Leçon 123 : Corps finis. Applications.

Rombaldi
Dreveton - Lhabouz
Berhuy (dev 1)
Francinou (dev 2)

Dans cette leçon, $\mathbb{K}$ désignera un corps commutatif, p un nombre premier et n un entier strictement positif.

I - Généralités préliminaires

1. Caractéristique et conséquences

Définition 1.1 Soit A un anneau unitaire et intègre. On considère le morphisme $\varphi : \mathbb{Z} \to A$, $n \mapsto n.1$. On définit alors la caractéristique de A, car A, comme l'unique entier $m \in \mathbb{N}$ tel que $\ker \varphi = m\mathbb{Z}$.

Proposition 1.2 La caractéristique est 0 ou un nombre premier.
De plus, si car $A = 0$ alors A est infini.

Contre-exemple 1.3
$\mathbb{F}_p(X)$ est infini mais de caractéristique p

Définition 1.4 On appelle sous-corps premier de $\mathbb{K}$, le plus petit sous-corps de $\mathbb{K}$.

Proposition 1.5 Le sous-corps premier de $\mathbb{K}$ est $\mathbb{Q}$ ou $\mathbb{F}_p$ pour un nombre premier p.

Corollaire 1.6 Si $\mathbb{K}$ est de caractéristique $p \neq 0$ alors $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectoriel.
En particulier, si $\mathbb{K}$ est fini, il existe $n \in \mathbb{N}^*$ tel que $|\mathbb{K}| = p^n$.

Exemple 1.7
il n'existe pas de corps de cardinal 6

2. Propriétés d'un corps fini

Définition - Proposition 1.8 Soit $\mathbb{K}$ un corps de caractéristique $p \neq 2$. On définit l'application $\phi : \mathbb{K} \to \mathbb{K}$, $x \mapsto x^p$. Il s'agit d'un morphisme de corps injectif que l'on appelle morphisme de Frobenius.

Proposition 1.9 Sous les hypothèses précédentes, les éléments fixés par ϕ sont exactement les éléments de $\mathbb{F}_p$.

Application 1.10
$Q \in \mathbb{F}_p[X] \iff Q(X^p) = Q(X)^p$

Théorème 1.11 Soit $\mathbb{K}$ un corps fini d'ordre p^n. Alors, tout sous-corps de $\mathbb{K}$ est de cardinal p^d avec d diviseur de n.
Réciproquement, pour tout diviseur d de n, il existe un unique sous-corps de $\mathbb{K}$ de cardinal p^d, à savoir $\mathbb{F} = \{x \in \mathbb{K} \mid x^{p^d} = x\}$.

Théorème 1.12 (Wedderburn) Soit A un corps fini (un anneau unitaire ~~sans diviseur de zéro~~ tel que $A^* = A \setminus \{0\}$). Alors A est commutatif.

développement 1

Lemme 1.13 Soient $d, n, q \in \mathbb{N}^*$ avec $q \geq 2$. Alors, $q^d - 1$ divise $q^n - 1$ si et seulement si d divise n. Le cas échéant, $\Phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$ pour d diviseur strict.

II - Construction de corps finis

1. Polynômes irréductibles de $\mathbb{F}_p[X]$

On note $U(m,p)$ l'ensemble des polynômes irréductibles unitaires de degré m de $\mathbb{F}_p[X]$ et $I(m,p) = \#U(m,p)$.

Lemme 2.1 Tout diviseur irréductible de $P_n = X^{p^n} - X$ est de degré divisant n. Réciproquement, pour tout $d \mid n$, tout polynôme $P \in U(d,p)$ divise P_n.

Théorème 2.2 Le polynôme P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en facteurs irréductibles :

$$X^{p^n} - X = \prod_{d \mid n} \prod_{P \in U(d,p)} P$$

développement 2

Théorème 2.3 En désignant par μ la fonction de Möbius, on a pour tout $n \in \mathbb{N}^*$, $I(n,p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$.

Corollaire 2.4 Pour tout $n \geq 1$, $I(n,p) \sim \frac{p^n}{n}$.

2. Construction formelle

Théorème 2.5 À un isomorphisme près, il n'existe qu'un seul corps à p^n éléments, $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ où $P \in I(n,p)$.

Proposition 2.6 Soient $m,n \in \mathbb{N}^*$. Alors $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ si et seulement si n divise m.

Exemple 2.7

On a : $\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16}$ mais $\mathbb{F}_8$ n'est pas un sous-corps de $\mathbb{F}_{16}$

Exemple 2.8

$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ est un corps à 4 éléments

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

×	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

3. Cyclicité de $\mathbb{F}_q^*$ et application

Proposition 2.9 Soit $q = p^n$. Alors $\mathbb{F}_q^*$ est cyclique.

Corollaire 2.10 Il existe $\xi \in \mathbb{F}_q$ tel que $\mathbb{F}_q^* = \mathbb{F}_q[\xi]$. On peut donc voir $\mathbb{F}_q$ comme $\mathbb{F}_p(\xi)$.

III - Étude des carrés

On considère $q = p^n$ avec $p > 2$.

Définition 3.1 On note $\mathbb{F}_q^2 := \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, x = y^2\}$ l'ensemble des carrés de $\mathbb{F}_q$ et $\mathbb{F}_q^{*2}$ les carrés non nuls.

Remarque 3.2 Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$.

Proposition 3.3 On a : $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

Proposition 3.4 Soit $x \in \mathbb{F}_q^*$. Alors $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.

Corollaire 3.5 Le produit de deux carrés ou non carrés est un carré, tandis que le produit d'un carré et d'un non carré est un non carré.

Définition 3.6 Pour tout $x \in \mathbb{F}_p^*$, on définit le symbole de Legendre comme l'entier $\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \in \mathbb{F}_p^{*2} \\ -1 \text{ sinon.} \end{cases}$

Proposition 3.7 Pour tout $x \in \mathbb{F}_p^*$, $x^{\frac{p-1}{2}} = \overline{\left(\frac{x}{p}\right)}$ dans $\mathbb{F}_p^*$

Proposition 3.8 L'application $\mathbb{F}_p^* \longrightarrow \{\pm 1\}$, $x \longmapsto \left(\frac{x}{p}\right)$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ sur $\{\pm 1\}$.

Application 3.9 Soient E un $\mathbb{F}_q$-espace vectoriel et $\alpha \in \mathbb{F}_q^*$ avec $\alpha \notin \mathbb{F}_q^{*2}$. Il y a alors deux classes d'équivalence de formes quadratiques non dégénérées de E, $Q_1 = I_n$ ou $Q_2 = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & \alpha \end{pmatrix}$