En pratique, on obtient les bases $\mathcal{B}$ et $\mathcal{C}$ en faisant des opérations élémentaires sur la matrice de f dans les bases standards :

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \xrightarrow[L_2'=L_2-3L_1]{} \begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix} \xrightarrow[L_1'=L_1+L_2]{} \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix} \xrightarrow[L_2'=\frac{L_2}{-2}]{} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

C'est exactement ce qu'on fera pour démontrer le théorème de classification des morphismes de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$.

<u>Déf.</u> : Soient $n \in \mathbb{N}$, $i,j \in \{1,\dots,n\}$. La matrice standard $e_{ij} \in M_{n\times n}(\mathbb{Z})$ est la matrice dont tous les coefficients sont nuls sauf l'élément (i,j) qui vaut 1.

<u>ex</u> : $(n=2)$ $e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ $e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

<u>Déf.</u> : Soit $n \in \mathbb{N}$. Une matrice de transvection à coefficients dans $\mathbb{Z}$ est une matrice de la forme $I_n + q e_{ij} =: e_{ij}(q)$ où $q \in \mathbb{Z}$, $i,j \in \{1,\dots,n\}$, $i \neq j$.

<u>exemples</u> : $n=2$, $e_{1,2}(3) = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$ $e_{2,1}(-36) = \begin{pmatrix} 1 & 0 \\ -36 & 1 \end{pmatrix}$

<u>Prop.</u> : Soit $a \in M_{n\times m}(\mathbb{Z})$ et $q \in \mathbb{Z}$.
1) Soient $i,j \in \{1,\dots,n\}$ $i\neq j$, la matrice $e_{ij}(q)a$ est la matrice obtenue à partir de la matrice a en remplaçant la i-ème ligne de a par la somme de la i-ème ligne de a et q fois la j-ème ligne de a.
2) Soient $i,j \in \{1,\dots,n\}$, $i \neq j$. La matrice $a e_{ij}(q)$ est obtenue à partir de a en rajoutant q fois la i-ème colonne de a à la j-ème colonne de a.

<u>Corollaire</u> : La matrice de transvection $e_{ij}(q)$ est inversible en tant que matrice à coefficients dans $\mathbb{Z}$ et $e_{ij}(q)^{-1} = e_{ij}(-q)$.

<u>Notation</u> : $\mathrm{diag}_{n\times m}(d_1,\dots,d_\ell) = \begin{pmatrix} d_1 & & & & \\ & \ddots & & 0 & \\ & & d_\ell & & \\ & 0 & & 0 & \\ & & & & \ddots \;\; 0 \end{pmatrix} \in M_{n\times m}(\mathbb{Z})$ lorsque $d_1,\dots,d_\ell \in \mathbb{Z}$, $\ell \leq \min\{m,n\}$

<u>Théorème</u> (forme normale de Smith) :

Soient $m,n \in \mathbb{N}$. Soit $a \in M_{n\times m}(\mathbb{Z})$. Il existe $u \in M_{n\times n}(\mathbb{Z})$, $v \in M_{m\times m}(\mathbb{Z})$, $\ell \in \mathbb{N}$, $d_1,\dots,d_\ell \in \mathbb{Z}\setminus\{0\}$ tels que
1) $uav = \mathrm{diag}(d_1,\dots,d_\ell)$
2) u et v sont des produits de matrices de transvection à coeff dans $\mathbb{Z}$
3) d_i divise d_{i+1}, $i=1,\dots,\ell-1$

La démonstration est basée sur l'algorithme de Smith qui marche sur n'importe quel anneau euclidien (ici $\mathbb{Z}$).
Au lieu de faire le cas général, illustrons cet algorithme sur un cas concret.

Soit $a = \begin{pmatrix} 2 & -2 & -2 \\ -4 & 1 & 5 \\ 0 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix} \in M_{4\times 3}(\mathbb{Z})$.

Dans un premier temps, on veut rendre nuls les éléments $(1,2)$ et $(1,3)$. Pour cela il suffit de rajouter colonne 1 à colonne 2.

$$a\underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{e_{1,2}(1)} = \begin{pmatrix} 2 & 0 & -2 \\ -4 & -3 & 5 \\ 0 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix}$$

De même pour rendre nul l'élément $(1,3)$:

$$a e_{12}(1) e_{13}(1) = \begin{pmatrix} 2 & 0 & 0 \\ -4 & -3 & 1 \\ 0 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix}$$

Créons des zéros en-dessous de l'élément (1,1).

$e_{21}(2)\, a\, e_{12}(1) e_{13}(1) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -3 & 1 \\ 0 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix} = a'$.

Remarquons qu'on peut rendre toute matrice a sous la forme grâce à ces opérations

$$\begin{pmatrix} * & 0 & \cdots & 0 \\ 0 & \circledast & \cdots & \circledast \\ \vdots & \vdots & & \vdots \\ 0 & \circledast & \cdots & \circledast \end{pmatrix} \quad \begin{array}{l} * = \text{non nul} \\ \circledast = \text{nul ou non nul} \end{array}$$

- En effet, si $a \neq 0$ et $a_{11} = 0$, il existe $a_{ij} \neq 0$. On remplace a par $a e_{j1}(1)$. Deux possibilités : $(a e_{j1}(1))_{11} \neq 0$, auquel cas on a obtenu une matrice dont l'élément (1,1) est non nul ; ou bien $(a e_{j1}(1))_{11} = 0$, auquel cas on rajoute la i-ème ligne de $a e_{j1}(1)$ à la première ligne : $e_{1i}(1)\, a e_{j1}(1)$ etc.
On peut donc toujours rendre $a_{11} \neq 0$ en multipliant par des matrices de transvection.
- Le reste sera une conséquence de la division euclidienne comme on verra ci-dessous. ici $2 \mid -2$ et $2 \mid -4$ donc pas besoin

Comme on veut que l'élément d_1 divise le reste de la matrice, on n'a pas terminé avec la première ligne et la première colonne.
On rajoute à la première ligne de a' la ligne contenant un élément non divisible par a_{11}. $e_{12}(1)\, a' = \begin{pmatrix} 2 & -3 & 1 \\ 0 & -3 & 1 \\ 0 & -2 & 1 \\ 0 & -2 & 1 \end{pmatrix}$.
On recommence à créer des zéros à droite et en-dessous de l'élément (1,1).
Interdit : $e_{12}(1)\, a' e_{12}(3/2)$
On effectue la division euclidienne de -3 par 2 : $-3 = (-2) \times 2 + 1$.
On a $q = -2$, $r = 1 = -3 - q \times 2$. On veut remplacer -3 par le reste dans cette division euclidienne, à savoir 1. Cela correspond à soustraire q fois la première colonne de la deuxième

$e_{12}(1)\, a' e_{12}(-q) = \begin{pmatrix} 2 & 1 & 1 \\ 0 & -3 & 1 \\ 0 & -2 & 1 \\ 0 & -1 & 1 \end{pmatrix}$ Puis on continue l'algorithme d'Euclide sur ces nombres $-3, 2, 1, 0$
$2 = 2 \times 1 + 0$: on retranche 2 fois colonne 2 de colonne 1.

$\to \begin{pmatrix} 0 & 1 & 1 \\ 6 & -3 & 1 \\ 4 & -2 & 1 \\ 2 & -1 & 1 \end{pmatrix}$ Puis, on rajoute colonne 2 à colonne 1 : $\begin{pmatrix} 1 & 1 & 1 \\ 3 & -3 & 1 \\ 2 & -2 & 1 \\ 1 & -1 & 1 \end{pmatrix}$ et on retranche la première de la 2ème : $\begin{pmatrix} 1 & 0 & 1 \\ 3 & -6 & 1 \\ 2 & -4 & 1 \\ 1 & -2 & 1 \end{pmatrix}$

Ensuite, on soustrait colonne 1 de colonne 3 : $\begin{pmatrix} 1 & 0 & 0 \\ 3 & -6 & -2 \\ 2 & -4 & -1 \\ 1 & -2 & 0 \end{pmatrix}$ On crée des zéros en-dessous de l'élément (1,1) : $d_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -6 & -2 \\ 0 & -4 & -1 \\ 0 & -2 & 0 \end{pmatrix} \xrightarrow{C_2' = C_2 - 3C_3}$

d_1 divise tous les autres éléments de la matrice.
On veut ensuite créer des zéros à droite et en-dessous de l'élément (2,2) jusqu'à obtenir un élément d_2 en (2,2) qui divise tous les éléments de la matrice si on supprime lignes 1, 2 et colonnes 1, 2.

$$\to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & -1 & -1 \\ 0 & -2 & 0 \end{pmatrix} \xrightarrow{C_2' = C_2 + C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -2 \\ 0 & -2 & -1 \\ 0 & -2 & 0 \end{pmatrix} \xrightarrow{C_3' = C_3 - C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & -2 & 1 \\ 0 & -2 & 2 \end{pmatrix} \xrightarrow{\substack{L_3' = L_3 - L_2 \\ L_4' = L_4 - L_2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\xrightarrow{L_2' = L_2 + L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix} \xrightarrow{C_2' = C_2 + 2C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 4 & 2 \end{pmatrix} \xrightarrow{C_2' = C_2 + C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 3 & 1 \\ 0 & 6 & 2 \end{pmatrix}$$

$$\xrightarrow{C_3' = C_3 - C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & -2 \\ 0 & 6 & -4 \end{pmatrix} \xrightarrow{\substack{L_3' = L_3 - 3L_2 \\ L_4' = L_4 - 6L_2}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1^{d_2} & 0 \\ 0 & 0 & -2 \\ 0 & 0 & -4 \end{pmatrix} \xrightarrow{L_4' = L_4 - 2L_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix} = \operatorname{diag}(1, 1, -2) = uav.$$

Déf. : Soient $a, b \in M_{n\times m}(\mathbb{Z})$. a et b sont équivalentes s'il existe $u \in GL_n(\mathbb{Z})$ et $v \in GL_m(\mathbb{Z})$ telles que $uav = b$.

Rappel : $GL_n(\mathbb{Z}) = \{u \in M_{n\times n}(\mathbb{Z}) \,/\, \exists u' \in M_{n\times n}(\mathbb{Z}) \text{ avec } uu' = I_n = u'u\}$
$= M_{n\times n}(\mathbb{Z})^\times$.

⚠ Si $u \in M_{n\times n}(\mathbb{Z})$ et $\det u \neq 0$, on n'a pas forcément $u \in GL_n(\mathbb{Z})$.
Par exemple $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \notin GL_2(\mathbb{Z})$.

En fait $GL_n(\mathbb{Z}) = \{u \in M_{n\times n}(\mathbb{Z}) \,/\, \det u = \pm 1\}$. exo
On a vu que $e_{ij}(q) \in GL_n(\mathbb{Z})$.

Théorème : Soit $a \in M_{n\times m}(\mathbb{Z})$. Alors il existe $d_1, \dots, d_\ell \in \mathbb{N}\setminus\{0\}$ avec $d_i \mid d_{i+1}$ tels que a est équivalente à $\mathrm{diag}(d_1, \dots, d_\ell)$.
De plus, $\ell, d_1, \dots, d_\ell$ sont uniquement déterminés par a.

Preuve : On applique Smith à a : $uav = \mathrm{diag}(d_1', \dots, d_\ell')$ où $d_i' \in \mathbb{Z}\setminus\{0\}$, $d_i' \mid d_{i+1}'$ et u et v sont des produits de matrices de transvection. On a $u \in GL_n(\mathbb{Z})$, $v \in GL_m(\mathbb{Z})$.

Soit $\Delta = \begin{pmatrix} \text{signe}(d_1') & & & & & \\ & \text{signe}(d_2') & & & 0 & \\ & & \ddots & & & \\ & & & \text{signe}(d_\ell') & & \\ & 0 & & & 1 & \\ & & & & & \ddots \; 1 \end{pmatrix} \in GL_n(\mathbb{Z})$.

$\Delta uav = \mathrm{diag}(d_1, \dots, d_\ell)$ où $d_i = |d_i'|$
$\Delta u \in GL_n(\mathbb{Z})$, $v \in GL_m(\mathbb{Z})$ et $d_i \mid d_{i+1}$, $d_i \in \mathbb{N}\setminus\{0\}$.
Cela montre l'existence.
L'unicité : $d_1 = |\mathrm{pgcd}(a_{ij})|$, $d_2 = |\mathrm{pgcd}(\{\text{mineurs } 2\times 2 \text{ de } a\})|$. □
(trop long)

Déf. : Soit $a \in M_{n\times m}(\mathbb{Z})$. Soient $d_1, \dots, d_\ell \in \mathbb{N}\setminus\{0\}$ tels que a équivalente à $\mathrm{diag}(d_1, \dots, d_\ell)$ avec $d_1 \mid d_2, \dots, d_{\ell-1} \mid d_\ell$.
Les entiers naturels $d_1, \dots, d_\ell$ sont les <u>facteurs invariants</u> de a.
Le nombre ℓ de facteurs invariants de a est le <u>rang</u> de a.

Corollaire : Soient $a, b \in M_{n\times m}(\mathbb{Z})$. a et b sont équivalentes ssi elles ont (même rang et) mêmes facteurs invariants.

Revenons aux sous-groupes de $\mathbb{Z}^n$:

Théorème : Soit $G \subseteq \mathbb{Z}^n$ un sous-groupe. Alors, il existe une base $e_1', \dots, e_n'$ de $\mathbb{Z}^n$ dans laquelle $G = \langle d_1 e_1', \dots, d_\ell e_\ell' \rangle$ où $\ell \leq n$, $d_i \in \mathbb{N}\setminus\{0\}$ et $d_i \mid d_{i+1}$.
(i.e. à changement de base près, tout sous-groupe de $\mathbb{Z}^n$ est "diagonal" ou encore de la forme $d_1\mathbb{Z} \times d_2\mathbb{Z} \times \dots \times d_\ell\mathbb{Z} \times \{0\} \times \dots \times \{0\}$)

Preuve : D'après un résultat précédent, G est de type fini, i.e. il existe $a_1, \dots, a_m \in \mathbb{Z}^n$ tq $G = \langle a_1, \dots, a_m \rangle$.
Soit $a \in M_{n\times m}(\mathbb{Z})$ de colonnes $a_1, \dots, a_m$. D'après le th précédent il existe $u \in GL_n(\mathbb{Z})$, $v \in GL_m(\mathbb{Z})$ telles que $uav = \mathrm{diag}(d_1, \dots, d_\ell)$ avec $d_i \in \mathbb{N}\setminus\{0\}$, $d_i \mid d_{i+1}$.
Soit $a' = av \in M_{n\times m}(\mathbb{Z})$ et $a_1', \dots, a_m'$ ses colonnes.
On a $a_j' \in \langle a_1, \dots, a_m \rangle = G$. Du coup, $\langle a_1', \dots, a_m' \rangle \subseteq \langle a_1, \dots, a_m \rangle$.
Comme $v \in GL_m(\mathbb{Z})$ on a aussi $\langle a_1', \dots, a_m' \rangle \supseteq \langle a_1, \dots, a_m \rangle$.
Du coup, $\langle a_1', \dots, a_m' \rangle = G$.
Soient $e_i' = u^{-1} e_i$, $i = 1, \dots, n$. $B' = (e_1', \dots, e_n')$ est une base de $\mathbb{Z}^n$.
Le vecteur coordonnées de a_j' dans la base B' est $ua_j' = (ua')_j = (uav)_j = \begin{cases} d_j e_j & \text{si } 1 \leq j \leq \ell \\ 0 & \text{sinon} \end{cases}$ i.e., $a_j' = \begin{cases} d_j e_j' & \text{si } 1 \leq j \leq \ell \\ 0 & \text{sinon} \end{cases}$.

$G = \langle a_1', \dots, a_n' \rangle = \langle a_1', \dots, a_\ell' \rangle = \langle a_1 e_1', \dots, d_\ell e_\ell' \rangle$. □

<u>Théorème</u> (Classification des groupes abéliens de type fini) :
Soit G un groupe abélien de type fini. Alors, il existe $r, \ell \in \mathbb{N}$ et $d_1, \dots, d_\ell \geq 2$ avec $d_i | d_{i+1}$ tels que G est isomorphe à $\frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \frac{\mathbb{Z}}{d_2\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{d_\ell\mathbb{Z}} \times \mathbb{Z}^r$.
De plus, $r, \ell, d_1, \dots, d_\ell$ sont uniquement déterminés par G.

<u>Preuve</u> : On a vu que G est isomorphe à $\mathbb{Z}^n/H$, où $H \subseteq \mathbb{Z}^n$ sous-groupe.
D'après le th. précédent, on peut supposer que $H = \langle d_1 e_1, d_2 e_2, \dots, d_{\ell'} e_{\ell'} \rangle$ où $\ell' \leq n$, $d_i \in \mathbb{N} \setminus \{0\}$, $d_i | d_{i+1}$.
Du coup, $H = d_1\mathbb{Z} \times \dots \times d_{\ell'}\mathbb{Z} \times \{0\} \times \dots \times \{0\} \subseteq \mathbb{Z}^n$
et $\mathbb{Z}^n/H \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_{\ell'}} \times \mathbb{Z} \times \dots \times \mathbb{Z}$
$= \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_{\ell'}} \times \mathbb{Z}^r$ où $r = n - \ell'$.
Soit $m \leq \ell'$ tq $d_1 = \dots = d_m = 1$, $d_{m+1} \neq 1$
$G \simeq \mathbb{Z}^n/H \simeq \mathbb{Z}_{d_{m+1}} \times \dots \times \mathbb{Z}_{d_{\ell'}} \times \mathbb{Z}^r$.
Poser $d_i = d_{m+i}$, $\ell = \ell' - m$. $G \simeq \mathbb{Z}^n/H \simeq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_\ell} \times \mathbb{Z}^r$. □