Master CSI 1

Arithmétique 1

Feuille d'exercices n° 3.

1 On rappelle qu'il y a exactement deux polynômes irréductibles de degré 3 sur $\mathbb{F}_2$, qui sont $P_1(X) = X^3 + X + 1$ et $P_2(X) = X^3 + X^2 + 1$. Soit $K_1 = \mathbb{F}_2[X]/P_1(X)\mathbb{F}_2[X]$. On note $\alpha = X \mod P_1(X)$.

1. Montrez qu'un élément β quelconque de K_1 a pour polynôme minimal sur $\mathbb{F}_2$ soit P_1, soit P_2, soit X, soit $X+1$. Que vaut β dans les 2 derniers cas ? Montrez que, si β est différent de 0 et 1, il est primitif.
2. Calculez le polynôme minimal sur $\mathbb{F}_2$ de β pour tout β dans K_1.
3. En déduire que $K_1 = \mathbb{F}_2(\beta)$ avec $P_2(\beta) = 0$ et que
$$K_1 = \mathbb{F}_2[X]/P_1(X)\mathbb{F}_2[X] \simeq \mathbb{F}_2[X]/P_2(X)\mathbb{F}_2[X].$$
4. Montrez que, pour tout $x \in K_1^*$, $x^7 = 1$. En déduire que les éléments de K_1 sont les racines du polynôme $X^8 - X \in \mathbb{F}_2[X]$, puis que
$$X^8 - X = X(X+1)P_1(X)P_2(X).$$

2 On rappelle que les polynômes irréductibles sur $\mathbb{F}_2$ de degré 4 sont $P_1(X) = X^4 + X^3 + X^2 + X + 1$, $P_2(X) = X^4 + X + 1$, $P_3(X) = X^4 + X^3 + 1$. Soit $K_1 = \mathbb{F}_2[X]/P_1(X)\mathbb{F}_2[X]$. On note $\alpha = X \mod P_1(X)$.

1. Montrez que α est d'ordre 5 dans K_1^*. Est-il primitif ?
2. A priori, et sans calculs, déduisez du théorème de l'élément primitif l'ordre des éléments de K_1^* et le nombre d'éléments ayant un ordre donné.
3. Montrez que $\alpha + 1$ est primitif.
4. Pour chaque élément de K_1^*, exprimé en fonction de α, donnez son ordre, son polynôme minimal sur $\mathbb{F}_2$ et son degré.
5. Identifiez un sous-corps de K_1 à 4 éléments.
6. Quel est le polynôme minimal de α sur ce sous-corps ?

3 On s'intéresse ici à des polynômes sur $\mathbb{F}_2$.

1. Justifier qu'un polyôme non nul a une racine dans $\mathbb{F}_2$ si et seulement si il a un facteur de degré 1.
2. Donner un polynôme non irréductible de degré 4 sans racine dans $\mathbb{F}_2$.
3. Trouver un polynôme non irréductible de degré 5 sans racine dans $\mathbb{F}_2$.
4. Donner une construction de $\mathbb{F}_{32}$.