

Algèbre et codage TD 02

Exercice 1. 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 2. Critère d'Eisenstein. Soit $F(X) = \sum_{0 \leq k \leq n} a_k X^k \in \mathbb{Z}[X]$. F est irréductible dans $\mathbb{Q}[X]$ s'il existe un nombre premier p qui ne divise pas a_n et divise tous les autres coefficients de F , et p^2 ne divise pas a_0 . Si, de plus F soit primitifs (i.e. à coefficients premiers entre eux) alors F est irréductible dans $\mathbb{Z}[X]$.

1. Déterminer les polynômes irréductibles de degré ≤ 4 de $\mathbb{F}_2[X]$.
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 3. 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 4. 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 5. 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 6. Soit $f(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in \mathbb{Z}[X]$. Supposons que $f(0)$ et $f(1)$ sont des entiers impaire. Montrer que $f(X)$ n'admet aucun racine entier.

Exercice 7. Soit $\mathbb{Q}_q$ un corps fini. Évaluer la somme et le produit des éléments non nuls de $\mathbb{F}_q$.