Feuille d'exercices 24.
Corrigé de trois exercices

Exercice 24.12 :

• Si φ est de la forme indiquée, c'est clairement un endomorphisme du groupe $(\mathbb{Z}^p, +)$. De plus, $det(A) = \pm 1$, donc $A^{-1} = \pm {}^tCof(A)$. 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 $det(A) = \pm 1$.

Exercice 24.13 :

"i)" est vrai si et seulement s'il existe $\alpha \in \mathbb{C}$ tel que $X - \alpha$ divise P et Q, c'est-à-dire s'il existe $\alpha \in \mathbb{C}$ tel que $X - \alpha$ divise $P \wedge Q$. $\mathbb{C}[X]$ étant algébriquement clos, ceci est vrai si et seulement si $P \wedge Q$ est un polynôme de degré supérieur à 1. On a montré que $i) \Longleftrightarrow ii)$.

Supposons ii) : $P \wedge Q$ divise P et Q, donc il existe $(U, V) \in \mathbb{C}[X]^2$ tel que $P = U(P \wedge Q)$ et $Q = V(P \wedge Q)$.
$VP - UQ = VU(P \wedge Q) - UV(P \wedge Q) = 0$. De plus, $deg(V) = deg(Q) - deg(P \wedge Q) \leq n-1$ d'après ii), et $deg(-U) = deg(P) - deg(P \wedge Q) \leq m - 1$.
Ainsi, on a prouvé que $ii) \Longrightarrow iii)$.
Réciproquement, supposons iii) : Il existe deux polynômes A et B de $\mathbb{C}[X]$, non nuls, tels que $deg(A) \leq n - 1$, $deg(B) \leq m - 1$ et $AP + BQ = 0$.

Raisonnons par l'absurde en supposant que P et Q sont premiers entre eux.
$AP = -BQ$, donc P divise BQ. D'après le théorème de Gauss, P divise B. Ainsi, il existe $R \in \mathbb{C}[X]$ tel que $B = RP$. $deg(R) = deg(B) - deg(P) < 0$, donc $R = 0$. On en déduit que $B = 0$, ce qui est faux. Ainsi, P et Q ne sont pas premiers entre eux. Comme ils sont non nuls, leur PGCD est de degré supérieur ou égal à 1.
Ainsi, $ii) \iff iii)$.

"iii)" est vrai si et seulement s'il existe deux polynômes A et B de $\mathbb{C}[X]$, tous deux nuls non nuls, tels que $deg(A) \leq n-1$, $deg(B) \leq m-1$ et $AP + BQ = 0$, donc si et seulement s'il existe deux familles toutes deux nulles non nulles $(a_i)_{0\leq i\leq n-1} \in \mathbb{C}^n$ et $(b_i)_{0\leq i\leq m-1} \in \mathbb{C}^m$ telles que $\sum_{i=0}^{n-1} a_i X^i P + \sum_{i=0}^{m-1} b_i X^i Q = 0$, donc $iii) \implies iv)$.
Réciproquement, si $iv)$, il existe $(a_0, \dots, a_{n-1}, b_0, \dots, b_{m-1}) \neq 0$
telle que $\sum_{i=0}^{n-1} a_i X^i P + \sum_{i=0}^{m-1} b_i X^i Q = 0$.
Dans ces conditions, si $(a_i)_{0\leq i\leq n-1} = 0$, alors $(b_i)_{0\leq i\leq m-1} = 0$, ce qui est faux, donc $(a_i)_{0\leq i\leq n-1} \neq 0$ et de même, $(b_i)_{0\leq i\leq m-1} \neq 0$, d'où "iii)".
On a prouvé que $iii) \iff iv)$.

Supposons iv) : La famille $(P, XP, \dots, X^{n-1}P, Q, XQ, \dots, X^{m-1}Q)$ est une famille de $\mathbb{C}_{n+m-1}[X]$. Dans la base canonique $(1, X, \dots, X^{n+m-1})$ de $\mathbb{C}_{n+m-1}[X]$, les vecteurs colonnes des coordonnées de ces polynômes sont respectivement
$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ a_0 \\ \vdots \\ a_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_0 \\ a_1 \\ \vdots \\ a_m \end{pmatrix}, \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ b_0 \\ \vdots \\ b_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ b_0 \\ b_1 \\ \vdots \\ b_n \end{pmatrix}.$$
Ainsi, la famille $(P, XP, \dots, X^{n-1}P, Q, XQ, \dots, X^{m-1}Q)$ est liée si et seulement si ces vecteurs colonnes sont liés, donc si et seulement si la matrice dont les colonnes sont ces vecteurs n'est pas inversible, ou encore si et seulement si cette matrice est de déterminant nul, or cette matrice est exactement celle qui est définie dans l'énoncé. On a donc prouvé que $iv) \iff v)$.
Ce déterminant s'appelle le résultant des deux polynômes P et Q.

Exercice 24.14 :

- Supposons que f est une famille liée.

Il existe une famille non nulle $(a_i)_{1\leq i\leq n} \in \mathbb{R}^n$ tel que $\sum_{i=1}^{n} a_i f_i = 0$.

Soit $(x_1, \dots, x_n) \in \mathbb{R}^n$. Notons $L_1, \dots, L_n$ les lignes de la matrice $M = \Big((f_i(x_j)\Big)_{\substack{1\leq i\leq n \\ 1\leq j\leq n}}$.

Pour tout $j \in \mathbb{N}_n$, $\sum_{i=1}^{n} a_i f_i(x_j) = 0$, donc $\sum_{i=1}^{n} a_i L_i = 0$. Ainsi, les lignes de M sont liées, ce qui prouve que $det(M) = 0$.
La contraposée de ce qui précède montre que, s'il existe une famille de n réels $(x_1, \dots, x_n)$ telle que $det\Big((f_i(x_j)\Big)_{\substack{1\leq i\leq n\\1\leq j\leq n}} \neq 0$, alors f est une famille libre.

- Réciproquement, supposons que f est une famille libre.

Soit $k \in \mathbb{N}_n$. Notons $R(k)$ l'assertion suivante :
il existe $(x_1, \dots, x_k) \in \mathbb{R}^k$ tel que $det\Big((f_i(x_j)\Big)_{\substack{1\leq i\leq k\\1\leq j\leq k}} \neq 0$.
Pour $k = 1$, f_1 est une application non identiquement nulle, car f est libre, donc il existe $x_1 \in \mathbb{R}$ tel que $f_1(x_1) \neq 0$. Ceci prouve $R(1)$.
Pour $1 \leq k \leq n-1$, supposons $R(k)$.
Soit $x \in \mathbb{R}$. Posons $\Delta(x) = \begin{vmatrix} f_1(x_1) & f_1(x_2) & \cdots & f_1(x_k) & f_1(x) \\ f_2(x_1) & f_2(x_2) & \cdots & f_2(x_k) & f_2(x) \\ \vdots & \vdots & & \vdots & \vdots \\ f_k(x_1) & f_k(x_2) & \cdots & f_k(x_k) & f_k(x) \\ f_{k+1}(x_1) & f_{k+1}(x_2) & \cdots & f_{k+1}(x_k) & f_{k+1}(x) \end{vmatrix}$. En développant $\Delta(x)$ selon la dernière colonne, on voit qu'il existe une famille $(b_1, \dots, b_{k+1})$ de $k+1$ réels indépendants de x telle que $\Delta(x) = \sum_{i=1}^{k+1} b_i f_i(x)$. De plus, $b_{k+1} = det\Big((f_i(x_j)\Big)_{\substack{1\leq i\leq k\\1\leq j\leq k}}$, donc, d'après $R(k)$, $b_{k+1} \neq 0$.
Supposons que Δ est l'application identiquement nulle. Alors $\sum_{i=1}^{k+1} b_i f_i = 0$ et $b_{k+1} \neq 0$, donc f est liée, ce qui est faux. Ainsi Δ n'est pas identiquement nulle, c'est-à-dire qu'il existe $x_{k+1} \in \mathbb{R}$ tel que $\Delta(x_{k+1}) \neq 0$. Or, $\Delta(x_{k+1}) = det\Big((f_i(x_j)\Big)_{\substack{1\leq i\leq k+1\\1\leq j\leq k+1}}$, donc $R(k+1)$ est prouvée.
Ainsi $R(n)$ est vraie, ce qui prouve la réciproque.