

Exercice I:

Soit \mathcal{E} un plan affine, et A, B, C 3 points affinement indépendants.

1) a) Pour $i \in \{1, 2, 3\}$, M_i est le point de coordonnées barycentriques (x_i, y_i, z_i) dans le repère (A, B, C) .
Montrer que:

$$M_1, M_2, M_3 \text{ sont alignés} \Leftrightarrow \begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix} = 0$$

b) Donner les équations barycentriques des droites (AB) , (AC) , (BC)

2) Soient I, J, K les milieux respectifs de $[BC]$, $[AC]$, $[AB]$. Soit M un point de \mathcal{E} distinct de A, B, C , de coordonnées barycentriques (α, β, γ) dans (A, B, C) . On note A' (resp. B', C') le symétrique de M par rapport à I (resp. J, K). Donner les coordonnées barycentriques de A', B', C' en fonction de α, β, γ dans le repère (A, B, C) .

3) Montrer que les droites (AA') , (BB') , (CC') sont concourantes en un point P .

4) O étant un point quelconque du plan \mathcal{E} , montrer que

$$2\overrightarrow{OP} = \overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC} - \overrightarrow{OM}$$

En déduire que les points M, P , et le centre de gravité G du triangle ABC sont alignés. Préciser la position de G par rapport à M et P .

Exercice II: Formes antisymétriques¹

Soit k un corps de caractéristique différente de 2. Soit ϕ une forme antisymétrique non dégénérée sur un espace vectoriel E de dimension finie.

1) a) Montrer que si E est de dimension 2, alors il existe une base de E telle que ϕ ait pour matrice $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ dans cette base. Dans ce cas on dit que l'espace est un plan symplectique pour ϕ .

b) Montrer que E est forcément de dimension paire.

2) Montrer que E est somme orthogonale de m plans symplectiques.

3) On considère l'anneau de polynômes en $n(n-1)/2$ indéterminées $A = \mathbb{Z}[x_{1,2}, \dots, x_{n-1,n}]$, et M la matrice antisymétrique formelle de taille n en les $x_{i,j}$.

a) Montrer que si n est impair, alors $\det(M) = 0$

b) On suppose que n est pair. Montrer que $\det M$ est le carré d'un élément de $\mathbb{Q}(x_{1,2}, \dots, x_{n-1,n})$, puis montrer que cet élément est en fait dans $\mathbb{Z}[x_{1,2}, \dots, x_{n-1,n}]$

Exercice III: 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 .²

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 $\Sigma = \{1, \dots, t - 1\}$

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 dimension³?

c) Montrer qu'un élément non nul m de l'idéal (g) de $\mathbb{F}_q[X]/(X^n - 1)$ exprimé dans la base $1, \dots, X^{n-1}$ a au moins t coordonnées non nulles. ⁴ 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 raccourcis de celui obtenu par la méthode précédente en prenant $q = 2^8$ et $t = 5$ sont utilisés dans les CD.

¹Cf par exemple Goblot, algèbre linéaire

²La matrice des vecteurs de base exprimée dans la base (x^i) est appelée matrice génératrice du code.

³en tant qu'espace vectoriel

⁴Un élément du code (g) est appelé un mot du code. La distance entre 2 mots est le nombre de coordonnées différentes des 2 vecteurs.