

LEÇON 144 - RACINES D'UN POLYNÔME ETC.

I Cadre théorique ([Ber25])

Dans toute cette partie, on fixe A un anneau (commutatif unitaire), B une A -algèbre et K un corps.

I.1 Racines, multiplicité

Théorème 1 : Soit $x \in B$. Il existe un unique morphisme de A -algèbres $ev_x : A[X] \rightarrow B$ tel que $ev_x(X) = x$ et pour tout $a \in A$, $ev_x(a) = a \cdot 1_B$.

Définition 2 (Racine) : Soit $P \in A[X]$. Un élément $r \in B$ est dit « racine de P » lorsque $ev_r(P) = 0$

Exemple 3 : Le polynôme $X^2 + 1 \in \mathbb{Z}[X]$ n'a pas de racine dans $\mathbb{Z}$ mais a deux racines i et $-i$ dans la $\mathbb{Z}$ -algèbre $\mathbb{C}$.

Remarque 4 : r est racine de P si, et seulement si, $(X - r)$ divise P dans $A[X]$.

Définition 5 (Multiplicité) : Soit $P \in A[X]$ et $r \in A$. On dit que r est racine de P avec multiplicité m si $(X - r)^m$ divise P et $(X - r)^{m+1}$ ne divise pas P .

Proposition 6 : Si K est un corps de caractéristique 0, $r \in K$ est racine de $P \in K[X]$ de multiplicité m si, et seulement si :

$$\forall k \in \llbracket 0, m-1 \rrbracket, (P^{(k)}(r) = 0) \wedge (P^{(m)}(r) \neq 0)$$

Lemme 7 : Pour $P \in A[X]$ non nul, P a au plus $\deg(P)$ racines comptées avec multiplicité dans A dès que A est intègre.

Contre-exemple 8 : Le polynôme $X^2 + 1$ a strictement plus de deux racines dans l'algèbre à division $\mathbb{H}$ des quaternions.

Application 9 (Cyclotomie dans $\mathbb{Q}$) : Notons μ_n^* l'ensemble des éléments d'ordre n dans $\mathbb{C}^*$ et

$$\Phi_n := \prod_{\omega \in \mu_n^*} (X - \omega) \in \mathbb{C}[X]$$

le n -ième polynôme cyclotomique complexe. Φ_n est un élément de $\mathbb{Z}[X]$, irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$. ([Per])

I.2 Polynômes symétriques

Définition 10 (Polynômes symétriques) : Le groupe symétrique $\mathfrak{S}_n$ agit sur l'anneau $A[X_1, \dots, X_n]$ via :

$$\sigma \cdot P(X_1, \dots, X_n) := P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

On appelle polynôme symétrique à n -variables tout point-fixe de cette action. On note $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ l'ensemble de ces polynômes.

Exemple 11 : Le polynôme $X_1X_2 + X_1X_3 + X_2X_3$ est symétrique dans $A[X_1, X_2, X_3]$ mais pas dans $A[X_1, \dots, X_4]$.

Définition 12 (Polynômes symétriques élémentaires) : Soit $P := \prod_{i=1}^n (T - X_i) \in A[X_1, \dots, X_n][T]$. On appelle « k -ième polynôme symétrique élémentaire en n -variables de A » le polynôme $\sigma_{n,k} \in A[X_1, \dots, X_n]$ tel que :

$$P = X^n + \sum_{k=0}^{n-1} (-1)^{n-k} \sigma_{n,n-k}(X_1, \dots, X_n) T^k$$

Proposition 13 : On a une expression combinatoire des polynômes symétriques élémentaires :

$$\sigma_{n,k} = \sum_{I \in P_k(\llbracket 1, n \rrbracket)} \prod_{i \in I} X_i$$

Remarque 14 : De la définition découlent les relations racines-coefficients : si B est un anneau intègre, A un sous-anneau de B et $P \in A[X]$ de degré n est scindé dans B (i. e. $P = \prod (T - r_i)$ avec $r_i \in B$) alors :

$$P = \sum_{k=0}^n (-1)^{n-k} \sigma_{n,k}(r_1, \dots, r_n) T^k$$

Théorème 15 (structure des polynômes symétriques) : Soit $P \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$. Il existe un unique polynôme $S \in A[X_1, \dots, X_n]$ tel que

$$P = S(\sigma_{n,1}, \dots, \sigma_{n,n})$$

Exemple 16 : $X^2 + Y^2 + Z^2 = \sigma_{3,1}^2 - 2\sigma_{3,2}$. Le polynôme $S := X^2 - 2Y$ convient donc.

Corollaire 17 (Kronecker) : Soit P un polynôme unitaire à coefficients dans $\mathbb{Z}$ dont toutes les racines complexes sont de module au plus 1. Si $z \in \mathbb{C}$ est une racine de P , $z = 0$ ou z est une racine de l'unité. ([CP22]) **(DÉVELOPPEMENT 1, 1/2)**

Application 18 : Soit G un sous-groupe fini de $GL_n(\mathbb{Z})$. On a la majoration :

$$|G| \leq (3^n - 1)(3^n - 3) \dots (3^n - 3^{n-1})$$

([CP22]) **(DÉVELOPPEMENT 1, 2/2)**

II Problèmes d'algèbre linéaire ([Rom])

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

Théorème 19 (Polynôme minimal) : L'ensemble $\{P \in K[X] \mid P(u) = 0\}$ est un idéal de $K[X]$. On appelle « polynôme minimal de u », noté π_u , l'unique générateur unitaire de cet idéal.

Exemple 20 :

1. u est nilpotent si, et seulement si, π_u est une puissance de X .
2. Soit L/K une extension finie de corps et $\alpha \in L$. Le polynôme minimal de l'endomorphisme K -linéaire de L $m_\alpha : x \mapsto \alpha x$ est le polynôme minimal de α sur K .
3. En dimension infinie, le polynôme minimal peut ne pas exister. Par exemple, l'endomorphisme de $\mathbb{R}^{\mathbb{N}}$ donné par $(x_n) \mapsto (x_{n+1})$ n'a pas de polynôme minimal.

Proposition 21 : Soit $P \in K[X]$ un polynôme annulateur de u . Si $\lambda \in K$ est une valeur propre de u , $P(\lambda) = 0$. Si de plus P est le polynôme minimal de u , toutes ses racines dans K sont valeurs propres de u .

Théorème 22 (Cayley-Hamilton) : Notons $\chi_u := \det(XI_d - u)$ le polynôme caractéristique de u . $\chi_u(u) = 0$. De plus, les facteurs irréductibles de χ_u et de π_u dans $K[X]$ sont les mêmes.

Application 23 : Pour $K = \mathbb{R}$, on peut approcher les valeurs propres de u à l'aide de la méthode de Newton appliquée à χ_u .

Proposition 24 : Les assertions suivantes sont équivalentes :

1. u est trigonalisable [resp. diagonalisable]
2. u admet un polynôme annulateur scindé [resp. à racines simples] dans K
3. π_u est scindé [resp. à racines simples] dans K

Application 25 (Matrice circulante) : On appelle matrice circulante universelle la matrice

$$C(X_1, \dots, X_n) := \begin{pmatrix} X_1 & X_2 & \dots & X_n \\ X_n & X_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \\ X_2 & \dots & & X_1 \end{pmatrix}$$

Il existe $F \in GL_n(\mathbb{C})$ tel que :

$$C(X_1, \dots, X_n) = F \cdot \text{Diag}(P(\omega^0), \dots, P(\omega^{n-1})) \cdot F^{-1}$$

avec $\omega := e^{\frac{2i\pi}{n}}$ et $P = T^n + \sum_{k=0}^{n-1} X_{k+1}T^k$. ([IP24])

Application 26 : On fixe $K = \mathbb{C}$ et on appelle « rayon spectral de u » le maximum des modules des valeurs propres de u , noté $\rho(u)$. Alors $\rho(u)$ est égal au supremum des $N(u)$, où N parcourt l'ensemble des normes d'opérateur sur $\mathcal{L}(E)$.

III Racines et théorie des corps

III.1 Adjonction de racines [Esc97]

On fixe L/K une extension de corps et $P \in K[X]$ un polynôme non constant.

Définition 27 (Extension de rupture) : On suppose P irréductible. On dit que L/K est une « extension de rupture » de P si L contient α tel que $P(\alpha) = 0$ et $L = K(\alpha)$.

Définition 28 (Extension de décomposition) : On dit que L/K est une « extension de décomposition de P » si P est scindé dans L de racines $(\alpha_1, \dots, \alpha_n)$ et si $L = K(\alpha_1, \dots, \alpha_n)$.

Exemple 29 : L'extension $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$ est une extension de décomposition de $X^3 - 2$. $\mathbb{C}/\mathbb{Q}$ n'en est pas une.

Théorème 30 : Soit $P \in K[X]$ non constant [resp. irréductible]. Il existe une extension de décomposition [resp. de rupture] de P unique à isomorphisme d'extension près. De plus, le degré de cet extension est majoré par $\deg(P)!$ [resp. égal à $\deg(P)$].

Application 31 (Corps finis) : Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. Il existe un corps de cardinal p^α unique à isomorphisme de corps près.

Définition 32 (Polynômes cyclotomiques, corps finis) : Soit $n \in \mathbb{N}^*$, p un nombre premier et q une puissance non triviale de p . On note $L/\mathbb{F}_q$ une extension de décomposition de $X^n - 1$ et $\mu_n^*(\mathbb{F}_q)$ l'ensemble (éventuellement vide) des éléments d'ordre n dans $L^\times$. On définit le n -ième polynôme cyclotomique de $\mathbb{F}_q$ comme le polynôme

$$\Phi_n := \prod_{\omega \in \mu_n^*(\mathbb{F}_q)} (X - \omega) \in L[X]$$

Théorème 33 : On suppose que n est premier avec p . Dans ce cas, $\Phi_n \in \mathbb{F}_q[X]$ et les facteurs irréductibles de Φ_n dans $\mathbb{F}_q[X]$ ont tous pour degré $[L : \mathbb{F}_q]$.

Application 34 : $\mathbb{F}_{7^4}$ est la plus petite extension de $\mathbb{F}_{49}$ (au sens du degré) qui contient une racine 10-ème primitive de l'unité.

III.2 Entiers algébriques (pas de ref!)

Soit $K/\mathbb{Q}$ un corps de nombres (i.e. une extension finie).

Définition 35 (Entier algébrique) : On appelle « entier algébrique » de K tout élément $z \in K$ admettant un polynôme annulateur unitaire à coefficients entiers. On note $\mathfrak{O}_K$ l'ensemble des entiers algébriques de K .

Lemme 36 : Soit $z \in K$. Alors $z \in \mathfrak{O}_K$ si, et seulement si, le polynôme minimal de z sur $\mathbb{Q}$, noté π_z , est à coefficients entiers.

Exemple 37 : Les rationnels entiers algébriques sont exactement les éléments de $\mathbb{Z}$.

Proposition 38 : $\mathfrak{O}_K$ est un sous-anneau de K .

Lemme 39 : On considère L/K une extension finie. Pour $\alpha \in L$, on note $m_\alpha : x \mapsto \alpha x$. C'est un endomorphisme $\mathbb{Q}$ -linéaire de L . De plus, l'application $\alpha \mapsto m_\alpha$ est un morphisme injectif de K -algèbres.

Définition 40 (Norme) : Pour $\alpha \in L$, on appelle norme de α sur K le déterminant de m_α , qu'on note $N(\alpha)$.

Proposition 41 : Notons n le degré de l'extension L/K .

1. La norme est multiplicative : $N(\alpha\beta) = N(\alpha)N(\beta)$.
2. Si π_α désigne le polynôme minimal de α sur K et d désigne son degré :

$$N(\alpha) = (-1)^n [\pi_\alpha(0)]^{n/d}$$

3. Si M/L est une extension telle que π_α est scindé dans M , de racines $(z_1, \dots, z_d)$ comptées avec multiplicité, alors

$$N(\alpha) = \prod z_i^{n/d}$$

(DÉVELOPPEMENT 2, 1/2)

Application 42 (Inversibles de $\mathfrak{O}_K$) : Soit $z \in \mathfrak{O}_K$. Les assertions suivantes sont équivalentes :

1. $z^{-1} \in \mathfrak{O}_K$
2. $N(z) = \pm 1$

(DÉVELOPPEMENT 2, 2/2)

Références

- [Ber25] Grégory BERHUY. *Algèbre, le Grand combat*. Calvage et Mounet, 2025. ISBN : 291635266X.
- [CP22] Philippe CALDERO et Marie PERONNIER. *Carnet de voyage en Algèbre*. Calvage et Mounet, 2022. ISBN : 9782493230034.
- [Esc97] Jean-Pierre ESCOFIER. *Théorie de Galois*. Dunod, 1997.
- [IP24] Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques, une sélection de développements*. Ellipses, 2024.
- [Per] Daniel PERRIN. *Cours d'algèbre*. Ellipses.
- [Rom] Jean-Etienne ROMBALDI. *Mathématiques pour l'agrégation, Algèbre et géométrie*.