Feuille d'exercices n° 5
Corps finis et chiffrements

Corps finis

Exercice 1. Décrire les éléments des anneaux suivants et en dresser les tables d'addition et de multiplication :

$$\mathbb{F}_2[X]/(X^2+1) \qquad \mathbb{F}_2[X]/(X^2+X+1) \qquad \mathbb{F}_2[X]/(X^3+X+1).$$

Lesquels de ces anneaux sont-ils des corps ?

Exercice 2. Soit $P = X^4 + X + 1 \in \mathbb{F}_2[X]$. On note $K = \mathbb{F}_2[X]/(P)$ et $\alpha = cl(X) \in K$.

i) Montrer que K est un corps. Quelle est sa caractéristique ?
Donner une base du $\mathbb{F}_2$-espace vectoriel K. Quel est le cardinal de K ?

ii) Quel est l'inverse de l'élément $1 + \alpha^2 + \alpha$ dans le groupe multiplicatif K^* ?

iii) Montrer que α est une racine primitive de l'unité de K.

Exercice 3. Soit $P = X^3 - X + 1 \in \mathbb{F}_3[X]$. On note $K = \mathbb{F}_3[X]/(P)$ et $\alpha = cl(X) \in K$.

i) Montrer que K st un corps. Quelle est sa caractéristique ? Donner une base du $\mathbb{F}_3$-espace vectoriel K. Quel est le cardinal de K ?

ii) Quels sont les ordres possibles des éléments de K^* ?

iii) Montrer que $\alpha^{13} = -1$ (on montrera que $\alpha^{13} = -1$ si et seulement si P divise $X(X-1)^4 + 1$ dans $\mathbb{F}_3[X]$). En déduire l'ordre de α dans K^*.

iv) Le polynôme $Q = X^4 + X^3 + X^2 + X + 1$ a-t-il des racines dans $K[X]$?

Exercice 4. Soit $P = X^2 + X + 2 \in \mathbb{F}_5[X]$. On note $K = \mathbb{F}_5[X]/(P)$ et $\alpha = cl(X) \in K$.

i) Montrer que K est un corps. Quelle est sa caratéristique ? Donner une base du $\mathbb{F}_5$-espace vetoriel K. Quel est le cardinal de K ?

ii) Montrer que $\mathbb{F}_5 = \{x \in K | x^5 = x\}$.

iii) Soit $a \in K \setminus \mathbb{F}_5$. Montrer que $P_a = (X-a)(X-a^5)$ est un polynôme irréductible de $\mathbb{F}_5$. Montrer que pour $Q \in \mathbb{F}_5[X]$, on a $Q(a) = 0$ si et seulement si P_a divise Q.

iv) Factoriser le polynôme $X^{25} - X$ dans $\mathbb{F}_5[X]$ et donner les racines dans K de chaque facteur.

Exercice 5. (Examen 2007) Soit $P = X^3 + X + 1$ dans $\mathbb{F}_5[X]$ et l'anneau $K = \mathbb{F}_5[X]/P$. On note $\alpha = Cl(x)$.

i) Montrer que K est un corps. Donner sa caractéristique, son cardinal ainsi qu'une base $\mathcal{B}$ en tant que F_5 espace vectoriel.

ii) Donner les développements de α^3, α^{15} et α^{30} dans $\mathcal{B}$. En déduire l'ordre de α et de 2α dans K^* ;

iii) Déterminer les coordonnées de l'inverse de $1 + \alpha$ dans $\mathcal{B}$;

iv) Que vaut $P(\alpha^5)$? En déduire les racines de P dans K.

Exercice 6.

i) Donner la liste des polynômes unitaires irréductibles de degré 2 de $\mathbb{F}_3[X]$.

ii) Soit $P = X^4 + X - 1 \in \mathbb{F}_3[X]$. On pose $K = \mathbb{F}_3[X]/(P)$, et $\alpha = cl(X) \in K$.

(a) Montrer que K est un corps. Quelle est sa caractéristique ?

(b) Donner une base de $\mathbb{F}_3$-espace vectoriel K. Quel est son cardinal ?

iii) On s'interesse ici au groupe multiplicatif K^*.

(a) Quels sont les ordres possibles des éléments de K^* ?

(b) Combien le corps K admet-il de racines primitives de l'unité dans K ?

iv) On cherche ici a démontrer que α est une racine primitive de l'unité dans K.

(a) Donner une condition nécessaire et suffisante sur α^{40} pour que α soit une racine primitive de l'unité dans K.

(b) Calculer α^{13}.

(c) Calculer α^{40} et conclure.

v) On cherche a factoriser le polynôme P dans le corps K.

(a) Montrer que α, α^3,α^9,α^{27} sont des éléments de K deux à deux distincts.

(b) Montrer que pour tout entier naturel i on a $P(X^{3^i}) = (P(X))^{3^i}$.

(c) Donner la décomposition de P en facteur irréductibles dans $K[X]$.

(d) En déduire les racines dans K du polynôme $P_1 = -X^4 + X^3 + 1$.

vi) (a) Quelles sont les racines dans K du polynôme $Q = X^4 + X^3 + X^2 + X + 1$?

(b) Même question avec $R = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$.

Exercice 7. On pose $P = X^4 + X + 1 \in \mathbb{F}_2[X]$ et $K = \mathbb{F}_2/(P)$. On note α la classe de X modulo P.

i) Montrer K est un corps.

ii) Déterminer le cardinal de K.

iii) Quel est l'ordre de α dans le groupe K^*.

iv) On pose $\beta = 1 + \alpha^3$. Déterminer le polynôme minimal de β dans $\mathbb{F}_2[X]$ (et dans $K[X]$?).

v) Montrer que le polynôme $F = X^3 + X + 1$ est irréductible dans $K[X]$. Déterminer le cardinal de $K[X]/(F)$.

Chiffrement El Gammal et Diffie-Hellman

Exercice 8. Alice et Bob souhaitent utiliser le protocole de Diffie-Hellman pour créer une clé secrète commune. Ils utilisent le corps K et l'élément x de l'exercice 3.
Alice choisit $a = 9$ et transmet x^9 à Bob. Celui-ci choisit b et lui envoie $x^b = 2 + x + 2x^2$. Quelle sera la clé secrète commune ?

Exercice 9. Alice et Bob souhaitent utiliser l'algorithme de chiffrement de El Gamal.

i) Montrer que $K = \mathbb{F}_2[X]/(X^4 + X + 1)$ est un corps, et que la classe de X (notée α dans la suite) est un générateur de $K^\times$.

ii) Alice rend public le triplet $(K, \alpha, 1 + \alpha^2)$ (c'est-à-dire que $\alpha^a = 1 + \alpha^2$). Bob veut coder le message $m = 1 + \alpha$, en utilisant $x = 5$. Que transmet-il à Alice ?

iii) Même question avec $m = \alpha + \alpha^3$ et $x = 4$.

iv) Vous interceptez le message $(\alpha^3, \alpha^3 + \alpha^2 + \alpha)$. Quel était le message de Bob ?