Master CSI 1 — 2020-2021

Arithmétique : DS du 25 novembre 2020

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.

a) Calculer α^{32} où α est la classe de X dans $\mathbb{F}_2[X]/(X^5+X^3+1)$. Pourquoi pouvez-vous en déduire que X^5+X^3+1 est irréductible dans $\mathbb{F}_2[X]$?

b) Donner un exemple de polynôme $P(X)$ de degré 6 dans $\mathbb{F}_2[X]$, non irréductible, tel que $X^{64} = X \mod P(X)$.

– EXERCICE 2. On considère la représentation de $\mathbb{F}_{16}$ donnée par $\mathbb{F}_2(\alpha)$ où α a pour polynôme minimal X^4+X+1.

Quels sont tous les polynômes minimaux sur $\mathbb{F}_2$ possibles des éléments de $\mathbb{F}_{16}$? Donner, pour chacun de ces polynômes P, un élément de $\mathbb{F}_2(\alpha)$ dont le polynôme minimal est P.

– EXERCICE 3.

a) On considère le polynôme X^6+X+1 dans $\mathbb{F}_2[X]$. Calculer X^{64} modulo X^6+X+1, et en déduire, en faisant attention, que X^6+X+1 est irréductible.

b) Montrer que X^6+X+1 est primitif.

c) Soit $\mathbb{F}_{64} = \mathbb{F}_2(\alpha)$ où α a X^6+X+1 comme polynôme minimal sur $\mathbb{F}_2$. Montrer que $\beta = \alpha^9$ est tel que $\mathbb{F}_2(\beta)$ est un sous-corps strict de $\mathbb{F}_2(\alpha)$: quel est son cardinal ?

d) Quel est le degré du polynôme minimal sur $\mathbb{F}_2$ de $\gamma = \alpha^7$? Ce polynôme est-il primitif ?

e) Trouver le polynôme minimal sur $\mathbb{F}_2$ de γ.

– EXERCICE 4.

a) Montrer que le polynôme X^4+X+1 est divisible par $X^2+X+\alpha$ dans $\mathbb{F}_4[X]$, où α est une racine de X^2+X+1. Quelle est la factorisation en irréductibles de X^4+X+1 sur $\mathbb{F}_4$?

b) Expliquer pourquoi aucun polynôme irréductible de degré 4 de $\mathbb{F}_2[X]$ n'est irréductible dans $\mathbb{F}_4[X]$.