Localisation des racines

Christophe Ritzenthaler

Localiser les racines signifie trouver toutes les racines (réelles ou complexes) d'un polynôme et les isoler dans des boules ou intervalles aussi finement que possible. On souhaite faire cela pour plusieurs raisons. Cela peut servir d'étape initiale avant une méthode de Newton pour s'assurer de la converge vers une racine donnée ou pour faire de l'arithmétique d'intervalles afin d'avoir des résultats exactes même en manipulant des racines approchées. On peut aussi faire cela pour obtenir des résultats d'existence (ou d'absence) de racines à des fins théoriques.

Il existe une pléthore de résultats sur le sujet. Nous nous contenterons de donner les plus immédiats et qui permettent d'aboutir à des résultats effectifs.

1 Calcul exact des racines d'un polynôme

Commençons par les polynômes de petits degrés pour lesquels on a des solutions exactes pour les racines sous forme de radicaux. Ceci ne rentre pas stricto sensu dans le cadre de la localisation mais les méthodes sont bien utiles. Rappelons qu'il n'y a pas de formule permettant d'exprimer de manière générale les racines d'un polynôme de degré 5 ou plus. Ce résultat est obtenu par la théorie de Galois.

Remarque 1. *On peut se demander quelles sont les équations de degré* 5 *résolubles par radicaux. Toute équation irréductible de degré* 5 *peut se mettre sous la forme* $x^5+ax+b=0$. *Celle-ci admet des solutions (Carl Runge, 1885) par radicaux si et seulement si il existe des rationnels* u, v *tels que*

$$a = \frac{5u^4(4v+3)}{v^2+1},\ b = \frac{4u^5(2v+1)(4v+3)}{v^2+1}.$$

Par exemple $x^5-5x^4-10x^3-10x^2-5x-1$ *admet comme unique solution réelle* $x = 1+\sqrt[5]{2}+\sqrt[5]{4}+\sqrt[5]{8}+\sqrt[5]{16}$. *Quant à* $x^5-5x+12$ *elle admet également des solutions sous formes de radicaux mais demande* 600 *symboles pour l'écrire.*

1.1 Degré 2

Rappelons le résultat connu.

Proposition 1.1. *Soit* ax^2+bx+c *un polynôme de degré* 2. *Les racines de ce polynômes sont*

$$\frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

1.2 Degré 3

Passons au degré 3. Soit $x^3 + ax^2 + bx + c$ un polynôme unitaire de degré 3. On effectue le changement de variable $x = z - a/3$ et on obtient une équation du type

$$z^3 + pz + q = 0, \quad p = b - a^2/3,\ q = 2a^3/27 - ab/3 + c.$$

On a deux cas possibles :

— $p = 0$. Dans ce cas l'équation s'écrit $z^3 = -q$ qui admet trois solutions dans $\mathbb{C}$ qu'on calcule en écrivant $-q = \rho \exp(i\vartheta)$.

— $p \neq 0$. On pose $z = u + v$ et on obtient alors

$$u^3 + v^3 + q + (3uv + p)(u + v) = 0.$$

On s'intérèsee au système suivant :

$$\begin{cases} u^3 + v^3 + q & = 0 \\ 3uv + p & = 0. \end{cases}$$

Ce système est équivalent à

$$\begin{cases} u^6 + qu^3 - p^3/27 & = 0 \\ v & = -p/3u. \end{cases}$$

Dans la première équation, on pose $y = u^3$ et on a

$$y^2 + qy - p^3/27.$$

On calcule une solution y_0 puis on remonte à u en prenant les 3 racines, puis à (u, v) qui donne z et de là x. Remarquons que l'on peut choisir la racine y_0 que l'on veut. L'autre choix donne en fait les valeurs correspondantes pour v^3 puisque $u^3 + v^3 = -q$.

Remarque 2. *De l'identité*

$$\frac{1}{3} = \frac{1}{2^2}(1 + \frac{1}{2^2})(1 + \frac{1}{2^4})(1 + \frac{1}{2^8})(1 + \frac{1}{2^{16}}) \cdots$$

on peut déduire une méthode simple de calcul de la racine cubique en utilisant uniquement les multiplications et la racine carrée sans mémoire : on presse le bouton racine carrée 2 *fois puis le bouton multiplication puis le bouton racine carrée* 4 *fois. Puis le bouton multiplication. Puis le bouton racine carrée* 8 *fois,. . . .*

1.3 Degré 4

Terminons avec le degré 4.
On part de l'équation $x^4 + ax^3 + bx^2 + cx + d = 0$. On effectue le changement de variable $x = z - a/4$. On obtient une équation réduite de la forme :

$$z^4 + pz^2 + qz + r = 0$$

avec

$$p = b - (3/8)a^2,\ q = c - ab/2 + (1/8)a^3,\ r = d - ac/4 + (1/16)ba^2 - (3/256)a^4.$$

On a deux cas pour l'équation en z :

— $q = 0$. L'équation s'écrit $z^4 + pz^2 + r = 0$. C'est une équation bicarrée que l'on sait résoudre.
— $q \neq 0$. L'équation s'écrit $z^4 + pz^2 + qz + r = 0$. On pose alors $2P - Q^2 = p$, $-2QR = q$ et $P^2 - R^2 = r$.
On a alors $(z^2+P)^2 - (Qz+R)^2 = 0$. Si l'on arrive à determiner un triplet (P_0, Q_0, R_0) qui satisfait les conditions, alors trouver les solutions de l'équation réduite revient à résoudre :

$$z^2 + P_0 + Q_0 z + R_0 = 0, \text{ ou } z^2 + P_0 - Q_0 z - R_0 = 0.$$

Il reste donc à determiner P_0, Q_0 et R_0. C'est à dire à résoudre le système

$$\begin{cases} 2P - Q^2 & = p \\ -2QR & = q \\ P^2 - R^2 & = r. \end{cases}$$

Ce système revient à :

$$\begin{cases} Q^2 & = 2P - p \\ R^2 & = P^2 - r \\ QR & = -q/2. \end{cases}$$

Ce qui revient à résoudre l'équation suivante en P :

$$P^3 - (p/2)P^2 - rP + (pr/2 - (1/8)q^2) = 0.$$

Puis on remonte à P, Q, R puis à z et enfin à x.

Remarque 3. *Pour une explication sur ces méthodes par les fonctions élémentaires des racines, voir [AF, p.436-450] ou [Goz, p.190].*

2 Cas des polynômes à coefficients complexes

2.1 Rayon maximal

Soit $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{C}[X]$ un polynôme unitaire de racines $z_1, \ldots, z_n$. Soit $r_0 = \max_{1 \leq k \leq n} |z_k|$. On a la majoration suivante :

Proposition 2.1.

$$r_0 \quad < \quad 1 + \sup(|a_k|)$$

Démonstration. Ecrivons $Q(X) = X^n - |a_{n-1}|X^{n-1} - \ldots - -|a_0| = X^n f(X)$ où f est une fonction continue, strictement croissante et bijective de $]0, +\infty[$ dans $]-\infty, 1[$. Elle admet donc une unique racine réelle $r > 0$.
Soit Z tel que $|Z| = r_0$. Puisque $P(Z) = 0$ on a

$$r_0^n \leq |a_{n-1}|r_0^{n-1} + \ldots + |a_0|.$$

Donc $Q(r_0) \leq 0$ et $r_0 \leq r$. Maintenant, si A est tel que

$$A^n > |a_{n-1}|A^{n-1} + \ldots + |a_0|$$

alors $A > r \geq r_0$. On prend $M = \max_{1 \leq k \leq n}(|a_k|)$ et $A = 1 + M$ d'où $A^n = (A-1)(A^{n-1} + \ldots + 1) + 1 > |a_{n-1}|A^{n-1} + \ldots + |a_0|$ donc $r_0 < 1 + M$. □

On peut aussi avoir de la même façon $r_0 \leq \max(1, \sum_{i=0}^{n-1} |a_k|)$ et $r_0 \leq \max\left((n|a_k|)^{1/k}\right)$.

Remarque 4. *En considérant les polynômes $X^n P(X^{-1})$ et $a_0 \neq 0$, on obtient des minorations pour les z_i. Par exemple*

$$\inf |z_k| \geq \frac{|a_0|}{1 + max_{1 \leq k \leq n}(|a_{n-k}|)}.$$

2.2 La mesure d'un polynôme

Nous avons besoin d'introduire la mesure d'un polynôme afin d'obtenir des résultats de séparation. Remarquons que celle-ci permet aussi d'obtenir des majorations sur la taille des facteurs irréductibles d'un polynôme à coefficients entiers.

Soit $f = a_n X^n + \ldots + a_0 \in \mathbb{C}[X]$ un polynôme de degré n de racines complexes $z_1, \ldots, z_n$. On note

$$\begin{aligned} ||f||_2 &= \left(\sum_{j=0}^{n} |a_j|^2 \right)^{1/2} \\ ||f||_1 &= \sum_{j=0}^{n} |a_j| \\ ||f||_\infty &= \max(|a_0|, \ldots, |a_n|) \\ M(f) &= |a_n| \prod_{j=1}^{n} \max(1, |z_j|). \end{aligned}$$

Lemme 2.1.

$$||f||_\infty \leq ||f||_2 \leq ||f||_1 \leq (n+1)||f||_\infty, \quad 2^{-n}||f||_1 \leq M(f) \leq ||f||_2.$$

Démonstration. Les trois premières inégalités sont triviales. Pour l'avant-dernière, on a la relation coefficients-racines

$$a_k = (-1)^{n-k} a_n \sum z_{i_1} \cdots z_{i_k}$$

d'où

$$|a_k| \leq |a_n| \sum |z_{i_1} \cdots z_{i_k}|$$

et

$$||f||_1 = \sum_{k=0}^{n} |a_k| \leq |a_n| \prod_{j=1}^{n} (1 + |z_j|) \leq |a_n| \prod_{j=1}^{n} 2 \max(1, |z_j|) \leq 2^n M(f).$$

Pour la dernière, on se ramène d'abord à considérer un polynôme unitaire en divisant par le coefficient dominant puis on applique la formule de Jensen

$$\frac{1}{2\pi} \int_0^{2\pi} \log |e^{i\vartheta} - a| d\vartheta = \log \max(|a|, 1),$$

d'où

$$\log M(f) = \frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\vartheta})| d\vartheta \tag{1}$$

Compte tenu de la concavité du logarithme

$$\log M(f) \leq \frac{1}{2}\log\left(\frac{1}{2\pi}\int_0^{2\pi}|f(e^{i\vartheta})|^2 d\vartheta\right) = \frac{1}{2}\log\left(\sum_{j=1}^{n}|a_j|^2\right)$$

(égalité de Parseval), d'où finalement $M(f) \leq ||f||_2$ (inégalité de Landau). □

Si les normes habituelles sont plus aisées à utiliser, $M(f)$ a l'avantage d'être multiplicative (claire sur la formule (1)). Compte tenu de l'inégalité de Landau, il vient

$$\begin{aligned} ||f||_\infty||g||_\infty &\leq ||f||_1||g||_1 \\ &\leq 2^m M(f)2^n M(g) \leq 2^{m+n}M(fg) \\ &\leq 2^{m+n}||fg||_2 \\ &\leq 2^{m+n}(m+n+1)||fg||_\infty \end{aligned}$$

Remarque 5. *Il existe une méthode pour calculer $M(P)$. Écrivons $P_m = a_n^{2^m}\prod_{j=1}^n(X - z_i^{2^m})$. On peut calculer les P_i grâce à la formule*

$$P_0 = P,\ P_{m+1}(X) = F_m(X)^2 - XG_m(X)^2$$

où on a écrit $P_m(X) = F_m(X^2) + XG_m(X^2)$. On a alors

$$2^{-n2^{-m}}||P_m||_2^{2^{-m}} \leq M(P) \leq ||P_m||_2^{2^{-m}}.$$

On a donc convergence de $||P_m||_2^{2^{-m}}$ vers $M(P)$.

2.3 Séparation

Soit P un polynôme de degré n à racines simples z_i (remarquons qu'on peut toujours se ramener à ce cas en considérant $P/\gcd(P, P')$). On pose

$$\delta = \min_{i\neq j}|z_i - z_j|.$$

Proposition 2.2. *Soit $\Delta = a_n^{2n-2}\prod_{i<j}(z_i - z_j)^2$ le discriminant de P.*

$$\delta \geq \sqrt{\frac{|\Delta|}{n^{n+2}}}||P||_2^{1-n}.$$

Démonstration. Compte tenu de l'inégalité de Landau, il suffit de montrer que

$$\delta \geq \sqrt{\frac{|\Delta|}{n^{n+2}}}M(P)^{1-n}$$

ce qui s'écrit encore

$$\delta \geq n^{-(n+2)/2}|a_n|^{n-1}|\prod_{i<j}(z_i - z_j)|M(P)^{1-n}$$

et finalement

$$|\prod_{i<j}(z_i - z_j)| \leq n^{(n+2)/2}\delta\left(\frac{M(P)}{|a_n|}\right)^{n-1}$$

On part du déterminant de Van der Monde

$$V = \prod(z_i - z_j) = \det \begin{bmatrix} 1 & \dots & 1 \\ z_1 & \dots & z_n \\ \vdots & & \vdots \\ z_1^{n-1} & \dots & z_n^{n-1} \end{bmatrix}$$

que l'on peut écrire

$$\det \begin{bmatrix} 1 & \dots & 0 & \dots & 1 \\ z_1 & \dots & z_i - z_j & \dots & z_n \\ \vdots & & & & \vdots \\ z_1^{n-1} & \dots & z_i^{n-1} - z_j^{n-1} & \dots & z_n^{n-1} \end{bmatrix}$$

On utilise alors le lemme de Hadamard : la valeur absolue du déterminant est majorée par le produit des normes euclidiennes de ses vecteurs colonnes. On obtient

$$|V| \leq \left(\sum_{h=0}^{n-1} |z_i^h - z_j^h|^2 \right)^{1/2} \left(\prod_{k \neq i} (1 + |z_k|^2 + \ldots + |z_k|^{2n-2}) \right)^{1/2}.$$

On a $|z_k| \leq \max(1, |z_k|)$ donc

$$s_k = \left(1 + |z_k|^2 + \ldots + |z_k|^{2n-2}\right)^{1/2} \leq \left(1 + \max(1, |z_k|)^2 + \ldots + \max(1, |z_k|)\right)^{2n-2})^{1/2}.$$

Mais $\max(1, |z_k|)^s \leq \max(1, |z_k|)^{2n-2}$ pour $0 \leq s \leq 2n-2$ de sorte que

$$s_k \leq n^{1/2} \max(1, |z_k|)^{n-1}$$

et donc

$$\left(\prod_{k \neq i} (1 + |z_k|^2 + \ldots + |z_k|^{2n-2}) \right)^{1/2} \leq n^{(n-1)/2} \prod_{k \neq i} \max(1, |z_k|)^{n-1} = n^{(n-1)/2} \left(\frac{M(P)}{|a_n| \max(1, |z_i|)} \right)^{n-1}.$$

On a donc

$$|V| \leq \left(\sum_{h=0}^{n-1} |z_i^h - z_j^h|^2 \right)^{1/2} \frac{1}{\max(1, |z_i|)^{n-1}} n^{(n-1)/2} \left(\frac{M(P)}{|a_n|} \right)^{n-1}.$$

Mais on a aussi

$$|z_i^h - z_j^h| \leq |z_i - z_j||z_i^{h-1} + z_j z_i^{h-2} + \ldots|$$

et si on suppose $|z_i| \geq |z_j|$ on voit que

$$|z_i^h - z_j^h| \leq |z_i - z_j| h |z_i|^{h-1} \leq |z_i - z_j| h \max(1, |z_i|)^{h-1} \leq |z_i - z_j|(n-1) \max(1, |z_i|)^{n-2}$$

d'où

$$\left(\sum_{h=0}^{n-1} |z_i^h - z_j^h|^2 \right)^{1/2} \leq |z_i - z_j|(n-1)^{3/2} \max(1, |z_i|)^{n-2} \leq |z_i - z_j| n^{3/2} \max(1, |z_i|)^{n-1}$$

et l'on obtient

$$|V| \leq |z_i - z_j| n^{(n+2)/2} \left(\frac{M(P)}{|a_n|} \right)^{n-1}.$$

□

Dans le cas où P est à coefficients entiers, on peut utiliser le fait que $|\Delta| \geq 1$ pour simplifier l'expression précédente.

Ces résultats ne permettent pas la localisation des racines. Il faut un analogue des suites de Sturm ci-dessous. Cela existe (c'est la méthode de l'indice de Cauchy) mais ne sera pas aborder ici.

Remarque 6. *Il existe des polynômes irréductibles (et donc à racines simples) à coefficients entiers et unitaires dont les racines sont arbitrairement proches. Considérons $P = X^n - 2(aX-1)^2$ pour $a \geq 10$ entier positif. Par le critère d'Eisenstein appliqué avec le premier 2, P est irréductible sur $\mathbb{Z}$. Notons que $P(a^{-1}) = a^{-n} > 0$ et si $h = a^{-(n+2)/2}$ on a*

$$P(a^{-1} \pm h) = \left(\frac{1}{a} \pm \frac{1}{aa^n}\right)^n - 2a^{-n} = \frac{1}{a^n}\left(1 \pm \frac{1}{a^n}\right)^n - \frac{2}{a^n} < 0.$$

Ainsi P a deux racines dans l'intervalle $]a^{-1}-h, a^{-1}+h[$, ce qui donne $\delta < 2h = 2a^{-(n+2)/2}$.

3 Cas des polynômes à coefficients réels

Pour les polynômes réels, on dispose d'autres méthodes pour localiser les racines.

3.1 Majorations

On commence par la règle de Newton.

Proposition 3.1. *Soit P un polynôme à coefficients réels de degré n. Soit L un réel tel que l'on ait $P^{(i)}(L) \geq 0$ pour $0 \leq i \leq n$. Alors toute racine réelle de P est majorée par L.*

Démonstration. Soit $x = L + y$ avec $y > 0$. D'après la formule de Taylor on a $P(x) = \sum y^i/i! P^{(i)}(L) > 0$ (car toutes les dérivées ne peuvent pas être nulles). □

On a également la règle de Lagrange et MacLaurin.

Proposition 3.2. *Soit P un polynôme à coefficients réels de la forme*

$$P(X) = X^n + a_1 X^{n-1} + \ldots + a_n$$

avec $a_i \geq 0$ pour $i = 1, \ldots, m-1$ et soit $A = \max(-a_m, \ldots, -a_n, 0)$. Alors toute racine réelle x de P vérifie $x < 1 + A^{1/m}$.

Démonstration. Pour $x \geq 1 + A^{1/m}$, on a $P(x) \geq x^n - A(1 + x + \ldots + x^{n-m}) > 0$. □

Par exemple si $P(X) = X^6 - 12X^4 - 2X^3 + 37X^2 + 10X - 10$ alors Newton donne $L = \sqrt{8}$ et Lagrande et MacLaurin $L = 1 + \sqrt{12}$.

3.2 Les suites de Sturm

Ceci est extrait de [Fra, p.230].

Théorème 3.1. *Soit $a < b$ deux nombres réels et $P_0, \ldots, P_s$ une suite de polynômes réels tels que*

1. *$P_0(a)P_0(b) \neq 0$;*
2. *P_s ne s'annule pas sur $[a, b]$;*

3. *si* $0 < j < s$ *et* $c \in [a,b]$ *tel que* $P_j(c) = 0$ *alors* $P_{j-1}(c)P_{j+1}(c) < 0$;

4. *si* $c \in]a,b[$ *et* $P_0(c) = 0$ *alors* $P_0(x)P_1(x)$ *est du signe de* $x - c$ *au voisinage de* c.

Pour $c \in [a,b]$, *on note* $V(c)$ *le nombre de changement de signes (sans compter le* 0*) dans la suite* $P_0(c), P_1(c), \ldots, P_s(c)$. *Le nombre de racines distinctes de* P_0 *dans* $[a,b]$ *est* $V(a) - V(b)$.

Démonstration. Soit $c \in [a,b]$ tel qu'il existe $i > 0$ et $P_i(c) = 0$. Alors d'après (2) $i < s$ et d'après (3) $P_{i-1}(x)P_{i+1}(x)$ reste strictement négatif sur un voisinage de c. On peut donc avoir globalement les cas suivants (et les situations en inversant tous les signes)

	$c-\epsilon$	c	$c+\epsilon$
P_{i-1}	$-$		$-$
P_i	$-$	0	$+$
P_{i+1}	$+$		$+$

	$c-\epsilon$	c	$c+\epsilon$
P_{i-1}	$-$		$-$
P_i	$+$	0	$+$
P_{i+1}	$+$		$+$

	$c-\epsilon$	c	$c+\epsilon$
P_{i-1}	$-$		$-$
P_i	$+$	0	$-$
P_{i+1}	$+$		$+$

,

	$c-\epsilon$	c	$c+\epsilon$
P_{i-1}	$-$		$-$
P_i	$-$	0	$-$
P_{i+1}	$+$		$+$

.

On en conclut que $V(x)$ n'est pas modifié par la traversé d'une racine de P_i pour $i > 0$.

Au contraire, soit $c \in]a,b[$ une racine de P_0. D'après (4) $P_0(x)P_1(x)$ est du signe de $x - c$ au voisinage de c. Donc pour $x = c - \epsilon$ il y a un changement de signe dans la suite entre $P_0(x)$ et $P_1(x)$ et pas pour $x = c + \epsilon$. On en conclut que $V(x)$ décroît de 1 en traversant une racine de P_0. Finalement $V(b) - V(a)$ compte bien le nombre de racines distinctes de P_0. □

Soit P un polynôme à coefficients réels tel que $P(a)P(b) \neq 0$. On peut toujours se ramener à P racines simples en considérant $P/\gcd(P, P')$. On suppose qu'on est donc dans ce cas et on va construire une suite de Sturm pour P.

On pose $P_0 = P, P_1 = P'$ et $P_{i+1} \equiv -P_{i-1} \pmod{P_i}$. Puisque au signe près il s'agit de l'algorithme d'Euclide, celui-ci s'arrête et on pose P_s le dernier résultat non nul qui est au signe près le pgcd de P et de P' et qui est donc une constante non nulle. La condition (2) est donc satisfaite. Soit maintenant $c \in [a,b]$ et $i > 0$ tel que $P_i(c) = 0$. Par construction il existe $Q \in \mathbb{R}[x]$ tel que $P_{i+1}(X) = -P_{i-1}(x) - Q_i(x)P_i(x)$. Donc pour $x = c$ on a $P_{i+1}(c) = -P_{i-1}(c)$. De plus $P_{i+1}(c) \neq 0$ car sinon c serait racine de P_s. On a donc la propriété (3). Enfin si $c \in]a,b[$ est une racine de P alors $P_1(c) = P'(c) \neq 0$ et donc

$$P(x)P_1(x) = P'(c)^2(x - c) + o(x - c)$$

est du signe de $(x - c)$ au voisinage de c.

Une fois défini un intervalle contenant les racines (grâce à une majoration sur $P(X)$ puis une autre sur $P(-X)$) on peut alors utiliser les suites de Sturm par dichotomie sur l'intervalle pour isoler les racines. Remarquons que le calcul des polynômes de la suite de Sturm n'est fait qu'une seul fois (et qu'il y en a au plus n) et qu'il suffit alors d'évaluer ces polynômes en des points avec une précision suffisantes pour déterminer leur signe.

Remarque 7. *Il existe un résultat plus faible (Budan-Fourier) qui donne la parité du nombre de racines. Ce résultat est utilisé avec la création d'une suite astucieuse de polynômes associés pour obtenir des développements en fraction continue des racines réelles. Voir le livre de Mignotte et* `https://en.wikipedia.org/wiki/Budan\%27s_theorem`.

3.3 Polynômes d'Hurwitz

La stabilité d'un système d'oscillateurs linéaires est liée à celle de son polynôme caractéristique, à coefficients réels positifs. Idem pour les filtres électriques linéaires.

Pour qu'un système soit stable, il faut que son polynôme caractéristique ait toutes ses racines à partie réelle négative. Un tel polynôme est appelé *polynôme de Hurwitz*. On a la caractérisation suivante.

Proposition 3.3. *$P(X) = a_nX^n + \ldots + a_0 \in \mathbb{R}[X]$ avec $a_0 > 0$ et $a_n \neq 0$ est un polynôme de Hurwitz si et seulement si*

$$\begin{vmatrix} a_1 & a_0 & 0 & \ldots & 0 \\ a_3 & a_2 & a_1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{2i-1} & a_{2i-2} & \ldots & a_{k+1} & a_k \end{vmatrix} > 0$$

for $i = 1, \ldots, n$ et où on a posé $a_j = 0$ si $j < 0$ ou $j > n$.

4 Polynômes sur $\mathbb{Z}$

Remarquons que si un polynôme à coefficients entiers est tel que le p.g.c.d. de ses coefficients est 1 alors il est irréductible sur $\mathbb{Z}$ si et seulement si il est irréductible sur $\mathbb{Q}$. Les deux questions sont donc liées très simplement.

Corollaire 4.1. *Soit f, g des polynômes à coefficients entiers de degré m et n tels que g divise f dans $\mathbb{Z}[X]$. On a l'inégalité $||g||_\infty \leq 2^n||f||_2$.*

Démonstration. Soit h tel que $gh = f$. On a $||g||_\infty||h||_\infty \leq 2^n||f||_2$. Comme g et h sont à coefficients entiers, $||g||_\infty$ et $||h||_\infty$ sont au moins égaux à 1. □

4.1 Irréductibilité

Théorème 4.1 ([MS, p.59])**.** *Soit $F = f^n + pg \in \mathbb{Z}[X]$ avec $p \geq 2$ premier, $n \geq 1$ et $f, g \in \mathbb{Z}[X]$ tel que $f \mod p$ est irréductible et $f \mod p$ ne divise pas $g \mod p$. Alors F est irréductible sur $\mathbb{Z}$.*

Démonstration. Supposons que $F = F_1F_2$. Puisque $F \equiv f^n \mod p$ et $f \mod p$ est irréductible, il existe $u, v \geq 1$ avec $u + v = n$ et $g_1, g_2 \in \mathbb{Z}[X]$ tels que

$$F_1 = f^u + pg_1, \quad F_2 + f^v + pg_2.$$

Supposons $u \leq v$ on a alors

$$g = f^u h + pg_1g_2$$

avec $h = g_2 + f^{v-u}g_1$. Réduisons modulo p, on obtient

$$g \equiv f^u h \mod p.$$

Contradiction puisque $f \mod p$ ne divise pas $g \mod p$. □

Corollaire 4.2 (Critère d'Eisenstein)**.** *Soit $F(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X] \setminus \mathbb{Z}$. S'il existe un premier $p \geq 2$ tel que p divise $a_0, \ldots, a_{n-1}$ et p^2 ne divise pas a_0 alors F est irréductible.*

Démonstration. On écrit $F = f^n + pg$ avec $f = X$ et $g = \frac{1}{p}(a_{n-1}X^{n-1} + \ldots + a_1X + a_0)$. On applique la proposition précédente. □

Remarque 8. *Il existe une autre version avec les mêmes hypothèses mais $a_n \neq 1$ et non divisible par p.*

Références

[AF] J.M. Arnaudiès, H. Fraysse : cours de mathématiques-1 Algèbre, Dunod Université.

[Gou] Gourdon

[Goz] I. Gozard, Théorie de Galois.

[Knu] Knuth tome 2.

[Fra] Francinou.

[MS] M. Mignotte, D. Stefanescu, *Polynomials, an algorithmic approach*, Springer.