Développements :

- Polynômes irréductibles sur un corps fini
- Loi de réciprocité quadratique

Références :

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

1. Généralités sur les corps finis

1.1. Sous-corps premier, caractéristique [Gozard, Perrin]

- Def : sous-corps premier
- Def : caractéristique
- Prop : la caractéristique d'un corps est nulle ou un nombre premier
- Rmq : si K est de caractéristique nulle, alors K est infini
- Prop : si K est un corps fini, alors :
  - sa caractéristique est un nombre premier p
  - son sous-corps premier est isomorphe à $\mathbb{F}_p$
  - il existe $n \in \mathbb{N}^*$ tel que $|K| = p^n$
- Thm : si K est un corps, alors tout sous-groupe fini de $K^\times$ est cyclique
- Thm de l'élément primitif pour les corps finis

1.2. Existence et unicité [Gozard]

- Prop : si K est un corps fini de caractéristique p, alors $\mathrm{Frob}_K : K \to K$ est un automorphisme
- Cor : dans un corps fini de caractéristique p, chaque élément admet une et une seule racine p-ème
- Thm : si p est un nombre premier, $n \in \mathbb{N}$ et $q = p^n$, alors :
  - il existe un corps fini à q éléments, obtenu comme corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$
  - deux corps de cardinal q sont isomorphes
- Notation : $\mathbb{F}_q$
- Cor : le produit des éléments de $\mathbb{F}_q^\times$ vaut -1
- Cor (théorème de Wilson) : si $n \in \mathbb{N}_{\geq 2}$, alors n est premier ssi $(n-1)! \equiv -1 \bmod p$

Dans toute la suite on considère p premier, $n \in \mathbb{N}^*$ et $q = p^n$.

2. Structure de $\mathbb{F}_q$

2.1. Sous-corps de $\mathbb{F}_q$ [Gozard, Ulmer]

- Thm :
  - si K est un sous-corps de $\mathbb{F}_q$, alors il existe $d \mid n$ tel que $|K| = p^d$
  - pour chaque $d \mid n$, il existe un unique sous-corps de cardinal p^d de $\mathbb{F}_q$ et ce sous-corps est isomorphe à $\mathbb{F}_{p^d}$
- Cor : $\mathbb{F}_q$ s'identifie à un sous-corps de $\mathbb{F}_{q'}$ ssi q' est une puissance de q
- Cor : pour $a, b \in \mathbb{N}^*$, au sens de l'inclusion :
  - $\inf(\mathbb{F}_{q^a}, \mathbb{F}_{q^b}) = \mathbb{F}_{q^d}$ où $d = \mathrm{pgcd}(a, b)$
  - $\sup(\mathbb{F}_{q^a}, \mathbb{F}_{q^b}) = \mathbb{F}_{q^m}$ où $m = \mathrm{ppcm}(a, b)$
- Ex : treillis des sous-corps de $\mathbb{F}_{2^{12}}$ (cf. annexe)

2.2. Carrés dans $\mathbb{F}_q$ [Gozard]

- Notation : $\mathbb{F}_q^{[2]} = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{\times[2]} = \{x^2 \mid x \in \mathbb{F}_q^\times\}$
- Prop : $\mathbb{F}_q^{\times[2]}$ est un sous-groupe de $\mathbb{F}_q^\times$
- Prop : si $p > 2$, alors :
  - $\mathbb{F}_q^{\times[2]}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^\times$
  - $-1 \in \mathbb{F}_q^{\times[2]}$ ssi $q \equiv 1 \bmod 4$
- Rmq : si $p = 2$, alors $\mathbb{F}_q^{[2]} = \mathbb{F}_q$ (en particulier $\mathbb{F}_q^{\times[2]} = \mathbb{F}_q^\times$)

2.3. Cas particulier : carrés dans $\mathbb{F}_p$ [Gozard]

- Def : symbole de Legendre $\left(\frac{\cdot}{p}\right)$ pour p premier impair
- Ex : $\left(\frac{5}{7}\right) = -1$
- Prop : pour tout $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = a^{(p-1)/2}$
- Prop : le symbole de Legendre est un morphisme de groupes $\mathbb{F}_p^\times \to \{-1, 1\}$
- Prop :
  - $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{si } p \equiv 1 \bmod 4 \\ -1 & \text{si } p \equiv 3 \bmod 4 \end{cases}$
  - $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \bmod 8 \\ -1 & \text{si } p \equiv \pm 3 \bmod 8 \end{cases}$
- Thm : loi de réciprocité quadratique

3. Dénombrement sur les corps finis

3.1. Polynômes irréductibles sur $\mathbb{F}_q$ [Gozard]

- Thm : si $P \in \mathbb{F}_p[X]$ est irréductible de degré n, alors $\mathbb{F}_q \cong \mathbb{F}_p[X]/P$
- Cor :
  - il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_p$
  - si $P \in \mathbb{F}_p[X]$ est irréductible de degré n, alors son corps de rupture $\mathbb{F}_q$ est aussi son corps de décomposition
- Thm : $X^{q^n} - X = \prod_{d|n} \prod_{Q \in I(q,d)} Q$, où $I(q,d)$ désigne l'ensemble des irréductibles unitaires de degré d sur $\mathbb{F}_q$
- Cor : $q^n = \sum_{d|n} d|I(q,d)|$
- Cor : $|I(q,n)| = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$
- Rmq : en particulier, $|I(q,n)| \sim q^n/n$ lorsque $n \to \infty$

3.2. Isomorphismes exceptionnels [Perrin]

- Prop : cardinal de $\mathrm{GL}_n(\mathbb{F}_q)$ et associés
- Thm : isomorphismes exceptionnels

Annexe [Ulmer]

- Treillis des sous-corps de $\mathbb{F}_{2^{12}}$