Leçon 125 : Extensions de corps. Exemples et applications.

Ulmer, Anneaux ...
Gourdon
Francinou (dev 2)

On considère $\mathbb{K}$ et $\mathbb{L}$ des corps commutatifs, tout corps sera supposé commutatif.

I _ Théorie des extensions

1. Degré d'une extension

Définition 1.1 Un sous-corps de $\mathbb{K}$ est un sous-anneau de $\mathbb{K}$ qui est un corps.

Définition 1.2 Une extension d'un corps $\mathbb{K}$, notée $\mathbb{K} \hookrightarrow \mathbb{L}$ ou $\mathbb{L}/\mathbb{K}$, est une paire $(\mathbb{L}, \varphi)$ où $\mathbb{L}$ est un corps et $\varphi : \mathbb{K} \longrightarrow \mathbb{L}$ est un morphisme d'anneaux.

Remarque 1.3 Comme les seuls idéaux d'un corps $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$, tout morphisme d'anneaux de $\mathbb{K}$ dans $\mathbb{L}$ est injectif. Nous pouvons donc identifier $\mathbb{K}$ à son image dans $\mathbb{L}$ et utiliser parfois la notation $\mathbb{K} \subset \mathbb{L}$.

Exemples 1.4

$\mathbb{R} \subset \mathbb{C}$, $\mathbb{R} \subset \mathbb{R}(X)$

Proposition 1.5 Soit $\mathbb{L}/\mathbb{K}$ une extension de corps alors $\mathbb{L}$ et $\mathbb{K}$ ont même caractéristique et même sous-corps premier.

Théorème - Définition 1.6 Soit $\mathbb{L}/\mathbb{K}$ une extension de corps. Le corps $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel et la dimension de $\mathbb{L}$ comme $\mathbb{K}$-espace vectoriel, notée $[\mathbb{L} : \mathbb{K}]$, est appelée degré de l'extension.

Remarque 1.7 Si $\mathbb{K}$ et $\mathbb{L}$ sont des corps finis, on a : $|\mathbb{L}| = |\mathbb{K}|^n$ avec $n = [\mathbb{L} : \mathbb{K}]$.

Exemples 1.8

$[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$

Théorème 1.9 (de la base télescopique) Soient $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ des corps, $(e_i)_i$ une base de $\mathbb{L}$ sur $\mathbb{K}$ et $(f_j)_j$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors la famille $(e_i f_j)_{ij}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.

Corollaire 1.10 (multiplicativité du degré) Soient $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ des corps, on a alors $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

2. Éléments algébriques

Définition 1.11 Soient $\mathbb{L}/\mathbb{K}$ une extension de corps et $\alpha_1, \dots, \alpha_n \in \mathbb{L}$. Le corps $\mathbb{L}(\alpha_1, \dots, \alpha_n)$ est le plus petit sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et les α_i.

Une extension de la forme $\mathbb{K}(\alpha)$ est dite monogène.

Définition 1.12 Soient $\mathbb{L}/\mathbb{K}$ une extension de corps et $\alpha \in \mathbb{L}$. On considère le morphisme $\varphi : \mathbb{K}[X] \longrightarrow \mathbb{L}$ tel que $\varphi(X) = \alpha$ et $\varphi|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$. Alors :

- si φ est injectif, on dit que α est transcendant sur $\mathbb{K}$
- sinon, on dit que α est algébrique sur $\mathbb{K}$. Cela signifie qu'il existe un polynôme $P \neq 0$ tel que $P(\alpha) = 0$. On a $\ker \varphi = (Q)$ où $Q \neq 0$ peut être supposé unitaire. On dit que Q est le polynôme minimal de α.

Exemples 1.13

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

Théorème 1.14 Soient $\mathbb{L}/\mathbb{K}$ une extension de corps et $\alpha \in \mathbb{L}$. Les propriétés suivantes sont équivalentes :

(i) α est algébrique

(ii) $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$

(iii) $\dim_{\mathbb{K}} \mathbb{K}[\alpha] < +\infty$

Proposition 1.15 Soit $\mathbb{L}/\mathbb{K}$ une extension de corps. On note $\mathcal{A}$ l'ensemble des nombres algébriques sur $\mathbb{K}$. Alors :

(i) $\mathcal{A}$ est un sous-corps de $\mathbb{L}$

(ii) si $\mathbb{L}$ est algébriquement clos alors $\mathcal{A}$ est algébriquement clos

(iii) si $\mathbb{K}$ est dénombrable alors $\mathcal{A}$ est dénombrable

développement 1

II – Polynômes et surcorps

1. Adjonction de racines

Définition 2.1 Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Un corps de rupture de P sur $\mathbb{K}$ est une extension monogène $\mathbb{L} = \mathbb{K}(\alpha)$ telle que $P(\alpha) = 0$.

Théorème 2.2 Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$, unique à isomorphisme près.

Exemples 2.3

- $\mathbb{C} := \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de X^2+1 sur $\mathbb{R}$
- $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/(X^3-2)$ est un corps de rupture de X^3-2 sur $\mathbb{Q}$

Définition 2.4 Soit $P \in \mathbb{K}[X]$, on appelle corps de décomposition de P sur $\mathbb{K}$, une extension $\mathbb{L}/\mathbb{K}$ telle que :

- dans $\mathbb{L}[X]$, P est scindé
- $\mathbb{L}$ est minimal pour cette propriété

Théorème 2.5 Tout polynôme $P \in \mathbb{K}[X]$ admet un corps de décomposition, unique à isomorphisme près. On le note $D_{\mathbb{K}}(P)$.

Exemples 2.6

$P = X^2 - 2$, $D_{\mathbb{Q}}(P) = \mathbb{Q}(\sqrt[2]{2})$

$P = X^3 - 2$, $D_{\mathbb{Q}}(P) = \mathbb{Q}(j, \sqrt[3]{2})$

Application 2.7 (théorème de Cayley-Hamilton) Soit $A \in \mathcal{M}_n(\mathbb{K})$, le polynôme caractéristique χ_A est un polynôme annulateur de A.

2. Les corps finis

Théorème 2.8 Soient p un nombre premier, $n \in \mathbb{N}$ et $q := p^n$. Il existe alors un corps $\mathbb{K}$ à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. De plus, $\mathbb{K}$ est unique à isomorphisme près, on le note $\mathbb{F}_q$.

Lemme 2.9 (inversion de Möbius) Soient $f : \mathbb{N}^* \longrightarrow \mathbb{R}$ multiplicative et $g(n) = \sum_{d|n} f(d)$. Alors pour tout $n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

Lemme 2.10 On considère $U(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbb{F}_q[X]$. Alors, pour $d|n$ et $P \in U(d,q)$, $P \mid X^{q^n} - X$ et, si P irréductible divise $X^{q^n} - X$, $\deg P | n$.

Proposition 2.11 Considérons $I(n,q) = \#U(n,q)$. Alors, $I(n,q) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

développement 2

Application 2.12 Pour tout $n \in \mathbb{N}^*$, $I(n,q) \geq 1$ et $I(n,q) \sim \frac{q^n}{n}$.

3. Extensions algébriques

Définition 2.13 Une extension $\mathbb{L}/\mathbb{K}$ est dite algébrique si pour tout $\alpha \in \mathbb{L}$, α est algébrique sur $\mathbb{K}$.

Théorème 2.14 Un corps $\mathbb{K}$ est algébriquement clos si et seulement si il vérifie un des items :

- tout polynôme $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$
- les irréductibles de $\mathbb{K}[X]$ sont les $X-a$, $a \in \mathbb{K}$
- si une extension $\mathbb{L}/\mathbb{K}$ est algébrique, $\mathbb{L} = \mathbb{K}$

Exemple 2.15

$\mathbb{R}$ n'est pas algébriquement clos

Théorème 2.16 (d'Alembert-Gauss) Le corps $\mathbb{C}$ est algébriquement clos.

Remarque 2.17 $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$