PSI* 2023/24 DL 3

Symétries, quaternions et sommes de carrés

Dans ce problème on s'intéresse aux sommes de carrés d'entiers (ou plus généralement de carrés d'éléments d'un anneau commutatif). On voit en particulier des formes pour le produit de deux sommes de n carrés pour $n = 1, 2, 4$ et 8 et on montre qu'il n'existe pas de formule analogue pour les autres valeurs de n, ce qui constitue un théorème établi par Hurwitz en 1898.

La partie I étudie des familles de symétries. La partie II introduit l'algèbre des quaternions ; pour l'essentiel elle est indépendante de la partie I. Dans la partie III on établit le théorème de Hurwitz en utilisant les parties I et II.

Travail demandé (pour le 18/10) : version minimum partie I, version standard I et II, version deluxe I-II-III.

Partie I - Symétries vectorielles

Dans cette partie on considère un espace vectoriel E de dimension finie $n \geq 1$ sur le corps $\mathbb{R}$ des réels ou le corps $\mathbb{C}$ des complexes.

Pour tout endomorphisme $u \in L(E)$ on posera $V_u^+ = \ker(u - \mathrm{Id}_E)$ et $V_u^- = \ker(u + \mathrm{Id}_E)$.

Soient F et G deux sous-espaces supplémentaires de E (ie $E = F \oplus G$). On appelle *symétrie* de E par rapport à F parallèlement à G l'endomorphisme s de E défini par

$$\forall (y, z) \in F \times G, \qquad s(y + z) = y - z$$

I.A - Symétries et involutions

I.A.1) Soient F et G deux sous-espaces supplémentaires de E et s la symétrie de E par rapport à F parallèlement à G.

a. Montrer que $V_s^+ = F$ et $V_s^- = G$.

b. Montrer que $s \circ s = \mathrm{Id}_E$. En déduire que s est un automorphisme de E.

c. Déterminer les valeurs propres et les sous-espaces propres de s. On discutera selon les sous-espaces F et G.

I.A.2) Soit s un endomorphisme de E tel que $s \circ s = \mathrm{Id}_E$. On pose $F = \ker(s - \mathrm{Id}_E)$ et $G = \ker(s + \mathrm{Id}_E)$.

a. Montrer que F et G sont deux sous-espaces supplémentaires de E.

b. En déduire que s est une symétrie dont on précisera les éléments.

I.B - Couples de symétries qui anticommutent

I.B.1) On suppose que s et t sont deux symétries et qu'elles anticommutent, c'est-à-dire que $s \circ t + t \circ s = 0$.

a. Prouver que V_s^+ et V_s^- vérifient les propriétés suivantes

— les égalités $t(V_s^+) = V_s^-$ et $t(V_s^-) = V_s^+$,

— l'égalité de dimension : $\dim V_s^+ = \dim V_s^-$

b. En déduire que n est pair.

I.C - H-systèmes

On appelle *H-système* d'endomorphismes de E toute famille finie de symétries de E qui anticommutent deux à deux, c'est-à-dire toute famille finie $(S_1, \dots, S_p)$ d'endomorphismes de E tels que

$$\begin{cases} \forall i & S_i \circ S_i = \mathrm{Id}_E \\ \forall i \neq j & S_i \circ S_j + S_j \circ S_i = 0 \end{cases}$$

De même, on appelle *H-système* de matrices de taille n toute famille finie $(A_1, \dots, A_p)$ de matrices de $\mathcal{M}_n(\mathbb{C})$ telles que

$$\begin{cases} \forall i & A_i^2 = \mathrm{I}_n \\ \forall i \neq j & A_i A_j + A_j A_i = 0 \end{cases}$$

Dans les deux cas, p est appelé *longueur* du H-système. On rappelle que $\dim E = n$.

I.C.1) Montrer que la longueur p d'un H-système d'endomorphismes de E est majorée par n^2.

I.C.2) Montrer que l'existence d'un H-système $(S_1, \dots S_p)$ d'endomorphismes de E équivaut à l'existence d'un H-système $(A_1, \dots, A_p)$ de matrices de taille n. En déduire que la longueur d'un H-système de E ne dépend que de la dimension n de E et pas de l'espace E (*pas ma faute, c'était écrit comme ça dans le sujet*[1]).

• **Dorénavant, on notera $p(n)$ le plus grand nombre entier $p \geq 1$ tel que E admet un H-système de longueur p.**

I.C.3. Soit n un entier impair. Prouver que $p(n) = 1$.

I.D - Majoration de $p(n)$.

I.D.1. On suppose ici que n est pair et on pose $n = 2m$. On considère

- un H-système $(S_1, \dots, S_p, T, U)$ de E,

- le sous-espace $E_0 = V_T^+ = \ker(T - \mathrm{Id})$,

- pour $j \in [\![1, p]\!]$, l'endomorphisme $R_j = iU \circ S_j$ de E *(il s'agit bien du $i \in \mathbb{C}$ tel que $i^2 = -1$)*

a. Montrer que pour tout $j \in [\![1, p]\!]$, le sous-espace E_0 est stable par R_j. On peut donc introduire s_j, endomorphisme de E_0 induit par R_j :

$$\begin{array}{rccc} s_j & : & E_0 & \longrightarrow & E_0 \\ & & x & \longmapsto & s_j(x) = R_j(x) \end{array}$$

b. Montrer que $(s_1, \dots, s_p)$ est un H-système de E_0.

c. En déduire que $p(2m) \leq p(m) + 2$.

I.D.2. Montrer que si $n = 2^d m$ avec m impair, $p(n) \leq 2d + 1$.

I.E - Constructions de H-systèmes maximaux.

I.E.1. Soient $N = p(n)$ et $(a_1, \dots, a_N)$ un H-système de matrices de taille n c'est-à-dire tel que

$$\forall i, a_i^2 = \mathrm{I}_n, \qquad \forall i \neq j, \ \ a_i a_j + a_j a_i = 0$$

En considérant les matrices suivantes de $\mathcal{M}_{2n}(\mathbb{C})$ écrites par blocs

$$A_j = \begin{pmatrix} a_j & 0 \\ 0 & -a_j \end{pmatrix}, (j \in [\![1, N]\!]), \qquad A_{N+1} = \begin{pmatrix} 0 & \mathrm{I}_n \\ \mathrm{I}_n & 0 \end{pmatrix}, \qquad A_{N+2} = \begin{pmatrix} 0 & i\,\mathrm{I}_n \\ -i\,\mathrm{I}_n & 0 \end{pmatrix},$$

montrer que $p(2n) \geq N + 2$.

I.E.2. Déterminer $p(n)$ en fonction de l'unique entier $d \in \mathbb{N}$ tel que n s'écrive $n = 2^d m$ avec m impair.

I.E.3. Ecrire pour chacun des entiers $n = 1, 2, 4$, un H-système de matrices de taille n et de longueur $p(n)$.

1. Cette formulation est mauvaise. L'énoncé demandait sans doute de montrer que l'ensemble des longueurs possibles des H-systèmes de E ne dépend que de la dimension de E.

Partie II - Quaternions, sommes de quatre carrés

Pour deux complexes a et b, on désigne par $M(a,b)$ la matrice $M(a,b) = \begin{pmatrix} a & -b \\ \overline{b} & \overline{a} \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$. Une matrice de la forme $M(a,b)$ sera appelée *quaternion*. On note $\mathbb{H} = \{M(a,b), (a,b) \in \mathbb{C}^2\}$ l'ensemble de tous les quaternions et on considère en particulier les quaternions

$$e = \mathrm{I}_2 = M(1,0), \qquad I = M(0,1), \qquad J = M(i,0), \qquad K = M(0,-i)$$

On veillera à ne pas confondre la matrice $I = M(0,1)$ et la matrice identité qui sera plutôt notée $e = \mathrm{I}_2 = M(1,0)$.

II.A - Le "corps" des quaternions.

II.A.1. a. Quelle est la dimension de $\mathcal{M}_2(\mathbb{C})$ en tant qu'espace vectoriel sur le corps $\mathbb{C}$ des complexes ? Quelle est sa dimension en tant qu'espace vectoriel sur le corps $\mathbb{R}$ des réels (on répondra en donnant directement la valeur, sans justification supplémentaire) ?

b. Montrer que $\mathbb{H}$ est un sous-espace vectoriel de l'espace vectoriel $\mathcal{M}_2(\mathbb{C})$, tous ces espaces étant vus comme espaces vectoriels sur $\mathbb{R}$. Montrer que $\mathbb{H}$ admet alors pour base (e, I, J, K).
Est-ce que $\mathbb{H}$ est également un espace vectoriel sur $\mathbb{C}$?

II.A.2. Montrer que $\mathbb{H}$ est stable par multiplication.

II.A.3. Montrer que l'application $\mathbb{H} \times \mathbb{H}$ dans $\mathbb{H}$ qui à deux quaternions associe leur produit $((q,q') \mapsto qq')$ est bilinéaire (en considérant toujours $\mathbb{H}$ comme un espace vectoriel réel).

II.A.4. Montrer que si $q \in \mathbb{H}$, $q \neq 0$, alors q est inversible et admet un inverse dans $\mathbb{H}$.

Remarque : $(\mathbb{H}, +, \times)$ *posssède en fait les propriétés usuelles d'un corps, sans la commutativité de* $\times$.

II.B - Conjugaison et sommes de quatre carrés.

Ainsi tout élément $q \in \mathbb{H}$ s'écrit de manière unique $q = xe + yI + zJ + tK$ avec x, y, z, t dans $\mathbb{R}$.
En outre, pour tout x, y, z, t dans $\mathbb{R}$ et $q = xe + yI + zJ + tK$, on pose $q^* = xe - yI - zJ - tK$ et $N(q) = x^2 + y^2 + z^2 + t^2 \in \mathbb{R}_+$.

II.B.1. a. Vérifier que, pour tout $q \in \mathbb{H}$, q^* est la transposée de la matrice dont les coefficients sont les conjugués des coefficients de q.

b. En déduire, pour tous $(q,r) \in \mathbb{H}^2$, $(qr)^* = r^* q^*$.

c. Montrer que $(q^*)^* = q$ et prouver que l'application $\mathcal{S} : q \mapsto q^*$ est un automorphisme du $\mathbb{R}$-espace vectoriel $\mathbb{H}$.

d. Pour $q \in \mathbb{H}$, exprimer qq^* à l'aide de $N(q)$. En déduire la relation suivante

$$\forall (q,r) \in \mathbb{H}^2, \qquad N(qr) = N(q)N(r)$$

II.B.2. a. Soient $(x, y, z, t) \in \mathbb{R}^4$ et $q = xe + yI + zJ + tK$. Exprimer la trace de la matrice $q \in \mathcal{M}_2(\mathbb{C})$ en fonction du réel x. Quel est le noyau de $\mathcal{S} + \mathrm{Id}_{\mathbb{H}}$?

b. En déduire, pour tous q_1, q_2 dans $\mathbb{H}$, $q_1 q_2 - q_2 q_1 = q_1^* q_2^* - q_2^* q_1^*$.

c. Soient a, b, c, d des quaternions. Etablir la relation

$$(acb^*)d + d^*(acb^*)^* = (acb^*)^* d^* + d(acb^*)$$

En déduire l'identité

$$(N(a) + N(b))(N(c) + N(d)) = N(ac - d^* b) + N(bc^* + da)$$

Partie III - Un théorème de Hurwitz

Soit un entier naturel $n \geq 1$. On munit $\mathbb{R}^n$ (identifié à l'espace $\mathcal{M}_{n,1}(\mathbb{R})$ des matrices colonnes de taille n), du produit scalaire et de la norme euclidienne usuels définis pour tout $X = (x_1, \ldots, x_n)$ et tout $Y = (y_1, \ldots, y_n)$ de $\mathbb{R}^n$ par

$$(X|Y) = X^\top Y = \sum_{k=1}^{n} x_k y_k \qquad \|X\| = \sqrt{\sum_{k=1}^{n} x_k^2}$$

L'objet de cette partie est d'étudier l'existence d'une application bilinéaire

$$B_n : (\mathbb{R}^n)^2 \longrightarrow \mathbb{R}^n$$

vérifiant

$$\forall (X,Y) \in (\mathbb{R}^n)^2, \qquad \|B_n(X,Y)\| = \|X\| \times \|Y\|$$

III.A - Des formules pour $n = 1, 2, 4, 8$.

III.A.1. On se place pour $n = 2$, en assimilant $\mathbb{C}$ à l'espace vectoriel réel $\mathbb{R}^2$. On considère l'application B_2 qui aux vecteurs $X = (x_1, x_2)$ et $Y = (y_1, y_2)$ associe le vecteur dont l'affixe est le produit des affixes de X et Y : $XY = (x_1 + ix_2)(y_1 + iy_2)$. Montrer que cette application est bilinéaire (NB : le corps des scalaires est $\mathbb{R}$) et vérifie les propriétés demandées.

III.A.2. Montrer que pour $n = 1$ et $n = 4$ il existe également une application bilinéaire convenable (pour $n = 4$ on pourra utiliser le produit de deux quaternions).

III.A.3. En utilisant l'identité obtenue à la question IIB2c, exhiber une application bilinéaire B_8 vérifiant les propriétés demandées.

III.B - Le théorème de Hurwitz

Dans la suite on suppose que $n \geq 3$ et qu'il existe une application bilinéaire B vérifiant

$$\forall (X,Y) \in (\mathbb{R}^n)^2, \qquad \|B(X,Y)\| = \|X\| \times \|Y\|$$

Soit $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$, et pour $i \in [\![1, n]\!]$, soit u_i l'application donnée par

$$\forall X \in \mathbb{R}^n, \qquad u_i(X) = B(X, e_i) \in \mathbb{R}^n$$

L'application u_i ainsi introduite est donc un endomorphisme de $\mathbb{R}^n$. On notera A_i la matrice de u_i dans la base canonique.

III.B.1.a. Pour X et Y dans $\mathbb{R}^n$, comment obtenir une expression de $(X|Y)$ à l'aide de $\|X + Y\|$ et $\|X - Y\|$?

b. Prouver quer pour tout $X \in \mathbb{R}^n$, on a

$$\forall Y = (y_1, \ldots, y_n) \in \mathbb{R}^n, \qquad \sum_{1 \leq i,j \leq n} y_i y_j (u_i(X)|u_j(X)) = \|X\|^2 \sum_{i=1}^{n} y_i^2$$

c. En déduire que les endomorphismes u_i vérifient les relations

$$\forall X \in \mathbb{R}^n, \begin{cases} \forall i & \|u_i(X)\| = \|X\| \\ \forall i \neq j & (u_i(X)|u_j(X)) = 0 \end{cases}$$

d. Montrer plus généralement les relations

$$\forall (X, X') \in (\mathbb{R}^n)^2, \qquad \begin{cases} \forall i & (u_i(X)|u_i(X') = (X|X') \\ \forall i \neq j & (u_i(X)|u_j(X')) + (u_j(X)|u_i(X')) = 0 \end{cases}$$

e. Montrer que les matrices A_i vérifient les relations

$$\begin{cases} \forall i & A_i^\top A_i = \mathrm{I}_n \\ \forall i \neq j & A_i^\top A_j + A_j^\top A_i = 0 \end{cases}$$

III.B.2. Pour $j = 1, 2, \ldots, n-1$ on note S_j la matrice complexe $S_j = iA_n^\top A_j$.

a. Prouver que $(S_1, \ldots, S_{n-1})$ est un H-système.

b. En déduire qu'on a l'inégalité $p(n) \geq n - 1$, en reprenant la notation $p(n)$ de la section I.C.

III.B.3. Prouver que n est un élément de $\{1, 2, 4, 8\}$.

III.C - Sommes de carrés

Pour p valant 1,2,4 ou 8, on note C_p l'ensemble des sommes de p carrés d'éléments de $\mathbb{Z}$. Montrer que C_p est stable pour la multiplication.