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

Romain Giuge

Dans cette leçon, A désignera un anneau commutatif et K un corps commutatif.

1 Définitions et premières propriétés

1.1 Polynômes irréductibles

Définition 1. Un polynôme $P \in A[X]$ est dit irréductible dans $A[X]$ ssi son degré est $\geqslant 1$ et ses seuls diviseurs dans $A[X]$ sont $\begin{cases} uP \text{ avec } u \in A^* \\ u \text{ avec } u \in A^*. \end{cases}$

Proposition 2. *Dans $K[X]$:*

(i) Tout polynôme de degré 1 est irréductible.

(ii) Tout polynôme irréductible de degré > 1 n'a pas de racine dans K.

Remarque 3. Réciproque de (ii) fausse en général (ex : $(X^2+1)^2$ sur $\mathbb{Q}$), mais vraie pour les polynômes de degré 2 ou 3.

Exemple 4. *Dans $\mathbb{C}$, les polynômes irréductibles sont exactement ceux de degré 1 (d'Alembert-Gauss). Dans $\mathbb{R}$, ce sont les polynômes de degré 1 et ceux de degré 2 à discriminant négatif. Dans $\mathbb{Z}[X]$, $2X$ n'est pas irréductible.*

Proposition 5. *Soient k un sous-corps de K et $P \in k[X]$.*

(i) Si P est irréductible dans $K[X]$, il l'est dans $k[X]$.

(ii) Si P est irréductible dans $k[X]$, il ne l'est pas nécessairement dans $K[X]$ (ex : $X^2+1 \in \mathbb{R}[X]$ réductible dans $\mathbb{C}[X]$).

Nous allons voir que l'on peut toujours trouver une extension de corps dans laquelle un polynôme irréductible donné sera réductible, et même scindé.

1.2 Corps de rupture d'un polynôme irréductible

Définition 6. Soit $P \in K[X]$ irréductible. Une extension L de K est appelée corps de rupture de P sur K s'il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $P(\alpha) = 0$.

Théorème 7. *Soit $P \in K[X]$ irréductible. Il existe un corps de rupture $L = K(\alpha)$ de P sur K, unique à isomorphisme près (prendre $L = K[X]/(P)$). De plus $[L : K]$ est égal au degré du polynôme minimal de α sur K.*

Exemple 8. *$\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de X^2+1, $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/(X^3-2)$ est un corps de rupture de X^3-2.*

Exemple 9. *Un corps de rupture de P ne contient pas nécessairement toutes les racines de P : $\mathbb{Q}(\sqrt[3]{2})$ ne contient pas $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ racines de X^3-2.*

1.3 Corps de décomposition

Définition 10. Soit $P \in K[X]$ (irréductible ou non). On appelle corps de décomposition de P sur K une extension L de K telle que :

(i) Dans $L[X]$, P est produit de facteurs de degré 1 (*i.e.* P a toutes ses racines dans L).

(ii) Le corps L est le plus petit vérifiant cette propriété (*i.e.* les racines de P engendrent L).

Théorème 11. *Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près. On le note $D_K(P)$. De plus, $[D_K(P) : K] \leqslant n!$.*

Exemple 12. *(i) $D_{\mathbb{Q}}(X^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, j)$. L'extension est de degré $6 = 3!$.*

(ii) $D_{\mathbb{Q}}(X^4 - 1) = \mathbb{Q}(i)$. L'extension est de degré $2 \neq 4!$.

2 Critères d'irréductibilité de polynômes

Dans cette partie, l'anneau A sera toujours supposé factoriel.

2.1 Lien entre $A[X]$ et $\mathrm{Frac}(A)[X]$

Définition 13. Soit $P = a_n X^n + \dots a_0 \in A[X]$. On définit le contenu de P, noté $c(P)$, par $c(P) = \mathrm{PGCD}(a_0, \dots, a_n)$ (défini modulo A^*). On dit que P est primitif si $c(P) = 1$.

Théorème 14 (Lemme de Gauss)**.** *Pour tout $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Proposition 15. *Les polynômes $P \in A[X]$ irréductibles dans $A[X]$ sont :*

(i) Les constantes $p \in A$ irréductibles dans A.

(ii) Les polynômes de degré $\geqslant 1$ primitifs et irréductibles dans $\mathrm{Frac}(A)[X]$.

Application 16. Si A est factoriel, alors $A[X]$ est factoriel (théorème de Gauss).

2.2 Critère d'Eisenstein

Théorème 17. *On note $K = \mathrm{Frac}(A)$. Soit $P = a_n X^n + \dots + a_0 \in A[X]$. Soit $p \in A$ irréductible. On suppose que p divise tous les a_i sauf a_n et que p^2 ne divise pas a_0. Alors P est irréductible dans $K[X]$ (donc aussi dans $A[X]$ si $c(P) = 1$).*

Exemple 18. *(i) Si p est un nombre premier, $P = X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}$ (Eisenstein appliqué à $P(X + 1)$ avec p).*

(ii) Soit $a = p_1^{\alpha_1} \dots p_r^{\alpha_r} \in \mathbb{Z}$. Si $r \geqslant 2$ et s'il existe i avec $\alpha_i = 1$, alors $X^n - a$ est irréductible sur $\mathbb{Z}$.

2.3 Réduction modulo un idéal premier

Théorème 19. *On note $K = \mathrm{Frac}(A)$. Soient I un idéal premier de A et $B = A/I$: B est un anneau intègre de corps de fractions L. Soit $P = a_n X^n + \dots + a_0 \in A[X]$ tel que $\overline{a_n} \neq 0$ dans B. Alors si $\overline{P}$ est irréductible sur B ou L, P est irréductible sur K (donc aussi dans $A[X]$ si $c(P) = 1$).*

Exemple 20. *(i) $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$ (par réduction modulo 2, on trouve $X^3 + X + 1$ qui n'a pas de racine dans $\mathbb{F}_2$).*

(ii) Si $p \in \mathbb{Z}$ premier, alors $X^p - X - 1$ est irréductible sur $\mathbb{Z}$ (car on peut prouver qu'il l'est sur $\mathbb{F}_p$).

Remarque 21. La réciproque est fausse : X^4+1 est irréductible sur $\mathbb{Z}$ mais réductible sur tous les $\mathbb{F}_p$, p premier.

2.4 Irréductibilité et extensions de corps

Théorème 22. *Soit $P \in K[X]$ de degré $n > 0$. Alors P est irréductible sur K ssi P n'a pas de racines dans les extensions L de K telles que $[L:K] \leqslant \frac{n}{2}$.*

Exemple 23. *X^4+X+1 est irréductible sur $\mathbb{F}_2$: on vérifie qu'il n'a pas de racines dans $\mathbb{F}_2$ et $\mathbb{F}_4 = \mathbb{F}_2[j]$ ($j^2+j+1=0$).*

On avait vu que l'irréductibilité n'était pas conservée en général par extension de corps (proposition 5). Mais on a :

Théorème 24. *Soient $P \in K[X]$ irréductible de degré n et L une extension de degré m avec $(m,n)=1$. Alors P est encore irréductible sur L.*

Exemple 25. *(i) X^3+X+1 est irréductible sur $\mathbb{Q}$ (pas de racine), donc aussi sur $\mathbb{Q}(i)$.*

(ii) Si X^3+X+1 n'a pas de racine dans $\mathbb{F}_p$ (par ex, $p=2$ ou 5), il est irréductible sur $\mathbb{F}_p$, donc aussi sur $\mathbb{F}_{p^n}$ si 3 ne divise pas n.

3 Applications à la théorie des corps

3.1 Construction des corps finis

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

Théorème 26. *Il existe un corps à q éléments unique à isomorphisme près. C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$, qu'on note $\mathbb{F}_q$.*

Théorème 27. *Il existe un polynôme irréductible de degré r sur $\mathbb{F}_p$ tel que $\mathbb{F}_q$ soit le corps de rupture de ce polynôme.*

Corollaire 28. *(i) Il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_p$.*

(ii) Si P est irréductible de degré r sur $\mathbb{F}_p$, alors P divise $X^{p^r} - X$ dans $\mathbb{F}_p$. On en déduit que son corps de rupture est son corps de décomposition.

Proposition 29. *On note $I_q(n)$ l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbb{F}_q$ et $N_q(n)$ son cardinal. Alors pour $n \geqslant 1$, on a :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in I_q(d)} P \quad \text{et} \quad N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d,$$

μ désignant la fonction de Möbius.

Remarque 30. On retrouve le corollaire 28 : l'expression de $N_q(n)$ montre que $N_q(n) > 0$, donc qu'il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_{p^r} = \mathbb{F}_p$ (avec $r=1$). Puis on retrouve le théorème 27 : soit P irréductible de degré r sur $\mathbb{F}_p$. Alors $L = \mathbb{F}_p[X]/(P)$ est un corps de cardinal $q = p^r$.

3.2 Extensions de corps

Définition 31. On dit qu'un élément $\alpha \in L$ est algébrique sur K s'il est racine d'un polynôme non nul à coefficients dans K.

Proposition 32. *Si α est algébrique sur K, alors l'ensemble des polynômes annulateurs de α est un idéal I non réduit à $\{0\}$ de $K[X]$ qui est principal. Il existe alors un unique $M_\alpha \in K[X]$ unitaire tel que $I = (M_\alpha)$. On appelle M_α le polynôme minimal de α.*

Proposition 33. *Soient $P \in K[X]$ et α dans une extension de K. P est le polynôme minimal de α ssi P est unitaire, $P(\alpha) = 0$ et P est irréductible dans $K[X]$.*

Théorème 34. *Si α est algébrique sur K, alors $[K(\alpha) : K] = \deg(M_\alpha)$ où M_α est le polynôme minimal de α sur K. Sinon (α est transcendant), $[K(\alpha) : K] = +\infty$.*

Signalons le théorème suivant :

Théorème 35 (Théorème de l'élément primitif)**.** *Soit L une extension de degré fini de K et séparable. Alors l'extension L admet un élément primitif, i.e. il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Application 36. On sait alors qu'on peut trouver $\alpha \in \mathbb{Q}(\sqrt[3]{2}, j) = D_{\mathbb{Q}}(X^3 - 2)$ tel que $\mathbb{Q}(\sqrt[3]{2}, j) = \mathbb{Q}(\alpha)$. On vérifie par exemple que $\alpha = \sqrt[3]{2} + j$ convient.

3.3 Polynômes cyclotomiques

Définition 37. Pour $n \in \mathbb{N}^*$, on définit Φ_n le n-ième polynôme cyclotomique sur $\mathbb{C}$ par $\Phi_n = \prod_{\omega \in U_n^*}(X - \omega)$, où U_n^* désigne l'ensemble des racines primitives n-ième de l'unité.

Proposition 38. $\Phi_n \in \mathbb{Z}[X]$.

Théorème 39. *Φ_n est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Z}$ car $c(\Phi_n) = 1$ (Φ_n est unitaire).*

Les applications des polynômes cyclotomiques sont nombreuses :

Application 40. (i) Soit $\omega \in U_n^*$. Alors $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$.

(ii) Soient $\omega \in U_n^*$ et $\omega' \in U_m^*$ avec $(n, m) = 1$. Alors $\mathbb{Q}(\omega) \cap \mathbb{Q}(\omega') = \mathbb{Q}$.

(iii) Cas particulier du théorème de Dirichlet : il existe une infinité de nombres premiers de la forme $\lambda n + 1$, $\lambda \in \mathbb{N}^*$.

(iv) Théorème de Wedderburn : tout corps fini est commutatif.

Développements :

1. Dénombrement des polynômes irréductibles sur un corps fini (théorème 29).
2. Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$ (théorème 39).

Références :

- Perrin - *Cours d'algèbre.*
- Gozard - *Théorie de Galois.*