

[Per]
[Goz]

125: Extensions de corps. Exemples et applications

Tous les corps sont commutatifs. K, L, M corps

I - Extensions de corps

1) Définitions et premières propriétés [Per] 65-66

- def extension + exemple $\mathbb{R} \subset \mathbb{C}$ $\mathbb{Q} \subset \mathbb{R}$
- L extension de $K \rightarrow L/K$ ev
- degré extension + exemple
- Base télescopique produit extensions
- $K(A) \subset L \subset K[x] \subset L$

2) Elements et extensions algébriques [Per] 66-67

- morphisme d'évaluation + éléments algébriques et transcendants.
- ex: $e, \pi, \sqrt{2}, i, \dots$
- α transcendant $\rightarrow K(\alpha) \cong K[x] \quad K(\alpha) \cong K(x)$
- α algébrique $\rightarrow K(\alpha) = K[x]$
- $[\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 2$
- extension finie, algébrique
- éléments algébriques = corps

II - Polynômes et extensions

1) Corps de rupture [Per] 70

- def + Th existence + exemple $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$

2) Corps de décomposition [Per] 71-72

- def + Th existence + ex $K = \mathbb{Q} \quad P(x) = x^2 - 2$
 $D_K(P) = \mathbb{Q}(\sqrt[3]{2}, j)$

3) Cloture algebrique [Goz] 62

- prop/def algebriquement clos
- $\mathbb{Q}, \mathbb{R}$ pas alg clos
- Th. Abel-Gauss

III - Applications

1) Corps finis [Per] 72-73

- def corps premiers
- def caracteristique
- existence et unicite corps a q elements
- cors

DEV1

2) Critere d'irreductibilite d'un polynome

- Critere d'Eisenstein

• ex

- P irred $\Leftrightarrow P$ n'a pas de racine [L. K] $\in \mathbb{Z}_2$

78

DEV2

12.5: Extensions de corps. Exemples et applications

Tous les corps sont supposés commutatifs. Soient K, L, M des corps

I-Extensions de corps

1) Définitions et premières propriétés

[Per] 65 Définition 1: On dit que L est une extension de corps de K noté L/K , lorsque $K \subset L$

Exemple 2: $\mathbb{C}$ est une extension de $\mathbb{R}$, $\mathbb{R}$ est une extension de $\mathbb{Q}$

Propriété 3: Si L/K extension de corps, L est un K -ev

Définition 4: On appelle degré de l'extension L/K la dimension de L comme K -ev. On la note $[L:K]$

Exemple 5: $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{R}, \mathbb{Q}] = +\infty$

Théorème 6: (Base télescopique)

Soient $K \subset L \subset M$ des corps, $(e_i)_{i \in I}$ base de L sur K , $(g_j)_{j \in J}$ base de M sur L . Alors la famille $(e_i g_j)_{(i,j) \in I \times J}$ est une base de M sur K

Corollaire 7: Si les extensions sont finies on a
 $[M:K] = [M:L][L:K]$

66 Définition 8: 1) Soit $K \subset L$ une extension et A une partie de L . On dit que A engendre L sur K et on écrit $L = K(A)$

Si L est le plus petit sous-corps de L contenant K .
 Si $A = \{\alpha_1, \dots, \alpha_n\}$, on note $L = K(\alpha_1, \dots, \alpha_n)$

2) L'extension $K \subset L$ est monogène si $L = K(\alpha)$ pour $\alpha \in L$

Remarque 9: Si $K \subset L$ et $\alpha \in L$, on note $K[\alpha]$ le sous anneau de L engendré par K et α . On a $K[\alpha] \subset K(\alpha)$

2) Elements et extensions algébriques

Définition 10: Soit $K \subset L$ extension et $\alpha \in L$. Soit $\varphi: K[x] \rightarrow L$ le morphisme d'évaluation en α .

1) Si φ est injectif, on dit que α est transcendant sur K

2) Sinon on dit que α est algébrique sur K . Ainsi il existe $P \in K[x]$ non nul tel que $P(\alpha) = 0$.

On a $\text{Ker}(\varphi) = (P)$ et on peut supposer P unitaire. On dit que P est le polynôme minimal de α sur K .

Exemples 11: e et π sont transcendants sur $\mathbb{Q}$

$\sqrt{2}, i, \sqrt[3]{2}, \dots$ sont algébriques sur $\mathbb{Q}$.

Proposition 12: Si α est transcendant, $K[\alpha] \cong K[X]$ et $K(\alpha) \cong K(X)$

Théorème 13: Soit $K \subset L$ une extension et $\alpha \in L$. On a les équivalences: 1) α est algébrique sur K

2) $K[\alpha] = K(\alpha)$

3) $[K(\alpha):K] < +\infty$

Si P est le polynôme minimal de α , P est irréductible et on a $[K(\alpha):K] = \deg(P)$. On l'appelle degré de α .

Exemple 14: $[Q(\sqrt{2}):Q]=2$

67

Définition 15: Soit $K \subset L$ une extension. On dit qu'elle est:

1) finie si $[L:K] < +\infty$

2) algébrique si $\forall x \in L, x$ est algébrique sur K

Proposition 16: Toute extension finie est algébrique

Théorème 17: Soit $K \subset L$ une extension. L'ensemble des éléments de L algébriques sur K forment un corps

II - Polynômes et extensions

1) Corps de rupture

70

Définition 18: Soit K corps, $P \in K[x]$ irréductible. Une extension $L \supset K$ est appelée corps de rupture de P sur K si L est une extension monogène $L = K(x)$ avec $P(x) = 0$

Théorème 19: Si $P \in K[x]$ irréductible, il existe un corps de rupture de P sur K , unique à isomorphisme près

Exemple 20: $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$ est un corps de rupture de (x^2+1) sur $\mathbb{R}$.

2) Corps de décomposition

71

Définition 21: Soit $P \in K[x]$ un polynôme de degré n . On appelle corps de décomposition de P sur K une extension L de K telle que: 1) P est scindé dans L
2) L est minimal pour cette propriété

Théorème 22: $\forall P \in K[x]$, il existe un corps de décomposition de P sur K , unique à isomorphisme près. On le note $D_K(P)$

Exemple 23: $K = \mathbb{Q}$, $P(x) = x^3 - 2$ on a $D_K(P) = \mathbb{Q}(\sqrt[3]{2})$

72

3) Cloture algébrique

Proposition 24: On a équivalence entre:

1) Tout polynôme de degré ≥ 1 de $K[x]$ est scindé sur K [G02]

52

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

3) Les seuls polynômes irréductibles de K sont ceux de degré 1.

Définition 25: On dit alors que K est algébriquement clos

Exemple 26: $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos

Théorème 27: (d'Alambert-Gauss) Le corps $\mathbb{C}$ est algébriquement clos

III - Applications

1) Corps finis

Définition 28: On appelle sous-corps premier de K , le plus petit sous-corps de K .

[P]

72

Définition 29: Soit $\varphi: \mathbb{Z} \rightarrow K, n \mapsto n \cdot 1_K$. Alors $\ker \varphi = p\mathbb{Z}$. Le nombre p est appelé la caractéristique du corps K . Il est nul ou premier. On note $\text{car}(K)$

Remarque 30: Si $\text{car}(K)=0$, $\forall \mathbb{Z} \subset K$, K est infini
 2) Si K est fini, on a $\text{car}(K)=p>0$. Le sous corps premier de K est $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. De plus son cardinal est une puissance de p .

73 Théorème 31: Pour tout $q=p^n$ avec p premier et $n \in \mathbb{N}$
 il existe un corps fini $\mathbb{F}_q$ tel que $|\mathbb{F}_q|=q$.
 C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.
 $\mathbb{F}_q$ est unique à isomorphisme près DEV 1

? Corollaire 32: i) $\forall \pi \in \mathbb{F}_p[x]$ irréductible de degré n : $\mathbb{F}_p[x]/\pi \cong \mathbb{F}_q$
 ii) si $\pi \in \mathbb{F}_p[x]$ est irréductible de degré n alors $\pi(x) \mid x^q - x$ dans $\mathbb{F}_p[x]$ et il s'en suit que π est scindé sur $\mathbb{F}_q$.
 2) Critère d'irréductibilité d'un polynôme

Théorème 33: (critère d'Eisenstein) DEV 2
 Soit A un anneau factoriel, $K = \text{Frac}(A)$. Soit $P(X) = \sum_{i=0}^n a_i X^i \in A[X]$. Soit $p \in A$ irréductible tel que:
 i) $p \nmid a_n$
 ii) $p \mid a_i \forall i \in \{0, n-1\}$
 iii) $p^2 \nmid a_0$
 Alors P est irréductible sur K donc sur A si $c(P)=1$

Exemple 3: Si p nombre premier de $\mathbb{N}$
 $P(X) = X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}$.

Théorème 35: Soit $P \in K[x]$ de degré $n > 0$.

P irréductible sur K ssi P n'a pas de racines dans les extensions L de K qui vérifient $[L:K] \leq n/2$

3) Corps cyclotomique?

Permettent lorsqu'un polynôme P ne possède pas de racine sur K d'introduire une racine symbolique dans un surcorps de K

$$\mathbb{Z}[i] \quad x^2 + 1$$

$$\begin{matrix} \mathbb{R} \subset \mathbb{C} \\ \mathbb{Q} \subset \mathbb{R} \\ K \subset L \end{matrix}$$

$$\longrightarrow \text{degré } [\mathbb{C} : \mathbb{R}] = 2$$

Th base télescopique
crucial car permet de
trouver le deg d'une
extension

Elmt et
extensions
algébriques

$$K \subset L \text{ et } \alpha \in L$$

125: Extension de corps
Exemples et applications

$\sqrt{2} \text{ dans } \mathbb{Q}$ } α racine de $P \in K[x]$
 $\Rightarrow$ algébrique
sinon transcendant $\pi, e, \dots$

Polynômes

Corps de rupture

$$\mathbb{C} = \mathbb{R}[x] / (x^2 + 1)$$

On passe d'un corps
où le polynôme est
irréductible à un corps
où il admet une racine

pas forcément
scindé

Corps de décomposition
 P scindé sur ce corps
 $\mathbb{Q}_K(x^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, j)$

$$\begin{aligned} \text{Algébrique: } K[\alpha] &= K(\alpha) \\ [K(\alpha) : K] &< +\infty \end{aligned}$$

Applications

critère d'irréductibilité

DEV2

Corps finis
 $\exists !$ corps q elmts
DEV1

$\longrightarrow$ alg des
t polynôme
est scindé

$\longrightarrow$ d'Alembert-Gauss
 $\mathbb{C}$ alg des