141

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

Tout sur $K[X]$ K un corps

I Généralités

1) Définition de l'irréductibilité et propriétés

Déf : Soit A un anneau unitaire intègre commutatif
Un élément $p \in A$ est irréductible si et ssi $p \notin A^*$ (p non inversible) et si $p = ab \Rightarrow a \in A^*$ ou $b \in A^*$

Ex : Les irréductibles de $\mathbb{Z}$ sont les nombres premiers

Déf : Un anneau A est dit factoriel si et ssi A est intègre et il existe un système de représentants $\mathcal{P}$ des irréductibles de A tel que
$\forall a \in A^* \setminus \{0\}$, a s'écrit de manière unique à un inversible près $a = u \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$ où $u \in A^*$ et où les $\nu_p(a)$ sont non nuls en nombre fini.

Ex : L'anneau $\mathbb{Z}$ est factoriel.
$\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel

Rapp : Si A est factoriel, alors $A[X]$ est factoriel.

Rq : théorème difficile et non trivial.
$\Rightarrow$ Récurrence, $K[X]$ est toujours factoriel.

Déf : Un polynôme P de $A[X]$ est irréductible si P est irréductible pour l'anneau $A[X]$ à $P \in (A[X])^* = A^*$ et si les seuls diviseurs de P sont les éléments de A^* et les polynômes uP, $u \in A^*$.

Ex : $(X-a)$ est irréductible pour $A[X]$ mais pas $(X-a)^2$

Déf : Le corps des fractions d'un anneau A est $Fr(A) = A \times A^*/\mathcal{R}$ où $(x,y) \mathcal{R} (x',y') \Leftrightarrow xy' = x'y$

Rq : Soit $P \in A[X]$ où $P(X) = \sum_{k=0}^{n} a_k X^k$, $P \neq 0$
Le contenu de P est le pgcd de la famille $(a_0, \dots, a_n)$ on le note $c(P)$ et il est défini à un inversible près
Rq : Le pgcd est défini à un inversible près via P.

Th : Les polynômes irréductibles de $A[X]$ sont :
- les éléments irréductibles de A
- les polynômes de contenu égal à 1 et irréductibles dans $Fr(A)[X]$ de degré non nul.

2) Corps de rupture

Rappels sur les ext. de corps

Déf : Soit L une extension de K noté $K \subseteq L$. Un élément $x \in L$ est algébrique si $\exists P \in K[X] \setminus \{0\}$ tq $P(x) = 0$

Déf/Prop : Soit l'extension $K \subseteq L$ et $x \in L$ algébrique.
$\Phi_x : K[X] \to L$, $P \mapsto P(x)$ est un morphisme d'anneaux de $K[X]$ principal
Alors il existe un unique polynôme unitaire π_x tel que $\pi_x(x) = 0$ et $\ker(\Phi_x) = \pi_x K[X]$.
On appelle ce polynôme le polynôme minimal de x.

Prop : π_x est irréductible.

Déf : Soit $P \in K[X]$ irréductible (K un corps)
Un corps de rupture de P sur K est une extension L de K tel que $\exists \alpha \in L$ tel que $P(\alpha) = 0$ et $K(\alpha) = L$

Prop : "Le" corps de rupture est unique à isomorphisme près.
et $K(\alpha) = K[X]/(P)$ en est un exemple.

Ex : $\mathbb{C}$ est le corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.

Aphé : Si L est le corps de rupture de $P \in K[X]$, alors le degré de l'extension est égal au degré de P.

Déf : Soit P un polynôme de $K[X]$ non scindé
Un corps de décomposition de P est une extension de K dans laquelle P est scindé et qui est minimal pour cette propriété.

Prop : "Le" corps de décomposition est unique à isomorphisme près.

Polynômes irréductibles

3) Critères d'irréductibilité

Critère d'Eisenstein

Th : Soit A un anneau factoriel et $P \in A[X]$: $P(X) = \sum_{k=0}^{n} a_k X^k$
Soit $p \in A$ un élément irréductible tq :
- $p \nmid a_n$ et $p^2 \nmid a_0$
- $p \mid a_k$ pour $k \in [\![0, n-1]\!]$

Alors P est irréductible dans $\mathrm{Frac}(A)[X]$

Rq : Si $c(P) = 1$ (ou est "primitif"), P irréductible de $A[X]$

Ex : Si $p \in \mathbb{P}$ premier, $X^{p-1} + \dots + X + 1$ irréductible sur $\mathbb{Z}$.
$X^n - 3$ irréductible sur $\mathbb{Z}$ $\forall n \in \mathbb{N}$

Ex Φ_p et Φ_{p^n} et récurrence

Irréductibilité par réduction modulo p

Th : Soient A un anneau factoriel et I un idéal premier
Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ tel que $a_n \notin A/I$
Alors : P irréductible sur A/I
$\Rightarrow$ P irréductible sur $\mathrm{Frac}(A)$

Cor : Pour $p \in \mathbb{P}$, si $p \nmid a_n$ et si $c(P) = 1$, alors
P irréductible dans $\mathbb{Z}/p\mathbb{Z}[X] \Rightarrow P$ irréductible $\mathbb{Z}[X]$

Ex : Pour $p \in \mathbb{P}$, $X^p - X - 1$ irréductible sur $\mathbb{Z}$.

Rq : La réciproque est fausse (considérer $X^n - 3$)

Critères utilisants les extensions

Th : Soit $P \in K[X]$ irréductible de degré n et soit L une extension de K de degré m tel que $n \wedge m = 1$
Alors P est irréductible sur L.

Ex : $X^2 + X + 1$ irréductible sur $\mathbb{Q}(i)$ puisque l'est sur $\mathbb{Q}$
$X^4 + 1$ irréductible sur $\mathbb{Q}$ mais pas $\mathbb{Q}(i)$ (pour $n = 4$)

Prop : Soit $P \in K[X]$ de degré non nul.
Alors P est irréductible sur K s'il n'a pas de racines dans toutes les extensions de K de degré $\leq \frac{d^\circ(P)}{2}$

Ex : Un polynôme de degré 3 est irréductible sur K s'il n'a pas de racines sur K.

Exos sur $\mathbb{F}_2[X]$

II Exemples et applications

1) Polynômes cyclotomiques

Notation : On note, pour $n \in \mathbb{N}^*$, U_n l'ensemble des racines n-ièmes de l'unité (complexes) et μ_n l'ensemble des racines primitives n-ièmes de l'unité.

Def : Soit $n \in \mathbb{N}^*$. On appelle n-ième polynôme cyclotomique qu'on note Φ_n le polynôme :
$$\Phi_n(X) = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{\substack{k \in \mathbb{Z}/n\mathbb{Z} \\ k \wedge n = 1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

Prop : 1) Φ_n est unitaire, à coefficients entiers et de degré $\varphi(n)$
2) $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ pour $n \in \mathbb{N}^*$

Rq : 2) permet de calculer successivement Φ_n

Ex : $\Phi_6(X) = X^2 - X + 1$ dans $\mathbb{Z}[X]$ donc

Coro : $\forall n \in \mathbb{N}^*$, Φ_n est irréductible dans $\mathbb{Q}[X]$

Rq : Pas trivial.

Prop : Pour $\zeta \in \mu_n$, Φ_n est le polynôme minimal de ζ.

2) Irréductibilité sur les corps finis

Regardons ce que deviennent les polynômes cyclotomiques.

Prop : Soit $\mathbb{F}_q$ le corps fini à q éléments
Soit $n \in \mathbb{N}^*$ tq $n \wedge q = 1$ et notons r, l'ordre de $\bar{q}$ de $(\mathbb{Z}/n\mathbb{Z})^*$
Alors $\Phi_n(X)$ se décompose dans $\mathbb{F}_q[X]$ en produit de polynômes unitaires distincts irréductibles de degré r

Ex : $\Phi_7(X) = 1 + X + \dots + X^6 = (1 + X + X^3)(1 + X^4 + X^3)$ dans $\mathbb{F}_2[X]$

Coro : Φ_n est irréductible sur $\mathbb{F}_q$ ssi $\langle q \rangle = (\mathbb{Z}/n\mathbb{Z})^*$

Ex : Φ_5 est irréductible sur $\mathbb{F}_3$

DEV 1 — Existence de polynômes irréductibles sur $\mathbb{F}_q$.

Soit $\mathbb{F}_q$ un corps à q éléments.
Notons $\mathcal{I}(n,q)$ l'ensemble des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_q$ et $I(n,q) = |\mathcal{I}(n,q)|$.

Alors :
1/ $X^n - 1 = \prod_{d|n} \prod_{P \in \mathcal{I}(d,q)} P \quad \forall n \in \mathbb{N}^*$

2/ $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$

3/ $I(n,q) \geq 1$

4/ $I(n,q) \sim \frac{q}{n}$ et analogue du th des nombres premiers

Lemme (Admis) : Soit μ la fonction de Möbius définie par
$\mu(n) = \begin{cases} (-1)^r & \text{si } n \text{ est produit de } r \text{ premiers distincts} \\ 0 & \text{si } p^2 \mid n \text{ pour } p \text{ premier} \\ 1 & \text{si } n = 1 \end{cases}$

Alors, pour $f : \mathbb{N}^* \to \mathbb{R}$ et $g\left(\begin{array}{l}\mathbb{N}^* \to \mathbb{R} \\ n \mapsto \sum_{d|n} f(d)\end{array}\right)$
alors on a la formule d'inversion : $f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right)$

3) Construction à la règle et au compas

Th de Wantzel : Soit $t \in \mathbb{C}$.
Si t est constructible à la règle et au compas alors $[\mathbb{Q}(t) : \mathbb{Q}]$ est une puissance de 2
car $\mathbb{Q}(t)$ le corps de rupture de t.

Th de Gauss : Si le polygone régulier à n côtés est constructible à la règle et au compas, alors n est produit de 2^a où $a \in \mathbb{N}$ et de nombres premiers de Fermat.

Rq : En fait si $\zeta \in \mathbb{U}_p$, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p)$ est une puissance de 2 (car $\pi_\zeta = \Phi_p$)
La réciproque est vraie, mais fait appel à la théorie de Galois.

Ex : Le pentagone est constructible et on peut le construire via $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$.

Rq : Le résultat apporte une réponse négative aux problèmes de constructions (duplication du cube et la quadrature du cercle)

4) Applications en algèbre linéaire

Déf : Soit E un K-ev de dim finie et soit $u \in \mathcal{L}(E)$
$\Phi_u \left(\begin{array}{l} K[X] \to \mathcal{L}(E) \\ P \mapsto P(u) \end{array}\right)$ est un morphisme d'anneaux
donc il existe un unique polynôme unitaire π_u tel que $\pi_u(0)$ et $(\pi_u) = \mathrm{Ker}(\Phi_u)$.
Ce polynôme est appelé polynôme minimal de u.

Rq Att : π_u n'est pas toujours irréductible !

Lemme des noyaux : Soit $f \in \mathcal{L}(E)$ et soit $P = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ la décomposition en facteurs irréductibles de P.
Alors $\mathrm{Ker}(P(f)) = \bigoplus_{i=1}^{r} \mathrm{Ker}(P_i^{\alpha_i}(f))$

Déf : Un endomorphisme f de $\mathcal{L}(E)$ est semi-simple si pour tout sev F de E f-stable, il existe un supplémentaire de F f-stable.

DEV 2 — Endomorphismes semi-simples

$f \in \mathcal{L}(E)$ est semi-simple si et ssi
π_f est produit de polynômes irréductibles 2 à 2 distincts

Rq : En fait, c'est la bonne notion de réduction car passe par extension :
f semi-simple de $\mathbb{R} \Leftrightarrow f$ diagonalisable dans $\mathbb{C}$

Pour $K = \mathbb{C}$ f semi-simple $\Leftrightarrow$
f diagonalisable $\Leftrightarrow \pi_f$ scindé à racines simples.

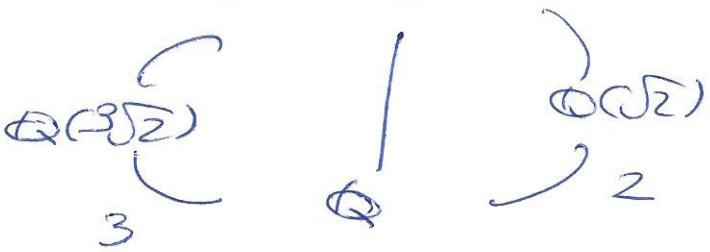
Exercice : Endomorphismes semi-simples

Q1 : Soit f tq $\pi_f = X(X^2+1)$ de $\mathbb{R}[X]$
Quels sont les sev f-stables de E ?

R : Vio le ss de f, c'est E et $\ker(f^2+Id)$.

Q2 : Degré de l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$?

R



Q3 : Degré de l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$

R : $\alpha = \sqrt{2}+\sqrt{3}$ - on a une rel sur α^2
et on peut montrer que c'est 4

Q4 : Mq χ_f et π_f ont mêmes facteurs irréductibles.

1) Transition : introduction de F(A)
corps de fraction pratique
un autre corps environnant :
le corps de rupture !

2) transition : il faut chercher
les polynômes de F(A) et
ramener les résultats des
extensions.

3) Cyclotomie = Division du cercle.
Partie logique

Rq : Ce qui est barré est vrai mais
signale les parties que je n'ai
pas écrit le jour de l'oral.

Références

[Per] PERRIN
[CL] CHAMBERT-LOIR - Algèbre corporelle
[Aud] AUDIN
[Gou] GOURDON - Algèbre
[Dem] DEMAZURE - Cours d'Algèbre.

Dév 1 : DEMAZURE
FRANCINOU-GIANELLA - Ex. pour l'Agreg Algèbre 1

Dév 2 : GOURDON
Objectif Agrégation.