Théorème de Sturm

Chen Thomas
t.chen.thomas1[at]gmail.com

17 mai 2024

Attention

1. Ce document contient certainement des coquilles. N'hésitez pas à me le signaler. De même si vous avez une question.
2. Pour les recasages, ce sont les miens mais ce développement se case peut-être ailleurs et je n'y ai pas réfléchi.
3. Il se peut que ce développement dure plus de 15 minutes. J'ai essayé de le découper pour faire des recollements personnalisés.

Leçons

- 142 : pgcd et ppcm, algorithmes de calcul. Applications.
- 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Références

[1] S. Francinou, H. Gianella, S. Nicolas. *Exercices de mathématiques. Oraux X-ENS, Algèbre 1.* Cassini, 2001.

Théorème 1. *[1] Soit $P \in \mathbb{R}[X]$. On définit la suite $(S_i)_{i\in[\![0,p]\!]}$ de sorte que $S_0 = P, S_1 = P'$ et S_{i+2} est l'opposé du reste de la division euclidienne de S_i par S_{i+1} avec $S_p \neq 0$ et $S_{p+1} = 0$. Pour tout $x \in \mathbb{R}$, on note $V(x)$ le nombre de changement de signes stricts dans l'uplet $(S_0(x), S_1(x), \cdots, S_p(x))$. Pour $a < b \in \mathbb{R}$ avec $P(a)P(b) \neq 0$, le nombre de racines distinctes de P dans $[a, b]$ est $V(a) - V(b)$.*

Démonstration. La famille $(S_i)_i$ existe et est bien construite : c'est l'algorithme d'Euclide sauf que l'on retient l'opposé du reste. Par construction, on a alors $\mathrm{pgcd}(S_i, S_{i+1}) = S_p$ pour $i \in [\![0, p]\!]$ [1]. On définit $T_i = \dfrac{S_i}{S_p}$ de sorte que T_i et T_{i+1} soient premiers entre eux. On note que $T_p = 1$ et T_0 est à racines simples et a les racines de P [2]. Si $S_p(x) =\neq 0$, en notant $V_1(x)$ le nombre de changement de signes stricts de $(T_0(x), \cdots, T_p(x))$, on a $V_1(x) = V(x)$ par construction.

En particulier, pour $x = a$ et $x = b$, l'égalité tient. En effet, puisque a n'est pas racine de P, a ne peut être racine de S_p qui divise P et pareillement pour b. Ainsi,

$$V_1(a) - V_1(b) = V(a) - V(b).$$

Il suffit donc de montrer que la quantité $V_1(a) - V_1(b)$ vaut le nombre de racines de P donc de T_0 sur $[a, b]$.

Etant donné que la liste des (T_i) est finie et que chaque T_i donne un nombre fini de racines, l'ensemble $A = \{x \in [a, b] : \exists i \in [\![0, p]\!], T_i(x) = 0\}$ est un ensemble fini. On peut donc considérer $\varepsilon' = \min(\{|x - y| : (x, y) \in A^2\})$ et $k = \left\lceil \dfrac{b-a}{\varepsilon'} \right\rceil$. On pose enfin $\varepsilon = \dfrac{b-a}{k} \leq \varepsilon'$.

Ainsi, il suffit d'observer trois choses. Si l'on connait $V_1(x)$ avec $x \in [a, b]$, on veut connaitre $V_1(x + \varepsilon)$ et

1. $\mathrm{pgcd}(a, 0) = a$ si $a \neq 0$
2. en effet, si α est racine de multiplicité q, alors $(X - \alpha)^{q-1} | P, P'$ donc $(X - \alpha)^{q-1} | S_p$

1. Si $[x, x+\varepsilon]$ contient une racine de P, alors $V_1(x+\varepsilon) = V_1(x) - 1$.
2. Si $[x, x+\varepsilon]$ contient une racine d'un T_i mais pas T_0, alors $V_1(x+\varepsilon) = V_1(x)$.
3. Si $[x, x+\varepsilon]$ ne contient aucune racine, il est clair que $V_1(x+\varepsilon) = V_1(x)$.

Soit donc $\alpha \in [x, x+\varepsilon]$.

1. Si α est racine de P, alors $P^2(\alpha) = 0$ donc P^2 présente un minimum en α. Ainsi, $(P^2)' = 2PP'$ est alors négative puis positive au voisinage de α, disons $\alpha \pm \eta$. Pour $|h| \leq \dfrac{1}{2}(\min(x+\varepsilon-\alpha, \alpha - x), \eta)$, on a donc $T_0(\alpha+h)T_1(\alpha+h) = S_p^2(\alpha+h)P(\alpha+h)P'(\alpha+h)$.

   Puisque $S_p^2(\alpha+h) > 0$ (on a $P(\alpha+h) \neq 0$ puisque $h < \varepsilon$), on a que le signe de $T_0(\alpha+h)T_1(\alpha+h)$ est le signe de $P(\alpha+h)P'(\alpha+h)$. Mais on a dit que PP' est négative puis positive sur $[\alpha - h, \alpha + h]$ donc PP' a le signe de h. Ainsi, sur $[x, \alpha - h]$, les signes entre P et P' sont opposés, puis deviennent le même sur la transition $[\alpha - h, \alpha + h]$ et ce jusqu'à $x + \varepsilon$: il y a un changement de signe en moins sur $[x, x+\varepsilon]$ et on a $V_1(x+\varepsilon) = V_1(x) - 1$.
2. Si α est racine d'un des T_i qui n'est pas T_0, déjà, $i < p$. La relation $S_{i-1} = A_iS_i - S_{i+1}$ donne $T_{i-1} = A_iT_i - T_{i+1}$ donc $T_{i-1}(\alpha) = -T_{i+1}(\alpha)$. α étant ni racine de T_{i+1}, ni racine de T_{i-1} (par primalité relative), on a $(T_{i-1}T_{i+1})(\alpha) < 0$. On a donc $T_{i-1}T_{i+1}$ non nul de signe opposé en α donc sur tout $[x, x+\varepsilon]$ par continuité et puisqu'ils ne s'y annulent pas. Ainsi, sur les indices $\{i-1, i, i+1\}$ entre x et $x+\varepsilon$, il y a autant de changement de signe.

En itérant le procédé k fois à partir de a, on a donc $V_1(a) - V_1(b)$ égal au nombre de racines de P car il y a autant de -1 que de racines de P. $\square$