L3 Algèbre effective - TD Corps intermédiaires

Novembre 2019

1. Soit K une $\mathbb{F}_p$-algèbre. On note F l'application $K \to K$, $x \mapsto x^p$, et $K^{<F^{\circ k}>}$ l'ensemble des points fixes de K sous l'action de F itéré k fois, c'est à dire $\{x \in K,\ F^{\circ k}(x) = x\}$

Montrer que pour $K = \mathbb{F}_{p^n}$, l'ensemble $K^{<F^{\circ k}>}$ est un sous-corps de K contenant $\mathbb{F}_p$. Montrer que ce sous-corps est $\mathbb{F}_p$ lorsque $k = 1$ et est K lui-même lorsque $k = n$.

Montrer que $X^4 - X$ divise $X^{16} - X$ dans $\mathbb{F}_2[X]$ (en fait dans $\mathbb{Z}[X]$, voir les notes de cours "Fp algèbres finis"). En déduire que ${\mathbb{F}_{16}}^{<F^{\circ 4}>} = \mathbb{F}_4$.

Donner une représentation de $\mathbb{F}_4$ comme quotient de $\mathbb{F}_2[X]$. Combien y a t-il d'automorphismes de $\mathbb{F}_4$? Combien y a t-il de morphismes de corps $\mathbb{F}_4 \to \mathbb{F}_{16}$?

2. On pose $Q = 1 + X + X^2 + X^3 + X^4$ et $K = \mathbb{F}_2[X]/(Q)$. On note x la classe de X dans K.

Quel est le rang de $F - \mathrm{id} : K \to K$ comme endomorphisme de $\mathbb{F}_2$-espaces vectoriels ? (Observer pour les calculs qu'on a $x^5 = 1$ dans K.) Qu'en déduit on sur Q ?

Observer que K contient $\mathbb{F}_4$ et expliciter un générateur y de $\mathbb{F}_4$ comme sous-algèbre de K (On pourra observer que pour $z \in K$, l'élément $z + F^{\circ 2}z$ est fixé par $F^{\circ 2}$ donc est dans $\mathbb{F}_4$).

Montrer que $(1, y)$ est une base de $\mathbb{F}_4 \subset K$ comme $\mathbb{F}_2$ - espace vectoriel et que $(1, x)$ est une base de K comme $\mathbb{F}_4$ - espace vectoriel. En déduire que $(x^i y^j)_{0 \leq i,j \leq 1}$ est une base de K comme $\mathbb{F}_2$ - espace vectoriel. Quelle en est la matrice des coordonnées relativement à la base $(1, x, x^2, x^3)$ et à un ordre à choisir sur les indices i, j ?

Calculer les coordonnées de x^2 dans la base $(x^i y^j)$. En déduire le polynome minimal $m_{x,\mathbb{F}_4}$ de x dans K vue comme $\mathbb{F}_4$-algèbre.

Montrer que $m_{x,\mathbb{F}_4}$ divise Q dans $\mathbb{F}_4[X]$.

Quel est le rang de $F^{\circ 2} - \mathrm{id} :\ \mathbb{F}_4[X]/(Q)\ \circlearrowleft$ comme endomorphisme de $\mathbb{F}_4$-espaces vectoriels ? Et de $F - \mathrm{id} :\ \mathbb{F}_4[X]/(Q)\ \circlearrowleft$ comme endomorphisme de $\mathbb{F}_2$-espaces vectoriels ? L'application $F - \mathrm{id} :\ \mathbb{F}_4[X]/(Q)\ \circlearrowleft$ est elle un endomorphisme de $\mathbb{F}_4$ - espaces vectoriels ?

Que donne l'algorithme de Berlekamp pour la factorisation de Q dans $\mathbb{F}_4[X]$?

3. Montrer de plusieurs façons que $1 + X + X^3$ est irréductible dans $\mathbb{F}_4[X]$. L'est il dans $\mathbb{F}_2[X]$? Qu'en est il pour $1 + X + X^5$?

```
K.<X>=PolynomialRing(GF(4),'X')
P=1+X^2+X^3
P.is_irreducible()
```

4.★ Montrer qu'aucun $P \in \mathbb{F}_2[X]$ de degré pair n'est irréductible dans $\mathbb{F}_4[X]$.

Peut on trouver $P \in \mathbb{F}_2[X]$ de degré impair, irréductible dans $\mathbb{F}_2[X]$ mais pas dans $\mathbb{F}_4[X]$?

5.★ Quel est le sous-corps $\left(\mathbb{F}_{p^n}\right)^{<F^{\circ k}>}$ selon k ?