use resultants.

$$\mathrm{res}_x(f_1(x,y), g_t(x,y)) = -y^2\left(t^3 - t - y\right)$$
$$\mathrm{res}_y(f_1(x,y), g_t(x,y)) = x^2\left(-t^2 + x + 1\right).$$

Simple case

- Let $\mathcal{C}_1$ be the curve defined by $f_1(x,y) = x^3 + x^2 - y^2$.
- We know $\mathrm{genus}(\mathcal{C}_1) = 0$ and $P = (0,0)$ is a double point.
- Then the curves defined by the parametrized lines $g_t(x,y) = y - tx$ are intersecting $f_1(x,y)$ in exactly one point.
- To compute the intersection points we use resultants.

$$\mathrm{res}_x(f_1(x,y), g_t(x,y)) = -y^2 \left(t^3 - t - y\right)$$
$$\mathrm{res}_y(f_1(x,y), g_t(x,y)) = x^2 \left(-t^2 + x + 1\right).$$

Simple case

- Let $\mathcal{C}_1$ be the curve defined by $f_1(x,y) = x^3 + x^2 - y^2$.
- We know $\mathrm{genus}(\mathcal{C}_1) = 0$ and $P = (0,0)$ is a double point.
- Then the curves defined by the parametrized lines $g_t(x,y) = y - tx$ are intersecting $f_1(x,y)$ in exactly one point.
- To compute the intersection points we use resultants.

$$\mathrm{res}_x(f_1(x,y), g_t(x,y)) = -y^2\left(t^3 - t - y\right)$$
$$\mathrm{res}_y(f_1(x,y), g_t(x,y)) = x^2\left(-t^2 + x + 1\right).$$

Simple case

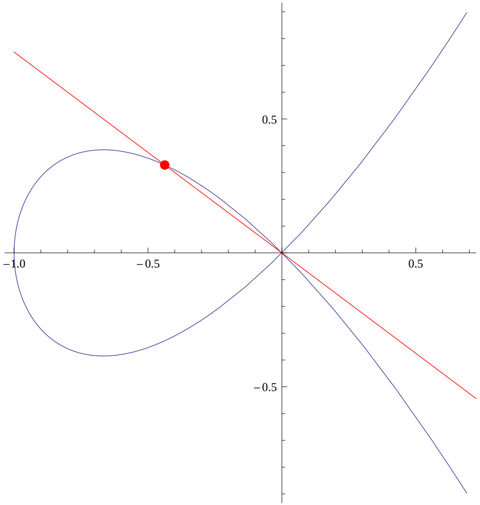
- Let $\mathcal{C}_1$ be the curve defined by $f_1(x, y) = x^3 + x^2 - y^2$.
- We know $\text{genus}(\mathcal{C}_1) = 0$ and $P = (0, 0)$ is a double point.
- Then the curves defined by the parametrized lines $g_t(x, y) = y - tx$ are intersecting $f_1(x, y)$ in exactly one point.
- To compute the intersection points we use resultants.

$$\text{res}_x(f_1(x, y), g_t(x, y)) = -y^2 \left(t^3 - t - y\right)$$
$$\text{res}_y(f_1(x, y), g_t(x, y)) = x^2 \left(-t^2 + x + 1\right).$$

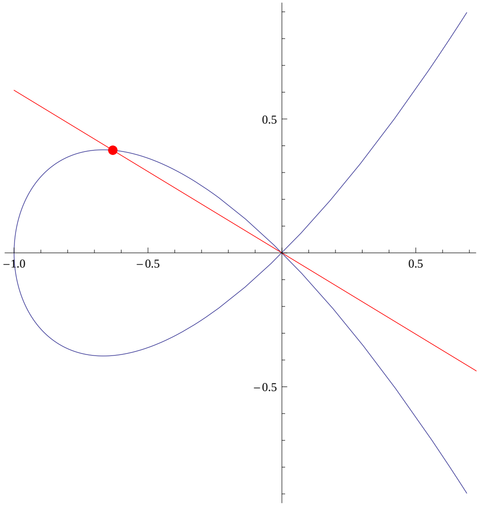
This yields the parametrization

$$x(t) = t^2 - 1, \quad y(t) = t^3 - t.$$

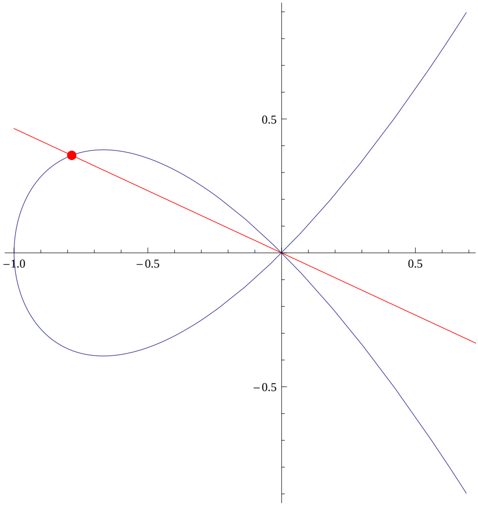
Simple case



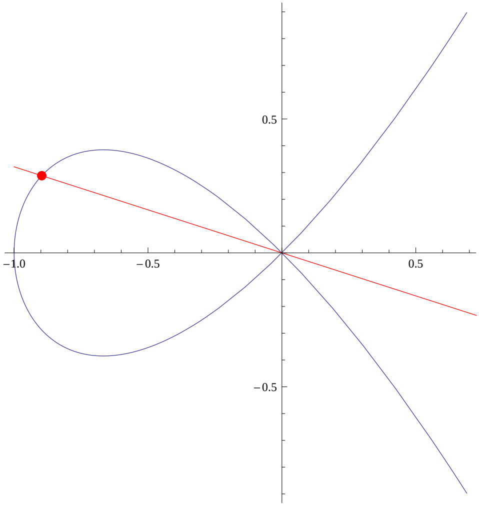
Simple case



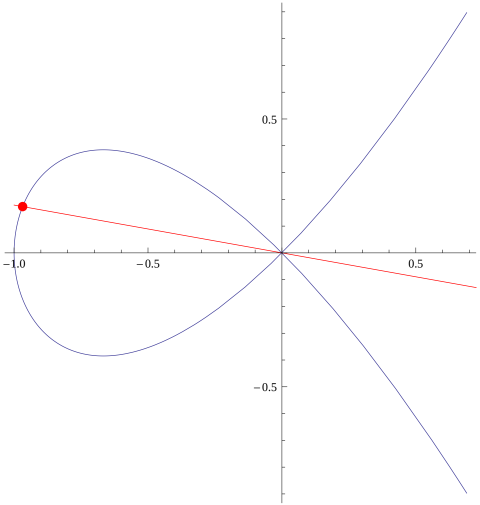
Simple case



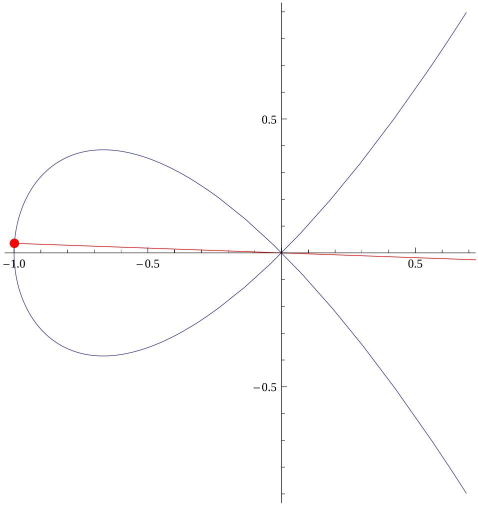
Simple case



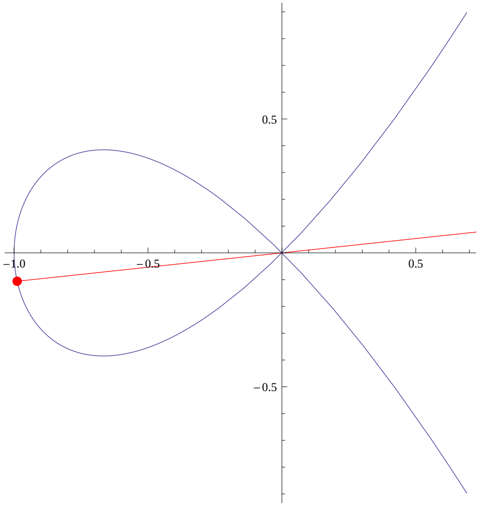
Simple case



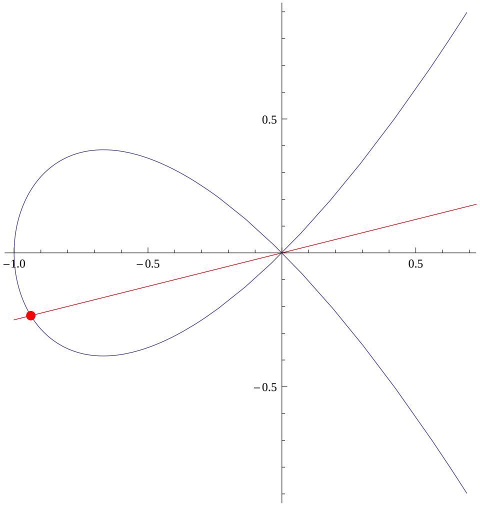
Simple case



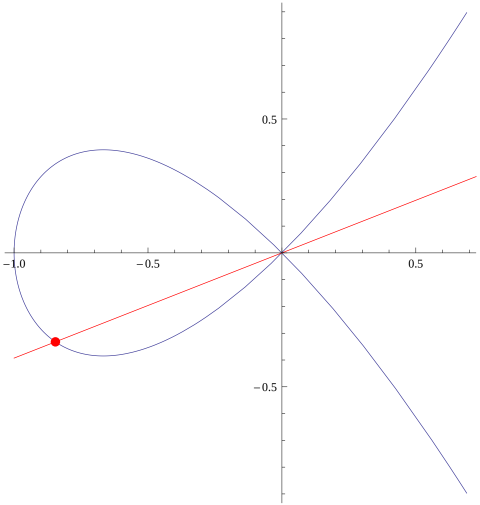
Simple case



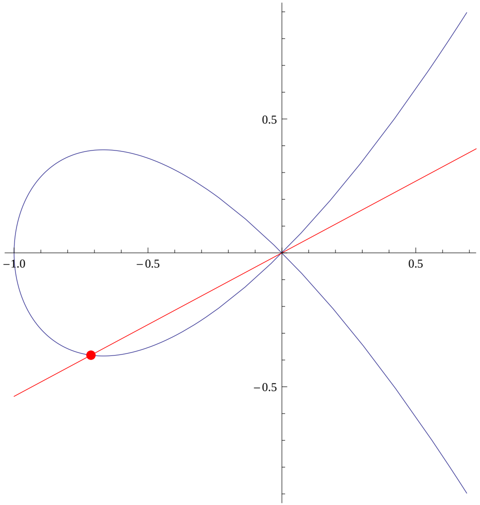
Simple case



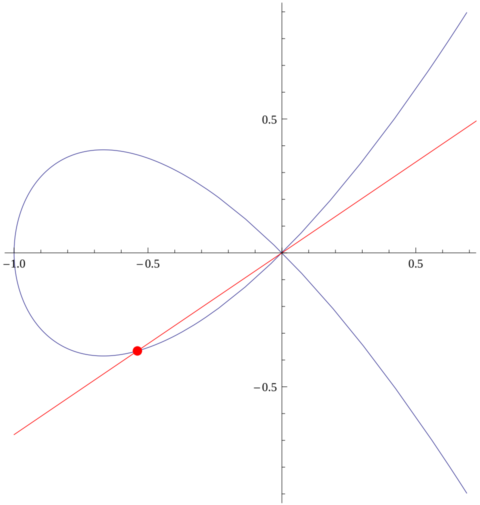
Simple case



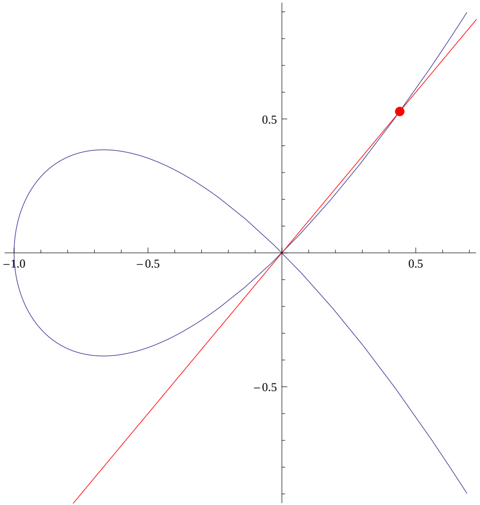
Simple case



Simple case



Simple case



Slightly more complicated

- Let $\mathcal{C}_3$ be the curve defined by

$$f_3(x, y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2).$$

Slightly more complicated

- Let $\mathcal{C}_3$ be the curve defined by

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2).$$

- The homogenization

$$f_3^*(x,y,z) = (x^2 + 4yz + y^2)^2 - 16(x^2 + y^2)z^2$$

Slightly more complicated

- Let $\mathcal{C}_3$ be the curve defined by

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2).$$

- The homogenization

$$f_3^*(x,y,z) = (x^2 + 4yz + y^2)^2 - 16(x^2 + y^2)z^2$$

- We know $\mathrm{genus}(\mathcal{C}_3) = 0$ and $P_1 = (0:0:1)$, $P_{2,3} = (1 : \pm \mathrm{i} : 0)$ are the three double points.

Slightly more complicated

- Let $\mathcal{C}_3$ be the curve defined by

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2).$$

- The homogenization

$$f_3^*(x,y,z) = (x^2 + 4yz + y^2)^2 - 16(x^2 + y^2)z^2$$

- We know $\mathrm{genus}(\mathcal{C}_3) = 0$ and $P_1 = (0:0:1)$, $P_{2,3} = (1:\pm\mathrm{i}:0)$ are the three double points.
- f_2^* and a polynomial a^* of degree 2 have exactly 8 intersection points counting multiplicities. Let $\mathcal{A}^*$ denote the projective curve corresponding to a^*.

Slightly more complicated

- Let $\mathcal{C}_3$ be the curve defined by

$$f_3(x,y) = (x^2+4y+y^2)^2 - 16(x^2+y^2).$$

- The homogenization

$$f_3^*(x,y,z) = (x^2+4yz+y^2)^2 - 16(x^2+y^2)z^2$$

- We know $\mathrm{genus}(\mathcal{C}_3) = 0$ and $P_1 = (0:0:1)$, $P_{2,3} = (1:\pm\mathrm{i}:0)$ are the three double points.
- f_2^* and a polynomial a^* of degree 2 have exactly 8 intersection points counting multiplicities. Let $\mathcal{A}^*$ denote the projective curve corresponding to a^*.
- In general: $\deg(f^*) = d$ and a polynomial a^* of degree $d-2$ have exactly $d(d-2)$ intersection points counting multiplicities.

Slightly more complicated

- Generic ansatz for

$$a^*(x,y,z) = a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2.$$

Slightly more complicated

- Generic ansatz for

$$a^*(x, y, z) = a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2.$$

- Take every m-fold singularity of f^* as an $(m-1)$-fold singularity of a^*.

Slightly more complicated

- Generic ansatz for

$$a^*(x,y,z) = a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2.$$

- Take every m-fold singularity of f^* as an $(m-1)$-fold singularity of a^*.
- Need 1 extra simple point on $\mathcal{C}_3$ as base point for a^*.

Slightly more complicated

- Generic ansatz for

$$a^*(x, y, z) = a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2.$$

- Take every m-fold singularity of f^* as an $(m-1)$-fold singularity of a^*.
- Need 1 extra simple point on $\mathcal{C}_3$ as base point for a^*.
- In general: Need $d-3$ extra simple points on $\mathcal{C}_3$ as base points for a^*.

Slightly more complicated

- Generic ansatz for

$$a^*(x, y, z) = a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2.$$

- Take every m-fold singularity of f^* as an $(m-1)$-fold singularity of a^*.
- Need 1 extra simple point on $\mathcal{C}_3$ as base point for a^*.
- In general: Need $d-3$ extra simple points on $\mathcal{C}_3$ as base points for a^*.
- Use these points to determine the coefficients a_k.

Slightly more complicated

- Generic ansatz for

$$a^*(x, y, z) = a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2.$$

- Take every m-fold singularity of f^* as an $(m-1)$-fold singularity of a^*.
- Need 1 extra simple point on $\mathcal{C}_3$ as base point for a^*.
- In general: Need $d-3$ extra simple points on $\mathcal{C}_3$ as base points for a^*.
- Use these points to determine the coefficients a_k.
- Every intersection point (counting multiplicities) of $\mathcal{C}^*$ and $\mathcal{A}^*$ is fixed, except for one!

Example

Let

$$a^*(x,y,z) = a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2.$$

with simple points $P_1 = (0:0:1), P_{2,3} = (1:\pm\mathrm{i}:0)$ and additional simple point $Q = (0:-8:1)$. Then

$$\begin{aligned}
a^*(0,0,1) = 0 \quad &\longrightarrow \quad a_5 = 0 \\
a^*(1,\mathrm{i},0) = 0 \quad &\longrightarrow \quad a_0 + \mathrm{i}a_1 - a_3 = 0 \\
a^*(1,-\mathrm{i},0) = 0 \quad &\longrightarrow \quad a_0 - \mathrm{i}a_1 - a_3 = 0 \\
a^*(0,-8,1) = 0 \quad &\longrightarrow \quad 64a_3 - 8a_4 + a_5 = 0
\end{aligned}$$

Example

Let

$$a^*(x,y,z) = a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2.$$

with simple points $P_1 = (0:0:1), P_{2,3} = (1:\pm\mathrm{i}:0)$ and additional simple point $Q = (0:-8:1)$. Then

$$\begin{aligned}
a^*(0,0,1) = 0 \quad &\longrightarrow \quad a_5 = 0 \\
a^*(1,\mathrm{i},0) = 0 \quad &\longrightarrow \quad a_0 + \mathrm{i}a_1 - a_3 = 0 \\
a^*(1,-\mathrm{i},0) = 0 \quad &\longrightarrow \quad a_0 - \mathrm{i}a_1 - a_3 = 0 \\
a^*(0,-8,1) = 0 \quad &\longrightarrow \quad 64a_3 - 8a_4 + a_5 = 0
\end{aligned}$$

This system has the solution

$$a_0 = \tfrac{1}{8}a_4, \quad a_1 = 0, \quad a_3 = \tfrac{1}{8}a_4, \quad a_5 = 0.$$

Example

Let

$$a^*(x,y,z) = a_0x^2 + a_1xy + a_2xz + a_3y^2 + a_4yz + a_5z^2.$$

with simple points $P_1 = (0:0:1), P_{2,3} = (1:\pm\mathrm{i}:0)$ and additional simple point $Q = (0:-8:1)$. Then

$$\begin{aligned}
a^*(0,0,1) = 0 \quad &\longrightarrow \quad a_5 = 0 \\
a^*(1,\mathrm{i},0) = 0 \quad &\longrightarrow \quad a_0 + \mathrm{i}a_1 - a_3 = 0 \\
a^*(1,-\mathrm{i},0) = 0 \quad &\longrightarrow \quad a_0 - \mathrm{i}a_1 - a_3 = 0 \\
a^*(0,-8,1) = 0 \quad &\longrightarrow \quad 64a_3 - 8a_4 + a_5 = 0
\end{aligned}$$

This system has the solution

$$a_0 = \tfrac{1}{8}a_4, \quad a_1 = 0, \quad a_3 = \tfrac{1}{8}a_4, \quad a_5 = 0.$$

$$a_2 = 1 \qquad \text{and} \qquad a_4 = t.$$

Example

We have

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$

and the affine adjoint curves

$$a_t(x,y) = \frac{1}{8}tx^2 + \frac{1}{8}ty^2 + ty + x.$$

Example

We have

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$

and the affine adjoint curves

$$a_t(x,y) = \tfrac{1}{8}tx^2 + \tfrac{1}{8}ty^2 + ty + x.$$

The non-constant factors of $\mathrm{res}_x(f(x,y), a_t(x,y))$ are

$$y^2, \quad y+8, \quad t^4y + 8t^4 + 8t^2y - 32t^2 + 16y,$$

Example

We have

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$

and the affine adjoint curves

$$a_t(x,y) = \tfrac{1}{8}tx^2 + \tfrac{1}{8}ty^2 + ty + x.$$

The non-constant factors of $\mathrm{res}_x(f(x,y), a_t(x,y))$ are

$$y^2, \quad y+8, \quad t^4y + 8t^4 + 8t^2y - 32t^2 + 16y,$$

Example

We have

$$f_3(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$

and the affine adjoint curves

$$a_t(x,y) = \frac{1}{8}tx^2 + \frac{1}{8}ty^2 + ty + x.$$

The non-constant factors of $\mathrm{res}_x(f(x,y), a_t(x,y))$ are

$$y^2, \quad y+8, \quad t^4y + 8t^4 + 8t^2y - 32t^2 + 16y,$$

The non-constant factors of $\mathrm{res}_y(f(x,y), a_t(x,y))$ are

$$x^3, \quad , t^4x + 32t^3 + 8t^2x + 16x$$

Example

We have

$$f_3(x, y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2)$$

and the affine adjoint curves

$$a_t(x, y) = \frac{1}{8}tx^2 + \frac{1}{8}ty^2 + ty + x.$$

The non-constant factors of $\mathrm{res}_x(f(x, y), a_t(x, y))$ are

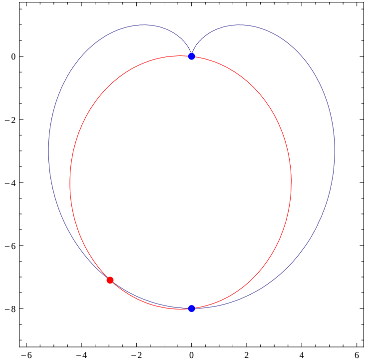
$$y^2, \quad y + 8, \quad t^4y + 8t^4 + 8t^2y - 32t^2 + 16y,$$

The non-constant factors of $\mathrm{res}_y(f(x, y), a_t(x, y))$ are

$$x^3, \quad , t^4x + 32t^3 + 8t^2x + 16x$$

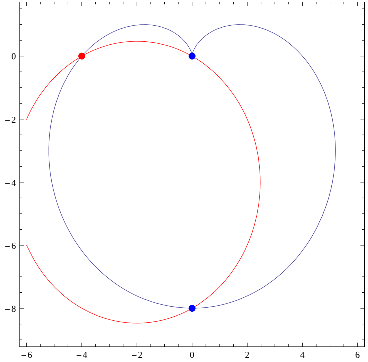
Parametrization

$$(x(t), y(t)) = \left(-\frac{32t^3}{\left(t^2+4\right)^2}, -\frac{8\left(t^4-4t^2\right)}{\left(t^2+4\right)^2} \right).$$



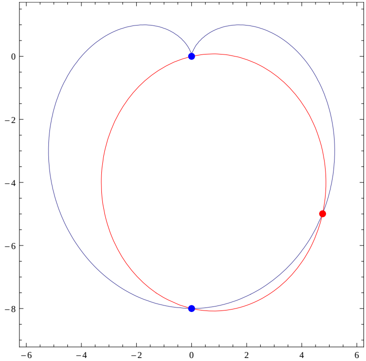
Parametrization

$$(x(t), y(t)) = \left(-\frac{32t^3}{\left(t^2+4\right)^2}, -\frac{8\left(t^4-4t^2\right)}{\left(t^2+4\right)^2} \right).$$



Parametrization

$$(x(t), y(t)) = \left(-\frac{32t^3}{\left(t^2+4\right)^2}, -\frac{8\left(t^4-4t^2\right)}{\left(t^2+4\right)^2}\right).$$



Some open questions

- What is a resultant and how to compute it?
- What is the intersection multiplicity and how to compute it?
- How do I determine simple simple points on the curve?
- How does the choice of simple points affect the parametrization?
- What about real parametrization?
- How do curves enter in cryptography?