Leçon 123 : Corps finis. Applications.

I Préliminaires sur les corps

1 Caractéristique d'un corps

- car($\mathbb{K}$) est soit nulle, soit un nombre premier, $\mathbb{K}$ est infini dans le premier cas et $|\mathbb{K}| = p^n$ dans le second
- Si $|\mathbb{K}| = p^n$, alors $\forall k \subset \mathbb{K}, |k| = p^d$ où $d|n$
- Si $|\mathbb{K}| = p^n$, alors $\forall d|n, \exists! k \subset \mathbb{K}$ tel que $|k| = p^d$
- cf. Figure 1 - Sous-corps de $\mathbb{F}_{2^{12}}$
- Morphisme de Frobenius

2 Extension de corps

- Degré d'une extension
- Corps de rupture, corps de décomposition

II Construction des corps finis

1 Comme corps de décomposition

- $\mathbb{F}_q := Dec_{\mathbb{F}_p}(X^q - X)$ où $q = p^n$
- On a unicité à isomorphisme près mais la construction est théorique

2 Comme corps de rupture

- Sur $\mathbb{F}_p$, il existe des polynômes unitaires irréductibles de tout degré
- $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[X]/(Q)$ où Q est irréductible sur $\mathbb{F}_p$ de degré n
- Construction plus simple pour faire des calculs mais il faut trouver un polynôme Q

III Carrés de $\mathbb{F}_q$

1 Caractérisation des carrés de $\mathbb{F}_q$

- DEV 1 : Cardinal des carrés de $\mathbb{F}_q$ + Caractérisation des carrés + Critère pour que -1 soit un carré + $\mathbb{Z}[i]$ est euclidien + Théorème des 2 carrés
- $\forall a, b \in \mathbb{F}_q^*, \forall c \in \mathbb{F}_q, \exists x, y \in \mathbb{F}_q, c = ax^2 + by^2$

2 Symbole de Legendre

- Définition
- $(\frac{a}{p}) = a^{\frac{p-1}{2}}$, c'est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{\pm 1\}$
- Loi de réciprocité quadratique

III Groupe linéaire sur $\mathbb{F}_q$

- DEV 2 : Cardinal de $GL_n(\mathbb{F}_q), SL_n(F_q), PGL_n(\mathbb{F}_q), PSL_2(\mathbb{F}_q), \mathbb{P}^{n-1}(\mathbb{F}_q)$ + Isomorphismes exceptionnels
- Critère de diagonalisabilité d'un endomorphisme sur un $\mathbb{F}_q$-espace vectoriel
- Dénombrement des endomorphismes diagonalisables sur $\mathbb{F}_q$

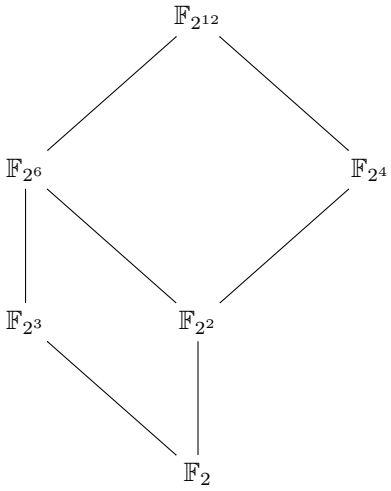

FIGURE 1 – Sous-corps de $\mathbb{F}_{2^{12}}$