**Leçon 123 - Corps finis. Applications.**

## 1. Généralités sur les corps finis. —

*1. Premières propriétés des corps finis, existence, unicité. —*

- Def : On appelle corps fini un corps ayant un nombre fini d'éléments.
- Ex : $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ est un corps fini pour p premier.
- Def+Pro : Pour tout anneau unitaire A, le noyau de l'unique morphisme d'anneaux de $\mathbb{Z}$ vers A est un idéal de $\mathbb{Z}$.
  Si cet idéal est réduit à $\{0\}$, on dit que $A$ est de caractéristique 0. S'il est engendré par $n \geq 1$, on dit que K est de caractéristique n.
- Pro : Pour K un corps, si $car(K) \neq 0$, alors $car(K) = p$ pour p premier.
- Pro : Pour K un corps fini, $car(K) \neq 0$. Pour p la caractéristique de K, K est une $\mathbb{F}_p$-algèbre , de dimension finie en tant que $\mathbb{F}_p$-espace vectoriel.
  On a ainsi $Card(K) = p^n$ pour un $n \geq 1$.
- Rem : Il n'existe ainsi aucun corps de cardinal 4 ou 105.
- Thm : Pour tout p premier, pour tout $n \geq 1$, il existe un corps fini de cardinal $p^n$. Un tel corps est unique à isomorphisme de $\mathbb{F}_p$-algèbre près. On le note $\mathbb{F}_{p^n}$.
- Rem : L'ensemble des éléments de $\mathbb{F}_{p^n}$ est solution de $x^{p^n} = x$. Le polynôme $X^{p^n} - X$ est ainsi scindé à racines simples sur $\mathbb{F}_{p^n}$.

*2. Le groupe des inversibles $\mathbb{F}_{p^n}^*$. —*

- Rem : Comme $\mathbb{F}_{p^n}$ est un corps, son groupe des inversibles est de cardinal $p^n - 1$.
- Pro : Pour tout $d|n$, l'ensemble des $x \in \mathbb{F}_{p^n}^*$ d'ordre d est exactement l'ensemble des solutions de $X^{p^d} - 1$ dans $\mathbb{F}_{p^n}$.
- App : $\mathbb{F}_{p^n}^*$ possède des éléments d'ordre q. Ce groupe est donc cyclique d'ordre $p^n - 1$.
- App : Théorème de Wedderburn : Soit A un anneau intègre fini (non supposé unitaire ou commutatif). Alors A est un corps fini.
- App : Les générateurs de $\mathbb{F}_{p^n}^*$ engendrent $\mathbb{F}_{p^n}$ comme $\mathbb{F}_p$-algèbre.
- Rem : La réciproque est fausse : Si x engendre $\mathbb{F}_{p^n}$ comme $\mathbb{F}_p$-algèbre, x n'est pas forcément d'ordre $p^n - 1$.

*3. Structure de $\mathbb{F}_{p^n}$. —*

- Pro : Les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ pour $d|n$, qui sont exactement les $\{x \in \mathbb{F}_{p^n} \text{ tq } x^{p^d} = x\}$.
- Ex : Dessin d'un treillis d'extensions de $\mathbb{F}_2$.
- Cor : Les $x \in \mathbb{F}_{p^n}$ tels que $\mathbb{F}_{p^n} = \mathbb{F}_p(x)$ sont exactement les éléments tels que $ord(x)|p^n - 1$ et $ord(x) \nmid p^d - 1$ pour tout $d|n$.
- Def : On définit le morphisme de Frobenius, Frob, sur $\mathbb{F}_{p^n}$ par $Frob(x) = x^p$.
- Pro : Frob est un automorphisme de $\mathbb{F}_{p^n}$ dont l'ensemble des points fixes est $\mathbb{F}_p$.
- Rem : Pour tout $d \geq 1$, $Frob^{(d)}(x) := Frob \circ .. \circ Frob(x) = x^{p^d}$.
- Pro : L'ensemble des points fixes de $Frob^{(d)}$ dans $\mathbb{F}_{p^n}$ est $F^{p^r}$ pour $r = pgcd(d, n)$.
- Pro : Soit $x \in \mathbb{F}_{p^n}$ de polynôme minimal $Irr(x, \mathbb{F}_p)$ sur $\mathbb{F}_p$ tel que $\mathbb{F}_{p^n} = \mathbb{F}_p(x) \simeq \mathbb{F}_p[X]/(Irr(x, \mathbb{F}_p))$. Un automorphisme $\phi$ de $\mathbb{F}_{p^n}$ qui préserve $\mathbb{F}_p$ est déterminé par l'image de x, qui doit être une racine de $Irr(x, \mathbb{F}_p)$.
  Il existe ainsi au plus n automorphismes de $\mathbb{F}_{p^n}$ qui laissent $\mathbb{F}_p$ stable.
- Thm : Le groupe des automorphismes de $\mathbb{F}_{p^n}$ qui laissent $\mathbb{F}_p$ stable est cyclique, de cardinal n, engendré par Frob.
- Rem : Pour $d|n$, on peut remplacer $\mathbb{F}_p$ et Frob par $\mathbb{F}_{p^d}$ et $Frob^{(d)}$ pour trouver que l'ensemble des automorphismes de $\mathbb{F}_{p^n}$ qui laissent $\mathbb{F}_{p^d}$ stable est le sous-groupe de $< Frob >$ engendré par $Frob^{(d)}$.
- App : Soit $P \in \mathbb{F}_{p^n}[X]$ tel que $P' = 0$. alors $P = Q^p$ pour un certain $Q \in \mathbb{F}_{p^n}[X]$.
- Pro : Tout polynôme irréductible sur $\mathbb{F}_{p^n}$ est premier avec son polynôme dérivé, donc à racines simples.

## 2. Carrés dans $\mathbb{F}_{p^n}$. —

*1. Généralités sur $\mathbb{F}_{p^n}^2$. —*

- Def : On définit $\mathbb{F}_{p^n}^2$ l'image de $x \mapsto x^2$ sur $\mathbb{F}_{p^n}$.
  On définit de même $(\mathbb{F}_{p^n}^*)^2$ l'ensemble des carrés de $\mathbb{F}_{p^n}^*$.
- Pro : Si $p = 2$, alors tous les éléments de $\mathbb{F}_{p^n}$ sont des carrés.
  Si $p \neq 2$, $Card(\mathbb{F}_{p^n}^*) = \frac{p^n - 1}{2}$.
- Pro : Si $p \neq 2$, $x \in \mathbb{F}_{p^n}^*$ est un carré ssi $x^{\frac{p^n-1}{2}} = 1$.
- App : -1 est un carré dans $\mathbb{F}_p$ ssi $p \equiv 1\ mod(4)$.
- App : Il existe une infinité de nombres premiers de la forme $4k + 1$.

*2. Symbole de Legendre. —*
On considère ici $p \neq 2$.

- Def : Pour tout $x \in \mathbb{F}_p$, on définit $(\frac{x}{p}) = \begin{cases} 1 \text{ si x} \in (\mathbb{F}_p^*)^2 \\ 0 \text{ si } x = 0 \\ -1 \text{ sinon} \end{cases}$ le symbole de Legendre.
- Pro : Le symbole de Legendre définit un morphisme de groupes de $\mathbb{F}_p^*$ vers $\{-1, 1\}$.
- Pro : $(\frac{x}{p}) = x^{\frac{p-1}{2}}$.
- Ex : $(\frac{-1}{p}) = (-1)^{\frac{p-1}{4}}$.
- **Dev** : Loi de réciprocité quadratique : Soient p,m des nombres premiers impairs distincts.
  Alors $(\frac{p}{m}) = (\frac{m}{p}).(-1)^{\frac{p-1}{2} \cdot \frac{m-1}{2}}$.
- Ex : $(\frac{23}{59}) = -1$
- Thm : $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

## 3. Polynômes sur un corps fini. —

*1. Clôture algébrique des corps finis. —*

- Def : Un corps K est dit algébriquement clos si tout polynôme de $K[X]$ non-constant admet une racine dans $K$.
- Pro : $\mathbb{F}_{p^n}$ n'est pas algébriquement clos car $X^{p^n} - X + 1$ n'a aucune racine dans $\mathbb{F}_{p^n}$.
- $F := \bigcup_{m \geq 1} \mathbb{F}_{p^{m!}}$ est un corps algébriquement clos contenant $\mathbb{F}_{p^n}$. (on parle alors de clôture algébrique de $\mathbb{F}_{p^n}$)

*2. Polynômes irréductibles sur un corps fini. —*

- Pro : Pour $d|n$ et pour tout tout $P \in \mathbb{F}_{p^d}[X]$ irréductible de degré $\frac{n}{d}$, on a un isomorphisme de $\mathbb{F}_{p^d}$-algèbres entre $\mathbb{F}_{p^n}$ et $\mathbb{F}_{p^d}[X]/(P)$.
- Cor : Il existe des polynômes irréductibles sur $\mathbb{F}_{p^n}$ de tout degré.
- Ex : $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1)$.
- Def : On note $I(n,q)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q$.
- Pro : $\forall n \geq 1$, $X^{q^n} - X = \Pi_{d|n} \Pi_{P \in I(d,q)} P$
- Def : On définit la fonction de Moëbius $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par :
  $\begin{cases} 0 \text{ si n a un facteur carré} \\ (-1)^r \text{ si } n = p_1..p_r \text{ avec } p_i \text{ premiers distincts} \end{cases}$.
- **Dev** : Pour tout $n \geq 1$, on a : $n.|I(n,q)| = \sum_{d|n} \mu(\frac{n}{d}).q^d$.
  On a ainsi $I(n,q) \sim \frac{q^n}{n}$ pour $n \to +\infty$.
- App : Test de Rabin : $P \in \mathbb{F}_q[X]$ est irréductible sur $\mathbb{F}_q$ ssi P divise $X^{q^n} - X$ et si $P \wedge X^{q^d} - X = 1$ pour tout d diviseur strict de n.
- Ex : Factorisation de $X^{2^3} - X$ sur $\mathbb{F}_2$.
- Pro : Soit $P \in \mathbb{F}_{p^n}[X]$ de degré $m \geq 2$. P est irréductible sur $K$ ssi P n'admet aucune racine dans tout $\mathbb{F}_{p^n d}$ pour $d \leq \lceil \frac{m}{2} \rceil$.
- App : Soit $P$ $in\mathbb{Z}[X]$, et p premier ne divisant pas le coefficient dominant de P. Si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Z}[X]$.
- Ex : $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$, donc irréductible sur $\mathbb{Z}$.
- Contre-ex : $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ mais est pourtant réductible dans tous les $\mathbb{F}_p[X]$.
- Def : Pour tout $n \geq 1$, on définit $\Phi_n(X) := \Pi_{k \wedge n = 1,\ k \leq n}(X - e^{2i\pi \frac{k}{n}}) \in \mathbb{C}[X]$, le n-ième polynôme cyclotomique.
- Pro : Pour tout $n \geq 1$, $\Phi_n$ est un polynôme unitaire à coefficients entiers, irréductible dans $\mathbb{Z}[X]$, de degré $\phi(n) = Card(\mathbb{Z}/n\mathbb{Z}^*)$ et tel que $\Pi_{d|n} \Phi_d = X^n - 1$.
  On peut ainsi projeter les polynômes cyclotomiques dans $\mathbb{F}_p[X]$ et avoir une décomposition de $X^n - 1$. en produit de polynômes.
- Pro : Pour tout $n = p^s.m$ avec $m \wedge p = 1$, $\Phi_n(X) = \Phi_m(X)^{p^s - p^{s-1}}$ dans $\mathbb{F}_p[X]$.
  Si $n \wedge p = 1$, alors tous les facteurs irréductibles de $\Phi_n$ dans $\mathbb{F}_q[X]$ sont de degré égal à l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Rem : Comme $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est cyclique que si $n = \widetilde{p}$ ou $n = 2\widetilde{p}$ avec $\widetilde{p}$ premier, une grande partie des polynômes cyclotomiques n'est automatiquement pas irréductible sur les $\mathbb{F}_q$.

*3. Polynômes à plusieurs variables sur $\mathbb{F}_q$. —*

- Def : Soit q une forme quadratique sur un corps K, avec $car(K) \neq 2$.
  Le discriminant de q est la classe de $det(A)$ dans $\mathbb{K}^*/((\mathbb{K}^*)^2)$ si q est non-dégénérée, et vaut 0 si q est dégénérée. Il ne dépend pas de la base choisie.
- Thm : Toute forme quadratique q sur un K-ev de dimension finie ($car(K) \neq 2$) possède une base dans laquelle sa forme polaire est diagonale.
- Lemme : Pour tous $a, b \in \mathbb{F}_{p^n}^*$, il existe $x, y \in \mathbb{F}_{p^n}$ tels que $ax^2 + by^2 = 1$.
- App : Classification des formes quadratiques sur les corps finis : Pour q forme quadratique non-dégénérée sur $\mathbb{F}_{p^n}^m$, il existe une base dans laquelle la forme polaire de q est de la forme $Diag(1, .., 1)$ ou bien $Diag(1, .., 1, \varepsilon)$ pour $\varepsilon$ un non-carré de $\mathbb{F}_{p^n}$.
- **Dev** : Théorème de Chevalley-Warning : Soit p premier, q une puissance de p, $n \geq 1$. Soient $P_1, .., P_r \in \mathbb{F}_q[X_1, .., X_n]$ tels que $\sum_{i \leq r} \deg_{tot}(P_i) < n$, et soit $V := \cup_i P_i^{-1}(\{0\})$. Alors $Card(V) \equiv 0 \mod(p)$.
- App : Théorème de Ginszbourg-Erdös-Sziv : Soit $n \geq 1$ et soient $a_1, .., a_{2n-1} \in \mathbb{Z}$. Alors il existe $1 \leq i_1 < i_2 < .. < i_n \leq 2n - 1$ tels que $a_{i_1} + .. + a_{i_n} \equiv 0 \mod(n)$.

**Références**


Perrin : Corps finis, existence, unicité, construction, groupe des inversibles, générateurs, structure, éléments primitifs, exemples. Extensions, clôture algébrique. Carrés dans les $\mathbb{F}_q$. Polynômes irred sur un corps fini. Discriminant d'une forme quadratique, classification.
Gozard : Corps, extensions de corps, exemples. Polynômes irréductibles sur un corps fini.
Gourdon : Symbole de Legendre.
FGN (Algèbre 1) : Polynômes irréductibles de degré n sur $\mathbb{F}_q$.(Dev)
Zavidovique : Th de Chevalley-Warning et de Erdös-Ginzburg-Sziv.(Dev)
Caldero,Germoni : Loi de réciprocité quadratique.(Dev)


---

*January 23, 2018*


*Vidal Agniel, École normale supérieure de Rennes*