4. Corps finis

Exercice 4.1 (Rappel de cours) Soit K un corps fini à q éléments.

1. Montrer qu'il existe un nombre premier p et un entier $n \geq 1$ tels que $q = p^n$.
2. Montrer que :
$$X^q - X = \prod_{x \in K} (X - x).$$
En déduire que K est un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.
3. Soit σ l'automorphisme de Frobenius sur K, *i.e.* $\sigma(x) = x^p$ pour tout $x \in K$. Montrer que
$$K^{\langle\sigma\rangle} = \mathbb{F}_p$$
En déduire que K est une extension galoisienne de $\mathbb{F}_p$ et que $\mathrm{Gal}(K/\mathbb{F}_p) = \langle\sigma\rangle$.

Exercice 4.2 Soit K un corps fini à q éléments de caractéristique p impair.

1. Montrer que l'application
$$\begin{array}{rccc} \varphi & : & K^\times & \to & K^\times \\ & & x & \mapsto & x^2 \end{array}$$
est un morphisme de groupes et que $\mathrm{Im}\varphi$ est d'indice 2 dans $K^\times$.
2. Soit $x \in K^\times$; montrer que x est un carré dans K si et seulement si $x^{(q-1)/2} = 1$.
3. Montrer que -1 est un carré dans K si et seulement si $q \equiv 1 \pmod 4$.
4. a) Soit L un corps contenant K sur lequel $X^4 + 1$ admet une racine α. Vérifier que :
$$\left(\alpha + \alpha^{-1}\right)^2 = 2.$$
b) En déduire que 2 est un carré dans K si et seulement si $q \equiv \pm 1 \pmod 8$.

Exercice 4.3

1. Factoriser $X^4 + 1$ sur $\mathbb{F}_p$ (avec p nombre premier). Distinguer les cas : $p = 2$, $p \equiv 1 \pmod 8$, $p \equiv -3 \pmod 8$, $p \equiv -1$ ou $3 \pmod 8$ et on utilisera l'exercice 4.2.
2. Montrer que $X^4 + 1$ est irréductible sur $\mathbb{Q}$.

Exercice 4.4 On considère le polynôme de $\mathbb{Z}[X]$ suivant :
$$Q(X) = X^9 + 9X^8 - X^3 + 3X^2 - 3X + 11.$$
Soit p un nombre premier, on notera par la suite $\overline{Q}_p$ la réduction de Q modulo p.

1. Montrer que $X^3 - X - 1$ est irréductible dans $\mathbb{F}_3[X]$.
2. Décomposer $\overline{Q}_3$ en produit de polynômes irréductibles de $\mathbb{F}_3[X]$.
3. Soit $\alpha \in \bar{\mathbb{F}}_2$ une racine de $X^4 + X + 1$ où $\bar{\mathbb{F}}_2$ désigne une clôture algébrique de $\mathbb{F}_2$. Décrire l'orbite
$$\{F^i(\alpha),\ i \geq 0\}$$
où F désigne l'automorphisme de Frobenius de $\bar{\mathbb{F}}_2/\mathbb{F}_2$. En déduire que $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

4. Décomposer $\overline{Q}_2$ en produit de facteurs irréductibles de $\mathbb{F}_2[X]$.
5. Montrer que Q est irréductible sur $\mathbb{Q}$.

Exercice 4.5 Soient p un nombre premier et $\bar{F}_p$ une clôture algébrique de $\mathbb{F}_p$. Soit n un entier non divisible par p.

1. Montrer que les racines n-ièmes de l'unité forment un sous-groupe cyclique U_n d'ordre n du groupe multiplicatif $\bar{F}_p^*$.
2. Montrer que si ξ est une racine primitive n-ième de l'unité (c'est-à-dire un générateur de U_n alors les racines primtives n-ième de l'unité sont les ξ^r pour $1 \leq r \leq n$ et r premier avec n. Notons U_n^* l'ensemble des racines primitives n-ièmes de l'unité.
3. On appelle polynôme cyclotomique d'indice n sur $\mathbb{F}_p$ le polynôme unitaire
$$\Phi_{n,\mathbb{F}_p} = \prod_{\xi \in U_n^*} (X_\xi).$$
Montrer que
$$X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{F}_p}.$$
4. Soit π la projection de $\mathbb{Z}$ sur $\mathbb{F}_p$. Montrer par récurrence que
$$\Phi_{n,\mathbb{F}_p} = \pi(\Phi_{n,\mathbb{Q}})$$
.
5. Montrer que $\Phi_{n,\mathbb{F}_p}$ est réductible sur $\mathbb{F}_p$ si et seulement s'il existe $m \leq \phi(n)/2$ tel que $\Phi_{n,\mathbb{F}_p}$ ait une racine dans $\mathbb{F}_{p^m}$.
6. En déduire que $\Phi_{n,\mathbb{F}_p}$ est irréductible sur $\mathbb{F}_p$ si et seulement si $\bar{p}$ est d'ordre $\phi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^*$.
7. Montrer que pour tout $p \neq 2$, $\Phi_{8,\mathbb{F}_p}$ est réductible sur $\mathbb{F}_p$.

Exercice 4.6 Soit p un nombre premier et K un corps fini de caractéristique différente de p.

1. Soit P un facteur irréductible dans $K[X]$ du polynôme
$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1.$$
Considérons le corps $L = K[X]/(P)$ et soit $\alpha = \overline{X}$ la classe de X dans L.
Montrer que α est d'ordre p dans $L^\times$ et en déduire que :
$$\mathrm{card}(K)^d \equiv 1 \pmod{p}$$
où $d = \deg P$.
2. On suppose que $\overline{\mathrm{card}(K)}$ engendre le groupe $\mathbb{F}_p^\times$. Montrer que Φ_p est irréductible sur K.
3. En déduire que si q est un nombre premier tel que $\overline{q}$ engendre $\mathbb{F}_p^\times$, alors Φ_p est irréductible sur $\mathbb{F}_q$.
4. Soient p et q deux nombres premiers. On suppose que $q \neq 2$, $p \equiv -1 \pmod 3$ et que $\overline{q}$ engendre $\mathbb{F}_p^\times$. Montrer que $X^{p+1} - X + q$ est irréductible sur $\mathbb{Q}$. (Indication : réduire modulo q et modulo 2 et utiliser la question précédente.)
Application : Montrer que $X^{18} - X + 3$ est irréductible sur $\mathbb{Q}$.