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. Par les restes chinois, on a

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

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 5.
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, invariants de similitudes*

Exercice 6. 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 7. 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.

Exercice 8.

1. Les invariants de similitude de M sur $\mathbb{k}$ sont une suite de polynômes $P_1, \cdots, P_s$ telle que $P_1|P_2 \cdots |P_s$, et il existe $P \in \mathrm{Gl}_n(\mathbb{k})$ tel que

$$PMP^{-1} = \begin{pmatrix} \mathcal{C}_{P_1} & & \\ & \ddots & \\ & & \mathcal{C}_{P_s} \end{pmatrix}$$

(où $\mathcal{C}_{P_i}$ est la matrice compagnon de P_i). Les P_i sont aussi des polynômes de K, et on a aussi $P \in Gl_n(K)$, donc par unicité des invariants de similitude, les P_i forment aussi les invariants de similitude de M sur K.

2. Avec les notations de la question précédente, on a que P_1 est le polynôme minimal de M, et on a vu que ce polynôme ne dépend pas du corps choisi.

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

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