

Leçon N° 12.5 : Extensions de corps : Exemples et applications.

Dans toute cette leçon, les corps sont supposés commutatifs.

I) Les techniques vectorielles

1) Degré d'une extension - Éléments algébriques

Définition 1: On dit que U est une extension de K lorsque $K \subseteq U$.

Exemple 2: $\mathbb{R} \subseteq \mathbb{C}$, $\mathbb{R} \subseteq \mathbb{R}(X)$

Proposition 3: Si $K \subseteq U$, U est un K -ev.

Définition 4: Si $\dim_K U < +\infty$, on pose $[U:K] = \dim_K U$.

On appelle ce nombre le degré de U sur K .

Théorème 5: (base télescopique) Soient $K \subseteq U \subseteq M$ des corps, $(e_i)_{i \in I}$ une base de U sur K , $(f_j)_{j \in J}$ une base de M sur U . Alors la famille $(e_i f_j)_{(i,j) \in I \times J}$ est une base de M sur K .

Corollaire 6: (multiplicativité des degrés) Si $K \subseteq U \subseteq M$ et si les degrés sont finis, on a $[M:K] = [M:U] \times [U:K]$.

Exemple 7: $\mathbb{C}$ est de degré 2 sur $\mathbb{R}$.

Définition 8: Si $K \subseteq U$ et $A \subseteq U$ une partie. On dit que A engendre U sur K (noté $U = K(A)$) lorsque U est le plus petit sous-corps de U contenant K et A .

Ex) L'extension $K \subseteq U$ est dite monogène lorsque il $\exists \alpha \in U$ tel que $U = K(\alpha)$.

Remarque 9: Si $K \subseteq U$, $\forall \alpha \in U$, $K[\alpha] \subseteq K(\alpha)$.

Définition 10: Si $K \subseteq U$ et $\alpha \in U$. Soit $\varphi: K[X] \rightarrow U$

le morphisme défini par $\varphi|_K = \text{id}$ et $\varphi(X) = \alpha$.

1) Si φ est injectif, on dit que α est transcendant sur K , $K[X] \xrightarrow{\sim} K[\alpha] \subseteq K(\alpha) \subseteq K(X)$.

2) Sinon on dit que α est algébrique sur K .

Définition - Proposition 11: Si $K \subseteq U$ et soit $\alpha \in U$ algébrique sur K .

Il existe un unique $P \in K[X]$ unitaire non nul tel que $P(\alpha) = 0$.

On appelle le polynôme minimal de α sur K .

Exemples 12: 1) e et π sont transcendents sur $\mathbb{Q}$.

2) X est transcendant sur $K[X]$.

3) $\sqrt{2}, i, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux respectifs $X^2 - 2$, $X^2 + 1$, $X^3 - 2$.

Théorème 13: Si $K \subseteq U$ et $\alpha \in U$, il y a équivalence entre:

1) α est algébrique sur K

2) $K[\alpha] = K(\alpha)$

3) $\dim_K K[\alpha] < +\infty$.

Plus précisément, si P est le polynôme minimal de α , P est irréductible et $\deg P = [K(\alpha):K]$ (est le degré de α).

Définition 14: 1) $K \subseteq U$ est dite purement algébrique lorsque $\forall \alpha \in U$, α est algébrique sur K .

2) $K \subseteq U$ est dite algébrique lorsque $\forall \alpha \in U$, α est algébrique sur K .

Proposition 15: Toute extension pure est algébrique.

Théorème 16: Si $K \subseteq U$, on pose $KA = \{ \alpha \in U \mid \alpha \text{ algébrique sur } K \}$. KA est un sous-corps de U .

Définition 17: K est dite algébriquement clos lorsque une des

conditions équivalentes ci-dessous est vérifiée:

1) $\forall P \in K[X]$ non constant, P admet une racine dans K .

2) $\forall P \in K[X]$ irréductible, P est produit de polynômes de degré 1.

3) Les éléments irréductibles de $K[X]$ sont de la forme $X - \alpha$, $\alpha \in K$.

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

Exemple 18: $\mathbb{C}$ est algébriquement clos.

$\mathbb{R}$ (défini comme en 16)) est algébriquement clos.

2) Applications cellulaires / construction des polyèdres : Constructibilité de la règle et au compas

Définition 19: On considère le plan euclidien $\mathbb{R}^2$ muni de deux points $O = (0, 0)$ et $I = (1, 0)$. Soit $\Gamma \subset \mathbb{R}^2$ et $\Gamma \in \mathbb{R}^2$. On dit que Γ est constructible à partir de A lorsque il existe deux éléments distincts $p, q \in \Gamma$ les deux points affines (P, Q) avec $P \neq Q$, $P, Q \in A$.
b) les cercles centrés en $P \in A$ de rayon QR avec $Q \neq R \in A$.
 Γ est dit constructible lorsque il existe une suite $A_0 \subset \dots \subset A_n$ de parties de $\mathbb{R}^2$ avec : $A_0 = \{O, I\}$, $\Gamma \in A_n$ et $A_i = A_{i-1} \cup \Gamma_i$ où Γ_i est constructible à partir de A_{i-1} .
Soit $x \in \mathbb{R}$. On dit que x est constructible lorsque $(x, 0) \in \Gamma$ est.

Proposition 20: 1) $\sqrt{2} \in \mathbb{Q}$, π est constructible.
2) $\forall x \in \mathbb{R}^*$ constructible, $\sqrt{x}$ est constructible (cf. Annexe).

Précoraire 21: Soit $x \in \mathbb{R}$ constructible. Alors x est algébrique sur $\mathbb{Q}$ et son degré $[\mathbb{Q}(\sqrt{x}) : \mathbb{Q}]$ est une puissance de 2. (ADTIS).
Applications 22: 1) On ne peut pas trisecter l'angle.

- 2) On ne peut pas trisecter l'angle.
- 3) On ne peut pas résoudre la quadrature du cercle (ADTIS).

3) Corps de rupture et corps de décomposition

Définition 23: Soit $P \in \mathbb{K}[X]$ irréductible. Une extension $U \subset \mathbb{K}$ est appelé corps de rupture de P sur $\mathbb{K}$ lorsque U est une extension monogène $U = \mathbb{K}(\alpha)$ avec $P(\alpha) = 0$.

Précoraire 24: Il y a existence au corps de rupture, unique à isomorphisme près.

Définition 25: Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}^*$. On appelle corps de décomposition de P sur $\mathbb{K}$ une extension U de $\mathbb{K}$ qui vérifie

- 1) dans $U[X]$, P est produit de facteurs de degré 1
 - 2) U est minimale pour cette propriété.
- Précoraire 26: $\forall P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près.

Exemple 27: On se place dans $\mathbb{Q}$.

Pour $P = X^3 - 2$, son corps de décomposition est $\mathbb{Q}(\sqrt[3]{2}, j)$

Pour $P = X^4 - 2$, son corps de décomposition est $\mathbb{Q}(\sqrt[4]{2}, i)$.

Définition 28: Une extension U de $\mathbb{K}$ est appelée clôture algébrique de $\mathbb{K}$ lorsque elle vérifie 1) U est algébrique sur $\mathbb{K}$.
2) U est algébrique sur $\mathbb{K}$.

Exemple 29: Il est la clôture algébrique de $\mathbb{R}$ mais pas de $\mathbb{Q}$, c'est $\mathbb{A}^1$.

Application 30: Il y a un nombre non dénombrable d'éléments appartenant à $\mathbb{A}^1$ sur $\mathbb{Q}$. C'est aussi un contre exemple d'une extension algébrique d'un corps fini.

II) Corps finis

Proposition 31: (Ceci est d'Eisenstein). Soit A un anneau premier et soit $U = \mathbb{F}_q(A)$. Soit $P = a_n X^n + \dots + a_1 X + a_0 \in A[X]$ soit $P \in A$ un élément irréductible.

Supposons 1) P divise a_0 , 2) P divise a_i $\forall i \in \{0, n-1\}$, 3) P^2 ne divise pas a_1 .

Alors P est irréductible dans $U[X]$, donc dans $A[X]$ si P est primitif.

Caractérisation et cardinal

Lemme 32: Soit $U \subset \mathbb{K}$ sont deux corps fins avec $\dim U = n$, alors $|U| = |\mathbb{K}|^n$.

Définition - Proposition 33: $\varphi : U \rightarrow U$ est un morphisme d'anneaux.

son noyau $\ker \varphi$ est de la forme P avec $P = 0$ ou premier.

Ce nombre est appelé la caractéristique de $\mathbb{K}$ noté $\text{car}(\mathbb{K})$.

Proposition 34: Si U est fini, $\text{car}(\mathbb{K}) > 0$. Plus précisément $|\mathbb{K}| = p^n$.

Définition - Proposition 35: Si $\text{car}(\mathbb{K}) = p > 0$, on appelle isomorphisme de Frobenius le morphisme de corps $\mathbb{K} \rightarrow \mathbb{K}$

Si $\mathbb{K}$ est fini, c'est un automorphisme.
Si $\mathbb{K} = \mathbb{F}_p$, c'est l'identité.

2) Corps finis et polynômes

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

Proposition 36: Il existe un corps $\mathbb{K}_q$ de q éléments. C'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. Il est unique à isomorphisme près.
On le note $\mathbb{F}_q$.

Proposition 37: $\mathbb{F}_q^*$ est cyclique $\simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

Notation 38: On note $A_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p[X]$ et $I(n, p)$ son cardinal.

Lemme 39: $X^{p^n} - X = \prod_{d|n} \prod_{f \in A_d(p)} f$

Appréhension 40: On appelle la fonction de Möbius en fonction

$$\mu: \mathbb{N} \rightarrow \begin{cases} (-1)^r & \text{si } n = p_1 \dots p_r \\ 0 & \text{si } n \text{ a des facteurs premiers carrés} \end{cases}$$

Proposition 41: (formule d'inversion de Möbius) $\forall (u, v) \in (\mathbb{N}^*)^2$

$$u_n = \sum_{d|n} v_d \iff v_n = \sum_{d|n} \mu(d) u_{n/d}$$

Application 42: $\forall n \in \mathbb{N}^*$, $I(n, p) = \frac{1}{n} \sum_{d|n} \mu(d) p^d$

En particulier, $I(n, p) \sim_{n \rightarrow +\infty} \frac{p^n}{n}$ et dénombre les polynômes irréductibles dans $\mathbb{F}_p[X]$ de tout degré.

III) D'autres critères pour irréductibilité des polynômes

Théorème 43: Soit $P \in \mathbb{K}[X]$ de degré $n > 0$.

P est irréductible sur $\mathbb{K}$ ssi P n'a pas de racines dans toutes les extensions $\mathbb{L}$ de $\mathbb{K}$ qui vérifient: $[\mathbb{L}:\mathbb{K}] \leq \frac{n}{2}$.
Exemple 44: $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Théorème 45: Soit $P \in \mathbb{K}[X]$ un polynôme irréductible de degré n et soit $\mathbb{L}$ une extension de degré m avec $nm = 1$.

Alors P est encore irréductible sur $\mathbb{L}$.

Exemples 46: 1) $X^3 + X + 1$ est irréductible sur $\mathbb{Q}(i)$ et $\mathbb{Q}$.

2) Si $X^3 + X + 1$ n'a pas de racines sur $\mathbb{F}_p$, 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 $3 \mid p-1$.

Théorème 47: Soient A un anneau factoriel et $\mathbb{K} = \mathbb{F}_A(A)$

soit $\mathbb{I}$ un idéal premier de A et $B = A/\mathbb{I}$ le corps de fraction $\mathbb{L}$.

Soit $P = a_n X^n + \dots + a_0 \in A[X]$ et $\bar{P}$ sa réduction modulo

$\mathbb{I}$. Soit $\bar{a}_n \neq 0$.

Alors: ($\bar{P}$ est irréductible sur B ou $\mathbb{L}$).

$\Rightarrow (P \text{ est irréductible sur } \mathbb{K})$.