Université de Paris 7 **Révisions du 26-03-2008** **agreg 2008 (F.Han)**

Exercice I: Codes cycliques

Soit q une puissance d'un nombre premier. Pour $n \in \mathbb{N}, n > 1$, on pose $H = \mathbb{F}_q[X]/(X^n - 1)$.

1) On appellera code cyclique de longueur n un idéal I de H vu comme $\mathbb{F}_q$-espace vectoriel. Montrer que I est principal, et donner une base de I en fonction d'un générateur bien choisi de I.[1]

2) Codes de Reed-Solomon. On suppose $q > 2$, et l'on pose $n = q - 1$. Soit $t \in \mathbb{N}, 1 < t \leq n$. On note $\Sigma = \{1, \ldots, t-1\}$

a) Montrer qu'il existe dans $\mathbb{F}_q$ une racine primitive n-ième de l'unité (On en choisira une notée ζ).

b) On considère le polynôme $g = \prod_{i \in \Sigma}(X - \zeta^i)$. Montrer que g permet de définir un code cyclique de longueur n. Quelle est sa dimension[2]?

c) Montrer qu'un élément non nul m de l'idéal (g) de $\mathbb{F}_q[X]/(X^n-1)$ exprimé dans la base $1, \ldots, X^{n-1}$ a au moins t coordonnées non nulles. [3] En déduire que la distance minimale entre 2 mots du code est t.

d) Remarquer que si l'on regarde maintenant ces $\mathbb{F}_q$ espaces vectoriels comme des $\mathbb{F}_p$ espaces vectoriels, alors ce code peut corriger $(t-1)/2 * s$ erreurs consécutives, (où $q = p^s$). Par exemple, deux codes racourcis de celui obtenu par la méthode précédente en prenant $q = 2^8$ et $t = 5$ sont utilisés dans les CD.

Exercice II: Polynômes orthogonaux[4]

Soit k un corps commutatif, et $(u_n) \in k^{\mathbb{N}}$. On définit sur $k[x]$ une forme bilinéaire symétrique ϕ par:

$$\phi(x^i, x^j) = u_{i+j}$$

1) Remarquer que $\phi(F.G, H) = \phi(F, G.H)$.

2) On note $D_n = \det(u_{i+j})_{0 \leq i,j \leq n}$.

a) Montrer que si les $(D_i)_{0 \leq i \leq n}$ sont non nuls, alors la famille $1, x, \ldots, x^n$ peut être orthogonalisée en une famille $(P_0, \ldots, P_n)$

b) Sous les hypothèses précédentes, montrer que P_n est proportionnel à:

$$\begin{vmatrix} u_0 & \ldots & u_n \\ \vdots & & \vdots \\ u_{n-1} & \ldots & u_{2n-1} \\ 1 & \ldots & x^n \end{vmatrix}$$

c) Toujours sous les hypothèses précédentes, montrer que pour pouvoir imposer en plus que $\phi(P_n, P_n)$ soit une constante γ non nulle, il faut que les rapports $(D_i/D_{i-1})_{0<i\leq n}$ soient congrus dans k^* modulos les carrés de k^*.

3) a) Donner un exemple de forme bilinéaire ϕ lorsque $k = \mathbb{R}$ provenant de l'analyse.

b) Toujours dans le cas réel, et sous l'hypothèse $(D_i)_{0 \leq i \leq n}$ non nuls, donner la signature de la restriction de ϕ aux polynômes de degré inférieur ou égal à n, en fonction des variations de signes des D_i

4) On considère la série formelle: $F(x) = \sum_{i=0}^{+\infty} u_i.x^i$. On suppose toujours les $(D_i)_{0 \leq i \leq n}$ non nuls. Montrer[5] que qu'il existe une fraction rationnelle $f_n(x)$ dont les numérateurs et dénominateurs ont degré au plus n telle que:

$$F(x) = f_n(x) + O(x^{2n})$$

où $O(x^{2n})$ désigne une série formelle en x divisible par x^{2n}

Exercice III:

1) On note $M \in \mathcal{M}_n(\mathbb{R})$ la matrice telle que $M_{i,j} = C_j^i$, où C_j^i est le coefficient binomial. Montrer que M est inversible et calculer son inverse.

[1] La matrice des vecteurs de base exprimée dans la base (x^i) est appelée matrice génératrice du code.

[2] en tant qu'espace vectoriel

[3] Un élément du code (g) est appelé un mot du code. La distance entre 2 mots est le nombre de coordonnées différentes des 2 vecteurs.

[4] CF Par ex Goblot, algèbre linéaire

[5] On pourra traduire les relations d'orthogonalité entre P_n et x^k en terme d'un produit astucieux dans $k[[x]]$