

## I. SYMÉTRIES VECTORIELLES

**I.A.1.a** Soit  $x$  appartenant à  $F_s$ . Alors puisque  $F$  et  $G$  sont deux sous-espaces vectoriels supplémentaires de  $E$ , il existe un unique couple  $(y, z)$  appartenant à  $F \times G$  tel que  $x = y + z$ . Ainsi,

$$s(x) = s(y + z) = y - z \quad (s \text{ est une symétrie})$$

de plus,  $s(x) = x = y + z \quad (x \in F_s)$

d'où,  $z = 0$  et ainsi  $x = y$

donc  $x \in F$ . Si bien que  $F_s \subset F$ .

Réciproquement, soit  $x \in F$ . Alors en appliquant la définition de  $s$  avec  $z = 0 \in G$ , il vient

$$s(x) = x \quad \text{et donc} \quad F \subset F_s$$

Finalement par double inclusion  $F = F_s$

Faisons de même pour  $G$  et  $G_s$ . Soit  $x \in G_s$ . Alors il existe un unique couple  $(y, z)$  appartenant à  $F \times G$  tel que  $x = y + z$ . Ainsi, il vient

$$y + z = x = -s(x) = -s(y + z) = -y + z$$

Ainsi  $x$  appartient à  $G$ , donc  $G_s \subset G$ . Soit  $x \in G$ , alors en appliquant la définition de  $s$  avec  $y = 0 \in F$  il vient  $s(x) = -x$ . Finalement, par double inclusion

$$G = G_s$$

**I.A.1.b** Soit  $x$  appartenant à  $E$ . Il existe un unique couple  $(y, z)$  dans  $F \times G$  tel que  $x = y + z$ . Ainsi,

$$s \circ s(x) = s(s(y + z)) = s(y - z) = y + z = x$$

d'où,  $s \circ s = \text{Id}_E$

L'endomorphisme  $s$  a donc pour inverse lui-même.

$$\boxed{\text{L'application } s \text{ est un automorphisme de } E.}$$

**I.A.1.c** D'après la question I.A.1.a,

$$\text{Ker}(s - \text{Id}_E) \oplus \text{Ker}(s + \text{Id}_E) = F_s \oplus G_s = F \oplus G = E.$$

Dès lors trois cas se présentent :

- Soient  $F_s = \text{Ker}(s - \text{Id}_E) \neq \{0_E\}$  et  $G_s = \text{Ker}(s + \text{Id}_E) \neq \{0_E\}$ . L'endomorphisme  $s$  a donc pour valeurs propres 1 et -1.
- Soit  $F_s = \{0_E\}$  et alors  $G_s = E$ .
- Soit  $G_s = \{0_E\}$  et alors  $F_s = E$ .

Il en découle trois conclusions possibles :

On a respectivement : soit  $F_s$  et  $G_s$  sont les deux espaces propres, les deux valeurs propres sont 1 et -1. Soit  $G_s$  est le seul espace propre, la seule valeur propre est -1. Ou soit  $F_s$  est le seul espace propre, la seule valeur propre est 1.

**I.A.2.a** Montrons tout d'abord que  $F \cap G = \{0_E\}$ . Soit  $x$  appartenant à  $F \cap G$ .

$$s(x) = x = -x \quad \text{donc} \quad x = 0_E$$

Ainsi,

$$F \cap G = \{0_E\}$$

Montrons ensuite que  $F + G = E$ . Soit  $x$  appartenant à  $E$ .

$$x = \frac{1}{2}(x - s(x) + x + s(x))$$

$$\text{Or,} \quad s((x - s(x))) = s(x) - x = -(x - s(x)) \quad \text{et} \quad s(x + s(x)) = s(x) + x$$

$$\text{donc,} \quad x - s(x) \in G \quad \text{et} \quad x + s(x) \in F$$

d'où,  $E \subset F + G$ . L'autre inclusion étant évidente, il vient

$$F \oplus G = E$$

**I.A.2.b** Tout d'abord, remarquons d'après la question précédente que  $F \oplus G = E$ . C'est la première condition pour avoir une symétrie par rapport à  $F$  parallèlement à  $G$ . De plus, pour tout  $(y, z)$  appartenant à  $F \times G$ :

$$s(y + z) = s(y) + s(z) = y - z$$

L'application  $s$  est la symétrie par rapport à  $F$  parallèlement à  $G$ .

**I.B.1.a** Soit  $x$  appartenant à  $F_s$ . Utilisons tout d'abord l'égalité  $s \circ t = -t \circ s$ .

$$s(t(x)) = -t(s(x)) = -t(x)$$

Ainsi,  $t(x) \in G_s$ . Par conséquent,

$$t(F_s) \subset G_s.$$

Soit  $x$  appartenant à  $G_s$ . De la même manière, on obtient

$$s(t(x)) = -t(s(x)) = t(-s(x)) = t(x)$$

d'où

$$t(G_s) \subset F_s$$

En appliquant  $t$  à ces deux inclusions et en remarquant que  $t \circ t = \text{Id}_E$  il vient

$$F_s \subset t(G_s) \quad \text{et} \quad G_s \subset t(F_s)$$

Finalement,

$$t(F_s) = G_s \text{ et } t(G_s) = F_s$$

**I.B.1.b** Utilisons la question précédente:

$$\dim(F_s) \geq \dim(t(F_s)) = \dim(G_s)$$

De même

$$\dim(G_s) \geq \dim(t(G_s)) = \dim(F_s)$$

Par double inégalité

$$\dim(G_s) = \dim(F_s)$$

Appliquons ensuite la question I.A.1. On sait que  $F_s \oplus G_s = E$ , d'où:

$$\dim(F_s) + \dim(G_s) = n$$

Finalement

$$2 \dim(F_s) = n$$

donc,

$$\text{L'entier } n \text{ est pair.}$$

**I.C.1** Il suffit de montrer qu'un  $H$ -système est libre. Soient  $(\lambda_i)_{1 \leq i \leq p} \in \mathbb{R}^p$  tel que

$$\sum_{i=1}^p \lambda_i S_i = 0 \quad (1)$$

Alors pour tout  $j$  tel que  $1 \leq j \leq p$  en composant l'égalité (1) une première fois par  $S_j$  à gauche puis une seconde fois par  $S_j$  à droite et en sommant les deux résultats obtenus, on obtient

$$\sum_{i=1}^p \lambda_i S_i \circ S_j + \sum_{i=1}^p \lambda_i S_j \circ S_i = 0$$

Ainsi, 
$$\sum_{i=1}^p \lambda_i (S_i \circ S_j + S_j \circ S_i) = 0$$

Utilisons alors le fait que  $S_j \circ S_i + S_i \circ S_j = 0$  pour tout  $i$  appartenant à  $\llbracket 1; p \rrbracket \setminus \{j\}$ . Il s'ensuit que

$$2\lambda_j S_j \circ S_j = 0$$

Appliquons ensuite l'identité  $S_j \circ S_j = \text{Id}_E$  qui est vraie pour tout  $i \in \llbracket 1; p \rrbracket$ . Il vient

$$2\lambda_j \text{Id}_E = 0$$

Finalement, 
$$\lambda_j = 0$$

Par conséquent un  $H$ -système est libre et donc de cardinal inférieur à  $\dim \mathcal{L}(E) = n^2$ .

$$p \leq n^2$$

**I.C.2** Soit  $\mathbf{B}$  une base de  $E$ , alors l'endomorphisme

$$\phi: \begin{cases} (\mathbf{L}(E), +, \cdot, \circ) \longrightarrow (\mathbf{M}_n(\mathbb{C}), +, \cdot, \times) \\ u \longmapsto \mathbf{M}_{\mathbf{B}}(u) \end{cases}$$

est un isomorphisme d'algèbre. Soit  $(S_1, \dots, S_p)$  un  $H$ -système d'endomorphismes de  $E$ . Alors, pour tout  $i$  appartenant à  $\llbracket 1; p \rrbracket$

$$\begin{aligned} S_i \circ S_i = \text{Id}_E &\Rightarrow \phi(S_i \circ S_i) = \phi(\text{Id}_E) \\ &\Rightarrow \phi(S_i) \times \phi(S_i) = \text{I}_n \end{aligned}$$

donc, 
$$\phi(S_i)^2 = \text{I}_n$$

Pour tout  $i \neq j$  appartenant à  $\llbracket 1; p \rrbracket$

$$\begin{aligned} S_i \circ S_j + S_j \circ S_i = 0 &\Rightarrow \phi(S_i \circ S_j) + \phi(S_j \circ S_i) = \phi(0) \\ &\Rightarrow \phi(S_i) \times \phi(S_j) + \phi(S_j) \times \phi(S_i) = 0 \end{aligned}$$

Ainsi, 
$$\phi(S_i) \times \phi(S_j) + \phi(S_j) \times \phi(S_i) = 0$$

Le système  $(\phi(S_1), \dots, \phi(S_p))$  vérifie donc les équations d'un  $H$ -système de matrices de taille  $n$ .

Réciproquement, soit  $(A_1, \dots, A_p)$  un  $H$ -système de matrices de  $\mathcal{M}_n(\mathbb{C})$ . En appliquant  $\phi^{-1}$  aux équations de ce  $H$ -système on obtient de la même manière que précédemment les équations suivantes :

$$\begin{aligned} \phi^{-1}(A_i) \circ \phi^{-1}(A_i) &= \phi^{-1}(A_i^2) = \phi^{-1}(\text{I}_n) = \text{Id}_E \\ \text{et} \quad \phi^{-1}(A_i) \circ \phi^{-1}(A_j) &+ \phi^{-1}(A_j) \circ \phi^{-1}(A_i) = 0 \end{aligned}$$

Ainsi, le système  $(\phi^{-1}(A_1), \dots, \phi^{-1}(A_p))$  vérifie les équations d'un  $H$ -système d'endomorphismes de  $E$ . Par conséquent,

L'existence d'un  $H$ -système d'endomorphismes de  $E$  est équivalente à l'existence d'un  $H$ -système de matrices de taille  $n$ .

Finalement, la recherche d'un  $H$ -système d'endomorphismes de  $E$  peut se ramener à celle d'un  $H$ -système de matrices de taille  $n$  de même longueur. Comme l'existence d'un  $H$ -système de matrices ne dépend que de  $n$ , c'est donc que les longueurs possibles pour un  $H$ -système de  $E$  ne dépendent elles aussi que de  $n$ .

Les valeurs possibles pour l'entier  $p$  ne dépendent que de  $n$ .

La deuxième partie de la question semble mal tournée. En effet, la longueur d'un  $H$ -système fixé ne dépend ni de  $E$  ni de  $n$  mais du  $H$ -système lui-même. Ainsi, il faut plutôt montrer que l'existence d'un  $H$ -système de  $E$  d'une longueur donnée ne dépend pas de  $E$  mais seulement de sa dimension  $n$ . De plus cela assure l'existence de l'entier  $p(n)$  défini lors de la question suivante.

**I.C.3** Dans la question I.B.1.b, on a vu que deux symétries anticommutaient, alors, l'entier  $n$  était pair. Par conséquent, si  $n$  est impair il ne peut exister de  $H$ -système de longueur supérieure à 1. Par suite,

$$p(n) \leq 1.$$

Or l'identité est une symétrie (et forme donc un  $H$ -système de longueur 1). Ainsi,

$$p(n) \geq 1$$

Finalement,

$$p(n) = 1$$

**I.D.1.a.** Les endomorphismes  $U$  et  $T$  sont des symétries qui anticommulent, de même pour  $S_j$  et  $T$ , d'après I.B.1,

$$S_j(E_0) = S_j(F_T) = G_T \quad \text{d'où,} \quad iU \circ S_j(E_0) = iU(G_T) = F_T = E_0$$

puisque  $U$  et  $T$  anticommulent,  $iU$  et  $T$  anticommulent. Finalement,

$$R_j(E_0) = E_0$$

Le sous-espace  $E_0$  est stable par  $R_j$ .

**I.D.1.b** Effectuons tout d'abord un calcul préliminaire. Soit  $x$  appartenant à  $E_0$  et  $i, j$  tel que  $1 \leq i, j \leq p$ . Il vient,

$$\begin{aligned} s_j \circ s_i(x) &= s_j \circ R_i(x) && (R_i|_{E_0} = s_i) \\ &= R_j \circ R_i(x) && (R_j|_{E_0} = s_j) \\ &= iU \circ S_j \circ iU \circ S_i(x) \\ &= -U \circ (S_j \circ U) \circ S_i(x) \\ &= -U \circ (-U \circ S_j) \circ S_i(x) \\ &= (U \circ U) \circ (S_j \circ S_i)(x) \\ s_j \circ s_i(x) &= S_j \circ S_i(x) && (U \text{ est une symétrie}) \end{aligned}$$

De ces calculs, déduisons tout d'abord que les endomorphismes de la famille  $(s_1, \dots, s_p)$  sont des symétries.

$$s_j \circ s_j(x) = S_j \circ S_j(x) = x$$

Cette égalité pour tout  $x$  dans  $E_0$ , entraîne l'égalité des endomorphismes.

$$s_j \circ s_j = \text{Id}_{E_0}$$

Montrons ensuite que les endomorphismes de la famille  $(s_1, \dots, s_p)$  anticommulent deux à deux. Soient  $x$  appartenant à  $E_0$  et  $i \neq j$  tel que  $1 \leq i, j \leq p$ . Alors, en appliquant l'égalité préliminaire

$$s_j \circ s_i(x) = S_j \circ S_i(x)$$

Utilisons ensuite le fait que  $S_j$  et  $S_i$  anticommulent. D'où

$$S_j \circ S_i(x) = -S_i \circ S_j(x) = -s_j \circ s_i(x)$$

Ainsi,

$$s_j \circ s_i = -s_i \circ s_j$$

Finalement,

$$(s_1, \dots, s_p) \text{ est un } H\text{-système de } E_0.$$

**I.D.1.c** D'après le résultat de la question I.B.1,

$$\dim(E_0) = \dim(F_T) = \frac{n}{2} = m$$

Dans la question précédente, on a montré que  $(s_1, \dots, s_p)$  était un  $H$ -système de  $E_0$ .

$$p \leq p(m)$$

Ainsi, la longueur du  $H$ -système  $(S_1, \dots, S_p, T, U)$  de  $E$  est plus petite que  $p(m) + 2$ . Ceci étant vrai pour tout  $H$ -système de  $E$ , on a :

$$p(2m) \leq p(m) + 2$$

**I.D.2** Procédons par récurrence sur  $d$ . Montrons par récurrence que la propriété

$$\mathcal{P}(d) : \text{"Si } n = 2^d m \text{ avec } m \text{ impair, alors } p(n) \leq 2d + 1"$$

est vraie pour tout  $d \geq 0$ .

- $\mathcal{P}(0)$  : D'après la question I.C.3, si  $m$  est impair :

$$p(m) = 1$$

En particulier  $\mathcal{P}(0)$  est vraie.

- $\mathcal{P}(d) \implies \mathcal{P}(d+1)$  : D'après la question I.D.1 :

$$p(2^{d+1}m) \leq p(2^d m) + 2$$

Appliquons ensuite l'hypothèse de récurrence à  $p(2^d m)$  :

$$p(2^{d+1}m) \leq 2d + 1 + 2 \leq 2(d+1) + 1$$

Ainsi  $\mathcal{P}(d)$  est vraie.

- Conclusion :  $\forall d \geq 0, \quad p(2^d m) \leq 2d + 1$

**I.E.1** Tout d'abord, notons que les blocs des matrices  $(A_j)_{1 \leq j \leq N+2}$  sont tous de taille  $n \times n$  ; ils sont donc compatibles pour la multiplication par blocs. Justifions l'égalité  $A_j^2 = I_{2n}$  pour tout  $j$  tel que  $1 \leq j \leq N+2$ . Pour  $j$  appartenant à  $\llbracket 1 ; N \rrbracket$

$$A_j^2 = \begin{pmatrix} a_j & 0 \\ 0 & -a_j \end{pmatrix}^2 = \begin{pmatrix} a_j^2 & 0 \\ 0 & (-a_j)^2 \end{pmatrix} = I_{2n}$$

Pour  $j = N+1$ ,  $A_{N+1}^2 = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}^2 = \begin{pmatrix} I_n^2 & 0 \\ 0 & I_n^2 \end{pmatrix} = I_{2n}$

Enfin, pour  $j = N+2$  on a de même

$$A_{N+2}^2 = \begin{pmatrix} 0 & iI_n \\ -iI_n & 0 \end{pmatrix}^2 = \begin{pmatrix} -(iI_n)^2 & 0 \\ 0 & -(iI_n)^2 \end{pmatrix} = I_{2n}$$

Finalement,  $\forall j \in \llbracket 1 ; N+2 \rrbracket, A_j^2 = I_{2n}$

Montrons ensuite que  $A_i A_j + A_j A_i = 0$  pour tout  $i \neq j$  tel que  $1 \leq i, j \leq N+2$ . Dans un premier temps pour  $i, j \in \llbracket 1 ; N \rrbracket$  :

$$\begin{aligned} A_i A_j + A_j A_i &= \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix} \begin{pmatrix} a_j & 0 \\ 0 & -a_j \end{pmatrix} + \begin{pmatrix} a_j & 0 \\ 0 & -a_j \end{pmatrix} \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix} \\ &= \begin{pmatrix} a_i a_j + a_j a_i & 0 \\ 0 & a_i a_j + a_j a_i \end{pmatrix} = 0 \end{aligned}$$

car  $a_i$  et  $a_j$  anticommulent. Pour  $i \leq N, j = N+1$  :

$$\begin{aligned} A_i A_{N+1} + A_{N+1} A_i &= \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix} \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} + \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix} \\ &= \begin{pmatrix} 0 & a_i \\ -a_i & 0 \end{pmatrix} + \begin{pmatrix} 0 & -a_i \\ a_i & 0 \end{pmatrix} = 0 \end{aligned}$$

et il en est de même pour  $i \leq N, j = N+2$  :

$$\begin{aligned} A_i A_{N+2} + A_{N+2} A_i &= \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix} \begin{pmatrix} 0 & iI_n \\ -iI_n & 0 \end{pmatrix} + \begin{pmatrix} 0 & iI_n \\ -iI_n & 0 \end{pmatrix} \begin{pmatrix} a_i & 0 \\ 0 & -a_i \end{pmatrix} \\ &= \begin{pmatrix} 0 & i a_i \\ i a_i & 0 \end{pmatrix} + \begin{pmatrix} 0 & -i a_i \\ -i a_i & 0 \end{pmatrix} = 0 \end{aligned}$$

Enfin, pour  $j = N+1, i = N+2$  :

$$\begin{aligned} A_i A_j + A_j A_i &= \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} 0 & iI_n \\ -iI_n & 0 \end{pmatrix} + \begin{pmatrix} 0 & iI_n \\ -iI_n & 0 \end{pmatrix} \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \\ &= \begin{pmatrix} -iI_n & 0 \\ 0 & iI_n \end{pmatrix} + \begin{pmatrix} iI_n & 0 \\ 0 & -iI_n \end{pmatrix} \\ A_i A_j + A_j A_i &= \begin{pmatrix} iI_n - iI_n & 0 \\ 0 & iI_n - iI_n \end{pmatrix} = 0 \end{aligned}$$

Par symétrie des rôles de  $i$  et  $j$  on a bien traité tous les cas, donc,

$$\forall i, j \in \llbracket 1 ; N+2 \rrbracket, i \neq j \quad A_i A_j + A_j A_i = 0$$

Finalement,  $(A_1, \dots, A_{N+2})$  est un  $H$ -système. Or, de la définition de l'entier  $p(n)$ , il découle qu'un  $H$ -système de taille  $n$  de longueur  $N = p(n)$  existe. On en déduit qu'un  $H$ -système de taille  $2n$  de longueur  $N+2$  existe. Il vient que

$$\boxed{p(2n) \geq N+2}$$

**I.E.2** Dans la question précédente on a démontré l'inégalité inverse à celle de la question I.D.1.c. En raisonnant de la même manière par récurrence sur  $d$ , on obtient l'autre sens de l'inégalité obtenue question I.D.2. Supposons que

$$\mathcal{P}(d) : \text{"si } n = 2^d m \text{ avec } m \text{ impair, alors } p(n) \geq 2d + 1"$$

est vraie pour tout  $d \geq 0$ .

- $\mathcal{P}(0)$  : D'après la question I.C.3, si  $m$  est impair :

$$p(m) = 1$$

En particulier  $\mathcal{P}(0)$  est vraie.

- $\mathcal{P}(d) \implies \mathcal{P}(d+1)$  : d'après la question I.D.1 :

$$p(2^{d+1}m) \geq p(2^d m) + 2$$

Appliquons ensuite l'hypothèse de récurrence à  $p(2^d m)$  :

$$p(2^{d+1}m) \geq 2d + 1 + 2 \geq 2(d+1) + 1$$

donc  $\mathcal{P}(d)$  est vraie.

- Conclusion :  $\forall d \geq 0, \quad p(2^d m) \geq 2d + 1$

**I.E.3** Résumons les idées utilisées pour la construction des  $H$ -systèmes pour  $n$  appartenant à  $\{1; 2; 4\}$  :

- Comme  $I_1^2 = I_1$ , la famille  $(I_1)$  est un  $H$ -système de matrices de taille 1.
- Pour obtenir un  $H$ -système de matrices de taille 2, il suffit d'appliquer la construction de la partie I.E à l'exemple déjà construit pour  $n = 1$ .
- Pour obtenir un  $H$ -système de matrices de taille 4, il suffit d'appliquer la construction de la partie I.E à l'exemple construit pour  $n = 2$ .

On obtient ainsi

Un  $H$ -système de  $\mathcal{M}_1(\mathbb{C})$  est donné par :

$$A_1 = (1)$$

Un  $H$ -système de  $\mathcal{M}_2(\mathbb{C})$  est donné par :

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad A_3 = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

Un  $H$ -système de  $\mathcal{M}_4(\mathbb{C})$  est donné par :

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad A_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 0 & i & 0 & 0 \\ -i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix} \quad A_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad A_5 = \begin{pmatrix} 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \\ -i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix}$$