144

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

Dans cette leçon, K désigne un corps commutatif. Soit $P \in K[X]$. Soit L/K une extension de K.

I - Racines d'un polynôme

[Rb] 362 **Def 1** : On dit que $\alpha \in L$ est une racine de P si $P(\alpha) = 0$.

On note $Z_L(P)$ l'ensemble des racines de P dans L.

Ex 2 : Soit $P = (X^2-2)(X^2+1) \in \mathbb{Q}[X]$. On a $Z_{\mathbb{Q}}(P) = \emptyset$, $Z_{\mathbb{R}}(P) = \{\pm\sqrt{2}\}$, $Z_{\mathbb{Q}(i)}(P) = \{\pm i\}$ et $Z_{\mathbb{C}}(P) = \{\pm\sqrt{2}, \pm i\}$.

[Rb] 362 **Prop 2** : $\forall \alpha \in K$, $\quad P(\alpha) = 0 \iff \exists Q \in K[X] : P = (X-\alpha)Q$

A - Multiplicité d'une racine

[Rb] 362 **Def 3** : La *multiplicité* de $\alpha \in K$ (dans P) est :

$$\mu_P(\alpha) := \max\{r \in \mathbb{N} \mid \exists Q \in K[X] : P = (X-\alpha)^r Q,\ Q(\alpha) \neq 0\}$$

On dit que α est (une racine) *simple* si $\mu_P(\alpha) = 1$, *double* si $\mu_P(\alpha) = 2$, *triple* si $\mu_P(\alpha) = 3$, etc.

Rq 4 : $\forall \alpha \in K$, $\quad \mu_P(\alpha) = 0 \iff P(\alpha) \neq 0$.

[Rb] 366 **Thm 5** (Formule de TAYLOR) : Supposons que $\mathrm{car}(K) = 0$.

$$\forall P \in K[X],\quad \forall a \in K,\qquad P(X) = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

[Rb] 366 **Prop 6** : Soit $\alpha \in K$. Les assertions suivantes sont équivalentes :

1▸ α est de multiplicité r dans P

2▸ $(X-\alpha)^r \mid P$ et $(X-\alpha)^{r+1} \nmid P$ (dans $K[X]$)

3▸ (Si $\mathrm{car}(K) = 0$) $\forall k \in [\![0, r-1]\!]$, $P^{(k)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$.

Rq 7 : Le point 3▸ est faux si $\mathrm{car}(K) > 0$: voir $P = X^p$ $(P' = 0)$.

Cor 8 : Si $P \neq 0$, alors $\deg(P) \geq \sum_{\alpha \in Z_K(P)} \mu_P(\alpha)$. Si $\deg(P) \leq n$ et si P a (au moins) $n+1$ racines comptées avec leurs multiplicités, alors $P = 0$.

Rq 9 : C'est faux si K est seulement un anneau : $\bar{4}X \in \mathbb{Z}/8\mathbb{Z}[X]$ est de degré 1 mais $\bar{4}\cdot\bar{0} = \bar{4}\cdot\bar{2} = \bar{4}\cdot\bar{4} = \bar{0}$.

B - Polynômes scindés. Irréductibilité.

Def 10 : On dit que P est *scindé sur K* si P est constant ou s'il existe $(\alpha_1, \dots, \alpha_n) \in K^n$ et $\lambda \in K$ tels que $P = \lambda(X-a_1)\cdots(X-a_n)$, autrement dit si $\deg(P) = \sum_{\alpha \in Z_K(P)} \mu_P(\alpha)$. [Go] 63

Ex 11 : $X^2+1 = (X+i)(X-i)$ est scindé sur $\mathbb{C}$ ou sur $\mathbb{Q}(i)$, mais pas sur $\mathbb{R}$.

Def 12 : On dit que K est *algébriquement clos* si tout polynôme de $K[X]$ est scindé sur K. [P] 67

Thm 13 (de D'ALEMBERT-GAUSS) : $\mathbb{C}$ est algébriquement clos. [P] 68

Prop 14 : Si $\deg(P) \in \{2, 3\}$, alors P est irréductible sur K si, et seulement si P n'a pas de racine. [Rb] 371

Rq 15 : C'est faux si $\deg(P) \geq 4$: considérer $(X^2+1)^2 \in \mathbb{R}[X]$. [P] 76

C - Localisation des racines

Thm 16 (Disques de GERSCHGÖRIN) : Soient $A = (a_{i,j})_{i,j} \in \mathcal{M}_n(\mathbb{C})$ et $\lambda \in Sp(A)$. [Rb] 651

Il existe $i \in [\![1, n]\!]$ tel que $|\lambda - a_{ii}| \leq \sum_{j \neq i} |a_{i,j}|$ FIGURE

(Plus de détails dans la partie II.C : Réduction des endomorphismes).

Thm 17 (de GAUSS-LUCAS) : Soit $P \in \mathbb{C}[X]$ non constant. DEV 1

$$Z_{\mathbb{C}}(P') \subset \mathrm{Conv}(Z_{\mathbb{C}}(P))$$

où, si $Z_{\mathbb{C}}(P) = \{\alpha_1, \dots, \alpha_r\}$, alors : [FGN] 229

$$\mathrm{Conv}(Z_{\mathbb{C}}(P)) = \left\{\sum_{k=1}^r \lambda_k \alpha_k \ :\ (\lambda_1, \dots, \lambda_r) \in [0,1]^r,\ \sum_{k=1}^r \lambda_k = 1\right\}$$

Appli 18 : 7 est le plus grand entier $n \geq 2$ tel que :

$$Z_{\mathbb{C}}((X+1)^n - X^n - 1) \in \{z \in \mathbb{C} \mid |z| = 1\}$$

[FGN] 213 [S] 573

> **Thm 19** (de KRONECKER) : Soit $P\in\mathbb{Z}[X]$ unitaire dont les racines complexes sont dans le disque unité, et tel que $P(0)\neq 0$. Alors les racines complexes de P sont des racines de l'unité. DEV 2.a

II – Fonctions symétriques en les racines

A – Polynômes symétrique élémentaires

[Rb] 55 [S] 559 **Def 20** : On dit que $A\in K[X_1,\dots,X_n]$ est symétrique si :
$$\forall\sigma\in\mathfrak{S}_n,\quad A(X_{\sigma(1)},\dots,X_{\sigma(n)})=A(X_1,\dots,X_n)$$

[Rb] 55 [S] 558 **Def 21** : Pour $k\in\mathbb{N}^*$, on définit le k^e *polynôme symétrique élémentaire*
$$\sigma_k(X_1,\dots,X_n)=\sum_{1\le i_1<\dots<i_k\le n} X_{i_1}\cdots X_{i_k}$$

[Rb] 55 [S] 559 **Thm 22** : Pour tout $A\in K[X_1,\dots,X_n]$ symétrique, il existe un unique $B\in K[X_1,\dots,X_n]$ tel que $A(X_1,\dots,X_n)=B(\sigma_1(X_1,\dots,X_n),\dots,\sigma_n(X_1,\dots,X_n))$.

[Rb] 368 [S] 559 **Thm 23** (relations coefficients-racines) : Supposons que P est scindé, écrivons
$$P=a_n(X-\alpha_1)\cdots(X-\alpha_n)=a_nX^n+a_{n-1}X^{n-1}+\dots+a_1X+a_0$$
On a alors $\forall k\in[\![0,n-1]\!]$, $a_k=(-1)^k\dfrac{\sigma_k(\alpha_1,\dots,\alpha_n)}{a_n}$.

Ex 24 : $P=X^3-X^2+2X+1$. On a :
$$\alpha^3+\beta^3+\gamma^3=(\alpha+\beta+\gamma)^3+3\alpha\beta\gamma-3(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\alpha\gamma)=-8$$

B – Discriminant

[S] 567-569 **Def 25** : Supposons qu'il existe $\lambda\in K$ et $(a_1,\dots,a_n)\in L^n$ tels que $P=\lambda\prod_{k=1}^{n}(X-a_k)$. Le discriminant de P sur K est :
$$\mathrm{disc}(P):=\lambda^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2=(-1)^{\frac{n(n-1)}{2}}\lambda^{2n-2}\prod_{i\neq j}(\alpha_i-\alpha_j)$$

Rq 26 : Il existe (un unique) $Q\in K[X_1,\dots,X_n]$ tel que :
$$\mathrm{disc}(P)=Q(\sigma_1(\alpha_1,\dots,\alpha_n),\dots,\sigma_n(\alpha_1,\dots,\alpha_n))$$

[S] 569 **Prop 27** : $\mathrm{disc}(P)=0 \iff P$ a une racine multiple

Ex 28 : $\forall(a,b,c)\in K^3$, $\mathrm{disc}(aX^2+bX+c)=b^2-4ac$.

III – Quelques applications

A – Corps de rupture et de décomposition

Soit $P\in K[X]$ non constant et irréductible sur K.

[P] 70-71 **Def 29** : • On dit que L est un corps de rupture de P sur K s'il existe $\alpha\in L$ tel que $P(\alpha)=0$ et $L=K(\alpha)$.

• On dit que L est un corps de décomposition de P sur K s'il existe $(\alpha_1,\dots,\alpha_n)\in L^n$ tel que $L=K(\alpha_1,\dots,\alpha_n)$ et P est scindé sur L (qui est encore défini si P n'est pas irréductible).

[P] 70-71 **Thm 30** : • P admet un unique corps de rupture à K-isomorphisme près. Plus précisément, $K[X]/\langle P\rangle$ est un corps de rupture de P sur K.

• P admet un unique corps de décomposition à K-isomorphisme près.

[P] 72 **Ex 31** : Pour $P=X^3-2\in\mathbb{Q}[X]$:
- $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$ sont des corps de rupture de P sur $\mathbb{Q}$.
- $\mathbb{Q}(j,\sqrt[3]{2})$ est un corps de décomposition de P sur $\mathbb{Q}$

Rq 32 : On peut donc parler des racines de P, sans préciser le corps, qui est alors implicitement un corps de décomposition de P. On note $Z(P)$ l'ensemble des racines de P. En particulier, si $\deg(P)\geq 1$, alors $\deg(P)=\sum_{\alpha\in Z(P)}\mu_P(\alpha)$.

B – Éléments algébriques

[P] 66 **Def 33** : Soit $\alpha\in L$. On dit que α est *algébrique sur K* s'il existe $P\in K[X]\setminus\{0\}$ tel que $P(\alpha)=0$. Sinon, on dit que α est *transcendant*.

[P] 66 **Def 34** : Soit $\alpha\in L$ algébrique sur K. L'ensemble $I_\alpha:=\{P\in K[X]\mid P(\alpha)=0\}$ est un idéal de $K[X]$, appelé idéal annulateur de α. Son unique générateur unitaire, noté $P_{\alpha,K}$, est appelé polynôme minimal de α sur K.

Ex 35 : $\alpha = \sqrt{1+\sqrt{3}}$ est algébrique sur $\mathbb{Q}$, $P_{\alpha,\mathbb{Q}} = X^4 - 2X^2 - 2$.

B - Réduction des endomorphismes

Soient $n \in \mathbb{N}^*$ et $A \in \mathcal{M}_n(K)$.

[M²] 54 [Rb] 604 Def 36 : • Le polynôme caractéristique de A est $\chi_A := \det(XI_n - A) \in K[X]$
• L'ensemble $I_A := \{P \in K[X] \mid P(A) = 0\}$ est un idéal non nul de $K[X]$, appelé idéal annulateur de A. Son unique générateur unitaire, noté π_A, est appelé polynôme minimal de A.

[M²] 81 [S] 569 Thm 37 (de Cayley - Hamilton) : $\chi_A(A) = 0$.

[Rb] 605 644 Prop 38 : $Z_K(\chi_A) = Z_K(\pi_A) = Sp_K(A)$

[M²] 55 Cor 39 : Si K est algébriquement clos, alors $Sp_K(A) \neq \emptyset$.

[M²] 56 Prop 40 : $\sum_{\lambda \in Z(\chi_A)} \mu_{\chi_A}(\lambda) \cdot \lambda = Tr(A)$ et $\prod_{\lambda \in Z(\chi_A)} \lambda^{\mu_{\chi_A}(\lambda)} = \det(A)$

Cor 41 : Si $\chi_A = \sum_{k=1}^{n} a_k X^k$, alors $a_0 = (-1)^n \det(A)$ et $a_{n-1} = -Tr(A)$ (et $a_n = 1$).

Ex 42 : Pour $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$: $\chi_A = \pi_A = X^2 + 1$, $Sp_{\mathbb{C}}(A) = \{\pm i\}$.

[Rb] 683 Thm 43 : Les assertions suivantes sont équivalentes :
1• A est diagonalisable
2• π_A est scindé à racines simples
3• Pour tout $\lambda \in Sp_K(A)$, $\mu_{\chi_A}(\lambda) = \dim(Ker(\lambda I_n - A))$.

Rq 44 : $\mu_{\chi_A}(\lambda)$ est appelée multiplicité algébrique de λ, et $\dim(Ker(\lambda I_n - A))$ est appelée multiplicité géométrique de λ.

[M²] 90 Cor 45 : Si χ_A est scindé à racines simples, alors A est diagonalisable.

D - Polynômes cyclotomiques

Soit $n \in \mathbb{N}^*$. L'ensemble $\mathbb{U}_n := \{z \in \mathbb{C} \mid z^n = 1\}$ est un groupe, dit des racines n-ièmes de l'unité. On note μ_n^* l'ensemble des générateurs de $\mathbb{U}_n$.

Prop 46 : $\mathbb{U}_n = \{\omega_n^k : 1 \leq k \leq n\}$, $\mu_n^* = \{\omega_n^k : k \wedge n = 1\}$ où $\omega_n = e^{i\frac{2\pi}{n}}$.

Def 47 : Le n^e polynôme cyclotomique est $\Phi_n := \prod_{\xi \in \mu_n^*} (X - \xi)$. [P] 80 [Rb] 385

Ex 48 : Pour p premier, $\Phi_p = X^{p-1} + X^{p-2} + \dots + X + 1$. [P] 81
$\Phi_1 = X - 1$, $\Phi_4 = X^2 + 1$, $\Phi_6 = X^2 - X + 1$, $\Phi_8 = X^4 + 1$

Prop 49 : $X^n - 1 = \prod_{d \mid n} \Phi_d$ [P] 80-83 [Rb] 386

Prop 50 : $\Phi_n \in \mathbb{Z}[X]$, il est irréductible sur $\mathbb{Q}$ (c'est le polynôme minimal de ω_n sur $\mathbb{Q}$). [P] 82-83 [Rb] 392

Prop 51 (Kronecker) : Soit $P \in \mathbb{Z}[X]$ unitaire irréductible sur $\mathbb{Q}$. Si les racines complexes de P sont dans le disque unité, alors $P = X$ ou il existe $k \in \mathbb{N}^*$ tel que $P = \Phi_k$. [Go] 95

DEV 2.b

Références

[Rb] Rombaldi
[P] Perrin
[Go] Gourdon
[FGN] Oraux X-ENS, Algèbre 1 [2e édition]
[S] Szpirglas

FIGURE

$$A = \begin{pmatrix} 2 & 0 & -2+i \\ 0 & i & 0 \\ i & 0 & -1-i \end{pmatrix}, \quad Sp(A) = \{1, i, -2-i\}$$