USTHB
Faculté de mathématiques
1ère Année Master ACC

Année: 2012 – 2013
Module: Corps Finis
04 Juin 2013

Epreuve finale

Exercice 1 (07 pts) Soit

$$f(x) = x^2 - 3 \in \mathbb{F}_7[x].$$

1. Montrer que $f(x)$ est irréductible dans $\mathbb{F}_7[x]$.
2. Décrire le corps $\mathbb{F}_{49}$ obtenu à partir du polynôme $f(x)$. (Donner une base de $\mathbb{F}_{49}/\mathbb{F}_7$)
3. Soit α une racine de $f(x)$ dans $\overline{\mathbb{F}_7}$. Quels sont les ordres possibles de α dans le groupe multiplicatif $\mathbb{F}_{49}^*$? Combien y a-t-il de générateurs dans $\mathbb{F}_{49}^*$?
4. Le polynôme $f(x)$ est-il primitif ? Quel est son ordre ?
5. Soit $\beta = \alpha + 1$. Quel est l'ordre de β dans le groupe multiplicatif $\mathbb{F}_{49}^*$? En déduire un polynôme primitif de $\mathbb{F}_7[x]$ de degré 2.

Exercice 2 (05 pts) Soit

$$f(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$$

1. Vérifier que $f(x) = (x^2 + x + 1)^3 (x^4 + x + 1)$.
2. Déterminer $ord(x^2 + x + 1)$. En déduire $ord\left((x^2 + x + 1)^3\right)$.
3. Déterminer $ord(x^4 + x + 1)$. En déduire $ord(f)$.
4. Est-ce que $ord(f)$ divise $2^{10} - 1$? Pourquoi ?

Exercice 3 (07 pts) .

1. Factoriser le polynôme

$$f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

dans $\mathbb{F}_2[x]$ en utilisant l'algorithme de Berlekamp.

2. Retrouver le résultat en considérant la factorisation du polynôme $x^8 - x$ dans $\mathbb{F}_2[x]$.

Exercice 4 (03 pts) Soit p un nombre premier impair, et soit $a \in \mathbb{F}_p^*$. Montrer que a est un carré dans $\mathbb{F}_p^*$ si et seulement si $a^{(p-1)/2} = 1$. En déduire les solutions de l'équation $x^6 = 1$ dans $\mathbb{F}_{13}$.