Master CSI 1

Arithmétique 1

Feuille d'exercices n° 5.

$\boxed{1}$ Soit $\mathbb{F}_q$, $q = p^k$. On note σ le Frobenius défini par $\sigma(x) = x^p$. On note Tr la trace.

1. Si $\alpha \in \mathbb{F}_q$ est de degré k, montrez que $\mathrm{Tr}(\alpha)$ est l'opposé du coefficient de X^{k-1} dans le polynôme minimal de α sur $\mathbb{F}_p$.
2. Applications : dans $\mathbb{F}_{2^6}$, α est racine du polynôme primitif $f(X) = X^6 + X + 1$. Calculez $\mathrm{Tr}(1)$, $\mathrm{Tr}(\alpha)$, $\mathrm{Tr}(\alpha^2)$, $\mathrm{Tr}(\alpha^3)$, $\mathrm{Tr}(\alpha^4)$, $\mathrm{Tr}(\alpha^6)$.
3. On définit la norme de $\alpha \in \mathbb{F}_q$ par

$$\mathrm{N}(\alpha) = \prod_{i=0}^{k-1} \sigma^i(\alpha) = \prod_{i=0}^{k-1} \alpha^{p^i}.$$

   (a) Montrez que $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$, que $\mathrm{N}(\sigma(\alpha)) = \mathrm{N}(\alpha)$ et que $\mathrm{N}(\alpha) \in \mathbb{F}_p$.

   (b) Montrez que, si α est de degré k sur $\mathbb{F}_p$, $\mathrm{N}(\alpha)$ est égal au coefficient constant du polynôme minimal de α sur $\mathbb{F}_p$ multiplié par $(-1)^k$.

$\boxed{2}$ Soit $K = \mathbb{F}_q$ un corps fini de caractéristique p et soit $L = \mathbb{F}_{q^2}$. On rappelle 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. Que se passe-t-il si $\alpha \in K$?

$\boxed{3}$ On définit la fonction de Mobius μ sur $\mathbb{N}$ de la manière suivante : $\mu(1) = 1$, $\mu(n) = 0$ si n admet un facteur carré, $\mu(p_1 ... p_k) = (-1)^k$, où p_1, ..., p_k sont des nombres premiers.

1. Montrer que $\sum_{d|n} \mu(d) = 1$ si $n = 1$ et $\sum_{d|n} \mu(d) = 0$ si $n > 1$.
2. Montrer que si $g(n) = \sum_{d|n} f(d)$ on a $f(n) = \sum_{d|n} \mu(d) g(n/d)$.
3. Application : partant de la formule sur $\mathbb{F}_p[X]$ de décomposition :

$$X^{p^n} - X = \prod_{\substack{P \text{ irréductible} \\ \deg(P)|n}} P(X),$$

   on obtient une égalité de fonctions arithmétiques en prenant le degré des polynômes. Donner ainsi une formule pour le nombre de polynômes irréductibles sur $\mathbb{F}_p$ de degré d.