

Leçon N°4: Racines d'un polynôme

Dans toute cette leçon, K est un corps, A est un anneau intègre.

I) Définitions et Premières propriétés

1) Aspect algébrique

Définition 1: Soit $P \in A[X]$, $P = \sum_{i=0}^n a_i X^i$, $(a_0, \dots, a_n) \in A^{n+1}$.

On définit la fonction polynomiale $\tilde{P}$ par $\tilde{P}: A \rightarrow A$, $x \mapsto \sum_{i=0}^n a_i x^i$.

On note α écrivainement $\tilde{P}(\alpha) = P(\alpha) \forall \alpha \in A$.

Définition 2: Soit $\alpha \in A$. On dit que α est une racine de P lorsque

$$P(\alpha) = 0.$$

Proposition 3: $\alpha \in \mathbb{Q}$ est racine de P ssi $(X - \alpha) \mid P$.

Définition 4: On dit que $\alpha \in A$ est une racine de P de multiplicité $k \in \mathbb{N}$ lorsque $\forall i \in [0, k-1]$, $(X - \alpha)^i \mid P$ et $(X - \alpha)^{k+1} \nmid P$.

Proposition 5: Soit $Q \in A[X]$ dont $(\lambda_1, \dots, \lambda_n)$ sont les racines de

multiplicité respectives $(m_1, \dots, m_n)$, alors $\deg(Q) = \sum_{i=1}^n m_i$.

Contre exemple 6: Ce n'est pas vrai si A n'est pas intègre: $\exists X$ a deux racines $\forall$.

Application 7: (Interpolation de Lagrange) Soient $(a_0, \dots, a_n) \in K^{n+1}$

et $\forall j \in [0, n]$, $L_j(\alpha_j) = b_j$.

On a alors $L = \sum_{j=0}^n b_j \prod_{i \neq j} \frac{X - \alpha_i}{\alpha_j - \alpha_i}$.

2) Aspect analytique:

Définition 8: On définit le polynôme dérivé de P par $P'(X) = \sum_{i=1}^n i a_i X^{i-1}$

Exemple 9: Si $Q = X^2 + X + 1$, $Q'(X) = 2X + 1$ sur $\mathbb{R}[X]$.

Définition 10: $\alpha \in K$ est une racine multiple nulle, si $P \in K[X]$, on

dit que $\alpha \in K$ est une racine de P de multiplicité (analytique)

$k \in \mathbb{N}^*$.

Exemple 11: Soit $P(X) = X^2 + 1$ sur $\mathbb{C}[X]$. On a $P'(X) = 2X$.

On voit que 0 est une racine multiple nulle de P de multiplicité 2.

Exemple 12: Soit $P(X) = X^2 + 1$ sur $\mathbb{R}[X]$. On a $P'(X) = 2X$.

On voit que 0 est une racine multiple nulle de P de multiplicité 2.

manque localisation des racines

Exemples et applications

Exemple 1: Soit $P(X) = X^2 + 1$ sur $\mathbb{R}[X]$. On a $P'(X) = 2X$.

Contre-exemple 1: Soit $P(X) = X^2 + 1$ sur $\mathbb{R}[X]$. On a $P'(X) = 2X$.

Définition 12: Le degré d'un monôme $a X^i$, $a \in A$, est i .

Le degré d'un polynôme $P(X) = \sum_{i=0}^n a_i X^i$ est $\max\{i \mid a_i \neq 0\}$.

On note $\deg(P)$ le degré d'un polynôme.

3) Lien avec l'irréductibilité:

Définition 13: Soit $P \in A[X]$. On dit que P est irréductible sur $A[X]$ si

$P = QR \Rightarrow Q$ ou $R \in A[X]^*$.

Proposition 14: Si P est irréductible sur $A[X]$, P n'a pas de racine sur A .

Contre-exemple 15: $P(X) = X^2 + 1$ est irréductible sur $\mathbb{R}[X]$ sans avoir

de racine sur $\mathbb{R}$.

Proposition 16: Si $P \in A[X]$ est de degré ≤ 3 , P est irréductible ssi

P n'a pas de racine sur A .

Exemples 17: 1) $X^2 + X + 1$ est irréductible sur $\mathbb{Z}[X]$.

2) $X^3 + X^2 + 1$ est irréductible sur $\mathbb{F}_2[X]$.

II) Fonctions symétriques

Définition 18: Un polynôme $P(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$ est dit

symétrique lorsque $\forall \sigma \in S_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Exemple 19: Dans $\mathbb{R}[X_1, X_2]$, le polynôme $X_1^2 + X_2^2 + X_1 + X_2$ est

symétrique.

Définition 20: $\forall k \in [1, n]$, le k -ième polynôme symétrique élémentaire

noté σ_k , est défini par $\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}$.

Propriété 21: (Relation coefficients racines) Soit $P \in A[X]$ un polynôme

scindé en facteurs linéaires: $P(X) = X^n + \sum_{i=1}^n a_i X^{n-i} = \prod_{i=1}^n (X - \lambda_i)$.

On a alors $\sigma_k = (-1)^k a_k$.

Exemple 22: Soit $P(X) = X^2 + 1$ sur $\mathbb{R}[X]$. On a $\sigma_1 = 0$ et $\sigma_2 = 1$.

Exemple 23: Soit $P(X) = X^3 + 1$ sur $\mathbb{C}[X]$. On a $\sigma_1 = 0$, $\sigma_2 = 0$ et $\sigma_3 = 1$.

alors $\forall k \in \{0, 1, \dots, n-1\}$, $\alpha_k = (-1)^{n-k} \sigma_{n-k}(\lambda_1, \dots, \lambda_n)$.

Exemple 22: $X^2 + aX + b = (X - \lambda_1)(X - \lambda_2)$
 $= X^2 - \sigma_1(\lambda_1, \lambda_2)X + \sigma_2(\lambda_1, \lambda_2)$

Théorème 23: Soit $(P_k)_{k \geq 0} \subset \mathbb{C}[X]$ une suite de polynômes complexes de degré n , soit $P \in \mathbb{C}[X]$ de degré n . Soient $(\lambda_i)_{i \in \{1, \dots, n\}}$ et $(\lambda_i)_{i \in \{1, \dots, n\}}$ les racines de P et P_k , respectivement de P simple avec multiplicité.

Alors: - si $V \in \mathbb{C}[1, n]$, $(\lambda_i)_{i \in \{1, \dots, n\}} \rightarrow \lambda_i$, alors $P_k \rightarrow P$ $\xrightarrow{k \rightarrow \infty}$

- si $(P_k)_{k \geq 0} \xrightarrow{k \rightarrow \infty} P$, on peut réécrire les $(\lambda_i)_{i \in \{1, \dots, n\}}$ de manière à ce que la suite $(\lambda_i)_{i \in \{1, \dots, n\}} \xrightarrow{k \rightarrow \infty} \lambda_i$ $\forall i \in \{1, \dots, n\}$.

Théorème 24: Si $P \in \mathbb{C}[X_1, \dots, X_n]$ est symétrique, $\exists! Q \in \mathbb{A}[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = Q(\sigma_1, \dots, \sigma_n)$.

Définition 25: $\forall i \in \{1, \dots, n\}$, on note $S_i = \sum_{j=1}^n X_j^i$ la i -ième somme de Newton.

Propriété 26 (Formule de Newton) $\forall i \in \{1, \dots, n\}$,

$$S_i - \sigma_1 S_{i-1} - \dots - (-1)^{i-1} \sigma_{i-1} S_1 + (-1)^i i \sigma_i = 0.$$

Exemple 27: $X_1^2 + X_2^2 + X_3^2 = \sigma_1^2 - 2\sigma_2$.

III) Applications en théorie des corps.

1) Généralités

Lemme 28: Soient $K \subseteq L \subseteq M$ des corps, $(\sigma_i)_{i \in I}$ une base de M sur K , $(\tau_j)_{j \in J}$ une base de M sur L . Alors la famille $(\sigma_i \tau_j)_{(i,j) \in I \times J}$ est une base de M sur K .

En particulier, si les degrés sont premiers, $[M:K] = [M:L][L:K]$.

Définition 29: Soit Q un polynôme irréductible sur $K[X]$. Soit α une racine de Q dans une extension de K telle que

$\exists \alpha \in L$ tel que $Q(\alpha) = 0$ et $L = K(\alpha)$.

Proposition 30: Il y a existence et unicité d'isomorphisme entre les corps de rupture.

Exemple 31: ① est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}[X]$. $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$.

Définition 32: Si L est une extension de K , $\alpha \in L$. On dit que α est algébrique sur K lorsque $\exists Q \in K[X]$ tel que $Q(\alpha) = 0$. Sinon, α est dit transcendant.

Théorème 33: Soient $K \subseteq L$ une extension et $\alpha \in L$. L.A.S.S.E.

1) α est algébrique sur K

2) $K[\alpha] = K(\alpha)$

3) $\dim_K K[\alpha] < +\infty$.

Exemple 34: $\sqrt{2}$ est algébrique sur $\mathbb{Q}$

π est transcendant sur $\mathbb{Q}$ (ADAMS).

Théorème 35: Soit $K \subseteq L$ une extension et $\alpha \in L$

$M = K(\alpha) \subseteq L$, α est algébriquement indépendant sur K

alors M est un corps - corps $\mathbb{R}$.

De plus, si α est algébriquement indépendant sur K et $\beta \in L$.

Définition 36: on dit que K est algébriquement clos lorsque tous les polynômes sur K sont scindés.

Théorème 37: (Valeurs propres) $\mathbb{C}$ est algébriquement clos.

2) Les corps finis

Proposition 38: Soit M fini, $|M| = p^n$ où p premier et $n \in \mathbb{N}^*$.

Théorème 39: $\forall q = p^n$, il existe un unique corps de cardinal q à isomorphisme près, noté $\mathbb{F}_q$. C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Théorème 40: $\mathbb{F}_{p^n}$ est cyclique isomorphe à $\mathbb{Z}/(n-1)\mathbb{Z}$.

Proposition 41: Soit $p \geq 2$, $x \in \mathbb{F}_q^{\times}$ avec $x^{\frac{q-1}{2}} = 1$

Corollaire 42: $(-1) \in \mathbb{F}_q^{\times^2}$ si et seulement si $q \equiv 1 \pmod{4}$

Notations 43: $V_n \subset \mathbb{N}^p$, $\forall q = p^n$, $A(n, q) = \{P \in \mathbb{F}_q[X] \text{ irréductibles de deg } n \text{ et unitaires}\}$
 $I(n, q) = \#(A(n, q))$.

Lemme 44: $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d, q)} P$

Théorème 45: $I(n, q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$ où μ est la fonction de Möbius
 En particulier $I(n, q) \geq 1 \forall n \in \mathbb{N}^*$, et $I(n, q) \sim \frac{1}{n} q^n$.

IV) Application à la cyclotomie.

Définition 46: Une racine n -ième primitive de l'unité est un élément $\zeta_n \in \mathbb{C} \setminus \mathbb{R}$ (corps de décomposition de $X^n - 1$ sur $\mathbb{C}$) tel que $\zeta_n^n = 1$ et $\forall k < n$, $\zeta_n^k \neq 1$.

Définition 47: Le n -ième polynôme cyclotomique $\Phi_n, n \in \mathbb{N}^*(x)$ est défini par $\Phi_{n, \mathbb{Q}} = \prod_{\zeta \in \mu_n^*(\mathbb{C})} (x - \zeta)$

Proposition 48: On a $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d \mid n} \Phi_d$.

Exemple 49: $\Phi_3 = x^2 + x + 1$, $\Phi_4 = x^2 + 1$, $\Phi_5 = x^4 + x^3 + x^2 + x + 1$...

Proposition 50: 1) $\forall n \in \mathbb{N}^*$, $\Phi_n, \mathbb{Q} \in \mathbb{Z}[X]$.

2) Soit $\sigma: \mathbb{Z} \rightarrow \mathbb{C}$ l'endomorphisme canonique, alors $\Phi_n, \mathbb{Q} = \sigma(\Phi_n, \mathbb{Q})$ (permet d'obtenir $\Phi_n, \mathbb{F}_p$).

Théorème 51: Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$ (Lemme sur $\mathbb{Q}$)
Application 52: (Gauss) Tout corps fini est commutatif.

IV) Réduction d'endomorphismes

Est un $\mathbb{K}$ -en- de dimension finie,

Théorème 53: Soit $\mathcal{B}$ une base de $\mathcal{E}$, $u \in \mathcal{L}(\mathcal{E})$ et $H = \text{mat}_{\mathcal{B}}(u)$.

On note $\chi_A = \chi_u = \det(XI_n - A)$.

Les valeurs propres de A sont exactement les racines de χ_A .

Lemme 54: (des racines) Soit $u \in \mathcal{L}(\mathcal{E})$ et soit $(P_j)_{1 \leq j \leq n}$ les polynômes de $\mathbb{K}[X]$ deux à deux premiers entre eux. On note $P = \prod_{j=1}^n P_j$. Alors $\text{ker}(P(u)) = \bigoplus_{j=1}^n \text{ker}(P_j(u))$

Théorème 55: Les assertions suivantes sont équivalentes:

- 1) $u \in \mathcal{L}(\mathcal{E})$ est irréductible
- 2) Il n'y a pas de polynôme annulateur de u strictement inférieur à χ_u
- 3) Πu est strictement irréductible.

Théorème 56: Les assertions suivantes sont équivalentes:

- 1) L'endomorphisme u est irréductible
- 2) $\exists P \in \mathbb{K}[X]$ tel que $P(u) = 0$ et tel que P est strictement inférieur à χ_u .
- 3) Πu est strictement irréductible.

Théorème 57: (Dandorf) Soit $u \in \mathcal{L}(\mathcal{E})$ tel que χ_u est irréductible sur $\mathbb{K}$.

1) $(1, n) \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que 1) u est irréductible sur $\mathbb{K}$

2) u est nilpotent

3) $u + u^2 = u$

4) u et u commutent,

de plus, 1 et 2 et 3 et 4 sont équivalents.