P. Maurer
ENS Rennes

# Leçon 125. Extensions de corps. Exemples et applications.

**Devs :**

- Théorème de Gauss-Wantzel
- Etude des polynômes cyclotomiques

**Références :**

1. Gozard, Théorie de Galois
2. Carrrega, Théorie des corps
3. Cours d'algèbre, Perrin

## 1 Corps, Extensions de corps

### 1.1 Corps, morphismes de corps et corps premiers

**Proposition 1.** *Soit $K$ un anneau non restreint à $\{0\}$. Les conditions suivantes sont équivalentes :*

- *Tout élément non nul de $K$ est inversible.*
- *L'ensemble $K^* = K \setminus \{0\}$ forme un groupe multiplicatif.*

*Si elles sont vérifiées, on dit que $K$ est un corps.*

**Proposition 2.** *Un corps est un anneau intègre.*

**Exemple 3.** $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. $\mathbb{Z}$ n'en est pas un.

**Exemple 4.** Pour $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre si et seulement si c'est un corps, si et seulement si $p$ est premier. Pour $p$ premier, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, c'est un corps à $p$ élément.

Cependant, il existe des anneaux intègres qui ne sont pas des corps (par exemple $\mathbb{R}[X]$).

**Proposition 5.** *Soit $K$ un corps. Tout homomorphisme d'anneau de $K$ dans un anneau $A$ est injectif.*

**Définition 6.** *Soit $A$ un anneau intègre. On définit son corps de fractions* $\mathrm{Frac}(A)$ *comme le plus petit corps contenant $A$ (à isomorphisme près).*

**Proposition 7.** *Soit $A$ un anneau intègre, et $K$ un corps. Soit $u$ un morphisme d'anneau injectif de $A$ vers $K$. Alors on peut prolonger $u$ en un morphisme de corps injectif de* $\mathrm{Frac}(A)$ *vers $K$.*

**Définition 8.** *On dit qu'un corps $K$ est premier si son seul sous-corps est lui-même. On appelle sous-corps premier de $K$ le sous corps engendré par $1_K$, l'intersection de tous les sous-corps de $K$.*

**Exemple 9.** $\mathbb{Q}$ et $\mathbb{F}_p$ sont des corps premier, pour $p$ premier. $\mathbb{Q}$ est le sous-corps premier de $\mathbb{C}$.

**Proposition 10.** *Soit $K$ un corps, et $\varphi: \mathbb{Z} \to K$ l'homomorphisme d'anneau défini par $\varphi(n) = n \cdot 1 = 1 + \cdots + 1$. L'ensemble $\operatorname{Ker} \varphi$ est un idéal de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ et comme $\mathbb{Z}/p\mathbb{Z} \simeq \operatorname{Im}(\varphi) \subset K$ est intègre, $p\mathbb{Z}$ est un idéal premier. Il y a donc deux cas : $p$ est nul ou $p$ est premier.*

**Définition 11.** *On appelle caractéristique de $K$ l'entier $p$ tel que $\operatorname{Ker} \varphi = p\mathbb{Z}$, et on le note $\mathrm{car}(K)$. On a donc $\mathrm{car}(K) = 0$ ou $\mathrm{car}(K) \in \mathbb{P}$.*

**Proposition 12.** *Si $\mathrm{car}(K) = p > 0$, alors pour tout $x \in K$, on a $px = 0$.*

**Exemple 13.** Les corps de caractéristique nulle sont infinis.

### 1.2 Extensions de corps

**Définition 14.** *Soit $K$ un corps. On appelle extension de $K$ tout corps $L$ tel qu'il existe un morphisme de corps $j$ de $K$ dans $L$. On note $L/K$ pour dire que $L$ est une extension de $K$.*

**Remarque 15.** $L$ est une extension de $K$ ssi $K$ peut être vu (à isomorphisme près) comme un sous-corps de $L$.

**Exemple 16.** $\mathbb{C}$ est une extension de $\mathbb{R}$ lui même extension de $\mathbb{Q}$.

**Exemple 17.** Tout corps $K$ est une extension de son sous-corps premier $P$.

**Définition 18.** *Soit $K$ un corps et $L/K$ une extension. On appelle degré de $L/K$ et on note $[L:K]$ la dimension de $L$ vu comme $K$-espace vectoriel : $[L:K] := \dim_K(L)$.*

**Théorème 19.** *(Base télescopique)*

*Soit $K \subset L \subset M$ des corps, $(e_i)_{i \in I}$ une base de $L$ sur $K$, $(f_j)_{j \in J}$ une base de $M$ sur $L$. Alors $(e_i f_j)_{i \in I, j \in J}$ est une base de $M$ sur $K$. En particulier, $[M:K] = [M:L][L:K]$.*

### 1.3 Extensions algébriques

**Définition 20.** *Soit $L/K$ une extension, et $A \subset L$. On dit que $A$ engendre $L$, et on écrit $L = K(A)$ si $L$ est le plus petit sous-corps de $L$ contenant $A$ et $K$. Si $A$ est fini et $A = \{\alpha_1, \ldots, \alpha_n\}$, on note $L = K(\alpha_1, \ldots, \alpha_n)$.*

**Définition 21.** *Soit $K$ un corps et $L$ une extension de $K$. Soit $\varphi: K[T] \to L$ l'homomorphisme défini par $\varphi_{|K} = \mathrm{id}_K$ et $\varphi(T) = \alpha$.*

*Si $\varphi$ est injectif, on dit que $\alpha$ est transcendant sur $K$. Sinon, on dit que $\alpha$ est algébrique sur $K$, et l'idéal $I = \mathrm{Ker}\,\varphi$ étant principal, on a $I = (P)$ avec $P$ irréductible (que l'on peut supposer unitaire). Le polynôme $P$ est, par définition, le polynôme minimal de $\alpha$ sur $K$, et on le note $\mu_\alpha$.*

**Exemple 22.** $\sqrt{2}$ et $i$ sont algébriques sur $\mathbb{Q}$, mais pas $\pi$ ni $e$.

**Remarque 23.** Le polynôme minimal d'un élément $\alpha$ algébrique sur $K$ est l'unique polynôme unitaire irréductible de $K[X]$ qui annule $\alpha$.

**Exemple 24.** $X^2 + 1$ est le polynôme minimal de $i$ sur $\mathbb{Q}$. $X - i$ est le polynôme minimal de $i$ sur $\mathbb{C}$.

**Théorème 25.** *Soit $K \subset L$ une extension et $\alpha \in L$. Les propriétés suivantes sont équivalentes :*

- *$\alpha$ est algébrique sur $K$*
- *On a $K[\alpha] = K(\alpha)$*
- *On a $\dim_K K[\alpha] < \infty$*

*Dans ce cas, on a $\deg(\mu_\alpha) = [K(\alpha): K]$.*

**Définition 26.** *Une extension $L/K$ est dite finie si on a $[L: K] < \infty$. Elle est dite algébrique si tous les éléments de $L$ sont algébriques sur $K$.*

**Remarque 27.** Une extension finie est toujours algébrique, mais la réciproque est fausse, par exemple $\mathbb{Q}\left[\left\{2^{\frac{1}{n}},\ n \in \mathbb{N}^*\right\}\right]$ est algébrique et infinie.

**Théorème 28.** *Soit $L/K$ une extension. Alors $M := \{x \in L :\ x \text{ est algébrique sur } K\}$ est un sous-corps de $L$.*

# 2 Recherche de racine et extensions

## 2.1 Corps de rupture

**Définition 29.** *Soit $P \in K[X]$ un polynôme irréductible dans $K[X]$. On dit que $L$ est un corps de rupture de $P$ si et seulement si $L$ est une extension monogène de $K$ engendrée par $K$ et une racine, notée $\alpha$, de $P$.*

**Remarque 30.** $L$ est alors une extension de $K$ de degré $\deg(P)$.

**Exemple 31.** Si $\deg(P) = 1$, $K$ est un corps de rupture de $P$.

**Théorème 32.** *Soit $P \in K[X]$ irréductible.*

1. *Il existe un corps de rupture de $P$.*
2. *Si $L = K(\alpha)$ et $L' = K(\beta)$ sont deux corps de rupture de $P$, alors $L$ et $L'$ sont $K$-isomorphes : il existe un unique $K$-isomorphisme $t: L \to L'$ tel que $t(\alpha) = \beta$.*

**Exemple 33.** $\mathbb{C}$ s'obtient comme corps de rupture de $X^2 + 1 \in \mathbb{R}[X]$.

**Exemple 34.** Le corps de rupture de $X^2 + X + 1 \in \mathbb{F}_2[X]$ donne un corps à 4 éléments.

**Corollaire 35.** *Si $P \in K[X]$ est de degré plus grand que 1, il existe une extension $L$ de $K$ dans laquelle $P$ possède au moins une racine, et cette extension est finie.*

**Proposition 36.** *Soit $P \in K[X]$ de degré $n$. $P$ est irréductible sur $K$ si et seulement si $P$ n'a pas de racine dans les extensions de $K$ de degré $\leq \frac{n}{2}$.*

**Remarque 37.** On retrouve l'irréductibilité des polynômes de degré 2 et 3.

**Théorème 38.** *Soit $P \in K[X]$ un polynôme irréductible de degré $n$, et $L$ une extension de degré $m$ avec $n \wedge m = 1$. Alors $P$ est encore irréductible sur $L$.*

## 2.2 Corps de décomposition

**Définition 39.** *Soit $L$ une extension de $K$. Soit $P \in K[X]$, avec $\deg(P) = n \in \mathbb{N}^*$. On dit que $L$ est un corps de décomposition de $P$ sur $K$ si $P$ s'écrit $P(X) = a\,(X - \alpha_1) \cdots (X - \alpha_n)$ avec $a, \alpha_1, \ldots, \alpha_n \in L$ et si $L = K(\alpha_1, \ldots, \alpha_n)$.*

**Remarque 40.** Dans ce cas, $L$ est une extension finie de $K$.

**Exemple 41.** $K$ est un corps de décomposition de tout polynôme de degré 1.

**Exemple 42.** $\mathbb{C} = \mathbb{R}(i)$ 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 $\mathbb{Q}$.

$\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $\sqrt[3]{2}$ sur $\mathbb{Q}$ mais pas un corps de décomposition.

**Théorème 43.** *Soit $P \in K[X]$ de degré $n \geq 1$.*

1. *Il existe un corps de décomposition $L$ de $P$ sur $K$, avec $[L: K] \leq n!$*
2. *Si $L$ et $L'$ sont deux corps de décomposition de $P$ sur $K$, alors il existe un $K$-isomorphisme de $L$ dans $L'$.*

**Théorème 44.** *(Théorème de l'élément primitif)*

*Sur un corps de caractéristique nulle, toute extension finie est monogène.*

### 2.3 Clotûre algébrique

**Définition 45.** *Les conditions suivantes sont équivalentes :*

1. *Tout polynôme de degré $\geq 1$ de $K[X]$ est scindé sur $K$*
2. *Tout polynôme de degré $\geq 1$ de $K[X]$ admet au moins une racine sur $K$*
3. *Les seuls polynômes irréductibles de $K[X]$ sont de degré 1*
4. *Toute extension algébrique de $K$ est identique à $K$ lui-même.*

*On dit que $K$ est algébriquement clos.*

**Exemple 46.** $\mathbb{Q}$ n'est pas algébriquement clos, car $X^2-2$ et $X^3-2$ n'ont pas de racines dans $\mathbb{Q}$.
$\mathbb{R}$ n'est pas algébriquement clos, car $X^2+1$ et $X^2+X+1$ n'ont pas de racine dans $\mathbb{R}$.

**Proposition 47.** *Tout corps algébriquement clos est infini.*

**Théorème 48.** *(D'Alembert-Gauss)*
*$\mathbb{C}$ est algébriquement clos.*

**Définition 49.** *Soit $K$ un corps, $L$ une extension de $K$. On dit que $L$ est une clotûre algébrique de $K$ si $L$ est algébrique sur $K$ et si $L$ est algébriquement clos.*

**Exemple 50.** $\mathbb{C}$ est une clotûre algébrique de $\mathbb{R}$.

**Théorème 51.** *Si $K$ est un corps, alors $\overline{K} = \{\alpha \in K : \alpha$ algébrique sur $K\}$ est une clôture algébrique de $K$.*

**Exemple 52.** $\overline{\mathbb{Q}}$ est une clotûre algébrique de $\mathbb{Q}$.

**Théorème 53.** [Admis] *(Steinitz)*
*Tout corps commutatif $K$ admet une clôture algébrique.*

## 3 Applications

### 3.1 Existence et unicité des corps finis

**Théorème 54.**
*Soit $p$ un nombre premier et $n \in \mathbb{N}^*$. On pose $q = p^n$.*

1. *Il existe un corps $K$ à $q$ éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.*
2. *En particulier, $K$ est unique à isomorphisme près. On le note $\mathbb{F}_q$.*

**Proposition 55.** *Soit $n, m \in \mathbb{N}$. Alors $\mathbb{F}_{p^n}$ s'injecte dans $\mathbb{F}_{p^m}$ si et seulement si $n|m$.*

**Exemple 56.** Les sous-corps de $\mathbb{F}_6$ sont $\mathbb{F}_4$ et $\mathbb{F}_2$.

**Théorème 57.** *(Wedderburn). Tout corps fini est commutatif.*

**Définition 58.** *On note $\mathbb{F}_q^*$ le groupe des inversibles de $\mathbb{F}_q$, donc $\mathbb{F}_q \setminus \{0\}$. On a ainsi $|\mathbb{F}_q^*| = q-1$.*

**Lemme 59.** *On note $\varphi$ l'indicatrice d'Euler. Alors $\varphi(n) = \sum_{d|n} \varphi(d)$.*

**Théorème 60.** *Le groupe $(\mathbb{F}_q^*, \times)$ est cyclique, donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.*

**Remarque 61.** En général, il est difficile d'exhiber un générateur de $\mathbb{F}_q^*$.

**Corollaire 62.** *(Théorème de l'élément primitif pour les corps finis).*
*Soit $L/\mathbb{F}_q$ une extension finie du corps fini $\mathbb{F}_q$. Alors il existe $\alpha \in L$ tel que $L = \mathbb{F}_q(\alpha)$.*

### 3.2 Cyclotomie

Dans ce qui suit, $K$ est un corps et $n \in \mathbb{N}^*$ est un entier tel que $\mathrm{car}(K) \nmid n$.

**Définition 63.** *On appelle groupe des racines $n^{\text{èmes}}$ de l'unité dans $K$, et on note $\mu_n(K)$ l'ensemble $\{\zeta \in K : \zeta^n = 1\}$. Une racine $n^{\text{ème}}$ de l'unité est dite primitive si de plus, pour tout $k$ divisant $n$, on a $\zeta^k \neq 1$. On note $\mu_n^*(K)$ l'ensemble des racines primitives $n^{\text{èmes}}$ de l'unité.*

**Définition 64.** *Le $n^{\text{ème}}$ polynôme cyclotomique sur $K$ est défini par :*

$$\Phi_{n,K}(X) := \prod_{\zeta \in \mu_n^*(K)} X - \zeta.$$

**Lemme 65.** *$\Phi_{n,K}(X)$ est unitaire, de degré $\varphi(n)$, et vérifie $X^n - 1 = \prod_{d|n} \Phi_{d,K}(X)$.*

**Développement 1 :**

**Théorème 66.** *(Polynômes cyclotomiques rationnels)*

*i. $\Phi_{n,\mathbb{Q}}(X)$ est à coefficients dans $\mathbb{Z}$.*

*ii. $\Phi_{n,\mathbb{Q}}(X)$ est irréductible sur $\mathbb{Z}$.*

**Théorème 67.** *(Cas des corps finis)*
*Les propositions suivantes sont équivalentes :*

*i. Il existe $p$ premier, avec $p \wedge n = 1$, tel que $\Phi_{n,\mathbb{F}_p}(X)$ soit irréductible sur $\mathbb{F}_p$.*

*ii.* $(\mathbb{Z}/n\mathbb{Z})^{\times}$ *est cyclique.*

### 3.3 Constructions à la règle et au compas

**Définition 68.** *Soit $E$ un sous ensemble du plan $\mathbb{R}^2$.*

- *On dit qu'un point $(x,y)$ est constructible sur $E$ en une étape si $(x,y)$ est l'intersection de deux objets parmi :*
    1. *L'ensemble des droites affines qui passent par deux éléments distincts de $E$*
    2. *L'ensemble des cercles dont le centre est un élément de $E$ et le rayon est la distance. entre deux points distincts de $E$.*

  *On note $C(E)$ l'ensemble des points constructibles sur $E$ en une étape.*
- *On définit par récurrence l'ensemble $C_n(E)$ des points constructibles sur $E$ en $n$ étapes par $C_{n+1}(E)=C(C_n(E))$.*
- *On dit que le point $(x,y)$ est constructible sur $E$ si $(x,y)\in\bigcup_{n=0}^{+\infty}C_n(E)$.*
- *Finalement, on dit qu'un nombre réel $x$ est constructible si $(x,0)$ est constructible sur $\{(0,0),(0,1)\}$.*

**Proposition 69.** *Soit $x,y$ des nombres constructibles.*
*Alors :*

- *La somme $x+y$ est constructible.*
- *La différence $x-y$ est constructible.*
- *Le produit $xy$ est constructible.*
- *Si $y\neq 0$, le quotient $x/y$ est constructible.*
- *La racine carrée $\sqrt{x}$ est constructible.*

**Théorème 70.** *(Wantzel, 1837)*

*Un nombre réel $a$ est constructible si et seulement si il existe $n\in\mathbb{N}$ et une suite finie de corps $(L_i)_{1\leq i\leq n}$ tels que :*

- $L_0=\mathbb{Q}$,
- $\forall i\in[\![1,n-1]\!]\quad L_i\subset L_{i+1}$ *et* $[L_{i+1}:L_i]=2$,
- $a\in L_n$.

*En particulier, tout nombre constructible est algébrique sur $\mathbb{Q}$ et son degré est une puissance de 2.*

**Définition 71.** *Soit $\theta\in\mathbb{R}$. On note $\hat{\theta}$ l'angle orienté dont une mesure en radian est $\theta$. L'angle $\hat{\theta}$ est dit constructible si le point $M$ du cercle de centre $O=(0,0)$ et de rayon 1 tel que $(\overrightarrow{\mathrm{OI}},\overrightarrow{\mathrm{OM}})=\hat{\theta}$, où $I=(1,0)$, est un point constructible.*

**Proposition 72.** *L'angle $\hat{\theta}$ est constructible si et seulement si le réel $\cos(\theta)$ est constructible.*

**Lemme 73.**

1. *Les angles de la forme $\widehat{\frac{2\pi}{2^\alpha}}$ sont constructibles pour $\alpha\in\mathbb{N}$.*
2. *Soient $n,m\in\mathbb{N}^*$ premiers entre eux. Alors l'angle $\widehat{\frac{2\pi}{mn}}$ est constructible si et seulement si les angles $\widehat{\frac{2\pi}{m}}$ et $\widehat{\frac{2\pi}{n}}$ le sont.*

**Développement 2 :**

**Théorème 74.** *(Gauss-Wantzel)*

*Soit $p$ un nombre premier impair, et $\alpha\in\mathbb{N}^*$. Alors l'angle $\widehat{\frac{2\pi}{p^\alpha}}$ est constructible si et seulement si $\alpha=1$ et $p$ est un nombre premier de Fermat, c'est-à-dire $p=1+2^{2^\beta}$ pour un certain $\beta\in\mathbb{N}$.*