Extensions de corps. Exemples et applications.

Cadre : Les corps seront tous supposés commutatifs. Soient K et L deux corps.

I) Extensions de corps

A] Définitions

Déf 1 : On dit que L est une extension (de corps) de K s'il existe $i : K \to L$ un morphisme de corps non nul.

Rem 2 : Un morphisme de corps non nul est injectif. Donc dans ce cas $K \hookrightarrow L$ et nous considérons parfois $K \subset L$ en identifiant K et $i(K)$. On note L/K.

Ex 3 : Toute inclusion de corps dans un autre définit en particulier une extension de corps.

Prop 4 : Soit L/K une extension de K. Alors L est un K-espace vectoriel.

Déf 5 : L'extension est dite finie si $\dim_K L < +\infty$. On définit alors le degré de l'extension par $[L:K] = \dim_K L$.

Ex 6 : L'extension $\mathbb{R} \hookrightarrow \mathbb{C}$ est finie de degré 2. En revanche, $\mathbb{Q} \hookrightarrow \mathbb{R}$ n'est pas une extension finie.

Thm 7 (de la base télescopique) : Soient L/K et M/L deux extensions finies. Alors M/K est finie et :
$$[M:K] = [M:L][L:K]$$

Déf 8 : Soient L/K une extension et $A \subset L$. On dit que A engendre L et on note $L = K(A)$ si L est le plus petit sous-corps de L contenant K et A. On dit que l'extension est monogène si $\exists \alpha \in L, A = \{\alpha\}$ et on note $L = K(\alpha)$.

Ex 9 : $\mathbb{C} = \mathbb{R}(i)$

B] Éléments et extensions algébriques

Soit L/K une extension.

Déf 9 : $\alpha \in L$ est dit algébrique sur K s'il existe $P \in K[X]$ non nul tel que $P(\alpha) = 0$. Il est transcendant sinon.

Ex 10 : $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$. Cependant, π est transcendant (admis).

Prop 11 : Soit $\alpha \in L$ algébrique sur K. L'ensemble des polynômes annulateurs de α est un idéal non nul de $K[X]$. On note π_α son unique générateur unitaire appelé polynôme minimal de α sur K.

Prop 12 : Si $\alpha \in L$ est transcendant, alors $K[\alpha] \simeq K[X]$ et $K(\alpha) \simeq K(X)$. En particulier, $K(\alpha) \neq K[\alpha]$.

Thm 13 : Soit $\alpha \in L$. On a équivalence entre :
- α est algébrique sur K
- $K[\alpha] = K(\alpha)$
- $\dim_K K[\alpha] < +\infty$

et dans ce cas $[K(\alpha):K] = \deg \pi_\alpha$.

Ex 14 : Si $\xi_n \in \mathbb{C}$ est n-ème racine primitive de l'unité, alors $[\mathbb{Q}(\xi_n):\mathbb{Q}] = \varphi(n)$ où φ est l'indicatrice d'Euler.

Déf 15 : On dit que L/K est une extension algébrique si $\forall x \in L$, x est algébrique sur K.

Prop 16 : Toute extension finie est algébrique.

Thm 17 : Soient L/K une extension et $M = \{x \in L \mid x \text{ est algébrique sur } K\}$. Alors M est un sous-corps de L. En particulier, $K \hookrightarrow M$ est une extension algébrique.

II) Extensions par adjonction de racines

A] Corps de rupture, de décomposition

Soit $P \in K[X]$.

Def 18 : L/K est dit corps de rupture de P si $\exists \alpha \in L$ / $L = K(\alpha)$ et $P(\alpha) = 0$.

Ex 19 : $\mathbb{C}$ est corps de rupture de X^2+1 sur $\mathbb{R}$.

Thm 20 : Si P est irréductible sur K, alors il existe un corps de rupture, unique à isomorphisme près.

Prop 21 : P est irréductible sur K si et seulement si il n'admet aucune racines dans les extensions L/K telles que $[L:K] \leqslant (\deg P)/2$

Ex 22 : $X^4 - X - 1$ est irréductible sur $\mathbb{F}_2$ (et donc sur $\mathbb{Q}$).

Prop 23 : Si P est irréductible de degré n sur K et que $[L:K] \wedge n = 1$, alors P est irréductible sur L.

Def 24 : L est un corps de décomposition de P si $\exists \alpha_1, \dots, \alpha_n \in L$ / $P(X) = \prod_{i=1}^{n} (X - \alpha_i)$ et $L = K(\alpha_1, \dots, \alpha_n)$.

Ex 25 : $\mathbb{C}$ est corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$.

Thm 26 : Il existe un corps de décomposition de P sur $\mathbb{Q}$, unique à isomorphisme près.

App 27 : Soit $A \in \mathcal{M}_n(K)$. On note $C(A)$ son commutant. Alors : $K[A] = C(A) \Leftrightarrow \pi_A = \chi_A$.

B] Application aux corps finis

Def 28 : Soit $\varphi : \mathbb{Z} \to K$, $n \mapsto n.1$. Alors $\exists p \in \mathbb{Z}$, $\ker \varphi = p\mathbb{Z}$. p est appelé caractéristique de K, noté $\operatorname{car} K$.

Prop 29 : Si $K \neq \{0\}$, $\operatorname{car} K = 0$ ou $\operatorname{car} K$ est premier.

Cor 30 : Soit $p = \operatorname{car} K$. Si $p = 0$, $\mathbb{Q} \hookrightarrow K$. Sinon, $\mathbb{F}_p \hookrightarrow K$.

Rem 31 : En particulier, tout corps fini est d'ordre une puissance d'un nombre premier.

Thm 32 : Soient p premier et $n \in \mathbb{N}$. On pose $q = p^n$. Alors il existe un unique corps à q éléments à isomorphisme près, noté $\mathbb{F}_q$.

C] Clôtures algébriques

Thm-def 33 : On a équivalence entre :

(i) Tout polynôme non constant admet une racine dans K.
(ii) Tout polynôme de $K[X]$ est produit de polynômes de degré 1
(iii) Les irréductibles de $K[X]$ sont les $X - a$, $a \in K$.
(iv) L/K algébrique $\Rightarrow L = K$

On dit dans ce cas que K est algébriquement clos.

Def 34 : L/K est une clôture algébrique si L est algébriquement clos et que L/K est algébrique.

Ex 35 : $\overline{\mathbb{Q}} = \{ x \in \mathbb{C} \mid x \text{ algébrique sur } \mathbb{Q} \}$ est une clôture algébrique de $\mathbb{Q}$ distincte de $\mathbb{C}$ ($\pi \notin \overline{\mathbb{Q}}$). $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Thm 36 : (de Steinitz) Tout corps admet une clôture algébrique, unique à isomorphisme près.

Prop 37 : Soient $m \leq n$ deux entiers. Alors $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$

Thm 38 : Soit $p \in \mathbb{N}$ premier. Alors $\bigcup_{n \geq 0} \mathbb{F}_{p^n}$ est une clôture algébrique de $\mathbb{F}_p$.

III) L'an avec les nombres constructibles

A] Le corps des nombres constructibles

Def 39 : Soient $B \subset \mathbb{C}$ fini et $z \in B$. z est dit

Constructible à partir de $\mathcal{B}$ si l'une des conditions suivantes est remplie :
- z est intersection de deux droites passant chacune par 2 points distincts de $\mathcal{B}$ (on parle de droites constructibles par rapport à $\mathcal{B}$)
- z est intersection de deux cercles dont le centre est un point de $\mathcal{B}$ et le rayon la distance entre deux points de $\mathcal{B}$ (on parle de cercles constructibles par rapport à $\mathcal{B}$)
- z est intersection entre une droite et un cercle chacuns constructibles par rapport à $\mathcal{B}$.

Def 40 : z est constructible s'il existe $z_1, \dots, z_n = z$ une suite de complexes tels que $\forall i \in [\![1; n-1]\!]$, z_i est constructible par rapports à $\{0; 1; z_1; \dots; z_{i-1}\}$.

Ex 41 : Si $e^{i\theta}$ est constructible (on dit que l'angle $\theta \in \mathbb{R}$ est constructible) alors $e^{i\frac{\theta}{2}}$ aussi.

Tout nombre rationnel est constructible.

Thm 42 : L'ensemble $\mathbb{E}$ des nombres réels constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

Thm 43 : (de Wantzel) Soit $x \in \mathbb{R}$. x est constructible si et seulement si il existe $\mathbb{Q} = L_1 \subset L_2 \subset L_3 \subset \dots \subset L_n$ des sous-corps de $\mathbb{R}$ tels que $x \in L_n$ et $\forall i \in [\![1; n-1]\!]$, $[L_{i+1} : L_i] = 2$.

Cor 44 : Tout nombre réel constructible est algébrique de degré une puissance de 2.

Rem 45 : La réciproque est fausse.

App 46 : (Quadrature du cercle) $\sqrt{\pi}$ n'est pas constructible

App 47 : (Duplication du cube) $\sqrt[3]{2}$ n'est pas constructible

Cor 48 : $\mathbb{E}$ est le plus petit sous-corps de $\mathbb{R}$ qui soit stable par racine carrée.

B] Constructibilité des polygones réguliers

Soit $n \in \mathbb{N}^*$.

Def 49 : On dit que le polygone régulier à n côtés est constructible si $e^{\frac{2i\pi}{n}}$ est constructible.

Thm 50 : Soient $p \in \mathbb{N}$ premier et $a \in \mathbb{N}^*$. $e^{\frac{2i\pi}{p^a}}$ est constructible si et seulement si $a = 1$ et p est un nombre premier de Fermat : $\exists n \in \mathbb{N}$, $p = 1 + 2^{2^n}$.

Thm 51 : (de Gauss-Wantzel) Le polygone régulier à n côtés est constructible si et seulement si n est produit d'une puissance de 2 et de nombres premiers de Fermat 2 à 2 distincts.

App 52 : Le polygone régulier à $17 = 1 + 2^4$ côtés est constructible

DEV 2

[2]

[2]

Références :
- Cours d'algèbre, Perrin [1]
- Théorie des corps, Carrega [2]