

Leçon 125 : Extensions de corps. Exemples et applications.

Matei Lefebvre

2025/2026

1 Généralités.

1.1 Extensions de corps.

[Goz09], II.1

~ 11 items.

définition extension | remarque : abusivement un sous-corps | exemples | structure de k -algèbre | définition degré | exemples | base télescopique | définition sous-extension | définition sous-extension engendrée, extension monogène | écriture comme corps de fraction | extension finie est de type fini

1.2 Éléments algébriques et transcendants.

[Per96], III.1.a

~ 10 items.

définition algébrique, transcendant | définition polynôme minimal | exemples | polynôme minimal est irréductible, définition degré | caractérisation éléments algébriques | définition extension algébrique : exemple : extension finie | sous-corps des algébriques | exemple : algébriques sur $\mathbb{Q}$ | définition algébriquement clos | D'Alembert-Gauss

1.3 Morphismes de corps.

[Goz09], II.2 et [Les+20], 21

~ 9 items.

définition $\text{Aut}(\mathbb{K})$ | définition k -morphisme, $\text{Aut}(\mathbb{K}/k)$ | $\text{Aut}(\mathbb{K})$ groupe et $\text{Aut}(\mathbb{K}/k)$ sous-groupe | exemples | $\text{Aut}(\mathbb{K}) = \text{Aut}(\mathbb{K}/\mathbb{K}_0)$ | lien extensions d'un morphisme sur $\mathbb{K}[\alpha]$ et conjugués de α | majoration nombre de k -morphismes | définition sous-corps fixe | DEV bonus : Artin

Dbon

Lemme. Si $\mathbb{L}/\mathbb{K}$ est une extension finie et $\mathbb{M}/\mathbb{K}$ une extension quelconque, alors $|\text{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{M})| \leq [\mathbb{L} : \mathbb{K}]$.

Théorème (d'Artin). Si G est un sous-groupe fini de $\text{Aut}(\mathbb{K})$, alors $[\mathbb{K} : \mathbb{K}^G] \leq |G|$. En particulier, $G = \text{Aut}_{\mathbb{K}^G}(\mathbb{K})$ et l'inégalité précédente est en fait une égalité.

[Les+20], 21

2 Extensions particulières.

2.1 Corps de rupture et de décomposition.

[Goz09], V.1-2

~ 8 items.

définition corps de rupture | exemples | existence, unicité | critères irréductibilité polynômes |
exemples | définition corps de décomposition | exemples | existence, unicité

2.2 Corps finis.

[Per96], III.2 et [Goz09], VII

~ 9 items.

caractéristique | morphisme de Frobenius | exemples | existence, unicité corps finis | groupe multiplicatif est cyclique | élément primitif | écriture d'un corps fini comme corps de rupture | exemple |
DEV 1 | sous-corps d'un corps fini

D1

Théorème (Algorithme de Berlekamp). Soit $P = P_1 \dots P_r \in \mathbb{F}_q[X]$ avec $P_1, \dots, P_r$ irréductibles 2 à 2 premiers entre eux. On note $S_P : \mathbb{F}_q[X]/(P) \rightarrow \mathbb{F}_q[X]/(P)$, c'est une application $\mathbb{F}_q$ -linéaire.

$$\overline{Q} \mapsto \overline{Q}^q = \overline{Q(X^q)}$$

On a alors $r = \dim(\ker(S_P - id)) = \deg(P) - \text{rg}(S_P - id)$. Si de plus $r \geq 2$ et $\overline{V} \in \ker(S_P - id) \setminus \mathbb{F}_q$, alors $P = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(P, V - \alpha)$ est une décomposition non triviale de P .

Lemme. Soit $P \in \mathbb{F}_q[X]$, alors :

1. $\text{pgcd}(P, P') = 1 \Leftrightarrow P$ n'a pas de facteur carré.
2. $\text{pgcd}(P, P') = P \Leftrightarrow \exists R \in \mathbb{F}_q[X], P = R^p$.
3. Si on est dans aucun des deux cas précédents, alors $P = \text{pgcd}(P, P') \cdot \frac{P}{\text{pgcd}(P, P')}$ est une décomposition non triviale de P .

(L'algo suivant est sûrement à mettre en annexe).

Algorithme (de factorisation d'un polynôme $P \in \mathbb{F}_q[X]$). Soit $P \in \mathbb{F}_q[X]$.

. Si P est constant :

. Fin de l'algorithme.

. Sinon :

. On calcule $D := \text{pgcd}(P, P')$.

. Si $D = 1$:

. On applique l'algorithme de Berlekamp à P .

. Si $D = P$:

. On trouve $R \in \mathbb{F}_q[X]$ tq $P = R^p$ (il suffit de mettre les coefficients de P à la puissance p^{n-1}).

. On applique l'algorithme à R .

. Sinon :

. On applique l'algorithme à D et $\frac{P}{D}$.

[BMP05], V.3.2 et [Dem09], IX.6

2.3 Extensions cyclotomiques.

[Goz09], VI.1

~ 9 items.

définition racines primitive (dans $\mathbb{C}$), cardinal | obtention des autres racines primitives | définition corps cyclotomique | définition polynôme cyclotomique | $X^n - 1 = \prod_{d|n} \Phi_d$ | $\Phi_n \in \mathbb{Z}[X]$ | formule pour

Φ_{p^n} | Φ_n irréductible sur $\mathbb{Q}$ | corollaire : polynôme minimal

3 Nombres constructibles à la règle et au compas.

[Goz09], IV et [Car01], II.1

~ 6 items.

Définition des nombres constructibles (complexes et réels) | quelques exemples de constructions | théorème de Gauss-Wantzel | corollaire : algébrique de degré une puissance de 2 | problèmes des grecs : quadrature du cercle, duplication du cube et trisection de l'angle | polygones constructibles : DEV 2

D2

Théorème. 1. Soit $n \geq 3$ et $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Alors, $e^{\frac{2i\pi}{n}}$ est constructible si et seulement si les $e^{\frac{2i\pi}{p_j^{\alpha_j}}}$ sont constructibles ;

2. $\forall \alpha \in \mathbb{N}$, $e^{\frac{2i\pi}{2^\alpha}}$ est constructible ;

3. Soient $p \geq 3$ un nombre premier et $\alpha \in \mathbb{N}^*$. Alors, $e^{\frac{2i\pi}{p^\alpha}}$ est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat (i.e. de la forme $p = 2^m + 1$).

[Car01], IV.2 et X.4.1

Références

[Per96] D. PERRIN. *Cours d'algèbre (Agrégation)*. ELLIPSES, 1996. ISBN : 9782729855529.

[Car01] J.C. CARREGA. *Théorie des corps : La règle et le compas*. HERMANN, 2001. ISBN : 9782705614492.

[BMP05] V. BECK, J. MALICK et G. PEYRÉ. *Objectif Agrégation*. H&K, 2005. ISBN : 9782914010924.

[Dem09] M. DEMAZURE. *Cours d'algèbre*. CASSINI, 2009. ISBN : 9782842251277.

[Goz09] I. GOZARD. *Théorie de Galois : Niveau L3-M1*. ELLIPSES, 2009. ISBN : 9782729842772.

[Les+20] D. LESESVRE et al. *131 développements pour l'oral - Agrégation externe Mathématiques/Informatique*. DUNOD, 2020. ISBN : 9782100795567.