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

Soit $(\mathbb{K}, +, .)$ un corps commutatif. Soit $P \in \mathbb{K}[X]$

1 Racines d'un polynôme

1.1 Racines et multiplicité

Définition 1 (ROM 362)**.** On dit que $\alpha \in \mathbb{K}$ est racine de P si $P(\alpha) = 0$.

Exemple 2 (ROM 362)**.** Un polynôme constant non nul n'a pas de racine et le polynôme nul a tous les éléments de $\mathbb{K}$ comme racine.

Proposition 3 (ROM 362)**.** $\forall \alpha \in \mathbb{K}$, $P(\alpha) = 0 \iff \exists Q \in \mathbb{K}[X], P = Q(X - \alpha)$. Prérequis anneau principal (euclidien) pour div euclidienne

Définition 4 (ROM 362)**.** Supposons que P soit non constant. Soient $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On dit que α est une racine d'ordre (ou de multiplicité) m de P si $(X - \alpha)^m$ divise P et $(X - \alpha)^{m+1}$ ne divise pas P.

Si $m = 1$, on dit que α est une racine simple.

Remarque 5 (ROM 362)**.** La mutliplicité m d'une racine vérifie $m \in [\![1, deg(P)]\!]$.

Théorème 6 (ROM 362)**.** Soit $\alpha_1, .., \alpha_r \in \mathbb{K}$ deux à deux distincts et $m_1, .., m_r \in \mathbb{N}^*$. Supposons P non constant. LASSE :

1. $\forall k \in [\![1, r]\!], \alpha_k$ est racine de P de multiplicité m_k
2. $\exists \mathbb{Q} \in \mathbb{K}[X]$, tel que $P(X) = Q(X) \prod_{k=1}^{r} (X - \alpha_k)^{m_k}$ et $\forall k \in [\![1, r]\!]$, $Q(\alpha_k) \neq 0$.

Corollaire 7 (ROM 363)**.** Si P est non constant et admet $r \geq 1$ racines distinctes de multiplicités $m_1, .., m_r$, alors $deg(P) \geq \sum_{k=1}^{r} m_k$.

Corollaire 8 (TL2 297)**.** Si $P \in \mathbb{K}_n[X]$ de degré n admet $n + 1$ racines deux à deux distincts, alors P est le polynôme nul.

Exemple 9 (ROM 363)**.** Si $P \in \mathbb{K}_n[X]$ admet plus de n racines comptés avec multiplicités, alors P est le polynôme nul.

Remarque 10 (ROM 363)**.** Ce n'est plus valable pour les polnômes à coefficients dans un anneau commutatif unitaire : $3X \in \mathbb{Z}/6\mathbb{Z}$ est de degré 1 mais possède 0 et 2 comme racines.

On peut mettre thm de Taylor si on veut..(ROM 366

1.2 Polynôme scindé et irréductibilité

REVOIR L'OOOORDRE

Définition 11 (ROM 364)**.** On dit que P est scindé sur $\mathbb{K}$ s'il est constant ou de degré $n \geq 1$ et admet $r \geq 1$ racines distinctes $\alpha_1, .., \alpha_r$ dans $\mathbb{K}$ de multiplicités respectives $m_1, .., m_r$ avec $\sum_{i=1}^{r} m_i = n$.

Si tous les m_i sont égaux à 1, on dit que le polynôme est scindé à racines simples.

Exemple 12 (No ref)**.** $(X+2)(X-3) \in \mathbb{R}[X]$ est scindé à racine simple.

Proposition 13 (ROM 364)**.** Un polynôme scindé non constant est de la forme $P(X) = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{m_k}$.

Définition 14 (ROM 370)**.** Un polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ est dit irréductible s'il est non constant et n'est divisible que par les constantes non nulles ou les polynômes λP, avec $\lambda \in \mathbb{K}^*$.

Exemple 15 (ROM 370)**.** $X^2 - 2$ est réductible dans $\mathbb{R}[X]$ avec $-\sqrt{2}$, $\sqrt{2}$ comme racines simples, mais pas dans $\mathbb{Q}[X]$.

Proposition 16 (un peu ROM 371)**.** Si $deg(P) \in \{2, 3\}$, P est irréductible si et seulement si il n'a pas de racines.

Contre-exemple 17 (No ref)**.** $(X + 1)^2 \in \mathbb{R}[X]$ est n'est pas irréductible, pourtant il n'admet pas de racines dans $\mathbb{R}$.

Théorème 18 (ROM 371 raccourci)**.** Tout polynôme non constant P est produit de polynômes irréductibles et une telle décomposition est unique (à permutation près).

Définition 19 (ROM 364)**.** On dit que $\mathbb{K}$ est algébriquement clos si tout polynôme $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$.

Théorème 20 (ROM 381)**.** [D'Alembert Gauss] $\mathbb{C}$ est algébriquement clos.

Exemple 21 (No ref)**.** $P = X^2 + 1$ est irréductible sur $\mathbb{R}[X]$ car il n'a pas de racines réelles ; cependant on peut le scinder sur $\mathbb{C}$ par $P = (X - i)(X + i)$.

1.3 Fonctions symétriques élémentaires

Permet de relier racines et coefficients

Définition 22 (ROM 367)**.** Soit $n \in \mathbb{N}$. On définit les fonctions symétriques élémentaires $\sigma_{n,k} : \mathbb{K}^n \to \mathbb{K}$, l'entier k étant compris entre 0 et n, par : $\forall \alpha = (\alpha_i)_{1 \leq i \leq n} \in K^n$,

$$\sigma_{n,k}(\alpha) = \begin{cases} 1 & \text{si } k = 0 \\ \sum\limits_{1 \leq i_1 \leq \ldots \leq i_k \leq n} \alpha_{i_1} \ldots \alpha_{i_k} & \text{si } k \in \{1, \ldots, n\} \end{cases}$$

Exemple 23 (ROM 367)**.** $\sigma_{n,1}(\alpha) = \sum_{i=1}^{n} \alpha_i$ et $\sigma_{n,n}(\alpha) = \prod_{i=1}^{n} \alpha_i$.

Remarque 24. ROM 367 La qualification "symétrique" vient du fait que pour toute permutation $\tau \in S_n$, on a $\sigma_{n,k}(\alpha_{\tau(1)}, .., \alpha_{\tau(n)}) = \sigma_{n,n}(\alpha) = \prod_{i=1}^{n} \alpha_i$

Théorème 25 (ROM 368)**.** Si $P(X) = \prod_{k=1}^{n} (X - \alpha_k)$ est un polynôme unitaire de degré $n \geq 1$ scindé dans $\mathbb{K}[X]$, on a alors $P(X) = \sum_{k=0}^{n} a_k X^{n-k}$ avec $\forall k \in \{0, 1, .., n\}, a_k = (-1)^k \sigma_{n,k}(\alpha_1, .., \alpha_n)$.

Application 26 (ROM 369 - 370)**.** [Poincaré] Formule de Poincaré : Si $(A_k)_{1 \leq k \leq n}$ est une suite d'évènements d'un espace probabilisé $(\Omega, \mathcal{B}, \mathbb{P})$, on a alors :

$$\mathbb{P}(\bigcup_{k=1}^{n} A_k) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \ldots < i_k \leq n} \mathbb{P}(A_{i_1} \cap \ldots \cap A_{i_k})$$

2 Cas complexe

On se place dans le cas $\mathbb{K} = \mathbb{C}$.

2.1 Localisation des racines

Définition 27 (TL2 302)**.** Soit $P = X^p + \sum_{k=0}^{p-1} a_k X^k \in \mathbb{K}[X]$ un polynôme unitaire de degré $p \geq 1$. On appelle matrice compagnon du polynôme P, noté C_P la matrice $\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ & . & . & . & \\ 0 & 0 & \ldots & 1 & -a_{p-1} \end{pmatrix} \in M_p(\mathbb{K})$.

Proposition 28 (TL2 302)**.** Soient $P \in \mathbb{K}[X]$ un polynôme unitaire de degré $p \geq 1$. $\chi_{C_P} = P$.

Remarque 29 (No ref)**.** Rechercher les racines d'un polynôme $P \in \mathbb{K}[X]$ revient donc à chercher les valeurs propres de sa matrice compagnon. Si P non unitaire on multiplie par inverse de son coef dominant.

Notation 30 (ROM 650)**.** On note pour tout $i \in [\![1, n]\!]$ $L_i = \sum_{j \neq i} |a_{i,j}|$ et $C_i = \sum_{j \neq i} |a_{j,i}|$. On note également $L = \max_{1 \leq i \leq n} \{L_i + |a_{i,i}|\}$ et $C = \max_{1 \leq i \leq n} \{C_i + |a_{i,i}|\}$

Théorème 31 (ROM 651)**.** [Gerschgöring-Hadamard] Soit $\mathbb{K} = \mathbb{C}$ et $\lambda \in Sp(A)$. Il existe un indice $i \in \{1, ..., n\}$ tel que $|\lambda - a_{i,i}| \leq L_i$

Corollaire 32 (ROM 651)**.** Pour toute valeur propre $\lambda \in \mathbb{C}$ de A on a $|\lambda| \leq \min\{L, C\}$.

une app : mat à diag dominante est inversible

2.2 Racines $n-$ième d'un nombre complexe

On s'intéresse dans cette partie aux racines des polynômes de la forme $X^n - \alpha$, où $\alpha \in \mathbb{C}$ et $n \in \mathbb{N}^*$.

Définition 33 (ROM 378)**.** Soit $\alpha \in \mathbb{C}$ et $n \in \mathbb{N}^*$. On appelle racine $n-$ième de α tout nombre complexe z tel que $z^n = \alpha$.

Exemple 34 (ROM 378)**.** 0 est l'unique racine $n-$ième de 0.

Proposition 35 (ROM 378)**.** Soit $\alpha = \rho e^{i\theta}$, avec $\rho > 0$ et $\theta \in [-\pi, \pi[$. Alors, $z_0 = \sqrt[n]{\rho} e^{i\frac{\theta}{n}}$ est solution de $z^n = \alpha$. De plus, toute autre solution $z \in \mathbb{C}$ vérifie $\left(\frac{z}{z_0}\right)^n = 1$.

Définition 36 (ROM 379)**.** Soit $n \in \mathbb{N}^*$. On appelle racine $n-$ième de l'unité toute racine $n-$ième de 1.

Notation 37. $\mathbb{U}_n$ l'ensemble des racine $n-$ième de l'unité

Proposition 38 (ROM 379)**.** Soit $n \in N^*$. Il y a exactement n racines $n-$ièmes de l'unité qui sont données par $w_k = e^{\frac{2ik\pi}{n}}$, pour tout $0 \leq k \leq n-1$.

Proposition 39 (ROM 379)**.** Soit $n \in \mathbb{N}^*$ et $z \in \mathbb{C}$. On a $z^n - 1 = \prod_{k=0}^{n-1} (z - \omega_k)$, où $\omega_k = e^{\frac{2i\pi k}{n}}$, pour tout $0 \leq k \leq n-1$, sont les racines $n-$ièmes.

Proposition 40 (ROM 379)**.** $\mathbb{U}_n$ est un groupe cyclique de $\mathbb{C}^*$ d'ordre n engendré par $\omega_1 = e^{\frac{2i\pi}{n}}$.

Corollaire 41. Soit $n \in \mathbb{N}^*$ et $\alpha = \rho e^{i\theta} \in \mathbb{C}$. α a exactement n racines $n-$ième données par $u_k = u_0 \omega_k = \sqrt[n]{\rho} e^{i\frac{\theta}{n}} e^{\frac{2i\pi k}{n}}$

3 Applications

3.1 Réduction d'endomorphisme

On considère $\mathbb{K}$ un corps, E un $\mathbb{K}-$espace vectoriel de dimension finie n et $u \in \mathcal{L}(E)$.

Proposition 42 (BER 958)**.** λ est une valeur propre de u si et seulement si $\chi_u(\lambda) = 0$.

Proposition 43 (BER 959, Mettre celles qui nous intéresse, scindé sans racine mult.)**.** Les propriétés suivantes sont équivalentes :

1. u est diagonalisable
2. $E = \bigoplus_{\lambda \in Sp_K(u)} E_\lambda$
3. χ_u est scindé, et pour tout $\lambda \in Sp_K(u)$, on a $dim_K(E_\lambda) = m_\lambda$
4. $\prod_{\lambda \in Sp(u)} (X - \lambda)$ annule u
5. il existe un polynôme P annulant u scindé sans racines multiples
6. μ_u est scindé sans racines multiples

Théorème 44 (ROM 676, GOU 174)**.** u est trigonalisable si et seulement si son polynôme caractéristique est scindé.

Proposition 45 (DEV 2)**.** Soit $A = \begin{pmatrix} a_1 & a_2 & . & . & . & a_n \\ a_n & a_1 & . & . & . & a_{n-1} \\ . & & . & & & . \\ . & & & . & & . \\ . & & & & . & . \\ a_2 & a_3 & . & . & . & a_1 \end{pmatrix} \in M_n(\mathbb{C})$ une matrice circulante. Posons $P(X) = \sum_{i=1}^{n} a_k X^{k-1}$. Alors $det(A) = \prod_{j=1}^{n} P(w^j)$ où $w = e^{2i\pi/n}$.

Application 46 (DEV 2)**.** Soit P un polygone du plan complexe à n côtés. Notons $(z_1, ..z_n) \in \mathbb{C}^n$ les affixes des sommets de P. On définit alors pas récurrence une suite de polygones $(P_k)_k$ avec $P_0 = P$ et où les sommets de P_{k+1} sont les milieux des arrêtes de P_k. Alors $(P_k)_k$ converge vers l'isobarycentre de P.

3.2 Corps de rupture

On considère dans cette partie un corps $\mathbb{K}$.

revoir avec leçon 141

Définition 47 (PER 70, ROM 418, BER 816)**.** On dit qu'une extension $\mathbb{L}$ de $\mathbb{K}$ est un corps de rupture d'un polynôme non constant $P \in \mathbb{K}[X]$ si le polynôme P a une racine ω dans $\mathbb{L}$ telle que $\mathbb{L} = \mathbb{K}[\omega]$.

Proposition 48 (No ref, pas sûre !)**.** Soit $\mathbb{L}$ le corps de rupture d'un polynôme P irréductible sur $\mathbb{K}[X]$. $[\mathbb{L} : \mathbb{K}] = deg(P)$

Théorème 49 (PER 70)**.** Soit $P \in \mathbb{K}[X]$. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

Exemple 50 (BER 818)**.** Prenons $P = X(X^2 + 1) \in \mathbb{Q}[X]$. $\mathbb{Q}/\mathbb{Q}$ et $\mathbb{Q}(i)/\mathbb{Q}$ sont deux corps de rupture de P. Ceci montre qu'il n'y a pas unicité. De plus ces extension ne sont pas isomorphe car elles n'ont pas le même degré A voir la derniere rem !!!

3.3 Polynômes cyclotomiques

Définition 51 (TL1 260, ou PER 80)**.** Une racine primitive $n$ème de l'unité est un générateur de $\mathbb{U}_n$

Notation 52. On note $\mathbb{U}_n^*$ l'ensemble des racines primitives $n-$ème de l'unité.

Exemple 53 (No ref)**.** $-1 \in \mathbb{U}_4$ mais ce n'est pas une racine primitive 4ème car $< -1 >= \{1, -1\}$. C'est cependant une racine 2ème de l'unité

Proposition 54 (TL1 260, un peu)**.** Les générateur de $\mathbb{U}_n$ sont les $e^{i2k\pi/n}$ où $k \in [\![1, n-1]\!]$ et $k \wedge n = 1$. Ainsi, $|\mathbb{U}_n^*| = \varphi(n)$, où φ est l'indicatrice d'Euler

Définition 55 (TL1 309)**.** Le $n-$ème polynôme cyclotomique est le polynôme unitaire ϕ_n dont les racines sont les racines primitives $n-$ème de l'unité : $\phi_n(X) = \prod_{\xi \in \mathbb{U}_n^*} (X - \xi)$

Proposition 56 (TL1 309, PER 80)**.** $deg(\phi_n) = \varphi(n)$

Exemple 57 (TL1 309)**.**
1. $\phi_1(X) = X - 1$
2. Si p est premier, $\varphi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + ... + X + 1$
3. $\phi_4(X) = X^2 + 1$

Proposition 58 (TL1 309)**.** Soit $n \geq 1$. Alors : $X^n - 1 = \prod_{d|n} \phi_d$

Théorème 59 (PER 82, DEV 1)**.** Pour $n \geq 1$, $\varphi_n(X) \in \mathbb{Z}[X]$ est un polynôme irréductible et unitaire, donc irréductible dans $\mathbb{Q}[X]$ également.