FEUILLE D'EXERCICES 5

Dans toute cette feuille, p désigne un nombre premier et $q := p^\alpha$ avec $\alpha \geq 1$.

A) Généralités sur les corps finis

1. Soit $\mathbb{A}$ un anneau commutatif unitaire intègre de caractéristique p et soit $n \geq 1$. Montrer que :
$$\forall x, y \in \mathbb{A}, \quad (x+y)^{p^n} = x^{p^n} + y^{p^n}.$$
Que dire si $\mathbb{A} = \mathbb{F}_{p^n}$?
2. On note $(\mathbb{F}_q^*)^2$ l'ensemble des éléments de $\mathbb{F}_q^*$ qui sont des carrés dans ce corps.
   (a) Si $p = 2$, montrer que $(\mathbb{F}_q^*)^2 = \mathbb{F}_q^*$.
   (b) Si $p \neq 2$, montrer que $|(\mathbb{F}_q^*)^2| = \frac{q-1}{2}$.
   (c) On suppose que p impair ; montrer que $a \in \mathbb{F}_q^*$ est un carré si et seulement si $a^{\frac{q-1}{2}} = 1$. En déduire que dans ce cas $\mathbb{F}_p[X]/(X^2+1)$ est un corps si et seulement si $p \equiv 3[4]$.
3. Quels sont les sous–corps de $\mathbb{F}_{4096}$? Décrire les injections existant entre ces derniers.
4. Déterminer une C.N.S sur n pour que l'idéal (n, X) soit premier dans $\mathbb{Z}[X]$. Même question concernant la maximalité.

B) Polynômes sur les corps finis

1. Le polynôme $X^4 + X^2 + 1$ est–il irréductible sur $\mathbb{F}_2$?
2. Dresser la liste des polynômes irréductibles de degré 3 sur $\mathbb{F}_3$.
3. Montrer que l'anneau $\mathbb{F}_2[X]/(X^2+X+1)$ est un corps isomorphe à $\mathbb{F}_4$. En déduire les tables d'addition et de multiplication ainsi qu'une $\mathbb{F}_2$–base de ce dernier corps . Quels sont les générateurs de $\mathbb{F}_4^\times$?
4. Que dire de $\mathbb{F}_p[X]/(X^2+X+1)$ avec $p = 3, 5$?
5. Pour $n \geq 1$ on note $A(n,q)$ l'ensemble des polynômes de degré n irréductibles sur $\mathbb{F}_q$. Fixons un entier $n \geq 1$.
   (a) Soit $d|n$ et soit $P \in A(d,q)$; montrer que $\mathbb{F}_q[X]/(P)$ est un corps isomorphe à $\mathbb{F}_{q^d}$. En déduire que si x est la classe de X dans $\mathbb{F}_q[X]/(P)$ on a $x^{q^n} = x$.
   (b) Montrer que l'on a dans $\mathbb{F}_{q^n}[X]$ l'égalité suivante :
$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P.$$
6. Justifier pourquoi $\mathbb{F}_3[X]/(X^2+2X+2)$ et $\mathbb{F}_3[X]/(X^2+1)$ sont des corps isomorphes. Expliciter un isomorphisme entre ces deux corps.