Mathématiques assistées par ordinateur

Chapitre 4 : Racines des polynômes réels et complexes

Michael Eisermann

Mat249, DLST L2S4, Année 2008-2009
www-fourier.ujf-grenoble.fr/~eiserm/cours#mao
Document mis à jour le 6 juillet 2009

INSTITUT FOURIER
UNIVERSITE JOSEPH FOURIER
SCIENCES.TECHNOLOGIE.SANTÉ

Objectifs de ce chapitre

On sait résoudre les équations polynomiales de degré $2, 3, 4$ avec les quatre opérations $+$, $-$, $*$, $/$ et les racines $\sqrt[2]{\ }$ et $\sqrt[3]{\ }$. En degré ≥ 5 ceci n'est plus possible.

Le théorème de Gauss–d'Alembert assure au moins l'existence des racines dans le corps des nombres complexes. Ce chapitre présente des méthodes pour effectivement localiser ces racines :

- Les règles de Descartes et de Budan–Fourier.
- La méthode de Sturm pour localiser les racines réelles.
- La méthode de Cauchy pour localiser les racines complexes.

Sommaire

Équations polynomiales

On veut résoudre une équation polynomiale (réelle ou complexe)

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Degré 1 : Pour l'équation $x + a_0 = 0$ on trouve la solution $x = -a_0$.

Degré 2 : Pour $x^2 + px + q = 0$ on trouve

$$\begin{aligned}
& & x^2 + px + q &= 0 \\
&\Leftrightarrow & \left(x + \frac{p}{2}\right)^2 - \frac{p^2}{4} + q &= 0 \\
&\Leftrightarrow & \left(x + \frac{p}{2}\right)^2 &= \frac{p^2}{4} - q \\
&\Leftrightarrow & x + \frac{p}{2} &= \pm\sqrt{\frac{p^2}{4} - q} \\
&\Leftrightarrow & x &= -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}
\end{aligned}$$

⚠ Pour toujours assurer l'existence des racines il faut passer aux nombres complexes. Par exemple, pour $x^2 + 1 = 0$ on trouve $x = \pm i$.

La formule de Tartaglia–Cardano

En degré 3 on cherche à résoudre

$$x^3 + ax^2 + bx + c = 0.$$

D'abord on substitue $x = y - a/3$ pour éliminer le terme quadratique :

$$y^3 + py + q = 0.$$

Après un petit calcul on trouve $p = b - \frac{a^2}{3}$ et $q = c + \frac{2a^3 - 9ab}{27}$.

Ensuite on remplace $y = z - p/3z$ et multiplie toute l'équation par z^3 :

$$z^6 + qz^3 - \frac{p^3}{27} = 0.$$

C'est une équation quadratique en z^3 ! On en déduit que

$$z^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Ceci permet de calculer z^3 puis z, puis y, et finalement x.

⚠ Programmer cette méthode sur ordinateur est un défi non trivial : pour les diverses racines il faut choisir / déterminer les bons signes !

Existence des racines

On veut résoudre une équation polynomiale (réelle ou complexe)

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Degré 1 : on trouve $x = -a_0$.

Degré 2 : on trouve $x = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0}$.

Degré 3 : formule de Tartaglia (1530), publiée par Cardano (1545)

Degré 4 : formule de Ferrari (1540), un élève de Cardano

Théorème (Ruffini 1799, Abel 1824, Galois 1832)

En degré ≥ 5 aucune formule générale de ce type n'existe, construite à partir des opérations $+$, $-$, $*$, $/$, et des radicaux $\sqrt[k]{\ }$.

On ne dispose donc pas de formule « magique » en degré supérieur. Peut-on néanmoins être sûr que des solutions existent ? dans $\mathbb{C}$?

Théorème (de Gauss–d'Alembert)

Pour tout polynôme $F = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ dans $\mathbb{C}[X]$ il existe $r_1, r_2, \ldots, r_n \in \mathbb{C}$ tels que $F = (X - r_1)(X - r_2)\cdots(X - r_n)$.

Racines rationnelles d'un polynôme rationnel

Considérons $P = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \cdots + \frac{a_n}{b_n}X^n$ dans $\mathbb{Q}[X]$.
Quitte à multiplier par $\operatorname{ppcm}(b_0, \ldots, b_n)$ on peut supposer $P \in \mathbb{Z}[X]$.

Proposition

Considérons $P = a_0 + a_1X + \cdots + a_nX^n$ dans $\mathbb{Z}[X]$.
Si $P(\frac{p}{q}) = 0$ où $\operatorname{pgcd}(p, q) = 1$, alors $p \mid a_0$ et $q \mid a_n$.
Si $a_0 \neq 0$ et $a_n \neq 0$, il n'existe qu'un nombre fini de candidats $\frac{p}{q}$.

Démonstration. Nous avons

$$q^n P(\tfrac{p}{q}) = a_0q^n + a_1q^{n-1}p^1 + \cdots + a_{n-1}q^1p^{n-1} + a_np^n.$$

Si $P(\frac{p}{q}) = 0$, alors $p \mid a_0q^n$ et $q \mid a_np^n$.
Puisque $\operatorname{pgcd}(p, q) = 1$, on a $p \mid a_0$ et $q \mid a_n$. $\square$

Corollaire

En testant tous les candidats, ceci permet de trouver toutes les racines rationnelles d'un polynôme rationnel donné. $\square$

Exercice

Déterminer les entiers $n \in \mathbb{Z}$ et $a \in \mathbb{Z}$ pour lesquels $\sqrt[n]{a}$ est rationnel.

Localisation grossière : la borne de Cauchy

Définition (borne de Cauchy)

Soit $F = X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0$ dans $\mathbb{C}[X]$.
On pose $M := \max\{\,|c_0|, \ldots, |c_{n-1}|\,\}$ et $\rho_F := 1 + M$.

Théorème (localisation grossière des racines)

Pour tout $z \in \mathbb{C}$ tel que $|z| \geq \rho_F$ on a $|F(z)| \geq 1$. Par conséquent, toute racine complexe de F est dans $B(\rho_F) = \{\, z \in \mathbb{C} \mid |z| < \rho_F \,\}$.

Démonstration. L'énoncé est vrai pour $F = X^n$: ici $M = 0$ et $\rho_F = 1$. Supposons donc $M > 0$ et $\rho_F > 1$. Pour $|z| \geq \rho_F$ on trouve

$$\begin{aligned} |F(z) - z^n| &= |c_0 + \cdots + c_{n-1}z^{n-1}| \leq |c_0| + \cdots + |c_{n-1}||z^{n-1}| \\ &\leq M + M|z| + \cdots + M|z|^{n-1} = M\tfrac{|z|^n - 1}{|z| - 1} \leq |z|^n - 1. \end{aligned}$$

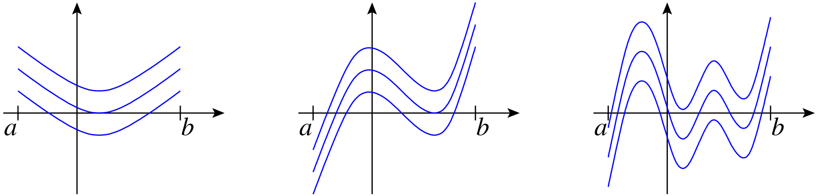
Ainsi nous obtenons

$$|z^n| = |z^n - F(z) + F(z)| \leq |z^n - F(z)| + |F(z)|, \quad \text{d'où}$$
$$|F(z)| \geq |z^n| - |F(z) - z^n| \geq |z|^n - (|z|^n - 1) = 1.$$

Ceci prouve que $|z| \geq \rho_F$ implique $|F(z)| \geq 1$. $\square$

Racines réelles d'un polynôme réel

Objectif : Comment déterminer/majorer le nombre de racines d'un polynôme réel $P \in \mathbb{R}[X]$ dans un intervalle donné $[a, b]$?



Si $P(a)P(b) < 0$ il y en a 1 ou 3 ou 5 ... (comptées avec multiplicité).
Si $P(a)P(b) > 0$ il y en a 0 ou 2 ou 4 ... (comptées avec multiplicité).
Comment déterminer ce nombre plus précisément ?

- La règles de Budan–Fourier et la règle de Descartes donnent des majorations à l'aide des dérivées $P, P', \ldots, P^{(n)}$ en a et b.

Ces règles sont faciles à appliquer mais restent approximatives.

- La méthode de Sturm calcule le nombre exact à l'aide de l'algorithme d'Euclide (divisions euclidiennes itérées).

C'est un résultat élémentaire, élégant, et époustouflant !

Variation de signes : définition

$$V(+,-) = V(-,+) = 1,$$
$$V(+,+) = V(-,-) = V(0,0) = 0,$$
$$V(+,0) = V(0,+) = V(-,0) = V(0,-) = \tfrac{1}{2}.$$

Définition (changements de signes, zéros inclus)

Pour une suite $(s_0, \dots, s_n)$ d'éléments dans $\mathbb{R}$ nous posons

$$V(s_0, \dots, s_n) := \sum_{k=1}^{n} V(s_{k-1}, s_k) = \sum_{k=1}^{n} \tfrac{1}{2}\big|\operatorname{sign}(s_{k-1}) - \operatorname{sign}(s_k)\big|.$$

Pour une suite $(S_0, \dots, S_n)$ de polynômes dans $\mathbb{R}[X]$ nous posons

$$V_a\big(S_0, \dots, S_n\big) := V\big(S_0(a), \dots, S_n(a)\big).$$

Pour la différence en $a, b \in \mathbb{R}$ nous écrivons $V_a^b := V_a - V_b$.

Définition (changements de signes, zéros exclus)

On forme d'abord la suite réduite $\hat{s}$ en supprimant les éléments nuls, puis on définit $\hat{V}(s) := V(\hat{s})$. De même pour $\hat{V}_a$ et $\hat{V}_a^b = \hat{V}_a - \hat{V}_b$.

Les règles de Descartes et de Budan–Fourier

Comment déterminer le nombre de racines de $P \in \mathbb{R}[X]$ dans $[a,b]$?
La règle de Descartes majore le nombre des racines positives :

Théorème (règle de Descartes)

Pour tout polynôme $P = c_0 + c_1 X + \cdots + c_n X^n$ *dans* $\mathbb{R}[X]^*$ *on a*

$$\underset{\text{mult}}{\#} \left\{ x \in \mathbb{R}_{>0} \;\middle|\; P(x) = 0 \right\} \quad \leq \quad \hat{V}(c_0, c_1, \ldots, c_n).$$

Pour les racines négatives on passe de $P(X)$ *à* $P(-X)$.

Budan et Fourier étendirent cette majoration à tout intervalle réel :

Théorème (règle de Budan–Fourier)

Pour tout polynôme $P = c_0 + c_1 X + \cdots + c_n X^n$ *dans* $\mathbb{R}[X]^*$ *on a*

$$\underset{\text{mult}}{\#} \left\{ x \in \left]a,b\right] \;\middle|\; P(x) = 0 \right\} \quad \leq \quad \hat{V}_a^b(P, P', \ldots, P^{(n)}).$$

On a égalité pour tout intervalle $]a,b] \subset \mathbb{R}$ *ssi* P *a* n *racines dans* $\mathbb{R}$.

Avantage : Cette majoration est facile à calculer.
Inconvénient : Elle surestime souvent le nombre de racines.
C'était l'état de l'art avant la découverte de Sturm en 1829.

Variation de signes : dérivées d'un polynôme

On considère un polynôme de degré n et ses dérivées :

$$\begin{aligned} P = P^{(0)} &= a_n X^n + \cdots + a_2 X^2 + a_1 X + a_0 \\ P' = P^{(1)} &= n a_n X^{n-1} + \cdots + 2a_2 X + a_1 \\ P'' = P^{(2)} &= n(n-1) a_n X^{n-2} + \cdots + 2a_2 \\ \cdots& \\ P^{(n)} &= n! a_n \end{aligned}$$

Pour $x \in \mathbb{R}$ on note $v(x) := \hat{V}\big(P(x), P'(x), \dots, P^{(n)}(x)\big)$
la variation des signes dans la suite $P, P', \dots, P^{(n)}$ évaluée en x.

Pour $x \to +\infty$ on trouve $v(x) = 0$ car

$$\operatorname{sign} P^{(k)}(x) = \operatorname{sign} \operatorname{dom} P^{(k)} = \operatorname{sign} a_n.$$

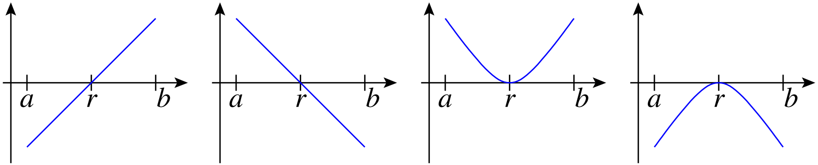
Pour $x \to -\infty$ on trouve $v(x) = n$ car

$$\operatorname{sign} P^{(k)}(x) = (-1)^{n-k} \operatorname{sign} \operatorname{dom} P^{(k)} = (-1)^{n-k} \operatorname{sign} a_n.$$

Notre objectif sera d'étudier le comportement de $v(x)$ au milieu.

Variation de signes : racines de P

Nous souhaitons comprendre $v(x)$ lors du passage d'une racine.



Pour une racine simple de P on trouve $v(a) - v(b) = 1$:
soit $(-, +, \dots) \to (0, +, \dots) \to (+, +, \dots)$,
soit $(+, -, \dots) \to (0, -, \dots) \to (-, -, \dots)$.

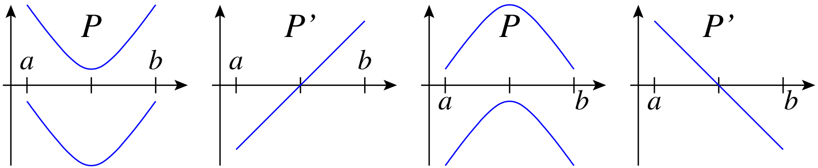
Pour une racine double de P on trouve $v(a) - v(b) = 2$:
soit $(+, -, +, \dots) \to (0, 0, +, \dots) \to (+, +, +, \dots)$,
soit $(-, +, -, \dots) \to (0, 0, -, \dots) \to (-, -, -, \dots)$.

Lors du passage d'une racine de multiplicité m la suite $(P, P', \dots, P^{(n)})$ perd m variations de signe :

Observation (passage d'une racine de P de multiplicité m)

Si $P(r) = P'(r) = \dots = P^{(m-1)}(r) = 0$ sont les seules racines de $P, P', \dots, P^{(n)}$ sur $]a, b]$, alors $v(a) - v(b) = m$. $\square$

Variation de signes : racines de $P^{(k)}$



Lors du passage d'une racine simple de P' on a $v(a) - v(b) = 0$ ou 2 :
soit $(+,-,+,\dots) \to (+,0,+,\dots) \to (+,+,+,\dots)$, $v(a) - v(b) = 2$,
soit $(-,-,+,\dots) \to (-,0,+,\dots) \to (-,+,+,\dots)$, $v(a) - v(b) = 0$,
soit $(+,+,-,\dots) \to (+,0,-,\dots) \to (+,-,-,\dots)$, $v(a) - v(b) = 0$,
soit $(-,+,-,\dots) \to (-,0,-,\dots) \to (-,-,-,\dots)$, $v(a) - v(b) = 2$.

Pour une racine double de P' on trouve $v(a) - v(b) = 2$:
soit $(*,+,-,+,\dots) \to (*,0,0,+,\dots) \to (*,+,+,+,\dots)$,
soit $(*,-,+,-,\dots) \to (*,0,0,-,\dots) \to (*,-,-,-,\dots)$.

Observation (passage d'une racine de $P^{(k)}$ pour $k \geq 1$)

Supposons que $k \geq 1$ et que $P^{(k)}(r) = \cdots = P^{(k+m-1)}(r) = 0$ sont les seules racines de $P, P', \dots, P^{(n)}$ sur $]a,b]$. Alors on trouve $v(a) - v(b) = m$ pour m pair, et $v(a) - v(b) = m \pm 1$ pour m impair. $\square$

La règle de Budan–Fourier : démonstration

Théorème (Budan 1807, Fourier 1820)

Soit $P \in \mathbb{R}[X]$. On note $m(a,b)$ le nombre des racines dans $]a,b]$, comptées avec multiplicités. Alors on a $m(a,b) \le v(a) - v(b)$.

Plus précisément, on a $m(a,b) = v(a) - v(b) - 2u$ où $u \in \mathbb{N}$.

On a l'égalité $m(a,b) = v(a) - v(b)$ pour tout $a < b$ dans $\mathbb{R}$ si et seulement si P est de degré n et admet n racines réelles.

Démonstration.
On a déjà observé que $v(a) - v(b) = m(a,b) + 2u$.
On a donc $m(a,b) = v(a) - v(b) - 2u \le v(a) - v(b)$.
Choisissons $]a_0, b_0]$ contenant les racines réelles de $P, P', \dots, P^{(n)}$.
Alors $v(a) = n$ pour tout $a \le a_0$ et $v(b) = 0$ pour tout $b \ge b_0$.
Si $m(a,b) < v(a) - v(b)$ sur un intervalle $]a,b]$, alors

$$\begin{aligned} m(a_0,b_0) &= m(a_0,a) + m(a,b) + m(b,b_0) \\ &< \big(v(a_0) - v(a)\big) + \big(v(a) - v(b)\big) + \big(v(b) + v(b_0)\big) = n. \end{aligned}$$

Par contraposé, si $m(a_0,b_0) = n$, alors $m(a,b) = v(a) - v(b)$. $\square$

La règle de Descartes : démonstration

Corollaire (règle de Descartes, 1637)

Soit $P = c_0 + c_1 X + c_2 X^2 + \cdots + c_n X^n$ *un polynôme réel.*

Alors P *admet au plus* $V(c_0, c_1, c_2, \ldots, c_n)$ *racines positives,*
et au plus $V(+c_0, -c_1, +c_2, \ldots, (-1)^n c_n)$ *racines négatives.*

S'il y en a moins, le défaut est un nombre pair.

Démonstration. On applique le théorème de Budan–Fourier :

- Pour $a = 0$ on a $v(0) = V(c_0, c_1, \ldots, c_n)$.
- Pour $b > 0$ assez grand on a $v(b) = 0$.

Ainsi $m(a, b) \leq v(a) - v(b) = V(c_0, c_1, \ldots, c_n)$.
Pour les racines négatives on considère $P(-X)$. □

Exemple

$P(X) = -1 - X + X^2 + X^3$ admet exactement une racine positive.
$P(-X) = -1 + X - X^2 - X^3$ admet 2 ou 0 racines positives.
Effectivement, on trouve la factorisation $P = (X - 1)(X + 1)^2$.

Le théorème de Sturm : énoncé

Théorème (Sturm 1829)

Pour tout polynôme réel $P \in \mathbb{R}[X]^*$ et tout intervalle $[a,b]$ nous avons

$$\#\{\, x \in [a,b] \mid P(x) = 0 \,\} \;=\; V_a^b\big(S_0, S_1, \dots, S_n\big).$$

D'éventuelles racines sur le bord $\{a,b\}$ comptent pour un demi.

Ici la suite $S_0, S_1, \dots, S_n$ est construite de $S_0 = P$ et $S_1 = P'$ par division euclidienne $S_{k+1} = -(S_{k-1} \operatorname{rem} S_k)$ jusqu'à ce que $S_{n+1} = 0$.

Ainsi $S_n \sim \operatorname{pgcd}(P, P')$ comme dans l'algorithme d'Euclide (ici signé). Si S_n n'est pas constant, il faut encore diviser $S_0, S_1, \dots, S_n$ par S_n.

Corollaire

Ce théorème permet de compter puis de localiser toutes les racines réelles : On commence par la borne de Cauchy puis on subdivise. . .

Le théorème de Sturm : exemples

Algorithme de Sturm : $S_0 := P, \quad S_1 := P', \quad S_{k+1} = -(S_{k-1} \operatorname{rem} S_k)$.

x	-3	-2	-1	0	1	2	3
$X^3 - 2X^2 + 1 = S_0$	-44	-15	-2	$+1$	0	$+1$	$+10$
$3X^2 - 4X = S_1$	$+39$	$+20$	$+7$	0	-1	$+4$	$+15$
$\frac{8}{9}X - 1 = S_2$	$-\frac{11}{3}$	$-\frac{25}{9}$	$-\frac{17}{9}$	-1	$-\frac{1}{9}$	$+\frac{7}{9}$	$+\frac{5}{3}$
$\frac{45}{64} = S_3$	$+\frac{45}{64}$	$+\frac{45}{64}$	$+\frac{45}{64}$	$+\frac{45}{64}$	$+\frac{45}{64}$	$+\frac{45}{64}$	$+\frac{45}{64}$
V	3	3	3	2	$\frac{3}{2}$	0	0

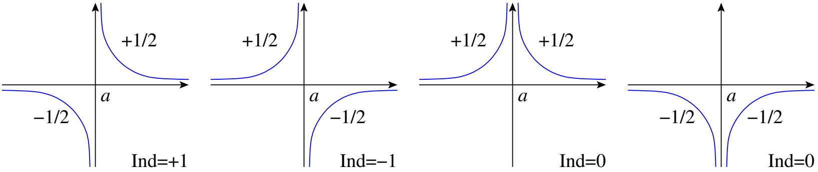
Dans cet exemple les racines sont 1 et $\frac{1+\sqrt{5}}{2} \approx 1.62$ et $\frac{1-\sqrt{5}}{2} \approx -0.62$.

x	-3	-2	-1	0	1	2	3
$X^3 - 2X^2 + 2 = S_0$	-43	-14	-1	$+2$	$+1$	$+2$	$+11$
$3X^2 - 4X = S_1$	$+39$	$+20$	$+7$	0	-1	$+4$	$+15$
$\frac{8}{9}X - 2 = S_2$	$-\frac{14}{3}$	$-\frac{34}{9}$	$-\frac{26}{9}$	-2	$-\frac{10}{9}$	$-\frac{2}{9}$	$+\frac{2}{3}$
$-\frac{99}{16} = S_3$	$-\frac{99}{16}$	$-\frac{99}{16}$	$-\frac{99}{16}$	$-\frac{99}{16}$	$-\frac{99}{16}$	$-\frac{99}{16}$	$-\frac{99}{16}$
V	2	2	2	1	1	1	1

Dans cet exemple il n'existe qu'une seule racine réelle, $r \approx -0.84$.

Pôles d'une fonction rationnelle

Soit $f = \frac{Q}{P} \in \mathbb{R}(X)^*$ une fraction rationnelle où $\mathrm{pgcd}(Q,P) = 1$.
On compte les pôles de f selon la convention suivante :



Définition (indice de Cauchy en un point)

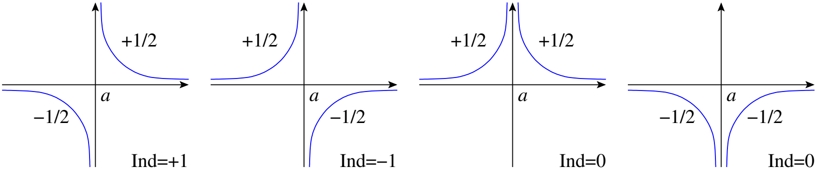
Pour $f \in \mathbb{R}(X)^*$ et $a \in \mathbb{R}$ on pose

$$\mathrm{Ind}_a(f) := \mathrm{Ind}_a^+(f) - \mathrm{Ind}_a^-(f) \quad \text{où}$$

$$\mathrm{Ind}_a^\varepsilon(f) := \begin{cases} +\frac{1}{2} & \text{si } \lim_a^\varepsilon f = +\infty, \\ -\frac{1}{2} & \text{si } \lim_a^\varepsilon f = -\infty, \\ 0 & \text{sinon.} \end{cases}$$

Par exemple, on a $\mathrm{Ind}_0\left(\frac{1}{x}\right) = 1$ et $\mathrm{Ind}_0\left(-\frac{1}{x}\right) = -1$ et $\mathrm{Ind}_0\left(\frac{\pm 1}{x^2}\right) = 0$.

L'indice de Cauchy : définition



Définition (indice de Cauchy sur un intervalle)

Pour $a < b$ dans $\mathbb{R}$ nous posons

$$\operatorname{Ind}_a^b(f) := \sum_{x \in]a,b[} \operatorname{Ind}_x(f) \quad + \quad \operatorname{Ind}_a^+(f) - \operatorname{Ind}_b^-(f).$$

Pour $b < a$ on pose $\operatorname{Ind}_a^b(f) := -\operatorname{Ind}_b^a(f)$, et finalement $\operatorname{Ind}_a^a(f) := 0$.

Remarque

L'indice de Cauchy jouit des propriétés semblables à l'intégrale :

1. $\operatorname{Ind}_a^b(f) + \operatorname{Ind}_b^c(f) = \operatorname{Ind}_a^c(f)$ pour tout $a, b, c \in \mathbb{R}$.
2. $\operatorname{Ind}_a^b(f \circ \tau) = \operatorname{Ind}_{\tau(a)}^{\tau(b)}(f)$ pour toute fonction affine $\tau(x) = px + q$.

L'indice de Cauchy compte les racines réelles

Proposition (dérivée logarithmique)

Pour $f \in \mathbb{R}(X)^*$ *on a* $\operatorname{Ind}_a(f'/f) = \begin{cases} +1 & \textit{si } a \textit{ est une racine de } f, \\ -1 & \textit{si } a \textit{ est un pôle de } f, \\ 0 & \textit{sinon.} \end{cases}$

Démonstration. On factorise $f = (X-a)^m g$ tel que $g(a) \in \mathbb{R}^*$.
On obtient $\frac{f'}{f} = \frac{m}{X-a} + \frac{g'}{g}$. Ainsi $\operatorname{Ind}_a\left(\frac{f'}{f}\right) = \operatorname{sign}(m)$. $\square$

Corollaire (racines réelles de polynômes réels)

L'indice $\operatorname{Ind}_a^b(P'/P)$ *compte les racines de* $P \in \mathbb{R}[X]^*$ *dans* $[a,b]$ *:*

$$\#\left\{ x \in [a,b] \;\middle|\; P(x) = 0 \right\} \quad = \quad \operatorname{Ind}_a^b\left(P'/P\right).$$

D'éventuelles racines sur le bord $\{a,b\}$ *comptent pour un demi.*

Problème : Comment calculer l'indice sans connaître les pôles ?
Solution : La suite de Sturm permet de calculer $\operatorname{Ind}_a^b(\frac{Q}{P})$.

La formule d'inversion de Cauchy

Formule d'inversion (Cauchy 1837)

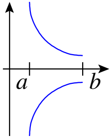
Si $P, Q \in \mathbb{R}[X]^*$ n'ont pas de racine commune en a ni en b, alors

$$\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) + \operatorname{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $\operatorname{pgcd}(P, Q) = 1$.

Si $[a, b]$ ne contient pas de racine de P ni de Q, alors les indices $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right)$ et $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right)$ sont nuls, puis le TVI assure que $V_a^b(P, Q) = 0$.

La formule est additive par rapport à bisection de l'intervalle.
Si $[a, b]$ contient de racines, on peut donc supposer que c'est a ou b.
Par symétrie nous pouvons supposer que $P(a) = 0$ et $Q(a) \neq 0$.
Sur $]a, b]$ les polynômes P, Q sont non nuls, donc de signe constant.



$$\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) = +\frac{1}{2} \quad \Rightarrow \quad V_a(P, Q) = \frac{1}{2}, \quad V_b(P, Q) = 0$$

$$\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) = -\frac{1}{2} \quad \Rightarrow \quad V_a(P, Q) = \frac{1}{2}, \quad V_b(P, Q) = 1$$

Dans les deux cas nous obtenons l'égalité énoncée. $\square$

Suites de Sturm

Définition (suite de Sturm)

Une suite $(S_0, \dots, S_n)$ dans $\mathbb{R}[X]$ est ***de Sturm*** sur $[a, b] \subset \mathbb{R}$ si $S_k(x) = 0$ pour $0 < k < n$ et $x \in [a, b]$ entraîne $S_{k-1}(x)S_{k+1}(x) < 0$.

Exemple. Pour $\frac{R}{S}$ où $\operatorname{pgcd}(R, S) = 1$ l'algorithme d'Euclide signé produit une suite de Sturm commençant par $S_0 = S$ et $S_1 = R$ puis

$$S_{k+1} = S_k Q_k - S_{k-1} \quad \text{jusqu'à} \quad S_n = \text{const.}$$

Exemple. On peut assouplir l'hypothèse : il suffit que

$$a_k S_{k+1} = S_k Q_k - b_k S_{k-1}$$

avec des constantes réelles $a_k, b_k > 0$.

Exemple. Plus généralement encore, il suffit que

$$A_k S_{k+1} = S_k Q_k - B_k S_{k-1}$$

avec des polynômes réels A_k, B_k vérifiant $A_k(x) > 0$ et $B_k(x) > 0$, puis $S_n(x) \neq 0$ pour tout x dans l'intervalle $[a, b]$ en question.

Le théorème de Sturm

Corollaire (de la formule d'inversion)

Si $(S_0, S_1, \dots, S_n)$ *est une suite de Sturm sur* $[a, b] \subset \mathbb{R}$*, alors*

$$\operatorname{Ind}_a^b\Big(\frac{S_1}{S_0}\Big) + \operatorname{Ind}_a^b\Big(\frac{S_{n-1}}{S_n}\Big) = V_a^b\big(S_0, S_1, \dots, S_{n-1}, S_n\big).$$

Démonstration. La formule d'inversion est télescopique :

$$\operatorname{Ind}_a^b\Big(\frac{S_1}{S_0}\Big) + \operatorname{Ind}_a^b\Big(\frac{S_0}{S_1}\Big) + \operatorname{Ind}_a^b\Big(\frac{S_2}{S_1}\Big) + \operatorname{Ind}_a^b\Big(\frac{S_1}{S_2}\Big) = V_a^b\big(S_0, S_1, S_2\big).$$

Les termes au milieu s'annulent : si $S_1(x) = 0$, alors $S_0(x)S_2(x) < 0$.

Théorème (fraction continue selon l'algorithme d'Euclide)

Pour R/S *où* $\operatorname{pgcd}(R, S) = 1$ *l'algorithme d'Euclide signé produit une suite de Sturm* $S_0 = S$*,* $S_1 = R$*, …,* $S_n = 1$*,* $S_{n+1} = 0$*. Ainsi*

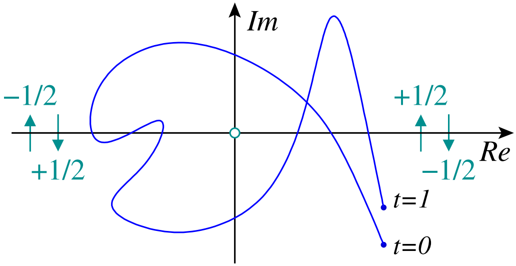
$$\operatorname{Ind}_a^b\big(R/S\big) = V_a^b\big(S_0, S_1, \dots, S_n\big).$$

Cette formule permet de calculer l'indice de Cauchy $\operatorname{Ind}_a^b\big(R/S\big)$.

L'indice de Cauchy compte le nombre de tours

Soient $R, S \in \mathbb{R}[X]$ deux polynômes réels et $F = R + iS$.

L'application $[0,1] \to \mathbb{C}$, $t \mapsto F(t)$, décrit un chemin dans le plan complexe, allant de $F(0)$ vers $F(1)$, à coordonnées $R(t) + iS(t)$.



Observation

L'indice $\frac{1}{2}\,\mathrm{Ind}_0^1\left(\frac{R}{S}\right)$ compte le nombre de tours autour de 0 :
traverser l'axe réel compte $\pm\frac{1}{2}$ selon le sens gauche / droite.

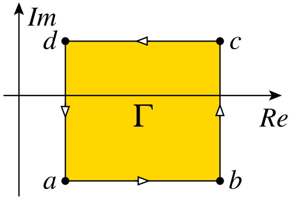
On suppose ici que le chemin $Q(t)$ ne passe pas par 0.
Autrement dit, R et S n'ont pas de racine commune.

Indice de Cauchy d'un polynôme complexe

Soit $P \in \mathbb{C}[X]$ un polynôme complexe.
Comment localiser ses racines ?

Objectif : établir une méthode effective analogue au théorème de Sturm réel.

Au lieu d'un intervalle $[a,b] \subset \mathbb{R}$
on considère un rectangle $\Gamma \subset \mathbb{C}$.



Calcul d'indice : On considère le chemin rectiligne de a vers b.
Par changement de variable on pose $F = P\big(a + (b-a)X\big)$.
Les parties $R = \operatorname{Re} F$ et $S = \operatorname{Im} F$ sont des polynômes réels.
L'application $[0,1] \to \mathbb{C}$, $t \mapsto F(t)$ décrit un chemin allant de $F(0) = P(a)$ vers $F(1) = P(b)$, à coordonnées $R(t) + iS(t)$.

Définition

On pose $\operatorname{ind}_a^b(P) := \frac{1}{2} \operatorname{Ind}_0^1\big(\frac{R}{S}\big)$. Pour le rectangle Γ on pose
$\operatorname{ind}_{\partial\Gamma}(P) := \operatorname{ind}_a^b(P) + \operatorname{ind}_b^c(P) + \operatorname{ind}_c^d(P) + \operatorname{ind}_d^a(P)$.

$\operatorname{ind}_{\partial\Gamma}(P)$ se calcule aussi efficacement que dans le cas réel :
Euclide pour la suite de Sturm de $\frac{R}{S}$, puis évaluation en 0 et 1.

L'indice de Cauchy compte les racines complexes

Proposition (exercice)

Pour $P = X - r$ *on a* $\operatorname{ind}_{\partial\Gamma}(P) = \begin{cases} 1 & \text{si } r \text{ est à l'intérieur de } \Gamma, \\ \frac{1}{2} & \text{si } r \text{ est sur un coté de } \Gamma, \\ \frac{1}{4} & \text{si } r \text{ est un sommet de } \Gamma, \\ 0 & \text{si } r \text{ est à l'extérieur de } \Gamma. \end{cases}$

Théorème (admis)

Si $P, Q \in \mathbb{C}[X]$ *n'ont pas de racines sur les sommets de* $\Gamma \subset \mathbb{R}^2$*, alors*

$$\operatorname{ind}_{\partial\Gamma}(P \cdot Q) = \operatorname{ind}_{\partial\Gamma}(P) + \operatorname{ind}_{\partial\Gamma}(Q).$$

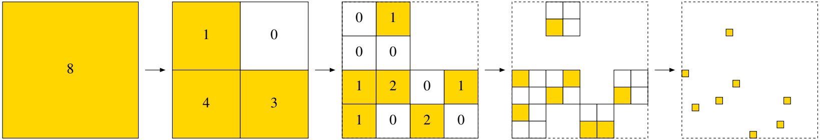
📖 M. Eisermann, *The Fundamental Theorem of Algebra made effective : an elementary real-algebraic proof via Sturm chains.*

Corollaire

Si $P \in \mathbb{C}[X]$ *n'admet pas de racine sur les sommets de* $\Gamma \subset \mathbb{R}^2$*, alors* $\operatorname{ind}_{\partial\Gamma}(P)$ *compte le nombre des racines de* P *dans* Γ*.*

Localisation des racines complexes

Par dichotomie, l'indice de Cauchy permet de localiser toutes les racines complexes d'un polynôme complexe donné $P \in \mathbb{C}[X]$.



◇ On commence par le carré $[-\rho, +\rho]^2$ où ρ est la borne de Cauchy. Chaque carré contenant des racines est subdivisé en quatre. On ne retient que ceux d'indice > 0, contenant des racines.

◇ On peut assurer que les racines de P sont simples, quitte à diviser par $\operatorname{pgcd}(P, P')$. Dès qu'on a bien séparé les racines, on passe à la méthode de Newton, qui converge plus rapidement.

Conclusion

Cette méthode a le mérite d'être élémentaire et facile à implémenter. Elle est suffisamment rapide pour des polynômes de degré moyen. Pour des polynômes de grand degré il existe des algorithmes plus économes, mais plus compliqués. (Schönhage 1982, Smale 1986.)