De la décomposition aux intégrales premières rationnelles: algorithmes et complexité

Guillaume Chèze

De la décomposition aux intégrales premières rationnelles: algorithmes et complexité

Guillaume Chèze

Institut de Mathématiques de Toulouse

JNCF 2015

Plan

Question :

Préférez-vous voir

$$f(X,Y) = (2X+3Y+7)^{100} + 5.(2X+3Y+7)^{76} + (2X+3Y+7) + 1$$

ou bien sa forme développée ?

$$f = u(h)$$
$$u(T) = T^{100} + 5T^{76} + T + 1$$
$$h(X,Y) = 2X + 3Y + 7.$$

Question :

Préférez-vous voir

$$f(X,Y) = (2X+3Y+7)^{100} + 5.(2X+3Y+7)^{76} + (2X+3Y+7) + 1$$

ou bien sa forme développée ?

$$f = u(h)$$
$$u(T) = T^{100} + 5T^{76} + T + 1$$
$$h(X,Y) = 2X + 3Y + 7.$$

Décomposition

Définition

Soit $f(X,Y)/g(X,Y) \in \mathbb{K}(X,Y)$,
f/g est ***décomposable*** *lorsque f/g peut s'écrire sous la forme :*

$$\boldsymbol{f/g = u(h) = u \circ h},$$

où $u \in \mathbb{K}(T)$, $\deg u \geq 2$ et $h \in \mathbb{K}(X,Y)$.

Exemple : $\mathbb{K} = \mathbb{Q}$, $u(T) = T^2 + T - 3$,

$$h(X,Y) = \frac{X}{Y}.$$

$$\frac{f}{g}(X,Y) = \frac{X^2 + XY + 3Y^2}{Y^2} = \left(\frac{X}{Y}\right)^2 + \left(\frac{X}{Y}\right) - 3.$$

Simplification : $h(X,Y)^{100} + 5.h^{76}(X,Y) + h(X,Y) + 1$.

Décomposition

Définition

Soit $f(X,Y)/g(X,Y) \in \mathbb{K}(X,Y)$,
*f/g est **décomposable** lorsque f/g peut s'écrire sous la forme :*

$$\boldsymbol{f/g = u(h) = u \circ h},$$

où $u \in \mathbb{K}(T)$, $\deg u \geq 2$ et $h \in \mathbb{K}(X,Y)$.

Exemple : $\mathbb{K} = \mathbb{Q}$, $u(T) = T^2 + T - 3$,
$h(X,Y) = \dfrac{X}{Y}$.

$$\frac{f}{g}(X,Y) = \frac{X^2 + XY + 3Y^2}{Y^2} = \left(\frac{X}{Y}\right)^2 + \left(\frac{X}{Y}\right) - 3.$$

Simplification : $h(X,Y)^{100} + 5.h^{76}(X,Y) + h(X,Y) + 1$.

Le cas des polynômes

Théorème (Noether 1915)

Si $\boldsymbol{f(X, Y)} \in \mathbb{K}\boldsymbol{[X, Y]}$ *est décomposable dans* $\mathbb{K}(X, Y)$ *alors* f *est décomposable dans* $\mathbb{K}[X, Y]$ *:*
il existe $\mathbf{u} \in \mathbb{K}[\mathbf{T}], \deg u \geq 2$ *et* $\boldsymbol{h} \in \mathbb{K}\boldsymbol{[X, Y]}$ *t.q.* $f = u(h)$.

Décomposition = Factorisation particulière

Si $f \in \mathbb{K}[X, Y]$ est décomposable sous la forme $f = u(h)$ alors

$$f = u(h) = \prod_i (h - t_i),$$

où $u(T) = \prod_i (T - t_i)$.

Décomposition = Factorisation particulière

Si $f \in \mathbb{K}[X, Y]$ est décomposable sous la forme $f = u(h)$ et $\mu \in \mathbb{K}$ alors

$$f - \mu = u(h) - \mu = \big(u - \mu\big)(h) = \prod_i (h - \mu_i),$$

où $u(T) - \mu = \prod_i (T - \mu_i)$.

Exemple :
$f(X, Y) = (X + Y)^2 + 1$ est décomposable,
avec $h(X, Y) = X + Y$, $u(T) = T^2 + 1$, et

$$f - \mu = (X + Y)^2 - (\mu - 1) = \big(h - \sqrt{\mu - 1}\big)\big(h + \sqrt{\mu - 1}\big).$$

Décomposition = Factorisation particulière

Si $f \in \mathbb{K}[X, Y]$ est décomposable sous la forme $f = u(h)$ et $\mu \in \mathbb{K}$ alors

$$f - \mu = u(h) - \mu = \big(u - \mu\big)(h) = \prod_i (h - \mu_i),$$

où $u(T) - \mu = \prod_i (T - \mu_i)$.

Exemple :
$f(X, Y) = (X + Y)^2 + 1$ est décomposable,
avec $h(X, Y) = X + Y$, $u(T) = T^2 + 1$, et

$$f - \mu = (X + Y)^2 - (\mu - 1) = \big(h - \sqrt{\mu - 1}\big)\big(h + \sqrt{\mu - 1}\big).$$

Théorème de Bertini-Krull

Théorème (Bertini, 1882 ; Krull 1937)

f/g *est indécomposable*

$\Updownarrow$

$\lambda f - \mu g$ *est irréductible dans* $\overline{\mathbb{K}}[X, Y]$ *pour tout* $(\lambda : \mu) \in \mathbb{P}^1(\overline{\mathbb{K}})$ *sauf un nombre fini.*

$\Updownarrow$

$Uf - Vg$ *est irréductible dans* $\overline{\mathbb{K}(U, V)}[X, Y]$.

Le spectre

Définition

Le ***spectre*** *de* $\dfrac{f(X,Y)}{g(X,Y)} \in \mathbb{K}(X,Y)$ *est l'ensemble :*

$$\sigma(f,g) = \{(\lambda : \mu) \in \mathbb{P}^1(\overline{\mathbb{K}}) \quad | \quad \lambda f - \mu g \text{ est absolument réductible,}$$
$$\text{ou } \deg(\lambda f - \mu g) < \deg(f/g)\}.$$

Théorème (Bertini ; Krull)

$\sigma(f,g)$ *est fini* $\iff$ f/g *est indécomposable.*

Bornes sur le spectre

$|\sigma(f,g)| \leq d^2 - 1$, Ruppert 1986.

$\rho(f,g) \leq d^2 - 1$, Lorenzini 1993, Vistoli 1993 :
$\rho(f,g) =$ “Nombre de facteurs absolument irréductibles de $\lambda f - \mu g$ où $(\lambda : \mu) \in \sigma(f,g)$.”

$m(f,g) \leq d^2 - 1$, Busé-C. 2011 :
$m(f,g) =$ “Nombre de facteurs absolument irréductibles (comptés avec multiplicité) de $\lambda f - \mu g$ où $(\lambda : \mu) \in \sigma(f,g)$.”

Théorème de Noether, 1922

Théorème (Ruppert 1986)

Soit $f(X, Y) = \sum_{0 \leq i+j \leq d} c_{i,j} X^i Y^j \in \mathbb{K}[X, Y]$, *où* $d \geq 2$.
Il existe un nombre fini de formes $\Phi_t(\ldots, C_{i,j}, \ldots)$ *dans* $\mathbb{Z}[\ldots, C_{i,j}, \ldots]$ *telles que*

$$\forall t, \Phi_t(\ldots, c_{i,j}, \ldots) = 0$$

si et seulement si

$$f(X, Y) = \sum_{0 \leq i+j \leq d} c_{i,j} X^i Y^j$$

est réductible dans $\overline{\mathbb{K}}[X, Y]$ *ou* $\deg(f) < d$.

De plus, $\deg \Phi_t \leq d^2 - 1$.

Théorème de Ruppert

Théorème (Ruppert 1986, Gao 2002)

Soit $f(X,Y) \in \mathbb{K}[X,Y]$ *sans facteurs carrés,* $\deg(f) = d$*, et soit* $f = f_1 \cdots f_r$ *sa factorisation en irréductibles dans* $\overline{\mathbb{K}}[X,Y]$*.*

$$E = \{(G,H) \in \left(\mathbb{K}[X,Y]_{\leq d-1}\right)^2 \mid \deg(XG + YH) \leq d-1\}$$

On considère l'application linéaire suivante :

$$\begin{array}{rcl} \mathcal{R}(f) : E & \longrightarrow & \mathbb{K}[X,Y] \\ (G,H) & \longmapsto & f^2.\left[\partial_Y\left(\frac{G}{f}\right) - \partial_X\left(\frac{H}{f}\right)\right] \end{array}$$

Alors $r - 1 = \dim_{\mathbb{K}} \ker \mathcal{R}(f)$*.*

Formes de Noether= Mineurs de $\mathcal{R}(f)$.

Théorème de Ruppert

Théorème (Ruppert 1986, Gao 2002)

Soit $f(X,Y) \in \mathbb{K}[X,Y]$ *sans facteurs carrés,* $\deg(f) = d$*, et soit* $f = f_1 \cdots f_r$ *sa factorisation en irréductibles dans* $\overline{\mathbb{K}}[X,Y]$*.*

$$E = \{(G,H) \in \left(\mathbb{K}[X,Y]_{\leq d-1}\right)^2 \mid \deg(XG + YH) \leq d-1\}$$

On considère l'application linéaire suivante :

$$\begin{array}{rcl} \mathcal{R}(f) : E & \longrightarrow & \mathbb{K}[X,Y] \\ (G,H) & \longmapsto & f^2.\left[\partial_Y\left(\frac{G}{f}\right) - \partial_X\left(\frac{H}{f}\right)\right] \end{array}$$

Alors $r - 1 = \dim_{\mathbb{K}} \ker \mathcal{R}(f)$*.*

Formes de Noether= Mineurs de $\mathcal{R}(f)$.

$m(f,g) \leq d^2 - 1$

On pose :

$$\mathbf{Spect}_{f,g}(U,V) := \mathbf{pgcd}\big(\Phi_t(Uf - Vg)\big)$$

On a :

$$Spect_{f,g}(\lambda,\mu) = 0 \iff (\lambda : \mu) \in \sigma(f,g)$$

Donc :

$$Spect_{f,g}(U,V) = \prod_{(\lambda_i:\mu_i)\in\sigma(f,g)} (U\mu_i - V\lambda_i)^{m_i},$$

Le nombre de facteurs absolument irréductibles (avec multiplicités) de $\lambda_i f - \mu_i g$ est inférieur à m_i.

$$m(f,g) \leq \sum_{(\lambda_i:\mu_i)\in\sigma(f,g)} m_i = \deg Spect_{f,g}(U,V) \leq d^2 - 1$$

$m(f,g) \leq d^2 - 1$

On pose :

$$\mathbf{Spect_{f,g}(U,V) := \mathrm{pgcd}\big(\Phi_t(Uf - Vg)\big)}$$

On a :

$$Spect_{f,g}(\lambda,\mu) = 0 \iff (\lambda : \mu) \in \sigma(f,g)$$

Donc :

$$\mathbf{Spect_{f,g}(U,V) = \prod_{(\lambda_i:\mu_i)\in\sigma(f,g)} (U\mu_i - V\lambda_i)^{m_i},}$$

Le nombre de facteurs absolument irréductibles (avec multiplicités) de $\lambda_i f - \mu_i g$ est inférieur à m_i.

$$\mathbf{m(f,g)} \leq \sum_{(\lambda_i:\mu_i)\in\sigma(f,g)} m_i = \deg Spect_{f,g}(U,V) \leq \mathbf{d^2 - 1}$$

$m(f,g) \leq d^2 - 1$

On pose :

$$\boldsymbol{Spect_{f,g}(U,V) := \mathrm{pgcd}\big(\Phi_t(Uf - Vg)\big)}$$

On a :

$$Spect_{f,g}(\lambda,\mu) = 0 \iff (\lambda : \mu) \in \sigma(f,g)$$

Donc :

$$\boldsymbol{Spect_{f,g}(U,V) = \prod_{(\lambda_i:\mu_i)\in\sigma(f,g)} (U\mu_i - V\lambda_i)^{m_i},}$$

Le nombre de facteurs absolument irréductibles (avec multiplicités) de $\lambda_i f - \mu_i g$ est inférieur à m_i.

$$\boldsymbol{m(f,g)} \leq \sum_{(\lambda_i:\mu_i)\in\sigma(f,g)} m_i = \deg Spect_{f,g}(U,V) \leq \boldsymbol{d^2 - 1}$$

Question

Les bornes

$$\deg(\Phi_t) \leq d^2 - 1,$$
$$m(f, g) \leq d^2 - 1,$$

sont elles optimales ?

Nguyen 2011 : Non, pour $\rho(f, g)$.

Remarques : -version creuse quasi-optimale (Busé-C, 2011).

- Stein a montré $\rho(f, 1) \leq d - 1$.

Question

Les bornes

$$\deg(\Phi_t) \leq d^2 - 1,$$
$$m(f,g) \leq d^2 - 1,$$

sont elles optimales ?

Nguyen 2011 : Non, pour $\rho(f,g)$.

Remarques : -version creuse quasi-optimale (Busé-C, 2011).

- Stein a montré $\rho(f,1) \leq d - 1$.

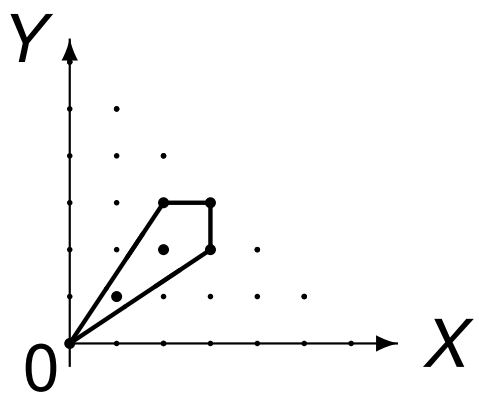
Question

Les bornes

$$\deg(\Phi_t) \leq d^2 - 1,$$
$$m(f,g) \leq d^2 - 1,$$

sont elles optimales ?
Nguyen 2011 : Non, pour $\rho(f,g)$.

Remarques : -version creuse quasi-optimale (Busé-C, 2011).



- Stein a montré $\rho(f,1) \leq d - 1$.

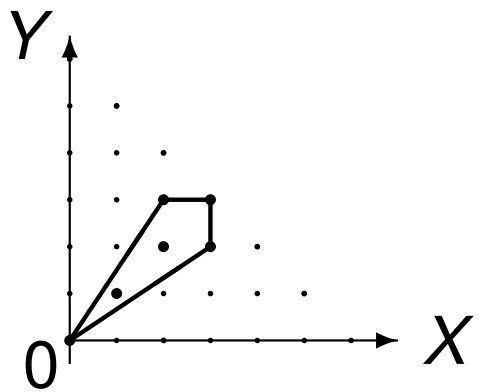
Question

Les bornes

$$\deg(\Phi_t) \leq d^2 - 1,$$
$$m(f,g) \leq d^2 - 1,$$

sont elles optimales ?
Nguyen 2011 : Non, pour $\rho(f,g)$.

Remarques : -version creuse quasi-optimale (Busé-C, 2011).



- Stein a montré $\rho(f,1) \leq d - 1$.

Étude du spectre et de l'indécomposabilité

- **Étude mod *p*** : Théorème à la Ostrowski pour le spectre et l'indécomposabilité.
  Bodin-Dèbes-Najib 2009, C-Najib 2010, Busé-C-Najib 2011

Théorème

$f(X,Y), g(X,Y) \in \mathbb{Z}[X,Y]$,
f/g indécomposable dans $\mathbb{Q}(X,Y)$,
$\exists \mathcal{H}$ t.q. $\mathcal{H} < p \Rightarrow \overline{f}/\overline{g}$ indécomposable dans $\mathbb{F}_p(X,Y)$.

- **Extension algébrique** et indécomposabilité.
  Busé-C-Najib 2011

Étude du spectre et de l'indécomposabilité

- **Étude mod p** : Théorème à la Ostrowski pour le spectre et l'indécomposabilité.
  Bodin-Dèbes-Najib 2009, C-Najib 2010, Busé-C-Najib 2011

Théorème

$f(X,Y), g(X,Y) \in \mathbb{Z}[X,Y]$,
f/g indécomposable dans $\mathbb{Q}(X,Y)$,
$\exists \mathcal{H}$ t.q. $\mathcal{H} < p \Rightarrow \overline{f}/\overline{g}$ indécomposable dans $\mathbb{F}_p(X,Y)$.

- **Extension algébrique** et indécomposabilité.
  Busé-C-Najib 2011

Étude du spectre et de l'indécomposabilité

- **Étude mod p** : Théorème à la Ostrowski pour le spectre et l'indécomposabilité.
  Bodin-Dèbes-Najib 2009, C-Najib 2010, Busé-C-Najib 2011

Théorème

$f(X,Y), g(X,Y) \in \mathbb{Z}[X,Y]$,
f/g indécomposable dans $\mathbb{Q}(X,Y)$,
$\exists \mathcal{H}$ t.q. $\mathcal{H} < p \Rightarrow \overline{f}/\overline{g}$ indécomposable dans $\mathbb{F}_p(X,Y)$.

- **Extension algébrique** et indécomposabilité.
  Busé-C-Najib 2011

Extension algébrique et indécomposabilité

Théorème

Soit $f/g \in \mathbb{K}(X_1, \ldots, X_n)$, *où* $\boldsymbol{n \geq 2}$.

$$f/g \text{ est indécomposable dans } \mathbb{K}(X_1, \ldots, X_n)$$
$$\Updownarrow$$
$$f/g \text{ est indécomposable dans } \overline{\mathbb{K}}(X_1, \ldots, X_n)$$

- Vrai pour les polynômes en une variable : Fried-MacRae 1969.
- Vrai pour les polynômes en plusieurs variables : Ayad 2002.
- Faux pour les fractions rationnelles en une variable : Gutierrez-Sevilla 2006.

Algorithmes de décomposition : approche générale

Entrée : $f \in \mathbb{K}(X_1, \ldots, X_x)$,
Sorties : $u \in \mathbb{K}(T)$, $h \in \mathbb{K}(X_1, \ldots, X_n)$, s'ils existent , tels que $f = u(h)$ où $\deg(u) \geq 2$.

1. Calculer h.
2. Calculer u.

Références :
Polynômes univariés : *Barton-Zippel 1985, Alagar-Thanh 1985, Kozen-Landau 1989.*
Fractions rationnelles univariées : *Zippel 1991, Alonso-Gutierrez-Recio 1995.*
Polynômes n variables : *Dickerson 1987, von zur Gathen 1990.*

Algorithmes de décomposition : approche générale

Entrée : $f \in \mathbb{K}(X_1, \ldots, X_x)$,
Sorties : $u \in \mathbb{K}(T)$, $h \in \mathbb{K}(X_1, \ldots, X_n)$, s'ils existent , tels que $f = u(h)$ où $\deg(u) \geq 2$.

1. Calculer h.
2. Calculer u.

Références :
Polynômes univariés : *Barton-Zippel 1985, Alagar-Thanh 1985, Kozen-Landau 1989*.
Fractions rationnelles univariées : *Zippel 1991, Alonso-Gutierrez-Recio 1995.*
Polynômes n variables : *Dickerson 1987, von zur Gathen 1990.*

Calcul de u

Decomp-u [Zippel, 1991]

Entrée : $f \in \mathbb{K}(X_1, \ldots, X_n)$, h et $\deg f = \deg_{X_n} f$
Sortie : u tel que $f = u \circ h$,

1. Calculer $\overline{f} = f(0, \ldots, 0, T)$, $\overline{h} = h(0, \ldots, 0, T)$.
2. $d_u := \deg(f)/\deg(h)$.
3. Calculer $H(T)$ tel que $\overline{h} \circ H = T \mod T^{2d_u+1}$.
4. Calculer $U = \overline{f} \circ H \mod T^{2d_u+1}$.
5. Calculer u, un $(d_u + 1; d_u)$ approximant de Padé de U.
6. Rendre u.

Preuve : $\overline{f} \circ H = u \circ \overline{h} \circ H = u$.

Complexité : $\tilde{\mathcal{O}}(d^n)$.

Calcul de u

Decomp-u [Zippel, 1991]

Entrée : $f \in \mathbb{K}(X_1, \ldots, X_n)$, h et $\deg f = \deg_{X_n} f$
Sortie : u tel que $f = u \circ h$,

1. Calculer $\overline{f} = f(0, \ldots, 0, T)$, $\overline{h} = h(0, \ldots, 0, T)$.
2. $d_u := \deg(f)/\deg(h)$.
3. Calculer $H(T)$ tel que $\overline{h} \circ H = T \mod T^{2d_u+1}$.
4. Calculer $U = \overline{f} \circ H \mod T^{2d_u+1}$.
5. Calculer u, un $(d_u + 1; d_u)$ approximant de Padé de U.
6. Rendre u.

Preuve : $\overline{f} \circ H = u \circ \overline{h} \circ H = u$.

Complexité : $\tilde{\mathcal{O}}(d^n)$.

Calcul de h à l'espagnole

Théorème (Fried-MacRae 1969, Schicho 1995)

$$f/g = u(h_1/h_2) \in \mathbb{K}(X_1, \ldots, X_n)$$
$$\Updownarrow$$
$$h_1(\underline{X})h_2(\underline{Y}) - h_1(\underline{Y})h_2(\underline{X}) \text{ divise } f(\underline{X})g(\underline{Y}) - f(\underline{Y})g(\underline{X})$$

Algorithme Gutierez-Rubio-Sevilla, 2001 :
Entrée : $f/g \in \mathbb{K}(X_1, \ldots, X_n)$.
Sortie : Une décomposition de f/g, si elle existe.

1. Factoriser $P(\underline{X}, \underline{Y}) = f(\underline{X})g(\underline{Y}) - f(\underline{Y})g(\underline{X})$ dans $\mathbb{K}[\underline{X}, \underline{Y}]$.
2. Pour chaque facteur H de P,
   Si H est $h_1(\underline{X})h_2(\underline{Y}) - h_1(\underline{Y})h_2(\underline{X})$, avec $\deg h_i > 1$
   alors calculer u
   sinon essayer un autre facteur de P.

$\Rightarrow$ complexité exponentielle.

Calcul de h à l'espagnole

Théorème (Fried-MacRae 1969, Schicho 1995)

$$f/g = u(h_1/h_2) \in \mathbb{K}(X_1, \ldots, X_n)$$
$$\Updownarrow$$
$$h_1(\underline{X})h_2(\underline{Y}) - h_1(\underline{Y})h_2(\underline{X}) \text{ divise } f(\underline{X})g(\underline{Y}) - f(\underline{Y})g(\underline{X})$$

Algorithme Gutierez-Rubio-Sevilla, 2001 :
Entrée : $f/g \in \mathbb{K}(X_1, \ldots, X_n)$.
Sortie : Une décomposition de f/g, si elle existe.

1. Factoriser $P(\underline{X}, \underline{Y}) = f(\underline{X})g(\underline{Y}) - f(\underline{Y})g(\underline{X})$ dans $\mathbb{K}[\underline{X}, \underline{Y}]$.
2. Pour chaque facteur H de P,
   Si H est $h_1(\underline{X})h_2(\underline{Y}) - h_1(\underline{Y})h_2(\underline{X})$, avec $\deg h_i > 1$
   alors calculer u
   sinon essayer un autre facteur de P.

$\Rightarrow$ complexité exponentielle.

Calcul de h à l'espagnole

Théorème (Fried-MacRae 1969, Schicho 1995)

$$f/g = u(h_1/h_2) \in \mathbb{K}(X_1, \ldots, X_n)$$
$$\Updownarrow$$
$$h_1(\underline{X})h_2(\underline{Y}) - h_1(\underline{Y})h_2(\underline{X}) \text{ divise } f(\underline{X})g(\underline{Y}) - f(\underline{Y})g(\underline{X})$$

Algorithme Gutierez-Rubio-Sevilla, 2001 :
Entrée : $f/g \in \mathbb{K}(X_1, \ldots, X_n)$.
Sortie : Une décomposition de f/g, si elle existe.

1. Factoriser $P(\underline{X}, \underline{Y}) = f(\underline{X})g(\underline{Y}) - f(\underline{Y})g(\underline{X})$ dans $\mathbb{K}[\underline{X}, \underline{Y}]$.
2. Pour chaque facteur H de P,
   Si H est $h_1(\underline{X})h_2(\underline{Y}) - h_1(\underline{Y})h_2(\underline{X})$, avec $\deg h_i > 1$
   alors calculer u
   sinon essayer un autre facteur de P.

$\Rightarrow$ complexité exponentielle.

Théorème (Lüroth)

Soit $\mathbb{L}$ *un corps tel que* $\mathbb{K} \subsetneq \mathbb{L} \subsetneq \mathbb{K}(X_1, \ldots, X_n)$ *et* $trdeg_{\mathbb{K}}\mathbb{L} = 1$ *alors il existe* $f/g \in \mathbb{K}(X_1, \ldots, X_n)$ *tel que* $\mathbb{L} = \mathbb{K}(f/g)$.

Gutierez-Rubio-Sevilla (2001) :

- Algorithme pour calculer le générateur de Lüroth, lorsque $\mathbb{L} = \mathbb{K}(f_1/g_1, \ldots, f_t/g_t)$.
- correspondance entre les extensions intermédiaires $\mathbb{L}$ de

$$\mathbb{K}(f/g) \subset \mathbb{L} \subset \mathbb{K}(X_1, \ldots, X_n)$$

de degré de transcendance 1, et les décompositions de f/g.

Idée : Si $\mathbb{L} = \mathbb{K}(f_1/g_1, \ldots, f_t/g_t) = \mathbb{K}(h)$ alors $f_i/g_i = u_i(h)$.
h est un "facteur commun".
Calculs de pgcd à la place des factorisations.

Théorème (Lüroth)

Soit $\mathbb{L}$ *un corps tel que* $\mathbb{K} \subsetneq \mathbb{L} \subsetneq \mathbb{K}(X_1, \ldots, X_n)$ *et* $trdeg_{\mathbb{K}}\mathbb{L} = 1$ *alors il existe* $f/g \in \mathbb{K}(X_1, \ldots, X_n)$ *tel que* $\mathbb{L} = \mathbb{K}(f/g)$.

Gutierez-Rubio-Sevilla (2001) :

- Algorithme pour calculer le générateur de Lüroth, lorsque $\mathbb{L} = \mathbb{K}(f_1/g_1, \ldots, f_t/g_t)$.
- correspondance entre les extensions intermédiaires $\mathbb{L}$ de

$$\mathbb{K}(f/g) \subset \mathbb{L} \subset \mathbb{K}(X_1, \ldots, X_n)$$

de degré de transcendance 1, et les décompositions de f/g.

Idée : Si $\mathbb{L} = \mathbb{K}(f_1/g_1, \ldots, f_t/g_t) = \mathbb{K}(h)$ alors $f_i/g_i = u_i(h)$.
h est un "facteur commun".
Calculs de pgcd à la place des factorisations.

Calcul de h avec le spectre

Si $f = u(h)$ avec h indécomposable
alors $f - \mu = \prod_i (h - \mu_i)$, où $u(\mu_i) = \mu$.

Algorithme probabiliste :
Si $\mu_i \notin \sigma(h, 1)$ alors les facteurs irréductibles de $f - \mu$ donnent h.

Complexité : (C. 2010)
Algorithme probabiliste : $\tilde{\mathcal{O}}(d^n)$.
Algorithme déterministe : $\tilde{\mathcal{O}}(d^{n+\omega+2})$.

Remarque : En ne considérant que les facteurs irréductibles l'algorithme Gutierez-Rubio-Sevilla est correct et polynomial.

Faisons le point

Factorisation (formes de Noether)

$\Downarrow$

Borne sur le spectre (factorisation de $\lambda f - \mu g$)

$m(f, g) \leq d^2 - 1$

$\Downarrow$

Algorithme de décomposition :

Algo déterministe $\tilde{\mathcal{O}}(d^{n+\omega+2})$

$\swarrow$ $\qquad$ $\searrow$

Moulin Ollagnier (2004) :

$\tilde{\mathcal{O}}(d^{n\omega})$

$\Downarrow$

Intégrale première rationnelle

Gutierez-Rubio-Sevilla (2001) :

$\tilde{\mathcal{O}}(2^d) \rightsquigarrow \tilde{\mathcal{O}}(d^{2n+\omega-1})$

Faisons le point

Factorisation (formes de Noether)

$\Downarrow$

Borne sur le spectre (factorisation de $\lambda f - \mu g$)

$m(f, g) \leq d^2 - 1$

$\Downarrow$

Algorithme de décomposition :

Algo déterministe $\tilde{\mathcal{O}}(d^{n+\omega+2})$

$\swarrow$ $\qquad$ $\searrow$

Moulin Ollagnier (2004) : $\tilde{\mathcal{O}}(d^{n\omega})$

$\Downarrow$

Intégrale première rationnelle

Gutierez-Rubio-Sevilla (2001) : $\tilde{\mathcal{O}}(2^d) \rightsquigarrow \tilde{\mathcal{O}}(d^{2n+\omega-1})$

Faisons le point

Factorisation (formes de Noether)

$\Downarrow$

Borne sur le spectre (factorisation de $\lambda f - \mu g$)

$m(f, g) \leq d^2 - 1$

$\Downarrow$

Algorithme de décomposition :

Algo déterministe $\tilde{\mathcal{O}}(d^{n+\omega+2})$

$\swarrow$ $\qquad$ $\searrow$

Moulin Ollagnier (2004) :

$\tilde{\mathcal{O}}(d^{n\omega})$

$\Downarrow$

Intégrale première rationnelle

Gutierez-Rubio-Sevilla (2001) :

$\tilde{\mathcal{O}}(2^d) \rightsquigarrow \tilde{\mathcal{O}}(d^{2n+\omega-1})$

Faisons le point

Factorisation (formes de Noether)

$\Downarrow$

Borne sur le spectre (factorisation de $\lambda f - \mu g$)

$m(f, g) \leq d^2 - 1$

$\Downarrow$

Algorithme de décomposition :

Algo déterministe $\tilde{\mathcal{O}}(d^{n+\omega+2})$

$\swarrow$ $\qquad$ $\searrow$

Moulin Ollagnier (2004) :

$\tilde{\mathcal{O}}(d^{n\omega})$

$\Downarrow$

Intégrale première rationnelle

Gutierez-Rubio-Sevilla (2001) :

$\tilde{\mathcal{O}}(2^d) \rightsquigarrow \tilde{\mathcal{O}}(d^{2n+\omega-1})$

Une nouvelle situation ?

$$(S)\ \begin{cases} \dot{X} = A(X, Y), \\ \dot{Y} = B(X, Y), \end{cases} \quad \text{où } A(X, Y), B(X, Y) \in \mathbb{K}[X, Y],$$

$\mathbb{K}$ est un corps de caractéristique zéro,
A et B sont premiers entre eux et $\deg A, \deg B \leq d$.

Nous souhaitons calculer (si elle existe) $F \in \mathbb{K}(X, Y)$ telle ques $F(X(t), Y(t)) = c$.
On dit que F est une intégrale première rationnelle.

Une nouvelle situation ?

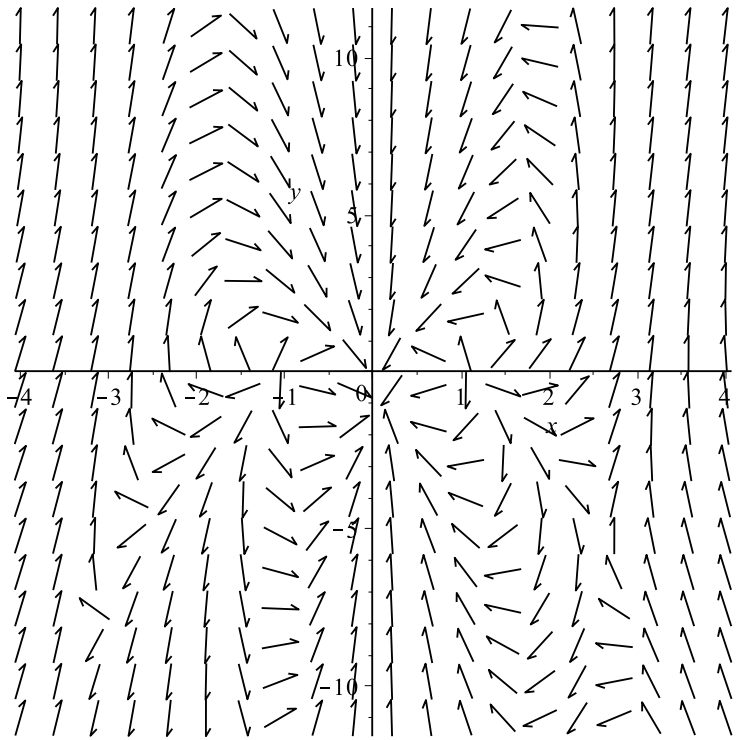
$$(S)\ \begin{cases} \dot{X} = A(X, Y), \\ \dot{Y} = B(X, Y), \end{cases} \quad \text{où } A(X, Y), B(X, Y) \in \mathbb{K}[X, Y],$$

$\mathbb{K}$ est un corps de caractéristique zéro,
A et B sont premiers entre eux et $\deg A, \deg B \leq d$.

Nous souhaitons calculer (si elle existe) $F \in \mathbb{K}(X, Y)$ telle ques $F(X(t), Y(t)) = c$.
On dit que F est une intégrale première rationnelle.

Un dessin

$$(S)\quad \begin{cases} \dot{X} = 2\,YX^4 - 2\,Y - Y^2X^2 + X^6 - X^2 + Y^2 - X^4 + 1 + X^3Y^2 \\ \qquad -20\,YX^3 + 18\,XY, \\ \dot{Y} = -9 + 9\,Y - 3\,X^2Y + 2\,XY + 30\,X^2 - 32\,X^4 + 9\,Y^2 - 30\,Y^2X^2 - 4\,YX^3 - 9\,Y^3 - 2\,XY^3 \\ \qquad -X^6Y + 5\,X^4Y^2 + 3\,X^2Y^3 + 10\,X^6 + X^8 + 4\,X^3Y^2 + 27\,YX^4 + 2\,YX^5, \end{cases}$$



Un dessin

$$F(X,Y) = \frac{\big(Y - X(X-3)(X+3)\big)(Y + X^2 - 1)}{Y^2 + X^4 - 1}$$

est une intégrale première rationnelle.

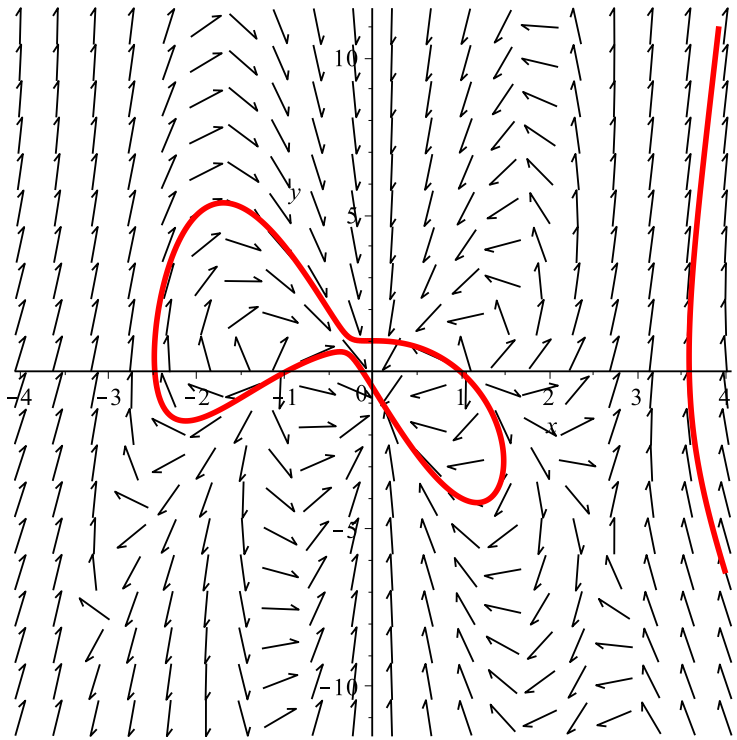


FIGURE: $F(X,Y) = 1$

Un dessin

$$F(X,Y) = \frac{\big(Y - X(X-3)(X+3)\big)(Y + X^2 - 1)}{Y^2 + X^4 - 1}$$

est une intégrale première rationnelle.

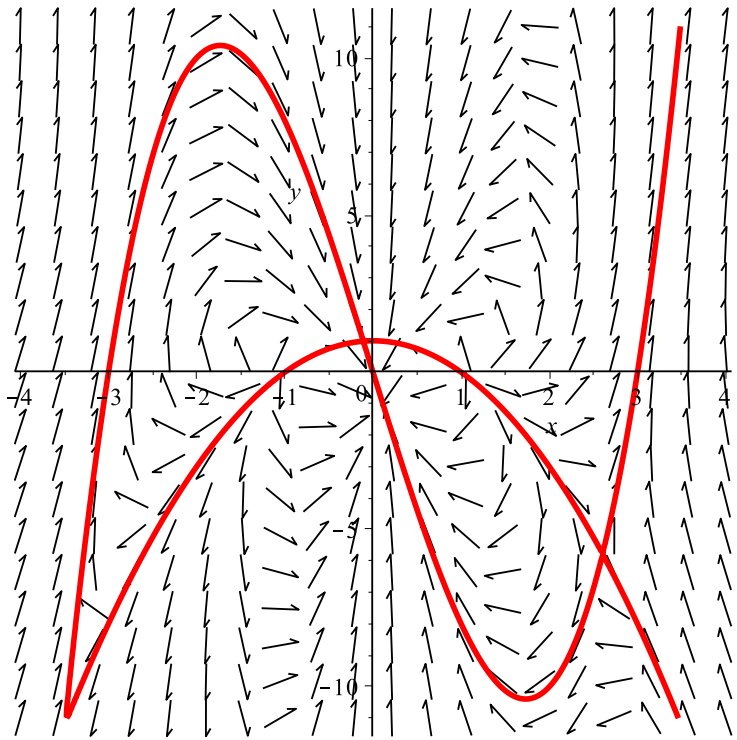


FIGURE: $F(X,Y) = 0$

La dérivation associée

Définition

$$\mathcal{D} = A(X, Y)\partial_X + B(X, Y)\partial_Y.$$

Définition

$F \in \mathbb{K}(X, Y) \setminus \mathbb{K}$ est une intégrale première rationnelle signifie $\mathcal{D}(F) = 0$.

$(X(t), Y(t))$ orbite et F intégrale première

$$\begin{aligned} \Rightarrow F(X(t), Y(t))' &= \partial_X F(X(t), Y(t)).\dot{X}(t) + \partial_Y F(X(t), Y(t)).\dot{Y}(t) \\ &= \mathcal{D}(F)(X(t), Y(t)) = 0 \\ \Rightarrow F(X(t), Y(t)) &= c. \end{aligned}$$

La dérivation associée

Définition

$$\mathcal{D} = A(X, Y)\partial_X + B(X, Y)\partial_Y.$$

Définition

$F \in \mathbb{K}(X, Y) \setminus \mathbb{K}$ est une intégrale première rationnelle signifie $\mathcal{D}(F) = 0$.

$\big(X(t), Y(t)\big)$ orbite et F intégrale première

$$\begin{aligned}
\Rightarrow F\big(X(t), Y(t)\big)' &= \partial_X F\big(X(t), Y(t)\big).\dot{X}(t) + \partial_Y F\big(X(t), Y(t)\big).\dot{Y}(t) \\
&= \mathcal{D}(F)\big(X(t), Y(t)\big) = 0 \\
\Rightarrow F\big(X(t), Y(t)\big) &= c.
\end{aligned}$$

Noyau d'une dérivation et indécomposabilité

Remarque : Si F est un intégrale première alors on peut toujours supposer F indécomposable.

$F = u(h)$
$\Rightarrow \mathcal{D}(F) = 0 = u'(h)\mathcal{D}(h)$
$\Rightarrow \mathcal{D}(h) = 0$ car $\deg(u) \geq 2$.

Proposition

On pose : $\mathbb{K}(X,Y)^{\mathcal{D}} = \{F/G \in \mathbb{K}(X,Y) \mid \mathcal{D}(F/G) = 0\}$.
Lorsque $\mathbb{K}(X,Y)^{\mathcal{D}} \neq \mathbb{K}$, *nous avons :*

$$\mathbb{K}(X,Y)^{\mathcal{D}} = \mathbb{K}\left(\frac{f}{g}\right)$$

où $\frac{f}{g}$ *est indécomposable.*

Noyau d'une dérivation et indécomposabilité

Remarque : Si F est un intégrale première alors on peut toujours supposer F indécomposable.

$F = u(h)$
$\Rightarrow \mathcal{D}(F) = 0 = u'(h)\mathcal{D}(h)$
$\Rightarrow \mathcal{D}(h) = 0$ car $\deg(u) \geq 2$.

Proposition

On pose : $\mathbb{K}(X,Y)^{\mathcal{D}} = \{F/G \in \mathbb{K}(X,Y) \mid \mathcal{D}(F/G) = 0\}$.
Lorsque $\mathbb{K}(X,Y)^{\mathcal{D}} \neq \mathbb{K}$*, nous avons :*

$$\mathbb{K}(X,Y)^{\mathcal{D}} = \mathbb{K}\left(\frac{f}{g}\right)$$

où $\frac{f}{g}$ *est indécomposable.*

Preuve

Nous avons : $\mathbb{K} \subset \mathbb{K}(X, Y)^{\mathcal{D}} \subset \mathbb{K}(X, Y)$
$\Rightarrow \mathbb{K}(X, Y)^{\mathcal{D}} = \mathbb{K}(f_1, f_2, f_3)$, où $f_i \in \mathbb{K}(X, Y)$.

Comme $A\partial_X f_i + B\partial_Y f_i = 0$, on obtient :

$$\partial_Y f_i . \partial_X f_j - \partial_X f_i . \partial_Y f_j = 0.$$

$\Rightarrow$ (critère jacobien + thm Lüroth)
$\mathbb{K}(X, Y)^{\mathcal{D}} = \mathbb{K}(F)$, où $F \in \mathbb{K}(X, Y)$.

Si $F = u(h)$ avec $\deg(u) \geq 2$ alors $\mathbb{K}(F) \subsetneq \mathbb{K}(h) \subset \mathbb{K}(X, Y)^{\mathcal{D}}$: absurde.

Preuve

Nous avons : $\mathbb{K} \subset \mathbb{K}(X, Y)^{\mathcal{D}} \subset \mathbb{K}(X, Y)$
$\Rightarrow \mathbb{K}(X, Y)^{\mathcal{D}} = \mathbb{K}(f_1, f_2, f_3)$, où $f_i \in \mathbb{K}(X, Y)$.

Comme $A\partial_X f_i + B\partial_Y f_i = 0$, on obtient :

$$\partial_Y f_i . \partial_X f_j - \partial_X f_i . \partial_Y f_j = 0.$$

$\Rightarrow$ (critère jacobien + thm Lüroth)
$\mathbb{K}(X, Y)^{\mathcal{D}} = \mathbb{K}(F)$, où $F \in \mathbb{K}(X, Y)$.

Si $F = u(h)$ avec $\deg(u) \geq 2$ alors $\mathbb{K}(F) \subsetneq \mathbb{K}(h) \subset \mathbb{K}(X, Y)^{\mathcal{D}}$: absurde.

Preuve

Nous avons : $\mathbb{K} \subset \mathbb{K}(X, Y)^{\mathcal{D}} \subset \mathbb{K}(X, Y)$
$\Rightarrow \mathbb{K}(X, Y)^{\mathcal{D}} = \mathbb{K}(f_1, f_2, f_3)$, où $f_i \in \mathbb{K}(X, Y)$.

Comme $A\partial_X f_i + B\partial_Y f_i = 0$, on obtient :

$$\partial_Y f_i . \partial_X f_j - \partial_X f_i . \partial_Y f_j = 0.$$

$\Rightarrow$ (critère jacobien + thm Lüroth)
$\mathbb{K}(X, Y)^{\mathcal{D}} = \mathbb{K}(F)$, où $F \in \mathbb{K}(X, Y)$.

Si $F = u(h)$ avec $\deg(u) \geq 2$ alors $\mathbb{K}(F) \subsetneq \mathbb{K}(h) \subset \mathbb{K}(X, Y)^{\mathcal{D}}$: absurde.

Intégrale première et clôture algébrique

Théorème (Man-MacCallum 1997, Bostan-C.-Cluzeau-Weil 2015)

Soit $\mathcal{D} = A(X,Y)\partial_X + B(X,Y)\partial_Y$ *une dérivation avec* $A, B \in \mathbb{K}[X,Y]$.
Si $\mathcal{D}$ *possède une intégrale première dans* $\overline{\mathbb{K}}(X,Y)$
alors $\mathcal{D}$ *possède une intégrale première dans* $\mathbb{K}(X,Y)$
de même degré.

Preuve

Soit f telle que $\overline{\mathbb{K}}(X, Y)^{\mathcal{D}} = \overline{\mathbb{K}}(f)$.
On considère

$$N(f) = \prod_{\sigma_i \in G} \sigma_i(f).$$

$\Rightarrow N(f) \in \mathbb{K}(X, Y)$ et $N(f)$ est aussi une intégrale première.
$\Rightarrow$ Il existe une intégrale première F dans $\mathbb{K}(X, Y)$ indécomposable.

$F(X, Y) \in \overline{\mathbb{K}}(X, Y)^{\mathcal{D}} = \overline{\mathbb{K}}(f) \Rightarrow F = u(f)$
Or F indécomposable dans $\overline{\mathbb{K}}(X, Y)$ car indécomposable dans $\mathbb{K}(X, Y)$.
$\Rightarrow \deg(u) = 1$ et $\deg(f) = \deg(F)$.

Preuve

Soit f telle que $\overline{\mathbb{K}}(X, Y)^{\mathcal{D}} = \overline{\mathbb{K}}(f)$.
On considère

$$N(f) = \prod_{\sigma_i \in G} \sigma_i(f).$$

$\Rightarrow N(f) \in \mathbb{K}(X, Y)$ et $N(f)$ est aussi une intégrale première.
$\Rightarrow$ Il existe une intégrale première F dans $\mathbb{K}(X, Y)$ indécomposable.

$F(X, Y) \in \overline{\mathbb{K}}(X, Y)^{\mathcal{D}} = \overline{\mathbb{K}}(f) \Rightarrow F = u(f)$
Or F indécomposable dans $\overline{\mathbb{K}}(X, Y)$ car indécomposable dans $\mathbb{K}(X, Y)$.
$\Rightarrow \deg(u) = 1$ et $\deg(f) = \deg(F)$.

La dérivation jacobienne

Définition

La dérivation jacobienne associée à f est $\mathcal{D}_f = A\partial_X + B\partial_Y$, *où*

$$A = \frac{\partial_Y f}{pgcd(\partial_Y f, \partial_X f)}, B = \frac{-\partial_X f}{pgcd(\partial_Y f, \partial_X f)}.$$

Proposition

Soit $f = u(h) \in \mathbb{K}[X, Y]$, *où* $h \in \mathbb{K}[X, Y]$ *est indécomposable.* $\mathbb{K}[X, Y]^{\mathcal{D}_f} = \mathbb{K}[h]$.

Preuve :

$f = u(h) \Rightarrow \partial_X f = u'(h)\partial_X(h)\,;\ \partial_Y f = u'(h)\partial_Y(h)$

$$\Rightarrow \mathcal{D}_f = \frac{\partial_Y h}{\mathrm{pgcd}(\partial_Y h, \partial_X h)}\partial_X + \frac{-\partial_X h}{\mathrm{pgcd}(\partial_Y h, \partial_X h)}\partial_Y$$

$h \in \ker \mathbb{K}(X, Y)^{\mathcal{D}_f}$

La dérivation jacobienne

Définition

La dérivation jacobienne associée à f est $\mathcal{D}_f = A\partial_X + B\partial_Y$, *où*

$$A = \frac{\partial_Y f}{pgcd(\partial_Y f, \partial_X f)}, \; B = \frac{-\partial_X f}{pgcd(\partial_Y f, \partial_X f)}.$$

Proposition

Soit $f = u(h) \in \mathbb{K}[X, Y]$, *où* $h \in \mathbb{K}[X, Y]$ *est indécomposable.* $\mathbb{K}[X, Y]^{\mathcal{D}_f} = \mathbb{K}[h]$.

Preuve :

$f = u(h) \Rightarrow \partial_X f = u'(h)\partial_X(h)\,;\; \partial_Y f = u'(h)\partial_Y(h)$

$$\Rightarrow \mathcal{D}_f = \frac{\partial_Y h}{\mathrm{pgcd}(\partial_Y h, \partial_X h)}\partial_X + \frac{-\partial_X h}{\mathrm{pgcd}(\partial_Y h, \partial_X h)}\partial_Y$$

$h \in \ker \mathbb{K}(X, Y)^{\mathcal{D}_f}$

L'algorithme de Moulin-Ollagnier

Entrée : $f \in \mathbb{K}[X, Y]$.
Sortie : $h \in \mathbb{K}[X, Y]$ tel que $f = u(h)$.

1. Résoudre $\mathcal{D}_f(H) = 0$ où $\deg(H) \leq \deg(f)$.
2. Rendre $H \in \ker \mathcal{D}_f$ de degré minimal.

Décomposer $\leftrightarrow$ Calculer une intégrale première

L'algorithme de Moulin-Ollagnier

Entrée : $f \in \mathbb{K}[X, Y]$.
Sortie : $h \in \mathbb{K}[X, Y]$ tel que $f = u(h)$.

1. Résoudre $\mathcal{D}_f(H) = 0$ où $\deg(H) \leq \deg(f)$.
2. Rendre $H \in \ker \mathcal{D}_f$ de degré minimal.

Décomposer $\leftrightarrow$ Calculer une intégrale première

Polynômes de Darboux

Remarque :
$\mathcal{D}(f/g) = 0 \iff \mathcal{D}(f)g = f\mathcal{D}(g)$
f divise $\mathcal{D}(f)$ et g divise $\mathcal{D}(g)$.

Définition

*Soit $f \in \overline{\mathbb{K}}[X, Y]$, f est un **polynôme de Darboux** pour la dérivation $\mathcal{D}$ s'il existe $\Lambda \in \overline{\mathbb{K}}[X, Y]$ tel que :*

$$\mathcal{D}(f) = \Lambda.f.$$

*Λ est le **cofacteur** de f, on pose $\Lambda = \mathrm{cof}(f)$.*

Remarque :
Si $\mathcal{D}(f/g) = 0$ alors $\lambda f - \mu g$ sont des polynômes de Darboux.

Polynômes de Darboux

Remarque :
$\mathcal{D}(f/g) = 0 \iff \mathcal{D}(f)g = f\mathcal{D}(g)$
f divise $\mathcal{D}(f)$ et g divise $\mathcal{D}(g)$.

Définition

*Soit $f \in \overline{\mathbb{K}}[X, Y]$, f est un **polynôme de Darboux** pour la dérivation $\mathcal{D}$ s'il existe $\Lambda \in \overline{\mathbb{K}}[X, Y]$ tel que :*

$$\mathcal{D}(f) = \Lambda.f.$$

*Λ est le **cofacteur** de f, on pose $\Lambda = \mathrm{cof}(f)$.*

Remarque :
Si $\mathcal{D}(f/g) = 0$ alors $\lambda f - \mu g$ sont des polynômes de Darboux.

Polynômes de Darboux

Remarque :
$\mathcal{D}(f/g) = 0 \iff \mathcal{D}(f)g = f\mathcal{D}(g)$
f divise $\mathcal{D}(f)$ et g divise $\mathcal{D}(g)$.

Définition

*Soit $f \in \overline{\mathbb{K}}[X, Y]$, f est un **polynôme de Darboux** pour la dérivation $\mathcal{D}$ s'il existe $\Lambda \in \overline{\mathbb{K}}[X, Y]$ tel que :*

$$\mathcal{D}(f) = \Lambda.f.$$

*Λ est le **cofacteur** de f, on pose $\Lambda = \mathrm{cof}(f)$.*

Remarque :
Si $\mathcal{D}(f/g) = 0$ alors $\lambda f - \mu g$ sont des polynômes de Darboux.

Remarques sur les polynômes de Darboux

1. $\boldsymbol{cof(f) = 0 \iff f}$ **est une intégrale première.**

2. $\boldsymbol{f = 0}$ **est une orbite du système différentiel.**
   Preuve :
   Soit (x, y) tel que $f(x, y) = 0$.
   $\mathcal{D}(f) = A\partial_X f + B\partial_Y f = \Lambda.f \Rightarrow \big(A(x, y), B(x, y)\big) \perp \nabla f(x, y)$
   La ligne de niveau $f = 0$ est tangente au vecteur $\big(A(x, y), B(x, y)\big)$.

3. $\boldsymbol{\deg(\mathrm{cof}(f)) \leq \max(\deg(A), \deg(B)) - 1}$,
   $\mathcal{D}(f) = A\partial_X(f) + B\partial_Y(f) = cof(f).f$
   $\Rightarrow d + \deg(f) - 1 \geq \deg(cof(f)) + \deg(f)$

4. $\boldsymbol{\deg(f) \leq ???}$, Poincaré, 1891.

Remarques sur les polynômes de Darboux

1. $\boldsymbol{cof(f) = 0 \iff f}$ **est une intégrale première.**

2. $\boldsymbol{f = 0}$ **est une orbite du système différentiel.**
   Preuve :
   Soit (x, y) tel que $f(x, y) = 0$.
   $\mathcal{D}(f) = A\partial_X f + B\partial_Y f = \Lambda.f \Rightarrow \big(A(x, y), B(x, y)\big) \perp \nabla f(x, y)$
   La ligne de niveau $f = 0$ est tangente au vecteur $\big(A(x, y), B(x, y)\big)$.

3. $\boldsymbol{\deg(\mathrm{cof}(f)) \leq \max(\deg(A), \deg(B)) - 1}$,
   $\mathcal{D}(f) = A\partial_X(f) + B\partial_Y(f) = cof(f).f$
   $\Rightarrow d + \deg(f) - 1 \geq \deg(cof(f)) + \deg(f)$

4. $\boldsymbol{\deg(f) \leq ???}$, Poincaré, 1891.

Remarques sur les polynômes de Darboux

1. $\boldsymbol{cof(f) = 0 \iff f}$ **est une intégrale première.**

2. $\boldsymbol{f = 0}$ **est une orbite du système différentiel.**
   Preuve :
   Soit (x, y) tel que $f(x, y) = 0$.
   $\mathcal{D}(f) = A\partial_X f + B\partial_Y f = \Lambda.f \Rightarrow \big(A(x, y), B(x, y)\big) \perp \nabla f(x, y)$
   La ligne de niveau $f = 0$ est tangente au vecteur $\big(A(x, y), B(x, y)\big)$.

3. $\boldsymbol{\deg(\mathrm{cof}(f)) \leq \max(\deg(A), \deg(B)) - 1}$,
   $\mathcal{D}(f) = A\partial_X(f) + B\partial_Y(f) = cof(f).f$
   $\Rightarrow d + \deg(f) - 1 \geq \deg(cof(f)) + \deg(f)$

4. $\boldsymbol{\deg(f) \leq ???}$, Poincaré, 1891.

Propriété fondamentale

Proposition

Soit $f = f_1.f_2$ *où* f_1, f_2 *sont premiers entre eux.*

$$f \text{ est un polynôme de Darboux.}$$
$$\Updownarrow$$
$$f_1 \text{ et } f_2 \text{ sont des polynômes de Darboux.}$$

De plus, $\mathrm{cof}(f) = \mathrm{cof}(f_1) + \mathrm{cof}(f_2)$.

Remarque :
$\mathrm{cof}(f_1/f_2) = \mathrm{cof}(f_1) - \mathrm{cof}(f_2)$.

Preuve

$\Downarrow$) f est un polynôme de Darboux et $f = f_1.f_2$.

$$\mathcal{D}(f_1)f_2 + f_1\mathcal{D}(f_2) = \mathcal{D}(f) = cof(f).f = cof(f).f_1.f_2$$

$\Uparrow$) f_i sont des polynômes de Darboux de cofacteurs $cof(f_i)$ et $f = f_1.f_2$.

$$\mathcal{D}(f) = \mathcal{D}(f_1.f_2) = cof(f_1).f_1.f_2 + f_1.cof(f_2)f_2 = \big(cof(f_1) + cof(f_2)\big)f.$$

Preuve

$\Downarrow$) f est un polynôme de Darboux et $f = f_1.f_2$.

$$\mathcal{D}(f_1)f_2 + f_1\mathcal{D}(f_2) = \mathcal{D}(f) = cof(f).f = cof(f).f_1.f_2$$

$\Uparrow$) f_i sont des polynômes de Darboux de cofacteurs $cof(f_i)$ et $f = f_1.f_2$.

$$\mathcal{D}(f) = \mathcal{D}(f_1.f_2) = cof(f_1).f_1.f_2 + f_1.cof(f_2)f_2 = \big(cof(f_1) + cof(f_2)\big)f.$$

Le théorème de Darboux, 1878

Théorème

Soient $A, B \in \mathbb{K}[X, Y]$, $\mathcal{D} = A\partial_X + B\partial_Y$, *et*
$d = \max\big(\deg(A), \deg(B)\big)$.
Soient $f_1, \ldots, f_\nu \in \overline{\mathbb{K}}[X, Y]$ *des polynômes de Darboux irréductibles.*
Si $\nu \geq \mathcal{B} + 1$, *où* $\mathcal{B} = d(d+1)/2$, *alors il existe* $e_i \in \overline{\mathbb{K}}$ *tels que :*

$$f = \prod_{i=1}^{\nu} f_i^{e_i} \text{ est une intégrale première.}$$

Preuve du théorème de Darboux

$cof(f) \in \overline{\mathbb{K}}[X, Y]_{\leq d-1}$

$\mathcal{B} = \dim_{\mathbb{K}} \overline{\mathbb{K}}[X, Y]_{\leq d-1}$
Comme $\nu \geq \mathcal{B} + 1$ il existe $e_i \in \overline{\mathbb{K}}$ tels que

$$\sum_{i=1}^{\nu} e_i cof(f_i) = 0 = cof\Big(\prod_{i=1}^{\nu} f_i^{e_i}\Big).$$

$$\Rightarrow \prod_{i=1}^{\nu} f_i^{e_i} \text{ est une intégrale première.}$$

Preuve du théorème de Darboux

$cof(f) \in \overline{\mathbb{K}}[X, Y]_{\leq d-1}$

$\mathcal{B} = \dim_{\mathbb{K}} \overline{\mathbb{K}}[X, Y]_{\leq d-1}$
Comme $\nu \geq \mathcal{B} + 1$ il existe $e_i \in \overline{\mathbb{K}}$ tels que

$$\sum_{i=1}^{\nu} e_i cof(f_i) = 0 = cof\Big(\prod_{i=1}^{\nu} f_i^{e_i}\Big).$$

$$\Rightarrow \prod_{i=1}^{\nu} f_i^{e_i} \text{ est une intégrale première.}$$

Le théorème de Jouanolou, 1979

Théorème

Soient $A, B \in \mathbb{K}[X, Y]$, $\mathcal{D} = A\partial_X + B\partial_Y$, *et*
$d = \max\big(\deg(A), \deg(B)\big)$.
Soient $f_1, \ldots, f_\nu \in \overline{\mathbb{K}}[X, Y]$ *des polynômes de Darboux irréductibles.*
Si $\nu \geq \mathcal{B} + \mathbf{2}$, *où* $\mathcal{B} = d(d+1)/2$, *alors il existe* $e_i \in \mathbb{Z}$ *tels que :*

$$f = \prod_{i=1}^{\nu} f_i^{e_i} \text{ est une intégrale première rationnelle.}$$

Remarques :
- Version creuse optimale, C. 2014.

Facteur intégrant

Définition

$\mathcal{R}$ *est un facteur intégrant* $\iff \mathcal{D}(\mathcal{R}) = -div(A,B).\mathcal{R}.$

Remarque :

$$\mathcal{D}(\mathcal{R}) = -div(A,B)\mathcal{R}$$

$$\Updownarrow$$

$$A\partial_X(\mathcal{R}) + B\partial_Y(\mathcal{R}) = -\big(\partial_X(A) + \partial_Y(B)\big)\mathcal{R}$$

$$\Updownarrow$$

$$\partial_X(\mathcal{R}A) = -\partial_Y(\mathcal{R}B).$$

Facteur intégrant

Définition

$\mathcal{R}$ *est un facteur intégrant* $\iff \mathcal{D}(\mathcal{R}) = -div(A, B).\mathcal{R}.$

Remarque :

$$\mathcal{D}(\mathcal{R}) = -div(A, B)\mathcal{R}$$

$$\Updownarrow$$

$$A\partial_X(\mathcal{R}) + B\partial_Y(\mathcal{R}) = -\big(\partial_X(A) + \partial_Y(B)\big)\mathcal{R}$$

$$\Updownarrow$$

$$\partial_X(\mathcal{R}A) = -\partial_Y(\mathcal{R}B).$$

Preuve du théorème de Jouanolou

Preuve de Darboux $\Rightarrow H_i = \prod_{j=1}^{\mathcal{B}+2} f_j^{e_{i,j}}$ est une intégrale première

$i = 1, 2$.

$\Rightarrow \log(H_i) = \sum_{j=1}^{\mathcal{B}+2} e_{i,j} \log(f_j)$ est une intégrale première.

$\Rightarrow A\partial_X\big(\log(H_i)\big) + B\partial_Y\big(\log(H_i)\big) = 0.$

$\Rightarrow \dfrac{\partial_X\big(\log(H_i)\big)}{B} = \dfrac{-\partial_Y\big(\log(H_i)\big)}{A} = R_i.$

$\exists R_i \in \mathbb{C}(X, Y), \quad AR_i = -\partial_Y\big(\log(H_i)\big), \quad BR_i = \partial_X\big(\log(H_i)\big).$

$\Rightarrow R_i \in \mathbb{C}(X, Y)$ est un facteur intégrant

R_1/R_2 est une intégrale première.

Preuve du théorème de Jouanolou

Preuve de Darboux $\Rightarrow H_i = \prod_{j=1}^{\mathcal{B}+2} f_j^{e_{i,j}}$ est une intégrale première

$i = 1, 2$.

$\Rightarrow \log(H_i) = \sum_{j=1}^{\mathcal{B}+2} e_{i,j} \log(f_j)$ est une intégrale première.

$\Rightarrow A\partial_X\big(\log(H_i)\big) + B\partial_Y\big(\log(H_i)\big) = 0.$

$\Rightarrow \dfrac{\partial_X\big(\log(H_i)\big)}{B} = \dfrac{-\partial_Y\big(\log(H_i)\big)}{A} = R_i.$

$\exists R_i \in \mathbb{C}(X, Y), \quad AR_i = -\partial_Y\big(\log(H_i)\big), \quad BR_i = \partial_X\big(\log(H_i)\big).$

$\Rightarrow R_i \in \mathbb{C}(X, Y)$ est un facteur intégrant

R_1/R_2 est une intégrale première.

Preuve du théorème de Jouanolou

Preuve de Darboux $\Rightarrow H_i = \prod_{j=1}^{\mathcal{B}+2} f_j^{e_{i,j}}$ est une intégrale première

$i = 1, 2$.

$\Rightarrow \log(H_i) = \sum_{j=1}^{\mathcal{B}+2} e_{i,j} \log(f_j)$ est une intégrale première.

$\Rightarrow A\partial_X\big(\log(H_i)\big) + B\partial_Y\big(\log(H_i)\big) = 0.$

$\Rightarrow \dfrac{\partial_X\big(\log(H_i)\big)}{B} = \dfrac{-\partial_Y\big(\log(H_i)\big)}{A} = R_i.$

$\exists R_i \in \mathbb{C}(X, Y), \quad AR_i = -\partial_Y\big(\log(H_i)\big), \quad BR_i = \partial_X\big(\log(H_i)\big).$

$\Rightarrow R_i \in \mathbb{C}(X, Y)$ est un facteur intégrant

R_1/R_2 est une intégrale première.

Preuve du théorème de Jouanolou

Preuve de Darboux $\Rightarrow H_i = \prod_{j=1}^{\mathcal{B}+2} f_j^{e_{i,j}}$ est une intégrale première

$i = 1, 2$.

$\Rightarrow \log(H_i) = \sum_{j=1}^{\mathcal{B}+2} e_{i,j} \log(f_j)$ est une intégrale première.

$\Rightarrow A\partial_X\big(\log(H_i)\big) + B\partial_Y\big(\log(H_i)\big) = 0.$

$\Rightarrow \dfrac{\partial_X\big(\log(H_i)\big)}{B} = \dfrac{-\partial_Y\big(\log(H_i)\big)}{A} = R_i.$

$\exists R_i \in \mathbb{C}(X, Y), \quad AR_i = -\partial_Y\big(\log(H_i)\big), \quad BR_i = \partial_X\big(\log(H_i)\big).$

$\Rightarrow R_i \in \mathbb{C}(X, Y)$ est un facteur intégrant

R_1/R_2 est une intégrale première.

Preuve du théorème de Jouanolou

Preuve de Darboux $\Rightarrow H_i = \prod_{j=1}^{\mathcal{B}+2} f_j^{e_{i,j}}$ est une intégrale première

$i = 1, 2$.

$\Rightarrow \log(H_i) = \sum_{j=1}^{\mathcal{B}+2} e_{i,j} \log(f_j)$ est une intégrale première.

$\Rightarrow A\partial_X\big(\log(H_i)\big) + B\partial_Y\big(\log(H_i)\big) = 0.$

$\Rightarrow \dfrac{\partial_X\big(\log(H_i)\big)}{B} = \dfrac{-\partial_Y\big(\log(H_i)\big)}{A} = R_i.$

$\exists R_i \in \mathbb{C}(X, Y), \quad AR_i = -\partial_Y\big(\log(H_i)\big), \quad BR_i = \partial_X\big(\log(H_i)\big).$

$\Rightarrow R_i \in \mathbb{C}(X, Y)$ est un facteur intégrant

R_1/R_2 est une intégrale première.

Preuve du théorème de Jouanolou

Preuve de Darboux $\Rightarrow H_i = \prod_{j=1}^{\mathcal{B}+2} f_j^{e_{i,j}}$ est une intégrale première

$i = 1, 2$.

$\Rightarrow \log(H_i) = \sum_{j=1}^{\mathcal{B}+2} e_{i,j} \log(f_j)$ est une intégrale première.

$\Rightarrow A\partial_X\big(\log(H_i)\big) + B\partial_Y\big(\log(H_i)\big) = 0.$

$\Rightarrow \dfrac{\partial_X\big(\log(H_i)\big)}{B} = \dfrac{-\partial_Y\big(\log(H_i)\big)}{A} = R_i.$

$\exists R_i \in \mathbb{C}(X, Y), \quad AR_i = -\partial_Y\big(\log(H_i)\big), \quad BR_i = \partial_X\big(\log(H_i)\big).$

$\Rightarrow R_i \in \mathbb{C}(X, Y)$ est un facteur intégrant

R_1/R_2 est une intégrale première.

La méthode de Darboux

Calcul d'une intégrale première rationnelle :

1. Trouver $d(d+1)/2+2$ polynôme de Darboux absolument irréductibles, notés f_i.
2. Calculer les cofacteurs $\mathrm{cof}(f_i)$.
3. Résoudre $\sum_i e_i.\mathrm{cof}(f_i) = 0$, avec $e_i \in \mathbb{Z}$.
4. Rendre $f = \prod_i f_i^{e_i}$.

Preuve : $cof(f) = \sum_i e_i.\mathrm{cof}(f_i) = 0$.

La méthode de Darboux est une méthode de **recombinaison**.

La méthode de Darboux

Calcul d'une intégrale première rationnelle :

1. Trouver $d(d+1)/2+2$ polynôme de Darboux absolument irréductibles, notés f_i.
2. Calculer les cofacteurs $\mathrm{cof}(f_i)$.
3. Résoudre $\sum_i e_i.\mathrm{cof}(f_i) = 0$, avec $e_i \in \mathbb{Z}$.
4. Rendre $f = \prod_i f_i^{e_i}$.

Preuve : $cof(f) = \sum_i e_i.\mathrm{cof}(f_i) = 0$.

La méthode de Darboux est une méthode de **recombinaison**.

La méthode de Darboux

Calcul d'une intégrale première rationnelle :

1. Trouver $d(d+1)/2+2$ polynôme de Darboux absolument irréductibles, notés f_i.
2. Calculer les cofacteurs $\mathrm{cof}(f_i)$.
3. Résoudre $\sum_i e_i.\mathrm{cof}(f_i) = 0$, avec $e_i \in \mathbb{Z}$.
4. Rendre $f = \prod_i f_i^{e_i}$.

Preuve : $cof(f) = \sum_i e_i.\mathrm{cof}(f_i) = 0$.

La méthode de Darboux est une méthode de **recombinaison**.

Algorithme déterministe de décomposition

$$f - \mu = \prod_i (h - \mu_i) = \prod_j f_j,$$

$h - \mu_i$ peut être réductible ($\mu_i \in \sigma(h, 1)$), f_j sont irréductibles.

Remarques :

- f_j sont des polynômes de Darboux pour $\mathcal{D}_f$.
- $h - \mu_1$ est une intégrale première de $\mathcal{D}_f$.
- $h - \mu_1 = \prod f_j^{e_j}$.

$\Rightarrow$ Les exposants e_j s'obtiennent par la méthode de Darboux.

Moulin Ollagnier, 2004 :
Système linéaire en $\mathcal{O}(d^n)$ inconnues, Complexité= $\mathcal{O}(d^{n\omega})$.

C., 2013 :
Système linéaire en $\mathcal{O}(d)$ inconnues, Complexité= $\tilde{\mathcal{O}}(d^{n+\omega-1})$.

Algorithme déterministe de décomposition

$$f - \mu = \prod_i (h - \mu_i) = \prod_j f_j,$$

$h - \mu_i$ peut être réductible ($\mu_i \in \sigma(h, 1)$), f_j sont irréductibles.

Remarques :

- f_j sont des polynômes de Darboux pour $\mathcal{D}_f$.
- $h - \mu_1$ est une intégrale première de $\mathcal{D}_f$.
- $h - \mu_1 = \prod f_j^{e_j}$.

$\Rightarrow$ Les exposants e_j s'obtiennent par la méthode de Darboux.

Moulin Ollagnier, 2004 :
Système linéaire en $\mathcal{O}(d^n)$ inconnues, Complexité= $\mathcal{O}(d^{n\omega})$.

C., 2013 :
Système linéaire en $\mathcal{O}(d)$ inconnues, Complexité= $\tilde{\mathcal{O}}(d^{n+\omega-1})$.

Algorithme déterministe de décomposition

$$f - \mu = \prod_i (h - \mu_i) = \prod_j f_j,$$

$h - \mu_i$ peut être réductible ($\mu_i \in \sigma(h, 1)$), f_j sont irréductibles.

Remarques :

- f_j sont des polynômes de Darboux pour $\mathcal{D}_f$.
- $h - \mu_1$ est une intégrale première de $\mathcal{D}_f$.
- $h - \mu_1 = \prod f_j^{e_j}$.

$\Rightarrow$ Les exposants e_j s'obtiennent par la méthode de Darboux.

Moulin Ollagnier, 2004 :
Système linéaire en $\mathcal{O}(d^n)$ inconnues, Complexité= $\mathcal{O}(d^{n\omega})$.

C., 2013 :
Système linéaire en $\mathcal{O}(d)$ inconnues, Complexité= $\tilde{\mathcal{O}}(d^{n+\omega-1})$.

Algorithme déterministe de décomposition

$$f - \mu = \prod_i (h - \mu_i) = \prod_j f_j,$$

$h - \mu_i$ peut être réductible ($\mu_i \in \sigma(h, 1)$), f_j sont irréductibles.

Remarques :

- f_j sont des polynômes de Darboux pour $\mathcal{D}_f$.
- $h - \mu_1$ est une intégrale première de $\mathcal{D}_f$.
- $h - \mu_1 = \prod f_j^{e_j}$.

$\Rightarrow$ Les exposants e_j s'obtiennent par la méthode de Darboux.

Moulin Ollagnier, 2004 :
Système linéaire en $\mathcal{O}(d^n)$ inconnues, Complexité= $\mathcal{O}(d^{n\omega})$.

C., 2013 :
Système linéaire en $\mathcal{O}(d)$ inconnues, Complexité= $\tilde{\mathcal{O}}(d^{n+\omega-1})$.

Synthèse

Factorisation (formes de Noether)

$\Downarrow$

Spectre (factorisation de $\lambda f - \mu g$) et **décomposition**

$\Downarrow$

Intégrale première rationnelle

$\Downarrow$

Méthode de Darboux pour calculer une intégrale première :
méthode de recombinaison

$\Downarrow$

Bonne complexité pour la décomposition

$\Downarrow$

Fin de la première partie

Synthèse

Factorisation (formes de Noether)

$\Downarrow$

Spectre (factorisation de $\lambda f - \mu g$) et **décomposition**

$\Downarrow$

Intégrale première rationnelle

$\Downarrow$

Méthode de Darboux pour calculer une intégrale première :
méthode de recombinaison

$\Downarrow$

Bonne complexité pour la décomposition

$\Downarrow$

Fin de la première partie

Synthèse

Factorisation (formes de Noether)

$\Downarrow$

Spectre (factorisation de $\lambda f - \mu g$) et **décomposition**

$\Downarrow$

Intégrale première rationnelle

$\Downarrow$

Méthode de Darboux pour calculer une intégrale première :
méthode de recombinaison

$\Downarrow$

Bonne complexité pour la décomposition

$\Downarrow$

Fin de la première partie

Synthèse

Factorisation (formes de Noether)

$\Downarrow$

Spectre (factorisation de $\lambda f - \mu g$) et **décomposition**

$\Downarrow$

Intégrale première rationnelle

$\Downarrow$

Méthode de Darboux pour calculer une intégrale première :
méthode de recombinaison

$\Downarrow$

Bonne complexité pour la décomposition

$\Downarrow$

Fin de la première partie

Synthèse

Factorisation (formes de Noether)

$\Downarrow$

Spectre (factorisation de $\lambda f - \mu g$) et **décomposition**

$\Downarrow$

Intégrale première rationnelle

$\Downarrow$

Méthode de Darboux pour calculer une intégrale première :
méthode de recombinaison

$\Downarrow$

Bonne complexité pour la décomposition

$\Downarrow$

Fin de la première partie

Synthèse

Factorisation (formes de Noether)

$\Downarrow$

Spectre (factorisation de $\lambda f - \mu g$) et **décomposition**

$\Downarrow$

Intégrale première rationnelle

$\Downarrow$

Méthode de Darboux pour calculer une intégrale première :
méthode de recombinaison

$\Downarrow$

Bonne complexité pour la décomposition

$\Downarrow$

Fin de la première partie

A suivre. . .

Des singularités (dessin $\rightarrow$ pas d'intégrales premières rationnelles),

$\Downarrow$

Problème de Poincaré indécidable dans le modèle BSS

$\Downarrow$

Une courbe qui vous laissera en extase (la courbe extatique)

$\Downarrow$

Calcul "effectifs" des polynômes de Darboux de degrés bornés

$\Downarrow$

Calcul d'intégrales premières rationnelles de degrés bornés.

A suivre. . .

Des singularités (dessin $\rightarrow$ pas d'intégrales premières rationnelles),

$\Downarrow$

Problème de Poincaré indécidable dans le modèle BSS

$\Downarrow$

Une courbe qui vous laissera en extase (la courbe extatique)

$\Downarrow$

Calcul "effectifs" des polynômes de Darboux de degrés bornés

$\Downarrow$

Calcul d'intégrales premières rationnelles de degrés bornés.

A suivre. . .

Des singularités (dessin $\rightarrow$ pas d'intégrales premières rationnelles),

$\Downarrow$

Problème de Poincaré indécidable dans le modèle BSS

$\Downarrow$

Une courbe qui vous laissera en extase (la courbe extatique)

$\Downarrow$

Calcul "effectifs" des polynômes de Darboux de degrés bornés

$\Downarrow$

Calcul d'intégrales premières rationnelles de degrés bornés.

A suivre. . .

Des singularités (dessin $\rightarrow$ pas d'intégrales premières rationnelles),

$\Downarrow$

Problème de Poincaré indécidable dans le modèle BSS

$\Downarrow$

Une courbe qui vous laissera en extase (la courbe extatique)

$\Downarrow$

Calcul "effectifs" des polynômes de Darboux de degrés bornés

$\Downarrow$

Calcul d'intégrales premières rationnelles de degrés bornés.

A suivre. . .

Des singularités (dessin $\rightarrow$ pas d'intégrales premières rationnelles),

$\Downarrow$

Problème de Poincaré indécidable dans le modèle BSS

$\Downarrow$

Une courbe qui vous laissera en extase (la courbe extatique)

$\Downarrow$

Calcul "effectifs" des polynômes de Darboux de degrés bornés

$\Downarrow$

Calcul d'intégrales premières rationnelles de degrés bornés.

Contexte

$$(S)\ \begin{cases} \dot{X} = A(X, Y), \\ \dot{Y} = B(X, Y), \end{cases} \quad \text{où } A(X, Y), B(X, Y) \in \mathbb{K}[X, Y],$$

$\mathbb{K}$ est un corps de caractéristique zéro,
A et B sont premiers entre eux et $\deg A, \deg B \leq d$.

$$\mathcal{D} = \boldsymbol{A(X, Y)\partial_X + B(X, Y)\partial_Y}.$$

***f* intégrale première :** $\mathcal{D}(f) = 0$.

***f* polynôme de Darboux :** $\mathcal{D}(f) = \Lambda.f$, où $\Lambda(X, Y) \in \mathbb{K}[X, Y]$.

Contexte

$$(S)\ \begin{cases} \dot{X} = A(X, Y), \\ \dot{Y} = B(X, Y), \end{cases} \quad \text{où } A(X, Y), B(X, Y) \in \mathbb{K}[X, Y],$$

$\mathbb{K}$ est un corps de caractéristique zéro,
A et B sont premiers entre eux et $\deg A, \deg B \leq d$.

$\mathcal{D} = \boldsymbol{A(X, Y)\partial_X + B(X, Y)\partial_Y}$.

***f* intégrale première :** $\mathcal{D}(f) = 0$.

***f* polynôme de Darboux :** $\mathcal{D}(f) = \Lambda.f$, où $\Lambda(X, Y) \in \mathbb{K}[X, Y]$.

Un dessin

$$F(X,Y) = \frac{\big(Y - X(X-3)(X+3)\big)(Y + X^2 - 1)}{Y^2 + X^4 - 1}$$

est une intégrale première rationnelle.

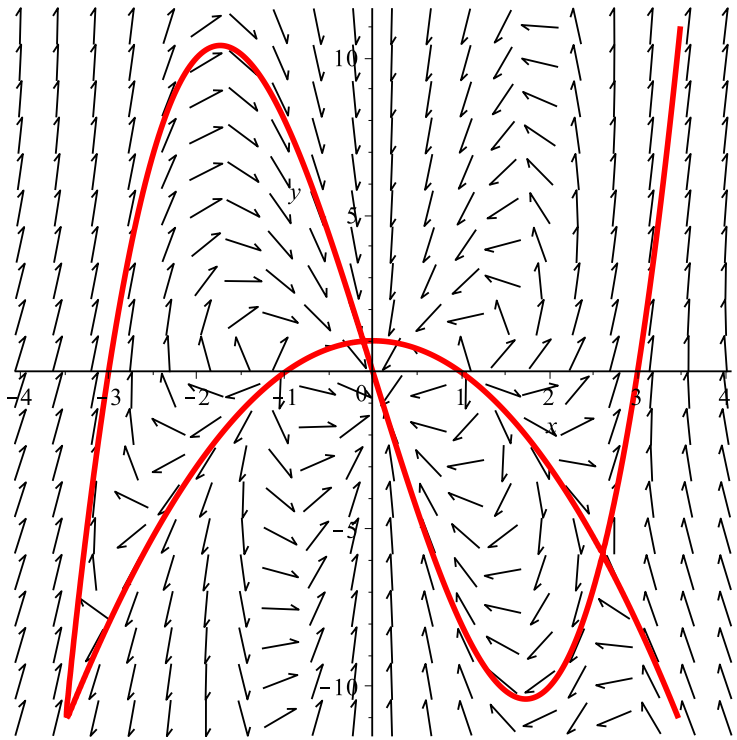


FIGURE: $F(X,Y) = 0$

Singularités

Définition

Soit $\mathcal{D} = A\partial_X + B\partial_Y$. Un point de coordonnées (x, y) est une singularité lorsque $A(x, y) = B(x, y) = 0$.

Exemple : $\dot{X} = aX \ , \ \dot{Y} = bY$
$D_{a,b} = aX\partial_X + bY\partial_Y$.
$(0; 0)$ est une singularité.

$X(t) = c_1 e^{at}$, $Y(t) = c_2 e^{bt}$.
$$\Rightarrow \frac{Y(t)^{a/b}}{X(t)} = c$$

$\frac{Y^{a/b}}{X} \rightsquigarrow$ intégrale première rationnelle $\Rightarrow a/b \in \mathbb{Q}$

Singularités

Proposition

Soit $\mathcal{D} = A\partial_X + B\partial_Y$ une dérivation.
On suppose que $\mathcal{D}$ possède une intégrale première rationnelle (respectivement polynomiale).
Soit (x, y) une singularité.
On suppose qu'au point (x, y) la jacobienne de l'application $(X, Y) \mapsto (A(X, Y), B(X, Y))$ est diagonalisable de valeurs propres a et b.

Dans ce cas a et b sont $\mathbb{Z}$-dépendants (respectivement $\mathbb{N}$-dépendants).

- Se généralise en n variables.

Singularités

Proposition

Soit $\mathcal{D} = A\partial_X + B\partial_Y$ une dérivation.
On suppose que $\mathcal{D}$ possède une intégrale première rationnelle (respectivement polynomiale).
Soit (x, y) une singularité.
On suppose qu'au point (x, y) la jacobienne de l'application $(X, Y) \mapsto (A(X, Y), B(X, Y))$ est diagonalisable de valeurs propres a et b.

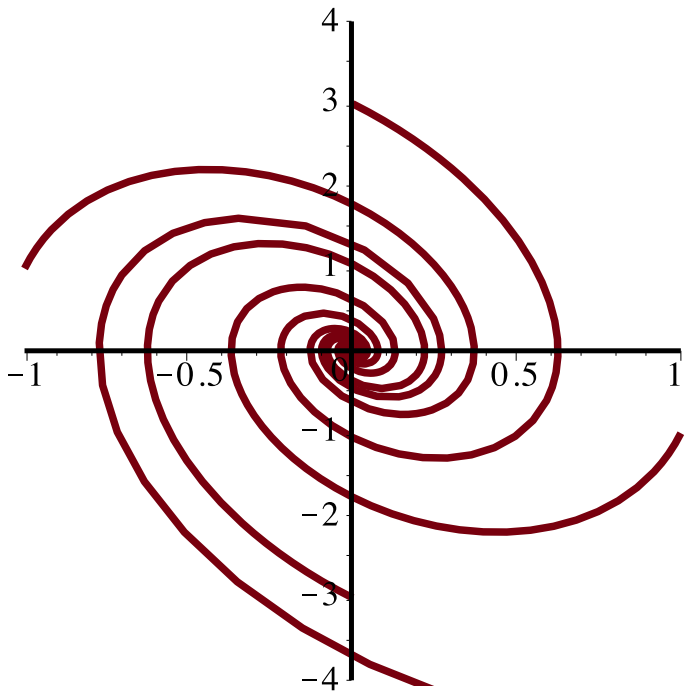
Dans ce cas a et b sont $\mathbb{Z}$-dépendants (respectivement $\mathbb{N}$-dépendants).

- Se généralise en n variables.

Exemple

$D = Y\partial_X + (2Y - 10X)\partial_Y$.
$(0; 0)$ est une singularité.

Les valeurs propres sont $1 + 3i$ et $1 - 3i$.



Comment calculer une intégrale première rationnelle ?

- $\mathcal{D}(f/g) = 0 \iff \mathcal{D}(f).g - f.\mathcal{D}(g) = 0$.
  Si $\deg(f/g)$ borné $\Rightarrow$ résolution d'un système quadratique.

- Recombinaison de polynômes de Darboux irréductibles.

$$\mathcal{D}(f) = \Lambda.f$$

  Si $\deg(f)$ borné $\Rightarrow$ résolution d'un système quadratique.
  ($\deg(\Lambda) \leq d - 1$)

- f/g intégrale première $\Rightarrow$ f et g sont des polynômes de Darboux.

Problème : Soit $\mathcal{D}$ une dérivation.
Peut on borner le degré des polynômes de Darboux irréductibles de $\mathcal{D}$?

Comment calculer une intégrale première rationnelle ?

- $\mathcal{D}(f/g) = 0 \iff \mathcal{D}(f).g - f.\mathcal{D}(g) = 0$.
  Si $\deg(f/g)$ borné $\Rightarrow$ résolution d'un système quadratique.

- Recombinaison de polynômes de Darboux irréductibles.

  $$\mathcal{D}(f) = \Lambda.f$$

  Si $\deg(f)$ borné $\Rightarrow$ résolution d'un système quadratique.
  $(\deg(\Lambda) \leq d - 1)$

- f/g intégrale première $\Rightarrow$ f et g sont des polynômes de Darboux.

Problème : Soit $\mathcal{D}$ une dérivation.
Peut on borner le degré des polynômes de Darboux irréductibles de $\mathcal{D}$?

Le degré des polynômes de Darboux irréductible est borné.

Proposition

Soit $\mathcal{D}$ une dérivation ayant une intégrale première rationnelle f/g.
Si P est un polynôme de Darboux irréductible alors il existe $(\lambda : \mu)$ tel que P divise $\lambda f - \mu g$.

Corollaire

Il existe un entier N dépendant de $\mathcal{D}$ tel que tous les polynômes de Darboux irréductibles sont de degrés inférieurs à N.

Preuve :
Si $\mathcal{D}$ a une infinité de polynômes de Darboux irréductibles alors (Thm. Jouanolou) $\mathcal{D}$ possède une intégrale première rationnelle.

Le degré des polynômes de Darboux irréductible est borné.

Proposition

Soit $\mathcal{D}$ une dérivation ayant une intégrale première rationnelle f/g.
Si P est un polynôme de Darboux irréductible alors il existe $(\lambda : \mu)$ tel que P divise $\lambda f - \mu g$.

Corollaire

Il existe un entier N dépendant de $\mathcal{D}$ tel que tous les polynômes de Darboux irréductibles sont de degrés inférieurs à N.

Preuve :
Si $\mathcal{D}$ a une infinité de polynômes de Darboux irréductibles alors (Thm. Jouanolou) $\mathcal{D}$ possède une intégrale première rationnelle.

LE Problème

Problème de Poincaré (1891) :

Soit $\mathcal{D} = A(X,Y)\partial_X + B(X,Y)\partial_Y$ une dérivation où $A(X,Y), B(X,Y) \in \mathbb{C}[X,Y]$, donner une méthode permettant de calculer une borne N sur le degré des polynômes de Darboux irréductibles de $\mathcal{D}$.

Remarque :

$$\mathcal{D} = X\partial_X - kY\partial_Y$$

admet $X^kY + 1$ comme polynôme de Darboux.

$$\Downarrow$$

On ne peut pas borner N en fonction du degré de la dérivation.

LE Problème

Problème de Poincaré (1891) :

Soit $\mathcal{D} = A(X,Y)\partial_X + B(X,Y)\partial_Y$ une dérivation où $A(X,Y), B(X,Y) \in \mathbb{C}[X,Y]$, donner une méthode permettant de calculer une borne N sur le degré des polynômes de Darboux irréductibles de $\mathcal{D}$.

Remarque :

$$\mathcal{D} = X\partial_X - kY\partial_Y$$

admet $X^kY + 1$ comme polynôme de Darboux.

$$\Downarrow$$

On ne peut pas borner N en fonction du degré de la dérivation.

Machine BSS

Machine BSS (Blum-Shub-Smale) : accepte en entrée des nombres réels, effectue de manière exacte les opérations : $+, -, \times, \div$ et les tests $<, >, \leq, \geq, =$.

Théorème (Blum-Shub-Smale, 1989)

Un ensemble $S \subset \mathbb{R}^n$ est décidable.

$\Updownarrow$

S et $\mathbb{R}^n \setminus S$ sont des unions dénombrables d'ensembles semi-algébriques.

Machine BSS

Machine BSS (Blum-Shub-Smale) : accepte en entrée des nombres réels, effectue de manière exacte les opérations : $+, -, \times, \div$ et les tests $<, >, \leq, \geq, =$.

Théorème (Blum-Shub-Smale, 1989)

Un ensemble $S \subset \mathbb{R}^n$ est décidable.

$$\Updownarrow$$

S et $\mathbb{R}^n \setminus S$ sont des unions dénombrables d'ensembles semi-algébriques.

Indécidabilité du problème de Poincaré dans le modèle BSS

Théorème

Il n'existe pas de machine BSS permettant de décider si une dérivation possède une intégrale première polynomiale.

Corollaire

Il n'existe pas de machine BSS permettant de résoudre le problème de Poincaré.

Preuve :
Si une telle machine existe alors il suffit de résoudre $\mathcal{D}(f) = 0$ où f est un polynôme à coefficients indéterminés et du degré donné par la machine.

Indécidabilité du problème de Poincaré dans le modèle BSS

Théorème

Il n'existe pas de machine BSS permettant de décider si une dérivation possède une intégrale première polynomiale.

Corollaire

Il n'existe pas de machine BSS permettant de résoudre le problème de Poincaré.

Preuve :
Si une telle machine existe alors il suffit de résoudre $\mathcal{D}(f) = 0$ où f est un polynôme à coefficients indéterminés et du degré donné par la machine.

Preuve du théorème

$$\mathcal{D}_\alpha = Xp(X)\partial_X - \big(\alpha p(X) + p'(X)X\big)\,Y\partial_Y,$$

où $\alpha \in \mathbb{C}$, $p(x) \in \mathbb{C}[X]$ sans facteurs carrés tel que $p(0) \neq 0$.
$(0;0)$ est une singularité.
Valeurs propres de la matrice jacobienne $p(0)$ et $-\alpha p(0)$.

$\mathcal{D}_\alpha$ a une intégrale première polynomiale $\iff$ $\alpha \in \mathbb{Q}^+$

$\Rightarrow$) Si $\mathcal{D}_\alpha$ possède une intégrale première polynomiale alors il existe $n_1, n_2 \in \mathbb{N}$ tels que $n_1 p(0) + n_2\big(-\alpha p(0)\big) = 0$.
$\Rightarrow \alpha = n_1/n_2$.

$\Leftarrow$) Si $\alpha = n_1/n_2$ avec $n_1, n_2 \in \mathbb{N}$ alors $f(X,Y) = X^{n_1} p(X) Y^{n_2}$ est une intégrale première polynomiale.

Décider si $\mathcal{D}_\alpha$ possède une intégrale première polynomiale
$\Updownarrow$
décider si $\alpha \in \mathbb{Q}^+$.

Preuve du théorème

$$\mathcal{D}_\alpha = Xp(X)\partial_X - \big(\alpha p(X) + p'(X)X\big)\,Y\partial_Y,$$

où $\alpha \in \mathbb{C}$, $p(x) \in \mathbb{C}[X]$ sans facteurs carrés tel que $p(0) \neq 0$.
$(0;0)$ est une singularité.
Valeurs propres de la matrice jacobienne $p(0)$ et $-\alpha p(0)$.

$\mathcal{D}_\alpha$ a une intégrale première polynomiale $\iff$ $\alpha \in \mathbb{Q}^+$

$\Rightarrow$) Si $\mathcal{D}_\alpha$ possède une intégrale première polynomiale alors il existe $n_1, n_2 \in \mathbb{N}$ tels que $n_1 p(0) + n_2\big(-\alpha p(0)\big) = 0$.
$\Rightarrow \alpha = n_1/n_2$.

$\Leftarrow$) Si $\alpha = n_1/n_2$ avec $n_1, n_2 \in \mathbb{N}$ alors $f(X,Y) = X^{n_1} p(X) Y^{n_2}$ est une intégrale première polynomiale.

Décider si $\mathcal{D}_\alpha$ possède une intégrale première polynomiale

$\Updownarrow$

décider si $\alpha \in \mathbb{Q}^+$.

Preuve du théorème

$$\mathcal{D}_\alpha = Xp(X)\partial_X - \big(\alpha p(X) + p'(X)X\big)\,Y\partial_Y,$$

où $\alpha \in \mathbb{C}$, $p(x) \in \mathbb{C}[X]$ sans facteurs carrés tel que $p(0) \neq 0$.
$(0;0)$ est une singularité.
Valeurs propres de la matrice jacobienne $p(0)$ et $-\alpha p(0)$.

$\mathcal{D}_\alpha$ a une intégrale première polynomiale $\iff$ $\alpha \in \mathbb{Q}^+$

$\Rightarrow$) Si $\mathcal{D}_\alpha$ possède une intégrale première polynomiale alors il existe $n_1, n_2 \in \mathbb{N}$ tels que $n_1 p(0) + n_2\big(-\alpha p(0)\big) = 0$.
$\Rightarrow \alpha = n_1/n_2$.

$\Leftarrow$) Si $\alpha = n_1/n_2$ avec $n_1, n_2 \in \mathbb{N}$ alors $f(X,Y) = X^{n_1} p(X) Y^{n_2}$ est une intégrale première polynomiale.

Décider si $\mathcal{D}_\alpha$ possède une intégrale première polynomiale
$\Updownarrow$
décider si $\alpha \in \mathbb{Q}^+$.

Singularités et bornes sur le degré

Définition

Une singularité est dicritique lorsqu'une infinité d'orbites passent par cette singularité.

Théorème (Carnicer (1994))

Si $P(X, Y)$ est un polynôme de Darboux irréductible et s'il n'y a pas de singularités dicritiques sur la courbe $P(X, Y) = 0$ alors

$$\deg(P) \leq d + 2.$$

Cerveau-Lins Neto (1991), Walcher (2000), Lei-Yang (2006), ...

Singularités et bornes sur le degré

Définition

Une singularité est dicritique lorsqu'une infinité d'orbites passent par cette singularité.

Théorème (Carnicer (1994))

Si $P(X, Y)$ est un polynôme de Darboux irréductible et s'il n'y a pas de singularités dicritiques sur la courbe $P(X, Y) = 0$ alors

$$\deg(P) \leq d + 2.$$

Cerveau-Lins Neto (1991), Walcher (2000), Lei-Yang (2006), ...

Un problème plus simple

$\mathcal{P}_1$: Pour une dérivation donnée $\mathcal{D}$ calculer une intégrale première rationnelle, ou ses polynômes de Darboux irréductibles.

$\mathcal{P}_2$: Pour une dérivation donnée $\mathcal{D}$ et **un entier N donné**, calculer une intégrale première rationnelle, ou ses polynômes de Darboux irréductibles de degrés $\leq N$.

Objectif : Résoudre $\mathcal{P}_2$.

Un problème plus simple

$\mathcal{P}_1$: Pour une dérivation donnée $\mathcal{D}$ calculer une intégrale première rationnelle, ou ses polynômes de Darboux irréductibles.

$\mathcal{P}_2$: Pour une dérivation donnée $\mathcal{D}$ et **un entier *N* donné**, calculer une intégrale première rationnelle, ou ses polynômes de Darboux irréductibles de degrés $\leq N$.

Objectif : Résoudre $\mathcal{P}_2$.

Un problème plus simple

$\mathcal{P}_1$: Pour une dérivation donnée $\mathcal{D}$ calculer une intégrale première rationnelle, ou ses polynômes de Darboux irréductibles.

$\mathcal{P}_2$: Pour une dérivation donnée $\mathcal{D}$ et **un entier *N* donné**, calculer une intégrale première rationnelle, ou ses polynômes de Darboux irréductibles de degrés $\leq N$.

Objectif : Résoudre $\mathcal{P}_2$.

Calcul des polynômes de Darboux de degré borné

Méthode naïve : Resolution du système polynomial :
$\mathcal{D}(f) = \Lambda.f$, où les coefficients de Λ et f sont indéterminés et $\deg(f) \leq N$.

C. 2011 :

Problème : Recombinaison des polynômes de Darboux irréductibles.

$\Rightarrow$ **Complexité exponentielle.**

$$\mathcal{D} = (\partial_Y \mathcal{F})\partial_X - (\partial_X \mathcal{F})\partial_Y, \text{ où } \mathcal{F}(X, Y) = Y \prod_{i=1}^{d-1} (X + i) + X.$$

La dérivation $\mathcal{D}$ possède au moins $2^{d-1} + 1$ polynômes de Darboux de degré $\leq d$.

Preuve : $(X + i)$ Darboux $\Rightarrow \prod_I (X + i)$ Darboux.

Calcul des polynômes de Darboux de degré borné

Méthode naïve : Resolution du système polynomial :
$\mathcal{D}(f) = \Lambda.f$, où les coefficients de Λ et f sont indéterminés et $\deg(f) \leq N$.

C. 2011 :

Problème : Recombinaison des polynômes de Darboux irréductibles.

$\Rightarrow$ **Complexité exponentielle.**

$$\mathcal{D} = (\partial_Y \mathcal{F})\partial_X - (\partial_X \mathcal{F})\partial_Y, \text{ où } \mathcal{F}(X, Y) = Y \prod_{i=1}^{d-1} (X + i) + X.$$

La dérivation $\mathcal{D}$ possède au moins $2^{d-1} + 1$ polynômes de Darboux de degré $\leq d$.

Preuve : $(X + i)$ Darboux $\Rightarrow \prod_I (X + i)$ Darboux.

Calcul des polynômes de Darboux de degré borné

Méthode naïve : Resolution du système polynomial : $\mathcal{D}(f) = \Lambda.f$, où les coefficients de Λ et f sont indéterminés et $\deg(f) \leq N$.

C. 2011 :

Problème : Recombinaison des polynômes de Darboux irréductibles.

$\Rightarrow$ **Complexité exponentielle.**

$$\mathcal{D} = (\partial_Y \mathcal{F})\partial_X - (\partial_X \mathcal{F})\partial_Y, \text{ où } \mathcal{F}(X, Y) = Y \prod_{i=1}^{d-1} (X + i) + X.$$

La dérivation $\mathcal{D}$ possède au moins $2^{d-1} + 1$ polynômes de Darboux de degré $\leq d$.

Preuve : $(X + i)$ Darboux $\Rightarrow \prod_I (X + i)$ Darboux.

Calcul des polynômes de Darboux de degré borné

Méthode naïve : Resolution du système polynomial :
$\mathcal{D}(f) = \Lambda.f$, où les coefficients de Λ et f sont indéterminés et $\deg(f) \leq N$.

C. 2011 :
Problème : Recombinaison des polynômes de Darboux irréductibles.
$\Rightarrow$ **Complexité exponentielle.**

$$\mathcal{D} = (\partial_Y \mathcal{F})\partial_X - (\partial_X \mathcal{F})\partial_Y, \text{ où } \mathcal{F}(X, Y) = Y \prod_{i=1}^{d-1}(X + i) + X.$$

La dérivation $\mathcal{D}$ possède au moins $2^{d-1} + 1$ polynômes de Darboux de degré $\leq d$.

Preuve : $(X + i)$ Darboux $\Rightarrow \prod_I (X + i)$ Darboux.

Contact

Définition

Une courbe paramètrée $\big(x(t), y(t)\big) \in \mathbb{C}[[t]]^2$ *et une courbe implicite* $f(X, Y) = 0$ *ont un ordre de contact* ν *en* $(x_0, y_0) = \big(x(0), y(0)\big)$ *lorsque* ν *est le plus grand entier tel que :*

$$f\big(x(t), y(t)\big) = 0 \mod t^{\nu-1}.$$

Si $\big(x(t), y(t)\big)$ est une orbite du système différentiel alors

$$\begin{aligned} \partial_t\Big(f\big(x(t), y(t)\big)\Big) &= \partial_x f(x(t), y(t)).x'(t) + \partial_y f(x(t), y(t)).y'(t) \\ &= \mathcal{D}(f)\big(x(t), y(t)\big) \end{aligned}$$

$$\Rightarrow f\big(x(t), y(t)\big) = \sum_{j=0}^{\infty} \mathcal{D}^j(f)(x_0, y_0)\frac{t^j}{j!},$$

avec $\mathcal{D}^0(f) = f$ et $\mathcal{D}^k(f) = \mathcal{D}\big(\mathcal{D}^{k-1}(f)\big)$.

Contact

Définition

Une courbe paramètrée $\big(x(t), y(t)\big) \in \mathbb{C}[[t]]^2$ *et une courbe implicite* $f(X, Y) = 0$ *ont un ordre de contact* ν *en* $(x_0, y_0) = \big(x(0), y(0)\big)$ *lorsque* ν *est le plus grand entier tel que :*

$$f\big(x(t), y(t)\big) = 0 \mod t^{\nu-1}.$$

Si $\big(x(t), y(t)\big)$ est une orbite du système différentiel alors

$$\begin{aligned} \partial_t\Big(f\big(x(t), y(t)\big)\Big) &= \partial_x f(x(t), y(t)).x'(t) + \partial_y f(x(t), y(t)).y'(t) \\ &= \mathcal{D}(f)\big(x(t), y(t)\big) \end{aligned}$$

$$\Rightarrow f\big(x(t), y(t)\big) = \sum_{j=0}^{\infty} \mathcal{D}^j(f)(x_0, y_0)\frac{t^j}{j!},$$

avec $\mathcal{D}^0(f) = f$ et $\mathcal{D}^k(f) = \mathcal{D}\big(\mathcal{D}^{k-1}(f)\big)$.

Contact

Définition

Une courbe paramètrée $\big(x(t), y(t)\big) \in \mathbb{C}[[t]]^2$ *et une courbe implicite* $f(X, Y) = 0$ *ont un ordre de contact* ν *en* $(x_0, y_0) = \big(x(0), y(0)\big)$ *lorsque* ν *est le plus grand entier tel que :*

$$f\big(x(t), y(t)\big) = 0 \mod t^{\nu-1}.$$

Si $\big(x(t), y(t)\big)$ est une orbite du système différentiel alors

$$\begin{aligned} \partial_t\Big(f\big(x(t), y(t)\big)\Big) &= \partial_x f(x(t), y(t)).x'(t) + \partial_y f(x(t), y(t)).y'(t) \\ &= \mathcal{D}(f)\big(x(t), y(t)\big) \end{aligned}$$

$$\Rightarrow f\big(x(t), y(t)\big) = \sum_{j=0}^{\infty} \mathcal{D}^j(f)(x_0, y_0)\frac{t^j}{j!},$$

avec $\mathcal{D}^0(f) = f$ et $\mathcal{D}^k(f) = \mathcal{D}\big(\mathcal{D}^{k-1}(f)\big)$.

Système linéaire et contact

$$f(X, Y) \in \mathbb{K}[X, Y]_{\leq N},$$

et f a un contact d'ordre inférieur à $(N+1)(N+2)/2$ en (x_0, y_0) avec une orbite.

$$\Updownarrow$$

$$f(X, Y) \in \ker \begin{pmatrix} v_1 & v_2 & \cdots & v_l \\ \mathcal{D}(v_1) & \mathcal{D}(v_2) & \cdots & \mathcal{D}(v_l) \\ \vdots & \vdots & \cdots & \vdots \\ \mathcal{D}^{l-1}(v_1) & \mathcal{D}^{l-1}(v_2) & \cdots & \mathcal{D}^{l-1}(v_l) \end{pmatrix},$$

où $\{v_1, \ldots, v_l\}$ est une base de $\mathbb{K}[x_0, y_0]_{\leq N}$, et $l = (N+1)(N+2)/2$.

La courbe extatique

Définition

Soit $\mathcal{D}$ une dérivation, la N-ième courbe extatique de $\mathcal{D}$, $\mathcal{E}_N(\mathcal{D})$, est le polynôme

$$\mathcal{E}_N(\mathcal{D}) = \det \begin{pmatrix} v_1 & v_2 & \cdots & v_l \\ \mathcal{D}(v_1) & \mathcal{D}(v_2) & \cdots & \mathcal{D}(v_l) \\ \vdots & \vdots & \cdots & \vdots \\ \mathcal{D}^{l-1}(v_1) & \mathcal{D}^{l-1}(v_2) & \cdots & \mathcal{D}^{l-1}(v_l) \end{pmatrix},$$

où $\{v_1, v_2, \ldots, v_l\}$ est une base de $\mathbb{K}[X, Y]_{\leq N}$,
$l = (N+1)(N+2)/2$, et $\mathcal{D}^k(v_i) = \mathcal{D}\big(\mathcal{D}^{k-1}(v_i)\big)$.

Propriété de la courbe extatique (1)

Proposition (Lagutinski 1911, Pereira 2001)

Les polynômes de Darboux de degré $\leq N$ sont des facteurs de $\mathcal{E}_N(\mathcal{D})$.

La courbe extatique est indépendante de la base choisie.
Nous pouvons prendre une base où $v_1 = P$.
Cela donne :

$$\begin{aligned} \mathcal{D}(P) &= \Lambda_1 P, \\ \mathcal{D}^2(P) &= \mathcal{D}(\Lambda_1 P) = \left(\Lambda_1^2 + \mathcal{D}(\Lambda_1)\right) P = \Lambda_2 P, \\ &\vdots \\ \mathcal{D}^{l-1}(P) &= \Lambda_{l-1} P, \end{aligned}$$

où $\Lambda_1, \Lambda_2, \ldots, \Lambda_{l-1}$ sont des polynômes.
$\Rightarrow$ P est un facteur de la première colonne de $\mathcal{E}_N(\mathcal{D})$.
$\Rightarrow$ P est un facteur de $\mathcal{E}_N(\mathcal{D})$.

Propriété de la courbe extatique (1)

Proposition (Lagutinski 1911, Pereira 2001)

Les polynômes de Darboux de degré $\leq N$ sont des facteurs de $\mathcal{E}_N(\mathcal{D})$.

La courbe extatique est indépendante de la base choisie.
Nous pouvons prendre une base où $v_1 = P$.
Cela donne :

$$\begin{aligned} \mathcal{D}(P) &= \Lambda_1 P, \\ \mathcal{D}^2(P) &= \mathcal{D}(\Lambda_1 P) = \left(\Lambda_1^2 + \mathcal{D}(\Lambda_1)\right) P = \Lambda_2 P, \\ &\vdots \\ \mathcal{D}^{l-1}(P) &= \Lambda_{l-1} P, \end{aligned}$$

où $\Lambda_1, \Lambda_2, \ldots, \Lambda_{l-1}$ sont des polynômes.
$\Rightarrow$ P est un facteur de la première colonne de $\mathcal{E}_N(\mathcal{D})$.
$\Rightarrow$ P est un facteur de $\mathcal{E}_N(\mathcal{D})$.

Exemple 1

$$D = -2X^2\partial_X + (1 - 4XY)\partial_Y$$

$$\Rightarrow \mathcal{E}_1(D) = \det = \begin{vmatrix} 1 & X & Y \\ 0 & -2X^2 & 1 - 4XY \\ 0 & 8X^3 & 24X^2Y - 4X \end{vmatrix} = -16YX^4.$$

$D(X) = -2X.X \Rightarrow X$ est un polynome de Darboux.
$D(Y) = 1 - 4XY \Rightarrow Y$ n'est pas un polynôme de Darboux.

Exemple 2

$D = \partial_X + 3X^2\partial_Y$

$P(X, Y) = Y - X^3$ est une intégrale première.
Les orbites sont du type $Y = X^3 + c$, $c \in \mathbb{C}$.

$$\mathcal{E}_1(D)(X, Y) = \begin{vmatrix} 1 & X & Y \\ 0 & 1 & 3X^2 \\ 0 & 0 & 6X \end{vmatrix} = 6X.$$

X n'est pas un polynôme de Darboux.

Ici $N = 1$ donc $(N + 1)(N + 2)/2 = 3$.

$\mathcal{E}_1(D)(0, y) = 0 \Rightarrow$ il existe un polynôme de degré 1 ayant un contact d'ordre 3 en $(0, y)$ avec une orbite.

Cela signifie qu'en $(0, y)$, la courbe $Y = X^3 + c$ a un point d'inflexion.

Exemple 2

$D = \partial_X + 3X^2\partial_Y$

$P(X, Y) = Y - X^3$ est une intégrale première.
Les orbites sont du type $Y = X^3 + c$, $c \in \mathbb{C}$.

$$\mathcal{E}_1(D)(X, Y) = \begin{vmatrix} 1 & X & Y \\ 0 & 1 & 3X^2 \\ 0 & 0 & 6X \end{vmatrix} = 6X.$$

X n'est pas un polynôme de Darboux.

Ici $N = 1$ donc $(N + 1)(N + 2)/2 = 3$.

$\mathcal{E}_1(D)(0, y) = 0 \Rightarrow$ il existe un polynôme de degré 1 ayant un contact d'ordre 3 en $(0, y)$ avec une orbite.

Cela signifie qu'en $(0, y)$, la courbe $Y = X^3 + c$ a un point d'inflexion.

Exemple 2

$D = \partial_X + 3X^2\partial_Y$

$P(X, Y) = Y - X^3$ est une intégrale première.
Les orbites sont du type $Y = X^3 + c$, $c \in \mathbb{C}$.

$$\mathcal{E}_1(D)(X, Y) = \begin{vmatrix} 1 & X & Y \\ 0 & 1 & 3X^2 \\ 0 & 0 & 6X \end{vmatrix} = 6X.$$

X n'est pas un polynôme de Darboux.

Ici $N = 1$ donc $(N + 1)(N + 2)/2 = 3$.

$\mathcal{E}_1(D)(0, y) = 0 \Rightarrow$ il existe un polynôme de degré 1 ayant un contact d'ordre 3 en $(0, y)$ avec une orbite.

Cela signifie qu'en $(0, y)$, la courbe $Y = X^3 + c$ a un point d'inflexion.

Propriétés de la courbe extatique (2)

Proposition (Lagutinski 1911, Pereira 2001)

$$\mathcal{E}_N(\mathcal{D}) = 0 \text{ et } \mathcal{E}_{N-1}(\mathcal{D}) \neq 0$$

$$\Updownarrow$$

$\mathcal{D}$ a une intégrale première rationnelle indécomposable de degré N.

$\Uparrow$). $\mathcal{D}$ a une intégrale première $f/g \in \mathbb{C}(X, Y)$.
$\mathcal{D}$ a une infinité de polynômes de Darboux de degré N : $\lambda f - \mu g$.
$\mathcal{E}_N(\mathcal{D})$ a une infinité de facteurs non triviaux de degré N.
$\mathcal{E}_N(\mathcal{D}) = 0$.

Propriétés de la courbe extatique (2)

Proposition (Lagutinski 1911, Pereira 2001)

$$\mathcal{E}_N(\mathcal{D}) = 0 \text{ et } \mathcal{E}_{N-1}(\mathcal{D}) \neq 0$$

$$\Updownarrow$$

$\mathcal{D}$ a une intégrale première rationnelle indécomposable de degré N.

$\Uparrow$). $\mathcal{D}$ a une intégrale première $f/g \in \mathbb{C}(X, Y)$.
$\mathcal{D}$ a une infinité de polynômes de Darboux de degré N : $\lambda f - \mu g$.
$\mathcal{E}_N(\mathcal{D})$ a une infinité de facteurs non triviaux de degré N.
$\mathcal{E}_N(\mathcal{D}) = 0$.

Un bout de réciproque

Lemme

Soit $\mathbb{L}$ un corps et $\mathcal{D}$ une dérivation sur $\mathbb{L}$. Nous avons l'équivalence suivante : $g_1, \ldots, g_l \in \mathbb{L}$ sont linéairement dépendants sur $\ker \mathcal{D}$ si et seulement si $W(g_1, \ldots, g_l) = 0$, où

$$W(g_1, \ldots, g_l) = \det \begin{pmatrix} g_1 & g_2 & \ldots & g_l \\ \mathcal{D}(g_1) & \mathcal{D}(g_2) & \ldots & \mathcal{D}(g_l) \\ \vdots & \vdots & \vdots & \vdots \\ \mathcal{D}^{l-1}(g_1) & \mathcal{D}^{l-1}(g_2) & \ldots & \mathcal{D}^{l-1}(g_l) \end{pmatrix}$$

est le Wronskien de $g_1, \ldots, g_l$ relativement à $\mathcal{D}$ et $\ker \mathcal{D}$ est l'ensemble des éléments de $\mathbb{L}$ annulant $\mathcal{D}$.

$\mathbb{L} = \mathbb{K}(X, Y)$, et $\{g_1, \ldots, g_l\}$ une base du $\mathbb{K}$ e.v. $\mathbb{K}[X, Y]_{\leq N}$.
$0 = \mathcal{E}_N(\mathcal{D}) = W(g_1, \ldots, g_l) \Rightarrow g_1, \ldots, g_l$ linéairement dépendants sur $\ker \mathcal{D} = \mathbb{K}(X, Y)^{\mathcal{D}}$.
$\Rightarrow \mathbb{K}(X, Y)^{\mathcal{D}} \neq \mathbb{K}$.

Un bout de réciproque

Lemme

Soit $\mathbb{L}$ un corps et $\mathcal{D}$ une dérivation sur $\mathbb{L}$. Nous avons l'équivalence suivante : $g_1, \ldots, g_l \in \mathbb{L}$ sont linéairement dépendants sur $\ker \mathcal{D}$ si et seulement si $W(g_1, \ldots, g_l) = 0$, où

$$W(g_1, \ldots, g_l) = \det \begin{pmatrix} g_1 & g_2 & \ldots & g_l \\ \mathcal{D}(g_1) & \mathcal{D}(g_2) & \ldots & \mathcal{D}(g_l) \\ \vdots & \vdots & \vdots & \vdots \\ \mathcal{D}^{l-1}(g_1) & \mathcal{D}^{l-1}(g_2) & \ldots & \mathcal{D}^{l-1}(g_l) \end{pmatrix}$$

est le Wronskien de $g_1, \ldots, g_l$ relativement à $\mathcal{D}$ et $\ker \mathcal{D}$ est l'ensemble des éléments de $\mathbb{L}$ annulant $\mathcal{D}$.

$\mathbb{L} = \mathbb{K}(X, Y)$, et $\{g_1, \ldots, g_l\}$ une base du $\mathbb{K}$ e.v. $\mathbb{K}[X, Y]_{\leq N}$.
$0 = \mathcal{E}_N(\mathcal{D}) = W(g_1, \ldots, g_l) \Rightarrow g_1, \ldots, g_l$ linéairement dépendants sur $\ker \mathcal{D} = \mathbb{K}(X, Y)^{\mathcal{D}}$.
$\Rightarrow \mathbb{K}(X, Y)^{\mathcal{D}} \neq \mathbb{K}$.

Complexité polynomiale

C. 2011 :
Soit $\mathcal{D} = A(X,Y)\partial_X + B(X,Y)\partial_Y$ telle que
$A(X,Y), B(X,Y) \in \mathbb{Z}[X,Y]$,
$\deg A \leq d$, $\deg B \leq d$,
$\|A\|_\infty \leq \mathcal{H}$, $\|B\|_\infty \leq \mathcal{H}$ et
A, B sont premiers entre eux.

1. Calcul des polynômes de Darboux irréductibles de degré $\leq N$ de manière déterministe avec $\mathcal{O}\left((dN\log(\mathcal{H}))^{\mathcal{O}(1)}\right)$ opérations binaires.

2. Calcul d'une intégrale première rationnelle de degré $\leq N$ avec $\mathcal{O}\left((dN\log(\mathcal{H}))^{\mathcal{O}(1)}\right)$ opérations binaires.

Complexité polynomiale

C. 2011 :
Soit $\mathcal{D} = A(X, Y)\partial_X + B(X, Y)\partial_Y$ telle que
$A(X, Y), B(X, Y) \in \mathbb{Z}[X, Y]$,
$\deg A \leq d$, $\deg B \leq d$,
$\|A\|_\infty \leq \mathcal{H}$, $\|B\|_\infty \leq \mathcal{H}$ et
A, B sont premiers entre eux.

1. Calcul des polynômes de Darboux irréductibles de degré $\leq N$ de manière déterministe avec $\mathcal{O}\left(\left(dN\log(\mathcal{H})\right)^{\mathcal{O}(1)}\right)$ opérations binaires.

2. Calcul d'une intégrale première rationnelle de degré $\leq N$ avec $\mathcal{O}\left(\left(dN\log(\mathcal{H})\right)^{\mathcal{O}(1)}\right)$ opérations binaires.

Faisons le point

Factorisation = Problème de recombinaison, facteurs dans $\mathbb{K}[[X]][Y]$.

$\Downarrow$

Algorithmes modernes de factorisation = Recombinaison via les dérivées logarithmiques, "méthode de Darboux"

$\Downarrow$

Décomposition = intégrales premières rationnelles, polynômes de Darboux

$\Downarrow$

Calcul des polynômes de Darboux = Problème de recombinaison résolu par la factorisation

Le retour du spectre

Soit f/g une fraction rationnelle indécomposable telle que $\deg(f/g) = N$.

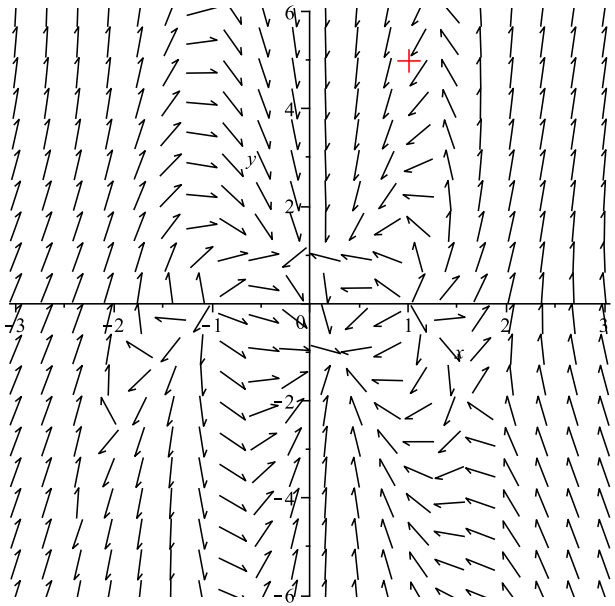
$$D_{f/g} = \left(\partial_Y\left(\frac{f}{g}\right).g^2\right)\partial_X - \left(\partial_X\left(\frac{f}{g}\right).g^2\right)\partial_Y$$

$$\mathbb{K}(X,Y)^{D_{f/g}} = \mathbb{K}\left(\frac{f}{g}\right)$$

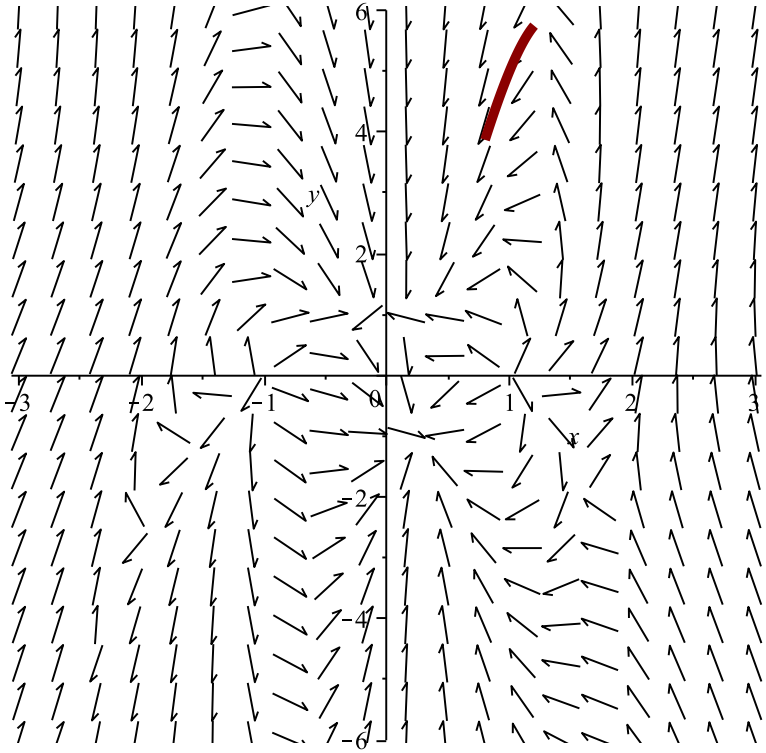
$$P(X,Y) \text{ divise } \lambda f - \mu g \text{ et } \deg(P) < N$$
$$\Downarrow$$
$$P \text{ est un polynôme de Darboux de } D_{f/g} \text{ et } \deg(P) < N.$$
$$\Downarrow$$
$$P \text{ est un facteur de } \mathcal{E}_{N-1}(D_{f/g}) \neq 0.$$
$$\Downarrow$$
$$|\sigma(f,g)| < \infty$$

Calcul d'intégrales premières rationnelles

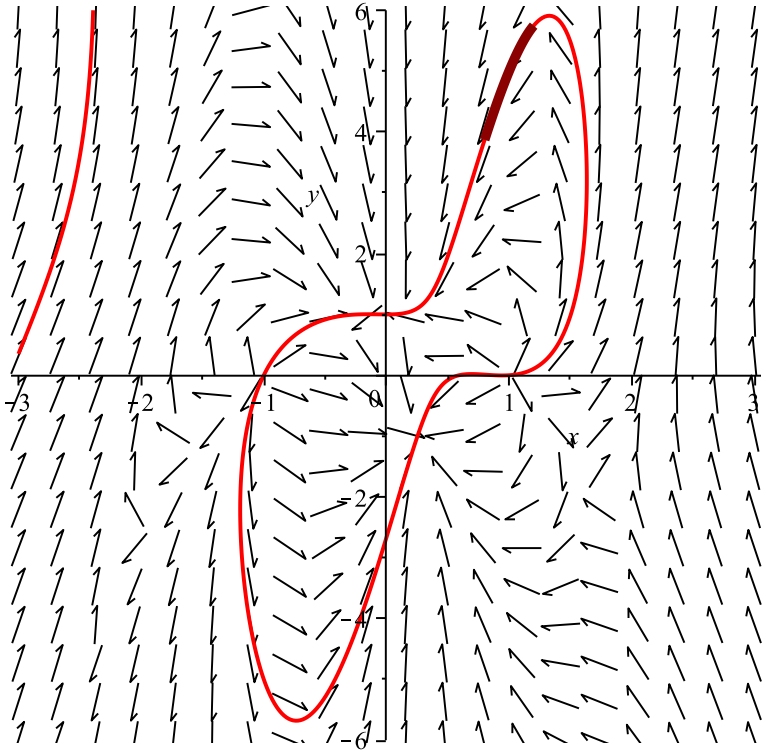
$$(S)\quad \begin{cases} \dot{X} = 2\,YX^4 - 2\,Y - Y^2X^2 + X^6 - X^2 + Y^2 - X^4 + 1 + X^3Y^2 \\ \qquad -20\,YX^3 + 18\,XY, \\ \dot{Y} = -9 + 9\,Y - 3\,X^2Y + 2\,XY + 30\,X^2 - 32\,X^4 + 9\,Y^2 - 30\,Y^2X^2 - 4\,YX^3 - 9\,Y^3 - 2\,XY^3 \\ \qquad -X^6Y + 5\,X^4Y^2 + 3\,X^2Y^3 + 10\,X^6 + X^8 + 4\,X^3Y^2 + 27\,YX^4 + 2\,YX^5, \end{cases} \qquad - X^7 + X^3 - 9\,XY^2 + 9\,X^5 - 9\,X + 2\,YX^5$$



Calcul d'intégrales premières rationnelles

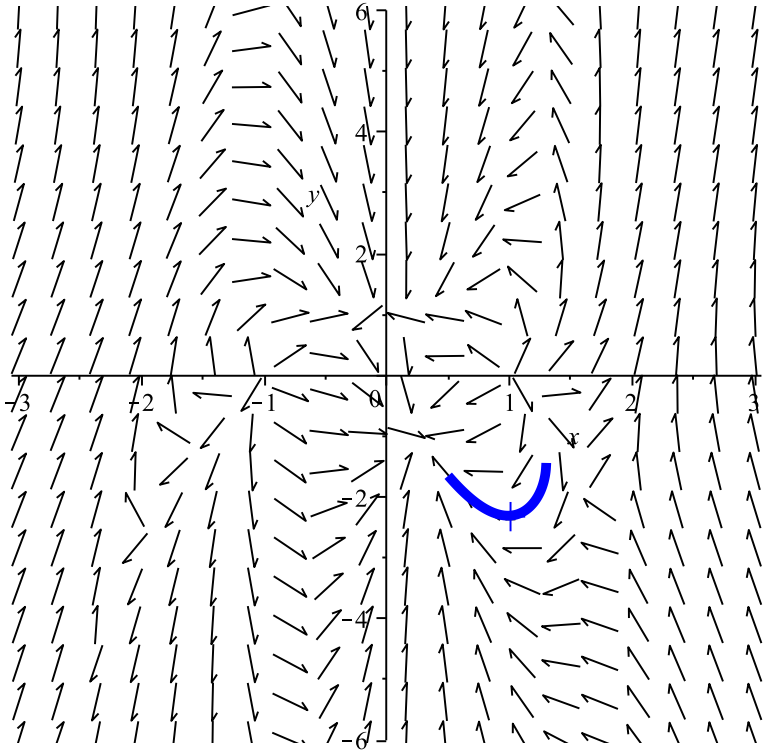


Calcul de $Y_1(X) \in \mathbb{K}[[X]]$.

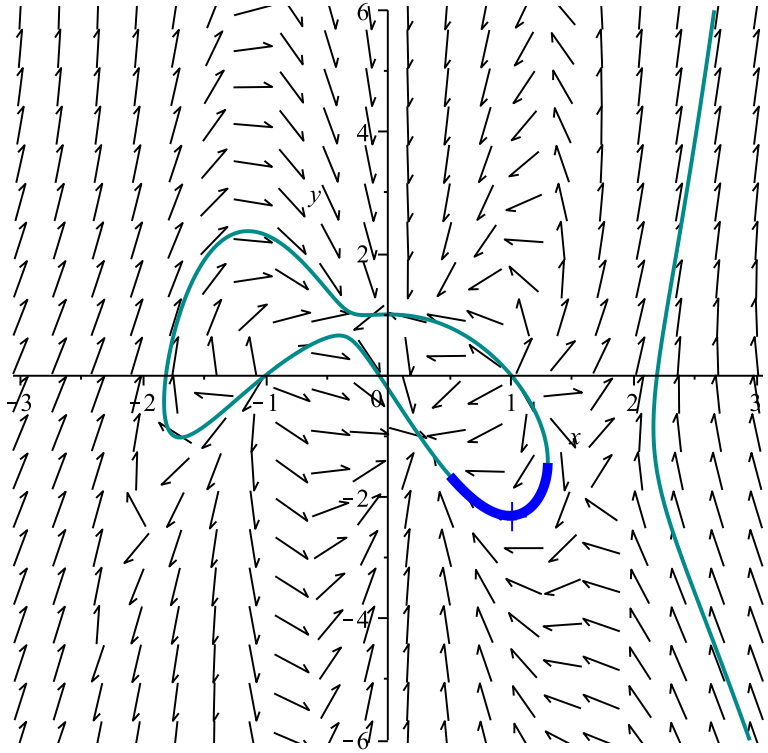


Calcul de $P_1(X, Y)$

Calcul d'intégrales premières rationnelles



Calcul de $Y_2(X) \in \mathbb{K}[[X]]$.

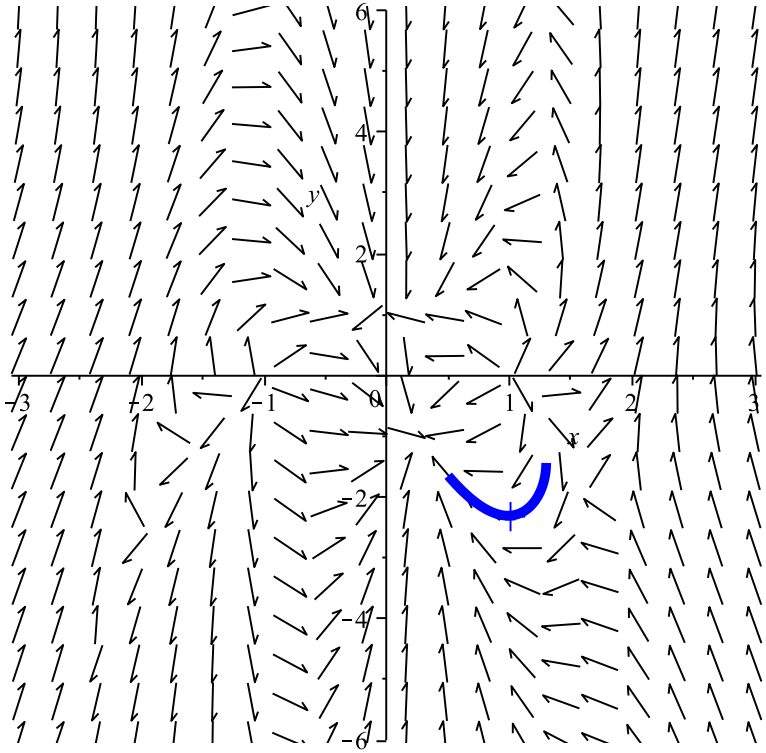


Calcul de $P_2(X, Y)$.

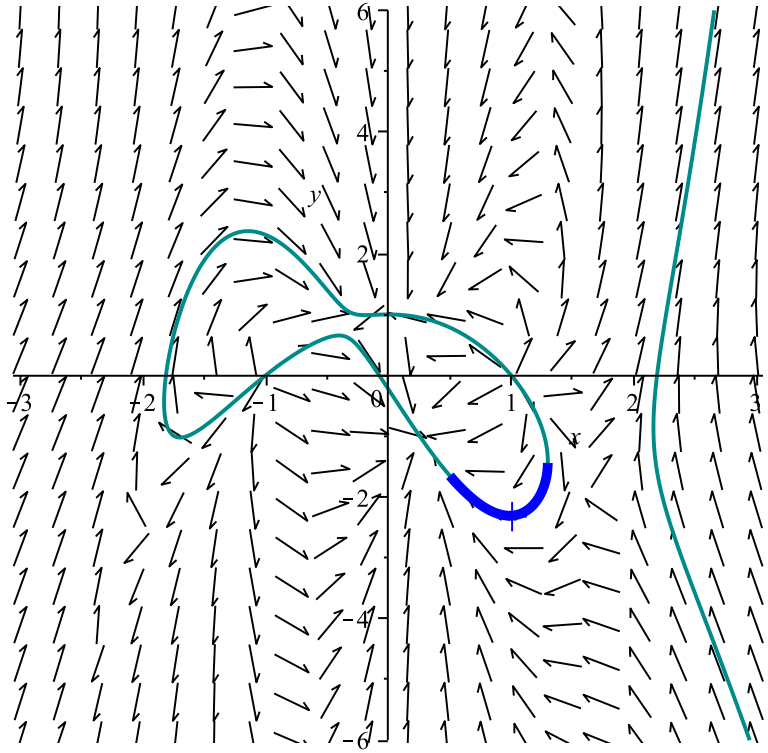
f/g est une intégrale première $\Rightarrow P_i = \lambda_i f - \mu_i g$

$$\Rightarrow \frac{P_1}{P_2} = \frac{\lambda_1 f - \mu_1 g}{\lambda_2 f - \mu_2 g} \text{ est une intégrale première.}$$

Calcul d'intégrales premières rationnelles



Calcul de $Y_2(X) \in \mathbb{K}[[X]]$.

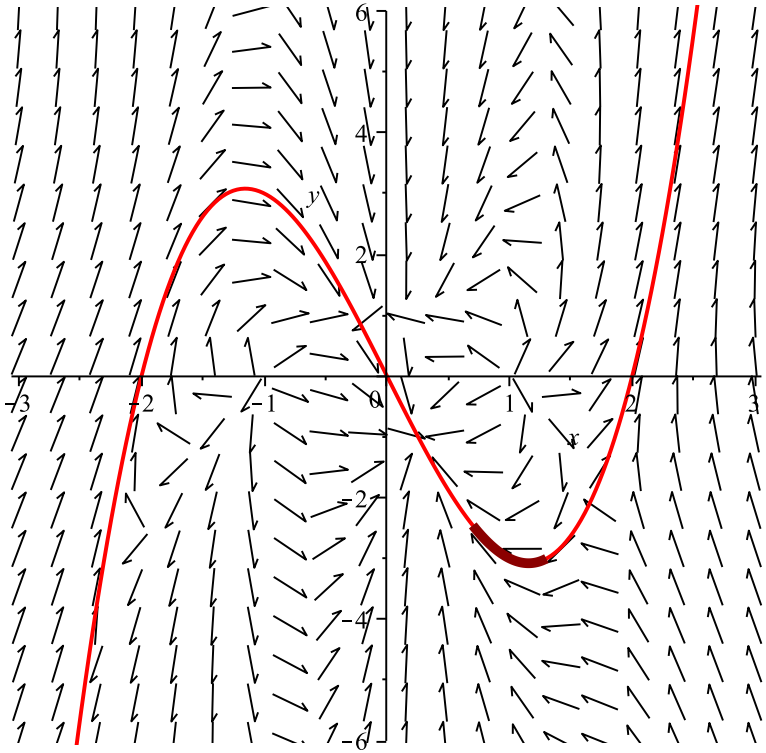


Calcul de $P_2(X, Y)$.

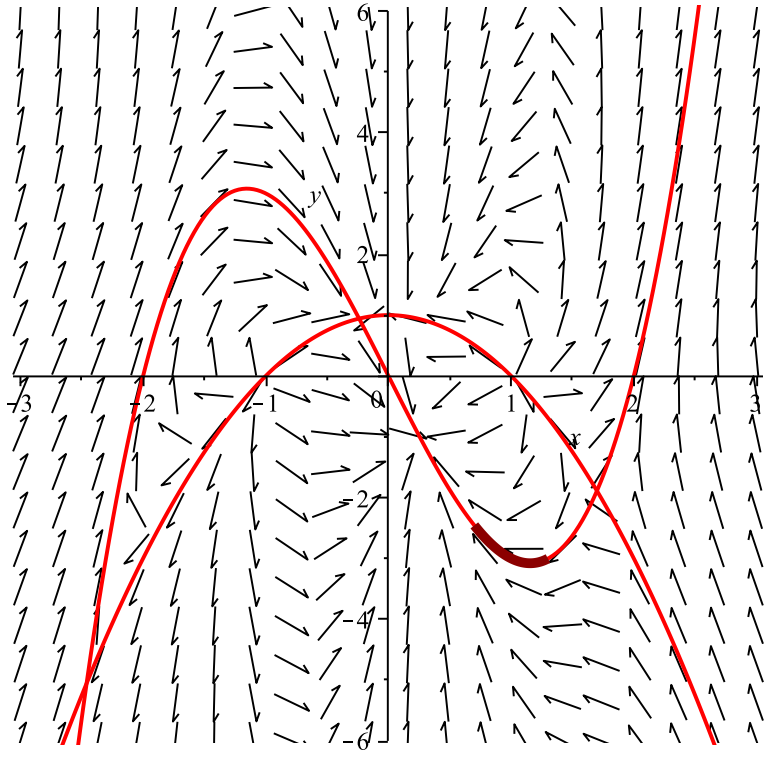
f/g est une intégrale première $\Rightarrow P_i = \lambda_i f - \mu_i g$

$$\Rightarrow \frac{P_1}{P_2} = \frac{\lambda_1 f - \mu_1 g}{\lambda_2 f - \mu_2 g} \text{ est une intégrale première.}$$

Calcul d'intégrales premières rationnelles



Calcul de $P_3(X)$.



Fibre réductible.

P_3 est un facteur de $\lambda f - \mu g$,
et $(\lambda : \mu) \in \sigma(f, g)$.

Calcul d'un paramétrage local d'une orbite

Lemme (Ferragut-Giacomini)

Soit (E) l'équation différentielle suivante :

$$(E): \quad \frac{dY}{dX} = \frac{B(X,Y)}{A(X,Y)}.$$

On suppose $A(0,Y) \not\equiv 0$.

Soit $c \in \mathbb{K}$ et $y_c(X)$ une série formelle solution de (E) qui vérifie $y(0) = c$.
Si (S) admet une intégrale première rationnelle f/g, alors $y_c(X)$ est une racine du polynôme $f(X,Y) - \mu g(X,Y) \in \mathbb{K}[X,Y]$, où $\mu = f(0,c)/g(0,c)$.

Preuve : $\mathcal{D}(f/g) = 0 \Rightarrow \mathcal{D}(f/g)(X, y_c(X)) = 0$.

$$\begin{aligned} 0 &= A(X, y_c(X)) \frac{\partial (f/g)}{\partial X}(X, y_c(X)) \\ &\quad + B(X, y_c(X)) \frac{\partial (f/g)}{\partial y}(X, y_c(X)), \end{aligned}$$

$$0 = \frac{\partial (f/g)}{\partial X}(X, y_c(X)) + \frac{B(X, y_c(X))}{A(X, y_c(X))} \cdot \frac{\partial (f/g)}{\partial y}(X, y_c(X)),$$

$$0 = \frac{\partial (f/g)}{\partial X}(X, y_c(X)) + \frac{dy_c(X)}{dX} \cdot \frac{\partial (f/g)}{\partial y}(X, y_c(X)),$$

$$0 = \frac{d\big(f/g(X, y_c(X))\big)}{dX}.$$

$\Rightarrow f/g(X, y_c(X)) = \mu$, où $\mu \in \mathbb{K}$.
$\Rightarrow (f - \mu g)(X, y_c(X)) = 0$.

Preuve : $\mathcal{D}(f/g) = 0 \Rightarrow \mathcal{D}(f/g)(X, y_c(X)) = 0.$

$$\begin{aligned} 0 &= A(X, y_c(X)) \frac{\partial (f/g)}{\partial X}(X, y_c(X)) \\ &\quad + B(X, y_c(X)) \frac{\partial (f/g)}{\partial y}(X, y_c(X)), \end{aligned}$$

$$0 = \frac{\partial (f/g)}{\partial X}(X, y_c(X)) + \frac{B(X, y_c(X))}{A(X, y_c(X))} \cdot \frac{\partial (f/g)}{\partial y}(X, y_c(X)),$$

$$0 = \frac{\partial (f/g)}{\partial X}(X, y_c(X)) + \frac{dy_c(X)}{dX} \cdot \frac{\partial (f/g)}{\partial y}(X, y_c(X)),$$

$$0 = \frac{d\big(f/g(X, y_c(X))\big)}{dX}.$$

$\Rightarrow f/g(X, y_c(X)) = \mu$, où $\mu \in \mathbb{K}$.
$\Rightarrow (f - \mu g)(X, y_c(X)) = 0.$

Preuve : $\mathcal{D}(f/g) = 0 \Rightarrow \mathcal{D}(f/g)(X, y_c(X)) = 0.$

$$\begin{aligned} 0 &= A\big(X, y_c(X)\big)\frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) \\ &\quad + B\big(X, y_c(X)\big)\frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big), \end{aligned}$$

$$0 = \frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) + \frac{B\big(X, y_c(X)\big)}{A\big(X, y_c(X)\big)} \cdot \frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big),$$

$$0 = \frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) + \frac{dy_c(X)}{dX} \cdot \frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big),$$

$$0 = \frac{d\big(f/g\big(X, y_c(X)\big)\big)}{dX}.$$

$\Rightarrow f/g\big(X, y_c(X)\big) = \mu$, où $\mu \in \mathbb{K}$.
$\Rightarrow \big(f - \mu g\big)\big(X, y_c(X)\big) = 0.$

Preuve : $\mathcal{D}(f/g) = 0 \Rightarrow \mathcal{D}(f/g)(X, y_c(X)) = 0.$

$$\begin{aligned} 0 &= A\big(X, y_c(X)\big)\frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) \\ &\quad + B\big(X, y_c(X)\big)\frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big), \end{aligned}$$

$$0 = \frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) + \frac{B\big(X, y_c(X)\big)}{A\big(X, y_c(X)\big)} \cdot \frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big),$$

$$0 = \frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) + \frac{dy_c(X)}{dX} \cdot \frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big),$$

$$0 = \frac{d\big(f/g\big(X, y_c(X)\big)\big)}{dX}.$$

$\Rightarrow f/g\big(X, y_c(X)\big) = \mu$, où $\mu \in \mathbb{K}$.
$\Rightarrow \big(f - \mu g\big)\big(X, y_c(X)\big) = 0.$

Preuve : $\mathcal{D}(f/g) = 0 \Rightarrow \mathcal{D}(f/g)(X, y_c(X)) = 0.$

$$\begin{aligned} 0 &= A\big(X, y_c(X)\big)\frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) \\ &\quad + B\big(X, y_c(X)\big)\frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big), \end{aligned}$$

$$0 = \frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) + \frac{B\big(X, y_c(X)\big)}{A\big(X, y_c(X)\big)} \cdot \frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big),$$

$$0 = \frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) + \frac{dy_c(X)}{dX} \cdot \frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big),$$

$$0 = \frac{d\big(f/g\big(X, y_c(X)\big)\big)}{dX}.$$

$\Rightarrow f/g\big(X, y_c(X)\big) = \mu$, où $\mu \in \mathbb{K}$.
$\Rightarrow \big(f - \mu g\big)\big(X, y_c(X)\big) = 0.$

Preuve : $\mathcal{D}(f/g) = 0 \Rightarrow \mathcal{D}(f/g)(X, y_c(X)) = 0$.

$$\begin{aligned} 0 &= A\big(X, y_c(X)\big)\frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) \\ &\quad + B\big(X, y_c(X)\big)\frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big), \end{aligned}$$

$$0 = \frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) + \frac{B\big(X, y_c(X)\big)}{A\big(X, y_c(X)\big)} \cdot \frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big),$$

$$0 = \frac{\partial(f/g)}{\partial X}\big(X, y_c(X)\big) + \frac{dy_c(X)}{dX} \cdot \frac{\partial(f/g)}{\partial y}\big(X, y_c(X)\big),$$

$$0 = \frac{d\big(f/g\big(X, y_c(X)\big)\big)}{dX}.$$

$\Rightarrow f/g\big(X, y_c(X)\big) = \mu$, où $\mu \in \mathbb{K}$.
$\Rightarrow \big(f - \mu g\big)\big(X, y_c(X)\big) = 0$.

Précision des calculs

Kannan, Lenstra, Lovász (1988) :
“Si nous connaissons la racine d’un polynôme irréductible avec une précision suffisamment grande alors nous pouvons trouver ce polynôme."

Lemme

Soit $y(X) \in \mathbb{K}[[X]]$ *une série formelle algébrique de polynôme minimal* $M(X, Y) \in \mathbb{K}[X, Y]$ *de degré* $\leq N$.
Si $\tilde{M} \in \mathbb{K}[X, Y]$ *est un polynôme de degré* $\leq N$ *satisfaisant*

$$(\star) : \ \tilde{M}(X, y(X)) \equiv 0 \mod X^{N^2+1},$$

alors $\tilde{M}(X, y(X)) = 0$.

Précision des calculs

Kannan, Lenstra, Lovász (1988) :
“Si nous connaissons la racine d’un polynôme irréductible avec une précision suffisamment grande alors nous pouvons trouver ce polynôme."

Lemme

Soit $y(X) \in \mathbb{K}[[X]]$ *une série formelle algébrique de polynôme minimal* $M(X, Y) \in \mathbb{K}[X, Y]$ *de degré* $\leq N$.
Si $\tilde{M} \in \mathbb{K}[X, Y]$ *est un polynôme de degré* $\leq N$ *satisfaisant*

$$(\star) : \ \tilde{M}(X, y(X)) \equiv 0 \mod X^{N^2+1},$$

alors $\tilde{M}(X, y(X)) = 0$.

Preuve

M satisfait $(\star)$ donc il existe $\tilde{M} \in \mathbb{K}[X, Y]$ de degré $\leq N$ satisfaisant $(\star)$.

Considerons $\mathcal{R}(X) := \mathrm{Res}_Y(M(X, Y), \tilde{M}(X, Y))$.
Il existe deux polynômes S et T dans $\mathbb{K}[X, Y]$ tels que $S\,M + T\,\tilde{M} = \mathcal{R}$.
$(\star) \Rightarrow \mathcal{R}(X) \equiv 0 \mod X^{N^2+1}$.

Théorème de Bezout$\Rightarrow \deg(\mathcal{R}) \leq \deg(M)\ \deg(\tilde{M}) \leq N^2$.
$\Rightarrow \mathcal{R} = 0$.
$\Rightarrow \gcd(M, \tilde{M})$ est non-trivial.
$\Rightarrow M$ divise $\tilde{M}$. $\square$

Preuve

M satisfait $(\star)$ donc il existe $\tilde{M} \in \mathbb{K}[X, Y]$ de degré $\leq N$ satisfaisant $(\star)$.

Considerons $\mathcal{R}(X) := \mathrm{Res}_Y(M(X, Y), \tilde{M}(X, Y))$.
Il existe deux polynômes S et T dans $\mathbb{K}[X, Y]$ tels que $S\,M + T\,\tilde{M} = \mathcal{R}$.
$(\star) \Rightarrow \mathcal{R}(X) \equiv 0 \mod X^{N^2+1}$.

Théorème de Bezout$\Rightarrow \deg(\mathcal{R}) \leq \deg(M)\ \deg(\tilde{M}) \leq N^2$.
$\Rightarrow \mathcal{R} = 0$.
$\Rightarrow \gcd(M, \tilde{M})$ est non-trivial.
$\Rightarrow M$ divise $\tilde{M}$. $\square$

Preuve

M satisfait $(\star)$ donc il existe $\tilde{M} \in \mathbb{K}[X, Y]$ de degré $\leq N$ satisfaisant $(\star)$.

Considerons $\mathcal{R}(X) := \mathrm{Res}_Y(M(X, Y), \tilde{M}(X, Y))$.
Il existe deux polynômes S et T dans $\mathbb{K}[X, Y]$ tels que $S\,M + T\,\tilde{M} = \mathcal{R}$.
$(\star) \Rightarrow \mathcal{R}(X) \equiv 0 \mod X^{N^2+1}$.

Théorème de Bezout$\Rightarrow \deg(\mathcal{R}) \leq \deg(M)\ \deg(\tilde{M}) \leq N^2$.
$\Rightarrow \mathcal{R} = 0$.
$\Rightarrow \gcd(M, \tilde{M})$ est non-trivial.
$\Rightarrow M$ divise $\tilde{M}$. $\square$

Calcul d'un polynôme minimal

Entrée: $y_c(X) \in \mathbb{K}[X]$ t.q. $\deg y_c \leq N^2 + 1$.
Sortie: Une solution minimale de $(\star)$ de degré $\leq N$ ou "Rien".

1. Soit $M(X, Y) = \sum_{i=0}^{N} \left(\sum_{j=0}^{N-i} m_{i,j} X^j \right) Y^i$.
2. Construire le système linéaire $(\mathcal{L})$ en les $m_{i,j}$:

$$M(X, y_c(X)) = \sum_{i=0}^{N} \left(\sum_{j=0}^{N-i} m_{i,j} X^j \right) y_c(X)^i \equiv 0 \mod X^{N^2+1}.$$

3. Si $(\mathcal{L})$ n'a pas de solutions non-triviales, alors Rendre "Rien".
4. Sinon calculer une base échelonnée de $\ker(\mathcal{L})$ pour trouver une solution de degré minimal en Y, Rendre cette solution.

Les mauvais cas

$y_c(X)$ est une racine du polynôme $f(X, Y) - \mu g(X, Y)$ avec $f(0, c) - \mu g(0, c) = 0$.

Les mauvais cas sont $\mathbf{(1 : \mu) \in \sigma(f, g)}$.

$\Rightarrow$ c doit donc éviter $\mathbf{|\sigma(f, g)|N}$ valeurs.

Le retour du spectre

Théorème (C. 2015)

Soit $\mathcal{D} = A\partial_X + B\partial_Y$, *où* $\deg(A), \deg(B) \leq d$.
Soit $f(X,Y)/g(X,Y) \in \mathbb{K}(X,Y)$ *indécomposable, une intégrale première de* $\mathcal{D}$.

$$|\sigma(f,g)| \leq \mathcal{B} + 5,$$

où $\mathcal{B} = d(d+1)/2$.

Version creuse existe.

Le retour du spectre

Théorème (C. 2015)

Soit $\mathcal{D} = A\partial_X + B\partial_Y$, *où* $\deg(A), \deg(B) \leq d$.
Soit $f(X,Y)/g(X,Y) \in \mathbb{K}(X,Y)$ *indécomposable, une intégrale première de* $\mathcal{D}$.

$$|\sigma(f,g)| \leq \mathcal{B} + 5,$$

où $\mathcal{B} = d(d+1)/2$.

Version creuse existe.

Preuve

$\gamma(f,g) = \{(\lambda:\mu) | \lambda f - \mu g = P^e, P \in \mathbb{K}[X,Y]\}$
$\gamma(f,g) \leq 3$ (Abhyankar-Heinzer-Sathaye, 2003)

Si $|\sigma(f,g) \setminus \gamma(f,g)| \geq \mathcal{B}+2$ alors il existe μ_i t.q.

$$f - \mu_i g = f_i^{m_i}.F_i,$$

où f_i est irréductible, f_i et F_i premier entre eux, $i = 1,\ldots,\mathcal{B}+2$.

Thm Jouanolou $\Rightarrow \exists e_i \in \mathbb{Z}$ t.q. $\prod_i f_i^{e_i}$ est une intégrale première rationnelle.

$$\Rightarrow \prod_i f_i^{e_i} = u(f/g) \Rightarrow \frac{\prod_{i\in I^+} f_i^{e_i}}{\prod_{i\in I^-} f_i^{e_i}} = \frac{\prod_k f - \alpha_k g}{\prod_l f - \alpha_l g}$$

$f_1 | f - \alpha g \ \Rightarrow \alpha = \mu_1$

F_1 apparaît à droite mais n'apparaît pas à gauche...

Preuve

$\gamma(f,g) = \{(\lambda:\mu) | \lambda f - \mu g = P^e, P \in \mathbb{K}[X,Y]\}$
$\gamma(f,g) \leq 3$ (Abhyankar-Heinzer-Sathaye, 2003)

Si $|\sigma(f,g) \setminus \gamma(f,g)| \geq \mathcal{B}+2$ alors il existe μ_i t.q.

$$f - \mu_i g = f_i^{m_i}.F_i,$$

où f_i est irréductible, f_i et F_i premier entre eux, $i = 1,\ldots,\mathcal{B}+2$.

Thm Jouanolou $\Rightarrow \exists e_i \in \mathbb{Z}$ t.q. $\prod_i f_i^{e_i}$ est une intégrale première rationnelle.

$$\Rightarrow \prod_i f_i^{e_i} = u(f/g) \Rightarrow \frac{\prod_{i\in I^+} f_i^{e_i}}{\prod_{i\in I^-} f_i^{e_i}} = \frac{\prod_k f - \alpha_k g}{\prod_l f - \alpha_l g}$$

$f_1 | f - \alpha g \ \Rightarrow \alpha = \mu_1$

F_1 apparaît à droite mais n'apparaît pas à gauche...

Preuve

$\gamma(f,g) = \{(\lambda:\mu) | \lambda f - \mu g = P^e, P \in \mathbb{K}[X,Y]\}$
$\gamma(f,g) \leq 3$ (Abhyankar-Heinzer-Sathaye, 2003)

Si $|\sigma(f,g) \setminus \gamma(f,g)| \geq \mathcal{B}+2$ alors il existe μ_i t.q.

$$f - \mu_i g = f_i^{m_i}.F_i,$$

où f_i est irréductible, f_i et F_i premier entre eux, $i = 1,\ldots,\mathcal{B}+2$.

Thm Jouanolou $\Rightarrow \exists e_i \in \mathbb{Z}$ t.q. $\prod_i f_i^{e_i}$ est une intégrale première rationnelle.

$$\Rightarrow \prod_i f_i^{e_i} = u(f/g) \Rightarrow \frac{\prod_{i\in I^+} f_i^{e_i}}{\prod_{i\in I^-} f_i^{e_i}} = \frac{\prod_k f - \alpha_k g}{\prod_l f - \alpha_l g}$$

$f_1 | f - \alpha g \ \Rightarrow \alpha = \mu_1$

F_1 apparaît à droite mais n'apparaît pas à gauche...

Preuve

$\gamma(f,g) = \{(\lambda:\mu) | \lambda f - \mu g = P^e, P \in \mathbb{K}[X,Y]\}$
$\gamma(f,g) \leq 3$ (Abhyankar-Heinzer-Sathaye, 2003)

Si $|\sigma(f,g) \setminus \gamma(f,g)| \geq \mathcal{B}+2$ alors il existe μ_i t.q.

$$f - \mu_i g = f_i^{m_i}.F_i,$$

où f_i est irréductible, f_i et F_i premier entre eux, $i = 1,\ldots,\mathcal{B}+2$.

Thm Jouanolou $\Rightarrow \exists e_i \in \mathbb{Z}$ t.q. $\prod_i f_i^{e_i}$ est une intégrale première rationnelle.

$$\Rightarrow \prod_i f_i^{e_i} = u(f/g) \Rightarrow \frac{\prod_{i\in I^+} f_i^{e_i}}{\prod_{i\in I^-} f_i^{e_i}} = \frac{\prod_k f - \alpha_k g}{\prod_l f - \alpha_l g}$$

$f_1 | f - \alpha g \ \Rightarrow \alpha = \mu_1$

F_1 apparaît à droite mais n'apparaît pas à gauche...

Preuve

$\gamma(f,g) = \{(\lambda:\mu) | \lambda f - \mu g = P^e, P \in \mathbb{K}[X,Y]\}$
$\gamma(f,g) \leq 3$ (Abhyankar-Heinzer-Sathaye, 2003)

Si $|\sigma(f,g) \setminus \gamma(f,g)| \geq \mathcal{B}+2$ alors il existe μ_i t.q.

$$f - \mu_i g = f_i^{m_i}.F_i,$$

où f_i est irréductible, f_i et F_i premier entre eux, $i = 1,\ldots,\mathcal{B}+2$.

Thm Jouanolou $\Rightarrow \exists e_i \in \mathbb{Z}$ t.q. $\prod_i f_i^{e_i}$ est une intégrale première rationnelle.

$$\Rightarrow \prod_i f_i^{e_i} = u(f/g) \Rightarrow \frac{\prod_{i\in I^+} f_i^{e_i}}{\prod_{i\in I^-} f_i^{e_i}} = \frac{\prod_k f - \alpha_k g}{\prod_l f - \alpha_l g}$$

$f_1 | f - \alpha g \ \Rightarrow \alpha = \mu_1$

F_1 apparaît à droite mais n'apparaît pas à gauche...

Preuve

$\gamma(f,g) = \{(\lambda:\mu) | \lambda f - \mu g = P^e, P \in \mathbb{K}[X,Y]\}$
$\gamma(f,g) \leq 3$ (Abhyankar-Heinzer-Sathaye, 2003)

Si $|\sigma(f,g) \setminus \gamma(f,g)| \geq \mathcal{B}+2$ alors il existe μ_i t.q.

$$f - \mu_i g = f_i^{m_i}.F_i,$$

où f_i est irréductible, f_i et F_i premier entre eux, $i = 1,\ldots,\mathcal{B}+2$.

Thm Jouanolou $\Rightarrow \exists e_i \in \mathbb{Z}$ t.q. $\prod_i f_i^{e_i}$ est une intégrale première rationnelle.

$$\Rightarrow \prod_i f_i^{e_i} = u(f/g) \Rightarrow \frac{\prod_{i\in I^+} f_i^{e_i}}{\prod_{i\in I^-} f_i^{e_i}} = \frac{\prod_k f - \alpha_k g}{\prod_l f - \alpha_l g}$$

$f_1 | f - \alpha g \ \Rightarrow \alpha = \mu_1$

F_1 apparaît à droite mais n'apparaît pas à gauche...

Calcul d'une intégrale première de degré $\leq N$

Algorithme Bostan-C.-Cluzeau-Weil (2015) :

1. Prendre deux points (x_1, y_1), (x_2, y_2).
2. Calculer $Y_i(X) \in \mathbb{K}[[X]]$ solution de :

$$\frac{dY_i}{dX} = \frac{B(X, Y_i)}{A(X, Y_i)}, \text{ et } Y_i(x_i) = y_i.$$

En pratique : Calcul de $Y_i(X) \mod X^{N^2+1}$ via la méthode de Newton.

3. Calculer le polynôme minimal $P_i(X, Y) \in \mathbb{K}[X, Y]$ de $Y_i(X)$.
En pratique : Résoudre un système linéaire, (Padé-Hermite).

4. Vérifier que P_1/P_2 est une intégrale première.
Si on évite le spectre alors on obtient une intégrale première rationnelle.

Calcul d'une intégrale première de degré $\leq N$

Algorithme Bostan-C.-Cluzeau-Weil (2015) :

1. Prendre deux points (x_1, y_1), (x_2, y_2).
2. Calculer $Y_i(X) \in \mathbb{K}[[X]]$ solution de :

$$\frac{dY_i}{dX} = \frac{B(X, Y_i)}{A(X, Y_i)}, \text{ et } Y_i(x_i) = y_i.$$

En pratique : Calcul de $Y_i(X)$ mod X^{N^2+1} via la méthode de Newton.

3. Calculer le polynôme minimal $P_i(X, Y) \in \mathbb{K}[X, Y]$ de $Y_i(X)$.
En pratique : Résoudre un système linéaire, (Padé-Hermite).

4. Vérifier que P_1/P_2 est une intégrale première.
Si on évite le spectre alors on obtient une intégrale première rationnelle.

Calcul d'une intégrale première de degré $\leq N$

Algorithme Bostan-C.-Cluzeau-Weil (2015) :

1. Prendre deux points (x_1, y_1), (x_2, y_2).
2. Calculer $Y_i(X) \in \mathbb{K}[[X]]$ solution de :

$$\frac{dY_i}{dX} = \frac{B(X, Y_i)}{A(X, Y_i)}, \text{ et } Y_i(x_i) = y_i.$$

En pratique : Calcul de $Y_i(X)$ mod X^{N^2+1} via la méthode de Newton.

3. Calculer le polynôme minimal $P_i(X, Y) \in \mathbb{K}[X, Y]$ de $Y_i(X)$.
En pratique : Résoudre un système linéaire, (Padé-Hermite).

4. Vérifier que P_1/P_2 est une intégrale première.
Si on évite le spectre alors on obtient une intégrale première rationnelle.

Calcul d'une intégrale première de degré $\leq N$

Algorithme Bostan-C.-Cluzeau-Weil (2015) :

1. Prendre deux points (x_1, y_1), (x_2, y_2).
2. Calculer $Y_i(X) \in \mathbb{K}[[X]]$ solution de :

$$\frac{dY_i}{dX} = \frac{B(X, Y_i)}{A(X, Y_i)}, \text{ et } Y_i(x_i) = y_i.$$

   En pratique : Calcul de $Y_i(X) \mod X^{N^2+1}$ via la méthode de Newton.

3. Calculer le polynôme minimal $P_i(X, Y) \in \mathbb{K}[X, Y]$ de $Y_i(X)$.
   En pratique : Résoudre un système linéaire,
   (Padé-Hermite).

4. Vérifier que P_1/P_2 est une intégrale première.
   Si on évite le spectre alors on obtient une intégrale première rationnelle.

Complexité

N tend vers l'infini.
$\deg A, \deg B \leq d$ et d est fixe.

Le calcul d'une intégrale rationnelle peut s'effectuer à l'aide d'un algorithme probabiliste utilisant au plus $\tilde{\mathcal{O}}(N^{2\omega})$ opérations arithmétiques dans $\mathbb{K}$, ($\tilde{\mathcal{O}}(N^{\omega+2})$ avec Padé-Hermite).

Le calcul d'une intégrale rationnelle peut s'effectuer à l'aide d'un algorithme déterministe utilisant au plus $\tilde{\mathcal{O}}(d^2 N^{2\omega+1})$ opérations arithmétiques dans $\mathbb{K}$.

Complexité polynomiale précédente (C. 2011) : $\boldsymbol{\tilde{\mathcal{O}}(N^{4\omega+4})}$.
Autres méthodes :
Méthode naïve, Ferragut-Giacomini.

Problèmes ouverts :

Factorisation dans un pinceau = Décomposition des fractions rationnelles
Bornes de Noether, Jouanolou optimales ?

Calcul de polynômes de Darboux et d'intégrales premières rationnelles
Problème de Poincaré ?

Racines entières et composition
(τ conjecture Shub-Smale $\rightsquigarrow$ Malajovich)
Soient $f_1, \ldots, f_k \in \mathbb{Z}[X]$. Trouver une borne sur le nombre maximum de racines entières distinctes de $f_1 \circ \cdots \circ f_k$.
Peut on avoir $\deg(f_1). \cdots . \deg(f_k)$ racines entières ?