Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

COURS À DISTANCE – SEMAINE 2 – ANNEAUX – CORRIGÉ TD1

Exercice 1. *Montrer que les ensembles munis de deux lois de composition suivants sont des anneaux. Déterminer s'ils sont commutatifs, unitaires, intègres.*

1. $(\mathbb{Q}, +, .)$.
   On sait que $(\mathbb{Q}, +)$ est un groupe commutatif. La multiplication dans $\mathbb{Q}$ est associative et distributive sur l'addition. Donc $(\mathbb{Q}, +, .)$ est un anneau. Il est commutatif car la multiplication est commutative dans $\mathbb{Q}$. Il est unitaire d'unité 1. Il est intègre : $rs = 0$ avec $r, s \in \mathbb{Q}$ implique $r = 0$ ou $s = 0$.

2. $(n\mathbb{Z}, +, .)$ *pour* $n \in \mathbb{N}^*$. Le couple $(n\mathbb{Z}, +)$ est un groupe commutatif comme sous-groupe du groupe commutatif $(\mathbb{Z}, +)$. La multiplication dans $\mathbb{Z}$, et donc dans $n\mathbb{Z}$, est associative et distributive sur l'addition. Donc $(n\mathbb{Z}, +, .)$ est un anneau. Il est commutatif car la multiplication est commutative dans $\mathbb{Z}$. Il est unitaire d'unité 1 si $n = 1$ mais il n'est pas unitaire si $n > 1$. Il est intègre : $rs = 0$ avec $r, s \in n\mathbb{Z}$ implique $r = 0$ ou $s = 0$.

3. $\left(\mathbb{Z}/_{n\mathbb{Z}}, +, .\right)$ *pour* $n \in \mathbb{N}^*$.
   On sait que $\left(\mathbb{Z}/_{n\mathbb{Z}}, +\right)$ est un groupe commutatif. La multiplication dans $\mathbb{Z}/_{n\mathbb{Z}}$ est induite par la multiplication dans $\mathbb{Z}$; on en déduit facilement qu'elle est associative et distributive sur l'addition. Donc $\left(\mathbb{Z}/_{n\mathbb{Z}}, +, .\right)$ est un anneau. Il est commutatif car la multiplication est commutative dans $\mathbb{Z}/_{n\mathbb{Z}}$. Il est unitaire d'unité $\overline{1}$. Pour l'intégrité, on sépare deux cas.
   Supposons n premier. Soient k et ℓ deux entiers tels que $\overline{k}.\overline{\ell} = \overline{0}$. Alors $k\ell$ est un multiple de n. Comme n est premier, d'après le lemme d'Euclide, k ou ℓ est multiple de n, donc $\overline{k} = \overline{0}$ ou $\overline{\ell} = \overline{0}$. Donc, dans ce cas, $\mathbb{Z}/_{n\mathbb{Z}}$ est intègre.
   Supposons maintenant n non premier. Alors il existe des entiers $p, q > 1$ tels que $n = pq$. Dans ce cas, $\overline{p}.\overline{q} = \overline{0}$. Mais, comme $1 < p < n$ et $1 < q < n$, $\overline{p} \neq \overline{0}$ et $\overline{q} \neq \overline{0}$. Donc, dans ce cas, $\mathbb{Z}/_{n\mathbb{Z}}$ n'est pas intègre.

4. $\big(\mathcal{M}_n(\mathbb{R}), +, .\big)$ *pour* $n \in \mathbb{N}^*$.
   On sait que $\big(\mathcal{M}_n(\mathbb{R}), +\big)$ est un groupe commutatif. La multiplication dans $\mathcal{M}_n(\mathbb{R})$ est associative et distributive sur l'addition. Donc $\big(\mathcal{M}_n(\mathbb{R}), +, .\big)$ est un anneau. Il est commutatif si $n = 1$ mais non commutatif si $n > 1$. En effet, si $A = (a_{ij})_{1 \leq i,j \leq n}$ est la matrice dont tous les coefficients sont nuls sauf $a_{1n} = 1$ et $B = (b_{ij})_{1 \leq i,j \leq n}$ est la matrice dont tous les coefficients sont nuls sauf $b_{11} = 1$, alors $AB \neq BA$. Il est unitaire d'unité la matrice identité. Il est intègre si $n = 1$ mais il n'est pas intègre si $n > 1$. En effet, avec les mêmes matrices A et B, on a $A \neq 0$, $B \neq 0$, mais $AB = 0$.

5. $\big(\mathrm{End}(E), +, \circ\big)$ *où E est un $\mathbb{K}$–espace vectoriel.*
   On vérifie facilement que $\big(\mathrm{End}(E), +\big)$ est un groupe commutatif. La loi multiplicative est ici la composition. Elle est associative, et, comme les endomorphismes de $\mathrm{End}(E)$ sont par définition des applications linéaires, elle est distributive sur l'addition. Donc $\big(\mathrm{End}(E), +, \circ\big)$ est un anneau. Il est unitaire d'unité l'application identité.
   Supposons que $\dim(E) = 1$. Alors les éléments de $\mathrm{End}(E)$ sont les applications $\left\{ \begin{array}{ccc} E & \to & E \\ x & \mapsto & \lambda x \end{array} \right.$ avec $\lambda \in \mathbb{K}$. Dans ce cas, $\mathrm{End}(E)$ est commutatif et intègre.
   Supposons maintenant que $\dim(E) > 1$ (ce qui inclut les espaces vectoriels de dimension infinie). On a alors deux éléments $x, y \in E$ indépendants dans E. On note F le sous-espace de E engendré par x et y et G un supplémentaire de F dans E. Alors tout $v \in E$ s'écrit de manière unique

$v = \lambda x + \mu y + z$ avec $\lambda, \mu \in \mathbb{K}$ et $z \in G$. On définit deux endomorphismes f et g de E par

$$f(\lambda x + \mu y + z) = \lambda y \quad \text{et} \quad g(\lambda x + \mu y + z) = \lambda x$$

pour tous $\lambda, \mu \in \mathbb{K}$ et $z \in G$. Alors $f \circ g = f \neq 0$ et $g \circ f = 0$. Ainsi $\mathrm{End}(E)$ n'est ni commutatif ni intègre.

6. $(\mathbb{R}[X], +, .)$ *où* $\mathbb{R}[X]$ *est l'ensemble des polynômes à coefficients réels à une indéterminée.*
   On vérifie facilement que $(\mathbb{R}[X], +)$ est un groupe commutatif. La multiplication des polynômes est associative et distributive sur l'addition. Donc $(\mathbb{R}[X], +, .)$ est un anneau. Il est commutatif car la multiplication est commutative dans $\mathbb{R}[X]$. Il est unitaire d'unité le polynôme constant 1. Il est intègre : $PQ = 0$ avec $P, Q \in \mathbb{R}[X]$ implique $P = 0$ ou $Q = 0$.

7. $\mathcal{F}(X, A) := \{f : X \to A\}$ *où* A *est un anneau et* X *un ensemble, avec la somme et la multiplication définies pour tous* $f_1, f_2 : X \to A$ *par* $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ *et* $(f_1.f_2)(x) = f_1(x).f_2(x)$ *pour tout* $x \in X$.
   En utilisant le fait que A est un anneau, on vérifie que $\mathcal{F}(X, A)$ est aussi un anneau. Il est commutatif si et seulement si A est commutatif.
   Supposons que h est une unité de $\mathcal{F}(X, A)$. Alors pour tout $f \in \mathcal{F}(X, A)$, $f.h = h.f = f$.Pour $a \in A$, notons f_a la fonction constante égale à a. Alors, pour $x \in X$, on a $f_a(x).h(x) = h(x).f_a(x) = f_a(x)$, c'est-à-dire $a.h(x) = h(x).a = a$. Ce n'est possible que si A admet un élément unité. Finalement, $\mathcal{F}(X, A)$ est unitaire si et seulement si A est unitaire, et dans ce cas l'unité de $\mathcal{F}(X, A)$ est la fonction constante égale à 1_A.
   Si X contient un seul élément, on vérifie facilement que $\mathcal{F}(X, A)$ est intègre si et seulement si A est intègre.
   Si A est l'anneau trivial, alors $\mathcal{F}(X, A)$ est aussi trivial ; en particulier, il est intègre.
   Supposons maintenant que X contient au moins deux éléments distincts et que A est non trivial. Prenons $y \neq z$ dans X. On définit deux fonctions f et g dans $\mathcal{F}(X, A)$ par

$$f(x) = \begin{cases} 1 & si \quad x = y \\ 0 & si \quad x \neq y \end{cases} \quad \text{et} \quad g(x) = \begin{cases} 1 & si \quad x = z \\ 0 & si \quad x \neq z \end{cases} \quad \text{pour tout } x \in X.$$

   Alors $f \neq 0$ et $g \neq 0$, mais $f.g = 0$. Donc $\mathcal{F}(X, A)$ n'est pas intègre.

Exercice 2. *On définit sur* $\mathbb{R}$ *les deux lois* $\oplus$ *et* $\otimes$ *par* $x \oplus y = x + y - 1$ *et* $x \otimes y = x + y - xy$. *Montrer que* $(\mathbb{R}, \oplus, \otimes)$ *est un corps.*
La loi $\oplus$ est associative : pour tous $x, y, z \in \mathbb{R}$, on a

$$\begin{aligned} x \oplus (y \oplus z) &= x \oplus (y + z - 1) \\ &= x + (y + z - 1) - 1 \\ &= x + y + z - 2 \end{aligned} \qquad \begin{aligned} (x \oplus y) \oplus z &= (x + y - 1) \oplus z \\ &= (x + y - 1) + z - 1 \; . \\ &= x + y + z - 2 \end{aligned}$$

Elle admet 1 comme élément neutre : $x \oplus 1 = 1 \oplus x = 1$. Tout $x \in \mathbb{R}$ admet un inverse pour $\oplus$, à savoir $2 - x$. Donc $(\mathbb{R}, \oplus)$ est un groupe. De plus, ce groupe est commutatif : on a clairement $x \oplus y = y \oplus x$ pour tous $x, y \in \mathbb{R}$.
La loi $\otimes$ est associative : pour tous $x, y, z \in \mathbb{R}$, on a

$$\begin{aligned} x \otimes (y \otimes z) &= x \otimes (y + z - yz) \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x + y + z - xy - yz - xz + xyz \end{aligned} \qquad \begin{aligned} (x \otimes y) \otimes z &= (x + y - xy) \otimes z \\ &= (x + y - xy) + z - (x + y - xy)z \; . \\ &= x + y + z - xy - yz - xz + xyz \end{aligned}$$

Elle est aussi distributive sur la loi $\oplus$: pour tous $x, y, z \in \mathbb{R}$, on a

$$\begin{aligned} x \otimes (y \oplus z) &= x \otimes (y + z - 1) \\ &= x + (y + z - 1) - x(y + z - 1) \\ &= 2x + y + z - xy - xz - 1 \end{aligned} \qquad \begin{aligned} (x \otimes y) \oplus (x \otimes z) &= (x + y - xy) \oplus (x + z - xz) \\ &= (x + y - xy) + (x + z - xz) - 1 \; . \\ &= 2x + y + z - xy - xz - 1 \end{aligned}$$

Donc $(\mathbb{R}, \oplus, \otimes)$ est un anneau.
On a un élément neutre pour la loi $\otimes$, à savoir 0 : $0 \otimes x = x = x \otimes 0$ pour tout $x \in \mathbb{R}$. Donc $(\mathbb{R}, \oplus, \otimes)$ est un anneau unitaire.
Si $x \in \mathbb{R}$ est différent de 1, l'élément neutre pour la loi $\oplus$, alors x admet un inverse pour la loi $\otimes$, à savoir $\frac{x}{x-1}$: $x \otimes \frac{x}{x-1} = \frac{x}{x-1} \otimes x = 0$. Donc $(\mathbb{R}, \oplus, \otimes)$ est un corps.

Exercice 3.

1. *Montrer que l'ensemble $\mathcal{S}_\mathbb{R}$ des suites à valeurs réelles est un anneau commutatif unitaire pour l'addition et la multiplication terme à terme. Est-il intègre ?*
   L'addition des suites réelles est associative et commutative et possède un élément neutre donné par la suite constante égale à 0. L'opposé d'une suite $(x_n)_{n\in\mathbb{N}} \in \mathcal{S}_\mathbb{R}$ est la suite $(-x_n)_{n\in\mathbb{N}} \in \mathcal{S}_\mathbb{R}$. Ainsi $(\mathcal{S}_\mathbb{R}, +)$ est un groupe abélien.
   La multiplication des suites réelles est associative et commutative et possède un élément neutre donné par la suite constante égale à 1. On vérifie aussi qu'elle est distributive sur l'addition. Donc $(\mathcal{S}_\mathbb{R}, +, .)$ est un anneau commutatif unitaire.
   Prenons les suites $x = (x_n)_{n\in\mathbb{N}}$ et $y = (y_n)_{n\in\mathbb{N}}$ définies comme suit :
   $$x_n = \begin{cases} 1 & si \quad n = 0 \\ 0 & si \quad n > 0 \end{cases} \qquad y_n = \begin{cases} 1 & si \quad n = 1 \\ 0 & si \quad n \neq 1 \end{cases}.$$
   ALors $x \neq 0$ et $y \neq 0$ mais $xy = 0$. L'anneau $(\mathcal{S}_\mathbb{R}, +, .)$ n'est donc pas intègre.

2. *Montrer que le sous-ensemble des suites réelles convergentes est un sous-anneau unitaire de $\mathcal{S}_\mathbb{R}$.*
   Notons $\mathcal{S}_\mathbb{R}^c \subset \mathcal{S}_\mathbb{R}$ le sous-ensemble des suites convergentes. Il contient les éléments neutres de l'addition et de la multiplication, qui sont des suites constantes donc convergentes. En particulier, il est non vide. Il est stable par addition : la somme de deux suites convergentes converge. Il est stable par passage à l'opposé : si $(x_n)_{n\in\mathbb{N}}$ converge vers ℓ, $(-x_n)_{n\in\mathbb{N}}$ converge vers $-\ell$. C'est donc un sous-groupe additif de $\mathcal{S}_\mathbb{R}$. Comme le produit de deux suites convergentes converge, $\mathcal{S}_\mathbb{R}^c$ est aussi stable par multiplication. Finalement, $\mathcal{S}_\mathbb{R}^c$ est un sous-anneau unitaire de $\mathcal{S}_\mathbb{R}$.

Exercice 4. *On note $\mathcal{F}(\mathbb{R}, \mathbb{R})$ l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. On le munit de l'addition et de la multiplication définies dans l'exercice 1, point 7.*

1. *Montrer que $\mathcal{F}(\mathbb{R}, \mathbb{R})$ est un anneau commutatif unitaire.*
   On applique l'exercice 1, point 7, avec $X = \mathbb{R}$ et $A = \mathbb{R}$. On voit que $\mathcal{F}(\mathbb{R}, \mathbb{R})$ est un anneau, commutatif car $\mathbb{R}$ est commutatif, et unitaire car $\mathbb{R}$ est unitaire. Rappelons que l'unité est la fonction constante égale à 1.

2. *Déterminer l'ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})^\times$ des inversibles.*
   Soit $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})^\times$. Alors il existe $g \in \mathcal{F}(\mathbb{R}, \mathbb{R})^\times$ telle que $f.g = 1_{\mathcal{F}(\mathbb{R},\mathbb{R})}$, c'est-à-dire que $f(x).g(x) = 1$ pour tout $x \in \mathbb{R}$. En particulier, on a $f(x) \neq 0$ pour tout $x \in \mathbb{R}$.
   Maintenant, prenons $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ telle que $f(x) \neq 0$ pour tout $x \in \mathbb{R}$. On définit une fonction $g : \mathbb{R} \to \mathbb{R}$ par $g(x) = \frac{1}{f(x)}$ pour tout $x \in \mathbb{R}$. Alors g est l'inverse de f.
   En conclusion, les inversibles de $\mathcal{F}(\mathbb{R}, \mathbb{R})$ sont les fonctions qui ne s'annulent en aucun point.

Exercice 5. *On considère les sous-ensembles suivants de $\mathcal{M}_2(\mathbb{R})$.*

$$A = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} ; x \in \mathbb{R} \right\} \qquad B = \left\{ \begin{pmatrix} x & x \\ -x & -x \end{pmatrix} ; x \in \mathbb{R} \right\}$$

1. *Sont-ils des anneaux ? intègres ? unitaires ? des corps ?*
   On sait déjà que $\mathcal{M}_2(\mathbb{R})$ est un anneau. Les sous-ensembles A et B contiennent la matrice nulle, ils sont stables par addition, par passage à l'opposé et par multiplication. Ce sont des sous-anneaux de $\mathcal{M}_2(\mathbb{R})$, donc des anneaux.

Soient $M = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$ et $N = \begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix}$ deux matrices dans A. Alors $MN = \begin{pmatrix} xy & 0 \\ 0 & 0 \end{pmatrix}$. Si $MN = 0$, alors $xy = 0$, donc $x = 0$ ou $y = 0$, et donc $M = 0$ ou $N = 0$. Ainsi A est intègre.
La matrice $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ commute avec toutes les matrices de A, c'est donc un élément neutre pour la multiplication dans A (pas dans $\mathcal{M}_2(\mathbb{R})$!). Donc A est un anneau unitaire.
Si une matrice $M = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$ est non nulle, alors $x \neq 0$ et M admet comme inverse la matrice $\begin{pmatrix} -x & 0 \\ 0 & 0 \end{pmatrix}$. Donc tous les éléments non nuls de A sont inversibles : A est un corps.
Quelles que soient les matrices M et N dans B, on a $MN = 0$. Donc tous les éléments de B sont des diviseurs de 0, en particulier aucun élément n'est inversible, et B ne peut pas posséder d'unité. Ainsi B n'est ni intègre, ni unitaire, ni un corps.

2. *Sont-ils des sous-anneaux de $\mathcal{M}_2(\mathbb{R})$? des sous-anneaux unitaires ?*
On a vu que A et B sont des sous-anneaux de $\mathcal{M}_2(\mathbb{R})$. Comme B ne possède pas d'unité, ce n'est pas un sous-anneau unitaire. Dans A, il y a une unité, mais ce n'est pas la même que dans $\mathcal{M}_2(\mathbb{R})$, à savoir la matrice identité, qui n'appartient pas à A. Donc A n'est pas non plus un sous-anneau unitaire de $\mathcal{M}_2(\mathbb{R})$.

Exercice 6. *Soit E un ensemble et $\mathcal{P}(E)$ l'ensemble des sous-ensembles de E. Pour tout $A, B \in \mathcal{P}(E)$, on rappelle que $A \Delta B := (A \cup B) \setminus (A \cap B)$.*

1. *Montrer que $\big(\mathcal{P}(E), \Delta, \cap\big)$ est un anneau commutatif et unitaire.*
Pour vérifier que Δ est une loi associative, on montre que $x \in (A\Delta B)\Delta C$ si et seulement si $x \in A\Delta(B\Delta C)$. On procède cas par cas, selon que x est ou non dans A, dans B, dans C, ce que résume le tableau suivant.

Si			*Alors*			
A	B	C	$A\Delta B$	$B\Delta C$	$(A\Delta B)\Delta C$	$A\Delta(B\Delta C)$
$\in$	$\in$	$\in$	$\notin$	$\notin$	$\in$	$\in$
$\in$	$\in$	$\notin$	$\notin$	$\in$	$\notin$	$\notin$
$\in$	$\notin$	$\in$	$\in$	$\in$	$\notin$	$\notin$
$\in$	$\notin$	$\notin$	$\in$	$\notin$	$\in$	$\in$
$\notin$	$\in$	$\in$	$\in$	$\notin$	$\notin$	$\notin$
$\notin$	$\in$	$\notin$	$\in$	$\in$	$\in$	$\in$
$\notin$	$\notin$	$\in$	$\notin$	$\in$	$\in$	$\in$
$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$

Pour tout sous-ensemble A de E, on a $\emptyset\Delta A = A = A\Delta\emptyset$, donc $\emptyset$ est un élément neutre pour Δ. De plus, pour tout A, on a $A\Delta A = \emptyset$, donc A admet un opposé, qui est A lui-même. Donc $\mathcal{P}(E)$ est un groupe, abélien car Δ est clairement commutative.
Il est clair que la loi $\cap$ est associative. Pour vérifier qu'elle est distributive sur Δ, on procède à nouveau cas par cas.

Si			*Alors*				
A	B	C	$A \cap B$	$A \cap C$	$B \Delta C$	$A \cap (B \Delta C)$	$(A \cap B) \Delta (A \cap C)$
$\in$	$\in$	$\in$	$\in$	$\in$	$\notin$	$\notin$	$\notin$
$\in$	$\in$	$\notin$	$\in$	$\notin$	$\in$	$\in$	$\in$
$\in$	$\notin$	$\in$	$\notin$	$\in$	$\in$	$\in$	$\in$
$\in$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$
$\notin$	$\in$	$\in$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$
$\notin$	$\in$	$\notin$	$\notin$	$\notin$	$\in$	$\notin$	$\notin$
$\notin$	$\notin$	$\in$	$\notin$	$\notin$	$\in$	$\notin$	$\notin$
$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$	$\notin$

Finalement, $\mathcal{P}(E)$ est un anneau. Il est commutatif car la loi $\cap$ est commutative et il est unitaire d'unité E car $A \cap E = E \cap A = A$ pour tout $A \in \mathcal{P}(E)$.

2. *Déterminer l'ensemble $\mathcal{P}(E)^\times$ des inversibles et l'ensemble des diviseurs de zéro. L'anneau $\mathcal{P}(E)$ est-il intègre ?*
   Un élément $A \in \mathcal{P}(E)$ est inversible si et seulement si il existe $B \in \mathcal{P}(E)$ tel que $A \cap B = E$, ce qui implique $A = B = E$. Ainsi E est le seul élément inversible.
   Soit $A \in \mathcal{P}(E)$ un sous-ensemble strictement inclu dans E. Alors son complémentaire A^c vérifie $A^c \neq \emptyset$ et on a $A \cap A^c = \emptyset$. Donc A est un diviseur de zéro.
   Si E contient au moins deux éléments distincts, disons x et y, alors $\{x\}$ est différent de $\emptyset$ et strictement inclu dans E, donc c'est un diviseur de zéro non trivial, et $\mathcal{P}(E)$ n'est pas intègre. Si E est de cardinal 0 ou 1, alors $\mathcal{P}(E)$ est intègre.

Remarque. N'hésitez pas à dessiner des patates !

Exercice 7. *Soit $(A, +)$ un groupe abélien et $\ .\ : A \times A \to A$ une opération associative sur A. Montrer que $(A, +, .\,)$ est un anneau si et seulement si, pour tout $a \in A$, les applications*

$$\begin{array}{ccc} A & \longrightarrow & A \\ b & \longmapsto & a.b \end{array} \qquad \textit{et} \qquad \begin{array}{ccc} A & \longrightarrow & A \\ b & \longmapsto & b.a \end{array}$$

sont des morphismes de groupes.

On a déjà que $(A, +)$ est un groupe abélien et que la multiplication est associative. Donc $(A, +, .\,)$ est un anneau si et seulement si la multiplication est distributive sur l'addition. Notons m_a^g et m_a^d les applications de A dans A données par $m_a^g(b) = a.b$ et $m_a^d(b) = b.a$. L'application m_a^g est un morphisme de groupes si et seulement si $m_a^g(b_1 + b_2) = m_a^g(b_1) + m_a^g(b_2)$, c'est-à-dire $a.(b_1 + b_2) = a.b_1 + a.b_2$, pour tous $b_1, b_2 \in A$. De même, L'application m_a^d est un morphisme de groupes si et seulement si $(b_1 + b_2).a = b_1.a + b_2.a$ pour tous $b_1, b_2 \in A$. Ainsi les applications m_a^g et m_a^d sont des morphismes de groupes pour tout $a \in A$ si et seulement si la multiplication est distributive sur l'addition.

Exercice 8. *Soient A_1 et A_2 des anneaux. On munit $A_1 \times A_2$ des lois de composition internes*

$$+ : \begin{array}{ccc} (A_1 \times A_2) \times (A_1 \times A_2) & \longrightarrow & A_1 \times A_2 \\ \big((a_1, a_2), (b_1, b_2)\big) & \longmapsto & (a_1 + b_1, a_2 + b_2) \end{array}$$

et

$$.\ : \begin{array}{ccc} (A_1 \times A_2) \times (A_1 \times A_2) & \longrightarrow & A_1 \times A_2 \\ \big((a_1, a_2), (b_1, b_2)\big) & \longmapsto & (a_1.b_1, a_2.b_2) \end{array}.$$

1. *Montrer que $(A_1 \times A_2, +, .\,)$ est un anneau. C'est ce qu'on appelle la structure d'anneau produit.*
   On vérifie directement en écrivant les définitions que $(A_1 \times A_2, +)$ est un groupe abélien et que la multiplication est associative et distributive sur l'addition.

2. *Montrer que* $(A_1 \times A_2, +, .)$ *est unitaire et/ou commutatif si et seulement si* A_1 *et* A_2 *le sont.*
Si A_1 et A_2 sont unitaires, alors $(1_{A_1}, 1_{A_2})$ est une unité de $A_1 \times A_2$. Réciproquement, supposons $A_1 \times A_2$ unitaire et notons (u, v) son unité. Alors, pour tout $a \in A_1$ et pour tout $b \in A_2$, on a $(u, v).(a, b) = (a, b).(u, v) = (a, b)$, c'est-à-dire $(u.a, v.b) = (a.u, b.v) = (a, b)$, donc $u.a = a.u = a$ et $v.b = b.v = b$. Ainsi u est une unité de A_1 et v est une unité de A_2.
L'anneau $A_1 \times A_2$ est commutatif si et seulement si

$$\begin{aligned}
& (a_1, a_2).(b_1, b_2) = (b_1, b_2).(a_1, a_2) && \text{pour tous } a_1, b_1 \in A_1 \text{ et } a_2, b_2 \in A_2, \\
\iff & (a_1.b_1, a_2.b_2) = (b_1.a_1, b_2.a_2) && \text{pour tous } a_1, b_1 \in A_1 \text{ et } a_2, b_2 \in A_2, \\
\iff & a_1.b_1 = b_1.a_1 \text{ et } a_2.b_2 = b_2.a_2 && \text{pour tous } a_1, b_1 \in A_1 \text{ et } a_2, b_2 \in A_2,
\end{aligned}$$

si et seulement si A_1 et A_2 sont commutatifs.