CONCOURS CENTRALE•SUPÉLEC

Mathématiques 2

PC

2014

4 heures Calculatrices autorisées

Symétries, quaternions et sommes de carrés

Dans ce problème, on s'intéresse aux sommes de carrés d'éléments dans un anneau commutatif. On voit en particulier des formules pour le produit de deux sommes de n carrés pour $n = 1$ 2, 4 et 8, et on démontre 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. Dans la partie IV, on étudie le théorème des quatre carrés d'un point de vue algorithmique. Dans la partie V, on démontre le théorème des quatre carrés en s'appuyant sur la partie II.

I Symétries vectorielles

Dans cette partie, on considère un espace vectoriel E de dimension finie $n \geqslant 1$ sur le corps $\mathbb{C}$ des nombres complexes.

Soient F et G deux sous-espaces supplémentaires de E (i.e. $E = F \oplus G$). On appelle *symétrie* (vectorielle) de E par rapport à F parallèlement à G l'endomorphisme s de E défini par $\forall (y,z) \in F \times G,\ s(y+z) = y - z$.

Pour tout endomorphisme u de E, on pose $F_u = \mathrm{Ker}(u - \mathrm{Id}_E)$ et $G_u = \mathrm{Ker}(u + \mathrm{Id}_E)$.

I.A – Symétries et involutions

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

a) Montrer que $F = F_s$ et $G = G_s$.

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 $F = \mathrm{Ker}(s - \mathrm{Id}_E)$ et $G = \mathrm{Ker}(s + \mathrm{Id}_E)$.

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) Soient s et t deux symétries de E qui anticommutent, c'est-à-dire telles que $s \circ t + t \circ s = 0$.

a) Prouver les égalités $t(F_s) = G_s$ et $t(G_s) = F_s$.

b) En déduire que F_s et G_s ont la même dimension et 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 $(S_1, ..., S_p)$ 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 $(A_1, ..., A_p)$ de matrices de $\mathcal{M}_n(\mathbb{C})$ telles que

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

Dans les deux cas, p est appelé *longueur* du H-système.

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 $(S_1, ..., S_p)$ de E équivaut à l'existence d'un H-système 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.

On note $p(n)$ le plus grand nombre entier $p \geqslant 1$ tel que E admet un H-système de cardinal 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 $(S_1, ..., S_p, T, U)$ de E,
– le sous-espace $E_0 = F_T = \mathrm{Ker}(T - \mathrm{Id})$,
– pour $j \in [\![1, p]\!]$, l'endomorphisme $R_j = \mathrm{i}U \circ S_j$ de E.

a) Montrer que, pour tout $j \in [\![1, p]\!]$, le sous-espace E_0 est stable par R_j.

b) Pour $j \in [\![1, p]\!]$, soit s_j l'endomorphisme de E_0 induit par R_j. Montrer que $(s_1, ..., s_p)$ est un H-système de E_0.

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

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

I.E – Constructions de H-systèmes maximaux

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

$$\forall i,\ a_i^2 = I_n \qquad \text{et} \qquad \forall i \neq j,\ a_i a_j + a_j a_i = 0$$

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

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

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

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) Écrire, pour chacun des entiers $n = 1$, 2, 4, un H-système de matrices de taille n de longueur $p(n)$.