ÉNS Lyon — Rappels d'algèbre
Préparation à l'agrégation — 2009-2010

Feuille d'exercices n°11

Exercice 1

Soient L/K une extension finie de corps et α un élément de K. Montrer que le polynôme caractéristique de la multiplication par α, vue comme endomorphisme K-linéaire de L, est un polynôme non nul à coefficients dans K qui annule α.

Exercice 2

Soit K un corps fini. Montrer que toute fonction de K dans lui-même est polynomiale.

Exercice 3

Soit K un corps. Déterminer les polynômes à coefficients dans K de dérivée nulle.

Exercice 4

Soient n un entier relatif non nul et p un diviseur premier de $n^4 - n^2 + 1$; montrer que p est congru à 1 modulo 12.

Exercice 5

Répéter dix fois : « $\mathbf{F}_4$ n'est pas $\mathbf{Z}/4\mathbf{Z}$ ».

Exercice 6

Combien le groupe $\mathbf{F}_q^\times$ possède-t-il de générateurs ?

Exercice 7

Soient p un nombre premier et n un entier strictement positif ; montrer que $\mathbf{F}_{p^n}^\times$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbf{F}_p)$.

Exercice 8

Soit p un nombre premier.

1. Combien y a-t-il de polynômes unitaires réductibles de degré 2 dans $\mathbf{F}_p[X]$? En déduire le nombre de polynômes unitaires irréductibles de degré 2 dans $\mathbf{F}_p[X]$. Déterminer ces polynômes pour $p = 2$ et pour $p = 3$.

2. Montrer qu'il existe $\frac{p(p^2-1)}{3}$ polynômes unitaires irréductibles de degré 3 dans $\mathbf{F}_p[X]$. Déterminer ces polynômes pour $p = 2$.
3. Déterminer les polynômes unitaires irréductibles de degré 4 dans $\mathbf{F}_2[X]$.

Exercice 9

Expliciter un isomorphisme entre les corps finis :

$$\mathbf{F}_2[X]/(X^3 + X + 1) \text{ et } \mathbf{F}_2[Y]/(Y^3 + Y^2 + 1).$$

Exercice 10

Construire les corps finis suivants :

1. $\mathbf{F}_4$, $\mathbf{F}_8$ et $\mathbf{F}_{16}$;
2. $\mathbf{F}_9$, $\mathbf{F}_{25}$ et $\mathbf{F}_{49}$.

Dans chacun des cas, donner un générateur du groupe multiplicatif et déterminer les sous-corps.

Exercice 11

Soient p un nombre premier, n un entier strictement positif, $q = p^n$ et $\mathbf{F}_q$ un corps fini à q éléments.

1. Soit K un sous-corps de $\mathbf{F}_q$. Montrer que $\operatorname{card} K = p^d$ avec $d|n$.
2. Soit $\varphi : \mathbf{F}_q \to \mathbf{F}_q$ défini par $\varphi(x) = x^p$. Montrer que φ est un automorphisme $\mathbf{F}_p$-linéaire du corps $\mathbf{F}_q$.
3. Montrer que K est l'ensemble des points fixes de φ^d.
4. Réciproquement, montrer que $K_d = \{x \in \mathbf{F}_q; \varphi^d(x) = x\}$ est un sous-corps de $\mathbf{F}_q$ de cardinal p^d. Montrer que c'est le seul.

Exercice 12

On rappelle que le polynôme $P(X) = X^4 + 1$ est irréductible sur $\mathbf{Z}$. Le but de cet exercice est de montrer qu'il est réductible dans tout corps fini.

1. Écrire la décomposition de P en facteurs irréductibles dans $\mathbf{F}_2[X]$.

Dans toute la suite, p désigne un nombre premier impair.

2. (a) Donner toutes les manières possibles d'écrire P comme produit de deux polynômes de degré 2 dans $\mathbf{C}[X]$.
   (b) Montrer qu'au moins l'un des des trois éléments -1, 2, -2 est un carré dans $\mathbf{F}_p$.
   (c) En déduire que P est réductible dans $\mathbf{F}_p[X]$.

3. (a) Montrer que P est réductible si et seulement si il possède une racine dans $\mathbf{F}_{p^2}$.

   (b) Montrer que P possède une racine dans $\mathbf{F}_{p^2}$ si et seulement si 8 divise $p^2 - 1$.

   (c) En déduire que P est réductible dans $\mathbf{F}_p[X]$.

Exercice 13

L'algèbre des quaternions $\mathbf{H}$ est la $\mathbf{R}$-algèbre $\mathbf{R} \oplus \mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k$ munie de la loi d'addition évidente, de la loi de multiplication $\mathbf{R}$-bilinéaire vérifiant $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$ et admettant 1 comme élément unité.

1. Soit $u = x + yi + zj + tk \in \mathbf{H}$. Que vaut le déterminant de l'endomorphisme $v \mapsto uv$ de $\mathbf{H}$?
2. En déduire que tout élément non nul de $\mathbf{H}$ est inversible dans $\mathbf{H}$.
3. Trouver les éléments u de $\mathbf{H}$ vérifiant $u^2 = -1$. En déduire qu'il existe une infinité de morphismes de $\mathbf{R}$-algèbres de $\mathbf{C}$ dans $\mathbf{H}$.