Parametrizing rational algebraic curves using integral bases

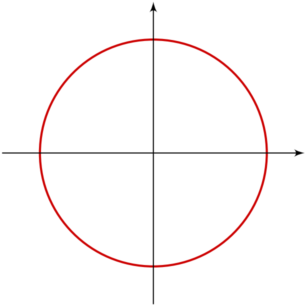
Based on a 1994 paper by Mark Van Hoeij

Thibaut Verron

Johannes Kepler University, Institute for Algebra, Linz, Austria

22 October 2020

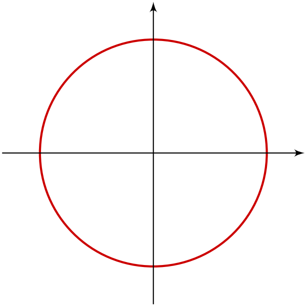
Algebraic curves and parametrization



$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$

Implicit representation

Algebraic curves and parametrization



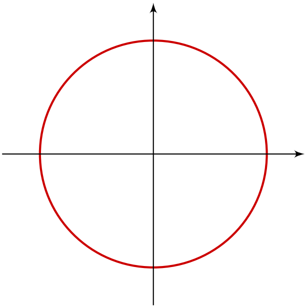
$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

Implicit representation

$$\left\{ \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right) : t \in \mathbb{R} \right\}$$

Parametric representation

Algebraic curves and parametrization



$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

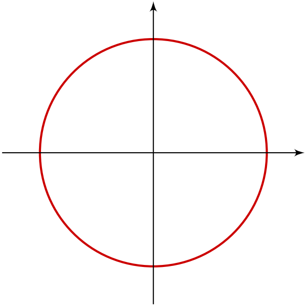
Implicit representation

Implicitization (elimination))

$$\left\{ \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right) : t \in \mathbb{R} \right\}$$

Parametric representation

Algebraic curves and parametrization



$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

Implicit representation

Parametrization

Implicitization (elimination))

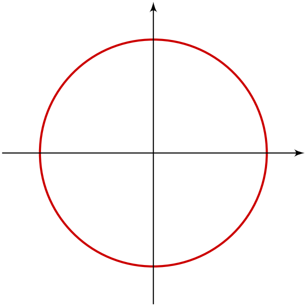
$$\left\{ \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right) : t \in \mathbb{R} \right\}$$

Parametric representation

Parametrization algorithms:

- Sendra, Winkler 1991, 1997
- Van Hoeij 1994, 1996
- Sendra 2002...

Algebraic curves and parametrization



$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$

Implicit representation

Parametrization ↓ ↑ Implicitization (elimination))

$$\left\{ \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right) : t \in \mathbb{R} \right\}$$

Parametric representation

Parametrization algorithms:

- Sendra, Winkler 1991, 1997
- Van Hoeij 1994, 1996: use integral bases
- Sendra 2002...

Integral elements in number fields

- Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$

Integral elements in number fields

- Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$
- All elements of K are algebraic
- Let $\beta \in K$, there exists $a_i, b_i \in \mathbb{Z}$, $d \in \mathbb{N}$ such that

$$\beta^d = \frac{a_0}{b_0} + \frac{a_1}{b_1}\beta + \cdots + \frac{a_{d-1}}{b_{d-1}}\beta^{d-1}$$

- The monic minimal polynomial of β is $\mu_\beta = X^d - \frac{a_{d-1}}{b_{d-1}} X^{d-1} - \cdots - \frac{a_0}{b_0} \in \mathbb{Q}[X]$

  (with d minimal)

Integral elements in number fields

- Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$
- All elements of K are algebraic
- Let $\beta \in K$, there exists $a_i, b_i \in \mathbb{Z}$, $d \in \mathbb{N}$ such that

$$\beta^d = \frac{a_0}{b_0} + \frac{a_1}{b_1}\beta + \cdots + \frac{a_{d-1}}{b_{d-1}}\beta^{d-1}$$

- The monic minimal polynomial of β is $\mu_\beta = X^d - \frac{a_{d-1}}{b_{d-1}}X^{d-1} - \cdots - \frac{a_0}{b_0} \in \mathbb{Q}[X]$ (with d minimal)
- β is integral if all the b_i are 1, or equivalently if $\mu_\beta \in \mathbb{Z}[x]$

Integral elements in number fields

- Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$
- All elements of K are algebraic
- Let $\beta \in K$, there exists $a_i, b_i \in \mathbb{Z}$, $d \in \mathbb{N}$ such that

$$\beta^d = \frac{a_0}{b_0} + \frac{a_1}{b_1}\beta + \cdots + \frac{a_{d-1}}{b_{d-1}}\beta^{d-1}$$

- The monic minimal polynomial of β is $\mu_\beta = X^d - \frac{a_{d-1}}{b_{d-1}}X^{d-1} - \cdots - \frac{a_0}{b_0} \in \mathbb{Q}[X]$ (with d minimal)
- β is integral if all the b_i are 1, or equivalently if $\mu_\beta \in \mathbb{Z}[x]$
- The set $\mathcal{O}_K$ of integral elements of K is called the ring of integers of K

Examples

Recall: $\beta \in \mathcal{O}_K \iff$ its monic minimal polynomial has coefficients in $\mathbb{Z}$

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$

Examples

Recall: $\beta \in \mathcal{O}_K \iff$ its monic minimal polynomial has coefficients in $\mathbb{Z}$

- $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$
- $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$

Examples

Recall: $\beta \in \mathcal{O}_K \iff$ its monic minimal polynomial has coefficients in $\mathbb{Z}$

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$
- Let $K = \mathbb{Q}[i]$, then $\mathcal{O}_K = \mathbb{Z}[i]$

Examples

Recall: $\beta \in \mathcal{O}_K \iff$ its monic minimal polynomial has coefficients in $\mathbb{Z}$

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$
- $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$
- Let $K = \mathbb{Q}[i]$, then $\mathcal{O}_K = \mathbb{Z}[i]$
- Let $K = \mathbb{Q}[\sqrt{5}]$, then $\varphi = \dfrac{1+\sqrt{5}}{2}$ is integral with $\varphi^2 - \varphi - 1 = 0$ and $\mathcal{O}_K = \mathbb{Z}[\varphi]$

Integral bases

- Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$ of degree n
- $\mathcal{O}_K$ = set of integral elements of K

Integral bases

- Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$ of degree n
- $\mathcal{O}_K$ = set of integral elements of K
- $\mathcal{O}_K$ is a ring and a free $\mathbb{Z}$ module with rank n

Integral bases

- Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$ of degree n
- $\mathcal{O}_K =$ set of integral elements of K
- $\mathcal{O}_K$ is a ring and a free $\mathbb{Z}$ module with rank n
- An integral basis of K is a basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module

Integral bases

- Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$ of degree n
- $\mathcal{O}_K =$ set of integral elements of K
- $\mathcal{O}_K$ is a ring and a free $\mathbb{Z}$ module with rank n
- An integral basis of K is a basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module
- Let $\mathcal{B} = (1, \alpha_1, \ldots, \alpha_{n-1})$ be an integral basis of K
- Property: $\beta \in K$ is integral if and only if the coefficients of β in $\mathcal{B}$ are in $\mathbb{Z}$

Integral bases

- Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$ of degree n
- $\mathcal{O}_K$ = set of integral elements of K
- $\mathcal{O}_K$ is a ring and a free $\mathbb{Z}$ module with rank n
- An integral basis of K is a basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module
- Let $\mathcal{B} = (1, \alpha_1, \ldots, \alpha_{n-1})$ be an integral basis of K
- Property: $\beta \in K$ is integral if and only if the coefficients of β in $\mathcal{B}$ are in $\mathbb{Z}$
- Integral bases can be effectively computed (Trager, Van Hoeij)

Summary: integral bases of number fields

> *Let $K = \mathbb{Q}[X]/\langle f \rangle$ be a finite extension of $\mathbb{Q}$ with degree n.*
> *An element $\beta \in K$ has a monic minimal polynomial $\mu \in \mathbb{Q}[X]$,*
> *and β is integral if $\mu \in \mathbb{Z}[X]$.*
>
> *The set of integral elements in K is denoted by $\mathcal{O}_K$,*
> *it is a free $\mathbb{Z}$-module with rank n.*
> *An integral basis of K is a basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module.*
>
> *Let $\mathcal{B} = \{1, b_1, \ldots, b_{n-1}\}$ be an integral basis of K and $\beta \in K$.*
> *β is integral if and only if all its coefficients in $\mathcal{B}$ lie in $\mathbb{Z}$.*

Integral bases of function fields

> *Let $K = k(X)[Y]/\langle f\rangle$ be a finite extension of $k(X)$ with degree n.*
> *An element $\beta \in K$ has a monic minimal polynomial $\mu \in k(X)[Y]$,*
> *and β is integral if $\mu \in k[X][Y]$.*
>
> *The set of integral elements in K is denoted by $\mathcal{O}_K$,*
> *it is a free $k[X]$-module with rank n.*
> *An integral basis of K is a basis of $\mathcal{O}_K$ as a $k[X]$-module.*
>
> *Let $\mathcal{B} = \{1, b_1, \ldots, b_{n-1}\}$ be an integral basis of K and $\beta \in K$.*
> *β is integral if and only if all its coefficients in $\mathcal{B}$ lie in $k[X]$.*

Integral algebraic functions and poles

- Let $K = k(X)[Y]/\langle f \rangle$ with f irreducible

Integral algebraic functions and poles

- Let $K = k(X)[Y]/\langle f \rangle$ with f irreducible
- Elements of K are functions (with poles) on the curve $\mathcal{C} = \{(x, y) \in k^2 : f(x, y) = 0\}$

Integral algebraic functions and poles

- Let $K = k(X)[Y]/\langle f \rangle$ with f irreducible
- Elements of K are functions (with poles) on the curve $\mathcal{C} = \{(x, y) \in k^2 : f(x, y) = 0\}$
- Property: $\beta(X, Y) \in K$ is integral if and only if β does not have any pole on $\mathcal{C}$

Integral algebraic functions and poles

- Let $K = k(X)[Y]/\langle f \rangle$ with f irreducible
- Elements of K are functions (with poles) on the curve $\mathcal{C} = \{(x, y) \in k^2 : f(x, y) = 0\}$
- Property: $\beta(X, Y) \in K$ is integral if and only if β does not have any pole on $\mathcal{C}$
- β is locally integral at x if it does not have any pole at $(x, \bullet) \in \mathcal{C}$

Integral algebraic functions and poles

- Let $K = k(X)[Y]/\langle f \rangle$ with f irreducible
- Elements of K are functions (with poles) on the curve $\mathcal{C} = \{(x, y) \in k^2 : f(x, y) = 0\}$
- Property: $\beta(X, Y) \in K$ is integral if and only if β does not have any pole on $\mathcal{C}$
- β is locally integral at x if it does not have any pole at $(x, \bullet) \in \mathcal{C}$
- A local integral basis of K at $X = x$ is a basis $\mathcal{B} = (1, \alpha_1, \ldots, \alpha_{n-1})$ of K such that
  - All α_i are locally integral at x
  - $\beta \in K$ is locally integral at x iff its coeffs in $\mathcal{B}$ do not have $X - x$ at the denominator

What is parametrizing?

Data: $f(X, Y) \in k[X, Y]$ irreducible, $\mathcal{C} = \{(x, y) : f(x, y) = 0\}$

Goal: find $x(T), y(T) \in k(T)$ such that

- for almost all $t \in k$, $(x(t), y(t)) \in \mathcal{C}$
- for almost all $(x, y) \in \mathcal{C}$, there exists $t \in k$ such that $x = x(t)$, $y = y(t)$

What is parametrizing?

Data: $f(X, Y) \in k[X, Y]$ irreducible, $\mathcal{C} = \{(x, y) : f(x, y) = 0\}$

Goal: find $x(T), y(T) \in k(T)$ such that

- for almost all $t \in k$, $f(x(t), y(t)) = 0$ in k
- for almost all $(x, y) \in \mathcal{C}$, there exists $t \in k$ such that $x = x(t)$, $y = y(t)$

What is parametrizing?

Data: $f(X,Y) \in k[X,Y]$ irreducible, $\mathcal{C} = \{(x,y) : f(x,y) = 0\}$

Goal: find $x(T), y(T) \in k(T)$ such that

- $f(x(T), y(T)) = 0$ in $k(T)$
- for almost all $(x,y) \in \mathcal{C}$, there exists $t \in k$ such that $x = x(t)$, $y = y(t)$

There is a morphism of fields:

$$\begin{aligned} k(X)[Y]/\langle f \rangle &\longrightarrow k(T) \\ X &\longmapsto x(T) \\ Y &\longmapsto y(T) \end{aligned}$$

What is parametrizing?

Data: $f(X, Y) \in k[X, Y]$ irreducible, $\mathcal{C} = \{(x, y) : f(x, y) = 0\}$

Goal: find $x(T), y(T) \in k(T)$ such that

- $f(x(T), y(T)) = 0$ in $k(T)$
- for almost all $(x, y) \in \mathcal{C}$, there exists a unique $t \in k$ such that $x = x(t)$, $y = y(t)$

There is an injective morphism of fields:

$$\begin{aligned} k(X)[Y]/\langle f \rangle &\longrightarrow k(T) \\ X &\longmapsto x(T) \\ Y &\longmapsto y(T) \end{aligned}$$

What is parametrizing?

Data: $f(X,Y) \in k[X,Y]$ irreducible, $\mathcal{C} = \{(x,y) : f(x,y) = 0\}$

Goal: find $x(T), y(T) \in k(T)$ such that

- $f(x(T), y(T)) = 0$ in $k(T)$
- for almost all $(x,y) \in \mathcal{C}$, there exists a unique $t \in k$ such that $x = x(t)$, $y = y(t)$

There is an isomorphism of fields:

$$\begin{aligned} k(X)[Y]/\langle f \rangle &\longrightarrow k(T) \\ X &\longmapsto x(T) \\ Y &\longmapsto y(T) \\ t(X,Y) &\longleftarrow\!\shortmid T \end{aligned}$$

What is parametrizing?

Data: $f(X,Y) \in k[X,Y]$ irreducible, $\mathcal{C} = \{(x,y) : f(x,y) = 0\}$

Goal: find $x(T), y(T) \in k(T)$ and $t(X,Y) \in k(X)[Y]/\langle f \rangle$ such that

- $f(x(T), y(T)) = 0$ in $k(T)$
- $K(t(X,Y)) = K(X)[Y]/\langle f \rangle$

There is an isomorphism of fields:

$$
\begin{array}{rcl}
k(X)[Y]/\langle f \rangle & \longrightarrow & k(T) \\
X & \longmapsto & x(T) \\
Y & \longmapsto & y(T) \\
t(X,Y) & \longleftarrow\!\!\dashv & T
\end{array}
$$

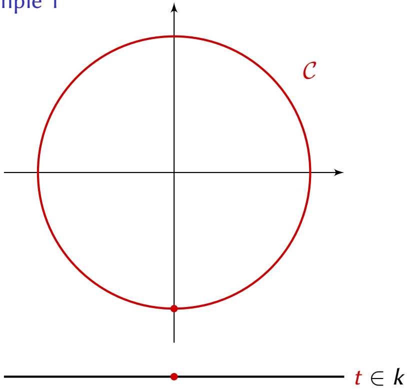
Such a $t(X,Y)$ is called a parameter for the curve.

How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

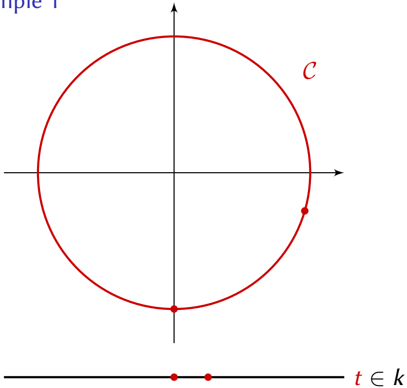


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

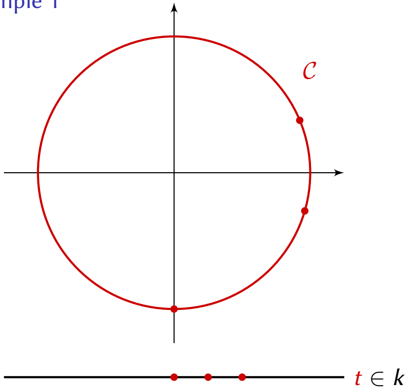


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

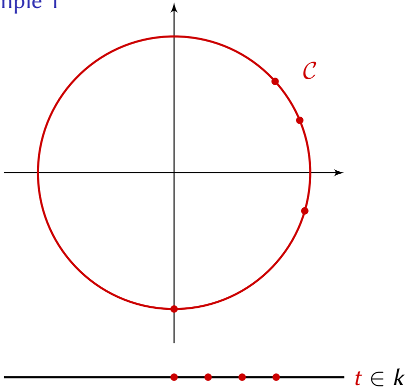


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

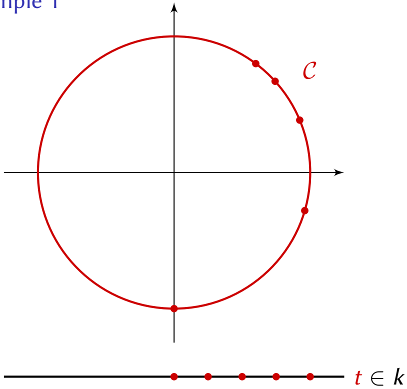


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

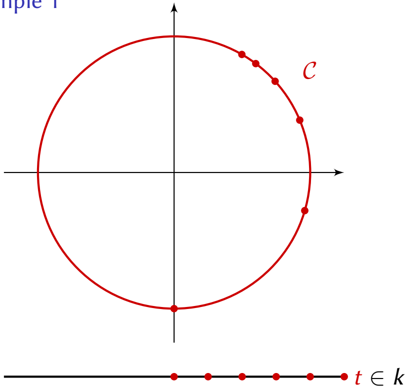


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

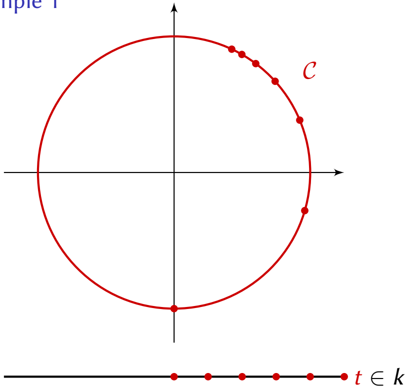


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

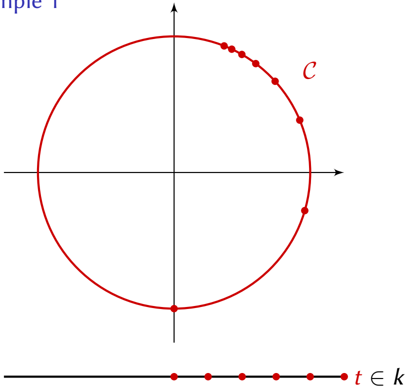


How to compute a parameter?

Characterization:

$t(X,Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

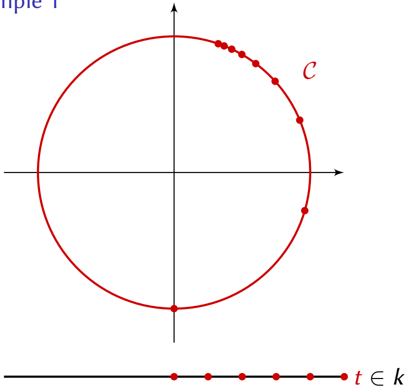


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

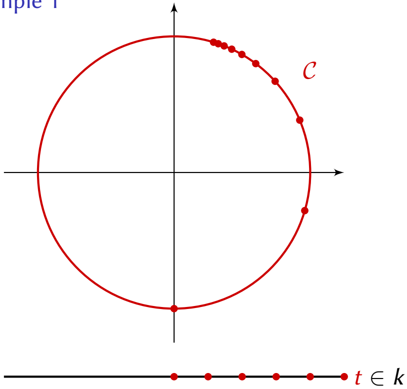


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

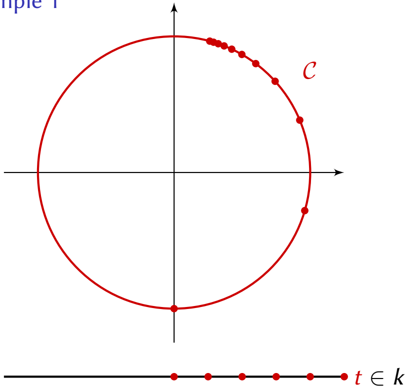


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

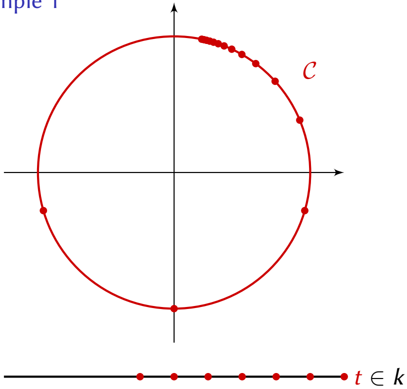


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

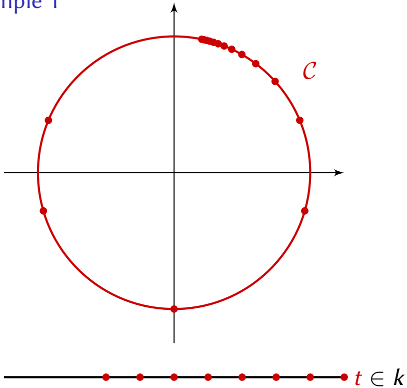


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

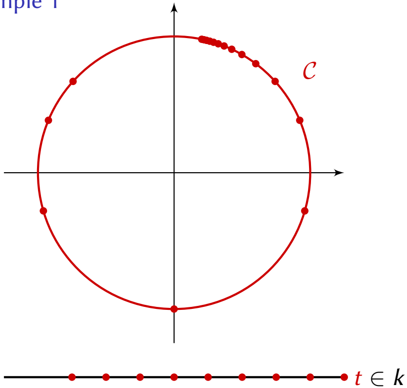


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

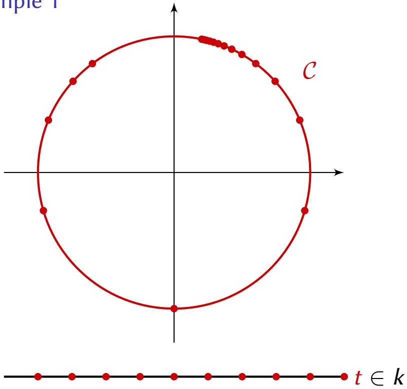


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

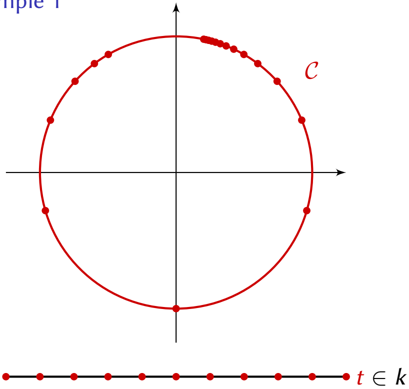


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

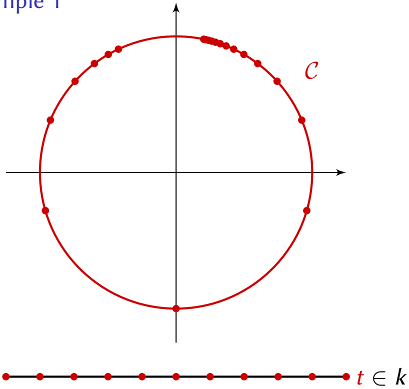


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

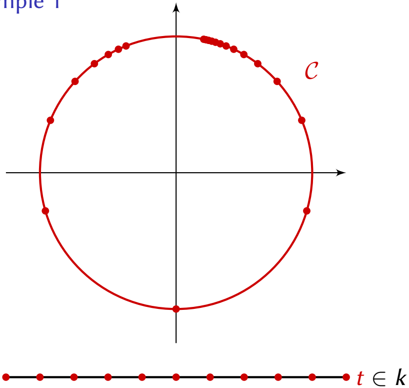


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

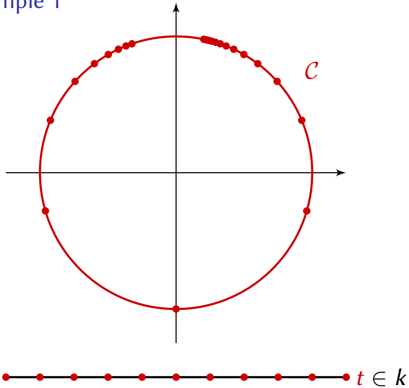


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

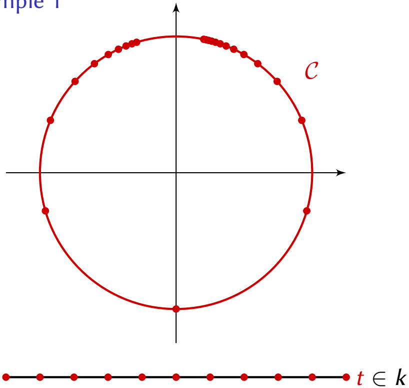


How to compute a parameter?

Characterization:

$t(X,Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

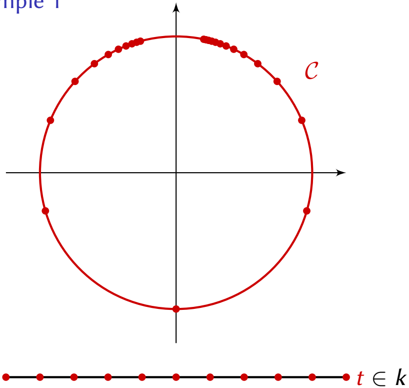
Example 1



Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

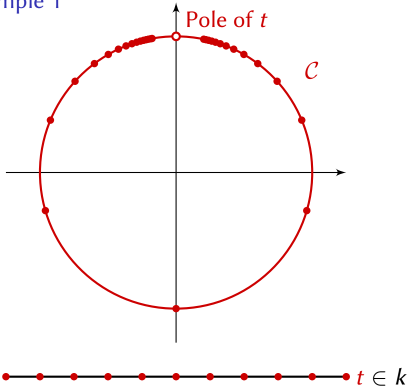


How to compute a parameter?

Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

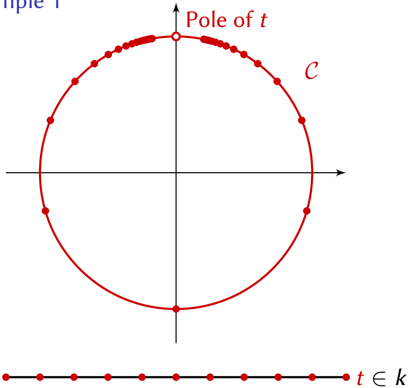


How to compute a parameter?

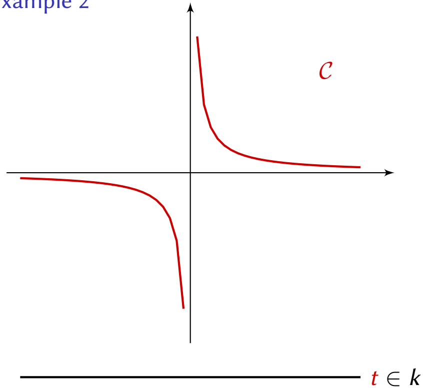
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

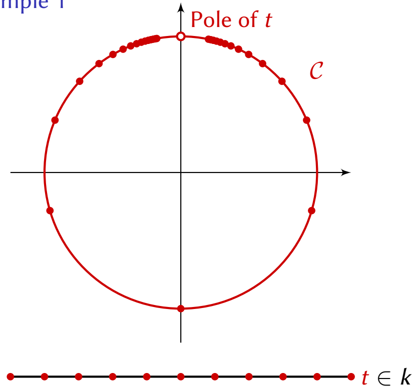


How to compute a parameter?

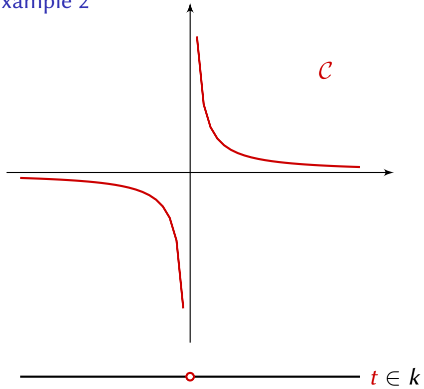
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

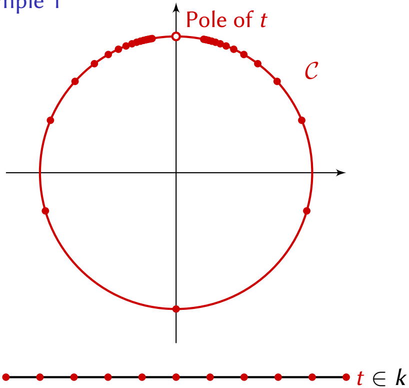


How to compute a parameter?

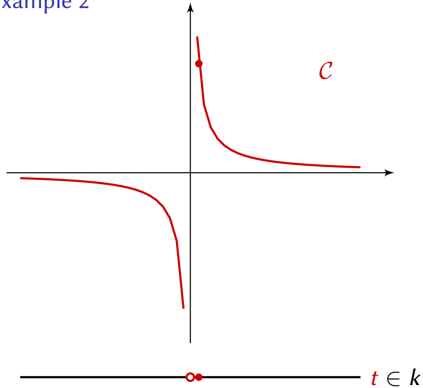
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

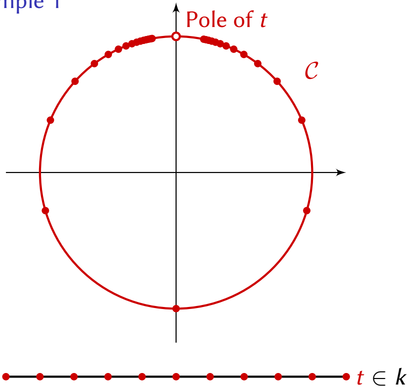


How to compute a parameter?

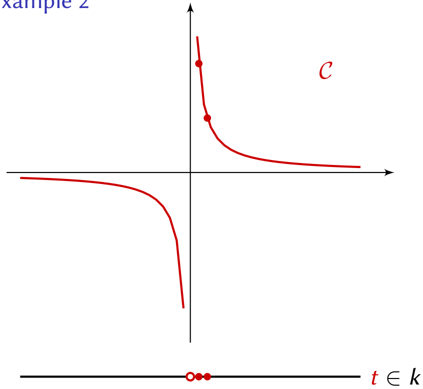
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

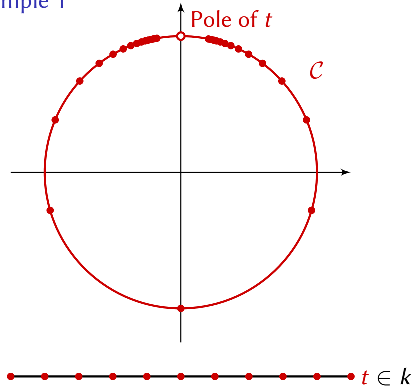


How to compute a parameter?

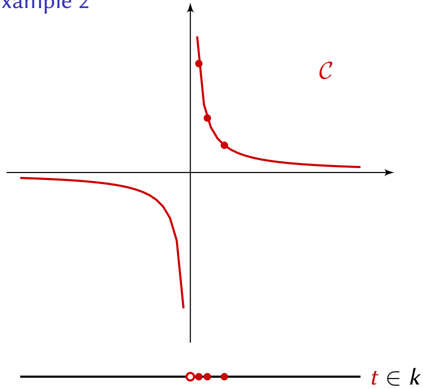
Characterization:

$t(X,Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

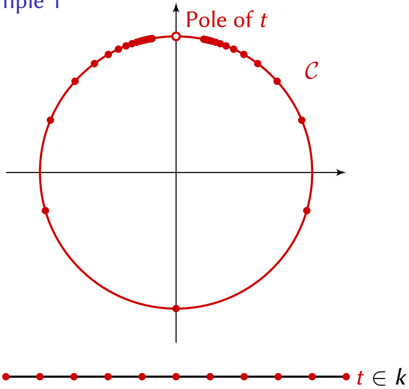


How to compute a parameter?

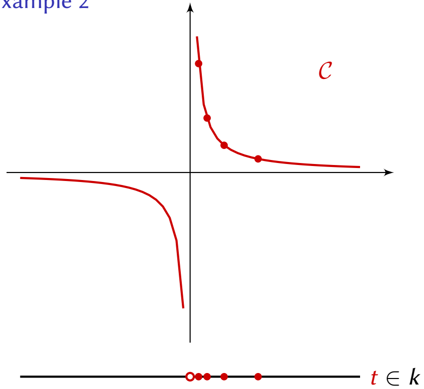
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

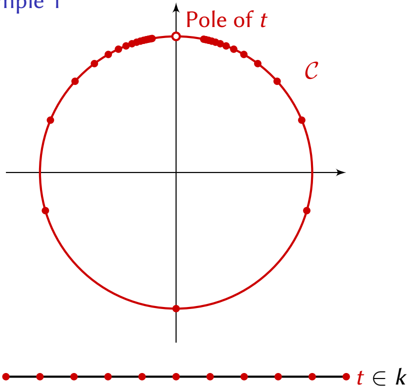


How to compute a parameter?

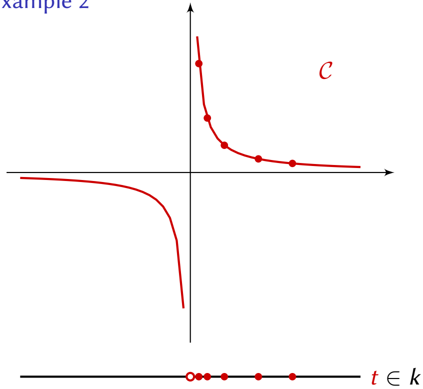
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

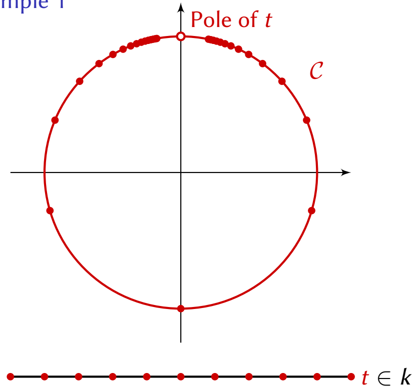


How to compute a parameter?

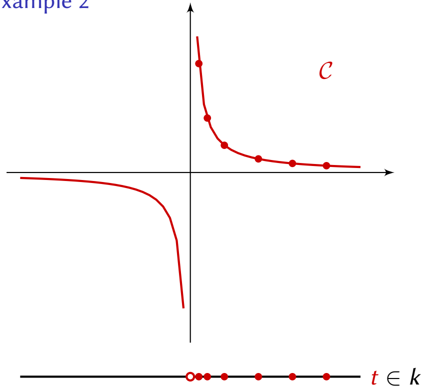
Characterization:

$t(X,Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



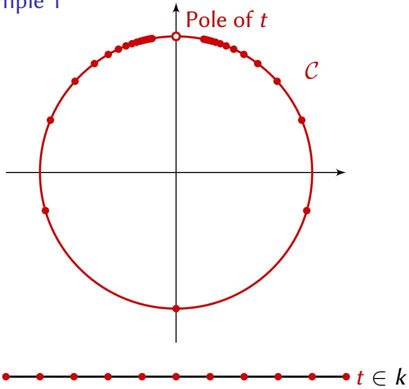
Example 2



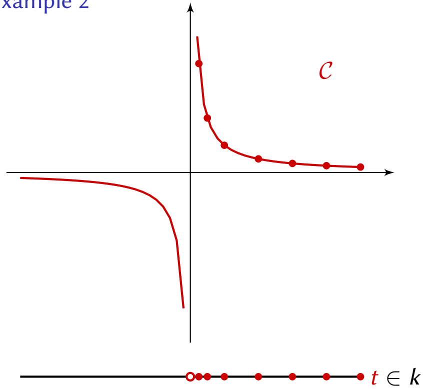
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

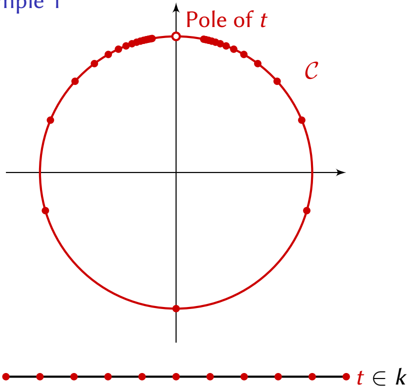


How to compute a parameter?

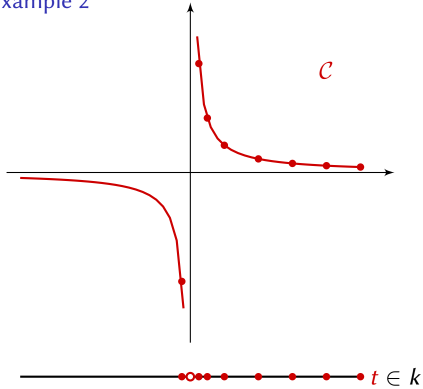
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

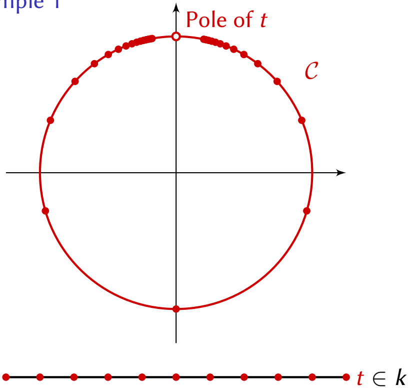


How to compute a parameter?

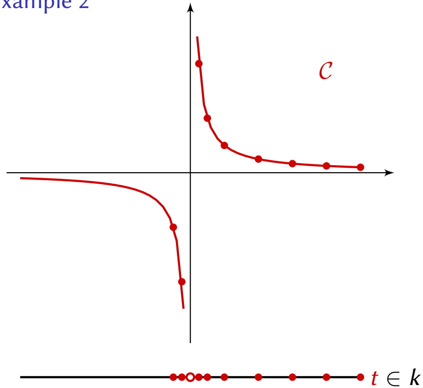
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

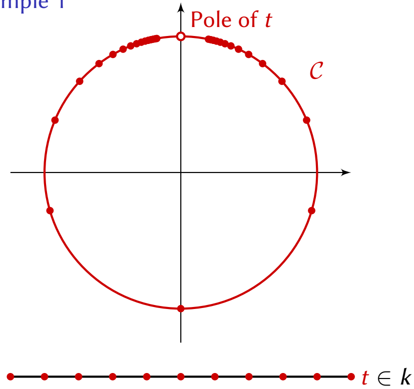


How to compute a parameter?

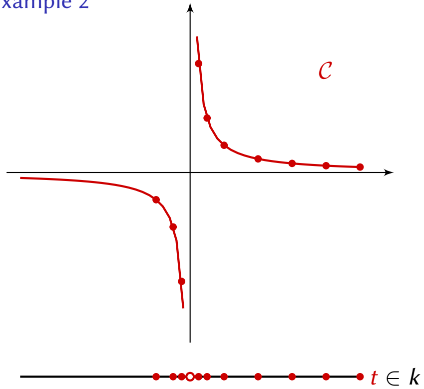
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

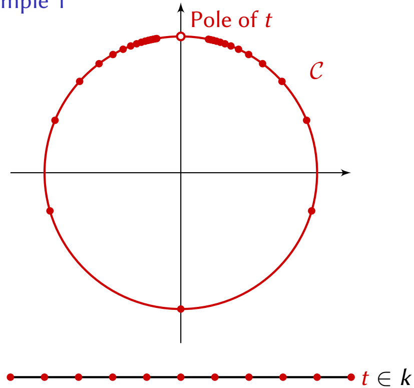


How to compute a parameter?

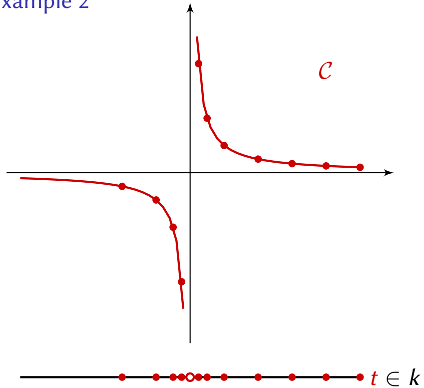
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

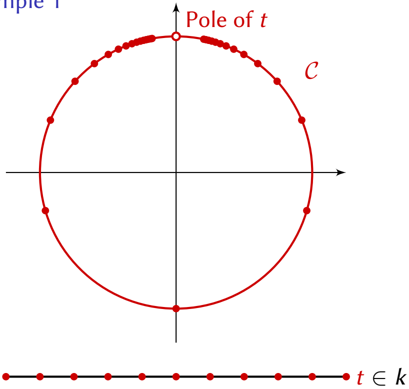


How to compute a parameter?

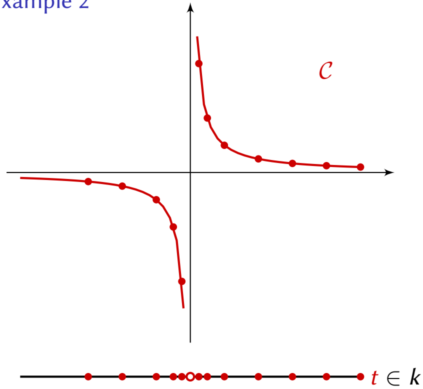
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

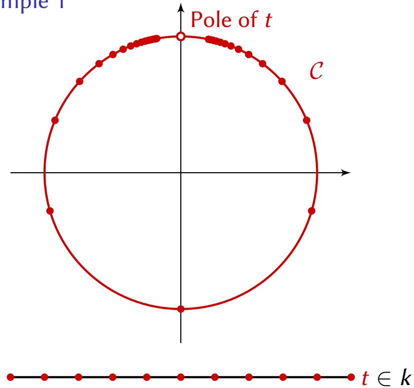


How to compute a parameter?

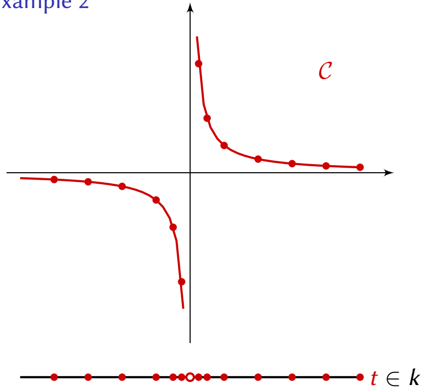
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

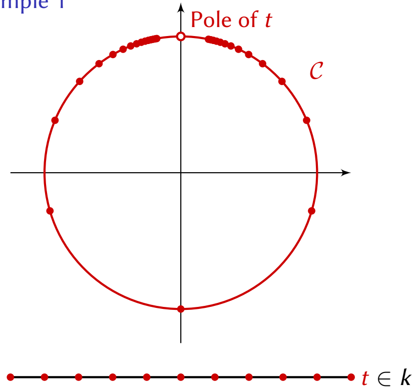


How to compute a parameter?

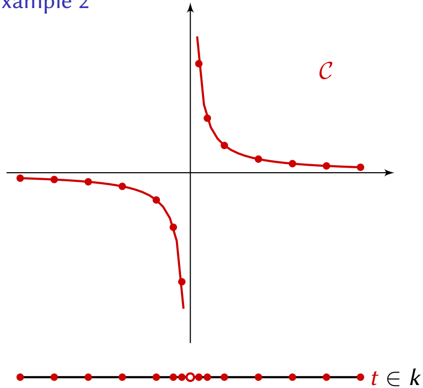
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1



Example 2

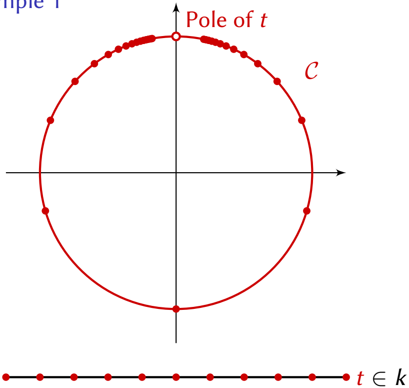


How to compute a parameter?

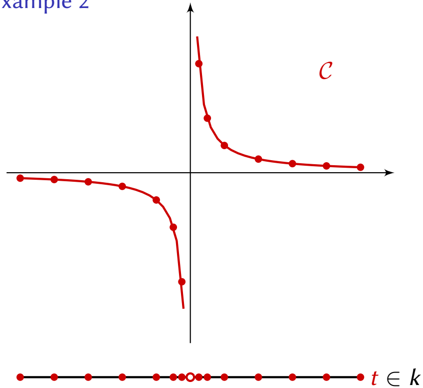
Characterization:

$t(X, Y) \in k(X)[Y]/\langle f \rangle$ is a parameter iff it has exactly one pole, with multiplicity 1, on $\mathcal{C}$

Example 1

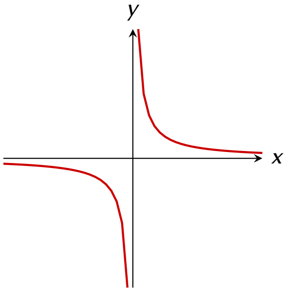


Example 2



Where is the pole of t?

$f(x, y) = 0$



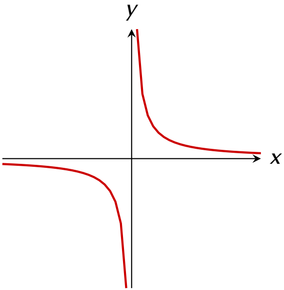
$xy - 1 = 0$

Points at infinity

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

$$f(x, y) = 0 \qquad f_h(x : y : z) = 0$$

$$f_h\left(\frac{x}{z} : \frac{y}{z} : 1\right)$$



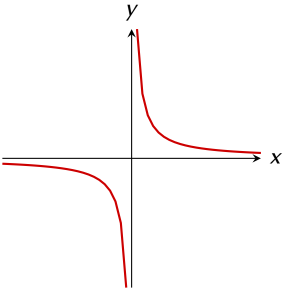
$xy - 1 = 0$
$(z \neq 0)$

$xy - z^2 = 0$

Points at infinity

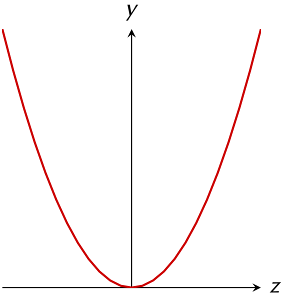
$$f(x,y)=0 \xrightarrow{z^d f\left(\frac{x}{z},\frac{y}{z}\right)} f_h(x:y:z)=0 \xrightarrow{f_h\left(1:\frac{y}{x}:\frac{z}{x}\right)} f_z(z,y)=0$$

$$f(x,y)=0 \xleftarrow{f_h\left(\frac{x}{z}:\frac{y}{z}:1\right)} f_h(x:y:z)=0 \xleftarrow{x^d f_z\left(\frac{z}{x},\frac{y}{x}\right)} f_z(z,y)=0$$



$xy-1=0$
$(z\neq 0)$

$xy-z^2=0$



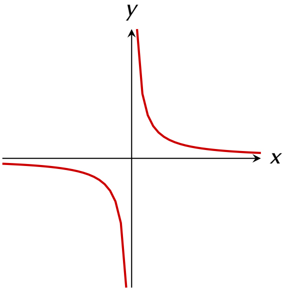
$y-z^2=0$
$(x\neq 0)$

Points at infinity

$$f(x,y)=0 \quad \xrightarrow{z^d f\left(\frac{x}{z},\frac{y}{z}\right)} \quad f_h(x:y:z)=0 \quad \xrightarrow{f_h\left(1:\frac{y}{x}:\frac{z}{x}\right)} \quad f_z(z,y)=0$$

$$f(x,y)=0 \quad \xleftarrow{f_h\left(\frac{x}{z}:\frac{y}{z}:1\right)} \quad f_h(x:y:z)=0 \quad \xleftarrow{x^d f_z\left(\frac{z}{x},\frac{y}{x}\right)} \quad f_z(z,y)=0$$

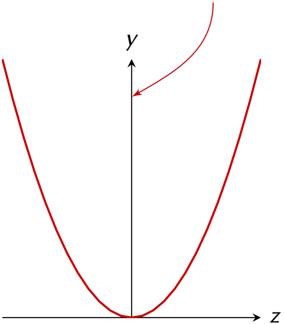
Finite plane



$xy-1=0$
$(z\neq 0)$

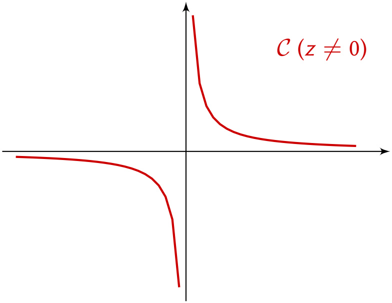
$xy-z^2=0$

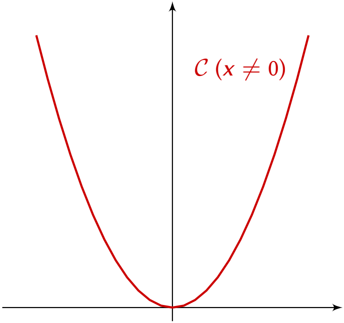
Line at infinity
$(z=0)$



$y-z^2=0$
$(x\neq 0)$

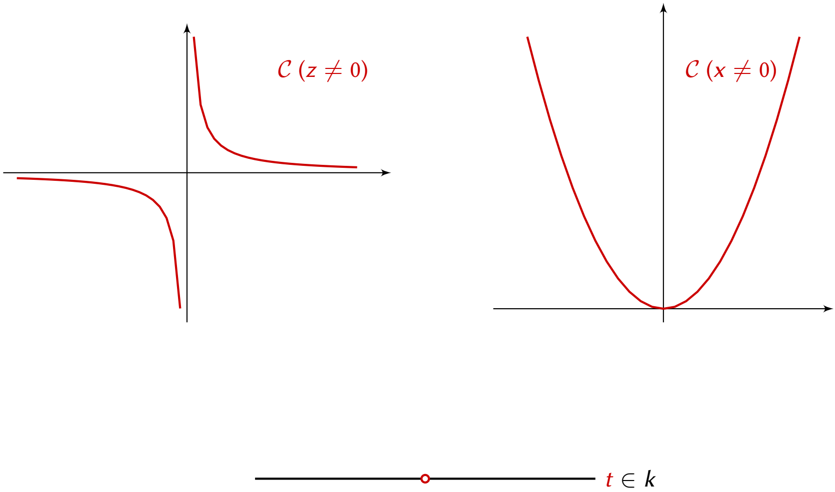
Back to example 2: pole at infinity



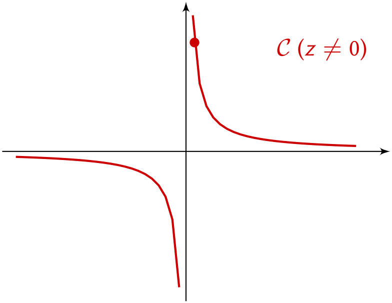


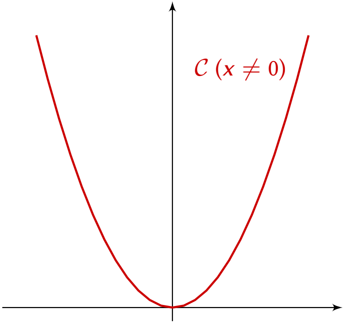
$t \in k$

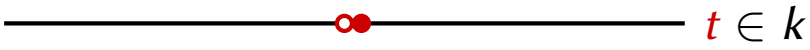
Back to example 2: pole at infinity



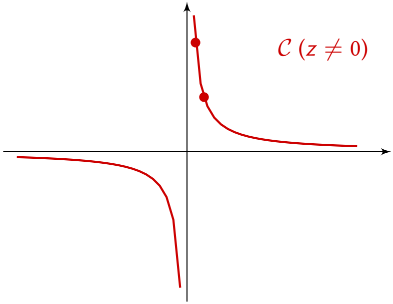
Back to example 2: pole at infinity

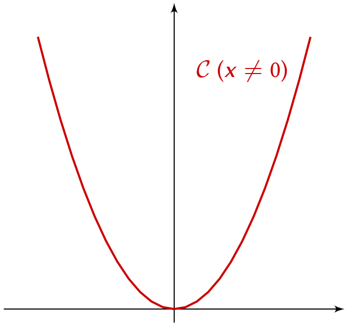




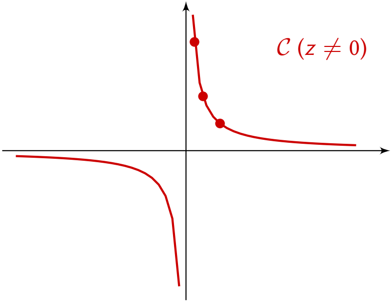


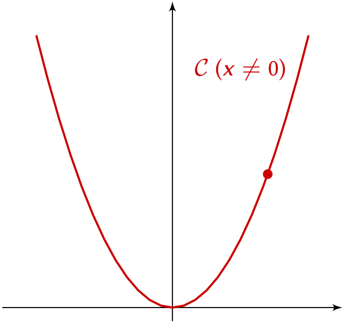
Back to example 2: pole at infinity

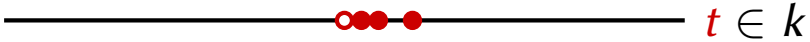




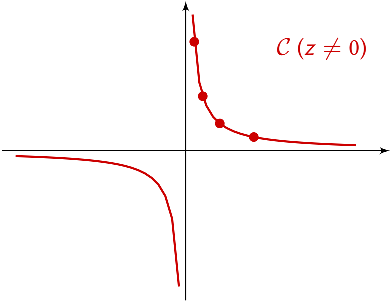
Back to example 2: pole at infinity

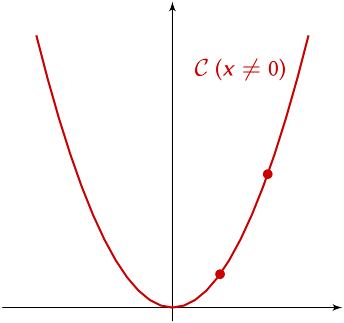


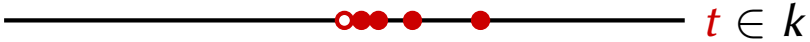




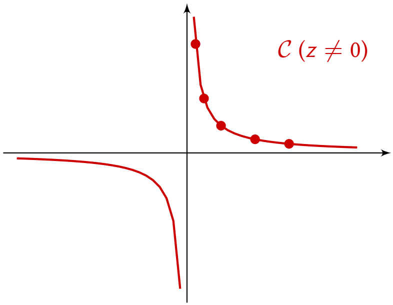
Back to example 2: pole at infinity

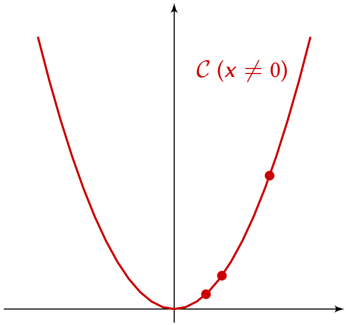


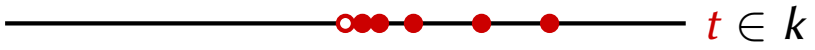




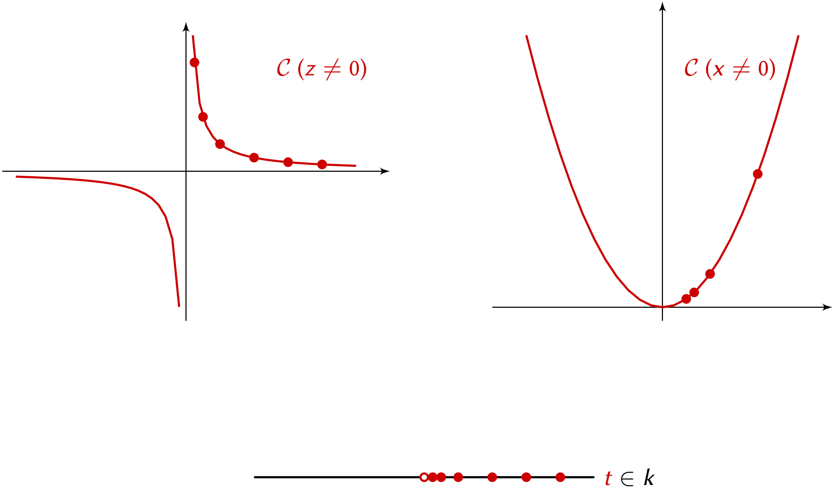
Back to example 2: pole at infinity



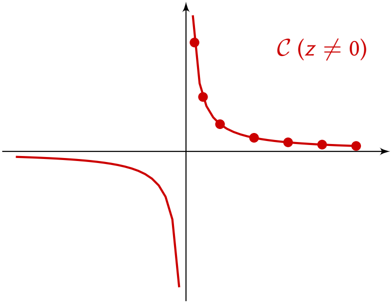


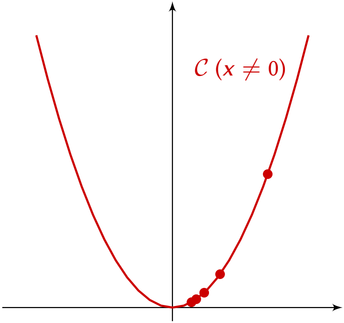


Back to example 2: pole at infinity

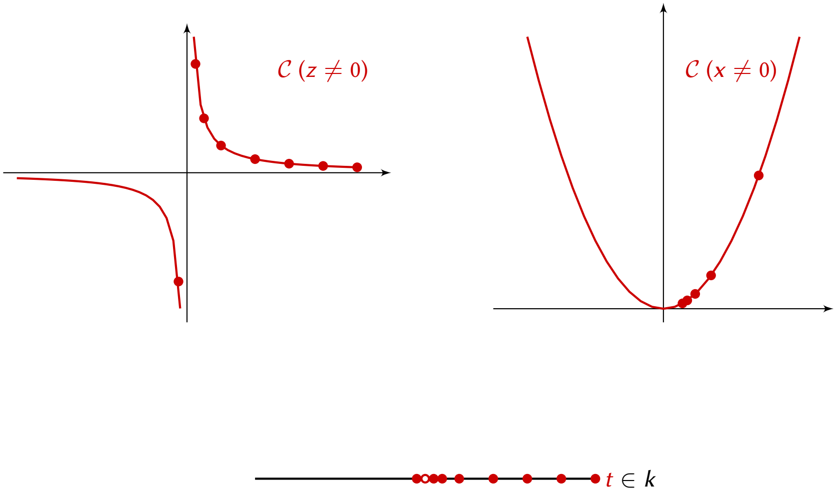


Back to example 2: pole at infinity

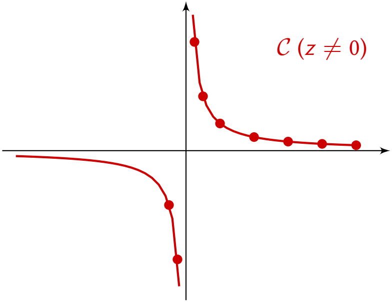


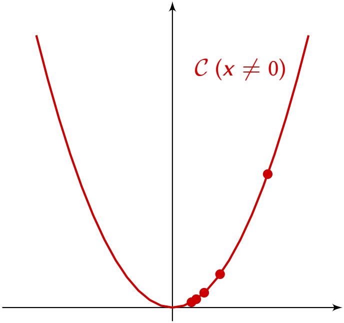


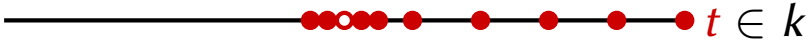
Back to example 2: pole at infinity



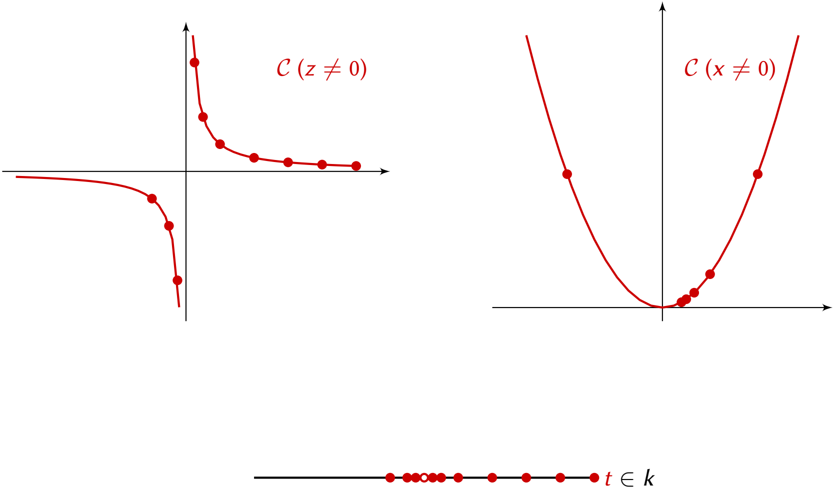
Back to example 2: pole at infinity



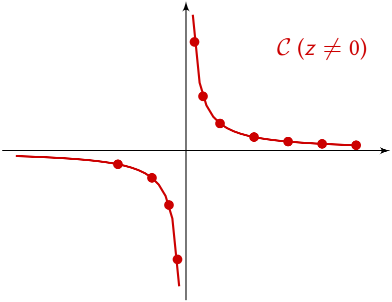


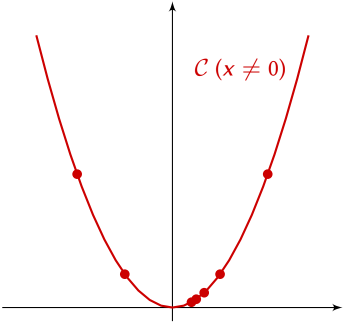


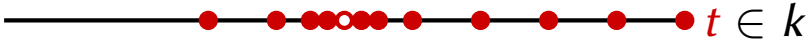
Back to example 2: pole at infinity



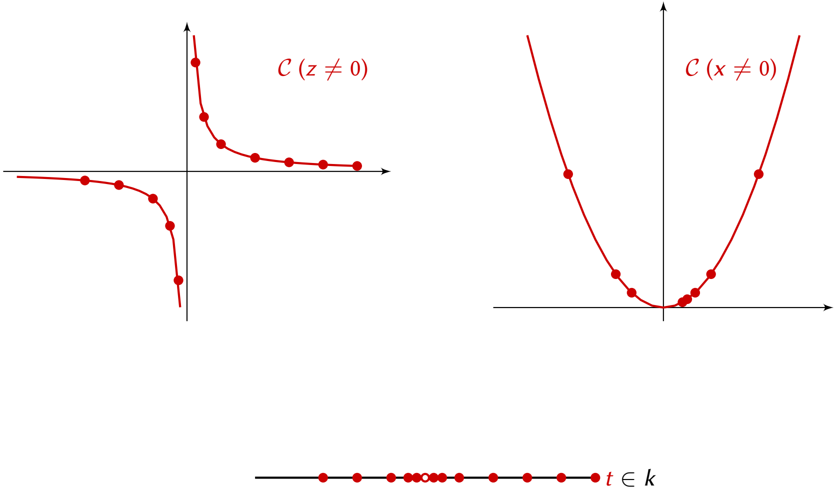
Back to example 2: pole at infinity



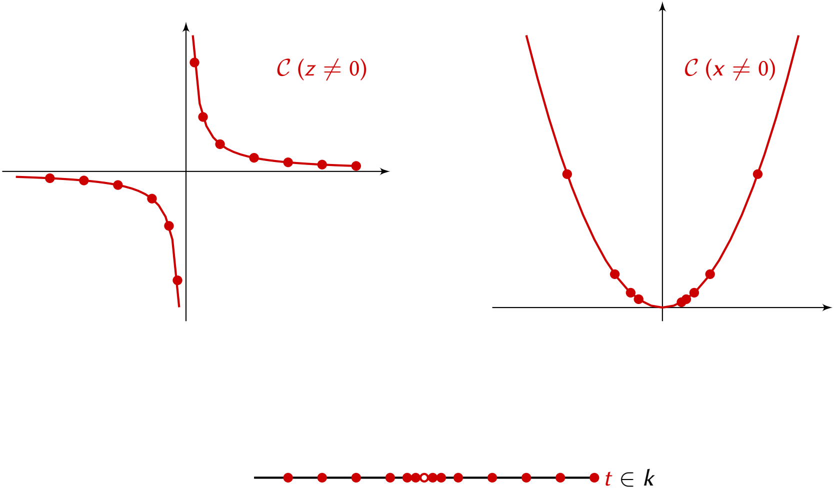




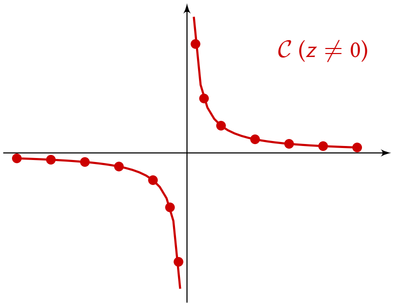
Back to example 2: pole at infinity

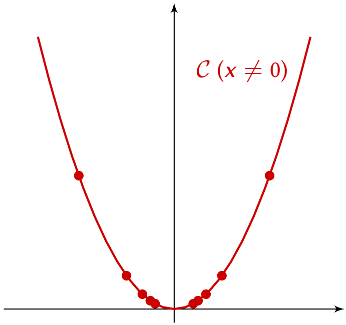


Back to example 2: pole at infinity

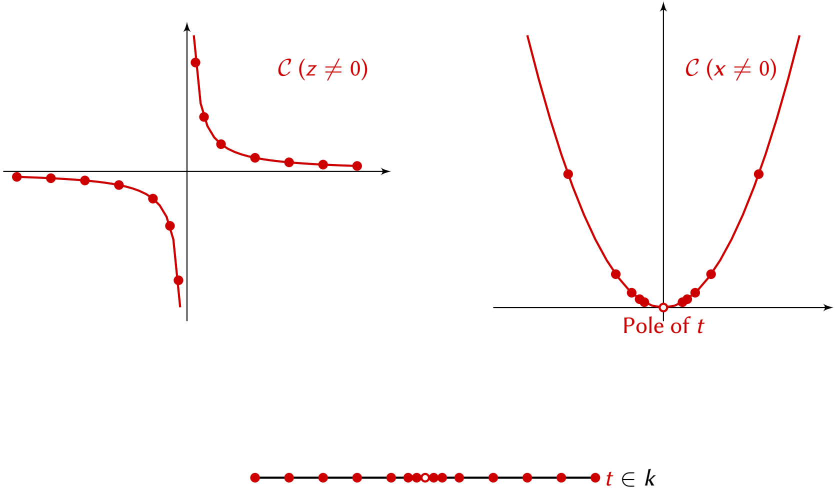


Back to example 2: pole at infinity





Back to example 2: pole at infinity



Full problem

Input: a polynomial $f \in k[X, Y]$ defining a curve $\mathcal{C}$

Output: $t(X, Y) \in k(X)[Y]/\langle f \rangle$ parameter for $\mathcal{C}$

Full problem

Input: a polynomial $f \in k[X, Y]$ defining a curve $\mathcal{C}$

Output: $t(X, Y) \in k(X)[Y]/\langle f \rangle$ parameter for $\mathcal{C}$

Hypotheses:

1. f is irreducible

Full problem

Input: a polynomial $f \in k[X, Y]$ defining a curve $\mathcal{C}$, a point $(x, y) \in \mathcal{C}$

Output: $t(X, Y) \in k(X)[Y]/\langle f \rangle$ parameter for $\mathcal{C}$

Hypotheses:

1. f is irreducible
2. (x, y) is a point of $\mathcal{C}$ such that y is a single root of $f(x, Y)$

Full problem

Input: a polynomial $f \in k[X, Y]$ defining a curve $\mathcal{C}$, a point $(x, y) \in \mathcal{C}$

Output: $t(X, Y) \in k(X)[Y]/\langle f \rangle$ parameter for $\mathcal{C}$

Hypotheses:

1. f is irreducible
2. (x, y) is a point of $\mathcal{C}$ such that y is a single root of $f(x, Y)$
3. $f_h(0 : 1 : 0) \neq 0$

Full problem

Input: a polynomial $f \in k[X, Y]$ defining a curve $\mathcal{C}$, a point $(x, y) \in \mathcal{C}$

Output: $t(X, Y) \in k(X)[Y]/\langle f \rangle$ parameter for $\mathcal{C}$

Hypotheses:

1. f is irreducible
2. (x, y) is a point of $\mathcal{C}$ such that y is a single root of $f(x, Y)$
3. $f_h(0 : 1 : 0) \neq 0$

Key idea: t is a parameter iff it has exactly one pole on $\mathcal{C}$ (including at infinity)

Full problem

Input: a polynomial $f \in k[X, Y]$ defining a curve $\mathcal{C}$, a point $(x, y) \in \mathcal{C}$

Output: $t(X, Y) \in k(X)[Y]/\langle f \rangle$ parameter for $\mathcal{C}$

Hypotheses:

1. f is irreducible
2. (x, y) is a point of $\mathcal{C}$ such that y is a single root of $f(x, Y)$
3. $f_h(0 : 1 : 0) \neq 0$

Key idea: t is a parameter iff it has exactly one pole on $\mathcal{C}$ (including at infinity)

- Integral bases tell us which functions do not have poles

Full problem

Input: a polynomial $f \in k[X, Y]$ defining a curve $\mathcal{C}$, a point $(x, y) \in \mathcal{C}$

Output: $t(X, Y) \in k(X)[Y]/\langle f \rangle$ parameter for $\mathcal{C}$

Hypotheses:

1. f is irreducible
2. (x, y) is a point of $\mathcal{C}$ such that y is a single root of $f(x, Y)$
3. $f_h(0 : 1 : 0) \neq 0$

Key idea: t is a parameter iff it has exactly one pole on $\mathcal{C}$ (including at infinity)

- Integral bases tell us which functions do not have poles
- ... but only on finite parts

Full problem

Input: a polynomial $f \in k[X, Y]$ defining a curve $\mathcal{C}$, a point $(x, y) \in \mathcal{C}$

Output: $t(X, Y) \in k(X)[Y]/\langle f \rangle$ parameter for $\mathcal{C}$

Hypotheses:

1. f is irreducible
2. (x, y) is a point of $\mathcal{C}$ such that y is a single root of $f(x, Y)$
3. $f_h(0 : 1 : 0) \neq 0$

Key idea: t is a parameter iff it has exactly one pole on $\mathcal{C}$ (including at infinity)

- Integral bases tell us which functions do not have poles
- ... but only on finite parts
- ... and we need a function with 1 pole

Overview of the algorithm

Split the projective plane into:

- The finite plane $A := \{z \neq 0\}$
- Part of the line at infinity $B := \{x \neq 0, z = 0\}$
- The last point at infinity $C := \{(0 : 1 : 0)\}$

Overview of the algorithm

Split the projective plane into:

- The finite plane $A := \{z \neq 0\}$
- Part of the line at infinity $B := \{x \neq 0, z = 0\}$
- The last point at infinity $C := \{(0 : 1 : 0)\}$

Algorithm:

1. Find a function P with 1 pole on the finite plane A

Overview of the algorithm

Split the projective plane into:

- The finite plane $A := \{z \neq 0\}$
- Part of the line at infinity $B := \{x \neq 0, z = 0\}$
- The last point at infinity $C := \{(0 : 1 : 0)\}$

Algorithm:

1. Find a function P with 1 pole on the finite plane A
2. Write equations characterizing functions with no pole on A

Overview of the algorithm

Split the projective plane into:

- The finite plane $A := \{z \neq 0\}$
- Part of the line at infinity $B := \{x \neq 0, z = 0\}$
- The last point at infinity $C := \{(0 : 1 : 0)\}$

Algorithm:

1. Find a function P with 1 pole on the finite plane A
2. Write equations characterizing functions with no pole on A
3. Write equations characterizing functions with no pole on the line at infinity B

Overview of the algorithm

Split the projective plane into:

- The finite plane $A := \{z \neq 0\}$
- Part of the line at infinity $B := \{x \neq 0, z = 0\}$
- The last point at infinity $C := \{(0 : 1 : 0)\}$

Algorithm:

1. Find a function P with 1 pole on the finite plane A
2. Write equations characterizing functions with no pole on A
3. Write equations characterizing functions with no pole on the line at infinity B
4. Solve them to find Q such that Q has no pole on A and $P + Q$ has no pole on B

Overview of the algorithm

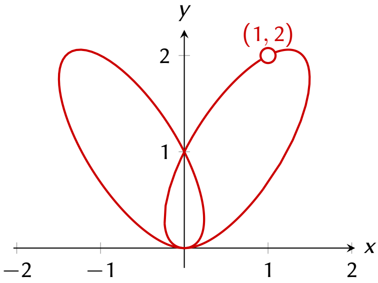
Split the projective plane into:

- The finite plane $A := \{z \neq 0\}$
- Part of the line at infinity $B := \{x \neq 0, z = 0\}$
- The last point at infinity $C := \{(0 : 1 : 0)\}$

Algorithm:

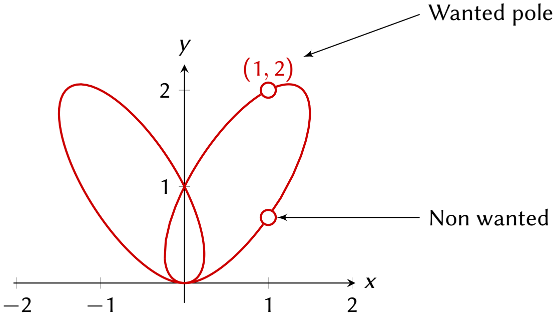
1. Find a function P with 1 pole on the finite plane A
2. Write equations characterizing functions with no pole on A
3. Write equations characterizing functions with no pole on the line at infinity B
4. Solve them to find Q such that Q has no pole on A and $P + Q$ has no pole on B
5. $P + Q$ is our parameter t

1. Finding a function with one pole



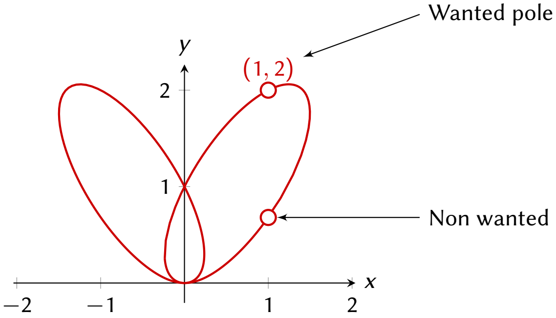
1. Finding a function with one pole

- $\dfrac{1}{X - x}$ would be nice if it didn't have more poles



1. Finding a function with one pole

- $\dfrac{1}{X - x}$ would be nice if it didn't have more poles
- We want a numerator which is 0 everywhere $f(x, Y)$ is 0, except at $Y = y$

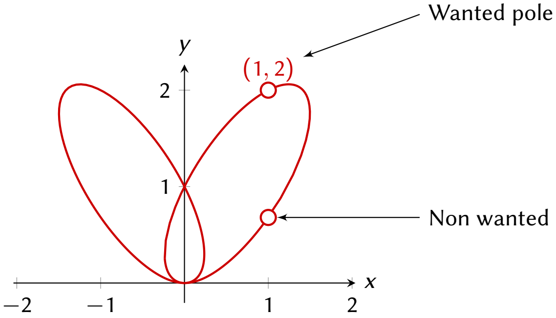


1. Finding a function with one pole

- $\dfrac{1}{X - x}$ would be nice if it didn't have more poles
- We want a numerator which is 0 everywhere $f(x, Y)$ is 0, except at $Y = y$

Construction

1. Write $f(x, Y) = (Y - y)g(Y)$ with $g(y) \neq 0$

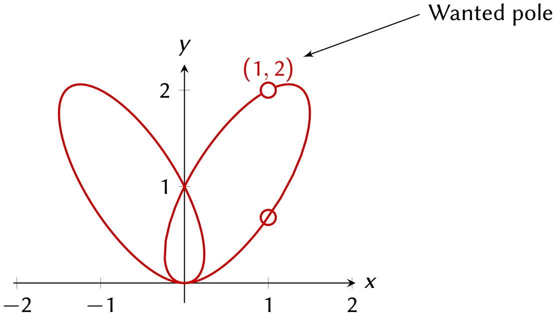


1. Finding a function with one pole

- $\dfrac{1}{X - x}$ would be nice if it didn't have more poles
- We want a numerator which is 0 everywhere $f(x, Y)$ is 0, except at $Y = y$

Construction

1. Write $f(x, Y) = (Y - y)g(Y)$ with $g(y) \neq 0$
2. P is $\dfrac{g(Y)}{X - x}$



2. Equations characterizing functions with no pole in A

1. Compute an integral basis $b_0, \dots, b_{n-1}$ of $k(x)[y]/\langle f \rangle$
2. Q does not have a pole in A iff $Q \in k[x]b_0 + \cdots + k[x]b_{n-1}$
3. Write an Ansatz $Q = \dfrac{\sum_{i+j \leq N} a_{ij} x^i y^j}{D(x)}$ where $N \in \mathbb{N}$ and $D \in k[x]$ are "sufficiently big"
4. Multiply out the denominators
5. Use reductions (e.g. ala Gröbner) to write $DQ = \bullet(x)\, Db_0 + \bullet(x)\, Db_{n-1} + r(x, y)$
6. The coefficients of r are linear in the a_{ij}, set them to 0 and obtain a system of equations

3. Equations characterizing functions with no poles in B

1. Compute an local integral basis $c_0, \ldots, c_{n-1}$ of $k(z)[y]/\langle f_z \rangle$
2. $P + Q$ does not have a pole in $B \setminus A$ iff $P + Q \in k[x]_{(z)} b_0 + \cdots + k[x]_{(z)} b_{n-1}$
3. Forget the denominators not divisible by z
4. Multiply out the rest of the denominators z^d
5. Use reductions (e.g. ala Gröbner) to write $z^d(P + Q) = \bullet(x)\, z^d c_0 + \bullet(x)\, z^d c_{n-1} + s(x, y)$
6. The coefficients of s are linear in the a_{ij}, set them to 0 and obtain a system of equations

Full process

1. Split $\mathcal{C}$ into $(\mathcal{C} \cap \{z = 1\}) \cup (\mathcal{C} \cap \{z = 0\})$
2. Compute P with exactly one pole at finite distance
3. Write an Ansatz for $Q = \dfrac{\sum_{i+j \leq N} a_{ij} x^i y^j}{D(x)}$
4. Compute an integral basis of $k(x)[y]/\langle f \rangle$
5. Find a linear system in the a_{ij} ensuring that Q does not have a pole at finite distance
6. Compute an integral basis of $k(z)[y]/\langle f_z \rangle$
7. Find a linear system in the a_{ij} ensuring that $P + Q$ does not have a pole at infinity
8. Solve the equations and find $t = P + Q$

Full process

1. Split $\mathcal{C}$ into $(\mathcal{C} \cap \{z = 1\}) \cup (\mathcal{C} \cap \{z = 0\})$
2. Compute P with exactly one pole at finite distance
3. Write an Ansatz for $Q = \dfrac{\sum_{i+j \leq N} a_{ij} x^i y^j}{D(x)}$
4. Compute an integral basis of $k(x)[y]/\langle f \rangle$
5. Find a linear system in the a_{ij} ensuring that Q does not have a pole at finite distance
6. Compute an integral basis of $k(z)[y]/\langle f_z \rangle$
7. Find a linear system in the a_{ij} ensuring that $P + Q$ does not have a pole at infinity
8. Solve the equations and find $t = P + Q$
9. Eliminate Y from the system $(T - t, f)$ and solve in X to find $x(T)$
10. Eliminate X from the system $(T - t, f)$ and solve in Y to find $y(T)$