TD n°10 : Corps finis, extensions normales

Dans toute la feuille, p est un nombre premier et $q = p^n$. On notera $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ un corps à p éléments.

Exercice 1. [Sous-corps d'un corps fini]

1. Soit $\mathbf{K}$ un sous-corps de $\mathbf{F}_q$. Montrer qu'il existe d divisant n tel que $\mathbf{K} \sim \mathbf{F}_{p^d}$.
2. Réciproquement, étant donné d un diviseur de n montrer qu'il existe un unique sous-corps de $\mathbf{F}_q$ isomorphe à $\mathbf{F}_{p^d}$.
3. Dessiner un diagramme montrant les inclusions possibles entre $\mathbf{F}_2$, $\mathbf{F}_4$, $\mathbf{F}_8$, $\mathbf{F}_{16}$, $\mathbf{F}_{32}$, $\mathbf{F}_{64}$, $\mathbf{F}_{128}$ et $\mathbf{F}_{256}$.

Exercice 2. [Automorphismes des corps finis]

1. Soit L/K une extension de corps. On note $Aut(L/K)$ l'ensemble des automorphismes de L dont la restriction à K est l'identité. Montrer que $Aut(L/K)$ est un groupe.
2. Montrer que si l'extension L/K est finie et monogène, alors le groupe $Aut(L/K)$ est fini de cardinal majoré par le degré d'extension $[L : K]$.
3. Soient p un nombre premier et A un anneau de caractéristique p. Montrer que l'application
$$\begin{aligned} Frob_A : A &\to A \\ x &\mapsto x^p \end{aligned}$$
est un endomorphisme de l'anneau A. On l'appelle l'*endomorphisme de Frobenius* de A.
4. Montrer que pour tout $n \geq 1$, $Frob_{\mathbf{F}_{p^n}}$ est un élément de $Aut(\mathbf{F}_{p^n}/\mathbf{F}_p)$.
5. Montrer que le groupe $Aut(\mathbf{F}_{p^n}/\mathbf{F}_p)$ est cyclique d'ordre n, dont $Frob_{\mathbf{F}_{p^n}}$ est un générateur.
6. Soit $\sigma \in Aut(\mathbf{F}_{p^n}/\mathbf{F}_p)$ un élément d'ordre k. Montrer que les points fixes de σ est un sous-corps de $\mathbf{F}_{p^n}$ isomorphe à $\mathbf{F}_{p^{n/k}}$

Exercice 3. [Polynômes irréductibles sur $\mathbb{F}_p$]

1. Montrer que $X^q - X$ est scindé à racines simples dans $\mathbb{F}_q$.
2. Soit P un facteur irréductible de $X^q - X$. Montrer que le degré de P divise n.
3. Réciproquement, soit P un polynôme unitaire irréductible dans $\mathbb{F}_p[X]$ dont le degré divise n. Montrer que P est un facteur simple de $X^q - X$.
4. Pour tout $d \in \mathbf{N}$ on note $\mathcal{I}(p, d)$ l'ensemble des polynômes unitaires irréductibles dans $\mathbf{F}_p[X]$ de degré d. Montrer que dans $\mathbf{F}_p[X]$ on a
$$X^q - X = \prod_{d|n} \prod_{P \in \mathcal{I}(p,d)} P$$
5. On note $I(p, d)$ le cardinal de $\mathcal{I}(p, d)$. Montrer que $p^n = \sum_{d|n} I(p, d)$. En déduire que l'ensemble $\mathcal{I}(p, d)$ est non vide.
6. Montrer que $\frac{p^n - p^{\lfloor n/2 \rfloor + 1}}{n} \leq I(n, p) \leq \frac{p^n}{n}$ En déduire qu'un polynôme unitaire de degré n "assez grand" choisi au hasard a au moins une chance sur n d'être irréductible.

Exercice 4. [Clôture algébrique des corps finis]
Soit p un nombre premier. Soit $\bar{\mathbf{F}}_p$ la réunion de la chaîne croissante (cf. Exercice 1)

$$\mathbf{F}_p \subset \mathbf{F}_{p^2} \subset \mathbf{F}_{p^6} \subset \cdots \subset \mathbf{F}_{p^{n!}} \subset \cdots$$

1. Montrer que $\bar{\mathbf{F}}_p$ est un corps, qui est une extension algébrique de $\mathbf{F}_p$.
2. Montrer que pour tout $n \geq 1$, il existe un unique plongement $\mathbf{F}_{p^n} \to \bar{\mathbf{F}}_p$.
3. Montrer que $\bar{\mathbf{F}}_p$ est une clôture algébrique de $\mathbf{F}_p$.

Exercice 5. Les extensions ci-dessous sont-elles normales ?

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$, $\mathbb{Q}(j,\sqrt{3})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2},j)/\mathbb{Q}$, $\mathbb{Q}(\cos(\frac{2\pi}{3})/\mathbb{Q}$, $\mathbb{Q}(e^{\frac{2i\pi}{n}})/\mathbb{Q}$ pour $n \in \mathbb{N}$.

Exercice 6.
1. Soit K une extension algébrique de $\mathbf{F}_p$. Montrer que $K/\mathbf{F}_p$ est normale.
2. Soit K un corps de caractéristique $p > 0$. Montrer que $K^p = \{x^p \mid x \in K\}$ est un sous-corps de K et que K/K^p est normale.
3. Soit n un entier non divisible par p, $L = \mathbf{F}_p(Y)$ et $K = \mathbf{F}_p(Y^n)$. Montrer que L/K est normale si et seulement si $p \equiv 1 \ (mod\ n)$.

Exercice 7. [Corps parfait]
Soit K un corps et $P \in K[X]$.
1. Montrer que si $car(K) = 0$, $P' = 0$ si et seulement si P est constant.
2. Montrer que si K est de caractéristique $p > 0$, alors $P' = 0$ si et seulement s'il existe $Q \in K[X]$ tel que $P = Q(X^p)$.
3. Une extension L/K est *séparable* si c'est une extension algébrique et que le polynôme minimal sur K de tout élément dans L admet des racines distinctes dans L. Un corps K est dit *parfait* si toute extension finie de K est séparable.
   (a) Montrer qu'un corps algébriquement clos est parfait.
   (b) Montrer qu'un corps de caractéristique nulle est parfait.
   (c) Montrer qu'un corps de caractéristique positive est parfait si et seulement si l'endomorphisme de Frobenius (cf. Exercice 2) est un isomorphisme.
   (d) Montrer qu'un corps fini est parfait.