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

Romain MAURICE

2022-2023

On se place dans le cas d'un corps commutatif $\mathbb{K}$, P un polynôme de $\mathbb{K}[X]$ et $n \in \mathbb{N}^*$. On note $\mathbb{F}_q$ le corps à q élément, avec $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ si p est premier.

1 Racines d'un polynôme

1.1 Racines et multiplicités

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

Proposition 2 : On a que $\alpha \in \mathbb{K}$ est une racine de P si et seulement si $X - \alpha$ divise P.

Définition 3 : On suppose P non constant, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On dit que α est racine d'ordre (ou de multiplicité) m de P si $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne divise pas P.

Remarque 4 : On parle de racine simple pour $m = 1$, de racines double pour $m = 2$ et de racines multiples pour $m \geq 2$. On peut dire que α est de multiplicité nulle si il n'est pas racine.

Théorème 5 : Soit P non constant et $\alpha_1, ..., \alpha_r$ dans $\mathbb{K}$ deux à deux distincts et $m_1, ..., m_r$ dans $\mathbb{N}^*$. Les deux assertions suivantes sont équivalentes :

i) Pour tout $k \in [\![1\,;r]\!]$, α_k est racine de P de multiplicité m_k.

ii) Il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P(X) = Q(X)\prod_{k=1}^{r}(X-\alpha_k)^{m_k}$ et $Q(\alpha_k) \neq 0$ pour tout $k \in [\![1\,;r]\!]$.

Corollaire 6 : Un polynôme $P \in \mathbb{K}[X]$ de degré $n \geq 1$ admet au plus n racines distinctes dans $\mathbb{K}$.

Application 7 : Si P et Q deux polynômes de degré n de $\mathbb{K}[X]$ coïncident en au moins $n+1$ points distincts, alors ils sont égaux.

Remarque 8 : Le résultat est faux sur les anneaux. Par exemple, dans $\mathbb{Z}/6\mathbb{Z}[x]$, le polynôme $3\overline{X}$ de degré 1 admet 2 racines $x_1 = 0$ et $x_2 = 2$ et n'est pas le polynôme nulle.

Proposition 9 : Si le corps $\mathbb{K}$ est infini, le morphisme de $\mathbb{K}$-algèbre $P \mapsto \tilde{P}$ qui associe à $P \in \mathbb{K}[X]$ la fonction polynomial $\tilde{P} \in \mathbb{K}^{\mathbb{K}}$ est injectif.

Remarque 10 : La non finitude de $\mathbb{K}$ est importante. En effet, pour un corps fini $\mathbb{F}_q$, on a $x^q = x$ pour tout $x \in \mathbb{F}_q$. Donc le polynôme $P(X) = X^q - X$ est non nulle mais la fonction polynomial est nulle car $\tilde{P}(x) = 0$ pour tout $x \in \mathbb{F}_q$.

Définition 11 : 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 $\sum_{i=1}^{r} m_i = n$. Dans le cas où tous les m_i sont égaux à 1, on dit que le polynôme est scindé à racines simples.

Définition 12 : On dit que le corps $\mathbb{K}$ est algébriquement clos si tout polynôme $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$.

Théorème (d'Alembert-Gauss) 13 : Le corps $\mathbb{C}$ est algébriquement clos.

Remarque 14 : Ces corps sont très pratiques, notamment en algèbre linéaire ou l'existence de racine pour le polynôme caractéristique ou minimal d'un endomorphisme u est très pratique.

Théorème 15 : Si $car(\mathbb{K}) = 0$, alors α est une racine de P d'ordre $m \geq 1$ si et seulement si $P^{(k)}(\alpha) = 0$ pour $k \in 0m-1$ et $P^{(m)}(\alpha) \neq 0$.

1.2 Irréductibilité et construction des corps finis

Définition 16 : Un polynôme $P \in \mathbb{K}[X]$ non nulle 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 17 : • Un polynôme de degré 1 est irréductible. Si le corps $\mathbb{K}$ est algébriquement clos, les polynômes de degré 1 sont alors les seuls polynômes irréductibles.

• Un polynôme de degré 2 est réductible dans $\mathbb{K}[X]$ si et seulement si il admet une racine double ou deux racines simples dans $\mathbb{K}$.

• $P(X) = X^2 - 2$ est réductible dans $\mathbb{R}[X]$ mais pas sur $\mathbb{Q}[X]$.

• Un polynôme de degré $1, 2, 3$ est réductible dans $\mathbb{K}[X]$ si et seulement si il admet au moins une racine dans $\mathbb{K}$.

Théorème 18 : On a que $\mathbb{K}[X]/(P)$ est un corps si et seulement si le polynôme P est irréductible.

Exemple 19 : On a que $\mathbb{R}[X]/(X^2+1)$ est un corps, qui est isomorphe à $\mathbb{C}$.

Définition 20 : On note $\mathcal{U}_n(p)$ l'ensemble de tous les polynômes unitaires irré-

ductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p)$ le cardinal de $\mathcal{U}_n(p)$. On pose le polynôme $P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$.

Exemple 21 : Comme tous les polynômes $P(X) = X - \lambda$ sont irréductible pour $\lambda \in \mathbb{F}_p$, on a $I_1(p) = p$.

Remarque 22 : Si $P \in \mathcal{U}_n(p)$, on a donc que $\mathbb{F}_p[X]/(P)$ est un corps fini de cardinal p^n. On peut le voir comme une extension de corps de $\mathbb{F}_p$ de degré n avec comme base $(\overline{X}^k)_{0 \leq k \leq n-1}$.
De cette manière, on peut associer l'existence de corps finis à l'existence de polynômes irréductibles.

Lemme 23 : Tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement, pour tout diviseur d de n, tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n.

Théorème 24 : Le polynôme P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en facteur irréductible, $P_n(X) = X^{p^n} - X = \prod_{d|n} \prod P \in \mathcal{U}_d(p) P$.

Remarque 25 : On peut alors compter le nombre de polynôme irréductible dans $\mathbb{F}_p[X]$. Par exemple, le nombre de polynômes irréductible de degré 2 dans $\mathbb{F}_2[X]$ est de 1, et c'est $X^2 + X + 1$.

Développement 26 : Pour tout entier naturel non nul n, on a $nI_n(p) = \sum_{d|n} \mu(d) p^{n/d}$. **Dev 1**

Corollaire 27 : Il existe des polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$.

Théorème 28 : A un isomorphisme près, il n'existe qu'un seul corps à p^n éléments, c'est le corps $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ où $P \in \mathcal{U}_n(p)$.

1.3 Adjonction de racines

Définition 29 : Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Une extension $\mathbb{L}$ de $\mathbb{K}$ est appelée un corps de rupture de P sur $\mathbb{K}$ si $\mathbb{L} = \mathbb{K}(\alpha)$ avec $P(\alpha) = 0$.

Exemple 30 : $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/(X^3 - 2)$ est un corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

Théorème 31 : Il existe un corps de rupture de P sur $\mathbb{K}$, unique à isomorphisme près.

Remarque 32 : Un polynôme n'est pas forcément entièrement factoriser sur un corps de rupture. On a $X^3 - 2 = (X - \sqrt[3]{2})Q(X)$ sur $\mathbb{Q}(\sqrt[3]{2})[X]$ mais on n'a pas les deux autres racines.

Définition 33 : Soit P de degré n. On appelle corps de décomposition de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ qui est telle que :
i) Dans $\mathbb{L}[X]$, P est produit de facteur de degré 1 (ou encore, P a "toutes" ses racines dans $\mathbb{L}$).
ii) Le corps $\mathbb{L}$ est minimal pour cette propriété (ou encore, les racines de P engendrent L).

Théorème 34 : Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près. On le note $D_{\mathbb{K}}(P)$.

Exemple 35 : Pour $P(X) = X^3 - 2$ sur $\mathbb{Q}$, on a $D_{\mathbb{Q}}(P) = \mathbb{Q}(\sqrt[3]{2}, j)$.

2 Fonctions symétriques élémentaires

2.1 Polynômes symétriques élémentaires

Soit $\mathbb{A}$ un anneau commutatif unitaire.
Définition 36 : Un polynôme $P \in \mathbb{A}[X_1, ..., X_n]$ est dit symétrique si pour tout $\sigma \in \mathcal{S}_n$, on a $P(X_{\sigma(1)}, ..., X_{\sigma(n)}) = P(X_1, ..., X_n)$.

Exemple 37 : Dans $\mathbb{R}[X, Y, Z]$, $P = XY + YZ + ZX$ est symétrique.

Définition 38 : Soit $M = X_1^{\alpha_1} ... X_n^{\alpha_n} \in \mathbb{A}[X_1, ..., X_n]$. Si $\sigma \in \mathcal{S}_n$, on pose $M_\sigma = X_{\sigma(1)}^{\alpha_1} ... X_{\sigma(n)}^{\alpha_n}$. Le polynôme $\sum_{M_\sigma \quad \text{distincts}} M_\sigma$ est symétrique. On l'appelle le symétrisé de M et on le note $\sum M$.

Exemple 39 : Dans $\mathbb{K}[X_1, X_2]$, on a $\sum X_1^2 X_2 = X_1^2 X_2 + X_1 X_2^2$.

Définition 40 : On appelle polynômes symétriques élémentaires de $\mathbb{A}[X_1, ..., X_n]$ les polynômes notés $e_k (0 \leq k \leq n)$ et définis par $e_k = \sum_{I \in \mathcal{P}_k([\![1\,;n]\!])} \prod_{i \in I} X_i$ ou $\mathcal{P}_k([\![1\,;n]\!])$ désigne l'ensemble des parties à k éléments de $\{1, ..., n\}$.

Théorème 41 : 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 pour tout $k \in [\![0\,;n]\!], a_k = (-1)^k e_k(\alpha_1, ..., \alpha_n)$.

2.2 Structure des polynômes symétrique

Définition 42 : Le degré total d'un monôme $aX_1^{i_1} ... X_n^{i_n}$, $a \neq 0$ est $i_1 + ... + i_n$. Si $P \in \mathbb{A}[X_1, ..., X_n]$, le degré total de P, noté $deg(P)$, est le plus grand degré total des monômes qui forment P.

Théorème 43 : Soit $P \in \mathbb{A}[X_1, ..., X_n]$ un polynôme symétrique dans $\mathbb{A}[X_1, ..., X_n]$. Alors il existe un unique polynôme $Q \in \mathbb{A}[X_1, ..., X_n]$ tel que $P(X_1, ..., X_n) = Q(e_1, ..., e_n)$.

Remarque 44 : On peut donc obtenir tous les polynômes symétriques de $\mathbb{A}[X_1, ..., X_n]$ a partir des polynômes symétriques élémentaires.

Exemple 45 : Soit $P(X, Y, Z) = X^3 + Y^3 + Z^3 \in \mathbb{R}[X, Y, Z]$. Alors $P(X, Y, Z) = e_1^3 - 3e_1e_2 + 3e_3$.

Application 46 : On va le voir juste après, mais ce théorème est très utile pour démontrer le théorème de Kronecker.

3 Localisation de racines

3.1 Propriétés générales

Théorème (Gauss-Lucas) 47 : Soit $P \in \mathbb{C}[X]$, avec $deg(P) \geq 2$. Alors les racines de P' appartiennent à l'enveloppe convexe des racines de P.

Théorème (Kronecker) 48 : Soit $\alpha \neq 0$ un entier algébrique (i.e un nombre algébrique dont le polynôme minimal unitaire est dans $\mathbb{Z}[X]$) dont tous les conjugués appartiennent à $D = \{z \in \mathbb{C}, |z| \leq 1\}$ le disque unité. Alors α est une racine de l'unité, i.e il existe $m \in \mathbb{N}^*$ tel que $\alpha^m = 1$. **Dev 2**

Corollaire 49 : Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible sur $\mathbb{Q}$ tel que toutes les racines complexes soient de modules au plus 1. Alors $P = X$ ou P est un polynôme cyclotomique.

3.2 Disque de Gerschgörin

Définition 50 : On associe au polynôme unitaire $P = X^n + \sum_{k=0}^{n-1} a_k X^k$ la matrice compagnon définie par

$$\mathcal{C}_P = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix} \in \mathcal{M}_n(\mathbb{K}).$$

Proposition 51 : Le polynôme caractéristique et minimale de $\mathcal{C}_P$ est P.

Remarque 52 : Cela nous permet d'étudier ce les racines du polynômes P sous le prisme de l'algèbre linéaire en considérant les valeurs propres sa matrice compagnon.

Définition 53 : Soit $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{C})$. On pose $R_i = \sum_{1 \leq j \neq i \leq n} |a_{i,j}|$ pour $i \in [\![1\,;n]\!]$. On dit que A est à diagonale strictement dominante si pour tout $i \in [\![1\,;n]\!]$, $|a - i, i| > R_i$.

Lemme (de Hadamard) 54 : Si $A \in \mathcal{M}_n(\mathbb{C})$ est à diagonale strictement dominante, alors A est inversible.

Théorème (disque de Gerschgörin) 55 : Soit $A \in \mathcal{M}_n(\mathbb{C})$. Alors on a $Sp(A) \subset \bigcup_{i=1}^n \{z \in \mathbb{C}, |z - a_{i,i}| \leq R_i\}$.

Remarque 56 : Cela nous permet d'avoir des informations sur la localisation des valeurs propres de la matrice, et donc sur les racines de P.

3.3 Suite de Sturm

Théorème 57 : Soit $P \in \mathbb{R}[X]$. On pose $S_0 = P, S_1 = P'$, puis, aussi longtemps que c'est possible, $S_{i-1} = A_i S_i - S_{i+1}$, avec $deg(S_{i+1}) < deg(S_i)$.
Pour x réel, on note $V(x)$ le nombre de changement de signes (stricts) de la suite $S_0(x), ..., S_p(x)$, lorsque $S_{p+1} = 0$. On a donc $V(x) = card(\{(i, j) | 0 \leq i < j \leq p, S_i(x)S_j(x) < 0 \text{ et } S_k(x) = 0 \text{ si } i < k < j\}$.
Soit $a < b$. On suppose que $P(a)P(b) \neq 0$. Alors le nombre de racines distinctes de P dans $[a, b]$ est égal à $V(a) - V(b)$.

Références :

1. Algèbre Gourdon
2. Algèbre et géométrie Rombaldi
3. Cours d'algèbre Perrin
4. Arithmétique Liret
5. FGN Algèbre tome 1 et 2
6. isenmann (rip)