Université de Bordeaux

Master 1 CSI
4TCY703U - Arithmétique
Feuille 5

Exercice 1. On pose $A = \mathbf{F}_3[Y]/\langle Y^4 + Y - 1\rangle$ et on note α la classe de Y dans A.
(1) Calculer α^{16} et α^{40}.
(2) En déduire que A est un corps.
(3) Trouver le polynôme minimal de $\alpha + 1$ sur $\mathbf{F}_3$.
(4) Quel est le degré de α^{10} sur $\mathbf{F}_3$?

Exercice 2. Soient p un nombre premier, K une extension finie de $\mathbf{F}_p$ et $b \in K$ tel que $(\forall y \in K)\ \mathsf{Tr}(by) = 0$. Montrer que $b = 0$.

Exercice 3. Soit K un corps fini de caractéristique p. Prouver que le Frobenius $K \to K$ est surjectif.

Exercice 4. Soient p un nombre premier et $P(X) = X^d - a_{d-1}X^{d-1} - \cdots - a_0 \in \mathbf{F}_p[X]$ irréductible. Notons V l'espace des suites $(u_n)_{n\geqslant 0} \in \mathbf{F}_p^{\mathbf{N}}$ telles que

$$u_n = a_{d-1}u_{n-1} + \cdots + a_0 u_{n-d}$$

pour tout $n \geqslant d$. Posons $K = \mathbf{F}_p[X]/\langle P(X)\rangle$ et notons α la classe de X dans K.
(1) Soit $b \in K$. On définit la suite $(f(b)_n)_{n\geqslant 0}$ par $f(b)_n = \mathsf{Tr}(b\alpha^n)$ pour tout $n \in \mathbf{N}$. Vérifier que $f(b) \in V$.
(2) En utilisant le résultat de l'exercice 2, montrer que l'application $f\colon K \to V$ est un isomorphisme de $\mathbf{F}_p$-espaces vectoriels.
(3) Soit $(u_n)_{n\geqslant 0} \in V$. Prouver que $(u_{pn})_{n\geqslant 0} \in V$ (on pourra utiliser l'exercice 3).
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 $\mathsf{Tr}(\alpha^n)$ pour tout $n \leqslant 3$, puis déterminer l'élément $b \in K$ tel que $f(b) = (u_n)_{n\geqslant 0}$.

Exercice 5. Soit C un code sur $\mathbf{F}_3$ de longueur 5 et de distance minimale 3. Démontrer que $\#C \leqslant 22$.

Exercice 6. (borne de Singleton). Soit K un corps fini de cardinal q. Soit C un code sur K de longueur n et de distance minimale d.
(1) Montrer que l'application $C \to K^{n-d+1}$ qui à $(c_1, \ldots, c_n)$ associe $(c_d, \ldots, c_n)$ est injective.
(2) En déduire que $\#C \leqslant q^{n-d+1}$.

Exercice 7. Soient K un corps fini et $a \in K^\times$ tel que $a \neq 1$. Désignons par C le code linéaire de matrice génératrice

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & a & 0 & 1 \end{bmatrix}$$

Trouver les paramètres de C.