Codes algébriques – Interrogation 1

01/03/2024

Aucun document et **aucun dispositif électronique** n'est autorisé.

Les **justifications** et le **soin** apportés aux réponses seront évalués.

Durée : 1h15

Exercice 1. Questions courtes (30 min).

Répondre aux questions suivantes en justifiant vos réponses.

Question 1.– Soit σ la permutation de $[1,6] := \{1,2,3,4,5,6\}$ donnée par

i	1	2	3	4	5	6
$\sigma(i)$	2	1	4	5	6	3

La permutation σ induit-elle un automorphisme du code binaire $\mathcal{C}$ engendré par la matrice

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} ?$$

Question 2.– Soit $\mathcal{I}$ l'idéal de $\mathbb{F}_2[x]/(x^6-1)$ engendré par le polynôme $a(x) = x(x+1)^2$. Donner une matrice génératrice du code cyclique associé à l'idéal $\mathcal{I}$.

Question 3.– Quel est le polynôme générateur du dual du code cyclique binaire de longueur 7 engendré par $g(x) = x^3 + x^2 + 1$?

Question 4.– Existe t-il un code cyclique de longueur 14 et de dimension 5 sur $\mathbb{F}_3$?

Exercice 2. Construction de codes cycliques (30 min).

Question 1.– Soit $P(x) = x^2 - x + 1 \in \mathbb{F}_5[x]$.

1. Démontrer que $P(x)$ est irréductible sur $\mathbb{F}_5$.
2. Soit α une racine de $P(x)$. Dans quelle extension de $\mathbb{F}_5$ se situe α ?
3. Démontrer que α est une racine primitive 6-ème de l'unité.

Question 2.– Déterminer une factorisation de $x^6 - 1$ en polynômes irréductibles.

Question 3.– Donner la liste des polynômes générateurs des codes cycliques de longueur 6 et de dimension 4 sur $\mathbb{F}_5$.

Exercice 3. Somme de codes cycliques (15 min).

Soient $\mathcal{A}$ et $\mathcal{B}$ deux codes linéaires de même longueur définis sur un même corps fini. On appelle **somme** de $\mathcal{A}$ et $\mathcal{B}$, notée $\mathcal{A}+\mathcal{B}$, l'espace vectoriel constitué des sommes d'éléments de $\mathcal{A}$ et de $\mathcal{B}$:

$$\mathcal{A}+\mathcal{B} = \{\boldsymbol{a}+\boldsymbol{b}, \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B}\}\,.$$

Question 1.– Démontrer que si $\mathcal{A}$ et $\mathcal{B}$ sont deux codes cycliques, alors $\mathcal{A}+\mathcal{B}$ est également un code cyclique.

Question 2.– On suppose encore que $\mathcal{A}$ et $\mathcal{B}$ sont deux codes cycliques. Soit $a(x)$ le polynôme générateur de $\mathcal{A}$ et $b(x)$ le polynôme générateur de $\mathcal{B}$. Quel est le polynôme générateur de $\mathcal{A}+\mathcal{B}$?