Université de Limoges
Faculté des Sciences & Techniques
Département de Mathématiques

Année 2010/2011

MASTER1–MATHÉMATIQUES
CORPS FINIS

Partiel du 08 novembre 2010
– Durée 2h –

Exercice 1

Donner un système minimal de générateurs du groupe $(\mathbb{Z}/60\mathbb{Z})^\times$.

Exercice 2

Déterminer les polynômes P de $\mathbb{F}_2[x]$ vérifiant :

$$\begin{cases} P(x) \equiv x & (\text{mod } x^2+x+1) \\ P(x) \equiv x^2+1 & (\text{mod } x^3+x+1). \end{cases}$$

Manipulations dans un petit corps

Dans la suite K désignera le corps $\mathbb{F}_3$, $f(x)$ le polynôme x^3-x+1 de $K[x]$, L l'anneau quotient $K[x]/(f(x))$ et α la classe de x dans L.

1. Montrer que f est irréductible sur K et en déduire la nature de L.
2. Donner le cardinal de L et décrire ses éléments.
3. Soit μ_α l'endomorphisme *multiplication par* α dans L et $\mathcal{B} = \{1, \alpha, \alpha^2\}$.
   a. Montrer que $\mathcal{B}$ est une base de L (en tant qu'espace vectoriel sur K).
   b. Donner la matrice A de μ_α relativement à $\mathcal{B}$.
   c. Montrer que, pour tout entier naturel n, on a : $A^{n+3} = A^{n+1} - A^n$.
4. Vérifier que α et $(\alpha-1)$ sont des racines de f dans L. Donner la décomposition de f en éléments irréductibles dans $L[x]$.
5. Montrer que les assertions suivantes sont équivalentes :
   i. $\alpha^{13} = -1$,
   ii. $f(x)$ divise $(x-1)^4x+1$ dans $K[x]$.
6. Montrer que $f(x)$ divise le polynôme $x^5-x^4-x^2+x+1$ dans $K[x]$.
7. En déduire que l'ordre de α est égal à 26.
8. Quel est l'ordre de α^2 ? Justifier.