Séries de Puiseux: un algorithme dichotomique

Adrien Poteaux[⋆] & Martin Weimann[✈] & Marc Rybowicz[†]

[⋆]: GAIA-CFHP - CO2 - CRIStAL - Université de Lille

[✈]: GAATI - Université de Polynésie Française

[†]: DMI - XLIM - Université de Limoges ; mort en Novembre 2016

JNCF 2018, Luminy

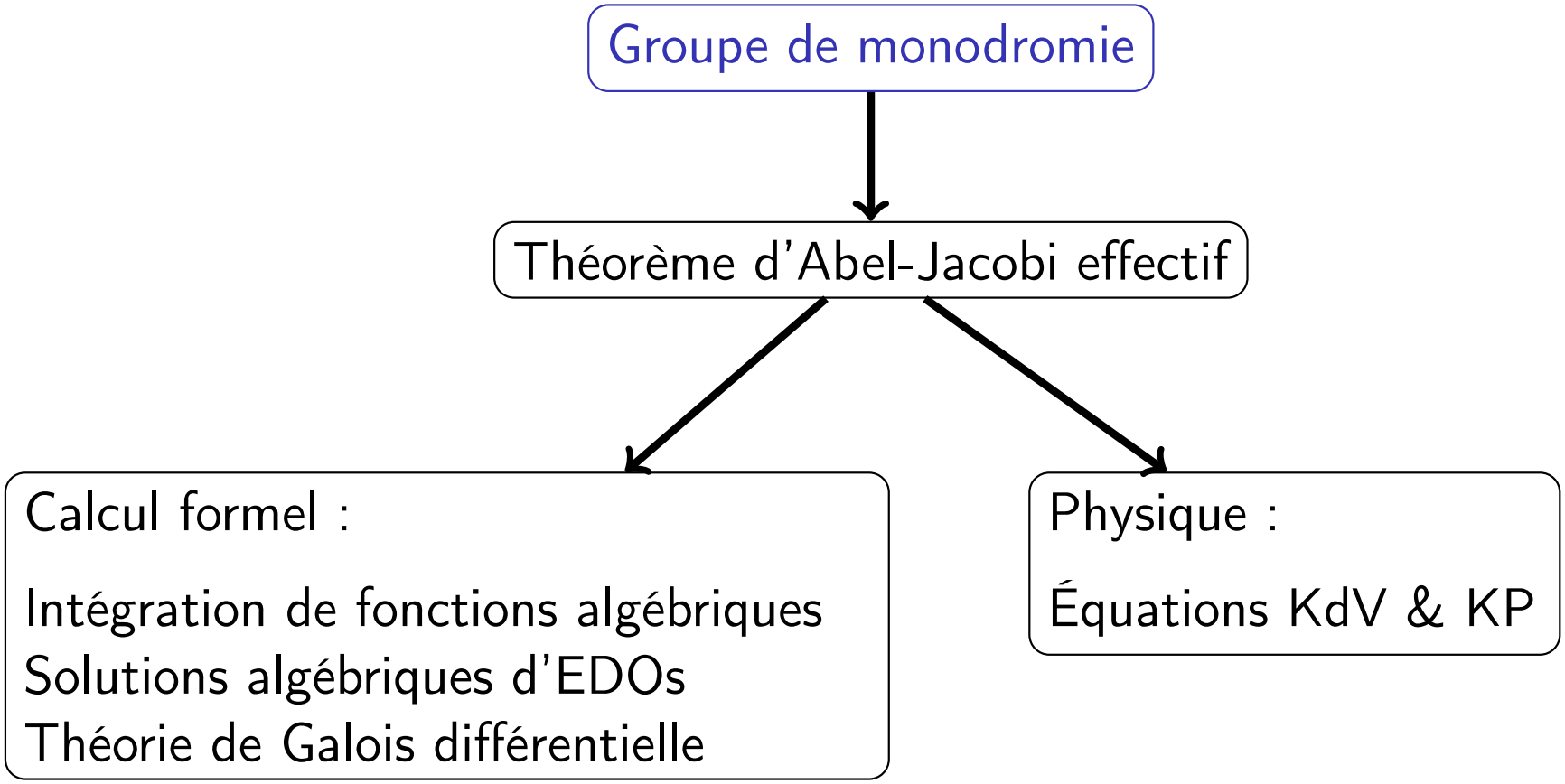
24 Janvier 2018

soumis à JFoCM

arXiv:1708.09067

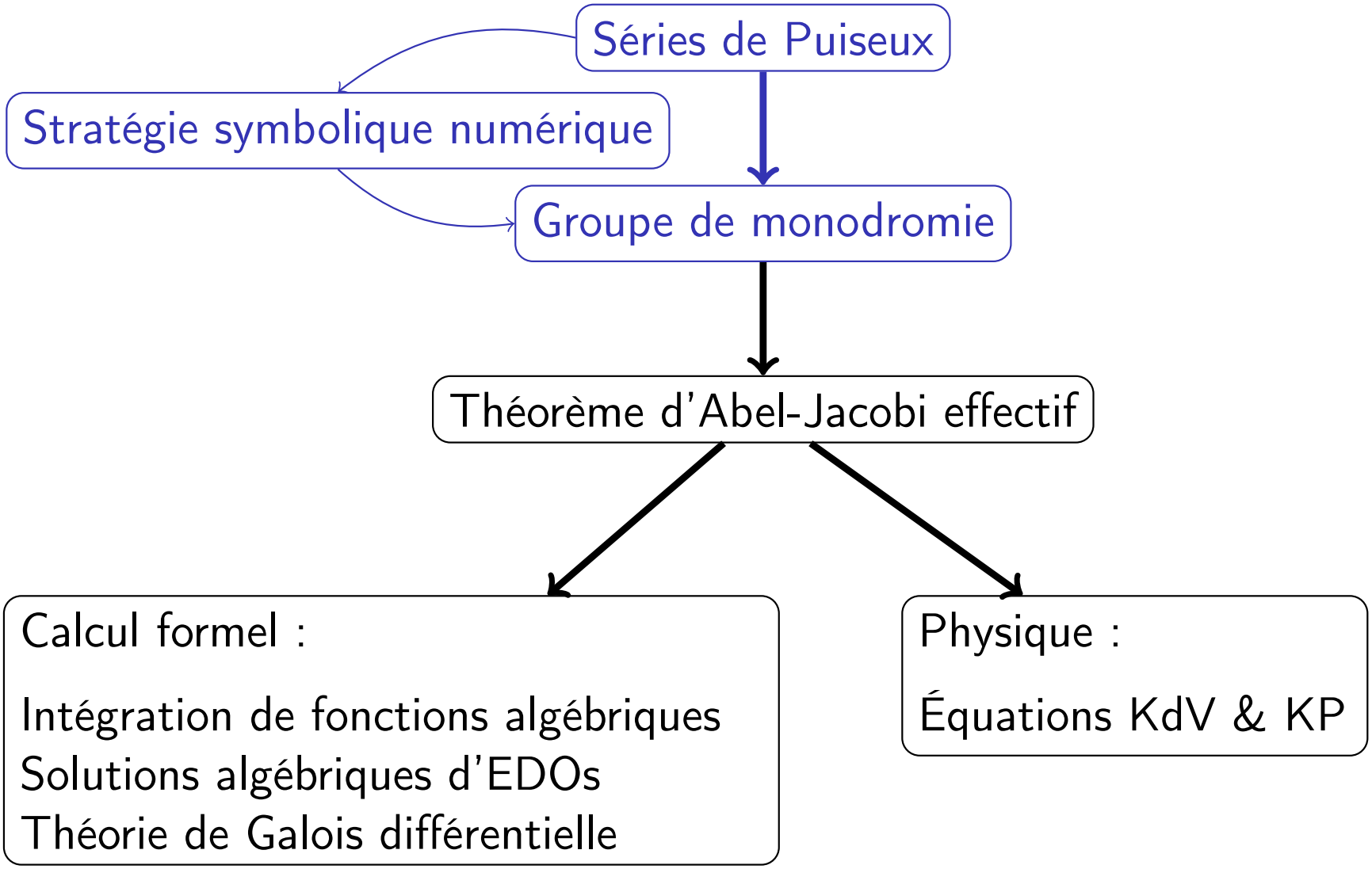
hal-01578214

Previsouly, in JNCF



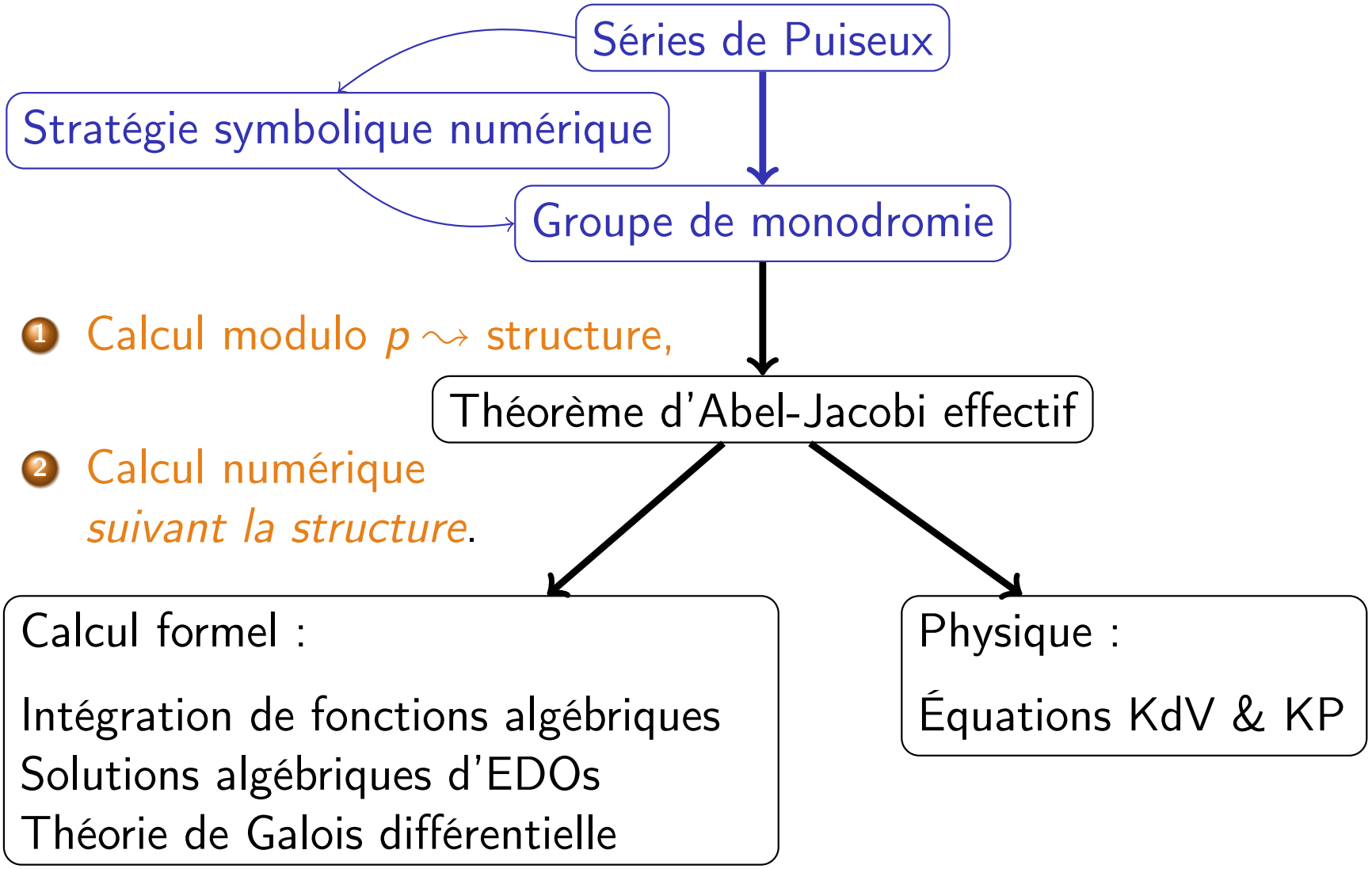
Luminy 2007

Previsouly, in JNCF



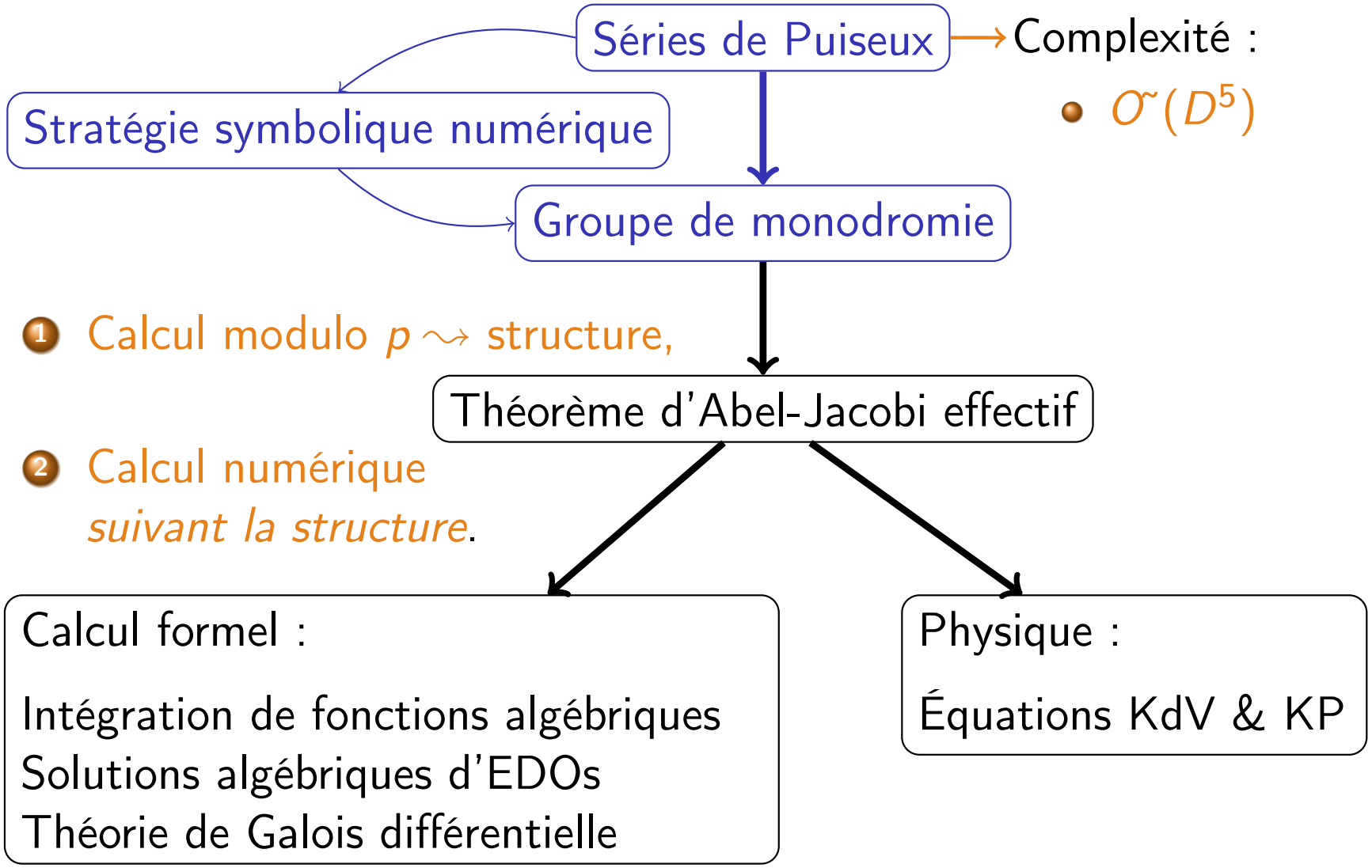
Luminy 2007

Previsouly, in JNCF



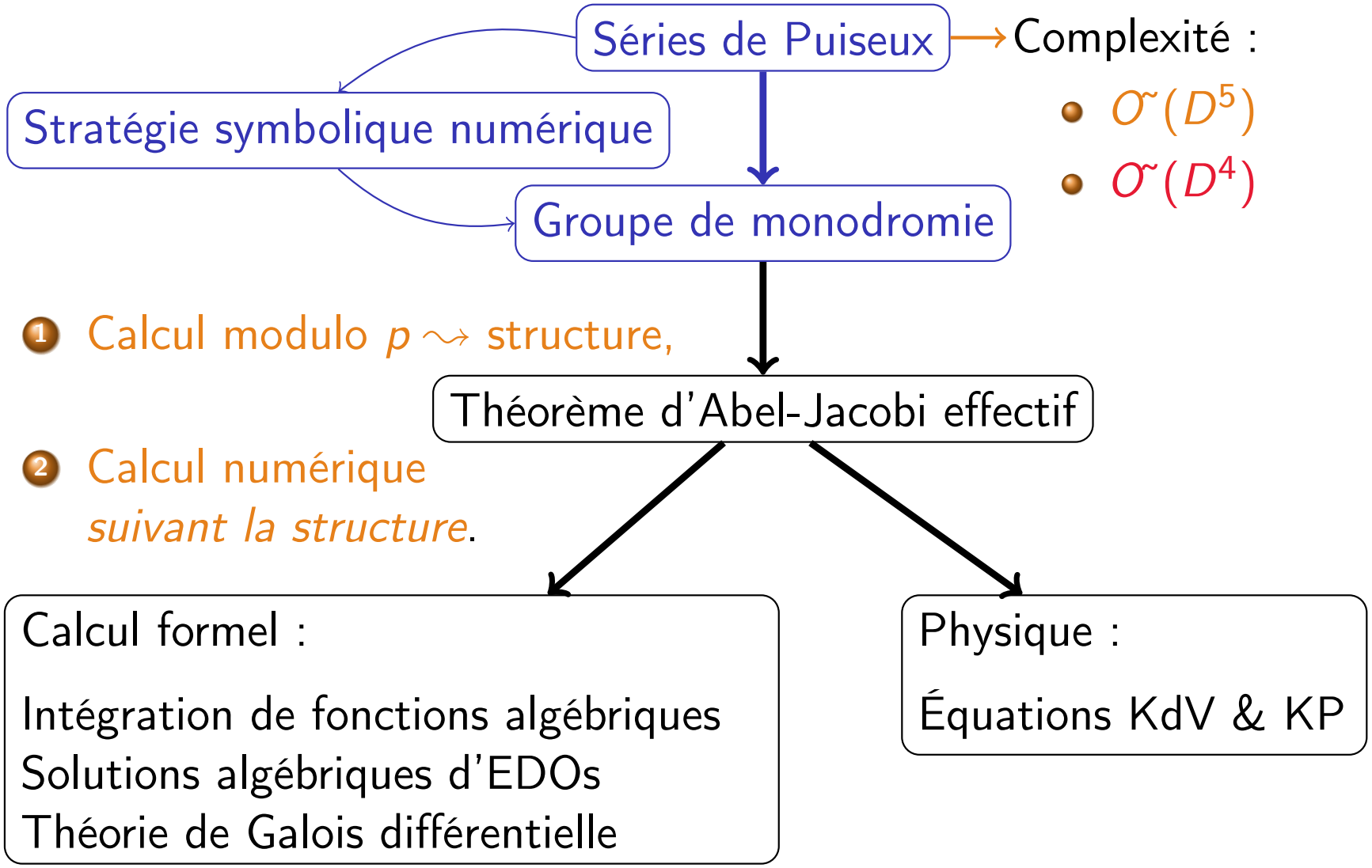
Luminy 2007 ; Luminy 2008

Previsouly, in JNCF



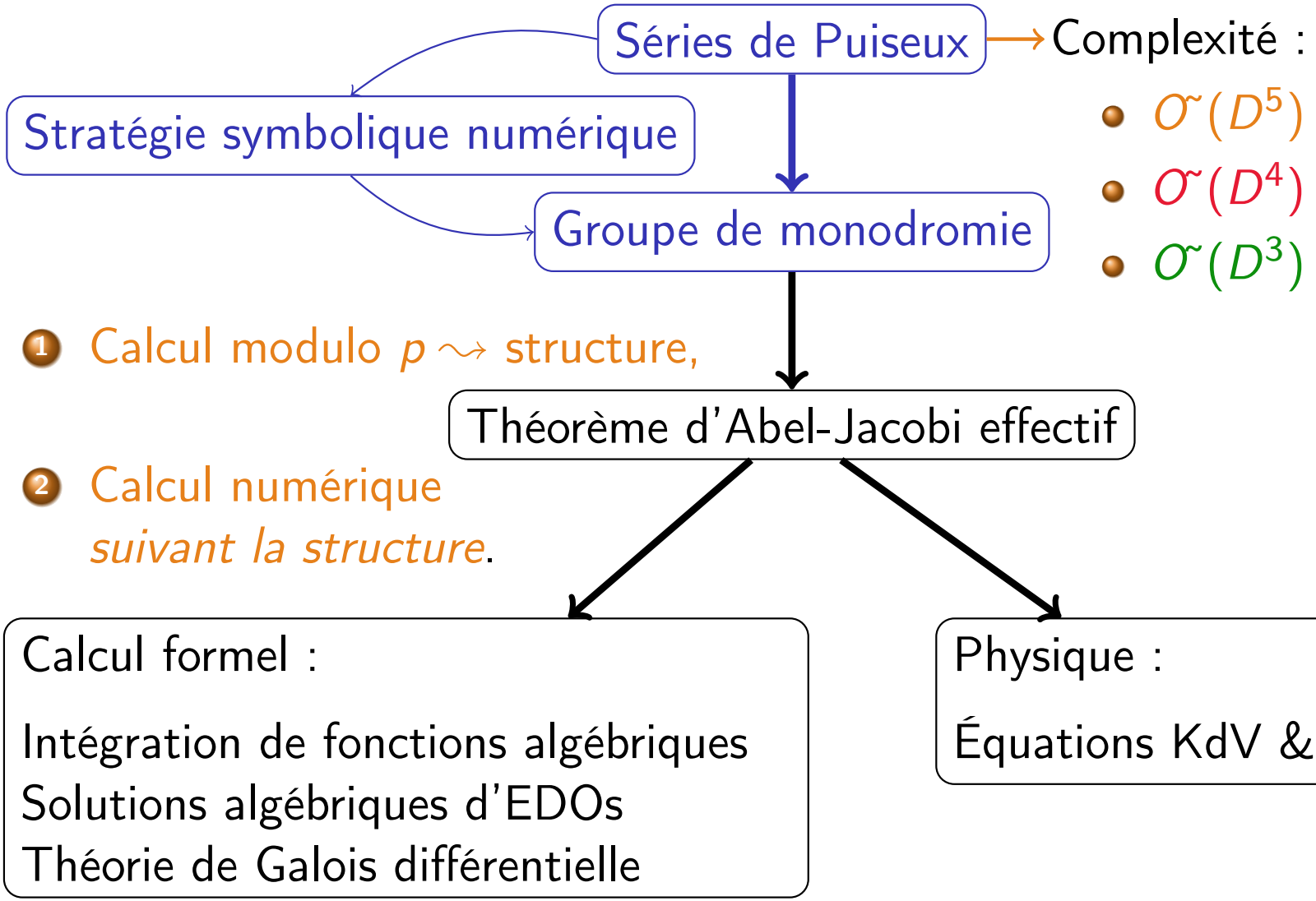
Luminy 2007 ; Luminy 2008

Previsouly, in JNCF



Luminy 2007 ; Luminy 2008 ; Cluny 2015

Previsouly, in JNCF



Luminy 2007 ; Luminy 2008 ; Cluny 2015 ; Aujourd'hui

Séries de Puiseux

Théorème (Puiseux, 1850)

$F \in \mathbb{K}[X][Y]$ possède d_Y racines distinctes dans $\overline{\mathbb{K}((X-x_0))}$:

$$Y_{ij}(X) = \sum_{k=n_i}^{\infty} \alpha_{i,k}\, \zeta_{e_i}^{jk}\, (X-x_0)^{\frac{k}{e_i}}$$

- $e_1, \cdots, e_s \in \mathbb{N}^\star$ *et* $d_Y = \sum_{i=1}^{s} e_i$
- $0 \leq j \leq e_i - 1$, $1 \leq i \leq s$,
- $n_i \in \mathbb{Z}$, $\alpha_{i,n_i} \neq 0$
- ζ_{e_i} *racine primitive de l'unité d'ordre* e_i

De plus, $\{\alpha_{i,k}\}$ appartiennent à une extension finie de $\mathbb{K}$.

$$\overline{\mathbb{K}((X-x_0))} = \bigcup_{e \in \mathbb{N}^\star} \overline{\mathbb{K}}(((X-x_0)^{1/e}))$$

Partie singulière

$$Y_{ij}(X) \quad = \quad \sum_{k=n_i}^{r_{ij}} \alpha_{ik}\, \zeta_{e_i}^{jk}\, X^{\frac{k}{e_i}} + \text{termes suivants}$$

r_{ij} est l'**indice de régularité** ; $r_i = r_{ij}$ pour $1 \leq j \leq e_i$

Termes suivants : calculés par exemple via Newton quadratique

Kung & Traub 1978 [All Algebraic Functions Can Be Computed Fast]

Exemple

$$F = \prod_{i=1}^{3}(Y - S_i(X)) + X^{19}Y \ \textit{avec}$$

- $S_1 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 - X^{15/2} + \ldots$
- $S_2 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 + X^{15/2} + \ldots$
- $S_3 = X + X^2 + X^3 + X^4 + \ldots$

Calcul d'une série de Puiseux : idée et outils

$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

$$\Longrightarrow \text{But : } Y(X) = \alpha\,X^{\frac{m}{q}} + \cdots \text{ s.t. } F(X,Y(X)) = 0$$

$$\begin{aligned} F(X, \alpha\,X^{\frac{m}{q}} + \cdots) \quad &= \alpha^6\,X^{\frac{6\,m}{q}} + \alpha^5\,X^{\frac{5\,m}{q}+1} + 5\,\alpha^4\,X^{\frac{4\,m}{q}+3} \\ &\quad -2\,\alpha^4\,X^{\frac{4\,m}{q}+1} + 4\,\alpha^2\,X^{\frac{2\,m}{q}+2} + X^5 - 3\,X^4 + \cdots \end{aligned}$$

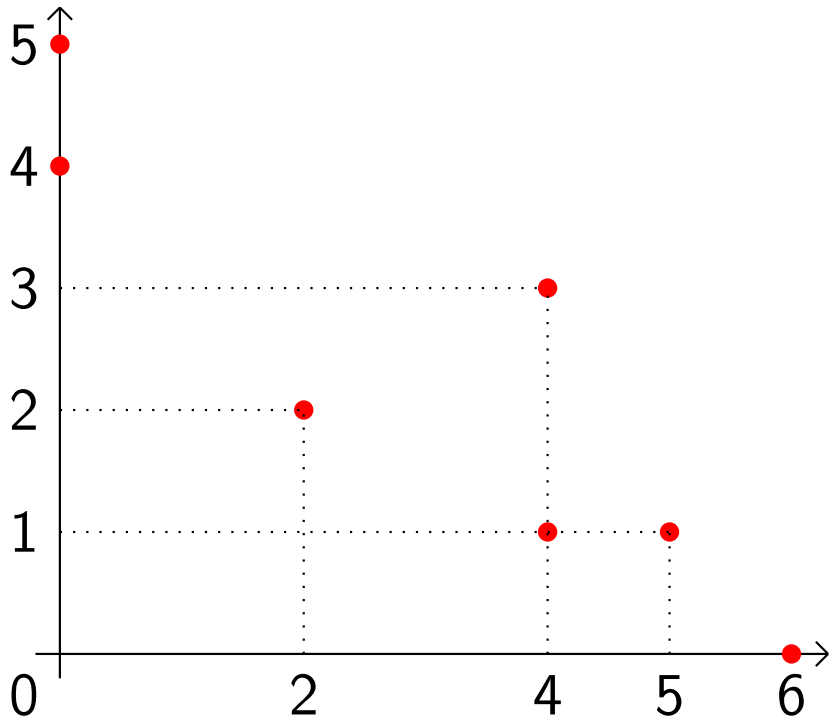
- On doit annuler au moins deux termes !

$$\Longrightarrow (m,q) \text{ t.q. deux exposants soient identiques}$$

Support d'un polynôme

$$F(X,Y) = Y^6X^0 + Y^5X^1 + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + Y^0X^5 - 3\,Y^0X^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$



Choix de (m, q) qui augmente l'ordre en X ?

$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

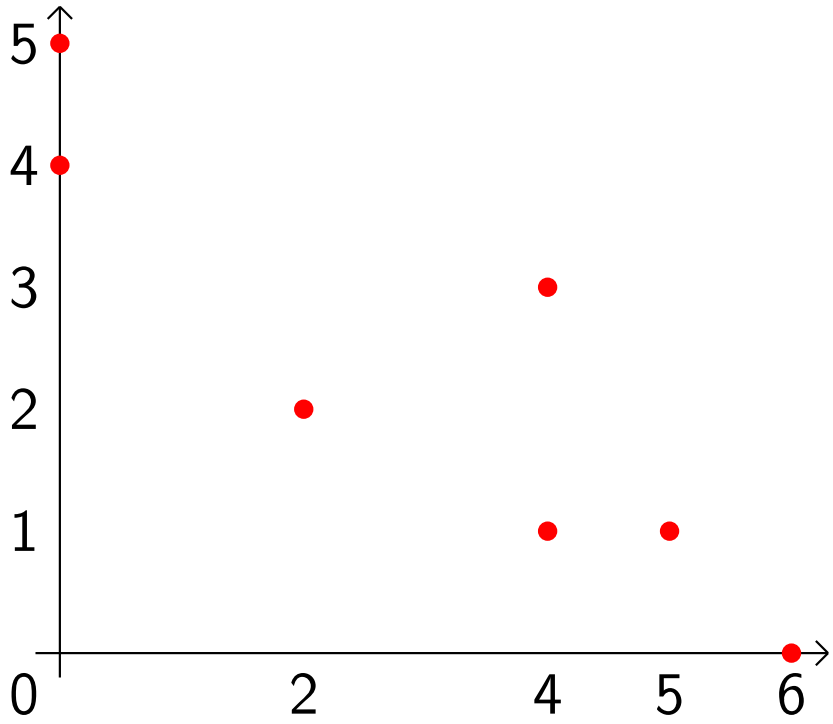
- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

$*$ (m, q) pour annuler deux termes ?

$\rightsquigarrow$ au moins 2 points sur $m\,i + q\,j = l$

$*$ augmenter l'ordre en X ?

$\rightsquigarrow$ pas d'autre point sous cette droite



Choix de (m, q) qui augmente l'ordre en X ?

$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

$*$ (m, q) pour annuler deux termes ?

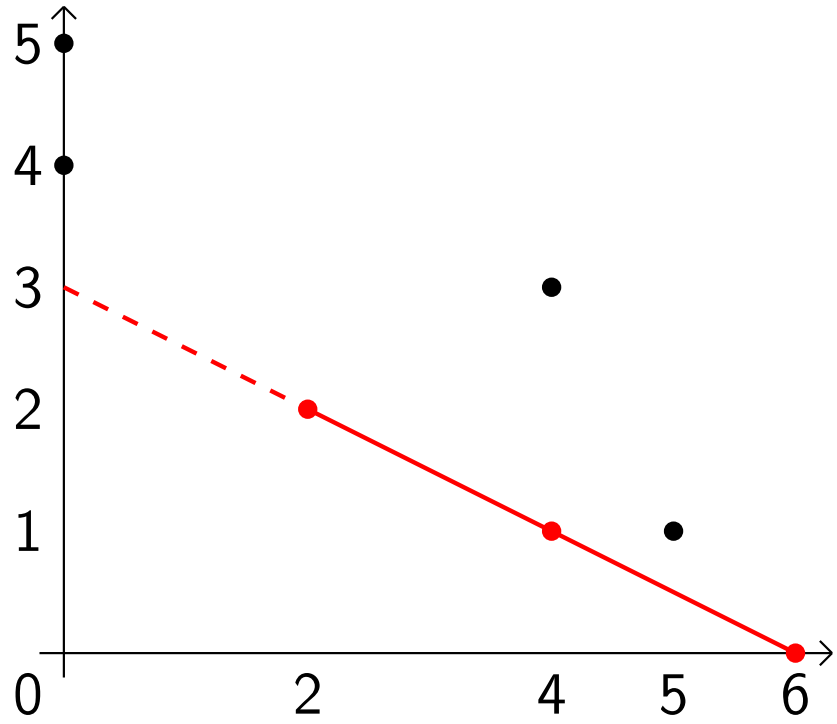
$\rightsquigarrow$ au moins 2 points sur $m\,i + q\,j = l$

$*$ augmenter l'ordre en X ?

$\rightsquigarrow$ pas d'autre point sous cette droite

(Δ_1) $i + 2\,j = 6$ est une telle droite

$$\rightsquigarrow S(X) = \alpha\,X^{1/2} + \cdots$$



Choix de (m, q) qui augmente l'ordre en X ?

$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

$*$ (m, q) pour annuler deux termes ?

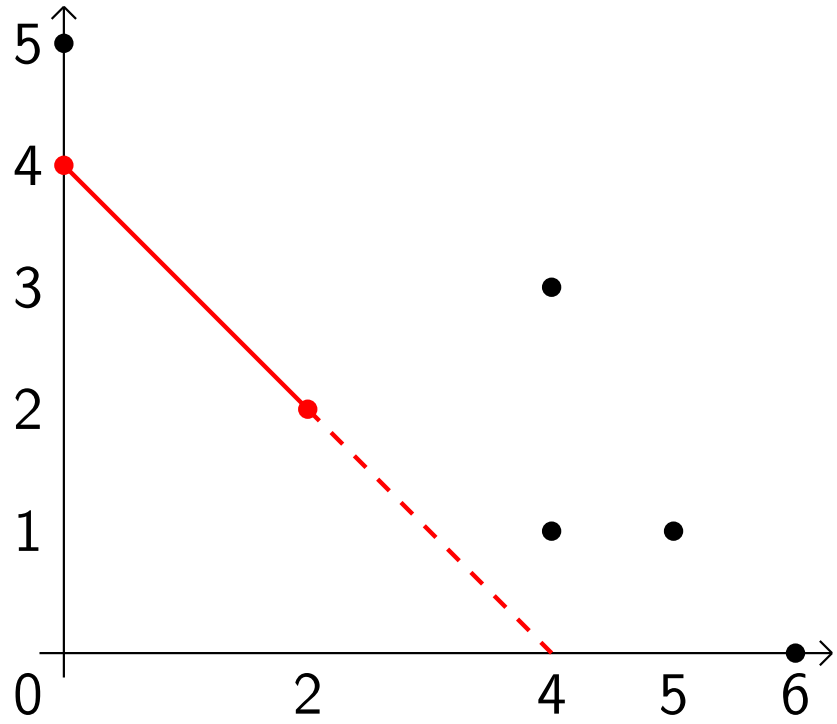
$\rightsquigarrow$ au moins 2 points sur $m\,i + q\,j = l$

$*$ augmenter l'ordre en X ?

$\rightsquigarrow$ pas d'autre point sous cette droite

(Δ_1) $i + 2\,j = 6$ est une telle droite

(Δ_2) $i + j = 4$ aussi

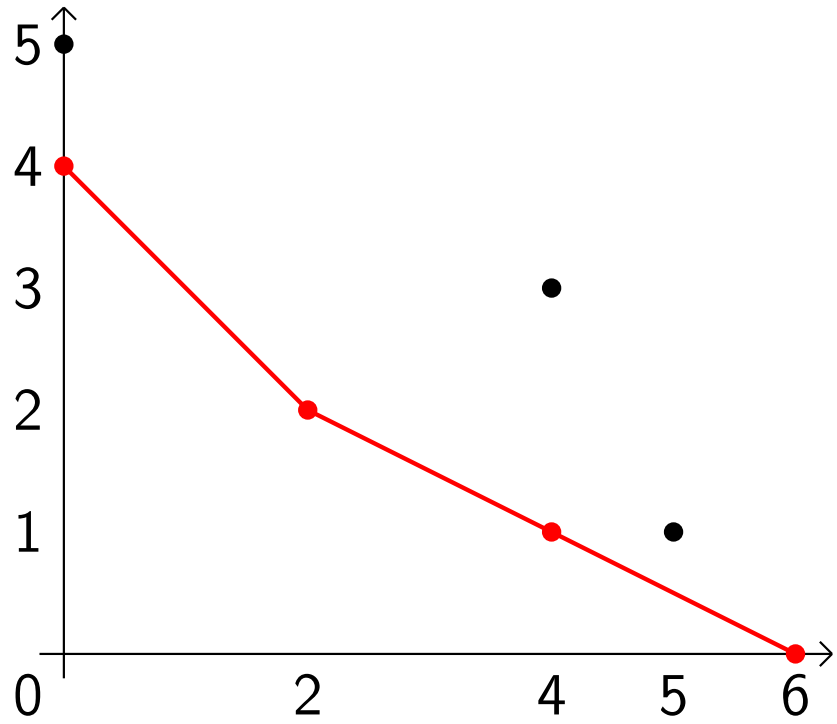


Polygone de Newton

$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

— $\mathcal{N}(F)$: partie inférieure de l'enveloppe convexe de Supp(F).



Choix de α qui augmente l'ordre en X ?

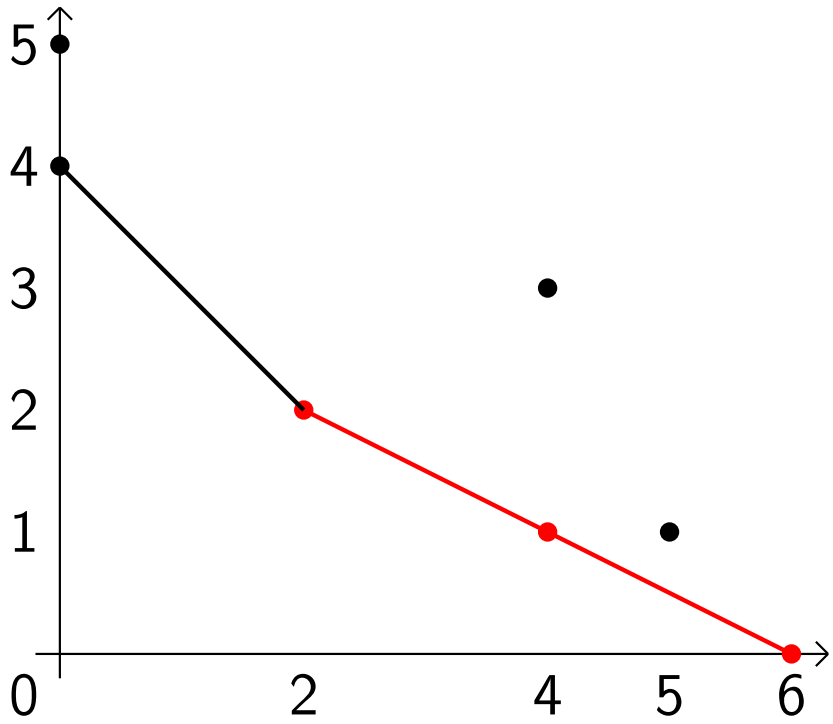
$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

— $\mathcal{N}(F)$: partie inférieure de l'enveloppe convexe de Supp(F).

$$F(T^2, \alpha\, T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2)\, T^6$$

$$-3\, T^8 + \alpha^5\, T^7 + (5\alpha^4 + 1)\, T^{10} + \ldots$$



Polynôme caractéristique

$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

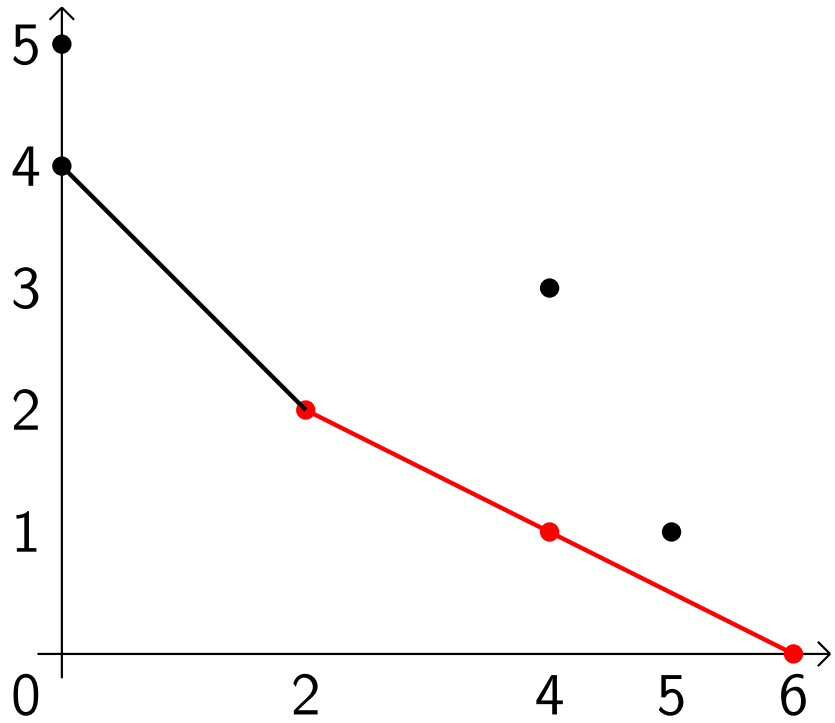
— $\mathcal{N}(F)$: partie inférieure de l'enveloppe convexe de Supp(F).

$$F(T^2, \alpha\, T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2)\, T^6$$

$$-3\, T^8 + \alpha^5\, T^7 + (5\alpha^4 + 1)\, T^{10} + \ldots$$

Polynôme caractéristique :

$$\phi_{\Delta_1}(\beta) = \beta^2 - 2\,\beta + 4$$



Algorithme de Newton-Puiseux

Pour chaque arête Δ de $\mathcal{N}(F)$

1. Factoriser $\phi_\Delta = \prod_{k=1}^{s} \phi_k^{M_k}$

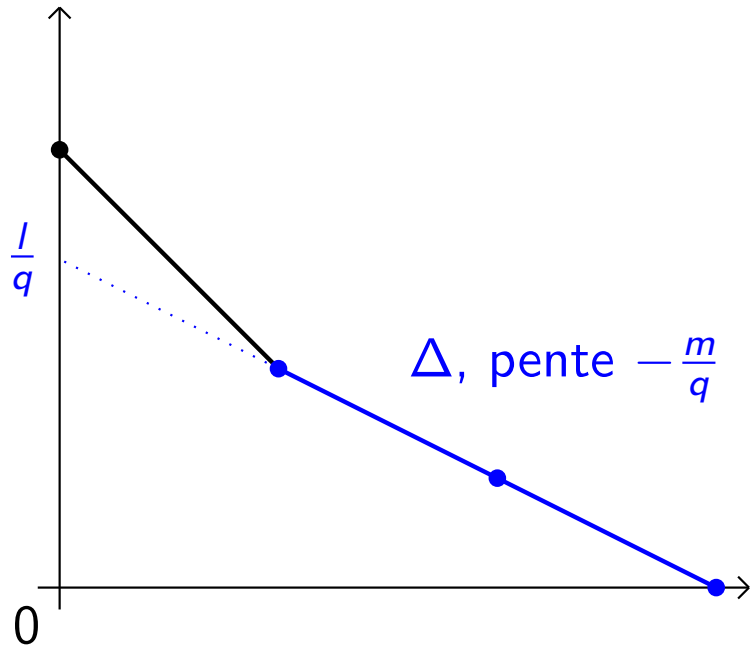
2. Pour chaque ϕ_k,

   transformation de Puiseux :

   $$F_{\Delta,\xi}(X,Y) = \frac{F(X^q, X^m(Y+\xi^{\frac{1}{q}}))}{X^l}$$

   avec ξ racine de ϕ_k.

3. Appels récursifs : $\{F_{\Delta,\xi}(X,Y)\}_{\Delta,\xi}$



Complexité arithmétique de l'algorithme de Newton-Puiseux

- D. Duval 1989 [Rational Puiseux Expansions] $\rightarrow (D^8)$
- calculs mod X^n, multiplication rapide $\rightarrow \tilde{O}(D^5)$

  Poteaux & Rybowicz [ISSAC 2008 ; AAECC 2011]
- moins d'appels récursifs (astuce + factorisation) $\rightarrow \tilde{O}(D^4)$

  Poteaux & Rybowicz [ISSAC 2015]
- Stratégie diviser pour régner $\rightarrow \tilde{O}(D^3)$

  Poteaux & Weimann [2018 ; arXiv 1708.09067]

Dans la suite : F unitaire ; factorisations univariées non comptées.

JNCF 2008

- Troncation modulo X^{n+1} ; $n = v_F = \mathrm{v}_X(\mathrm{Disc}_Y(F))$,
- Une transformation de Puiseux = n shifts univariés $\tilde{O}(v_F\, d_Y)$
- Total : #termes $\leq v_F$ $\tilde{O}(v_F^2 d_Y)$
- Séries de Puiseux au-dessus de 0 $\tilde{O}(D^5)$
- tous les points critiques $\tilde{O}(D^5)$

JNCF 2015 : moins d'étapes

S.S. Abhyankar [Newton's theorem] Hyp : F unitaire.

- $F_1(X, Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X)\, Y^k$
- On ne peut avoir $\mathcal{N}(F_1) = \Delta$, $q = 1$ et $\phi_\Delta(T) = (T - \xi)^{d_Y}$

$\Longrightarrow$ nombre d'étapes en $O(\rho \log(d_Y))$.

$$S_1 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 - X^{15/2}$$
$$S_2 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 + X^{15/2}$$
$$S_3 = X + X^2 + X^3 + X^4$$

JNCF 2015 : moins d'étapes

S.S. Abhyankar [Newton's theorem] Hyp : F unitaire.

- $F_1(X, Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X)\, Y^k$
- On ne peut avoir $\mathcal{N}(F_1) = \Delta$, $q = 1$ et $\phi_\Delta(T) = (T - \xi)^{d_Y}$

$$\Longrightarrow \text{nombre d'étapes en } O(\rho \log(d_Y)).$$

$$S_1 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 - X^{15/2}$$
$$S_2 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 + X^{15/2}$$
$$S_3 = X + X^2 + X^3 + X^4$$

JNCF 2015 : moins d'étapes

S.S. Abhyankar [Newton's theorem] Hyp : F unitaire.

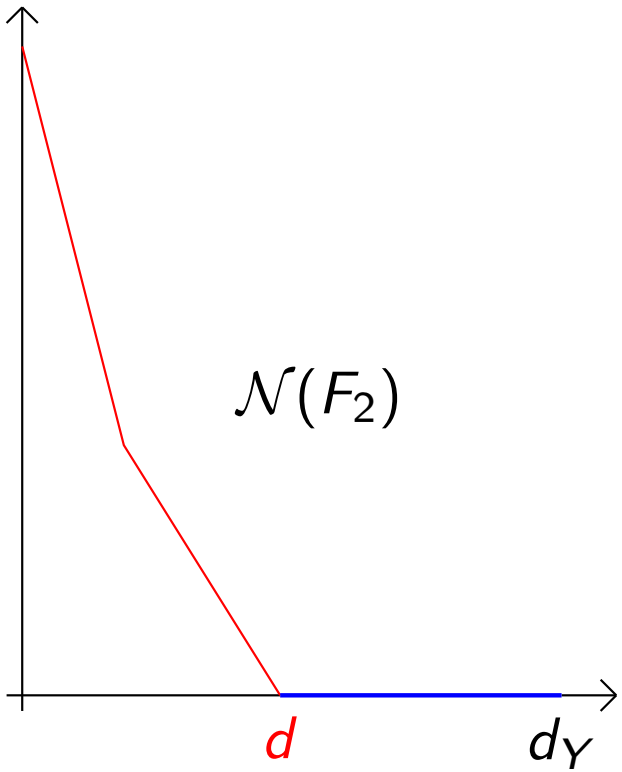
- $F_1(X, Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X)\, Y^k$
- On ne peut avoir $\mathcal{N}(F_1) = \Delta$, $q = 1$ et $\phi_\Delta(T) = (T - \xi)^{d_Y}$

$$\Longrightarrow \text{nombre d'étapes en } O(\rho \log(d_Y)).$$

$$S_1 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 - X^{15/2}$$
$$S_2 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 + X^{15/2}$$
$$S_3 = X + X^2 + X^3 + X^4$$

Théorème de préparation de Weierstrass.

$$F_2 = \frac{F_1(X^q, X^m(Y + \xi^{\frac{1}{q}}))}{X^l}$$



- $F_2(0, Y) = Y^d\, p(Y)$ avec $p(0) \neq 0$,
- Lemme de Hensel :

  $F_2 = F_3\, P$ dans $\mathbb{K}[[X]][Y]$ avec :

  - F_3 unitaire en Y,
  - $F_3(0, Y) = Y^d$,
  - $P(0, Y) = p(Y)$.
- Idée :
  1. Lemme de Hensel modulo X^{n+1},
  2. Appels récursifs avec $F_3(X, Y)$.
- Complexité : $\tilde{O}(d_Y\, n)$

Complexité

$s_k = \#\{(\Delta, \xi)\}$

1. astuce d'Abhyankar : shift bivarié — $\tilde{O}(n\, d_Y)$
2. Puiseux-shift : un par (Δ, ξ) — $s_k\, \tilde{O}(n\, d_Y)$
3. Théorème de préparation de Weierstrass — $s_k\, \tilde{O}(n\, d_Y)$
4. Appels récursifs.

- Total : $\sum_k s_k \in O(\rho \log(dy))$ — $\tilde{O}(\rho\, n\, d_Y)$
- $n = v_F (= \mathrm{v}_X(\mathrm{Disc}_Y(F)))$ — $\tilde{O}(\rho\, v_F\, d_Y) \subset \tilde{O}(D^4)$

Un algorithme diviser pour régner (F unitaire)

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\tilde{O}(v_F\, d_Y)$

Un algorithme diviser pour régner (F unitaire)

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\quad \tilde{O}(v_F\, d_Y)$
   - G facteur de F mod $X^{O(v_F/d_Y)}$; $d_Y(G) \geq d_Y/2$,
   - $H = F/G$ mod $X^{O(v_F/d_Y)}$,

Un algorithme diviser pour régner (F unitaire)

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\quad \tilde{O}(v_F\, d_Y)$
   - G facteur de F mod $X^{O(v_F/d_Y)}$; $d_Y(G) \geq d_Y/2$,
   - $H = F/G$ mod $X^{O(v_F/d_Y)}$,
2. $U\,G + V\,H = X^k$ dans $\mathbb{K}[[X]][Y]$,
   - Moroz-Schost [ISSAC'16] : $\tilde{O}(d_Y\, k)$

Un algorithme diviser pour régner (F unitaire)

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\quad \tilde{O}(v_F\, d_Y)$
   - G facteur de F mod $X^{O(v_F/d_Y)}$; $d_Y(G) \geq d_Y/2$,
   - $H = F/G$ mod $X^{O(v_F/d_Y)}$,
2. $U\,G + V\,H = X^k$ dans $\mathbb{K}[[X]][Y]$, $\quad \tilde{O}(v_F)$
   - Moroz-Schost [ISSAC'16] : $\tilde{O}(d_Y\, k)$
   - On prouve $k \in (v_F/d_Y)$,

Un algorithme diviser pour régner (F unitaire)

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\tilde{O}(v_F\, d_Y)$
   - G facteur de F mod $X^{O(v_F/d_Y)}$; $d_Y(G) \geq d_Y/2$,
   - $H = F/G$ mod $X^{O(v_F/d_Y)}$,
2. $U\,G + V\,H = X^k$ dans $\mathbb{K}[[X]][Y]$, $\tilde{O}(v_F)$
   - Moroz-Schost [ISSAC'16] : $\tilde{O}(d_Y\, k)$
   - On prouve $k \in (v_F/d_Y)$,
3. Adaptation Hensel $\rightsquigarrow$ $F = G \cdot H$ modulo X^{v_F+1}, $\tilde{O}(v_F\, d_Y)$

Un algorithme diviser pour régner (F unitaire)

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\tilde{O}(v_F\, d_Y)$
   - G facteur de F mod $X^{O(v_F/d_Y)}$; $d_Y(G) \geq d_Y/2$,
   - $H = F/G$ mod $X^{O(v_F/d_Y)}$,
2. $U\,G + V\,H = X^k$ dans $\mathbb{K}[[X]][Y]$, $\tilde{O}(v_F)$
   - Moroz-Schost [ISSAC'16] : $\tilde{O}(d_Y\, k)$
   - On prouve $k \in (v_F/d_Y)$,
3. Adaptation Hensel $\rightsquigarrow$ $F = G \cdot H$ modulo X^{v_F+1}, $\tilde{O}(v_F\, d_Y)$
4. Appel récursif pour H $2\times\tilde{O}(v_F\, d_Y)$

Un algorithme diviser pour régner (F unitaire)

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\tilde{O}(v_F\, d_Y)$
   - G facteur de F mod $X^{O(v_F/d_Y)}$; $d_Y(G) \geq d_Y/2$,
   - $H = F/G$ mod $X^{O(v_F/d_Y)}$,
2. $U\,G + V\,H = X^k$ dans $\mathbb{K}[[X]][Y]$, $\tilde{O}(v_F)$
   - Moroz-Schost [ISSAC'16] : $\tilde{O}(d_Y\, k)$
   - On prouve $k \in (v_F/d_Y)$,
3. Adaptation Hensel $\rightsquigarrow$ $F = G \cdot H$ modulo X^{v_F+1}, $\tilde{O}(v_F\, d_Y)$
4. Appel récursif pour H $2\times\tilde{O}(v_F\, d_Y)$

- Pas de factorisation univariée ? D5 Dahan-Schost-Maza-Wu-Xie05

Un algorithme diviser pour régner $v_F = \mathrm{v}_X(\mathrm{Res}_Y(F, F_Y))$

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\tilde{O}(v_F\, d_Y)$
   - G facteur de F mod $X^{O(v_F/d_Y)}$; $d_Y(G) \geq d_Y/2$,
   - $H = F/G$ mod $X^{O(v_F/d_Y)}$,
2. $U\,G + V\,H = X^k$ dans $\mathbb{K}[[X]][Y]$, $\tilde{O}(v_F)$
   - Moroz-Schost [ISSAC'16] : $\tilde{O}(d_Y\, k)$
   - On prouve $k \in (v_F/d_Y)$,
3. Adaptation Hensel $\rightsquigarrow$ $F = G \cdot H$ modulo X^{v_F+1}, $\tilde{O}(v_F\, d_Y)$
4. Appel récursif pour H $2\times\tilde{O}(v_F\, d_Y)$

- Pas de factorisation univariée ? D5 Dahan-Schost-Maza-Wu-Xie05
- Cas non unitaire : $F = u\,F_0\,F_\infty \mod X^{v_F+1}$ $\tilde{O}(v_F\, d_Y)$

Un algorithme diviser pour régner $v_F = \mathrm{v}_X(\mathrm{Res}_Y(F, F_Y))$

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\tilde{O}(v_F\, d_Y)$
   - G facteur de F mod $X^{O(v_F/d_Y)}$; $d_Y(G) \geq d_Y/2$,
   - $H = F/G$ mod $X^{O(v_F/d_Y)}$,
2. $U\,G + V\,H = X^k$ dans $\mathbb{K}[[X]][Y]$, $\tilde{O}(v_F)$
   - Moroz-Schost [ISSAC'16] : $\tilde{O}(d_Y\, k)$
   - On prouve $k \in (v_F/d_Y)$,
3. Adaptation Hensel $\rightsquigarrow$ $F = G \cdot H$ modulo X^{v_F+1}, $\tilde{O}(v_F\, d_Y)$
4. Appel récursif pour H $2\times\tilde{O}(v_F\, d_Y)$

- Pas de factorisation univariée ? D5 Dahan-Schost-Maza-Wu-Xie05
- Cas non unitaire : $F = u\,F_0\,F_\infty \mod X^{v_F+1}$ $\tilde{O}(v_F\, d_Y)$

Total : $\tilde{O}(v_F\, d_Y) \subset \tilde{O}(D^3)$

Un algorithme diviser pour régner $v_F = \mathrm{v}_X(\mathrm{Res}_Y(F, F_Y))$

1. $n \in (v_F/d_Y) \rightsquigarrow$ la moitié des séries, $\tilde{O}(v_F\, d_Y)$
   - G facteur de F mod $X^{O(v_F/d_Y)}$; $d_Y(G) \geq d_Y/2$,
   - $H = F/G$ mod $X^{O(v_F/d_Y)}$,
2. $U\,G + V\,H = X^k$ dans $\mathbb{K}[[X]][Y]$, $\tilde{O}(v_F)$
   - Moroz-Schost [ISSAC'16] : $\tilde{O}(d_Y\, k)$
   - On prouve $k \in (v_F/d_Y)$,
3. Adaptation Hensel $\rightsquigarrow$ $F = G \cdot H$ modulo X^{v_F+1}, $\tilde{O}(v_F\, d_Y)$
4. Appel récursif pour H $2\times\tilde{O}(v_F\, d_Y)$

- Pas de factorisation univariée ? D5 Dahan-Schost-Maza-Wu-Xie05
- Cas non unitaire : $F = u\,F_0\,F_\infty \mod X^{v_F+1}$ $\tilde{O}(v_F\, d_Y)$

Total : $\tilde{O}(v_F\, d_Y) \subset \tilde{O}(D^3)$

Tous les points critiques : $\tilde{O}(D^3)$