Master CSI 1 2023-2024

Arithmétique : DS du 6 novembre 2024

Master Sciences et Technologies, mention Mathématiques ou Informatique, parcours Cryptologie et Sécurité informatique

Responsable : Gilles Zémor

Durée : 1h30. Sans document. Les exercices sont indépendants.

– EXERCICE 1. Soit $A = \mathbb{F}_2[X]/(X^5+1)$.

a) Combien l'anneau A contient-il d'éléments ? Combien d'éléments contient le groupe multiplicatif A^* des éléments inversibles de A ?

b) Que vaut l'ordre multiplicatif de X^2+X+1 dans A^* ? Le groupe A^* est-il cyclique ?

c) Montrer que la somme de deux éléments quelconques de A^* n'est pas dans A^*.

d) Quel est l'unique élément non nul y de A tel que $yX = y$?

– EXERCICE 2.

a) Calculer X^{64} dans $\mathbb{F}_2[X]/(X^8+X+1)$. En déduire que les degrés des facteurs irréductibles de X^8+X+1 sont 2 ou 3 ou 6.

b) Calculer X^8+X+1 modulo X^3+X+1 et en déduire que les degrés des facteurs irréductibles de X^8+X+1 sont 2 et 6.

c) En déduire la décomposition en facteurs irréductibles de X^8+X+1.

– EXERCICE 3.

a) Calculer X^9 dans $\mathbb{F}_2[X]/(X^6+X^3+1)$. Dans $\mathbb{F}_2[X]/(X^6+X^3+1)$, quel est l'ordre de X ?

b) Pourquoi peut-on en déduire, sans calcul supplémentaire, que X^6+X^3+1 est irréductible dans $\mathbb{F}_2[X]$?

c) Si α est une racine de X^6+X^3+1 dans $\mathbb{F}_{64}$, quel est le polynôme minimal de α^3 ?

– EXERCICE 4.

a) Montrer que le corps à 16 éléments $\mathbb{F}_{16}$ se représente comme $\mathbb{F}_2(\alpha)$ où α est un élément de polynôme minimal X^4+X+1. Quel est l'ordre multiplicatif de α ?

b) Rappeler ce qu'est la trace $\mathrm{Tr}()$ de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$ et calculer

$$\mathrm{Tr}(1), \mathrm{Tr}(\alpha), \mathrm{Tr}(\alpha^2), \mathrm{Tr}(\alpha^3).$$

c) On pose $e_1 = 1, e_2 = \alpha, e_3 = \alpha^2, e_4 = \alpha^3$. Pourquoi est-ce que e_1, e_2, e_3, e_4 est une base de $\mathbb{F}_{16}$ vu comme espace vectoriel sur $\mathbb{F}_2$? On rappelle que cela veut dire que toute somme non vide d'éléments distincts de l'ensemble $\{e_1, e_2, e_3, e_4\}$ est non nulle et que tout élément de $\mathbb{F}_{16}$ s'écrit comme somme d'éléments de $\{e_1, e_2, e_3, e_4\}$.

d) Sachant que e_1, e_2, e_3, e_4 est une base de $\mathbb{F}_{16}$, montrer que pour tout élément x non nul de $\mathbb{F}_{16}$, xe_1, xe_2, xe_3, xe_4 est aussi une base de $\mathbb{F}_{16}$.

e) Soient $f_1 = \alpha^{-1}, f_2 = \alpha^2, f_3 = \alpha, f_4 = 1$. Montrer que f_1, f_2, f_3, f_4 est une base de $\mathbb{F}_{16}$.

f) Montrer que pour tous $i, j = 1, 2, 3, 4$,

$$\mathrm{Tr}(e_i f_j) = 0 \text{ si } i \neq j \quad \text{et } \mathrm{Tr}(e_i f_i) = 1.$$