144 - RACINES DE POLYNÔMES. FONCTIONS SYMÉTRIQUES ÉLÉMENTAIRES. EXEMPLES ET APPLICATIONS

I) Les polynômes algébriques et leur racines

1) Relations degré - racines

Définition 1 : Soit A un anneau, $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ et $b \in A$. On dit que b est racine de P si $\sum_{i=0} a_i b^i = 0$

Proposition 2 : Soit $P \in A[X]$, $b \in A$ (A est un anneau) b est racine de P ssi $X - b \mid P$

Corollaire 3 : Si A est un anneau intègre, tout polynôme non nul P possède au plus $\deg P$ racines de $A[X]$

Contre-exemple 4 : $-2X$ possède 0 et 2 comme racines dans $\mathbb{Z}/4\mathbb{Z}$

- Soit $A, B \in M_n(\mathbb{C})$ tel que $AB = 0$. Alors λB ($\lambda \in \mathbb{C}$) est racine de AX.

Application 5 : par $n+1$ points distincts de $\mathbb{R}$, passe un unique polynôme de degré au plus n (interpolation de Lagrange)

Définition 6 : Soit $P \in A[X]$, $b \in A$, $m \geq 0$. On dit que b est racine de multiplicité m de P si $(X-b)^m \mid P$ et $(X-b)^{m+1} \nmid P$.
Si $m = 1$, la racine est dite simple

Proposition 7 : Soit K un corps de caractéristique nulle, $P \in K[X]$. Alors b est racine de multiplicité m de P ssi $\forall i \in [\![1, m-1]\!]$ $P^{(i)}(b) = 0$ et $P^{(m)}(b) \neq 0$

Contre-exemple 8 : 1 est racine de multiplicité p de $(X-1)^p \in \mathbb{Z}_p\mathbb{Z}$, mais $P' = 0$ (p est premier)

Application 9 : - diagonalisabilité des endomorphismes d'espace vectoriel possédant un polynôme annulateur scindé à racines simples

2) Relations coefficients - racines

Définition 10 : Soit $P = \sum_{i=0}^{n} a_i X^{n-i} \in K[X]$, admettant $x_1, \dots, x_n$ racines (avec multiplicité). La p-ième fonction symétrique élémentaire est $\sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} x_{i_1} \cdots x_{i_p}$

Proposition 11 : $\sigma_p = (-1)^p \dfrac{a_p}{a_0}$, pour tout $p = 1, \dots, n$

Application 12 : (Kronecker) Soit $P \in \mathbb{Z}[X]$ unitaire, de racines complexes de module ≤ 1, alors P est produit de polynômes cyclotomiques et d'une puissance de X. | DEV 1

Application 13 : résolution de $\begin{cases} x+y+z = 1 \\ 1/x + 1/y + 1/z = 1 \\ xyz = -4 \end{cases}$

Définition 14 : Soit A un anneau. Soit $P \in A[X_1, \dots, X_n]$. On dit que P est symétrique si $\forall \sigma \in \mathfrak{S}_n$ $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$

Exemple 15 : les polynômes symétriques élémentaires $\Sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \cdots X_{i_p}$ sont symétriques ($p \in [\![1, n]\!]$)

Théorème 16 : Soit A un anneau commutatif. Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique. Alors il existe un unique $Q \in A[X_1, \dots, X_n]$ tel que $P = Q(\Sigma_1, \dots, \Sigma_n)$

Exemple 17 : $P = \sum_{\sigma = (123)} X_{\sigma(1)}^2 (X_{\sigma(2)} + X_{\sigma(3)}) = \Sigma_1 \Sigma_2 - 3 \Sigma_3$

Exemple 18 : Soit $P \in \mathbb{Z}[X]$ unitaire, de racines (complexes) $z_1, \dots, z_n$. Soit $Q \in \mathbb{Z}[X_1, \dots, X_n]$ symétrique. Alors $Q(z_1, \dots, z_n) \in \mathbb{Z}$

Application 19 : (d'Alembert-Gauss). $\mathbb{C}$ est algébriquement clos.

Définition 20 (somme de Newton) On définit la k-ième somme de Newton par $S_k = \sum_{i=1}^{n} x_i^k$.

Proposition 21 (relation de Newton). $\forall k \le n$ $S_k = -\sum_{i=1}^{k} (-1)^i \Sigma_i S_{k-i}$

Pour $k \geq n$ $\sum_{i=0}^{n} (-1)^i \Sigma_i S_{k-i} = 0$

Application 22 : Soit $A \in M_n(K)$ avec K de caractéristique nulle ou de caractéristique strictement plus grande que n, alors A est nilpotente ssi $\forall k = 1, \dots, n$ $\mathrm{Trace}(A^k) = 0$.

II) Adjonction de racines

1) Polynôme irréductible et corps de rupture

Définition 23 : $P \in K[X]$ est irréductible si ($P = P_1P_2 \Rightarrow P_1$ ou P_2 constant) $P_1, P_2 \in K[X]$

Remarque 24 : - un polynôme irréductible de degré > 1 n'a pas de racines (donc X^3+X+1 est réductible sur $\mathbb{F}_{3^k}$, $k \geq 1$)

Déf/Théorème 25 : Soit $P \in K[X]$ irréductible il existe un unique (à iso près) corps de rupture de P, i.e. une extension $L = K(x)$ de K avec $x \in K$ tel que $P(x) = 0$

Exemple 26 : $\mathbb{Q}(\sqrt[3]{2})$ est le corps de rupture de X^3-2 sur $\mathbb{Q}$.

Application 27 : Soit $P \in k[X]$ irréductible de degré n et K une extension de k de degré (i.e. de dimension en tant que k-ev) m, premier avec n. Alors P est irréductible sur K.

Contre-exemple 28 : X^4+1 est irréductible sur $\mathbb{Q}$, mais est réductible dans $\mathbb{Q}(i)$ (extension de degré 2 de $\mathbb{Q}$) : $X^4+1 = (X^2+i)(X^2-i)$

Théorème 29 : $\Phi_n = \prod_{\substack{k=1 \\ k\wedge n=1}}^{n} (X - e^{\frac{2ik\pi}{n}}) \in \mathbb{Z}[X]$ et est irréductible sur $\mathbb{Q}$

DEV 2

Proposition 30 : Soit $P \in k[X]$ non nul de degré n. Alors P est irréductible sur k ssi P n'a pas de racines dans les extensions K de k de degré $\leq n/2$

Exemple 31 : X^4+1 est réductible sur $\mathbb{Z}/p\mathbb{Z}$, pour tout p premier.

2) Corps de décomposition

Déf/Théorème 32 : Soit $P \in K[X]$, il existe un unique (à iso près) corps de décomposition de P, i.e. une extension L de K tel que P soit scindé sur $L[X]$ et que L soit minimal pour cette propriété.

Exemple 33 : $\mathbb{Q}(\sqrt[3]{2}, j)$ est le corps de décomposition de X^3-2

Application 34. Soit p un nombre premier. Il existe un unique corps à p^n éléments, pour tout $n \in \mathbb{N}$. C'est le corps de décomposition de $X^{p^n}-X$

III) Localisation des racines dans $\mathbb{R}$ ou $\mathbb{C}$ de polynômes de $\mathbb{R}[X]$ ou $\mathbb{C}[X]$.

1) Méthodes d'analyse réelle

Lemme 35 (Cauchy) : Soit $P = X^n + \sum_{i=1}^{n} a_i X^{n-i}$, qui n'est pas un monôme et $Q = X^n - \sum_{i=1}^{n} |a_i| X^{n-i}$. Alors Q admet une unique racine $\alpha > 0$, qui est simple. Les autres racines de Q sont de module $\leq \alpha$. De plus, en notant ρ ... avec $z_1, \dots, z_n$ racines de P : $(2^{1/n}-1)\alpha \leq \rho \leq \alpha$

Proposition 36 : $\rho \leq \min\left(1 + \max_{i=1..n} |a_i|, \max\left(1, \sum_{i=1}^{n} |a_i|\right), 2\max_{i=1..n} |a_i|^{1/i}\right)$

Si $\forall i = 1, \dots, n$ $a_i \neq 0$, $\rho \leq \max_{i=1..n} \frac{|a_i|}{|a_{i-1}|}$

2) Matrices compagnons

Remarque 37 : avec les mêmes notations qu'en 35/36, l'inégalité $\rho \le \min(1+\max_i |a_i|, \max(1, \sum_{i=1}^{n} |a_i|))$ peut se démontrer en considérant la matrice compagnon associée à P et en appliquant le théorème des disques de Gershgorin

Lemme 38 (Schur) : toute matrice $A \in M_n(\mathbb{C})$ est trigonalisable en base orthonormée

Proposition 39 : Soit $P \in \mathbb{C}_n[X]$ de degré n. Pour tout $\varepsilon > 0$, $\exists \delta > 0$ $\forall Q \in \mathbb{C}_n[X]$, $\deg Q = n$, $\|P-Q\| \le \delta \Rightarrow Z(Q) \subset Z(P) + D(0,\varepsilon)$

($Z(Q) = \{$ racines complexes de $Q \}$)

Proposition 40 : Soit $P \in \mathbb{C}_n[X]$ de degré n. On suppose que P possède une racine λ de multiplicité $m_\lambda \ge 2$. Alors, $\forall \varepsilon > 0$ $\exists \delta > 0$ $\forall Q \in \mathbb{C}_n[X]$ $\deg Q = n$,
$(\|P-Q\| \le \delta) \Rightarrow \mathrm{card}(Z(Q) \cap B(\lambda, \varepsilon)) = m_\lambda$

3) Racines de P'

Proposition 41 (Gauss-Lucas). Soit $P \in \mathbb{C}[X]$. Les racines de P' sont contenues dans l'enveloppe convexe de celles de P.

Application 42. Soit $P = \prod_{i=1}^{n} (X - x_i)$ avec $x_1 < \dots < x_n$ des réels. En remplaçant x_k par un réel de $]x_k, x_{k+1}[$, toutes les racines de P' croissent

4) Méthodes d'analyse complexe

Proposition 43 (Rouché). Soit $P, S \in \mathbb{C}[X]$ et γ le bord d'un disque de $\mathbb{C}$ tel que $\forall z \in \gamma$ $|S(z)| < |P(z)|$ alors le nombre de zéros de P ~~dans~~ à l'intérieur de γ est égal à celui de $P+S$

Exemple 44 : $P(z) = 3z^{15} + 4z^8 + 6z^5 + 19z^4 + 3z + 2$ admet 4 zéros dans $D(0,1)$ et 11 dans $D(0,2) \setminus \overline{D}(0,1)$

Application 45 : Soit $P = X^n + \sum_{i=1}^{n} a_i X^{n-i} \in \mathbb{C}[X]$. Alors P admet n racines dans $D(0, 1 + \max_{i=1,\dots,n} |a_i|)$ (d'Alembert-Gauss)

5) Comptage du nombre de racines (Sturm)

Proposition 46 : Soit $P \in \mathbb{R}[X]$ et (S_i) définie par $S_0 = P$, $S_1 = P'$, $S_{i-1} = Q_i S_i - S_{i+1}$. Pour $x \in \mathbb{R}$, on note $V(x)$ le nombre de changements de signe dans $S_i(x)$. Soit $a < b$ non racines de P. Alors le nombre de racines réelles distinctes ~~de~~ de P dans $[a,b]$ est égal à $V(a) - V(b)$

Application 47 : méthode de Givens pour le calcul des valeurs propres de matrices tridiagonales

Proposition 48 (Sylvester) : Soit $P \in \mathbb{R}[X]$ de degré n et $A = (s_{i+j-2})$ avec s_k k-e somme de Newton associée aux racines complexes de P. Alors la signature de la forme quadratique canoniquement associée à A est $(n+2c, 2c)$ où n est le nombre de racines réelles distinctes de P, et $2c$ les racines distinctes, complexes, non réelles de P

Références : - Gourdon, algèbre - Tauvel, Cours d'Algèbre
- Perrin, Cours d'algèbre - Prasolov, Polynomials
- Queffélec, Analyse complexe et applications
- Ciarlet, Introduction à l'analyse numérique matricielle et optimisation

Suggestions : - algébriques (algébriquement clos)
- entiers algébriques et théorème de Burnside
(131 développements pour l'agrégation).