UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Examen (première session)

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits. ***Justifiez toutes vos réponses.*** *Il est bon de relire sa copie...*

Durée : 2 heures

Le barème est donné à titre indicatif.

Exercice 1 (5 points)

1 Enoncer le théorème de Lagrange.

2 Soit G un groupe et a un élément d'ordre k dans G . Soit p un entier naturel. Donner sans justification l'ordre de a^p ?

3 Le groupe $\mathfrak{S}_3$ des permutations de $\{1,2,3\}$ est-il cyclique ? (justifier)

4 Enoncer le théorème de la division euclidienne dans $k[X]$.

5 Enoncer le théorème de la division euclidienne dans $\mathbf{Z}[i]$.

Exercice 2 (3 points)

1 La classe [51] est-elle inversible dans l'anneau $\mathbf{Z}/131\mathbf{Z}$. Si oui, calculer 92×51^{-1} dans $\mathbf{Z}/131\mathbf{Z}$. Le résultat doit être représenté par un nombre compris entre 0 et 130.

2 Trouver l'ensemble des diviseurs de zéro dans $\mathbf{Z}/16\mathbf{Z}$. (Dans cet exercice on ne considère pas le 0 comme un diviseur de zéro.) Représenter chaque classe par un nombre compris entre 1 et 15.

Exercice 3 (4 points)

1 On rappelle que le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$ est X^2+X+1. Montrer que le polynôme X^4+X+1 est irréductible dans $\mathbb{F}_2[X]$. (On pourra admettre le résultat de cette question et continuer).

2 On note $A := \mathbb{F}_2[X]/ < X^4+X+1 >$ l'anneau quotient de $\mathbb{F}_2[X]$ par l'idéal engendré par P. La classe de $3X^5+X^2+X+7$ est-elle nulle dans A ? L'anneau A est-il un corps ? Comment obtenir dans chque classe un représentant de degré minimal ? Combien l'anneau A a-t-il d'éléments ?

3 On note α la classe du polynôme X dans A. Déterminer α^4 et α^{15} comme polynômes de degré au plus 3 en α.

4 Le polynôme $X^{15}-1$ est-il un multiple de X^4+X+1 dans $\mathbb{F}_2[X]$?

Exercice 4 (5 points)

1 On considère le code binaire, linéaire engendré par la matrice

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

Quel est son alphabet ? sa longueur ? sa dimension ? un polynôme générateur ? son nombre de mots ?

2 Le code est-il cyclique ?

3 Ecrire une matrice de contrôle. Montrer que la distance du code est au moins 3. Combien d'erreurs peut-on alors détecter ? combien d'erreurs peut-on alors corriger ?

4 Le mot $(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$ est-il un mot de code ? Si non, en supposant qu'il n'a qu'une erreur, écrire le mot de code dont il provient.

Exercice 5 (3.5 points)

1 Le nombre 613 est-il premier ?

2 Peut-il s'écrire comme somme de deux carrés ?

3 Calculer 35^2 modulo 613.

4 Effectuer la division euclidienne de 613 par $35 + i$ dans l'anneau $\mathbf{Z}[i]$ des entiers de Gauss.

5 Ecrire 613 comme somme de deux carrés.

Un corrigé sera disponible sur internet.