TD n°2 - Solutions.

Exercice 1. Soit k un corps et $A = k[X,Y]/(X^2, XY, Y^2)$.
(i) Déterminer les éléments inversibles de A.
(ii) Déterminer tous les idéaux principaux de A.
(iii) Déterminer tous les idéaux de A.

Solution. (i) Soient x et y les images de X et Y dans A. On a $x^2 = xy = y^2$, ainsi tou élément de A s'écrit sous la forme $a + bx + cy$ avec a, b et c dans k. Cet élément est inversible si et seulement s'il existe a', b' et c' dans k tels que

$$(a + bx + cy)(a' + b'x + c'y) = 1$$

c'est-à-dire

$$aa' + (ab' + a'b)x + (ac' + a'c)y = 1.$$

Ceci impose que l'on ait $aa' = 1$, $ab' + a'b = 0$ et $ac' + a'c = 0$. Ce système a une solution si et seulement si $a \neq 0$, la solution est alors $a' = \frac{1}{a}$, $b' = -\frac{b}{a^2}$ et $c' = -\frac{c}{a^2}$. Ainsi $a+bx+cy$ est inversible si et seulement si $a \neq 0$.
(ii) Soit I un idéal principal de A. Si $I = A$, alors I est engendré par un élément inversible quelconque. Supposons $I \neq A$, alors I est engendré par un élément non inversible donc de la forme $bx + cy$. Il reste à déterminer à quelle condition deux éléments $bx + cy$ et $b'x + c'y$ définissent le même idéal c'est-à-dire à quelle condition ils diffèrent par multiplication par un inversible.
On cherche donc $\alpha + \beta x + \gamma y$ tel que $\alpha \neq 0$ et $(\alpha + \beta x + \gamma y)(bx + cy) = b'x + c'y$. Ceci nous donne $\alpha b = b'$ et $\alpha c = c'$, c'est-à-dire les couple (b, c) et (b', c') sont proportionnels. Ainsi, on voit que si $b \neq 0$, on peut supposer $b = 1$ et on a $c \in k$ quelconque. Si par contre $b = 0$ et $c \neq 0$, on peut supposer $c = 1$ et on a le couple $(0, 1)$, enfin il y a le couple $(0, 0)$. Les idéaux principaux de A sont donc A, $(x + cy)$, (y) et (0).
(iii) Soit I un idéal non principal de A. Alors I est engendré par deux éléments qui sont de la forme $ax + by$ et $cx + dy$ (ils ne peuvent être inversibles sinon $I = A$ est principal) et non proportionnels. Ainsi les vecteurs (a, b) et (c, d) engendrent tout k^2 c'est-à-dire que $ax + by$ et $cx + dy$ engendrent tous les termes de la forme $\alpha x + \beta y$. L'idéal I contient donc l'idéal (x, y). Or $A/(x, y) \simeq k$ donc (x, y) est maximal. Comme $I \neq A$, on a $I = (x, y)$ qui est le seul idéal non principal de A.

Exercice 2. Soit k un corps et A une k-algèbre de dimension finie comme k-espace vectoriel.

a) Montrer qu'une algèbre *intègre* de dimension finie sur un corps est un corps [Montrer que l'application de multiplication par a non nul est injective puis surjective].

b) Soit $\mathfrak{p} \in \mathrm{Spec}(A) = \{\mathfrak{p} \ / \ \mathfrak{p} \text{ est un idéal premier}\}$.
Montrer que $A/\mathfrak{p}$ est de dimension finie sur k.

c) Montrer que $\mathfrak{p}$ est un idéal maximal.
Soient $\mathfrak{p}_i \in \mathrm{Spec}(A), i = 1, \cdots, n$ des idéaux distincts.

d) Montrer que la flèche

$$A \to \bigoplus_{i=1}^{n} A/\mathfrak{p}_i$$

est surjective. En déduire l'inégalité $n \leq \dim_k(A)$.
On suppose dorénavant A réduite (c'est-à-dire nil(A) = 0).

e) Montrer que la flèche

$$A \to \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(A)} A/\mathfrak{p}$$

est un isomorphisme d'anneaux.

f) Considérons l'algèbre $A = \mathbb{R}[X]/((X^2 + a)X(X + 1))$ avec $a \in \mathbb{R}$.
À quelle condition sur $a \in \mathbb{R}$, l'algèbre A est elle réduite ?

g) Dans le cas où A est réduite, expliciter l'isomorphisme précédent.

Solution. (ı) Soit $a \in A$ un élément non nul. Il faut montrer que a est inversible. Considérons alors l'application A-linéaire (et donc k-linéaire) :

$$\mu_a : A \to A$$
$$x \mapsto ax.$$

Son noyau est formé des $x \in A$ tels que $ax = 0$ mais comme A est intègre et $a \neq 0$, on a $x = 0$. Ainsi μ_a est injective et comme A est un k-espace vectoriel de dimension finie, elle est aussi surjective. Il existe donc $b \in A$ tel que $\mu_a(b) = 1_A$ c'est-à-dire $ab = 1_A$ et donc a est inversible d'inverse b.
(ıı) Soit $\mathfrak{p} \in \mathrm{Spec}(A) = \{\mathfrak{p} \ / \ \mathfrak{p} \text{ est un idéal premier}\}$.
(ıı).a. On a une application A-linéaire (et donc k-linéaire) surjective $A \to A/\mathfrak{p}$. Ainsi comme A est de dimension finie sur k, c'est aussi le cas de $A/\mathfrak{p}$.
(ıı).b. La k-algèbre $A/\mathfrak{p}$ est de dimension finie et intègre (car $\mathfrak{p}$ est un idéal premier). On peut donc appliquer le **1.** pour dire que $A/\mathfrak{p}$ est un corps. Ainsi $\mathfrak{p}$ est maximal.
Soient $\mathfrak{p}_i \in \mathrm{Spec}(A), i = 1, \cdots, n$ des idéaux distincts.
(ıı).c. On a vu au (ıı).b que les $\mathfrak{p}_i$ sont maximaux, ainsi si $\mathfrak{p}_i \neq \mathfrak{p}_j$, alors $\mathfrak{p}_i + \mathfrak{p}_j$ est un idéal contenant strictement $\mathfrak{p}_i$ et par maximalité, on a $\mathfrak{p}_i + \mathfrak{p}_j = A$. On peut donc appliquer le lemme chinois aux $\mathfrak{p}_i$. Et on a

$$A/(\mathfrak{p}_1 \cdots \mathfrak{p}_n) \simeq \bigoplus_{i=1}^{n} A/\mathfrak{p}_i.$$

Ainsi l'application

$$A \to \bigoplus_{i=1}^{n} A/\mathfrak{p}_i$$

s'identifie à

$$A \to A/(\mathfrak{p}_1 \cdots \mathfrak{p}_n)$$

qui est évidement surjective.
Comme les $\mathfrak{p}_i$ sont premiers, on a $A/\mathfrak{p}_i \neq 0$ donc $\dim_k(A/\mathfrak{p}_i) \geq 1$. On voit alors que

$$\dim_k(A) \geq \dim_k \left(\bigoplus_{i=1}^{n} A/\mathfrak{p}_i \right) \geq n.$$

(ıı).d D'après ce qui précède, on a nécessairement $\mathrm{card}(\mathrm{Spec}(A)) \leq \dim_k(A)$, c'est-à-dire qu'on a un nombre fini d'idéaux premiers. On peut donc reprendre le raisonnement précedent avec tous les idéaux premiers et on a

$$A/(\prod_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}) \simeq \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(A)} A/\mathfrak{p}.$$

Cependant, on a évidement que

$$\prod_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} \subset \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} = \mathrm{Nil}(A)$$

et ce dernier idéal est nul car A est réduite. Ainsi, on a l'isomorphisme

$$A \simeq \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(A)} A/\mathfrak{p}.$$

(ıı) Considérons l'algèbre $A = \mathbb{R}[X]/((X^2 + a)X(X + 1))$ avec $a \in \mathbb{R}$.
(ıı).a On a ici un anneau factoriel $\mathbb{R}[X]$, ainsi le quotient $A = \mathbb{R}[X]/((X^2 + a)X(X + 1))$ est réduit si et seulement si l'élément $(X^2 + a)X(X + 1)$ n'a pas de facteur carré. Il y a alors quatre cas à distinguer :
1. Si $a > 0$, alors $X^2 + a$ est irréductible sur $\mathbb{R}$, il n'y a pas de facteur carré et A est réduite.
2. Si $a = 0$, alors il y a un facteur carré (et même cube) : X^3 et A n'est pas réduite.
3. Si $a = -1$, alors $X^2 + a = (X - 1)(X + 1)$ et $(X + 1)^2$ est un facteur carré, A n'est pas réduite.
4. Si $a < 0$ et $a \neq -1$, alors $X^2 + a = (X + \sqrt{-a})(X - \sqrt{-a})$ et il n'y a pas de facteur carré, A est réduite.

(ıı).b Notons $\overline{P}$ la classe d'un polynôme $P \in \mathbb{R}[X]$ dans A. L'isomorphisme précedent est alors donné dans le cas 4. par

$$A \simeq \mathbb{R}[X]/(X - a) \oplus \mathbb{R}[X]/(X + a) \oplus \mathbb{R}[X]/(X) \oplus \mathbb{R}[X]/(X + 1) \simeq \mathbb{R}^4$$
$$\overline{P} \mapsto (P(a), P(-a), P(0), P(1)).$$

Dans le cas 1. il est donné par

$$A \simeq \mathbb{R}[X]/(X^2+a) \oplus \mathbb{R}[X]/(X) \oplus \mathbb{R}[X]/(X+1) \simeq \mathbb{C} \oplus \mathbb{R}^2$$

$$\overline{P} \mapsto (\alpha X + \beta, P(0), P(1)) \mapsto (P(\sqrt{-a}), P(0), P(1))$$

avec

$$\sqrt{-a} = i\sqrt{a}, \quad \alpha = \frac{P(\sqrt{-a}) - P(-\sqrt{-a})}{2\sqrt{-a}} \quad \text{et} \quad \beta = \frac{P(\sqrt{-a}) + P(-\sqrt{-a})}{2}.$$

Dans le cas 4, le morphisme se factorise par $\mathbb{R}[X]/(X^2+a) \oplus \mathbb{R}[X]/(X) \oplus \mathbb{R}[X]/(X+1)$ et la seconde formule est encore valable ce qui donne une formule valable dans tous les cas.

Exercice 3. Un anneau est dit local s'il contient un unique idéal maximal.

a) Montrer qu'un anneau A est local si et seulement si $A \backslash A^*$ est un idéal.

b) À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est il local ?

c) Soient A un anneau local, I, J deux idéaux de A et $a \in A$ un élément non diviseur de 0 tels que $IJ = (a)$. Montrer qu'il existe $x \in I$ et $y \in J$ tels que $a = xy$. En déduire que $I = (x)$ et $J = (y)$.

Solution. a) Si A est local, notons $\mathfrak{m}$ l'idéal maximal. Tout élément non-inversible est inclus dans un idéal maximal, qui est nécessairement $\mathfrak{m}$. Donc $A \backslash A^* \subset \mathfrak{m}$. Réciproquement les éléments de $\mathfrak{m}$ ne sont pas inversible et donc $A \backslash A^* = \mathfrak{m}$ est bien un idéal.

Réciproquement, tout idéal propre I est constitué d'éléments non-inversibles, donc $I \subset A \backslash A^*$. Si donc $A \backslash A^*$ est un idéal, alors c'est le plus grand idéal propre. Donc A est bien local.

b) Si $A = \mathbb{Z}/n\mathbb{Z}$, les idéaux maximaux sont les pA, où p décrit les nombres premiers divisant n. Donc A est local si et seulement si n est une puissance d'un nombre premier.

c) Supposons par l'absurde que pour tout $(x, y) \in I \times J$, $a \notin (xy)$. Comme $xy \in (a)$, il existe $u \in A$ tel que $xy = ua$. Or $u \notin A^\times$ car sinon $xy \in A$, donc $u \in \mathfrak{m}$. Donc $xy \in a\mathfrak{m}$. Comme c'est vrai pour tout couple (x, y), on en déduit $IJ \subset a\mathfrak{m} \subsetneq (a)$. Contradiction.

1 Modules

Exercice 4. Soit M un A-module, on définit $M^\vee = \hom_A(M, A)$. On dit que M est réflexif si le morphisme naturel $\theta : M \to M^{\vee\vee}$ défini par $m \mapsto \theta(m) = (\varphi \mapsto \varphi(m))$ avec $\varphi \in M^\vee = \hom_A(M, A)$ est un isomorphisme. Soit $f \in \mathrm{End}_A M$, on définit sa transposée ${}^t f \in \mathrm{End}_A M^\vee$ par ${}^t f(\varphi) = \varphi \circ f$ pour tout $\varphi \in M^\vee = \hom_A(M, A)$.

a) Montrer que l'ensemble des polynômes P de $A[X]$ tels que $P(f) = 0$ est un idéal que l'on notera $I(f)$.

b) Montrer que $I(f) \subset I({}^t f)$.

c) Montrer que ${}^t({}^t f) \circ \theta = \theta \circ f$.

d) Montrer que si M est réflexif, on a $I(f) = I({}^t f)$.

Solution. a) Considérons le morphisme de A-modules$\psi : A[X] \to \mathrm{End}_A M$ défini par $\psi(P) = P(f)$. On a $I(f) = \ker \psi$ donc c'est un idéal.

b) Soit $P \in I(f)$ On a alors $P(f) = 0$. On calcule alors $P({}^t f)(\varphi)$ pour $\varphi \in M^\vee$. On a $P({}^t f)(\varphi) = \varphi \circ P(f) = 0$ car $P \in I(f)$. On a donc $P({}^t f) = 0$ donc $P \in I({}^t f)$. On a bien $I(f) \subset I({}^t f)$.

c) On a

$$\big({}^t({}^t f) \circ \theta\big)(m) = {}^t({}^t f)(\theta(m)) = \theta(m) \circ {}^t f$$

et pour $\varphi \in M^\vee$, on a

$$\Big(\big({}^t({}^t f) \circ \theta\big)(m)\Big)(\varphi) = (\theta(m) \circ {}^t f)(\varphi) = (\theta(m))(\varphi \circ f) = \varphi(f(m)).$$

Par ailleurs, on a

$$(\theta \circ f)(m) = \theta(f(m))$$

et pour $\varphi \in M^\vee$, on a

$$\big((\theta \circ f)(m)\big)(\varphi) = \big(\theta(f(m))\big)(\varphi) = \varphi(f(m)),$$

ce qui prouve l'égalité ${}^t({}^t f) \circ \theta = \theta \circ f$.

d) Si M est réflexif on a donc ${}^t({}^tf) = \theta \circ f \circ \theta^{-1}$. Soit $P \in I({}^tf)$. On a alors $P \in I({}^t({}^tf))$, ainsi $P(\theta \circ f \circ \theta^{-1}) = P({}^t({}^tf)) = 0$ c'est-à-dire $\theta \circ P(f) \circ \theta^{-1} = 0$. Comme θ est inversible, ceci impose que $P(f) = 0$ donc $P \in I(f)$.

Exercice 5. Soit M un A-module

a) On suppose que M est monogène, montrer qu'il existe un idéal I de A tel que $M \simeq A/I$.

b) On suppose que $M \neq (0)$ est simple (c'est-à-dire que ses seuls sous-modules sont (0) et M). Montrer que M est monogène, engendré par tout élément non nul de M. Montrer que M est isomorphe à $A/\mathfrak{m}$ où $\mathfrak{m}$ est un idéal maximal de A.

c) Quels sont les $\mathbb{Z}$-modules simples ?

Solution. a) Soit m un générateur de M et considérons le morphisme de A-module $f : A \to M,\ a \mapsto am$. Il est surjectif (car m engendre M) et son noyau est un idéal I de A. Le morphisme $\overline{f} : A/I \to M$ est donc un isomorphisme.

b) Soit $m \in M$ un élément non nul et soit N le sous-module de M engendré par m. Comme $0 \neq m \in N$, le sous-module N est non nul, c'est donc M tout entier. L'élément m engendre donc M.

D'après la question précédente, on sait qu'il existe un idéal $\mathfrak{m}$ tel que $M \simeq A/\mathfrak{m}$. Il reste à vérifier que cet idéal est maximal. Soit donc I un idéal contenant strictement $\mathfrak{m}$, alors on a la suite exacte

$$0 \to I/\mathfrak{m} \to M \simeq A/\mathfrak{m} \to A/I \to 0.$$

Le module $I/\mathfrak{m}$ est donc un sous-module strict de M, il doit être nul c'est-à-dire $I = \mathfrak{m}$ donc $\mathfrak{m}$ est maximal.

c) D'après la question précédente, les modules simples de $\mathbb{Z}$ sont de la forme $\mathbb{Z}/\mathfrak{m}$ où $\mathfrak{m}$ est un idéal maximal. Il reste à déterminer les idéaux maximaux de $\mathbb{Z}$. Comme $\mathbb{Z}$ est principal, on a $\mathfrak{m} = (n)$ avec $n \in \mathbb{Z}$. L'idéal, (n) est maximal si et seulement si $\mathbb{Z}/(n)$ est un corps, c'est le cas si et seulement si n est premier. Les $\mathbb{Z}$ modules simples sont les $\mathbb{Z}/(p)$ avec p un nombre premier.

Exercice 6. Soit A un anneau intègre et M un A-module. On dit que $x \in M$ est de torsion si il existe $a \in A - \{0\}$ tel que $ax = 0$. On note $T(M)$ l'ensemble des éléments de torsion de M. Si $T(M) = 0$ on dit que M est sans torsion.

a) Montrer que l'ensemble des éléments de torsion de M est un sous-module de M.

b) Montrer que $M/T(M)$ est sans torsion.

c) Montrer que si $f : M \to N$ est un morphisme de A-modules alors $f(T(M)) \subset T(N)$.

Solution. (i) Il faut montrer que $T(M)$ est non vide et stable par addition et multiplication par un scalaire.
Il est clair que $0 \in T(M)$ car $(0 : 0) = \mathrm{Ann}(0) = M$.
Soit maintenant m et m' dans TM), a et a' dans A et x et x' dans $M - \{0\}$ tels que $xm = 0$ et $x'm' = 0$. Alors on a $(xx')(ax + a'm') = ax'(xm) + ax(x'm') = 0$ et $xx' \neq 0$ car A est intègre. Ainsi $T(M)$ est stable par addition et multiplication par un scalaire.
$T(M)$ est donc un sous-module de M.
(ii) Soient $Cl(m) \in M/T(M)$ et $a \in A - \{0\}$ tels que $a \cdot Cl(m) = 0$. Ceci signifie que $am \in T(M)$. Il existe donc $x \in A - \{0\}$ tel que $x(am) = 0$ et donc $(xa)m = 0$. Comme $a \in A - \{0\}$ et $x \in A - \{0\}$ on a $xa \in A - \{0\}$ (A intègre) et donc $m \in T(M)$. On a donc $Cl(m) = 0$ ce qui signifie que le seul élément de torsion de $M/T(M)$ est 0, le module $M/T(M)$ est donc sans torsion.
(iii) Soit $m \in T(M)$ et $x \in A - \{0\}$ tels que $xm = 0$. On considère alors $f(m)$ et on a $af(m) = f(am) = f(0) = 0$. L'élément $f(m)$ est donc de torsion d'où l'inclusion $f(T(M)) \subset T(N)$.

Exercice 7. Soit M un A-moduleet $m \in M$ un élément dont l'annulateur $\mathrm{Ann}(m)$ est réduit à (0). Montrer que Am est facteur direct de M si et seulement si il existe $f \in M^\vee = \hom_A(M, A)$ tel que $f(m) = 1$. Montrer qu'alors on a $M = Am \oplus \ker f$.

Solution. Soit N un facteur direct de Am de sorte que $M = Am \oplus N$. Comme $\mathrm{Ann}(m) = (0)$, l'homomorphisme $A \to Am,\ a \mapsto am$ est un isomorphisme. On peut alors définir une forme linéaire f sur M par $f(am, n) = a$. On a bien $f(m) = 1$.
Réciproquement, s'il existe un tel f, le noyau de f est un sous-module N de M. De plus, si $am \in Am \cap N$, alors $f(am) = a = 0$ donc $Am \cap N = 0$. Enfin, si $m' \in M$, on écrit $m' = f(m')m + (m' - f(m')m)$. On a $f(m')m \in Am$ et $f(m' - f(m')m) = 0$ donc $m' - f(m')m \in N$ ce qui prouve que $Am \oplus N = M$.

Exercice 8. 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 9. 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 5 pour une preuve plus générale).

Exercice 10. 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 11. 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 12. 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 $(e_1, \dots, e_n)$ 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-module$\theta : \ker\varphi \oplus \mathrm{Im}\,\psi \to M$ 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 $(f_i)_{1\le i\le k}$ 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 $\ker\varphi \simeq M/\,\mathrm{Im}\,\psi$ est un quotient d'un module de type fini et est donc aussi de type fini.

Exercice 13. Soit P un A-module. Montrer que les propriétés suivantes sont équivalentes :
(a) pour tout morphisme surjectif de A-module $g : E \to F$ et pour tout $f \in \hom_A(P, F)$, il existe $h \in \hom_A(P, E)$ 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 14. 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.

Exercice 15. Lemme de Nakayama.

a) 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).

b) En déduire que si A est local, $I = \mathfrak{m}$ son idéal maximal et $M = \mathfrak{m}M$ alors $M = 0$.

c) 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 16. 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 17. 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 Noetherianité

Exercice 18. 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 $(b_{n,k})_{1 \le k \le k_n}$. 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 $(P_{n,k})_{1 \le n \le n_0, 1 \le k \le k_n}$, 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 $d \le n_0$, 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 19. 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 20. Soient M, M' et M'' trois A-modules et $i : M' \to M$ un homomorphisme injectif et $\pi : M \to M''$ 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 21. 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 22. (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 $u=\sum u_ix_i+ta$ avec $t\in A$. Mais alors $ta=u-\sum u_ix_i\in I$ donc $t\in(I:a)$. On peut donc écrire $t=\sum t_jy_j$. On a donc

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

(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 23. Soit A un anneau noethérien et I un idéal réduit (c'est-à-dire $I = \sqrt{I}$). On veut montrer qu'il existe des idéaux premiers $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ de A tels que $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$
Supposons par l'absurde qu'il existe un idéal réduit qui n'est pas intersection finie d'idéaux premiers, et soit I_0 maximal parmi les idéaux réduits qui ne sont pas intersection finie d'idéaux premiers (justifier l'extistence d'un tel I_0).

a) Montrer qu'il existe $a, b \notin I_0$ tels que $ab \in I_0$. On note $J = I_0 + aA$ et $K = I_0 + bA$.
b) Montrer que $JK \subset I_0 \subset J \cap K$.
c) Montrer que $I_0 = \sqrt{J} \cap \sqrt{K}$.
d) En déduire une contradiction.

Solution. Comme A est noethérien toute famille non vide d'idéaux admet un élément maximal, en particulier la famille des idéaux réduits qui ne sont pas intersection finie d'idéaux premiers.

a) Comme I_0 n'est pas un idéal premier, il existe $a, b \notin I_0$ tels que $ab \in I_0$.
b) $I_0 \subset J$ et $I_0 \subset K$ donc $I_0 \subset J \cap K$. De plus si $x_1 = i_1 + ay_1 \in J$ et $x_2 = i_2 + by_2 \in K$ avec $i_1, i_2 \in I_0$ et $y_1, y_2 \in A$, $x_1x_2 = i_1i_2 + ay_1i_2 + by_2i_1 + aby_1y_2 \in I_0$ en tant que combinaison linéaire d'éléments de I_0. Or JK est engendré par les éléments de la forme x_1x_2, donc $JK \subset I$.
c) De la question précédente, on déduit que $\sqrt{JK} \subset \sqrt{I_0} \subset \sqrt{J \cap K}$. Comme I_0 est réduit $\sqrt{I_0} = I_0$. De plus $\sqrt{JK} = \sqrt{J \cap K} = \sqrt{J} \cap \sqrt{K}$ d'après l'exo 1, donc les deux inclusions dans $\sqrt{JK} \subset \sqrt{I_0} \subset \sqrt{J \cap K}$ sont des égalités.
d) Comme $I_0 \subsetneq J \subset \sqrt{J}$ et $I_0 \subsetneq K \subset \sqrt{K}$ et comme $\sqrt{J}$ et $\sqrt{K}$ sont réduits, on en déduit par maximalité de I_0 que $\sqrt{J}$ et $\sqrt{K}$ sont des intersections finies d'idéaux premiers. Comme $I_0 = \sqrt{J} \cap \sqrt{K}$, I_0 est lui aussi intersection finie d'idéaux premiers. D'où la contradiction.

Exercice 24. 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 $u = x$ et $n = 0$. Si $x \in (a)$, il existe un unique x_1 tel que $x = ax_1$ (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.
D'où l'existence, il reste à prouver l'unicité. Supposons $x = ua^n = va^m$ 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 25. 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 26. 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

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

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

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

dont le noyau est $\ker(f) \cap \mathrm{Im}(f^{n_0})$. 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

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

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 27. 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 28. 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 $\{m_0 + m_1 X + \ldots + m_d X^d$, 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

$$(\sum a_i X^i) \cdot (\sum m_j X^j) = \sum (\sum a_i m_j) X^{i+j}.$$

(ii) Soit $P = \sum a_i X^i \in A[X]$, 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 $ma_i X^{n+i} = 0$ 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 $\phi(\sum m_i X^i) = \sum Cl(m_i)X^i$ 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 $P = \sum m_i X^i \in M[X]$, il existe des $a_{i,j} \in A$ tels que $m_i = \sum_j a_{i,j}\mu_j$ donc

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

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 29. Soient M et N deux A-modules.
(i) Soit $u \in \mathrm{End}_A M$. 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 $u \in \mathrm{End}_A M$.
(ii) Soient $u \in \mathrm{End}_A M$ et $v \in \mathrm{End}_A N$, 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 $u \in \mathrm{End}_A M$ 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.