TD 12 : corrigé

2. Mise sous forme normale

1.
$$\begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1 & -1 \\ 2 & 5 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}$$

On aimerait utiliser le 2 en haut à gauche (élément de stathme minimal) pour, par des opérations élémentaires sur les lignes et les colonnes, éliminer les autres éléments des premières ligne et colone. Cependant, 2 ne divise pas les autres éléments de la matrice sur sa ligne (3) et sur sa colonne (5). On utilise alors la division euclidienne $3 = 2 \times 1 + 1$ et une opération sur les lignes ($L_2 \leftarrow L_2 - L_1$) pour obtenir un élément de stathme plus petit. Après réarrangement ($L_1 \longleftrightarrow L_2$), on obtient la deuxième matrice. Maintenant, l'élément en haut à gauche divise bel et bien les éléments sur sa ligne et sur sa colonne et on peut faire une opération de lignes ($L_2 \leftarrow L_2 - 2L_1$) puis une opération de colonnes ($C_2 \leftarrow C_2 + C_1$) pour obtenir la matrice finale. La matrice est donc équivalente (sur $\mathbb{Z}$) à $\mathrm{diag}(1,7)$.

2.
$$\begin{pmatrix} 3 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 3 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 2 \\ 3 & 2 & 1 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & -4 & -8 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 8 & 4 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

On commence par réarranger ($L_1 \longleftrightarrow L_3$) pour qu'un élément de stathme minimal (1) se retrouve en haut à gauche (deuxième matrice). Cet élément divise alors les autres sur ses ligne et colonne et on peut par des opérations sur les lignes d'abord ($L_2 \leftarrow L_2 - 2L_1$, $L_3 \leftarrow L_3 - 3L_1$) et les colonnes ensuite ($C_2 \leftarrow C_2 - 2C_1$, $C_3 \leftarrow C_3 - 3C_1$), éliminer ces éléments (troisième matrice). Il nous reste à effectuer les mêmes opérations sur la matrice 2×2 en bas à droite. Commençons par un peu de nettoyage ($L_2 \leftarrow -L_2$, $L_3 \leftarrow -L_3$, licite parce que -1 est inversible dans $\mathbb{Z}$, puis $C_2 \longleftrightarrow C_3$) pour obtenir la quatrième matrice. 4 divisant 0 et 8, il ne reste plus qu'à appliquer une opération ($L_3 \leftarrow L_3 - 2L_2$) pour obtenir la dernière matrice, qui est sous la forme voulue. La matrice est donc équivalente (sur $\mathbb{Z}$) à $\mathrm{diag}(1,4,4)$.

3.
$$\begin{pmatrix} X+4 & 2 \\ 2X-4 & X+1 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1 & X/2+2 \\ X+1 & 2X-4 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -X^2/2 - X/2 - 6 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & X^2+X+12 \end{pmatrix}$$

On place l'élément de stathme minimal en haut à gauche ($C_1 \longleftrightarrow C_2$) puis, tant qu'à faire, on le rend égal à 1 ($L_1 \leftarrow L_1/2$, licite parce que $1/2$ est inversible dans $\mathbb{Q}[X]$) pour obtenir la deuxième matrice. Il divise alors les éléments présents sur sa ligne et sur sa colonne, que l'on peut donc simplement éliminer ($L_2 \rightarrow L_2 - (X+1)L_1$, $C_2 \leftarrow C_2 - (X/2+2)C_1$) pour obtenir la matrice suivante. Puisque -2 est inversible dans $\mathbb{Q}[X]$, on peut effectuer une dernière simplification ($L_2 \leftarrow -2L_2$) afin d'obtenir le résultat. La matrice est équivalente (sur $\mathbb{Q}[X]$) à $\mathrm{diag}(1, X^2+X+12)$.

3. Quelques contre-exemples

1. – Si on note $(e_i)_{i=1}^n$ la base canonique du $\mathbb{Z}$-module $\mathbb{Z}^n$, la famille $(2e_i)_{i=1}^n$ est une famille libre (une relation de liaison $\sum a_i \cdot 2e_i = 0$ ($a_i \in \mathrm{A}$) définirait une relation de liaison entre les e_i, donc on aurait $2a_i = 0$ et enfin $a_i = 0$) qui n'est pas génératrice (toute combinaison linéaire de ces vecteurs a des coordonnées paires).

– La famille $(2,3)$ engendre le $\mathbb{Z}$-module libre $\mathbb{Z}$ (ne serait-ce que parce que l'image contient $1 = 3-2$) et est minimale pour cette propriété (ni 2 ni 3 n'engendrent seuls $\mathbb{Z}$). En revanche, ce n'est pas une base, parce que l'on a la relation de liaison $0 = 3\cdot 2 - 2\cdot 3$. (D'ailleurs, le module libre de rang un $\mathbb{Z}$ ne saurait avoir une base à deux vecteurs).

– Tout idéal de A est un sous-A-module du A-module libre A (et réciproquement, d'ailleurs). Supposons qu'un tel idéal I soit un A-module libre. On peut alors trouver une base $(m_i)_{i\in \mathrm{I}}$ du A-module I. Si I avait au moins deux éléments a et b, les vecteurs de base m_a et m_b seraient liés par la relation $m_b m_a - m_a m_b = 0$, qui est bien une relation de liaison sur A, ce qui est absurde. On a donc $|\mathrm{I}| = 0$ ou 1. Dans ce premier cas, I est l'idéal nul, et dans le second, si on note m le seul élément de la base, on a bien $\mathrm{I} = m\mathrm{A} = (m)$. En tout cas, I est principal.

Ainsi, tout idéal non principal de A fournit un sous-module non libre du A-module (libre) A. Il en va ainsi par exemple de $(2,\mathrm{X})$ dans $\mathbb{Z}[\mathrm{X}]$.

2. Il est important de remarquer que « $\mathbb{Z}$-module » et « groupe abélien » sont des expressions parfaitement synonymes l'une de l'autre. Notamment, si M est un groupe abélien (ou un $\mathbb{Z}$-module, puisque c'est pareil), une partie de M est un sous-groupe si et seulement si c'est un sous-$\mathbb{Z}$-module. Ainsi, un sous-$\mathbb{Z}$-module de $\mathrm{G} = \mathbb{Z}/4\mathbb{Z}$ isomorphe à $\mathbb{Z}/2\mathbb{Z}$ n'est rien d'autre qu'un sous-groupe de cardinal 2, et on voit aisément que $\mathrm{H} = \{0 \bmod 4, 2 \bmod 4\}$ est le seul possible. Un supplémentaire S fournirait un isomorphisme $\mathbb{Z}/4\mathbb{Z} \simeq \mathrm{H}\times\mathrm{S}$ et serait donc un sous-groupe de cardinal 2, ce qui entraîne $\mathrm{S} = \mathrm{H}$, contredisant la définition. Ainsi, ce sous-$\mathbb{Z}$-module n'admet pas de supplémentaire.

6. Isomorphisme de $\mathrm{K}[\mathrm{X}]$-modules

Nous allons donc utiliser la définition de l'annulateur d'un A-module M :

$$\mathrm{Ann}(\mathrm{M}) = \left\{ a \in \mathrm{A} \,\middle|\, \forall m \in \mathrm{M}, am = 0 \right\}.$$

Déjà, remarquons que si M et M′ sont des A-modules isomorphes (appelons $\varphi : \mathrm{M} \to \mathrm{M}'$ un isomorphisme), leurs annulateurs sont égaux :

$$\forall x \in \mathrm{M}, ax = 0 \Leftrightarrow \forall x \in \mathrm{M}, \varphi(ax) = 0 \Leftrightarrow \forall x \in \mathrm{M}, a\varphi(x) = 0 \Leftrightarrow \forall y \in \mathrm{M}', ay = 0.$$

Ensuite, montrons que si I est un idéal dans un anneau A, l'annulateur du A-module A/I est $\mathrm{Ann}(\mathrm{A}/\mathrm{I}) = \mathrm{I}$. Tout d'abord, si $a \in \mathrm{I}$ et $[x]_\mathrm{I} \in \mathrm{A}/\mathrm{I}$, $a[x]_\mathrm{I} = [ax]_\mathrm{I} = 0$ car $ax \in \mathrm{I}$. Réciproquement, si $a \in \mathrm{Ann}(\mathrm{A}/\mathrm{I})$, on a $0 = a[1]_\mathrm{I} = [a]_\mathrm{I}$ et $a \in \mathrm{I}$.

Ainsi, si les K[X]-modules $\mathrm{K}[\mathrm{X}]/(\mathrm{P})$ et $\mathrm{K}[\mathrm{X}]/(\mathrm{Q})$ sont isomorphes, leurs annulateurs (P) et (Q) sont égaux et, comme P et Q sont unitaires, on a $\mathrm{P} = \mathrm{Q}$.

En revanche, ni l'isomorphisme en tant qu'anneaux ni celui en tant que K-espace vectoriel n'impliquent l'égalité des polynômes. Par exemple, si $\alpha \in \mathrm{K}$, le morphisme (de K-algèbres, c'est-à-dire d'anneaux et de K-espaces vectoriels) surjectif $\text{év}_\alpha : \mathrm{K}[\mathrm{X}] \to \mathrm{K}$ défini par $\text{év}_\alpha(\mathrm{P}) = \mathrm{P}(\alpha)$ a pour noyau les polynômes s'annulant en α, c'est-à-dire l'idéal principal $(\mathrm{X}-\alpha)$. Il definit donc, d'après le théorème de factorisation, un isomorphisme $\overline{\text{év}_\alpha} : \mathrm{K}[\mathrm{X}]/(\mathrm{X}-\alpha) \to \mathrm{K}$. Ainsi, deux choix différents de α fournissent deux quotients qui sont des anneaux et des K-espaces vectoriels isomorphes.

7. Corps et modules libres

L'annulateur d'un module libre (non nul) est réduit à l'idéal nul. En effet, si $(e_i)_{i\in \mathrm{I}}$ est une base d'un A-module M, on a pour un $i_0 \in \mathrm{I}$: $a \in \mathrm{Ann(M)} \Rightarrow a e_{i_0} = 0$. Mais cette dernière relation est une relation de liaison sur A donc elle implique $a = 0$.

Supposons alors que tous les A-modules sont libres. Soit I un idéal de A. On a vu dans l'exercice précédent que I était l'annulateur de A/I. La propriété entraîne donc que tout idéal de A est trivial ce qui entraîne d'après un TD précédent que A est un corps.

11. Groupes abéliens finis

Le cours offre deux formes canoniques sous lesquelles peuvent s'exprimer un groupe abélien fini :

- La *décomposition en facteurs invariants* $\mathrm{G} = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_s\mathbb{Z}$, où les d_i sont des entiers non nuls vérifiant $d_i | d_{i+1}$;
- La *décomposition en diviseurs élémentaires* $\mathrm{G} = \displaystyle\bigoplus_{p \text{ premier}} \left(\bigoplus_{i=1}^{r^{(p)}} \mathbb{Z}/p^{\alpha_i^{(p)}}\mathbb{Z} \right)$ qui décompose les parties relevant des différents p premiers.

Pour mettre sous ces formes un groupe abélien fini déjà donné sous forme de produits de groupes cycliques, on utilise le théorème chinois. On obtient ainsi :

- $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}) \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/60\mathbb{Z}$;
- $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}) \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$;
- $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^2 \oplus (\mathbb{Z}/3\mathbb{Z})^2 \oplus (\mathbb{Z}/5\mathbb{Z})^2 \simeq \mathbb{Z}/30\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$.