**Développements :**

- Polynômes irréductibles sur un corps fini
- Théorème de Gauss-Wantzel

**Références :**

- Cours d'algèbre, Perrin
- Théorie de Galois, Gozard

# 1. Structure des extensions de corps

## 1.1. Définitions et résultats généraux [Gozard, Perrin]

- Def : une extension de corps est un morphisme de corps $\varphi : K \to L$
- Notation : $L/K$ si le morphisme est clair
- Ex : $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $K(X)/K$ pour $K$ corps
- Prop : si $L/K$ extension, alors $L$ est une $K$-algèbre pour $\lambda \cdot x = \varphi(\lambda)x$
- Def : degré de $L/K$, notée $[L : K]$
- Ex : $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$
- Thm : base télescopique
- Cor : si $M/L/K$ extensions, alors $[M : K] = [M : L][L : K]$
- Def : extension monogène
- Ex : $\mathbb{C} = \mathbb{R}(i)$
- Prop : une extension de degré premier est monogène

## 1.2. Structure des extensions monogènes [Gozard]

- Notation : pour $L/K$ extension, $a \in L$ et $P \in K[X]$, on note $\mathrm{ev}_a(P) = P(a)$
- Def : élément transcendant, élément algébrique, polynôme minimal noté $\mu_{a,K}$
- Prop : le polynôme minimal d'un élément algébrique est irréductible
- Thm : si $L/K$ extension et $a \in L$, alors :
  - si $a$ est transcendant sur $K$, alors $\mathrm{ev}_a : K(X) \to K(a)$ est un isomorphisme de corps
  - si $a$ est algébrique sur $K$, alors $\overline{\mathrm{ev}_a} : K(X)/\mu_{a,K} \to K(a)$ est un isomorphisme de corps et $(1, a, \dots, a^{d-1})$ est une base de $K(a)$, où $d = \deg \mu_{a,K}$
- Thm : pour $L/K$ extension et $a \in L$, s'équivalent :
  - $a$ est algébrique sur $K$
  - $K[a]$ est de dimension finie sur $K$

    - $K[a] = K(a)$
- Cor : si $a \in L \setminus \{0\}$ est algébrique sur $K$, alors $a^{-1} \in K[a]$

## 1.3. Extensions algébriques [Gozard]

- Def : extension algébrique, extension transcendante
- Ex : $\mathbb{C}/\mathbb{R}$ est algébrique de degré 2, $\mathbb{R}/\mathbb{Q}$ est transcendante
- Prop : si $L/K$ est algébrique et $A$ est une $K$-algèbre telle que $K \subseteq A \subseteq L$, alors $A$ est un corps
- Prop : une extension de degré fini est algébrique
- Rmq : réciproque fausse, par exemple avec $\mathbb{Q}(\mathcal{P})/\mathbb{Q}$

# 2. Adjonction de racines

## 2.1. Corps de rupture [Gozard]

- Def : corps de rupture
- Ex : $\mathbb{Q}(\sqrt{2})$ est un corps de rupture de $X^2 - 2$ sur $\mathbb{Q}$
- Thm : si $K$ corps et $P \in K[X]$ irréductible, alors :
    - $P$ admet un corps de rupture
    - deux corps de rupture sont isomorphes, à unique isomorphisme près
- Ex : construction de $\mathbb{C}$
- Ex : construction de $\mathbb{F}_4$ (cf. annexe)
- Cor : si $P \in K[X]$ de degré $\geq 1$, alors il existe une extension de $K$ dans laquelle $P$ a une racine

## 2.2. Corps de décomposition [Gozard]

- Def : corps de décomposition
- Ex : $\mathbb{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$
- Thm : si $K$ corps et $P \in K[X]$ de degré $\geq 1$, alors :
    - $P$ admet un corps de décomposition $L$ vérifiant $[L : K] \leq n!$
    - deux corps de décomposition sont isomorphes
- Rmq : un corps de rupture n'est pas un corps de décomposition en général, par exemple avec l'extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, j)$

## 2.3. Clôture algébrique [Gozard]

- Prop : pour $K$ corps, s'équivalent :
    - tout polynôme de degré $\geq 1$ de $K[X]$ est scindé sur $K$

    - tout polynôme de degré $\geq 1$ de $K[X]$ a une racine dans $K$
    - les irréductibles de $K[X]$ sont les polynômes de degré 1
    - $K$ est la seule extension algébrique de $K$
- Def : si $K$ vérifie les conditions ci-dessus, il est dit algébriquement clos
- Ex : $\mathbb{Q}$ et $\mathbb{R}$ ne le sont pas
- Prop : un corps algébriquement clos est infini
- Thm : d'Alembert-Gauss
- Cor : irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$
- Def : clôture algébrique
- Ex : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$
- Thm : Steinitz (admis)

# 3. Applications en algèbre et en géométrie

## 3.1. Corps finis [Gozard]

- Thm : si $K$ est un corps fini, alors :
    - sa caractéristique est un nombre premier $p$
    - son sous-corps premier est isomorphe à $\mathbb{F}_p$
    - son cardinal est une puissance de $p$
- Thm : si $p$ est premier, $n \in \mathbb{N}^*$ et $q = p^n$, alors :
    - il existe un corps fini à $q$ éléments, corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$
    - deux corps à $q$ éléments sont isomorphes
- Notation : $\mathbb{F}_q$ désigne "le" corps à $q$ éléments
- Prop : si $q = p^n$, alors
    - un sous-corps de $\mathbb{F}_q$ est de cardinal $p^d$ avec $d \mid n$
    - pour chaque diviseur $d$ de $n$, $\mathbb{F}_q$ a un unique sous-corps de cardinal $p^d$
- Thm : $X^{q^n} - X$ est le produit des irréductibles unitaires de $\mathbb{F}_q[X]$ de degré divisant $n$
- Thm : nombre d'irréductibles unitaires de $\mathbb{F}_q[X]$

## 3.2. Nombres constructibles à la règle et au compas [Gozard]

- Def : point constructible
- Def : nombre constructible
- Prop : constructibilité de médiatrices, milieux, parallèles, bissectrices
- Thm : l'ensemble des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée
- Thm : Wantzel
- Cor : si $x$ est constructible, alors $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de 2

- Rmq : en particulier, tout nombre constructible est algébrique
- App : impossibilité de la duplication du cube, de la quadrature du cercle, et de la trisection de l'angle en général
- Def : polygone régulier constructible
- Thm : Gauss-Wantzel

## Annexe

- Tables ($+$ et $\times$) de $\mathbb{F}_4$
- Diverses constructions à la règle et au compas