TD 24 : corrigé de l'exercice 13

Exercice 22.13 :

• Si φ est de la forme indiquée, c'est clairement un endomorphisme du groupe $(\mathbb{Z}^p, +)$. De plus, $det(A) = \pm 1$, donc $A^{-1} = \pm {}^t Cof(A)$. Ainsi, A^{-1} est une matrice dont les coefficients sont aussi dans $\mathbb{Z}$. L'application $X \longmapsto A^{-1}X$ est donc un endomorphisme de $\mathbb{Z}^p$, qui est clairement l'inverse de φ, donc φ est un automorphisme du groupe $(\mathbb{Z}^p, +)$.

• Réciproquement, supposons que φ est un automorphisme du groupe $(\mathbb{Z}^p, +)$.
Soit $X \in \mathbb{Z}^p$. On montre par récurrence sur $n \in \mathbb{N}$ que $\varphi(nX) = n\varphi(X)$. De plus, $\varphi(-X) = -\varphi(X)$, donc, pour tout $n \in \mathbb{Z}$, $\varphi(nX) = n\varphi(X)$.
Notons $e = (e_1, \ldots, e_p)$ la base canonique de $\mathbb{R}^p$.
Si $X = \sum_{i=1}^{p} x_i e_i \in \mathbb{Z}^p$, $\varphi(X) = \sum_{i=1}^{p} x_i \varphi(e_i)$. Notons A la matrice de $\mathcal{M}_p(\mathbb{R})$ dont la $j^{\text{ème}}$ colonne est constituée par $\varphi(e_j)$. Ainsi, $\varphi(X) = AX$.
Clairement, les coefficients de A sont dans $\mathbb{Z}$.
De même, il existe $B \in \mathcal{M}_p(\mathbb{R})$ telle que, pour tout $X \in \mathbb{Z}^p$, $\varphi^{-1}(X) = BX$, les coefficients de B étant dans $\mathbb{Z}$.
Pour tout $i \in \mathbb{N}_p$, $ABe_i = \varphi(\varphi^{-1}(e_i)) = e_i$, donc les matrices AB et I_p ont la même image de la base canonique. Ainsi, $AB = I_p$. En particulier, $det(A)det(B) = 1$, mais $det(A)$ et $det(B)$ sont des entiers relatifs, donc $det(A) = \pm 1$.