MP* Lycée Kérichen **2020-2021**

DM bis n°15

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.

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

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 $(S_1, \ldots, S_p)$ 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 $(A_1, \ldots, A_p)$ de matrices de $\mathcal{M}_n(\mathbb{C})$ telles que

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

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 $(S_1, \ldots, S_p)$ 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 $(S_1, \dots, S_p, T, U)$ de E,
— le sous-espace $E_0 = F_T = \mathrm{Ker}(F - \mathrm{id})$,
— 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 $(s_1, \dots, s_p)$ 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 Construction 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

$$\forall i,\ a_i^2 = \mathrm{id}_E \quad \text{et} \quad \forall i \neq j,\ a_i a_j + a_j a_i = 0.$$

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

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

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 $p(n)$.

Partie II – Quaternions et sommes de carrés

Pour $(a, b) \in \mathbb{C}^2$, on désigne par $M(a, b)$ la matrice carrée complexe $M(a, b) = \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$.

Une matrice de la forme $M(a, b)$ sera appelée *quaternion*. On considèrera en particulier les quaternions $e = I_2 = M(1, 0)$, $I = M(0, 1)$, $J = M(\mathrm{i}, 0)$, $K = M(0, \mathrm{i})$ et on notera $\mathbb{H} = \{M(a, b) \mid (a, b) \in \mathbb{C}^2\}$ le sous-ensemble de $\mathcal{M}_2(\mathbb{C})$ constitué par tous les quaternions.

On veillera à ne pas confondre la matrice $I = M(0, 1)$ et la matrice unité $I_2 = e = M(1, 0)$.

II.A Le « corps » des quaternions

On munit l'ensemble $\mathcal{C} = \mathcal{M}_2(\mathbb{C})$ des matrices complexes à deux lignes et deux colonnes de l'addition $+$, de la multiplication $\times$ usuelles et de la multiplication par un réel notée $\cdot$ et définie usuellement par

$$\forall \lambda \in \mathbb{R}, \quad \forall M = \begin{pmatrix} a & b \\ c & a \end{pmatrix} \in \mathcal{C}, \quad \lambda \cdot M = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda a \end{pmatrix}$$

On rappelle que $(\mathcal{C}, +, \times, \cdot)$ est une algèbre sur le corps $\mathbb{R}$ des réels.

II.A.1 (a) Donner, sans justification, une base et la dimension de $\mathcal{C}$ sur le corps $\mathbb{R}$.

(b) Montrer que $\mathbb{H}$ est un sous-espace vectoriel réel de $\mathcal{C}$ et que $\{e, I, J, K\}$ en est une base sur le corps $\mathbb{R}$.

(c) Montrer que $\mathbb{H}$ est stable par multiplication.

II.A.2 Montrer que $(\mathbb{H} \setminus \{0\}, \times)$ est un sous-groupe non commutatif du groupe linéaire $(\mathrm{GL}_2(\mathbb{C}), \times)$.
$(\mathbb{H}, +, \times)$ a toutes les propriétés d'un corps sauf la commutativité de $\times$: on dit que c'est un *anneau à divisions* (ou, parfois, un *corps non commutatif*).

II.A.3 (a) Calculer les produits deux à deux des matrices e, I, J, K. On présentera les résultats dans une table à double entrée.

(b) En déduire que $(\mathrm{i}I, \mathrm{i}J, \mathrm{i}K)$ est un H-système.

II.B Conjugaison et normes

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

(c) Montrer que $q^{**} = q$ pour tout $q \in \mathbb{H}$ et que $q \mapsto q^*$ 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 valable pour tout $(q,r) \in \mathbb{H}^2$

$$N(qr) = N(q)N(r)$$

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.

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

(c) Soient a,b,c,d des quaternions. Établir la relation $(acb^*)d + d^*(acb^*)^* = (acb^*)^*d^* + d(acb^*)$.
En déduire l'identité $(N(a)+N(b))(N?' + N(d)) = N(ac - d^*b) + N(bc^* + da)$.

Partie III – Un théorème de Hurwitz

Soit un entier naturel $n \geqslant 1$. On munit $\mathbb{R}^n$ du produit scalaire usuel et de la norme euclidienne usuelle définis, pour tout $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ de $\mathbb{R}^n$, par

$$(X|Y) = \sum_{k=1}^{n} x_k y_k \quad \text{et} \quad \|X\| = \sqrt{\sum_{k=1}^{n} x_k^2}$$

L'objet de cette partie est d'étudier l'existence d'une application bilinéaire $B_n \colon (\mathbb{R}^n)^2 \to \mathbb{R}^n$ vérifiant

$$\forall X, Y \in \mathbb{R}^n, \quad \|B_n(X,Y)\| = \|X\|\,\|Y\| \tag{III.1}$$

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

III.A.1 Montrer l'existence d'une telle application bilinéaire B_n lorsque n est l'un des entiers 1, 2, 4.
Pour $n = 2$ (respectivement 4) on pourra considérer le produit de deux nombres complexes (respectivement de deux quaternions).

III.A.2 En utilisant la question II.B.2 montrer, pour $n = 8$, l'existence d'une application bilinéaire vérifiant (III.1). On ne demande pas d'expliciter une application bilinéaire B_8, mais seulement de prouver son existence.

III.B Le théorème de Hurwitz

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

$$\forall X, Y \in \mathbb{R}^n, \quad \|X\|\,\|Y\| = \|B(X,Y)\| \tag{III.2}$$

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

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

La matrice de u_i dans la base canonique de $\mathbb{R}^n$ sera notée A_i.

III.B.1 (a) Prouver que, pour tout $X \in \mathbb{R}^n$, on a

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

(b) En déduire que les endomorphismes u_i vérifient les relations

$$\forall i,j = 1, \ldots, n, \quad \forall X \in \mathbb{R}^n, \quad \|u_i(X)\| = \|X\| \quad \text{et} \quad i \neq j \Rightarrow (u_i(X)|u_j(X)) = 0$$

et plus généralement

$$\forall i,j = 1, \ldots, n, \quad \forall X, X' \in \mathbb{R}^n, \quad (u_i(X)|u_i(X')) = (X|X') \quad \text{et} \quad i \neq j \Rightarrow (u_i(X)|u_j(X')) + (u_j(X)|u_i(X')) = 0$$

(c) Prouver que les matrices A_j vérifient les relations $\forall i,j = 1, \ldots, n$, ${}^tA_iA_i = I_n$ et $i \neq j \Rightarrow {}^tA_iA_j + {}^tA_jA_i = 0$.

III.B.2 Pour $j = 1, \ldots, n-1$ on note S_j la matrice complexe $S_j = \mathrm{i}\,{}^tA_nA_j$.

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

(b) En déduire qu'on a l'inégalité $p(n) \geqslant n - 1$ où $p(n)$ est défini dans la section I.C.

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

Partie IV – Représentation des parties de $\mathbb{N}$ et quelques algorithmes

Soient X et Y deux parties de $\mathbb{N}$. On note $X+Y$ l'ensemble des sommes d'un élément de X et d'un élément de Y, c'est-à-dire $X+Y=\{x+y|x\in X, y\in Y\}\subset\mathbb{N}$.

Dans les questions suivantes, on supposera que les parties X et Y considérées contiennent 0 de sorte que $X+Y$ contiendra toujours X et Y.

Soit $N\in\mathbb{N}$. On représente une partie X de $[\![0,N]\!]$ par le tableau A indexé de 0 à N, tel que, pour $i\in[\![0,N]\!]$, on ait $A[i]=1$ si $i\in X$, $A[i]=0$ sinon.

IV.A Écrire en langage Maple ou Mathematica une fonction ou une procédure carres telle que, pour $N\in\mathbb{N}^*$, `carres(N)` retourne le tableau associé à l'ensemble des carrés inférieurs ou égaux à N. On n'utilisera pas la fonction racine carrée.

On note $\mathcal{P}=\{1,2,3,5,7,\ldots\}\subset\mathbb{N}$ la réunion de $\{1\}$ et de l'ensemble des nombres premiers.

Le crible d'Ératosthène est l'algorithme qui, dans un tableau des entiers de 1 à N, consiste à :
— à l'étape 1, supprimer les multiples de 2 strictement supérieurs à 2 ;
— à l'étape 2, supprimer les multiples de 3 strictement supérieurs à 3 ;
— à l'étape k, supprimer les multiples stricts du plus petit entier p_k qui n'a pas encore été supprimé.

À la fin du processus, les entiers supérieurs ou égaux à 2 qui n'ont pas été supprimés sont les nombres premiers inférieurs ou égaux à N. (On ne demande pas de justifier ce résultat.)

IV.B Écrire en langage Maple ou Mathematica une fonction ou une procédure `Eratosthene` utilisant l'algorithme ci-dessus et telle que, pour $N\in\mathbb{N}^*$, `Eratosthene(N)` retourne le tableau C associé à l'ensemble $X=\{p\in\mathcal{P}\,|\,p\leqslant N\}\cup\{0\}$. On rappelle que C est un tableau de 0 et de 1, indexé de 0 à N et caractérisé par

$$C[i]=1 \iff i=0 \quad\text{ou}\quad (1\leqslant i\leqslant N \text{ et } N \text{ est premier})$$

IV.C Écrire en langage Maple ou Mathematica une fonction ou une procédure somme telle que, si A et B sont des tableaux de 0 et de 1 indexés de 0 à N représentant respectivement les parties X et Y de $\{0,\ldots,N\}$, `somme(A,B,N)` retourne le tableau C représentant l'ensemble Z des éléments de $\{1,\ldots,N\}$ sommes d'un élément de X et d'un élément de Y.

IV.D En utilisant les fonctions ou les procédures `carres` et `somme`, écrire en langage `Maple` ou `Mathematica` une fonction ou une procédure `quatrecarres` telle que `quatrecarres(N)` retourne vrai si tout entier de 1 à N est somme de quatre carrés d'entiers et retourne faux sinon.

Partie V – Sommes de carrés dans un anneau

V.A Soit $(A,+,\times)$ un anneau commutatif. Pour $p\in\mathbb{N}^*$, on note $C_p(A)$ l'ensemble des sommes de p carrés d'éléments de A. Prouver que pour tout anneau A, les ensembles $C_p(A)$ sont stables pour la multiplication lorsque p vaut 1, 2, 4 ou 8.

On pourra utiliser les formes bilinéaires B_p définies partie III et, éventuellement, se limiter au cas où l'anneau A est l'anneau $\mathbb{Z}$ des entiers relatifs.

V.B Le théorème des quatre carrés

On note $\mathbb{G}=\{xe+yI+zJ+tK\,|\,x,y,z,t\in\mathbb{Z}\}$ l'ensemble des quaternions « entiers ».

V.B.1 (a) Montrer que $\mathbb{G}$ est un sous-groupe de $\mathbb{H}$ pour l'addition et qu'il est stable par multiplication.

(b) Montrer que pour tout $q\in\mathbb{H}$, il existe $\mu\in\mathbb{G}$ tel que $N(q-\mu)\leqslant 1$.

(c) Quel est l'ensemble des $q\in\mathbb{H}$ tels que $\forall\mu\in\mathbb{G},\ N(q-\mu)\geqslant 1$?

V.B.2 Soit p un nombre premier impair. Pour tout entier $r\in\mathbb{Z}$, on note $\varphi(r)$ le reste de la division euclidienne de r^2 par p. On a donc $0\leqslant\varphi(r)\leqslant p-1$ et $r^2-\varphi(r)\in p\mathbb{Z}$.

(a) Montrer que la restriction de φ à $\{0,\ldots,\frac{p-1}{2}\}$ est injective.

(b) On considère les ensembles $X=\{p-\varphi(r)\,|\,0\leqslant r\leqslant\frac{p-1}{2}\}$ et $Y=\{\varphi(s)+1\,|\,0\leqslant s\leqslant\frac{p-1}{2}\}$.
Montrer que X et Y sont inclus dans $\{1,\ldots,p\}$ et que leur intersection est non vide. En déduire qu'il existe $u,v\in\{0,\ldots,\frac{p-1}{2}\}$ et $m\in\{1,\ldots,p-1\}$ tels que $u^2+v^2+1=mp$.

V.B.3 On suppose encore que p est un nombre premier impair. Justifier qu'il existe $m\in\{1,\ldots,p-1\}$ et $\mu=xe+yI+zJ+tK\in\mathbb{H}\setminus\{0\}$ tels que $N(\mu)=mp$. On choisit m minimal et on suppose que $m>1$.

(a) Montrer que si m était pair, un nombre pair des entiers x,y,z,t serait impair et aboutir à une contradiction.

On pourra écrire $(\frac{x-y}{2})^2+(\frac{x+y}{2})^2=\frac{x^2+y^2}{2}$.

(b) On suppose m impair. Montrer qu'il existe $\nu\in\mathbb{G}$ tel que $N(\mu-m\nu)<m^2$.

(c) Prouver que $\mu'=\frac{1}{m}\mu(\mu-m\nu)^*$ est dans $\mathbb{G}\setminus\{0\}$ et que $N(\mu')$ est un multiple de p strictement inférieur à mp. Conclure.

V.B.4 Montrer que tout entier naturel est somme de quatre carrés d'entiers.