Algèbre Commutative 2023/2024
T.D.4

Exercice 1:
(1) Si $n \geq 2$ est un entier, montrer que la suite de $\mathbb{Z}$-modules $0 \to \mathbb{Z} \xrightarrow{n\cdot} \mathbb{Z} \to \mathbb{Z}/n \to 0$ n'est pas scindée.
(2) On considère les structure de $\mathbb{Z}[X]$-modules suivantes sur $\mathbb{Z}^2$
   (a) $X \cdot (a,b) = (a+b, b)$;
   (b) $X \cdot (a,b) = (b,a)$.
   Dans le cas (a), la suite exacte courte de $\mathbb{Z}[X]$-modules

$$0 \to \mathbb{Z} \xrightarrow{a \to (a,0)} \mathbb{Z}^2 \to \mathbb{Z} \to 0$$

   est-elle scindée? Même question avec la suite exacte courte de $\mathbb{Z}[X]$-modules

$$0 \to \mathbb{Z} \xrightarrow{a \to (a,a)} \mathbb{Z}^2 \to \mathbb{Z} \to 0$$

   dans le cas (b). Que se passe-t-il si on remplace $\mathbb{Z}$ par $\mathbb{Q}$?

Commençons par calculer la structure de $\mathbb{Z}[X]$-module sur le noyau et le quotient de chacune des suites exactes courtes. Pour (a), on a $X \cdot 1 = X \cdot (1,0) = (1,0) = 1$ sur le noyau et $X \cdot \overline{(0,b)} = \overline{X \cdot (0,b)} = \overline{(b,b)} = \overline{(0,b)}$ donc aussi $X \cdot 1 = 1$ sur le quotient. Pour (b), on a $X \cdot 1 = X \cdot (1,1) = (1,1) = 1$ sur le noyau et comme dans le quotient on a $\overline{(a,b)} + \overline{(b,a)} = 0$, $X \cdot \overline{(a,b)} = \overline{X \cdot (a,b)} = \overline{(b,a)} = -\overline{(a,b)}$ *i.e.* $X \cdot 1 = -1$ sur le quotient. Dans le cas, si la suite exacte courte de $\mathbb{Z}[X]$-module était scindée, $\mathbb{Z}^2$ serait le $\mathbb{Z}$-module trivial, ce qui n'est pas le cas... Dans le cas (b), si la suite exacte courte de $\mathbb{Z}[X]$-module était scindée disons par $s : \mathbb{Z} \to \mathbb{Z}^2$, on aurait $-s(\overline{(a,b)}) = s(X \cdot \overline{(a,b)}) = X \cdot s(\overline{(a,b)})$ donc si $s(\overline{(a,b)}) = (a,b) + (c,c)$ (on utilise $p \circ s = Id$ ici), $-(a,b) - (c,c) = (b,a) + (c,c)$ ou encore $a + b + 2c = 0$. Or pour $(a,b) = (0,1)$ (ou $(1,0)$), cette équation n'a pas de solution c dans $\mathbb{Z}$. Si on remplace $\mathbb{Z}$ par $\mathbb{Q}$, la suite exacte courte (a) reste non scindée (l'endomorphisme $(a,b) \to X \cdot (a,b)$ n'est pas diagonalisable) alors que la suite exacte courte (b) le devient (l'endomorphisme $(a,b) \to X \cdot (a,b)$ est diagonalisable).

Exercice 2: Soit

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

un diagramme commutatif de morphismes de A-modules dont les lignes horizontales sont exactes.
(1) Montrer que si α_1 est surjective et α_2, α_4 sont injectives alors α_3 est injective.
(2) Montrer que si α_5 est injective et α_2, α_4 sont surjectives alors α_3 est surjective.

(1) Le fait que α_4 est injectif et la commutativité du diagramme assurent que $\ker(\alpha_3) \subset im(u_2) = \ker(u_3)$ car $m_3 \in \ker(\alpha_3)$ implique $0 = v_3 \circ \alpha_3(m_3) = \alpha_4 \circ u_3(m_3)$ donc (α_4 injectif) $u_3(m_3) = 0$. En particulier $\ker(\alpha_3) = \ker(\alpha_3|^{im(u_2)})$ et on peut appliquer le serpent à:

$$\begin{array}{ccccccccc} & & M_1 & \xrightarrow{u_1} & M_2 & \xrightarrow{u_2} & im(u_2) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3|_{im(u_2)}} & & \\ 0 & \longrightarrow & N_1/\ker(v_1) & \xrightarrow{\overline{v}_1} & N_2 & \xrightarrow{v_2} & N_3 & & \end{array}$$

(2) Le fait que α_2 est surjectif et la commutativité du diagramme assurent que $\ker(v_3) \subset im(\alpha_3)$ car $im(v_2) = im(v_2 \circ \alpha_2)$ (α_2 surjectif) et $im(v_2 \circ \alpha_2) = im(\alpha_3 \circ u_2) \subset im(\alpha_3)$. Il suffit donc de montrer

que $M_3 \to N_3 \twoheadrightarrow N_3/\ker(v_3)$ est surjectif. Ce qui résulte du serpent appliqué à:

$$\begin{array}{ccccccc} M_3 & \xrightarrow{u_3} & M_4 & \xrightarrow{u_4} & im(u_4) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5|_{im(u_4)}} & & \\ 0 & \longrightarrow & N_3/\ker(v_3) & \xrightarrow{\overline{v}_3} & N_4 & \xrightarrow{v_4} & N_5 \end{array}$$

Exercice 3: (Noetherien vs artinien). Soit A un anneau.
(1) On suppose que l'idéal nul est produit d'un nombre fini $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ d'idéaux maximaux (non nécéssairement distincts). Montrer que A est artinien ssi A est noetherien.
(2) Montrer qu'un anneau artinien est toujours noetherien.

(1) On considère la suite décroissante de sous-A-modules

$$M_0 = M \supset M_1 = \mathfrak{m}_1 \supset M_2 = \mathfrak{m}_1\mathfrak{m}_1 \supset \cdots \supset M_{r-1} = \mathfrak{m}_1 \cdots \mathfrak{m}_{r-1} \supset M_r = 0$$

Pour $i = 1, \dots, r$, M_{i-1}/M_i est un $A/\mathfrak{m}_i =: k_i$-espace vectoriel. Par une induction immédiate, en utilisant que si $0 \to M' \to M \to M'' \to 0$ est une suite exacte courte de A-modules M est noetherien (resp. artinien) ssi M', M'' sont noetheriens (resp. artiniens), on a que M est noetherien (resp. artinien) ssi M_{i-1}/M_i est noetherien (resp. artinien), $i = 1, \dots, r$. Mais pour un espace vectoriel V sur un corps k on a V noetherien ssi $dim_k(V) < +\infty$ ssi V artinien.
(2) On a vu qu'un anneau artinien A ne posséde qu'un nombre fini d'idéaux premiers=maximaux $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ et que $\mathcal{J}_A = \sqrt{0} = \cap_{1\|eqi\leq r}\mathfrak{m}_i = \prod_{1\leq i\leq r} \mathfrak{m}_i$ (la dernière égalité est le lemme chinois) est nilpotent *i.e.* qu'il existe $N \geq 1$ tel que $\prod_{1\leq i\leq r} \mathfrak{m}_i^N = 0$. L'assertion résulte donc de la Question (1).

Exercice 4: (A-modules simples). Soit A un anneau. On dit qu'un A-module M est simple s'il est non nul et si ses seuls sous-A-modules sont $\{0\}$ et M.
(1) Montrer que si M_1, M_2 sont deux A-modules simples tout morphisme de A-modules $f : M_1 \to M_2$ est soit nul soit un isomorphisme.
(2) Montrer qu'à isomorphisme près, les A-modules simples sont exactement les $A/\mathfrak{m}$ avec $\mathfrak{m} \in spm(A)$. Quels sont les A-modules simples d'un anneau principal?

(1) Soit $f : M_1 \to M_2$ un morphisme de A-modules non nul. Comme $\ker(f) \subsetneq M_1$ est un sous-A-module et que M_1 est simple, on a forcément $\ker(f) = 0$. De même, comme $0 \subsetneq im(f) \subset M_2$ est un sous-A-module et que M_2 est simple, on a forcément $im(f) = M_2$.
(2) On peut déjà observer que
- Tout A-module de la forme s $A/\mathfrak{m}$ est simple. En effet, plus généralement, si $I \subset A$ est un idéal, la projection canonique $p_I : A \twoheadrightarrow A/I$ induit une bijection $M \subset A/I \mapsto p_I^{-1}(M) \subset A$ (d'inverse $J \subset A \mapsto I/J \subset A/I$) entre les sous-$A$-modules de A/I et les sous-A-modules (= idéaux) de A qui contiennent I. Donc A/I est un A-module simple si et seulement si les seuls idéaux de A qui contiennent I sont I et A *i.e.* si et seulement si $I \in spm(A)$.
- Pour tout $\mathfrak{m}, \mathfrak{m}' \in spm(A)$, $A/\mathfrak{m}$ et $A/\mathfrak{m}'$ sont isomorphes comme A-modules si et seulement si $\mathfrak{m} = \mathfrak{m}'$. En effet, supposons qu'on ait un isomorphisme de A-modules $\phi : A/\mathfrak{m} \tilde{\to} A/\mathfrak{m}'$. Comme $\overline{1} \neq \overline{0}$ dans $A/\mathfrak{m}$ on a forcément $\phi(\overline{1}) \neq \overline{0}$ dans $A/\mathfrak{m}'$ *i.e.* $\phi(\overline{1}) = \overline{a}$ pour un certain $a \notin \mathfrak{m}'$. Or, pour tout $\alpha \in \mathfrak{m}$ on a d'une part $\phi(\overline{\alpha}) = \phi(\overline{0}) = \overline{0}$ et, d'autre part, $\phi(\overline{\alpha}) = \phi(\alpha \cdot \overline{1}) = \alpha \cdot \phi(\overline{1}) = \overline{\alpha a}$. Donc $\alpha a \in \mathfrak{m}'$ et comme $a \notin \mathfrak{m}'$ avec $\mathfrak{m}'$ premier (car maximal), $\alpha \in \mathfrak{m}'$. Cela montre que $\mathfrak{m} \subset \mathfrak{m}'$ et donc, par maximalité de $\mathfrak{m}$, $\mathfrak{m} = \mathfrak{m}'$.

Soit maintenant M un A-module simple. Comme M est non nul, on peut choisir $0 \neq m \in M$. Comme $0 \subsetneq Am \subset M$ est un sous-A-module et que M est simple, on a forcément $Am = M$. Considérons le morphisme surjectif de A-modules $L_m : A \twoheadrightarrow Am = M$, $a \mapsto am$. Son noyau $I := \ker(L_m) \subset A$ est un idéal de A et par prop. univ. du quotient $L_m : A \twoheadrightarrow Am = M$ se factorise en un isomorphisme de A-modules $A/I \tilde{\to} M$. Mais comme M est simple, $I \in spm(A)$.

Exercice 5: Soit A un anneau. Pour tout $X = (X_{i,j})_{1\leq i,j\leq r} \in M_r(A)$, on définit $det(X) = \sum_{\sigma\in\mathcal{S}_r} \epsilon(\sigma) \prod_{1\leq j\leq r} X_{\sigma(j),j}$ et on rappelle la formule classique ${}^tCom(X)X = det(X)I_r$, où $Com(X) \in M_r(A)$ est la comatrice de X définie par $Com(X)_{i,j} = (-1)^{i+j} det(X[i,j])$ et $X[i,j] \in M_{r-1}(A)$ est la matrice obtenue à partir de X en supprimant la i-ème ligne et la j-ème colonne. On regarde X comme un morphisme de A-modules $X : A^r \to A^r$, $C \mapsto XC$.

(1) Montrer que les PSSE:

(i) $X : A^r \to A^r$ est surjectif;
(ii) $X : A^r \to A^r$ est un isomorphisme;
(iii) $det(X) \in A^\times$.

(2) Montrer que les PSSE:

(i) $X : A^r \to A^r$ est injectif;
(ii) $det(X) \in A \setminus A_{tors}$.

(1) (iii) $\Rightarrow$ (ii) résulte de ${}^tCom(X)X = det(X)I_r$ et (ii) $\Rightarrow$ (i) est tautologique. Pour (i) $\Rightarrow$ (iii), considérons la A-base canonique $e_i = (\delta_{i,j})_{1\leq j\leq r}$, $i = 1,\dots,r$ de A^r. Comme$X : A^r \to A^r$ est surjectif, pour chaque $i = 1,\dots,r$ il existe $\epsilon_i \in A^r$ tel que $X\epsilon_i = e_i$. Ecrivons $\epsilon_j = \sum_{1\leq i\leq r} Y_{i,j}e_i$ de sorte qu'en posant $Y = (Y_{i,j})_{1\leq i,j\leq r} \in M_r(A)$ la relation $X\epsilon_i = e_i$, $i = 1,\dots,r$ devienne $XY = I_r$. Donc $det(X)det(Y) = det(XY) = det(I_r) = 1$, ce qui montre bien que $det(X) \in A^\times$.

(2) (ii) $\Rightarrow$ (i) résulte encore de ${}^tCom(X)X = det(X)I_r$. Pour (i) $\Rightarrow$ (ii), raisonnons par l'absurde. Si $det(A)$ est de torsion il existe $0 \neq a \in A$ tel $adet(A) = 0$. Soit $s \leq r$ le plus grand entier tel qu'il existe une matrice e Y de taille $s \times s$ extraite de X et telle que $adet(Y) \neq 0$; on veut montrer que $s = r$. Déjà, comme $X : A^r \to A^r$ est injectif, il existe au moins un coefficient $X_{i,j}$ tel que $X_{i,j}a \neq 0$ donc $s \geq 1$. Supposons $s < r$. Quitte à multiplier X à gauche et à droite par des matrices de permutations, opsq $Y = (X_{i,j})_{1\leq i,j\leq s}$. Pour $k = 1,\dots,r$, notons $Y[k] \in M_{s+1}(A)$ la matrice définie par $Y[k]_{i,j} = Y_{i,j} = X_{i,j}$, $1 \leq i,j \leq s$, $Y[k]_{i,s+1} = X_{i,s+1}$, $i = 1,\dots,s$ et $Y[k]_{s+1,j} = X_{k,j}$, $j = 1,\dots,s+1$. Par maximalité de s on a $adet(Y[k]) = 0$, $k = s+1,\dots,r$ et comme pour $k = 1,\dots,s$ les matrices $Y[k]$ ont deux lignes égales, on a $det(Y[k]) = 0$ donc *a fortiori* $adet(Y[k]) = 0$. En développant selon la dernière ligne, $adet(Y[k]) = \sum_{1\leq j\leq s+1}(-1)^{s+1+j}a_{k,j}adet(Y[k][s+1,j])$, $k = 1,\dots,r$ implique que $C \in A^r$ défini par $C_i = (-1)^i adetY[k][s+1,i]$, $i = 1,\dots,s+1$, $C_i = 0$, $i = s+2,\dots,r$ est dans $\ker(X)$. Mais $C_{s+1} = (-1)^{s+1}adetY \neq 0$ par définition de Y.

Exercice 6: (Lemme de Nakayama). Soit A un anneau et M un A-module *de type fini*.

(1) Soit $I \subset A$ un idéal tel que $IM = M$. Montrer qu'il existe $a \in I$ tel que $(1+a)M = 0$;
(2) Si on suppose de plus que I est contenu dans le radical de Jacobson de A montrer que $IM = M$ implique $M = 0$.

(1) Fixons un système $m_1,\dots,m_r$ de générateurs de M comme A-modules. L'égalité $M = IM$ assure que tout $m \in M$ s'écrit comme combinaison linéaire à coefficients dans I des $m_1,\dots,m_r$. Cela s'applique en particulier à chacun des m_j, $j = 1,\dots,r$: il existe une matrice $r\times r$ $U = (u_{i,j})_{1\leq i,j\leq r}$ à coefficients dans I telle que $m_j = \sum_{1\leq i\leq r} u_{i,j}m_i$, $j = 1,\dots,r$. Notons $p : \oplus_{1\leq i\leq r} Am_i \twoheadrightarrow \sum_{1\leq i\leq r} Am_i = M$ le morphisme canonique. On a donc $p\circ(Id-U) = 0$ donc $p\circ(Id-U){}^tCom(Id-U) = det(Id-U)p = 0$. Comme $p : \oplus_{1\leq i\leq r} Am_i \twoheadrightarrow M$ est surjectif, cela montre que $det(Id-U)M = 0$. Or $det(Id-U) \in 1+I$; cela se voit par exemple en développant $det(Id-U)$ avec la formule $det(Id-U) = \sum_{\sigma\in\mathcal{S}_r} \epsilon(\sigma)\prod_{1\leq j\leq r}(\delta_{\sigma(j),j} - a_{\sigma(j),j})$: tous les termes de la somme sont dans I sauf celui correspondant à $\sigma = Id$ qui est dans $1+I$.
(2) Il suffit de se rappeler que si I est contenu dans le radical de Jacobson de A, $1+I \subset A^\times$ (en effet, s'li existe $a \in I$ tel que $1+a \notin A^\times$ il existe $\mathfrak{m} \in spm(A)$ tel que $1+a \in \mathfrak{m}$ donc $1 = (1+a)-a \in \mathfrak{m}$: contradiction.

Exercice 7: (A-Modules projectifs). Soit A un anneau et P un A-module.

(1) Montrer que les PSSE
   (a) Pour tout morphisme surjectif de A-modules $v : M \twoheadrightarrow M''$ et pour tout morphisme de A-modules $f : P \to M''$ il existe un morphisme de A-modules $\widetilde{f} : P \to M$ tel que $v \circ \widetilde{f} = f$;
   (b) Pour tout morphisme surjectif de A-modules $v : M \twoheadrightarrow P$ il existe un morphisme de A-modules $s : P \to M$ tel que $v \circ s = Id_P$;
   (c) Il existe un A-module Q tel que $P \oplus Q$ soit un A-module libre.

   On dit qu'un A-module qui vérifie les propriétés équivalentes (a), (b), (c) est un A-module projectif.
(2) Montrer que tout A-module est quotient d'un A-module projectif.

Exercice 8: (A-Modules injectifs). Soit A un anneau et I un A-module.

(1) [Utilise Zorn] Montrer que les PSSE
   (a) Pour tout morphisme injectif de A-modules $u : M' \hookrightarrow M$ et pour tout morphisme de A-modules $f : M' \to I$ il existe un morphisme de A-modules $\widetilde{f} : M \to I$ tel que $\widetilde{f} \circ u = f$;
   (b) Pour tout idéal J de A et tout morphisme de A-modules $f : J \to I$ il existe un morphisme de A-modules $\widetilde{f} : A \to I$ tel que $\widetilde{f}|_J = f$.

   On dit qu'un A-module qui vérifie les propriétés équivalentes (a), (b) est un A-module injectif.
(2) Montrer que $\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module injectif mais que $\mathbb{Q}$ et $\mathbb{Q}/\mathbb{Z}$ sont des $\mathbb{Z}$-modules injectifs;
(3) Montrer qu'un produit de A-modules injectifs est injectif.
(4) Montrer que tout $\mathbb{Z}$-module M se plonge dans un $\mathbb{Z}$-module injectif.

Rem: L'énoncé reste vrai pour un anneau A quelconque mais la preuve est plus astucieuse.

(1) (b) est un cas particulier de (a) donc (a) $\Rightarrow$ (b) est tautologique. Inversement, Introduisons l'ensemble $\mathcal{E}$ des couples (N, ϕ) où $N \subset \mathcal{E}$ est un sous-A-module et $\phi : N \to I$ est un morphisme de A-modules tel que $\phi \circ u = f$ que l'on ordonne par $(N_1, \phi_1) \leq (N_2, \phi_2)$ si $N_1 \subset N_2$ et $\phi_2 \ddot{\imath}_{N_1} = \phi_1$. On a $\mathcal{E} \neq \emptyset$ puisque $(u(N), f \circ (u|^{u(N)})^{-1}) \in \mathcal{E}$ et on vérifie immédiatement que $(\mathcal{E}, \leq)$ est ordonné inductif donc, par Zorn, contient un élément maximal (N, ϕ). Si on montre que $N = M$ on aura gagné. Sinon, fixons $m \in M \setminus N$. On veut prolonger $\phi : N \to I$ à $N + Am$. Pour cela, introduisons l'idéal $J := L_m^{-1}(N) := \{a \in A \mid am \in N\}$ et considérons le morphisme de A-module $v : J \to I$, $a \mapsto \phi(am)$. Par (b) il existe un unique morphisme de A-modules $\widetilde{v} : A \to I$ tel que $\widetilde{v}|_J = v$. Par prop. univ de la somme directe on en déduit un morphisme de A-modules $F : N \oplus Am \to I$, $n \oplus am \mapsto \phi(n) + \widetilde{v}(a)$. Par définitinon de J, on a $J \ker(N \oplus Am \twoheadrightarrow N + Am)$, $a \mapsto (-am) \oplus am$ et pour tout $a \in J$ $F((-am) \oplus am) = -\phi(am) + \widetilde{v}(a) = -\phi(am) + \phi(am) = 0$. Cela montre que $F : N \oplus Am \to I$, $n \oplus am \mapsto \phi(n) + \widetilde{v}(a)$ se factorise de façon unique en un morphisme de A-modules $\widetilde{f} : N + An \to I$ et, par construction, $\widetilde{f}|_N = \phi$, ce qui contredit la maximalité de (N, ϕ).

(2) Prenons $u : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto 2n$ et $f = Id : \mathbb{Z} \to \mathbb{Z}$. S'il existait un morphisme de A-modules $\widetilde{f} : \mathbb{Z} \to \mathbb{Z}$ tel que $\widetilde{f} \circ u = f$ on aurait $2\mathbb{Z} = \mathbb{Z}$: contradiction. Pour $I = \mathbb{Q}$ ou $\mathbb{Q}/\mathbb{Z}$, le point essentiel est que I est divisible *i.e.* pour tout $n \in \mathbb{Z}$ la multiplication par n $I \to I$ est surjective. Donc $J := a\mathbb{Z} \hookrightarrow \mathbb{Z}$ est l'inclusion d'un idéal et $u : J \to I$ un morphisme quelconque de $\mathbb{Z}$-modules, il suffit de choisir $\nu \in I$ tel que $a\nu = u(a)$ et de considérer l'unique morphisme de $\mathbb{Z}$-module $\widetilde{u} : \mathbb{Z} \to I$, $1 \mapsto \nu$. Par construction, on a bien $\widetilde{u}|_J = u$.

(3) C'est la propriété universelle du produit: si I_k, $k \in K$ est une famille de A-module injectif, pour tout morphisme injectif de A-modules $u : M' \hookrightarrow M$ et pour tout morphisme de A-modules $f : M' \to \prod_{k \in K} I_k$ notons $f_k := p_k \circ f : M' \to I_k$. Comme I_k est un A-module injectif, il existe un morphisme de A-modules $\widetilde{f_k} : M \to I_k$ tel que $\widetilde{f_k} \circ u = f$. Par prop. univ. du produit il existe alors un unique morphisme de A-module $\widetilde{f} : M \to \prod_{k \in K} I_k$ tel que $p_k \circ \widetilde{f} = \widetilde{f_k}$, $k \in K$. Par construction, on a $\widetilde{f} \circ u = f$.

(4) On consdère une présentation $0 \to R \to \mathbb{Z}^{(I)} \to M \to 0$ de M. Le morphisme canonique de $\mathbb{Z}$-modules $\mathbb{Z}^{(I)} \hookrightarrow \mathbb{Q}^{(I)} \twoheadrightarrow \mathbb{Q}^{(I)}/R$ se factorise en un morphisme injectif de $\mathbb{Z}$-modules $M \simeq \mathbb{Z}^{(I)}/R \hookrightarrow \mathbb{Q}^{(I)}/R$. Le $\mathbb{Z}$-module $\mathbb{Q}^{(I)}/R$ étant divisible, il est injectif par le même argument que celui utilisé pour $\mathbb{Q}$ et $\mathbb{Q}/\mathbb{Z}$.

Exercice 9: Soit A un anneau principal de corps des fractions K et soit $G \subset \mathrm{GL}_n(K)$ un sous-groupe. On suppose qu'il existe $0 \neq a \in A$ tel que $aG \subset M_n(A)$. Montrer qu'il existe $g \in \mathrm{GL}_n(K)$ tel que $gGg^{-1} \subset M_n(A)$. En déduire que pour tout sous-groupe fini $G \subset \mathrm{GL}_n(\mathbb{Q})$ il existe $g \in \mathrm{GL}_n(\mathbb{Q})$ tel que $gGg^{-1} \subset M_n(\mathbb{Z})$.

Notons $M := A^n \subset V := K^n$ et $N := \sum_{g \in G} gM \subset V$. Par construction N est un sous-A-module G-stable de V qui contient M (prendre $g = Id$) et, par hypothèse, $aN \subset M$, ce qui se réécrit $N \subset aM$. Mais aM est un A-module libre de rang n. Donc comme A est principal, N est aussi un A-module libre de rang $r \leq n$. Comme N contient M, on a en fait $r = n$. On a donc un isomorphisme de A-modules $\phi : A^{\oplus n} \tilde{\to} N$. Pour tout $g \in G$ on a donc $g\phi(A^{\oplus n}) = gN \subset N = \phi(A^{\oplus n})$ *i.e.* $\phi^{-1}g\phi(A^{\oplus n}) \subset A^{\oplus n}$. En termes matriciels, si on note $\phi(e_j) = \sum_{1 \leq i \leq n} \phi_{i,j} e_i$ et $\Phi = (\phi_{i,j})_{1 \leq i,j \leq n} \in \mathrm{GL}_n(K)$, cela revient à $\Phi^{-1} G \Phi \subset M_n(A)$. La deuxième partie de l'énoncé est le cas particulier $A = \mathbb{Z}$ en observant que si $G \subset \mathrm{GL}_n(\mathbb{Q})$ est fini, on peut prendre pour a le produit des dénominateurs des coefficients non nuls des éléments de G.

Les exercices qui suivent sont des applications du théorème de structure des modules de type fini sur les anneaux principaux.

Exercice 10: (Classification des classes de conjugaison par les invariants de similitude) On rappelle que si V est un k-espace vectoriel de dimension finie tout endomorphisme $u : V \to V$ définit une structure de $k[T]$ module V_u sur V par $P(T)v = P(u)(v)$, $P \in k[T]$, $v \in V$. Le $k[T]$-module V_u est évidemment de type fini et de torsion. Il existe donc une unique suite de polynômes $P_{u,1}|P_{u,2}|\cdots|P_{u,r_u}$ telle que

$$V_u \simeq k[T]/P_{u,1} \oplus \cdots \oplus k[T]/P_{u,r_u}.$$

On dit que la suite $P_{u,1}|P_{u,2}|\cdots|P_{u,r_u}$ est la suite des *invariants de similitude* de l'endomorphisme u.

(1) Soit $u, u' : V \to V$ deux endomorphismes. Montrer qu'il existe $\phi \in \mathrm{Aut}_k(V)$ tel que $u = \phi \circ u' \circ \phi^{-1}$ si et seulement si u et u' ont mêmes invariants de similitude.
(2) Calculer le polynôme minimal et le polynôme caractéristique de u en fonction de sa suite d'invariants de similitude. Montrer plus précisément qu'il existe une base du k-espace vectoriel V dans laquelle u a pour matrice la matrice diagonale par blocs dont les blocs diagonaux sont les matrices compagnons des $P_{u,i}$.
(3) Calculer le nombre de classes de conjugaison (sous $\mathrm{GL}_n(\mathbb{F}_q)$) dans $M_n(\mathbb{F}_q)$, dans $\mathrm{GL}_n(\mathbb{F}_q)$.

(1) Par définition, un automorphisme $\phi \in \mathrm{Aut}_k(V)$ tel que $u = \phi \circ u' \circ \phi^{-1}$ est la même chose qu'un isomorphisme de $k[X]$-modules $\phi : V_{u'} \tilde{\to} V_u$.
(2) Si on se fixe un isomorphisme de $k[X]$-module $\phi : V_u \tilde{\to} k[T]/P_{u,1} \oplus \cdots \oplus k[T]/P_{u,r_u}$ et qu'on prend pour k-base ϵ l'image inverse par ϕ de la concaténation des k-bases $\overline{1}, \ldots, \overline{X}^{d_{u,i}-1}$ (où $d_{u,i} = deg(P_{u,i})$), $i = 1, \ldots, r_u$, la matrice de u dans ϵ est de la forme demandée. En observant que le polynôme minimal de la matrice compagnon d'un polynôme P est P (puisque, par division euclidienne, P est le polynôme minimal de T agissant par multiplication à droite sur $k[T]/P...$), on en déduit que le polynôme minimal de u est le ppcm des $P_{u,i}$, $i = 1, \ldots, r_u$ et que le polynôme caractéristique de u est le produit des $P_{u,i}$, $i = 1, \ldots, r_u$.
(3) Cela revient à compter les suites d'invariants de similitude (resp. les suites d'invariants de similitude dont le terme constant est non nul)...

Exercice 11: (Théorème de la base adaptée) Soit A un anneau principal, M un A-module libre de rang r et $N \subset M$ un sous-A-module. L'objectif de cet exercice est de montrer qu'il existe un unique entier $0 \leq s \leq r$, une unique suite $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ d'idéaux de A et $m_1, \ldots, m_r \in M$ tels que

$$N = \bigoplus_{1 \leq i \leq s} Ad_i m_i \subset \bigoplus_{1 \leq i \leq r} Am_i = M.$$

(1) Justifier l'unicité (sous réserve d'existence).
(2) Notons $\mathcal{E}$ l'ensemble des $\lambda(N)$, $f \in \mathrm{Hom}_A(M, A)$. Montrer que $\mathcal{E}$ possède un élément maximal I pour l'inclusion.
(3) Fixons $f \in \mathrm{Hom}_A(M, A)$ tel que $I = f(N) = Ad_1$ et $n_1 \in N$ tel que $f(n_1) = d_1$. Montrer que pour tout $g \in \mathrm{Hom}_A(M, A)$, $g(n_1) \in I$.
(4) Montrer qu'il existe $m_1 \in M$ tel que $n_1 = d_1 m_1$. En déduire que $M = Am_1 \oplus \ker(f)$ et $N = Ad_1 m_1 \oplus \ker(f) \cap N$.
(5) Conclure par récurrence sur le rang de M.

(1) L'unicité de s et de la suite $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ résulte du théorème de structure car $r - s$ est le rang de la partie libre de M/N et $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_s$ est la suite des invariants de la partie de torsion de M/N.
(2) Comme A est noetherien, $\mathcal{E}$ contient au moins un élément maximal $f(N) = Ad_1 = Af(n_1)$.
(3) Cela résulte de la maximalité de $f(N)$ dans $\mathcal{E}$: pour tout $g : M \to A$ on a $g(n_1) \in g(N) \subset f(N) = Ad_1$.
(4) Choisissons une A-base quelconque $\mu_1, \ldots, \mu_r$ de M et notons $p_i : M \twoheadrightarrow A\mu_i \simeq A$ la projection correspondante sur la i-ème coordonnée. On a, dans cette base, $n_1 = \sum_{a \leq i \leq r} a_i \mu_i$ et en appliquant (3) aux p_i, on obtient que d_1 divise a_i, $i = 1, \ldots, r$. Donc en écrivant $a_i = d_1 b_i$ pour un certain $b_i \in A$, $i = a, \ldots, r$, on peut prendre $m_1 = \sum_{1 \leq i \leq r} b_i \mu_i$. De $d_1 m_1 = n_1$, on déduit $f(d_1 m_1) = d_1 f(m_1) = f(n_1) = d_1$ donc comme A est intègre, $f(m_1) = 1$. Cela donne une décomposition $M \simeq \ker(f) \oplus Am_1$ ($m = (m - f(m)m_1) + f(m)m_1$ telle que $N = \ker(f) \cap N \oplus Ad_1 m_1$.
(5) On peut donc appliquer l'hypothèse de recurrence à $\ker(f) \cap N \subset \ker(f)$ puisqu'on sait que $\ker(f)$ est un A-module libre de rang r pour obtenir une suite $A \supsetneq Ad_2 \supset \cdots \supset Ad_s \supsetneq 0$ d'idéaux de A et $m_2, \ldots, m_r \in \ker(f)$ tels que

$$\ker(f) \cap N = \bigoplus_{2 \leq i \leq s} Ad_i m_i \subset \bigoplus_{2 \leq i \leq r} Am_i = \ker(f).$$

Il reste à voir que $Ad_1 \supset Ad_2$. Ecrivons $Ad_1 + Ad_2 = Ad$ et fixons $u_1, u_2 \in A$ tels que $u_1 a_1 + u_2 a_2 = d$. Avec $g := u_1 pr_1 + u_2 pr_2 : M \to A$ et $\nu := d_1 m_1 + d_2 m_2 \in N$ on a $g(\nu) = c$ donc $f(N) = Ad_1 \subset Ac = Ag(\nu) \subset g(N)$. Par maximalité de $f(N)$ dans $\mathcal{E}$ on en déduit $Ad_1 = Ac$ *i.e.* $Ad_1 \supset Ad_2$.

Exercice 12: (Classes d'équivalence) On considère l'action de $\mathrm{GL}_n(A) \times \mathrm{GL}_m(A)$ sur $M_{n,m}(A)$ donnée par $(P, Q) \cdot M = PMQ^{-1}$. Montrer que l'ensemble des classes d'équivalence $M_{n,m}(A)/\mathrm{GL}_n(A) \times \mathrm{GL}_m(A)$ est classifié par les suites $Ad_1 \supset Ad_2 \supset \cdots \supset Ad_n$ d'idéaux de A. Noter que dans le cas où $A = k$ est un corps commutatif, on retrouve le thèorème de classification des classes d'équivalence par le rang de la matrice.

On suppose $m \geq n$. Notons $M := A^m$, $N := A^n$ et soit $f : M \to N \in \mathrm{Hom}_A(M, N)$. Par le théorème de la base adaptée pour $f(M) \subset N$ il existe un unique $0 \leq r \leq n$, une unique suite d'idéaux $A \supsetneq Ad_1 \supset Ad_2 \supset \cdots \supset Ad_r \supsetneq 0$ et des éléments $\nu_1, \ldots, \nu_n \in N$ tels que

$$f(M) = \oplus_{1 \leq i \leq r} Ad_i \nu_i \subset \oplus_{1 \leq i \leq n} A\nu_i = N.$$

Comme $f(M)$ est un A-module libre, la suite exacte courte

$$0 \to \ker(f) \to M \xrightarrow{f} f(M) \to 0$$

est scindée. Notons $s : f(M) \to M$ un scindage. On a alors $M \simeq \ker(f) \oplus s(f(N))$. Comme A est principal et M est un A-module libre, $\ker(f) \subset M$ est encore un A-module libre. En concaténant la A-base $s(d_1\nu_1), \ldots, s(d_{\nu n})$ de M et une A-base de $\ker(f)$, on obtient une A-base $\mu_1, \ldots, \mu_n$ de M. La matrice de f dans les bases $\mu_1, \ldots, \mu_m$ et $\nu_1, \ldots, \nu_n$ est de la forme

$$D(d_1, \ldots, d_n) := \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 \\ 0 & d_2 & & 0 & 0 \\ 0 & & \cdots & & \\ 0 & & & d_n & 0 \end{pmatrix}.$$

On a donc montré que si $f, g : M \to N$ sont des morphismes de A-modules tels que $N/f(M) \simeq N/g(M)$ alors f, g sont équivalents. La réciproque est presque immédiate car s'il existe des automorphismes $\phi \in Aut_A(M)$, $\psi \in Aut_A(N)$ tels que $f \circ \phi = \psi \circ g$ alors $\psi : N \tilde{\to} N$ se restreint en un isomorphisme de A-modules $\psi : g(M) \tilde{\to} f(\phi(M)) = f(M)$ donc induit un isomorphisme de A-modules $\overline{\psi} : N/g(M) \tilde{\to} N/f(M)$.

Exercice 13: Soit M un $\mathbb{Z}$-module libre de rang fini m et $\phi \in \mathrm{End}_{\mathbb{Z}}(M)$ tel que $\phi \otimes \mathbb{Q} \in \mathrm{Aut}_{\mathbb{Q}}(M \otimes \mathbb{Q})$ est inversible. Montrer que $\phi(M) \subset M$ est d'indice fini et calculer $[M : \phi(M)]$.

Par le théorème de la base adaptée, on peut trouver des $\mathbb{Z}$-bases ϵ, ϵ' de M telles que, dans ces bases, la matrice de ϕ est de la forme $D(d_1, \ldots, d_m)$ avec $d_1 | \cdots | d_m$ des entiers > 0 puisque $\phi \otimes \mathbb{Q}$ est un automorphisme. On a donc $det(\phi) = \pm d_1 \cdots d_m = \pm[M : \phi(M)]$ (ici le signe $\pm$ vient de ce que les déterminants des matrices de changement de base sont dans $\mathbb{Z}^\times = \{\pm 1\}$).