141. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Introduction : $K[X]$ étant un anneau factoriel, tout polynôme se décompose en produit d'irréductibles, ce qui justifie d'étudier cette notion.

Soit K un corps.

1 Polynômes irréductibles

1.1 Premières définitions et propriétés

Définition 1. Un polynôme $P \in K[X]$ est dit irréductible s'il est non inversible et si ses seuls diviseurs sont ses éléments associés et les éléments inversibles.

***Exemple* 2.** *Tout polynôme de degré 1 est irréductible.*

Remarque 3. L'irréductibilité d'un polynôme dépend du corps K.

***Exemple* 4.** X^2+1 *est irréductible dans* $\mathbb{Q}[X]$ *et* $\mathbb{R}[X]$ *mais pas dans* $\mathbb{C}[X]$.

Proposition 5. un polynôme de $K[X]$ irréductible n'admet pas de racine dans K.

***Contre-exemple* 6.** $(X^2+1)^2$ *n'a pas de racine mais n'est pas irréductible dans* $\mathbb{R}[X]$.

Lemme 7. Soient $P, Q \in K[X]$. Si P est irréductible, on a $P \nmid Q$ ssi $P \wedge Q = 1$.

Théorème 8. Soit $P \in K[X]$. Il existe des polynômes irréductibles $P_1, \cdots, P_r$ et $\alpha \in K$ tels que $P = \alpha P_1 \cdots P_r$, et cette décomposition est unique.

***Application* 9** (Décomposition en éléments simples)**.** *Soit* $F \in K(X)$ *de forme irréductible* $\frac{A}{B}, \deg(B) \geq 1$. *On note* $B = bQ_1^{k_1} \cdots Q_n^{k_n}$ *où les* Q_i *sont irréductibles unitaires non associés.*
Alors il existe une unique famille de $k_1 + \cdots + k_n + 1$ *polynômes* $E, (P_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq k_i}}$ *telle que* $\dfrac{A}{B} = E + \displaystyle\sum_{i=1}^{n} \sum_{j=1}^{k_i} \frac{P_{i,j}}{Q_i^j}$ *et* $\forall i, j, \deg\left(\dfrac{P_{i,j}}{Q^j}\right) < 0$.

***Application* 10** (Lemme des noyaux)**.** *Soit* E *un* K*-ev de dimension* n*, soit* $u \in \mathcal{L}(E)$*, soit* $K \in K[X]$ *de décomposition en produit d'irréductibles* $P = \alpha P_1^{m_1} \cdots P_r^{m_r}, m_1, \cdots, m_r \geq 1$. *Alors* $\ker(P(u)) = \displaystyle\bigoplus_{i=1}^{r} \ker(P_i^{m_i}(u))$.

Définition 11. Soit L/K une extension de corps, soit $a \in L$. Il est dit algébrique sur K s'il existe $P \in K[X], P(a) = 0$. On appelle polynôme minimal de a et on note π_a le polynôme unitaire de degré minimal de $K[X]$ dont a est racine.

Proposition 12. π_a est irréductible dans $K[X]$.

1.2 Adjonction de racines

Proposition 13. Soit $P \in K[X]$. Alors P est irréductible, si et seulement si, $K[X]/(P)$ est un corps.

Définition 14. Soit $P \in K[X]$ irréductible. On appelle corps de rupture de P une extension de corps L/K telle qu'il existe $\alpha \in L$ avec $P(\alpha) = 0$ et $L = K(\alpha)$.

Théorème 15. $K[X]/(P)$ est un corps de rupture de P engendré par K et $\overline{X}$, et si $L = K(\alpha), L' = K(\beta)$ sont deux corps de rupture de P, alors il existe un unique K-isomorphisme $\varphi : L \to L'$ tel que $\varphi(\alpha) = \beta$.

***Exemple* 16.** $\mathbb{C}$ *est le corps de rupture de* $P = X^2 + 1 \in \mathbb{R}[X]$.

***Exemple* 17.** $\mathbb{F}_4 \simeq \mathbb{F}_2/(X^2+X+1)$ *est le corps de rupture de* $X^2+X+1 \in \mathbb{F}_2[X]$.

Définition 18. Soit $P \in K[X]$.
On dit qu'une extension L/K est un corps de décomposition de P s'il existe $\lambda, \alpha_1, \cdots, \alpha_r \in L$ tel que sur L, $P = \lambda(X - \alpha_1) \cdots (X - \alpha_r)$ et $L = K(\alpha_1, \cdots, \alpha_r)$.

***Exemple* 19.** $\mathbb{C}$ *est un corps de décomposition de* $X^2 + 1 \in \mathbb{R}[X]$ *et* $\mathbb{Q}(j, \sqrt[3]{2})$ *est un corps de décomposition de* $X^3 - 2 \in \mathbb{Q}[X]$.

Proposition 20. Si L, L' sont deux corps de décomposition de P, alors ils sont K-isomorphes.

***Application* 21.** *Si* p *premier,* $n \in \mathbb{N}^*, q = p^n$*, le corps fini* $\mathbb{F}_q$ *est défini comme le corps de décomposition de* $X^q - X \in \mathbb{F}_p[X]$.

2 Critères d'irréductibilité

2.1 Pour un polynôme de degré 2 ou 3

Proposition 22. Soit $P \in K[X]$ avec $\deg(P) \in \{2, 3\}$. Alors P est irréductible, si et seulement si, il ne possède pas de racine.

2.2 Dans $\mathbb{R}$ ou $\mathbb{C}$

Théorème 23 (D'Alembert-Gauss)**.** Soit $P \in \mathbb{C}[X]$. Alors P possède une racine dans $\mathbb{C}$.

Corollaire 24. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Proposition 25. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

2.3 Dans $\mathbb{Q}$ et $\mathbb{Z}$

Définition 26. Soit $P \in \mathbb{Z}[X]$. On appelle contenu de P, et on note $c(P)$, le PGCD de ses coefficients. P est dit primitif si $c(P) = 1$.

***Exemple* 27.** $2X^2 + 3X + 4$ *est primitif mais* $2X^2 + 8X + 4$ *ne l'est pas.*

Proposition 28. Soient $P, Q \in \mathbb{Z}[X]$. On a $c(PQ) = c(P)c(Q)$.

Théorème 29. Soit $P \in \mathbb{Z}[X]$ primitif. Alors P est irréductible dans $\mathbb{Z}[X]$, si et seulement si, il l'est dans $\mathbb{Q}[X]$.

Théorème 30 (Eisenstein)**.** Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, soit $p \in \mathbb{N}^*$ premier. On suppose que $p \nmid a_n$, que pour tout $k \in [\![0, n-1]\!], p | a_k$ et $p^2 \nmid a_0$. Alors P est irréductible dans $\mathbb{Q}[X]$.

***Exemple* 31.** *Pour tout* $n \in \mathbb{N}^*$*, pour tout* $p \in \mathbb{N}^*$ *premier,* $X^n - p$ *est irréductible dans* $\mathbb{Q}[X]$ *et* $\mathbb{Z}[X]$*.*

***Exemple* 32.** $X^4 + X^3 + X^2 + X + 1$ *est irréductible dans* $\mathbb{Q}[X]$ *et* $\mathbb{Z}[X]$*.*

Théorème 33. Soit $P \in \mathbb{Z}[X]$, soit $p \in \mathbb{N}^*$ premier. On note $\overline{P}$ le polynôme de $\mathbb{F}_p[X]$ obtenu en réduisant les coefficients de P modulo p. Alors si $\deg(\overline{P}) = \deg(P)$ et $\overline{P}$ irréductible dans $\mathbb{F}_p[X]$, alors P irréductible dans $\mathbb{Q}[X]$.

***Exemple* 34.** $P = 3X^2 + 17X - 11$ *est irréductible dans* $\mathbb{Q}[X]$*.*

***Contre-exemple* 35.** $X^4 + 1$ *est irréductible dans* $\mathbb{Z}[X]$ *mais réductible dans* $\mathbb{F}_p[X]$ *pour tout* $p \in \mathbb{N}^*$ *premier.*

Définition 36. Soit $n \in \mathbb{N}^*$.
On définit le n-ème polynôme cyclotomique $\Phi_n = \prod_{\substack{k \wedge n = 1 \\ k \leq n}} (X - e^{2ik\pi/n})$.

Proposition 37. Pour tout $n \in \mathbb{N}^*, \Phi_n \in \mathbb{Z}[X]$ et est irréductible dans $\mathbb{Q}[X]$.

2.4 Dans un corps fini

Lemme 38. Soit $P \in \mathbb{F}_q[X], \deg(P) = n$, soit $E = \mathbb{F}_q[X]/(P)$. On a $\dim(E) = n$ et si $\phi : E \to E$ est définie par $\phi(Q) = Q^q$, ϕ est linéaire.

On note S_P la matrice de ϕ.

Algorithme 39 (Berlekamp)**.** Soit $P \in \mathbb{F}_q[X]$ unitaire sans facteur carré.

1. On calcule $S_P - I_n$ et si $r := n - \mathrm{rg}(S_p - I) = 1$, on retourne P.
2. Sinon, calculer $V \in \ker(S_p - I_n)$ non constant modulo P, et pour tout $\alpha \in \mathbb{F}_q$, calculer $D_\alpha = pgcd(P, V - \alpha)$. Appliquer l'algorithme à D_α.

Théorème 40. L'algorithme de Berlekamp termine et retourne la décomposition de P en facteurs irréductibles.

Algorithme 41. Soit $P \in \mathbb{F}_q[X]$.

1. Calculer $D = P \wedge P'$.
2. Si $D = P$, calculer R tel que $P = R^p$ et appliquer l'algorithme à R. Si $D = 1$, appliquer Berlekamp à P. Sinon, appliquer Berlekamp à P/D et retourner en 1 avec D.

Théorème 42. Cet algorithme termine et retourne la décomposition de P en facteurs irréductibles.

3 Endomorphismes semi-simples

Définition 43. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, soit $u \in \mathcal{L}(E)$. On dit que u est semi-simple si tout sous-espace stable par u admet un supplémentaire stable.

Proposition 44. u est semi-simple si les polynômes irréductibles de la décomposition de π_u sont deux à deux distincts.

Définition 45. Si E est euclidien, u est dit normal s'il commute avec son adjoint.

Proposition 46. Si $u \in \mathcal{L}(E)$ est normal, il admet une droite ou un plan stable sur lequel le polynôme minimal de l'endomorphisme induit est irréductible, et le supplémentaire est également stable.

***Application* 47.** *Réduction des endomorphismes normaux.*

Développements

— Irréductibilité des polynômes cyclotomiques.
— Algorithme de Berlekamp.

Références

[1] I. Gozard, Théorie de Galois, Ellipses.

[2] E. Ramis, C. Deschamps, J. Odoux, Cours de mathématiques spéciales - Algèbre 1, Masson.

[3] A. Szpirglas et al., Algèbre L3, Pearson.