Université de Bordeaux — **Master CSI**
Année 2016-1017 — **Arithmétique**

Devoir Surveillé, 9 novembre 2016

Durée 2h00, documents interdits

Exercice 1 –

1) À l'aide de la factorisation de $X^9 - X$ dans $\mathbb{F}_3[X]$, calculer le nombre de polynômes unitaires irréductibles de degré 2 de $\mathbb{F}_3[X]$.

2) Les déterminer explicitement.

3) On considère l'anneau $A = \dfrac{\mathbb{F}_3[X]}{\langle X^4+1\rangle}$. Montrer que A n'est pas un corps.

4) Comme à l'accoutumée on note $A^\times$ le groupe multiplicatif des inversibles de A. Déterminer $|A^\times|$.

5) Soit α la classe de X dans A. Montrer que $\alpha \in A^\times$ et déterminer son ordre dans ce groupe.

6) Montrer que pour tout $x \in A$ on a $x^9 = x$.

7) Le groupe $A^\times$ est-il cyclique ?

Exercice 2 –

1) Montrer que $\dfrac{\mathbb{F}_5[X]}{\langle X^3+X+1\rangle}$ est un corps que l'on identifiera à $\mathbb{F}_{125}$.

2) Soit $x \in \mathbb{F}_{125} \setminus \mathbb{F}_5$. Quel est le degré de x sur $\mathbb{F}_5$?

3) Combien y a-t-il dans $\mathbb{F}_{125}$ d'éléments primitifs ?

4) On note α la classe de X dans $\mathbb{F}_{125}$. L'élément α est-il primitif ? *Indication* : on pourra calculer successivement α^3, α^4, α^5, α^{15}, α^{30} et α^{31}.

5) Montrer que $\beta = 2\alpha$ est un élément primitif de $\mathbb{F}_{125}$.

6) En déduire un polynôme unitaire irréductible primitif de degré 3 de $\mathbb{F}_5[X]$.

7) Exprimer les racines de $X^3 + X + 1$ dans $\mathbb{F}_{125}$ comme polynômes en α de degré $\leqslant 2$.

8) Quel est le polynôme minimal de $\alpha + 1$ sur $\mathbb{F}_5$?

Exercice 3 – Figure ci-dessous le schéma des sous-corps de $\mathbb{F}_{2^{30}}$. Dans ce schéma $A \longrightarrow B$ signifie que A et B sont des sous-corps de $\mathbb{F}_{2^{30}}$ vérifiant $A \subsetneq B$ et qu'il n'y a pas de sous-corps C de $\mathbb{F}_{2^{30}}$ vérifiant $A \subsetneq C \subsetneq B$.

$$
\begin{tikzcd}
 & \mathbb{F}_{2^{30}} & \\
N \arrow[ur] & \mathbb{F}_{2^{10}} \arrow[u] & M \arrow[ul] \\
L \arrow[u] \arrow[ur] & K \arrow[ul] \arrow[ur] & \mathbb{F}_{2^2} \arrow[ul] \arrow[u] \\
 & \mathbb{F}_2 \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}
$$

1) Quels sont les corps K, L, M, N ?

2) Quels sont les degrés des extensions N/L et $\mathbb{F}_{2^{30}}/K$?

3) On admettra ici que $X^{10} + X^3 + 1$ est irréductible primitif dans $\mathbb{F}_2[X]$. On identifie $\mathbb{F}_{2^{10}}$ à $\mathbb{F}_2[X]/\langle X^{10} + X^3 + 1\rangle$. On note α la classe de X dans $\mathbb{F}_{2^{10}}$ et on pose $\beta = \alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2$. Montrer que β appartient à un sous-corps strict de $\mathbb{F}_{2^{10}}$ distinct de $\mathbb{F}_2$ que l'on précisera.

4) Trouver un élément appartenant à l'autre sous-corps strict de $\mathbb{F}_{2^{10}}$ distinct de $\mathbb{F}_2$, et l'exprimer comme polynôme en α de degré $\leqslant 9$.

5) Quelle est la forme de la décomposition en produit d'irréductibles (leur nombre et leurs degrés respectifs) de $P(X) = X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ dans $\mathbb{F}_2[X]$?

6) Montrer que $P(X)$ est scindé à racines simples dans M.

Exercice 4 –

1) Montrer que $P(X) = X^5 + X^3 + 1 \in \mathbb{F}_2[X]$ est irréductible dans $\mathbb{F}_2[X]$.

2) En remarquant que 31 est premier, prouver que $P(X)$ est primitif.

3) On considère la suite $(s_i)_{i\geqslant 0}$ définie par $s_0 = s_1 = s_2 = s_3 = s_4 = 1$ et la relation $s_{i+5} = s_{i+3} + s_i$ pour tout $i \geqslant 0$. Montrer que $(s_i)_{i\geqslant 0}$ est périodique et déterminer sans calcul sa période.

4) Soit α la classe de X dans $\mathbb{F}_2[X]/\langle P(X)\rangle$ que l'on identifie à $\mathbb{F}_{32}$. Si $x \in \mathbb{F}_{32}$, on note $\mathrm{Tr}(x)$ la trace de x dans $\mathbb{F}_{32}$. Calculer $\mathrm{Tr}(1)$, $\mathrm{Tr}(\alpha)$, $\mathrm{Tr}(\alpha^2)$, $\mathrm{Tr}(\alpha^3)$ et $\mathrm{Tr}(\alpha^4)$.

5) Calculer les premiers termes de $(s_i)_{i\geqslant 0}$ et en déduire un entier $k \geqslant 0$ tel que $s_i = \mathrm{Tr}(\alpha^{i+k})$ pour tout $i \geqslant 0$.