UNIVERSITÉ DE RENNES 1

Théorie des nombres

Devoir maison

Exercice 1.

Soit $f = X^3 + X + 1 \in F_5[X]$. Soit $K = \mathbb{F}_5[X]/(f)$, et $\alpha \in K$ la classe de X.

a. Déterminer une base de $K = \mathbb{F}_5[X]/(f)$ comme $\mathbb{F}_5$-espace vectoriel. Montrer que tout élément de K s'écrit de manière unique sous la forme $a_0 + a_1\alpha + a_2\alpha^2$, avec $a_0, a_1, a_2 \in \mathbb{F}_5$.

b. Montrer que K est un corps. Quel est son cardinal ?

c. Déterminer l'inverse de $\alpha - 2$ dans K.

d. Déterminer l'ordre de α dans le groupe multiplicatif $(\mathbb{F}_5[X]/(f))^\times$. Afin d'éventuellement simplifier vos calculs, on vous donne le résultat du calcul $\alpha^{30} = 1 + \alpha^2$

e. Déterminer le polynôme minimal de $\beta = \alpha - 2$.

Exercice 2.

a. Déterminer le polynôme cyclotomique $\Phi_8 \in \mathbb{Z}[X]$.

b. Soit Ψ l'image de Φ_8 dans $\mathbb{Z}/3\mathbb{Z}[X]$. Factoriser Ψ en produit de polynômes irréductibles.

c. Montrer que $\mathbb{F}_9$ est isomorphe à $K = (\mathbb{Z}/3\mathbb{Z}[X])/(X^2 + X - 1)$.

d. On note $\alpha \in K$ la classe de X. Montrer que chaque élément de $\mathbb{F}_9$ s'écrit de manière unique sous la forme $a + b\alpha$ avec $a, b \in \mathbb{Z}/3\mathbb{Z}$.

e. Trouver une racine primitive 8-ème de l'unité dans K.

f. Combien y a-t-il de racines primitives cinquièmes de l'unité dans F_9 ? S'il y en a, les écrire sous la forme $a + b\alpha$ comme ci-dessus.

g. Même question pour les racines primitives quatrièmes de l'unité. Factoriser $X^4 - 1$ en polynômes irréductibles dans $K[X]$.

h. Même question pour les racines primitives troisièmes de l'unité. Factoriser $X^3 - 1$ en polynômes irréductibles dans $K[X]$.

Suite au verso...

Exercice 3.

On fixe p un nombre premier, et n un entier tel que $n \wedge p = 1$. Soit Ψ_n l'image du polynôme cyclotomique Φ_n dans $\mathbb{Z}/p\mathbb{Z}[X]$, et K une extension finie de $\mathbb{Z}/p\mathbb{Z}$ dans laquelle Ψ_n est scindé. On note $U \subset K^\times$ le sous-groupe des racines n-ièmes de l'unité, et $U^* \subset U$ le sous-ensemble des racines primitives n-ièmes de l'unité dans K. On note $\phi : K \to K$ l'automorphisme de Frobénius défini par $\phi : x \mapsto x^p$.

a. Soit $f \in \mathbb{Z}/p\mathbb{Z}[X]$ un polynôme unitaire, scindé dans K. Montrer que si $\alpha \in K$ est une racine de f alors α^p aussi.
   Étant donné $\alpha \in K$, on définit $\Lambda_\alpha = \{\alpha^{p^k} | k \in \mathbb{Z}\}$.

b. Soit $\alpha \in K$ une racine de Ψ_n. Montrer que pour tout entier $k \wedge n = 1$, α^k est encore une racine de Ψ_n et que $\{\alpha^k | k \wedge n = 1\} = U^*$.

c. Supposons que la classe de p dans $\mathbb{Z}/n\mathbb{Z}^*$ engendre le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^*$. On veut démontrer que Ψ_n est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

   (i) Soit $F \in \mathbb{Z}/p\mathbb{Z}[X]$ un diviseur irréductible de Ψ_n, et $\alpha \in K$ une racine de F.
   Montrer que $\Lambda_\alpha = U^*$.

   (ii) En déduire que Ψ_n est irréductible.

   On va maintenant démontrer la réciproque. Dans toute la suite, on fixe α une racine de Ψ_n.

d. Soit $P \in K[X]$ le polynôme défini par $P = \prod_{\lambda \in \Lambda_\alpha} (X - \lambda)$. Montrer que P est un diviseur de Ψ_n dans $K[X]$.

e. Montrer que les coefficients de P sont fixes par l'action de l'automorphisme de Frobenius de K. En déduire que P appartient à $\mathbb{Z}/p\mathbb{Z}[X]$, et que P est aussi un diviseur de Ψ_n dans $\mathbb{Z}/p\mathbb{Z}[X]$.

f. En déduire que si $\Lambda_\alpha \subsetneq U^*$, Ψ_n n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

g. Considérons le cas particulier où $n = 12$ et $p = 5$, utiliser la question précédente pour montrer que Φ_{12} n'est pas irréductible modulo 5.

h. Montrer en général que si la classe de p dans $\mathbb{Z}/n\mathbb{Z}^*$ n'engendre pas le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^*$, alors Φ_n n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.