TD4 : Anneaux noethériens et modules

Diego Izquierdo

Les exercices 1, 3 (questions 1 et 2), 12, 7, 13 ont été traités pendant la séance, ainsi que la question 2 de l'exercice 15 et l'exercice 5 du TD5.

Exercice 2 : Vrai ou faux ? Le retour

Soit A un anneau.

1. Tout quotient d'un anneau noethérien est noethérien.

> **Indications :** VRAI : Soient A un anneau et I un idéal de A. Soit J un idéal de A/I. Soit $\tilde{J} = p^{-1}(J)$ où $p : A \to A/I$ est la projection canonique. Comme A est noethérien, il existe $j_1, ..., j_r \in A$ tels que $\tilde{J} = (j_1, ..., j_r)$. On a alors $J = p(\tilde{J}) = (p(j_1), ..., p(j_r))$.

2. Tout anneau factoriel est noethérien.

> **Indications :** FAUX : Dans le TD3, nous avons vu que $\mathbb{Z}[(X_n)_{n\in\mathbb{N}}]$ est factoriel. Mais il n'est pas noethérien puisque l'idéal engendré par les X_n (pour $n \in \mathbb{N}$) n'est pas de type fini.

3. Tout anneau euclidien est noethérien.

> **Indications :** VRAI : Un anneau euclidien est principal, donc noethérien.

4. Si I est un idéal de type fini de A et A/I est noethérien, alors A est noethérien.

> **Indications :** FAUX : Prendre A la sous-$\mathbb{C}$-algèbre de $\mathbb{C}[X, Y]$ engendrée par les $X^n Y$ pour $n > 0$. D'après l'exercice 1 du TD2, A n'est pas noethérien, mais $A/XA \cong \mathbb{C}[T]$ est principal.

5. Un produit fini d'anneaux noethériens est un anneau noethérien.

> **Indications :** VRAI : Soient $A_1, ..., A_r$ des anneaux. Soit $A = \prod_i A_i$. Soit I un idéal de A. Il existe $I_1, ..., I_r$ des idéaux de $A_1, ..., A_r$ tels que $I = \prod_i I_i$. Pour chaque I, il existe $a_{i,1}, ..., a_{i,s_i} \in A_i$ tels que $I_i = (a_{i,1}, ..., a_{i,s_i})$. L'idéal I est alors engendré par les éléments de la forme $(b_1, ..., b_r)$, avec $b_1 = 0$, ..., $b_{i-1} = 0$, $b_i = a_{i,j}$, $b_{i+1} = 0$, ..., $b_r = 0$.

6. Toute famille génératrice minimale de A^n est de cardinal au moins n.

> **Indications :** VRAI : S'il existait une famille génératrice de A^n de cardinal au plus $n-1$, il existerait un morphisme surjectif de A-modules $f : A^{n-1} \to A^n$. Soit $(e_1, ..., e_n)$ la base canonique de A^n. Pour chaque $i \in \{1, ..., n\}$, soit $x_i \in A^{n-1}$ tel que $f(x_i) = e_i$. Soient $g : A^n = A^{n-1} \oplus A \to A^n, (x, y) \mapsto f(x)$ et $h : A^n \to A^n = A^{n-1} \oplus A, e_i \mapsto (x_i, 0)$. On vérifie aisément que $g \circ h = Id$. Donc $\det g \det h = 1$. Mais $\det h = 0$: absurde !

7. Toute famille libre maximale de A^n est une base de A^n.

> **Indications :** FAUX : (2) est une famille libre maximale de $\mathbb{Z}$ mais n'est pas une base.

8. Toute famille génératrice minimale de A^n est une base.

> **Indications :** FAUX : $(2, 3)$ est une famille génératrice minimale du $\mathbb{Z}$-module $\mathbb{Z}$, mais n'est pas une base.

9. Il existe un $\mathbb{Z}$-module qui n'a pas de famille libre maximale.

> **Indications :** FAUX : Soit M un groupe abélien. Soit $\mathcal{E}$ l'ensemble des familles libres de M. Il est non vide puisqu'il contient la famille vide. On vérifie aisément que l'inclusion est un ordre inductif. Par conséquent, $\mathcal{E}$ possède un élément maximal.

10. Un $\mathbb{Z}$-module sans torsion est libre.

> **Indications :** FAUX : Le groupe abélien $\mathbb{Q}$ est sans torsion, mais il n'est pas libre puisqu'il est divisible.

11. Si $0 \to M_1 \to M_2 \to M_3 \to 0$ est une suite exacte de A-modules et M_1 et M_3 sont libres de rang fini, alors M_2 est libre de rang $\mathrm{rg}(M_1) + \mathrm{rg}(M_3)$.

> **Indications :** VRAI : On note $f : M_1 \to M_2$ et $g : M_2 \to M_3$ les morphismes apparaissant dans la suite exacte. Soit $(e_1, ..., e_r)$ une base de M_3. Soient $x_1, ..., x_r$ des éléments de M_2 tels que $g(x_i) = e_i$ pour chaque i. Soit $h : M_3 \to M_2$ le morphisme tel que $h(e_i) = x_i$ pour chaque i. On vérifie alors que $M_1 \oplus M_3 \to M_2, (x, y) \mapsto f(x) + h(y)$ est un isomorphisme de A-modules, ce qui achève la preuve.

Exercice 3 (à préparer) : Un exemple d'anneau non noethérien

Soit $A = \{P \in \mathbb{Q}[X] \mid P(0) \in \mathbb{Z}\}$.

1. Montrer que A n'est pas factoriel.

2. Montrer que A n'est pas noethérien.

3. Montrer que A est de Bézout, c'est-à-dire que tout idéal de type fini de A est principal.

Indications : Par récurrence, on est ramené à prouver que tout idéal de A engendré par deux éléments $a+XP$ et $b+XQ$ avec $a,b\in\mathbb{Z}$ et $P,Q\in\mathbb{Q}[X]$ est principal.
Supposons dans un premier temps $a\neq 0$ et $b\neq 0$. Soit alors $R\in\mathbb{Q}[X]$ l'unique polynôme vérifiant $(a+XP,b+XQ)=(1+XR)$ dans $\mathbb{Q}[X]$. Aussi, soit c le pgcd de a et b dans $\mathbb{Z}$. Montrons que $(a+XP,b+XQ)=(c+cXR)$ dans A. L'inclusion $\subseteq$ est directe par définition de c et de R. Réciproquement, il existe $u+XU$ et $v+XV\in\mathbb{Q}[X]$ vérifiant

$$(a+XP)(u+XU)+(b+XQ)(v+XV)=c(1+XR). \tag{1}$$

En particulier, on remarque $au+bv=c$ (mais non nécessairement à coefficients dans $\mathbb{Z}$). Prenons $\alpha,\beta\in\mathbb{Z}$ avec $a\alpha+b\beta=c$; on a alors $a(\alpha-u)+b(\beta-v)=0$. On écrit alors

$$(a+XP)(u+XU+\frac{\alpha-u}{b}(b+XQ))+(b+XQ)(v+XV+\frac{\beta-v}{a}(a+XP))=c+cXR.$$

Cela prouve l'inclusion $\supseteq$ dans le cas $ab\neq 0$.
Maintenant, si on a $a\neq 0$ et $b=0$ (l'autre cas étant symétrique), on procède comme précédemment jusqu'à obtenir (1). Là, on remarque $au=c=\pm a$ (puisque $b=0$) et donc $u\in\mathbb{Z}$. Reste à écrire

$$vXQ=(a+XP)(\frac{v}{a}XQ)+(XQ)(-\frac{v}{a}XP)$$

pour voir que l'on a

$$c(1+XR)=(a+XP)(u+XU+\frac{v}{a}XQ)+(XQ)(XV-\frac{v}{a}XP).$$

Enfin, si on a $a=0$ et $b=0$, il existe $n,m\in\mathbb{N}^*$ tels que l'on puisse écrire

$$XP=\frac{1}{n}X^m(a'+XP'),\quad XQ=\frac{1}{n}X^m(b'+XQ'),$$

avec $a',b'\in\mathbb{Z}$, l'un des deux au moins étant non nul. Cela nous ramène aux cas précédents et termine la preuve.

Exercice 4 : Un autre exemple d'anneau non noethérien

On rappelle qu'un nombre complexe x est un *entier algébrique* s'il existe un polynôme $P\in\mathbb{Z}[X]$ unitaire tel que l'on ait $P(x)=0$. On note $\overline{\mathbb{Z}}$ l'anneau des entiers algébriques.

1. Rappeler pourquoi $\overline{\mathbb{Z}}$ est un anneau.

Indications : Corollaire 3.4 du polycopié d'Algèbre 1.

2. Montrer que $\overline{\mathbb{Z}}$ n'est pas factoriel.

Indications : Pour chaque entier $n\geq 1$, on a $2=(\sqrt[n]{2})^n$. Il suffit donc de montrer que $x_n=\sqrt[n]{2}$ n'est pas inversible dans $\overline{\mathbb{Z}}$. Comme $x_n^{-n}=\frac{1}{2}$, il suffit de montrer que $\frac{1}{2}\notin\overline{\mathbb{Z}}$. Cela découle immédiatement de la remarque suivante : le coefficient dominant d'un polynôme à coefficients dans $\mathbb{Z}$ annulant $\frac{1}{2}$ est pair.

3. Montrer que $\overline{\mathbb{Z}}$ n'est pas noethérien.

Indications : Pour chaque entier $n \geq 1$, on note $I_n = (\sqrt[n!]{2})$. On a alors $I_n \subseteq I_{n+1}$ pour tout n. Supposons qu'il existe $n \geq 1$ tel que $I_n = I_{n+1}$. Cela impose que $x_0 = 2^{\frac{1}{(n+1)!} - \frac{1}{n!}} \in \overline{\mathbb{Z}}$. On en déduit que $2^{n-1} x_0^{(n+1)!} = \frac{1}{2} \in \overline{\mathbb{Z}}$: absurde (voir question 2) ! Donc $\overline{\mathbb{Z}}$ n'est pas noethérien.

4. Comme dans l'exercice 3, on peut montrer que $\overline{\mathbb{Z}}$ est un anneau de Bézout, mais la preuve dépasse largement le cadre de ce cours.

Exercice 5 : Anneau des fonctions continues

Soit X un espace topologique métrisable. À quelle condition sur X l'anneau des fonctions continues de X dans $\mathbb{R}$ est-il noethérien ?

Indications : Notons $C(X)$ l'anneau des fonctions continues de X dans $\mathbb{R}$. Si X est fini, on a $C(X) \cong \mathbb{R}^X$, qui est bien noethérien. Réciproquement, supposons que $C(X)$ est noethérien. Soit $x_0 \in X$. Supposons que $\{x_0\}$ n'est pas ouvert. Pour chaque $n \geq 1$, on note $f_n : X \to \mathbb{R}, x \mapsto d(x, x_0)^{1/n!}$ et $I_n = (f_n)$. La suite (I_n) est une suite croissante d'idéaux qui ne stationne pas : absurde ! Donc $\{x_0\}$ est ouvert et X est muni de la topologie discrète. On en déduit que $C(X) \cong \mathbb{R}^X$. Comme $C(X)$ est noethérien, X est fini.

Exercice 6 : Séries formelles

Soit A un anneau noethérien. Montrer que $A[[X]]$ est noethérien.

Indications : S'inspirer de la preuve du théorème de Hilbert.

Exercice 8 : Noethérianité et factorialité

Soit A un anneau intègre noethérien. Montrer que tout élément non nul de A s'écrit sous la forme $up_1...p_n$ avec $u \in A^\times$ et p_i irréductible pour chaque i. L'anneau A est-il forcément factoriel ?

Indications : Supposons que A possède un élément qui ne s'écrit pas sous la forme désirée. Soit $\mathcal{E}$ la famille des idéaux principaux engendrés par un élément de A qui ne s'écrit pas sous la forme désirée. Par noethérianité de A, la famille $\mathcal{E}$ possède un élément maximal I pour l'inclusion. Soit x un générateur de I. Comme $I \in \mathcal{E}$, x n'est ni inversible ni irréductible. On peut donc écrire $x = yz$ avec y et z non inversibles. Par maximalité de I, y et z s'écrivent sous la forme $up_1...p_n$ avec $u \in A^\times$ et p_i irréductible pour chaque i. Il en est donc de même pour x : absurde ! Donc tout élément non nul de A s'écrit sous la forme $up_1...p_n$ avec $u \in A^\times$ et p_i irréductible pour chaque i. Par contre, A n'est pas forcément factoriel : par exemple, $A = \mathbb{C}[T^2, T^3] = \mathbb{C}[X, Y]/(X^2 - Y^3)$ est noethérien non factoriel.

Exercice 9 : Une caractérisation des anneaux noethériens

Soient A un anneau, I un idéal de A et a un élément de A. Montrer que si $I + (a)$ et $\{x \in A \mid ax \in I\}$ sont des idéaux de type fini de A, alors I est de type fini. En déduire que A est noethérien si, et seulement si, tous ses idéaux

premiers sont de type fini.

Indications : On écrit $I + (a) = (f_1, ..., f_r)$ et $\{x \in A \mid ax \in I\} = (g_1, ..., g_s)$. Pour $i \in \{1, ..., r\}$, on écrit $f_i = h_i + ak_i$ avec $h_i \in I$ et $k_i \in A$. On vérifie alors aisément que $I = (h_1, ..., h_r, ag_1, ..., ag_s)$.
Supposons maintenant que tout idéal premier de A est de type fini. Soit $\mathcal{E}$ la famille constituée des idéaux de A qui ne sont pas de type fini, et supposons que $\mathcal{E}$ soit non vide. L'inclusion est un ordre inductif sur $\mathcal{E}$. Donc, d'après le lemme de Zorn, $\mathcal{E}$ possède un élément maximal I_0. Par hypothèse, I_0 n'est pas premier, donc il existe $a, b \in A$ tels que $a \notin I_0$, $b \notin I_0$ et $ab \in I_0$. Par maximalité $I_0 + (a)$ et $I_0 + (b)$ sont de type fini. Donc $\{x \in A \mid ax \in I_0\}$ et $\{x \in A \mid bx \in I_0\}$ ne sont pas de type fini, et toujour par maximalité, $\{x \in A \mid ax \in I_0\} = \{x \in A \mid bx \in I_0\} = I_0$. Mais alors $A = \{x \in A \mid abx \in I_0\} = I_0$: absurde ! Donc $\mathcal{E}$ est vide.

Exercice 10 : Modules de type fini
Soient A un anneau, M un A-module de type fini et $n \in \mathbb{N}$. Considérons un morphisme surjectif de A-modules $u : M \to A^n$. Montrer que $\mathrm{Ker}(u)$ est un A-module de type fini.

Indications : Soit $(e_1, ..., e_n)$ la base canonique de A^n. Pour chaque i, soit $x_i \in M$ tel que $u(x_i) = e_i$. Soit $f : A^n \to M, e_i \mapsto x_i$. On remarque alors que $A^n \oplus \mathrm{Ker}(u) \to A, (x, y) \mapsto f(x) + y$ est un isomorphisme. Par conséquent, $\mathrm{Ker}(u)$ est un quotient de M, qui est de type fini. Cela achève la preuve.

Exercice 11 : Sous-groupes du groupe des racines de l'unité
Faire la liste des sous-groupes du groupe des racines de l'unité dans $\mathbb{C}^\times$.

Indications : Soit U le groupe des racines de l'unité. Soit V un sous-groupe. Les groupes U et V sont de torsion. On a donc :

$$U = \bigoplus_p U\{p\},$$

$$V = \bigoplus_p V\{p\},$$

et pour chaque premier p, $V\{p\}$ est un sous-groupe de $U\{p\}$. Soit p un nombre premier. On vérifie aisément que, pour tout $r \geq 1$, si $V\{p\}$ possède un élément d'ordre p^r, alors $V\{p\}$ contient $U[p^r]$. On en déduit que $V\{p\} = U\{p\}$ ou $V\{p\} = U[p^r] = \mu_{p^r}$ pour un certain $r \geq 0$. Par conséquent, les sous-groupes de U sont donc les $\bigoplus_p V_p$ avec $V_p = U\{p\}$ ou $V_p = \mu_{p^{r_p}}$ pour un certain $r_p \geq 0$.

Exercice 14 : Modules noethériens et polynômes
Soient A un anneau et M un A-module. Montrer que $M[X]$ est un $A[X]$-module noethérien si, et seulement si, M est un A-module noethérien.

Indications : Supposons M noethérien. Soit N un sous-A[X]-module de M[X]. Montrons qu'il est de type fini. Soit

$N_n = \{m \in M / \exists P \in N : deg(P) = n$ et m est le coefficient dominant de $P\} \cup \{0\}$.

Les N_n sont des A-modules et la suite $(N_n)_n$ est croissante. Comme M est noethérien, la suite des $(N_n)_n$ est stationnaire, disons à partir de n_0 et les modules N_n sont engendrés par un nombre fini d'éléments, les $(b_{n,k})_{1 \leq k \leq k_n}$. Pour chaque paire (n,k), notons $P_{n,k} \in N$ un polynôme de degré n dont le coefficient dominant est $b_{n,k}$. Nous allons montrer que N est engendré par les $(P_{n,k})_{1 \leq n \leq n_0, 1 \leq k \leq k_n}$. Soit N_0 le sous-A[X]-module de $M[X]$ engendré par ces éléments. Soit $P \in N$ de degré d. Montrons par récurrence sur d que $P \in N_0$. Notons m le coefficient dominant de P. On a $m \in N_d$. Si $d \leq n_0$, alors $m = \sum_k a_k b_{d,k}$ pour certains $a_k \in A$ et donc $Q = P - \sum_k a_k P_{d,k} \in N$ est de degré strictement inférieur à d Par hypothèse de récurrence, on déduit que $Q \in N_0$, ce qui montre que $P \in N_0$. Si $d > n_0$, alors $m \in N_d = N_{n_0}$ et il existe des $a_k \in A$ tels que $Q = P - X^{d-n_0} \sum_k a_k P_{n_0,k} \in N$ est encore de degré strictement inférieur à d. On conclue comme précédemment.

Exercice 15 : Chasses au diagramme

1. Soit A un anneau. Soient $f : M \to N$ et $g : N \to P$ des morphismes de A-modules. Montrer qu'il existe une suite exacte :

$$0 \to \mathrm{Ker}(f) \to \mathrm{Ker}(g \circ f) \to \mathrm{Ker}(g) \to \mathrm{Coker}(f) \to \mathrm{Coker}(g \circ f) \to \mathrm{Coker}(g) \to 0.$$

2. On considère un diagramme commutatif de A-modules à lignes exactes :

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5. \end{array}$$

On suppose que les morphismes f_1, f_2, f_4, f_5 sont des isomorphismes. Montrer que f_3 est un isomorphisme.

Exercice 16 : Déterminant

Soient R un anneau et n un entier naturel non nul. Soit $f : R^n \to R^n$ un morphisme de R-modules. Soit A la matrice de f dans la base canonique de R^n.

1. Montrer que les assertions suivantes sont équivalentes :
(i) f est surjectif ;
(ii) f est un isomorphisme ;
(iii) $\det(A) \in R^\times$.

Indications : Les implications $(iii) \Rightarrow (ii) \Rightarrow (i)$ sont évidentes. Supposons (i) et notons $(e_1, ..., e_n)$ la base canonique de R^n. Soient $x_1, ..., x_n \in R^n$ tels que $f(x_i) = e_i$ pour chaque i. Soit $g : R^n \to R^n, e_i \mapsto x_i$. On a alors $f \circ g = Id$. Par conséquent, en notant B la matrice de g, on a $\det(A)\det(B) = 1$, et donc $\det(A) \in R^\times$. Cela prouve aussi que f est un isomorphisme.

2. Montrer que les assertions suivantes sont équivalentes :

(i) f est injectif ;
(ii) $\det(A)$ n'est pas un diviseur de 0 dans R.

Indications : La formule ${}^t\mathrm{Com}(A)A = \det(A)I_n$ montre que $(ii) \Rightarrow (i)$. Supposons maintenant (i). Supposons que $\det(A)$ est un diviseur de 0 dans R. Soit $b \in R$ non nul tel que $b\det(A) = 0$. Soit N une sous-matrice carrée de taille maximale de A telle que $b\det(N) \neq 0$. Soit r la taille de N. Comme f est injectif, $r \geq 1$. Quitte à réordonner les lignes et les colonnes de A, on peut supposer que N est situé en haut à gauche de A. En notant $A = (a_{ij})$, on considère pour chaque $i \in \{1, ..., n\}$ la matrice :

$$A_i = \begin{pmatrix} a_{1,1} & \dots & a_{1,r+1} \\ \vdots & & \vdots \\ a_{r,1} & \dots & a_{r,r+1} \\ a_{i,1} & \dots & a_{i,r+1} \end{pmatrix}.$$

On vérifie alors que $b\det A_i = 0$ pour tout i. Par conséquent, pour chaque i, en développant par rapport à la dernière ligne, on a $b\sum_{j=1}^{r+1}(-1)^j a_{i,j}\mu_j = 0$ où μ_j désigne le mineur correspondant au coefficient de position $(r+1, j)$. Cela montre que le vecteur $(-b\mu_1, b\mu_2, ..., (-1)^{r+1}b\mu_{r+1}, 0, ..., 0)$ est dans le noyau de f. Or $b\mu_{r+1} \neq 0$: absurde ! Donc $\det(A)$ n'est pas un diviseur de 0 dans R.

Exercice 17 : Théorème de Cayley-Hamilton

Soit R un anneau.

1. Soit M un R-module de type fini. Soient $m_1, ..., m_n$ des générateurs de M. Soit f un endomorphisme de M, et considérons une matrice $A = (a_{ij}) \in \mathcal{M}_n(R)$ telle que $f(m_i) = \sum_{j=1}^n a_{ij}m_j$ pour $1 \leq i \leq n$. On note $P(X) = \det(XI_n - A)$. Montrer que $P(f) = 0$.

Indications : Voir le théorème 3.2 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).

2. Soit M un R-module de type fini.

(a) Soit I un idéal de R tel que $IM = M$. Montrer qu'il existe $a \in I$ tel que $(1 - a)M = 0$.

Indications : Voir le corollaire 3.5 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).

(b) Déduire qu'un endomorphisme surjectif de M est un isomorphisme. Comparer ce résultat à la question 1. de l'exercice précédent.

Indications : Voir le corollaire 3.3 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).

3. Montrer que, si m et n sont deux entiers naturels et $g : R^m \to R^n$ est un morphisme injectif de R-modules, alors $m \leq n$.

Indications : Supposons $m > n$. Soit $\tilde{g} : R^m \to R^m = R^n \times R^{m-n}, x \mapsto (g(x), 0)$. On note $(e_1, ..., e_n)$ la base canonique de R^n. D'après la question 1., il existe un polynôme unitaire P à coefficients dans R tel que $P(\tilde{g}) = 0$. Soit P_0 un tel polynôme de degré minimal. On remarque que $0 = P_0(e_n) = P_0(0)e_n$. Par conséquent, $P_0(0) = 0$ et il existe $Q \in R[X]$ unitaire tel que $P_0 = XQ$ et $\deg Q = \deg P_0 - 1$. On a alors $\tilde{g} \circ Q(\tilde{g}) = 0$. Mais par hypothèse, le morphisme $\tilde{g}$ est injectif, et donc $Q(\tilde{g}) = 0$: absurde !

Exercice 18 (important) : Modules projectifs et injectifs

Soit A un anneau.

1. Soient M, N et P trois A-modules. Si l'on a une suite exacte $0 \to M \to N \to P \to 0$, peut-on en déduire que $N \cong M \oplus P$?

Indications : Non : Prendre la suite exacte de $\mathbb{Z}$-modules naturelle :

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

2. Soient M, N et P trois A-modules. Montrer que les trois conditions suivantes sont équivalentes :

- il existe un isomorphisme $N \cong M \oplus P$.
- il existe une suite exacte de A-modules $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ et un morphisme de A-modules $s : P \to N$ tel que $g \circ s = \mathrm{Id}_P$.
- il existe une suite exacte de A-modules $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ et un morphisme de A-modules $t : N \to M$ tel que $t \circ f = \mathrm{Id}_M$.

Indications : La première propriété implique les deux autres de manière évidente. Si la deuxième propriété est vérifiée, on remarque que $M \oplus P \to N, (m, p) \mapsto f(m) + s(p)$ est un isomorphisme, d'où la première propriété. Si la troisième propriété est vérifiée, on remarque que $N \to M \oplus P, n \mapsto (t(n), g(n))$ est un isomorphisme, d'où la première propriété.

3. On dit qu'un A-module P est *projectif* si la propriété suivante est vérifiée : si M et N sont des A-modules tels qu'il existe une suite exacte $0 \to M \to N \to P \to 0$, alors il existe un isomorphisme $N \cong M \oplus P$.

(a) Montrer qu'un A-module est projectif si, et seulement si, il est un facteur direct d'un A-module libre.

Indications : Soit P un A-module projectif. Soit R le A-module libre de base $(e_p)_{p \in P}$. Le morphisme $f : R \to P, e_p \mapsto p$ est surjectif. On en déduit que $R \cong \mathrm{Ker}(f) \oplus P$, ce qui montre que P est un facteur direct d'un A-module libre. Réciproquement, soit P un A-module facteur direct d'un A-module libre R. On écrit $R = P \oplus T$. Considérons une suite exacte $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$. On a alors une suite exacte :

$$0 \to M \oplus T \to N \oplus T \to R \to 0.$$

Soit (e_i) une base de R. Pour chaque i, soit $x_i \in N \oplus T$ tel que l'image de x_i dans R est e_i. Soit $u : R \to N \oplus T, e_i \mapsto x_i$. Ce morphisme induit naturellement un morphisme $s : P \to N$ vérifiant $g \circ s = Id$. La question 2 permet alors de conclure que $N \cong M \oplus P$, ce qui achève la preuve.

(b) Montrer que si A est un corps, alors tout A-module est projectif.

Indications : Dans ce cas, tout A-module est libre, donc projectif.

(c) Montrer que si $A = \mathbb{Z}$, un A-module de type fini est projectif si, et seulement si, il est libre. En utilisant la classification des modules de type fini sur un anneau principal que vous verrez en cours cette semaine, on peut montrer que ce résultat subsiste si A est principal.

Indications : Si M est un groupe abélien de type fini projectif, alors il est facteur direct d'un groupe abélien libre : il n'a donc pas de torsion et est lui-même libre d'après la classification des groupes abéliens de type fini.

(d) Supposons que $A = B \times C$ où B et C sont des anneaux non nuls. Montrer que B est un A-module projectif non libre.

Indications : Comme B est un facteur direct de A, il est projectif. Par contre, il n'est pas libre puisqu'il est annulé par $\{0\} \times C$.

On se place dans le cas où A est l'anneau des fonctions continues 2π-périodiques de $\mathbb{R}$ dans $\mathbb{R}$.

(e) Soit P le A-module formé des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ telles que $f(x + 2\pi) = -f(x)$ pour tout $x \in \mathbb{R}$. En construisant un isomorphisme de A-modules $P \oplus P \cong A \oplus A$, montrer que P est projectif. Est-il libre ?

Indications : Les morphismes de A-modules suivants son bien définis et sont inverses l'un de l'autre :

$$\begin{array}{ccc} A \oplus A & \xrightarrow{\sim} & P \oplus P \\ (f, g) & \mapsto & \left(f\cos\left(\frac{x}{2}\right) + g\sin\left(\frac{x}{2}\right), f\sin\left(\frac{x}{2}\right) - g\cos\left(\frac{x}{2}\right)\right) \end{array} ;$$

$$\begin{array}{ccc} P \oplus P & \xrightarrow{\sim} & A \oplus A \\ (f, g) & \mapsto & \left(f\cos\left(\frac{x}{2}\right) + g\sin\left(\frac{x}{2}\right), f\sin\left(\frac{x}{2}\right) - g\cos\left(\frac{x}{2}\right)\right) \end{array} .$$

On a donc un isomorphisme $P \oplus P \cong A \oplus A$ qui montre que P est projectif comme A-module.
Supposons P libre. D'après l'isomorphisme précédent, il serait de rang 1, engendré par un certain $p \in P$. Parce que p vérifie $p(2\pi) = -p(0)$, p s'annule en un point $x \in [0, 2\pi[$: il s'ensuit que tout élément de P s'annule en ce même point x, ce qui est absurde (on peut translater le graphe de p horizontalement).

(f) Soit N le A-module constitué des fonctions continues f de $\mathbb{R}$ dans $\mathbb{R}$ à décroissance rapide (c'est-à-dire telles que, pour tout $n \geq 0$, on a $\lim\limits_{x\to+\infty} x^n f(x) = \lim\limits_{x\to-\infty} x^n f(x) = 0$). Montrer qu'il existe un facteur direct du A-module N isomorphe à P.

Indications : Soit $f \in N$. On note $F(f) : \mathbb{R} \to \mathbb{R}, x \mapsto \sum_{k\in\mathbb{Z}} (-1)^k f(x + 2k\pi)$. On remarque que F définit un morphisme de A-modules $N \to P$. Soit $\lambda : \mathbb{R} \to \mathbb{R}$ qui est affine sur chaque intervalle $[2k\pi, 2(k + 1)\pi]$ pour $k \in \mathbb{Z}$ et telle que $\lambda(2k\pi) = \frac{1}{3\cdot 2^{|k|}}$. On vérifie que λ est continue à décroissance rapide et que $\sum_{k\in\mathbb{Z}} \lambda(x + 2k\pi) = 1$ pour tout $x \in \mathbb{R}$. On en déduit que, si $g \in P$, alors $F(\lambda g) = g$. Le morphisme $F : N \to P$ est donc surjectif. Comme P est projectif, il existe un facteur direct du A-module N isomorphe à P.

4. On dit qu'un A-module M est *injectif* si la propriété suivante est vérifiée : si N et P sont des A-modules tels qu'il existe une suite exacte $0 \to M \to N \to P \to 0$, alors il existe un isomorphisme $N \cong M \oplus P$.

(a) Montrer qu'un A-module M est injectif si, et seulement si, pour tout idéal I de A, tout morphisme de A-modules $I \to M$ s'étend en un morphisme de A-modules $A \to M$.

Indications : Supposons M injectif. Soient I un idéal de A et $f : I \to M$ un morphisme de A-modules. On note $i : I \to A$ l'injection canonique. Soit $N = (M \oplus A)/\{(f(x), i(x)) | x \in I\}$. On considère les deux morphismes $g : A \to N, a \mapsto (0, a)$ et $h : M \to N, m \mapsto (-m, 0)$. On remarque que h est injective et que le diagramme suivant commute :

$$\begin{array}{ccc} A & \xrightarrow{g} & N \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle h} \\ I & \xrightarrow{f} & M. \end{array}$$

Comme h est injective et M est un module injectif, il existe un morphisme de A-modules $t : N \to M$ tel que $t \circ h = \mathrm{Id}_M$. On remarque alors que, pour $x \in I$, on a $t(g(i(x))) = t(h(f(x))) = f(x)$. Donc $t \circ g : A \to M$ prolonge f.

Réciproquement, supposons que pour tout idéal I de A, tout morphisme de A-modules $I \to M$ s'étend en un morphisme de A-modules $A \to M$. Considérons une suite exacte de A-modules $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$. Soit $\mathcal{E}$ la famille des couples (N', t') où N' est un sous-module de N contenant M et t' est un morphisme $N' \to M$ vérifiant $t \circ f = Id$. On munit $\mathcal{E}$ de l'ordre suivant : $(N', t') \prec (N'', t'')$ si $N' \subseteq N''$ et $t''|_{N'} = t'$. La famille $\mathcal{E}$ est non vide, et l'ordre $\prec$ est inductif. Donc, d'après le lemme de Zorn, $\mathcal{E}$ possède un élément maximal (N_0, t_0). Supposons que $N_0 \neq N$. Soit $n \in N \setminus N_0$. Soit $N_1 = N_0 + An$. Soient $u : A \to N_1, a \mapsto an$ et $v : N_1 \to N_1/N_0$ la projection canonique. Soient $I = \mathrm{Ker}(v \circ u)$ et $w : I \to M, x \mapsto t_0(u(x))$. Par hypothèse, w s'étend en un morphisme $z : A \to M$. On vérifie alors que $t_1 : N_1 = N_0 + An \to M, n_0 + an \mapsto t_0(n_0) + z(a)$ (pour $n_0 \in N_0$ et $a \in A$) est un morphisme de A-modules bien défini tel que $t_1 \circ f = Id$: absurde par maximalité de (N_0, t_0) ! Donc $N_0 = N$, et la question 2. permet de conclure.

(b) Montrer que si A est un corps, alors tout A-module est injectif.

Indications : Dans ce cas, les idéaux de A sont (0) et A, et donc l'énoncé est évident.

(c) Est-ce que $\mathbb{Z}$ est un $\mathbb{Z}$-module injectif ? Pour $n > 0$, est-ce que $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}/n\mathbb{Z}$-module injectif ?

Indications : Le groupe abélien $\mathbb{Z}$ n'est pas injectif, puisque l'on a une suite exacte :

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0,$$

mais $\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
Montrons que $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}/n\mathbb{Z}$-module injectif. Soient I un idéal de $\mathbb{Z}/n\mathbb{Z}$ et $f : I \to \mathbb{Z}/n\mathbb{Z}$ un morphisme de $\mathbb{Z}/n\mathbb{Z}$-modules. Il existe $m|n$ et $k \in \mathbb{Z}$ tels que $I = m\mathbb{Z}/n\mathbb{Z}$ et $f(\overline{m}) = k\overline{m}$. Soit $\tilde{f} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme qui envoie $\overline{1}$ sur $\overline{k}$. On remarque alors que $\tilde{f}|_I = f$. Cela montre que $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}/n\mathbb{Z}$-module injectif.

On se place maintenant dans le cas $A = \mathbb{Z}$.

(d) Montrer qu'un groupe abélien M est injectif si, et seulement si, il est divisible, c'est-à-dire que pour tout $m \in M$ et tout $n \in \mathbb{N}^*$, il existe $m' \in M$ tel que $m = nm'$.

Indications : Soit M un groupe abélien divisible. Soient I un idéal de $\mathbb{Z}$ et $f : I \to M$ un morphisme. Il existe $n \in \mathbb{N}$ et $m \in M$ tels que $I = (n)$ et $f(n) = m$. Comme M est divisible, il existe $m' \in M$ tel que $nm' = m$. Si l'on définit le morphisme $\tilde{f} : \mathbb{Z} \to M, 1 \mapsto m'$, on remarque que $\tilde{f}|_I = f$. Par conséquent M est injectif.
Réciproquement, soit M un groupe abélien injectif. Soient $n \in \mathbb{N}^*$ et $m \in M$. On définit $f : n\mathbb{Z} \to M, n \mapsto m$. Comme M est injectif, il existe $\tilde{f} : \mathbb{Z} \to M$ tel que $\tilde{f}|_{n\mathbb{Z}} = f$. On remarque que $nf(1) = m$, et donc M est divisible.

(e) Quels sont les groupes abéliens de type fini injectifs ?

Indications : D'après la question précédente et le théorème de classification des groupes abéliens de type fini, le seul groupe abélien de type fini injectif est la groupe trivial.

(f) Montrer que le groupe abélien $\mathbb{R}/\mathbb{Z}$ possède un facteur direct isomorphe à $\mathbb{R}/\mathbb{Q}$.

Indications : On a une suite exacte :

$$0 \to \mathbb{Q}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Q} \to 0.$$

Le groupe abélien $\mathbb{Q}/\mathbb{Z}$ est divisible, donc injectif. Par conséquent :

$$\mathbb{R}/\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Q}.$$

Exercice 19 : Le groupe $\mathbb{Z}^{\mathbb{N}}$ n'est pas abélien libre

On considère le groupe abélien $M = \mathbb{Z}^{\mathbb{N}}$. Le but de cet exercice est de montrer que M n'est pas abélien libre. On procède par l'absurde en supposant que M admet une base B. Pour $n \in \mathbb{N}$, on note e_n l'élément de M dont tous les termes sont nuls, sauf le n-ème qui vaut 1. On écrit alors e_n comme combinaison linéaire d'une partie finie B_n de B, et on note N le sous-groupe de M engendré par les éléments de $\bigcup_{n\in\mathbb{N}} B_n$.

1. Soit $S = \{(\epsilon_n n!)_{n\in\mathbb{N}} \mid \epsilon_n \in \{-1, 1\}\}$. Montrer qu'il existe $s \in S$ tel que $s \notin N$.

> **Indications :** Le groupe N est infini dénombrable alors que S ne l'est pas. Donc il existe $s \in S$ tel que $s \notin N$.

2. Montrer que, pour chaque $k \in \mathbb{N}^*$, il existe $y \in M/N$ tel que $\overline{s} = ky$.

> **Indications :** Notons $s = (\epsilon_n n!)_{n\in\mathbb{N}}$. Comme $e_0, ..., e_{k-1}$ sont dans N, on remarque que $\overline{s}$ coïncide avec la classe de $(\delta_n n!)_{n\in\mathbb{N}}$ où $\delta_n = 0$ si $n < k$ et $\delta_n = \epsilon_n$ sinon. On voit immédiatement que $(\delta_n n!)_{n\in\mathbb{N}}$ est multiple de k dans M, ce qui achève la preuve.

3. En déduire une contradiction.

> **Indications :** Le groupe abélien M/N est libre, mais possède un élément divisible non nul !

Exercice 20 (culturel) : Sous-groupes d'un groupe abélien libre

Dans cet exercice, nous allons montrer que tout sous-groupe d'un groupe abélien libre est abélien libre. Considérons donc A un groupe abélien libre, et soit X une base de A. Soit A_0 un sous-groupe de A. Soit $\mathcal{E}$ l'ensemble des triplets (Y, B, ϕ), où Y est une partie de X telle que $A_0 \cap A^{(Y)}$ est abélien libre, B est une base de $A_0 \cap A^{(Y)}$ et $\phi : B \to X$ une injection. Si (Y, B, ϕ) et (Y', B', ϕ') sont deux éléments de $\mathcal{E}$, on dira que $(Y, B, \phi) \preceq (Y', B', \phi')$ si $Y \subseteq Y'$, $B \subseteq B'$ et $\phi = \phi'|_B$. Cela définit une relation d'ordre sur $\mathcal{E}$.

1. Montrer que $\mathcal{E}$ possède un élément maximal pour $\preceq$.

2. En déduire que A_0 est abélien libre.

Nous allons maintenant appliquer ce résultat pour montrer que le groupe $\mathbb{Z}^{\mathbb{N}}$ n'est pas abélien libre par une méthode différente de celle de l'exercice 19. Pour chaque entier x, on note $v_2(x)$ la valuation 2-adique de x (avec la convention $v_2(0) = +\infty$).

3. Soit N le sous-groupe de $\mathbb{Z}^{\mathbb{N}}$ constitué des suites $(x_n)_{n\in\mathbb{N}}$ telles que $\lim\limits_{n\to+\infty} v_2(x_n) = +\infty$. Montrer que $N/2N$ est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension dénombrable.

4. En déduire que $\mathbb{Z}^{\mathbb{N}}$ n'est pas abélien libre.