Extensions de corps - Exemples et applications

I Notion d'extension

1) Degré d'une extension

Définition 1: Si K et L sont deux corps avec $K \subset L$, on dit que L est une extension (de corps) de K et que K est un sous-corps de L.

Exemples 2: $\mathbb{Q} \subset \mathbb{C}$, $\mathbb{R} \subset \mathbb{R}(X)$, $\mathbb{F}_p \subset \mathbb{F}_{p^n}$

Remarque 3: On ne considérera que des corps commutatifs.

Remarque 4: Si $K \subset L$ sont des corps, L est un K-espace vectoriel

Définition 5: Si $K \subset L$ est une extension et que L est un K-espace vectoriel de dimension finie, alors on appelle degré de L sur K l'entier $[L:K] = \dim_K L$, on dit que l'extension est finie.

Remarque 6: Si K et L sont des corps finis, $|L| = |K|^{[L:K]}$

Théorème 7 (base télescopique): Soit $K \subset L \subset M$ des corps, $(l_i)_{i \in I}$ une base de L sur K, $(m_j)_{j \in J}$ une base de M sur L. Alors $(l_i m_j)_{(i,j) \in I \times J}$ est une base de M sur K. En particulier, si ce sont des extensions finies, $[M:K] = [M:L][L:K]$.

Exemple 8: $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$

2) Extension engendrée par une partie

Définition 9: Soit $K \subset L$ des corps, A une partie de L. On dit que A engendre L sur K, noté $L = K(A)$ si L est le plus petit sous-corps de L contenant K et A.

Exemple 10: $\mathbb{C} = \mathbb{R}(i)$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Définition 11: Soit $K \subset L$ une extension, $\alpha \in L$, $\varphi : K[T] \to L$ le morphisme ~~de~~ donné par $\varphi_{|K} = id_K$ et $\varphi(T) = \alpha$.

— Si φ est injectif, α est dit transcendant sur K.

— Sinon, α est dit algébrique sur K. Alors $\mathrm{Ker}(\varphi) \subset K[T]$ est un idéal engendré par un certain $\pi_\alpha \in K[T] \setminus \{0\}$ unitaire. π_α est appelé polynôme minimal de α sur K.

Exemple 12: e, π sont transcendants sur $\mathbb{Q}$
$\sqrt{2}, i, \sqrt[3]{12}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux $X^2 - 2$, $X^2 + 1$, $X^3 - 12$ respectivement.

Remarque 13: Si α est transcendant, $K(\alpha) \simeq K(T)$

Proposition 14: Soit $K \subset L$ une extension, $\alpha \in L$. α est algébrique sur K si et seulement si $[K(\alpha):K] < +\infty$. Dans ce cas $[K(\alpha):K] = \deg \pi_\alpha$ (π_α: polynôme minimal de α)

Définition 15: Une extension $K \subset L$ est dite algébrique si tout $\alpha \in L$ est algébrique.

Théorème 16: Si $K \subset L$ est une extension, alors $M = \{x \in L \mid x \text{ algébrique sur } K\}$ est un sous-corps de L contenant K, $K \subset M$ est une extension algébrique

Exemple 17: $\mathbb{Q}(\sqrt[7]{5} + \sqrt[13]{7}\sqrt[8]{3})$ est algébrique sur $\mathbb{Q}$

Remarque 18: $\{x \in L \mid x \text{ algébrique sur } K\}$ n'est pas forcément une extension finie de K. (exemple: $K = \mathbb{Q}$)

II Adjonction de racines

1) Corps de rupture et corps de décomposition

Définition 19: Soit K un corps et $P \in K[X]$ irréductible. Une extension $K \subset L$ est appelée corps de rupture de P si $\exists a \in L$, $P(a) = 0$ et $L = K(a)$

Exemple 20: $\mathbb{C}$ est le corps de rupture de $X^2 + 1 \in \mathbb{R}[X]$.

Théorème 21: Soit K un corps, $P \in K[X]$ irréductible. Il existe L un corps de décomposition de P, unique à isomorphisme près.

Définition 22: Soit K un corps, $(P_i)_{i \in I} \in K[X]^I$. On appelle corps de décomposition de $(P_i)_{i \in I}$ une extension L de K telle que chaque P_i est scindé sur L et $L = K(\{x \in K \mid \exists i \in I,\ P_i(x) = 0\})$.

Théorème 23 : Soit $f : K \to K'$ un isomorphisme de corps, $P \in K[X]$ non constant, $\bar{f} : K[X] \to K'[X]$ prolongeant f.
- Il existe L un corps de décomposition de P.
- Si L' est un corps de décomposition de $\bar{f}(P)$, il existe $g : L \to L'$ un isomorphisme de corps vérifiant $g_{|K} = f$.

Remarque 24 : L'isomorphisme g est en général non unique.

Exemples 25 : Pour $X^3 - 2 \in \mathbb{Q}[X]$, c'est $\mathbb{Q}(\sqrt[3]{2}, j)$
Pour $X^4 - 2 \in \mathbb{Q}[X]$, c'est $\mathbb{Q}(\sqrt[4]{2}, i)$

DEV 1

Théorème 26 (élément primitif) : Soit K un corps de caractéristique nulle. Alors toute extension finie de K est monogène.

Contre-exemple 27 : Soit K un corps de caractéristique $p > 0$, $L = K(T, U)$ et $L_0 = K(T^p, U^p)$. Alors L n'est pas une extension monogène de L_0 mais $[L : L_0] = p^2$.

Exemples 28 : $\mathbb{Q}(i, j) = \mathbb{Q}(ij)$, si $p, q \in \mathbb{N}$ sont premiers, $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$

2) Clôture algébrique

Définition 29 : Une extension $K \subset L$ est dite algébriquement fermée si tout $x \in L$ algébrique sur K est dans K.

Proposition 30 : Soit $K \subset L$ une extension. $M = \{x \in L \mid x \text{ alg. sur } K\}$ est algébriquement fermée dans L. M est appelée fermeture algébrique de K dans L.

Théorème 31 : Un corps K est algébriquement clos si et seulement si K est algébriquement fermé dans toutes ses extensions.

Remarque 32 : La fermeture algébrique d'un sous-corps dans un corps algébriquement clos est close (exemple : la fermeture algébrique de $\mathbb{Q}$ de $\mathbb{C}$, de degré infini)

Théorème 33 : Tout corps possède une extension algébriquement close.

Définition 34 : Une extension $K \subset L$ est une clôture algébrique de K si elle est algébriquement close et algébrique.

Théorème 35 (Steinitz) : Tout corps K possède une clôture algébrique L. Si L' en est une autre, il existe un isomorphisme $\theta : L \to L'$ tel que $\theta_{|K} = id_K$.

3) Le cas des corps finis

Définition 36 : Le sous-corps premier d'un corps K est le plus petit sous-corps de K contenant 1.

Proposition 37 : Les sous-corps premiers sont $\mathbb{Q}$ et $\mathbb{Z}/p\mathbb{Z}$ où $p \in \mathbb{N}$ est premier.

Théorème 38 : Soit $p \in \mathbb{N}$ premier, $n \in \mathbb{N}$, $q = p^n$. Il existe un unique corps de cardinal q (unique à isomorphisme près), noté $\mathbb{F}_q$. On peut l'obtenir comme corps de décomposition de $X^q - X \in \mathbb{F}_p[X]$.

Remarque 39 : Si $Q \in \mathbb{F}_p[X]$ est irréductible, $\mathbb{F}_p[X]/(Q) \simeq \mathbb{F}_{p^{\deg Q}}$

Théorème 40 : Avec $K(n,q) = \#\left\{P \in \mathbb{F}_q[X] \;\middle|\; \begin{array}{l} P \text{ irréductible unitaire} \\ \deg P = n \end{array}\right\}$

on a $K(n,q) \underset{n \to \infty}{\sim} \dfrac{q^n}{n}$.

Proposition 41 : L'application $F : \left| \begin{array}{l} \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \\ x \mapsto x^p \end{array} \right.$ est un automorphisme ($p \in \mathbb{N}$ premier, $n \in \mathbb{N}^*$)

Si $d | n$ alors $\mathbb{F}_{p^d} = \mathrm{Fix}(F^d)$

Proposition 42 : Soit $p \in \mathbb{N}$ premier. Alors $\forall m \leq n$, $\mathbb{F}_{p^{m!}} \subset \mathbb{F}_{p^{n!}}$ et

$\overline{\mathbb{F}_p} := \bigcup_{n \in \mathbb{N}^*} \mathbb{F}_{p^{n!}}$ est une clôture algébrique de $\mathbb{F}_p$.

III Construction à la règle et au compas

1) Extensions quadratiques

Notations : $\mathrm{Aut}(K)$: groupe des automorphismes du corps K.

$\mathrm{Inv}(K) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma^2 = id_K\}$.

Proposition 43 : Soit $K \subset L$ une extension avec $\mathrm{car}(K) \neq 2$. L est une extension quadratique de K si et seulement si $\exists a \in L \setminus K$, $a^2 \in K$ et $L = K(a)$

Exemple 44 : $[\mathbb{C}:\mathbb{R}] = 2$, $i^2 = -1 \in \mathbb{R}$; $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, $\sqrt{2}^2 \in \mathbb{Q}$

Proposition 45 : Soit $\sigma \in \mathrm{Inv}(K) \setminus \{id_K\}$ et $L = \mathrm{Fix}(\sigma)$

Alors $[K:L] = 2$ et si $\mathrm{car}(K) \neq 2$, $\exists a \in K$, $a^2 \in L$, $\sigma(a) = -a$ et $K = L(a)$

si $\mathrm{car}(K) = 2$, $\exists (a,\alpha) \in K \times L$, $\begin{cases} a^2 + a + \alpha = 0 \\ \sigma(a) = 1 + a \\ K = L(a) \end{cases}$

Exemple 46 : $\sigma(x \mapsto x^{p^n}) \in \mathrm{Inv}(\mathbb{F}_{p^{2n}}) \setminus \{id\}$

et $\mathrm{Fix}(\sigma) \simeq \mathbb{F}_{p^n}$

2) Nombres constructibles

Définition 47 : Un point $M \in \mathbb{R}^2$ est constructible à la règle et au compas à partir de $A \subset \mathbb{R}^2$ s'il existe $M_0, \dots, M_n \in \mathbb{R}^2$ tels que $M = M_n$ et pour $i \in [\![1,n]\!]$, M_i est l'intersection de deux éléments parmi :

- une droite passant par deux points de $A \cup \{M_0, \dots, M_{i-1}\}$
- un cercle centré en un point de $A \cup \{M_0, \dots, M_{i-1}\}$ et de rayon la distance entre deux points de cet ensemble

Exemple 48 : Les $(x,0) \in \mathbb{Q} \times \mathbb{R}$ sont constructibles à partir de $\{(0,0);(0,1)\} =: A$. Si $x \geq 0$ et $(x,0)$ constructible à partir de A, alors $(\sqrt{x},0)$ l'est aussi

Théorème 49 (Wantzel) : Soit $A = \{(0,0),(1,0)\}$, $K_0 = \mathbb{Q}$ le sous-corps de $\mathbb{R}$ engendré par 0 et 1. Un point $(x,y) \in \mathbb{R}^2$ est constructible à partir de A si et seulement s'il existe des extensions quadratiques $K_0 \subset \dots \subset K_s$ telles que $x, y \in K_s$.

DEV 2

Corollaire 50 : La quadrature du cercle est impossible.

La duplication du cube est impossible.

Proposition 51 (Gauss) : le polygone régulier à n côtés est constructible si et seulement si $n = 2^k p_1 \dots p_r$ où les p_i sont premiers distincts de la forme $2^{2^{k_i}} + 1$.