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

1 Échauffement : cas de R et de C

Théorème 1 (D'Alembert-Gauss)**.** *Tout polynôme $P \in \mathbf{C}[X]$ admet une racine dans $\mathbf{C}$. Ainsi, tout polynôme complexe est scindé dans $\mathbf{C}$, et les irréductibles de $\mathbf{C}[X]$ sont exactement les polynômes de degré 1.*

Trigonalisation

Corollaire 1. *Les irréductibles de $\mathbf{R}[X]$ sont exactement :*
– les polynômes de degré 1,
– les polynômes de degré 2 à discriminant strictement négatif.

Forme générale des endomorphismes normaux

2 Irréductibilité dans un anneau factoriel

2.1 Généralités

Soit A un anneau factoriel et K son corps des fractions.

Définition 1. Soit $P = \sum_{i=1}^{n} a_i X^i \in A[X] \setminus \{0\}$. On appelle *contenu* de P le nombre $c(P) = pgcd(a_1, \dots a_n)$. Un polynôme est dit *primitif* si son contenu est égal à 1.

Proposition 1. $\forall P, Q \in A[X] \setminus \{0\},\ c(PQ) = c(P)c(Q)$.

Proposition 2. *Les polynômes $P \in A[X]$ irréductibles dans $A[X]$ sont :*
– les constantes $p \in A$, irréductibles dans A,
– les polynômes P de degré ≥ 1, primitifs et irréductibles dans $K[X]$.

Remarque. On applique traditionnellement ce résultat à $A = \mathbf{Z}$ et $K = \mathbf{Q}$.

Théorème 2 (Gauss)**.** *$A[X]$ est factoriel.*

Remarque. On a alors l'existence et l'unicité de la décomposition en éléments simples dans $A[X]$.

Remarque. Lemme d'Euclide, Bézout...

2.2 Critères d'irréductibilité

Proposition 3. *Soit $P \in A[X]$ de degré ≤ 3. Alors P est irréductible ssi il n'a pas de racine dans A.*

Proposition 4 (Critère d'Eisenstein)**.** *Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ et $p \in A$ un irréductible. On suppose que p ne divise pas a_n, que $\forall i \in \{0, \ldots, n-1\}$, $p | a_i$ et que p^2 ne divise pas a_0. Alors P est irréductible dans $K[X]$.*

Exemple. $X^n + p$ et $X^n + p$, avec $p \in \mathbf{Z}$ premier, sont irréductibles dans $\mathbf{Z}[X]$ $\forall n \geq 1$. $X^{p-1} + \cdots + X + 1$ est irréductible dans $Z[X]$ pour p un entier naturel premier.

Proposition 5. *Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$, I un idéal premier de A, avec $a_n \notin I$, L le corps des fractions de A/I et π la projection de A sur A/I. Si $\pi(P)$ est irréductible dans $L[X]$, alors P est irréductible dans $K[X]$.*

Exemple. $X^p - X - 1$ est irréductible sur $\mathbf{Q}$.

3 Corps de rupture, corps de décomposition

On se donne K un corps commutatif

3.1 Corps de rupture

Soit P un polynôme irréductible de $K[X]$.

Définition 2. Une extension L de K est appelée un *corps de rupture* de P si $\exists \alpha \in L$ tq $P(\alpha) = 0$ et $L = K[\alpha]$.

Exemple. $K[X]/(P)$ est un corps de rupture de P.

Proposition 6. *Soient L une extension de K et $\alpha \in L$ une racine de P. Lpsse :*

(i) $[L : K] = d^\circ P$,

(ii) $L = K[\alpha]$,

(iii) *L est un corps de rupture de P.*

Théorème 3 (Unicité du corps de rupture)**.** *Soient $i : K \to K'$ un isomorphisme de corps, que l'on étend de $K[X]$ vers $K'[X]$. Soit $P \in K[X]$ irréductible et $P' = i(P)$. Soit L (resp. L') un corps de rupture de P sur K (resp. de P' sur K') engendré par x (resp. x'). Alors il existe un unique isomorphisme φ de L sur L' étendant i et vérifiant $\varphi(x) = x'$.*

Exemple. $\mathbf{C}$ est le corps de rupture sur $\mathbf{R}$ du polynôme $X^2 + 1$.

On en déduit deux critères d'irréductibilité :

Proposition 7. *Soit $P \in K[X]$ de degré $n > 0$. Alors P est irréductible sur K ssi pour toute extension finie L de K telle que $[L : K] \leq n/2$, P n'a pas de racine dans L.*

Exemple. $X^4 + 4X^3 - 2X^2 - X + 3$ est irréductible sur $\mathbf{Z}$.

Proposition 8. *Soient $P \in K[X]$ irréductible de degré n et L une extension de degré m de K. Si $m \wedge n = 1$, alors P est irréductible sur L.*

Exemple. $X^3 + X + 1$ est irréductible sur $\mathbf{Q}(i)$ comme sur $\mathbf{Q}$.

3.2 Corps de décomposition

Soit $P \in K[X]$ de degré $n \geq 1$

Définition 3. on dit qu'une extension L de K est un *corps de décoposition* de P si P est scindé sur L et si L est engendré sur K par les racines de P.

Théorème 4. *1. Il existe un corps de décompostion de P.*

2. *Deux corps de décomposition de P sont isomorphes (attention, un tel isomorphisme n'est pas unique).*
3. *Si L est un corps de décomposition de P, alors $[L : K] \leq n!$.*

4 Applications

4.1 Polynômes cyclotomiques

Soit K un corps de caractéristique p, et n un entier positif, premier à p si $p > 0$. Posons K_n un corps de décomposition de $X^n - 1$ sur K, et $\mu_{n,K}$ l'ensemble des racines de $X^n - 1$ dans K_n, qui forme un sous-groupe fini de K_n et qui est donc cyclique. On note $\mu^*_{n,K}$ l'ensemble des générateurs de $\mu_{n,K}$, appelés *racines primitives n-ièmes de l'unité.*

Définition 4. On appelle n-ième polynôme cyclotomique le polynôme

$$\Phi_{n,K} = \prod_{\zeta \in \mu^*_{n,K}} (X - \zeta)$$

Proposition 9. *1. $|\mu^*_{n,K}| = \varphi(n)$,*

2. *$X^n - 1 = \prod_{d|n} \Phi_{d,K}$,*
3. *$\Phi_{n,K} \in K_0[X]$, où K_0 est le sous-corps premier de K,*
4. *$\Phi_{n,\mathbf{Q}} \in \mathbf{Z}[X]$*

Application (Wedderburn).

Théorème 5. *$\Phi_{n,\mathbf{Q}}$ est irréductible sur $\mathbf{Z}[X]$.*

4.2 Corps finis

On pose $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

Remarque. Un polynôme P de degré n sur un corps commutatif a au plus n racines.

Théorème 6. *Si K est un corps fini, il existe p premier et $n > 0$ tq $|K| = p^n$. Inversement, pour tout nombre premier p et entier non nul n, il existe un corps de cardinal p^n. Un tel corps est corps de décomposition de $X^{p^n} - X$ sur $\mathbf{F}_p$, en particulier deux corps de même cardinal sont isomorphes.*

Définition 5. Un corps de cardinal q est alors noté $\mathbf{F}_q$.

Théorème 7. *Soit $q = p^n$. Posons $\mathcal{P}_{d,q} = \{P \in \mathbf{F}_q[X]/P$ irréductible unitaire de $d^\circ d\}$. Alors*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_{d,q}} P$$

Corollaire 2 ([Dem])**.** *Critère d'irréductibilité : divise $X^{q^n} - X$, ne divise pas $X^{q^d} - X$.*

Application. Tout polynôme irréductible sur $\mathbf{F}_q$ a ses racines simples dans $\overline{\mathbf{F}_q}$ (corps parfait).

Théorème 8. *Réduction de Φ_n dans $\mathbf{F}_q$ [Dem].*

Proposition 10. *Construction effective de corps finis.*

Théorème 9. *Berlekamp.*

4.3 Nombres constructibles

Théorème de Gauss Perrin, applications, théorème de Gauss-Wantzel.

4.4 Algèbre linéaire

Lemme 1. *Soit $P \in k[X]$. $P(u)$ est inversible ssi P est premier à π_u.*

Polynôme minimal, lemme des noyaux et application à Dunford dans un corps algébriquement clos, réduction de Jordan, endomorphismes semi-simples.

Références

Perrin
Demazure
Carrega
Beck
Gourdon