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

Pandou

2 mai 2022

1 Arithmétique des polynômes

1.1 Structure arithmétique de $K[X]$

Dans cette partie, K est un corps.

Théorème 1 (Division euclidienne)**.** *Soit $A, B \in K[X]$ avec $B \neq 0$. Alors, il existe un unique couple $(Q, R) \in K[X]^2$ tel que*

$$A = BQ + R \qquad et \qquad \deg(R) < \deg(B)$$

Corollaire 2. *$K[X]$ est principal.*

Théorème 3 (Bézout)**.** *$P_1, ..., P_n \in K[X]$ sont premiers entre eux dans leur ensemble si et seulement s'il existe $U_1, ..., U_n \in K[X]$ tels que $U_1P_1 + ... + U_nP_n = 1$.*

Définition 4. *On dit que $P \in K[X]$ est irréductible si P n'est pas constant et si P n'admet pas de diviseurs de degré $\geqslant 1$.*

Remarque 5 : Si L/K est une extension de corps, il est possible que P soit irréductible sur $K[X]$, mais pas sur $L[X]$: $X^2 + 1$ sur $\mathbb{R}$ et $\mathbb{C}$.
Par contre, si P est irréductible sur $L[X]$, il l'est aussi sur $K[X]$.

Proposition 6.

1. *Tout polynôme de degré 1 est irréductible.*
2. *Tout polynôme irréductible de degré $\geqslant 2$ n'a pas de racine dans K.*
3. *Les polynômes irréductibles de degré 2 et 3 sont exactement ceux qui n'ont pas de racine dans K.*

Remarque 7 : La réciproque 2. est fausse : $(X^2 + 1)^2$ n'a pas de racine dans $\mathbb{R}$, mais est réductible.

Théorème 8 (Factorialité)**.** *Soit $P \in K[X]$ non nul, alors P se décompose de façon unique sous la forme $\lambda P_1^{\alpha_1}...P_k^{\alpha_k}$ où P_i est irréductible et unitaire.*

1.2 Structure arithmétique dans $R[X]$

Dans cette partie, R est un anneau commutatif intègre.

Théorème 9. *On peut effectuer une division euclidienne de A par B dans $R[X]$ si le coefficient dominant de B est inversible dans R.*

Proposition 10. *$R[X]$ est un principal si, et seulement si, R est un corps.*

Définition 11. *On dit que $x \in R$ est irréductible si x n'est pas inversible et si $x = ab$ impose a ou b est inversible.*

Exemple 12 :

- Dans $\mathbb{Z}$, les irréductibles sont les nombres premiers.
- Dans $K[X]$, les irréductibles sont les polynômes irréductibles.

Définition 13. *On dit que R est factoriel si*

1. *Tout élément non nul x de R s'écrit $x = up_1...p_r$ avec $u \in R^\times$ et $p_1, ..., p_r$ irréductibles.*
2. *La décomposition est unique à permutation et aux inversibles près.*

Définition 14. *Si R est factoriel et $P \in K[X]$, on note $c(P)$ le contenu de P, c'est le pgcd des coefficients de P. On dit que P est primitif si $c(P) = 1$.*

Lemme 15 (Gauss)**.**

$$\forall P, Q \in R[X], c(PQ) = c(P)c(Q)$$

Théorème 16. *Si R est factoriel, alors $R[X]$ aussi.*

1.3 Critères d'irréductiblité

Théorème 17. *Soit R un anneau factoriel et $K = \mathrm{Frac}(R)$. Alors les irréductibles de $R[X]$ sont :*

1. *les polynômes constants, irréductibles dans R.*
2. *les polynômes de degré $\geqslant 1$ primitifs et irréductibles dans $K[X]$.*

Théorème 18. *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 de discriminant < 0.

Théorème 19 (Critère d'Eisenstein). *Soit R un anneau factoriel et $K = \mathrm{Frac}(R)$. On note $P = a_n X^n + ... + a_0 \in R[X]$ et soit p un irréductible de R. On suppose que*

1. *p ne divise pas a_n.*
2. *p divise tous les a_i, $i \leqslant n-1$.*
3. *p^2 ne divise pas a_0.*

Alors, P est irréductible sur $K[X]$.

Applications 20 :

- $X^n - 2$ est irréductible pour tout $n \geqslant 1$ sur $\mathbb{Q}[X]$.
- $\Phi_p(X) = X^{p-1} + ... + X + 1$ est irréductible sur $\mathbb{Q}[X]$.

Théorème 21 (Réduction). *Soit p un nombre premier et $P(X) = a_n X^n + ... + a_0 \in \mathbb{Z}[X]$. On suppose que $a_n \neq 0 \mod (p)$, alors si P est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible sur $\mathbb{Q}[X]$.*

Exemples 22 :

- $X^3 + 2022X^2 + 2021X - 2023$ est irréductible sur $\mathbb{Q}[X]$.
- $X^p - X - 1$ est irréductible sur $\mathbb{Z}[X]$.

Remarque 23 : La réciproque est fausse : $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$, mais réductible dans tous les $\mathbb{F}_p[X]$.

DEVELOPPEMENT 1

Lemme 24. *Soit $P(X) = a_m X^m + ... + a_1 X + a_0 \in \mathbb{Z}[X]$, on suppose que les a_i sont positifs et on note $M = \sup_{i \leqslant m-2} |a_i|$. Alors, les racines α de P vérifient*

$$\mathrm{Re}(\alpha) \leqslant 0 \qquad ou \qquad |\alpha| < \frac{1 + \sqrt{1+4M}}{2}$$

Théorème 25 (Critère de Cohn). *Soit $b \geqslant 3$ et p un nombre premier dont l'écriture en base b est $a_m b^m + ... + a_1 b + a_0$. Alors, le polynôme $P(X) = a_m X^m + ... + a_1 X + a_0$ est irréductible dans $\mathbb{Q}[X]$.*

Exemples 26 :

- $6X^4 + 5X^3 + 5X^2 + 3X + 7$ est irréductible dans $\mathbb{Q}[X]$.
- $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$ car $\overline{10001}^4 = 257$ en base 4.

Remarque 27 : Le théorème est toujours vrai pour $b = 2$, mais plus difficile à montrer.

2 Extensions de corps

2.1 Premières définitions

Définition 28. *On dit que L/K est une extension de corps si L est un surcorps de K. On note alors $[L : K]$ la dimension de L en tant que K-espace vectoriel, si $[L : K] < +\infty$, on dit que l'extension est finie.*
On dit que L/K est monogène s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Théorème 29 (Base téléscopique). *Soit $K \subset L \subset M$ des corps, (e_i) une K-base de L, (f_j) une L-base de M. Alors, $(e_i f_j)$ est une K-base de M.*

Corollaire 30. *M/K est finie si, et seulement si, M/L et L/K sont finies et alors*

$$[M : K] = [M : L] \times [L : K]$$

2.2 Corps de rupture et corps de décomposition

Définition 31. *Soit P irréductible sur $K[X]$. On dit que L/K est un corps de rupture de P sur K si L est engendrée par une racine de P.*

Théorème 32. *Soit $P \in K[X]$ irréductible, alors il existe un corps de rupture de P sur K, unique à isomorphisme près : il est isomorphe à $K[X]/(P)$.*

Exemples 33 :

- $\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de $X^2 + 1$.
- $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2$. On voit qu'un corps de rupture ne contient pas nécessairement toutes les racines de P.

Théorème 34. *Soit $P \in K[X]$ de degré $\geqslant 1$. Alors, P est irréductible sur K si, et seulement si, P n'a pas de racines dans les extensions L/K telles que $[L : K] \leqslant \frac{n}{2}$.*

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

Théorème 36. *Soit $P \in K[X]$ irréductible de degré n et L/K une extension de degré m avec $m \wedge n = 1$. Alors, P est irréductible sur L.*

Exemple 37 : $X^3 + X + 1$ est irréductible sur $\mathbb{Q}(i)$.

Définition 38. *Soit $P \in K[X]$, on dit que L/K est un corps de décomposition de P sur K si, et seulement si, P est scindé sur $L[X]$ et si L est engendré par l'ensemble des racines de P.*

Théorème 39. *Soit $P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près.*

Exemples 40 : Un corps de décomposition de $X^3 - 2$ est $\mathbb{Q}(\sqrt[3]{2}, j)$.

2.3 Algébricité

Définition 41. *Soit L/K une extension et $\alpha \in L$. On considère $\varphi : K[T] \longrightarrow L$ qui envoie T sur α.*

- *Si φ est injectif, on dit que α est transcendant.*
- *Sinon, on dit que α est algébrique et on note μ_α le générateur unitaire de $\mathrm{Ker}(\varphi)$, appelé polynôme minimal de α.*

Théorème 42. *Soit L/K une extension de corps et $\alpha \in L$. Alors, on a équivalence entre :*

1. *α est algébrique sur K.*
2. *$K[\alpha] = K(\alpha)$.*
3. *$\big[K(\alpha) : \big] < +\infty$.*

Dans ce cas, μ_α est irréductible et $\big[K(\alpha) : K\big] = \deg(\mu_\alpha)$.

Théorème 43. *Soit K un corps, on a équivalence entre :*

1. *Tout polynôme de $K[X]$ de degré $\geqslant 1$ admet une racine dans K.*
2. *Tout polynôme de $K[X]$ est produit de polynômes de degré 1.*
3. *Les irréductibles de $K[X]$ sont les $(X - a)$ pour $a \in K$.*
4. *Si L/K est algébrique, alors $L = K$.*

On dit alors que K est algébriquement clos.

Définition 44. *Soit K un corps. Une clôture algébrique de K est une extension algébrique $\overline{K}/K$ telle que $\overline{K}$ est algébriquement clos.*

Théorème 45 (Admis)**.** *Tout corps admet une clôture algébrique, unique à isomorphisme près.*

3 Applications aux corps finis

3.1 Construction et réalisation

Proposition 46. *Soit K un corps fini, alors la caractéristique de K est un nombre premier p et il existe $n \geqslant 1$ tel que $\mathrm{Card}(K) = p^n$.*

Proposition 47. *L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si, et seulement si, p est premier. Dans ce cas, on le note $\mathbb{F}_p$.*

Théorème 48. *Soit p premier, $n \geqslant 1$ et $q = p^n$. Il existe, à isomorphisme près, un unique corps à q éléments : il est isomorphe au corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.*

Théorème 49. *Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Alors, il existe un unique corps à q éléments dans $\overline{\mathbb{F}_p}$: c'est l'ensemble des racines de $X^q - X$.*

3.2 Automorphismes de $\mathbb{F}_q$

Proposition 50. *On note $q = p^n$, alors l'application $x \in \mathbb{F}_q \longmapsto x^p \in \mathbb{F}_q$ est un automorphisme, appelé automorphisme de Frobenius.*

DEVELOPPEMENT 2

Lemme 51. *Soit $P \in \mathbb{F}_p[X]$ irréductible de degré m, alors P divise $X^{p^n} - X$ si, et seulement si, m divise n.*

Proposition 52. *Soit $P \in \mathbb{F}_p[X]$ irréductible de degré m, alors toutes les racines de P dans $\overline{\mathbb{F}_p}$ sont de la forme $\alpha, \alpha^p, ..., \alpha^{p^{m-1}}$ où α est une racine de P.*

Théorème 53. *Les $\mathbb{F}_p$-automorphismes de $\mathbb{F}_q$ sont des puissances de l'automorphisme de Frobenius.*

Références :

- Arnaudiès, Fraysse. Cours de mathématiques - Algèbre.
- Gourdon, Algèbre.
- Gozard, Théorie de Galois.
- Perrin, Cours d'algèbre.
- Tauvel, Algèbre pour l'agrégation.