Université de Bordeaux — **Arithmétique – M1MA7W01**
Master 1 CSI — 2013–2014

FEUILLE D'EXERCICES n° 5

Exercice 1 – Combien y a-t-il de polynômes unitaires primitifs de degré 7 sur $\mathbb{F}_5$? Combien d'éléments primitifs dans $\mathbb{F}_{5^7}$?

Exercice 2 –

1) Énumérer les classes cyclotomiques binaires modulo 11.

2) En déduire que le polynôme $1 + X + X^2 + \cdots + X^{10} = (X^{11} - 1)/(X - 1)$ est irréductible sur $\mathbb{F}_2$.

Exercice 3 –

1) Énumérer les classes cyclotomiques ternaires modulo 23.

2) En déduire la forme de la factorisation de $X^{23} - 1$ dans $\mathbb{F}_3[X]$.

3) Quelle est la plus petite extension de $\mathbb{F}_3$ dans laquelle le polynôme $X^{23} - 1$ se factorise entièrement ?

Exercice 4 – Soit $q = p^k$, où p est premier et $k \geqslant 1$. On note $\sigma : x \mapsto x^p$ le Frobenius sur $\mathbb{F}_q$ et $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ la trace.

1) Si $\alpha \in \mathbb{F}_q$ est de degré k, montrer que $\mathrm{Tr}(\alpha)$ est l'opposé du coefficient de X^{k-1} dans le polynôme minimal de α sur $\mathbb{F}_p$.

2)a) On note α la classe de X dans $\mathbb{F}_2[X]/(f)$, où $f = X^6 + X + 1$ est *primitif*.

b) Calculer $\mathrm{Tr}(1)$, $\mathrm{Tr}(\alpha)$, $\mathrm{Tr}\left(\alpha^2\right)$, $\mathrm{Tr}\left(\alpha^3\right)$, $\mathrm{Tr}\left(\alpha^4\right)$, et $\mathrm{Tr}\left(\alpha^6\right)$.

3) On définit la norme de $\alpha \in \mathbb{F}_q$ par $\mathrm{N}(\alpha) := \prod_{0 \leqslant i < k} \sigma^i(\alpha) = \prod_{0 \leqslant i < k} \alpha^{p^i}$.

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

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

Exercice 5 – Soit $K = \mathbb{F}_q$ un corps de caractéristique p et soit $L = \mathbb{F}_{q^2}$.

1) Soit $\alpha \in L$. Montrer que $t = \alpha + \alpha^q$ et $n = \alpha^{q+1}$ sont dans K.

2) Déduire de la question précédente que $X^2 - tX + q \in L[X]$ est en fait à coefficients dans K, et a α pour racine. Quelle est son autre racine ?

3) Montrer que si $\alpha \notin K$, alors $X^2 - tX + n$ est le polynôme minimal de α. Que se passe-t-il quand $\alpha \in K$?