

Sur le calcul efficace des séries de Puiseux

Adrien Poteaux^{*} & Marc Rybowicz[†]

^{*}: CFHP - CO2 - CRIStAL - Université de Lille

[†]: DMI - XLIM - Université de Limoges

JNCF 2015, Cluny

3 Novembre 2015

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \leadsto$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3Y + 2 \leadsto y_1 = 1, y_2 = 2,$
- $F(Y) = Y^2 - Y + 1 \leadsto y_1 = 4, y_2 = 8 \quad (\mathbb{K} = \mathbb{F}_{11})$
 $\leadsto y_1 = \frac{1+\sqrt{5}}{2}, y_2 = \frac{1-\sqrt{5}}{2} \quad (\mathbb{K} = \mathbb{Q})$
 $\leadsto y_1 = 1.618, y_2 = -0.618 \quad (\mathbb{K} = \mathbb{C})$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3Y + 2 \rightsquigarrow y_1 = 1, y_2 = 2,$
- $F(Y) = Y^2 - Y + 1 \rightsquigarrow y_1 = 4, y_2 = 8 \quad (\mathbb{K} = \mathbb{F}_{11})$
 $\rightsquigarrow y_1 = \frac{1+\sqrt{5}}{2}, y_2 = \frac{1-\sqrt{5}}{2} \quad (\mathbb{K} = \mathbb{Q})$
 $\rightsquigarrow y_1 = 1.618, y_2 = -0.618 \quad (\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ polynômes ?

Exemple

$$Y^2 - (2X + 3)Y + X^2 + 3X + 2 \rightsquigarrow \left. \begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array} \right\} \in \mathbb{K}[X]$$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3Y + 2 \rightsquigarrow y_1 = 1, y_2 = 2,$
- $F(Y) = Y^2 - Y + 1 \rightsquigarrow \begin{array}{ll} y_1 = 4, y_2 = 8 & (\mathbb{K} = \mathbb{F}_{11}) \\ \rightsquigarrow y_1 = \frac{1+\sqrt{5}}{2}, y_2 = \frac{1-\sqrt{5}}{2} & (\mathbb{K} = \mathbb{Q}) \\ \rightsquigarrow y_1 = 1.618, y_2 = -0.618 & (\mathbb{K} = \mathbb{C}) \end{array}$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Taylor ?

Exemple

$$\begin{aligned} Y^2 - (2X + 3)Y + X^2 + 3X + 2 &\rightsquigarrow \left. \begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array} \right\} \in \mathbb{K}[X] \\ (1 - X)Y - 1 &\rightsquigarrow Y_1(X) = 1 + X + X^2 + \dots \in \mathbb{K}[[X]] \end{aligned}$$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3Y + 2 \rightsquigarrow y_1 = 1, y_2 = 2,$
- $F(Y) = Y^2 - Y + 1 \rightsquigarrow y_1 = 4, y_2 = 8 \quad (\mathbb{K} = \mathbb{F}_{11})$
 $\rightsquigarrow y_1 = \frac{1+\sqrt{5}}{2}, y_2 = \frac{1-\sqrt{5}}{2} \quad (\mathbb{K} = \mathbb{Q})$
 $\rightsquigarrow y_1 = 1.618, y_2 = -0.618 \quad (\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Laurent ?

Exemple

$$Y^2 - (2X + 3)Y + X^2 + 3X + 2 \rightsquigarrow \left. \begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array} \right\} \in \mathbb{K}[X]$$
$$X^2(1 - X)Y - 1 \rightsquigarrow Y_1(X) = X^{-2} + X^{-1} + 1 + X + \dots \in \mathbb{K}((X))$$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3Y + 2 \rightsquigarrow y_1 = 1, y_2 = 2,$
- $F(Y) = Y^2 - Y + 1 \rightsquigarrow y_1 = 4, y_2 = 8 \quad (\mathbb{K} = \mathbb{F}_{11})$
 $\rightsquigarrow y_1 = \frac{1+\sqrt{5}}{2}, y_2 = \frac{1-\sqrt{5}}{2} \quad (\mathbb{K} = \mathbb{Q})$
 $\rightsquigarrow y_1 = 1.618, y_2 = -0.618 \quad (\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Laurent ?

Exemple

$$Y^2 - (2X + 3)Y + X^2 + 3X + 2 \rightsquigarrow \left. \begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array} \right\} \in \mathbb{K}[X]$$

$$X^2(1 - X)Y - 1 \rightsquigarrow Y_1(X) = X^{-2} + X^{-1} + 1 + X + \dots \in \mathbb{K}((X))$$

$$Y^3 - X$$

$$\rightsquigarrow Y_i(X) = \xi_3^i \sqrt[3]{X}, \xi_3^3 = 1 \in \overline{\mathbb{K}}[X^{1/3}]$$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3Y + 2 \rightsquigarrow y_1 = 1, y_2 = 2,$
- $F(Y) = Y^2 - Y + 1 \rightsquigarrow y_1 = 4, y_2 = 8 \quad (\mathbb{K} = \mathbb{F}_{11})$
 $\rightsquigarrow y_1 = \frac{1+\sqrt{5}}{2}, y_2 = \frac{1-\sqrt{5}}{2} \quad (\mathbb{K} = \mathbb{Q})$
 $\rightsquigarrow y_1 = 1.618, y_2 = -0.618 \quad (\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Laurent ?

Exemple

$$Y^2 - (2X + 3)Y + X^2 + 3X + 2 \rightsquigarrow \left. \begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array} \right\} \in \mathbb{K}[X]$$

$$X^2(1 - X)Y - 1 \rightsquigarrow Y_1(X) = X^{-2} + X^{-1} + 1 + X + \dots \in \mathbb{K}((X))$$

$$(1 + X)^2 Y^2 - 2(X + 1)Y - X + 1$$

$$\rightsquigarrow Y_i(X) = 1 + \xi_2^i X^{1/2} - X - \xi_2^i X^{3/2} + X^2 + \dots \in \mathbb{K}[[X^{1/2}]]$$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3Y + 2 \rightsquigarrow y_1 = 1, y_2 = 2,$
- $F(Y) = Y^2 - Y + 1 \rightsquigarrow y_1 = 4, y_2 = 8 \quad (\mathbb{K} = \mathbb{F}_{11})$
 $\rightsquigarrow y_1 = \frac{1+\sqrt{5}}{2}, y_2 = \frac{1-\sqrt{5}}{2} \quad (\mathbb{K} = \mathbb{Q})$
 $\rightsquigarrow y_1 = 1.618, y_2 = -0.618 \quad (\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Puiseux

Exemple

$$Y^2 - (2X + 3)Y + X^2 + 3X + 2 \rightsquigarrow \left. \begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array} \right\} \in \mathbb{K}[X]$$

$$X^2(1 - X)Y - 1 \rightsquigarrow Y_1(X) = X^{-2} + X^{-1} + 1 + X + \dots \in \mathbb{K}((X))$$

$$X^2(1 + X)^2 Y^2 - 2(X + 1)Y - X + 1$$
$$\rightsquigarrow Y_i(X) = X^{-1} + \xi_2^i X^{-1/2} - 1 - \xi_2^i X^{1/2} + \dots \in \mathbb{K}((X^{1/2}))$$

Théorème (Puisseux, 1850)

Il existe $e_1, \dots, e_s \in \mathbb{N}^$ tels que $d_Y = \sum_{i=1}^s e_i$ et F (vu comme un polynôme univarié en Y) possède d_Y racines distinctes dans $\overline{\mathbb{K}((X - x_0))}$ qui peuvent s'écrire de la façon suivante :*

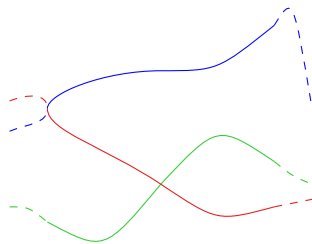
$$Y_{ij}(X) = \sum_{k=n_i}^{\infty} \alpha_{i,k} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}}$$

avec :

- $0 \leq j \leq e_i - 1, 1 \leq i \leq s,$
- $n_i \in \mathbb{Z}, \alpha_{i,n_i} \neq 0$
- ζ_{e_i} racine primitive de l'unité d'ordre e_i

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

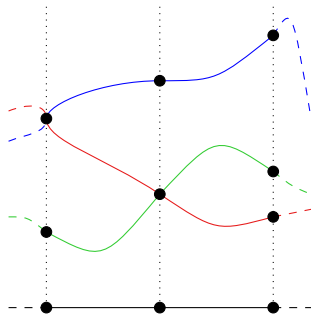
Racines de $F \in \mathbb{K}[X][Y]$



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

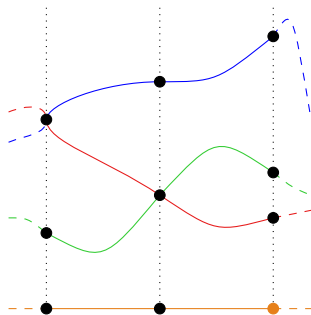
- **Fibre** en $x_0 \in \mathbb{C} : \mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}.$



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

- **Fibre** en $x_0 \in \mathbb{C} : \mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}.$
- **Point régulier** : $\#\mathcal{F}(x_0) = d_Y.$

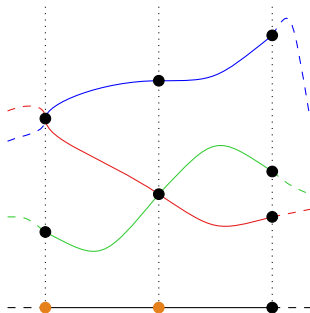


$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

- **Fibre** en $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}$.
- **Point régulier** : $\#\mathcal{F}(x_0) = d_Y$.

- **Point critique** : $\#\mathcal{F}(x_0) < d_Y$.
 $\implies$ racines de $\text{Res}_Y(F, F_Y)$.



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

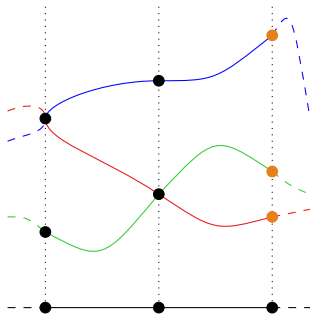
- **Fibre** en $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}$.
- **Point régulier** : $\#\mathcal{F}(x_0) = d_Y$.

d_Y séries de Taylor :

$$Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik}(X - x_0)^k$$

(Théorème des fonctions implicites)

- **Point critique** : $\#\mathcal{F}(x_0) < d_Y$.
 $\implies$ racines de $\text{Res}_Y(F, F_Y)$.



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

- **Fibre** en $x_0 \in \mathbb{C} : \mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}.$
- **Point régulier** : $\#\mathcal{F}(x_0) = d_Y.$

d_Y séries de Taylor :

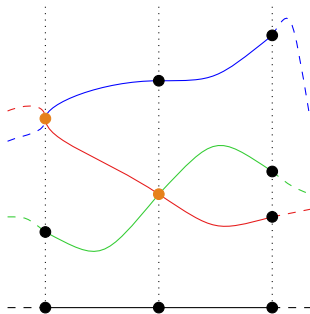
$$Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik} (X - x_0)^k$$

(Théorème des fonctions implicites)

- **Point critique** : $\#\mathcal{F}(x_0) < d_Y.$
 $\implies$ racines de $\text{Res}_Y(F, F_Y).$

Séries de Puiseux :

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



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Partie singulière

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

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

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

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

Cet exposé : complexité arithmétique sur $\mathbb{F}_{p^n}$

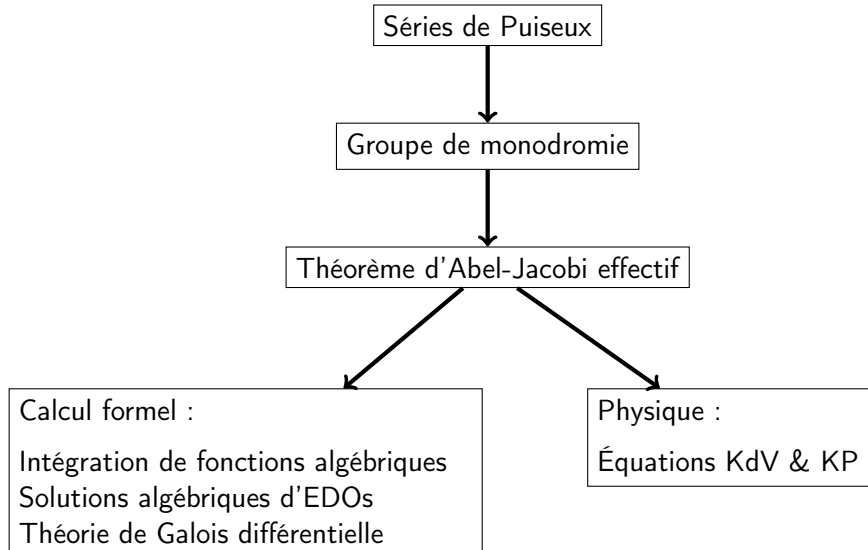
- Article associé : *Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields* (ISSAC'15)
- Les références numérotées / les numéros de pages sont celles de ce papier.

On ne considère pas :

- croissance des coefficients / complexité binaire sur $\mathbb{K} = \mathbb{Q}$
 - expliqué dans Chistov [12], Walsh [53,54]
 - stratégie symbolique / numérique P. & Rybowicz [39,41...]

On suppose $p > \deg_Y(F)$ (comme dans P. & Rybowicz [39,41])

Motivation initiale



Séries de Puiseux et monodromie locale

$$H(X, Y) = (Y^3 - X)((Y - 1)^2 - X)(Y - 2 - X^2) + X^2 Y^5$$

$$2 - 3X^2 - \frac{9}{2}X^3 + \dots$$

$\Rightarrow e = 1 : 1\text{-cycle.}$

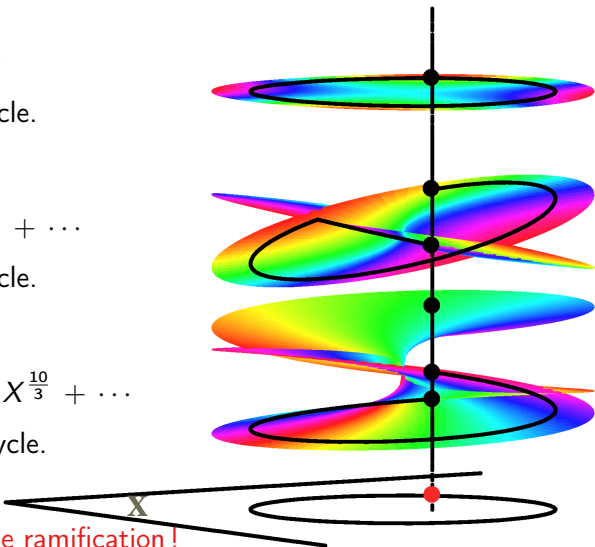
$$1 + \zeta_2^i X^{\frac{1}{2}} + \frac{1}{2} \zeta_2^i X^{\frac{3}{2}} + \dots$$

$\Rightarrow e = 2 : 2\text{-cycle.}$

$$\zeta_3^i X^{\frac{1}{3}} + \frac{1}{6} X^3 + \frac{5}{12} \zeta_3^i X^{\frac{10}{3}} + \dots$$

$\Rightarrow e = 3 : 3\text{-cycle.}$

La monodromie locale
correspond aux indices de ramification !



Calcul d'une série de Puiseux : idée et outils

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

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

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

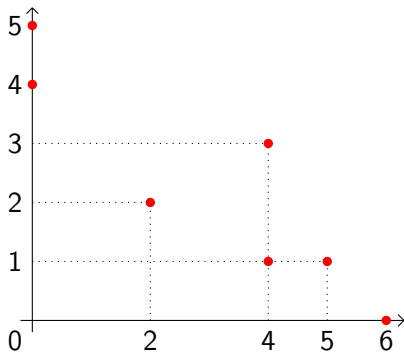
- On doit annuler au moins deux termes !

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

Support d'un polynôme

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

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



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

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

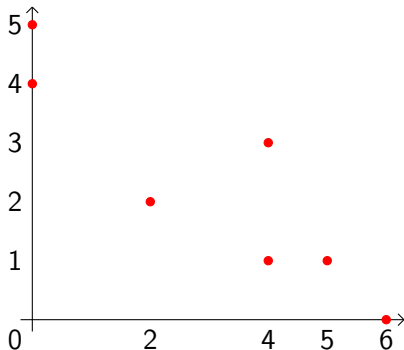
- $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

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

$\leadsto$ au moins 2 points sur $mi + qj = l$

- * augmenter l'ordre en X ?

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



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

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

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

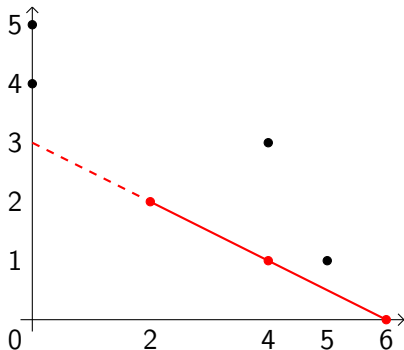
- * (m, q) pour annuler deux termes ?

$\leadsto$ au moins 2 points sur $mi + qj = l$

- * augmenter l'ordre en X ?

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

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



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

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

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

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

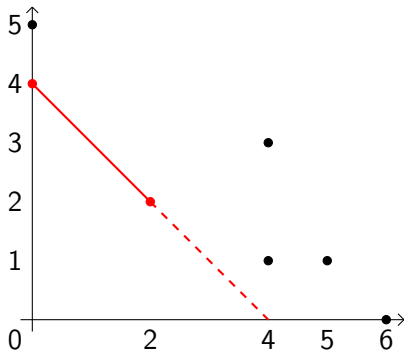
$\leadsto$ au moins 2 points sur $mi + qj = l$

- * augmenter l'ordre en X ?

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

$(\Delta_1) \ i + 2j = 6$ est une telle droite

$(\Delta_2) \ i + j = 4$ aussi

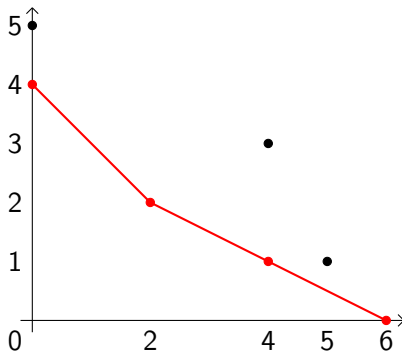


Polygone de Newton

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

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

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



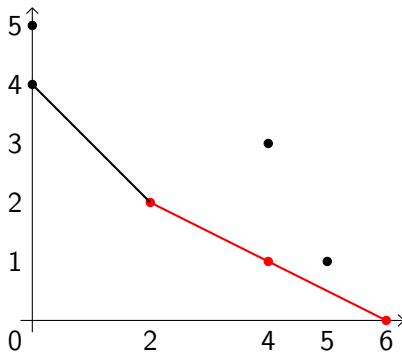
Choix de α qui augmente l'ordre en X ?

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

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

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

$$F(T^2, \alpha T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2) T^6 - 3 T^8 + \alpha^5 T^7 + (5\alpha^4 + 1) T^{10} + \dots$$



Polynôme caractéristique

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

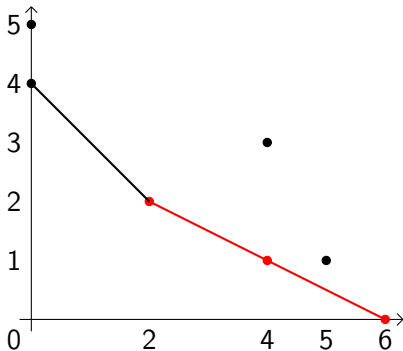
- $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

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

$$\begin{aligned} F(T^2, \alpha T) &= (\alpha^6 - 2\alpha^4 + 4\alpha^2) T^6 \\ &\quad - 3 T^8 + \alpha^5 T^7 + (5\alpha^4 + 1) T^{10} + \dots \end{aligned}$$

Polynôme caractéristique :

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



Algorithme de Newton-Puiseux rationnel Duval [22,23]

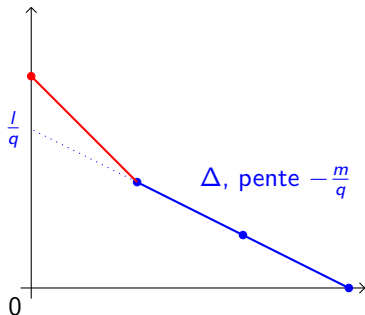
Pour chaque arête Δ de $\mathcal{N}(F)$

- Factoriser $\phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$
- Pour chaque facteur ϕ_k , **RNP-shift** :

$$H_{\Delta, \xi_k}(X, Y) = \frac{F(\xi_k^v X^q, X^m(\xi_k^u + Y))}{X^l}$$

avec

- ξ_k t.q. $\phi_k(\xi_k) = 0$,
 - (u, v) tel que $uq - vm = 1$.
- Appels récurifs : $\{H_{\Delta, \xi_k} ; M_k > 1\}_{\Delta, \xi_k}$



Développements de Puiseux rationnels

Définition (Duval, 1989)

- F irréductible dans $\mathbb{K}[X, Y]$: « un développement par place »

$$R_i(T) = (X_i(T), Y_i(T)) = \left(\lambda_i T^{e_i}, \sum_{k=n_i}^{\infty} \beta_{i,k} T^k \right) \in \overline{\mathbb{K}}((T))^2$$

avec

- $e_i > 0$, $n_i \in \mathbb{Z}$, $\lambda_i \neq 0$, et $\beta_{i,n_i} \neq 0$,
- paramétrisation irréductible : $R_i(T) \notin \overline{\mathbb{K}}((T^\kappa))$ pour $\kappa > 1$
- $R_i(T)$ invariant par l'action du groupe de Galois $\mathcal{G}(\overline{\mathbb{K}}/\mathbb{K})$
- $F = F_1 \cdots F_r$ sans carré : $\{\text{dvts de Puiseux rationnels de } F_k\}$

Si l'on note :

- ρ le nombre de développements rationnels.
- $\mathbb{K}_i$ le corps des coefficients de R_i et $f_i = [\mathbb{K}_i : \mathbb{K}]$.

Théorème :

$$\sum_{i=1}^{\rho} e_i f_i = d_Y$$

Lien avec la factorisation.

Développements de Puiseux rationnels :

$$F = \prod_{i=1}^{\rho} F_i \text{ avec } F_i \text{ irréductible dans } \mathbb{K}[[X]][Y]$$

Action du groupe de Galois :

$$F_i = \prod_{j=1}^{f_i} F_{ij} \text{ avec } F_{ij} \text{ irréductible dans } \overline{\mathbb{K}}[[X]][Y]$$

Séries de Puiseux :

$$F_{ij} = A_{d_Y} \prod_{k=0}^{e_i-1} \left(Y - S_{ij}(X^{1/e_i} \zeta_{e_i}^k) \right) \text{ avec } S_{ij} \in \overline{\mathbb{K}}[[X]]$$

État de l'art (Newton-Puiseux)

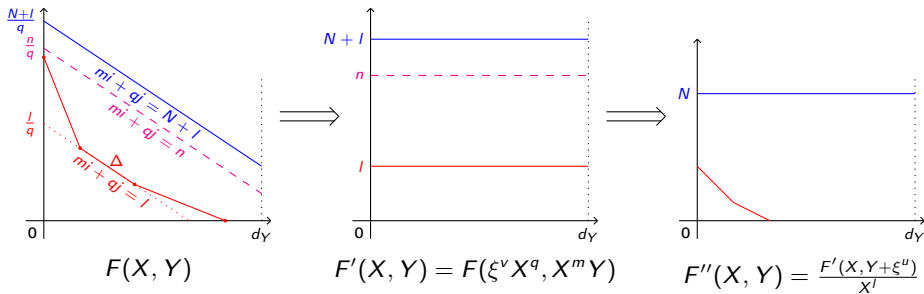
- Newton (1676) : donne le principe.
- Puiseux (1850) : première procédure.
- Chystov 1986 [12] : complexité binaire polynomiale.
- Duval 1989 [23] : algorithme rationnel $\rightarrow O(D^8)$ op. dans $\mathbb{K}$.
- Walsh 2000 [54] : $\tilde{O}(d_Y^{32} d_X^4)$ (algo classique).
- Walsh 1999 [53] : taille polynomiale des coefficients de certains développements rationnels.
- P. & Rybowicz 2008 [39, 40] : algorithme en $\tilde{O}(D^5)$ op. dans $\mathbb{K}$.

État de l'art (complexité arithmétique)

- variantes de l'algorithme Newton-Puiseux
 - Duval [22, 23] $\rightarrow O(D^8)$
 - P. & Rybowicz [39, 40] $\rightarrow \tilde{O}(D^5)$
- Factorisation dans $\mathbb{F}_q[[X]][Y]$ ou $\overline{\mathbb{F}_q}[[X]][Y]$ (algorithme de Montes)
 - Bauch, Nart & Stainsby [3] : $\tilde{O}(D^5)$, test d'irréductibilité test $\tilde{O}(D^4)$
 - voir aussi Pauli [37, 38], Ford & Veres [25]
- méthodes à la Hensel
 - Sasaki, Inaba, Kako [28, 44, 45]
 - Berthomieu, Quintin, Lecerf [5] (cas particulier)

on note $v_F = v_X(\text{Disc}_Y(F))$; P. & Rybowicz [39, 40] :

- Un RNP-shift mod X^N : $\mathcal{O}(N d_Y)$,



- Borne de troncation : $N \leq v_F$,
- Nombre d'étapes borné par v_F .

$\Rightarrow$ complexité en $\mathcal{O}(v_F^2 d_Y) \subset \mathcal{O}(d_X^2 d_Y^3) \subset \mathcal{O}(D^5)$

Contributions : amélioration de l'algorithme Newton-Puiseux

- astuce d'Abhyankhar : moins d'étapes ($O(d_X d_Y) \rightarrow \tilde{O}(d_Y)$)
 - polynôme distingué nécessaire.
- Factorisation de F dans $\mathbb{F}_q[[X]][Y]$ au fur et à mesure de l'algorithme
 - réduit d_Y pour les appels récurrents,
 - rend le polynôme distingué.

$\implies$ nouvel algorithme en $\tilde{O}(D^4)$.
- Factorisation rapide de F selon le polygone de Newton

Moins d'étapes ?

Idée : Réduire d_Y à chaque étape

Comment ? Calcul direct des racines communes

Abhyankar [1] : Si F est unitaire,

- $$G(X, Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X) Y^k$$

- On ne peut avoir $\mathcal{N}(G) = \Delta$, $q = 1$ et $\phi_\Delta(T) = (T - \xi)^{d_Y}$

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

Moins d'étapes ?

Idée : Réduire d_Y à chaque étape

Comment ? Calcul direct des racines communes

Abhyankar [1] : Si F est unitaire,

- $G(X, Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X) Y^k$

- On ne peut avoir $\mathcal{N}(G) = \Delta$, $q = 1$ et $\phi_\Delta(T) = (T - \xi)^{d_Y}$

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

Exemple 2 p. 303 :

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

$$S_2 = X + X^2 + X^3 + 17X^4 + X^5 + X^6 + X^7 + X^{15/2}$$

$$S_3 = X + X^2 + X^3 + X^4$$

Moins d'étapes ?

Idée : Réduire d_Y à chaque étape

Comment ? Calcul direct des racines communes

Abhyankar [1] : Si F est unitaire,

- $G(X, Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X) Y^k$

- On ne peut avoir $\mathcal{N}(G) = \Delta$, $q = 1$ et $\phi_\Delta(T) = (T - \xi)^{d_Y}$

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

Exemple 2 p. 303 :

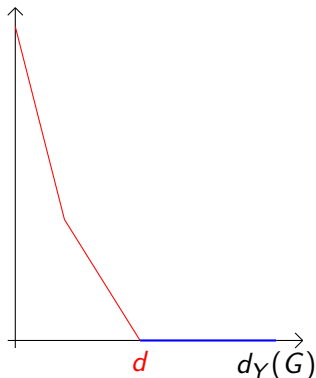
$$S_1 = X + X^2 + X^3 + 17X^4 + X^5 + X^6 + X^7 - X^{15/2}$$

$$S_2 = X + X^2 + X^3 + 17X^4 + X^5 + X^6 + X^7 + X^{15/2}$$

$$S_3 = X + X^2 + X^3 + X^4$$

Théorème de préparation de Weierstrass.

Après un RNP-shift :



- $G(0, Y) = Y^d p(Y)$ avec $p(0) \neq 0$,

- Lemme de Hensel :

$G = HP$ in $\mathbb{F}_q[[X]][Y]$ avec :

- H unitaire en Y ,
- $H(0, Y) = Y^d$,
- $P(0, Y) = p(Y)$.

- Algorithme :

- 1 Lemme de Hensel modulo X^{N+1} ,
- 2 Appels récursifs avec $H(X, Y)$.

- Complexité : $\mathcal{O}(d_Y N)$

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

① Abhyankar : shift bivarié $\mathcal{O}(N d_Y)$

② RNP-shift : un par (Δ, ξ) $s_k \mathcal{O}(N d_Y)$

③ Théorème de préparation de Weierstrass $s_k \mathcal{O}(N d_Y)$

④ Appels récursifs.

• Total : $\sum_k s_k \in \mathcal{O}(\rho \log(dy))$ $\mathcal{O}(\rho N d_Y)$

• $N = v_F(= v_X(\text{Disc}_Y(F)))$ $\mathcal{O}(\rho v_F d_Y) \subset \mathcal{O}(d_X d_Y^3)$

• Factorisations P. & Rybowicz [39,40] $\mathcal{O}(d_Y^3 + d_Y^2 \log(q))$

Calcul de complexité fin : famille d'exemples

Exemple (exemple 3, p. 305)

$$F(X, Y) = \prod_{k=1}^N (Y - S_k) \text{ avec}$$

$$S_1(X) = 2X$$

$$S_2(X) = X + 2X^2$$

... ..

$$S_{N-1}(X) = X + X^2 + \dots + X^{N-2} + 2X^{N-1}$$

$$S_N(X) = X + X^2 + \dots + X^{N-2} + X^{N-1} + 2X^N$$

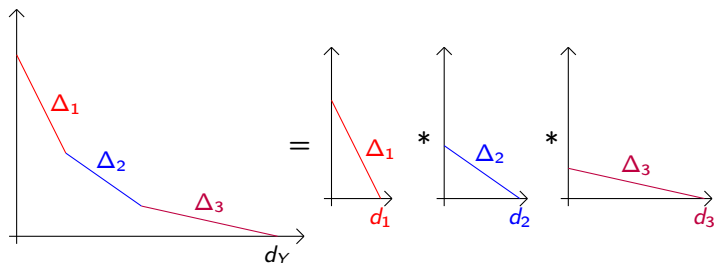
- $\rho = d_Y = N$, $d_X \in \Theta(N^2)$. $v_F \in \Theta(N^3) = \Theta(d_X d_Y)$.
- Cost is $N^3 \times (N + (N-1) + \dots + 3 + 2) \simeq N^5$.

$\Rightarrow$ complexité en $\Theta(d_X d_Y^3)$.

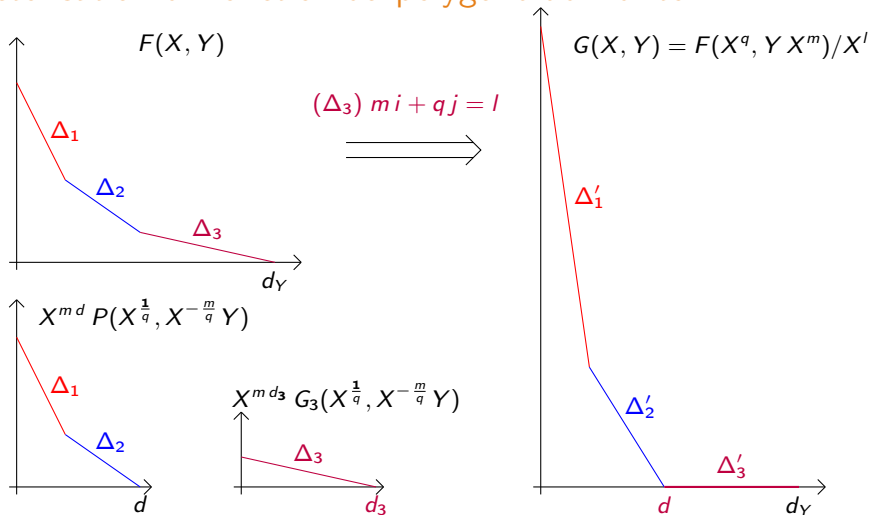
Factorisation en fonction du polygone de Newton

En théorie, on a dans $L[[X]][Y]$:

$$F = F_1 * F_2 * F_3$$

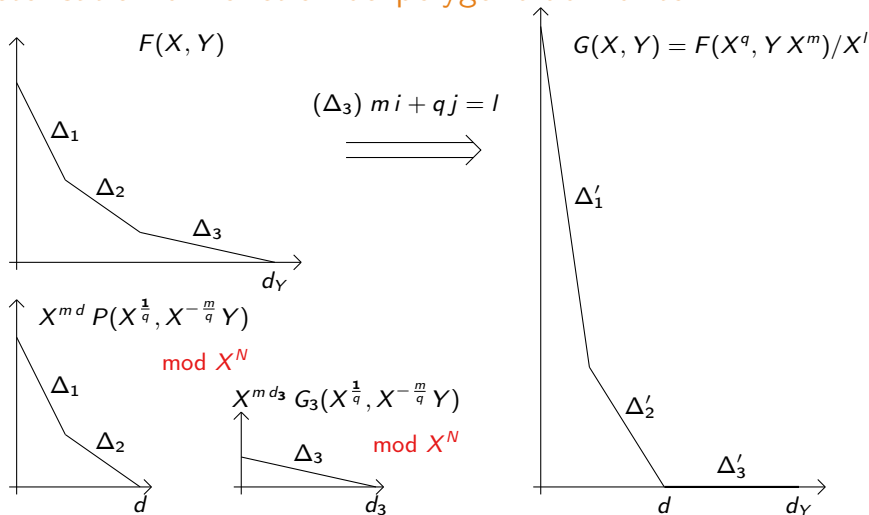


Factorisation en fonction du polygone de Newton



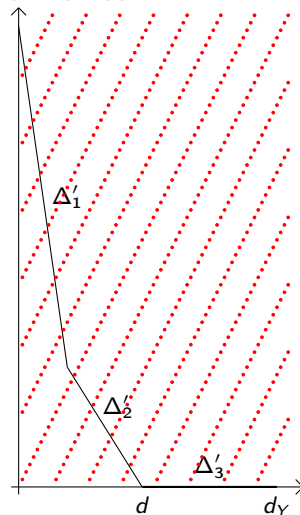
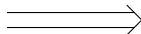
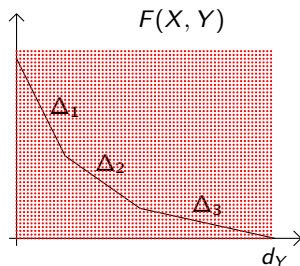
$$G(X, Y) = P(X, Y) G_3(X, Y) \xLeftrightarrow{\text{Lemme de Hensel}} G(0, Y) = Y^d g_3(Y)$$

Factorisation en fonction du polygone de Newton



$$G(X, Y) = P(X, Y) G_3(X, Y) \xleftarrow{\text{Lemme de Hensel}} G(0, Y) = Y^d g_3(Y) \bmod X^{qN}$$

Factorisation en fonction du polygone de Newton



Lebreton, Schost, van der Hoeven [34]

Conclusion

- Une meilleure complexité (pire des cas) au-dessus de $x = 0$.

$$\sigma(D^5) \implies \sigma(D^4)$$

- Ne marche pas sur *tous* les points critiques.
 - Factorisation trop coûteuse,
 - Devrait passer avec un algorithme à la D5
Della Dora, Dicrescenzo, Duval [20]
- Factorisation rapide selon $\mathcal{N}(F)$ en utilisant Lebreton, Schost, van der Hoeven [34]

Encore mieux ?

- **Idée** : on calcule $d_Y/2$ séries "faciles" $\leadsto$ factoriser $F = G H$.
 - $G \leftrightarrow S_1, \dots, S_{d_Y/2}$ (séries « faciles » $\rightarrow N \in O(d_X)$)
 - $H \leftrightarrow S_{d_Y/2+1}, \dots, S_{d_Y}$ (séries « difficiles »)
- Problème : $G(0, Y)$ et $H(0, Y)$ pas premiers entre eux,
- G et H sans racines communes, i.e. premiers dans $K(X)[Y]$,
- Euclide dans $K(X)[Y]$: $U_0 G + V_0 H = 1$,
 $U_0, V_0 \in K(X)[Y]$, $d_Y(U_0) < d_Y(H)$ et $d_Y(V_0) < d_Y(G)$
- $k = -\min(v_X(U_0), v_X(V_0)) \leadsto U G + V H = X^k \pmod{X^M}$.
- Adaptation du lemme de Hensel ? $\implies$ Oui si $M > 4k$ ► détails

??? Borne sur k ???

Merci !

Lemme de Hensel adapté

- On a :
- $F = G \cdot H + X^M \alpha(X, Y),$
 - $U \cdot G + V \cdot H = X^k + X^M \beta(X, Y); \text{ hyp : } M > 4k.$

On définit :

- $\tilde{G} = G + X^{M-k} \alpha \cdot V \pmod{X^{2M-2k}}$
- $\tilde{H} = H + X^{M-k} \alpha \cdot U \pmod{X^{2M-2k}}$
- $\tilde{U} = U - (X^{M-k} \beta + 2X^{M-2k} \alpha \cdot U \cdot V) \cdot U \pmod{X^{2M-4k}}$
- $\tilde{V} = V - (X^{M-k} \beta + 2X^{M-2k} \alpha \cdot U \cdot V) \cdot V \pmod{X^{2M-4k}}$

- Alors :
- $F = \tilde{G} \cdot \tilde{H} \pmod{X^{2M-2k}}$
 - $\tilde{U} \cdot \tilde{G} + \tilde{V} \cdot \tilde{H} = X^k \pmod{X^{2M-4k}}$

⬅ retour