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

Sauf mention contraire, les corps sont supposés commutatifs.

I - Irréductibilité de polynômes

1. Racines et polynômes irréductibles

Définition 1. Soit A un anneau. Un polynôme P de $A[X]$ est dit **irréductible** si $\deg(A) \geq 1$ et ses seuls diviseurs dans $A[X]$ sont les polynômes uP où $u \in A^\times$.

[GOZ] p. 8

Remarque 2. Soit $\mathbb{K}$ un corps. Alors, $\mathbb{K}[X]$ est euclidien, donc principal, donc factoriel.

Définition 3. Soient $\mathbb{L}$ un corps et $\mathbb{K}$ un sous-corps de $\mathbb{L}$. Soit $P \in \mathbb{K}[X]$.

- Une **racine** est un élément $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.
- La **multiplicité** de α comme racine de P est le plus grand $n \in \mathbb{N}$ tel que $(X-a)^n$ divise P dans $\mathbb{K}[X]$.
- La somme des multiplicités des racines de P dans $\mathbb{K}$ est inférieure ou égale à $\deg(P)$. En cas d'égalité, on dit que P est **scindé** *sur* $\mathbb{K}$ (ou *dans* $\mathbb{K}[X]$).

Proposition 4. (i) Tout polynôme de degré 1 est irréductible.

(ii) Tout polynôme irréductible de degré strictement supérieur à 1 n'a pas de racine dans $\mathbb{K}$.

Contre-exemple 5. $(X^2+1)^2$ n'a pas de racine dans $\mathbb{Q}$, mais est réductible dans $\mathbb{Q}[X]$.

Proposition 6. La réciproque de la Proposition 4 Point (ii) est vraie pour les polynômes de degré 2 ou 3.

Proposition 7. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ un polynôme de degré n tel que $a_0 \neq 0$. Si $\alpha = \frac{p}{q} \in \mathbb{Q}$ est une racine de P, en supposant $\frac{p}{q}$ irréductible, alors $p \mid a_0$ et $q \mid a_n$.

Exemple 8. $X^3 + X + 1$ n'a pas de racine dans $\mathbb{Q}$.

p. 19

2. Quelques critères d'irréductibilité

Soit A un anneau factoriel.

Définition 9. Pour tout polynôme non nul $P \in A[X]$, on appelle **contenu** de P, noté $\gamma(P)$, le PGCD des coefficients de P. P est dit **primitif** si $\gamma(P) = 1$.

p. 10

Lemme 10 (Gauss)**.** (i) Le produit de deux polynômes primitifs est primitif.

(ii) $\forall P, Q \in A[X] \setminus \{0\}, \gamma(PQ) = \gamma(P)\gamma(Q)$.

Théorème 11. Soient $\mathbb{K}$ le corps des fractions de A et $P \in A[X]$ de degré supérieur ou égal à 1. Alors, P est irréductible dans $A[X]$ si et seulement si P est irréductible dans $\mathbb{K}[X]$ et $\gamma(P) = 1$.

[DEV]

Théorème 12 (Critère d'Eisenstein)**.** Soient $\mathbb{K}$ le corps des fractions de A et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. On suppose qu'il existe $p \in A$ irréductible tel que :

(i) $p \mid a_i, \forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{K}[X]$.

Exemple 13. Soit p un nombre premier. Le polynôme $\Phi_p = \sum_{k=0}^{p-1} X^k$ est irréductible dans $\mathbb{Z}[X]$.

Application 14. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$.

[PER] p. 67

Théorème 15 (Critère d'irréductibilité modulo p)**.** Soient $\mathbb{K}$ le corps des fractions de A et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. Soit I un idéal premier de A. On pose $B = A/I$ et $\mathbb{L}$ le corps des fractions de B. On suppose $a_n \notin I$.

Si $\overline{P}$ est irréductible dans $\mathbb{L}[X]$, alors P est irréductible dans $\mathbb{K}[X]$.

[GOZ] p. 12

Exemple 16. Le polynôme $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$.

II - Adjonction de racines

Soit $\mathbb{K}$ un corps commutatif.

1. Extensions algébriques

[PER] p. 66

Définition 17. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Soit $\mathrm{ev}_\alpha : \mathbb{K}[X] \to \mathbb{L}$ le morphisme d'évaluation en α.

- On note $\mathrm{Ann}(\alpha)$ l'idéal des polynômes annulateurs de α. Notons qu'on a $\mathrm{Ann}(\alpha) = \mathrm{Ker}(\mathrm{ev}_\alpha)$.
- Si ev_α est injectif, on dit que α est **transcendant** sur $\mathbb{K}$.
- Sinon, α est dit **algébrique** sur $\mathbb{K}$.

Exemple 18.
- e et π sont transcendants sur $\mathbb{Q}$ (théorèmes d'Hermite et de Lindemann).
- $\sqrt{2}$, i, ... sont algébriques sur $\mathbb{Q}$.

Proposition 19. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Les assertions suivantes sont équivalentes.

(i) α est algébrique sur $\mathbb{K}$.
(ii) $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.
(iii) $[\mathbb{K}[\alpha] : \mathbb{K}] < +\infty$.

Proposition 20. En reprenant les notations précédentes, si α est transcendant, on a

$$\mathbb{K}[\alpha] \cong \mathbb{K}[X] \text{ et } \mathbb{K}(\alpha) \cong \mathbb{K}(X)$$

Définition 21. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Si α est algébrique sur $\mathbb{K}$, alors $\mathrm{Ann}(\alpha)$ est un idéal principal non nul. Donc, il existe $P \in \mathbb{K}[X]$ unitaire tel que $\mathrm{Ann}(\alpha) = (P)$. On note π_α ce polynôme P : c'est le **polynôme minimal** de α sur $\mathbb{K}$.

Exemple 22. Sur $\mathbb{Q}$, on a $\pi_{\sqrt{2}} = X^2 - 2$ et $\pi_i = X^2 + 1$.

[GOZ] p. 31

Proposition 23. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Soient $P \in \mathbb{K}[X]$. Les assertions suivantes sont équivalentes :

(i) $P = \mu_\alpha$.
(ii) $P \in \mathrm{Ann}(\alpha)$ et est unitaire et $\forall R \in \mathrm{Ann}(\alpha) \setminus \{0\}$, $\deg(P) \leq \deg(R)$.
(iii) $P \in \mathrm{Ann}(\alpha)$ et est unitaire et irréductible dans $\mathbb{K}[X]$.

2. Corps de rupture

[GOZ] p. 57

Définition 24. Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $P \in \mathbb{K}[X]$ irréductible. On dit que $\mathbb{L}$ est un **corps de rupture** de P si $\mathbb{L} = \mathbb{K}[\alpha]$ où $\alpha \in \mathbb{L}$ est une racine de P.

Exemple 25. En reprenant les notations précédentes, si $\deg(P) = 1$, alors $\mathbb{K}$ est un corps de rupture de P.

Théorème 26. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$.

— Il existe un corps de rupture de P.

— Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P, alors il existe un unique $\mathbb{K}$-isomorphisme $\varphi : \mathbb{L} \to \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.

Application 27. $X^2 + 1$ est un polynôme irréductible sur $\mathbb{R}$ dont $\mathbb{R}[X]/(X^2+1)$ est un corps de rupture. On pose alors $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$, le corps des nombres complexes, et on note i la classe de X dans l'anneau quotient.

Remarque 28. Si $\mathbb{L}$ est un corps de rupture d'un polynôme $P \in \mathbb{K}[X]$, on a $[\mathbb{L} : \mathbb{K}] = \deg(P)$. Plus précisément, une base de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel est $(1, \alpha, \dots, \alpha^{\deg(P)-1})$.

3. Corps de décomposition

Définition 29. Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$. On dit que $\mathbb{L}$ est un **corps de décomposition** de P si :

— Il existe $a \in \mathbb{L}$ et $\alpha_1, \dots, \alpha_n \in \mathbb{L}$ tels que $P = a(X - \alpha_1)\dots(X - \alpha_n)$.

— $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$.

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

— $\mathbb{C}$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$.

Théorème 31. Soit $P \in \mathbb{K}[X]$ un polynôme de degré supérieur ou égal à 1.

— Il existe un corps de décomposition de P.

— Deux corps de décomposition de P sont $\mathbb{K}$-isomorphes.

[FGN2] p. 160

Application 32. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On note $\mathcal{C}(A)$ le commutant de A. Alors,

$$\mathbb{K}[A] = \mathcal{C}(A) \iff \pi_A = \chi_A = \det(XI_n - A)$$

4. Clôture algébrique

[GOZ] p. 62

Proposition 33. Les assertions suivantes sont équivalentes :

(i) Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 est scindé sur $\mathbb{K}$.

(ii) Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 admet au moins une racine dans $\mathbb{K}$.

(iii) Les seuls polynômes irréductibles de $\mathbb{K}[X]$ sont ceux de degré 1.

(iv) Toute extension algébrique de $\mathbb{K}$ est égale à $\mathbb{K}$.

Définition 34. Si $\mathbb{K}$ vérifie un des points de la Proposition 33, $\mathbb{K}$ est dit **algébriquement clos**.

Proposition 35. Tout corps algébriquement clos est infini.

Contre-exemple 36. $\mathbb{Q}$ et même $\mathbb{R}$ ne sont pas algébriquement clos.

Théorème 37 (D'Alembert-Gauss)**.** $\mathbb{C}$ est algébriquement clos.

Définition 38. On dit que $\mathbb{L}$ est une **clôture algébrique** de $\mathbb{K}$ si $\mathbb{L}$ est une extension de $\mathbb{K}$ algébriquement close et si

$$\forall x \in \mathbb{L}, \exists P \in \mathbb{K}[X] \text{ tel que } P(x) = 0$$

Exemple 39.
— $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
— $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ est algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$.

Théorème 40 (Steinitz)**.** (i) Il existe une clôture algébrique de $\mathbb{K}$.

(ii) Deux clôtures algébriques de $\mathbb{K}$ sont $\mathbb{K}$-isomorphes.

III - Polynômes cyclotomiques

Définition 41. On appelle m-**ième polynôme cyclotomique** le polynôme

$$\Phi_m = \prod_{\xi \in \mu_m^*} (X - \xi)$$

Théorème 42. (i) $X^m - 1 = \prod_{d|m} \Phi_d$.

(ii) $\Phi_m \in \mathbb{Z}[X]$.

(iii) Φ_m est irréductible sur $\mathbb{Q}$.

Corollaire 43. Le polynôme minimal sur $\mathbb{Q}$ de tout élément ξ de μ_m^* est Φ_m. En particulier,

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m)$$

Application 44 (Théorème de Wedderburn)**.** Tout corps fini est commutatif.

Lemme 45. Soient $a \in \mathbb{N}$ et p premier tels que $p \mid \Phi_n(a)$ mais $p \nmid \Phi_d(a)$ pour tout diviseur strict d de n. Alors $p \equiv 1 \mod n$.

[GOU21] p. 99

[DEV]

Application 46 (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n.

IV - Polynômes irréductibles sur $\mathbb{F}_q$

Soient p un nombre premier et $n \in \mathbb{N}^*$. On pose $q = p^n$.

Théorème 47.

$$\mathbb{F}_q = \mathbb{F}_p[X]/(P)$$

où $P \in \mathbb{F}_p[X]$ est un polynôme irréductible de degré n sur $\mathbb{F}_p$.

Corollaire 48. (i) Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.

(ii) Si $P \in \mathbb{F}_p[X]$ est un polynôme irréductible sur $\mathbb{F}_p$ de degré n, alors P divise $X^q - X$. En particulier, il est scindé sur $\mathbb{F}_q$. Donc son corps de rupture $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ est aussi son corps de décomposition.

Théorème 49. Pour tout $j \in \mathbb{N}^*$, on note $I(p,q)$ l'ensemble des polynômes irréductibles unitaires de degré j sur $\mathbb{F}_p$. Alors,

$$X^q - X = \prod_{d|n} \prod_{Q \in I(p,q)} Q$$

Corollaire 50.

$$q = \sum_{d|n} d|I(p,d)|$$

Définition 51. On définit la **fonction de Möbius**, notée μ, par

$$\mu : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ n & \mapsto & \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 \dots p_k \text{ avec } p_1, \dots, p_k \text{ premiers distincts} \\ 0 & \text{sinon} \end{cases} \end{array}$$

Théorème 52 (Formule d'inversion de Möbius)**.** Soient f et g des fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ telles que $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d)$. Alors,

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

Corollaire 53.

$$\forall n \in \mathbb{N}^*, |I(p,q)| = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

Bibliographie

Oraux X-ENS Mathématiques **[FGN2]**

Serge Francinou, Hervé Gianella et Serge Nicolas. *Oraux X-ENS Mathématiques. Volume 2*. 2e éd. Cassini, 16 mars 2021.
https://store.cassini.fr/fr/enseignement-des-mathematiques/111-oraux-x-ens-mathematiques-nouvelle-serie-vol-2.html.

Les maths en tête **[GOU21]**

Xavier Gourdon. *Les maths en tête. Algèbre et probabilités*. 3e éd. Ellipses, 13 juill. 2021.
https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.

Théorie de Galois **[GOZ]**

Ivan Gozard. *Théorie de Galois. Niveau L3-M1*. 2e éd. Ellipses, 1er avr. 2009.
https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html.

Cours d'algèbre **[PER]**

Daniel Perrin. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.
https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html.