Examen du 23 janvier 2006

Durée 2 heures

Les documents, calculatrices et téléphones portables sont interdits.

Toutes les réponses devront être soigneusement justifiées.

⋆ ⋆ ⋆ ⋆

Exercice 1. — Nombres parfaits. On dit qu'un entier n est positif si $n \geq 1$.
Étant donné un entier positif n, on désigne par $D(n)$ l'ensemble des diviseurs δ de n tels que $1 \leq \delta \leq n$, et pas $S(n)$ la somme des éléments de $D(n)$.
On dit qu'un entier positif n est parfait si $S(n) = 2n$.
Soit a et b deux entiers positifs.

1. Soit $\delta \in D(ab)$. On pose $ab = k\delta$ et
$$d = \text{pgcd}\,(a, \delta), \quad a = da', \quad \delta = d\delta'.$$
   (a) Montrer que δ' divise b.
   (b) En conclure que tout diviseur du produit ab est le produit d'un diviseur de a et d'un diviseur de b.
2. En déduire que l'application ψ définie sur $D(a) \times D(b)$ par
$$\psi(u, v) = uv \in \mathbb{N}^*$$
admet pour image $D(ab)$.
3. Montrer que ψ est une bijection de $D(a) \times D(b)$ sur $D(ab)$ si et seulement si $\text{pgcd}\,(a, b) = 1$.
4. Montrer que si $\text{pgcd}\,(a, b) = 1$, on a $S(ab) = S(a)S(b)$.
5. Montrer qu'un entier positif p est premier si et seulement si $S(p) = p + 1$.
6. Soit k un entier positif. Montrer que le nombre $n = 2^{k-1}(2^k - 1)$ est parfait si et seulement si le nombre $2^k - 1$ est premier.
7. Que peut-on en déduire pour $k = 2$, 3, 4, 5, 6 et 7 ?

Exercice 2. — On considère l'anneau $\mathbb{K} = \mathbb{F}_2[X]/\langle X^4 + X^3 + 1\rangle$, on désigne par $\alpha = \overline{X}$ la classe d'équivalence du polynôme X dans $\mathbb{K}$, et par
$$\mathcal{B} = \{1,\, \alpha,\, \alpha^2,\, \alpha^3\}$$
la base canonique du $\mathbb{F}_2$-espace vectoriel $\mathbb{K}$.

1. Montrer que $\mathbb{K}$ est un corps. Quel est son cardinal ? Sa caractéristique ?
2. Exprimer α^5 dans la base $\mathcal{B}$.
3. En déduire que α est un élément primitif de $\mathbb{K}$.
4. On pose $a = \alpha^5$. Déterminer l'ordre de a dans le groupe $\mathbb{K}^*$.
5. Montrer que l'on a $a^2 + a + 1 = 0$.
6. En déduire que l'ensemble $\mathbb{L} = \{0, 1, a, a^2\}$ est un sous-corps de $\mathbb{K}$.
7. Montrer que $\mathbb{L} = \{x \in \mathbb{K} \,|\, x^4 = x\}$.
8. En déduire que $\mathbb{L}$ est l'unique sous-corps de cardinal 4 de $\mathbb{K}$.
9. Montrer que $\mathbb{L}$ et $\mathbb{F}_2$ sont les uniques sous-corps de $\mathbb{K}$ distincts de $\mathbb{K}$.
(*Cette question est facultative, les candidats qui la traiteront bénéficieront d'un bonus de points.*)

Exercice 3. — 1. Déterminer le rang de la matrice G_1, à coefficients dans $\mathbb{F}_2$, définie par

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

2. Soit C_1 le code linéaire sur $\mathbb{F}_2$, de matrice génératrice G_1.
   (a) Déterminer la longueur, la dimension et le nombre de mots du code C_1.
   (b) Le code C_1 est-t-il systématique ? Pourquoi ?
3. Soit C_2 le code linéaire sur $\mathbb{F}_2$, de matrice génératrice G_2 définie par

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

   (a) Montrer que le code C_2 est systématique.
   (b) Montrer que les codes C_1 et C_2 sont équivalents.
   (c) Montrer que la matrice

$$H_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

   est une matrice de contrôle du code C_2.
   (d) Déterminer la distance minimale d du code C_2.
4. Déduire de la matrice H_2 une matrice de contrôle H_1 du code C_1.
5. Un message m de longueur 4 est encodé par la matrice G_1, le mot 1110010 est reçu. On fait l'hypothèse d'au plus une erreur lors de la transmission.
   (a) Déterminer le mot de code émis.
   (b) Déterminer le message m.