Cadre : $\mathbb{K}$ est un corps commutatif

I Racines d'un polynôme

1) Définitions et premières propriétés

Définition 1. Pour $P \in \mathbb{K}[X]$, on dit que $a \in \mathbb{K}$ est racine de P si $(X-a)$ divise P dans $\mathbb{K}[X]$.

Exemple 2. *1 et -1 sont racines de* $X^2 - 1$.

Proposition 3. *Les racines de* $P \in \mathbb{K}[X]$ *dans* $\mathbb{K}$ *sont exactement les éléments* $a \in \mathbb{K}$ *tels que* $P(a) = 0$.

Exemple 4. *Les racines de* $X^n - 1$ *sont les racines n-ièmes de l'unité.*

Définition 5. On dit que $a \in \mathbb{K}$ est racine de $P \in \mathbb{K}[X]$ d'ordre $k \in \mathbb{N}^\star$ si $(X-a)^k$ divise P et $(X-a)^{k+1}$ ne le divise pas.

Proposition 6. *Si* $P \in \mathbb{K}[X]$ *est de degré n, alors P a au plus n racines dans* $\mathbb{K}$.

Remarque 7. *Ceci est faux si* $\mathbb{K}$ *n'est qu'un anneau : Dans* $M_2(\mathbb{R})$, X^2 *admet toutes les matrices de la forme* $\left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right)$ *comme racine, soit une infinité.*

Corollaire 8. *Si* $\mathbb{K}$ *est infini, il y a bijection entre les polynômes et les fonctions polynomiales associées.*

Théorème 9. *On suppose* $\mathbb{K}$ *de caractéristique nulle. Soit* $P \in \mathbb{K}[X]$ *non nul. Alors* $a \in \mathbb{K}$ *est racine d'ordre* $k \in \mathbb{N}^\star$ *de P si, et seulement si :*

$$\forall\, i \in [\![0, k-1]\!],\ P^{(i)}(a) = 0 \quad et \quad P^{(k)}(a) \neq 0$$

Remarque 10. *Le résultat précédent est vrai en caractéristique quelconque, mais seulement pour les racines simples.*

Corollaire 11. *Soient* $a_1, \dots, a_n \in \mathbb{K}$ *deux à deux distincts. L'application suivante est un isomorphisme d'espace vectoriel :*

$$\varphi : \left| \begin{array}{ccc} \mathbb{K}_{n-1}[X] & \longrightarrow & \mathbb{K}^n \\ P & \longmapsto & (P(a_i))_{i \in [\![1,n]\!]} \end{array} \right.$$

Remarque 12. *L'antécédent d'un n-uplet est le polynôme interpolateur de Lagrange associé à ce n-uplet.*

Définition 13. On dit que $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$ si on peut écrire :

$$P(X) = \lambda \prod_{i=1}^{r} (X - a_i)^{m_i} \quad \text{avec} \quad m_i \in \mathbb{N}^\star, a_i \in \mathbb{K}, \lambda \in \mathbb{K}$$

Remarque 14. *Deux polynômes scindés sont premiers entre eux si, et seulement si, ils n'ont aucune racine commune.*

Définition 15. Soit $P \in \mathbb{K}[X]$. On dit que P est irréductible sur $\mathbb{K}[X]$ lorsque P n'est pas constant et si $P = QR$, avec $Q, R \in \mathbb{K}[X]$, implique que soit Q soit R est constant.

Proposition 16. *On se place dans* $\mathbb{K}[X]$, *alors :*

(i) Tout polynôme de degré 1 est irréductible.

(ii) Tout polynôme irréductible de degré 2 ou plus n'a pas de racine dans $\mathbb{K}$.

Remarque 17. $(X^2+1)^2$ *est de degré 4 et n'a pas de racine dans* $\mathbb{R}$ *mais, n'est pas irréductible sur* $\mathbb{R}$.

Théorème 18 (D'Alembert-Gauss)**.** *Tout polynôme non constant de* $\mathbb{C}[X]$ *admet une racine dans* $\mathbb{C}$.

Application 19. *Toute matrice à coefficients complexes est trigonalisable.*

Corollaire 20. *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré 1. Ceux de* $\mathbb{R}[X]$ *sont les polynômes de degré 1 et ceux de degré 2 sans racine.*

2) Corps de rupture, de décomposition

Définition 21. Soit $P \in \mathbb{K}[X]$ irréductible. Une extension monogène $\mathbb{L}$ de $\mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ si elle est engendré par $\mathbb{K}$ et par une racine α de P.

Remarque 22. $\mathbb{L}$ *est alors une extension de* $\mathbb{K}$ *de degré le degré de P.*

Exemple 23. *Si P est de degré 1,* $\mathbb{K}$ *est un corps de rupture de P.*

Théorème 24. *Tout polynôme irréductible sur* $\mathbb{K}$ *admet un corps de rupture, qui est unique à* $\mathbb{K}$*-isomorphisme près.*

Exemple 25. $\mathbb{C}$ *est le corps de rupture de* $X^2 + 1$ *sur* $\mathbb{R}$.

Exemple 26. *Le corps de rupture de X^2+X+1 sur $\mathbb{F}_2$ est un corps à 4 éléments.*

Corollaire 27. *Pour tout polynôme sur $\mathbb{K}$, il existe une extension de $\mathbb{K}$ dans laquelle il admet au moins une racine.*

Définition 28. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit $P \in \mathbb{K}[X]$ de degré n. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si P est scindée sur $\mathbb{L}[X]$, et si $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$ avec $\alpha_k \in \mathbb{L}$ des racines de P.

Remarque 29. *Un corps de décomposition est une extension finie.*

Exemple 30. $\mathbb{K}$ *est corps de décomposition de tout polynôme de degré 1.*

Exemple 31. $\mathbb{C}$ *est un corps de décomposition de tout polynôme réel irréductible de degré 2.*

Exemple 32. $\mathbb{Q}[\sqrt{2}]$ *est un corps de décomposition de X^2-2 sur $\mathbb{Q}$.*

Théorème 33. *Soit $P \in \mathbb{K}[X]$ de degré $n \geqslant 1$. Alors il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près, de degré au plus $n!$.*

Exemple 34. $\mathbb{Q}[\sqrt[3]{2}]$ *est un corps de rupture de X^3-2 sur $\mathbb{Q}$, mais ce n'est pas un corps de décomposition.*

Théorème 35. *Soient p un nombre premier, $\alpha, n \in \mathbb{N}^\star$ et $q = p^\alpha$. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes unitaires irréductibles de degré d sur $\mathbb{F}_q$. Alors :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$$

Proposition 36 (Inversion de Möbius)**.** *On note μ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d|n} g(d)$. Alors :*

$$\forall\, n \in \mathbb{N}^\star,\ g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

Corollaire 37. *Si $I(q,d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

$$I(q,n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{+\infty}{\sim} \frac{q^n}{n}$$

II Fonctions symétriques élémentaires

Ici, A désigne un anneau commutatif unitaire intègre, et soit $n \in \mathbb{N}^\star$.

1) Définitions et premières propriétés

Définition 38. Le groupe symétrique $\mathfrak{S}_n$ agit sur $A[X_1, \dots, X_n]$ par :

$$\begin{array}{ccc} \mathfrak{S}_n \times A[X_1, \dots, X_n] & \longrightarrow & A[X_1, \dots, X_n] \\ (\sigma, P(X_1, \dots, X_n) & \longmapsto & P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \end{array}$$

Les points fixes sous cette action, notés $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$, sont appelés polynômes symétriques à n variables.

Exemple 39. *Tout polynôme à une variable est symétrique.*

Définition 40. Pour tous $n \in \mathbb{N}^\star$ et $k \in [\![0, n-1]\!]$, les polynômes suivants sont symétriques, et sont appelés polynômes symétriques élémentaires :

$$\Sigma_k = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} X_{i_1} \dots X_{i_k}$$

Théorème 41. *Soit $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$ où $a_n \neq 0$. Dans un corps de décomposition de P, $P(X) = a_n(X-\alpha_0)\dots(X-\alpha_n)$. Alors :*

$$a_k = a_n (-1)^n \Sigma_{n-k+1}(\alpha_0, \dots, \alpha_n)$$

C'est une équivalence.

Application 42. *Le déterminant d'une matrice (resp. sa trace) est un coefficient de son polynôme caractéristique, produit (resp. somme) de ses valeurs propres dans une clôture algébrique.*

Proposition 43 (Formules de Newton)**.** *On pose $S_k = \sum_{i=1}^n X_i^k$, alors :*

(i) $\forall\, k \in [\![1, n]\!],\ \sum_{i=0}^k (-1)^i \Sigma_i S_{k-i} = 0$, *avec* $\Sigma_0 = 1$.

(ii) $\forall\, k \geqslant n,\ \sum_{i=0}^n (-1)^i \Sigma_i S_{k-i} = 0$

Application 44. *Une matrice $A \in M_n(\mathbb{K})$ est nilpotente d'ordre n si, et seulement si, pour tout $k \in [\![1, n]\!]$, $\mathrm{tr}(A^k) = 0$.*

2) Structure des polynômes symétriques

Définition 45. Soit $X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in A[X_1, \dots, X_n]$ un monôme. On définit son poids comme $\sum_{k=1}^{n} k\alpha_k$. On appelle poids d'un polynôme $P \in A[X_1, \dots, X_n]$ le maximum des poids des monômes dont il est la somme. Par convention, on pose que le poids de 0 est $-\infty$.

Exemple 46. *Le poids de Σ_k est $nk - \frac{k(k-1)}{2}$.*

Théorème 47. *Soit $P \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$. Il existe un unique $Q \in A[X_1, \dots, X_n]$ tel que $P = Q(\Sigma_1, \dots, \Sigma_n)$. Autrement dit, tout polynôme symétrique est polynôme en les polynômes symétriques élémentaires. De plus, le poids de Q est le degré de P.*

Exemple 48. *Dans $A[X, Y]$, $X^2 + Y^2 = (X + Y)^2 - 2XY$.*

III Applications

1) Polynômes cyclotomiques

Définition 49. Soit $n \in \mathbb{N}^\star$, on définit $\Phi_n \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\xi \in \mu_n^\star} (X - \xi)$, où $\mu_n^\star \subset \mathbb{C}$ désigne les racines primitives n-ième de l'unité.

Proposition 50. *Pour $n \in \mathbb{N}^\star$, Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 51. *Pour $n \in \mathbb{N}^\star$, $X^n - 1 = \prod_{d|n} \Phi_d(n)$*

Exemple 52. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Lemme 53. *Soient $A, B \in \mathbb{Q}[X]$ non nuls. On suppose que $P = AB \in \mathbb{Z}[X]$. Si A et P sont unitaires, alors A et B sont à coefficients entiers.*

Proposition 54. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Proposition 55. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Q}[X]$.*

2) Localisation des racines

Lemme 56. *Une matrice à coefficients complexes à diagonale dominante est inversible.*

Définition 57. Soit $A_(a_{i,j}) \in M_n(\mathbb{C})$. Le i-ième disque de Gerschgorin est le disque fermé de centre $a_{i,j}$ et de rayon $r_i = \sum_{j=1}^{n} \sum_{i \neq j} |a_{i,j}|$.

Théorème 58. *Les valeurs propres d'une matrice complexe sont situées dans la réunion des disques de Gerschgorin.*

Théorème 59 (Gauss-Lucas)**.** *Soit P un polynôme à coefficients complexes de degré au moins 2. Les racines de P' sont contenues dans l'enveloppe convexe de celles de P.*

Développements

- Étude des polynômes cyclotomiques (54,55) [Per]
- Dénombrement des polynômes irréductibles unitaires sur $\mathbb{F}_q$ (35,36,37) [Tau]

Références

[Per] Daniel Perrin. *Cours d'Algèbre.* Ellipses
[Tau] Patrice Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet