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

# FEUILLE D'EXERCICES n° 6

**Exercice 1** – Soient $p$ un nombre premier et $K$ une extension finie de $\mathbb{F}_p$.

**1)** Soit $b \in K$ tel que $\forall y \in K$, $\mathrm{Tr}(by) = 0$. Montrer que $b = 0$.

**2)** Démontrer que le Frobenius $K \to K$ est surjectif.

**Exercice 2** – Soit $p$ un nombre premier. Soit $P = X^d - a_{d-1}X^{d-1} - \cdots - a_0 \in \mathbb{F}_p[X]$ irréductible. Désignons par $V$ l'espace des suites $(u_n)_{n\geqslant 0} \in \mathbb{F}_p^{\mathbb{N}}$ telles que $u_n = a_{d-1}u_{n-1} + \cdots + a_0u_{n-d}$ pour tout $n \geqq d$. Posons $K = \mathbb{F}_p[X]/\langle P\rangle$ et notons $\alpha$ la classe de $X$ dans $K$.

**1)** Soit $b \in K$ ; on définit la suite $(f(b)_n)_{n\geqslant 0}$ en posant $f(b)_n = \mathrm{Tr}(b\alpha^n)$ pour tout $n \in \mathbb{N}$. Vérifier que $f(b) \in V$.

**2)** Montrer que l'application $f\colon K \to V$ est un isomorphisme de $\mathbb{F}_p$-espaces vectoriels.

**3)** Soit $(u_n)_{n\geqslant 0} \in V$. Montrer que $(u_{pn})_{n\geqslant 0} \in V$.

On suppose maintenant $p = 2$ et $P = X^4 - X - 1$. Considérons la suite $(u_n)_{n\geqslant 0} \in V$ telle que $(u_0, u_1, u_2, u_3) = (1, 0, 0, 0)$.

**4)** Calculer $u_n$ pour tout $n \leqslant 18$. Quelle est la période de la suite $(u_n)$ ?

**5)** Calculer $\mathrm{Tr}(\alpha^n)$ pour tout $n \leqslant 3$, puis déterminer l'élément $b \in K$ tel que $f(b) = (u_n)_{n\geqslant 0}$.

**Exercice 3** – Soient $K$ un corps fini et $a \in K \setminus \{0, 1\}$. Désignons par $C$ le code linéaire de matrice génératrice

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & a & 0 & 1 \end{pmatrix}.$$

Trouver les paramètres de $C$.

**Exercice 4** – Soit $K$ un corps fini. Soient $n$ un entier $\geqslant 1$ et $a \in K^*$. Notons $C$ le code (linéaire) de longueur $n$ défini par $C = \{(c, ac, \cdots, a^{n-1}c) \ ; \ c \in K\}$.

**1)** Quels sont les paramètres de $C$ ?

**2)** À quelle condition sur $n$ et $a$ le code $C$ est-il cyclique ?

**Exercice 5** – Soit $K$ un corps fini. Soit $n$ un entier $\geqslant 2$. On pose

$$C = \{(c_1, \cdots, c_n) \in K^n \colon c_1 + \cdots + c_n = 0\}.$$

**1)** Déterminer les paramètres du code linéaire $C$.

**2)** Vérifier que $C$ est un code cyclique et trouver son polynôme générateur.

**Exercice 6** –

**1)** Montrer qu'il n'existe pas de code $\mathbb{F}_3$-linéaire de paramètres $(5, 3, 3)$. [*Utiliser la borne de Hamming*]

**2)** Montrer qu'il n'existe pas de code $\mathbb{F}_3$-linéaire de paramètres $(5, 2, 4)$. [*Un tel code serait MDS, considérer son dual*]