Leçon 141 : Polynômes irréductibles à une indéterminée : corps de rupture, exemples et applications

Ouvrages : Perrin, Gozard, (Gourdon pour alg. lin.), Francinou 1 (exos agreg)

Notations

I - Irréductibilité

1) Définitions

2) Critères d'irréductibilité

II - Extensions de corps

1) Éléments et extensions algébriques

2) Corps de rupture, corps de décomposition

3) Clôture algébrique

III - Exemples et applications

1) Polynômes cyclotomiques

2) Corps finis

DEV 1 : Φ_n irréductible + lemme

DEV 2 : Formule d'inversion de Möbius et dénombrement des polynômes irréductibles sur $\mathbb{F}_q$.

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

Dans cette leçon, A désigne un anneau commutatif unitaire et K un corps commutatif.
E est un K-espace vectoriel de dimension finie.

I - Irréductibilité

1) Définitions [GOU] [GOZ] [PER]

DEF 1 : Soit $P \in A[X]$. On dit que P est irréductible lorsque $P \notin A[X]^\times (= A^\times)$ et $P = AB \Rightarrow A \in A[X]^\times$ ou $B \in A[X]^\times$.

DEF 2 : Soit $k \subset K$ un sous-corps et $P \in k[X]$. Une racine (ou un zéro) de P dans K est un élément $\alpha \in K$ tel que $P(\alpha) = 0$.
La multiplicité de α comme racine est le plus grand $n \in \mathbb{N}$ tel que $(X-\alpha)^n$ divise $P(X)$ dans $K[X]$.

PROP 3 : Soit $P \in K[X]$. Alors :
- Si $\deg(P) = 1$, P est irréductible sur K
- Si P est irréductible et $\deg(P) > 1$, alors P n'a pas de racines dans K.
- Si $\deg(P) \in \{2;3\}$, P est irréductible si et seulement si P est sans racines dans K.

EX 4 : $(X^2+1)^2$ est sans racine dans $\mathbb{Q}$ mais réductible dans $\mathbb{Q}[X]$.

EX 5 : $P(X) = 2X$ est réductible dans $\mathbb{Z}[X]$.

PROP 6 : Si K est un corps, $K[X]$ est euclidien

THM 7 (Lemme des noyaux) : Soit $u \in \mathcal{L}(E)$ et $P = P_1 \dots P_k \in K[X]$ avec $\forall i \neq j \in [\![1;k]\!]$, $P_i \wedge P_j = 1$. Alors :
$$\ker(P(u)) = \bigoplus_{i=1}^{k} \ker(P_i(u))$$

EX 8 : La décomposition de Ku assure une décomposition de E en sous-espace stable par u.

2) Critères d'irréductibilité [GOZ]

PROP 9 : Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, $a_n \neq 0$, $a_0 \neq 0$.
Soit $\alpha = \frac{p}{q} \in \mathbb{Q}^*$. Si α est racine de P, alors $q \mid a_n$ et $p \mid a_0$.

DEF 10 : Soit A un anneau factoriel. Pour tout polynôme non nul $P \in A[X]$, on appelle contenu de P et on note $c(P)$ le PGCD des coefficients de P. Si $c(P) = 1$, P est dit primitif.

LEMME 11 :
- Le produit de deux polynômes primitifs est primitif
- $\forall (P,Q) \in (A[X] \setminus \{0\})^2$, $c(PQ) = c(P)\,c(Q)$.

THM 12 : Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$ le corps des fractions de A. Soit $P \in A[X]$, $\deg(P) \geq 1$.
P est irréductible dans $A[X]$ si et seulement si P est irréductible dans $K[X]$ et $c(P) = 1$.

EX 13 : Les polynômes irréductibles de $\mathbb{Z}[X]$ sont :
- les nombres premiers et leurs opposés
- les polynômes primitifs de degré ≥ 1 irréductibles dans $\mathbb{Q}[X]$.

THM 14 : Si A est factoriel, alors $A[X]$ est factoriel

THM 15 : Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$
Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$, $\deg(P) \geq 1$. On suppose qu'il existe $p \in A$ irréductible tel que $p \nmid a_n$, $\forall k \in [\![0; n-1]\!]$, $p \mid a_k$ et $p^2 \nmid a_0$. Alors P est irréductible dans $K[X]$.

EX 16 : $\forall n \in \mathbb{N}$, $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ donc dans $\mathbb{Z}[X]$. $\forall p$ premier $\Phi_{p,\mathbb{Q}}(X)$ est irréductible dans $\mathbb{Q}[X]$ donc dans $\mathbb{Z}[X]$.

PROP 17 : Soient K un corps et $P \in K[X]$. Alors P est irréductible ssi $K[X]/(P)$ est un corps.

EX 18 : $\mathbb{R}[X]/(X^2+1)$ est un corps (isomorphe à $\mathbb{C}$).

THM 19 : Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$.
Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$, $\deg(P) \geq 1$. Soit I un idéal premier de A, $B = A/I$ (B est intègre), $L = \mathrm{Frac}(B)$. On suppose $a_n \notin I$, si le réduit modulo I $\tilde{P}(X)$ est irréductible dans $L[X]$, alors P est irréductible dans $K[X]$.

EX 20 : $P(X) = X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$

II - Extensions de corps

1) Eléments et extensions algébriques [PER]

DEF 21 : Soient K, L des corps, $K \subset L$. On dit que L est une extension de corps de K. On note L/K l'extension.

EX 22 : $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{R} \subset \mathbb{R}(X)$ sont des extensions de corps.

DEF 23 : On appelle degré de l'extension L/K la dimension de L en tant que K-espace vectoriel. On le note $[L:K]$.

THM 24 (de la base téléscopique) : Soient $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une K-base de L, $(f_j)_{j\in J}$ une L-base de M. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une K-base de M.

COR 25 : Avec les notations précédentes, si ces quantités sont finies : $[M:K] = [M:L][L:K]$.

DEF 26 : Soit L/K une extension et $A \subset L$. On dit que A engendre L sur K et on note $L = K(A)$ lorsque L est le plus petit sous-corps de L contenant K et A. Si $A = \{\alpha_1, \dots, \alpha_n\}$, on note $L = K(\alpha_1, \dots, \alpha_n)$.
- L/K est dite primitive lorsqu'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

DEF 27 : Soit L/K une extension, $\alpha \in L$. Soit $\varphi : K[T] \to L$ le morphisme défini par $\varphi_{|K} = \mathrm{Id}_K$ et $\varphi(T) = \alpha$.
Si φ est injectif, on dit que α est transcendant sur K. Sinon, on dit que α est algébrique sur K. Le générateur de $\ker(\varphi)$ est appelé polynôme minimal de α sur K. On le note μ_α.

EX 28 : $\sqrt{2}$, i, $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ avec $\mu_{\sqrt{2}}(X) = X^2 - 2$, $\mu_i(X) = X^2 + 1$, $\mu_{\sqrt[3]{2}}(X) = X^3 - 2$.
π et e sont transcendants sur $\mathbb{Q}$ (admis).

THM 29 : Soit L/K une extension et $\alpha \in L$. Les assertions suivantes sont équivalentes :
- α est algébrique sur K
- On a $K[\alpha] = K(\alpha)$
- $[K(\alpha):K] < \infty$

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

DEF 30 : L/K est dite algébrique lorsque : $\forall \alpha \in L$, α est algébrique sur K. L/K est dite finie lorsque $[L:K] < \infty$.

PROP 31 : Si L/K est finie, alors L/K est algébrique.

2) Corps de rupture, corps de décomposition (AFR) (GOZ)

DEF 32 : Soit $P \in K[X]$ irréductible. Une extension L de K est appelée un corps de rupture de P sur K si L est une extension primitive $L = K(\alpha)$ avec $P(\alpha) = 0$.

THM 33 : Soit $P \in K[X]$ irréductible. Il existe un unique corps de rupture de P sur K à isomorphisme près.

EX 34 : $\mathbb{Q}(\sqrt{2})$ est un corps de rupture de $X^2 - 2$.
$\mathbb{C}$ est un corps de rupture de $X^2 + 1$.

DEF 35 : Soit $P \in K[X]$. On appelle corps de décomposition de P sur K toute extension L de K telle que P est scindé dans L et L est minimal pour cette propriété.

THM 36 : Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près. On le note $D_K(P)$.

EX 37 : $D_{\mathbb{Q}}(X^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, j)$, $D_{\mathbb{Q}}(X^4 - 2) = \mathbb{Q}(\sqrt[4]{2}, i)$.

APPLICATION 38 : Tout endomorphisme est trigonalisable sur le corps de décomposition de son polynôme caractéristique.

PROP 39 : Soit $P \in K[X]$. Alors P est irréductible si et seulement si P est sans racines sur toute extension de degré inférieur à $\frac{\deg(P)}{2}$.

REM 40 : En pratique, on utilisera ce critère plutôt pour des corps finis.

PROP 41 : Soit $P \in K[X]$ irréductible de degré n. Soit L une extension de degré m sur K avec $m \wedge n = 1$. Alors P est irréductible dans $L[X]$.

EX 42 : $X^3 + 4X + 2$ est irréductible sur $\mathbb{Q}$ et $\mathbb{Q}(i)$.

3) Clôture algébrique : [GOZ]

PROP 43 : Soit K un corps. Les assertions suivantes sont équivalentes :
- Tout polynôme de degré ≥ 1 de $K[X]$ est scindé sur K.
- Tout polynôme de degré ≥ 1 de $K[X]$ admet une racine dans K.
- Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.
- Toute extension algébrique de K est identique à K.

On dit alors que K est algébriquement clos.

PROP 44 : Tout corps algébriquement clos est infini.

THM 45 : (D'Alembert-Gauss) Le corps $\mathbb{C}$ est algébriquement clos.

COR 46 : Les polynômes irréductibles de $\mathbb{C}[X]$ sont ceux de degré 1.
Les polynômes irréductibles de $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de degré 2 sans racine réelle.

DEF 47: Soit L/K une extension. On dit que L est une clôture algébrique de K lorsque L est algébrique sur K et L est algébriquement clos.

EX 48: $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$

• L'ensemble des éléments de $\mathbb{C}$ algébriques sur $\mathbb{R}$ est une clôture algébrique de $\mathbb{R}$

THM 49: • Tout corps commutatif K admet une clôture algébrique $\tilde{K}$.

• Si $\tilde{K}_1$ et $\tilde{K}_2$ sont deux clôtures algébriques de K, alors il existe un K-isomorphisme de $\tilde{K}_1$ sur $\tilde{K}_2$.

III - Exemples et applications

1) Polynômes cyclotomiques [PER]

DEF 50: Soit K un corps. L'ensemble des racines n-ièmes de l'unité dans K est noté $\mu_n(K) = \{\zeta \in K \mid \zeta^n = 1\}$. Une racine n-ième primitive de 1 est un élément ζ de K tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour $d < n$. On note $\mu_n^*(K)$ l'ensemble des racines n-ième primitive de l'unité dans K.

DEF 51: Le n-ième polynôme cyclotomique $\Phi_{n,K}(X)$ est donné par la formule $\Phi_{n,K}(X) = \prod_{\zeta \in \mu_n^*(K)} (X - \zeta)$.

PROP 52: $\Phi_{n,K}$ est unitaire de degré $\varphi(n)$.

PROP 53: $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.

EX 54: $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, $\Phi_8 = X^4 + 1$

PROP 55: $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$ $\forall n \in \mathbb{N}$. DEV 1 [Gou]

LEMME 56: Soient $P, A, B \in \mathbb{Q}[X]$ non nuls. On suppose que $P \in \mathbb{Z}[X]$ et que $P = AB$, P et A unitaires. Alors A et B sont dans $\mathbb{Z}[X]$.

THM 57: $\forall n \in \mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X)$ est irréductible dans $\mathbb{Q}[X]$

COR 58: Si ζ est une racine primitive n-ième de l'unité dans un corps de caractéristique nulle, son polynôme minimal sur $\mathbb{Q}$ est Φ_n donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$

2) Corps finis [PER]

DEF 59: Soit K un corps. On appelle sous-corps premier de K le plus petit sous-corps de K (contenant 1).

DEF 60: Soit $\varphi : \mathbb{Z} \to K$ le morphisme d'anneaux défini par $\varphi(n) = n \cdot 1 = 1 + \cdots + 1$ (n fois).

$\ker(\varphi)$ est un idéal de $\mathbb{Z}$ de la forme $p\mathbb{Z}$ et comme $\mathbb{Z}/p\mathbb{Z} \simeq \mathrm{Im}(\varphi) \subset K$ donc est intègre, $p\mathbb{Z}$ est un idéal premier : donc $p = 0$ ou p est un nombre premier. p est appelé la caractéristique de K notée $\mathrm{car}(K)$.

PROP 61: Si $\mathrm{car}(K) = p > 0$, $F : K \to K$, $x \mapsto x^p$ est un morphisme de corps.

Si $K = \mathbb{F}_p$, $F = \mathrm{Id}$, Si K est fini, F est bijectif.

THM 62: Soit p un nombre premier et $n \in \mathbb{N}^*$, $q = p^n$.

• Il existe un corps à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

• En particulier, K est unique à isomorphisme près. On le note $\mathbb{F}_q$.

EX 63: $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ $\quad \mathbb{F}_3 = \mathbb{F}_3[X]/(X^2+X-1)$

DEF 64: On définit μ la fonction de Möbius par : $\mu(1) = 1$, $\mu(n) = 0$ si n contient un facteur carré, $\mu(p_1 \cdots p_r) = (-1)^r$ si $p_1, \ldots, p_r$ sont des nombres premiers distincts.

PROP 65: $\forall n \geq 2$, $\sum_{d \mid n} \mu(d) = 0$ DEV 2

THM 66: Soit $f : \mathbb{N}^* \to G$, G groupe abélien. On pose $g(n) = \sum_{d \mid n} f(d)$

Alors $f(n) = \sum_{d \mid n} \mu(\frac{n}{d}) g(d) = \sum_{d \mid n} \mu(d) g(\frac{n}{d})$

THM 67: Soit $n \in \mathbb{N}^*$. On note $A(n,q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles unitaires et de degré n et $I(n,q) = \#A(n,q)$

Alors $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d,q)} P(X)$

THM 68: $I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu(\frac{n}{d}) q^d$, $I(n,q) \underset{+\infty}{\sim} \frac{q^n}{n}$.

REM 69: $\forall n, q$, $I(n,q) \geq 1$.