Extensions de corps. Exemples et applications.

125

I] Corps et extension de corps.

1) Définition et premières propriétés

Déf 1: k est un corps si k est un anneau commutatif dont tous les éléments non nuls sont inversibles.

Ex 2: $\mathbb{R}$, $\mathbb{C}$, si A est un anneau intègre alors $Frac(A)$ (son corps des fractions) est un corps. $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Déf 3: On appelle caractéristique d'un corps k l'entier positif générateur de l'idéal $Ker(\varphi) \subseteq \mathbb{Z}$ où $\varphi : \mathbb{Z} \longrightarrow k$ est l'unique morphisme d'anneau.

Rem 4: Si $car(k) = 0$ alors k est infini.

Prop 5: Si $car(k) = p$ alors p est premier.

Notation 6: Soit p un nombre premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps à p éléments.

Ex 7: $Car(\mathbb{R}) = 0$, $Car(\mathbb{F}_p) = p$.

Prop 8: Soit k un corps de caractéristique p premier, on appelle endomorphisme de Frobénius, $\mathcal{F} : \begin{array}{l} k \longrightarrow k \\ x \longmapsto x^p \end{array}$ qui est un $\mathbb{F}_p$-endomorphisme de k. Si k est fini alors $\mathcal{F}$ est un automorphisme et si $k = \mathbb{F}_p$, $\mathcal{F} = id$.

Déf 9: k un corps, on appelle extension de corps de k tout corps K tel qu'il existe un morphisme de corps $j : k \longrightarrow K$ et on note K/k.

Rem 10: Tout morphisme de corps est injectif.

Ex 11: $\mathbb{C}$ est une extension de $\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, tout corps k est une extension de son sous-corps premier. Ainsi tout corps de caractéristique nulle est une extension de $\mathbb{Q}$ et tout corps de caractéristique p est une extension de $\mathbb{F}_p$. $k(T)$ est une extension de k.

Déf/prop 12: Soit K/k alors K est muni d'une structure de k-ev et on pose $[K:k] = dim_k(K)$ qui est le degré de K sur k.

Rem 13: Si k et K sont des corps finis, $|K| = |k|^n$ où $n = [K:k]$

Ex 14: $[k(X):k] = +\infty$, $[\mathbb{R};\mathbb{Q}] = +\infty$ et $[\mathbb{C};\mathbb{R}] = 2$.

Théorème 15: Soit K/k, E un $\mathbb{K}$-ev, $(e_i)_{i\in I}$ une $\mathbb{K}$-base de E et $(\alpha_j)_{j\in J}$ une k-base de K alors $(\alpha_j e_i)_{I\times J}$ est une base de E en tant que k-ev.

Ex 16: $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 4$

Appli 17: les sous-corps de $\mathbb{F}_{64}$ sont les $\mathbb{F}_p^d$ avec $d|6$ [Fig 1]

Cor 18: Soit L/k et K/L alors $[K:k] = [K:L][L:k]$ et si certaines des dimensions sont infinies l'énoncé signifie $[K:k] = +\infty$ si et seulement si $[K:L] = +\infty$ ou $[L:k] = +\infty$.

Déf 19: Soit L/K, on appelle K-automorphisme de L un automorphisme du corps L qui est l'identité sur K. $Aut_K(L)$ est l'ensemble formé par ces automorphismes.

Thm 20: $Aut_K(K(X)) \simeq PGL_2(K)$. Plus précisément, l'application qui a une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ associe la substitution $\sigma_M : F \mapsto F\left(\frac{dX-b}{-cX+a}\right)$ définit un morphisme de groupes σ qui se factorise en un isomorphisme $\hat{\sigma} : PGL_2(K) \longrightarrow Aut_K(K(X))$

2) Extension algébrique.

Déf 21: Soit K/k et A une partie de K. On dit que A engendre K sur k et on écrit $K = k(A)$ si K est le plus petit sous-corps de K contenant k et A. Si A est fini, on note $K = k(\alpha_1, \dots, \alpha_n)$.

• K/k est dite monogène s'il existe $\alpha \in K$ tel que $K = k(\alpha)$.

Rem 22: Soit K/k et $\alpha \in K$. On note $k[\alpha]$ le sous-anneau de K engendré par k et α.

Déf 23 Soit K/k et $\alpha \in K$. Soit $\varphi : k[T] \longrightarrow \mathbb{K}$ défini par $\varphi_{|k} = id_k$ et $\varphi(T) = \alpha$.

1) Si φ est injectif alors α est transcendant sur k

2) Sinon α est algébrique sur k. Il existe donc un unique polynôme

unitaire $P \in R[T]$ non nul tel que $P(\alpha)=0$ et si $I=(Ker\varphi)$, $I=(P)$ et P est appelé polynôme minimal de α sur R.

Ex 24 : e et π sont transcendant sur $\mathbb{Q}$ [Admis], ...

Dans $R(T)$, T est transcendant sur R.

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

Prop 25 : Si α est transcendant sur R alors $R[\alpha] \simeq R[T]$ et $R(\alpha) \simeq R(T)$

Thm 26 : Soit K/R et $\alpha \in K$. On a les équivalences :

1) α est algébrique sur R
2) $R[\alpha] = R(\alpha)$
3) $\dim_R R[\alpha] < +\infty$

Plus précisément si P est le polynôme minimal de α, P est irréductible et $\dim_R R[\alpha] = [R[\alpha] : R] = d°P$. Cet entier est le degré de α.

Déf 27 : K/R est finie si $[K:R] < +\infty$

- K/R est dit algébrique si $\forall \alpha \in K$, α est algébrique sur R.

Rem 28 : K/R est finie $\Rightarrow$ K/R est algébrique

Appli 29 : Si L/K est une extension finie de caractéristique nulle alors $\exists \alpha \in L$ tel que $L = K(\alpha)$ [Thm de l'élément primitif]

Prop 30 $\mathbb{F}_q^*$ est un groupe cyclique avec $q=p^n$, p premier, $n \in \mathbb{N}^*$.

Appli 31 : Soit K un corps fini alors toute extension de degré fini de K est monogène.

Thm 32 Soit L/K et $\Pi = \{x \in L \mid x \text{ est algébrique sur } K\}$ alors Π est un sous-corps de L.

Ex 33 : Soit $A = \{\alpha \in \mathbb{C} \mid \alpha \text{ est algébrique sur } \mathbb{Q}\}$ A est un corps et est algébrique sur $\mathbb{Q}$ mais $A/\mathbb{Q}$ n'est pas finie. En particulier la réciproque de la remarque 28 est fausse.

II] Adjonction de racines

1) Le corps de rupture

Déf 34 : Soit $P \in R[X]$ un polynôme irréductible. K/R est appelé un corps de rupture de P sur R si K est une extension monogène $K = R(\alpha)$ avec $P(\alpha)=0$.

Ex 35 : $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/(X^3-2)$ est le corps de rupture de X^3-2

$\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est le corps de rupture de X^2+1.

$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ est le corps de rupture de X^2+X+1.

Thm 36 : Soit $P \in R[X]$ irréductible. Il existe un corps de rupture de P sur R unique à R-isomorphisme près.

Appli 37 : Irréductibilité de certains polynômes (cf II.4).

Appli 38 Si ζ est une racine primitive n-ième de l'unité alors $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$ où $\varphi(n)$ est l'indicatrice d'Euler.

Prop 39 Pour tout $p \in \mathbb{Z}$ premier avec n, si $n \geq 3$ alors $[\mathbb{Q}(\cos(\frac{2\pi p}{n})):\mathbb{Q}] = \frac{\varphi(n)}{2}$

2) Les corps de décompositions.

Déf 40 : Soit $P \in K[X]$ un polynôme quelconque de degré n. On appelle corps de décomposition de P sur R une extension L/K telle que :

1) Dans $L[X]$, P est scindé
2) L est minimal pour cette propriété ie si L'/K vérifie 1) $\exists \varphi : L \to L'$ R-morphisme de corps.

Ex 41 : $K=\mathbb{Q}$, $P(X) = X^3-2$, $L = \mathbb{Q}(\sqrt[3]{2}, j)$

- $K=\mathbb{Q}$, $P(X) = X^4-2$, $L = \mathbb{Q}(\sqrt[4]{2}, i)$
- $K=\mathbb{Q}$, Φ_n le n-ième polynôme cyclotomique sur $\mathbb{Q}$, $\mathbb{Q}(e^{\frac{2i\pi}{n}})$ est un corps de décomposition de Φ_n.

Thm 42 : $\forall P \in R[X]$ il existe un corps de décomposition de P sur R unique à R-isomorphisme près

Appli 43 : Soit p premier et $q=p^n$ avec $n \in \mathbb{N}^*$.

1) Il existe un corps fini à q éléments. C'est un corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$
2) Si F et F' sont deux corps à q éléments ils sont $\mathbb{F}_p$-isomorphes

3) Clôture algébrique d'un corps

Prop/Déf 44 : K un corps. Les conditions suivantes sont équivalentes :

1) Tout polynôme de degré ≥ 1 de $K[X]$ est scindé sur K

2) Tout polynôme de degré ≥ 1 de $K[X]$ admet au moins une racine dans K.

3) Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.

4) Toute extension algébrique de K est isomorphe à K lui-même.

On dit alors que K est algébriquement clos.

Ex 45 : $\mathbb{Q}$ n'est pas algébriquement clos car X^2-2, X^2+1 et X^2+X+1 n'ont pas de racines dans $\mathbb{Q}$. $\mathbb{R}$ n'est pas algébriquement clos car X^2+1 n'a pas de racines dans $\mathbb{R}$.

Prop 46 : Tout corps algébriquement clos est infini.

Thm 47 : [D'Alembert-Gauss] : $\mathbb{C}$ est algébriquement clos.

Déf 48 : Soit L/K. L est une clôture algébrique de K si et seulement si L est algébrique sur K et est algébriquement clos.

Ex 49 $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Thm 50 . [Steinitz][ADMIS] 1) Tout corps K admet une clôture algébrique $\hat{K}$.

2) Si $\hat{K_1}$ et $\hat{K_2}$ sont deux clôtures algébriques de K alors il existe un K-isomorphisme de $\hat{K_1}$ sur $\hat{K_2}$.

4) Irréductibilité des polynômes et extensions de corps.

Thm 51 : Soit $P\in K[X]$ de degré $n>0$. Alors P est irréductible sur K si et seulement si P n'a pas de racines dans les extensions K de K vérifiant $[K:K]\leq \frac{n}{2}$.

Ex 52 : X^4+X+1 est irréductible sur $\mathbb{F}_2$ et $X^4+8X^2+17X-1$ aussi.

Thm 53 : Soit $P\in K[X]$ irréductible de degré n et K une extension de degré m. Si m et n sont premiers entre eux alors P est irréductible sur K.

Ex 54 : X^3+X+1 est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Q}$.

III] Construction à la règle et au compas [noté constructible]

Déf 55 : P un plan affine orienté. X une partie de P de cardinal ≥ 2. On considère

a) les droites affines (A,B), $(A,B)\in X^2$, $A\neq B$

b) les cercles $C(A,\|AB\|)$, $(A,B)\in X^2$, $A\neq B$.

Π est constructible en un pas à partir de X ssi $\Pi=\{\gamma_1\cap\gamma_2\}$ avec γ_1 et γ_2 une droite ou un cercle, $\gamma_1\neq\gamma_2$.

Déf 56 : Soit $B_0\in P$, $\mathrm{card}(B_0)\geq 2$. Π est constructible à partir de B_0 si $\exists \Pi_1,\dots,\Pi_n$ points de P tq $A_0=B_0$ et $\forall i$ $A_i=A_{i-1}\cup\{\Pi_i\}$ et $\forall i$ Π_i est constructible en un pas à partir de A_{i-1}.

Thm 57 : $E=\{$nombres réels constructibles$\}$ est un sous corps de $\mathbb{R}$ stable par racine carrée.

Prop 58 : F un sous-corps de $\mathbb{R}$, $\mathcal{U}=F\times F$, $D=\{$droites affines$\}$ et $C=\{$cercles$\}$ définies comme dans déf 55 avec $X=\mathcal{U}$. $(d_1,d_2)\in D^2$ et $d_1\neq d_2$ alors : $(C_1,C_2)\in C^2$ et $C_1\neq C_2$

. Si $\Pi\in\{d_1\cap d_2\}$, $\Pi\in\mathcal{U}$

. Si $\Pi\in\{d_1\cap d\gamma_1\}\cup\{C_1\cap C_2\}$ alors $\Pi\in\mathcal{U}$ ou $\exists G$ une extension quadratique de F tel que $\Pi\in G\times G$

Thm 59 [Wantzel] : Soit $t\in\mathbb{R}$, t est constructible ssi $\exists(L_0,\dots,L_p)$ une suite finie de sous corps de $\mathbb{R}$ tel que . $L_0=\mathbb{Q}$, $\forall i\in[\![0,p-1]\!]$ $[L_{i+1}:L_i]=2$ et $t\in L_p$.

Coro 60 Soit $x\in\mathbb{R}$. Si x est constructible alors $\exists c\in\mathbb{N}$ tq $[\mathbb{Q}(x):\mathbb{Q}]=2^c$

Appli 61 : Impossibilité de dupliquer le cube

Appli 62 : $\theta=\pi/9$ n'est pas trisectable.

Prop 63 : Si $a\in\mathbb{R}_+$, a transcendant $\Leftrightarrow\sqrt{a}$ transcendant.

Appli 64 : La quadrature du cercle est impossible.

Déf 65 : Soit $n\in\mathbb{N}^*$. Le polygône régulier à n côtés est constructible si et seulement si $\cos(\frac{2\pi}{n})$ est constructible.

Lemme 66 : Soit $(m,n)\in\mathbb{N}^{*2}$, m et n premiers entre eux. Le polygône régulier à nm côtés est constructible si et seulement si les polygônes réguliers à m et n côtés sont constructibles.

Thm 69 : Soit $n\in\mathbb{N}$, $n\geq 2$. Le polygône régulier à n côtés est constructible ssi

– $\exists\alpha\in\mathbb{N}^*$ tel que $n=2^\alpha$

– $\exists\alpha\in\mathbb{N}$ et $p_1,\dots,p_k$ nombres de Fermat ($2^{2^n}+1$, $n\in\mathbb{N}$) distincts et premiers tel que $n=2^\alpha p_1\dots p_k$

DVT

$$\begin{tikzcd}
 & \mathbb{F}_{64} = \mathbb{F}_{2^6} & \\
\mathbb{F}_{2^2} \arrow[ur, phantom, "\subset" sloped] & & \mathbb{F}_{2^3} \arrow[ul, phantom, "\supset" sloped] \\
 & \mathbb{F}_2 \arrow[ul, phantom, "\subset" sloped] \arrow[ur, phantom, "\subset" sloped] &
\end{tikzcd}$$

Fig 1 : Inclusion des sous-corps de $\mathbb{F}_{64}$.

Références : Audin Géométrie

Perrin Cours d'Algèbre

Gozard Théorie de Galois

Francinou - Gianella Algèbre 1 : exercices de mathématiques pour l'agrégation

~~Spir~~ Szpirglas Algèbre 3.