

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

Dans cette leçon on considère A un anneau unitaire intègre commutatif et $\mathbb{K}$ un corps.

1 Irréductibilité dans $A[X]$

1.1 Définitions et propriétés

Définition 1. Un polynôme $P \in A[X]$ est dit irréductible si il n'est pas inversible et si $P = AB$ avec $A, B \in A[X]$ alors A inversible ou B inversible

Exemple 2. Si A est un corps alors les polynômes de degré 1 sont les seuls polynômes irréductibles.

Définition 3. Pour $P = a_n X^n + \dots + a_0 \in A[X]$ on définit le contenu de P noté $c(P) = \text{pgcd}(a_0, \dots, a_n)$ modulo les inversibles de A . On dit que P est primitif lorsque $c(P) = 1$.

Lemme 4. Pour $P, Q \in A[X]$ on a $c(PQ) = c(P)c(Q)$ modulo les inversibles.

Proposition 5. Les polynômes irréductibles de $A[X]$ sont les constantes de A irréductibles dans A et les polynômes $P \in A[X]$ avec $\deg P \geq 1$, primitifs et irréductibles dans $\text{Frac}(A)[X]$.

Exemple 6. Les polynômes irréductibles de $\mathbb{Z}[X]$ sont les entiers premiers et leurs opposés et les polynômes P de degré supérieur ou égal à 1, primitifs et irréductibles dans $\mathbb{Q}[X]$.

Théorème 7. Soit $P \in \mathbb{K}[X]$, les conditions suivantes sont équivalentes :

1. $\mathbb{K}[X]/(P)$ est un corps,
2. L'anneau $\mathbb{K}[X]/(P)$ est intègre,
3. P est irréductible.

1.2 Critères d'irréductibilité

Proposition 8. Soit $P \in A[X]$ non constant, si P est réductible dans $\mathbb{K}[X]$, alors il existe $Q, R \in A[X]$ non constants tels que $P = QR$.

Proposition 9. Soient $P, Q \in \mathbb{K}[X]$ unitaires non constants tels que $PQ \in A[X]$ alors $P, Q \in A[X]$.

Théorème 10. (Critère d'Eisenstein) Soit A anneau factoriel et $\mathbb{K}$ son corps des fractions. Soit $P(X) = a_n X^n + \dots + a_0 \in A[X]$ et $p \in A$ irréductible. Si on a les conditions suivantes :

1. $p \nmid a_n$,
2. $p \mid a_i$ pour $i \in \{0, \dots, n-1\}$,
3. $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{K}[X]$ (donc si $\text{pgcd}(a_i) = 1$ il l'est dans $A[X]$).

Exemple 11. Pour p premier dans $\mathbb{N}$, $X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}$.

Pour tout $n \in \mathbb{N}^*$ le polynôme $X^n - 2$ est irréductible sur $\mathbb{Z}$.

Remarque 12. Le deuxième exemple nous donne l'existence d'extensions de $\mathbb{Q}$ de n'importe quel degré puis l'existence des nombres transcendants sur $\mathbb{R}$.

Théorème 13. (Réduction) Soient A un anneau factoriel et $\mathbb{K}$ son corps des fractions, I idéal premier de A et $B = A/I$ intègre de corps des fractions L . Soit $P(X) = a_n X^n + \dots + a_0 \in A[X]$ et $\bar{P}$ sa réduction modulo I . On suppose que $\bar{a}_n \neq 0$ dans B . Si $\bar{P}$ est irréductible sur B ou $\mathbb{L}$ alors P est irréductible sur $\mathbb{K}$.

Exemple 14. Si $A = \mathbb{Z}$ et $I = (p)$ avec p premier alors $B = \mathbb{F}_p$ est un corps. Par exemple $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$ en réduisant modulo 2 dans $\mathbb{F}_2$.

2 Théorie des corps

2.1 Généralités

Définition 15. Soient $\mathbb{K}$ et $\mathbb{L}$ des corps. On dit que $\mathbb{L}$ est une extension de $\mathbb{K}$ lorsque $\mathbb{K} \subset \mathbb{L}$.

Théorème 16. (Base télescopique) Soient $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ des corps, $(e_i)_{i \in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j \in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors la famille $(e_i f_j)_{(i,j) \in I \times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.

Corollaire 17. (Multiplicativité du degré) Dans la situation précédente on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 18. Soit $\alpha \in \mathbb{L}$ et soit $\phi_\alpha : \mathbb{K}[X] \rightarrow \mathbb{L}$ défini par $\phi_\alpha|_{\mathbb{K}} = id_{\mathbb{K}}$ et $\phi_\alpha(X) = \alpha$.

Si ce morphisme est injectif on dit que α est transcendant sur $\mathbb{K}$. Sinon il est dit algébrique sur $\mathbb{K}$.

Définition 19. Soit $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$, $\ker(\phi_\alpha)$ est un idéal non nul de $\mathbb{K}[X]$ qui est principal. Il existe donc un unique polynôme unitaire de $\mathbb{K}[X]$ général de $\ker(\phi_\alpha)$. Il est appelé polynôme minimal de α sur $\mathbb{K}$ et noté $\pi_{\alpha, \mathbb{K}}$.

Exemple 20. Les nombres e et π sont transcendants sur $\mathbb{Q}$ (mais pas sur $\mathbb{R}$). Les nombres $\sqrt{5}, i, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ et $\pi_{\sqrt{5}}(X) = X^2 - 5$, $\pi_i(X) = X^2 + 1$ et $\pi_{\sqrt[3]{2}}(X) = X^3 - 2$.

Proposition 21. Soit $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Alors $\pi_{\alpha, \mathbb{K}}$ est irréductible dans $\mathbb{K}[X]$.

Définition 22. Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ irréductible. Une extension $\mathbb{L} \supset \mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ lorsque $\mathbb{L}$ est une extension monogène $\mathbb{L} = \mathbb{K}[\alpha]$ avec $P(\alpha) = 0$.

Théorème 23. Soit $P \in \mathbb{K}$ irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$ unique à isomorphisme près.

Définition 24. Soit $P \in \mathbb{K}[X]$ de degré n (irréductible ou non). On appelle corps de décomposition de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ telle que :

1. Dans $\mathbb{L}[X]$, P est produit de polynôme de degré 1 (ou alors P a toutes ses racines dans $\mathbb{L}$).
2. Le corps $\mathbb{L}$ est minimal pour cette propriété (ou alors les racines de P engendrent $\mathbb{L}$).

Théorème 25. Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près que l'on note $D_{\mathbb{K}}(P)$.

Exemple 26. Dans $\mathbb{Q}$, $X^3 - 2$ a pour corps de décomposition $\mathbb{Q}(\sqrt[3]{2}, j)$.

2.2 Corps finis

Définition 27. Soit $\varphi : \mathbb{Z} \rightarrow \mathbb{K}$; $n \mapsto 1 + \dots + 1$ morphisme d'anneau. Son noyau est un idéal premier de $\mathbb{Z}$ de la forme $p\mathbb{Z}$ avec p premier ou $p = 0$. Ce nombre est appelé caractéristique de $\mathbb{K}$ noté $\text{car}(\mathbb{K})$

Remarque 28. Si $\text{car}(\mathbb{K}) = 0$ alors $\mathbb{K}$ contient $\mathbb{Z}$ (et $\mathbb{Q}$) donc est infini.

Si $\mathbb{K}$ est fini alors $\text{car}(\mathbb{K}) > 0$, son sous corps premier est $\mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$ et $|\mathbb{K}| = p^n$.

Proposition 29. Soit $\mathbb{K}$ un corps fini de caractéristique p et de cardinal $q = p^n$ on a :

1. Si $\mathbb{L}$ est une extension finie de $\mathbb{K}$, alors il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[\alpha]$.
2. Si $\mathbb{M}$ est un sous corps de $\mathbb{K}$ alors $|\mathbb{M}| = p^m$ avec m divise n .
3. Soit $d|n$ alors il existe un unique sous corps $\mathbb{M}$ de $\mathbb{K}$ tel que $|\mathbb{M}| = p^d$. On a $\mathbb{M} = \{x \in \mathbb{K} | x^{p^d} = x\}$ et $\mathbb{M}$ est isomorphe à $\mathbb{F}_{p^d}$.

Exemple 30. $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1)$ et $\mathbb{F}_9 \cong \mathbb{F}_3[X]/(X^2 + X - 1)$

Proposition 31. Soit $\mathbb{K}$ corps fini de cardinal q , $\overline{\mathbb{K}}$ une clôture algébrique et $m \in \mathbb{N}^*$. Alors il existe une unique extension $\mathbb{L}$ de $\mathbb{K}$ telle que $[\mathbb{L} : \mathbb{K}] = m$, de plus $|\mathbb{L}| = q^m$ et $\mathbb{L} = \{x \in \overline{\mathbb{K}} | x^{q^m} = x\}$.

Proposition 32. Pour tout $m, n \in \mathbb{N}^*$ on a $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n|m$.

Lemme 33. Le polynôme $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

Théorème 34. Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}^*$, alors P irréductible si et seulement si P n'a pas de racines dans les extensions de $\mathbb{K}$ de degré inférieur ou égal à $n/2$.

Exemple 35. $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

2.3 Dénombrement des polynômes irréductibles de $\mathbb{F}_p$

Définition 36. On définit la fonction de Möbius comme $\mu(1) = 1$, $\mu(n) = (-1)^r$ si $n = \prod_{i=1}^r p_i$ dans sa décomposition en facteurs carrés et $\mu(n) = 0$ sinon.

Théorème 37. (Möbius) Soient $(u_n)_{n \in \mathbb{N}^*}$ et $(v_n)_{n \in \mathbb{N}^*}$ des suites réelles alors $\forall n \in \mathbb{N}^*, u_n = \sum_{d|n} v_d \iff \forall n \in \mathbb{N}^*, v_n =$

$$\sum_{d|n} \mu(d) u_{\frac{n}{d}}.$$

On pose $P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$ et $\mathcal{U}_d(p) = \{P \in \mathbb{F}_p[X] \mid \deg(P) = d, \text{ irréductible et unitaire} \}$ pour tout $n \in \mathbb{N}^*$ et p premier fixé.

Lemme 38. Tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n . Réciproquement pour tout diviseur d de n tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n .

Théorème 39. Le polynôme P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a $X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P(X)$.

Théorème 40. Pour tout entier $n \in \mathbb{N}^*$ on a $|\mathcal{U}_n(p)| = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$.

3 Polynômes cyclotomiques

Définition 41. Une racine n -ième primitive de l'unité de $\mathbb{K}$ est un élément $\zeta \in \mathbb{K}$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour tout $d < n$. C'est un générateur de $\mu_n(\mathbb{K})$ de sorte qu'il y ait $\varphi(n)$ racines primitives de l'unité, leur ensemble est noté $\mu_n^*(\mathbb{K})$.

Définition 42. Le n -ième polynôme cyclotomique de $\mathbb{K}$ est $\Phi_n(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$.

Exemple 43. Sur $\mathbb{Q}$ on a $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$ et $\Phi_4(X) = X^2 + 1$.

Remarque 44. Si $\zeta \in \mu_n^*(\mathbb{K})$ alors les ζ^d avec $\text{pgcd}(d, n) = 1$. Le polynôme $\Phi_n(X)$ est unitaire de degré $\varphi(n)$.

Proposition 45. On a $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Proposition 46. Dans $\mathbb{Q}$ on a $\Phi_n(X) \in \mathbb{Z}[X]$.

Théorème 47. Le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

Théorème 48. Soit $\zeta \in \mu_n^*(\mathbb{K})$, alors Φ_n est le polynôme minimal de ζ sur $\mathbb{Q}$.

Corollaire 49. Soit $\zeta \in \mu_n^*(\mathbb{K})$, alors $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Dev 1 : Dénombrement des polynômes irréductibles de $\mathbb{F}_p$ 37,38,39 et 40

Dev 2 : Eisenstein 4,8, 9 et 10

Dev 3 : Polynômes cyclotomiques irréductibles 46 et 47

Références

- [PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.
- [ROM17] Jean-Étienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Supérieur, 2017.
- [TAU07] Patrice TAUVEL : Corps commutatifs et théorie de Galois : cours et exercices. Calvage et Mounet, 2007.

RAPPORT DU JURY :

Les généralités sur les algèbres de polynômes à une variable sont supposées connues. Le bagage théorique permettant de définir corps de rupture et corps de décomposition doit être présenté. Ces notions doivent être illustrées dans différents types de corps (réels, rationnels, corps finis) ; les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur $\mathbb{F}_2$ ou $\mathbb{F}_3$. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et les polynômes minimaux de quelques nombres algébriques, par exemple les polynômes cyclotomiques. Le théorème de la base télescopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes sont incontournables. Des applications du corps de décomposition doivent être mentionnées, par exemple en algèbre linéaire.

Pour aller plus loin, on peut montrer que l'ensemble des nombres algébriques sur le corps $\mathbb{Q}$ des rationnels est un corps algébriquement clos, s'intéresser aux nombres constructibles à la règle et au compas, et éventuellement s'aventurer en théorie de Galois.