Université Claude Bernard LYON 1
Licence - ATN

PROJET : Un critère d'irréductibité de polynômes

1 Enveloppes convexes inférieures

On considère un ensemble fini $\mathcal{E} = \{E_k = (x_k, y_k)/0 \leq k \leq n\}$ de points du plan. On suppose que les *abcisses* des points de $\mathcal{E}$ sont *deux à deux distinctes* (pour une abscisse donnée, on ne garde dans $\mathcal{E}$ que le point d'ordonnée minimale) et que $\mathcal{E}$ est *ordonné selon les abscisses croissantes.* Pour tout $M \in \mathbb{R}$ on pose :

$$w_M = \min(\{y_k - Mx_k/0 \leq k \leq n\})$$

et on désigne par Δ_M la droite d'équation :

$$Y = MX + w_M$$

On a $\mathcal{E} \cap \Delta_M \neq \emptyset$ et tous les points de $\mathcal{E}$ sont situés *au dessus* de la doite Δ_M.
On désigne par i_M^- (*resp.* i_M^+) le plus petit (*resp.* le plus grand) indice k ($0 \leq k \leq n$) pour lequel $E_k \in \Delta_M$.

Lemme 1 *Soient $M, M' \in \mathbb{R}$:*

1. *On suppose $M' > M$; alors pour tout $x \leq x_{i_M^+}$ (resp. $x < x_{i_M^+}$) on a $Mx+w_M \geq M'x+w_{M'}$ resp. $Mx + w_M > M'x + w_{M'}$)*
2. *On suppose $M' < M$; alors pour tout $x \geq x_{i_M^-}$ (resp. $x > x_{i_M^-}$) on a $Mx+w_M \geq M'x+w_{M'}$ resp. $Mx + w_M > M'x + w_{M'}$)*

$\triangledown$ Plaçons nous dans le cas $M' > M$ et posons $j = i_M^+$ de sorte que $w_M = y_j - Mx_j$. Pour $x < x_j$ on a alors :

$$\begin{array}{rcl} Mx + w_M & = & Mx + y_j - Mx_j \\ & = & M(x - x_j) + y_j \\ & > & M'(x - x_j) + y_j \\ & = & M'x + (y_j - M'x_j) \\ & = & M'x + w_{M'} \end{array}$$

Pour $x = x_j$ on a :

$$\begin{array}{rcl} Mx_j + w_m & = & y_j \\ & = & M'x_j + (y_j - M'x_j) \\ & \geq & M'x_j + w_{M'} \end{array}$$

On procède de même dans le cas $M' < M$. $\triangle$

Lemme 2 *Pour $M < M'$ on a $i_M^+ \leq i_{M'}^-$.*

∇ On pose $j = i^+_M$. Pour tout $0 \le k < j$, on a $x_k < x_j$ de sorte que :

$$y_k \ge Mx_k + w_M > M'x_k + w_{M'}$$

de sorte que $i^-_{M'} \ge j$. $\triangle$

Lemme 3 *Pour $M' > M$ assez proche de M on a :*

$$i^+_M = i^-_{M'} = i^+_{M'}$$

∇ On pose $j = i^+_M$. Puisque j est le plus grand indice pour lequel le minimum est réalisé on a pour tout $j < k \le n$:

$$y_k - Mx_k > y_j - Mx_j$$

Comme le nombre des indices k est fini, pour M' *assez proche* de M on a encore :

$$y_k - M'x_k > y_j - M'x_j$$

ce qui montre que :

$$i^-_{M'} \le i^+_{M'} \le j = i^+_M \le i^-_{M'}$$

$\triangle$

Lemme 4 *Pour tout x, $x_0 < x < x_n$, il existe M tel que :*

$$x_{i^-_M} \le x \le x_{i^+_M}$$

∇ Pour x fixé, la fonction $\varphi : M \longrightarrow Mx + w_M$ est continue puisque c'est le minimum des fonctions continues $M \longrightarrow M(x_k - x) + y_k$ pour $0 \le k \le n$. De plus on a $\lim\limits_{M \to +\infty} \varphi(M) = -\infty$: comme $x < x_n$ on a $M(x - x_n) + y_n \to -\infty$ pour $M \to +\infty$
De même on a $\lim\limits_{M \to -\infty} \varphi(M) = -\infty$.
Soit M un point en lequel φ atteint un maximum local. Supposons que $x > x_{i^+_M}$. Pour $M' > M$ assez proche de M on aurait $x_{i^+_M} = x_{i^-_{M'}}$ et par suite $x > x_{i^-_{M'}}$. Il en résulterait que $\varphi(M) = Mx + w_M < M'x + w_{M'} = \varphi(M')$ ce qui contredirait le fait que M soit un maximum local. $\triangle$

Lemme 5 *Pour tout x, $x_0 \le x < x_n$ il existe un unique M tel que $x_{i^-_M} \le x < x_{i^+_M}$.*

∇ Les intervalles $[x_{i^-_M}, x_{i^+_M}[$ sont deux à deux disjoints d'où l'unicité.
Si $x \notin \{x_k / 0 \le k \le n\}$ (*ie.* n'est pas l'abscisse d'un point de $\mathcal{E}$) le lemme précédent montre qu'il existe M tel que $x_{i^-_M} < x < x_{i^+_M}$.
Supposons maintenant que $x = x_k$ avec $0 \le k < n$. Prenons x' tel que $x = x_k < x' < \dfrac{\delta}{2}$ où δ est la distance minimale entre les abscisses des points de $\mathcal{E}$.
Il existe alors M tel que $x_{i^-_M} < x' < x_{i^+_M}$ de sorte que l'on a $x_{i^-_M} \le x = x_k < x' < x_{i^+_M}$. $\triangle$

On définit l'*enveloppe convexe inférieure* de $\mathcal{E}$ comme l'ensemble :

$$\mathcal{C}(\mathcal{E}) = \{(x, y) / x_0 \le x \le x_n \text{ et } y \ge Mx + w_M \text{ pour tout } M \in \mathbb{R}\}$$

Proposition 1 *Soit $P = (x, y)$ un point du plan tel que $x_0 \le x \le x_n$; on a $P \in \mathcal{C}(\mathcal{E})$ si et seulement s'il existe $M \in \mathbb{R}$ tel que $x_{i^-_M} \le x \le x_{i^+_M}$ et $y \ge Mx + w_M$.*

$\triangledown$ pour $P=(x,y)\in\mathcal{C}(\mathcal{E})$ on a $x_0\leq x\leq x_n$ de sorte qu'il existe M avec $x_{i_M^-}\leq x\leq x_{i_M^+}$ et l'on a $y\geq Mx+w_M$ par défintion de $\mathcal{C}(\mathcal{E})$.
Réciproquement soit $P=(x,y)$ tel qu'il existe $M\in\mathbb{R}$ avec $x_{i_M^-}\leq x\leq x_{i_M^+}$ et $y\geq Mx+w_M$. Pour $M'\in\mathbb{R}$, si $M'>M$ comme $x\leq x_{i_M^+}$ on a $Mx+w_M\geq M'x+w_{M'}$ de sorte que $y\geq M'x+w_{M'}$. De même si $M'<M$ comme $x\geq x_{i_M^-}$ on a encore $y\geq Mx+w_M\geq M'x+w_{M'}$ et finalement $P\in\mathcal{C}(\mathcal{E})$. $\triangle$

Corollaire 1 *$\mathcal{C}(\mathcal{E})$ est le plus petit ensemble contenant $\mathcal{E}$ qui est convexe et stable par translations vers le haut (ie. pour $(x,y)\in\mathcal{C}(\mathcal{E})$ on a $(x,y')\in\mathcal{C}(\mathcal{E})$ pour tout $y'\geq y$).*

$\triangledown$ Il est clair que $\mathcal{C}(\mathcal{E})$ est convexe (car intersection de demi-espaces), contient $\mathcal{E}$ et est stable par les translations vers le haut.
Réciproquement si $\mathcal{C}'$ vérifie ces propiétés, pour tout M, il contient les points $E_{i_M^-}$ et $E_{i_M^+}$, donc le segment $[E_{i_M^-},E_{i_M^+}]$ et la bande verticale située au dessus. Finalement on a $\mathcal{C}(\mathcal{E})\subset\mathcal{C}'$. $\triangle$

Ainsi il existe un nombre fini de réels M tels que le segment $[E_{i_M^-},E_{i_M^+}]$ ne soit pas réduit à un point. On a $M_1<M_2<\cdots<M_r$ et $x_0=x_{i_{M_1}^-}<x_{i_{M_1}^+}=x_{i_{M_2}^-}<\cdots<x_{i_{M_r}^+}=x_n$.
On pose $P_0=E_{i_{M_1}^-}$, $P_i=E_{i_{M_i}^+}=E_{i_{M_{i+1}}^-}$ pour $1\leq r-1$ et $P_r=E_{i_{M_r}^+}$. La ligne polygonale $\mathcal{N}$ de sommets $P_0,\cdots,P_r$ est le *polygone de Newton* de $\mathcal{E}$. Les sommets P_i de $\mathcal{N}$ se calculent alors au moyen de l'algorithme (rudimentaire) suivant :

Algorithme 1 (ConvexeInf)

1. *entrée : la liste L des points du nuage*
2. *construire la liste LO obtenue en ordonnant par abscisses croissantes les points de L et, dans le cas d'abcisses égales, en ne conservant que le point d'ordonné minimale*
3. *soit n le nombre d'éléments de $L0$*
4. *initialiser PN en prenant la liste contenant le premier point de LO.*
5. *boucle "parcours" : pour i variant de 2 à n*
   {
   (a) *prendre P_{scr} le dernier point de la liste PN*
   (b) *prendre P_{but} le $i^{\text{ème}}$ point de la liste LO*
   (c) *former l'équation $Y=aX+b$ de la droite D_i passant par les points P_{scr} et P_{but}*
   (d) *boucle "cherche" : pour j de $i+1$ à n*
       {
       si le point LO_j est au dessous de la droite D_i alors sortir de la boucle "cherche"
       } fin boucle "cherche"

   (e) *si $j=n+1$ alors* rajouter P_{but} à la fin de la liste PN

   } fin boucle "parcours"

6. *sortie : la liste PN des sommets de l'enveloppe convexe inférieure de L*

Remarque : les conditions (d) et (e) signifie que s'il n'existe aucun point LO_j, $i+1\leq j\leq n$ en dessous ou sur la droite D_i alors on rajoute P_{but} à la fin de la liste PN.

2 Le critère de Dumas

Soit K un corps (commutatif) ; une valuation est une application :

$$v : K \longrightarrow \mathbb{R} \cup \{+\infty\}$$

vérifiant les propriétés suivantes :

1. $v(0) = +\infty$ et $v(K^\star) \subset \mathbb{R}$
2. $v : K^\star \longrightarrow \mathbb{R}$ est un homomorphisme de groupes
3. $v(x+y) \geq \min(v(x), v(y))$ pour tout $x, y \in K^\star$ tels que $x + y \neq 0$.

Lemme 6 *Si $v(x) \neq v(y)$ on a $v(x+y) = \min(v(x), v(y))$*

∇ Supposons par exemple que $v(x) < v(y)$. On a évidemment $v(x+y) \geq v(x)$. Mais $x = (x+y)-y$ de sorte que $v(x) \geq \min(v(x+y), v(y))$. On a donc $v(x) \geq v(x+y)$. $\triangle$

Prenons $K = \mathbb{Q}$ et p un entier premier. Pour $x \in \mathbb{Z}$, $x \neq 0$ on désigne par $v_p(x) \geq 0$ le plus grand entier tel que $p^{v_p(x)}$ divise x. Pour $\frac{x}{y} \in \mathbb{Q}\star$ on pose $v_p(\frac{x}{y}) = v_p(x) - v_p(y)$. On définit ainsi la valuation *p-adique* sur $\mathbb{Q}$.

On considère une valuation $v = v_p$ la valuation p-adique sur le corps $K = \mathbb{Q}$ Pour tout polynôme $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ on considère l'ensemble :

$$\mathcal{E}(f) = \{(i, v(a_i))/0 \leq i \leq n \text{ et } a_i \neq 0\}$$

et son enveloppe convexe inférieure $\mathcal{C}(f)$. Pour tout $M \in \mathbb{R}$ on pose

$$v_M(f) = \min(\{v(a_i) - Mi/0 \leq i \leq n\})$$

On désigne par $i_M^+(f)$ (*resp.* $i_M^-(f)$) le plus grand (*resp.* le plus petit) indice pour lequel ce minimum est atteint.
Si $l_M(f) = i_M^+(f) - i_M^-(f) > 0$, M est l'une des *pentes* du polygone de Newton de f et on dit $l_M(f)$ est sa *largeur*. Notons que l'on a $M \in \mathbb{Q}$.
On désignera par $\mathcal{M}(f) \subset \mathbb{Q}$ l'ensemble des pentes du polygone de Newton de f ; on a

$$\sum_{M \in \mathcal{M}(f)} l_M(f) = \deg(f) - \operatorname{ord}(f)$$

Proposition 2 *v_M est une valuation et l'on a pour tout polynôme $f \in K[X]$:*

$$\begin{aligned} i_M^+(fg) &= i_M^+(f) + i_M^+(g) \\ i_M^-(fg) &= i_M^-(f) + i_M^-(g) \end{aligned}$$

En particulier on a :

$$l_M(fg) = l_M(f) + l_M(g)$$

et

$$\mathcal{M}(fg) = \mathcal{M}(f) \cup \mathcal{M}(g)$$

∇ Les relations $v_M(f) = 0$ si et seulement si $f = 0$ et $v_M(f+g) \geq \min(v_M(f), v_M(g))$ sont immédiates. C'est la relation $v_M(f+g) = v_M(f) + v_M(g)$ qu'il s'agit d'établir.
Posons $f = \sum_{i=0}^{m} a_i X^i$, $g = \sum_{j=0}^{n} b_j X^j$ et $fg = \sum_{k=0}^{m+n} c_k X^k$ où $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.
On a alors :

$$v(c_k) \geq \min_{0 \leq i \leq k} (v(a_i) + v(b_{k-i})$$

de sorte que :

$$v(c_k) - Mk \geq \min_{0 \leq i \leq k} ((v(a_i) - Mi) + (v(b_{k-i} - M(k-i))$$

d'où

$$v(c_k) - Mk \geq v_M(f) + v_M(g)$$

pour $0 \leq k \leq m+n$ et finalement :

$$v_M(fg) \geq v_M(f) + v_M(g)$$

Posons $r = i_M^-(f)$ et $s = i_M^-(g)$. Il faut donc montrer les relations :

$$\begin{cases} i_M^-(fg) = r + s \\ v_M(fg) \leq v_M(f) + v_M(g) \end{cases}$$

Pour cela considérons la somme :

$$c_{r+s} = \sum_{i=0}^{k} a_i b_{r+s-i}$$

Par définition de r et s on a :

$$\begin{cases} v_M(f) = v(a_r) - Mr \\ v(a_i) - Mi > v_M(f) \text{ pour } i < r \end{cases} \qquad \begin{cases} v_M(g) = v(b_s) - Ms \\ v(b_j) - Mj > v_M(g) \text{ pour } j < s \end{cases}$$

Dans la somme c_{r+s} le terme $a_r b_s$ pour lequel $i = r$ (et $r + s - i = s$) est tel que :

$$\begin{aligned} v(a_r b_s) &= v(a_r) + v(b_s) \\ &= v_M(f) + v_M(g) + M(r+s) \end{aligned}$$

et *tous les autres termes* sont de valuation *strictement supérieure* : par exemple pour $i < r$ on a $v(a_i) > v_M(f) + Mi$ et $v(b_{r+s-i}) \geq v_M(g) + M(r+s-i)$ de sorte que $v(a_i b_{r+s-i}) > v_M(f) + v_M(g) + M(r+s)$.
Ainsi on a :

$$v(c_{r+s}) = v_M(f) + v_M(g) + M(r+s)$$

de sorte que :

$$v(c_{r+s}) - M(r+s) = v_M(f) + v_M(g)$$

et donc que :

$$v_M(fg) \leq v_M(f) + v_M(g)$$

le minimum étant atteint pour $r+s$. Si $k < r+s$ chaque terme de c_k est de valuation strictement supérieure à $v_M(f) + v_M(g) + Mk$ de sorte que $i_M^-(fg) = r + s$. $\triangle$

Pour toute pente $M \in \mathcal{M}(f)$ de largeur l_M ; on pose $h_M = Ml_M$ et $\lambda_M = \text{pgcd}(h_M, l_M)$. On a alors :

$$M = \frac{h_M}{l_M} = \frac{\lambda_M r_M}{\lambda_M s_M} = \frac{r_M}{s_M}$$

avec la fraction $\dfrac{r_M}{s_M}$ *irréductible.*

Corollaire 2 (critère de Dumas) *Soit f un polynôme de coefficient constant non nul ; les degrés possibles des facteurs de f sont de la forme :*

$$\sum_{M\in\mathcal{M}(f)} k_M s_M$$

avec $0 \leq k_M \leq \lambda_M$.
En particulier si $f \in K[X]$ est un polynôme de coefficient constant non nul (ie. tel que $f(0) \neq 0$) possédant une seule pente M vérifiant $l_M = s_M$; alors f est irréductible.

$\triangledown$ En effet si h est un facteur de f, le coefficient constant de h est non nul et l'on a $\sum\limits_{M\in\mathcal{M}(h)} l_M(h) = \deg(h)$. De plus $\mathcal{M}(h) \subset \mathcal{M}(f)$ et $l_M(h) \leq l_M(f)$.
Soit $M \in \mathcal{M}(f)$; Si $M \in \mathcal{M}(f) \setminus \mathcal{M}(h)$ on a $k_M = 0$; si $M \in \mathcal{M}(h)$, $l_M(h) \neq 0$ est un multiple (entier) de s_M (le dénominateur irréductible de M) inférieur ou égal à $l_M(f) = \lambda_M s_M$ d'où $l_M(h) = k_m s_m$ avec $1 \leq k_M \leq \lambda_M$.
Supposons en particulier $\mathcal{M}(f) = \{M\}$ et $l_M = \deg(f) = s_M$ *ie.* $\lambda_M = 1$. les degrés possibles des facteurs irréductibles de f sont de la forme $k_M s_M$ avec $0 \leq k_M \leq \lambda_M$ donc égaux à 0 ou $\deg(f)$. $\triangle$

Corollaire 3 (critère d'Eisenstein) *Soit $f \in K[X]$ un polynôme de degré n tel que $v(a_n) = 0$, $v(a_0) = 1$, $v(a_i) \geq 1$ pour $1 \leq i \leq n$, alors f est irréductible.*

$\triangledown$ Le polygone de Newton de f possède une unique pente $M = -\dfrac{1}{n}$ et on a $i_M^- = 0$ et $i_M^+ = n$ de sorte que $l_M = n = s_M$. On peut alors appliquer le critère de Dumas. $\triangle$

Exercices.

Exercice 1.

1. Tracer les points de la liste $L = [[6,4],[-3,5],[1,4],[0,1],[3,3],[4,5],[-2,2],[1,7],[-3,6]]$.
2. Ecrire une fonction `Prepare` qui étant donné une liste L, pour des points de même abscisse ne conserve que celui d'ordonnée minimale puis ordonne la liste selon les abscisses croissantes.
3. Ecrire une fonction `convexe_inf` permettant de calculer l'enveloppe convexe inférieure d'une liste de points.
   Calculer la liste PN des sommets de l'*enveloppe convexe inférieure* de L.
4. Tracer sur un même dessin *le nuage de points* L et son enveloppe convese inférieure.

Exercice 2.
On considère les polynômes $f = X^10 + 11X^9 + 55X^8 + 165X^7 + 330X^6 + 462X^5 + 462X^4 + 330X^3 + 165X^2 + 55X + 11$, $g = X^7 + 1320X^6 - 14751X^5 - 1330X^3 + 1330X^2 - 161172X^4 - 1320X - 11$ et $h = fg$.

1. Ecrire une fonction `polygone_newton` permettant de calculer un polynôme de Newton.
2. Tracer sur une même dessin les polygones de Newton de f, g et h en utilisant des couleurs différentes pour $p = 11$.

3. Ecrire une fonction `bouts_pente(` qui à une polygone de Newton L (décrit par la liste de ses sommets) et un nombre rationnel M associe la plus petite et la plus grande des abscisses i_M^- et i_M^+ des points d'intersertion $L \cap \Delta_M$.
4. Ecrire une fonction `pentes` permettant de calculer les pentes d'un polygone de Newton.
5. Ecrire une fonction `bouts` permettant de calculer pour chaque pente M les bouts (i_M^-, i_M^+)
6. Ecrire une fonction `degree_facteurs_irreduc(` qui à partir de la liste des pentes M et de la liste des couples (i_M^-, i_M^+) correspondants d'un polygone de Newton d'un polynôme renvoie les degrés possibles des facteurs irréductibles de ce polynôme.
   Tester cette fonction avec les polynômes f, g et h.

Exercice 3.
On considère le polynôme $f = 25X^8 - 3X^3 + 15X^2 + 45$.

1. Tracer le polygone de Newton de f pour $p = 5$; en déduire les degrés possibles des facteurs irréductibles de f
2. Faire de même pour $p = 3$.
3. En déduire que f est irréductible.

Exercice 4.
On considère le polynôme *exponentiel tronqué* :

$$f_n = \sum_{k=0}^{n} \frac{1}{k!} X^k$$

1. Tracer les polygones de Newton de f_n pour les diviseurs premiers p de n (fixé au préalable)
2. Etudier l'irréductibilité de f_n.
3. Peut-on énoncer et démontrer un résultat général ?