144

Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Soient k un corps commutatif, K une extension de corps de k et n un entier naturel non nul. On dit que $a \in K^n$ est une racine de $P \in k[X_1,\dots,X_n]$ dans K^n lorsque P est dans le noyau de l'application $ev_a : k[X_1,\dots,X_n] \longrightarrow K$, $Q \longmapsto Q(a)$.

I Arithmétique et théorie des corps

1) Propriétés arithmétiques de $k[X]$ [RDO]

p.173 **Prop 1:** Soit a dans k. Sont équivalents :
i) a est racine de P
ii) $X-a$ divise P dans $k[X]$

p.175 **Déf-Prop 2:** On dit que $a \in k$ est racine d'ordre $m \in \mathbb{N}^*$ de P lorsque l'une des assertions équivalentes suivantes est vérifiée :
i) $\exists Q \in k[X],\ P=(X-a)^m Q$ et $Q(a) \neq 0$
ii) $(X-a)^m$ divise P dans $k[X]$ mais pas $(X-a)^{m+1}$

p.172 **Th 3 (Formule de Taylor):**
Si k est de caractéristique nulle alors pour tout $a \in k$, on a $P=\sum_{n \in \mathbb{N}} \frac{P^{(n)}(a)}{n!}(X-a)^n$.

p.174 **Application 4:** Si k est de caractéristique nulle et $a \in k$, alors a est racine d'ordre $m \in \mathbb{N}^*$ de P ssi $P(a)=P'(a)=\dots=P^{(m-1)}(a)=0$ et $P^{(m)}(a) \neq 0$.

p.175 **Contre-exemple 5:** $(X-1)^p$ admet 1 pour racine d'ordre p mais toutes ses dérivées sont nulles dans $\mathbb{F}_p[X]$.

p.176 **Déf 6:** On dit que $P \in k[X]$ est scindé sur k s'il existe $a, \alpha_1, \dots, \alpha_n \in k$ tels que $P = a\prod_{i=1}^{n}(X-\alpha_i)$.
En particulier n est le degré de P (sauf si $P=0$) et les α_i sont ses racines.

Prop 7: Si P est irréductible alors il n'admet pas de racines dans k.

Remarque 8: La réciproque est fausse comme le montre $(X^2+1)^2$ dans $\mathbb{R}[X]$. Cependant elle est vraie en petit degré.

Prop 9: Si $\deg P \leq 3$ et si P n'a pas de racines dans k alors P est irréductible.

Exemple 10: X^2+X+1 est irréductible dans $\mathbb{F}_2[X]$.

2) Extensions algébriques [Tau]

p.79 **Déf 11:** Si K/k est une extension de k et $a \in K$, $k(a)$ est le plus petit sous-corps de K contenant a et k. a est dit algébrique sur k s'il existe $P \in k[X] \setminus \{0\}$ tel que $P(a)=0$, i.e. si ev_a est non injectif.
a est dit transcendant sur k dans le cas contraire.
On dit que K/k est une extension algébrique si tous les éléments de K sont algébriques sur k.

p.80 **Prop 12:** Toute extension de degré finie est algébrique.

[Cal] p.31 **Contre-exemple 13:** Si p_n désigne le n-ième nombre premier et $F_n = \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$, alors $F = \bigcup_{n \in \mathbb{N}^*} F_n$ est une extension algébrique de $\mathbb{Q}$ de degré infini.

p.30 **Th 14:** Si $a \in K$ est algébrique sur k alors $k(a)=k[a]$, $k(a)$ est un k-espace vectoriel de dimension finie n dont la famille $(1, a, \dots, a^{n-1})$ est une base.

3) Racines et extensions de corps [Tau]

Déf 15 : Si P est irréductible, on appelle corps de rupture de P toute extension K/k telle que P ait une racine α dans K et telle que $K = k(\alpha)$.

Exemple : $\mathbb{Q}(\sqrt[3]{5})$ est un corps de rupture de $X^3 - 5 \in \mathbb{Q}[X]$

Th 17 : Si P est irréductible, $k[X]/(P)$ est un corps de rupture de P, et c'est le seul à isomorphisme près.

Déf 18 : On appelle corps de décomposition de P toute extension K/k telle que P soit scindé sur K, et si $\alpha_1, \dots, \alpha_n$ désignent les racines de P dans K alors $K = k(\alpha_1, \dots, \alpha_n)$.

Exemples 19 : - $\mathbb{Q}(\sqrt[3]{5}, j)$ est un corps de décomposition de $X^3 - 5$, qui n'est pas son corps de rupture.
- $\mathbb{Q}(e^{\frac{2i\pi}{n}})$ avec n premier est un corps de décomposition de $X^n - 1$, et son corps de rupture.

Th 20 : Il existe un unique corps de décomposition de P à isomorphisme près.

4) Clôtures algébriques [Cal]

Déf 21 : On dit que k est algébriquement clos si tout polynôme de $k[X]$ (non constant) admet une racine dans k.

Th 22 (D'Alembert-Gauss) : $\mathbb{C}$ est algébriquement clos.

Remarque 23 : $\mathbb{R}$ n'est pas algébriquement clos, les corps finis ne sont pas algébriquement clos.

Déf 24 : On dit que K/k est une clôture algébrique de k si K est algébrique sur k et est algébriquement clos.

Th 25 (Steinitz) (admis) : Tout corps admet une clôture algébrique unique à isomorphisme près.

Exemple 26 : - $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.
- $\bigcup_{n \in \mathbb{N}^*} \mathbb{F}_{p^{n!}}$ est la clôture algébrique de $\mathbb{F}_p$.

II Localisation et dénombrement de racines

1) Localisation sur $\mathbb{R}$ ou $\mathbb{C}$

Th 27 (Rolle) : Si $a, b \in \mathbb{R}$, $a < b$ et $P(a) = P(b)$ alors P' admet une racine dans $]a, b[$.

Application 28 : Si P est scindé sur $\mathbb{R}[X]$ alors P' aussi.

Th 29 (Newton) : Si $P = \prod_{i=1}^{n} (X - \xi_i)^{m_i}$, avec $\xi_1 < \dots < \xi_n$ et les m_i entiers ($\neq 0$) alors la suite définie par $\begin{cases} x_0 > \xi_n \\ x_{n+1} = x_n - \frac{P(x_n)}{P'(x_n)} \end{cases}$ converge vers ξ_n. De plus si $m_n = 1$, alors pour tout $c > 0$, $|x_n - \xi_n| = o(c^n)$ quand $n \to +\infty$.

Th 30 (Gershgörin) : Soit $A = (a_{i,j})_{1 \le i,j \le n} \in \mathcal{M}_n(\mathbb{C})$. Pour $1 \le i \le n$, on note $R_i = \sum_{\substack{1 \le j \le n \\ j \neq i}} |a_{i,j}|$.

Alors $\mathrm{Sp}\, A \subset \bigcup_{i=1}^{n} \{z \in \mathbb{C},\ |z - a_{i,i}| \le R_i\}$.

2) Dénombrement de racines

Th 31 (Sturm) : Soit P dans $\mathbb{R}[X]$ à racines simples non constant. On définit la suite $(P_i)_i$ par : $P_0 = P$, $P_1 = P'$, $P_{i+1} = -P_{i-1} \bmod P_i$ pour $i \ge 1$ et $s \in \mathbb{N}$ le plus petit indice tel que $P_{s+1} = 0$. En notant $V(x) = |\{(i,j),\ 0 \le i < j \le s,\ P_i(x)P_j(x) < 0,\ P_k(x) = 0 \text{ si } i < k < j\}|$, le nombre de racines distinctes de P dans $[a, b] \subset \mathbb{R}$ est $V(a) - V(b)$.

p.99 p.100 p.103 p.104 p.67 p.35 p.73 p.74 p.76 p.77

[Cal] p.39 et p.84

[Rom] p.137

DVPT 1

[Ch-LF] p.210

[FGN] p.80

[FG] p.230

Jordan pièges

DVPT2

[Zav] p. 32

Th 32 (Chevalley-Warning) : Si $\mathrm{car}(k) = p$, k est fini, $(f_a)_{a\in A}$ une famille finie de $k[X_1,\dots,X_n]$ telle que $\sum_{a\in A} \deg f_a < n$, alors $|\{x \in k^n, \forall a \in A, f_a(x) = 0\}| = 0 [p]$.

III Polynômes symétriques

1) Action de S_n sur $k[X_1,\dots,X_n]$ [RDO]

Déf 33 : On dit que $P \in k[X_1,\dots,X_n]$ est symétrique si pour tout $\sigma \in S_n$, $\sigma \cdot P := P(X_{\sigma(1)},\dots,X_{\sigma(n)}) = P$.

Exemple 34 : Le polynôme $X_1^2 + X_2^2 + X_3^2$ est symétrique dans $k[X_1,X_2,X_3]$.

Déf 35 : Pour $1 \le k \le n$, on définit le k-ième polynôme symétrique élémentaire comme $\Sigma_k := \sum_{1 \le i_1 < \dots < i_k \le n} X_{i_1} \dots X_{i_k}$.

Exemples 36 : On a $\Sigma_1 = X_1 + \dots + X_n$ et $\Sigma_n = X_1 \dots X_n$.

Prop 37 : Pour $1 \le k \le n$, Σ_k est homogène de degré k et de degré partiel 1 par rapport à chaque X_i.

2) Structure de l'ensemble des polynômes symétriques [RDO]

Prop 38 : Les polynômes symétriques forment une sous-k-algèbre de $k[X_1,\dots,X_n]$.

Th 39 : Tout polynôme symétrique est un polynôme en les polynômes symétriques élémentaires.

Exemple 40 : $X_1^3 + X_2^3 + X_3^3 = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$.

Th 41 (Méthode de Waring) : Soit P dans $k[X_1,\dots,X_n]$ non nul, homogène et symétrique, de coefficient dominant (pour l'ordre lexicographique) a_i, avec $i \in \mathbb{N}^n$. Alors le polynôme $P - a_i (\Sigma_1)^{i_1 - i_2} (\Sigma_2)^{i_2 - i_3} \dots (\Sigma_{n-1})^{i_{n-1} - i_n} (\Sigma_n)^{i_n}$ est symétrique, homogène, ne possédant pas le monôme $a_i X_1^{i_1} \dots X_n^{i_n}$ et il est nul ou de degré strictement inférieur à celui de P pour l'ordre lexicographique.

Application 42 (du Th 39) : Toute fonction de $\mathcal{M}_n(\mathbb{C})$ dans $\mathbb{C}$ polynomiale et invariante par conjugaison est un polynôme en les coefficients du polynôme caractéristique.

Th 43 (Sommes de Newton) : Pour $k \in \mathbb{N}$, posons $S_k = \sum_{i=1}^n X_i^k$.

Si $1 \le p \le n$, $S_p - \Sigma_1 S_{p-1} + \dots + (-1)^{p-1} \Sigma_{p-1} S_1 + (-1)^p p \Sigma_p = 0$.

Si $p > n$, $S_p - \Sigma_1 S_{p-1} + \dots + (-1)^n \Sigma_n S_{p-n} = 0$.

Prop 44 (Relations coefficients-racines) : Si $P = \sum_{i=0}^n a_i X^i$ avec $a_n \neq 0$ est scindé avec $\alpha_1,\dots,\alpha_n$ pour racines alors pour $1 \le k \le n$, $\Sigma_k(\alpha_1,\dots,\alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}$.

Application 45 : Les racines d'un polynôme dépendent continûment du polynôme pour la norme $\|\sum_{n=0}^d a_n X^n\| = \sum_{n=0}^d |a_n|$.

4) Résultant [Mér]

Déf 46 : On appelle résultant de $P \in k_p[X]$ et $Q \in k_q[X]$ le déterminant de $\varphi : k_{q-1}[X] \times k_{p-1}[X] \to k_{q+p-1}[X]$, $(U,V) \mapsto UP + VQ$.

Prop 47 : Le résultant de P et Q est nul ssi P et Q ont un facteur commun non nul dans $k[X]$.

Prop 48 : Si $P = a_0(X-x_1)\dots(X-x_p)$ et $Q = b_0(X-y_1)\dots(X-y_q)$ alors $\mathrm{Res}(P,Q) = a_0^q \prod_{i=1}^p Q(x_i) = (-1)^{pq} b_0^p \prod_{i=1}^q P(y_i)$.

Th 49 (Borne de Bézout) : Si k est infini, $P, Q \in k[X,Y]$ sont premiers entre eux, alors $|\{(x,y) \in k^2, P(x,y) = Q(x,y) = 0\}| \le \deg P \deg Q$.

DVPT3

p. 200 p. 201 p. 203 p. 200 p. 206

[Gou] p. 79

p. 207 [Gou] p. 60 [FG] p. 377 p. 378 p. 384 p. 36

Références :

[Cal] Josette Calais, "Extensions de corps - théorie de Galois", Ellipses, 2006

[Ch-LF] Antoine Chambert-Loir, Stéfane Fermigier, "Analyse 2 - Exercices", Masson, 1999

[FG] Serge Francinou, Hervé Gianella, "Exercices de mathématiques pour l'agrégation - Algèbre 1", Masson, 1997

[FGN] ———————, Serge Nicolas, "Oraux X-ENS - Algèbre 2", Cassini, 2009

[Gou] Xavier Gourdon, "Algèbre", Ellipses, 2008

[Mér] Jean-Yves Mérindol, "Nombres et algèbre", EDP Sciences, 2006

[RDO] E. Ramis, C. Deschamps, J. Odoux, "Cours de mathématiques spéciales - Algèbre 1", Masson, 1992

[Rom] Jean-Etienne Rombaldi, "Eléments d'analyse réelle", EDP Sciences, 2004

[Tau] Patrice Tauvel, "Corps commutatifs et théorie de Galois", Calvage & Mounet, 2008

[Zav] Maxime Zavidovique, "Un max de maths", Calvage & Mounet, 2013

Théorème de Chevalley-Warning

Leçons : 120, 121, 123, 142, 144, 170, 180, 190.

Références :

Un Max de maths p.32,
M. Zavidovique,
Calvage et Mounet, 2013.

Cours d'arithmétique p.12,
J-P. Serre,
Hermann, 1998.

Olympiades internationales de mathématiques p.87,
P. Bourgade,
Cassini, 2005.

Le développement

Soient p un nombre premier et m, n deux entiers naturels non nuls.On pose $q = p^n$ et on considère A un ensemble et $(f_a)_{a\in A}$ une famille de polynômes de $k[X_1, \dots, X_m]$ telle que

$$\sum_{a\in A} \deg f_a < m.$$

Soit $Z(f_a : a \in A)$ l'ensemble des racines communes aux polynômes f_a. L'objectif de ce développement est d'établir un résultat concernant le cardinal de $Z(f_a : a \in A)$.

Dans toute la suite, on note pour tout polynôme $P \in \mathbb{F}_q[X_1, \dots, X_m]$

$$S(P) = \sum_{x\in\mathbb{F}_q^m} P(x).$$

Pour commencer, on a besoin de démontrer le lemme suivant sur les sommes de puissances dans les corps finis.

Lemme.
Soit u un entier naturel. Alors :

$$\sum_{x\in\mathbb{F}_q} x^u = \begin{cases} -1 & \text{si } u \geq 1 \text{ et } q-1 \text{ divise } u \\ 0 & \text{sinon} \end{cases}.$$

Démonstration.
Si u est nul, le résultat est immédiat tandis que si u est non nul et divisible par $q-1$, alors

$$S(X^u) = 0^u + \sum_{x\in\mathbb{F}_q^*} 1 = q - 1 = -1.$$

Enfin, si u n'est pas divisible par $q-1$, sachant que $\mathbb{F}_q^*$ est cyclique, il existe $y \in \mathbb{F}_q^*$ tel que y^u soit différent de 1. On a alors :

$$S(X^u) = \sum_{x\in\mathbb{F}_q^*} x^u = \sum_{x\in\mathbb{F}_q^*} (yx)^u = y^u S(X^u).$$

Comme y^u est distinct de 1, il s'ensuit que $S(X^u) = 0$. □

Théorème (Chevalley-Warning).

$$\#Z(f_a : a \in A) \equiv 0 \mod (p).$$

Démonstration.
Considérons le polynôme

$$P(X_1,\dots,X_m)=\prod_{a\in A}(1-f_a^{q-1}(X_1,\dots,X_m)).$$

Remarquons dans un premier temps que P est la fonction caractéristique de $Z(f_a : a\in A)$:

- Si $x\in k^m$ vérifie $f_a(x)=0$ pour tout $a\in A$, alors $P(x)=1$.
- Si $x\in k^m$ n'est pas un élément de $Z(f_a : a\in A)$, il existe $a\in A$ tel que $f_a(x)$ ne vaut pas 0, alors d'après le théorème de Lagrange, $f_a(x)^{q-1}=1$ et donc $P(x)=0$.

On en déduit alors que :

$$S(P)=\sum_{x\in Z(F_a:a\in A)}1+\sum_{x\notin Z(f_a:a\in A)}0\equiv \#Z(f_a : a\in A) \mod (p).$$

Par hypothèse sur les degrés des polynômes f_a, il vient que $\deg P < m(q-1)$. On peut donc écrire

$$P=\sum_{|u|<m(q-1)}\alpha_u X^u,$$

où les α_u sont des éléments de k. A partir de là :

$$S(P)=\sum_{x\in\mathbb{F}_q^m}\sum_{|u|<m(q-1)}\alpha_u x^u=\sum_{|u|<m(q-1)}\alpha_u S(X^u),$$

avec

$$\forall u\in\mathbb{F}_q^m : S(X^u)=\sum_{(x_1,\dots,x_m)\in\mathbb{F}_q^m}x_1^{u_1}\dots x_m^{u_m}=\left(\sum_{x_1\in\mathbb{F}_q}x_1^{u_1}\right)\dots\left(\sum_{x_m\in\mathbb{F}_q^{u_m}}x_m^{u_m}\right)=\prod_{i=1}^{m}S(X^{u_i}).$$

Or, si $|u|<m(q-1)$, il existe $i\in[\![1,m]\!]$ tel que $u_i<q-1$ donc d'après le lemme précédent, $S(X^{u_i})=0$ ce qui entraîne que $S(P)=0$ et le résultat s'ensuit. □

A présent, on utilise le théorème de Chevalley-Warning pour démontrer le théorème d'arithmétique d'Erdös-Gizburg-Ziv.

Théorème (Erdös-Gizburg-Ziv).
Soit n un entier naturel non nul. Alors parmi $2n-1$ entiers $a_1,\dots,a_{2n-1}$, on peut en trouver n dont la somme est divisible par n.

Démonstration.
Notons EGZ l'ensemble des entiers naturels vérifiant la propriété énoncée dans le théorème précédent. L'objectif est de montrer que $EGZ=\mathbb{N}^*$.

Soit p un nombre premier. Montrons que p est élément de EGZ. Soient pour cela $a_1,\dots,a_{2p-1}$ des entiers. Considérons les deux polynômes de $\mathbb{F}_p[X]$ suivants :

$$P_1(X_1,\dots,X_{2p-1})=\sum_{k=1}^{2p-1}X_k^{p-1},$$

$$P_2(X_1,\dots,X_{2p-1})=\sum_{k=1}^{2p-1}a_iX_k^{p-1}.$$

Ces deux polynômes vérifient $\deg P_1+\deg P_2=2p-2<2p-1$ et ont $(0,\dots,0)$ pour racine commune donc d'après le théorème de Chevalley-Warning, ils possèdent une racine commune non nulle $(x_1,\dots,x_{2p-1})$. D'après le théorème de Lagrange, pour tout x de $\mathbb{F}_p$, $x^{p-1}=1$ si est seulement si x est non nul donc en notant W l'ensemble des indices i pour lesquels x_i est non nul, il vient

$$P_1(x_1,\dots,x_{2p-1})=\sum_{i\in W}x_i^{p-1}=|W|=0.$$

Ainsi, $|W|$ est un entier divisible par p vérifiant $1 \leq |W| \leq 2p-1$ donc $|W| = p$ et on note $W = \{i_1, \ldots, i_p\}$. Vient ensuite

$$P_2(x_1, \ldots, x_{2p-1}) = \sum_{j=1}^{p} a_{i_j} = 0,$$

donc p divise $a_{i_1} + \ldots + a_{i_p}$ et le résultat est démontré.

Montrons à présent que EGZ est stable par multiplication. D'après le théorème fondamental de l'arithmétique, la démonstration sera achevée. Soient donc m et n deux éléments de EGZ. Considérons $a_1, \ldots, a_{2mn-1}$ des entiers. Etant donné que $n \in$ EGZ, il existe $I_1 \subset \{1, \ldots, 2mn-1\}$ de cardinal n tel que

$$\sum_{i \in I_1} a_i \equiv 0 \mod (n).$$

De même, il existe $I_2 \subset \{1, \ldots, 2mn-1\} \setminus I_1$ de cardinal n tel que

$$\sum_{i \in I_2} a_i \equiv 0 \mod (n).$$

On termine ce procédé après avoir construit l'ensemble d'indices I_{2m-1} car au bout de $2m-2$ étapes, il reste $2nm - 1 - (2m-2)n = 2n-1$ entiers. Pour tout $j \in \{1, \ldots, 2m-1\}$, on considère l'entier c_j défini par

$$\sum_{i \in I_j} a_i = c_j n.$$

Alors comme m est un élément de EGZ, on peut considérer $J \subset \{1, \ldots 2m-1\}$ de cardinal m tel que

$$\sum_{j \in J} c_j \equiv 0 \mod (m).$$

A partir de là :

$$\sum_{j \in J} \sum_{i \in I} a_i = n \left(\sum_{j \in J} c_j \right) \equiv 0 \mod (mn)$$

ce qui termine la démonstration. □

Pour information

Il faut savoir que la quantité $2n-1$ dans le théorème d'Erdös-Gizburg-Ziv est incompressible comme le montre l'exemple constitué de $n-1$ "0" et $n-1$ "1".

Il existe une autre méthode plus combinatoire pour démontrer que les nombres premiers sont éléments de EGZ. Etant donnés p un nombre premier et $a_1, \ldots a_{2p-1}$ des entiers, on considère pour tout $J \subset \{1, \ldots, 2p-1\}$ la somme $S_J = \sum_{i \in J} x_i$. L'idée est alors de calculer de deux manières différentes la quantité

$$\Sigma = \sum_{J \subset \{1, \ldots, 2p-1\} \,:\, \#J = p} S_J^{p-1}.$$

Tout d'abord, S_J^{p-1} est la somme de divers monômes de degré $p-1$ faisant intervenir k facteurs $(1 \leq k \leq p-1)$ que l'on peut écrire sous la forme $\lambda x_{i_1}^{a_{i_1}} \ldots x_{i_k}^{a_{i_k}}$. Ce type de monôme se retrouve, avec le même coefficient, dans le développement de S_J pour $\binom{2p-1-k}{p-k}$ ensembles J distincts : il suffit d'avoir pour J un ensemble contenant $i_1, \ldots, i_k$ puis de choisir les $p-k$ indices restants dans les $2p-1-k$ indices disponibles. Ainsi, après le développement complet de Σ, tout monôme est un multiple de $\binom{2p-1-k}{p-k}$ donc est divisible par p. L'entier Σ est donc nul dans $\mathbb{F}_p$.

D'autre part, si aucun des S_J n'était divisible par p, on aurait pour tout J, $S_J^{p-1} \equiv 1 \mod (p)$ et Σ est non nul modulo p. Ceci constitue une contradiction avec le paragraphe précédent donc il existe J de cardinal p tel que $S_J \equiv 0 \mod (p)$.

Méthode de Newton pour les polynômes

Leçons : 144, 218, 223, 226, 232.

Référence :

Exercices de mathématiques pour l'agrégation - Analyse 2 p.204,
A. Chambert-Loir et S. Fermigier,
Masson, 1995.

Le développement

On se propose dans ce développement de présenter la méthode de Newton pour l'approximation des racines réelles pour les polynômes scindés sur $\mathbb{R}$. Comme $\mathbb{R}$ est un corps infini, on se permet dans toute la suite de confondre polynôme et fonction polynomiale associée.

Soient $a_1, \dots, a_r$ des réels distincts ordonnés selon les indices et $m_1, \dots, m_r$ des entiers naturels non nuls. Considérons le polynôme $P(X) = \prod_{i=1}^{m} (X - a_i)^{m_i}$ et la suite réelle (x_n) définie par

$$\begin{cases} x_0 > a_r, \\ \forall n \geq 0 : x_{n+1} = x_n - \dfrac{P(x_n)}{P'(x_n)}. \end{cases}$$

On sera par la suite amené à utiliser la décomposition en éléments simples de P'/P, donnée par

$$\frac{P'(X)}{P(X)} = \sum_{i=1}^{r} \frac{m_i}{X - a_i}.$$

Tout d'abord, on étudie la fonction qui donne naissance à la suite récurrente (x_n).

Lemme.
La fonction définie par

$$f : \begin{array}{ccc}]a_r, +\infty[& \to & \mathbb{R} \\ x & \mapsto & x - \dfrac{P(x)}{P'(x)} \end{array}$$

se prolonge par continuité en a_r par $f(a_r) = a_r$ et même, admet un prolongement de classe C^1 sur $[a_r, +\infty[$ donné par $f'(a_r) = 1 - \frac{1}{m_r}$. De plus, f est strictement croissante sur $[a_r, +\infty[$.

Démonstration.
Remarquons que d'après le théorème de Gauss-Lucas, les racines de P' sont dans l'enveloppe convexe des racines de P, *ie* dans $[a_1, a_r]$ et ainsi, la fonction f est bien définie. D'après la décomposition en éléments simple de P'/P, on obtient ensuite :

$$\forall x > a_r : f(x) = x - \left(\sum_{i=1}^{r} \frac{m_i}{x - a_i} \right)^{-1},$$

et le prolongement par continuité de f annoncé est immédiat. f étant une somme de fonctions dérivables sur $]a_r, +\infty[$, elle est elle-même dérivable sur cet intervalle avec :

$$\forall x > a_r : f'(x) = \frac{P(x)P''(x)}{(P'(x))^2} = \frac{P(x)P''(x)}{(P(x))^2} \cdot \left(\frac{P(x)}{P'(x)} \right)^2.$$

Or, en dérivant la décomposition en éléments simples de P'/P sur $]a_r, +\infty[$, ce qui reste possible, on obtient,

$$\forall x > a_r : \frac{P''(x)P(x) - (P'(x))^2}{(P(x))^2} = -\sum_{i=1}^{r} \frac{m_i}{(x - a_i)^2},$$

ce qui conduit à l'égalité suivante :

$$\forall x > a_r : f'(x) = 1 - \left(\sum_{i=1}^{r} \frac{m_i}{x - a_i}\right)^{-2} \left(\sum_{i=1}^{r} \frac{m_i}{(x - a_i)^2}\right).$$

On en déduit que $\lim_{x \to a_r} f'(x) = 1 - \frac{1}{m_r}$ et f admet bien un prolongement $\mathcal{C}^1$ sur $[a_r, +\infty[$. Enfin, d'après le théorème de Gauss-Lucas, les racines de P', puis celles de P'' sont dans l'enveloppe convexe des racines de P, *ie* dans $[a_1, a_r]$ ce qui montre que P', P' et P'' ont un signe constant sur $[a_r, +\infty[$ d'après le théorème des valeurs intermédiaires (ce sont des fonctions continues). Or P est unitaire donc P' et P'' ont un coefficient dominant positif, ce qui entraîne que f' est positive sur $[a_r, +\infty[$ et ainsi, f croit strictement sur cet intervalle. □

On pourrait montrer de la même façon que f admet un prolongement de classe $\mathcal{C}^2$ en a_r.
On va à présent démontrer que la suite (x_n) est bien définie et qu'elle converge vers la plus grande racine de P.

Proposition.
La suite (x_n) est bien définie, décroit strictement et converge vers a_r.

Démonstration.
D'après la proposition précédente, l'intervalle $]a_r, +\infty[$ est stable par f donc (x_n) est bien définie. Etant donné que $x_0 > a_r$ et que la fonction f est strictement croissante sur $[a_r, +\infty[$, il s'ensuit par récurrence immédiate que $x_n > a_r$ pour tout entier naturel n. De plus, on obtient à partir de la décomposition en éléments simples de P'/P que

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \left(\sum_{i=1}^{r} \frac{m_i}{x_n - a_i}\right)^{-1}.$$

Cela entraine la décroissance stricte de la suite (x_n). Comme elle est de plus minorée, le théorème de la limite monotone donne la convergence de (x_n). Par continuité de f, sa limite est un réel de $[a_r, +\infty[$ qui annule P/P', *ie* vaut a_r. □

Il s'agit à présent d'étudier la vitesse de convergence de convergence de la suite (x_n). Deux cas se présentent suivant la valeur de m_r.

Proposition.
Si a_r est une racine simple de P, alors pour tout $c > 0$, $|x_n - a_r| \underset{n \to +\infty}{=} o(c^n)$.

Démonstration.
Soit n un entier naturel. Sachant que f est continue sur $[a_r, x_n]$ et dérivable sur $]a_r, x_n[$, l'égalité des accroissements finis donne l'existence de $y_n \in]a_r, x_n[$ tel que

$$x_{n+1} - a_r = f(x_n) - f(a_r) = (x_n - a_r) f'(y_n).$$

Comme (x_n) converge vers a_r et que f' est continue, la caractérisation séquentielle de la continuité entraine la convergence de la suite de terme général $f'(y_n)$ vers $f'(a_r)$ qui est nulle par hypothèse et en vertu du lemme préliminaire. Ainsi :

$$\forall c > 0, \exists N \in \mathbb{N}, \forall n \geq N : |f'(y_n)| < c.$$

On en déduit alors :

$$\forall c > 0, \exists N \in \mathbb{N}, \forall n \geq N : |x_{n+1} - a_r| \leq c|x_n - a_r|.$$

On a donc démontré que pour tout $c > 0$, $|x_n - a_r| \underset{n \to +\infty}{=} \mathcal{O}((c/2)^n) = o(c^n)$. □

Proposition.
Si a_r est une racine d'ordre au moins 2 de P, alors il existe $c > 0$ tel que

$$|x_n - a_r| \underset{n \to +\infty}{\sim} c\left(1 - \frac{1}{m_r}\right)^n.$$

Démonstration.
Soit n un entier naturel. Tout comme dans la démonstration précédente, on appliquer l'égalité des accroissements finis à la fonction f sur l'intervalle $[a_r, x_n]$ ce qui entraîne l'existence de $y_n \in]a_r, x_n[$ tel que

$$x_{n+1} - a_r = (x_n - a_r)f'(y_n).$$

Ici encore on invoque la caractérisation séquentielle de la continuité avec f' et la suite (y_n) pour justifier que la suite de terme général $f'(y_n)$ converge vers $f'(a_r) = 1 - \frac{1}{m_r}$ qui est un réel compris strictement entre 0 et 1 par hypothèse, ce qui par ailleurs montre que $\ln f'(a_r)$ est un réel non nul. De plus, on a déjà remarqué que la suite (x_n) est strictement minorée par a_r donc les quantités $x_{n+1} - a_r$ et $x_n - a_r$ sont strictement positives. On peut donc passer au logarithme dans l'égalité précédente, ce qui amène

$$\ln(x_{n+1} - a_r) - \ln(x_n - a_r) = \ln f'(y_n) \underset{n\to+\infty}{\to} \ln f'(a_r).$$

Le théorème de Césaro donne alors :

$$\ln(x_n - a_r) \underset{n\to+\infty}{\sim} n \ln\left(1 - \frac{1}{m_r}\right).$$

Redonnons nous un entier naturel n. f est de classe $\mathcal{C}^1$ sur $[a_r, x_n]$ et deux fois dérivables sur $]a_r, x_n[$ donc d'après l'égalité de Taylor-Lagrange, il existe $z_n \in]a_r, x_n[$ tel que

$$x_{n+1} - a_r = f'(a_r)(x_n - a_r) + \frac{f''(z_n)}{2}(x_n - a_r)^2.$$

Par continuité de f'' sur $]a_r, +\infty[$ et la convergence de (z_n) vers a_r, la suite de terme général $f''(z_n)$ est bornée car convergente par caractérisation séquentielle de la continuité et l'égalité précédente nous montre que

$$\frac{x_{n+1} - a_r}{f'(a_r)(x_n - a_r)} - 1 \underset{n\to+\infty}{=} \mathcal{O}(x_n - a_r).$$

De plus, l'équivalent précédent nous montre que si $f'(a_r) < c < 1$, alors $|x_n - a_r| \underset{n\to+\infty}{=} \mathcal{O}(c^n)$ et ainsi, la série de terme général

$$\ln(x_{n+1} - a_r) - \ln(x_n - a_r) - \ln f'(a_r) = \ln\left(\frac{x_{n+1} - a_r}{f'(a_r)(x_n - a_r)}\right) \underset{n\to+\infty}{=} \mathcal{O}(c^n).$$

converge. Par conséquent, la suite de terme général $\ln(x_n - a_r) - n \ln f'(a_r)$ converge vers un certain réel λ. Finalement :

$$x_n - a_r \underset{n\to+\infty}{\sim} e^{\lambda}\left(1 - \frac{1}{m_r}\right)^n.$$

□

Pour information

Il existe un moyen de considérer un $x_0 > a_r$ sans avoir aucune idée de la valeur de a_r. En effet si on pose $P(X) = X^n + \alpha_0 X^{n-1} + \ldots + \alpha_n$, alors pour toute racine a de P :

$$|a|^n = \left|\sum_{i=1}^{n-1} \alpha_i a^{n-1-i}\right| \leq \sum_{i=1}^{n-1} |\alpha_i||a^{n-1-i}|,$$

ce qui entraîne

$$a \leq \max\left(1, \sum_{i=1}^{n} |\alpha_i|\right).$$

Dès le départ, on peut diviser P par le PGCD de P et de P' pour que a_r soit une racine simple, ce qui accélère la vitesse de convergence. Pour approcher les autres racines de P, on applique alors la méthode de Newton au polynôme $P/(X - a_r)$.

Borne de Bezout

Leçons : 142, 143, 144.

Références :

Mathématiques L3 - Algèbre p.592,
A. Szpirglas,
Pearson Education, 2009.

Nombres et algèbre p.386
J-Y. Mérindol,
EDP Sciences, 2006.

Cours de Calcul Formel - Algorithmes fondamentaux p.157,
P. Saux-Picart
Ellipses, 1999.

Le développement

Soit k un corps commutatif. On se propose dans ce développement de majorer le nombre de points d'intersection de deux courbes planes à valeurs dans k.

Théorème.
Soient A et B deux polynômes de $k[X,Y]$ de degrés totaux respectifs m et n. Si A et B sont premiers entre eux et que k est de cardinal infini, alors $\#Z(A)\cap Z(B) \leq mn$.

Démonstration.
Si A et B n'ont pas de racine commune, le résultat est évident et dans toute la suite, on suppose que $Z(A)\cap Z(B)$ est non vide.

On note $R_Y = \mathrm{Res}_Y(A,B)$ et $R_X = \mathrm{Res}_X(A,B)$. Pour tout $(x,y) \in Z(A)\cap Z(B)$, il vient $R_Y(x) = R_X(y) = 0$. Comme A et B sont premiers entre eux, R_Y est un polynôme non nul de $k[X]$ et il a au plus $\deg R_Y$ racines. Ainsi, il y a au plus $\deg R_Y$ possibilités pour l'abscisse d'un point de $Z(A)\cap Z(B)$. De la même façon, il y a au plus $\deg R_X$ possibilités pour l'ordonnées de ces points. On en déduit que

$$\#Z(A)\cap Z(B) \leq \deg R_X \deg R_Y.$$

Notons à présent

$$A(X,Y) = \sum_{k=0}^{p} a_k(X)Y^k \quad B(X,Y) = \sum_{k=0}^{q} b_k(X)Y^k,$$

où $\deg a_k \leq m-k$, $\deg b_k \leq n-k$ et a_p, b_q sont deux éléments non nuls de $k[X]$. Alors

$$R_Y = \det(\mathrm{Syl}_Y(A,B)) = \begin{vmatrix} a_p & \dots & \dots & \dots & a_0 & & \\ & \ddots & & & & \ddots & \\ & & a_p & \dots & \dots & \dots & a_0 \\ b_q & \dots & \dots & b_0 & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & b_q & \dots & \dots & b_0 \end{vmatrix}.$$

On note $\mathrm{Syl}_Y(A,B) = (c_{i,j})$. Alors

$$\forall i \in [\![1,q]\!] : \quad \deg c_{i,j} = \begin{cases} \deg a_{p-(j-i)} & \text{si } i \leq j \leq p+i \\ 0 & \text{sinon} \end{cases} \leq m-p+j-i,$$

$$\forall i \in [\![q+1,q+p]\!] : \quad \deg c_{i,j} = \begin{cases} \deg b_{i-j} & \text{si } i-q \leq j \leq i \\ 0 & \text{sinon} \end{cases} \leq n-i+j.$$

On en déduit :

$$\forall \sigma \in \mathfrak{S}_{p+q} : \deg\left(\varepsilon(\sigma)\prod_{i=1}^{p+q} c_{i,\sigma(i)}\right) = \sum_{i=1}^{p+q} \deg c_{i,\sigma(i)} \leq \sum_{i=1}^{q}(m-p+\sigma(i)-i) + \sum_{i=q+1}^{q+p}(n-i+\sigma(i))$$

$$= mq - pq + np = mn + (m-p)(q-n) \leq mn,$$

et avec la formule du déterminant, $\deg R_Y \leq mn$. On obtient de même $\deg R_X \leq mn$ puis

$$\#\,\mathrm{Z}(A) \cap \mathrm{Z}(B) \leq (mn)^2.$$

Pour achever la démonstration, il ne reste plus qu'à affiner la majoration précédente. Dans ce but, on numérote les éléments de $\mathrm{Z}(A) \cap \mathrm{Z}(B) = \{(x_i, y_i) : i \in [\![1,r]\!]\}$ et on pose

$$\mathcal{E} = \left\{ \frac{x_i - x_j}{y_j - y_i} : y_j \neq y_i, i, j \in [\![1,r]\!] \right\}.$$

Alors $\#\mathcal{E} < +\infty$ et k^* est infini donc on peut considérer $u \in k^* \setminus \mathcal{E}$. Remarquons le fait suivant :

$$\forall i, j \in [\![1,r]\!] : x_i - x_j \neq u(y_j - y_i) \Leftrightarrow x_i + uy_i \neq x_j + uy_j.$$

On effectue alors le changement de variables suivant :

$$\begin{cases} X' = X + uY \\ Y' = Y \end{cases} \quad \begin{cases} \tilde{A}(X',Y') = A(X,Y) \\ \tilde{B}(X',Y') = B(X,Y) \end{cases}.$$

Soit alors la fonction

$$\varphi : \begin{array}{ccc} \mathrm{Z}(A) \cap \mathrm{Z}(B) & \to & \mathrm{Z}(\mathrm{Res}_{Y'}(\tilde{A},\tilde{B})) \\ (x,y) & \mapsto & x + uy \end{array}.$$

La fonction φ est bien définie car si $(x,y) \in \mathrm{Z}(A) \cap \mathrm{Z}(B)$, alors $A(x,y) = B(x,y) = 0$ puis $\tilde{A}(x+uy,y) = \tilde{B}(x+uy,y) = 0$ ce qui se réécrit $\mathrm{Res}_{Y'}(\tilde{A},\tilde{B})(x+uy) = 0$. De plus, φ est injective puisque u n'est pas un élément de $\mathcal{E}$ et d'après la remarque faite après l'introduction de u. Ainsi :

$$\#\,\mathrm{Z}(A) \cap \mathrm{Z}(B) \leq \#\,\mathrm{Z}(\mathrm{Res}_{Y'}(\tilde{A},\tilde{B})) \leq \deg \mathrm{Res}_{Y'}(\tilde{A},\tilde{B}) \leq mn$$

d'après le point précédent, ce qui achève la démonstration.

□