Université de Paris 7 **Exercices du 5-10-2007** **agreg 2008 (F.Han[1])**

Exercice I:

1) Donner le nombre de solutions de l'équation $x^3 - 1 = 0$ dans $\mathbb{F}_5$, $\mathbb{F}_{25}$, $\mathbb{F}_{5^3}$?

2) Même question dans $\mathbb{F}_{5^r}$.

Exercice II:

1) a) Soit $f \in \mathbb{F}_3[X]$. Montrer que si 0 est racine double de f et de f', alors 0 est racine triple de f.

b) Est ce vrai pour $f \in \mathbb{F}_4[X]$?

2) On considère le polynôme $f = X^5 - X^2 - X - 1$ de $\mathbb{F}_3[X]$.

a) Combien f a-t-il de racines dans $\mathbb{F}_3$? Dans $\mathbb{F}_9$?

b) Factoriser f dans $\mathbb{F}_3[X]$

c) Factoriser f dans $\mathbb{F}_9[X]$. (On exprimera tout élément de $\mathbb{F}_9$ de manière "réduite")

d) Factoriser f dans $\mathbb{F}_{27}[X]$. (On exprimera tout élément de $\mathbb{F}_{27}$ de manière "réduite")

Exercice III:

1) Rappeler la définition de $\Phi_8(x) \in \mathbb{C}[x]$ (le polynôme cyclotomique associé aux racines 8-ièmes de l'unité), et calculez[2] le. Est il irréductible dans $\mathbb{Q}[x]$?

2) Etudier le groupe multiplicatif $(\mathbb{Z}/8\mathbb{Z})^\times$ de l'anneau $\mathbb{Z}/8\mathbb{Z}$.

3) Soit p un nombre premier, et α une racine de Φ_8 dans une extension de $\mathbb{Z}/p\mathbb{Z}$.

a) Quel est l'ordre de α?

b) Etudier l'action du morphisme de Frobénius sur α.

c) Conclure que pour tout nombre premier Φ_8 est réductible dans $\mathbb{Z}/p\mathbb{Z}[x]$, et qu'il y est produit de 2 carrés de polynômes irréductibles de $\mathbb{Z}/p\mathbb{Z}[x]$

4) Quel est le corps de décomposition de Φ_8

Exercice IV:

Trouver les racines multiples du polynôme

$$f(X) = X^7 + X^5 + X^4 - X^3 - X^2 - X + 1$$

de $\mathbb{F}_3[X]$ dans le corps de décomposition de f.

Exercice V: Fonction de Möbius

On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par $\mu(1) = 1$, $\mu(n) = 0$ si n a un facteur multiple, et $\mu(p_1 \dots p_r) = (-1)^r$ si $p_1, \dots, p_r$ sont des premiers distincts.

1) Pour $f : \mathbb{N}^* \to A$ où $(A, +)$ est un groupe abélien. On pose $g(n) = \sum_{d|n} f(d)$. Montrer que

$$f(n) = \sum_{d|n} \mu(n/d).g(d)$$

Exercice VI: Nombre de polynôme irréductibles sur $\mathbb{F}_q$

(Cf D. Perrin "cours d'algèbre" ExIII.4) Soit $I(n, q)$ le nombre de polynômes irréductibles, unitaires, de degré n de $\mathbb{F}_q[x]$. ($q = p^k$ où p est un nombre premier)

1) Montrer[3] que $\sum_{d|n} d.I(d, q) = q^n$

2) En déduire la formule: $I(n, q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$

3) Montrer que $nI(n, q)$ est le nombre d'éléments de $\mathbb{F}_q^n$ qui ne sont dans aucun sous-corps propre de $\mathbb{F}_q$ contenant $\mathbb{F}_q$

[1] http://www.math.jussieu.fr/~han/agreg

[2] On peut montrer qu'ils sont tous dans $\mathbb{Z}[x]$

[3] Etudier les facteurs de $X^{q^n} - X$

Exercice VII:

Soit k un corps commutatif de caractéristique $p \neq 0$, et $\mathbb{F}_p$ son sous-corps premier, et $a \in k^*$.

1) Exprimer les racines du polynôme $f \in k[x]$ tel que $f(x) = x^p - x - a$ en fonction de l'une d'entre elles $\alpha \in K$, où K est un surcorps convenable de k.

2) On suppose qu'il existe un polynôme irréductible $d \in k[x]$ de degré $r \geq 2$ qui divise f.

a) Montrer qu'il existe $s \in \mathbb{F}_p$ tel que $d(x + s) = d(x)$.

b) En déduire que $r = p$.

3) a) Trouver une condition nécéssaire et suffisante pour que f soit irréductible sur k.

b) Montrer que si $f(x)$ est irréductible alors $f_t(x) = x^p - x - ta$ où $t \in \mathbb{F}_p$, $t \neq 0$ est aussi irréductible sur k.