Factorisation par les pentes des polynômes de Ore

Xavier Caruso

Séminaire *calculs et preuves*

1er mars 2016

Polynômes de Ore

Le cas d'un endomorphisme

Soient : $\mathfrak{A}$ — un anneau (commutatif)

$\theta : \mathfrak{A} \to \mathfrak{A}$ — un morphisme d'anneaux

À ces données, on associe l'anneau $\mathfrak{A}[X, \theta]$:

- ses éléments sont les polynômes à coefficients dans $\mathfrak{A}$
- l'addition est l'addition usuelle des polynômes
- règle de multiplication :

$$X^n \cdot a = \theta^n(a) \cdot X^n \qquad (a \in \mathfrak{A})$$

Exemples

- $\theta = \mathrm{id} \implies$ on retrouve les polynômes usuels
- $\mathfrak{A} = \mathbb{C}$, $\theta =$ conjugaison complexe
- $\mathfrak{A} = \mathbb{F}_q$, $\theta =$ Frobenius
- $\mathfrak{A} = k(x)$, $\theta : x \mapsto x + 1$

Le cas d'une dérivation

Soient : $\mathfrak{A}$ — un anneau (commutatif)

$\partial : \mathfrak{A} \to \mathfrak{A}$ — une dérivation
i.e. $\partial(ab) = a \cdot \partial(b) + \partial(a) \cdot b$

À ces données, on associe l'anneau $\mathfrak{A}[X, \partial]$:

- ses éléments sont les polynômes à coefficients dans $\mathfrak{A}$
- l'addition est l'addition usuelle des polynômes
- règle de multiplication :

$$X \cdot a = a \cdot X + \partial(a) \quad (a \in \mathfrak{A})$$

Exemples

- $\partial = 0 \implies$ on retrouve les polynômes usuels
- $\mathfrak{A} = k(x)$, $\partial = \frac{d}{dx}$
- $\mathfrak{A} = \mathcal{M}(D)$, $\partial = \frac{d}{dx}$

Division euclidienne à droite

Proposition

On suppose que $\mathfrak{A} = K$ est un **corps**

Soient $A, B \in K[X, \bullet]$ avec $B \neq 0$

Alors, il existe $Q, R \in K[X, \bullet]$ uniques tels que :

- $A = QB + R$, et
- $\deg R < \deg B$

Attention

Dans la cas d'un endomorphisme, la division euclidienne à gauche n'existe pas en général (sauf si θ est bijectif)

Conséquences

L'anneau $K[X, \bullet]$ est principal à gauche
En particulier, il existe de PGCD à droite et des PPCM à gauche

Modules à gauche sur $\mathfrak{A}[X, \bullet]$

un module à gauche sur $\mathfrak{A}[X, \theta]$

= un $\mathfrak{A}$-module $\mathcal{M}$ muni de $f : \mathcal{M} \to \mathcal{M}$ *semi-linéaire*
i.e. $f(ax) = \theta(a) \cdot f(x)$

un module à gauche sur $\mathfrak{A}[X, \partial]$

= un $\mathfrak{A}$-module $\mathcal{M}$ muni d'une dérivation $d : \mathcal{M} \to \mathcal{M}$
i.e. $d(ax) = a \cdot d(x) + \partial(a) \cdot x$

Exemple typique : $\mathcal{M}_P = \mathfrak{A}[X, \bullet] \,/\, \mathfrak{A}[X, \bullet]\, P$

Décomposition des modules et factorisation

- **Trigonalisation :** si $P = BA$, alors :

$$\mathcal{M}_P\, A \subset \mathcal{M}_P \quad \text{et} \quad \mathcal{M}_P \,/\, \mathcal{M}_P\, A \simeq \mathcal{M}_B$$

- **Diagonalisation :** si $\mathfrak{A}$ est un corps et si $P = BA = A'B'$ avec $\deg A = \deg A'$ et $\mathrm{PGCD}(A, B') = 1$, alors :

$$\mathcal{M}_P = \mathcal{M}_P\, A \oplus \mathcal{M}_P\, B' \simeq \mathcal{M}_B \oplus \mathcal{M}_A$$

Corps ultramétriques

Valeurs absolues

Soit K un corps

Une valeur absolue sur K est une fonction $|\cdot| : K \to \mathbb{R}^+$ t.q. :

- $|x| = 0$ si, et seulement si $x = 0$
- $|xy| = |x| \cdot |y|$
- $|x + y| \leq |x| + |y|$

Une valeur absolue définit une distance d sur K

On dit qu'elle est complète si (K, d) est complet :
toute suite de Cauchy pour la distance d converge

Exemples

- $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ avec les valeurs absolues usuelles
- $\mathbb{Q}$ muni de la valeur absolue p-adique : $|x| = p^{-v_p(x)}$

  où $v_p(n)$ est le plus grand s tel que p^s divise n

  et $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$

Valeurs absolues ultramétriques

Une valeur absolue sur K est dite ultramétrique lorsque l'inégalité triangulaire est renformée comme suit :

- $|x+y| \leq \max\left(|x|, |y|\right)$

Exemples

- $\mathbb{Q}$ muni de la valeur absolue p-adique
- $k(x)$ muni de $|f(x)| = e^{-\mathrm{ord}_0(f(x))}$
  où ord_0 désigne l'ordre d'annulation en 0

Dans les deux exemples ci-dessus, les corps ne sont pas complets pour la valeur absolue indiquée.

Exemples de corps ultramétriques complets

- $\mathbb{Q}_p$: le corps des nombres p-adiques
- $k((x))$: le corps des séries de Laurent à coeff. dans k
- toute extension finie d'un corps ultramétrique complet

Le contexte de l'exposé

Notations et hypothèses

K — un corps **complet** pour une valeur absolue **ultramétrique**

$\theta : K \to K$ — un morphisme d'anneaux **continu**

$\partial : K \to K$ — une dérivation **lipschitzienne**

Cas particuliers notables

- $K = \mathbb{Q}_p$, $\quad \theta = \mathrm{id}$
- $K/\mathbb{Q}_p$ finie, $\quad \theta \in \mathrm{Gal}(K/\mathbb{Q}_p)$
- $K = k((u))$, $\quad \theta : u \mapsto u^b \quad (b \in \mathbb{N}^\star)$
- $K = \mathcal{M}(\mathbb{Z}_p)$, $\quad \partial = \frac{d}{dx}$

Objectif de l'exposé

Étudier des propriétés de factorisation dans $K[X, \bullet]$

Étendre et rendre effectif le théorème de factorisation par les pentes

Le contexte de l'exposé

Notations et hypothèses

K — un corps **complet** pour une valeur absolue **ultramétrique**

$\theta : K \to K$ — un morphisme d'anneaux **continu**

$\partial : K \to K$ — une dérivation **lipschitzienne**

Deux paramètres importants

b — l'unique nombre réel strictement positif tel que

$$(\forall x \in K) \qquad |\theta(x)| = |x|^b$$

Exemple : $b = 1$ si $K/\mathbb{Q}_p$ est une extension finie

$b = b$ si $\theta : u \to u^b$ sur $k((u))$

ρ — une constante de Lipschitz pour ∂ :

$$(\forall x \in K) \qquad |\partial(x)| \leq \rho \cdot |x|$$

Exemple : $\rho = 1$ si $\partial = \frac{d}{dx}$ sur $\mathcal{M}(\mathbb{Z}_p)$

Polygones de Newton

Définition

Soit $P = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \in K[X, \bullet]$

Le cas d'un endomorphisme

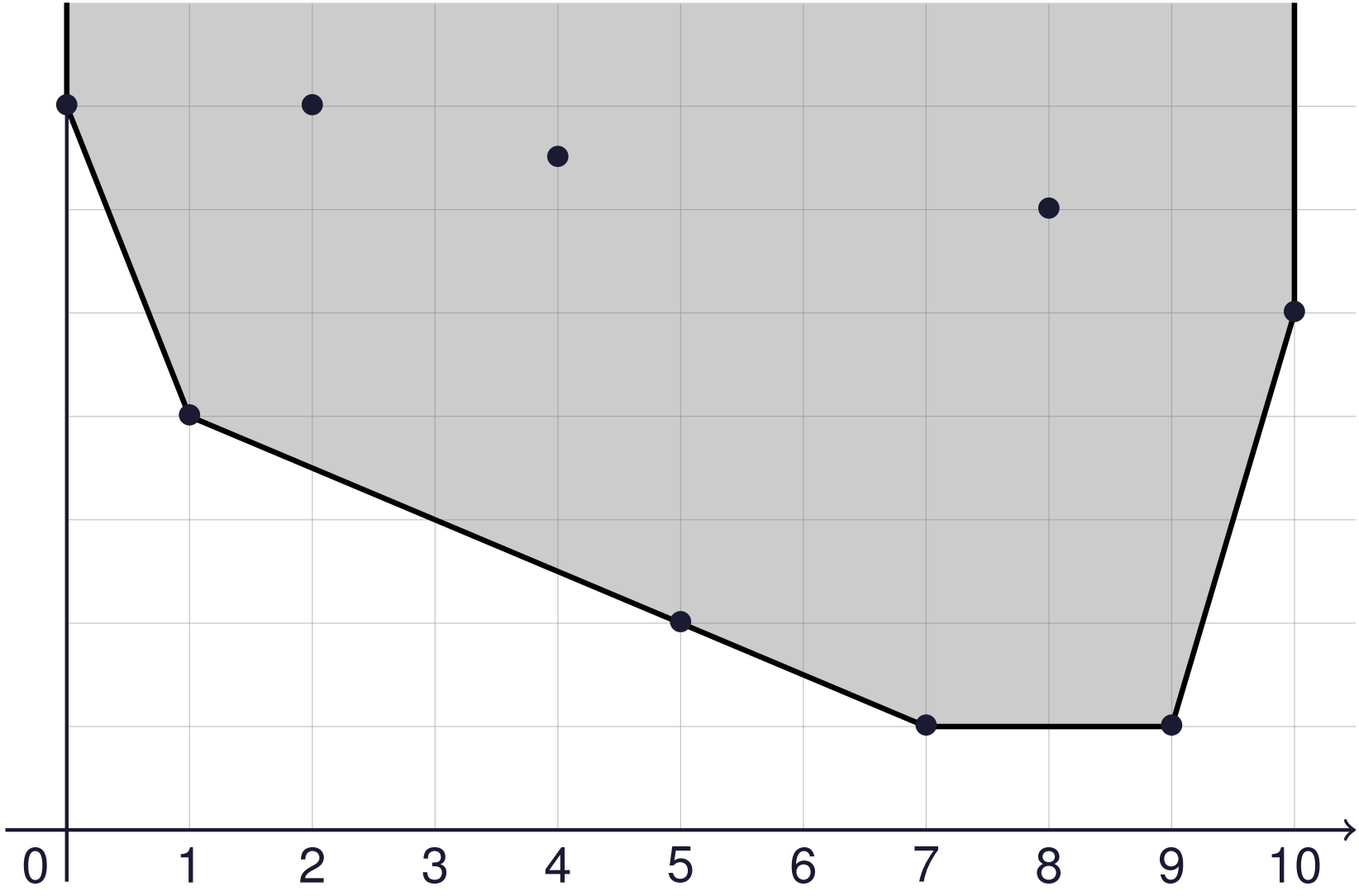
Le polygone de Newton NP_P de P est l'enveloppe convexe dans le plan des points

$$\infty \cdot (0, 1) \quad \text{et} \quad \big([i]_b, -\log |a_i| \big) \quad (0 \leq i \leq d)$$

où $[i]_b = 1 + b + \cdots + b^{i-1}$ est le b-analogue de i.

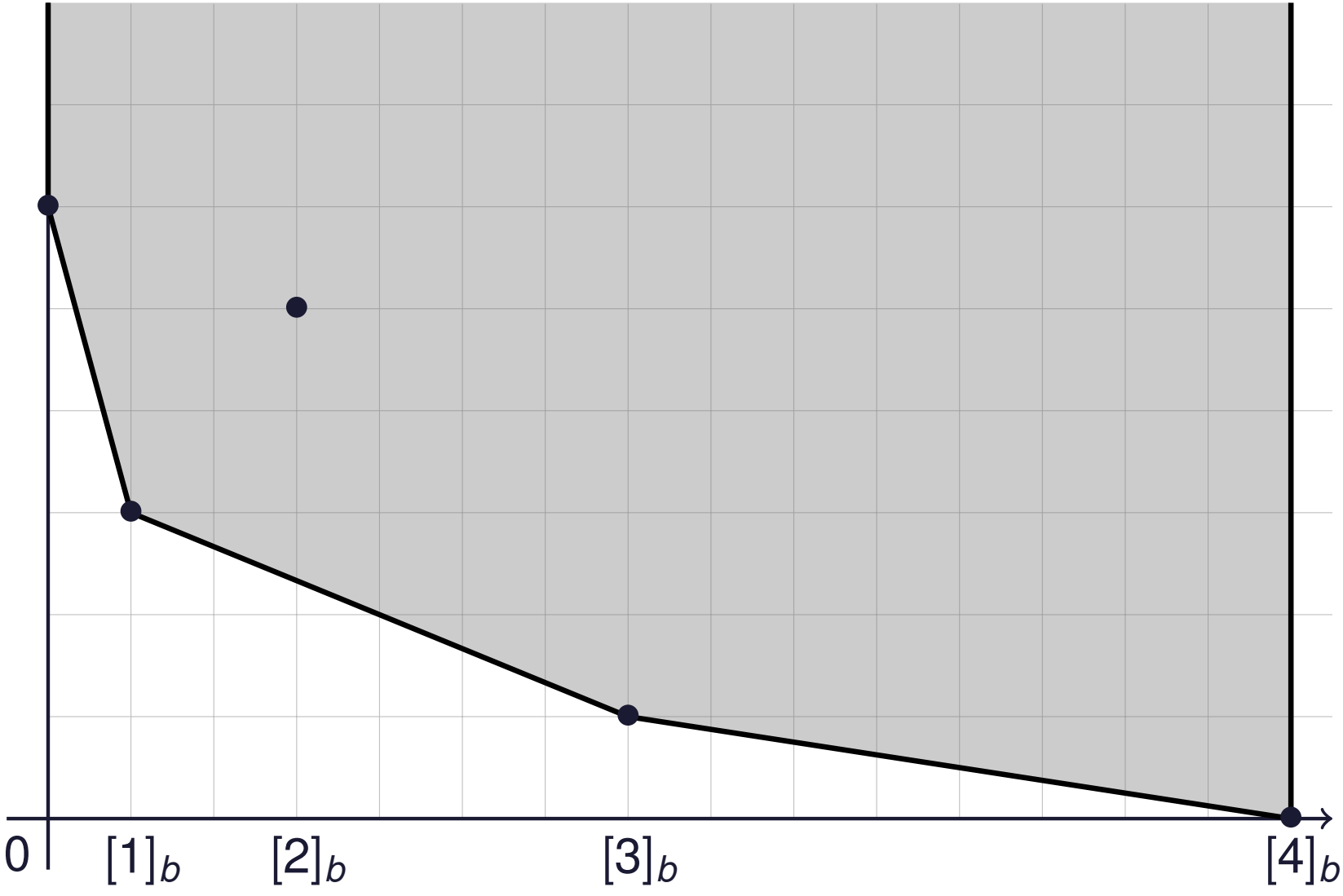
Exemples

Cas d'un endomorphisme — $b = 1$



Exemples

Cas d'un endomorphisme — $b = 2$



Définition

Soit $P = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \in K[X, \bullet]$

Le cas d'un endomorphisme

Le polygone de Newton NP_P de P est l'enveloppe convexe dans le plan des points

$$\infty \cdot (0, 1) \quad \text{et} \quad \big([i]_b, -\log |a_i| \big) \quad (0 \leq i \leq d)$$

où $[i]_b = 1 + b + \cdots + b^{i-1}$ est le b-analogue de i.

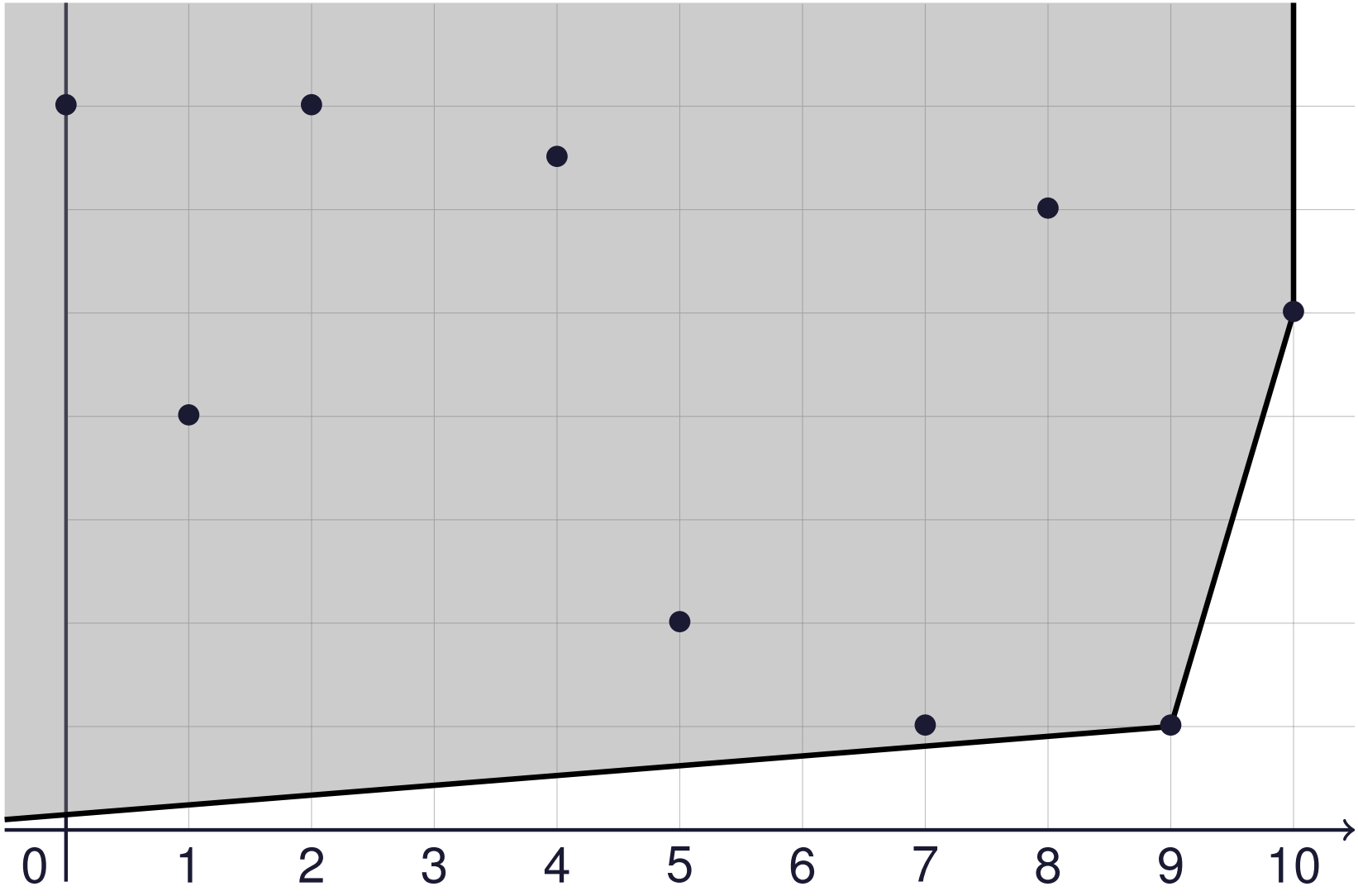
Le cas d'une dérivation

Le polygone de Newton NP_P de P est l'enveloppe convexe dans le plan des points

$$-\infty \cdot (1, \log \rho), \quad \infty \cdot (0, 1)$$
$$\text{et} \quad \big(i, -\log |a_i|\big) \quad (0 \leq i \leq d)$$

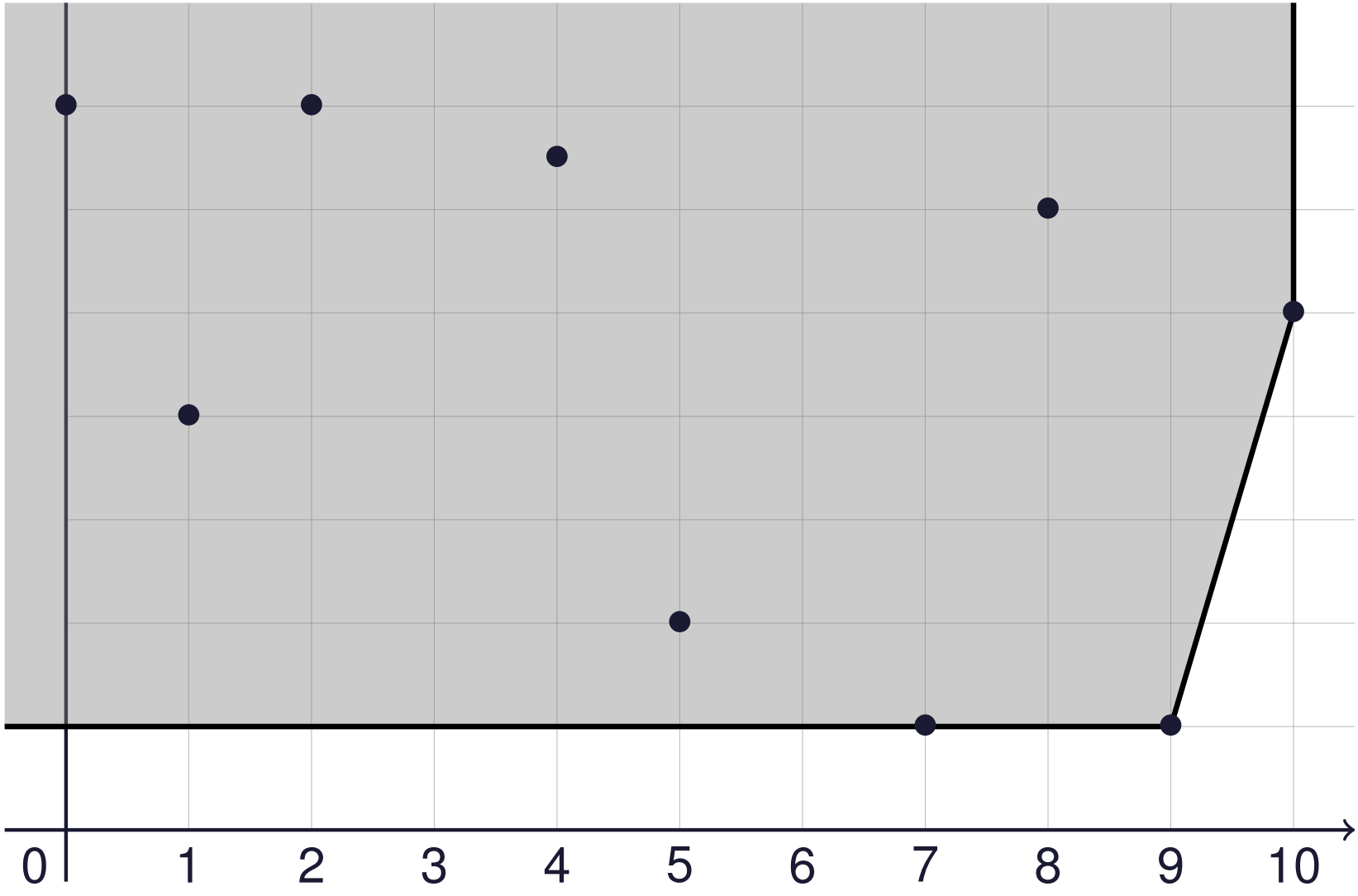
Exemples

Cas d'une dérivation — $\rho > 1$



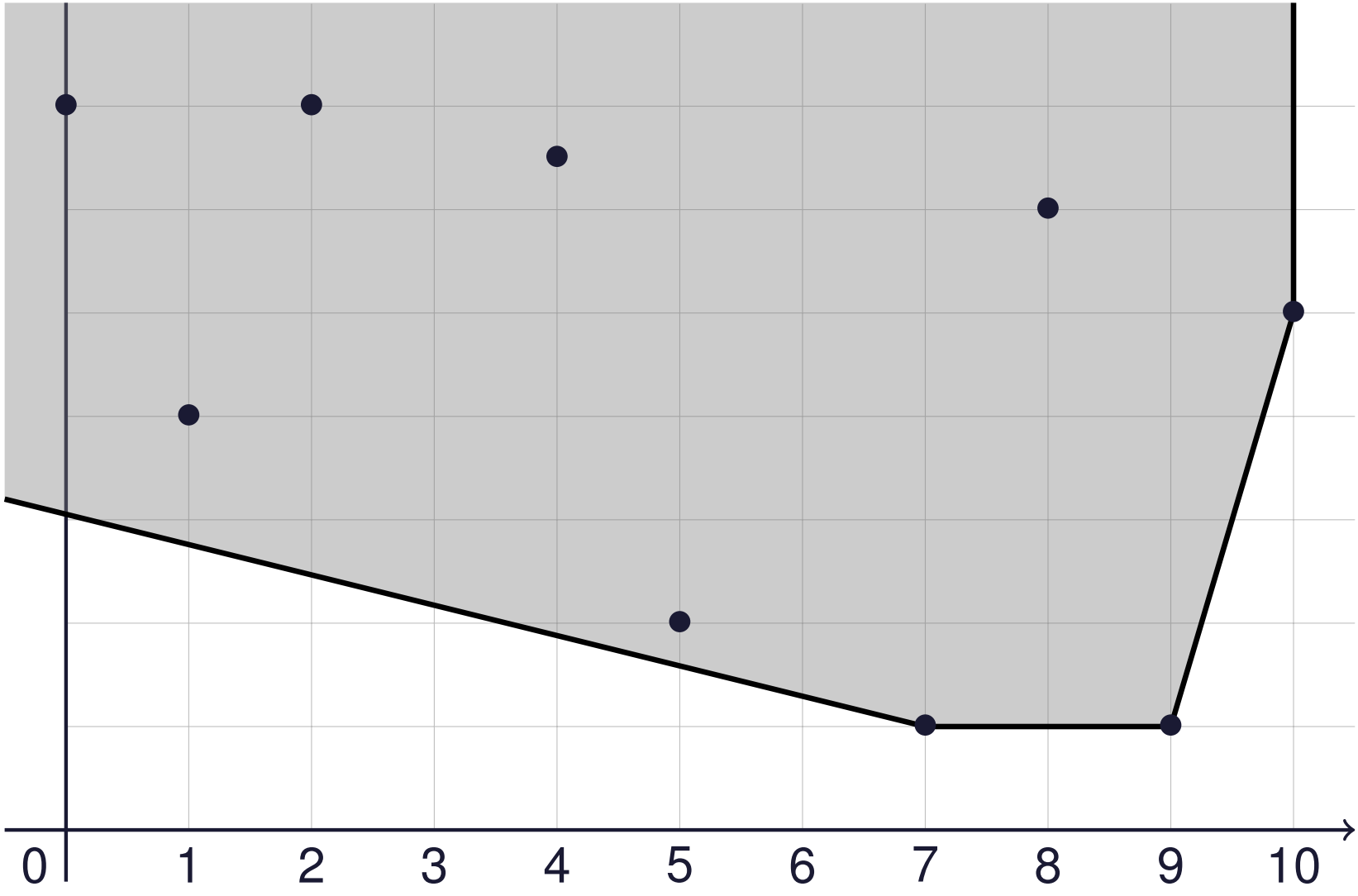
Exemples

Cas d'une dérivation — $\rho = 1$



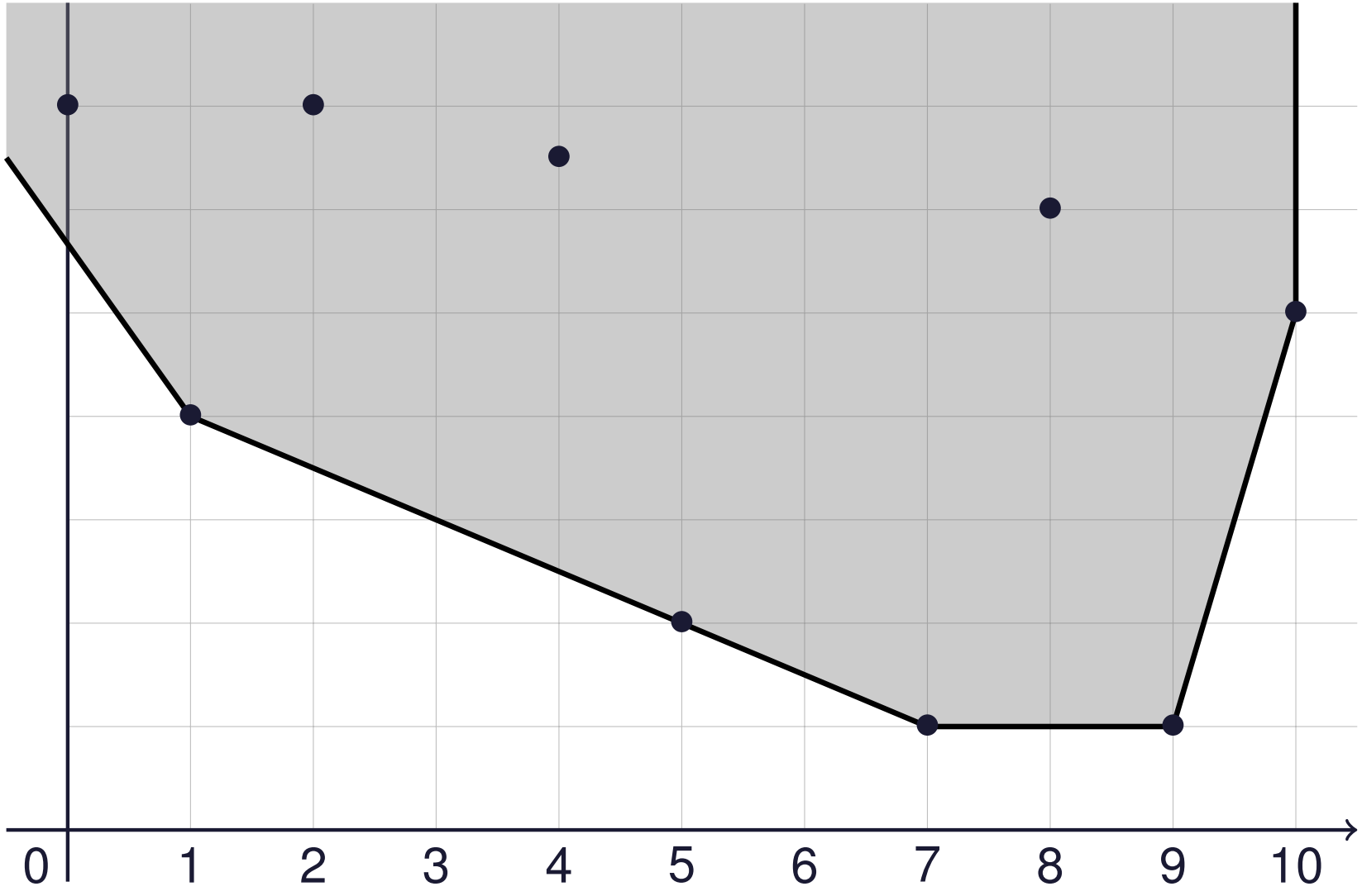
Exemples

Cas d'une dérivation — $\rho < 1$



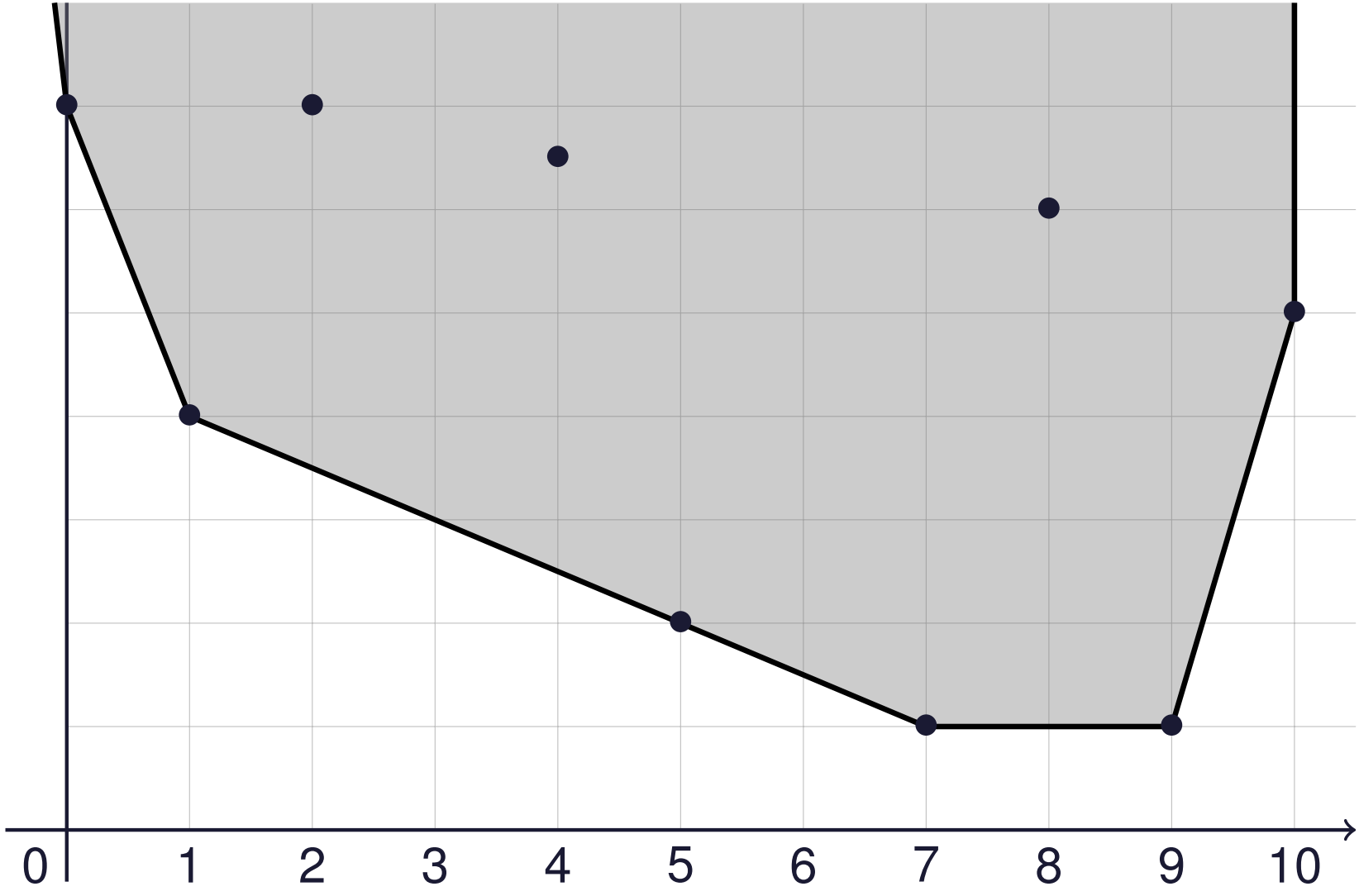
Exemples

Cas d'une dérivation — $\rho < 1$

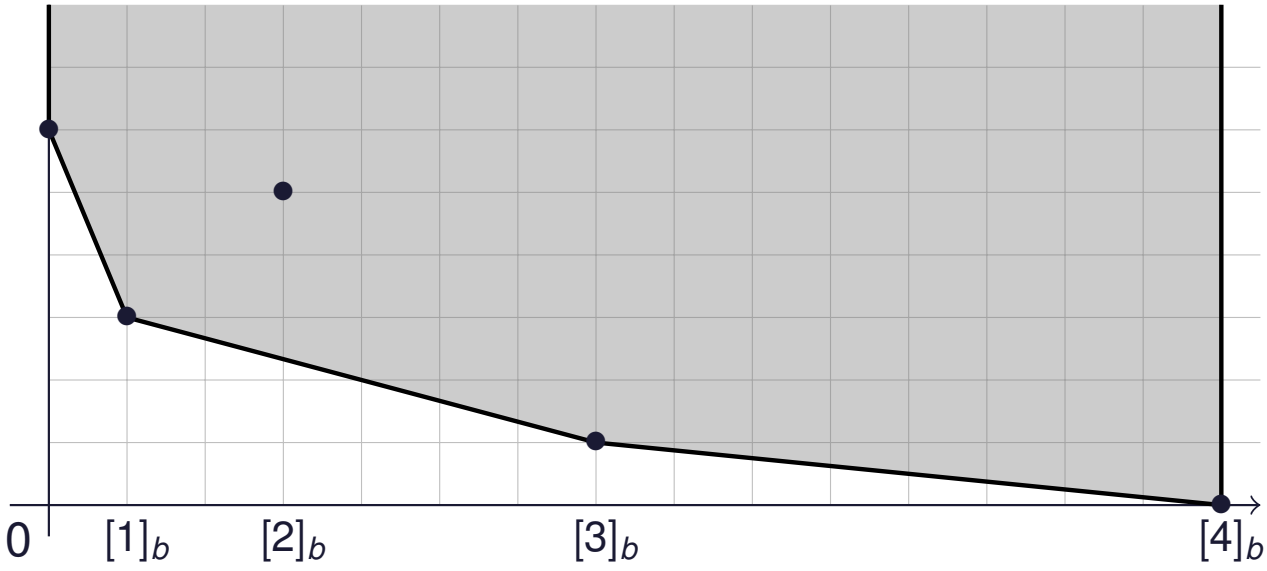


Exemples

Cas d'une dérivation — $\rho \ll 1$



Pentes des polygones de Newton



Les pentes de NP_P sont

- dans le cas d'un endomorphisme :

$$\mu_i = \frac{\mathrm{NP}_P([i]_b) - \mathrm{NP}_P([i-1]_b)}{[i]_b - [i-1]_b} \qquad (1 \leq i \leq d)$$

- dans le cas d'une dérivation :

$$\mu_i = \mathrm{NP}_P(i) - \mathrm{NP}_P(i-1) \qquad (1 \leq i \leq d)$$

Propriétés de multiplicativité

Fonctions de Herbrand

$$\begin{aligned} \mathrm{NP}^\star_P &= \text{transformée de Legendre de } \mathrm{NP}_P \\ \varphi_P &= \mathrm{id} + (b-1)\cdot \mathrm{NP}^\star_P \\ \psi_P &= (\varphi_P)^{-1} \end{aligned}$$

Note : $\varphi_P = \psi_P = \mathrm{id}$ dans le cas différentiel ou lorsque $b = 1$

Pentes d'un produit

Les pentes d'un produit $B \cdot A$ sont :

$$\psi_A(\text{pentes de } B) \quad \bigcup \quad \text{pentes de } A$$

En fait, la « vraie » formule est

$$\varphi_{BA} = \varphi_B \circ \varphi_A$$

$$\mathrm{NP}^\star_{BA} = \mathrm{NP}^\star_B + \mathrm{NP}^\star_A \quad \text{si } b = 1$$

Factorisation
par les pentes

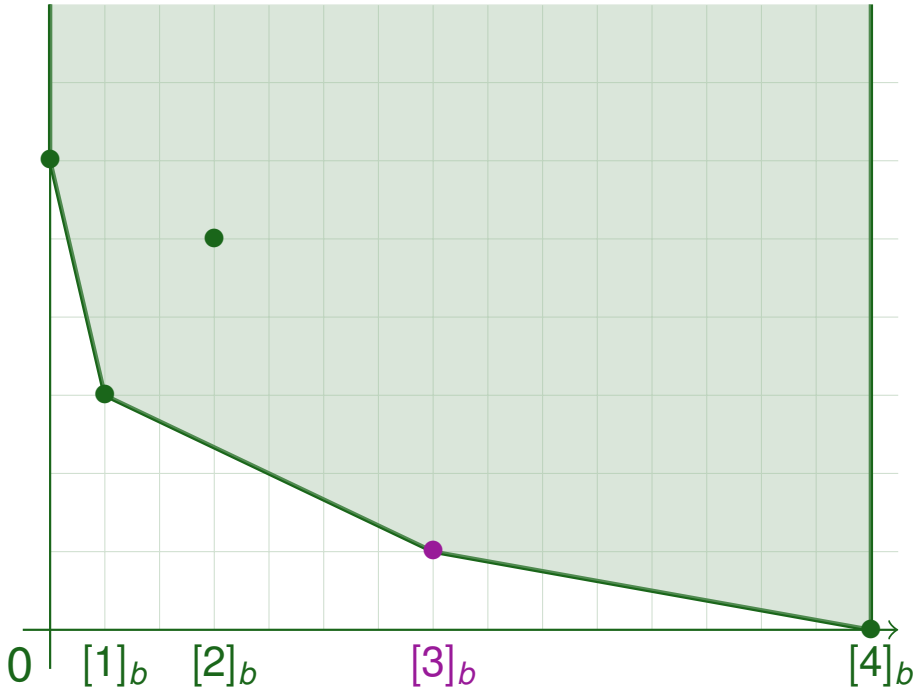
Le théorème de factorisation

Soit $P \in K[X, \bullet]$

Soit d un entier tel que NP_P ait un *point extrémal* à l'abscisse $[d]_b$

On définit la suite $(A_i)_{i \geq 0}$ par récurrence :

$$A_0 = P[:d]$$
$$A_{i+1} = A_i + (P \,\%\, A_i)$$



Alors $(A_i)_{i \geq 0}$ converge vers $A \in K[X, \bullet]$ vérifiant :

- **Divisibilité :** A est un diviseur à droite de P
  (*i.e.* il existe $B \in K[X, \bullet]$ tel que $P = BA$)
- **Polygone de Newton :** $\mathrm{NP}_A = \mathrm{NP}_P \cap \left([0, [d]_b] \times \mathbb{R}\right)$

Accélération de la convergence

La convergence de la suite (A_i) est linéaire

On gagne un nombre constant de chiffres à chaque itération

Cas commutatif

On peut utiliser un schéma de type Newton :

Initialisation : $A_0 = P[:d], \quad V_0 = 1$

Récurrence :
$$A_{i+1} = A_i + \left(V_i P \;\%\; A_i\right)$$
$$V_{i+1} = \left[2V_i - V_i^2 \cdot (P /\!\!/ A_{i+1})\right] \;\%\; A_{i+1}$$

La convergence est alors quadratique

Le nombre de chiffres corrects est doublé à chaque itération

Cas général

Peut-on adapter le schéma ci-dessus ?

Applications

Deux situations classiques

Le cas commutatif

Le théorème de factorisation était alors déjà bien connu...

mais l'algorithme (rapide), lui, semble nouveau !

Le cas d'une extension de $\mathbb{Q}_p$

$$K = \mathbb{Q}_{p^n} = \mathbb{Q}_p[T]/F(T)$$
avec $F(T)$ de degré n et irréductible mod p

$$\theta = \text{Frobenius}, \quad \textit{i.e.}\ \theta(T) \equiv T^p \pmod{p}$$

Dans ce cas : théorème de factorisation
$\simeq$ théorème de Dieudonné–Manin

Mais, à nouveau, l'algorithme est nouveau !

De plus, notre théorème s'étend *verbatim* à une extension finie $K/\mathbb{Q}_p$ *quelconque* et à $\theta \in \mathrm{Gal}(K/\mathbb{Q}_p)$ *quelconque*

Représentations galoisiennes

On étudie les $\mathbb{F}_q$-représentations de $G = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$,
i.e. les morphismes :

$$G \to \mathrm{GL}_d(\mathbb{F}_q)$$

À une telle représentation, on sait associer :

$$P \in \mathbb{F}_p((u))\left[X, \theta : u \mapsto u^q\right]$$

C'est (le début de) la théorie des (φ, Γ)-modules

Notre théorème peut ainsi être utilisé pour décomposer certaines représentations galoisiennes

De tels résultats apparaissent déjà dans la thèse de Le Borgne
mais notre approche les englobe dans un cadre plus large
et se prête peut-être davantage à généralisation

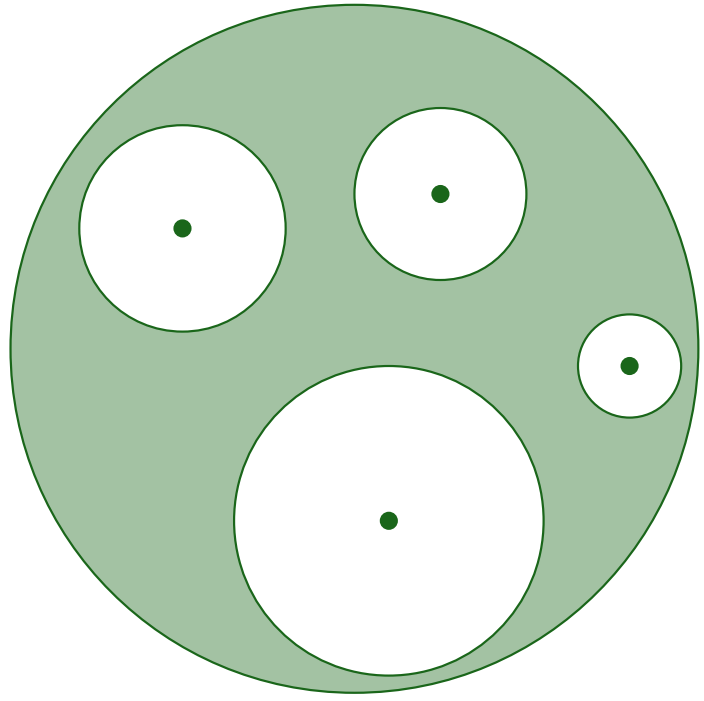
Équations différentielles p-adiques

$$\mathcal{H}(\mathbb{Z}_p) = \left\{ \sum_{i=0}^{\infty} a_i x^i, \quad \begin{array}{l} a_i \in \mathbb{Q}_p \\ a_i \to 0 \end{array} \right\}$$

muni de $|\cdot| = \sup |a_i|$

$$\mathcal{M}(\mathbb{Z}_p) = \left(\text{Frac } \mathcal{H}(\mathbb{Z}_p)\right)^{\wedge}$$

$$\partial = d/dx$$



On a alors $\rho = 1$, *i.e.* $\log \rho = 0$

Les pentes > 0 de NP_P sont liées aux
rayons de convergence des solutions de l'équa. diff. :

$$P(f) = 0 \quad \text{(où } X \text{ agit par la dérivation usuelle)}$$

Notre algorithme (+ une idée due à Pulita) permet de calculer :

- les rayons de convergence
- la filtration par ces rayons du module différentiel associé

Perspectives

Accélération de la convergence

Accélérer la convergence de la suite $(A_i)_{i \geq 0}$
au délà du cas commutatif

Cas favorable : le centre de $K[X, \bullet]$ est d'indice fini dans $K[X, \bullet]$

Précision numérique

Étudier les pertes de précision lors du calcul des A_i

Écrire une version stable de l'algorithme si nécessaire

Globalisation

Étendre le résultat à des anneaux de base plus généraux

Ingrédient essentiel : les espaces de Berkovich et/ou de Huber

Merci pour vos solutions