TD 3. $\mathbb{Z}$-modules

Exercice 1

a) Vérifier que tout groupe abélien est un $\mathbb{Z}$-module.

b) Soit i une racine (complexe) de X^2+1. On considère $\mathbb{Z}[i] = \{P(i),\ P \in \mathbb{Z}[X]\}$.
Vérifier que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$; montrer que c'est un $\mathbb{Z}$-module libre de rang 2, en donner une base.
[On pourra montrer que tout $x \in \mathbb{Z}[i]$ s'écrit de façon unique $x = a + ib$ avec $a, b \in \mathbb{Z}$.]

c) On pose $\varphi = \frac{1+\sqrt{5}}{2}$. De quel trinôme φ est-il racine ? Déterminer son conjugué $\overline{\varphi}$ (l'autre racine du trinôme) ; calculer $\varphi + \overline{\varphi}$ et $\varphi\overline{\varphi}$. Montrer que $\mathbb{Z}[\varphi]$ est un $\mathbb{Z}$-module libre de rang 2.
[Pour l'unicité, on se ramènera à montrer que, si $0 = a + b\varphi$ avec $a, b \in \mathbb{Z}$, alors $a = b = 0$, en considérant $a + b\overline{\varphi}$.]

Exercice 2 (Torsion)

Un $\mathbb{Z}$-module M est *de torsion* si pour tout $x \in M$, il existe $n \in \mathbb{Z} \setminus \{0\}$ tel que $nx = 0$; il est *sans torsion* si :

$$\forall n \in \mathbb{Z}\,,\ \forall x \in M\,,\ nx = 0 \Rightarrow (\,n = 0 \text{ ou } x = 0\,)\ .$$

a) Donner un exemple de $\mathbb{Z}$-module de torsion, un exemple de $\mathbb{Z}$-module sans torsion et un exemple de $\mathbb{Z}$-module qui ne soit ni l'un ni l'autre.

b) Montrer qu'un module qui n'est pas sans torsion n'est pas libre.
[On pourra montrer que 0 s'écrit de plusieurs façons combinaison linéaire des éléments d'un système générateur donné.]

On vient de montrer que «libre» entraîne «sans torsion» ; la réciproque n'est pas vraie en général, comme va le montrer l'exercice suivant (on verra ensuite qu'un $\mathbb{Z}$-module de type fini sans torsion est toujours libre).

Exercice 3 ($\mathbb{Q}$)

On considère le corps des rationnels $\mathbb{Q}$. Vérifier que c'est un $\mathbb{Z}$-module et montrer :

a) qu'il est sans torsion ;

b) qu'il n'est pas de type fini, c'est-à-dire que $\mathbb{Q}$ n'admet pas de famille génératrice finie en tant que $\mathbb{Z}$-module *(on pourra raisonner par l'absurde)* ;

c) qu'entre deux nombres rationnels quelconques existe toujours une relation de dépendance linéaire sur $\mathbb{Z}$. En déduire que $\mathbb{Q}$ n'est pas libre.

d) Existe-t-il un système générateur pour $\mathbb{Q}$?

e) Montrer que $\mathbb{Q}/\mathbb{Z}$ est un $\mathbb{Z}$-module de torsion.

f) Faire de même (questions a-e) en remplaçant $\mathbb{Q}$ par $\mathbb{Z}[x]$ pour $x \in \mathbb{Q} \setminus \mathbb{Z}$.

Exercice 4
Soit M un $\mathbb{Z}$-module de type fini. Par le théorème de structure des $\mathbb{Z}$-modules de type fini, on a un isomorphisme de $\mathbb{Z}$-modules :

$$M \simeq \mathbb{Z}^n \times \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z} \ ,$$

où $n, r \in \mathbb{N}$ et $d_1, \ldots, d_r \in \mathbb{N}$ avec $d_1|d_2|\cdots|d_r$.

a) Vérifier que l'on peut supposer $d_1 \neq 1$ et $d_r \neq 0$.

b) On suppose M sans torsion, en déduire que $r = 0$, puis que M est libre. L'hypothèse «de type fini» est-elle indispensable ?

c) À l'aide du théorème de structure des $\mathbb{Z}$-modules, déterminer le nombre de groupes abéliens d'ordre 400 à isomorphisme près.

Exercice 5 (Facteurs invariants)
Soit L le sous-$\mathbb{Z}$-module de $\mathbb{Z}^2$ engendré par $v_1 = (1,2)$ et $v_2 = (2,7)$: $L = \mathbb{Z}v_1 + \mathbb{Z}v_2$. On va déterminer les facteurs invariants de $\mathbb{Z}^2/L$ (les nombres d_i du théorème de structure).

a) Soit $f : \mathbb{Z}^2 \to \mathbb{Z}$ l'homorphisme défini par $f(x,y) = x$; montrer que $f(L) = \mathbb{Z}$ et trouver $u_1 \in L$ tel que $f(u_1) = 1$; déterminer $u_2 \in \mathbb{Z}^2$ tel que $\ker(f) = \mathbb{Z}u_2$.

b) Vérifier qu'alors

$$\mathbb{Z}^2 = \mathbb{Z}u_1 \oplus \mathbb{Z}u_2 \quad \text{et} \quad L = \mathbb{Z}u_1 + (L \cap \mathbb{Z}u_2) \ ;$$

déterminer $L \cap \mathbb{Z}u_2$.

c) Vérifier que tout élément de $\mathbb{Z}^2$ est congru à 0, u_2 ou $-u_2$ modulo L ; en déduire les facteurs invariants de $\mathbb{Z}^2/L$.

d) Faire de même pour le sous-$\mathbb{Z}$-module $\mathbb{Z}(2,0) + \mathbb{Z}(0,3)$ de $\mathbb{Z}^2$ (on considèrera l'homomorphisme $g(x,y) = y - x$).

Exercice 6 (Indice)
Soient L, M des sous-$\mathbb{Z}$-modules de même rang n de $\mathbb{Z}^n$ avec $L \subseteq M$.

a) Étant données deux bases $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_n)$ de M, et U la matrice de passage de l'une à l'autre, montrer que $\det(U) = \pm 1$.
[On pourra considérer la matrice de passage dans l'autre sens V ; que vaut $\det(UV)$?]

b) On note $d_1, \ldots, d_n$ les facteurs invariants de M/L. Vérifier que l'*indice* de L dans M (c'est-à-dire le cardinal de M/L) vaut

$$[M : L] = d_1 \cdots d_n \ .$$

c) On sait (théorème de la *base adaptée*) qu'il existe une base $(x_1, \ldots, x_n)$ de M telle que $(d_1x_1, \ldots, d_nx_n)$ soit une base de L. En déduire que, pour toutes bases $(y_1, \ldots, y_n)$ de M, $(z_1, \ldots, z_n)$ de L, on a, en notant A la matrice des z_i dans $(y_1, \ldots, y_n)$:

$$[M : L] = \det(A) \ .$$

[On commencera par établir le résultat pour des bases bien choisies, puis on l'étendra à toutes les bases grâce au résultat du a)*.]*