UNIVERSITÉ DE RENNES 1

Préparation à l'agrégation

Théorie des corps (feuille 2)

Exercice 1

Soit q une puissance d'un nombre premier impair. Le but de cet exercice est de montrer que 2 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv \pm 1 \pmod 8$. Pour cela, on va distinguer deux cas, selon que -1 est un carré ou non.

Remarquez le rôle joué dans cet exercice par des racines de l'unité bien choisies.

Comme le groupe $\mathbb{F}_q^\times$ est cyclique, on fixe un isomorphisme $\theta : \mathbb{F}_q^\times \to \mathbb{Z}/(q-1)\mathbb{Z}$.

(a) Quels sont les éléments d'ordre 2 dans $\mathbb{F}_q^\times$? dans $\mathbb{Z}/(q-1)\mathbb{Z}$? En déduire $\theta(-1)$.

(b) Quels sont les multiples de 2 dans $\mathbb{Z}/(q-1)\mathbb{Z}$?

(c) En déduire que -1 est un carré dans $\mathbb{F}_q^\times$ si et seulement si $q \equiv 1 \pmod 4$.

(d) Pour quels q existe-t-il un $\zeta \in \mathbb{F}_q^\times$ d'ordre 8 ? (On pourra considérer $\theta(\zeta)$.)

(e) Supposons qu'il existe un $\zeta \in \mathbb{F}_q^\times$ d'ordre 8. En considérant $\zeta + \zeta^{-1}$, montrer que 2 est un carré dans $\mathbb{F}_q$.

(f) Supposons que -1 et 2 sont des carrés dans $\mathbb{F}_q$. Montrer que $\mathbb{F}_q^\times$ contient un élément d'ordre 8. (On pourra donner une formule explicite.)

(g) En déduire que si -1 est un carré dans $\mathbb{F}_q$, alors 2 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1 \pmod 8$.

On suppose désormais que -1 n'est pas un carré dans $\mathbb{F}_q$.

(h) Montrer que 2 est un carré dans $\mathbb{F}_q$ si et seulement si -2 n'est pas un carré dans $\mathbb{F}_q$.

(i) Montrer que $\mathbb{F}_{q^2}$ contient un élément ζ d'ordre 8.

(j) Calculer $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\zeta)$. (On pourra utiliser le morphisme de Frobenius.)

(k) En déduire que 2 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv -1 \pmod 8$.

Exercice 2

Soit k un corps fini de cardinal q, et soit L/k une extension de degré d. Soit $\varphi : L \to L$, $x \mapsto x^q$.

(a) Montrer que le polynôme $X^d - 1$ annule φ.

(b) Soit $P(X) \in k[X]$ tel que $P(\varphi) = 0$. Montrer qu'on ne peut pas avoir $\deg P < d$. (Indication : remarquer que $P(\varphi)(x)$, pour $x \in L$, s'écrit comme un polynôme en x.)

(c) En déduire que le polynôme minimal de φ, comme application k-linéaire, est $X^d - 1$.

(d) En déduire l'ordre de φ dans le groupe des automorphismes k-linéaires de L.

(e) Montrer que les endomorphismes φ^i, $0 \leqslant i < d$, sont linéairement indépendants sur k.

(f) Soit $x \in L$ un vecteur cyclique pour φ. Montrer que les $\varphi^i(x)$, $0 \leqslant i < d$, forment une k-base de L.

(g) Soit d' un diviseur de d. Montrer que l'ensemble K des points fixes de $\varphi^{d'}$ est un sous-corps de L. Si θ est un générateur de $L^\times$, montrer qu'il contient $\prod_{i=0}^{\frac{d}{d'}-1} \varphi^{d'i}(\theta)$ et déterminer son cardinal.

Exercice 3

Soit k un corps de caractéristique $p > 0$. On considère le polynôme $P(X) = X^p - X - a$, pour $a \in k$.

(a) Dans le cas $a = 0$, déterminer les racines de P dans k.

(b) Soit L une extension de k. Montrer que si P a une racine dans L, alors il est scindé à racines simples sur L.

(c) Supposons que P n'a pas de racine dans k. Soit Q un facteur irréductible de P sur k, soit L un corps de rupture de Q, et soit $x \in L$ tel que $Q(x) = 0$. Montrer que $\mathrm{Tr}_{L/k}(x) - (\deg Q)x \in \mathbb{F}_p$. (Indication : que peut-on dire des autres racines de Q ?) En déduire que P est irréductible sur k.

On peut montrer que toute extension de degré p de k, galoisienne de groupe de Galois cyclique, est de la forme précédente. On va le faire dans le cas particulier où les corps sont finis.

Soit L une extension de k de degré p. On suppose que L est un corps fini. Soit $q := |k|$, et soit $\varphi : L \to L$, $x \mapsto x^q$.

(d) Montrer que $\sum_{i=0}^{p-1} \varphi^i \neq 0$ (cf. l'exercice précédent).

(e) Soit $x \in L$ tel que $\mathrm{Tr}_{L/k}(x) \neq 0$. Posons

$$\alpha := \frac{1}{\mathrm{Tr}_{L/k}(x)} \sum_{i=0}^{p-1} i\varphi^i(x).$$

Montrer que $\alpha - \varphi(\alpha) = 1$.

(f) Soit Q le polynôme minimal de α sur k. Montrer que les racines de Q sont les $\alpha + x$, $x \in \mathbb{F}_p$, et que $L = k[\alpha]$.

(g) Montrer que $Q(X - \alpha) = X^p - X$.

(h) En déduire que $Q(X) = X^p - X + \alpha^p$ et $\alpha^p \in k$.