

Leçon N° 141 : Polynômes irréductibles et une indéterminée. Corps de rupture. Exemples et applications

Dans toute cette leçon, K est un corps commutatif, A est un anneau commutatif unitaire intègre.

I) Préliminaires.

1) Définitions et premières propriétés

Définition 1 : Soit $f \in A[X]$. On dit que f est irréductible lorsque f est non nul et lorsque $\forall (g, h) \in A[X]^2$,

$$(f = gh) \Rightarrow (g \in A[X]^* \text{ ou } h \in A[X]^*)$$

Proposition 2 : Soit $f \in A[X]$ qui irréductible. Si f n'est pas constant et ne peut pas s'écrire comme produit de deux polynômes non constants.

Exemple 3 : $2X$ est réductible dans $\mathbb{Z}[X]$ mais irréductible dans $\mathbb{R}[X]$.

2) $(X^2 + 1)$ est réductible dans $\mathbb{C}[X]$ mais irréductible dans $\mathbb{R}[X]$.

Proposition 4 : Soit $\alpha \in A$, alors α est irréductible dans $A[X]$ si et seulement si α est irréductible dans A .

Proposition 5 : Soit $f \in K[X]$ de degré 2 ou 3, f est irréductible si f n'a pas de racines dans K .

Contre exemple 6 : $(X^2 + 1)^2$ est réductible sur $\mathbb{R}[X]$ sans avoir de racine sur $\mathbb{R}$.

2) quelques critères d'irréductibilité. On suppose A factoriel.

Définition 7 : On dit que $f = \sum_{i=0}^n a_i X^i \in A[X]$ est primitif lorsque $\text{pgcd}(a_i) = 1$.

Exemple 8 : Tout polynôme unitaire est primitif.

2) $2X + 3 \in \mathbb{Z}[X]$ est primitif.

Proposition 8 : Les $pc(A[X])$ irréductibles de $A[X]$ sont les :

- 1) $p \in A$, irréductibles dans A .
- 2) $pc(A[X])$ non constants primitifs et irréductibles dans $\text{Fact}(A[X])$.

Lemme 9 (critère de Gauss) : Soit I un idéal premier de A et $B = A/I$. Soit $\bar{p} = \sum_{i=0}^n \bar{a}_i X^i \in A[X]$ et $\bar{p}$ sa réduction modulo I . Si $\bar{a}_n \neq 0$ dans B , alors :

Si $\bar{p}$ est irréductible sur B ou $\text{Fact}(B)$, alors p est irréductible sur $\text{Fact}(A)$.

Exemple 10 : $X^3 + 462X^2 + 2433X + 67691$ est irréductible sur $\mathbb{Z}$.

Lemme 11 : $\forall p$ premier, $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

Application 12 : $\forall p$ premier, $X^p - X - 1$ est irréductible sur $\mathbb{Z}$.

Proposition 13 (critère d'Eisenstein) : Soit $p = \sum_{i=0}^n a_i X^i \in A[X]$ et p un irréductible de A . Si :

- 1) $\forall i \in \{0, \dots, n-1\}$, $a_i \in pA$
- 2) $\nexists i \in \{0, \dots, n\}$ tel que $a_i \in p^2 A$
- 3) $a_n \notin pA$

alors p est irréductible dans $\text{Fact}(A[X])$.

Application 14 : $\forall p$ premier, $X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Z}$.

Proposition 15 : Si A est factoriel, alors $A[X]$ est factoriel.

Proposition 16 : $K[X]$ est euclidien pour le degré.

II) Corps de rupture / corps de décomposition.

A) Généralités

Définition 17 : Soient $K \subseteq L$ deux corps, on dit que L est une extension de K lorsque $K \subseteq L$.

Proposition 18 : Soit L une extension de K . L est un K -espace vectoriel et de dimension finie, on note $[L:K] = \dim_K L$ appelé degré de L sur K .

Si K et L sont pairs, on a $[L] = [K][L:K]$.

Proposition 19 : (Base des K -vecteurs) Soient $K \subseteq L \subseteq M$ des corps.

Si $(e_i)_{i \in I}$ et $(f_j)_{j \in J}$ sont des bases de L sur K et M sur L .

alors $(e, f)(e, g) \in I \times J$ est une borne de II sur II .

Corollaire 20: (multiplicité des degrés) Si U est un sous-espace, on a $[H:U] = [H:U] \times [U:U]$.

Définition 24: Soit $U \subseteq U$ sous-espace et $B \subseteq U$. On dit que B engendre U sur U lorsque U est le plus petit $\mathbb{C}$ -espace engendré par B et U . On note $U = \langle B \rangle$.

Définition 22: L'endomorphisme α est dit monogène lorsque α est $\mathbb{C}$ -linéaire sur U et $U = \langle \alpha \rangle$.

Proposition 23: $U[\alpha] \subseteq U(\alpha)$ et $U[\alpha] = \{P(\alpha), P \in U[X]\}$ et $U(\alpha) = \{F(\alpha), F \in U(X)\}$.

Définition 24: Soit $U \subseteq U$ sous-espace, $\alpha \in U$, $\varphi: U[X] \rightarrow U$ définie par $\varphi(P) = P(\alpha)$. Soit $U = \langle \alpha \rangle$ et $U = \langle \alpha \rangle$.

Exemple 25: 1) $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ de polynôme minimal $X^2 - 2$.

2) π est transcendant sur $\mathbb{Q}$ (Hilbert's 1st problem).

Proposition 26: Si α est transcendant sur U , $U[\alpha] \cong U[X]$ et $U(\alpha) \cong U(X)$.

Théorème 27: Soit $U \subseteq U$ et $\alpha \in U$. $U[\alpha] \cong U[X]$ et $U(\alpha) \cong U(X)$.

1) α est algébrique sur U , $U[\alpha] \cong U(\alpha)$ et $U(\alpha) \cong U[X]$ et $U(\alpha) \cong U(X)$.

Exemple 28: Soit $U \subseteq U$ sous-espace. On note $U = \langle \alpha \rangle$ et $U = \langle \alpha \rangle$.

Exemple 29: $\mathbb{Q}$ est un sous-espace de $\mathbb{C}$ algébriquement clos.

Définition 30: U est dit algébriquement clos lorsque une des assertions équivalentes suivantes :

1) Tout polynôme non constant de $U[X]$ admet une racine sur U .

2) Tout polynôme non constant de $U[X]$ est divisible par un polynôme de degré 1.

3) Les irréductibles de $U[X]$ sont de degré 1.

4) Si $U \subseteq U$ est algébrique, $U = U$.

Définition - Proposition 31: Soit $P \in U[X]$ irréductible. Une automorphisme α de U est appelé racine de P si $P(\alpha) = 0$. Un tel α existe et est unique si $U = \langle \alpha \rangle$ et $P(\alpha) = 0$. Un tel α existe et est unique si $U = \langle \alpha \rangle$ et $P(\alpha) = 0$.

Exemple 32: 1) $\sqrt{2}$ est une racine de $X^2 - 2$ sur $\mathbb{Q}$ et $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

2) $\mathbb{Q}(\sqrt{2})$ est un corps de racines de $X^2 - 2$ sur $\mathbb{Q}$ et $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Définition - Proposition 33: Soit $P \in U[X]$ de degré n . On appelle corps de racines de P un sous-espace V de U tel que P a toutes ses racines sur V et que V est engendré par ces racines.

Exemple 34: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est un corps de racines de $X^2 - 2$ et $X^2 - 3$ sur $\mathbb{Q}$.

2) Les corps finis

Définition - Proposition 35: $\varphi: \mathbb{Z} \rightarrow U$ est un morphisme de groupes. Son noyau $\ker \varphi$ est de la forme $p\mathbb{Z}$ avec $p \in \mathbb{N}$.

On p premier. Le noyau est appelé caractéristique de U et on le note $\text{car}(U)$.

Proposition 36: Si U est fini, $\text{car}(U) > 0$.

Corollaire 37: Le noyau d'un morphisme fini est un sous-espace fini.

Définition - Proposition 38: Si $\text{car}(U) = p > 0$, on appelle morphisme de Frobenius le morphisme de corps $U \rightarrow U$ défini par $\varphi(x) = x^p$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Si U est fini, φ est une permutation de U et $\varphi^n = \text{id}$.

Théorème 34: Soient p premier, $n \in \mathbb{N}^*$, $q = p^n$.

Il existe un corps $\mathbb{K}$ à q éléments unique à isomorphisme près. C'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$.

Notation 40: Soient p premier, $n \in \mathbb{N}^*$, $q = p^n$.

On note $A(n, p)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_p[X]$ et $I(n, p) = \#A(n, p)$.

Lemme 41: $X^q - X = \prod_{p \in A(n, p)} P$

Définition 42: On appelle fonction de Möbius la fonction définie par: $\mu(n) = \begin{cases} 1 & \text{si } n=1 \\ (-1)^r & \text{si } n = \prod_{i=1}^r p_i \text{, } p_i \text{ sont PPFPs distincts} \\ 0 & \text{si } n \text{ a des facteurs carrés} \end{cases}$

Théorème 43: (formule d'inversion de Möbius) $\forall (n, d) \in (\mathbb{N}^*)^2$.

$$\mu(n) = \sum_{d|n} \mu(d) \iff \mu(n) = \sum_{d|n} \mu(d) \mu\left(\frac{n}{d}\right)$$

Application 44: $\forall n \in \mathbb{N}^*$, $I(n, p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^{\frac{n}{d}}$.
(En particulier, $\forall n \in \mathbb{N}^*$, $I(n, p) \geq 1$ et $I(n, p) \sim \frac{p^n}{n}$).

3) D'autres critères d'irréductibilité

Théorème 45: Soit $P \in \mathbb{K}[X]$ de degré $n > 0$. P est irréductible sur $\mathbb{K}$ si p n'a pas de racines dans tous les extensions $\mathbb{L}$ de $\mathbb{K}$ qui vérifient $[\mathbb{L} : \mathbb{K}] \leq \frac{n}{2}$.

Exemple 46: $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Théorème 47: Soit $P \in \mathbb{K}[X]$ un polynôme irréductible de degré n et soit $\mathbb{L}$ une extension de degré m avec $n \nmid m = 1$. Alors P est encore irréductible sur $\mathbb{L}$.

Exemple 48: $1) X^3 + X + 1$ est irréductible sur $\mathbb{Q}(i)$.

c) si $X^3 + X + 1$ n'a pas de racines dans $\mathbb{F}_p$, il est irréductible sur $\mathbb{F}_p$ et donc aussi sur $\mathbb{F}_{p^3}$ si $3 \nmid p-1$. Mais il est réductible dans $\mathbb{F}_{p^3}$ pour $p \in \mathbb{N}^*$.

III) Cyclotomes

Définition 49: Une racine n -ième primitive du 1 unité est un élément $\zeta_n \in \mathbb{K}_n$ corps de décomposition de $\mathbb{K}_n$ de $X^n - 1$ tel que $\zeta_n^n = 1$ et $\forall d < n$, $\zeta_n^d \neq 1$. On note $\mu_n^*(\mathbb{K}_n)$ l'ensemble.

Proposition 50: $\forall n \in \mathbb{N}^*$, $|\mu_n^*(\mathbb{K}_n)| = \varphi(n)$ où φ est l'indicatrice d'Euler.

Définition 51: Soit $n \in \mathbb{N}^*$, on définit le n -ième polynôme cyclotomique $\Phi_n, \mu \in \mathbb{K}_n[X]$ par $\Phi_n, \mu = \prod_{\zeta \in \mu_n^*(\mathbb{K}_n)} (X - \zeta)$.

Proposition 52: $\forall n \in \mathbb{N}^*$, Φ_n, μ est unitaire à degré $\varphi(n)$.

Proposition 53: $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d|n} \Phi_d$

Exemple 54: $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, $\Phi_5 = X^4 + X^3 + X^2 + X + 1$, $\Phi_6 = X^2 - X + 1, \dots$

Proposition 55: $\forall n \in \mathbb{N}^*$, $\Phi_n, \mu \in \mathbb{Z}[X]$

Théorème 56: $\forall n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Q}$ et sur $\mathbb{R}$.

Corollaire 57: Soit $\zeta \in \mu_n^*(\mathbb{K}_n)$ avec $\text{con}(\zeta) = 0$.

Le polynôme minimal de ζ est Φ_n et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Application 58: $\mu_n^*(\mathbb{K}_n)$

de 2.