Leçon 144 : Racines d'un polynôme, fonctions symétriques élémentaires. Exemples et applications.

I. Définitions, premières propriétés

1) Racines d'un polynôme [GOU]

Déf 1 : soit $\mathbb{K}$ un corps commutatif, L une extension (éventuellement triviale) de $\mathbb{K}$, et $P \in \mathbb{K}[X]$. On dit que $a \in L$ est racine de P si $P(a)=0$

Prop 2 : Soit $a \in \mathbb{K}$, et $P \in \mathbb{K}[X]$; on a :
a racine de $P \Leftrightarrow (X-a)$ divise P.

Déf 3 : soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $k \in \mathbb{N}^*$; on dit que a est une racine d'ordre k de P si $\begin{cases} (X-a)^k \mid P \\ (X-a)^{k+1} \nmid P \end{cases}$

Prop 4 : Soit $\mathbb{K}$ corps de caractéristique nulle, $P \in \mathbb{K}[X] \setminus \{0\}$ et $a \in \mathbb{K}$
a est racine d'ordre k de P si et seulement si $\begin{cases} (i) \ \forall 0 \le i \le k-1, \ P^{(i)}(a)=0 \\ (ii) \ P^{(k)}(a) \neq 0 \end{cases}$

Ex 5 : ... $P = X^3 \in \mathbb{Z}/32\mathbb{Z}[X]$; 0 est racine d'ordre 3 et pourtant $P^{(3)}(0)=0$.

Prop 6 : Soit $P \in \mathbb{K}[X]$, $a_1, \dots, a_p \in \mathbb{K}$ des racines de P, 2 à 2 distinctes, d'ordres respectifs $k_1, \dots, k_p \in \mathbb{N}^*$; Alors :
$\exists Q \in \mathbb{K}[X]$, $\forall 1 \le i \le p$, $Q(a_i) \neq 0$ et $P(X) = \prod_{i=1}^{p} (X-a_i)^{k_i} \cdot Q(X)$

Rem 7 : Cela implique que le nombre de racines (comptées avec multiplicité) d'un polynôme est majoré par son degré.

Ex 8 : A nouveau, ce n'est plus vrai si $\mathbb{K}$ n'est pas un corps : $P = 4X \in \mathbb{Z}/8\mathbb{Z}$ a 3 racines distinctes, 0 et 2 et 4, et pourtant $\deg(P)=1$.

Application 9 : le groupe multiplicatif d'un corps fini est cyclique.

Théorème 10 : Soit $\mathbb{K}$ un corps infini, et $P \in \mathbb{K}[X]$ tel que $\forall x \in \mathbb{K}$, $P(x)=0$.
Alors $P=0$

Ex 11 : Ce n'est plus vrai dans un corps fini : par exemple, $P = X^p - X \in \mathbb{F}_p[X]$ s'annule en chaque point de $\mathbb{F}_p$, et pourtant $P \neq 0$.

Application 12 : * Si $\mathbb{K}$ est infini, on a bijection entre $\mathbb{K}[X]$ et l'ensemble des fonctions polynômes $\mathbb{K} \to \mathbb{K}$
* Unicité des polynômes de Tchebychev de 1ère espèce ($\cos n\theta = \cos(n\theta)$)

Déf 13 : $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$ si on peut écrire :
$P = \lambda \prod_{i=1}^{p} (X-a_i)^{k_i}$, $\lambda \in \mathbb{K}$, $\forall i \in [\![1,p]\!]$, $a_i \in \mathbb{K}$, $k_i \in \mathbb{N}^*$.

Déf 14 : $P \in \mathbb{K}[X]$ est dit irréductible dans $\mathbb{K}[X]$ si :
* $\deg P \ge 1$
* $P = QR \Rightarrow Q$ ou R est une constante non-nulle.

Prop 15 : (i) Tout polynôme de degré 1 est irréductible.
(ii) Un polynôme irréductible dans $\mathbb{K}$, de degré >1, n'admet pas de racines dans $\mathbb{K}$.

Rem 16 : si $\deg(P) \in [2,3]$, la réciproque de (ii) est vraie.

Ex 17 : * les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
* les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant négatif.
* Dans $\mathbb{Q}[X]$, il y a des irréductibles de tout degré ($X^n - 2$, $n \in \mathbb{N}^*$ par exemple)

2) Adjonction de racines : corps de rupture, corps de décomposition. [GOZ]

Pb : Comment construire une (ou des) racine(s) pour un polynôme irréductible de degré >1 ?

Déf 18 : soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ irréductible ; une extension $\mathbb{K} \hookrightarrow L$ de $\mathbb{K}$ est un corps de rupture de P sur $\mathbb{K}$ s'il existe $\alpha \in L$ tel que : $\begin{cases} P(\alpha)=0 \\ L = \mathbb{K}(\alpha) \end{cases}$

Thm 19 : Soit $P \in \mathbb{K}[X]$, irréductible. Alors il existe un corps de rupture de P sur $\mathbb{K}$, isomorphe à $\mathbb{K}[X]/(P)$

Ex 20 : * $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$ est un corps de rupture pour X^2+1 sur $\mathbb{R}$.
* $\mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}[X]/(X^2-3)$
* $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2+X+1)$

Déf 21 : Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$, et L une extension de $\mathbb{K}$. L est un corps de décomposition de P sur $\mathbb{K}$ si : (i) $\exists \alpha \in L$, $(a_1, \dots, a_p) \in L^p$ tq $P = \alpha \prod_{i=1}^{p} (X-a_i)$
(ii) $L = \mathbb{K}(a_1, \dots, a_p)$

Thm 22 : soit $P \in \mathbb{K}[X]$; il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près ; on le note $\mathrm{Dec}(P)$

Application 23 : Existence et unicité d'un corps fini de cardinal $q = p^n$, p premier, $n \in \mathbb{N}^*$.

Ex 24 : * $\mathbb{K} = \mathbb{Q}$, $P = X^3 - 2$: $\mathrm{Dec}(P) = \mathbb{Q}(\sqrt[3]{2}, j)$
* $\mathbb{K} = \mathbb{Q}$, $P = X^4 - 2$ $\mathrm{Dec}(P) = \mathbb{Q}(\sqrt{2}, i)$

II Polynômes symétriques, fonctions symétriques élémentaires - [GOZ]

On se place dans un anneau commutatif intègre $(A,+,\cdot)$.

On pose, pour $\sigma\in\mathfrak{S}_n$ et $P\in A[X_1,\dots,X_n]$, $\sigma\cdot P = P(X_{\sigma(1)},\dots,X_{\sigma(n)})$; cela définit une action du groupe $\mathfrak{S}_n$ sur $A[X_1,\dots,X_n]$.

Déf 25 : $P\in A[X_1,\dots,X_n]$ est dit symétrique, ssi, $\forall\sigma\in\mathfrak{S}_n$, $\sigma\cdot P = P$.

Ex 26 :
- $P=\prod_{i<j}(X_i-X_j)$ est un polynôme symétrique
- $\forall p\in\mathbb{N}$, $S_p=\sum_{i=1}^{n} X_i^p$ est un polynôme symétrique (Sommes de Newton)

Déf 27 : Les polynômes $\Sigma_1,\dots,\Sigma_n$, définis par $\forall i\in[\![1,n]\!]$, $\Sigma_i=\sum_{1\le k_1<\dots<k_i\le n} X_{k_1}\cdots X_{k_i}$, sont des polynômes symétriques, appelés fonctions symétriques élémentaires.

Thm 28 : (Structure des polynômes symétriques) Soit $P\in A[X_1,\dots,X_n]$ symétrique de degré p. Alors il existe un unique polynôme $Q\in A[X_1,\dots,X_n]$, de poids p, tel que
$$P(X_1,\dots,X_n)=Q(\Sigma_1,\dots,\Sigma_n)$$

Ex 29 : dans $A[X_1,X_2,X_3]$: $\cdot\ X_1^2(X_2+X_3)+X_2^2(X_1+X_3)+X_3^2(X_1+X_2) = \Sigma_1\Sigma_2-3\Sigma_3$
$\cdot\ X_1^2+X_2^2+X_3^2 = \Sigma_1^2-2\Sigma_2$

Rem 30 : La démonstration du théorème de structure nous donne un algorithme pour déterminer Q.

Application 31 : (Relations coefficients / racines) ; soit $P\in A[X]$, $(d_1,\dots,d_n)\in A^n$ tels que $P=\prod_{i=1}^{n}(X-d_i)$; alors si $P=X^n+a_{n-1}X^{n-1}+\dots+a_1X+a_0$, on a :
$$\forall i\in[\![1,n]\!],\ a_{n-i}=(-1)^i\Sigma_i(d_1,\dots,d_n)$$

Application 32 : soit $P\in A[X]$ unitaire, B un anneau c.u tel que P soit scindé sur B, $(d_1,\dots,d_n)\in B^n$ ses racines ; alors pour tout $F\in A[X_1,\dots,X_n]$, $F(d_1,\dots,d_n)\in A$.

[X-ENS 1] **Thm 33 (Kronecker) :** Soit $P\in\mathbb{Z}[X]$, unitaire, dont les racines complexes sont toutes de module inférieur ou égal à 1, et tel que $P(0)\neq 0$. Alors les racines de P sont des racines de l'unité.
[Développement]

Cor 34 : Les seuls polynômes unitaires irréductibles de $\mathbb{Z}[X]$ dont les racines (complexes) sont dans $\overline{D}(0,1)$ sont X et les polynômes cyclotomiques.

[X-ENS 1] **Prop 35 :** (Sommes de Newton) $\forall p\in\mathbb{N}^*$, $S_p=\sum_{i=1}^{n} X_i^p\in A[X_1,\dots,X_n]$ est un polynôme symétrique, et on a les relations :
(i) $\forall p\ge n$, $S_p-\Sigma_1S_{p-1}+\dots+(-1)^{n-1}\Sigma_{n-1}S_{p-n+1}+(-1)^n\Sigma_nS_{p-n}=0$
(ii) $\forall 1\le p\le n-1$, $S_p-\Sigma_1S_{p-1}+\dots+(-1)^{p-1}\Sigma_{p-1}S_1+(-1)^p\Sigma_p=0$

[X-ENS 1] **Application 36 :** soit $A\in\mathcal{M}_n(\mathbb{C})$, telle que $\forall k\in\mathbb{N}^*$, $\mathrm{Tr}(A^k)=0$; alors A est nilpotente.

[X-ENS 2] **Application 37 :** $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} x^k = \begin{cases} 0 \text{ si } k\not\equiv p-1 \\ -1 \text{ si } k\mid p-1 \end{cases}$

III Localisation des racines [MIG] - [CH-F]

1) Méthode de Newton pour les polynômes [CH-F]

Thm 38 : Soient $\lambda_1,\dots,\lambda_r\in\mathbb{R}$, $k_1,\dots,k_r\in\mathbb{N}^*$ $(r\ge 2)$ et $P=\prod_{i=1}^{r}(X-\lambda_i)^{k_i}$
soit $x_0>\lambda_r$; on pose, $\forall n\in\mathbb{N}$, $x_{n+1}=x_n-\dfrac{P(x_n)}{P'(x_n)}$.
Alors la suite $(x_n)_{n\in\mathbb{N}}$ décroit strictement, et $x_n\xrightarrow[n\to+\infty]{}\lambda_r$.

Rem 39 : Convergence locale de la méthode.

2) Localisation dans le cas réel. [MIG]

Prop 39 : Soit $P\in\mathbb{R}_n[X]$, $L\in\mathbb{R}$ tel que $\forall 0\le i\le n$, $P^{(i)}(L)\ge 0$. Alors toute racine réelle x de P vérifie $x\le L$ (Règle de Newton)

Prop 40 : (Règle de Lagrange Maclaurin)
Soit $P(X)=X^n+a_1X^{n-1}+\dots+a_n\in\mathbb{R}[X]$ avec $a_i\ge 0$ pour tout $i\in[\![1,n-1]\!]$
notons $A=\max\{-a_m,\dots,-a_n,0\}$
Alors toute racine réelle $x\in\mathbb{R}^+$ vérifie $x<1+A^{1/m}$

Prop 41 : (Règle de Descartes)
soit $P\in\mathbb{R}[X]$, $P=X^n+a_1X^{n-1}+\dots+a_mX^{n-m}-a_{m+1}X^{n-m-1}-\dots-a_n$
où $a_i\ge 0$ pour $1\le i\le m$.
Soit $c\in\mathbb{R}^+$ tel que $P(c)\ge 0$; alors toute racine réelle x de P vérifie $x\le c$.

Prop 42 : (règle de Cauchy)
Soient $a_{m_1},a_{m_2},\dots$, avec $m_1>m_2>\dots$, les coefficients strictement négatifs d'un polynôme $P\in\mathbb{R}[X]$.
Notons $P=X^n+a_1X^{n-1}+\dots+a_n$, et soit k le nombre de ses coefficients négatifs.
Alors toute racine réelle x du polynôme P vérifie :
$$x\le\max\left\{(k\,|a_{m_1}|)^{1/m_1},\dots,(k\,|a_{m_n}|)^{1/(n-m_n)}\right\}$$

Ex 43 : $P(X)=X^6-12X^4-2X^3+37X^2+10X-10$
Les règles précédentes donnent, respectivement, les bornes suivantes :
- Newton : $\sqrt{8}$
- Lagrange-Maclaurin : $1+\sqrt{37}$
- Cauchy : 6

3) Localisation dans le cas complexe. [G-A], [X-ENS 1]

Thm 44 : (Enestrom - Kakeya)

Soit $P(X) = a_0 X^{n-1} + \dots + a_{n-1}$, où les a_i sont tous >0. Alors, pour toute racine ζ de P (complexe), on a :

$$\min_{1 \le i \le n-1} \left\{ \frac{a_i}{a_{i-1}} \right\} \le |\zeta| \le \max_{1 \le i \le n-1} \left\{ \frac{a_i}{a_{i-1}} \right\}$$

Thm 45 (Ostrowsky)

(Avec les mêmes notations). On suppose que $\forall k \in \{k_1, \dots, k_m\}, \left| \frac{a_k}{a_{k-1}} \right| < \gamma$

Si $\operatorname{pgcd}(n, k_1, \dots, k_m) = 1$, alors $|\zeta| < \gamma$.

Thm 46 (Gauss-Lucas) Soit $P \in \mathbb{C}[X]$, non constant,

Alors les racines de P' sont dans l'enveloppe convexe de celles de P.

Application 47 : * $P \in \mathbb{C}[X]$ non constant, Δ une droite de $\mathbb{C}$, H_1 et H_2 les 2 demi-plans délimités par Δ (ouverts)

Si P' a une racine dans H_1, alors $P(H_2) = \mathbb{C}$

* soit $P \in \mathbb{C}[X]$, tel que P a 2 racines réelles distinctes et $P'' \mid P$. Alors, toutes les racines de P sont réelles et simples.)

IV Comptage de racines.

1) Continuité, régularité

Thm 48 : (continuité des racines d'un polynôme)

[G-O-V] Soit $P(X) = \prod_{i=1}^{n} (X - \lambda_i) \in \mathbb{C}[X]$; soit $(P_m)_{m \in \mathbb{N}}$ une suite de polynômes unitaires de degré n, tel que $P_m \xrightarrow[m \to +\infty]{} P$.

Alors on a, $\forall m \in \mathbb{N}$, $P_m = (X - \lambda_{1,m}) \dots (X - \lambda_{n,m})$ avec $\lambda_{i,m} \xrightarrow[m \to +\infty]{} \lambda_i$, $\forall i \in [\![1, n]\!]$

Thm 49 : (Régularité des racines simples)

[G-A] Soit $P \in \mathbb{R}_n[X]$, x_0 une racine simple de P. Alors x_0 dépend localement de P de manière C^∞.

Rem 50 : C'est une conséquence du thm des fonctions implicites.

Application 51 : On en déduit un résultat similaire sur la régularité des valeurs propres simples d'une matrice.

2) Comptage par l'analyse réelle.

Déf 52 : $P \in \mathbb{R}[X]$, $a < b \in \mathbb{R}$. On dit que $P_0 = P, P_1, \dots, P_r$ est une suite de Sturm pour P sur $[a,b]$ si :

(i) $P(a) P(b) \neq 0$

(ii) P_r ne s'annule pas sur $[a,b]$

(iii) si $c \in]a,b[$ est tq $P(c) = 0$, alors $P(x) P_1(x)$ est du signe de $x - c$ au voisinage de c.

(iv) si $c \in]a,b[$, et $P_j(c) = 0$ pour $j \in [\![1, r-1]\!]$, alors $P_{j-1}(c) P_{j+1}(c) < 0$.

Déf 53 : On définit le nombre de variations de signe de la suite au point x, noté $V(x)$ par : $V(x) = \#\{(i,j) / 0 \le i < j \le r,\ P_i(x) P_j(x) < 0 \text{ et } P_k(x) = 0 \ \forall\, i < k < j\}$

Thm 54 (Sturm) :

Soit $P \in \mathbb{R}[X]$, $a < b \in \mathbb{R}$. Si $P_0, \dots, P_r$ est une suite de Sturm pour P sur $[a,b]$, le nombre de racines distinctes de P sur $[a,b]$ est égal à $|V(b) - V(a)|$

Thm 55 (Budan-Fourier) :

Soient $P \in \mathbb{R}[X]$, $a < b \in \mathbb{R}$, tels que $P(a) P(b) \neq 0$; soit $V(a)$ le nombre de changement de signes dans la suite $P(a), P'(a), \dots, P^{(n)}(a)$. Alors le nombre de zéros de P dans $[a,b]$, comptés avec multiplicité, est de la forme :

$$V(a) - V(b) - 2m, \quad m \in \mathbb{N}$$

3) Utilisation des formes quadratiques

Déf 56 : Soit $P \in \mathbb{R}[X]$, $P = a_0 + a_1 X + \dots + a_n X^n$; on associe à P le polynôme symétrique

$$L(X,Y) = \frac{P(X)P'(Y) - P(Y)P'(X)}{X - Y} = \sum_{i,j=0}^{n-1} a_{ij} X^i Y^j \in \mathbb{R}[X,Y]$$

ainsi que la forme quadratique : $Q(P,u) = \sum_{i,j=0}^{n-1} a_{ij} u_i u_j$, où $u = (u_0, \dots, u_{n-1}) \in \mathbb{R}^n$

Thm 57 : Supposons P sans racines multiples. La forme quadratique $Q(P)$ a [DEVELOPPEMENT] pour signature $(p, r-p)$, avec p le nombre de racines réelles distinctes de P, et $2r$ le nombre de racines complexes distinctes.

4) Comptage par l'analyse complexe.

Thm 58 : (Résidus) : soit f holomorphe sur $D = U \setminus \{a_1, \dots, a_r\}$, γ un chemin continu fermé de D tel que $\operatorname{Is}(\gamma) = 0$, $\forall a \notin U$. Alors : $\frac{1}{2i\pi} \int_\gamma f(z)\,dz = \sum_{k=1}^{r} \operatorname{Is}(\gamma, a_k) \operatorname{Res}(f, a_k)$

Thm 59 (Rouché) Soit $P, Q \in \mathbb{C}[X]$, γ 1 lacet de $\mathbb{C}$ sans point double. Si on a : $\forall z \in \gamma$, $|P(z) - Q(z)| < |P(z)| + |Q(z)|$, alors P et Q ont même nombre de zéros à l'intérieur de γ

Exo : $X^3 - 5X^2 + X - 2$ a 3 racines dans $D(0,1)$.

Bibliographie :

- [Gou] : Gourdon, Algèbre
- [X-ENS ...] : Oraux X-ENS, tome n°..., Francinou-Gianella-Nicolas
- [O-A] : Objectif Agrég
- [M&G] : Mignotte, Mathématiques pour le calcul formel.
- [Gos] : Gozard, Théorie de Galois
- [C-F] ou [CH-F] : Chambert-Loir, Fermigier, Analyse pour l'agrégation.