NOM : ILIQUEL Prénom : Lucas Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : 125 : Extensions de corps, Exemples et applications

Autre sujet :

[Perrin] [Gozard]

I. Généralités sur les extensions de corps

1) Extensions de corps

Définition 1 Soit (L,K) un couple de corps tels que $K \subset L$. On dit que L est une extension du corps K et on note L/K (on dit aussi que K sous corps de L).

Exemple 2 $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}[i]/\mathbb{Q}$ où $\mathbb{Q}[i] = \{a+ib, (a,b) \in \mathbb{Q}^2\}$
$K(X)/K$ pour K corps quelconque.

Rq 3 $L/K \Rightarrow L$ est un K-espace vectoriel.

Déf 4 On pose $\dim_K L =: [L:K]$ le degré de l'extension. Si $[L:K] < +\infty$, on parle d'extension finie.

Ex 5 $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{R}:\mathbb{Q}] = +\infty$ ($\mathbb{R}$ $\mathbb{Q}$-ev de dimension ∞)

Rem 6 $[L:K] = 1 \Leftrightarrow L = K$

Thm 7 (Base télescopique) Soit M/L et L/K deux extensions, et soit $(e_i)_{i\in I}$ L-base de M et $(f_j)_{j\in J}$ K base de L. Alors M/K extension, et une K-base de M est donnée par $(e_i f_j)_{(i,j)\in I\times J}$.

Cor 8 $[M:K] = [M:L][L:K]$ Dès qu'un côté de l'égalité est < ∞

Application 9 $[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}] = 4$

Déf 10 • Soit L/K extension et $A \subset L$. On dit que A engendre L sur K et on note $L = K(A)$ si L est le plus petit sous-corps de L contenant A.
• Si A fini, on dit que $L = K(a_1, \dots, a_n)$ est de type fini. Si A est un singleton, on dit que L est monogène.

Prop 11 Si L/K extension de degré fini, alors elle est de type fini.

Rem 12 Réciproque fausse (par exemple avec $K(X)/K$).

Exemple 13 $\forall a \in K$, $K(a)/K$ est monogène (car $K(a) = K$)

Prop 14 Si $[L:K] = p$ premier, alors l'extension est monogène

2) Morphismes

Déf 15 • Soit L/K et M/K deux extensions. $\varphi : L \to M$ est un K-morphisme de corps si c'est un morphisme de corps et que $\forall x \in K$, $\varphi(x) = x$
• Si $L = M$, on parle de K-endomorphisme. Si f bijectif, c'est un K-isomorphisme. Si $f: L \to L$ K-endomorphisme bijectif, on parle de K-automorphisme.

Rq 16 $f : L \to M$ K-morphisme $\Leftrightarrow$ f morphisme de K-algèbres

Prop-Déf 17 (Groupe de Galois) On note $\mathrm{Gal}(L/K)$ l'ensemble des K-automorphismes de corps de L lorsque L/K extension. C'est un groupe pour $\circ$ et on le nomme groupe de Galois de L/K.

Exemple 18 $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \{id_{\mathbb{R}}\}$, $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{id, z \mapsto \bar{z}\}$

Proposition 19 $|\mathrm{Gal}(L/K)| \leqslant [L:K]$

Proposition 20 Soit $f \in \mathrm{End}(K)$. Alors $\mathrm{Fix}(f) = \{x \in K \mid f(x) = x\}$ est un sous-corps de K

II. Extensions de corps et polynômes

1) Éléments algébriques et transcendants

Déf 21 Soit L/K extension, et soit $\alpha \in L$. Soit $\varphi : K[X] \to L$ le K-morphisme tel que $\varphi(X) = \alpha$. On a 2 possibilités :
1) Si φ injective, on dit que α est transcendant sur K.
2) Sinon α est dit transcendant.

Dans le cas 2, $\exists P \in K[X]$ tel que $P(\alpha) = 0$. L'idéal $\{P \in K[X] \mid P(\alpha) = 0\}$ est principal par principalité de $K[X]$: $\exists! \mu_{\alpha,K}$ polynôme unitaire de $K[X]$ (non nul) tel que $I = (\mu_{\alpha,K})$

Déf 21' $\mu_{\alpha,K}$ ainsi défini est le polynôme minimal de α sur K. Il est unitaire, annule α, ~~et est irréductible~~.

Exemple 22 • (Admis) e et π sont transcendants sur $\mathbb{Q}$.
• $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, $\mu_{\sqrt{2},\mathbb{Q}} = X^2 - 2$.

1'

Proposition 23 Soit α transcendant sur K. alors $K[\alpha] \cong K[T]$ et $K(\alpha) \cong K(T)$.

Rem 24 On a alors $\neg(K[T] \cong K(T))$.

Thm 25 Soit L/K extension et $\alpha \in L$. Sont équivalents :
1) α est algébrique sur K
2) $K[\alpha] \cong K(\alpha)$
3) $[K[\alpha]:K] < +\infty$.

En particulier si ces propriétés sont vérifiées, alors $\mu_{\alpha,K}$ est irréductible sur K et $d^\circ \mu_{\alpha,K} = [K(\alpha):K]$.

Ex 26 $\mathbb{R}/\mathbb{Q}$. $\alpha = 2^{1/n} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ et $\mu_{\alpha,\mathbb{Q}}(X) = X^n - 2$.

Cor 27 En posant $n := [K[\alpha]:K]$ pour α algébrique sur K, la famille $(\alpha^i)_{0 \leq i \leq n-1}$ forme une base de $K[\alpha]$ en tant que K-espace vectoriel.

Rem 28 $\alpha \in L$ algébrique sur K, on dit que $n := [K[\alpha]:K]$ est le degré de α sur K.

Exercice 29 (Extension quadratique). Soit $d \in \mathbb{N}^*$ d n'est pas un carré ssi $[\mathbb{Q}[\sqrt{d}]:\mathbb{Q}] = 1$.
Dans ce cas, $Gal(\mathbb{Q}[\sqrt{d}]/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ contient id et $(a+b\sqrt{d} \mapsto a-b\sqrt{d})$ "conjugaison".

Exercice 30 Construire $\mathbb{Q}[\sqrt{2},\sqrt{3}]$, et exhiber le polynôme minimal de $\sqrt{2}+\sqrt{3}$.

Prop 31 Soit L/K extension. L'ensemble $A := \{\alpha \in L \mid \alpha$ algébrique sur $K\}$ est un sous-corps de L contenant K. Il est appelé fermeture algébrique de K dans L.

Déf 32 L/K extension. On dit que L est une extension algébrique de K si tous ses éléments sont algébriques sur K.

Exemple 33 A défini en 31 est la plus grande extension algébrique de K.

Proposition 34 L/K extension de degré fini $\Rightarrow$ L/K algébrique.

Application 35 Soit $(\alpha_1, \dots, \alpha_s) \in L^s$ où L/K extension, et α_i algébrique sur K $\forall i$. alors $K(\alpha_1, \dots, \alpha_s)/K$ algébrique.

Théorème 36 M/L et L/K extensions (on parle aussi de tour d'extension $K \subset L \subset M$) M/K algébrique $\Leftrightarrow$ M/L et L/K algébriques.

② Adjonction des racines

déf 37 Soit K corps et $P \in K[X]$ irréductible. On appelle corps de rupture de P sur K une extension L telle que $L = K(\alpha)$ où α est racine de P

Exemple 38 si $d^\circ P = 1$, K est un corps de rupture.

Théorème 39 $P \in K[X]$ irréductible admet un corps de rupture, unique à K-isomorphisme près (c'est $K[X]/(P)$).

Proposition 40 Les K-automorphismes de $K[X]/(P)$ corps de rupture de P irréductible correspondent bijectivement aux racines de P.

Exemple 41 Construction du corps $\mathbb{C}$ comme $\mathbb{R}[X]/(X^2+1)$. $Gal(\mathbb{C}/\mathbb{R}) = \{id, z \mapsto \bar{z}\}$

Appli 42 Construction de $\mathbb{F}_2[X]/(X^2+X+1)$ corps à 4 éléments (figure 1)

Déf 43 Soit E/K extension. Soit $P \in K[X]$ de degré $n \in \mathbb{N}^*$. On appelle E corps de décomposition de P sur K si et seulement si : P a toutes ses racines dans E, et celles engendrent E.

Rq 43' Ainsi E extension algébrique de degré fini.

Théorème 44 K corps, $P \in K[X]$ de degré n. alors $\exists E$ corps de décomposition de P sur K tel que $[E:K] \leq n!$ et celui-ci est unique à K-isomorphisme près. On le note $D_K(P)$.

Déf 45 $Gal(D_K(P), K)$ est appelé groupe de Galois de P.

Exercice 46 (Galois inverse) pour p premier $\exists P \in \mathbb{Q}[X]$ de degré p tel que $Gal(D_{\mathbb{Q}}(P)/\mathbb{Q}) \cong \mathfrak{S}_p$. DVPT 1

Exemple 47 $D_{\mathbb{Q}}(X^3-2) = \mathbb{Q}[\sqrt[3]{2}, j]$.

Déf 48 $\bar{K}/K$ extension est appelée clôture algébrique de K si $\bar{K}$ est algébriquement clos (i.e. $\forall P \in \bar{K}[X]$ $d^\circ P \geq 1 \Rightarrow P$ scindé) et $\bar{K}/K$ extension algébrique.

Exemple 49 • $\mathbb{C}$ par D'Alembert-Gauss (clôture algébrique de $\mathbb{R}$) est algébriquement clos.

III. Exemple d'application classique

① Les corps finis

Proposition 50 Soit K corps fini, alors car $K = p$ est un nombre premier et $\exists n \in \mathbb{N}$ tel que $|K| = p^n$.

Exemple 51 Il n'y a pas de corps de cardinal 6.

Prop 52 car $K = p$. K fini. $\varphi_p : x \mapsto x^p$ le morphisme de Frobénius est un automorphisme.

Thm 53 p premier et $n \in \mathbb{N}^*$. Il existe un corps de cardinal p^n : c'est $D_{\mathbb{F}_p}(X^{p^n} - X)$. Le corps est unique à $\mathbb{F}_p$-automorphisme près. On le note $\mathbb{F}_q$ où $q = p^n$.

Proposition 54 $(\mathbb{F}_q^*, \times)$ est un groupe cyclique.

Rem 54' • En général, on ne sait pas trouver un générateur de $\mathbb{F}_q^*$.
• proposition vraie aussi $\forall G \leqslant \mathbb{F}_q^*$.

Application 55 (Polynômes irréductibles sur $\mathbb{F}_p$) $* q = p^n$, on a $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$ où $\pi \in \mathbb{F}_p[X]$ irréductible quelconque de d° n.
$*$ (Admis) Il y a $\frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}$ polynômes irréductibles de degré n sur $\mathbb{F}_p[X]$.

② Construction à la règle et au compas

Soit $O = (0,0)$ et $I = (1,0)$ dans le plan euclidien $\mathbb{R}^2$. On veut étudier les nombres "constructibles à la règle et au compas" à partir de O et I : pour un ensemble de départ A on considère :
ⓐ $\langle P, Q \rangle$ les droites affines où $P, Q \in A^2$, $P \neq Q$.
ⓑ les cercles centrés en $P \in A$ passant par $Q \in A$.

Déf 56 • Soit $A \subset \mathbb{R}^2$ et $M \in \mathbb{R}^2$. On dit que M est constructible en 1 pas à partir de A s'il existe deux éléments distincts de type ⓐ ou ⓑ tel que M en soit un point d'intersection.
• $M \in \mathbb{R}^2$ est dit constructible si il existe une suite $A_0 \subset \dots \subset A_m \subset \mathbb{R}^2$ telle que $A_0 = \{O, I\}$, $M \in A_m$ et $\forall i$ $A_{i+1} = A_i \cup \{M_i\}$ où M_i est A_i-constructible.
• $x \in \mathbb{R}$ est dit constructible si $(x, 0)$ l'est.

Application 57 Les $(n, 0)$, $(0, n)$ $n \in \mathbb{N}$, $(x, 0)$ $x \in \mathbb{Q}$ sont constructibles. $\sqrt{x}$ constructible si x l'est.

Théorème 58 (Wantzel) x constructible $\Leftrightarrow$ $\exists L_1 \subset \dots \subset L_p$ une tour d'extensions telle que $L_1 = \mathbb{Q}$, $x \in L_p$ et $\forall i \in [\![1, p-1]\!]$ $[L_{i+1} : L_i] = 2$

Corollaire 59 x constructible $\Rightarrow$ $[\mathbb{Q}[x] : \mathbb{Q}]$ est une puissance de 2.

Exercices 60 • Impossibilité de trisecter l'angle $\pi/3$.
• Impossibilité de la duplication du cube.
• Impossibilité de la quadrature du cercle

Définition 61 On dit qu'un angle θ est constructible si les conditions équivalentes suivantes sont vérifiées : $\sin\theta$ constructible, $\cos\theta$ constructible ou $(\cos\theta, \sin\theta)$ constructible.

Définition 62 On dit que le polygone régulier à n côtés est constructible si $\frac{2\pi}{n}$ est constructible.

Théorème 63 Les polygones réguliers constructibles ont $n = 2^\alpha p_1 \dots p_r$ côtés où $\alpha \geq 0$ et $\forall i$, $p_i = 1 + 2^{2^{k}}$ un nombre premier de Fermat (et $p_i \neq p_j$ $\forall i \neq j$). DVPT 2

Exemple 64 : Figure 2 : polygone régulier à 5 côtés.

[CARRE GA]

Construction d'un corps à 4 éléments : $\mathbb{F}_2[X]/_{(X^2+X+1)}$

$+$	0	$\bar{1}$	j	j^2
0	0	$\bar{1}$	j	j^2
$\bar{1}$	$\bar{1}$	0	j^2	j
j	j	j^2	0	$\bar{1}$
j^2	j^2	j	$\bar{1}$	0

$\times$	0	$\bar{1}$	j	j^2
0	0	0	0	0
$\bar{1}$	0	$\bar{1}$	j	j^2
j	0	j	j^2	$\bar{1}$
j^2	0	j^2	$\bar{1}$	j

$\mathbb{F}_2[X]/_{(X^2+X+1)} = \mathbb{F}_2[j]$ (j image de X par la surjection canonique $\mathbb{F}_2[X] \to \mathbb{F}_2[X]/_{(X^2+X+1)}$) ($j^2 = j+1$)