

Chapitre 2 : Corps finis.

EXERCICE 1 : Ecrire la table d'addition et de multiplication d'un corps à 4 éléments.

Soit K un corps fini à 4 éléments. Soit $\alpha \in K$, $\alpha \neq 0$ et $\alpha \neq 1$. Alors $1+\alpha \in K$. On ne peut pas avoir $1+\alpha = 1$ puisque $\alpha \neq 0$, ni $1+\alpha = \alpha$ (impossible). De plus $1+\alpha = 0 \Rightarrow \alpha = -1$. Alors le groupe $(\{1, -1\}, \times)$ serait un sous-groupe ^{d'ordre 2} du groupe multiplicatif d'ordre 3 K^* ce qui est impossible. Donc $K = \{0, 1, \alpha, 1+\alpha\}$

Table d'addition

+	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$1+1=0$ car K est de caractéristique 2 car $|K|=4=2^2$.

Table de multiplication :

	1	α	$1+\alpha$
1	1	α	$1+\alpha$
α	α	$1+\alpha$	1
$1+\alpha$	$1+\alpha$	1	α

K^* est un groupe cyclique d'ordre 3 donc $\alpha^2 \neq \alpha$ et $\alpha^2 \neq 1$ donc $\alpha^2 = 1+\alpha$ et la table s'en déduit

EXERCICE 2 : Soit le polynôme $P = 1+X+X^2 \in \mathbb{F}_2[X]$.

1) Montrer que P est irréductible dans $\mathbb{F}_2$.

Si P n'est pas irréductible il admet un facteur de degré 1 et donc une racine dans $\mathbb{F}_2$. Or $P(0) = 1$ et $P(1) = 1+1+1=1$ donc P n'a pas de racine dans $\mathbb{F}_2$ et est donc irréductible dans $\mathbb{F}_2$.

2) Déterminer le corps K de décomposition de P .

Déterminons le corps de rupture de $P = 1+X+X^2$. Comme P est irréductible, ce corps est bien défini. Il est donné par

$$\frac{\mathbb{F}_2[X]}{(1+X+X^2)} \quad \text{soit } \pi: \mathbb{F}_2[X] \longrightarrow \frac{\mathbb{F}_2[X]}{(1+X+X^2)} \quad \text{la projection canonique. Posons } \alpha = \pi(X). \text{ Alors } \alpha^2 + \alpha + 1 = 0 \text{ et donc}$$

$\alpha^2 = -1 - \alpha = 1 + \alpha$. Le corps de rupture de P est donc $\mathbb{F}_2[\alpha]$. Comme α^2 vérifie $(\alpha^2)^2 + \alpha^2 + 1 = (1+\alpha)(1+\alpha) + \alpha^2 + 1 = 1 + \alpha^2 + \alpha^2 + 1 = 0$, α^2 est aussi une racine de P appartenant à $\mathbb{F}_2[\alpha]$. Le corps de rupture de P est donc le corps de décomposition de P puisqu'il contient toutes les racines de P .

- 3) Montrer que $\mathbb{K}$ est un corps fini contenant 4 éléments. Par construction $\mathbb{K}$ est un espace vectoriel de dimension 2 sur $\mathbb{F}_2$ et $\{1, \alpha\}$ en est une base. Les éléments sont donc $\{0, 1, \alpha, 1+\alpha\}$ (seules combinaisons linéaires de 1 et α à coefficients dans $\mathbb{F}_2$).

EXERCICE 3 : 1) Montrer que si $\mathbb{K}$ est un corps fini, tout sous-groupe du groupe multiplicatif $\mathbb{K}^*$ est cyclique. Comme $\mathbb{K}$ est d'ordre fini le groupe multiplicatif $\mathbb{K}^*$ des éléments inversibles est cyclique. Tout sous-groupe de $\mathbb{K}^*$ est donc cyclique.

2) Déterminer les groupes multiplicatifs $\mathbb{K}^*$ lorsque $\mathbb{K} = \mathbb{F}_p$ avec $p = 2, 3, 5, 7, 11$. Trouver dans chaque cas un générateur de $\mathbb{K}^*$. Le groupe multiplicatif $\mathbb{F}_p^*$ est cyclique d'ordre $p-1$. Il est isomorphe à $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$. Le problème se résume donc à chercher un générateur.

- $p = 2$ $\mathbb{F}_2^* = \{1\}$.
- $p = 3$ $\mathbb{F}_3^* = \{\bar{1}, \bar{2}\} = \langle \bar{2} \rangle$
- $p = 5$ $\mathbb{F}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \langle \bar{2} \rangle = \langle \bar{3} \rangle$
- $p = 7$ $\mathbb{F}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = \langle \bar{3} \rangle = \langle \bar{5} \rangle$
- $p = 11$ $\mathbb{F}_{11}^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}\} = \langle \bar{2} \rangle = \langle \bar{6} \rangle = \langle \bar{7} \rangle = \langle \bar{8} \rangle$

EXERCICE 4 : On considère le corps fini $\mathbb{F}_{2^m}$ contenant 2^m éléments. On pose $\mathbb{F}_{2^m}^2 = \{x \in \mathbb{F}_{2^m} / \exists y \in \mathbb{F}_{2^m} \text{ vérifiant } x = y^2\}$ l'ensemble des carrés de $\mathbb{F}_{2^m}$.

1) Déterminer $\mathbb{F}_{2^m}^2$ pour $m=1$ et $m=2$.

$$\mathbb{F}_2^2 = \{0, 1\}$$

$$\mathbb{F}_4^2 : \mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}. \text{ On a } 0^2 = 0, 1^2 = 1, \alpha^2 = 1+\alpha \text{ et } (1+\alpha)^2 = \alpha. \text{ Donc } \mathbb{F}_4^2 = \{0, 1, \alpha, 1+\alpha\} = \mathbb{F}_4.$$

($\mathbb{F}_4$ a été déterminé à l'exercice 1).

2) Montrer qu'en général $\mathbb{F}_{2^m}^2 = \mathbb{F}_{2^m}$.

Comme $\mathbb{F}_{2^m}$ est de caractéristique 2 l'homomorphisme de Frobenius

$$F : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m} \text{ est donné par}$$

$$F(x) = x^2.$$

Il est injectif donc il est surjectif car $\mathbb{F}_{2^m}$ est un ensemble fini. Ainsi tout élément de $\mathbb{F}_{2^m}$ est un carré.

EXERCICE 5 : On considère les corps finis $\mathbb{F}_{p^m}$ pour $p > 2$. Notons $\mathbb{F}_{p^m}^2$ l'ensemble des carrés de $\mathbb{F}_{p^m}$ (voir exercice 4)

1) Déterminer $\mathbb{F}_5^2, \mathbb{F}_7^2$.

$$\bullet \mathbb{F}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}. \text{ On a } \bar{0}^2 = \bar{0}, \bar{1}^2 = \bar{1}, \bar{2}^2 = \bar{4}, \bar{3}^2 = \bar{4} \text{ et } \bar{4}^2 = \bar{1} \text{ d'où } \mathbb{F}_5^2 = \{\bar{0}, \bar{1}, \bar{4}\}.$$

$$\bullet \mathbb{F}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}. \text{ On a } \bar{0}^2 = \bar{0}, \bar{1}^2 = \bar{1}, \bar{2}^2 = \bar{4}, \bar{3}^2 = \bar{2}, \bar{4}^2 = \bar{2}, \bar{5}^2 = \bar{4}, \bar{6}^2 = \bar{1} \text{ d'où } \mathbb{F}_7^2 = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}\}.$$

$$2) \text{ Montrer que } |\mathbb{F}_{p^m}^2| = \frac{p^m + 1}{2} \text{ et } |\mathbb{F}_{p^m}^{*2}| = \frac{p^m - 1}{2}$$

$$\text{avec } \mathbb{F}_{p^m}^{*2} = \mathbb{F}_{p^m}^2 \cap \mathbb{F}_{p^m}^*.$$

Considérons l'application $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$ donnée par

$$f(x) = x^2. \quad (\text{comme } p > 2 \text{ ce n'est pas l'homomorphisme de Frobenius}).$$

L'application f est un endomorphisme du groupe $\mathbb{F}_{p^m}^*$. Son image est $\mathbb{F}_{p^m}^{*2}$ et son noyau est

$\text{Ker}(f) = \{-1, 1\}$. Ainsi $\mathbb{F}_{p^m}^{*2}$ est isomorphe à $\frac{\mathbb{F}_{p^m}^*}{\text{Ker}(f)}$. Il est donc un sous-groupe d'indice 2 de

$$\mathbb{F}_{p^m}^* . \quad \text{Ainsi} \quad |\mathbb{F}_{p^m}^{*2}| = \frac{|\mathbb{F}_{p^m}^*|}{2} = \frac{p^m - 1}{2} .$$

Comme $\mathbb{F}_{p^m}^2 = \mathbb{F}_{p^m}^{*2} \cup \{0\}$ on a $|\mathbb{F}_{p^m}^2| = \frac{p^m + 1}{2} .$

3) Montrer que $x \in \mathbb{F}_{p^m}^{*2}$ si et seulement si $x^{\frac{p^m-1}{2}} = 1$.

Soit $x \in \mathbb{F}_{p^m}^{*2}$. Le groupe $\mathbb{F}_{p^m}^{*2}$ est par définition un sous-groupe du groupe $\mathbb{F}_{p^m}^*$ qui est cyclique. Le groupe $\mathbb{F}_{p^m}^{*2}$ est donc un groupe cyclique. De plus on sait que son ordre est $\frac{p^m-1}{2}$. Ainsi $x^{\frac{p^m-1}{2}} = 1$.

Réciproquement si x vérifie $x^{\frac{p^m-1}{2}} = 1$. Alors $\langle x \rangle$ est un groupe cyclique dont l'ordre divise $\frac{p^m-1}{2}$.