

Leçon 12S: Extension de corps, exemples et applications.

I. Notion d'extension de corps M, K corps commutatif.

a) Extension de corps et structure d'espace vectoriel

Def. 1: Si $K \subset L$ on dit que L est une extension de K (note L/K)

Ex. 2: $\mathbb{C}/\mathbb{R}/\mathbb{Q}$

Rap. / Def. 3: L/K , L est K -ev. Si $\dim_K L < \infty$ on pose $\dim_K L := [L:K]$ appelée degré de L sur K .

Thm. 4: (Base télescopique) $M/L/K$ (e_i) base de L sur K , (f_j) base de M sur L alors ($e_i f_j$) est une base de M sur K

Cor. 5: $M/L/K$ eq les degrés sont finis ($[M:K] = [M:L][L:K]$).

b) Éléments algébriques

Def. 6: L/K et $A \subset L$, on dit que A engendre L sur K et on note $L = K(A)$ si L est la plus petite extension de K contenant K et A .
Si $A = \{\alpha_1, \dots, \alpha_n\}$ on note $K(\alpha_1, \dots, \alpha_n)$. L est dite monogène si il existe α tq $L = K(\alpha)$.

Def. 7: L/K , $\alpha \in L$. Si il existe $P \in K[X]$ tq $P(\alpha) = 0$ alors on dit que α est algébrique sur K . Sinon on dit que α est transcendant.

Thm / Def. 8: L/K , $\alpha \in L$. ASSE: (i) α algébrique sur K (ii) $K(\alpha) = K[\alpha]$
(iii) $\dim_K K(\alpha) < \infty$. Si $\mu_{\alpha, K}$ est le pol. minimal de α sur K alors $\dim_K K(\alpha) = \deg(\mu_{\alpha, K})$ cet entier est appelé degré.

Def. 9: Si $\alpha \in L$ est algébrique sur K , alors $\{P \in K[X] \mid P(\alpha) = 0\}$ est un idéal non nul, donc admet un unique générateur ($\mu_{\alpha, K}$) appelé pol. minimal de α sur K .

Ex. 10: i algébrique sur $\mathbb{R}$, $\mu_i = x^2 + 1$, $\sqrt{2}$ algébrique sur $\mathbb{Q}$, $\mu_{\sqrt{2}} = x^2 - 2$

Def. 11: L/K est dite finie si $[L:K] < \infty$. L/K est dite algébrique si $\forall \alpha \in L$ α est algébrique sur K .

Rmq. 12: Toute extension finie est algébrique.

Thm 13: L/K l'ensemble des éléments algébriques sur K est un sous corps de L .

Thm 14: $L/M/K$. L/K est algébrique si M/K et L/M algébrique

Ex. 15: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ algébrique et $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(\sqrt{2})$ algébrique.
Donc $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ algébrique.

II Extension de corps et polynômes

a) Corps de rupture et décomposition

Def. 16: Soit $P \in K[X]$ irréductible. On dit que L est un corps de rupture de P sur K si $\exists \alpha \in L$ tq $P(\alpha) = 0$ et $L = K(\alpha)$

Thm. 17: Soit $P \in K[X]$. Le corps $K(\alpha)$ est l'unique corps de rupture de P à isomorphisme près.

Ex. 18: $\mathbb{C} \simeq \mathbb{R}(\sqrt{2})$
($X^2 + 1$)

Def. 19: Soit $P \in K[X]$ de deg. n . On appelle corps de décomp. de P sur K une extension L/K tq:
• dans $L[X]$ P est produit de facteurs de deg. 1
• L est minimal pour cette ppt.

Thm 20: $\forall P \in K[X]$, il existe un corps de décomp. de P sur K . Celui-ci est unique à iso près. Note $D_K(P)$

Ex. 21: Dans $\mathbb{Q}$, $P = X^3 - 2$ $D_K(P) = \mathbb{Q}(\sqrt[3]{2}, i)$

Thm. 22: (Élément primitif) K corps continu infini. Toute extension L/K est monogène.

b) Cloture algébrique.

Def. 23: K est dit algébriquement clos si il vérifie une de ces propriétés:

- $\forall P \in K[X]$, P admet une racine dans K (P de deg ≥ 1)
- $\forall P \in K[X]$ est produit de pol. de deg. 1.
- Les irr. de $K[X]$ sont $X - a$ ($a \in K$)
- Si L/K algébrique, alors $L = K$.

[PER]
p. 72

Def. 24: $\bar{K}/K$ est une clôture algébrique si $\bar{K}$ algébrique sur K et $\bar{K}/K$ algébrique.

Ex. 25: $\mathbb{C}$ est algébriquement clos (D'Alembert - Gauss)
 $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

c) Application: Construction des corps finis p^{10} et $q=p^m$

Def. 26: On appelle sous corps premier de K le plus petit sous corps de K .

Def. 27: $\varphi: \mathbb{Z} \rightarrow K$, le générateur de $\text{Ker}(\varphi)$ est appelé caractéristique de K , noté $\text{car}(K)$.

Prop. 28: $\text{car}(K)$ est nul ou p premier. Si $\text{car}(K)=0$ alors K est infini et contient $\mathbb{Q}$. Si $\text{car}(K)=p$ le sous corps premier de K est $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Prop. 29: Si $\text{car}(K)=p$ alors $|K|=p^m$ $m \in \mathbb{N}$.

Thm. 30: (Existence et unicité corps finis) Il existe un corps à q éléments, c'est le corps de décomp. de $X^q - X$ sur $\mathbb{F}_p$. Il est unique à iso près et est noté $\mathbb{F}_q$.

d) Critère d'irréductibilité

Thm 31: (Eisenstein) A factoriel, $K = \text{fr}(A)$, $P = a_n X^n + \dots + a_0$ ($a_i \in A$)
 $P \in A$ irréductible. Si:

- $p \nmid a_n$
- $p \mid a_i \quad \forall i \in \{0, \dots, n-1\}$
- $p^2 \nmid a_0$

Alors P irr dans $K[X]$ (et dans $A[X]$ si $\text{pgcd}(a_i)=1$)

Ex. 32: $X^2 + 3X + 12$ est irréductible dans $\mathbb{Q}[X]$

Thm 33: A factoriel, $K = \text{fr}(A)$ et I idéal premier de A et $B = A/I$, $L = \text{fr}(B)$
 $P = a_n X^n + \dots + a_0 \in A[X]$, $\bar{P}$ sa réduction modulo I . Si $\bar{a}_n \neq 0$ et $\bar{P}$ irr. sur L ou B alors P est irr. sur K .

Rmq. 34: le cas d'utilisation fréquent est $A = \mathbb{Z}$, $I = (p)$, $B = \mathbb{F}_p$

Ex. 35: $X^3 + 962X^2 + 2433X - 67691$ irr. sur $\mathbb{Z}$. En effet réduit mod. 2 il reste $X^3 + X + 1$ qui est irr. sur $\mathbb{F}_2$.

Thm. 36: $P \in K[X]$ de deg. n . P irr. sur K si P n'a pas de racines dans K/k tq $[K:k] \leq \frac{n}{2}$.

Thm. 35: $P \in K[X]$ irr. de deg. n et K/k de degré m tq $\text{pgcd}(m, n) = 1$ alors P est irr. sur K .

II - Polynômes cyclotomiques

$\mu_n = \{ \zeta \in \mathbb{C} \mid \zeta^n = 1 \}$ μ_n^* les générateurs de ce groupe.

Def. 36: $n \in \mathbb{N}^*$, on définit le n -ème pol. cyclo:
$$\Phi_n = \prod_{\zeta \in \mu_n^*} (X - \zeta)$$

Prop. 37: $X^n - 1 = \prod_{d \mid n} \Phi_d$

Prop. 38: Φ_n est unitaire de deg. $\phi(n)$ (indicateur d'Euler)

Rmq. 39: Avec 37 on a $\Phi_n(X) = \frac{X^n - 1}{\prod_{d \mid n, d \neq n} \Phi_d(X)}$

Ex. 40: $\Phi_3 = X^2 + X + 1$, $\Phi_5 = X^4 + X^3 + X^2 + X + 1$...

Prop. 41: $\Phi_n \in \mathbb{Z}[X]$

Thm 42: Φ_n est irr. sur $\mathbb{Z}[X]$

Cor. 43: $\zeta \in \mu_n^*$ le pol. min de ζ sur $\mathbb{Q}$ est Φ_n et $[\mathbb{Q}(\zeta):\mathbb{Q}] = \phi(n)$

Thm. 44: (Wedderburn) Tout corps fini est commutatif

[PER]
p. 76
- 79

[PER]
p. 72
- 73

[PER]
p. 80
- 81

[PER]
p. 83
REV

IV. Construction à la règle et au compas

a) Corps des nombres constructibles

Def. 45: $\mathbb{Z} \subset \mathbb{R}^2$ ayant au moins 2 éléments et B fini. Les éléments de B sont appelés point de base.

Un point $M \in \mathbb{R}^2$ est constructible à partir de B si il existe une suite finie de points de $\mathbb{R}^2$ finissant par M :

$M : M_1, \dots, M_n = M$ tq $\forall i \in \{1, \dots, n\}$ M_i est le point d'intersection

- de 2 droites
- d'une droite et d'un cercle.
- de 2 cercles.

Ces droites et cercles sont obtenus à l'aide de $E_i = \{B_1, \dots, B_{n_i}\}$ où :

- chaque droite passe par 2 points distincts de E_i
- chaque cercle est centré en un point de E_i et a pour rayon la distance entre 2 points de E_i

Ex. 46: On prendra $B = \{(0,0), (1,0)\}$

Def. 47: Un réel est dit constructible si c'est une des coordonnées dans $\mathbb{R}^2$ d'un point constructible

Thm. 48: L'ensemble $\mathbb{C}$ des nombres constructibles est un corps de $\mathbb{R}$ stable par racine carrée.

Thm. 49: (Wantzel) $\mathbb{C} \subset \mathbb{R}$ est constructible si $\exists p \geq 1$ et $L_1, \dots, L_p$ des sous corps de $\mathbb{R}$ tq :

- $L_1 = \mathbb{Q}$
- $\forall j \in \{1, \dots, p-1\} \quad L_j \subset L_{j+1}$ et $[L_{j+1} : L_j] = 2$
- $\mathbb{C} \subset L_p$.

Cor. 50: Tout nombre constructible est algébrique de degré 2.

Ex. 51: Duplication du cube est impossible car $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

c) Constructibilité des polygones

Def. 52: Un angle θ est dit constructible si $\cos(\theta)$ est constructible.

Lemme 53: m, n 1^{er} entre eux, $\frac{2\pi}{mn}$ constructible si $\frac{2\pi}{m}$ et $\frac{2\pi}{n}$ sont constructibles

Lemme 54: $n \geq 3$ tq $n = p_1^{a_1} \dots p_k^{a_k}$ (décomp en mb pre) le poly. à n côté est constructible si $\frac{2\pi}{p_i^{a_i}}$ constructible

Théorème 55: p 1^{er} de Fermat ($p = 1 + 2^{2^k}$) alors $\frac{2\pi}{p}$ const.

Thm. 56: angle $\frac{2\pi}{p^a}$ const. Et p 1^{er} ≥ 3 $\frac{2\pi}{p^a}$ const si $a=1$ et p pre de Fermat

Thm. 57: (Gauss-Wantzel) Les polygones réguliers constr. sont ceux à 2^a côté où $2^a p_1 \dots p_r$ (où p_i mb 1^{er} de Fermat) const.

Ref:

[ZPER] Perrin, cours d'algèbre.

[BER] Berhuy, Algèbre le grand combat

[CAR] Carrega, théorie des corps à la règle et au compas