Master CSI 1

Arithmétique 1

Feuille d'exercices n° 5.

1 Soit $\mathbb{F}_q$, $q = p^k$.

1. Démontrez si cela n'a pas été fait en cours que, pour tout $\alpha, \beta \in \mathbb{F}_q$, $\text{trace}(\alpha) + \text{trace}(\beta) = \text{trace}(\alpha + \beta)$.
2. Démontrez, si cela n'a pas été fait en cours, que $\text{trace}(\sigma(\alpha)) = \text{trace}(\alpha)$, où σ est l'automorphisme de Frobenius.
3. Si $\alpha \in \mathbb{F}_q$ est de degré k, montrez que $\text{trace}(\alpha)$ est l'opposé du coefficient de X^{k-1} dans le polynôme minimal de α sur $\mathbb{F}_p$. Que se passe-t-il si α est de degré un diviseur strict de k ?
4. Applications : dans $\mathbb{F}_{2^6}$, α est racine du polynôme primitif $f(X) = X^6 + X + 1$. Calculez $\text{trace}(1)$, $\text{trace}(\alpha)$, $\text{trace}(\alpha^2)$, $\text{trace}(\alpha^3)$, $\text{trace}(\alpha^4)$, $\text{trace}(\alpha^6)$.

2 Soit $K = \mathbb{F}_q$ un corps fini de caractéristique p et soit $L = \mathbb{F}_{q^2}$. On rappele que $K \subset L$ et $[L : K] = 2$.

1. Soit $\alpha \in L$. Montrez que $t = \alpha + \alpha^q$ et $n = \alpha^{1+q}$ appartiennent à K.
2. Déduire de la question précédente que le polynôme $X^2 - tX + n$ appartient à $K[X]$ et a α pour racine. Quelle est son autre racine ?
3. Montrez que, si $\alpha \notin K$, le polynôme $X^2 - tX + n$ est le polynôme minimal de α sur K.

3

Soit $F = \mathbb{F}_{2^L}$. Comme d'habitude, on note $\sigma(x) = x^2$ le Frobenius. On pose, pour tout $a \in F$,

$$\text{trace}(a) = a + a^2 + a^4 + \cdots + a^{2^{L-1}} = a + \sigma(a) + \cdots + \sigma^{L-1}(a).$$

Soit $f(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_L x^L$ un polynôme de $\mathbb{F}_2[x]$ de degré L que l'on suppose irréductible. On fixe une racine α de f dans F. On a donc $F = \mathbb{F}_2[\alpha]$.

On rappelle que l'on dit que f engendre la suite $s = (s_0, s_1, \dots)$ si pour tout $j \geq L$, on a :

$$s_j = \sum_{i=1}^{L} c_i s_{j-i} = c_1 s_{j-1} + c_2 s_{j-2} + \cdots + c_L s_{j-L}.$$

1. (a) Montrez que, si $\text{trace}(b) = 0$, alors b est racine d'un polynôme de degré 2^{L-1}. En déduire qu'il existe $b \in F$ tel que $\text{trace}(b) \neq 0$.
   (b) Montrez que, si $\text{trace}(au) = 0$ pour tout $u \in F$, alors $a = 0$.
2. (a) Montrez que, pour tout $\beta \in F$, la suite définie par $s_j = \text{trace}(\beta\alpha^{-j})$ pour $j \geq 0$ est engendrée par f.
   (b) En déduire que l'application de F dans l'éspace vectoriel des suites engendrées par f qui à β associe la suite $s = s(\beta)$ définie par $s_j = \text{trace}(\beta\alpha^{-j})$ pour $j \geq 0$ est un isomorphisme d'espaces vectoriels.

(c) Pour tout entier t, on note $s^{(t)}$ la suite définie par

$$(s^{(t)})_j = s_{tj}.$$

i. Exemple : $f(x) = x^4 + x^3 + 1$. On sait que f est irréductible sur $\mathbb{F}_2$ et que ses racines engendrent $\mathbb{F}_{16}^*$. Soit

$$s = 100010011010111\ldots$$

Quels sont les bits suivants de s ? Calculez le début de $s^{(2)}$, $s^{(3)}$, $s^{(5)}$, et le plus petit polynôme qui les engendre... avec le minimum de calculs et sans faire appel au théorème du cours.

ii. Retour au cas général : montrez que la suite $s^{(t)}$ est engendrée par le polynôme minimal de α^t sur $\mathbb{F}_2$.

iii. Vérifiez sur l'exemple précédent

iv. Toujours l'exemple : d'après ce qui précède, si α est une racine de f, il existe $\beta \in F$ tel que $s = s(\beta)$. Calculez β.