CORRIGÉ – CHAPITRE 5

STRUCTURES ALGÉBRIQUES

Anneaux : définition et calculs

EXERCICE 1 ⋆

On suit l'ordre **NADA** : neutres, groupe abélien additif, distributivité, associativité multiplicative.

1. L'ensemble $(\mathbb{N}\,;+)$ n'est pas un groupe, puisque 3 n'y admet pas d'opposé.

$$\boxed{\text{Ce n'est pas un anneau : l'axiome } \mathbf{A} \text{ échoue.}}$$

2. Les quatre axiomes sont vérifiés, et la multiplication est commutative :

$$\boxed{(\mathbb{Z}\,;+\,;\times) \text{ est un anneau commutatif, de neutres 0 et 1.}}$$

3. L'ensemble $(2\mathbb{Z}\,;+)$ est bien un groupe abélien, et la multiplication y est interne, associative et distributive. Mais $1 \notin 2\mathbb{Z}$:

$$\boxed{\text{Ce n'est pas un anneau : il n'y a pas de neutre multiplicatif.}}$$

4. On procède de la même manière, la multiplication des rationnels étant commutative :

$$\boxed{(\mathbb{Q}\,;+\,;\times) \text{ est un anneau commutatif.}}$$

5. Les quatre axiomes se vérifient point par point, à partir de ceux de $\mathbb{R}$. Les neutres sont la fonction nulle et la fonction constante égale à 1.

$$\boxed{(\mathbb{R}^{\mathbb{R}}\,;+\,;\times) \text{ est un anneau commutatif.}}$$

6. De même, coordonnée par coordonnée, avec pour neutres $(0\,;0)$ et $(1\,;1)$.

$$\boxed{(\mathbb{R}^2\,;+\,;\times) \text{ est un anneau commutatif.}}$$

7. D'après le chapitre 3, $(\mathcal{P}(E)\,;\Delta)$ est un groupe abélien de neutre $\varnothing$. L'intersection est associative, commutative, de neutre E, et elle est distributive sur Δ : pour $x \in E$, appartenir à $A \cap (B \,\Delta\, C)$ signifie appartenir à A et à exactement l'un des deux ensembles B et C, c'est-à-dire à exactement l'un des deux ensembles $A \cap B$ et $A \cap C$.

$$\boxed{(\mathcal{P}(E)\,;\Delta\,;\cap) \text{ est un anneau commutatif, dès que } E \neq \varnothing.}$$

La restriction $E \neq \varnothing$ est nécessaire : sinon $\mathcal{P}(E) = \{\varnothing\}$ et les deux neutres coïncideraient, ce que la définition interdit.

EXERCICE 2 ⋆

1. On part de $0_A = 0_A + 0_A$ et l'on multiplie par x, en utilisant la distributivité :

$$0_A \times x = (0_A + 0_A) \times x = 0_A \times x + 0_A \times x$$

Comme $(A\,;+)$ est un groupe, on peut simplifier par $0_A \times x$:

$$\boxed{0_A \times x = 0_A}$$

2. On calcule, en utilisant la distributivité puis la question 1 :

$$xy + (-x)y = \big(x + (-x)\big)y = 0_A \times y = 0_A$$

donc $(-x)y$ est l'opposé de xy :

$$\boxed{(-x)y = -(xy)}$$

En appliquant deux fois ce résultat : $(-x)(-y) = -\big(x(-y)\big) = -\big(-(xy)\big)$, d'où :

$$\boxed{(-x)(-y) = xy}$$

3. On développe sans jamais échanger l'ordre des facteurs :

$$\boxed{(x+y)^2 = x^2 + xy + yx + y^2} \qquad \boxed{(x+y)(x-y) = x^2 - xy + yx - y^2}$$

4. Les deux termes centraux se regroupent en $2xy$ et se simplifient en 0_A précisément lorsque $xy = yx$.

$$\boxed{\text{Les identités remarquables usuelles ne valent que si } x \text{ et } y \text{ commutent.}}$$

Piège : c'est en particulier le cas dans tout anneau commutatif, mais pas dans l'anneau des matrices carrées.

EXERCICE 3 ⋆⋆

1. Les deux éléments $(1\,;0)$ et $(0\,;1)$ sont non nuls, et :

$$(1\,;0) \times (0\,;1) = (1 \times 0\,;\, 0 \times 1) = (0\,;0)$$

$$\boxed{(1\,;0) \text{ et } (0\,;1) \text{ sont des diviseurs de zéro de } \mathbb{R}^2.}$$

2. Les fonctions f et g ne sont pas nulles, puisque $f(1) = 2$ et $g(-1) = 2$. Pourtant, pour tout réel x :

$$f(x)g(x) = \big(|x| + x\big)\big(|x| - x\big) = |x|^2 - x^2 = x^2 - x^2 = 0$$

$$\boxed{f \text{ et } g \text{ sont des diviseurs de zéro de } \mathbb{R}^{\mathbb{R}}.}$$

3. Dans $\mathbb{Z}/6\mathbb{Z}$, les classes $\overline{2}$ et $\overline{3}$ sont non nulles et $\overline{2} \times \overline{3} = \overline{6} = \overline{0}$.

$$\boxed{\overline{2} \text{ et } \overline{3} \text{ sont des diviseurs de zéro de } \mathbb{Z}/6\mathbb{Z}.}$$

4. Soit x inversible, et supposons $xy = 0_A$. En multipliant à gauche par x^{-1} :

$$y = 1_A \times y = (x^{-1}x)y = x^{-1}(xy) = x^{-1} \times 0_A = 0_A$$

$$\boxed{\text{Un élément inversible n'est jamais un diviseur de zéro.}}$$

5. Dans un corps, tout élément non nul est inversible, donc n'est pas un diviseur de zéro d'après la question 4.

$$\boxed{\text{Un corps ne possède aucun diviseur de zéro.}}$$

EXERCICE 4 ⋆⋆

1. En appliquant l'hypothèse à l'élément $x + x$, puis en développant comme à l'exercice 2 :

$$x + x = (x+x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$$

En simplifiant $x + x$ dans le groupe $(A\,;+)$, il vient :

$$\boxed{x + x = 0_A, \text{ c'est-à-dire } -x = x, \text{ pour tout } x \in A.}$$

2. On applique l'hypothèse à $x+y$:

$$x+y=(x+y)^2=x^2+xy+yx+y^2=x+xy+yx+y$$

En simplifiant $x+y$ des deux côtés :

$$\boxed{xy+yx=0_A}$$

3. La question 2 donne $xy=-(yx)$, et la question 1 appliquée à l'élément yx donne $-(yx)=yx$.

$$\boxed{xy=yx \text{ : l'anneau } A \text{ est commutatif.}}$$

4. Dans $\mathcal{P}(E)$ muni de Δ et $\cap$, le carré d'un élément A est $A\cap A=A$.

$$\boxed{(\mathcal{P}(E)\,;\Delta\,;\cap) \text{ est un anneau de Boole.}}$$

On y vérifie d'ailleurs les deux résultats intermédiaires : $A\,\Delta\,A=\varnothing$ est bien le neutre additif, conformément à la question 1.

EXERCICE 5 ⋆⋆⋆

1. Soient n et m tels que $x^n=0_A$ et $y^m=0_A$, et posons $p=\max(n\,;m)$. L'anneau étant commutatif :

$$(xy)^p=x^py^p$$

et l'un des deux facteurs est nul, puisque $p\geqslant n$ ou $p\geqslant m$ — en réalité les deux.

$$\boxed{xy \text{ est nilpotent.}}$$

2. L'anneau étant commutatif, la formule du binôme s'applique :

$$(x+y)^{n+m-1}=\sum_{k=0}^{n+m-1}\binom{n+m-1}{k}x^k y^{n+m-1-k}$$

Examinons un terme d'indice k. Si $k\geqslant n$, alors $x^k=0_A$. Sinon $k\leqslant n-1$, et l'exposant de y vaut $n+m-1-k\geqslant m$, donc $y^{n+m-1-k}=0_A$. Tous les termes sont nuls.

$$\boxed{x+y \text{ est nilpotent.}}$$

3. On reconnaît une somme géométrique. Avec $x^n=0_A$:

$$(1_A-x)(1_A+x+x^2+\cdots+x^{n-1})=1_A-x^n=1_A$$

les termes intermédiaires se télescopant. L'anneau étant commutatif, le produit dans l'autre ordre donne le même résultat.

$$\boxed{1_A-x \text{ est inversible, d'inverse } 1_A+x+\cdots+x^{n-1}.}$$

4. Soit n tel que $(uv)^n=0_A$. On écrit alors :

$$(vu)^{n+1}=\underbrace{vu\cdot vu\cdots vu}_{n+1\text{ facteurs}}=v\,\underbrace{(uv)(uv)\cdots(uv)}_{n\text{ facteurs}}\,u=v\,(uv)^n\,u=v\times 0_A\times u=0_A$$

$$\boxed{vu \text{ est nilpotent.}}$$

Remarque : ce regroupement ne demande que l'associativité, et non la commutativité. C'est pourquoi la question reste valable dans un anneau quelconque, contrairement aux trois précédentes.

Sous-anneaux

EXERCICE 6 ⋆

On applique la caractérisation : $1_A \in B$, puis stabilité par différence et par produit.

1. L'entier 1 n'est pas pair.

$$\boxed{2\mathbb{Z} \text{ n'est pas un sous-anneau de } \mathbb{Z} : \text{il ne contient pas 1.}}$$

2. On a $1 \in \mathbb{Z}$, et la différence comme le produit de deux entiers sont des entiers.

$$\boxed{\mathbb{Z} \text{ est un sous-anneau de } \mathbb{Q}.}$$

3. Même argument avec les rationnels.

$$\boxed{\mathbb{Q} \text{ est un sous-anneau de } \mathbb{R}.}$$

4. On a $1 = 1 + 0\sqrt{3}$. Soient $x = a + b\sqrt{3}$ et $y = c + d\sqrt{3}$ avec a, b, c, d entiers :

$$x - y = (a - c) + (b - d)\sqrt{3} \qquad \text{et} \qquad xy = (ac + 3bd) + (ad + bc)\sqrt{3}$$

les coefficients obtenus étant entiers.

$$\boxed{B \text{ est un sous-anneau de } \mathbb{R}.}$$

5. La fonction constante égale à 1 est continue, et la différence comme le produit de deux fonctions continues le sont.

$$\boxed{B \text{ est un sous-anneau de } \mathbb{R}^{\mathbb{R}}.}$$

6. La fonction constante égale à 1 ne s'annule pas en 0.

$$\boxed{B \text{ n'est pas un sous-anneau : il ne contient pas } 1_{\mathbb{R}^{\mathbb{R}}}.}$$

Piège : cette partie est pourtant stable par différence et par produit. C'est bien la condition $1_A \in B$ qui fait défaut, et elle n'est pas une formalité.

7. La fonction constante égale à 1 vérifie $f(1) = f(2)$. Et si $f(1) = f(2)$ et $g(1) = g(2)$, alors :

$$(f - g)(1) = f(1) - g(1) = f(2) - g(2) = (f - g)(2) \qquad (fg)(1) = f(1)g(1) = f(2)g(2) = (fg)(2)$$

$$\boxed{B \text{ est un sous-anneau de } \mathbb{R}^{\mathbb{R}}.}$$

EXERCICE 7 ⋆⋆

1. On a $1 = 1 + \mathrm{i} \times 0 \in \mathbb{Z}[\mathrm{i}]$. Soient $z = a + \mathrm{i}b$ et $z' = c + \mathrm{i}d$ avec a, b, c, d entiers :

$$z - z' = (a - c) + \mathrm{i}(b - d) \qquad \text{et} \qquad zz' = (ac - bd) + \mathrm{i}(ad + bc)$$

Les quatre coefficients obtenus sont entiers.

$$\boxed{\mathbb{Z}[\mathrm{i}] \text{ est un sous-anneau de } \mathbb{C}.}$$

2. (a) La conjugaison est un morphisme d'anneaux, donc $\overline{zz'} = \overline{z}\,\overline{z'}$:

$$N(z)N(z') = z\overline{z}\,z'\overline{z'} = (zz')(\overline{z}\,\overline{z'}) = (zz')\overline{(zz')} = N(zz')$$

$$\boxed{N(z)N(z') = N(zz')}$$

(b) Pour $z = a + \mathrm{i}b$ avec $(a\,;b) \in \mathbb{Z}^2$:

$$N(z) = z\overline{z} = (a+\mathrm{i}b)(a-\mathrm{i}b) = a^2+b^2$$

somme de deux carrés d'entiers.

$$\boxed{N(z) = a^2+b^2 \in \mathbb{N}}$$

(c) Soit z inversible dans $\mathbb{Z}[\mathrm{i}]$: il existe $z' \in \mathbb{Z}[\mathrm{i}]$ tel que $zz' = 1$. En appliquant N :

$$N(z)N(z') = N(1) = 1$$

Or $N(z)$ et $N(z')$ sont deux entiers naturels de produit 1 : ils valent tous deux 1.

$$\boxed{N(z) = 1}$$

(d) La condition $a^2+b^2 = 1$ avec a et b entiers impose $(a\,;b) \in \{(1\,;0)\,;(-1\,;0)\,;(0\,;1)\,;(0\,;-1)\}$. Réciproquement, ces quatre nombres sont bien inversibles dans $\mathbb{Z}[\mathrm{i}]$, puisque $1\times 1 = 1$, $(-1)\times(-1) = 1$ et $\mathrm{i}\times(-\mathrm{i}) = 1$.

$$\boxed{\text{Les inversibles de } \mathbb{Z}[\mathrm{i}] \text{ sont } 1,\ -1,\ \mathrm{i} \text{ et } -\mathrm{i}.}$$

On reconnaît le groupe $\mathbb{U}_4$ du chapitre 4.

EXERCICE 8 ⋆⋆

1. On a $1 = \dfrac{1}{1} \in A$, le dénominateur 1 étant impair. Soient $x = \dfrac{m}{n}$ et $y = \dfrac{m'}{n'}$ deux éléments de A, avec n et n' impairs. Alors :

$$x - y = \frac{mn' - m'n}{nn'} \qquad \text{et} \qquad xy = \frac{mm'}{nn'}$$

Le produit nn' de deux entiers impairs est impair, et les numérateurs sont entiers.

$$\boxed{A \text{ est un sous-anneau de } \mathbb{Q}.}$$

2. Soit x un élément non nul de A, écrit sous forme irréductible $x = \dfrac{m}{n}$ avec $n > 0$. Ce dénominateur est nécessairement impair : il divise le dénominateur impair d'une écriture quelconque de x.

L'élément x est inversible dans A si et seulement si $\dfrac{1}{x} = \dfrac{n}{m}$ appartient à A. Cette fraction étant déjà irréductible, cela équivaut à ce que $|m|$ soit impair.

$$\boxed{\begin{array}{l}\text{Les inversibles de } A \text{ sont les fractions } \dfrac{m}{n} \text{ irréductibles}\\ \text{dont le numérateur } \textit{et} \text{ le dénominateur sont impairs.}\end{array}}$$

Par exemple $\dfrac{3}{5}$ est inversible, alors que $\dfrac{2}{5}$ ne l'est pas : son inverse $\dfrac{5}{2}$ a un dénominateur pair.

EXERCICE 9 ⋆⋆

1. On a $B \cap C \subset A$. De plus 1_A appartient à B et à C, donc à $B \cap C$. Soient enfin x et y dans $B \cap C$. Comme B est un sous-anneau, $x - y$ et xy appartiennent à B ; comme C en est un, ils appartiennent aussi à C.

$$\boxed{B \cap C \text{ est un sous-anneau de } A.}$$

2. Le couple $(1\,;1)$ appartient à $\mathbb{Q}\times\mathbb{Z}$ comme à $\mathbb{Z}\times\mathbb{Q}$. Les deux parties sont stables par différence et par produit, ceux-ci se calculant coordonnée par coordonnée : ce sont bien deux sous-anneaux de $\mathbb{Q}^2$.

Considérons alors $\left(\frac{1}{2}\,;1\right) \in B$ et $\left(1\,;\frac{1}{2}\right) \in C$. Leur somme vaut :

$$\left(\frac{3}{2}\,;\frac{3}{2}\right)$$

dont aucune des deux coordonnées n'est entière : elle n'appartient ni à B, ni à C.

$B \cup C$ n'est pas stable par addition, donc n'est pas un sous-anneau de $\mathbb{Q}^2$.

3. Soit $(B_i)_{i\in I}$ une famille de sous-anneaux de A, et $B = \bigcap_{i\in I} B_i$. Chaque B_i contient 1_A, donc B aussi. Et si x et y appartiennent à B, alors pour tout i les éléments $x - y$ et xy appartiennent à B_i, donc à B.

Oui : une intersection quelconque de sous-anneaux est un sous-anneau.

On retrouve l'asymétrie déjà rencontrée aux chapitres 3 et 4 : l'intersection se comporte bien, la réunion non.

L'anneau $\mathbb{Z}/n\mathbb{Z}$

EXERCICE 10 ⋆

1. On calcule sur les représentants, puis on réduit modulo 7.

$$\overline{5}+\overline{4}=\overline{9}=\overline{2} \qquad \overline{3}\times\overline{5}=\overline{15}=\overline{1} \qquad \overline{6}^2=\overline{36}=\overline{1} \qquad \overline{2}^5=\overline{32}=\overline{4}$$

puisque $9 = 7 + 2$, $15 = 2 \times 7 + 1$, $36 = 5 \times 7 + 1$ et $32 = 4 \times 7 + 4$.

2. On procède de même modulo 12.

$$\overline{7}+\overline{8}=\overline{15}=\overline{3} \qquad \overline{5}\times\overline{9}=\overline{45}=\overline{9} \qquad \overline{4}\times\overline{3}=\overline{12}=\overline{0} \qquad -\overline{1}=\overline{11}$$

Le troisième calcul fournit au passage deux diviseurs de zéro de $\mathbb{Z}/12\mathbb{Z}$.

3. On calcule les puissances successives de $\overline{3}$ dans $\mathbb{Z}/7\mathbb{Z}$:

$$\overline{3}^1=\overline{3} \quad \overline{3}^2=\overline{2} \quad \overline{3}^3=\overline{6} \quad \overline{3}^4=\overline{4} \quad \overline{3}^5=\overline{5} \quad \overline{3}^6=\overline{1}$$

La suite est donc périodique de période 6. Or $100 = 6 \times 16 + 4$, d'où :

$$\overline{3}^{100} = (\overline{3}^6)^{16} \times \overline{3}^4 = \overline{1}^{16} \times \overline{4} = \overline{4}$$

Le reste de la division de 3^{100} par 7 vaut 4.

EXERCICE 11 ⋆

1. On calcule chaque produit ij puis son reste modulo 8.

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

2. Les lignes contenant le neutre $\overline{1}$, signalé en ocre, sont celles de $\overline{1}$, $\overline{3}$, $\overline{5}$ et $\overline{7}$. Dans chacune, le $\overline{1}$ se trouve sur la diagonale.

Les inversibles sont $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$, et chacun est son propre inverse.

Ce sont exactement les classes des entiers impairs, c'est-à-dire des entiers premiers avec 8.

3. Les zéros situés hors de la première ligne et de la première colonne, en bleu pétrole, signalent les diviseurs de zéro.

Les diviseurs de zéro sont $\overline{2}$, $\overline{4}$ et $\overline{6}$.

4. Les classes $\overline{2}$, $\overline{4}$ et $\overline{6}$ sont non nulles et non inversibles.

$\mathbb{Z}/8\mathbb{Z}$ n'est pas un corps, ce que le théorème 1 prévoyait puisque $8 = 2^3$ n'est pas premier.

On observe de plus que chaque classe non nulle est *soit* inversible, *soit* diviseur de zéro : c'est le résultat général de l'exercice 16.

EXERCICE 12 ⋆⋆

1. L'entier 7 étant premier, $\overline{3}$ est inversible dans $\mathbb{Z}/7\mathbb{Z}$, et $\overline{3} \times \overline{5} = \overline{15} = \overline{1}$ donne $\overline{3}^{-1} = \overline{5}$. En multipliant l'équation par $\overline{5}$:

$$\overline{x} = \overline{5} \times \overline{2} = \overline{10} = \overline{3} \qquad \text{d'où} \qquad \boxed{\mathcal{S} = \{\overline{3}\}}$$

2. Ici $\overline{3}$ n'est pas inversible dans $\mathbb{Z}/12\mathbb{Z}$, et l'on ne peut pas simplifier. On teste donc les douze classes, ou l'on remarque que $3x \equiv 0\ [12]$ équivaut à $12 \mid 3x$, c'est-à-dire $4 \mid x$:

$$\boxed{\mathcal{S} = \{\overline{0}\,;\,\overline{4}\,;\,\overline{8}\}}$$

3. On calcule les cinq carrés de $\mathbb{Z}/5\mathbb{Z}$: $\overline{0}$, $\overline{1}$, $\overline{4}$, $\overline{4}$, $\overline{1}$.

$$\boxed{\mathcal{S} = \{\overline{1}\,;\,\overline{4}\}}$$

4. La diagonale de la table de l'exercice 11 donne les huit carrés : $\overline{0}$, $\overline{1}$, $\overline{4}$, $\overline{1}$, $\overline{0}$, $\overline{1}$, $\overline{4}$, $\overline{1}$.

$$\boxed{\mathcal{S} = \{\overline{1}\,;\,\overline{3}\,;\,\overline{5}\,;\,\overline{7}\}}$$

Comparaison. L'équation $\overline{x}^{\,2} = \overline{1}$ s'écrit $(\overline{x} - \overline{1})(\overline{x} + \overline{1}) = \overline{0}$. Dans $\mathbb{Z}/5\mathbb{Z}$, qui est un corps d'après le théorème 1, il n'y a pas de diviseur de zéro : l'un des deux facteurs est nul, d'où au plus deux solutions. Dans $\mathbb{Z}/8\mathbb{Z}$, qui n'est pas un corps, le produit peut être nul sans qu'aucun facteur ne le soit — par exemple pour $\overline{x} = \overline{3}$, où $\overline{2} \times \overline{4} = \overline{0}$.

C'est l'absence de diviseurs de zéro qui limite le nombre de solutions dans un corps.

EXERCICE 13 ⋆⋆

1. On calcule les sept carrés de $\mathbb{Z}/7\mathbb{Z}$:

$$\overline{0}^{\,2} = \overline{0} \quad \overline{1}^{\,2} = \overline{1} \quad \overline{2}^{\,2} = \overline{4} \quad \overline{3}^{\,2} = \overline{2} \quad \overline{4}^{\,2} = \overline{2} \quad \overline{5}^{\,2} = \overline{4} \quad \overline{6}^{\,2} = \overline{1}$$

Les carrés de $\mathbb{Z}/7\mathbb{Z}$ sont $\overline{0}$, $\overline{1}$, $\overline{2}$ et $\overline{4}$: il y en a 4.

2. Notons $\mathcal{C}$ l'ensemble des carrés. Par définition, $\mathcal{A} = \{\overline{a} - \overline{c} \mid \overline{c} \in \mathcal{C}\}$. L'application $\overline{c} \mapsto \overline{a} - \overline{c}$ est injective, puisque $\overline{a} - \overline{c} = \overline{a} - \overline{c}\,'$ entraîne $\overline{c} = \overline{c}\,'$ dans le groupe $(\mathbb{Z}/7\mathbb{Z}\,;+)$.

$\mathcal{A}$ possède 4 éléments.

3. Les ensembles $\mathcal{C}$ et $\mathcal{A}$ sont deux parties de $\mathbb{Z}/7\mathbb{Z}$, qui compte 7 éléments. Or :

$$\operatorname{card}\mathcal{C} + \operatorname{card}\mathcal{A} = 4 + 4 = 8 > 7$$

Ils ne peuvent donc pas être disjoints. Soit alors $\overline{z}$ un élément commun : il existe $\overline{y}$ tel que $\overline{z} = \overline{y}^{\,2}$, et il existe $\overline{x}$ tel que $\overline{z} = -\overline{x}^{\,2} + \overline{a}$. En égalant :

$$\overline{y}^{\,2} = -\overline{x}^{\,2} + \overline{a} \qquad \text{c'est-à-dire} \qquad \overline{x}^{\,2} + \overline{y}^{\,2} = \overline{a}$$

$$\boxed{\text{L'équation } \overline{x}^{\,2} + \overline{y}^{\,2} = \overline{a} \text{ admet une solution pour tout } \overline{a} \in \mathbb{Z}/7\mathbb{Z}.}$$

4. On applique ce qui précède à $\overline{a} = -\overline{1} = \overline{6}$. Parmi les carrés, on cherche deux valeurs de somme $\overline{6}$: les carrés $\overline{2}$ et $\overline{4}$ conviennent, atteints respectivement en $\overline{3}$ et $\overline{2}$.

$$3^2 + 2^2 = 9 + 4 = 13 = 7 + 6$$

$$\boxed{(u\,;v) = (3\,;2) \text{ convient : } 3^2 + 2^2 \equiv -1\ [7].}$$

Corps

EXERCICE 14 ⋆

	Corps ?	Justification
$(\mathbb{Z}\,;+\,;\times)$	non	2 est non nul et non inversible.
$(\mathbb{Q}\,;+\,;\times)$	**oui**	Tout rationnel non nul $\frac{p}{q}$ a pour inverse $\frac{q}{p}$.
$\mathbb{Z}/5\mathbb{Z}$	**oui**	5 est premier (théorème 1).
$\mathbb{Z}/6\mathbb{Z}$	non	$6 = 2\times 3$ n'est pas premier ; $\overline{2}$ n'est pas inversible.
$\mathbb{Z}/11\mathbb{Z}$	**oui**	11 est premier.
$\mathbb{Z}/12\mathbb{Z}$	non	12 n'est pas premier ; $\overline{4}$ n'est pas inversible.
$(\mathbb{R}^2\,;+\,;\times)$	non	$(1\,;0)$ est un diviseur de zéro (exercice 3).
$(\mathbb{R}^{\mathbb{R}}\,;+\,;\times)$	non	Les fonctions de l'exercice 3 sont des diviseurs de zéro.

Piège : pour les deux derniers, il ne suffit pas de dire qu'une fonction peut s'annuler. C'est la présence de *diviseurs de zéro* qui interdit d'être un corps, d'après la question 5 de l'exercice 3.

EXERCICE 15 ⋆⋆

1. *Sous-anneau de* $\mathbb{C}$. On a $1 = 1 + \mathrm{i}\times 0 \in \mathbb{Q}[\mathrm{i}]$, et les calculs de l'exercice 7 restent valables avec des coefficients rationnels :

$$(a+\mathrm{i}b) - (c+\mathrm{i}d) = (a-c) + \mathrm{i}(b-d) \qquad (a+\mathrm{i}b)(c+\mathrm{i}d) = (ac-bd) + \mathrm{i}(ad+bc)$$

Commutativité. Elle est héritée de $\mathbb{C}$.

Inversibles. Soit $z = a + \mathrm{i}b$ non nul, c'est-à-dire $(a\,;b) \neq (0\,;0)$. Alors $a^2 + b^2$ est un rationnel strictement positif, et :

$$\frac{1}{a+\mathrm{i}b} = \frac{a-\mathrm{i}b}{a^2+b^2} = \frac{a}{a^2+b^2} - \mathrm{i}\,\frac{b}{a^2+b^2}$$

dont les deux coefficients sont rationnels.

$$\boxed{\mathbb{Q}[\mathrm{i}] \text{ est un corps.}}$$

2. *Sous-anneau de* $\mathbb{R}$. On a $1 = 1 + 0\sqrt{d}$, et :

$$(a+b\sqrt{d}\,) - (c+e\sqrt{d}\,) = (a-c) + (b-e)\sqrt{d} \qquad (a+b\sqrt{d}\,)(c+e\sqrt{d}\,) = (ac+d\,be) + (ae+bc)\sqrt{d}$$

Inversibles. Soit $x = a+b\sqrt{d}$ non nul. Montrons d'abord que $a^2 - db^2 \neq 0$. Supposons le contraire.

- Si $b = 0$, alors $a^2 = 0$, donc $a = 0$ et $x = 0$: exclu.
- Si $b \neq 0$, alors $d = \left(\dfrac{a}{b}\right)^2$, donc $\sqrt{d} = \left|\dfrac{a}{b}\right| \in \mathbb{Q}$, ce qui contredit l'hypothèse.

Le dénominateur ne s'annule donc jamais, et l'on peut écrire :

$$\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-db^2} = \frac{a}{a^2-db^2} - \frac{b}{a^2-db^2}\sqrt{d}$$

$$\boxed{\mathbb{Q}[\sqrt{d}\,] \text{ est un corps.}}$$

Piège : l'hypothèse $\sqrt{d} \notin \mathbb{Q}$ n'est pas décorative. Sans elle, $a^2 - db^2$ pourrait s'annuler pour un x non nul — et de fait, si $\sqrt{d}$ était rationnel, l'ensemble se réduirait à $\mathbb{Q}$.

EXERCICE 16 ⋆⋆

1. La classe $\overline{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement s'il existe $\overline{u}$ tel que $\overline{x}\,\overline{u} = \overline{1}$, c'est-à-dire :

$$\exists u \in \mathbb{Z},\ xu \equiv 1\ [n] \iff \exists (u\,;v) \in \mathbb{Z}^2,\ xu = 1 + (-v)n \iff \exists (u\,;v) \in \mathbb{Z}^2,\ xu + nv = 1$$

et le théorème de Bézout identifie cette dernière condition à la primalité entre x et n.

$$\boxed{\overline{x} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} \iff x \text{ et } n \text{ sont premiers entre eux.}}$$

2. Les entiers de $[\![0\,;9]\!]$ premiers avec 10 sont 1, 3, 7 et 9. On cherche les inverses en balayant les produits :

$$\overline{1} \times \overline{1} = \overline{1} \qquad \overline{3} \times \overline{7} = \overline{21} = \overline{1} \qquad \overline{9} \times \overline{9} = \overline{81} = \overline{1}$$

$$\boxed{\overline{1}^{\,-1} = \overline{1} \qquad \overline{3}^{\,-1} = \overline{7} \qquad \overline{7}^{\,-1} = \overline{3} \qquad \overline{9}^{\,-1} = \overline{9}}$$

3. Soit $\overline{x}$ non nul et non inversible. D'après la question 1, x et n ne sont pas premiers entre eux : notons $d > 1$ leur plus grand diviseur commun. Posons $y = \dfrac{n}{d}$, qui est un entier vérifiant $1 \leqslant y < n$, donc $\overline{y} \neq \overline{0}$. Comme d divise x :

$$xy = x \times \frac{n}{d} = \frac{x}{d} \times n \equiv 0\ [n]$$

$$\boxed{\overline{x}\,\overline{y} = \overline{0} \text{ avec } \overline{y} \neq \overline{0} : \text{la classe } \overline{x} \text{ est un diviseur de zéro.}}$$

Dans $\mathbb{Z}/n\mathbb{Z}$, tout élément non nul est donc *soit* inversible, *soit* diviseur de zéro : il n'y a pas de troisième possibilité.

4. D'après la question 1, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si tout entier x de $[\![1\,;n-1]\!]$ est premier avec n, c'est-à-dire si n n'admet aucun diviseur strictement compris entre 1 et n.

$$\boxed{\mathbb{Z}/n\mathbb{Z} \text{ est un corps si et seulement si } n \text{ est premier.}}$$

EXERCICE 17 ⋆

Trois conditions sont à vérifier : φ est un morphisme pour l'addition, $\varphi(xy) = \varphi(x)\varphi(y)$, et $\varphi(1_A) = 1_B$.

1. La conjugaison respecte la somme et le produit, et $\overline{1} = 1$. Morphisme d'anneaux.

2. C'est exactement la proposition 2 du cours, qui définit les deux lois de $\mathbb{Z}/n\mathbb{Z}$ par $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x}\,\overline{y} = \overline{xy}$, et l'on a $\overline{1} = 1_{\mathbb{Z}/n\mathbb{Z}}$. Morphisme d'anneaux.

3. On a $(f+g)(a) = f(a) + g(a)$, $(fg)(a) = f(a)g(a)$, et la fonction constante égale à 1 vaut 1 en a. Morphisme d'anneaux.

4. L'application est additive, mais $\varphi(1) = 2 \neq 1$. Non : la condition sur 1 échoue.

5. On a $|1 + (-1)| = 0$ alors que $|1| + |-1| = 2$. Non : l'application n'est pas additive.

6. On a $\varphi(x+y) = (x+y\,;x+y) = \varphi(x) + \varphi(y)$, $\varphi(xy) = (xy\,;xy) = \varphi(x)\varphi(y)$, et $\varphi(1) = (1\,;1) = 1_{\mathbb{Z}^2}$. Morphisme d'anneaux.

7. L'application est additive et multiplicative, car $(x\,;0)(y\,;0) = (xy\,;0)$. Mais $\varphi(1) = (1\,;0)$, alors que le neutre de $\mathbb{Z}^2$ est $(1\,;1)$. Non : la condition sur 1 échoue.

8. On a $\varphi(1+1) = 4$ alors que $\varphi(1) + \varphi(1) = 2$. Non : l'application n'est pas additive.

Piège de la question 7 : cette application satisfait les deux conditions portant sur les lois, et échoue uniquement sur $\varphi(1_A) = 1_B$. C'est la meilleure justification de la remarque du cours : cette condition doit être exigée séparément, car elle ne se déduit pas des autres.

EXERCICE 18 ⋆⋆

1. L'application φ étant en particulier un morphisme du groupe $(A\,;+)$ dans le groupe $(B\,;\oplus)$, la proposition 3 du chapitre 4 s'applique directement.

$$\boxed{\operatorname{Ker}\varphi \text{ est un sous-groupe de } (A\,;+).}$$

2. Soient $x \in \operatorname{Ker}\varphi$ et $a \in A$. Alors :

$$\varphi(ax) = \varphi(a) \otimes \varphi(x) = \varphi(a) \otimes 0_B = 0_B$$

la dernière égalité venant de la question 1 de l'exercice 2, appliquée dans l'anneau B. Le calcul est identique pour xa.

$$\boxed{\forall x \in \operatorname{Ker}\varphi,\ \forall a \in A, \quad ax \in \operatorname{Ker}\varphi \text{ et } xa \in \operatorname{Ker}\varphi.}$$

Une partie vérifiant ces propriétés s'appelle un *idéal* de A : elle est bien plus que stable, elle est *absorbante*.

3. Un sous-anneau doit contenir 1_A. Or $1_A \in \operatorname{Ker}\varphi$ signifierait $\varphi(1_A) = 0_B$, alors que $\varphi(1_A) = 1_B$ par définition d'un morphisme d'anneaux. Il faudrait donc $1_B = 0_B$, ce que la définition d'un anneau interdit.

$$\boxed{\operatorname{Ker}\varphi \text{ n'est jamais un sous-anneau de } A.}$$

4. Pour la réduction modulo n, on a $\overline{x} = \overline{0}$ si et seulement si n divise x. Pour l'évaluation en a, on cherche les fonctions d'image nulle en a.

$$\boxed{\operatorname{Ker}\pi = n\mathbb{Z} \qquad \text{et} \qquad \operatorname{Ker}\left(f \mapsto f(a)\right) = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(a) = 0\}}$$

Le premier noyau justifie la notation $\mathbb{Z}/n\mathbb{Z}$: c'est le quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

EXERCICE 19 ⋆⋆

1. *Initialisation.* On a $\varphi(0) = 0_A$ puisque φ est un morphisme de groupes additifs, et $0 \cdot 1_A = 0_A$ par convention.

Hérédité. Supposons $\varphi(n) = n \cdot 1_A$. Alors :

$$\varphi(n+1) = \varphi(n) + \varphi(1) = n \cdot 1_A + 1_A = (n+1) \cdot 1_A$$

en utilisant $\varphi(1) = 1_A$, qui fait partie de la définition d'un morphisme d'anneaux.

Extension à $\mathbb{Z}$. Pour $n < 0$, la propriété 1 du chapitre 4 donne :

$$\varphi(n) = \varphi(-(-n)) = -\varphi(-n) = -((-n) \cdot 1_A) = n \cdot 1_A$$

$$\boxed{\forall n \in \mathbb{Z}, \quad \varphi(n) = n \cdot 1_A}$$

2. L'expression obtenue ne dépend que de l'anneau A, et nullement du morphisme choisi : deux morphismes d'anneaux de $\mathbb{Z}$ dans A coïncident donc en tout point.

$$\boxed{\text{Il existe au plus un morphisme d'anneaux de } \mathbb{Z} \text{ dans } A.}$$

Remarque : on vérifie sans peine que $n \mapsto n \cdot 1_A$ en est effectivement un. L'anneau $\mathbb{Z}$ occupe donc une place particulière : il se envoie d'une unique façon dans n'importe quel anneau.

3. Pour $A = \mathbb{Z}/n\mathbb{Z}$, le neutre est $\overline{1}$ et $k \cdot \overline{1} = \overline{k}$: le morphisme est la réduction modulo n. Pour $A = \mathbb{R}$, le neutre est 1 et $k \cdot 1 = k$: le morphisme est l'inclusion de $\mathbb{Z}$ dans $\mathbb{R}$.

$$\boxed{\operatorname{Ker}\varphi = n\mathbb{Z} \text{ dans le premier cas} \qquad \operatorname{Ker}\varphi = \{0\} \text{ dans le second.}}$$

Exercices de synthèse

EXERCICE 20 : VRAI OU FAUX

1. **Vraie** Ce sont les diviseurs de zéro, signalés par le cours et rencontrés dans $\mathbb{R}^2$, $\mathbb{R}^{\mathbb{R}}$ et $\mathbb{Z}/6\mathbb{Z}$ (exercice 3).

2. **Vraie** Seule l'addition est supposée commutative dans la définition. L'anneau des matrices carrées de l'exercice 21 en est un contre-exemple.

3. **Fausse** L'ensemble $2\mathbb{Z}$ ne contient pas 1 : la première condition de la proposition 1 échoue (exercice 6).

4. **Vraie** C'est exactement la définition du cours.

5. **Vraie** C'est le théorème 1, redémontré de deux façons aux exercices 16 et 22.

6. **Vraie** Un élément inversible n'est jamais diviseur de zéro (exercice 3), et dans un corps tout élément non nul l'est.

7. **Fausse** L'application $x \mapsto (x\,;0)$ de $\mathbb{Z}$ dans $\mathbb{Z}^2$ est additive et multiplicative, mais envoie 1 sur $(1\,;0) \neq (1\,;1)$. La condition doit donc être exigée à part.

8. **Fausse** Il ne contient jamais 1_A (exercice 18). C'est un *idéal*, ce qui est une autre notion.

9. **Vraie** Le développement donne $x^2 + xy + yx + y^2$, et les deux termes centraux se regroupent lorsque $xy = yx$ (exercice 2).

10. **Fausse** L'ensemble $\mathbb{Z}$ est un sous-anneau du corps $\mathbb{Q}$, sans être un corps : 2 n'y est pas inversible.

EXERCICE 21 ⋆⋆⋆

1. La matrice identité s'obtient pour $a = 1$ et $b = 0$, donc $I_2 \in \mathcal{C}$. Soient ensuite deux éléments de $\mathcal{C}$. Leur différence vaut :

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

qui est encore de la forme voulue. Quant au produit, la formule donnée fournit :

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix}$$

$\mathcal{C}$ est un sous-anneau de $\mathcal{M}$.

2. Les deux coefficients $ac-bd$ et $ad+bc$ du produit sont inchangés lorsqu'on échange le couple $(a\,;b)$ et le couple $(c\,;d)$.

$\mathcal{C}$ est commutatif, bien que $\mathcal{M}$ ne le soit pas.

3. Soit M un élément non nul de $\mathcal{C}$, c'est-à-dire $(a\,;b) \neq (0\,;0)$. Posons $N = a^2+b^2 > 0$ et considérons :

$$M' = \begin{pmatrix} \frac{a}{N} & \frac{b}{N} \\ -\frac{b}{N} & \frac{a}{N} \end{pmatrix}$$

qui appartient à $\mathcal{C}$, avec les coefficients $\frac{a}{N}$ et $-\frac{b}{N}$. Le produit vaut :

$$M \times M' = \begin{pmatrix} \frac{a^2+b^2}{N} & \frac{-ab+ab}{N} \\ \frac{ab-ab}{N} & \frac{a^2+b^2}{N} \end{pmatrix} = I_2$$

Comme $\mathcal{C}$ est commutatif, le produit dans l'autre ordre donne le même résultat.

$\mathcal{C}$ est un anneau commutatif dont tout élément non nul est inversible : c'est un corps.

4. L'application ϕ est bijective, de réciproque $a+\mathrm{i}b \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Elle est additive d'après le calcul de la question 1, et l'on vérifie qu'elle respecte le produit :

$$\phi(M \times M') = (ac-bd) + \mathrm{i}(ad+bc) = (a+\mathrm{i}b)(c+\mathrm{i}d) = \phi(M) \times \phi(M')$$

Enfin $\phi(I_2) = 1$.

ϕ est un isomorphisme d'anneaux de $\mathcal{C}$ sur $\mathbb{C}$.

Les nombres complexes admettent donc une réalisation matricielle : la multiplication par $a+\mathrm{i}b$ dans $\mathbb{C}$ n'est autre que cette matrice, qui est d'ailleurs celle d'une similitude directe du plan.

EXERCICE 22 ⋆⋆⋆

1. Soient x et y dans A tels que $m_a(x) = m_a(y)$, c'est-à-dire $ax = ay$. Alors, par distributivité :

$$a(x-y) = ax - ay = 0_A$$

Comme $a \neq 0_A$ et que A ne possède aucun diviseur de zéro, il vient $x-y = 0_A$.

m_a est injective.

2. L'application m_a est une application injective de l'ensemble *fini* A dans lui-même. D'après la question 4 de l'exercice 17 du chapitre 4, elle est donc surjective.

m_a est surjective.

3. En particulier, 1_A possède un antécédent : il existe $b \in A$ tel que $ab = 1_A$, et $ba = 1_A$ par commutativité. Ainsi tout élément non nul de A est inversible, et A est un anneau commutatif non nul.

A est un corps.

4. Soient $\overline{x}$ et $\overline{y}$ dans $\mathbb{Z}/p\mathbb{Z}$ tels que $\overline{x}\,\overline{y} = \overline{0}$ avec $\overline{x} \neq \overline{0}$. L'égalité signifie que p divise xy, donc, par le lemme d'Euclide, que p divise x ou p divise y. Le premier cas donnerait $\overline{x} = \overline{0}$, ce qui est exclu : donc p divise y, c'est-à-dire $\overline{y} = \overline{0}$.

$\mathbb{Z}/p\mathbb{Z}$ ne possède aucun diviseur de zéro lorsque p est premier.

5. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est commutatif, fini — il compte p éléments — et sans diviseur de zéro d'après la question 4. Les questions 1 à 3 s'appliquent donc.

Si p est premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Cette démonstration n'utilise pas le théorème de Bézout, contrairement à celle du cours et à celle de l'exercice 16 : elle repose uniquement sur la finitude de l'anneau et sur le lemme d'Euclide.