

Leçon 125 : Extensions de corps. Exemples et applications.

Félix NI

2025-2026

Table des matières

1 Généralités	1
1.1 Extension de corps	1
1.2 Eléments algébriques et transcendants	2
1.3 Morphismes de corps	2
2 Extensions particulières	3
2.1 Corps de rupture et de décomposition	3
2.2 Corps finis	3
2.3 Extension cyclotomique	4
3 Nombres constructibles à la règle et au compas	5
4 Développements	5
K, L, M désignent des corps (commutatifs).	

1 Généralités

1.1 Extension de corps

[1] : Gozard

Définition 1. L est appelée extension de K s'il existe un morphisme de corps $i : K \rightarrow L$. On note alors L/K .

Remarque 2. Si $i : K \rightarrow L$ réalise l'extension L/K , alors i est injectif et $i(K)$ est un sous-corps de L . On identifiera K et $i(K)$. On pourra noter $K \subset L$ plutôt que L/K .

Exemple 3. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ et $K \subset K(X)$.

Proposition 4. Si $K \subset L$, alors, $(\lambda, x) \in K \times L \mapsto i(\lambda)x \in L$ induit une structure de K -algèbre sur L .

Définition 5. On appelle degré de L/K le nombre $[L : K] := \dim_K(L) \in \mathbb{N} \cup \{+\infty\}$. S'il est fini, on dit que L/K est une extension finie.

Exemple 6. - Si $K \subset L$, alors $[L : K] = 1$ ssi $L = K$.

- $[\mathbb{R} : \mathbb{Q}] = +\infty$, $[\mathbb{C} : \mathbb{R}] = 2$, $[K(X) : K] = +\infty$.

Théorème 7 (Base télescopique). Supposons que $K \subset L \subset M$. Soit $(e_i)_{i \in I}$ une K -base de L et $(\alpha_j)_{j \in J}$ une L -base de M . Alors $(\alpha_j e_i)_{(i,j) \in I \times J}$ est une K -base de M .

En particulier, M/K est finie ssi M/L et L/K le sont, et dans ce cas $[M : K] = [M : L][L : K]$.

Définition 8. Si $K \subset L$, et P est une partie de L , on note $K(P)$ le plus petit sous-corps de L qui contient K et P . On a alors $K \subset K(P) \subset L$.

Si $P = \{a_1, \dots, a_n\}$, on note plus simplement $K(a_1, \dots, a_n)$.

Proposition 9. Si K, L, P sont comme précédemment, on note $K[P]$ la sous- K -algèbre de L engendrée par P . Alors $K(P)$ est le corps des fractions de $K[P]$.

Proposition 10. Si L/K est finie, alors il existe $a_1, \dots, a_n \in L$ tels que $L = K[a_1, \dots, a_n]$.

1.2 Eléments algébriques et transcendants

[4] : Perrin

Définition 11. Supposons que $K \subset L$ et soit $\alpha \in L$, on note $\text{ev}_\alpha : K[X] \longrightarrow L, P \mapsto P(\alpha)$.

- Si ev_α est injectif, on dit que α est transcendant sur K
- Sinon, on dit que α est algébrique sur K . Alors $\ker(\text{ev}_\alpha)$ est un idéal principal, engendré par un unique polynôme de $K[X]$ irréductible unitaire. Il est noté $\mu_{\alpha,K}$ et est appelé polynôme minimal de α sur K .

Exemple 12. Dans $K(X)$, X est transcendant sur K . Les nombres $\sqrt{2}$ et i sont algébriques sur $\mathbb{Q}$, de polynômes minimaux respectifs $X^2 - 2$ et $X^2 + 1$.

Théorème 13. Supposons que $K \subset L$ et soit $\alpha \in L$. Les ASSE

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

Lorsque c'est le cas, on a $K(\alpha) \simeq K[X]/(\mu_{\alpha,K})$, $[K(\alpha) : K] = \deg(\mu_{\alpha,K})$, et $(1, \alpha, \alpha^2, \dots, \alpha^{[K(\alpha):K]-1})$ est une K -base de $K(\alpha)$.

Définition 14. On dit que l'extension L/K est algébrique si pour tout $\alpha \in L$, α est algébrique sur K .

Proposition 15. Si L/K est finie, alors elle est algébrique.

Théorème 16. Supposons que $K \subset L$ et posons $L' = \{x \in L \mid x \text{ est algébrique sur } K\}$. Alors L' est un sous-corps de L .

Exemple 17. $\overline{\mathbb{Q}} := \{x \in \mathbb{C} \mid x \text{ est algébrique sur } \mathbb{Q}\}$ est une extension algébrique de $\mathbb{Q}$ mais non finie. De plus, $\overline{\mathbb{Q}}$ est dénombrable, donc il existe des nombres complexes transcendants sur $\mathbb{Q}$.

Définition 18. Les ASSE :

- (i) Tout polynôme $P \in K[X]$ de degré ≥ 1 admet une racine dans K .
- (ii) Tout polynôme $P \in K[X]$ est produit de polynômes de degré 1.
- (iii) Les éléments irréductibles de $K[X]$ sont les $X - a$, $a \in K$.
- (iv) Si une extension $K \subset L$ est algébrique, alors $L = K$.

Dans ce cas, on dit que K est algébriquement clos.

Théorème 19 (D'Alembert-Gauss). $\mathbb{C}$ est algébriquement clos.

1.3 Morphismes de corps

[1] : Gozard

Définition 20. On appelle automorphisme de K tout morphisme de corps bijectif $K \longrightarrow K$. Leur ensemble est noté $\text{Aut}(K)$.

Supposons que $K \subset L$ et $K \subset M$. On appelle K -morphisme (de corps) de L sur M tout morphisme $\sigma : L \longrightarrow M$ de K -algèbre. Si σ est bijective, on dit que c'est un K -isomorphisme. Si de plus, $L = M$, on dit que c'est un K -automorphisme de L , dont l'ensemble est noté $\text{Aut}(L/K)$ ou $\text{Aut}_K(L)$.

Proposition 21. $(\text{Aut}(L), \circ)$ est un groupe. $\text{Aut}(L/K)$ en est un sous-groupe.

Exemple 22. $\text{Aut}(\mathbb{R}) = \{\text{id}_{\mathbb{R}}\}$ et $\text{Aut}(\mathbb{C}/\mathbb{R}) = \{\text{id}_{\mathbb{C}}, (z \mapsto \bar{z})\}$.

Proposition 23. Supposons que $K \subset L$ et $K \subset M$. Soit $\alpha \in L$, $\sigma : L \longrightarrow M$ un K -morphisme, et $P \in K[X]$. Alors $\sigma(P(\alpha)) = P(\sigma(\alpha))$. En particulier, α est une racine de P ssi $\sigma(\alpha)$ est une racine de P .

Proposition 24. Soit K' un corps, on suppose que $\exists i : K \longrightarrow K'$ un isomorphisme (de corps). i induit un isomorphisme d'anneaux $i : K[X] \longrightarrow K'[X], \sum \lambda_k X^k \mapsto \sum i(\lambda_k) X^k$.

- 1) Soit $P \in K[X]$ irréductible. Alors $i(P)$ est irréductible dans $K'[X]$.

2) Supposons qu'on ait $K \subset L$ et $K' \subset L'$, $\alpha \in L, \alpha' \in L'$ des racines respectives de P et $i(P)$. Alors $\exists ! j : K(\alpha) \longrightarrow K'(\alpha')$ isomorphisme prolongeant i et tel que $j(\alpha) = \alpha'$.

Lemme 25. Supposons que $K \subset L$ et soit H une partie de $\text{Aut}(L/K)$. Alors $L^H := \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\}$ est un sous-corps de L et est appelé corps fixe de H . On a alors $K \subset L^H \subset L$.

Proposition 26 (DEV1). Supposons que $K \subset L$ et $K \subset M$ avec L/K finie. Alors il y a au plus $[L : K]$ K -morphisms de L sur M .

Théorème 27 (Artin). [DEV1, [1] ou [3]] Soit H un sous-groupe fini de $\text{Aut}(L)$. Alors L/L^H est finie, $|H| = [L : L^H]$, et $H = \text{Aut}(L/L^H)$.

2 Extensions particulières

2.1 Corps de rupture et de décomposition

[1] : Gozard

Définition 28. Soit $P \in K[X]$ irréductible dans $K[X]$. On dit que L est un corps de rupture de P sur K si $\exists \alpha \in L$ racine de P telle que $L = K(\alpha)$.

Exemple 29. - $\mathbb{C} = \mathbb{R}(i)$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.

- $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(j\sqrt[3]{2})$ sont des corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

Théorème 30. Soit $P \in K[X]$ irréductible sur $K[X]$. Alors :

(i) Il existe un corps de rupture de P sur K

(ii) Si $L = K(\alpha)$ et $L' = K(\beta)$ sont deux corps de rupture de P , alors $\exists ! t : L \longrightarrow L'$ K -isomorphisme tel que $t(\alpha) = \beta$.

Corollaire 31 (Critères d'irréductibilité). Soit $P \in K[X]$ de degré n . Alors :

- P est irréductible dans $K[X]$ ssi P n'a pas de racine dans les extensions L de K telles que $[L : K] \leq n/2$.

- Si P est irréductible dans $K[X]$, et L/K est de degré m avec $m \wedge n = 1$, alors P est irréductible dans $L[X]$.

Exemple 32 ([4]). $X^3 + X + 1$ est irréductible sur $\mathbb{Q}$ donc sur $\mathbb{Q}(i)$. Cependant, $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Q}(i)$.

Définition 33. Soit $P \in K[X]$ de degré n . On dit que L est un corps de décomposition de P sur K si $\exists \alpha_1, \dots, \alpha_n \in L$ tels que $P = a(X - \alpha_1) \dots (X - \alpha_n)$ et $L = K(\alpha_1, \dots, \alpha_n)$.

Exemple 34. - $\mathbb{C} = \mathbb{R}(i)$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$, et $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$.

- $\mathbb{Q}(\sqrt[3]{2})$ n'est pas un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$, mais $\mathbb{Q}(\sqrt[3]{2}, j)$ en est un.

Théorème 35. Soit $P \in K[X]$ de degré n . Alors :

- Il existe un corps de décomposition L de P sur K , et on a $[L : K] \leq n!$.

- Si L et L' sont deux corps de décomposition de P sur K , alors il existe un K -isomorphisme de L sur L' .

On peut donc noter $D_K(P)$ "le" corps de décomposition de P sur K .

2.2 Corps finis

[4] : Perrin

Définition 36. Le sous-corps premier de K , noté K_0 , est l'intersection de tous les sous-corps de K . C'est aussi le sous-corps de K engendré par 1_K . On a bien sûr $K_0 \subset K$.

Proposition 37. K et K_0 ont même caractéristique c , et :

- soit $c = 0$, alors $K_0 \simeq \mathbb{Q}$

- soit c est un nombre premier, et $K_0 \simeq \mathbb{Z}/p\mathbb{Z}$

Ainsi, si K est fini, alors c est un nombre premier, et il existe $n \in \mathbb{N}^*$ tel que $|K| = p^n$ (c'est $n = [K : \mathbb{Z}/p\mathbb{Z}]$).

Proposition 38. Supposons que K soit de caractéristique $p > 0$. Alors $F : K \longrightarrow K, x \mapsto x^p$ est un morphisme (de corps), appelé morphisme de Frobenius. Si K est fini, $F \in \text{Aut}(K)$, et si $K = \mathbb{Z}/p\mathbb{Z}$, alors $F = \text{id}_{\mathbb{Z}/p\mathbb{Z}}$.

Théorème 39 ([1]). Soit p un nombre premier, $n \in \mathbb{N}^*$ et $q = p^n$. Alors :

- $D_{\mathbb{Z}/p\mathbb{Z}}(X^q - X)$ est un corps à q éléments
- Si L et L' sont deux corps à q éléments, alors ils sont $\mathbb{Z}/p\mathbb{Z}$ -isomorphes.

On note $\mathbb{F}_q$ "le" corps à q éléments.

Théorème 40. Soit $q = p^n$ avec p premier et $n \in \mathbb{N}^*$. Le groupe $(\mathbb{F}_q^*, \times)$ est cyclique (donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$).

Plus généralement, tout sous-groupe fini de L^* (avec L corps quelconque) est cyclique.

Corollaire 41 (Théorème de l'élément primitif pour les corps finis). *[[1]]* Soit K un corps fini et L/K une extension finie. Alors il existe $\xi \in L$ tel que $L = K(\xi)$.

2.3 Extension cyclotomique

[4] : Perrin

Soit $n \in \mathbb{N}^*$ et $P_n = X^n - 1 \in K[X]$.

Définition 42. L'ensemble $\mu_n(K) := \{\zeta \in K \mid \zeta^n = 1\}$ est appelé ensemble des racines n -èmes de l'unité dans K . C'est un sous-groupe fini de K^* , donc cyclique.

Proposition 43. Notons $K_n = D_K(P_n)$ et supposons que la caractéristique p de K ne divise pas n . Alors P_n est SARS sur K_n , donc $|\mu_n(K_n)| = n$ et $\mu_n(K_n) \simeq \mathbb{Z}/n\mathbb{Z}$. De plus, il existe d diviseur de n tel que $\mu_n(K) \simeq \mathbb{Z}/d\mathbb{Z}$.

Remarque 44. Si $p \mid n$, alors $X^n - 1 = (X^{n/p} - 1)^p$, donc P_n a des racines multiples dans toute extension de K . On supposera que $p \nmid n$ dans la suite.

Définition 45. Une racine n -ème primitive de l'unité est un élément $\zeta \in K_n$ tel que $\zeta^n = 1$ et $\forall d < n, \zeta^d \neq 1$, i.e. un générateur du groupe $\mu_n(K_n)$. Leur ensemble est noté $\mu_n^*(K_n)$. On a donc $\forall \zeta \in \mu_n^*(K_n), K(\zeta) = K_n$ ("extension cyclotomique").

Le n -ème polynôme cyclotomique est $\Phi_{n,K} := \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta) \in K_n[X]$.

Proposition 46. - $|\mu_n^*(K_n)| = \varphi(n)$ (indicatrice d'Euler). $\Phi_{n,K}$ est donc unitaire de degré $\varphi(n)$.

- Si $\zeta \in \mu_n^*(K_n)$, alors $\mu_n^*(K_n) = \{\zeta^m \mid m \wedge n = 1\}$.

- $X^n - 1 = \prod_{d \mid n} \Phi_{d,K}$

Exemple 47. On a $\Phi_{1,K} = X - 1$, $\Phi_{2,K} = X + 1$, $\Phi_{3,K} = X^2 + X + 1$, $\Phi_{4,K} = X^2 + 1, \dots$ Si n est premier, alors $\Phi_{n,K} = \sum_{k=0}^{n-1} X^k$.

Proposition 48. On a $\Phi_{n,K} \in \mathbb{Z}[X]$, et en notant $\sigma : \mathbb{Z} \longrightarrow K$ le morphisme d'anneau canonique, on a $\Phi_{n,K} = \sigma(\Phi_{n,\mathbb{Q}})$.

En particulier, si K_0 est le sous-corps premier de K , alors $\Phi_{n,K} = \Phi_{n,K_0} \in K_0[X]$ et on peut omettre l'indice K .

Théorème 49. $\Phi_n \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$. Si $\zeta \in \mathbb{C}$ est une racine n -ème de l'unité, on a donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Exemple 50. $\Phi_8 = X^4 + 1$ est réductible sur tous les corps $\mathbb{F}_p$.

3 Nombres constructibles à la règle et au compas

[1] : Gozard

On identifie le plan $\mathbb{R}^2$ avec $\mathbb{C}$. Si $r > 0$ et $A \neq B \in \mathbb{R}^2$, on note (AB) la droite passant par A et B , $\|AB\|$ la longueur du segment $[AB]$, et $C(A, r)$ le cercle de centre A et de rayon r .

Définition 51. Soit $X \subset \mathbb{R}^2$. On dit qu'un point $M \in \mathbb{R}^2$ est constructible en un pas à partir de X si $\exists A, B, A', B' \in X$ tq

- ou bien $M \in (AB) \cap (A'B')$
- ou bien $M \in C(A, \|AB\|) \cap C(A', \|A'B'\|)$
- ou bien $M \in C(A, \|AB\|) \cap (A'B')$

Définition 52. Soit $\mathcal{B}_0 \subset \mathbb{R}^2$, et $\forall i \in \mathbb{N}, \mathcal{B}_{i+1}$ est défini comme l'ensemble des points constructibles en un pas à partir de $\mathcal{B}_i$.

Si $M \in \mathbb{R}^2$, alors $M \in \bigcup_{n \in \mathbb{N}} \mathcal{B}_n$ ssi il existe $M_1, \dots, M_n \in \mathbb{R}^2$ tels que $M_n = M$ et $\forall i \in \llbracket 1, n-1 \rrbracket, M_{i+1}$ est constructible en un pas à partir de $\mathcal{B}_0 \cup \{M_1, \dots, M_i\}$. Dans ce cas, on dit que M est constructible à partir de $\mathcal{B}_0$.

On prend $\mathcal{B}_0 = \{0, 1\} \subset \mathbb{C}$ dans la suite.

Proposition 53 (Utiliser l'annexe). Soit $A \neq B$ et C trois points constructibles

- 1) La symétrique de C par rapport à l'origine est constructible.
- 2) Le milieu et la médiatrice de $[AB]$ sont constructibles.
- 3) La perpendiculaire à (AB) passant par C est constructible.
- 4) La parallèle à (AB) passant par C est constructible.

Proposition 54. Soit $x, y \in \mathbb{R}$, alors $(x, 0)$ est constructible ssi $(0, x)$ est constructible. On dit alors que x est constructible.

De plus, (x, y) est constructible ssi x et y sont constructibles.

Théorème 55. L'ensemble $\mathbb{E}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée. En particulier, $\mathbb{Q} \subset \mathbb{E}$

Théorème 56 (Wantzel). Soit $x \in \mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Alors x est constructible ssi il existe $L_0 \subset \dots \subset L_p$ des sous-corps de $\mathbb{K}$ vérifiant $L_0 = \mathbb{Q}$, $x \in L_p$ et $\forall i \in \llbracket 0, p-1 \rrbracket, [L_{i+1} : L_i] = 2$.

Corollaire 57. Si $x \in \mathbb{R}$ est constructible, alors il existe $p \in \mathbb{N}$ tel que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^p$. En particulier, x est algébrique sur $\mathbb{Q}$.

Exemple 58. - (Quadrature du cercle) π est transcendant sur $\mathbb{Q}$ (théorème de Lindemann) donc non constructible. On ne peut donc pas construire un carré de même aire qu'un disque constructible.

- (Duplication du cube) $\sqrt[3]{2}$ n'est pas constructible. On ne peut donc pas construire (l'arête d')un cube de volume double d'un cube constructible.

Définition 59. Soit p premier impair. S'il existe $n \in \mathbb{N}$ tel que $p = 2^n + 1$, alors n est une puissance de 2. On définit donc $F_k := 2^{2^k} + 1$ le k -ème nombre de Fermat.

Théorème 60 (Polygones réguliers constructibles, Gauss-Wantzel). [DEV2, [2] ou [1]] Un polygone régulier à n côtés est constructible ssi n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts.

4 Développements

- Théorème d'Artin, [1] ou [3]
- Polygones réguliers constructibles, [2] ou [1]

Références

- [1] Ivan Gozard. *Théorie de Galois, 2e édition*. ellipses, 2009.
- [2] Lucas Isenmann and Timothée Pecatte. *L'oral à l'agreg de maths, 2e édition*. ellipses, 2024.
- [3] Didier Lesesvre, Pierre Montagnon, Pierre Le Barbenchon, and Théo Pierron. *Je prépare 131 développements pour l'oral*. Dunod, 2020.
- [4] Daniel Perrin. *Cours d'algèbre*. ellipses, 1996.