EPFL Automne 2022
Algebre Lineaire Avancee, MATH-110

Série 4 - Solution

---

1 Anneaux

Solution 1.

1) En premier on montre que $(M_2(A), +, 0_2)$ est un groupe commutatif.

— Neutralité de 0_2 : Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2$ arbitraire. On a

$$\begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0_A + a & 0_A + b \\ 0_A + c & 0_A + d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix}$$

Ici on a utilisé la neutralité de 0_A dans A.

— Inversibilité : Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2$ arbitraire. L'inverse est $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} \in M_2$ car

$$\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a + a & -b + b \\ -c + c & -d + d \end{pmatrix} = \begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

Ici on a utilisé l'inversiblilité de $+$ dans A.

— Associativité : Soient $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}, \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \in M_2$ arbitraire. On a

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right) + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

$$= \begin{pmatrix} (a + a') + a'' & (b + b') + b'' \\ (c + c') + c'' & (d + d') + d'' \end{pmatrix} = \begin{pmatrix} a + a' + a'' & b + b' + b'' \\ c + c' + c'' & d + d' + d'' \end{pmatrix}$$

$$= \begin{pmatrix} a + (a' + a'') & b + (b' + b'') \\ c + (c' + c'') & d + (d' + d'') \end{pmatrix} = \ldots = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \right)$$

Ici on a utilisé l'associativité de $+$ dans A.

— Commutativité : Soient $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & b' \\ c' & d' \end{pmatrix} \in M_2$. On a

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}+\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} = \begin{pmatrix} a'+a & b'+b \\ c'+c & d'+d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}+\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Ici on a utilisé la commutativité de $+$ dans A.

Maintenant il reste à verifier l'associativité et la neutralité de $\times$ ainsi que la distributivité de $+$ et de $\times$ pour prouver que M_2 est un anneau.

— Neutralité de Id_2 : Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2$ arbitraire. On a

$$\begin{pmatrix} 1_A & 0_A \\ 0_A & 1_A \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1_A a + 0_A c & 1_A b + 0_A d \\ 0_A a + 1_A c & 0_A b + 1_A d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \begin{pmatrix} 1_A a + 0_A b & 0_A a + 1_A b \\ 1_A c + 0_A d & 0_A c + 1_A d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} 1_A & 0_A \\ 0_A & 1_A \end{pmatrix}$$

Ici on a utilisé la neutralité de 1_A dans A.

— Associativité de la multiplication : Soient $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & b' \\ c' & d' \end{pmatrix}, \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \in M_2$ arbitraire. On a

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

$$= \begin{pmatrix} (aa' + bc')a'' + (ab' + bd')c'' & (aa' + bc')b'' + (ab' + bd')d'' \\ (ca' + dc')a'' + (cb' + dd')c'' & (ca' + dc')b'' + (cb' + dd')d'' \end{pmatrix}$$

$$= \begin{pmatrix} a(a'a'' + b'c'') + b(c'a'' + d'c'') & a(a'b'' + b'd'') + b(c'b'' + d'd'') \\ c(a'a'' + b'c'') + d(c'a'' + d'c'') & c(a'b'' + b'd'') + d(c'b'' + d'd'') \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a'a'' + b'c'' & a'b'' + b'd'' \\ c'a'' + d'c'' & c'b'' + d'd'' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}\right)$$

Ici on a utilisé l'associativité de $\times$ dans A.

— Distributivité : Soient $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & b' \\ c' & d' \end{pmatrix}, \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \in M_2$ arbitraire. On a

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}\right) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' + a'' & b' + b'' \\ c' + c'' & d' + d'' \end{pmatrix}$$

$$= \begin{pmatrix} a(a'+a'')+b(c'+c'') & a(b'+b'')+b(d'+d'') \\ c(a'+a'')+d(c'+c'') & c(b'+b'')+d(d'+d'') \end{pmatrix}$$
$$= \begin{pmatrix} aa'+bc'+aa''+bc'' & ab'+bd'+ab''+bd'' \\ ca'+dc'+ca''+dc'' & cb'+dd'+cb''+dd'' \end{pmatrix}$$
$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

et de maniére similaire on obtient

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}.$$

2) Pour prouver que M_2 est non commutatif dans le cas oú $0_A \neq 1_A$, il suffit de calculer

$$\begin{pmatrix} 1_A & 1_A \\ 0_A & 1_A \end{pmatrix} \times \begin{pmatrix} 1_A & 0_A \\ 1_A & 1_A \end{pmatrix} = \begin{pmatrix} 1_A+1_A & 1_A \\ 1_A & 1_A \end{pmatrix} \neq \begin{pmatrix} 1_A & 1_A \\ 1_A & 1_A+1_A \end{pmatrix} = \begin{pmatrix} 1_A & 0_A \\ 1_A & 1_A \end{pmatrix} \times \begin{pmatrix} 1_A & 1_A \\ 0_A & 1_A \end{pmatrix}.$$

Si $0_A = 1_A$ on a $0_2 = Id_2$ et M_2 ne posséde qu'un seul élément. Ainsi dans ce cas, M_2 est commutatif.

3) En calculant, on voit que

$$\det(\mathrm{Id}_2) = 1 \cdot 1 + 0 \cdot 0 = 1$$

où on a utilise que 0 est absorbant. De plus pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $N = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$, on calcule

$$\det(M \cdot N) = \det \begin{pmatrix} ax+by & az+bt \\ cx+dy & cz+dt \end{pmatrix} = (ax+by)(cz+dt) - (az+tb)(cx+dy)$$
$$= axcz + bycz + bydt + axdt - azxc - tbcx - azdy - tbdy = axdt - tbcx - azdy + bycz$$
$$= (ad-bc)(xt-zy) = \det(M) * \det(N)$$

4) On montre que si M est inversible alors $\det(M) \in A^\times$.
Soit M une matrice inversible. On a donc qu'il existe M' tel que $M \cdot M' = \mathrm{Id}_2$. On a donc $\det(M \cdot M') = 1$. Par la question precedente, on a donc que $1 = \det(M) \cdot \det(M')$ et donc que $\det(M)$ est inversible.

5) On verifie que la matrice M' donnée est bien l'inverse de M.
On calcule donc

$$M \cdot M' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
$$= \frac{1}{ad-bc} \begin{pmatrix} ad-bc & ba-ba \\ cd-cd & -bc+ad \end{pmatrix} = \mathrm{Id}_2$$

On reverifie de la même manière que $M' \cdot M = \mathrm{Id}_2$.

6) On rappelle que, si A est un anneau, alors on note $A^\times$ le groupe des éléments inversibles de A muni de la multiplication interne de A. Donc, il suffit de vérifier si det est un morphisme de groupe pour les multiplications. On a, par la question 3), que $det(M \cdot N) = \det(M) \cdot \det(N)$, ce qui nous confirme bien que det est un morphisme de groupe. On a donc que $\det(M^{-1}) = \det(M)^{-1}$ ce qui se vérifie bien par les calculs de la question 4.

Solution 2. 1) Soient $a, g, h \in A$. On a

$$[\times a](g+h) = a(g+h) = ag + ah = [\times a](g) + [\times a](h).$$

Ici, nous avons utilisé la distributivité dans l'anneau A. Ainsi c'est un morphisme et comme l'ensemble de dèpart est le même que l'ensemble d'arrivé, c'est un endomorphisme.

2) On a $[\times a](1_A) = a.1_A = a$. Alors si $a \neq 1_A, 0_A$, $[\times a]$ n'est pas un morphisme d'anneau car la condition $[\times a](1_A) = 1_A, 0_A$ n'est pas vérifiée.

— Si $a = 0_A$, alors $[\times 0_A](a') = 0_A \quad \forall a' \in A$, et en particulier $[\times 0_A](1_A) = 0_A$ et
$$[\times 0_A](b.c) = 0_A = 0_A.0_A = [\times 0_A](b).[\times 0_A](c)$$
donc on a bien un morphisme d'anneau, le morphisme trivial.

— Si $a = 1_A$, alors $[\times 1_A](a') = 1_A.a' = a' \quad \forall a' \in A$, et en particulier $[\times 1_A](1_A) = 1_A$ et
$$[\times 1_A](b.c) = b.c = [\times 1_A](b).[\times 1_A](c)$$
donc on a bien un morphisme d'anneau, l'endomorphisme identité.

3) On montre tout d'abord que l'application $[\times \bullet]$ est un morphisme de groupes entre $(A, +)$ et $(End_{Gr}(A), +)$.
Soient $a, b \in A$. On a :

$$[\times(a+b)](c) = (a+b).c = a.c + b.c = [\times a](c) + [\times b](c) = ([\times a] + [\times b])(c) \quad \forall c \in A$$
$$\Rightarrow [\times(a+b)] = ([\times a] + [\times b])$$

et on a bien un morphisme de groupes. (On a utilisé ici la distributivité dans l'anneau.)
On vérifie maintenant les conditions pour être un morphisme d'anneau :

$$[\times 1_A](b) = 1_A.b = b = Id_A(b) = 1_{End_{Gr}(A)}(b) \quad \forall b \in A \Rightarrow [\times 1_A] = 1_{End_{Gr}(A)}$$

et cette condition est vérifiée.
Vérifions la seconde : Soient $a, b \in A$. On a :

$$[\times(a.b)](c) = (a.b).c = a.(b.c) = [\times a](b.c) = [\times a]([\times b](c)) = ([\times a]\circ[\times b])(c) \quad \forall c \in A \Rightarrow [\times(a.b)] = [\times a] \circ [\times b]$$

et on a bien un morphisme d'anneau.

4) On utilise ici la proposition 3.4 (stabilité par morphismes) du cours. $A.\mathrm{Id}_A = \{[\times a] | a \in A\} = [\times A]$ est l'image de A par le morphisme $[\times \bullet]$. Par la proposition 3.4, l'image d'un anneau par un morphisme d'anneau est un sous-anneau de l'anneau d'arrivée, ici $End_{Gr}(A)$. Donc $A.\mathrm{Id}_A \subset End_{Gr}(A)$ est bien un sous-anneau.

5) Montrons que $ker([\times \bullet])$ est trivial. On a evidemment que $0 \in ker([\times \bullet])$. Soit maintenant $0 \neq a \in A$ et montrons que $[\times a] \neq 0_{\mathrm{End}_{Gr}(A)}$. On a que $[\times a](1) = 1 * a = a \neq 0$ ce qui nous permet donc de conclure. On a finalement donc bien que $ker([\times \bullet])$ est trivial. On a donc que $[\times \bullet]$ est injectif et donc A est isomorphe a l'image de $ker([\times \bullet])$, qui est un sous-anneau de $\mathrm{End}_{Gr}(A)$ comme dit precedemment.

2 Modules sur un anneau

Solution 3. 1. On traite d'abord le cas $n \geqslant 0$.
On a

$$n_A \star m = (1_A + 1_A + \cdots + 1_A) \star m = m + m + \cdots + m = n.m$$

ou toutes les sommes sont n fois. Le meme raisonnement se fait sur le cas $n < 0$.

Solution 4. 1) Posons $X = \{(x, y, z) \in \mathbb{Z}^3, x + 2y + 3z = 0\} \subset \mathbb{Z}^3$ Vérifions d'abord que $(X, +)$ est un sous-groupe de $(\mathbb{Z}^3, +)$:

- X non-vide : $(2, -1, 0) \in X$ car $2 + 2 * (-1) + 3 * 0 = 0$
- Soient $(a, b, c), (a', b', c') \in X$. Montrons que $(a, b, c) - (a', b', c') = (a - a', b - b', c - c') \in X$:

  $(a-a')+2(b-b')+3(c-c') = a-a'+2b-2b'+3c-3c' = (a+2b+3c)-(a'+2b'+3c') = 0-0 = 0$

  On a utilisé ici que la soustraction sur $\mathbb{Z}^3$ est l'inverse de la somme, que la somme est commutative, et que la multiplication est distributive. Ainsi $(a - a', b - b', c - c') \in X$ et X est bien un sous-groupe de $\mathbb{Z}^3$

Montrons maintenant que X est stable pour la multiplication par les scalaire, i.e. $\forall n \in \mathbb{Z}, (a,b,c) \in X$, alors $n*(a,b,c) = (n*a, n*b, n*c) \in X$. On a :

$$(n*a) + 2(n*b) + 3(n*c) = n*(a+2b+3c) = n*0 = 0$$

Donc $n*(a,b,c) \in X$, où on a utilisé que la multiplication dans $\mathbb{Z}$ est commutative. Ainsi, X est bien un sous-module non-nul de $\mathbb{Z}^3$.

2) Posons $Y = \{(x,y,z) \in \mathbb{Z}^3, x+2y+3z = 3x+2y+z = 0\} \subset \mathbb{Z}^3$ On procède de la même manière que dans la partie 1. Vérifions d'abord que $(Y,+)$ est un sous-groupe de $(\mathbb{Z}^3,+)$:

- Y non-vide : $(1,-2,1) \in Y$ car $1+2*(-2)+3*1 = 3*1+2*(-2)+1 = 0$
- Soient $(a,b,c),(a',b',c') \in Y$ Montrons que $(a,b,c)-(a',b',c') = (a-a',b-b',c-c') \in Y$:

  $(a-a')+2(b-b')+3(c-c') = a-a'+2b-2b'+3c-3c' = (a+2b+3c)-(a'+2b'+3c') = 0-0 = 0$

  et

  $3(a-a')+2(b-b')+(c-c') = 3a-3a'+2b-2b'+c-c' = (3a+2b+c)-(3a'+2b'+c') = 0-0 = 0$

  On a utilisé ici que la soustraction sur $\mathbb{Z}^3$ est l'inverse de la somme, que la somme est commutative, et que la multiplication est distributive. Ainsi $(a-a',b-b',c-c') \in Y$ et Y est bien un sous-groupe de $\mathbb{Z}^3$

Montrons maintenant que Y est stable pour la multiplication par les scalaire, i.e. $\forall n \in \mathbb{Z}, (a,b,c) \in Y$, alors $n*(a,b,c) = (n*a, n*b, n*c) \in Y$. On a :

$$(n*a) + 2(n*b) + 3(n*c) = n*(a+2b+3c) = n*0 = 0$$

et

$$3(n*a) + 2(n*b) + (n*c) = n*(3a+2b+c) = n*0 = 0$$

Donc $n*(a,b,c) \in Y$, où on a utilisé que la multiplication dans $\mathbb{Z}$ est commutative. Ainsi, Y est bien un sous-module non-nul de $\mathbb{Z}^3$.

3 Modules et familles generatrices

Solution 5.

1) Dans le cas ou $\Delta = 0$, on remarque que, avec $(x,y) = (ma+nb, mc+nd) \in \mathbb{Z}.(a,c) + \mathbb{Z}.(b,d)$

$$d(ma+nb) - b(mc+nd) = m(ad-bc) + n(bd-bd) = 0$$

ce qui nous permet de conclure que la paire donnee ne genere pas $\mathbb{Z}^2$

2) Supposons maintenant Δ non nul et non inversible et supposons par l'absurde que $\{(a,c),(b,d)\}$ genere $\mathbb{Z}^2$. On a donc l'existence de $(m,n),(m',n') \in \mathbb{Z}^2$ tels que $m.(a,c)+n.(b,d)=(1,0)$ et $m'.(a,c)+n'.(b,d)=(0,1)$. On obtient donc

$$\begin{cases} m.a+n.b=1 \\ m.c+n.d=0 \end{cases}$$

En notant $(L1)$ la premiere ligne et $(L2)$ la seconde, en faisant $(d.L1-b.L2)$ on obtient l'equation

$$\begin{aligned} & m.a.d+n.b.d-m.c.b-n.d.b=d \\ \iff\ & m(a.d-b.c)+n(bd-bd)=d \\ \iff\ & \Delta.m=d \end{aligned}$$

d'ou Δ divise d. De meme, en faisant $(-c.L1+a.L2)$ on obitent $\Delta.n=-c$ d'ou Δ divise c. En refaisant le meme procede avec l'autre equation obtenue pour $(0,1)$, on obtient que Δ divise b et a. On obtient donc que Δ divise n'importe quelle combinaison lineaire de a et b et donc en particulier, vu que 1 est une combinaison lineaire de a et b par $(L1)$, on obtient que Δ divise 1 ce qui est absurde et nous permet donc de conclure.

Solution 6. 1) Pour montrer que A^d est engendré par $\mathscr{B}$ on commence par prendre un élément arbitraire $a=(a_1,a_2,\ldots,a_d)\in A^d$. On peut ecrire a comme combinaison linéaire des éléments $\mathbf{e}_i$ car $u_i \in A^\times$ est inversible. Ainsi, il existe $u_i^{-1}\in A$ tel que $u_iu_i^{-1}=1$. On a

$$\begin{aligned} (a_1,a_2,\ldots,a_d) &= (a_1,0,\ldots,0)+(0,a_2,0,\ldots,0)+\ldots+(0,\ldots,0,a_d) \\ &= a_1(1,0,\ldots,0)+a_2(0,1,0,\ldots,0)+\ldots+a_d(0,\ldots,0,1) \\ &= a_1u_1^{-1}(u_1,0,\ldots,0)+a_2u_2^{-1}(0,u_2,0,\ldots,0)+\ldots+a_du_d^{-1}(0,\ldots,0,u_d) \\ &= a_1u_1^{-1}\mathbf{e}_1+a_2u_2^{-1}\mathbf{e}_2+\ldots+a_du_d^{-1}\mathbf{e}_d \in \langle\mathscr{B}\rangle. \end{aligned}$$

2) Supposons que l'écriture d'un élément $a=(a_1,\ldots,a_d)\in A^d$ ne soit pas unique. Alors il existe des coefficients $b_1,\ldots b_d\in A$ et $c_1,\ldots,c_d\in A$ tels que

$$b_1\mathbf{e}_1+\ldots+b_d\mathbf{e}_d=(a_1,\ldots,a_d)=c_1\mathbf{e}_1+\ldots+c_d\mathbf{e}_d,$$

et sans perte de généralité $b_i\neq c_i$ pour un $i\in\{1,\ldots,d\}$. Comme la i-ème position dans $\mathbf{e}_j$ est 0 pour $j\neq i$ nous obtenons à la i-ème position a_i de a que $b_iu_i=c_iu_i$. Cela implique que $b_iu_iu_i^{-1}=c_iu_iu_i^{-1}$ et donc $b_i=c_i$, en contradiction avec notre supposition $b_i\neq c_i$. Donc l'écriture est unique.

Solution 7. Soit M un A-module et $X \subset M$. On rappelle que le sous-module engendré par X est défini par :

$$\langle X \rangle = \bigcap_{X \subset N \subset M} N$$

1) Soit $X \subset Y$. Alors on a :

$$\langle Y \rangle = \bigcap_{Y \subset N \subset M} N \supset \left((\bigcap_{Y \subset N \subset M} N) \cap (\bigcap_{\substack{X \subset N \subset M \\ Y \not\subseteq N}} N) \right) = \bigcap_{X \subset N \subset M} N = \langle X \rangle$$

Remarque. On a ici utilisé la définition du sous-module engendré par un ensemble comme intersection de tous les sous-modules contenant cet ensemble, mais il est également possible de résoudre cet exercice en utilisant la proposition 3.9, à savoir l'expression du sous-module comme combinaison linéaire des éléments de l'ensemble.

2) Etant donne que $\langle Y \rangle$ contient une famille generatrice, on a qu'il existe $F \subset \langle Y \rangle$ tel que $\langle F \rangle = M$. On a donc que $M = \langle F \rangle \subset \langle \langle Y \rangle \rangle$ par la question precedente. On a donc que $\langle \langle Y \rangle \rangle = M$. Il suffit maintenant de verifier que $\langle \langle Y \rangle \rangle = \langle Y \rangle$. On a d'abord que $\langle \langle Y \rangle \rangle \supset \langle Y \rangle$, par definition. De plus, on a que $\langle Y \rangle$ est un sous module de M contenant $\langle Y \rangle$. Il apparait donc dans l'intersection definissant $\langle \langle Y \rangle \rangle$ et on obtient donc que $\langle \langle Y \rangle \rangle \subset \langle Y \rangle$ et cela nous permet donc de conclure que $\langle \langle Y \rangle \rangle = \langle Y \rangle$ et donc que Y est generateur.

Remarque. Autrement, on aurait pu aussi remarquer tout élément de M peut être écrit comme combinaison linéaire (finie) d'éléments de F, et tout élément de F est une combinaison lineaire d'elements de Y. Donc tout élément de M peut s'écrire comme combinaison linéaire (finie) d'éléments de Y, et Y est ainsi une famille génératrice.

3) Par la partie 1) de l'exercice, on a :

$$X \cap Y \subset X \Rightarrow \langle X \cap Y \rangle \subset \langle X \rangle, \quad X \cap Y \subset Y \Rightarrow \langle X \cap Y \rangle \subset \langle Y \rangle$$

donc

$$\langle X \cap Y \rangle \subset \langle X \rangle \cap \langle Y \rangle$$

Considérons le $\mathbb{Z}$-module $(\mathbb{Z}, +), X = \{1\}, Y = \{-1\}$ Alors $X \cap Y = \emptyset$, et $\langle X \cap Y \rangle = \langle \emptyset \rangle = \{0\}$, mais $\langle X \rangle = \mathbb{Z}, \langle Y \rangle = \mathbb{Z}$ car $\mathbb{Z}$ est engendré par 1, respectivement par -1, et donc $\langle X \rangle \cap \langle Y \rangle = \mathbb{Z}$.

Solution 8 On rappelle qu'un sous-module est un sous-groupe stable par multiplication par scalaire.
1) Vérifions tout d'abord que $L + M$ est un sous-groupe :

— $L + M$ est non-vide car L et M sont des sous-modules de N, en particulier des sous-groupes, donc non-vide, et $\exists l \in L, m \in M$ et $l + m \in L + M$

— Soient $l + m, l' + m' \in L + M$, i.e. $l, l' \in L, m, m' \in M$. Alors

$$(l+m)+(-(l'+m')) = l+m+(-l')+(-m') = (l+(-l'))+(m+(-m')) \in L+M$$

car L, M des sous-modules, donc $(l+(-l')) \in L, (m+(-m')) \in M$ (on a utilisé la commutativité du groupe additif). Ainsi $L + M$ est bien un sous-groupe.

On montre maintenant que $L + M$ est stable par multiplication par scalaires :
Soient $a \in A, l + m \in L + M$ Alors

$$a * (l + m) = a * l + a * m \in L + M$$

car $a * l \in L, a * m \in M$ vu que L et M sont des sous-modules, donc stables par multiplication par des scalaires. (On a utilisé la distributivité de la multiplication par scalaires.) Ainsi $L + M$ est bien un sous-module.

Montrons maintenant que $\langle L \cup M \rangle = L + M$. Comme toujours lorsqu'on veut montrer une égalité entre des ensembles (on s'intéresse ici aux ensembles sous-jacents), on utilise la double inclusion. Montrons d'abord $L + M \subset \langle L \cup M \rangle$:
Soit $l + m \in L + M$. Alors

$$l + m = 1_A * l + 1_A * m \in \langle L \cup M \rangle$$

car combinaison linéaire d'éléments de $L \cup M$. Donc $L + M \subset \langle L \cup M \rangle$.
Montrons maintenant l'autre inclusion, à savoir $\langle L \cup M \rangle \subset L + M$:
Soit $x \in \langle L \cup M \rangle$. En utilisant la proposition 3.9,

$$\exists a_1, \ldots, a_n \in A, x_1, \ldots, x_n \in L \cup M \quad \text{tq} \quad x = \sum_{i=1}^{n} a_i * x_i.$$

Intuitivement, on a envie de pouvoir séparer les termes de la somme pour avoir d'un côté les éléments de L et de l'autre ceux de M. C'est exactement ce qu'on va faire, et on peut le faire car la somme est finie et la loi d'addition commutative.
Pour chaque x_i, soit $x_i \in L$, soit $x_i \in M \backslash L$ (on sépare juste $L \cup M$ en deux sous-ensembles disjoints, car $L \cup M = L \amalg (M \backslash L)$ où $\amalg$ représente l'union disjointe.) Alors

$$x = \sum_{i=1}^{n} a_i * x_i = \sum_{\substack{x_i \in L \\ 1 \leq i \leq n}} a_i * x_i + \sum_{\substack{x_i \in M \backslash L \\ 1 \leq i \leq n}} a_i * x_i$$

Posons

$$l = \sum_{\substack{x_i \in L \\ 1 \leq i \leq n}} a_i * x_i \qquad m = \sum_{\substack{x_i \in M \backslash L \\ 1 \leq i \leq n}} a_i * x_i$$

Alors $l \in L$ et $m \in M$ car L, M des sous-modules. Donc $x = l + m \in L + M$, et $\langle L \cup M \rangle \subset L + M$. On conclut que $\langle L \cup M \rangle = L + M$.

2) On procède à nouveau par double inclusion. X une partie génératrice de L, donc $X \subset L$. Y un partie génératrice de M, donc $Y \subset M$. En combinant, on obtient $(X \cup Y) \subset (L \cup M)$. En utilisant la partie 1 de l'exercice 6, cela implique $\langle X \cup Y \rangle \subset \langle L \cup M \rangle = L + M$, ce qui montre la première inclusion.
Montrons maintenant l'autre inclusion. Soit $l + m \in L + M$. Comme X et Y sont des parties génératrices de L et M respectivement,

$$\exists x_1, \ldots, x_n \in X, \quad y_1, \ldots, y_r \in Y, \quad a_1, \ldots, a_n, b_1, \ldots, b_r \in A \quad tq$$
$$l = a_1 * x_1 + \ldots + a_n * x_n \quad et \quad m = b_1 * y_1 + \ldots + b_r * y_r$$

Alors

$$l + m = a_1 * x_1 + \ldots + a_n * x_n + b_1 * y_1 + \ldots + b_r * y_r$$

avec $a_1, \ldots, a_n, b_1, \ldots, b_r \in A, \quad x_1, \ldots, x_n, y_1, \ldots, y_r \in X \cup Y$. Donc $l + m \in \langle X \cup Y \rangle$, et $L + M \subset \langle X \cup Y \rangle$. On conclut donc que $\langle X \cup Y \rangle = L + M$.

Solution 9. 1) On suppose qu'il existe des applications A-linéaire φ et φ' telles que $\varphi \neq \varphi'$ mais $\varphi(m) = \varphi'(m)$ pour tout $m \in \mathscr{B}$. On veut trouver une contradiction. Si $\varphi \neq \varphi'$ il existe $x \in M$ tel que $\varphi(x) \neq \varphi'(x)$. On sait que $\mathscr{B}$ est un famille génératrice donc il existe des éléments $a_i \in A$ et $m_i \in \mathscr{B}$ tels que

$$x = a_1 m_1 + \ldots + a_n m_n.$$

Car φ et φ' sont A-linéaire on peut écrire

$$\varphi(x) = a_1 \varphi(m_1) + \ldots + a_n \varphi(m_n) \quad \text{et}$$

$$\varphi'(x) = a_1 \varphi'(m_1) + \ldots + a_n \varphi'(m_n).$$

Comme $\varphi(m_i) = \varphi'(m_i)$ pour tout $m_i \in \mathscr{B}$, on obtient la contradiction $\varphi'(x) = \varphi(x)$, ce qui prouve l'affirmation.

Sans contradiction : Soit φ et φ' deux applications A-linéaires de M vers N telles que

$$\forall m \in \mathscr{B}, \ \varphi'(m) = \varphi'(m). \tag{3.1}$$

Pour tout élément $x \in M$ il existe un entier $n \in \mathbb{N}$, des coefficients $a_i \in A$ et des éléments générateurs $m_i \in \mathscr{B}$ tels que

$$x = a_1 m_1 + \ldots + a_n m_n.$$

Ainsi,

$$\begin{aligned}\varphi(x) &= \varphi(a_1m_1 + \ldots + a_nm_n)\\ &= a_1\varphi(m_1) + \ldots a_n\varphi(m_n) \quad (\varphi \text{ est } A\text{-lineaire})\\ &= a_1\varphi'(m_1) + \ldots a_n\varphi'(m_n) \quad (3.1)\\ &= \varphi'(a_1m_1 + \ldots + a_nm_n) \quad (\varphi' \text{ est } A\text{-lineaire})\\ &= \varphi'(x)\end{aligned}$$

et $\varphi = \varphi'$.

2) On défini $\varphi((1,0))$ et $\varphi((0,1))$ de manière à ce que φ respecte les propriétés d'une application $\mathbb{Z}$-linéaire.

$$\varphi((0,1)) = \varphi((1,2)) - \varphi((1,1)) = (3,1) - (1,3) = (2,-2)$$

$$\varphi((1,0)) = \varphi((1,1)) - \varphi((0,1)) = (1,3) - (2,-2) = (-1,5)$$

Les valeurs de $\varphi((0,1))$ et $\varphi((1,0))$ sont uniques car la manière d'écrire $(1,0)$ et $(0,1)$ avec $(1,1)$ et $(1,2)$ est unique : D'après la partie 2) de l'exercise 5 on sait que $(1,1),(1,2)$ est une famille génératrice. Avec les calculs de l'exercise 4 on sait que la manière d'écrire $(1,0)$ et $(0,1)$ avec $(1,1)$ et $(1,2)$ est unique.

Pour $(m,n) \in \mathbb{Z}^2$ on obtient

$$\varphi((m,n)) = m\varphi((1,0)) + n\varphi((0,1)) = m(-1,5) + n(2,-2) = (-m+2n, 5m-2n).$$

La valeur de $\varphi((n,m))$ est unique car le manière d'écrire (m,n) avec $(1,0)$ et $(0,1)$ est unique. Donc φ est une application $\mathbb{Z}$-linéaire.

3) En premier on montre que $\mathscr{B}$ est encore une famille génératrice. Pour cela, soit $\mathscr{B}' := \{(1,1),(1,2)\}$. On sait que $\langle\mathscr{B}\rangle = \mathbb{Z}^2$ car $\mathscr{B}'$ est une famille génératrice. En utilisant la partie 1) de l'exercise 6 on obtient que $\mathbb{Z}^2\langle\mathscr{B}'\rangle \subset \langle\mathscr{B}\rangle \subset \mathbb{Z}^2$ car $\mathscr{B}' \subset \mathscr{B}$ donc $\langle\mathscr{B}\rangle = \mathbb{Z}^2$ et donc $\mathscr{B}$ est une famille génératrice. Si φ était une application $\mathbb{Z}$-linéaire, on aurait

$$2\varphi((1,1)) - \varphi((1,2)) = \varphi((2,2)) - \varphi((1,2)) = \varphi((1,0))$$

mais

$$2\varphi((1,1)) - \varphi((1,2)) = 2(1,3) - (3,1) = (-1,5) \neq (1,-2) = \varphi((1,0)).$$

Ainsi il n'existe pas d'application $\mathbb{Z}$ linéaire telle que

$$\varphi'(1,1) = (1,3),\ \varphi'(1,2) = (3,1),\ \varphi'(1,0) = (1,-2).$$

Notez que en comparaison avec la deuxieme partie, le manière d'écrire $(1,0)$ avec les éléments $(1,1),(1,2)$ et $(1,0)$ n'est pas unique.