Algèbre et codage
TD 02

Exercice 1. Soit K un corps commutatif. Montrer que l'anneau K[X] est principal.

Exercice 2. Soit P un polynôme de K[X]. Le groupe des éléments inversibles de $K[X]/(P)$ est formé des classes des polynômes qui sont premiers avec P.

Exercice 3. ***Critère d'Eisenstein.*** *Soit* $P(X) = \sum_{0 \leqslant k \leqslant n} a_k X^k \in \mathbb{Z}[X]$. *Le polynôme P est irréductible dans* $\mathbb{Q}[X]$ *dans la circonstance suivante : il existe un nombre premier p qui ne divise pas* a_n, *divise tous les autres coefficients de P et est tel que* p^2 *ne divise pas* a_0. *Si, de plus.* $c(P) = 1$. *alors P est irréductible dans* $\mathbb{Z}[X]$.

1. Déterminer les polynômes irréductibles de degré $\leqslant 4$ de $\mathbb{F}\ [X]$.
2. Montrer que $X^5 + 21X^2 - 63$ est irréductible dans $\mathbb{Z}[X]$.
3. Décomposer $X^n - 1$ en produit de facteurs irréductibles dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$ pour $n = 3, 7$.

Exercice 4. Soient K un corps fini d'ordre q, g un générateur de K^* et $a \in K^*$. Donner un test pour déterminer si a est un carré ou non dans K. Si oui, montrer comment calculer simplement une racine carré de a dans le cas où $q = 3[4]$.

Exercice 5. Parmi les polynômes suivants, lesquels sont irréductibles dans $\mathbb{Z}[X]$, dans $\mathbb{Q}[X]$, dans $\mathbb{F}_p[X]$.

$$X^4 - 2x^2 + 4, \quad X^4 + 1, \quad X^4 + 4x^2 + 4.$$

Indication : *Soit g un générateur de G. Posons* $a = g^n, b = g^m, ab = g^{n+m}$. *L'un des 3 nombres* $n, m, m + n$ *est nécessairement pair et la puissance de g correspondante est un carré.*

Exercice 6. Par les polynômes $f(x) = x^2 + x - 1$ et $g(x) = x^3 - x + 1$, construire un corps fini contient 4, 8, 9, et 27 éléments. Trouver les tableaux de multiplication des corps de 4 et 9 éléments.

Exercice 7. Soit $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in \mathbb{Z}[X]$. Supposons que $f(0)$ et $f(1)$ sont des entiers impaire. Montrer que $f(X)$ n'admet aucun racine entier.

Exercice 8. Soit $\mathbb{F}_q$ un corps fini. Évaluer la somme et le produit des éléments non nuls de $\mathbb{F}_q$.