Polytechnique MP 2016 Mathématiques A.

Première partie.

1a) $M^{-1} = \underbrace{\frac{1}{\det M}}_{\in \mathbb{Z}^*} \underbrace{{}^t\mathrm{com}(M)}_{\in M_n(\mathbb{Z})} \in M_n(\mathbb{Q})$

1b) ii) => i) si $\det M = \pm 1$ $M^{-1} = \pm {}^t\mathrm{com}(M) \in M_n(\mathbb{Z})$

i) => ii) $MM^{-1} = I_n$.

si $M^{-1} \in M_n(\mathbb{Z})$ alors $\det(M^{-1}) \in \mathbb{Z}$ et

$\underbrace{\det M}_{\in \mathbb{Z}} \underbrace{\det M^{-1}}_{\in \mathbb{Z}} = 1$

Donc $\det M$ est inversible dans $\mathbb{Z}$ et $\det M = \pm 1$.

2.a) Si $M \in M_n(\mathbb{Z})$ alors $M(\mathbb{Z}^n) \subset \mathbb{Z}^n$ car $\mathbb{Z}$ est un anneau.

Or si $M \in GL_n(\mathbb{Z})$ alors

d'une part $M \in GL_n(\mathbb{Z})$ donc $M(\mathbb{Z}^n) \subset \mathbb{Z}^n$.

d'autre part $M^{-1} \in M_n(\mathbb{Z})$ donc $M^{-1}(\mathbb{Z}^n) \subset \mathbb{Z}^n$

dont $MM^{-1}(\mathbb{Z}^n) \subset M(\mathbb{Z}^n)$

soit $\mathbb{Z}^n \subset M(\mathbb{Z}^n)$

et finalement $M(\mathbb{Z}^n) = \mathbb{Z}^n$

. Si $M(\mathbb{Z}^n) = \mathbb{Z}^n$ alors

d'une part $M \in GL_n(\mathbb{R})$ car l'image de M contient la base canonique dont les éléments sont dans $\mathbb{Z}^n$.

d'autre part $M^{-1}(\mathbb{Z}^n) = M^{-1}M(\mathbb{Z}^n) = \mathbb{Z}^n$, donc l'image de la base canonique, donc les colonnes de M^{-1} sont des éléments de $\mathbb{Z}^n$ et par conséquent $M^{-1} \in M_n(\mathbb{Z})$ et $M \in GL_n(\mathbb{Z})$

2b) Posons $T = \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}$ alors $MT = \sum_{i=1}^{n} t_i x_i$

i ⇒ ii) Supposons que M soit dans $GL_n(\mathbb{Z})$.

Soit MT un point entier de P

alors $T = M^{-1} MT \in \mathbb{Z}^n$ donc $T = \begin{pmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_n \end{pmatrix}$ avec $\varepsilon_i \in \{0,1\}$.

Réciproquement si $T = \begin{pmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_n \end{pmatrix}$ avec $\varepsilon_i \in \{0,1\}$ alors

$T \in \mathbb{Z}^n$ donc $MT \in \mathbb{Z}^n$.

ii) ⇒ i) Supposons que M ne soit pas dans $GL_n(\mathbb{Z})$

c'est-à-dire $M^{-1} \notin M_n(\mathbb{Z})$.

On a $MM^{-1} = I_n$. et il existe une colonne $C_j = (m'_{i,j})_{1 \le i \le n}$.

de M^{-1} dont les coefficients ne sont pas tous des entiers.

on peut écrire $C_j = C'_j + T_j$ où $C'_j \in \mathbb{Z}^j$ et $T_j = (t_{i,j})_{1 \le i \le n}$

avec $t_{i,j} \in [0,1]$ $1 \le i \le n$ et $\exists i_0$ $t_{i_0} \in]0,1[$.

On aura $MC_j = (\delta_{i,j})_{1 \le i \le j} \in \mathbb{Z}^n$

donc $MT_j = MC_j - MC'_j \in \mathbb{Z}^n$.

le point $\sum t_{i,j} x_i$ est donc un point entier de P qui

n'est pas un des $\sum \varepsilon_i x_i$ $\varepsilon_i \in \{0,1\}$.

ii ⇒ i est donc prouvée par la contraposée.

3) Notons $T(\alpha, i, j) = I_n + \alpha E_{i,j}$. , $M = (m_{k,\ell})_{1 \le k, \ell \le n}$.

Soit $M' = (m'_{k,\ell})_{1 \le k, \ell \le n} = T(\alpha, i, j) M$.

$$m'_{k,\ell} = \sum_{p=1}^{n} (\delta_{k,p} + \alpha \delta_{k,i} \delta_{p,j}) m_{p,\ell} = m_{k,\ell} + \alpha \delta_{k,i} m_{j,\ell}$$

M' est obtenue en ajoutant à la $i^{\text{ème}}$ ligne de M sa j-ième multipliée par α. De même

$M\,T(\alpha, i, j)$ est obtenue en ajoutant à la j-ème colonne de M sa i-ème multipliée par α.

4a) On peut écrire $N = \left(\begin{array}{c|c} a_2 & \\ & N_1 \\ a_n & \end{array} \right)$

En développant par rapport à la première ligne on aura.

$$\det M = \cancel{\det}\ a_1 \det \left(N_1 \left| \begin{array}{c} v a_2 \\ \\ v a_n \end{array} \right. \right) + (-1)^{n+1} u \det N$$

$$= a_1 v \cdot (-1)^{n-2} \det \left(\begin{array}{c|c} a_2 & \\ & N_1 \\ a_n & \end{array} \right) + (-1)^{n+1} u \det N$$

signature d'un cycle de longueur $n-1$

$$\underline{\det M = (-1)^n (a_1 v - u) \det N}$$

4b) $\dfrac{a_1}{\operatorname{pgcd}(a_1, a_2, \ , a_n)}$ et $\dfrac{\operatorname{pgcd}(a_2, \ , a_n)}{\operatorname{pgcd}(a_1, \ , a_n)}$ sont des entiers premiers entre eux (car $\operatorname{pgcd}(a_1, \ , a_n) = \operatorname{pgcd}(a_1, \operatorname{pgcd}(a_2, \ , a_n))$)

Il existe donc (d'après Bézout) un couple (U, V) dans $\mathbb{Z}^2$ tel que

$$1 = \frac{a_1}{\operatorname{pgcd}(a_1, \ , a_n)} V + \frac{\operatorname{pgcd}(a_2, \ , a_n)}{\operatorname{pgcd}(a_1, \ , a_n)} U$$

on choisit $\underline{\cancel{u} = (-1)^n \dfrac{V}{\operatorname{pgcd}(a_2, \ , a_n)}}$ $\quad \underline{\cancel{u} = (-1)^{n-1} \cancel{\ } U}$

$$1 = (-1)^n (a_1 \cancel{v} - \cancel{u}) \frac{\operatorname{pgcd}(a_2, \ , a_n)}{\operatorname{pgcd}(a_1, \ , a_n)}$$

Donc si $\det N = \operatorname{pgcd}(a_2, \ , a_n)$, on a bien $\det M = \operatorname{pgcd}(a_1, \ , a_n)$. De plus $u \in \mathbb{Z}$ et $\forall i \geq 2$ $\operatorname{pgcd}(a_2, \ , a_n)$ divise a_i donc $v a_i \in \mathbb{Z}$.

Par conséquent <u>M est bien dans $M_n(\mathbb{Z})$</u>

4c) On conclut immédiatement <u>par récurrence</u>, le résultat étant vrai pour $n = 1$. On peut même affirmer que M est de la forme $\begin{pmatrix} a_1 & 0 & \cdots & 0 & u_1 \\ \vdots & & & u_2 & \\ & & \cdots & & \\ a_n & u_{n-1} & \cdots & & u_1 \end{pmatrix}$

p.o.

5a) $(x'_1, \quad , x'_n)$ est une famille de n vecteurs de $\mathbb{Q}^{n-1}$, elle est donc liée. Il existe $(a_1, \quad , a_n) \in \mathbb{Q}^n$ tel que $\sum_{i=1}^{n} a_i x'_i$. En multipliant par le dénominateur commun à tous les a_i, on peut se ramener au cas où ~~tous~~ les a_i sont des entiers, premiers entre eux dans leur ensemble.

5b) D'après la question 4 il existe une matrice A_1 dont la première colonne est $\begin{pmatrix} a_1 \\ \\ a_n \end{pmatrix}$ et dont le déterminant vaut $\mathrm{pgcd}(a_1, \quad , a_n)$, soit 1. A_1 est donc dans $GL_n(\mathbb{Z})$.

De plus la première colonne de $MA_1 = \sum_{i=1}^{n} a_i x_i$. Le choix des a_i montre que cette colonne est de la forme $\begin{pmatrix} c_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. (*)

Quitte à remplacer A_1 par $-A_1$ on peut supposer $\tilde{c}_{1,1} > 0$.

5c) Pour $j \geq 2$ on peut écrire $\tilde{c}_{1,j} = q_j \tilde{c}_{1,1} + r_j$ avec $0 \leq r_j < \tilde{c}_{1,1}$.

Si on multiplie $\tilde{C}$ par $I_n - q_j E_{1,j}$ seul sa j-ième colonne est modifiée. De plus, si on note $\tilde{C}'$ cette nouvelle matrice on aura $\tilde{c}'_{1,j} = \tilde{c}_{1,j} - q_j \tilde{c}_{1,1} = r_j$ avec $0 \leq r_j < \tilde{c}_{1,1}$

En faisant cela pour chacune des colonnes et en remarquant que cela revient à multiplier par $I_n - q_j E_{1,j}$ qui est de déterminant 1 et donc dans $GL_n(\mathbb{Z})$. On obtient pour une matrice A'_1 toujours dans $GL_n(\mathbb{Z})$

$$\tilde{C} = MA'_1 = \begin{pmatrix} \tilde{c}_{11} & \tilde{c}_{1,2} & \cdots & \tilde{c}_{1,n} \\ 0 & & & \\ \vdots & & \tilde{C}' & \\ 0 & & & \end{pmatrix}$$ avec $\tilde{c}_{i,j} \in [0, \tilde{c}_{1,1}[$ et $\tilde{c}_{1,1} > 0$

(*) $c_{1,1} \neq 0$ car $M \begin{pmatrix} a_1 \\ \\ a_n \end{pmatrix} \neq 0$ puisque $\begin{pmatrix} a_1 \\ \\ a_n \end{pmatrix} \neq 0$ et $(x_1, \quad , x_n)$ est libre.

5d) Conclusion par récurrence.

Pour $n=1$ le résultat est vrai (prendre $A=(1)$ ou (-1) suivant le signe de $m_{1,1}$. La condition sur $c_{i,j}$ $i<j$ est sans pertinence.

On suppose le résultat vrai à l'ordre $n-1$. On se donne M dans $M_n(\mathbb{Z})$.

le travail préliminaire montre qu'il existe A_1 dans $GL_n(\mathbb{Z})$ tel que MA_1 est de la forme $\left(\begin{array}{c|c} \tilde{c}_{11} & \tilde{c}_{1,2} \quad \tilde{c}_{1,n} \\ \hline \begin{matrix}0\\ \vdots\\ 0\end{matrix} & \tilde{C}_1 \end{array}\right)$

On applique l'hypothèse de récurrence à $\tilde{C}_1$, qui se transforme en C_1 adéquate par $\tilde{\tilde{C}}_1 = \tilde{C}_1 \tilde{A}_1$.

Alors si $A_2 = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \tilde{A}_1 \end{array}\right)$ A_2 est dans $GL_n(\mathbb{Z})$ et

$C = M A_1 A_2$ répond à la question.

6) le résultat se déduit immédiatement du précédent en passant à la transposée, ~~si on ...~~

Défi : Programmer la réduction précédente en Python.

Python ne calculant pas naturellement avec les entiers, pour déterminer les a_i, on remplacera la transformation

$V \leftarrow V - \frac{p}{q} W$ de la méthode du pivot classique par

l'opération $V \leftarrow qV - pW$. Cette opération ayant tendance à faire croître rapidement les coefficients, il sera bon d'exploiter autant que possible les contenus des vecteurs, c'est-à-dire les pgcd de leurs coefficients.