Correction TD 5

† *Groupes abéliens de type fini*
Pour des raisons de lisibilité, on notera exceptionnellement $\mathbb{Z}/m$ au lieu de $\mathbb{Z}/m\mathbb{Z}$.
Rappelons à toutes fins utiles le joli théorème des restes chinois : si m et n sont premiers entre eux, alors

$$\mathbb{Z}/m \times \mathbb{Z}/n \simeq \mathbb{Z}/(nm)$$

et ça arrive d'ailleurs seulement si m et n sont premiers entre eux, dans le cas général, on a

$$\mathbb{Z}/m \times \mathbb{Z}/n \simeq \mathbb{Z}/(ppcm(m,n)) \times \mathbb{Z}/(pgcd(m,n))$$

Exercice 1. On sait que $8 = 2^3$, comme 2 n'est évidemment pas premier avec lui même, un groupe abélien d'ordre 8 est de la forme $\prod_{i=1}^n \mathbb{Z}/2^{n_i}$ tel que $\sum_{i=1}^n n_i = 3$, (autrement dit les n_i forment une ***partition*** de 3), les seuls options sont bien-sûr $3, 1+2, 1+1+1$, d'où les 3 groupes abéliens d'ordre 8 :

$$\mathbb{Z}/8, \quad \mathbb{Z}/2 \times \mathbb{Z}/4, \quad Z/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$$

Exercice 2.
1. On a $36 = 4.9 = 2^2.3^2$, par le théorème des restes chinois, un groupe d'ordre 36 est produit d'un groupe d'ordre 4 par un groupe d'ordre 9, les partitions de 2 sont $1+1$ et 2, il y a donc deux groupes d'ordre 4 (resp. 9) :

$$\mathbb{Z}/4, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \qquad (resp. \mathbb{Z}/9, \quad \mathbb{Z}/3 \times \mathbb{Z}/3)$$

il y a donc 4 groupes abéliens d'ordre 36 :
- $\mathbb{Z}/4 \times \mathbb{Z}/9 = \mathbb{Z}/36$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9 = \mathbb{Z}/2 \times \mathbb{Z}/18$
- $\mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/3 \times \mathbb{Z}/12$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/6 \times \mathbb{Z}/6$

2. On a $72 = 8.9 = 2^3.9^2$, par le théorème des restes chinois, un groupe d'ordre 72 est produit d'un groupe d'ordre 8 par un groupe d'ordre 9, les partitions de 3 sont $1+1+1, 1+2, 3$, et les partitions de 2 sont $1+1$ et 2, il y a donc 3 groupes abéliens d'ordre 8 (ceux de l'exercice 1) et deux groupes abéliens d'ordre 9 (ceux de la question précédente). On a donc 6 groupes abéliens d'ordre 72
- $\mathbb{Z}/8 \times \mathbb{Z}/9 = \mathbb{Z}/72$
- $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/9 = \mathbb{Z}/2 \times \mathbb{Z}/36$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9 = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/18$
- $\mathbb{Z}/8 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/3 \times \mathbb{Z}/24$
- $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/6 \times \mathbb{Z}/12$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 = \mathbb{Z}/2 \times \mathbb{Z}/6 \times \mathbb{Z}/6$

3. On a $180 = 4.5.9 = 2^2.5.2^2$, par le théorème des restes chinois, un groupe d'ordre 180 est produit d'un groupe d'ordre 4, d'un groupe d'ordre 5 et d'un groupe d'ordre 9. Les partitions de 2 sont $1+1$ et 2, et 1 est l'unique partition de 1. Il y a donc deux groupes abéliens, d'ordre 4 et deux groupes abéliens d'ordre 9, et un groupe abélien d'ordre 5, d'où au final 4 groupes d'ordre 180 :

- $\mathbb{Z}/4 \times \mathbb{Z}/9 \times \mathbb{Z}/5 = \mathbb{Z}/180$
- $\mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/5 = \mathbb{Z}/3 \times \mathbb{Z}/60$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9 \times \mathbb{Z}/5 = \mathbb{Z}/2 \times \mathbb{Z}/90$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/5 = \mathbb{Z}/6 \times \mathbb{Z}/30$

Exercice 3. Utilisons le théorème des restes chinois pour décomposer M en produit de $\mathbb{Z}/p^n\mathbb{Z}$ avec p premier :

$$\begin{aligned} M &= \mathbb{Z}/5 \times \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/9 \times \mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/9 \times \mathbb{Z}/4 \\ &= \mathbb{Z}/2 \times (\mathbb{Z}/4)^3 \times \mathbb{Z}/3 \times (\mathbb{Z}/9)^2 \times \mathbb{Z}/5 \end{aligned}$$

c'est la décomposition en modules indécomposables.
Pour déterminer les facteurs invariants, essayons de faire le plus grand module possible avec les restes chinois : c'est $\mathbb{Z}/4 \times \mathbb{Z}/9 \times \mathbb{Z}/5 = \mathbb{Z}/180$, on a donc

$$M = \mathbb{Z}/2 \times (\mathbb{Z}/4)^2 \times \mathbb{Z}/3 \times \mathbb{Z}/9 \times \mathbb{Z}/180$$

et on recommence la procédure sur les facteurs restants, :

$$\begin{aligned} M &= \mathbb{Z}/2 \times (\mathbb{Z}/4)^2 \times \mathbb{Z}/3 \times \mathbb{Z}/9 \times \mathbb{Z}/180 \\ &= (\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/3) \times (\mathbb{Z}/4 \times \mathbb{Z}/9) \times \mathbb{Z}/180 \\ &= \mathbb{Z}/2 \times (\mathbb{Z}/4 \times \mathbb{Z}/3) \times \mathbb{Z}/36 \times \mathbb{Z}/180 \\ &= \mathbb{Z}/2 \times \mathbb{Z}/12 \times \mathbb{Z}/36 \times \mathbb{Z}/180 \end{aligned}$$

Et voila les facteurs invariants.

Exercice 4. Quelles sont les opérations auxquelles on a droit ?
- Ajouter un multiple entier d'une ligne à une autre ligne ($L_i \leftarrow L_i + kL_j$)
- Ajouter un multiple entier d'une colonne à une autre colonne ($C_i \leftarrow C_i + kC_j$)
- Échanger deux lignes ($L_i \leftrightarrow L_j$)
- Échanger deux colonnes ($C_i \leftrightarrow C_j$)
- Multiplier une colonne ou une ligne par -1

Toutes ces opérations correspondent à la multiplication, à gauche ou à droite, par des matrices de $\mathrm{GL}_n(\mathbb{Z})$.
- $L_i \leftarrow L_i + kL_j$ correspond à multiplier à gauche par la matrice $I_n + kE_{i,j}$ (une matrice identité, avec en plus un coefficient k en (i,j).
- $C_i \leftarrow C_i + kC_j$ correspond à multiplier à droite par la matrice $I_n + kE_{j,i}$ (une matrice identité, avec en plus un coefficient k en (j,i).
- $L_i \leftrightarrow L_j$ correspond à multiplier à gauche par une matrice de permutation : Des 1 sur la diagonale, sauf les indices i,j remplacés par des 0, et des 1 en (i,j) (j,i).
- $C_i \leftrightarrow C_j$ correspond à multiplier à droite par une matrice de permutation : Des 1 sur la diagonale, sauf les indices i,j remplacés par des 0, et des 1 en (i,j) (j,i).

Pour A :

$$\begin{pmatrix} 2 & 0 & -10 & 16 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & 12 & -8 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

$$C_3 \leftarrow C_3 + 5C_1 \ : \begin{pmatrix} 2 & 0 & 0 & 16 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & 12 & -8 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

$$C_4 \leftarrow C_4 - 8C_1 \ : \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & 12 & -8 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

$$L_2 \leftarrow L_2 + L_4 \ : \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 12 & -8 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

$$L_3 \leftarrow L_3 + 2L_4 \ : \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

$$L_2 \leftrightarrow L_4 \ : \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$C_2 \leftrightarrow C_4 \ : \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Toutes ces transformations correspondent à multiplier à droite par la matrice

$$Q = \begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & -8 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -8 & 5 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

et à multiplier à gauche par la matrice

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Autrement dit, on a $PAQ = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, les diviseurs élémentaires de A sont $(2, 4, 12)$.

Pour B (tableau à lire de gauche à droite, puis de haut en bas) :

$\begin{pmatrix}0 & 48 & 12 & -46\\ 0 & 12 & 0 & -10\\ 0 & 8 & 4 & -8\\ 0 & 0 & 0 & 2\end{pmatrix}$	$L_1 \leftarrow L_1 + 23L_4 \ : \begin{pmatrix}0 & 48 & 12 & 0\\ 0 & 12 & 0 & -10\\ 0 & 8 & 4 & -8\\ 0 & 0 & 0 & 2\end{pmatrix}$
$L_2 \leftarrow L_2 + 5L_4 \ : \begin{pmatrix}0 & 48 & 12 & 0\\ 0 & 12 & 0 & 0\\ 0 & 8 & 4 & -8\\ 0 & 0 & 0 & 2\end{pmatrix}$	$L_3 \leftarrow L_3 + 4L_4 \ : \begin{pmatrix}0 & 48 & 12 & 0\\ 0 & 12 & 0 & 0\\ 0 & 8 & 4 & 0\\ 0 & 0 & 0 & 2\end{pmatrix}$
$C_2 \leftarrow C_2 - 2C_3 \ : \begin{pmatrix}0 & 24 & 12 & 0\\ 0 & 12 & 0 & 0\\ 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 2\end{pmatrix}$	$L_1 \leftarrow L_1 - 2L_2 \ : \begin{pmatrix}0 & 0 & 12 & 0\\ 0 & 12 & 0 & 0\\ 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 2\end{pmatrix}$
$L_1 \leftarrow L_1 - 3L_3 \ : \begin{pmatrix}0 & 0 & 0 & 0\\ 0 & 12 & 0 & 0\\ 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 2\end{pmatrix}$	$L_1 \leftrightarrow L_4 \ : \begin{pmatrix}0 & 0 & 0 & 2\\ 0 & 12 & 0 & 0\\ 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$
$C_1 \leftrightarrow C_4 \ : \begin{pmatrix}2 & 0 & 0 & 0\\ 0 & 12 & 0 & 0\\ 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$	$L_2 \leftrightarrow L_3 \ : \begin{pmatrix}2 & 0 & 0 & 0\\ 0 & 0 & 4 & 0\\ 0 & 12 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$
$C_2 \leftrightarrow C_3 \ : \begin{pmatrix}2 & 0 & 0 & 0\\ 0 & 4 & 0 & 0\\ 0 & 0 & 12 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$	

Moralité : les matrices A et B sont équivalentes (quitte à changer les bases au départ et à l'arrivée, elles représentent la même application linéaire).

Exercice 5. Par les restes chinois, on a

$$\mathbb{Z}/pq \times \mathbb{Z}/p2 = \mathbb{Z}/p \times \mathbb{Z}/q \times \mathbb{Z}/p^2 = \mathbb{Z}/p \times \mathbb{Z}/p^2 q$$

les facteurs invariants de ce $\mathbb{Z}$-module sont donc p, p^2q, qui sont différents de p^3q, le seul facteur invariant de $\mathbb{Z}/p^3q$

Exercice 6.
1. Premièrement μ_∞ est non vide car il contient 1. Ensuite, pour $z \in \mu_\infty$ tel que $\mu^n = 1$. On a $(\mu^{-1})^n) = (\mu^n)^{-1} = 1^{-1} = 1$ donc $z^{-1} \in \mu_\infty$. Enfin, soient $z, z' \in \mu_\infty$ et n, n' tels que $z^n = 1 = z'^{n'}$, on a $(zz')^{nn'} = z^{nn'} z'^{nn'} = 1$ car z, z' commutent ($\mathbb{C}^*$ est commutatif).
2. On rappelle que $\mathbb{S}^1 = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$. Soit $z = e^{i\theta} \in \mathbb{S}^1$, si $z \in \mu_\infty$ et $z^n = 1$, on a $e^{in\theta} = 1$. On sait que

$$e^{in\theta} = 1 \Leftrightarrow n\theta \equiv 0[2\pi] \Leftrightarrow \exists k \in \mathbb{Z} \mid n\theta = 2k\pi \Leftrightarrow \exists k \in \mathbb{Z} \mid \theta = \frac{2k}{n}\pi \Leftrightarrow \theta \in \mathbb{Q}\pi$$

Il suffit donc de prendre un θ qui ne soit pas un multiple rationnel de π, par exemple $e^{i\sqrt{2}\pi}$ n'est pas dans μ_∞.
3.a) Par définition de μ_∞, tous ses éléments sont d'ordre fini. Or si μ_∞ admet une partie libre, il admet un sous-groupe libre, en particulier dont les éléments sont d'ordre infinis (c'est toujours vrai pour un groupe libre, ou pour un module libre).
b). Si μ_∞ est de type fini et sans partie libre, alors le théorème de classification indique que μ_∞ est un produit de groupes cycliques, en particulier finis : μ_∞ serait un groupe fini.
c). Il est clair que μ_∞ n'est pas un groupe fini ! Il contient tous les $e^{\frac{2i\pi}{n}}$ pour $n \in \mathbb{N}$.

Exercice 7.
1. C'est un fait général : les inversibles d'un anneau commutatif unitaire forment un groupe abélien. Le produit est une loi associative et commutative avec un élément neutre (par définition d'un anneau commutatif unitaire), donc $\mathbb{Z}/n$ muni de la multiplication forme un monoïde, et les éléments inversibles d'un monoïde forment toujours un groupe !

2. Il faut déjà commencer par déterminer l'ordre de ces groupes, il est connu que $|(\mathbb{Z}/n)^\times|$ est le nombre d'entiers de $[\![1, n-1]\!]$ qui sont premiers avec n, donc

- $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$
- $(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$
- $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$
- $(\mathbb{Z}/16\mathbb{Z})^\times = \{1, 3, 5, 7, 9, 11, 13, 15\}$

Donc $(\mathbb{Z}/9\mathbb{Z})^\times$ est d'ordre 6, il n'y a qu'un seul groupe abélien d'ordre 6 : $\mathbb{Z}/6\mathbb{Z}$.
$(\mathbb{Z}/5\mathbb{Z})^\times$ est d'ordre 4, il y a donc deux possibilités, mais on a que 2 est d'ordre 4 dans $(\mathbb{Z}/5\mathbb{Z})^\times$, donc ce groupe est $\mathbb{Z}/4$ (en fait, le groupe des inversible d'un corps fini est toujours fini !)
$(\mathbb{Z}/8\mathbb{Z})^\times$ est lui aussi d'ordre 4, c'est $\mathbb{Z}/2 \times \mathbb{Z}/2$ car il ne contient que des éléments d'ordre 2 ($3^2 = 9 \equiv 1[8]$, $7^2 = 49 \equiv 1[8]$,...)
Enfin, $(\mathbb{Z}/16\mathbb{Z})^\times$ est d'ordre 8, ce qui laisse trois possibilités (celles de l'exercice 1), en calculant directement, on voit que $\{1, 7, 9, 15\}$ sont d'ordre 2, et que $\{3, 5, 11, 13\}$ sont d'ordre 4, il n'y a pas d'éléments d'ordre 8, donc ce n'est pas $\mathbb{Z}/8$, et il y a des éléments d'ordre 4, donc ce n'est pas $(\mathbb{Z}/2)^3$ (qui ne contient que des éléments d'ordre 2), cela nous laisse donc seulement $(\mathbb{Z}/16)^\times \simeq \mathbb{Z}/2 \times \mathbb{Z}/4$.

† *Facteurs indécomposables*

Exercice 8. Pour G_1, on considère la matrice $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, que l'on va chercher à écrire sous la forme $\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ avec $d_1|d_2$, en faisant des opérations ligne/colonne.

$$\begin{aligned}
& \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \\
L_1 \leftarrow L_1 + L_2 \ &: \begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix} \\
C_2 \leftarrow C_2 - C_1 \ &: \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \\
C_1 \leftarrow C_1 - C_2 \ &: \begin{pmatrix} 1 & 1 \\ -3 & 3 \end{pmatrix} \\
L_2 \leftarrow L_2 + 3L_1 \ &: \begin{pmatrix} 1 & 1 \\ 0 & 6 \end{pmatrix} \\
C_2 \leftarrow C_2 - C_1 \ &: \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}
\end{aligned}$$

Autrement dit

$$\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

On a donc

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$$

Et $\binom{4}{-3}, \binom{-1}{1}$ est une base de $\mathbb{Z}^2$, adaptée à G_1 car $\binom{4}{-3}, \binom{-6}{6}$ est une base de G_1. Le quotient $\mathbb{Z}^2/G_1$ est alors donné par $\mathbb{Z}/6\mathbb{Z}$ (c'est donné par les facteurs invariants).
Pour G_2, on considère la matrice $M = \begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix}$, que l'on va chercher à écrire sous la forme $\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ avec $d_1 | d_2$, en faisant des opérations ligne/colonne.

$$\begin{aligned}
& \begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix} \\
L_1 \leftarrow L_1 - L_2 \ : & \begin{pmatrix} 2 & -1 \\ 0 & 4 \end{pmatrix} \\
C_1 \leftarrow C_1 + C_2 \ : & \begin{pmatrix} 1 & -1 \\ 4 & 4 \end{pmatrix} \\
C_2 \leftarrow C_2 + C_1 \ : & \begin{pmatrix} 1 & 0 \\ 4 & 8 \end{pmatrix} \\
L_2 \leftarrow L_2 - 4L_1 \ : & \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}
\end{aligned}$$

Autrement dit

$$\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -4 & 5 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}$$

On a donc

$$\begin{pmatrix} 2 & 3 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$$

Et $\binom{5}{4}, \binom{1}{1}$ est une base de $\mathbb{Z}^2$, adaptée à G_2 car $\binom{5}{4}, \binom{8}{8}$ est une base de G_2. Le quotient $\mathbb{Z}^2/G_2$ est alors donné par $\mathbb{Z}/8\mathbb{Z}$ (c'est donné par les facteurs invariants).

Exercice 9. C'est un peu technique, notons $G = x\mathbb{Z}$ le sous-module de $\mathbb{Z}^4$ engendré par x, on cherche à calculer une base adaptée à ce sous-module, on trouve donc les facteurs invariants de la matrice

$$\begin{pmatrix} 10 \\ 6 \\ 7 \\ 11 \end{pmatrix}$$

:

$$\begin{pmatrix} 10 \\ 6 \\ 7 \\ 11 \end{pmatrix}$$

$$L_3 \leftarrow L_3 - L_2 \ : \begin{pmatrix} 10 \\ 6 \\ 1 \\ 11 \end{pmatrix}$$

$$L_1 \leftarrow L_1 - 9L_3 \ : \begin{pmatrix} 1 \\ 6 \\ 1 \\ 11 \end{pmatrix}$$

$$L_2 \leftarrow L_2 - 6L_1 \ : \begin{pmatrix} 1 \\ 0 \\ 1 \\ 11 \end{pmatrix}$$

$$L_3 \leftarrow L_3 - L_1 \ : \begin{pmatrix} 1 \\ 0 \\ 0 \\ 11 \end{pmatrix}$$

$$L_4 \leftarrow L_4 - 11L_1 \ : \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

On obtient donc

$$\begin{pmatrix} 10 & 0 & 9 & 0 \\ 6 & 1 & 0 & 0 \\ 7 & 1 & 1 & 0 \\ 11 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = x$$

les colonnes de cette matrice donnent la base de $\mathbb{Z}^4$ voulue.

† *Invariants de similitude et décomposition de Frobenius*

Exercice 10.
1.a) C'est évident, on rappelle que $M.e_i$ est toujours la i-ème colonne de la matrice M, pour $i \in [\![1, n-1]\!]$, cette colonne est le vecteur de base canonique e_{i+1}. On constate d'ailleurs que

$$M.e_n = \begin{pmatrix} -a_0 \\ -a_1 \\ \vdots \\ -a_{n-1} \end{pmatrix} = -\sum_{i=1}^{n} a_{i-1} e_i$$

b). Soit $Q = \sum_{i=0}^{n-1} b_i X^i = \sum_{i=1}^{n} b_{i-1} X^{i-1}$ un polynôme de degré $\leqslant n-1$. Si $Q(M) = 0$, on a en particulier $Q(M).e_1 = 0$. Par ailleurs, on calcule

$$Q(M).e_1 = \sum_{i=1}^{n} b_{i-1} M^{i-1}.e_1 = \sum_{i=1}^{n} b_{i-1} e_i$$

Il s'agit là d'une combinaison linéaire sur la base $(e_i)_{i\in[\![1,n]\!]}$, si elle est nulle, c'est que tous ses coefficients (les b_i) sont nuls, autrement dit $Q = 0$.
c). On a

$$P(M).e_1 = M^n.e_1 + \sum_{i=0}^{n-1} a_i M^i.e_1 = M.e_n + \sum_{i=0}^{n-1} a_i e_{i+1} = -\sum_{i=1}^{n} a_{i-1}e_i + \sum_{i=1}^{n} a_{i-1}e_i = 0$$

d). Premièrement, montrons que P est annulateur de M. Il faut montrer que $P(M).e_i = 0$ pour $i \in [\![1,n]\!]$. On l'a déjà montré pour $i = 1$, pour $i \geqslant 2$, on a

$$P(M).e_i = P(M)M^{i-1}.e_1 = M^{i-1}P(M).e_1 = M^{i-1}.0 = 0$$

car les polynômes en M commutent les uns avec les autres (puisque les puissances d'une matrice fixée commutent entre elles). On sait maintenant que P est annulateur, et la question b) nous apprend que P a un degré minimal avec cette propriété : P est bien le polynôme minimal de M. 2. Le polynôme caractéristique de M doit être de degré n et divisé par le polynôme minimal, comme le polynôme minimal de M est lui aussi de degré n (et unitaire...), les polynômes minimaux et caractéristique de M sont égaux.

Exercice 11.
1. La décomposition de Frobenius de M dans k est donnée par une matrice $P \in \mathrm{GL}_n(k)$ telle que PMP^{-1} soit de la forme

$$\begin{pmatrix} \mathcal{C}(P_1) & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}(P_r) \end{pmatrix}$$

où $P_r|P_{r-1}|...|P_1$. On a de plus que P_1 est le polynôme minimal de M sur k, et le produit des P_i est le polynôme caractéristique de M sur k.
En voyant les P_i et P comme à coefficients dans K, on constate que la réduite de Frobenius de M sur k est candidate pour être "une réduite de Frobenius" de M sur K, on conclut par unicité de la réduction de Frobenius.
Les polynômes caractéristiques et minimaux sont calculable à partir de la seule donnée de la réduite de Frobenius.
La réduite de Frobenius caractérise la classe de similitude : deux matrices sont semblables si et seulement si elles ont même réduite de Frobenius.

Exercice 12. Soit $P = \sum_{i=0}^{m} a_i X^i$, on a

$$P(M)(x) = \sum_{i=0}^{m} a_i M^i.x = \sum_{i=0}^{m} a_i \lambda^i x = P(\lambda)x$$

Si μ est le polynôme minimal de M, on a $0 = \mu(M)(x) = \mu(\lambda)x$, comme x est non nul, cela entraîne $\mu(\lambda) = 0$.

Exercice 13.
1. On commence par exprimer les facteurs irréductibles de X^4, ceux-ci ne dépendent en l'occurrence pas du corps choisi, et sont évidemment X, X, X, X. Le polynôme minimal de u contient au moins une copie de chaque facteur irréductible, autrement dit c'est X, X^2, X^3 ou bien X^4.

1. Si $\mu_u = X^4$, alors $\mu_u = \chi_u$, u est cyclique et on a

$$u \sim \mathcal{C}(X^4) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

2. Si $\mu_u = X^3 = P_1$, alors $P_2 = X$, et

$$u \sim \begin{pmatrix} \mathcal{C}(X^3) & 0 \\ 0 & \mathcal{C}(X) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

3. Si $\mu_u = X^2$, alors soit $P_2 = X$ et $P_1 = X$, ou alors $P_2 = X^2$, on a alors respectivement

$$u \sim \begin{pmatrix} \mathcal{C}(X^2) & 0 & 0 \\ 0 & \mathcal{C}(X) & 0 \\ 0 & 0 & \mathcal{C}(X) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$u \sim \begin{pmatrix} \mathcal{C}(X^2) & 0 \\ 0 & \mathcal{C}(X^2) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

4. Si $\mu_u = X$, alors $P_2 = X$ car il doit diviser $P_1 = X$, on a $P_3 = P_4 = X$ pour la même raison et on obtient

$$u \sim \begin{pmatrix} \mathcal{C}(X) & 0 & 0 & 0 \\ 0 & \mathcal{C}(X) & 0 & 0 \\ 0 & 0 & \mathcal{C}(X) & 0 \\ 0 & 0 & 0 & \mathcal{C}(X) \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Autre façon peut-être plus rapide : Les invariants de similitude possible sont paramétrés par les partitions de 4 (la puissance de X donnant χ_u). Les partitions de 4 sont

$$4 \qquad 3+1 \qquad 2+2 \qquad 2+1+1 \qquad 1+1+1+1$$

Ces partitions donnent respectivement les invariants

$$(X^4) \qquad (X^3, X^1) \qquad (X^2, X^2) \qquad (X^2, X^1, X^1) \qquad (X^1, X^1, X^1, X^1)$$

Qui sont bien tous les invariants listés plus haut.

2. Ici, c'est un peu différent car la décomposition en facteurs irréductibles de χ_u dépend du corps k choisi. Sur $\mathbb{Q}$ et $\mathbb{R}$, X^2+X+1 est irréductible, donc l'unique facteur irréductible de χ_u est X^2+X+1. Les décompositions possibles sont alors paramétrées par les partitions de 2.

- La partition (2) donne le cas d'un endomorphisme cyclique (avec $\mu_u = \chi_u = (X^2+X+1) = X^4+2X^3+3X^2+2X+1$).

$$u \sim \mathcal{C}(\chi_u) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & -3 \\ 0 & 0 & 1 & -2 \end{pmatrix}$$

- La partition $(1,1)$ donne les invariants $P_1 = X^2+X+1 = P_2$, on a alors

$$u \simeq \begin{pmatrix} \mathcal{C}(X^2+X+1) & 0 \\ 0 & \mathcal{C}(X^2+X+1) \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Sur $\mathbb{C}$, c'est différent : on a $X^2+X+1 = (X-j)(X-j^2)$ où $j = e^{\frac{2i\pi}{3}}$. Les facteurs irréductibles de χ_u sont donc $X-j$ et $X-j^2$. Comme dans le cas des nombres premiers, les suites d'invariants possibles sont paramétrées par les couples de partitions de 2 (une partition pour les facteurs $X-j$, l'autre pour $X-j^2$).

- Le couple $((2),(2))$ donne la suite $((X-j)^2(X-j^2)^2) = ((X^2+X+1)^2)$ que nous avons déjà traité (ça reste une possibilité sur $\mathbb{C}$, mais c'était déjà une possibilité sur $\mathbb{Q}$).
- Le couple $((2),(1+1))$ donne la suite $((X-j)^2(X-j^2),(X-j^2)) = ((X^2+X+1)(X-j),(X-j^2))$

$$u \sim \begin{pmatrix} \mathcal{C}((X^2+X+1)(X-j)) & 0 \\ 0 & \mathcal{C}(X-j^2) \end{pmatrix} = \begin{pmatrix} 0 & 0 & j & 0 \\ 1 & 0 & j-1 & 0 \\ 0 & 1 & j-1 & 0 \\ 0 & 0 & 0 & j^2 \end{pmatrix}$$

- Le couple $((1+1),(2))$ donne la suite $((X-j)(X-j^2)^2,(X-j)) = ((X^2+X+1)(X-j^2),(X-j))$

$$u \sim \begin{pmatrix} \mathcal{C}((X^2+X+1)(X-j)) & 0 \\ 0 & \mathcal{C}(X-j^2) \end{pmatrix} = \begin{pmatrix} 0 & 0 & j^2 & 0 \\ 1 & 0 & j^2-1 & 0 \\ 0 & 1 & j^2-1 & 0 \\ 0 & 0 & 0 & j \end{pmatrix}$$

- Le couple $((1+1),(1+1))$ donne la suite $((X^2+X+1),(X^2+X+1))$ que nous avons aussi déjà rencontré précédemment.

3. Sur $\mathbb{C}$, le polynôme caractéristique de M est donné par $(X-j)(X-j^2)(X-\sqrt{2})(X+\sqrt{2})$, il s'agit d'un polynôme scindé à racines simples, donc égal au polynôme minimal de M. Autrement dit sur tous les corps donnés, les polynômes caractéristiques et minimaux de M sont égaux, le seul polynôme apparaissant dans les invariants de similitude de M est donc $(X^2+X+1)(X^2-2) = X^4+X^3-X^2-2X-2$, la réduite de Frobenius de M est donc

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