

Solution du Capes 2017 épreuve 1

Problème 1

Partie A: $\mathbb{Z}$ -bases du réseau

I. $\mathcal{C} = \{e_1, e_2\}$ est la base canonique de $\mathbb{R}^2$. On vérifie que e_1 et e_2 sont des éléments de $\mathcal{R}$ et que tout élément $X = \begin{pmatrix} a \\ b \end{pmatrix} = ae_1 + be_2$ peut s'écrire de manière unique comme combinaison linéaire à valeurs dans $\mathbb{Z}$ de $\mathcal{C}$. Aussi, $\mathcal{C}$ est une $\mathbb{Z}$ -base du réseau.

II.

1. $A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_1x + a_2y \\ b_1x + b_2y \end{pmatrix} = xe'_1 + ye'_2$.
2. On suppose dans cette question que (e'_1, e'_2) est une $\mathbb{Z}$ -base de $\mathcal{R}$.
 - (a) Alors e'_1 et e'_2 sont des éléments de $\mathcal{R}$, d'où $e'_1, e'_2 \in \mathbb{Z}^2$. Il s'ensuit donc que a_1, a_2, b_1, b_2 sont des éléments de $\mathbb{Z}$.
 - (b) Puisque (e'_1, e'_2) est une $\mathbb{Z}$ -base de $\mathbb{R}$, d'après la seconde hypothèse tout élément de $\mathcal{R}$ peut s'écrire comme combinaison linéaire à coefficients dans $\mathbb{Z}$ de e'_1, e'_2 . Or, $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ sont des éléments de $\mathcal{R}$ d'où il existe $(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4$ tels que $x_1e'_1 + y_1e'_2 = e_1$ et $x_2e'_1 + y_2e'_2 = e_2$.
 - (c) Posons $B = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$. Alors

$$AB = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} = \begin{pmatrix} a_1x_1 + a_2y_1 & a_1x_2 + a_2y_2 \\ b_1x_1 + b_2y_1 & b_1x_2 + b_2y_2 \end{pmatrix}$$

Nous reconnaissons alors la première colonne comme étant celle de $x_1e'_1 + y_1e'_2 = x_1 \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} + y_1 \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. De même, nous reconnaissons la seconde colonne comme étant $x_2e'_1 + y_2e'_2 = \begin{pmatrix} a_1x_2 + a_2y_2 \\ b_1x_2 + b_2y_2 \end{pmatrix} = e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Aussi, nous obtenons bien que $AB = I_2$.

- (d) Les matrices A et B sont à coefficients entiers, donc leur déterminant est aussi un entier (par exemple $\det(A) = a_1b_2 - b_1a_2$ avec $(a_1, a_2, b_1, b_2) \in \mathbb{Z}^4$). Or, le déterminant est une application multiplicative, nous avons $\det(AB) = \det(A)\det(B)$. Donc de la question précédente, nous avons que $\det(AB) = \det(I_2) = 1$ d'où $\det(A) \times \det(B) = 1$. Comme $\det(A)$ et $\det(B)$ sont des entiers relatifs,

ils, il s'ensuit que $\det(A) = \det(B) \in \{-1, 1\}$.

Complément: En fait le déterminant est un morphisme. Rappelons que $GL_n(\mathbb{R})$ est l'ensemble des matrices inversibles de taille n pour la multiplication matricielle. On étend ensuite la formule $\det(AB) = \det(A)\det(B)$ aux matrices non inversibles. On voit que si A est non inversible, alors AB ne l'est pas non plus. Si A est inversible, alors AB est inversible et l'inverse de AB , alors $ABC = I$ d'où BC serait l'inverse de A . On voit que si $\det(A) = \det(AB) = 0$ et la formule est alors vérifiée aussi.

3. On suppose ici que $(a_1, a_2, b_1, b_2) \in \mathbb{Z}^4$ et que $\det(A) \in \{-1, 1\}$.

- (a) Puisque $\det(A) \in \{-1, 1\}$, nous avons $\det(A) \neq 0$ et donc A est une matrice inversible. D'après la formule, nous savons que

$$A = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \quad \text{donc} \quad A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Il s'ensuit donc que les coefficients de la matrice A^{-1} sont aussi des entiers relatifs.

- (b) $e'_1 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$ et $e'_2 = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$ sont deux vecteurs à coordonnées dans $\mathbb{Z}$, donc sont des éléments de $\mathbb{Z}^2$. De plus, puisque la matrice A est inversible, il existe $B = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$ telle que $AB = I_2$. En considérant les vecteurs colonnes, cela conduit à $x_1 e'_1 + y_1 e'_2 = e_1$ et $x_2 e'_1 + y_2 e'_2 = e_2$. Comme (e_1, e_2) forme une base de $\mathbb{Z}^2$, nous en déduisons que tout élément $X \in \mathcal{R}$ est combinaison linéaire à coefficients entiers de e'_1 et e'_2 , d'où (e'_1, e'_2) est une $\mathbb{Z}$ -base de $\mathcal{R}$.

4. Nous avons montré que (e'_1, e'_2) est une $\mathbb{Z}$ -base de $\mathcal{R}$ si et seulement si la matrice A (formée des vecteurs colonnes e'_1, e'_2) est à coefficients réels et de déterminant ± 1 .

III. Soit $e'_1 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$.

- Supposons que $e'_1 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$ soit le premier vecteur d'une $\mathbb{Z}$ -base de $\mathcal{R}$, c'est-à-dire qu'il existe $e'_2 = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$ tel que (e'_1, e'_2) est une $\mathbb{Z}$ -base de $\mathcal{R}$. Notons comme précédemment $A = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}$. Alors par la question **II**, nous savons que $\det(A) = \pm 1$ d'où $a_1 b_2 - b_1 a_2 = \pm 1$. Aussi, d'après l'identité de Bezout, nous en déduisons que a_1, b_1 sont premiers entre eux.
- Supposons que a_1 et b_1 sont premiers entre eux: alors d'après l'identité de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tels que $a_1 u + b_1 v = 1$. Alors en posant $a_2 = u$ et $b_2 = -v$ nous en déduisons que la matrice $A = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}$, nous avons $A \in \mathcal{M}_2(\mathbb{Z})$ et $\det(A) = 1$. Aussi, $(e'_1; e'_2)$ (les deux vecteurs colonnes de A) est une $\mathbb{Z}$ -base de $\mathcal{R}$.
- $e'_1 = \begin{pmatrix} 7 \\ 10 \end{pmatrix}$. Alors les coefficients de Bezout sont (par exemple) $7 \times 3 + (-2) \times 10 = 1$. D'où $e'_2 = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ est un vecteur tel que (e'_1, e'_2) est une $\mathbb{Z}$ -base de $\mathcal{R}$.

Partie B: transformations linéaires du réseau

Soit $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ une application linéaire de matrice A dans la base canonique $\mathcal{C} = (e_1, e_2)$.

I. Supposons déjà que $f(\mathcal{R}) \subset \mathcal{R}$. Aussi, pour tout $X \in \mathcal{R}$, $f(X) \in \mathcal{R}$. Ainsi, $\forall X = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{R}$, $f(X)$ est un vecteur à coefficients entiers. Il suffit alors de prendre les images de f des vecteurs $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ pour conclure. En effet, si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, alors $Ae_1 = \begin{pmatrix} a \\ c \end{pmatrix}$ et $Ae_2 = \begin{pmatrix} b \\ d \end{pmatrix}$ sont à coefficients entiers, d'où les coefficients de A sont tous des entiers relatifs.

Réciproquement, supposons que la matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ai tous ses coefficients entiers. Alors pour tout vecteur $X \in \mathcal{R}$, nous aurons $f(X) \in \mathcal{R}$ (puisque les coefficients seront des entiers).

II. On suppose ici que $f(\mathcal{R}) = \mathcal{R}$.

- Puisque $e_1, e_2 \in \mathcal{R}$ sont des éléments de $\mathcal{R} = \text{Im}(f)$ sont linéairement indépendants, il s'ensuit que $\text{Im}(f)$ contient deux vecteurs linéairement indépendants.

2. $\text{Im}(f)$ contient e_1 et e_2 , donc désignons par u_1, u_2 leurs antécédents. Soit $X = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{R}$ quelconque: nous avons alors par linéarité de f :

$$f(xu_1 + yu_2) = xf(u_1) + yf(u_2) = xe_1 + ye_2 = X$$

Il s'ensuit que f est surjective.

Comme f est une application linéaire de $\mathbb{R}^2$ dans lui-même, nous savons que *bijective* $\Leftrightarrow$ *surjective* $\Leftrightarrow$ *injective*. Ainsi, puisque f est surjective, f est bijective.

3. La fonction f étant bijective, on désigne par f^{-1} sa fonction réciproque. De $f(\mathcal{R}) = \mathcal{R}$, nous déduisons que $f^{-1}(\mathcal{R}) \subset \mathcal{R}$.
4. L'application f étant bijective, sa matrice associée A est inversible: aussi, on note A^{-1} sa matrice inverse. Cette matrice est associée à la fonction réciproque f^{-1} . De $f^{-1}(\mathcal{R}) \subset \mathcal{R}$, nous déduisons que les coefficients de A^{-1} sont tous des entiers relatifs (on procède comme en question)