TD 4 - Modules sur un anneau principal

† *Bases adaptées et forme normale de Smith*

Exercice 1. Trouver les diviseurs élémentaires des matrices entières

$$A = \begin{pmatrix} 2 & 0 & -10 & 16 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & 12 & -8 \\ 0 & 0 & 0 & 4 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0 & 48 & 12 & -46 \\ 0 & 12 & 0 & -10 \\ 0 & 8 & 4 & -8 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

Exercice 2.

1. Trouver une base adaptée pour le sous-module N de $\mathbb{Z}^4$ déterminé par les équations

$$\begin{cases} x + 2y + 2z + t = 0 \\ 2x + y + z + 2t = 0 \end{cases}$$

2. On considère les applications linéaires $f : \mathbb{Z}^3 \to \mathbb{Z}$ et $g : \mathbb{Z}^2 \to \mathbb{Z}^3$ données respectivement par les matrices

$$f = \begin{pmatrix} 2 & 2 & 2 \end{pmatrix}, \ g = \begin{pmatrix} -2 & 0 \\ 0 & -2 \\ 2 & 2 \end{pmatrix}$$

   a) Montrer que $f \circ g = 0$, en déduire que $\operatorname{Im} g \subset \operatorname{Ker} f$.
   b) Déterminer une base adaptée de $\operatorname{Im} f$ dans $\mathbb{Z}$. En déduire le quotient $\mathbb{Z}/\operatorname{Im} f$.
   c) Déterminer une base adaptée de $\operatorname{Im} g$ dans $\operatorname{Ker} f$. En déduire le quotient $\operatorname{Ker} f/\operatorname{Im} g$.

   (*Félicitations, vous venez de calculer l'homologie d'un groupe ! Rendez-vous en M2 pour comprendre ce que ça veut dire !*).

† *Groupes abéliens finis*

Exercice 3 (Théorème des restes chinois). Soient $m, n \in \mathbb{N}$ premiers entre eux. Pour $k \in \mathbb{Z}$, on note $k[n]$ la classe de k modulo n.

1. Quel est le noyau du morphisme naturel $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ envoyant k sur $(k[n], k[m])$?
2. Si n et m sont premiers entre eux, en déduire l'existence d'un unique morphisme injectif $\overline{f} : \mathbb{Z}/(nm)\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ envoyant $k[nm]$ sur $(k[n], k[m])$.
3. Montrer que $\overline{f}$ est un isomorphisme.
4. En général, montrer que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/\mathrm{pgcd}(m,n)\mathbb{Z} \times \mathbb{Z}/\mathrm{ppcm}(m,n)\mathbb{Z}$.

Exercice 4. Déterminer tous les groupes abéliens d'ordre 36, puis tous ceux d'ordre 72 et 180.

Exercice 5. Donner les facteurs invariants ainsi que la décomposition en modules indécomposables du $\mathbb{Z}$-module

$$M = \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Exercice 6. Si p et q sont deux nombres premiers entre eux, les groupes $(\mathbb{Z}/pq\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})$ et $\mathbb{Z}/p^3q\mathbb{Z}$ peuvent ils être isomorphes ?

Exercice 7 (Unicité dans la décomposition en facteurs invariants). Soit G un groupe abélien de la forme

$$G = \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$$

avec $d_1|d_2|\cdots|d_n$.

1. Montrer que tout élément g de G est tel que $d_n.g = 0$. Montrer qu'il existe $g \in G$ tel que $k.g \neq 0$ pour $1 \leqslant k < d_n$.
2. Soit maintenant une autre décomposition $G \simeq \mathbb{Z}/\delta_1\mathbb{Z} \times \cdots \times \mathbb{Z}/\delta_m\mathbb{Z}$ avec $\delta_1|\delta_2|\cdots|\delta_m$. Montrer que $d_n = \delta_m$.
3. Montrer que la décomposition d'un groupe abélien en facteurs invariants est unique (*on pourra raisonner par récurrence sur le cardinal de* G).

Exercice 8. Soit $n \geqslant 1$, on appelle partition de n une suite croissante d'entiers positifs $\lambda = (\lambda_1, \ldots, \lambda_k)$ telle que $\lambda_1 + \cdots + \lambda_k = n$.

1. Montrer qu'il y a (à isomorphisme près) trois groupes abéliens d'ordre 8.
2. On fixe p un nombre premier. Soit λ une partition de n, on pose $G(\lambda) := Z/p^{\lambda_1}\mathbb{Z} \times \mathbb{Z}/p^{\lambda_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\lambda_k}\mathbb{Z}$.
   a) Montrer que $G(\lambda)$ est un groupe abélien de cardinal p^n.
   b) Montrer que, si $\lambda \neq \mu$, alors $G(\lambda)$ et $G(\mu)$ ne sont pas isomorphes.
   c) En déduire que le nombre de groupes abéliens (à isomorphisme près) de cardinal p^n est égal au nombre de partitions de n. (ATTENTION ! Jusqu'à nouvel ordre, ceci ne compte pas comme un résultat du cours).
3. Calculer toutes les partitions de l'entier 7.
4. En déduire les groupes abéliens (à isomorphisme près) d'ordre 128. Combien y en a-t-il ? (*À titre de comparaison, il y a 2298 groupes non abéliens d'ordre* 128).

Exercice 9. On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

1. Montrer qu'il s'agit d'un groupe abélien pour la multiplication.
2. Écrire comme produits de groupes cycliques les groupes

$$(\mathbb{Z}/9\mathbb{Z})^\times, \quad (\mathbb{Z}/5\mathbb{Z})^\times, \quad (\mathbb{Z}/8\mathbb{Z})^\times, \quad (\mathbb{Z}/16\mathbb{Z})^\times.$$

(*Indication : pour* $(\mathbb{Z}/16\mathbb{Z})^\times$, *on pourra calculer l'ordre des éléménts et appliquer l'exercice 8*)

† *Invariants de similitudes et décomposition de Frobenius*

Soit $M \in \mathcal{M}_n(k)$ une matrice. On rappelle que les invariants de similitude de M forment une suite de polynômes unitaires $(P_1(X), \ldots, P_k(X))$ telle que $P_k(X)$ est le polynôme minimal de M et telle que $\prod_{i=1}^n P_i(X)$ est le polynôme caractéristique de M (en particulier, la somme des degrés des P_i vaut n).

Exercice 10. Calculer les invariants de similitude de la matrice

$$M := \begin{pmatrix} 3 & 2 & -2 \\ -1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Exercice 11. On considère $k \subset K$ deux corps, et $M \in \mathcal{M}_n(k)$

1. Donner les invariants de similitude possibles pour un endomorphisme $u \in \mathcal{L}(k^4)$ dont le polynôme caractéristique est

$$\chi_u = X^4$$

dans les cas suivants : $k = \mathbb{Q}, k = \mathbb{R}, k = \mathbb{C}$.

2. Même question avec $\chi_u = (X^2+X+1)^2$.
3. Soit la matrice
$$\begin{pmatrix} 12 & 4 & 14 & 3 \\ -6 & -2 & -7 & -2 \\ -8 & -2 & -10 & -2 \\ 1 & 2 & 0 & -1 \end{pmatrix}$$
Déterminer les invariants de similitude de M pour $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2})$ (*indication : le polynôme caractéristique de M est $(X^2+X+1)(X^2-2)$, ne vous embêtez pas à le recalculer*).

Exercice 12. Considérons (pour $m \in \mathbb{R}$), la matrice
$$A_m := \begin{pmatrix} 2 & m-1 & -1 \\ 1-m & m & m-1 \\ 1 & m-1 & 0 \end{pmatrix}$$

1. Montrer que le polynôme caractéristique de A_m est $(X-m)(X-1)^2$.
2. Calculer $(A_m - m\,\mathrm{Id})(A_m - \mathrm{Id})$, en déduire la valeur du polynôme minimal de m suivant la valeur de m.
3. En déduire les invariants de similitude de A_m en fonction de m.

Soit $P \in k[X]$ un polynôme unitaire de degré n s'écrivant
$$P(X) := X^n + \sum_{i=0}^{n-1} a_i X^i$$
On définit $\mathcal{C}(P) \in \mathcal{M}_n(k)$ la ***matrice compagnon*** de P par
$$\mathcal{C}(P) := \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Exercice 13. Soit $P \in k[X]$ un polynôme unitaire comme ci-dessus. On pose $M := \mathcal{C}(P)$ la matrice compagnon de P.

1. a) Montrer que, pour $i \in [\![1, n-1]\!]$, on a $M.e_i = e_{i+1}$.
   b) Montrer que si Q est un polynôme de degré $\leqslant n-1$, alors $Q(M) \neq 0$.
   c) Montrer que $P(M).e_1 = 0$.
   d) En déduire que P est le polynôme minimal de M.
2. Montrer que le polynôme caractéristique de M est aussi égal à P.
3. En déduire la suite des invariants de similitude de P.

Exercice 14. Soient $k \subset K$ deux corps, et $M \in \mathcal{M}_n(k)$.

1. Montrer que la décomposition de Frobenius de M à coefficients dans k est également la décomposition de Frobenius de M à coefficients dans K.
2. En déduire que les polynômes caractéristiques et minimaux de M dans k sont les mêmes que dans K.
3. En déduire que deux matrices de $\mathcal{M}_n(k)$ sont semblables dans $\mathcal{M}_n(k)$ si et seulement si elles sont semblables dans $\mathcal{M}_n(K)$.