Correction Algèbre - Modules I

Exercice 1.

Soit A un anneau commutatif non nul.

1. Soit $f : A^r \to A^r$ une application linéaire, de matrice P dans la base canonique. Montrer que f est surjective si, et seulement si, $\det(P)$ est inversible dans A, et que ceci est équivalent à f bijective.
2. Montrer que f est injective si, et seulement si, $\det P$ et non nul et n'est pas diviseur de zéro dans A.
   Indication : Si $\det(P) = a$ *est diviseur de zéro, on fixera* b *non nul dans* A *tel que* $ab = 0$*, et on considérera un mineur* m *de taille maximale* s *dans* P *tel que* $mb \neq 0$*; puis on construira un vecteur colonne non nul annulé par* P *à partir de mineurs de taille* s *de* P*.*
3. En déduire que si $s > r$, une application linéaire de A^s dans A^r n'est pas injective.
4. Montrer que si un A-module M est engendré par une famille de r éléments, alors toute famille comportant au moins $r+1$ éléments dans M est liée.
5. Soit I un idéal non principal de A. Montrer que I n'est pas un A-module libre. Montrer plus généralement qu'un idéal I d'un anneau A est un sous-module libre de A, si et seulement si, I est principal et engendré par un élément non diviseur de zéro de A.

Solution.

1. Supposons $\det P \in A^\times$. Alors l'identité de la comatrice $P\widetilde{P} = \widetilde{P}P = \det(P)I_r$ (où $\widetilde{P}$ est la transposée de la comatrice) donne que P est inversible, d'inverse $\det(P)^{-1}\widetilde{P}$. Si maintenant P est inversible, l'application f est bijective, donc en particulier surjective. Supposons enfin f surjective. Alors on construit une matrice Q telle que $PQ = I_r$ en prenant pour vecteurs colonnes de Q des vecteurs envoyés sur les vecteurs $e_1, e_2, \ldots, e_r$ de la base canonique. Alors $\det(P)\cdot\det(Q) = 1$, donc $\det(P)$ est inversible.
2. Supposons $\det(P)$ non diviseur de zéro. Soit X un vecteur colonne tel que $P \cdot X = 0$. Alors $(\widetilde{P}P)X = 0$, d'où $\det(P)\cdot X = 0$, ce qui implique que toutes les coordonnées de X sont nulles puisque $\det(P)$ n'est pas diviseur de zéro. Ainsi f est injective. Supposons réciproquement que $\det(P) = a$ vérifie $ab = 0$ avec b non nul dans A, et montrons que f n'est pas injectif. Si tous les coefficients p_{ij} de P vérifient $p_{ij} \cdot b = 0$, il est clair que f n'est pas injective, puisque P annule par exemple le vecteur $(b, b, \ldots, b)$. Sinon, on peut choisir un mineur m de taille maximale tel que $mb \neq 0$, et ce mineur est de taille $s < r$ vu que $\det(P)\cdot b = 0$. Supposons (pour simplifier les notations) que ce soit le mineur correspondant aux s premières lignes et aux s premières colonnes de P. Soit X le vecteur $(x_1, \ldots, x_s, x_{s+1}, 0, \ldots, 0)$ avec $x_i = b(-1)^i m_i$, où $m_{s+1} = m$ et pour $1 \leqslant i \leqslant s$, m_i est le mineur (s, s) obtenu en gardant les s premières lignes et les $s+1$ premières colonnes à l'exception de la i-ième. Alors $X \neq 0$ car $x_{s+1} \neq 0$ vu que $bm \neq 0$; mais les coordonnées y_i de PX sont toutes nulles : en effet, la formule de développement du déterminant par rapport à une ligne donne qu'elles sont obtenues soit (pour les s premières) comme le produit de b par un déterminant de taille $s+1$ ayant deux lignes égales, soit (pour les suivantes) comme le produit de b par un mineur de taille $s+1$ de P, produit qui est nul par hypothèse. Donc f n'est pas injective.
3. Soit j l'injection linéaire de A^r dans A^s qui envoie $(x_1, \ldots, x_r)$ sur $(x_1, \ldots, x_r, 0, \ldots, 0)$. Si $g : A^s \to A^r$ était linéaire injective, il en irait de même de $f := j \circ g : A^s \to A^s$. Mais la matrice de f dans la base canonique a ses $(s-r)$ dernières lignes nulles, donc son déterminant est nul, donc d'après **2.** l'application linéaire g ne peut pas être injective.
4. Un A-module M engendré par r éléments est un quotient de A^r, et il suffit donc de montrer qu'une famille $(x_1, \ldots, x_s)$ de s éléments avec $s > r$ est liée dans A^r. Ceci résulte de **3.**, vu que l'application linéaire de A^s dans A^r qui envoie $(\alpha_1, \ldots, \alpha_s)$ sur $\sum_{i=1}^{s} \alpha_i x_i$ ne peut pas être injective.
5. Il résulte de **4.** que si M est un A-module libre de type fini r, un sous-module libre de M est forcément de rang au plus r. En particulier, un idéal non principal d'un anneau commutatif non nul A ne peut pas être un A-module libre puisque A lui-même est un module libre de rang 1.
   On rappelle que les idéaux de A sont exactement les sous-A-modules de A. Si I est un idéal principal de A engendré par un élément a qui n'est pas un diviseur de 0, alors I est un module libre car a est une famille génératrice et libre de I. Réciproquement, soit $I \subseteq A$ un idéal qui soit un sous-module libre de A. Soit $(a_j)_{j\in J}$ une base de I en tant que A-module.

Comme I est non nul, on a que J est non vide. Supposons que J a au moins deux éléments et soient $a_j \neq a_k$ deux éléments distincts. On a alors

$$a_j \cdot a_k - a_k \cdot a_j = 0$$

et par liberté, cela implique que $a_j = 0$ et $a_k = 0$, ce qui est absurde car ils constituent une famille libre. Ainsi J a un seul élément, disons a. Comme a est une famille libre, a est sans torsion donc a n'est pas un diviseur de 0 et comme $\{a\}$ est génératrice, on a bien que $I = (a)$ est principal.

Exercice 2 — Exemples et contre-exemples. Soit A un anneau commutatif non nul. On suppose que A n'est pas un corps. Donner des exemples :

1. de A-modules non libres et montrer que si tout A-module est libre alors A est un corps ;
2. D'une famille libre à n éléments dans A^n qui n'est pas une base ;
3. D'une partie génératrice minimale qui ne soit pas une base ;
4. De sous-modules n'ayant pas de supplémentaire ;
5. De module libre ayant un sous-module qui n'est pas libre.
6. Soit A un anneau intègre et K son corps de fractions. On suppose que $K \neq A$ (*i.e.* A n'est pas un corps). Montrer que K n'est pas libre comme A-module.

Solution.

1. Par exemple $\mathbf{Z}/n\mathbf{Z}$ pour $n \in \mathbf{N}^\times$ n'est pas un $\mathbf{Z}$-module libre car tout module libre est sans torsion ou encore $\mathbf{Q}$ car divisible. De manière plus générale, si I est un idéal propre non nul[1], alors A/I n'est pas libre pour les mêmes raisons que $\mathbf{Z}/n\mathbf{Z}$ car tous ses éléments sont de torsion et si[2] $A \neq \mathrm{Frac}(A)$, alors le A-module $\mathrm{Frac}(A)$ n'est pas libre. En effet, pour deux éléments $x = \frac{a}{b}$ et $y = \frac{c}{d}$ avec a, b, c, d des éléments de A et $cd \neq 0$, on a $bcx = ac = ady$ et donc on voit que si a ou c est non nul, la famille (x, y) est liée. Mais si $a = c = 0$, alors $x = y = 0$ et le résultat persiste. Une famille libre a donc au plus un élément et comme $\mathrm{Frac}(A) \neq 0$, une famille génératrice a au moins un élément. Si $\mathrm{Frac}(A)$ était libre, une base de $\mathrm{Frac}(A)$ aurait un élément mais pour tout $x \in \mathrm{Frac}(A)$ non nul, $\mathrm{Frac}(A)$ n'est pas engendré par x en tant que A-module car sinon $x^2 \in Ax$ donc $x \in A$ et $Ax = \mathrm{Frac}(A) \subseteq A$ ce qui est exclu. Pour finir, on a vu que si A n'est pas un corps, il existe des A-modules non libres. Réciproquement, si tout A-module est libre, soit I un idéal de A non nul. On a alors pour tout $\overline{a} \in A/I$ et tout $i \in I \setminus \{0\}$ que $i \cdot \overline{a} = 0$ si bien que $\overline{a}$ n'est pas libre. Ainsi, A/I doit être égal à $\{0\}$ et $I = A$. Les seuls idéaux de A sont donc I et $\{0\}$ ce qui implique que A est un corps d'après le TD III ;
2. Pour $A = \mathbf{Z}$ et $n = 1$, il est clair que 2 est une famille libre mais non génératrice. Plus généralement, pour n éléments $m_i = (d_{ij})$ de A^n, alors ils forment une famille libre (voir[3] l'exercice 1) si, et seulement si, $\det(d_{ij})$ n'est pas un diviseur de 0 et génératrice si, et seulement si, $\det(d_{ij}) \in A^\times$. On en déduit des exemples d'applications linéaires injectives $A^n \to A^n$ qui ne sont pas des isomorphismes !
3. Par exemple, avec $A = \mathbf{Z}$ et $M = \mathbf{Z}/2\mathbf{Z}$, alors $\overline{1}$ est génératrice minimale mais non libre (car c'est un élément de torsion) ;
4. À nouveau, on considère $A = \mathbf{Z}$, $M = A$ et le sous-A-module de M donné par $N = 2\mathbf{Z}$. Ce dernier n'a pas de supplémentaire. En effet, soient P un sous-module de M tel que $P \cap N = \{0\}$ et $p \in P$. Alors $2p \in P \cap N$ donc $2p = 0$ ce qui implique que $P = \{0\}$ mais $N \oplus \{0\} \neq M$.
5. On considère $A = \mathbf{Z}/4\mathbf{Z}$ et $M = A$ qui est donc libre en tant que A-module. Soit alors $N = 2\mathbf{Z}/4\mathbf{Z}$ le sous-module engendré par la classe de 2. Le sous-A-module N de M n'est pas libre car sinon il serait isomorphe à A^k pour un certain entier k et donc de cardinal $4k$. Or, il est de cardinal 2. La question **7.** fournit des contre-exemples plus généraux comme par exemple $A = k[X, Y]$ avec k un corps qui est libre sur lui-même tandis que (X, Y) n'est pas libre.
6. Voir la question **1.**

1. Ce qui est possible lorsque A n'est pas un corps.
2. Là encore, ce qui est le cas si A n'est pas un corps.
3. Car une famille $(e_1, \ldots, e_r)$ de A^n est libre si, et seulement si,

$$\begin{array}{ccc} A^r & \longrightarrow & A^n \\ (\lambda_1, \ldots, \lambda_r) & \longmapsto & \displaystyle\sum_{i=1}^{r} \lambda_i e_i \end{array}$$

est injective et génératrice si, et seulement si, cette application est surjective.

Exercice 3 — Modules projectifs. Soit P un A-module. Montrer que les propriétés suivantes sont équivalentes :

a) pour tout morphisme surjectif de A-module $g : E \to F$ et pour tout $f \in \mathrm{Hom}_A(P, F)$, il existe $h \in \mathrm{Hom}_A(P, E)$ tel que $f = g \circ h$;

b) pour tout morphisme surjectif $\pi : M \to P$, il existe un morphisme $s : P \to M$ tel que $\pi \circ s = \mathrm{Id}_P$ (un tel morphisme s est appelé une section de π);

c) Il existe un A-module M tel que $M \oplus P$ est libre.

Un A-module P vérifiant ces propriétés est appelé *module projectif*. Montrer qu'un A-module libre est projectif et donner un exemple de $\mathbf{Z}$-module qui n'est pas projectif.

Solution. Pour obtenir l'implication a) $\Rightarrow$ b), il suffit de prendre $g = \pi$ et $f = \mathrm{Id}_P$ dans a).
Passons alors à l'implication b) $\Rightarrow$ c). Soit $(x_i)_{i\in I}$ une famille génératrice de P. Cela fournit un morphisme surjectif $\pi : A^{(I)} \to P$. Par b), il existe alors une section $s : P \to A^{(I)}$ telle que $\pi \circ s = \mathrm{Id}_P$. Si $s(x) = 0$, alors $x = \pi \circ s(x) = 0$ et donc s est injective, ce qui permet d'identifier P avec son image dans $A^{(I)}$. Montrons alors que $A^{(I)} = s(P) \oplus \mathrm{Ker}(\pi)$. Soit $x \in s(P) \cap \mathrm{Ker}(\pi)$, alors $x = s(y)$ pour $y \in P$ et $y = \pi \circ s(y) = \pi(x) = 0$ donc $s(P) \cap \mathrm{Ker}(\pi) = \{0\}$. Si maintenant $x \in A^{(I)}$, alors $z = s(\pi(x)) \in s(P)$ et $\pi(x - z) = \pi(x) - \pi \circ s(\pi(x)) = 0$ si bien que $x = z + (x - z) \in s(P) + \mathrm{Ker}(\pi)$ et qu'on a bien $A^{(I)} = s(P) \oplus \mathrm{Ker}(\pi)$. On a ainsi établi c).
Terminons par l'implication c) $\Rightarrow$ a). Supposons donnés M et I tels que $P \oplus M \cong A^{(I)}$ et notons $(e_i)_{i\in I}$ la base canonique de $A^{(I)}$ ainsi que $s : P \to A^{(I)}$ l'injection canonique et $\pi : A^{(I)} \to P$ la projection. Noter qu'on a alors $\pi \circ s = \mathrm{Id}_P$. Soient alors g et f comme dans a) et a_i une préimage de $f(\pi(e_i))$ par g pour tout $i \in I$. Alors il existe un unique morphisme $\varphi : A^{(I)} \to E$ tel que $\varphi(e_i) = a_i$ pour tout $i \in I$ par propriété universelle des modules libres. Comme $g \circ \varphi$ et $f \circ \pi$ coïncident sur les e_i pour tout $i \in I$. Ainsi $g \circ \varphi = f \circ \pi$. On a alors, en posant $h = \varphi \circ s$, que $g \circ h = g \circ \varphi \circ s = f \circ \pi \circ s = f$ et on a donc a) et établi l'équivalence des trois propriétés.
Il est alors facile de construire des modules projectifs, en prenant tout facteur direct d'un module libre. En particulier, tout module libre est immédiatement projectif par la caractérisation c).

Remarque : On a les propriétés suivantes : si A est principal, alors tout $A[X_1, \ldots, X_n]$-module projectif de type fini est libre[4]. Cette propriété reste également vraie si A est un anneau de Bézout commutatif ou de valuation discrète. On a également que sur un anneau local, tout module projectif est libre mais ces résultats sont hors de portée de ce cours[5] ! Le cours fournit en revanche le résultat sur un anneau principal[6]. Sur un anneau intègre en général, le résultat est faux. En effet, pour $A = \mathbf{Z}[i\sqrt{5}]$, un idéal non principal ne peut pas être libre (voir l'exercice mais il s'agit d'un A-module projectif (difficile). Enfin en prévision du DM II, tout module projectif est plat. La réciproque est fausse, mais tout module plat de présentation finie est projectif.

Reste à donner un exemple de $\mathbf{Z}$-module non projectif. À la lumière de ce qui précède, on sait en effet que sur un anneau principal, projectif est équivalent à libre. Il suffit alors de prendre un module non libre. On est seulement en mesure de déduire cela du cours pour un module de type fini à l'aide du[7] Théorème 4.1 du cours. En particulier, un $\mathbf{Z}/n\mathbf{Z}$ convient. Mais le résultat plus profond de Kaplansky fournit que le résultat vaut même sans cette hypothèse de type fini et en réalité on a bien que le $\mathbf{Z}$-module $\mathbf{Q}$ n'est pas projectif non plus. Pour le voir, on peut établir que $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Q}, \mathbf{Z}) = \{0\}$ car l'image d'un tel morphisme est un sous-module de $\mathbf{Z}$ divisible, autrement dit nécessairement $\{0\}$. On conclut alors en raisonnant par l'absurde. Si $\mathbf{Q}$ était projectif, il serait facteur direct d'un $\mathbf{Z}^{(I)}$ et on aurait donc une injection canonique $\iota : \mathbf{Q} \to \mathbf{Z}^{(I)}$. Mais, puisque $\mathbf{Z}^{(I)} \cong \bigoplus_{i\in I} \mathbf{Z}$, pour tout $i \in I$, on a une projection $\pi_i : \mathbf{Z}^{(I)} \to \mathbf{Z}$ telle que $\pi_i \circ \iota \in \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Q}, \mathbf{Z})$. Autrement dit, toutes ces projections sont nulles, ce qui revient à dire que ι est l'application nulle, contredisant son injectivité !

Exercice 4. Soit A un anneau, M un A-module de type fini et $\phi : M \to A^n$ un morphisme surjectif de A-modules.

1. Montrer que ϕ admet un inverse à droite ψ (*i.e.* il existe $\psi : A^n \to M$ tel que $\phi \circ \psi = id_{A^n}$).

2. Montrer que $M \simeq \mathrm{Ker}\phi \oplus \mathrm{Im}\psi$.

3. Montrer que $\mathrm{Ker}\phi$ est de type fini.

4. Il s'agit du *théorème de Quillen-Suslin*.

5. Il proviennent des articles de recherche *Projective modules over polynomial rings* publié par Daniel Quillen à Inventiones Mathematicae en 1976 et *Projective modules* publié par Irving Kaplansky à Annals of Mathematics en 1958

6. Où l'article de Kaplansky permet également (mais c'est difficile) de s'affranchir de l'hypothèse de type fini.

7. On a vu que libre implique projectif et par c), projectif implique sous-module d'un module libre sur un anneau principal.

Solution.

1. Soit $(e_1, \dots, e_n)$ la base canonique de A^n. Par surjectivité, il existe pour tout $i \in \{1, \dots, n\}$, un élément $m_i \in M$ tel que $\varphi(m_i) = e_i$. On peut alors définir un (unique) morphisme de A-modules $\psi : A^n \to M$ par $\psi(e_i) = m_i$ pour tout $i \in \{1, \dots, n\}$. Cela est possible grâce à la propriété universelle des modules libres et que A^n est libre. On a alors clairement que $\varphi \circ \psi(e_i) = e_i$ si bien que $\varphi \circ \psi = \mathrm{Id}_{A^n}$, autrement dit un inverse à droite.
2. On vérifie que le morphisme de A-modules $\theta : \mathrm{Ker}(\varphi) \oplus \mathrm{Im}(\psi) \to M$ défini par $\theta(m + e') = m + \psi(e)$ pour tous $m \in \mathrm{Ker}(\varphi)$ et $e \in \mathrm{Im}(\psi)$ est un isomorphisme. Supposons donnés $m \in \mathrm{Ker}(\varphi)$ et $e' = \psi(e) \in \mathrm{Im}(\psi)$ avec $e \in A^n$ tels que $\theta(m + e') = m + \psi(e) = 0$. En appliquant φ, il vient $\varphi(\psi(e)) = 0$ mais $\varphi(\psi(e)) = e$ si bien que $e = 0$ et par suite, $e' = \psi(e) = 0$ et $m = 0$. L'application est donc injective. Pour la surjectivité, on prend $m \in M$ et on pose $m_0 = m - \psi(\varphi(m))$. On a alors par un simple calcul que
$$\varphi(m_0) = \varphi(m) - \varphi(\psi(\varphi(m))) = \varphi(m) - \varphi(m) = 0$$
de sorte que $m_0 \in \mathrm{Ker}(\varphi)$. On a alors clairement que $m = \theta(m_0 + \psi(\varphi(m)))$ ce qui établit ma surjectivité et le résultat [8].
3. Puisque M est de type fini, on peut trouver un entier naturel k et des générateurs $(f_i)_{1 \leqslant i \leqslant k}$ de M. On écrit alors pour tout $i \in \{1, \dots, k\}$, $f_i = \theta(m_i + \psi(v_i))$ pour un certain $m_i \in \mathrm{Ker}(\varphi)$ et $v_i \in A^n$. Montrons alors que les m_i avec $i \in \{1, \dots, k\}$ engendrent $\mathrm{Ker}(\varphi)$. En effet, soit $m \in \mathrm{Ker}(\varphi)$, comme les $(f_i)_{1 \leqslant i \leqslant k}$ engendrent M, on peut écrire
$$m = \sum_{i=1}^{k} a_i f_i = \sum_{i=1}^{k} a_I(m_i + \psi(v_i)) = \sum_{i=1}^{k} a_i m_i + \psi\left(\sum_{i=1}^{k} a_i v_i\right) = \theta\left(\sum_{i=1}^{k} a_i m_i + \sum_{i=1}^{k} a_i v_i\right)$$
pour $a_1, \dots, a_k \in A$. Par ailleurs, on a vu en question précédente que $m = \theta(m_0 + \psi(\varphi(m))) = \theta(m + 0)$ car $m \in \mathrm{Ker}(\varphi)$. Par injectivité de θ, il vient que $m = \sum_{i=1}^{k} a_i m_i$, ce qui conclut la démonstration.
On pouvait bien évidemment aussi conclure en remarquant que **2.** implique que $\mathrm{Ker}(\varphi) \cong M/\mathrm{Im}(\psi)$ et qu'un quotient d'un module de type fini est toujours de type fini.

Exercice 5 — Lemme de Nakayama. Cet exercice est en lien avec les exercices 11 et 12 de la feuille de TD III sur les anneaux.

1. Soit M un A-module de type fini et I un idéal de A. Supposons $M = IM$. Montrer qu'il existe alors $a \in I$ tel que $(1 + a)M = 0$. *Indication : Choisir $1 + a$ déterminant d'une matrice.*
2. En déduire que si A est local, $I = \mathcal{M}$ son idéal maximal et $M = IM$ alors $M = 0$.
3. Soit $\mathcal{R}$ le radical de Jacobson de A (*i.e.* l'intersection de de tous ses idéaux maximaux). Montrer que si $\mathcal{R}M = M$, alors $M = 0$.
4. Soit A un anneau et I un idéal de type fini de A tel que $I^2 = I$. Montrer qu'il existe $e \in A$ tel que $e^2 = e$ et $I = (e)$. On appelle un tel élément un *idempotent* de A.

Solution.

1. On rappelle que IM est le sous-module engendré par les im avec $i \in I$ et $m \in M$. On considère $m_1, \dots, m_n$ des générateurs de M avec $n \in \mathbf{N}^\times$. Comme $M = IM$, pour tout $i \in \{1, \dots, n\}$, il existe $b_{i1}, \dots, b_{in} \in I$ tels que $m_i = \sum_{j=1} n b_{ij} m_j$. Notons alors B la matrice $(b_{ij})_{1 \leqslant i,j \leqslant n}$. On a alors immédiatement que $(I_n - B)X = 0$ avec $X = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$. Or, $\det(I_n - B) = \widetilde{(I_n - B)}(I_n - B)$ si bien que pour tout $i \in \{1, \dots, n\}$, $\det(I_n - B)m_i = 0$ et par conséquent $\det(I_n - B)m = 0$ pour tout $m \in M$. Mais développant ce déterminant, on voit immédiatement [9] qu'il est de la forme $1 + a$ avec $a \in I$.
2. Dans ce cas, on a que pour tout $a \in \mathfrak{M}$, $1 + a \in A^\times$ (par exemple car $1 + a \notin \mathfrak{M}$ et qu'on a vu dans le TD III que ces éléments sont non inversibles [10]). Ainsi, par **1.**, il existe $a \in \mathfrak{M}$ tel que $(1 + a)M = 0$ qui implique que $M = 0$.

8. Le fait d'avoir un morphisme étant évident.

9. Ou on remarque qu'il s'agit du polynôme caractéristique évalué en 1 et on a le résultat comme B est à coefficients dans I ce qui implique que tous les coefficients sont dans I mis à part le coefficient dominant qui vaut 1.

10. Ou directement, si cet élément n'est pas inversible, alors l'idéal $(1 + a)$ est un idéal propre contenu dans un idéal maximal. Comme il n'y en a qu'un, on en déduit que $(1 + a) \subseteq \mathfrak{M}$ et donc $1 + a \in \mathfrak{M}$, ce qui est absurde car cela implique que $1 \in \mathfrak{M}$.

3. Par **1.**, on a de même $a \in \mathfrak{R}$ tel que $(1+a)M = 0$. Il suffit donc de montrer que $1+a$ est inversible pour conclure. Si ce n'est pas le cas, alors l'idéal engendré par $1+a$ est inclus dans un idéal maximal $\mathfrak{M}$. Mais par définition $a \in \mathfrak{M}$ si bien que $1 \in \mathfrak{M}$, ce qui est absurde.

4. On a $I \cdot I = I$ et I est un A-module de type fini donc par le lemme de Nakayama (question **1.**), il existe $a \in I$ tel que $(1+a)I = 0$. Posons alors $e = -a$. On a $e \in I$ et donc $(1+a)e = (1-e)e = 0$ soit $e^2 = e$. Reste à établir que $I \subseteq (e)$. Soit $x \in I$. On a $(1-e)x = 0$ soit $x = ex \in (e)$, ce qui permet de conclure !

Exercice 6. Soit k un corps, $P \in k[X]$ et $A = k[X]/(P)$.

1. Quelle est la dimension de A comme k-espace vectoriel ? Donnez-en une base.

2. On pose $M = \mathrm{Hom}_k(A, k)$; donner une base de M.

3. Pour $f \in A$ et $u \in M$, on définit $f \cdot u \in M$ par $(f \cdot u)(g) = u(f \cdot g)$ pour tout $g \in A$. Montrer que cette loi munit M d'une structure de A-module libre de rang 1. Donnez-en une base.

Solution.

1. La dimension est clairement $d = \deg(P)$ et une base $\overline{1}, \overline{X}, \ldots, \overline{X}^{d-1}$. On a clairement une structure de k-espace vectoriel et on obtient le caractère générateur grâce à une division euclidienne par P et la liberté à la main (on aurait un polynôme de degré strictement inférieur dans le noyau de la surjection canonique, soit dans (P), ce qui est impossible).

2. La base duale est alors donnée par $u_0, \ldots, u_{d-1}$ où pour tout $i, j \in \{0, \ldots, d-1\}$, on a $u_i\left(\overline{X}^j\right) = \delta_{i,j}$ où $\delta_{i,j}$ dénote le symbole de Kronecker. Noter ici qu'on considère une base en tant que k-espace vectoriel.

3. Il est clair que cela définit une structure de A-module. On peut supposer sans perte de généralité (puisque k est un corps), que P est unitaire et donné par $P = X^d - a_{d-1}X^{d-1} - \cdots - a_0$ avec $a_0, \ldots, a_{d-1} \in k$. Montrons alors que u_{d-1} est une base de M comme A-module, ce qui permettra de conclure. Calculons les $\overline{X}^j \cdot u_{d-1}$ pour tout $j \in \{0, \ldots, d-1\}$. On a pour tout $\lambda_0, \ldots, \lambda_{d-1} \in k$

$$1 \cdot u_{d-1}\left(\sum_{i=0}^{d-1} \lambda_i \overline{X}^i\right) = u_{d-1}\left(\sum_{i=0}^{d-1} \lambda_i \overline{X}^i\right) = \lambda_{d-1}$$

puis

$$\begin{aligned}\overline{X} \cdot u_{d-1}\left(\sum_{i=0}^{d-1} \lambda_i \overline{X}^i\right) &= u_{d-1}\left(\sum_{i=0}^{d-1} \lambda_i \overline{X}^{i+1}\right) \\ &= u_{d-1}\left(\sum_{i=1}^{d-1} \lambda_{i-1} \overline{X}^i + \lambda_{d-1}\overline{X}^d\right) = u_{d-1}\left(\sum_{i=1}^{d-1} \lambda_{i-1}\overline{X}^i + \lambda_{d-1}\left(a_{d-1}X^{d-1} + \cdots + a_0\right)\right) = \lambda_{d-2} + \lambda_{d-1}a_{d-1}.\end{aligned}$$

Par récurrence, on voit que $\overline{X}^k \cdot u_{d-1}\left(\sum_{i=0}^{d-1} \lambda_i \overline{X}^i\right)$ est de la forme λ_{d-k} plus une combinaison linéaire de $\lambda_{d-k+1}, \ldots, \lambda_{d-1}$ à coefficients dans k. On en déduit que la matrice de $\left(u_{d-1}, \overline{X} \cdot u_{d-1}, \ldots, \overline{X}^{d-1} \cdot u_{d-1}\right)$ dans la base $(u_{d-1}, \ldots, u_1, u_0)$ est triangulaire supérieure avec des 1 sur la diagonale. Elle est donc inversible si bien que tout élément de M s'écrit de manière unique comme combinaison linéaire de $u_{d-1}, \overline{X} \cdot u_{d-1}, \ldots, \overline{X}^{d-1} \cdot u_{d-1}$. Autrement dit, pour tout $u \in M$, il existe un unique $\overline{Q} \in A$ tel que $u = \overline{Q} \cdot u_{d-1}$ et ainsi u_{d-1} est bien une base de M comme A-module.

Exercice 7. Soit

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\pi} M'' \longrightarrow 0$$

une suite exacte de A-modules. Montrer que les propriétés suivantes sont équivalentes :

(i) Il existe $r \in \mathrm{Hom}_A(M, M')$ tel que $r \circ i = \mathrm{Id}_{M'}$;

(ii) Il existe $s \in \mathrm{Hom}_A(M'', M)$ tel que $\pi \circ s = \mathrm{Id}_{M''}$;

(iii) Il existe $s \in \mathrm{Hom}_A(M'', M)$ tel que $M = i(M') \oplus s(M'')$;

(iv) La suite suivante est exacte pour tout A-module N

$$0 \longrightarrow \mathrm{Hom}_A(N, M') \xrightarrow{i_*} \mathrm{Hom}_A(N, M) \xrightarrow{\pi_*} \mathrm{Hom}_A(M, M'') \longrightarrow 0\,;$$

(v) La suite suivante est exacte pour tout A-module N

$$0 \longrightarrow \mathrm{Hom}_A(M'', N) \xrightarrow{\pi^*} \mathrm{Hom}_A(M, N) \xrightarrow{i_*} \mathrm{Hom}_A(M', N) \longrightarrow 0\,.$$

Une suite vérifiant ces propriétés s'appelle une *suite scindée*.

SOLUTION.

Montrons dans un premier temps que (i) $\Rightarrow$ (ii). On pose $\sigma = \mathrm{Id}_M - i \circ r$. Si $m = i(m')$ pour $m' \in M'$, alors $\sigma(m) = m - i(r(i(m'))) = m - i(m') = 0$ si bien que σ passe au quotient par $i(M') = \mathrm{Ker}(\pi) \cong M'$ pour fournir un morphisme [11] $s : M/i(M') = M/\mathrm{Ker}(\pi) \cong M'' \to M$. De plus, si $m'' \in M''$, par surjectivité, il existe $m \in M$ tel que $m'' = \pi(m)$ et $\pi \circ s(m'') = \pi(\sigma(m)) = \pi(m - i(r(m))) = \pi(m) - \pi \circ i(r(m)) = \pi(m) = m''$ si bien qu'on a bien $\pi \circ s = \mathrm{Id}_{M''}$.

Passons alors à l'implication (ii) $\Rightarrow$ (iii). L'application s est clairement injective donc l'application $i(M') \cap s(M'') = \{0\}$. En effet, soit $m \in i(M') \cap s(M'')$. Il existe alors $m' \in M'$ et $m'' \in M''$ tels que $m = i(m') = s(m'')$. En prenant l'image par π, il vient d'une part $\pi(m) = \pi(s(m'')) = m''$ et d'autre part $\pi(m) = \pi(i(m')) = 0$ si bien que $m'' = 0$ et finalement $i(m') = 0$ et $m' = 0$ donc $m = 0$. Soit alors $m \in M$, alors $m - s(\pi(m))$ est dans $\mathrm{Ker}(\pi) = i(M')$ et $m = i(m - s(\pi(m))) + s(\pi(m)) \in i(M') + s(M'')$ et $m \in i(M') + s(M'')$, ce qui établit bien que $M = i(M') \oplus s(M'')$.

Passons alors à l'implication (iii) $\Rightarrow$ (i). On constate que pour tout $m \in M$, $m - s(\pi(m)) \in i(M')$ donc il existe $r(m) \in M'$ tel que $i(r(m)) = m - s(\pi(m))$. Comme i est injective, $r(m)$ est unique et l'application $r : m \mapsto r(m)$ est bien définie et un homomorphisme de M dans M'. Il vérifie $i(r(i(m'))) = i(m') - s(\pi(i(m'))) = i(m')$ si bien que pour tout $m' \in M'$, on a $r(i(m')) = m'$ soit $r \circ i = \mathrm{Id}_{M'}$. On a donc obtenu l'équivalence de (i), (ii) et (iii).

Établissons alors l'implication (ii) $\Rightarrow$ (iv). L'injectivité de i_* est immédiate. En effet, i_* est donnée par $f \mapsto i \circ f$. Soit alors f dans le noyau de i_*, on a alors $i \circ f = 0$ et par injectivité de i, cela implique immédiatement $f = 0$. De même, il est clair que $\mathrm{Ker}(\pi_*) = \mathrm{Im}(i_*)$. Soit $f \in \mathrm{Ker}(\pi_*)$. On a alors $\pi \circ f = 0$. Ainsi pour tout $x \in N$, on a $\pi(f(x)) = 0$ donc $f(x) \in \mathrm{Ker}(\pi) = \mathrm{Im}(i)$ et il existe $m_x \in M'$ tel que $f(x) = i(m_x)$. Par injectivité de i, ce m_x est unique. On pose alors $g : N \to M'$ définie par $g(x) = m_x$ (par injectivité, cette application est bien définie et un morphisme [12]). On a alors $f = i \circ g$ soit $f \in \mathrm{Im}(i_*)$. Réciproquement, si $f \in \mathrm{Im}(i_*)$, alors il existe g telle que $f = i \circ g$. Ainsi, pour tout $x \in N$, $\pi(f(x)) = \pi(i(g(x))) = 0$ et on a l'inclusion réciproque. Noter qu'on n'a pas encore utilisé l'hypothèse (ii). Reste donc à voir la surjectivité de π_*. Soit $\varphi \in \mathrm{Hom}_A(N, M'')$. On a $\pi_*(s \circ \varphi) = \pi \circ s \circ \varphi = \varphi$ ce qui permet de conclure.

Réciproquement, montrons que (iv) $\Rightarrow$ (ii). Il suffit pour ce faire d'appliquer l'hypothèse à $N = M''$ et $\varphi = \mathrm{Id}_{M''}$. La surejctivité de π_* fournit alors l'existence d'un morphisme $\psi : M'' \to M$ tel que $\psi \circ \pi = \mathrm{Id}_{M''}$.

Passons alors à l'implication (i) $\Rightarrow$ (v). L'application π^* est donnée par $f \mapsto f \circ \pi$. Montrons alors que cette application est injective. Soit f telle que $df \circ \pi = 0$. Pour tout $x \in M''$, il existe par surjectivité de π un $m \in M$ tel que $x = \pi(m)$ et donc $f(x) = f(\pi(m)) = 0$ si bien que $f = 0$. Établissons alors que $\mathrm{Ker}(i^*) = \mathrm{Im}(\pi^*)$. Soit $f \in \mathrm{Ker}(i_*)$. On a alors $f \circ i = 0$. On a donc $\mathrm{Im}(i) = \mathrm{Ker}(\pi) \subseteq \mathrm{Ker}(f)$. Il s'ensuit que $f : M \to N$ passe au quotient modulo $i(M')$ pour donner une application $g : M'' \cong M/i(M') \to N$ vérifiant $f = g \circ \pi$ et finalement $f \in \mathrm{Im}(\pi^*)$. Réciproquement, si $f \in \mathrm{Im}(\pi^*)$, alors il existe g tel que $f = g \circ \pi$ et il est immédiat de voir que $f \circ i = 0$ car $\pi \circ i = 0$. Finalement, reste à établir la surjectivité [13] de i^*. Soit $\varphi : M' \to M$. On a alors $\varphi = \varphi \circ (r \circ i) = (\varphi \circ r) \circ i = i^*(\varphi \circ r)$, ce qui permet de conclure. Enfin, pour la réciproque (v) $\Rightarrow$ (i), il suffit de prendre $N = M'$ et $\varphi = \mathrm{Id}_{M'}$. La surjectivité [14] de i^*, il vient $\psi : M \to M'$ tel que $i^*(\psi) = \psi \circ i = \mathrm{Id}_{M'}$.

REMARQUE : Noter que cette propriété est fausse pour les groupes en général. En effet, une extension de groupe est scindée à droite (propriété (ii)) si, et seulement si, c'est un produit semi-direct et est scindée à gauche (propriété (i)) si, et seulement si, c'est un produit direct. `https://kconrad.math.uconn.edu/blurbs/grouptheory/splittinggp.pdf` En revanche, le résultat est vrai pour les groupes abéliens et plus généralement dans toute catégorie abélienne.

11. De manière plus précise, on obtient par factorisation un morphisme $\tilde{s} : M/i(M') = M/\mathrm{Ker}(\pi) \to M$ tel que $\tilde{s}(\overline{m}) = \sigma(m)$ pour tout $m \in M$ avec $\overline{m}$ désignant la classe de m dans le quotient $M/i(M')$. Par ailleurs, on a un isomorphisme $\tilde{\pi} : M/i(M') \to M''$ provenant de la factorisation de π. On peut alors définir $s : M'' \to M$ par $s(m'') = \tilde{s}\left(\tilde{\pi}^{-1}(m'')\right)$ pour tout $m'' \in M''$. En d'autres termes, si $m'' = \pi(m)$, alors $s(m'') = \sigma(m)$.

12. Par exemple pour $n, n' \in N$, $f(n) = i(m_n)$ et $f(n') = i(m_{n'})$. On a alors $f(n + n') = f(n) + f(n') = i(m_n) + i(m_{n'}) = i(m_n + m_{n'})$ soit par unicité $m_{n+n'} = m_n + m_{n'}$.

13. Noter qu'à nouveau, on n'a encore pas fait appel à l'hypothèse.

14. Noter que cela ne peut provenir que de cette surjectivité, puisque toutes les autres propriétés d'exactitude sont automatiques !

Exercice 8 — Chasse au diagramme.

1. Soit A un anneau, et soit

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N \\ & & & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle w} \\ 0 & \longrightarrow & L' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' \end{array}$$

un diagramme de morphismes de A-modules tel que les deux lignes sont exactes et $g' \circ v = w \circ g$.
Montrer qu'il existe un unique morphisme $u : L \longrightarrow L'$ tel que $f' \circ u = v \circ f$. Si v est injective, montrer que u l'est aussi.

2. Soit A un anneau, et soit

$$\begin{array}{ccccccc} L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & & & \\ L' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' & \longrightarrow & 0 \end{array}$$

un diagramme de morphismes de A-modules tel que les deux lignes sont exactes et $f' \circ u = v \circ f$.
Montrer qu'il existe un unique morphisme $w : N \longrightarrow N'$ tel que $g' \circ v = w \circ g$. Si v est surjective, montrer que w l'est aussi.

Solution.

1. Un tel morphisme est nécessairement unique par injectivité de f'. Soit alors $\ell \in L$ et considérons $m' = v(f(\ell)) \in M'$. Montrons que $m' \in \mathrm{Im}(f') = \mathrm{Ker}(g')$. Calculons alors $g'(m') = w(g(f(\ell)))$. Mais $f(\ell) \in \mathrm{Im}(f) = \mathrm{Ker}(g')$ si bien que $g(f(\ell)) = 0$ et $g'(m') = 0$. On a donc bien que $m' \in \mathrm{Im}(f')$ et par conséquent, il existe un unique $\ell' \in L'$ tel que $m' = f'(\ell')$. On pose alors l'application bien définie $u : L \longrightarrow L'$ par $\ell \mapsto \ell'$. On a clairement $f' \circ u = v \circ f$ et il ne reste alors plus qu'à établir que u est un morphisme pour conclure. Soient alors $\lambda \in A$, $\ell_1, \ell_2 \in L$. On a alors $u(\ell_1) = \ell'_1$ et $u(\ell_2) = \ell'_2$ avec

$$f'(\lambda\ell'_1 + \ell'_2) = \lambda f(\ell'_1) + f(\ell'_2) = \lambda v(f(\ell_1)) + v(f(\ell_2)) = v \circ f(\lambda\ell_1 + \ell_2).$$

Or, par ailleurs, on a $v \circ f(\lambda\ell_1 + \ell_2) = f'(u(\lambda\ell_1 + \ell_2))$. Par injectivité de f', il vient que

$$u(\lambda\ell_1 + \ell_2) = \lambda\ell'_1 + \ell'_2 = \lambda u(\ell_1) + u(\ell_2)$$

ce qui termine la démonstration. Si maintenant v est injective, comme f l'est aussi, alors $v \circ f$ est injective. On en déduit alors immédiatement que u est injective [15].

2. On procède de manière analogue. Commençons par établir l'unicité. Soit $w : N \longrightarrow N'$ répondant à la question. Alors pour tout $n \in N$, par surjectivité de g, il existe $m \in M$ tel que $n = g(m)$. Ainsi, $w(n) = w(g(m)) = g'(v(m))$ est entièrement déterminé. Par ailleurs, cela est indépendant du choix de m car si $n = g(m) = g(m')$, alors $m - m' \in \mathrm{Ker}(g) = \mathrm{Im}(f)$. Ainsi, il existe $\ell \in L$ tel que $m = m' + f(\ell)$ et $g'(v(m)) = g'(v(m')) + g'(v(f(\ell))) = g'(v(m')) + g'(f'(u(\ell)))$. Mais $\mathrm{Im}(f') = \mathrm{Ker}(g')$ si bien que $g'(f'(u(\ell)))$ et $g'(v(m)) = g'(v(m'))$. Reste donc à construire w. Soit $n \in N$. Par le raisonnement précédent, on a l'existence d'un $m \in M$ tel que $n = g(m)$ et on peut définir $w : N \longrightarrow N'$ par $w(n) = g'(v(m))$ où cette application est bien définie d'après ce qui précède. Reste alors à montrer qu'il s'agit d'un morphisme. Soient alors $\lambda \in A$, $n_1, n_2 \in N$. On a alors $w(n_1) = g'(v(m_1))$ et $w(n_2) = g'(v(m_2))$ avec m_i un antécédent quelconque de n_i par g pour $i \in \{1, 2\}$. On a alors

$$\lambda w(n_1) + w(n_2) = \lambda g'(v(m_1)) + g'(v(m_2)) = g' \circ v(\lambda m_1 + m_2).$$

Or, $\lambda m_1 + m_2$ est un antécédent de $\lambda n_1 + n_2$ par g car $g(\lambda m_1 + m_2) = \lambda g(m_1) + g(m_2) = \lambda n_1 + n_2$. Ainsi, $g' \circ v(\lambda m_1 + m_2) = w(\lambda n_1 + n_2)$ et finalement $w(\lambda n_1 + n_2) = \lambda w(n_1) + w(n_2)$, ce qui permet de conclure. Pour finir, il est clair que si v est surjective, comme g' l'est, alors $w \circ g = g' \circ v$ est surjective, ce qui implique aisément que w est surjective.

Exercice 9 — Lemme des 5. Soit A un anneau, et soit

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle u_1} & & \downarrow{\scriptstyle u_2} & & \downarrow{\scriptstyle u_3} & & \downarrow{\scriptstyle u_4} & & \downarrow{\scriptstyle u_5} \\ M'_1 & \xrightarrow{f'_1} & M'_2 & \xrightarrow{f'_2} & M'_3 & \xrightarrow{f'_3} & M'_4 & \xrightarrow{f'_4} & M'_5 \end{array}$$

15. Si x est dans son noyau, alors $u(x) = 0$ mais en prenant l'image par f', $f'(u(x)) = v(f(x)) = 0$ donc $x = 0$.

un diagramme de morphisme de A-modules tel que les deux lignes sont exactes et chaque carré est commutatif. Montrer les énoncés suivants.

1. Si u_2 et u_4 sont surjectives et si u_5 est injective, alors u_3 est surjective.
2. Si u_2 et u_4 sont injectives et si u_1 est surjective, alors u_3 est injective.
3. Si u_1 est surjective, u_5 est injective et u_2 et u_4 sont des isomorphismes, alors u_3 est un isomorphisme.

Solution.

1. Soit $m_3' \in M_3'$. On a alors que $f_3'(m_3') \in M_4'$ et par surjectivité de u_4, il existe $m_4 \in M_4$ tel que $f_3'(m_3') = u_4(m_4)$. On constate alors que $f_4'(u_4(m_4)) = f_4' \circ f_3'(m_3') = 0$ car par exactitude $f_4' \circ f_3' = 0$. Mais, $f_4'(u_4(m_4)) = u_5 \circ f_4(m_4)$ si bien que par injectivité de u_5, il vient que $f_4(m_4) = 0$. Par suite, $m_4 \in \mathrm{Ker}(f_4) = \mathrm{Im}(f_3)$ et il existe $m_3 \in M_3$ tel que $m_4 = f_3(m_3)$. On obtient donc $f_3'(m_3') = u_4 \circ f_3(m_3) = f_3'(u_3(m_3))$ et $m_3' - u_3(m_3) \in \mathrm{Ker}(f_3') = \mathrm{Im}(f_2')$. Il existe ainsi $m_2' \in M_2'$ tel que $m_3' = f_2'(m_2') + u_3(m_3)$. Par surjectivité de u_2, on obtient $m_2 \in M_2$ tel que $m_2' = u_2(m_2)$ et $f_2'(m_2') = f_2'(u_2(m_2)) = u_3 \circ f_2(m_2)$. Finalement, $m_3' = u_3(f_2(m_2) + m_3)$ et u_3 est bien surjective.
2. Considérons $m_3 \in \mathrm{Ker}(u_3)$. On a alors $u_3(m_3) = 0$. On a alors $f_3' \circ u_3(m_3) = 0$ mais $f_3' \circ u_3(m_3) = u_4 \circ f_3(m_3)$ donc $f_3(m_3) \in \mathrm{Ker}(u_4)$ si bien que par injectivité de u_4, on a $m_3 \in \mathrm{Ker}(f_3) = \mathrm{Im}(f_2)$. Il s'ensuit qu'il existe $m_2 \in M_2$ tel que $m_3 = f_2(m_2)$. De $u_3(m_3) = 0$, on obtient $u_3 \circ f_2(m_2) = 0$. Mais, $u_3 \circ f_2(m_2) = f_2' \circ u_2(m_2)$ et $u_2(m_2) \in \mathrm{Ker}(f_2') = \mathrm{Im}(f_1')$. On a donc $m_1' \in M_1'$ tel que $u_2(m_2) = f_1'(m_1')$. Par surjectivité de u_1, il existe $m_1 \in M_1$ tel que $m_1' = u_1(m_1)$ et $u_2(m_2) = f_1' \circ u_1(m_1) = u_2 \circ f_1(m_1)$. Par injectivité de u_2, il vient $m_2 = f_1(m_1)$ et $m_3 = f_2(f_1(m_1))$ mais par exactitude $f_2 \circ f_1 = 0$ et donc $m_3 = 0$ et u_3 est bien injective.
3. Il suffit de combiner **1.** et **2.**

Exercice 10 — Lemme du serpent. Soit A un anneau, et soit

$$\begin{array}{ccccccccc} L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 & & \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle w} & & & & \\ 0 & \longrightarrow & L' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' & & \end{array}$$

un diagramme de morphismes de A-modules tel que les deux lignes sont exactes et $v \circ f = f' \circ u$ et $w \circ g = g' \circ v$.

1. Montrer que la restriction de f à $\mathrm{Ker}(u)$ a son image contenue dans $\mathrm{Ker}(v)$. Énoncer un résultat analogue pour g.
2. Montrer que l'application $\overline{f'} : L'/\mathrm{Im}(u) \to M'/\mathrm{Im}(v)$ définie[16] par $\overline{x} \mapsto \overline{f'(x)}$ est bien définie et énoncer un résultat similaire pour g'.
3. Définir un morphisme $\delta : \mathrm{Ker}(w) \to L'/\mathrm{Im}(u)$.
4. Montrer que la suite

$$\mathrm{Ker}(u) \xrightarrow{f_{|\mathrm{Ker}(u)}} \mathrm{Ker}(v) \xrightarrow{g_{|\mathrm{Ker}(v)}} \mathrm{Ker}(w) \xrightarrow{\delta} L'/\mathrm{Im}(u) \xrightarrow{\overline{f'}} M'/\mathrm{Im}(v) \xrightarrow{\overline{g'}} N'/\mathrm{Im}(w)$$

est exacte.

Solution.

1. Soit $\ell \in \mathrm{Ker}(u)$ et établissons que $f(\ell) \in \mathrm{Ker}(v)$. Pour ce faire, calculons $v \circ f(\ell) = f'(u(\ell)) = f'(0) = 0$, ce qui permet d'obtenir le résultat. De même, $g(\mathrm{Ker}(v)) \subseteq \mathrm{Ker}(w)$.
2. Si $\overline{x} = \overline{y}$, alors il existe $\ell \in L$ tel que $x = y + u(\ell)$. On a alors $f'(x) = f'(y) + f' \circ u(\ell) = f'(y) + v \circ f(\ell)$ si bien que $f'(x) - f'(y) \in \mathrm{Im}(v)$ et $\overline{f'(x)} = \overline{f'(y)}$ et $\overline{f'}$ est bien définie et clairement linéaire. De même, l'application $\overline{g'} : M'/\mathrm{Im}(v) \to N'/\mathrm{Im}(w)$ définie par $\overline{x} \mapsto \overline{g'(x)}$ est bien définie et linéaire.
3. On définit un morphisme $\delta : \mathrm{Ker}(w) \to L'/\mathrm{Im}(u)$ de la façon suivante. Soit $n \in \mathrm{Ker}(w)$. Comme g est surjective, il existe $m \in M$ tel que $g(m) = n$. On a alors que $v(m) \in \mathrm{Ker}(g') = \mathrm{Im}(f')$. Il existe donc un unique $\ell' \in L'$ tel que $f'(\ell') = v(m)$. On pose alors $\delta(n) = \overline{\ell'} \in L'/\mathrm{Im}(u)$. Cela fournit une application bien définie et indépendante de l'antécédent $m \in M$. En effet, si $g(m) = g(m')$ pour $m, m' \in M$, alors $m - m' \in \mathrm{Ker}(g) = \mathrm{Im}(f)$ si bien qu'il existe $\ell \in L$ tel que $m = m' + f(\ell)$.

16. On parle de *conoyaux*.

On a alors $v(m) = v(m') + v \circ f(\ell) = v(m') + f'(u(\ell))$. Il existe alors un unique (par injectivité de f') $\ell' \in L'$ et $\ell'' \in L'$ tels que $v(m) = f'(\ell')$ et $v(m') = f'(\ell'')$ de sorte que $f'(\ell') = f'(\ell'' + u(\ell))$ et $\ell' - \ell'' \in \mathrm{Im}(u)$. Ainsi, on a bien $\overline{\ell'} = \overline{\ell''} \in L'/\mathrm{Im}(u)$. Reste à justifier que l'on a bien construit un morphisme de A-modules. Pour ce faire, soient $\lambda \in A$ et $n_1, n_2 \in \mathrm{Ker}(w)$. On a alors par construction que si $m_1, m_2 \in M$ sont deux antécédents par g quelconques de n_1 et n_2 respectivement alors il existe un unique $\ell'_1 \in L'$ et $\ell'_2 \in L'$ tels que $f'(\ell'_i) = v(m_i)$ et $\delta(n_i) = \ell'_i$ pour $i \in \{1, 2\}$. On a donc

$$\lambda\delta(n_1) + \delta(n_2) = \lambda\ell'_1 + \ell'_2.$$

Mais $\lambda m_1 + m_2$ est alors un antécédent de $\lambda n_1 + n_2$ par g et il est alors clair que $f'(\lambda\ell'_1 + \ell'_2) = v(\lambda m_1 + m_2)$. On en déduit que $\delta(\lambda n_1 + n_2) = \lambda\ell'_1 + \ell'_2$ soit que $\delta(\lambda n_1 + n_2) = \lambda\delta(n_1) + \delta(n_2)$, ce qui conclut la démonstration.

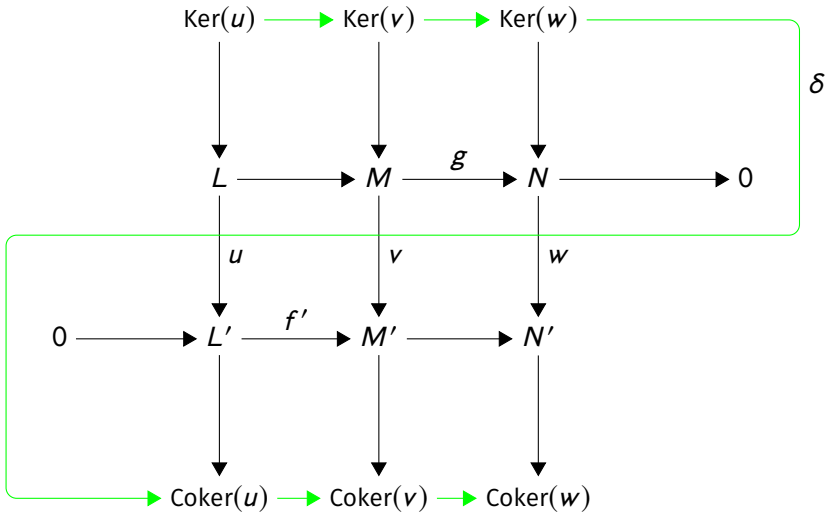
4. Toutes ces flèches ont bien un sens d'après les questions précédentes. Montrons pour commencer que $\mathrm{Im}(f_{|\mathrm{Ker}(u)}) = \mathrm{Ker}(g_{|\mathrm{Ker}(v)})$. Soit $m \in \mathrm{Ker}(g_{|\mathrm{Ker}(v)})$. On a alors $v(m) = g(m) = 0$. En particulier, $m \in \mathrm{Ker}(g) = \mathrm{Im}(f)$ si bien qu'il existe $\ell \in L$ tel que $m = f(\ell)$. Calculons alors $f' \circ u(\ell) = v(f(\ell)) = v(m) = 0$ si bien que par injectivité de f', $u(\ell) = 0$ et $u \in \mathrm{Ker}(u)$. On a donc bien que $m \in \mathrm{Im}(f_{|\mathrm{Ker}(u)})$. Réciproquement, si $m \in \mathrm{Im}(f_{|\mathrm{Ker}(u)})$, alors il existe $\ell \in \mathrm{Ker(u)}$ tel que $m = f(\ell)$. On a alors vu en **1.** que $m = f(\ell) \in \mathrm{Ker(v)}$ et de plus, $g(m) = g \circ f(\ell) = 0$ car $g \circ f = 0$ si bien que $m \in \mathrm{Ker}(g_{|\mathrm{Ker}(v)})$.

Établissons ensuite que $\mathrm{Im}(\overline{f'}) = \mathrm{Ker}(\overline{g'})$. Soit $\overline{m'} \in \mathrm{Ker}(\overline{g'})$. On a alors $\overline{g'(m')} = \overline{0}$ soit $g'(m') \in \mathrm{Im}(w)$. En particulier, il existe $n \in N$ tel que $g'(m') = w(n)$. Par surjectivité de g, il existe $m \in M$ tel que $n = g(m)$ et $g'(m') = w(g(m)) = g'(v(m))$ si bien que $m' - v(m) \in \mathrm{Ker}(g') = \mathrm{Im}(f')$ et il exite $\ell' \in L'$ tel que $m' = v(m) + f'(\ell')$ soit tel que $\overline{m'} = \overline{f'}(\overline{\ell'})$ et on ainsi que $\overline{m'} \in \mathrm{Im}(\overline{f'})$. Réciproquement, soit $\overline{m'} \in \mathrm{Im}(\overline{f'})$, alors il existe $\overline{\ell'} \in L'/\mathrm{Im}(u)$ tel que $\overline{m'} = \overline{f'}(\overline{\ell'})$, autrement dit $m' - f'(\ell') \in \mathrm{Im}(v)$ et il existe $m \in M$ tel que $m' = f'(\ell') + v(m)$. On calcule alors $g'(m') = g'(f'(\ell')) + g'(v(m)) = w(g(m))$ car $g' \circ f' = 0$. Finalement, $\overline{g'}(\overline{m'}) = \overline{g'(m')} = 0 \in N'/\mathrm{Im}(w)$ et on a bien l'égalité souhaitée.

Passons alors à l'égalité $\mathrm{Im}(g_{|\mathrm{Ker}(v)}) = \mathrm{Ker}(\delta)$. Soit $n \in \mathrm{Ker}(\delta)$. On a alors $w(n) = 0$ et $\delta(n) = 0$. On écrit $n = g(m)$ pour un antécédent $m \in M$ quelconque et on considère l'unique $\ell' \in l'$ tel que $v(m) = f'(\ell')$. On a alors $\ell' = 0$ si bien que $v(m) = 0$ et $m \in \mathrm{Ker(v)}$. Ainsi, puisque $n = g(m)$, on a bien que $n \in \mathrm{Im}(g_{|\mathrm{Ker}(v)})$. Réciproquement, soit $n \in \mathrm{Im}(g_{|\mathrm{Ker}(v)})$ si bien qu'il existe $m \in M$ vérifiant $v(m) = 0$ et tel que $n = g(m)$. Par injectivité de f', le seul $\ell' \in L'$ tel que $f'(\ell') = v(m)$ est donc $\ell' = 0$ si bien que par construction, $\delta(n) = 0$ et $n \in \mathrm{Ker}(\delta)$.

Enfin, pour terminer et conclure à l'exactitude, il reste à établir l'égalité $\mathrm{Ker}(\overline{f'}) = \mathrm{Im}(\delta)$. Soit $\overline{\ell'} \in \mathrm{Ker}(\overline{f'})$, autrement dit il existe $m \in M$ tel que $f'(\ell') = v(m)$. On pose alors $n = g(m)$ et par construction, on a $\delta(n) = \overline{\ell'}$ de sorte que $\overline{\ell'} \in \mathrm{Im}(\delta)$. Réciproquement, soit $\overline{\ell'} \in \mathrm{Im}(\delta)$. Il existe donc $n \in N$ tel que $\overline{\ell'} = \delta(n)$. Choisissons alors un antécédent $m \in M$ par g de n de sorte que $g(m) = n$. On sait qu'on a alors, pour l'unique $\ell'' \in L'$ tel que $v(m) = f'(\ell'')$, on a $\delta(n) = \overline{\ell''}$. On a donc l'existence d'un $\ell \in L$ tel que $\ell' = \ell'' + u(\ell)$ si bien que $f'(\ell') = f'(\ell'') + f'(u(\ell)) = f'(\ell'') + v(f(\ell))$ et $\overline{f'}(\overline{\ell'}) = \overline{f'(\ell')} = \overline{f'(\ell'')} = \overline{0}$ et $\overline{\ell'} \in \mathrm{Ker}(\overline{f'})$.

Noter que les exercices 16, 17 et 18 sont importants en algèbre homologique ou cohomologique et valent plus généralement dans ce que l'on appelle une *catégorie abélienne*. Le nom de *lemme du serpent* vient de la représentation ci-dessous de la suite exacte de la question **4.** :



Exercice 11. On considère M l'ensemble des triplets $(x, y, z) \in \mathbf{Z}^3$ tels que $x + y + z \equiv 0 \pmod 2$.

1. Montrer que M est un sous-$\mathbf{Z}$-module libre de type fini de rang 3 de $\mathbf{Z}^3$.
2. Donner une $\mathbf{Z}$-base de M.
3. Montrer que $\mathbf{Z}^3/M$ n'a que deux sous-modules, $\{0\}$ et lui-même. On parle de *module simple*.
4. Soient A un anneau principal, L un A-module libre de rang fini et M un sous-A-module de L. Montrer que M admet un supplémentaire dans L si, et seulement si, L/M est sans torsion. Le module M de la question précédente admet-il un supplémentaire dans $\mathbf{Z}^3$?

Solution.

1. On vérifie immédiatement qu'il s'agit d'un sous-$\mathbf{Z}$-module de $\mathbf{Z}^3$ qui est donc de type fini (car $\mathbf{Z}$ est noethérien). Pour montrer que M est libre, d'après le cours comme $\mathbf{Z}$ est principal, il suffit de montrer qu'il est sans torsion. Or, c'est clair car M est un sous-module de $\mathbf{Z}^3$ qui est sans torsion. Par ailleurs, en tant que sous-module libre de $\mathbf{Z}^3$, on a immédiatement [17] que M est de rang $\leqslant 3$. Pour conclure, il suffit d'exhiber trois vecteurs $\mathbf{Z}$-libres [18] de M. On peut par exemple prendre $(2, 0, 0)$, $(0, 2, 0)$ et $(0, 0, 2)$.
2. Attention au fait qu'ici, une famille libre de trois vecteurs n'est pas forcément une $\mathbf{Z}$-base de M (voir exercice 2)! Montrons alors que $e_1 = (1, -1, 0)$, $e_2 = (1, 0, -1)$ et $e_3 = (2, 0, 0)$ est une base de M. On montre aisément que la famille est $\mathbf{Z}$-libre (elle l'est sur $\mathbf{Q}$ donc *a fortiori* sur $\mathbf{Z}$). Reste à établir le caractère générateur. Soit $u = (x, y, z) \in M$, on a alors
$$u = -ye_1 - zu_2 + \frac{x + y + z}{2} e_3$$
qui est bien à coefficients entiers par définition de M.
3. Considérons l'application $\varphi : \mathbf{Z}^3 \to \mathbf{Z}/2\mathbf{Z}$ définie par $(x, y, z) \mapsto \overline{x + y + z}$. Cette application est $\mathbf{Z}$-linéaire et surjective (par exemple $\varphi(1, 0, 0) = \overline{1}$) et de noyau M si bien que par théorème de factorisation, $\mathbf{Z}^3/M \cong \mathbf{Z}/2\mathbf{Z}$, ce qui fournit immédiatement le résultat.
4. Supposons pour commencer que M ait un supplémentaire N dans L. On a alors $L/M \cong N$ et $N \subseteq L$. Comme L est sans torsion, il en est de même pour N et donc de L/M.
Réciproquement, supposons que L/M est sans torsion. Le théorème de structure fournit que L/M est libre de rang, disons r, engendré par $(\overline{e_1}, \dots, \overline{e_r})$ avec $e_i \in L$ et où $\overline{e_i}$ représente la classe de e_i dans le quotient L/M pour tout $i \in \{1, \dots, r\}$. Notons alors N le sous-A-module engendré par les e_i et montrons qu'il s'agit d'un supplémentaire de M.
Soit $x = \sum_{i=1}^{r} x_i e_i \in M \cap N$ (car $x \in N$) avec $x_1, \dots, x_r \in A$. Alors, puisque $x \in M$, on a
$$\overline{x} = \sum_{i=1}^{r} x_i \overline{e_i} = 0$$
et par conséquent $x_1 = \cdots = x_r = 0$ car $(\overline{e_1}, \dots, \overline{e_r})$ est une base de L/M. Ainsi $M \cap N = \{0\}$. Soit alors $x \in L$, on a alors l'existence de $x_1, \dots, x_r \in A$ tels que
$$\overline{x} = \sum_{i=1}^{r} x_i \overline{e_i} \quad \text{si bien que} \quad x - \sum_{i=1}^{r} x_i e_i \in M.$$
On a donc bien $x = N + M$, ce qui conclut la démonstration, N est un supplémentaire de M dans L.
D'après **3.**, on en déduit que M n'admet pas de supplémentaire dans $\mathbf{Z}^3$.

Exercice 12.

Soit A un anneau commutatif. Soit B une A-algèbre. Un élément $b \in B$ est dit *entier* sur A s'il existe $P \in A[X]$ unitaire tel que $P(b) = 0$.

1. Montrer que si $b \in B$ est entier sur A, alors le A-module $A[b]$ est de type fini.

17. Ou plus simplement, le cours fournit, $\mathbf{Z}$ étant principal, que tout sous-module d'un $\mathbf{Z}$-module libre de type fini est lui-même libre de type fini.
18. Cela fournit une application $\mathbf{Z}$-linéaire de $\mathbf{Z}^3$ dans M injective si bien que le rang de M est supérieur à 3.

Soit maintenant $b \in B$, on suppose qu'il existe un $A[b]$-module D qui est fidèle[19] (*i.e.* tel que pour tout $\alpha \in A[b]$ non nul, il existe $x \in D$ tel que $\alpha \cdot x \neq 0$) et de type fini en tant que A-module. On choisit une famille génératrice $(d_1, \ldots, d_n)$ du A-module D et on écrit pour tout $i \in \{1, \ldots, n\}$:

$$b \cdot d_i = \sum_{j=1}^{n} a_{ij} d_j$$

avec $a_{ij} \in A$.

2. Soit $d \in A[b]$ le déterminant de la matrice[20] $(\delta_{ij} b - a_{ij})_{1 \leqslant i,j, \leqslant n}$, où δ_{ij} est le symbole de Kronecker. Montrer que $d \cdot d_i = 0$ pour tout $i \in \{1, \ldots, n\}$.

3. En déduire que $d = 0$, puis que b est entier sur A.

4. Montrer la réciproque de **1.** : si $b \in B$ est tel que le A-module $A[b]$ est de type fini, alors b est entier sur A. Montrer que cette condition est aussi équivalente à l'existence d'une sous-algèbre de B contenant b et de type fini en tant que A-module.

5. Montrer que si $b_1, \ldots, b_n \in B$ sont entiers sur A, alors le A-module $A[b_1, \ldots, b_n]$ est de type fini.

6. On suppose que B est un A-module de type fini. Montrer alors que tout élément de B est entier sur A (on dit alors que B est entier sur A).

7. Montrer que si C est une A-algèbre et B est entier sur A, alors $B \otimes_A C$ est entier sur C. La $A[X]$-algèbre $B[X]$ est-elle alors entière sur $A[X]$?

Solution.

1. L'hypothèse dit qu'il existe $a_0, \ldots, a_{n-1}$ dans A tels que

$$b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 = 0.$$

Soit A' le sous A-module de $A[b]$ engendré par $1, b, \ldots, b^{n-1}$. L'égalité ci-dessus donne que $b^n \in A'$. En multipliant par b^i, on obtient, pour tout $i \in \mathbf{N}^\times$,

$$b^{n+i} + a_{n-1} b^{n-1+i} + \cdots + a_1 b^{i+1} + a_0 b^i = 0,$$

d'où il résulte immédiatement par récurrence sur i que $b^{n+i} \in A'$ pour tout $i \in \mathbf{N}$. On en déduit que $A' = A[b]$, et donc $A[b]$ est un A-module de type fini, engendré par $1, b, \ldots, b^{n-1}$.

2. Soit Q la matrice $(\delta_{ij} b - a_{ij})_{1 \leqslant i,j, \leqslant n}$ et X le vecteur colonne $(d_1, \ldots, d_n)$. On a $Q \cdot X = 0$, donc d'après l'identité de la comatrice

$$dX = (\widetilde{Q} Q) X = 0.$$

Ainsi $d d_i = 0$ pour tout i.

3. Comme le A-module D est engendré par $(d_1, \ldots, d_n)$, il résulte de **2.** que $dx = 0$ pour tout $x \in D$. D'autre part, le $A[b]$-module D est fidèle, d'où finalement $d = 0$. En écrivant l'expression explicite du déterminant, cela fournit un polynôme unitaire $P \in A[X]$ tel que $P(b) = 0$.

4. Supposons le A-module $A[b]$ de type fini. Comme $A[b]$ est en particulier un $A[b]$-module fidèle (vu que si $\alpha \in A[b]$ est non nul, alors $\alpha \cdot 1 = \alpha \neq 0$), **3.** implique que b est entier[21] sur A. Dans ce cas, $A[b]$ est une sous-algèbre de B contenant b

19. Autrement dit

$$\begin{array}{ccc} A[b] & \longrightarrow & \mathrm{End}(M) \\ a & \longmapsto & [m \mapsto a \cdot m] \end{array}$$

est injective et vous pouvez voir le lien avec une action de groupe fidèle qui correspond à un morphisme

$$\begin{array}{ccc} G & \longrightarrow & \mathfrak{S}(X) \\ g & \longmapsto & [x \mapsto g \cdot x] \end{array}$$

injectif.

20. À coefficients dans $A[b]$.

21. Dans ce cas, on pouvait raisonner différemment. Supposons que $P_1, \ldots, P_r$ engendrent $A[b]$ comme A-module. Alors par définition, les P_i sont des polynômes en b à coefficients dans A. Notons d le maximum de leurs degré, on a alors que $b^{d+1} \in A[b]$ est combinaison linéaire des $P_1, \ldots, P_r$ à coefficients dans A, ce qui fournit un polynôme annulateur unitaire de degré $d+1$. Mais cette méthode tombe en défaut lorsqu'on veut généraliser à un sous-module qui contient b puisque les générateurs ne sont plus des polynômes en b à coefficients dans A.

et de type fini comme A-module ; réciproquement, si une telle sous-algèbre existe, elle est aussi un $A[b]$-module fidèle [22], donc par **3.** on a encore que b est entier sur A.

5. On procède par récurrence sur n, le cas $n = 1$ résultant de **1**. Comme b_n est entier sur A, il l'est a fortiori sur $A[b_1, \dots, b_{n_1}]$, et donc $A[b_1, \dots, b_{n_1}, b_n]$ est un $A[b_1, \dots, b_{n_1}]$-module de type fini, tandis que $A[b_1, \dots, b_{n_1}]$ est un A-module de type fini par hypothèse de récurrence. On en déduit finalement que $A[b_1, \dots, b_{n_1}, b_n]$ est un A-module de type fini.

6. Soit $b \in B$, alors B est une sous-algèbre de B contenant b et de type fini comme A-module ; on applique alors **4.**

7. Tout élément x de $B \otimes_A C$ s'écrit comme une somme finie

$$x = \sum_{i=1}^{n} (b_i \otimes c_i)$$

avec $b_i \in B$ et $c_i \in C$. Il suffit alors d'après **4.** de montrer que le C-module $A[b_1, \dots, b_n] \otimes_A C$ est de type fini, puisque c'est une sous C-algèbre de $B \otimes_A C$ qui contient x. Or **.** donne que $A[b_1, \dots, b_n]$ est un A-module de type fini, d'où le résultat [23]. Ceci vaut en particulier pour $C = A[X]$, donc $B[X] = B \otimes_A A[X]$ est entière sur $A[X]$.

Exercice 13.

Soient A un anneau commutatif et B une A-algèbre. On note A_1 l'ensemble des éléments de B qui sont entiers sur A. Cet exercice fait appel aux résultats de l'exercice précédent.

1. Montrer que A_1 est un sous-anneau de B qui contient l'image de A dans B. On dit que A_1 est la *fermeture intégrale* de A dans B.

2. Soit C une B-algèbre. Montrer que si c est entier sur B et B est entier sur A, alors c est entier sur A.

3. Avec les notations de **1.**, montrer que la fermeture intégrale de A_1 dans B est A_1.

4. On suppose A intègre, de corps des fractions K. On dit que A est *intégralement clos* si la fermeture intégrale de A dans K est A. Montrer que si A est factoriel, alors A est intégralement clos, mais que l'anneau $\mathbf{Z}[i\sqrt{3}]$ n'est pas intégralement clos.

Soit A un anneau intègre de corps des fractions K. Soit L une extension de K (*i.e.* un corps qui contient K). Soit $x \in L$ un élément entier sur A, on note $P \in K[X]$ le polynôme minimal de x sur K, c'est-à-dire le polynôme unitaire non nul de degré minimal de $K[X]$ qui annule x.

5. Montrer qu'il existe un polynôme unitaire $Q \in \mathbf{Z}[X]$ tel que $Q(x) = 0$ et P divise Q dans $K[X]$.

6. Soient $a_1, \dots, a_r$ les racines de P (dans un corps de décomposition M de P sur K). Montrer que les a_i sont entiers sur A pour tout $i \in \{1, \dots, r\}$.

7. En déduire que si A est intégralement clos, alors $P \in A[X]$.

8. On prend $A = \mathbf{Z}$, $K = \mathbf{Q}$, $L = \mathbf{Q}(i\sqrt{5})$. Montrer que si $y \in L$ est entier sur $\mathbf{Z}$, il est racine d'un polynôme unitaire de $\mathbf{Z}[X]$ de degré 1 ou 2.

9. Montrer que $\mathbf{Z}(i\sqrt{5})$ est la fermeture intégrale de $\mathbf{Z}$ dans $\mathbf{Q}(i\sqrt{5})$. En particulier, $\mathbf{Z}(i\sqrt{5})$ est intégralement clos (mais pas factoriel).

Solution.

22. En effet, je rappelle qu'une A-algèbre C ne contient pas nécessairement A comme sous-anneau mais que par définition, on a un morphisme d'anneaux $\varphi : A \to C$ et que tout élément non nul de $A[b] \subseteq C$ est de la forme

$$a_n \cdot b^n + \cdots + a_0 \cdot 1_B = \varphi(a_n) b^n + \cdots \varphi(a_0)$$

et que pour la fidélité, il suffit de prendre $1_C = \varphi(1_A)$ et on a alors pour tout $\alpha \neq 0$ de $A[b]$ que $\alpha \cdot 1_C = \alpha \neq 0$.

23. Que vous pouvez soit voir à la main en prenant des générateurs $d_1, \dots, d_r$ de $A[b_1, \dots, b_n]$ et montrer qu'alors les $d_1 \otimes 1, \dots, d_r \otimes 1$ sont générateurs soit raisonner en disant qu'être de type fini revient à se donner un morphisme surjectif $\pi : A^r \to A[b_1, \dots, b_n]$ et puisque prendre le produit tensoriel conserve la surjectivité, cela fournit un morphisme A-linéaire tel que $\pi \otimes 1 : A^r \otimes_A C \to A[b_1, \dots, b_n] \otimes_A C$. Ce morphisme est alors clairement C-linéaire car pour $c \in C$,

$$\pi \otimes 1\big(c((a_1, \dots, a_r) \otimes c')\big) = \pi \otimes 1\big((a_1, \dots, a_r) \otimes (cc')\big) = \pi(a_1, \dots, a_r) \otimes (cc') = c\big(\pi(a_1, \dots, a_r) \otimes c'\big) = c(\pi \otimes 1)\big((a_1, \dots, a_r) \otimes c'\big).$$

Autrement dit on a un morphisme C-linéaire surjectif $C^r \to A[b_1, \dots, b_n] \otimes_A C$ car $A^r \otimes_A C \cong C^r$ et $A[b_1, \dots, b_n] \otimes_A C$ est un C-module de type fini.

1. Il est immédiat que A_1 contient l'image de A dans B, vu que tout élément a de A est annulé par le polynôme unitaire $(X-a) \in A[X]$. On a clairement aussi $0 \in A_1$ et $1 \in A_1$. Soient alors $x, y \in A_1$. D'après le **5.** de l'exercice précédent, on sait que $A[x,y]$ est un A-module de type fini. Comme c'est une sous-algèbre de B qui contient $x-y$ et xy, on en déduit que $x-y$ et xy sont entiers sur A d'après le **4.** de l'exercice précédent. Finalement, A_1 est bien un sous-anneau de B.

2. Soit $c \in C$, il est entier sur B, d'où un polynôme unitaire

$$P = X^n + b_{n-1}X^{n-1} + \cdots + b_0$$

qui annule c avec $b_0, \ldots, b_{n-1} \in B$. Plus précisément, cela dit que c est entier sur $A[b_0, \cdots, b_{n-1}]$, lequel est un A-module de type fini d'après le **5.** de l'exercice précédent. Comme le **4.** de l'exercice précédent dit alors que $A[b_0, \ldots, b_{n-1}, c]$ est un $A[b_0, \ldots, b_{n-1}]$-module de type fini, on obtient finalement que $A[b_0, \ldots, b_{n-1}, c]$ est un A-module de type fini, et comme c'est une sous A-algèbre de C qui contient c, on obtient (toujours d'après le **4.** de l'exercice précédent) que c est entier sur A. On a donc bien montré que C est entier sur A.

3. D'après **2.**, tout élément de B qui est entier sur A_1 est déjà entier sur A, donc est dans A_1.

4. Supposons A factoriel. Soit $x = \frac{p}{q}$ un élément de K qui est entier sur A. On peut supposer que p et q sont premiers entre eux. Par définition on a alors des éléments $a_{n-1}, \ldots, a_0$ de A tels que

$$\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_0 = 0.$$

En multipliant par q^n, on obtient alors que q divise p^n, ce qui n'est possible que si q est inversible, puisque p et q sont premiers entre eux et A est factoriel. Ainsi, $x \in A$.

5. L'anneau $\mathbf{Z}[i\sqrt{3}]$ n'est pas intégralement clos car l'élément $\frac{-1+i\sqrt{3}}{2}$ de son corps des fractions annule le polynôme X^2+X+1.

6. Comme x est entier, il est annulé par un polynôme unitaire $Q \in A[X]$. Par définition du polynôme minimal (qui engendre l'idéal de $K[X]$ constitué des polynômes qui annulent x), le polynôme P divise Q dans $K[X]$.

7. Comme P divise Q, les a_i annulent Q, qui est unitaire dans $A[X]$. Ces a_i sont donc entiers sur A.

8. Comme les coefficients de P sont des polynômes à coefficients entiers (les polynômes symétriques élémentaires) en les a_i, ils sont aussi entiers sur A. En particulier, ils sont dans A si A est intégralement clos.

9. On observe que tout $y \in L$ est racine d'un polynôme de degré 1 ou 2 de $\mathbf{Q}[X]$. D'après **2.**, son polynôme minimal est à coefficients dans $\mathbf{Z}$.

10. On a déjà que $i\sqrt{5}$ et entier sur $\mathbf{Z}$, car il annule X^2+5. Ainsi la fermeture intégrale B de $\mathbf{Z}$ dans $\mathbf{Q}(i\sqrt{5})$ contient $\mathbf{Z}(i\sqrt{5})$. Réciproquement, si $y \in B$, alors d'après **4.** il annule un polynôme unitaire P de degré 1 ou 2 à coefficients dans $\mathbf{Z}$, qui est son polynôme minimal. Le cas de degré 1 est trivial. Dans le cas où P est de degré 2 et $y = \alpha + i\beta\sqrt{5}$ (avec α, β dans $\mathbf{Q}$), ce polynôme minimal est $(X-\alpha)^2 + 5\beta^2$. Alors, d'après **3.**, on a $-2\alpha \in \mathbf{Z}$ et $\alpha^2 + 5\beta^2 \in \mathbf{Z}$. Si $\alpha \in \mathbf{Z}$, alors $5\beta^2 \in \mathbf{Z}$ ce qui implique $\beta \in$ (écrire $\beta = \frac{u}{v}$ avec u et v entiers premiers entre eux). Si $\alpha = w/2$ avec w entier impair, alors $w^2/4 + 5u^2/v^2$ est entier, ce qui implique $v = 2$ (regarder les valuations 2-adiques et 5-adiques) et $w^2 + 5u^2$ divisible par 4. Mais c'est impossible avec w impair en regardant modulo 4. Finalement, on a bien α et β dans $\mathbf{Z}$, d'où $y \in \mathbf{Z}(i\sqrt{5})$.

Exercice 14.

Soit A un anneau commutatif. Soit I un ensemble ordonné filtrant (c'est-à-dire que si (i,j) sont dans I, il existe $k \in I$ tel que $k \geqslant i$ et $k \geqslant j$). Soit $(M_i)_{i\in I}$ une famille de A-modules. On suppose donné pour tout $j \geqslant i$ un morphisme de A-modules $f_{ij} : M_i \to M_j$ avec $f_{ii} = \mathrm{Id}$ et $f_{jk} \circ f_{ij} = f_{ik}$ pour tous i, j, k de I vérifiant $i \leqslant j \leqslant k$.

On considère l'ensemble E des couples (i, x_i) avec $i \in I$ et $x_i \in M_i$ (E est l'*union disjointe* des M_i).

1. On définit une relation $\sim$ sur E par $(i,x_i) \sim (j,x_j)$ s'il existe $k \in I$ vérifiant : $k \geqslant i$, $k \geqslant j$, et $f_{ik}(x_i) = f_{jk}(x_j)$. Montrer que c'est une relation d'équivalence.

On appelle *limite inductive* des M_i l'ensemble quotient M de E par cette relation et φ_i l'application de M_i dans M qui envoie x_i sur la classe de (i,x_i).

2. Montrer qu'il existe une unique structure de A-module sur M telle que les applications φ_i soient des morphismes de A-modules. On note

$$M = \varinjlim_{i\in I} M_i.$$

3. Montrer que le A-module $\bigoplus_{i\in I} M_i$ est isomorphe à une limite inductive des $\bigoplus_{i\in J} M_i$, où J est une partie finie de I.

4. Montrer que si N est un A-module, alors pour toute famille de morphismes $u_i : M_i \to N$ vérifiant $u_j \circ f_{ij} = u_i$ si $i \geqslant j$, il existe un unique morphisme $u : M := \varinjlim_{i\in I} M_i \to N$ tel que $u_i = u \circ \varphi_i$.

5. Montrer que

$$N \otimes_A \varinjlim_{i\in I} M_i \simeq \varinjlim_{i\in I}(N \otimes_A M_i).$$

Solution.

L'exemple prototypique de limite inductive qu'il faut avoir en tête concerne la relation d'ordre donnée par l'inclusion auquel cas il faut penser à la limite inductive comme à une réunion et aux applications f_{ij} comme à une inclusion de M_i dans M_j comme on le verra par exemple dans l'exercice suivant.

1. La relation est réflexive via le fait que $f_{ii} = \mathrm{Id}$. Elle est clairement symétrique. Si enfin $(i, x_i) \sim (j, x_j)$ et $(j, x_j) \sim (k, x_k)$, alors il existe $\ell, m \in I$ avec : $l \geqslant i, \ell \geqslant j, m \geqslant j, m \geqslant k$ et

$$f_{i\ell}(x_i) = f_{j\ell}(x_j) \quad \text{et} \quad f_{jm}(x_j) = f_{km}(x_k).$$

On choisit alors $n \in I$ supérieur ou égal à ℓ et m. Alors

$$f_{in}(x_i) = f_{\ell n}(f_{i\ell}(x_i)) = f_{\ell n}(f_{j\ell}(x_j)) = f_{jn}(x_j) = f_{mn}(f_{jm}(x_j)) = f_{mn}(f_{km}(x_k)) = f_{kn}(x_k),$$

ce qui montre que $(i, x_i) \sim (k, x_k)$. La relation est donc bien transitive.

2. Soient $x, y \in M$ et $\alpha \in A$. Choisissons $k \in I$ tels que x et y s'écrivent $x = \varphi_k(x_k)$, $y = \varphi_k(y_k)$ avec $x_k, y_k \in M_k$ (ce qui est possible [24] en prenant k assez grand). On doit [25] alors poser

$$\alpha \cdot x := \varphi_k(\alpha \cdot x_k) \quad \text{et} \quad (x + y) := \varphi_k(x_k + y_k).$$

Vérifions que ceci est bien indépendant du choix de k. Si on prend un autre $\ell \in I$ avec $x = \varphi_\ell(x_\ell)$ et $y = \varphi_\ell(y_\ell)$, alors on peut choisir m supérieur ou égal à k et ℓ tel que $f_{km}(x_k) = f_{\ell m}(x_\ell)$ et $f_{km}(y_k) = f_{\ell m}(y_\ell)$ (ici on traduit simplement que l'égalité [26] $\varphi_\ell(x_\ell) = \varphi_k(x_k)$ revient à dire que $(k, x_k) \sim (\ell, x_\ell)$ et de même pour $(k, y_k) \sim (\ell, y_\ell)$). Alors $\alpha \cdot x_k$ (resp. $(x_k + y_k)$) a même image $\alpha \cdot f_{km}(x_k)$ (*resp.* $f_{km}(x_k) + f_{km}(y_k)$) dans M_m via [27] f_{km} que $\alpha \cdot x_\ell$ (*resp.* $(x_\ell + y_\ell)$) via [28] $f_{\ell m}$. Ainsi [29] $\varphi_k(\alpha \cdot x_k) = \varphi_\ell(\alpha \cdot x_\ell)$ et $\varphi_k(x_k + y_k) = \varphi_\ell(x_\ell + y_\ell)$ dans la limite inductive M.

Il est alors immédiat qu'on a bien défini une structure de A-module sur M telle que les φ_i soient des morphismes de A-modules.

3. Soient J et J' deux parties finies de I avec $J \subset J'$. On définit un morphisme

$$f_{JJ'} : \bigoplus_{i\in J} M_i \to \bigoplus_{i\in J'} M_i$$

en envoyant $(x_i)_{i\in J}$ sur $((x_i), 0, \ldots, 0)$. On voit alors facilement que $\bigoplus_{i\in I} M_i$ est la limite inductive des $\bigoplus_{i\in J} M_i$ pour J fini, relativement à ces morphismes $f_{JJ'}$. En effet, on sait que la limite inductive $\varinjlim \bigoplus_{i\in J} M_i$ existe et l'application de la réunion disjointe vers la somme directe donnée par $(J, (x_j)_{j\in J}) \mapsto \big((x_j)_{j\in J}, 0\big)$ pour $J \subseteq I$ fini et $(x_j)_{j\in J} \in \bigoplus_{i\in J} M_i$ passe au quotient [30] pour donner une application de la limite inductive vers $\bigoplus_{i\in I} M_i$ qui est clairement linéaire et injective. Pour voir qu'elle est surjective, il suffit de voir qu'un élément de $\bigoplus_{i\in I} M_i$ est de la forme $\big((x_j)_{j\in J}, 0\big)$ avec J fini et provient donc de la classe de $(J, (x_j)_{j\in J})$, ce qui permet d'établir le résultat.

24. En effet, par définition, x est la classe d'un (i, x_i), autrement dit $x = \varphi_i(x_i)$ et de même $y = \varphi_j(y_j)$. Maintenant, il existe $k \geqslant i, j$ et on a alors clairement (y penser toujours en termes d'inclusion) que $(i, x_i) \sim (k, f_{ik}(x_i))$ (car $f_{ik}(x_i) = f_{kk}(f_{ik}(x_i))$) si bien que $x = \varphi_k(x_k)$ avec $x_k = f_{ik}(x_i) \in M_k$ et de même $(j, y_j) \sim (k, f_{jk}(y_j))$ et $y = \varphi_k(y_k)$ avec $y_k = f_{jk}(y_j) \in M_k$.

25. On n'a pas le choix pour rendre les φ_k linéaires.

26. Noter qu'on obtient en fait $r \geqslant k, \ell$ tel que $f_{kr}(x_k) = f_{\ell r}(x_\ell)$ et $s \geqslant k, \ell$ tel que $f_{ks}(y_k) = f_{\ell s}(y_\ell)$ puis on choisit $m \geqslant r, s$ et on a $f_{rm}(f_{kr}(x_k)) = f_{km}(x_k)$ et $f_{rm}(f_{\ell r}(x_\ell)) = f_{\ell m}(x_\ell)$ de sorte que $f_{km}(x_k) = f_{\ell m}(x_\ell)$ et de même $f_{km}(y_k) = f_{\ell m}(y_\ell)$.

27. Qui est, elle, A-linéaire.

28. Idem.

29. En effet, on a $f_{km}(\alpha \cdot x_k) = f_{\ell m}(\alpha \cdot x_\ell)$ et on prend l'image par φ_m et on utilise le fait que $\varphi_j \circ f_{ij} = \varphi_i$ ce qui traduit le fait simple que $(i, x_i) \sim (j, f_{ij}(x_i))$.

30. On aurait pu utiliser également la question suivante avec les inclusions.

4. On doit nécessairement définir u en envoyant tout $x = \varphi_i(x_i)$ sur $u_i(x_i)$. Si maintenant $x = \varphi_i(x_i) = \varphi_j(x_j)$, on peut trouver k au moins égal à i et j avec $f_{ik}(x_i) = f_{jk}(x_j)$. Alors

$$u_i(x_i) = u_k(f_{ik}(x_i)) = u_k(f_{jk}(x_j)) = u_j(x_j),$$

ce qui montre que u est bien défini. C'est clairement un morphisme de A-modules.

5. La preuve est exactement analogue au cas particulier d'une somme directe, vu en cours. On commence par vérifier que les morphismes $\mathrm{Id} \otimes f_{ij} : N \otimes_A M_i \to N \otimes_A M_i$ lorsque $j \geqslant i$ fournissent un système inductif pour lequel on peut parler de $\varinjlim_{i\in I}(N \otimes_A M_i)$. On a alors de même $\mathrm{Id} \otimes \varphi_i : N \otimes_A M_i \to \varinjlim_{i\in I}(N \otimes_A M_i)$. On a ensuite que le morphisme bilinéaire Φ suivant

$$\begin{array}{ccc} N \times \varinjlim_{i\in I} M_i & \longrightarrow & \varinjlim_{i\in I}(N \otimes_A M_i) \\ n \otimes \varphi_i(x_i) & \longmapsto & \mathrm{Id} \otimes \varphi_i(n \otimes x_i) \end{array}$$

dont on vérifie immédiatement que c'est indépendant du choix de i. Par ailleurs, toute application bilinéaire $N \times \varinjlim_{i\in I} M_i \to P$ pour P un A-module induit une application bilinéaire $f : N \times M_i \to P$ (via φ_i) qui se factorise par propriété universelle de $N \otimes_A M$ par une unique application linéaire $u_i : N \otimes_A M_i \to P$ et la question **4.** fournit un unique morphisme $\tilde{f} : \varinjlim_{i\in I}(N \otimes_A M_i) \to P$ tel que $f = \tilde{f} \circ \Phi$, ce qui démontre que $\varinjlim_{i\in I}(N \otimes_A M_i)$ satisfait la propriété universelle de $N \otimes_A \varinjlim_{i\in I} M_i$ et ce qui permet de conclure !

Exercice 15.

Soient A un anneau principal et B un A-module sans torsion (*i.e.* l'égalité $ax = 0$ avec $a \in A$ et $x \in B$ implique $a = 0$ ou $x = 0$). Soient $u : M \to N$ un morphisme injectif de A-modules et $u_B : M \otimes_A B \to N \otimes_A B$ le morphisme induit. Cet exercice utilise l'exercice 14.

1. Montrer que si B est un A-module de type fini, alors u_B est injectif.

2. On ne suppose plus que B est de type fini. Montrer que B est isomorphe à la limite inductive d'une famille de A-modules de type fini.

3. En déduire que le résultat de **1.** vaut encore sans l'hypothèse que B est de type

4. Montrer par contre que si B est de type fini mais n'est plus supposé sans torsion, le résultat de **1.** tombe en défaut.

Solution.

1. On a vu que dans ce cas B est isomorphe à A^r avec $r \in \mathbf{N}$. Alors u_B s'identifie au morphisme $M^r \to N^r$ induit par u, lequel est clairement injectif. En effet, sait que cela implique que B est libre et qu'il existe donc une base $(e_1, \ldots, e_r)$. On a alors $B = \bigoplus_{i=1}^r Ae_i$. On a alors

$$M \otimes_A B = \bigoplus_{i=1}^r M \otimes_A Ae_i.$$

Or, l'application bilinéaire $M \times Ae_i \to M$ donnée par $(m, ae_i) \mapsto a \cdot m$ donne lieu à un morphisme $f : M \otimes_A Ae_i \to M$ surjectif car $f(m \otimes e_i) = m$ et injectif car tout élément de $M \otimes_A Ae_i$ est de la forme[31] $m \otimes ae_i$ pour un certain $a \in A$ et il est clair que si $f(m \otimes ae_i) = 0$ alors $m \otimes ae_i = 0$ puisque M est sans torsion. On vérifie que l'inverse est donné par $m \mapsto m \otimes e_i$. On a donc que u_B s'identifie à l'application $M^r \to N^r$ par

$$(m_1, \ldots, m_r) \mapsto \sum_{i=1}^r m_i \otimes e_i \mapsto \sum_{i=1}^r u(m_i) \otimes e_i \mapsto (u(m_1), \ldots, u(m_r))$$

où la première application correspond à l'isomorphisme $M^r \to \bigoplus_{i=1}^r M \otimes_A Ae_i = M \otimes_A B$, la seconde à u_B et la dernière à l'isomorphisme $N \otimes_A B = \bigoplus_{i=1}^r N \otimes_A Ae_i \cong N^r$.

2. On ordonne par inclusion les sous-modules de type fini de B, et pour deux tels modules C, D avec $C \subset D$, on prend pour f_{CD} l'inclusion (qui est un morphisme de A-modules). Il est alors immédiat que B s'identifie à la limite inductive de tous ses sous-modules de type fini en raisonnant comme dans le cas de la somme directe dans l'exercice précédent, vu que tout $x \in B$ est dans un tel sous-module, par exemple celui engendré par x.
Noter qu'on est, en quelque sorte, passé à la limite à partir des modules de type fini.

31. Et donc en fait de la forme $m \otimes e_i$ par A-linéarité et cette écriture est unique. En effet, si $m \otimes e_1 = m' \otimes e_1$ avec $m \neq m'$, alors on aboutit à une contradiction puisque l'application bilinéaire $M \times Ae_1 \to M$ qui envoie (m, ae_1) sur am ne s'annule pas en $(m - m', e_1)$.

3. On écrit $B = \varinjlim B_i$, où chaque B_i est de type fini. Alors, en utilisant le **5.** de l'exercice précédent, on voit que u_B s'identifie au morphisme

$$\varinjlim(M \otimes_A B_i) \to \varinjlim(N \otimes_A B_i)$$

induit par u. Ce morphisme est donné et bien défini par

$$\mathrm{Id} \otimes \varphi_i(m \otimes b_i) \mapsto \mathrm{Id} \otimes \varphi_i(u(m) \otimes b_i)$$

Soit x un élément de $\ker u_B$. Il est représenté par un $x_i \in M \otimes_A B_i$ (autrement dit $x = \mathrm{Id} \otimes \varphi_i(x_i)$), alors son image dans $N \otimes_A B_j$ est nulle pour un certain $j \geq i$ par définition de la limite inductive, d'où il résulte que l'image x_j de x_i dans $M \otimes_A B_j$ est nulle par injectivité de u_j, et donc que x est nul. On utilise ici le diagramme commutatif suivant où $u_i : M \otimes_A B_i \to N \otimes_A B_i$ est le morphisme induit par u

$$\begin{array}{ccc} M \otimes_A B_i & \xrightarrow{u_i} & N \otimes_A N_i \\ \downarrow{\scriptstyle f_{ij}} & & \downarrow{\scriptstyle g_{ij}} \\ M \otimes_A B_j & \xrightarrow{u_j} & N \otimes_A B_j \end{array}$$

Notre élément du noyau qui est la classe d'un élément de $M \otimes_A B_i$ est envoyé par u_B (après identification) sur la classe d'un élément de $N \otimes_A N_i$ qui n'est pas nécessairement nul dans $N \otimes_A N_i$ mais dans la limite inductive, autrement dit dans un $N \otimes_A N_j$ pour $j \geqslant i$. Mais alors, en poussant x_i dans $M \otimes_A B_j$, on obtient un élément du noyau de u_j qui est réduit à 0. Comme (i, x_i) est équivalent à l'élément $(j, f_{ij}(x_i))$ qui est nul, on en déduit que la classe de (i, x_i) est nulle dans la limite projective et par conséquent que $x = 0$ et que u_B est injective.

4. Comme on l'a vu en cours, le résultat est déjà faux avec $B = \mathbf{Z}/n\mathbf{Z}$, en considérant l'injection de $\mathbf{Z}$ dans $\mathbf{Q}$.