TD10 : Modules de type fini sur un anneau principal

Diego Izquierdo

L'exercice 0 et les deux premières questions de l'exercice 2 sont à préparer avant la séance. Nous traiterons les exercices dans l'ordre suivant : 0, questions 1 et 2 de l'exercice 2, 5, 14.

Exercice 0 (à préparer) : TD8 et TD9
Faire la question 3 de l'exercice 6 du TD8 et l'exercice 3 du TD9.

Exercice 1 : Facteurs invariants
Trouver les facteurs invariants du $\mathbb{Z}$-module :

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}.$$

Exercice 2 (questions 1 et 2 à préparer) : Examen 2012

1. Soient $n \geq 1$ un entier et u_1, ..., u_n des éléments de $\mathbb{Z}^n$ linéairement indépendants dans l'espace vectoriel $\mathbb{Q}^n$. Soit M le sous-groupe de $\mathbb{Z}^n$ engendré par $u_1, ..., u_n$. Montrer que l'indice de M dans $\mathbb{Z}^n$ est égal à la valeur absolue du déterminant des vecteurs $u_1, ..., u_n$ dans la base canonique.
2. Soit M sous-groupe de $\mathbb{Z}^3$ engendré par $u_1 = (2, 1, 1)$, $u_2 = (1, 2, 1)$ et $u_3 = (1, 1, 2)$. Calculer $\mathbb{Z}^3/M$.
3. Plus généralement, soit $(u_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$ la matrice telle que $u_{i,j} = 2$ si $i = j$ et $u_{i,j} = 1$ sinon, et notons u_1, ..., u_n les vecteurs colonne de cette matrice. Soit M le sous-groupe de $\mathbb{Z}^n$ engendré par $u_1, ..., u_n$. Calculer $\mathbb{Z}^n/M$.

Exercice 3 : Bases adaptées

1. Donner une base adaptée pour le sous-$\mathbb{Z}$-module M de $\mathbb{Z}^4$ engendré par $(2, -1, 0, 0)$, $(-1, 2, -1, -1)$, $(0, -1, 2, 0)$ et $(0, -1, 0, 2)$. Calculer le quotient $\mathbb{Z}^4/M$.
2. Même question pour le sous-$\mathbb{Z}$-module M de $\mathbb{Z}^3$ engendré par $(4, 8, 16)$, $(1, 5, 10)$, $(6, 2, 4)$ et $(5, 8, 6)$.
3. Même question pour le sous-module de $\mathbb{Z}^3$ défini par $5x+7y+35z = 0$.
4. Même question pour le sous-module de $\mathbb{Z}^3$ défini par $x + 2y + 3z \equiv 0 \mod 4$.
5. Même question pour le sous-$\mathbb{C}[[X]]$-module de $\mathbb{C}[[X]]^2$ engendré par $((1 - X)^{-1}, (1 - X^2)^{-1})$ et $((1 + X)^{-1}, (1 + X^2)^{-1})$.

6. Exhiber deux sous-$\mathbb{Z}$-modules M et N de $\mathbb{Z}^2$ de rang 2 tels qu'il n'existe pas une base (e_1, e_2) de $\mathbb{Z}^2$ pour laquelle on peut trouver des entiers a, b, c, d tels que (ae_1, be_2) est une base de M et (ce_1, de_2) est une base de N.

Exercice 4 : $\mathbb{Z}[i]$-modules finis

1. Combien existe-t'il de $\mathbb{Z}[i]$-modules de cardinal 3 à isomorphisme près ? de cardinal 5 ? de cardinal 9 ?
2. *(plus difficile)* Combien existe-t'il de $\mathbb{Z}[i]$-modules de cardinal $5^3 \cdot 6^4$ à isomorphisme près ?

Exercice 5 : Retour sur le théorème des deux carrés

Soit p un nombre premier congru à 1 modulo 4. Montrer qu'il est possible de munir $\mathbb{Z}/p\mathbb{Z}$ d'une structure de $\mathbb{Z}[i]$-module. En déduire qu'il existe deux entiers a et b tels que $p = a^2 + b^2$.

Exercice 6 : Une caractérisation des anneaux principaux

Soit A un anneau commutatif unitaire intègre et noethérien. Montrer que A est principal si, et seulement si, tout module de type fini sans torsion sur A est libre.

Exercice 7 : Matrices à coefficients dans des anneaux euclidiens

Soit A un anneau euclidien. Soit $M \in \mathcal{M}_{m,n}(A)$.

1. Montrer qu'il existe $P \in \mathcal{M}_m(A)$ et $Q \in \mathcal{M}_n(A)$ produits de matrices élémentaires telles que PMQ est de la forme :

$$\begin{pmatrix} d_1 & 0 & 0 & \dots & 0 & \dots & 0 \\ 0 & d_2 & 0 & \dots & 0 & \dots & 0 \\ 0 & 0 & d_3 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & d_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 0 & \dots & 0 \end{pmatrix}$$

où $d_1, \dots, d_r$ sont des éléments de A tels que $d_1 | d_2 | d_3 | \dots | d_r$.

2. Montrer que, si $M \in GL_n(A)$, alors il existe $P \in \mathcal{M}_n(A)$ produit de

matrices élémentaires telle que :

$$PM = \begin{pmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 1 & 0 \\ 0 & 0 & ... & 0 & \det(M) \end{pmatrix}.$$

En déduire que le sous-groupe de $GL_n(A)$ engendré par les matrices élémentaires est $SL_n(A)$.

Exercice 8 : Partiel 2014

Soit A un groupe abélien. Pour $n \in \mathbb{N}^*$, on note $S(A,n)$ l'ensemble des sous-groupes de A d'indice n.

1. Soit $X \in S(A,n)$. Montrer que $nA \subseteq X$.

2. Montrer qu'il existe une bijection entre $S(A,n)$ et $S(A/nA,n)$.

3. Soient $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$. Montrer que, si $m \wedge n = 1$, alors il existe une bijection entre $S((\mathbb{Z}/mn\mathbb{Z})^N, mn)$ et $S((\mathbb{Z}/m\mathbb{Z})^N, m) \times S((\mathbb{Z}/n\mathbb{Z})^N, n)$.

4. Montrer que $S(\mathbb{Z}^2, 2)$ possède 3 éléments, que l'on explicitera.

5. Faire la liste des éléments de $S(\mathbb{Z}^2, n)$. Pour ce faire, on pourra faire la liste des $X \in S(\mathbb{Z}^2, n)$ tels que $X \cap (\mathbb{Z} \oplus 0) = a\mathbb{Z} \oplus 0 \subseteq \mathbb{Z}^2$ pour chaque diviseur positif a de n. En déduire que $|S(\mathbb{Z}^2, n)| = \sum_{a|n} a$, puis expliciter les séries génératrices $\sum_{r\geq 0} |S(\mathbb{Z}^2, p^r)| T^r$ et $\sum_{n\geq 1} |S(\mathbb{Z}^2, n)| n^{-s}$.

6. Faire la liste des éléments de $S(\mathbb{Z}^3, n)$. En déduire que $|S(\mathbb{Z}^3, n)| = \sum_{ab|n} a^2 b$, puis expliciter les séries génératrices $\sum_{r\geq 0} |S(\mathbb{Z}^3, p^r)| T^r$ et $\sum_{n\geq 1} |S(\mathbb{Z}^3, n)| n^{-s}$.

Exercice 9 : Arbre de Bruhat-Tits

Soit p un nombre premier. On note V_0 le $\mathbb{Z}$-module $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$. Soit $\mathcal{V}_1$ l'ensemble des sous-$\mathbb{Z}$-modules d'indice p dans V_0.

1. Montrer que $\mathcal{V}_1$ a exactement $p+1$ éléments.

Soient V_1 un élément de $\mathcal{V}_1$ et $\mathcal{V}_2$ l'ensemble de ses sous-modules d'indice p.

2. Montrer que $\mathcal{V}_2$ a exactement $p+1$ éléments et qu'il contient un unique sous-module homothétique à V_0.

On munit l'ensemble (de sommets)

$$\mathcal{T}_p = \{\text{sous-}\mathbb{Z}\text{-modules de } \mathbb{Z}^2 \text{ d'indice une puissance de } p\}/(\text{homothétie})$$

de la structure de graphe suivante : une arête relie v à v' s'il existe des représentants V et V' de v et v' respectivement tels que V est un sous-module d'indice p de V'.

3. Montrer que l'on a une arête $v \to v'$ si et seulement si il existe une arête $v' \to v$.

Les questions suivantes établissent alors que la structure de graphe conférée à $\mathcal{T}_p$ est en fait un arbre non orienté. Soient v et v' deux sommets de $\mathcal{T}_p$.

4. Montrer qu'il existe des représentants $V_{(0)}$ et $V_{(n)}$ de v et v' respectivement ainsi que des $V_{(i)}$ pour $1 \leq i \leq n-1$ vérifiant $V_{(0)} \supseteq V_{(1)} \supseteq \cdots \supseteq V_{(n)}$ et tels que $V_{(i+1)}$ est d'indice p dans $V_{(i)}$ pour tout i.

Soient $v_0, v_1, \ldots, v_{n-1}, v_n = v_0$ des sommets où chaque v_i est relié à v_{i+1} par une arête.

5. Montrer que l'on a $n = 0$ ou bien ($n \geq 2$ et il existe $1 \leq i \leq n-1$ avec $v_{i+1} = v_{i-1}$).

Exercice 10 : Groupes abéliens finis

Soient A et B deux groupes abéliens finis tels que $|A[n]| = |B[n]|$ pour tout $n > 0$. Montrer que A et B sont isomorphes.

Exercice 11 (difficile) : Groupes abéliens de type cofini

0. *(Quesion préliminaire)* Soit M un groupe abélien. Soit N un sous-groupe de M. On suppose N divisible (ie tel que, pour tout entier $n > 0$, la multiplication par n sur N est surjective). Montrer que M est isomorphe à $N \oplus M/N$.

Soit A un groupe abélien de torsion tel que, pour tout entier naturel non nul n, le sous-groupe de n-torsion $A[n]$ est fini. On dit alors que A est de torsion de type cofini. Nous cherchons à comprendre la structure de A.

1. Fixons un nombre premier p et supposons que A est de torsion p-primaire.

(a) Montrer que A possède un plus grand sous-groupe divisible A_{div} (au sens de l'inclusion).

(b) Montrer qu'il existe $r \geq 0$ tel que $A_{div} \cong (\mathbb{Q}/\mathbb{Z})\{p\}^r$.

(c) Soit $\overline{A} = A/A_{div}$. Montrer que $\overline{A}$ est fini.

(d) En déduire qu'il existe des entiers naturels non nuls $n_1, ..., n_k$ tels que $A \cong (\mathbb{Q}/\mathbb{Z})\{p\}^r \oplus \bigoplus_{i=1}^k \mathbb{Z}/p^{n_i}\mathbb{Z}$.

2. Déduire de la question précédente la structure des groupes abéliens de torsion de type cofini.

Soit maintenant B un groupe abélien de type cofini, c'est-à-dire un groupe abélien tel que, pour tout entier naturel non nul n, les groupes $B[n]$ et B/n sont finis. On note $h_n(B) = \frac{|B[n]|}{|B/n|}$ et on cherche maintenant à comprendre la fonction $n \mapsto h_n(B)$.

3. (a) Considérons $0 \to B \to C \to D \to 0$ une suite exacte de groupes abéliens. Montrer que, si deux parmi les trois groupes B, C, D sont de type cofini, alors le troisième l'est aussi et pour tout $n > 0$, on a :

$$h_n(C) = h_n(B)h_n(D).$$

(b) Soit $n > 0$ un entier. Considérons la décomposition de n en produit de facteurs premiers $n = p_1^{b_1}...p_s^{b_s}$. Montrer que $h_n(B) = \prod_{i=1}^{s} h_{p_i^{b_i}}(B)$.

4. (a) Soit A un groupe fini. Montrer que $h_n(A) = 1$ pour tout $n > 0$.

(b) Soit A un groupe de torsion de type cofini. Montrer que A est un groupe de type cofini et qu'il existe une famille d'entiers naturels $(r_p)_{p\in\mathbb{P}}$ (où $\mathbb{P}$ est l'ensemble des nombres premiers) telle que, pour tout entier $n > 0$, on a :

$$h_n(A) = \prod_{p\in\mathbb{P}} p^{r_p v_p(n)}.$$

Ici, $v_p(n)$ désigne la valuation p-adique de n.

5. Fixons un nombre premier ℓ. Montrer qu'il existe un groupe de torsion de type cofini A, un entier naturel m, un groupe abélien C, un groupe abélien D sur lequel la multiplication par ℓ est un automorphisme et des suites exactes :

$$0 \to A \to B \to C \to 0$$
$$0 \to \mathbb{Z}^m \to C \to D \to 0.$$

6. En déduire qu'il existe une famille d'entiers relatifs $(r_p)_{p\in\mathbb{P}}$ (où $\mathbb{P}$ est l'ensemble des nombres premiers) telle que, pour tout entier $n > 0$:

$$h_n(B) = \prod_{p\in\mathbb{P}} p^{r_p v_p(n)}.$$

Exercice 12 : Polynôme caractéristique et similitude

Soient K un corps, $n \geq 1$ un entier et $P \in K[X]$ un polynôme unitaire de degré n. On note p la fonction partition, qui à un entier $i \geq 1$ associe le nombre de façons distinctes de représenter i comme somme d'entiers.

1. Exprimer, en fonction de la décomposition en facteurs irréductibles de P, le nombre de classes de similitude de matrices de $\mathcal{M}_n(K)$ ayant P pour polynôme caractéristique.

2. Expliciter le résultat pour $P = X^2(X-1)^3(X+1)$.

3. Combien y a-t'il de classes de similitude dans $\mathcal{M}_3(\mathbb{Z}/2\mathbb{Z})$?

Exercice 13 : Endomorphismes de polynôme minimal donné

Soient K un corps et $P \in K[X]$ un polynôme non constant. Soit Σ l'ensemble des entiers naturels n tels qu'il existe un K-espace vectoriel V de dimension n muni d'un endomorphisme linéaire u de polynôme minimal égal à P. Montrer qu'il existe $N \in \mathbb{N}$ et $d \in \mathbb{N}^*$ tels que $\Sigma \cap [N, +\infty[= d\mathbb{N} \cap [N, +\infty[$. Que vaut d ?

Exercice 14 : Examen 2011
Soit K un corps. Pour chaque polynôme unitaire $P \in K[X]$, on note $C(P)$ la matrice compagnon associée. Si P et Q sont deux polynômes unitaires, déterminer les invariants de similitude de la matrice :

$$\begin{pmatrix} C(P) & 0 \\ 0 & C(Q) \end{pmatrix}.$$

Exercice 15 : Commutant
Soient K un corps infini et V un K-espace vectoriel non nul de dimension finie. Pour u un endomorphisme de V, on note $\mathcal{C}(u) = \{v \in \mathrm{End}_K(V) \mid uv = vu\}$ et $\mathcal{P}(u) = \{P(u) \mid P \in K[X]\}$.

1. Soit $u \in \mathrm{End}_K(V)$. Montrer que $\mathcal{P}(u) = \bigcap_{v \in \mathcal{C}(u)} \mathcal{C}(v)$.

2. Soit $u \in \mathrm{End}_K(V)$. Montrer que les propriétés suivantes sont équivalentes :

(i) u est cyclique ;

(ii) le polynôme minimal de u est égal (au signe près) au polynôme caractéristique ;

(iii) $\mathcal{C}(u) = \mathcal{P}(u)$;

(iv) V n'a qu'un nombre fini de sous-espace stables par u.