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

Ouvrages : Gourdon, Perrin, Gozard, Caldero (CVA), Francinou X-ENS Alg. 1

I - Racines d'un polynôme

1) Définitions et propriétés

2) Polynôme dérivé - formules de Taylor

II - Polynômes symétriques élémentaires

1) Définitions et premières propriétés

2) Théorème de structure

III - Théorie des corps et polynômes

1) Extension algébrique

2) Corps de rupture et de décomposition

3) Racines de l'unité - polynômes cyclotomiques

IV - Application à la réduction de matrices

V - Localisation de racines

DEV 1 : Théorème de Kronecker

DEV 2 : Irréductibilité de Φ_n

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

On considère $\mathbb{K}$ un corps commutatif, A un anneau commutatif intègre unitaire.

I - Racines d'un polynôme [GOZ]

DEF 1 : Soit $P \in K[X]$ et L une extension de K. On dit que $a \in L$ est une racine (ou un zéro) de P lorsque $P(a) = 0$.

PROP 2 : Soit $a \in K$ et $P \in K[X]$. Alors : $P(a) = 0 \Leftrightarrow (X-a) \mid P$ dans $K[X]$.

DEF 3 : Soit $P \in K[X]$, $a \in K$ et $h \in \mathbb{N}^*$. On dit que a est une racine d'ordre h de P lorsque $(X-a)^h \mid P$ et $(X-a)^{h+1} \nmid P$.

PROP 4 : Soit $P \in K[X]$, $a_1, \dots, a_r \in K$ des racines de P d'ordre $h_1, \dots, h_r$ (a_i distincts deux à deux). Alors il existe $Q \in K[X]$ tel que $P(X) = (X-a_1)^{h_1} \dots (X-a_r)^{h_r} Q(X)$ et $\forall i,\ Q(a_i) \neq 0$.

COR 5 : Si $\deg(P) \geq 1$, alors P a au plus $\deg(P)$ racines dans K comptées avec multiplicité.

EX 6 : Le COR 5 est faux si $P \in A[X]$ avec A un anneau : $P(X) = 4X \in (\mathbb{Z}/8\mathbb{Z})[X]$ a 3 racines : 0, 2 et 4 mais $\deg(P) = 1$!

PROP 7 : Soit $P \in K[X]$ tel que : $\forall x \in K,\ P(x) = 0$. Si $\#K = +\infty$, $P = 0$.

DEF 8 : Un polynôme $P \in K[X]$ est dit scindé sur $\mathbb{K}$ lorsqu'on peut écrire $P(X) = \lambda (X-a_1)^{h_1} \dots (X-a_r)^{h_r}$, $\lambda \in K$, $\forall i \in [\![1;r]\!]$, $a_i \in K$, $h_i \in \mathbb{N}^*$.

REM 9 : Deux polynômes P et Q de $K[X]$ scindés sur $\mathbb{K}$ sont premiers entre eux si et seulement s'ils n'ont aucune racine commune.

DEF 10 : Soit $P \in K[X]$, $P = \sum_{i=0}^{n} a_i X^i$. On appelle fonction polynomiale associée à P la fonction $\tilde{P} : \mathbb{K} \longrightarrow \mathbb{K}$, $x \longmapsto \sum_{i=0}^{n} a_i x^i$.

REM 11 : Si $\#K = +\infty$, l'application $P \mapsto \tilde{P}$ est une bijection, si K est fini, on peut avoir $\tilde{P} = 0$ sans que P soit nul...

DEF 12 : Soit $P = \sum_{i=0}^{n} a_i X^i \in K[X]$. On appelle polynôme dérivé de P le polynôme $P' = \sum_{i=1}^{n} i a_i X^{i-1}$.

REM 13 : Cette définition coïncide avec la dérivée de la fonction polynomiale associée.

THM 14 : Si $\mathrm{car}(K) = 0$, tout polynôme $P \in K[X]$, $\deg(P) \leq n$ vérifie : $\forall a \in K$, $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k$

COR 15 : Si $\mathrm{car}(K) = 0$, $P \in K[X]$, $P \neq 0$, $a \in K$ est racine d'ordre h de P si et seulement si $\forall i \in [\![0; h-1]\!]$, $P^{(i)}(a) = 0$ et $P^{(h)}(a) \neq 0$.

REM 16 : Le cas de $P = X^3 \in \mathbb{Z}/3\mathbb{Z}[X]$ et $a = \bar{0}$ montre que ceci est faux en caractéristique non nulle.

II - Polynômes symétriques élémentaires

[GOZ] 1) Définitions et relations coefficients - racines

DEF 16 : Soit $P \in A[X_1, \dots, X_n]$. On dit que P est symétrique lorsque $\forall \sigma \in \mathfrak{S}_n$, $\sigma.P(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.
On note $A[X_1, \dots, X_n]^{\mathfrak{S}_n} := \{P \in A[X_1, \dots, X_n] \mid \forall \sigma \in \mathfrak{S}_n, \sigma.P = P\}$.

EX 17 : $\prod_{i \neq j} (X_i - X_j) \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$

DEF 18 : Soit $e \in \mathbb{N}^*$. On appelle somme de Newton d'indice e le polynôme symétrique $S_e(X_1, \dots, X_n) = \sum_{i=1}^{n} X_i^e$.

DEF 19 : Les n polynômes suivants sont symétriques :
$\sigma_1 = \sum_{i=1}^{n} X_i$; $\sigma_2 = \sum_{i<j} X_i X_j$, ..., $\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}$, ..., $\sigma_n = X_1 \dots X_n$.
On les appelle les polynômes symétriques élémentaires de $A[X_1, \dots, X_n]$.

PROP 20 : Chaque σ_k est la somme de $\binom{n}{k}$ monômes de degré k, est homogène et a pour degré partiel 1 en chacune des variables $X_1, \dots, X_n$.

THM 21 (Relations coefficients-racines) Soit $P \in A[X]$, $(\alpha_1, \dots, \alpha_n) \in A^n$. Alors :
$P(X) = (X-\alpha_1) \dots (X-\alpha_n) \Leftrightarrow P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ où $\forall i \in [\![1;n]\!]$, $a_{n-i} = (-1)^i \sigma_i(\alpha_1, \dots, \alpha_n)$

2) Théorème de structure [GOZ]

DEF 22 : Soit un monôme $aX_1^{\alpha_1} \dots X_n^{\alpha_n}$ où $a \in A \setminus \{0\}$ et les $\alpha_i \in \mathbb{N}$. On appelle poids de ce monôme l'entier $\sum_{i=1}^{n} i\alpha_i$.
Soit $P \in A[X_1, \dots, X_n]$: on appelle poids de P le maximum des poids des monômes non nuls dont il est la somme.

EX 23 : Le poids de σ_k est $nk - \frac{k(k-1)}{2}$.

PROP 24 : Soit $P \in A[X_1, \dots, X_n]$, $P \neq 0$, π son poids. Alors le polynôme $Q(X_1, \dots, X_n) = P(\sigma_1, \dots, \sigma_n)$ est symétrique et $\deg_{tot}(Q) \leq \pi$.

LEMME 25 : Soit $P \in A[X_1, \dots, X_n]$ tel que pour tout $j \in [\![1;n]\!]$, $P(X_1, \dots, X_{j-1}, 0, X_{j+1}, \dots, X_n) = 0$. Alors P est divisible par σ_n dans $A[X_1, \dots, X_n]$.

THM 26 (Structure) : Soit $P \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$, $\deg_{tot}(P) = k$. Il existe un unique polynôme $Q \in A[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = Q(\sigma_1, \dots, \sigma_n)$. Q est de poids k et de degré égal au degré partiel de P par rapport à l'une des variables $X_1, \dots, X_n$.

EX 27 : $S_2 = X_1^2 + \dots + X_n^2 = \sigma_1^2 - 2\sigma_2$.

DEV 1

[FRA1 p 183]

THM 28 (Kronecker) : Soit $P \in \mathbb{Z}[X]$ unitaire dont les racines complexes sont de module inférieur ou égal à 1. On suppose $P(0) \neq 0$. Alors toutes les racines de P sont des racines de l'unité.

THM 29 (Identité de Newton) : On a la formule de récurrence suivante : $\forall k \in [\![1;n]\!]$, $k\sigma_k = \sum_{i=1}^{k} (-1)^{i-1} S_i \sigma_{k-i}$. Le système obtenu est triangulaire inversible.

COR 30 : On obtient par récurrence, $\forall k \in [\![1;n]\!]$, $k < \mathrm{car}(A)$, $\sigma_k \in \frac{1}{k!} A[S_1, \dots, S_n]$

III - Théorie des corps et polynômes

1) Extension algébrique [PER] [GOZ]

DEF 31 : Soit L/K une extension et $\alpha \in L$. On dit que α est algébrique K lorsqu'il existe $P \in K[X] \setminus \{0\}$, $P(\alpha) = 0$ i.e lorsque le morphisme $\varphi : K[T] \to L$, $P \mapsto P(\alpha)$ est non injectif. Le générateur de $\ker(\varphi)$ est alors appelé polynôme minimal de α et noté μ_α.

EX 32 : $\sqrt{2}$; i ; $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ et $\mu_{\sqrt{2}} = X^2 - 2$, $\mu_i = X^2 + 1$; $\mu_{\sqrt[3]{2}} = X^3 - 2$.

THM 33 : Soit L/K une extension et $\alpha \in L$. Les assertions suivantes sont équivalentes
- α est algébrique sur K
- $K[\alpha] = K(\alpha)$
- $\dim_K(K(\alpha)) < \infty$. Dans ce cas, $\dim_K(K(\alpha)) = \deg(\mu_\alpha)$.

DEF 34 : On dit que L/K est algébrique lorsque pour tout $\alpha \in L$, α est algébrique sur K.

THM 35 : Soit L/K une extension. Alors $M = \{x \in L \mid x \text{ algébrique sur } K\}$ est un sous-corps de L.

DEF 36 : Un corps K est dit algébriquement clos lorsqu'il vérifie l'une des propriétés équivalentes suivantes :
- Tout polynôme $P \in K[X]$, $\deg(P) \geq 1$ admet une racine dans K
- Tout polynôme $P \in K[X]$, $\deg(P) \geq 1$ est scindé sur K.
- Les seuls polynômes irréductibles de $K[X]$ sont de degré 1
- Toute extension algébrique de K est identique à K.

EX 37 : $\mathbb{Q}$ n'est pas algébriquement clos

THM 38 : $\mathbb{C}$ est algébriquement clos.

PROP 39 : Tout corps algébriquement clos est infini.

DEF 40 : Soit L/K une extension. On dit que L est une clôture algébrique de K lorsque L est algébrique sur K et L est algébriquement clos.

THM 41 (Steinitz) (admis) : Tout corps commutatif K admet une clôture algébrique $\tilde{K}$.
- Si $\tilde{K}_1$ et $\tilde{K}_2$ sont deux clôtures algébriques de K, alors il existe un K-isomorphisme de $\tilde{K}_1$ sur $\tilde{K}_2$.

2) Corps de rupture et de décomposition [PER]

DEF 42 : Soit $P \in K[X]$ irréductible. Une extension L/K est appelée un corps de rupture de P sur K lorsque L est une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$.

THM 43 : Soit $P \in K[X]$ irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

EX 44 : $\mathbb{Q}(\sqrt[3]{2})$ pour $X^3 - 2$; $\mathbb{Q}(\sqrt[4]{2})$ pour $X^4 - 2$.

DEF 45 : Soit $P \in K[X]$, $\deg(P) = n$. On appelle corps de décomposition de P sur K une extension L de K telle que
- Dans $L[X]$, P est scindé,
- L est minimal pour cette propriété

THM 46 : Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près. On le note $D_K(P)$.

EX 47 : $D_{\mathbb{Q}}(X^3 - 2) = \mathbb{Q}[\sqrt[3]{2}, j]$; $D_{\mathbb{Q}}(X^4 - 2) = \mathbb{Q}(\sqrt[4]{2}, i)$.

THM 48 : Soit $p \in \mathbb{N}$ premier, $n \in \mathbb{N}^*$, $q = p^n$.
- Il existe un corps K à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$, K est unique à isomorphisme près. On le note $\mathbb{F}_q$.

3) Racines de l'unité et polynômes cyclotomiques [PER]

DEF 49 : On note $\mu_n(K) = \{\zeta \in K \mid \zeta^n = 1\}$ l'ensemble des racines n-ièmes de l'unité dans K, ($n \in \mathbb{N}$).

PROP 50 : $\mu_n(K)$ est cyclique en tant que sous-groupe de K^*.

DEF 51 : Une racine primitive n-ième de l'unité est un $\zeta \in \mu_n(K)$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour tout $d < n$. On note $\mu_n^*(K)$ leur ensemble

PROP 52: On a $\# \mu_n^*(K) = \varphi(n)$

DEF 53: Le n-ième polynôme cyclotomique $\phi_{n,K}$ est donné par la formule $\prod_{\zeta \in \mu_n^*(K)} (X - \zeta)$.

PROP 54: $\phi_{n,K}$ est unitaire, de degré $\varphi(n)$.

REM 55: Si ζ est une racine primitive n-ième de l'unité, les autres sont les ζ^m avec $m \wedge n = 1$.

PROP 56: On a la formule $X^n - 1 = \prod_{d \mid n} \phi_d(X)$, on en déduit que $\phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$.

EX 57: $\phi_1(X) = X - 1$, $\phi_3(X) = X^2 + X + 1$, $\phi_4(X) = X^2 + 1$, $\phi_6(X) = X^2 - X + 1$.

REM 58: Si $K = \mathbb{C}$, $\mu_n^*(\mathbb{C}) = \left\{ e^{\frac{2i\pi k}{n}} \mid k \in [\![0; n-1]\!], k \wedge n = 1 \right\}$

DEV 2

LEMME 59: Soient $P, A, B \in \mathbb{Q}[X]$ non nuls. On suppose que $P \in \mathbb{Z}[X]$, que $P = AB$ et P et A sont unitaires. Alors A et B sont dans $\mathbb{Z}[X]$.

THM 60: $\forall n \in \mathbb{N}^*$, ϕ_n est irréductible sur $\mathbb{Q}$ [GOZ]

IV - Application à la réduction de matrices [GOU]

Soit E un K-espace vectoriel de dimension $n \in \mathbb{N}^*$, $u \in \mathcal{L}(E)$ et A la matrice de u dans une base $\mathcal{B}$ de E, $A \in \mathcal{M}_n(K)$.

DEF 61: On appelle polynôme caractéristique de A le polynôme de $K[X]$ défini par $\chi_A(X) = \det(A - XI_n)$.

PROP 62: λ est valeur propre de A si et seulement si $\chi_A(\lambda) = 0$.

COR 63: Soit $(\lambda_1, \dots, \lambda_n)$ les valeurs propres de A dans une clôture algébrique, comptées avec multiplicité :
Alors $\mathrm{Tr}(A) = \sum_{k=1}^{n} \lambda_k$ et $\det(A) = \prod_{k=1}^{n} \lambda_k$.

THM 64: A est diagonalisable si et seulement si pour tout $i \in [\![1; n]\!]$, $\dim(E_{\lambda_i}) = h_i$ où E_{λ_i} est le sous-espace propre associé à λ_i et h_i la multiplicité de λ_i comme racine de χ_A.

THM 65: A est trigonalisable dans K si et seulement si χ_A est scindé sur K.

DEF 66: On appelle polynôme minimal de A le générateur de $\ker(\varphi)$ où $\varphi : K[X] \longrightarrow \mathcal{M}_n(K)$, $P \longmapsto P(A)$. On le note π_A.

PROP 67: λ est valeur propre de A si et seulement si $\pi_A(\lambda) = 0$.

PROP 68: A est diagonalisable sur K si et seulement si π_A est scindé à racines simples dans K.

EX 69: Soit $P \in K[X]_n$, $P = X^n + \sum_{i=0}^{n-1} a_i X^i$. La matrice compagnon
$C_P = \begin{pmatrix} 0 & & (0) & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & & \\ (0) & & 1 \quad 0 & -a_{n-1} \end{pmatrix}$ est diagonalisable si et seulement si P est scindé à racines simples dans K.

V - Localisation de racines [CAL] [FRA]

THM 70: (Disques de Gershgorin)
Soit $A \in \mathcal{M}_n(\mathbb{C})$, $A = (a_{i,j})_{1 \le i,j \le n}$. Soit $R_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} |a_{i,j}|$ et $D_i = \{ z \in \mathbb{C} \mid |z - a_{i,i}| < R_i \}$, $Sp_{\mathbb{C}}(A) = \{ \lambda \in \mathbb{C} \mid \lambda \text{ valeur propre de } A \}$
Alors $Sp_{\mathbb{C}}(A) \subset \bigcup_{i=1}^{n} D_i$

THM 71: (Gauss - Lucas) Soit $P \in \mathbb{C}[X]$ non constant. Alors les racines de P' sont dans l'enveloppe convexe des racines de P.

EX 72: Le plus grand entier $n \geq 2$ tel que les racines non nulles de $(X+1)^n - X^n - 1$ soient de module 1 est 7.

THM 73: Soit $(P_k)_{k \geq 0}$ une suite de polynômes de $\mathbb{C}_n[X]$ qui tend vers un polynôme P.
On note $(\lambda_{k,i})_{i \in [\![1; n]\!]}$ les racines de P_k comptées avec multiplicité et $(\lambda_i)_{i \in [\![1; n]\!]}$ celles de P.
Alors, quitte à renuméroter les $\lambda_{k,i}$, $\forall i \in [\![1; n]\!]$, on a $\lambda_{k,i} \xrightarrow[k \to +\infty]{} \lambda_i$

REM 74: Ce résultat vaut aussi pour $A_k \longrightarrow A$ trigonalisables.