Extension de corps. Exemple et application

k est un corps

I) Généralités

1) Définition et exemples

Déf 1: Une extension de k est un corps (K, f) où K est un corps et $f : k \to K$ un morphisme. f est alors injectif et k s'identifie à $f(k) \subset K$. On fera systématiquement cette identification.

Ex: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Prop 2: Soit $k \subset K$ une extension de corps. K est un k-espace vectoriel et même une k-algèbre. On dit que K est une extension de k si K est une base de K sur k. Le cardinal d'une base de K est le degré $[K:k]$ de l'extension. Une extension de degré fini est dite finie.

Déf 3: $k \subset K$ extension, $S \subset K$. $k[S] = \{P(x_1 \dots x_n),\ n \in \mathbb{N},\ P \in k[X_1 \dots X_n],\ x_1 \dots x_n \in S\}$ est l'anneau k-algèbre de K contenant S.

$k(S) = \{F(x_1 \dots x_n),\ n \in \mathbb{N},\ F \in k(X_1 \dots X_n),\ x_1 \dots x_n \in S,\ F(x_1 \dots x_n) \text{ défini}\}$ est le plus petit sous-corps de K contenant k et S. (sous-extension engendrée)

Thm 4 (base télescopique): Soit $k \subset K \subset L$ des extensions (tour d'extension). Soit $(\alpha_i)_{i \in I}$ base du k-ev K et $(\beta_j)_{j \in J}$ base du K-ev L. Alors $(\alpha_i \beta_j)_{(i,j) \in I \times J}$ est une base du k-ev L. Ainsi
$$[L:k] = [L:K]\,[K:k].$$

Ex: $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}] = 6$.

2) Extensions algébriques et transcendantes

Soit $k \subset K$ extension, $\alpha \in K$

Prop 5: Le morphisme d'anneaux $\varphi : k[X] \to K$, $P \mapsto P(\alpha)$ est soit injectif : alors $\ker \varphi = \{0\}$: α est dit transcendant sur k

. $\ker \varphi = (\Pi_\alpha)$ où Π_α irréductible unitaire : α est algébrique sur k. Π_α est le polynôme minimal de α sur k.

Rq 6: Si α transcendant sur k, $k(\alpha) \simeq k(X)$

On a l'équivalence : α algébrique sur k de polynôme minimal $\Pi_\alpha \iff k[\alpha] = k(\alpha) \iff [k(\alpha):k] < +\infty$ et alors $[k(\alpha):k] = \deg \Pi_\alpha$ et $\{1, \alpha \dots \alpha^{\deg \Pi_\alpha - 1}\}$ est une k-base de $k(\alpha)$.

Ex: $\alpha \sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ et $\Pi_\alpha = X^3 - 2$

Déf 7: $k \subset K$ est algébrique si tout élément de K est algébrique sur k.

Ex: Une extension finie est algébrique.

Cor 8: $k \subset L$ extension.

. Si L/k est de type fini ($L = k(S)$ avec $|S| < +\infty$) et algébrique, elle est finie

. $\{x \in L \mid x \text{ algébrique sur } k\}$ est un sous-corps de L

. Si $L = k(S)$ où les éléments de S sont algébriques, L est algébrique.

Cor 9: Si $k \subset K \subset L$ extensions, L/k algébrique $\iff$ L/K et K/k le sont aussi.

Ex: $\sqrt{2} + \sqrt{3}$ est algébrique sur $\mathbb{Q}$.

$\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ algébrique sur } \mathbb{Q}\}$ est la clôture algébrique de $\mathbb{Q}$ (y plus loin)

Rq: $k \subset K$ algébrique, $\alpha, \beta \in K$ annulés par $P, Q \in k[X]$. Le résultant permet de calculer un polynôme annulant $\alpha + \beta$ ou $\alpha\beta$.

Ex: π, e transcendants sur $\mathbb{Q}$ (admis).

II) Grandes familles d'extensions classiques

1) Corps de rupture et de décomposition

K corps.

Def 10 : Soit $P \in K[X]$ irréductible. Un corps de rupture de P est une extension $K \subset L$ avec $\alpha \in L$ tq $L = K(\alpha)$ et $P(\alpha) = 0$.

Ex : $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2 \in \mathbb{Q}[X]$

Thm 11 : $P \in K[X]$ irréductible admet un unique corps de rupture, unique à isomorphisme près.

Def 12 : Un corps de décomposition de P sur K ($P \in K[X]$ quelconque) est une extension $K \subset L$ tq :
- P est scindé à racines simples dans $L[X]$
- L est engendré sur K par les racines de P.

Thm 13 : $P \in K[X]$. P a un unique corps de décomposition à isomorphisme près.

Ex : $\mathbb{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition de $X^3 - 2 \in \mathbb{Q}[X]$

Def 14 : K est algébriquement clos si il vérifie une des équivalences suivantes :
- $P \in K[X]$ de deg ≥ 1 a une racine dans K
- $P \in K[X]$ est scindé simple sur K
- Les irréductibles de $K[X]$ sont les $X - a$, $a \in K$
- Si $K \subset L$ algébrique, $L = K$.

Def : Une extension $K \subset \overline{K}$ est une clôture algébrique de K si $\overline{K}$ est algébriquement clos et $\overline{K}/K$ est algébrique.

Ex : $\mathbb{Q} \subset \overline{\mathbb{Q}}$ défini précédemment.

Thm 15 : Tout corps admet une unique clôture algébrique à isomorphisme près.

2) Extension séparables et corps finis

K corps.

Prop 16 : $P \in K[X]$. $P \wedge P' = 1$ ssi P n'a que des racines simples dans $\overline{K}$ ssi les facteurs irréductibles de P sont de multiplicité 1 dans $K[X]$. On dit alors que P est séparable.

Def 17 : K est parfait ssi tout polynôme irréductible est séparable.

Def 18 : $k \subset K$. $\alpha \in K$ séparable si π_α est séparable.
$k \subset K$ algébrique est séparable si tout $\alpha \in K$ est séparable.

Prop 19 : Si k parfait, toute extension algébrique est séparable.

Ex : Les corps finis et de caractéristique nulle sont parfaits.

Thm 20 : $k \subset K$ séparable et fini. Alors il existe $\alpha \in K$ tq $K = k(\alpha)$. Dans ce cas les corps L tq $k \subset L \subset K$ sont en nombre fini.

Ex : $\mathbb{F}_p(X^p, Y^p) \subset \mathbb{F}_p(X, Y)$ non séparable.

Prop 21 : Soit K un corps fini. Il existe p premier unique appelé caractéristique de K tq $\mathbb{F}_p \subset K$. Il existe $n \in \mathbb{N}$ tq $|K| = p^n$.

Ex : Il n'y a pas de corps fini de cardinal 6.

Thm 22 : p premier, $n \in \mathbb{N}^*$. Il existe un unique corps de cardinal p^n à isomorphisme près. C'est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_{p^n}$.

Prop 23 : $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n \mid m$ de deg $n \geq 1$

Thm 24 : Le nombre de polynômes irréductibles unitaires sur $\mathbb{F}_q[X]$ est donné par $I(q,n) = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{n/d}$ où μ est la fonction de Möbius. Ce nombre est > 0.

III) Extension cyclotomique et application

1) Extension cyclotomique sur $\mathbb{Q}$

Déf 25 : $n \geq 1$. α est racine primitive $n^{\text{ième}}$ de l'unité ssi α engendre le groupe $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. (Ex racine primitive n-ième de l'unité est $e^{\frac{2i\pi}{n}}$ car $k \wedge n = 1$.

Déf 26 : Le n-ième polynôme cyclotomique est $\Phi_n = \prod_{k \wedge n = 1} \left(X - e^{\frac{2ik\pi}{n}}\right)$.

On note $\xi_n = e^{\frac{2i\pi}{n}}$.

Thm 27 : $X^n - 1 = \prod_{d \mid n} \Phi_d$

- $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$
- Φ_n est irréductible sur $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$

Ex 28 : $\mathbb{Q}(\xi_n)/\mathbb{Q}$ est une extension régulière de degré $\varphi(n)$. C'est le corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$.

2) Application à la constructibilité

Déf 29 : $A \subset \mathbb{R}^2$ et $M \in \mathbb{R}^2$. M est constructible en un pas à partir de A s'il existe deux éléments distincts, droite ou cercle, dont un pas des points de A dont M soit un point d'intersection.

Déf 30 : M est constructible s'il existe $A_0 \subset \dots \subset A_n$ tq $A_0 = \{(0,0), (1,0)\}$, $M \in A_n$, $A_i = A_{i-1} \cup \{M_i\}$ avec M_i constructible en un pas à partir de A_{i-1}, $1 \leq i \leq n$.

$x' \in \mathbb{R}$ est constructible ssi $(x, 0)$ l'est.

Prop 31 : Les points suivants sont constructibles :
$(n, 0), n \in \mathbb{Z}$; $(0, n), n \in \mathbb{Z}$; $(x, 0), x \in \mathbb{Q}$, $\sqrt{n}$ si n constructible.

Thm 32 (Wantzel) : $z \in \mathbb{C}$ (identifié à $\mathbb{R}^2$) est constructible ssi il existe une suite $K_0 = \mathbb{Q} \subset \dots \subset K_n$ de sous corps de $\mathbb{C}$ tq $z \in K_n$ et $\forall i$, $[K_i : K_{i-1}] = 2$.

Cor 33 : $\sqrt[3]{2}$, π ne sont pas constructibles. L'ensemble des nombres constructibles est un sous corps de $\mathbb{C}$.

Déf 33 : Le polygone régulier à n côtés est constructible ssi $\xi_n \in \mathbb{C}$ l'est ssi $\left(\cos\left(\frac{2\pi}{n}\right), \sin\left(\frac{2\pi}{n}\right)\right)$ l'est.

Prop 34 : Si $n = pq$ avec $p \wedge q = 1$. ξ_n constructible ssi ξ_p et ξ_q le sont.

Thm 35 : ξ_n constructible $\Leftrightarrow$ il existe $r \geq 0$, $p_1, \dots, p_r$ premiers de Fermat distincts tq $n = 2^r p_1 \dots p_r$.

Fn : Le polygone régulier à 5 et 17 côtés sont constructibles.

[redacted]