141

Polynômes irréductibles d'une indéterminée. Corps de rupture. Exemples et Applications

I Polynomes irréductibles

$\mathbb{K}$ un corps

1) Definitions

Def 1: Soit A un anneau commutatif unitaire. On appelle polynome à une indéterminé à coefficients dans A toute suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A tous nuls à partir d'un certain rang

Rmq 2: Soit P un polynôme sur A, on le représente de la manière suivante : $P(X) = \sum_{i=0}^{n} a_i X^i$ où $n+1$ est le rang à partir duquel $(a_i)_{i\geq n+1}$ est nulle. on appelle n son degré.

Ex 3: $P(X) = X^2+3X+1$ est un polynome de degré 2 sur $\mathbb{Z}$.
$P(X) = X^3+\sqrt{2}X-\pi$ est un polynôme de degré 3 sur $\mathbb{R}$

Prop 4: Si $A=\mathbb{K}$ un corps. Alors l'ensemble des polynomes sur $\mathbb{K}$ noté $\mathbb{K}[X]$ a une structure d'anneau euclidien.

Thm 5: Soit $A, B \in \mathbb{K}[X]$, $B\neq 0$
Alors il existe un unique couple $(Q,R)\in\mathbb{K}[X]^2$ tel que $A=BQ+R$ et $\deg(R) < \deg(B)$

Corollaire 6: $\mathbb{K}[X]$ est principal.

Ex 7: $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ sont principaux

Ex 8: $\mathbb{Z}[X]$ ne l'est pas car $\langle 2, X\rangle$ n'est pas monogène

Rmq 9: $\mathbb{K}[X]$ a la même structure que les entiers de $\mathbb{Z}$

Def 10: Soient $P, Q \in \mathbb{K}[X]$, on dit que P divise Q noté $P \mid Q$ si il existe un polynome $R\in\mathbb{K}[X]$ tel que $RP = Q$.

Ex 11: $X+1 \mid X^2-1$ car $(X+1)(X-1) = X^2-1$

Def 12: Un polynôme $P\in\mathbb{K}[X]$ est dit irréductible dans $\mathbb{K}[X]$ si P n'est pas constant et si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les constantes non nulles et les polynômes associés à P.

Ex 13: $X-3$ est irréductible sur $\mathbb{Q}$.

Thm 14: Soit $P\in\mathbb{K}[X]$ un polynome non nul. Alors P se décompose de manière unique à l'ordre près sous la forme $P = \lambda P_1^{\alpha_1}\cdots P_k^{\alpha_k}$ où $\lambda\in\mathbb{K}^\times$, $\alpha_i\in\mathbb{N}^*$ et P_i sont distincts, unitaires et irréductibles sur $\mathbb{K}$.

Ex 15: $X^4-1 = (X^2+1)(X+1)(X-1)$ sur $\mathbb{Q}$

2) Critère d'irréductibilité

Thm 16: (Eisenstein) Soit A un anneau factoriel et $K = Fr(A)$. Soit $P = \sum_{i=0}^{n} a_i X^i$ avec $a_i\in A$
Soit $p\in A$ irréductible. Si :
(i) $p\nmid a_n$ (ii) $p\mid a_i$ $\forall i\in\{0,\dots,n-1\}$ (iii) $p^2\nmid a_0$
Alors P est irréductible dans $K[X]$

Ex 17: X^4+3X^2-6X+3 est irréductible sur $\mathbb{Q}$ avec $p=3$

Thm 18: (réduction modulaire) Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$
Soit p premier. On note $\overline{P}$ la réduction de P modulo p
on suppose que $\overline{a_n}\neq 0$
Alors si $\overline{P}$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$, alors P est irréductible sur $\mathbb{Q}$ (et sur $\mathbb{Z}$ si polynome unitaire)

Ex 19: X^2+3X+1 est irréductible sur $\mathbb{Q}$ car X^2+1 l'est sur $\mathbb{Z}/3\mathbb{Z}$

Réciproque fausse 20: X^4+1 est irréductible sur $\mathbb{Q}$ mais réductible sur tout $\mathbb{Z}/p\mathbb{Z}$.

Prop 21 : Un polynôme P de degré inférieur à 3 est irréductible sur $\mathbb{K}$ ssi P n'a pas de racines dans $\mathbb{K}$

Ex 22 : X^2-3 est irréductible sur $\mathbb{Q}$

Contre exemple 23 : X^4+1 n'a pas de racine dans $\mathbb{R}$ mais $X^4+1 = (X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$

II : Extensions de corps

1) Cadre

Def 24 : Soit $\mathbb{K}$ un corps, on appelle extension de $\mathbb{K}$ tout corps $\mathbb{L}$ contenant un sous corps isomorphe à $\mathbb{K}$.

Prop 25 : Soit $\mathbb{L}/\mathbb{K}$ une extension de $\mathbb{K}$, $\mathbb{L}$ a une structure d'espace vectoriel sur $\mathbb{K}$

Ex 26 : La plus petite extension de $\mathbb{Q}$ contenant $\sqrt{2}$ note $\mathbb{Q}(\sqrt{2})$ est un esp vect de dimension 2 sur $\mathbb{Q}$: $\mathbb{Q}(\sqrt{2}) = \{a+\sqrt{2}b, a,b \in \mathbb{Q}\}$

Def 27 : La dimension de cet espace vectoriel est appelé degré de l'extension $\mathbb{L}/\mathbb{K}$ (il peut être fini ou infini) noté $[\mathbb{L}:\mathbb{K}]$

Ex 28 : $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$

Thm 29 : (Base télescopique). Quelles que soient les extensions de corps $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$, on a
$[\mathbb{M}:\mathbb{K}] = [\mathbb{M}:\mathbb{L}][\mathbb{L}:\mathbb{K}]$

Ex 30 : $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$
d'où $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$.

$[\mathbb{Q}(\pi,\sqrt{2}):\mathbb{Q}] = [\mathbb{Q}(\pi,\sqrt{2}):\mathbb{Q}(\pi)][\mathbb{Q}(\pi):\mathbb{Q}]$
d'où $[\mathbb{Q}(\pi,\sqrt{2}):\mathbb{Q}] = \infty$ car $[\mathbb{Q}(\pi):\mathbb{Q}] = \infty$

Appli 31 : Construction à la règle et au compas

2) Corps de rupture, corps de décomposition.

Def 32 : Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ irréductible.
L'extension $\mathbb{L}/\mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ si $\mathbb{L}$ possède une racine de P et pour tout autre corps $\mathbb{M}$ qui contient une racine de P alors $\mathbb{M}$ est une extension de $\mathbb{L}$.

Ex 33 : $\mathbb{C}$ peut être vu comme corps de rupture de X^2+1 sur $\mathbb{R}$.

Appli 34 : Critère de primalité des nombres de Mersenne
N_q premier $\Leftrightarrow (2+\sqrt{3})^{2^{q-1}} \equiv -1 [N_q]$

DEVIS

Thm 35 : Soit $P \in \mathbb{K}[X]$ irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$, unique à isomorphisme près.

Ex 36 : $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[X]/(X^2-2)$

Def 37 : Soit $P \in \mathbb{K}[X]$. On appelle corps de décomposition de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ qui vérifie :
- P est produit de facteurs de degré 1 dans $\mathbb{L}[X]$
- Si $\mathbb{M}$ vérifie cela, alors $\mathbb{M}$ est une extension de $\mathbb{L}$.

Rmq 38 : P n'est pas forcément irréductible

Ex 39 : $\mathbb{C}$ est un corps de décomposition de X^4+1 sur $\mathbb{R}$

Thm 40 : Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près. On le note $D_{\mathbb{K}}(P)$.

Ex 41 : $D_{\mathbb{Q}}(X^3-2) = \mathbb{Q}(\sqrt[3]{2}, i)$

III Théorie algébrique des nombres

1) Extensions algébriques

Def 42 : Soit $\alpha \in \mathbb{L}/\mathbb{K}$, α est dit algébrique sur $\mathbb{K}$ s'il existe un polynôme P sur $\mathbb{K}$, tel que $P(\alpha)=0$
Dans le cas contraire on dit que α est transcendant sur $\mathbb{K}$

Ex 43 : $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ car X^2-2 annule $\sqrt{2}$
i est algébrique sur $\mathbb{Q}$ car X^2+1 annule i
π est transcendant sur $\mathbb{Q}$ (admis)

Thm 44 : Soit α algébrique sur $\mathbb{K}$, il existe un unique polynôme P annulateur de α, unitaire, irréductible sur $\mathbb{K}$ tel que $\mathbb{K}(\alpha) = \mathbb{K}[X]/(P)$
De plus on a $[\mathbb{K}(\alpha):\mathbb{K}]$ = degré de P
P est le polynôme minimal de α sur $\mathbb{K}$.

Rmq 45 : $\mathbb{K}(\alpha)$ est le corps de rupture de P sur $\mathbb{K}$.

Def 46 : Une extension $\mathbb{L}/\mathbb{K}$ est algébrique sur $\mathbb{K}$, si tout élément de $\mathbb{L}/\mathbb{K}$ est algébrique sur $\mathbb{K}$.

Thm 47 : Toute extension $\mathbb{L}/\mathbb{K}$ de degré fini est algébrique sur $\mathbb{K}$

Ex 48 : $\mathbb{Q}(\sqrt{2})$ est algébrique car $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$
$\mathbb{Q}\left(\left(e^{i\frac{2\pi}{n}}\right)_{n\in\mathbb{N}}\right)$ est algébrique mais n'est pas de degré fini

Def 49 : Un corps $\mathbb{K}$ est dit algébriquement clos si tout polynôme non constant de $\mathbb{K}[X]$ a au moins une racine dans $\mathbb{K}$.

Thm 50 : Le corps $\mathbb{C}$ est algébriquement clos

Rmq 51 : Tout polynôme sur $\mathbb{C}$ est produit de facteurs de degré 1.

Def 52 : On appelle clôture algébrique d'un corps $\mathbb{K}$, toute extension $\mathbb{L}$ de $\mathbb{K}$ telle que
(i) $\mathbb{L}$ est algébrique sur $\mathbb{K}$
(ii) $\mathbb{L}$ est un corps algébriquement clos.

Ex 53 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ mais pas de $\mathbb{Q}$

2) Corps de nombre et corps cyclotomique.

Def 54 : Un corps de nombres est une extension $\mathbb{K}$ de $\mathbb{Q}$ de degré fini.

Ex 55 : $\mathbb{Q}(\sqrt{2})$ est un corps de nombre ($\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt[3]{2})$ aussi)

Def 56 : Un corps quadratique est un corps de nombre de degré 2

Prop 57 : Tout corps quadratique s'écrit $\mathbb{Q}(\sqrt{d})$ avec d sans facteur carré.

Ex 58 : $\mathbb{Q}(\sqrt{3})$ est un corps quadratique

Def 59 : Pour ω_n une racine primitive $n^{ième}$ de l'unité on dit que $\mathbb{Q}(\omega_n)$ est une extension cyclotomique de $\mathbb{Q}$

Prop 60 : $[\mathbb{Q}(\omega_n):\mathbb{Q}] = \varphi(n)$ avec φ l'indicatrice d'Euler

Ex 61 : $[\mathbb{Q}(e^{i\frac{2\pi}{5}}):\mathbb{Q}] = 4$ car $\varphi(5)=4$

Def 62 : Le polynôme $\Phi_n(X) = \prod_{\omega\in\Omega_n}(X-\omega)$ où Ω_n est l'ensemble des racines primitives $n^{ième}$ de l'unité
est appelé $n^{ième}$ polynôme cyclotomique

Thm 63 : Pour tout n, les polynômes Φ_n sont irréductibles sur $\mathbb{Q}$

Ex 64 : $\Phi_1(X) = X-1$ $\Phi_2(X) = X+1$ $\Phi_3(X) = X^2+X+1$
$\Phi_4(X) = X^2+1$ $\Phi_5(X) = X^4+X^3+X^2+X+1$

Prop 65 : Pour p premier, $\Phi_p(X) = X^{p-1}+X^{p-2}+\dots+X+1$

AEN2