Université de Bordeaux
Mathématiques
Année 2014-2015

Master CSI
M1MA7W01
Arithmétique

Devoir Surveillé, 3 novembre 2014

Durée 2h00, documents interdits

Exercice 1 –

1) Soit $P(X) = X^3 + X^2 + X + 1 \in \mathbb{F}_5[X]$. Factoriser le polynôme $P(X)$ dans $\mathbb{F}_5[X]$.

2) L'anneau $A = \dfrac{\mathbb{F}_5[X]}{(P(X))}$ est-il un corps ? Quel est son cardinal ? Quelle est sa caractéristique ?

3) À l'aide du théorème chinois, déterminer le cardinal de $A^\times$, le groupe multiplicatif des éléments inversibles de A.

4) Montrer, toujours à l'aide du théorème chinois, que tout élément de $A^\times$ a pour ordre un diviseur de 4.

5) On se propose de retrouver ce résultat sans utiliser le théorème chinois. Soit α la classe de X dans A.
a) Montrer que $\alpha^5 = \alpha$.
b) En déduire que tout $\beta \in A$ vérifie $\beta^5 = \beta$.
c) Conclure.

6) Soit $Q(X) = X^3 + X^2 + X + 3 \in \mathbb{F}_5[X]$. Montrer que $Q(X)$ est irréductible dans $\mathbb{F}_5[X]$.

7) Combien y a-t-il de polynômes unitaires irréductibles de degré 3 dans $\mathbb{F}_5[X]$?

8) On considère le corps $\dfrac{\mathbb{F}_5[X]}{(Q(X))}$ que l'on identifie à $\mathbb{F}_{125}$. Combien y a-t-il d'éléments primitifs dans $\mathbb{F}_{125}$?

9) Soit γ la classe de X dans $\mathbb{F}_{125}$. Calculer l'inverse de γ comme combinaison linéaire à coefficients dans $\mathbb{F}_5$ de 1, γ, γ^2.

10) Quelles sont a priori les valeurs possibles de l'ordre de γ dans $\mathbb{F}_{125}^\times$?

11) Calculer γ^3, γ^4 et γ^{31} (toujours comme combinaisons linéaires à coefficients dans $\mathbb{F}_5$ de 1, γ, γ^2 et en cherchant à minimiser le nombre de calculs pour γ^{31}).

12) Le polynôme $Q(X)$ est-il un polynôme irréductible primitif de $\mathbb{F}_5[X]$?

13) Combien y a-t-il de polynômes unitaires irréductibles primitifs de degré 3 dans $\mathbb{F}_5[X]$?

Exercice 2 –

1) Montrer que $P(X) = X^6 + X^3 + 1 \in \mathbb{F}_2[X]$ est un polynôme irréductible non primitif de $\mathbb{F}_2[X]$.

2) On identifie $\dfrac{\mathbb{F}_2[X]}{(P(X))}$ à $\mathbb{F}_{64}$ et on note α la classe de X dans $\mathbb{F}_{64}$. Quels sont les sous-corps de $\mathbb{F}_{64}$? Faire le schéma des inclusions.

3) Montrer que $\alpha^3 + 1$ appartient à un sous-corps strict de $\mathbb{F}_{64}$.

4) Même question avec $\alpha^4 + \alpha^2 + \alpha$.

5) Quels sont les polynômes minimaux sur $\mathbb{F}_2$ de $\alpha^3 + 1$ et $\alpha^4 + \alpha^2 + \alpha$?

6) On considère la suite $(s_i)_{i \geqslant 0}$ définie par $s_0 = 1$, $s_i = 0$ pour $1 \leqslant i \leqslant 5$ et par la relation de récurrence linéaire $s_{i+6} = s_i + s_{i+3}$ pour tout $i \geqslant 0$. Cette suite est-elle une MLS ? Répondre à cette question sans calculer les premiers termes de la suite.

7) On considère la suite $(t_i)_{i \geqslant 0}$ définie par $t_i = s_i$ pour $0 \leqslant i \leqslant 5$ et par la relation de récurrence linéaire $t_{i+6} = t_{i+1} + t_i$ pour tout $i \geqslant 0$. Calculer les premiers termes de cette suite et en déduire sa période. Que dire du polynôme $Q(X) = X^6 + X + 1$ dans $\mathbb{F}_2[X]$?

8) Soit β une racine de $Q(X)$ dans $\mathbb{F}_{64}$. Exprimer t_i comme trace d'une puissance de β dans $\mathbb{F}_{64}$. *Indication* : il suffit de calculer (si possible de façon astucieuse) $\mathrm{Tr}(\beta^i)$ pour $0 \leqslant i \leqslant 4$.

Exercice 3 –

1) Donner la forme de la factorisation de $X^{16} + 2$ dans $\mathbb{F}_3[X]$ (nombre de facteurs irréductibles et leurs degrés respectifs).

2) Même question avec $X^{144} + 2$.