SPÉCIALE MP* : CORRIGÉ DE L'ÉPREUVE DES MINES 98 MATH 2

Première partie : construction d'une base de $\mathbb{Z}^n$ 23

I.1. $\det(M) = \pm 1$: Si M de $\mathcal{M}(n,\mathbb{Z})$ admet un inverse M' dans $\mathcal{M}(n,\mathbb{Z})$, alors $MM' = I$ et $\det(M).\det(M') = 1$ et l'entier $\det(M)$ est inversible dans $\mathbb{Z}$ donc vaut ± 1. 2

Réciproquement, une matrice M de $\mathcal{M}(n,\mathbb{Z})$ dont le déterminant est $\varepsilon = \pm 1$ est inversible dans $\mathcal{M}(n,\mathbb{Z})$ puisque son inverse est $M' = \varepsilon\,\text{comatrice}\,(M)^{\mathrm{T}}$ 3

I.2. Existence de v :

- Si $d \neq 0$, d'après l'algorithme d'Euclide, il existe des coefficients entiers s et t tels que $sa + tb = d$ (même si $a = 0$ ou $b = 0$), alors $\boxed{V = \begin{pmatrix} s & t \\ -b' & a' \end{pmatrix}}$, où $a' = \dfrac{a}{d}$ et $b' = \dfrac{b}{d}$, répond à la question et V dépend de x. 2
- Si $d = 0$ alors $V = I_2$ convient (car $x = (0,0)$). 2

I.3. a. Existence de u : D'après la question précédente, il existe V telle que $V\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. On prend alors $U = V^{-1} \in \mathrm{GL}(2,\mathbb{Z})$. 2

y existe : Le second vecteur colonne de U convient : il est bien indépendant de x puisque $\det(x,y) = 1 \neq 0$. Tout vecteur w de $\mathbb{Z}^2$, peut bien s'écrire sous la forme $ax + by = w$, $(a,b) \in \mathbb{Z}^2$, grâce à la relation $U\begin{pmatrix} a \\ b \end{pmatrix} = W$, sachant que U est inversible dans $\mathrm{GL}(2,\mathbb{Z})$. 3

b. Existence de v_{n-1} : Il suffit d'écrire par blocs $W'_{n-1} = \begin{pmatrix} I_{n-2} & 0 \\ 0 & W_{n-1} \end{pmatrix}$ où W_{n-1} est la matrice d'ordre 2 vue au I.2 *(I_{n-2} étant la matrice unité d'ordre $n-2$).* 1

Existence de v_k : On procède par récurrence descendante, le mode de construction précédent, en groupant deux par deux les deux dernières lignes et colonnes d'indice k et $k-1$.

Hypothèse de récurrence : $\exists v_{k+1} \in \mathrm{GL}(n,\mathbb{Z}) \mid v_{k+1}(x) = y^{k+1}$ pour $1 \leqslant k \leqslant n-2$.

D'après le I.2, il existe W_k matrice d'ordre 2 telle que $W_k\begin{pmatrix} x_k \\ d_{k+1} \end{pmatrix} = \begin{pmatrix} d_k \\ 0 \end{pmatrix}$. En posant $W'_k = \begin{pmatrix} I_{n-k+1} & & 0 \\ & W_k & \\ 0 & & I_{k-1} \end{pmatrix}$, on a $W'_k \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ d_{k+1} \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_{k-1} \\ d_k \\ 0 \end{pmatrix}$ ce qui prouve la propriété à l'ordre $k-1$. 3

Existence de u : En suivant les constructions précédentes, la matrice $V = W'_1 \ldots W'_{n-1}$ transforme le vecteur x en e_1, puisque le dernier pgcd est 1, d'après l'hypothèse de primarité des composantes de x.

Chaque V_i étant inversible dans $\mathrm{GL}(n,\mathbb{Z})$, la matrice $U = V^{-1}$ convient. 2

c. Existence d'une base de $\mathbb{Z}^n$: L'ensemble des vecteurs colonnes de U, convient évidemment ! En effet, si $W = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in \mathbb{Z}^n$ alors $V\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \mathbb{Z}^n$ et on en déduit $w = \lambda_1 x + \lambda_2 z^2 + \cdots + \lambda_n z^n$ donc la famille est génératrice.

Elle est libre car $U \in \mathrm{GL}(n,\mathbb{Z})$. C'est donc une "base" car les coefficients λ_i sont entiers. 3

Deuxième partie : Matrices $\mathbb{Z}$-congruentes 16

II.1. a. B **est aussi dans** $S_n^+(n,\mathbb{R})$ **:** Comme $B = U^{\mathrm{T}}AU$ on a

$$B^{\mathrm{T}} = U^{\mathrm{T}}A^{\mathrm{T}}(U^{\mathrm{T}})^{\mathrm{T}} = B$$ 1

car A est symétrique et $(U^{\mathrm{T}})^{\mathrm{T}} = U$, B est donc symétrique. En outre

$$(X|BX) = X^{\mathrm{T}}U^{\mathrm{T}}AUX = (ux|Aux) \geqslant 0$$

puisque $a \in S^+(n,\mathbb{R})$. De plus $(X|BX) = 0$ implique $UX = 0$ puisque A est définie et $X = 0$ puisque U est inversible ; par conséquent $B \in S^+(n,\mathbb{R})$. 3

En fait A et B sont les matrices d'une même forme quadratique.

b. $\det(A) = \det(B)$**,** $m(A) = m(B)$ **:** $\det(B) = \det(U)^2 \det(A) = (\varepsilon)^2 \det(A) = \det(A)$ car on a vu à la question I.1 que $\det U = \pm 1$. 1

On a $m(B) = \inf(U(X)|A(U(X)) \geqslant m(A)$ (minimum sur l'ensemble des vecteurs $Y = UX$). L'inégalité inverse est immédiate (symétrie de la congruence) donc $m(A) = m(B)$. 2

c. Exemple : B **est dans** $S_n^+(n,\mathbb{R})$ **; calculer** $m(B)$ **:** B est bien dans $S^+(2,\mathbb{R})$ car les déterminants "en coins" sont 2 et 6-4=2 > 0 ; On peut dire aussi que la forme quadratique associée à B est

$$q(X) = 2x^2 + 3y^2 - 4xy = 2(x-y)^2 + y^2$$

est bien définie positive. 2

$m(B) = 1$ **:** $m(B) \leqslant 1$ car $q\begin{pmatrix}1\\1\end{pmatrix} = 1$ et $m(B) \in \mathbb{N}^*$ soit en utilisant le résultat de la question suivante, soit en distinguant les cas :

- si $x_1 = x_2$ alors $q(X) \geqslant x_2^2 \geqslant 1$ car $X \neq 0$,
- si $x_1 \neq x_2$ alors $q(X) \geqslant 2(x_1 - x_2)^2 \geqslant 2$ car $|x_1 - x_2| \geqslant 1$. 2

II.2. a. Comparer $m(A)$ **et** a_{11} **:** Comme $q(e_1) = a_{11}$, on a $\boxed{m(a) \leqslant a_{11}}$ 1

Existence de z **:** z existe, car un ensemble fini de vecteurs non nuls, admet toujours un minimum (atteint). 1

Les coordonnées de z **sont premières entre elles, et** $m(A) > 0$ **:** $m(z)$ est bien non nul car $m(z) = (z|Az)$ et $A \in S^+(n,\mathbb{R})$. Si les coordonnées non nulles de z, avaient un pgcd d, on aurait $z = dz_0$, et $m(A) = q(z) = d^2q(z_0) = d^2q(z_0) \geqslant q(z_0)$, $m(A)$ ne serait pas le minimum de $q(X)$, si $|d| > 1$; elles sont donc bien premières entre elles. 2

b. Il existe B $\mathbb{Z}-$ **congruente à** A **telle que** $m(B) = b_{11}$ **:** Soit Z la colonne des composantes de z, comme les z_i sont premiers entre eux, la question (I.3.b) assure l'existence d'une matrice U de $\mathrm{GL}(n,\mathbb{Z})$ telle que $z = u(e_1)$; si on pose $B = U^{\mathrm{T}}AU$, elle est bien $\mathbb{Z}-$congruente à A et d'après (II.1.b)

$$m(A) = Z^{\mathrm{T}}AZ = (Ue_1|AUe_1) = (e_1|Be_1) = b_{11} = m(B)\ (= m(B) \text{ car } m(A) = m(B)).$$ 2

Troisième partie : Majorer $m(A)$ 43

III.1. a. CNS pour que A **soit dans** $S^+(2,\mathbb{R})$ **:** La forme quadratique $q(X) = ax^2 + 2bxy + cy^2$ est définie positive, or $q(e_1) = a$ et $q(e_2) = c$, d'où les deux inégalités $a > 0$, $c > 0$. Comme $q(be_1 - ae_2) = ab^2 + ca^2 - 2b^2a = a(ac - b^2)$, on a aussi la troisième. 2

Réciproque : on a $q(X) = a(x + \frac{b}{a}y)^2 + \frac{b^2-ac}{a}y^2$ qui est définie positive ! 2

b. CS pour que A **soit dans** $S^+(2,\mathbb{R})$ **:** En effet la condition nécessaire et suffisante, précédente est bien satisfaite alors puisque

$$c \geqslant a > 0 \text{ et } ac - b^2 \geqslant a^2 - b^2 \geqslant 3b^2 \begin{cases} > 0 & \text{si } b \neq 0 \\ ac - b^2 = ac > 0 & \text{si } b = 0 \end{cases}$$ 2

Calculer alors $m(A)$: $m(A) \leqslant a$ d'après (II.2.a). Montrons l'inégalité inverse.
Posons $Z = (x, y) \neq (0, 0)$ tel que $x, y \in \mathbb{Z}$.

- si $xy = 0$ alors $q(Z) = (Z|AZ) = \begin{cases} ax^2 \geqslant a & \text{si } y = 0 \\ cy^2 \geqslant c \geqslant a & \text{si } x = 0 \end{cases}$
- si $xy \neq 0$ alors $q(Z) = ax^2 + 2bxy + cy^2 \geqslant ax^2 - 2|b||xy| + cy^2$
  - $\geqslant ax^2 + 2|b||y|(|y| - |x|)$ car $c \geqslant 2|b|$
  - $\geqslant cx^2 + 2|b||x|(|x| - |y|)$ car $a \geqslant c \geqslant 2|b|$

  Par conséquent $q(z) \begin{cases} \geqslant ax^2 \geqslant a & \text{lorsque } |y| \geqslant |x| \\ \geqslant cy^2 \geqslant c \geqslant a & \text{lorsque } |y| \leqslant |x| \end{cases}$.

Dans tous les cas $q(z) \geqslant a$ donc $\boxed{m(A) = a}$. 5

III.2. Existence de A_2 : On cherche U, sous la forme indiquée par l'énoncé

$$U = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \quad \text{et } A_2 = U^{\mathrm{T}} A_1 U = \begin{pmatrix} a_1 & \lambda a_1 + b_1 \\ \lambda a_1 + b_1 & \lambda^2 a_1 + 2\lambda b_1 + c_1 \end{pmatrix}$$

On a donc $a_2 = a_1 > 0$. Il reste à réaliser la seconde condition $2|b_2| \leqslant a_2 \leqslant c_2$, pour un choix convenable d'un $\lambda \in \mathbb{Z}$. 1

Comme $c_2 = \lambda^2 a_1 + 2\lambda b_1 + c_1 = q\begin{pmatrix} \lambda \\ 1 \end{pmatrix} \geqslant m(A_1) = a_1 = a_2$, est satisfaite automatiquement grâce à l'hypothèse. 2

Il ne reste plus qu'à réaliser (ce qui veut dire choisir un λ entier relatif) $2|b_2| \leqslant a_2$.
Or cette dernière condition équivaut à $-a_1 \leqslant 2\lambda a_1 + 2b_1 \leqslant a_1 \iff \frac{-a_1 - 2b_1}{2a_1} \leqslant \lambda \leqslant \frac{+a_1 - 2b_1}{2a_1}$ comme l'écart des deux extrèmes est $\frac{a_1 - 2b_1}{2a_1} - \frac{-a_1 - 2b_1}{2a_1} = 1$, il y a au moins *(et d'ailleurs au plus deux, au cas où les deux bornes seraient entières)* entiers dans cet intervalle. 3

Existence de A_3 réduite :

- Si $b_2 \geqslant 0$: $A_3 = A_2$ fait l'affaire.
- Si $b_2 < 0$, posons V=diag(-1,1) (W=diag(1,-1) marche aussi), alors

$$V \in \mathrm{GL}(2, \mathbb{Z}) \text{ et } A_3 = V^{\mathrm{T}} A_2 V = \begin{pmatrix} a_2 & -b_2 \\ -b_2 & c_2 \end{pmatrix} \text{ convient.} \quad 2$$

III.3. Majoration de $m(A)$: Soit $A \in S^+(2, \mathbb{R})$ alors

- $\exists A_1$ $\mathbb{Z}$-congruente à A telle que $a_1 = m(A_1) = m(A)$, $\det A_1 = \det A$,
- $\exists A_2$ $\mathbb{Z}$-congruente à A_1 telle que $a_2 = m(A_2) = m(A_1)$, $\det A_2 = \det A_1$ et qui vérifie de plus $0 < a_2$, $0 \leqslant 2|b_2| \leqslant a_2 \leqslant c_2$,
- $\exists A_3$ $\mathbb{Z}$-congruente à A_2 telle que $a_3 = m(A_3) = m(A_1)$, $\det A_3 = \det A_2$, A_3 réduite.

On a donc $a_3 = m(A)$ et $\det A_3 = \det A$, on utilise alors les deux inégalités

$$a_3^2 \leqslant a_3 c_3 \text{ et } b_3^2 \leqslant \frac{a_3^2}{4} \text{ ce qui donne } \frac{3a_3^2}{4} = a_3^2 - \frac{a_3^2}{4} \leqslant a_3 c_3 - b_3^2$$

soit $\frac{3}{4} m(A)^2 \leqslant \det A$ ce qui s'écrit encore $\boxed{m(A) \leqslant \frac{2}{\sqrt{3}} \sqrt{\det(A)}}$ ce qui est bien l'inégalité annoncée (appelée inégalité d'HERMITE). 4

Vérifier sur la matrice B de (II.1.c) : On a en effet

$$b_1 = m(B) = 1 \leqslant \frac{2}{\sqrt{3}} \sqrt{2} = \frac{2\sqrt{2}}{\sqrt{3}}. \quad 0$$

III.4. a. Sous espace vectoriel stable : On a $a(e_i) = \sum_{k=1}^{n} a_{ki} e_k$ d'où

$$a_{11} a(e_i) - a_{1i} a(e_1) = \sum_{k=1}^{n} (a_{11} a_{ki} - a_{1i} a_{k1}) e_k$$

et on vérifie sans peine que le coefficient de e_1 est nul.
Conclusion : $\mathrm{Vect}(e_2,\dots,e_n)$ est stable par f. 2

b. Relier $\det(A)$ et $\det(B)$: Comme par blocs $\det(V)=\det(V^{\mathrm{T}})=1$ on a aussi par blocs $\det(A)=a_{i,1}\det(\frac{1}{a_{1,1}}B)=\frac{\det(B)}{a_{1,1}^{n-2}}$ (car $\det(tB)=t^{ordre\ de\ B}\det(B)$).

Conclusion : $\boxed{\det(A)=\dfrac{\det(B)}{a_{1,1}^{n-2}}}$ 2

c. Relation à démontrer : Il suffit de faire le calcul par blocs en posant $X=\begin{pmatrix}x_1\\ Y\end{pmatrix}$. ... 2

Démontrer que B appartient à $S^+(n-1,\mathbb{R})$: Soit $x_F=x_2e_2+..+x_ne_n\in F$, et prenons $x_1=-\sum_{k=2}^{n}\dfrac{a_{i,k}}{a_{1,1}}x_k$, de telle sorte que $y_1=x_1+\sum_{k=2}^{n}\dfrac{a_{i,k}}{a_{1,1}}x_k=0$. La relation précédente devient, en posant $x=x_1e_1+x_F$: $(x_F|f(x_F))=a_{1,1}(x|a(x))>0$, lorsque $x_F\neq 0$ (car $x_F\neq 0\Longrightarrow x\neq 0$). Comme B est symétrique $B\in S^+(n-1,\mathbb{R})$. 3
En fait B est la matrice de la restriction à F d'une forme quadratique définie positive.

III.5. a. z_1 existe : $y=vz$ s'écrit matriciellement $Y=VZ$ avec $\begin{cases}y_1=z_1+\sum_{k=2}^{n}\dfrac{a_{i,k}}{a_{1,1}}z_k\\ y_j=z_j,\ j\geqslant 2\end{cases}$

Pour avoir $|y_1|\leqslant\frac{1}{2}$, avec $z_1\in\mathbb{Z}$, il suffit de prendre **L'entier le plus proche** de $-\sum_{k=2}^{n}\dfrac{a_{i,k}}{a_{1,1}}z_k$ comme valeur de z_1. 2

En déduire que A vérifie (R) : Soit alors $z=z_1e_1+z_F$ (élément non nul de $\mathbb{Z}^n$, puisque d'après la conséquence de (II.2.a) z_F ne peut être nul car $m(B)$ ne l'est pas), avec comme il a été rappelé au début de la question :

$$\begin{cases}y_1=z_1+\sum_{k=2}^{n}\dfrac{a_{i,k}}{a_{1,1}}z_k\\ y_j=z_j,\ j\geqslant 2\end{cases}.$$

On a $m(A)\leqslant(z|a(z))=a_{1,1}(y_1)^2+\frac{1}{a_{1,1}}(z_F|b(z_F))\leqslant\frac{a_{1,1}}{4}+\frac{m(B)}{a_{1,1}}$, puisque $|y_1|\leqslant\frac{1}{2}$.
Comme $a_{1,1}=m(A)$, on a donc :

$$\frac{3}{4}(m(A))^2\leqslant m(B)\leqslant\Big(\frac{4}{3}\Big)^{\frac{n-2}{2}}\big(\det(B)\big)^{\frac{1}{n-1}}.$$

Donc $(m(A))^{2(n-1)}\leqslant\big(\frac{4}{3}\big)^{\frac{n(n-1)}{2}}\det(B)=\big(\frac{4}{3}\big)^{\frac{n(n-1)}{2}}(m(A))^{n-2}\det(A)$.
Comme on a $m(A)>0$, il vient $(m(A))^n\leqslant\big(\frac{4}{3}\big)^{\frac{n(n-1)}{2}}\det(A)$, il y a bien transfert de la récurrence. 5

b. Toute A de $S^+(2,\mathbb{R})$ vérifie (R) : La relation (R) est vérifiée par récurrence pour $n\geqslant 2$. Pour $n=2$ elle a été établie en (III.3). Si elle est vraie au rang $n-1\geqslant 2$, soit $A\in S^+(n,\mathbb{R})$. Il existe $A_1\in S^+(n,\mathbb{R})|A_1\equiv A$ et $m(A)=m(A_1)=a_{1,1}$ (II.2.b.).
On peut alors construire $B\in S^+(n-1,\mathbb{R})$ selon la procédure du (III.4) et via (III.5.a) aboutir à $m(A_1)\leqslant\big(\frac{4}{3}\big)^{\frac{n(n-1)}{2}}\det(A_1)^{\frac{1}{n}}$.
A vérifie donc (R) puisque $m(A)=m(A_1)$ et $\det(A)=\det(A_1)$.
L'inégalité d'HERMITE (Charles 1822-1901)

$$\boxed{m(A)\leqslant\left(\frac{4}{3}\right)^{\frac{n-1}{2}}\det(A)^{\frac{1}{n}}}$$

est donc établie pour toute matrice de $S^+(n,\mathbb{R})$, $n\geqslant 2$. 4