TD n°3.

Tous les anneaux sont ici supposés commutatifs et unitaires.
On pourra commencer par les exercices 2, 11, 29, 33 et 44.

Exercice 1. Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module libre. Plus généralement, montrer que si tout A-module est libre, alors A est un corps (ou l'anneau nul).

Solution. Si $m \in \mathbb{Z}/n\mathbb{Z}$, $n \cdot m = 0$, donc $\{m\}$ n'est pas une famille libre. Donc toute partie libre de $\mathbb{Z}/n\mathbb{Z}$ est vide, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas libre.
Plus généralement, si $I \neq 0$ est un idéal de A et $\bar{a} \in A/I$, alors $i \cdot \bar{a} = 0$ pour tout élément de $I \neq \{0\}$ donc $\bar{a}$ n'est pas libre, donc toute famille libre de A/I est vide. Donc A/I ne peut être libre que si $I = 0$ ou $A/I = 0$. Donc si tout A-module est libre, A n'a que 0 et A comme idéaux, donc est un corps.

Exercice 2. Donner des exemples :
(i) De A-modules non libres,
(ii) d'une famille libre à n éléments dans A^n qui n'est pas une base,
(iii) d'une partie génératrice minimale qui ne soit pas une base,
(iv) de sous-module n'ayant pas de supplémentaire,
(v) de module libre ayant un sous-module qui n'est pas libre.

Solution. (i) Il y en a beaucoup, par exemple les $\mathbb{Z}$-modules $\mathbb{Z}/n\mathbb{Z}$ pour $n \neq 0$. Ils ne sont pas libres car tous les éléments sont de torsion : n annule tous les éléments. Plus généralement si I est un idéal propre et non nul de A, alors A/I n'est pas libre. Un idéal non principal n'est pas libre non plus. On peut vérifier que $\mathbb{Q}$ n'est pas $\mathbb{Z}$-libre non plus. . .
(ii) Considérons $A = \mathbb{Z}$ et $n = 1$ et prenons un élément de $\mathbb{Z}$, par exemple 2. Alors 2 est sans torsion donc 2 est libre mais 2 n'engendre pas tout $\mathbb{Z}$. De façon plus générale, si on prend n éléments $m_i = (d_{i,j})$ de $\mathbb{Z}^n$, ils forment une famille libre si et seulement si $\det(d_{i,j}) \neq 0$ et une famille génératrice si et seulement si $\det(d_{i,j}) = \pm 1$. Par exemple $(1, 2)$ et $(0, 1)$ forment une famille libre et génératrice de $\mathbb{Z}^2$, en effet si $(x, y) \in \mathbb{Z}^2$ alors $(x, y) = x(1, 2) + (y - 2x)(0, 1)$ qui est une combinaison linéaire à coefficients entiers. Par contre les vecteurs $(1, 2)$ et $(1, 0)$ forment une famille libre mais non génératrice : le vecteur $(0, 1)$ s'écrit $\frac{1}{2}(1, 2) - \frac{1}{2}(1, 0)$ mais n'a pas d'écriture à coefficients entiers.
(iii) Soit encore $A = \mathbb{Z}$ et soit $M = \mathbb{Z}/2\mathbb{Z}$ qui est un A-module. Alors $Cl(1) \in \mathbb{Z}/2\mathbb{Z}$ est une famille génératrice évidement minimale mais non libre car $Cl(1)$ est annulé par 2 donc est un élément de torsion.
(iv) Soit encore $A = \mathbb{Z}$, soit $M = \mathbb{Z}$ et soit $N = 2\mathbb{Z}$ le sous-A-module de M. Le sous-module N n'a pas de supplémentaire. En effet, soit P un sous-module de M tel que $P \cap N = 0$. Soit $p \in P$, on a alors $2p \in P \cap N$ donc $2p = 0$ ce qui implique $p = 0$. Ainsi $P = 0$ est le seul sou-module de M qui peut être en somme directe avec N. Cependant $N \oplus (0) = N \neq M$.
(v) Soit $A = \mathbb{Z}/4\mathbb{Z}$ qui est libre sur lui-même et $M = 2\mathbb{Z}/4\mathbb{Z}$ le sous-module engendré par la classe de 2. On voit alors que M n'est pas libre, en effet sinon on aurait $M = (\mathbb{Z}/4\mathbb{Z})^k$ donc le cardinal de M serait $4k$, alors que le cardinal de M est 2.
On pourrait aussi montrer que $(X, Y) \subset k[X, Y]$ n'est pas libre sur $k[X, Y]$ (cf. exercice 4 pour une preuve plus générale).

Exercice 3. Soit A un anneau intègre et K son corps des fractions. On suppose que $K \neq A$ (c'est-à-dire que A n'est pas un corps), montrer que K n'est pas libre comme A-module.

Solution. Si x et y sont deux éléments de K, écrivons $x = \frac{a}{b}$ et $y = \frac{c}{d}$ avec a, b, c et d des éléments de A tels que $b \neq 0$ et $d \neq 0$. On a ainsi $bcx = ac = ady$. Si a ou c est non nul, cette relation prouve que la famille $\{x, y\}$ est liée. Si $a = c = 0$, on a $x = y = 0$ et la famille $\{x, y\}$ est encore liée.
Ainsi toute famille libre de K a au plus un élément. Comme $K \neq 0$, une famille génératrice de K a au moins un élément. Ainsi une base de K si elle existe a exactement un élément.
Soit donc $x \in K$, $x \neq 0$ et montrons que x n'engendre pas K comme A-module. Si c'était le cas, on aurait $x^2 \in Ax$ donc $x \in A$. Mais alors $Ax \subset A$ et comme x engendre K, on aurait $K \subset A$. C'est absurde.

Exercice 4. Montrer 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. Rappelons que les idéaux de A sont exactement les sous-A-modulede A.
Si I est un idéal principal de A engendré par un élément a non diviseur de 0, alors I est un module libre. En effet, $\{a\}$ est une famille génératrice et libre (car a n'est pas diviseur de 0) de I.
Réciproquement, soit $I \subset A$ un idéal qui est un sous-module libre de A. Soit $(a_j)_{j\in J}$ une base de I comme A-module. Comme I est non nul, on a J non vide. Supposons que J a au moins deux éléments, et soient a_j et a_k deux éléments distincts de la base. Alors on a

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

et comme la famille $\{a_k, a_j\}$ est libre ceci impose $a_j = 0$ et $-a_k = 0$, c'est-à-dire $a_j = a_k = 0$ ce qui est absurde puisqu'ils forment une famille libre. Ainsi J a un seul élément et la base $(a_j)_{j\in J}$ est donnée par une seul élément disons a. Comme $\{a\}$ forme une famille libre, l'élément a est sans torsion. Comme $\{a\}$ est une famille génératrice on a bien $I = (a)$ qui est principal.

Exercice 5. (i) Soit M un A-module libre de type fini et supposons $A \neq 0$. Montrer que toutes les bases de M ont le même cardinal.
Indice : choisir un idéal maximal de A et se ramener au cas des espaces vectoriel.
(ii) Trouver un module M tel que $M \simeq M \oplus M$.

Solution. (i) Il suffit de montrer que si $f : A^{(I)} \to A^{(J)}$ est un isomorphisme alors $\mathrm{Card}(I) = \mathrm{Card}(J)$. Soit $\mathfrak{m}$ un idéal maximal de A et $k = A/\mathfrak{m}$. Alors f envoie $\mathfrak{m}^{(I)}$ sur $\mathfrak{m}^{(J)}$, d'où un isomorphisme $A^{(I)}/\mathfrak{m}^{(I)} \to A^{(J)}/\mathfrak{m}^{(J)}$. Donc f induit un isomorphisme $k^{(I)} \to k^{(J)}$. Donc $\mathrm{Card}(I) = \mathrm{Card}(J)$.
(ii) Il suffit de prendre un ensemble infini et de considérer le A-modulelibre M de base I. Alors $M \oplus M$ est le A-modulelibre de base $I \coprod I$ (union disjointe). Comme I est infini, on peut trouver une bijection entre I et $I \coprod I$ d'où un isomorphisme entre M et $M \oplus M$.

Exercice 6. Soit k un corps, $P \in k[X]$ et $A = k[X]/(P)$.
(i) Quelle est la dimension de A comme k-espace vectoriel ? Donnez-en une base.
(ii) On pose $M = A^\vee = \mathrm{Hom}_k(A, k)$; donner une base de M.
(iii) Pour $f \in A$ et $u \in M$ on définit $f \cdot u \in M$ par $(f \cdot u)(g) = u(f \cdot g)$. Montrer que cette loi munit M d'une structure de A-module libre de rang 1. Donnez-en une base.

Solution. Soit $n = \deg P$.
(i) Montrons que A est de dimension $\deg P$ comme k-espace vectoriel et que la famille $\{1, Cl(X), \cdots, Cl(X^{n-1})\}$ en est une base. Soit $Q \in A$, la division euclidienne de Q par P donne $Q = PA + R$ avec R de degré $r < n$. On a alors $Cl(Q) = Cl(R)$. Or R est une combinaison linéaire de la famille $\{1, X, \cdots, X^{n-1}\}$ donc $Cl(Q) = Cl(R)$ est combinaison linéaire de la famille $\{1, Cl(X), \cdots, Cl(X^{n-1})\}$ qui est donc génératrice. Elle est libre, en effet si $\sum_{i=0}^{n-1} a_i Cl(X^i) = 0$ dans A, celà signifie que le polynôme $\sum_{i=0}^{n-1} a_i X^i$ est multiple de P, il doit donc être nul. Ainsi $a_i = 0$ pour tout i.
(ii) La base duale est $(u_0, \cdots, u_{n-1})$ où $u_i : A \to k$ est définie par $u_i(X^j) = 0$ si $i \neq j$ et $u_i(X^i) = 1$.
(iii) On peut supposer que P est unitaire, notons $P = X^n - a_{n-1}X^{n-1} - \cdots - a_0$. Montrons que $\varphi = u_{n-1}$ est une base de M comme A-module
On calcule $X^k \cdot \varphi$. On a

$$1 \cdot \varphi(\sum_{i=0}^{n-1} \lambda_i X^i) = \lambda_{n-1}$$

$$X \cdot \varphi(\sum_{i=0}^{n-1} \lambda_i X^i) = \varphi(\sum_{i=0}^{n-1} \lambda_i X^{i+1}) = \lambda_{n-1}a_{n-1} + \lambda_{n-2}$$

et par récurrence, si $0 \leq k \leq n-1$, alors $X^k \cdot \varphi(\sum_{i=0}^{n-1} \lambda_i X^i)$ est de la forme λ_{n-k} plus une combinaison linéaire de $\lambda_{n-k+1}, \cdots, \lambda_{n-1}$. Il en résulte que la matrice de $(\varphi, X \cdot \varphi, \cdots, X^{n-1} \cdot \varphi)$ dans la base $(u_{n-1}, \cdots, u_1, u_0)$ est triangulaire supérieure avec des 1 sur la diagonale. Elle est inversible si bien que tout élément de M s'écrit de manière unique comme combinaison linéaire de $\varphi, X \cdot \varphi, \cdots, X^{n-1} \cdot \varphi$. Ainsi φ est une base de M comme A-module.

Exercice 7. Soit A un anneau et T une matrice $n \times m$ à coefficients dans A. Cette matrice représente un homomorphisme de modules $u : A^m \longrightarrow A^n$. Posons $M = \mathrm{Coker}\, u = A^n/\mathrm{Im}(u)$.
(i) Montrer que $(0 : M) = (\mathrm{Im}(u) : A^n)$.
(ii) Montrer que si $m \geq n$ alors les mineurs maximaux de T (c'est à dire les déterminants des sous matrices $n \times n$ de T) appartiennent à $(0 : M)$.
Indice : traiter tout d'abord le cas $m = n$.

Solution. (i) Rappelons que $(\operatorname{Im} u : A^n) = \{a \in A \ / \ aA^n \subset \operatorname{Im} u\}$. Soit $a \in A$, on a $a \in (0 : M) = \operatorname{Ann}(M)$ si et seulement si pour tout $m \in M$, on a $am = 0$. Soit $x \in A^n$ et $m = Cl(x) \in M$. On a alors $aCl(x) = 0$ dans M donc $ax \in \operatorname{Im} u$ et ainsi $a \in (\operatorname{Im} u : A^n)$.
Réciproquement, si $a \in (\operatorname{Im} u : A^n)$, alors pour tout $x \in A^n$, on a $ax \in \operatorname{Im} u$. Soit $m \in M$, on a $m = Cl(x)$ pour un $x \in A^n$. Alors $am = Cl(ax) = 0$ car $ax \in \operatorname{Im} u$. Ainsi $a \in (0 : M)$.
(ii) Supposons d'abord que $m = n$. Alors on a $T\,{}^t\mathrm{Com}(T) = {}^t\mathrm{Com}(T)T = \det(T)I_n$ où I_n est la matrice identité de taille $n \times n$. Si $x \in A^n$, on a $\det(T)x = T\,{}^t\mathrm{Com}(T)x \in \operatorname{Im} u$ et donc $\det(T) \in (\operatorname{Im} u, A^n) = (0 : M)$.
Si $m > n$, choisissons une partie $I \subset \{1, \cdots, m\}$ de cardinal n et notons T_I la matrice extraite de T donc on n'a gardé que les colonnes d'indice dans I. On constate que T_I est la matrice de la restriction de u à $A^I = \{x = (x_1, \cdots, x_m) \in A^m \ / \ x_i = 0 \text{ si } i \notin I\}$. Ainsi si $x \in A^n$, on a $\det(T_I)x \in u(A^I) \subset u(A^m) = \operatorname{Im} u$ et donc $\det(T_I) \in (\operatorname{Im} u : A^n) = (0 : M)$.

Exercice 8. Soit A un anneau et $u : A^n \longrightarrow A^n$ un morphisme de matrice M_u dans la base canonique de A^n. Posons $M = \operatorname{Coker} u = A^n / \operatorname{Im}(u)$ et soit $u^* : A^n \longrightarrow A^n$ dont la matrice M_{u^*} est la matrice transposée des cofacteurs de M_u. Enfin pour $k \in \{1, \ldots, n\}$ soit J_k l'idéal engendré par les k-mineurs de M_u (c'est-à-dire les déterminants des sous-matrices $k \times k$ de M_u). Remarquer que $J_n = (\det(M_u))$ et que J_{n-1} est engendré par les coefficients de M_{u^*}.
(i) Soit $a \in (0 : M)$ et $\mu_a : A^n \longrightarrow A^n$, $x" \longmapsto ax$; montrer qu'il existe un morphisme $v : A^n \longrightarrow "A^n$ tel que $\mu_a = u \circ v$, et que $\det(M_u) \cdot M_v = aM_{u^*}$.
(ii) Montrer que $(0 : M) \subset (J_n : J_{n-1})$.
On suppose désormais que $\det(M_u)$ n'est pas diviseur de zéro.
(iii) Montrer que u^* est injectif.
(iv) Soit $a \in (J_n : J_{n-1})$; montrer qu'il existe $w : A^n \longrightarrow A^n$ tel que $au^* = \det(M_u) \cdot w$. Montrer alors que $u \circ w = \mu_a$.
(v) Montrer que $(0 : M) = (J_n : J_{n-1})$.

Solution. (i) On a $a \in (0 : M)$ c'est-à-dire que pour $x \in A^n$, on a $ax \in \operatorname{Im} u$. En particulier, pour tout $i \in [1, n]$, on a $ae_i \in \operatorname{Im} u$ donc il existe f_i tel que $u(f_i) = ae_i$. Définissons alors $v : A^n \to A^n$ par $v(e_i) = f_i$. On a alors $u \circ v(e_i) = u(v(e_i)) = u(f_i) = a_i e_i$ donc $u \circ v = \mu_a$. Au niveau des matrice on a $M_u M_v = aI_n$ où I_n est la matrice identité de taille $n \times n$. Par ailleurs, on sait que $\det(M_u)I_n = M_{u^*}M_u$, donc si on multiplie (disons à gauche) la relation $M_u M_v = aI_n$ par M_{u^*}, on obtient $\det(M_u)M_v = aM_{u^*}$.
(ii) Soit $a \in (0 : M)$ et v comme précédement, la relation $\det(M_u)M_v = aM_{u^*}$ montre que si x est un coefficient de M_{u^*}, alors $ax \in (\det(M_u)) = J_n$. Comme J_{n-1} est engendré par les coefficients de M_{u^*}, on a $aJ_{n-1} \subset J_n$.
(iii) Comme $\det(M_u)I_n = M_u M_{u^*}$, tout vecteur x tel que $u^*(x) = 0$ vérifie $\det(M_u)x = 0$. Comme $\det(M_u)$ n'est pas diviseur de 0 ceci impose que $x = 0$.
(iv) Soit $a \in (J_n : J_{n-1})$, alors, comme pour tout i le vecteur $u^*(e_i)$ est à coefficients dans J_{n-1}, on a $au^*(e_i)$ est à coefficients dans J_n. On peut donc écrire $au^*(ei) = \det(M_u)f_i$ avec $f_i \in A^n$. Soit alors $w : A^n \to A^n$ définie par $w(e_i) = f_i$. On a alors $au^*(e_i) = \det(M_u)f_i = \det(M_u)w(e_i)$ donc $au^* = \det(M_u)w$. En composant à gauche par u, on a $a\det(M_u)I_n = au^*u = \det(M_u)u \circ w$ donc $\det(M_u)(aI_n - u \circ w) = 0$. Comme $\det(M_u)$ n'est pas diviseur de 0, ceci impose $aI_n - u \circ w$ ou encore $u \circ w = \mu_a$.
(v) Soit $a \in (J_n : J_{n-1})$ et $x \in A^n$, on a alors $ax = u(w(x))$ donc $ax \in \operatorname{Im} u$ et ainsi $a \in (0 : M)$.

Exercice 9. Soit P un A-module. Montrer que les propriétés suivantes sont équivalentes :
(a) pour tout morphisme surjectif de A-module $g : E \longrightarrow F$ et pour tout $f \in \operatorname{Hom}_A(P, F)$, il existe $h \in \operatorname{Hom}_A(P, E)$ tel que $f = g \circ h$,
(b) pour tout morphisme surjectif $\pi : M \to P$, il existe un morphime $s : P \to M$ 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.
Donner un exemple de $\mathbb{Z}$-module qui n'est pas projectif.

Solution. Pour a) implique b), il suffit d'appliquer a) à $g = \pi$ et et $f = \mathrm{Id}_P$.

Pour b) implique c), soit $(x_i)_{i \in I}$ une famille génératrice de P. On en déduit un morphisme surjectif $\pi : A^{(I)} \to P$. D'après b), il existe $s : P \to A^{(I)}$ tel que $\pi \circ s = \mathrm{Id}_P$. Si $s(x) = 0$, $x = \pi s(x) = 0$, donc s est injective, ce qui permet d'identifier P avec son image par s dans $A^{(I)}$. Montrons que $A^{(I)} = s(P) \oplus \ker(\pi)$.
Si $x \in s(P) \cap \ker(\pi)$, alors alors $x = s(y)$ et $y = \pi s(y) = \pi(x) = 0$, donc $x = 0$: la somme est bien directe.
Si $x \in A^{(I)}$, alors $s\pi(x) \in s(P)$ et $\pi(x - s\pi(x)) = \pi(x) - \pi s \pi(x) = 0$ donc $x = s\pi(x) + (x - s\pi(x) \in s(P) + \ker(\pi)$. D'où c).

Pour c) implique a), supposons $P \oplus M = A^{(I)}$ et notons (e_i) la base canonique de $A^{(I)}$, $s : P \to A^{(I)}$ l'injection canonique et $\pi : A^{(I)} \to P$ la projection (on a $\pi s = \mathrm{Id}_P$). Soit a_i une préimage de $f\pi(e_i)$ par g. Alors il existe un unique morphisme $\phi : A^{(I)} \to E$ tel que $\phi(e_i) = a_i$ d'après la propriété universelle des modules libres. Comme $g\phi$ et $f\pi$ coincident en e_i pour tout i, $\phi g = f\pi$. Soit $h = \phi s$. Alors $gh = g\phi s = f\pi s = f$ comme voulu.

Exercice 10. Soit J un A-module. On dit que J est un A-module injectif si, pour tout morphisme injectif $i : N \to M$ de A-modules et tout morphisme de $f : N \to J$ de A-module, il existe un morphisme $g : M \to J$ tel que $f = gi$.

a) Montrer que $\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module injectif.

b) Soit J un A-module tel que tout morphisme $f : I \to J$ de A-modules où I est un idéal de A se prolonge en un morphisme $A \to J$. On veut montrer que J est injectif.
Soit donc N un sous-A-module d'un A-module M et soit $f : N \to J$ un morphisme.

  i) Montrer en utilisant le lemme de Zorn qu'il existe un prolongement f' de f à un sous-module N' de M contenant N tel que f' ne peut se prolonger à aucun sous-module N'' de M contenant strictement N'.

  ii) Soit $x \in M$ et soit $I = \{a \in A, ax \in N'\}$. En utilisant le morphisme $g : I \to J$ défini par $g(a) = f'(ax)$, montrer que f' se prolonge à $N' + Ax$.

  iii) En déduire que $N' = M$ et que J est injectif.

c) Montrer que $\mathbb{Q}$ et $\mathbb{Q}/\mathbb{Z}$ sont des $\mathbb{Z}$-modules injectifs.

d) Montrer qu'un produit (quelconque) de modules injectifs est encore injectif.

e) Montrer que tout $\mathbb{Z}$-module s'injecte dans un $\mathbb{Z}$-module injectif.

Solution. a) Soient $N = M = \mathbb{Z}$, $i : \mathbb{Z} \to \mathbb{Z}$ la multiplication par 2 et $f = \mathrm{Id}_{\mathbb{Z}}$. Si g existe $2g(1) = g(2) = g(i(1)) = f(1) = 1$, ce qui n'est pas possible dans $\mathbb{Z}$.

  i) Soit A l'ensemble des couples (N', f') où N' est un sous-module de M contenant N et $f' : N \to J$ est un prolongement de f. On ordonne A par $(N', f') \leq (N'', f'')$ si et seulement si $N' \subset N''$ et $f''_{N'} = f'$. Montrons que toute partie totalement ordonnée $(N_i, f_i)_{i \in I}$ de A est majorée dans A. Soit $N_0 = \bigcup_i N_i$. Si $n \in N_0$, il existe $i \in I$ tel que $n \in N_i$ et on pose $f_0(n) = f_i(n_i)$, ce qui ne dépend pas du choix de i. On vérifie facilement que (N_0, f_0) est un majorant de $(N_i, f_i)_{i \in I}$. Le lemme de Zorn nous dit que A admet un élément maximal.

  ii) On définit $g : I \to J$ par $g(a) = f'(ax)$. Par hypothèse on peut prolonger g en $g' : A \to J$.
  Soit $g'' : N' \oplus A \to J$ défini par $g''(n, a) = f'(n) + g'(a)$. Soit $\phi : N' \oplus A \to N' + Ax$ définie par $\phi(n, a) = n + ax$, phi est surjective et si $(n, a) \in \ker \phi$, alors $ax = -n$ donc $a \in I$ et $g''(n, a) = f'(n) + g(ax) = 0$. Donc g'' se factorise en un morphisme $N' + Ax \to J$ prolongeant f'.

  iii) Par maximalité de (N', f'), on en déduit $N' + Ax = N'$, donc $x \in N'$ pour tout $x \in M$. Donc $N' = M$ et donc J est bien injectif.

b) Appliquons le critère b). Si $I = 0$, on peut prolonger f par 0. Sinon Soit $f : n\mathbb{Z} \to \mathbb{Q}$ un morphisme, posons $f(a) = g(na)/n$ pour $a \in \mathbb{Z}$. Alors f prolonge g. Si $f : n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ est un morphisme, soit x une préimage dans $\mathbb{Q}$ de $f(n)$ et y l'image dans $\mathbb{Q}/\mathbb{Z}$ de x/n. ALors on peut prolonger f par $g(a) = ay$.

c) Soit $J = \prod_i J_i$ un produit de modules injectifs, notons $p_i : J \to J_i$ la projection. Soit $i : N \to M$ et $f : N \to J$ comme dans l'énoncé. Alors comme J_i est injectif, il existe $g_i : M \to J_i$ tel que $g_i i = p_i f$. En posant $g(m) = (g_i(m))_i$, on obtient un morphisme $g : M \to J$ cherché.

d) Soit M un $\mathbb{Z}$-module. Si $x \in M - \{0\}$, Soit $n\mathbb{Z}$ l'annulateur de x. On obtient un morphisme $f_x : Ax \to \mathbb{Q}/\mathbb{Z}$ envoyant x sur $1/n$. Le morphisme f_x se prolonge par injectivité de $\mathbb{Q}/\mathbb{Z}$ en un morphisme $g_x : M \to \mathbb{Q}/\mathbb{Z}$ tel que l'image de x soit non nulle. Le morphisme $M \to \prod_{x \in M-0} \mathbb{Q}/\mathbb{Z}$ est injectif et $\prod_{x \in M-0} \mathbb{Q}/\mathbb{Z}$ est injectif comme voulu.

1 Modules de type fini

Exercice 11. Soit A un anneau, M un A module de type fini et $\varphi : M \to A^n$ un morphisme surjectif de A-modules.
(i) Montrer que φ admet un inverse à droite ψ (c'est-à-dire qu'il existe $\psi : A^n \to M$ tel que $\varphi \circ \psi = id_{A^n}$).
(ii) Montrer que $M \simeq \mathrm{Ker}\varphi \oplus \mathrm{Im}\psi$.
(iii) Montrer que $\mathrm{Ker}\varphi$ est de type fini.

Solution. (i) Notons $(e_1, \ldots, e_n)$ la base standard de A^n. Comme φ est surjectif, il existe pour tout $i \in [1, n]$ un élément $m_i \in M$ tel que $\varphi(m_i) = e_i$. Définissons alors un homomorphisme de A-modules $\psi : A^n \to M$ par $\psi(e_i) = m_i$ pour tout i (ceci est possible car A^n est libre). On a alors $\varphi(\psi(e_i)) = e_i$ pour tout i c'est-à-dire $\varphi \circ \psi = id_{A^n}$.
(ii) On vérifie que l'homomorphisme de A-moduleθ : $\ker \varphi \oplus \operatorname{Im} \psi \to M$ défini par $\theta(m \oplus e) = m + \psi(e)$ est un isomorphisme. En effet, si $\theta(m \oplus e) = 0$, alors $m + \psi(e) = 0$. Si on applique φ, on a $\varphi(m + \psi(e)) = \varphi(m) + \varphi(\psi(e)) = e = 0$, puis $\psi(e) = 0$ et $m = 0$. Ceci prouve l'injectivité. Pour la surjectivité on prend $m \in M$ et on pose $m_0 = m - \psi(\varphi(m))$. On a alors $\varphi(m_0) = \varphi(m) - \varphi(\psi(\varphi(m))) = \varphi(m) - \varphi(m) = 0$, c'est-à-dire $m_0 \in \ker \varphi$. Mais alors on a $m = \theta(m_0 \oplus \varphi(m))$ donc θ est surjective.
(iii) Soient $(f_i)_{1 \leq i \leq k}$ des générateurs de M. On écrit pour tout i, $f_i = \theta(m_i \oplus \psi(v_i))$ avec $m_i \in \ker \varphi$ et $v_i \in A^n$. Montrons que les m_i engendrent $\ker \varphi$. En effet, soit $m \in \ker \varphi$, comme les (f_i) engendrent M, on peut écrire

$$m = \sum_i a_i f_i = \sum_i a_i(m_i + \psi(f_i)) = \sum_i a_i m_i + \psi\big(\sum_i a_i v_i\big) = \theta\big((\sum_i a_i m_i) \oplus (\sum_i a_i vi)\big).$$

Cependant on a vu que $m = \theta(m - \psi(\varphi(m)) \oplus \varphi(m))$ donc comme $m \in \ker \varphi$, on a $m = \theta(m \oplus 0)$. Comme θ est un isomorphisme on a $(\sum_i a_i m_i) \oplus (\sum_i a_i vi) = m \oplus 0$ et donc $m = \sum_i a_i m_i$.
On peut aussi remarquer que $\ker \varphi \simeq M / \operatorname{Im} \psi$ est un quotient d'un module de type fini et est donc aussi de type fini.

Exercice 12. Soit A un anneau, I un idéal de A et M un A-module de type fini, montrer que

$$\sqrt{\operatorname{Ann}(M/IM)} = \sqrt{\operatorname{Ann}(M) + I}.$$

Solution. Il est clair que $\operatorname{Ann}(M)$ et I sont contenus dans $\operatorname{Ann}(M/IM)$. On a donc l'inclusion $\operatorname{Ann}(M) + I \subset \operatorname{Ann}(M/IM)$ et donc $\sqrt{\operatorname{Ann}(M) + I} \subset \sqrt{\operatorname{Ann}(M/IM)}$.
Soit maintenant $a \in \operatorname{Ann}(M/IM)$, on a $aM \subset IM$. Soient $m_1, \cdots, m_n$ des générateurs de M. Il existe des $b_{i,j} \in I$ tels que

$$am_i = \sum_j b_{i,j} m_j.$$

Si B désigne la matrice des $(b_{i,j})$, la matrice $a\mathrm{Id} - B$ annule le vecteur $(m_1, \cdots, m_n)$. Mais alors on a $\det(a\mathrm{Id} - B) = {}^t\mathrm{Com}(a\mathrm{Id} - B)(a\mathrm{Id} - B)$ donc $\det(a\mathrm{Id} - B)$ annule aussi le vecteur $(m_1, \cdots, m_n)$. Comme les m_i sont les générateurs de M, on a $\det(a\mathrm{Id} - B)$ annule M donc $\det(a\mathrm{Id} - B) \in \operatorname{Ann}(M)$. Cependant, si on écrit le déterminant développé, on voit que $\det(a\mathrm{Id} - B) = a^n + b$ où $b \in I$. Ainsi $a^n \in \operatorname{Ann}(M) + I$ donc $a \in \sqrt{\operatorname{Ann}(M) + I}$. On en déduit donc $\operatorname{Ann}(M/IM) \subset \sqrt{\operatorname{Ann}(M) + I}$, puis $\sqrt{\operatorname{Ann}(M) + I} \subset \sqrt{\operatorname{Ann}(M/IM)}$.

Exercice 13. Lemme de Nakayama.
(i) Soit M un A-module de type fini et I un idéal de A. Supposons que $M = IM$, montrer qu'il existe alors $a \in I$ tel que $(1 + a)M = 0$ (choisir $1 + a$ déterminant d'une matrice).
(ii) En déduire que si A est local, $I = \mathfrak{m}$ son idéal maximal et $M = \mathfrak{m}M$ alors $M = 0$.
(iii) Soit $\mathfrak{R}$ le radical de Jacobson de A (c'est-à-dire l'intersection de tous les idéaux maximaux). Montrer que si $\mathfrak{R}M = M$, alors $M = 0$.

Solution. (i) Soit $m_1, \cdots, m_n$ des générateurs de M. Comme $M = IM$, il existe de $b_{i,j} \in I$ tels que $m_i = \sum_j b_{i,j} m_j$. Notons B la matrice formée par les $(b_{i,j})$. La matrice $\mathrm{Id} - B$ annule M et comme on a $\det(\mathrm{Id} - B) = {}^t\mathrm{Com}(\mathrm{Id} - B)(\mathrm{Id} - B)$, le scalaire $\det(\mathrm{Id} - B)$ annule aussi M. Si on développe ce détermiant, il est de la forme $1 + a$ avec $a \in I$, d'où le résultat.
(ii) Si de plus A est local et $I = \mathfrak{m}$, alors $a \in \mathfrak{m}$ et $1 + a$ est inversible. La condition $(1 + a)M = 0$ donne $M = 0$.
(iii) Une fois encore on a $a \in \mathfrak{R}$ tel que $(1 + a)M = 0$. Il reste à montrer que $1 + a$ est inversible. Supposons que ce n'est pas le cas, alors l'idéal $(1 + a)$ est strictement contenu dans A. Il existe donc un idéal maximal $\mathfrak{m}$ le contenant (lemme de Zorn). Mais alors $1 + a \in \mathfrak{m}$ et $a \in \mathfrak{R} \subset \mathfrak{m}$ donc $1 \in \mathfrak{m}$, c'est absurde.

Exercice 14. 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 $I = (e)$.
Indice : utiliser le lemme de Nakayama pour trouver $a \in I$ tel que $(1 + a)I = 0$.

Solution. On a $I \cdot I = I$ donc par le lemme de Nakayama (car I est un A-module de type fini), on a $a \in I$ tel que $(1 + a)I = 0$. On pose alors $e = -a$ et on a $e \in I$, $(1 - e)e = 0$ c'est-à-dire $e = e^2$. Soit maintenant $x \in I$, on a $(1 - e)x = 0$, donc $x = xe \in (e)$ donc $I = (e)$.

Exercice 15. Soient A un anneau, M un A-module, N un A-module de type fini et $u : M \longrightarrow N$ un homomorphisme de A-modules. Soit $\mathfrak{R}$ le radical de Jacobson de A ($\mathfrak{R}$ est l'intersection de tous les idéaux maximaux de A).
(i) Montrer que u induit un homomorphisme $v : M/\mathfrak{R}.M \longrightarrow N/\mathfrak{R}.N$.
(ii) Remarquer que si I est un idéal de A et $N' \subset M'$ sont deux A-modules alors on a

$$I \cdot (M'/N') = (I \cdot M' + N')/N'.$$

(iii) On suppose que v est surjectif, calculer $\operatorname{Im} u + \mathfrak{R} \cdot N$ et en déduire que u est surjectif.

Solution. (i) Il suffit de montrer que $\mathfrak{R}M$ est contenu dans le noyau du morphisme composé

$$f : M \xrightarrow{u} N \to N/\mathfrak{R}N.$$

On a alors un morphisme $M/\mathfrak{R}M \to M/\ker f$ que l'on peut composer avec $M/\ker f \to N/\mathfrak{R}N$.
Soit donc $am \in \mathfrak{R}M$ avec $a \in \mathfrak{R}$ et $m \in M$. Son image par u est alors $u(am) = au(m) \in \mathfrak{R}N$ donc $am \in \ker f$.
(ii) Considérons l'application A-linéaire $\varphi : I \cdot (M'/N') \to (I \cdot M' + N')/N'$ définie par $\varphi(\sum a_i Cl(m_i)) = Cl(\sum a_i m_i)$ (avec ici $a_i \in I$ et $m_i \in M'$). Elle est bien définie car si $\sum a_i Cl(m_i) = 0 \in M'/N'$ c'est-à-dire $\sum a_i m_i \in N'$, alors $\varphi(\sum a_i Cl(m_i)) = Cl(\sum a_i m_i) = 0$. De plus, si $\varphi(\sum a_i Cl(m_i)) = 0$, alors $Cl(\sum a_i m_i) = 0$ donc $\sum a_i m_i \in N'$ et donc $\sum a_i Cl(m_i) = 0$, φ est donc injective. Par ailleurs si $m = \sum a_i m_i + n \in (I \cdot M' + N')$ avec $a_i \in I$, $m_i \in M'$ et $n \in N'$, alors on a $Cl(m) = Cl(\sum a_i m_i) = \varphi(\sum a_i Cl(m_i))$ donc $m \in \operatorname{Im} \varphi$ et φ est surjective. Le morphisme φ est l'isomorphisme recherché.
(iii) Il est clair que $\operatorname{Im} u + \mathfrak{R}N \subset N$, nous montrons l'égalité. L'hypothèse v surjectif signifie que le morphisme $f : M \xrightarrow{u} N \to N/\mathfrak{R}N$ est surjectif. Soit maintenant $n \in N$ et soit $Cl(n)$ sont image dans $N/\mathfrak{R}N$. Il existe donc $m \in M$ tel que $Cl(u(m)) = Cl(n)$. Ceci signifie que $n - u(m) \in \mathfrak{R}N$ et donc $n = u(m) + n'$ avec $n' \in \mathfrak{R}N$.
Pour montrer la surjectivité de u, nous appliquons le (ii) à $I = \mathfrak{R}$, $M' = N$ et $N' = \operatorname{Im} u$. On a alors $\mathfrak{R} \cdot (N/\operatorname{Im} u) = (\mathfrak{R} \cdot N + \operatorname{Im} u)/\operatorname{Im} u = N/\operatorname{Im} u$. Si on note $P = N/\operatorname{Im} u$, le A-module$P$ vérifie $\mathfrak{R}P = P$, par le lemme de Nakayama (iii) on a $P = 0$.

2 Modules et anneaux noethériens

Exercice 16. Montrer que si M est un A-module noethérien alors $M[X]$ est un $A[X]$-module noethérien.

Solution. Il suffit d'adapter la preuve du théorème de transfert de Hilbert.
Soit N un sous-$A[X]$-module de $M[X]$. Montrons qu'il est engendré par un nombre fini d'éléments. Soit

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

Les N_n sont des A-moduleet la suite $(N_n)_n$ est croissante. En effet, si m et p sont dans N_n, alors il existe P et Q dans N de degrés n et de coefficients dominant respectifs m et p. Alors $P + Q \in N$ est de degré n et de coefficient dominant $m + p$. De plus si $a \in A$, alors $aP \in N$ de degré n et de coefficient dominant am. N_n est donc un A-module. De plus si $m \in N_n$ et que $P \in N$ de degré n et de coefficient dominant m, alors $XP \in N$ de degré $n+1$ et de coefficient dominant m, donc $m \in N_{n+1}$ donc la suite des $(N_n)_n$ est croissante.
Comme M est noethérien, la suite des $(N_n)_n$ est stationnaire, disons à partir de n_0 et les modules N_n sont engendrés par un nombre fini d'éléments, les $(b_{n,k})_{1 \leq k \leq k_n}$. Pour chaque paire (n, k), notons $P_{n,k} \in N$ un polynôme de degré n dont le coefficient dominant est $b_{n,k}$. Nous allons montrer que N est engendré par les $(P_{n,k})_{1 \leq n \leq n_0, 1 \leq k \leq k_n}$, soit donc N' le sous-$A[X]$-module de $M[X]$ engendré par ces éléments.
Soit $P \in N$ de degré d. Nous allons montrer par récurrence sur d que $P \in N'$. Notons m le coefficient dominant de P, on a $m \in N_d$. Si $d \leq n_0$, alors $m = \sum_k a_k b_{d,k}$ donc $Q = P - \sum_k a_k P_{d,k} \in N$ est de degré strictement inférieur à d donc $Q \in N'$ par hypothèse de récurrence et donc $P \in N'$. Si $d > n_0$, alors $m \in N_d = N_{n_0}$ donc $m = \sum_k a_k b_{n_0,k}$ et $Q = P - X^{d-n_0} \sum_k a_k P_{n_0,k} \in N$ est encore de degré strictement inférieur à d, on conclue comme précédemment.

Exercice 17. Soit A un anneau. Si $A[X]$ est noethérien, A est-il nécessairement noethérien ?

Solution. Oui : on sait que tout quotient d'un module (ou d'un anneau) noethérien est encore noethérien (cours). Or $A = A[X]/(X)$ donc A est noethérien si $A[X]$ l'est.

Exercice 18. Soient M, M' et M'' trois A-modules et $i : M' \longrightarrow M$ un homomorphisme injectif et $\pi : M \longrightarrow M''$ un homomorphisme surjectif tels que $\pi \circ i = 0$. Montrer que M est noethérien si et seulement si M', M'' et $\ker \pi / \operatorname{Im} i$ sont noethériens.

Solution. Si M est noethérien alors tout sous-module (donc en particulier M' et $\ker \pi$) et tout quotient (en particulier M'') de M sont noethériens. Ensuite tout quotient de $\ker \pi$ est noethérien (car on vient de voir que $\ker \pi$ est noethérien) donc $\ker \pi / \operatorname{Im} i$ est noethérien.
Réciproquement, on a un complexe $0 \to M' \to M \to M'' \to 0$ qui est exact partout sauf au centre (sa cohomologie est $\ker \pi / \operatorname{Im} i$). On a donc des suites exactes $0 \to \ker \pi \to M \to M'' \to 0$ et $0 \to \operatorname{Im} i \to \ker \pi \to \ker \pi / \operatorname{Im} i \to 0$. De plus comme i est injective, on a un isomorphisme entre M' et son image par i c'est-à-dire $\operatorname{Im} i$. Ainsi $\operatorname{Im} i$ est noethérien et comme $\ker \pi / \operatorname{Im} i$ l'est aussi, on a (cf. execice précédent et grâce à la seconde suite exacte) $\ker \pi$ est noethérien. Grâce à la première suite exacte et le fait que M'' est noethérien on en déduit (toujours exercice précédent) que M est noethérien.

Exercice 19. Soient M un A-module et N_1 et N_2 deux sous-module de M. Montrer que N_1 et N_2 sont noethériens si et seulement si $N_1 + N_2$ est noethérien, et que M/N_1 et M/N_2 sont noethériens si et seulement si $M/(N_1 \cap N_2)$ est noethérien.

Solution. Remarquons tout d'abord que la une suite exacte $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ nous dit que le module $M_1 \oplus M_2$ est noethérien si et seulement si M_1 et M_2 le sont.
Montrons que la suite $0 \to N_1 \cap N_2 \xrightarrow{i} N_1 \oplus N_2 \xrightarrow{\pi} N_1 + N_2 \to 0$ donnée par $i(n) = (n, -n)$ et $\pi(n_1, n_2) = n_1 + n_2$ est exacte. En effet, i est injective, π surjective et $\operatorname{Im} i \subset \ker \pi$. Par ailleurs, si $(n_1, n_2) \in \ker \pi$, alors $n_1 + n_2 = 0$ donc $n = n_1 = -n_2 \in N_1 \cap N_2$, donc $(n_1, n_2) = (n, -n) \in \operatorname{Im} i$.
Si N_1 et N_2 sont noethériens, alors $N_1 \oplus N_2$ l'est et donc $N_1 \cap N_2$ et $N_1 + N_2$ aussi (cf. exercice 83). Réciproquement, si $N_1 + N_2$ est noethérien, alors $N_1 \cap N_2$ l'est comme sous-module et donc (cf. exercice 83) $N_1 \oplus N_2$ l'est. Les deux modules N_1 et N_2 sont alors aussi noethériens.
Pour la seconde question, on remarque que l'on a la suite exacte

$$0 \to M/(N_1 \cap N_2) \xrightarrow{i} M/N_1 \oplus M/N_2 \xrightarrow{\pi} M/(N_1 + N_2) \to 0$$

où $i(Cl(m)) = (Cl(m), -Cl(m))$ et $\pi((Cl(m_1), Cl(m_2))) = Cl(m_1 + m_2)$. En effet, on a bien π surjective, i injective et $\operatorname{Im} i \subset \ker \pi$. Par ailleurs si $(Cl(m_1), Cl(m_2)) \in \ker \pi$, alors $Cl(m_1+m_2) = 0$ donc $m_1+m_2 \in N_1+N_2$ c'est-à-dire $m_1 + m_2 = n_1 + n_2$ avec $n_i \in N_i$. On a donc $m_1 - n_1 = -(m_2 - n_2)$ et $(Cl(m_1), Cl(m_2)) = (Cl(m_1 - n_1), -Cl(m_1 - n_1)) = i(Cl(m_1 - n_1)$ donc $\ker \pi = \operatorname{Im} i$.
Une fois que l'on sait que la suite est exacte, si M/N_1 et M/N_2 sont noethériens, alors $M/N_1 \oplus M/N_2$ aussi et donc $M/(N_1 \cap N_2)$ est noethérien. Réciproquement, si $M/(N_1 \cap N_2)$ est noethérien, alors $M/(N_1 + N_2)$ en est un quotient donc noethérien et ainsi $M/N_1 \oplus M/N_2$ est aussi noethérien. On en déduit que M/N_1 et M/N_2 sont noethériens.

Exercice 20. Soit M un A-module noethérien et $u \in \operatorname{Hom}(M, M)$. Montrer que u est bijective si et seulement si u est surjective (on pourra utiliser le lemme du serpent).

Solution. Supposons que u n'est pas surjective, on va montrer que la suite des $(\ker u^n)$ est alors non stationnaire (ce qui contredira l'hypothèse M noethérien).
Remarquons tout d'abord que comme u est surjective, c'est aussi le cas de u^n pour tout $n > 0$. On a alors pour tout $n > 0$ les suites exactes $0 \to \ker u^n \to M \to M \to 0$. On peut donc écrire le diagramme

$$\begin{array}{ccccccccc}
 & & 0 & & & & 0 & & \\
 & & \downarrow & & & & \downarrow & & \\
 & & N & & 0 & & \ker u & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \ker u^n & \to & M & \overset{u^n}{\to} & M & \to & 0 \\
 & & \downarrow \mathrm{id} & & \downarrow \mathrm{id} & & \downarrow u & & \\
0 & \to & \ker u^{n+1} & \to & M & \overset{u^{n+1}}{\to} & M & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & Q & & 0 & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

et le lemme du serpent nous donne la suite exacte $0 \to \ker u^n \to \ker u^{n+1} \to \ker u \to 0$. Ainsi si u n'est pas injective, on a $\ker u \neq 0$ et donc l'inclusion $\ker u^n \subset \ker u^{n+1}$ est stricte. La suite des $(\ker u^n)$ n'est donc pas stationnaire, c'est impossible si M est noethérien.

Exercice 21. Soit M un A-module noethérien et $I = (0 : M)$. Montrer que A/I est un anneau noethérien.

Solution. Soient $m_1, \cdots, m_n$ des générateurs de M comme A-module. Considérons le morphisme $A \to M^n$ défini par $a \mapsto (am_1, \cdots, am_n)$. Son noyau contient I et si a est dans le noyau, alors pour tout $m \in M$, on peut écrire $m = \sum a_i m_i$ donc $am = \sum a_i a m_i = 0$. Ainsi I est exactement le noyau. Par le théorème de factorisation, on peut donc voir A/I comme un sous-module de M^n, il est donc noethérien (comme A-module et la structure de A/I-module sur A/I est exatement la même que celle de A-module).

Exercice 22. L'anneau $A = k[X_1, X_2, \cdots, X_n, \cdots]$ est-il noethérien ?

Solution. On considère la suite croissante d'idéaux $((X_1, \cdots, X_n))_{n \in \mathbb{N}^*}$ et on montre qu'elle n'est pas stationnaire. Si c'était le cas il existerait $n \in N^*$ tel que $X_{n+1} \in (X_1, \cdots, X_n)$. Il existerait alors des polynômes P_i_inA tels que $X_{n+1} = \sum_i X_i P_i$. On peut alors évaluer cette égalité en un point $(x_1, \cdots, x_n, x_{n+1}, \cdots, x_m)$ (on peut s'arrêter à m car il n'y a qu'un nombre fini de polynômes P_i qui font chacun intervenir un nombre fini de variables. Si on suppose que $x_i = 0$ pour $1 \leq i \leq n$ et $x_{n+1} = 1$, on a alors $1 = 0$ ce qui est absurde.

Exercice 23. Soit A un anneau et $(I_n)_{n>0}$ une suite croissante d'idéaux de type fini. Montrer que $I = \bigcup I_n$ est de type fini si et seulement si la suite est stationnaire.

Solution. Si la suite est stationnaire, on a $I = I_n$ pour un certain n donc I est de type fini. Réciproquement si I est de type fini, soient $(a_1, \cdots, a_k)$ des générateurs de I. On a alors l'existence d'un n assez grand tel que pour tout i, on ait $a_i \in I_n$. Mais alors $I = I_n$ et la suite est stationnaire.

Exercice 24. (i) Soient A un anneau non noethérien, $a \in A$ et I un idéal de A. Montrer que si les idéaux $I + (a)$ et $(I : a) = \{x \in A \ / \ ax \in I\}$ sont de type fini, alors I l'est.
(ii) Montrer qu'un anneau est noethérien si et seulement si tous ses idéaux premiers sont de type fini.
Indice : Considérer un idéal maximal parmi ceux qui ne sont pas de type fini.

Solution. (i) Soient $z_1, \cdots, z_n$ des générateurs de $I + (a)$. Alors on peut écrire $z_i = x_i + aa_i$ avec $x_i \in I$ et $a_i \in A$. On constate alors que l'idéal engendré par a et les x_i est contenu dans $I + (a)$ et contient les z_i, c'est donc $I + (a)$.
Soient $y_1, \cdots, y_m$ des générateurs de $(I : a)$, on a $ay_i \in I$. Montrons que l'on a

$$I = (x_1, \cdots, x_n, ay_1, \cdots, ay_m).$$

L'inclusion $(x_1, \cdots, x_n, ay_1, \cdots, ay_m) \subset I$ est évidente. Soit $u \in I$, on a $u \in I + (a)$ donc $u = \sum u_i x_i + ta$ avec $t \in A$. Mais alors $ta = u - \sum u_i x_i \in I$ donc $t \in (I : a)$. On peut donc écrire $t = \sum t_j y_j$. On a donc

$$u = \sum u_i x_i + \sum t_j (ay_j) \in (x_1, \cdots, x_n, ay_1, \cdots, ay_m).$$

(ii) Si A est noethérien, tous ses idéaux et donc en particulier les idéaux premiers sont de type fini.
Réciproquement, supposons que tous les idéaux premiers soient de type fini et soit E l'ensemble des idéaux de A qui ne sont pas de type fini. On veut montrer que $E = \emptyset$. Supposons que ce n'est pas le cas.
L'ensemble E est ordonné par l'inclusion et est inductif : si (I_n) est une suite croissante d'idéaux qui ne sont pas de type fini, alors $I = \bigcup I_n$ n'est pas de type fini (si c'était le cas on aurait $I = (a_1, \cdots, a_k)$ et il existerait n tel que $a_i \in I_n$ pour tout i donc $I = I_n$ qui serait de type fini, c'est absurde).
D'après le lemme de Zorn, il existe donc un (ou des) élément(s) maximal (maximaux) dans E. Soit I un tel élément maximal, il n'est pas de type fini donc n'est pas premier. Il existe donc a et $b \notin I$ tels que $ab \in I$.
On a alors $I \subsetneq I + (a)$, donc $I + (a)$ est de type fini. De plus $I \subsetneq (I : a)$ (car il est clair que $I \subset (I : a)$ et $b \in (I : a)$, $b \notin I$) donc $(I : a)$ est de type fini. Le (i) nous dit que I est de type fini, c'est une contradiction donc $E = \emptyset$ et A est noethérien.

Exercice 25. Soit A un anneau intègre et noethérien. On suppose que A admet un unique idéal maximal $\mathfrak{m}$ (c'est-à-dire A est un anneau local) et que cet idéal est engendré par un élément non nul a.
(i) Montrer que $u \in A$ est inversible si et seulement si $u \notin \mathfrak{m}$.
(ii) Montrer que tout élément non nul x de A s'écrit d'une manière unique sous la forme $x = ua^n$ où $u \in A^\times$ et $n \in \mathbb{N}$.

Solution. (i) Si u est inversible, alors $(u) = A$ donc $u \notin \mathfrak{m}$. Si par contre u n'est pas inversible, alors $(u) \neq A$ donc il existe un idéal maximal contenant (u). Mais il y a un unique idéal maximal $\mathfrak{m}$ donc $u \in \mathfrak{m}$.
(ii) Soit $x \in A$ non nul. Si $x \notin \mathfrak{m} = (a)$, on a directement l'écriture avec $u = x$ et $n = 0$. Si $x \in (a)$, on écrit $x = ax_1$. L'écriture de x_1 est unique car A est intègre et $a \neq 0$. Si $x_1 \in (a)$, on continue et on écrit $x_1 = ax_2$, etc. On construit ainsi une suite d'éléments x_n tous non nuls (sinon x serait nul).
Si la suite s'arrête, on a écrit $x = a^n x_n$ avec $x_n \notin (a) = \mathfrak{m}$ donc x_n est inversible.

Si elle ne s'arrête pas, on a alors une suite croissante d'idéaux :

$$(x) \subset (x_1) \subset \cdots \subset (x_n) \cdots$$

qui doit être stationnaire car A est noethérien. On a donc $(x_n) = (x_{n+1})$ pour un certain n. Ceci donne $x_{n+1} = ux_n = uax_{n+1}$ et comme $x_{n+1} \neq 0$, on a $ua = 1$ c'est-à-dire a inversible, c'est impossible.
On a donc toujours une écriture $x = ua^n$, il reste à prouver l'unicité. Soient deux écritures $x = ua^n = va^m$ avec u et v inversibles et supposons par exemple que $m \geq n$. On a alors $u = va^{m-n}$ et comme u est inversible, ceci impose $m = n$ puis $u = v$.

Exercice 26. Soit A un anneau local dont l'idéal maximal est principal en gendré par a et tel que $\bigcap_{n>0} \mathfrak{m}^n = 0$.
(i) Montrer que $u \in A$ est inversible si et seulement si $u \notin \mathfrak{m}$.
(ii) Montrer que tout élément non nul x de A s'écrit sous la forme $x = ua^n$ où $u \in A^\times$ et $n \in \mathbb{N}$.
(iii) Montrer que tout idéal I est de la forme (a^n).
(iv) En déduire que A est un anneau principal.

Solution. (i) Si u est inversible, alors $(u) = A$ donc $u \notin \mathfrak{m}$. Si par contre u n'est pas inversible, alors $(u) \neq A$ donc il existe un idéal maximal contenant (u). Mais il y a un unique idéal maximal $\mathfrak{m}$ donc $u \in \mathfrak{m}$.
(ii) Soit $x \in A$ non nul. Par hypothèse on a donc un $k \in \mathbb{N}$ tel que $x \notin \mathfrak{m}^k$. Soit $n \in \mathbb{N}$ le plus grand entier tel que $x \in \mathfrak{m}^n$. On a alors $x = ua^n$ et $u \notin \mathfrak{m}$ (sinon $x \in \mathfrak{m}^{n+1}$). Ainsi u est inversible.
On a donc toujours une écriture $x = ua^n$.
(iii) Soit I un idéal, pour tout $x \in I$, on définit n_x le plus grand entier tel que $x \in \mathfrak{m}^{n_x}$. Soit alors $n_I = \min\{n_x \ / \ x \in I\}$. On a alors $I = (a^{n_I})$. En effet, si $x \in I$, alors $x = ua^{n_x}$ avec u inversible et $n_x \geq n_I$, on a donc $x = ua^{n_x - n_I}a^{n_I}$ donc $x \in (a^{n_I})$. Ainsi $I \subset (a^{n_I})$. Par ailleurs, comme $n_I = \min\{n_x \ / \ x \in I\}$, il existe $x \in I$ tel que $n_x = n_I$. Ainsi $x = ua^{n_I}$ avec u inversible. L'idéal I contient donc a^{n_I}.
(iv) On vient de voir que tout idéal de A est principal (donc de type fini), l'anneau A est donc noethérien.

Exercice 27. Soit M un A-modulenoethérien et soit $\varphi : M \to M$ un endomorphisme de M. Montrer qu'il existe un entier n tel que $\ker \varphi^n \cap \operatorname{Im} \varphi^n = 0$.

Solution. La suite des sous-modules $(\ker \varphi^n)$ est croissante donc stationnaire car M est noethérien. Il existe donc $n \in \mathbb{N}$ tel que pour tout $m \geq n$, on ait $\ker \varphi^m = \ker \varphi^n$.
Si $x \in \ker \varphi^n \cap \operatorname{Im} \varphi^n$, alors il existe $y \in M$ tel que $x = \varphi^n(y)$. Mais alors $\varphi^{2n}(y) = \varphi^n(x) = 0$ donc $y \in \ker \varphi^{2n} = \ker \varphi^n$. On a donc $x = \varphi^n(y) = 0$.

Exercice 28. Soit $f : A \to A$ un morphisme d'anneaux.
(i) On suppose A noethérien, montrer qu'il existe un entier $n \geq 1$ tel que $\ker(f^n) = \ker(f^{n+1})$. En déduire que l'application

$$f : \operatorname{Im}(f^n) \to \operatorname{Im}(f^{n+1})$$

est injective.
(ii) Montrer que si f est surjective et A noethérien, alors elle est bijective.
(iii) Montrer qu'on ne peut remplacer dans la question précédente l'hypothèse « surjective » par « injective ».
(iv) Montrer que l'on ne peut se passer de l'hypothèse noethérien (considérer par exemple $A = k[X_1, \cdots, X_n, \cdots]$ un anneau de polynômes à une infinité de variables et f convenable).

Solution. (i) Considérons la suite des noyaux $(\ker(f^n))_{n \in \mathbb{N}}$. C'est une suite croissante d'idéaux de A. En effet, si $x \in \ker(f^n)$, alors $f^{n+1}(x) = f(f^n(x)) = f(0) = 0$ donc $x \in \ker(f^{n+1})$.
Comme A est noethérien, cette suite croissante d'idéau est stationnaire donc il existe un $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$ on ait

$$\ker(f^n) = \ker(f^{n_0}).$$

On considère alors l'application

$$f : \operatorname{Im}(f^{n_0}) \to \operatorname{Im}(f^{n_0+1})$$

dont le noyau est $\ker(f) \cap \operatorname{Im}(f^{n_0})$. Un point du noyau est alors de la forme $x = f^{n_0}(y)$ et vérifie $f(x) = 0$ donc $f^{n_0+1}(y) = 0$. On a donc $y \in \ker(f^{n_0} + 1) = \ker(f^{n_0})$. Ainsi $x = f^{n_0}(y) = 0$ donc la flèche est injective.
(ii) Si on suppose de plus f surjective, alors on voit que f^{n0} et f^{n_0+1} sont aussi surjectives et l'application

$$f : \operatorname{Im}(f^{n_0}) \to \operatorname{Im}(f^{n_0+1})$$

devient la flèche

$$f : A \to A.$$

Elle est injective d'après ce qui précède, comme elle est surjectve par hypothèse, c'est un isomorphisme.
(iii) Prenons $A = k[X]$ et le morphisme de k-algèbres de A dans lui-même définit par $X \mapsto X^2$. Il est évidement injectif, mais n'est pas surjectif car X n'est pas dans l'image.
(iv) Considérons $A = k[X_1, \cdots, X_n, \cdots]$ un anneau de polynômes à une infinité de variables et définissons le morphisme de k-algèbres $f : A \to A$ par l'image des générateurs :

$$f(X_1) = 0 \quad \text{et} \quad f(X_{i+1}) = X_i \quad \text{pour} \quad i \geq 1.$$

On voit alors que tous les X_i pour $i \geq 1$ sont dans l'image de f donc f est surjective alors que X_1 est dans le noyau de f donc f n'est pas injective.

Exercice 29. Soit A un anneau noethérien et G un groupe fini opérant sur A par automorphismes d'anneaux. On note $A^G = \{a \in A : \forall g \in G, ga = a\}$. Vérifier que A^G est un sous-anneau de A.
On suppose que le cardinal de G est inversible dans A et on défini $p : A \to A$ par

$$p(a) = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} ga.$$

(i) Montrer que pour tout $g \in G$, on a $g \circ p = p \circ g = p$.
(ii) Montrer que p est un projecteur (c'est-à-dire $p^2 = p$) qui est A^G-linéaire (mais en général pas un morphisme d'anneaux.
(iii) Montrer que l'image de p est A^G.
(iv) Soit I un idéal de A^G et IA l'idéal de A engendré par I. Montre que $p(IA) = I$.
(v) Montrer que A^G est noethérien.

Solution. (i) On calcule

$$g \circ p(a) = g\left(\frac{1}{\mathrm{card}(G)} \sum_{h \in G} ha\right) = \frac{1}{\mathrm{card}(G)} \sum_{h \in G} (gh)a = \frac{1}{\mathrm{card}(G)} \sum_{gh \in G} gha = p(a).$$

De même on a

$$p \circ g(a) = \frac{1}{\mathrm{card}(G)} \sum_{h \in G} h(ga) = \frac{1}{\mathrm{card}(G)} \sum_{h \in G} (hg)a = \frac{1}{\mathrm{card}(G)} \sum_{hg \in G} (hg)a = p(a).$$

(ii) On calcule

$$p \circ p = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} g \circ p = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} p = \frac{1}{\mathrm{card}(G)} \ \mathrm{card}(G)\ p = p.$$

Si $\lambda \in A^G$ est invariant par le groupe G, alors on a

$$p(\lambda a) = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} g(\lambda a) = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} \lambda g(a) = \lambda \frac{1}{\mathrm{card}(G)} \sum_{g \in G} ga = \lambda p(a).$$

Le projecteur p est donc bien A^G linéaire.
(iii) Soit $\lambda \in A^G$, on a alors

$$p(\lambda) = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} g(\lambda) = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} \lambda = \lambda \frac{1}{\mathrm{card}(G)} \ \mathrm{card(G)} = \lambda.$$

ce qui prouve que A^G est contenu dans l'image de p. Par ailleurs, si $x \in \mathrm{Im}\, p$, alors on a $x = p(y)$ et pour tout $g \in G$, on a

$$g(x) = g(p(y)) = g \circ p(y) = p(y) = x$$

donc $x \in A^G$.
(iv) Comme $I \subset A^G$ et que p est l'identité sur A^G, on a $p(I) = I$. Or on a $I \subset IA$ donc $I \subset p(IA)$.
Soit maintenant $x \in IA$, on peut alors écrire $x = \sum_i a_i x_i$ avec $a_i \in A$ et $x_i \in I$. Mais alors comme p est A^G linéaire, on a

$$p(x) = \sum_i x_i p(a_i)$$

et $x_i \in I$ et $p(a_i) \in A^G$, on a donc $p(x) \in I$ car I est un idéal de A^G.

(v) Soit I un idéal de A^G, il faut montrer qu'il est de type fini. On a vu que $I = p(IA)$ où IA est un idéal de A. Comme A est noethérien, ce dernier idéal est de type fini : $IA = (a_1, \cdots, a_n)$. Mais alors comme I engendre IA, les a_i s'écrivent :

$$a_i = \sum_j x_{i,j} b_{i,j}$$

où la somme est finie avec $b_{i,j} \in I$ et $x_{i,j} \in A$. On voit donc que les $b_{i,j} = p(b_{i,j})$ engendrent IA comme idéal de A. Montrons qu'ils engendrent I comme idéal de A^G.
En effet, si $x \in I$, alors on sait que $x \in p(IA)$ donc $x = p(y)$ avec $y \in IA$. Mais alors on peut écrire $y = \sum_{i,j} y_{i,j} b_{i,j}$ avec $y_{i,j} \in A$. On a alors comme $b_{i,j} \in I \subset A^G$ et que p est A^G-linéaire :

$$x = p(y) = \sum_{i,j} p(y_{i,j} b_{i,j}) = \sum_{i,j} p(y_{i,j}) b_{i,j}.$$

Comme les $p(y_{i,j})$ sont dans A^G, ceci prouve que les $b_{i,j}$ engendrent I comme idéal de A^G.

Exercice 30. On dit qu'un anneau R est gradué s'il existe une décomposition $R = \bigoplus_{n=0}^{\infty} R_n$ où les R_n sont des sous-groupes de $(R, +)$ vérifiant $R_n \cdot R_m \subset R_{n+m}$.
(i) Montrer que R_0 est alors un sous-anneau de R. Montrer aussi que $I = \bigoplus_{n=1}^{\infty} R_n$ est un idéal de R.
(ii) On suppose que R_0 est noethérien et que R est de type fini comme R_0-algèbre. Montrer que R est noethérien.
(iii) Réciproquement, on suppose R noethérien, montrer que R_0 est noethérien. Montrer qu'il existe des éléments $x_1, \cdots, x_r \in R$ avec $x_i \in R_{n(i)}$ pour un entier $n(i) \geq 1$ tels que $I = (x_1, \cdots, x_r)$. Montrer alors par récurrence que pour tout n, on a $R_n \subset R_0[x_1, \cdots, x_r]$. En déduire que R est une R_0-algèbre de type fini.
(iv) On se donne un anneau noethérien A et I un idéal de A. Soit $R(I)$ l'e,semble des polynômes $P \in A[T]$ tels que $P = \sum a_n T^n$ avec $a_n \in I^n$. Montrer que $R(I)$ est noethérien.

Solution. (i) Il est clair que R_0 est stable par addition, l'opposé et la multiplication. C'est donc un sous-anneau. De même, I est un sous-groupe abélien de R et si $x = \sum x_n \in R$ et $y = \sum y_n \in I$ (donc $y_0 = 0$), alors

$$xy = \sum_{n=0}^{\infty} \sum_{k+m=n} x_k y_m$$

et la composante de degré 0 est nul car elle fait toujours intervenir y_0. Ainsi $xy \in I$ et I est un idéal de R.
(ii) Toute algèbre de type fini sur un anneau noethérien est est anneau noethérien.
(iii) Comme l'application $R/I \to R_0$ définie par $\sum x_n \to x_0$ est un isomorphisme, R_0 est un quotient d'un anneau noethérien donc est noethérien.
Soient x_i des générateurs (en nombre fini car R est noethérien) de I. Si $x_i = \sum_n x_{i,n}$ avec $x_{i,n} \in R_n$, on a $x_{i,n} \in I$ et la famille $(x_{i,n})$ engendre a fortiori I. Quitte à remplacer les x_i par les $x_{i,n}$ on peut donc supposer que pour tout i, on a $x_i \in R_{n(i)}$.
Montrons par récurrence que $R_n \subset R_0[x_1, \cdots, x_r]$. C'est vrai pour $n = 0$. Supposons que c'est vrai pour tout $k \in [0, n-1]$ et soit $y \in R_n$. Comme $y \in I$, il existe des $y_i \in R$ tels que $y = \sum_i y_i x_i$. On écrit $y_i = \sum_m y_{i,m}$ avec $y_{i,m} \in R_m$. En comparant les termes dans R_n on a

$$y = \sum_{i=1}^{r} y_{i,n-n(i)} x_i.$$

Pour tout i, si $n - n(i) < 0$, alors $y_{i,n-n(i)} = 0$ et si $n - n(i) \geq 0$, alors comme $n(i) \geq 1$, on a par hypothèse de récurrence $y_{i,n-n(i)} \in R_0[x_1, \cdots, x_r]$. On voit donc que $y \in R_0[x_1, \cdots, x_r]$ et $R_n \subset R_0[x_1, \cdots, x_r]$.
Il est résulte que $R = \bigoplus_{n=0}^{\infty} R_n \subset R_0[x_1, \cdots, x_r]$. L'autre inclusion étant évidente on a égalité et R est engendrée comme R_0-algèbre par les x_i.
(iv) On a $R(I) = \bigoplus_{n=0}^{\infty} R(I)_n$, avec $R(I)_n = I^n T^n \simeq I^n$. Si I est engendré par $P_1, \cdots, P_r$, on voit que $R(I)$ est engendrée par les $P_i T$ comme $R(I)_0$-algèbre. Par suite, $R(I)$ est un anneau noethérien.

Exercice 31. Idéaux associés.
Soit A un anneau noetherien. Si M est un A-module, et $m \in M$ on note $\mathrm{Ann}(m) = \{a \in A, am = 0\}$. On note $\mathrm{Ass}(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) : \exists m \in M, \mathfrak{p} = \mathrm{Ann}(m)\}$.

a) Montrer que, si $M \neq 0$, $\mathrm{Ass}(M)$ est non vide. Montrer plus précisément que $\bigcup_{\mathfrak{p}\in \mathrm{Ass}(M)} \mathfrak{p} = \{a \in A : \exists x \in M\backslash\{0\}, ax = 0\}$.

b) Montrer que, si M est de type fini, il existe une suite de sous-modules $0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$ tels que $M_k/M_{k-1} = A/\mathfrak{p}_k$ avec $\mathfrak{p}_k \in \mathrm{Spec}\, A$.

c) Montrer que si $N \subset M$ est un sous-module, $\mathrm{Ass}(M) \subset \mathrm{Ass}\, N \cup \mathrm{Ass}\, M/N$.

d) Montrer que si S est une partie multiplicative de A, $\mathrm{Ass}_{S^{-1}A}(S^{-1}M) = \mathrm{Ass}_A(S^{-1}M) = \mathrm{Ass}(M) \cap \mathrm{Spec}(S^{-1}A)$.

e) Montrer que $\mathrm{Ass}(M) \subset \mathrm{Supp}(M) := \{\mathfrak{p} \in \mathrm{Spec}(A) : M_{\mathfrak{p}} \neq 0\}$ et $\mathrm{Ass}(M)$ contient les éléments minimaux de $\mathrm{Supp}(M)$.

Solution. a) Soit $\mathfrak{p}$ un élément maximal pour l'inclusion de $\{\mathrm{Ann}(m), m \in M\backslash\{0\}\}$ (un tel élément maximal existe parce que A est noetherien). Montrons que $\mathfrak{p}$ est premier. Soient $f, g \in A$ tels que $fg \in \mathfrak{p}$ et supposons $f \notin \mathfrak{p}$. Soit $m \in M$ tel que $\mathfrak{p} = \mathrm{Ann}(m)$. Comme $\mathfrak{p} \subsetneq \mathfrak{p} + Af \subset \mathrm{Ann}(gm)$, par maximalité de $\mathfrak{p}$, on a $gm = 0$, et donc $g \in \mathrm{Ann}(m)$, ce qui prouve que $\mathfrak{p}$ est premier, et donc dans $\mathrm{Ass}(M)$.

L'inclusion $\bigcup_{\mathfrak{p}\in \mathrm{Ass}(M)} \mathfrak{p} \subset \{a \in A : \exists x \in M\backslash\{0\}, ax = 0\}$ est évidente. Réciproquement, soit a tel qu'il existe $x \in M\backslash\{0\}$ tel que $ax = 0$. Il existe un élément maximal $\mathfrak{p}$ de $\{\mathrm{Ann}(m), m \in M\backslash\{0\}\}$ qui contient $\mathrm{Ann}(x)$. Alors $\mathfrak{p} \in \mathrm{Ass}(M)$ et $a \in \mathfrak{p}$.

b) On construit M_k par récurrence. Supposons M_k construit et $M_k \neq M$. Soit $\mathfrak{p} = \mathrm{Ann}(m) \in \mathrm{Ass}(M/M_k)$. L'application $A \to M/M_k : a \mapsto am$ induit une injection $f : A/\mathfrak{p} \to M/M_k$. Soit M_{k+1} l'image réciproque dans M de l'image de f.La suite M_k est strictement croissante tant que $M_k \neq M$, donc par noetherianité et finitude de M, il existe k tel que $M = M_k$.

c) Soit $\mathfrak{p} \in \mathrm{Ass}(M)$ et soit $m \in M$ tel que $\mathfrak{p} = \mathrm{Ann}(m)$. Si il existe $a \notin \mathfrak{p}$ tel que $am \in M_1$ alors $\mathrm{Ann}(am) = \{b \in A : ba \in \mathfrak{p}\} = \mathfrak{p}$ par primalité de $\mathfrak{p}$ et donc $\mathfrak{p} \in \mathrm{Ass}\, M_1$. Sinon, en notant $\bar{m}$ l'image de m dans M_2, $\mathrm{Ann}(\bar{m}) = \mathfrak{p}$ et donc $\mathfrak{p} \in \mathrm{Ass}\, M_2$.

d) Soit $\mathfrak{p} = \mathrm{Ann}(m/s) \in \mathrm{Ass}_A(S^{-1}M)$. Comme $m/s \neq 0$, $S \cap \mathrm{Ann}_A(m/s) = \emptyset$. Par noetherianité, l'ensemble $\{\mathrm{Ann}(s'm)\}_{s'\in S}$ admet un élément maximal ; soit $s'_0 \in S$ correspondant. Pour tout $s' \in S$, $\mathrm{Ann}(s'_0 m) \subset \mathfrak{p}$ et si $p \in \mathfrak{p}$, il existe $s'' \in S$ tel que $ps''m = 0$ et donc $p \in \mathrm{Ann}(s''s'_0 m)$. Par maximalité de s'_0, $p \in \mathrm{Ann}(s'_0 m)$ et donc $\mathfrak{p} \in \mathrm{Ass}(M)$: $\mathrm{Ass}_A(S^{-1}M) \subset \mathrm{Ass}(M) \cap \mathrm{Spec}(S^{-1}A)$.

Réciproquement Si $\mathfrak{p} = \mathrm{Ann}(m) \in \mathrm{Ass}(M) \cap \mathrm{Spec}(S^{-1}A)$, $\mathrm{Ann}_A(m/s) = \{a : \exists s' \in S, s'a \in \mathfrak{p}\} = \mathfrak{p}$ par primalité de $\mathfrak{p}$, donc $\mathrm{Ass}_A(S^{-1}M) = \mathrm{Ass}(M) \cap \mathrm{Spec}(S^{-1}A)$.

Si $m/s \in S^{-1}M$, $\mathrm{Ann}_{S^{-1}A}(m/s) = S^{-1}\,\mathrm{Ann}_A(m/s)$ d'où l'autre égalité.

e) Si $\mathfrak{p} \in \mathrm{Ass}(M)$, $\mathfrak{p} \in \mathrm{Ass}(M_{\mathfrak{p}})$ d'après la question précédente, et donc $M_{\mathfrak{p}} \neq 0 : \mathfrak{p} \in \mathrm{Supp}(M)$. Si $\mathfrak{p}$ est un élément minimal de $\mathrm{Supp}\, M$, alors $\mathrm{Supp}_{A_{\mathfrak{p}}} M_{\mathfrak{p}} = \{\mathfrak{p}\}$. Comme $\mathrm{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) \subset \mathrm{Ass}\, M$ est une partie non vide de $\mathrm{Supp}_{A_{\mathfrak{p}}} M_{\mathfrak{p}} = \{\mathfrak{p}\}$, elle contient $\mathfrak{p}$.

Exercice 32. Décomposition primaire.

On suppose encore A noetherien. Un A-module M est dit coprimaire si $\mathrm{Ass}(M)$ est un singleton. Un sous-A-module N de M est dit primaire si M/N est coprimaire.

a) Soit M un A-module non nul. Montrer que M est coprimaire si et seulement si pour tout $a \in A$ diviseur de 0 dans M et pour tout $x \in M$, il existe $n \in \mathbb{N}$ tel que $a^n x = 0$.

b) Soit M un module de type fini et N un sous-module. Montrer qu'il existe une famille fini (Q_i) de sous-modules primaires de M tels que $N = \bigcap Q_i$.

Solution. a) Supposons M coprimaire et soit $\mathfrak{p}$ l'unique idéal associé. On doit donc montrer que si $a \in \mathfrak{p}$, pour tout $x \in M$, il existe n tel que $a^n x = 0$, c'est-à-dire $M[\frac{1}{a}] = 0$. En utilisant exo 31.d, $\mathrm{Ass}(M[\frac{1}{a}]) = \mathrm{Ass}(M) \cap \{\mathfrak{q} \in \mathrm{Spec}\, A, a \notin \mathfrak{q}\} = \emptyset$ puisque $a \in \mathfrak{p}$. Donc $M[\frac{1}{a}]$ est nul d'après exo 31.a.

Supposons que pour tout $a \in A$ diviseur de 0 dans M et pour tout $x \in M$, il existe $n \in \mathbb{N}$ tel que $a^n x = 0$. Soit $\mathfrak{p} = \{a \in A : \exists x \in M\backslash\{0\}, ax = 0\} = \{a \in A : \forall x \in M, \exists n \in N, a^n x = 0\}$. Soit $\mathfrak{q} = \mathrm{Ann}(x) \in \mathrm{Ass}(M)$, alors, $\mathfrak{q} \subset \mathfrak{p}$ d'après exo 31.a. Par hypothèse, si $a \in \mathfrak{p}$, il existe n tel que $a^n x = 0$ et donc $a^n \in \mathfrak{q}$. Par primalité de $\mathfrak{q}$, $a \in \mathfrak{q} : \mathfrak{p} \subset \mathfrak{q}$. Donc tout idéal associé est $\mathfrak{p}$ et comme $\mathrm{Ass}(M) \neq \emptyset$, $\mathrm{Ass}(M) = \{\mathfrak{p}\}$.

b) Quitte à remplacer M par M/N, on peut supposer $N = \{0\}$.

Pour $\mathfrak{p} \in \mathrm{Ass}(M)$, soit $Q_{\mathfrak{p}}$ un élément maximal de $\{N \subset M, \mathfrak{p} \notin \mathrm{Ass}(N)\}$ (il en existe par noetherianité de A et finitude de M et car cet ensemble est non vide puisque $\{0\}$ en fait partie). Montrons que $\mathrm{Ass}(M/Q_{\mathfrak{p}}) = \{\mathfrak{p}\}$. D'abord, comme $\mathfrak{p} \in \mathrm{Ass}(M) \subset \mathrm{Ass}(Q_{\mathfrak{p}}) \cup \mathrm{Ass}(M/Q_{\mathfrak{p}})$ et $\mathfrak{p} \notin \mathrm{Ass}(Q_{\mathfrak{p}})$, on a $\mathfrak{p} \in \mathrm{Ass}(M/Q_{\mathfrak{p}})$. Si

$\mathfrak{q} \in \mathrm{Ass}(M/Q_\mathfrak{p})$, alors il existe $x \in M$ tel que $\mathfrak{q} = \mathrm{Ann}(\bar{x})$ où $\bar{x}$ est l'image de x dans $M/Q_\mathfrak{p}$. On a une suite exacte

$$0 \to Q_\mathfrak{p} \to Q_\mathfrak{p} + Ax \to A/\mathfrak{q} \to 0$$

et donc $\mathrm{Ass}(Q_\mathfrak{p} + Ax) \subset \mathrm{Ass}(Q_\mathfrak{p}) \cup \mathrm{Ass}(A/\mathfrak{q})$. Par maximalité de $Q_\mathfrak{p}$, $\mathfrak{p} \in \mathrm{Ass}(Q_\mathfrak{p} + Ax)$ et donc $\mathfrak{p} \in \mathrm{Ass}(A/\mathfrak{q}) = \{\mathfrak{q}\}$. Donc $\mathfrak{p} = \mathfrak{q}$: $Q_\mathfrak{p}$ est bien primaire. Maintenant, $\mathrm{Ass}(\bigcap_\mathfrak{p} Q_\mathfrak{p}) \subset \bigcap_\mathfrak{p} \mathrm{Ass}(Q_\mathfrak{p}) = \emptyset$ car pour tout $\mathfrak{p} \in \mathrm{Ass}(M), \mathfrak{p} \notin \mathrm{Ass}(Q_\mathfrak{p})$. Donc $\bigcap_\mathfrak{p} Q_\mathfrak{p} = 0$ d'après exo 31.a.

3 Produit tensoriel

Exercice 33. Montrer que $\mathbb{Z}/m\mathbb{Z} \otimes_\mathbb{Z} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$ où d est le pgcd de m et n.
Plus généralement, si A est un anneau et I, J sont des idéaux de A, alors $A/I \otimes_A A/J \simeq A/(I+J)$.

Solution. Considérons $\pi_1 : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ qui envoie $a + m\mathbb{Z}$ sur $a + d\mathbb{Z}$ et $\pi_2 : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ qui envoie $a + n\mathbb{Z}$ sur $a + d\mathbb{Z}$. On obtient un morphisme $f : \mathbb{Z}/m\mathbb{Z} \otimes_\mathbb{Z} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$ en envoyant $a \otimes b$ sur $\pi_1(a)\pi_2(b)$. Ce morphisme est surjectif car $a + d\mathbb{Z} = f((a + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}))$.
Soit $\sum_i (a_i + m\mathbb{Z}) \otimes (b_i + n\mathbb{Z}) \in \ker f$. Alors $\sum_i a_i b_i \in d\mathbb{Z}$. Donc , par le théorème de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $\sum_i a_i b_i = um + vn$. Alors

$$\sum_i (a_i+m\mathbb{Z})\otimes(b_i+n\mathbb{Z}) = \sum_i a_i b_i (1+m\mathbb{Z})\otimes(1+n\mathbb{Z}) = (um+vn)(1+m\mathbb{Z})\otimes(1+n\mathbb{Z}) = (um+m\mathbb{Z}\otimes 1+n\mathbb{Z})+(1+m\mathbb{Z})\otimes(vn+n\mathbb{Z}) =$$

Donc f est injectif.
Le cas général se traite de la même façon.

Exercice 34. Soient A un anneau, I un idéal de A et M un A-module. Montrer que $A/I \otimes_A M \simeq M/IM$, où IM est le sous-module de M engendré par $\{am, a \in I, m \in M\}$.

Solution. Considérons l'application $\phi : A \times M \to M/IM$ qui à (a, m) associe $a\bar{m}$. Si $a_1 + I = a_2 + I$, alors $\phi(a_1, m) = \phi(a_2, m)$ donc ϕ se factorise en une application $A/I \times M \to M/IM$. Cette application est bilinéaire donc induit un morphisme $f : A/I \otimes M \to M/IM$, envoyant $\bar{a} \otimes m$ sur $a\bar{m}$. Le morphisme f est surjectif, car $\bar{m} = f(\bar{1} \otimes m)$.
Soit $x = \sum_i \bar{a}_i \otimes m_i \in \ker f$. Alors $f(x) = \overline{\sum_i a_i m_i} = 0$ donc (il existe une famille (b_j) d'éléments de I et une famille (n_j) d'éléments de M tels que $\sum_i a_i m_i = \sum_j b_j n_j$ avec Alors

$$\sum_i \bar{a}_i \otimes m_i = \sum_i \bar{1} \otimes a_i m_i = \bar{1} \otimes \sum_i a_i m_i = \bar{1} \otimes \sum_j b_j n_j = \sum_j \bar{b}_j \otimes n_j = 0$$

car $\bar{b}_j = 0$. Donc f est injectif.

Exercice 35. Soit A un anneau. Soit $\phi : M_1 \to M_2$ un morphisme de A-module. Soit N un A-module et considérons $\phi \otimes \mathrm{Id}_N : M_1 \otimes N \to M_2 \otimes N$, qui envoie $m \otimes n$ sur $\phi(m) \otimes n$.

a) Montrer que si ϕ est surjective, $\phi \otimes \mathrm{Id}_N$ est surjective.
b) Donner un exemple, pour $A = \mathbb{Z}$ et $N = \mathbb{Z}/n\mathbb{Z}$, d'un morphisme ϕ injectif tel que $\phi \otimes \mathrm{Id}_N$ ne soit pas injectif.

Solution. a) Soit $(m_2, n) \in M_2 \times N$. Soit $m_1 \in M_1$ tel que $m_2 = \phi(m_1)$. Alors $m_2 \otimes n = \phi \otimes \mathrm{Id}_N(m_1 \otimes n)$, donc l'image de $\phi \otimes \mathrm{Id}_N$ contient tous les $\mathfrak{m}_2 \otimes n$. Or $(m_2 \otimes n)_{(m_2,n) \in M_2 \times N}$ engendre $M_2 \otimes N$.

b) Soit $\phi : \mathbb{Z} \to \mathbb{Z}$ la multiplication par 2, ϕ est bien injective. $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ s'identifie avec $\mathbb{Z}/2\mathbb{Z}$ en envoyant $a \otimes b$ sur ab. Alors $\phi \otimes \mathbb{Z}/2\mathbb{Z} : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ est la multiplication par 2, qui n'est pas injective (c'est le morphisme nul).

Exercice 36. Montrer que $M \otimes_A (N_1 \oplus N_2) \simeq (M \otimes_A N_1) \oplus (N \otimes A)$.

4 Polynômes

Exercice 37. Soit A un anneau et soit S un ensemble. Montrer qu'il existe une unique (à isomorphisme près) A-algèbre $A[S]$ et une fonction $i : S \to A[S]$ telles que, pour toute A-algèbre B muni d'une fonction $j : S \to A[S]$, il existe un unique morphisme $f : A[S] \to B$ de A-algèbres tel que $j = fi$.

Exercice 38. Soit M un A-module d'annulateur I. On désigne par $M[X]$ l'ensemble des polynômes à coefficients dans M, c'est-à-dire $\{m_0 + m_1X + \ldots + m_dX^d$, avec $\forall i : m_i \in M\}$.
(i) Montrer que $M[X]$ est naturellement pourvu d'une structure de $A[X]$-module.
(ii) Quel est l'annulateur de $M[X]$?
(iii) Soit N un sous-A-module de M ; montrer que $(M/N)[X] \simeq M[X]/N[X]$.
(iv) Montrer que si M est de type fini alors $M[X]$ est un $A[X]$-module de type fini.
(v) Montrer que si M est un A-module libre alors $M[X]$ est un $A[X]$-module libre.

Solution. (i) On définit la structure de $A[X]$-module par

$$(\sum a_iX^i) \cdot (\sum m_jX^j) = \sum (\sum a_im_j)X^{i+j}.$$

(ii) Soit $P = \sum a_iX^i \in A[X]$, tel que pour tout $Q \in M[X]$, on a $PQ = 0$. En prenant $Q = mX^n$ avec $m \in M$ et $n \in \mathbb{N}$, on obtient $ma_iX^{n+i} = 0$ pour tout i c'est-à-dire $ma_i = 0$. Ainsi pour tout i, on a $a_i \in I$. Autrement dit $P \in I[X]$, l'idéal de $A[X]$ des polynômes à coefficients dans I. L'annulateur de $M[X]$ est donc $I[X]$.
(iii) Considérons l'application $A[X]$-linéaire

$$\phi : M[X] \to (M/N)[X]$$

définie par $\phi(\sum m_iX^i) = \sum Cl(m_i)X^i$ où $Cl(m)$ est la classe de m dans M/N. Elle est surjective et son noyau est $N[X]$ d'où l'isomorphisme demandé.
(iv) Soit $(\mu_1, \cdots, \mu_n)$ une famille de générateurs de M comme A-module. Si $P = \sum m_iX^i \in M[X]$, il existe des $a_{i,j} \in A$ tels que $m_i = \sum_j a_{i,j}\mu_j$ donc

$$P = \sum_i \sum_j a_{i,j}\mu_jX^i = \sum_j (\sum_i ai, jX^i)\mu_j$$

est combinaison linéaire dans $A[X]$ des μ_j. Ainsi les μ_j engendrent $M[X]$ comme $A[X]$-module.
(v) Soit (μ_j) une base de M comme A-module. Le même argument qu'à la question précédente montre que la famille (μ_j) engendre $M[X]$ en tant que $A[X]$-module. Il rste à montrer que c'est une famille libre. Suposons qu'il existe une relation $\sum_j P_j\mu_j$ avec $P_j \in A[X]$. En écrivant $P_j = \sum_i a_{i,j}X^j$, on a

$$0 = \sum_j \sum_i a_{i,j}X^i\mu_j = \sum_i (\sum_j a_{i,j}\mu_j)X^i,$$

ce qui impose $\sum_j a_{i,j}\mu_j = 0$ pour tout i et comme (μ_j) est une famille libre on a $a_{i,j} = 0$ pour tout i et j.

Exercice 39. Soient M et N deux A-modules.
(i) Soit $u \in \mathrm{End}_AM$. Montrer qu'il existe une unique structure de $A[X]$-module sur M telle que $X \cdot m = u(m)$ (et $1 \cdot m = m$) pour tout $m \in M$. On notera M_u le $A[X]$-module M muni de cette structure.
Montrer que cette application $u \mapsto M_u$ induit une bijection entre les structures de $A[X]$-modules sur M et les endomorphismes $u \in \mathrm{End}_AM$.
(ii) Soient $u \in \mathrm{End}_AM$ et $v \in \mathrm{End}_AN$, déterminer tous les homomorphismes de $A[X]$-modules de M_u dans N_v.
(iii) Si $M = N$, à quelle condition a-t-on $M_u \simeq N_v$?
(iv) Comment pouvez-vous interpréter les résultats de l'exercice lorsque $A = k$ est un corps et $M = k^n$ est l'espace vectoriel standard de dimension n sur k ?
Montrer que tous les éléments de M_u sont de torsion.

Solution. (i) Soit $P \in A[X]$, si $X \cdot m = u(m)$, alors $X^n \cdot m = u^n(m)$ et donc $P \cdot m = P(u)(m)$. Il y a donc au plus une structure de $A[X]$-module sur M telle que $X \cdot m = u(m)$.
Par ailleurs, en posant $P \cdot m = P(u)(m)$, on définit bien une structure de $A[X]$-module sur M. En effet, on a $(P + P') \cdot m = (P + P')(u)(m) = P(u)(m) + P'(u)(m) = P \cdot m + P' \cdot m$ et $(PP') \cdot m = (PP')(u)(m) = P(u)(P'(u)(m)) = P \cdot (P' \cdot m)$.
Réciproquement, étant donnée une structure de $A[X]$-module sur M, on $u \in \mathrm{End}_AM$ par $u(m) = X \cdot m$ (il est immédiat que u est A-linéaire).
(ii) Soit $\varphi : M_u \to N_v$ un morphisme de $A[X]$-modules. Si a et a' sont dans A et m et m' dans M, on a $\varphi(ma + m'a') = a \cdot \varphi(m) + a' \cdot \varphi(m') = a\varphi(m) + a'\varphi(m')$ donc φ est A-linéaire. Par ailleurs, $\varphi(X \cdot m) = \varphi(u(m)) = X \cdot \varphi(m) = v(\varphi(m))$ donc on a $\varphi \circ u = v \circ \varphi$.
Réciproquement, si $\varphi \in \mathrm{Hom}_A(M, N)$ est un homomorphisme de A-modules tel que $\varphi \circ u = v \circ \varphi$, il induit un homomorphisme $A[X]$-linéaire de M_u dans N_v. En effet, il suffit de vérifier que $\varphi(X \cdot m) = X \cdot \varphi(m)$ ce qui est équivalent à $\varphi \circ u = v \circ \varphi$.

(III) On a $M_u \simeq M_v$ si et seulement si il existe $\varphi : M \to N$ tel que $\varphi \circ u = v \circ \varphi$ qui soit bijectif et donc la bijection réciproque $\psi : N \to M$ vérifie $\psi \circ v = u \circ \psi$. Cette dernière condition est en fait automatiquement vérifiée si φ est bijectif. Ainsi $M_u \simeq M_v$ si et seulement s'il existe un isomorphisme φ du A-module M tel que $v = \varphi \circ u \circ \varphi^{-1}$.
(IV) Si $A = k$ est un corps et $M = k^n$, les endomorphismes de M s'identifient à leur matrice. On trouve que $M_u \simeq M_v$ si et seulement si les matrices de u et v sont semblables (conjuguées).
Soit $m \in M$ et soit μ_f le polynôme caractéristique (ou minimal) de f. On a alors $\mu_f \cdot m = \mu_f(f)(m) = 0(m) = 0$ car f est annulé par son polynôme caractéristique (ou minimal). Remarquons que cette démonstration fonctionne encore pour M un A-modulede type fini.

5 Suites exactes, complexes

Une suite de morphismes de A-modules

$$\cdots \longrightarrow M_0 \xrightarrow{f_0} M_1 \longrightarrow \cdots \longrightarrow M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} \cdots$$

est dite exacte si pour tout entier i tel que f_{i-1} et f_i soient définis,

$$\ker f_i = \operatorname{Im} f_{i-1}.$$

Exercice 40. Soit $f : M \to N$ un morphisme de A-module, montrer que l'on a la suite exacte :

$$0 \to \ker f \to M \to N \to \operatorname{Coker}(f) \to 0.$$

Montrer qu'elle se décompose en deux suites exactes :

$$0 \to \ker f \to M \to \operatorname{Im} f \to 0 \qquad \text{et} \qquad 0 \to \operatorname{Im} f \to N \to \operatorname{Coker}(f) \to 0.$$

Solution. Le morphisme $\ker f \to M$ est injectif, son noyau est donc (0) qui est l'image du morphisme $0 \to \ker f$. L'image de $\ker f \to M$ est $\ker f$ qui est bien le noyau de $f : M \to N$. Le noyau de $N \to \operatorname{Coker} f$ est $\operatorname{Im} f$ qui est bien l'image de $f : M \to N$. Enfin le noyau de $\operatorname{Coker} f \to 0$ est $\operatorname{Coker} f$ qui est bien l'image de $N \to \operatorname{Coker} f$. Ces raisonnements ont montré que les deux dernières suites sont exactes.

Exercice 41. Soit $(0) \longrightarrow M' \xrightarrow{i} M \xrightarrow{"\pi} M'' \longrightarrow (0)$ une suite exacte de A-modules ; " montrer que les cinq propriétés suivantes sont équivalentes :
(I) $\exists r \in \operatorname{Hom}_A(M, M')$ tel que $r \circ i = \operatorname{Id}_{M'}$,
(II) $\exists s \in \operatorname{Hom}_A(M'', M)$ tel que $\pi \circ s = \operatorname{Id}_{M''}$,
(III) $\exists s \in \operatorname{Hom}_A(M'', M)$ tel que $M = i(M') \oplus s(M'')$,
(IV) $(0) \longrightarrow \operatorname{Hom}_A(N, M') \xrightarrow{i_*} \operatorname{Hom}_A(N, M) \xrightarrow{\pi_*} \operatorname{Hom}_A(N, M'') \longrightarrow (0)$ est une suite exacte pour tout A-module N,
(V) $(0) \longrightarrow \operatorname{Hom}_A(M'', N) \xrightarrow{\pi^*} \operatorname{Hom}_A(M, N) \xrightarrow{i^*} \operatorname{Hom}_A(M', N) \longrightarrow (0)$ est une suite exacte pour tout A-module N.

On dit qu'une suite exacte qui vérifie ces propriétés est scindée.

Solution. Montrons (I)⇒(II) : posons $\sigma = \operatorname{Id}_M - i \circ r$. Si $m = i(m')$, $\sigma(m) = m - i(r(i(m'))) = m - i(m') = 0$, si bien que σ passe au quotient par M'. On en déduit une application A-linéaire $s : M'' \to M$. De plus, si $m'' = \pi(m) \in M''$, on a $(\pi \circ s)(m'') = \pi(\sigma(m)) = \pi(m - i(r(m))) = \pi(m) - (\pi \circ i)(r(m)) = \pi(m) = m''$. Par suite $\pi \circ s = \operatorname{Id}_{M''}$.
Montrons (II)⇒(III) : remarquons que l'application s est injective donc l'application $M' \oplus M'' \to M$, $(m', m'') \mapsto (i(m', s(m''))$ est injective (si $i(m') + s(m'') =$, en appliquant π on trouve $m'' = 0$ puis $i(m') = 0$ donc $m' = 0$ car i est injective). Elle est surjective car si $m \in M$, alors $m - s(\pi(m)) \in \ker \pi = M'$ et $m = i(m - s(\pi(m))) + s(\pi(m))$.
Montrons (III)⇒(I) : on constate que $m - s(\pi(m)) \in i(M')$, il existe donc $r(m) \in M'$ tel que $i(r(m)) = m - s(\pi(m))$. Comme i est injective, $r(m)$ est unique et l'application $m \mapsto r(m)$ est un homomorphisme de M dans M'. Il vérifie $i(r(i(m'))) = i(m') - s(\pi(i(m'))) = i(m')$ donc $r \circ i = \operatorname{Id}_{M'}$.
Montrons (II)⇒(IV) : le seul endroit du complexe où l'exactitude est problématique est la surjectivité de la flèche π_*. Or si $\varphi \in \operatorname{Hom}(N, M'')$, on a $\pi_*(s \circ \varphi) = \pi \circ s \circ \varphi = \varphi$ si bien que $\varphi \in \operatorname{Im}(\pi_*)$ et π_* est surjective.
Réciproquement, pour établir (IV)⇒(II), il suffit d'appliquer l'hypothèse à $N = M''$ et $\varphi = \operatorname{Id}_{M''}$. On trouve $\psi : M'' \to M$ tel que $\pi_*(\psi) = \psi \circ \pi = \operatorname{Id}_{M''}$.
Montrons (I)⇒(V) : seule la surjectivité de i^* n'est pas automatique. Si $\varphi : M' \to M$ est un morphisme, on a $\varphi = \varphi \circ (r \circ i) = (\varphi \circ r) \circ i = i^*(\varphi \circ r) \in \operatorname{Im} i^*$.
Enfin montrons (V)⇒(I) : on applique l'hypothèse à $N = M'$ et $\varphi = \operatorname{Id}_{M'}$. On trouve $\psi : M \to M'$ tel que $i^*(\psi) = \psi \circ i = \operatorname{Id}_{M'}$.

Exercice 42. Soient $M_1, \ldots, M_n$ des A-modules et $f_i : M_i \longrightarrow M_{i+1}$ des homomorphismes de A-modules. On dit que $M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} M_n$ est un complexe (resp. une suite exacte) si pour tout i : $\mathrm{Im}(f_i) \subset \ker(f_{i+1})$ (resp. $\mathrm{Im}(f_i) = \ker(f_{i+1})$).
(i) Soit $(0) \longrightarrow M' \xrightarrow{i} M \xrightarrow{\pi} M'' \longrightarrow (0)$ une suite exacte. Montrer que i est injectif et que π est surjectif.
(ii) Soit $M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} M_n$ un complexe. Montrer que ce complexe est une suite exacte si et seulement si pour tout i les suites $(0) \longrightarrow \ker f_i \longrightarrow M_i \xrightarrow{f_i} \ker f_{i+1} \longrightarrow (0)$ sont exactes.
(iii) On suppose que A est un corps et que les M_i sont des k-espaces vectoriels de dimension finie. Soit

$$0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} M_n \to 0$$

une suite exacte. Montrer que

$$\sum_{i=1}^{n} (-1)^i \dim M_i = 0.$$

Solution. (i) Le noyau de i est l'image de $(0) \to M'$, donc nul. L'image de π est le noyau de $M'' \to (0)$, donc π est surjective.
(ii) Comme $\mathrm{Im}\, f_i \subset \ker f_{i+1}$, on a une application $f_i : M_i \to \ker f_{i+1}$ et un complexe $(0) \to \ker f_i \to M_i \to \ker f_{i+1} \to (0)$. Dire que ce complexe est une suite exacte revient à dire que l'image de f_i dans $\ker f_{i+1}$ est égale à $\ker f_{i+1}$. Celà équivaut à l'exactitude du complexe.
(iii) Si A est un corps et si $(0) \to \ker f_i \to M_i \to \ker fi+1 \to (0)$ est exacte, on peut trouver un supplémentaire de $\ker f_i$ dans M_i qui sera isomorphe à $\ker f_{i+1}$. Ainsi pour tout $i \in [1, n]$, on a $\dim M_i = \dim \ker f_i + \dim \ker f_{i+1}$ (on a noté $f_0 = 0$ et $f_{n+1} = 0$). On a alors

$$\sum_{i=1}^{n} (-1)^i \dim M_i = \sum_{i=1}^{n} (-1)^i \dim \ker f_i + \sum_{i=1}^{n} (-1)^i \dim \ker f_{i+1}$$

donc

$$\sum_{i=1}^{n} (-1)^i \dim M_i = \dim \ker f_0 + (-1)^n \dim \ker f_{n+1} = 0.$$

Exercice 43. Lemme du serpent.
Considérons le diagramme suivant de morphismes de modules :

$$\begin{tikzcd}
 & M_1 \arrow[r, "i"] \arrow[d, "f_1"] & M_2 \arrow[r, "p"] \arrow[d, "f_2"] & M_3 \arrow[r] \arrow[d, "f_3"] & 0 \\
0 \arrow[r] & N_1 \arrow[r, "j"] & N_2 \arrow[r, "q"] & N_3 &
\end{tikzcd}$$

et supposons que les lignes sont des suites exactes et que l'on a les égalités de composées : $f_2 \circ i = j \circ f_1$ et $f_3 \circ p = q \circ f_2$.
(i) Montrer que ce diagramme induit deux diagrammes

$$\ker(f_1) \to \ker(f_2) \to \ker(f_3) \quad \text{et} \quad \mathrm{Coker}(f_1) \to \mathrm{Coker}(f_2) \to \mathrm{Coker}(f_3)$$

qui sont des suites exactes.
(ii) Montrer qu'il existe une flèche canonique $f : \ker(f_3) \to \mathrm{Coker}(f_1)$ tel que la suite

$$\ker(f_1) \to \ker(f_2) \to \ker(f_3) \xrightarrow{f} \mathrm{Coker}(f_1) \to \mathrm{Coker}(f_2) \to \mathrm{Coker}(f_3)$$

est excate.
(iii) Montrer que la flèche $\ker(f_1) \to \ker(f_2)$ (resp. $\mathrm{Coker}(f_2) \to \mathrm{Coker}(f_3)$) est injective (resp. surjective) si et seulement si i (resp. q) l'est.

Solution. Nous ne vérifierons pas les propriétés de linéarités de morphismes, elles découlent directement et facilement des définitions.
(i) Soit $x \in \ker(f_1)$, alors on peut lui associer $i(x) \in M_2$. Montrons que $i(x) \in \ker(f_2)$ ce qui définira le morphisme de $\ker(f_1) \to \ker(f_2)$. En effet, on a $f_2(i(x)) = j(f_1(x)) = j(0) = 0$. De même, si $x \in \ker(f_2)$, alors $p(x)$ est dans $\ker(f_3)$ et on définit ainsi le morphisme de $\ker(f_2) \to \ker(f_3)$.

Vérifions que la suite est exacte. Si $x \in i(\ker(f_1))$, alors $p(x) = 0$ donc on a bien l'inclusion $i(\ker(f_1)) \subset \ker(p|_{\ker(f_2)})$. Soit maintenant $x \in \ker(p) \cap \ker(f_2)$. Alors comme la première ligne est exacte, il existe $y \in M_1$ tel que $x = i(y)$. Mais alors on a $0 = f_2(x) = f_2(i(y)) = j(f_1(y))$ et comme j est injective, on a $f_1(y) = 0$ et donc $y \in \ker(f_1)$.
De même, si $x \in \mathrm{Coker}(f_1)$, alors soit $x' \in N_1$ un antécédent de x. On définit l'image de x dans $\mathrm{Coker}(f_2)$ par l'image de $j(x')$ dans $\mathrm{Coker}(f_2)$. Ceci est bien défini car si x'' est un autre antécédent de x, alors $x' - x'' = f_1(y)$ avec $y \in M_1$. Mais alors $j(x') - j(x'') = j(f_1(y)) = f_2(i(y))$ donc $j(x')$ et $j(x'')$ ont la même image dans $\mathrm{Coker}(f_2)$ ce qui définit un morphisme $\mathrm{Coker}(f_1) \xrightarrow{k} \mathrm{Coker}(f_2)$. De la même manière on définit un morphisme $\mathrm{Coker}(f_2) \xrightarrow{r} \mathrm{Coker}(f_3)$.
Vérifions que la suite est exacte. Si $x \in k(\mathrm{Coker}(f_1))$, alors il existe $y \in \mathrm{Coker}(f_1)$ tel que $x = k(y)$. Si y' est un représentant de y dans N_1, alors $x' = j(y')$ est un représentant de x dans N_2. On a alors $r(x)$ qui est l'image de $q(x')$ dans $\mathrm{Coker}(f_3)$. Cependant $q(x') = q(j(y')) = 0$ par exactitude de la seconde ligne. On a bien l'inclusion $k(\mathrm{Coker}(f_1)) \subset \ker(r)$. Soit maintenant $x \in \ker(r)$ et soit x' est un représentant de x dans N_2. Alors, on a que $q(x') \in \mathrm{Im}(f_3)$ donc il existe $y \in M_3$ tel que $q(x') = f_3(y)$. Par sujectivité de p, il existe $z \in M_2$ tel que $y = p(z)$ donc on a $q(x') = f_3(p(z)) = q(f_2(z))$. On a donc $x' - f_2(z) \in \ker(q)$ donc il existe $t \in N_1$ tel que $j(t) = x' - f_2(z)$. Mais alors $x' = j(t) + f_2(z)$ et x est l'image de $j(t)$ dans $\mathrm{Coker}(f_2)$ c'est-à-dire que x est l'image par k de la classe de $j(t)$ dans $\mathrm{Coker}(f_1)$.
(ɪɪ) Soit x un élément de $\ker(f_3)$, construisons un élément $f(x)$ dans $\mathrm{Coker}(f_1)$. Comme x est un élément de M_3, il existe $y \in M_2$ tel que $x = p(y)$. Considérons alors $f_2(y)$, il est dans le noyau de q. En effet, on a $q(f_2(y)) = f_3(p(y)) = f_3(x) = 0$ car $x \in \ker(f_3)$. Mais alors comme la seconde ligne est exacte, on sait qu'il existe $z \in N_1$ tel que $j(z) = f_2(y)$. L'élément $f(x)$ de $\mathrm{Coker}(f_1)$ est l'image de z.
Le seul choix qui a été fait pour définir ce morphisme est celui de l'élément $y \in M_2$ tel que $p(y) = x$. Soit y' un autre élément tel que $p(y') = x$. Alors on a $y' - y = i(t)$ pour $t \in M_1$. Mais alors $f_2(y') - f_2(y) = f_2(i(t)) = j(f_1(t))$ donc si z' vérifie $j(z') = f_2(y')$, on a $j(z') - j(z) = f_2(y') - f_2(y) = j(f_1(t))$ ce qui impose par injectivité de j que $z' - z = f_1(t)$ c'est-à-dire que les images de z et z' dans $\mathrm{Coker}(f_1)$ sont égales. Le morphisme f est bien défini.
Pour montrer l'exactitude, il faut montrer que $\ker(f)$ est l'image du morphisme $\ker(f_2) \to \ker(f_3)$ et que $\mathrm{Im}(f)$ est le noyau du morphisme $\mathrm{Coker}(f_1) \to \mathrm{Coker}(f_2)$.
Soit x dans l'image de $\ker(f_2) \to \ker(f_3)$, c'est-à-dire $x = p(y)$ avec $y \in \ker(f_2)$. On calcule alors $f(x)$. Un relevé de x est y, on lui applique f_2 et on a $f_2(y) = 0$ donc $f_2(y) = j(0)$ c'est-à-dire $z = 0$ et $f(x) = 0$. Soit maintenant $x \in \ker(f)$. On prend $y \in M_2$ tel que $p(y) = x$ et z tel que $j(z) = f_2(y)$. On a alors $z \in \mathrm{Im}(f_3)$ donc il existe $t \in M_1$ tel que $z = f_1(t)$. Mais alors $f_2(y) = j(z) = j(f_1(t)) = f_2(i(t))$ donc $y - i(t) \in \ker(f_2)$. Mais alors on a $p(y - i(t)) = p(y) = x$ (car la première ligne est exacte) donc x est bien dans l'image de $\ker(f_2) \to \ker(f_3)$.
Soit $f(x)$ un élément de l'image de f. Notons encore $y \in M_2$ tel que $p(y) = x$ et $z \in N_1$ tel que $j(z) = f_2(y)$. L'image de $f(x)$ par le morphisme $\mathrm{Coker}(f_1) \to \mathrm{Coker}(f_2)$ est donnée par la classe de $j(z)$ dans $\mathrm{Coker}(f_2)$. Mais $j(z) = f_2(y)$ donc son image est nulle dans $\mathrm{Coker}(f_2)$. Si maintenant t est un élément du noyau de $\mathrm{Coker}(f_1) \to \mathrm{Coker}(f_2)$. Soit z un relevé de t dans M_1, alors la classe de $j(z)$ dans $\mathrm{Coker}(f_2)$ est nulle ce qui signifie qu'il existe $y \in M_2$ tel que $j(z) = f_2(y)$. Alors si on pose $x = p(y)$, on a bien $f(x) = t$.
(ɪɪɪ) Soit x dans le noyau de $\ker(f_1) \to \ker(f_2)$, alors il est aussi dans le noyau de i. Réciproquement, si x est dans $\ker(i)$, alors on a $0 = f_2(i(x)) = j(f_1(x))$ et comme j est injectif on a $f_1(x) = 0$ donc $x \in \ker(f_1)$ et est donc dans le noyau de $\ker(f_1) \to \ker(f_2)$. On a la première équivalence.
Supposons q surjectif et soit $x \in \mathrm{Coker}(f_3)$. Soit alors x' un antécédent de x dans N_3, par sujectivité de q, il existe $y' \in N_2$ tel que $q(y') = x'$. Si y est la classe de y' dans $\mathrm{Coker}(f_2)$, alors l'image de y par le morphisme $\mathrm{Coker}(f_2) \to \mathrm{Coker}(f_3)$ est x. Réciproquement, si le morphisme $\mathrm{Coker}(f_2) \to \mathrm{Coker}(f_3)$ est surjectif, soit $x' \in N_3$ et x son image dans $\mathrm{Coker}(f_3)$. Il existe alors $y \in \mathrm{Coker}(f_2)$ tel que l'image de y par le morphisme $\mathrm{Coker}(f_2) \to \mathrm{Coker}(f_3)$ est x. Ceci signifie que si y' est un antécédent de y dans N_2, on a que x est la classe de $q(y')$ dans $\mathrm{Coker}(f_3)$. Il existe donc $z \in M_3$ tel que $x' - q(y') = f_3(z)$. Mais alors par surjectivité de p, il existe $t \in M_2$ tel que $p(t) = z$ et on a $x' = q(y') + f_3(p(t)) = q(y') + q(f_2(t))$ et on a la surjectivité.

Exercice 44. Lemme des 5.
Considérons le diagramme commutatif suivant à lignes exactes :

$$\begin{tikzcd}
M_1 \arrow[r] \arrow[d, "f_1"] & M_2 \arrow[r] \arrow[d, "f_2"] & M_3 \arrow[r] \arrow[d, "f_3"] & M_4 \arrow[r] \arrow[d, "f_4"] & M_5 \arrow[d, "f_5"] \\
N_1 \arrow[r] & N_2 \arrow[r] & N_3 \arrow[r] & N_4 \arrow[r] & N_5
\end{tikzcd}$$

Montrer que :

a) si f_1 est surjective et f_2, f_4 sont injectives, alors f_3 est injective ;

b) si f_5 est injective et f_2, f_4 sont surjectives, alors f_3 est surjective.

Exercice 45. Théorème d'acyclicité.
Soit A un anneau, et soient $a, \beta \in A$ tels que $(a) + (b) = A$. Soit M un A-module. Montrer que la suite

$$0 \longrightarrow M \xrightarrow{\phi} M[\frac{1}{a}] \oplus M[\frac{1}{b}] \xrightarrow{\psi} M[\frac{1}{ab}],$$

où $\phi(m) = (m/1, m/1)$ et $\psi(m/a^i, m'/b^j) = (ma^j b^{i+j} - m' a^{i+j} b^i)/(ab)^{i+j}$, est une suite exacte.
Généraliser à une famille génératrice quelconque $(a_i)_{i \in I}$ de A.