Université de Limoges
Faculté des Sciences & Techniques
Département de Mathématiques

Année 2010/2011

MASTER 1 - MATHÉMATIQUES
CORPS FINIS

Examen du 05 janvier 2010
– Durée 2h –

Exercice 1

Soit $\mathbb{F}_7$ le corps de Galois à 7 éléments, $\mathbb{M}_2(\mathbb{F}_7)$ l'anneau des matrices 2×2 sur $\mathbb{F}_7$ et

$$A = \left\{ \begin{pmatrix} a & 6b \\ b & a \end{pmatrix} \in \mathbb{M}_2(\mathbb{F}_7) \ / \ (a, b) \in \mathbb{F}_7^2 \right\}.$$

Montrer que A est un corps commutatif dont on donnera le cardinal et les sous-corps.

Exercice 2

Soit dans $\mathbb{F}_2[x]$,

$$f(x) = x^3 + x + 1, \ g(x) = x^3 + x^2 + 1 \text{ et } \ h(x) = x^2 + x + 1.$$

1. Soit α une racine de f dans une extension convenable de $\mathbb{F}_2$ et $K = \mathbb{F}_2[\alpha]$.
   - Montrer que K est un corps et que α est une racine primitive de K.
   - Montrer que g se décompose en facteurs linéaires sur K et donner sa décomposition.
   - Donner une représentation matricielle des éléments de K. En déduire que le seul triplet de $\mathbb{F}_2^3$ vérifiant l'équation $x^3 + y^3 + z^3 + xyz + xz^2 + xy^2 + yz^2 = 0$ est le triplet $(0, 0, 0)$.
   - Soit θ une racine de g dans une extension convenable de $\mathbb{F}_2$. Exhiber un isomorphisme entre K et $\mathbb{F}_2[\theta]$.
2. Soit β une racine de h dans une extension convenable de $\mathbb{F}_2$ et $L = K[\beta]$.
   - Montrer que h est irréductible sur K et en déduire que L est un corps dont on donnera le cardinal.
   - Donner les sous-corps de L.
   - Soit $\gamma = \alpha + \beta$. Montrer que $L = \mathbb{F}_2[\gamma]$ et donner le polynôme minimal de γ sur $\mathbb{F}_2$.

Exercice 3

Soit dans $\mathbb{F}_2[x]$, $f(x) = x^6 + x^4 + x^3 + x^5 + x^2 + x + 1$.
1. Factoriser f sur $\mathbb{F}_2$ (en utilisant l'algorithme de factorisation de Berlekamp).
2. Décrire le corps de décomposition de f sur $\mathbb{F}_2$.

Exercice 4

Donner la décomposition en facteurs irréductibles sur $\mathbb{F}_3$ de $x^7 - x^6 + x^4 + x^3 - x^2 + 1$.