Exercice 1. *Soit M une matrice de $\mathbb{M}_n(\mathbb{R})$; les lettres L, L' (resp. U, U') désigne des matrices triangulaires inférieures (resp. supérieures) avec des coefficients diagonaux égaux à 1. La lettre D désigne une matrice diagonale.*

(1) Montrez que l'on peut mettre M sous la forme LU (resp. LDU) si et seulement si $\det M^{(k)} = 1$ (resp. $\det M^{(k)} \neq 0$) pour tout $1 \leq k \leq n$ où $M^{(k)}$ désigne le mineur principal d'ordre k.

(2) Écrire la matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ sous la forme $U'LU$. Trouvez une matrice de $\mathbb{M}_2(\mathbb{R})$ qui ne peut pas s'écrire sous la forme LDU où D désigne une matrice diagonale.

(3) On note M_k la matrice obtenue à partir de M en substituant sa dernière ligne à sa ligne d'indice k. On suppose que $\det M_k^{(k)} \neq 0$ pour tout $1 \leq k \leq n$. Montrez que l'on peut mettre, de manière unique, M sous la forme $U'LU$ où U, U' ont des coefficients nuls en dehors de sa diagonale et de la dernière colonne.

(4) Soit $M \in GL_n(\mathbb{R})$, montrez qu'il existe U' avec $n-1$ coefficients nuls sur sa dernière colonne telle que les k première lignes de $(U'M)^{(k+1)}$ sont indépendantes pour tout $k < n$.

(5) Montrez que toute matrice M de déterminant n peut se mettre sous la forme $L'U'LU$ où L' a ses coefficients nuls hors de sa diagonale et de sa dernière ligne.

Preuve : (1) La preuve est identique dans le cas respé, on traite la décomposition LU. Supposons par récurrence que $M^{(n-1)} = LU$. On a

$$M = \begin{pmatrix} LU & A \\ B & m \end{pmatrix} = \begin{pmatrix} L & 0 \\ BU^{-1} & 1 \end{pmatrix} \begin{pmatrix} U & L^{-1}A \\ 0 & m' \end{pmatrix}$$

où $m' = m - BU^{-1}L^{-1}A$. Par passage au déterminant on a $m' = 1$ d'où le résultat. Pour l'unicité si $LU = L'U'$ alors $L'^{-1}L = U'U^{-1}$ qui est forcément égale à l'identité.

(2) La décomposition

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & -\tan(\theta/2) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \sin\theta & 1 \end{pmatrix} \begin{pmatrix} 1 & -\tan(\theta/2) \\ 0 & 1 \end{pmatrix}$$

est utilisée pour implémenter la rotation des images numériques. La matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ne peut pas s'écrire sous la forme LDU.

(3) On note $(c_1, \cdots, c_{n-1}, 1)$ les coefficients de la dernière colonne de U'^{-1}. Par multi-linéarité du déterminant on a

$$\det(U'^{-1}M)^{(k)} = \det M^{(k)} + \sum_{j=1}^{k} c_j M_j^{(k)}$$

Les équations $\det(U'^{-1}M)^{(k)} = 1$ pour $1 \leq k \leq n-1$ forment un système triangulaire inversible car $\det M_k^{(k)} \neq 0$, il a donc une unique solution et $(U'^{-1}M)^{(k)} = LU$ d'après (1).

(4) On démontre cette propriété pour tout $k \leq r$ par récurrence sur $r < n$ en utilisant que les matrices U' forment un groupe. On note $U_{k,k}$ la matrice identité et $U_{k,l}$ $(k < l < n)$la matrice qui par multiplication à gauche ajoute la ligne l à la ligne k. On extrait de M les matrices supérieures gauche $M^{(i,j)} \in \mathbb{M}_{i,j}(\mathbb{R})$.

Pour $r = 1$, $\mathrm{rg} M^{(n,2)}) = 2$ garantit $\mathrm{rg} M^{(n-1,2)} \geq 1$. Si la première ligne de $M^{(n-1,2)}$ est nulle on note $l > 1$ l'indice d'une ligne non nulle, sinon on pose $l = 1$. La matrice $U' = U_{1,l}$ convient, i.e. la première ligne de $(U_{1,l}M)^{(2)}$ n'est pas nulle.

On suppose que M satisfait la propriété pour tout $k \leq r-1$ si bien que les $r-1$ premières lignes de $M^{(n-1,r+1)}$ sont indépendantes. Par ailleurs, $\mathrm{rg} M^{(n-1,r+1)} \geq \mathrm{rg} M^{(n,r+1)} - 1 = r$. On choisit $U' = U_{r,l}$ où $l = r$ si la r-ième ligne de $M^{(n-1,r+1)}$ est indépendante des précédentes et $l > r$ est l'indice d'une ligne indépendante sinon. Les r premières lignes de $(U'M)^{(k+1)}$ sont alors indépendantes pour tout $k \leq r$.

(5) Soit U_0 la matrice obtenue en appliquant la question précédente à M. On remarque que $L_0 = L'^{-1}$ est de la même forme que L' et donc que U_0 et L_0 commutent. Pour tout vecteur v indépendant des $(n-1)$-premières

lignes de M, on peut choisir L_0 telle que la multiplication à gauche de L_0 sur M change la dernière ligne de M en v. Par construction de U_0, il est possible de choisir les coefficients de v successivement pour que L_0U_0M satisfasse les hypothèses de la question (3). En notant U_1 la matrice U' obtenue en appliquant la question (3) à L_0U_0M on obtient $U_0L_0M = L_0U_0M = U_1LU$. On conclut en posant $U' = U_0^{-1}U_1$.

Exercice 2. *Soit (e_1, e_2, e_3) la base canonique de $\mathbb{Z}^3$ et soit $L \subset \mathbb{Z}^3$ le sous-groupe engendré par les vecteurs*

$$e_1' := 2e_1 - e_2 + e_3, \quad e_2' := e_1 + 4e_2 - e_3, \quad e_3' := 3e_1 - e_2 - e_3$$

Trouver une base adaptée au sous-module L de $\mathbb{Z}^3$ et décrire $\mathbb{Z}^3/L$. Peut-on obtenir ce dernier résultat de manière plus rapide ?

Preuve : *Convention d'écriture de produits de matrices*: on opère sur les lignes d'une matrice A en la multipliant à gauche par des matrices L_i et on présente le calcul de la manière suivante où I désigne la matrice identité:

$$\begin{array}{ccc} & I & A \\ L_1 & L_1 & L_1A \\ L_2 & L_2L_1 & L_2L_1A \\ \cdots & \cdots & \cdots \end{array}$$

De même pour opérer sur les colonnes d'une matrice A on la multiplie à droite par des matrices R_i et on présente le calcul comme suit

$$\begin{array}{cccc} & R_1 & R_2 & \cdots \\ A & AR_1 & AR_2 & \cdots \\ I & R_1 & R_1R_2 & \cdots \end{array}$$

On écrit la matrice de passage

$$\begin{pmatrix} 2 & 1 & 3 \\ -1 & 4 & -1 \\ 1 & -1 & -1 \end{pmatrix}$$

et on commence par opérer sur les lignes

$$\begin{array}{ccc}
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 2 & 1 & 3 \\ -1 & 4 & -1 \\ 1 & -1 & -1 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix} & \begin{pmatrix} 2 & 1 & 3 \\ 1 & -1 & -1 \\ 0 & -3 & 2 \end{pmatrix} \\
\begin{pmatrix} 0 & 1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 2 \\ 0 & -1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & -1 \\ 0 & -3 & -5 \\ 0 & -3 & 2 \end{pmatrix}
\end{array}$$

puis sur les colonnes

$$\begin{array}{cccc}
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & -1 & 3 \end{pmatrix} \\
\begin{pmatrix} 1 & -1 & -1 \\ 0 & -3 & -5 \\ 0 & -3 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 3 & 2 \\ 0 & 3 & -5 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 3 & -5 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 8 & -21 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & 2 \\ 0 & -2 & 5 \\ 0 & 1 & -3 \end{pmatrix}
\end{array}$$

puis finalement

$$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 2 \\ 0 & -1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 8 & -21 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -8 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 2 \\ 8 & -1 & -15 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -21 \end{pmatrix}$$

La base adaptée est alors donnée par

$$f_1 = e'_1 = \begin{pmatrix} 2 & -1 & 1 \end{pmatrix} \quad f_2 = -e'_1 - 2e'_2 + e'_3 = \begin{pmatrix} -1 & -8 & 0 \end{pmatrix}$$

$$21f_3 = 2e'_1 + 5e'_2 - 3e'_3 = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$$

Comme vérification des calculs précédents on peut vérifier que le produit

$$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 2 \\ 8 & -1 & -15 \end{pmatrix} \begin{pmatrix} 2 & -1 & 0 \\ -1 & -8 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

est la matrice identité.

On en déduit alors que $\mathbb{Z}^3/L \simeq \mathbb{Z}/21\mathbb{Z}$. Le calcul du déterminant de la matrice de départ nous aurait donc donné 21 qui est donc égal au produit des facteurs invariants ce qui impose $a_1 = a_2 = 1$ et $a_3 = 21 = 3.7$ et donc $\mathbb{Z}^3/L \simeq \mathbb{Z}/21\mathbb{Z}$. On pourra se référer à l'exercice suivant.

Exercice 3. *Soit $x = (n_1, \dots, n_p) \in \mathbb{Z}^p$.*
a) Montrer que les conditions suivantes sont équivalentes :

1. *PGCD $(n_1, \dots, n_p) = 1$*
2. *Il existe $A \in SL_p(\mathbb{Z})$ telle que $A^t x =^t (1, 0, \dots, 0)$*
3. *Le vecteur x fait partie d'une base de $\mathbb{Z}^p$.*

b) On pose $p = 4$ et $x = (10, 6, 7, 11)$. Compléter x en une base de $\mathbb{Z}^4$.

Preuve : (i) implique (ii): le résultat se démontre par récurrence; la première étape du calcul est la suivante:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \cdots & u & v \\ 0 & \cdots & -n_r/(n_r, n_{r-1}) & n_{r-1}/(n_r, n_{r-1}) \end{pmatrix} \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} n_1 \\ \vdots \\ (n_r, n_{r-1}) \\ 0 \end{pmatrix}$$

où u et v sont les coefficients de Bezout entre n_{r-1} et n_r: $un_{r-1} + vn_r = (n_r, n_{r-1})$.

On considère $f : \mathbb{Z}^r \longrightarrow \mathbb{Z}$ défini par $f(a_1, \cdots, a_r) = a_1 n_1 + \cdots + a_r n_r$. Le théorème de la base adaptée, nous assure l'existence d'une base $(e_1, \cdots, e_n)$ de $\mathbb{Z}^n$ tel que $\operatorname{Ker} \phi = \mathbb{Z}a_1 e_1 \oplus \cdots \oplus \mathbb{Z}a_r e_r$ avec $a_i | a_{i+1}$ dans $\mathbb{Z}$ que l'on appelle les facteurs invariants de $\mathbb{Z}^n / \operatorname{Ker} \phi$; on a en outre que les a_i sont tous égaux à 1 pour $1 \leq i < r$ et $a_r = 0$ (par un argument de dimension). Ainsi si on note A transposée de la matrice de passage de la base $(e_r, e_{r-1}, \cdots, e_1)$ dans la base canonique, on a $A \in SL_r(\mathbb{Z})$ et $A \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

(ii) implique (iii): il est évident que la famille $\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = A^{-1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, A^{-1} \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots, A^{-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ forme une base de $\mathbb{Z}^n$.

(iii) implique (i): soit $e_2, \cdots, e_r$ une famille qui complète $\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}$ en une base et on note A la matrice de passage de cette base dans la base canonique; on calcule le déterminant de A en le développant par rapport à la première colonne de sorte que celui-ci est divisible par le pgcd des n_i qui est donc égal à 1 car $\det A = \pm 1$.

Exemples: le premier cas est simple car on a la relation $7 - 6 = 1$ de sorte que la matrice suivante est de déterminant -11

$$\begin{pmatrix} 10 & 6 & 7 & 11 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

de sorte que les 4 vecteurs colonnes de la transposée de la matrice ci-dessus constituent une base de $\mathbb{Z}^4$.
Dans le deuxième exemple on a la relation de Bezout: $1 = 6.6 - 2.10 - 15$. On cherche donc 6 coefficients a, b, c, d, e, f tels que $cf - de = 6$, $af - be = 2$ et $ad - bc = -1$. Par exemple la matrice suivante convient

$$\begin{pmatrix} 6 & 1 & 0 \\ 10 & 0 & -1 \\ 15 & 6 & 2 \end{pmatrix}$$

Exercice 4. *Résoudre dans $\mathbb{Z}^4$ le système*

$$\begin{pmatrix} 3 & 2 & 3 & 4 \\ 1 & -2 & 1 & -1 \end{pmatrix} X = \begin{pmatrix} -8 \\ -3 \end{pmatrix}$$

Preuve : Résoudre cette équation revient comme d'habitude à trouver une solution particulière, puis déterminer le noyau de la matrice en question. On fait d'une pierre deux coups en cherchant les éléments du noyau de la matrice

$$\begin{pmatrix} 3 & 2 & 3 & 4 & 8 \\ 1 & -2 & 1 & -1 & 3 \end{pmatrix}$$

dont la dernière coordonnées est 1. Les calculs sont les suivants où l'on calcule à chaque étape la matrice de passage:

$$\begin{array}{ccc}
 & \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ -3 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 3 & 2 & 3 & 4 & 8 \\ 1 & -2 & 1 & -1 & 3 \end{pmatrix} & \begin{pmatrix} \underline{0} & 1 & 3 & 4 & 8 \\ 8 & 3 & 1 & -1 & 3 \end{pmatrix} & \begin{pmatrix} 0 & \underline{0} & 1 & 4 & 8 \\ 8 & 8 & 3 & -1 & 3 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ -3 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 2 & 3 & 1 & 0 & 0 \\ -3 & -3 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}
\end{array}$$

$$\begin{array}{c}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & \underline{0} & 1 & 8 \\ 8 & 8 & 13 & 3 & 3 \end{pmatrix} \\ \begin{pmatrix} 2 & 3 & 4 & 1 & 0 \\ -3 & -3 & -4 & -1 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\end{array} \quad \begin{array}{c}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 8 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 0 & \underline{0} & 1 \\ 8 & 8 & 13 & 21 & 3 \end{pmatrix} \\ \begin{pmatrix} 2 & 3 & 4 & 8 & 1 \\ -3 & -3 & -4 & -8 & -1 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\end{array} \quad \begin{array}{c}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ \underline{0} & 8 & 13 & 21 & 3 \end{pmatrix} \\ \begin{pmatrix} -1 & 3 & 4 & 8 & 1 \\ 0 & -3 & -4 & -8 & -1 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\end{array}$$

$$\begin{array}{c}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 13 & 5 & 0 & 0 \\ 0 & -8 & -3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & \underline{0} & 1 & 21 & 3 \end{pmatrix} \\ \begin{pmatrix} -1 & 7 & 3 & 8 & 1 \\ 0 & -7 & -3 & -8 & -1 \\ 1 & -13 & -5 & 0 & 0 \\ 0 & 8 & 3 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix}\end{array} \quad \begin{array}{c}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 21 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \underline{0} & 1 & 3 \end{pmatrix} \\ \begin{pmatrix} -1 & 7 & 55 & 3 & 1 \\ 0 & -7 & -55 & -3 & -1 \\ 1 & -13 & -105 & -5 & 0 \\ 0 & 8 & 63 & 3 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}\end{array}$$

Ainsi une solution particulière est $X_0 = (55, -55, -105, 63)$ et l'ensemble des solutions est l'ensemble $X_0 + \alpha(-1, 0, 1, 0, 0) + \beta(7, -7, -13, 8)$ où α, β décrivent $\mathbb{Z}$.

Exercice 5. *Soient n un entier positif et $G \subset \mathbb{Z}^n$ un sous-groupe de rang n. Soit $(g_1, \cdots, g_n)$ une base de G ; on note M la matrice de passage de cette base dans la base canonique de $\mathbb{Z}^n$.*

(i) Montrer que le groupe $\mathbb{Z}^n/G$ est fini.

(ii) Montrer que card$((\mathbb{Z}^n/G)) = |\det M|$.

(iii) Soit H un groupe abélien engendré par trois éléments h_1, h_2, h_3 soumis aux relations

$$3h_1 + h_2 + h_3 = 0$$

$$25h_1 + 8h_2 + 10h_3 = 0$$

$$46h_1 + 20h_2 + 11h_3 = 0$$

Montrer que card$(H) = 19$ puis que $H \simeq \mathbb{Z}/19\mathbb{Z}$. Quelle généralisation cela suggère-t-il ?

(iv) Triangulariser la matrice

$$\begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix}$$

en multipliant à droite par une matrice de $SL_3(\mathbb{Z})$ que l'on précisera.

(v) En déduire un isomorphisme $\varphi : H \simeq \mathbb{Z}/19\mathbb{Z}$ et préciser les valeurs de $\varphi(h_1), \varphi(h_2), \varphi(h_3)$.

Preuve :

(i) Le théorème de la base adaptée fournit une base $(f_1, \cdots, f_n)$ de $\mathbb{Z}^n$ ainsi que des entiers $1 < a_1 | \cdots | a_n \neq 0$ tels que $(a_1 f_1, \cdots, a_n f_n)$ soit une base de G. On obtient alors $\mathbb{Z}^n/G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$.

(ii) D'après ce qui précède, on a donc $\mathrm{card}(\mathbb{Z}^n/G) = \prod_{i=1}^n a_i$ qui est donc égal à $\det M$.

(iii) Soit $M = \begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix}$ de sorte que $M \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ Il existe alors des matrices $L, R \in GL_3(\mathbb{Z})$ telles que $M = L\mathrm{diag}(a_1, a_2, a_3)R$ avec $a_1|a_2|a_3$. En outre si on pose $\begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} := R \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}$, H est aussi engendré par h'_1, h'_2, h'_3 et l'équation $L\mathrm{diag}(a_1, a_2, a_3) \begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ est équivalente à

$$\begin{cases} a_1 h'_1 = 0 \\ a_2 h'_2 = 0 \\ a_3 h'_3 = 0 \end{cases}$$

et donc $H \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \mathbb{Z}/a_3\mathbb{Z}$, avec $a_1.a_2.a_3 = \det M$. L'énoncé nous suggère de simplement calculer $\det M$; on vérifie aisément qu'il est égal à -19 (cf. (iv) ci-après) comme annoncé. On obtient alors $a_1 = a_2 = 1$ et $a_3 = 19$.

De manière général si la décomposition en facteurs premiers de $\det M$ ne fait apparaître aucune multiplicité (i.e. $p^2 \not| \det M$ pour tout premier p), alors tous les a_i sont égaux à 1 sauf le dernier égal à $\det M$ et le groupe quotient est alors cyclique.

(iv) On calcule

$$\begin{array}{cccc}
 & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & -1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix} \\
\begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix} & \begin{pmatrix} 3 & 1 & 0 \\ 25 & 8 & 2 \\ 46 & 20 & -9 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 8 & -1 & 2 \\ 20 & 14 & -9 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 8 & 1 & 0 \\ 20 & -14 & -19 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & -1 & 0 \\ 1 & 3 & -1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 2 \\ 1 & -3 & -5 \\ 0 & 0 & -1 \end{pmatrix}
\end{array}$$

(v) On a $\begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & -3 & -5 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}$ ce qui s'inverse facilement (la matrice est "triangulaire") soit $h_3 = h'_3$, $h_2 + 2h_3 = h'_1$ soit $h_2 = h'_1 - 2h'_3$ et $h_1 - 3h_2 - 5h_3 = h'_2$ soit $h_1 = 3h'_1 + h'_2 - h'_3$. Comme $\psi(h'_1) = \psi(h'_2) = 0$ et $\psi(h'_3) = 1$, on obtient $\psi(h_1) = -1$, $\psi(h_2) = -2$ et $\psi(h_3) = 1$.