

125 Extensions de corps. Exemples et applications.

Sauf mention contraire, les corps sont supposés commutatifs. Soit \mathbb{K} un corps.

I - Extensions de corps

1. Généralités

a. Définition

Définition 1. On appelle **extension** de \mathbb{K} tout corps \mathbb{L} tel que

$$\exists j : \mathbb{K} \rightarrow \mathbb{L} \text{ morphisme de corps}$$

On note cela \mathbb{L}/\mathbb{K} .

[GOZ]
p. 21

Remarque 2. — Si \mathbb{K} est un sous-corps de \mathbb{L} , alors \mathbb{L} est une extension de \mathbb{K} .

- Réciproquement, un morphisme de corps $j : \mathbb{K} \rightarrow \mathbb{L}$ est forcément injectif. Par conséquent, le sous-corps $\mathbb{K}' = j(\mathbb{K})$ de \mathbb{L} est isomorphe à \mathbb{K} .
- Aux notations abusives près, on a donc

$$\mathbb{K} \text{ est un sous-corps de } \mathbb{L} \iff \mathbb{L} \text{ est une extension de } \mathbb{K}$$

Exemple 3. — \mathbb{C} est une extension de \mathbb{R} .

- \mathbb{R} est une extension de \mathbb{Q} .
- $\mathbb{K}(X)$ est une extension de \mathbb{K} .

Proposition 4. Soit \mathbb{L} une extension de \mathbb{K} dont on note j le morphisme d'inclusion. Alors, muni du "produit par un scalaire" défini par

$$\forall \lambda \in \mathbb{K}, \forall x \in \mathbb{L}, \lambda x = j(\lambda) \cdot x$$

\mathbb{L} est une algèbre sur \mathbb{K} .

b. Degré

Définition 5. Soit \mathbb{L} une extension de \mathbb{K} . On appelle **degré** de \mathbb{L}/\mathbb{K} et on note $[\mathbb{L} : \mathbb{K}]$ la dimension de \mathbb{L} considéré comme un espace vectoriel sur \mathbb{K} .

Remarque 6. — $[\mathbb{L} : \mathbb{K}] = 1 \iff \mathbb{L} = \mathbb{K}$.

— Le degré d'une extension peut être fini ($[\mathbb{C} : \mathbb{R}] = 2$) ou infini ($[\mathbb{R} : \mathbb{Q}] = +\infty$).

Théorème 7 (Base télescopique). Soient \mathbb{L} un sur-corps de \mathbb{K} et E un espace vectoriel sur \mathbb{L} . Soient $(e_i)_{i \in I}$ une base de E en tant que \mathbb{L} -espace vectoriel et $(\alpha_j)_{j \in J}$ une base de \mathbb{L} en tant que \mathbb{K} -espace vectoriel.

Alors $(\alpha_j e_i)_{(i,j) \in I \times J}$ est une base de E en tant que \mathbb{K} -espace vectoriel.

Corollaire 8 (Multiplicativité des degrés). Soient \mathbb{L} une extension de \mathbb{K} et \mathbb{M} une extension de \mathbb{L} . Alors, sont équivalentes :

- (i) \mathbb{M} est un \mathbb{K} -espace vectoriel de dimension finie.
- (ii) \mathbb{M} est un \mathbb{L} -espace vectoriel de dimension finie et \mathbb{L} est un \mathbb{K} -espace vectoriel de dimension finie.

On a alors :

$$\dim_{\mathbb{K}}(M) = \dim_{\mathbb{L}}(M) \dim_{\mathbb{K}}(L) \iff [\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$$

c. Générateurs

Définition 9. Soit \mathbb{L} une extension de \mathbb{K} .

- Soit $A \subseteq \mathbb{L}$. On dit que A **engendre** \mathbb{L} sur \mathbb{K} si \mathbb{L} est le plus petit sous corps de \mathbb{L} contenant \mathbb{K} et A . On note cela $\mathbb{L} = \mathbb{K}(A)$ ou, si $A = \{\alpha_1, \dots, \alpha_n\}$ est fini, $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ et \mathbb{L} est alors **de type fini**.
- L'extension \mathbb{L}/\mathbb{K} est dite **monogène** s'il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$.

[PER]
p. 66

Exemple 10. — Une extension \mathbb{L} de \mathbb{K} de degré fini est de type fini sur \mathbb{K} .

- Si $[\mathbb{L} : \mathbb{K}]$ est un nombre premier, alors \mathbb{L} est une extension monogène de \mathbb{K} .

[GOZ]
p. 23

Remarque 11. Si $\mathbb{L} = \mathbb{K}(\alpha)$ est une extension monogène de \mathbb{K} , il n'y a pas unicité de α . Tout élément $u \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(u)$ est appelé **élément primitif** de \mathbb{L}/\mathbb{K} .

[PER]
p. 66

Définition 12. Soient \mathbb{L} une extension de \mathbb{K} et $\alpha \in \mathbb{L}$. On note $\mathbb{K}[\alpha]$ le sous-anneau de \mathbb{L} engendré par \mathbb{K} et α .

Proposition 13. En reprenant les notations précédentes :

- (i) Si $x \in \mathbb{K}[\alpha]$, $x = P(\alpha)$ avec $P \in \mathbb{K}[X]$.
- (ii) Si $x \in \mathbb{K}(\alpha)$, $x = \frac{P(\alpha)}{Q(\alpha)}$ avec $P, Q \in \mathbb{K}[X]$ et $Q(\alpha) \neq 0$.
- (iii) $\mathbb{K}[\alpha] \subseteq \mathbb{K}(\alpha)$.

2. Algébricité

Définition 14. Soient \mathbb{L} une extension de \mathbb{K} et $\alpha \in \mathbb{L}$. Soit $\text{ev}_\alpha : \mathbb{K}[X] \rightarrow \mathbb{L}$ le morphisme d'évaluation en α .

- On note $\text{Ann}(\alpha)$ l'idéal des polynômes annulateurs de α . Notons qu'on a $\text{Ann}(\alpha) = \text{Ker}(\text{ev}_\alpha)$.
- Si ev_α est injectif, on dit que α est **transcendant** sur \mathbb{K} .
- Sinon, α est dit **algébrique** sur \mathbb{K} .

Exemple 15. — e et π sont transcendants sur \mathbb{Q} (théorèmes d'Hermite et de Lindemann).

- $\sqrt{2}, i, \dots$ sont algébriques sur \mathbb{Q} .

Proposition 16. Soient \mathbb{L} une extension de \mathbb{K} et $\alpha \in \mathbb{L}$. Les assertions suivantes sont équivalentes.

- (i) α est algébrique sur \mathbb{K} .
- (ii) $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.
- (iii) $[\mathbb{K}[\alpha] : \mathbb{K}] < +\infty$.

Proposition 17. En reprenant les notations précédentes, si α est transcendant, on a

$$\mathbb{K}[\alpha] \cong \mathbb{K}[X] \text{ et } \mathbb{K}(\alpha) \cong \mathbb{K}(X)$$

Définition 18. Soient \mathbb{L} une extension de \mathbb{K} et $\alpha \in \mathbb{L}$. Si α est algébrique sur \mathbb{K} , alors $\text{Ann}(\alpha)$ est un idéal principal non nul. Donc, il existe $P \in \mathbb{K}[X]$ unitaire tel que $\text{Ann}(\alpha) = (P)$. On note π_α ce polynôme P : c'est le **polynôme minimal** de α sur \mathbb{K} .

Exemple 19. Sur \mathbb{Q} , on a $\pi_{\sqrt{2}} = X^2 - 2$ et $\pi_i = X^2 + 1$.

Proposition 20. Soient \mathbb{L} une extension de \mathbb{K} et $\alpha \in \mathbb{L}$. Soient $P \in \mathbb{K}[X]$. Les assertions suivantes sont équivalentes :

- (i) $P = \pi_\alpha$.
- (ii) $P \in \text{Ann}(\alpha)$ et est unitaire et $\forall R \in \text{Ann}(\alpha) \setminus \{0\}, \deg(P) \leq \deg(R)$.
- (iii) $P \in \text{Ann}(\alpha)$ et est unitaire et irréductible dans $\mathbb{K}[X]$.

[GOZ]
p. 31

Définition 21. Soit \mathbb{L} une extension de \mathbb{K} .

- \mathbb{L}/\mathbb{K} est dite **finie** si $[\mathbb{L} : \mathbb{K}] < +\infty$.
- \mathbb{L}/\mathbb{K} est dite **algébrique** si tout élément de \mathbb{L} est algébrique sur \mathbb{K} .

[PER]
p. 67

Proposition 22. Toute extension finie est algébrique.

Contre-exemple 23. On considère

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ est algébrique sur } \mathbb{Q}\}$$

alors, $\overline{\mathbb{Q}}$ est une extension algébrique de \mathbb{Q} mais n'est pas finie (cf. Application 26).

Lemme 24 (Gauss). Soit A un anneau factoriel. Alors :

- (i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est associé à 1).
- (ii) $\forall P, Q \in A[X] \setminus \{0\}, \gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

[GOZ]
p. 10

[DEV]

Théorème 25 (Critère d'Eisenstein). On suppose que \mathbb{K} le corps des fractions d'un anneau factoriel A . Soit $P = \sum_{i=0}^n a_i X^i \in A[X]$ de degré $n \geq 1$. On suppose qu'il existe $p \in A$ irréductible tel que :

- (i) $p \mid a_i, \forall i \in \llbracket 0, n-1 \rrbracket$.
- (ii) $p \nmid a_n$.
- (iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{K}[X]$.

Application 26. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur \mathbb{Z} .

[PER]
p. 67

II - Adjonction de racines

1. Corps de rupture

Définition 27. Soient \mathbb{L} une extension de \mathbb{K} et $P \in \mathbb{K}[X]$ irréductible. On dit que \mathbb{L} est un **corps de rupture** de P si $\mathbb{L} = \mathbb{K}[\alpha]$ où $\alpha \in \mathbb{L}$ est une racine de P .

[GOZ]
p. 57

Exemple 28. En reprenant les notations précédentes, si $\deg(P) = 1$, alors \mathbb{K} est un corps de rupture de P .

Théorème 29. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur \mathbb{K} .

- Il existe un corps de rupture de P .
- Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P , alors il existe un unique \mathbb{K} -isomorphisme $\varphi : \mathbb{L} \rightarrow \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.

Application 30. $X^2 + 1$ est un polynôme irréductible sur \mathbb{R} dont $\mathbb{R}[X]/(X^2 + 1)$ est un corps de rupture. On pose alors $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$, le corps des nombres complexes, et on note i la classe de X dans l'anneau quotient.

Remarque 31. Si \mathbb{L} est un corps de rupture d'un polynôme $P \in \mathbb{K}[X]$, on a $[\mathbb{L} : \mathbb{K}] = \deg(P)$. Plus précisément, une base de \mathbb{L} en tant que \mathbb{K} -espace vectoriel est $(1, \alpha, \dots, \alpha^{\deg(P)-1})$.

2. Corps de décomposition

Définition 32. Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$. On dit que \mathbb{L} est un **corps de décomposition** de P si :

- Il existe $a \in \mathbb{L}$ et $\alpha_1, \dots, \alpha_n \in \mathbb{L}$ tels que $P = a(X - \alpha_1) \dots (X - \alpha_n)$.
- $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$.

Exemple 33. — \mathbb{K} est un corps de décomposition de tout polynôme de degré 1 sur \mathbb{K} .

- \mathbb{C} est un corps de décomposition de $X^2 + 1$ sur \mathbb{R} .

Théorème 34. Soit $P \in \mathbb{K}[X]$ un polynôme de degré supérieur ou égal à 1.

- Il existe un corps de décomposition de P .
- Deux corps de décomposition de P sont \mathbb{K} -isomorphes.

[DEV]

Application 35. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On note $\mathcal{C}(A)$ le commutant de A . Alors,

$$\mathbb{K}[A] = \mathcal{C}(A) \iff \pi_A = \chi_A = \det(XI_n - A)$$

[FGN2]
p. 160

3. Clôture algébrique

Proposition 36. Les assertions suivantes sont équivalentes :

- (i) Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 est scindé sur \mathbb{K} .
- (ii) Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1 admet au moins une racine dans \mathbb{K} .
- (iii) Les seuls polynômes irréductibles de $\mathbb{K}[X]$ sont ceux de degré 1.
- (iv) Toute extension algébrique de \mathbb{K} est égale à \mathbb{K} .

[GOZ]
p. 62

Définition 37. Si \mathbb{K} vérifie un des points de la Proposition 36, \mathbb{K} est dit **algébriquement clos**.

Proposition 38. Tout corps algébriquement clos est infini.

Contre-exemple 39. \mathbb{Q} et même \mathbb{R} ne sont pas algébriquement clos.

Théorème 40 (D'Alembert-Gauss). \mathbb{C} est algébriquement clos.

Définition 41. On dit que \mathbb{L} est une **clôture algébrique** de \mathbb{K} si \mathbb{L} est une extension de \mathbb{K} algébriquement close et si

$$\forall x \in \mathbb{L}, \exists P \in \mathbb{K}[X] \text{ tel que } P(x) = 0$$

Exemple 42. — \mathbb{C} est une clôture algébrique de \mathbb{R} .

- $\overline{\mathbb{Q}}$ du Contre-exemple 23 est une clôture algébrique de \mathbb{Q} .

Théorème 43 (Steinitz). (i) Il existe une clôture algébrique de \mathbb{K} .
(ii) Deux clôtures algébriques de \mathbb{K} sont \mathbb{K} -isomorphes.

III - Corps particuliers

1. Corps finis

Soit $q = p^n$ où p est un nombre et n un entier supérieur ou égal à 1.

Proposition 44. Les conditions suivantes sont équivalentes :

- (i) n est un nombre premier.
- (ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
- (iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

p. 3

Notation 45. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Théorème 46. (i) Il existe un corps fini à q éléments : c'est le corps de décomposition de $X^q - X$ sur \mathbb{F}_p .
(ii) Si F et F' sont deux corps finis à q éléments, ils sont \mathbb{F}_p -isomorphes.
On peut donc noter \mathbb{F}_q l'unique (à isomorphisme près) corps fini à q éléments.

p. 85

Théorème 47. Soit F un corps fini. Alors :

- (i) Sa caractéristique est un nombre premier p .
 - (ii) Il existe $n \geq 1$ tel que $|F| = p^n$.
- On a donc $F = \mathbb{F}_{p^n}$.

p. 81

Exemple 48. Il n'existe pas de corps fini à 6 éléments.

Théorème 49. Tout sous-groupe du groupe multiplicatif d'un corps fini est cyclique.

Corollaire 50.

$$\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$$

Proposition 51. Soit F un corps fini de caractéristique p et soit ξ un générateur de F^* . Alors,

en posant $n = [F : \mathbb{F}_p]$, on a

$$F = \bigoplus_{i=0}^n \mathbb{F}_p \xi^i$$

Théorème 52 (Élément primitif pour les corps finis). Soit \mathbb{L} une extension de degré fini de \mathbb{K} . Si \mathbb{K} est un corps fini, alors \mathbb{L} est monogène.

Théorème 53. (i) Si \mathbb{K} est un sous-corps de \mathbb{F}_q , alors il existe $d \mid n$ tel que $|\mathbb{K}| = p^d$.
(ii) Pour chaque diviseur d de n , \mathbb{F}_q a un et un seul sous-corps de cardinal p^d . Il est isomorphe à \mathbb{F}_{p^d} .

p. 91

2. Corps cyclotomiques

Soit m un entier supérieur ou égal à 1.

Définition 54. On définit

$$\mu_m = \{z \in \mathbb{C}^* \mid z^m = 1\}$$

l'ensemble des **racines m -ièmes de l'unité**. C'est un groupe (cyclique) pour la multiplication dont l'ensemble des générateurs, noté μ_m^* , est formé des **racines primitives m -ièmes de l'unité**.

p. 67

Proposition 55. (i) $\mu_m^* = \{e^{\frac{2ik\pi}{m}} \mid k \in \llbracket 0, m-1 \rrbracket, \text{pgcd}(k, m) = 1\}$.
(ii) $|\mu_m^*| = \varphi(m)$, où φ désigne l'indicatrice d'Euler.

Proposition 56. Le sous-corps $\mathbb{Q}(\xi)$ de \mathbb{C} ne dépend pas de la racine m -ième primitive ξ de l'unité considérée.

Définition 57. On appelle **corps cyclotomique**, un corps de la forme de la Proposition 56 (ie. engendré par une racine primitive de l'unité).

Définition 58. On appelle **m -ième polynôme cyclotomique** le polynôme

$$\Phi_m = \prod_{\xi \in \mu_m^*} (X - \xi)$$

Théorème 59. (i) $X^m - 1 = \prod_{d \mid m} \Phi_d$.
(ii) $\Phi_m \in \mathbb{Z}[X]$.

(iii) Φ_m est irréductible sur \mathbb{Q} .

Corollaire 60. Le polynôme minimal sur \mathbb{Q} de tout élément ξ de μ_m^* est Φ_m . En particulier,

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m)$$

Application 61 (Théorème de Wedderburn). Tout corps fini est commutatif.

Application 62 (Dirichlet faible). Pour tout entier n , il existe une infinité de nombres premiers congrus à 1 modulo n .

[GOU21]
p. 99

Bibliographie

Oraux X-ENS Mathématiques

[FGN2]

Serge FRANCINO, Hervé GIANELLA et Serge NICOLAS. *Oraux X-ENS Mathématiques. Volume 2*. 2^e éd. Cassini, 16 mars 2021.

<https://store.cassini.fr/fr/enseignement-des-mathematiques/111-oraux-x-ens-mathematiques-nouvelle-serie-vol-2.html>.

Les maths en tête

[GOU21]

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3^e éd. Ellipses, 13 juill. 2021.

<https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html>.

Théorie de Galois

[GOZ]

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2^e éd. Ellipses, 1^{er} avr. 2009.

<https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html>.

Cours d'algèbre

[PER]

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.

<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.