SPÉCIALE MP* : DEVOIR SURVEILLÉ

Soit n un entier naturel supérieur ou égal à 2 ; soit $(e_1, e_2, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$. $\mathbb{R}^n$ est muni d'une structure d'espace vectoriel euclidien grâce au produit scalaire $(x|y)$ défini par la relation

$$(x|y) = \sum_{i=1}^{n} x_i y_i = X^{\mathrm{T}} Y \ ;$$

x et y sont deux vecteurs de $\mathbb{R}^n$ de coordonnées respectives $(x_i)_{i\in[1,n]}$ et $(y_i)_{i\in[1,n]}$; X et Y désignent les matrices colonnes associées aux vecteurs x et y.

Soit $\mathbb{Z}^n$ le sous-ensemble des vecteurs de x de $\mathbb{R}^n$ dont les coordonnées dans la base canonique sont toutes des entiers relatifs :

$$\mathbb{Z}^n = \{x \mid x \in \mathbb{R}^n,\ x = (x_i)_{i\in[1,n]},\ x_i \in \mathbb{Z}\}.$$

Par définition une "base" de l'ensemble $\mathbb{Z}^n$ est une suite $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ de vecteurs tels que

(*i*) La suite $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ est une base de $\mathbb{R}^n$.
(*ii*) Chaque vecteur ε_i, $i \in [1, n]$ appartient à $\mathbb{Z}^n$.
(*iii*) Tout vecteur x appartenant à $\mathbb{Z}^n$ est une combinaison linéaire des vecteurs ε_i, $i \in [1, n]$:

$$x = \sum_{i=1}^{n} x_i \varepsilon_i$$

où les coefficients x_i, $i \in [1, n]$ sont des entiers relatifs.

Soit M une matrice appartenant à $\mathcal{M}(n;\mathbb{R})$, on note $M = (m_{ij})$ où i désigne la ligne et j la colonne. Le sous-ensemble des matrices réelles d'ordre n inversible est noté $\mathrm{GL}(n;\mathbb{R})$.

Soit $\mathcal{M}(n;\mathbb{Z})$ l'ensemble des matrices carrées d'ordre n dont les coefficients sont des entiers relatifs, on note $\mathrm{GL}(n;\mathbb{Z})$ le sous-ensemble des matrices inversibles de $\mathcal{M}(n;\mathbb{Z})$ dont l'inverse appartient à $\mathcal{M}(n;\mathbb{Z})$:

$$\mathrm{GL}(n;\mathbb{Z}) = \{M \mid M \in \mathcal{M}(n;\mathbb{Z}) \cap \mathrm{GL}(n;\mathbb{R}) \text{ et } M^{-1} \in \mathcal{M}(n;\mathbb{Z})\}.$$

Notation : soient A, B,... des matrices appartenant à $\mathcal{M}(n;\mathbb{R})$, les endomorphismes de $\mathbb{R}^n$ associés à ces matrices dans la base canonique de $\mathbb{R}^n$ sont notés a, b,...

Soit $\mathcal{S}^+(n;\mathbb{R})$ l'ensemble des matrices symétriques $A \in \mathcal{M}(n;\mathbb{R})$ telles que la forme quadratique associée $q(x) = (x|a(x)) = X^{\mathrm{T}} A X$ définisse un produit scalaire.

Le but du problème est d'établir, pour une matrice A de $\mathcal{S}^+(n;\mathbb{R})$, une relation entre le minimum $m(A)$ de la forme quadratique $q(x)$ définie ci-dessus, lorsque x est un vecteur appartenant à $\mathbb{Z}^n$ différent du vecteur nul (noté 0), et le déterminant de la matrice A. Cette relation est connue sous le nom de relation d'Hermite.

Première partie : construction d'une base de $\mathbb{Z}^n$

I.1. Déterminant d'une matrice de $\mathrm{GL}(n;\mathbb{Z})$:
Soit M une matrice appartenant à $\mathcal{M}(n,\mathbb{Z})$; démontrer que, pour que cette matrice M appartienne à l'ensemble $\mathrm{GL}(n;\mathbb{Z})$, il faut et il suffit que $\det M = \pm 1$.

I.2. Un résultat préliminaire :
Soit P l'application de $\mathbb{Z}\times\mathbb{Z}$ dans $\mathbb{Z}$ qui, à deux entiers relatifs a et b associe l'entier $P(a,b)$ égal :

- au P.G.C.D. de a et b s'ils sont tous les deux différents de 0,
- à l'entier relatif a ou b lorsque respectivement b ou a est nul i.e.

$$P(a,0) = a,\ P(0,b) = b,\ P(0,0) = 0.$$

Soit x un vecteur appartenant à $\mathbb{Z}^2$ de coordonnées a et b. Établir l'existence d'un endomorphisme v de $\mathbb{R}^2$ associé à une matrice V, appartenant à $\mathrm{GL}(2;\mathbb{Z})$, telle que l'image du vecteur x par l'endomorphisme v soit le vecteur de coordonnées $(d,0)$ où d est l'entier $P(a,b)$: $V\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}d\\0\end{pmatrix}$, on posera $V=\begin{pmatrix}\alpha & \beta\\ \alpha' & \beta'\end{pmatrix}$.

I.3. Recherche de "base" dans $\mathbb{Z}^n$:

Soit $x=(x_i)_{i\in[1,n]}$ un vecteur de $\mathbb{Z}^n$, différent de 0, dont les coordonnées différentes de 0 sont des entiers premiers entre eux dans leur ensemble.

a. L'entier n est égal à deux : démontrer qu'il existe un endomorphisme u de matrice U appartenant à $\mathrm{GL}(2;\mathbb{Z})$ tel que le vecteur x soit l'image du vecteur e_1 par u : $x=u(e_1)$.
En déduire qu'il existe un vecteur $y\in\mathbb{Z}^2$ tel que la famille (x,y) soit une "base" de $\mathbb{Z}^2$.

b. L'entier n est supérieur ou égal à 3 : soit $(d_i)_{i\in[1,n]}$ la suite des entiers définis par les relations suivantes :
- $d_{n-1}=P(x_n,x_{n-1})$;
- pour tout entier $1\leqslant i\leqslant n-2$, $d_i=P(d_{i+1},x_i)$.

Pour tout entier k compris entre 1 et $n-1$, y^k est le vecteur dont les coordonnées sont $x_1,x_2,\dots,x_{k-1},d_k,0,\dots,0$.
Démontrer l'existence d'un endomorphisme v_{n-1} tel que $v_{n-1}(x)=y^{n-1}$ (de coordonnées $x_1,x_2,\dots,x_{n-2},d_{n-1},0$).
Démontrer, pour tout entier k, l'existence d'un endomorphisme v_k de matrice V_k appartenant à $\mathrm{GL}(n;\mathbb{Z})$ telle que l'image du vecteur x par l'endomorphisme v_k, soit le vecteur y_k : $v_k(x)=y^k$.
En déduire l'existence d'un endomorphisme u de matrice U appartenant à $\mathrm{GL}(n;\mathbb{Z})$ tel que la relation $x=u(e_1)$ ait lieu.

c. Démontrer qu'il existe $n-1$ vecteurs $z^2,z^3,\dots,z^n$ tels que la famille $(x,z^2,z^3,\dots,z^n)$ soit une "base" de $\mathbb{Z}^n$.

Deuxième partie : Matrices $\mathbb{Z}$-congruentes

Deux matrices A et B appartenant à $\mathcal{M}(n;\mathbb{R})$ sont dites $\mathbb{Z}$-congruentes si et seulement s'il existe une matrice U appartenant à $\mathrm{GL}(n;\mathbb{Z})$ telle que la relation $B=U^{\mathrm{T}}AU$ ait lieu. Il est admis que cette propriété est une relation d'équivalence notée $A\equiv B$.

Soit A une matrice de $\mathcal{S}^+(n;\mathbb{R})$. L'ensemble des valeurs prises par la forme quadratique, associée à A, $q(x)=(x|a(x))=X^{\mathrm{T}}AX$, lorsque x est un vecteur non nul de $\mathbb{Z}^n$, est un ensemble de réels strictement positifs. Il est admis que la borne inférieure $m(A)$ de cet ensemble existe et est un réel positif ou nul :

$$m(A)=\inf_{x\in\mathbb{Z}^n\setminus\{0\}}(x|a(x))\geqslant 0.$$

Le but de cette partie est de montrer que, dans $\mathcal{S}^+(n;\mathbb{R})$, toute matrice A est $\mathbb{Z}$-congruente à une matrice B de $\mathcal{S}^+(n;\mathbb{R})$ telle que $m(B)$ soit égal au coefficient b_{11}.

II.1. Propriétés des matrices $\mathbb{Z}$-congruentes :

Soient A et B deux matrices de $\mathcal{M}(n;\mathbb{R})$ $\mathbb{Z}$-congruentes. La matrice A appartient à l'ensemble $\mathcal{S}^+(n;\mathbb{R})$.

a. Démontrer que la matrice B appartient aussi à l'ensemble $\mathcal{S}^+(n;\mathbb{R})$.

b. Établir les relations : $\det A=\det B$, $m(A)=m(B)$.

c. Soit B la matrice définie par la relation : $B=\begin{pmatrix}2 & -2\\ -2 & 3\end{pmatrix}$. Établir que la matrice B appartient à l'ensemble $\mathcal{S}^+(2;\mathbb{R})$ (utiliser la forme quadratique associée à cette matrice) ; déterminer le réel $m(B)$.

II.2. Propriétés du réel $m(A)$:

Dans cette question, la matrice A, associée à l'endomorphisme a, appartient à l'ensemble $\mathcal{S}^+(n;\mathbb{R})$.

a. Comparer les réels $m(A)$ et a_{11}.
Il est admis qu'il n'existe qu'un nombre fini de vecteurs x de $\mathbb{Z}^n$ vérifiant $(x|a(x)) \leqslant a_{11}$.
En déduire l'existence d'au moins un vecteur z appartenant à $\mathbb{Z}^n$ vérifiant l'égalité

$$(z|a(z)) = m(A).$$

Soient $z_1, z_2, \ldots, z_n$ les coordonnées de ce vecteur z. Démontrer que les coordonnées différentes de 0 sont des entiers relatifs premiers entre eux dans leur ensemble et que le réel $m(A)$ est strictement positif.

b. Démontrer qu'il existe une matrice B $\mathbb{Z}$-congruente à la matrice A telle que la relation $b_{11} = m(B)$ ait lieu.

Troisième partie : Majoration de $m(A)$

Le but de cette partie est d'établir, pour une matrice A appartenant à l'ensemble $\mathcal{S}^+(n;\mathbb{R})$, une relation simple donnant une majoration du réel $m(A)$ au moyen du déterminant de A. Cette relation est d'abord établie pour les matrices d'ordre 2 en introduisant la définition de matrice "réduite" puis établie pour les matrices d'ordre n.

III.1. Relations vérifiées par les coefficients d'une matrice de $\mathcal{S}^+(2;\mathbb{R})$:

On considère une matrice A symétrique d'ordre 2 qui s'écrit $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$

a. Démontrer qu'une matrice A appartient à $\mathcal{S}^+(2,\mathbb{R})$ si et seulement si ses coefficients vérifient les relations :

$$a > 0,\ c > 0 \text{ et } ac - b^2 > 0.$$

b. Démontrer que, pour qu'une matrice A appartienne à $\mathcal{S}^+(2,\mathbb{R})$, il suffit que ses coefficients vérifient les relations $0 < a$, $2|b| \leqslant a \leqslant c$.
Déterminer le réel $m(A)$ lorsque les coefficients a, b et c vérifient les inégalités ci-dessus.

Une matrice A de $\mathcal{S}^+(2,\mathbb{R})$ est dite "réduite" lorsque ses coefficients a, b et c vérifient les relations : $0 < a$, $0 \leqslant 2b \leqslant a \leqslant c$.

III.2. Matrice "réduite" $\mathbb{Z}$-congruente à une matrice donnée :

Soit $A_1 = \begin{pmatrix} a_1 & b_1 \\ b_1 & c_1 \end{pmatrix}$ une matrice appartenant à $\mathcal{S}^+(2,\mathbb{R})$ telle que le réel $m(A_1)$ soit égal au coefficient a_1.

Démontrer qu'il existe une matrice $A_2 = \begin{pmatrix} a_2 & b_2 \\ b_2 & c_2 \end{pmatrix}$, $\mathbb{Z}$-congruente à la matrice A_1, dont les coefficients vérifient les relations : $0 < a_2$, $2|b_2| \leqslant a_2 \leqslant c_2$.

Établir cette propriété en recherchant une matrice $U = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, où λ est un entier relatif, qui vérifie la relation suivante : $A_2 = U^{\mathrm{T}} A_1 U$.

En déduire qu'il existe une matrice A_3 (appartenant à $\mathcal{S}^+(2;\mathbb{R})$) "réduite" et $\mathbb{Z}$-congruente à la matrice A_1.

III.3. Relation entre les réels $m(A)$ et $\det A$:

Démontrer que, pour toute matrice A de $\mathcal{S}^+(2;\mathbb{R})$, les réels $m(A)$ et $\det A$ sont liés par la relation suivante :

$$m(A) \leqslant \frac{2}{\sqrt{3}} \sqrt{\det A}.$$

Vérifier la relation ci-dessus pour la matrice B définie à la question **II.1.c**.

III.4. Matrice B induite par une matrice A :

L'entier n est supposé supérieur où égal à 3. Étant donné une matrice $A = (a_{ij})$ de $\mathcal{S}^+(n;\mathbb{R})$, dont le coefficient a_{11} est différent de 0, soit V la matrice dont les coefficients v_{ij}, $1 \leqslant i \leqslant n$,

$1 \leqslant j \leqslant n$, sont définis par les relations :

$$v_{ij} = \begin{cases} 1 & \text{si } i = j \\ \dfrac{a_{1j}}{a_{11}} & \text{si } i = 1 \text{ et } j \geqslant 2 \\ 0 & \text{dans les autres cas.} \end{cases} \qquad V = \begin{pmatrix} 1 & \frac{a_{12}}{a_{11}} & \frac{a_{13}}{a_{11}} & \dots & \frac{a_{1n}}{a_{11}} \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Soient a l'endomorphisme de matrice associée A dans la base canonique $(e_1, e_2, \dots, e_n)$ de $\mathbb{R}^n$ et f l'endomorphisme défini par les relations :

$$\forall i,\ 1 \leqslant i \leqslant n,\ f(e_i) = a_{11}a(e_i) - a_{1i}a(e_1).$$

a. Démontrer que le sous-espace vectoriel F de $\mathbb{R}^n$ engendré par les vecteurs $e_2, e_3, \dots, e_n$ est stable par l'endomorphisme f.
Soit B la matrice d'ordre $n-1$ associée à la restriction de l'endomorphisme f (noté encore f) au sous-espace vectoriel F dans la base $(e_2, e_3, \dots, e_n)$. Il est admis que la matrice V, définie ci-dessus vérifie la relation ci-après :

$$A = V^{\mathrm{T}} \begin{pmatrix} a_{11} & 0 \\ 0 & \frac{1}{a_{11}}B \end{pmatrix} V.$$

b. Établir la relation qui lie les déterminants des matrices A et B entre eux.

c. Étant donné un vecteur x de $\mathbb{R}^n$: $x = \sum_{i=1}^{n} x_i e_i$, soit x_F le vecteur du sous-espace vectoriel F défini par la relation : $x_F = \sum_{i=2}^{n} x_i e_i$. Soit y le vecteur $v(x)$ image du vecteur x par l'endomorphisme v de matrice associée V. Démontrer la relation :

$$(x|a(x)) = a_{11}y_1^2 + \frac{1}{a_{11}}(x_F|f(x_F)).$$

Démontrer que la matrice B appartient à l'ensemble $\mathcal{S}^+(n-1;\mathbb{R})$.

III.5. Relation entre les réels $\det A$ **et** $m(A)$:
Le but de cette question est d'établir, pour toute matrice A de $\mathcal{S}^+(n;\mathbb{R})$, la relation ci-dessous, établie lorsque $n = 2$:

$$m(A) \leqslant \left(\frac{4}{3}\right)^{\frac{n-1}{2}} (\det A)^{1/n}. \qquad \text{(R)}$$

a. Deux hypothèses sur la matrice A sont formulées :
- $m(A) = a_{11}$;
- la relation (R) ci-dessus est vraie pour la matrice B construite à partir de la matrice A comme à la question précédente.

D'après la question **II.2.a.**, il existe un vecteur $z_F = \sum_{i=2}^{n} z_i e_i$ (appartenant à $\mathbb{Z}^{n-1}$) pour lequel l'égalité $(z_F|f(z_F)) = m(B)$ a lieu.
Démontrer qu'il existe un entier relatif z_1 tel que le vecteur z, de $\mathbb{Z}^n$, défini par la relation : $z = z_1e_1 + z_F$, est transformé par l'endomorphisme v, de matrice associée V, en un vecteur y ($y = v(z)$) dont la première coordonnée y_1 vérifie $|y_1| \leqslant \frac{1}{2}$.
En déduire que la matrice A vérifie la relation (R).

b. Démontrer, pour toute matrice A de $\mathcal{S}^+(n;\mathbb{R})$, la relation (R).