

HEC Paris – ESSEC Business School

Mathématiques I

Mathématiques approfondies

Sujet adapté – 2004

Table des matières

1	L'opération Δ sur les parties d'un ensemble	2
	<i>Thèmes abordés : espaces vectoriels ; applications linéaires.</i>	<i>2</i>
2	Une autre algèbre linéaire	2
	<i>Thèmes abordés : espaces vectoriels ; applications linéaires.</i>	<i>2</i>
3	Un code correcteur d'erreurs	4
	<i>Thèmes abordés : espaces vectoriels ; applications linéaires.</i>	<i>4</i>
4	Distinguere falsum vero	5
	<i>Thèmes abordés : espaces vectoriels ; applications linéaires ; Python.</i>	<i>5</i>

Les parties du sujet contenant des éléments n'étant plus au programme depuis 2022 ont été adaptées pour convenir aux nouveaux programmes de la filière Mathématiques approfondies en vigueur depuis 2023.

Sur la transmission de messages

Le but de ce problème est de construire un système permettant de détecter et de corriger automatiquement des erreurs apparues lors de la transmission de messages binaires. Dans tout le problème, m , n , p désignent des entiers naturels non nuls.

1 L'opération Δ sur les parties d'un ensemble

Thèmes abordés : espaces vectoriels ; applications linéaires.

On considère un ensemble $E = \{e_1, \dots, e_n\}$ ayant n éléments. La différence symétrique de deux parties A et B de E , notée $A\Delta B$, est l'ensemble des éléments de E qui appartiennent à l'une et pas à l'autre. On admet que l'opération Δ est commutative et associative et que, pour toute partie A de E ,

$$A\Delta\emptyset = A, \quad A\Delta A = \emptyset.$$

Pour toutes parties A et B de E , on pose $d(A, B) = \text{Card}(A\Delta B)$.

- 1) a) Pour une partie A de E , déterminer $d(A, \emptyset)$ et $d(A, E)$.
b) Montrer que, pour toutes parties A et B de E , $d(A, B) = d(A\Delta B, \emptyset)$.
- 2) Une partie A de E peut être représentée par le n -uplet $(x_1, \dots, x_n)$ défini par, pour tout $i \in \{1, \dots, n\}$, $x_i = 1$ si $e_i \in A$ et $x_i = 0$ sinon.
 - a) Les parties A , B , $A\Delta B$ étant représentées respectivement par $(x_1, \dots, x_n)$, $(y_1, \dots, y_n)$ et $(z_1, \dots, z_n)$, construire, pour un entier i fixé de $\{1, \dots, n\}$, une table à deux lignes et deux colonnes donnant les valeurs de z_i en fonction de celles de x_i et y_i . Comparer z_i et $|x_i - y_i|$.
 - b) Montrer que, pour toutes parties A , B et C de E , $d(A, C) \leq d(A, B) + d(B, C)$.

2 Une autre algèbre linéaire

Thèmes abordés : espaces vectoriels ; applications linéaires.

On considère l'ensemble $\mathbb{K} = \{0, 1\}$ et $\mathcal{M}_{p,n}(\mathbb{K})$ l'ensemble des matrices à p lignes et n colonnes à coefficients dans $\mathbb{K}$. Sur $\mathbb{K}$, on définit l'addition $\dot{+}$ et la multiplication $\cdot$ par les tables suivantes :

$$\begin{array}{c|cc} \dot{+} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}.$$

La multiplication sur $\mathbb{K}$ est celle des réels ; les deux opérations sont associatives et commutatives, et la multiplication est distributive par rapport à l'addition.

Pour $A = (a_{i,j})$ et $B = (b_{i,j})$ de $\mathcal{M}_{p,n}(\mathbb{K})$, on définit $A \dot{+} B = (c_{i,j})$ par $c_{i,j} = a_{i,j} \dot{+} b_{i,j}$. Pour $\varepsilon \in \mathbb{K}$, on définit $\varepsilon \cdot A = (\varepsilon \cdot a_{i,j})$. Enfin, si $A \in \mathcal{M}_{p,n}(\mathbb{K})$ et $B \in \mathcal{M}_{n,m}(\mathbb{K})$, on définit $A \dot{\times} B = (c_{i,j})$ par

$$c_{i,j} = a_{i,1} \cdot b_{1,j} \dot{+} \dots \dot{+} a_{i,n} \cdot b_{n,j}.$$

La loi $\dot{+}$ sur $\mathcal{M}_{p,n}(\mathbb{K})$ est commutative, associative, d'élément neutre la matrice nulle $\mathcal{O}$; $\dot{\times}$ est distributive par rapport à $\dot{+}$. En particulier, pour toute matrice A , $A \dot{+} \mathcal{O} = A$ et $A \dot{+} A = \mathcal{O}$.

On appelle *code* toute partie non vide C de $\mathcal{M}_{n,1}(\mathbb{K})$ telle que $\forall (x, y) \in C^2$, $x \dot{+} y \in C$.

- 1) On considère les colonnes de $\mathcal{M}_{5,1}(\mathbb{K})$

$$x_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad x_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \quad x_4 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

et l'ensemble $C = \{\varepsilon_1 x_1 \dot{+} \varepsilon_2 x_2 \dot{+} \varepsilon_3 x_3 \dot{+} \varepsilon_4 x_4 : (\varepsilon_1, \dots, \varepsilon_4) \in \mathbb{K}^4\}$.

- Montrer que C est un code. Déterminer tous ses éléments à l'aide de x_1, x_2, x_4 .
- Existe-t-il une famille (u_1, u_2) d'éléments de C telle que $\{\varepsilon_1 u_1 \dot{+} \varepsilon_2 u_2 : (\varepsilon_1, \varepsilon_2) \in \mathbb{K}^2\} = C$?
- Montrer que $\varepsilon_1 x_1 \dot{+} \varepsilon_2 x_2 \dot{+} \varepsilon_4 x_4 = \mathcal{O} \Rightarrow \varepsilon_1 = \varepsilon_2 = \varepsilon_4 = 0$.

Une famille $(u_1, \dots, u_q)$ d'éléments de $\mathcal{M}_{p,n}(\mathbb{K})$ est dite $\mathbb{K}$ -libre lorsque

$$\forall (\varepsilon_1, \dots, \varepsilon_q) \in \mathbb{K}^q, \quad \varepsilon_1 u_1 \dot{+} \dots \dot{+} \varepsilon_q u_q = \mathcal{O} \Rightarrow \varepsilon_1 = \dots = \varepsilon_q = 0.$$

Dans le cas contraire, elle est dite $\mathbb{K}$ -liée. Une famille $(u_1, \dots, u_q)$ d'éléments d'un code C est une $\mathbb{K}$ -base de C lorsqu'elle est $\mathbb{K}$ -libre et que tout élément x de C s'écrit $x = \varepsilon_1 u_1 \dot{+} \dots \dot{+} \varepsilon_q u_q$ avec $(\varepsilon_1, \dots, \varepsilon_q) \in \mathbb{K}^q$. Dans la suite, $n \geq 2$.

- Pour $x = {}^t(x_1, \dots, x_n)$ et $y = {}^t(y_1, \dots, y_n)$ de $\mathcal{M}_{n,1}(\mathbb{K})$, $d(x, y)$ désigne le nombre d'indices $i \in \{1, \dots, n\}$ tels que $x_i \neq y_i$.
 - Montrer que, pour tout $(x, y) \in \mathcal{M}_{n,1}(\mathbb{K})^2$, $d(x, y) = d(x \dot{+} y, \mathcal{O})$.
 - Montrer que, pour tout $(x, y, z) \in \mathcal{M}_{n,1}(\mathbb{K})^3$, $d(x, z) \leq d(x, y) + d(y, z)$.
- Soit C un code non réduit à $\{\mathcal{O}\}$.
 - Montrer que C admet une $\mathbb{K}$ -base. On pourra considérer, après avoir justifié son existence, le cardinal maximum d'une famille $\mathbb{K}$ -libre d'éléments de C .
 - Montrer que si $(u_1, \dots, u_q)$ est une $\mathbb{K}$ -base de C , tout élément de C s'écrit de manière unique sous la forme $\varepsilon_1 u_1 \dot{+} \dots \dot{+} \varepsilon_q u_q$. En déduire le cardinal de C en fonction du cardinal d'une de ses $\mathbb{K}$ -bases.
 - Montrer que toutes les $\mathbb{K}$ -bases de C ont le même cardinal.
 - Si q est le cardinal d'une $\mathbb{K}$ -base de C et $(v_1, \dots, v_q)$ est une famille $\mathbb{K}$ -libre de C , montrer que $(v_1, \dots, v_q)$ est une $\mathbb{K}$ -base de C .
- On suppose $1 \leq p \leq n$. On note I_p la matrice identité de taille p et $Q \in \mathcal{M}_{p,n}(\mathbb{K})$ une matrice dont p colonnes sont les p colonnes distinctes de I_p . On définit $C_Q = \{x \in \mathcal{M}_{n,1}(\mathbb{K}) : Q \dot{\times} x = \mathcal{O}\}$.
 - Montrer que C_Q est un code.
 - Montrer que, pour tout $(x_1, \dots, x_n) \in \mathbb{K}^n$, il existe une permutation σ de $\{1, \dots, n\}$ telle que

$$Q \dot{\times} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (I_p \ P) \dot{\times} \begin{pmatrix} x_{\sigma(1)} \\ \vdots \\ x_{\sigma(n)} \end{pmatrix},$$

où $P \in \mathcal{M}_{p,n-p}(\mathbb{K})$.

- c) En déduire le nombre d'éléments de C_Q et le cardinal d'une de ses $\mathbb{K}$ -bases.
- d) Si $Q = (B \ I_p)$ avec $B \in \mathcal{M}_{p,n-p}(\mathbb{K})$, montrer que les colonnes de $\begin{pmatrix} I_{n-p} \\ B \end{pmatrix}$ constituent une base de C_Q .
- e) Si A est une partie non vide de $\mathbb{N}$, $\min A$ désigne son plus petit élément. On suppose $r > 1$, que toute famille de $r - 1$ colonnes de Q est $\mathbb{K}$ -libre dans $\mathcal{M}_{p,1}(\mathbb{K})$, et qu'il existe une famille $\mathbb{K}$ -liée de r colonnes de Q . Montrer que $r = \min\{d(x, \mathcal{O}) : x \in C_Q \setminus \{\mathcal{O}\}\}$.

3 Un code correcteur d'erreurs

Thèmes abordés : espaces vectoriels ; applications linéaires.

On suppose $p \geq 2$ et $n = 2^p - 1$. On considère une matrice H dont les colonnes sont les n éléments non nuls de $\mathcal{M}_{p,1}(\mathbb{K})$ et on définit $C_H = \{u \in \mathcal{M}_{n,1}(\mathbb{K}) : H \dot{\times} u = \mathcal{O}\}$.

- 1) Déterminer le cardinal des $\mathbb{K}$ -bases de C_H .
- 2) Montrer que $\min\{d(u, v) : (u, v) \in C_H^2, u \neq v\} = 3$.
- 3) Pour $v \in \mathcal{M}_{n,1}(\mathbb{K})$, on définit $B_v = \{u \in \mathcal{M}_{n,1}(\mathbb{K}) : d(u, v) \leq 1\}$.
 - a) Déterminer le cardinal de B_v .
 - b) Montrer que si v et w sont deux éléments distincts de C_H , alors $B_v \cap B_w = \emptyset$.
 - c) Montrer que $\bigcup_{v \in C_H} B_v = \mathcal{M}_{n,1}(\mathbb{K})$.
- 4) Soit $z \in \mathcal{M}_{n,1}(\mathbb{K}) \setminus C_H$.
 - a) Montrer qu'il existe un seul élément v de C_H tel que $d(z, v) = 1$; cet élément est noté $\Phi(z)$.
 - b) Montrer qu'il existe un seul élément $e \in \mathcal{M}_{n,1}(\mathbb{K})$ tel que $d(e, \mathcal{O}) = 1$ et $H \dot{\times} z = H \dot{\times} e$. Comparer $\Phi(z)$ et $z \dot{+} e$.
- 5) Dans cette question uniquement, $p = 3$, $n = 7$, et

$$H_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

- a) Montrer que C_{H_1} a pour $\mathbb{K}$ -base (c_1, c_2, c_3, c_4) , où

$$c_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad c_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad c_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad c_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

- b) On veut transmettre quatre symboles $\eta_1, \eta_2, \eta_3, \eta_4 \in \mathbb{K}$. On transmet les sept composantes de $y = \eta_1 c_1 \dot{+} \eta_2 c_2 \dot{+} \eta_3 c_3 \dot{+} \eta_4 c_4$. La colonne reçue est $y^* = {}^t(0, 1, 0, 0, 1, 1, 0)$ et une seule de ses composantes est erronée. Déterminer les valeurs exactes de $\eta_1, \eta_2, \eta_3, \eta_4$ (on utilisera $H_1 \dot{\times} y^*$).

- c) Une colonne $z \in C_{H_1}$ est transmise et la colonne reçue z^* comporte deux erreurs. Montrer que le calcul de $H_1 \dot{\times} z^*$ permet de déceler des erreurs, mais pas d'identifier les deux composantes erronées.

4 Distinguer falsum vero

Thèmes abordés : espaces vectoriels ; applications linéaires ; Python.

On reprend les notations de la partie précédente, avec $p \geq 2$ et $n = 2^p - 1$.

- 1) Pour $k \in \{1, \dots, n\}$, on considère son écriture en base deux $k = \sum_{i=1}^p \varepsilon_{i,k} 2^{i-1}$ et la matrice $H_2 = (\varepsilon_{i,k})_{1 \leq i \leq p, 1 \leq k \leq n}$. Soient $\eta_1, \dots, \eta_{n-p} \in \mathbb{K}$. On transmet $y = \eta_1 d_1 + \dots + \eta_{n-p} d_{n-p}$, où $(d_1, \dots, d_{n-p})$ est une base de C_{H_2} . Le message reçu est y^* et une seule erreur est survenue. Si

$$H_2 \dot{\times} y^* = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \quad \text{et} \quad k = \sum_{i=1}^p x_i 2^{i-1},$$

montrer que l'erreur s'est produite à la composante numéro k de y .

- 2) Dans cette question, $p = 3$ et $n = 7$.

- a) On pose

$$d_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad d_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad d_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \quad d_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Déterminer la matrice H_2 et montrer que (d_1, d_2, d_3, d_4) est une $\mathbb{K}$ -base de C_{H_2} .

- b) Primus pense avoir trouvé les trois premiers chiffres significatifs x, y, z (en base dix) d'une constante ζ . Chaque chiffre de 0 à 9 est écrit en base deux à quatre positions : 5 est représenté par 0101 et 9 par 1001. Ainsi $x = x_4 x_3 x_2 x_1$, $y = y_4 y_3 y_2 y_1$, $z = z_4 z_3 z_2 z_1$, avec par exemple $x = x_1 + 2x_2 + 2^2 x_3 + 2^3 x_4$.

Primus transmet les trois colonnes

$$x_1 d_1 + x_2 d_2 + x_3 d_3 + x_4 d_4, \quad y_1 d_1 + y_2 d_2 + y_3 d_3 + y_4 d_4, \quad z_1 d_1 + z_2 d_2 + z_3 d_3 + z_4 d_4.$$

Il y a au plus une erreur par colonne. Secundus reçoit, écrites bout à bout, les trois colonnes :

$$111011010000110010111.$$

Quel est probablement le nombre que Primus et Secundus semblent sur le point de découvrir ?

- c) Secundus décide d'écrire un programme **en Python** qui permet de retrouver, à partir des colonnes reçues, les chiffres envoyés par Primus. Comment peut-il procéder ?